ปัญหาทางกฎหมายเกี่ยวกับข้อมูลไบโอเมตริก ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

Legal Issues Concerning Biometrics Data Under the Personal Data Protection Act B.E. 2562

รัชนี แตงอ่อน[1]

Ratchanee Tangon

Received: July 14, 2021 Revised: July 15, 2021 Accepted: August 10, 2021

บทคัดย่อ (Abstract)

บทความวิชาการนี้ได้ศึกษาปัญหาทางกฎหมายเกี่ยวกับข้อมูลไบโอเมตริก (biometric data) ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในประเด็นที่เกี่ยวข้องกับการบัญญัติความหมาย การตีความกฎหมายและการบังคับใช้ข้อมูลไบโอเมตริก จากการศึกษาพบว่ายังมีประเด็นที่ต้องพิจารณาหลายประการ ได้แก่ ความหมายของข้อมูลไบโอเมตริก การเก็บรวบรวมข้อมูลไบโอเมตริกต้องใช้เทคโนโลยีเข้ามาช่วยในการเก็บรวบรวมและประมวลผลข้อมูล เช่น ภาพจำลองหน้าตา จำลองม่านตา จำลองลายนิ้วมือ เป็นต้น ข้อมูลไบโอเมตริกเป็นข้อมูลส่วนบุคคลที่อ่อนไหว (sensitive personal data) เป็นความลับที่เจ้าของข้อมูลไม่ประสงค์ให้เปิดเผยต่อสาธารณะ ซึ่งมีความแตกต่างจากข้อมูลส่วนบุคคลทั่วไป เช่น ชื่อ สกุล อายุ อาชีพ นิสัยการกิน กิจวัตรประจำวันทั่วไป เป็นต้น เนื่องจากบทบัญญัติของกฎหมายดังกล่าวยังไม่ชัดเจน ขอบเขตการบังคับใช้ที่คลุมเครือ จึงเป็นประเด็นสำคัญของบทความวิชาการนี้ที่สะท้อนให้เห็นถึงข้อสังเกตบางประการที่แตกต่างจากกฎหมายของสหภาพยุโรป ดังนั้น บทบัญญัติที่เกี่ยวกับข้อมูลไบโอเมตริก

[1]ผศ.ดร.อาจารย์ประจำภาควิชานิติศาสตร์, คณะรัฐศาสตร์และนิติศาสตร์ มหาวิทยาลัยบูรพา

Asst. Prof. Dr., Department of Law, Faculty of Political Science and Law, Burapha University

Email : ratchanee_tangon@hotmail.com

ควรได้รับการแก้ไขให้เกิดความชัดเจนมากยิ่งขึ้น เพื่อป้องกันไม่ให้เกิดปัญหาการตีความ การบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย

คำสำคัญ (Keywords): ไบโอเมตริก สิทธิในความเป็นส่วนตัว การคุ้มครองข้อมูลส่วนบุคคล

Abstract

The purpose of this study is to examine the legal issues, interpretation and enforcement of biometric data under the Personal Data Protection Act B.E. 2562. Several issues, including the definition of biometric data and biometric data collection, require technology to assist in data collection and process, such as face image, iris image and fingerprint image should be reconsidered. Unlike general personal information, such as name, surname, age, occupation, eating habits, general daily activities, biometric data is sensitive personal data that the personal data prefers them not to be disclosed. Due to unclear definitions and enforcement of the Personal Data Protection Act B.E. 2562, this study compares the said Act with the EU Laws in order to specify key differences. It is essential that the Personal Data Protection Act B.E. 2562 relating to biometric data be revised and clarified to prevent interpretation and enforcement issues.

Keywords: Biometrics; right of privacy; personal data protection

บทนำ (Introduction)

ความทันสมัยและความก้าวหน้าทางเทคโนโลยีสารสนเทศ ทำให้มนุษย์ต้องปรับตัวต่อการเปลี่ยนแปลงทางสังคมที่เกิดขึ้นอย่างรวดเร็วเมื่อระบบคอมพิวเตอร์เข้ามาเป็นส่วนหนึ่งของชีวิตประจำวันของผู้คนในสังคม การเข้าถึงข้อมูลต่าง ๆ ในระบบคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตจึงจำเป็นอย่างยิ่งที่รัฐต้องให้ความสำคัญต่อการคุ้มครองข้อมูลส่วนบุคคลไม่ให้มีการแทรกแซงหรือล่วงละเมิดข้อมูลส่วนบุคคลโดยผิดกฎหมาย ประเทศไทยในฐานะประเทศสมาชิกขององค์กรสหประชาชาติต้องเคารพสิทธิมนุษยชนและต้องให้ความคุ้มครองสิทธิในความเป็นส่วนตัว (right of privacy) ของประชาชนตามประกาศของปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal

Declaration of Human Rights หรือ UDHR) (กุลพล พลวัน, 2547 : 34) ข้อมูลส่วนบุคคลถูกนำไปใช้ทั้งในหน่วยงานของรัฐและองค์ทางธุรกิจ กรณีองค์กรทางธุรกิจ การนำข้อมูลส่วนบุคคลของลูกค้ามาใช้ต้องได้รับความยินยอมเสียก่อนที่จะนำข้อมูลลูกค้าไปใช้ หากองค์กรธุรกิจนำข้อมูลของลูกค้าไปขายหรือหาประโยชน์ผิดกับวัตถุประสงค์ที่ให้ไว้กับลูกค้าย่อมเป็นการละเมิดข้อมูลส่วนบุคคลย่อมผิดกฎหมาย (ณฐพร วิริยะลัพภะและธเนศ สุจารีกุล, 2563 : 2196)

สำหรับบทความวิชาการนี้ นำเสนอประเด็นทางกฎหมายเกี่ยวกับข้อมูลที่เป็นไบโอเมตริก (Biometric) ซึ่งเป็นข้อมูลส่วนบุคคลที่อ่อนไหว (sensitive personal data) ประเภทหนึ่ง (ในบทความนี้ จะเรียกว่า “ไบโอเมตริก”) คำว่า ไบโอเมตริก (Biometric) ประกอบขึ้น จากคำว่า ไบโอ (Bio) หมายถึงสิ่งมีชีวิต และ คำว่าเมตริก (metrics) หมายถึงคุณลักษณะที่ สามารถถูกวัดค่าหรือประเมินจำนวนได้ พอนำสองคำมารวมกันจึงสามารถอธิบายได้ว่า ไบโอเมตริก คือเทคโนโลยีที่ใช้คุณลักษณะหรือ พฤติกรรมของสิ่งมีชีวิตที่เป็นเอกลักษณ์ และสามารถเทียบวัดหรือนับจำนวนได้มาผนวกเข้ากับหลักการทางสถิติ เพื่อการแยกแยะ หรือจดจำบุคคล (นัยนา มาแสง, 2551 : 3) ในปัจจุบันนี้ความก้าวหน้าอย่างรวดเร็วของเทคโนโลยีไบโอเมตริก นำมาซึ่งการเปลี่ยนแปลงของการจัดเก็บข้อมูลส่วนบุคคล เทคโนโลยีข้อมูลไบโอเมตริกนำมาใช้เก็บข้อมูลส่วนบุคคล ประกอบด้วยอุปกรณ์เพื่อใช้ในการอ่านค่าเกี่ยวกับบุคคลและระบบซึ่งใช้ในการเชื่อมต่อกับอุปกรณ์ที่บันทึกข้อมูลไบโอเมตริกเกี่ยวกับบุคคลนั้นเพื่อทำการระบุตัวบุคคล หรือยืนยันตัวบุคคล ระบบนี้จะทำการวัดค่าหรือวิเคราะห์คุณลักษณะของบุคคล เช่น รูปหน้า รูปแบบของเสียง ลายนิ้วมือ ลายมือ หรือม่านตา เป็นต้น ทั้งนี้ เทคโนโลยีไบโอเมตริกเป็นเทคโนโลยี ซึ่งผสมผสานกับเทคโนโลยีอื่น ๆ ประกอบด้วย เช่น เทคโนโลยีด้านการแพทย์ เทคโนโลยีทางคอมพิวเตอร์ สถิติ วิทยาศาสตร์ หรือคณิตศาสตร์ เป็นต้น (อธิพร สิทธิธีรรัตน์, 2558 : 41) ดังนั้น ข้อมูลไบโอเมตริกจึงเป็นข้อมูลส่วนบุคคลที่สำคัญอย่างยิ่งที่จะไม่ให้ผู้ใดมาละเมิดข้อมูลส่วนบุคคลโดยปราศจากความยินยอมจากเจ้าของข้อมูลนี้ซึ่งในต่างประเทศก็ให้ความสำคัญอย่างยิ่งโดยบัญญัติไว้อย่างชัดเจนในกฎหมายคุ้มครองข้อมูลส่วนบุคคลในสหภาพยุโรปและประเทศอื่นๆ เช่นกัน

สำหรับประเทศไทย เมื่อได้ศึกษาพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ตามมาตรา 26 และมาตรา 27 พบว่า ยังไม่มีความชัดเจนเกี่ยวกับข้อมูลไบโอเมตริกส่วนบุคคลทั้งประเด็นทางกฎหมายที่เกี่ยวข้องกับข้อมูลอ่อนไหว (sensitive data) การกำหนดความหมายประเภทของข้อมูลอ่อนไหว ขอบเขตของกิจกรรมในการข้อมูลอ่อนไหวนี้ไปใช้ซึ่งแตกต่างจากข้อมูล

ส่วนบุคคลทั่วไป รวมถึงการประมวลผลข้อมูลอ่อนไหวว่าหากเป็นข้อมูลไบโอเมตริกต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลแค่ไหน เพียงใด เป็นต้น เหล่านี้จึงเป็นประเด็นที่บทความนี้ได้นำเสนอโดยศึกษาจากงานวิชาการของนักวิชาการต่างประเทศและนักวิชาการไทย เพื่อให้ได้แนวทางพัฒนากฎหมายรวมถึงข้อเสนอแนะบางประการที่เกี่ยวข้องกับการคุ้มครองข้อมูลไบโอเมตริกตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

แนวคิดสิทธิในความเป็นอยู่ส่วนตัว การคุ้มครองข้อมูลส่วนบุคคล และไบโอเมตริก

สิทธิความเป็นอยู่ส่วนตัวเป็นสิทธิมนุษยชนประการหนึ่ง ที่มาของสิทธิมนุษยชนมาจากคำสอนของศาสนาคริสต์ที่เชื่อว่ามนุษย์ทุกคนเกิดมาเสมอภาคกัน มีศักดิ์ศรีแห่งความเป็นมนุษย์เหมือนกันซึ่งสอดคล้องกับแนวคิดกฎหมายและสิทธิตามธรรมชาติที่เชื่อว่าเป็นสิทธิติดตัวมาตั้งแต่เกิด ผู้ใช้อำนาจปกครองไม่มีอำนาจที่จะลบล้างหรือล่วงเกินสิทธินี้ได้ (บรรเจิด สิงคะเนติ และคณะ, 2554 : 1) มนุษย์ทุกคนมีสิทธิเป็นเจ้าของข้อมูลส่วนตัวของตนและสามารถเก็บเป็นความลับไว้ไม่ประสงค์ให้ผู้ใดล่วงละเมิดข้อมูลของตนโดยปราศจากความยินยอมของผู้เป็นเจ้าของข้อมูลนั้น ไม่ว่าจะเป็นบุคคลใดไม่มีสิทธิที่จะล่วงละเมิดข้อมูลส่วนบุคคลเว้นแต่เป็นสิ่งที่กฎหมายกำหนดให้อำนาจไว้ (หทัยชนก หร่ายวงศ์, 2559 : 16)

องค์กรสหประชาชาติได้กำหนดให้ความคุ้มครองสิทธิความเป็นอยู่ส่วนตัวของมนุษย์ไว้ชัดเจน รวมถึง “ความเป็นส่วนตัวดิจิทัล” “ความเป็นส่วนตัวในโลกไซเบอร์” หรือ “ความเป็นส่วนตัวออนไลน์” เหล่านี้บัญญัติไว้ในข้อ 12 ของปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ปีค.ศ.1948 (Universal Declaration of Human Rights หรือ UDHR) และต่อมาได้รับการรับรองไว้ในข้อ 17 ของกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (International Covenant on Civil and Political Rights หรือ ICCPR) ที่รับรองโดยสมัชชาใหญ่แห่งสหประชาชาติเมื่อวันที่ 19 ธันวาคม ปี ค.ศ. 1966 (Pauletto, 2021 : 2)

ต่อมาสหภาพยุโรป (European Union) ร่วมกันกำหนดกฎหมายที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคลในสหภาพยุโรปขึ้น คือ ระเบียบการคุ้มครองข้อมูลของสหภาพยุโรป ในปีค.ศ.1995 ที่เรียกว่า Directive 95/46/EC เป็นข้อบังคับเกี่ยวกับการเก็บข้อมูลส่วนบุคคลและการประมวลผลข้อมูลส่วนบุคคลซึ่งใช้มานานหลายปี จนถึงวันที่ 25 พฤษภาคม ปี ค.ศ. 2018 สภายุโรปได้รับรองกฎหมายที่ชื่อว่า ระเบียบว่าด้วยการคุ้มครองข้อมูลทั่วไป (General Data Protection Regulation

หรือ GDPR) มีผลใช้บังคับหลังจากวันที่ 25 พฤษภาคม ปี ค.ศ. 2018 กฎหมายนี้กำหนดกรอบสิทธิและภาระผูกพันของข้อมูลส่วนบุคคลที่จะถูกรวบรวมและประมวลผลข้อมูล (เจ้าของข้อมูล) และสำหรับบริษัทเอกชนและหน่วยงานของรัฐ ซึ่งเป็นผู้ควบคุมข้อมูล (data controller) ที่รวบรวมและประมวลผลข้อมูลส่วนบุคคลเหล่านี้ อย่างไรก็ตาม กฎหมายว่าด้วยการคุ้มครองของข้อมูลส่วนบุคคลของสหภาพยุโรปนี้มีบรรทัดฐานที่แตกต่างกันแต่ละประเทศที่เป็นสมาชิกที่จำเป็นต้องเพิ่มเติมในการแปลภาษาแต่ละประเทศให้เป็นภาษาทางการให้เหมาะสมกับประเทศของตน เนื่องจากความแตกต่างในระบบกฎหมายและวัฒนธรรม การดำเนินการตามกฎหมายของคำสั่งคุ้มครองข้อมูลแตกต่างกันไปในแต่ละประเทศสมาชิกสหภาพยุโรป ในทำนองเดียวกัน ความแตกต่างทางวัฒนธรรมก็ส่งผลให้การปฏิบัติต่างกันในการดำเนินการเพื่อปกป้องข้อมูลส่วนบุคคลในประเทศสมาชิกสหภาพยุโรป (Custers et al., 2018 : 235)

สำหรับประเด็นการคุ้มครองข้อมูลไบโอเมตริกส่วนบุคคล ในปัจจุบันนี้ กฎหมาย GDPR ให้คำนิยาม ข้อมูลไบโอเมตริก ซึ่งเป็นข้อมูลอ่อนไหว ได้บัญญัติไว้ชัดเจนใน GDPR ข้อ 4 (14) และข้อ 9 ดังนี้ GDPR ข้อ 4 (14) ได้ให้คำนิยาม ข้อมูลไบโอเมตริก หมายถึง “ข้อมูลส่วนบุคคลที่เป็นผลมาจากการประมวลผลทางเทคนิคที่เฉพาะเจาะจง (specific technical processing) เกี่ยวกับกายภาพ สรีรวิทยา หรือ ลักษณะทางพฤติกรรมของบุคคลธรรมดา ซึ่งทำให้สามารถยืนยันลักษณะที่ระบุตัวตนเฉพาะของบุคคลนั้นได้ เช่น ภาพจำลองใบหน้า หรือ ข้อมูลจำลองลายนิ้วมือ” (ปิยะบุตร บุญอร่ามเรือง และคณะ, 2563 : 61) สอดคล้องกับงานวิจัยของอธิพร สิทธิธีรรัตน์ที่ว่า ข้อมูลไบโอเมตริก หมายถึง ข้อมูลส่วนบุคคลเกิดจากการประมวลผลโดยใช้เทคนิคเฉพาะเกี่ยวกับกายภาพ หรือความประพฤติของบุคคลนั้น ซึ่งทำให้บ่งชี้ลักษณะเฉพาะของบุคคล เช่น รูปหน้า หรือลายนิ้วมือ (อธิพร สิทธิธีรรัตน์, 2558 : 80) ทั้งนี้ ตามมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ก็ได้บัญญัติไว้เช่นกัน แต่ยังไม่มีให้ความหมายที่ชัดเจน

นอกจากนิยามความหมายของ ข้อมูลไบโอเมตริก GDPR ยังกำหนดให้ข้อมูลไบโอเมตริกเป็นได้ทั้งข้อมูลอ่อนไหว (sensitive data) และข้อมูลทั่วไปไม่อ่อนไหว (non-sensitive data) ขึ้นอยู่กับกับการนำไปใช้ ทั้งนี้ ตาม GDPR ข้อ 9 กำหนดไว้เฉพาะว่า ข้อมูลไบโอเมตริกถือเป็นข้อมูลอ่อนไหวหากเป็นการใช้ไปเพื่อการระบุตัวตนอย่างเฉพาะเจาะจงของบุคคล (uniquely identifying a natural person) ดังนั้น หากเป็นข้อมูลที่มีลักษณะเป็นข้อมูลไบโอเมตริกเช่นกัน แต่หากไม่ได้นำไปใช้เพื่อการระบุตัวตนอย่างเฉพาะเจาะจงของบุคคลนั้น ก็ไม่เป็นข้อมูลอ่อนไหว แต่ให้

ถือเป็นข้อมูลส่วนบุคคลที่จะได้รับความคุ้มครองระดับทั่วไปเท่านั้น (ปิยะบุตร บุญอร่ามเรือง และคณะ, 2563 : 62) จะเห็นได้ว่า ข้อมูลไบโอเมตริกเป็นได้ทั้งข้อมูลทั่วไปและข้อมูลอ่อนไหว ขึ้นอยู่กับกิจกรรมหรือการนำข้อมูลไปใช้เพื่อการใด เพราะหากนำข้อมูลไบโอเมตริกไปใช้ระบุอัตลักษณ์ของบุคคลเป็นการเฉพาะเจาะจงแล้วย่อมเป็นข้อมูลอ่อนไหวที่ต้องได้รับการคุ้มครองเป็นพิเศษมากกว่าการนำข้อมูลไบโอเมตริกไปใช้ในกิจการทั่วไป

ที่มาของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นหนึ่งในกฎหมายที่อยู่ในโครงการกฎหมายเกี่ยวกับเทคโนโลยีที่ประเทศไทยพัฒนาเพื่อรองรับกับการเปลี่ยนแปลงของสังคมที่ระบบคอมพิวเตอร์เข้ามามีบทบาทกับชีวิตมนุษย์ สำหรับการกระทำความผิดต่อข้อมูลส่วนบุคคลหรือข้อมูลความลับมีระดับความร้ายแรงของภยันตรายแตกต่างกัน ขึ้นอยู่กับผู้กระทำความผิดเป็นปัจเจกชน หรือหน่วยงานของรัฐ เนื้อหาที่ถูกละเมิดเกี่ยวกับเรื่องเกี่ยวกับประเด็นปัญหาใดเป็นต้น (สาวตรี สุขศรี, 2563 : 63)

ที่มาของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย สภาผู้แทนราษฎรมีการพิจารณาร่างกฎหมายและรับหลักการของกฎหมายนี้เรียบร้อยตั้งแต่ ปี พ.ศ. 2556 แต่ต้องสะดุดลงเพราะมีการยุบสภาผู้แทนราษฎรเสียก่อนด้วยเหตุผลประเด็นทางการเมืองของประเทศ ต่อมาเมื่อวันที่ 28 ธันวาคม พ.ศ. 2561 สภานิติบัญญัติแห่งชาติให้ความเห็นชอบผ่านร่างกฎหมายและพิจารณาออกกฎหมายโดยให้ชื่อว่า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ประกาศในราชกิจจานุเบกษาเพื่อบังคับใช้ในวันที่ 27 พฤศจิกายน พ.ศ. 2562 (สุพิศ ปราณีตพลกรัง, 2563 : 4) อย่างไรก็ตาม กฎหมายนี้ได้ขยายเวลาการบังคับใช้ไปในวันที่ 1 มิถุนายน พ.ศ. 2565 เพื่อให้หน่วยงานต่าง ๆ ที่เกี่ยวข้องไม่ว่าจะเป็นหน่วยงานของรัฐ องค์กรเอกชน ประชาชนและบุคคลที่เกี่ยวข้องกับการบังคับใช้กฎหมายนี้ได้เตรียมการให้พร้อมกับกฎหมายนี้ต่อไป

เมื่อพิจารณาถึงเจตนารมณ์ของพระราชบัญญัติดังกล่าวเพื่อให้สอดคล้องกับการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวตามหลักสิทธิมนุษยชน และตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 มาตรา 32 บัญญัติไว้ดังนี้ *“บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว การกระทำอันเป็นการละเมิดหรือกระทบต่อสิทธิของบุคคลตามวรรคหนึ่ง หรือการนำข้อมูล ส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใดๆ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจ*

ตามบทบัญญัติแห่งกฎหมาย ที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ” จะเห็นได้ว่า การคุ้มครองข้อมูลส่วนบุคคลที่จะไม่ให้มีบุคคลใดมาล่วงละเมิดสิทธิความเป็นอยู่ส่วนตัวของผู้อื่น เว้นแต่เป็นการกระทำเพื่อประโยชน์สาธารณะ เป็นหลักกฎหมายที่รัฐธรรมนูญ มาตรา 32 ได้รับรองและคุ้มครองสิทธิไว้อย่างชัดเจน

ปัญหาการบังคับใช้กฎหมายเกี่ยวกับข้อมูลไบโอเมตริกตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

ข้อมูลไบโอเมตริกเป็นที่ยอมรับระดับสากลถึงความน่าเชื่อถือ ปลอดภัยและแม่นยำในการยืนยันอัตลักษณ์บุคคลได้อย่างถูกต้อง จำเป็นต้องพิจารณาประเด็นการคุ้มครองข้อมูลไบโอเมตริกตามกฎหมายของประเทศไทยได้แก่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ตามมาตรา 26 และมาตรา 27 ว่ามีความชัดเจนและครอบคลุมกับความหมายของข้อมูลไบโอเมตริกการประมวลผลข้อมูลไบโอเมตริกหรือไม่เพียงใด เมื่อได้ศึกษางานวิจัยและบทความวิชาการของประเด็นทางกฎหมาย ดังต่อไปนี้

1. กรณีขอบเขตของ “ข้อมูลไบโอเมตริก” ตามมาตรา 26

มาตรา 26 ได้กำหนดเกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคลไว้ดังนี้

1.1 มาตรา 26 วรรคหนึ่ง

มาตรา 26 วรรคหนึ่งความว่า “*ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่...*”

ข้อมูลตามมาตรา 26 วรรคหนึ่งนี้ เป็นข้อมูลชีวภาพ เช่น ดีเอ็นเอ (DNA) ลายพิมพ์นิ้วมือ ข้อมูลประวัติอาชญากรรม เป็นข้อมูลที่มีความอ่อนไหว (sensitive personal data) การเก็บรวบรวมข้อมูลจึงต้องได้รับความยินยอมโดยชัดแจ้ง (explicit consent) จากเจ้าของข้อมูลส่วนบุคคลนั้น (สุพิศ ปราณีตพลกรัง, 2563 : 35) ที่สำคัญคือ แบบของการให้ความยินยอมโดยชัดแจ้งต้องระบุการเป็นข้อมูลอ่อนไหวให้ชัดเจน และต้องแยกต่างหากจากความยินยอมในกรณีปกติ (ปิยะ บุตร บุญอร่ามเรือง และคณะ, 2563 : 311) แต่อย่างไรก็ตาม กฎหมายไม่ได้กำหนดคำเรียกหรือคำ

นิยาม “ไบโอเมตริก” ไว้ให้ชัดเจน เมื่อได้ศึกษาเปรียบเทียบกับกฎหมาย GDPR ข้อ 4 (14) ซึ่งได้ให้คำนิยาม ข้อมูลไบโอเมตริก หมายถึง ขอมูลสวนบุคคลที่เปนผลมาจากการประมวลผลทางเทคนิคที่เฉพาะเจาะจงเกี่ยวกับกายภาพ สรีรวิทยา หรือ ลักษณะทางพฤติกรรมของบุคคลธรรมดา ซึ่งทำให้สามารถยืนยันลักษณะที่ระบุตัวตนเฉพาะของบุคคลนั้นได เช่น ภาพจำลองใบหน่า หรือ ข้อมูลจำลองลายนิ้วมือ เป็นต้น

สำหรับ “ข้อมูลสุขภาพ”และข้อมูล “ความพิการ” ตามมาตรา 26 วรรคหนึ่งแยกสองคำออกจากกัน แต่ตาม GDPR กำหนดให้ ข้อมูลความพิการอยู่ในความหมายของข้อมูลสุขภาพ (ปิยะ บุตร บุญอร่ามเรือง และคณะ, 2563 : 49)

1.2 มาตรา 26 วรรคสอง

มาตรา 26 วรรคสอง ความว่า “*ข้อมูลชีวภาพตามวรรคหนึ่งให้หมายถึงข้อมูลส่วนบุคคลที่เกิดจากการใช้เทคนิคหรือเทคโนโลยีที่เกี่ยวข้องกับการนำลักษณะเด่นทางกายภาพ หรือทางพฤติกรรมของบุคคลมาใช้ทำให้สามารถยืนยันตัวตนของบุคคลนั้นที่ไม่เหมือนกับบุคคลอื่นได้ เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองม่านตา หรือข้อมูลจำลองลายนิ้วมือ*”

หากจะพิจารณาว่า ตามมาตรา 26 วรรคสองคือ ข้อมูลไบโอเมตริก ย่อมจะตรงกับความหมายตามกฎหมาย GDPR ข้อ 4 (14) เพียงแต่มาตรา 26 วรรคสอง ให้หมายความรวมเข้าไปกับ ข้อมูลชีวภาพ แต่ถ้าเป็นข้อมูลไบโอเมตริกต้องมีลักษณะเฉพาะเจาะจงและต้องใช้เทคนิคอื่นๆ เข้าไปเก็บข้อมูลด้วยไม่ว่าจะเป็นเทคโนโลยีทางการแพทย์ เทคโนโลยีคอมพิวเตอร์ ยกตัวอย่างข้อมูลไบโอเมตริก เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองม่านตา หรือข้อมูลจำลองลายนิ้วมือ และในกรณีที่เป็นการเก็บรวบรวมข้อมูลส่วนบุคคล เป็นต้น ซึ่งผู้เป็นเจ้าของข้อมูลต้องให้ความยินยอมโดยชัดแจ้งเช่นเดียวกับมาตรา 26 วรรคหนึ่ง (สุพิศ ปราณีตพลกรัง, 2563 : 37) เว้นแต่เข้าข้อยกเว้น ตามมาตรา 26 (1) (2) (3) (4) (5) (ก) ถึง (จ) ที่เก็บรวบรวมข้อมูลไม่จำเป็นต้องขอความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลนั้น

จะเห็นได้ว่า ข้อมูลที่เป็นอัตลักษณ์ของบุคคลต้องถือเป็นข้อมูลชีวภาพที่ต้องได้รับความยินยอมโดยชัดแจ้งก่อนจะมีการเก็บรวบรวมข้อมูล สำหรับข้อมูลไบโอเมตริก แตกต่างจากข้อมูลชีวภาพ เพราะข้อมูลไบโอเมตริก ยกตัวอย่าง ข้อมูลจำลองลายนิ้วมือถือว่าเป็นเอกลักษณ์เฉพาะของแต่ละคนซึ่งไม่เหมือนกัน แม้จะเป็นบุคคลในครอบครัวเดียวกัน การนำลายพิมพ์นิ้วมือมาใช้เพื่อยืนยันตัวตนเป็นที่นิยมทั้งในหน่วยงานของรัฐ เช่น การทำบัตรประชาชน การทำประวัติอาชญากร

เป็นต้นและองค์กรเอกชนต่าง ๆ เช่น การให้พนักงานของบริษัทยืนยันตัวตนในการทำงานด้วยวิธีการแสกนนิ้วมือ เป็นต้น (อธิพร สิทธิธีรรัตน์, 2558 : 44) จำเป็นต้องให้ความคุ้มครองข้อมูลที่เฉพาะเจาะจงลงไปให้ชัดเจน ดังนั้น ในปัจจุบันเทคโนโลยีการใช้ลายนิ้วมือเป็นที่นิยมในการเข้าสู่ระบบปฏิบัติการทำงานของสมาร์ทโฟนบางรุ่น เพราะมีความรวดเร็ว แม่นยำ ถูกปลอมแปลงยากด้วย แต่อย่างไรก็ตาม ลายพิมพ์นิ้วมือของบุคคลอาจถูกละเมิดได้ง่าย เพราะหากมีบุคคลอื่นเก็บลายพิมพ์นิ้วมือจากพื้นผิววัตถุเช่น กระจก แก้ว พื้นกระเบื้อง ก็สามารถนำไปคัดลอกและนำไปใช้ประโยชน์ได้โดยปราศจากความยินยอมได้ง่าย ๆ ซึ่งจะเกิดผลเสียหายแก่เจ้าของลายพิมพ์นิ้วมือนั้นได้

1.3 มาตรา 26 วรรคสาม

มาตรา 26 วรรคสาม ความว่า *“ในกรณีที่เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมต้องกระทำภายใต้การควบคุมของหน่วยงานที่มีอำนาจหน้าที่ตามกฎหมาย หรือได้จัดให้มีมาตรการคุ้มครองข้อมูลส่วนบุคคลตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด”*

การเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมกฎหมายบัญญัติให้ต้องกระทำภายใต้การควบคุมของหน่วยงานที่มีอำนาจหน้าที่ตามกฎหมาย หรือได้จัดให้มีมาตรการคุ้มครองส่วนบุคคลตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด (สุพิศ ปราณีตพลกรัง, 2563 : 37) การเก็บรวบรวมและการประมวลผลข้อมูลประวัติอาชญากรรมของประเทศไทยแตกต่างจากของ GDPR ตรงที่ว่า GDPR ได้แยกข้อมูลประเภทประวัติอาชญากรรม (personal data relating to criminal convictions and offences) ไว้เป็นข้อมูลประเภทหนึ่งที่ต้องแยกออกมาเป็นการเฉพาะ เนื่องจากการให้ความคุ้มครองสิทธิของเจ้าของข้อมูลในประวัติอาชญากรรมนั้นอย่างเพียงพอ (appropriate safeguard) ซึ่งแตกต่างจากมาตรา 26 วรรคสามตามกฎหมายไทยข้อมูลประวัติอาชญากรรมถือเปนข้อมูลออนไหวซึ่งต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลก่อนถึงจะสามารถประมวลผลข้อมูลได้ ตามมาตรา 27 วรรคหนึ่ง (ปิยะบุตร บุญอร่ามเรือง และคณะ, 2563 : 48) สำหรับข้อมูลประวัติอาชญากรรมต้องเก็บรวบรวมภายใต้การดำเนินงานของสำนักงานตำรวจแห่งชาติตามที่กฎหมายกำหนดเท่านั้นเพื่อประโยชน์ในการดำเนินคดีอาญาควรต้องการแยกจากมาตรา 26 เพราะตามมาตรา 26 วรรคหนึ่งและวรรคสองเป็นการเก็บรวบรวมข้อมูลที่เป็นอัตลักษณ์ส่วนบุคคลอันเป็นข้อมูลชีวภาพและข้อมูลไบโอเมตริกซึ่งการคุ้มครองข้อมูลวัตถุประสงค์ของการนำไปใช้ของทั้งหน่วยงานของรัฐและเอกชน การประมวลข้อมูลก็ย่อมแตกต่าง

จากการเก็บรวบรวมข้อมูลและการประมวลผลข้อมูลประวัติอาชญากรรมของสำนักงานตำรวจแห่งชาติที่เป็นไปเพื่อประโยชน์สาธารณะและเพื่อกระบวนการยุติธรรมทางอาญาเป็นหลัก

2. ข้อมูลไบโอเมตริกเป็นข้อมูลอ่อนไหวต้องได้รับความคุ้มครองเป็นพิเศษ ตามมาตรา 27

GDPR ได้แบ่งข้อมูลส่วนบุคคลออกเป็น 2 ประเภท คือข้อมูลส่วนบุคคล และข้อมูลส่วนบุคคลประเภทพิเศษ ซึ่งข้อมูลส่วนบุคคลได้แก่ข้อมูลทั่วไปเกี่ยวกับบุคคลผู้เป็นเจ้าของข้อมูลส่วนบุคคล ซึ่งมีหลักเกณฑ์ในการเก็บรวบรวม ใช้ หรือเปิดเผยแตกต่างไปจากข้อมูลที่มีลักษณะพิเศษซึ่งจะกล่าวต่อไป โดยข้อมูลส่วนบุคคลประเภทพิเศษนี้เป็นข้อมูลซึ่งมีความอ่อนไหว ทั้งนี้ GDPR กำหนดให้ห้ามทำการประมวลผลข้อมูลที่เปิดเผยถึงเชื้อชาติ แหล่งกำเนิดชาติพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนาหรือปรัชญา การเป็นสมาชิกสภาพแรงงาน และการประมวลผลข้อมูลเกี่ยวกับพันธุกรรมและข้อมูลไบโอเมตริกหรือข้อมูลเกี่ยวกับสุขภาพหรือพฤติกรรมทางเพศ เว้นแต่จะได้ความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลหรือเข้าข้อยกเว้นตามกฎหมาย GDPR (อธิพร สิทธิธีรรัตน์, 2558 : 80)

ลักษณะของการประมวลผลข้อมูลส่วนบุคคลทั่วไปกับข้อมูลอ่อนไหวแตกต่างกันขึ้นอยู่กับการนำข้อมูลเหล่านั้นไปใช้เพื่อวัตถุประสงคใด หากถูกใช้เพื่อวัตถุประสงคในการบงชี้สิ่งเป็นการเฉพาะเจาะจง เชน เชื้อชาติหรือศาสนา ก็จะทำให้การประมวลผลในลักษณะดังกลาวย่อมเปนการประมวลผลข่อมูลสวนบุคคลประเภทของข้อมูลออนไหว แตหากถูกใช้เพื่อการยืนยันตัวตนหรือระบุตัวตนทั่ว ๆ ไปถือเป็นข้อมูลทั่วไปอันได้แก่ เพศ ชื่อ สกุล อายุ อาชีพ เหล่านี้ถือว่าเปนการประมวลผลข่อมูลสวนบุคคลธรรมดาทั่วไป (ปิยะบุตร บุญอร่ามเรือง และคณะ, 2563 : 49-50) เนื่องจากข้อมูลไบโอเมตริกสามารถระบุตัวตนหรืออัตลักษณ์ของบุคคลแต่ละคนได้อย่างแม่นยำและน่าเชื่อถือเช่นการนำเทคนิคจำลองใบหน้า จอม่านตา ลายนิ้วมือเก็บเป็นข้อมูลเป็นต้น ทั้งยังถูกนำไปใช้อย่างแพร่หลายในองค์กรธุรกิจและหน่วยงานของรัฐ ดังนั้นการจัดเก็บข้อมูล การประมวลผลข้อมูล และการเปิดเผยข้อมูลจึงต้องมีหลักเกณฑ์ หรือข้อจำกัดที่เคร่งครัดกว่าข้อมูลส่วนบุคคลทั่วไป เพราะการละเมิดข้อมูลส่วนบุคคลที่มีความอ่อนไหวย่อมกระทบต่อสิทธิความเป็นส่วนตัวของบุคคลมากกว่าข้อมูลส่วนบุคคลทั่วไปทั้งในด้านของความรู้สึก ผลกระทบต่อจิตใจ การเปิดเผยข้อมูลอ่อนไหวอาจทำให้ความอับอาย เสื่อมเสียต่อชื่อเสียงตนเองและครอบครัวได้

ยกตัวอย่างกรณีประเทศมาเลเซีย ข้อมูลส่วนบุคคลของลูกจ้างในการจ้างแรงงานเป็นไปตามกฎหมายที่เกี่ยวข้องกับการจ้างแรงงาน ซึ่งข้อมูลของลูกจ้างถือเป็นข้อมูลอ่อนไหวประการหนึ่ง

ข้อมูลนี้จะถูกเก็บไว้ที่นายจ้าง โดยนายจ้างเก็บข้อมูลเพื่อการจัดการในบันทึกการจ้างงาน สำหรับข้อมูลอ่อนไหวต้องได้รับความยินยอมโดยชัดแจ้งจากลูกจ้างผู้เป็นเจ้าของข้อมูลก่อนที่ข้อมูลของลูกจ้างจะถูกประมวลผล ตามมาตรา 40 แห่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศมาเลเซีย ปี ค.ศ. 2010 (Hassan, 2012 : 701)

กรณีประเทศไทย ประเด็นที่น่าเป็นห่วงว่าข้อมูลส่วนบุคคลจะถูกล่วงละเมิดหรือไม่ หากมีการนำข้อมูลไบโอเมตริกเช่นการจำลองใบหน้า จำลองม่านตาซึ่งเป็นข้อมูลอ่อนไหวแล้วหน่วยงานของรัฐนำข้อมูลดังกล่าวไปใช้อาจเป็นการละเมิดข้อมูลส่วนบุคคลได้ จำเป็นต้องกำหนดเงื่อนไขหรือหลักเกณฑ์พิเศษให้ชัดเจน ยกตัวอย่าง กรณีการกระทำโดยหน่วยงานของรัฐได้แก่ ธนาคารกรุงไทย ใน ปีพ.ศ. 2563 พบปัญหาที่เป็นข้อวิตกกังวลของประชาชนที่การยืนยันตัวเองให้ความยินยอมเกี่ยวกับข้อมูลส่วนบุคคลเพื่อเข้าร่วมโครงการภาครัฐผ่านทางแอปพลิเคชั่น “เป๋าตังค์” ที่ให้มีการสแกนใบหน้า เป็นโครงการของรัฐที่เกิดขึ้นในช่วงที่ประเทศไทยประสบปัญหาโรคติดเชื้อไวรัสโคโรนา 2019 (COVID-19) ประชาชนกลัวว่าข้อมูลส่วนบุคคลจะถูกล่วงละเมิดและธนาคารกรุงไทยปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือไม่ อย่างไรก็ตาม ธนาคารกรุงไทยได้ยกเลิกระบบการให้ความยินยอมแล้ว แม้ตอนแรกธนาคารฯ ให้เหตุผลว่าเพื่อป้องกันการทุจริตหากมีการสวมสิทธิกัน แต่ต่อมาเมื่อเกิดกระแสทางสังคมว่ารู้สึกไม่ปลอดภัยว่าข้อมูลส่วนมูลจะถูกนำไปใช้โดยปราศจากความยินยอมในกรณีอื่น ๆ ได้ (ไทยรัฐนิวส์, 2564) จะเห็นได้ว่าจากข่าวข้างต้น แม้พระราชบัญญัติดังกล่าวจะถูกประกาศการเลื่อนบังคับใช้ไปอย่างเป็นทางการในปีพ.ศ.2565 เนื่องจากสถานการ์โรคติดเชื้อไวรัสโคโรนา 2019 แต่ธนาคารกรุงไทย ต้องเคารพในสิทธิส่วนบุคคลของประชาชนด้วยเสมอ นอกจากนี้ การสแกนใบหน้าหรือข้อมูลส่วนตัวอันได้แก่ข้อมูลบัตรประชาชน ประวัติอาชีพ รายได้ต่าง ๆ รัฐจะเก็บไว้แล้วจะถูกนำไปใช้ในโครงการอื่น ๆ โดยที่ประชาชนไม่ได้ให้ความยินยอม รัฐจึงไม่สามารถทำได้ ดังนั้น เป็นสิ่งที่จำเป็นอย่างยิ่งที่หน่วยงานของรัฐ ธนาคารกรุงไทยต้องคำนึงถึงหลักความยินยอมอย่างเคร่งครัดตามบทบัญญัติของกฎหมาย

บทสรุป (Conclusion)

การคุ้มครองข้อมูลส่วนบุคคลเป็นสิทธิในความเป็นส่วนตัวประการหนึ่งที่ได้รับการรับรองและคุ้มครองตามกฎหมายและกติการะหว่างประเทศโดยกำหนดว่า บุคคลทุกคนย่อมได้รับการรับรองและคุ้มครองความเป็นส่วนตัว ครอบครัว ที่อยู่อาศัย เกียรติยศ ชื่อเสียงซึ่งเป็นสิทธิตามธรรมชาติที่ติดตัวมนุษย์มาตั้งแต่กำเนิดที่จะไม่ให้ใครมาล่วงละเมิดหรือให้รัฐมาแทรกแซงได้ เว้นแต่กฎหมายจะบัญญัติไว้ชอบธรรมและชัดแจ้ง ในกลุ่มประเทศสหภาพยุโรปให้การรับรองคุ้มครองสิทธิในความเป็นส่วนตัวโดยเฉพาะข้อมูลส่วนบุคคลไว้อย่างชัดเจนเพื่อถือเป็นแนวทางปฏิบัติให้แก่ประเทศสมาชิกสหภาพยุโรป ตั้งแต่ปี ค.ศ. 1995 ระเบียบการคุ้มครองข้อมูลของสหภาพยุโรปที่เรียกว่า Directive 95/46/EC จนกระทั่งในปี ค.ศ. 2018 สภายุโรปได้รับรองกฎหมายที่ชื่อว่าระเบียบว่าด้วยการคุ้มครองข้อมูลทั่วไป (General Data Protection Regulation หรือ GDPR) เพื่อเป็นข้อบังคับเกี่ยวกับการเก็บข้อมูลส่วนบุคคลและการประมวลผลข้อมูลส่วนบุคคล อย่างไรก็ตาม แนวทางปฏิบัติและการประมวลผลข้อมูลโดยใช้เทคโนโลยีไบโอเมตริกอาจจะแตกต่างกันไปในแต่ละประเทศสมาชิกสหภาพยุโรปได้ขึ้นอยู่กับบริบททางการเมือง เศรษฐกิจและสังคม

สำหรับประเทศไทย การรับรองและคุ้มครองสิทธิในความเป็นส่วนตัวเป็นไปตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อคุ้มครองข้อมูลส่วนบุคคลไม่ให้มีการแทรกแซงหรือล่วงละเมิดข้อมูลใด ๆ ซึ่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ประกาศใช้อย่างเป็นทางการแล้วแต่ขยายเวลาการบังคับใช้กฎหมายให้เริ่มใช้วันที่ 1 มิถุนายน พ.ศ. 2565 ด้วยเหตุผลของสถานการณ์ทางการเมืองและโรคติดเชื้อไวรัสโคโรนา 2019 เพื่อให้เกิดความพร้อมกับทุกภาคส่วนทั้งหน่วยงานของรัฐ องค์กรเอกชน ประชาชนและบุคคลที่เกี่ยวข้องที่ต้องปฏิบัติตามหลักเกณฑ์ของกฎหมายที่มีหลักเกณฑ์และเงื่อนไขหลายประการ เมื่อกฎหมายที่บัญญัติขึ้นมาใหม่ พนักงานเจ้าหน้าที่ที่มีอำนาจหน้าที่ตามพระราชบัญญัตินี้ต้องมีความรู้ความเชี่ยวชาญเพียงพอในการปฏิบัติหน้าที่ทั้งหน่วยงานที่เกี่ยวข้อง ไม่ว่าจะเป็นหน่วยงานของรัฐและองค์กรทางธุรกิจยังต้องพัฒนาการทำงานให้มีเจ้าหน้าที่ผู้รับผิดชอบในการปฏิบัติการให้ตรงตามเนื้อหาและวัตถุประสงค์ของกฎหมายด้วยมิฉะนั้นจะต้องถูกดำเนินการตามกฎหมายทั้งทางแพ่ง ทางอาญา และทางปกครอง

บทความนี้จึงได้ศึกษาบทกฎหมายตามพระราชบัญญัติดังกล่าวแล้วพบว่า ยังมีปัญหาความไม่มีความชัดเจนเกี่ยวกับความหมายข้อมูลไบโอเมตริก การเก็บรวบรวม การประมวลผลข้อมูลไบโอเมตริก ข้อมูลไบโอเมตริกซึ่งเป็นข้อมูลอ่อนไหวต้องกำหนดเงื่อนไขและหลักเกณฑ์ที่ไม่เหมือนกับ

ข้อมูลส่วนบุคคลทั่วไป ตามมาตรา 26 และมาตรา 27 ซึ่งแตกต่างจาก GDPR ของสหภาพยุโรป ดังนั้น ข้อเสนอแนะสำหรับการแก้ไขปรับปรุงพระราชบัญญัติดังกล่าวก็คือ ต้องกำหนดให้ชัดเจนเกี่ยวกับความหมายของคำว่า ข้อมูลไบโอเมตริก ความหมายของข้อมูลอ่อนไหว การใช้ข้อมูลไบโอเมตริกในการประมวลผลข้อมูลส่วนบุคคลควรแยกกิจกรรมให้ชัดเจน เหล่านี้ จึงเป็นสิ่งสำคัญมากที่ต้องใช้ข้อกำหนดที่ชัดเจนในการประมวลผลข้อมูลไบโอเมตริก แม้ว่า ข้อกำหนดทางกฎหมายเกี่ยวกับข้อมูลไบโอเมตริกจะเข้มงวดเกินไป ทำให้ผู้ควบคุมข้อมูลอาจจะต้องเสียค่าใช้จ่ายมากขึ้นกว่าเดิมและต้องปฏิบัติตามขั้นตอนของกฎหมายที่มีหลักเกณฑ์ที่ค่อนข้างยุ่งยากเช่น ข้อกำหนดสำหรับการให้ความยินยอม ข้อกำหนดที่เข้มงวดขึ้นสำหรับมาตรการรักษาความปลอดภัย ก็เพื่อให้เกิดความเชื่อมั่นต่อประชาชนว่าข้อมูลส่วนบุคคลของตนจะไม่ถูกล่วงละเมิดหรือถูกนำไปใช้โดยผิดวัตถุประสงค์ อย่างไรก็ตาม การเข้มงวดที่มากเกินไปของกฎหมาย เพื่อนำข้อมูลไบโอเมตริกไปใช้ในการประมวลผลข้อมูลส่วนบุคคลอาจส่งผลเสียต่อการพัฒนาเทคโนโลยีใหม่ๆ หรือทำให้เกิดความยุ่งยากในการดำเนินธุรกิจได้ ดังนั้น รัฐจึงต้องมีหน้าที่ทำให้เกิดความเชื่อมั่นต่อประชาชนในขณะเดียวกันก็ต้องทำให้เกิดความสมดุลระหว่างสิทธิในความเป็นส่วนตัวกับการดำเนินกิจการต่าง ๆ ของผู้ควบคุมข้อมูลให้ไปในทิศทางเดียวกัน ไม่ขัดแย้งกัน เพื่อจะได้พัฒนาประเทศและการดำเนินธุรกิจไปข้างหน้าพร้อมกับการปกป้องคุ้มครองสิทธิส่วนบุคคลของประชาชนไปด้วยกัน

เอกสารอ้างอิง (References)

กุลพล พลวัน. (2547). **สิทธิมนุษยชนในสังคมโลก.** กรุงเทพฯ : สำนักพิมพ์นิติธรรม.

ณฐพร วิริยะลัพภะและธเนศ สุจารีกุล. (2563). ปัญหาทางกฎหมายเกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562: ศึกษากรณีหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 39. **ในรายงานการประชุมนำเสนอผลงานวิจัยระดับบัณฑิตศึกษา ครั้งที่ 15 ปีการศึกษา 2563**. หน้า 2195-2204. กรุงเทพฯ : มหาวิทยาลัยรังสิต.

ไทยรัฐนิวส์. (2564). **“กรุงไทยยกเลิกระบบยินยอม ในแอปเป๋าตังค์แล้ว.”** [ออนไลน์]. เข้าถึงได้จาก : https://news.ch7.com/detail/491497 สืบค้น 5 กรกฎาคม 2564.

นัยนา มาแสง. (2551, มกราคม). “เทคโนโลยีไบโอเมตริก.” **วารสารวิชาการมหาวิทยาลัยธนบุรี.** 2(1): 3-6.

บรรเจิด สิงคะเนติ และคณะ. (2554). **รายงานการวิจัยเรื่องปัญหาและมาตรการทางกฎหมายในการรับรองและคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว (Right to privacy).** กรุงเทพฯ : สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ.

ปิยะบุตร บุญอร่ามเรือง และคณะ. (2563). **Thailand data Protection Guidelines 3.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล**. ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. กรุงเทพฯ : โรงพิมพ์จุฬาลงกรณ์มหาวิทยาลัย.

สาวตรี สุขศรี. (2563). **กฎหมายว่าด้วยอาชญากรรมคอมพิวเตอร์และอาชญากรรมไซเบอร์.** (พิมพ์ครั้งที่ 2). กรุงเทพฯ : โครงการตำราและเอกสารประกอบการสอน คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์.

สุพิศ ปราณีตพลกรัง. (2563). **การคุ้มครองข้อมูลส่วนบุคคล.** กรุงเทพฯ : สำนักพิมพ์นิติธรรม.

หทัยชนก หร่ายวงศ์. (2559). **ปัญหาเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลด้านสุขภาพ.** วิทยานิพนธ์ระดับปริญญาโท (นิติศาสตรมหาบัณฑิต) คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์.

อธิพร สิทธิธีรรัตน์. (2558). **ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลในบริบท**

อิเล็กทรอนิกส์. วิทยานิพนธ์ระดับปริญญาโท (นิติศาสตรมหาบัณฑิต) คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์.

Custers et al., (2018). “A comparison of data protection legislation and policies across the EU.” **Computer Law & Security Review.** 34 (2) : 234-243.

Hassan, K. H. (2012). “Personal data protection in employment: New legal Challenges for Malaysia.” **Computer Law & Security Review.** 28 (6) : 696-703.

Puletto, C. (2021). “Options towards a global standard for the protection of individuals with regard to the processing of personal data.” **Computer Law & Security Review.** 40 : 1-21.