การคุ้มครองข้อมูลชีวมาตรภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

Biometric Data Protection under the Personal Data Protection Act 2019

เมธิชา ยุบลชิต[1]

คณะนิติศาสตร์ มหาวิทยาลัยศรีปทุม 2410/2 ถนนพหลโยธิน แขวงเสนานิคม เขตจตุจักร กรุงเทพฯ 10900
เมล์ติดต่อ: Methichc_y@hotmail.com

Methicha Yuboolchit

School of Law, Sripatum University, 2410/2 Phahonyothin Road, Sena Nikhom, Chatuchak, Bangkok 10900, E-mail: Methichc_y@hotmail.com

Received: July 9, 2020; Revised: April 7, 2021; Accepted: April 27, 2021

บทคัดย่อ

บทความฉบับนี้ มีวัตถุประสงค์เพื่อศึกษามาตรการทางกฎหมายและความเป็นส่วนตัวของชีวมาตร ปัจจุบันชีวมาตร (Biometrics) ถูกนำมาใช้พัฒนาเทคโนโลยีด้านวิทยาศาสตร์ หรือใช้กับแอปพลิเคชันต่าง ๆ การเก็บรักษาข้อมูลชีวมาตรในรูปดิจิทัลจะถูกบันทึกไว้ในระบบฐานข้อมูลของผู้ให้บริการ จึงเสี่ยงต่อการถูกคุกคามและไวต่อความเสียหายมากกว่าข้อมูลในรูปแบบอื่น ๆ อย่างไรก็ตามภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 6 บัญญัติให้ความคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป แต่มิได้ให้ความคุ้มครองข้อมูลชีวมาตรที่ชัดเจนและครอบคลุมเพียงพอ เช่น ร่องรอยเท้าดิจิทัล (Digital footprints) ซึ่งข้อมูลต่าง ๆ ของผู้ใช้บริการค้างอยู่ในระบบออนไลน์และอาจถูกนำไปใช้ระบุตัวตนในอนาคตได้ตลอด ซึ่งเจ้าของข้อมูลมี “สิทธิที่จะถูกลืม” (Right to be forgotten) เพราะว่าร่องรอยเท้าดิจิทัลยังคงอยู่เสมอ ผู้เขียนจึงขอเสนอแนะให้มีการแก้ไขคำนิยามว่าด้วยการคุ้มครองข้อมูลชีวมาตรไว้เป็นการเฉพาะ

[1] นักวิจัยอิสระ (Researcher)

โดยเพิ่มคำนิยามคำว่า “ข้อมูลชีวมาตร (Biometrics)” ไว้ในมาตรา 6 เพื่อให้ได้รับการคุ้มครองในการใช้เทคโนโลยีชีวมาตร (Biometrics) ตามที่กฎหมายบัญญัติไว้ให้เทียบเท่ากับมาตรฐานสากล

คำสำคัญ: ข้อมูลส่วนบุคคล ข้อมูลชีวมาตร ข้อมูลที่ละเอียดอ่อน ความเป็นส่วนตัว

Abstract

The purpose of this abstract is to study the legal and privacy measures of biometric systems. At present, biometrics are used throughout for technology development and various applications. The retention of biometric data in digital format by the service provider may be vulnerable to threats and damage than other forms of information. However, under the Personal Data Protection Act 2019, Section 6 provides for general protection of personal information, but it does not provide adequate and clear biometric data protection, such as digital footprints where the user's information is stuck online and may be used to identify that particular person in the future. The data subject has "Right to be forgotten" because digital footprints are always intact. Therefore, the author recommends a specific revision of the definition of biometric data protection. By adding the word definition "Biometric data (Biometrics)" in Section 6 to be protected in the use of biometric technology (Biometrics) as provided by law to be equivalent to that of international standards.

Keywords: Personal Data, Biometric Data, Sensitive Data, Privacy

1. บทนำ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ประกาศในราชกิจจานุเบกษา เมื่อวันที่ 24 พฤษภาคม 2562 โดยจะมีผลกระทบต่อหน่วยงานรัฐ หรือองค์กรเอกชน รวมทั้งภาคประชาชน แม้ว่ากฎหมายมีผลบังคับใช้เพื่อควบคุมในการรวบรวมและเก็บข้อมูลส่วนบุคคลแล้ว แต่ยังมีประเด็นที่น่าสังเกตว่าในทางปฏิบัติ หรือการบังคับใช้กฎหมายในเรื่องการเก็บ “ข้อมูลชีวมาตร (Biometrics)” และการใช้เทคโนโลยีชีวมาตรของหน่วยงานรัฐ หรือหน่วยงานเอกชนเกี่ยวกับความเสี่ยงที่อาจมีการละเมิดสิทธิความเป็นส่วนตัว

ปัจจุบันเป็นยุคข่าวสารดิจิทัล อย่างไรก็ตาม การนำข้อมูลชีวมาตรไปประมวลผลข้อมูลนั้น จึงขึ้นอยู่กับการรักษาความปลอดภัย และการรับรองความถูกต้องของระบบไบโอเมตริกซ์ ซึ่งแตกต่างจากการใช้รหัสผ่าน หรือพาสเวิร์ด (Password) ที่สามารถแก้ไขเปลี่ยนแปลงรหัสผ่านได้ในกรณีที่มีการแฮค (Hack) ข้อมูลของผู้ใช้บริการออนไลน์ นอกจากนี้ รหัสผ่านผู้ใช้ยังสามารถจดบันทึกไว้ได้ด้วยตนเอง แต่เมื่อข้อมูลชีวมาตรไม่สามารถเปลี่ยนแปลงลายนิ้วมือ หรือลักษณะใบหน้าได้ จึงทำให้มีความเสี่ยงที่ข้อมูลชีวมาตรถูกแฮค (Hack) สำเร็จ ดังนั้น จึงต้องควรคำนึงถึงมาตรการป้องกันอย่างรัดกุมของรหัสผ่านที่ดีก็จะไม่ตกอยู่ในสถานการณ์เช่นเดียวกับข้อมูลชีวมาตรที่บุคคลอื่นสามารถที่จะนำไปใช้เพื่อการแสวงหาผลประโยชน์โดยมิชอบ ทั้งนี้ การนำเทคโนโลยีไบโอเมตริกซ์มาช่วยในการทำธุรกรรมต่าง ๆ หรือการนำข้อมูลชีวมาตรมาใช้ในทางการค้าได้อย่างมีประสิทธิภาพ เพียงแค่ใช้ลายนิ้วมือก็สามารถซื้อขายสินค้าได้สะดวกและรวดเร็วนั้น ประกอบกับความก้าวหน้าทางเทคโนโลยีทำให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลทำได้โดยง่าย สะดวก รวดเร็ว ซึ่งการใช้ข้อมูลชีวมาตรจะไม่เหมือนกับการใช้รหัสผ่านที่เป็นตัวเลข หรือบัตรแถบแม่เหล็กนั้นเอง

เนื่องจากข้อมูลชีวมาตร (Biometrics) นี้มีลักษณะเฉพาะของแต่ละบุคคลที่มีความถูกต้องแม่นยำสูงและมีความคงสภาพ ซึ่งลอกเลียนแบบได้ยาก จึงมีความน่าเชื่อถือเหมาะสมในการพิสูจน์และระบุตัวบุคคล นอกจากนี้ ผู้ประกอบการธุรกิจทางออนไลน์ หรือสถาบันทางการเงิน หรืออหน่วยงานภาครัฐ เช่น สำนักงานทะเบียนราษฎร์ได้ถูกนำมาใช้กับการระบุยืนยันตัวบุคคล และได้ทำการจัดเก็บ รวบรวมข้อมูลชีวมาตรไว้ในระบบฐานข้อมูลของตน[2] นำระบบไบโอเมตริกซ์ไปใช้ในการทำธุรกรรมต่าง ๆ ภายในองค์กร หรือการให้บริการกับลูกค้า เช่น การสแกนลายนิ้วมือ การสแกนม่านตา สแกนใบหน้า เป็นต้น อาจมีการเข้าถึงข้อมูลของผู้ใช้บริการ หรือนำข้อมูลส่วนบุคคลไปใช้งานโดยมิได้รับอนุญาต ก่อให้เกิดการล่วงละเมิดสิทธิ

[2] มัณฑณา ศรีพงษ์พันธ์, “ปัญหาทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล:ศึกษาเฉพาะกรณีข้อมูลตำแหน่งของผู้ใช้บริการ,” (วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยศรีปทุม, 2561): 46.

ความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลสร้างความเดือดร้อน รำคาญ หรือก่อความเสียหายให้แก่เจ้าของข้อมูล หากมีการเข้าถึงข้อมูลชีวมาตรจะไม่สามารถเปลี่ยนแปลงแก้ไขได้และมีผลกระทบร้ายแรงต่อชีวิตของผู้ที่เป็นเจ้าของข้อมูลส่วนบุคคลเหล่านี้ ควรต้องคำนึงถึงความเสี่ยงในการเข้าถึงข้อมูลชีวมาตร จึงจำเป็นต้องมีมาตรการทางกฎหมายเพื่อกำหนดหลักเกณฑ์ในการกำกับดูแล และให้ความคุ้มครองข้อมูลชีวมาตร

ด้วยเหตุนี้ การเก็บรักษาต้องเก็บข้อมูลชีวมาตรได้เฉพาะบางประเภท หรือลดขนาดระบบของฐานข้อมูลในการประมวลผลข้อมูลชีวมาตร (Biometrics) ต้องมีการขอความยินยอมหรือบังคับให้หน่วยงานขององค์กรต่าง ๆ หรือผู้ให้บริการ หรือผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บข้อมูลชีวมาตรประเภทใดได้นั้น จะต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนอย่างชัดเจน มิใช่การยินยอมโดยอัตโนมัติ และเจ้าของข้อมูลส่วนบุคคลสามารถถอนความยินยอมเมื่อไหร่ก็ได้ โดยไม่มีข้อแม้หรือเงื่อนไข เว้นแต่จะมีข้อจำกัดสิทธิโดยบทบัญญัติของกฎหมาย หรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลก่อนที่จะค้นหาข้อมูลชีวมาตร เพื่อปกป้อง และควบคุมการจัดเก็บ การใช้ หรือการแบ่งปันข้อมูลชีวมาตร โดยจะต้องเปิดเผยนโยบายแจ้งเตือนก่อนเป็นลายลักษณ์อักษรเกี่ยวกับกระบวนการในการดำเนินงาน ระยะเวลาในการทำลายข้อมูลชีวมาตร และรับรองความโปร่งใส เพื่อให้เกิดความเชื่อมั่นของประชาชนที่จะได้รับการคุ้มครองสิทธิตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562[3] โดยเพิ่มบทนิยามคำว่า “ข้อมูลชีวมาตร (Biometrics) ในมาตรา 6 เพื่อป้องกันผลกระทบจากกฎหมายในการใช้ข้อมูลชีวมาตร

2. การระบุตัวตนของบุคคลด้วยเทคโนโลยีไบโอเมตริกซ์

ปัจจุบันการบริการต่าง ๆ ในการทำธุรกรรมง่ายขึ้นและรวดเร็วมากขึ้นผู้บริโภคทั่วไปสามารถเข้าถึงแหล่งบริการทางออนไลน์ผ่านทางอิเล็กทรอนิกส์ และขณะเดียวกันอยู่ในช่วงเปลี่ยนถ่ายระบบจากการยืนยันตัวตนด้วยการใส่รหัสผ่านเป็นตัวเลข มาเป็นระบบชีวมาตร (Biometrics) ซึ่งสามารถพิจารณาได้ ต่อไปนี้

2.1 ความหมายของชีวมาตร หรือไบโอเมตริกซ์ (Biometrics)

หมายถึง “ลักษณะทางกายภาพ และพฤติกรรมที่สามารถวัดผลได้ ซึ่งทำให้สามารถสร้างและยืนยันตัวตนของแต่ละบุคคลได้” จำแนกลักษณะเฉพาะ (Identification) ดังนั้น ลักษณะทางชีวมาตรตั้งแต่การสแกนลายนิ้วมือรวมถึงเครื่องสแกนม่านตา หรือการจดจำใบหน้า และ

[3] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 23 (3)

การรู้จำเสียง[4] แม้ว่าสิ่งเหล่านี้จะเป็นลักษณะทางกายภาพที่ใช้กันมากที่สุดสำหรับผู้บริโภค แต่ก็มีแอปพลิเคชันอื่น ๆ ที่มุ่งเน้นไปที่พฤติกรรม เช่น การจดจำเสียง (Voice recognition) การกดแป้นพิมพ์ (Keystroke dynamics) วิเคราะห์การเดิน (Gait analysis) การวิเคราะห์ลายเซ็น (Signature analysis) ไบโอเมตริกซ์ทางปัญญา (Cognitive biometrics) ลักษณะการใช้เมาส์ (Mouse use characteristics)[5] เป็นต้น

2.2 การจัดการข้อมูลส่วนบุคคลที่อ่อนไหวง่าย (Sensitive data)

หน่วยงานภาครัฐได้มีการใช้ระบบชีวมาตรนี้ในการลงทะเบียนซิมการ์ด โดยเฉพาะอย่างยิ่งธุรกรรมออนไลน์ด้านการเงินการธนาคาร ในการชำระเงินผ่านอุปกรณ์สมาร์ตโฟน หรือการบริการต่าง ๆ เพื่อเพิ่มความปลอดภัยในการปลดล็อคแอปพลิเคชัน โดยไม่ต้องใส่รหัส (Password) หรือใช้แทนการปลดล็อคแอปพลิเคชันในกรณีลืมรหัสเข้าใช้งาน หรือป้องกันการเข้าถึงข้อมูลในระบบสมาร์ตโฟน หากข้อมูลชีวมาตรชนิดนี้หายไป หรือตกไปอยู่ในการครอบครองของบุคคลอื่นได้ ย่อมจะไม่สามารถแก้ไขได้เหมือนรหัสผ่าน ดังนั้น สิทธิในข้อมูลส่วนบุคคลนี้ ควรให้บุคคลใดบ้างมีสิทธิที่จะเข้าถึงและใช้ประโยชน์จากผู้เป็นเจ้าของข้อมูลเหล่านี้ได้บ้าง และที่สำคัญประการหนึ่ง กล่าวคือ การจัดการข้อมูลส่วนบุคคลที่อ่อนไหวง่าย (Sensitive data)[6] ซึ่งมีความละเอียดอ่อนและสุ่มเสี่ยงต่อการนำไปใช้เพื่อแสวงหาผลประโยชน์ และการเลือกปฏิบัติอย่างไม่เป็นธรรม จึงต้องดำเนินการด้วยความระมัดระวังพิเศษ ได้แก่ การจำแนกประเภทข้อมูลชีวมาตร และหรือข้อมูลส่วนบุคคล และการบังคับใช้ ตามประเภทของความเสี่ยงและความร้ายแรงของผลกระทบต่อสิทธิและเสรีภาพของบุคคล ถือว่าเป็นข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวโดยแท้

อย่างไรก็ตาม ปัญหาการนำข้อมูลส่วนบุคคลไปใช้โดยมิได้รับความยินยอมก่อน หรือแม้กระทั้งให้ความยินยอมแล้วก็ตาม ก็ต้องคำนึงถึงสิทธิส่วนตัวของบุคคลที่ผู้อื่นจะล่วงละเมิดมิได้ อันเป็นสิทธิในความเป็นส่วนตัวของแต่ละบุคคล อันนำมาซึ่งการศึกษาเปรียบเทียบกฎหมายที่เกี่ยวกับการควบคุมการใช้ข้อมูลชีวมาตร รวมถึง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และพระราชบัญญัติคุ้มครองข้อมูลไบโอเมตริกซ์ของรัฐอิลลินอยส์ Illinois Biometric Information Privacy Act: 2008 (BIPA) แห่งสหรัฐอเมริกา ซึ่งมีความสอดคล้องกับกฎ ระเบียบ

---

[4] อภิชัย แผลงศร, *เอกสารประกอบการบรรยาย การระบุบุคคล (Identification)* (กรุงเทพฯ: ภาควิชานิติเวชวิทยา คณะแพทยศาสตร์ มหาวิทยาลัยศรีนครินทรวิโรฒ, 2559), 52.

[5] เอกรินทร์ ซื่อธานุวงศ์, "ระบบตรวจสอบลายนิ้วมือฝังตัว," (วิทยานิพนธ์ปริญญามหาบัณฑิต คณะวิศวกรรมศาสตร์ มหาวิทยาลัยสงขลานครินทร์, 2548), 23.

[6] ศิริกุล ภู่พันธ์, "ข้อความคิดว่าด้วยข้อมูลข่าวสารส่วนบุคคล," (วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัย ธรรมศาสตร์, 2548), 83.

ข้อบังคับของ General Data Protection Regulation: 2018 (GDPR) แห่งสหภาพยุโรปอันเป็นต้นแบบของมาตรการทางกฎหมาย ซึ่งคุ้มครองและป้องกันสิทธิในความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคล โดยจะนำไปใช้ได้ต่อเมื่อได้รับความยินยอมจากผู้เป็นเจ้าของข้อมูลก่อนโดยชัดแจ้ง หากมีการเก็บรวบรวม การใช้ การประมวลผลข้อมูล หรือจำเป็นต่อการปฏิบัติงาน หรือจำเป็นสำหรับการปกป้องผลประโยชน์ที่สำคัญของแต่ละบุคคล โดยหลักการสำคัญของกฎหมาย (BIPA) ห้ามประมวลผลข้อมูล เปิดเผย เช่าซื้อ ซื้อขาย เว้นแต่ กระทำไปเพื่อความมั่นคงปลอดภัยของสังคม หรือมีกฎหมายบัญญัติให้กระทำได้ ตาม 740 ILCS 14/15 (c)[7]

ประวัติโดยย่อของกฎหมายข้อมูลชีวมาตรแห่งรัฐอิลลินอยส์ (Biometric Information Privacy:BIPA) ซึ่งบังคับเมื่อปี ค.ศ 2008 เป็นครั้งแรกที่รัฐอิลลินอยส์ให้ความสำคัญเกี่ยวกับลายนิ้วมือ และมีการบังคับใช้กฎหมายดังกล่าวเพิ่มอีกในสองรัฐ คือ รัฐเท็กซัส กฎหมายการใช้กฎระเบียบการระบุตัวตนทางชีวมาตร (Texas Biometric Identifier Statute: BIS) และรัฐวอชิงตัน กฎหมายการระบุตัวตนทางชีวมาตรของวอชิงตัน (Washington Biological Identification Law: BI) จากการศึกษามาตรการทั้งสามรัฐข้างต้น พบว่า รัฐอิลลินอยส์ (BIPA) ห้ามมิให้องค์กรต่าง ๆ ที่มีข้อมูลชีวมาตรเปิดเผยข้อมูลส่วนบุคคลดังกล่าว เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลก่อน ซึ่งต้องแจ้ง “ล่วงหน้า” ตั้งแต่ครั้งแรกที่เริ่มใช้ ตาม 740 ILCS 10/15 (b)[8] หลักความยินยอม มิใช่เพียงแค่ “แจ้ง” หากองค์กรผู้ให้บริการไม่แจ้งขอให้ความยินยอมล่วงหน้าเป็นลายลักษณ์อักษรแก่เจ้าของข้อมูลทราบก่อน และควบคุมการจัดเก็บรวบรวมข้อมูลชีวมาตร โดยไบโอเมตริกซ์ (Biometrics) รวมถึงลายนิ้วมือ (DNA) ท่าทางการเดิน จังหวะการพิมพ์ การพิมพ์เสียง รูปแบบหลอดเลือดดำและรูปทรงของใบหน้า หรือเพียงแค่ชื่อไม่กี่ชื่อ เป็นต้น สำหรับผู้ให้บริการด้านการดูแลสุขภาพรวบรวมข้อมูลที่ระบุตัวตนเกี่ยวกับผู้ป่วยนั้น ซึ่งโดยปกติจะรวมถึงข้อมูลพันธุกรรม (DNA)[9] เมื่อมีการละเมิดก็เพียงพอที่จะนำคดีขึ้นสู่ศาล แม้ว่าเจ้าของข้อมูลส่วนบุคคลจะไม่ได้รับผลกระทบจากการไม่แจ้งความยินยอมดังกล่าวนั้นก็ตาม ผู้เสียหายไม่จำเป็นต้องแสดงความเสียหายเพิ่มเติม กฎหมายก็ถือว่าละเมิดกฎหมาย ผู้เสียหายสามารถเรียกค่าเสียหายได้เองตามความเหมาะสม ซึ่งมีเฉพาะมลรัฐอิลลินอยส์ ซึ่งมลรัฐอื่นต้องได้รับอนุญาต

---

[7] 740 ILCS 14/15 (c) No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person’s or a customer’s biometric identifier or biometric information.

[8] (740 ILCS 14/15)

Sec. 15. Retention; collection; disclosure; destruction.

(b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person’s or a customer’s biometric identifier or biometric information, unless it first:

[9] Hannah Zimmerman, “The Data of You: Regulating Private Industry’s Collection of Biometric Information,” *Kansas Law Reviews* 66 (2018): 637-617.

จากศาลก่อน ด้วยเหตุนี้ จึงมีความจำเป็นในการแก้ไขมาตรการทางกฎหมาย เพื่อคุ้มครองสิทธิในความเป็นส่วนตัวนี้ต้องอาศัยบทบัญญัติของกฎหมายที่เกี่ยวข้องคุ้มครอง และป้องกันสิทธิในความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคล เช่น ตัวอย่าง คดี Rosenbach v. Six Flags

เมื่อวันที่ 25 มกราคม 2019[10] ศาลฎีกาแห่งรัฐอิลลินอยส์ได้กลับคำพิพากษาของศาลอุทธรณ์ของรัฐไว้ว่าเป็นการละเมิดกฎหมายความเป็นส่วนตัวด้านข้อมูลทางชีวมาตรของรัฐอิลลินอยส์ “BIPA” 740 ILL COMP. STAT 14 (2008) คดี โจทก์ Rosenbach และ Six Flags จำเลย โดย Rosenbach โจทก์ได้ทำการซื้อบัตรผ่านเข้าสู่ซีซันสวนสนุกให้บุตรชายวัย 14 ปี ของโจทก์ ซึ่งเป็นส่วนหนึ่งของการทัศนศึกษาที่สวนสนุก Six Flags Amusement Park โดยบุตรชายของโจทก์จะต้องถูกส่งสแกนลายนิ้วมือเพื่อใช้บัตรผ่านเข้าสวนสนุก โดยบุตรชายของโจทก์ก่อนหน้านี้เคยพยายามเปิดใช้งานบัตรผ่านดังกล่าวแล้ว แต่ไม่สามารถใช้งานได้ โดยโจทก์ไม่ได้รับการแจ้งเกี่ยวกับข้อกำหนดการสแกนลายนิ้วมือ หรือวิธีการใช้ หรือจัดเก็บข้อมูลที่สำคัญแต่อย่างใด แม้ว่าโจทก์จะไม่ได้กล่าวอ้างว่าการละเมิดครั้งนี้ก่อให้เกิดความเสียหายทางการเงินหรือด้านอื่น ๆ ใดก็ตาม แต่จากการตรวจสอบข้อเท็จจริงเหล่านี้แล้ว ศาลฎีการัฐอิลลินอยส์ได้ยอมรับข้อโต้แย้งของโจทก์ว่านโยบายของจำเลย ซึ่งไม่ได้แจ้งเกี่ยวกับการใช้ข้อมูลชีวมาตรก็เป็นการเพียงพอในการละเมิดกฎหมาย (BIPA) แล้ว

ดังนั้น จะเห็นได้ว่ารัฐอิลลินอยส์ได้บัญญัติกฎหมายเพื่อคุ้มครองให้บุคคลสามารถควบคุมข้อมูลชีวมาตร หรือไบโอเมตริกซ์ของตนได้ โดยบัญญัติกฎหมายให้มีการ “แจ้ง” เตือนให้เจ้าของข้อมูลทราบในการใช้ข้อมูลชีวมาตร เช่น ลายนิ้วมือ ดีเอ็นเอ การสแกนใบหน้า และข้อมูลทางชีววิทยาอื่น ๆ พระราชบัญญัติข้อมูลไบโอเมตริกซ์ (BIPA) ห้ามมิให้หน่วยงานต่าง ๆ หรือบริษัทเอกชนรวบรวมข้อมูลชีวมาตรของบุคคล ตาม 740 ILCS 14/25 (d) และระยะเวลาในการเก็บรักษาข้อมูล กฎหมายยังกำหนดให้ บริษัทต่าง ๆ ต้องปกป้องความลับของข้อมูลชีวมาตร ตาม 740 ILCS 14/25 (e)[11]

มาตรการกฎหมาย (BIPA) กำหนดให้องค์กรธุรกิจที่รวบรวม หรือจัดเก็บข้อมูลชีวมาตรต้องดำเนินการดังต่อไปนี้

1. กำหนดนโยบายเป็นลายลักษณ์อักษรพร้อมวิธีการเก็บรักษาข้อมูล และแนวทางในการทำลายตัวระบุชีวมาตรอย่างถาวร

---

[10] Illinois Official Reports Supreme Court, “Rosenbach v. Six Flags Entertainment Corp., 2019 IL 123186,” accessed July 29, 2020, https://courts.illinois.gov/Opinions/SupremeCourt/2019/123186.pdf.

[11] 740 ILCS 14/25 (e) Nothing in this Act shall be construed to apply to a contractor, subcontractor, or agent of a State agency or local unit of government when working for that State agency or local unit of government.

2. นโยบายแจ้งเตือนให้เจ้าของข้อมูลชีวมาตรทราบเป็นลายลักษณ์อักษรว่าข้อมูลชีวมาตรกำลังจะถูกรวบรวม หรือจัดเก็บตามวัตถุประสงค์และระยะเวลาที่จะจัดเก็บและการใช้ตัวระบุชีวมาตร

3. ได้ตอบรับการให้ความยินยอมเป็นลายลักษณ์อักษรจากเจ้าของข้อมูล และ

4. ไม่ส่งต่อข้อมูลชีวมาตร หรือเปิดเผยข้อมูลชีวมาตรให้กับบุคคลที่สามโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลเสียก่อน

เมื่อนำหลักการดังกล่าวมาพิจารณาเปรียบเทียบกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พบว่า ยังมิได้มีมาตรการกำหนดให้ผู้ประกอบธุรกิจต่าง ๆ แจ้งเตือนให้บุคคลทราบถึง “มาตรฐานการดูแลที่เหมาะสม” ในการจัดเก็บ รวบรวม ส่ง หรือการปกป้องข้อมูลชีวมาตร หรือไบโอเมตริกซ์ เพื่อปกป้องความเป็นส่วนตัวของบุคคลที่ให้ใช้ข้อมูล โดยกำหนดให้หน่วยงานธุรกิจที่รวบรวม หรือจัดเก็บข้อมูลชีวมาตรจะต้องดำเนินการอย่างไรภายใต้บทบัญญัติของกฎหมาย

3. วิเคราะห์พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ความเป็นส่วนตัวของข้อมูลชีวมาตร (Biometrics) ควรจะมีความหมายอย่างไร

เมื่อวันที่ 7 ตุลาคม 2557 โดยสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ (สขร.) เสนอร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ถูกบรรจุเข้าไปในวาระของสภานิติบัญญัติแห่งชาติ (สนช.) ไปแล้วหนึ่งฉบับ ซึ่งเป็นกฎหมายที่เสนอโดยสำนักนายกรัฐมนตรี ได้ค้างพิจารณามาจากสภา ซึ่งสภานิติบัญญัติแห่งชาติได้เสนอร่างกฎหมายพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ...สองฉบับภายใต้ชื่อเดียวกันที่ผ่านการพิจารณาแล้ว เรื่องที่ 1135/2558 เมื่อเปรียบเทียบร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ...ทั้งสองฉบับ จะพบหลักการที่เปลี่ยนแปลงไปในร่างพระบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับใหม่ ดังนี้

3.1 ปัญหาคำจำกัดความของคำนิยามศัพท์ “ข้อมูลชีวมาตร (Biometrics)

แก้ไขนิยามศัพท์ ของคำว่า “ข้อมูลส่วนบุคคล” ใหม่ให้สั้นลงแต่ตีความได้กว้างขึ้น จากข้อมูลส่วนบุคคลที่เกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม ประวัติการทำงาน หรือประวัติกิจกรรม และเลขหมาย รหัส หรือสิ่งที่บ่งบอกลักษณะอื่นที่จะทำให้รู้ตัวบุคคลนั้นได้ เช่น ลายนิ้วมือ แผ่นบันทึกลักษณะ เสียงของคน รูปถ่าย

เหลือเพียงข้อมูลเกี่ยวข้องกับบุคคล[12] ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม ตามนัยมาตรา 6 ฉบับปัจจุบัน ซึ่งเป็นการบัญญัติคำนิยามแบบกว้าง และเป็นการทั่วไป

จากปัญหาคำจำกัดความของคำนิยาม **"ข้อมูลชีวมาตร (Biometrics)"**[13] ซึ่งเป็นข้อมูลลับเฉพาะของบุคคลที่มีความอ่อนไหวง่าย อีกทั้ง มิได้จำแนกประเภทของข้อมูลส่วนบุคคลให้มีความชัดเจน อาจส่งผลกระทบในทางปฏิบัติแก่ผู้ควบคุม หรือผู้ประมวลผลข้อมูล และเจ้าของข้อมูลส่วนบุคคล อาจตีความหมายตามเจตนาของตนว่าเป็นข้อมูลทั่วไป หรือหากเกิดข้อพิพาทจำต้องใช้ดุลยพินิจในการตีความหมายเพื่อการบังคับใช้กฎหมายให้เป็นตามบทบัญญัติ จึงต้องพิจารณาความหมายของ "ข้อมูลชีวมาตร (Biometrics)" ดังนี้

"ข้อมูลชีวมาตร (Biometrics)" ซึ่งเป็นข้อมูลที่เกิดจากเทคโนโลยีด้านชีวมาตรและทางการแพทย์ และเทคโนโลยีทางคอมพิวเตอร์เข้าด้วยกัน เพื่อยืนยันในการระบุความเป็นตัวตน (Individual's Identity) จึงเป็นข้อมูลลับเฉพาะของบุคคลที่มีความอ่อนไหวง่าย จะต้องได้รับการคุ้มครองเป็นกรณีพิเศษเฉพาะเจาะจง และจำแนกประเภทออกจากข้อมูลทั่วไป

จากการศึกษาผู้เขียนเห็นว่า ควรให้ความสำคัญคำนิยามศัพท์ข้อมูลชีวมาตร ซึ่งมีความแตกต่างกันในประเภทของข้อมูลส่วนบุคคล โดยทำการเปรียบเทียบกับพระราชบัญญัติคุ้มครองข้อมูลไบโอเมตริกซ์ของสหรัฐอเมริกาดังนี้

พระราชบัญญัติคุ้มครองข้อมูลไบโอเมตริกซ์ของสหรัฐอเมริกา (Biometric Information Privacy Act 2008: BIPA) ได้บัญญัติคำนิยามประเภท "ข้อมูลชีวมาตร (Biometrics)" โดยจำแนกประเภทของข้อมูลชีวมาตรให้ชัดเจนออกจากประเภทข้อมูลทั่วไป เว้นแต่ ข้อมูลที่ได้จากการรวบรวม หรือขั้นตอนที่ได้รับการยกเว้นภายใต้คำจำกัดความ ตาม Section 10[14] ทำให้ผู้ปฏิบัติหน้าที่เกี่ยวกับข้อมูลส่วนบุคคลดังกล่าวนี้ ไม่จำต้องตีความหมายว่าข้อมูลที่เกิดจากผลทางเทคโนโลยีตามพระราชบัญญัติทางกายวิภาคแห่งรัฐอิลลินอยส์เป็นข้อมูลประเภทใด กฎหมายไม่เพียงกำหนดให้ต้องปฏิบัติตาม "เกณฑ์มาตรฐานในการดูแลที่เหมาะสมในองค์กรเอกชน" กฎหมายยังได้อธิบายการใช้เทคโนโลยี (Biometrics) อีกด้วย ดังนั้น องค์กร

---

[12] ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ผ่านการพิจารณาแล้ว เรื่องที่1135/2558

[13] นัยนา มาแสง, "*เทคโนโลยีไบโอเมตริกซ์*," *วารสารวิชาการ มหาวิทยาลัยธนบุรี* 2, ฉ.1 (2551): 3-6.

[14] (740 ILCS 14/10) Section. 10. Definitions. In this Act. reads:

"Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual, "Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers," accessed December 24, 2019, http://gtclawgroup.com/wp-content/uploads/2017/11/Illinois-2017-law-Biometric-Information-Privacy-Act.pdf.

ที่อยู่ภายใต้ BIPA จึงต้องตรวจสอบให้แน่ใจว่า “ข้อมูลชีวมาตร” ได้รับการปกป้องและคุ้มครองมิให้ถูกละเมิดเป็นกรณีพิเศษ

เมื่อเปรียบเทียบคำนิยามศัพท์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ผู้เขียน พบว่า มีเจตนามุ่งให้เป็นกฎหมายกลางและตีความได้กว้างนั้น อาจเพราะมีกฎหมายอื่น ๆ บัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในลักษณะใดไว้เป็นการเฉพาะแล้ว แต่ก็มิได้บัญญัติคำนิยามศัพท์ไว้ในมาตรา 6 บทนิยามแต่อย่างใด จึงมิอาจทราบความหมายเฉพาะได้ว่า “ข้อมูลชีวมาตร” เป็นข้อมูลที่เกิดจากเทคนิค และเทคโนโลยีทางการแพทย์ที่มีความละเอียดอ่อน และเป็นข้อมูลลับเฉพาะของบุคคล ซึ่งต้องระวังเป็นกรณีพิเศษ และต้องจำแนกประเภทข้อมูลชีวมาตรออกจากข้อมูลทั่วไป เมื่อพิจารณากฎหมาย BIPA ของสหรัฐอเมริกาได้บัญญัติ “ข้อมูลชีวมาตร” ไว้ในบทนิยามคำศัพท์ และจำแนกประเภทข้อมูลชีวมาตรออกจากข้อมูลส่วนบุคคลทั่วไปไว้อย่างชัดเจน ตาม 740 ILCS 14/10 จึงสามารถทราบ และเข้าใจได้ว่าข้อมูลใดมีความละเอียดอ่อนไหวง่าย และข้อมูลใดเป็นข้อมูลทั่วไป เพื่อประโยชน์ในการทำธุรกรรมต่าง ๆ หรือในการพิสูจน์ยืนยันตัวตนของบุคคล ในระบบดิจิทัล

ผู้เขียนพบข้อสังเกตว่า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ตามนัยมาตรา 24 “ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่มีความจำเป็นเพื่อการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ.....”

มาตรา 27 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่ข้อมูลส่วนบุคคลที่เก็บรวบรวมได้รับการยกเว้น โดยไม่ต้องขอความยินยอมตาม มาตรา 24 หรือมาตรา 26

แม้ปรากฏว่ามาตรา 26 บัญญัติห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับข้อมูลชีวมาตร โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลก่อนนั้นก็ตาม แต่ก็ยังมีประเด็นในเรื่องการบังคับใช้กฎหมายของหน่วยงานรัฐหลายแห่ง อาจใช้อำนาจรัฐในการบังคับการเก็บข้อมูลชีวมาตรของประชาชน โดยไม่คำนึงถึงผลกระทบที่จะเกิดกับเจ้าของข้อมูลชีวมาตรในกรณีที่เกิดการรั่วไหล หรือถูกนำข้อมูลชีวมาตรไปใช้ในทางที่มิชอบโดยเจ้าหน้าที่ของรัฐเอง[15]

ดังนั้น การบัญญัติคำนิยามศัพท์ “ข้อมูลชีวมาตร (Biometrics)” สามารถทำให้ทราบถึงประเภทข้อมูลที่เกิดจากเทคโนโลยีทางการแพทย์ซึ่งเป็นข้อมูลลับเฉพาะของบุคคลโดยแท้

---

[15] ประชาไทย, “กลุ่มนักวิชาการยื่นหนังสือนายกฯ ห่วงรัฐเก็บข้อมูลชีวมาตรไม่โปร่งใส ไม่มีธรรมาภิบาล,” สืบค้นเมื่อ 9 สิงหาคม 2562, https://prachatai.com/journal/2019/08/83824.

ที่ต้องระมัดระวังเป็นกรณีพิเศษ ในทางปฏิบัติจะทำให้ผู้ควบคุม หรือผู้ประมวลผลข้อมูล และเจ้าของข้อมูลเข้าใจถึงความหมายของ “ข้อมูลชีวมาตร” ตรงกัน รวมถึง เข้าใจว่าข้อมูลประเภทใดเป็นข้อมูลทั่วไป และหากเกิดข้อพิพาทไม่จำต้องใช้ดุลยพินิจของศาลในการตีความ เพื่อการบังคับใช้กฎหมาย เนื่องจากมีบทบัญญัติซึ่งกำหนดประเภทของ “ข้อมูลชีวมาตร” ไว้อย่างชัดแจ้ง

3.2 หลักการความยินยอม (Consent) ข้อมูลชีวมาตร (Biometrics)

สำหรับธุรกิจออนไลน์ต้องให้แน่ใจว่าความเป็นส่วนตัวของผู้ใช้บริการที่เข้าเว็บไซต์นั้นจะต้องได้รับความคุ้มครอง กล่าวคือ ก่อนที่ข้อมูลส่วนบุคคลจะถูกเก็บรวบรวม ใช้ การเผยแพร่ ผู้ใช้บริการต้องได้รับแจ้งเตือนการให้ความยินยอมเป็นลายลักษณ์อักษรก่อน จึงจำเป็นต้องมีนโยบายความเป็นส่วนตัวนี้ สิทธิความเป็นส่วนตัวของผู้ใช้บริการต้องมีมาตรการป้องกันการเข้าถึงจากสาธารณะเป็นสิ่งสำคัญ แต่ต้องอยู่ภายใต้กฎหมายในการถูกจำกัดสิทธิ อันเป็นข้อยกเว้นของกฎระเบียบ ข้อบังคับในการประมวลผลข้อมูลส่วนบุคคล โดย Biometric Information Privacy Act 2008 (BIPA) ของสหรัฐอเมริกา มุ่งเน้นความสำคัญเช่นเดียวกันกับ GDPR ของสหภาพยุโรป ดังนี้[16]

1. ความยินยอมอย่างอิสระ (Freely given) ดำเนินการตรวจสอบได้ชัดเจนและยืนยันได้ (Verified using a clear, affirmative action) แจ้งเตือนความยินยอม (Informed) เฉพาะเจาะจง (Specific) ไม่คลุมเคลือ (Unambiguous)

2. แนวทางปฏิบัติของผู้ประกอบการธุรกิจในบางประการต้องทำเพื่อหลีกเลี่ยงการละเมิดความเป็นส่วนตัว ต้องมิใช่การให้ความยินยอมโดยอัตโนมัติในรูปแบบของการเว้นช่องว่างให้ผู้ใช้บริการทำเครื่องหมาย[17] เช่น

1) ผู้ให้บริการต้องต้องไม่ทำเครื่องหมาย ใด ๆ ในช่องก่อนได้รับความยินยอม หากผู้ใช้บริการไม่คลิกยอมรับนโยบายอย่างอิสระเสรี หรือไม่คลุมเครือ การขอความยินยอมที่ถูกต้องตาม GDPR ผู้ใช้บริการจะต้องตกลงให้ความยินยอมด้วยตนเอง เช่น การเลือกเครื่องหมายถูกในช่อง เพื่อเปิดการใช้งาน ดังนั้น ระบบจึงไม่ควรตั้งค่าเริ่มต้นให้มีเครื่องหมายใด ๆ ให้เลือกในช่องขอความยินยอมไว้ตั้งแต่แรก โดยจะถือว่าการที่ผู้ใช้บริการนิ่งเฉยเป็นการให้ความยินยอมไม่ได้ ดังนั้น จึงไม่เป็นความยินยอมที่ถูกต้องภายใต้กฎของ GDPR

---

[16] GDPR, “General Data Protection Regulation,” accessed July 29, 2020, https://www.privacypolicies.com/blog/gdpr/.

[17] PrivacyPolicies, “Blog Effectively Using an “I Agree to Privacy Policy” Checkbox,” accessed July 29, 2020, https://www.privacypolicies.com/blog/agree-privacy-policy-checkbox/.

2) เมื่อใดก็ตามที่เป็นการลงทะเบียนผู้ใช้บริการใหม่ต้องไม่ดำเนินการยืนยันข้อมูลเพิ่มเติมโดยอัตโนมัติ แม้ว่าจะเป็นแนวทางปฏิบัติที่ทำกันทั่วไปของผู้ให้บริการเพื่อหลีกเลี่ยงรับความยินยอมโดยอัตโนมัติ

3) ผู้ให้บริการต้องไม่ผูกมัดด้วยการทำช่องเครื่องหมายประเภทต่าง ๆ เช่นเดียวกับการยอมรับนโยบาย และได้รับความยินยอมร่วมกันด้วย

หลักเกณฑ์ดังกล่าว ผู้ประกอบธุรกิจควรใช้ช่องแยกสำหรับแต่ละสิ่งที่ต้องการขอความยินยอมและใช้ช่องทำเครื่องหมายยอมรับนโยบายเพื่อต้องการให้ได้รับความยินยอมก่อนตามข้อตกลงของสัญญานั้น ๆ

หลักความยินยอมตามพระราชบัญญัติข้อมูลความเป็นส่วนตัวทางชีวมาตรของสหรัฐอเมริกา (Biometric Information Privacy Act 2008: BIPA) ในการเปิดเผยข้อมูลส่วนบุคคล กฎหมายห้ามมิให้องค์กรต่าง ๆ ที่มีข้อมูลส่วนบุคคลเปิดเผยข้อมูลส่วนบุคคลนั้น เว้นแต่ ได้รับความยินยอมจากเจ้าของข้อมูลก่อน ซึ่งต้องแจ้ง “ล่วงหน้า” ตั้งแต่ครั้งแรกที่เริ่มใช้หลักความยินยอม มิใช่เพียงแค่ “แจ้ง” หากองค์กรผู้ให้บริการไม่แจ้งขอให้ความยินยอมล่วงหน้าเป็นลายลักษณ์อักษรและวัตถุประสงค์เฉพาะสำหรับการเก็บรวบรวม รักษา เปิดเผย ใช้ การลบ หรือการทำลายอย่างถาวรเมื่อไม่ประสงค์แก่เจ้าของข้อมูลทราบก่อน และไม่สามารถรับข้อมูลดังกล่าวได้โดยอัตโนมัติ เมื่อมีการละเมิดก็เพียงพอที่จะนำคดีขึ้นสู่ศาล แม้ว่าเจ้าของข้อมูลส่วนบุคคลจะไม่ได้รับผลกระทบจากการไม่แจ้งเตือนขอให้ความยินยอมดังกล่าวนั้นก็ตาม จึงแสดงให้เห็นว่ากฎหมายของ BIPA ในเรื่องการขอให้ความยินยอมโดยมิได้แจ้งเตือนล่วงหน้าเป็นลายลักษณ์อักษร และต้องตอบรับความยินยอมเป็นลายลักษณ์อักษรที่ให้ความสำคัญตั้งแต่ครั้งแรกเริ่มใช้

หลักการให้ความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ภายใต้มาตรา 19 วรรคสอง[18] โดยบัญญัติความยินยอมดังนี้ “เว้นแต่โดยสภาพไม่อาจขอความยินยอมได้” ซึ่งผู้เขียนเห็นว่าเป็นการให้ความยินยอม “โดยปริยาย”[19]

---

[18] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562.

มาตรา 19 ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้ หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น เว้นแต่บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้

การขอความยินยอมต้องทำโดยชัดแจ้ง เป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เว้นแต่ โดยสภาพไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้

[19] นรินทร์ จุ่มศรี, “มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลจากการใช้บริการเครือข่ายสังคมออนไลน์,” (วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ปรีดี พนมยงค์ มหาวิทยาลัยธุรกิจบัณฑิตย์, 2555), 36.

หากเป็นการบัญญัติการขอให้ความยินยอมโดยปริยายจะเป็นการเปิดช่องกว้างจนเกินไปในการขอให้ความยินยอม[20] เช่นนี้ อาจส่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลโดยตรง

หลักความยินยอม (Consent) ในการปฏิบัติตามสัญญาต้องมิใช่การให้ความยินยอมโดยปริยาย หรือมิใช่การให้ความยินยอมโดยอัตโนมัติ และต้องแจ้งผลกระทบ “ก่อน” ให้ถอนความยินยอมให้เจ้าของข้อมูลทราบตั้งแต่ครั้งแรก

โดยควรพิจารณาเปรียบเทียบตามหลักความยินยอม ดังนี้

1) หลักความเหมาะสมในการเก็บข้อมูล หมายถึง การเก็บรวบรวมข้อมูลต้องแจ้งเตือนในการขอความยินยอมและมีการแจ้งถึงวัตถุประสงค์ในการนำข้อมูลไปใช้จากเจ้าของข้อมูลก่อนเสมอ (หลัก Consent)

2) หลักข้อจำกัดในการนำไปใช้ หมายถึง ข้อมูลส่วนบุคคลจะต้องไม่ถูกนำไปเปิดเผยเกินจากขอบวัตถุประสงค์ที่ได้ขอความยินยอมจากเจ้าของข้อมูล (เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูล หรือตามบทบัญญัติของกฎหมาย)

ดังนั้น หลักความยินยอม (Consent) โดยผู้ให้บริการต้องประกาศแจ้งเตือนเป็นลายลักษณ์อักษรที่เกี่ยวข้องในการขอให้ความยินยอม และต้องแจ้งวัตถุประสงค์ในเรื่องนั้น ๆ โดยไม่จำกัดว่าจะอยู่ในรูปแบบใด ๆ ที่เข้าใจได้ และเข้าถึงได้ง่ายโดยใช้ภาษาที่ชัดเจน

เมื่อเปรียบเทียบกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังมิได้ให้ความสำคัญในเรื่องหลักการแจ้งเตือนขอให้ความยินยอมและต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนและต้องแจ้งถึงวัตถุประสงค์ในการนำข้อมูลไปใช้ให้ผู้เป็นเจ้าของข้อมูลทราบก่อน โดยต้องมิใช่การให้ความยินยอมโดยปริยายเช่นตามนัยมาตรา 19 วรรคสอง

3.3 ระยะเวลาในการเก็บรักษาข้อมูลชีวมาตร (Biometrics)

มาตรการในการเก็บรักษาข้อมูลชีวมาตร ซึ่งถูกบันทึกไว้ในระบบฐานข้อมูลนั้น เช่น ระบบสมาร์ตโฟน อาจถูกคุกคามผ่านระบบการประมวลผลข้อมูลและอาจเชื่อมโยงไปยังฐานข้อมูลได้ ผู้เขียน ตั้งข้อสังเกตว่า การเก็บรักษาข้อมูลส่วนบุคคลมีผลกระทบโดยตรงต่อ**ผลประโยชน์ส่วนตัวของบุคคล** โดยเฉพาะในยุคสังคมข่าวสาร อาจส่งผลกระทบโดยตรงต่อผลประโยชน์ส่วนตัวของบุคคล และไม่คำนึงว่าจะมีการใช้ข้อมูลในครั้งต่อไปจะเกิดขึ้นหรือไม่ก็ตาม ซึ่งข้อมูลส่วนบุคคลที่ถูกรวบรวมบนเครือข่ายอินเทอร์เน็ตสามารถสืบค้นได้ง่าย

---

[20] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ในกรณีที่การถอนความยินยอมส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลในเรื่องใด ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงผลกระทบจากการถอนความยินยอมนั้น

(Searchable) ทำให้การจัดเก็บข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มิได้มีมาตรการแจ้งเตือนเกี่ยวกับระยะเวลาในการเก็บรวบรวมข้อมูลส่วนบุคคลไว้ได้นานเท่าใด

แต่ปรากฏว่าได้บัญญัติระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคลไว้ภายใต้มาตรา 23 (3) โดยบัญญัติไว้ดังนี้ “อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม” การบัญญัติระยะเวลาที่อาจคาดหมายได้ เช่นนี้ เป็นการกำหนดระยะเวลาที่ไม่ชัดเจนแต่อย่างใด ในเรื่องระยะเวลาในการจัดเก็บรักษาข้อมูลส่วนบุคคล อาจทำให้ผู้ให้บริการกำหนดระยะเวลานานเท่าใดก็ได้ตามอำเภอใจ ขณะเดียวกันวิธีการเก็บรักษาในรูปแบบใหม่ ๆ เกิดขึ้นเสมอและสะดวก ซึ่งง่ายต่อการจัดเก็บข้อมูลส่วนบุคคลดังกล่าว อาจเป็นการเอื้อประโยชน์ให้แก่ผู้ให้บริการในการเก็บรวบรวมข้อมูลส่วนบุคคลดังกล่าวตามเจตนารมณ์ของตนได้ ด้วยเหตุนี้ จะกระทำอย่างไรให้ข้อมูลส่วนบุคคลถูกลบเลือนเพื่อมิให้มีข้อมูลค้างอยู่ในระบบ (Digital footprint) ในการป้องกันสิทธิความเป็นส่วนตัวภายใต้กฎหมายฉบับนี้[21] ดังจะได้ศึกษากับกฎมายของ (BIPA) ต่อไปนี้

พระราชบัญญัติคุ้มครองข้อมูลไบโอเมตริกซ์ (Biometric Information Privacy Act 2008: BIPA) กำหนดให้หน่วยงานและองค์กรต่าง ๆ ต้องปฏิบัติตามกฎหมาย โดยห้ามจัดเก็บข้อมูลชีวมาตรในกรณีมีวัตถุประสงค์เพื่อทางการค้า ซึ่งข้อมูลชีวมาตรอยู่ในความครอบครองของตน โดยปราศจากการแจ้งเตือนในการขอให้ความยินยอมก่อนและระยะเวลาในการเก็บรวบรวมข้อมูลชีวมาตรได้บางประเภท เพื่อลดขนาดของฐานข้อมูลในการจัดเก็บข้อมูลส่วนบุคคล ซึ่งตามกฎทั่วไปข้อมูลจะต้องถูกทำลายทันทีที่ไม่จำเป็นสำหรับวัตถุประสงค์อีกต่อไป หรือภายใน 3 ปี นับแต่เริ่มแรกเก็บข้อมูลชีวมาตร ตาม 740 ILCS 14/15[22] จึงจะต้องประกาศแจ้งนโยบายเป็นลายลักษณ์อักษร รวมถึงชี้แจงวัตถุประสงค์ และแจ้งเตือนระยะเวลาให้เจ้าของข้อมูลทราบล่วงหน้าก่อนที่จะทำการรวบรวมในรูปแบบตารางและระบุรายละเอียดว่าจะเก็บข้อมูลอย่างไร

---

[21] อธิพร สิทธิธีรรัตน์, “ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลในบริบทอิเล็กทรอนิกส์,” (วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2558), 24.

[22] 740 ILCS 14/15

Sec. 15. Retention; collection; disclosure; destruction

(a) A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual’s last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.

และเมื่อใดข้อมูลส่วนบุคคลจะถูกทำลายอย่างถาวร หรือตามข้อสัญญาขึ้นอยู่กับว่าระยะเวลาใดจะถึงกำหนดก่อน

แม้ว่าการกำหนดระยะเวลาของกฎหมาย (BIPA) ได้กำหนดให้หน่วยงานและองค์กรต่าง ๆ ในการแจ้งเตือนการขอให้ความยินยอมก่อนและระยะเวลาในการเก็บรวบรวมข้อมูลชีวมาตรได้ภายในเวลา 3 ปี ดังกล่าวนั้น อาจเป็นระยะเวลานานจนเกินไปสำหรับประเทศไทย เมื่อพิจารณาพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 23 (3) มิได้มีมาตรการแจ้งเตือนเกี่ยวกับระยะเวลาในการเก็บรวบรวมข้อมูลส่วนบุคคลไว้ได้นานเท่าใด การบัญญัติระยะเวลาที่อาจคาดหมายได้ อาจทำให้ผู้ให้บริการกำหนดระยะเวลานานเท่าใดก็ได้ตามอำเภอใจ จึงควรกำหนดให้ผู้ให้บริการ หรือผู้ควบคุมข้อมูลมีหน้าที่แจ้งเตือนระยะเวลาการจัดเก็บข้อมูลโดยบัญญัติเรื่องระยะเวลาให้เป็นการแน่นอนเป็นลายลักษณ์อักษรให้เจ้าของข้อมูลส่วนบุคคลทราบก่อน หรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลทราบถึงรายละเอียดและระยะเวลาในการจัดเก็บ ใช้ เปิดเผย ลบ หรือทำลายข้อมูล หรือเมื่อสิ้นสุดตามวัตถุประสงค์ทางธุรกิจ หรือตามข้อตกลงของสัญญา” เว้นแต่วัตถุประสงค์ของกฎหมาย ดังนั้น “ข้อมูลส่วนบุคคลควรเก็บไว้ได้ภายใน 6 เดือน ซึ่งเป็นระยะเวลาไม่มาก หรือน้อยจนเกินไปเมื่อเปรียบเทียบกับกฎหมายของสหรัฐอเมริกาแล้ว

4. การบังคับใช้กฎหมายเพื่อให้เป็นไปตามบทบัญญัติ

มาตรการป้องกันไว้ดีกว่าแก้ (Proactive not reactive; preventative not remedial) ปัจจุบันเทคโนโลยีสามารถพัฒนาแอปพลิเคชันสำหรับสมาร์ตโฟน เพื่อทำธุรกรรมทางการเงินการธนาคารในระบบออนไลน์ หรืออุปกรณ์อิเล็กทรอนิกส์ เพียงแค่นิ้วเดียว เนื่องจากข้อมูลดิจิทัลแพร่หลายสามารถจะเชื่อมโยงกับผลประโยชน์ส่วนตัวเจ้าของข้อมูลได้โดยตรง จึงจำต้องมีการป้องกันความปลอดภัยสิ่งที่จะทำให้เชื่อมโยงถึงข้อมูลส่วนบุคคลนั้นได้

ผู้เขียน จึงนำคดี K Box Entertainment Group เพื่อศึกษาเป็นแนวทางกับกฎหมายประเทศไทย เพื่อผู้ให้บริการต้องดำเนินการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 22 ซึ่งกำหนดให้การจัดเก็บรวบรวมข้อมูลส่วนบุคคลนั้น ไว้ได้เท่าที่จำเป็นตามมาตรา 23 ในการเก็บรวบรวมข้อมูลส่วนบุคคลของผู้ให้บริการ หรือผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งเตือนให้เจ้าของข้อมูลทราบก่อน หรือขณะเก็บข้อมูลถึงวัตถุประสงค์ของการเก็บรวบรวมและต้องมีมาตรการเพียงพอและเหมาะสมกับความเสี่ยงว่าจะถูกละเมิดข้อมูลชีวมาตรได้ เพื่อจำกัดสิทธิผู้ให้บริการได้ตระหนักถึงการจัดการให้องค์กร หรือธุรกิจของตนมีมาตรการที่ถูกต้อง

เหมาะสมเพื่อให้เป็นไปตามบทบัญญัติกฎหมาย เช่น กรณี K Box Entertainment Group[23]

ศาลสั่งปรับค่าเสียหายหน่วยงาน (K Box Entertainment Group) ที่ข้อมูลส่วนตัวของลูกค้ามีการรั่วไหลออกไป โดยถูกสั่งปรับ 50,000 ดอลลาร์สิงคโปร์ เนื่องจากถูกโจมตีในระบบฐานข้อมูล เมื่อปี 2014 และระบบฐานข้อมูลลูกค้ามีการรั่วไหล นอกจากนี้ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ (Personal Data Protection Commission: PDPC) ดำเนินการแจ้งเตือนไปยังหน่วยงานและบริษัทอื่น ๆ อีก 7 แห่ง ให้เพิ่มมาตรการรักษาข้อมูลของลูกค้า เนื่องจาก พบว่า หลายหน่วยงานมีการรักษาความปลอดภัยของข้อมูลที่ยังไม่ดีพอ ด้วยเหตุนี้ จึงทำให้ทราบถึงมาตรการในการแจ้งเตือนเมื่อมีการรั่วไหลของข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานต่าง ๆ เพื่อความปลอดภัยต้องทำการแจ้งทันทีที่ทราบสำหรับข้อมูลของผู้ใช้บริการมีการรั่วไหล อย่างไรก็ตาม PDPC แจ้งให้ภาคธุรกิจปรับการเก็บข้อมูลในแบบอื่น ๆ เช่น การเก็บเลขบัตรประชาชนบางส่วนไว้เท่านั้น หรือการเก็บชื่อผู้ใช้บริการจะถูกเก็บเฉพาะชื่อเท่านั้น ซึ่งถูกกำหนดขึ้นโดยหน่วยงานของ PDPC ดังนั้น จึงมีความจำเป็นที่ภาคธุรกิจของประเทศไทยที่ต้องลดการเก็บข้อมูลส่วนตัวของประชาชน หรือเก็บข้อมูลโดยไม่สมเหตุสมผล โดยเฉพาะข้อมูลชีวมาตร ที่มีความเสี่ยงในปัญหาด้านความเป็นส่วนตัวของข้อมูลส่วนบุคคล

โดยพระราชบัญญัติคุ้มครองข้อมูลไบโอเมตริกซ์ (Biometric Information Privacy Act 2008: BIPA) ของสหรัฐอเมริกาให้ความสำคัญในเรื่องข้อจำกัดเฉพาะข้อมูลชีวมาตรให้ได้รับการลงทะเบียน หรือลดรูปแบบในระบบฐานข้อมูล และต้องแจ้งเกี่ยวกับข้อกำหนดการสแกนลายนิ้วมือ หรือวิธีการใช้ หรือจัดเก็บข้อมูลที่สำคัญ และห้ามเช่าซื้อ ซื้อขายข้อมูลชีวมาตร ซึ่งมีมาตรการในการกำหนดให้ต้องประกาศแจ้งเตือนนโยบายเกี่ยวกับการเก็บรักษาและการเข้าถึงข้อมูลชีวมาตรในรูปแบบของตารางให้เจ้าของข้อมูลทราบ “ล่วง” หน้า และการแจ้งเตือนถึงเหตุละเมิด ตาม 740 ILCS 14/15 แก่เจ้าของข้อมูลส่วนบุคคลทราบและทำลายข้อมูลชีวมาตรเมื่อหมดวัตถุประสงค์อย่างถาวร ภายในเวลา 3 ปี นับตั้งแต่เริ่มเก็บข้อมูลชีวมาตร ซึ่งจะต้องมีมาตรการรักษาความปลอดภัยอย่างเคร่งครัดเป็นพิเศษ โดย BIPA กำหนดโทษปรับการละเมิดความเป็นส่วนตัวทางข้อมูลชีวมาตร หรือข้อมูลไบโอเมตริกซ์ ตามกฎหมายปรับ 1,000 ดอลลาร์ในความเสียหายที่ต้องจ่าย หรือความเสียหายที่เกิดขึ้นจริง สำหรับการละเมิดโดยประมาท ซึ่งโทษปรับสูงสุด 5,000 ดอลลาร์ สำหรับการละเมิดโดยเจตนา หรือโดยประมาท และกฎหมายบัญญัติให้สิทธิของผู้เสียหายสามารถเรียกค่าธรรมเนียมและค่าเยียวยาในการจ้างทนายความ

---

[23] ETDA สพธอ., “ข่าวสั้นกฎหมายคุ้มครองข้อมูลส่วนบุคคล,” สืบค้นเมื่อ 2 กันยายน 2562, https://www.thaicert.or.th/newsbite/2016-04-22-03.html.

ได้ตามความเหมาะสม ซึ่งสิทธินี้มีเฉพาะรัฐอิลลินอยส์เท่านั้น โดยปกติจะต้องได้รับอนุญาตจากศาลก่อน

ดังนั้น หลักสำคัญในการคุ้มครองความปลอดภัยของความเป็นส่วนตัวของข้อมูลชีวมาตร (Biometrics) ซึ่งเป็นข้อมูลส่วนบุคคลที่มีลักษณะลับเฉพาะ หรือมีความอ่อนไหวง่ายเป็นพิเศษ (Sensitive data) นั้น จึงเป็นประเด็นที่สำคัญต้องให้การคุ้มครองอย่างเคร่งครัด โดยห้ามประมวลผลข้อมูล เว้นแต่ได้รับความยินยอมก่อน และเจ้าของข้อมูลสามารถเข้าถึงข้อมูลของตนได้ตลอดเพื่อตรวจการจัดเก็บรวบรวม หรือสามารถปฏิเสธข้อมูลที่ได้ให้ความยินยอมไว้ได้ตลอด ซึ่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ 2562 ยังมิได้มีมาตรการแจ้งเตือนให้ทราบก่อนในการขอให้ความยินยอม และแจ้งเตือนระยะเวลาในการเก็บรวบรวมไว้ได้นานเท่าใดนั้น จึงควรมีมาตรการป้องกันความปลอดภัยในระดับมาตรฐานที่น่าพอใจ ซึ่งในขณะเดียวกันสังคมได้มีการเปลี่ยนแปลงการสื่อสารผ่านทางระบบอิเล็กทรอนิกส์เป็นอย่างมากในปัจจุบัน จึงต้องมีมาตรการทางกฎหมายในระดับที่ได้มาตรฐาน จึงนำไปสู่ข้อเสนอแนะ

5. บทสรุปและข้อเสนอแนะ

5.1 สรุป

จากการศึกษามาตรการทางกฎหมายที่เกี่ยวกับการคุ้มครองข้อมูลชีวมาตรของสหรัฐอเมริกา และปัญหาที่จะนำไปปรับใช้กับข้อมูลชีวมาตร (Biometrics) ได้ให้ความหมายไว้โดยเฉพาะเจาะจง จึงได้รับการคุ้มครองเป็นกรณีพิเศษเฉพาะตามพระราชบัญญัติคุ้มครองข้อมูลไบโอเมตริกซ์ (Biometric Information Privacy Act 2008: BIPA) เมื่อพิจารณาพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ตามมาตรา 6 ได้ให้ความหมาย “ข้อมูลส่วนบุคคล” หมายถึงข้อมูลเกี่ยวข้องกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่มิได้ให้ความหมาย ข้อมูลชีวมาตร (Biometrics) จึงเป็นการให้ความคุ้มครองข้อมูลทั่วไป กล่าวคือข้อมูลชีวมาตรเป็นข้อมูลส่วนบุคคลเกี่ยวกับร่างกายของมนุษย์ที่สามารถเก็บรวบรวมได้ง่ายและเป็นการยากที่เจ้าของข้อมูลชีวมาตรจะระวังตัวได้ เช่น การถ่ายรูป หรือกล้องวงจรปิด หรือลายนิ้วจากเจ้าของจับต้องสิ่งของ และเมื่อมีความนิยมในการนำข้อมูลชีวมาตรมาใช้ในการยืนยันตัวบุคคลทำให้บุคคลที่มีข้อมูลชีวมาตรของผู้อื่นนั้น จึงสามารถที่จะนำมาใช้เพื่อแสดงตนเป็นเจ้าของข้อมูลชีวมาตรได้ จากความหมายดังกล่าวจะเห็นได้ว่าข้อมูลชีวมาตรไม่ได้รวมอยู่ในความหมายของข้อมูลส่วนบุคคลแต่อย่างใด ส่งผลให้การเก็บรวบรวม ใช้ หรือเปิดเผยนั้นไม่ได้รับความคุ้มครองเท่าที่ควร หากผู้เก็บรวบรวมข้อมูลชีวมาตรไม่ทราบประเภทของข้อมูลใด

ที่จะต้องใช้ความระมัดระวังตามที่กฎหมายบัญญัติไว้ อาจส่งผลกระทบต่อเจ้าของข้อมูลชีวมาตร ดังนั้น จึงเป็นสาเหตุที่กล่าวมาแล้วข้างต้นว่า ข้อมูลชีวมาตร (Biometrics) ซึ่งเป็นข้อมูลที่มีความอ่อนไหวง่าย และสามารถถูกละเมิดความเป็นส่วนตัวของเจ้าของข้อมูลได้ตลอด

ผู้เขียนเสนอแนะควรแก้ไขพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยเพิ่มคำนิยามศัพท์ “ข้อมูลชีวมาตร” ไว้ในมาตรา 6 ซึ่งเป็นข้อมูลลับเฉพาะของบุคคล (Sensitive data) และมาตรการแจ้งเตือนในการขอให้ความยินยอมก่อน และแจ้งเตือนระยะเวลาการเก็บรวบรวม ใช้ เปิดเผย ลบ หรือทำลาย หรือสิทธิที่จะถูกลืม (Right to be forgotten) ควรบัญญัติระยะเวลาให้เป็นการที่แน่นอนว่าเก็บได้นานเท่าใด โดยข้อมูลส่วนบุคคลควรเก็บไว้ได้ภายใน 6 เดือน ในมาตรา 23 (3) และแจ้งเตือนการเข้าถึงข้อมูลได้ตลอดระยะเวลาในขณะการเก็บรวบรวม หรือการประมวลผลยังคงดำเนินต่อไปให้เจ้าของข้อมูลทราบ เพื่อให้ผู้ประกอบธุรกิจตระหนักในการแจ้งเตือนการขอให้ความยินยอม เพื่อป้องกันการละเมิดข้อมูลส่วนบุคคลในภาคธุรกิจดิจิทัล

ดังนั้น กฎหมาย BIPA ของสหรัฐอเมริกา จึงให้ความสำคัญกับผลกระทบด้านสิทธิในความเป็นส่วนตัว (The right to privacy) ที่เจ้าของข้อมูลสามารถเข้าถึงข้อมูลส่วนบุคคลของตนได้ หากข้อมูลนั้นผิดพลาด หรือบกพร่องสามารถทำการแก้ไขข้อมูลนั้นได้ตาม 740 ILCS 14/25 และความปลอดภัยของข้อมูลส่วนบุคคล ซึ่งข้อมูลส่วนบุคคลที่เกิดจากการประมวลผลทางเทคนิค หรือการยืนยันอัตลักษณ์ของบุคคลนั้น ๆ หรือสามารถเชื่อมโยงไปยังบุคคลได้ ซึ่งหากพิจารณาจากความสอดคล้องกับกฎหมายของ GDPR แล้ว โดยหลักการต้องแจ้งเตือนการขอความยินยอม และแจ้งเตือนผลกระทบก่อนถอนการให้ความยินยอม โดยห้ามผู้ให้บริการระบบออนไลน์ใช้ความยินยอมโดยวิธีอัตโนมัติ ซึ่งจะต้องประกาศแจ้งหลักเกณฑ์และนโยบายในรูปแบบตารางเป็นลายลักษณ์อักษรอย่างชัดเจน ในการขอความยินยอมให้เจ้าของข้อมูลทราบก่อน รวมทั้งมาตรการในการทำลายข้อมูลชีวมาตร (Biometrics) หรือสิทธิที่จะขอลบข้อมูล (Right to erasure) หรือสิทธิที่จะถูกลืม (Right to be forgotten) เมื่อสิ้นสุดวัตถุประสงค์ทางธุรกิจทันที ผู้ให้บริการต้องคำนึงถึงมาตรการความเป็นส่วนตัวของข้อมูลชีวมาตรให้เป็นไปตามบทบัญญัติของกฎหมายและรับรองความโปร่งใส

5.2 ข้อเสนอแนะ

จากการศึกษาวิเคราะห์พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ 2562 ผู้เขียนพบว่า มิได้บัญญัติคำนิยามของ “ข้อมูลชีวมาตร” ไว้ในมาตรา 6 แต่อย่างใด เนื่องจากข้อมูลชีวิมาตรนั้นเป็นข้อมูลลับเฉพาะของบุคคลโดยแท้ จึงจำเป็นต้องบัญญัติคำนิยามเพื่อให้ประชาชนเข้าใจความหมายของข้อมูลชีวมาตรตรงกัน และจำแนกประเภทของข้อมูลแต่ละ

ประเภท เพื่อให้ได้รับความคุ้มครองกรณีพิเศษออกจากข้อมูลส่วนบุคคลทั่วไป เนื่องจากข้อมูลชีวมาตรนั้นห้ามประมวลผล เว้นแต่ จะได้รับความยินยอมจากเจ้าของข้อมูลก่อนเพื่อประโยชน์ของบุคคลนั้น หรือเว้นแต่วัตถุประสงค์ของกฎหมายบัญญัติไว้ รวมทั้งยังไม่มีมาตรการในการแจ้งเตือนถึงสิทธิต่าง ๆ ก่อนที่จะดำเนินการใด ๆ ให้เจ้าของข้อมูลทราบก่อนไว้แต่อย่างใด เช่น สิทธิที่จะได้รับการแจ้งการเก็บข้อมูล สิทธิที่จะได้รับแจ้งการเข้าถึง สิทธิในการแก้ไข สิทธิในการจำกัดการประมวลผลข้อมูล สิทธิในการถ่ายโอนข้อมูล สิทธิในการปฏิเสธไม่ให้ใช้ข้อมูล สิทธิที่จะไม่ใช้การตัดสินใจด้วยวิธีการอัตโนมัติในการประมวลผล สิทธิในการลบ อันเป็นสิทธิที่ควรคำนึงถึงลำดับต้น ๆ เมื่อเปรียบเทียบกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มิได้มีมาตรการในการแจ้งเตือนระยะเวลาในการเก็บรวบรวมข้อมูลนานเท่าใด รวมทั้งมาตรการในการป้องกันการตอบแบบอัตโนมัติ ซึ่งเจ้าของข้อมูลนั้นควรเข้าถึงข้อมูลได้ในระยะเวลาเท่าใด และสามารถจำกัดขอบเขตการให้ใช้ หรือปฏิเสธการให้ใช้ข้อมูลของตนได้ โดยต้องคำนึงถึงแนวทางในการปฏิบัติให้สอดคล้องกับกฎหมาย GDPR ของสหภาพยุโรป ซึ่งประเทศไทยไม่สามารถหลีกเลี่ยงที่จะต้องติดต่อรับส่งข้อมูลกับสหภาพยุโรปได้ ด้วยเหตุนี้ จึงต้องมีการปรับปรุงแก้ไขกฎหมายในการบังคับใช้กฎหมายเพื่อป้องกันการถูกละเมิดความเป็นส่วนตัวในข้อมูลชีวมาตร

อย่างไรก็ตาม ผู้เขียนขอเสนอแนะแก้ไขเพิ่มเติมบทบัญญัติของกฎหมายในเรื่องการ คำนิยามของ “ข้อมูลชีวมาตร (Biometrics)” การแจ้งเตือนสิทธิในการขอความยินยอมและผลกระทบในการถอนความยินยอม การเข้าถึงข้อมูลส่วนบุคคลของตนได้เพื่อแก้ไขข้อมูลที่ผิดพลาด หรือบกพร่อง ซึ่งยังมิได้มีการบัญญัติไว้ และการกำหนดระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคลได้นานเท่าใด ซึ่งมาตรการดังกล่าว จะต้องแจ้งเตือนสิทธิให้แก่เจ้าของข้อมูลทราบก่อน ดังนี้

1) เพิ่มคำนิยามศัพท์ “ข้อมูลชีวมาตร หรือข้อมูลไบโอเมตริกซ์ (Biometrics)” เพื่อให้เข้าใจความหมายตรงกัน และจำแนกประเภทของข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนไว้อย่างชัดเจนใน มาตรา 6

2) การแจ้งเตือนสิทธิในการขอให้ความยินยอมก่อน ซึ่งมิใช่ความยินยอมโดยปริยาย หรือความยินยอมโดยอัตโนมัติ และต้องแจ้งผลกระทบ ให้เพิ่ม “ก่อน” ถอนความยินยอมใน มาตรา 19 วรรคหก

3) การแจ้งเตือนสิทธิการเข้าถึงข้อมูลส่วนบุคคลได้ตลอดในขณะที่ถูกเก็บรวบรวม หรือประมวลผลข้อมูลยังดำเนินต่อไปไว้ใน มาตรา 30

4) การแจ้งเตือนสิทธิในเรื่องระยะเวลาในการเก็บรวบรวมข้อมูลส่วนบุคคล และกำหนด

ระยะเวลาให้เป็นการที่แน่นอนไว้ได้ภายใน 6 เดือน ในมาตรา 23 (3)

5) เพิ่มบทบัญญัติสิทธิในการแก้ไข (Rights to be rectification) เพื่อให้สิทธิผู้ควบคุมข้อมูลส่วนบุคคลสามารถแก้ไขข้อมูลส่วนบุคคลที่ผิดพลาดได้ตาม มาตรา 29 (2)

ดังนั้น เมื่อพิจารณา พบว่า การคุ้มครองความเป็นส่วนตัวของพระราชบัญญัติคุ้มครองข้อมูลชีวมาตร (Biometric Information Privacy Act 2008: BIPA) ของสหรัฐอเมริกา ได้ให้การคุ้มครองข้อมูลชีวมาตร หรือประเภทข้อมูลที่มีความละเอียดอ่อน โดยจำแนกประเภทข้อมูลแต่ละประเภทได้อย่างชัดเจน “ห้ามเก็บรวบรวมข้อมูลที่มีความอ่อนไหว” (Sensitive data) เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูลก่อน หรือตามวัตถุประสงค์ของกฎหมาย อันเป็นแนวทางที่สากลประเทศปฏิบัตินั้น ซึ่งปัญหาที่เกี่ยวข้องกับการละเมิดความเป็นส่วนตัวของข้อมูลชีวมาตรถือว่าเป็นภัยที่ใกล้ตัวที่สำคัญของผู้บริโภค โดยต้องตระหนักและให้ความสำคัญเป็นอย่างมาก

เนื่องจากข้อมูลชีวมาตรจะไม่สามารถเปลี่ยนแปลงข้อมูลใด ๆ ได้เช่นเดียวกันกับรหัสผ่าน (Password) ในการเข้าระบบแอปพลิเคชันเพื่อใช้บริการต่าง ๆ หากมีการละเมิดจะส่งผลกระทบร้ายแรงต่อชีวิตส่วนบุคคลผู้ที่เป็นเจ้าของข้อมูลชีวมาตร ด้วยเหตุนี้ ควรมีการประเมินผลกระทบด้านการปกป้องข้อมูลชีวมาตร หากข้อมูลดังกล่าวมีความเสี่ยงสูงต่อสิทธิและเสรีภาพขั้นพื้นฐานของบุคคลตามกฎหมาย โดยมิได้พิจารณาถึง “เหตุผลและความจำเป็น” อย่างรอบคอบต่อผลกระทบที่อาจเกิดขึ้นกับเจ้าของข้อมูลชีวมาตร ในกรณีที่ “ข้อมูลรั่วไหลและถูกนำไปใช้โดยมิชอบ” ซึ่งเป็นสาระสำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จึงจำเป็นต้องตรากฎหมายให้สอดคล้องกับกฎหมายยุคดิจิทัล โดยประเทศไทยมิอาจหลีกเลี่ยงในการติดต่อสื่อสารรับส่งข้อมูลส่วนบุคคลของผู้ใช้บริการซึ่งมีอยู่ทั่วโลกได้

Reference

A Group of Academics Submitting the Prime Minister 's Letter, The State Concerned about Collecting Biometrics Data was not Transparent, Lacking of Good Governance. 20

Akarin Suthanuwong. "The Fingerprint Authentication System Embedded." Master's thesis, Faculty of Engineering, Prince of Songkla University, 2005. [in Thai].

Apichai Plaengsorn. *Lecture Document (Identification).* Bangkok: Department of Forensic Science, Faculty of Medicine, Srinakharinwirot University, 2016. [in Thai].

Athiporn Sitthitheerarat. "Issues of Personal Data Protection Laws in the Electronic Context." Master's thesis, Faculty of Law, Thammasat University, 2015. [in Thai].

Atthakorn Sukpunaphan. "Right to be Forgotten: From a Ruling to a New Dimension Under the EU Data Protection Law." *Balance Health* 64, no.3 (2017): 46. [in Thai].

ETDA PAD. "Short News, Personal Information Protection Law." Accessed September 29, 2020. https://www.thaicert.or.th/newsbite/2016-04-22-03.html.

GDPR. "General Data Protection Regulation." Accessed July 29, 2020, https://www.privacypolicies.com/blog/gdpr/.

Illinois Official Reports Supreme Court. "Rosenbach v. Six Flags Entertainment Corp., 2019 IL 123186." Accessed July 29, 2020, https://courts.illinois.gov/Opinions/SupremeCourt/2019/123186.pdf.

Litigation Under Illinois Biometric Information Privacy Act Highlights Biometric Data Risks. 24,2019.

Mantana Sripongphan. "Legal Issues Regarding the Protection of Personal Data: Study a Specific Case of the User's Location Information." Master's thesis, Faculty of Law, Sripatum University, 2018. [in Thai].

Naiyana Masaeng. “Biometric Technology.” *Academic Journal Thonburi University* 2, no.1 (2008): 3-6. [in Thai].

Privacy Policies. “Blog Effectively Using an “I Agree to Privacy Policy” Checkbox.” Accessed July 29, 2020. https://www.privacypolicies.com/blog/agree-privacy-policy-checkbox/.

Sirikul Phuphan. “The Message is Thought with Personal Information.” Master’s thesis, Faculty of Law, Thammasat University, 2005 [in Thai].

Zimmerman, Hannah. “The Data of You: Regulating Private Industry’s Collection of Biometric Information.” *Kansas Law Reviews* 66 (2018): 637-671.