มาตรการในการคุ้มครองข้อมูลชีวมาตร ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

Personal Data Protection Act B.E. 2562: Rules and Guidelines on Thailand's Biometric Personal Data Protection

ทัชชภร มหาแถลง

Thatchaporn Mahathalang

คณะนิติศาสตร์ มหาวิทยาลัยศรีปทุม กรุงเทพมหานคร ประเทศไทย

School of Law Sripatum University Bangkok Thailand

E-mail: thatchaporn.ma@spu.ac.th

บทคัดย่อ

ประเทศไทยได้ประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อกำหนดหลักเกณฑ์กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคล สำหรับป้องกันการละเมิดข้อมูลส่วนบุคคลที่ก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล และประเทศชาติโดยรวม โดยเฉพาะการจัดเก็บข้อมูลชีวมาตร ปัญหาดังกล่าวมีผลมาจากความก้าวหน้าทางเทคโนโลยีที่ทำให้การเข้าถึงข้อมูลส่วนบุคคลได้โดยง่าย อย่างไรก็ตาม ยังพบว่ากฎหมายฉบับนี้ในเรื่องของการเก็บรวมรวม ใช้ ประมวลผล และการส่งหรือโอนข้อมูลไปยังต่างประเทศยังเป็นประเด็นที่สมควรนำมาพิจารณาศึกษาเพิ่มเติม สำหรับปรับปรุง แก้ไข หรือเพิ่มเติมบทบัญญัติกฎหมายของประเทศไทย อันเป็นประโยชน์ด้านการคุ้มครองข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพมากยิ่งขึ้น โดยได้ศึกษาเปรียบเทียบจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศ

คำสำคัญ: *กฎหมายคุ้มครองข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคล ข้อมูลชีวภาพ*

Abstract

Thailand has enacted the Personal Data Protection Act B.E. 2562 to set the criteria, mechanisms, or regulatory measures on personal data protection in order to prevent personal data breaches that cause damage to the personal data and the country as a whole, especially the biometric data. Such problem is the result from advanced technology that makes it easier to access personal information. However, this law concerning on collection, usage, ย

processing and transmission, or transferring information abroad is still to be considered for further study by comparing the international data protection laws to improve, amend, or add to the statutory provisions of such Act for the benefit and the effectiveness of personal information protection.

Keywords: *Personal data protection law, Personal data, Biometric Information.*

1. บทนำ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ได้ประกาศในราชกิจจานุเบกษาเมื่อวันที่ 24 พฤษภาคม 2562 และกฎหมายฉบับดังกล่าวจะมีผลบังคับใช้เมื่อพ้นกำหนด 1 ปีนับตั้งแต่ที่ได้ประกาศในราชกิจจานุเบกษา และกฎหมายฉบับนี้จะมีผลกระทบทั้งต่อภาคประชาชน หน่วยงานรัฐและหน่วยงานเอกชน เนื่องจากปัจจุบันมีการล่วงละเมิด สิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวก และรวดเร็ว แม้จะมีกฎหมายฉบับนี้ออกมาควบคุมในการรวบรวมและเก็บข้อมูลส่วนบุคคลแล้ว แต่ยังมีประเด็นที่น่าคิดว่าในทางปฏิบัติหรือการบังคับใช้กฎหมายฉบับนี้ เช่น ประเด็นเรื่องการเก็บข้อมูลส่วนบุคคล ซึ่งในส่วนของกฎหมายจะมีข้อมูลที่จำเป็นหรือบังคับให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บได้ หรือเป็นกรณีการให้ความยินยอม (consent) ของผู้เป็นเจ้าของข้อมูลส่วนบุคคลที่จะยินยอมให้เก็บข้อมูลส่วนบุคคลดังกล่าวหรือไม่ และอีกประเด็นคือเรื่องการเก็บข้อมูลชีวมาตร (Biometrics) และการใช้เทคโนโลยีชีวมาตรของหน่วยงานรัฐหรือหน่วยงานเอกชนกับความเสี่ยงที่อาจมีการละเมิดสิทธิส่วนบุคคล

ข้อมูลชีวมาตรเป็นข้อมูลส่วนบุคคลที่เกิดจากการประมวลผลทางเทคนิคเฉพาะที่เกี่ยวข้องกับลักษณะทางกายภาพ สรีรวิทยา และพฤติกรรมของคนตามธรรมชาติ เช่น ภาพใบหน้า ลายนิ้วมือ หรือม่านตา (มติชน, 2562) ส่วนเทคโนโลยีชีวมาตร (Biometrics Technology) เป็นแนวคิดการนำเอาเทคโนโลยีด้านชีวภาพทางการแพทย์และเทคโนโลยีด้านคอมพิวเตอร์มาบูรณาการเข้าด้วยกัน เพื่อใช้กำหนดหรือระบุคุณลักษณะเฉพาะส่วนบุคคลทั้งด้านกายภาพและพฤติกรรม (สุพล พรหมมาพันธุ์, 2563) ได้แก่ เทคโนโลยีการจดจำใบหน้า (Face Recognition Technology) เทคโนโลยีจดจำลายนิ้วมือ เทคโนโลยีจดจำม่านตา ซึ่งเทคโนโลยีชีวมาตรที่กล่าวมานี้ เป็นเทคโนโลยีในการระบุตัวตน (Identification) และการพิสูจน์ยืนยันตัวบุคคล (Verification) ซึ่งเทคโนโลยีชีวมาตรนี้ ได้ถูกนำมาใช้ในชีวิตประจำวันของเราหลายๆอย่าง เช่น การสแกนลายนิ้วมือ สแกนใบหน้าในการใช้โทรศัพท์มือถือ การระบุเวลาเข้า-ออกในการทำงาน การเข้า-ออกสถานที่พักอาศัยหรือหน่วยงานต่างๆ การชำระเงินหรือการใช้บัตรเครดิตทางออนไลน์ การทำธุรกรรมทางการเงินออนไลน์ เป็นต้น

ปัจจุบันมีการเก็บข้อมูลชีวมาตรของประชาชน บันทึกในฐานข้อมูลของหน่วยงานรัฐและเอกชนเป็นจำนวนมาก เช่น ฐานข้อมูลบัตรประชาชนของกรมการปกครอง กระทรวงมหาดไทย การจัดเก็บข้อมูลส่วนบุคคลในการทำหนังสือเดินทาง (Passport) ของกระทรวงการต่างประเทศ การจัดเก็บอัตลักษณ์ในการลงทะเบียนซิมการ์ดของสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) ที่ได้มีการ

ออกประกาศให้หน่วยงานเอกชนที่ประกอบกิจการโทรคมนาคมไปดำเนินการ เป็นต้น ด้วยวิธีการไม่ว่าจะเป็นการเก็บภาพถ่าย การเก็บข้อมูลบัตรประชาชน การพิสูจน์อัตลักษณ์และลายนิ้วมือ รวมถึงม่านตาทำให้มีความเสี่ยงที่จะเกิดการรั่วไหลหรือนำไปใช้ประโยชน์ในทางที่มิชอบ เกิดความเสียหายต่อผู้เป็นเจ้าของข้อมูลฯ เพราะข้อมูลเหล่านี้เป็นข้อมูลเฉพาะตัวบุคคลที่สามารถระบุอัตลักษณ์ตัวบุคคล เจ้าของข้อมูลไม่สามารถแก้ไขข้อมูลชีวมาตรของตนเองได้ อีกทั้งยังส่งผลกระทบต่อความมั่นคงและเศรษฐกิจของประเทศ ดังนั้น สมควรที่จะมีมาตรการหรือแนวทางปฏิบัติสำคัญหรือเป็นการเฉพาะที่ภาครัฐจะต้องตระหนักและให้ความสนใจ เพื่อป้องกันไม่ให้เกิดปัญหาที่กล่าวมานี้

จากบริบทในสังคมโลกปัจจุบันที่มีความก้าวหน้าของเทคโนโลยีสารสนเทศ การเชื่อมต่อกันด้วยเทคโนโลยีสารสนเทศทำให้ง่ายต่อการสืบค้นและเข้าถึงข้อมูลต่างๆ ได้อย่างสะดวกรวดเร็วยิ่งขึ้น และยังสามารถเผยแพร่หรือถ่ายโอนข้อมูลจากที่หนึ่งไปยังอีกที่หนึ่งได้อย่างรวดเร็ว ประกอบกันสถานการณ์การระบาดของไวรัสโคโรน่า (COVID – 19) ในปัจจุบันของประเทศไทยทำให้วิถีชีวิตและการดำเนินกิจกรรมต่างๆ เปลี่ยนแปลงไปอย่างมาก มีการใช้เทคโนโลยีมากยิ่งขึ้น มีการใช้แอพพลิเคชั่นต่างๆ ทั้งของหน่วยงานภาครัฐ เช่น หมอชนะ ที่เมื่อผู้ใช้ดาวน์โหลดแอพพลิเคชั่นดังกล่าวจะต้องมีการจัดเก็บข้อมูลอัตลักษณ์ด้วยวิธีการถ่ายภาพ เป็นต้น รวมถึงภาคเอกชนเช่นกัน ข้อมูลส่วนบุคคล โดยแฉพาะอย่างยิ่งข้อมูลชลีวมาตรจึงมีความสำคัญมากยิ่งขึ้น และมีความเสี่ยงโดยง่ายที่จะถูกเอาไปใช้โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลก่อน ซึ่งอาจส่งผลกระทบกระเทือนต่อประโยชน์ส่วนบุคคล ตลอดจนชื่อเสียงเกียรติยศ และประเทศชาติโดยรวม ดังที่ปรากฏเป็นข่าวเรื่องการละเมิดความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลเกิดขึ้นทั่วโลก ตัวอย่าง บริษัทด้านการตลาด Exactis ของมลรัฐฟอริดา ประเทศสหรัฐอเมริกา ทำข้อมูลลูกค้ารั่วไหลส่งผลกระทบต่อประชาชนจำนวน 340 ล้านคน ทำให้มลรัฐแคลิฟอเนียได้มีการปรับปรุงกฎหมาย The California Consumer Privacy Act 2018 บริษัท British Airway ได้ทำข้อมูลผู้ใช้งานหลายแสนรายที่ใช้บัตรเครดิตเกี่ยวกับส่วนของรางวัลหลุดออกไปด้วยฝีมือของแฮคเกอร์ Amazon ยอมรับเกิดเหตุผิดพลาดทางเทคนิคจนเป็นเหตุให้ข้อมูล ชื่อ และ อีเมลของลูกค้าหลุดไป หรือแม้กระทั่ง Facebook ยังเคยประสบปัญหาดังกล่าวเช่นกัน และในประเทศไทยในกรณีบริษัท Lazada ทำข้อมูลลูกค้ารั่วไหล ซึ่งบริษัทได้ยืนยันว่า ไม่ได้รั่วไหลมาจากระบบของลาซาด้า แต่สันนิษฐานว่าเกิดจากผู้ประกอบการที่รับช่วงต่อการขาย เป็นต้น เหตุการณ์ดังกล่าวได้ส่งผลให้ทุกภาคส่วนเกิดความตระหนักว่าข้อมูลพื้นฐานหรือข้อมูลส่วนบุคคลที่เป็นส่วนหนึ่งของการเข้าถึงระบบเทคโนโลยีสารสนเทศสมัยใหม่จะถูกนำไปใช้ประโยชน์ หรือเป็นโทษหากไม่ได้รับการคุ้มครองที่ปลอดภัยและเชื่อถือได้

2. รายละเอียด

2.1 มาตรการทางกฎหมายของประเทศไทยในการคุ้มครองข้อมูลชีวมาตร

ในส่วนของกฎหมายไทยนั้น รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ได้มีบทบัญญัติมาตรา 32 ที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลไว้ว่า

“บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว

การกระทำอันละเมิดหรือกระทบต่อสิทธิของบุคคลตามวรรคหนึ่ง หรือการนำข้อมูลส่วนบุคคลไปใช้ในประโยชน์ไม่ว่าในทางใดๆ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย ที่ตราขึ้นเพียงเท่าจำเป็นเพื่อประโยชน์สาธารณะ”

แต่เดิมก่อนที่จะมีการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ได้มีพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 ที่มีบทบัญญัติถึงการคุ้มครองข้อมวลส่วนบุคคลของประชาชนที่อยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐ ต่อมาได้มีหน่วยงานที่ต้องเกี่ยวข้องกับการเก็บรักษาข้อมูลส่วนบุคคลได้มีมาตรการเพื่อคุ้มครองข้อมูลส่วนบุคคล เช่น ประกาศของธนาคารแห่งประเทศไทย เรื่อง หลักเกณฑ์การกำกับดูแลผู้ให้บริการระบบชำระเงินที่มีความสำคัญ ข้อ 4.2.5 (3) ได้วางหลักเกณฑ์ด้านการคุ้มครองสมาชิกเกี่ยวกับการเก็บรักษาข้อมูลของสมาชิก ทั้งการกำหนดนโยบายในการเก็บรักษาข้อมูลส่วนบุคคล การเข้าถึงข้อมูลส่วนบุคคล การจัดระบบการจัดเก็บข้อมูลส่วนบุคคลและการรักษาความลับของข้อมูลส่วนบุคคล ประกาศคณะกรรมการกิจการโทรคมนาคมแห่งชาติ เรื่อง มาตรการคุ้มครองสิทธิของผู้ใช้บริการเกี่ยวกับข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัวและเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม ข้อ 8 ที่วางหลักเกณฑ์ให้ผู้รับใบอนุญาตจะต้องเก็บรักษาข้อมูลส่วนบุคคลของผู้ใช้บริการตลอดระยะเวลา 3 เดือนสุดท้ายของการใช้บริการนับถัดจากวันที่ใช้บริการในปัจจุบัน และข้อ 3 ที่วางหลักเกณฑ์ให้ผู้รับใบอนุญาตจะประมวลผลข้อมูลส่วนบุคคลได้โดยได้รับความยินยอมจากผู้ใช้บริการ และต้องกระทำเพื่อประโยชน์ในการดำเนินกิจการโทรคมนาคมเท่านั้น เป็นต้น

ภายหลังได้มีการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งมีผลบังคับใช้ไปกาลทั่วไปแล้วนั้น หากพิจารณากฎหมายฉบับนี้จะพบว่าบทบัญญัติมาตรา 24 (1) มีหลักการห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการป้องกันที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล (2) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล (3) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น (4) เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินการภารกิจเพื่อประโยชน์สาธารณะของเจ้าของข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้รับมอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล ตลอดจน (5) เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลหรือนิติบุคคลเว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลรวมถึง (6) เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

อีกทั้งบทบัญญัติมาตรา 27 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลตามความนิยามมาตรา 6 ใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้น ไม่ต้องขอความยินยอมตามมาตรา 24 ที่กล่าวมาข้างต้นหรือข้อยกเว้นการเก็บรวมรวมข้อมูลส่วนบุคคลโดยปราศจากความยินยอมของเจ้าของข้อมูลส่วนบุคคลตามบทบัญญัติ

มาตรา 26 เช่นกัน กล่าวคือ ข้อยกเว้นทั้ง 2 มาตรานี้ เป็นไปเพื่อความจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะด้านต่างๆของผู้ควบคุม ข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล รวมถึงเป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

อย่างไรก็ตาม หากพิจารณาต่อในส่วนของ มาตรา 26 แม้จะห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับข้อมูลชีวภาพ โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล แต่บทบัญญัติของกฎหมายดังกล่าวได้ปรากฏถึงข้อยกเว้นให้ทั้งภาครัฐและภาคเอกชนสามารถเก็บรวบรวมข้อมูลส่วนบุคคลได้โดยปราศจากความยินยอม ดังนั้น อาจเป็นการเปิดโอกาสให้หน่วยงานของรัฐหลายแห่งที่เกี่ยวข้องกับการจัดเก็บข้อมูลส่วนบุคคลใช้อำนาจรัฐเก็บข้อมูลชีวมาตรของประชาชน โดยไม่ได้พิจารณาเหตุผลและความจำเป็นอย่างรอบคอบ ซึ่งอาจมีผลกระทบต่อผู้เป็นเจ้าของข้อมูลชีวมาตรในกรณีที่ข้อมูลรั่วไหลและถูกนำไปใช้โดยมิชอบได้

นอกจากนี้เรื่องการส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศที่ต้องนำมาและพิจารณาถึงแนวทางการป้องกันการรั่วไหลข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งข้อมูลชีวมาตรอีกด้วย ดังนี้ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 16 ได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลจะต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ และเป็นไปตามหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลตามที่คณะกรรมการประกาศกำหนด เว้นแต่เป็นการปฏิบัติตามกฎหมายหรือได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศ เป็นความจำเป็นเพื่อปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น และเป็นการกระทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลเพื่อประโยชน์ของเจ้าของมูลส่วนบุคคล ตลอดจนเพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคล หรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้ รวมถึงเป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญตามบทบัญญัติมาตรา 28 ของกฎหมายฉบับเดียวกัน

จากหลักการเก็บรวบรวม การใช้ข้อมูลส่วนบุคคล การส่งหรือโอนข้อมูลส่วนบุคคลข้างต้น ผู้เขียนมีข้อสังเกตว่ากฎหมายฉบับนี้มุ่งที่จะให้ความสำคัญกับหลักความยินยอม (consent) ของเจ้าของข้อมูลส่วนบุคคลเป็นประการสำคัญอันจะเข้าข้อยกเว้นที่หน่วยงานหรือองค์กรต่างๆ โดยเฉพาะอย่างยิ่งภาคเอกชนผู้ควบคุมข้อมูลส่วนบุคคลสามารถกระทำได้ แต่สิ่งที่น่ากังวล คือ การรั่วไหลของข้อมูลส่วนบุคคลจากมาตรฐานการจัดเก็บ การส่ง และการโอนข้อมูลส่วนบุคคล และผู้เขียนมีความเห็นว่าเป็นการให้พื้นที่ของภาคเอกชนในการดำเนินการส่งหรือโอนข้อมูลส่วนบุคคล ทั้งนี้ แม้ว่ากฎหมายจะให้อำนาจและหน้าที่แก่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นผู้วินิจฉัยกรณีที่มีปัญหาเกี่ยวกับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลตามบทบัญญัติมาตรา 28 วรรคสองพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ก็ตาม

นอกจากนี้ ยังพบในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลตามคำนิยามมาตรา 6 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ซึ่งอยู่ในราชอาณาจักรได้กำหนดนโยบายในการคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ต่างประเทศและอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน หากนโยบายในการคุ้มครองข้อมูลส่วนบุคคลดังกล่าวได้รับการตรวจสอบและรับรองจากสำนักงาน การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศที่เป็นไปตามนโยบายในการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับกาตรวจสอบและรับรองดังกล่าวให้สามารถกระทำได้โดยได้รับยกเว้นไม่ต้องปฏิบัติตามหลักกฎหมายการส่งหรือโอนข้อมูลไปยังต่างประเทศข้างต้นประกอบกับนโยบายในการคุ้มครองข้อมูลส่วนบุคคล ลักษณะของเครือกิจการหรือธุรกิจเดียวกันเพื่อการประกอบกิจการธุรกิจร่วมกัน และหลักเกณฑ์และวิธีการตรอบสอบให้เป็นไปตามที่คณะกรรมการกำหนดตามมาตรา 29 ตลอดจนการเข้าข้อยกเว้นในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลข้อมูลส่วนบุคคลได้จัดให้มีมาตรการคุ้มครองที่เหมาะสมสามารถบังคับตามสิทธิของเจ้าของข้อมูลส่วนบุคคลได้ รวมทั้งมีมาตรการเยียวยาทางกฎหมายที่มีประสิทธิภาพตามหลักเกณฑ์และวิธีการที่คณะกรรมการกำหนดไม่จำเป็นต้องปฏิบัติตามหลักเกณฑ์มาตรา 28 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ตามมาตรา 29 วรรคสามของกฎหมายฉบับเดียวกัน

ผู้เขียนมีความเห็นว่าเป็นการเพิ่มพื้นทีให้ภาคเอกชนง่ายต่อการดำเนินการส่งหรือโอนข้อมูลส่วนบุคคลโดยเฉพาะข้อมูลชีวมาตรไปยังต่างประเทศมากยิ่งขึ้น โดยอาศัยอำนาจดุลพินิจของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นสาระสำคัญ ดังนั้น สมควรมีมาตรการ มาตรฐาน และระบบการตรวจสอบให้มีความเป็นมาตรฐานอย่างมีประสิทธิภาพและสามารถนำมาใช้ได้อย่างเป็นรูปธรรม เพื่อป้องกันการรั่วไหลของข้อมูลส่วนบุคคล โดยเฉพาะข้อมูลชีวมาตร ตลอดจนมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลทางกฎหมายให้มีความชัดเจน ทั้งนี้ผู้เขียนได้ศึกษาหลักเกณฑ์ แนวทาง และมาตรการทางกฎหมายของต่างประเทศ

2.2 มาตรการของต่างประเทศในการคุ้มครองข้อมูลชีวมาตร

ผู้เขียนได้ศึกษาถึงมาตรการทางกฎหมาย แนวทางหรือแนวปฏิบัติ และหลักเกณฑ์ต่างๆ ที่มีผลบังคับใช้ของต่างประเทศ ดังนี้ การคุ้มครองข้อมูลส่วนบุคคลตามแนวทางขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data) เป็นแนวทางปฏิบัติขั้นต่ำเพื่อให้ประเทศสมาชิกได้นำไปปฏิบัติภายในแต่ละประเทศ แนวปฏิบัตินี้ไม่ได้แยกระหว่างหน่วยงานรัฐและหน่วยงาน ภาคเอกชน และไม่ได้แยกว่าเป็นการประมวลผลข้อมูลเกี่ยวกับบุคคลโดยวิธีอัตโนมัติหรือวิธี ประมวลผลด้วยมือ โดยความหมายของข้อมูลส่วนบุคคล (Personal data) หมายถึง ข้อมูลใด ๆ ที่เกี่ยวข้องเฉพาะตัวบุคคล หรือสามารถชี้ให้เห็นลักษณะเฉพาะตัวของบุคคลที่เป็นเจ้าของข้อมูลได้ โดยมีหลักการในการคุ้มครองข้อมูลส่วนบุคคลด้วยกัน 8 ข้อ (OECD, 2013) ให้ถือปฏิบัติ นอกจากนี้ ยังมีการคุ้มครองข้อมูลส่วนบุคคลในทางสากลที่ปรากฏอยู่ในกฎหมายระหว่างประเทศ ได้แก่ ข้อบังคับสหภาพยุโรป (European Directive 95/46/EC) ข้อตกลงรัฐสภายุโรป (Council of Europe) กรอบการคุ้มครองข้อมูลส่วนบุคคล GDPR ของสหภาพยุโรป (General Data Protection

Regulation) และกรอบคุ้มครองข้อมูลส่วนบุคคลของกลุ่มความร่วมมือทางเศรษฐกิจเอเชีย – แปซิฟิก (APEC) (APEC Privacy Framework)

ในส่วนของสหประชาชาติ (United Nations) นั้น ได้กำหนดหลักเกณฑ์ที่เกี่ยวกับข้อมูลส่วนบุคคลไว้ในกรอบการคุ้มครองข้อมูลส่วนบุคคลของสหประชาชาติ ในส่วนข้อมูลส่วนบุคคลที่จัดเก็บด้วยคอมพิวเตอร์ (Guidelines for the Regulation of Computerized Personal Data Files) สหประชาชาติได้กำหนดหลักเกณฑ์เกี่ยวกับข้อมูลส่วนบุคคลไว้ใน “แนวทางการควบคุมข้อมูลส่วนบุคคลที่จัดเก็บด้วยคอมพิวเตอร์” โดยมีหลักสำคัญ 10 หลักมาใช้ปฏิบัติ (กลุ่มงานบริการวิชาการ สำนักงานเลขาธิการผู้แทนราษฎร, 2560)

ในส่วนของข้อมูลชีวมาตรที่ถือว่าเป็นข้อมูลเฉพาะตัวบุคคลที่สามารถระบุอัตลักษณ์ตัวบุคคลได้ และถือว่าเป็นข้อมูลส่วนบุคคลที่มีความสำคัญเป็นพิเศษ ซึ่งนานาประเทศได้ให้ความสำคัญเป็นอย่างยิ่ง โดยกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป หรือ GDPR (General Data Protection Regulation) ข้อ 9 มีหลักห้ามทำการบันทึกหรือประมวลผลข้อมูลดังกล่าว เว้นแต่ผู้เป็นเจ้าของข้อมูลจะให้ความยินยอมโดยชัดเจน หรือข้อมูลชีวมาตรนั้นจำเป็นสำหรับการปฏิบัติงาน ความมั่นคงปลอดภัยของสังคม หรือปกป้องคุ้มครองทางสังคม ข้อมูลชีวมาตรจำเป็นสำหรับการปกป้องผลประโยชน์ที่สำคัญของแต่ละบุคคล แต่บุคคลเหล่านั้นไม่สามารถให้ความยินยอมได้ หรือข้อมูลชีวมาตรนั้นมีจำเป็นสำหรับประเด็นทางกฎหมาย หรือจำเป็นต่อประโยชน์สาธารณะ ประเทศสหรัฐอเมริกาเป็นประเทศที่มีกฎหมายให้ความคุ้มครองในเรื่องข้อมูลส่วนบุคคลในส่วนของข้อมูลชีวมาตรโดยเฉพาะ คือ Biometric Information Privacy Act (BIPA) ของมลรัฐอิลลินอยส์ ที่ได้ออกมาในเดือนตุลาคมปี 2008 และต่อมามลรัฐวอชิงตันและมลรัฐเท็กซัสได้ผ่านกฎหมายในเรื่องนี้เช่นเดียวกัน ซึ่ง BIPA กำหนดให้หน่วยงานต่างๆในรัฐอิลลินอยส์ต้องปฏิบัติตามกฎหมายที่เกี่ยวกับการรวบรวมและจัดเก็บข้อมูลชีวมาตร โดยมีหลักการมาตรา 15 ที่สำคัญดังนี้ 1) การเก็บ การรวบรวมและการเปิดเผยข้อมูลชีวมาตร ต้องได้รับความยินยอมจากผู้เป็นเจ้าของข้อมูลโดยชัดแจ้ง 2) ต้องทำลายข้อมูลชีวมาตรเมื่อถึงเวลาที่เหมาะสม กล่าวคือ 3 ปีนับแต่วันที่เริ่มเก็บข้อมูลฯดังกล่าว และ 3) ต้องมีมาตรการรักษาความปลอดภัยในการเก็บข้อมูลชีวมาตรอย่างเคร่งครัด และความพิเศษของกฎหมายนี้ คือ ประชาชนที่ถูกละเมิดสามารถยื่นฟ้องเพื่อเรียกค่าเสียหายอันเนื่องมาจากการละเมิดโดยกำหนดอัตราค่าเสียหายและค่าเยียวยาเป็นจำนวนเงินลงไปในตัวบทกฎหมายตามบทบัญญัติมาตรา 20 รวมถึงคำนิยามของข้อมูลชีวิมาตรไว้อย่างชัดเจนตามบทบัญญัติมาตรา 8

สำหรับมลรัฐเท็กซัส ได้มีพระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคลในเรื่องข้อมูลชีวมาตรออกมาในปี ค.ศ.2009 มาตรา 503.001 ได้มีการห้ามเก็บข้อมูลชีวมาตรในกรณีที่มีวัตถุประสงค์เพื่อการค้าโดยปราศจากการแจ้งและให้ความยินยอมเป็นลายลักษณ์อักษร นอกจากนี้ยังจำกัดการจำหน่ายและการเปิดเผยข้อมูลชีวมาตรของแต่ละบุคคล ในรัฐวอชิงตันได้ประกาศใช้กฎหมายดังกล่าวในปี ค.ศ.2017 ห้ามไม่ให้หน่วยงานหรือผู้ควบคุมข้อมูลส่วนบุคคลป้อนข้อมูลชีวมาตรลงในฐานข้อมูลของหน่วยงานโดยต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบล่วงหน้าและเจ้าของข้อมูลส่วนบุคคลต้องให้ความยินยอมประกอบกับต้องมีมาตรการป้องกันการใช้ข้อมูลชีวมาตรดังกล่าวในภายหลัง

อีกทั้งได้ปรากฏถึงการสั่งห้ามเจ้าหน้าที่หน่วยงานราชการ รวมทั้งสำนักงานตำรวจใช้งานระบบจดจำใบหน้า (Face Recognition) ของคณะผู้บริหารนครซานฟรานซิสโก แคลิฟอร์เนีย ประเทศสหรัฐอเมริกา ที่มีมติ 8 ต่อ 1 เสียง

โดยให้หน่วยงานต่างๆ จะต้องรายงานรายละเอียดการสอดแนมที่ใช้งานอยู่เป็นประจำ และระบบที่จะมีการใช้งานในอนาคต นอกจากนี้ แต่ละหน่วยงานจะต้องขออนุมัติจากคณะผู้บริหารเมืองก่อน หากต้องการใช้งานเทคโนโลยีจดจำใบหน้าต่อไป ซึ่งนครซานฟรานซิสโกนับได้ว่าเป็นเมืองแรกของประเทศสหรัฐอเมริกาที่มีคำสั่งห้ามใช้และสั่งซื้อเทคโนโลยีจดจำใบหน้าเพื่อปกป้องสิทธิของประชาชน อย่างไรก็ตาม คำสั่งห้ามดังกล่าวไม่มีผลถึงการใช้งานระบบสแกนใบหน้า หรือ เฟซ ไอดี (Face ID) ที่ประชาชนทั่วไป หน่วยงานภาครัฐ และภาคเอกชนใช้งานอยู่ (ไทย พีบีเอส, 2562)

ประเทศแคนาดาได้มีกฎหมายที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลอันบรรพ 1 มาตรา 5 ข้อ 4.1.4 (Personal Information Protection and Electronic Documents Acts, Schedule 1 (Section 5) 4.1.4. เป็นการบังคับใช้กับข้อมูลส่วนบุคคลที่อยู่ในครอบครองของเอกชนและเรื่องเอกสารอิเล็กทรอนิกส์ด้วย ซึ่งกฎหมายฉบับนี้มีบทบัญญัติของกฎหมายที่มีลักษณะคล้ายคลึงกับประเทศต่างๆ ที่ได้หยิบยกมาข้างต้น แต่มีประเด็นที่น่าสนใจตรงที่ว่ากำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องมีนโยบายและข้อปฏิบัติของตนเพื่อการปฏิบัติตามหลักเกณฑ์ต่างๆ ที่กฎหมายกำหนดอย่างมีประสิทธิภาพ ซึ่งรวมถึงมีข้อปฏิบัติเกี่ยวกับคุ้มครองข้อมูลส่วนบุคคล การตั้งหน่วยงานรับเรื่องร้องเรียนหรือร้องขอ การฝึกอบรมลูกจ้าง และการสร้างความเข้าใจแก่ผู้ร่วมงานในนโยบายและข้อปฏิบัติของตน หรือการพัฒนาข้อมูลเพื่อการอธิบายถึงนโยบายหรือข้อปฏิบัติของตนหรือมาตรการต่างๆ

ประเทศสหพันธรัฐเยอรมนีมีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ได้แก่ Federal Data Protection Act 2018 มาตรา 1 ซึ่งมีขอบเขตการบังคับใช้แก่หน่วยงานของรัฐระดับสหพันธ์และระดับมลรัฐที่ใช้อำนาจตามกฎหมายสหพันธ์หรือเป็นหน่วยงานของศาล และบังคับใช้แก่เอกชนซึ่งเก็บรวบรวม ใช้ หรือดำเนินการกับข้อมูลส่วนบุคคล ไม่ด้วยวิธีทางอิเล็กทรอนิกส์หรือไม่ก็ตาม

อนึ่ง คำว่า “ดำเนินการ” (process) ได้มีบทนิยามไว้หมายถึง การเก็บรักษา การแก้ไขปรับปรุง การยับยั้ง การลบ หรือการเปิดเผยข้อมูลส่วนบุคคล ซึ่งการเปิดเผยข้อมูลยังได้อธิบายด้วยว่า หมายถึง การเปิดเผยต่อบุคคลที่สาม หรือการส่งผ่านบุคคลที่สาม หรือส่งให้บุคคลที่สามารถเรียกดูได้

ตลอดจนประเทศสหพันธรัฐเยอรมนียังได้มีหลักเกณฑ์การส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศตามบทบัญญัติมาตรา 15-16 โดยได้มีบทบัญญัติห้ามให้โอนข้อมูลไปยังประเทศที่ไม่มีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ยกเว้นการส่งหรือโอนข้อมูลไปในประเทศสหภาพยุโรปสามารถกระทำได้แต่ต้องเป็นไปตามหลักเกณฑ์ต่างๆ ของกฎหมายอย่างเคร่งครัดรวมถึงได้บัญญัติถึงกรณีข้อยกเว้นการโอนข้อมูลไปยังต่างประเทศไว้ว่า จะต้องได้รับความยินยอมจากผู้ทรงสิทธิ เป็นการปฏิบัติการตามสัญญาที่ทำกับผู้ทรงสิทธิ หรือเพื่อปฏิบัติตามมาตรการตามที่ผู้ทรงสิทธิร้องขอ เป็นการปฏิบัติตามสัญญาระหว่างผู้ควบคุมข้อมูลกับผู้ซึ่งได้รับโอนข้อมูลเพื่อประโยชน์ของผู้ทรงสิทธิ

นอกจากนี้ ยังมีการคุ้มครองข้อมูลส่วนบุคคลในทางสากลที่ปรากฏอยู่ในกฎหมายระหว่างประเทศ ได้แก่ ข้อบังคับสหภาพยุโรป (European Directive 95/46/EC) ข้อตกลงรัฐสภายุโรป (Council of Europe) กรอบการคุ้มครอง

ข้อมูลส่วนบุคคล GDPR ของสหภาพยุโรป (General Data Protection Regulation) และกรอบคุ้มครองข้อมูลส่วนบุคคลของกลุ่มความร่วมมือทางเศรษฐกิจเอเชีย – แปซิฟิก (APEC) (APEC Privacy Framework)

ดังนั้น จะเห็นได้ว่ากฎหมายของต่างประเทศพยายามที่จะควบคุมและปกป้องข้อมูลชีวมาตรที่หน่วยงานต่างๆ ไม่ว่าภาครัฐหรือเอกชนรวบรวมใช้งานและจัดเก็บข้อมูล และมีมาตรการรักษาความปลอดภัยของข้อมูลขั้นสูงสุด รวมถึงการเปิดโอกาสให้ประชาชนสามารถฟ้องเรียกร้องค่าเสียหายจากการถูกละเมิดในข้อมูลชีวมาตรได้ สำหรับประเทศไทยนั้นอาจจะพิจารณาหาทางป้องกันไม่ให้เกิดความเสียหายที่จะเกิดขึ้นกับประชาชนจากการเก็บข้อมูลชีวมาตร โดยคำนึงถึงสิทธิความเป็นส่วนตัวในข้อมูลส่วนบุคคลของประชาชนตามรัฐธรรมนูญเป็นหลัก สำหรับปัญหาทางกฎหมายของประเทศไทยในการคุ้มครองข้อมูลชีวมาตรนั้น ผู้เขียนจะขอกล่าวเป็นรายประเด็นในหัวข้อถัดไป

3. ผลการศึกษา

ดังที่กล่าวมาข้างต้นถึงหลักเกณฑ์กฎหมายตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในเรื่องของการจัดเก็บรักษาและการใช้ข้อมูลส่วนบุคคล และหลักเกณฑ์ แนวทาง และหลักกฎหมายของต่างประเทศสามารถพิจารณาได้ว่าประเทศไทยได้นำแนวทางขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนามาปรับใช้กับพระราชบัญญัติฉบับนี้ แต่ในส่วนเนื้อหาสาระสำคัญยังพบว่าสมควรที่จะพิจารณาถึงประเด็นต่างๆ ไม่ว่าจะเป็นคำนิยามข้อมูลชีวมาตร (Biometrics) ที่ยังขาดความชัดเจน กล่าวคือ มีเพียงคำอธิบายตามมาตรา 26 วรรคสองแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่บัญญัติว่า ข้อมูลชีวภาพตามวรรคหนึ่งให้หมายถึงข้อมูลส่วนบุคคลที่เกิดจากการใช้เทคนิคหรือเทคโนโลยีที่เกี่ยวข้องกับการนำลักษณะเด่นทางกายภาพหรือทางพฤติกรรมของบุคคลมาใช้ทำให้สามารถยืนยันตัวตนของบุคคลนั้นที่ไม่เหมือนกับบุคคลอื่นได้ เช่น ข้อมูลจำลองใบหน้า ข้อมูลของม่านตา หรือข้อมูลจำลองนิ้วมือ ซึ่งในมาตรานี้ใช้คำว่า “ข้อมูลชีวภาพ” ในขณะที่สากลใช้คำว่า “ข้อมูลชีวมาตร” และยังเป็นเพียงส่วนเนื้อหาของกฎหมายโดยปราศจากคำนิยามตามบทบัญญัติของกฎหมายในมาตรา 6 ของกฎหมายฉบับนี้ ในขณะที่กฎหมายของต่างประเทศที่ได้มีการตรากฎหมายที่เกี่ยวข้องโดยตรงกับการเก็บข้อมูลข้อมูลชีวมาตร เช่น Biometric Information Privacy Act (BIPA) ของมลรัฐอิลลินอยส์ มลรัฐเท็กซัส และมลรัฐวอชิงตันของประเทศสหรัฐอเมริกา

อีกทั้ง คำว่า ดำเนินการ (Process) ที่ถือได้ว่าเป็นคำสำคัญที่กฎหมายจะได้อธิบายได้ว่าหมายถึงอะไรที่หน่วยงานต่างๆ และบุคคลใดสามารถกระทำได้บ้าง หากนำมาเปรียบเทียบกับประเทศสหพันธรัฐเยอรมนีได้บัญญัติไว้อย่างชัดเจนเพื่อใช้บังคับกับหน่วยงานระดับสหพันธ์และระดับมลรัฐ รวมถึงหน่วยงานเอกชนด้วย

ประเด็นต่อมาในเรื่องของการ “ห้าม” ทำการบันทึกหรือประมวลผลข้อมูลพบว่าพระราชบัญญัติฉบับนี้เน้นการตราบทบัญญัติในส่วนของการห้ามบันทึกข้อมูลส่วนบุคคล แต่ยังไม่พบการห้ามประมวลผลอย่างชัดเจนมีเพียงกรณีกำหนดนโยบายในการคุ้มครองข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลไปยังผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลต่างประเทศและอยู่ในเครือกิจการหรือธุรกิจเดียวกันตา

มาตรา 29 และมาตรา 40 ในเรื่องของหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลเท่านั้น ซึ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป หรือ GDPR ได้บัญญัติการห้ามบันทึกหรือประมวลผลข้อมูลชีวมาตรไว้อย่างชัดเจนพร้อมกำหนดข้อยกเว้นที่สามารถดำเนินการดังกล่าวได้

ในขณะที่ล่าสุด นายแพทย์สุธี ทุวิรัตน์ กรรมการสมาคมความมั่นคงปลอดภัยระบบสารสนเทศ หรือ TISA เปิดเผย กับ “ฐานเศรษฐกิจ” ว่ากรณีธนาคารแห่งประเทศไทย (ธปท.) กำลัง ผลักดันให้มีการใช้ระบบการพิสูจน์และยืนยันตัวตนทาง ดิจิทัล (Digital ID) โดยการเอาเทคโนโลยีชีวมาตร (Biometric) เช่น การจดจำใบหน้า ลายนิ้วมือ หรือม่านตา มาใช้ในการพิสูจน์ยืนยันตัวบุคคลในการทำธุรกรรมทางการเงิน (Biometric Payment) กำลังส่งผลกระทบต่อเงินฝากธนาคารคนไทย และมีโอกาสถูกแฮกเกอร์สวมรอยถอนหรือสั่งโอนไปจนเกลี้ยงบัญชีโดยไม่รู้ตัว (ฐานเศรษฐกิจ, 2560) รวมถึงหนังสือเดินทาง (Passport) รุ่นใหม่ของประเทศไทย โดยกระทรวงการต่างประเทศ ซึ่งแต่เดิมมีการเก็บข้อมูลทั้ง ภาพถ่าย และลายพิมพ์นิ้วมือสิบนิ้ว แต่ต่อไปนี้จะมีการ เก็บข้อมูลชีวมาตรม่านตา (Iris) ด้วย ซึ่งทางกระทรวงฯ ได้ให้เหตุผลว่าการเก็บข้อมูลชีวมาตรดังกล่าวเป็นคุณลักษณะความปลอดภัยสูงสุดในการป้องกันการปลอมแปลงหนังสือเดินทาง (สุพล พรหมมาพันธุ์, 2562) ซึ่งแตกต่างจากประเทศอื่น เช่น สหรัฐอเมริกา (U.S. Passport Service guide , 2021) เก็บเฉพาะข้อมูลภาพถ่ายดิจิทัลอย่างเดียว ไม่ให้เก็บลายพิมพ์นิ้วมือ ในสหภาพยุโรป เช่น ประเทศ สหราชอาณาจักรให้เก็บเฉพาะภาพถ่ายดิจิทัล (Biometric Passport-GOV.UK, 2017) ประเทศสหพันธรัฐเยอรมนีเก็บลายพิมพ์นิ้วมือและภาพถ่ายดิจิทัล (Biomerticupdate.com, 2020) และประเทศเนเธอร์แลนด์เก็บลายนิ้วมือ ทั้งนี้เป็นประเทศเดียวในสหภาพยุโรปที่วางแผนว่าจะเก็บลายพิมพ์นิ้วมือเหล่านี้จากส่วนกลาง เป็นต้น (Government of Netherlands, 2021)

นอกเหนือจากหลักเกณฑ์ตามกฎหมายในเรื่องของการเก็บรวบรวม การใช้ การส่งหรือการโอน การประมวลผลข้อมูลแล้วนั้น ผู้เขียนยังมีความเห็นว่า การฝึกอบรมลูกจ้างและการสร้างความเข้าใจแก่ผู้ร่วมงานในนโยบายและข้อปฏิบัติของตน กล่าวคือ ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล ตลอดจนการพัฒนาข้อมูลเพื่อการอธิบายถึงนโยบายหรือข้อปฏิบัติหรือมาตรการต่างๆ ของหน่วยงาน มีความสำคัญเช่นเดียวกัน สมควรพิจารณาให้ตราเป็นตัวบทกฎหมายให้หน่วยงานภาคเอกชนและเรื่องเอกสารอิเล็กทรอนิกส์ด้วยนำไปปฏิบัติเช่นเดียวกับประเทศแคนาดาที่ได้มีบทบัญญัติในเรื่องดังกล่าวไว้อย่างเป็นรูปธรรม

จากการวิเคราะห์ในประเด็นต่างๆ ที่ผู้เขียนได้กล่าวไว้ข้างต้น ผู้เขียนสามารถสรุปได้ว่าประเทศไทยได้มีการผลักดันกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล จึงได้จัดทำและตรากฎหมายพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ขึ้น ซึ่งมีผลบังคับใช้แล้วในปัจจุบัน อย่างไรก็ตามผู้เขียนได้ศึกษาและพิจารณาตัวบทกฎหมายของพระราชบัญญัติฉบับนี้ ยังพบข้อสังเกตบางประการที่ควรพิจารณาเพิ่มเติม แก้ไข และปรับปรุงกฎหมายดังกล่าว ซึ่งผู้เขียนได้ศึกษาหลักเกณฑ์ แนวทาง และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศ เช่น สหภาพยุโรป มลรัฐอิลลินอยด์ มลรัฐวอชิงตัน และมลรัฐเท็กซัส ประเทศสหรัฐอเมริกา ประเทศแคนาดา ประเทศสหพันธรัฐเยอรมนี เป็นต้น โดยมีรายละเอียด ดังต่อไปนี้

1. นิยามศัพท์ เนื่องจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีเพียงนิยามศัพท์คำว่า ข้อมูลส่วนบุคคล ปรากฏในบทบัญญัติมาตรา 3 ของกฎหมายฉบับนี้ ส่วนคำวาข้อมูลชีวมาตรในกฎหมายฉบับนี้ใช้คำว่าข้อมูลชีวภาพที่ปรากฏอยู่ในบทบัญญัติมาตรา 26 วรรคสอง ดังนั้น ควรบัญญัติคำว่า ข้อมูลชีวภาพแยกออกมาให้ชัดเจนเช่นเดียวกับคำว่า ข้อมูลส่วนบุคคล เพราะข้อมูลชีวมาตรถือเป็นข้อมูลส่วนบุคคลที่มีความสำคัญอย่างยิ่งที่จะระบุถึงอัตลักษณะเฉพาะของบุคคล และเสนอให้เปลี่ยนจากคำว่าชีวภาพเป็นคำว่าชีวมาตราตามหลักสากล เช่น นิยามศัพท์กฎหมายของมลรัฐอิลลินอยด์ มลรัฐวอชิงตัน และมลรัฐเท็กซัส ประเทศสหรัฐอเมริกา

2. กฎหมายควรระบุถึงการดำเนินการหรือกระบวนการให้ชัดเจนถึงการเก็บรักษา การแก้ไขปรับปรุง การยับยั้ง การลบ หรือการเปิดเผยข้อมูลส่วนบุคคล ซึ่งยังหมายความรวมถึง การเปิดเผยต่อบุคคลที่สามหรือการส่งผ่านบุคคลที่สามหรือส่งให้บุคคลที่สารถเรียกดูข้อมูลส่วนบุคคลได้ ด้วยตราบทบัญญัติกฎหมายที่เนื้อหาสาระครอบคลุมเพื่อง่ายต่อความเข้าใจและการปฏิบัติได้อย่างถูกต้องของหน่วยงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคล โดยศึกษาจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสหพันธรัฐเยอรมนี หรือคำว่า กระบวนการของสหภาพยุโรปที่ปรากฏในมาตรา 4 ของ General Data Protection Regulation ที่หมายความถึง ดำเนินการหรือชุดการดำเนินการใดๆ ซึ่งกระทำต่อข้อมูลส่วนบุคคลหรือชุดข้อมูลส่วนบุคคล ไม่ว่าจะโดยวิธีการอัตโนมัติหรือไม่ เช่น การเก็บ บันทึก จัดระบบ จัดโครงสร้าง เก็บรักษา เปลี่ยนแปลงหรือปรับเปลี่ยน การรับ พิจารณา ใช้ เปิดเผยด้วยการส่งต่อ เผยแพร่ หรือการกระทำอื่นใดซึ่งทำให้เกิดความพร้อมใช้งาน การจัดวาง หรือผสมเข้าด้วยกัน การจำกัด การลบ หรือการทำลาย

3. หลักการห้ามบันทึกและประมวลผลข้อมูลส่วนบุคคลของผู้ประมวลผลข้อมูลส่วนบุคคล โดยเฉพาะข้อมูลชีวมาตรควรบัญญัติให้ชัดเจนมากขึ้น เช่นเดียวกับกกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปที่มีขอบเขตการบังคับใช้ในเชิงพื้นที่ โดยไม่คำนึงถึงว่าบริษัทนั้นจะตั้งอยู่ที่ใด การสรปะมวลผลจะได้กระทำในสหภาพยุโรปหรือไม่ และยังบังคับใช้กับทุกกิจกรรมที่เป็นการจำหน่ายสินค้าและบริการแก่พลเมืองของสหภาพยุโรป รวมถึงทุกกิจกรรมที่มีลักษณะเป็นการติดตามพฤติกรรมของพลเมืองที่เกิดขึ้นในสหภาพยุโรป (ศูนย์วิจัยและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2561)

4. ควรจัดให้มีการจัดอบรมลูกจ้างและการสร้างความเข้าใจแก่ผู้ร่วมงานในนโยบายและข้อปฏิบัติของตน กล่าวคือ ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล ตลอดจนการพัฒนาข้อมูลเพื่อการอธิบายถึงนโยบายหรือข้อปฏิบัติหรือมาตรการต่างๆ ของหน่วยงาน และให้ทำรายงานการดำเนินการดังกล่าวต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ด้วยการตราเป็นบทบัญญัติกฎหมาย หากฝ่าฝืนไม่ปฏิบัติตามให้มีโทษทางกฎหมาย เช่น กฎหมายคุ้มครองข้อมูลส่วนบุคคลประเทศแคนาดา และเป็นไปตามสิทธิที่จะได้รับการคุ้มครองโดยเจ้าหน้าที่ที่รับผิดชอบ (Data Protection Officers: DPO) ของสหภาพยุโรป ซึ่งกรณีที่เกิดความเสียหายหรือการรั่วไหลของข้อมูลสหภาพยุโรปได้มีบทกำหนดโทษปรับสำหรับผู้ไม่ปฏิบัติตามข้อกำหนดไว้เป็นจำนวนเงินถึง 20 ล้านยูโร หรือในอัตราร้อยละ 2-4 ของรายได้ต่อปี

5. นอกเหนือจากเนื้อหาตัวบทกฎหมายแล้ว นโยบายของภาครัฐที่ประกาศออกมาสมควรหรือไม่ที่ทั้งภาครัฐและภาคเอกชนจะจัดเก็บทั้งข้อมูลส่วนบุคคลและข้อมูลชีวมาตรไว้ในเอกสารทางราชการ หรือข้อมูลของบริษัท

ผู้ประกอบกิจการภาคเอกชน ซึ่งเปรียบเทียบกับการดำเนินการของต่างประเทศแล้วพบว่าได้เลือกเก็บอย่างงใดอย่างหนึ่ง เช่น เก็บภาพถ่ายดิจิทัล หรือลายพิมพ์นิ้วมือ

6. นอกจากนี้ ถึงแม้ว่าประเทศไทยจะเป็นประเทศสมาชิกในกรอบการคุ้มครองข้อมูลส่วนบุคคลของเอเปค (APEC Privacy Framework) กลุ่มความร่วมมือทางเศรษฐกิจเอเชีย – แปซิฟิก (APEC) ก็ตาม แต่ประเทศไทยจำเป็นต้องพัฒนาระบบการจัดเก็บข้อมูลส่วนบุคคลให้มีประสิทธิภาพมากขึ้น เพื่อให้เป็นไปตามหลักการทั้ง 9 ข้อ ได้แก่ 1) การป้องกันความเสียหาย 2) การแจ้งให้ทราบ 3) การจำกัดการรวบรวมข้อมูล 4) การใช้ข้อมูลส่วนบุคคล 5) ทางเลือก 6) ความสมบูรณ์ของข้อมูลส่วนบุคคล 7) การป้องกันความเสียหาย 8) การเข้าถึงและการแก้ไข และ 9) ความรับผิดชอบ อันจะส่งผลดีต่อความเชื่อมั่นของประเทศอื่นๆ ในสหภาพยุโรปในกรณีที่จะมีการส่งหรือโอนข้อมูลส่วนบุคคลมยังประเทศไทย ตลอดจนภาครัฐจะต้องมีนนโยบายหรือแนวทาง มาตรการที่มีความเป็นมาตรฐานกลางในเรื่องของระบบตรวจสอบและจัดเก็บข้อมูลบุคคลที่มีประสิทธิภาพ ตลอดจนมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลขั้นสูงสุด โดยเฉพาะข้อมูลชีวมาตร เพื่อให้หน่วยงานต่างๆ นำไปปฏิบัติและนำมาใช้เพื่อป้องกันการรั่วไหลของข้อมูลส่วนบุคคลที่อาจก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ไม่ว่าจะเป็นต่อชีวิต ร่างกาย ทรัพย์สิน และชื่อเสียงหรือเกียรติยศ รวมถึงการป้องกันข้อพิพาทระหว่างประเทศจากการส่งหรือโอนข้อมูลส่วนบุคคลด้วย เพื่อประโยชน์ด้านความมั่นคงและเศรษฐกิจของประเทศ

อย่างไรก็ตาม การตราบทบัญญัติด้วยการเพิ่มเติมหรือแก้ไขกฎหมายจะต้องกระทำโดยคำนึงถึงสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลของประชาชน และไม่เป็นการเพิ่มภาระให้หน่วยงานเอกชนมากจนเกินไปตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560

4. เอกสารอ้างอิง

กลุ่มงานบริการวิชาการ สำนักงานเลขาธิการผู้แทนราษฎร. (2560). เอกสารประกอบการพิจารณา ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล.... สืบค้นเมื่อ 25 มกราคม 2564 จาก https://library2.parliament.go.th/giventake/content_hr/hr24/ap006-2556.pdf.

ฐานเศรษฐกิจ. (2560). ยื่นร้องนายก หวั่นล้วงตับ สแกนใบหน้า. สืบค้นเมื่อ 25 มกราคม 2564 จาก https://www.thansettakij.com/content/407027).

ไทย พีบีเอส. (2562). ซานฟรานซิสโก ห้ามซื้อขาย-ใช้งานระบบจดจำใบหน้า. สืบค้นเมื่อ 25 มกราคม 2564 จาก https://news.thaipbs.or.th/content/280068.

มติชน. (2562). เรื่อง เทคโนโลยีระบุตัวตน “ชีวมาตร” น่ากลัวหรือไม่. สืบค้นเมื่อ 25 มกราคม 2564 จาก https://www.matichon.co.th/news-monitor/news_1679649.

ศูนย์วิจัยและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. (2561). Thailand Data Protection Guidelines 1.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล. กรุงเทพมหานคร: โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

สุพล พรหมมาพันธุ์. (2563). การพิสูจน์ตัวตนด้วยเทคโนโลยีชีวมาตรกับความเสี่ยงในการละเมิดสิทธิส่วนบุคคล. สืบค้นเมื่อ 24 มกราคม 2564 จาก https://he02.tci-thaijo.org/index.php/rtafmg/article/download/242341/164857/.

สุพล พรหมมาพันธุ์. (2562). เก็บประเด็นสำคัญจากเวทีเสวนา การเก็บข้อมูลชีวมาตร (Biometrics) ของหน่วยงานรัฐกับการละเมิดสิทธิส่วนบุคคลและผลกระทบต่อความมั่นคงของประเทศ. สืบค้นเมื่อ 24 มกราคม 2564 จาก http://dspace.spu.ac.th/bitstream/123456789/6461/1/บทความ%20การเก็บข้อมูลชีวมาตรฯ%20CIO%20World%20August%202019.pdf.

Biomerticupdate.com. (2020). Germany to require fingerprints and biometric images for government IDs. Retrieved March 9, 2021 from https://www.biometricupdate.com/202011/germany-to-require-fingerprints-and-biometric-images-for-government-ids.

Biometric Passport-GOV.UK. (2017). Guidance Biometric Passports. Retrieved March 9, 2021 from https://www.gov.uk/government/publications/biometric-passports-and-passport-readers/biometric-passports-and-passport-readers.

Government of Netherlands. (2021). Use of biometric data of foreign nationals. Retrieved March 9, 2021 from https://www.government.nl/topics/identification-documents/use-of-biometric-data-of-foreign-nationals.

OECD. (2013). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Retrieved January 26, 2021 from http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

U.S. Passport Service Guide. (2021). E-Passport: All About the Electronic Passport. Retrieved March 9, 2021 from https://www.us-passport-service-guide.com/e-passport.html.