

ความท้าทายในการจัดเก็บข้อมูลโดยการใช้เทคโนโลยีชีวมาตรกับมิติของ
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลปี 2562
THE CHALLENGES IN DATA COLLECTION USING BIOMETRIC
TECHNOLOGY WITH DIMENSION OF THE PERSONAL DATA
PROTECTION ACT 2019

สุพล พรหมมาพันธุ์

ผู้ช่วยศาสตราจารย์ สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสาร

คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม

E-mail: supon.ph@spu.ac.th

อำนาจ วังจิ้น

ผู้ช่วยศาสตราจารย์ สำนักวิชาศึกษาทั่วไป มหาวิทยาลัยศรีปทุม

E-mail: amnart.va@spu.ac.th

บทคัดย่อ

เนื่องด้วยปัจจุบัน เทคโนโลยีสารสนเทศมีการเปลี่ยนแปลงไปอย่างรวดเร็ว การจัดเก็บข้อมูลส่วนบุคคล มีหลายช่องทาง หลากหลายวัตถุประสงค์ โดยเฉพาะการจัดเก็บข้อมูลโดยการใช้เทคโนโลยีชีวมาตร ได้แก่ การจัดเก็บลายพิมพ์นิ้วมือ ภาพถ่าย ฝ่ามือ ม่านตา ใบหน้า เสียงพูด ลายเซ็น ดีเอ็นเอ เป็นต้น ดังนั้น จึงเป็นความท้าทายอย่างมาก และอาจมีความเสี่ยงต่อการละเมิดสิทธิส่วนบุคคล เพราะพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลปี 2562 ได้มีผลบังคับใช้แล้ว เมื่อวันที่ 1 มิถุนายน พ.ศ.2565 บทความนี้มีวัตถุประสงค์ คือ (1) เพื่อศึกษาถึงวัตถุประสงค์ในการจัดเก็บข้อมูลส่วนบุคคลโดยการใช้เทคโนโลยีชีวมาตร, (2) เพื่อวิเคราะห์ถึงความท้าทายของการใช้เทคโนโลยีชีวมาตรกับมิติของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ปี พ.ศ. 2562, (3) เพื่อให้บุคคลทั่วไปรู้จักวิธีการปกป้องข้อมูลส่วนบุคคลและความมั่นคงปลอดภัยของสารสนเทศ, และ (4) เพื่อป้องกันบุคคลและองค์กรไม่ให้กระทำการผิดกฎหมาย หลังจากได้ทำการศึกษาวิเคราะห์แล้ว สรุปว่า หน่วยงานของรัฐบาล และภาคธุรกิจควรจัดเก็บข้อมูลส่วนบุคคลเฉพาะเท่าที่จำเป็นเท่านั้น พร้อมทั้งควรมีมาตรการการรักษาความมั่นคงปลอดภัยที่ดีด้วย

คำสำคัญ: ความเป็นส่วนตัว, ข้อมูลส่วนบุคคล, เทคโนโลยีชีวมาตร, ความมั่นคงปลอดภัย

ABSTRACT

Because of the present Information Technology has changed rapidly. There are many ways to collect Personal Information, various purposes especially for data storage using Biometric Technology, including storing fingerprints, photographs, palms, iris, faces, speech, signatures, DNA, etc. So it's a huge challenge of government

agencies and businesses, and may be at risk of infringing on privacy rights. Because, the Personal Data Protection Act of 2019 came into effect on June 1, 2022. The objectives are: (1) To study the purpose of collecting personal data by using Biometric Technology, (2) To analyze the challenges of using Biometric Technology with dimension of the Personal Data Protection Act of 2019, (3) To make the public know how to protect personal information and information security, and (4) To prevent individuals and organizations from committing illegal acts. After analyzing the study, it was concluded that government agencies and the business sector should only store personal data as needed and should have good security measures as well.

Keywords: Privacy, Personal Data, Biometric Technology, Security

1. บทนำ

เนื่องด้วยการจัดเก็บข้อมูลส่วนบุคคลในปัจจุบันมีการเก็บข้อมูลกันผ่านทางอุปกรณ์หลายช่องทาง เช่น สมาร์ทโฟน, คอมพิวเตอร์ส่วนบุคคล, กล้องวงจรปิด, เซ็นเซอร์, เครื่องสแกน เป็นต้น และมีหลากหลายวัตถุประสงค์ด้วยกัน เช่น หน่วยงานรัฐบาล มีการจัดเก็บข้อมูลเพื่อนำมาใช้ในการสนับสนุนการขับเคลื่อนทางเศรษฐกิจ เช่น การจัดทำบัตรสวัสดิการแห่งรัฐ เป็นต้น ส่วนภาคธุรกิจ มีการจัดเก็บข้อมูลเพื่อใช้ประโยชน์ในการตัดสินใจดำเนินธุรกิจ เช่น การอนุมัติสินเชื่อ เป็นต้น ข้อมูลส่วนบุคคล คือ ข้อมูลเกี่ยวกับบุคคลที่สามารถระบุตัวบุคคลนั้นได้ ทั้งทางตรงหรือทางอ้อม แต่จะไม่นับรวมข้อมูลของผู้ที่เสียชีวิตไปแล้ว ข้อมูลส่วนบุคคล ได้แก่ ชื่อ-นามสกุล หรือชื่อเล่น / เลขประจำตัวประชาชน, เลขหนังสือเดินทาง, เลขบัตรประกันสังคม, เลขใบอนุญาตขับขี่, เลขประจำตัวผู้เสียภาษี, เลขบัญชีธนาคาร, เลขบัตรเครดิต, ที่อยู่, อีเมล, เลขโทรศัพท์ เป็นต้น ในเว็บไซต์วิกิพีเดีย สารานุกรมเสรี (2565) ได้แสดงให้เห็นว่า ข้อมูลส่วนบุคคลมักเป็นข้อมูลที่ไม่ได้ใช้ในการแยกแยะอัตลักษณ์ แต่หากนำมาใช้รวมกันก็อาจชี้เฉพาะตัวบุคคลได้เช่นกัน ได้แก่ ประเทศ รัฐ หรือเมืองที่มีถิ่นฐานพำนักอยู่ อายุ เพศหรือเชื้อชาติ สถานศึกษา หรือสถานที่ทำงาน เงินเดือนเงินจ้าง หรือตำแหน่งหน้าที่การทำงาน ประวัติอาชญากรรม เมื่อบุคคลไม่ประสงค์ออกนาม การกล่าวถึงบุคคลนั้น มักจะประกอบด้วยข้อมูลข้างต้นสองหรือสามประการ เช่น “ผู้ชายอายุ 34 ปีที่ทำงานในห้างสรรพสินค้า X” ลักษณะเช่นนี้ เป็นการเปิดเผยข้อมูลส่วนบุคคลบางส่วน แต่ไม่ถึงกับทำให้สาธารณชนแยกแยะตัวบุคคลที่ถูกกล่าวถึงได้ว่าเป็นใคร อย่างไรก็ตามหากมีข้อมูลมากขึ้นอาจทำให้แยกแยะตัวบุคคลได้ โดยเฉพาะในคดีอาชญากรรม จึงได้มีการเสนอหลักฐานข้อมูลหลายประการที่บ่งบอกถึงตัวอาชญากร ในปี ค.ศ.1990 ได้มีการแสดงให้เห็นว่า ประชาชนชาวอเมริกัน 87% สามารถถูกระบุเฉพาะเจาะจงได้ด้วยเพียง เพศ รหัสไปรษณีย์ และวันเกิด

เทคโนโลยีชีวมาตร (Biometric Technology) คือ แนวคิดการนำเอาเทคโนโลยีด้านชีวภาพทางการแพทย์และเทคโนโลยีด้านคอมพิวเตอร์มาบูรณาการเข้าด้วยกัน เพื่อใช้กำหนดหรือระบุคุณลักษณะเฉพาะส่วนบุคคลทั้งด้านกายภาพ และพฤติกรรม ได้แก่ ลายพิมพ์นิ้วมือ ภาพถ่าย ฝ่ามือ ม่านตา ใบหน้า เสียงพูด ลายเซ็น ดีเอ็นเอ เป็นต้น เพื่อใช้ประโยชน์ในการจัดเก็บข้อมูลกิจกรรมหลายอย่าง เช่น การทำบัตรประจำตัวประชาชน การทำหนังสือเดินทาง เป็นต้น

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลปี พ.ศ. 2562 ได้ประกาศใช้ในราชกิจจานุเบกษาเมื่อวันที่ 24 พฤษภาคม พ.ศ. 2562 และมีผลบังคับใช้โดยสมบูรณ์ เมื่อวันที่ 1 มิถุนายน พ.ศ.2565 เหตุผลในการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลนั้น เป็นมิติที่ท้าทายอย่างยิ่ง เนื่องจากปัจจุบันมีการล่วงละเมิดสิทธิ

ความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมาก จนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การจัดเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวก และรวดเร็ว ก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวม สมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้น เพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป สำหรับข้อมูลชีวมาตรนี้ นายแพทย์สุธี ทวีรัตน์ (2565) ได้กล่าวถึงความหมายของ “ชีวมาตร” เรื่อง เทคโนโลยีระบุตัวตนว่า “ชีวมาตร” น่ากลัวหรือไม่ โดยกล่าวเอาไว้ว่า “ชีวมาตร” หรือ ไบโอมेटริกซ์ คือ ข้อมูลส่วนบุคคลที่เป็นเทคโนโลยีในการระบุตัวตน ได้แก่ 1. ภาพถ่าย 2. ลายนิ้วมือ และ 3. ม่านตา ซึ่ง “หน้าตา” เปลี่ยนได้ แต่ซ้ำเป็นเหตุผลให้ต้องทำบัตรประชาชนใหม่ทุก 5 ปี ทว่า “ลายนิ้วมือ” คือเซลล์ที่ตายของผิวหนังจึงไม่เปลี่ยนแปลง ส่วน “ม่านตา” เป็นอวัยวะที่ไม่ได้บอกแก่เพียงลักษณะ แต่ยังบอกถึงสุขภาพ พฤติกรรม และ โรคทางพันธุกรรม ได้หลายโรคอีกด้วย

2. วัตถุประสงค์

- (1) เพื่อศึกษาถึงวัตถุประสงค์ในการจัดเก็บข้อมูลส่วนบุคคลโดยการใช้เทคโนโลยีชีวมาตร
- (2) เพื่อวิเคราะห์ถึงความท้าทายของเทคโนโลยีชีวมาตรกับมิติของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ปี พ.ศ. 2562
- (3) เพื่อให้บุคคลทั่วไปรู้จักวิธีการปกป้องข้อมูลส่วนบุคคลและความมั่นคงปลอดภัยของสารสนเทศ
- (4) เพื่อป้องกันบุคคลและองค์กรไม่ให้กระทำการผิดกฎหมาย

3. หัวข้อ (1) วัตถุประสงค์ในการจัดเก็บข้อมูลส่วนบุคคลโดยการใช้เทคโนโลยีชีวมาตร

ในการจัดเก็บข้อมูลด้วยวิธีนี้มีวัตถุประสงค์ เพื่อก่อให้เกิดความปลอดภัยสูงสุด และเพื่อใช้ประโยชน์ในการยืนยันตัวตน เช่น (1) เพื่อการขอรับบริการจากภาครัฐ (2) เพื่อทำหนังสือเดินทาง (3) เพื่อประโยชน์ทางธุรกิจ เป็นต้น การจัดเก็บข้อมูลส่วนบุคคล โดยการใช้เทคโนโลยีชีวมาตรนี้ ควรจัดเก็บเฉพาะเท่าที่มีความจำเป็นเท่านั้น ไม่ควรจัดเก็บแบบพร่ำเพรื่อ เช่น ควรจัดเก็บเฉพาะภาพถ่าย ลายพิมพ์นิ้วมือเท่านั้น ไม่ควรจัดเก็บม่านตา และ DNA เพราะอาจจะเข้าข่ายการละเมิดความเป็นส่วนตัว หรือสิทธิส่วนบุคคลได้ สำหรับการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยนั้น มีตราไว้หลายแห่ง เช่น ในรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 มาตรา 32 ระบุว่า “บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว การกระทำอันเป็นการละเมิดหรือกระทบต่อสิทธิของบุคคลตามวรรคหนึ่ง หรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใด ๆ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ” สำหรับเทคโนโลยีชีวมาตร ที่ได้รับความนิยมอย่างแพร่หลายในปัจจุบันมีหลายประเภทในหนังสือของ Gary B. Shelly (2020) ได้เขียนเอาไว้ ดังนี้ คือ

(1) เครื่องสแกนลายพิมพ์นิ้วมือ (Fingerprint Scanner) ในปัจจุบันมีการนำเอาเครื่องสแกนลายพิมพ์นิ้วมือเข้าไปใช้กันเป็นจำนวนมาก โดยเฉพาะเกี่ยวกับเรื่องการชำระเงิน ธุรกิจขนาดเล็ก ร้านขายของชำ และร้านขายปลีก เป็นต้น ศรัณย์ สัมฤทธิ์เดชขจร (2565) นักวิจัยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (เนคเทค) กล่าวว่าโดยทั่วไปแล้วการสแกนลายนิ้วมือ อาจแบ่งได้ 3 ลักษณะได้แก่ เซ็นเซอร์ประจุไฟฟ้า เซ็นเซอร์อุณหภูมิ และเซ็นเซอร์แสง เทคโนโลยีสองแบบแรกผู้ใช้ต้องแตะไปที่เซ็นเซอร์โดยตรง ทำให้อายุการใช้งานสั้น

และมีปัญหาเรื่องการบำรุงรักษา โดยในต่างประเทศที่มีอากาศหนาวจะเกิดไฟฟ้าสถิตทำลายเซ็นเซอร์ได้ ขณะที่ระบบแสงจะทนกว่าและมีคุณสมบัติรวมของเทคโนโลยีอื่นมาไว้ด้วยหลักการทำงานของเซ็นเซอร์แสง คือ การสะท้อนกลับหมดของแสงด้วยการอาศัยแสงสีแดงส่องลายนิ้วมือที่วางอยู่บนเลนส์สะท้อนกลับตัวหัว เซ็นเซอร์เช่นเดียวกับการใช้นิ้วจับแก้วที่มีน้ำอยู่ภายใน ซึ่งการสะท้อนของแสง ทำให้เรามองลายนิ้วมือได้อย่างชัดเจนและมีผลสรุปทางวิทยาศาสตร์กล่าวว่า มนุษย์ชาติจำนวน 600 ล้านคน เมื่อผ่านมาเป็นระยะเวลา 300 ปี จะมีโอกาสที่ลายนิ้วมือซ้ำกันเพียง 1 คู่ ในส่วนของทารกเมื่ออยู่ในครรภ์มารดาเป็นเวลา 7 เดือนก็มีลายนิ้วมือเป็นของตัวเอง ครั้นเมื่อโตใหญ่ขึ้นเป็นผู้ใหญ่ลายนิ้วมือก็ไม่ได้เปลี่ยนแปลง



รูปภาพที่ 1 และ 2 เครื่องสแกนลายนิ้วมือตรวจสอบการพิสูจน์ตัวตนของนักท่องเที่ยวยุคใหม่ การตรวจจับใบหน้า การสแกนลาย พิมพ์นิ้วมือ และการสแกนม่านตา (Iris) เพื่อการทำธุรกรรมด้านการเงิน เช่น บัตร ATM (Gary B. Shelly 2020: 567)

(2) ระบบเครื่องจดจำใบหน้า (A Face Recognition Systems) โดยระบบนี้จะดึงรูปภาพของใบหน้า และทำการเปรียบเทียบกับรูปภาพจริงของผู้ใช้ที่ถูกต้องตามกฎหมาย ระบบการจดจำใบหน้านี้ถูกพัฒนาขึ้นมาใช้เพื่อรักษาความปลอดภัยของบุคคลผู้ที่เดินเข้าออกในห้างงาน, การดำเนินการกับผู้กระทำความผิดทางกฎหมาย, การตรวจตรารักษาความปลอดภัย และการใช้การจดจำใบหน้าของบุคคลที่ผ่านเข้าออกตามสนามบินเพื่อป้องกันความปลอดภัย เทคโนโลยีชนิดนี้มีความชาญฉลาดมาก มันสามารถที่จะจดจำคนได้ทั้งคนที่สวมแว่นตา และไม่ได้สวมแว่นตา คนที่ไปทำศัลยกรรมตกแต่งใบหน้า หรือคนที่สวมใส่เครื่องประดับ และแม้กระทั่งคนที่ปรับเปลี่ยนทรงผมใหม่ หรือใส่วิกผมปลอมก็ตาม

(3) ระบบการจดจำม่านตา (Iris Recognition System) เป็นระบบรักษาความปลอดภัยที่มีประสิทธิภาพสูงมาก โดยจะมีกล้องสำหรับถ่ายรูปร่ม่านตาของคน และอ่านจดจำบันทึกเปรียบเทียบรูปแบบของม่านตาที่ถูกจัดเก็บไว้ในคอมพิวเตอร์เช่นเดียวกับการพิมพ์ลายนิ้วมือ ระบบนี้ส่วนใหญ่มักใช้ในการรักษาความปลอดภัยในหน่วยงานของรัฐบาล เช่น ในกองทัพ รวมถึงสถาบันทางการเงิน ในมลรัฐเท็กซัสมีการใช้เทคโนโลยีนี้ในการทำบัตร ATM ให้กับลูกค้าและสามารถเบิกถอนเงินสดได้อย่างรวดเร็ว

4. หัวข้อ (2) เพื่อศึกษาวิเคราะห์ถึงความท้าทายของเทคโนโลยีชีวมาตรกับมิติของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ปี 2562

ในการจัดเก็บบันทึกข้อมูลส่วนบุคคล หรือข้อมูลส่วนตัวด้วยเทคโนโลยีชีวมาตรนั้น นับว่าเป็นความท้าทายอย่างยิ่ง เพราะอาจมีความเสี่ยงในการละเมิดสิทธิส่วนบุคคล และมีข้อมูลบางชนิดเป็นข้อมูลที่อ่อนไหว ถูกนิยามว่า ไซเบอร์ (2565) ได้กล่าวไว้ว่า ข้อมูลส่วนบุคคลที่มีความอ่อนไหว มีปรากฏในมาตรา 6 ได้แก่ ข้อมูลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนา หรือปรัชญา พฤติกรรมทางเพศ

ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดที่คณะกรรมการประกาศกำหนด บุคคลที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล ได้แก่ (1) เจ้าของข้อมูลส่วนบุคคล, (2) ผู้ควบคุมข้อมูลส่วนบุคคล, (3) ผู้ประมวลผลข้อมูลส่วนบุคคล, และ (4) เจ้าหน้าที่ที่คุ้มครองข้อมูลส่วนบุคคล

ค่านายแพทย์สุธี ทวีรัตน์ ได้เปิดเผยกับ “ฐานเศรษฐกิจ” ว่ากรณีธนาคารแห่งประเทศไทย (ธปท.) กำลังผลักดันให้มีการใช้ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital ID) โดยการนำเอาเทคโนโลยีชีวมาตร เช่น การจดจำใบหน้า ลายนิ้วมือ หรือม่านตา มาใช้ ในการพิสูจน์ยืนยันตัวตนบุคคลในการทำธุรกรรมทางการเงิน กำลังส่งผลกระทบต่อเงินฝากธนาคารคนไทย และมีโอกาสถูกแฮกเกอร์สวมรอยถอนหรือสั่งโอนไปจนเกลี้ยงบัญชีโดยไม่รู้ตัว ทั้งยังไม่สามารถที่จะเรียกร้องความรับผิดชอบจากธนาคารได้ ปัจจุบันมีการบังคับเก็บข้อมูลชีวมาตรประชาชน ได้แก่ ภาพถ่ายใบหน้า ลายนิ้วมือ 10 นิ้ว โดยหน่วยงานรัฐ เช่น การทำบัตรประชาชน หนังสือเดินทาง ลงทะเบียนซิมมือถือ เป็นต้น

บทความของสุพล พรหมมาพันธุ์ (2563) เขียนว่า ในเวทีเสวนาเมื่อวันศุกร์ที่ 12 กรกฎาคม พ.ศ.2562 เวลา 13.30.16.30 น. สมาคมความมั่นคงปลอดภัยสารสนเทศ และคณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม ร่วมกันจัดเสวนาประชาชน เรื่อง “การเก็บข้อมูลชีวมาตร (Biometrics) ของหน่วยงานรัฐกับการละเมิดสิทธิส่วนบุคคลและผลกระทบต่อความมั่นคงของประเทศ” โดยผู้ร่วมเสวนา เช่น อาจารย์ปริญญา หอมอนเนก ประธานและผู้จัดการ, ACIS Professional Center Co., Ltd. (ACIS), นพ.สุธี ทวีรัตน์ กรรมการสมาคมความมั่นคงปลอดภัยสารสนเทศ, พ.ต.อ.ญาณพล ยั่งยืน ณ ห้องพัชรกิติยาภา อาคารเฉลิมพระบารมี 50 ปี ซอยศูนย์วิจัย ด.เพชรบุรีตัดใหม่ กรุงเทพฯ อาจารย์ปริญญา หอมอนเนก (2562) กล่าวว่า ในประเทศไทย พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ปี 2562 ประกาศใช้แล้ว เมื่อวันที่ 24 พฤษภาคม พ.ศ.2562 ถ้าเป็นข้อมูลอีเมล, Facebook รั่วไหลยังสามารถแก้ไขได้ด้วยเปลี่ยน Password แต่ถ้าเป็นข้อมูลชีวมาตรเหล่านี้รั่วไหลแล้วจะทำอย่างไร เช่น ลายพิมพ์นิ้วมือ ฝ่ามือ ใบหน้า เรตินา ม่านตา (Iris) ลายเส้น ดีเอ็นเอ เสียง เป็นต้น ซึ่งข้อมูลเหล่านี้รั่วไหลแล้วไม่สามารถนำกลับมาได้ แก้ไขได้ยากอีกด้วย



รูปภาพที่ 3 การเสวนาประชาชน เรื่อง “การเก็บข้อมูลชีวมาตร (Biometrics) ของหน่วยงานรัฐกับการละเมิดสิทธิส่วนบุคคลและผลกระทบต่อความมั่นคงของประเทศ” (<https://www.spu.ac.th/activities>: 2019)

นายแพทย์สุธี ทวีรัตน์ กล่าวว่า มี 2 เรื่องหลัก คือ (1) หนังสือเดินทาง (Passport) รุ่นใหม่ของประเทศไทย โดยกระทรวงการต่างประเทศ ซึ่งแต่เดิมมีการเก็บข้อมูลทั้งภาพถ่าย และลายพิมพ์นิ้วมือสิบนิ้ว แต่ต่อไปนี้จะมีการเก็บข้อมูลชีวมาตรม่านตา (Iris) ด้วย ซึ่งทางกระทรวงฯ ได้ให้เหตุผลว่า การเก็บข้อมูลชีวมาตรดังกล่าวเป็นคุณลักษณะความปลอดภัยสูงสุดในการป้องกันการปลอมแปลงหนังสือเดินทาง ซึ่งแตกต่างจากประเทศอื่น เช่น สหรัฐอเมริกาเก็บเฉพาะข้อมูลภาพถ่ายอย่างเดียว ไม่ให้เก็บลายพิมพ์นิ้วมือ ในสหภาพยุโรป เก็บเฉพาะภาพถ่าย

และลายพิมพ์นิ้วมือเพียง 2 นิ้ว เช่น ประเทศเยอรมันนี่ มีการเก็บม่านตา ส่วนประเทศเนเธอร์แลนด์เก็บลายพิมพ์นิ้วมือ เป็นต้น (2) การลงทะเบียนชีวมาตรที่ด้วยวิธีอัตลักษณ์ คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) มีนโยบายการให้ลงทะเบียนชีวมาตรที่ทั้งการตรวจสอบใบหน้า และสแกนลายพิมพ์นิ้วมือทั่วประเทศ เมื่อเก็บข้อมูลเหล่านี้ไปแล้ว มันใจได้อย่างไรว่าข้อมูลไม่รั่วไหล แม้กระทั่งข้อมูลบัตรประชาชนของบุคคลสำคัญหลายคนถูกนำไปลงทะเบียนซ้ำกันหลายครั้ง เคยมีกรณีศึกษาตัวอย่างเรื่องการละเมิดข้อมูลส่วนบุคคล 2 เรื่อง คือ กรณีแรก เว็บไซต์ The standard (2565) รายงานว่า สายการบินบริติช แอร์เวย์ ในเครือบริษัท อินเทอร์เน็ตในชั้นเนล แอร์ไลน์ส กรุ๊ป (IAG) ถูกสำนักงานคณะกรรมการข้อมูลของสหราชอาณาจักร (ICO) ลงโทษปรับเงินเป็นจำนวน 183.39 ล้านปอนด์ (ประมาณ 7,069,820,000 บาท) สืบเนื่องจากกรณีการรั่วไหลของข้อมูลทางการเงิน และข้อมูลลูกค้า กรณีที่สอง หนังสือพิมพ์โพสต์ทูเดย์ (Post Today) (2565) รายงานว่า โรงแรม แมริออท (Marriott) อินเทอร์เน็ตในชั้นเนล เครือธุรกิจโรงแรมรายใหญ่ที่สุดในโลก โคนเน็กเกอร์เจาะระบบดึงข้อมูลลูกค้า 500 ล้านคน นับตั้งแต่ปี 2014 และอาจต้องจ่ายค่าปรับสูงถึง 200 ล้านดอลลาร์ ท้ายสุด นพ.สุธี ทวีรัตน์ ได้มีข้อเสนอแนะต่อทางรัฐบาลดังนี้ คือ (1) รัฐควรจะหลีกเลี่ยงการบังคับเก็บข้อมูลชีวมาตรของประชาชน เก็บเท่าที่จำเป็นจริงๆ (2) รัฐควรจะต้องกำกับดูแลมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ และคุ้มครองข้อมูลส่วนบุคคลของข้อมูลชีวมาตร อย่างมีธรรมาภิบาลเปิดเผย โปร่งใส (3) รัฐไม่ควรจะยอมให้เอกชน เข้ามาบริหารจัดการฐานข้อมูลชีวมาตร และ (4) รัฐต้องมีมาตรการเยียวยาแก้ไขเจ้าของข้อมูลที่เกิดการรั่วไหล และได้รับความเสียหาย

สำหรับเรื่องการคุ้มครองข้อมูลส่วนบุคคลนี้ มีต้นแบบมาจากกฎหมายคุ้มครองข้อมูลส่วนบุคคล สิทธิของข้อมูลส่วนบุคคลของสหภาพยุโรป ซึ่งได้มีผลบังคับใช้เมื่อวันที่ 25 พฤษภาคม พ.ศ. 2561 ในรายงานวิจัยของฉุนกร และคณะ (2565) รายงานว่า สำหรับลักษณะของบันทึกตามกฎหมายต่างประเทศมีปรากฏอยู่ในกฎหมายของสหภาพยุโรป (European Union หรือ EU) ที่เรียกว่า GDPR (General Data Protection Regulation) เป็นกฎระเบียบที่ว่าด้วยการคุ้มครองบุคคลเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล และอิสระของการโอนข้อมูลข้ามพรมแดน ซึ่งบัญญัติรายละเอียดของบันทึกอยู่ในมาตรา 30 (1) ว่า “ผู้ควบคุมและตัวแทนของผู้ควบคุมมีหน้าที่เก็บรักษาบันทึกกิจกรรมการประมวลผลอันประกอบด้วยรายการดังต่อไปนี้ (A) ชื่อและข้อมูลที่ใช้ติดต่อกับผู้ควบคุมข้อมูล ตัวแทนของผู้ควบคุม และเจ้าหน้าที่คุ้มครองข้อมูล (B) วัตถุประสงค์ของการประมวลผล (C) ประเภทของข้อมูลส่วนบุคคลและเจ้าของข้อมูล (D) ประเภทของผู้รับหรืออาจได้รับข้อมูลส่วนบุคคล (E) มาตรการคุ้มครองข้อมูลส่วนบุคคลที่โอนไปนอกสหภาพยุโรปหรือองค์กรระหว่างประเทศ (F) ระยะเวลาสำหรับเก็บรักษาข้อมูลส่วนบุคคลแต่ละประเภท และ (G) มาตรการรักษาความปลอดภัยแก่ข้อมูลส่วนบุคคล”

บทความวิจัยของอัจจิมา มณฑาพันธุ์ (2565) เรื่อง “การวิเคราะห์ เปรียบเทียบการระบุตัวตน โดยการใช้ลักษณะเฉพาะทางกายภาพของร่างกาย” รายงานว่า เนื่องจากชีวมาตรเป็นสิ่งที่ติดมากับบุคคลตั้งแต่เกิดยากที่จะปลอมแปลง และจากการศึกษาข้อมูล วิเคราะห์เปรียบเทียบชีวมาตรที่เป็น ลักษณะเฉพาะทางกายภาพจำนวน 9 ประเภท ได้แก่ ลายนิ้วมือ ใบหน้า ม่านตา จอประสาทตา จมูก ใบหู ลายฝ่ามือ สารพันธุกรรม และคลื่นสมอง ทำให้สามารถ สรุปข้อดีและข้อเสียของการระบุตัวตนโดยการใช้ลักษณะเฉพาะทางกายภาพแต่ละประเภทได้ เช่น ข้อดีของลายนิ้วมือคือลายนิ้วมือจะไม่มีการเปลี่ยนแปลงรูปแบบตั้งแต่แรกเกิด จนถึงกระทั่งวันตาย แต่อาจมีการเปลี่ยนขนาดตามขนาดร่างกาย ลายนิ้วมือมีรูปแบบเฉพาะในแต่ละบุคคลจึงเป็นคุณสมบัติที่สำคัญในการระบุตัวตนได้เป็นอย่างดี

ในบทความวิจัยของบรรเจิด สิงคะเนติ และคณะ (2565) เรื่อง “กรณีการถ่ายภาพของผู้อื่นโดยผู้ที่ถูกถ่ายภาพนั้นไม่ได้ให้ความยินยอมและ นำไปพิมพ์เผยแพร่” รายงานว่า กรณีสื่อมวลชนถ่ายภาพผู้ที่ได้รับความเสียหายในคดีลวงละเมิดทางเพศ หรือ ใช้กล้องที่มีเลนส์ซูมภาพบุคคลอื่นให้เห็นใบหน้าของบุคคลนั้นในระยะใกล้ชิด แล้วนำไปตีพิมพ์เผยแพร่ในสื่อสิ่งพิมพ์ หรือกรณีบุคคลคอยติดตามถ่ายภาพบุคคลอื่นในลักษณะคุกคาม (ป้าปาราซี) โดยบุคคลผู้ถูกถ่ายภาพนั้นไม่ได้ให้ความยินยอม ซึ่งการกระทำดังกล่าวย่อมก่อให้เกิดความเสียหายแก่ผู้เสียหายในคดีลวงละเมิดทางเพศ หรือก่อให้เกิดความเดือนร้อนรำคาญแก่ผู้ถูกถ่ายภาพ และอาจก่อให้เกิดความไม่ปลอดภัยแก่ชีวิตร่างกายของผู้ถูกถ่ายภาพนั้นอีกด้วย

5. หัวข้อ (3). เพื่อให้บุคคลทั่วไปรู้จักวิธีการปกป้องข้อมูลส่วนบุคคล และความมั่นคงปลอดภัยของสารสนเทศ

สำหรับวิธีการปกป้องข้อมูลส่วนบุคคล สามารถทำได้ คือ (1) การเข้ารหัสลับ (Encryption) หรือรหัสผ่าน ซึ่งเกี่ยวข้องกับทฤษฎีของคณิตศาสตร์ ในการถ่ายโอนข้อมูลดิจิทัลถึงกัน และมีการแปลงรหัส มีการถอดรหัส เพื่อสร้างความความปลอดภัยให้เกิดขึ้นในระบบ เพื่อป้องกันไม่ให้ผู้อื่นสามารถล่วงรู้ได้ (2) กำแพงกันบุกรุกหรือไฟร์วอลล์ (Fire Walls) เป็นซอฟต์แวร์ชนิดหนึ่ง ซึ่งเป็นทฤษฎีของการควบคุมความปลอดภัยบนอินเทอร์เน็ต และเครือข่ายคอมพิวเตอร์ (Security Networks Software) ซอฟต์แวร์ชนิดนี้ ทำหน้าที่ในการตรวจสอบ และดูแลสัญญาณจราจรของการส่งข้อมูลบนเครือข่าย จะอนุญาตให้เฉพาะผู้มีสิทธิ์เท่านั้นเข้ามาใช้งานในเครือข่ายได้ (3) การสำรองเพิ่มข้อมูล (Backup Files) การสำรองเพิ่มข้อมูล เป็นการป้องกันเพิ่มข้อมูลเกิดการสูญหายหรือสูญหาย ได้แก่การทำสำเนาไว้หลายๆ ชุด เมื่อต้นฉบับเสียหาย สามารถใช้ชุดสำรองที่จัดทำไว้ได้

6. หัวข้อ (4). เพื่อป้องกันบุคคลและองค์กรไม่ให้กระทำการผิดกฎหมาย

การที่ได้ศึกษาเรื่องแนวทางการจัดเก็บข้อมูลส่วนบุคคล ด้วยเทคโนโลยีชีวมาตร นั้น ทำให้บุคคลและองค์กร ตระหนักถึงวิธีการจัดเก็บข้อมูลส่วนบุคคลที่ถูกต้อง เพื่อไม่ให้เสี่ยงต่อการละเมิดสิทธิส่วนบุคคล ส่วนตัว หรือสิทธิข้อมูลส่วนบุคคล เพราะว่าบทลงโทษทางกฎหมายนั้นรุนแรง ถ้าผู้กระทำความผิดเป็นนิติบุคคล กรรมการ / ผู้จัดการ / ผู้สั่ง / บุคคลที่รับผิดชอบในการดำเนินงาน / บุคคลที่มีหน้าที่สั่งการต้องระวางโทษในความผิดนั้นด้วย (มาตรา 81) สำหรับบทลงโทษ นั้นแบ่งเป็น 3 ด้าน คือ (1). มาตรการทางแพ่ง อัตราโทษ คือ จ่ายค่าเสียหายตามจริง สิ้นไหมทดแทนสูงสุด 2 เท่า ของค่าเสียหายตามจริง (อายุความ 3 ปี นับตั้งแต่วันที่รู้ตัว หรือ 10 ปี นับตั้งแต่ละเมิด) (2). มาตรการทางอาญา อัตราโทษจำคุกสูงสุด 1 ปี ปรับไม่เกิน 1,000,000 บาท หรือทั้งจำทั้งปรับ (ความผิดอันยอมความได้) (3). มาตรการทางปกครอง ปรับไม่เกิน 5,000,000 บาท

5. สรุป

ดังนั้น จะเห็นได้ว่า การจัดเก็บข้อมูลส่วนบุคคลด้วยเทคโนโลยีชีวมาตร ไม่ว่าจะเป็นการจัดเก็บลายพิมพ์นิ้วมือ ภาพถ่าย ฝ่ามือ ม่านตา ใบหน้า เสียงพูด ลายเซ็น ดีเอ็นเอ เป็นต้น นับว่าเป็นความท้าทายอย่างยิ่งหน่วยงานของรัฐบาล และภาคธุรกิจ รวมถึงบุคคลที่เกี่ยวข้องได้แก่ (1) เจ้าของข้อมูลส่วนบุคคล, (2) ผู้ควบคุมข้อมูลส่วนบุคคล, (3) ผู้ประมวลผลข้อมูลส่วนบุคคล, และ (4) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ควรจัดเก็บข้อมูลเท่าที่จำเป็นเท่านั้น เช่น ควรจัดเก็บเฉพาะลายพิมพ์นิ้ว ภาพถ่ายเท่านั้น ไม่ควรจัดเก็บข้อมูลทุกอย่าง เช่น ม่านตา

และ DNA เพราะอาจมีความเสี่ยงต่อการละเมิดความเป็นส่วนตัวส่วนตัวหรือสิทธิส่วนบุคคล เนื่องจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ปี 2562 มีผลบังคับใช้แล้ว ตั้งแต่วันที่ 1 มิถุนายน พ.ศ. 2565 เป็นต้นมา

6. ข้อเสนอแนะ

(1) หน่วยงานของรัฐบาล และภาคธุรกิจ ควรหลีกเลี่ยงการบังคับใช้ในการจัดเก็บข้อมูลส่วนบุคคลด้วยเทคโนโลยีชีวมาตร และควรจัดเก็บข้อมูลเท่าที่จำเป็นจะต้องใช้เท่านั้น และควรมีมาตรการเยียวยาแก้ไขให้กับเจ้าของข้อมูลส่วนบุคคลที่เกิดการรั่วไหล และได้รับความเสียหาย

(2) ทุกหน่วยงาน ควรมีมาตรการป้องกันกำกับดูแลความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเข้มแข็ง อย่าให้ข้อมูลรั่วไหล และมีหลักกรรมมาภิบาลที่โปร่งใสสามารถตรวจสอบได้

(3) รัฐบาลไม่ควรจะยอมให้หน่วยงานภาคเอกชน เข้ามาบริหารจัดการฐานข้อมูลชีวมาตร เพราะจะมีการเปลี่ยนแปลงบริษัทผู้ประมวลข้อมูลบ่อยครั้ง ซึ่งมีความเสี่ยงต่อการรั่วไหลของข้อมูลส่วนบุคคล นอกจากนี้ควรมีการเผยแพร่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ปี 2562 นี้ให้ทั่วถึง

7. เอกสารอ้างอิง

ณัฐพร วิริยะลัทปะ และคณะ. (2563). ปัญหาทางกฎหมายเกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.

2562 : ศึกษากรณีหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 39. *หนังสือประมวลบทความการประชุมนำเสนอผลงานวิจัยระดับบัณฑิตศึกษามหาวิทยาลัยรังสิต ครั้งที่ 15 ประจำปี 2563*, วันที่ 13 สิงหาคม 2563 ณ มหาวิทยาลัยรังสิต, 2195-2204.

ปริญญา หอมอนอก. (2562). *สไลด์การประกอบการบรรยายเรื่อง การจัดเก็บข้อมูลชีวมาตร (Biometrics) ของหน่วยงานรัฐกับการละเมิดสิทธิส่วนบุคคลและผลกระทบต่อความมั่นคงของประเทศ*, 2562.

บรรเจิด สิงคะเนติ และคณะ. (2565). *ปัญหาและมาตรการทางกฎหมายในการรับรอง และคุ้มครองสิทธิในความเป็นส่วนตัว (Right to privacy)*, [ออนไลน์]. สืบค้นเมื่อวันที่ 11 กันยายน 2565. หน้า 88-91. จาก <http://library.nhrc.or.th/ulib/document/Fulltext/F06924.pdf>

เดอะสแตนดาร์ด (Thestandard). (2565). *British Airways ถูกสั่งปรับเงินเป็นสถิติกว่า 7 พันล้านบาท จากกรณีข้อมูลลูกค้ารั่วไหล ในปี 2018*, [ออนไลน์]. สืบค้นเมื่อวันที่ 23 กันยายน 2565 จาก <https://thestandard.co/british-airways-fine-over-passenger-data-breach/>

โพสต์ทูเดย์ (Postoday). (2565). *"เมเรอท"อ่วม! เจอแฮ็กข้อมูลลูกค้า 500 ล้านราย ส่อเสียค่าปรับ 200 ล้านดอลลาร์*, [ออนไลน์]. สืบค้นเมื่อวันที่ 23 กันยายน 2565 จาก <https://www.postoday.com/world/572621>

ศรัณย์ สัมฤทธิ์เดชขจร. (2565). *ไบโอเมตริกซ์ (Biometric) คืออะไร*, [ออนไลน์]. สืบค้นเมื่อวันที่ 9 กันยายน 2565 จาก <http://www.hitop.co.th/bio-metric.html>

สุธิ ทวีรัตน์. (2565) *ยื่นร้องนายก หวันฉ่างดับ สแกนใบหน้า, หนังสือพิมพ์ฐานเศรษฐกิจ*, หน้า 1 ฉบับที่ 3,495 วันที่ 11 – 14 สิงหาคม พ.ศ. 2562. [ออนไลน์]. สืบค้นเมื่อวันที่ 17 กันยายน 2565 จาก <https://www.thansettakij.com/content/407027>

สุพล พรหมมาพันธุ์. (2563). *การพิสูจน์ตัวตนด้วยเทคโนโลยีชีวมาตรกับความเสี่ยงในการละเมิดสิทธิส่วนบุคคล, วารสารแพทยศาสตรมหาวิทาลัย, 66(1), หน้า 32-42.*

- วิกิพีเดีย สารานุกรมเสรี. (2565). *ข้อมูลที่ระบุตัวบุคคลได้* [ออนไลน์]. ค้นเมื่อวันที่ 22 สิงหาคม 2565, จาก:
<https://th.wikipedia.org/wiki/ข้อมูลที่ระบุตัวบุคคลได้>.
- อัจฉิมา มณฑาทันธุ์.(2565). *การวิเคราะห์ เปรียบเทียบการระบุตัวตน โดยการใช้ลักษณะเฉพาะทางกายภาพของร่างกาย (A Comparative Analysis of Physiological Biometrics Authentication)* [ออนไลน์]. สืบค้นเมื่อวันที่ 10 กันยายน 2565 จาก <http://dspace.spu.ac.th/bitstream/>
- อุดมชีพ ไพโรเกษตร. (2565). *เอกสารประกอบการบรรยายเรื่อง “บทบาทของผู้ประกอบการ SMEs ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล PDPA”* โครงการ เติมนุ่น ค่อยอด เพิ่มศักยภาพ SMEs ไทย ไปกับธนาคารออมสินและสมาพันธ์เอสเอ็มอีไทย. 2565. หน้า 5-17.
- Gary B. Shelly. (2020), *Discovering Computers 2020 A Gateway to Information Web Enhance “Discovering Computers 2020: A Gateway to Information Web Enhanced Introductory” Thomson Course Technology, 2020: 263.*