บทที่ 4

วิเคราะห์การคุ้มครองความเป็นส่วนตัวของข้อมูลไบโอเมตริกซ์ (Biometrics)

จากการศึกษาแนวความคิดทฤษฎี ความหมายและรูปแบบของการคุ้มครองข้อมูลส่วนบุคคลเป็นสิทธิและเสรีภาพขั้นพื้นฐานเท่าเทียมกันของบุคคลที่จะติดต่อสัมพันธ์กับบุคคลอื่นและถูกจำกัดสิทธิภายใต้รัฐธรรมนูญ ก็ต้องใช้สิทธิและเสรีภาพของตนให้ถูกต้องเหมาะสมด้วย เพราะแม้ว่าการใช้สิทธิและเสรีภาพจะเป็นการกระทำเพื่อให้เกิดประโยชน์แก่ตน แต่ต้องคำนึงความเสียหายผู้อื่นที่ได้รับและประโยชน์ของสังคมประกอบกันด้วย ซึ่งการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติข้อมูลข่าวสาร พุทธศักราช 2540 เป็นกรณีให้การคุ้มครองข้อมูลส่วนบุคคลเฉพาะข้อมูลที่อยู่ในความครอบครองของหน่วยงานภาครัฐเท่านั้น แต่มิได้ให้ความคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานเอกชน หรือบุคคล ตลอดรวมทั้งมาตรการทางกฎหมายที่ใช้บังคับในการให้ความคุ้มครองข้อมูลส่วนบุคคลในกรณีข้อมูลไบโอเมตริกซ์ (Biometrics) อีกทั้งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พุทธศักราช 2562 โดยมุ่งเน้นการคุ้มครองภัยคุกคามทางไซเบอร์ที่ให้อำนาจเจ้าพนักงานหน้าที่องค์กรที่ได้จัดตั้งขึ้นตามพระราชบัญญัติมากจนเกินไป โดยการอิงการป้องกัน “ภัยคุกคามทางไซเบอร์” การมีอำนาจดังกล่าว จึงกลายเป็นการล้วงล้ำความไม่ปลอดภัยในสิทธิความเป็นส่วนตัวของประชาชนจนเกินไป

ผู้วิจัยจึงได้ศึกษาเปรียบเทียบกฎหมายการคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศและประเทศไทย พบว่า ปัจจุบันมีการเก็บ รวบรวม ใช้ เปิดเผย หรือทำลายข้อมูลไบโอเมตริกซ์ผ่านระบบเทคโนโลยี และถูกเก็บไว้ในฐานข้อมูลขนาดใหญ่ (Big data) เพื่อที่นำไปใช้ในเชิงพาณิชย์และการติดต่อสื่อสารเป็นการทั่วไป ซึ่งข้อมูลไบโอเมตริกซ์เป็นข้อมูลที่มีความละเอียดอ่อนเป็นข้อมูลลับเฉพาะตัวโดยแท้ โดยปัจจุบันเป็นยุคดิจิทัลมีข้อมูลจำนวนมากที่เกิดจากการปฏิสัมพันธ์กันระหว่างบุคคลผ่านทางอุปกรณ์ที่เชื่อต่อกันกับอินเทอร์เน็ต อันเป็นการง่ายต่อการถูกละเมิดได้และก่อให้เกิดความเสียหายแก่เจ้าของมูลส่วนบุคคล ซึ่งยากต่อการแก้ไขเปลี่ยนแปลงเมื่อมีการละเมิด จากปัญหาดังกล่าวเป็นผลสืบเนื่องจากปัญหาทางกฎหมายบางประการที่ยังไม่มีความชัดเจนและเหมาะสมเพียงพอ โดยมีปัญหาเกี่ยวกับการคุ้มครองข้อมูลไบโอเมตริกซ์ที่จะได้วิเคราะห์ดังต่อไปนี้

4.1 วิเคราะห์ปัญหาเกี่ยวกับคำจำกัดความของข้อมูลส่วนบุคคล

จากการศึกษาพบว่า ปัญหาความไม่ชัดเจนของคำจำกัดความของคำนิยามศัพท์ “ข้อมูลไบโอเมตริกซ์” (Biometrics) ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 มาตรา 6 บัญญัติว่า “ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรง หรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ แต่มิได้บัญญัติ “ข้อมูลพันธุกรรมและข้อมูลไบโอเมตริกซ์” ซึ่งเป็นข้อมูลที่มีความละเอียดอ่อนและอ่อนไหวง่ายต่อความรู้สึก

ผู้วิจัยเห็นว่า การจำกัดความของคำนิยามศัพท์ในลักษณะเช่นนี้ อันเป็นการให้คำจำกัดความของคำนิยามศัพท์แบบกว้างเป็นการทั่วไป อีกทั้ง ยังไม่มีความชัดเจนในการจำแนกประเภทว่า “ข้อมูลส่วนบุคคล” ตามพระราชบัญญัติฉบับนี้ มีเจตนาให้ข้อมูลส่วนบุคคลมีความหมายว่าอย่างไรบ้าง อีกทั้งมีเจตนาให้ครอบคลุมถึงข้อมูลใดบ้าง หากความไม่ชัดเจนของคำนิยามอาจส่งผลกระทบได้ดังนี้

1. หากบุคคลทั่วไปมิอาจเข้าใจความหมายข้อมูลที่มีความละเอียดอ่อน (Sensitive data) เมื่อได้ยืนยันความยินยอมในระบบ หรือการให้ยินยอมเพื่อการปฏิบัติตามสัญญาดังกล่าวแล้ว จึงถือได้ว่าบุคคลนั้นได้อ่านและเข้าใจเนื้อหาของคำร้องขอฉบับดังกล่าวนี้อย่างละเอียดแล้ว และยืนยันว่าข้อมูลต่าง ๆ ที่ได้แจ้งให้ทราบนั้นถูกต้องก็จะมีผลบังคับใช้ตามกฎหมาย ดังนั้น เมื่อไม่มีนิยามคำศัพท์ที่ชัดเจนในพระราชบัญญัติฉบับนี้ อาจทำให้การบังคับใช้กฎหมายมีปัญหาเกิดการตีความโดยเจ้าหน้าที่เพื่อประโยชน์ของผู้มีอำนาจในเวลานั้น แต่อย่างไรก็ตาม ข้อมูลส่วนบุคคลดังกล่าวนี้ สิทธิผู้เป็นเจ้าของข้อมูลสามารถที่เข้าถึงข้อมูลของตน สามารถแก้ไขข้อมูลให้ถูกต้อง รวมถึงสิทธิในการรับทราบ และจัดการข้อมูลนั้นได้ กล่าวคือ อาจหมายถึงการทำลาย หรือระงับข้อมูลส่วนตัวนั้นได้

2. กรณีที่กฎหมายได้บัญญัติให้กระทำในการเปิดเผยข้อมูลส่วนบุคคลได้ หรือยกเว้นโดยไม่ต้องได้รับความยินยอมก่อน หรือแม้จะให้ความยินยอมตามสัญญาก็ตาม แต่ยังคงปรากฏให้เห็นอยู่เสมอว่า ข้อมูลส่วนบุคคลที่ผู้ให้บริการเก็บไว้ในระบบฐานข้อมูล และมีหน้าที่ต้องควบคุมดูแลอย่างดีนั้น ได้ถูกเปิดเผยและนำไปใช้ประโยชน์ไม่ว่าในทางใด ๆ หากผู้ให้บริการขอให้บุคคลนั้นยอมรับนโยบายของผู้ให้บริการเช่นนี้ การปฏิเสธที่จะให้บริการแก่ผู้ใช้บริการก็อาจเกิดขึ้นได้หากบุคคลนั้นไม่รับเงื่อนไขของเว็บไซต์ อาจจะทำให้ผู้ใช้บริการไม่ได้รับบริการนั้นได้ อันเป็นการขัดต่อพระราชบัญญัติฉบับนี้นั้น อย่างไรก็ตาม แม้ว่า (GDPR) จะมีกฎข้อบังคับที่เข้มงวด แต่ก็มีข้อยกเว้นที่อนุญาตให้มีการรวบรวมและใช้ข้อมูลที่มีความอ่อนไหวซึ่งอาศัย

ข้อยกเว้น หากเจ้าของข้อมูลยินยอมด้วยตนโดยให้ความสำคัญกับการได้รับความยินยอมจากเจ้าข้อมูลก่อน ส่วนประเด็นปัญหาในการจำกัดความของ “ความยินยอม” ใน (GDPR) กล่าวคือ การที่นำไปใช้แล้วไม่พิจารณาในเรื่องการให้ความยินยอมอย่างเสรี (Freely given) จนเกิดความไม่สมดุลของอำนาจระหว่างผู้ควบคุมข้อมูลกับเจ้าของข้อมูล

ดังนั้น ส่งผลในทางปฏิบัติแก่เจ้าของข้อมูล หรือผู้ควบคุม หรือผู้ประมวลผลข้อมูล อาจตีความตามเจตนาของตนว่าข้อมูลใดเป็นข้อมูลส่วนบุคคลที่อ่อนไหวง่าย หรือข้อมูลทั่วไป ทำให้ผู้ปฏิบัติต้องตีความว่าข้อมูลใดบ้างเป็นข้อมูลส่วนบุคลที่ต้องเก็บ รวบรวม เปิดเผย หรือใช้ได้อย่างระมัดระวัง หรือในกรณีเกิดข้อพิพาทจำต้องใช้ดุพินิจในการตีความในการบังคับใช้กฎหมายตามพระราชบัญญัติฉบับนี้อย่างไร จากการศึกษาผู้วิจัยมีข้อสังเกตเกี่ยวกับประเภทข้อมูลส่วนบุคคลว่า“ข้อมูลพันธุกรรม และข้อมูลไบโอเมตริกซ์” (Biometrics) ตามคำนิยามศัพท์มาตรา 6 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ควรมีความหมายที่ชัดเจนและสอดคล้องตามหลักสากล ดังนี้

ประการแรก การบัญญัติคำนิยามในมาตรา 6 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 ยังไม่มีความชัดเจนประเภทของข้อมูลส่วนบุคคล

ผู้วิจัยได้พิจารณาแล้วเห็นว่าควรบัญญัติคำนิยาม “ข้อมูลพันธุกรรม” (Heredity) ซึ่งหมายถึง สิ่งที่เป็นลักษณะต่าง ๆ ของสิ่งมีชีวิตที่ได้รับการถ่ายทอดลักษณะต่าง ๆ จะถูกถ่ายทอดจากบรรพบุรุษไปสู่รุ่นลูกหลาน โดยหน่วยพันธุกรรมในเซลล์ที่เรียกว่า ยีน หรือ ดีเอ็นเอ (DNA) ของบุคคลนั้น ๆ ได้แก่ ลักษณะสีนัยน์ตา สีผม สีผิว ความสูง น้ำหนักตัว สติปัญญา ความถนัด เป็นต้น ซึ่งสามมารถเป็นได้ทั้งข้อมูลส่วนบุคคลทั่วไปและข้อมูลอ่อนไหว รวมทั้งโดยเฉพาะอย่างยิ่ง “ข้อมูลไบโอเมตริกซ์” (Biometrics) หมายถึง ข้อมูลที่เกิดจากเทคโนโลยีด้านชีวมาตรความรู้ทางการแพทย์และเทคโนโลยีทางคอมพิวเตอร์เข้าด้วยกัน โดยเทคโนโลยี (Biometrics) สามารถใช้ลักษณะทางกายภาพของบุคคล (Physical) เช่น ลายนิ้วมือ รูม่านตา โครงสร้างใบหน้า เพื่อยืนยันและระบุความเป็นตัวตน (Individual’s Identity) อันเป็นข้อมูลบ่งชี้และเชื่อมโยงไปยังตัวบุคคลนั้นได้ จึงต้องให้ความสำคัญในการพิจารณาว่า “ข้อมูลพันธุกรรม” เป็นได้ทั้งข้อมูลทั่วไปและข้อมูลที่มีความละเอียดอ่อน ส่วนกรณี “ข้อมูลไบโอเมตริกซ์” ซึ่งเป็นข้อมูลลับเฉพาะที่มีความอ่อนไหวง่ายจะต้องได้รับการคุ้มครองในหมวดหมู่พิเศษ และจำแนกประเภทออกจากข้อมูลทั่วไปจะทำให้ผู้ควบข้อมูล หรือผู้ประมวลผลข้อมูล และเจ้าของข้อมูลส่วนบุคคลทราบถึงประเภทของข้อมูลส่วนบุคคลแต่ละประเภทที่ต้องระมัดระวังในการทำธุรกรรมต่าง ๆ เช่นเดียวกันกับสากลประเทศโดยจะได้ทำการศึกษาเปรียบเทียบความแตกต่าง ดังต่อไปนี้

“ข้อมูลทางพันธุกรรม” ให้หมายถึง ข้อมูลส่วนบุคคลที่เกี่ยวกับพันธุกรรมของบุคคลธรรมดา ซึ่งได้รับ หรือสืบทอดมา โดยข้อมูลนี้นี้มีเอกลักษณ์พิเศษเกี่ยวกับสรีรวิทยา หรือสุขภาพของบุคคลนั้น โดยแสดงผลจากการวิเคราะห์ตัวอย่างทางชีวมาตรของบุคคลนั้น ด้วยเหตุเพราะว่า “ข้อมูลพันธุกรรม” เป็นข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน หากเกิดจากเทคนิคทางการแพทย์และเป็นได้ทั้งข้อมูลทั่วไป ซึ่งในทางปฏิบัติหากจำแนกประเภทของข้อมูลให้เหมาะสมง่ายต่อการดำเนินงานประเภทนั้น ๆ

“ข้อมูลไบโอเมตริกซ์” ให้หมายถึง ข้อมูลส่วนบุคคลที่เกิดจากการประมวลผลทางเทคนิคเฉพาะที่เกี่ยวข้องกับลักษณะทางกายภาพสรีรวิทยา หรือพฤติกรรมของบุคคลธรรมดาซึ่งอนุญาต หรือ การระบุอัตลักษณ์ของบุคคลนั้น เช่น ภาพใบหน้า หรือข้อมูลลายนิ้วมือ ด้วยเหตุเพราะว่า “ข้อมูลไบโอเมตริกซ์” (Biometrics) เป็นข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวโดยแท้ของบุคคลมีความละเอียดอ่อนและอ่อนไหวง่าย และสุ่มเสี่ยงต่อการถูกใช้ และในการเลือกปฏิบัติอย่างไม่เป็นธรรม หากมีการรั่วไหลของข้อมูล หรือละเมิด ก่อให้เกิดความเสียหาย สูญหาย เปลี่ยนแปลง การเปิดเผยโดยไม่ได้รับอนุญาต หรือเข้าถึงข้อมูลส่วนบุคคล เป็นการยากที่ผู้เป็นเจ้าของข้อมูลจะทำการแก้ไขเปลี่ยนแปลงได้ จึงจำเป็นให้ความคุ้มครองอยู่ในหมวดพิเศษเฉพาะและดำเนินการด้วยความระมัดระวังเป็นพิเศษ

“หมวดหมู่ประเภทข้อมูลพิเศษของข้อมูลส่วนบุคคล” โดยเป็นข้อมูลที่แสดงถึงเชื้อชาติ หรือ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนา หรือ อุดมการณ์ หรือ การเป็นสมาชิกสหภาพแรงงาน ควรจัดจำแนกประเภท เพื่อให้ได้รับการคุ้มครองในหมวดหมู่พิเศษเฉพาะ ได้แก่ ข้อมูลทางพันธุกรรม ข้อมูลไบโอเมตริกซ์เพื่อระบุเอกลักษณ์ของบุคคลธรรมดา ข้อมูลด้านสุขภาพ และข้อมูลเกี่ยวกับชีวิตเพศ หรือรสนิยมทางเพศ เป็นต้น

ประการสุดท้าย ความแตกต่างของคำนิยามศัพท์

ภายใต้ข้อบังคับของสหภาพยุโรปคำว่า “ข้อมูลส่วนบุคคล” หมายถึง “ข้อมูลใด ๆ ก็ตามที่เกี่ยวข้องถึงการบ่งชี้ตัวบุคคลธรรมดา หรือที่อาจบ่งชี้ได้ถึงตัวบุคคลธรรมดาไม่ว่าโดยทางตรงหรือทางอ้อม โดยเฉพาะการอ้างอิงถึงตัวบ่งชี้ เช่น ชื่อ หมายเลขประจำตัว กายภาพ สรีรวิทยา พันธุกรรม” ของบุคคลนั้นที่เกี่ยวข้องกับบุคคลที่สามารถระบุตัวตน หรือระบุตัวบุคคลนั้นได้ ซึ่งได้บัญญัติ “ข้อมูลพันธุกรรม” โดยถูกบัญญัติไว้ให้เป็นการทั่วไปด้วย แต่อย่างไรก็ตาม ภายใต้ข้อบังคับ Regulation (EU) 2016/679 Article 4 (13) (14) และ Regulation (EU) 2018/1725 Article 3 (17) (18) ของ (GDPR) จะเห็นได้ว่า คำนิยามของกฎหมายทั้งสองฉบับนี้ถูกบัญญัติไว้คนละมาตรา แต่ได้บัญญัติคำนิยามศัพท์ดังกล่าว โดยจำแนกต่างหากออกจากข้อมูลส่วนบุคคลทั่วไปอย่างชัดเจน ซึ่งสหภาพยุโรปให้ความคุ้มครอง “ข้อมูลพันธุกรรมและข้อมูลไบโอเมตริกซ์” เป็นข้อมูล

ที่มีความอ่อนไหวไว้ในหมวดหมู่พิเศษเฉพาะ ตาม Regulation (EU) 2018/1725 Article 10 และ Regulation (EU) 2016/679 Article 9 ดังที่ผู้วิจัยได้วิเคราะห์ไว้ในบทที่ 3[1] ซึ่งกฎระเบียบของสหภาพยุโรปได้ให้การคุ้มครองเป็นพิเศษเฉพาะในข้อมูลส่วนบุคคลบางประเภทว่ามีความละเอียดอ่อนและจำเป็นต้องป้องกันอย่างเข้มงวด

สำหรับการประมวลผลข้อมูลพันธุกรรมและข้อมูลไบโอเมตริกซ์ดังกล่าว อันเป็นข้อมูลที่บ่งชี้เฉพาะของบุคคลโดยแท้จริงตามธรรมชาติของแต่ละบุคคลนั้น ๆ โดยเฉพาะอย่างยิ่งเกี่ยวกับสิทธิขั้นพื้นฐานและเสรีภาพที่จะต้องได้รับการคุ้มครองเฉพาะเจาะจงเป็นพิเศษ เนื่องจากการประมวลผลข้อมูลส่วนบุคคลนั้น อาจสร้างความเสี่ยงให้แก่เจ้าของข้อมูลได้ โดยสหภาพยุโรปจึงให้การคุ้มครองในหมวดหมู่พิเศษ (ข้อมูลที่ละเอียดอ่อน) ดังนั้น คำจำกัดความจึงไม่เพียงแต่เฉพาะข้อมูลทั่วไปเท่านั้น แต่ยังรวมถึงข้อมูลที่สามารถบ่งชี้ หรือเชื่อมโยงได้ว่าข้อมูลที่ละเอียดอ่อนนั้นสามารถระบุตัวตนเกี่ยวกับบุคคลนั้นได้ และยังง่ายต่อผู้ปฏิบัติไม่ต้องตีความว่าข้อมูลดังกล่าวเป็นประเภททั่วไปหรือไม่ เมื่อข้อมูลอยู่ในหมวดหมู่พิเศษ จึงต้องห้ามการประมวลผล เว้นแต่กฎหมายอนุญาต

สหรัฐอเมริกา Privacy Act 1994 [2] ได้บัญญัติคำนิยามไว้ในมาตรา 5 U.S.C.§ 552 a (a) (4) คำว่า “บันทึก” หมายถึง สิ่งใด ๆ ที่ข้อมูลนั้นเกี่ยวกับบุคคล การเก็บ รวบรวม การเก็บรักษา ใช้ หรือเปิดเผย..... ชื่อบุคคล เลขบัตรประจำตัวประชาชน สัญลักษณ์ หรือบ่งชี้สิ่งอื่นใดที่สามารถระบุตัวบุคคลนั้นได้ เช่น ลายพิมพ์นิ้วมือ หรือ ลายพิมพ์เสียง หรือ รูปภาพ ซึ่งคำจำกัดความดังกล่าวนี้บ่งชี้ได้ว่าสิ่งอื่นใดสามารถระบุตัวบุคคลนั้นได้ ที่เกิดจากการใช้เทคโนโลยีไบโอเมตริกซ์นั้นด้วย โดยเป็นการบัญญัติแบบกว้าง ๆ เป็นการทั่วไป แต่ก็มิได้มีการจำแนกข้อมูลที่อ่อนไหวออกจากข้อมูลทั่วไป แต่อย่างไรก็ตาม สหรัฐอเมริกาได้ตราพระราชบัญญัติคุ้มครองข้อมูลความเป็นส่วนตัวทางชีวมาตร (Biometric Information Privacy Act 2008: BIPA) ซึ่งได้บัญญัติคำนิยามศัพท์ “ข้อมูลไบโอเมตริกซ์” เป็นข้อมูลที่มีความอ่อนไหว โดยจำแนกออกจากข้อมูลทั่วไป เว้นแต่ข้อมูลที่ได้จากการรวบรวม หรือ ขั้นตอน ที่ได้ยกเว้นภายใต้คำจำกัดความ และมิได้บัญญัติ “ข้อมูลพันธุกรรม” ไว้ในหมวดหมู่ข้อมูลที่มีความอ่อนไหว แต่ข้อมูลทางพันธุกรรมมีการควบคุมภายใต้พระราชบัญญัติทางกายวิภาคของรัฐอิลลินอยส์ จึงทำให้คำนิยามศัพท์ของข้อมูลส่วนบุคคลมีความชัดเจนและทำให้ผู้ปฏิบัติเกี่ยวกับข้อมูลส่วนบุคคลดังกล่าวนี้ไม่ต้องตีความ ซึ่งข้อมูลที่เกิดจากผลทางเทคนิคแสดงให้เห็นว่าเป็นข้อมูลที่อ่อนไหวที่ได้รับรองให้ความคุ้มครองในกรณีพิเศษ

---

[1] โปรดดู ประเด็นที่หนึ่ง จากข้อ 3.2.4 ในหน้าที่ 153

[2] โปรดดู ประเด็นที่หนึ่ง จาก ข้อ 3.3.4 ในหน้าที่ 192

ในกรณีสหพันธ์รัฐสาธารณรัฐเยอรมนี[3] คำจำกัดความข้อมูลส่วนบุคคลของ (BDSG) ได้บัญญัติคำนิยามศัพท์ โดยเฉพาะการอ้างอิงถึงสิ่งบ่งชี้ตัวตนของลักษณะทางพันธุกรรมของบุคคล ถูกบัญญัติให้อยู่ในหมวดข้อมูลประเภททั่วไป แต่อย่างไรก็ตาม (BDSG) ได้มีการบัญญัติข้อมูลทางพันธุกรรม และข้อมูลไบโอเมตริกซ์ให้เป็นข้อมูลที่มีความอ่อนไหวได้ถูกบัญญัติให้จำแนกออกจากข้อมูลส่วนบุคคลทั่วไป ที่เกิดจากการประมวลผลทางเทคนิคในการยืนยันตัวตนของบุคคลที่เกี่ยวข้องกับลักษณะทางกายภาพที่สามารถบ่งชี้อัตลักษณ์ของแต่ละบุคคลออกจากบุคคลอื่น ซึ่งมีความส่งเสี่ยงสูงที่จะถูกละเมิด จึงถูกบัญญัติให้ได้การคุ้มครองในหมวดหมู่ประเภทข้อมูลพิเศษตาม Section 48 และตามคำนิยามของ Section 46

สาธารณรัฐสิงคโปร์[4] ในการให้คำจำกัดความของข้อมูลส่วนบุคคล (Personal Data Protection Act 2012: PDPA) ได้บัญญัติคำนิยามศัพท์ “ข้อมูลส่วนบุคคล” ได้ให้การคุ้มครองเป็นการทั่วไป ซึ่งเป็นที่น่าสังเกตในการคุ้มครองข้อมูลส่วนบุคคลเกี่ยวกับผู้ที่ถึงแก่กรรมภายใน 10 ปี ถูกบัญญัติให้การคุ้มครองเมื่อพิจารณาแล้ว มีความแตกต่างจากสหภาพยุโรปที่มิได้ให้ความคุ้มครองผู้ที่ถึงแก่กรรม และมิได้คุ้มครองข้อมูลส่วนบุคคลเกี่ยวกับการติดต่อทางธุรกิจอันเป็นข้อยกเว้นของ (PDPA) แม้ว่าจะเป็นข้อมูลเกี่ยวกับบุคคล ซึ่งมิใช่เพื่อวัตถุประสงค์เป็นการส่วนตัว เว้นแต่ จะได้ระบุไว้อย่างชัดเจน (PDPA) ได้ถูกบัญญัติคำนิยามศัพท์ไว้กว้าง ๆ โดยมิได้มีการบัญญัติ “ข้อมูลพันธุกรรม” และ“ข้อมูลไบโอเมตริกซ์” ซึ่งเป็นข้อมูลที่มีความละเอียดอ่อนไว้ในพระราชบัญญัติฉบับนี้แต่อย่างใด แต่อย่างไรก็ตาม ข้อมูลไบโอเมตริกซ์ที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ที่ถูกใช้ในระบบของธุรกรรมต่าง ๆ เช่น ธนาคาร การใช้สมาร์ทโฟน เป็นต้น โดยมาตรฐานของสาธารณรัฐสิงคโปร์ให้ความคุ้มครองข้อมูลไบโอเมตริกซ์ย่อมไม่แตกต่างไปจากข้อมูลส่วนบุคคลประเภทอื่น ๆ

เพราะฉะนั้น เมื่อเปรียบเทียบกับคำนิยามของสหภาพยุโรป ซึ่งเป็นกลุ่มประเทศที่ใช้กฎระเบียบในการตรากฎหมายที่ให้การยินยอมกันทั่วโลกในการคุ้มครองข้อมูลส่วนบุคคลของ Regulation (EU) 2016/679 และ Regulation (EU) 2018/1725 โดยกฎหมายทั้งฉบับนี้มีความเหมือนกันในการให้การคุ้มครอง “ข้อมูลพันธุกรรม”และ“ข้อมูลไบโอเมตริกซ์” เป็นข้อมูลที่อ่อนไหวง่ายโดยบัญญัติจำแนกไว้อย่างชัดเจน เพื่อไม่เกิดการตีความในทางปฏิบัติแก่ผู้ควบคุม ผู้ประมวลผล และเจ้าของข้อมูล รวมทั้งข้อมูลที่ให้การคุ้มครองในหมวดหมู่ประเภทข้อมูลพิเศษห้ามมิให้ประมวลผล โดยมิได้รับการยินเป็นลายลักษณ์อักษรจากเจ้าของข้อมูลก่อน หรือ เว้นแต่

---

[3] โปรดดูประเด็นที่หนึ่ง จากข้อ 3.4.2 ในหน้าที่ 212

[4] โปรดดูประเด็นที่หนึ่ง จากข้อ 3.5.2 ในหน้าที่ 226

กฎหมายให้อำนาจ หากมีการละเมิดข้อมูลดังกล่าวข้างต้น โดยบัญญัติโทษไว้ค่อนข้างสูงในความเสียหายนั้น ๆ โดยเฉลี่ยค่าปรับร้อยละ 4 ของประกอบการรายได้ทั่วโลก หรือ 20 ล้าน ยูโร

ดังนั้น เมื่อพิจารณาตามมาตรา 6 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 มิได้มีการบัญญัติ “ข้อมูลพันธุกรรม”และ“ข้อมูลไบโอเมตริกซ์” ไว้ในหมวดของคำนิยามศัพท์ และจำแนกประเภทข้อมูลที่อ่อนไหวง่ายให้การคุ้มครองในกรณีพิเศษ เพื่อมิให้เกิดการตีความในทางปฏิบัติอย่างครอบคลุมและชัดเจน ในการให้คำจำกัดคำนิยามศัพท์ แต่ถูกบัญญัติเป็นข้อห้ามประมวลผลตามมาตรา 26[5] หรือเว้นแต่กฎหมายอนุญาตให้กระทำได้ ผู้วิจัยจึงเห็นสมควรให้มีการบัญญัติ “ข้อมูลพันธุกรรม”และ“ข้อมูลไบโอเมตริกซ์” จำแนกออกจากข้อมูลทั่วไป และให้ความคุ้มครองข้อมูลในหมวดพิเศษต่างหาก ซึ่งข้อมูลประเภทนี้ได้ใช้กันอย่างแพร่หลาย โดยเฉพาะยุคสมาร์ทโฟนได้เป็นส่วนหนึ่งของชีวิตประจำวัน ดังนั้น “ข้อมูลพันธุกรรม” และ “ข้อมูลไบโอเมตริกซ์” จึงเป็นข้อมูลที่อ่อนไหวที่ต้องจัดอยู่ในหมวดหมู่ข้อมูลประเภทพิเศษ ควรถูกบัญญัติเพิ่มเติมไว้ในมาตรา 6 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 เนื่องจาก (Biometrics) เป็นข้อมูลความเฉพาะตัว และ“อ่อนไหวง่าย” หากทำการจัดเก็บไม่ได้มาตรฐาน และมีการรั่วไหลของข้อมูลจะทำให้บุคคลผู้เป็นเจ้าของข้อมูลนั้นเสียหาย “ตลอดชีวิต” เพราะ (Biometrics) เป็นข้อมูลที่เปลี่ยนแปลงแก้ไขไม่ได้ จึงควรบัญญัติคำนิยามศัพท์ไว้ให้ชัดเจน ในการคุ้มครองข้อมูลส่วนบุคคลตามหลักสากลและการพัฒนาทางเศรษฐกิจของประเทศไทย

4.2 วิเคราะห์หลักการความยินยอม (Consent) และการถอนความยินยอม ของข้อมูลไบโอเมตริกซ์ (Biometrics)

หลักการขอความยินยอม และการถอนความยินยอมตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 มาตรา 19 วรรคสอง ในการให้ความยินยอม “ข้อมูลส่วนบุคคล” จากเจ้าของข้อมูลส่วนบุคคล กฎหมายได้เปิดช่องไว้ว่า หากโดยสภาพไม่อาจขอความยินยอมโดยการทำเป็นหนังสือ หรือ ทำผ่านระบบอิเล็กทรอนิกส์ได้ อาจขอความยินยอมด้วยวิธีการอื่นได้ โดยบัญญัติคำว่า “โดยสภาพไม่อาจขอความยินยอม” หมายความว่าอย่างไร หรือเป็นในกรณีผู้ควบคุมข้อมูลพยายามติดต่อขอความยินยอมโดยวิธีการที่กฎหมายกำหนดแล้ว แต่ยังไม่สามารถขอความยินยอมจากเจ้าของข้อมูลได้ หรืออาจเพราะว่าช่องทางการติดต่อที่เจ้าของข้อมูลให้ไว้ไม่อัพเดทอีกต่อไป หรือเป็นกรณีที่เจ้าของข้อมูลมิได้ให้ความสนใจที่จะให้ความยินยอม และความยินยอมนั้นยังจำเป็นต่อผู้ให้บริการอยู่หรือไม่ หากผู้ควบคุมข้อมูลสามารถที่จะกำหนดระยะเวลาอันสมควรให้เจ้าของข้อมูลตอบกลับ และหากไม่มีการตอบกลับภายในระยะเวลาดังกล่าวให้ถือว่า

[5] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562.

เป็นการให้ความยินยอม“โดยปริยายได้หรือไม่” เมื่อไม่สามารถขอความยินยอมได้การให้บริการดังกล่าวนั้น ก็อาจจะต้องหยุดชะงักลง ซึ่งส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลมากกว่า อาจส่งผลให้เกิดปัญหาการตีความว่า เงื่อนไขความยินยอมตามที่กฎหมายกำหนดให้ต้องขอความยินยอมก่อน หรือเป็นการความยินยอมโดยปริยายหรือไม่ หากพิจารณาเปรียบเทียบตามหลักกฎหมายต่างประเทศและประเทศไทย ในการความยินยอมและการถอนความยินยอมของข้อมูลทั่วไปและ“ข้อมูลพันธุกรรม และ ข้อมูลไบโอเมตริกซ์” การให้ความยินยอมจึงมีความสำคัญมากในด้านกฎหมายโดยเฉพาะอย่างยิ่งในบริบทของการปกป้องข้อมูลส่วนบุคคล เมื่อเก็บรวบรวมข้อมูลส่วนบุคคลต้องได้รับการแจ้งความยินยอมอย่างชัดเจนก่อนเสมอ ซึ่งต้องได้รับการยินยอมจากเจ้าของข้อมูล โดยต้องมีการยอมรับเป็นลายลักษณ์อักษรเพื่อเก็บไว้ใช้เป็นหลักฐาน ไม่ว่าจะเป็นในรูปแบบของกระดาษ เอกสาร หรือผ่านทางระบบอิเล็กทรอนิกส์ ดังต่อไปนี้

ประเด็นปัญหาการยินยอมทางอิเล็กทรอนิกส์ (Electronic consent)[6] เป็นการให้ความยินยอมด้วยลายเซ็นที่อยู่ในรูปแบบอิเล็กทรอนิกส์โดยบุคคล เช่น Cookies History Password เพื่อเป็นการยืนยัน หรือลงนามในเอกสารอิเล็กทรอนิกส์ โดยใช้สัญลักษณ์ได้แก่ รูปภาพ ใบหน้า ลายนิ้วมือ หรือการพิมพ์ชื่อด้วยคีย์บอร์ดที่ผู้ใช้สามารถเห็นได้ง่าย ทำให้ทราบได้ว่าใครเป็นเจ้าของลายเซ็น ซึ่งลายเซ็นนี้แสดงให้บุคคลเห็นว่า ใครเป็นคนลงนามในเอกสาร และยืนยันว่าบุคคลนั้นเห็นด้วยกับข้อกำหนด หรือสิ่งใดก็ตามที่เขียนลงในเอกสาร แล้วยินยอมด้วยการคลิก “I agree” ใน Electronic form ต่าง ๆ เป็นต้น จะต้องมิใช่การยินยอมล่วงหน้า

ดังนั้น เมื่อทำการคลิก “I agree หรือ Ok” จึงถือได้ว่าบุคคลนั้นได้อ่านและเข้าใจเนื้อหาของคำร้องขอฉบับดังกล่าวนี้อย่างละเอียดแล้ว และยืนยันว่าข้อมูลต่าง ๆ ที่ได้แจ้งให้ทราบว่านั้นเป็นความจริง ถูกต้อง เข้าใจดีว่าการตรวจสอบเพื่อยืนยันอำนาจตัวตน และถิ่นที่อยู่นั้น อันเป็นการจำเป็นอย่างยิ่งเพื่อให้การดำเนินการอนุญาตให้เข้าถึง การทำสำเนา หรือการเปิดเผยการได้มาของข้อมูลเป็นไปได้อย่างถูกต้องครบถ้วน จึงถือได้ว่าเป็นการลงนามในเอกสารอิเล็กทรอนิกส์

ลายมือชื่ออิเล็กทรอนิกส์ คือ การระบุตัวตนของเจ้าของลายเซ็น ที่แสดงถึงการยินยอม และ การรับรู้ข้อความบนเอกสารนั้น ๆ เหมือนกับลายเซ็นในรูปเอกสารที่เป็นกระดาษ แต่สิ่งที่แตกต่างออกไปก็ตรงที่ลายเซ็นนี้เป็นการสร้างขึ้นด้วยระบบอิเล็กทรอนิกส์ กล่าวคือ ถูกสร้างขึ้นด้วยคอมพิวเตอร์ ไม่ได้ถูกเซ็นด้วยปลายปากกาที่ประทับตราอยู่บนแผ่นกระดาษด้วยรอยหมึก

---

[6] โปรดดูในหน้าที่ 227

(Paper - based form) นั้น ซึ่งเอกสารในรูปของแผ่นกระดาษเป็นการยากต่อการแก้ไข และการจัดเก็บที่ยากกว่าในรูปแบบของเอกสารอิเล็กทรอนิกส์[7]

ข้อแตกต่าง ของการลงลายมือชื่ออิเล็กทรอนิกส์นี้ คือ สามารถเซ็นเอกสารในเวลาใด หรือสถานที่ไหนก็ได้ อีกทั้งยังไม่ต้องเปลืองกระดาษในการปริ้นท์ออกมาให้ยุ่งยาก สามารถส่งเอกสารกันได้ทางอีเมล์ซึ่งมีความรวดเร็ว เพื่อใช้ในการยืนยันเรื่องสำคัญต่าง ๆ ได้หลายเรื่อง เช่น เรื่องการยินยอมให้แก้ไขข้อมูลสินค้าที่ผู้ใช้เลือกไว้ เป็นต้น แต่ลายมือชื่ออิเล็กทรอนิกส์จะสามารถอ้างอิง และ มีความน่าเชื่อถือมากพอว่าลายมือชื่อนั้น ๆ ถูกสร้างขึ้นโดยเจ้าของตัวจริงหรือไม่ เช่น การเข้าระบบเพื่อเซ็น มีความหนาแน่นมากน้อยแค่ไหน หรือผู้อื่นสามารถแอบแฝงได้ง่ายหรือไม่ ถ้าหากระบบนั้นมีความน่าเชื่อถือจริง การรับรองได้ว่าลายมือชื่อนี้เป็นของเจ้าตัวแน่นอนก็สามารถใช้ในทางกฎหมายได้ ดังนั้น ลายมือชื่ออิเล็กทรอนิกส์เหมือนกับลายเซ็นกระดาษ และใช้อ้างอิงในทางกฎหมายได้ โดยลายเซ็นอิเล็กทรอนิกส์สามารถมีส่วนประกอบดังต่อไปนี้

1. การจับภาพของอินเทอร์เน็ต 2. การตรวจสอบข้อมูล 3. วิธีการลงนาม 4. การตรวจสอบผู้ใช้โดยบัญชีผู้ใช้งานทั้งบัญชีหลัก และบัญชีย่อย มีสิทธิในการเข้าถึงข้อมูลได้ต้องรักษารหัสทั้ง Login และ Password ให้เป็นความลับแต่เพียงผู้เดียวและห้ามมิให้ส่งต่อ หรือให้ผู้อื่นกระทำการ Login เข้าระบบโดยเด็ดขาด ทางผู้ควบคุม จะถือว่าผู้ที่สามารถใช้ Login และ Password เข้าใช้งานได้นั้นก็คือ เจ้าของบัญชีเท่านั้น หลังจากใช้งานเสร็จก็ควรทำการ Logout ออกจากระบบทุกครั้ง เพื่อความปลอดภัย และควรตั้งค่า Browser ไม่ให้จดจำ ในการ Login และ Password ประวัติ (History) และข้อมูลคุกกี้ (Data Cookies) โดยปกติคุกกี้จะถูกใช้เพื่อจัดเก็บข้อมูลเล็ก ๆ ไว้ในเบราว์เซอร์ ข้อมูลที่ถูกส่งจากเว็บเซิร์ฟเวอร์เซอร์ ซึ่งจะถูกส่งกลับมายังเว็บเซิร์ฟเวอร์ทุกครั้งที่เว็บเบราว์เซอร์ร้องขอข้อมูล ซึ่งปกติคุกกี้ เพื่อให้เว็บเซิร์ฟเวอร์สามารถจดจำสถานการณ์ใช้งานของเว็บเบราว์เซอร์ที่มีต่อเว็บเซิร์ฟเวอร์ เช่น คุกกี้ (Data Cookies) เพื่อจดจำชื่อบัญชีผู้ใช้เวลาที่ผู้ใช้เข้าเว็บเซิร์ฟเวอร์ที่เป็นเวลาเข้าเว็บครั้งล่าสุด ที่ผู้ใช้เลือกรายการไว้ ข้อมูลในคุกกี้ดังกล่าวนี้ สามารถจดจำเว็บไซต์ผู้ใช้ได้ คือ กระบวนการจัดเก็บข้อมูลและการประมวลผลข้อมูลของผู้ใช้บริการ เพื่อความปลอดภัยในการใช้งาน ซึ่งถือเป็นความรับผิดชอบของผู้ใช้งาน

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (General Data Protection Regulation) ไม่จำเป็นต้องได้รับความยินยอมในรูปแบบใด ๆ โดยเฉพาะตราบใดที่มีการแจ้งความยินยอมก่อนและการให้ข้อมูลเป็นที่ยอมรับได้ โดยให้ความสำคัญมากในการตรวจสอบให้แน่ใจว่าเอกสาร และเนื้อหาเว็บไซต์ทั้งหมดของบุคคลนั้น อธิบายถึงสิ่งที่ตั้งใจจะกระทำกับข้อมูลที่จะถูกรวบรวม เก็บ

---

[7] พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 แก้ไขเพิ่มเติม (ฉบับที่4) พ.ศ. 2562. มาตรา 26 ประกอบมาตรา 4.

เปิดเผยใช้ ซึ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ตามมาตรา 4 (1)[8] บัญญัติให้ข้อมูลส่วนบุคคลให้หมายความรวมถึงอัตลักษณ์ของบุคคล หรือสิ่งที่สามารถทำให้ระบุตัวตนในทางออนไลน์ได้ด้วย (Online identifier)[9] ข้อมูลออนไลน์ เช่น cookies IP address ข้อมูลพิกัด GPS ซึ่งในส่วนอารัมภบท ข้อที่ 30 ของ (GDPR) ได้ให้คำอธิบายเพิ่มเติมไว้ว่า บุคคลธรรมดาอาจเชื่อมโยงกับตัวตนออนไลน์ที่จัดเตรียมโดยอุปกรณ์ หรือแอพพลิเคชั่น และโปรโตคอล เช่น อินเทอร์เน็ตโปรโตคอล ตัวระบุคุกกี้ (Cookie identifiers) หรือตัวระบุอื่น ๆ โดยสิ่งนี้อาจทิ้งร่องรอยดิจิทัลไว้ (Digital footprints) และโดยเฉพาะอย่างยิ่งอัตลักษณ์ของบุคคลที่ใช้ระบุตัวตนและข้อมูลอื่น ๆ ที่ได้รับจากเซิร์ฟเวอร์ อาจถูกใช้เพื่อสร้างโปร์ไฟล์ของบุคคลได้และสามารถใช้ระบุตัวบุคคลได้

ดังนั้น คุกกี้ (Cookies) ตามกฎหมาย (GDPR) จึงเป็นส่วนหนึ่งของข้อมูลส่วนบุคคลที่ได้รับการคุ้มครองในการกระทำต่อข้อมูลส่วนบุคคลดังกล่าว จึงต้องได้รับความยินยอมก่อนโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลด้วย โดยผู้ให้ความยินยอมจะต้องมีการกระทำที่แสดงออกในการให้ความยินยอมด้วยตาม (Affirmative action) อารัมภบทข้อ 32 และ 42 ประกอบมาตรา 7 (2) หลักการความยินยอม (Consent) มีกฎเกณฑ์พื้นฐานอยู่ 7 ประการ สำหรับระบบรักษาความปลอดภัยข้อมูลไบโอเมตริกซ์ เช่น เอกลักษณ์ ความเป็นสากล ความคงทน การรวบรวม ประสิทธิภาพ การยอมรับ และการหลีกเลี่ยง ที่จะเป็นพื้นฐานในการให้ความยินยอมใน การเก็บ รวบรวม เปิดเผย ใช้ ลบ หรือทำลาย ข้อมูลส่วนบุคคลดังกล่าว จึงเป็นเรื่องละเอียดอ่อนหากมีการละเมิดใด ๆ ในระบบข้อมูลที่จัดเก็บข้อมูลไบโอเมตริกซ์สามารถนำไปสู่ผลกระทบร้ายแรงและผู้ใช้อาจสูญเสียเอกลักษณ์ไบโอเมตริกซ์อย่างถาวร การปฏิบัติตามกฎหมายนั้นขึ้นอยู่กับการได้รับความยินยอมจากเจ้าของข้อมูลก่อน ผู้เป็นเจ้าของข้อมูลส่วนบุคคลนั้น จึงควรพิจารณาดังนี้

1. หลักความเหมาะสมในการเก็บข้อมูล หมายถึง การเก็บรวบรวมข้อมูลต้องได้รับความยินยอมและมีบอกกล่าวถึงวัตถุประสงค์ในการนำข้อมูลไปใช้จากเจ้าของข้อมูลก่อนเสมอ (หลัก Consent)

2. หลักข้อจำกัดในการนำไปใช้หมายถึง ข้อมูลส่วนบุคคลจะต้องไม่ถูกนำไปเปิดเผยเกินจากขอบวัตถุประสงค์ที่ได้ขอความยินยอมจากเจ้าของข้อมูล เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูล หรือเป็นไปตามบทบัญญัติของกฎหมาย

ความยินยอมจากผู้ให้ข้อมูลต้องการประกาศเป็นลายลักษณ์อักษรที่เกี่ยวข้องในการให้ความยินยอมและเรื่องอื่น ๆ คำขอความยินยอมจะต้องนำเสนอในลักษณะที่เห็นได้ชัดเจนจากเรื่อง

---

[8] Regulation (EU) 2016/679 และ Regulation (EU) 2018/1725

[9] โปรดดูในบทที่ 3 ในหน้าที่ 147

อื่น ๆ ในรูปแบบที่เข้าใจได้และเข้าถึงได้ง่าย โดยใช้ภาษาที่ชัดเจน หากส่วนหนึ่งส่วนใดของคำประกาศดังกล่าวไม่เกี่ยวข้องให้ถือเป็นการละเมิดกฎข้อบังคับไม่มีผลผูกพันตาม Regulation (EU) 2016/679 และ Regulation (EU) 2018/1725 ตามมาตรา 7 หลักการถอนความยินยอมของ Regulation (EU) 2016/679 และ Regulation (EU) 2018/1725 ตามมาตรา 7 (3) ได้จำแนกอย่างชัดเจนไว้ 6 ประการ[10]

ดังที่ผู้วิจัยได้วิเคราะห์ไว้ในบทที่ 3[11] ซึ่งในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 หลักในการถอนความยินยอมนั้น เจ้าของข้อมูลสามารถถอนความยินยอมได้ตลอดเวลา และง่ายในการถอนความยินยอม โดยผู้ควบคุมจะต้องแจ้งให้ทราบถึงสิทธินั้นก่อนที่จะให้ความยินยอมตาม GDPR มาตรา 7 ข้อ 3 โดยใช้คำว่า “ก่อน” ที่จะให้ความยินยอม ซึ่งจะเป็นเรื่องที่เข้าใจได้ง่ายที่จะถอนความยินยอม แต่ปรากฏว่า มาตรา 19 วรรคหก แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 ได้บัญญัติไว้ว่า “ในกรณีที่การถอนความยินยอมส่งผลกระทบต่อเจ้าของมูลส่วนบุคคลในเรื่องใด ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลทราบถึงผลกระทบจากการถอนความยินยอมนั้นก่อน” ดังนั้นหาก “ข้อมูลพันธุกรรม และ ข้อมูลไบโอเมตริกซ์” ซึ่งเป็นข้อมูลที่อ่อนไหว เมื่อได้ให้ความยินยอมไปก่อนหน้าแล้ว แต่ภายหลังมีเหตุที่จะถอนความยินยอมนั้น ผู้ควบคุมจะแจ้งให้ทราบก่อน หรือในขณะให้ความยินยอมให้ทราบผลกระทบที่จะเกิดขึ้นต่อข้อมูลส่วนบุคคลที่ได้ให้ความยินยอมไปแล้วนั้น เช่น กรณีเช่าหอพักได้ให้ความยินยอมข้อมูลไบโอเมตริกซ์ใช้กับระบบรักษาปลอดภัยของหอพัก แต่เนื่องเจ้าของข้อมูลได้ที่พักใหม่ราคาถูกว่าที่เดิม จึงขอยกเลิก แต่ปรากฏว่า ผู้ให้บริการแจ้งว่าต้องเสียค่าปรับเพราะได้ทำการบรรณทึกข้อมูลไบโอเมตริกซ์ไว้ในระบบแล้ว หากต้องการยกเลิกต้องชำระค่าปรับ ในขณะขอยกเลิก โดยมิได้แจ้งให้ทราบก่อน ซึ่งไม่เป็นธรรมแก่ผู้ใช้บริการ และเป็นการหลอกลวง หรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ดังกล่าว กรณีเช่นนี้จึงอาจจะต้องตีความว่าการกระทำเช่นนี้เป็นการแจ้งผลกระทบตอนไหนก็ได้หรือไม่ อย่างไร ผู้วิจัยจึงเห็นควรบัญญัติคำว่า “ก่อน” ถอนความยินยอมเพิ่มในมาตรา 19 วรรคหก เพื่อมิให้เกิดการตีความดังกล่าวในทางปฏิบัติจริง

จากหลักการความยินยอม (Consent)[12] และการถอนคำยินยอมข้อมูลส่วนบุคคล (Privacy Act 1994) ของสหรัฐอเมริกา โดยการกำหนดให้หน่วยงานของรัฐที่มีหน้าที่ดูแลระบบการบันทึกต้องยินยอมเจ้าของข้อมูลส่วนบุคคล โดยเจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึงข้อมูลตรวจสอบ

---

[10] โปรดดูในหน้าที่ 158 ประเด็นที่สอง

[11] โปรดดูในประเด็นที่สอง จากข้อที่ 3.3.4 ในหน้าที่ 194

[12] โปรดดูในประเด็นที่สอง จากข้อที่ 3.3.4 ในหน้าที่ 194

ความถูกต้องและขอสำเนาข้อมูลส่วนบุคคลของตนได้ และหน่วยงานของรัฐจะต้องพิจารณาและตอบรับคำขอของเจ้าของข้อมูลส่วนบุคคลภายใน 30 วันทำการ หากหน่วยงานของรัฐปฏิเสธคำขอนั้น หน่วยงานของรัฐจะต้องแจ้งเหตุผลในการปฏิเสธ และแจ้งหน่วยงานที่เจ้าของข้อมูลส่วนบุคคลสามารถอุทธรณ์คำสั่งได้ และพระราชบัญญัติคุ้มครองข้อมูลไบโอเมตริกซ์ (Biometric Information Privacy Act 2008 :BIPA) โดยบัญญัติให้ความยินยอมจะต้องแจ้งล่วงหน้าเป็นลายลักษณ์อักษรเกี่ยวกับการเก็บ รักษา เปิดเผย ใช้ การลบ การทำลายข้อมูลไบโอเมตริกซ์อย่างถาวร เมื่อไม่ประสงค์และไม่สามารถรับข้อมูลดังกล่าวได้ “การยินยอมโดยมิได้แจ้งล่วงหน้าเป็นลายลักษณ์อักษร” ตาม740 ILCS 10/15 (b) หากไม่ได้รับความยินยอมเป็นลายลลักษณ์อักษรล่วงหน้าก่อน และก็สามารถแสดงให้เห็นถึงการละเมิดนั้นได้ที่จะนำคดีขึ้นสู่ศาล แม้ว่าเจ้าของข้อมูลจะไม่ได้รับผลกระทบหรือไม่ จากการที่ไม่แจ้งผลกระทบการถอนความยินยอมก่อนดังกล่าวนั้นก็ตาม

จากหลักการความยินยอม (Consent)[13] และการถอนความยินยอมข้อมูลไบโอเมตริกซ์ Federal Data Protection Act 2018 (BDSG) ได้บัญญัติหลักการให้ความยินยอมในการประมวลผลข้อมูลส่วนบุคคลจะต้องได้รับ “การแจ้งก่อนให้ความยินยอม” ไว้โดยเฉพาะเจาะจงชัดเจนและไม่คุมเครือเป็นลายลักษณ์อักษรต้องเป็นไปตามวัตถุประสงค์ของเจ้าข้อมูลที่เกี่ยวข้องกับผู้ให้ความยินยอมนั้นตาม (BDSG) Section 51โดยเป็นตามข้อบังคับของ ของ Regulation (EU) 2016/679 และ Regulation (EU) 2018/1725 ตามมาตรา 7 ข้อ 3

จากหลักการความยินยอม (Consent)[14] และการถอนความยินยอมของสาธารณรัฐสิงคโปร์ตามพระราชบัญญัติ Personal Data Protection Act 2012 (PDPA) ในการประมวลผลข้อมูลส่วนบุคคล หรือ เก็บ รวบรวม ใช้ เปิดเผย ลบ หรือ ทำลาย จะต้องได้รับความยินยอมจากเจ้าของข้อมูล “ก่อนดำเนินการใด ๆ” และเจ้าของข้อมูลสามารถปฏิเสธ หรือยกเลิกความยินยอมได้ ซึ่งองค์กรไม่อาจกำหนดให้การให้ความยินยอมเป็นเงื่อนไข เกินกว่าความสมเหตุสมผลต่อการให้บริการนั้น ๆได้

เพราะฉะนั้น เมื่อเปรียบเทียบการขอความยินยอมทั้ง 4 ประเทศแล้วจะเห็นได้ว่าหากเจ้าของข้อมูลส่วนบุคคลมีความประสงค์ที่จะถอนข้อมูลของตน ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องทำการแจ้งผลกระทบในการถอนข้อมูลดังกล่าว “ก่อนล่วงหน้าที่จะให้ความยินยอม” นั้นจึงแสดงให้เห็นว่าทั้ง 4 ประเทศ ได้มีการบัญญัติคำว่า “ก่อน” ถอนความยินยอม เพื่อให้ทราบถึงผลกระทบที่จะเกิดขึ้นกับเจ้าข้อมูลเมื่อถอนความยินยอมดังกล่าว แต่พระราชบัญญัติคุ้มครองข้อมูล

---

[13] โปรดดูในประเด็นที่สอง จากข้อที่ 3.4.2 ในหน้าที่ 212

[14] โปรดดูใน ประเด็นที่สอง จากข้อที่ 3.5.2 ในหน้าที่ 226

ส่วนบุคคล พ.ศ. 2562 มาตรา 19 วรรคหก ดังกล่าวนี้ มิได้บัญญัติคำว่า“ก่อน” ถอนความยินยอมไว้ให้ชัดแจ้งแต่อย่างใด หากเกิดกรณีละเมิดขึ้นกับ “ข้อมูลพันธุกรรม และ ข้อมูลไบโอเมตริกซ์” ที่เป็นข้อมูลที่อ่อนไหว เมื่อได้ให้ความยินยอมไปก่อนหน้าแล้ว แต่ภายหลังมีเหตุที่จะถอนความยินยอมนั้น เช่น การใช้ข้อมูลเกินความจำเป็น โดยการยินยอมให้ใช้ทั้งลายนิ้วมือ ม่านตา รูปทรงใบหน้า เป็นต้น ย่อมอาจเกิดผลกระทบที่ไม่พึงประสงค์แก่เจ้าของข้อมูลได้ ว่าต้องแจ้งก่อน หรือภายหลังก็ได้ ดังนั้น ผู้วิจัยเห็นควรบัญญัติคำว่า “ก่อน” ถอนความยินยอมเพิ่มในมาตรา 19 วรรคหก เพื่อความชัดเจนและเป็นประโยชน์ในทางปฏิบัติทั้งสองฝ่าย

4.3 วิเคราะห์ผู้ควบคุม ผู้ประมวลผล ผู้ใช้บริการในการบังคับใช้กฎหมายโดยเฉพาะอย่างยิ่งระยะเวลาในการเก็บ รักษาข้อมูลไบโอเมตริกซ์ (Biometrics)

ตามหลักสิทธิที่จะถูกลืม (Right to be forgotten) ภายหลังที่ลบอาจยังมีข้อมูลค้างอยู่ในระบบ (Digital footprint) การเก็บรักษาข้อมูลส่วนบุคคลเป็นส่วนที่สำคัญในการทำงานของระบบไบโอเมตริกซ์ เช่น ระบบสมาร์ทโฟน ซึ่งเป็นข้อมูลของผู้ใช้บริการที่อยู่ในระบุที่มีขนาดใหญ่ เช่น คอมพิวเตอร์คลาวด์ หรือไอคลาวด์ ที่มีพื้นที่มากกว่าในระบบของผู้ใช้บริการแบบหลายคนที่สามารถเชื่องโยงไปยังฐานข้อมูลได้มากและสะดวก จึงมีความจำเป็นที่จะต้องมีชุดของข้อมูลส่วนบุคคลหลายชุด และยิ่งไปกว่านั้น การเฝ้าระวังในการเชื่อมโยงฐานข้อมูลส่วนบุคคลที่สามารถบ่งชี้ถึงตัวบุคคลนั้นได้ อันเป็นเป้าหมายของระบบที่กำหนดจะต้องเก็บข้อมูลส่วนตัวของบุคคลนั้นเพื่อความปลอดภัยไว้ในระบบแบบไบโอเมตริกซ์ตามที่นิยามไว้ในข้างต้น

โดยระบบจะบันทึกไว้ในฐานระบบที่มีความน่าเชื่อ ในการเก็บข้อมูลไบโอเมตริกซ์ให้ปลอดภัยได้มากที่สุด แต่อย่างไรก็ตาม ก็ยังสามารถคุกคามความเป็นส่วนตัวของแต่ละบุคคลได้ผ่าน “การประมวลผลข้อมูลที่ผิดวิธีและการเชื่อมโยงฐานข้อมูลผ่านฐานข้อมูลไบโอเมตริกซ์” ตั้งข้อสังเกตว่า การเก็บรักษาข้อมูลส่วนบุคคลมีผลกระทบโดยตรงต่อผลประโยชน์ส่วนตัวของแต่ละบุคคล โดยไม่คำนึงว่าการใช้ข้อมูลในครั้งต่อไปจะเกิดขึ้นหรือไม่ โดยเฉพาะอย่างยิ่งการพิจารณาในการเก็บข้อมูลส่วนบุคคลขึ้นอยู่กับผู้ให้บริการเท่านั้น ข้อสรุปนี้ ขัดแย้งกับความต้องการของฐานข้อมูลในระบบมิใช่มีแต่ข้อมูลทั่วไปเท่านั้นยังครอบถึงข้อมูลไบโอเมตริกซ์ ด้วย

การจำแนกประเภทของข้อมูลไบโอเมตริกซ์ และระยะเวลาที่เก็บข้อมูลนั้น ซึ่งเป็นปัจจัยที่มีผลต่อการอนุญาตให้ใช้ “ข้อมูลพันธุกรรม และ ข้อมูลไบโอเมตริกซ์” ที่จะยืนยันว่าการเก็บข้อมูลดังกล่าว จะไม่เป็นปัญหาภายในขอบเขตของสิทธิในความเป็นส่วนตัว การเก็บรักษา ใช้ เปิดเผย ลบ หรือทำลายข้อมูลไบโอเมตริกซ์ ซึ่งสามารถทำให้เกิดการรบกวนกับสิทธิความเป็นส่วนตัวได้ รวมทั้ง สิทธิที่จะถูกลืม (Right to be forgotten) เพื่อให้ข้อมูลส่วนบุคคลของเจ้าข้อมูล

ถูกลบเลือน หรือลืมไปเสียจากระบบโลกออนไลน์ โดยการแจ้งเป็นลายลักษณ์ จึงเป็นแนวคิดที่สอดคล้องกับข้อเท็จจริงในการพัฒนาทางเทคโนโลยีในปัจจุบัน เนื่องจากสถานการทางสังคมเปลี่ยนแปลงไปสู่ยุคสังคมข้อมูลข่าวสาร(Information society) ซึ่งข้อมูลจำนวนมหาศาล (Big data) ที่อยู่ในโลกออนไลน์มีแนวโน้มที่จะถูกรวบรวม (Collected) จัดเก็บ (Stored) และประมวลผล (Processed) อย่างต่อเนื่อง และอัตโนมัติบนเครือข่ายอินเตอร์เน็ตที่สามารถสืบค้นได้ง่าย (Searchable) ด้วยเหตุนี้ ด้วยความมีอยู่ของข้อมูลดังกล่าวอาจก่อทั้งผลดี และอาจจะส่งผลเสียแก่เจ้าของข้อมูล แนวโน้มข้อกังวลเกี่ยวกับการประมวลผลข้อมูลไบโอเมตริกซ์ในระบบออนไลน์จะกระทำอย่างไรให้ข้อมูลส่วนบุคคลนี้ถูกจดจำในระบบออนไลน์น้อยที่สุดและสิ่งใดบ้างที่ควรถูกลบเลือนไป (how to remember less and what should be forgotten) ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 หรือไม่ อย่างไรโดยการเปรียบเทียบกับต่างประเทศ ดังต่อไปนี้

กฎหมาย (GDPR) Article 17 วรรคหนึ่ง (a) ถึง (f)[15] ได้กำหนดถึงเหตุที่เจ้าของข้อมูลส่วนบุคคลอาจเรียกร้องให้ผู้ประมวลผลข้อมูลลบข้อมูลส่วนบุคคลของตนเสียไว้อย่างละเอียดและชัดเจนยิ่งขึ้น อาทิ ข้อมูลส่วนบุคคลดังกล่าวไม่มีความจำเป็นต่อการประมวลผลอีกต่อไป ผู้เป็นเจ้าของข้อมูลส่วนบุคคลได้ยกเลิกความยินยอมที่เคยได้ให้ไว้สำหรับการประมวลผลข้อมูล และเจ้าของข้อมูลส่วนบุคคลได้คัดค้านการประมวลผลข้อมูลนั้น และไม่มีเหตุอันชอบด้วยกฎหมายอื่น ๆ ที่ได้รับความคุ้มครองเหนือกว่าสำหรับการประมวลผลข้อมูลต่อไป ข้อมูลส่วนบุคคลนั้นถูกประมวลผลโดยมิชอบด้วยกฎหมาย หรือมีความจำเป็นต้องถูกลบประวัติเพื่อให้เป็นไปตามที่กฎหมายบัญญัติ รวมตลอดถึงกรณีที่ข้อมูลส่วนบุคคลเกี่ยวกับเยาวชนที่ถูกจัดเก็บโดยผู้ให้บริการสังคมข้อมูลข่าวสาร (Information society services) ยิ่งกว่านั้น Article 17 วรรคสอง ของ (GDPR) ยังได้กำหนดมาตรการใหม่เพื่อให้การใช้ (Right to be forgotten) ให้มีประสิทธิผลมากยิ่งขึ้นนั้น โดยกำหนดหน้าที่ให้ผู้ประมวลผลข้อมูล เมื่อได้รับคำร้องขอจากเจ้าของข้อมูลส่วนบุคคลให้ลบข้อมูลข้อมูลส่วนบุคคล จะต้องดำเนินการแจ้งผู้ประมวลผลข้อมูลรายอื่น ๆ ที่ประมวลผลข้อมูลที่เกี่ยวข้องกับคำร้องขอนั้น ให้ดำเนินการลบ link สำเนา หรือ ผลลัพธ์ที่เกี่ยวกับข้อมูลส่วนบุคคลดังกล่าวนั้นด้วย ทั้งนี้ โดยพิจารณาความเป็นไปได้ในทางเทคโนโลยี และต้นทุนค่าใช้จ่ายตามสมควรแก่กรณี

มาตรการใหม่นี้ แม้มีข้อบกพร่องในประเด็นตรงที่ยังไม่มีการกำหนดสภาพบังคับแก่ผู้ประมวลผลข้อมูลรายอื่น ๆ ที่ได้รับแจ้งการร้องขอลบข้อมูลส่วนบุคคลจากผู้ประมวลผลข้อมูลรายแรก ให้มีผลเสมือนเป็นการได้รับคำร้องจากเจ้าของข้อมูลส่วนบุคคลโดยตรง เพื่อให้กระบวนการยื่นคำร้องต่อผู้ประมวลผลข้อมูลทั้งหมดมีผลด้วยการยื่นคำร้องเพียงฉบับเดียว แต่ก็เป็นที่คาดการณ์กันว่า

---

[15] โปรดดูบทที่ 3 ในหน้าที่ 150

เมื่อพิจารณาประกอบกับหลักเกณฑ์ที่ชัดเจนว่าเจ้าของข้อมูลส่วนบุคคลสามารถร้องขอให้ลบข้อมูลส่วนบุคคลต่อผู้ประมวลผลข้อมูลได้เป็นการทั่วไปแล้ว ย่อมสามารถเพิ่มโอกาสให้เจ้าของข้อมูลส่วนบุคคลมีโอกาสได้รับการเยียวยาความเสียหาย โดยการลบข้อมูลส่วนบุคคลจากผู้ประมวลผลรายอื่นมากยิ่งขึ้น เช่น กรณีมีการร้องขอให้ Google ลบข้อมูลส่วนบุคคล โดยนัยของวรรคนี้ Google ย่อมต้องดำเนินการแจ้งไปยังเจ้าของ Webpage ที่ปรากฏร่องรอยดิจิทัลของผลการค้นหาทั้งหมด รวมตลอดจนผู้ให้บริการ Search engine รายอื่น เพื่อให้ทราบถึงคำร้องที่ Google ได้รับ และผลการตัดสินใจลบของ Google ย่อมเพิ่มความเป็นไปได้ที่ผู้ประมวลผลข้อมูลรายอื่นจะได้ทำการลบข้อมูลส่วนบุคคลในส่วนของตนตามแบบอย่างของ Google เพื่อหลีกเลี่ยงความรับผิดตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล หากเจ้าของข้อมูลส่วนบุคคลดำเนินการร้องขอต่อตนโดยตรงในภายหลัง

ในส่วนของข้อยกเว้นนั้น Article 17 วรรคสาม (a) ถึง (e) ของ (GDPR) ได้กำหนดข้อยกเว้นหน้าที่ของผู้ประมวลผลข้อมูลตามวรรคหนึ่งและวรรคสองไว้อย่างชัดเจนหลายประการ อาทิ เพื่อเป็นการใช้สิทธิในเสรีภาพในการแสดงความคิดเห็นและการเข้าถึงข้อมูลข่าวสาร (Right of freedom of expression and information) เพื่อให้เป็นไปตามหน้าที่ตามที่กฎหมายบัญญัติ หน้าที่เพื่อประโยชน์สาธารณะ หรือการดำเนินการในนามขององค์กรของรัฐ ซึ่งผู้ประมวลผลจะต้องประมวลผลข้อมูลต่อไป ยกเว้น เพื่อประโยชน์สาธารณะเพื่อวัตถุประสงค์ทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ ของ (GDPR) เท่านั้น

เงื่อนไขทั่วไปขึ้นอยู่กับความยินยอม และเป็นลายลักษณ์อักษรตาม Regulation (EU) 2016/679 และ Regulation (EU) 2018/1725 ที่ผู้ควบคุมจะกระทำการใดต้องกระทำด้วยความชอบภายใต้กฎหมายตามมาตรา 6 กรณีเกี่ยวข้องกับข้อมูลส่วนบุคคลพิเศษในการเชื่อมโยงระหว่างวัตถุประสงค์ที่มีการรวบรวมข้อมูลส่วนบุคคลและวัตถุประสงค์ของการประมวลผลประเภทข้อมูลอ่อนไหวเพิ่มเติมของ GDPR ตามมาตรา 9 ประเภทของข้อมูลที่อยู่ภายใต้การประมวลผล กลุ่มข้อมูลที่เกี่ยวข้องหน่วยงาน เพื่อวัตถุประสงค์ที่อาจเปิดเผยข้อมูลส่วนบุคคล,ข้อจำกัดวัตถุประสงค์ ระยะเวลาการเก็บรักษา การดำเนินการและขั้นตอนการประมวลผล รวมถึงมาตรการต่าง ๆ เพื่อให้มั่นใจว่าเป็นไปตามกระบวนการทางกฎหมายและเป็นธรรม เว้นแต่ การประมวลผลข้อมูลเฉพาะอื่น ๆ ที่กำหนดไว้ในมาตรา 9 ตามวัตถุประสงค์ของผลประโยชน์สาธารณะและเป็นไปตามวัตถุประสงค์ที่ถูกต้องตามกฎหมาย

กฎหมาย (GDPR) ได้จำแนกความแตกต่างระหว่างข้อมูลส่วนบุคคลที่ถูกรวบรวม และข้อมูลส่วนบุคคลที่ได้จากแหล่งอื่น ๆ ซึ่งผู้ควบคุมจะอยู่ภายใต้ข้อผูกพันในแจ้งข้อมูล “ภายในระยะเวลาที่เหมาะสมหลังจากได้รับข้อมูลส่วนบุคคล แต่ไม่เกินภายใน 1 เดือน โดยคำนึงถึงสถานการณ์เฉพาะที่ข้อมูลส่วนบุคคลถูกประมวลผล” ไม่ว่าในกรณีใด ๆ หากข้อมูลส่วนบุคคล

จะถูกใช้เพื่อจุดประสงค์ในการสื่อสารกับข้อมูลส่วนบุคคล หรือหากมีการเปิดเผยข้อมูลดังกล่าวไปยังบุคคลที่สามข้อมูลนั้น ผู้ควบคุมจะต้องแจ้งการให้ข้อมูลกับเรื่องข้อมูลก่อนการติดต่อครั้งแรกกับบุคคลนั้น หรือ บุคคลนั้นให้ไว้ก่อนที่จะมีการเปิดเผยตาม Regulation (EU) 2016/679 มาตรา 14 ข้อ 3 (a) Regulation (EU) 2018/1725 มาตรา 16 ข้อ 3 (a) การเก็บรักษาจำกัดแบบ โดยองค์กรต้องปฏิบัติตามระยะเวลาการเก็บข้อมูลที่จำเป็นและวิธีการเก็บรักษา เช่น ข้อมูลไบโอเมตริกซ์ดิบที่ใช้ในการสร้างแบบสำหรับไบโอเมตริกซ์เฉพาะและจะถูกลบ หรือทำลายทันทีที่มีการสร้างแบบไบโอเมตริกซ์ เมื่อมีการอนุญาตการเข้าถึงข้อมูลของบุคคลนั้นหยุดลง หรือถูกถอนออกแล้ว ข้อมูลบันทึกและข้อมูลระบุตัวตนจะถูกเก็บรักษาไว้นานตามที่ผู้ให้บริการได้ประกาศแจ้งไว้ก่อนให้ความยินยอมสำหรับการบันทึก แต่อาจถูกเก็บไว้ในโหมดเก็บถาวรหากกฎหมายกำหนดไว้เพื่อจุดประสงค์ในการโต้แย้งตามกฎหมายที่มีผลบังคับใช้

การแจ้งระยะเวลาเก็บรักษาข้อมูลส่วนบุคคล โดย (Privacy Act 1994)[16] ได้กำหนดให้หน่วยงานของรัฐต้องทำรายงานข้อมูลส่วนบุคคลเกี่ยวกับวัน เวลา ของข้อมูลบุคคล โดยจะต้องเก็บรายงานดังกล่าวไว้เป็นเวลา 5 ปี หรือ ตลอดอายุของบันทึก ถ้าระยะเวลาใดยาวกว่าให้ถือเอาระยะเวลานั้น พระราชบัญญัติคุ้มครองข้อมูลไบโอเมตริกซ์ (BIPA) โดยกำหนดให้องค์กรเอกชนที่ครอบครองข้อมูลไบโอเมตริกซ์ จะต้องมีนโยบายเป็นลายลักษณ์อักษรเกี่ยวกับวัตถุประสงค์เฉพาะและระยะเวลาที่จะทำการรวบรวมจัดเก็บและใช้ข้อมูลไบโอเมตริกซ์ โดยกำหนดให้ทำตารางการเก็บ รักษา รวบรวม เปิดเผย และแนวทางสำหรับทำลายข้อมูลอย่างถาวรเมื่อไม่ประสงค์ โดยจะต้องประกาศนโยบายและแจ้งล่วงหน้าเป็นตารางสำหรับองค์กรเอกชน ซึ่งจะต้องระบุรายละเอียดว่าจะเก็บข้อมูลอย่างไรและเมื่อใดจะถูกทำลายเมื่อไม่ประสงค์ ตาม 740 ILCS 14/15

พระราชบัญญัติคุ้มครองข้อมูลไบโอเมตริกซ์ของ (BIPA) กำหนดให้บริษัทที่อยู่ในความครอบครองข้อมูลไบโอเมตริกซ์ต้องมีมาตรการดังนี้

(1) มีนโยบายที่เป็นลายลักษณ์อักษรเปิดเผยต่อสาธารณชนจัดทำตารางเวลาการเก็บรักษาและแนวทางสำหรับการทำลายตัวระบุไบโอเมตริกซ์และข้อมูลไบโอเมตริกซ์อย่างถาวรตามข้อตกลง หรือ ภายใน 3 ปีนับจากการมีปฏิสัมพันธ์ครั้งสุดท้ายกับบุคคลใดก็ตามที่เกิดขึ้นก่อน

(2) ปฏิบัติตามนโยบายดังกล่าว

(3) ก่อนที่จะได้รับข้อมูลไบโอเมตริกซ์จะต้องแจ้งให้ผู้เข้าร่วมทราบว่าข้อมูลไบโอเมตริกซ์ที่กำลังจะถูกรวบรวม หรือจัดเก็บ หรือวัตถุประสงค์เฉพาะและระยะเวลาที่มีการรวบรวมจัดเก็บรวบรวม การใช้ข้อมูลไบโอเมตริกซ์ และดำเนินการยินยอมเป็นลายลักษณ์อักษร

---

[16] โปรดดูในบทที่ 3 ประเด็นที่สาม จากข้อที่ 3.3.4 ในหน้าที่ 192

โดย (BIPA) ยังห้ามมิให้ บริษัท ขายแลกเปลี่ยน หรือทำกำไรจากข้อมูลไบโอเมตริกซ์ของบุคคล เปิดเผย หรือเผยแพร่ข้อมูลดังกล่าว โดยไม่ได้รับความยินยอม เว้นแต่ กฎหมายอนุญาตให้กระทำได้

การแจ้งระยะเวลาเก็บรักษาข้อมูลส่วนบุคคลของ (BDSG)[17] โดยผู้ให้บริการ หรือ ผู้ควบคุมโดยการประมวลผลข้อมูลไบโอเมตริกซ์ไม่ว่าทั้งหมด หรือบางส่วนด้วยวิธีการอัตโนมัติ หรือด้วยวิธีการประมวลผลแบบอื่น ๆ ของข้อมูลส่วนบุคคลก็เป็นส่วนหนึ่งของการจัดเก็บข้อมูลจะต้องได้รับอนุญาตก่อน หากมีการประมวลผลข้อมูลส่วนบุคคลเพิ่มเติมนอกเหนือจากที่เก็บข้อมูลไว้ หรือ ข้อมูลถูกเปรียบเทียบเข้ากับวัตถุประสงค์เดิม ผู้ควบคุมจะถูกกำจัดสิทธิ์ตาม (GDPR) โดยข้อมูลส่วนบุคคลจะถูกเก็บไว้ตามระยะเวลาของข้อตกลงที่เป็นไปตามวัตถุประสงค์ หรือสัญญา หรือ การเก็บรักษาตามระยะของกฎหมายกำหนดไว้เท่านั้น ซึ่งหากไม่มีการแจ้งระยะเวลาเก็บข้อมูลผู้ควบคุมให้คำนึงถึงการประมวลผลภายในระยะเวลาที่เหมาะสม แต่ไม่เกิน 2 สัปดาห์ตาม Section 32 (3)

การแจ้งระยะเวลาเก็บรักษาข้อมูลส่วนบุคคลของ (PDPA)[18] ได้กำหนดให้องค์กรต้องไม่เก็บรักษาเอกสาร ซึ่งเป็นข้อมูลส่วนบุคคลที่ได้รับการประมวลผล หรือวิธีการที่ข้อมูลส่วนบุคคลนั้นสามารถเชื่อมโยงไปยังตัวบุคคลบุคคลใดบุคคลหนึ่งได้และไม่ให้เก็บรักษาข้อมูลส่วนบุคคลหรือต้องลบข้อมูลส่วนบุคคล โดยทันทีที่มีเหตุผลอันสมควรที่สันนิษฐานได้ว่า ในการเก็บ รวบรวม เปิดเผย ใช้ หรือไม่จำเป็นสำหรับธุรกิจ หรือตามวัตถุประสงค์ทางกฎหมายอีกต่อไปเพราะฉะนั้นเมื่อเปรียบเทียบการเก็บรักษาข้อมูลส่วนบุคคลของต่างประเทศ ซึ่งแสดงได้ถึงความชัดเจนกำหนดให้องค์กรมีนโยบายในการแจ้งระยะเวลาการเก็บรวบรวมข้อมูลส่วนบุคคลก่อนให้ความยินยอม และพิจารณาได้ว่า ขอบเขตการแจ้งระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 มาตรา 23 (3) ซึ่งการกำหนดให้ผู้ควบคุมข้อมูลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อน หรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคล กล่าวคือ ได้บัญญัติไว้ว่า “ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม” การกำหนดระยะดังกล่าวไม่มีความชัดเจน อาจทำให้ผู้ให้บริการกำหนดระยะเวลาตามเจตนาของตนได้

เนื่องจากด้วยวิธีการเก็บรักษาข้อมูลมีในรูปแบบลักษณะเดิม ๆ มีความซับซ้อนในการเก็บแต่ในขณะที่วิธีการเก็บแบบใหม่ ๆ ง่ายต่อการเก็บและง่ายในการใช้ข้อมูลส่วนบุคคลได้เกิดขึ้นอยู่เสมอนั้น การกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องระบุไว้ตั้งแต่แรกเริ่มในขณะเก็บรวบรวม

---

[17] โปรดดูในบทที่ 3 ประเด็นที่สาม จากข้อที่ 3.4.2 ในหน้าที่ 212

[18] โปรดดูในบทที่ 3 ประเด็นที่สาม จากข้อที่ 3.5.2 ในหน้าที่ 226

ข้อมูลส่วนบุคคลถึงระยะเวลาในการเก็บรวบรวมข้อมูลนั้น อันเป็นการดีต่อผู้ปฏิบัติ และความเคลือบคลุมจะทำให้เกิดการตีความและอาจไม่สามารถปฏิบัติได้จริงใน “ระยะเวลาที่อาจคาดหมายได้สำหรับการเก็บรวบรวม” โดยไม่มีความชัดเจนอาจทำให้ตีความหมายและจะต้องมีการประเมินความเป็น “มาตรฐานของการเก็บรวบรวม” เพื่อกำหนดระยะเวลาที่คาดหมายสำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลได้อย่างไร เช่น กรณีเจ้าของข้อมูลใช้ระบบสแกนนิ้วมือในหอพักชั่วคราว เมื่อยกเลิกการพักอาจไม่ได้กลับมาอีก ผู้ให้บริการก็ควรเก็บข้อมูลดังกล่าวได้ไม่เกินกฎหมายบัญญัติไว้ ดังนั้น ผู้วิจัยเห็นควร แก้ไขการกำหนดความชัดเจนในการแจ้งระยะเวลาการเก็บรวบรวมข้อมูลส่วนบุคคล มาตรา 23 (3) เนื่องจากในบางกรณี ผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถที่จะกำหนดระยะเวลาสำหรับการเก็บรวบรวมข้อมูลดังกล่าวข้างต้นได้ ไม่ว่าจะเป็นตามจริง หรือตามที่ “อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม” ด้วยเหตุดังกล่าวนี้ จึงควรกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งประกาศหลักเกณฑ์และนโยบายเกี่ยวกับระยะเวลาการเก็บข้อมูลส่วนบุคคลว่า “ข้อมูลส่วนบุคคลจะเก็บไว้ไม่เกิน 6 เดือน และให้ทำลายทันที หรือสิ้นสุดตามวัตถุประสงค์ทางธุรกิจ หรือ ตามข้อตกลงของสัญญา” ให้เป็นไปตามสิทธิในการขอลบข้อมูลที่เกี่ยวกับตนในระบบออนไลน์ (Right to erase) หรือสิทธิที่จะถูกลืมภายหลังที่ลบ (Right to be forgotten) เว้นแต่ตามวัตถุประสงค์ของกฎหมายได้บัญญัติไว้

4.4 วิเคราะห์บทลงโทษเพื่อความมั่นคงปลอดภัยของข้อมูลไบโอเมตริกซ์ (Biometrics)

การป้องกันไว้ดีกว่าแก้ (Proactive not reactive; preventative not remedial) ข้อมูล (Controllers) จะต้องดำเนินการระบุอัตลักษณ์ (Re-identification) ด้วยความก้าวหน้าทางเทคโนโลยีที่ทำให้ชีวิตง่ายขึ้น โดยการใช้ความรู้ในระดับที่สูงขึ้นผ่านการประดิษฐ์อุปกรณ์ต่าง ๆ นั้น อย่างไรก็ตาม นวัตกรรมทางเทคโนโลยีแต่ละอย่างก็ยังแผงมากับภัยคุกคามที่ซ่อนเร้นต่อผู้ใช้ หนึ่งในภัยคุกคามที่สำคัญ คือ การขโมยข้อมูลไบโอเมตริกซ์และข้อมูลส่วนบุคคล เช่น การใช้บริการทางธนาคารออนไลน์ระบบสมาร์ทโฟน ผู้ใช้ย่อมพยายามรักษาความปลอดภัยข้อมูลด้วยรหัสผ่านที่เข้ารหัสและเลขบัตรประจำตัว ในการใช้มาตรการรักษาความปลอดภัยนี้ มีทั้งข้อได้เปรียบของการรักษาความปลอดภัย คือ ไม่ต้องจดจำรหัสให้ยุ่งยาก และข้อบกพร่องข้อมูลส่วนบุคคลสามารถถูกแฮค (Hack) ได้จริงจากมิจฉาชีพ จึงนำไปสู่การเกิดระบบรักษาความปลอดภัยไบโอเมตริกซ์ การอนุญาตให้เปิดเผยชุดข้อมูลที่สร้างขึ้นมาจากข้อมูลส่วนบุคคล แม้จะมีการลบชื่อ หรือสิ่งที่จะทำให้เชื่อมโยงถึงบุคคลไปแล้ว ก็ยังมีโอกาสที่ข้อมูลชุดดังกล่าวที่จะถูกนำไปเชื่อมโยงกับข้อมูลชุดอื่น ๆ เพื่อระบุกับอัตลักษณ์บุคคลได้ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562

ดังนั้น ข้อยกเว้นในการเผยแพร่ข้อมูลส่วนบุคคล จึงควรคำนึงถึงความเสี่ยงดังกล่าวและดำเนินการให้แน่ใจว่าการลบชื่อ หรือสิ่งเชื่อมโยงได้กระทำอย่างเพียงพอและสุดความสามารถในการที่จะไม่ก่อให้เกิดการละเมิดต่อบุคคลในข้อมูลภายหลัง จึงควรมีการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลที่ได้ใช้กับองค์กรธุรกิจต่าง ๆ เพื่อความเหมาะสมในการส่งเสริมผู้ให้บริการมีมาตรการและวิธีปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่มีประสิทธิภาพ รวมทั้งทำให้ผู้เป็นเจ้าของข้อมูลส่วนบุคคลสามารถป้องกันข้อมูลของตนได้ ในกรณีที่ข้อมูลอาจมีความเสี่ยงว่าจะถูกละเมิดได้ จึงมีความจำเป็นที่บัญญัติในเรื่องการแจ้งเตือนเหตุละเมิดข้อมูลส่วนบุคคล เว้นแต่ การละเมิดข้อมูลส่วนบุคคลนั้น ไม่น่าจะก่อให้ให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพของบุคคล โดยผู้วิจัยเห็นว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 ที่ใช้บังคับได้กำหนดหน้าที่ของผู้ให้บริการยังไม่มีความสอดคล้องกับสากล ดังต่อไปนี้

กฎหมายของ (GDPR) มิได้กำหนดความรับผิดทางอาญาไว้อย่างชัดเจนสำหรับการประมวลผลข้อมูลส่วนบุคคลในการละเมิดกฎระเบียบ โดยบทลงโทษหลัก ๆ ที่บัญญัติไว้ใน (GDPR) คือ โทษปรับทางปกครอง นอกจากนี้ประเทศสมาชิกสหภาพยุโรปไม่จำเป็นต้องแก้ไขกฎหมายของตน เพื่อรวมบทบัญญัติเกี่ยวกับความรับผิดทางอาญาสำหรับการประมวลผลข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย มาตรการควบคุมความปลอดภัยของข้อมูลจะเป็นภาระหน้าที่พิเศษให้องค์กร และความเป็นส่วนตัวในสหภาพยุโรป ตาม (GDPR) ได้บัญญัติไว้ในมาตรา 32 ว่า “ผู้ควบคุมและผู้ประมวลผลจะใช้มาตรการทางเทคนิคและองค์กรที่เหมาะสมเพื่อให้แน่ใจว่าระดับความปลอดภัยที่เหมาะสมกับความเสี่ยง” เป็นสิ่งที่สำคัญที่สุดเสมอ แต่การจัดเก็บข้อมูลที่มีความอ่อนไหวสูง โดยจะต้องปฏิบัติตามกฎระเบียบ Regulation (EU) 2018/1725 หลักความรับผิดชอบ ซึ่ง (GDPR) ให้ความสำคัญเน้นที่ “ผู้ควบคุมในทางปฏิบัติ” ซึ่งเป็นเจ้าของผู้ประกอบธุรกิจเนื่องจากเจ้าของธุรกิจมีหน้าที่จะต้องการดำเนินการแจ้งเหตุละเมิดตามกฎระเบียบ (EU) Regulation (EU) 2016/679 และการนำข้อกฎหมายไปใช้ในเชิงที่ไม่ตรงกับวัตถุประสงค์ เช่น ดังต่อไปนี้

(1) Article 15 ผู้เป็นเจ้าของข้อมูลมีสิทธิเข้าตรวจสอบข้อมูลทั้งหมดของตนที่ผู้ให้บริการเก็บบันทึกไว้ซึ่งผู้ให้บริการหลายรายอนุญาตให้ผู้ใช้ดาวน์โหลดข้อมูลออกมา เพื่อตรวจสอบว่าถูกเก็บข้อมูลอะไรไปบ้าง หากกรณีผู้ประสงค์ร้ายสามารถเข้าถึงบัญชีผู้ใช้ได้ก็สามารถสั่งดาวน์โหลดข้อมูลทั้งหมดที่เกี่ยวข้องออกมาดูได้

(2) Article 17 ผู้เป็นเจ้าของข้อมูลมีสิทธิขอให้ Search engine นำข้อมูลของตนออกจากผลการค้นหา ซึ่งมีหลายกรณีที่ผู้ต้องสงสัยในคดีฉ้อโกงหรือผู้ที่ได้รับคำวิจารณ์แบบแง่ลบได้ขอให้ Search engine นำข้อมูลเหล่านั้นออกจากผลการค้นหา (สิทธิในการลบ)

(3) Article 21 ผู้เป็นเจ้าของข้อมูลมีสิทธิ์เลือกได้ว่าจะอนุญาตให้นำข้อมูลส่วนตัวไปใช้ในการวิเคราะห์ได้หรือไม่ ซึ่งทำให้ผู้ให้บริการบางรายปฏิเสธ ถ้าหากผู้ใช้ไม่ยินยอมที่จะเปิดเผยข้อมูลก็อาจไม่ได้รับการให้บริการ หรือไม่สามารถเข้าถึงเนื้อหาได้เทียบเท่ากับผู้ที่ยินยอมให้นำข้อมูลไปใช้งาน (สิทธิ์ในการคัดค้าน)

(4) Article 10 ข้อมูลส่วนบุคคลที่เป็นลักษณะเฉพาะธรรมชาติของบุคคลที่มีความอ่อนไหวอย่างยิ่งเกี่ยวกับสิทธิขั้นพื้นฐานและเสรีภาพได้รับการคุ้มครองที่เฉพาะเจาะจง เพื่อความมั่นคงปลอดภัย เนื่องจากบริบทของการประมวลผลสามารถสร้างความเสี่ยงที่สำคัญต่อสิทธิขั้นพื้นฐานและเสรีภาพ ข้อมูลส่วนบุคคลดังกล่าวไม่ควรถูกประมวลผล เว้นแต่ จะมีการปฏิบัติตามเงื่อนไขเฉพาะที่กำหนดไว้ในข้อบังคับนี้ การประมวลผลข้อมูลส่วนตัวประเภทพิเศษเนื่องจากครอบคลุมโดยคำจำกัดความของข้อมูลไบโอเมตริกซ์เมื่อประมวลผลด้วยวิธีการทางเทคนิคเฉพาะซึ่งอนุญาตให้มีการระบุตัวตน หรือการรับรองความถูกต้องของบุคคลตามข้อบังคับตามข้อบังคับ (29) โดยข้อกำหนดเฉพาะสำหรับการประมวลผลข้อมูลที่ละเอียดอ่อน นอกเหนือจากหลักการทั่วไปและกฎระเบียบอื่น ๆ โดยเฉพาะอย่างยิ่งเกี่ยวกับเงื่อนไขสำหรับการประมวลผลที่ถูกกฎหมาย (Derogations) จำแนกออกจากข้อห้ามทั่วไป สำหรับการประมวลผลข้อมูลส่วนบุคคลประเภทพิเศษดังกล่าว และได้รับการจัดเตรียมไว้อย่างชัดเจน ในกรณีต้องได้รับความยินยอมก่อนอย่างชัดเจน หรือในแง่ของความต้องการเฉพาะ

การกำหนดบทลงโทษและค่าปรับสำหรับการละเมิดปรับสูงสุด 20 ล้านยูโร หรือร้อยละ 4 ของรายได้ทั้งหมดทั่วโลกของปีงบประมาณ ตาม Regulation (EU) 2016/679 Article 83 ข้อ 5 สำหรับองค์กรที่มีการประมวลข้อมูลส่วนบุคคลอย่างผิดกฎหมาย หรือไม่สามารถปกป้องข้อมูลได้ รวมทั้ง เจ้าของข้อมูลแต่ละบุคคลขอให้องค์กรนำข้อมูลส่วนตัวของตนออกจากระบบอัตโนมัติที่ใช้ประมวลและจัดการข้อมูลด้วย โดยมาตรการของการละเมิดข้อมูลส่วนบุคคลผู้ควบคุมจะต้องแจ้งเตือนล่าช้าได้ไม่เกิน 72 ชั่วโมง หลังจากทราบว่ามีการกาละเมิดข้อมูลส่วนบุคคลต่อเจ้าหน้าที่กำกับดูแล เว้นแต่ การละเมิดนั้น ไม่น่าจะส่งผลกระทบให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพของบุคคลนั้น ในกรณีที่การแจ้งเตือนไปยังผู้ดูแลการป้องกันข้อมูลในสหภาพยุโรปไม่สามารถแจ้งได้ภายใน 72 ชั่วโมง จะต้องมีเหตุผลสำหรับความล่าช้านั้นตามมาตรา 33 ในการปฏิบัติตามมาตรการทางเทคนิคและทางการจัดการองค์กรที่เหมาะสม โดยคำนึง “ความทันสมัยและค่าใช้จ่ายในการดำเนินงาน” และลักษณะ ขอบเขต บริบท และวัตถุประสงค์ในการประมวลผล ตลอดจนความเสี่ยงในการเปลี่ยนแปลงที่เป็นไปได้และเข้มงวดสำหรับสิทธิและเสรีภาพของบุคคลธรรมดา

อย่างไรก็ตามตาม เนื่องจากสหภาพยุโรปมีลักษณะเป็นองค์กรบริหารเหนือรัฐ (Sup national) ดังที่ผู้วิจัยได้กล่าวมาแล้วในบทที่ 3[19] โดยมุ่งเน้นเฉพาะมาตรการโทษปรับและโทษทางปกครองเท่านั้น ผู้วิจัยจึงได้พิจารณาจากเหตุดังต่อไปนี้ กล่าวคือ

1. คณะกรรมาธิการของสหภาพยุโรปไม่มีสภานะเป็นรัฐบาล (Government) รัฐบาลหมายถึง องค์การและคณะบุคคลซึ่งใช้อำนาจในการปกครองประเทศอย่างเป็นอิสระ ไม่ขึ้นแก่รัฐบาลของรัฐอื่นใด หรือหน่วยงาน ซึ่งนำเอาความต้องการของรัฐไปกำหนดและบังคับการให้เป็นไปตามนั้น และไม่มีรัฐใดที่จะอยู่ได้โดยปราศจากรัฐบาล โดยรัฐบาลเป็นผู้ทำหน้าที่คุ้มครองรักษาความสงบภายในและป้องกันการรุกรานจากภายนอก

2. กฎหมายที่ให้อำนาจในการออกบทบัญญัติที่มีโทษบังคับทางอาญา

3. การบังคับใช้โทษทางอาญาจะต้องบังคับผ่านเจ้าพนักงานหน้าที่ของรัฐในการบังคับจับคุมผู้กระทำความผิดที่มีโทษทางอาญา

ดังจะเห็นได้จาก อารัมภบทข้อ 149 ของ (GDPR) บทนำ “ประเทศสมาชิกควรจะวางกฎเกณฑ์เกี่ยวกับบทลงโทษทางอาญาสำหรับการละเมิดกฎข้อบังคับนี้รวมถึงการละเมิดกฎแห่งชาติที่นำมาใช้และภายในขอบเขตของระเบียบฉบับนี้” นอกจากนี้ตามมาตรา 84 (1) ของ (GDPR) ประเทศสมาชิกจะวางระเบียบเกี่ยวกับบทลงโทษอื่น ๆ ที่ใช้บังคับกับการละเมิดกฎข้อบังคับนี้โดยเฉพาะอย่างยิ่งสำหรับการละเมิดที่ไม่ต้องเสียค่าปรับทางปกครองตามมาตรา 83 และจะใช้มาตรการทั้งหมดที่จำเป็น เพื่อให้มั่นใจว่ามีการนำไปปฏิบัติแล้วการลงโทษดังกล่าวจะต้องมีประสิทธิภาพ หมายความว่า ประเทศสมาชิกมีอิสระที่จะแนะนำความรับผิดทางอาญาสำหรับการประมวลผลข้อมูลส่วนบุคคลที่ผิดกฎหมายตามดุลยพินิจของตน ดังนั้น จึงเห็นได้ว่า การจัดทำกฎหมายฉบับแรกของประเทศไทยที่บังคับใช้กับการคุ้มครองข้อมูลส่วนบุคคลในประเทศโดยคณะผู้ร่างกฎหมายไทยได้นำแนวคิดมาจากกฎระเบียบว่าด้วยการป้องกันข้อมูลทั่วไปของสหภาพยุโรป (GDPR) ซึ่งมีการปรับเปลี่ยนให้เหมาะสมกับมุมมองของชาติ และได้เพิ่มบทบัญญัติเกี่ยวกับความรับผิดทางอาญาในพระราชบัญญัติคุ้มครองข้อมูลส่วน พุทธศักราช 2562

บทลงโทษเพื่อความมั่นคงปลอดภัยของพระราชบัญญัติคุ้มครองข้อมูลไบโอเมตริกซ์ของ (BIPA)[20] โดยกำหนดให้ข้อมูลไบโอเมตริกซ์ เป็นข้อมูลที่ถูกสร้างขึ้นโดยวิธีการอัตโนมัติของลักษณะทางชีวมาตรของแต่ละบุคคล และข้อจำกัดเฉพาะข้อมูลไบโอเมตริกซ์ที่ได้รับการลงทะเบียน หรือลดรูปแบบในฐานข้อมูล โดยไม่มีการแจ้งเตือนล่วงหน้าให้ทราบก่อนและให้ความยินยอม เว้นแต่จะมีคุณสมบัติตรงตามเกณฑ์ที่กำหนด โดยมีมาตรการกำหนดให้ประกาศ

---

[19] โปรดดูในหน้าที่ 114

[20] โปรดดูในบทที่ 3 ประเด็นที่สี่ จากข้อ 3.3.4 ในหน้าที่ 192

นโยบายเกี่ยวกับการเก็บรักษาและการเข้าถึงข้อมูลไบโอเมตริกซ์เป็นตารางแก่เจ้าของข้อมูล และแจ้งเหตุละเมิดตาม 740 ILCS 14/15 ต้องได้รับแจ้งเกี่ยวกับข้อกำหนดการพิมพ์ลายนิ้วมือ หรือวิธีการใช้หรือจัดเก็บข้อมูลที่สำคัญ

บทลงโทษเพื่อความมั่นคงปลอดภัยของ (BDSG)[21] ในการแจ้งเตือนการละเมิดข้อมูลไบโอเมตริกซ์นั้น จึงได้ดำเนินการด้วยความระมัดระวังเป็นกรณีพิเศษตามกฎหมายของ (BDSG) ในการประมวลผลข้อมูลส่วนบุคคลที่จะต้องได้รับอนุญาตก่อนจากเจ้าของข้อมูล ซึ่งผู้ควบคุมและผู้ประมวลผลจะต้องคำนึงถึงสถานะของต้นทุนการดำเนินการและลักษณะขอบเขตขอบเขตและวัตถุประสงค์ของการประมวลผลรวมถึงความเสี่ยงของโอกาสและความรุนแรงที่แตกต่างกัน สำหรับผลประโยชน์ที่ได้รับการคุ้มครองตามกฎหมายของบุคคลจะต้องใช้มาตรการทางเทคนิคและองค์กรที่จำเป็นเพื่อให้มั่นใจในระดับความปลอดภัยที่เหมาะสมกับความเสี่ยง เมื่อประมวลผลข้อมูลส่วนบุคคลโดยเฉพาะอย่างยิ่งเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลประเภทพิเศษ โดยผู้ควบคุมจะต้องคำนึงถึงหลักเกณฑ์ทางเทคนิคและคำแนะนำที่เกี่ยวข้องจากสำนักงานกลางเพื่อความปลอดภัยของข้อมูลตาม Section 64

มาตรการความมั่นคงปลอดภัยของ (PDPA)[22] ตามมาตรา 24[23] กำหนดให้องค์กรมีหน้าที่ในการรักษาความปลอดภัยของข้อมูลที่อยู่ในความครอบครองแต่ไม่ได้มีการกำหนดมาตรการด้านความปลอดภัยไว้เป็นพิเศษจึงเป็นหน้าที่ขององค์กรต้องจัดให้มีมาตรการในการรักษาความปลอดภัยที่เหมาะสมกับลักษณะและการใช้ข้อมูลนั้น ๆ ตามมาตรา 25 กำหนดให้ทำลายข้อมูลเมื่อหมดความจำเป็นตามวัตถุประสงค์แล้วและการเก็บข้อมูล (Retention) นั้นไม่จำเป็นต่อวัตถุประสงค์เชิงกฎหมาย หรือธุรกิจอื่นอีก องค์กรเป็นหน่วยงานป้องกันข้อมูลส่วนบุคคล ซึ่งอยู่ในความครอบครอง หรืออยู่ในการความควบคุมขององค์กร

จากการศึกษาวิเคราะห์มาตรการในการลงโทษของต่างประเทศ ผู้วิจัยพบว่ามาตรการทางกฎหมายประเทศไทยยังไม่มีความสอดคล้องกับสากล ดังนี้

ประการแรก มาตรการมาตรการความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของกฎหมาย (GDPR)[24] ได้มีการกำหนดบทลงโทษหากกระทำการฝ่าฝืนจะมีบทลงโทษสำหรับองค์กรที่ฝ่าฝืนตามข้อกำหนดของ (GPPR) สูง โดยมุ่งเน้นโทษปรับและโทษทางปกครองเท่านั้น โดยจะหลีกเลี่ยงมาตรการลงโทษทางอาญา หนึ่งในวัตถุประสงค์ของกฎการคุ้มครองข้อมูลทั่วไป (GDPR) คือ

---

[21] โปรดดูในบทที่ 3 ประเด็นที่สี่ จากข้อ 3.4.2 ในหน้าที่ 212

[22] โปรดดูในบทที่ 3 ประเด็นที่สี่จากข้อ 3.5.2 ในหน้าที่ 226

[23] Personal Data Protection Act 2012

[24] โปรดดูในบทที่ 3 ประเด็นที่สี่ จากข้อ 3.2.4 ในหน้าที่ 153

การปกป้องสิทธิขั้นพื้นฐานและเสรีภาพของบุคคลโดยเฉพาะอย่างยิ่งสิทธิในการปกป้องข้อมูลส่วนบุคคลของสหภาพยุโรป สิทธิในการใช้ชีวิตส่วนตัวได้ถูกกำหนดไว้ในอนุสัญญาว่าด้วยสิทธิมนุษยชนแห่งยุโรป มาตรา 8[25] ให้สิทธิในการเคารพชีวิตส่วนตัวและครอบครัวบ้านและการโต้ตอบการประชุมได้รับการจัดตั้งขึ้นเป็นกฎหมายในประเทศสวีเดน สิทธิที่จะเคารพในชีวิตส่วนตัวและชีวิตครอบครัวนั้นได้กำหนดไว้ในข้อ 7 ของสนธิสัญญา (EU) ว่าด้วยสิทธิขั้นพื้นฐาน นอกจากนี้ยังมีบทบัญญัติพิเศษเกี่ยวกับการปกป้องข้อมูลส่วนบุคคล ตามมาตรา 8 สนธิสัญญามีผลผูกพันตามกฎหมายสำหรับประเทศสมาชิกสหภาพยุโรปทั้งหมด อันเกี่ยวข้องกับสิทธิในการใช้ชีวิตส่วนตัวและการปกป้องข้อมูลส่วนบุคคลในรูปแบบพื้นฐานของการออกกฎหมาย เพื่อให้ผู้ประกอบการธุรกิจตระหนักถึงความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล โดยมุ่งเน้นที่ผู้ควบคุมซึ่งเป็นประกอบการมีหน้าที่พึงระวังความเสียหายที่จะเกิดขึ้นจึงได้มีมาตรการโทษปรับที่สูงเพื่อให้สอดคล้องกับยุคดิจิทัล

พระราชบัญญัติ (BIPA) กำหนดโทษปรับมาจากสาเหตุของการกระทำโดยการละเมิดความเป็นส่วนตัวทางชีวมาตรตามกฎหมายปรับมากกว่า 1,000 ดอลลาร์ ในความเสียหายที่ต้องจ่าย หรือความเสียหายที่เกิดขึ้นจริง สำหรับการละเมิดโดยประมาท ซึ่งโทษปรับมากกว่า 5,000 ดอลลาร์สำหรับความเสียหาย หรือความเสียหายที่แท้จริง สำหรับการละเมิดโดยเจตนา หรือโดยประมาทและกฎหมายยังให้มีสิทธิผู้เสียหายเรียกค่าธรรมเนียมและค่าใช้จ่ายทนายความได้ตามความเหมาะสมด้วย

พระราชบัญญัติ (BDSG) หากมีการละเมิดข้อมูลส่วนบุคคลได้กำหนดบทลงโทษสูงทั้งยังมีโทษทางอาญา แต่อย่างไรก็ตาม กฎหมาย BDSG ก็ต้องคำนึงถึงความสอดคล้องของข้อบังคับของ GDPR สำหรับการดำเนินคดีเพื่อกำหนดโทษปรับสูงถึง 100,000 ยูโร และโทษทางอาญาจำคุกไม่เกิน 2 ปี และสำหรับนายจ้างที่มีการละเมิดข้อมูลส่วนบุคคลของพนักงาน (BDSG) จะต้องเสียค่าปรับสูงถึง 300,000 ยูโร ต่อการละเมิดข้อมูลส่วนบุคคล และพนักงานจะสามารถเรียกร้องค่าเสียหายจากการละเมิดที่ถูกกล่าวหาได้และสหภาพแรงงานสามารถยื่นคำร้องเพื่อขอคำสั่งศาลได้โดยแจ้งเตือนเมื่อพบว่าข้อมูลรั่วไหล หน่วยงานควบคุมข้อมูลและผู้ประมวลผลข้อมูลต้องแจ้งให้หน่วยงานกำกับดูแล และเจ้าของข้อมูลทราบภายใน 72 ชั่วโมง ซึ่งมาตรการดังกล่าวอาจทำให้ผู้ประมวลผลข้อมูลส่วนบุคคลต้องตระหนักในการที่จะต้องรับโทษและระมัดระวังในการประมวลผลข้อมูลดังกล่าว

---

[25] European Convention on Human Rights (ECHR)

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act 2012: PDPA) ในมาตรการเพื่อป้องกันมิให้ข้อมูลส่วนบุคคลนั้น ถูกเข้าถึงโดยไม่ได้รับอนุญาต แก้ไข ใช้ เปิดเผย คัดลอก เปลี่ยนแปลง ทำลาย หรือความเสี่ยงอื่นที่มีลักษณะเช่นเดียวกันและในการเก็บรักษาข้อมูลส่วนบุคคลนั้น ข้อมูลส่วนบุคคลจะถูกเก็บไว้ในเซิร์ฟเวอร์ส่วนกลางเพื่อปกป้องความลับ และความปลอดภัยของข้อมูลส่วนบุคคลภายใต้การบริการผ่านเทคโนโลยีการป้องกันความปลอดภัยทางกายภาพและการบริหารในการรักษาความปลอดภัย หากมีการละเมิดโดยฝ่าฝืนต่อกฎหมายการฝ่าฝืนกฎหมายอาจต้องรับโทษถึง 100,000 SGD หรือต้องโทษจำคุกไม่เกิน 12 เดือน หรือทั้งจำทั้งปรับ ทั้งนี้ ผู้อำนวยการและเจ้าหน้าที่ของหน่วยงานสามารถถูกฟ้องร้องความรับผิดชอบจากความผิดที่หน่วยงานเป็นผู้กระทำได้ด้วย

ประการที่สอง เมื่อพิจารณาถึงหลักเกณฑ์ในการกำหนดบทลงโทษของประเทศไทยตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 หากฝ่าฝืนจะมีบทลงโทษสำหรับองค์กร หรือบุคคลที่ฝ่าฝืน ดังที่ได้พิจารณาไว้ในบทที่ 3 หน้าที่ 116-117 โดยมีหลักเกณฑ์ดังนี้

มาตรการลงโทษทางแพ่ง (Civil Penalty) กล่าวคือ เป็นเรื่องที่เกี่ยวกับสิทธิ หรือหน้าที่ของบุคคล โดยมุ่งให้ผู้กระทำผิดอาจต้องถูกดำเนินมาตรการต่าง ๆ ได้แก่ การชำระค่าปรับทางแพ่ง ถูกเรียกคืนผลประโยชน์ที่ได้ไปจากการกระทำผิด ให้ชดใช้ค่าใช้จ่าย หรือส่งมอบทรัพย์สิน หรือละเว้นการกรทำอย่างใดอย่างหนึ่ง เพื่อประโยชน์ของผู้ฟ้องคดี ในกรณีตามมาตรา 78 ซึ่งเป็นมาตรการเพื่อ “ปราม” มิให้ผู้ประกอบการกล้ากระทำความผิดอีก ในเชิงลงโทษ คือ “ค่าเสียหายเชิงลงโทษ” โดยการชดใช้เพิ่มขึ้นจากจำนวนค่าเสียหายที่แท้จริงได้ตามที่ศาลกำหนด แต่ไม่เกินสองเท่าของค่าเสียหายที่แท้จริง โดยศาลอาจกำหนดให้จ่ายค่าเสียหายโดยคำนึงถึงความร้ายแรงของความเสียหายของผลประโยชน์ที่ผู้ประกอบการได้รับจากข้อมูลส่วนบุคคลนั้น ดังนั้น มาตรการทางแพ่งเป็นมาตรการบังคับ เพื่อใช้ในปัญหาระหว่างเอกชนและเอกชนให้เกิดความเป็นธรรม โดยมีการสร้างสิทธิและหน้าที่ต่าง ๆ ขึ้นตามความเหมาะสมของเรื่องนั้น ๆ[26]

มาตรการลงโทษทางอาญา (Criminal penalty) กล่าวคือ โทษทางอาญามีวัตถุประสงค์นำมาปรับใช้กับ บทบัญญัติในแต่ละเรื่องได้ชัดเจน แม้ว่าบทบัญญัติในกฎหมายอาญาโดยทั่วไปจะบัญญัติขึ้นมา ด้วยเหตุผลทางศีลธรรม แต่ก็มีบทบัญญัติในบางเรื่องด้วยเหตุผลทางเทคนิค ซึ่งสามารถนำทฤษฎีกฎหมายสามชั้นมาปรับความให้เข้ากับกฎหมายอาญาได้ดังนี้

หากบทบัญญัติที่ได้กำหนดด้วยเหตุผลทางศีลธรรมย่อมเป็นเรื่องที่ประชาชนสามารถรับรู้ได้โดยสามัญสำนึกถึงความถูกผิดในเรื่องนั้น แม้ในบางเรื่องจะมีหลักกฎหมายเพิ่มเติมอยู่ ก็สามารถเรียนรู้เพิ่มเติมได้ เพราะเรื่องที่ปรับแต่งมาจากหลักเดิม แต่ถ้ากฎหมายใดบัญญัติด้วยเหตุผลทางเทคนิค

---

[26] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562.

นั้นย่อมมิใช่เรื่องที่ประชาชนจะรู้ได้ด้วยสามัญสำนึกของตนเสมอไป เพราะบางเรื่องมิใช่มาจากพื้นฐาน ทางศีลธรรม หากจะเข้าใจในเหตุผลที่บทบัญญัติของกฎหมายนั้น จึงเป็นเรื่องสำคัญยิ่งมิฉะนั้น อาจจะเกิดปัญหาว่า แม้นักกฎหมายก็อาจใช้กฎหมายไม่สอดคล้องกับความเป็นจริงก็ได้ ผู้วิจัยเห็นว่าบทบัญญัติกฎหมายอาญาดังกล่าวเป็นกฎหมายเทคนิค ซึ่งบัญญัติขึ้นมาด้วยเหตุผลพิเศษ

ในการลงโทษ เพื่อเป็นการแก้แค้นตอบโต้ต่อการกระทำ หรือ พฤติกรรมที่ผู้กระทำผิดได้กระทำการอันเป็นการฝ่าฝืนต่อกฎหมายอาญา และยังเป็นการแสดงออกให้เห็นถึงการไม่ยอมรับในการกระทำ หรือ พฤติกรรมดังกล่าว และไม่ยอมรับในตัวของผู้กระทำผิด เช่นนี้ ทำให้โทษทางอาญาจึงมีความแตกต่างจาก การบังคับใช้กฎหมายประเภทอื่น ๆ (Sanctions) ด้วยความพิเศษของวัตถุประสงค์เพื่อจริยธรรมทางสังคม และความรุนแรงของการลงโทษของรัฐ (Die Ernst der Staatliche strafe: The severity of state penalty) มีโทษทางอาญาสูงและจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1 ล้านบาท[27]โดยมีโทษทางอาญาจำคุกใน 3 กรณี กล่าวคือ (1) การเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26 (มาตรา 79) (2) การเปิดเผยข้อมูลส่วนบุคคลที่ได้รับรู้มาจากการปฏิบัติหน้าที่ (มาตรา 80) และ (3) กรรมการ หรือผู้จัดการต้องรับผิดด้วย ถ้าสั่งการ หรือละเว้นไม่สั่งการ

มาตรการลงโทษทางปกครอง (Administrative penalty) กล่าวคือ โทษทางปกครองอันเป็นกฎหมายเทคนิคมีสภาพบังคับ (Sanction) สำหรับการกระทำที่ฝ่าฝืนกฎหมาย หรือไม่ปฏิบัติตามบทบัญญัติที่ต้องให้กระทำ และห้ามมิให้กระทำการ หรือ การบังคับให้ต้องกระทำการนั้น ซึ่งยังมิใช่เรื่องร้ายแรงที่ผิดศีลธรรม หรือ ความสงบเรียบร้อยของสังคม หรือความมั่นคงของรัฐ โดยผู้กระทำการที่ฝ่าฝืนกฎหมายที่มีโทษทางปกครอง มิใช่อาชญากร แต่เป็นผู้กระทำผิดกฎระเบียบเล็กน้อยในสังคมเท่านั้น เนื่องจากมีข้อบังคับต่าง ๆ ตามบทบัญญัติของกฎหมาย เพื่อให้กฎหมายมีผลบังคับใช้ในการควบคุมและกับความประพฤติของบุคคลในอนาคต โดยโทษทางปกครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 นั้นมีโทษปรับมากถึง 5 ล้านบาท สำหรับผู้ควบคุมข้อมูล และผู้ประมวลผลข้อมูล ตามมาตรา 83 และมาตรา 87[28]

ดังนั้น เพื่อมาตรการให้ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลต้องชดใช้ค่าสินไหมทดแทนหากฝ่าฝืน โดยมีสาระสำคัญ คือ การเก็บ ใช้ เปิดเผย ข้อมูลส่วนบุคคล ต้องได้รับความยินยอมจากเจ้าของข้อมูลอย่างชัดเจน และเจ้าของข้อมูลมีสิทธิถอนความยินยอมภายหลังได้ รวมถึงมีสิทธิขอให้ลบ หรือทำลายเมื่อการเก็บ ใช้ เปิดเผย ทำโดยไม่ชอบด้วยกฎหมาย หรือเมื่อถอนความยินยอมไม่ว่าจะเกิดจากการจงใจ หรือประมาท อันเป็นการกระทำการไปโดยไม่มีเหตุอันควร หรือเพื่อบรรเทาความเสียหายที่อาจจะเกิดขึ้นต่อเจ้าของข้อมูลในการป้องความเสียหายที่กำลังจะเกิดขึ้น

---

[27] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562.

[28] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562.

หรือระงับเสียหายตามความรับผิดทางแพ่ง ซึ่งมาตรการทางปกครองเป็นเรื่องความสัมพันธ์ระหว่างรัฐกับเอกชน ที่มุ่งรักษาประโยชน์ร่วมกันของสังคมในการลงโทษปรับทางปกครอง แต่มาตรการบังคับใช้โทษทางอาญาต่อบุคคลผู้กระทำการฝ่าฝืนกฎหมาย ในลักษณะของความผิดทางอาญา เพราะมีกฎหมายห้ามมิให้กระทำไว้โดยรัฐ

ทั้งนี้ เพื่อต้องการให้เกิดความสงบเรียบร้อยขึ้นในสังคมและให้บริการสาธารณะของรัฐตามรัฐธรรมนูญ[29] ที่ได้ให้อำนาจไว้หากเป็นการกระทำที่ผู้กระทำมีเจตนาชั่วร้าย หรือก่อให้เกิดภยันตราย ร้ายแรง ถึงขนาดที่ต้องถูกตั้งข้อรังเกียจได้อย่างมากจากสังคม จึงมีวัตถุประสงค์ในการแก้แค้นตอบแทนให้สาสม หรือเป็นการข่มขู่ หรือป้องกันอาชญากรรม หรือเป็นการตัดโอกาสในการกระทำความผิดต่อสังคม โดยมาตรการโทษทางปกครองสามารถที่จะดำเนินการควบคู่ไปกับการดำเนินมาตรการโทษทางอาญาได้ โดยไม่ถือว่าเป็นการดำเนินการซ้ำซ้อนกัน เพราะเป็นคนละมาตรการทางกฎหมายกันไม่จำเป็นต้องสอดคล้อง หรือถือตามซึ่งกันและกัน ในขณะที่โทษทางปกครองเป็นมาตรการการลงโทษสำหรับความผิดที่ได้กระทำในแต่ละกรรม โดยหลักจึงไม่อาจลงโทษปรับทางปกครองซ้ำกับโทษทางอาญาในความผิดเดียวกันได้ ตามบทบัญญัติของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 จึงได้มีมาตรการจำแนกโทษทางแพ่ง โทษทางอาญา และโทษทางปกครอง ด้วยเหตุดังกล่าวข้างต้น

ผู้วิจัยเห็นว่า การมีมาตรการกำหนดโทษทางแพ่ง โทษทางอาญา และโทษทางปกครองดังกล่าวนี้ ควรมีความสอดคล้องกับ กฎหมายของ (GDPR) เนื่องจากภาคธุรกิจที่มีการใช้ข้อมูลส่วนบุคคลจำนวนมากที่ดำเนินงานภายในสหภาพยุโรป และบริษัทที่ประกอบธุรกิจ หรือหวังจะประกอบธุรกิจกับพลเมืองของสหภาพยุโรปจะต้องปฏิบัติตามกฎหมาย (GDPR) แม้ว่าบริษัทที่อยู่นอกสหภาพยุโรปก็จะต้องได้รับผลกระทบ หากมีการนำเสนอสินค้า หรือบริการแก่พลเมืองของสหภาพยุโรปและเก็บข้อมูลส่วนบุคคลของพลเมืองของสหภาพยุโรป ในขณะเดียวกันก็ควรมีข้อพึงระวังและข้อปฏิบัติที่แตกต่างออกไป หากผู้ประกอบการในประเทศไทยมีการประกอบธุรกิจ หรือบริการโดยช่องทางออนไลน์ให้กับบุคคลธรรมดาใน (EU) สามารถเข้าถึงได้และมีการประมวลผลข้อมูลของบุคคลดังกล่าวนั้น ซึ่งความสำคัญทางการค้าระหว่างประเทศจึงมีมูลค่าทางเศรษฐกิจสูง ย่อมเข้าข่ายต้องปฏิบัติตามกฎหมาย (GDPR) เช่น การจำแนกประเภทข้อมูลที่มีความอ่อนไหว (Sensitive data) ออกต่างหากจากข้อมูลทั่วไป การให้ความยินยอมอย่างเสรี (Freely Given) ซึ่งมีวัตถุประสงค์ที่เฉพาะเจาะจงในการขอความยินยอม (Specific) แจ้งการประมวลผลข้อมูลให้เจ้าของข้อมูลส่วนบุคคลทราบ (Informed) เจ้าของข้อมูลต้องแสดงความยินยอมอย่างไม่กำกวม (Unambiguous) สิทธิในการได้รับแจ้งข้อมูล (Right to be informed) สิทธิในการเข้าถึงข้อมูล (Right of access) สิทธิในการแก้ไข

[29] รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560.

ข้อมูลของตนให้ถูกต้อง (Right to rectification) สิทธิในการลบ (Right to erasure) หรือ “สิทธิที่จะถูกลืม” (Right to be forgotten) สิทธิในการจำกัดการประมวลผลข้อมูล(Right to restriction of processing) สิทธิในการโอนย้ายข้อมูล (Right to data portability) สิทธิในการคัดค้าน (Right to object) สิทธิในการคัดค้านการตัดสินใจแทนโดยอัตโนมัติ (Right on automated Individual decision-making, including profiling) เป็นต้น

เนื่องจากการละเมิดข้อมูลส่วนบุคคลเป็นข้อกำหนดความรับผิดทางแพ่ง (Civil Liability) ที่กำหนดให้บุคคลมีหน้าที่พึงระวัง ไม่ให้เกิดความเสียหายแก่ผู้อื่น (Duty to Care) หากเกิดความเสียหายขึ้น ผู้ก่อเหตุต้องชดใช้บนพื้นฐานของแนวการของกฎหมายละเมิดที่จะต้องมุ่งไปที่ “แนวการกำหนดความรับผิด เพื่อจูงใจให้บุคคลยับยั้งถึงเหตุแห่งความเสียหายเป็นการล่วงหน้า (Ex ante)” หากสามารถช่วยยับยั้งเหตุได้ก่อน ก็จะไม่ต้องพิจารณาเรื่องการชดเชยความเสียหาย พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล 2562 กำหนดให้ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องแจ้งรายละเอียดการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลให้กับเจ้าของข้อมูลทราบก่อน และเจ้าของข้อมูลส่วนบุคคล สามารถติดต่อผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล ในเรื่องเกี่ยวกับสิทธิของตนได้ แต่เนื่องจากผู้ประมวลผลข้อมูลส่วนบุคคลมีข้อจำกัด หรือ อาจไม่มีข้อมูลที่จะทราบได้ว่าตนกำลังประมวลผลอยู่นั้นเป็นข้อมูลส่วนบุคคล และไม่มีความสัมพันธ์กับเจ้าของข้อมูล เช่น ผู้ให้บริการไอคลาวด์ ตามมาตรา 41 วรรคห้า[30] หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลจึงควรมุ่งเน้นในมาตรการด้านการรักษาความปลอดภัยของระบบให้มีความเหมาะตามสมควร ผู้ประมวลผลข้อมูลส่วนบุคคลจึงไม่ควรมีความรับผิดต่อเจ้าของข้อมูล เว้นแต่ ในกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลกระทำการขัดคำสั่งของผู้ควบคุม อันมิชอบด้วยกฎหมาย โดยทั่วไปผู้ประมวลผลข้อมูลส่วนบุคคลจะไม่ต้องตัดสินใจเกี่ยวข้องกับการเก็บ รวบรวม การใช้ หรือ เปิดเผยข้อมูลส่วนบุคคล และอาจมีเพียงเล็กน้อย หรืออาจไม่มีเลย สำหรับการตัดสินใจ

ประเด็นมาตรการโทษปรับในกรณีเศรษฐศาสตร์กับอาชญาวิทยา หรืออาชญาเศรษฐศาสตร์ (Economics of crime) ผู้วิจัยพบว่า ผู้ก่ออาชญากรรมก็ไม่แตกต่างจากบุคคลทั่วไปที่มีพฤติกรรมเป็นเหตุเป็นผล (Rational behavior) ในเชิงเศรษฐศาสตร์ โดยบุคคลนั้นจะตัดสินใจก่ออาชญากรรมก็ต่อเมื่อผลประโยชน์ที่คาดว่าจะได้รับสูงกว่าโทษที่จะคาดว่าจะได้รับจากการก่ออาชญากรรมนั้น ซึ่งปัจจัยที่ส่งผลต่อการก่ออาชญากรรมแบ่งได้ 4 ส่วน

---

[30] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562.

(1) ประโยชน์ของการก่ออาชญากรรม (2) ความน่าจะเป็นที่การก่ออาชญากรรมจะสำเร็จ (3) โทษของการก่ออาชญากรรม (4) ความน่าจะเป็นที่อาชญากรถูกลงโทษ หากผู้คิดก่ออาชญากรรมเชื่อว่า ก่อนจะลงมือกระทำอะไรหากได้มีการคะเนว่า จะได้รับผลลัพธ์อันคุ้มค่า ก็จะกระทำการหากไม่คุ้มค่า หรือเสียหายก็จะงดเว้นการกระทำนั้น เมื่อต้องการเพิ่มทางอาญาโอกาสจับกุมผู้กระทำผิดให้ได้รับโทษมากขึ้นก็ต้องลงทุนเพิ่มขึ้นในระบบเจ้าพนักงานตำรวจ ศาล และกระบวนการยุติธรรม เพิ่มเวลาจำคุกให้นานขึ้น เพิ่มบทลงโทษอื่น ๆ ให้หนักขึ้น ไม่ว่าจะโดยวิธีการใด สังคมย่อมได้รับประโยชน์ แต่การเพิ่มลงโทษทางอาญาทั้งที่มีโอกาสจับกุมได้ต่ำนั้น สังคมจะต้องเสียต้นทุนส่วนหนึ่งไปกับงบประมาณที่ลงทุนไปกับกระบวนการยุติธรรม กล่าวคือ มีความเสี่ยงที่จะตัดสินผิดพลาดจากการจับกุมและลงโทษผู้บริสุทธิ์ ฉะนั้น เมื่อมีการเพิ่มบทลงโทษโดยเพิ่มค่าปรับการกำหนดบทลงโทษปรับที่เพิ่มอัตราค่าปรับจะไม่สร้างภาระต่อสังคมมากนัก แต่ถ้าเพิ่มมาตรการโทษจำคุกรัฐจะเสียต้นทุน หรือต้องรับภาระมากขึ้น ในการบริหารเรือนจำ ค่าจ้างพนักงานเจ้าหน้าที่และอื่น ๆ ตามมา ในขณะที่การเพิ่มค่าปรับจะทำให้รัฐมีรายได้เพิ่มขึ้น

ด้วยเหตุนี้ ผู้ประมวลผลข้อมูลส่วนบุคคลจึงไม่ควรมีความรับผิดในการใช้ความเสียหายเช่นเดียวกันกับผู้ควบคุมข้อมูลส่วนบุคคลที่เกี่ยวเนื่องกับโทษทางอาญาด้วย อันเป็นการกำหนดโทษความผิดเด็ดขาด บุคคลที่อาจเกี่ยวข้องกับการไม่ปฏิบัติหน้าที่ดังกล่าวอาจมีจำนวนมาก ซึ่งมีหน้าที่ความรับผิดชอบที่หลากหลาย และ อาจอยู่ในหลายประเทศ ซึ่งการบัญญัติให้บุคคลที่มีหน้าที่ความรับผิดชอบเพียงเล็กน้อยจะต้องรับโทษทางอาญาไปด้วยตามมาตรา 79 และ มาตรา 80 ดังกล่าวนั้น ผู้ที่ต้องรับผิดสำหรับการกระทำความผิดควรเป็นผู้ประกอบการธุรกิจ มิใช่บุคคลธรรมดา ที่ไม่ปฏิบัติตามกฎหมาย โดยค่าปรับที่มีจำนวนสูง ควรถูกบังคับใช้แก่ผู้ประกอบการธุรกิจและความเสี่ยงอื่น ๆ ซึ่งผู้ประกอบการธุรกิจมีหน้าที่ควบคุมดูแลบุคคลที่อยู่ในความดูแลของตนมิให้มีการละเมิดนโยบายต่าง ๆ ของบริษัท จึงควรมีแค่มาตรการทางแพ่งและมาตรการทางปกครองก็เป็นการเพียงพอ

เพราะฉะนั้น เมื่อเปรียบเทียบกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 ในการจัดให้มีการแยกข้อมูลที่ละเอียดอ่อนออกจากหลักการทั่วไปอย่างเหมาะสม ในด้านวิธีปฏิบัติการรักษาความมั่นคงปลอดภัยของข้อมูลที่มีประสิทธิภาพ เพื่อให้ผู้เป็นเจ้าของข้อมูลได้รับการคุ้มครองข้อมูลส่วนบุคคลประเภทพิเศษที่ควรได้รับการปกป้องที่สูงกว่าข้อมูลทั่วไป ในการที่จะถูกถูกละเมิดที่สำคัญเฉพาะที่มีความเสี่ยงสูง ที่อาจก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลที่จำเป็นและเพื่อให้เกิดความตระหนัก เมื่อมีการประมวลผลผู้ควบคุมข้อมูลควรทำการตรวจสอบ อย่างไรก็ตาม ตามบทบัญญัติของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 ในปัจจุบันยังมิได้กำหนดให้จำแนกข้อมูลไบโอเมตริกซ์ให้ได้รับความคุ้มครองอยู่ในหมวดหมู่

ประเภทพิเศษ ซึ่งเป็นข้อมูลที่ละเอียดอ่อนออกจากข้อมูลทั่วไป ให้มีความสอดคล้องกับวิธีปฏิบัติตามแนวสากลและให้เกิดความตระหนักถึงความมั่นคงปลอดภัยในประเภทข้อมูลพิเศษต้องห้ามประมวลผล เว้นแต่ กฎหมายได้บัญญัติให้กระทำได้ โดยการแก้ไขดังต่อไปนี้

ผู้วิจัยเห็นควร ให้มีการกำหนดบทบัญญัติเรื่องผู้ให้บริการ หรือ ผู้ควบคุม หรือเจ้าของข้อมูลส่วนบุคคล ควรทราบข้อมูลประเภทพิเศษซึ่งมีความละเอียดอ่อน เพื่อให้มีมาตรการในทางปฏิบัติที่สำคัญอย่างยิ่งที่ผู้ควบคุมข้อมูลจะต้องมีระยะเวลาเพียงพอในการประเมินความเสี่ยงอย่างถี่ถ้วน เพื่อกำหนดขอบเขตของความเสี่ยงต่อความมั่นคงปลอดภัยและป้องกันมิให้มีการเปิดเผยข้อมูลประเภทข้อไบโอเมตริกซ์ ตามมาตร 26 โดยบัญญัติให้ “ข้อมูลพันธุกรรม และข้อมูลไบโอเมตริกซ์เป็นข้อมูลที่มีความอ่อนไหวง่ายต้องได้รับการคุ้มครองเป็นข้อมูลประเภทพิเศษจำแนกต่างหากออกจากข้อมูลส่วนบุคคลทั่วไป” ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล โดยคำนึงถึงลักษณะของข้อมูลและความเสี่ยงที่จะเกิดขึ้นจากการประมวลผลสำหรับข้อมูล และสิทธิของบุคคลเพื่อรักษาความสมบูรณ์และความลับของข้อมูลประเภทพิเศษที่อ่อนไหวง่าย

บทสรุป

จากการศึกษาประเด็นที่ได้กล่าวมาแล้วตามข้อ 4.1- 4.4 ผู้วิจัยพบว่าเมื่อศึกษาเปรียบเทียบกับกฎหมายต่างประเทศ เช่น สหภาพยุโรป ข้อมูลส่วนบุคคลได้หมายความรวมถึง (Biometric Data) ไว้อย่างชัดเจน โดยกฎหมายได้อธิบายการใช้เทคโนโลยี (Biometrics) เพื่อให้ได้ข้อมูลส่วนบุคคลทั้งในเชิงกายภาพและพฤติกรรม รวมถึงคุณลักษณะต่าง ๆ ที่สามารถจำแนกลักษณะเฉพาะของแต่ละบุคคลได้ ดังนั้น จึงเป็นข้อมูลส่วนบุคคล ที่ได้รับความคุ้มครองภายใต้กฎหมายข้อมูลส่วนบุคคลของประเทศในกลุ่มสหภาพยุโรป โดย “ข้อมูลพันธุกรรม และ ข้อมูลไบโอเมตริกซ์” เป็นข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนและอ่อนไหวง่าย ได้ให้ความสำคัญในการคุ้มครอง ใน “หมวดหมู่พิเศษของข้อมูลส่วนบุคคล” และอยู่ภายใต้ข้อจำกัด ซึ่งต้องบัญญัติจำแนกต่างหากออกจากข้อมูลทั่วไปให้อย่างชัดเจน เพื่อมิให้เกิดการตีความในทางปฏิบัติจริงของการบัญญัติคำนิยามศัพท์

แม้ว่า “ข้อมูลพันธุกรรม” จะถูกบัญญัติไว้ในข้อมูลส่วนบุคคลไว้ในหมวดหมู่ข้อมูลทั่วไปก็ตาม Regulation (EU) 2016/679 Article 4 และ Regulation (EU) 2018/1725 Article 3 ซึ่งเมื่อพิจารณาถึงคำนิยามศัพท์ตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มิได้บัญญัติคำนิยามศัพท์ “ข้อมูลพันธุกรรม และ ข้อมูลไบโอเมตริกซ์” ไว้ในหมวดคำนิยามศัพท์แต่อย่างใด รวมถึงความชัดเจนในการคุ้มครองข้อมูลไว้ในหมวดหมู่ประเภทข้อมูลพิเศษเฉพาะในฐานะข้อมูลที่มีความอ่อนไหวง่าย แต่อย่างไรก็ตาม ข้อมูลไบโอเมตริกซ์ได้ถูกบัญญัติไว้ในตาม 26 ห้ามมิให้เก็บรวบรวมข้อมูลเกี่ยวกับ “ข้อมูลพันธุกรรม และ ข้อมูลไบโอเมตริกซ์” โดยพบว่า “ข้อมูลพันธุกรรม

และ ข้อมูลไบโอเมตริกซ์” นั้นได้รับการความคุ้มครองเป็นการทั่วไปเช่นเดียวกับข้อมูลทั่วไป ฉะนั้นอาจต้องทำให้เกิดการตีความว่าเป็นข้อมูลทั่วไปหรือไม่ อย่างไร ในทางปฏิบัติจริงเมื่อมีการละเมิดข้อมูลประเภทพิเศษดังกล่าว ที่จะต้องตั้งอยู่บนพื้นฐานของความยินยอมพร้อมแจ้งผลกระทบในการถอนความยินยอม ตามมาตรา 19 วรรคหก แห่งพระราชบัญญัติคุ้มรองข้อมูลส่วนบุคคล พุทธศักราช 2562

แม้ปรากฏว่ากฎหมายไทยได้บัญญัติหลักการขอความยินยอมไปในทิศทางเดียวกับกฎหมาย (GDPR) ก็ตาม แต่ยังไม่มีความชัดเจนในการใช้ลักษณะของ (Active consent) เช่น ในคดี C-673/17 ศาลยุติธรรมแห่งสหภาพยุโรป ตัดสินว่าการขอความยินยอมให้ใช้คุกกี้ (Cookies) บนเว็บไซต์ของผู้ให้บริการโดยใช้ (Pre-ticked checkbox) นั้น ไม่ชอบด้วยกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยการให้ความยินยอมนั้นต้องเป็นความยินยอมโดยอิสระ ชัดเจน และได้รับแจ้งข้อมูลที่เพียงพอต่อการตัดสินใจ ไม่สร้างความสับสนหลงผิด และต้องมีการแสดงออกของการกระทำโดยชัดแจ้งว่ามีการให้ความยินยอม (Active consent) โดยหากเป็นกรณีที่ได้เลือกมาให้แล้ว (Pre-select tick) กรณีเช่นนี้ ถือไม่ได้ว่าได้มีการให้ความยินยอมก่อน ซึ่งจากคดีข้างต้นทำให้เข้าใจได้ว่า การใช้ “คุกกี้” ที่ฝังมาในอุปกรณ์ต่าง ๆ บนเว็บไซต์ต้องขอความยินยอมและความยินยอมนั้นต้องชอบด้วยเงื่อนไขของกฎหมายด้วย อีกทั้งหลักเกณฑ์และนโยบายเกี่ยวกับระยะเวลาการเก็บข้อมูลส่วนบุคคลว่า “ข้อมูลส่วนบุคคลจะเก็บไว้ไม่เกินภายใน 6 เดือน ให้ทำลายทันที หรือสิ้นสุดตามวัตถุประสงค์ทางธุรกิจ หรือตามข้อตกลงของสัญญา” สิทธิในการขอลบข้อมูลที่เกี่ยวกับตนในระบบออนไลน์ (Right to erase) หรือสิทธิที่จะถูกลืมภายหลังที่ลบในระบบออนไลน์ (Right to be forgotten) เพื่อมุ่งเน้นไปที่การคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสมและเพียงพอ

เมื่อพิจารณาถึงการกำหนดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสมและสอดคล้องกับการรักษาความลับของข้อมูลส่วนบุคคลในประเทศไทย เพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล การพิสูจน์ตัวตนแบบเทคนิคไบโอเมตริกซ์ซึ่งกำลังได้รับความนิยมเป็นอย่างสูง แต่ก็มาพร้อมกับความท้าทายในที่จะการปกป้องความเสี่ยง และปัจจัยที่สำคัญที่สุดที่ต้องพิจารณาก่อนนำระบบไบโอเมตริกซ์มาใช้เพื่อปฏิบัติตามข้อกำหนดทางกฎหมายคุ้มครองข้อมูลส่วนบุคคล แต่อย่างไรก็ตาม พบว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พุทธศักราช 2562 ฉบับปัจจุบันยังพบปัญหาในกรณีคำนิยามศัพท์ “ข้อมูลพันธุกรรม และ ข้อมูลไบโอเมตริกซ์” ยังไม่มีความชัดเจนและครอบคลุมเพียงพอ แต่อย่างใด ในการให้ความคุ้มครองข้อมูลดังกล่าวข้างต้น จึงอาจก่อให้เกิดความเสี่ยงที่จะถูกละเมิดและอาจต้องใช้ดุลยพินิจตีความเป็นการทั่วไปได้ หรือไม่อย่างไร เมื่อศึกษาเปรียบเทียบกับการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป สหรัฐอเมริกา และสหพันธ์รัฐสาธารณรัฐเยอรมนีแล้วนั้น เนื่องจากสหภาพยุโรป

(European Union: EU) ได้ออก (General Data Protection Regulation) โดยเป็นกฎหมายที่ให้ความคุ้มครองข้อมูลส่วนบุคคลได้บังคับใช้เมื่อวันที่ 25 พฤษภาคม พุทธศักราช 2561

นอกจากนี้ ยังมีผลบังคับใช้แก่การส่งข้อมูลภายในประเทศสมาชิกสหภาพยุโรปแล้ว ผู้ประกอบการในไทยที่ต้องติดต่อ รับส่งข้อมูลส่วนบุคคลของประชาชนในประเทศที่เป็นสมาชิกสหภาพยุโรป (Cross-Border Data Transfer Issues) ก็ต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมและเพียงพอเช่นเดียวกันด้วย พบว่า สหภาพยุโรปได้ให้ความสำคัญในการคุ้มครอง “ข้อมูลพันธุกรรม และ ข้อมูลไบโอเมตริกซ์” ต้องห้ามประมวลผล เว้นแต่ ได้รับความยินยอมเป็นอักษรก่อน และแยกข้อมูลที่ละเอียดอ่อนออกจากข้อมูลทั่วไปอย่างชัดเจน จัดให้รับการคุ้มครองอยู่ใน “หมวดหมู่พิเศษ” และเจ้าของข้อมูลต้องให้ความยินยอมก่อน (Consent) ในการเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ผู้เก็บรวบรวม ที่ผู้ใช้ แจ้งไว้ตั้งแต่แรกแล้วเท่านั้น กล่าวคือ ต้องขออนุมัติจากผู้เป็นเจ้าของข้อมูลก่อน เช่น หากแอพพลิเคชั่นหนึ่งจะเก็บข้อมูลไบโอเมตริกซ์ของบุคคลไว้ในระบบ ก็ต้องมีข้อความให้บุคคลนั้นกดยืนยันเพื่อยินยอม พร้อมแจ้งวัตถุประสงค์ในการเก็บรวบรวม และการใช้ หากบุคคลนั้นไม่ยินยอมให้ใช้ข้อมูล ผู้ให้บริการแอพพลิเคชั่นนั้น ก็ไม่สามารถใช้ข้อมูลของผู้ใช้บริการได้ ผู้ให้บริการเก็บรวบรวมข้อมูลต้องรักษาความมั่นคงปลอดภัยของข้อมูล ไม่ให้มีการเปลี่ยนแปลงแก้ไข หรือถูกเข้าถึงโดยผู้ที่ไม่เกี่ยวข้องกับข้อมูล จะต้องเก็บข้อมูลให้เป็นความลับ และไม่เปิดเผยให้กับผู้อื่น เจ้าของข้อมูลมีสิทธิถอนความยินยอม ขอให้ลบ หรือทำลายข้อมูลเมื่อใดก็ได้ หากเป็นความประสงค์ของเจ้าของข้อมูล โดยผู้ให้บริจะต้องแจ้งผลกระทบจากเหตุการณ์ถอนนั้น “ก่อนล่วงหน้าที่จะให้ความยินยอม” นั้น ทั้งนี้ ก็เพื่อป้องกันความเสี่ยงที่จะมีผลกระทบไปถึงการรักษาความลับ(Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคลที่ก่อให้เกิดแนวโน้มให้เกิดผลกระทบเชิงลบ หรือความเสียหายในระดับบุคคล หรือ องค์กร และมาตรการในการกำหนดโทษจะมีเฉพาะโทษทางปกครองและโทษปรับเท่านั้น จากประเด็นปัญหาดังที่ได้กล่าวมาข้างต้นแล้วนั้น จึงนำไปสู่ข้อเสนอแนะที่ผู้ศึกษาจะได้นำเสนอในบทต่อไป