แนวทางการปรับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลกับกิจกรรมของรัฐที่ได้รับการยกเว้น
Guidelines for the Implementation of Personal Data Protection Laws with Exempted Government Activities

เขมภัทร ทฤษฎิคุณ[1]
Khemmapat Trisadikoon

บทคัดย่อ

สิทธิความเป็นส่วนตัวได้มีการรับรองไว้รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 มาตรา 32 โดยกำหนดหน้าที่ผูกพันให้รัฐต้องคุ้มครองรักษาสิทธิความเป็นส่วนตัวของประชาชน ซึ่งข้อมูลส่วนบุคคลเป็นส่วนหนึ่งของความเป็นส่วนตัวเป็นเหตุให้ในเวลาต่อมารัฐบาลจึงตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ขึ้นมา

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีสถานะเป็นกฎหมายทั่วไปในการคุ้มครองข้อมูลส่วนบุคคลโดยกำหนดหลักการคุ้มครองข้อมูลส่วนบุคคลทั้งในหน่วยงานของรัฐและเอกชนและไม่จำกัดว่าข้อมูลส่วนบุคคลดังกล่าวจะอยู่ในรูปแบบกระดาษหรือเป็นข้อมูลอิเล็กทรอนิกส์ อย่างไรก็ดี พระราชบัญญัติฉบับนี้ได้ยกเว้นไม่นำมาใช้บังคับกับกิจกรรมที่มีการประมวลผลข้อมูลส่วนบุคคลบางประเภท ซึ่งรวมถึงกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของหน่วยงานของรัฐในเรื่องการดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ และการพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญาตามมาตรา 4 (2) และ (5) โดยพระราชบัญญัติเพียงแต่กำหนดว่า หน่วยงานของรัฐจะต้องกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลสำหรับกิจกรรมที่ได้รับการยกเว้น ซึ่งอาจไม่เพียงพอต่อการบรรลุวัตถุประสงค์ในการคุ้มครองข้อมูลส่วนบุคคล

บทความนี้ต้องการศึกษาแนวทางการปรับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กับกิจกรรมของรัฐที่ได้รับการยกเว้นตามกฎหมาย และศึกษาแนวทางการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปและสหราชอาณาจักร ซึ่งเป็นต้นแบบในการยกร่างพระราชบัญญัติของไทยเพื่อนำแนวทางดังกล่าวมาเสนอแนะให้กับหน่วยงานของรัฐไทยใช้เป็นกรอบในการคุ้มครองข้อมูลส่วนบุคคลในกิจกรรมที่ได้รับยกเว้น

คำสำคัญ: กฎหมายคุ้มครองข้อมูลส่วนบุคคล, หน่วยงานด้านความมั่นคงของรัฐ, หน่วยงานบังคับใช้กฎหมาย

Abstract

The right to privacy is recognized and protected by the Constitution of the Kingdom of Thailand, B.E. 2560 (2017) in Article 32, which imposes an obligation on the state to safeguard and protect the privacy rights of individuals. Personal data is an integral part of privacy, which led to the enactment of the Personal Data Protection Act, B.E. 2562 (2019) by the government in the future.

The Personal Data Protection Act B.E. 2562 (2019) is a general law that governs the protection of personal data, both in public and private sectors, regardless of whether the personal data is in paper or electronic format. However, this law does not apply to certain types of personal data processing activities, including the processing of personal data by state agencies involved in the maintenance of state security, the adjudication of court cases, the execution of court orders, and the proceedings in criminal justice under Article 4 (2) and (5). The law merely requires state

[1] นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์, นักวิจัยอาวุโส สถาบันวิจัยเพื่อการพัฒนาประเทศไทย (ทีดีอาร์ไอ)
LL.M. at Thammasat University, Senior Researcher, Thailand Development Research Institute (TDRI)

agencies to establish data protection measures for exempted activities, which may not be sufficient to achieve the objectives of personal data protection.

This article aims to study the guidelines for implementing the Personal Data Protection Act B.E. 2562 (2019) in relation to exempted activities under the law, as well as to explore the guidelines for personal data protection under the data protection laws of the European Union and the United Kingdom, which serve as models for drafting Thai legislation. The objective is to provide recommendations for Thai government agencies to adopt these guidelines as a framework for protecting personal data in exempted activities.

Keywords: Personal Data Protection Law, National Security Authorities, Law Enforcement Authorities

บทนำ

การคุ้มครองข้อมูลส่วนบุคคลเป็นปัจจัยหลักที่นำไปสู่การรักษาสิทธิความเป็นส่วนตัว (right to privacy) เนื่องจากข้อมูลส่วนบุคคลเป็นสิ่งที่เน้นย้ำให้เห็นถึงความเป็นตัวตนและอัตลักษณ์ของบุคคล ซึ่งเมื่อถูกละเมิดแล้วจะกระทบต่อสิทธิความเป็นส่วนตัวของบุคคล หรือก้าวให้ถึงที่สุดกระทบต่อสิทธิในความเป็นตัวตนของมนุษย์คนนั้นๆ[2] อาทิ การล่วงรู้ความคิดเห็นทางการเมืองของบุคคลอาจจะนำไปสู่การเลือกปฏิบัติ (discrimination) หรือนำไปสู่การบังคับใช้กฎหมายเพื่อป้องกันความเห็นต่างทางการเมือง ซึ่งการกระทำดังกล่าวกระทบต่อตัวตนหรืออัตลักษณ์ของบุคคลนั้น ๆ ในกรณีเช่นนี้การคุ้มครองข้อมูลส่วนบุคคลจึงเป็นสิ่งจำเป็นที่รัฐต้องให้รัฐต้องคุ้มครองและรักษาข้อมูลส่วนบุคคลของประชาชนภายในรัฐโดยจัดให้มีบทบัญญัติของกฎหมายเพื่อมาคุ้มครอง ซึ่งกรณีของประเทศไทยคือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

บริบทของประเทศไทยนั้นคล้ายคลึงกับประเทศต่าง ๆ ในโลกที่มีการตรากฎหมายคือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ขึ้นมาเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวของบุคคลโดยการกำหนดสิทธิในข้อมูลส่วนบุคคลและกำหนดหลักเกณฑ์การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ซึ่งเรียกรวมกันว่าการประมวลผลข้อมูลส่วนบุคคล โดยพระราชบัญญัตินี้มีวัตถุประสงค์เพื่อเป็นกฎหมายทั่วไปที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคลโดยไม่จำกัดว่า กิจกรรมการประมวลผลข้อมูลส่วนบุคคลนั้นจะกระทำโดยหน่วยงานของรัฐหรือเอกชน และไม่ว่าข้อมูลนั้นจะถูกจัดเก็บอยู่ในรูปแบบกระดาษหรือไฟล์อิเล็กทรอนิกส์ อย่างไรก็ดี พระราชบัญญัติฉบับนี้ได้กำหนดข้อยกเว้นไม่ให้นำสิทธิและหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลไปใช้กับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ และการพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญาโดยจะเรียกรวมว่าหน่วยงานบังคับใช้กฎหมายตามมาตรา 4 (2) และ (5) ซึ่งการยกเว้นดังกล่าวทำให้หน่วยงานของรัฐที่ดำเนินกิจกรรมการประมวลผลข้อมูลส่วนบุคคลดังกล่าวมีหน้าที่เพียงรักษาความมั่นคงปลอดภัยของข้อมูลเท่านั้น[3] ซึ่งลักษณะดังกล่าวอาจทำให้เกิดช่องว่างในการบังคับใช้กฎหมายกับหน่วยงานของรัฐโดยหน่วยงานของรัฐอ้างประโยชน์เพื่อรักษาความมั่นคงปลอดภัยในการคุกคามสิทธิความเป็นส่วนตัวของประชาชนได้ ประกอบกับสถานการณ์ในช่วงที่ผ่านมาหน่วยงานของรัฐด้านความมั่นคงมีแนวโน้มที่จะคุกคามสิทธิความเป็นส่วนตัวของผู้มีความเห็นต่างทางการเมืองผ่านการสอดส่องการกระทำโดยรัฐดังกรณีที่มีการกล่าวหาจากนักกิจกรรมว่า หน่วยงานของรัฐด้านความมั่นคงสอดส่องนักกิจกรรมโดยใช้โปรแกรม สปายแวร์

---

[2] นคร เสรีรักษ์, *ความเป็นส่วนตัว: ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย* (พิมพ์ครั้งที่ 2 สำนักพิมพ์แพร่: พี.เพรส 2563) 62.

[3] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 4 วรรคสาม.

(spyware) ชื่อเพกาซัส (Pegasus)[4] ประกอบกับข้อยกเว้นที่กำหนดให้หน่วยงานของรัฐมีหน้าที่รับผิดชอบเฉพาะรักษาความมั่นคงปลอดภัยของข้อมูลเท่านั้นอาจกลายเป็นการส่งเสริมให้หน่วยงานของรัฐละเมิดสิทธิในข้อมูลส่วนบุคคลโดยปราศจากความรับผิดชอบและกลายเป็นการลอยนวลพ้นผิดไป สภาพดังกล่าวสะท้อนภาพของความไม่เพียงพอต่อการบรรลุวัตถุประสงค์ในการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และสิทธิความเป็นส่วนตัวที่รัฐธรรมนูญรับรองไว้ จึงสมควรที่จะต้องมีการกำหนดแนวทางการปรับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลกับกิจกรรมของหน่วยงานของรัฐที่ได้รับการยกเว้น เพื่อปิดช่องว่างของกฎหมายที่อาจนำไปสู่การละเมิดข้อมูลส่วนบุคคลและสิทธิความเป็นส่วนตัวโดยหน่วยงานของรัฐ

บทความนี้ประกอบด้วยเนื้อหา 4 ส่วน ได้แก่ (1) หลักการคุ้มครองข้อมูลส่วนบุคคลของไทย (2) ข้อยกเว้นการคุ้มครองข้อมูลส่วนบุคคลในกิจกรรมของรัฐที่ได้รับการยกเว้นตามกฎหมายไทย (3) แนวทางการคุ้มครองข้อมูลส่วนบุคคลของกิจกรรมของรัฐที่ได้รับการยกเว้นในต่างประเทศ และ (4) ข้อเสนอแนะในการปรับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลกับกิจกรรมของรัฐที่ได้รับการยกเว้น

1. หลักการคุ้มครองข้อมูลส่วนบุคคลของไทย

ก่อนหน้าการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การคุ้มครองข้อมูลส่วนบุคคลของไทยถูกกำหนดไว้ในกฎหมายหลายฉบับที่แตกต่างกัน อาทิ พระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ. 2540 ได้กำหนดหลักเกณฑ์การคุ้มครองข้อมูลข่าวสารส่วนบุคคล[5] ในความครอบครองของหน่วยงานของรัฐ ซึ่งในเวลาต่อมาได้มีแนวคิดที่จะกำหนดหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป ประกอบกับกระแสการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับอิทธิพลมาจากสหภาพยุโรปที่มีได้มีการตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation: GDPR) ซึ่งทำให้ประเทศไทยได้มีการยกร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่มี GDPR เป็นต้นแบบ[6]

การคุ้มครองข้อมูลส่วนบุคคลมีเป้าหมายสำคัญ 2 ประการ คือ ประการแรก การคุ้มครองสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคล (data subject) โดยกำหนดสิทธิให้กับเจ้าของข้อมูลส่วนบุคคลในการควบคุมและจัดการข้อมูลส่วนบุคคลของตนเองที่อยู่ในการควบคุมของผู้ควบคุมข้อมูลส่วนบุคคล (data controller) และประการที่สอง การสร้างหน้าที่ความรับผิดชอบให้กับผู้ควบคุมข้อมูลส่วนบุคคลในการประมวลผลและรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดสิทธิของเจ้าของข้อมูลส่วนบุคคลเอาไว้ 7 ประการ ได้แก่ สิทธิที่จะได้รับการแจ้งให้ทราบ (right to be informed)[7] โดยเป็นสิทธิที่เจ้าของข้อมูลส่วนบุคคลจะได้รับทราบข้อมูลเกี่ยวกับการประมวลผลของผู้ควบคุมข้อมูลส่วนบุคคลทั้งวัตถุประสงค์ ฐานความชอบธรรมที่ใช้ในการประมวลผลหรือเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล โดยต้องได้รับการแจ้งก่อนหรือขณะที่มีการประมวลข้อมูล[8] สิทธิในการเพิกถอนความยินยอม (right to withdraw consent)[9] โดยเป็นสิทธิของเจ้าของข้อมูลส่วนบุคคลขอถอนความยินยอมที่ได้ให้ไว้ในการประมวลผลข้อมูลส่วนบุคคล[10] สิทธิในการขอเข้าถึงข้อมูลส่วนบุคคล

---

[4] เขมภัทร ทฤษฎิคุณ, (25 กรกฎาคม 2565), ‘ช่องโหว่กฎหมาย PDPA เมื่อ ‘Big Brother’ ต้องคุกคามความเป็นส่วนตัวของประชาชน’ <https://waymagazine.org/pdpa-big-brother/> สืบค้นเมื่อ 15 พฤษภาคม 2566.

[5] ข้อมูลข่าวสารส่วนบุคคลเป็นคำที่ใช้เรียกข้อมูลส่วนบุคคลตามพระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ. 2540, ดู บทนิยาม “ข้อมูลข่าวสารส่วนบุคคล” พระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ. 2542 มาตรา 3.

[6] สภานิติบัญญัติแห่งชาติ, บันทึกการประชุมคณะกรรมาธิการวิสามัญพิจารณาร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ครั้งที่ 18 วันพุธที่ 27 กุมภาพันธ์ 2562, 98.

[7] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 23.

[8] กิรติพงศ์ แนวมาลี เขมภัทร ทฤษฎิคุณ และคณะ, *แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล: หน่วยงานของรัฐ* (สำนักพิมพ์สถาบันวิจัยเพื่อการพัฒนาประเทศไทย 2564) 28, คณาธิป ทองรวีวงศ์, *คำอธิบายหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล* (สำนักพิมพ์นิติธรรม 2564) 455.

[9] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 19 (5).

[10] กิรติพงศ์ แนวมาลี เขมภัทร ทฤษฎิคุณ และคณะ (เชิงอรรถ 8) 28, คณาธิป ทองรวีวงศ์ (เชิงอรรถ 8) 434.

(right to access)[11] โดยเป็นสิทธิของเจ้าของข้อมูลส่วนบุคคลที่แสดงต่อผู้ควบคุมข้อมูลส่วนบุคคลในการเข้าถึงข้อมูลของตนเองเพื่อตรวจสอบและรับรู้รายละเอียดเกี่ยวข้อง และสามารถขอรับสำเนาข้อมูลที่ถูกเก็บรวบรวมไว้[12] สิทธิในการโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่น (right to data portability)[13] โดยเป็นสิทธิของเจ้าของข้อมูลส่วนบุคคลในการโอนย้ายข้อมูลที่จัดเก็บในระบบเทคโนโลยีในความครอบครองของผู้ควบคุมข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลอีกรายหนึ่ง[14] สิทธิในการคัดค้านการประมวลผล (right to object)[15] โดยเป็นสิทธิของเจ้าของข้อมูลส่วนบุคคลที่ไม่เห็นด้วยในการประมวลผลข้อมูลของผู้ควบคุมข้อมูลส่วนบุคคลที่อาศัยฐานความชอบธรรมในการประมวลผลเพื่อประโยชน์สาธารณะหรือความจำเป็นเพื่อการปฏิบัติตามกฎหมาย เพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลแยกข้อมูลดังกล่าวออกจากข้อมูลชุดอื่นและยุติการประมวลผลข้อมูลนั้น[16] สิทธิขอให้ระงับการใช้ข้อมูล (right to restriction of processing)[17] โดยเป็นสิทธิของเจ้าของข้อมูลส่วนบุคคลที่ร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจำกัดหรือหยุดการใช้ข้อมูลส่วนบุคคลในบางสถานการณ์[18] สิทธิในการแก้ไขข้อมูล (right to rectification)[19] โดยเป็นสิทธิให้เจ้าของข้อมูลส่วนบุคคลสามารถดำเนินการแก้ไขข้อมูลที่อยู่กับผู้ควบคุมข้อมูลส่วนบุคคลให้ถูกต้อง ทันสมัย และตรงกับความเป็นจริงเพื่อไม่ให้เกิดความเข้าใจผิดในการประมวลผลข้อมูล[20] และสิทธิในการลบหรือทำลายข้อมูลส่วนบุคคล (right to erasure)[21] โดยเป็นสิทธิของเจ้าของข้อมูลส่วนบุคคลในการขอลบข้อมูลที่หมดวัตถุประสงค์ในการใช้งานหรือทำให้อยู่ในรูปแบบที่ไม่สามารถระบุตัวตนของบุคคลได้อีกต่อไป รวมถึงข้อมูลที่ไม่สามารถอ้างฐานความชอบธรรมในการจัดเก็บข้อมูลส่วนบุคคลอีกต่อไป[22]

อย่างไรก็ดี สิทธิทั้ง 7 ประการอาจจะไม่สามารถนำมาใช้ได้กับทุกสถานการณ์เนื่องจากมีเหตุผลเฉพาะเรื่องที่จำกัดการใช้สิทธิในบางบริบท ตัวอย่างเช่น กรณีที่พนักงานเจ้าหน้าที่อาศัยฐานความชอบธรรมปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะตามมาตรา 45 (1) ของพระราชบัญญัติโรงแรม พ.ศ. 2547 เพื่อตรวจสอบทะเบียนผู้เข้าพักและบัตรทะเบียนผู้เข้าพัก กรณีเช่นนี้สิทธิคัดค้านการประมวลผลของเจ้าของข้อมูลส่วนบุคคลอาจถูกปฏิเสธการใช้สิทธิเนื่องจากประโยชน์สาธารณะตามกฎหมายมีมากกว่าสิทธิของเจ้าของข้อมูลส่วนบุคคล[23] ทั้งนี้ ความสามารถจะใช้สิทธิจะบรรลุวัตถุประสงค์ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือไม่ขึ้นอยู่กับสถานการณ์ของการใช้สิทธินั้น ๆ โดยผู้ควบคุมข้อมูลส่วนบุคคลยังมีหน้าที่ความรับผิดชอบให้กับผู้ควบคุมข้อมูลส่วนบุคคลในการประมวลผลและรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

หน้าที่ความรับผิดชอบให้กับผู้ควบคุมข้อมูลส่วนบุคคลในการประมวลผลและรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลเป็นด้านสะท้อนของการรับรองสิทธิของเจ้าของข้อมูลส่วนบุคคลประกอบกับหน้าที่จำเป็นเพื่อบรรลุวัตถุประสงค์ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยประกอบด้วยหน้าที่ย่อย 6 ประการ ได้แก่ หน้าที่ประมวลผลข้อมูลส่วนบุคคลโดยชอบด้วยกฎหมาย เป็นธรรม และเปิดเผย โดยระบุฐานความชอบด้วยกฎหมายและประกาศวัตถุประสงค์ให้ชัดเจนในการประมวลผล หน้าที่ประมวลผลข้อมูลส่วนบุคคลโดยจำกัดวัตถุประสงค์โดยประมวลผลข้อมูลส่วนบุคคลเฉพาะในวัตถุประสงค์ที่มีการเก็บรวบรวมข้อมูลส่วนบุคคลและไม่เกินไปกว่าวัตถุประสงค์นั้น หน้าที่ในการประมวลข้อมูลส่วนบุคคลที่ถูกต้องโดยจัดให้มีมาตรการหรือวิธีการดำเนินการที่เหมาะสมเพื่อรับรองว่าข้อมูลที่เก็บรวบรวมนั้นถูกต้องและเป็นปัจจุบัน หน้าที่จำกัดระยะเวลา

---

[11] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 30.

[12] กิรติพงศ์ แนวมาลี เขมภัทร ทฤษฎิคุณ และคณะ (เชิงอรรถ 8) 29, คณาธิป ทองรวีวงศ์ (เชิงอรรถ 8) 422-423.

[13] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 31.

[14] กิรติพงศ์ แนวมาลี เขมภัทร ทฤษฎิคุณ และคณะ (เชิงอรรถ 8) 29, คณาธิป ทองรวีวงศ์ (เชิงอรรถ 8) 452.

[15] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 32.

[16] กิรติพงศ์ แนวมาลี เขมภัทร ทฤษฎิคุณ และคณะ (เชิงอรรถ 8) 30-31, คณาธิป ทองรวีวงศ์ (เชิงอรรถ 8) 445-447.

[17] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 34.

[18] กิรติพงศ์ แนวมาลี เขมภัทร ทฤษฎิคุณ และคณะ (เชิงอรรถ 8) 33-34, คณาธิป ทองรวีวงศ์ (เชิงอรรถ 8) 448-449.

[19] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 35.

[20] กิรติพงศ์ แนวมาลี เขมภัทร ทฤษฎิคุณ และคณะ (เชิงอรรถ 8) 35, คณาธิป ทองรวีวงศ์ (เชิงอรรถ 8) 430-431.

[21] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 33.

[22] กิรติพงศ์ แนวมาลี เขมภัทร ทฤษฎิคุณ และคณะ (เชิงอรรถ 8) 31-32.

[23] เพิ่งอ้าง, 30.

โดยจัดเก็บข้อมูลส่วนบุคคลเฉพาะตามเวลาเท่าที่จำเป็นแก่การประมวลผล หน้าที่ประมวลผลโดยเป็นความลับ โดยระมัดระวังและใช้มาตรการรักษาความปลอดภัยของการประมวลผลข้อมูลส่วนบุคคล และหน้าที่ประมวลผลโดยรับผิดชอบต่อกิจกรรมการประมวลผลข้อมูลส่วนบุคคล[24]

หน้าที่ทั้ง 6 ประการนี้เป็นหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลที่ต้องดำเนินการโดยเคร่งครัดไม่ว่า ผู้ควบคุมข้อมูลส่วนบุคคลนั้นจะเป็นหน่วยงานของรัฐหรือเอกชน ซึ่งการยกเว้นการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลกับกิจกรรมของหน่วยงานของรัฐที่เกี่ยวกับความมั่นคงและหน่วยงานบังคับใช้กฎหมายตามมาตรา 4 (2) และ (5) อาจจะไม่เพียงพอกับวัตถุประสงค์ในการคุ้มครองข้อมูลส่วนบุคคลและสิทธิความเป็นส่วนตัว

2. ข้อยกเว้นการคุ้มครองข้อมูลส่วนบุคคลในกิจกรรมของรัฐที่ได้รับการยกเว้นตามกฎหมายไทย

การยกเว้นการคุ้มครองข้อมูลส่วนบุคคลในกิจกรรมของรัฐมีวัตถุประสงค์เพื่อมิให้การดำเนินการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มากระทบต่อการดำเนินภารกิจของรัฐหรือทำให้เป้าหมายในการรักษาประโยชน์สาธารณะของรัฐได้รับผลกระทบจากการต้องปฏิบัติตามหลักเกณฑ์ที่ปรากฏในพระราชบัญญัติ อาทิ การต้องขอความยินยอม หรือการต้องแจ้งรายละเอียดการประมวลผลข้อมูลส่วนบุคคลให้กับเจ้าของข้อมูลส่วนบุคคลทราบ ซึ่งจะทำให้ภารกิจของรัฐไม่สามารถบรรลุวัตถุประสงค์ที่ต้องรักษาตามกฎหมาย[25]

การยกเว้นการคุ้มครองข้อมูลส่วนบุคคลกับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลตามกฎหมายไทยปรากฏอยู่ในมาตรา 4 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยยกเว้นให้กับกิจกรรม 6 ลักษณะ โดยกล่าวเฉพาะถึงกิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการใช้อำนาจรัฐมี 3 ลักษณะ ได้แก่ (1) การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์[26] การยกเว้นดังกล่าวมุ่งเน้นการดำเนินการของหน่วยงานของรัฐเกี่ยวกับการป้องกันปราบปรามอาชญากรรม (criminal offences) รวมถึงการดำเนินการป้องกันภัยคุกคามต่อความปลอดภัยสาธารณะที่เกี่ยวกับความมั่นคงของรัฐ (national security)[27] (2) การประมวลผลข้อมูลส่วนบุคคลของสภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าวตามอำนาจหน้าที่ของสภาดังกล่าว[28] การยกเว้นดังกล่าวเป็นไปเพื่อคุ้มครองเอกสิทธิ์และการดำเนินงานของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา และคณะกรรมาธิการของสภา[29] ซึ่งสอดคล้องกับ รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ได้รับรองเอกสิทธิ์ของสมาชิกสภาไว้[30] และ (3) การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา[31] การยกเว้นดังกล่าวมุ่งเน้นการดำเนินการนำข้อมูลส่วนบุคคลไปใช้กับการดำเนินการของฝ่ายตุลาการ เพื่อป้องกันมิให้หน่วยงานที่มีอำนาจตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลเข้าไปแทรกแซงการใช้อำนาจของฝ่ายตุลาการ[32] อนึ่ง การยกเว้นการคุ้มครองข้อมูลส่วนบุคคลที่บทความฉบับนี้มุ่งศึกษา

---

[24] เพิ่งอ้าง, 6.

[25] รัฐสภา จุรีมาศ, ‘ข้อพิจารณาการได้รับยกเว้นตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล: กรณีศึกษากฎหมายของสหราชอาณาจักร’ (2564) วารสารวิทยาลัยสงฆ์นครลำปาง ปีที่ 10 ฉบับที่ 3, 160.

[26] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 4 (2).

[27] คณาธิป ทองรวีวงศ์ (เชิงอรรถ 8) 59.

[28] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 4 (4).

[29] ข้อยกเว้นไม่บังคับใช้กฎหมายกับกิจกรรมประมวลผลข้อมูลส่วนบุคคลของฝ่ายนิติบัญญัตินี้ไม่ปรากฏในกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation: GDPR) แต่หากพิจารณาอารัมภบทของ GDPR แล้วจะเห็นได้ว่า กฎหมายไม่มุ่งให้การบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลกระทบต่อการทำงานของฝ่ายนิติบัญญัติ, ดู สภานิติบัญญัติแห่งชาติ, บันทึกการประชุมคณะกรรมาธิการวิสามัญพิจารณาร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ครั้งที่ 16 วันศุกร์ที่ 1 กุมภาพันธ์ 2562, 4, คณาธิป ทองรวีวงศ์ (เชิงอรรถ 8) 59.

[30] รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 มาตรา 124.

[31] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 4 (5).

[32] คณาธิป ทองรวีวงศ์ (เชิงอรรถ 8) 60.

แนวทางการปรับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลจะพิจารณาเฉพาะกรณีจำกัดเฉพาะกรณี (1) หน่วยงานของรัฐด้านความมั่นคงของรัฐ และ (3) หน่วยงานบังคับใช้กฎหมาย

ในการยกเว้นการบังคับใช้กฎหมายตามมาตรา 4 (2) และ (5) นั้นหน่วยงานที่จะได้รับการยกเว้นจะต้องเข้าลักษณะตามองค์ประกอบ 2 ประการประกอบกันคือ องค์ประกอบด้านองค์กรหรือหน่วยงานประกอบกับวัตถุประสงค์[33] ซึ่งหากไม่ครบองค์ประกอบทั้งสองประการแล้วจะไม่เข้าเงื่อนไขที่จะได้รับการยกเว้นตามกฎหมาย ตัวอย่างเช่น กรณีของข้อยกเว้นของหน่วยงานความมั่นคงของรัฐ องค์ประกอบแรกคือ หน่วยงานนั้นจะต้องเป็นหน่วยงานที่มีหน้าที่เกี่ยวกับความมั่นคงของรัฐ และองค์ประกอบที่สอง กิจกรรมที่ได้รับการยกเว้นจะต้องเป็นกิจกรรมที่ปรากฏอยู่ในมาตรา 4 (2) คือ กิจกรรมด้านความมั่นคงทางการคลัง การรักษาความปลอดภัยของประชาชน การป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์ ตัวอย่างของกรณีนี้คือ สำนักงานข่าวกรองแห่งชาติอาศัยอำนาจตามพระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ. 2562 เก็บรวบรวมข้อมูลส่วนบุคคลมาใช้เพื่อวัตถุประสงค์ในกิจกรรมข่าวกรอง

ในกรณีข้อยกเว้นด้านหน่วยงานบังคับใช้กฎหมาย องค์ประกอบแรกคือ หน่วยงานนั้นจะต้องเป็นศาลและหน่วยงานด้านกระบวนการยุติธรรมที่เกี่ยวข้อง อาทิ หน่วยงานอัยการ หน่วยงานบังคับคดี หน่วยงานรับผิดชอบเรื่องการวางทรัพย์ และองค์ประกอบที่สอง กิจกรรมที่ได้รับการยกเว้นจะต้องเป็นกิจกรรมที่ปรากฏอยู่ในมาตรา 4 (5) คือ กิจกรรมด้านการพิจารณาพิพากษาคดีโดยไม่จำกัดว่าเป็นคดีแพ่ง คดีอาญา คดีปกครอง และคดีรัฐธรรมนูญ กิจกรรมด้านการวางทรัพย์ และกิจกรรมด้านการบังคับคดี ตัวอย่างเช่น ศาลอาญาดำเนินคดีอาศัยอำนาจตามประมวลกฎหมายวิธีพิจารณาความอาญาเพื่อรับฟังข้อมูลส่วนบุคคลของจำเลย

ผลของการยกเว้นการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ให้กับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของหน่วยงานของรัฐ ทำให้หน่วยงานของรัฐที่ได้รับการยกเว้นมีหน้าที่จะต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลสำหรับข้อมูลส่วนบุคคลที่ได้รับการยกเว้นในกิจกรรมให้เป็นไปตามมาตรฐานที่กฎหมายกำหนด[34] คือ ตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565

อย่างไรก็ดี พึงสังเกตไว้ว่า หน้าที่ตามข้อยกเว้นการคุ้มครองข้อมูลส่วนบุคคลในกิจกรรมของรัฐค่อนจะจำกัดเมื่อเปรียบเทียบกับหลักการของ GDPR ซึ่งประเทศไทยใช้เป็นต้นแบบในการยกร่างพระราชบัญญัติแล้ว กฎหมายจะกำหนดให้ต้องมีการตรามาตรการสำหรับกิจกรรมที่ได้รับการยกเว้นไว้เป็นการเฉพาะสำหรับหน่วยงานของรัฐด้านความมั่นคงของรัฐ และหน่วยงานบังคับใช้กฎหมาย[35] สภาพดังกล่าวทำให้ในตอนแรกมีการเสนอให้มีการตราเรื่องความมั่นคงสาธารณะไว้เป็นหมวดเฉพาะในพระราชบัญญัติฉบับนี้[36] ซึ่งสุดท้ายหมวดดังกล่าวไม่ผ่านการพิจารณาออกมาเมื่อกฎหมายมีการประกาศใช้ และแม้จะมีการอธิบายว่า ในภาครัฐมีการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 แต่พระราชบัญญัติฉบับนี้มีวัตถุประสงค์เพื่ออำนวยความสะดวกให้ประชาชนเข้าถึงข้อมูลข่าวสารของราชการ[37] มิใช่เป็นการคุ้มครองข้อมูลส่วนบุคคลเป็นการเฉพาะประกอบกับหน่วยงานของรัฐด้านความมั่นคง อาทิ สำนักข่าวกรองแห่งชาติ สำนักงานสภาความมั่นคงแห่งชาติ และหน่วยงานของรัฐแห่งอื่นตามที่กำหนดในกฎกระทรวงอาจจะกำหนดหลักเกณฑ์เพื่อจัดการกับข้อมูลข่าวสารส่วน

---

[33] เพิ่งอ้าง, 53.

[34] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 4 วรรคสาม.

[35] ความเห็นของผู้ช่วยศาสตราจารย์ ดร. ปิยะบุตร บุญอร่ามเรือง ซึ่งอธิบายว่า ตาม GDPR การยกเว้นหน่วยงานของรัฐจะมีกฎหมายอีกฉบับรองรับเพื่อให้การคุ้มครองข้อมูลส่วนบุคคลยังมีผลผูกพันหน่วยงานของรัฐ ดู สภานิติบัญญัติแห่งชาติ, บันทึกการประชุมคณะกรรมาธิการวิสามัญพิจารณาร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ครั้งที่ 13 วันศุกร์ที่ 28 มกราคม 2562, 3.

[36] สภานิติบัญญัติแห่งชาติ, บันทึกการประชุมคณะกรรมาธิการวิสามัญพิจารณาร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ครั้งที่ 16 วันศุกร์ที่ 1 กุมภาพันธ์ 2562, 6.

[37] สมชัย วัฒนการุณ, *คำอธิบายพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540* (สำนักพิมพ์บริษัท พี. เพรส จำกัด 2561) 1-2.

บุคคลที่อยู่ในความควบคุมดูแลของหน่วยงาน[38] ซึ่งอาจไม่ได้มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

นอกจากนี้ ข้อยกเว้นในการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลตามมาตรา 4 (2) และ (5) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นมีขอบเขตกว้างเนื่องจากถูกแก้ไขเพิ่มเติมในชั้นของคณะกรรมาธิการวิสามัญพิจารณาร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... โดยในกรณีของกิจกรรมการประมวลผลข้อมูลของหน่วยงานของรัฐที่เกี่ยวกับความมั่นคงได้ขยายขอบเขตออกไปครอบคลุมการรักษาความมั่นคงทางการคลังของรัฐ ซึ่งเป็นเรื่องทางภาษี หรือหน่วยงานที่บังคับใช้กฎหมายได้ขยายขอบเขตออกไปครอบคลุมถึงกิจกรรมของฝ่ายปกครองบางประการ อาทิ การบังคับคดี และการวางทรัพย์[39] ทำให้มีประเด็นต้องพิจารณาว่าขอบเขตของเรื่องโดยเฉพาะอย่างยิ่งกรณีของ “ความมั่นคงของรัฐ” ควรจะเป็นเช่นไร เพราะโดยสภาพคำว่า ความมั่นคงของรัฐเป็นถ้อยคำที่ไม่เฉพาะเจาะจงในทางกฎหมาย (indefinite legal concept) ซึ่งเปิดโอกาสให้เจ้าหน้าที่ของรัฐที่บังคับใช้กฎหมายมีดุลพินิจในการตีความข้อเท็จจริงในแต่ละกรณีเป็นการเฉพาะ ๆ[40] ซึ่งหน่วยงานของรัฐอาจใช้ดุลพินิจโดยโน้มเอียงไปสู่การให้ความสำคัญกับความมั่นคงของรัฐบาล อาทิ การดักฟังหรือติดตามนักกิจกรรมที่อยู่ตรงข้ามกับรัฐบาล[41] ผลของการไม่มีหลักเกณฑ์ดังกล่าวอาจทำให้หน่วยงานของรัฐจะอ้างข้อยกเว้นเพื่อความมั่นคงของรัฐจนละเมิดต่อสิทธิในข้อมูลส่วนบุคคลและสิทธิความเป็นส่วนตัว

สภาพการณ์ดังกล่าวทำให้เห็นว่า การยกเว้นการคุ้มครองข้อมูลส่วนบุคคลในกิจกรรมของรัฐที่ได้รับการยกเว้นตามกฎหมายไทยมีปัญหา 2 ประการคือ ประการแรก การคุ้มครองข้อมูลส่วนบุคคลไม่ควรจะต้องถูกยกเว้นโดยสิ้นเชิงจากการคุ้มครองข้อมูลส่วนบุคคล การเคารพสิทธิความเป็นส่วนตัว และการตรวจสอบการบังคับใช้กฎหมายโดยอิสระ[42] และประการที่สอง การขาดแนวทางในการคุ้มครองข้อมูลส่วนบุคคลกับหน่วยงานของรัฐที่ได้รับการยกเว้น ซึ่งสร้างสมดุลระหว่างการดำเนินการเพื่อประโยชน์ของรัฐและสิทธิในข้อมูลส่วนบุคคลและสิทธิความเป็นส่วนตัว[43]

3. แนวทางการคุ้มครองข้อมูลส่วนบุคคลของกิจกรรมของรัฐที่ได้รับการยกเว้นในต่างประเทศ

ระบบกฎหมายคุ้มครองข้อมูลส่วนบุคคลในโลกนี้สามารถแบ่งได้เป็น 3 รูปแบบใหญ่คือ ระบบแบบเปิด (open model) ซึ่งมุ่งเน้นการให้ผู้ควบคุมข้อมูลส่วนบุคคลตัดสินใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะภาคเอกชน โดยไม่มีกฎหมายทั่วไปที่กำหนดแนวทางการคุ้มครองข้อมูลส่วนบุคคล แต่ใช้กฎหมายในรายสาขาเป็นแบบ “Patchwork System” ตัวอย่างของประเทศในลักษณะนี้คือ สหรัฐอเมริกา ระบบการใช้ข้อมูลส่วนบุคคลอย่างมีเงื่อนไข (conditional model) เป็นระบบที่กฎหมายกำหนดมาตรฐานการใช้ประโยชน์จากข้อมูลส่วนบุคคล ตัวอย่างของประเทศในลักษณะนี้คือ สหภาพยุโรปและสหราชอาณาจักร และระบบควบคุม (control model) ซึ่งเป็นกรณีที่รัฐกำหนดเงื่อนไขในการใช้ข้อมูลส่วนบุคคลอย่างเข้มงวด แต่เปิดช่องให้รัฐบาลสามารถเข้าแทรกแซงได้ ตัวอย่างของประเทศในลักษณะนี้คือ จีนและรัสเซีย[44] จากลักษณะดังกล่าวเมื่อพิจารณาพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และความเป็นมาในการยกร่างพระราชบัญญัติแล้วมีลักษณะ

---

[38] พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มาตรา 22.

[39] คณาธิป ทองรวีวงศ์ (เชิงอรรถ 8) 53-54 และ 60, ตัวอย่างของการประชุมที่มีการแก้ไขขอบเขตของบทบัญญัติมาตรา 4 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ดู สภานิติบัญญัติแห่งชาติ, บันทึกการประชุมคณะกรรมาธิการวิสามัญพิจารณาร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ครั้งที่ 16 วันศุกร์ที่ 1 กุมภาพันธ์ 2562, 3-4.

[40] เอกบุญ วงศ์สวัสดิ์กุล, ‘การควบคุมอำนาจดุลพินิจของฝ่ายปกครองโดยศาลไทย’ (วิทยานิพนธ์ นิติศาสตร์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ 2534) 23.

[41] เขมภัทร ทฤษฎิคุณ (เชิงอรรถ 4).

[42] Privacy International, *A Guide for Policy Engagement on Data Protection: The Keys to Data Protection* (Privacy International 2018) 29.

[43] คณาธิป ทองรวีวงศ์ (เชิงอรรถ 8) 31.

[44] เขมภัทร ทฤษฎิคุณ, (เมษายน 2565), ‘การศึกษาความจำเป็นและแนวทางในการจัดทำแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล’ <https://tdri.or.th/2022/06/necessity-and-guidelines-for-the-preparation-of-personal-data-protection-practices/> สืบค้นเมื่อ 15 พฤษภาคม 2566.

เป็นระบบการใช้ข้อมูลส่วนบุคคลอย่างมีเงื่อนไข[45] การศึกษาแนวทางการคุ้มครองข้อมูลส่วนบุคคลของกิจกรรมของรัฐที่ได้รับการยกเว้นในต่างประเทศในส่วนนี้จะใช้แนวทางของสหภาพยุโรปและสหราชอาณาจักร

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปหรือ GDPR กำหนดหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปเพื่อใช้บังคับเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสมาชิกในสหภาพยุโรป ทั้งหมดนั้น GDPR ได้กำหนดแนวทางการคุ้มครองข้อมูลส่วนบุคคลของกิจกรรมของรัฐเอาไว้ 3 ลักษณะ ดังนี้

กรณีที่ 1 การใช้อำนาจรัฐเพื่อประโยชน์ในด้านความมั่นคงและการบังคับใช้กฎหมายนั้น ตามอารัมภบทของ GDPR ได้อธิบายว่า กฎระเบียบเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลนี้จะไม่นำไปใช้กับกิจกรรมที่อยู่นอกเหนือขอบเขตของสหภาพยุโรปซึ่งรวมถึงกิจกรรมด้านความมั่นคงของชาติ[46]

กรณีที่ 2 การดำเนินการเพื่อวัตถุประสงค์ในการป้องกัน สืบสวน ตรวจจับ หรือดำเนินคดีกับความผิดหรือการลงโทษทางอาญา ซึ่งรวมถึงการรักษาความปลอดภัยสาธารณะและการดำเนินการเคลื่อนย้ายข้อมูลดังกล่าวเพื่อป้องกันภัยคุกคามที่อาจจะเกิดขึ้นจากการกระทำความผิดอาจไม่ต้องดำเนินการตามหลักเกณฑ์ของ GDPR แต่ให้ไปดำเนินการตามกฎหมายเฉพาะ อาทิ Directive (EU) 2016/680[47] ซึ่งเป็นกำหนดกฎเกณฑ์เฉพาะในการคุ้มครองบุคคลธรรมดาจากการประมวลผลข้อมูลส่วนบุคคลโดยหน่วยงานของรัฐที่มีอำนาจเพื่อวัตถุประสงค์ในการป้องกัน การสืบสวน การตรวจจับ หรือการฟ้องร้องการกระทำความผิดหรือการดำเนินการลงโทษทางอาญา และการเคลื่อนย้ายข้อมูลดังกล่าวโดยเสรี ซึ่งรัฐสมาชิกสหภาพยุโรปอาจจะมอบหมายให้หน่วยงานของรัฐที่มีอำนาจรับผิดชอบตามจุดมุ่งหมายของ Directive (EU) 2016/680 จะถือว่าได้ดำเนินการภายใต้ขอบเขตของ GDPR แล้ว นอกจากนี้ รัฐสมาชิกควรที่จะมีการออกกฎหมายเฉพาะหรือแก้ไขกฎหมายเดิมเพื่อให้สอดคล้องกับ GDPR โดยพิจารณาความสอดคล้องกับรัฐธรรมนูญ การจัดการองค์กร และการบริหารภายในรัฐสมาชิกนั้น ๆ โดยกฎหมายดังกล่าวอาจจะมีข้อจำกัดสิทธิบางประการเท่าที่จำเป็นและเหมาะสมสำหรับสังคมประชาธิปไตยที่จะใช้ในการรักษาผลประโยชน์สำคัญบางประการเป็นการเฉพาะ[48]

กรณีที่ 3 การดำเนินกิจกรรมของศาลและหน่วยงานด้านกระบวนการยุติธรรมอื่น ๆ โดยกำหนดให้ประเทศสมาชิกไปกำหนดหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลที่ใช้บังคับเฉพาะกับศาลและหน่วยงานด้านกระบวนการยุติธรรมอื่น ๆ แต่หลักเกณฑ์ดังกล่าวไม่รวมถึงการปฏิบัติหน้าที่ในฐานะองค์กรตุลาการ เพื่อรักษาความเป็นอิสระของศาลในการปฏิบัติหน้าที่ตุลาการ รวมถึงการบังคับใช้กับหน่วยงานด้านกระบวนการยุติธรรมอื่น ๆ ที่มีส่วนในการสนับสนุนการทำงานของศาลในฐานะองค์กรตุลาการ การกำหนดหลักเกณฑ์นั้นควรรับประกันว่าการปฏิบัติงานภายใต้กระบวนการยุติธรรมเป็นไปตามข้อกำหนดของ GDPR เพื่อเสริมสร้างการรับรู้ของผู้มีส่วนเกี่ยวข้องในกระบวนการยุติธรรมในการปฏิบัติตามข้อกำหนดของ GDPR[49]

จากลักษณะดังกล่าวจะเห็นได้ว่า GDPR ของสหภาพยุโรปมีความมุ่งหมายที่จะให้ประเทศสมาชิกของสหภาพยุโรปมีอิสระในการกำหนดหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการใช้อำนาจรัฐเพื่อประโยชน์ด้านความมั่นคง การดำเนินการเพื่อวัตถุประสงค์ในการป้องกัน สืบสวน ตรวจจับ หรือดำเนินคดีกับความผิดหรือการลงโทษทางอาญา และการดำเนินกิจกรรมของศาลและหน่วยงานด้านกระบวนการยุติธรรมอื่น ๆ ที่มีส่วนเกี่ยวข้องกับการปฏิบัติหน้าที่ของศาลในฐานะองค์กรตุลาการ โดยให้ประเทศสมาชิกกำหนดหลักเกณฑ์ไว้ในกฎหมายเฉพาะหรือแก้ไขกฎหมายเดิมเพื่อให้สอดคล้องกับหลักเกณฑ์ที่กำหนดไว้ใน GDPR โดยมีสาระสำคัญ 4 ประการ ได้แก่ ประการแรก กำหนดไว้ชัดเจนและบัญญัติไว้ในกฎหมาย ประการที่สอง เคารพสิทธิและเสรีภาพขั้นพื้นฐานของบุคคล ประการที่สาม เป็นมาตรการที่จำเป็นและได้สัดส่วนในสังคมประชาธิปไตย และประการที่สี่ มาตรการดังกล่าวหากไม่ใช้จะกระทบต่อเป้าประสงค์ที่ชอบด้วยกฎหมาย ทำให้การยกเว้นไม่ใช่บังคับกับหน่วยงาน

---

[45] เพิ่งอ้าง.

[46] Recital 16 GDPR.

[47] Recital 19 GDPR.

[48] Recital 19 GDPR.

[49] Recital 20 GDPR.

ของรัฐของสหภาพยุโรปตาม GDPR เป็นไปอย่างมีเงื่อนไขภายใต้กฎเฉพาะที่มีการรับประกันสิทธิของเจ้าของข้อมูลส่วนบุคคล[50]

อนึ่ง ในสหภาพยุโรปรัฐสมาชิกยังต้องผูกพันตามอนุสัญญายุโรปว่าด้วยสิทธิมนุษยชน (European Convention of Human Right: ECHR) รับรองสิทธิความเป็นส่วนตัวของบุคคลไว้ในข้อบทที่ 8[51] ในกรณีที่มีการละเมิดสิทธิความเป็นส่วนตัวในลักษณะดังกล่าวข้อพิพาทที่เกิดขึ้นสามารถนำไปสู่ศาลสิทธิมนุษยชนแห่งสหภาพยุโรป (European Court of Human Rights: ECtHR) ได้ โดยเรื่องใช้อำนาจของเจ้าหน้าที่ของรัฐตามกฎหมายเฉพาะในการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ในด้านความมั่นคงนั้น ศาลสิทธิมนุษยชนแห่งสหภาพยุโรปได้เคยวางแนวคำพิพากษาไว้ว่า การเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ด้านความมั่นคงสามารถกระทำได้ ทั้งนี้ ในการเก็บรวมข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในด้านความมั่นคงหน่วยงานของรัฐต้องคำนึงถึงความชอบธรรมในการจัดเก็บและรวบรวมข้อมูลส่วนบุคคล โดยต้องพิจารณาตามหลักความจำเป็น (necessity) ความได้สัดส่วน (proportionality) และวัตถุประสงค์เฉพาะ (purpose specification) ในการเก็บรวบรวมและเข้าถึงข้อมูลด้วยเพื่อไม่ให้การกระทำในลักษณะดังกล่าวกลายเป็นละเมิดสิทธิมนุษยชน[52] โดยในคดี Allan v. the United Kingdom ศาลตัดสินให้การแอบบันทึกบทสนทนาส่วนตัวของผู้ต้องขังกับเพื่อนในพื้นที่เยี่ยมของเรือนจำและกับผู้ต้องหาร่วมในห้องขังเป็นการรบกวนสิทธิในชีวิตส่วนตัวของผู้สมัคร เนื่องจากไม่มีระบบกฎหมายควบคุมการใช้อุปกรณ์บันทึกแอบแฝงโดยตำรวจในเวลาที่เกี่ยวข้อง การรบกวนนี้จึงไม่เป็นไปตามกฎหมาย และขัดต่อข้อบทที่ 8 ของ ECHR[53] หรือในคดี Roman Zakharov v. Russia โจทก์ได้ยื่นฟ้องดำเนินคดีกับผู้ให้บริการเคลื่อข่ายโทรศัพท์ที่แอบติดตั้งอุปกรณ์สกัดกั้นการสื่อสารทางโทรศัพท์โดยไม่ได้มีคำสั่งศาลอนุญาตให้ติดตั้ง โดยบทบัญญัติทางกฎหมายภายในประเทศที่ควบคุมการสกัดกั้นการสื่อสารไม่ได้ให้การรับประกันที่เพียงพอและมีประสิทธิภาพต่อความเด็ดขาดและความเสี่ยงของการละเมิด โดยเฉพาะอย่างยิ่งกฎหมายภายในประเทศไม่ได้กำหนดให้ลบข้อมูลที่เก็บไว้หลังจากบรรลุวัตถุประสงค์ของการจัดเก็บแล้ว และแม้ว่าจะต้องได้รับอนุญาตจากศาล แต่การตรวจสอบโดยศาลก็ถูกจำกัด[54] หรือในคดี Szabó and Vissy v. Hungary โจทก์ฟ้องว่ากฎหมายของฮังการีไม่มีรายละเอียดเพียงพอเกี่ยวกับการป้องกันการละเมิดสิทธิความเป็นส่วนตัวและอาจเปิดโอกาสให้เจ้าหน้าที่ของรัฐใช้อำนาจโดยพลการ โดยกฎหมายไม่ได้กำหนดให้หน่วยงานของรัฐต้องขออนุญาตจากศาลก่อนการเข้าถึงข้อมูลส่วนบุคคล[55]

นอกจากนี้ ในกรณีที่หน่วยงานของรัฐมีการเก็บรวบรวมข้อมูลส่วนบุคคลโดยเจ้าของข้อมูลส่วนบุคคลไม่สามารถทราบได้ เจ้าของข้อมูลจะต้องได้รับการแจ้งเกี่ยวกับการรวบรวมข้อมูลส่วนบุคคลนั้นทันทีที่สามารถเปิดเผยกิจกรรมดังกล่าวโดยไม่กระทบต่อการสืบสวนการกระทำความผิด รวมถึงการเฝ้าระวังโดยอาศัยวิธีการทางเทคนิคหรืออัตโนมัติต้องตั้งอยู่บนพื้นฐานทางกฎหมายที่เหมาะสม[56]

ดังนี้แล้ว แม้ GDPR ของสหภาพยุโรปจะให้อิสระในการออกแบบหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการใช้อำนาจรัฐเพื่อประโยชน์ด้านความมั่นคง การดำเนินการเพื่อวัตถุประสงค์ในการป้องกัน สืบสวน ตรวจจับ หรือดำเนินคดีกับความผิดหรือการลงโทษทางอาญา และการดำเนินกิจกรรมของศาลและ

---

[50] Privacy International (เชิงอรรถ 42) 30.

[51] Article 8 ECHR

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[52] European Union Agency for Fundamental Rights and Council of Europe, (April 2018), 'Handbook on European Data Protection Law' p. 277. <http://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdfp> Accessed 15 May 2023

[53] ECtHR, Allan v. the United Kingdom, No. 48539/99, 5 November 2002.

[54] ECtHR, Roman Zakharov v. Russia, No. 47143/06, 4 December 2015.

[55] ECtHR, Szabó and Vissy v. Hungary, No. 37138/14, 12 January 2016.

[56] European Union Agency for Fundamental Rights and Council of Europe (เชิงอรรถ 52) 277.

หน่วยงานด้านกระบวนการยุติธรรมอื่นๆ ที่มีส่วนเกี่ยวข้องกับการปฏิบัติหน้าที่ของศาลในฐานะองค์กรตุลาการ ซึ่งเป็นการยอมรับความชอบธรรมของรัฐในการเข้าถึงข้อมูลส่วนบุคคล แต่รัฐสมาชิกก็ไม่อาจละเลยต่อหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลได้ รัฐสมาชิกยังต้องคำนึงถึงสิทธิของเจ้าของข้อมูลส่วนบุคคลเป็นสำคัญเพื่อจำกัดผลกระทบที่อาจจะเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคลมากที่สุด

ส่วนกรณีของประเทศสหราชอาณาจักรนั้นพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2018 (Data Protection Act 2018: DPA 2018) ซึ่งเป็นพระราชบัญญัติที่ตราขึ้นเพื่อให้สอดคล้องกับ GDPR ของสหภาพยุโรป โดยกำหนดให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปตาม GDPR[57] เว้นแต่ได้มีการกำหนดเนื้อหาเฉพาะสำหรับการประมวลผลข้อมูลส่วนบุคคลในกิจกรรมที่เกี่ยวกับศาลและองค์กรที่เกี่ยวข้องกับกระบวนการยุติธรรมไว้ในส่วนที่ 3 ของ DPA 2018 และการประมวลผลข้อมูลส่วนบุคคลในกิจกรรมของหน่วยสืบราชการลับที่เกี่ยวกับด้านข่าวกรองไว้ในหมวดที่ 4 ของ DPA 2018 โดยมีรายละเอียดดังนี้

กรณีที่ 1 การประมวลผลข้อมูลส่วนบุคคลในกิจกรรมที่เกี่ยวกับศาลและองค์กรที่เกี่ยวข้องกับกระบวนการยุติธรรม โดยบทบัญญัตินี้ใช้บังคับกับหน่วยงานที่มีอำนาจดำเนินการเพื่อวัตถุประสงค์ในการบังคับใช้กฎหมายจึงใช้จำกัดเฉพาะศาลที่พิจารณาคดีอาญา ตำรวจ เรือนจำ หน่วยงานบังคับใช้กฎหมายที่ไม่ใช่ตำรวจ และหน่วยงานอื่นที่มีหน้าที่ตามกฎหมายในการใช้อำนาจสาธารณะหรือเพื่อวัตถุประสงค์ในการบังคับใช้กฎหมายใด ๆ[58] ซึ่งหากเป็นกิจกรรมการประมวลผลโดยหน่วยงานของรัฐในลักษณะดังกล่าวจะต้องปฏิบัติตามแนวปฏิบัตินี้[59] โดยกิจกรรมที่มีวัตถุประสงค์ในการบังคับใช้กฎหมาย หมายถึง วัตถุประสงค์ของการป้องกัน การสืบสวน การตรวจจับหรือการฟ้องร้องความผิดทางอาญาหรือการดำเนินการตามบทลงโทษทางอาญา รวมถึงการป้องกันและป้องกันภัยคุกคามต่อความมั่นคงสาธารณะ[60] โดยภายใต้ส่วนที่ 3 ของ DPA 2018 ผู้ควบคุมข้อมูลส่วนบุคคลที่มีวัตถุประสงค์เพื่อการบังคับใช้กฎหมายมีหน้าที่ 6 ประการ ดังนี้[61]

(1) มาตรา 35 กำหนดหน้าที่ในการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการบังคับใช้กฎหมายโดยคำนึงถึงกฎหมายและความยุติธรรม และหน่วยงานที่ปฏิบัติตามกฎหมายจะต้องแสดงให้เห็นว่าการกระทำนั้นอ้างอิงอยู่กับบทบัญญัติของกฎหมายใด โดยอาจจะอาศัยอำนาจจากกฎหมายมากกว่าหนึ่งฉบับก็ได้ รวมถึงต้องผลโดยคำนึงถึงความยุติธรรม กล่าวคือ ไม่ประมวลผลในลักษณะที่เป็นอันตรายเกินควร คาดไม่ถึง หรือทำให้เข้าใจผิดต่อบุคคลที่เกี่ยวข้อง นอกจากนี้ยังกำหนดให้คุณต้องมีความชัดเจนและเปิดเผยกับบุคคลเกี่ยวกับวิธีที่คุณใช้ข้อมูลของพวกเขาตามความเหมาะสม โดยสอดคล้องกับความคาดหวังที่สมเหตุสมผลของเจ้าของข้อมูลส่วนบุคคล[62]

(2) มาตรา 36 กำหนดหน้าที่ในการประมวลผลข้อมูลส่วนบุคคลจะต้องเป็นไปตามวัตถุประสงค์ที่กฎหมายกำหนดไว้ กล่าวคือ เพื่อประโยชน์ในการบังคับใช้กฎหมาย และจะต้องไม่ถูกประมวลผลในลักษณะที่ไม่สอดคล้องกับวัตถุประสงค์ที่รวบรวมไว้ในตอนแรก โดยไม่สามารถดำเนินการเพื่อวัตถุประสงค์ที่ไม่สอดคล้องกับเหตุผลดั้งเดิมและเหตุผลอันสมควรสำหรับการประมวลผล[63]

---

[57] GOV.UK, 'Data Protection' <https://www.gov.uk/data-protection#:~:text=The%20Data%20Protection%20Act%202018%20is%20the%20UK's%20implementation%20of,used%20fairly%2C%20lawfully%20and%20transparently> Accessed 15 May 2023.

[58] กรณีของประเทศสหราชอาณาจักร DPA 2018 ตารางที่ 7 จะมีการกำหนดรายชื่อหน่วยงานที่เกี่ยวข้องกับการบังคับใช้กฎหมายที่ต้องปฏิบัติตามส่วนที่ 3 ของพระราชบัญญัติฉบับนี้เอาไว้อย่างชัดเจน อาทิ หน่วยงานรัฐบาลของสหราชอาณาจักรใดๆ นอกเหนือจากหน่วยงานที่ไม่ใช่กระทรวง และกำหนดตำแหน่งของหัวหน้าเจ้าหน้าที่ตำรวจและหน่วยงานตำรวจอื่นๆ ที่ต้องปฏิบัติตามส่วนที่ 3 นี้ อาทิ ผู้อำนวยการสำนักงานปราบปรามอาชญากรรมแห่งชาติ ผู้อำนวยการสรรพากรชายแดน และหัวหน้าหน่วยงานดำเนินการทางการเงิน.

[59] Section 29 DPA 2018.

[60] Section 31 DPA 2018.

[61] Section 34 DPA 2018.

[62] Information Commissioner's Office, 'Guideline to Legal Enforcement: Principles' <https://ico.org.uk/for-organisations/guide-to-le-processing/principles/.> Accessed 15 May 2023.

[63] Ibid.

(3) มาตรา 37 กำหนดหน้าที่ในการประมวลผลข้อมูลส่วนบุคคลจะต้องเก็บรวบรวมข้อมูลเท่าที่เพียงพอ เกี่ยวข้อง และไม่เกินไปเมื่อเทียบกับวัตถุประสงค์ในการประมวลผล โดยผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจำกัดเฉพาะสิ่งที่จำเป็นสำหรับวัตถุประสงค์ที่คุณกำลังประมวลผล[64]

(4) มาตรา 38 กำหนดหน้าที่ในการประมวลผลข้อมูลส่วนบุคคลจะต้องใช้ข้อมูลที่ถูกต้องและจำเป็นต้องดำเนินการปรับปรุงให้ทันสมัยอยู่เสมอ รวมถึงจะต้องดำเนินการทุกขั้นตอนตามสมควรเพื่อให้แน่ใจว่าข้อมูลส่วนบุคคลที่ไม่ถูกต้องจะถูกลบหรือแก้ไขโดยไม่ชักช้า นอกจากนี้ ผู้ควบคุมข้อมูลส่วนบุคคลควรจะต้องแยกแยะความแตกต่างระหว่างข้อมูลส่วนบุคคลที่อิงตามข้อเท็จจริงและข้อมูลที่มีพื้นฐานมาจากความคิดเห็นหรือการประเมิน อาทิ คำให้การของพยาน รวมถึงต้องสามารถแยกแยะข้อมูลระหว่างบุคคลประเภทต่างๆ อาทิ ผู้ต้องสงสัย จำเลย เหยื่อ และพยาน[65]

(5) มาตรา 39 กำหนดหน้าที่ในการประมวลผลข้อมูลส่วนบุคคลจะต้องเก็บไว้ไม่เกินความจำเป็นสำหรับวัตถุประสงค์ในการประมวลผล และต้องมีการกำหนดเวลาที่เหมาะสมสำหรับการตรวจสอบเป็นระยะถึงความจำเป็นในการจัดเก็บข้อมูลส่วนบุคคล รวมถึงตรวจสอบอย่างสม่ำเสมอเพื่อให้แน่ใจว่าคุณไม่ได้จัดเก็บไว้นานเกินความจำเป็น[66]

(6) มาตรา 40 กำหนดหน้าที่ในการประมวลผลข้อมูลส่วนบุคคลจะต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล โดยจะต้องมีมาตรการทางเทคนิคและองค์กรเพื่อให้แน่ใจว่าผู้ควบคุมข้อมูลส่วนบุคคลได้ป้องกันข้อมูลด้วยระดับความปลอดภัยที่เหมาะสม[67]

นอกจากนี้ DPA 2018 ได้กำหนดเงื่อนไขเฉพาะในการประมวลผลข้อมูลส่วนบุคคลอ่อนไหว (sensitive data) สำหรับกิจกรรมการบังคับใช้กฎหมาย ดังระบุไว้ในตารางที่ 8 ของ DPA 2018 โดยครอบคลุมกิจกรรมต่างๆ ที่สามารถทำให้ประมวลผลข้อมูลส่วนบุคคลอ่อนไหวได้ ได้แก่ วัตถุประสงค์ด้านการพิจารณาคดีและทางกฎหมายเพื่อประโยชน์สาธารณะสำคัญ วัตถุประสงค์ที่จำเป็นต่อการอำนวยความยุติธรรม วัตถุประสงค์จำเป็นในการปกป้องผลประโยชน์ที่สำคัญของเจ้าของข้อมูลหรือบุคคลอื่น วัตถุประสงค์จำเป็นสำหรับการปกป้องเด็กและบุคคลที่มีความเสี่ยง วัตถุประสงค์จำเป็นแก่การใช้สิทธิเรียกร้องทางกฎหมาย วัตถุประสงค์สำหรับการพิจารณาคดีของศาล วัตถุประสงค์จำเป็นเพื่อป้องกันการทุจริต วัตถุประสงค์จำเป็นสำหรับการเก็บถาวร การวิจัย หรือวัตถุประสงค์ทางสถิติ และกรณีข้อมูลส่วนบุคคลนั้นเป็นข้อมูลสาธารณะ[68]

แม้ว่า DPA 2018 จะยกเว้นการนำบทบัญญัติของ GDPR มาใช้กับหน่วยงานบังคับใช้กฎหมาย แต่ตามพระราชบัญญัติฉบับนี้ได้กำหนดสิทธิของเจ้าของข้อมูลส่วนบุคคลเอาไว้ในลักษณะเดียวกันกับที่มีการกำหนดไว้ใน GDPR อาทิ สิทธิที่จะได้รับการแจ้งให้ทราบ สิทธิในการขอเข้าถึงข้อมูลส่วนบุคคล สิทธิในการแก้ไขข้อมูล และสิทธิในการลบหรือทำลายข้อมูลส่วนบุคคล[69] นอกจากนี้ พระราชบัญญัตินี้ยังได้กำหนดหลักเกณฑ์ในการประมวลผลข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลในกิจกรรมเกี่ยวกับศาลและองค์กรที่เกี่ยวข้องกับกระบวนการยุติธรรม[70]

กรณีที่ 2 การประมวลผลข้อมูลส่วนบุคคลในกิจกรรมของหน่วยสืบราชการลับที่เกี่ยวกับด้านข่าวกรองโดยบทบัญญัติส่วนนี้กำหนดหลักเกณฑ์การประมวลผลข้อมูลส่วนบุคคลที่ดำเนินการโดยหน่วยสืบราชการลับโดยบทบัญญัติส่วนนี้ยกร่างขึ้นเพื่อให้สอดคล้องกับอนุสัญญาว่าด้วยการคุ้มครองบุคคลที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลโดยอัตโนมัติของสหภาพยุโรป (Convention for the Protection of Individuals with regard to Automatic

---

[64] Ibid.

[65] Ibid.

[66] Ibid.

[67] Ibid.

[68] Information Commissioner's Office, 'Guideline to Legal Enforcement: Conditions for Sensitive Processing' <https://ico.org.uk/for-organisations/guide-to-le-processing/conditions-for-sensitive-processing/> Accessed 15 May 2023.

[69] see Part 3 Chapter 3 DPA 2018.

[70] see Part 3 Chapter 4 DPA 2018.

Processing of Personal Data or Convention 108+)[71] โดยบทบัญญัติในส่วนนี้จะใช้บังคับกับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่ดำเนินการโดยหน่วยงานรักษาความปลอดภัย (MI5) หน่วยข่าวกรองลับ (Secret Intelligence Service: SIS) และกองบัญชาการสื่อสารภาครัฐ (Government Communications Headquarters: GCHQ)[72] ซึ่งจุดเน้นของการประมวลผลข้อมูลส่วนบุคคลในส่วนที่ 4 นี้มุ่งเน้นไปที่การกำหนดหลักเกณฑ์การประมวลผลข้อมูลส่วนบุคคลด้วยวิธีอัตโนมัติไม่ว่าทั้งหมดหรือบางส่วน[73] โดยภายใต้ส่วนที่ 4 ของ DPA 2018 ผู้ควบคุมข้อมูลส่วนบุคคลที่มีวัตถุประสงค์ที่เกี่ยวกับด้านข่าวกรองมีหน้าที่ 6 ประการ ดังนี้[74]

(1) มาตรา 86 กำหนดหน้าที่ในการประมวลผลข้อมูลส่วนบุคคลจะต้องถูกต้องตามกฎหมาย ยุติธรรม และโปร่งใส โดยผู้ประมวลผลข้อมูลส่วนบุคคลควรจะจัดการข้อมูลส่วนบุคคลในลักษณะที่เจ้าของข้อมูลส่วนบุคคลคาดหมายได้อย่างสมเหตุสมผลเท่านั้น และไม่ใช้ข้อมูลในลักษณะที่ส่งผลเสียที่ไม่เป็นธรรมต่อเจ้าของข้อมูลส่วนบุคคล ซึ่งรวมถึงการใช้ข้อมูลที่พ้นไปจากวัตถุประสงค์ในการจัดเก็บข้อมูลนั้น และในกรณีที่ต้องใช้วิธีการดักฟังควรจะต้องทำเท่าที่ได้สัดส่วนและทำโดยชอบด้วยกฎหมายโดยเฉพาะอย่างยิ่งตาม Human Rights Act 1998[75]

(2) มาตรา 87 กำหนดหน้าที่ในการประมวลผลข้อมูลส่วนบุคคลโดยจำกัดวัตถุประสงค์ โดยจัดเก็บข้อมูลเฉพาะตามวัตถุประสงค์ที่ชัดเจนและถูกต้องตามกฎหมายตามหลักเกณฑ์ที่กฎหมายกำหนด และหากต้องผู้ควบคุมข้อมูลส่วนบุคคลประสงค์จะใช้ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ที่แตกต่างจะต้องทำให้แน่ใจว่าวัตถุประสงค์ใหม่นั้นเข้ากันได้กับวัตถุประสงค์ดั้งเดิมของคุณ อาทิ การเก็บถาวรเพื่อสาธารณประโยชน์ การวิจัยทางวิทยาศาสตร์หรือประวัติศาสตร์ หรือสถิติโดยมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล[76]

(3) มาตรา 88 กำหนดหน้าที่ในการประมวลผลข้อมูลส่วนบุคคลต้องดำเนินการให้เพียงพอ เกี่ยวข้องและไม่มากเกินไป โดยจะต้องเก็บรวบรวมข้อมูลเฉพาะเท่าที่จะบรรลุวัตถุประสงค์ตามกฎหมายเท่านั้น และจะต้องตรวจสอบให้แน่ใจว่าผู้ควบคุมไม่ได้ประมวลผลมากกว่าที่คุณต้องการ รวมถึงตรวจสอบให้แน่ใจว่าได้มีการทำลายข้อมูลดังกล่าวเมื่อสิ้นวัตถุประสงค์ในการเก็บรวบรวมข้อมูลแล้ว[77]

(4) มาตรา 89 กำหนดหน้าที่ในการประมวลผลข้อมูลส่วนบุคคลต้องดำเนินการด้วยความแม่นยำ โดยต้องคำนึงว่า การเก็บรวบรวมข้อมูลจะต้องไม่ทำโดยถูกต้องและไม่ทำให้เกิดความเข้าใจผิดเกี่ยวกับข้อเท็จจริงใดๆ รวมถึงตรวจสอบให้แน่ใจว่าแหล่งที่มาและสถานะของข้อมูลส่วนบุคคลนั้นชัดเจน[78]

(5) มาตรา 90 กำหนดหน้าที่ในการประมวลผลข้อมูลส่วนบุคคลต้องมีความรับผิดชอบในการจัดเก็บโดยดำเนินลบหรือทำลายข้อมูลส่วนบุคคลดังกล่าวเมื่อหมดวัตถุประสงค์ในการจัดเก็บ รวมถึงมีนโยบายที่ชัดเจนในการจัดการกับข้อมูลส่วนบุคคลเมื่อหมดประโยชน์แล้ว[79]

(6) มาตรา 91 กำหนดหน้าที่ในการประมวลผลข้อมูลส่วนบุคคลจะต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล โดยจะต้องมีมาตรการทางเทคนิคและองค์กรเพื่อให้แน่ใจว่าผู้ควบคุมข้อมูลส่วนบุคคลได้ป้องกันข้อมูลด้วยระดับความปลอดภัยที่เหมาะสม[80]

ในลักษณะเดียวกันกับการประมวลผลข้อมูลส่วนบุคคลของกิจกรรมที่เกี่ยวกับศาลและองค์กรที่เกี่ยวข้องกับกระบวนการยุติธรรม กิจกรรมการประมวลผลข้อมูลส่วนบุคคลโดยหน่วยสืบราชการลับที่เกี่ยวกับด้าน

---

[71] Information Commissioner's Office, 'Intelligence services processing: Scope and key definitions' <https://ico.org.uk/for-organisations/intelligence-services-processing/scope-and-key-definitions/> Accessed 15 May 2023.

[72] Section 82 DPA 2018.

[73] Section 82 DPA 2018.

[74] Section 85 DPA 2018.

[75] Information Commissioner's Office, 'Intelligence services processing: Principles' <https://ico.org.uk/for-organisations/intelligence-services-processing/principles/> Accessed 15 May 2023.

[76] Ibid.

[77] Ibid.

[78] Ibid.

[79] Ibid.

[80] Ibid.

ข่าวกรองก็จะต้องเคารพสิทธิของเจ้าของข้อมูลส่วนบุคคลในลักษณะเดียวกัน[81] นอกจากนี้ พระราชบัญญัตินี้ยังได้กำหนดหลักเกณฑ์ในการประมวลผลข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลในกิจกรรมเกี่ยวกับด้านข่าวกรอง[82]

จากการศึกษาแนวทางการคุ้มครองข้อมูลส่วนบุคคลของกิจกรรมของรัฐที่ได้รับการยกเว้นในต่างประเทศของสหภาพยุโรปและสหราชอาณาจักรจะเห็นได้ว่า การยกเว้นการคุ้มครองข้อมูลส่วนบุคคลสำหรับกิจกรรมของหน่วยงานของรัฐนั้นไม่มีการยกเว้นอย่างเด็ดขาดที่ปราศจากภาระผูกพัน กิจกรรมของหน่วยงานของรัฐที่ได้รับการยกเว้นยังจะต้องปฏิบัติหน้าที่บางประการตามกฎหมายเฉพาะที่กำหนดหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคล โดยกฎหมายมุ่งเน้นไปที่ความชัดเจนของข้อยกเว้นและรายละเอียดของการยกเว้น[83]

4. ข้อเสนอแนะในการปรับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลกับกิจกรรมของรัฐที่ได้รับการยกเว้น

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดข้อยกเว้นบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลกับกิจกรรมของรัฐตามมาตรา 4 ของพระราชบัญญัติดังกล่าว โดยมีวัตถุประสงค์เพื่อป้องกันมิให้การปฏิบัติตามพระราชบัญญัตินี้กระทบต่อการดำเนินภารกิจของรัฐ อย่างไรก็ดี การยกเว้นการบังคับใช้ดังกล่าวได้กำหนดเพียงหน้าที่ให้หน่วยงานของรัฐที่ได้รับการยกเว้นจะต้องรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล โดยไม่มีกฎหมายอื่นมากำหนดแนวทางการป้องกันมิให้หน่วยงานของรัฐที่ได้รับการยกเว้นนำข้อมูลส่วนบุคคลไปใช้โดยไม่จำเป็น ได้สัดส่วน และบรรลุวัตถุประสงค์โดยกระทบต่อสิทธิของเจ้าของข้อมูลให้น้อยที่สุด

ในทางสากลการยกเว้นการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลจะไม่ยอมรับให้ทำได้ในลักษณะที่เด็ดขาด แต่จะกำหนดหน้าที่ให้กับหน่วยงานของรัฐในฐานะผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการบางประการเพื่อคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล โดยเมื่อศึกษาแนวทางการคุ้มครองข้อมูลส่วนบุคคลของกิจกรรมของรัฐที่ได้รับการยกเว้นในต่างประเทศพบว่า กรณีของสหภาพยุโรปและสหราชอาณาจักรนั้นกฎหมายไม่ยอมรับให้มีการยกเว้นการบังคับใช้กฎหมายกับหน่วยงานของรัฐด้านความมั่นคงและหน่วยงานบังคับใช้กฎหมายในวัตถุประสงค์ด้านความมั่นคงและการบังคับใช้กฎหมายโดยสมบูรณ์ แต่จะยกเว้นอย่างมีเงื่อนไขโดยกำหนดให้หน่วยงานของรัฐต้องคำนึงถึงความจำเป็น ความได้สัดส่วน และวัตถุประสงค์ของการกระทำที่เฉพาะเจาะจง รวมถึงมีหลักประกันสิทธิในข้อมูลส่วนบุคคลและสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคล ในขณะที่หน้าที่รักษาความมั่นคงปลอดภัยของข้อมูลเป็นเพียงหน้าที่ขั้นต่ำของผู้ควบคุมข้อมูลส่วนบุคคลที่เป็นหน่วยงานที่ได้รับการยกเว้นเท่านั้น

ดังนี้ เพื่อให้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีความรัดกุมมากยิ่งขึ้นและสามารถบรรลุวัตถุประสงค์ในการคุ้มครองข้อมูลส่วนบุคคลจึงเสนอให้มีการการดำเนินการใน 2 ลักษณะ ดังนี้

ประการแรก คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่เป็นหน่วยงานบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ควรจะจัดทำแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลสำหรับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของหน่วยงานของรัฐด้านความมั่นคงและหน่วยงานบังคับใช้กฎหมาย แม้ว่าพระราชบัญญัติฉบับนี้จะยกเว้นการดำเนินงานสำหรับหน่วยงานของรัฐที่มีวัตถุประสงค์ดังกล่าว แต่หน่วยงานของรัฐยังคงผูกพันต้องคุ้มครองความเป็นส่วนตัวตามบทบัญญัติมาตรา 124 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2562 การจัดทำแนวปฏิบัตินี้แม้จะไม่มีสถานะทางกฎหมายแต่เป็นมาตรฐานที่ควรจะเป็นของการคุ้มครองข้อมูลส่วนบุคคล แต่ถ้าหน่วยงานของรัฐด้านความมั่นคงและหน่วยงานบังคับใช้กฎหมายไม่ได้ปฏิบัติตามหลักเกณฑ์ดังกล่าว อาจจะถือได้ว่าหน่วยงานของรัฐทั้งสองประเภทไม่ได้ใช้ความระมัดระวังเพียงพอตามมาตรฐานที่ควรจะเป็น และนำมาซึ่งความรับผิดเพื่อละเมิดของหน่วยงานของรัฐ

หลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลที่ควรจะกำหนดไว้ในแนวปฏิบัติควรกำหนดหน้าที่ให้หน่วยงานของรัฐมีหน้าที่ต้องใช้ข้อมูลส่วนบุคคลโดยคำนึงถึงความชอบด้วยกฎหมาย การสมวัตถุประสงค์ในการใช้ข้อมูลส่วนบุคคลตามกฎหมาย การใช้ข้อมูลส่วนบุคคลเท่าที่จำเป็น การลบข้อมูลส่วนบุคคลเมื่อหมดความจำเป็น

---

[81] see Part 4 Chapter 3 DPA 2018.

[82] see Part 4 Chapter 4 DPA 2018.

[83] Privacy International (เชิงอรรถ 42) 29.

และการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล รวมถึงควรกำหนดสิทธิของเจ้าของข้อมูลส่วนบุคคลใน 4 เรื่อง ได้แก่ สิทธิที่จะได้รับการแจ้งให้ทราบ สิทธิในการขอเข้าถึงข้อมูลส่วนบุคคล สิทธิในการแก้ไขข้อมูล และสิทธิในการลบหรือทำลายข้อมูลส่วนบุคคล เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถนำสิทธิดังกล่าวไปใช้เรียกร้องให้รัฐดำเนินการตามหน้าที่ที่รัฐธรรมนูญกำหนดไว้

ประการที่สอง แก้ไขเพิ่มเติมพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยกำหนดหมวด 2/1 เพื่อกำหนดหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลสำหรับหน่วยงานของรัฐที่มีวัตถุประสงค์ในการรักษาความมั่นคงปลอดภัยของรัฐ และหน่วยงานบังคับใช้กฎหมาย โดยข้อเสนอแนะนี้เป็นข้อเสนอแนะในระยะยาวเพื่อให้เกิดความชัดเจนในการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลกับหน่วยงานของรัฐทั้งสองประเภทเพื่อกำหนดขั้นตอนและมาตรฐานขั้นต่ำในการคุ้มครองข้อมูลส่วนบุคคลที่ควรพิจารณาเอาไว้ เพื่อป้องกันมิให้หน่วยงานด้านความมั่นคงของรัฐและหน่วยงานบังคับใช้กฎหมาย อาศัยมาตรการที่ไม่ได้สัดส่วน โดยเฉพาะอย่างยิ่งการแอบเก็บข้อมูลส่วนบุคคลไปใช้โดยปราศจากความรับผิดชอบ โดยหลักการพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่แก้ไขเพิ่มเติมควรจะมีลักษณะไปในทิศทางเดียวกันกับ DPA 2018

นอกจากนี้ อีกประเด็นหนึ่งที่ควรจะต้องพิจารณาก็คือ ในการแก้ไขเพิ่มเติมพระราชบัญญัติคุ้มครองข้อมูล พ.ศ. 2562 ควรกำหนดกลไกในการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลและตรวจสอบการใช้อำนาจรัฐเพื่อวัตถุประสงค์ในการรักษาความมั่นคงปลอดภัยของรัฐเป็นพิเศษ เนื่องจากลักษณะของการใช้อำนาจของหน่วยงานของรัฐประเภทนี้สามารถริเริ่มการใช้อำนาจที่อาจจะนำไปสู่การละเมิดสิทธิของเจ้าของข้อมูลส่วนบุคคลได้ จึงควรกำหนดให้ในกรณีที่มีการหน่วยงานของรัฐมีการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ด้านความมั่นคงโดยที่เจ้าของข้อมูลส่วนบุคคลไม่อาจทราบได้จำเป็นต้องขออนุญาตศาลเพื่อดำเนินการ โดยระบุวัตถุประสงค์ ความจำเป็น มาตรการที่จะดำเนินการ ฐานความชอบธรรม บทบัญญัติของกฎหมาย และระยะเวลาในการจัดเก็บ รวมถึงกำหนดสิทธิให้เจ้าของข้อมูลส่วนบุคคลสามารถร้องขอต่อศาลเพื่อใช้สิทธิตามกฎหมายเมื่อเห็นว่าหน่วยงานของรัฐมิได้ปฏิบัติตามหลักเกณฑ์ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

บทสรุป

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีช่องว่างในการบังคับใช้กฎหมายกับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของหน่วยงานของรัฐที่เกี่ยวข้องกับความมั่นคงของรัฐและบังคับใช้กฎหมาย เพื่อให้สามารถบรรลุวัตถุประสงค์ในการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้อย่างเต็มที่จึงควรจะต้องมีการกำหนดหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลสำหรับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของหน่วยงานของรัฐที่มีวัตถุประสงค์เพื่อความมั่นคงของรัฐ และเพื่อการบังคับใช้กฎหมาย โดยดำเนินการตามข้อเสนอแนะข้างต้น

บรรณานุกรม

ภาษาไทย

กิรติพงศ์ แนวมาลี เขมภัทร ทฤษฎิคุณ และคณะ, *แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล: หน่วยงานของรัฐ* (สำนักพิมพ์สถาบันวิจัยเพื่อการพัฒนาประเทศไทย 2564).

เขมภัทร ทฤษฎิคุณ, (เมษายน 2565), ‘การศึกษาความจำเป็นและแนวทางในการจัดทำแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล’ <https://tdri.or.th/2022/06/necessity-and-guidelines-for-the-preparation-of-personal-data-protection-practices/> สืบค้นเมื่อ 15 พฤษภาคม 2566.

เขมภัทร ทฤษฎิคุณ, (25 กรกฎาคม 2565), ‘ช่องโหว่กฎหมาย PDPA เมื่อ ‘Big Brother’ ต้องคุกคามความเป็นส่วนตัวของประชาชน’ <https://waymagazine.org/pdpa-big-brother/> สืบค้นเมื่อ 15 พฤษภาคม 2566.

คณาธิป ทองรวีวงศ์, *คำอธิบายหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล* (สำนักพิมพ์นิติธรรม 2564).

นคร เสรีรักษ์, *ความเป็นส่วนตัว: ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย* (พิมพ์ครั้งที่ 2 สำนักพิมพ์แพร่: พี.เพรส 2563).

รัฐสภา จุรีมาศ, 'ข้อพิจารณาการได้รับยกเว้นตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล: กรณีศึกษากฎหมายของสหราชอาณาจักร' (2564) วารสารวิทยาลัยสงฆ์นครลำปาง ปีที่ 10 ฉบับที่ 3.

สภานิติบัญญัติแห่งชาติ. บันทึกการประชุมคณะกรรมาธิการวิสามัญพิจารณาร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ครั้งที่ 13 วันศุกร์ที่ 28 มกราคม 2562.

สภานิติบัญญัติแห่งชาติ. บันทึกการประชุมคณะกรรมาธิการวิสามัญพิจารณาร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ครั้งที่ 16 วันศุกร์ที่ 1 กุมภาพันธ์ 2562.

สภานิติบัญญัติแห่งชาติ. บันทึกการประชุมคณะกรรมาธิการวิสามัญพิจารณาร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ครั้งที่ 18 วันศุกร์ที่ 27 กุมภาพันธ์ 2562.

สมชัย วัฒนการุณ, *คำอธิบายพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540* (สำนักพิมพ์บริษัท พี. เพรส จำกัด 2561).

เอกบุญ วงศ์สวัสดิ์กุล, 'การควบคุมอำนาจดุลพินิจของฝ่ายปกครองโดยศาลไทย' (วิทยานิพนธ์ นิติศาสตร์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ 2534).

ภาษาอังกฤษ

European Union Agency for Fundamental Rights and Council of Europe, (April 2018), 'Handbook on European Data Protection Law' <http://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdfp> Accessed 15 May 2023.

GOV.UK., 'Data Protection' <https://www.gov.uk/data-protection#:~:text=The%20Data%20Protection%20Act%202018%20is%20the%20UK's%20implementation%20of,used%20fairly%2C%20lawfully%20and%20transparently> Accessed 15 May 2023.

Information Commissioner's Office, 'Guideline to Legal Enforcement: Principles' <https://ico.org.uk/for-organisations/guide-to-le-processing/principles/> Accessed 15 May 2023.

_____, 'Guideline to Legal Enforcement: Conditions for Sensitive Processing' <https://ico.org.uk/for-organisations/guide-to-le-processing/conditions-for-sensitive-processing/> Accessed 15 May 2023.

_____, 'Intelligence services processing: Scope and key definitions' <https://ico.org.uk/for-organisations/intelligence-services-processing/scope-and-key-definitions/> Accessed 15 May 2023.

_____, 'Intelligence services processing: Principles' <https://ico.org.uk/for-organisations/intelligence-services-processing/principles/> Accessed 15 May 2023.