แนวทางการเปิดเผยข้อมูลข่าวสารของราชการตามพระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ. 2540 ที่มีข้อมูลส่วนบุคคลรวมอยู่ด้วย

An Approach for Disclosure of Official Information containing Personal Data

*ดร.ปิติ เอี่ยมจำรูญลาภ**

คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

Dr. Piti Eiamchamroonlarp

Faculty of Law, Chulalongkorn University

วันที่รับบทความ 17 กุมภาพันธ์ 2566; วันแก้ไขบทความ 15 พฤษภาคม 2566; วันตอบรับบทความ 26 พฤษภาคม 2566

บทคัดย่อ

การเปิดเผยข้อมูลข่าวสารของราชการที่มีข้อมูลส่วนบุคคลตามพระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ. 2540 นั้นสามารถดำเนินการโดยไม่เป็นการทำลายการคุ้มครองความเป็นส่วนตัวของปัจเจกบุคคลและสามารถเกิดขึ้นควบคู่ไปกับการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ อย่างไรก็ตาม การบังคับใช้กฎหมายดังกล่าวจะต้องคำนึงถึงปัจจัยต่างๆ เพื่อสร้างความสมดุลระหว่างความโปร่งใสภาครัฐและความเป็นส่วนตัวของปัจเจกบุคคล การดำเนินการดังกล่าวอาจดำเนินการได้โดยการแยกแยะองค์ประกอบของข้อมูลเพื่อแยกข้อมูลที่จำเป็นต่อการตรวจสอบการทำงานภาครัฐและข้อมูลที่กระทบต่อความเป็นส่วนตัวของปัจเจกบุคคล ข้อมูลข่าวสารของราชการมีส่วนที่แสดงให้เห็นถึงความถูกต้องโปร่งใสและตรวจสอบได้ของหน่วยงานของรัฐซึ่งสามารถแยกจากเนื้อหาของข้อมูลที่เผยถึงตัวตนของปัจเจกบุคคลได้ นอกจากนี้ โดยหลักแล้วหน่วยงานของรัฐที่มีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ยังมีหน้าที่ต้องรักษาความมั่นคงปลอดภัยทางของข้อมูลส่วนบุคคลตามมาตรฐานที่กำหนดขึ้นตามมาตรา 37(1) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มีส่วนสนับสนุนให้หน่วยงานของรัฐที่ครอบครองข้อมูลส่วนบุคคลป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อีกด้วย

คำสำคัญ: ข้อมูลส่วนบุคคล, สิทธิในความเป็นส่วนตัว, ข้อมูลข่าวสารของราชการ, ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

---

*ผู้ช่วยศาสตราจารย์ ผู้อำนวยการหลักสูตร LL.M. (Business Law) International Program คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ที่อยู่: 254 ถนนพญาไท แขวงวังใหม่ เขตปทุมวัน กรุงเทพมหานคร 10330

E-mail: piti.e@chula.ac.th

Abstract

Disclosure of official information which also contain personal data in accordance with the Official Information Act B.E. 2540 (1997) can be made without infringing a right to privacy of individuals. This disclosure can also be simultaneously deemed a lawful action under the Personal Data Protection Act B.E. 2562 (2019). However, this harmonization can only be achieved when a disclosing state agency strikes fair balance between transparency in the public sector and a right to privacy of individuals. This balancing activity can be conducted by analyzing and differentiating content of the information in question. Content of the information that appears necessary for public governance examination can be separated from the part that reveals identity of an individual. In addition, a state agency that is also a data controller under the Personal Data Protection Act B.E. 2562 (2019) owes a statutory duty to ensure security of personal data it possesses in accordance with Section 37(1) of the Personal Data Protection Act B.E. 2562 (2019). This implementation can contribute to a state agency's responsibilities to prevent, handle, and mitigate risks associated with cyber threats.

Keywords: personal data, right to privacy, official information, security of personal data

1. บทนำ

สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการอธิบายว่าพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 (“พระราชบัญญัติข้อมูลข่าวสารของราชการฯ”) มีเจตนารมณ์ที่ต้องการให้ประชาชนมีโอกาสอย่างกว้างขวางในการรับข้อมูลข่าวสารเกี่ยวกับการดำเนินการต่างๆ ของรัฐ เพื่อที่ประชาชนจะได้แสดงความคิดเห็นและใช้สิทธิทางการเมืองได้ถูกต้องตรงกับความจริง เป็นการพัฒนาระบอบประชาธิปไตยให้มั่นคง ประชาชนมีโอกาสรู้ถึงสิทธิและหน้าที่ของตนอย่างเต็มที่ ส่งเสริมให้การบริหารงานของรัฐเป็นไปอย่างมีความโปร่งใส[1] แนวคิดดังกล่าวสอดคล้องกับความสัมพันธ์ระหว่างประชาธิปไตยกับการเข้าถึงข้อมูลที่รัฐครอบครองในต่างประเทศ เช่น EU Directive 2019/1024 (on open data and the re-use of public sector information) ที่อธิบายว่าการทำให้เอกสารใดๆ ที่รัฐครอบครอง (ทั้งที่เกี่ยวกับกระบวนการทางการเมืองและขั้นตอนทางกฎหมายและทางปกครอง) กลายเป็นข้อมูลที่สาธารณชนสามารถเข้าถึงได้เป็นการทั่วไปเป็นองค์ประกอบขั้นพื้นฐานที่ส่งเสริมสิทธิที่จะรับรู้ (right to information) ซึ่งเป็นพื้นฐานของหลักประชาธิปไตย[2] นอกจากนี้ การที่สาธารณชนสามารถเข้าถึงข้อมูลที่รัฐครอบครองยังมีส่วนส่งเสริมความโปร่งใส (Transparency) ความรับผิดชอบ (Accountability) ซึ่งเป็นปัจจัยช่วยส่งเสริมให้เกิดการเปลี่ยนแปลงจากประเทศที่ปกครองโดยรัฐบาลเผด็จการไปเป็นรัฐบาลที่ปกครองโดยและเพื่อประชาชน[3]

อย่างไรก็ตาม การเข้าถึงข้อมูลที่รัฐครอบครองอาจเป็นการรุกล้ำความเป็นส่วนตัวของบุคคลได้ เช่น กรณีที่ข้อมูลนั้นสามารถเปิดเผยถึงตัวตนของปัจเจกบุคคล เช่น เจ้าหน้าที่รัฐหรือประชาชน เมื่อบุคคลเหล่านี้ได้รับความคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560[4] นอกจากนี้ ปัจเจกบุคคลยังมีสถานะเป็นเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ) อีกด้วย ด้วยเหตุนี้จึงเกิด “ความท้าทาย” ในการสร้างความสมดุลระหว่างการส่งเสริมความโปร่งใสผ่านการเปิดเผยข้อมูลที่รัฐครอบครองกับการคุ้มครองสิทธิในความเป็นส่วนตัวผ่านการบังคับใช้สิทธิในข้อมูลส่วนบุคคล โดยบทความนี้จะวิเคราะห์ความสัมพันธ์และการทำงานร่วมกันระหว่างสิทธิที่บุคคลสามารถร้องขอข้อมูลข่าวสารของราชการตามมาตรา 11 แห่ง พระราชบัญญัติข้อมูลข่าวสารของราชการฯ ซึ่งมีข้อยกเว้นตามมาตรา 15 วรรคหนึ่ง (6) พระราชบัญญัติข้อมูลข่าวสารของราชการฯ ในกรณีที่การเปิดเผยจะเป็นการรุกล้ำสิทธิส่วนบุคคลโดยไม่สมควร และการคุ้มครองสิทธิส่วนบุคคลตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ การสร้างความสมดุลนี้เป็นการวิเคราะห์และเสนอ “โอกาส” ที่จะทำให้กฎหมายทั้งสองฉบับสามารถทำงานร่วมกันได้ และช่วยให้ความโปร่งใสในภาครัฐตลอดจนการ

---

[1] สำนักงานคณะกรรมการข้อมูลข่าวสารราชการ, *สิทธิรับรู้ข้อมูลข่าวสารของประชาชน* (พิมพ์ครั้งที่ 2, บริษัทสามเจริญพาณิชย์ (กรุงเทพ) จำกัด 2549) 7.

[2] EU Directive 2019/1024 (on open data and the re-use of public sector information), Preamble (43).

[3] Nurhan Kocaoglu and Andrea Figari, *Using the Right to Information as an Anti-Corruption Tool* (Berlin, Germany Transparency International 2006) 5.

[4] รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 มาตรา 32 วรรคหนึ่ง.

พัฒนาประชาธิปไตยไม่รุกล้ำความเป็นส่วนตัวของปัจเจกบุคคลมากเกินสมควร และในขณะเดียวกันทำให้การคุ้มครองความเป็นส่วนตัวของปัจเจกบุคคลไม่เป็นอุปสรรคต่อความโปร่งใสในภาครัฐตลอดจนการพัฒนาประชาธิปไตย

2. เนื้อหา

2.1 การคุ้มครองสิทธิส่วนบุคคลโดยหน่วยงานรัฐ

โดยทั่วไปแล้ว “หน่วยงานของรัฐ”[5] ตกอยู่ในบังคับของทั้ง พระราชบัญญัติข้อมูลข่าวสารของราชการฯ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ในส่วนของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ บัญญัติห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลหากมิได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล โดยมีข้อยกเว้นคือเป็นกรณีที่ผู้ควบคุมดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นการปฏิบัติตามกฎหมาย[6] ในขณะที่ มาตรา 11 วรรคหนึ่งแห่ง พระราชบัญญัติข้อมูลข่าวสารของราชการฯ บัญญัติรับรองสิทธิของบุคคลให้มีสิทธิขอข้อมูลข่าวสารที่หน่วยงานรัฐครอบครอง ดังนั้น หากเจ้าหน้าที่ของหน่วยงานรัฐเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 11 วรรคหนึ่งแห่ง พระราชบัญญัติข้อมูลข่าวสารของราชการฯ ย่อมเป็นการกระทำที่ชอบด้วยกฎหมาย

2.1.1 ข้อมูลส่วนบุคคลในความครอบครองของหน่วยงานรัฐ

ตามมาตรา 4 แห่ง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ บัญญัติว่าพระราชบัญญัตินี้ไม่ใช้บังคับกับหน่วยงานรัฐบางประเภท ได้แก่ (ก) การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์[7] (ข) สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าว ซึ่งเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมาธิการ แล้วแต่กรณี[8] และ (ค) การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการ

---

[5] พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มาตรา 4. บัญญัติว่า “หน่วยงานของรัฐ” หมายความว่า ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ ส่วนราชการสังกัดรัฐสภา ศาลเฉพาะในส่วนที่ไม่เกี่ยวกับการพิจารณาพิพากษาคดี องค์กรควบคุมการประกอบวิชาชีพ หน่วยงานอิสระของรัฐและหน่วยงานอื่นตามที่กำหนดในกฎกระทรวง

[6] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24 (6) ประกอบ 27 วรรคหนึ่ง.

[7] เพิ่งอ้าง มาตรา 4 วรรคหนึ่ง (2).

[8] เพิ่งอ้าง มาตรา 4 วรรคหนึ่ง (4).

ยุติธรรมทางอาญา[9] ดังนั้น หน่วยงานรัฐและเจ้าหน้าที่รัฐที่ไม่ได้เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามภารกิจข้างต้นจึงมีหน้าที่ต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ

จากข้อยกเว้นข้างต้นจึงมีหน่วยงานของรัฐที่ไม่ได้รับการยกเว้นและมีหน้าที่ต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ เช่น กรณีขององค์กรปกครองส่วนท้องถิ่นในการปฏิบัติภารกิจของตน เทศบาลตำบล (ราชการส่วนท้องถิ่น) มีหน้าที่ต้องทำในเขตเทศบาลเช่นรักษาความสะอาดของถนน หรือทางเดินและที่สาธารณะ รวมทั้งการกำจัดมูลฝอยและสิ่งปฏิกูล[10] ส่วนองค์การบริหารส่วนตำบลมีหน้าที่ต้องทำในเขตองค์การบริหารส่วนตำบลในการรักษาความสะอาดของถนน ทางน้ำ ทางเดิน และที่สาธารณะ รวมทั้งกำจัดมูลฝอยและสิ่งปฏิกูล[11] การปฏิบัติภารกิจของเทศบาลตำบลและองค์การบริหารส่วนตำบลนั้นไม่เข้าข้อยกเว้นตามมาตรา 4 แห่ง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ในการกำจัดมูลฝอยและสิ่งปฏิกูลนั้นเป็นบริการสาธารณะที่สามารถถูกส่งได้โดยระบบออนไลน์และฐานข้อมูลอิเล็กทรอนิกส์ เนื่องจากเทศบาลตำบลสามารถสร้างระบบการยื่นและรับคำร้องผ่านทางระบบออนไลน์ได้

องค์การบริหารส่วนตำบลบางปลา อำเภอบางพลี จังหวัดสมุทรปราการได้พัฒนาและใช้งานระบบการ “คำร้องขอถังขยะ” โดยระบุให้ผู้ร้องต้องกรอกข้อมูล (ซึ่งรวมไปถึงข้อมูลส่วนบุคคล) เช่น ชื่อ-สกุลของผู้ยื่นคำขอ ที่อยู่ของผู้ยื่นคำขอ เบอร์ติดต่อของผู้ยื่นคำขอ และจำนวนถังขยะที่ขอรับ[12] เมื่อผู้ยื่นคำขอกรอกข้อมูลดังกล่าวผ่านระบบออนไลน์ (เช่น พิมพ์ในหน้าเว็บไซต์) ข้อมูลจะถูกเก็บรวบรวมและใช้โดยเจ้าหน้าที่ขององค์การบริหารส่วนตำบลบางปลาเพื่อพิจารณาและตอบสนองต่อคำขอดังกล่าว

2.1.2 หน้าที่ของหน่วยงานรัฐตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ

ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลเพื่อให้บริการข้างต้น องค์กรปกครองส่วนท้องถิ่นเป็นผู้มีอำนาจตัดสินใจว่าจะเก็บรวบรวมข้อมูลส่วนบุคคลประเภทใดและจะใช้เพื่อวัตถุประสงค์ใดเพื่อจัดหาถังขยะให้กับผู้ยื่นคำขอ ด้วยเหตุนี้ องค์กรปกครองส่วนท้องถิ่นจึงมีสถานะเป็น “ผู้ควบคุมข้อมูลส่วนบุคคล” ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ[13] และมีหน้าที่ต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ บัญญัติโดยสามารถยกตัวอย่างหน้าที่ที่สำคัญได้ เช่น

---

[9] เพิ่งอ้าง มาตรา 4 วรรคหนึ่ง (5).

[10] พระราชบัญญัติเทศบาล พ.ศ. 2496 มาตรา 50 วรรคหนึ่ง (3).

[11] พระราชบัญญัติสภาตำบลและองค์การบริหารส่วนตำบล พ.ศ. 2537 มาตรา 67 (2).

[12] องค์การบริหารส่วนตำบลบางปลา, ‘คำร้องขอถังขยะ’ (Bangpla OSS, 27 ตุลาคม 2562) <https://bangpla.oss.in.th/public/ oss/data/formgeneral/id/61/menu/0> สืบค้นวันที่ 27 ตุลาคม 2565.

[13] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 6. “ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

2.1.2.1 จัดเก็บข้อมูลเท่าที่จำเป็น (Data Minimization) และชี้แจงรายละเอียดการประมวลผล (Right to be informed/Transparency)

กล่าวคือจะต้องเก็บรวบรวมให้น้อยที่สุดเท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมาย (data minimization)[14] ต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียดเกี่ยวกับวัตถุประสงค์ ฐานทางกฎหมาย ระยะเวลาการเก็บรักษาข้อมูล โอกาสที่ข้อมูลส่วนบุคคลจะถูกเปิดเผย ข้อมูลเกี่ยวกับตัวองค์กรปกครองส่วนท้องถิ่นในฐานะผู้ควบคุมข้อมูลส่วนบุคคล และสิทธิของเจ้าของข้อมูลส่วนบุคคล[15]

2.1.2.2 อ้างอิงฐานทางกฎหมาย (Lawful basis for processing)

คำว่า “ฐานทางกฎหมาย (legal basis)” ในบริบทของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลนั้นหมายถึงเงื่อนไขที่ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้โดยชอบด้วยกฎหมาย เช่น การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามมาตรา 19 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ หรือการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลโดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามมาตรา 24 เช่น เป็นการจำเป็นเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคล[16] และเป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล[17] ในกรณีนี้ องค์กรปกครองส่วนท้องถิ่นอาจระบุว่าการเก็บและใช้ข้อมูลตามตามแบบฟอร์มคำขอถังขยะนั้นมีความจำเป็นเพื่อดำเนินการตามคำขอของผู้ยื่นคำขอ

2.1.2.3 รักษาความมั่นคงปลอดภัยของข้อมูล (Data Security)

องค์กรปกครองส่วนท้องถิ่นในฐานะผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด[18] นอกจากนี้ ยังต้องจัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษาหรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม[19]

---

[14] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 22.

[15] เพิ่งอ้าง มาตรา 23.

[16] เพิ่งอ้าง มาตรา 24 (3).

[17] เพิ่งอ้าง มาตรา 24 (4).

[18] เพิ่งอ้าง มาตรา 37 (1).

[19] เพิ่งอ้าง มาตรา 37 (3).

ข้อมูลเกี่ยวกับการยื่นคำขอที่เผยให้เห็นถึงตัวตนของผู้ยื่นคำขอส่งผ่านระบบออนไลน์นั้นมีสถานะเป็นทั้ง “ข้อมูลส่วนบุคคล” ทั้งตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ และ พระราชบัญญัติข้อมูลข่าวสารของราชการฯ และขณะเดียวกันก็เป็นข้อมูลข่าวสารราชการเนื่องจากอยู่ในความครอบครองของหน่วยงานรัฐ หากปรากฏว่ามีบุคคลที่สามยื่นคำขอเพื่อขอรับข้อมูล

2.2 การสร้างสมดุลระหว่างการเปิดเผยข้อมูลข่าวสารของราชการกับการคุ้มครองความเป็นส่วนตัวของปัจเจกบุคคลในทางปฏิบัติ

โดยทั่วไปแล้ว “สิทธิในความเป็นอยู่ส่วนตัว (Right to Privacy)” หมายถึง สิทธิของบุคคลที่ไม่ถูกเปิดเผยต่อสาธารณชนโดยปราศจากความต้องการ และสิทธิที่จะไม่ถูกรัฐแทรกแซงโดยปราศจากเหตุผลอันสมควร (หรือในเรื่องที่รัฐไม่มีเหตุเกี่ยวข้อง)[20] สิทธิในความเป็นอยู่ส่วนตัวในเชิงของข้อมูล (informational privacy) จำกัดการเข้าถึงบุคคลอื่นในการเข้าถึง เผยแพร่ และใช้ข้อมูลเกี่ยวกับบุคคลอื่น (information about oneself)[21] ในมิติของความสัมพันธ์ระหว่างปัจเจกบุคคลกับรัฐนั้น สิทธิในความเป็นอยู่ส่วนตัวมุ่งที่จะจำกัดขอบเขตของอำนาจรัฐในการเข้าแทรกแซงความเป็นส่วนตัวของปัจเจกบุคคล[22] นอกเหนือจากความเป็นส่วนตัวในเชิงของข้อมูลแล้ว ความเป็นส่วนตัวยังหมายรวมถึงการไม่ถูกบุคคลอื่นและรัฐแทรกแซงทางกายภาพและในทางทรัพย์สินอีกด้วย[23]

เพื่อแสดงให้เห็นถึงตัวอย่างการสร้างสมดุลระหว่างการเปิดเผยข้อมูลข่าวสารของราชการกับการคุ้มครองความเป็นส่วนตัวของปัจเจกบุคคล บทความนี้จะยกตัวอย่างถึงการวินิจฉัยอุทธรณ์คำสั่งมิให้เปิดเผยข้อมูลข่าวสารของเทศบาลตำบลด่านเกวียนเกี่ยวกับค่าตอบแทน (คำวินิจฉัยคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารสาขาสังคม การบริหารราชการแผ่นดินและการบังคับใช้กฎหมาย (ที่ สค 200/2565)) และคำพิพากษาของศาลสหรัฐอเมริกาที่ศาลมีคำสั่งมิให้มีการเปิดเผยข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมในกระบวนยุติธรรมทางอาญา (คดี U.S. Department of Justice v. Reporters Committee)

2.2.1 คำวินิจฉัยคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารสาขาสังคม การบริหารราชการแผ่นดินและการบังคับใช้กฎหมาย (ที่ สค 200/2565)

คำวินิจฉัยนี้เป็นการวินิจฉัยถึงคำอุทธรณ์คำสั่งมิให้เปิดเผยข้อมูลข่าวสารของเทศบาลตำบลด่านเกวียนเกี่ยวกับค่าตอบแทน โดยผู้อุทธรณ์ได้ยื่นคำขอข้อมูลข่าวสารของเทศบาลตำบลด่านเกวียนเกี่ยวกับค่าตอบแทน 3 รายการ ได้แก่

---

[20] ปิติ เอี่ยมจำรูญลาภ,*การให้รัฐเข้าถึงและได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกันในสหรัฐอเมริกา* (สถาบันพระปกเกล้า 2562) 6-7.

[21] Jed Rubemfeld, ‘The Right of Privacy’ (1989) 102 Harvard Law Review 737, 740.

[22] เพิ่งอ้าง 737.

[23] Anita L. Allen, ‘Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm’ (2000) 32 Connecticut Law Review 861, 866.

(1) <u>รายการที่ 1</u> สำเนาคำสั่งการจ่ายเงินประโยชน์ตอบแทนอื่นเป็นกรณีพิเศษ อันมีลักษณะเป็นเงินรางวัลประจำปีสำหรับพนักงานเทศบาล ลูกจ้างประจำ และพนักงานจ้าง ของเทศบาลด่านเกวียน ประจำปีงบประมาณ พ.ศ. 2563 จำนวน 1 ชุด

(2) <u>รายการที่ 2</u> สำเนารายการประชุมคณะกรรมการพิจารณาจ่ายเงินประโยชน์ตอบแทนอื่นเป็นกรณีพิเศษ อันมีลักษณะเป็นเงินรางวัลประจำปีสำหรับพนักงานเทศบาล ลูกจ้างประจำ และพนักงานจ้างของเทศบาลด่านเกวียน ประจำปีงบประมาณ พ.ศ. 2563 จำนวน 1 ชุด

(3) <u>รายงานที่ 3</u> สำเนาหลักฐานการลงรับหนังสือขอรับประโยชน์ตอบแทนอื่นเป็นกรณีพิเศษของผู้รับมอบอำนาจ[24]

คณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารสาขาสังคม การบริหารราชการแผ่นดินและการบังคับใช้กฎหมาย พิจารณาแล้วเห็นว่า ข้อมูลทั้งสามรายการ *“ไม่มีข้อความใดเข้าลักษณะที่หน่วยงานของรัฐหรือเจ้าหน้าที่ของรัฐอาจมีคำสั่งมิให้เปิดเผยได้ตามมาตรา 15 แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการฯ”*[25] โดยคณะกรรมการยังได้วินิจฉัยต่อไปว่า

> *“...การเปิดเผยข้อมูลข่าวสารจะแสดงให้เห็นถึงความถูกต้องโปร่งใส และตรวจสอบได้ของหน่วยงานของรัฐ เมื่อไม่ปรากฏว่าการเปิดเผยข่าวสารจะก่อให้เกิดอันตรายต่อชีวิตหรือความปลอดภัยของบุคคลคนหนึ่งบุคคลใด ดังนั้น เมื่อพิจารณาถึงการปฏิบัติหน้าที่ตามกฎหมายของหน่วยงานของรัฐ ประโยชน์สาธารณะ และประโยชน์ของเอกชนที่เกี่ยวข้องประกอบกันแล้ว จึงเห็นควรเปิดเผยข้อมูลข่าวสารรายการที่ 1 ถึงรายการที่ 3...”*[26]

อย่างไรก็ตาม คณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารได้กำหนดให้ลบ ตัดทอน หรือกระทำด้วยประการใดๆ ที่ไม่เป็นการเปิดเผยข้อมูลข่าวสารส่วนบุคคลบุคคลหรือข้อมูลข่าวสารในขอบเขตสิทธิส่วนบุคคล ได้แก่ อัตราเงินเดือน อัตราค่าตอบแทน และจำนวนเงินที่จ่ายโบนัส ของผู้รับประโยชน์ตอบแทนอื่นเป็นกรณีพิเศษ ซึ่งการเปิดเผยจะเป็นการรุกล้ำสิทธิส่วนบุคคลโดยไม่สมควรตามมาตรา 15 วรรคหนึ่ง (5) แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการฯ”[27]

2.2.2 คดี *U.S. Department of Justice v. Reporters Committee*

ข้อมูลส่วนบุคคลอาจถูกเก็บรวบรวมในฐานข้อมูลของรัฐ เช่น ข้อมูลเกี่ยวกับพฤติกรรมที่ถูกกล่าวหาว่าไม่ชอบด้วยกฎหมายอาจถูกเก็บรวบรวมโดยเจ้าหน้าที่ของรัฐในกระบวนยุติธรรมทางอาญา โดยมีกรณีศึกษาได้แก่คดี *U.S. Department of Justice v. Reporters Committee* ซึ่งถูกพิพากษาโดยศาลฎีกาของสหรัฐอเมริกาในปี ค.ศ. 1989 ในคดีดังกล่าว นักข่าวได้ยื่นคำร้องข้อมูลเกี่ยวกับพี่น้องสี่คนซึ่งถูกกล่าวหาว่าได้รับข้อมูลจากเจ้าหน้าที่รัฐสภาที่มีพฤติกรรมทุจริตตามกฎหมายว่าด้วยเสรีภาพในข้อมูลข่าวสาร

---

[24] คำวินิจฉัยคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารสาขาสังคม การบริหารราชการแผ่นดินและการบังคับใช้กฎหมาย ที่ สค 200/2565.

[25] เพิ่งอ้าง 3.

[26] เพิ่งอ้าง 4.

[27] เพิ่งอ้าง.

(Freedom of Information Act หรือ “FOIA”) เมื่อคำขอถูกปฏิเสธ นักข่าวจึงได้ฟ้องคดีต่อศาลโดยอาศัยฐานที่ว่าการปฏิเสธนั้นจำกัดสิทธิในการเข้าถึงข้อมูลที่เข้าถึงได้โดยสาธารณะ (publicly available information)

กรณีมีข้อสังเกตว่า FOIA ของสหรัฐอเมริกานั้นมีเจตนารมณ์และสาระสำคัญที่สามารถเทียบเคียงได้กับพระราชบัญญัติข้อมูลข่าวสารราชการฯ[28] ของประเทศไทยซึ่งสามารถแสดงได้ตาม ตารางที่ 1 ดังนี้

ตารางที่ 1 : เปรียบเทียบเจตนารมณ์และสาระสำคัญของ FOIA (สหรัฐอเมริกา) และ พระราชบัญญัติข้อมูลข่าวสารราชการฯ

กฎหมาย	FOIA (สหรัฐอเมริกา)	พระราชบัญญัติข้อมูลข่าวสารราชการฯ
เจตนารมณ์	ให้ประชาชนมีสิทธิรับรู้ถึงข้อมูลเกี่ยวกับรัฐบาลของตน[29] เพื่อการตรวจสอบ (inspection) และการขอสำเนา (copying)[30]	ให้ประชาชนมีโอกาสอย่างกว้างขวางในการรับข้อมูลข่าวสารเกี่ยวกับการดำเนินการต่างๆ ของรัฐ เพื่อที่ประชาชนจะได้แสดงความคิดเห็นและใช้สิทธิทางการเมืองได้ถูกต้องตรงกับความจริง
หลักการสำคัญ	ให้สิทธิแก่สารธารณชนให้สามารถเรียกร้องการเข้าถึง (request access) ข้อมูลใดๆ จากหน่วยงานรัฐในสหพันธรัฐ	หน่วยงานรัฐมีหน้าที่ตามมาตรา 9 ต้องจัดให้มีข้อมูลข่าวสารของราชการให้ประชาชนได้เข้าตรวจดู และรับรองสิทธิของประชาชนในการยื่นคำขอข้อมูลข่าวสารราชการตามมาตรา 11
ข้อยกเว้น (ตัวอย่าง)	ไม่เปิดเผยในกรณีมีความจำเป็นเพื่อรักษาความเป็นส่วนตัวของบุคคล ความมั่นคงของรัฐ และการบังคับใช้กฎหมาย	ไม่เปิดเผยในกรณีมีความจำเป็นเพื่อรักษาความเป็นส่วนตัวของบุคคล ความมั่นคงของรัฐ และการบังคับใช้กฎหมายตามมาตรา 15
การดำเนินการ	หากปรากฏความจำเป็นอย่างชัดเจนที่จะต้องป้องกันการรุกล้ำความเป็น	ถ้ามีส่วนที่ต้องห้ามมิให้เปิดเผยตามมาตรา 14 หรือมาตรา 15 อยู่ด้วย ให้ลบหรือตัดทอนหรือ

[28] รองศาสตราจารย์ คณาธิป ทองรวีวงศ์ ได้ตั้งข้อสังเกตเอาไว้ว่า “สำหรับการใช้ดุลพินิจในการเปิดเผยข้อมูลนั้น กฎหมาย FOIA มีหลักการคล้ายคลึงกับพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ของไทย ดังที่ได้วิเคราะห์มาแล้ว แต่พบว่ามีข้อแตกต่างที่สำคัญในส่วนของการใช้ดุลพินิจไม่เปิดเผยข้อมูล ซึ่งตามกฎหมายไทยนั้น มิได้มีการกำหนดโทษสำหรับกรณีเจ้าพนักงานใช้ดุลพินิจไม่เปิดเผย แต่มีการกำหนดโทษในกรณีการเปิดเผยข้อมูลที่ไม่ชอบด้วยกฎหมาย อย่างไรก็ตาม เมื่อเปรียบเทียบกับ กฎหมาย FOIA พบว่า มีการกำหนดโทษทางวินัยสำหรับเจ้าหน้าที่ซึ่งไม่อนุญาต (Withholding) ให้เปิดเผยข้อมูลหากเป็นการกระทำตามอำเภอใจหรือตามอารมณ์ (Arbitrarily or capriciously) จึงเห็นได้ว่า กฎหมาย FOIA มุ่งเน้นหลักการสนับสนุนสิทธิได้รู้ (Right to know) โดยให้หน่วยงานของรัฐเปิดเผยข้อมูลข่าวสารมากกว่ากรณีของกฎหมายไทย โปรดดู คณาธิป ทองรวีวงศ์, ‘ข้อยกเว้นของการเปิดเผยข้อมูลตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 : ศึกษากรณีข้อมูลส่วนบุคคล’ (2560) 1(1) วารสารนิติศาสตร์และสังคมท้องถิ่น 47, 62.

[29] FOIA, ‘What is the FOIA?’ (United States Department of Justice, 2022) <https://www.foia.gov/faq.html> accessed 31 October 2022.

[30] US Code § 552 (Public information; agency rules, opinions, orders, records, and proceedings), (a)(2).

ตารางที่ 1 : เปรียบเทียบเจตนารมณ์และสาระสำคัญของ FOIA (สหรัฐอเมริกา) และ พระราชบัญญัติข้อมูลข่าวสารราชการฯ		
กฎหมาย	FOIA (สหรัฐอเมริกา)	พระราชบัญญัติข้อมูลข่าวสารราชการฯ
(กรณีจำเป็นเพื่อคุ้มครองความเป็นส่วนตัว)	ส่วนตัวเกินสมควร (unwarranted invasion of personal privacy) หน่วยงานของรัฐสามารถลบรายละเอียดออกได้[31]	ทำโดยประการอื่นใดที่ไม่เป็นการเปิดเผยข้อมูลข่าวสารนั้น (มาตรา 9 วรรคสอง)

ศาลฎีกาของสหรัฐอเมริกาวินิจฉัยว่าข้อมูลที่ถูกร้องขอนั้นแม้จะเคยเป็นข้อมูลสาธารณะอยู่ ณ เวลาหนึ่ง แต่เมื่อคำนึงถึงต้นทุนในการระบุถึงข้อมูล ตำแหน่งที่เก็บ และการเข้าถึง ทำให้เกิดความความคาดหวังอย่างสมเหตุสมผลในความเป็นส่วนตัว (reasonable expectation of privacy)[32] ข้อมูลเกี่ยวกับตัวพี่น้องทั้งสี่นั้นไม่ได้เป็นข้อมูลสาธารณะเพียงเพราะครั้งหนึ่งเคยเป็นข้อมูลสาธารณะ แต่ความคาดหวังอย่างสมเหตุสมผลในความเป็นส่วนตัวนั้นมีอยู่เนื่องจากความยุ่งยากในการเข้าถึงข้อมูลนั้น (practical obscurity)[33] คดี *U.S. Department of Justice v. Reporters Committee* ได้แสดงให้เห็นว่าข้อมูลที่ถูกเก็บรวบรวมโดยรัฐนั้นอาจก่อให้เกิดสถานการณ์ที่จะต้องมีการใช้สิทธิที่จะถูกลืม[34]ได้ เช่น เป็นกรณีที่ข้อมูลส่วนบุคคลของปัจเจกบุคคลถูกเก็บรวบรวมโดยเจ้าหน้าที่รัฐในกระบวนยุติธรรม[35]

2.2.3 แนวทางในการสร้างสมดุลระหว่างความโปร่งใสภาครัฐกับสิทธิในความเป็นส่วนตัวของปัจเจกบุคคล

คำวินิจฉัยคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารสาขาสังคม การบริหารราชการแผ่นดินและการบังคับใช้กฎหมาย (ที่ สค 200/2565) และคดี *U.S. Department of Justice v. Reporters Committee* แสดงให้เห็นว่าการเปิดเผยข้อมูลที่หน่วยงานรัฐครอบครองนั้นสามารถเกิดขึ้นโดยไม่เป็นการทำลายการคุ้มครองความเป็นส่วนตัวของปัจเจกบุคคล

---

[31] Ibid.

[32] Christopher Kotfila, 'This Message Will Self-Destruct: The Growing Role of Obscurity and Self-Destructing Data in Digital Communication' (2014) Bulletin of the Association for Information Science and Technology 40(2) 12, 13.

[33] Ibid.

[34] สิทธิที่จะถูกลืม (Right to be Forgotten) หมายถึง สิทธิของเจ้าของข้อมูลส่วนบุคคลที่ข้อมูลส่วนบุคคลของตนจะถูกลบทำลาย หรือทำให้ไม่สามารถระบุตัวตนได้เมื่อหมดความจำเป็นที่ข้อมูลนั้นจะต้องถูกประมวลผลหรือเข้าถึงได้อีกต่อไป ไม่ว่าจะโดยการที่เจ้าของข้อมูลส่วนบุคคลร้องขอหรือผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการโดยปราศจากการร้องขอของเจ้าของข้อมูลส่วนบุคคล

[35] ปิติ เอี่ยมจำรูญลาภ, *บทบัญญัติทางกฎหมายว่าด้วยสิทธิที่จะถูกลืม (Right to be Forgotten) และแนวทางแก้ไขกฎหมายที่เกี่ยวข้อง* (สถาบันพระปกเกล้า 2565) 58.

ข้อมูลข่าวสารของเทศบาลตำบลด่านเกวียนเกี่ยวกับค่าตอบแทนนั้นเป็นข้อมูลที่ช่วยให้ข่าวสารจะแสดงให้เห็นถึงความถูกต้องโปร่งใส และตรวจสอบได้ของหน่วยงานของรัฐ โดยการเปิดเผยเพื่อสร้างความโปร่งใสดังกล่าวไม่จำเป็นต้องมีการเปิดเผยถึงตัวตนของปัจเจกบุคคล ด้วยเหตุนี้ จึงมีการไม่เปิดเผยข้อมูลส่วนที่จะกระทบต่อสิทธิส่วนบุคคลได้ ในขณะที่ คดี *U.S. Department of Justice v. Reporters Committee* ก็แสดงให้เห็นว่าข้อมูลส่วนบุคคลที่เคยมีประโยชน์จากการให้สารณชนเข้าถึง ณ เวลาหนึ่ง อาจหมดความจำเป็นที่จะต้องถูกเข้าถึงได้เมื่อเวลาผ่านพ้นไป โดยสามารถแสดงแนวทางการวิเคราะห์ได้ตามตารางที่ 2 ดังนี้

ตารางที่ 2 : แนวทางการวิเคราะห์เพื่อสร้างความสมดุลระหว่าง ความโปร่งใสภาครัฐและความเป็นส่วนตัวของปัจจเจกบุคคล		
ข้อมูล	ค่าตอบแทนการจ่ายเงินประโยชน์ตอบแทนอื่นเป็นกรณีพิเศษ รายการประชุมคณะกรรมการพิจารณาจ่ายเงินประโยชน์ตอบแทนอื่น สำเนาหลักฐานการลงรับหนังสือขอรับประโยชน์ตอบแทนอื่นขององค์กรปกครองส่วนท้องถิ่น	
การแยกแยะองค์ประกอบ	ส่วนที่แสดงถึงเฉพาะการปฏิบัติงานของหน่วยงานรัฐเท่านั้น	ส่วนที่ระบุถึงตัวตนของผู้รับเงินได้ (เป็นข้อมูลส่วนบุคคล)
ประโยชน์ที่ถูกคุ้มครอง	ประโยชน์สาธารณะ (ความถูกต้องโปร่งใส และตรวจสอบได้ของหน่วยงานของรัฐ)	สิทธิในความเป็นส่วนตัว
มิติด้านเวลา	เป็นข้อมูลข่าวสารราชการซึ่งอาจมีการลบทำลายเมื่อถึงเวลาที่กฎหมายกำหนด	เมื่อเวลาพ้นผ่านไปอาจไม่ความจำเป็นที่สาธารณชนจะต้องเข้าถึงข้อมูลนี้
การเปิดเผยข้อมูล	✓	✗

ตารางที่ 2 แสดงให้เห็นว่าการเปิดเผยข้อมูลข่าวสารของราชการเพื่อสร้างความโปร่งใสภาครัฐนั้นสามารถดำเนินการโดยไม่เป็นการทำลายการคุ้มครองข้อมูลส่วนบุคคลจนเกินสมควรและสามารถเกิดขึ้นควบคู่ไปกับการคุ้มครองข้อมูลส่วนบุคคลตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ได้

2.3 ความท้าทายในการรักษาความมั่นคงปลอดภัยของข้อมูล

ความท้าทายในโลกยุคดิจิทัลอาจเกิดขึ้นจากปัญหาความปลอดภัยทางไซเบอร์ “ข้อมูลข่าวสารของราชการ” ที่หน่วยงานรัฐครอบครองอาจถูกเก็บรวบรวมและเก็บรักษาโดยระบบอิเล็กทรอนิกส์ ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ (ฉบับที่ 4) พ.ศ. 2564 กำหนดให้ยกเลิกความในข้อ 29 แห่งระเบียบสำนักนายกรัฐมนตรี ว่าด้วยงานสารบรรณ พ.ศ. 2526 ซึ่งแก้ไขเพิ่มเติมโดยระเบียบสำนักนาย กรัฐมนตรี ว่าด้วยงานสารบรรณ (ฉบับที่ 2) พ.ศ. 2548 และให้ใช้ความต่อไปนี้แทน

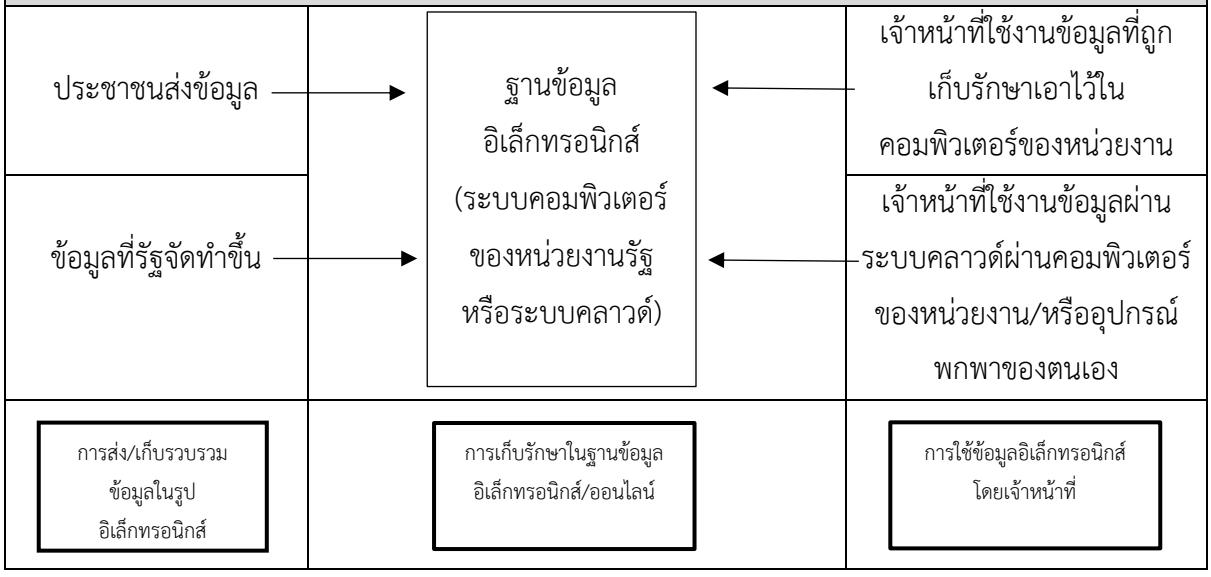
"การติดต่อราชการให้ดำเนินการด้วยระบบสารบรรณอิเล็กทรอนิกส์เป็นหลักเว้นแต่กรณีที่เป็นข้อมูลข่าวสารลับชั้นลับที่สุดตามระเบียบว่าด้วยการรักษาความลับของทางราชการหรือเป็นสิ่งที่เป็นความลับของทางราชการชั้นลับที่สุดตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ หรือมีเหตุจำเป็นอื่นใดที่ไม่สามารถรถดำเนินการด้วยระบบสารบรรณอิเล็กทรอนิกส์ได้"[36]

นอกจากนี้ ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ (ฉบับที่ 4) พ.ศ. 2564 ยังให้ยกเลิกความในวรรคสองของข้อ 27 แห่งระเบียบสำนักนายกรัฐมนตรี ว่าด้วยงานสารบรรณ พ.ศ. 2526 ซึ่งแก้ไขเพิ่มเติมโดยระเบียบสำนักนายกรัฐมนตรี ว่าด้วยงานสารบรรณ (ฉบับที่ 2) พ.ศ. 2548 ซึ่งให้นิยามของ "หนังสืออื่น"[37] เอาไว้ และให้ใช้ข้อความต่อไปนี้แทน

"สื่อกลางบันทึกข้อมูลตามวรรคหนึ่ง หมายความว่า สื่อใดๆ ที่อาจใช้บันทึกข้อมูลได้ด้วยอุปกรณ์ทางอิเล็กทรอนิกส์ รวมตลอดทั้งพื้นที่ที่ส่วนราชการใช้ในการจัดเก็บข้อมูลอิเล็กทรอนิกส์ด้วย เช่น บริการคลาวด์ (cloud computing)"[38]

เมื่อพิจารณาระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณซึ่งถูกแก้ไขเพิ่มเติมข้างต้นแล้ว กล่าวได้ว่าหน่วยงานรัฐสามารถเก็บรวบรวมและใช้ข้อมูลข่าวสารราชการซึ่งถูกเก็บในรูปอิเล็กทรอนิกส์และอาจถูกเก็บรักษาในระบบคลาวด์ได้โดยสามารถแสดงให้เห็นตัวอย่างตามแผนภาพที่ 1 ดังนี้

แผนภาพที่ 1 : การเก็บรวบรวม เก็บรักษา และใช้ข้อมูลข่าวสารราชการในรูปแบบอิเล็กทรอนิกส์



[36] ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ (ฉบับที่ 4) พ.ศ. 2564 ข้อ 7.

[37] "หนังสืออื่น" คือ หนังสือหรือเอกสารอื่นใดที่เกิดขึ้นเนื่องจากการปฏิบัติงานของเจ้าหน้าที่เพื่อเป็นหลักฐานในราชการ ซึ่งรวมถึงภาพถ่าย ฟิลม์ แถบบันทึกเสียง แถบบันทึกภาพ และสื่อกลางบันทึกด้วย หรือหนังสือของบุคคลภายนอก ที่ยื่นต่อเจ้าหน้าที่และเจ้าหน้าที่ได้รับเข้าทะเบียนของทางราชการแล้ว มีรูปแบบตามที่กระทรวง ทบวง กรม จะกำหนดขึ้นตามความเหมาะสม เว้นแต่มีแบบตามกฎหมายเฉพาะเรื่องให้ทำตามแบบ เช่น โฉนด แผนที่ แบบ แผนผัง สัญญา หลักฐานการสืบสวนและคำร้อง เป็นต้น

[38] ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ (ฉบับที่ 4) พ.ศ. 2564 ข้อ 6.

การส่งหรือเก็บรวบรวมข้อมูลในรูปอิเล็กทรอนิกส์ การเก็บรักษาในฐานข้อมูลอิเล็กทรอนิกส์หรือออนไลน์ การใช้ข้อมูลอิเล็กทรอนิกส์โดยเจ้าหน้าที่นั้นอาจภัยคุกคามทางไซเบอร์[39] จากการกระทำของอาชญากรไซเบอร์และอาจรั่วไหลอันเกิดจากการประมาทของเจ้าหน้าที่ของหน่วยรัฐ

2.3.1 การรักษาความมั่นคงปลอดภัยไซเบอร์

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 (“พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ฯ”) ให้นิยามของ “การรักษาความมั่นคงปลอดภัยไซเบอร์” เอาไว้ว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ[40] ส่วน “ภัยคุกคามทางไซเบอร์” หมายความว่า การกระทำหรือการดำเนินการใดๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง[41]

หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศมีหน้าที่ตาม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ฯต้องจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว[42]

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานสำหรับให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนำไปใช้เป็นแนวทางในการจัดทำหรือนำไปใช้เป็นประมวลแนวทางปฏิบัติของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตน และในกรณีที่หน่วยงานดังกล่าวยังไม่มีหรือมีแต่ไม่ครบถ้วนหรือไม่สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ให้นำประมวลแนวทางปฏิบัติและกรอบมาตรฐานดังกล่าวไปใช้บังคับ[43]
นอกจากนี้ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้ออกประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการ

---

[39] “ไซเบอร์” หมายความรวมถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมต่อกันเป็นการทั่วไป

[40] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 3.

[41] เพิ่งอ้าง.

[42] เพิ่งอ้าง มาตรา 44 วรรคหนึ่ง.

[43] เพิ่งอ้าง มาตรา 44 วรรคสาม.

รักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 เพื่อเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญ หรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากลเพื่อสนับสนุนการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ[44]

2.3.2 การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

การมีมาตรการความมั่นคงปลอดภัยที่เหมาะสมมีวัตถุประสงค์เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยผู้ที่ไม่ได้รับอนุญาตทั้งเจตนาและไม่ได้เจตนา ซึ่งในบางกรณีความมั่นคงปลอดภัยของข้อมูลอาจถือเป็นความมั่นคงปลอดภัยทางไซเบอร์ประเภทหนึ่ง เนื่องจากเป็นการป้องกันเครือข่ายและระบบข้อมูลขององค์กรจากการโจมตีทางไซเบอร์ และยังครอบคลุมถึงเรื่องมาตรการความมั่นคงปลอดภัยทางกายภาพและทางองค์กร (physical and organisational security measures) อีกด้วย[45]

มาตรา 37(1) แห่ง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ เป็นส่วนหนึ่งที่แสดงให้เห็นว่ากฎหมายสามารถสร้างแนวทางการดำเนินการเพื่อสร้างความมั่นคงปลอดภัยแก่ข้อมูลส่วนบุคคล โดยกฎหมายบัญญัติให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่

“จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด”

ตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 มาตรการรักษาความความมั่นคงปลอดภัย หมายความว่า “การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของ

---

[44] ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564, บทนำ.

[45] ปิติ เอี่ยมจำรูญลาภ และ ปรีชา เลิศอัศววิวัฒน์, ‘โครงการศึกษาและพัฒนามาตรฐานความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Samsung Knox Solutions)’ (รายงานผลการวิจัยเสนอต่อบริษัท ไทยซัมซุง อิเลคโทรนิคส์ จำกัด), คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย 2564.

ข้อมูลส่วนบุคคล ทั้งนี้เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ[46]

มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องครอบคลุมการเก็บรวบรวม ใช้และเปิดเผยข้อมูลส่วนบุคคล ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ไม่ว่าข้อมูลส่วนบุคคลดังกล่าวจะอยู่ในรูปแบบเอกสารหรือในรูปแบบอิเล็กทรอนิกส์ หรือรูปแบบอื่นใดก็ตาม[47] นอกจากนี้ มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องประกอบด้วยมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) ที่เหมาะสม ซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่จำเป็นด้วย โดยคำนึงถึงระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบจากเหตุการละเมิดข้อมูลส่วนบุคคล[48]

2.3.3 แนวทางในการรักษาความมั่นคงปลอดภัยของข้อมูอิเล็กทรอนิกส์และการใช้งานข้อมูลในฐานข้อมูลอิเล็กทรอนิกส์

การที่หน่วยงานของรัฐ (ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ องค์กรฝ่ายนิติบัญญัติ องค์กรฝ่ายตุลาการ องค์กรอิสระ องค์การมหาชน และหน่วยงานอื่นของรัฐ) มีหน้าที่ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตาม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ฯ และมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ซึ่งมีหน้าที่ต้องรักษาความมั่นคงปลอดภัยทางของข้อมูลส่วนบุคคลตามมาตรฐานที่กำหนดขึ้นตามมาตรา 37(1) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ย่อมนับได้ว่าเป็น “โอกาส” ที่หน่วยงานของรัฐจะสามารถบริหารจัดการความเสี่ยงอันเกิดจากภัยคุกคามทางไซเบอร์หรือการรั่วไหลของข้อมูลส่วนบุคคลโดยความประมาทเลินเล่อ ซึ่งสามารถแสดงตัวอย่างได้ตามตารางที่ 3 ด้านล่างนี้

---

[46] ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ข้อ 3.

[47] เพิ่งอ้าง ข้อ 4(1).

[48] เพิ่งอ้าง ข้อ 4(2).

ตารางที่ 3 : ตัวอย่างแนวทางในการรักษาความมั่นคงปลอดภัยของข้อมูลอิเล็กทรอนิกส์และการใช้งานข้อมูลในฐานข้อมูลอิเล็กทรอนิกส์		
กฎหมาย	พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ฯ	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ
สถานะของหน่วยงาน	หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	ผู้ควบคุมข้อมูลส่วนบุคคล
ความท้าทาย	ถูกอาชญากรไซเบอร์ใช้โปรแกรมไม่พึงประสงค์โดยมุ่งประทุษร้ายต่อข้อมูลคอมพิวเตอร์ของหน่วยงานของรัฐ	เจ้าหน้าที่ทำอุปกรณ์พกพาส่วนตัวซึ่งสามารถเข้าถึงข้อมูลส่วนบุคคลในฐานะข้อมูลออนไลน์ได้หาย
มาตรการ (ตัวอย่าง)	- จัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ[49] - จัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์[50]	- นโยบายการรักษาความมั่นคงปลอดภัยของข้อมูลภายในองค์กร โดยกำหนดข้อปฏิบัติแก่เจ้าหน้าที่ และ จำกัดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลเท่าที่จำเป็นต่อการปฏิบัติงานเท่านั้น - จัดหาอุปกรณ์มือถือที่ได้รับการออกแบบมาด้วยความปลอดภัยซึ่งมีเทคโนโลยีการพิสูจน์ตัวตน มีนวัตกรรมการจดจำใบหน้าและลายนิ้วมือ เสียง การเข้าถึงข้อมูลแม้ว่าอุปกรณ์จะสูญหายหรือถูกขโมย

3. บทสรุป

เมื่อพิจารณาแล้วว่ารัฐต้องเก็บรวบรวมข้อมูลเท่าที่จำเป็นและชี้แจงรายละเอียดการประมวลผลข้อมูลที่ถูกเก็บรวบรวม การดำเนินการเพื่อเก็บรวบรวมและเก็บรักษาข้อมูลต้องระบุว่าการเก็บและใช้ข้อมูลนั้นมีความจำเป็นเพื่อดำเนินการอย่างไร และในกรณีการเปิดเผยข้อมูลข่าวสารของราชการตามพระราชบัญญัติข้อมูลข่าวสารราชการฯ นั้นสามารถดำเนินการโดยไม่เป็นการทำลายการคุ้มครองความเป็นส่วนตัวของปัจเจกบุคคลและสามารถเกิดขึ้นควบคู่ไปกับการคุ้มครองข้อมูลส่วนบุคคลตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ได้ อย่างไรก็ตาม การบังคับใช้กฎหมายดังกล่าวจะต้องคำนึงถึงปัจจัยต่างๆ เพื่อสร้างความสมดุล

[49] ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564, 17.

[50] เพิ่งอ้าง 5.

ระหว่างความโปร่งใสภาครัฐและความเป็นส่วนตัวของปัจเจกบุคคล การดำเนินการดังกล่าวอาจดำเนินการได้โดยการแยกแยะองค์ประกอบของข้อมูลเพื่อแยกข้อมูลที่จำเป็นต่อการตรวจสอบการทำงานภาครัฐและข้อมูลที่กระทบต่อความเป็นส่วนตัวของปัจเจกบุคคล เมื่อได้แยกแยะข้อมูลดังกล่าวแล้วก็จะเห็นถึงประโยชน์ของการเปิดเผยข้อมูลในแต่ละส่วนกล่าวคือส่วนที่เป็นประโยชน์สาธารณะและส่วนที่เป็นข้อมูลส่วนบุคคล การเปิดเผยสามารถเลือกเฉพาะส่วนที่ไม่เป็นการรุกล้ำความเป็นส่วนตัวเกินสมควรหรือส่วนที่ไม่จำเป็นต่อการตรวจสอบการทำงานของหน่วยงานรัฐได้ซึ่งเป็นแนวทางการปฏิบัติที่สอดคล้องกับการดำเนินการในต่างประเทศ เช่น กฎหมาย FOIA ของสหรัฐอเมริกา โดยเมื่อพิจารณาร่วมกับแนวทางตามกฎหมายไทยดังปรากฏในคำวินิจฉัยคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารสาขาสังคม การบริหารราชการแผ่นดินและการบังคับใช้กฎหมาย (ที่ สค 200/2565) แล้วจะเห็นว่ารัฐจะต้องเปิดเผยข้อมูลข่าวสารของราชการที่จะแสดงให้เห็นถึงความถูกต้องโปร่งใส และตรวจสอบได้ของหน่วยงานของรัฐ อย่างไรก็ตามเป็นหน้าที่ของรัฐที่การเปิดเผยเพื่อสร้างความโปร่งใสดังกล่าวจะต้องไม่กระทบต่อข้อมูลที่การเปิดเผยจะเป็นการรุกล้ำสิทธิส่วนบุคคลโดยไม่สมควร และต้องพิจารณาถึงสถานการณ์ที่จะต้องมีการใช้สิทธิที่จะถูกลืมได้ เช่น เป็นกรณีที่ข้อมูลส่วนบุคคลของปัจเจกบุคคลถูกเก็บรวบรวมโดยเจ้าหน้าที่รัฐในกระบวนยุติธรรม ดังนั้นการร้องขอให้เปิดเผยข้อมูลข่าวสารของทางราชการเพื่อตรวจสอบความโปร่งใสในอนาคต หน่วยงานของรัฐจึงต้องมีความระวัดระวังทั้งในเรื่องของการจัดเก็บข้อมูลส่วนบุคคลและการเปิดเผยข้อมูลส่วนบุคคลให้เป็นไปตามพระราชบัญญัติข้อมูลข่าวสารของราชการฯและพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ อันเป็นสร้างสมดุลระหว่างการเปิดเผยข้อมูลข่าวสารของราชการกับการคุ้มครองความเป็นส่วนตัวของปัจเจกบุคคลในทางปฏิบัติให้เหมาะสม

เนื่องจากติดต่อราชการได้กลายเป็นการดำเนินการด้วยระบบสารบรรณอิเล็กทรอนิกส์เป็นหลัก การส่งหรือเก็บรวบรวมข้อมูลในรูปอิเล็กทรอนิกส์ การเก็บรักษาในฐานข้อมูลอิเล็กทรอนิกส์หรือออนไลน์ การใช้ข้อมูลอิเล็กทรอนิกส์โดยเจ้าหน้าที่ย่อมกลายเป็นสิ่งที่หลีกเลี่ยงไม่ได้ ซึ่งหน่วยงานของรัฐครอบครองอยู่ตามพระราชบัญญัติข้อมูลข่าวสารของราชการฯ และรวมถึงการที่ข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ อยู่ในรูปข้อมูลอิเล็กทรอนิกส์หรือออนไลน์ ซึ่งสิ่งเหล่านี้ก่อให้เกิด “ความท้าทาย” เช่นภัยคุกคามทางไซเบอร์อันเป็นกระทำโดยจงใจของอาชญากรไซเบอร์ หรือการรั่วไหลของข้อมูลอันอาจเกิดจากการประมาทของเจ้าหน้าที่ของหน่วยรัฐ ซึ่งหน่วยงานของรัฐมีหน้าที่ทั้งตามพระราชบัญญัติ ความมั่นคงทางไซเบอร์ ในฐานะเป็นหน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการรักษาความมั่นคงปลอดภัยของข้อมูอิเล็กทรอนิกส์และการใช้งานข้อมูลในฐานข้อมูลอิเล็กทรอนิกส์ และหน้าที่ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ในฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล ในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

การที่หน่วยงานของรัฐมีหน้าที่ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามพระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ฯ และขณะเดียวกันก็มีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ซึ่งมีหน้าที่ต้องรักษาความมั่นคงปลอดภัยทางของข้อมูล

ส่วนบุคคลตามมาตรฐานที่กำหนดขึ้นตามมาตรา 37(1) แห่ง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ และประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2565 ย่อมนับได้ว่าเป็น “โอกาส” ที่หน่วยงานของรัฐจะสามารถบริหารจัดการความเสี่ยงอันเกิดจากภัยคุกคามทางไซเบอร์หรือการรั่วไหลของข้อมูลส่วนบุคคลโดยความประมาทเลินเล่อได้ โดยเป็นการรักษาและคุ้มครองข้อมูลส่วนบุคคลโดยอาศัยอำนาจหน้าที่ที่กฎหมายทั้งสองฉบับส่งเสริมซึ่งกันและกันในการคุ้มครองข้อมูลส่วนบุคคล เช่น การจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์เพื่อเป็นแนวทางปฏิบัติของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตน ร่วมกับการจัดหาอุปกรณ์ที่ได้รับการออกแบบมาด้วยความปลอดภัยให้กับเจ้าหน้าที่ เป็นต้น ขั้นตอนการรักษาข้อมูลส่วนบุคคลในแง่นี้จำเป็นต้องคำนึงถึงทั้งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ และพระราชบัญญัติความมั่นคงทางไซเบอร์ฯ

ผู้สนับสนุนหลักในการจัดพิมพ์วารสาร

บทความแต่ละบทความเป็นความคิดเห็นอิสระของผู้เขียน