ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลประเภทข้อมูลชีวภาพ*

แสงระวี วิปุลาคม**
สราวุธ ปิติยาศักดิ์***

Received: April 15,2021
Revised: September 26,2021
Accepted: September 28,2021

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อ (1) ศึกษาแนวคิดเกี่ยวกับข้อมูลส่วนบุคคล ข้อมูลชีวภาพ และลักษณะทั่วไปของเทคโนโลยีเกี่ยวกับการใช้ข้อมูลชีวภาพ (2) ศึกษามุมมองที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลสำหรับข้อมูลชีวภาพตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักร (DPA) และกฎหมายคุ้มครองข้อมูลชีวภาพของรัฐอิลลินอยส์ ประเทศสหรัฐอเมริกา (BIPA) และ (3) วิเคราะห์พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เปรียบเทียบกับส่วนที่เกี่ยวข้องกับข้อมูลชีวภาพตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักร (DPA) และกฎหมายคุ้มครองข้อมูลชีวภาพของรัฐอิลลินอยส์ ประเทศสหรัฐอเมริกา (BIPA) ผลการศึกษาพบว่า (1) โดยรวมกฎหมายคุ้มครองข้อมูลชีวภาพของไทยสอดคล้องกับแนวคิดเกี่ยวกับข้อมูลส่วนบุคคล และแนวคิดเกี่ยวกับข้อมูลชีวภาพในการให้ความคุ้มครองเจ้าของข้อมูลส่วนบุคคล หากแต่สามารถปรับปรุงเพื่อให้มีความคุ้มครองข้อมูลชีวภาพที่เหมาะสมมากขึ้นได้ (2) กฎหมายคุ้มครองข้อมูลส่วนบุคคล GDPR ของสหภาพยุโรป และ BPA ของสหราชอาณาจักรนั้นสอดคล้องกันและให้ความคุ้มครองข้อมูลชีวภาพในลักษณะเดียวกัน ทางด้านกฎหมายคุ้มครองข้อมูลชีวภาพ BIPA ของรัฐอิลลินอยส์ให้ความคุ้มครองข้อมูลชีวภาพโดยเฉพาะ อีกทั้งยังมีการให้คำจำกัดความที่ชัดเจน หากแต่มิได้มีการกำหนดแนวทางในการรักษาความปลอดภัยไว้ สำหรับรัฐอิลลินอยส์และสหราชอาณาจักรนั้น ศาลได้มีคำพิพากษาให้การฟ้องคดีสามารถกระทำได้โดยมิต้องเกิดความเสียหายอันสามารถกำหนดมูลค่าได้ (3) กฎหมายคุ้มครองข้อมูลชีวภาพของไทยสอดคล้องกับกฎหมายคุ้มครองข้อมูลชีวภาพ

---

* ส่วนหนึ่งของวิทยานิพนธ์ ปริญญานิติศาสตรมหาบัณฑิต มหาวิทยาลัยสุโขทัยธรรมาธิราช

** น.บ. (นิติศาสตรบัณฑิต), Bachelor of Applied Science (Computing), Master of Science (Computer Science), Master of Business Administration (Finance), Sasin Graduate Institute of Business Administration

*** น.บ. (นิติศาสตรบัณฑิต) (เกียรตินิยมอันดับหนึ่ง), บธ.บ. (บริหารธุรกิจบัณฑิต), LL.M. (Master of Law), SJD. (Doctor of Legal Science), University of Hong Kong, Hong Kong SAR, China. ศาสตราจารย์ประจำสาขาวิชานิติศาสตร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช

ของสหภาพยุโรปและของสหราชอาณาจักร หากแต่มิได้มีการกำหนดแนวทางในการรักษาความปลอดภัยอย่างพอเพียงเพื่อคุ้มครองข้อมูลชีวภาพ และไม่มีการประเมินผลกระทบและความจำเป็นในการเก็บข้อมูลก่อนการประมวลผลข้อมูลชีวภาพ การวิจัยนี้จึงเสนอแนวทางในการปรับปรุงกฎหมายคุ้มครองข้อมูลชีวภาพของไทย โดยควรมีการปรับเปลี่ยนคำจำกัดความของคำว่า “ข้อมูลชีวภาพ” ให้มีความเหมาะสม อีกทั้งปรับเปลี่ยนการรักษาความปลอดภัยสำหรับข้อมูลชีวภาพให้มีการคุ้มครองข้อมูลชีวภาพโดยยึดหลักมาตรฐานสากลในการรักษาความปลอดภัย และมีการประเมินผลกระทบและความจำเป็นในการเก็บข้อมูลก่อนการประมวลผลข้อมูลชีวภาพ สำหรับการร้องเรียนการละเมิดข้อมูลชีวภาพเจ้าของข้อมูลส่วนบุคคลไม่จำเป็นต้องได้รับความเสียหายหรือความเดือดร้อนอันสามารถกำหนดมูลค่าได้จึงจะสามารถร้องเรียนได้ การลงโทษสำหรับการละเมิดข้อมูลส่วนบุคคลประเภทชีวภาพควรกำหนดอัตราโทษทางปกครองโดยกำหนดจำนวนค่าปรับต่อผู้เสียหายหนึ่งราย เพื่อเป็นการป้องปรามให้ผู้ควบคุมข้อมูลส่วนบุคคลกำหนดให้มีมาตรการการรักษาความปลอดภัยข้อมูลชีวภาพที่เหมาะสม

คำสำคัญ การคุ้มครองข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลชีวภาพ ฐานการประมวลผล การรักษาความปลอดภัยข้อมูลชีวภาพ

****ผู้รับผิดชอบบทความ**: นางสาวแสงระวี วิปุลาคม นักศึกษาระดับปริญญาโท หลักสูตรนิติศาสตรมหาบัณฑิต มหาวิทยาลัยสุโขทัยธรรมาธิราช Email : sangrave@yahoo.com

Legal Problems Regarding Personal Data Protection for Biometrics*

Sangravee Vipulakom**
Dr. Saravuth Pitiyasak***

Abstract

The objectives of this thesis are to (1) study concepts relating to personal data, biometrics data, and general characteristics of biometric technology; (2) study perspectives in relations to data privacy laws on biometrics from EU's Data Protection Regulation (GDPR), UK's Data Protection Act, Illinois Biometrics Information Protection Act and (3) analyze Thailand's Personal Data Protection Act 2019 and make comparisons with EU's Data Protection Regulation (GDPR), UK's Data Protection Act (DPA), and Illinois Biometrics Information Protection Act (BIPA). The results of the study are (1) overall Thai Personal Data Protection Act is in line with the concepts of personal data and biometrics data in terms of providing protection for data subjects. However, the act can be improved to provide more suitable protections ; (2) European Union's GDPR and United Kingdom's DPA are in line and provide the same level of protection for biometrics data, while Illinois's BIPA provide protection exclusively for biometrics data with clear definition but did not provide guidance for biometrics data security. Furthermore, courts in Illinois and United Kingdom have adjudicated that lawsuit can be filed even without actual and/or financial damages; (3) While PDPA's protection for biometrics data are in line with GDPR and DPA, the guideline for biometrics data protection has not been determined. Also, it does not require impact assessment and the justifications prior to the use of biometrics data. This study proposes improvement of Personal Data Protection law by adjusting the definition of the word "Biometrics" accordingly. Furthermore, the security of biometrics should be based on international standard, and impact assessment and the justifications for using biometrics should always be done prior to the decision to use biometrics technology. Data subjects

* Part of the thesis for Master of Laws,Degree Sukhothai Thammathirat Open University

** Bachelor of Applied Science (Computing), Master of Science (Computer Science), Master of Business Administration (Finance), Sasin Graduate Institute of Business Administration

*** SJD. (Doctor of Legal Science), University of Hong Kong, Hong Kong SAR, China. Professor, School of Laws, Sukhothai Thammathirat Open University

should be able to file complaints or lawsuits on biometrics violations without having to proof actual or financial damages. Penalties for violations relating to biometrics under Personal Data Protection Act 2019 should be set per data subject instead of per violation. This will be a deterrence to data controller and encourage them to put in place proper security measures.

Keywords: Personal Data Protection, Biometrics Data, Lawful Basis, Biometrics Security

****Corresponding Author:** Miss Sangravee Vipulakom. Master of Laws Degree, Sukhothai Thammathirat Open University. Email : sangrave@yahoo.com

1. บทนำ

ความก้าวหน้าทางเทคโนโลยีในยุคดิจิทัลทำให้มีการนำข้อมูลอัตลักษณ์บุคคล หรือข้อมูลชีวภาพ (biometrics) มาใช้ในการยืนยันตัวตน (authentication/verification) และการระบุตัวตน (identification) อย่างแพร่หลาย ทำให้หลายประเทศเริ่มตระหนักถึงความเสียหายที่อาจเกิดขึ้นได้จากการรั่วไหลของข้อมูลชีวภาพ และความเสี่ยงของการนำข้อมูลชีวภาพไปใช้ในทางมิชอบ ในปี พ.ศ. 2551 รัฐอิลลินอยส์ เป็นรัฐแรกของสหรัฐอเมริกาที่ประกาศใช้กฎหมายที่ให้ความคุ้มครองข้อมูลส่วนบุคคลประเภทชีวภาพโดยเฉพาะ คือ Biometric Information Privacy Act (BIPA) ในขณะที่ General Data Protection Regulation (GDPR) ของสหภาพยุโรปนั้นได้ให้ความสำคัญกับข้อมูลชีวภาพเป็นพิเศษ โดยจัดข้อมูลชีวภาพเป็นข้อมูลส่วนบุคคลพิเศษ (special categories of personal data) ซึ่งต้องมีการควบคุมการประมวลผลในระดับที่สูง อนึ่ง แม้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของประเทศไทยได้มีการกำหนดให้ข้อมูลชีวภาพเป็นข้อมูลที่มีความอ่อนไหวสูง หากแต่มิได้กำหนดมาตรการ แนวทาง หลักเกณฑ์ หรือข้อปฏิบัติในการคุ้มครองข้อมูลชีวภาพที่ต่างไปจากข้อมูลส่วนบุคคลอื่น ๆ และขณะนี้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลอยู่ในขั้นตอนของการร่างกฎหมายลำดับรอง จึงเป็นที่น่ากังวลว่าข้อมูลชีวภาพจะได้รับการคุ้มครองอย่างเหมาะสมหรือมีการกำหนดวิธีการรักษาความปลอดภัยที่ดีพอหรือไม่

การรั่วไหลของข้อมูลชีวภาพสามารถก่อให้เกิดความเสียหายอันไม่อาจระงับหรือแก้ไขได้ ดังนั้น กฎเกณฑ์ในการเก็บรวบรวม ใช้ และเปิดเผยจึงควรเข้มงวดกว่าข้อมูลส่วนบุคคลประเภทอื่น ควรมีการจำกัดให้เก็บรวบรวมข้อมูลชีวภาพได้เท่าที่จำเป็น และต้องมีการศึกษาผลกระทบของการเก็บรวบรวมข้อมูลชีวภาพเสียก่อน รวมทั้งในขั้นตอนการขอความยินยอมควรมีการแจ้งให้ทราบถึงผลกระทบของการเก็บข้อมูลชีวภาพ นอกจากนี้กระบวนการในการร้องเรียนหรือฟ้องร้องการละเมิดข้อมูลชีวภาพนั้นควรมีความแตกต่างจากกระบวนการร้องเรียนสำหรับข้อมูลส่วนบุคคลอื่น ๆ โดยไม่ควรรอให้เกิดความเสียหายก่อนจึงจะอนุญาตให้ทำการร้องเรียนหรือฟ้องร้องตามกฎหมายได้ และอาจต้องพิจารณาความเหมาะสมของบทลงโทษสำหรับกรณีการกระทำผิดที่เกี่ยวกับข้อมูลชีวภาพให้มีความเหมาะสมอีกด้วย จึงควรศึกษาและพัฒนากฎหมายคุ้มครองข้อมูลส่วนบุคคลประเภทชีวภาพของไทยเพื่อให้เจ้าของข้อมูลส่วนบุคคลได้รับการคุ้มครองอย่างเหมาะสม

2. วัตถุประสงค์

1. เพื่อศึกษาแนวความคิดเกี่ยวกับข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลชีวภาพ และลักษณะทั่วไปของเทคโนโลยีเกี่ยวกับการใช้ข้อมูลชีวภาพ

2. เพื่อเปรียบเทียบกฎหมายคุ้มครองข้อมูลส่วนบุคคลสำหรับข้อมูลประเภทชีวภาพตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักร (DPA) และกฎหมายคุ้มครองข้อมูลชีวภาพของรัฐอิลลินอยส์ ประเทศสหรัฐอเมริกา (BIPA)

3. เพื่อศึกษาปัญหาเกี่ยวกับกฎหมายการคุ้มครองข้อมูลส่วนบุคคลประเภทชีวภาพในประเทศไทย

3. วิธีดำเนินการวิจัย

การดำเนินการวิจัยในครั้งนี้ใช้วิธีการศึกษาข้อมูลเอกสาร ได้แก่ ตัวบทกฎหมาย คำพิพากษา หนังสือ บทความ วิทยานิพนธ์ วิจัย และสื่ออิเล็กทรอนิกส์อื่น ๆ ที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งข้อมูลส่วนบุคคลชีวภาพ ทั้งภาษาไทย และภาษาต่างประเทศ

4. ขอบเขตของการวิจัย

การศึกษาวิจัยครั้งนี้ ผู้วิจัยมุ่งเน้นถึงปัญหาตามบทบัญญัติใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยทำการศึกษาเฉพาะการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลประเภทชีวภาพของภาคเอกชนเท่านั้น ทั้งนี้ผู้วิจัยจะดำเนินการศึกษาจาก พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เปรียบเทียบกับกฎหมาย General Data Protection Regulation (GDPR) ของสหภาพยุโรป และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักร (DPA) และกฎหมายคุ้มครองข้อมูลส่วนบุคคลชีวภาพของรัฐอิลลินอยส์ ประเทศสหรัฐอเมริกา (BIPA)

5. ผลการวิจัย

5.1 แนวคิดและทฤษฎีที่เกี่ยวข้องกับข้อมูลส่วนบุคคลและข้อมูลชีวภาพ

จากการศึกษาข้อมูลจากเอกสารพบว่าเดิมทีสิทธิส่วนบุคคลแบ่งออกได้เป็น 4 ประเภท คือ 1) ความเป็นส่วนตัวของบุคคล (Privacy of the person) 2) ความเป็นส่วนตัวของพฤติกรรมของบุคคล (Privacy of personal behavior) 3) ความเป็นส่วนตัวของข้อมูลส่วนบุคคล (Privacy of personal data) และ 4) ความเป็นส่วนตัวของการสื่อสารของบุคคล (Privacy of personal communication) (Clarke, 1997) ซึ่งต่อมาการพัฒนาอย่างก้าวกระโดดของเทคโนโลยีทำให้มีการปรับเปลี่ยนสิทธิส่วนบุคคลออกเป็น 7 ประเภท คือ 1) ความเป็นส่วนตัวของบุคคล (Privacy of the person) 2) ความเป็นส่วนตัวด้านพฤติกรรมและการกระทำ (Privacy of behavior and action 3) ความเป็นส่วนตัวด้านการสื่อสาร (Privacy of communication) 4) ความเป็นส่วนตัวด้านข้อมูลและรูปถ่าย (Privacy of data and image) 5) ความเป็นส่วนตัวด้านความคิดและความรู้สึก (Privacy of thoughts and feelings) 6) ความเป็นส่วนตัวด้านที่ตั้งและพื้นที่ (Privacy of location and space) และ 7) ความเป็นส่วนตัวด้านการสมาคม (Privacy of association) (Friedewald, Finn, & Wright, 2013) เนื่องจากเทคโนโลยีได้พัฒนาจนเข้ามาเป็นส่วนหนึ่งของชีวิตมากขึ้น เทคโนโลยีมีความสามารถในการนำรูปถ่าย ความคิดและความรู้สึก รวมถึงตำแหน่งที่ตั้งและพื้นที่ส่วนตัวไปใช้ได้อย่างง่ายดาย นอกจากนี้เทคโนโลยีสามารถบันทึกข้อมูลส่วนบุคคลทุกอย่างไว้ได้ ไม่ว่าจะเป็นปุ่มทุกปุ่มที่กด เว็บทุกเว็บที่เข้าดู การเคลื่อนหรือคลิกเม้าส์ไปยังตำแหน่งต่าง ๆ อาจมีการบันทึกได้เสมอโดยที่ไม่รู้ตัว

ดังนั้น องค์การเพื่อความร่วมมือและการพัฒนาทางเศรษฐกิจ (The Organization for Economic Cooperation and Development หรือ OECD) จึงได้กำหนดกรอบในการคุ้มครองข้อมูลส่วนบุคคลที่เรียกว่า “ข้อแนะนำเกี่ยวกับแนวทางการคุ้มครองความเป็นส่วนตัวและการส่งผ่านข้อมูลส่วนบุคคลระหว่างประเทศ (Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data)” ซึ่งกำหนดหลักเกณฑ์

ไว้ว่า การเก็บข้อมูลส่วนบุคคลนั้นจะต้องเก็บเท่าที่จำเป็น อย่างถูกต้องด้วยกฎหมาย และต้องได้รับความยินยอมจากเจ้าของข้อมูล ข้อมูลที่ทำการเก็บต้องเกี่ยวข้องกับวัตถุประสงค์ในการเก็บข้อมูล และต้องมีความถูกต้องและเป็นปัจจุบัน โดยจะต้องมีการระบุวัตถุประสงค์อย่างชัดเจนและใช้ภายในวัตถุประสงค์ที่ได้ระบุไว้เท่านั้น รวมทั้งยังต้องมีการดูแลรักษาความปลอดภัยอย่างเหมาะสม นอกจากนี้ผู้รวบรวมข้อมูลส่วนบุคคลยังต้องมีนโยบายการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่มีความโปร่งใสโดยให้เจ้าของข้อมูลมีส่วนร่วมในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลด้วย โดยเอกสารฉบับนี้ได้รับการยอมรับโดยทั่วไปว่าเป็นหลักเกณฑ์พื้นฐานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่สำคัญ และหลายประเทศได้นำไปบัญญัติเป็นกฎหมายภายในของตน (สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์, 2558) ทั้งนี้ประเทศไทยได้นำหลักการสำคัญ 8 ประการตามแนวทางดังกล่าวมาบัญญัติไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลอีกด้วย (สราวุธ ปิติยาศักดิ์, 2561)

ข้อมูลชีวภาพนั้นอาจเป็นข้อมูลลักษณะทางสรีระหรือลักษณะทางพฤติกรรมก็ได้ (Smith, Mann, & Urbas, 2018) แต่ต้องเป็นข้อมูลที่มีความเป็นเอกลักษณ์ เป็นสากล และเป็นถาวรจึงจะสามารถนำมาใช้ในการยืนยันตัวตนได้ นอกจากนี้ยังควรมีความง่ายในการเก็บตัวอย่าง เป็นที่ยอมรับว่าสามารถนำไปใช้เพื่อยืนยันตัวตนหรือระบุตัวตนได้ โดยปลอมหรือหลอกระบบได้ยาก อีกทั้งยังต้องมีความแม่นยำในการนำไปใช้อีกด้วย (Coseraru, 2017) (Kindt, 2013)

ขั้นตอนในการทำงานของระบบยืนยันตัวตนชีวภาพ เริ่มจากการลงทะเบียนโดยเก็บข้อมูลของเจ้าของข้อมูลส่วนบุคคลเข้าระบบ เช่น การถ่ายรูป การสแกนลายนิ้วมือ เป็นต้น จากนั้น ระบบจะนำข้อมูลที่ได้ไปทำให้ปรกติ คือกำจัดข้อมูลไม่พึงประสงค์ออก แล้วจึงนำไปสกัดคุณลักษณะ และสร้างแม่แบบไว้ในระบบ เมื่อเจ้าของข้อมูลส่วนบุคคลต้องการยืนยันตัวตน เช่น ต้องการเข้าถึงข้อมูลในบัญชีเงินฝากของตนเอง ระบบจะเก็บข้อมูลชีวภาพจากเจ้าของข้อมูลส่วนบุคคลอีกครั้ง กำจัดข้อมูลไม่พึงประสงค์ออก นำไปสกัดคุณลักษณะและนำไปเทียบกับแม่แบบที่ได้สร้างไว้ในขั้นตอนลงทะเบียน และหากเป็นขั้นตอนการระบุตัวตน ระบบจะนำข้อมูลที่เก็บจากเจ้าของข้อมูลส่วนบุคคลที่ได้กำจัดข้อมูลไม่พึงประสงค์ออกและสกัดคุณลักษณะแล้วไปเปรียบเทียบกับข้อมูลทั้งหมดที่ระบบเก็บไว้ในฐานข้อมูล (Kindt, 2013)

อนึ่ง หลักการคุ้มครองข้อมูลชีวภาพที่เหมาะสมควรประกอบด้วย 1) ความยินยอมของเจ้าของข้อมูล 2) เจ้าของข้อมูลได้รับการแจ้งข้อมูลที่ชัดเจนและโปร่งใสจากผู้ควบคุมข้อมูลส่วนบุคคล รวมถึงรายละเอียดต่าง ๆ ที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล 3) มีการเก็บข้อมูลเท่าที่จำเป็น ใช้ภายใต้วัตถุประสงค์ที่กำหนด 4) ข้อมูลต้องมีความถูกต้อง และเป็นปัจจุบันเสมอ 5) มีการกำหนดจำนวนและขอบเขตของการใช้งานข้อมูล โดยใช้เฉพาะที่จำเป็น มีวัตถุประสงค์ที่ชัดเจนและถูกต้องตามกฎหมาย 6) ใช้หลักการไม่เปิดเผยตัวตน เพื่อลดปัญหาการละเมิดความเป็นส่วนตัว (Toli, 2018)

การนำข้อมูลชีวภาพมาใช้นั้นมีความเสี่ยง ทั้งความเสี่ยงที่เกิดจากธรรมชาติของข้อมูลชีวภาพเอง และความเสี่ยงที่เกิดจากความผิดพลาดของระบบข้อมูลชีวภาพ ซึ่งอาจเกิดจากวิธีการทำงานของระบบหรือเกิดจากการโจมตีจากภายนอก การนำข้อมูลชีวภาพมาใช้มากขึ้นทำให้เกิดความเสี่ยงมากขึ้นตามไปด้วย เนื่องจากการปลอมแปลงข้อมูลชีวภาพบางชนิดสามารถทำได้อย่างง่ายดาย เช่น การปลอมลายนิ้วมือหรือแม้แต่การปลอมม่านตาจากรูปถ่ายก็สามารถทำได้ ดังนั้นการใช้ข้อมูลชีวภาพอาจทำให้ผู้สุจริตกลายเป็นผู้ต้องหา หรืออาจเพิ่มอัตราการเกิดอาชญากรรม (Kent, 2005) (Pfitzmann, 2008) ซึ่งความเสี่ยงเหล่านี้ล้วนเกิดจากธรรมชาติของข้อมูลชีวภาพ นอกจากนี้ความผิดพลาดของระบบข้อมูลชีวภาพอาจเกิดขึ้นได้ ซึ่งส่วนหนึ่งเป็นความผิดพลาดที่เกิดจากธรรมชาติของวิธีการทำงานของระบบเอง อันอาจทำให้เจ้าของข้อมูลส่วนบุคคลไม่สามารถใช้บริการหรือซื้อสินค้าที่ใช้ระบบข้อมูลชีวภาพได้ หรือไม่สามารถกระทำการยืนยันตัวตนได้ (Kindt, 2013) และเมื่อมีการใช้ข้อมูลชีวภาพมากขึ้นย่อมทำให้ข้อมูลชีวภาพนั้นตกเป็นเป้าหมายของการโจมตีอย่างหลีกเลี่ยงมิได้

เนื่องจากข้อมูลส่วนบุคคลประเภทชีวภาพเป็นข้อมูลที่อ่อนไหว ข้อมูลชีวภาพบางชนิดอาจทำให้ผู้เก็บรวบรวมได้รู้ข้อมูลเกี่ยวกับเจ้าของข้อมูลที่เจ้าของข้อมูลไม่ต้องการให้ผู้อื่นทราบ เช่น ข้อมูลด้านสุขภาพบางอย่าง (“Alcohol’s Effects on Eye Health,”) หรือความสนใจทางเพศ (Hall & Kimura, 1994) ดังนั้นการเก็บข้อมูลชีวภาพจึงเสี่ยงต่อการละเมิดความเป็นส่วนตัวของเจ้าของข้อมูลอีกด้วย

5.2 เปรียบเทียบกฎหมายคุ้มครองข้อมูลชีวภาพของ สหภาพยุโรป สหราชอาณาจักร รัฐอิลลินอยส์ และไทย

ผู้วิจัยได้ทำการศึกษาเปรียบเทียบกฎหมายการคุ้มครองข้อมูลส่วนบุคคลสำหรับข้อมูลชีวภาพระหว่าง กฎหมาย *General Data Protection Regulation* (*GDPR*) ของสหภาพยุโรป และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักร (DPA) ซึ่งนำเอาหลักการของ GDPR มาใช้ และกฎหมายคุ้มครองข้อมูลส่วนบุคคลชีวภาพของรัฐอิลลินอยส์ ประเทศสหรัฐอเมริกา (BIPA) ซึ่งเป็นพระราชบัญญัติฉบับแรกของประเทศสหรัฐอเมริกาที่ให้ความคุ้มครองข้อมูลชีวภาพโดยเฉพาะ และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของไทย โดยทำการเปรียบเทียบใน 5 ประเด็นหลัก คือ 1) คำจำกัดความของข้อมูลชีวภาพ 2) การประมวลผลข้อมูลชีวภาพที่ชอบด้วยกฎหมาย 3) การรักษาความปลอดภัย 4) การร้องเรียน และ 5) บทลงโทษ และศึกษาเฉพาะกรณีการเก็บรวบรวมใช้ และเปิดเผยข้อมูลส่วนบุคคลประเภทชีวภาพของภาคเอกชน จากการศึกษาสามารถสรุปผลการวิจัยได้ดังนี้

5.2.1 คำจำกัดความ

สหภาพยุโรป	“ข้อมูลชีวภาพ” หมายถึง “ข้อมูลส่วนบุคคลที่เกิดจากการประมวลผลโดยใช้เทคนิคพิเศษที่เกี่ยวกับลักษณะทางกายภาพ ทางสรีรวิทยาหรือพฤติกรรมของบุคคล ซึ่งสามารถนำไปใช้เพื่อระบุตัวตน หรือใช้เพื่อยืนยันตัวตนของบุคคล เช่น ภาพใบหน้า หรือลายนิ้วมือ”
สหราชอาณาจักร	“ข้อมูลชีวภาพ” หมายถึง “ข้อมูลส่วนบุคคลที่เกิดจากการประมวลผลโดยใช้เทคนิคพิเศษที่เกี่ยวกับลักษณะทางกายภาพ ทางสรีรวิทยาหรือพฤติกรรมของบุคคล ซึ่งสามารถนำไปใช้เพื่อระบุตัวตน หรือใช้เพื่อยืนยันตัวตนของบุคคล เช่น ภาพใบหน้า หรือลายนิ้วมือ”
รัฐอิลลินอยส์ สหรัฐอเมริกา	● “สิ่งระบุตัวตนชีวภาพ (Biometrics Identifier)” หมายถึง “การสแกนม่านตาหรือจอประสาทตา ลายนิ้วมือ เสียง หรือการสแกนมือ หรือใบหน้า ทั้งนี้สิ่งระบุตัวตนชีวภาพ ไม่รวมถึงตัวอย่างลายมือ ลายเซ็น ภาพถ่าย ตัวอย่างทางชีวภาพของมนุษย์ที่ใช้สำหรับการทดสอบหรือการคัดกรองทางวิทยาศาสตร์ ข้อมูลประชากร คำอธิบายรอยสัก คำอธิบายทางกายภาพ เช่น ส่วนสูง น้ำหนัก สีผม หรือสีตา นอกจากนี้ สิ่งระบุตัวตนชีวภาพยังไม่รวมถึง อวัยวะ เนื้อเยื่อ หรือชิ้นส่วนที่ได้จากการบริจาคตามที่กำหนดไว้ในพระราชบัญญัติการบริจาคอวัยวะ (Illinois Anatomical Gift Act - 755 ILCS 50/) หรือเลือด หรือเซรุ่ม ที่เก็บไว้ในนามของผู้รับหรือผู้ที่อาจได้รับการปลูกถ่ายอวัยวะ ไม่ว่าอวัยวะนั้นจะมาจากผู้ที่ยังมีชีวิตอยู่ หรือมาจากผู้ที่เสียชีวิตไปแล้ว และได้รับหรือเก็บรักษาโดยหน่วยงานจัดหาอวัยวะที่ได้รับมอบหมายจากรัฐบาลกลาง สิ่งระบุตัวตนชีวภาพไม่รวมถึงวัสดุชีวภาพที่มีการควบคุมภายใต้พระราชบัญญัติความเป็นส่วนตัวข้อมูลทางพันธุกรรม (Genetic Information Privacy Act) สิ่งระบุตัวตนชีวภาพไม่รวมถึงข้อมูลที่ได้จากผู้ป่วยในการดูแลสุขภาพหรือข้อมูลที่รวบรวม ใช้หรือเก็บรักษาเพื่อการรักษาพยาบาล การชำระเงิน หรือการดำเนินงานภายใต้พระราชบัญญัติประกันสุขภาพและความรับผิดชอบต่อหน้าที่ (Health Insurance Portability and Accountability Act 1996) ของรัฐบาลกลาง สิ่งระบุตัวตนชีวภาพไม่รวมถึงการเอกซเรย์ ไม่ว่าจะเป็นการเอกซเรย์รังสี เอกซเรย์คอมพิวเตอร์ (ซีทีสแกน) เอ็มอาร์ไอ PET/CT สแกน หรือการเอกซเรย์เต้านม (mammography) หรือภาพของกายวิภาคของมนุษย์ที่ใช้ในการวินิจฉัยพยากรณ์โรคหรือรักษาโรค หรือสภาวะด้านสุขภาพอื่น ๆ หรือเพื่อตรวจสอบเพิ่มเติมการทดสอบหรือการคัดกรองทางวิทยาศาสตร์” ● “ข้อมูลชีวภาพ (Biometric Information)” หมายถึง “ข้อมูลสิ่งระบุตัวตนชีวภาพใด ๆ โดยไม่คำนึงถึงวิธีการที่ถูกบันทึก แปลง จัดเก็บ หรือใช้ ที่นำไปใช้ในการระบุตัวบุคคล ทั้งนี้ ข้อมูลชีวภาพ ไม่รวมถึงข้อมูลที่ได้มาจากข้อมูลหรือขั้นตอนที่อยู่ภายใต้การยกเว้นของสิ่งระบุตัวตนชีวภาพ”
ไทย	“ข้อมูลส่วนบุคคลประเภทชีวภาพ” หมายถึง “ข้อมูลส่วนบุคคลที่เกิดจากการใช้เทคนิคหรือเทคโนโลยีที่เกี่ยวข้องกับการนำลักษณะเด่นทางกายภาพหรือทางพฤติกรรมของบุคคลมาใช้ทำให้สามารถยืนยันตัวตนของบุคคลนั้นที่ไม่เหมือนกับบุคคลอื่นได้ เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองม่านตา หรือข้อมูลจำลองลายนิ้วมือ”

5.2.2 การประมวลผลข้อมูลชีวภาพที่ชอบด้วยกฎหมาย

สหภาพยุโรป	● ความยินยอมโดยชัดแจ้ง ● ความจำเป็นสำหรับการปฏิบัติหน้าที่ ● ประโยชน์สำคัญต่อชีวิต ● กิจกรรมโดยชอบขององค์กรไม่แสวงหาผลกำไร ● เปิดเผยข้อมูลต่อสาธารณชน ● สิทธิเรียกร้องตามกฎหมาย ● ประโยชน์สาธารณะที่สำคัญ ● ประโยชน์สาธารณะด้านการคุ้มครองและประกันสังคม ● ประโยชน์ด้านสาธารณสุข ● จดหมายเหตุ การวิจัยหรือทางสถิติ
สหราชอาณาจักร	● ความยินยอมโดยชัดแจ้ง ● ความจำเป็นสำหรับการปฏิบัติหน้าที่ ● ประโยชน์สำคัญต่อชีวิต ● กิจกรรมโดยชอบขององค์กรไม่แสวงหาผลกำไร ● เปิดเผยข้อมูลต่อสาธารณชน ● สิทธิเรียกร้องตามกฎหมาย ● ประโยชน์สาธารณะที่สำคัญ ● ประโยชน์สาธารณะด้านการคุ้มครองและประกันสังคม ● ประโยชน์ด้านสาธารณสุข ● จดหมายเหตุ การวิจัยหรือทางสถิติ
รัฐอิลลินอยส์ สหรัฐอเมริกา	● ความยินยอมเป็นลายลักษณ์อักษร ● ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวม ซื้อ หรือรับโดยทางการค้า สิ่งระบุตัวตนทางชีวภาพ หรือข้อมูลส่วนบุคคลประเภทชีวภาพ ยกเว้นจะได้แจ้งให้เจ้าของข้อมูลชีวภาพทราบเป็นลายลักษณ์อักษร และได้รับอนุญาตจากเจ้าของข้อมูลชีวภาพเป็นลายลักษณ์อักษร ● ห้ามมิให้ขาย เช่า แลกเปลี่ยน หรือทำกำไรจากสิ่งระบุตัวตนทางชีวภาพ หรือข้อมูลส่วนบุคคลประเภทชีวภาพกับบุคคลที่สาม และต้องปฏิบัติต่อข้อมูลชีวภาพเสมือนเป็นข้อมูลที่ละเอียดอ่อนและเป็นความลับ ● ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลที่ครอบครองสิ่งระบุตัวตนทางชีวภาพ หรือข้อมูลส่วนบุคคลประเภทชีวภาพเปิดเผยหรือเปิดเผยซ้ำ ยกเว้นได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือการเปิดเผยหรือเปิดเผยซ้ำนั้นทำให้ธุรกรรมทางการเงินของเจ้าของข้อมูลส่วนบุคคลเสร็จสมบูรณ์ หรือเป็นสิ่งที่ต้องกระทำภายใต้กฎหมายของรัฐ หรือรัฐบาลกลาง หรือกฎหมายเทศบาล หรือเป็นการเปิดเผยข้อมูลตามคำสั่งของศาล หรือหมายศาลที่ออกโดยศาลที่มีอำนาจ

ไทย	การประมวลผลข้อมูลชีวภาพ ซึ่งเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวนั้นต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลเสมอ ยกเว้นในกรณีดังต่อไปนี้ ● ประโยชน์สำคัญต่อชีวิต ● กิจกรรมโดยชอบขององค์กรไม่แสวงหาผลกำไร ● เปิดเผยข้อมูลต่อสาธารณชน ● สิทธิเรียกร้องตามกฎหมาย ● การปฏิบัติตามกฎหมาย ● วัตถุประสงค์ทางเวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ ● ประโยชน์ด้านสาธารณสุข ● ประโยชน์สาธารณะด้านการคุ้มครองและประกันสังคม ● การวิจัยหรือทางสถิติ ● ประโยชน์สาธารณะที่สำคัญ

5.2.3 การรักษาความปลอดภัย

สหภาพยุโรป	● ใช้มาตรการทางด้านเทคนิคและทางด้านองค์กรที่เหมาะสมเพื่อรักษาความปลอดภัยของการประมวลผลข้อมูลส่วนบุคคล โดยมีการกำหนดมาตรการไว้ เช่น ต้องมีการเข้ารหัสหรือทำให้เป็นข้อมูลแฝง ระบบงานต้องมีความสามารถในการเก็บรักษาความลับ ความสมบูรณ์ การเข้าถึงได้ มีความสามารถในการกู้คืนการเข้าถึงระบบ มีกระบวนการทดสอบและประเมินประสิทธิภาพอย่างสม่ำเสมอ เป็นต้น ● กำหนดแนวทางในการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ● ในการประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงให้มีการประเมินผลกระทบการคุ้มครองข้อมูลส่วนบุคคลเสมอ ● ให้มีการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อหมดความจำเป็น หรือเจ้าของข้อมูลส่วนบุคคลร้องขอให้ลบหรือถอนความยินยอม ● ให้มีการแจ้งการรั่วไหลของข้อมูลส่วนบุคคลแก่หน่วยงานกำกับดูแลภายใน 72 ชั่วโมง ● ให้มีการบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล
สหราชอาณาจักร	● สำหรับการรักษาความปลอดภัยของข้อมูลส่วนบุคคลนั้น DPA ไม่ได้มีบทบัญญัติเพิ่มเติมจาก GDPR หากแต่มีบทยกเว้นสำหรับการแจ้งถึงการละเมิดข้อมูลส่วนบุคคล(Data Breach Notification) ซึ่งบัญญัติให้มีการยกเว้นมิต้องแจ้งการละเมิดข้อมูลส่วนบุคคลหากการประมวลผลข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อการหลีกเลี่ยงการละเมิดสิทธิของสภาผู้แทนราษฎร และ เพื่อวัตถุประสงค์ด้านการสื่อสารมวลชน ด้านวิชาการ ด้านศิลปะ ด้านวรรณกรรม
รัฐอิลลินอยส์ สหรัฐอเมริกา	● ต้องมีการพัฒนานโยบายที่เป็นลายลักษณ์อักษรและเปิดเผยต่อสาธารณชน โดยในนโยบายนั้นต้องกำหนดตารางการเก็บรักษา และแนวทางสำหรับการทำลายสิ่งระบุตัวตน หรือข้อมูลส่วนบุคคลประเภทชีวภาพอย่างถาวรเมื่อวัตถุประสงค์ในการเก็บรวบรวมสิ่งระบุตัวตนหรือข้อมูลดังกล่าวได้สำเร็จลุล่วงหรือภายใน 3 ปี นับจากวันสุดท้ายที่ผู้ควบคุมข้อมูลส่วนบุคคลประเภทชีวภาพได้ติดต่อกับเจ้าของข้อมูลส่วนบุคคล แล้วแต่วันใดจะถึงก่อน

ไทย	● ผู้ควบคุมข้อมูลส่วนบุคคลต้องใช้มาตรการที่เหมาะสมเพื่อรักษาความปลอดภัยของข้อมูลส่วนบุคคล โดยต้องมีการทบทวนและปรับปรุงให้มีประสิทธิภาพอยู่เสมอ โดยมีการกำหนดมาตรฐานขั้นต่ำสำหรับหน่วยงานและกิจการที่ยังไม่อยู่ภายใต้บังคับของพระราชบัญญัติฉบับนี้ ● ให้มีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล สำหรับผู้ควบคุมข้อมูลส่วนบุคคลที่เป็นหน่วยงานของรัฐ หรือกรณีที่มีการใช้ข้อมูลส่วนบุคคลเป็นจำนวนมาก หรือหากกิจกรรมหลักเป็นการเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหว ● ให้มีการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อหมดความจำเป็น เช่น เจ้าของข้อมูลส่วนบุคคลร้องขอให้ลบหรือถอนความยินยอม หรือเมื่อพ้นระยะเวลาการเก็บรักษาหรือข้อมูลส่วนบุคคลนั้นไม่มีความเกี่ยวข้อง หรือเกินความจำเป็นตามวัตถุประสงค์ ● ต้องแจ้งเหตุการณ์รั่วไหลของข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง ● ต้องมีการบันทึกรายการเพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถตรวจสอบได้

5.2.4 การร้องเรียน

สหภาพยุโรป	● เจ้าของข้อมูลส่วนบุคคลต้องได้รับความเดือดร้อน หรือความเสียหายแก่ทรัพย์สิน หรือสิ่งอื่นใดอันเป็นผลจากการละเมิดข้อกำหนดจึงจะมีสิทธิได้รับค่าสินไหมทดแทน ● เจ้าของข้อมูลส่วนบุคคลมีสิทธิยื่นฟ้องหน่วยงานกำกับดูแลในกรณีที่หน่วยงานกำกับดูแลไม่ดำเนินการจัดการกับคำร้อง หรือไม่แจ้งเจ้าของข้อมูลส่วนบุคคลให้ทราบถึงความคืบหน้าหรือผลของคำร้องภายใน 3 เดือน หรือเจ้าของข้อมูลส่วนบุคคลต้องการอุทธรณ์คำตัดสินของหน่วยงานกำกับดูแล ● เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการฟ้องคดีต่อผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล หากเห็นว่าผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลกระทำการละเมิดสิทธิของตนภายใต้ข้อกำหนด GDPR
สหราชอาณาจักร	● เมื่อพิจารณาแล้วเห็นว่าผู้ควบคุมข้อมูลประมวลผลข้อมูลส่วนบุคคลของตนละเมิดข้อกำหนดตาม GDPR เจ้าของข้อมูลส่วนบุคคลมีสิทธิยื่นคำร้องต่อ ICO ได้ ● หากเจ้าของข้อมูลส่วนบุคคลเห็นว่าผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลกระทำการอันเป็นการละเมิดสิทธิของตนภายใต้ข้อกำหนด GDPR และ DPA เจ้าของข้อมูลส่วนบุคคลมีสิทธิยื่นฟ้องผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลต่อศาล
รัฐอิลลินอยส์ สหรัฐอเมริกา	● เมื่อเห็นว่าการประมวลผลข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นการละเมิดข้อกำหนดของ BIPA เจ้าของข้อมูลส่วนบุคคลมีสิทธิยื่นฟ้องคดีต่อศาลได้ โดยสามารถยื่นฟ้องคดีต่อศาลของรัฐ (State Circuit Court) หรือศาลแขวงของรัฐบาลกลาง (Federal State Court) ได้ ทั้งนี้ในการยื่นฟ้องคดีสามารถยื่นฟ้องคดีแบบกลุ่ม (Class Action) ได้ เนื่องจากลักษณะของการละเมิดมักมีผู้เสียหายเป็นจำนวนมาก ทั้งนี้ BIPA ไม่ได้มีการกำหนดอายุความสำหรับการฟ้องคดี ● เจ้าของข้อมูลส่วนบุคคลสามารถยื่นฟ้องได้แม้ยังไม่ได้รับความเสียหายจากการละเมิด

ไทย	● เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้าง ฝ่าฝืนหรือไม่ปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือประกาศของคณะกรรมการ ● หากเจ้าของข้อมูลส่วนบุคคลเห็นว่าผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล กระทำการละเมิดบทบัญญัติของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แล้วก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล เจ้าของข้อมูลส่วนบุคคลสามารถยื่นฟ้องคดีต่อศาลได้

5.2.5 **บทลงโทษ**

สหภาพยุโรป	● การฝ่าฝืนข้อกำหนด GDPR ต้องระวางโทษทางปกครองไม่เกิน 10,000,000 ยูโร หรือ 20,000,000 ยูโร หรือในกรณีขององค์กรธุรกิจ (undertakings) ต้องระวางค่าปรับทางปกครองไม่เกินร้อยละ 2 หรือร้อยละ 4 ของมูลค่ายอดขายทั่วโลกของปีงบประมาณก่อนหน้า แล้วแต่จำนวนใดจะสูงกว่า ทั้งนี้ขึ้นอยู่กับฐานความผิด ● ประเภทของข้อมูลส่วนบุคคลที่ได้รับผลกระทบจากการละเมิดอาจทำให้จำนวนค่าปรับสูงขึ้น ทั้งนี้ขึ้นอยู่กับการพิจารณาของหน่วยงานกำกับดูแล
สหราชอาณาจักร	● บทลงโทษสำหรับผู้ฝ่าฝืนข้อกำหนดของ DPA อยู่ในรูปของค่าปรับทางปกครอง โดย ICO หน่วยงานผู้มีหน้าที่กำกับดูแลเป็นผู้มีอำนาจในการลงโทษ อัตราค่าปรับของการละเมิดบทบัญญัติของ DPA มี 2 ระดับ 1) ระดับสูงสุด คือ ไม่เกิน 20,000,000 ยูโร หรือในกรณีขององค์กรธุรกิจ (undertakings) ต้องระวางค่าปรับทางปกครองไม่เกินร้อยละ 4 ของมูลค่ายอดขายทั่วโลกของปีงบประมาณก่อนหน้า แล้วแต่จำนวนใดจะสูงกว่า หรือ 2) ระดับทั่วไป ต้องระวางโทษทางปกครองไม่เกิน 10,000,000 ยูโร หรือในกรณีขององค์กรธุรกิจ (undertakings) ต้องระวางค่าปรับทางปกครองไม่เกินร้อยละ 2 ของมูลค่ายอดขายทั่วโลกของปีงบประมาณก่อนหน้า แล้วแต่จำนวนใดจะสูงกว่า
รัฐอิลลินอยส์ สหรัฐอเมริกา	● สำหรับการฝ่าฝืนบทบัญญัติของ BIPA โดยประมาท ผู้กระทำการละเมิดจะต้องจ่ายค่าสินไหม 1,000 เหรียญสหรัฐ หรือค่าเสียหายตามจริง แล้วแต่จำนวนใดจะสูงกว่า ● สำหรับการฝ่าฝืนบทบัญญัติของ BIPA โดยเจตนา หรือโดยปราศจากความระมัดระวัง ผู้กระทำการละเมิดจะต้องจ่ายค่าสินไหม 5,000 เหรียญสหรัฐ หรือค่าเสียหายตามจริง แล้วแต่จำนวนใดจะสูงกว่า ● นอกจากนี้ผู้ละเมิดยังต้องจ่ายค่าฤชาธรรมเนียมและค่าใช้จ่ายของทนายที่สมเหตุสมผล รวมถึงค่าธรรมเนียมพยานผู้เชี่ยวชาญและค่าใช้จ่ายในการดำเนินคดีอื่น ๆ และการชดเชยอื่นใดตามแต่ศาลของรัฐหรือศาลรัฐบาลกลางเห็นสมควร

ไทย	● โทษทางแพ่ง : ค่าสินไหมทดแทนสำหรับความเสียหายที่เกิดขึ้นภายใต้หลักความรับผิดเด็ดขาด (strict liability) ซึ่งรวมค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้ว และศาลอาจสั่งให้จ่ายค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มได้ ทั้งนี้ต้องไม่เกินสองเท่าของค่าสินไหมทดแทนที่แท้จริง ● โทษทางอาญา : หากการละเมิดทำให้เกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย มีโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ และหากการละเมิดดังกล่าวเป็นไปเพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น อาจถูกลงโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1,000,000 บาท หรือทั้งจำทั้งปรับ เนื่องจากความผิดนี้มิได้เป็นความผิดต่อรัฐหรือสังคมโดยรวมจึงเป็นความผิดอันยอมความได้ ในกรณีที่ผู้ประกอบธุรกิจเป็นนิติบุคคล กรรมการ ผู้จัดการ หรือผู้ที่รับผิดชอบการดำเนินงานของนิติบุคคลนั้นอาจจะต้องรับผิดเป็นส่วนตัวสำหรับการกระทำความผิดนั้น ๆ ด้วย ● โทษทางปกครอง : มีโทษขั้นต่ำอยู่ที่ 500,000 บาท และโทษสูงสุดอยู่ที่ 5,000,000 บาท ขึ้นอยู่กับความร้ายแรงของการกระทำความผิดและขนาดของกิจการของผู้ที่กระทำผิด

6. อภิปรายผล

6.1 คำจำกัดความ

สหราชอาณาจักรได้ให้คำจำกัดความของ “ข้อมูลชีวภาพ” ไว้ เหมือนกันกับของสหภาพยุโรป โดยคำจำกัดความของข้อมูลชีวภาพตาม GDPR และ DPA นั้นประกอบด้วย 4 ส่วน คือ 1) ต้องเป็นข้อมูลส่วนบุคคล 2) ต้องเป็นข้อมูลที่ได้จากการประมวลผลโดยใช้เทคนิคพิเศษ 3) ต้องเกี่ยวกับลักษณะทางกายภาพ หรือทางสรีรวิทยา หรือพฤติกรรมของบุคคล และ 4) ต้องสามารถนำไปใช้ระบุตัวตน หรือใช้เพื่อระบุตัวตนได้

สำหรับ BIPA ของรัฐอิลลินอยส์สหรัฐอเมริกาได้บัญญัติไว้ชัดเจนว่าสิ่งใดมิถือว่าเป็นข้อมูลสิ่งระบุตัวตนชีวภาพ เช่น ตัวอย่างลายมือ ลายเซ็น ภาพถ่าย คำอธิบายรอยสัก คำอธิบายทางกายภาพ เช่น ส่วนสูง น้ำหนัก สีผม หรือสีตา เป็นต้น และได้ระบุอย่างชัดเจนว่าวัสดุหรือสิ่งอื่นใดที่เกี่ยวกับชีวภาพซึ่งอยู่ภายใต้กฎหมายอื่นไม่ถือว่าเป็นสิ่งระบุตัวตนชีวภาพภายใต้บทบัญญัติของ BIPA เช่น พ.ร.บ. การบริจาคอวัยวะ (Illinois Anatomical Gift Act - 755 ILCS 50/) พ.ร.บ. ความเป็นส่วนตัวข้อมูลทางพันธุกรรม (Genetic Information Privacy Act) เป็นต้น

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ให้คำจำกัดความไว้ตามแนวทางของ GDPR แต่มีข้อปลีกย่อยที่ต่างออกไป โดย พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ระบุว่า “เป็นการนำลักษณะเด่นทางกายภาพ หรือทางพฤติกรรมของบุคคลมาใช้” ในขณะที่ GDPR และ DPA ระบุว่า “ต้องเกี่ยวกับลักษณะทางกายภาพ หรือทางสรีรวิทยา หรือพฤติกรรมของบุคคล”

ในขณะที่ GDPR และ DPA กำหนดว่าข้อมูลทางสรีรวิทยานั้นหากมีการนำมาใช้เพื่อระบุตัวตนหรือยืนยันตัวตนแล้วจะถือว่าเป็นข้อมูลชีวภาพ แต่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นกำหนดให้เฉพาะข้อมูลทางกายภาพและพฤติกรรมที่นำมาใช้เพื่อระบุตัวตนหรือยืนยันตัวตนเป็นข้อมูลชีวภาพ ดังนั้น ภายใต้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ข้อมูลชีวภาพบางอย่าง เช่น คลื่นสมอง หรือจังหวะการเต้นของหัวใจ ซึ่งเป็น

ข้อมูลทางสรีรวิทยาที่สามารถนำมาใช้ในการระบุตัวตนและยืนยันตัวตนได้นั้นไม่ถือว่าเป็นข้อมูลชีวภาพ

นอกจากนี้ คำจำกัดความที่บัญญัติไว้ใน GDPR, DPA, BIPA และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นไม่มีกฎหมายใดที่ถือว่าข้อมูลชีวภาพตั้งต้นที่นำไปใช้ในการสร้างแม่แบบ เช่น ภาพถ่ายใบหน้า หรือภาพถ่ายลายนิ้วมือนั้นเป็นข้อมูลชีวภาพ เนื่องจากข้อมูลตั้งต้นนั้นไม่ได้เป็นข้อมูลที่ได้มาจากการใช้เทคนิคหรือเทคโนโลยี

เนื่องจากการพัฒนาของเทคโนโลยีแบบก้าวกระโดดอาจทำให้สิ่งที่ไม่ได้เป็นข้อมูลชีวภาพในปัจจุบันกลายเป็นข้อมูลชีวภาพได้ในอนาคต ภาพถ่ายซึ่งในอดีตไม่สามารถนำไปใช้เพื่อวัตถุประสงค์ในการระบุตัวตนหรือยืนยันตัวตนได้ เนื่องจากไม่มีความคมชัดเพียงพอ หรือไม่ได้อยู่ในรูปแบบที่สามารถนำไปใช้สำหรับการระบุตัวตนหรือยืนยันตัวตนได้ แต่ด้วยเทคโนโลยีในปัจจุบันไม่เพียงแต่จะสามารถนำภาพถ่ายไปใช้ในการระบุตัวตนหรือยืนยันตัวตนได้ แต่ลายนิ้วมือจากภาพถ่ายที่ถ่ายในระยะไกลยังสามารถนำไปใช้สร้างลายนิ้วมือด้วยปริ้นเตอร์ 3 มิติ เพื่อปลดล็อกไอโฟนได้อีกด้วย (Scharr, 2014) ในปัจจุบันแม้สารพันธุกรรมหรือดีเอ็นเออาจนำไปใช้ยืนยันตัวตนหรือระบุตัวตนได้ แต่ไม่อาจถือว่าเป็นข้อมูลชีวภาพได้เนื่องจากไม่สามารถใช้ในการยืนยันตัวตนหรือระบุตัวตนในลักษณะอัตโนมัติ (automate) ในทันทีทันใด (real-time) ได้ การตรวจพิสูจน์ดีเอ็นเอนั้นมีหลายขั้นตอนและใช้เวลานาน อีกทั้งบางขั้นตอนมิใช่วิธีการอัตโนมัติ (Kindt, 2013) จึงยังไม่สามารถใช้ดีเอ็นเอในลักษณะเดียวกับข้อมูลชีวภาพได้ อย่างไรก็ดีในอนาคตอาจสามารถใช้ดีเอ็นเอในการยืนยันตัวตนหรือระบุตัวตนแบบอัตโนมัติในทันทีทันใดได้ หรือแม้กระทั่งข้อมูลอื่น ๆ ที่คาดไม่ถึงในปัจจุบันอาจถูกนำมาใช้ในการยืนยันตัวตนหรือระบุตัวตนในลักษณะดังกล่าวได้

ทั้งนี้ Els J. Kindt ผู้เขียนหนังสือ Privacy and Data Protection Issues of Biometrics Applications ได้เสนอคำจำกัดความของ “ข้อมูลชีวภาพ” ไว้อย่างน่าสนใจดังนี้

“ข้อมูลชีวภาพ คือ ข้อมูลส่วนบุคคลทั้งหมดซึ่ง (ก) เกี่ยวข้องโดยตรงหรือโดยอ้อมกับลักษณะทางชีววิทยาหรือพฤติกรรมที่เป็นเอกลักษณ์เฉพาะของมนุษย์และ (ข) ถูกใช้หรือเหมาะสมที่จะใช้โดยวิธีอัตโนมัติ (ค) เพื่อวัตถุประสงค์ในการระบุตัวตน การยืนยันตัวตนหรือการตรวจสอบการเรียกร้องสิทธิของบุคคลธรรมดา”

คำจำกัดความนี้ระบุให้ถือว่าข้อมูลที่เกี่ยวข้องกับลักษณะทางชีววิทยาหรือพฤติกรรมที่เป็นเอกลักษณ์เฉพาะของมนุษย์ไม่ว่าจะโดยตรงหรือโดยอ้อมเป็นข้อมูลชีวภาพทั้งหมด ดังนั้นข้อมูลชีวภาพตั้งต้นจึงถือว่าเป็นข้อมูลชีวภาพตามคำจำกัดความนี้ นอกจากนี้แล้ว คำจำกัดดังกล่าวยังครอบคลุมถึงข้อมูลชีวภาพที่ยังไม่ถูกใช้เป็นข้อมูลชีวภาพ แต่มีความเหมาะสมที่จะถูกนำไปใช้เป็นข้อมูลชีวภาพในอนาคตอีกด้วย กล่าวคือข้อมูลชีวภาพบางอย่าง เช่น ข้อมูลดีเอ็นเอ ซึ่งสามารถนำไปใช้ระบุตัวตน หรือยืนยันตัวตนได้แต่ยังไม่สามารถนำไปใช้แบบอัตโนมัติในทันทีทันใดได้นั้นไม่ถือว่าเป็นข้อมูลชีวภาพตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือแม้กระทั่ง GDPR และ DPA แต่ตามคำจำกัดความนี้ถือว่าเป็นข้อมูลชีวภาพ ซึ่งการให้คำจำกัดความนี้เป็นการเปิดกว้างสำหรับรองรับวิวัฒนาการทางเทคโนโลยีในอนาคต

6.2 หลักเกณฑ์การประมวลผลข้อมูลชีวภาพ

เมื่อเปรียบเทียบหลักเกณฑ์ในการประมวลผลข้อมูลส่วนบุคคลประเภทชีวภาพที่ถูกต้องตามกฎหมายระหว่าง GDPR, DPA และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในด้านของการให้ความยินยอมแล้ว ผู้วิจัยพบว่าการประมวลผลข้อมูลส่วนบุคคลประเภทชีวภาพที่ถูกต้องตามกฎหมายต้องได้รับความยินยอมอย่างชัดแจ้งทั้งหมด แม้ในตัวบทกฎหมายของ BIPA จะมิได้ระบุว่าต้องได้รับความยินยอมอย่างชัดแจ้ง แต่ได้มีการบัญญัติไว้ในข้อแม้ของการได้รับความยินยอมไว้ว่าต้องได้รับความยินยอมเป็นลายลักษณ์อักษร ซึ่งถือว่าต้องได้รับความยินยอมอย่างชัดแจ้ง

นอกจากนี้ GDPR, DPA และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังมีหลักเกณฑ์การประมวลผลข้อมูลส่วนบุคคลประเภทชีวภาพที่เหมือนกัน ดังนี้ 1) ประโยชน์สำคัญต่อชีวิต 2) กิจกรรมโดยชอบขององค์กรไม่แสวงหาผลกำไร 3) เปิดเผยข้อมูลต่อสาธารณชน 4) สิทธิเรียกร้องตามกฎหมาย 5) ประโยชน์ด้านสาธารณสุข 6) ประโยชน์สาธารณะด้านการคุ้มครองและประกันสังคม 7) การวิจัยหรือทางสถิติ และ 8) ประโยชน์สาธารณะที่สำคัญ

สำหรับหลักเกณฑ์วัตถุประสงค์ทางเวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์นั้น พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้บัญญัติเป็นหลักเกณฑ์แยกออกมา แต่ GDPR และ DPA ได้บัญญัติไว้เป็นส่วนหนึ่งภายใต้หลักเกณฑ์ประโยชน์สาธารณะด้านการคุ้มครองและประกันสังคม นอกจากนี้ ในกรณีการประมวลผลเพื่อการวิจัยหรือทางสถิตินั้น GDPR และ DPA บัญญัติว่าสามารถทำได้หากเป็นความจำเป็นสำหรับวัตถุประสงค์ในการจัดเก็บในลักษณะจดหมายเหตุ ในขณะที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้น มิได้ระบุเจาะจงว่าต้องเป็นการเก็บในลักษณะจดหมายเหตุ

สำหรับหลักเกณฑ์ความจำเป็นสำหรับการปฏิบัติหน้าที่ตาม GDPR และ DPA นั้น พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มิได้มีการบัญญัติหลักเกณฑ์นี้ไว้ แต่กำหนดไว้ให้เป็นการใช้สิทธิตามกฎหมาย โดยสามารถใช้หลักเกณฑ์สิทธิเรียกร้องตามกฎหมายภายใต้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้

6.3 การรักษาความปลอดภัย

GDPR และ DPA ได้กำหนดให้การประมวลผลข้อมูลส่วนบุคคลต้องมีมาตรการทั้งด้านเทคนิคและทางด้านองค์กรที่เหมาะสม โดยต้องเป็นไปตามหลักการคุ้มครองข้อมูลส่วนบุคคลด้วยการออกแบบ (data protection by design) และการคุ้มครองข้อมูลส่วนบุคคล (data protection by default) สำหรับ BIPA นั้นมิได้มีการกำหนดหลักเกณฑ์ในการรักษาความปลอดภัยของข้อมูลส่วนบุคคลไว้ แต่กำหนดว่าต้องมีนโยบายในการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่เป็นลายลักษณ์อักษร และต้องเปิดเผยต่อสาธารณชน

ด้าน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องใช้มาตรการที่เหมาะสมเพื่อรักษาความปลอดภัยของข้อมูลส่วนบุคคล และต้องมีการทบทวน และปรับปรุงให้มีประสิทธิภาพอยู่เสมอโดยจะมีการกำหนดมาตรฐานขั้นต่ำไว้ แต่ในขณะที่ยังมีการยกเว้นการบังคับใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และยังมิได้ใช้ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลว่าด้วยมาตรฐานขั้นต่ำ

เกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล เพื่อให้องค์กรต่าง ๆ สามารถดำเนินการปรับปรุงมาตรการการรักษาความปลอดภัยของข้อมูลส่วนบุคคลให้รองรับข้อกำหนดตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายลำดับรองได้นั้น องค์กรเอกชนหลายแห่งในประเทศไทยจึงให้ความสนใจไปที่การจัดทำมาตรฐานความปลอดภัยให้แก่ข้อมูลหรือ ISO 27001 (Information Security Standard) ซึ่งเป็นมาตรฐานที่เป็นที่ยอมรับในระดับสากลสำหรับการวางมาตรการความปลอดภัยของข้อมูล (ศุภวัชร์ มาลานนท์ & ชิโนภาส อุดมผล, 2020) ซึ่งคาดว่าน่าจะเพียงพอสำหรับการรักษาความปลอดภัยของข้อมูลส่วนบุคคล สำหรับสถาบันการเงินนั้น ธนาคารแห่งประเทศไทยเองได้มีการพัฒนา “แนวปฏิบัติการใช้เทคโนโลยีชีวมิติ (Biometric Technology) ในการให้บริการทางการเงิน” เพื่อใช้อ้างอิงเป็นมาตรฐานเพื่อให้มั่นใจว่าการให้บริการทางการเงินที่เกี่ยวข้องกับเทคโนโลยีชีวภาพนั้นมีความมั่นคงปลอดภัย โดยแนวปฏิบัติดังกล่าวสอดคล้องกับมาตรฐานสากล และครอบคลุมตั้งแต่ระดับนโยบายขององค์กรไปจนถึงแนวทางการดำเนินการและการบริหารความเสี่ยง

GDPR และ DPA กำหนดให้มีการประเมินผลกระทบการคุ้มครองข้อมูลส่วนบุคคลสำหรับการประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงสูง และหากผลกระทบที่อาจเกิดต่อเจ้าของข้อมูลส่วนบุคคลสูงจะต้องมีการรักษาความปลอดภัยที่สูงตามไปด้วย แต่ BIPA และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไม่ได้มีการกำหนดให้มีการประเมินผลกระทบการคุ้มครองข้อมูลส่วนบุคคลไว้แต่อย่างใด

นอกจากนี้ GDPR, DPA และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดแนวทางในการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไว้ แต่ BIPA นั้นไม่ได้มีการกำหนดแนวทางในการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

สำหรับการลบหรือทำลายข้อมูลส่วนบุคคล GDPR, DPA และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดให้ลบข้อมูลส่วนบุคคลเมื่อหมดความจำเป็น หรือเมื่อเจ้าของข้อมูลส่วนบุคคลขอร้องให้ลบ แต่สำหรับ BIPA ได้กำหนดไว้ว่าต้องลบเมื่อวัตถุประสงค์สำเร็จลุล่วง หรือภายใน 3 ปี นับจากวันสุดท้ายที่ผู้ควบคุมข้อมูลส่วนบุคคลประเภทชีวภาพได้ติดต่อกับเจ้าของข้อมูลส่วนบุคคลแล้วแต่วันใดจะถึงก่อน

ในขณะที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดข้อยกเว้นสำหรับการลบข้อมูลส่วนบุคคลไว้ว่า ไม่ต้องลบหากการเก็บรักษานั้นมีวัตถุประสงค์ในการใช้เพื่อเสรีภาพในการแสดงความคิดเห็น หรือการใช้เพื่อสิทธิเรียกร้องตามกฎหมาย เช่น การเก็บรักษาเพื่อการศึกษาวิจัยหรือสถิติ หรือการเก็บรักษาเป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เพื่อประโยชน์สาธารณะด้านการสาธารณสุข เป็นต้น ด้าน GDPR และ DPA ได้กำหนดว่าไม่ต้องลบข้อมูลส่วนบุคคลในกรณีที่การประมวลผล 1) มีความจำเป็นเพื่อการใช้สิทธิเสรีภาพในการแสดงออกและการเข้าถึงข้อมูล 2) การปฏิบัติตามกฎหมาย 3) เพื่อประโยชน์สาธารณะเกี่ยวกับสุขภาพของประชาชน และ 4) วัตถุประสงค์ในการเก็บรวบรวมเพื่อประโยชน์สาธารณะ เพื่อการวิจัยทางวิทยาศาสตร์หรือประวัติศาสตร์ หรือวัตถุประสงค์ทางสถิติ

สำหรับการรั่วไหลของข้อมูลส่วนบุคคลนั้น GDPR, DPA และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดให้ต้องมีการแจ้งหน่วยงานกำกับดูแลในกรณีที่มีการรั่วไหลของข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง อย่างไรก็ดี DPA ได้กำหนดข้อยกเว้นสำหรับการแจ้งการรั่วไหลของข้อมูลส่วนบุคคลต่อหน่วยงานกำกับดูแลในกรณีที่การประมวลผลข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อวัตถุประสงค์ในการหลีกเลี่ยงการละเมิดสิทธของสภาผู้แทนราษฎร หรือเพื่อวัตถุประสงค์ด้านการสื่อสารมวลชน ด้านวิชาการ ด้านศิลปะ และด้านวรรณกรรม

อนึ่ง การบันทึกรายการการประมวลผลข้อมูลส่วนบุคคลนั้นได้มีการกำหนดไว้ใน GDPR, DPA และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ให้มีการบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ แต่สำหรับ BIPA ไม่มีข้อกำหนดเกี่ยวกับการบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้แต่อย่างใด

6.4 การร้องเรียน

เจ้าของข้อมูลส่วนบุคคลสามารถร้องเรียนต่อหน่วยงานกำกับดูแลได้หากได้รับความเดือดร้อน หรือเกิดความเสียหายแก่ทรัพย์สินอันเป็นผลจากการละเมิดข้อกำหนดใน GDPR และ DPA รวมถึงมีสิทธิยื่นฟ้องหน่วยงานกำกับดูแล และมีสิทธิในการฟ้องคดีต่อผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้โดยเจ้าของข้อมูลส่วนบุคคลสามารถร้องเรียนได้หากเกิดความเสียหาย อย่างไรก็ดี ศาลในสหราชอาณาจักรได้มีคำพิพากษาว่าความเสียหายนั้น แม้เป็นเพียงการที่เจ้าของข้อมูลส่วนบุคคลสูญเสียการควบคุมข้อมูลส่วนบุคคลของตนก็ถือเป็นความเสียหายที่ต้องได้รับการเยียวยา (Covington & Burling LLP, 2019) นอกจากนี้ ศาลฎีกาของรัฐอิลลินอยส์ได้พิพากษาว่าเจ้าของข้อมูลส่วนบุคคลสามารถฟ้องคดีได้แม้ว่าความเดือดร้อนเพียงอย่างเดียวที่ได้รับคือการถูกละเมิดสิทธิตามกฎหมาย (Rosenbach v. Six Flags Entertainment Corp., 2019 IL 123186) สำหรับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดว่าหากมีการฝ่าฝืน หรือไม่ปฏิบัติตามข้อกำหนดในพระราชบัญญัตินี้ เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อหน่วยงานกำกับดูแลเช่นกัน และหากการละเมิดนั้นทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล เจ้าของข้อมูลส่วนบุคคลสามารถยื่นฟ้องคดีต่อศาลได้ อย่างไรก็ดี เนื่องจาก พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังไม่มีการบังคับใช้อย่างเต็มรูปแบบ จึงยังไม่มีการร้องเรียน ไม่มีการฟ้องคดีต่อศาล ดังนั้นจึงไม่มีคำพิพากษาศาลฎีกาอันสามารถจะนำมาเป็นแนวทางได้

ด้านการดำเนินคดีแบบกลุ่ม (class action) นั้นสามารถทำได้ในสหราชอาณาจักรตามคำพิพากษาของศาลอุทธรณ์ในคดี Lloyd v Google LLC [2019] EWCA Civ 1599 ที่ให้ถือว่า Richard Lloyd เป็นตัวแทนของผู้ใช้ไอโฟนที่ใช้เว็บเบราว์เซอร์ซาฟารีทั้งหมดในประเทศอังกฤษและเวลส์ (Covington & Burling LLP, 2019) ทางด้านรัฐอิลลินอยส์การดำเนินคดีแบบกลุ่มโดยถือว่าโจทก์เป็นตัวแทนของเจ้าของข้อมูลส่วนบุคคลที่ถูกละเมิดทั้งหมดสามารถทำได้เช่นเดียวกันตามกฎหมายของสหรัฐอเมริกา เนื่องจากลักษณะของการละเมิดมักมีผู้เสียหายเป็นจำนวนมาก

สำหรับการละเมิดข้อมูลส่วนบุคคลตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นมีอายุความ 3 ปี นับแต่วันที่ผู้เสียหายได้รับรู้ถึงความ

เสียหายและรู้ตัวผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ต้องรับผิด หรือ 10 ปีนับแต่วันที่มีการละเมิดข้อมูลส่วนบุคคล ส่วน GDPR, DPA และ BIPA นั้นมิได้มีการกำหนดอายุความไว้ในตัวบทแต่อย่างใด

6.5 บทลงโทษ

GDPR และ DPA ได้กำหนดบทลงโทษทางปกครองไม่เกิน 10,000,000 ยูโร หรือ 20,000,000 ยูโร หรือในกรณีขององค์กรธุรกิจค่าปรับทางปกครองไม่เกินร้อยละ 2 หรือร้อยละ 4 ของมูลค่ายอดขายทั่วโลกของปีงบประมาณก่อนหน้า แล้วแต่จำนวนใดจะสูงกว่า ทั้งนี้ขึ้นอยู่กับฐานความผิดและประเภทของข้อมูลส่วนบุคคลที่ถูกละเมิด สำหรับบทลงโทษของ BIPA นั้นเป็นบทลงโทษทางปกครองเช่นเดียวกัน โดยหากเป็นการกระทำโดยประมาทต้องจ่ายค่าสินไหม 1,000 เหรียญสหรัฐ หรือค่าเสียหายตามจริง แล้วแต่จำนวนใดจะสูงกว่า แต่หากเป็นการกระทำโดยเจตนาค่าปรับจะสูงถึง 5,000 เหรียญสหรัฐ หรือค่าเสียหายตามจริง แล้วแต่จำนวนใดจะสูงกว่า ทั้งนี้การคำนวณค่าปรับสำหรับ BIPA นั้น อัตราบทลงโทษเป็นค่าเสียหายต่อราย ซึ่งหากมีจำนวนผู้เสียหายมากเท่าใดค่าเสียหายก็มากขึ้นเท่านั้น ดังเช่นกรณี Patel v. Facebook ซึ่ง Facebook ยินยอมจ่ายค่าเสียหายให้ 550 ล้านเหรียญสหรัฐในการไกล่เกลี่ย และในเวลาต่อมายอมเพิ่มเป็น 650 ล้านเหรียญสหรัฐ ซึ่งเจ้าของข้อมูลส่วนบุคคลจะได้รับค่าสินไหมเฉลี่ยที่ 200-400 เหรียญต่อคน ยังถือได้ว่าน้อยกว่าบทปรับขั้นต่ำที่กำหนดไว้ที่ 1,000 เหรียญสหรัฐอยู่มาก

อนึ่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นกฎหมายฉบับเดียวภายใต้ขอบเขตการวิจัยที่กำหนดโทษทางแพ่ง โทษทางอาญา และโทษทางปกครอง สำหรับโทษทางอาญานั้นอ้างอิงมาจากการกระทำผิดโดยการหมิ่นประมาทและการกระทำผิดโดยการทุจริต สำหรับโทษทางแพ่งนั้นได้กำหนดให้ใช้หลักความรับผิดเด็ดขาด (strict liability) โดยจะต้องชดใช้ค่าสินไหมทดแทนไม่ว่าจะจงใจหรือประมาทเลินเล่อ ทั้งนี้ได้กำหนดให้ค่าสินไหมทดแทนขึ้นอยู่กับความเสียหายที่เกิดขึ้นตามจริง รวมถึงค่าใช้จ่ายที่ได้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้ว นอกจากค่าสินไหมทดแทนที่แท้จริงแล้วศาลอาจสั่งให้จ่ายค่าสินไหมทดแทนเพื่อการลงโทษได้ไม่เกินสองเท่าของค่าสินไหมทดแทนที่ได้จ่ายไปตามจริง สำหรับโทษทางปกครองนั้นขึ้นอยู่กับความร้ายแรงของการกระทำความผิด และขนาดของกิจการของผู้กระทำความผิด

7. ข้อเสนอแนะ

7.1 คำจำกัดความ

การให้คำจำกัดความของ “ข้อมูลชีวภาพ” ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไม่คุ้มครองข้อมูลชีวภาพตั้งต้นที่นำไปใช้ในการสร้างแม่แบบ เช่น ภาพถ่ายใบหน้า หรือภาพถ่ายลายนิ้วมือไม่ถือว่าเป็นข้อมูลชีวภาพ เนื่องจากไม่ได้เป็นข้อมูลที่ได้มาจากการใช้เทคนิคหรือเทคโนโลยี แต่ข้อมูลเหล่านี้ล้วนมีความสำคัญที่ต้องได้รับการคุ้มครองเท่าเทียมกับข้อมูลแม่แบบ เนื่องจากสามารถนำไปใช้สร้างข้อมูลแม่แบบเพื่อนำไปใช้ในการยืนยันตัวตนหรือระบุตัวตนต่อไปได้

นอกจากนี้ คำจำกัดความดังกล่าวยังไม่ครอบคลุมถึงข้อมูลชีวภาพที่ยังไม่ถูกใช้เป็นข้อมูล

ชีวภาพ แต่มีความเหมาะสมที่จะถูกนำไปใช้เป็นข้อมูลชีวภาพในอนาคตอีกด้วย ดังนั้นการให้คำจำกัดความของคำว่า “ข้อมูลชีวภาพ” จึงควรเปิดกว้างเพื่อรองรับเทคโนโลยีในอนาคต

เนื่องจากคำว่า “ชีวภาพ” ที่คนทั่วไปคุ้นเคยกัน และตามความหมายในพจนานุกรมฉบับราชบัณฑิตยสถานนั้น หมายถึง “1) น. ความเป็นสิ่งมีชีวิต 2) ว. เกี่ยวกับสิ่งที่มีชีวิตและสิ่งที่สืบเนื่องมาจากสิ่งมีชีวิต เช่น วิทยาศาสตร์ชีวภาพ ปุ๋ยชีวภาพ” ดังนั้น คำว่า “ข้อมูลชีวภาพ” ตามความหมายที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้บัญญัติไว้ อาจทำให้เกิดความเข้าใจคลาดเคลื่อนได้ ความหมายของคำว่า “ชีวภาพ” จึงตรงกับคำว่า “biological” มากกว่า “biometrics” และเนื่องจากข้อมูลชีวภาพตามความหมายของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นจะต้องเกิดจากการใช้เทคนิคหรือเทคโนโลยีที่เกี่ยวข้องกับการนำลักษณะเด่นทางกายภาพ หรือพฤติกรรมของบุคคลมาใช้ในการยืนยันตัวตน ผู้วิจัยจึงขอเสนอให้เปลี่ยนคำว่า “ข้อมูลชีวภาพ” เป็น “ข้อมูลชีวมาตร” ซึ่งจะทำให้ได้ความหมายชัดเจนและสามารถเข้าใจได้ง่ายขึ้น

นอกจากนี้ ผู้วิจัยจึงเสนอให้ปรับคำจำกัดความตามแนวทางของ BIPA เพื่อกำหนดให้ชัดเจนว่าสิ่งใดถือเป็นข้อมูลชีวภาพเพื่อลดความจำเป็นในการตีความ และตามแนวทางของ Kindt เพื่อให้ครอบคลุมข้อมูลชีวภาพตั้งต้น และข้อมูลที่อาจเป็นข้อมูลชีวภาพได้ในอนาคต ดังนี้

“ข้อมูลชีวมาตร” หมายถึง “ข้อมูลส่วนบุคคลที่เกิดจากการใช้หรือเหมาะสมที่จะใช้เทคนิคหรือเทคโนโลยีที่เกี่ยวข้องโดยตรงหรือโดยอ้อมกับการนำลักษณะเด่นทางกายภาพ ทางสรีรวิทยาหรือทางพฤติกรรมของบุคคลมาใช้ทำให้สามารถยืนยันตัวตนของบุคคลนั้นที่ไม่เหมือนกับบุคคลอื่นได้ เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองม่านตา หรือข้อมูลจำลองลายนิ้วมือ ทั้งนี้ไม่รวมถึง ตัวอย่างทางชีวภาพของมนุษย์ที่ใช้สำหรับการทดสอบหรือการคัดกรองทางวิทยาศาสตร์ ข้อมูลประชากร คำอธิบายรอยสัก คำอธิบายทางกายภาพ เช่น ส่วนสูง น้ำหนัก สีผม หรือสีตา นอกจากนี้ ข้อมูลชีวมาตรยังไม่รวมถึงอวัยวะ เนื้อเยื่อ หรือชิ้นส่วนที่ได้จากการบริจาคหรือเลือด หรือเซรุ่ม ที่เก็บไว้ในนามของผู้รับหรือผู้ที่อาจได้รับการปลูกถ่ายอวัยวะ ไม่ว่าอวัยวะนั้นจะมาจากผู้ที่ยังมีชีวิตอยู่หรือมาจากผู้ที่เสียชีวิตไปแล้ว และไม่รวมถึงการเอกซเรย์ ไม่ว่าจะเป็นการเอกซเรย์รังสี เอกซเรย์คอมพิวเตอร์ ซีทีสแกน เอ็มอาร์ไอ เพ็ทสแกน หรือการเอกซเรย์เต้านม หรือภาพของกายวิภาคของมนุษย์ที่ใช้ในการวินิจฉัยพยากรณ์โรคหรือรักษาโรค หรือสภาวะด้านสุขภาพอื่น ๆ หรือเพื่อตรวจสอบเพิ่มเติมการทดสอบหรือการคัดกรองทางวิทยาศาสตร์”

7.2 หลักเกณฑ์การประมวลผลข้อมูลชีวภาพ

เมื่อพิจารณาแล้วผู้วิจัยเห็นว่าหลักเกณฑ์ในการประมวลผลข้อมูลชีวภาพตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นมีความเหมาะสมอยู่แล้ว เนื่องจากการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลชีวภาพโดยไม่ได้รับความยินยอมโดยชัดแจ้งสามารถกระทำได้ภายใต้หลักเกณฑ์ที่จำกัด

7.3 การรักษาความปลอดภัย

ผู้วิจัยมีความเห็นว่า พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ควรกำหนดให้มีการคุ้มครองข้อมูลส่วนบุคคลด้วยการออกแบบ (data protection by design) และการคุ้มครอง

ข้อมูลส่วนบุคคลขั้นพื้นฐาน (data protection by default) ตามแนวทางของ GDPR และ DPA และควรมีการกำหนดมาตรการต่างๆ ตามความเหมาะสม เช่น การเข้ารหัสลับข้อมูล (encrypt) การทำให้เป็นข้อมูลแฝงที่ไม่สามารถระบุตัวตนได้ (Pseudonymized) หรือการมีกระบวนการในการทดสอบประเมินประสิทธิภาพของมาตรการด้านเทคนิคและมาตรการด้านองค์กรอย่างสม่ำเสมอ นอกจากนี้ การรักษาความปลอดภัยของข้อมูลส่วนบุคคลประเภทชีวภาพควรใช้เทคโนโลยีที่ทันสมัยที่ยึดแนวทางการปฏิบัติด้านการรักษาความปลอดภัยที่เหมาะสมกับการรักษาความปลอดภัยข้อมูลส่วนบุคคลชีวภาพและยึดหลักมาตรฐานที่เป็นที่ยอมรับในระดับสากลในการรักษาความปลอดภัยของระบบข้อมูลชีวภาพอีกด้วย

นอกจากนี้ ผู้วิจัยเสนอว่าในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลประเภทชีวภาพนั้นควรมีการประเมินผลกระทบและความจำเป็นในการเก็บข้อมูลเสียก่อน และไม่ควรมีการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลชีวภาพที่ไม่จำเป็น ดังนั้นหากจะมีการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลประเภทชีวภาพ หากทำการประเมินผลกระทบแล้วผลที่ได้คือมีความเสี่ยงสูง ควรได้รับการอนุมัติจากคณะกรรมการคุ้มครองส่วนบุคคลเสียก่อนเช่นเดียวกับ GDPR และ DPA

นอกจากนี้ผู้วิจัยเห็นว่าแนวปฏิบัติของธนาคารแห่งประเทศไทยในการใช้เทคโนโลยีชีวมิตินั้นมีความเหมาะสมที่จะนำมาใช้เป็นแนวปฏิบัติสำหรับองค์กรธุรกิจที่มิใช่การให้บริการทางการเงิน แม้ว่าแนวปฏิบัติในการรักษาความปลอดภัยสำหรับองค์กรที่ให้บริการทางการเงินจะเข้มงวดรัดกุมกว่าองค์กรในภาคธุรกิจอื่น แต่ข้อมูลส่วนบุคคลประเภทชีวภาพนั้นมีความสำคัญและหากมีการรั่วไหล หรือถูกนำไปใช้ในทางไม่เหมาะสม อาจสร้างความเสียหายให้กับเจ้าของข้อมูลส่วนบุคคลได้อย่างมหาศาล

7.4 การร้องเรียน

เนื่องจากลักษณะพิเศษของข้อมูลส่วนบุคคลประเภทชีวภาพ ทำให้ความเสียหายที่อาจเกิดขึ้นจากการละเมิด หรือการรั่วไหลของข้อมูลส่วนบุคคลประเภทชีวภาพนั้นไม่อาจระงับได้ ดังนั้นจึงไม่สามารถประเมินความเสียหายอันอาจเกิดขึ้นได้ ผู้วิจัยจึงเสนอแนะว่าในการยื่นคำร้องต่อหน่วยงานกำกับดูแล หรือฟ้องคดีต่อศาลนั้นเจ้าของข้อมูลส่วนบุคคลเพียงสูญเสียการควบคุมข้อมูลส่วนบุคคลหรือถูกละเมิดสิทธิตามกฎหมายก็เพียงพอที่จะยื่นคำร้องได้แล้ว มิจำเป็นต้องได้รับความเสียหายด้านการเงินหรือความเดือดร้อนอันสามารถกำหนดมูลค่าได้ เพียงสูญเสียการควบคุมข้อมูลส่วนบุคคลหรือถูกละเมิดสิทธิตามกฎหมายก็สามารถถือได้ว่าเจ้าของข้อมูลส่วนบุคคลได้รับความเสียหายที่ต้องได้รับการเยียวยาแล้ว ทั้งนี้เป็นไปตามแนวทางที่ศาลอุทธรณ์ในสหราชอาณาจักรได้พิพากษาไว้ในคดี Lloyd v Google และศาลฎีกาในรัฐอิลลินอยส์ได้พิพากษาไว้ในคดี Rosenbach v. Six Flags

7.5 บทลงโทษ

ผู้วิจัยเห็นสมควรที่จะคงโทษทางอาญาไว้เพื่อให้ใช้ข้อมูลชีวภาพด้วยความระมัดระวัง เนื่องจากการรั่วไหลของข้อมูลส่วนบุคคลประเภทชีวภาพอาจทำให้เจ้าของข้อมูลส่วนบุคคลได้รับความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย เพื่อป้องกันมิให้เกิดการกระทำผิดตามทฤษฎีของการลงโทษเพื่อข่มขู่ยับยั้ง

สำหรับโทษทางปกครองเป็นการปรับสำหรับการกระทำความผิดที่เป็นการฝ่าฝืนหรือไม่

ปฏิบัติตามบทบัญญัติของกฎหมายหรือคำสั่งของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จึงควรคงโทษทางปกครองไว้แต่ให้ปรับอัตราโทษเป็นต่อราย เช่นเดียวกันกับบทลงโทษของรัฐอิลลินอยส์เพื่อเป็นการป้องปรามมิให้มีการละเมิดและให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้ความระมัดระวังและมาตรการในการรักษาความปลอดภัยที่เหมาะสม นอกจากนี้ยังทำให้อัตราบทลงโทษนั้นได้สัดส่วนกับจำนวนข้อมูลส่วนบุคคลชีวภาพที่ได้รับผลกระทบอีกด้วย

อนึ่ง ผู้วิจัยเสนอให้คงบทลงโทษทางแพ่งไว้ อย่างไรก็ดี เนื่องจากการละเมิดข้อมูลส่วนบุคคลประเภทชีวภาพนั้นไม่สามารถรอให้เกิดความเสียหายที่มีมูลค่าแล้วจึงทำการฟ้องคดี ทำให้อาจไม่สามารถประเมินความเสียหายเป็นจำนวนเงินได้ แต่จากแนวทางการพิพากษาของศาลฎีกาของรัฐอิลลินอยส์พิพากษาในคดีของ Rosenbach v. Six Flags และคำพิพากษาของศาลอุทธรณ์อังกฤษในคดี Lloyd v. Google สามารถสรุปได้ว่าความเสียหายจากการละเมิดการประมวลผลข้อมูลส่วนบุคคลแม้ยังไม่เกิดความเสียหายที่สามารถจับต้องได้ก็ถือว่าเป็นความเสียหายที่เกิดขึ้นจริงแล้ว ซึ่งค่าเสียหายให้เป็นไปตามดุลพินิจของศาล

References

Alcohol's Effects on Eye Health. Retrieved from https://guardionhealth.com/alcohols-effect-eye-health/

Clarke, R. (1997). *Introduction to Dataveillance and Information Privacy, and Definitions of Terms.* In X. Consultancy (Ed.). Retrieved from http://www.rogerclarke.com/DV/Intro.html

Coseraru, R. (2017). *Facial Recognition Systems and their Data Protection Risks Under the GDPR.* (Master Thesis), Tilburg University, Retrieved from http://arno.uvt.nl/show.cgi?fid=143731

Covington & Burling LLP. (2019). *Landmark Case Opens the Door to UK Data Protection Consumer Class Actions.* Retrieved from https://www.cov.com/en/news-and-insights/insights/2019/10/landmark-case-opens-the-door-to-uk-data-protection-consumer-class-actions

Friedewald, M., Finn, R., & Wright, D. (2013). *Seven Types of Privacy.* Retrieved from https://www.researchgate.net/publication/258892458_Seven_Types_of_Privacy

Hall, J. A., & Kimura, D. (1994). Dermatoglyphic Asymmetry and Sexual Orientation in Men. *Behavioral Neuroscience, 108*(6), 1203-1206.

Kent, J. (2005). *Malaysia car thieves steal finger.* Retrieved from http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm

Kindt, E. J. (2013). *Privacy and Data Protection Issues of Biometrics Applications.* New York: Springer.

Pfitzmann, A. (2008). Biometrics - How to Put to Use and How Not at All? In S. Furnell, S. K. Katsikas, & A. Lioy (Eds.), *Trust, Privacy and Security in Digital Business, LNCS* (Vol. 5185, pp. 3-5). Springer-Verlag Berlin Heidelberg: TrustBus 2008.

Saravuth Pitiyasak (2018). *Cloud Computing Policy and Personal Data Protection in the Cloud among the European Union,* the United States, Australia and ASEAN: A Thailand Perspective. Thailand Research Fund (TRF) (in Thai).

Scharr, J. (2014). iPhone Hack Fools Touch ID with Hand Photos. *Tom's Guide.* Retrieved from https://www.tomsguide.com/us/iphone-touch-id-hack,news-20066.html

Smith, M., Mann, M., & Urbas, G. (2018). *Biometrics, Crime and Security.* New York: Routledge.

Supawat Malanon, & Chinopass Udomphol (2020). ISO 27001 Standard and Personal Data Protection Act. *Kaohoon Business Online.* Retrieved from Kaohoon Business Online News website: https://www.kaohoon.com/content/379182 (in Thai).

Thammasat University-Research and Consultancy Institute. (2015). *A complete report on the Study and Development of Personal Data Protection Guidelines under the ASEAN Community.* Retrieved from http://www.oic.go.th/FILEWEB/CABIWEBSITE/DRAWER01/GENERAL/DATA0007/00007559.PDF (in Thai).

Toli, C.-A. (2018). *Secure and Privacy-Preserving Biometric Systems.* (Doctor of Engineering Science (PhD)), Katholieke Universiteit Leuven, Retrieved from https://www.esat.kuleuven.be/cosic /publications/thesis-308.pdf