ผลกระทบทางลบอันเกิดจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปและพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

Negative impacts of European General Personal Data Protection Regulation (GDPR) and Personal Data Protection Act B.E. 2562 on stakeholders

คณาธิป ทองรวีวงศ์ (Kanathip Thograweewong)
มหาวิทยาลัยเกษมบัณฑิต (Kasem Bundit University)
Email: kanathip.tho@kbu.ac.th

Received September 30, 2020; **Revised** December 11, 2020; **Accepted** February 20, 2021

Abstract

The research aimed to study 1) Negative impact in several aspects caused by the principles, elements, and conditions of European General Personal Data Protection Regulation (GDPR) 2) Negative impact in several aspects caused by the principles, elements, and conditions of Thailand's Personal Data Protection Act B.E. 2562 by comparative analysis with GDPR 3) proposal to reduce the negative impact. The methodology of this research is qualitative research by conducting content analysis and comparative analysis of Thai and European Union law. The research results were found as follows On the one hand, The General Data Protection Regulation (GDPR) of the European Union has provisions to protect the personal data of people such as requiring business sectors who are deemed as "data controller" to provide a measure for protecting personal data and granting several rights to the data subject. On the other hand, this law causes a negative impact in several dimensions for various stakeholders such as causing unfair trade competition, the prohibitive cost of compliance for small and medium business, limiting certain human rights especially freedom of speech, providing an opportunity for abuses and cybercrimes. As for Thailand, "The Personal Data Protection Act" has been enacted and take effect in May B.E. 2563. The comparative analysis indicates that this Act has similar content and element to GDPR. Consequently, the research indicates the tendency of negative impacts from this law as those caused by GDPR.

Keywords: Negative Impact; The General Data Protection Regulation (GDPR); The Personal Data Protection Act B.E. 2562 Personal Data Protection.

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์ 1) ศึกษาผลกระทบทางลบมิติต่าง ๆ ที่เกิดจากองค์ประกอบและเงื่อนไขของกฎหมายคุ้มครองข้อมูลส่วนบุคคลสหภาพยุโรป (GDPR) 2) ศึกษาผลกระทบทางลบมิติต่าง ๆ ที่เกิดจากองค์ประกอบและเงื่อนไขของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยศึกษาเปรียบเทียบกับกฎหมายสหภาพยุโรป 3) เพื่อทำข้อเสนอแนะในการลดผลกระทบทางลบ งานวิจัยนี้ใช้วิธีการวิจัยเชิงคุณภาพ โดยการศึกษาข้อมูลเอกสารเพื่อศึกษาหลักกฎหมาย องค์ประกอบของกฎหมายคุ้มครองข้อมูลของไทยและกฎหมายสหภาพยุโรป ด้วยการวิเคราะห์เนื้อหาเชิงเปรียบเทียบ ผลการวิจัยพบว่า แม้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปมีหลักการคุ้มครองข้อมูลส่วนบุคคล โดยกำหนดหน้าที่ให้ผู้ควบคุมข้อมูลส่วนบุคคลกำหนดมาตรการรักษาความปลอดภัยข้อมูลส่วนบุคคล และให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลหลายประการ แต่ส่งผลกระทบทางลบในหลายมิติ เช่น การแข่งขันที่เป็นธรรมระหว่างผู้ประกอบการรายใหญ่และรายย่อย อุปสรรคทางการค้าและการสร้างผู้ประกอบการรายใหม่ การจำกัดสิทธิเสรีภาพโดยเฉพาะเสรีภาพในการแสดงความคิดเห็น การเปิดช่องให้มีผู้นำไปใช้โดยมิชอบและอาชญากรรมไซเบอร์ ในส่วนของประเทศไทยมีการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในเดือนพฤษภาคม พ.ศ. 2562 ผลการวิเคราะห์เปรียบเทียบเนื้อหาพบว่า กฎหมายนี้มีบทบัญญัติ องค์ประกอบคล้ายคลึงกับกฎหมายสหภาพยุโรป จึงมีแนวโน้มส่งผลกระทบทางลบได้เช่นเดียวกับกฎหมายสหภาพยุโรป

คำสำคัญ: ผลกระทบทางลบ; กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป; พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562; การคุ้มครองข้อมูลส่วนบุคคล

บทนำ

ในเดือน พฤษภาคม ค.ศ. 2018 กฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับใหม่ของสหภาพยุโรป (General Data Protection Regulation: GDPA) มีผลใช้บังคับแทนที่กฎหมายเดิม (Directive 95/46/EC) กฎหมายนี้กำหนดหน้าที่และความรับผิดแก่ผู้ควบคุมข้อมูล (Data Controller) ซึ่งแบ่งเป็นสามกลุ่มหลักคือ หน้าที่รักษาความปลอดภัยของข้อมูลส่วนบุคคลของผู้อื่นที่ตนครอบครองหรือใช้ประโยชน์ หน้าที่เกี่ยวกับการดำเนินการตามเงื่อนไขในการเก็บรวบรวม การใช้ เปิดเผยข้อมูลส่วนบุคคล และหน้าที่ดำเนินการตอบสนองต่อสิทธิของเจ้าของข้อมูลส่วนบุคคล อย่างไร ก็ตามเงื่อนไขและองค์ประกอบของกฎหมายนี้ส่งผลกระทบทางลบต่อผู้มีส่วนเกี่ยวข้อง (Stakeholder) ในแง่มุมต่าง ๆ เช่น ผลกระทบจากต้นทุนการดำเนินการของผู้ประกอบการที่ต้องดำเนินการให้สอดคล้องกับกฎหมาย (Scott, Cerulus and Kayali, 2018; Campbell, Goldfarb and Tucker, 2015) ผลกระทบในการแข่งขันและการประกอบธุรกิจ (Russel, 2018; Schiff, 2018) ผลกระทบในแง่การลงทุนและการค้าระหว่างประเทศ (Lyons, 2018) และผลกระทบต่อสิทธิเสรีภาพของบุคคล (South, 2018; Kollmeyer, 2018) เป็นต้น

ในส่วนของกฎหมายไทย ก่อนหน้าปี พ.ศ. 2562 ไม่มีกฎหมายคุ้มครองข้อมูลเป็นกฎหมายเฉพาะ แต่มีกฎหมายอื่นหลายฉบับที่เกี่ยวข้องกับข้อมูลส่วนบุคคล (Kanathip Thongrawewong, 2016) ในเดือนกุมภาพันธ์ พ.ศ. 2562 สภานิติบัญญัติแห่งชาติ ได้ลงมติเห็นชอบร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล และประกาศในราชกิจจานุเบกษา เดือนพฤษภาคม พ.ศ. 2562 แต่ให้บทบัญญัติในส่วนที่กำหนดหน้าที่แก่ผู้ควบคุมข้อมูลส่วนบุคคล

มีผลใช้บังคับในอีกหนึ่งปี นับแต่ประกาศในราชกิจจานุเบกษา อย่างไรก็ตาม วันที่ 21 พฤษภาคม พ.ศ. 2563 “พระราชกฤษฎีกา กำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคล ไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2563” กำหนดยกเว้นหน้าที่ประการต่าง ๆ ของผู้ควบคุมข้อมูลส่วนบุคคลในกิจการ หรือหน่วยงาน 22 ประเภท ไปจนถึงวันที่ 31 พฤษภาคม พ.ศ. 2564 โดยหมายเหตุท้ายพระราชกฤษฎีกานี้ระบุถึงความไม่พร้อมของผู้มีหน้าที่ตามกฎหมายนี้ จะเห็นได้ว่าการตราพระราชบัญญัติ โดยกำหนดระยะเวลาบังคับใช้หนึ่งปี และเมื่อครบหนึ่งปีมีการตราพระราชกฤษฎีเพื่อยกเว้นชั่วคราวไปอีกหนึ่งปี สะท้อนถึงความไม่พร้อมของผู้เกี่ยวข้องรวมทั้งผลกระทบอันเกิดจากพระราชบัญญัตินี้

งานวิจัยนี้จึงศึกษาว่าองค์ประกอบและเงื่อนไขของกฎหมายของสหภาพยุโรป ส่งผลกระทบในมิติใดบ้าง จากนั้นจะศึกษาองค์ประกอบและเงื่อนไขของกฎหมายไทยเปรียบเทียบกับกฎหมายสหภาพยุโรป และนำผลกระทบทางลบอันเกิดจากองค์ประกอบและเงื่อนไขของกฎหมายสหภาพยุโรป มาประเมินผลกระทบทางลบของกฎหมายไทย

วัตถุประสงค์การวิจัย

1. เพื่อศึกษาผลกระทบทางลบในมิติต่าง ๆ ที่เกิดจากหลักกฎหมาย องค์ประกอบและเงื่อนไขของกฎหมายคุ้มครองข้อมูลส่วนบุคคลสหภาพยุโรป (GDPR)

2. เพื่อนำกฎหมายและผลกระทบจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป มาวิเคราะห์เปรียบเทียบกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของไทย

3. เพื่อจัดทำข้อเสนอแนะเชิงนโยบายเพื่อลดผลกระทบทางลบอันเกิดจากกฎหมายนี้

ขอบเขตการวิจัย

ขอบเขตด้านเนื้อหา การวิจัยครั้งนี้ศึกษาเฉพาะหลักกฎหมาย องค์ประกอบของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation: GDPR) กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักร และแนวทางตีความของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสหราชอาณาจักร

ขอบเขตด้านระยะเวลา เป็นการศึกษาในระยะเวลาก่อนกฎหมายไทย มีผลใช้บังคับในวันที่ 1 มิถุนายน 2564 จึงไม่ครอบคลุมการศึกษาเชิงปริมาณเกี่ยวกับการบังคับใช้

ทบทวนวรรณกรรม

สิทธิความเป็นส่วนตัว (Right of Privacy) อันเป็นพื้นฐานแนวคิดของการคุ้มครองข้อมูลส่วนบุคคล เป็นสิทธิขั้นพื้นฐานของมนุษย์ (Arendt, 1973) กล่าวคือ เป็นสิทธิที่ติดตัวคนมาตั้งแต่กำเนิด จึงมีลักษณะเช่นเดียวกับสิทธิมนุษยชน (Donnelly, 1982) ในความหมายดั้งเดิมอาจพิจารณาว่าเป็นสิทธิที่จะอยู่ตามลำพัง (Right to be let alone) กล่าวคือ ปราศจากการแทรกแซงจากบุคคลภายนอก (Warren and Brandies, 1890) แต่การพิจารณาในแง่ปราศจากการแทรกแซงหรือความลับอาจทำให้สิทธินี้กว้างเกินไป โดยเฉพาะในสภาพสังคมที่มีการติดต่อระหว่างบุคคล ทำให้การไม่ถูกแทรกแซงเป็นไปได้ยาก (Westin, 1967) ต่อมาจึงมีการพัฒนาการแนวคิดว่าไม่จำกัดเฉพาะการปราศจากการแทรกแซง แต่หมายถึงการจำกัดการเข้าถึงปัจเจกชนโดยบุคคลอื่น (Rubenfield, 1989) อย่างไรก็ตาม ในทางวิชาการ

สิทธิดังกล่าวยังคงมีความหมายและขอบเขตกว้าง (Schoeman, 1984) โดยอาจจำแนกพิจารณาได้หลายมิติ ซึ่งรวมถึงการคุ้มครองข้อมูลส่วนบุคคลด้วย (Solove, 2006) ตามกฎหมายต่างประเทศ เช่น สหรัฐอเมริกา สิทธิในความเป็นอยู่ส่วนตัวปรากฏในกฎหมายคอมมอนลอว์ และกฎหมายอื่น เช่น กฎหมายลักษณะละเมิด (Bloustein, 1984)

ในระดับกฎหมายระหว่างประเทศ ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ขององค์การสหประชาชาติ (UN's Universal Declaration of Human Rights ค.ศ. 1948) ข้อ 12 กำหนดรับรองสิทธิในความเป็นอยู่ส่วนตัวไว้อย่างชัดเจน อันเป็นหลักการเดียวกับกติกาสากลว่าด้วยสิทธิทางแพ่งและการเมือง ขององค์การสหประชาชาติ (International Covenant on Civil and Political Rights ค.ศ. 1966) ซึ่งรับรองสิทธินี้ไว้ในข้อ 17

กฎหมายต่างประเทศ โดยเฉพาะกฎหมายสหภาพยุโรปที่กำหนดหลักการคุ้มครองข้อมูลส่วนบุคคล จึงเป็นส่วนหนึ่งของการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว (Cate, 1995) โดยหลักสำคัญประการหนึ่งของกฎหมายนี้ คือ การวางเงื่อนไขการใช้ การเปิดเผย การโอนข้อมูลส่วนบุคคล ซึ่งรวมถึงข้อจำกัดด้านการโอนข้อมูลออกนอกประเทศ (Fromholz, 2000)

จากการทบทวนวรรณกรรม สรุปได้ว่า สิทธิในความเป็นอยู่ส่วนตัว จัดเป็นส่วนหนึ่งของสิทธิขั้นพื้นฐาน หรือสิทธิมนุษยชนของปัจเจกชน และเป็นกรอบแนวคิดพื้นฐานของการตรากฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลสหภาพยุโรป สำหรับกฎหมายไทย มีการระบุถึงสิทธินี้ในเหตุผลของการตราพระราชบัญญัติ อย่างไรก็ตาม องค์ประกอบและเงื่อนไขของกฎหมายนี้อาจส่งผลกระทบในทางลบต่อสิทธิดังกล่าวของเจ้าของข้อมูล ดังจะศึกษาในงานวิจัยนี้

วิธีดำเนินการวิจัย

เนื่องจากการวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาผลกระทบทางลบจากตัวบท องค์ประกอบ และเงื่อนไขของกฎหมาย รวมทั้งการตีความและการปรับใช้กฎหมาย (Application of law) จึงใช้**วิธีการศึกษาเชิงคุณภาพ** (Qualitative Research) ด้วยการศึกษาข้อมูลเอกสาร (Documentary Research)

ข้อมูลที่ใช้ในการวิจัย ข้อมูลเอกสาร จากตัวบทกฎหมายที่เกี่ยวข้อง โดยเฉพาะกฎหมายคุ้มครองข้อมูลส่วนบุคคลสหภาพยุโรป (GDPR) แนวการตีความของสหภาพยุโรปกฎหมายคุ้มครองข้อมูลส่วนบุคคลสหราชอาณาจักร แนวทางตีความของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสหราชอาณาจักร แนวคิดทฤษฎีทางกฎหมายที่เกี่ยวข้องจากตำรา หนังสือ บทความวิชาการ บทความวิจัย

การวิเคราะห์ข้อมูล ใช้วิธีการวิเคราะห์เนื้อหา (Content analysis) เป็นการกระทำกับข้อมูลที่ได้จากเอกสาร โดยวิเคราะห์เชิงบรรยาย (Descriptive) รวมทั้งวิเคราะห์โดยการเปรียบเทียบข้อมูล โดยวิเคราะห์เนื้อหาจากตัวบทกฎหมายสหภาพยุโรป แนวทางการตีความของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป นำมาเปรียบเทียบกับเนื้อหาของตัวบทกฎหมายตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของไทย ซึ่งเป็นการศึกษาวิเคราะห์เนื้อหาเชิงเปรียบเทียบด้วยการบรรยาย (Comparative analysis)

ผลการวิจัย

ผลการวิจัยตามวัตถุประสงค์ข้อ 1 ชี้ให้เห็นว่าหลักกฎหมาย องค์ประกอบและเงื่อนไขของกฎหมายคุ้มครองข้อมูลส่วนบุคคลสหภาพยุโรป ส่งผลกระทบทางลบ 7 ด้าน ดังนี้ 1) ผลกระทบในแง่ภาระต้นทุนทางธุรกิจและ

การแข่งขันทางการค้าที่ไม่เป็นธรรม 2) ผลกระทบในแง่ของการสร้างโอกาสให้กับการโจมตีทางไซเบอร์ 3) ผลกระทบในแง่การสร้างโอกาสให้เกิดการโจรกรรมข้อมูลส่วนบุคคล 4) ผลกระทบต่อเสรีภาพในการแสดงความคิดเห็น 5) ผลกระทบอันเกิดจากการปฏิบัติเพื่อให้สอดคล้องกับกฎหมายด้วยวิธีการที่เกินไปกว่ากฎหมายกำหนด 6) กฎหมายคุ้มครองข้อมูลส่วนบุคคลส่งผลในแง่เพิ่มอำนาจรัฐในการควบคุมข้อมูล 7) กฎหมายคุ้มครองข้อมูลส่วนบุคคลตราขึ้นในสภาพแวดล้อมที่ขาดการมีส่วนร่วมอย่างเหมาะสม

ผลการวิจัยตามวัตถุประสงค์ข้อ 2 ชี้ให้เห็นว่าหลักกฎหมาย องค์ประกอบ และเงื่อนไขของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของไทย คล้ายคลึงกับกฎหมายสหภาพยุโรป จึงส่งผลกระทบทางลบ 7 ด้าน ในลักษณะเดียวกับกฎหมายสหภาพยุโรป

ผลการวิจัยตามวัตถุประสงค์ข้อ 3 จากผลกระทบทางลบทั้ง 7 ด้าน ผู้วิจัยจึงมีข้อเสนอแนะเชิงนโยบาย ในการเสนอยกเลิกพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

อภิปรายผล

การอภิปรายผลการวิจัยแยกตามผลกระทบแต่ละด้าน โดยแต่ละด้านจะเริ่มจากการอภิปรายผลกระทบตามกฎหมายสหภาพยุโรป เพื่อตอบสนองวัตถุประสงค์การวิจัยข้อ 1 จากนั้นจะอภิปรายผลการวิเคราะห์เปรียบเทียบกับกฎหมายไทย เพื่อตอบสนองวัตถุประสงค์การวิจัยข้อ 2

1. ผลกระทบในแง่ภาระต้นทุนทางธุรกิจและการแข่งขันทางการค้าที่ไม่เป็นธรรม

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ก่อให้เกิดต้นทุนการทำให้สอดคล้อง (Cost for compliance) ดังนี้

– หลักการจัดให้มีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคล ปรากฏในกฎหมายคุ้มครองข้อมูลส่วนบุคคลสหภาพยุโรปมาตรา 24 ซึ่งกำหนดให้ผู้ควบคุมข้อมูลต้องจัดให้มีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม (The controller shall implement appropriate technical and organizational measures) ผลการศึกษาเปรียบเทียบกับกฎหมายไทย พบว่า หลักการนี้ปรากฏในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(1) ซึ่งกำหนดหน้าที่ให้ผู้ควบคุมข้อมูลส่วนบุคคล จัดให้มีมาตรการการรักษาความปลอดภัยที่เหมาะสม นอกจากนี้มาตรา 40 ยังกำหนดหน้าที่ลักษณะเดียวกันให้กับผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งรวมถึงผู้ให้บริการต่าง ๆ ที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้บริการ เช่น การรับฝากข้อมูล การจ้างวิเคราะห์ข้อมูล เป็นต้น หลักการดังกล่าวส่งผลให้ผู้ประกอบธุรกิจต้องลงทุนในหลายมิติ เช่น ระบบเครือข่ายซอฟต์แวร์เกี่ยวกับการรักษาความปลอดภัยของข้อมูล การจ้างที่ปรึกษาทางเทคนิค และบุคลากรเกี่ยวกับความปลอดภัยทางคอมพิวเตอร์

– หลักการกำหนดหน้าที่ให้ผู้ควบคุมข้อมูลต้องแจ้งเหตุข้อมูลรั่วไหลหรือถูกล่วงละเมิด (Data breach notification) โดยแยกเป็นสองกรณี คือการแจ้งต่อหน่วยงานกำกับ เช่น คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หลักการนี้ปรากฏในกฎหมายสหภาพยุโรป มาตรา 33 (Notification of a personal data breach to the supervisory authority) และการแจ้งเหตุข้อมูลรั่วไหลหรือล่วงละเมิดต่อเจ้าของข้อมูล หลักการนี้ปรากฏในกฎหมายคุ้มครองข้อมูลส่วนบุคคลสหภาพยุโรป มาตรา 34 (Communication of a personal data breach to the data subject) ผลการศึกษาเปรียบเทียบกับกฎหมายไทย พบว่า หลักการนี้ปรากฏในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(2) ซึ่งจำแนกเป็นการแจ้งต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและการแจ้งต่อเจ้าของข้อมูล หลักการนี้ส่งผลให้เกิดภาระต้นทุนการทำให้สอดคล้องกับกฎหมาย เช่น ก่อนการแจ้งต้องมีการประเมินสถานการณ์

ตรวจสอบข้อเท็จจริง และหลักฐานทางอิเล็กทรอนิกส์ (Forensic) ซึ่งต้องอาศัยงบประมาณ และการจ้างผู้เชี่ยวชาญ รวมทั้งต้นทุนในการปฏิบัติการส่งข้อมูลการแจ้งต่าง ๆ

– หลักการให้สิทธิแก่เจ้าของข้อมูลในการร้องขอเข้าถึง (Right to access) ข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของผู้ควบคุมข้อมูลส่วนบุคคล รวมทั้งขอทราบรายละเอียดต่าง ๆ เกี่ยวกับการประมวลผลข้อมูลของตน หลักการนี้ปรากฏในกฎหมายสหภาพยุโรป มาตรา 15 (Right of access by the data subject) ผลการศึกษาเปรียบเทียบ พบว่า หลักการนี้ปรากฏในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 30 และ 31 หลักการนี้ส่งผลให้เกิดภาระต้นทุนการทำให้สอดคล้องกับกฎหมาย กล่าวคือ ผู้ควบคุมข้อมูลต้องจัดให้มีระบบรองรับคำร้องขอ ต้องจัดให้มีเจ้าหน้าที่จัดการเกี่ยวกับคำขอ รวมทั้งมีหน้าที่ตาม มาตรา 39 ในการเก็บบันทึกข้อมูลและรายละเอียดเกี่ยวกับการดำเนินการ หรือตอบสนองต่อคำขอดังกล่าว

หลักกฎหมายข้างต้นส่งผลในแง่การสร้างต้นทุนการทำให้สอดคล้อง (Cost for compliance) ซึ่งแยกวิเคราะห์ได้ 3 ประเด็นย่อย คือ

1.1) ผลกระทบต่อการแข่งขันทางการค้าและผู้ประกอบการขนาดย่อม

เมื่อพิจารณาในภาพรวมระดับประเทศ ผลการวิจัยในสหรัฐอเมริกา ชี้ว่าหากสหรัฐอเมริกา ตรากฎหมายเช่น GDPR จะส่งผลต่อต้นทุนการทำให้สอดคล้องของบริษัทสหรัฐอเมริกา กว่า 150 พันล้านเหรียญ ซึ่งสูงกว่างบประมาณการลงทุนในเครือข่ายคอมพิวเตอร์ของสหรัฐ ถึงสองเท่า (Spalter, 2018) และต้นทุนดังกล่าวจัดเป็นหนึ่งในสามของรายได้จากการค้าอิเล็กทรอนิกส์ทั้งปีในสหรัฐอเมริกา หากพิจารณาในระดับภาคธุรกิจ สามารถแยกผลกระทบต่อผู้มีส่วนเกี่ยวข้อง (stakeholders) โดยแยกเป็นสองด้าน ดังนี้

ด้านที่หนึ่ง กฎหมายคุ้มครองข้อมูลส่วนบุคคลสหภาพยุโรป สร้างความได้เปรียบให้กับผู้ประกอบธุรกิจรายใหญ่ หลังจากการบังคับใช้ของ GDPR ผลการศึกษาในสหรัฐอเมริกา พบว่า ผู้ประกอบธุรกิจรายใหญ่ เช่น Google, Facebook, Amazon มีส่วนแบ่งตลาดในยุโรปมากขึ้น (Scott, Cerulus and Kayali, 2018) ความได้เปรียบดังกล่าวเกิดจากปัจจัยหลายประการ (Campbell, Goldfarb and Tucker, 2015) เช่น ต้นทุนการดำเนินการให้สอดคล้องกับ GDPR เป็นข้อได้เปรียบของธุรกิจขนาดใหญ่ ซึ่งมีงบประมาณเพื่อการนี้ เช่น การอัพเกรดระบบป้องกัน การจ้างผู้เชี่ยวชาญด้านความปลอดภัย การร่างสัญญาและนโยบาย

ด้านที่สอง กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป สร้างความเสียเปรียบแก่ผู้ประกอบการขนาดกลางและย่อม (SME) ผลการวิจัยในสหรัฐอเมริกาชี้ พบว่า ผู้ประกอบธุรกิจขนาดกลางและย่อมที่เกี่ยวข้องกับการโฆษณาออนไลน์ (Ad tech) สูญเสียส่วนแบ่งตลาดประมาณสองในสาม หลังจากกฎหมายสหภาพยุโรป (GDPR) ใช้บังคับในปี ค.ศ. 2018 (Björnf, 2018) ธุรกิจขนาดกลางและย่อมในสหรัฐอเมริกา ที่ได้รับผลกระทบจากกฎหมาย GDPR ได้แก่ ธุรกิจการโฆษณาออนไลน์ (Ad tech) ธุรกิจเกี่ยวกับการวิเคราะห์ข้อมูลในสื่อสังคมออนไลน์ (social media analytics) (Russel, 2018) ธุรกิจเกี่ยวกับการติดตามข้อมูลเพื่อการโฆษณา (Ad tracking) หลายแห่งปิดตัวเพราะได้รับผลกระทบ (Schiff, 2018) ธุรกิจเกี่ยวกับเกมส์ออนไลน์ ความบันเทิงออนไลน์ ยุติการให้บริการเมื่อพิจารณาชั่งน้ำหนักกับต้นทุนที่จะต้องปฏิบัติให้สอดคล้องกับกฎหมายสหภาพยุโรป (Good, 2018)

1.2) ผลกระทบในแง่อุปสรรคต่อการเข้าสู่ตลาด

แม้ว่าการสร้างภาระต้นทุนการทำให้สอดคล้องกับกฎหมายจะเป็นผลกระทบที่เกิดจากกฎหมายอื่นเช่นกัน แต่เงื่อนไขและหลักการของ GDPR ส่งผลกระทบที่รุนแรงในระดับที่เป็นการกีดกันการเข้าสู่ตลาด (Cost prohibitive) จากผลสำรวจธุรกิจข้ามชาติขนาดใหญ่ พบว่า Google, Facebook, Amazon รวมทั้งธุรกิจขนาดใหญ่อีก 500 แห่ง

รายงานว่าได้ใช้ต้นทุนประมาณ 8 ล้านเหรียญสหรัฐ ในการทำให้สอดคล้องกับกฎหมาย GDPR เมื่อเปรียบเทียบกับธุรกิจขนาดกลางและย่อม ผลการสำรวจชี้ให้เห็นว่า การทำให้สอดคล้องไม่สามารถเป็นไปได้ในแง่ต้นทุนที่ผู้ประกอบการต้องแบกรับ (The International Association of Privacy Professionals (IAPP), 2018a) ภาระต้นทุนดังกล่าวส่งผลต่อธุรกิจขนาดย่อมและการระดุมทุนสำหรับสตาร์ทอัพ (Venture capital market) ผลวิจัยในสหรัฐอเมริกา ชี้ว่า การระดมทุนที่ลดลงในช่วง ค.ศ. 2017 – 2018 ส่งผลต่อการจ้างงานถึง 30,000 ตำแหน่ง (Jia, Jin, Wagman, 2018) ภาระต้นทุนที่สูงเช่นนี้ ส่งผลในแง่การกีดกันการเข้าสู่ตลาด และการแข่งขันสำหรับผู้ประกอบการขนาดย่อม ดังกล่าวข้างต้น

1.3) ผลกระทบในแง่การค้าและการลงทุนระหว่างประเทศ

GDPR ได้รับการวิจารณ์ว่าเป็นอุปสรรคทางการค้า (Trade barrier) ซึ่งส่งผลให้ผู้ประกอบการนอกสหภาพยุโรป เช่น บริษัทสหรัฐอเมริกา ขนาดกลางและย่อม อันจะส่งผลเชิงบวกต่อธุรกิจขนาดกลางและย่อมของสหภาพยุโรป (Lyons, 2018) จะเห็นได้ว่า ธุรกิจสหรัฐอเมริกา ที่ให้บริการในสหภาพยุโรป ซึ่งมีลักษณะการดำเนินการเก็บข้อมูลส่วนบุคคล ตัดสินใจยุติกิจการหรือการดำเนินการในสหภาพยุโรป เนื่องจากไม่สามารถแบกรับต้นทุนการปฏิบัติให้สอดคล้องกับกฎหมายสหภาพยุโรป (www.warportal.com, 2018) อย่างไรก็ตาม ในอีกมุมหนึ่ง GDPR ส่งผลทางลบต่อธุรกิจขนาดกลางและย่อม รวมทั้งสตาร์ทอัพของสหภาพยุโรปด้วยเช่นกัน อาทิ ผู้ประกอบธุรกิจการตลาดออนไลน์ของสหรัฐอเมริกาที่ให้บริการในสหภาพยุโรป ยุติการให้บริการก่อนที่ GDPR จะมีผลบังคับใช้ในปี ค.ศ. 2018 ซึ่งส่งผลกระทบต่อลูกจ้างในสหภาพยุโรป (Shields, 2018)

ผลการเปรียบเทียบกับกฎหมายไทย พบว่า หลักกฎหมายดังกล่าวของสหภาพยุโรป ปรากฏในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จึงส่งผลในแง่การสร้างต้นทุนการทำให้สอดคล้อง (Cost for compliance) เช่นเดียวกับกฎหมายสหภาพยุโรป

2. ผลกระทบในแง่ของการสร้างโอกาสให้กับการโจมตีทางไซเบอร์

แม้ว่าโดยหลักแล้ว GDPR มีหลักการคุ้มครองข้อมูลส่วนบุคคล โดยกำหนดให้ผู้ควบคุมข้อมูลต้องจัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสม (Data security) แต่เนื่องจากหลักกฎหมายบางประการส่งผลในลักษณะของการสร้างโอกาสสำหรับอาชญากรรมไซเบอร์ชนิดต่าง ๆ เช่น หลักกฎหมายที่ให้สิทธิเจ้าของข้อมูลทำการร้องขอในเรื่องต่าง ๆ แก่ผู้ควบคุมข้อมูลส่วนบุคคล เช่น คำร้องขอให้แก้ไขข้อมูล คำร้องขอให้ลบหรือทำลายข้อมูล (มาตรา 15 – 21) หลักกฎหมายดังกล่าว ในแง่หนึ่งเป็นการให้สิทธิเจ้าของข้อมูลทำการควบคุมข้อมูลส่วนบุคคลของตน (Right to control personal data) แต่ในอีกแง่หนึ่ง ส่งผลเป็นการสร้างเงื่อนไข และเปิดโอกาสสำหรับอาชญากรรมไซเบอร์บางชนิด ซึ่งแยกพิจารณาได้ดังนี้

2.1) การสร้างโอกาสให้กับการโจมตีแบบปฏิเสธบริการ (Denial–of–service หรือ DDoS)

การให้สิทธิเจ้าของข้อมูลในการเข้าถึง (Right of access) รวมถึงการขอสำเนาข้อมูลของตน ทำให้ผู้ควบคุมข้อมูลมีหน้าที่จัดให้มีช่องทางสำหรับ ส่งคำขอโดยเฉพาะอย่างยิ่งในรูปแบบข้อมูลคอมพิวเตอร์ โดยส่งตามช่องทางอิเล็กทรอนิกส์ ส่งผลให้อาชญากรไซเบอร์ อาศัยการร้องขอทางอิเล็กทรอนิกส์ ในฐานะเป็นช่องทางโจมตี (Data requests as attack vector) เช่น โจมตีแบบปฏิเสธบริการ โดยโจมตีเว็บไซต์และศูนย์บริการลูกค้า ด้วยคำขอในเวลาเดียวกันจำนวนมาก หรืออาชญากรอาจอาศัยอุปกรณ์ของผู้ใช้งานที่เชื่อมต่อจำนวนมากในฐานะบอทเน็ต (Botnet) เพื่อโจมตีเว็บไซต์ของผู้ประกอบการที่มีหน้าที่รับคำร้องขอตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (Henderson, 2018)

2.2) การสร้างโอกาสให้กับการโจมตีโดยใช้มัลแวร์

การให้สิทธิเจ้าของข้อมูลส่งคำร้องขอต่าง ๆ โดยเฉพาะคำร้องทางระบบอิเล็กทรอนิกส์นั้น หากผู้ควบคุมข้อมูลเปิดโอกาสให้ส่งทางจดหมายอิเล็กทรอนิกส์ จะเปิดช่องให้อาชญากรใช้วิธีการโจมตีโดยแนบไฟล์ที่มีมัลแวร์ชนิดต่าง ๆ อันจะส่งผลกระทบต่อระบบหรือข้อมูลของผู้ควบคุมข้อมูล รวมไปถึงผู้เกี่ยวข้องอื่น ๆ นอกจากนี้ จากผลกระทบทางลบต่อการโจมตีแบบปฏิเสธบริการดังกล่าวข้างต้น ผู้ควบคุมข้อมูลบางรายอาจใช้วิธีทางเทคนิคเพื่อลดความเสี่ยงจากการโจมตีดังกล่าว แต่กลับสร้างโอกาสสำหรับการโจมตีด้วยมัลแวร์ เช่น ผู้ควบคุมต้องการป้องกันการโจมตีแบบปฏิเสธบริการ ซึ่งอาชญากรอาศัยช่องทางจากคำร้องขอของเจ้าของข้อมูล จึงกำหนดให้เจ้าของข้อมูลยื่นคำขอทางอีเมล เปิดโอกาสให้อาชญากรใช้วิธีการโจมตีโดยแนบไฟล์ซึ่งมีมัลแวร์ เป็นต้น (Henderson, 2018)

ผลการเปรียบเทียบกับกฎหมายไทย พบว่า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 30 – 34 ให้สิทธิเจ้าของข้อมูลรวมทั้งสิทธิขอเข้าถึง ตรวจสอบ ขอสำเนาข้อมูลของตน ฯลฯ ดังนั้น ผลกระทบทางลบอันเกิดจากกฎหมายสหภาพยุโรปดังกล่าวสามารถเกิดขึ้นกับผู้มีส่วนได้เสียต่าง ๆ ในประเทศไทยได้

3. ผลกระทบในแง่การสร้างโอกาสให้เกิดการโจรกรรมข้อมูลส่วนบุคคล

แม้ว่าโดยหลักการแล้ว กฎหมายคุ้มครองข้อมูลส่วนบุคคลสหภาพยุโรป มีหลักการรักษาความปลอดภัยของข้อมูลส่วนบุคคล แต่หลักการในส่วนของสิทธิเจ้าของข้อมูลเปิดโอกาสให้เกิดการส่งข้อมูลคำร้องจากเจ้าของข้อมูลไปยังผู้ควบคุมข้อมูลส่วนบุคคล (มาตรา 15 – 21) โดยการส่งคำร้องดังกล่าวซึ่งกระทำทางระบบอิเล็กทรอนิกส์ นอกจากส่งผลให้เกิดความเสี่ยงต่อการโจมตีทางไซเบอร์รูปแบบต่าง ๆ ที่กระทบต่อการทำงานของระบบ หรือข้อมูลคอมพิวเตอร์ของผู้เกี่ยวข้องดังกล่าวแล้ว ยังส่งผลให้เกิดสภาพแวดล้อมที่เอื้ออำนวยแก่อาชญากรรมคอมพิวเตอร์ ที่กระทำต่อข้อมูลส่วนบุคคล เช่น การโจรกรรมข้อมูลระบุตัวบุคคล หรือข้อมูลเอกลักษณ์ (Identity theft) (ANA, 2019) เช่น การที่กฎหมายให้สิทธิเจ้าของข้อมูลร้องขอข้อมูลส่วนบุคคลที่เกี่ยวกับตน (Right of access) เปิดทางให้อาชญากรรมใช้โอกาสจากหลักการนี้ใช้เทคนิคต่าง ๆ ส่งคำร้องขอข้อมูลส่วนบุคคลของผู้อื่น โดยแอบอ้างเป็นบุคคลดังกล่าว ส่งผลได้มาซึ่งข้อมูลส่วนบุคคลของเหยื่อ (Martino et al, 2019) ผลการวิจัยเชิงทดลอง ซึ่งคณะผู้วิจัยใช้เทคนิคต่าง ๆ ในการปลอมตัว (Impersonate) เป็นเจ้าของข้อมูลส่วนบุคคล ชี้ให้เห็นว่าการใช้วิธีการวิศวกรรมทางสังคม (Social engineering) การแสวงหาข้อมูลจากแหล่งต่าง ๆ เช่น สื่อสังคมออนไลน์ สามารถนำไปประกอบในการปลอมตัว (Impersonate) เป็นเจ้าของข้อมูลและยื่นคำร้องต่อผู้ควบคุมข้อมูลขอใช้สิทธิเข้าถึงข้อมูล (Right of access) ส่งผลให้ผู้ปลอมตัวได้มาซึ่งข้อมูลส่วนบุคคลอื่นของเจ้าของข้อมูล รวมถึงข้อมูลละเอียดอ่อน เช่น ข้อมูลธุรกรรม บัญชีการเงิน (Martino et al, 2019) เป็นต้น

ผลการเปรียบเทียบกับกฎหมายไทย พบว่า หลักการให้สิทธิเจ้าของข้อมูลตามกฎหมายยุโรป ปรากฏในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 30 – 34 ซึ่งให้สิทธิเจ้าของข้อมูลหลายประการ ในด้านของผู้ประกอบการที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ปฏิบัติตามกฎหมาย โดยจัดให้มีระบบและการตอบสนองต่อการใช้สิทธิของเจ้าของข้อมูลในการยื่นคำร้องต่าง ๆ ดังนั้น ผลกระทบทางลบอันเกิดจากกฎหมายสหภาพยุโรปดังกล่าวสามารถเกิดขึ้นกับผู้มีส่วนได้เสียต่าง ๆ ในประเทศไทยได้ เช่น เจ้าของข้อมูลที่อาจตกเป็นเหยื่อของการโจรกรรมข้อมูลเอกลักษณ์ โดยอาชญากรปลอมตัวเป็นเจ้าของข้อมูล และแอบอ้างสิทธิยื่นคำร้องขอข้อมูลอื่น ๆ ของเจ้าของข้อมูล

4. ผลกระทบต่อสิทธิเสรีภาพของบุคคล

4.1 เสรีภาพในการแสดงความคิดเห็น (Freedom of speech) ซึ่งครอบคลุมทั้งการรับและส่งข้อมูลข่าวสาร กฎหมายคุ้มครองข้อมูลส่วนบุคคล ส่งผลกระทบในลักษณะการจำกัดการเผยแพร่ข้อมูลข่าวสาร ดังจะเห็นได้จากผู้ประกอบการสื่อออนไลน์ของสหรัฐอเมริกา ประมาณ 1,000 ราย เช่น เว็บไซต์ข่าว นิตยสาร ได้ยุติการให้บริการหลังจากกฎหมายคุ้มครองข้อมูลสหภาพยุโรปมีผลใช้บังคับ ส่งผลกระทบต่อการเข้าถึงข้อมูลของทั้งประชาชนสัญชาติอเมริกันในสหภาพยุโรป และประชาชนยุโรปที่ประสงค์เข้าถึงข้อมูลข่าวสารของประเทศนอกสหภาพยุโรป (South, 2018; Kollmeyer, 2018) สาเหตุของผลกระทบในมิตินี้ มีหลายประการ เช่น

– ภาระต้นทุนที่สูง ตามที่ดังกล่าวมาแล้วส่งผลให้ผู้ประกอบธุรกิจสื่อไม่สามารถดำเนินการต่อไปได้ โดยเฉพาะอย่างยิ่งผู้ประกอบธุรกิจสื่อออนไลน์ขนาดกลางและย่อม

– สิทธิของเจ้าของข้อมูลในการขอให้ลบ หรือทำลายข้อมูลระบุตัวของตน (Right to erase or right to be forgotten) เปิดทางให้มีการใช้เพื่อวัตถุประสงค์อื่น (Abuse) เช่น เพื่อปิดกั้นการวิพากษ์วิจารณ์แสดงความคิดเห็น นอกจากนี้บุคคลสาธารณะหรือภาครัฐอาจอาศัยกลไกดังกล่าวเพื่อปิดกั้นเนื้อหาผิดกฎหมาย (Illegal content) ของประเทศหนึ่งซึ่งไม่ผิดกฎหมายประเทศอื่น เช่น การร้องขอต่อผู้ประกอบการสื่อออนไลน์เพื่อให้ปิดกั้นข้อมูลที่ผิดกฎหมายประเทศหนึ่งจากการเข้าถึงได้ในประเทศอื่น ๆ (The International Association of Privacy Professionals (IAPP), 2018b)

ผลการเปรียบเทียบกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พบว่า มีหลักจำกัดการเปิดเผยหรือเผยแพร่ข้อมูลข่าวสาร จึงส่งผลต่อเสรีภาพในการแสดงความคิดเห็นได้เช่นเดียวกับกฎหมายสหภาพยุโรป

4.2 สิทธิในความเป็นอยู่ส่วนตัวของเจ้าของข้อมูลส่วนบุคคล (Right to privacy) จากการทบทวนวรรณกรรมจะเห็นได้ว่าสิทธิในความเป็นอยู่ส่วนตัว เป็นกรอบแนวคิดพื้นฐานของกฎหมายคุ้มครองข้อมูลส่วนบุคคล อย่างไรก็ตาม องค์ประกอบและเงื่อนไขของกฎหมายคุ้มครองข้อมูลส่วนบุคคล อาจส่งผลกระทบทางลบต่อสิทธินี้ เช่น การสร้างโอกาสให้กับอาชญากรรมที่ส่งผลต่อความเป็นส่วนตัวของเจ้าของข้อมูล ดังกล่าวที่มาแล้ว รวมทั้งการที่ผู้ประกอบการใช้วิธีการปฏิบัติเพื่อให้สอดคล้องกับกฎหมายด้วยเทคนิคต่าง ๆ อันส่งผลให้เจ้าของข้อมูลมีความเสี่ยงต่อการถูกล่วงละเมิดข้อมูลส่วนบุคคลมากขึ้น ดังจะกล่าวในผลกระทบข้อต่อไป

5. ผลกระทบอันเกิดจากการปฏิบัติเพื่อให้สอดคล้องกับกฎหมาย ด้วยวิธีการที่เกินไปกว่ากฎหมายกำหนด หน้าที่ และโทษของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ส่งผลให้ผู้ประกอบการซึ่งอยู่ในฐานะผู้ควบคุมข้อมูล ดำเนินการต่าง ๆ เพื่อให้สอดคล้องกับกฎหมาย ด้วยวิธีการที่กว้างกว่าหรือนอกเหนือจากที่กฎหมายกำหนด เช่น องค์กรกำกับการจดทะเบียนโดเมนเนม (The Internet Corporation for Assigned Names and Numbers: ICANN) ประกาศเกณฑ์ที่กำหนดให้มีการปิดบัง หรือไม่แสดงข้อมูลที่แสดงรายละเอียดของเจ้าของชื่อโดเมน (WHOIS) ซึ่งแต่เดิมเป็นข้อมูลที่แสดงปรากฏต่อสาธารณะ ทั้งนี้ เพื่อให้สอดคล้องกับหลักเกณฑ์และข้อกำหนดของกฎหมาย GDPR (ICANN, 2018) แม้ว่ากฎหมายสหภาพยุโรปจะไม่ใช้บังคับกับข้อมูล ซึ่งไม่ใช่ข้อมูลระบุตัวบุคคล รวมทั้งไม่บังคับใช้กับการจดทะเบียนโดเมนเนมของนิติบุคคล ดังนั้น โดยหลักแล้วข้อมูลจดทะเบียนโดเมนเม ซึ่งไม่อาจระบุตัวบุคคลหรือเป็นโดเมนเนมของนิติบุคคล จะไม่อยู่ในขอบเขตของกฎหมายนี้ แต่กฎหมายเปิดโอกาสให้ผู้ประกอบการบางรายทำการจำกัด หรือห้ามการเข้าถึงข้อมูลบางอย่าง ดังเช่นข้อมูลจดทะเบียนโดนเมนเนม เนื่องจากกฎหมายนี้มีถ้อยคำตัวบทที่กว้าง รวมทั้งคลุมเครือและไม่ชัดเจน (Broad and vague) รวมทั้งมีโทษปรับในอัตราสูง ทำให้ผู้ประกอบการเลือกที่จะลดความเสี่ยง โดยมีแนวปฏิบัติที่กว้างและเกินกว่ากฎหมายกำหนด แนวปฏิบัติของผู้ประกอบการดังกล่าว

ส่งผลกระทบทางลบในหลายแง่มุม เช่น 1) ผลต่อการป้องกันและปราบปรามอาชญากรรม เนื่องจากข้อมูลแสดงการจดทะเบียนโดเมนเนม (WHOIS) จำเป็นสำหรับการบังคับใช้กฎหมายเพื่อป้องกันและปราบปรามอาชญากรรมไซเบอร์ต่าง ๆ (Tews, 2018) ดังนั้น การปิดบังข้อมูลดังกล่าวส่งผลกระทบทางลบในแง่ของการสร้างอุปสรรคต่อการป้องกันและปราบปรามอาชญากรรมไซเบอร์ 2) ผลต่อสิทธิเสรีภาพอื่น เช่น สิทธิที่จะได้รู้ (Right to know) เนื่องจากข้อมูลที่แสดงถึงการจดทะเบียนโดเมนเนม ในหลายกรณีมีความจำเป็นต่อประโยชน์สาธารณะ เช่น ผู้บริโภคที่ต้องการระบุตัวผู้จดทะเบียนเว็บไซต์ที่นำเสนอสินค้าหรือบริการ ดังนั้น การปกปิดข้อมูลดังกล่าวอาจพิจารณาว่าการคุ้มครองสิทธิเจ้าของข้อมูลไม่ได้สัดส่วนกับสิทธิอื่น (Epstein, 2018) เช่น สิทธิได้รู้ เสรีภาพในการแสดงความคิดเห็น เป็นต้น

นอกจากนี้ การที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดเงื่อนไขและหน้าที่หลายประการ ผู้ควบคุมข้อมูลส่วนบุคคลจึงใช้เทคนิควิธีการต่าง ๆ เพื่อให้สอดคล้องกับกฎหมาย อันส่งผลให้เจ้าของข้อมูลมีความเสี่ยงต่อการถูกล่วงละเมิดข้อมูลส่วนบุคคลมากขึ้น เช่น การใช้วิธียกเลิกช่องทางบริการอื่นและให้ลูกค้าเข้าใช้บริการผ่านแอพพลิเคชั่นเท่านั้น เพื่อให้ลูกค้าทุกคนของตนกดปุ่ม “ทราบ” การแจ้งรายละเอียดตามมาตรา 23 ส่งผลให้ลูกค้าที่ไม่ประสงค์ให้มีการเก็บรวบรวมข้อมูลส่วนบุคคลจำต้องเข้าสู่ระบบการเก็บข้อมูลทางอิเล็กทรอนิกส์ ซึ่งเป็นการจำกัดสิทธิในการควบคุมข้อมูลของตนและสร้างโอกาสแก่อาชญากรรมไซเบอร์

ผลการศึกษาเปรียบเทียบกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พบว่า กำหนดหลักการและองค์ประกอบคล้ายคลึงกับกฎหมายสหภาพยุโรป ดังนั้น จึงมีปัญหาความกว้าง คลุมเครือและไม่ชัดเจนคล้ายกับกฎหมายสหภาพยุโรป ลักษณะเช่นนี้ส่งผลกระทบในทางลบได้ในลักษณะเดียวกับกฎหมายสหภาพยุโรป

6. กฎหมายสหภาพยุโรป ส่งผลในแง่เพิ่มอำนาจรัฐในการควบคุมข้อมูล

แม้ว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป จะมีหลักการที่ให้สิทธิเจ้าของข้อมูลในการควบคุมข้อมูลและตัดสินใจเกี่ยวกับข้อมูลของตน ดังปรากฏในบทบัญญัติเกี่ยวกับสิทธิเจ้าของข้อมูล แต่กฎหมายนี้ส่งผลเพิ่มอำนาจรัฐ ดังจะเห็นได้จากกฎหมายนี้กำหนดเงื่อนไข แนวปฏิบัติต่าง ๆ ที่ผู้ประกอบธุรกิจในฐานะผู้ควบคุมข้อมูลต้องปฏิบัติตาม (Layton, 2019)

ผลการเปรียบเทียบกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พบว่า กำหนดหน้าที่หลายประการแก่ผู้ประกอบธุรกิจ นอกจากนี้ ในตัวบทหลายมาตรากำหนดให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลออกประกาศกำหนดรายละเอียด ซึ่งส่งผลกระทบต่อหน้าที่ผู้เกี่ยวข้อง แม้ว่าคณะกรรมการจะมีสถานะเป็นองค์กรอิสระ แต่เนื่องจากร่างกฎหมายนี้เสนอโดยฝ่ายบริหาร รวมทั้งมีการกำหนดอำนาจหน้าที่หลายประการแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ตลอดจนการสรรหาหรือที่มาของคณะกรรมการดังกล่าว ล้วนแต่อยู่บนพื้นฐานการจัดการของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม จึงมีประเด็นการครอบงำของฝ่ายบริหาร

7. สภาพแวดล้อมการตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ขาดการมีส่วนร่วมอย่างเหมาะสม

กฎหมายคุ้มครองข้อมูลส่วนบุคคลสหภาพยุโรป ตราขึ้นในสภาพแวดล้อมที่ขาดการมีส่วนร่วมอย่างเหมาะสม โดยจำแนกเป็นสองระดับ คือ 1) ระดับกระบวนการตรากฎหมาย กฎหมายฉบับนี้ได้รับการวิพากษ์วิจารณ์ว่า ตราขึ้นในระหว่างช่วงเวลาที่ผู้มีสิทธิออกเสียงไม่ได้มีส่วนร่วมอย่างเหมาะสม (Voter Disengagement) (Curtice, 2016) กล่าวคือ ผู้มีส่วนร่วมออกเสียงในสภายุโรปลดลงจากร้อยละ 62 ในปี ค.ศ. 1979 เหลือร้อยละ 42 ในปี ค.ศ. 2014 (European Parliament, 2018) ดังนั้น แม้ว่ากฎหมายจะผ่านด้วยเสียงข้างมาก แต่ก็อยู่ในสภาวะเสียงข้างมากที่กระจัดกระจายและไม่ได้มาจากการมีส่วนร่วมอย่างเหมาะสม (diffuse, disgruntled, and unorganized majority) 2) ระดับของการมีส่วนร่วมจากประชาชน พบว่า ประชาชนยุโรปเพียงจำนวนน้อยที่ตระหนักถึงการตรากฎหมายนี้ เช่น

ผลสำรวจในสหราชอาณาจักร พบว่า ร้อยละ 34 ของประชาชนรับรู้ถึงกฎหมาย GDPR (Cooke, 2018) ผลสำรวจยังชี้ให้เห็นว่า ประชาชนยุโรปประสงค์ที่จะให้มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลในระดับประเทศของตนมากกว่าในระดับกฎหมายสหภาพยุโรป (Layton and Celant, 2017)

ผลการเปรียบเทียบกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พบว่า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ตราขึ้นในช่วงเวลาที่รีบเร่ง และขาดการมีส่วนร่วมที่เหมาะสมในสองระดับ คล้ายคลึงกับกฎหมายสหภาพยุโรป กล่าวคือ คณะรัฐมนตรี เสนอร่างกฎหมายดังกล่าวเข้าสู่สภานิติบัญญัติแห่งชาติปลายปี พ.ศ. 2561 และสภาดังกล่าวลงมติผ่านกฎหมายในช่วงปลายเดือนกุมภาพันธ์ พ.ศ. 2562 ก่อนการเลือกตั้งทั่วไปเดือนมีนาคม พ.ศ. 2563 เพียงไม่ถึงหนึ่งเดือน แม้ว่ากฎหมายดังกล่าวดำเนินการตามกระบวนการ เช่น มีการจัดรับฟังความคิดเห็นสาธารณะถูกต้องตามแบบพิธีของการตรากฎหมาย แต่จากสภาพแวดล้อมดังกล่าวจะเห็นได้ว่าร่างกฎหมายถูกผลักดันจากหน่วยงานรัฐที่เสนอกฎหมาย และไม่ได้ผ่านการพิจารณาจากสภาที่มาจากการเลือกตั้งของประชาชน

จะเห็นได้ว่ากฎหมายสหภาพยุโรป (GDPR) เป็นกฎหมายใหม่ที่เพิ่งมีผลใช้บังคับในปี ค.ศ. 2018 องค์ประกอบ และเงื่อนไขหลายประการส่งผลกระทบทางลบหลายแง่มุม รวมทั้งยังขาดแนวปฏิบัติและแนวคำวินิจฉัยตลอดจนแนวทางลดผลกระทบดังกล่าว การที่ฝ่ายบริหารและฝ่ายนิติบัญญัติของไทยตรากฎหมายตามแนวทางกฎหมายสหภาพยุโรป โดยเร่งด่วนจึงนำไปสู่ผลกระทบในลักษณะเช่นเดียวกัน

สรุปผล

1. กฎหมายคุ้มครองข้อมูลส่วนบุคคลสหภาพยุโรป ส่งผลกระทบทางลบ 7 ด้าน ได้แก่ ภาระต้นทุนทางธุรกิจและการแข่งขันทางการค้าที่ไม่เป็นธรรม การสร้างโอกาสให้กับการโจมตีทางไซเบอร์และการโจรกรรมข้อมูลส่วนบุคคล ผลกระทบต่อเสรีภาพในการแสดงความคิดเห็น ผลกระทบอันเกิดจากการปฏิบัติเพื่อให้สอดคล้องกับกฎหมายด้วยวิธีการที่เกินไปกว่ากฎหมายกำหนด เพิ่มอำนาจรัฐในการควบคุมข้อมูล กฎหมายคุ้มครองข้อมูลส่วนบุคคลตราขึ้นในสภาพแวดล้อมที่ขาดการมีส่วนร่วมอย่างเหมาะสม

2. หลักกฎหมาย องค์ประกอบและเงื่อนไขของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของไทย คล้ายคลึงกับกฎหมายสหภาพยุโรป จึงส่งผลกระทบทางลบ 7 ด้าน ในลักษณะเดียวกับกฎหมายสหภาพยุโรป

3. จากผลกระทบทางลบทั้ง 7 ด้าน ผู้วิจัยจึงนำเสนอข้อเสนอแนะในหัวข้อต่อไป

ข้อเสนอแนะ

ข้อเสนอแนะเชิงนโยบาย

1. ข้อเสนอแนะในระยะสั้น เสนอให้ฝ่ายนิติบัญญัติยกเลิกพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อป้องกันผลกระทบดังเช่นกรณีตัวอย่างของสหภาพยุโรป

2. ข้อเสนอในระยะยาว เสนอให้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลขึ้นใหม่ หลังจากสหภาพยุโรปมีแนวทางแก้ปัญหาหรือลดผลกระทบทางลบด้านต่าง ๆ รวมทั้งรอระยะเวลาศึกษาการบังคับใช้ และแก้ปัญหาในระดับประเทศสมาชิกสหภาพยุโรป

ข้อเสนอแนะในการวิจัยครั้งต่อไป

เนื่องจากการวิจัยนี้มีขอบเขตเฉพาะการวิเคราะห์ผลกระทบทางลบ จากตัวบท เงื่อนไข และองค์ประกอบของกฎหมาย โดยยังมิได้ศึกษาในประเด็นการบังคับใช้กฎหมาย (Enforcement) จึงสามารถวิจัยครั้งต่อไปในเชิงปริมาณด้วยการทำแบบสอบถาม กลุ่มประชากรตัวอย่างที่ได้รับผลกระทบ

องค์ความรู้ใหม่

1. ผลการวิจัยพบว่า กฎหมายคุ้มครองข้อมูลส่วนบุคคลสหภาพยุโรป (GDPR) ส่งผลกระทบทางลบ 7 ด้าน

2. ผลการวิจัยพบว่า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีองค์ประกอบ เงื่อนไขคล้ายคลึงกับกฎหมายของสหภาพยุโรป จึงสามารถส่งผลกระทบทางลบได้ในลักษณะเดียวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลสหภาพยุโรป (GDPR)

3. ผลการวิจัยชี้ให้เห็นข้อเสนอแนะเชิงนโยบายทั้งในระยะสั้นและระยะยาว เพื่อลดผลกระทบทางลบของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

References

Arendt, H. (1973). *The Human Condition.* Chicago: University of Chicago Press.

Björn, G. (2018). *Study: Google Is the Biggest Beneficiary of the GDPR.* Retrieved March 22, 2020, from https://cliqz.com/en/magazine/study–google–is–the–biggest–beneficiary–of–the–gdpr

Bloustein, E. J. (1984). *Privacy as an Aspect of Human Dignity,* in Philosophical Dimensions of privacy: An Anthology, Schoeman, F. D. (ed.). Cambridge University Press, 156–202. https://doi.org/10.1017/CBO9780511625138.007

Campbell, J., Goldfarb, A., & Tucker, C. (2015). Privacy regulation and market structure. *Journal of Economics & Management Strategy, 24*(1), 47–73.

Cate, F. H. (1995). The EU Data Protection Directive, Information Privacy, and the Public Interest. *IOWA Law Review, 80*, 431–443.

Cooke, K. (2018). *Data Shows Awareness of GDPR Is Low amongst Consumers.* Retrieved March 5, 2020, from https://uk.kantar.com/public–opinion/policy/2018/data–shows–awareness–of–gdpr–is–low–amongst–consumers/

Curtice, J. (2016). *How Deeply Does Britain's Euroscepticism Run?.* Retrieved February 5, 2020, from https://www.bsa.natcen.ac.uk/media/39024/euroscepticism.pdf

Donnelly, J. (1982). Human Rights and Human Dignity. *The American Political Science Review, 76*(2), 303–316.

Epstein, A. R. (2018). A Not Quite Contemporary View of Privacy. *Harvard Journal of Public Policy, 41*(1), 94–116.

European Parliament. (2018). *Results of the 2014 European elections*. Retrieved March 12, 2020, from http://www.europarl.europa.eu/elections2014–results/en/turnout.html

Fromholz, J. M. (2000). The European Union data privacy directive. *Berkeley technology law journal, 15*(1), 460–484.

Good, O. S. (2018). *Super Monday Night Combat will close down, citing EU's new digital privacy law.* Retrieved February, 18, 2020, from https://www.polygon.com/2018/4/28 /17295498/super–monday–night–combat–shutting–down–gdpr

Henderson, L. (2018). *GDPR is being abused by cyber–criminals to breach complacent Businesses.* Retrieved March 15, 2020, from https://gdpr.report/news/2018/07/04/gdpr–is–being–abused–by–cyber–criminals–to–breach–complacent–businesses/

Kollmeyer, B. (2018). *Chicago Tribune, Los Angeles Times go dark in Europe after GDPR fail.* Retrieved February 18, 2020, from, https://www.marketwatch.com/story/chicago–tribune–la–times–go–dark–in–europe–after–gdpr–fail–2018–05–25#

Layton, R., & Celant, S. (2017). How the GDPR Compares to Best Practices for Privacy, Accountability and Trust. *SSRN,* 1–23. http://dx.doi.org/10.2139/ssrn.2944358

Layton, R. (2019). *The 10 Problems of the GDPR The US can learn from the EU's mistakes and leapfrog its policy*. Washington, D.C.: American Enterprize Institute.

Lyons, D. (2018). *GDPR: Privacy as Europe's Tariff by other means?.* Retrieved January 17, 2020, from http://www.aei.org/publication/gdpr–privacy–as–europes–tariff–by–other–means/

Martino, M. D., Robyns, P., Weyts, W., Quax, P., Lamotte, W., & Andries, K. (2019), Personal Information Leakage by Abusing the GDPR " Right of Access*". Proceedings of the Fifteenth Symposium on Usable Privacy and Security,* August 12–13, 2019 – Santa Clara, CA, USA. 371–386.

Rubenfield, J. (1989). The Right of Privacy. *Harvard Law Review, 102*(4), 737–807.

Russel, J. (2018). *RIP Klout.* Retrieved January 25, 2020, from https://techcrunch.com/2018/05 /10/rip–klout/

Schoeman, F. D. (1984). *Philosophical Dimensions of privacy: An Anthology*. UK: Cambridge University Press.

Scott, M., Cerulus, L., & Kayali, L. (2018). *Six months in, Europe's Privacy revolution favors Google, Facebook.* Retrieved February 15, 2020, from https://www.politico.eu/article/gdpr–facebook–google–privacy–data–6–months–in–europes–privacy–revolution–favors–google–facebook/

Shields, R. (2018). *Verve to focus on US growth as It plans closure of European offices ahead of GDPR.* Retrieved March 18, 2020, from https://www.thedrum.com/news/2018/04/18/verve–focus–us–growth–it–plans–closure–european–offices–ahead–gdpr

Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review, 154*(3), 477–560.

South, J. (2018). *More than 1,000 U.S. news sites are still unavailable in Europe, two months after GDPR took effect.* Retrieved March 5, 2020, from https://www.niemanlab.org/2018/08/more–than–1000–u–s–news–sites–are–still–unavailable–in–europe–two–months–after–gdpr–took–effect/

Spalter, J. (2018). *Broadband CapEx Investment Looking Up in 2017.* Retrieved March, 15, 2020, from https://www.ustelecom.org/broadband–capex–investment–looking–up–in–2017/

Tews, S. (2018). *How European Data Protection Law Is Upending the Domain Name System.* Retrieved February 22, 2020, from https://www.aei.org/publication/how–european– data–protection–law–is–upending–the–domain–name–system/

The International Association of Privacy Professionals (IAPP). (2018a). *European Commission sides with Google in RTBF Case.* Retrieved March 15, 2020, from https://iapp.org/news/a/ec–sides–with–google–in–rtbf–case/

The International Association of Privacy Professionals (IAPP). (2018b). *Global 500 companies to spend $7.8B on GDPR compliance.* Retrieved February 22, 2020, from https://iapp.org/news/a/survey

The Internet Corporation for Assigned Names and Numbers (ICANN). (2018). *Temporary Specification for gTLD Registration Data.* Retrieved March, 15, 2020, from https://www.icann.org/resources/pages/gtld–registration–data–specs–en

Thongraweewong, K. (2016). *Reform of Thai Personal Data Protection Law to enter the ASEAN Community.* Bangkok: The Secretariat of the House of Representatives.

Warren, D. S., & Brandies, L. D. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5), 193–220.

Westin, A. F. (1967). *Privacy and Freedom*. New York: Atheneum.

www.warportal.com. (2018). *Important Notice Regarding European Region Access*. Retrieved March 20, 2020, from http://blog.warpportal.com/?p=10892