บทที่ 5

บทสรุปและข้อเสนอแนะ

5.1 บทสรุป

ปัจจุบันเป็นสังคมแห่งการติดต่อสื่อสาร ข้อมูลส่วนบุคคลจึงมีความสำคัญต่อการดำเนินกิจกรรมต่าง ๆ จากการนำเทคโนโลยีที่ทันสมัยมาใช้โดยเฉพาะคอมพิวเตอร์ถูกนำมาใช้ในการจัดเก็บข้อมูล การสืบค้นข้อมูล การเข้าถึงข้อมูล การรับ หรือการส่งข้อมูลส่วนบุคคล จึงสะดวกและสามารถเข้าถึงข้อมูลส่วนบุคคลได้ง่าย โดยเฉพาะในภาคธุรกิจที่มีข้อมูลส่วนบุคคลของผู้บริโภคที่อยู่ในความครอบครองของตน โดยมีทั้งข้อมูลทั่วไป และข้อมูลไบโอเมตริกซ์ที่เป็นข้อมูลบ่งชี้ถึงเอกลักษณ์เฉพาะของบุคคลนั้นได้ ซึ่งในหลาย ๆ ประเทศได้ให้ความสำคัญในเรื่องสิทธิความเป็นส่วนตัว (The right to privacy) โดยสิทธิทางเศรษฐกิจสังคมและวัฒนธรรมในสิทธิขั้นพื้นฐานอันเป็นสิทธิของบุคคลตามหลักขั้นพื้นฐานของกฎหมายที่จะอยู่ตามลำพังโดยปราศจากการรบกวนหรือสอดแทรกจากผู้อื่นที่จะทำให้เกิดความเดือดร้อน รำคาญใจ เสียหาย อับอาย หรือ การแสวงหาประโยชน์โดยมิชอบ เนื่องจากกฎหมายที่บังคับใช้ในระดับสากลเกี่ยวกับสิทธิในความเป็นส่วนตัวจึงเป็นสิ่งสำคัญของบุคคล

แนวความคิดในการละเมิดข้อมูลส่วนบุคคลอยู่ภายใต้ข้อจำกัดของนโยบายสาธารณะจากความอยากรู้ อยากเห็น หรือมีประสงค์ร้ายนั้น อยู่ภายใต้การคุ้มครองของกฎหมายในการละเมิดความเป็นส่วนตัว อันเป็นสิทธิที่จะไม่ถูกรบกวนทางอารมณ์ โดยการอ้างสิทธิของบุคคลเพื่อทำให้ชื่อเสียงผู้นั้นกลับคืนแทนในความเสียหาย หรือได้รับคำสั่งจากศาล สำหรับการคุกคามที่ไม่สอดคล้องกับความเป็นส่วนตัวที่จะได้รับแจ้งตามกฎหมาย เพื่อให้ผู้ที่ตกเป็นเหยื่อได้รับการเยียวยาผ่อนคลายความเครียด ตามที่กฎหมายกำหนดจะต้องดำเนินการประเมินผลกระทบความเป็นส่วนตัวเมื่อพิจารณาในการให้ความคุ้มครองของกฎหมาย GDPR โดยเฉพาะมาตรการในการลงโทษที่ใช้บังคับกับการละเมิดกฎข้อบังคับฉบับนี้ โดยกฎหมายของ GDPR มิได้กำหนดความรับผิดทางอาญาไว้อย่างชัดเจน สำหรับการประมวลผลข้อมูลส่วนบุคคลในการละเมิดกฎระเบียบโดยบทลงโทษหลัก ๆ ที่บัญญัติไว้ใน GDPR คือโทษปรับทางปกครอง โดยเฉพาะอย่างยิ่งสำหรับการละเมิดที่จะต้องเสียค่าปรับทางปกครองตาม Article 83 อันควรคำนึงถึงวิธีปฏิบัติที่นิยมของหน่วยงานเชิงพาณิชย์ ซึ่งเป็นมาตรการความรับผิดทางแพ่ง (Civil Liability) โดยบุคคลอื่นมีหน้าที่

พึงระวังมิให้เกิดความเสียหายแก่บุคคลอื่น สำหรับการประมวลผลข้อมูลส่วนบุคคลมีหลายรูปแบบ เหตุผลสำคัญ นั้นคือ เนื่องมาจากการประมวลผลข้อมูลไบโอเมตริกซ์หลายรูปแบบจำเป็นต้องเกี่ยวข้องกับการใช้เทคโนโลยีใหม่ ๆ ซึ่งเป็นปัจจัยสำคัญที่ GDPR กล่าวคือ การปกป้องสิทธิขั้นพื้นฐานและเสรีภาพของบุคคลโดยเฉพาะอย่างยิ่งสิทธิในการปกป้องข้อมูลส่วนบุคคลของสหภาพยุโรปและให้สิทธิในการเคารพชีวิตส่วนตัวและครอบครัวมีสิทธิในการสื่อสารและการโต้ตอบ สิทธิในการใช้ชีวิตส่วนตัวและการปกป้องข้อมูลส่วนบุคคลในรูปแบบพื้นฐานของการออกกฎหมายเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลภายใต้กฎระเบียบการคุ้มครองข้อมูลทั่วไปของ GDPR ใหม่ และเพื่อให้สอดคล้องกับสังคมดิจิทัลที่ทันสมัยและเพื่อจูงใจให้บุคคลเกิดความยับยั้งถึงการละเมิด หรือเหตุแห่งความเสียหายเป็นการล่วงหน้า

กฎระเบียบว่าด้วยการคุ้มครองข้อมูลทั่วไปมีผลบังคับใช้ในหลักการกับการดำเนินงานและกิจกรรมทุกประเภทไม่ว่าบุคคลใดจะเป็นผู้ดำเนินการประมวลผลข้อมูลส่วนบุคคล โดยบังคับใช้กับบริษัท สมาคมองค์กรหน่วยงานและบุคคลทั่วไป แต่ยังมีข้อยกเว้นบางประการ ตัวอย่างเช่น การประมวลผลข้อมูลส่วนบุคคลของภาคเอกชน และไม่นำมาใช้เมื่อมีผู้ประมวลผลข้อมูลส่วนบุคคลควบคู่กับการใช้สิทธิในการแสดงความคิดเห็น หรือการกำหนดเงื่อนไขของการดำเนินการประเมินผลกระทบความเป็นส่วนตัว โดยผู้ให้บริการจะต้องป้องกันมากกว่าการแก้ไข กล่าวคือ ควรคาดคะเนถึงเหตุการณ์ที่ไม่พึงประสงค์และเหตุสุ่มเสี่ยงต่อความเป็นส่วนตัวของผู้ใช้และดำเนินมาตรการการป้องกันไว้ก่อนที่จะเกิดขึ้นจริง เริ่มต้นจากการตระหนักถึงคุณประโยชน์ของการปฏิบัติตามนโยบายความเป็นส่วนตัวที่เข้มข้นขึ้น ยึดมั่นในการใช้มาตรการสูงสุดในการคุ้มครองความเป็นส่วนตัว

ในขณะเดียวกันเทคโนโลยีใหม่ ๆ มาพร้อมกับความสะดวกสบายมากขึ้น แต่ก็ยังคงเพิ่มความกังวลเกี่ยวกับการละเมิดความเป็นส่วนตัวและข้อมูลส่วนบุคคลนั้นด้วย โดยความเป็นส่วนตัวต้องฝังตัวอยู่ในระบบตั้งแต่เริ่มใช้งานก่อนที่จะเก็บข้อมูล และมีผลต่อเนื่องตลอดอายุการเก็บรักษาข้อมูล (Digital footprints) เพื่อสร้างความมั่นใจว่าข้อมูลส่วนบุคคลทั้งหมดได้รับการคุ้มครองและถูกทำลายทิ้งเมื่อสิ้นสุดการใช้งานต้องประจักษ์และโปร่งใส (Visibility and Transparency - Keep it Open) ผู้มีส่วนได้ส่วนเสียทุกคนจะต้องได้รับการแจ้งถึงมาตรการทางธุรกิจและเทคโนโลยีที่ใช้เพื่อให้บรรลุวัตถุประสงค์ที่แจ้งไว้ และอนุญาตให้ขอตรวจสอบได้ กรรมวิธีทั้งหมดต้องโปร่งใสทั้งต่อผู้ใช้และผู้ให้บริการ เมื่อมีการนำข้อมูลชีวมาตรมาใช้ เช่น ลายนิ้วมือ การจดจำใบหน้าและการจดจำเสียงนั้น จึงกลายเป็นส่วนหนึ่งของชีวิตของบุคคลในประเทศไทยที่หลีกเลี่ยงไม่ได้ ไม่ว่าจะสมัครขอรับ ID รับซิมการ์ด หรือแม้กระทั่งการเดินทางเข้าออกประเทศทั้งชาวไทยและชาวต่างชาติ จึงต้องมีการให้ข้อมูลไบโอเมตริกซ์ กับทั้งภาครัฐและเอกชน ในขณะที่วิธีการบางอย่าง

ในการใช้งานไบโอเมตริกซ์สำหรับการพิสูจน์ตัวตนของผู้ใช้นั้นสะดวกขึ้น แต่พื้นที่เก็บข้อมูลขนาดใหญ่ (Big data) ของข้อมูลส่วนบุคคลนี้มาพร้อมกับความเสี่ยงด้านความปลอดภัย

ผู้วิจัยพบว่า จากมุมมองด้านความปลอดภัยของข้อมูลไบโอเมตริกซ์จะได้รับความเสี่ยงมากกว่าข้อมูลประเภทอื่น ๆ โดย “ข้อมูลไบโอเมตริกซ์สามารถใช้ได้ทั้งทางตรงและหรือทางอ้อมในการระบุตัวบุคคลใดบุคคลหนึ่ง เนื่องจากลักษณะดังกล่าวนี้ จึงสามารถพิจารณาได้ว่าข้อมูลส่วนบุคคลนี้เป็นหนึ่งในประเภทของข้อมูลที่ละเอียดอ่อนที่สุดที่องค์กรจะต้องมีความสามารถจัดการเป็นกรณีพิเศษได้ ด้วยเหตุผลนี้ ทำให้จำนวนอาชญากรบนโลกไซเบอร์กำหนดเป้าหมายมายังข้อมูลไบโอเมตริกซ์โดยเฉพาะ ซึ่งอาจสูงกว่าชนิดข้อมูลอื่น ๆ” นั้น ผู้วิจัยจึงทำการศึกษาการคุ้มครองข้อมูลส่วนบุคคลในกรณี ข้อมูลไบโอเมตริกซ์ (Biometrics) จากกรณีที่ได้กล่าวมาแล้วในข้างต้น เพื่อมาตรการในการป้องกันความมั่นคงปลอดภัยของข้อมูลไบโอเมตริกซ์ในกระบวนการเก็บ รวบรวม เปิดเผย ใช้ ลบ หรือทำลาย ซึ่งข้อมูลที่มีความละเอียดอ่อนสูงที่มีส่วนเกี่ยวข้องกับการใช้เทคนิค หรือเทคโนโลยีกับข้อมูลส่วนบุคคล หรือองค์กรในหลายภาคส่วนที่อยู่ในการครอบครองที่มีความแตกต่างจากข้อมูลส่วนบุคคลทั่วไป ข้อมูลดังกล่าวอาจถูกนำไปใช้ประโยชน์ในหลาย ๆ ด้าน หรือเพื่อประโยชน์ในเชิงพาณิชย์ อาจก่อให้เกิดการละเมิดความเป็นส่วนตัวได้ จึงมีความจำเป็นต้องบัญญัติคำนิยามศัพท์และประเภทข้อมูลให้มีความชัดเจนว่าข้อมูลใดควรได้รับการคุ้มครองเป็นกรณีเฉพาะ โดยจากการศึกษาได้ข้อสรุปดังนี้

5.1.1. ปัญหาเกี่ยวกับคำจำกัดความของ “ข้อมูลไบโอเมตริกซ์” (Biometrics) ยังไม่ชัดเจนตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 โดยมีประเด็นศึกษา ดังนี้

1. ปัญหาความไม่ชัดเจนของคำนิยามศัพท์ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 โดยให้คำนิยามศัพท์ตามมาตรา 6 “ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม โดยเฉพาะมิได้บัญญัติคำนิยามศัพท์ “ข้อมูลทางพันธุกรรม” และ “ข้อมูลไบโอเมตริกซ์” หากพิจารณาแล้วการบัญญัติคำนิยามเช่นนี้ เป็นการให้คำนิยามแบบกว้างเป็นการทั่วไป จึงทำให้เกิดความไม่ชัดเจนของประเภทของข้อมูลส่วนบุคคล หากเกิดกรณีข้อพิพาทอาจตีความซึ่งส่งผลกระทบในทางปฏิบัติจริงตามที่กฎหมายกำหนดบังคับใช้อย่างถูกต้องไม่โดยบัญญัติคำนิยาม “ข้อมูลทางพันธุกรรม” และ “ข้อมูลไบโอเมตริกซ์” เพื่อให้ผู้บริโภคเข้าใจความหมายและประเภทของข้อมูลไบโอเมตริกซ์ เพื่อระมัดระวังในการเก็บรวบรวมข้อมูลส่วนบุคคลที่อ่อนไหวมาก ๆ หรือข้อมูลอื่นใดซึ่งกระทบต่อความรู้สึกของประชาชน โดยระบุการต้องแจ้งเตือนในการให้ความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนตั้งแต่ครั้งแรกที่เริ่มใช้ โดยเฉพาะสหภาพยุโรป สหรัฐอเมริกา สหพันธ์รัฐสาธารณรัฐเยอรมนี ได้บัญญัติคำนิยามศัพท์ไว้อย่างชัดเจน

ยกเว้น สาธารณรัฐสิงคโปร์ มิได้บัญญัติคำนิยามศัพท์ของข้อมูลดังกล่าวนี้ แต่ได้รับการคุ้มครองไม่ต่างจากข้อมูลทั่วไปและมีกฎหมายอื่นก่อนอยู่หน้าแล้วให้การรับรอง

2. การจำแนกประเภทข้อมูลทั่วไปและข้อมูลไบโอเมตริกซ์ไว้ในหมวดหมู่พิเศษเฉพาะ ซึ่ง “ข้อมูลทางพันธุกรรม” และ “ข้อมูลไบโอเมตริกซ์” สามารถใช้ระบุตัวบุคคลใดบุคคลหนึ่งได้ เนื่องจากมีลักษณะพิเศษเป็นได้ทั้งทางและทางอ้อมตรง จึงสามารถพิจารณาได้ว่าข้อมูลดังกล่าวนี้จึงเป็นหนึ่งในประเภทข้อมูลที่ละเอียดอ่อนที่สุดที่ควรบัญญัติคำนิยามศัพท์ และจัดจำแนกประเภทในการคุ้มครองเป็นพิเศษเฉพาะไว้ในพระราชบัญญัติฉบับปัจจุบันนี้โดยเฉพาะ จากการศึกษาพบว่า “ข้อมูลทางพันธุกรรม” และ “ข้อมูลไบโอเมตริกซ์” ของ GDPR BIPA BDSG ได้บัญญัติคำนิยามศัพท์และจำแนกประเภทออกจากข้อมูลส่วนบุคคลทั่วไป โดยให้ได้รับการคุ้มครองข้อมูลละเอียดอ่อนในหมวดหมู่ข้อมูลพิเศษเฉพาะ ดังนี้

(1) “ข้อมูลทางพันธุกรรม” ซึ่งเป็นข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนจัดให้อยู่ในหมวดทั่วไป แต่ก็ยังถูกบัญญัติจำแนกไว้หมวดพิเศษเฉพาะอย่างชัดเจนของ Regulation (EU) 2016/679 Article 4 (13) Regulation (EU) 2018/1725 ตาม Article 3 (17) พระราชบัญญัติ (BIPA) ถูกบัญญัติไว้ใน 740 ILCS 14/1 et seq พระราชบัญญัติ (BDSG) ถูกบัญญัติไว้ใน Section 46 (11) ส่วนกรณีของพระราชบัญญัติ (PDPA) ซึ่งได้บัญญัติ ข้อมูลส่วนบุคคลทั้งหลายเป็นการทั่วไป “ข้อมูลทางพันธุกรรม” และ “ข้อมูลไบโอเมตริกซ์” มิได้บัญญัติคำนิยามไว้แต่อย่างใด

(2) “ข้อมูลไบโอเมตริกซ์” (Biometrics) ซึ่งเป็นข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนและอ่อนไหวง่ายจัดให้จำแนกอยู่ในหมวดพิเศษของ Regulation (EU) 2016/679 Article 4 (14) และ Regulation (EU) 2018/1725 ตาม Article 3 (18) ซึ่งเป็นหมวดหมู่ข้อมูลส่วนพิเศษ ถูกบัญญัติห้ามมิให้มีการประมวลผลไว้ในของ Regulation (EU) 2016/679 Article 9 (1) และ Regulation (EU) 2018/1725 Article 10 (1) พระราชบัญญัติ (BIPA) ถูกบัญญัติไว้ใน 740 ILCS 14/1 et seq พระราชบัญญัติ BDSG ถูกบัญญัติไว้ใน Section 46 (12) (14) การประมวลผลของข้อมูลส่วนบุคคลชนิดพิเศษตามที่อ้างอิงถึงในบทมาตราของ Article 9 (1) ของกฎระเบียบ (EU) 2016/679

5.1.2. หลักการความยินยอม (Consent) ของข้อมูลไบโอเมตริกซ์ (Biometrics)

การให้ความยินยอมในกรณีข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนซึ่งจะต้องได้รับการคุ้มครองอยู่ในหมวดหมู่ข้อมูลพิเศษนั้น การให้ความยินยอมในการประมวลผล การเก็บ เปิดเผย ใช้ ลบ หรือการทำลายนั้น ผู้ให้บริการต้องขอความยินยอมก่อนดำเนินการใด ๆ โดยเป็นลายลักษณ์อักษรด้วยภาษาที่เข้าใจง่ายชัดเจนและสามารถถอนความยินยอมได้ตลอดโดยการถอนความยินยอมจะต้องไม่กระทบต่อสิทธิที่ได้ให้ความยินยอมไว้แล้ว โดยผู้ให้บริการ หรือผู้ควบข้อมูลต้องแจ้งผลกระทบดังกล่าว ก่อนล่วงหน้าที่ได้รับความยินยอมจากเจ้าของข้อมูลทราบก่อนเสมอ รวมถึง

แจ้งวัตถุประสงค์ของการเก็บรวบรวมและการนำข้อมูลข้อมูลไบโอเมตริกซ์ (Biometrics) ไปใช้แก่เจ้าของข้อมูลส่วนบุคคล ในกรณีการแจ้งผลกระทบแก่เจ้าของข้อมูลส่วนบุคคลทราบก่อน จึงต้องให้ความสำคัญอย่างยิ่งในเรื่องผลกระทบต่อบุคคลผู้เป็นเจ้าของข้อมูลเป็นอย่างมากเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล “การให้ความยินยอม” และ “การถอนความยินยอม” จะต้องแจ้งก่อนทุกกรณี แต่ปรากฏว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 มาตรา 19 วรรคหก พบว่าได้บัญญัติไว้เฉพาะ “การให้ความยินยอม” แก่เจ้าของข้อมูลส่วนบุคคลทราบก่อนนั้น มีความสอดคล้องกับสหภาพยุโรป แต่ไม่ได้บัญญัติให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำการแจ้งผลกระทบในการถอนข้อมูลดังกล่าว “ก่อนล่วงหน้า หรือในขณะที่จะให้ความยินยอม” ในกรณีที่กล่าวมาข้างต้นแล้ว ซึ่งเป็นการบัญญัติขัดต่อกฎหมายสากล อาจก่อให้เกิดความสับสนเกี่ยวกับข้อมูลส่วนบุคคล และส่งผลให้ผู้ประกอบธุรกิจ หรือผู้ควบคุมข้อมูลส่วนบุคคล อาจละเลยในการแจ้งเตือนเรื่องผลกระทบจากการถอนความยินยอม “ก่อนล่วงหน้าที่จะให้ความยินยอม” และอาจก่อให้เกิดความเสียหายต่อภาคธุรกิจในกรณีที่ผู้ควบคุมละเมิดข้อกำหนดกฎหมายต่างประเทศ หรืออาจทำให้ผู้ประกอบธุรกิจในประเทศไทยถูกดำเนินการฟ้องร้องคดีในต่างประเทศได้

5.1.3. การแจ้งระยะเวลาการเก็บรักษาข้อมูลไบโอเมตริกซ์ (Biometrics)

การแจ้งระยะเวลาในการเก็บรักษาข้อมูลไบโอเมตริกซ์เมื่อหมดวัตถุความประสงค์แล้ว โดยสหภาพยุโรป สหรัฐอเมริกา สหพันธ์รัฐสาธารณรัฐเยอรมนี สาธารณรัฐสิงคโปร์ ซึ่งในแนวทางการเก็บรวบรวมข้อมูลส่วนบุคคล หรือการตรวจเก็บข้อมูลอัตลักษณ์ของบุคคล ซึ่งจะถูกเก็บโดยกระบวนการที่ใช้ระยะเวลาอันรวดเร็ว ระมัดระวัง และเพื่อไม่ให้เป็นการล่วงล้ำข้อมูลส่วนบุคคลในรูปแบบระบบดิจิทัลในการใช้ระบบสแกนใบหน้า ลายนิ้วมือ ด้วยเครื่องสแกนนิ้วมือดิจิทัลต่าง ๆ นี้ นอกจากนี้ผู้ควบคุมจะมีภาระผูกพันที่จะแจ้งให้องค์กรมีมาตรการที่เหมาะสมและมาตรการทางเทคนิคเพื่อความมั่นคงปลอดภัย เพื่อให้มั่นใจว่ามีการประมวลผลข้อมูลส่วนบุคคลที่จำเป็นตั้งแต่จุดเริ่มต้นใช้ และจำนวนของข้อมูลส่วนบุคคลที่ได้รวบรวม หรือขอบเขตของการประมวลผลระยะเวลาของการจัดเก็บและการเข้าถึง โดยเฉพาะอย่างยิ่งมาตรตามของ Regulation (EU) 2016/679 Article 14 ข้อ 3 (a) Regulation (EU) 2018/1725 Article 16 3 (a) ดังกล่าวนี้ ทำให้มั่นใจได้ว่าข้อมูลส่วนบุคคลได้รับป้องกันตั้งเริ่มต้นใช้และไม่สามารถเข้าถึงได้จากการแทรกแซงของบุคคลต่อบุคคล

ดังนั้น ผู้ควบคุมข้อมูลส่วนบุคคลยังต้องมีหน้าที่โดยตรงกับการใช้สิทธิเจ้าของข้อมูลในการที่จะต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 เช่น สิทธิในการขอเข้าถึงและขอสำเนาข้อมูลหากเจ้าของข้อมูลส่วนบุคคลร้องขอ ผู้ควบคุมข้อมูลจะต้องมีระบบที่สามารถปฏิบัติตามคำขอของเจ้าของข้อมูลส่วนบุคคลได้ภายในระยะเวลาที่กฎหมาย

กำหนด ซึ่งผู้ประมวลผลข้อมูลส่วนบุคคลมิได้มีหน้าที่โดยตรงต่อเจ้าของข้อมูลส่วนบุคคลตามกฎหมาย แต่ปรากฏว่ากฎหมายได้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานไว้เท่านั้น เพราะฉะนั้น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 จึงควรการกำหนดให้ผู้ควบคุมข้อมูลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ “ก่อน” หรือ ในขณะเก็บรวบรวมข้อมูลส่วนบุคคลให้ทราบชัดเจน โดยให้ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งประกาศหลักเกณฑ์และนโยบายเกี่ยวกับระยะเวลาการเก็บข้อมูลส่วนบุคคลว่า “ข้อมูลส่วนบุคคลจะเก็บไว้ภายใน 6 เดือน ให้ทำลายทันที หรือสิ้นสุดตามวัตถุประสงค์ทางธุรกิจ หรือตามข้อตกลงของสัญญา” เว้นแต่กฎหมายบัญญัติให้อำนาจไว้

5.1.4. บทลงโทษเพื่อความมั่นคงปลอดภัยของข้อมูลไบโอเมตริกซ์ (Biometrics)

“ความเสี่ยง” เกี่ยวข้องกับการสูญเสียที่อาจเกิดขึ้นได้ตลอดเวลา ด้วยความเติบโตของเทคโนโลยีอัจฉริยะ ความเสี่ยงจึงเพิ่มขึ้นอย่างทวีคูณ อย่างไรก็ตาม ความเสี่ยงจะบรรเทาลงได้ โดยไม่จัดเก็บข้อมูลส่วนบุคคลที่มีความละเอียดที่อาจก่อให้เกิดในการเลือกปฏิบัติโดยไม่เป็นธรรม หรือความไม่เท่าเทียมกันแก่บุคคลใดนั้นได้ ซึ่งการใช้ข้อมูลไบโอเมตริกซ์นี้ถูกใช้อยู่อย่างแพร่หลายในประเทศต่าง ๆ มากมาย เพราะฉะนั้นจากความสูญเสียที่จะเกิดขึ้นในแต่ครั้งนี้ จึงมีความจำเป็นแล้วหรือไม่ ที่ประเทศไทยจะได้มีมาตรการป้องกันไว้ดีกว่าแก้ไข ด้วยระบบไบโอเมตริกซ์ ซึ่งเป็นเทคนิคทางด้านชีวมาตรกับเทคโนโลยีทางคอมพิวเตอร์เข้าด้วยกัน โดยมีการบันทึกไว้ในฐานข้อมูลเป็นจำนวนมาก กล่าวอีกนัยหนึ่ง คือ เป็นเทคโนโลยีที่ใช้สำหรับยืนยันตัวบุคคลด้วยการเปรียบเทียบ (Pattern ของ Physical) หรือพฤติกรรมต่าง ๆ ของมนุษย์ด้วยระบบเทคโนโลยีคอมพิวเตอร์

ด้วยเหตุดังกล่าวข้างต้น ผู้ควบคุม และผู้ประมวลผลข้อมูลส่วนบุคคลจึงมีส่วนเกี่ยวข้องกับข้อมูลส่วนบุคคลที่แตกต่างกัน โดยกฎหมายกำหนดหน้าที่และความรับผิดของทั้งสองบุคคลนี้ ซึ่งกำหนดหน้าที่และความรับผิดสำหรับผู้ควบคุมข้อมูลส่วนบุคคลไว้ค่อนข้างมาก เพราะถือว่าเป็นผู้ประกอบธุรกิจที่รับผิดชอบโดยตรงนั้น กล่าวคือ ผู้ควบคุมข้อมูลส่วนบุคคลจะมีหน้าที่ในการจัดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่ตนจัดเก็บไว้ เพื่อป้องกันการสูญหาย การเข้าถึง หรือแก้ไขโดยปราศจากอำนาจ รวมถึงจะต้องจัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบ หรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา แต่ผู้ประมวลผลข้อมูลส่วนบุคคล “มีเพียงหน้าที่ในการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลเท่านั้น” โดยไม่มีหน้าที่ในการจัดให้มีระบบตรวจสอบเพื่อดำเนินการลบข้อมูลดังกล่าว โดยหน้าที่สำคัญอีกประการหนึ่งของผู้ควบคุมข้อมูลส่วนบุคคล คือ หน้าที่ในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลให้แก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบโดยไม่ชักช้าภายใน 72 ชั่วโมง และหากการละเมิดดังกล่าวมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล โดยต้อง

แจ้งเหตุแห่งการละเมิดพร้อมแนวทางการเยียวยาดังกล่าวแก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า แต่ปรากฏว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลกำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลมีเพียงหน้าที่ในการแจ้งให้ผู้ควบคุมข้อมูลทราบเมื่อเกิดเหตุละเมิดข้อมูลเท่านั้น ซึ่งสหภาพยุโรปกำหนดให้ผู้ประมวลข้อมูลส่วนบุคคลมีหน้าตรวจสอบเพื่อรักษารักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ตาม Regulation Article 28 (f)

ผู้วิจัยพบว่า สหภาพยุโรป สหรัฐอเมริกา สหพันธ์รัฐสาธารณรัฐเยอรมนี สาธารณรัฐสิงคโปร์ โดยกำหนดให้องค์กรที่ครอบครองข้อมูลส่วนบุคคลมีนโยบายแจ้งเป็นลายลักษณ์อักษรในการให้ความยินยอม การถอนยินยอม ทราบก่อนล่วงหน้าที่จะให้ความยินยอม รวมทั้งต้องแจ้งระยะเวลาในการเก็บ รวบรวม ลบ หรือทำลาย ตามข้อตกลงของสัญญา นอกจากนี้ ยังบัญญัติให้มีการจำแนกประเภทข้อมูลที่ละเอียดอ่อน (Biometrics) ออกจากข้อมูลทั่วไป เพื่อความมั่นคงปลอดภัยในประมวลผล การเก็บ รวบรวม ให้มีความแตกต่างจากประเภทข้อมูลทั่วไป ยกเว้น สาธารณรัฐสิงคโปร์มิได้บัญญัติประเภทข้อมูลไบโอเมตริกซ์ไว้แต่อย่างใด เพียงบัญญัติไว้เป็นการทั่วไป แต่อย่างไรก็ตาม มาตรการลงโทษตามกฎระเบียบของ (GPPR) สำหรับองค์กรที่ฝ่าฝืนค่อนข้างสูงโดยมุ่งเน้นโทษปรับสูงถึง 20 ล้านยูโร หรือร้อยละ 4 ของรายได้ทั้งหมดทั่วโลกของปีงบประมาณก่อนหน้า มาตรการดังกล่าวนี้ ถือว่าเป็นมาตรฐานที่สูงมากสำหรับการปกป้องข้อมูลส่วนบุคคล ซึ่งมีความแตกต่างจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 ฉบับนี้ โดยเฉพาะมิได้จำแนกประเภทข้อมูลที่ละเอียดอ่อนออกจากประเภทข้อมูลทั่วไปและมาตรการลงโทษทางอาญา เพื่อให้มีความสอดคล้องกับวิธีปฏิบัติตามแนวสากลและก่อให้เกิดความตระหนักถึงความมั่นคงปลอดภัยในประเภทข้อมูลพิเศษต้องห้ามประมวลผล เว้นแต่ กฎหมายบัญญัติให้กระทำได้ ฉะนั้น ผู้ให้บริการ หรือผู้ควบคุม หรือเจ้าของข้อมูลส่วนบุคคล จึงควรอย่างยิ่งที่ทราบถึงประเภทของข้อมูลส่วนบุคคลนี้ ประการสำคัญอย่างยิ่งของผู้ควบคุมข้อมูลส่วนบุคคลต้องมีระยะเวลาเพียงพอในการประเมินความเสี่ยงอย่างถี่ถ้วน เพื่อกำหนดขอบเขตของความเสี่ยงต่อความมั่นคงปลอดภัยและป้องกันมิให้มีการเปิดเผยข้อมูลส่วนบุคคลก่อนได้รับความยินยอม เพื่อให้สอดคล้องกับสหภาพยุโรป โดยผู้วิจัยจะได้ทำตารางการเปรียบเทียบสำหรับปัญหามาตรการทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลไบโอเมตริกซ์ ต่อไปนี้

ตารางที่ 1: เปรียบเทียบนิยามคำศัพท์

No	สาระสำคัญ	สหภาพยุโรป	สหรัฐอเมริกา	สหพันธ์รัฐสาธารณรัฐเยอรมนี	สาธารณรัฐสิงคโปร์	ประเทศไทย
1.	คำนิยามศัพท์	"ข้อมูลทางพันธุกรรม" หมายถึง ข้อมูลส่วนบุคคลที่เกี่ยวกับพันธุกรรมของบุคคลธรรมดาซึ่งได้รับ หรือสืบทอดมา โดยข้อมูลนี้นี้มีเอกลักษณ์พิเศษเกี่ยวกับสรีรวิทยา หรือ สุขภาพของบุคคลนั้น โดยแสดงผลจากการวิเคราะห์ตัวอย่างทางชีวภาพของบุคคลนั้น ซึ่งเป็นทั้งข้อมูลทั่วไปและเป็นข้อมูลที่ละเอียดอ่อนตาม Article 3 (17) "ข้อมูลไบโอเมตริกซ์" หมายถึง ข้อมูลส่วนบุคคลที่เกิดจากการประมวลผลทางเทคนิคเฉพาะที่เกี่ยวข้องกับลักษณะทางกายภาพ สรีรวิทยา หรือ พฤติกรรมของบุคคลธรรมดา ซึ่งอนุญาต หรือ การระบุอัตลักษณ์ของบุคคลนั้น เช่น ภาพใบหน้า หรือ ข้อมูลลายนิ้วมือ (Dactyloscopic) ตาม Regulation 2018/1725 Article 3 (18)[2]	"ข้อมูลไบโอเมตริกซ์" หมายถึง ข้อมูลใด ๆ ก็ตาม โดยไม่คำนึกถึงวิธีการบันทึก แปลง จัดเก็บ หรือ แชร์โดย การอ้าอิงอัตลักษณ์จาก การระบุตัวตนด้วย ระบบไบโอเมตริกซ์ เพื่อใช้ระบุตัวตนของบุคคล ข้อมูลไบโอเมตริกซ์ไม่รวม ถึงข้อมูลที่ได้มาจากการ รวบรวม หรือ ขั้นตอน ที่ได้ยกเว้น ภายใต้คำจำกัดความของระบบไบโอเมตริกซ์ตามบังคับนี้ ตาม Section 740 ILCS 14/10 "ข้อมูลทางพันธุกรรม" มีการควบคุมภายใต้ พระราชบัญญัติความเป็นส่วนตัว[1]	"ข้อมูลทางพันธุกรรม" (Genetic data) หมายถึง ข้อมูลส่วนบุคคลที่เกี่ยวข้อง กับลักษณะทางพันธุกรรมที่ สืบทอด หรือได้มาของบุคคล ธรรมดาซึ่งให้ข้อมูลเฉพาะ เกี่ยวกับสรีรวิทยา หรือ สุขภาพของบุคคลธรรมดา นั้นและโดยเฉพาะอย่างยิ่ง จากการวิเคราะห์ตัวอย่างทาง ชีวภาพ จากบุคคลธรรมดาที่ มีปัญหา ซึ่งเป็นทั้งข้อมูล ทั่วไปและข้อมูลที่ละเอียดอ่อน ตาม Section 46 (1) (11) "ข้อมูลไบโอเมตริกซ์" (Biometric data) หมายถึง ข้อมูลส่วนบุคคลที่เกิดจาก การประมวลผลทางเทคนิค เฉพาะที่เกี่ยวข้องกับลักษณะ ทางกายภาพ สรีรวิทยา หรือ พฤติกรรมของบุคคลซึ่ง อนุญาต หรือ การยืนยันการ ระบุเอกลักษณ์ของบุคคล ธรรมดานั้น โดยเฉพาะภาพ ใบหน้า หรือ ข้อมูลลายนิ้วมือ (Dactyloscopic) ตาม BDSG-new[3] Section 46 (12)	ไม่มี	ไม่มี

[1] โปรดดูในหน้าที่ 123

[2] โปรดดูในหน้าที่ 158

[3] โปรดดูในหน้าที่ 201

ตารางที่ 2: เปรียบเทียบประเภทข้อมูล

No	สาระสำคัญ	สหภาพยุโรป	สหรัฐอเมริกา	สหพันธ์รัฐสาธารณรัฐเยอรมนี	สาธารณรัฐสิงคโปร์	ประเทศไทย
2.	**ประเภท**	จำแนกประเภทข้อมูล	จำแนกประเภทข้อมูล	จำแนกประเภทข้อมูล	ไม่มีการจำแนก	ไม่มีการจำแนก
	ข้อมูลส่วน	"ข้อมูลทางพันธุกรรม" โดย	"ข้อมูลไบโอเมตริกซ์"	"ข้อมูลทางพันธุกรรม	ประเภทข้อมูล	ประเภทข้อมูล
	บุคคล	บัญญัติอยู่ในหมวดหมู่ทั่วไป	เป็นข้อมูลละเอียดอ่อน	และข้อมูลไบโอ	เพียงบัญญัติ	เพียงบัญญัติ
		Regulation (EU) 2016/679	ซึ่งได้รับการคุ้มครองใน	เมตริกซ์"ได้ถูกจำแนก	เกี่ยวกับข้อมูล	เกี่ยวกับข้อมูล
		Article 4 (13) และ	หมวดหมู่ข้อมูลพิเศษ	ประเภทต่างหากจาก	ส่วนบุคคล	ส่วนบุคคล
		Regulation2018/1725	ตาม Section	ข้อมูลทั่วไปตาม	เป็นการทั่วไป	เป็นการทั่วไป
		Article 3 (17)	740 ILCS 14/10	ตาม Section 46 (14)		แต่อย่างไรก็ตาม
		โดยจำแนกประเภทข้อมูล	แต่ไม่รวมถึงข้อมูล	โดยได้รับการคุ้มครอง		มาตรา 26 บัญญัติ
		"ข้อมูลไบโอเมตริกซ์" ตาม	"ข้อมูลทางพันธุกรรม"	ในการประมวลผลข้อมูล		ข้อยกเว้นห้ามการ
		Regulation (EU) 2016/679	จึงมิได้บัญญัติประเภท	ไบโอเมตริกซ์กรณีพิเศษ		ประมวลผลข้อมูล
		Article 4 (13) และ	ข้อมูลพันธุกรรมไว้ใน	ของ BDSG-new		ไบโอเมตริกซ์
		Regulation (EU) 2016/679	พระราชบัญญัติ (BIPA)	ตาม Section 48		ซึ่งได้รับการ
		Article 3 (17) และ	ดังคำนิยามคำศัพท์[4]	ดังคำนิยามคำศัพท์[5]		คุ้มครองข้อมูล
		Regulation (EU) 2018/1725				ที่เกิดจากการใช้
		Article 3 (18)				เทคนิค หรือ
		ให้ได้รับการคุ้มครองตาม				เทคโนโลยี
		หมวดหมู่ข้อมูลพิเศษตาม				ดังที่ได้กล่าวไว้[6]
		Regulation (EU) 2016/679				
		Article 9 และ				
		Regulation (EU) 2018/1725				
		Article 10				
		ถูกบัญญัติห้ามมิให้มีการ				
		ประมวลผล เว้นแต่ ข้อยกเว้น				
		ตามกฎหมาย				
		ดังคำนิยามคำศัพท์[7]				

[4] โปรดดูในหน้าที่ 182

[5] โปรดดูในหน้าที่ 208

[6] โปรดดูในหน้าที่ 97

[7] โปรดดูในหน้าที่ 123

ตารางที่ 3: เปรียบเทียบก่อนให้ความยินยอม

No	สาระสำคัญ	สหภาพยุโรป	สหรัฐอเมริกา	สหพันธ์รัฐสาธารณรัฐเยอรมนี	สาธารณรัฐสิงคโปร์	ประเทศไทย
3.	ความยินยอมจากเจ้าของข้อมูลไบโอเมตริกซ์	การให้ความยินยอมข้อมูล	การให้ความยินยอม	การให้ความ	การให้ความ	การให้ความ
		“ไบโอเมตริกซ์” เพื่อการ	ต้องให้ความยินยอม	ยินยอมข้อมูล	ยินยอมข้อมูล	ยินยอมข้อมูล
		ประมวลผลเก็บรวบรวม	ข้อมูล “ไบโอเมตริกซ์”	“ไบโอเมตริกซ์”	“ไบโอเมตริกซ์”	“ไบโอเมตริกซ์”
		ข้อมูลส่วนบุคคลจะต้องมี	ตั้งแต่ครั้งแรกโดยการ	ในการประมวล	ไม่มี	ไม่มี
		วัตถุประสงค์อย่างน้อย 1 ข้อ	กำหนดให้ผู้บริการ	ข้อมูลส่วนบุคคล	โดยเป็นการขอ	โดยจะเป็นการขอ
		ตาม Regulation (EU)	แจ้งเป็นลายลักษณ์อักษร	จะต้องทำการแจ้ง	ความยินยอม	ความยินยอม
		2016/679 Article 9 ข้อ 2 (a)	เกี่ยวกับการเก็บ รักษา	โดยเฉพาะเจาะจง	ข้อมูลทั่วไป ตาม	ในลักษณะข้อมูล
		ความยินยอมโดยอิสะ ชัดเจน	เปิดเผย ใช้ ลบ ทำลาย	ชัดเจนโดยอิสระ	Consent required	ส่วนบุคคลทั่วไป
		ได้รับแจ้งข้อมูลที่เพียงพอต่อ	ข้อมูลอย่างถาวรเมื่อไม่	ประกาศเป็นลาย	13 และ	ผู้ควบคุมข้อมูล
		การตัดสินใจ ไม่สับสน	ประสงค์และไม่สามารถ	ลักษณ์อักษรอย่าง	Notification of	ส่วนบุคคลต้อง
		ไม่หลงผิด มีการให้	รับข้อมูลได้ เว้นแต่	เป็นอิสระแจ้งข้อ	purpose 20	แจ้งวัตถุประสงค์
		ความยินยอม (Active consent)	จะมีการแจ้งเรื่อง	แตกต่างให้ชัด	เป็นลายลักษณ์	โดยชัดแจ้งเป็น
		ตาม Article 4 (11)	ดังในหน้าที่ 222	ตาม BDSG-new	อักษรอย่างอิสะ	หนังสือ หรือทำ
		กรณีที่ได้เลือกมาให้แล้ว	ในย่อหน้าแรก	Section 51 (2)	ตาม Provision of	โดยผ่านระบบ
		(Pre-select tick) กรณีนี้	กรณีไม่แจ้งความยินยอม	ซึ่งความยินยอม	Consent 14[8]	อิเล็กทรอนิกส์
		ไม่ถือว่าได้มีการยินยอม	ตาม 740 ILCS 10/15 (b)	ต้องสอดคล้องกับ		เว้นแต่
		(Silence pre-ticked boxes or	หากมีการละเมิดอันเป็น	(EU) 2016/679		โดยสภาพไม่อาจ
		inactivity should not	การเพียงพอที่จะนำคดี	Article 9 (1)[9]		ขอความยินยอม
		therefore, constitute consent.)	ขึ้นสู่ศาล[10]			ด้วยวิธีการ
		เช่น กรณี คดี Planet 49[11]				ดังกล่าว ตาม
						มาตรา 19[12]

[8] โปรดดูในหน้าที่ 218

[9] โปรดดูในหน้าที่ 164

[10] โปรดดูในหน้าที่ 185 และ 186

[11] โปรดดูในหน้าที่ 147

[12] โปรดดูในหน้าที่ 99 ข้อ 3.1.7.1

ตารางที่ 4: เปรียบเทียบการถอนคำยินยอม

No	สาระสำคัญ	สหภาพยุโรป	สหรัฐอเมริกา	สหพันธ์รัฐสาธารณรัฐเยอรมนี	สาธารณรัฐสิงคโปร์	ประเทศไทย
4.	การถอนความยินยอมของเจ้าของข้อมูล	กำหนดให้ผู้ให้บริการ	กำหนดให้ผู้ให้บริการ	กำหนดให้ผู้ให้บริการ	กำหนดให้	กำหนดให้
		ต้องแจ้งผลกระทบ	ต้องแจ้งผลกระทบใน	ต้องแจ้งผลกระทบ	ผู้ให้บริการต้อง	ผู้ให้บริการต้อง
		ล่วงหน้าในการถอน	การการถอน “ก่อน”	“ก่อน” ดำเนินการใด	แจ้งผลกระทบ	แจ้งผลกระทบ
		ความยินยอมให้ทราบ	จะดำเนินการใด ตาม	ตาม BDSG- new	“ก่อน”	แต่มิได้บัญญัติ
		ถึงสิทธินั้น “ก่อน” ที่	Section 740	Section 51 (3)[13]	เป็นลายลักษณ์อักษร	คำว่า “ก่อน” ที่จะ
		จะให้ความยินยอม	ILCS 14/25 (b) (3)[14]		ตาม Withdrawal	ให้ความยินยอม
		ตาม Regulation (EU)			of consent (16)[15]	ไว้ในมาตรา 19
		2016/679 Article 7 (3)[16]				วรรคหก[17]

[13] โปรดดูในหน้าที่ 206

[14] โปรดดูในหน้าที่ 185

[15] โปรดดูในหน้าที่ 227

[16] โปรดดูหน้าที่ 164

[17] โปรดดูในหน้าที่ 101

ตารางที่ 5: เปรียบเทียบการแจ้งระยะเวลาในการเก็บ รักษาข้อมูลไบโอเมตริกซ์

No	สาระสำคัญ	สหภาพยุโรป	สหรัฐอเมริกา	สหพันธ์รัฐสาธารณรัฐเยอรมนี	สาธารณรัฐสิงคโปร์	ประเทศไทย
5.	การแจ้งระยะเวลาการเก็บรวบรวมข้อมูลส่วนบุคคล	กำหนดให้ผู้ให้บริการจะต้องแจ้งระยะเวลาในการเก็บ รักษา “ข้อมูลไบโอเมตริกซ์” ซึ่งจะเป็นไปตามหลัก (Right to be forgotten) แก่เจ้าของข้อมูลก่อนการติดต่อครั้งแรกภายในระยะเวลาที่เหมาะสมหลังจากได้รับข้อมูลส่วนบุคคล แต่ไม่เกิน “ภายใน 1 เดือน”โดยคำนึงถึงสถานการณ์เฉพาะที่ข้อมูลส่วนบุคคลถูกประมวลผล” ตามRegulation (EU) 2016/679 Article 14 ข้อ 3 (a)[20]	โดยกำหนดให้ผู้ให้บริการจะต้องแจ้งระยะเวลาการเก็บ ใช้ "ข้อมูลไบโอเมตริกซ์" โดยมีนโยบายแสดงตารางเป็นลายลักษณ์อักษรตามวัตถุประสงค์ หรือภายใน 3 ปี ตาม Section 740 ILCS 14/15 (3)[18]	หากไม่มีการแจ้งระยะเวลาการเก็บใช้ “ข้อมูลไบโอเมตริกซ์” ผู้ควบคุมต้องคำนึงถึงการรวบรวม เก็บใช้ข้อมูลส่วนบุคคลภายในระยะเวลาที่เหมาะสมแต่ไม่เกิน 2 สัปดาห์ ตาม BDSG-new Section 32 (3)[19]	ไม่มีการกำหนดแจ้งระยะเวลาการเก็บใช้ “ข้อมูลไบโอเมตริกซ์” แต่ให้เป็นไปตามวัตถุประสงค์และองค์กรจะต้องยุติการเก็บรักษาข้อมูลส่วนบุคคลทันทีที่ไม่จำเป็นสำหรับวัตถุประสงค์ทางกฎหมาย หรือธุรกิจอีกต่อไป ตาม Retention Of personal data (25)[21]	ไม่มีการกำหนดแจ้งระยะเวลาการเก็บรักษา ใช้“ข้อมูลไบโอเมตริกซ์” ไว้อย่างชัดเจนแต่อย่างไรโดยได้บัญญัติไว้ว่า“กำหนดระยะเวลาที่อาจคาดหมายได้ในการเก็บรวบรวมตามมาตรฐานของการเก็บรวบรวม” มาตรา 23 (3) จึงเป็นการกำหนดระยะเวลาให้ผู้ให้บริการกำหนดเวลาตามเจตนาของตน[22]

[18] โปรดดูในหน้าที่ 185

[19] โปรดดูในหน้าที่ 213 ประเด็นที่สาม

[20] โปรดดูในหน้าที่ 159 ประเด็นที่สาม

[21] โปรดดุในหน้าที่ 227 ประเด็นที่สาม

[22] โปรดดูในหน้าที่ 100

ตารางที่ 6: เปรียบเทียบบทลงโทษ

No	สาระสำคัญ	สหภาพยุโรป	สหรัฐอเมริกา	สหพันธ์รัฐสาธารณรัฐเยอรมนี	สาธารณรัฐสิงคโปร์	ประเทศไทย
6.	บทลงโทษ	สำหรับการละเมิดของ	สำหรับการละเมิด	สำหรับการละเมิด	สำหรับการละเมิด	สำหรับการละเมิด
		(EU) โดยเน้นมาตรการ	ความเป็นส่วนตัว	สำหรับการจงใจหรือ	โดยมีมาตรการ	พระราชบัญญัติ
		ลงโทษปรับทางปกครอง	ข้อมูลทางชีวมาตร	ประมาท ได้กำหนด	ลงโทษปรับและโทษ	คุ้มครองข้อมูล
		สูงสุด 20 ล้าน ยูโร หรือ	ปรับมากกว่า	บทลงโทษสูงทั้งโทษ	ทางอาญา ซึ่งโทษ	ส่วนบุคคล
		ร้อยละ 4 ของรายได้	1,000 ดอลลาร์	ทางอาญาและโทษทาง	ปรับถึง 100,000	พุทธศักราช 2562
		ทั้งหมดทั่วโลกของ	สำหรับการละเมิด	ปกครอง สำหรับการ	ดอลลาร์สิงคโปร์	ได้บัญญัติ
		ปีงบประมาณRegulation	โดยประมาทตาม	ดำเนินคดีปรับสูงถึง	หรือต้องรับโทษจำคุก	บทลงโทษทางแพ่ง
		(EU) 2016/679 Article	Section 5-202	100,000 ยูโร และโทษ	ไม่เกิน 12 เดือน หรือ	โทษทางอาญา
		83 ข้อ 5	โดยมุ่งเน้นโทษ	ทางอาญาจำคุกไม่เกิน	ทั้งจำทั้งปรับตาม	โดยปรับไม่เกิน
		การแจ้งเตือนเมื่อพบว่า	ปรับมากกว่า	2 ปีต่อความเสียหาย	Offences and	1,000,000 บาท
		ข้อมูลรั่วไหล หน่วยงาน	5,000 ดอลลาร์	ตาม Section 41(1) การ	Penalties 51 (5)	จำคุกไม่เกิน 1 ปี
		ควบคุมข้อมูลจะต้องแจ้ง	สำหรับความ	แจ้งเตือน หากพบว่า	การแจ้งเตือนว่า	ตามมาตรา 79
		ให้หน่วยงานกำกับดูแล	เสียหาย ที่แท้จริง	ข้อมูลรั่วไหล	มีการกระทำผิด	**การ** แจ้งเตือน เมื่อ
		และเจ้าของข้อมูลทราบ	ตาม740ILCS14/20	หน่วยงานควบคุม	(Breach notification)	พบว่าข้อมูลรั่วไหล
		ภายใน 72 ชั่วโมง ตาม	(1) และ (2)	ข้อมูลและผู้ประมวล	ไม่มีบัญญัติไว้	แก่สำนักงานและ
		Article 33 (1) และ	ผู้ควบคุมและ	ผลข้อมูลจะต้องแจ้ง	แต่หน่วยงานย่อยของ	ให้ผู้ควบคุมข้อมูล
		กำหนดให้ผู้ประมวลผล	ผู้ประมวลผลต้อง	ให้หน่วยงานกำกับดูแล	รัฐอาจสามารถจะออก	ต้องแจ้งให้
		ข้อมูลต้องแจ้งผู้ควบคุม	แจ้งการลงทะเบียน	และเจ้าของข้อมูลทราบ	ข้อบังคับเป็นพิเศษนี้	หน่วยงานกำกับ
		ทราบทันทีหลังจาก	ไบโอเมตริกซ์	ภายใน 72 ชั่วโมง ตาม	ได้ตาม Section 37	ดูแล และเจ้าของ
		ทราบว่ามีการละเมิด	ล่วงหน้าก่อน[23]	BDSG-new Section	(5) (e)[24]	ข้อมูลทราบ
		ข้อมูลส่วนบุคคลตาม		65 (1) และกำหนดให้ผู้		ภายใน 72 ชั่วโมง
		Article 33 (2)[25]		ประมวลผลข้อมูลต้อง		กำหนดให้ผู้
				แจ้งผู้ควบคุมทราบ		ประมวลผลข้อมูล
				ทันทีหลังจากทราบว่ามี		มีหน้าที่แจ้งการ
				การละเมิดข้อมูลส่วน		ละเมิดให้ผู้
				บุคคล ตาม Section		ควบคุมทราบตาม
				65 (2)[26]		มาตรา 40 (1)[27]

[23] โปรดดูในหน้าที่ 195 ประเด็นที่สี่

[24] โปรดดูในหน้าที่ 228 - 232

[25] โปรดดูในหน้าที่ 164 ประเด็นที่สี่

[26] โปรดดูในหน้าที่ 213ประเด็นที่สี่

[27] โปรดดูในหน้าที่ 109

5.2 ข้อเสนอแนะ

จากสภาพปัญหาดังกล่าวมาแล้วข้างต้น ผู้วิจัยจึงเห็นควร จัดให้มีมาตรการในการแก้ไขปัญหาดังกล่าวให้มีความชัดเจนและสอดคล้องกับนานาประเทศต่างให้ความสำคัญเป็นอย่างยิ่ง โดยเฉพาะปัญหาที่เกี่ยวข้องกับการละเมิดความเป็นส่วนตัวในด้านข้อมูลไบโอเมตริกซ์ อันถือว่าเป็นปัญหาสำคัญที่ผู้บริโภคต้องตระหนักและให้ความสำคัญเป็นอย่างมาก เนื่องการพัฒนาทางเทคโนโลยีก้าวล้ำทำให้ผู้ประกอบการทั้งหลายมีความสามารถในการเก็บ รวบรวมข้อมูลส่วนบุคคล โดยเฉพาะสามารถที่จะเฝ้าติดตามพฤติกรรมในการใช้บริการเว็บไซต์ของผู้ใช้บริการได้ โดยที่ผู้ใช้บริการก็ไม่อาจทราบ และไม่ได้ให้ความยินยอมในการกระทำดังกล่าว หรือแม้กระทั้งจะมีการให้ความยินยอมแล้วก็ตาม ก็ยังอาจนำข้อมูลส่วนบุคคลไปใช้เกินขอบเขตที่ได้ให้ความยินยอมไว้นั้น ทั้งนี้ อาจนำ “ข้อมูลส่วนบุคคลไบโอเมตริกซ์” ไปใช้เพื่อประโยชน์ของผู้ประกอบธุรกิจ หรือนำไปใช้เพื่อประโยชน์ในทางธุรกิจอื่น ๆ อันเป็นการส่งผลกระทบต่อความเป็นส่วนตัวของผู้บริโภค หรือทำให้ผู้บริโภคขาดความเชื่อถือในการกระทำธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งเป็นการทำลายความเชื่อมั่นต่อการพาณิชย์ทางอิเล็กทรอนิกส์ เพื่อให้กฎหมายครอบคลุมในการให้ความคุ้มครองข้อมูลทุกประเภท รวมทั้งครอบคลุมถึงองค์กรเอกชน หรือหน่วยงานของภาครัฐทุกองค์กร ทั้งนี้ ผู้วิจัยได้ศึกษาบันทึกหลักการและเหตุผลประกอบร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.....ก็มิได้ให้คำนิยามของ “ข้อมูลไบโอเมตริกซ์” ไว้แต่อย่างใด แต่ปรากฏว่า “ห้ามเก็บรวบรวมข้อมูลที่มีความอ่อนไหว” (Sensitive data) ซึ่งไม่สอดคล้องกับมาตรา 26 เว้นแต่ จะได้รับความยินยอมตามมาตรา 24 (เดิม) ผู้วิจัยขอเสนอแนะแนวแก้ไขปัญหา ดังนี้

1. ควรเพิ่มบทบัญญัติในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 ดังนี้

คำนิยามศัพท์ ตามมาตรา 6 โดยเพิ่มคำนิยาม “ข้อมูลทางพันธุกรรม” หมายถึง ข้อมูลส่วนบุคคลที่เกี่ยวกับพันธุกรรมของบุคคลธรรมดาซึ่งได้รับ หรือสืบทอดมา โดยข้อมูลพันธุกรรมนี้มีเอกลักษณ์พิเศษเกี่ยวกับสรีรวิทยา หรือสุขภาพของบุคคลนั้น ที่เกิดจากการแสดงผลทางการวิเคราะห์ตัวอย่างทางชีวภาพของบุคคลนั้น โดยเป็นได้ทั้งข้อมูลทั่วไป และข้อมูลที่ละเอียดอ่อนที่ต้องจำแนกประเภทเพื่อให้ผู้ควบคุมตระหนักถึงความปลอดภัยในการจัดเก็บรวบรวม

“ข้อมูลไบโอเมตริกซ์” หมายถึง ข้อมูลส่วนบุคคลที่เกิดจากการประมวลผลทางเทคนิคเฉพาะที่เกี่ยวข้องกับลักษณะทางกายภาพสรีรวิทยา หรือพฤติกรรมของบุคคลธรรมดาซึ่งอนุญาตหรือการยืนยันระบุอัตลักษณ์ของบุคคลนั้น เช่น ภาพใบหน้า หรือข้อมูลลายนิ้วมือ (Dactyloscopic) ซึ่งเป็นข้อมูลเฉพาะโดยแท้จริงของตัวบุคคลนั้น ข้อมูลไบโอเมตริกซ์ ซึ่งเป็นข้อมูลส่วนบุคคลประการหนึ่งที่จะต้องถูกจำแนกอยู่ในประเภทข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive

Personal Information) ซึ่งมีลักษณะพิเศษ กล่าวคือ เป็นข้อมูลที่มีความละเอียดอ่อน หรือมีความอ่อนไหวของข้อมูลสูงกว่าข้อมูลส่วนบุคคลประเภททั่วไป ควรถูกบัญญัติไว้ในบทนิยามคำศัพท์ โดยการให้ได้รับการคุ้มครองไว้ในหมวดหมู่ข้อมูลประเภทพิเศษเฉพาะ

2. หลักการความยินยอม (Consent) และการถอนความยินยอมข้อมูลไบโอเมตริกซ์ ประเด็นปัญหาเพื่อมาตรการในความปลอดภัยนของระบบออนไลน์ โดยการใช้ (Browser) ในการจดจำข้อมูลไบโอเมตริกซ์ที่เข้า (Login) และ (Password) เช่น ข้อมูลคุกกี้ (Data Cookies) รวมถึงประวัติ (History) เพื่อความปลอดภัยในการใช้งานของผู้ใช้งาน โดยข้อคุกกี้ (Data Cookies) ต้องมิใช่การยินยอมโดยอัตโนมัติ ซึ่งต้องมีความชัดเจนในการให้ความยินยอม โดยผู้ใช้บริการมีหน้าที่ต้องแจ้งประกาศหลักเกณฑ์และนโยบายในรูปแบบตารางเป็นลายลักษณ์อักษร รวมทั้งการถอนคำยินยอมที่มีผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลที่จะต้องแจ้งผลกระทบนั้น “ก่อน” ที่จะให้ความยินยอม หรือ ในขณะให้ความยินยอมนั้น ไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 มาตรา 19 วรรคหก หากเจ้าของข้อมูลส่วนบุคคลมีความประสงค์ที่จะถอนข้อมูลของตน ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องทำการแจ้งผลกระทบในการถอนข้อมูลดังกล่าวให้แก่เจ้าของข้อมูลทราบก่อน โดยบัญญัติเพิ่มเติมคำว่า “ก่อน” ที่จะให้ความยินยอมนั้น ๆ

3. การเพิ่มมาตรการความปลอดภัยในการแจ้งระยะเวลาเก็บรักษาข้อมูลไบโอเมตริกซ์ (Biometrics) โดยการแจ้งระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลประเภทพิเศษเกี่ยวกับการประมวลผล การเก็บ รวบรวม เปิดเผย ใช้ ลบ หรือทำลายข้อมูลไบโอเมตริกซ์ในระบบออนไลน์ถูกจดจำในระบบออนไลน์ให้น้อยที่สุดและไม่มีเหตุอันควรให้เก็บรักษาอีกต่อไปแล้ว เพื่อให้ข้อมูลส่วนบุคคลของเจ้าของข้อมูลถูกลบร่องรอยดิจิทัล (Digital footprints) หรือลืมไปเสียจากระบบออนไลน์ ควรมีการแจ้งระยะเวลาที่ข้อมูลจะอยู่ในระบบฐานข้อมูลนานเท่าไร และ “สิทธิที่จะขอลบข้อมูล” (Right to erasure) หรือ สิทธิที่จะถูกลืม (Right to be forgotten) ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 มาตรา 23 (3) ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม” เมื่อพิจารณาการกำหนดระยะเวลาในการเก็บรวบรวมไว้ดังกล่าวนั้น ประเด็นปัญหาการบัญญัติคำว่า “โดยอาจคาดหมายได้” อาจทำให้ผู้ควบคุม หรือผู้ประมวลผลข้อมูลส่วนบุคคลอาจคาดหมายตามเจตนาตนได้ โดยเป็นการไม่ตระหนักถึงความสำคัญถึงข้อมูลที่มีความละเอียดอ่อนดังกล่าว จึงควรกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่แจ้งประกาศหลักเกณฑ์และนโยบายเกี่ยวกับระยะเวลาการเก็บรวบรวมไว้ของข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน ควรบัญญัติระยะเวลาให้เป็นการที่แน่นอนไว้ว่า “ข้อมูลส่วนบุคคลจะเก็บไว้ได้ภายใน 6 เดือน หรือควรให้ทำลายทันที หรือสิ้นสุดตามวัตถุประสงค์ทางธุรกิจ หรือตามข้อตกลงของสัญญา” เพื่อให้สอดคล้อง

ตามหลักสิทธิที่จะถูกลืม (Right to be forgotten) จากระบบออนไลน์ เว้นแต่ ตามวัตถุประสงค์ของกฎหมายได้บัญญัติไว้

4. มาตรการในการป้องกันความมั่นคงปลอดภัยและบทลงโทษ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 ควรจำแนกประเภทของข้อมูลที่มีความละเอียดอ่อนให้รับการคุ้มครองในหมวดหมู่ข้อมูลส่วนบุคคลพิเศษเฉพาะ โดยกำหนดมาตรการในการลงโทษและกำหนดหน้าที่ผู้ควบคุมจึงควรมุ่งเน้นมาตรการด้านการรักษาความมั่นคงปลอดภัยของระบบให้ตระหนักถึงความระมัดระวังอย่างมากในการประมวลผล การเก็บ รวบรวม เปิดเผย ใช้ ลบ หรือทำลาย ซึ่งเป็นข้อมูลส่วนบุคคลที่สามารถบ่งชี้อัตลักษณ์เฉพาะของบุคคลได้นั้น ซึ่งมีความแตกต่างจากข้อมูลทั่วไป ควรคุ้มครองอย่างเหมาะสมตามของประเภทข้อมูลในด้านวิธีการ วิธีปฏิบัติการรักษาความมั่นคงปลอดภัยให้มีประสิทธิภาพยิ่งขึ้น เพื่อให้มีความสอดคล้องกับเศรษฐกิจดิจิทัลทั่วโลก หรือวิธีปฏิบัติตามกรอบมาตรฐานของสากลยอมรับเท่าที่จะเป็นไปได้ โดยพระราชบัญญัติฉบับนี้ ได้บัญญัติความผิดไว้ทั้งโทษทางแพ่งและโทษทางอาญาในกรณีที่มีการละเมิด ในกรณีที่ไม่ปฏิบัติตามได้มีโทษปรับทางปกครองสูงถึง 5 ล้านบาทและบทลงโทษทางอาญา จำคุกไม่เกิน 1 ปี และค่าเสียหายเชิงลงโทษสูงถึงสองเท่าของความเสียหายที่เกิดขึ้นจริงนั้น โดยผู้วิจัยเห็นว่ารัฐจะต้องไม่ออกกฎหมายบังคับใช้เฉพาะประเทศไทยเท่านั้น อันจะเป็นการขัดขวางการลงทุนในการการพัฒนาธุรกิจให้ก้าวทันกับยุคเทคโนโลยีปัจจุบันและในอนาคตที่ผู้ประกอบธุรกิจอาจต้องรับโทษทางอาญา ซึ่งจะไม่ก่อให้เกิดประโยชน์แต่ประการใด

กรณีมีการละเมิดควรมีบทลงโทษปรับเพิ่มตามการกระทำนั้น ๆ ว่ากระทำโดยจงใจ หรือประมาท ตามกฎหมายที่ได้บัญญัติไว้สำหรับการละเมิดนั้น สำหรับผู้ควบคุมและผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งไม่สอดคล้องกับ GDPR ตามArticle 83 ของ Regulation (EU) 2018/1725 อันเป็นข้อกำหนดความรับผิดทางแพ่ง (Civil Liability) เพื่อให้บุคคลมีหน้าที่พึงระวังไม่ให้เกิดความเสียหายแก่ผู้อื่น (Duty of Care) หากเกิดความเสียหายขึ้น โดยเฉพาะพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธราช 2562 ฉบับปัจจุบัน ซึ่งเป็นบทกำหนดโทษทางอาญาสำหรับผู้ควบคุมและผู้ประมวลผลข้อมูลส่วนบุคคลรวมทั้งความรับผิดของบุคคลธรรมดาด้วย สำหรับการกระทำที่ฝ่าฝืนพระราชบัญญัติฉบับนี้

ปัญหาดังกล่าวนี้ ทำให้ประเทศไทยเกิดสภาพกฎหมายอาญาเฟ้อ (Over-criminalization) ซึ่งความผิดโทษทางอาญายังได้ปรากฏอยู่ในอยู่ตามพระราชบัญญัติต่าง ๆ อีกหลายร้อยฉบับ สถานการณ์ดังกล่าวส่งผลเสียหลายประการ ทำให้โทษทางอาญาไม่มีความเหมาะสมกับการประกอบธุรกิจในยุคดิจิทัลแต่อย่างใด เพราะในแนวทางแก้ไขเยี่ยวยาดังกล่าว อาจเกินสัดส่วนกับความเสี่ยงที่ได้รับ ดังกล่าวไว้ในข้อที่ 4 หน้าที่ 238 - 240 แม้ว่าในบางประเทศจะมีการกำหนดโทษ

ทางอาญา แต่ก็มิใช่แนวทางสากล จึงควรกำหนดสัดส่วนมาตรการลงโทษผู้ที่ไม่ปฏิบัติตามกฎหมาย ตลอดจนค่าสินไหมทดแทนที่เป็นตัวเงินและมาตรการการเยียวยา เพื่อควบคุมผู้กระทำที่ฝ่าฝืน โดยผ่านทางกระบวนการลงโทษทางปกครอง หรือมาตรการทางแพ่งก็เป็นการเพียงพอแล้ว ซึ่งต้องแก้ไขดังนี้

(1) โดยการแก้ไขยกเลิก มาตรา 79 และมาตร 80 ออก ซึ่งมาตร 79 ซึ่งเป็นการกำหนดความรับผิดโดยเด็ดขาด โดยไม่พิจารณาถึงกรณีที่ได้กระทำไปโดยมีเหตุอันควร หรือเพื่อบรรเทาความเสียหายที่อาจเกิดขึ้นได้ แล้วทำการแก้ไขเพิ่มเติมมาตร 77 และมาตรา 78

(2) โดยการบัญญัติไม่ให้ผู้ประมวลข้อมูลส่วนบุคคลต้องรับผิดออก เนื่องจากผู้ประมวลผลข้อมูลจะต้องรับผิดต่อความเสียหายที่เกิดจากการประมวลผลข้อมูลส่วนบุคคลเฉพาะในกรณีไม่ปฏิบัติหน้าที่ของตนตามพระราชบัญญัตินี้ และเพิ่มเติมอนุสาม ไว้ในมาตรา 77 โดยบัญญัติดังนี้ “(3) โดยเป็นการกระทำการไปโดยมีเหตุอันควร หรือเพื่อเป็นการบรรเทาความเสียหายที่อาจเกิดขึ้นได้ต่อเจ้าของข้อมูลส่วนบุคคล” จึงควรจำกัดเพียงผู้ควบคุมข้อมูลเท่านั้น อาจป้องกันผู้ควบคุมข้อมูลส่วนบุคคลจากความรับผิดโดยเด็ดขาดตามมาตร 79

เมื่อพิจารณาสาระสำคัญของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธราช 2562 ซึ่งได้แก่ การเก็บการใช้ หรือ การเปิดเผย ลบ หรือทำลายข้อมูลส่วนบุคคลต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อน โดยมีการแจ้งวัตถุประสงค์ในการเก็บ ใช้ เปิดเผยอย่างชัดเจน และต้องทำเท่าที่จำเป็นที่ให้ความยินยอมไว้ โดยมีการกำหนดหน้าที่ของผู้ควบคุมและประมวลผลข้อมูลส่วนบุคคลในการจัดมาตรการรักษาความปลอดภัยและบันทึกข้อมูลส่วนบุคคล โดยการกำหนดมาตรฐานในการโอนย้ายข้อมูลไปต่างประเทศ รวมถึงการเพิ่มสิทธิ์ของเจ้าของข้อมูลส่วนบุคคลในการโต้แย้งระงับการใช้ข้อมูล หากฝ่าฝืนจะต้องมีโทษทางปกครองและหรือโทษทางอาญา เมื่อเปรียบเทียบกับกฎหมายของ (GDPR) ในกรณีกำหนดบทลงโทษเฉพาะโทษปรับทางปกครองเท่านั้น แต่ปรากฏว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธราช 2562 โดยบัญญัติมาตรการลงโทษทางอาญาอันเป็นโทษจำคุกนั้น ทั้งนี้ จะเป็นการผลักให้ผู้ประกอบการธุรกิจต้องตกอยู่ภายใต้ความเสี่ยงที่จะรับโทษอาญา ซึ่งไม่สอดคล้องกับยุคดิจิทัลที่ผู้ประกอบการธุรกิจมีอยู่ทั่วโลก

ประเด็นที่น่าสนใจตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธราช 2562 ผู้วิจัยได้ศึกษาเปรียบเทียบแล้ว ปรากฏว่า มิได้มีความสอดคล้องกับกฎหมาย GDPR ในมาตรการให้ความยินยอมตาม Article 9 และมาตรการบทลงโทษทางอาญา ในเรื่องการให้ความยินยอมในการประมวลข้อมูลไบโอเมตริกซ์ต้องยินยอมอย่างชัดเจนเฉพาะเจาะจงเพื่อให้เป็นไปตามวัตถุประสงค์ของเจ้าของข้อมูล ซึ่งต้องระบุการยินยอมในการประมวลข้อมูลไบโอเมตริกซ์นั้น โดยต้องเป็นลายลักษณ์อักษรต้องอย่างน้อย 1 ข้อ แต่ปรากฏว่า บทบัญญัติในพระราชบัญญัติคุ้มครองข้อมูล

ส่วนบุคคล พุทธศักราช 2562 ในมาตรา 19 การให้ความยินยอมในการประมวลผลข้อมูลส่วนบุคคลเป็นการทั่วไปนั้น ไม่แจ้งเตือน “การขอความยินยอมต้องแจ้งตั้งแต่เริ่มแรกโดยชัดแจ้ง” ซึ่งต้องมิใช่การยินยอมเช่นเดียวกับข้อมูลส่วนบุคคลทั่วไป ดังนั้น การขอยินยอมในข้อมูลไบโอเมตริกซ์ควรบัญญัติให้ไว้โดยเฉพาะเจาะจงเป็นลายลักษณ์อักษรชัดเจนและไม่คลุมเครือ มิใช่การยินยอมโดยอัตโนมัติและต้องเป็นไปตามวัตถุประสงค์ของเจ้าข้อมูลส่วนบุคคลที่เกี่ยวข้องกับผู้ให้ความยินยอมเท่านั้น หรือไม่อย่างไร อันเป็นประเด็นที่ควรศึกษาต่อไปอย่างยิ่ง

ตัวอย่างเช่น

รูปภาพที่ 9 : ความยินยอมสำหรับการประมวลผลข้อมูลส่วนบุคคลประเภทพิเศษตามหลักเกณฑ์ของสหภาพยุโรป[28]

Purposes for processing special categories of personal data

Special Category Lawful Basis: We are permitted to process your personal data because;	You have given your explicit consent to the processing	It is necessary to protect someone's vital interests or they are incapable of giving consent	It is necessary for the establishment, exercise or defence of legal claims	It is necessary for reasons of substantial public interest
Providing legal advice to our clients			×	×
Investigating, evaluating, demonstrating, monitoring, improving and reporting on our compliance with relevant legal and regulatory requirements [such as anti-money laundering and client verification checks]				×
Complying with [or assisting others' compliance with] regulatory requirements involving steps being taken to establish the existence of any unlawful act, dishonesty, malpractice, or other seriously improper conduct				×
Complying with our general regulatory and statutory requirements				×
Responding to binding requests or search warrants or orders from courts, governmental, regulatory and/or enforcement bodies and authorities or sharing information [on a voluntary basis] with the same			×	×
Obtaining legal advice, establishing, defending and enforcing our legal rights and obligations in connection with, any legal proceedings [including prospective legal proceedings]			×	×
Hosting you at our offices [and/or other appropriate venues] and providing hospitality services	× [For your dietary and access requirements]	× [In case of accidents at our offices or whilst at a hospitality event which we host]		

[28] WENDY HOPKINS FAMILY LAW PRACTICE. (2019). ***Privacy Notice***. (ออนไลน์). เข้าถึงได้จาก : https://wendyhopkins.co.uk/privacy-notice/. [2562, 4 พฤศจิกายน].

จากที่ประเด็นปัญหาที่กล่าวมาแล้วทั้งหมดข้างต้น ในเรื่องมาตรการทางกฎหมายในการให้ความคุ้มครองข้อมูลไบโอเมตริกซ์นั้น แม้ผู้วิจัยจะได้กล่าวถึงสภาพปัญหาและมาตรการทางกฎหมายในการแก้ปัญหาไว้บางประการแล้วก็ตาม ด้วยผู้วิจัยมีข้อจำกัดในการค้นคว้าวิจัยทางด้านข้อมูลเอกสารวิจัยและการดันแปลงข้อมูลจากภาษาต่างประเทศมาเป็นภาษาไทยตลอดจนระยะเวลาอันจำกัดในการศึกษาตามหลักสูตรนิติศาสตรมหาบัณฑิตทำให้งานวิจัยฉบับนี้ จึงทำได้เพียงที่ได้กล่าวมาแล้วข้างต้น อย่างไรก็ตาม หากมีบุคคลใด หรือ นักศึกษาท่านใด สนใจประสงค์ที่จะศึกษาวิจัยในหัวข้อประเด็นนี้ต่อไป ผู้วิจัยเห็นว่ายังคงมีบางประเด็นปัญหาสำคัญที่อาจทำวิจัยต่อเพิ่มเติมได้ ดังนี้

1. ความยินยอมที่อยู่ในรูปแบบอิเล็กทรอนิกส์ (Electronic consent) เช่น กรณี Cookies History Password ควรมีมาตรการอย่างไร
2. มาตรการภายหลังลบข้อมูลส่วนบุคคลในระบบออนไลน์ (Right to erase) หรือ “สิทธิที่จะถูกลืม”ภายหลังที่ลบ (Right to be Forgotten)
3. มาตรการในการคุ้มครองข้อมูลส่วนบุคคลของผู้เยาว์ควรได้การคุ้มครองในระดับใดซึ่งมีความเปราะบางเป็นพิเศษ ควรมีมาตรการอย่างไร
4. “สิทธิที่จะถูกลืมจากความทรงจำของสาธารณะ” และ “สิทธิที่จะขอลบข้อมูล” หรือ Right to erasure โดย ณ ที่นี้ ประชาชนจะผู้เป็น “เจ้าของข้อมูล” (Data subject) และมีสิทธิที่จะขอลบข้อมูลนี้ได้หรือไม่
5. มาตรการของสิทธิซ้อนทับกับสิทธิ โดยสิทธิที่จะถูกลืม และ สิทธิในการรับรู้ข้อมูลข่าวสารนั้น การที่สิทธิที่จะถูกลืมทำให้เป็นเรื่องของสิทธิมนุษยชนและสิทธิในการรับรู้ข้อมูลข่าวสารเป็นเรื่องของสิทธิเสรีภาพในการแสดงออกก็เป็นสิทธิมนุษยชนควรมีมาตรการอย่างไร
6. มาตรการลงโทษทางอาญา (Criminal penalty) ประเทศไทยควรมีหรือไม่ อย่างไร