ข้อพิจารณาการได้รับยกเว้นตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล : กรณีศึกษากฎหมายของสหราชอาณาจักร

CONSIDERATIONS FOR EXEMPTION FROM PERSONAL DATA PROTECTION LAWS: A CASE STUDY OF UK LAWS

รัฐสภา จุรีมาศ *
Rattasapa Chureemas

Received: 2021-10-15
Revised: 2021-12-22
Accepted: 2021-12-31

บทคัดย่อ

แนวคิดในการคุ้มครองข้อมูลส่วนบุคคลมีวัตถุประสงค์เพื่อคุ้มครองสิทธิส่วนบุคคลของประชาชนมิให้ถูกล่วงละเมิดในการเข้าถึง นำไปใช้ รวบรวมและตลอดจนจัดเก็บข้อมูลนั้น ๆ ภายใต้สิทธิในความเป็นส่วนตัว (Privacy) อันปราศจากการรบกวนและการแทรกแซงจากสังคม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จึงถูกตราขึ้นเพื่อวางมาตรการพิทักษ์สิทธิในข้อมูลส่วนบุคคลที่บุคคลใด ๆ ก็ตามจะเข้าถึง นำไปใช้ รวบรวมและจัดเก็บข้อมูลของบุคคลใดจะต้องได้รับการยินยอมจากผู้เป็นเจ้าของข้อมูลก่อน ทั้งนี้ ในบางกรณีจำเป็นต้องได้รับการยกเว้นจากขั้นตอนกระบวนการขอความยินยอมด้วยมีเหตุผลและความจำเป็นอย่างยิ่ง ดังที่ได้มีการตราข้อยกเว้นไว้ในมาตรา 4 ของพระราชบัญญัติดังกล่าว

อย่างไรก็ตาม กรณีที่ได้รับการยกเว้นนั้นจำเป็นอย่างยิ่งในฐานะกฎหมายกลางที่ต้องว่าแนวทางปฏิบัติในกรณีที่จะกระทำต่อข้อมูลส่วนบุคคลโดยปราศจากการปฏิบัติตามเงื่อนไขตามพระราชบัญญัตินั้น ซึ่งจากการศึกษาพบว่ายังไม่มีแนวทางที่ชัดเจนปรากฏในพระราชบัญญัติถึงมาตรการที่หน่วยงาน หรือ บุคคลที่ได้รับยกเว้นตามมาตรา 4 จะต้องดำเนินการหรือมีขั้นตอนอย่างใด ๆ ที่กำหนดไว้เพื่อป้องกันการกระทำโดยมิชอบ จากการศึกษาพระราชบัญญัติอำนาจในการสืบสวนสอบสวน (The Investigatory Powers Act 2016) และพระราชบัญญัติคุ้มครองข้อมูล (The Data Protection Act) กฎหมายของสหราชอาณาจักรพบวางมีการวางแนวทางขั้นต้น เพื่อป้องกันการอาศัยข้อยกเว้นตามกฎหมายในการกระทำต่อข้อมูลส่วนบุคคลโดยมิชอบ ผู้วิจัยเห็นว่าจะการศึกษานี้จะนำไปสู่การสร้างเป็นแนวทางในการพัฒนากฎหมายกลางในการคุ้มครองข้อมูลส่วนบุคคลได้ดียิ่งขึ้นต่อไป

คำสำคัญ: คุ้มครองข้อมูลส่วนบุคคล, สิทธิส่วนบุคคล, ข้อยกเว้น

* อาจารย์ประจำหลักสูตรนิติศาสตรบัณฑิต คณะสังคมศาสตร์ มหาวิทยาลัยศรีนครินทรวิโรฒ, เบอร์โทร: 089-027-8787, E-mail: Rattasapa@g.swu.ac.th

ABSTRACT

The concept of personal data protection aims to protect the privacy rights of people in order to not to be harassed in accessing, using, collecting and as well as storing such information under the right to privacy without interference and interference from society. The Personal Data Protection Act B.E. 2562 is enacted to put in place measures to protect the rights of personal data that any person will access, use, collect and store information of any person must obtain the consent of the owner. In some cases, it is necessary to be exempt from the consent process by reason and the absolute necessity. As an exception enacted in Section 4 of the Act.

However, exemption cases are essential, as the federal law should provide guidelines for dealing with personal data without fulfilling the requirements of the Act. From the study, it was found that there is no clear guideline in the Act regarding the measures that any state authority or persons who are exempted under Section 4 to have any duty or processed to prevent from wrongdoing. A study of The Investigatory Powers Act 2016 and The Data Protection Act, UK law found a preliminary orientation. To prevent reliance on legal exceptions to misuse personal data. The researcher believes that this study will lead to the creation of a guideline to develop a central law to better protect personal data.

Keywords: Personal Data Protection, Rights of Privacy, Exemption

1. บทนำ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act B.E. 2562 (2019) หรือ PDPA) กำหนดสาระสำคัญของพระราชบัญญัติฉบับดังกล่าวคือการวางมาตรการในการให้ความคุ้มครองการใช้ข้อมูลส่วนบุคคล อาทิ ข้อมูลการศึกษา ข้อมูลฐานะการเงิน ข้อมูลประวัติสุขภาพ ข้อมูลประวัติอาชญากรรม ข้อมูลประวัติการทำงาน และข้อมูลส่วนบุคคลอื่น ๆ ไม่ว่าจะเป็น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียง เลขบัตรประชาชน หรือเลขหมายเอกสารส่วนตัวอื่น ๆ โดยกำหนดห้ามไม่ให้ผู้อื่น หรือหน่วยงานอื่นใด ตลอดจนหน่วยงานรัฐ นำข้อมูลดังกล่าวไปใช้เพื่อประโยชน์ในด้านใดด้านหนึ่งที่เจ้าของข้อมูลไม่ยินยอมให้นำไปใช้ประโยชน์

ปัจจุบันการติดต่อกับหน่วยงานและองค์กรต่าง ๆ ทั้งภาครัฐและเอกชน ต้องดำเนินการผ่านทางการใช้ข้อมูลส่วนบุคคล ซึ่งทำให้บุคคลจำเป็นต้องเปิดเผยข้อมูลดังกล่าวต่อบุคคลหรือหน่วยงานนั้น ๆ ทั้งที่ยินยอมหรือไม่ยินยอมในการให้ข้อมูลดังกล่าว โดยเฉพาะอย่างยิ่งในการทำธุรกรรมต่าง ๆ เช่น การเปิดบัญชีเงินฝากกับสถาบันการเงิน จำเป็นต้องให้ข้อมูลส่วนตัวทั้งสำเนาบัตรประชาชน ที่อยู่ เบอร์โทรศัพท์เพื่อการติดต่อ อย่างไรก็ตามข้อมูลดังกล่าวไม่ได้ถูกจำกัดเฉพาะกับบุคคลผู้รับข้อมูลเพียงผู้เดียว แต่กลับมีการนำข้อมูลดังกล่าวไปดำเนินการใช้ในเชิงพาณิชย์ ซึ่งถือเป็นการละเมิดสิทธิส่วนบุคคล กฎหมายคุ้มครองข้อมูลส่วนบุคคลจึงเข้ามามีบทบาทแก้ไขปัญหาโดยกำหนดให้องค์กรหรือหน่วยงานที่เกี่ยวข้องที่เก็บข้อมูลส่วน

บุคคลของประชาชนไม่ว่าจะเป็นบริษัทเอกชน หรือหน่วยงานภาครัฐ ต้องไม่นำเอาข้อมูลส่วนตัวของเราไปใช้ในกิจกรรมอื่น ๆ ที่เราไม่ยินยอม

อย่างไรก็ตาม กฎหมายฉบับดังกล่าวยังมีประเด็นที่ต้องพิจารณาถึงความเหมาะสมในการบังคับใช้กฎหมายฉบับนี้ว่า เป็นไปตามวัตถุประสงค์ของกฎหมายอย่างแท้จริงหรือไม่ ดังจะเห็นได้จากข้อกำหนดการยกเว้นการบังคับใช้ของกฎหมายฉบับนี้ในมาตรา 4 ที่กำหนดให้การกระทำบางประการของหน่วยงานรัฐไม่อยู่ภายใต้การคุ้มครองข้อมูลส่วนบุคคล อาทิ การเก็บข้อมูล การใช้ข้อมูล และการเปิดเผยข้อมูล เพื่อประโยชน์ของตัวเองหรือกิจกรรมในครอบครัวหรือ การดำเนินงานของหน่วยงานของรัฐที่มีหน้าที่รักษาความมั่นคงของรัฐ ซึ่งรวมถึง ความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับ การป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์หรือ การเปิดเผยข้อมูลส่วนบุคคลเพื่อกิจการสื่อมวลชน ศิลปกรรม หรือวรรณกรรม ตามจริยธรรมของวิชาชีพหรือเป็นประโยชน์สาธารณะหรือ การทำงานของสภาผู้แทนราษฎร วุฒิสภา และรัฐสภา ในการพิจารณาตามอำนาจหน้าที่ การพิจารณาคดีของศาล และเจ้าหน้าที่ในกระบวนการยุติธรรม และการดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิก

จากกรณีดังกล่าว ยังเป็นช่องโหว่ทางกฎหมายที่ไม่เป็นไปตามวัตถุประสงค์ของการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ดังเช่นกฎหมายในลักษณะเดียวกันในต่างประเทศที่แม้จะมีข้อยกเว้นในลักษณะทำนองเดียวกัน แต่กำหนดหลักเกณฑ์ เงื่อนไข และขั้นตอน วิธีการต่าง ๆ เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลยังคงมีความชัดเจนตามวัตถุประสงค์ของกฎหมาย

อย่างไรก็ตามปัญหาสำคัญของการเข้าถึงข้อมูลส่วนบุคคลมีนั้น การอนุญาตให้รัฐกระทำการดังกล่าวย่อมเสมือนเป็นการยอมรับการให้อำนาจแก่รัฐในการล่วงล้ำถึงข้อมูลส่วนบุคคลอย่างไม่เหมาะสม อันเป็นสิทธิเสรีภาพของประชาชนขั้นพื้นฐานในการที่จะติดต่อสื่อสารระหว่างกัน ฉะนั้น จึงกล่าวได้ว่าเป็นการกระทำที่กระทบต่อสิทธิส่วนบุคคลอันเป็นหนึ่งในหลักสิทธิมนุษยชนซึ่งได้รับรองโดยองค์การสหประชาชาติ ที่จะต้องได้รับความคุ้มครอง หรือกระทำการภายใต้การควบคุมอย่างเคร่งครัด ฉะนั้นในการที่รัฐกระทำการเพื่อเข้าถึงหรือได้มาซึ่งข้อมูลที่บุคคลสื่อสารกันจำเป็นต้องมีกฎหมายกำหนดไว้เป็นการเฉพาะและต้องดำเนินการตามวัตถุประสงค์เฉพาะกาลตามกฎหมายและขั้นตอนตามที่กฎหมายกำหนดไว้อย่างเคร่งครัดด้วย ตลอดจนบทลงโทษของผู้กระทำการล่วงละเมิดข้อมูลดังกล่าวโดยมิชอบด้วยกฎหมายด้วย

ดังนั้น การหาแนวทางแก้ไขด้วยการกำหนดนโยบายทางกฎหมาย เช่น การบังคับใช้กฎหมายเพื่อคุ้มครองและควบคุมการเข้าถึงข้อมูลจึงเป็นเรื่องจำเป็นอย่างยิ่ง หรือการหาแนวทางป้องกันการเข้าถึงรหัสข้อมูลส่วนบุคคล ย่อมเป็นการแก้ไขปัญหาที่สมดุลกัน ทั้งนี้ ในหลายประเทศรวมทั้งสหราชอาณาจักรได้กำหนดกฎหมายที่เกี่ยวข้องในการให้อำนาจหรือรับรองอำนาจแห่งรัฐในการเข้าถึงข้อมูลของบุคคลส่วนบุคคลตลอดจนสิทธิในการสอดแนม (Surveillance) ข้อมูลดังกล่าวด้วย ซึ่งกำหนดไว้ในกระบวนการสอบสวนและสืบสวน (Investigatory Powers) โดยเจ้าพนักงานของรัฐที่เกี่ยวข้อง ซึ่งมีอำนาจในการออกคำสั่งให้มีการดักข้อมูล การบันทึกข้อมูล และการถอดความที่มีการสื่อสารทางโทรคมนาคม รวมถึงการสืบสวนคดีอาชญากรรมของหน่วยงานอื่นซึ่งบังคับใช้กฎหมายด้วยนั้น อาจมีความจำเป็นต้องได้รับการอนุญาตโดยกำหนดบุคคลซึ่งมีคุณสมบัติเฉพาะเพื่อให้สามารถเข้าถึงข้อมูลนี้ได้โดยตรง

การศึกษาวิจัยฉบับนี้ มุ่งเน้นการศึกษาผลกระทบต่อการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ผลกระทบต่อการกำหนดให้มีการยกเว้นการเข้าถึงข้อมูลโดยปราศจากความยินยอมโดยปราศจากหลักเกณฑ์ ขั้นตอน หรือวิธีการที่เหมาะสม และการศึกษามาตรการของสหราชอาณาจักรตามกฎหมายว่าด้วย The Investigatory Powers Act 2016 (IPA) และพระราชบัญญัติคุ้มครองข้อมูล (The Data Protection Act) ที่มีส่วนสัมพันธ์กันในบางประเด็น เพื่อให้เกิดข้อเสนอแนะเบื้องต้นในการกำหนดอำนาจของรัฐ และขั้นตอนอันควรมีเพื่อเข้าถึงข้อมูลส่วนบุคคลของประชาชน

2. วัตถุประสงค์ของการวิจัย

2.1 เพื่อศึกษาแนวคิดและทฤษฎีของการคุ้มครองข้อมูลส่วนบุคคล และการให้อำนาจรัฐเพื่อเข้าถึงข้อมูลส่วนบุคคล

2.2 เพื่อศึกษาผลกระทบต่อการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ผลกระทบต่อการกำหนดให้มีการยกเว้นการเข้าถึงข้อมูลโดยปราศจากความยินยอมโดยปราศจากหลักเกณฑ์ ขั้นตอน หรือวิธีการที่เหมาะสม

2.3 เพื่อศึกษาการให้อำนาจรัฐเพื่อเข้าถึงข้อมูลส่วนบุคคลแนวทางปฏิบัติในสหราชอาณาจักร

2.4 เพื่อศึกษาวิเคราะห์หลักเกณฑ์ของสหราชอาณาจักรในการสร้างแนวทางหรือเสนอแนะข้อพึงกำหนดเบื้องต้นในการให้อำนาจรัฐเพื่อเข้าถึงข้อมูลส่วนบุคคลของประเทศไทยอย่างเหมาะสม

3. วิธีดำเนินการวิจัย

3.1 รูปแบบการวิจัย

ในการศึกษาวิจัยฉบับนี้ใช้วิธีการวิจัยเชิงคุณภาพ (Qualitative Research) และวิจัยเอกสาร (Documentary Research) โดยทำการวิจัยจากเอกสาร การค้นคว้ารวบรวมจากหนังสือ ตำรา วารสารทางกฎหมาย บทความทางวิชาการจากวารสารทางวิชาการต่างๆ คำพิพากษาศาลฎีกา หนังสือพิมพ์ รายงานการวิจัย ผลงานการศึกษาวิจัยของนักวิชาการผู้ทรงคุณวุฒิ วิทยานิพนธ์ และรวมถึงข้อมูลทางสื่ออิเล็กทรอนิกส์ทั้งข้อมูลภายในประเทศและต่างประเทศ ที่เกี่ยวข้องกับสภาพปัญหาและแนวคิดของการให้อำนาจรัฐเพื่อเข้าถึงหรือได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกัน โดยเฉพาะกฎหมาย Investigatory Power Act 2016 และพระราชบัญญัติคุ้มครองข้อมูล (The Data Protection Act) ของสหราชอาณาจักร โดยผู้วิจัยทำการรวบรวมข้อมูลดังกล่าว วิเคราะห์ข้อมูลเพื่อศึกษาเปรียบเทียบ และนำเสนอโดยวิธีการพรรณนา (Descriptive)

3.2 เครื่องมือการวิจัย

1. เอกสารทางวิชาการ หนังสือ ตำรา บทความ คำพิพากษาฎีกา เกี่ยวกับการการคุ้มครองข้อมูลส่วนบุคคลและการให้อำนาจรัฐเข้าถึงข้อมูลส่วนบุคคล

2. แนวคิดและแนวทางการบังคับใช้กฎหมายในการคุ้มครองข้อมูลส่วนบุคคลและการให้อำนาจรัฐเพื่อเข้าถึงข้อมูลส่วนบุคคลของสหราชอาณาจักร

3. วิเคราะห์หลักเกณฑ์ของสหราชอาณาจักรในการดำเนินการเข้าถึงข้อมูลส่วนบุคลโดยชอบด้วยกฎหมาย

3.3 ขอบเขตของการวิจัย

งานวิจัยฉบับนี้ผู้วิจัยมุ่งเน้นในการศึกษาแนวคิดและทฤษฎีของการคุ้มครองข้อมูลส่วนบุคคลและการให้อำนาจรัฐเพื่อเข้าถึงข้อมูลส่วนบุคคล ตลอดจนผลกระทบต่อการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยเฉพาะอย่างยิ่งผลกระทบต่อการกำหนดให้มีการยกเว้นการเข้าถึงข้อมูลโดยปราศจากความยินยอมโดยปราศจากหลักเกณฑ์ ขั้นตอน หรือวิธีการที่เหมาะสม ศึกษาเปรียบเทียบและวิเคราะห์การให้อำนาจรัฐเพื่อเข้าถึงข้อมูลส่วนบุคคลและแนวทางปฏิบัติในสหราชอาณาจักร ภายใต้ความคุ้มครองความเป็นส่วนตัวของบุคคล (Data Privacy) The Investigatory Power Act 2016 และพระราชบัญญัติคุ้มครองข้อมูล (The Data Protection Act) เพื่อวิเคราะห์หลักเกณฑ์ของสหราชอาณาจักรในการสร้างแนวทางหรือเสนอแนะข้อพึงกำหนดในการให้อำนาจรัฐเพื่อเข้าถึงข้อมูลส่วนบุคคลของประเทศไทยอย่างเหมาะสมต่อไป เพื่อวางแนวทางในการป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยมิชอบ

4. ผลการวิจัย

เมื่อพิจารณาเจตนารมณ์หลักในการคุ้มครองข้อมูลส่วนบุคคลตามหลักสากลและตามเหตุผลของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีเจตจำนงหลักเพื่อเป็นกฎหมายกลางในการให้ความคุ้มครองการถูกละเมิดต่อข้อมูลส่วนบุคคลของประชาชนที่เกิดขึ้นอยู่ในปัจจุบัน โดยประชาชนผู้เป็นเจ้าของข้อมูลย่อมมีสิทธิที่จะยินยอม หรือปฏิเสธ ตลอดจนเพิกถอนความยินยอม จากการดำเนินการเข้าถึงข้อมูลส่วนบุคคลของตนได้ ฉะนั้น การกำหนดหลักเกณฑ์และมาตรการต่าง ๆ จึงควรกำหนดให้ประชาชนผู้เป็นเจ้าของข้อมูลส่วนบุคคลได้รับความคุ้มครองอย่างสูงสุด อย่างไรก็ตามจากการศึกษาพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ปรากฏว่ามีการกำหนดข้อยกเว้นบางประการ[1] ที่ผู้วิจัยเห็นว่าควรได้รับการ

[1] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กล่าวคือ “มาตรา 4 พระราชบัญญัตินี้ไม่ใช้บังคับแก่

(1) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น

(2) การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์

(3) บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมไว้เฉพาะเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น

(4) สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าวซึ่งเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎรวุฒิสภา รัฐสภา หรือคณะกรรมาธิการแล้วแต่กรณี

(5) การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

(6) การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

การยกเว้นไม่ให้นำบทบัญญัติแห่งพระราชบัญญัตินี้ทั้งหมดหรือแต่บางส่วนมาใช้บังคับแก่ผู้ควบคุมข้อมูลส่วนบุคคลในลักษณะใด กิจการใด หรือหน่วยงานใดทำนองเดียวกับผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง หรือเพื่อประโยชน์สาธารณะอื่นใด ให้ตราเป็นพระราชกฤษฎีกา

กำหนดให้มีแนวปฏิบัติจากการได้รับการยกเว้นเพื่อดำเนินการบางอย่างตามเหตุผลและความจำเป็นที่ไม่ต้องดำเนินการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อให้สอดคล้องต่อเจตนารมณ์หลักของพระราชบัญญัติดังกล่าวมีวัตถุประสงค์เพื่อเป็นกฎหมาย ระเบียบ ข้อบังคับกลางที่กำหนดให้หน่วยงานรัฐเอกชนต่าง ๆ ต้องปฏิบัติตาม

ทั้งนี้ จากการศึกษากฎหมายของสหราชอาณาจักรพบว่า ได้มีการกำหนดแนวทางและมาตรการในการกำกับดูแลการกระทำที่ได้รับยกเว้นให้ไม่ต้องปฏิบัติตาม The Investigatory Powers Act 2016 และ Personal Data Protection Act 2018 อย่างเป็นระบบขั้นตอนและรูปธรรม กล่าวคือ

1. ภายใต้แนวคิดและทฤษฎีของการคุ้มครองข้อมูลส่วนบุคคล และการให้อำนาจรัฐเพื่อเข้าถึงข้อมูลส่วนบุคคลของสหราชอาณาจักรตาม The Investigatory Powers Act 2016 มีกรณีกำหนดเหตุจำเป็นอย่างยิ่งที่หน่วยงานรัฐสามารถเข้าถึงข้อมูลส่วนบุคคลเพื่อรวบรวมได้โดยปราศจากความยินยอมตามความในมาตรา 24 ไม่อาจรอกระบวนการออกหมายตามขั้นตอนเพื่อดำเนินการเข้าถึงข้อมูล และต้องปรากฏว่าเป็นกรณีมีเหตุคุกคามต่อชีวิตหรืออาชญากรรมร้ายแรง[2] พระราชบัญญัติฉบับนี้กำหนดให้สามารถดำเนินการได้โดยไม่ต้องผ่านกระบวนการพิจารณาของศาลตามมาตรา 23 ดังเช่นกรณีทั่วไป ซึ่งโดยปกติต้องได้รับความเห็นชอบจากศาลเสียก่อนจึงจะออกหมายใช้แก่กรณีต่าง ๆ ได้ อย่างไรก็ตาม กฎหมายกำหนดว่าแม้จะอนุญาตให้สามารถดำเนินกระบวนการไปโดยไม่ผ่านขั้นตอนการพิจารณาของศาลแล้วนั้น หากแต่ต้องนำหมายมายื่นให้ศาลพิจารณาภายใน 3 วันนับแต่วันที่ออกหมายในกรณีเร่งด่วน ซึ่งหากศาลพิจารณาเห็นชอบการบังคับใช้หมายก็สามารถดำเนินการต่อไปได้ แต่หากปรากฏแก่กรณีว่าศาลพิจารณาไม่เห็นชอบกระบวนการใด ๆ ที่ได้กระทำไปนั้น ศาลจะพิจารณาให้เก็บรักษาอย่างเป็นความลับและกระบวนการอื่น ๆ ที่อยู่ขณะนั้นหรือที่จะได้กระทำในอนาคตให้ยุติโดยเร็วที่สุด[3]

จะเห็นได้ว่าแม้มีกรณีกำหนดข้อยกเว้นการดำเนินการตามปกติของกฎหมายที่มีหลักเกณฑ์และขั้นตอนตาม The Investigatory Powers Act 2016 ที่ต้องดำเนินการตาม Code of Practice นั้น อย่างไรก็ตามการยกเว้นไม่ใช่การยกเว้นโดยสิ้นเชิงแต่มีกรอบและกระบวนการที่กำหนดให้บุคคลที่ดำเนินการรวบรวมข้อมูลดังกล่าวต้องดำเนินการภายหลังจากได้รับข้อมูลนั้น ๆ มาโดยทันที ทั้งนี้เพื่อเป็นการป้องกันการอาศัยข้อยกเว้นในการดำเนินการอย่างหนึ่งอย่างใดโดยมิชอบ

2. การให้อำนาจรัฐเพื่อเข้าถึงข้อมูลส่วนบุคคลแนวทางปฏิบัติในสหราชอาณาจักรตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล 2018 หรือ Data Protection Act (DPA) โดยกฎหมายฉบับนี้มีจุดประสงค์เพื่อช่วยให้บุคคลหรือประชาชนในสหราชอาณาจักร สามารถควบคุมข้อมูลส่วนบุคคลและปกป้องสิทธิของตนได้ โดยที่ DPA นี้ ครอบคลุมข้อมูลส่วนบุคคลตั้งแต่การสื่อสารในทางการตลาดไปจนถึงการบริหารการจัดการข้อมูล ซึ่ง DPA ให้อำนาจในการควบคุมและความรับผิดชอบ โดยหน่วยงานคุ้มครองข้อมูลของส

ผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง (2) (3) (4) (5) และ (6) และผู้ควบคุมข้อมูลส่วนบุคคลของหน่วยงานที่ได้รับยกเว้นตามที่กำหนดในพระราชกฤษฎีกาตามวรรคสอง ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานด้วย”

[2] Sára Gabriella Hoffman. **General Data Protection Regulation (GDPR) A Stripe guide to the European privacy and data protection changes**. [Online] Available from: https://stripe.com/us/guides/general-data-protection-regulation. [25 MAY 2020].

[3] Section 25 of Investigatory Powers Act 2016.

หราชอาณาจักร The Information Commissioner's Office (ICO) ที่มีบทบาทสำคัญหลายประการ เช่น การรับและตรวจสอบข้อร้องเรียนเกี่ยวกับการละเมิด DPA และการพัฒนาส่งเสริมแนวทางปฏิบัติเพื่อใช้ในการปกป้องข้อมูลและการให้คำแนะนำแก่สาธารณะ และให้คำปรึกษาแก่ธุรกิจและหน่วยงานสาธารณะเกี่ยวกับวิธีการปฏิบัติตาม DPA

ซึ่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (DPA) ได้มีหลักการสำหรับองค์กรหรือธุรกิจใด ๆ เพื่อหลีกเลี่ยงบทลงโทษและค่าปรับ โดยสอดคล้องกับมาตรา 5 ของ GDPA ซึ่งสามารถแบ่งออกเป็น 6 ข้อ ได้แก่

1) ดำเนินการตามกฎหมายและด้วยความโปร่งใส : โดยที่องค์กรต่าง ๆ จำเป็นต้องอยู่ภายใต้กฎหมาย GDPR ในการรวบรวมและใช้ข้อมูลส่วนบุคคล และจะต้องใช้ข้อมูลส่วนบุคคลในทางที่เป็นธรรมและไม่ก่อให้เกิดอันตรายหรือทำให้เข้าใจผิดต่อบุคคลอื่น

2) ใช้เพื่อวัตถุประสงค์ที่ระบุชัดเจนและถูกต้องตามกฎหมาย : การที่องค์กรใช้ข้อมูลเพื่อวัตถุประสงค์อื่นนอกเหนือจากที่ระบุไว้อาจเป็นการที่ขัดต่อกฎหมายและไม่สามารถทำได้ เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลหรือมีภาระผูกพันที่ชัดเจนที่กำหนดไว้ในกฎหมาย

3) ประมวลผลเฉพาะวัตถุประสงค์ในการรวบรวม ไม่ควรเก็บข้อมูลไว้มากกว่าที่ต้องการ : องค์กรสามารถรวบรวมข้อมูลให้เพียงพอเพื่อให้สามารถทำตามวัตถุประสงค์ตามที่ได้อำนาจมา แต่ข้อมูลควรเป็นข้อมูลที่เกี่ยวข้องกับวัตถุประสงค์เท่านั้น ไม่ควรเก็บข้อมูลไว้มากกว่าที่ต้องการ

4) บริษัทหรือองค์กรควรดำเนินการตามขั้นตอนที่เหมาะสมเพื่อให้แน่ใจว่าข้อมูลส่วนบุคคลที่เก็บไว้เป็นข้อมูลที่ถูกต้อง หากไม่ควรจะลบหรือแก้ไขโดยเร็วที่สุด

5) บริษัทหรือองค์กรไม่ควรเก็บข้อมูลส่วนบุคคลไว้นานเกินความจำเป็น ข้อมูลที่สามารถเก็บไว้นานได้หรือเป็นการเก็บถาวรจะต้องเป็นข้อมูลที่ได้รับอนุญาตเพื่อสาธารณประโยชน์หรือการวิจัยทางวิทยาศาสตร์หรือประวัติศาสตร์เท่านั้น

6) บริษัทหรือองค์กรต่าง ๆ จำเป็นต้องตรวจสอบให้แน่ใจว่าข้อมูลส่วนบุคคลที่ได้เก็บมาได้เหมาะสมหรือไม่ รวมถึงจะต้องมีการป้องกันการสูญเสีย การทำลายหรือความเสียหายจากอุบัติเหตุอีกด้วย

ทั้งนี้ นอกจากหลัก 6 ข้อที่กล่าวมาแล้วยังมีมาตรการพิเศษในการคุ้มครองทางกฎหมายที่เข้มงวดมากยิ่งขึ้นสำหรับข้อมูลที่เป็นข้อมูล “ละเอียดอ่อน” เช่น เชื้อชาติ ภูมิหลังทางชาติพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนา การเป็นสมาชิกสหภาพแรงงาน สุขภาพ พันธุศาสตร์ชีวิตทางเพศหรือรสนิยมทางเพศ และข้อมูลความผิดทางอาญา ซึ่งสิ่งนี้เรียกว่า “ข้อมูลหมวดหมู่พิเศษ” และข้อมูลดังกล่าวจะแตกต่างจากข้อมูลส่วนบุคคลอื่น ๆ เพราะไม่สามารถอ้างเหตุผลด้านผลประโยชน์ที่ชอบด้วยกฎหมายและใช้ข้อมูลหมวดหมู่พิเศษในการทำอะไรบางอย่าง เช่น เพื่อทำการตลาดสำหรับธุรกิจ บริษัทหรือองค์กรต่าง ๆ ต้องใช้ความระมัดระวังเป็นพิเศษเพื่อให้มั่นใจในความปลอดภัยของข้อมูลนี้

ในกรณีเพื่อวัตถุประสงค์ในการปกป้องความมั่นคงแห่งชาติ เช่น ภัยคุกคามที่เกี่ยวกับการพัฒนาเทคโนโลยีคอมพิวเตอร์[4] ตามมาตรา 26 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (DPA) ได้มีการกำหนดข้อยกเว้นสำหรับการที่จะต้องได้รับอนุญาตในการเข้าถึงข้อมูลตามที่ระบุไว้ใน GDPR ซึ่งก็คือ มาตรา

[4] Information Commissioner’s Office. **National security and defense**. [Online] Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/national-security-and-defence/. [30 MAY 2021].

26 (1) เพื่อวัตถุประสงค์ในการปกป้องความมั่นคงของชาติหรือ (2) วัตถุประสงค์ในการป้องกันความมั่นคงของชาติในประการอื่น และการได้รับข้อยกเว้น จะต้องทำด้วยความ "จำเป็น" เพื่อปกป้องความมั่นคงของชาติเท่านั้น โดยความจำเป็นนี้ก็คงยังเชื่อมโยงกับมาตรฐานสิทธิมนุษยชนอยู่ จึงคงต้องพิจารณาถึงผลกระทบที่เกิดขึ้นจริงเป็นกรณี ๆ ไป ซึ่งตามมาตรานี้การยกเว้นจะส่งผลให้

1) ยกเว้นหลักการคุ้มครองข้อมูลใด ๆ ที่ถูกระบุไว้ใน GDPR เพื่อให้สามารถเข้าถึงข้อมูลส่วนบุคคลเพื่อจุดประสงค์ด้านความมั่นคงของประเทศและเพื่อการป้องกันความมั่นคงของประเทศ

2) การยกเว้นสิทธิใด ๆ ของบุคคลที่พึงมีในข้อมูลส่วนบุคคลของตนในการเก็บรักษา หรือปกปิด เป็นต้น

3) ยกเว้นการรายงานในการละเมิดข้อมูลส่วนบุคคล

4) ข้อกำหนดบางประการระหว่างประเทศ

5) การที่ต้องปฏิบัติตามหน้าที่และอำนาจการบังคับใช้กฎหมายของคณะกรรมาธิการ

อย่างไรก็ตามในการได้รับข้อยกเว้น เพื่อวัตถุประสงค์ในการปกป้องความมั่นคงของชาติจำเป็นที่จะต้องตรวจสอบให้แน่ใจเสมอว่าการการเข้าถึงข้อมูลส่วนบุคคล ผู้ที่สามารถได้รับข้อยกเว้นจะต้องปฏิบัติตามหลักการคุ้มครองข้อมูลสิทธิและหน้าที่เพื่อปกป้องความมั่นคงของชาติภายใต้มาตรา 6 ของ GDPR ที่ได้กล่าวไว้ข้างต้น เช่น ในการประมวลผลนั้นจำเป็นสำหรับการปฏิบัติตามหน้าที่ทางกฎหมายที่มีผลบังคับใช้ และต้องทำให้ถูกต้องตามกฎหมายสำหรับการดำเนินการและได้ปฏิบัติตามเอกสารและภาระหน้าที่ด้านความรับผิดชอบอื่น ๆ ซึ่งจะต้องไม่ใช่การยกเว้นในลักษณะทั่วไป แต่ต้องเป็นลักษณะเฉพาะในขอบเขตที่จำเป็นเพื่อปกป้องความมั่นคงของชาติ โดยต้องสามารถชี้ให้เห็นความเชื่อมโยงที่ชัดเจนระหว่างการปฏิบัติตามข้อกำหนดเฉพาะและผลกระทบที่อาจเกิดขึ้นต่อความมั่นคงของชาติ และต้องบันทึกการใช้การยกเว้นและสามารถแสดงให้เห็นถึงความจำเป็นและความเป็นสัดส่วนโดยคำนึงถึงสิทธิของเจ้าของข้อมูลและผลประโยชน์ที่ชอบด้วยกฎหมาย[5]

หากพิจารณาในมาตรา 26 ของ DPA ที่เป็นข้อยกเว้นของการประมวลผลข้อมูลเพื่อวัตถุประสงค์ด้านความมั่นคงแห่งชาติ ต้องใช้ข้อบังคับพิเศษตามมาตรา 28 ของ DPA ที่จะต้องได้รับการอนุญาตให้ประมวลผลข้อมูลเพื่อป้องกันความมั่นคงแห่งชาติ และจำต้องตรวจสอบว่ามีการป้องกันสิทธิ์และเสรีภาพของเจ้าของข้อมูล[6] ซึ่งมาตรา 28 มีเงื่อนไขในการดำเนินการกล่าวคือ ห้ามมิให้ประมวลผลข้อมูลส่วนบุคคลประเภทพิเศษ ที่มีวัตถุประสงค์เพื่อป้องกันความมั่นคงของชาติหรือเพื่อวัตถุประสงค์ในการป้องกันประเทศและการป้องกันสิทธิและเสรีภาพของเจ้าของข้อมูลอย่างเหมาะสม และมาตรา 32 เป็นการรักษาความปลอดภัยของการประมวลผล แต่ไม่สามารถบังคับใช้กับผู้ควบคุมหรือผู้ประมวลผลได้ในกรณีที่เป็นการประมวลผลข้อมูลส่วนบุคคลที่มีวัตถุประสงค์ในการป้องกันความมั่นคงของชาติหรือวัตถุประสงค์ในการป้องกันประเทศ เมื่อมาตรา 32 ไม่สามารถบังคับใช้ได้กับผู้ควบคุมหรือผู้ประมวลผล จึงต้องใช้มาตรการรักษา

[5] Ibid.

[6] Information Commissioner's Office. **National security and defense**. [Online] Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/national-security-and-defence/. [30 MAY 2021].

ความปลอดภัยที่เหมาะสมกับความเสี่ยงภัยที่เกิดจากการประมวลผลข้อมูลส่วนบุคคล โดยผู้ควบคุมต้องดำเนินการตามมาตรการ กล่าวคือ

1) ป้องกันการประมวลผลโดยไม่ได้รับอนุญาตหรือการรบกวนระบบที่ใช้ในการเชื่อมต่อกับการประมวลผล

2) ตรวจสอบว่าสามารถได้รับข้อมูลที่แม่นยำจากการประมวลผล

3) ตรวจสอบระบบที่ใช้ในการเชื่อมต่อกับระบบที่ใช้ในการประมวลผลว่าถูกต้อง เมื่อมีการถูกรบกวน

4) ตรวจสอบว่าข้อมูลส่วนบุคคลที่เก็บรักษาไม่เสียหาย หากระบบเกิดการเชื่อมต่อผิดพลาด[7]

ข้อยกเว้นตามมาตรา 26 และมาตรา 28 จะมีผลบังคับใช้ต่อเมื่อมีความจำเป็นพอสมควรในการป้องกันความมั่นคงของชาติ เนื่องจาก ได้เชื่อมโยงกับมาตรฐานสิทธิมนุษยชนในความเป็นส่วนตัว กล่าวคือ การแทรกแซงสิทธิความเป็นส่วนตัวต้องมีความจำเป็นและเป็นไปตามหลักประชาธิปไตยเพื่อตอบสนองความต้องการของสังคม อีกทั้งข้อยกเว้นสามารถบังคับใช้กับการป้องกันข้อมูลจำนวนมากได้ โดยต้องพิจารณาเป็นกรณีไป โดยเฉพาะวัตถุประสงค์เพื่อความมั่นคงของชาติที่ยังไม่มีน้ำหนักมากที่จะทำการประมวลผลข้อมูลต้องพิจารณาถึงผลกระทบที่แท้จริงต่อความมั่นคงของชาติ หากพิจารณาแล้วเห็นว่าการปฏิบัติตามข้อกำหนด GDPR อย่างเหมาะสมก็จะไม่กระทบต่อความมั่นคงของชาติ ไม่จำเป็นต้องพิสูจน์ว่าการปฏิบัติตามข้อกำหนดจะนำไปสู่อันตรายหรือภัยคุกคาม เพียงแสดงให้เห็นว่ามีความเป็นไปได้ที่อาจเกิดผลเสียต่อความมั่นคงของชาติไม่ว่าทางตรงหรือทางอ้อม ยกตัวอย่างเช่น เสรีภาพในการให้ข้อมูล ซึ่งศาลมีความเห็นว่าผู้ก่อการร้ายอาจจูงใจให้ช่วยเหลือตนได้มาก จึงเป็นเหตุพอสมควรในการที่จะระงับข้อมูลที่อาจช่วยเหลือผู้ก่อการร้าย เมื่อข้อมูลดังกล่าวได้ถูกรวมเข้ากับข้อมูลอื่นๆ แต่ในกรณีที่ความมั่นคงของชาติอาจได้รับผลกระทบเพียงเล็กน้อยหรือข้อมูลไม่เกี่ยวข้องกับความมั่นคง ย่อมไม่เป็นเหตุให้ใช้บังคับข้อยกเว้นได้ [8]

3. สำหรับประเทศไทยได้กำหนดให้มีขั้นตอนและมาตรการในการดำเนินการต่อข้อมูลส่วนบุคคลของประชาชนในกรณีเป็นการกระทำต่อความมั่นคงปลอดภัยไซเบอร์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ซึ่งเป็นกฎหมายลำดับรองที่ใช้ควบคู่กับกรณียกเว้นตามมาตรา 4 (2) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ในประเด็นดังกล่าว กล่าวคือ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ.2562 มีระบบและกลไกในการขับเคลื่อนกฎหมายโดยการจัดการผ่านทางหน่วยงานภาครัฐ ซึ่งตามมาตรา 45 ของพระราชบัญญัติฉบับนี้ได้ระบุไว้ว่าหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้าง พื้นฐานสำคัญทางสารสนเทศ มีหน้าที่ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน ซึ่งได้ระบุหน้าที่ของหน่วยงานรัฐในการจัดการหรือควบคุมกำกับดูแลโดยหน่วยงานของรัฐได้จัดตั้งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ทั้งนี้กระบวนการในการจัดการของคณะกรรมการมีการจัดทำนโยบายและแผนว่าด้วยการ

---

[7]Legislation. **Data Protection Act 2018 (Article 28)**. [Online] Available from: https://www.legislation.gov.uk/ukpga/2018/12/section/28/enacted. [30 June 2021].

[8]Information Commissioner's Office. **National security and defense**. [Online] Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/national-security-and-defence/. [30 MAY 2020].

รักษาความมั่นคงปลอดภัยไซเบอร์เพื่อเสนอคณะรัฐมนตรีให้ความเห็นชอบและประกาศในราชกิจจานุเบกษา และจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแลหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนำไปใช้เป็นแนวทางในการจัดทำหรือนำไปใช้เป็นประมวลแนวทางปฏิบัติของตนเอง

กลไกหรือการดำเนินกระบวนการในการรับมือกับภัยคุกคามทางไซเบอร์ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศ ซึ่งในการดำเนินการป้องกัน รับมือ เพื่อลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้นตามมาตรา 60 มีการกำหนดลักษณะของภัยคุกคามทางไซเบอร์ตามระดับความรุนแรงเป็น 3 ระดับ กล่าวคือ

1) ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง หมายถึงภัยคุกคามทางไซเบอร์ในระดับที่ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ หรือ การให้บริการของรัฐนั้นด้อยประสิทธิภาพลง

2) ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หมายถึงภัยคุกคามทางไซเบอร์ที่มีจุดมุ่งหมายในการโจมตีโครงสร้างพื้นฐานสำคัญของประเทศให้เสียหายจนไม่สามารถทำงานหรือให้บริการได้

3) ภัยคุกคามทางไซเบอร์ในระดับวิกฤต หมายถึงภัยภัยคุกคามทางไซเบอร์ในระดับวิกฤติที่มีลักษณะ ล้มเหลวทั้งระบบจนรัฐไม่สามารถควบคุมการทำงานจากส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้ หรือ ทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขัน และอาจส่งผลกระทบต่อสวัสดิภาพของประชาชน กระทบต่อความสงบเรียบร้อย ทำให้ประเทศตกอยู่ในภาวะคับขัน มีการก่อการร้าย มีการทำสงคราม[9]

ทั้งนี้ ในการรับมือและบรรเทาความเสียหายจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรงตามมาตรา 65 มีอำนาจออกคำสั่งเฉพาะเท่าที่จำเป็นเพื่อป้องกันคุกคามทางไซเบอร์ให้บุคคล ผู้ครอบครอง ผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือผู้ดูแลระบบคอมพิวเตอร์ซึ่งมีเหตุอันเชื่อได้ว่าเป็นผู้เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ดำเนินการดังนี้

1) เฝ้าระวังคอมพิวเตอร์หรือระบบคอมพิวเตอร์ในช่วงระยะเวลาใดระยะเวลาหนึ่ง

2) ตรวจสอบคอมพิวเตอร์หรือระบบคอมพิวเตอร์เพื่อหาข้อบกพร่องที่กระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ วิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์

3) ดำเนินมาตรการแก้ไขภัยคุกคามทางไซเบอร์เพื่อจัดการข้อบกพร่องหรือกำจัดชุดคำสั่ง ไม่พึงประสงค์ หรือระงับบรรเทาภัยคุกคามทางไซเบอร์ที่ดาเนินการอยู่

4) รักษาสถานะของข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ด้วยวิธีการใด ๆ เพื่อดำเนินการ ทางนิติวิทยาศาสตร์ทางคอมพิวเตอร์

5) เข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบ คอมพิวเตอร์ที่เกี่ยวข้องเฉพาะเท่าที่จำเป็น เพื่อป้องกันภัยคุกคามทางไซเบอร์

ในกรณีมีเหตุจำเป็นที่จะต้องเข้าถึงข้อมูลเพื่อป้องกันชุดคำสั่งที่ไม่พึงประสงค์โดยการเข้าถึงข้อมูลของคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือ ข้อมูลอื่นที่เกี่ยวข้องกับระบบที่ต้องเข้าถึงข้อมูลเพื่อเป็นการ

[9] Acinfotec. **องค์กรต้องปรับตัวอย่างไร เมื่อ พ.ร.บ. ไซเบอร์ 2562 ประกาศใช้แล้ว**. [ออนไลน์] แหล่งที่มา: https://www.acinfotec.com/2019/07/23/thai-cyber-law-2562/. [24 พฤษภาคม 2564].

รับมือและบรรเทาความเสียหายจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรงตามมาตรา 65 ในกรณีที่มีความจำเป็นตาม (5) นี้เป็นกระบวนการดำเนินการที่ทำได้โดยคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์[10] มอบหมายให้เลขาธิการยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้เจ้าของกรรมสิทธิ์ ผู้ครอบครอง ผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือผู้ดูแลระบบคอมพิวเตอร์ตามวรรคหนึ่งดำเนินการตามคำร้อง ทั้งนี้ คำร้องที่ยื่นต่อศาลต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดบุคคลหนึ่งกำลังกระทำหรือจะกระทำการอย่างใดอย่างหนึ่งที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ซึ่งในการพิจารณาคำร้องให้ยื่นเป็นคำร้องไต่สวนคำร้องฉุกเฉินและให้ศาลพิจารณาไต่สวนโดยเร็ว ซึ่งมีระบบที่คล้ายคลึงกล่าวคือ ระบบ Double Lock System หรือ Safeguard ซึ่งเป็นมาตรการป้องกันการแทรกแซง หรือ ใช้อำนาจของรัฐมนตรีโดยมิชอบ ทั้งนี้ กระบวนการของศาลตาม (5) การพิจารณาคำร้องให้ยื่นเป็นคำร้องไต่สวนคำร้องฉุกเฉินและให้ศาลพิจารณาไต่สวนโดยเร็วซึ่งเป็นการไต่สวนโดยเร็วทำให้กระบวนการไต่สวนนั้นอาจเกิดความผิดพลาดมากกว่าการไต่สวนที่ผ่านพิจารณาก่อน

ในส่วนของภัยคุกคามทางไซเบอร์ในระดับวิกฤตเป็นกรณีที่เกิดความล้มเหลวทั้งระบบโดยรัฐไม่สามารถควบคุมการทำงานจากส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้ หรือ ทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขันนั้นพระราชบัญญัติไซเบอร์นี้จึงได้บัญญัติกฎหมายในมาตรา 67 ไว้เป็นกรณีที่เป็นภัยคุกคามระดับวิกฤต และมีความจำเป็นสามารถเข้าดำเนินการได้ทันทีโดยไม่ต้องรอหมายศาลเหมือนในส่วนของภัยคุกคามระดับร้ายแรง ซึ่งมีวิธีการโดยคณะกรรมการอาจมอบหมายให้เลขาธิการมีอำนาจดำเนินการได้ทันทีเท่าที่จำ เป็นเพื่อป้องกันและเยียวยาความเสียหายก่อนล่วงหน้าได้โดยไม่ต้องยื่นคำร้องต่อศาลแต่หลังจากการดำเนินการดังกล่าวให้แจ้งรายละเอียดการดำเนินการดังกล่าวต่อศาลที่มีเขตอำนาจทราบโดยเร็ว และให้เป็นหน้าที่และอำนาจของสภาความมั่นคงแห่งชาติ ในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ตามกฎหมายว่าด้วยสภาความมั่นคงแห่งชาติและกฎหมายอื่นที่เกี่ยวข้อง

ทั้งนี้ในเชิงปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์นั้นไม่เพียงแต่หน่วยงานรัฐที่พึงตระหนักและปฏิบัติตามแต่เป็นหน้าที่ของประชาชนทุกคนที่ต้องช่วยกันเฝ้าระวังภัยให้ข้อมูลที่เป็นประโยชน์และช่วยอำนวยความสะดวกต่อการทำงานของรัฐรวมถึงการให้เบาะแสเพื่อเป็นการป้องกันและสามารถแก้ไขอย่างทันท่วงทีในการป้องกันนี้เพื่อเป็นการปิดช่องโหว่ที่อาจส่งผลกระทบให้เกิดความเสียหายต่อประเทศชาติ ซึ่งในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศที่อยู่ในความดูแลและความคุ้มครองของหน่วยงานของรัฐ หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ถ้าในกรณีที่เกิดขึ้นนั้นให้หน่วยงานนั้นดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้องข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงานนั้นรวมถึงพฤติการณ์แวดล้อมของตน เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ หากผลการตรวจสอบปรากฏว่าเกิดขึ้นหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

[10] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 12 ในการดำเนินการตามหน้าที่และอำนาจของคณะกรรมการตามมาตรา 9 ให้มีคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรียกโดยย่อว่า “กกม.”

5. อภิปรายผลการวิจัย

จากการศึกษาการกำหนดข้อยกเว้นตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยที่พระราชบัญญัติดังกล่าวมีวัตถุประสงค์ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีเหตุผลอันเป็นสาระสำคัญคือ มีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อน รำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวกและรวดเร็ว ก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวม ฉะนั้น เห็นได้ว่าสาระสำคัญของพระราชบัญญัติคือการคุ้มครองข้อมูลส่วนบุคคลของประชาชนเพื่อป้องกันมิให้มีการเข้าถึง จัดเก็บ รวบรวม หรือนำข้อมูลส่วนบุคคลของประชาชนไปเผยแผ่หรือใช้โดยปราศจากความยินยอมของเจ้าของข้อมูลก่อน ตลอดจนมีสิทธิที่จะทราบได้ว่าในกรณีตนได้ให้ความยินยอมไปนั้นผู้ควบคุมหรือรวบรวมข้อมูลได้นำข้อมูลดังกล่าวไปใช้ด้วยเหตุผลหรือวัตถุประสงค์อย่างใด ๆ อย่างไรก็ตามปรากฏตามมาตรา 4 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้การกระทำในบางกรณีไม่อยู่ในบังคับที่ต้องปฏิบัติตามหลักเกณฑ์ เงื่อนไขและวิธีการตามพระราชบัญญัติดังกล่าว กล่าวคือ

กฎหมายได้เปิดช่องให้หน่วยงานรัฐนั้นสามารถเก็บข้อมูลได้โดยไม่ต้องบอกกล่าวขอความยินยอมจากบุคคลนั้น แม้ว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลนั้นมีหลักการคุ้มครองความเป็นส่วนตัวแต่ในขณะเดียวกันกฎหมายก็ได้กำหนดข้อยกเว้นในการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย หรือ การกระทำบางอย่างเกี่ยวกับข้อมูลส่วนบุคคลได้ หากพิจารณาจากมาตรา 4 (2) ได้กำหนดขอบเขตการบังคับตามบทบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักประกันสิทธิส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล โดยจะไม่ใช้บังคับแก่การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือ การรักษาความปลอดภัยของประชาชนรวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ การรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งการบัญญัติมาตรา 4 (2) นั้นนำไปสู่กรณีที่กฎหมายเปิดช่องให้หน่วยงานรัฐได้เข้ามาควบคุมข้อมูลส่วนบุคคลในมาตรา 24 (4) และ (6) ที่ระบุว่า ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลไม่ได้ ยกเว้นเป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือ ปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล หรือ เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

ดังนั้นมาตรการของหน่วยงานภาครัฐที่มีกฎหมายอื่นรองรับ เช่น พระราชบัญญัติข่าวกรอง พระราชบัญญัติสภาความมั่นคงแห่งชาติ หรือชุดกฎหมายความมั่นคง 3 ฉบับ กล่าวคือ กฎอัยการศึก พระราชกำหนดการบริหารราชการในยามฉุกเฉิน พระราชบัญญัติการรักษาความมั่นคงภายใน ซึ่งมีลักษณะเดียวกันนั้นย่อมเข้าตามลักษณะข้อยกเว้นตามความในมาตรา 4 ทำให้หน่วยงานรัฐสามารถสั่งให้ผู้ควบคุมระบบรวบรวมข้อมูลมาให้โดยไม่ต้องมีความยินยอมจากเจ้าของข้อมูล

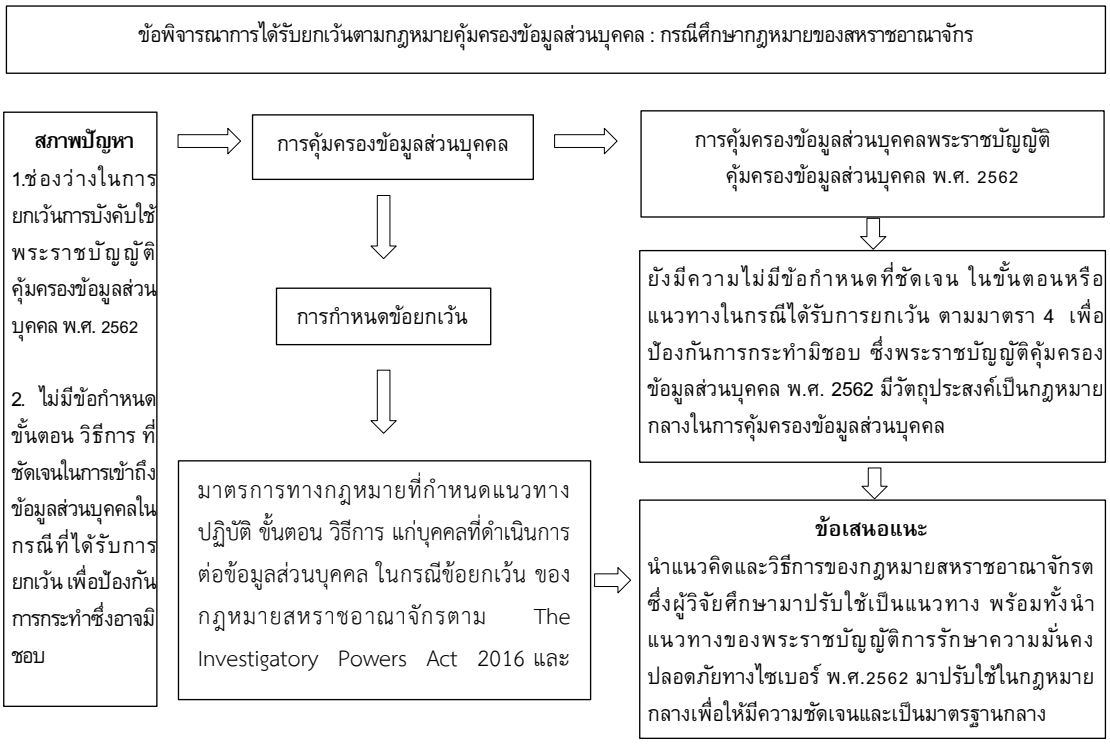
ซึ่งตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 นิยามในการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ได้กล่าวไว้ข้างต้นนั้นได้ให้คำนิยามที่ คลอบคลุมถึงมาตรา 4 ไว้กล่าวคือการดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลัง

ของรัฐ หรือ การรักษาความปลอดภัยของประชาชนรวมทั้งหน้าที่เกี่ยวกับ การป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังนั้นหน้าที่ของการป้องกันที่กล่าวไว้ในมาตรา 4 นั้นเป็นหน้าที่ที่พระราชบัญญัติไซเบอร์ได้กำหนดไว้ในกฎหมายฉบับนี้เช่นกัน อย่างไรก็ตามพระราชบัญญัติไซเบอร์นั้นไม่ได้ระบุหรือให้คำนิยามที่คลอบคลุมทุกเรื่องในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลในมาตรา 4 แต่มาตรา 4 บัญญัติให้ใช้ตามพระราชบัญญัติไซเบอร์ ซึ่งหากพิจารณาการบังคับใช้กฎหมายนี้จึงไม่มีกฎหมายกลางหรือกล่าวได้ว่าไม่มีกฎหมายที่เข้ามาคุ้มครองในลักษณะเฉพาะที่จะเข้ามาคุ้มครองข้อมูลการดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ

อย่างไรก็ตามกฎหมายนี้ที่ได้บัญญัติที่ออกมาควบคู่กับกฎหมายคุ้มครองข้อมูลส่วนบุคคล ซึ่งโดยหลักแล้วนั้นอาจมีความย้อนแย้งกัน เพราะการเข้าถึงหรือได้มาซึ่งข้อมูลส่วนบุคคลของผู้อื่นโดยไม่ได้รับความยินยอม เป็นความผิดตามกฎหมายคุ้มครองข้อมูลแต่กฎหมายนั้นก็ได้มีการกำหนดยกเว้นสำหรับการกระทำที่เกิดจากการใช้อำนาจโดยกฎหมายดังเช่นพระราชบัญญัติมั่นคงไซเบอร์แล้ว

นอกจากนี้ในการกำหนดให้บางกรณีที่ไม่ต้องอยู่ภายใต้การบังคับใช้ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้น หากพิจารณาจากกฎหมายพบว่าหากเป็นกรณีเพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้นตาม (1) ซึ่งมีเหตุผลรองรับเพราะเป็นกรณีใช้ข้อมูลเพื่อวัตุประสงค์ส่วนตนหรือกิจกรรมในครอบครัวย่อมไม่กระบทถึงสิทธิของบุคคลอื่น อย่างไรก็ตามพบว่าในกรณีอนุมาตราอื่นนั้นที่แม้จะมีการกำหนดให้ต้องมีการควบคุมความปลอดภัยข้อมูลดังกล่าวตามวรรค 2 ประกอบวรรค 3 โดยผู้ควบคุม

อย่างไรก็ตามกรณียกเว้นอื่น ๆ นั้น จากการศึกษาผู้วิจัยพบว่าแม้ในบางกรณีมีเหตุผลและความจำเป็นในการยกเว้นตามกฎหมายเฉพาะของเรื่องนั้น ๆ ควบคู่กับพระราชบบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แต่ในหลายฉบับยังมิได้มีการกำหนดมาตรการ เงื่อนไข ในการกำกับดูแลการเข้าถึงข้อมูล รวบรวมข้อมูล จัดเก็บข้อมูล หรือขั้นตอนพิเศษที่เรียกว่ามาตรการ Double Lock System อย่างเป็นระบบที่ชัดเจนเพื่อคุ้มครองการเข้าถึงได้มา รวบรวม จัดเก็บ ข้อมูลส่วนบุคคลของประชาชนโดยมิชอบ ดังที่ได้กำหนดวิธีการมาตรการ เงื่อนไข ตามแนวทาง The Investigatory Power Act หรือ The Data Protection Act หรือพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 หรือตามกฎหมายบางฉบับที่กำหนดขั้นตอนไว้ ผู้วิจัยจึงมีความเห็นว่าเพื่อให้กฎหมายดังกล่าวซึ่งมีวัตถุประสงค์ใช้อย่างกฎหมายกลางในการควบคุมการละเมิดข้อมูลส่วนบุคคลของประชาชนอย่างเต็มความสามารถนั้น จำเป็นอย่างยิ่งที่ต้องกำหนดให้มีแนวทางภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อเป็นข้อกำหนดกลางให้ทุกหน่วยงานที่เข้าข่ายการได้รับการยกเว้นตามมาตรา 4 ต้องปฏิบัติตามอย่างเสมอภาคและมุ่งคุ้มครองประชาชนอย่างแท้จริง



ภาพประกอบที่ 1: องค์ความรู้ใหม่ที่ได้จากงานวิจัย

6. ข้อเสนอแนะ

ผู้วิจัยมีข้อเสนอแนะต่อการจัดทำกฎหมายลำดับรอง หรือกำหนดเป็นตารางเงื่อนไขแนบท้ายกฎหมายเพื่อให้การเข้าถึงข้อมูล จัดเก็บข้อมูล หรือนำข้อมูลที่ได้มาไปใช้เพื่อประโยชน์ประการใดประการหนึ่งตามมาตรา 4 ที่ได้รับยกเว้นให้กระทำการต่อข้อมูลส่วนบุคคลได้ โดยไม่ต้องดำเนินการตามแนวทางของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้น ควรการกำหนดขั้นตอน วิธีการกลาง โดยอาจกำหนดมีกระบวนการ Double Lock System เพื่อให้เกิดความชัดเจนในการดำเนินการดังกล่าว และเพื่อป้องกันการดำเนินการอย่างใด ๆ ในทางที่ไม่ชอบเพื่อให้ได้มาซึ่งข้อมูล จัดเก็บ รวบรวม หรือนำไปใช้ในข้อมูลส่วนบุคคลนั้น ๆ โดยอาจดำเนินการในลักษณะตาม The Investigatory Power Act 2016 ในกรณีประสงค์เข้าถึงข้อมูลเพื่อการดำเนินการสอบสวน สืบสวนการกระทำความผิดอาญา หรือตามหลักแนวทางการดำเนินการภายใต้ข้อยกเว้นของ The Data Protection Act 2018 หรือพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ต่อข้อมูลดังกล่าวเพื่อดำเนินการตามวัตถุประสงค์ภายใต้ข้อยกเว้นนั้น ๆ

7. กิตติกรรมประกาศ

การวิจัยนี้สำเร็จลงได้ด้วยความช่วยเหลือของผู้มีส่วนสนับสนุน ทั้งข้อเสนอแนะ ข้อมูล เอกสารตำรา ต่าง ๆ จนเป็นผลสำเร็จ และขอขอบพระคุณคณะสังคมศาสตร์ มหาวิทยาลัยศรีนครินทรวิโรฒที่

สนับสนุนทุนวิจัยภายใต้โครงการวิจัยการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยต่อมาตรการของรัฐในการเข้าถึงข้อมูลของประชาชน : ศึกษาเปรียบเทียบกฎหมายของสหราชอาณาจักร ในครั้งนี้

เอกสารอ้างอิง

นคร เสรีรักษ์. **ความเป็นส่วนตัว: ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย**, เชียงใหม่. ฟ้าฮ่าม, 2557.

สุขวสา ถมังรักษ์สัตว์, “การคุ้มครองข้อมูลส่วนบุคคลของเด็กบนสื่ออิเล็กทรอนิกส์”. **วารสารเกษมบัณฑิต** ปีที่ 20 ฉบับที่ 1 (มกราคม- มิถุนายน 2562): 136 – 137.

Acinfotec. **องค์กรต้องปรับตัวอย่างไร เมื่อ พ.ร.บ. ไซเบอร์ 2562 ประกาศใช้แล้ว**. [ออนไลน์] แหล่งที่มา: https://www.acinfotec.com/2019/07/23/thai-cyber-law-2562/. [24 พฤษภาคม 2564].

Information Commissioner’s Office. **National security and defense**. [Online] Available from: https://ico. org.uk/fororganisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/national- security-and-defence/. [30 MAY 2021].

Legislation. **Data Protection Act 2018 (Article 28)**. [Online] Available from: https://www.legislation.gov.uk/ukpga/ 2018/12/section/28/enacted. [30 June 2021].

Sára Gabriella Hoffman. **General Data Protection Regulation (GDPR) A Stripe guide to the European privacy and data protection changes**. [Online] Available from: https://stripe.com/us/guides/general-data-protection- regulation. [25 MAY 2020].

Home Office. **Interception of Communication, Code of Practice**. Pursuant to Schedule 7 to the Investigatory Powers Act 2016, March 2018

Home Office. **National Security Notices, Code of Practice**. Pursuant to Schedule 7 to the Investigatory Powers Act 2016, March 2018

Ian J. **Lloyd. Information Technology Law, (Great Britain**. United Kingdom: Oxford University Press, 1 2017).

The Henry Jackson Society. **Investigatory Powers Review**. [Online] Available from: https://terrorismlegislationreviewer.independent.gov.uk/wpcontent/uploads/2015/06/Submissions-H-Z.pdf. [30 April 2021].