การคุ้มครองข้อมูลชีวมาตรภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

Biometric Personal Data Protection under Personal Data Protection Act B.E. 2560

Received: 31 กรกฎาคม 2563
Revised: 24 กันยายน 2563
Accepted: 25 กันยายน 2563

ผู้ช่วยศาตราจารย์ทัชชภร มหาแถลง*
Assistant Professor Thatchaporn Mahathalang**

บทคัดย่อ

เนื่องจากปัจจุบันมีการละเมิดข้อมูลส่วนบุคคลที่ก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล โดยเฉพาะการจัดเก็บข้อมูลชีวมาตร ซึ่งมีผลมาจากความก้าวหน้าทางเทคโนโลยีที่ก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล การเข้าถึงข้อมูลส่วนบุคคลทำได้โดยง่าย สะดวก และรวดเร็ว อันมีผลกระทบต่อความมั่นคง และเศรษฐกิจโดยรวม ประเทศไทยจึงได้มีการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2560 ขึ้น เพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคล

อย่างไรก็ตาม กฎหมายฉบับนี้ยังมีประเด็นที่น่าศึกษาวิเคราะห์เพิ่มเติมในเรื่องของการเก็บรวมรวม ใช้ ประมวลผล และการส่งหรือโอนข้อมูลไปยังต่างประเทศ โดยได้ศึกษาเปรียบเทียบจากกฎหมายคุ้มครองส่วนบุคคลของต่างประเทศ ได้แก่ สหภาพยุโรป ประเทศสหรัฐอเมริกา ประเทศแคนาดา และประเทศสหพันธรัฐเยอรมัน เพื่อนำมาปรับปรุง แก้ไข หรือเพิ่มเติมบทบัญญัติกฎหมายของประทศไทยอันเป็นประโยชน์ด้านการคุ้มครองข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

คำสำคัญ: กฎหมายคุ้มครองข้อมูลส่วนบุคคล, ข้อมูลส่วนบุคคล, ข้อมูลชีวภาพ

Abstract

Nowadays, the violation of personal information causes damage to the information owners, especially the biometric data, because the advance technology made the acquire access and disclose of personal data easily. Due to mentional problem

* ผู้ช่วยคณบดีคณะนิติศาสตร์ มหาวิทยาลัยศรีปทุม
** Assistant Dean, Faculty of Law, Sripathum University

may affect Thailand's national security and economy; therefore, the Government promulgated the Personal Data Protection Act 2017 to specify criteria, mechanisms, or regulatory measures regarding the protection of personal data.

However, this Act still has some issues that should study further regarding the collection, usage, processing transmission, and or transferring of information to other countries. This study employed a comparative study of personal data protection laws of foreign countries such as the European Union, the United States of America, Canada, and Germany should in order to improve or amend the Thai law to become more efficient in the protection of personal data.

Keywords: Personal data protection law, Personal data, biometric information.

1. บทนำ

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

ข้อมูลชีวมาตรเป็นข้อมูลส่วนบุคคลที่เกิดจากการประมวลผลทางเทคนิคเฉพาะที่เกี่ยวข้องกับลักษณะทางกายภาพ สรีรวิทยา และพฤติกรรมของคนตามธรรมชาติ เช่น ภาพใบหน้า ลายนิ้วมือ หรือม่านตา[1] ส่วนเทคโนโลยีชีวมาตร (Biometrics Technology) เป็นแนวคิดการนำเอาเทคโนโลยีด้านชีวภาพทางการแพทย์และเทคโนโลยีด้านคอมพิวเตอร์มาบูรณาการเข้าด้วยกัน เพื่อใช้กำหนดหรือระบุ

[1] มติชนออนไลน์, "เรื่อง เทคโนโลยีระบุตัวตน "ชีวมาตร" น่ากลัวหรือไม่" https://www.matichon.co.th/news-monitor/news_1679649 (last visited 27 July 2020).

คุณลักษณะเฉพาะส่วนบุคคลทั้งด้าน กายภาพและพฤติกรรม[2] 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.) ที่ได้มีการออกประกาศให้หน่วยงานเอกชนที่ประกอบกิจการโทรคมนาคมไปดำเนินการ เป็นต้น ด้วยวิธีการไม่ว่าจะเป็นการเก็บภาพถ่าย การเก็บข้อมูลบัตรประชาชน การพิสูจน์อัตลักษณ์และลายนิ้วมือ รวมถึงม่านตาทำให้มีความเสี่ยงที่จะเกิดการรั่วไหลหรือนำไปใช้ประโยชน์ในทางที่มิชอบ เกิดความเสียหายต่อผู้เป็นเจ้าของข้อมูลฯ เพราะข้อมูลเหล่านี้เป็นข้อมูลเฉพาะตัวบุคคลที่สามารถระบุอัตลักษณ์ตัวบุคคล เจ้าของข้อมูลไม่สามารถแก้ไขข้อมูลชีวมาตรของตนเองได้ อีกทั้งยังส่งผลกระทบต่อความมั่นคงและเศรษฐกิจของประเทศ ดังนั้น อาจจะกล่าวได้ว่าข้อมูลชีวมาตรจึงเป็นข้อมูลเฉพาะตัวบุคคลที่สามารถระบุอัตลักษณ์ตัวบุคคลและเป็นข้อมูลส่วนบุคคลที่มีความสำคัญเป็นพิเศษ จึงสมควรที่จะมีมาตรการหรือแนวทางปฏิบัติสำคัญหรือเป็นการเฉพาะที่ภาครัฐจะต้องตระหนักและให้ความสนใจ เพื่อป้องกันไม่ให้เกิดปัญหาที่กล่าวมานี้

จากบริบทในสังคมโลกปัจจุบันที่มีความก้าวหน้าของเทคโนโลยีสารสนเทศ การเชื่อมต่อกันด้วยเทคโนโลยีสารสนเทศทำให้ง่ายต่อการสืบค้นและเข้าถึงข้อมูลต่างๆ ได้อย่างสะดวกรวดเร็วยิ่งขึ้น และยังสามารถเผยแพร่หรือถ่ายโอนข้อมูลจากที่หนึ่งไปยังอีกที่หนึ่งได้อย่างรวดเร็ว ประกอบกันสถานการณ์การระบาดของไวรัสโคโรน่า (COVID – 19) ในปัจจุบันทำให้วิถีชีวิตและการดำเนินกิจจกรรมต่างๆ ของคนทั่วโลกเปลี่ยนแปลงไปอย่างมาก ซึ่งรวมถึงประเทศไทยด้วยการใช้เทคโนโลยีมากยิ่งขึ้น ยิ่งส่งผลให้สังคมโลกกลายเป็นสังคมสารสนเทศโดยสมบูรณ์ เทคโนโลยี สารสนเทศกลายเป็นส่วนหนึ่งของชีวิตมนุษย์ ในขณะเดียวกันความเจริญก้าวหน้าของเทคโนโลยี สารสนเทศได้ส่งผลกระทบเชิงลบกับความเป็นส่วนตัวของบุคคล ข้อมูลส่วนบุคคลจึงมีความสำคัญมากยิ่งขึ้น และมีความเสี่ยงโดยง่ายที่จะถูกเอาไปใช้โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลก่อน ซึ่งอาจส่งผลกระทบกระเทือนต่อประโยชน์ส่วนบุคคล ตลอดจนชื่อเสียงเกียรติยศ ดังที่ปรากฏเป็นข่าวเรื่องการละเมิดความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลเกิดขึ้นทั่วโลก เหตุการณ์ดังกล่าวได้ส่งผลให้ทั้งภาครัฐ ภาคเอกชน และ

[2] สุพล พรหมมาพันธุ์, “การพิสูจน์ตัวตนด้วยเทคโนโลยีชีวมาตรกับความเสี่ยงในการละเมิดสิทธิส่วนบุคคล” https://he02.tci-thaijo.org/index.php/rtafmg/article/download/242341/164857/, (last visited 27 July 2020).

ภาคประชาชนเกิดความตระหนักว่าข้อมูลพื้นฐานหรือข้อมูลส่วนบุคคลที่เป็นส่วนหนึ่งของการเข้าถึงระบบเทคโนโลยีสารสนเทศสมัยใหม่จะถูกนำไปใช้ประโยชน์ หรือเป็นโทษหากไม่ได้รับการคุ้มครองที่ปลอดภัยและเชื่อถือได้

2. กฎหมายที่เกี่ยวข้องกับข้อมูลส่วนบุคคลและข้อมมูลชีวมาตรของประเทศไทย

ในส่วนของกฎหมายไทยนั้น รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ได้มีบทบัญญัติมาตรา 32 ที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลไว้ว่า

"บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว

การกระทำอันละเมิดหรือกระทบต่อสิทธิของบุคคลตามวรรคหนึ่ง หรือการนำข้อมูลส่วนบุคคลไปใช้ในประโยชน์ไม่ว่าในทางใดๆ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงเท่าจำเป็นเพื่อประโยชน์สาธารณะ"

แต่เดิมก่อนที่จะมีการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ได้มีพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 ที่มีบทบัญญัติถึงการคุ้มครองข้อมวลส่วนบุคคลของประชาชนที่อยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐ ต่อมาได้มีหน่วยงานที่ต้องเกี่ยวข้องกับการเก็บรักษาข้อมูลส่วนบุคคลได้มีการมาตรการเพื่อคุ้มครองข้อมูลส่วนบุคคล เช่น ประกาศของธนาคารแห่งประเทศไทย เรื่อง หลักเกณฑ์การกำกับดูแลผู้ให้บริการระบบชำระเงินที่มีความสำคัญ[3] ประกาศคณะกรรมการกิจการโทรคมนาคมแห่งชาติ เรื่อง มาตรการคุ้มครองสิทธิของผู้ใช้บริการเกี่ยวกับข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัว และเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม[4] เป็นต้น

ภายหลังได้มีการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งมีผลบังคับใช้ไปกาลทั่วไปแล้วนั้น หากพิจารณากฎหมายฉบับนี้จะพบว่าบทบัญญัติมาตรา 24 มีหลักการห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการป้องกันที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล[5] เพื่อป้องกันหรือระงับ

---

[3] ประกาศของธนาคารแห่งประเทศไทย เรื่อง หลักเกณฑ์การกำกับดูแลผู้ให้บริการระบบชำระเงินที่มีความสำคัญ ข้อ 4.2.5 (3).

[4] ประกาศคณะกรรมการกิจการโทรคมนาคมแห่งชาติ เรื่อง มาตรการคุ้มครองสิทธิของผู้ใช้บริการเกี่ยวกับข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัว และเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม,ข้อ 8 และข้อ 3.

[5] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 24 (1).

อันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล[6] เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น[7] เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินการภารกิจเพื่อประโยชน์สาธารณะของเจ้าของข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้รับมอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล[8] ตลอดจนเป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลหรือนิติบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล[9] รวมถึงเป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล[10]

อีกทั้งบทบัญญัติมาตรา 27 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคล[11]ใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้น ไม่ต้องขอความยินยอมตามมาตรา 24 ที่กล่าวมาข้างต้น หรือข้อยกเว้นการเก็บรวมรวมข้อมูลส่วนบุคคลโดยปราศจากความยินยอมของเจ้าของข้อมูลส่วนบุคคลตามบทบัญญัติมาตรา 26[12] กล่าวคือ ข้อยกเว้นทั้ง 2 มาตรานี้ เป็นไปเพื่อความจำเป็นเพื่อการปฏิบัติหน้าที่ในการ

---

[6] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 24 (2).

[7] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24 (3).

[8] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 24 (4).

[9] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 24 (5).

[10] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 24 (6).

[11] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 6 ในพระราชบัญญัตินี้

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

[12] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562,

มาตรา 26 ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(1) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม

(2) เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคมหรือองค์กรที่ไม่แสวงหาผลกำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงานให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหาผลกำไรตามตามวัตถุประสงค์ดังกล่าวโดยไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหาผลกำไรนั้น

ดำเนินภารกิจเพื่อประโยชน์สาธารณะด้านต่างๆของผู้ควบคุม ข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล รวมถึงเป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

อย่างไรก็ตาม หากพิจารณาต่อในส่วนของ มาตรา 26 แม้จะห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับข้อมูลชีวภาพ โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล แต่บทบัญญัติของกฎหมายที่กล่าวมาแล้ว ยังมีประเด็นเรื่องการบังคับใช้ของหน่วยงานของรัฐหลายแห่งในการใช้อำนาจรัฐบังคับเก็บข้อมูลชีวมาตรของประชาชน โดยไม่ได้พิจารณาเหตุผลและความจำเป็นอย่าง

---

(3) เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล

(4) เป็นการจำเป็นเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการช้สิทธิเรียกร้องตามกฎหมาย

(5) เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ

(ก) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบการให้บริการด้านสังคมสงเคราะห์ ทั้งนี้ ในกรณีที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือผู้ที่มีหน้าที่รักษายข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติการตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์

(ข) ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติตต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

(ค) การคุ้มครองแรงงาน การประกันสังคม หรือหลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองทางสังคม ซึ่งการเก็บข้อมูลส่วนบุคคลเป็นสิ่งจำเป็นในการปฏิบัติตามสิทธิหรือหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคล โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

(ง) การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น ทั้งนี้ ต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น และได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ตามที่คณะกรรมการประกาศกำหนด

(จ) ประโยชน์สาธารณะที่สำคัญ โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิธิขั้นพื้นฐานและประโยชน์ทของเจ้าของข้อมูลส่วนบุคคล

รอบคอบ ซึ่งอาจมีผลกระทบต่อผู้เป็นเจ้าของข้อมูลชีวมาตรในกรณีที่ข้อมูลรั่วไหลและถูกนำไปใช้โดยมิชอบ

นอกจากเรื่องการจัดเก็บข้อมูลส่วนบุคคลที่ควรจะให้ความใส่ใจแล้วยังรวมถึงการส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศที่ยังต้องนำมาและพิจารณาถึงแนวทางการป้องกันการรั่วไหลข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งข้อมูลชีวมาตรอีกด้วย ดังนี้ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลจะต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ และเป็นไปตามหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลตามที่คณะกรรมการประกาศกำหนด[13] เว้นแต่เป็นการปฏิบัติตามกฎหมายหรือได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศ เป็นความจำเป็นเพื่อปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น และเป็นการกระทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลเพื่อประโยชน์ของเจ้าของมูลส่วนบุคคล ตลอดจนเพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคล หรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้ รวมถึงเป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ[14]

จากหลักการเก็บรวบรวม การใช้ข้อมูลส่วนบุคคล การส่งหรือโอนข้อมูลส่วนบุคคลข้างต้น ผู้เขียนมีข้อสังเกตว่ากฎหมายฉบับนี้มุ่งที่จะให้ความสำคัญกับหลักความยินยอม (consent) ของเจ้าของข้อมูลส่วนบุคคลเป็นประการสำคัญอันจะเข้าข้อยกเว้นที่หน่วยงานหรือองค์กรต่างๆ โดยเฉพาะอย่างยิ่งภาคเอกชนผู้ควบคุมข้อมูลส่วนบุคคลสามารถกระทำได้ แต่สิ่งที่น่ากังวล คือ การรั่วไหลของข้อมูลส่วนบุคคลจากมาตรฐานการจัดเก็บ การส่ง และการโอนข้อมูลส่วนบุคคล และผู้เขียนมีความเห็นว่าเป็นการให้พื้นที่ของภาคเอกชนในการดำเนินการส่งหรือโอนข้อมูลส่วนบุคคล ทั้งนี้ แม้ว่ากฎหมายจะให้อำนาจและหน้าที่แก่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นผู้วินิจฉัยกรณีที่มีปัญหาเกี่ยวกับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคล[15] ก็ตาม

---

[13] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 16 คณะกรรมการมีหน้าที่และอำนาจ ดังต่อไปนี้

(5) ประกาศกำหนดหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ

[14] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 28.

[15] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 28 วรรคสอง.

นอกจากนี้ ยังพบในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล[16]ซึ่งอยู่ในราชอาณาจักรได้กำหนดนโยบายในการคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ต่างประเทศและอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน หากนโยบายในการคุ้มครองข้อมูลส่วนบุคคลดังกล่าวได้รับการตรวจสอบและรับรองจากสำนักงาน การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศที่เป็นไปตามนโยบายในการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับกาตรวจสอบและรับรองดังกล่าวให้สามารถกระทำได้โดยได้รับยกเว้นไม่ต้องปฏิบัติตามหลักกฎหมายการส่งหรือโอนข้อมูลไปยังต่างประเทศข้างต้น ประกอบกับนโยบายในการคุ้มครองข้อมูลส่วนบุคคล ลักษณะของเครือกิจการหรือธุรกิจเดียวกันเพื่อการประกอบกิจการธุรกิจร่วมกัน และหลักเกณฑ์และวิธีการตรอบสอบให้เป็นไปตามที่คณะกรรมการกำหนด[17] ตลอดจนการเข้าข้อยกเว้นในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลข้อมูลส่วนบุคคลได้จัดให้มีมาตรการคุ้มครองที่เหมาะสมสามารถบังคับตามสิทธิของเจ้าของข้อมูลส่วนบุคคลได้ รวมทั้งมีมาตรการเยียวยาทางกฎหมายที่มีประสิทธิภาพตามหลักเกณฑ์และวิธีการที่คณะกรรมการกำหนดไม่จำเป็นต้องปฏิบัติตามหลักเกณฑ์มาตรา 28 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562[18]

ผู้เขียนมีความเห็นว่ายิ่งเป็นการเพิ่มพื้นที่ให้ภาคเอกชนง่ายต่อการดำเนินการส่งหรือโอนข้อมูลส่วนบุคคล โดยเฉพาะข้อมูลชีวมาตรไปยังต่างประเทศมากยิ่งขึ้น โดยอาศัยอำนาจดุลพินิจของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นสาระสำคัญ ดังนั้น สมควรมีมาตรการ มาตรฐาน และระบบการตรวจสอบให้มีความเป็นมาตรฐานอย่างมีประสิทธิภาพและสามารถนำมาใช้ได้อย่างเป็นรูปธรรม เพื่อป้องกันการรั่วไหลของข้อมูลส่วนบุคคล โดยเฉพาะข้อมูลชีวมาตร ตลอดจนมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลทางกฎหมายให้มีความชัดเจน ทั้งนี้ผู้เขียนได้ศึกษาหลักเกณฑ์ แนวทางและมาตรการทางกฎหมายของต่างประเทศ โดยรายละเอียดจะได้กล่าวไว้ในหัวข้อถัดไป

3. สาระสำคัญของกฎหมายต่างประเทศที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลและข้อมูลชีวมาตร

ในหัวข้อนี้ ผู้เขียนได้ศึกษาถึงมาตรการทางกฎหมาย แนวทางหรือแนวปฏิบัติ และหลักเกณฑ์ต่างๆ ที่มีผลบังคับใช้ของต่างปประเทศ ดังนี้ การคุ้มครองข้อมูลส่วนบุคคลตามแนวทางขององค์การ

---

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

“ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

[17] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 29.

[18] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 29 วรรคสาม.

เพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data) เป็นแนวทางปฏิบัติขั้นต่ำเพื่อให้ประเทศสมาชิกได้นำไปปฏิบัติภายในแต่ละประเทศ แนวปฏิบัตินี้ไม่ได้แยกระหว่างหน่วยงานรัฐและหน่วยงานภาคเอกชน และไม่ได้แยกว่าเป็นการประมวลผลข้อมูลเกี่ยวกับบุคคลโดยวิธีอัตโนมัติหรือวิธีประมวลผลด้วยมือ โดยความหมายของข้อมูลส่วนบุคคล (Personal data) หมายถึง ข้อมูลใด ๆ ที่เกี่ยวข้องเฉพาะตัวบุคคล หรือสามารถชี้ให้เห็นลักษณะเฉพาะตัวของบุคคลที่เป็นเจ้าของข้อมูลได้ โดยมีหลักการในการคุ้มครองข้อมูลส่วนบุคคลด้วยกัน 8 ข้อ[19] ได้แก่ 1) หลักข้อจำกัดในการเก็บรวบรวมข้อมูล (Collection Limitation Principle) 2) หลักคุณภาพของข้อมูล (Data Quality Principle) 3) หลักการกำหนดวัตถุประสงค์ (Purpose Specification Principle) 4) หลักการจำกัดการใช้ข้อมูลส่วนบุคคล (Use limitation Principle) 5) หลักการรักษาความปลอดภัย (Security Safeguards Principle) 6) หลักการเปิดเผยข้อมูล (Openness Principle) 7) หลักการมีส่วนร่วมของปัจเจกบุคคล (Individual Participation Principle) และ 8) หลักความรับผิดชอบ (Accountability Principle) 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” โดยมีหลักสำคัญที่ว่าด้วย 1) หลักความชอบด้วยกฎหมายและความเป็นธรรม (Principle of lawfulness and fairness) 2) หลักความถูกต้อง (Principle of accuracy) 3) หลักการระบุวัตถุประสงค์โดยเฉพาะเจาะจง (Principle of the purpose-specification) 4) หลักการเข้าถึงข้อมูล (Principle of interested-person access) 5) หลักการไม่เลือกปฏิบัติ (Principle of non-discrimination) 6) การกำหนดข้อยกเว้น (Power to make exceptions) 7) หลักการรักษาความปลอดภัย (Principle of security) 8) หลักการกำกับดูแล (Supervision and

[19] OECD, “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data” http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last visited 29 July 2020).

sanctions) 9) หลักการส่งข้อมูลข้ามแดน (Transborder data flows) และ 10) หลักขอบเขตการใช้ข้อปฏิบัติ (Field of application)[20]

ในส่วนของข้อมูลชีวมาตรที่ถือว่าเป็นข้อมูลเฉพาะตัวบุคคลที่สามารถระบุอัตลักษณ์ตัวบุคคลได้ และถือว่าเป็นข้อมูลส่วนบุคคลที่มีความสำคัญเป็นพิเศษ ซึ่งนานาประเทศได้ให้ความสำคัญเป็นอย่างยิ่ง โดยกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป หรือ GDPR (General Data Protection Regulation) มีหลักห้ามทำการบันทึกหรือประมวลผลข้อมูลดังกล่าว เว้นแต่ผู้เป็นเจ้าของข้อมูลจะให้ความยินยอมโดยชัดเจน หรือข้อมูลชีวมาตรนั้นจำเป็นสำหรับการปฏิบัติงาน ความมั่นคงปลอดภัยของสังคม หรือปกป้องคุ้มครองทางสังคม ข้อมูลชีวมาตรจำเป็นสำหรับการปกป้องผลประโยชน์ที่สำคัญของแต่ละบุคคล แต่บุคคลเหล่านั้นไม่สามารถให้ความยินยอมได้ หรือข้อมูลชีวมาตรนั้นมีจำเป็นสำหรับประเด็นทางกฎหมาย หรือจำเป็นต่อประโยชน์สาธารณะ[21]

ประเทศสหรัฐอเมริกาเป็นประเทศที่มีกฎหมายให้ความคุ้มครองในเรื่องข้อมูลส่วนบุคคลในส่วนของข้อมูลชีวมาตรโดยเฉพาะ คือ Biometric Information Privacy Act (BIPA) ของมลรัฐอิลลินอยส์ ที่ได้ออกมาในเดือนตุลาคมปี 2008 และต่อมามลรัฐวอชิงตันและมลรัฐเท็กซัสได้ผ่านกฎหมายในเรื่องนี้เช่นเดียวกัน ซึ่ง BIPA กำหนดให้หน่วยงานต่างๆในรัฐอิลลินอยส์ต้องปฏิบัติตามกฎหมายที่เกี่ยวกับการรวบรวมและจัดเก็บข้อมูลชีวมาตร โดยมีหลักการที่สำคัญดังนี้ 1) การเก็บ การรวบรวมและการเปิดเผยข้อมูลชีวมาตร ต้องได้รับความยินยอมจากผู้เป็นเจ้าของข้อมูลโดยชัดแจ้ง 2) ต้องทำลายข้อมูลชีวมาตรเมื่อถึงเวลาที่เหมาะสม กล่าวคือ 3 ปีนับแต่วันที่เริ่มเก็บข้อมูลฯดังกล่าว และ 3) ต้องมีมาตรการรักษาความปลอดภัยในการเก็บข้อมูลชีวมาตรอย่างเคร่งครัด[22] และความพิเศษของกฎหมายนี้ คือ ประชาชนที่ถูกละเมิดสามารถยื่นฟ้องเพื่อเรียกค่าเสียหายอันเนื่องมาจากการละเมิดโดยกำหนดอัตราค่าเสียหายและค่าเยียวยาเป็นจำนวนเงินลงไปในตัวบทกฎหมาย[23] รวมถึงคำนิยามของข้อมูลชีวิมาตรไว้อย่างชัดเจน[24]

สำหรับมลรัฐเท็กซัส ได้มีพระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคลในเรื่องข้อมูลชีวมาตรออกมาในปี ค.ศ.2009 ซึ่งได้มีการห้ามเก็บข้อมูลชีวมาตรในกรณีที่มีวัตถุประสงค์เพื่อการค้าโดยปราศจากการแจ้งและให้ความยินยอมเป็นลายลักษณ์อักษร นอกจากนี้ยังจำกัดการจำหน่ายและการ

---

[20] กลุ่มงานบริการวิชาการ สำนักงานเลขาธิการผู้แทนราษฎร, “เอกสารประกอบการพิจารณาร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล.... https://library2.parliament.go.th/giventake/content_hr/hr24/ap006-2556.pdf (last visited 30 July 2020), หน้า 83 - 84.

[21] General Data Protection Regulation, article 9 Processing of special categories of personal data.

[22] Illinois Biometric Information Privacy Act 2oo8, section 15.

[23] Illinois Biometric Information Privacy Act 2008, section 20.

[24] Illinois Biometric Information Privacy Act 2008, section 10.

เปิดเผยข้อมูลชีวมาตรของแต่ละบุคคล[25] ในรัฐวอชิงตัน ได้ประกาศใช้กฎหมายดังกล่าวในปี ค.ศ.2017 ห้ามไม่ให้หน่วยงานหรือผู้ควบคุมข้อมูลส่วนบุคคลป้อนข้อมูลชีวมาตรลงในฐานข้อมูลของหน่วยงาน โดยต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบล่วงหน้าและเจ้าของข้อมูลส่วนบุคคลต้องให้ความยินยอม ประกอบกับต้องมีมาตรการป้องกันการใช้ข้อมูลชีวมาตรดังกล่าวในภายหลัง[26]

อีกทั้งได้ปรากฏถึงการสั่งห้ามเจ้าหน้าที่หน่วยงานราชการ รวมทั้งสำนักงานตำรวจใช้งานระบบจดจำใบหน้า (Face Recognition) ของคณะผู้บริหารนครซานฟรานซิสโก แคลิฟอร์เนีย ประเทศสหรัฐอเมริกา ที่มีมติ 8 ต่อ 1 เสียง โดยให้หน่วยงานต่างๆ จะต้องรายงานรายละเอียดการสอดแนมที่ใช้งานอยู่เป็นประจำ และระบบที่จะมีการใช้งานในอนาคต นอกจากนี้ แต่ละหน่วยงานจะต้องขออนุมัติจากคณะผู้บริหารเมืองก่อน หากต้องการใช้งานเทคโนโลยีจดจำใบหน้าต่อไป ซึ่งนครซานฟรานซิสโกนับได้ว่าเป็นเมืองแรกของประเทศสหรัฐอเมริกาที่มีคำสั่งห้ามใช้และสั่งซื้อเทคโนโลยีจดจำใบหน้าเพื่อปกป้องสิทธิของประชาชน อย่างไรก็ตาม คำสั่งห้ามดังกล่าวไม่มีผลถึงการใช้งานระบบสแกนใบหน้า หรือเฟซ ไอดี (Face ID) ที่ประชาชนทั่วไป หน่วยงานภาครัฐ และภาคเอกชนใช้งานอยู่[27]

ประเทศแคนาดาได้มีกฎหมายที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลอันเป็นการบังคับใช้กับข้อมูลส่วนบุคคลที่อยู่ในครอบครองของเอกชนและเรื่องเอกสารอิเล็กทรอนิกส์ด้วย ซึ่งกฎหมายฉบับนี้มีประเด็นที่น่าสนใจตรงที่ว่ากำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องมีนโยบายและข้อปฏิบัติของตนเพื่อการปฏิบัติตามหลักเกณฑ์ต่างๆ ที่กฎหมายกำหนดอย่างมีประสิทธิภาพ ซึ่งรวมถึงมีข้อปฏิบัติเกี่ยวกับคุ้มครองข้อมูลส่วนบุคคล การตั้งหน่วยงานรับเรื่องร้องเรียนหรือร้องขอ การฝึกอบรมลูกจ้าง และการสร้างความเข้าใจแก่ผู้ร่วมงานในนโยบายและข้อปฏิบัติของตน หรือการพัฒนาข้อมูลเพื่อการอธิบายถึงนโยบายหรือข้อปฏิบัติของตนหรือมาตรการต่างๆ[28]

ประเทศสหพันธรัฐเยอรมันมีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ได้แก่ Federal Data Protection Act 2018 ซึ่งมีขอบเขตการบังคับใช้แก่หน่วยงานของรัฐระดับสหพันธ์และระดับมลรัฐที่ใช้อำนาจตามกฎหมายสหพันธ์หรือเป็นหน่วยงานของศาล และบังคับใช้แก่เอกชนซึ่งเก็บรวบรวมใช้ หรือดำเนินการกับข้อมูลส่วนบุคคล ไม่ด้วยวิธีทางอิเล็กทรอนิกส์หรือไม่ก็ตาม

อนึ่ง คำว่า “ดำเนินการ” (process) ได้มีบทนิยามไว้หมายถึง การเก็บรักษา การแก้ไขปรับปรุง การยับยั้ง การลบ หรือการเปิดเผยข้อมูลส่วนบุคคล ซึ่งการเปิดเผยข้อมูลยังได้อธิบายด้วยว่าหมายถึง การเปิดเผยต่อบุคคลที่สาม หรือการส่งผ่านบุคคลที่สาม หรือส่งให้บุคคลที่สามารถเรียกดูได้[29]

---

[25] The Texas Capture or Use of Biometric Identifier Act (CUBI) 2009, Chapter 503 Biometric Identifiers, section 503.001.

[26] Washington State’s law regarding biometric identifiers, RCW 19.375.020.

[27] ไทย พีบีเอส ออนไลน์, "ซานฟรานซิสโก" ห้ามซื้อขาย-ใช้งานระบบจดจำใบหน้า” https://news.thaipbs.or.th/content/280068 (last visited 31 July 2020).

[28] Personal Information Protection and Electronic Documents Acts, Schedule 1 (Section 5) 4.1.4.

[29] Federal Data Protection Act 2018, Section 1.

ตลอดจนประเทศสหพันธรัฐเยอรมันยังได้มีหลักเกณฑ์การส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ โดยได้มีบทบัญญัติห้ามให้โอนข้อมูลไปยังประเทศที่ไม่มีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ยกเว้นการส่งหรือโอนข้อมูลไปในประเทศสหภาพยุโรปสามารถกระทำได้แต่ต้องเป็นไปตามหลักเกณฑ์ต่างๆ ของกฎหมายอย่างเคร่งครัด[30] รวมถึงได้บัญญัติถึงกรณีข้อยกเว้นการโอนข้อมูลไปยังต่างประเทศไว้ว่า จะต้องได้รับความยินยอมจากผู้ทรงสิทธิ เป็นการปฏิบัติการตามสัญญาที่ทำกับผู้ทรงสิทธิ หรือเพื่อปฏิบัติตามมาตรการตามที่ผู้ทรงสิทธิร้องขอ เป็นการปฏิบัติตามสัญญาระหว่างผู้ควบคุมข้อมูลกับผู้ซึ่งได้รับโอนข้อมูลเพื่อประโยชน์ของผู้ทรงสิทธิ

ดังนั้น จะเห็นได้ว่ากฎหมายของต่างประเทศพยายามที่จะควบคุมและปกป้องข้อมูลชีวมาตร ที่หน่วยงานต่างๆไม่ว่าภาครัฐหรือเอกชนรวบรวมใช้งานและจัดเก็บข้อมูล และมีมาตรการรักษาความปลอดภัยของข้อมูลขั้นสูงสุด รวมถึงการเปิดโอกาสให้ประชาชนสามารถฟ้องเรียกร้องค่าเสียหายจากการถูกละเมิดในข้อมูลชีวมาตรได้ สำหรับประเทศไทยนั้นอาจจะพิจารณาหาทางป้องกันไม่ให้เกิดความเสียหายที่จะเกิดขึ้นกับประชาชนจากการเก็บข้อมูลชีวมาตร โดยคำนึงถึงสิทธิความเป็นส่วนตัวในข้อมูลส่วนบุคคลของประชาชนตามรัฐธรรมนูญเป็นหลัก

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)

ดังนั้น จะเห็นได้ว่ากฎหมายของต่างประเทศพยายามที่จะควบคุมและปกป้องข้อมูลชีวมาตรที่หน่วยงานต่างๆ ไม่ว่าภาครัฐหรือเอกชนรวบรวมใช้งานและจัดเก็บข้อมูล และมีมาตรการรักษาความปลอดภัยของข้อมูลขั้นสูงสุด รวมถึงการเปิดโอกาสให้ประชาชนสามารถฟ้องเรียกร้องค่าเสียหายจากการถูกละเมิดในข้อมูลชีวมาตรได้ สำหรับประเทศไทยนั้นอาจจะพิจารณาหาทางป้องกันไม่ให้เกิดความเสียหายที่จะเกิดขึ้นกับประชาชนจากการเก็บข้อมูลชีวมาตร โดยคำนึงถึงสิทธิความเป็นส่วนตัวในข้อมูลส่วนบุคคลของประชาชนตามรัฐธรรมนูญเป็นหลัก

4. บทวิเคราะห์กฎหมายตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ดังที่กล่าวมาข้างต้นถึงหลักเกณฑ์กฎหมายตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในเรื่องของการจัดเก็บรักษาและการใช้ข้อมูลส่วนบุคคล และหลักเกณฑ์ แนวทาง และหลักกฎหมายของต่างประเทศสามารถพิจารณาได้ว่าประเทศไทยได้นำแนวทางขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data) มาปรับใช้กับพระราชบัญญัติฉบับนี้ แต่ในส่วนเนื้อหา

[30] Federal Data Protection Act 2018, Section 15-16.

สาระสำคัญยังพบว่าสมควรที่จะพิจารณาถึงประเด็นต่างๆ ไม่ว่าจะเป็นคำนิยามข้อมูลชีวมาตร (Biometrics) ที่ยังขาดความชัดเจน กล่าวคือ มีเพียงคำอธิบายตามมาตรา 26 วรรคสองแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่บัญญัติว่า ข้อมูลชีวภาพตามวรรคหนึ่งให้หมายถึงข้อมูลส่วนบุคคลที่เกิดจากการใช้เทคนิคหรือเทคโนโลยีที่เกี่ยวข้องกับกาสรนำลักษณะเด่นทางกายภาพหรือทางพฤติกรรมของบุคคลมาใช้ทำให้สามารถยืนยันตัวตนของบุคคลนั้นที่ไม่เหมือนกับบุคคลอื่นได้ 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 หากนำมาเปรียบเทียบกับประเทศสหพันธรัฐเยอรมันได้บัญญัติไว้อย่างชัดเจนเพื่อใช้บังคับกับหน่วยงานระดับสหพันธ์และระดับมลรัฐรวมถึงหน่วยงานเอกชนด้วย

ประเด็นต่อมาในเรื่องของการ “ห้าม” ทำการบันทึกหรือประมวลผลข้อมูลพบว่าพระราชบัญญัติฉบับนี้เน้นการตราบทบัญญัติในส่วนของการห้ามบันทึกข้อมูลส่วนบุคคล แต่ยังไม่พบการห้ามประมวลผลอย่างชัดเจนมีเพียงกรณีกำหนดนโยบายในการคุ้มครองข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลไปยังผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลต่างประเทศและอยู่ในเครือกิจการหรือธุรกิจเดียวกันตามาตรา 29 และมาตรา 40 ในเรื่องของหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลเท่านั้น ซึ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปหรือ GDPR ได้บัญญัติการห้ามบันทึกหรือประมวลผลข้อมูลชีวมาตรไว้อย่างชัดเจนพร้อมกำหนดข้อยกเว้นที่สามารถดำเนินการดังกล่าวได้

ในขณะที่ล่าสุด นายแพทย์สุธี ทุวิรัตน์ กรรมการสมาคมความมั่นคงปลอดภัยระบบสารสนเทศหรือ TISA เปิดเผย กับ “ฐานเศรษฐกิจ” ว่ากรณีธนาคารแห่งประเทศไทย (ธปท.) กำลัง ผลักดันให้มีการใช้ระบบการพิสูจน์และยืนยันตัวตนทาง ดิจิทัล (Digital ID) โดยการเอาเทคโนโลยีชีวมาตร (Biometric) เช่น การจดจำใบหน้า ลายนิ้วมือ หรือม่านตา มาใช้ในการพิสูจน์ยืนยันตัวบุคคลในการทำธุรกรรมทางการเงิน (Biometric Payment) กำลังส่งผลกระทบต่อเงินฝากธนาคารคนไทย และมีโอกาสถูกแฮกเกอร์สวมรอยถอนหรือสั่งโอนไปจนเกลี้ยงบัญชีโดยไม่รู้ตัว[31] รวมถึงหนังสือเดินทาง (Passport) รุ่นใหม่ของประเทศไทย โดยกระทรวงการต่างประเทศ ซึ่งแต่เดิมมีการเก็บข้อมูลทั้งภาพถ่าย และลายพิมพ์นิ้วมือสิบนิ้ว แต่ต่อไปนี้จะมีการ เก็บข้อมูลชีวมาตรม่านตา (Iris) ด้วย ซึ่งทางกระทรวงฯ ได้ให้เหตุผลว่าการเก็บข้อมูลชีวมาตรดังกล่าวเป็นคุณลักษณะความปลอดภัยสูงสุดในการ

[31] ฐานเศรษฐกิจออนไลน์, “ยื่นร้องนายก หวั่นล้วงตับ สแกนใบหน้า” https://www.thansettakij.com/content/407027 (last visited 31 July 2020).

ป้องกันการปลอมแปลงหนังสือเดินทาง[32] ซึ่งแตกต่างจากประเทศอื่น เช่น สหรัฐอเมริกา[33]เก็บเฉพาะข้อมูลภาพถ่ายดิจิทัลอย่างเดียว ไม่ให้เก็บลายพิมพ์นิ้วมือ ในสหภาพยุโรป เช่น ประเทศสหราชอาณาจักรให้เก็บเฉพาะภาพถ่ายดิจิทัล ประเทศสหพันธรัฐเยอรมันเก็บลายพิมพ์นิ้วมือเพียง 2 นิ้ว และภาพถ่ายดิจิทัล และประเทศเนเธอร์แลนด์เก็บลายนิ้วมือ ทั้งนี้เป็นประเทศเดียวในสหภาพยุโรปที่วางแผนว่าจะเก็บลายพิมพ์นิ้วมือเหล่านี้จากส่วนกลาง เป็นต้น[34]

นอกเหนือจากหลักเกณฑ์ตามกฎหมายในเรื่องของการเก็บรวบรวม การใช้ การส่งหรือการโอน การประมวลผลข้อมูลแล้วนั้น ผู้เขียนยังมีความเห็นว่า การฝึกอบรมลูกจ้างและการสร้างความเข้าใจแก้ผู้ร่วมงานในนโยบายและข้อปฏิบัติของตน กล่าวคือ ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล ตลอดจนการพัฒนาข้อมูลเพื่อการอธิบายถึงนโยบายหรือข้อปฏิบัติหรือมาตรการต่างๆ ของหน่วยงาน มีความสำคัญเช่นเดียวกัน สมควรพิจารณาให้ตราเป็นตัวบทกฎหมายให้หน่วยงานภาคเอกชนและเรื่องเอกสารอิเล็กทรอนิกส์ด้วยนำไปปฏิบัติ เช่นเดียวกับประเทศแคนาดาที่ได้มีบทบัญญัติในเรื่องดังกล่าวไว้อย่างเป็นรูปธรรม

5. สรุปและเสนอแนะ

จากการวิเคราะห์ในประเด็นต่างๆ ที่ผู้เขียนได้กล่าวไว้ข้างต้น ผู้เขียนสามารถสรุปได้ว่าประเทศไทยได้มีการผลักดันกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลสส่วนบุคคล จึงได้จัดทำและตรากฎหมายพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ขึ้น ซึ่งมีผลบังคับใช้แล้วในปัจจุบัน อย่างไรก็ตามผู้เขียนได้ศึกษาและพิจารณาตัวบทกฎหมายของพระราชบัญญัติฉบับนี้ ยังพบข้อสังเกตบางประการที่ควรพิจารณาเพิ่มเติม แก้ไข และปรับปรุงกฎหมายดังกล่าว ซึ่งผู้เขียนได้ศึกษาหลักเกณฑ์แนวทาง และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศ เช่น สหภาพยุโรป มลรัฐอิลลินอยด์ มลรัฐวอชิงตัน และมลรัฐเท็กซัส ประเทศสหรัฐอเมริกา ประเทศแคนาดา ประเทศสหพันธรัฐเยอรมัน เป็นต้น โดยมีรายละเอียด ดังต่อไปนี้

---

[32] สุพล พรหมมาพันธุ์, “เก็บประเด็นสำคัญจากเวทีเสวนา การเก็บข้อมูลชีวมาตร (Biometrics) ของหน่วยงานรัฐกับการละเมิดสิทธิส่วนบุคคลและผลกระทบต่อความมั่นคงของประเทศ” http://www.cioworldmagazine.com/supon-phrommaphan-biometrics-data-collection-privacy-violations/ (last visited 27 July 2020).

[33] Biometric Passport, “United States” https://en.wikipedia.org/wiki/Biometric_passport#United_States last visited 31 July 2020.

[34] Biometric Passport, “European Union” https://en.wikipedia.org/wiki/Passports_of_the_European_Union (last visited 31 July 2020).

ที่	ประเด็น	รายละเอียด	กฎหมายต่างประเทศ
1	นิยามศัพท์	ควรบัญญัติคำว่า ข้อชีวมาตรแยกออกมาให้ชัดเจน เพราะข้อมูลชีวมาตรถือเป็นข้อมูลส่วนบุคคลที่มีความสำคัญอย่างยิ่งที่จะระบุถึงอัตลักษณะเฉพาะของบุคคล และเสนอให้เปลี่ยนจากคำว่าชีวภาพเป็นคำว่าชีวมาตราตามหลักสากล	นิยามศัพท์กฎหมายของมลรัฐอิลลินอยด์ มลรัฐวอชิงตัน และมลรัฐเท็กซัส ประเทศสหรัฐอเมริกา
2	การดำเนินการหรือกระบวนการ	กฎหมายควรระบุถึงการดำเนินการหรือกระบวนการให้ชัดเจน ด้วยตราบทบัญญัติกฎหมายที่เนื้อหาสาระครอบคลุมเพื่อง่ายต่อความเข้าใจและการปฏิบัติได้อย่างถูกต้องของหน่วยงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคล	กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศของสหพันธรัฐเยอรมัน
3	การห้ามบันทึกและประมวลผลข้อมูลส่วนบุคคลของผู้ประมวลผลข้อมูลส่วนบุคคล	หลักการห้ามบันทึกและประมวลผลข้อมูลส่วนบุคคลของผู้ประมวลผลข้อมูลส่วนบุคคล โดยเฉพาะข้อมูลชีวมาตรควรบัญญัติให้ชัดเจนมากขึ้น	กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป
4	การจัดอบรมลูกจ้างและการสร้างความเข้าใจแก่ผู้ร่วมงาน	ควรจัดให้มีการจัดอบรมลูกจ้างและการสร้างความเข้าใจแก่ผู้ร่วมงานในนโยบายและข้อปฏิบัติของตน กล่าวคือ ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลตลอดจนการพัฒนาข้อมูลเพื่อการอธิบายถึงนโยบายหรือข้อปฏิบัติหรือมาตรการต่างๆ ของหน่วยงาน และให้ทำรายงานการดำเนินการดังกล่าวต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ด้วยการตราเป็นบทบัญญัติกฎหมาย หากฝ่าฝืนไม่ปฏิบัติตามให้มีโทษทางกฎหมาย	กฎหมายคุ้มครองข้อมูลส่วนบุคคลประเทศแคนาดา

ที่	ประเด็น	รายละเอียด	กฎหมายต่างประเทศ
5	นโยบายของภาครัฐ	นอกเหนือจากเนื้อหาตัวบทกฎหมายแล้ว นโยบายของภาครัฐที่ประกาศออกมาสมควรหรือไม่ที่ทั้งภาครัฐและภาคเอกชนจะจัดเก็บทั้งข้อมูลส่วนบุคคลและข้อมูลชีวมาตรไว้ในเอกสารทางราชการ หรือข้อมูลของบริษัทผู้ประกอบกิจการภาคเอกชน ซึ่งเปรียบเทียบกับการดำเนินการของต่างประเทศแล้วพบว่าได้เลือกเก็บอย่างใดอย่างหนึ่ง เช่น เก็บภาพถ่ายดิจิทัล หรือลายพิมพ์นิ้วมือ	กฎหมายคุ้มครองข้อมูลส่วนบุคคลประเทศสหรัฐอเมริกา
6	การส่งหรือโอนข้อมูลส่วนบุคคล	1) ถึงแม้ว่าประเทศไทยจะเป็นประเทศสมาชิกในกรอบการคุ้มครองข้อมูลส่วนบุคคลของเอเปค (APEC Privacy Framework) กลุ่มความร่วมมือทางเศรษฐกิจเอเชีย – แปซิฟิก (APEC) ก็ตาม แต่ประเทศไทยจำเป็นต้องพัฒนาระบบการจัดเก็บข้อมูลส่วนบุคคลให้มีประสิทธิภาพมากขึ้น เพื่อมาเชื่อมั่นของประเทศอื่นๆ ในสหภาพยุโรปในกรณีที่จะมีการส่งหรือโอนข้อมูลส่วนบุคคลยังประเทศไทย ตลอดจนภาครัฐจะต้องมีนโยบายหรือแนวทาง มาตรการที่มีความเป็นมาตรฐานกลางในเรื่องของระบบตรวจสอบและจัดเก็บข้อมูลบุคคลที่มีประสิทธิภาพ ตลอดจนมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลขั้นสูงสุด โดยเฉพาะข้อมูลชีวมาตร เพื่อให้หน่วยงานต่างๆ นำไปปฏิบัติและ	-

ที่	ประเด็น	รายละเอียด	กฎหมายต่างประเทศ
		นำมาใช้เพื่อป้องกันการรั่วไหลของข้อมูลส่วนบุคคลที่อาจก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ไม่ว่าจะเป็นต่อชีวิต ร่างกาย ทรัพย์สิน และชื่อเสียงหรือเกียรติยศ 2) การเปิดโอกาสให้ส่งหรือโอนข้อมูลไปยังต่างประเทศนั้น สมควรรที่จะมีหลักเกณฑ์และเงื่อานไขที่มีความเคร่งครัดเป็นอย่างมาก เพราะนอกจากจะส่งผลกระทบต่อเจ้าของข้อมูลชีวมาตรแล้ว ยังอาจกระทบนต่อความมั่นคงของชาติได้อีกด้วย และยังเป็นการป้องกันข้อพิพาทระหว่างประเทศจากการส่งหรือโอนข้อมูลส่วนบุคคลด้วย ดังนั้น จึงต้องเน้นและให้ความสำคัญของข้อมูลชีวมาตรเป็นกรณีพิเศษแตกต่างจากข้อมูลส่วนบุคคลโดยทั่วไป เพื่อประโยชน์ด้านความมั่นคงและเศรษฐกิจของประเทศ	

อย่างไรก็ตาม การตราบทบัญญัติด้วยการเพิ่มเติมหรือแก้ไขกฎหมายจะต้องกระทำโดยคำนึงถึงสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลของประชาชน และไม่เป็นการเพิ่มภาระให้หน่วยงานเอกชนมากจนเกินไปตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560

บรรณานุกรม

กลุ่มงานบริการวิชาการ สำนักงานเลขาธิการผู้แทนราษฎร. “เอกสารประกอบการพิจารณา ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล…” https://library2. parliament.go.th/giventake/content_hr/hr24/ap006-2556.pdf (last visited 30 July 2020).

ฐานเศรษฐกิจออออนไลน์. “ยื่นร้องนายก หวั่นล้วงตับ สแกนใบหน้า” https://www.thansettakij.com/content/407027 (last visited 31 July 2020).

ไทย พีบีเอส ออนไลน์. "ซานฟรานซิสโก" ห้ามซื้อขาย-ใช้งานระบบจดจำใบหน้า” https://news.thaipbs.or.th/content/280068 (last visited 31 July 2020).

มติชนออนไลน์. เรื่อง “เทคโนโลยีระบุตัวตน “ชีวมาตร” น่ากลัวหรือไม่” https://www.matichon.co.th/news-monitor/news_1679649 (last visited 27 July 2020).

สุพล พรหมมาพันธุ์. “การพิสูจน์ตัวตนด้วยเทคโนโลยีชีวมาตรกับความเสี่ยงในการละเมิดสิทธิส่วนบุคคล” https://he02.tci-thaijo.org/index.php/rtafmg/article/download/242341/164857/, (last visited 27 July 2020).

สุพล พรหมมาพันธุ์. “เก็บประเด็นสำคัญจากเวทีเสวนา การเก็บข้อมูลชีวมาตร (Biometrics) ของหน่วยงานรัฐกับการละเมิดสิทธิส่วนบุคคลและผลกระทบต่อความมั่นคงของประเทศ” http://www.cioworldmagazine.com/supon-phrommaphan-biometrics-data-collection-privacy-violations/ (last visited 27 July 2020).

Biometric Passport. “European Union” https://en.wikipedia.org/wiki/Passports_of_the_European_Union (last visited 31 July 2020).

Biometric Passport, “United States” https://en.wikipedia.org/wiki/Biometric_passport#United_States last visited 31 July 2020.

OECD. “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data” http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last visited 29 July 2020).

Biometric Passport. “United States” https://en.wikipedia.org/wiki/Biometric_passport#United_States last visited 31 July 2020.