

แนวทางการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลใน
การพัฒนาเมืองอัจฉริยะ: กรณีศึกษาเมืองอัจฉริยะพิษณุโลก
Guidelines for Data Protection Impact Assessment (DPIA) in
Smart City Development: A Case Study of Phitsanulok Smart City

เมธิณี สุวรรณกิจ¹

คณะนิติศาสตร์ มหาวิทยาลัยนเรศวร 99 หมู่ 9 ตำบลท่าโพธิ์ อำเภอเมือง จังหวัดพิษณุโลก 65000

เมลติดต่อ: methinees@nu.ac.th

Methinee Suwannakit

Faculty of Law, Naresuan University, 99, Moo 9, Tha Pho, Mueang, Phitsanulok, 65000,

E-mail: methinees@nu.ac.th

Received: May 30, 2025; Revised: August 8, 2025; Accepted: October 2, 2025

บทคัดย่อ

บทความวิจัยนี้ได้นำเสนอแนวทางการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลในการพัฒนาเมืองอัจฉริยะ กรณีศึกษาเมืองอัจฉริยะพิษณุโลก โดยได้ดำเนินการวิจัยแบบผสมผสานประกอบด้วย การศึกษากฎหมายเปรียบเทียบ การวิเคราะห์ข้อมูลเอกสาร และการสัมภาษณ์ถึงโครงสร้างเพื่อสำรวจความคิดเห็นของเจ้าของข้อมูลส่วนบุคคล จากการศึกษพบว่าผลกระทบข้อมูลส่วนบุคคลในเมืองอัจฉริยะพิษณุโลกมีความเสี่ยงสูง มีเส้นทางการไหลของข้อมูลที่ซับซ้อน มีเขตพื้นที่ซับซ้อน และมีหน่วยงานที่เกี่ยวข้องเป็นจำนวนมาก จึงควรมีการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล จัดทำแผนผังการไหลเวียนของข้อมูลอย่างละเอียด จัดทำบันทึกข้อตกลงการเป็นผู้ควบคุมข้อมูลส่วนบุคคลร่วม ประเมินความจำเป็นและได้สัดส่วน ประเมินความเสี่ยงและดำเนินการตามมาตรการจัดการความเสี่ยงที่เหมาะสม โดยบทความนี้ได้รับความเสี่ยงพร้อมเสนอมาตรการจัดการความเสี่ยงใน 3 ประเด็นหลัก ดังนี้ (1) ข้อมูลรั่วไหลอันเกิดจากความเสี่ยงภายในและภายนอก (2) เจ้าของข้อมูลส่วนบุคคลไม่สามารถควบคุมการใช้งานข้อมูลของตนได้ และ (3) ผลกระทบต่อสิทธิและเสรีภาพอื่นๆ

คำสำคัญ: การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล กฎหมายคุ้มครองข้อมูลส่วนบุคคล เมืองอัจฉริยะ

¹ อาจารย์ประจำ, คณะนิติศาสตร์ มหาวิทยาลัยนเรศวร (Lecturer, Faculty of Law, Naresuan University)



Abstract

This research article presents a guideline for data protection impact assessment (DPIA) in the development of smart cities, using Phitsanulok Smart City as a case study. The study employs a mixed-methods approach, including comparative legal analysis, document analysis, and semi-structured interviews to gather the perspectives of data subjects. The findings reveal that personal data processing in Phitsanulok smart cities entails high risks due to complex data flow pathways, overlapping jurisdictions, and the involvement of numerous stakeholders. Therefore, a personal data protection impact assessment (DPIA) is necessary. This should include detailed data flow mapping, the establishment of joint data controller agreements, assessments of necessity and proportionality, as well as risk assessments and the implementation of appropriate risk mitigation measures. The article identifies risks and proposes risk mitigation measures in three key areas: (1) data breaches resulting from internal and external risks; (2) the inability of data subjects to control the use of their personal data; and (3) adverse impacts on other rights and freedoms.

Keywords: Data Protection Impact Assessment, Personal Data Protection Act, Smart City

1. บทนำ

ในปัจจุบันเมืองต่าง ๆ ทั่วโลกได้ให้ความสำคัญกับการพัฒนาเมืองให้น่าอยู่และทันสมัยไปพร้อมกับการพัฒนาเทคโนโลยี แนวคิดเรื่องเมืองอัจฉริยะจึงได้ถูกนำมาใช้เพื่อการบริหารและจัดการเมืองมีประสิทธิภาพแม้เมืองอัจฉริยะจะไม่มีนิยาม หรือความหมายที่ชัดเจนโดยจะแปรผันไปตามความต้องการ วัตถุประสงค์ และวิธีการดำเนินการของแต่ละเมือง แต่เป็นที่ยอมรับตรงกันว่าลักษณะสำคัญที่บ่งบอกความเป็นเมืองอัจฉริยะ คือเทคโนโลยีสารสนเทศ ซึ่งประกอบไปด้วยเทคโนโลยีขั้นสูง หรือนวัตกรรมที่ทันสมัยกับข้อมูลมหัต (Big Data)² สำหรับประเทศไทย ประกาศคณะกรรมการขับเคลื่อนการพัฒนาเมืองอัจฉริยะที่ 1/2562 ได้ให้นิยามเมืองอัจฉริยะว่าเป็นเมืองที่ใช้ประโยชน์จากเทคโนโลยีและนวัตกรรมที่ทันสมัยและชาญฉลาด เพื่อเพิ่มประสิทธิภาพของการให้บริการและการบริหารจัดการเมือง ลดค่าใช้จ่ายและการใช้ทรัพยากรของเมืองและประชากรเป้าหมาย โดยเน้นการออกแบบที่ดี และการมีส่วนร่วมของภาคธุรกิจและภาคประชาชนในการพัฒนาเมืองภายใต้แนวคิดการพัฒนาเมืองน่าอยู่ เมืองทันสมัย ให้ประชาชนในเมืองมีคุณภาพชีวิตที่ดี มีความสุข อย่างยั่งยืน³ แม้นิยามดังกล่าวจะไม่ได้กล่าวถึง ข้อมูลมหัต หรือสารสนเทศโดยตรง แต่ปัจจัยสำคัญที่ช่วยส่งเสริมให้การทำงานของเทคโนโลยีและนวัตกรรมตลอดจนการบริการและการบริหารจัดการเมืองอัจฉริยะมีประสิทธิภาพและชาญฉลาดล้วนเกี่ยวข้องกับการประมวลผลข้อมูลมหัตซึ่งรวมถึงข้อมูลส่วนบุคคล การประมวลผลดังกล่าว จึงอาจส่งผลกระทบต่อประชากรในเมืองอัจฉริยะผู้เป็นเจ้าของข้อมูลส่วนบุคคล (Data Subjects) เพื่อสร้างความมั่นใจให้ประชากรใช้บริการหรือร่วมกิจกรรมต่าง ๆ ในเมืองอัจฉริยะ จึงควรดำเนินการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA) (ซึ่งต่อไปนี้จะเรียกว่า DPIA)

แม้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (ซึ่งต่อไปนี้จะเรียกว่า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล) ไม่ได้บังคับให้ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ต้องจัดทำ DPIA แต่ผู้ควบคุมข้อมูลส่วนบุคคลควรดำเนินการ เพื่อช่วยให้ตนปฏิบัติตามหน้าที่ต่าง ๆ ตามที่กำหนดในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ได้อย่างถูกต้องครบถ้วน และเพื่อให้สามารถประเมิน ระบุความเสี่ยงและชี้แจงมาตรการที่เหมาะสมในการรักษาความปลอดภัย หรือเพื่อลดความเสี่ยงได้ เช่น มาตรา 37(4) กำหนดให้ผู้ควบคุม

² Laurens Vandercruysse, Caroline Buts, Michael Doods, "A typology of Smart City services: The case of Data Protection Impact Assessment," *Cities* 104 (2020): 102731.

³ ประกาศคณะกรรมการขับเคลื่อนการพัฒนาเมืองอัจฉริยะที่ 1/2562 เรื่อง หลักเกณฑ์การประเมินและคุณสมบัติ วิธีการและกระบวนการในการพิจารณาการเป็นเมืองอัจฉริยะ พ.ศ. 2562.



ข้อมูลส่วนบุคคลต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลตามความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล โดยในกรณีที่มีการละเมิดมีความเสี่ยงสูงให้แจ้งเหตุละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมแนวทางการเยียวยา นอกจากนี้ มาตรา 37(1), 39(8), 40(2) และมาตรา 4 วรรคสาม ยังได้กำหนดให้ผู้ควบคุมข้อมูล และ/หรือ ผู้ประมวลผลข้อมูลต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม ซึ่งการที่จะจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมได้นั้นจำเป็นต้องมีการประเมินความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลเช่นกัน

บทความวิจัยนี้ จึงมีวัตถุประสงค์ เพื่อเสนอแนวทางการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลในการพัฒนาเมืองอัจฉริยะ ศึกษากรณีเมืองอัจฉริยะพิษณุโลก ซึ่งอาจใช้เป็นต้นแบบสำหรับเมืองอัจฉริยะอื่นๆ

บทความวิจัยฉบับนี้ เป็นงานวิจัยเชิงคุณภาพ (Qualitative Research) โดยใช้วิธีการวิจัยแบบผสมผสาน (Multi-methods) ประกอบด้วย การศึกษากฎหมายเปรียบเทียบ (Comparative Law) และการวิเคราะห์ข้อมูลเอกสาร (Documentary Research) นอกจากนี้ ยังมีการสำรวจความคิดเห็นของประชากรในเขตพื้นที่เมืองอัจฉริยะพิษณุโลกด้วยวิธีการสัมภาษณ์แบบกึ่งโครงสร้าง (Semi-Structured Interview) โดยมุ่งเน้นการใช้คำถามปลายเปิด ซึ่งได้ประเด็นคำถามมาจากการทบทวนวรรณกรรม ตัวอย่างคำถาม เช่น “ท่านมีความกังวลว่าข้อมูลส่วนบุคคลของท่านจะถูกละเมิด หรือได้รับผลกระทบจากการใช้บริการสาธารณะหรือไม่” “ท่านมีความกังวลเรื่องใดมากที่สุด” และ “ความกังวลนั้นส่งผลต่อการตัดสินใจใช้บริการเมืองอัจฉริยะของท่าน หรือไม่ เพราะเหตุใด” สำหรับการเลือกกลุ่มตัวอย่างเพื่อเก็บรวบรวมข้อมูลนั้น ผู้วิจัยได้เลือกกลุ่มนิสิตและประชากรที่ใช้บริการสาธารณะในเขตพื้นที่มหาวิทยาลัยนเรศวร จำนวน 24 คน และประชากรในเขตอำเภอเมืองพิษณุโลกและเขตเทศบาลนครพิษณุโลก รวม 17 คน เนื่องจาก ข้อจำกัดทางด้านเวลาจึงไม่ได้สำรวจกลุ่มตัวอย่างในเขตพื้นที่อำเภอนครไทย โดยใช้วิธีการเลือกกลุ่มเป้าหมายแบบบังเอิญ (Accidental Sampling) ไม่มีการสร้างเงื่อนไข หรือกำหนดลักษณะของกลุ่มเป้าหมายเป็นพิเศษ เพราะผู้วิจัยเห็นว่าประชากรทุกคนในพื้นที่ต่างเป็นผู้มีส่วนได้ส่วนเสียและมีความเสี่ยงที่จะได้รับผลกระทบจากการประมวลผลข้อมูลส่วนบุคคล เมื่อได้ข้อมูลมาแล้ว ผู้วิจัยได้ใช้วิธีการวิเคราะห์เนื้อหา (Content Analysis) ในการวิเคราะห์และแปลผลข้อมูล

แม้ขนาดกลุ่มตัวอย่างและการเลือกกลุ่มเป้าหมายแบบบังเอิญจะมีข้อจำกัด แต่ก็สามารถนำมาใช้เป็นข้อมูลเบื้องต้นในการวิเคราะห์ความคิดเห็นของประชากรและพิจารณาความเสี่ยงอันถือเป็นขั้นตอนหนึ่งในการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลได้

อนึ่ง เนื่องจากบทความวิจัยนี้ มุ่งเน้นการศึกษาแนวทางการคุ้มครองข้อมูลส่วนบุคคลด้านกฎหมายเป็นหลัก จึงมีข้อจำกัดในการนำเสนอมาตรการลดความเสี่ยง หรือการจัดการข้อมูลในเชิงเทคนิค และบทความวิจัยนี้เป็นเพียงแนวทางการจัดทำ DPIA ไม่ใช่บทสรุปของการจัดทำ DPIA สำหรับเมืองอัจฉริยะพิษณุโลก แต่ภาครัฐ ภาคเอกชน ภาคการศึกษา ตลอดจนหน่วยงานที่เกี่ยวข้องกับการพัฒนาเมืองอัจฉริยะสามารถนำผลการวิจัยนี้ไปพัฒนาต่อยอดและใช้ประโยชน์ได้

2. การทำงานของเมืองอัจฉริยะพิษณุโลก

จังหวัดพิษณุโลกได้ถูกกำหนดให้เป็นหนึ่งในจังหวัดต้นแบบของแผนขับเคลื่อนการพัฒนาเมืองอัจฉริยะของประเทศไทยภายใต้แนวทางการขับเคลื่อนประเทศไทย 4.0 และกรอบยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561-2580) ซึ่งได้กำหนดการพัฒนาและดำเนินการเมืองอัจฉริยะในเขตพื้นที่อำเภอเมืองพิษณุโลก เทศบาลนครพิษณุโลก อำเภอนครไทย และมหาวิทยาลัยนเรศวร⁴ ครอบคลุมพื้นที่อำเภอเมือง 732.54 ตร.ม. จำนวนประชากรประมาณ 281,945 คน และพื้นที่อำเภอนครไทย 303 ตร.ม. จำนวนประชากรประมาณ 84,807 คน⁵ โดยการดำเนินการเมืองอัจฉริยะในเขตพื้นที่อำเภอเมืองพิษณุโลกและอำเภอนครไทยจะอยู่ภายใต้ โครงการเมืองอัจฉริยะจังหวัดพิษณุโลก ในความรับผิดชอบขององค์การบริหารส่วนจังหวัด ส่วนโครงการพิษณุโลกนครอัจฉริยะอย่างยั่งยืน จะอยู่ในเขตพื้นที่เทศบาลนครพิษณุโลกโดยมีเทศบาลนครพิษณุโลกเป็นผู้รับผิดชอบ และโครงการต้นแบบเมืองอัจฉริยะ (NU Smart City) (ซึ่งต่อไปจะเรียกว่า NU Smart City) ตั้งอยู่ในเขตพื้นที่ตำบลท่าโพธิ์ อำเภอเมือง มีมหาวิทยาลัยนเรศวรเป็นผู้รับผิดชอบ เพื่อให้เกิดความชัดเจนเมื่อกล่าวถึงกรณีศึกษา เมืองอัจฉริยะพิษณุโลก ในบทความวิจัยฉบับนี้ จะครอบคลุมเขตพื้นที่การดำเนินงานของทั้ง 3 โครงการ

ในการพัฒนาเมืองอัจฉริยะ โครงการเมืองอัจฉริยะจังหวัดพิษณุโลก ได้กำหนดแผนการพัฒนา 4 ด้าน จาก 7 ด้านตามที่ประกาศคณะกรรมการขับเคลื่อนการพัฒนาเมืองอัจฉริยะที่ 1/2562 ได้กำหนด⁶ ได้แก่ สิ่งแวดล้อมอัจฉริยะ (Smart Environment) เศรษฐกิจ

⁴ สำนักงานส่งเสริมเศรษฐกิจดิจิทัล “บทสรุปผู้บริหาร: เมืองอัจฉริยะจังหวัดพิษณุโลก,” สืบค้นจากแพลตฟอร์มข้อมูลเมืองอัจฉริยะ (City Data Platform) เมื่อ 10 มกราคม 2567, https://drive.google.com/file/d/1QCtAcVgfc_kQExfzNlrlQMx2s6Xv3O/view

⁵ สำนักงานแรงงานจังหวัดพิษณุโลก, “รายงานสถานการณ์แรงงานจังหวัดพิษณุโลกไตรมาส 1 ปี 2568,” สืบค้นเมื่อ 28 พฤษภาคม 2568, <https://phitsanulok.mol.go.th/wp-content/uploads/sites/23/2025/05/รายงานสถานการณ์ไตรมาส-1-ปี-2568.pdf>

⁶ ประกาศคณะกรรมการขับเคลื่อนการพัฒนาเมืองอัจฉริยะที่ 1/2562 เรื่อง หลักเกณฑ์การประเมินและคุณสมบัติ วิธีการและกระบวนการในการพิจารณาการเป็นเมืองอัจฉริยะ



อัจฉริยะ (Smart Economy) การบริหารภาครัฐอัจฉริยะ (Smart Governance) และการขนส่งอัจฉริยะ (Smart Mobility) ในขณะที่ โครงการพิษณุโลกนครอัจฉริยะอย่างยั่งยืน ได้กำหนดพัฒนาทั้ง 7 ด้าน จึงรวมถึง พลังงานอัจฉริยะ (Smart Energy) พลเมืองอัจฉริยะ (Smart People) และการดำรงชีวิตอัจฉริยะ (Smart Living)⁷ และโครงการ NU Smart City ได้กำหนดการพัฒนา 3 ด้าน ได้แก่ พลังงานอัจฉริยะ สิ่งแวดล้อมอัจฉริยะและการขนส่งอัจฉริยะ โดยในระยะแรก จังหวัดพิษณุโลกได้มุ่งพัฒนาโครงข่ายคมนาคมและโครงสร้างพื้นฐาน เพื่อสนับสนุนการออกแบบและการพัฒนาสู่เมืองอัจฉริยะ เช่น การติดตั้งเสาอัจฉริยะเพื่อปล่อยสัญญาณไวไฟ (Wi-Fi) ในพื้นที่สาธารณะ และมีการพัฒนาระบบข้อมูลเมือง (City Data Platform) ซึ่งได้มีการจัดตั้งคณะทำงาน กำหนดชุดข้อมูลที่เกี่ยวข้อง กำหนดธรรมาภิบาลข้อมูล กำหนดลำดับขั้นของการเข้าถึงข้อมูล ได้แก่ ประชาชน หน่วยงานเอกชนและผู้ประกอบการ หน่วยงานภาครัฐ และผู้บริหารหน่วยงาน และมีการกำหนดการแลกเปลี่ยนข้อมูลผ่าน ส่วนต่อประสานโปรแกรมประยุกต์ (Application Programming Interface: API (ซึ่งต่อไปจะเรียกว่า API)⁸ นอกจากนี้ ในการพัฒนาเมืองอัจฉริยะพิษณุโลกในด้านต่าง ๆ ยังมีการใช้เทคโนโลยีและนวัตกรรม เช่น แอปพลิเคชัน ซอฟต์แวร์ อินเทอร์เน็ตประสาทรสรรพสิ่ง (Internet of Things: IoT ซึ่งต่อไปนี้จะเรียกว่า IoT) ระบบเซ็นเซอร์ ระบบตำแหน่งบนโลก (Global Positioning System: GPS ซึ่งต่อไปนี้จะเรียกว่า GPS) และระบบสารสนเทศภูมิศาสตร์ (Geographic Information System: GIS ซึ่งต่อไปนี้จะเรียกว่า GIS) และมีการนำข้อมูลหลายประเภทเข้าสู่ระบบเป็นจำนวนมาก รวมถึงข้อมูลส่วนบุคคลของประชากรในพื้นที่ อาทิ

1. สิ่งแวดล้อมอัจฉริยะ โครงการพัฒนาเทคโนโลยีการป้องกันและบรรเทาสาธารณภัย และระบบตรวจวัดคุณภาพอากาศ ต้องมีการบริหารจัดการข้อมูลตามเวลาจริง (Real-Time) เพื่อเสริมประสิทธิภาพการทำงานของ GPS และแอปพลิเคชัน
2. พลังงานอัจฉริยะ โครงการระบบบริหารจัดการไฟฟ้าสาธารณะโดยการควบคุมและสั่งการซึ่งต้องอาศัยฐานข้อมูล
3. ด้านเศรษฐกิจอัจฉริยะ โครงการแพลตฟอร์มบริหารจัดการผลผลิตทางการเกษตร ซึ่งใช้ชื่อว่า กิลอล่า (Kilola) ต้องใช้ฐานข้อมูลขนาดใหญ่ เพื่อวางแผนการจัดซื้อและการผลิต ตลอดจนการเพิ่มประสิทธิภาพผลผลิต นอกจากนั้น ศูนย์อนุรักษ์ไก่ชนนเรศวร ยังได้พัฒนานวัตกรรมในการจัดการฟาร์มเลี้ยงไก่ซึ่งต้องใช้เทคโนโลยี IoT สั่งการผ่านแอปพลิเคชันที่มีเซ็นเซอร์สำหรับติดตามและควบคุมสภาพแวดล้อม

⁷ สำนักงานส่งเสริมเศรษฐกิจดิจิทัล, “บทสรุปผู้บริหาร: พิษณุโลกนครอัจฉริยะอย่างยั่งยืน,” สืบค้นจากแพลตฟอร์มข้อมูลเมืองอัจฉริยะ (City Data Platform), สืบค้นเมื่อ 10 มกราคม 2568, <https://drive.google.com/file/d/1XQ51mDGUSgyKVofSuA6vapgYzvJYJp3W/view>

⁸ “บทสรุปผู้บริหาร: เมืองอัจฉริยะจังหวัดพิษณุโลก.”

4. การบริหารภาครัฐอัจฉริยะ โครงการปรับปรุงข้อมูลแผนที่ ภาษีและทะเบียนทรัพย์สิน ต้องมีการรวบรวมและวิเคราะห์ข้อมูลต่างๆ นอกจากนี้ ยังมีบริการเข้าถึงบริการภาครัฐผ่านช่องทางออนไลน์ ซึ่งต้องมีการเก็บรวบรวมใช้ของผู้ส่วนบุคคลของประชากรในพื้นที่

5. ขนส่งอัจฉริยะ โครงการพัฒนาเทคโนโลยีแสดงตำแหน่งระบบขนส่งมวลชนและจุดจอดรถขนส่งสาธารณะจังหวัดพิษณุโลก มีการใช้เทคโนโลยีแสดงตำแหน่งระบบขนส่งมวลชนซึ่งจำเป็นต้องมีการประมวลผลข้อมูลตามเวลาจริง (Real-Time) เช่น แอปพลิเคชันแคร์คุน (Carekoon Mobility Platform) เป็นแอปพลิเคชันที่มาจากความร่วมมือของภาครัฐและเอกชน โดยได้บูรณาการแพลตฟอร์มการคมนาคมขนส่งร่วมกับบริการสาธารณสุข เพื่อช่วยเหลือผู้สูงอายุที่อยู่ตามลำพัง ผู้พิการ รวมถึงบุคคลที่มีข้อจำกัดในการเดินทาง และยังได้ช่วยเติมเต็มโครงสร้างพื้นฐานของการขนส่งอัจฉริยะภายในจังหวัดพิษณุโลกโดยช่วยให้ผู้ใช้งานสามารถเห็นตำแหน่งของรถประจำทางบนจอมือถือได้ และกองบริการเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยเนเรศวรยังได้พัฒนาแอปพลิเคชัน NU Transit เพื่ออำนวยความสะดวกแก่ผู้ใช้บริการรถไฟฟ้าในเขตพื้นที่มหาวิทยาลัย โดยจะแสดงข้อมูลการเดินทางรถไฟฟ้าแบบตามเวลาจริง นอกจากนี้ เทศบาลนครพิษณุโลกยังมีระบบตรวจจับระดับจราจรในเมือง โดยเชื่อมโยงเครือข่ายตามเวลาจริงและระบบติดตามรถโดยสารสาธารณะ และมีการยกระดับมาตรฐานความปลอดภัยในชีวิตและทรัพย์สินและป้องกันอุบัติเหตุบนท้องถนนทั่วทั้งจังหวัดพิษณุโลก ด้วยการติดตั้งกล้องโทรทัศน์วงจรปิด (Closed-Circuit Television: CCTV) (ซึ่งต่อไปจะเรียกว่า CCTV)

6. พลเมืองอัจฉริยะ เทศบาลนครพิษณุโลกได้มีการพัฒนาหอสมุดดิจิทัลและส่งเสริมการเรียนรู้ด้านเทคโนโลยีสารสนเทศ

7. การดำรงชีวิตอัจฉริยะ เทศบาลนครพิษณุโลกมีโครงการจัดทำระบบเก็บข้อมูลคุณภาพชีวิตผู้สูงอายุในทุกมิติ และมีการพัฒนาระบบสาธารณะต่างๆ เพื่อรองรับผู้สูงอายุ

จากแผนการพัฒนาเมืองอัจฉริยะพิษณุโลกเห็นได้ว่าปัจจัยหลักของการพัฒนาเมืองอัจฉริยะพิษณุโลกมีความคล้ายคลึงกับเมืองอัจฉริยะอื่นๆ กล่าวคือ มีการพัฒนาเทคโนโลยีหรือนวัตกรรมและระบบฐานข้อมูลมหัต และมีความร่วมมือทั้งภาครัฐและภาคเอกชน



3. หลักการและขั้นตอนการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล

การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลหรือ DPIA นั้นเป็นแนวความคิดที่มีมานานแล้ว โดยได้รับอิทธิพลมาจากเครื่องมือหรือนโยบายด้านกฎหมายสิ่งแวดล้อม เช่น การประเมินผลกระทบด้านสิ่งแวดล้อม (Environment Impact Assessment หรือ EIA)⁹ Article 29 Data Protection Working Party ซึ่งเป็นหน่วยงานอิสระของสหภาพยุโรป ได้ให้ความหมายของ DPIA ว่าหมายถึง กระบวนการที่ถูกออกแบบเพื่ออธิบายการประมวลผลข้อมูล ประเมินความจำเป็นและความได้สัดส่วนของการประมวลผลนั้น และช่วยจัดการความเสี่ยงที่จะกระทบต่อสิทธิและเสรีภาพของประชาชนซึ่งเกิดจากการประมวลผล ด้วยการประเมินความเสี่ยงและการตัดสินใจใช้มาตรการต่างๆ เพื่อจัดการความเสี่ยง¹⁰ โดยการจัดทำ DPIA นั้นควรดำเนินการก่อนเริ่มโครงการต่างๆ จากการศึกษาคู่มือ หรือแนวทางการจัดทำ DPIA ของสหภาพยุโรป¹¹ สหราชอาณาจักร¹²และประเทศสิงคโปร์¹³ ต่างมีแนวทาง หรือขั้นตอนที่คล้ายคลึงกัน ซึ่งแนวทางการจัดทำ DPIA กรณีเมืองอัจฉริยะพิษณุโลก อาจสรุปเป็นขั้นตอนได้ดังต่อไปนี้

⁹ Reuben Binns, "Data Protection Impact Assessments: A Meta-Regulatory Approach," *International Data Privacy Law* 7, no. 1 (2017): 22-35.

¹⁰ Article 29 Data Protection Working Party (WP29), "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (wp248rev.01)," 4, accessed April 20, 2023, <https://ec.europa.eu/newsroom/article29/items/611236/en>.

¹¹ Article 29 Data Protection Working Party (WP29), "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (wp248rev.01)," 16-18, accessed April 20, 2023, <https://ec.europa.eu/newsroom/article29/items/611236/en>.

¹² Information Commissioner's Office, "Data Protection Impact Assessments (DPIAs)," accessed April 20, 2023, <https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias-1-0.pdf>

¹³ Personal Data Protection Commission Singapore, "Guide to Data Protection Impact Assessments," accessed April 20, 2023, <https://www.pdpc.gov.sg/help-and-resources/2017/11/guide-to-data-protection-impact-assessments>.

3.1 ระบุความจำเป็นในการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล

ตามระเบียบการคุ้มครองข้อมูลทั่วไปแห่งสหภาพยุโรป (The EU General Data Protection Regulation ซึ่งต่อไปจะเรียกว่า GDPR) ผู้ควบคุมข้อมูลส่วนบุคคลถูกบังคับให้ต้องดำเนินการจัดทำ DPIA เฉพาะในกรณีที่เป็นการประมวลผล ซึ่งมีแนวโน้มว่าจะเกิดความเสียหายสูง ที่จะกระทบต่อสิทธิและเสรีภาพของบุคคล¹⁴ ดังนั้น ในขั้นตอนแรกจึงต้องพิจารณาว่าการประมวลผลข้อมูลส่วนบุคคลในโครงการต่างๆ มีความเสี่ยงสูง หรือไม่ และระบุความจำเป็นในการจัดทำ DPIA ทั้งนี้ ในการประเมินว่าการประมวลผลข้อมูลส่วนบุคคลในกิจการ บริการ โครงการหรือผลิตภัณฑ์ใหม่ใดมีความเสี่ยงสูงที่จะกระทบสิทธิและเสรีภาพของบุคคล มาตรา 35(3) แห่ง GDPR ให้คำนึงจากลักษณะดังนี้ (1) ระบบประมวลผลข้อมูลส่วนบุคคลอัตโนมัติที่มีลักษณะกว้างโดยให้รวมถึงการทำโปรไฟล์ (Profiling) (2) การประมวลผลข้อมูลอ่อนไหว หรือข้อมูลอาชญากรรมที่มีปริมาณมาก และ (3) การเฝ้าติดตาม (Monitor) บริเวณพื้นที่สาธารณะที่มีปริมาณมากอย่างเป็นระบบ¹⁵

จากลักษณะดังกล่าวจะเห็นได้ว่าการประมวลผลข้อมูลส่วนบุคคลในเมืองอัจฉริยะพิษณุโลกนั้น เป็นการประมวลผลที่มีความเสี่ยงสูงเนื่องจาก (1) มีการนำระบบประมวลผลอัตโนมัติมาใช้ (2) มีการประมวลผลข้อมูลอ่อนไหวตามมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ในปริมาณมาก เช่น แอปพลิเคชันแคร์คันที่มีการประมวลผลข้อมูลสุขภาพและข้อมูลความพิการ และ (3) มีระบบเฝ้าติดตาม หรือตรวจสอบในบริเวณพื้นที่สาธารณะเป็นบริเวณกว้าง เช่น การติดตั้ง CCTV ตามถนน สถานีรถไฟ สนามบิน ตลาดและบริเวณพื้นที่สาธารณะอื่นๆ ดังนี้ จึงสรุปได้ว่า การประมวลผลในเมืองอัจฉริยะพิษณุโลกนั้น เป็นการประมวลผลที่มีความเสี่ยงสูงและจำเป็นต้องจัดทำ DPIA

อย่างไรก็ตาม ลักษณะของความเสี่ยงสูงตามที่กำหนดใน GDPR นั้น เป็นเพียงตัวอย่างเพื่อให้เกิดความชัดเจน Article 29 Data Protection Working Party จึงได้ออกแนวปฏิบัติสำหรับการประเมินความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคลเพิ่มเติม¹⁶ โดยได้กำหนดข้อพิจารณาการประมวลผลที่มีแนวโน้มมีความเสี่ยงสูง 9 ลักษณะ หากเข้าอย่างน้อย 2 ลักษณะ จาก 9 ลักษณะนี้ให้ถือว่าเป็นการประมวลผลที่มีความเสี่ยงสูงและต้องดำเนินการจัดทำ DPIA ซึ่งการประมวลผลข้อมูลส่วนบุคคลในเมืองอัจฉริยะพิษณุโลก อาจเข้าลักษณะต่างๆ ถึง 6 ลักษณะ จาก 9 ลักษณะ ดังต่อไปนี้

¹⁴ The EU General Data Protection Regulation (GDPR), Article 35

¹⁵ The EU General Data Protection Regulation (GDPR), Article 35(3)

¹⁶ Article 29 Data Protection Working Party (WP29), “Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 (wp248rev.01),” 9-11



1. การติดตามตรวจสอบอย่างเป็นระบบ (Systematic Monitoring) การประมวลผลข้อมูลเพื่อเฝ้าติดตามหรือเฝ้าสังเกตเจ้าของข้อมูลส่วนบุคคลอย่างเป็นระบบ เช่น การติดตั้ง CCTV เพื่อตรวจตราประชาชนในเขตพื้นที่สาธารณะของเมืองพิษณุโลก ซึ่งการประมวลผลในลักษณะนี้ มักจะกระทำโดยเจ้าของข้อมูลส่วนบุคคลไม่รู้ตัวและไม่สามารถรู้ได้ว่าข้อมูลของตนจะถูกนำไปใช้อย่างไร และเป็นการยากที่เจ้าของข้อมูลส่วนบุคคลจะหลีกเลี่ยงไม่เข้าถึง หรือใช้บริการพื้นที่สาธารณะ

2. ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) เป็นการประมวลผลข้อมูลอ่อนไหวที่มีความเสี่ยงสูงว่าจะกระทบต่อสิทธิและเสรีภาพของประชาชน เช่น แอปพลิเคชัน แคร่คุณและระบบเก็บข้อมูลคุณภาพชีวิตผู้สูงอายุของเทศบาลนครพิษณุโลกที่มีการประมวลผลข้อมูลสุขภาพและความพิการ ซึ่งถือเป็นข้อมูลอ่อนไหว¹⁷

3. การประมวลผลข้อมูลขนาดใหญ่ (Large Scale Processing) การประมวลผลในเมืองอัจฉริยะพิษณุโลกเป็นการประมวลผลข้อมูลส่วนบุคคลที่มีปริมาณมากโดยพิจารณาจากจำนวนประชากรซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้อง ขอบเขตกิจกรรมที่ต้องการการประมวลผล ขนาดของเมือง และระยะเวลาของการประมวลผล เป็นต้น

4. การรวมชุดข้อมูล (Combining Datasets) การประมวลผลข้อมูลส่วนบุคคลในเมืองอัจฉริยะพิษณุโลกอาจมีการรวมชุดข้อมูลที่ได้มาจากการดำเนินการ (Operations) ตั้งแต่ 2 ชุดขึ้นไป ซึ่งมีวัตถุประสงค์ในการประมวลผลที่แตกต่างกัน และ/หรือ มีผู้ควบคุมข้อมูลส่วนบุคคลต่างกัน ทำให้การประมวลผลนั้นเกินขอบเขตความคาดหวังอันสมเหตุสมผลของเจ้าของข้อมูล (the Reasonable Expectations of the Data Subject)

5. เจ้าของข้อมูลที่เปราะบาง (Vulnerable data subjects) เนื่องจากการประมวลผลข้อมูลในเมืองอัจฉริยะพิษณุโลกนั้นเป็นการประมวลผลกลุ่มประชากรจำนวนมาก จึงอาจรวมถึงกลุ่มผู้เปราะบาง และยังมีแอปพลิเคชัน หรือระบบที่ถูกออกแบบมา เพื่อช่วยเหลือกลุ่มผู้เปราะบางที่มีข้อจำกัดในการให้ความยินยอม คัดค้าน หรือการใช้สิทธิ เช่น เด็ก ผู้เยาว์ ผู้ป่วย ผู้พิการ หรือคนชรา

6. การใช้ในลักษณะนวัตกรรมและสร้างสรรค์ (Innovative Use) การนำเทคโนโลยีใหม่มาประยุกต์ใช้ถือว่ามีความเสี่ยงสูงเพราะอาจส่งผลกระทบต่อเจ้าของข้อมูลและต่อสังคมที่ไม่อาจคาดเดาได้ เช่น การใช้ IoT เพื่อเชื่อมโยงกับอุปกรณ์ต่างๆ หรือเทคโนโลยีอื่นๆ ในเมืองอัจฉริยะพิษณุโลก

¹⁷ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 26

จากที่กล่าวมาข้างต้น จึงสรุปได้ว่าการประมวลผลในเมืองอัจฉริยะพิษณุโลกนั้นถือเป็นการประมวลผลที่มีความเสี่ยงสูงที่จะกระทบสิทธิและเสรีภาพของบุคคล จึงมีความจำเป็นต้องจัดทำ DPIA

3.2 อธิบายกระบวนการประมวลผลข้อมูลส่วนบุคคล

ในการอธิบายการประมวลผลข้อมูลส่วนบุคคลนั้น ควรอธิบายลักษณะการเก็บรวบรวม และใช้ข้อมูลส่วนบุคคล รวมถึงผู้ที่มีอำนาจเข้าถึงข้อมูล การส่งต่อ หรือแบ่งปันข้อมูล ระยะเวลาในการจัดเก็บข้อมูล เทคโนโลยีที่เกี่ยวข้อง ตลอดจนขอบเขตการประมวลผลข้อมูลส่วนบุคคล เช่น แหล่งที่มาของข้อมูล ประเภทของข้อมูลส่วนบุคคล ปริมาณ ความถี่ในการประมวลผล ระยะเวลาในการประมวลผล จำนวนเจ้าของข้อมูลส่วนบุคคลและพื้นที่ที่เกี่ยวข้อง¹⁸ นอกจากนี้ ยังควรมีการระบุรายละเอียดอื่น ๆ เช่น ขอบเขตอำนาจของผู้ควบคุมข้อมูลส่วนบุคคลและวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล อย่างไรก็ตาม การอธิบายรายละเอียดการประมวลผลข้อมูลส่วนบุคคลในกรณีศึกษานี้อาจประสบปัญหา หรือความท้าทาย เนื่องจากการทำงานของระบบเมืองอัจฉริยะพิษณุโลกมีเขตพื้นที่ทับซ้อนของโครงการและมีหน่วยงานเข้ามาเกี่ยวข้องเป็นจำนวนมาก การไหลเวียนของข้อมูล จึงมีความซับซ้อนและยากที่จะระบุแหล่งที่มาของข้อมูล โดยเฉพาะในกรณีที่มีการใช้ระบบอัตโนมัติในการแลกเปลี่ยนข้อมูล ดังนั้น จึงควรจัดทำแผนผังการไหลเวียนของข้อมูล (Data Flow Diagram) อย่างละเอียด เพื่อช่วยให้เห็นภาพรวมของการประมวลผลของเมืองอัจฉริยะมากยิ่งขึ้นว่าข้อมูลส่วนบุคคลได้มาจากไหน ถูกส่งผ่านและเก็บไว้ที่ใด ใครเกี่ยวข้องบ้าง เป็นต้น

3.3 ระบุหน่วยงานหรือองค์กร บุคคล และผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง

หลังจากอธิบายกระบวนการในการประมวลผลข้อมูลส่วนบุคคลแล้ว ต้องมีการระบุหน่วยงาน หรือองค์กร บุคคลและผู้มีส่วนได้เสียที่เกี่ยวข้องกับการประมวลผลนั้นด้วย จากแผนการดำเนินการโครงการพัฒนาเมืองอัจฉริยะจังหวัดพิษณุโลกได้มีการทำศูนย์เก็บข้อมูล (Data Center) และได้กำหนดบทบาทและหน้าที่ของผู้ที่เกี่ยวข้องในการดูแลและบริหารจัดการข้อมูล ได้แก่ นักวิเคราะห์ข้อมูล เจ้าหน้าที่ฝ่ายพัฒนาเทคโนโลยีสารสนเทศ เจ้าของข้อมูล ผู้ใช้งานข้อมูล ผู้มีอำนาจการอนุมัติในการให้ข้อมูล และผู้ดูแลระบบ¹⁹ และโครงการพิษณุโลก

¹⁸ Article 29 Data Protection Working Party (WP29), "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (wp248rev.01)," 16-18.

¹⁹ "บทสรุปผู้บริหาร: เมืองอัจฉริยะจังหวัดพิษณุโลก."



นครอัจฉริยะอย่างยั่งยืนได้มีการกำหนดระบบข้อมูลเมืองและธรรมาภิบาลข้อมูล (Data Governance)²⁰ อย่างไรก็ดี เนื่องจากการไหลของข้อมูลส่วนบุคคล (Data Flow) ในเมืองอัจฉริยะนั้น มีความซับซ้อน กระจัดกระจาย และมีทั้งภาครัฐและเอกชนเข้ามาเกี่ยวข้อง จึงก่อให้เกิดปัญหาในการกำหนดสถานะและหน้าที่ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ซึ่งแบ่งเป็น 2 ประเภท ได้แก่ (1) ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และ (2) ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ซึ่งจะดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่ง หรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล²¹

จากการศึกษา ยังพบความซ้ำซ้อนในอำนาจและหน้าที่ระหว่างองค์กรปกครองส่วนท้องถิ่นและการทับซ้อนในเขตพื้นที่โครงการเมืองอัจฉริยะ เนื่องจาก องค์การบริหารส่วนจังหวัดมีอำนาจบริหารในเขตจังหวัด ตามมาตรา 8 แห่งพระราชบัญญัติองค์การบริหารส่วนจังหวัด พ.ศ. 2540 จึงทับซ้อนกับเขตพื้นที่ของเทศบาลนครพิษณุโลก อำเภอ นครไทย และเขตพื้นที่ขององค์การบริหารส่วนตำบลท่าโพธิ์ ซึ่งเป็นที่ตั้งของมหาวิทยาลัยนเรศวร แม้ว่าจะมีการแบ่งเขตการบริหารโครงการเมืองอัจฉริยะพิษณุโลก โดยกำหนดให้ โครงการเมืองอัจฉริยะจังหวัดพิษณุโลก อยู่ในเขตพื้นที่อำเภอเมืองพิษณุโลกและอำเภอ นครไทย ภายใต้ความรับผิดชอบขององค์การบริหารส่วนจังหวัด ส่วนโครงการพิษณุโลกนครอัจฉริยะอย่างยั่งยืน นั้น อยู่ในเขตพื้นที่เทศบาลนครพิษณุโลกภายใต้ความรับผิดชอบของเทศบาลนครพิษณุโลก และโครงการ NU Smart City อยู่ในเขตพื้นที่มหาวิทยาลัยนเรศวรภายใต้ความรับผิดชอบของมหาวิทยาลัย แต่โครงการอัจฉริยะบางโครงการอาจมีพื้นที่ทับซ้อนกัน หรือมีการหมุนเวียนข้อมูลระหว่างกัน เช่น โครงการขนส่งอัจฉริยะและการติดตั้งระบบรักษาความปลอดภัย CCTV ซึ่งมีความต่อเนื่องทั่วทั้งจังหวัด จึงยากที่จะระบุผู้รับผิดชอบในเขตพื้นที่ทับซ้อน นอกจากนี้ การเปลี่ยนแปลงผู้บริหารองค์กรปกครองส่วนท้องถิ่น หรือผู้บริหารมหาวิทยาลัยตามวาระยังอาจก่อให้เกิดการเปลี่ยนแปลงด้านนโยบายและขาดความต่อเนื่องในการดำเนินการโครงการต่าง ๆ ดังนั้น เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลในเมืองอัจฉริยะมีความชัดเจนและต่อเนื่อง จึงควรกำหนดบทบาทและหน้าที่ขององค์กรปกครองส่วนท้องถิ่นและหน่วยงานต่าง ๆ ในจังหวัดพิษณุโลกตลอดจนระยะเวลาในการดำเนินการโครงการต่าง ๆ ให้ชัดเจน

ทั้งนี้ ผู้วิจัยเห็นว่าองค์การบริหารส่วนจังหวัด ควรเป็นผู้รับผิดชอบหลักของโครงการเมืองอัจฉริยะของจังหวัดพิษณุโลกและมีหน้าที่ดำเนินการจัดทำแผนและประสานการจัดทำแผนการพัฒนาโครงการเมืองอัจฉริยะในเขตพื้นที่ขององค์กรปกครองส่วนท้องถิ่นอื่น ๆ

²⁰ “บทสรุปผู้บริหาร: พิษณุโลกนครอัจฉริยะอย่างยั่งยืน.”

²¹ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 6.

และเป็นเครือข่ายหลักในการเชื่อมโยงแผนงานโครงการที่ดำเนินโดยองค์กรปกครองส่วนท้องถิ่นอื่น²² เนื่องจาก ลักษณะของโครงการเมืองอัจฉริยะพิษณุโลกตรงกับกรอบอำนาจหน้าที่ขององค์กรบริหารส่วนจังหวัด ตามประกาศคณะกรรมการกระจายอำนาจให้แก่องค์กรปกครองส่วนท้องถิ่น เรื่อง กำหนดอำนาจและหน้าที่ในการจัดระบบบริการสาธารณะขององค์กรบริหารส่วนจังหวัด ซึ่งได้กำหนดลักษณะการดำเนินงานขององค์กรบริหารส่วนจังหวัดในการให้บริการสาธารณะ โดยให้องค์การบริหารส่วนจังหวัดดำเนินงานที่ปรากฏถึงกิจกรรมที่เป็นภาพรวม หรือเข้าไปดำเนินงานโครงการในลักษณะที่มีความคาบเกี่ยวต่อเนื่อง หรือมีผู้ที่ได้รับประโยชน์ในองค์กรปกครองส่วนท้องถิ่นมากกว่า 1 แห่งขึ้นไป²³ นอกจากนี้ ผู้วิจัย เห็นควรกำหนดให้องค์การบริหารส่วนจังหวัดเป็นผู้ควบคุมข้อมูล (Data Controller) ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ โดยกำหนดให้เทศบาลนครพิษณุโลกและมหาวิทยาลัยนเรศวร ตลอดจนภาคเอกชนต่างๆ ที่เกี่ยวข้องเป็นผู้ควบคุมข้อมูลส่วนบุคคลร่วม (Joint Controller) สำหรับกิจกรรมที่ทำร่วมกัน หรือในการให้บริการในพื้นที่ทับซ้อน และควรดำเนินการจัดทำบันทึกข้อตกลงการเป็นผู้ควบคุมข้อมูลส่วนบุคคลร่วม (Joint Controller Agreement) เพื่อกำหนดขอบเขตอำนาจหน้าที่และความรับผิดชอบต่อเจ้าของข้อมูลส่วนบุคคลและความรับผิดชอบระหว่างกันให้ชัดเจน และเพื่อให้การดำเนินการต่างๆ เป็นไป ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ เช่น การกำหนดวัตถุประสงค์และขอบเขตของการประมวลผลข้อมูลส่วนบุคคล และหน้าที่ในการแจ้งวัตถุประสงค์ดังกล่าวแก่เจ้าของข้อมูลส่วนบุคคล

นอกจากนี้ ผู้ควบคุมข้อมูลส่วนบุคคลยังต้องดำเนินการสำรวจความเห็นของเจ้าของข้อมูลส่วนบุคคล ซึ่งถือเป็นผู้มีส่วนได้ส่วนเสียในโครงการเมืองอัจฉริยะด้วย โดยการขอความยินยอมในการเก็บรวบรวมข้อมูลไม่ถือเป็นการสำรวจความเห็น ทั้งนี้ ผู้วิจัยได้สำรวจความคิดเห็นของกลุ่มประชากรตัวอย่างในเมืองอัจฉริยะพิษณุโลกซึ่งถือเป็นเจ้าของข้อมูลส่วนบุคคลเบื้องต้นด้วยแบบสัมภาษณ์กึ่งโครงสร้าง จากการสำรวจพบว่ากลุ่มตัวอย่างมีความกังวลว่าข้อมูลส่วนบุคคลของตนจะถูกละเมิด หรือได้รับผลกระทบจากการให้บริการสาธารณะในเมืองอัจฉริยะ และความกังวลดังกล่าวส่งผลต่อการตัดสินใจใช้บริการ โดยผู้ให้ข้อมูล 3 คน กล่าวว่า หากเสี่ยงได้จะไม่ใช้บริการสาธารณะในเมืองอัจฉริยะ หรือใช้เฉพาะที่จำเป็น ดังนั้น เพื่อสร้างความมั่นใจให้แก่เจ้าของข้อมูลส่วนบุคคล จึงควรดำเนินการประเมินความจำเป็นและความได้สัดส่วน ระบุความเสี่ยงและจัดการความเสี่ยงตามขั้นตอนต่อไป

²² ประกาศคณะกรรมการกระจายอำนาจให้แก่องค์กรปกครองส่วนท้องถิ่น เรื่อง กำหนดอำนาจและหน้าที่ในการจัดระบบบริการสาธารณะขององค์กรบริหารส่วนจังหวัด ประกาศ ณ วันที่ 19 สิงหาคม 2546, ข้อ 2

²³ ประกาศคณะกรรมการกระจายอำนาจให้แก่องค์กรปกครองส่วนท้องถิ่น เรื่อง กำหนดอำนาจและหน้าที่ในการจัดระบบบริการสาธารณะขององค์กรบริหารส่วนจังหวัด ประกาศ ณ วันที่ 19 สิงหาคม 2546, ข้อ 1



3.4 ประเมินความจำเป็นและความสำเร็จส่วนในการประมวลผลข้อมูลส่วนบุคคล

เนื่องจากการประมวลผลข้อมูลส่วนบุคคลเป็นปัจจัยหลักที่จะทำให้ระบบของเมืองอัจฉริยะมีประสิทธิภาพแต่การคุ้มครองข้อมูลส่วนบุคคลมีความสำคัญเป็นอย่างยิ่ง ดังนั้นในการพัฒนาเมืองอัจฉริยะผู้ควบคุมข้อมูลส่วนบุคคล จึงต้องประเมินความจำเป็นและได้สัดส่วน

โดยหลักความจำเป็นและได้สัดส่วนนั้น แฝงอยู่ในหลายมาตราของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ อาทิ มาตรา 22 ที่ได้กำหนดหลักเกณฑ์การเก็บรวบรวมข้อมูลส่วนบุคคลโดยให้เก็บรวบรวมได้เท่าที่จำเป็นภายในวัตถุประสงค์อันชอบด้วยกฎหมาย (Data Minimization) และมาตรา 37(3) ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ดำเนินการลบ หรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการรักษา หรือไม่เกี่ยวข้อง หรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ ดังนี้ หากกิจกรรมสามารถบรรลุวัตถุประสงค์ได้โดยไม่จำเป็นต้องเก็บข้อมูลที่ระบุตัวบุคคล การวิเคราะห์ข้อมูลควรใช้วิธีการทางเทคนิคทำให้เป็นข้อมูลนิรนาม (Anonymous Data) หรือข้อมูลแฝง (Pseudonymous Data) ซึ่งไม่สามารถระบุตัวบุคคล เช่น ในกรณีที่ต้องการวิเคราะห์ปัญหาการจราจร หรือความหนาแน่นของประชากรในบางพื้นที่ในเมืองอัจฉริยะ อาจใช้วิธีการขอให้หน่วยงานเครือข่ายแบ่งปันข้อมูลนิรนามและรวบรวมข้อมูลดังกล่าว เพื่อมาวิเคราะห์ด้วยเทคนิคเดียวกับที่รัฐบาลอิตาลีและเยอรมันใช้ในการติดตามความเคลื่อนไหวของประชาชนของในช่วงที่เชื้อไวรัสโคโรนาระบาด²⁴ หรือการเก็บข้อมูลมั่วเพื่อประโยชน์ทางด้านสถิติ หรือการวิจัย เช่น การเก็บสถิติการเกิดอุบัติเหตุ หรือการตรวจวัดคุณภาพอากาศ อาจทำได้โดยใช้เทคนิคการทำให้เป็นข้อมูลนิรนาม หรือข้อมูลแฝงเช่นเดียวกัน

นอกจากนี้ หลักความจำเป็นและได้สัดส่วนยังเชื่อมโยงกับฐานในการประมวลผลอันชอบด้วยกฎหมาย (Lawfulness of Processing) ซึ่งหน่วยงานต่าง ๆ มักพิจารณาฐานความยินยอมเป็นลำดับแรก แต่ฐานความยินยอมนี้ จะถูกจำกัดด้วยหลักจำกัดวัตถุประสงค์ (Purpose Limitation) ตามมาตรา 19 และมาตรา 23 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ กล่าวคือ การประมวลผลข้อมูลส่วนบุคคลจะทำได้เฉพาะวัตถุประสงค์ที่เจาะจงซึ่งได้รับความยินยอมโดยชัดแจ้งและชอบด้วยกฎหมาย โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องได้

²⁴ Rama Krishna Reddy Kummitha, "Smart Technologies for Fighting Pandemics: The Techno- and Human- Driven Approaches in Controlling the Virus Transmission," *Government Information Quarterly* 37, no. 3 (2020/07/01/ 2020), <https://dx.doi.org/https://doi.org/10.1016/j.giq.2020.101481>.

รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อน หรือในขณะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล และมาตรา 21 กำหนดว่าจะทำเพิ่มเติม หรือแตกต่างจากวัตถุประสงค์ที่ได้แจ้งไว้ไม่ได้ เช่น ถ้าผู้ควบคุมข้อมูลส่วนบุคคลได้รับความยินยอมให้เก็บรวบรวมข้อมูลส่วนบุคคลจากผู้ใช้บริการระบบขนส่งสาธารณะ เพื่อวัตถุประสงค์ในการอำนวยความสะดวกในการเดินทางในเมืองอัจฉริยะ ผู้ควบคุมข้อมูลจะไม่สามารถใช้ข้อมูล เพื่อวัตถุประสงค์อื่น เช่น วัตถุประสงค์ด้านสุขภาพ หรือวัตถุประสงค์เพื่อป้องกันอาชญากรรมหรือติดตามอาชญากร ทั้งนี้ ในการแจ้งวัตถุประสงค์ที่เจาะจงนั้นการใช้ประโยชน์ที่คลุมเครือถูกมองว่าไม่เพียงพอและไม่ถือเป็นการแจ้งวัตถุประสงค์ที่เจาะจงโดยชัดเจนตามมาตรา 19 เช่น การแจ้งว่ามี การเก็บรวบรวมข้อมูลส่วนบุคคล เพื่อพัฒนาประสบการณ์ของผู้ใช้งาน เพื่อประโยชน์ในการวิจัยหรือการตลาด หรือเพื่อความปลอดภัยทางไซเบอร์²⁵ อย่างไรก็ตาม การปฏิบัติตามหลักจำกัดวัตถุประสงค์ในบริบทเมืองอัจฉริยะอาจประสบปัญหา หรือความท้าทาย ด้วยลักษณะการทำงานของเมืองอัจฉริยะที่มีการประมวลผลข้อมูลของกิจกรรมที่หลากหลายและมีหลายหน่วยงานมาเกี่ยวข้อง และการดำเนินงานเมืองอัจฉริยะจะมีประสิทธิภาพได้ต้องมีการแบ่งปันข้อมูล ข้อมูลส่วนบุคคลจึงอาจถูกใช้งานด้วยวัตถุประสงค์ที่แตกต่างจากวัตถุประสงค์ที่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลในตอนแรก และ/หรือ อาจถูกประมวลผลโดยหน่วยงานที่ไม่ได้รับความยินยอมจากเจ้าของข้อมูลโดยตรง อีกทั้งรูปแบบการทำงานของ IoT ยังมีการแลกเปลี่ยนข้อมูลส่วนบุคคลโดยอัตโนมัติระหว่างเครื่องมือต่าง ๆ และข้อมูลส่วนบุคคลยังอาจถูกรวบรวมและเก็บโดยอัตโนมัติสู่ฐานข้อมูลมหัต ซึ่งหน่วยงานต่าง ๆ สามารถเข้าถึงข้อมูลได้²⁶ จึงยากที่จะหาแหล่งที่มาของข้อมูลส่วนบุคคล ทำให้ไม่สามารถแจ้งวัตถุประสงค์ใหม่ในการประมวลผลให้เจ้าของข้อมูลทราบ เพื่อขอความยินยอมเพิ่มเติมตามมาตรา 21 นอกจากนั้น เนื่องจากกิจกรรมส่วนมากในเมืองอัจฉริยะจะเกิดขึ้นในพื้นที่สาธารณะและมีผู้ใช้บริการเป็นจำนวนมาก จึงยากที่จะขอความยินยอมผู้ใช้บริการทุกคนเพื่อเก็บ รวบรวม ใช้ ข้อมูลส่วนบุคคล เช่น การติดตั้ง CCTV ในพื้นที่สาธารณะ ฉะนั้น ในทางปฏิบัติการประมวลผลข้อมูลโดยอาศัยฐานความยินยอมอย่างเดียวจึงอาจไม่เพียงพอต่อการทำงานของเมืองอัจฉริยะ

²⁵ Kamrul Faisal, "Applying the Purpose Limitation Principle in Smart-City Data-Processing Practices: A European Data Protection Law Perspective," *Communication Law and Policy* 28, no. 1 (2023): 67-97

²⁶ อัญริกา ณ พิบูลย์, "ความท้าทายทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลในบริบทของเมืองอัจฉริยะ (Smart City) Legal Challenges of the Protection of Personal Data in the Context of Smart City," *วารสารบัณฑิตศึกษานิติศาสตร์* 13, ฉบับที่ 2 (2563): 271-294.



หน่วยงานต่าง ๆ ในเมืองอัจฉริยะทั้งภาครัฐและเอกชนจึงอาจพิจารณาฐานทางกฎหมายอื่น ๆ ตามมาตรา 24, 26 และ 27 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ในการประมวลผลข้อมูลส่วนบุคคล โดยในการพิจารณาเลือกใช้ฐานตามกฎหมายแต่ละฐานนั้นขั้นแรกต้องพิจารณาประเภทของข้อมูลโดยแบ่งเป็นข้อมูลส่วนบุคคลปกติและข้อมูลส่วนบุคคลอ่อนไหว หากเป็นข้อมูลส่วนบุคคลปกติให้พิจารณาตาม มาตรา 24 และ 27 เช่น มาตรา 24(1) ฐานวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยหรือสถิติ มาตรา 24 (2) ฐานป้องกันหรือระงับอันตรายต่อชีวิต ร่างกายหรือสุขภาพ และมาตรา 24(4) ฐานการจำเป็น เพื่อการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ ซึ่งหน่วยงานของรัฐรวมถึงเอกชนที่ปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่มีอำนาจตามกฎหมายอย่างเจาะจง อาจอาศัยฐานดังกล่าวในการประมวลผลข้อมูลส่วนบุคคลในเมืองอัจฉริยะ แต่หากงานตามหน้าที่ดังกล่าวสามารถดำเนินการได้โดยไม่จำเป็นต้องประมวลผลข้อมูลส่วนบุคคล หรือสามารถดำเนินการได้ด้วยวิธีการอื่น ย่อมไม่สามารถอาศัยฐานนี้ได้ และต้องประเมินว่าการประมวลผลข้อมูลที่กระทบต่อสิทธิของเจ้าของข้อมูลส่วนบุคคลนั้นได้สัดส่วนกับประโยชน์สาธารณะที่จะได้รับ หรือไม่ และในการประมวลผลข้อมูลอ่อนไหว เช่น ข้อมูลสุขภาพ ข้อมูลชีวภาพและประวัติอาชญากรรม ให้พิจารณาฐานทางกฎหมายที่กำหนดเฉพาะใน มาตรา 26 แห่งพระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคลฯ อาทิ ฐานความจำเป็นในการปฏิบัติตามกฎหมายเพื่อประโยชน์สาธารณะที่สำคัญตามมาตรา 26 (5)(จ) ซึ่งจำเป็นต้องชั่งน้ำหนักความได้สัดส่วนระหว่างการคุ้มครองข้อมูลส่วนบุคคลและการบรรลุวัตถุประสงค์ เพื่อประโยชน์สาธารณะ เช่น การเก็บรวบรวม ใช้ข้อมูลชีวภาพในกรณีเมืองอัจฉริยะที่ได้มีการนำระบบจดจำใบหน้ามาใช้ต้องประมวลผลเฉพาะกรณีที่น่าจำเป็นและได้สัดส่วนกับประโยชน์สาธารณะเท่านั้น

อนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลทั้งภาครัฐและเอกชนอาจใช้ฐานการจำเป็น เพื่อประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล (Legitimate Interest) ตามมาตรา 24(5) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ แทนฐานความยินยอมสำหรับกิจกรรมการประมวลผลหลายกิจกรรมเพราะเป็นฐานที่กว้าง อย่างไรก็ตาม มาตรา 24(5) ได้กำหนดว่าผู้ควบคุมข้อมูลส่วนบุคคลจะทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลได้ หากประเมินแล้วความจำเป็น เพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคลมีความสำคัญมากกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล ดังนั้นจึงต้องมีการประเมิน หรือชั่งน้ำหนักระหว่างความจำเป็น เพื่อประโยชน์โดยชอบด้วยกฎหมายและสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลก่อน โดยในการประเมิน หรือชั่งน้ำหนักนั้นอาจใช้การประเมินความจำเป็นและความสมเหตุสมผล (Legitimate Interests Assessment: LIA

ซึ่งต่อไปนี้จะเรียกว่า LIA) 3 ขั้นตอนตามแนวทางของสหราชอาณาจักร²⁷ ดังนี้ ขั้นตอนที่ 1 ให้พิจารณาวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล (Purpose Test) โดยให้พิจารณาว่าเป็นประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลหรือไม่ ขั้นตอนที่ 2 ให้ทดสอบความจำเป็น (Necessity Test) โดยให้พิจารณาว่าการประมวลผลข้อมูลส่วนบุคคลนั้น มีความจำเป็นในบรรลุวัตถุประสงค์ตามขั้นตอนที่ 1 หรือไม่ และได้สัดส่วนหรือไม่ ในกรณีนี้ผู้ควบคุมข้อมูลส่วนบุคคลอาจชี้แจงได้ว่าการประมวลผล CCTV ที่ติดตั้งเป็นไป เพื่อความปลอดภัย (Purpose Test) โดยจะเก็บรวบรวม ใช้ ข้อมูลเฉพาะที่จำเป็น และมีระยะเวลาในการเก็บที่จำกัด (Necessity Test) อย่างไรก็ตาม ต้องไม่อ้างฐานประโยชน์โดยชอบด้วยกฎหมายที่กว้างเกินไป เช่น กรณีการติดตั้ง CCTV เพื่อรักษาความปลอดภัย (Security Safety) อาจมีวัตถุประสงค์รวมถึงประเด็นอาชญากรรมได้ แต่ไม่สามารถกว้างไปจนรวมถึงความสะอาด หรือสุขอนามัย (Sanitary)²⁸ และขั้นตอนที่ 3 ให้ทดสอบความสมดุลระหว่างประโยชน์ของผู้ควบคุมข้อมูลและสิทธิขั้นพื้นฐานของเจ้าของข้อมูล ซึ่งตามมาตรา 24(5) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ของไทยหมายถึงเฉพาะสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลเท่านั้น จึงไม่นำสิทธิขั้นพื้นฐานอื่นๆ ตามรัฐธรรมนูญมาพิจารณา

ในการทดสอบความสมดุล (Balancing test) (ซึ่งต่อไปนี้จะเรียกว่า Balancing Test) ให้พิจารณาความคาดหวังที่สมเหตุสมผลของเจ้าของข้อมูลส่วนบุคคล (the Reasonable Expectations of the Data Subject) และซึ่งน้ำหนักการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลกับสิทธิหรือเสรีภาพของผู้ควบคุมข้อมูลส่วนบุคคล หรือของบุคคลอื่น ตลอดจนประโยชน์สาธารณะ โดยในการชั่งน้ำหนักนั้นสิทธิของเจ้าของข้อมูลส่วนบุคคลจะมีน้ำหนักมากกว่าประโยชน์อันชอบธรรมของผู้ควบคุมข้อมูลส่วนบุคคล หากการประมวลผลข้อมูลส่วนบุคคลนั้นเกินความคาดหวังที่สมเหตุสมผล โดยผู้วิจัย มองว่าการนำข้อมูลที่ได้จาก CCTV ในพื้นที่สาธารณะไปใช้นอกวัตถุประสงค์การรักษาความปลอดภัยอาจเกินความคาดหวังที่สมเหตุสมผลของเจ้าของข้อมูล เช่น การนำไปวิเคราะห์พฤติกรรมอื่นๆ ของบุคคล และการแบ่งปันข้อมูลระหว่างหน่วยงานต่างๆ ก็อาจเกินความคาดหวังอันสมเหตุสมผลของเจ้าของข้อมูล

²⁷ Information Commissioner's Office (ICO), "Legitimate Interests," accessed December 25, 2024, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/legitimate-interests/>.

²⁸ Office of Data Protection Commissioner, "Ireland, Twentieth Annual Report of the Data Protection Commissioner 2008," accessed January 24, 2025, <https://www.dataprotection.ie/sites/default/files/uploads/2018-12/AR2008.pdf>.



นอกจากนั้น ในกรณีการติดตั้ง CCTV ในพื้นที่สาธารณะยังเกิดคำถามว่าเจ้าของข้อมูลส่วนบุคคลสามารถคาดหวังความเป็นส่วนตัว หรือการคุ้มครองข้อมูลส่วนบุคคลของตนในพื้นที่สาธารณะได้ หรือไม่ เพียงใด เพื่อตอบคำถามดังกล่าวอาจพิจารณาแนวทางที่ศาลอังกฤษ หรือศาลแห่งสหราชอาณาจักรได้เคยวางไว้ในคดีละเมิดข้อมูลส่วนบุคคล (Tort of Misuse of Private Information) โดยในหลายคดีศาลมองว่า ความคาดหวังที่สมเหตุสมผลในความเป็นส่วนตัวของบุคคลในพื้นที่สาธารณะจะน้อยกว่าในพื้นที่ส่วนตัว²⁹ อย่างไรก็ตาม จากคดี *Campbell v Mirror Group Newspapers Ltd*³⁰ และ *Murray v Express Newspapers Plc*³¹ สามารถสรุปได้ว่านอกจากสถานที่แล้วความคาดหวังที่สมเหตุสมผลของเจ้าของข้อมูลยังขึ้นอยู่กับปัจจัยอื่นๆ เช่น ลักษณะของกิจกรรมในพื้นที่สาธารณะ ลักษณะ หรือประเภทของข้อมูลส่วนบุคคลและผลกระทบที่อาจเกิดขึ้นกับเจ้าของข้อมูล ในคดี *Campbell* แม้ข้อมูลที่ปรากฏจะเป็นรูปภาพขณะที่แคมป์เบลล์ (Campbell) กำลังเดินบนถนนสาธารณะ แต่ศาลมองว่าเธอสามารถคาดหวังความเป็นส่วนตัวได้เพราะเป็นภาพขณะที่เธอกำลังเดินออกมาจากสมาคมผู้ติดยาเสพติดนิรนาม และในคดี *Murray* การคุ้มครองข้อมูลส่วนบุคคล หรือสิทธิของเด็กได้เพิ่มน้ำหนักให้แก่ความคาดหวังความเป็นส่วนตัว แม้ภาพที่ปรากฏจะเกิดขึ้นบนถนนสาธารณะ จากคดีดังกล่าวจะเห็นว่าบุคคลยังสามารถคาดหวังความเป็นส่วนตัว หรือการคุ้มครองข้อมูลส่วนบุคคลของตนในพื้นที่สาธารณะได้ในบางกรณี

กล่าวโดยสรุป การประเมินความจำเป็นและได้สัดส่วนต้องพิจารณาเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามความจำเป็นและได้สัดส่วน โดยคำนึงถึงหลักการจำกัดวัตถุประสงค์และฐานการประมวลผลอันชอบด้วยกฎหมาย

3.5 การระบุและประเมินความเสี่ยง

ก่อนเริ่มโครงการเมืองอัจฉริยะผู้ควบคุมข้อมูลส่วนบุคคลต้องระบุความเสี่ยงที่อาจเกิดขึ้นจากการทำงานของระบบเมืองอัจฉริยะทั้งด้านร่างกาย จิตใจ และทรัพย์สิน และประเมินว่าความเสี่ยงนั้น มีโอกาสจะเกิดขึ้นและมีความร้ายแรงมากน้อยเพียงใด โดยในการประเมินความเสี่ยงนั้น ควรประเมินจากมุมมองของเจ้าของข้อมูลส่วนบุคคลด้วย เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลบรรลุวัตถุประสงค์มากที่สุด³² ดังนั้น การระบุและประเมินความเสี่ยง

²⁹ Methinee Suwannakit, "The Protection of Privacy and Private Information in the Digital Age: A Comparative Study of English and Thai law Applying to Individual Media Users," (PhD thesis, University of Glasgow, UK, 2023), 103-104.

³⁰ *Campbell v Mirror Group Newspapers Ltd* [2004] UKHL 22

³¹ *Murray v Express Newspapers Plc* [2008] EWCA Civ 446

³² Michael Friedewald, Ina Schiering, Nicholas Martin and Dara Hallinan, "Data Protection Impact Assessments in Practice Experiences from Case Studies" in Computer Security ESORICS 2021 International Workshops Revised Selected Papers, Germany, October 4-8 2021

ในบทความวิจัยฉบับนี้ จึงใช้วิธีผสมผสานระหว่างการทบทวนวรรณกรรม การวิเคราะห์เอกสาร ประกอบกับมุมมองของกลุ่มตัวอย่างในเมืองอัจฉริยะพิษณุโลกที่ถอดมาจากการสัมภาษณ์ กึ่งโครงสร้างด้วยวิธีวิเคราะห์เนื้อหา (Content Analysis) ซึ่งสามารถระบุความเสี่ยงได้ดังต่อไปนี้

1. ข้อมูลรั่วไหล จากการสัมภาษณ์แบบกึ่งโครงสร้างผู้ให้ข้อมูลส่วนมากจะใช้วลีที่ คล้ายคลึงกันว่ามีความกังวลว่า ข้อมูลของตนจะรั่วไหล ข้อมูลหลุด ข้อมูลรั่ว หรือ ข้อมูลถูกเปิดเผย เป็นต้น ดังนั้น ผู้วิจัย จึงได้กำหนดให้วลี ข้อมูลรั่วไหล เป็นรหัส ซึ่งหมายถึงการที่ข้อมูลส่วนบุคคลหลุดออกไปนอกองค์กร หรือหลุดไปสู่ผู้อื่นโดยไม่ได้รับอนุญาต และกำหนดให้ข้อมูลรั่วไหล เป็นความเสี่ยง เมื่อถอดรหัสต่อมาจะเห็นว่าการที่ผู้ให้ข้อมูลมีความกังวลว่าข้อมูลของตนจะรั่วไหลนั้น เป็นเพราะผู้ให้ข้อมูลต่างกังวลต่อผลกระทบที่จะตามมา เช่น ถูกมิฉฉาชีพ หรือบุคคลอื่นนำข้อมูลไปใช้ในทางที่ไม่ถูกต้อง ทำให้ตนถูกหลอกลวง เกิดความเสียหายทางการเงินและทรัพย์สิน ซึ่งผลกระทบทั้งหลายนี้สอดคล้องกับความเสี่ยงที่ถูกระบุในงานวิจัยหลายฉบับ นอกจากนี้ กลุ่มตัวอย่างบางส่วนยังกังวลว่าข้อมูลส่วนบุคคลของตนจะถูกเปิดเผย ซึ่งผู้วิจัยมองว่าเป็นความเสี่ยงประเภทเดียวกันกับข้อมูลรั่วไหล ทั้งนี้ การเปิดเผยข้อมูลส่วนบุคคลสู่สาธารณะนั้น นอกจากจะมีความเสี่ยงว่าจะเกิดความเสียหายทางการเงิน ยังอาจเกิดความเสียหายแก่จิตใจ หรือแก่ชื่อเสียงได้ เช่น การเปิดเผยภาพของบุคคลขณะทำกิจกรรมที่น่าอับอายสู่สาธารณะ

อนึ่ง จากการทบทวนวรรณกรรมและวิเคราะห์เอกสารพบว่า การดำเนินการต่าง ๆ ของระบบเมืองอัจฉริยะรวมถึงเมืองอัจฉริยะพิษณุโลก ต้องมีการแลกเปลี่ยนข้อมูลระหว่าง อุปกรณ์หรือหน่วยงาน โดยมี IoT คอยเชื่อมระหว่างเซนเซอร์และอุปกรณ์ต่าง ๆ แต่ระดับการรักษาความปลอดภัยของระบบ IoT ยังอยู่ในระดับค่อนข้างต่ำ³³ และการเชื่อมต่อผ่าน API ดังที่ระบุในแผนพัฒนาเมืองอัจฉริยะพิษณุโลกก็ยังมีขีดจำกัดในการรักษาความปลอดภัย เพราะ API เป็นระบบที่เน้นให้มีการแบ่งปันข้อมูลระหว่างกันอย่างมีประสิทธิภาพ แต่ระบบการรักษาความปลอดภัยของข้อมูลส่วนบุคคลอาจไม่มีประสิทธิภาพมากนัก³⁴ นอกจากนี้ ระบบของเมืองอัจฉริยะจะมีการนำข้อมูลไปเก็บไว้บนระบบประมวลผลแบบกลุ่มเมฆหรือคลาวด์ (Cloud) (ซึ่งต่อไปนี้จะเรียกว่า Cloud) ที่เข้าถึงผ่านอินเทอร์เน็ต จึงมีความเสี่ยงที่ข้อมูลจะเกิดการรั่วไหล ถูกโจรกรรมข้อมูลส่วนบุคคล หรือข้อมูลเอกลักษณ์ (Identity Theft) ได้ง่าย เช่น การที่แฮกเกอร์

³³ Lilian Edwards, "Privacy, Security and Data Protection in Smart Cities: A Critical EU LAW Perspective," *European Data Protection Law Review*, 2, no. 1 (2016): 10-11, Elvira Ismagilova et al., "Security, Privacy and Risks within Smart Cities: Literature Review and Development of a Smart City Interaction Framework," *Information Systems Frontiers* 24, no. 2 (2022), 1-22.

³⁴ อัญธิกา ณ พิบูลย์, "ความท้าทายทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลในบริบทของเมืองอัจฉริยะ (Smart City) Legal Challenges of the Protection of Personal Data in the Context of Smart City," 283.



ใช้มัลแวร์ดักจับข้อมูลส่วนบุคคลของหน่วยงานต่าง ๆ ที่เก็บไว้บน Cloud หรือดักจับข้อมูลระหว่างการแลกเปลี่ยนของอุปกรณ์ต่าง ๆ ผ่าน IoT หรือ APIs หรือการรั่วไหลของข้อมูล อาจเกิดจากภัยคุกคาม หรือความผิดพลาดของระบบหรือเทคโนโลยีนั่นเอง

จากที่กล่าวมาข้างต้น สามารถจำแนกความเสี่ยงเรื่องข้อมูลรั่วไหลออกเป็น 2 มิติ ได้แก่ (1) ความเสี่ยงจากภายใน เป็นความเสี่ยงที่เกิดจากตัวผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล หรือบุคลากรภายในหน่วยงาน หรือองค์กรต่าง ๆ เอง ซึ่งอาจเป็นการกระทำโดยไม่มีเจตนา แต่เป็นเพราะไม่มีความรู้ หรือความเชี่ยวชาญ หรืออาจเป็นการกระทำโดยประมาทเลินเล่อ หรือขาดการวางแผน จึงนำข้อมูลไปใช้ผิดจากวัตถุประสงค์ที่ได้รับความยินยอม ส่งต่อ หรือแบ่งปันให้บุคคลภายนอกโดยไม่ได้รับอนุญาต เข้าถึง หรือเผยแพร่ข้อมูลส่วนบุคคลโดยปราศจากอำนาจ หรือโดยมิชอบ นอกจากนี้ การรั่วไหลของข้อมูลอาจเกิดจากการใช้ หรือเปิดเผยโดยเจตนาของหน่วยงานหรือองค์กร โดยอาศัยฐานทางกฎหมายที่กว้างเกินไปหรือเกินความจำเป็น และ (2) ความเสี่ยงจากภายนอก เป็นความเสี่ยงที่เกิดจากบุคคลภายนอกหรือความเสี่ยงทางเทคนิค เช่น ภัยคุกคามจากอาชญากรรม หรือโจรกรรมข้อมูล หรือภัยคุกคามที่เกิดจากเทคนิค หรือระบบที่ผิดพลาดทำให้ข้อมูลรั่วไหล

โดยผู้วิจัยประเมินว่า ความเสี่ยงเรื่องข้อมูลรั่วไหลนี้ มีโอกาสที่จะเกิดขึ้นในระดับสูง มีความร้ายแรงสูงและถือเป็นความเสี่ยงที่มีความสำคัญมากที่สุด โดยการที่ข้อมูลรั่วไหลนั้น อาจส่งผลกระทบต่อทั้งจิตใจและทรัพย์สินของเจ้าของข้อมูล นอกจากนี้ ในระบบเมืองอัจฉริยะพิษณุโลกยังมีการเก็บรวบรวมใช้ข้อมูลส่วนบุคคลอ่อนไหว เช่น ข้อมูลสุขภาพ ข้อมูลชีวภาพ เป็นจำนวนมาก ตลอดจนมีการบันทึกข้อมูลแหล่งที่อยู่ (Location Data) ซึ่งหากข้อมูลประเภทนี้รั่วไหลจะยิ่งมีความร้ายแรงสูง³⁵

2. เจ้าของข้อมูลส่วนบุคคลไม่สามารถควบคุมการใช้งานข้อมูลส่วนบุคคลของตนได้ รหัส ข้อมูลรั่วไหล ยังสะท้อนถึงความกังวลของเจ้าของข้อมูลที่ไม่สามารถควบคุมการใช้งานข้อมูลส่วนบุคคลของตนเองได้ เนื่องจาก การทำงานในระบบเมืองอัจฉริยะมีความซับซ้อน และการทำงานของระบบเมืองอัจฉริยะจะมีประสิทธิภาพได้ต้องมีการแบ่งปันข้อมูลระหว่างอุปกรณ์และระหว่างหน่วยงานเกี่ยวข้องทั้งภาครัฐและเอกชน จึงเกิดความเสี่ยงที่ข้อมูลส่วนบุคคลของเจ้าของข้อมูลจะถูกนำไปใช้นอกเหนือจากวัตถุประสงค์ที่ได้ให้ความยินยอมไว้ ถูกเข้าถึงโดยไม่มีสิทธิหรือปราศจากอำนาจ หรือถูกส่งต่อไปยังหน่วยงานอื่นหรือถูกนำข้อมูล

³⁵ เมธิชา บุณยชิต, "การคุ้มครองข้อมูลชีวมาตรภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562," *วารสารนิเทศศาสตร์ มหาวิทยาลัยนเรศวร* 14 ฉบับที่ 1 (มกราคม-มิถุนายน 2564): 49-71.

ไปใช้โดยไม่รู้ตัว ส่งผลให้เจ้าของข้อมูลสูญเสียอำนาจควบคุมการใช้งานข้อมูลส่วนบุคคลของตน นอกจากนี้ ยังอาจเกิดความยากลำบากต่อเจ้าของข้อมูลในการติดตามเส้นทางข้อมูลส่วนบุคคลของตน หรือทำให้เกิดความสับสนเมื่อต้องการใช้สิทธิตามที่กฎหมายกำหนด เช่น สิทธิถอนความยินยอมและสิทธิในการขอเข้าถึงข้อมูลส่วนบุคคลที่เกี่ยวกับตน ซึ่งผู้วิจัยประเมินว่าความเสี่ยงนี้มีโอกาสที่จะเกิดขึ้นสูง และมีความร้ายแรงที่จะกระทบต่อสิทธิในการควบคุมข้อมูลของตนเอง หรือสิทธิในการตัดสินใจในเรื่องของตนเองสูง (Autonomy)

3. ผลกระทบต่อสิทธิและเสรีภาพอื่นๆ เนื่องจากในเมืองอัจฉริยะพิษณุโลกมีการติดตั้ง CCTV อยู่ทั่วทุกจุดของเมือง ประชาชนจึงอาจถูกละเมิดสิทธิความเป็นส่วนตัว หรือถูกแทรกแซงในความเป็นอยู่ส่วนตัวและถูกติดตามจากภาครัฐ (Surveillance) โดยเฉพาะในพื้นที่สาธารณะ³⁶ สิทธิความเป็นส่วนตัว หรือสิทธิส่วนบุคคล (Privacy) ในแง่นี้เป็นมุมมองของสิทธิมนุษยชนซึ่งต่างจากสิทธิในข้อมูลส่วนบุคคล ถูกรับรองและคุ้มครองตามมาตรา 32 แห่งรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 โดยมีฐานมาจากสิทธิที่จะอยู่ตามลำพัง (Right to be Let Alone) โดย Samuel D. Warren และ Louis D. Brandies และแนวความคิดการต้องการอยู่คนเดียว หรือการจำกัดการเข้าถึง การไม่ถูกแทรกแซงพื้นที่ส่วนตัว การมีอำนาจตัดสินใจ หรือปกครองตนเอง (Autonomy) และศักดิ์ศรีความเป็นมนุษย์ นอกจากนี้ ประชาชนยังอาจถูกติดตามหรือสอดส่องแม้ในพื้นที่ส่วนตัว หรือเคหสถานจากโทรศัพท์เคลื่อนที่ แอปพลิเคชัน เซนเซอร์ และอุปกรณ์ต่างๆ ดังนั้น นอกจากความเสี่ยงจากการกระทบสิทธิความเป็นส่วนตัว ยังมีความเสี่ยงในการกระทบเสรีภาพอื่นๆ ของประชาชน เช่น เสรีภาพในเคหสถานและเสรีภาพในการติดต่อสื่อสาร ซึ่งการถูกจำกัดสิทธิส่วนบุคคลและเสรีภาพนี้จะนำมาสู่การถูกควบคุมหรือการเซ็นเซอร์ตัวเองของประชาชน (Self-Censorship)³⁷ โดยผู้วิจัยมองว่าผลกระทบต่อสิทธิและเสรีภาพในแง่นี้มีโอกาสที่จะเกิดขึ้นสูงและมีความร้ายแรงในเชิงความเสียหายต่อสิทธิหรือจิตใจ เกิดการเซ็นเซอร์ตัวเอง ทั้งยังอาจทำให้ประชาชนไม่ไว้วางใจภาครัฐ

³⁶ Lilian Edwards, "Privacy, Security and Data Protection in Smart Cities: A Critical EU LAW Perspective." 13-14.

³⁷ Amalia Berggren, "Surveillance in Nineteen Eighty-Four: The Dismantling of Privacy in Oceania," (BA Thesis, Faculty of Art and Social Sciences, Department of Languages, English Department, Karlstad University 2016); James Boyle, "Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors," *University of Cincinnati Law Review* 66 (1997): 177.



3.6 การระบุมাত্রการในการจัดการหรือลดความเสี่ยงต่างๆ

หลังจากระบุและประเมินความเสี่ยงแล้วขั้นตอนต่อไปต้องระบุมাত্রการในการจัดการหรือลดความเสี่ยงนั้น ซึ่งถือเป็นขั้นตอนที่สำคัญที่สุดเพราะแสดงถึงการวางแผนที่ดี โดยควรระบุว่ามาตรการที่เลือกนำมาใช้นั้น สามารถจัดการหรือลดความเสี่ยงได้ หรือไม่ เพียงใด และหลังจากใช้มาตรการดังกล่าวแล้วความเสี่ยงจะลดลง หรือไม่ เพียงใด ทั้งยังควรวิเคราะห์ว่ามาตรการต่างๆ นั้นมีข้อดีและข้อเสียอย่างไร

1. ข้อมูลรั่วไหล ในการจัดการ หรือลดความเสี่ยงจากข้อมูลรั่วไหลนี้ผู้วิจัยจำแนกออกเป็น 2 มิติ ได้แก่ ความเสี่ยงจากภายในและภายนอก

1) ความเสี่ยงที่เกิดจากภายใน สามารถจัดการได้โดยการฝึกอบรมให้ความรู้บุคคลภายในหน่วยงาน และการปฏิบัติตามประกาศกระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563 และ 2565 เช่น กำหนดความรับผิดชอบของผู้ใช้งาน กำหนดเกี่ยวกับการอนุญาตและสิทธิการเข้าถึงข้อมูลโดยคำนึงถึงหลักการให้สิทธิเท่าที่จำเป็น มีมาตรการตรวจสอบและกำกับดูแลภายใน มีการแจ้งนโยบาย หรือแนวปฏิบัติแก่บุคลากร ทั้งนี้ เนื่องจากในบริบทเมืองอัจฉริยะนั้นมีการแบ่งปันข้อมูลระหว่างหน่วยงาน หรือองค์กรเป็นจำนวนมาก จึงควรมีการจัดทำบันทึกข้อตกลงการแบ่งปันข้อมูล ขอบเขตอำนาจหน้าที่และความรับผิดชอบระหว่างกันให้ชัดเจน โดยควรมีการจัดทำ DPIA ร่วมกัน

2) การจัดการหรือลดความเสี่ยงจากภายนอก เช่น ภัยคุกคามจากอาชญากรรม หรือภัยคุกคามทางเทคนิคสามารถจัดการ หรือลดความเสี่ยงได้โดยการใช้มาตรการในเชิงเทคนิค ซึ่งในเบื้องต้นควรเก็บข้อมูลเท่าที่จำเป็น (Data Minimization) และแยกข้อมูลเพิ่มเติมออกไปเพื่อให้ไม่สามารถระบุตัวบุคคลได้ (Pseudonymisation) หรือทำให้เป็นข้อมูลนิรนาม (Anonymisation) ควบคุมการเข้าถึงข้อมูลส่วนบุคคลโดยใช้ระบบการพิสูจน์และยืนยันตัวตนตลอดจนการเข้ารหัส (Encryption) ข้อมูลส่วนบุคคล มีกระบวนการทดสอบและประเมินประสิทธิภาพของมาตรการทางเทคนิคอย่างสม่ำเสมอ³⁸ และควรดำเนินการตามหลักการคุ้มครองข้อมูลส่วนบุคคลโดยการออกแบบและกำหนดค่าเริ่มต้น (Data Protection by Design and Default) ทั้งนี้ เนื่องจาก ระบบเมืองอัจฉริยะขึ้นอยู่กับ IoT และการแลกเปลี่ยนข้อมูลระหว่างอุปกรณ์ จึงควรศึกษาและปฏิบัติตามมาตรการคุ้มครองข้อมูลและจัดการความ

³⁸ The EU General Data Protection Regulation (GDPR), Article 32.

เสี่ยงในเรื่องการรั่วไหลของข้อมูลส่วนบุคคลในกรณี IoT โดยเฉพาะ อาทิ มาตรการของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติของสหรัฐอเมริกา (National Institute of Standards and Technology: NIST) (ซึ่งต่อไปนี้จะเรียกว่า NIST) ในกรณี IoT³⁹ เช่น ในการแลกเปลี่ยนข้อมูลบนระบบ IoT ต้องมีการเข้ารหัส (Encryption) ที่เข้มแข็ง โดยเฉพาะข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Data) ที่เป็นเรื่องละเอียดอ่อน และต้องมีการยืนยันตัวตนระหว่างอุปกรณ์คอมพิวเตอร์ก่อนส่งข้อมูลเสมอ มีการใช้ระบบการจัดการข้อมูลแบบรวมศูนย์โดยใช้เครื่องมือที่ได้มาตรฐานในการจัดการการแลกเปลี่ยนข้อมูลระหว่างอุปกรณ์ และแต่ละองค์กรต้องปฏิบัติตามนโยบาย หรือระเบียบที่วางไว้ร่วมกัน

2. เจ้าของข้อมูลส่วนบุคคลไม่สามารถควบคุมการใช้งานข้อมูลของตนได้ เพื่อลดความเสี่ยงในข้อนี้ควรคำนึงถึงหลักจำกัดวัตถุประสงค์ (Purpose limitation) ตามมาตรา 19 และมาตรา 23 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ โดยทำการประมวลผลข้อมูลส่วนบุคคลเฉพาะวัตถุประสงค์ที่ได้รับความยินยอมโดยชัดแจ้งเท่านั้น และต้องแจ้งรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลอย่างชัดเจนด้วยข้อความที่เข้าถึงได้ง่าย เข้าใจง่าย และใช้ภาษาที่อ่านง่าย ไม่คลุมเครือ ไม่เก็บรวบรวมหรือใช้ข้อมูลนอกขอบวัตถุประสงค์ที่แจ้งหรือนอกเหนือความคาดหมายอันสมเหตุสมผลของเจ้าของข้อมูล นอกจากนี้ ยังต้องคำนึงถึงหลักความเป็นอิสระในการให้ความยินยอมตามมาตรา 19 วรรคสี่ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ โดยต้องไม่นำการให้ความยินยอมมาเป็นเงื่อนไขในการให้บริการใดๆ ของเมืองอัจฉริยะ และต้องพิจารณาถึงความไม่สมดุลเชิงอำนาจต่อรอง เนื่องจากผู้ควบคุมข้อมูลส่วนบุคคลส่วนมากในเมืองอัจฉริยะเป็นหน่วยงานของรัฐ จึงทำให้ประชากรอยู่ในสถานะที่ด้อยกว่า ดังนั้น เพื่อเพิ่มอำนาจควบคุมข้อมูลส่วนตัวของประชากร ควรเสนอทางเลือกในการใช้บริการหากประชาชนปฏิเสธไม่ให้ความยินยอมประมวลผลข้อมูลส่วนบุคคล เช่น หากผู้ใช้บริการแอปพลิเคชันแคร่คุณหรือ NU Transit ปฏิเสธไม่ยอมให้บันทึกข้อมูลแหล่งที่อยู่ (Location Data) ผู้ใช้บริการต้องยังสามารถใช้บริการแอปพลิเคชันดังกล่าวได้แต่ประสิทธิภาพอาจจะลดลง นอกจากนั้น หน่วยงานต่างๆ ยังไม่ควรนำข้อมูลส่วนบุคคลที่ได้รับความยินยอมจากการใช้บริการหนึ่งไปต่อยอดหรือบูรณาการกับบริการหรือกิจกรรมหรือโครงการอื่นๆ ในเมืองอัจฉริยะนอกขอบวัตถุประสงค์ หากมีการนำข้อมูลไปใช้โดยมีวัตถุประสงค์แตกต่างจากที่ได้แจ้งไว้ต้องดำเนินการ ตามมาตรา 21 ก่อน กล่าวคือ ต้องมีการแจ้งวัตถุประสงค์ใหม่

3. ผลกระทบต่อสิทธิและเสรีภาพอื่นๆ ในเมืองอัจฉริยะ พิชญ์โลกได้มีการ

³⁹ NIST (National Institute of Standards and Technology), US Department of Commerce, "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks," (2019), accessed December 20, 2024. <https://doi.org/10.6028/NIST.IR.8228>.



ติดตามหรือสอดส่องประชาชน (Surveillance) เพื่อประโยชน์ด้านความปลอดภัย ลดจำนวนอาชญากรรม และจำนวนอุบัติเหตุ เป็นต้น อย่างไรก็ตาม เพื่อลดผลกระทบต่อสิทธิและเสรีภาพของประชาชน ต้องคำนึงถึงความจำเป็นและได้สัดส่วน ทั้งนี้ เมื่อพิจารณา Balancing Test จะเห็นว่าประชาชนสามารถคาดหมายความเป็นส่วนตัวได้อย่างสมเหตุสมผลในพื้นที่ส่วนตัว ดังนั้น การติดตาม หรือสอดส่องในพื้นที่ส่วนตัวนี้ จึงควรออกแบบระบบให้ประชาชนหรือผู้ใช้บริการสามารถเลือกที่จะไม่ถูกติดตาม หรือถูกประมวลผลข้อมูลส่วนบุคคลของตน (opt-out) ได้ อย่างไรก็ตาม ในบริเวณพื้นที่สาธารณะที่ความคาดหมายความเป็นส่วนตัวของประชาชนลดลง หรือในกรณีที่มีการขังน้ำหนัแล้วการติดตามและประมวลผลข้อมูลส่วนบุคคลมีความจำเป็นมากกว่า เพื่อความปลอดภัย หรือประโยชน์สาธารณะ เป็นต้น ก็ควรมีการเก็บรวบรวม ใช้ ข้อมูลส่วนบุคคลเท่าที่จำเป็น (Data Minimization) ที่สำคัญควรดำเนินการด้วยความโปร่งใส (Transparency) โดยต้องมีการแจ้งนโยบายเรื่องสิทธิส่วนบุคคลต่อสาธารณะและแจ้งรายละเอียดต่าง ๆ เกี่ยวกับการเก็บ รวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล เช่น ขอบเขตของการปฏิบัติการของ CCTV และขอบเขตการติดตามและสอดส่องประชาชน (Monitoring) นอกจากนี้ ต้องจัดให้มีการรับฟังความคิดเห็นและความมีส่วนร่วมของประชาชนอย่างสม่ำเสมอ มีการพัฒนาภาครัฐระบบเปิด (Open Government) เพื่อให้ประชาชนในพื้นที่ที่สามารถเข้าถึงเอกสารต่าง ๆ หรือติดตามตรวจสอบการทำงานของภาครัฐได้

3.7. การตรวจตราและทบทวน DPIA

เมื่อได้มีการจัดทำ DPIA และประเมินตามขั้นตอนต่าง ๆ ตามที่กล่าวมาข้างต้นจนครบถ้วนแล้ว ควรมีการบันทึกและจัดทำข้อสรุป เช่น ภาพรวมของความเสี่ยงที่เหลืออยู่พร้อมวางแผนการดำเนินการต่าง ๆ และต้องติดตามและตรวจสอบการดำเนินการตามที่ได้กำหนดไว้ เพื่อทบทวน ปรับปรุง หรือเปลี่ยนแปลง DPIA ภายหลังจากที่ได้ดำเนินการตามที่วางแผน

4. บทสรุปและข้อเสนอแนะ

จากการศึกษาพบว่า การประมวลผลข้อมูลส่วนบุคคลในเมืองอัจฉริยะพิษณุโลกนั้น มีความเสี่ยงสูง ก่อนเริ่มโครงการจึงควรมีการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลตามขั้นตอนต่าง ๆ และเนื่องจากลักษณะการประมวลผลข้อมูลส่วนบุคคลในเมืองอัจฉริยะมีความซับซ้อน จึงควรมีการจัดทำแผนผังการไหลเวียนของข้อมูลภายในเมืองอย่างละเอียด นอกจากนั้น เพื่อแก้ปัญหาความซ้ำซ้อนในอำนาจและหน้าที่ระหว่างองค์กรปกครองส่วนท้องถิ่น และความทับซ้อนในเขตพื้นที่โครงการเมืองอัจฉริยะ บทความวิจัยได้เสนอให้ องค์การบริหารส่วนจังหวัดเป็นผู้รับผิดชอบโครงการหลักโดยมีหน้าที่ประสานและเชื่อมโยงแผนงานโครงการเมืองอัจฉริยะในแต่ละพื้นที่ และกำหนดให้เป็นผู้ควบคุมข้อมูลส่วนบุคคล

โดยมีเทศบาลนครพิษณุโลกและมหาวิทยาลัยเนเธอร์แลนด์หน่วยงานภาครัฐและภาคเอกชนต่างๆ ที่เกี่ยวข้องเป็นผู้ควบคุมข้อมูลส่วนบุคคลร่วมในกิจกรรมที่ทำร่วมกัน หรือมีเขตพื้นที่การให้บริการทับซ้อนกัน เพื่อกำหนดขอบเขตอำนาจหน้าที่และความรับผิดชอบให้ชัดเจน ให้ดำเนินการจัดทำบันทึกข้อตกลงการเป็นผู้ควบคุมข้อมูลส่วนบุคคลร่วม ทั้งนี้ ในการประเมินความจำเป็นและความได้สัดส่วนให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวม และใช้ข้อมูลส่วนบุคคลได้เท่าที่จำเป็นภายในวัตถุประสงค์อันชอบด้วยกฎหมาย (Data Minimization) และภายใต้ฐานความยินยอมซึ่งต้องคำนึงถึงหลักจำกัดวัตถุประสงค์ (Purpose Limitation) หรือฐานทางกฎหมายอื่นๆ (Lawfulness of Processing) ซึ่งบทความวิจัยได้เสนอให้ใช้การประเมิน LIA ตามแนวทางของสหราชอาณาจักรมาช่วยชี้แจงนำหน้กระหว่างความจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายและสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคล

นอกจากนั้น บทความวิจัยได้ระบุและเสนอมาตรการจัดการ หรือลดความเสี่ยงจากการประมวลผลข้อมูลส่วนบุคคลในเมืองอัจฉริยะพิษณุโลก 3 ประการ ดังนี้ (1) ความเสี่ยงจากข้อมูลรั่วไหลซึ่งเกิดจากภายในสามารถจัดการได้โดยการฝึกอบรม หรือให้ความรู้บุคคลภายในหน่วยงาน มีมาตรการตรวจสอบและกำกับดูแลภายใน มีการแจ้งนโยบาย หรือแนวปฏิบัติแก่บุคลากร และมีการจัดทำบันทึกข้อตกลงการเป็นผู้ควบคุมข้อมูลส่วนบุคคลระหว่างองค์กร เป็นต้น ส่วนความเสี่ยงจากภายนอกสามารถจัดการได้ด้วยมาตรการในเชิงเทคนิคต่างๆ (2) เพื่อลดความเสี่ยงที่เจ้าของข้อมูลส่วนบุคคลจะไม่สามารถควบคุมการใช้งานข้อมูลของตนได้ การประมวลผลต้องคำนึงหลักจำกัดวัตถุประสงค์ (Purpose Limitation) ต้องให้อิสระในการให้ความยินยอมแก่เจ้าของข้อมูล และควรเสนอทางเลือกในการปฏิเสธไม่ให้ความยินยอมในการประมวลผลข้อมูลส่วนบุคคล (3) เพื่อลดผลกระทบต่อสิทธิส่วนบุคคลและเสรีภาพอื่นๆ ของประชาชน ต้องประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงความจำเป็นและได้สัดส่วน ดำเนินการด้วยความโปร่งใส ตรวจสอบได้ และมีการรับฟังความคิดเห็นของเจ้าของข้อมูลส่วนบุคคล



References

- Article 29 Data Protection Working Party (WP29). "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679 (wp248rev.01)." Accessed April 20, 2023. <https://ec.europa.eu/newsroom/article29/items/611236/en>.
- Berggren, Amalia. "Surveillance in Nineteen Eighty-Four: The Dismantling of Privacy in Oceania." BA Thesis, Faculty of Art and Social Sciences, Department of Languages, English Department, Karlstad University 2016.
- Binns, Reuben. "Data Protection Impact Assessments: A Meta-Regulatory Approach." *International Data Privacy Law* 7, no. 1 (2017): 22-35.
- Boyle, James. "Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors." *University of Cincinnati Law Review* 66 (1997): 177.
- Edwards, Lilian. "Privacy, Security and Data Protection in Smart Cities: A Critical EU LAW Perspective." *European Data Protection Law Review* 2, no. 1 (2016): 13-14.
- Digital Economy Promotion Agency. "Executive Summary: Phitsanulok Sustainable Smart City." Accessed January 10, 2025. <https://drive.google.com/file/d/1XQ51mDGUSgyKVofSuA6vapgYzvJYJp3W/view>. [In Thai]
- Digital Economy Promotion Agency. "Executive Summary: Phitsanulok Smart City." Accessed January 10, 2024. https://drive.google.com/file/d/1QCtAcVgfc_kQExfzNlrlQMax2s6Xv3O/view. [In Thai]
- Faisal, Kamrul. "Applying the Purpose Limitation Principle in Smart-City Data-Processing Practices: A European Data Protection Law Perspective." *Communication Law and Policy* 28, no. 1 (2023): 67-97.
- Information Commissioner's Office. "Data Protection Impact Assessments (DPIAs)." Accessed April 20, 2023. <https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias-1-0.pdf>

- Information Commissioner's Office (ICO). "Legitimate Interests." Accessed December 25, 2024. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/legitimate-interests/>
- Ismagilova, Elvira, Laurie Hughes, Nripendra P Rana, and Yogesh K Dwivedi. "Security, Privacy and Risks within Smart Cities: Literature Review and Development of a Smart City Interaction Framework." *Information Systems Frontiers* 24, no. 2 (2022): 1-22.
- Krishna, Rama Reddy Kummitha. "Smart Technologies for Fighting Pandemics: The Techno- and Human- Driven Approaches in Controlling the Virus Transmission." *Government Information Quarterly* 37, no. 3 (2020/07/01/ 2020). <https://dx.doi.org/https://doi.org/10.1016/j.giq.2020.101481>.
- Methicha Yuboolchit. "Biometric Data Protection under the Personal Data Protection Act 2019". *Naresuan University Law Journal* 14, no. 1 (June 18, 2021): 49–71. accessed June 18, 2025. <https://so04.tci-thaijo.org/index.php/lawnujournal/article/view/244415>. [In Thai]
- Michael Friedewald, Ina Schiering, Nicholas Martin and Dara Hallinan, "Data Protection Impact Assessments in Practice Experiences from Case Studies" in Computer Security ESORICS 2021 International Workshops Revised Selected Papers, Germany, October 4-8 2021.
- Na Pibul, Auntika. Legal challenges of the protection of personal data in the context of Smart City. *Graduate Law Journal* 13 no.2 (2020), 271–294. [In Thai]
- NIST (National Institute of Standards and Technology), US Department of Commerce. "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks." (2019). Accessed December 20, 2024. <https://doi.org/10.6028/NIST.IR.8228>
- Office of Data Protection Commissioner. "Ireland, Twentieth Annual Report of the Data Protection Commissioner 2008." Accessed January 24, 2025. <https://www.dataprotection.ie/sites/default/files/uploads/2018-12/AR2008.pdf>
- Personal Data Protection Commission Singapore. "Guide to Data Protection Impact Assessments." Accessed April 20, 2023. <https://www.pdpc.gov.sg/help-and-resources/2017/11/guide-to-data-protection-impact-assessments>.



- Phitsanulok Provincial Labour Office. Labour Situation Report, Phitsanulok Province, Q1 2025. 2025. Accessed May 28, 2025. <https://phitsanulok.mol.go.th/wp-content/uploads/sites/23/2025/05/-1-2568.pdf>. [In Thai]
- Suwannakit, Methinee, "The Protection of Privacy and Private Information in the Digital Age: A Comparative Study of English and Thai law Applying to Individual Media Users," (PhD thesis, University of Glasgow, UK, 2023), 103-104.
- Vandercruysse, Laurens, Caroline Buts, Michael Doms. "A typology of Smart City services: The case of Data Protection Impact Assessment" Cities 104 (2020) 102731.