ปัญหาการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562: ความท้าทายของ SMEs ยุคดิจิทัล

Problems of Implementing the Data Privacy Protection Act, B.E. 2562 (2019): Challenge for SMEs in Digital Era

*อรรถพล หมานสนิท**
*รัฐยา ผานิชชัย**

บทคัดย่อ

ปัจจุบันนี้การใช้เทคโนโลยีในยุคดิจิทัลขององค์กรธุรกิจ SMEs อาจส่งผลกระทบในทางลบต่อเจ้าของข้อมูลส่วนบุคคลได้ โดยที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้บัญญัติขึ้นเพื่อปกป้องสิทธิที่เจ้าของข้อมูลส่วนบุคคลพึงมีความเป็นส่วนตัวที่จะไม่ถูกกระทำความเดือดร้อนรำคาญ หรือเสียหาย อีกทั้งยังคุ้มครองประโยชน์ของสาธารณชนในบริบทเศรษฐกิจโดยภาพรวมของประเทศอันเกี่ยวเนื่องมาจากผลกระทบของการละเมิดข้อมูลส่วนบุคคลด้วย อย่างไรก็ตาม การบังคับใช้กฎหมายดังกล่าวย่อมเป็นความท้าทายให้ SMEs ต้องปฏิบัติตามเงื่อนไขที่กฎหมายฉบับนี้กำหนดขึ้น และหากฝ่าฝืนย่อมได้รับบทลงโทษทั้งการชดเชยความเสียหายทางแพ่งและการชำระค่าปรับทางปกครอง ดังนั้น บทความวิจัยฉบับนี้ จึงนำบทบัญญัติแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บางมาตรามาวิเคราะห์เปรียบเทียบกับตัวอย่างการบังคับใช้กฎหมายของประเทศสหรัฐอเมริกา โดยผลการวิจัยพบว่า SMEs ควรต้องปรับตัวในการบริหารจัดการข้อมูลส่วนบุคคลของลูกค้าด้วยการกำหนดตัวบุคลากรผู้รับผิดชอบและมาตรการปกป้องและเยียวยาปัญหาที่เหมาะสม ซึ่งรวมถึงการฝึกอบรมบุคลากรของตนเพื่อส่งเสริมให้มีการปฏิบัติตามบทบัญญัติแห่งกฎหมายอย่างถูกต้อง

คำสำคัญ : การคุ้มครองข้อมูลส่วนบุคคล ความคุ้มครองทางกฎหมาย ธุรกิจขนาดกลางและขนาดย่อม (SMEs) ยุคดิจิทัล

*อาจารย์ประจำคณะบริหารธุรกิจ สถาบันการจัดการปัญญาภิวัฒน์.

Abstract

As a matter fact that the digital technology implemented by SMEs sector may cause adversely effect to individuals. As a result, the Data Privacy Protection Act, B.E. 2562 (2019) was enacted in order to prevent the privacy right of personal data subject from being violated or damaged as well as to protect public interest in term of mutual economic context that would be impacted from the personal data infringement. Nevertheless, the legal enforcement of the mentioned Act may be challenge for SMEs to apply with the condition of this law as the infringement leads to civil indemnity and administrative damages also. As a consequence, this article mentioned some section of the Data Privacy Protection Act, B.E. 2562 (2019) to be analyzed and compared with the law enforced in the United States of America to propose suggestion for SMEs to comply with the said law. A research found that SMEs should adjust the management of personal data of customer by the designation of a person who takes responsibility for data control. Furthermore, the protective measure and proper remedy as well as comprehension enhancement for staff are the essential factors to comply with data privacy protection efciently.

Keywords : data privacy, legal protection, Small and Medium Enterprises (SMEs), digital era

บทนำ

การคุ้มครองสิทธิส่วนบุคคลนั้น ได้มีการกล่าวถึงมาเป็นระยะเวลานาน ดังที่ปรากฏในปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ. 1949 (Universal Declaration of Human Rights of 1949) มาตรา 12 ซึ่งบัญญัติไว้เป็นสาระสำคัญถึงข้อห้ามการแทรกแซงโดยพลการในความเป็นส่วนตัว ครอบครัว ที่อยู่อาศัย หรือการติดต่อทางจดหมายโดยเด็ดขาด อีกทั้งยังห้ามกระทำการโจมตีเกียรติและชื่อเสียงของผู้อื่น โดยทุกคนพึงได้รับความคุ้มครองตามกฎหมายจากการแทรกแซงหรือการโจมตีดังกล่าว[1] ทั้งนี้ การให้ข้อมูลส่วนบุคคลของตนแก่องค์กรธุรกิจต่าง ๆ ผู้ให้ข้อมูลย่อมมีสิทธิในความเป็นอยู่ส่วนบุคคลอันเกี่ยวข้องกับข้อมูลส่วนบุคคลนั้น ซึ่งสิทธิในความเป็นอยู่ส่วนบุคคลในข้อมูลส่วนบุคคลจะคุ้มครองสำหรับผู้ให้ข้อมูลที่เป็นบุคคลธรรมดาเท่านั้น ไม่รวมถึงกรณีที่นิติบุคคลเป็นผู้ให้ข้อมูล แม้ว่าการให้ข้อมูลนั้นจะเป็นไปเพื่อประโยชน์

[1] Universal Declaration of Human Rights of 1949, opened for signature 10 December 1948 (entered into force 3 September 1953) Art. 12 No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

ส่วนตัวในการประกอบกิจการของตัวองค์กรนิติบุคคลนั้นเองก็ตาม เพราะนิติบุคคลโดยสภาพแล้วย่อมไม่มีสิทธิในความเป็นอยู่ส่วนบุคคลแต่อย่างใด[2]

ในช่วงระยะเวลาต่อมา เมื่อนานาประเทศทั่วโลกมีการพัฒนาระบบคอมพิวเตอร์และสร้างสรรค์นวัตกรรมดิจิทัลต่างๆ เกิดการเปลี่ยนผ่านเป็นยุคดิจิทัลขึ้น เทคโนโลยียุคดิจิทัลนี้ได้สร้างความสะดวกรวดเร็วในการเก็บรวบรวมใช้ และเปิดเผยข้อมูลส่วนบุคคล อีกทั้งยังสามารถนำเอกสารหรือข้อมูลส่วนบุคคลที่เดิมอยู่ในรูปแบบอนาล็อก ให้มาจัดเก็บไว้ในรูปแบบข้อมูลทางอิเล็กทรอนิกส์ที่สามารถเก็บไว้ได้ยาวนานและสามารถแพร่กระจายออกไปได้อย่างรวดเร็ว โดยเฉพาะอย่างยิ่งในสถานการณ์ปัจจุบันนี้ได้มีการรวบรวมข้อมูลในลักษณะเป็นฐานข้อมูล หรือมีการจัดเก็บเป็น Big Data เพื่อจะได้นำไปประมวลผลแล้ววิเคราะห์ด้วยเทคโนโลยีปัญญาประดิษฐ์ (Articial Intelligence) จึงกล่าวอีกนัยหนึ่งได้ว่ายุคดิจิทัลในปัจจุบันนี้เป็นยุคแห่งการปฏิวัติทางเทคโนโลยีโดยแท้จริง และผู้ที่สามารถเข้าถึงเทคโนโลยีเพื่อนำไปแสวงหาประโยชน์ได้มากกว่า ก็จะเป็นผู้ประกอบการธุรกิจที่มีรายได้เพิ่มมากขึ้นด้วย ซึ่ง SMEs หลายแห่งก็เป็นองค์กรธุรกิจที่ได้อาศัยเทคโนโลยีในการวิจัยและพัฒนา เพื่อให้เกิดเป็นผลิตภัณฑ์ใหม่ๆ ที่ทันสมัย และมีนวัตกรรมที่สร้างสรรค์สำหรับตอบสนองต่อความต้องการของผู้บริโภคมากยิ่งขึ้นด้วย

อย่างไรก็ตาม จากพฤติการณ์ดังกล่าวจะเห็นได้ว่าการใช้เทคโนโลยีในยุคดิจิทัลขององค์กรธุรกิจอาจส่งผลกระทบในทางลบต่อเจ้าของข้อมูลส่วนบุคคลได้ เช่น เกิดปัญหาการโจมตีที่แพร่หลายทางไซเบอร์เพื่อล่วงรู้ข้อมูลส่วนบุคคลและนำไปใช้ในการฉ้อโกงทรัพย์สิน การนำข้อมูลส่วนบุคคลของผู้อื่นไปแสวงหาประโยชน์โดยมิชอบโดยนายหน้าค้าข้อมูล การเสนอขายสินค้าหรือบริการที่รุกล้ำสิทธิความเป็นส่วนตัวของผู้บริโภค ตลอดจนการใช้เทคโนโลยีเพื่อติดตามค้นหาเจ้าของข้อมูลส่วนบุคคลโดยอาศัยการทำ Proling[3] หรือการใช้ Mac Address หรือ IP Address ฯลฯ เหล่านี้ล้วนเป็นการกระทำที่ทำให้เจ้าของข้อมูลส่วนบุคคลได้รับความเสียหายด้านทรัพย์สิน สิทธิเสรีภาพความเป็นอยู่ส่วนตัว

---

[2] ธนาชัย สุนทรอนันตชัย ปกรณ์ ปาลวงษ์พานิชและกษมา สุขนิวัฒน์ชัย “มาตรการทางกฎหมายในการเข้าถึงและการใช้ประโยชน์ จากข้อมูลข่าวสารของรัฐและการคุ้มครองปกป้อง ผู้ให้ข้อมูล” (2561) 8:2 *วารสารคณะนิติศาสตร์ มหาวิทยาลัยหัวเฉียวเฉลิมพระเกียรติ* 107, 118.

[3] “ Proling” หรือ “Behavioural Tracking” คือการติดตามพฤติกรรมของบุคคลผ่านทางอินเทอร์เน็ตโดยผู้ถูกติดตามไม่รู้ตัวและมีการสร้างทะเบียนประวัติของบุคคลนั้น ผู้ติดตามจะอาศัยข้อมูลดังกล่าวมาวิเคราะห์และประมวลผลโดยระบบอัตโนมัติให้เกิดผลลัพธ์ตามที่ตนเองต้องการ โดยมักนำไปเปรียบเทียบกับข้อมูลของบุคคลอื่น ซึ่งสถานการณ์ปัจจุบันพบว่านิยมนำมาใช้กับการเสนอโฆษณาบนอินเทอร์เน็ตเพื่อที่จะได้จัดกลุ่มผู้ต้องการบริโภคสินค้าหรือบริการ เช่น การติดตามผู้ใช้ที่เข้าชมเว็บไซต์แต่ละครั้ง หรือติดตามการเยี่ยมชมเว็บไซต์อื่นๆ ของผู้ใช้ ดัดแปลงจาก European Union Agency for Cybersecurity, *Privacy considerations of online behavioural tracking* (20 July, 2019) European Union Agency for Cybersecurity <https://www.enisa.europa.eu/publications/privacy-considerations-of-online-behavioural-tracking>.

รวมถึงบุคคลใกล้ชิดเจ้าของข้อมูลส่วนบุคคลก็อาจได้รับความเดือดร้อนเสียหายไปด้วย ซึ่งความเสี่ยงในการถูกละเมิดสิทธิในข้อมูลส่วนบุคคลก็เป็นประเด็นที่ท้าท้ายอย่างยิ่งสำหรับผู้ประกอบธุรกิจ SMEs ด้วยเหตุผลที่ความเสียหายที่อาจเกิดขึ้นจะไม่เพียงทำให้ธุรกิจหยุดชะงักหรือชะลอตัวลงไปเท่านั้น หากแต่ยังสามารถสร้างความเสียหายในระยะยาวไปถึงชื่อเสียงขององค์กรธุรกิจตลอดจนผู้บริโภคกลุ่มเป้าหมายสูญเสียความเชื่อมั่นต่อตัว SMEs ที่ไม่ได้ปฏิบัติตามกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลอีกด้วย

ดังนั้น บทความวิจัยฉบับนี้จึงมุ่งศึกษาวิเคราะห์ข้อมูลเอกสารเพื่อนำไปสู่ข้อเสนอแนวทางที่เหมาะสมสำหรับการปรับตัวของ SMEs ภายใต้บริบทยุคดิจิทัล ที่ได้มีการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยมีการนำกรณีการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นในประเทศสหรัฐอเมริกาและแนวทางการบังคับใช้กฎหมายของประเทศสหรัฐอเมริกามาเป็นตัวอย่างการศึกษาเปรียบเทียบ

วัตถุประสงค์ของการวิจัย

เพื่อศึกษาหลักและแนวคิดเกี่ยวกับในการคุ้มครองข้อมูลส่วนบุคคล โดยนำมาเป็นพื้นฐานการวิเคราะห์ไปถึงกฎหมายของประเทศไทย และตัวอย่างกฎหมายตลอดจนการบังคับใช้กฎหมายของต่างประเทศ คือประเทศสหรัฐอเมริกา เพื่อชี้ให้เห็นว่า SMEs จะได้รับอุปสรรคอย่างไรจากการบังคับใช้กฎหมายของประเทศไทยและควรมีแนวทางในการลดอุปสรรคดังกล่าวอย่างไร ภายใต้บริบทยุคดิจิทัล

วิธีดำเนินการวิจัย

บทความนี้เป็นการศึกษาวิจัยเชิงคุณภาพด้วยการวิจัยเอกสาร (Documentary Research) กล่าวคือ เป็นการศึกษาค้นคว้าและวิเคราะห์ข้อมูลจากหลักกฎหมาย บทความ งานวิจัย เอกสาร รวมถึงข้อมูลจากสื่ออิเล็กทรอนิกส์ต่าง ๆ ที่เกี่ยวข้อง

ประโยชน์ที่คาดว่าจะได้รับ

ทำให้ทราบถึงหลักและแนวคิดเกี่ยวกับการคุ้มครองข้อมูลในส่วนบุคคล เพื่อใช้เป็นพื้นฐานการวิเคราะห์ไปถึงกฎหมายของประเทศไทย และตัวอย่างกฎหมายตลอดจนการบังคับใช้กฎหมายของต่างประเทศ คือประเทศสหรัฐอเมริกา จนนำไปสู่ความรู้ความเข้าใจถึงแนวทางในการลดอุปสรรคของ SMEs ในการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ภายใต้บริบทยุคดิจิทัล

ผลการวิจัย

1. หลักและแนวคิดการให้ความคุ้มครองข้อมูลส่วนบุคคล

1.1 หลักการคุ้มครองข้อมูลส่วนบุคคลตามประกาศขององค์การสหประชาชาติ

องค์การสหประชาชาติมีการประกาศใช้ Guidelines for the Regulation of Computerized Personal Data Files (United Nations 1990) ให้

เป็นแนวปฏิบัติสำหรับประเทศสมาชิกทั้งหลายทั่วโลก ซึ่งประเทศต่าง ๆ สามารถอาศัยเป็นข้อแนะนำในการยกร่างกฎหมายภายในประเทศของตนได้ โดยมีหลักการที่สำคัญ ดังต่อไปนี้[4]

(1) หลักความชอบด้วยกฎหมายและความเป็นธรรม (Principle of lawfulness and fairness) กำหนดให้ข้อมูลซึ่งเกี่ยวกับบุคคลต้องมีการจัดเก็บรวบรวมและนำมาประมวลผลอย่างเป็นธรรม โดยวิธีการที่ชอบด้วยกฎหมาย ทั้งนี้ การนำข้อมูลไปใช้จะต้องไม่ขัดต่อวัตถุประสงค์และหลักการของกฎบัตรสหประชาชาติ

(2) หลักความถูกต้อง (Principle of accuracy) ได้กำหนดให้บุคคลซึ่งมีหน้าที่รวบรวมข้อมูลหรือมีหน้าที่เก็บข้อมูล จะต้องตรวจสอบความถูกต้องและความเกี่ยวข้องกับวัตถุประสงค์ของข้อมูลที่ได้จัดเก็บรวบรวมนั้น โดยจะต้องสร้างความมั่นใจได้ว่าข้อมูลที่ได้เก็บรวบรวมมีความสมบูรณ์เพื่อหลีกเลี่ยงความผิดพลาด และต้องสร้างความมั่นใจได้ว่าข้อมูลนั้นเป็นข้อมูลปัจจุบันเสมอ ๆ หรือตราบเท่าที่ข้อมูลนั้นยังมีการนำมาใช้ประมวลผล

(3) หลักการกำหนดวัตถุประสงค์ (Principle of the purpose-specication) กำหนดให้ต้องมีการระบุวัตถุประสงค์ในเก็บรวบรวมข้อมูลส่วนบุคคลและระบุถึงการนำข้อมูลส่วนบุคคลตามวัตถุประสงค์ดังกล่าวไปใช้งาน โดยจะต้องเป็นวัตถุประสงค์ที่ชอบด้วยกฎหมายอีกด้วย และภายหลังที่ได้ระบุวัตถุประสงค์ตลอดจนระบุถึงการนำข้อมูลส่วนบุคคลไปใช้งานแล้ว จะต้องเผยแพร่หรือแจ้งให้บุคคลที่เกี่ยวข้องได้ทราบ เพื่อให้มั่นใจได้ใน 3 กรณี คือ

ก. ข้อมูลส่วนบุคคลทั้งหมดที่ได้มีการเก็บรวบรวมและบันทึกนั้นยังคงเกี่ยวข้องและสอดคล้องตามวัตถุประสงค์ที่กำหนดไว้

ข. ข้อมูลส่วนบุคคลนั้นจะไม่มีการนำไปใช้หรือเปิดเผยเพื่อวัตถุประสงค์อื่นซึ่งขัดแย้งกับวัตถุประสงค์ที่ได้แจ้งไว้ เว้นแต่จะได้รับความยินยอมจากบุคคลที่เกี่ยวข้อง

ค. ระยะเวลาที่เก็บรวบรวมข้อมูลส่วนบุคคลต้องไม่เกินกำหนดสำหรับการดำเนินการให้บรรลุวัตถุประสงค์ที่ได้แจ้งไว้

(4) หลักการเข้าถึงของผู้มีส่วนได้เสีย (Principle of interested-person access) กำหนดให้บุคคลที่แสดงตนว่าเป็นเจ้าของข้อมูลส่วนบุคคล ย่อมมีสิทธิรับทราบว่าข้อมูลส่วนบุคคลของตนได้มีการนำไปประมวลผลหรือไม่ ซึ่งผู้เก็บรวบรวมข้อมูลส่วนบุคคลพึงแจ้งแก่เจ้าของข้อมูลส่วนบุคคลในรูปแบบที่เจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึงได้โดยไม่ชักช้าหรือมีค่าใช้จ่ายจนเกินสมควร ในกรณีนี้เจ้าของข้อมูลส่วนบุคคลย่อมมีสิทธิขอแก้ไขหรือลบข้อมูลส่วนบุคคลของตน ในกรณีที่พบว่าข้อมูลดังกล่าวไม่ถูกต้อง การเก็บรวบรวมไม่ชอบด้วยกฎหมาย หรือเกินความจำเป็น ซึ่งผู้เก็บรวบรวมข้อมูลส่วนบุคคลมีหน้าที่เสีย

[4] Ofce of the United Nations High Commissioner for Human Rights, *Guidelines for the Regulation of Computerized Personal Data Files : nal report / submitted by Louis Joinet, Special Rapporteur* (20 July, 2019) United Nations Digital Library <https://digitallibrary.un.org/record/43365>.

ค่าใช้จ่ายในการดำเนินการเช่นว่านี้ อีกทั้งให้ใช้หลักการเข้าถึงของผู้มีส่วนได้เสียนี้สำหรับทุกคนโดยไม่คำนึงถึงข้อสัญญาหรือถิ่นที่อยู่

(5) หลักการไม่เลือกปฏิบัติ (Principle of non-discrimination) กำหนดถึงข้อห้ามเก็บรวบรวมข้อมูลซึ่งอาจก่อให้เกิดการเลือกปฏิบัติโดยไม่เป็นธรรม รวมไปถึงข้อมูลเกี่ยวกับเชื้อชาติ ชาติพันธุ์ แหล่งกำเนิด สีผิว พฤติกรรมทางเพศ ความคิดเห็นทางการเมือง ศาสนา ความเชื่อทางปรัชญา หรือความเชื่ออื่นๆ ตลอดจนข้อมูลที่เกี่ยวข้องกับการเป็นสมาชิกสมาคมหรือสหภาพแรงงาน เว้นแต่ กรณีที่อยู่ภายใต้ข้อยกเว้นตามหลักการกำหนดข้อยกเว้น (Power to make exceptions)

(6) หลักการกำหนดข้อยกเว้น (Power to make exceptions) กำหนดให้ข้อยกเว้น (1) ถึง (4) ข้างต้น สามารถกำหนดได้เพียงเฉพาะในกรณีที่จำเป็นเพื่อรักษาความมั่นคงของประเทศ รักษาความสงบเรียบร้อยของประชาชน รักษาสุขอนามัยของประชาชน รักษาศีลธรรมอันดีของประชาชน หรือคุ้มครองสิทธิเสรีภาพของบุคคลอื่น ซึ่งข้อยกเว้นดังกล่าวต้องระบุไว้โดยชัดแจ้งและกำหนดการป้องกันที่เหมาะสมไว้ด้วย ตลอดจนจะต้องประกาศเป็นกฎหมายหรือกฎเกณฑ์อื่นที่เทียบเท่ากับกฎหมาย แต่กรณีข้อยกเว้น (5) อันเป็นหลักการไม่เลือกปฏิบัติสามารถกำหนดขึ้นภายใต้ข้อจำกัดแห่งปฏิญญาสากลว่าด้วยสิทธิมนุษยชนและกฎหมายอื่นที่เกี่ยวข้องในการคุ้มครองสิทธิมนุษยชนและการป้องกันการเลือกปฏิบัติโดยไม่เป็นธรรม

(7) หลักความปลอดภัย (Principle of Security) กำหนดให้ผู้เก็บรวบรวมข้อมูลส่วนบุคคลพึงจัดให้มีมาตรการป้องกันข้อมูลจากภยันตรายที่เกิดขึ้นโดยธรรมชาติ เช่น ความสูญหายโดยอุบัติเหตุ การทำลายหรือภยันตรายที่เกิดจากบุคคล เช่น การเข้าถึงโดยไม่ได้รับอนุญาต การนำข้อมูลไปใช้ในทางหลอกลวงหรือการโจมตีจากไวรัสคอมพิวเตอร์

(8) หลักการกำกับดูแลและการมีสภาพบังคับ (Supervision and sanction) กำหนดให้กฎหมายของประเทศสมาชิกพึงจัดรูปองค์กรที่ทำหน้าที่กำกับดูแลและเฝ้าระวังตามหลักการดังที่กล่าวมา หากพบว่ามีการฝ่าฝืนกฎหมายระหว่างประเทศที่มีเจตนารมณ์เพื่อใช้บังคับให้เป็นไปตามหลักการเช่นว่านี้ จะต้องมีการกำหนดมาตรการทางอาญาหรือมาตรการลงโทษอื่น และมีการชดเชยที่เหมาะสมแก่เจ้าของข้อมูลส่วนบุคคลด้วย

(9) หลักการโอนข้อมูลข้ามแดน (Transborder data flows) กำหนดให้การโอนข้อมูลข้ามแดนสามารถกระทำได้อย่างเสรี และประเทศที่มีการโอนหรือการรับโอนนั้นจะต้องมีมาตรการคุ้มครองความเป็นส่วนตัวโดยเสมอภาคกัน

(10) หลักขอบเขตการบังคับใช้ (Field of application) หลักการข้างต้นทั้งหมดที่กล่าวมาจะต้องนำมาบังคับใช้สำหรับข้อมูลทางคอมพิวเตอร์ ทั้งกรณีที่เป็นสาธารณะ กรณีเป็นส่วนตัว และข้อมูลที่จัดเก็บด้วยมือ โดยอาจกำหนดเป็นบทบัญญัติที่เฉพาะเจาะจง เพื่อขยายขอบเขตหลักการต่างๆ ให้คลอบคลุมถึงข้อมูล

เกี่ยวกับนิติบุคคล โดยเฉพาะอย่างยิ่งกรณีที่ข้อมูลเหล่านั้นมีบางส่วนซึ่งเกี่ยวข้องกับบุคคลธรรมดา

จากข้อมูลดังกล่าวจะเห็นได้ว่า แม้กฎหมายระหว่างประเทศฉบับนี้จะมีลักษณะเป็น Soft law ที่ไม่ได้มีบทลงโทษประเทศผู้ฝ่าฝืนต่อหลักเกณฑ์ แต่บรรดาประเทศสมาชิกสหประชาชาติก็จะต้องปฏิบัติตามเพื่อไม่ให้เป็นผลร้ายในทางปฏิบัติต่อความร่วมมือทางเศรษฐกิจ หรือได้รับการตอบโต้จากการฝ่าฝืนพันธกรณีใดๆ ขององค์การสหประชาชาติ ซึ่งประเทศไทยในฐานะที่เป็นสมาชิกองค์การสหประชาชาติก็ได้อาศัยหลักดังกล่าวมาอนุวัติการให้เป็นกฎหมายภายในประเทศด้วย ดังจะได้กล่าวต่อไปถึงสาระสำคัญของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1.2 แนวคิดการคุ้มครองสิทธิการโอนข้อมูลส่วนบุคคลที่อยู่ในรูปแบบอิเล็กทรอนิกส์ (Right to Data Portability)

แนวคิดการคุ้มครองสิทธิในการโอนข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์ (Right to data portability) นี้ เป็นการมุ่งให้ความคุ้มครองเกี่ยวกับสิทธิที่เจ้าของข้อมูลส่วนบุคคลสามารถโอนข้อมูลส่วนบุคคลของตนไปยังผู้ประกอบการหรือแอพพลิเคชั่นอื่นๆ ในรูปแบบที่สามารถใช้งานได้ โดยที่การโอนข้อมูลส่วนบุคคลนี้ เจ้าของข้อมูลส่วนบุคคลยังคงสามารถจัดการกับข้อมูลที่แสดงเอกลักษณ์ หรือข้อมูลอื่นๆ ของตนเองได้ ทั้งนี้ นอกจากสิทธิดังกล่าวจะคุ้มครองประโยชน์ของผู้บริโภคในการเข้าถึงข้อมูลการบริโภคของตนเองเพื่อนำมาใช้วิเคราะห์และปรับปรุงพฤติกรรมการบริโภคของตนแล้ว ยังเป็นการช่วยให้ผู้บริโภคสามารถควบคุมข้อมูลส่วนบุคคลของตนหรือขอให้ผู้ประกอบการโอนข้อมูลนั้นไปยังผู้ประกอบการหรือผู้ให้บริการรายอื่น ซึ่งนับได้ว่าเป็นการแข่งขันทางการค้าที่เป็นธรรม เพราะสามารถช่วยสนับสนุนให้ผู้ประกอบการรายอื่นๆ นำข้อมูลไปใช้พัฒนาสินค้าหรือบริการของตน จนทำให้ผู้บริโภคได้ใช้สินค้าหรือบริการที่มีราคาไม่สูงเกินสมควรอีกด้วย[5]

อย่างไรก็ตาม แนวคิดนี้มีประเด็นปัญหาอันเนื่องมาจากการที่ผู้ประกอบการสามารถเก็บข้อมูลส่วนบุคคลโดยอาศัยรูปแบบทางอิเล็กทรอนิกส์ที่แตกต่างกันไป ส่งผลให้ข้อมูลในรูปแบบดังกล่าวไม่สามารถนำไปใช้กับ ผู้ประกอบการรายอื่นได้ และการกำหนดรูปแบบการเก็บข้อมูลที่แตกต่างกันนี้ ย่อมสร้างภาระความลำบากให้แก่ผู้ประกอบการในธุรกิจขนาดกลางและขนาดย่อม (Small and medium-sized enterprises SMEs) เพราะ SMEs อาจยังไม่มีทรัพยากรมนุษย์ เทคโนโลยี และเงินทุนที่หมาะสมเพียงพอในการพัฒนาโปรแกรมการจัดเก็บข้อมูลส่วนบุคคลดังเช่นบริษัทขนาดใหญ่ จนกระทั่ง SMEs อาจจำต้องออกจากการเป็นผู้แข่งขันในตลาดสินค้าหรือบริการดังเช่นว่านั้นไป[6]

---

[5] Peter Swire and Yianni Lagos "Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique" (2013) 72:2 *Maryland Law Review* 335, 336-337.

[6] Ibid, 352-353.

จากหลักและแนวคิดการให้ความคุ้มครองข้อมูลส่วนบุคคลดังกล่าวจะเห็นได้ว่า SMEs ต้องเผชิญกับความท้าทายในการจัดระบบการเก็บรวบรวมข้อมูลส่วนบุคคล เพื่อที่จะได้นำข้อมูลเหล่านั้นไปวิเคราะห์หรือสร้างมูลค่าเพิ่มทางเศรษฐกิจให้แก่องค์กรธุรกิจของตนได้อย่างสะดวกรวดเร็ว โดยที่การบริหารจัดการระบบเก็บข้อมูลส่วนบุคคลที่สอดคล้องตามหลักสากลดังที่ปรากฏในประกาศขององค์การสหประชาชาติย่อมช่วยลดต้นทุนและความเสี่ยงอันเกิดจากการละเมิดข้อมูลส่วนบุคคลอีกด้วย

2. สาระสำคัญของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2.1 เหตุผลในการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ในส่วนหมายเหตุท้ายพระราชบัญญัติฉบับนี้ได้ระบุไว้ว่า “เนื่องจากปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญ หรือความเสียหาย ให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวก และรวดเร็ว ก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวม สมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้น เพื่อกำหนดหลักเกณฑ์กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป”

จากหมายเหตุท้ายพระราชบัญญัติดังที่กล่าวมา จะเห็นได้ว่าเหตุผลของประเทศไทยในการคุ้มครองข้อมูลส่วนบุคคลนั้น ก็เพื่อที่จะให้เกิดความตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลในยุคดิจิทัลที่ข้อมูลส่วนบุคคลสามารถเกิดการแพร่กระจายออกไปอย่างกว้างขวางและรวดเร็วภายใต้บริบทการสื่อสารผ่านระบบอินเทอร์เน็ต โดยที่ได้เน้นถึงสิทธิที่เจ้าของข้อมูลส่วนบุคคลพึงมีความเป็นส่วนตัวที่จะไม่ถูกกระทำความเดือดร้อน รำคาญ หรือเสียหาย อีกทั้งยังให้มุมมองไปถึงประโยชน์สาธารณชนที่จะพึงได้รับจากการปกป้องคุ้มครองมิให้ได้รับความเสียหายทางเศรษฐกิจโดยรวมของประเทศอันเกี่ยวเนื่องมาจากการละเมิดข้อมูลส่วนบุคคลด้วย

2.2 สาระสำคัญเกี่ยวกับหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล

ในมาตรา 5 แห่งพระราชบัญญัติดังกล่าวได้กำหนดนิยามคำว่า “ผู้ควบคุมข้อมูลส่วนบุคคล” ไว้ให้หมายความถึงบุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ซึ่งจากหลักเกณฑ์ดังกล่าวข้างต้นจะเห็นได้ว่า SMEs หลายแห่งมักทำธุรกิจออนไลน์ที่ทำให้ SMEs นั้นเป็นผู้ควบคุมข้อมูลส่วนบุคคลตามความหมายแห่งพระราชบัญญัตินี้ เช่น กรณีการทำธุรกิจนั้นได้มีการรับข้อมูลส่วนบุคคลของลูกค้ามาเพื่อจะได้วิเคราะห์ข้อมูลแล้วเจรจาต่อรองก่อนจัดส่งสินค้าหรือให้บริการให้ตรงกับความต้องการของลูกค้า การทำธุรกิจด้านสุขภาพที่มีการรวบรวมข้อมูลสุขภาพกายหรือจิตใจของลูกค้า ฯลฯ

สำหรับมาตรา 25 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้น ได้บัญญัติไว้เป็นสาระสำคัญมิให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่

(1) ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า แต่ต้องไม่เกินสามสิบวันนับแต่วันที่เก็บรวบรวมและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือ

(2) เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26 ซึ่งเป็นประเด็นเกี่ยวกับกรณีข้อยกเว้นการให้ความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล

เมื่อพิจารณาหลักเกณฑ์ตามมาตรา 25 ข้างต้นจะเห็นได้ว่าหลักกฎหมายดังกล่าวมีเจตนารมณ์ที่สอดคล้องกับแนวคิดการคุ้มครองสิทธิการโอนข้อมูลส่วนบุคคลที่อยู่ในรูปแบบอิเล็กทรอนิกส์ดังที่ได้กล่าวมาแล้วในหัวข้อ 2.2 เพราะการบังคับให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ในทางงดเว้นในอันที่จะต้องไม่ดำเนินการรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรงนั้น หากตีความในทางตรงกันข้ามก็เท่ากับว่าเป็นการรับรองสิทธิของเจ้าของข้อมูลส่วนบุคคลที่จะสามารถโอนข้อมูลส่วนบุคคลของตนไปยังผู้ประกอบการหรือแอพพลิเคชั่นอื่น ๆ โดยที่เจ้าของข้อมูลส่วนบุคคลยังคงสามารถจัดการกับข้อมูลที่แสดงเอกลักษณ์ หรือข้อมูลอื่น ๆ ของตนเองไปพร้อมกันได้ด้วย และ SMEs ในฐานะที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลก็จำเป็นจะต้องบริหารจัดการเพื่อขออนุญาตเจ้าของข้อมูลส่วนบุคคลเพื่อที่จะเข้าถึงและใช้ประโยชน์จากข้อมูลส่วนบุคคลดังกล่าวด้วย ซึ่งแม้ว่าการบริหารจัดการดังกล่าวจะเป็นการเพิ่มต้นทุนให้กับ SMEs แต่ผู้วิจัยก็เห็นว่ามีความคุ้มค่ากว่าการต้องเสียค่าใช้จ่ายในการแก้ไขปัญหาต่าง ๆ ภายหลังที่ SMEs ได้กระทำการอันฝ่าฝืนต่อกฎหมายไปแล้ว

ส่วนมาตราที่บัญญัติไว้โดยสอดคล้องอย่างมีนัยสำคัญกับ Guidelines for the Regulation of Computerized Personal Data Files (United Nations 1990) ที่ได้กล่าวมาแล้วในหัวข้อ 2.1 คือมาตรา 37 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นี้ ได้บัญญัติไว้เป็นสาระสำคัญถึงหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล คือ

(1) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด

(2) ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

(3) จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนด ระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น การเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา 24 (1) หรือ (4) หรือมาตรา 26 (5) (ก) หรือ (ข) การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย

(4) แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

เมื่อพิจารณาประกอบกับมาตรา 37 ข้างต้น อาจมองได้ว่ากฎหมายฉบับนี้เพิ่มภาระในการบริหารจัดการและค่าใช้จ่ายในการประกอบธุรกิจให้กับ SMEs มากขึ้น และหาก SMEs ไม่ปฏิบัติตามกฎหมายเช่นว่านี้ก็จะต้องชดใช้ค่าเสียหายทางแพ่งตามมาตรา 77 ซึ่งได้บัญญัติไว้เป็นสาระสำคัญให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งดำเนินการใดๆ เกี่ยวกับข้อมูลส่วนบุคคลอันเป็นการฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติแห่งพระราชบัญญัตินี้ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้นแก่เจ้าของข้อมูลส่วนบุคคล ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่ก็ตาม อันแสดงให้เห็นว่าเป็นความรับผิดโดยเคร่งครัด (strict liability) จะอ้างข้อยกเว้นเพื่อไม่ต้องรับผิดได้เพียงกรณีเหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั้นเอง หรือเป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามหน้าที่และอำนาจตามกฎหมาย ได้เท่านั้น นอกจากนี้ ยังมีโทษปรับทางปกครองตามมาตรา 83 อีกไม่เกิน 3 ล้านบาท ซึ่งผู้วิจัยเห็นว่าเป็นอัตราโทษที่ค่อนข้างสูงสำหรับ SMEs รายที่มีสินทรัพย์จำนวนไม่มากนัก อย่างไรก็ตาม อีกแง่มุมหนึ่ง ผู้วิจัยเห็นว่าหาก SMEs สามารถปฏิบัติตามหลักกฎหมายดังกล่าวได้ครบถ้วน SMEs ผู้ควบคุมข้อมูลส่วนบุคคลรายนั้น ก็จะได้รับความคุ้มครองไม่ต้องรับผิดทางแพ่งเกี่ยวกับการละเมิดข้อมูลส่วนบุคคล เพราะสามารถอ้างได้ว่ามิได้จงใจหรือประมาทเลินเล่อกระทำให้ผู้อื่นเสียหาย และไม่จำต้องได้รับโทษปรับทางปกครองด้วยเหตุผลเช่นเดียวกันนี้ด้วย

2.3 ระยะเวลาในการปรับตัวของ SMEs เพื่อปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ตามมาตรา 2 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้บัญญัติไว้เป็นสาระสำคัญให้พระราชบัญญัตินี้มีผลใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษา เป็นต้นไป (วันที่เริ่มมีผลใช้บังคับคือวันที่ 28 พฤษภาคม 2562) เว้นแต่บทบัญญัติในหมวด 2 หมวด 3 หมวด 5 หมวด 6 หมวด 7 และความในมาตรา 95 และมาตรา 96 ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษา เป็นต้นไป

โดยที่มาตรา 96 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้บัญญัติไว้เป็นสาระสำคัญให้การดำเนินการออกระเบียบและประกาศตามพระราชบัญญัตินี้ ให้ดำเนินการให้แล้วเสร็จภายในหนึ่งปีนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ ซึ่งสามารถตีความได้ว่ากรณีที่กฎหมายฉบับนี้กำหนดให้ต้องออกกฎหมายลำดับรองมารองรับวิธีการปฏิบัติต่างๆ หน่วยงานของรัฐผู้รับผิดชอบสามารถดำเนินการให้แล้วเสร็จได้ภายในหนึ่งปีหลังจากพระราชบัญญัติฉบับนี้มีผลใช้บังคับ และผู้วิจัยเห็นว่าระยะเวลาในการออกกฎหมายลำดับรองนี้ คือระยะเวลาที่ SMEs จะต้องเร่งปรับตัวให้สามารถบริหารจัดการองค์กรธุรกิจของตนให้เป็นไปตามหลักเกณฑ์แห่งพระราชบัญญัติฉบับนี้ หาก SMEs สามารถปรับตัวได้ไวก็ย่อมจะเป็นผลดีในการลดความเสี่ยงที่จะกระทำผิดกฎหมาย

3. ตัวอย่างกฎหมายและการบังคับใช้กฎหมายการคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกา

แม้ว่าในปัจจุบันนี้ประเทศสหรัฐอเมริกาจะยังไม่มีการตรากฎหมายที่มุ่งคุ้มครองข้อมูลส่วนบุคคลเป็นกฎหมายกลางที่ใช้บังคับเป็นการทั่วไป แต่อย่างไรก็ตาม ประเทศสหรัฐอเมริกาได้มีการตรากฎหมายเฉพาะซึ่งเกี่ยวข้องโดยตรงกับการคุ้มครองข้อมูลส่วนบุคคล เพื่อใช้บังคับสำหรับองค์กรหรือหน่วยงานบางหน่วยงานเท่านั้น เช่น Health Insurance Portability and Accountability Act of 1996 (HIPAA หรือที่มีการเรียกเป็นอีกชื่อหนึ่งว่า Kennedy-Kassebaum Health Insurance Portability and Accountability Act) ซึ่งเป็นกฎหมายที่กำหนดหลักเกณฑ์ให้ความคุ้มครองความเป็นส่วนตัวและความปลอดภัยในข้อมูลด้านสุขภาพ และนำมาบังคับใช้สำหรับองค์กรหรือหน่วยงานด้านสุขภาพเท่านั้น ส่วน The Financial Services Modernization Act of 1999 (Gramm-Leach-Billey Actหรือ GLB) เป็นกฎหมายที่มุ่งคุ้มครองความปลอดภัยและความเป็นส่วนตัวในข้อมูลทางการเงินส่วนบุคคล และใช้บังคับสำหรับสถาบันการเงินเท่านั้น อีกทั้งยังมีแนวปฏิบัติในการกำกับดูแลตนเอง (Self-regulatory guidelines) และได้วางกรอบการกำกับดูแลตนเอง (Self-regulatory framework) เพื่อใช้บังคับภายในหน่วยงานหรือองค์กร[7]

[7] อธิพร สิทธิธีรรัตน์, *ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลในบริบทอิเล็กทรอนิกส์* (นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2558) 57-58.

นอกจากนี้ ประเทศสหรัฐอเมริกายังจัดตั้งองค์กร Federal Trade Commission (FTC) ซึ่งทำหน้าที่หลักในสองประเด็น คือ ประเด็นการคุ้มครองผู้บริโภค และประเด็นการส่งเสริมการแข่งขันทางการค้า โดยในส่วนการคุ้มครองผู้บริโภคนั้น FTC จะดำเนินมาตรการเพื่อให้หยุดการกระทำอันเป็นการเอารัดเอาเปรียบ ฉ้อโกง หรือหลอกลวงในตลาดการค้า และมีหน้าที่สืบสวนสอบสวนดำเนินคดีต่อบริษัทตลอดจนบุคคลธรรมดาที่กระทำละเมิดต่อกฎหมาย เพื่อป้องกันมิให้เกิดการละเมิดความเป็นส่วนตัวของผู้บริโภค โดยเฉพาะอย่างยิ่งในกรณีที่ผู้ประกอบธุรกิจกระทำการให้ข้อมูลอันเป็นการหลอกลวงหรือไม่เป็นธรรมแก่ผู้บริโภค กล่าวอีกนัยหนึ่งได้ว่า FTC เป็นองค์กรหลักผู้มีอำนาจใช้บังคับกฎหมายด้วยวิธีการตีความคำมั่นที่ผู้ประกอบการได้เคยให้ไว้แก่ผู้บริโภค แต่กลับมิได้ปฏิบัติตาม เพราะได้กระทำการอันไม่เป็นธรรมและหลอกลวงทางการค้า (Unfair and Deceptive Act) ตามมาตรา 5 แห่ง Federal Trade Commission Act (FTC Act)[8] ดังนั้น ผู้ประกอบการที่ใช้หรือมีข้อมูลส่วนบุคคลของผู้บริโภคไว้ในความครองครอง จึงมีหน้าที่และความรับผิดชอบในการให้ข้อมูลที่เพียงพอแก่ผู้บริโภคเกี่ยวกับเรื่องความปลอดภัยและความเป็นส่วนตัวในการใช้สินค้าหรือรับบริการตลอดจนต้องมีการดำเนินการบังคับใช้มาตรการคุ้มครองความปลอดภัยอย่างเพียงพอภายในองค์กร เพื่อป้องกันข้อมูลผู้บริโภคมิให้ถูกขโมยไปโดยแฮกเกอร์ หรือมิให้มีกรณีการรั่วไหลของข้อมูลหรือเกิดการใช้งานที่ผิดไปจากวัตถุประสงค์ภายในองค์กรนั้นๆ เอง[9]

สำหรับกรณีตัวอย่างที่น่าสนใจอย่างยิ่งเกี่ยวกับการบังคับใช้มาตรา 5 แห่ง FTC Act ดังกล่าว คือกรณีผู้ถูกกล่าวหาคือบริษัทเทรนด์เนต[10] ซึ่งเป็นเหตุการณ์ที่เกิดขึ้นระหว่างปี ค.ศ. 2012 โดยมีข้อเท็จจริงปรากฏว่าภาพจากกล้องวีดีโอรักษาความปลอดภัยได้มีการเผยแพร่สู่สาธารณชนทางอินเทอร์เน็ต ซึ่งเทรนด์เนตเป็นผู้กระทำการจำหน่ายสินค้ากล้องรักษาความปลอดภัย เพื่อวัตถุประสงค์การใช้งานทั้งภายในครัวเรือน และในสถานที่ทำงานของบริษัทผู้บริโภค กล้องดังกล่าวจะถ่ายทอดภาพวีดีโอและเสียงเพื่อส่งตรงไปให้ผู้ใช้งานได้รับชมภาพและเสียงถ่ายทอดสดทางอินเทอร์เน็ต ต่อมามีผู้บุกรุกโดยอาศัยข้อบกพร่องอันเกิดจากการตั้งค่าการทำงานของซอฟต์แวร์ที่ผิดพลาดของบริษัท จนทำให้ผู้บุกรุกนั้นสามารถค้นเจอที่อยู่ทางอินเทอร์เน็ตของผู้ใช้งานกล้องนี้ได้จากเว็บไซต์ของบริษัท แม้ว่าผู้ใช้งานจะตั้งค่าไม่ให้เผยแพร่ข้อมูลจากกล้องสู่สาธารณะแล้วก็ตาม แต่ผู้บุกรุกก็ยังสามารถเข้าถึงข้อมูลภาพ และเสียง

---

[8] Section 5, *Federal Trade Commission Act 1938*.

[9] อธิพร สิทธิธีรรัตน์, อ้างแล้ว 9, 58.

[10] In the Matter of TRENDnet, Inc. (FTC 2014) อ้างใน วิสาขา ภู่สำรวจ "การคุ้มครองข้อมูลส่วนบุคคล จากมุมมองกฎหมายคุ้มครองผู้บริโภค: กรณีศึกษาจาก Federal Trade Commission สหรัฐอเมริกาและข้อพิจารณาสำหรับไทย" ใน อาร์ม ตั้งนิรันดรวรพล มาลสุขุม และพีรพงศ์ จงไพศาลสกุล, *กฎหมายกับเศรษฐกิจ รวมบทความทางวิชาการเพื่อเป็นเกียรติแด่ ศาสตราจารย์ ดร.ศักดา ธนิตกุล ครูของ พ ศักดา 60 ปี* (กรุงเทพฯ: โรงพิมพ์เดือนตุลา, 2561) 443, 456-458.

ที่ถ่ายทอดสดออนไลน์จากกล้องของผู้ใช้งานได้จำนวนมากกว่าร้อยเครื่อง และได้โพสต์ข้อความเกี่ยวกับการรั่วไหลของข้อมูลจากเทรนด์เนตดังกล่าวบนอินเทอร์เน็ต ตลอดจนแชร์ลิงค์สำหรับชมภาพวิดีโอจากกล้องของผู้ใช้งานมากกว่าเจ็ดร้อยเครื่องแบบออนไลน์ ซึ่งภาพและเสียงจากกล้องดังกล่าวแสดงข้อมูลเกี่ยวกับพื้นที่ส่วนตัวภายในบ้าน และการใช้ชีวิตประจำวันของผู้ใช้งานที่มีเด็กเล็กอยู่ด้วย อีกทั้งรหัสไอพีแอดเดรสยังแสดงถึงที่ตั้ง เมืองและรัฐ ที่อยู่อาศัยของผู้ใช้งาน อันเป็นข้อมูลที่มีความอ่อนไหวเพราะก่อให้เกิดความเสี่ยงภัยต่อชีวิตและทรัพย์สินของผู้บริโภคด้วย[11]

กรณีนี้สรุปสาระสำคัญได้ว่า FTC มีความเห็นว่า ตั้งแต่ช่วงปี 2010 จนถึงวันที่เกิดเหตุการณ์ดังกล่าว บริษัทเทรนด์เนตได้มีการรับรองโดยชัดแจ้งหรือปริยายว่าบริษัทได้ดำเนินการอย่างเพียงพอและเหมาะสมเพื่อให้ผู้บริโภคแน่ใจได้ว่ากล้องและแอพพลิเคชั่นทางโทรศัพท์เคลื่อนที่นั้นมีความปลอดภัยสำหรับข้อมูลเกี่ยวกับพื้นที่ส่วนตัวของผู้บริโภคทั้งในบ้านและสถานที่ทำงาน โดยพิจารณาได้จากชื่อทางการค้าว่า "Secur-View" คำบรรยายสินค้าบนกล่องบรรจุภัณฑ์ เว็บไซต์ โฆษณา และแอพพลิเคชั่นทางโทรศัพท์เคลื่อนที่ ตลอดจนสติกเกอร์รูปกุญแจล็อคและข้อความที่ระบุว่าสินค้ามีความปลอดภัยและสามารถคุ้มครองความปลอดภัยแก่ผู้ที่อยู่อาศัยและครอบครัว ทรัพย์สิน หรือธุรกิจของผู้ใช้งาน แต่จากข้อเท็จจริงที่เกิดขึ้นแสดงให้เห็นได้ว่าคำรับรองดังกล่าวไม่เป็นความจริง และทำให้ผู้บริโภคเกิดความเข้าใจผิด เพราะในทางปฏิบัติเทรนด์เนตปล่อยให้มีการส่งและเก็บรักษารหัสผ่านของผู้ใช้งานในรูปแบบข้อความที่อ่านได้ บนอินเทอร์เน็ตและอุปกรณ์มือถือของผู้ใช้งาน ทั้งที่สามารถใช้ซอฟต์แวร์ฟรีซึ่งมีอยู่อย่างแพร่หลายเพื่อป้องกันกรณีดังกล่าวได้อยู่แล้ว แต่กลับไม่ได้ดำเนินการ นอกจากนี้ เทรนด์เนตยังไม่มีขั้นตอนการติดตามรายงานข้อบกพร่องเกี่ยวกับความปลอดภัยที่ได้รับจากผู้ทำวิจัย นักวิชาการ หรือสาธารณชน ทั้งที่สามารถกระทำได้โดยปราศจากค่าใช้จ่าย รวมถึงมีการบริหารจัดการเพื่อแก้ไขข้อบกพร่องดังกล่าวล่าช้าจนเกินสมควร โดยบริษัทไม่ได้มีการทดสอบซอฟต์แวร์อย่างเพียงพอ ไม่มีการทบทวนระบบรักษาความปลอดภัย หรือการทำงานในส่วนสำคัญก่อนที่จะปล่อยสินค้าออกสู่ตลาด ไม่มีการทดลองเจาะเข้าระบบและเขียนโปรแกรม เพื่อทำให้แน่ใจว่ามีการจำกัดการเข้าถึงข้อมูลตามที่บริษัทได้รับรองไว้ นอกจากนี้ บริษัทยังไม่ได้ให้คำแนะนำอย่างเพียงพอหรือมีการจัดอบรมพนักงานเกี่ยวกับความรับผิดชอบในการทดสอบการออกแบบและความปลอดภัยของกล้องและซอฟต์แวร์ที่เกี่ยวข้อง การกระทำดังกล่าวจึงเป็นการปฏิบัติที่ไม่เป็นธรรมซึ่งขัดต่อบทบัญญัติมาตรา 5 ของ FTC Act[12]

[11] เพิ่งอ้าง
[12] เพิ่งอ้าง

ในท้ายที่สุดได้มีข้อตกลงยุติข้อพิพาทที่ FTC ทำขึ้นกับบริษัทเทรนด์เนต ซึ่งข้อตกลงดังกล่าวชี้ให้เห็นถึงความจำเป็นต้องมีมาตรการรักษาความปลอดภัยและความเป็นส่วนตัวของข้อมูลจากวิธีการและเครื่องมือที่มีอยู่อย่างแพร่หลายในการป้องกันภัยและค่าใช้จ่ายที่เกิดขึ้นจากการจัดหามาตรการนั้น เพื่อคุ้มครองข้อมูลส่วนตัวของผู้บริโภค โดยที่มาตรการป้องกันเช่นว่าจะต้องเพียงพอและเหมาะสม ซึ่งต้องอาศัยปัจจัยระดับความอ่อนไหวของข้อมูล ปริมาณข้อมูลที่อยู่ในความครอบครอง ขนาดหรือความซับซ้อนของสภาพธุรกิจ ตลอดจนค่าใช้จ่ายเพื่อจัดหาเครื่องมือในการปรับปรุงระบบรักษาความปลอดภัยและความเสี่ยงภัยที่เกี่ยวข้องกับข้อมูลผู้บริโภค ครอบคลุมทั้งมาตรการเชิงบริหาร มาตรการเชิงเทคนิค หรือมาตรการทางกายภาพ ทั้งนี้ จะกระทำได้โดยจัดให้มีโปรแกรมเกี่ยวกับความเป็นส่วนตัวและความปลอดภัยของข้อมูลที่ใช้ในองค์กร ซึ่งอย่างน้อยต้องประกอบไปด้วย 1) มาตรการแต่งตั้งเจ้าหน้าที่ดูแลความเป็นส่วนตัวของข้อมูลซึ่งเป็นพนักงานองค์กร เพื่อทำหน้าที่ดูแลการปฏิบัติตามหรือประสานงานในโปรแกรมความเป็นส่วนตัวและความปลอดภัยของข้อมูล 2) มาตรการที่สามารถระบุ ประเมิน หรือควบคุมความเสี่ยงซึ่งหมายความรวมถึงการดำเนินการฝึกอบรมพนักงานเรื่องความเป็นส่วนตัวและความปลอดภัยของข้อมูล การตรวจสอบและทดสอบมาตรการรักษาความปลอดภัยของข้อมูลที่มีอยู่อย่างสม่ำเสมอและปรับปรุง เมื่อถึงคราวจำเป็น กระบวนการคัดกรองผู้ให้บริการที่เหมาะสม และข้อจำกัดการเข้าถึงข้อมูลส่วนบุคคลและเข้าทำสัญญากับผู้ให้บริการดังกล่าว เพื่อให้มั่นใจได้ว่าองค์กรมีการใช้มาตรการป้องกันที่เหมาะสมในการปฏิบัติต่อข้อมูลส่วนบุคคล[13]

4. การศึกษาเปรียบเทียบหลักเกณฑ์ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กับกรณีศึกษาของประเทศสหรัฐอเมริกา

เนื่องจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นี้ เพิ่งมีผลใช้บังคับเมื่อวันที่ 28 พฤษภาคม 2562

จากหลักเกณฑ์ตามมาตรา 37 แห่งพระ-ราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของประเทศไทย เมื่อเปรียบเทียบกับผลการใช้บังคับกฎหมายของประเทศสหรัฐอเมริกากรณีเทรนด์เนต จะเห็นได้ว่า สาระสำคัญมีความสอดคล้องไปในทิศทางเดียวกันสำหรับการกำหนดหน้าที่ให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องมีมาตรการรักษาความปลอดภัยและความเป็นส่วนตัวของข้อมูล เพื่อคุ้มครองข้อมูลส่วนตัวของผู้บริโภค โดยที่มาตรการป้องกันเช่นว่าจะต้องเพียงพอและเหมาะสมด้วย ซึ่งแนวทางการบังคับใช้กฎหมายของประเทศสหรัฐอเมริกานั้น ได้ขยายความรายละเอียดเกี่ยวกับความเหมาะสมของมาตรการโดยให้คำนึงถึงปัจจัยระดับความอ่อนไหวของข้อมูล ปริมาณข้อมูลที่อยู่ในความครอบครอง ขนาดหรือความซับซ้อนของสภาพธุรกิจ ตลอดจนค่าใช้จ่ายเพื่อจัดหาเครื่องมือในการปรับปรุงระบบ

[13] เพิ่งอ้าง

รักษาความปลอดภัยและความเสี่ยงภัยที่เกี่ยวข้องกับข้อมูลผู้บริโภค ครอบคลุมทั้งมาตรการเชิงบริหาร มาตรการเชิงเทคนิค หรือมาตรการทางกายภาพ เหล่านี้ย่อมเป็นสิ่งที่ SMEs ของประเทศไทยพึงนำมาใช้พิจารณาเพื่อจัดเตรียมมาตรการคุ้มครองข้อมูลส่วนบุคคลด้วย

นอกจากนี้ จากส่วนที่สำคัญประเด็นหนึ่งในความเห็นของ FTC เกี่ยวกับข้อผิดพลาดของบริษัทเทรนด์เนต คือ การไม่ได้ให้คำแนะนำอย่างเพียงพอหรือมีการจัดอบรมพนักงานเกี่ยวกับความรับผิดชอบในการทดสอบการออกแบบและความปลอดภัยของกล้องและซอฟต์แวร์ที่เกี่ยวข้อง ถ้อยความดังกล่าวชี้ให้เห็นได้ว่าองค์กรผู้ใช้บังคับกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกาตระหนักถึงความสำคัญของการเผยแพร่ความรู้ในส่วนที่เกี่ยวข้องกับการปกป้องการรั่วไหลของข้อมูลส่วนบุคคลภายใต้บริบทยุคดิจิทัลที่ข้อมูลข่าวสารมีการแพร่กระจายได้อย่างกว้างขวางและรวดเร็วมาก ซึ่งเมื่อพิจารณาตามกฎหมายของประเทศไทยแล้ว จะเห็นได้ว่าแม้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะไม่ได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลที่เป็นเอกชนแต่ละรายมีหน้าที่ต้องจัดให้มีการฝึกอบรมเกี่ยวกับระบบการรักษาความปลอดภัยสำหรับข้อมูลส่วนบุคคล แต่ก็มีความจำเป็นที่ SMEs ของประเทศไทยพึงต้องคำนึงถึงวิธีการดังกล่าวด้วย เพื่อประโยชน์ในการปฏิบัติตามหลักเกณฑ์แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นี้ด้วย

บทสรุปและข้อเสนอแนะ

จากที่ผู้วิจัยได้ศึกษาถึงหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กับกรณีศึกษาของประเทศสหรัฐอเมริกา นั้น จะเห็นได้ว่า SMEs ของประเทศไทยขณะนี้ต้องเผชิญหน้ากับความท้าทายในการที่ควรเร่งพิจารณาว่าภายในองค์กรของตนมีระบบและกลไกการจัดการข้อมูลส่วนบุคคลอย่างไรบ้าง บุคลากรของ SMEs เองที่สามารถเข้าถึงข้อมูลควรเป็นผู้ใดได้บ้าง และจะต้องคำนึงถึงกรณีพันธมิตรองค์กรธุรกิจที่อาจมีการแลกเปลี่ยนหรือส่งผ่านข้อมูลส่วนบุคคลให้แก่กันด้วย มีการจัดระบบการควบคุมข้อมูลอย่างไร รวมถึงถ้าเกิดสถานการณ์อันไม่ปกติต่าง ๆ ขึ้นเกี่ยวกับการรั่วไหลของข้อมูลส่วนบุคคล SMEs จะมีแผนการรับมืออย่างไร จะแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบอย่างไร ซึ่งจำเป็นต้องอาศัยเทคนิควิธีการด้านการสื่อสารทั้งภายในและภายนอกองค์กรด้วยเป็นสำคัญ และจะบริหารจัดการเพื่อเยียวยาความเสียหายของผู้ถูกละเมิดข้อมูลส่วนบุคคลตลอดจนความเสียหายขององค์กรธุรกิจตนได้อย่างไร

นอกจากนี้ จากแนวทางการบังคับใช้กฎหมายของประเทศสหรัฐอเมริกาจะเห็นได้ว่าการให้ความสำคัญกับการฝึกอบรมให้ความรู้บุคลากรขององค์กรธุรกิจเป็นสิ่งที่พึงกระทำอย่างยิ่ง ซึ่งผู้วิจัยเห็นว่าควรต้องอาศัยรูปแบบและวิธีการถ่ายทอดความรู้ประกอบกับประสบการณ์ที่น่าสนใจและสามารถทำความเข้าใจได้ง่าย เพราะ SMEs อาจประกอบไปด้วยบุคลากรที่มีจำนวน

ไม่มากนัก และอาจมีผู้เชี่ยวชาญด้านเทคโนโลยีที่เป็นบุคลากรขององค์กรเองในจำนวนจำกัด อีกทั้งการพัฒนาปรับปรุงระบบเทคโนโลยีสาระสนเทศของ SMEs ให้สอดคล้องกับสถานการณ์ปัจจุบันอยู่เสมอก็จะช่วยลดปัญหาการรั่วไหลของข้อมูลส่วนบุคคลได้ ซึ่งเมื่อมีการพัฒนาปรับปรุงระบบคราวใด SMEs ก็พึงต้องจัดอบรมให้ความรู้และข้อมูลที่จำเป็นแก่บุคลากรของ SMEs ในคราวนั้น อย่างไรก็ตาม ในส่วนบทลงโทษการฝ่าฝืนมาตรา 37 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับกรณี SMEs เป็นผู้กระทำความผิดนั้น ผู้วิจัยมีข้อเสนอแนะเพิ่มเติมถึงการตีความบทลงโทษปรับทางปกครองไม่เกิน 3 ล้านบาท ว่า การกำหนดอัตราโทษอย่างสูงดังกล่าว กระบวนการยุติธรรมพึงต้องพิจารณาถึงบริบทการดำเนินธุรกิจของ SMEs ด้วยว่าเป็นองค์กรธุรกิจที่อาจมีทุนทรัพย์น้อยหรือมีขีดความสามารถในการแข่งขันน้อยเมื่อเปรียบเทียบกับความได้เปรียบทางเทคโนโลยีขององค์กรธุรกิจขนาดใหญ่ และเมื่อชั่งน้ำหนักความร้ายแรงแห่งการกระทำผิดของ SMEs กับผลเสียหายที่เกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคลแล้ว SMEs สมควรชำระค่าปรับมากน้อยเพียงใด โดยมองว่าวัตถุประสงค์ของการลงโทษนี้เป็นการมุ่งฟื้นฟูแก้ไขให้ SMEs ปรับปรุงตนเองมิให้กระทำผิดกฎหมาย เพราะ SMEs เป็นประเภทองค์กรธุรกิจที่มีจำนวนมากถึงกว่าร้อยละ 90 ขององค์กรธุรกิจทั้งหมดในประเทศไทย และเป็นกำลังสำคัญยิ่งในการขับเคลื่อนเศรษฐกิจและพัฒนาสังคมของประเทศไทยในปัจจุบันด้วย

บรรณานุกรม

ธนาชัย สุนทรอนันตชัย ปกรณ์ ปาลวงษ์พานิชและกษมา สุขนิวัฒน์ชัย “มาตรการทางกฎหมายในการเข้าถึงและการใช้ประโยชน์ จากข้อมูลข่าวสารของรัฐและการคุ้มครองปกป้อง ผู้ให้ข้อมูล” (2561) 8: 2 *วารสารคณะนิติศาสตร์ มหาวิทยาลัยหัวเฉียวเฉลิมพระเกียรติ.*

อธิพร สิทธิธีรรัตน์, *ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลในบริบทอิเล็กทรอนิกส์* (นิติศาสตรมหาบัณฑิตคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2558).

อาร์ม ตั้งนิรันดร วรพล มาลสุขุมและพีรพงศ์ จงไพศาลสกุล, *กฎหมายกับเศรษฐกิจ รวมบทความทางวิชาการเพื่อเป็นเกียรติแด่ ศาสตราจารย์ ดร.ศักดา ธนิตกุล ครูของ พ ศักดา 60 ปี* (กรุงเทพฯ: โรงพิมพ์เดือนตุลา, 2561).

European Union Agency for Cybersecurity, *Privacy considerations of online behavioural tracking* (20 July, 2019) European Union Agency for Cybersecurity <https://www.enisa.europa.eu/publications/privacy-considerations-of-online-behavioural-tracking>.

Ofce of the United Nations High Commissioner for Human Rights, *Guidelines for the Regulation of Computerized Personal Data Files: nal report / submitted by Louis Joinet, Special Rapporteur* (20 July, 2019) United Nations Digital Library <https://digitallibrary.un.org/record/43365>.

Peter Swire and Yianni Lagos “Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique” (2013) 72:2 *Maryland Law Review.*