ความท้าทายทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคล ในบริบทของเมืองอัจฉริยะ (SMART CITY)

LEGAL CHALLENGES OF THE PROTECTION OF PERSONAL DATA IN THE CONTEXT OF SMART CITY

อัญธิกา ณ พิบูลย์

Auntika Na Pibul

อาจารย์ประจำ คณะนิติศาสตร์ สถาบันบัณฑิตพัฒนบริหารศาสตร์ : auntika.n@nida.ac.th

Lecturer, School of Law, National Institute of Development Administration : auntika.n@nida.ac.th

Received : May 20, 2020

Revised : June 27, 2020

Accepted : June 29, 2020

บทคัดย่อ

บทความฉบับนี้เป็นการนำเสนอผลการศึกษาวิจัยในเรื่องความท้าทายทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลในบริบทของเมืองอัจฉริยะ โดยวิเคราะห์จากเอกสารทางกฎหมายต่าง ๆ ที่เกี่ยวข้องงานวิจัยนี้มีคำถามหลักในการวิจัย คือ “อะไรคือความท้าทายทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลในบริบทของเมืองอัจฉริยะ” เนื่องจากการทำงานของเมืองอัจฉริยะนั้นมีการใช้เทคโนโลยีหลากหลายประเภทในการบริหารจัดการโครงสร้างของเมือง กล่าวคือ มีการเชื่อมโยงอุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ ผ่านเครือข่ายอินเตอร์เน็ต ภายใต้แนวความคิดของ Internet of Things ส่งผลให้มีการเก็บรวบรวมข้อมูลส่วนบุคคลเป็นจำนวนมากในลักษณะของ Big Data เพื่อนำไปใช้ในการวิเคราะห์และคาดเดาผลซึ่งเป็นการทำงานของระบบ Machine Learning โดยข้อมูลทั้งหมดนี้ได้รับการประมวลผลอยู่บนโครงสร้างของ Cloud Computing จากการศึกษาวิจัยจึงพบว่าลักษณะการประมวลผลข้อมูลส่วนบุคคลในบริบทของเมืองอัจฉริยะ ทำให้เกิดความท้าทายทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคล 2 ประเด็น ดังนี้ (1) ประเด็นเกี่ยวกับการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล และ (2) ประเด็นเกี่ยวกับการกำหนดสถานะ หน้าที่ และความรับผิดของผู้ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล ผู้เขียนจึงเสนอแนะแนวทางที่พอจะเป็นไปได้ในการจัดการกับความท้าทายดังกล่าว ทั้งนี้เพื่อเป็นการคุ้มครองความปลอดภัยของข้อมูลส่วนบุคคลและสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคล

คำสำคัญ

การคุ้มครองข้อมูลส่วนบุคคล, ความท้าทายทางกฎหมาย, เมืองอัจฉริยะ, Internet of Things, Big Data, Machine Learning, Cloud Computing

ABSTRACT

This article presents the result of the research project about the legal challenges of the protection of personal data in the context of smart city by adopting document-based methodology. The main research question of this project was that: “What are the legal challenges of the protection of personal data in the context of smart city?”. With regard to the nature of smart city, various kinds of technology, are adopted to manage and control the city’s infrastructure. Firstly, the operation of the “Internet of Things” which is the concept about connecting all the electronic devices via the Internet generates the collection of a large amount of

personal data which is called “Big Data”. The Big Data is the main resource under the process of the data analytic for making a prediction which is the major function of “Machine Learning”. And all personal data are processed in the “Cloud Computing” infrastructure. From the study, it was found that the processing of personal data in the context of smart city brought about two main legal challenges: (1) the issue about obtaining consent from the data subjects; and (2) the issue about identifying status, responsibility and liability of the parties involved in the processing of personal data. Finally, the potential approaches for addressing such legal challenges were suggested with a view to protecting the personal data and the right to privacy of the data subjects in the context of smart city.

Keywords

Personal Data Protection, Legal Challenges, Smart City, Internet of Things, Big Data, Machine Learning, Cloud Computing

1. บทนำ

ในปัจจุบันเทคโนโลยีมีความเจริญก้าวหน้าไปอย่างมาก ข้อมูลข่าวสารต่าง ๆ ถูกนำเข้าสู่ระบบออนไลน์ทั้งหมด ทำให้ทุกคนสามารถเข้าถึงข้อมูลข่าวสารได้อย่างรวดเร็วผ่านทางเครือข่ายอินเทอร์เน็ต ซึ่งข้อมูลเหล่านี้ถูกนำไปใช้เพื่อสร้างประโยชน์ในกิจกรรมของทั้งภาครัฐ และภาคเอกชนมากมาย หนึ่งในกิจกรรมดังกล่าว ก็คือ การสร้างเมืองอัจฉริยะ โดยการเชื่อมต่อโครงสร้างพื้นฐานของเมือง เช่น ระบบไฟฟ้า ประปา โทรศัพท์ และบริการของภาครัฐหรือภาคเอกชนให้เป็นเครือข่ายเดียวกันบนระบบอินเทอร์เน็ตเป็นแนวคิดในการนำเอาเทคโนโลยีขั้นสูงและนวัตกรรมใหม่ ๆ เข้ามาควบคุมและพัฒนาการบริหารจัดการเมือง เพื่อให้มีการใช้ทรัพยากรให้เกิดประสิทธิภาพสูงสุด ตลอดจนลดผลกระทบต่อสิ่งแวดล้อม ลดค่าใช้จ่าย ประหยัดพลังงาน ทำให้เกิด ความเติบโต ทางเศรษฐกิจแบบยั่งยืน และพัฒนาคุณภาพชีวิตให้แก่ผู้ที่อยู่อาศัยในเมืองทุกคน[1]

แนวความคิดของการสร้างเมืองอัจฉริยะเกิดขึ้นพร้อม ๆ กับการพัฒนาอย่างก้าวกระโดดของเทคโนโลยีต่าง ๆ การทำงานของเมืองอัจฉริยะจึงได้นำเอาเทคโนโลยีหลากหลายรูปแบบ ได้แก่ Internet of Things, Big Data, Machine Learning และ C loudComputing[2] มาใช้เพื่อประมวลผลข้อมูล ในช่วงระยะเวลาที่ผ่านมาจะเห็นได้ว่าประเทศต่าง ๆ ได้มีการนำเอาแนวคิดของเมืองอัจฉริยะมาใช้เพื่อจัดการทรัพยากรในเมืองให้มีประสิทธิภาพยิ่งขึ้นและสร้างความสะดวกสบายให้กับประชาชนในเมืองมากยิ่งขึ้น แต่อย่างไรก็ตามเนื่องจากลักษณะการทำงานของเมืองอัจฉริยะนั้นจำเป็นต้องใช้ข้อมูลจำนวนมาก ซึ่งรวมถึงข้อมูลส่วนบุคคลเป็นปัจจัยหลักในการวิเคราะห์และประมวลผลเพื่อกำหนดลักษณะของกิจกรรมใน การให้บริการประเภทต่าง ๆ ดังนั้น ข้อมูลส่วนบุคคลจึงถูกเก็บรวบรวมประมวลผลและส่งต่อไปโดยระบบอัตโนมัติ ซึ่งกรณีนี้จะมีหน่วยงานภาคเอกชนต่าง ๆ เข้ามาเกี่ยวข้องในลักษณะของการเสนอขายสินค้าและบริการต่าง ๆ เพื่ออำนวยความสะดวกให้กับประชาชนอันเป็นวัตถุประสงค์ที่สำคัญประการหนึ่งของการสร้างเมืองอัจฉริยะ แต่อย่างไรก็ตาม กิจกรรมดังกล่าว ทำให้หน่วยงานภาคเอกชนสามารถเข้าถึงข้อมูลส่วนบุคคลของประชาชนจำนวนมากได้ ซึ่งการควบคุมการเข้าถึงข้อมูลดังกล่าวก็เป็นไปได้ยาก อีกทั้งมีความเป็นไปได้ที่การเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลดังกล่าว อาจจะไม่ได้ปฏิบัติตามหลักเกณฑ์ตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดไว้ ซึ่งกรณีนี้จะส่งผลกระทบโดยตรงต่อความปลอดภัยของข้อมูลส่วนบุคคลของเจ้าของข้อมูลในฐานะเป็นผู้ใช้สินค้าและบริการต่าง ๆ ในเมืองอัจฉริยะ

จึงอาจกล่าวได้ว่าลักษณะของการประมวลผลข้อมูลส่วนบุคคลในบริบทของเมืองอัจฉริยะสามารถทำให้เกิดความท้าทายทางกฎหมายในคุ้มครองข้อมูลส่วนบุคคล ซึ่งสามารถแยกพิจารณาออกได้เป็น 2 ประเด็น ดังต่อไปนี้ (1) เรื่องการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลซึ่งเป็นฐานทางกฎหมายประการหนึ่ง (legal basis) ที่ทำให้หน่วยงานภาคเอกชนสามารถเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลของประชาชน ในลักษณะเพื่อเป็นการเสนอขายสินค้าและบริการแก่เจ้าของข้อมูลส่วนบุคคลได้โดยชอบด้วยกฎหมาย ; (2) เรื่องการกำหนดสถานะ หน้าที่ความรับผิดของหน่วยงานภาคเอกชนที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล โดยเฉพาะในกรณีที่มีการละเมิดข้อมูลเกิดขึ้น ซึ่งทั้งสองประเด็นส่งผลให้เกิดความเสี่ยงต่อความปลอดภัยของข้อมูลส่วนบุคคลและการคุ้มครองสิทธิ

---

[1] Annalisa Cocchia, “Smart and Digital City : A Systematic Literature Review,” in Renata Paolo Dameri, Camille Rosenthal-Sabroux (eds), Smart City How to Create Public and Economic Value, p.13 - 43. Springer, 2014.

[2] เนื่องจากยังไม่มีการกำหนดคำศัพท์ภาษาไทยสำหรับคำศัพท์ภาษาอังกฤษเหล่านี้ ซึ่งเป็นที่ยอมรับและเข้าใจได้เป็นการทั่วไปโดยสำนักงานราชบัณฑิตยสภา ผู้เขียนจึงยังคงใช้คำศัพท์ภาษาอังกฤษเหล่านี้เมื่ออ้างถึงเทคโนโลยีดังกล่าว โดยคำศัพท์แต่ละคำมีความหมายดังต่อไปนี้ (1) Internet of Things หมายถึงระบบที่มีการเชื่อมโยงอุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ เข้าด้วยกันผ่านระบบเครือข่ายอินเทอร์เน็ต ; (2) Big Data หมายถึง ฐานข้อมูลขนาดใหญ่ ; (3) Machine Learning หมายถึง ระบบการเรียนรู้ได้ด้วยตัวเองของเครื่องจักร ; (4) Cloud Computing หมายถึงระบบการให้บริการทรัพยากรคอมพิวเตอร์ผ่านเครือข่ายอินเทอร์เน็ตทั้งนี้รายละเอียดของเทคโนโลยีแต่ละประเภทผู้เขียนได้นำเสนอไว้ในข้อ 2.2

ความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคล อันเป็นสิทธิขั้นพื้นฐานของประชาชนที่ควรได้รับความคุ้มครอง[3] ด้วยเหตุนี้ผู้เขียนจึงเลือกศึกษาประเด็นความท้าทายทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลของประชาชนในบริบทของเมืองอัจฉริยะ ในฐานะที่เป็นประเด็นซึ่งไม่ค่อยได้รับความสนใจมากนักเมื่อเทียบกับประเด็นในเรื่องความสะดวกสบายที่ประชาชนจะได้รับจากระบบการทำงานของเมืองอัจฉริยะซึ่งนำเอาเทคโนโลยีที่มีความทันสมัยต่าง ๆ มาใช้

วัตถุประสงค์ของบทความฉบับนี้ คือ การนำเสนอผลการศึกษาวิจัยเพื่อหาคำตอบต่อคำถามของงานวิจัยที่ว่า “อะไรคือความท้าทายทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลในบริบทของเมืองอัจฉริยะ” ซึ่งในการค้นหาคำตอบดังกล่าว ผู้เขียนได้กำหนดขอบเขตในการศึกษาวิจัยออกเป็น 4 หัวข้อ ดังต่อไปนี้

(1) แนวคิดและลักษณะการทำงานของเมืองอัจฉริยะที่เกี่ยวข้องกับการใช้เทคโนโลยีต่าง ๆ ในการประมวลผลข้อมูลส่วนบุคคล

(2) หลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลในบริบทของเมืองอัจฉริยะตามกฎหมายของสหภาพยุโรป และกฎหมายไทย

(3) บทวิเคราะห์ความท้าทายทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลที่เกิดขึ้นจากการปรับใช้หลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลกับการประมวลผลข้อมูลส่วนบุคคลในบริบทของเมืองอัจฉริยะ

(4) ข้อเสนอแนะแนวทางในการจัดการกับความท้าทายทางกฎหมาย ในการคุ้มครองข้อมูลส่วนบุคคลในบริบทของเมืองอัจฉริยะ

งานวิจัยนี้ใช้วิธีการวิจัยเชิงเอกสาร (Documentary Research) เพื่อค้นหาคำตอบดังกล่าว โดยมุ่งศึกษา

(1) เอกสารขั้นปฐมภูมิ (primary document) ได้แก่ กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation) และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทย (พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)

(2) เอกสารชั้นทุติยภูมิ (secondary document) ได้แก่ หนังสือ บทความในวารสารภาษาไทยและต่างประเทศ รวมทั้งข้อมูลจากหน่วยงานของสหภาพยุโรปที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล เช่น Article 29 Data Protection Working Party (A29WP) และ European Data Protection Board (EDPB) รวมทั้งข้อมูลจากเว็บไซต์ของหน่วยงานต่าง ๆ ที่เกี่ยวข้อง

2. ความทั่วไปเกี่ยวกับเมืองอัจฉริยะ

2.1 แนวคิดและลักษณะของเมืองอัจฉริยะ

แนวคิดของเมืองอัจฉริยะ คือ การนำระบบเทคโนโลยีดิจิทัล หรือระบบเทคโนโลยีสารสารสนเทศและการสื่อสาร (Information Communication Technology (ICT)) มาบูรณาการเพื่อบริหารจัดการเมืองที่มีความซับซ้อนให้มีประสิทธิภาพมากยิ่งขึ้น ช่วยลดต้นทุนการบริหารจัดการลดต้นทุนด้านพลังงาน เพิ่มความสะดวกคล่องตัวให้กับวิถีชีวิตของประชาชน มีความปลอดภัย มีสิ่งแวดล้อมที่ดี มีคุณภาพชีวิตที่ดีขึ้น และแนวคิดดังกล่าวถือเป็นการพัฒนาอย่างยั่งยืนในลักษณะของการแก้ไขปัญหาสังคมเมือง โดยใช้เทคโนโลยีและนวัตกรรม เพื่อสร้างโครงสร้างพื้นฐานที่สำคัญของเมืองถือเป็นตัวเชื่อมต่อความต้องการของประชาชนกับระบบงานบริการของทางภาครัฐ และภาคเอกชนให้มีประสิทธิภาพสูงสุด[4] กลไกสำคัญในการขับเคลื่อนเมืองอัจฉริยะ คือ การเชื่อมข้อมูลและเทคโนโลยีเข้าด้วยกัน โดยนำเทคโนโลยีประเภทต่าง ๆ เข้ามามีส่วนร่วมในการวางโครงสร้างพื้นฐานของระบบงานบริการของทั้งภาครัฐและ

[3] Jesse W. Woo, “Smart Cities Pose Privacy Risks and Other Problems, But that Doesn't Mean We Shouldn't Build Them,” University of Missouri-Kansas City Law Review 83:4, p.953 - 971 (2017). And Liesbet van Zoonen, “Privacy Concerns in Smart Cities,” Government Information Quarterly. 33:3, p.1 – 9 (2016).

[4] Emmanouil Tranos and Drew Gertner, “Smart Networked Cities?,” Innovation : The European Journal of Social Science Research 25:2, p.175 – 190 (April 2012).

ภาคเอกชนเพื่อเพิ่มศักยภาพให้เมืองมีประสิทธิภาพมากขึ้น ทั้งนี้เพื่อเป็นการตอบสนองความต้องการของคนทุกเพศทุกวัยได้อย่างตรงจุด ซึ่งหมายถึงการพัฒนาคุณภาพชีวิตของคนในสังคมเมืองให้ดีขึ้น

แต่อย่างไรก็ตาม ยังไม่พบคำนิยามของเมืองอัจฉริยะที่ได้รับการยอมรับเป็นการทั่วไป คำนิยาม ที่พบมีความหลากหลายแตกต่างกันไปขึ้นอยู่กับว่า หน่วยงานใดจะเป็นผู้ให้คำนิยาม[5] จากการศึกษา ผู้เขียนสามารถสรุปสาระสำคัญของลักษณะของเมืองอัจฉริยะได้ 3 ประการ ดังต่อไปนี้

(1) โครงข่ายของเซ็นเซอร์ที่มีการเชื่อมโยงกับอุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ เช่น รถยนต์ มาตรวัดไฟฟ้า หรือเครื่องใช้ไฟฟ้าภายในบ้าน เช่น ตู้เย็น โทรทัศน์ เครื่องปรับอากาศ ฯลฯ ซึ่งอุปกรณ์เหล่านี้จะเชื่อมโยงกันในโครงข่ายดิจิทัล ที่เรียกกันว่า Internet of Things[6] โดยระบบเซ็นเซอร์ จะควบคุมการทำงานของอุปกรณ์อิเล็กทรอนิกส์ และจะสร้างข้อมูลจำนวนมหาศาลในลักษณะที่เรียกว่า Big Data;[7]

(2) โครงข่ายของการสื่อสารแบบดิจิทัลที่มีสร้างข้อมูลขึ้นอย่างต่อเนื่องโดยใช้วิธีการรับข้อมูลจากแหล่งอื่น ๆ เป็นจำนวนมาก (data streaming)[8] ในรูปแบบตามเวลาจริง (real time) ซึ่งสามารถเชื่อมต่อกันภายในโครงข่ายและระหว่างโครงข่ายได้ ทั้งนี้ก็เพื่อให้ มีการประมวลผลให้ได้ผลลัพธ์ที่มีประโยชน์สูงสุด

(3) โครงข่ายที่มีประสิทธิภาพสูง ซึ่งทำงานอยู่บนโครงสร้างของ Cloud Computing[9] ซึ่งให้บริการพื้นที่จัดเก็บข้อมูลต่าง ๆ ของโครงข่ายที่มีการเชื่อมโยงกันอย่างมหาศาล เพื่อให้การทำงานของระบบมีความรวดเร็ว และได้ผลลัพธ์ที่แม่นยำ

2.2 การทำงานของเมืองอัจฉริยะที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล

ปัจจัยหลักที่สำคัญในการทำงานของเทคโนโลยีในเมืองอัจฉริยะก็คือ ข้อมูลจึงทำให้ต้องมีการนำเข้าสู่ระบบซึ่งข้อมูลหลากหลายประเภทเป็นจำนวนมาก ซึ่งรวมถึงข้อมูลส่วนบุคคลด้วย โดยข้อมูลดังกล่าวจะถูกนำเข้าสู่ระบบการทำงานของเทคโนโลยีต่าง ๆ ดังนี้ (1) Internet of Things ซึ่งเป็น เทคโนโลยีที่เชื่อมโยงอุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ เข้าด้วยกันบนเครือข่ายอินเทอร์เน็ตทำให้เราสามารถควบคุมการใช้งานอุปกรณ์ผ่านทางเครือข่ายอินเทอร์เน็ต เช่น การเปิด ปิด อุปกรณ์เครื่องใช้ไฟฟ้า โดยสั่งการผ่านทางมือถือได้ ซึ่งเทคโนโลยี Internet of Things นี้ จะทำงานร่วมกันกับเทคโนโลยีที่ใช้ระบุสิ่งต่าง ๆ โดยใช้คลื่นวิทยุ (Radio Frequency Identification (RFID)) และระบบเซ็นเซอร์เพื่อให้อุปกรณ์ต่าง ๆ สามารถเชื่อมต่อและรับส่งข้อมูลถึงกันได้[10] โดยข้อมูลดังกล่าวจะได้รับการประมวลผลโดยใช้ระบบขั้นตอนการแก้ไขปัญหา (Algorithm) ภายใต้การทำงานของเทคโนโลยีการเรียนรู้ได้ด้วยตัวเองของเครื่องจักรที่เรียกว่า (2) Machine Learning[11] ทั้งนี้เพื่อวิเคราะห์และคาดเดาผลลัพธ์ต่าง ๆ ให้สอดคล้องกับความต้องการของผู้ใช้บริการแต่ละรายให้ได้มากที่สุด ซึ่งระบบการทำงานนี้จะสร้างฐานข้อมูลขนาดใหญ่ที่มีความซับซ้อน

---

[5] Annalisa Cocchia*, อ้างแล้ว* เชิงอรรถที่ 1, น.18 - 19.

[6] Vlasios Tsiatsis, Stamatis Karnouskos, Jan Holler, David Boyle and Catherine Mulligan, Internet of Things : Technologies and Applications for a New Age of Intelligence, 2nd edition (Academic Press, 2018), p.5 - 36.

[7] Zhu Han, Mingyi Hong and Dan Wang, Signal Processing and Networking for Big Data Applications, (Cambridge University Press, 2017), p.11 - 30.

[8] Andrew G. Psaltis, Streaming Data : Understanding the Real-time Pipeline, (New York : Manning Publications Co., 2017), p.3 - 12.

[9] Erl Thomas, Zaigham Mahmood and Ricaldo Puttini, Cloud Computing : Concept Technology & Technology, (Prentice Hall, 2013), p.25 - 50.

[10] Gaurav Sarin, "Developing Smart Cities Using Internet of Things : An Empirical Study," SSRN Electronic Journal, (May 2016).

[11] Zaheer Allam and Zaynah A. Dhunny, "On Big Data, Artificial Intelligence and Smart Cities in Cities," Cities 89, (January 2019), p.80 - 91

หลากหลาย และมีการเปลี่ยนแปลงได้อย่างรวดเร็ว ในลักษณะที่เรียกว่า (3) Big Data[12] โดยข้อมูลเหล่านี้จะได้รับการประมวลผลอยู่บนโครงสร้างที่มีประสิทธิภาพสูงของ (4) Cloud Computing อันเป็นเทคโนโลยีการให้บริการ ระบบคอมพิวเตอร์ และทรัพยากรคอมพิวเตอร์ผ่านเครือข่ายอินเทอร์เน็ต ทำให้ผู้ใช้บริการไม่จำเป็นต้องลงทุนซื้อซอฟแวร์และฮาร์ดแวร์ ลดภาระความรับผิดชอบในการดูแลทรัพยากรคอมพิวเตอร์ โดยผู้ใช้บริการ Cloud Computing สามารถเพิ่มลดจำนวนเองได้ตามความต้องการและจ่ายตามที่ใช้เท่านั้น

ซึ่งเมื่อพิจารณาโดยภาพรวมของกิจกรรมที่เกิดขึ้นในเมืองอัจฉริยะแล้ว เห็นได้อย่างชัดเจนว่าจะเป็นกิจกรรมที่ในลักษณะที่เป็นการดำเนินร่วมกันระหว่างหน่วยงานภาครัฐและภาคเอกชน (Public Private Partnerships (PPP)) กล่าวคือ ภาครัฐมักจะอยู่ในฐานะเป็นให้ทุนสนับสนุนแก่หน่วยงานภาคเอกชนที่มีเทคโนโลยี และความเชี่ยวชาญต่าง ๆ เข้ามาสร้างและพัฒนาเมืองอัจฉริยะรวมทั้งให้เสนอสินค้าและให้บริการต่าง ๆ ในเมืองอัจฉริยะ[13] ดังนั้น ความเข้าใจที่ว่าข้อมูลส่วนบุคคลของประชาชนที่ได้รับการเก็บรวบรวมในบริบทของเมืองอัจฉริยะจะอยู่ภายใต้การครอบครองและควบคุมโดยหน่วยงานภาครัฐแต่เพียงหน่วยงานเดียว จึงเป็นสิ่งที่ไม่ตรงกับข้อเท็จจริงที่เกิดขึ้น เนื่องจากในการดำเนินกิจกรรมต่าง ๆ ภายในเมืองอัจฉริยะเพื่อให้บรรลุวัตถุประสงค์นั้น ข้อมูลส่วนบุคคลของประชาชนจะได้รับการเก็บรวบรวมโดยทั้งหน่วยงานภาครัฐและภาคเอกชน ซึ่งหากพิจารณาข้อเท็จจริงแล้วอาจกล่าวได้ว่า หน่วยงานภาคเอกชนต่าง ๆ เข้ามามีบทบาทเกี่ยวข้องกับการเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของประชาชนมากกว่าหน่วยงานภาครัฐเสียอีก ยกตัวอย่างเช่น หน่วยงานภาคเอกชนที่ให้บริการเครือข่ายอินเทอร์เน็ตต่าง ๆ ถูกมองว่าเป็นต้นทางในการได้รับ และเก็บรวบรวมข้อมูลส่วนบุคคลของประชาชนเป็นจำนวนมากเพราะกิจกรรมต่างที่เกิดขึ้นจะใช้ฐานออนไลน์เป็นเครื่องมือหลักในการเนินการ[14] ซึ่งจากข้อเท็จจริงนี้ทำให้ข้อมูลดังกล่าวถูกนำแบ่งปันให้หน่วยงานต่าง ๆ ในภาคเอกชน เพื่อวัตถุประสงค์ในการเสนอขายสินค้าและบริการต่าง ๆ จึงมีนักวิชาการจำนวนกล่าวไว้ว่า สัดส่วนของข้อมูลส่วนบุคคลในบริบทของเมืองอัจฉริยะที่ได้รับการประมวลผล โดยหน่วยงานภาคเอกชนนั้นมีมากกว่าหน่วยงานภาครัฐ จากข้อเท็จจริงดังกล่าวจึงเกิดประเด็นปัญหาถกเถียงกันในเรื่องความเป็นเจ้าของข้อมูลดังกล่าว ซึ่งโยงไปถึงประเด็นว่าหน่วยงานภาคเอกชนสามารถนำเอาข้อมูลดังกล่าวไปใช้ในกิจกรรมของตนในการเสนอขายสินค้า หรือบริการได้หรือไม่ เพราะการได้รับข้อมูลมานั้นเจ้าของข้อมูลได้ทราบวัตถุประสงค์ของการให้ข้อมูลว่าเป็นไป เพื่อการให้บริการสาธารณะต่าง ๆ ของภาครัฐ[15] ประเด็นนี้จึงก่อให้เกิดปัญหาทางกฎหมาย ซึ่งจะขอนำเสนอบทวิเคราะห์ปัญหาดังกล่าวในข้อ 4 ต่อไป

เมื่อพิจารณาถึงกิจกรรมต่าง ๆ ที่เกิดขึ้นในบริบทของเมืองอัจฉริยะแล้ว จะเห็นได้ว่าข้อมูลส่วนบุคคลจะได้รับการเก็บรวบรวมโดยหน่วยงานภาครัฐ และหน่วยงานภาคเอกชนในลักษณะต่าง ๆ เพื่อนำไปใช้สำหรับวัตถุประสงค์แตกต่างกันไป ดังต่อไปนี้

(1) ข้อมูลส่วนบุคคลที่ใช้เพื่อวัตถุประสงค์ของหน่วยงานของรัฐ

- เพื่อการให้บริการสาธารณะ

---

[12] Andrea De Mauro, “What is Big Data? A Consensual Definition and a Review of Key Research Topics,” 4th International Conference on Integrated Information conference, Madrid, September 2014. And Gartner IT Glossary, “What is Big Data?,” retrieved on January 12, 2020, from www.gartner.com/it-glossary/big-data.

[13] Smart Cities Council, “Smart Cities Financing Guide,” retrieved on January 12, 2020, from https ://smartcitiescouncil.com/resources/smart-cities-financing-guide.

[14] Marco Balabanovic, Paul Galwas, “Whose Smart City is it Anyway?,” retrieved on January 28, 2020, from https://www.scl.org/articles/3389-whose-smart-city-is-it-anyway.

[15] BIS Research Paper No. 135, “Global Innovators : International Case Studies on Smart Cities (2013),” retrieved on January 28, 2020, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/249397/bis-13-1216-global-innovators-international-smartcities.pdf.

ข้อมูลส่วนนี้ได้รับมาจากเจ้าของข้อมูลส่วนบุคคลโดยตรงจากการที่เจ้าของข้อมูลลงทะเบียนไว้กับสำนักงานเขต หรืออำเภอ ในส่วนที่เกี่ยวกับประชาชน และผู้อยู่อาศัยเป็นการเก็บรวมข้อมูลส่วนบุคคลที่เกี่ยวกับสิทธิทางแพ่งของพลเมือง เช่น การแจ้งเกิด การแจ้งตาย และการจดทะเบียนสมรส ข้อมูลที่อยู่อาศัย และข้อมูลการเลือกตั้ง นอกจากนั้นยังได้รับข้อมูลจากเจ้าของข้อมูลส่วนบุคคลโดยตรงจากการที่เจ้าของข้อมูลทำธุรกรรมทางออนไลน์ประเภทต่าง ๆ กับหน่วยงานของรัฐ เช่น การจ่ายภาษี การลงทะเบียนประกันสังคม[16] โดยมีวัตถุประสงค์หลักในการเอื้อหนุนการจัดการเมือง การวางผังเมือง การจัดสรรการให้บริการและสวัสดิการต่าง ๆ ของรัฐแก่ประชาชน

- เพื่อการเฝ้าระวังและรักษาความปลอดภัย

ข้อมูลส่วนนี้ได้รับมาจากเจ้าของข้อมูลส่วนบุคคลโดยตรงจากการเก็บรวบรวมของหน่วยงานทางปกครองและหน่วยงานตำรวจ เช่น ข้อมูลเกี่ยวกับประวัติการกระทำความผิดของประชาชน และยังมีข้อมูลที่เก็บรวบรวมจากการทำงานของอุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ เช่น ข้อมูลเกี่ยวกับพฤติกรรมของประชาชนที่ได้มาจากภาพถ่ายจากกล้องวงจรปิด นอกจากนั้นยังมีข้อมูลที่เก็บรวบรวมได้จากฐานออนไลน์ของผู้ให้บริการออนไลน์ประเภทต่าง ๆ ยกตัวอย่างเช่น ในประเทศเนเธอร์แลนด์ รัฐบาลได้จัดทำโปรแกรมเพื่อค้นหาความเสี่ยงที่ของประชาชนที่จะเป็นผู้กระทำความผิดที่มีชื่อเรียกว่า SyRI โปรแกรมนี้จะเก็บรวบรวมข้อมูลที่เป็นพฤติกรรมของประชาชนทางออนไลน์เพื่อวิเคราะห์ว่าประชาชนแต่ละคนมีแนวโน้มที่จะกระทำความผิดหรือไม่ ซึ่งบุคคลที่ถูกจัดว่าเป็นผู้ที่มีความเสี่ยงที่จะกระทำความผิดจะได้รับการจัดกลุ่มและบันทึกไว้ จากนั้นก็จะมีการแบ่งปันข้อมูลดังกล่าวกันระหว่างหน่วยงานของรัฐ[17]

(2) ข้อมูลส่วนบุคคลที่ใช้เพื่อวัตถุประสงค์ของหน่วยงานภาคเอกชน

ข้อมูลส่วนนี้ได้รับมาโดยตรงจากเจ้าของข้อมูลส่วนบุคคลจากการที่ ประชาชนเข้ามาซื้อสินค้า และบริการประเภทต่าง ๆ ซึ่งเจ้าของข้อมูลส่วนบุคคลจะต้องกรอกข้อมูลต่าง ๆ ไว้กับผู้ขายสินค้าและบริการประเภทนั้น ๆ เอง ซึ่งการซื้อขายสินค้าในปัจจุบัน มักจะอยู่ในรูปแบบของออนไลน์ ในกรณีนี้จึงทำให้หน่วยงานภาคเอกชนต่าง ๆ ได้รับข้อมูลส่วนบุคคลของประชาชนจากฐานออนไลน์เป็นจำนวนมาก ไม่ว่าจะเป็นการได้รับโดยตรงจากเจ้าของข้อมูล หรือได้รับจากการแบ่งปันมาจากหน่วยงานภาคเอกชนอื่น ๆ หรือได้รับมาจากการแบ่งปันกันเองในระบบอัตโนมัติจากการทำงานของเทคโนโลยีประเภทต่าง ๆ ยกตัวอย่างเช่น กรณีเครื่องใช้ไฟฟ้าอัจฉริยะส่งข้อมูลระหว่างกันเองในระบบหรือส่งข้อมูลให้ผู้ให้รายบริการอื่น เพื่อวัตถุประสงค์ในการอำนวยความสะดวกให้แก่ผู้ใช้บริการ ซึ่งก็คือเจ้าของข้อมูลส่วนบุคคล (เช่น กรณี ตู้เย็นอัจฉริยะ ส่งคำสั่งซื้อของไปยังร้านซุปเปอร์มาเก็ต เมื่อตัวเซ็นเซอร์จับได้ว่าของในตู้เย็นมีปริมาณลดลงหรือหมดไป)[18]

3. หลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายของสหภาพยุโรปและกฎหมายไทย

3.1 กฎหมายคุ้มครองข้อมูลส่วนบุคคลแห่งสหภาพยุโรป (General Data Protection Regulation)

General Data Protection Regulation หรือ GDPR เป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่บังคับใช้ทั่วทั้งสหภาพยุโรปตั้งแต่วันที่ 25 พฤษภาคม พ.ศ. 2560[19] โดยกำหนดหลักเกณฑ์ต่าง ๆ เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล เพื่อทำให้การคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล

---

[16] Ilja Braun, “High-Risk Citizens,” retrieved on January 28, 2020, from https://algorithmwatch.org/en/story/high-risk-citizens.

[17] Netherlands Committee of Jurists for Human Rights, “Rights Groups Sue Dutch State for Profiling Citizens,” retrieved on January 28, 2020, from https://www.liberties.eu/en/news/ngos-start-proceedings-against-dutch-government-over-syri/14329.

[18] Gaurav Sarin, “Developing Smart Cities Using Internet of Things: An Empirical Study,” SSRN Electronic Journal, (May 2016).

[19] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).

เป็นไปในมาตรฐานเดียวกันในทุกประเทศสมาชิก ซึ่งสิทธินี้เป็นสิทธิขั้นพื้นฐานที่ได้รับการรับรองและได้รับความคุ้มครองตามมาตรา 8 ของอนุสัญญายุโรปว่าด้วยสิทธิมนุษยชน (European Convention on Human Rights (ECHR)) และมาตรา 8 ของกฎบัตรสิทธิขั้นพื้นฐานของสภายุโรป the Charter of Fundamental Rights of the European Union

GDPR ได้รับการยอมรับว่าเป็นกฎหมายที่ค่อนข้างมีความเข้มงวด โดยกำหนดให้การประมวลผลข้อมูลส่วนบุคคลต้องเป็นตามหลักกฎหมาย เป็นธรรมและมีความโปร่งใส[20] และมีวัตถุประสงค์เป็นไปตามที่กฎหมายกำหนดไว้เท่านั้น[21] โดย GDPR จะบังคับใช้กับการประมวลผลข้อมูลส่วนบุคคล ในกรณีที่

1. ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ในสหภาพยุโรป ไม่ว่าการประมวลผลข้อมูลส่วนบุคคลนั้นได้กระทำในหรือนอกสหภาพยุโรปก็ตาม;[22]

2. ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่นอกสหภาพยุโรป GDPR ใช้บังคับแก่การประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในสหภาพยุโรป เมื่อกิจกรรมในการประมวลผลข้อมูลนั้นเกี่ยวกับ การเสนอสินค้าหรือบริการให้แก่เจ้าของ (a)ข้อมูลส่วนบุคคลซึ่งอยู่ในสหภาพยุโรป โดยไม่คำนึงว่าจะมีการชำระเงินหรือไม่ การเฝ้าติดตามพฤติกรรมของเจ้าของ (b) ;ข้อมูลส่วนบุคคลที่เกิดขึ้นในสหภาพยุโรป[23]

ทั้งนี้ เพื่อทำให้เกิดความเข้าใจที่ชัดเจน GPDR กำหนดคำนิยามของของกิจกรรมที่อยู่ภายใต้บังคับ ซึ่งก็คือการประมวลข้อมูลไว้ว่า หมายถึง “การกระทำใด ๆ ต่อข้อมูลส่วนบุคคล ไม่ว่าจะด้วยวิธีการโดยอัตโนมัติ หรือไม่ก็ตาม เช่น การรวบรวม การบันทึก การจัดระบบ การวางโครงสร้าง การเก็บ การปรับปรุง การเปลี่ยนแปลง การกู้คืน การจัดตำแหน่ง การผสมรวม การใช้ การเปิดเผยโดยการโอน การจ่ายแจก หรือกระทำการอื่นใดที่ทำให้ข้อมูลมีการแพร่หลาย การรวบรวม การจำกัด การลบ หรือการทำลาย”[24] และได้กำหนดคำนิยามของข้อมูลที่จะได้รับความคุ้มครองโดย GDPR ซึ่งก็คือ ‘ข้อมูลส่วนบุคคล’ ไว้ว่า หมายถึง “ข้อมูลที่สามารถระบุตัวบุคคลได้ไม่ว่าโดยทางตรงหรือทางอ้อม ยกตัวอย่างเช่น ชื่อ นามสกุล เลขประจำตัวประชาชน ข้อมูลที่แสดงถึงสถานที่ตั้ง หรือข้อมูลใด ๆ ที่แสดงถึงลักษณะทางกายภาพ ทางชีวภาพ ทางกรรมพันธุ์ ทางจิตใจ ทางเศรษฐกิจ ทางวัฒนธรรม หรืออัตลักษณ์ทางสังคมของบุคคลดังกล่าว”[25]

นอกจากนั้น เพื่อให้การกำหนดหน้าที่ในการปฏิบัติตามหลักเกณฑ์ของกฎหมายและการกำหนดความรับผิดของผู้ที่เกี่ยวข้องกับการประมวลผลข้อมูลนั้นมีความชัดเจน GDPR กำหนดสถานะของผู้ที่เกี่ยวข้องกับการประมวลผลข้อมูลไว้ 2 สถานะ ดังนี้ (1) ผู้ควบคุมข้อมูล (data controller) ซึ่งเป็นผู้กำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูล ;[26] และ (2) ผู้ประมวลผลข้อมูล (data processor) ซึ่งเป็นผู้ประมวลผลตามคำสั่งของผู้ควบคุมข้อมูลดังกล่าว[27]

GDPR กำหนดให้กับผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลมีหน้าที่ในการปฏิบัติตามหลักเกณฑ์ต่าง ๆ แตกต่างกันไปเพื่อให้เหมาะสมกับลักษณะในการถือครองข้อมูลส่วนบุคคล โดยมีวัตถุประสงค์หลักเพื่อสนับสนุนอำนาจในการตัดสินใจ การควบคุมดูแลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของเจ้าของข้อมูล และในขณะเดียวกันก็เป็นการคุ้มครองความปลอดภัยของข้อมูลส่วนบุคคลด้วย

[20] GDPR, Article 5 (1) (a).
[21] GDPR, Article 5 (1) (b).
[22] GDPR, Article 3 (1).
[23] GDPR, Article 3 (2).
[24] GDPR, Article 4 (2).
[25] GDPR, Article 4 (1).
[26] GDPR, Article 4 (7).
[27] GDPR, Article 4 (8).

ตัวอย่างหน้าที่ของผู้ควบคุมข้อมูล[28] คือ ใช้มาตรการทางเทคนิค และมาตรการขององค์กรที่เหมาะสมเพื่อให้สามารถเห็นได้ว่า การประมวลผลข้อมูลส่วนบุคคลนั้นเป็นไปตามหลักเกณฑ์ของ GDPR โดยจะต้องกำหนดให้มีการประมวลผลเฉพาะข้อมูลส่วนบุคคลที่จำเป็นตามวัตถุประสงค์ที่เฉพาะเจาะจง รวมทั้งเลือกผู้ประมวลผลข้อมูลที่แสดงให้เห็นได้ว่า มีมาตรการทางเทคนิค และมาตรการขององค์กรที่เหมาะสมเท่านั้น ผู้ควบคุมข้อมูลที่หน้าที่ดำเนินการตามคำร้องขอใช้สิทธิต่าง ๆ ของเจ้าของข้อมูลส่วนบุคคล อาทิเช่น (1) สิทธิที่จะร้องขอให้ผู้ควบคุมข้อมูลแก้ไขข้อมูลส่วนบุคคลของตนให้ถูกต้องโดยไม่ชักช้า[29] (2) สิทธิที่จะคัดค้านการประมวลผลข้อมูลส่วนบุคคลของตน[30]

ตัวอย่างหน้าที่ของผู้ประมวลผลข้อมูล[31] คือ ประมวลผลข้อมูลส่วนบุคคลโดยใช้มาตรการทางเทคนิคและมาตรการขององค์กรที่เหมาะสม และผู้ประมวลผลข้อมูลจะต้องได้รับอนุญาตจากผู้ควบคุมข้อมูลเป็นลายลักษณ์อักษรก่อนการจ้างช่วงผู้ประมวลผลข้อมูลได้ ทั้งนี้การประมวลผลข้อมูลส่วนบุคคลต้องอยู่ภายใต้สัญญาที่มีผลผูกพันทางกฎหมายระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล ระบุถึงสาระสำคัญ ระยะเวลา บริบท และวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล ประเภทของข้อมูลส่วนบุคคล กลุ่มของข้อมูลส่วนบุคคล สิทธิและหน้าที่ของผู้ควบคุมข้อมูล

GDPRกำหนดหลักเกณฑ์เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลซึ่งถือเป็นหลักการที่เป็นหัวใจหลักสำคัญของกฎหมายคุ้มครองข้อมูลส่วนบุคคล ไว้ว่า ข้อมูลส่วนบุคคลจะต้องได้รับการประมวลผล ในลักษณะที่ชอบด้วยกฎหมาย (lawfulness) ยุติธรรม (fairness) และมีความโปร่งใส (transparency)[32] ซึ่ง GDPR กำหนดลักษณะของการประมวลผลที่ชอบด้วยกฎหมายไว้ว่าจะต้องเป็นการประมวลผลที่เป็นไปตาม ฐานทางกฎหมาย(legal basis) อย่างหนึ่งอย่างใด ดังต่อไปนี้[33] (1) เจ้าของข้อมูลให้ความยินยอมสำหรับการประมวลผลข้อมูลส่วนบุคคลของตนเพื่อวัตถุประสงค์เฉพาะเจาะจงประการเดียวหรือหลายประการ (ฐานความยินยอม) ; (2) การประมวลผลมีความจำเป็น เพื่อปฏิบัติตามสัญญาที่เจ้าของข้อมูลเป็นคู่สัญญา หรือเพื่อปฏิบัติตามคำร้องขอของเจ้าของข้อมูลก่อนเข้าทำสัญญา (ฐานสัญญา) ; (3) การประมวลผลมีความจำเป็นเพื่อปฏิบัติหน้าที่ตามกฎหมายของผู้ควบคุมข้อมูล (ฐานหน้าที่ตามกฎหมาย) ; (4) การประมวลผลมีความจำเป็นเพื่อปกป้องประโยชน์ที่สำคัญของเจ้าของข้อมูล (ฐานประโยชน์สำคัญ) ; (5) การประมวลผลมีความจำเป็นต่อการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูล (ฐานภารกิจรัฐ) ; (6) การประมวลผลมีความจำเป็นเพื่อประโยชน์อันชอบธรรมของผู้ควบคุมข้อมูล (ฐานประโยชน์อันชอบธรรม) แต่อย่างไรก็ตาม หากข้อมูลนั้นเป็นข้อมูลอ่อนไหว (sensitive data)[34] GDPR กำหนดฐานทางกฎหมายในการประมวลผลข้อมูลที่แตกต่างไปเล็กน้อย ทั้งนี้เพื่อเพิ่มระดับในการคุ้มครองความปลอดภัยของข้อมูล อาทิเช่น เมื่อได้รับความยินยอมจากเจ้าของข้อมูล, การประมวลผลมีความจำเป็นเพื่อประโยชน์สาธารณะทั่วไป และการประมวลผลมีความจำเป็น เพื่อการจัดทำงานวิจัยทางวิทยาศาสตร์และ ทางประวัติศาสตร์

กรณีที่การประมวลข้อมูลส่วนบุคคลนั้นเกิดขึ้นจากฐานความยินยอมของเจ้าของข้อมูลส่วนบุคคล GDPR กำหนดลักษณะและเงื่อนไขของความยินยอมที่จะทำให้การประมวลข้อมูลส่วนบุคคลนั้นชอบด้วยกฎหมายไว้ ดังนี้[35] (1) เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมอย่างอิสรเสรี (Freely given) ; (2) มีวัตถุประสงค์ที่เฉพาะเจาะจงในการขอความยินยอม (Specific) ; (3) มีการแจ้งเกี่ยวกับการประมวลผลข้อมูลให้เจ้าของข้อมูลส่วนบุคคลทราบ

[28] GDPR, Article 24 – 25.

[29] GDPR, Article 16.

[30] GDPR, Article 21.

[31] GDPR, Article 28.

[32] GDPR, Article 5.

[33] GDPR, Article 6.

[34] GDPR, Article 9 กำหนดไว้ว่า ข้อมูลอ่อนไหว คือ ข้อมูลที่เปิดเผย เชื้อชาติ เผ่าพันธุ์ ความเห็นทางการเมือง การนับถือศาสนา ความเชื่อ สมาชิกสหภาพการค้า ข้อมูลทางพันธุกรรม ข้อมูลทางชีวภาพ ข้อมูลเกี่ยวกับสุขภาพ ข้อมูลที่แสดงให้เห็นพฤติกรรมทางเพศ รสนิยมทางเพศ เป็นต้น

[35] GDPR, Article 4 (11), 7.

(Informed) ; (4) เจ้าของข้อมูลต้องแสดงความยินยอมอย่างไม่กำกวม (Unambiguous) ; (5) เจ้าของข้อมูลมีสิทธิที่จะถอนความยินยอมได้ตลอดเวลา โดยก่อนการให้ความยินยอม เจ้าของข้อมูลจะต้องได้รับแจ้งถึงรายละเอียดเกี่ยวกับการถอนความยินยอมด้วย โดยที่การถอนความยินยอมนี้จะต้องกระทำได้โดยง่าย[36] นอกจากนั้น GDPR ยังกำหนดไว้ว่าผู้ควบคุมข้อมูลจะต้องสามารถแสดงให้เห็นได้ว่า เจ้าของข้อมูลส่วนส่วนบุคคลให้ความยินยอมต่อการประมวลผลข้อมูลส่วนบุคคลนั้นแล้ว[37]

ในกรณีที่ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลฝ่าฝืนไม่ปฏิบัติตามหน้าที่ GDPR กำหนดบทลงโทษไว้ว่าอาจจะต้องจ่ายค่าปรับในอัตราสูงสุดไม่เกิน 20 ล้านยูโร หรือไม่เกิน 4% ของมูลค่าการซื้อขายรวมทั่วโลกของปีงบการเงินก่อน แล้วแต่จำนวนเงินใดจะสูงกว่า[38]และหากเกิดความเสียหายต่อเจ้าของข้อมูล ควบคุมข้อมูล และผู้ประมวลผลก็จะต้องรับผิดชดใช้ค่าเสียหายที่เกิดขึ้นจริงให้กับเจ้าของข้อมูลอย่างเต็มจำนวน[39]

3.2 กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย

หลักเกณฑ์การคุ้มครองข้อมูลของไทยปรากฏอยู่ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งจะมีผลบังคับใช้อย่างเต็มรูปแบบในวันที่ 27 พฤษภาคม 2563 โดยมีเนื้อหาสาระที่สอดคล้องกับ GDPR ของสหภาพยุโรป เนื่องจาก GDPR ถูกนำมาเป็นกฎหมายแม่แบบในการยกร่างกฎหมายฉบับนี้วัตถุประสงค์ของกฎหมายฉบับนี้ก็เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพและเพื่อให้มีมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคลที่มีประสิทธิภาพ โดยจะบังคับใช้กับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในกรณีดังต่อไปนี้

1. ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่าการเก็บรวบรวม ใช้ หรือเปิดเผยนั้น ได้กระทำในหรือนอกราชอาณาจักรก็ตาม

2. ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่นอกราชอาณาจักร พระราชบัญญัตินี้ใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล ซึ่งอยู่ในราชอาณาจักรโดยการดำเนินกิจกรรมเป็นกิจกรรม ดังต่อไปนี้ (1) การเสนอสินค้าหรือบริการให้แก่เจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร (2) การเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักร[40]

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กำหนดคำนิยามของ “ผู้ควบคุมข้อมูลส่วนบุคคล”และ “ผู้ประมวลผลข้อมูลส่วนบุคคล” ไว้เหมือนกับที่ GDPR กำหนดไว้[41] แต่กำหนดคำนิยามของคำว่า “ข้อมูลส่วนบุคคล” ไว้แตกต่างกันกับคำนิยามที่กำหนดไว้โดย GDPR ในส่วนที่ข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ[42] ในส่วนหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลนั้น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดไว้ค่อนข้างคล้ายคลึงกันกับที่ GDPR กำหนดไว้ ซึ่งสามารถดูรายละเอียดได้ตั้งแต่ มาตรา 19 - 40

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดหลักเกณฑ์การเก็บรวบรวม ใช้ หรือเปิดเผยมูลบุคคลส่วนบุคคล (ฐานทางกฎหมาย) ไว้ว่าให้ทำได้เท่าที่จำเป็น ภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายเท่านั้น โดยที่เจ้าของข้อมูลต้องให้ความยินยอมโดยชัดแจ้งไว้ก่อนหรือในขณะนั้น[43] หรือเป็นการดำเนินการภายใต้ฐานทาง

[36] GDPR, Article 7 (3).

[37] GDPR, Article 7 (1).

[38] GDPR, Article 83.

[39] GDPR, Article 82.

[40] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 5.

[41] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 6.

[42] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 6.

[43] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 19 - 22.

กฎหมายอื่น ๆ ที่เหมาะสม[44] ดังนี้ (1) เพื่อจัดทำเอกสารทางประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ ; (2) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกายหรือสุขภาพของบุคคล ; (3) จำเป็นเพื่อปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา หรือดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญา ; (4) จำเป็นเพื่อปฏิบัติหน้าที่ในการดำเนินภารกิจ เพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล ; (5) จำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของเจ้าของข้อมูลส่วนบุคคล ; (6) เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล แต่ในกรณีที่เป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลที่มีความอ่อนไหว พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้การกระทำดังกล่าวสามารถทำได้หากได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล หรือเป็นการดำเนินการภายใต้ฐานทางกฎหมายอื่น ๆ ที่มีความแตกต่างบางประการกับกรณีของข้อมูลส่วนบุคคล ยกตัวอย่างเช่น เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือเป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย[45]

หลักเกณฑ์เกี่ยวกับการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ถูกกำหนดไว้ในมาตรา 19 ซึ่งมีสาระสำคัญที่คล้ายคลึงกับหลักเกณฑ์ที่ GDPR กำหนดไว้ กล่าวคือ (1) การขอความยินยอมต้องทำโดยชัดแจ้งเป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เว้นแต่โดยสภาพไม่อาจขอได้ ; (2) การแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลควรใช้ภาษาที่อ่านง่าย และไม่เป็นการหลอกลวง หรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ ; (3) ต้องเป็นการให้ความยินยอมโดยอิสระของเจ้าของข้อมูลส่วนบุคคล ; และ (4) เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเสียเมื่อใดก็ได้โดยจะต้องถอนความยินยอมได้ง่ายเช่นเดียวกับการให้ความยินยอม[46]

บทกำหนดความรับผิดและโทษสำหรับผู้ที่ฝ่าฝืนไม่ปฏิบัติตามและทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลแบ่งออกเป็น 3 กรณี ได้แก่ (1) ความรับผิดทางแพ่ง เป็นการชดใช้ค่าเสียหายที่เกิดขึ้นจริงแก่เจ้าของข้อมูลและมีค่าเสียหายเชิงลงโทษตามคำสั่งศาล[47] ; (2) ความรับผิดทางอาญา มีโทษจำคุก ไม่เกิน 1 ปี หรือ ปรับไม่เกิน 1 ล้านบาท หรือทั้งจำทั้งปรับ และเป็นความผิดอันยอมความได้ แต่กรรมการหรือผู้จัดการของนิติบุคคลอาจต้องรับโทษด้วย[48]; (3) ความรับผิดทางปกครอง มีโทษปรับสูงสุดไม่เกิน 5 ล้านบาท ศาลมีอำนาจในการยึดหรืออายัดทรัพย์สินเพื่อนำออกขายทอดตลาด เพื่อชำระค่าปรับทางปกครอง[49]

4. บทวิเคราะห์ความท้าทายทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลในบริบทเมืองอัจฉริยะ

จากหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลที่กำหนดไว้ใน GDPR และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้น จะเห็นได้ว่าหน่วยงานภาครัฐและภาคเอกชนที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ในบริบทของเมืองอัจฉริยะมีหน้าที่ต้องปฏิบัติตามหลักเกณฑ์ที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดไว้ แต่อย่างไรก็ตาม จากการศึกษาวิจัยพบว่าลักษณะการเคลื่อนไหวของข้อมูลส่วนบุคคลในบริบทของเมืองอัจฉริยะทำให้เกิดความยากลำบากในการปฏิบัติตามหลักเกณฑ์ดังกล่าวอยู่หลายประการ ซึ่งในกรณีนี้ย่อมส่งผลกระทบโดยตรงต่อความปลอดภัยของข้อมูลส่วนบุคคลในบริบทของเมืองอัจฉริยะค่อนข้างมาก

ดังจะเห็นได้ว่า รูปแบบการทำงานของเทคโนโลยี Internet of Things ส่งผลให้ข้อมูลส่วนบุคคลถูกนำเข้าสู่ระบบการทำงานเชิงอัตโนมัติ ข้อมูลส่วนบุคคลจะได้รับการแลกเปลี่ยนกันเองระหว่างเครื่องมือเครื่องใช้อิเล็กทรอนิกส์ต่าง ๆ เพื่อที่จะสามารถให้บริการได้ตรงกับความต้องการของผู้ใช้บริการให้ได้มากที่สุด โดยไม่เสียค่าใช้จ่ายที่สูง

---

[44] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 24.

[45] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 26.

[46] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 19.

[47] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 77 – 78.

[48] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 79.

[49] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 82 – 89.

จนเกินไป ทำให้ผู้ใช้ทุกคนสามารถเข้าถึงบริการต่าง ๆ ได้อย่างสะดวกสบาย แต่อย่างไรก็ตาม ระดับของการรักษาความปลอดภัยในระบบของ Internet of Things นั้น ถูกมองว่าอยู่ในระดับที่ค่อนข้างต่ำ เครื่องมือเครื่องใช้อิเล็กทรอนิกส์ต่าง ๆ ที่ใช้ในการเชื่อมโยงกันผ่านระบบอินเทอร์เน็ตส่วนมากจะถูกสร้างขึ้นมาโดยไม่มีระบบการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่ดีนัก เพราะมุ่งเน้นในเรื่องของราคาที่ย่อมเยา และไม่มีระบบปฏิบัติการอิสระของตน เพื่อเอื้อให้มีการแชร์ข้อมูลระหว่างกันได้อย่างไร้อุปสรรค ในส่วนของการเชื่อมต่อมักจะอยู่บนระบบ Wireless Communications Protocols or APIs ซึ่งมีขีดจำกัดในเรื่องของระดับ ในการรักษาความปลอดภัยในกรณีการส่งต่อข้อมูลระหว่างกัน[50] ผลสำรวจจากคณะกรรมาธิการสหภาพยุโรป (European Commission) แสดงให้เห็นอย่างชัดเจนว่า การทำงานของเทคโนโลยี Internet of Things อันเป็นกลไกหลักของการทำงานของเมืองอัจฉริยะนั้นทำให้ข้อมูลมีการแบ่งปันกันเองอัตโนมัติในระบบซึ่งก่อให้เกิดความเสี่ยงต่อความปลอดภัยของข้อมูลส่วนบุคคล ดังนั้นจึงทำให้ 81% ของประชาชนกลุ่มเป้าหมายมีความกังวลว่า ข้อมูลส่วนบุคคลของตนอาจจะได้รับการประมวลผลในลักษณะที่มิชอบด้วยกฎหมาย[51]

นอกจากนั้น การทำงานของเทคโนโลยี Machine Learning ซึ่งจะมีการนำข้อมูลส่วนบุคคลเข้าสู่ระบบการประมวลผล เพื่อการคาดเดาผลลัพธ์โดยใช้ Algorithm นั้น จะส่งผลให้มีการสร้างข้อมูลชุดใหม่ ๆ ซึ่งจะที่มีการส่งต่อไปยังหลากหลายหน่วยงานที่เกี่ยวข้องเพื่อให้บรรลุวัตถุประสงค์ในการให้บริการให้มีความสอดคล้องกับความต้องการของประชาชน ซึ่งเป็นเจ้าของข้อมูลมากที่สุด แต่อย่างไรก็ตามกรณีนี้อาจก่อให้ความเสี่ยงในการที่จะมีการละเมิดข้อมูลส่วนบุคคลได้[52] และด้วยเหตุที่ข้อมูลส่วนบุคคลทั้งหมดจะได้รับการเก็บรวบรวมอัตโนมัติเข้าสู่ฐานข้อมูลขนาดใหญ่ที่เรียกว่า Big Data ซึ่งค่อนข้างมีความซับซ้อนและหลากหลาย มีการเปลี่ยนแปลงอย่างรวดเร็ว และสามารถเข้าถึงได้โดยหลากหลายหน่วยงาน จึงให้เกิดความเสี่ยงต่อความปลอดภัยของข้อมูลส่วนบุคคลที่อยู่ในระบบทั้งหมด[53]

และในขณะเดียวกันข้อมูลส่วนบุคคลทั้งหมดเหล่านี้ได้รับการประมวลผลอยู่บนโครงสร้างของ Cloud Computing ซึ่งเป็นแหล่งให้บริการทรัพยากรทางคอมพิวเตอร์ที่มีความหลากหลายและมีขนาดใหญ่ โครงสร้างของ Cloud Computing เกิดขึ้นจากการรวมกันของทรัพยากรหลายประเภท และมีโครงสร้างเป็นชั้น (layer) กล่าวคือโครงสร้างของทรัพยากรประเภทหนึ่งสามารถตั้งอยู่บนโครงสร้างของทรัพยากรประเภทอื่นได้ ลักษณะของโครงสร้างเช่นนี้ ทำให้ข้อมูลส่วนบุคคลที่อยู่ในระบบโครงสร้างของ Cloud Computing มีความกระจัดกระจาย นำไปสู่ความเป็นไปได้ในการเกิดขึ้นของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลโดยมิชอบด้วยกฎหมายโดยบุคคลหรือหน่วยงานที่ปราศจากอำนาจ[54]

---

[50] HP Fortify, “Report Internet of Things Research Study (2014),” Retrieved on January 22, 2020, from https://www8.hp.com/us/en/hp-news/press-release.html?id=1744676.

[51] European Commission, “Conclusions of the Internet of Things public consultation,” Retrieved on January 20, 2020, from http://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation.

[52] OVIC, “Artificial intelligence and privacy Issues paper,” Retrieved on January 22, 2020, from https://ovic.vic.gov.au/wp-content/uploads/2018/08/AI-Issues-Paper-V1.1.pdf

[53] Ira Rubinstein, “Big Data: The End of Privacy or a New Beginning?,” International Data Privacy Law (2013 Forthcoming), NYU School of Law, Public Law Research Paper No.12 - 56. Available at SSRN : https://ssrn.com/abstract=2157659

[54] Rajasi Gore, “Privacy Breach: A Concern of Cloud Integrated IoT Framework for Smart City,” in Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT), held at Malaviya National Institute of Technology, Jaipur (India), March 26 - 27, 2018.

จากสถานการณ์ดังกล่าวข้างต้น จึงอาจสรุปได้ว่าลักษณะและรูปแบบของการประมวลผลข้อมูลส่วนบุคคลในบริบทของเมืองอัจฉริยะทำให้เกิดความท้าทายทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคล ซึ่งงานวิจัยนี้มุ่งศึกษาประเด็นความท้าทายดังกล่าว โดยสามารถแบ่งพิจารณาออกได้เป็น 2 ประเด็น ดังต่อไปนี้

4.1 ประเด็นเกี่ยวกับการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

วัตถุประสงค์ที่สำคัญประการหนึ่งของกฎหมายคุ้มครองข้อมูลส่วนบุคคล คือ การให้อำนาจแก่เจ้าของข้อมูลส่วนบุคคลในการควบคุมข้อมูลส่วนบุคคลของตนเองได้ ซึ่งฐานความยินยอมถูกมองว่าเป็นเครื่องมือที่สำคัญของเจ้าของข้อมูลที่จะใช้ในการควบคุม ดูแล และคงไว้ซึ่งอำนาจของเจ้าของข้อมูลที่มีต่อข้อมูลส่วนบุคคลของตนเอง และในกรณีนี้เพื่อให้เจ้าของข้อมูลสามารถพิจารณาตัดสินใจได้อย่างถี่ถ้วนว่าจะให้ความยินยอมแก่หน่วยงานต่าง ๆ ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลของตนหรือไม่ และเพื่อให้เป็นไปตามหลักความโปร่งใสอันเป็นหลักการสำคัญของกฎหมายคุ้มครองข้อมูลส่วนบุคคล กฎหมายกำหนดให้ผู้ควบคุมข้อมูล เมื่อจะมีการขอความยินยอมจากเจ้าของข้อมูลมีหน้าที่ต้องแจ้งให้เจ้าของข้อมูลทราบเกี่ยวกับรายละเอียดต่าง ๆ ดังต่อไปนี้[55] อาทิ เช่น วัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล, ประเภทของข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวม ใช้ หรือเปิดเผย, ระยะเวลาในการเก็บรวบรวมข้อมูลส่วนบุคคล, ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจถูกเปิดเผย, ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล ผู้แทน หรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในเรื่องของสถานที่ติดต่อ วิธีการติดต่อ รวมทั้งแจ้งสิทธิต่าง ๆ ของเจ้าของข้อมูลที่กฎหมายกำหนดไว้[56] (อาทิ เช่น สิทธิในการถอนความยินยอม, สิทธิในการขอเข้าถึงและขอเข้ารับสำเนาข้อมูลส่วนบุคคลเกี่ยวกับตน)

แต่อย่างไรก็ตาม ความยินยอมของเจ้าของข้อมูลมิใช่ฐานทางกฎหมายเพียงประการเดียวที่สามารถทำให้หน่วยงานภาคเอกชนสามารถเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้โดยชอบด้วยกฎหมาย นักวิชาการทางกฎหมายคุ้มครองข้อมูลส่วนบุคคลได้ให้ความเห็นว่า ในกรณีที่การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเป็นเรื่องยาก และต้องใช้ค่าใช้จ่ายที่ค่อนข้างสูงในการที่จะได้มา หน่วยงานอาจพิจารณาเลือกใช้ฐานทางกฎหมายอื่น ๆ เพื่อให้สามารถเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้โดยชอบด้วยกฎหมาย และฐานทางกฎหมายที่มักถูกนำมาใช้ คือ ฐานในเรื่องประโยชน์อันชอบธรรมของผู้ควบคุมข้อมูลส่วนบุคคล[57] แต่อย่างไรก็ตามฐานทางกฎหมายนี้ก็ไม่สามารถนำไปใช้ได้ในทุกบริบทจะต้องพิจารณาก่อนว่าหน่วยงานดังกล่าวมีภารกิจอย่างไร หากการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลดังกล่าวเป็นกระทำตามภารกิจของหน่วยงาน ซึ่งเป็นการกระทำที่จำเป็นเพื่อประโยชน์อันชอบธรรมของหน่วยงานในฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลแล้ว และการกระทำดังกล่าวมีความสำคัญมากกว่าการคุ้มครองสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล หน่วยงานดังกล่าวก็สามารถเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลดังกล่าวได้โดยชอบด้วยกฎหมายโดยไม่ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล แต่หากลักษณะของการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลไม่ได้เป็นไปตามเงื่อนไขที่กฎหมายกำหนดแล้ว ฐานความยินยอมก็จะเข้ามามีบทบาทสำคัญ

นอกจากนั้น ในกรณีนี้ที่หากข้อมูลดังกล่าวเป็นข้อมูลที่มีลักษณะอ่อนไหว (sensitive data) อาทิ เช่น เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม และข้อมูลชีวภาพแล้ว ฐานความยินยอมยังคงเป็นฐานทางกฎหมายที่ได้รับความสนใจ และมักถูกนำไปใช้โดยหน่วยงานภาคเอกชนต่าง ๆ เมื่อจะต้องมีการการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลประเภทดังกล่าว ทั้งนี้ เนื่องจากกฎหมายคุ้มครองส่วนบุคคลจะให้คุ้มครองข้อมูลประเภทนี้ในระดับที่ค่อนข้างสูงไปกว่าข้อมูลส่วนบุคคลทั่วไป เพราะข้อมูลประเภทนี้เป็นเรื่องส่วนตัวของเจ้าของข้อมูลส่วนบุคคลโดยแท้ มีความละเอียดอ่อน และอาจถูกนำไปใช้เป็นสาเหตุในการ

[55] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 23.

[56] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 30 - 42.

[57] Lilian Edwards, “Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective,” European Data Protection Law Review. 2: 1. (2016).

เลือกปฏิบัติซึ่งจะส่งผลกระทบต่อเจ้าของข้อมูลค่อนข้างมาก กฎหมายคุ้มครองข้อมูลส่วนบุคคลจึงกำหนดฐานทางกฎหมายสำหรับการประมวลผลข้อมูลประเภทนี้ในลักษณะที่ค่อนข้างจำกัด[58] และเป็นไปเพื่อบรรลุวัตถุประสงค์สำหรับกิจกรรมที่มีความสำคัญ เพื่อประโยชน์สาธารณะเท่านั้น ดังนั้น หากหน่วยงานภาคเอกชนทั่วไปต้องการที่จะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลประเภทนี้ เพื่อบรรลุวัตถุประสงค์อื่นๆนอกเหนือจากวัตถุประสงค์ดังกล่าวแล้ว ฐานความยินยอมก็จะเข้ามามีบทบาทสำคัญต่อการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลอ่อนไหวของหน่วยงานภาคเอกชน

ดังนั้น หากหน่วยงานภาคเอกชนต้องการที่จะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลหรือข้อมูลอ่อนไหวในบริบทการทำงานของเมืองอัจฉริยะโดยใช้ฐานความยินยอมแล้ว ประเด็นต่อไปที่ต้องพิจารณาคือ จะมีปัญหาและอุปสรรคใดบ้างที่จะทำให้หน่วยงานไม่สามารถขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลได้ ในการที่จะตอบคำถามนี้ได้ ก็จะต้องพิจารณาถึงรูปแบบและลักษณะของการได้รับข้อมูลส่วนบุคคลของหน่วยงานภาคเอกชนต่าง ๆ ซึ่งเมื่อพิจารณากิจกรรมทั้งหมดที่เกิดขึ้นในบริบทของเมืองอัจฉริยะแล้ว พบว่าหน่วยงานภาคเอกชนในฐานะผู้ให้บริการจะได้รับข้อมูลส่วนบุคคลของประชาชนในฐานะเป็นผู้ใช้บริการได้ใน 2 กรณีดังต่อไปนี้

(1) ข้อมูลที่ได้รับจากเจ้าของข้อมูลส่วนบุคคลโดยตรง

เมื่อเจ้าของข้อมูลส่วนบุคคลซื้อสินค้าหรือเข้าใช้บริการต่าง ๆ จากหน่วยงานภาคเอกชนนั้น ๆ การเก็บรวบรวมข้อมูลในส่วนนี้จึงสามารถเก็บได้โดยตรงจากเจ้าของข้อมูล อันเกิดขึ้นจากการแสดงความประสงค์ของเจ้าของข้อมูลส่วนบุคคลเอง ยกตัวอย่าง เช่น การที่เจ้าของข้อมูลซื้อเสื้อผ้าจากเว็บไซต์ ซึ่งเป็นแบรนด์ของผู้ขายเอง อาทิ เช่น www.zara.co.th หรือติดต่อขอใช้บริการเครือข่ายอินเตอร์จากผู้ให้บริการที่เป็นเจ้าของเครือข่ายรายต่าง ๆ อาทิ เช่น www.ais.co.th ในกรณีนี้การที่หน่วยงานจะขอความยินยอมจากเจ้าของข้อมูล เพื่อเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจึงไม่น่าจะเป็นเรื่องยาก เพราะหน่วยงานมีโอกาสติดต่อเจ้าข้อมูลได้เองโดยตรง จึงสามารถแจ้งรายละเอียดต่าง ๆ ตามที่กฎหมายกำหนดไว้ได้อย่างครบถ้วน ซึ่งทำให้เจ้าของข้อมูลจะสามารถพิจารณาตัดสินใจได้อย่างถี่ถ้วนว่าจะให้ความยินยอมหรือไม่ และหากเจ้าของข้อมูลให้ความยินยอม ความความยินยอมนี้ก็จะมีองค์ประกอบครบถ้วนตามที่กฎหมายกำหนดไว้ซึ่งจะเป็นฐานทางกฎหมายที่ทำให้หน่วยงานภาคเอกชนสามารถเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลได้โดยชอบด้วยกฎหมาย

แต่หากเป็นกรณีที่หน่วยงานภาคเอกชนทำหน้าที่ในการช่วยเหลือ สนับสนุนหน่วยงานภาครัฐ ในการให้บริการสาธารณะประเภทต่าง ๆ อาทิ เช่น กรณีหน่วยงานภาคเอกชนเป็นผู้ให้บริการพื้นที่จัดเก็บข้อมูลออนไลน์ ซึ่งได้รับข้อมูลส่วนบุคคลจากเจ้าของข้อมูลที่เป็นประชาชนเข้ามาลงทะเบียนรับบริการจากหน่วยงานของรัฐ ในกรณีนี้หากผู้ให้บริการรายนี้นำข้อมูลที่ได้รับมาไปใช้ เพื่อการนำเสนอสินค้า และบริการของตนเองไปยังเจ้าของข้อมูล ก็จะถือว่าเป็นการไม่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล เป็นการใช้ข้อมูลส่วนบุคคลที่มิชอบด้วยกฎหมาย ซึ่งในกรณีหากผู้ให้บริการรายนี้ต้องการใช้ข้อมูล ดังกล่าวก็จะต้องทำหนังสือขอความยินยอมส่งไปยังเจ้าของข้อมูลส่วนบุคคล แต่อย่างไรก็ตาม ในกรณีนี้เจ้าของข้อมูลอาจจะมีความสับสนถึงแหล่งที่มาและวิธีการในการได้มาซึ่งข้อมูลของผู้ให้บริการรายนี้ ซึ่งเมื่อพิจารณาดูแล้วจะเป็นกรณีของการใช้ข้อมูลโดยมิชอบด้วยกฎหมาย เพราะเป็นการนำเอาข้อมูลไปใช้นอกเหนือจากวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลไว้เมื่อตอนได้รับข้อมูล ดังนั้น การติดต่อไปยังเจ้าของข้อมูลโดยตรงเพื่อขอความยินยอมในการใช้ข้อมูลส่วนบุคคล เพื่อให้บรรลุวัตถุประสงค์ในการนำเสนอสินค้า และบริการของผู้ให้บริการ ซึ่งเจ้าของข้อมูลไม่เคยได้รับรู้มาก่อน จึงมีแนวโน้มสูงที่เจ้าของข้อมูลจะไม่ให้ความยินยอม[59]

---

[58] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 26

[59] A. Michael Froomkin, “Big Data : Destroyer of Informed Consent,” Yake Journal of Health Policy, Law, and Ethics. Forthcoming ; University of Miami Legal Studies Research Paper Forthcoming. (September 2019). from https://ssrn.com/abstract=3405482.

(2) ข้อมูลที่ได้รับจากการแบ่งปันข้อมูลระหว่างหน่วยงานเอกชน

หน่วยงานภาคเอกชนสามารถเก็บรวบรวมข้อมูลได้จากการแบ่งปันข้อมูลจากหน่วยงานภาคเอกชนอื่น ๆ ที่ได้รับข้อมูลมาโดยตรงจากเจ้าของข้อมูล (อาทิ เช่น ผู้ให้บริการเครือข่ายอินเทอร์เน็ตส่งข้อมูลให้แก่บริษัทที่ทำธุรกิจโรงแรม) ซึ่งถ้าหากการเปิดเผยข้อมูลของหน่วยงานเอกชนดังกล่าว เป็นการเปิดเผยที่ไม่ได้มีฐานกฎหมายรองรับ เจ้าของข้อมูลมิได้รับทราบถึงรายละเอียดของกิจกรรมนั้นมาก่อนใน (หากใช้ฐานสัญญา) และไม่ได้ให้ความยินยอมไว้ก่อน (หากใช้ฐานความยินยอม) และไม่ได้เป็นการกระทำที่เป็นไปเพื่อประโยชน์อันชอบธรรมของหน่วยงานผู้ที่แบ่งปันข้อมูลในฐานะผู้ควบคุมข้อมูลส่วนบุคคล (หากใช้ฐานเพื่อประโยชน์อันชอบธรรม) แล้ว การที่หน่วยงานภาคเอกชนที่ได้รับการแบ่งปันข้อมูล นำเอาข้อมูลไปใช้ก็ถือว่าเป็นการใช้ข้อมูลโดยมิชอบด้วยกฎหมาย ในกรณีนี้หากหน่วยงานที่ได้รับการแบ่งปันข้อมูลมาจะติดต่อขอความยินยอมโดยตรงจากเจ้าของข้อมูล ซึ่งในกรณีนี้กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้เปิดโอกาสให้ทำได้ มาตรา 25 ของพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดไว้ว่าผู้ควบข้อมูลสามารถเก็บรวบรวมข้อมูลจากแหล่งอื่นได้ หากได้แจ้งถึงการเก็บข้อมูลจากแหล่งอื่นให้เจ้าของข้อมูลทราบโดยไม่ชักช้า แต่ต้องไม่เกินสามสิบวันนับแต่วันที่เก็บรวบรวมและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

แต่อย่างไรก็ตาม เจ้าของข้อมูลส่วนบุคคลจะให้หรือไม่ให้ความยินยอมนั้นเป็นเรื่องที่ไม่แน่นอน ขึ้นอยู่กับว่าเจ้าของข้อมูลจะมีความเชื่อถือต่อหน่วยงานที่ขอความยินยอมมากน้อยเพียงใด รวมทั้งข้อเท็จจริงในเรื่องแหล่งที่มาของข้อมูลก็เป็นปัจจัยหลักที่จะส่งผลให้เจ้าของข้อมูลตัดสินใจให้ความยินยอมหรือไม่ นอกจากนั้น ในกรณีนี้ถือว่าหน่วยงานภาคเอกชนที่แบ่งปันข้อมูลกระทำการโดยปราศจากอำนาจ เป็นการฝ่าฝืนไม่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

หน่วยงานภาคเอกชนยังสามารถเข้าถึง เก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ในกรณีที่ข้อมูลมีการแบ่งปันกันเองในระบบการทำงานของเทคโนโลยีต่าง ๆ ที่ถูกนำมาใช้ในบริบทของเมืองอัจฉริยะ เพื่อเป็นการอำนวยความสะดวกให้ประชาชน ทำให้การเก็บรวบรวมข้อมูลส่วนหนึ่งของหน่วยงานภาคเอกชน อาจจะอยู่ในรูปแบบของการจัดเก็บจากระบบการทำงานอัตโนมัติ ยกตัวอย่าง เช่น การทำงานของระบบเครื่องใช้ไฟฟ้าอัจฉริยะ ซึ่งจะมีการส่งข้อมูลไปยังผู้ให้บริการประเภทอื่น ๆ ของการแลกเปลี่ยนกันเองในระบบ ในกรณีนี้มีความเป็นได้สูงที่จะทำให้ผู้ให้บริการที่ทำธุรกิจประเภทอื่น ๆ ซึ่งถือเป็นบุคคลที่สามสามารถเข้าถึงข้อมูลดังกล่าวได้ ซึ่งก็จะทำให้สามารถทราบถึงพฤติกรรมในการอุปโภคบริโภคของผู้ใช้บริการแต่ราย เพื่อจะได้สามารถผลิตสินค้าหรือบริการได้ตรงตามความต้องการของผู้ใช้บริการให้ได้มากที่สุด และอาจจะมีการนำเสนอสินค้าและบริการมายังเจ้าของข้อมูลส่วนบุคคลดังกล่าว[60]

โดยหากการเปิดเผยข้อมูลต่อบุคคลที่สามนี้ แม้เป็นการกระทำที่เกิดขึ้นโดยระบบอัตโนมัติเป็นการกระทำโดยปราศจากอำนาจ กล่าวคือ เจ้าของข้อมูลมิได้รับทราบถึงรายละเอียดของกิจกรรมนั้นมาก่อนใน (หากใช้ฐานสัญญา) และไม่ได้ให้ความยินยอมไว้ก่อน (หากใช้ฐานความยินยอม) และไม่ได้เป็นการกระทำที่เป็นไปเพื่อประโยชน์อันชอบธรรม หน่วยงานที่ดูแลระบบการทำงานของเครื่องใช้ไฟฟ้าอัจฉริยะดังกล่าว (หากใช้ฐานเพื่อประโยชน์อันชอบธรรม) ในกรณีนี้ก็จะถือว่าผู้ดูแลระบบเครื่องใช้ไฟฟ้าอัจฉริยะกระทำการอันเป็นการฝ่าฝืนหลักเกณฑ์ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ทำให้ข้อมูลถูกเปิดเผยต่อบุคคลที่สามโดยปราศจากอำนาจ[61]

กรณีนี้ หากผู้ให้บริการรายอื่น ๆ นำเอาข้อมูลที่ได้มาจากระบบอัตโนมัติไปใช้ ก็ถือเป็นการใช้ที่มิชอบด้วยกฎหมาย หากผู้ให้บริการรายนี้ต้องการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเพื่อที่ทำให้จะสามารถเก็บรวบรวมใช้ข้อมูลนั้นได้โดยชอบด้วยกฎหมายตามที่มาตรา 25 ของพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดไว้ กรณีอาจเกิดความยากลำบากต่อผู้ควบคุมข้อมูลส่วนบุคคลในการแจ้งแหล่งที่มาของ

---

[60] HP Fortify, “Report Internet of Things Research Study (2014),” Retrieved on January 22, 2020, from https://www8.hp.com/us/en/hp-news/press-release.html?id=1744676, p.5.

[61] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562, มาตรา 24 (3)(5).

ข้อมูล ซึ่งอาจจะไม่ทราบได้แน่ชัดว่ามาจากแหล่งใด นอกจากนั้นในกรณีที่ได้รับข้อมูลส่วนบุคคลมาบางส่วน โดยไม่มีข้อมูลเกี่ยวกับการติดต่อไว้ ในกรณีนี้การติดต่อไปยังเจ้าของข้อมูลส่วนบุคคลโดยตรงจึงเป็นเรื่องที่ค่อนข้างยาก ซึ่งอาจจะต้องเสียเวลา และค่าใช้จ่ายในการค้นหาข้อมูลต่าง ๆ เพิ่มเติม และการกระทำดังกล่าวอาจเป็นการได้มาโดยมิชอบด้วยกฎหมายซึ่งข้อมูลอีกชุดหนึ่ง ดังนั้น จึงอาจสรุปได้ว่าการติดต่อขอความยินยอมจากเจ้าของข้อมูลโดยตรงในกรณีนี้ จึงเป็นเรื่องที่ค่อนข้างยากและอาจจะไม่สามารถเกิดขึ้นได้เลย

จึงอาจกล่าวโดยสรุปได้ว่า การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล โดยบุคคลที่สามที่จะทำให้ได้รับเป็นความยินยอมที่ชอบด้วยกฎหมายเป็นไปตามหลักเกณฑ์ที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดไว้นั้น ไม่ใช่เรื่องง่าย ทั้งนี้เนื่องจากลักษณะของการได้มา ซึ่งข้อมูลไม่ได้เกิดขึ้นโดยตรงจากเจ้าของข้อมูล นอกจากนั้นหากมีการติดต่อโดยตรงไปยังเจ้าของข้อมูลส่วนบุคคลแล้ว มีความเป็นไปได้สูงที่เจ้าของข้อมูลจะปฏิเสธไม่ให้ความยินยอม[62] เนื่องจากการเก็บรวบรวมข้อมูลดังกล่าว เจ้าของข้อมูลมักจะเห็นว่าเป็นการกระทำที่เป็นประโยชน์ต่อผู้ขอความยินยอมในเชิงเพื่อหากำไร มากกว่าเป็นประโยชน์ต่อเจ้าของข้อมูลเอง กล่าวคือเจ้าของข้อมูลไม่สามารถ คาดหมายได้ถึงผลประโยชน์ที่จะเกิดขึ้นต่อตนเอง จึงไม่สามารถที่จะประเมินระดับความเสี่ยงที่จะเกิดขึ้นกับข้อมูลส่วนบุคคลของตนเมื่อเทียบกับความคุ้มค่าของประโยชน์ที่จะได้รับอันจะส่งผลให้เจ้าของข้อมูลตัดสินใจในการให้ความยินยอมได้[63]

จากสถานการณ์ข้างต้น ในทางปฏิบัติจึงทำให้ไม่ค่อยมีการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลสำหรับกรณีข้อมูลส่วนบุคคลที่ได้รับมาจากระบบอัตโนมัติ ดังนั้น จึงอาจกล่าวได้ว่าการดำเนินการต่าง ๆ ของผู้ให้บริการที่เกิดขึ้น โดยใช้ข้อมูลส่วนบุคคลที่ได้รับมาในลักษณะนี้ จึงไม่เป็นไปตามหลักเกณฑ์และเงื่อนไขที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลส่วนบุคคลกำหนดไว้ ซึ่งจะส่งผลโดยตรงต่อความปลอดภัยของข้อมูลส่วนบุคคลดังกล่าว

4.2 ประเด็นเกี่ยวกับการกำหนดสถานะ หน้าที่ และความรับผิดของผู้ที่เกี่ยวข้องกับการประมวลผล ข้อมูลส่วนบุคคล

กฎหมายคุ้มครองข้อมูลส่วนบุคคลให้ความสำคัญกับการคุ้มครองความปลอดภัยของข้อมูลส่วนบุคคล และสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลค่อนข้างมาก ดังจะเห็นได้ว่ามีการกำหนด สถานะของผู้ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลโดยพิจารณาจากลักษณะของกิจกรรมที่ผู้เกี่ยวข้องแต่ละรายกระทำต่อข้อมูลส่วนบุคคล ซึ่งกฎหมายแบ่งสถานะของผู้ที่เกี่ยวข้องออกเป็น 2 ประเภท ดังนี้ (1) ผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งเป็นผู้ที่มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และ (2) ผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งเป็นผู้ที่ดำเนินการเกี่ยวกับ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลตามคำสั่ง หรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล โดยจะไม่มีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลในเวลาเดียวกัน ทั้งนี้ การแบ่งสถานะดังกล่าวก็เพื่อให้สามารถกำหนดภาระหน้าที่ในการปฏิบัติตามหลักเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคลให้เหมาะสมกับผู้ที่มีสถานะที่แตกต่างกันไป ซึ่งถ้าหากฝ่าฝืนไม่ปฏิบัติตามก็จะมีความผิด และต้องได้รับโทษตามที่กฎหมายกำหนดไว้

แต่อย่างไรก็ตาม จากที่ได้กล่าวมาแล้วในข้อ 4.1 รูปแบบและลักษณะของการเคลื่อนไหวของข้อมูลส่วนบุคคลในบริบทของเมืองอัจฉริยะนั้นมีความหลากหลาย ซับซ้อน กระจัดกระจาย และเป็นไปโดยการทำงานของระบบอัตโนมัติของเทคโนโลยีต่าง ๆ สถานการณ์เหล่านี้ทำให้เกิดความยากลำบาก ในการติดตามเส้นทางการเคลื่อนไหวของข้อมูล ผู้เก็บรวบรวม ใช้ ข้อมูล และกิจกรรมต่าง ๆ ที่เกิดขึ้นกับข้อมูล ซึ่งก่อให้เกิดปัญหาในการพิจารณาต่อไปว่ามีข้อมูลส่วนบุคคลที่เกิดขึ้นใหม่จากการทำงานโดยระบบอัตโนมัติหรือไม่ ถ้ามีแล้วก็เกิดขึ้นจากทำงานของระบบใด ใครเป็นเจ้าของข้อมูลดังกล่าว มีการแลกเปลี่ยนข้อมูลดังกล่าวไปให้หน่วยงานใดบ้าง อย่างไรบ้าง หน่วยงานใดสามารถ

---

[62] Mark Lizar and Mary Hodder, “Usable consents: tracking and managing use of personal data with consent transaction receipts,” in Proceedings of UbiComp (Adjunct), Seattle, WA, USA, September 13 - 17, 2014, from http://dx.doi.org/10.1145/2638728.2641681, p.647 – 652.

[63] Lilian Edwards, “Privacy, Security and Data Protection in Smart Cities : A Critical EU Law Perspective,” European Data Protection Law Review. 2: 1. (2016).

เข้าถึงข้อมูลดังกล่าวได้บ้าง เนื่องจากจากการที่ไม่ทราบข้อเท็จจริงที่ว่าแต่ละหน่วยงานที่ได้รับแบ่งปันข้อมูลที่เกิดขึ้นจากระบบอัตโนมัตินั้นนำเอาข้อมูลดังกล่าวไปใช้ในลักษณะใดบ้าง และข้อมูลนั้นเกิดขึ้นจากการประมวลผลของระบบใด และมีการแบ่งปันจากระบบใด จึงก่อให้เกิดปัญหาในการพิจารณากำหนดสถานะของหน่วยงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ซึ่งจะมีความเชื่อมโยงกันกับการพิจารณาระบุหน้าที่ และความรับผิดของหน่วยงานดังกล่าวด้วย

ดังนั้นการพิจารณาว่าหน่วยงานที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้รับมาจากระบบอัตโนมัติในบริบทของเมืองอัจฉริยะนั้น จะมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลตามคำนิยามที่กำหนดไว้ ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลจึงไม่ใช่เรื่องง่ายผลกระทบที่เกิดขึ้นคือหากไม่สามารถระบุสถานะตามกฎหมายของหน่วยงานที่เกี่ยวข้องได้ ก็จะเป็นเรื่องยากที่จะระบุหน้าที่และความผิดของหน่วยงานดังกล่าวได้

โดยงานวิจัยนี้ได้พิจารณาสถานการณ์ต่าง ๆ ที่อาจจะเกิดขึ้นในกรณีที่มีการแบ่งปันข้อมูลกันเองในระบบโดยอัตโนมัติในบริบทของเมืองอัจฉริยะ ซึ่งทำให้หน่วยงานที่เป็นบุคคลที่สามสามารถเข้าถึงข้อมูลดังกล่าวได้ แล้ววิเคราะห์ถึงลักษณะของกิจกรรมของแต่ละหน่วยงานที่ได้กระทำต่อข้อมูลส่วนบุคคล ทั้งนี้เพื่อเป็นแนวทางวิเคราะห์กำหนดสถานะ หน้าที่และความรับผิดของหน่วยงานที่เกี่ยวข้อง ซึ่งมีรายละเอียด ดังต่อไปนี้

<u>กรณีแรก</u> หากหน่วยงานที่เป็นบุคคลที่สามได้รับข้อมูลไปในบริบทที่เจ้าของข้อมูลอาจคาดหมายได้ว่า ข้อมูลจะได้รับการเปิดเผยไปยังหน่วยงานดังกล่าว กล่าวคือ หน่วยงานดังกล่าว มีหน้าที่เกี่ยวข้องที่ต้องนำข้อมูลเหล่านั้นไปประมวลผล เพื่อที่จะสามารถให้บริการแก่เจ้าของข้อมูลได้ตรงตามความต้องการหน่วยงานนี้จะมีสถานะเป็นผู้ประมวลผลข้อมูลที่มีหน้าที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่ง หรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งเป็นผู้ให้บริการที่ได้รับข้อมูลมาโดยตรงจากเจ้าของข้อมูล โดยความสัมพันธ์ระหว่างผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลควรจะอยู่ในรูปแบบของสัญญาที่กำหนดหน้าที่ ความรับผิด เงื่อนไขในการประมวลผลให้เป็นไปตามความประสงค์ของเจ้าของข้อมูลส่วนบุคคล[64]

<u>กรณีที่สอง</u> ข้อมูลที่ได้รับมาจากระบบการทำงานอัตโนมัติ ซึ่งโดยส่วนใหญ่มักจะเกิดขึ้นในกรณีที่เจ้าของข้อมูลไม่สามารถคาดหมายได้จากการให้ความยินยอมในครั้งแรก เมื่อมีการนำข้อมูลเข้าสู่ระบบการทำงานของเทคโนโลยีต่าง ๆ ภายหลังจากการอ่านนโยบายความเป็นส่วนตัวของผู้ควบคุมข้อมูลส่วนบุคคลที่เจ้าของข้อมูลได้มีการให้ความยินยอมไปแล้ว ดังนั้น หน่วยงานที่ได้รับข้อมูลมาจากระบบอัตโนมัติในกรณีนี้ จึงมักเป็นหน่วยงานที่ไม่ได้เกี่ยวข้องโดยตรงกับการให้บริการนั้น ๆ แก่เจ้าของข้อมูลส่วนบุคคล อาทิ เช่น ได้รับข้อมูลจากระบบการประมวลผลของระบบการทำงานของ Big Data จึงทำให้สามารถเข้าถึงข้อมูลที่อยู่ในความครอบครองของผู้ให้บริการแต่ละรายได้เมื่อมีการเชื่อมโยงกันของฐานข้อมูลต่าง ๆ เช่น ข้อมูลเกี่ยวกับพฤติกรรมของประชาชนในการใช้บริการประเภทต่าง ๆ ซึ่งในบางครั้งอาจเชื่อมโยงไปถึงข้อมูลอ่อนไหว ในกรณีนี้หน่วยงานเหล่านี้อาจมีสถานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลที่มีอำนาจหน้าที่ตัดสินใจอย่างเต็มที่เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเหล่านั้นในกิจกรรมต่าง ๆ เพื่อประโยชน์ของหน่วยงานโดยเฉพาะ (ซึ่งส่งผลให้หน่วยงานดังกล่าวต้องหาฐานในทางกฎหมายในการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลดังกล่าว เพื่อเป็นการปฏิบัติตามหลักเกณฑ์ของกฎหมายคุ้มครองข้อมูลส่วนบุคคล)[65]

ผลการวิเคราะห์ข้างต้นเป็นเพียงการวิเคราะห์จากการคาดคะเนข้อเท็จจริงที่อาจเกิดขึ้นเมื่อมีการแบ่งปันข้อมูลกันเองในโดยอัตโนมัติในระบบอันจะทำให้หน่วยงานต่าง ๆ สามารถเข้าถึงข้อมูลส่วนบุคคลของประชาชนเป็นจำนวนมากได้ แต่อย่างไรก็ตาม ยังคงมีอีกหลายสถานการณ์ที่หน่วยงานที่ได้รับข้อมูลมาโดยไม่ทราบแหล่งที่มาที่ชัดเจนของข้อมูล อันเนื่องจากอาจจะเป็นข้อมูลที่เกิดขึ้นใหม่ภายหลังจากการประมวลผลของเทคโนโลยีต่าง ๆ ดังนั้นจึงสามารถสรุปได้ว่า พฤติการณ์ของการแบ่งปันข้อมูลในระบบโดยอัตโนมัติ ในบริบทของเมืองอัจฉริยะทำให้เกิดความ

---

[64] Daniela Popescul and Laura Diana Radu, “Data Security in Smart Cities : Challenges and Solutions,” <u>Informatică Economică</u>. 20:1. (2016).

[65] Janine S. Hiller and Jordan M. Blanke, “Smart Cities, Big Data, and the Resilience of Privacy,” <u>Hastings Law Journal</u>. 68:2. (2017).

ยากลำบากในการกำหนดสถานะ หน้าที่และความรับผิดของหน่วยงานต่าง ๆ ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล ซึ่งปัญหาดังกล่าวอาจส่งผลต่อความปลอดภัยของข้อมูลส่วนบุคคลในบริบทของเมืองอัจฉริยะได้เช่นกัน

บทสรุปและข้อเสนอแนะ

แนวคิดการสร้างเมืองอัจฉริยะ ถูกนำมาใช้ในการวางแผนเมืองให้มีความน่าอยู่อย่างยั่งยืน โดยองค์ประกอบของเมืองอัจฉริยะ สามารถแบ่งพิจารณาได้เป็น 2 ส่วน ดังนี้ (1) เทคโนโลยี ที่ถูกนำมาปรับใช้กับเมืองเพื่อพัฒนาโครงสร้างพื้นฐานของระบบการให้บริการของหน่วยงานทั้งภาครัฐ และภาคเอกชนผ่านการวิเคราะห์ข้อมูลต่าง ๆ เช่น การใช้เทคโนโลยีวิเคราะห์ความแออัดของการจราจรบนท้องถนนเพื่อให้ประชาชนสามารถวางแผนการเดินทางได้, การพัฒนาด้านเทคโนโลยีทางการแพทย์ที่ทำให้ผู้ป่วยสามารถเข้าถึงระบบดูแลสุขภาพโดยที่ตัวเองยังอยู่ที่บ้านได้ การวิเคราะห์พฤติกรรมการบริโภคของประชาชนจากการใช้บริการออนไลน์ในรูปแบบต่าง ๆ เพื่อทำให้สามารถให้เสนอสินค้า และบริการที่สอดคล้องกับความต้องการของประชาชนให้ได้มากที่สุด เป็นต้น ; (2). ประชาชน ที่มีความเกี่ยวข้องกับเมืองคือ หัวใจหลักในการออกแบบ และวางแผนพัฒนาเมือง (User-Centered Design) ผ่านการเลือกใช้เทคโนโลยีที่เหมาะสม สอดรับกับรูปแบบการดำเนินชีวิตประชาชนที่มีการเปลี่ยนแปลงไปในแต่ละบริบทของสังคม[66]

แนวคิดของเมืองอัจฉริยะ มิใช่แต่เพียงการนำเทคโนโลยีต่าง ๆ มาใช้เพื่อเพิ่มความสะดวกสบายให้แก่ประชาชนที่อาศัยอยู่ในเมืองเท่านั้น แต่ยังเป็นการนำเอาเทคโนโลยีหลากหลายรูปแบบมาใช้ในการแก้ไขปัญหาต่าง ๆ ในสังคมด้วย แนวคิดเมืองอัจฉริยะนี้จึงเริ่มเข้ามามีบทบาทสำคัญในการดำรงชีวิตประจำวันของมนุษย์มากยิ่งขึ้น ประเทศไทยได้นำเอาแนวความคิดนี้เข้ามาปรับใช้เช่นกัน แต่อย่างไรก็ตาม ประเด็นปัญหาในเรื่องความปลอดภัยของข้อมูลส่วนบุคคลและการคุ้มครองสิทธิความเป็นส่วนตัวก็ยังเป็นประเด็นสำคัญที่ทุกภาคส่วนยังคงมีความกังวล และพยายามหาแนวทางที่มีประสิทธิภาพที่สุดมาใช้ในการแก้ไขปัญหาดังกล่าว

ผลการศึกษาวิจัยแสดงให้เห็นชัดเจนว่า การทำงานของเมืองอัจฉริยะ ซึ่งประกอบด้วยการทำงานของเทคโนโลยี Internet of Things, Big Data, Machine Learning, Cloud Computing ทำให้ลักษณะการเคลื่อนไหวของข้อมูลมีความหลากหลาย ซับซ้อน และกระจัดกระจาย จึงทำให้หน่วยงานภาคเอกชนต่าง ๆ สามารถเข้าถึงข้อมูลส่วนบุคคลของประชาชนจำนวนมากได้โดยที่อาจจะไม่ได้ปฏิบัติตามหลักเกณฑ์ที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้กำหนดไว้ จากสถานการณ์ดังกล่าวจึงสามารถสรุปได้ว่าลักษณะของการประมวลผลข้อมูลส่วนบุคคลในบริบทของเมืองอัจฉริยะทำให้เกิดความท้าทายทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคล โดยงานวิจัยนี้มุ่งศึกษา 2 ประเด็นดังต่อไปนี้

(1) ประเด็นเกี่ยวกับการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล กล่าวคือ เมื่อข้อมูลส่วนบุคคลได้รับการประมวลผลโดยเทคโนโลยีต่าง ๆ จึงอาจทำให้ข้อมูลมีการแลกเปลี่ยนกันเองในระบบการทำงานอัตโนมัติ ทำให้มีหน่วยงานภาคเอกชนสามารถเข้าถึงข้อมูลส่วนดังกล่าวได้ ซึ่งในกรณีนี้หากการขอความยินยอมเป็นฐานทางกฎหมายเดียวที่จะสามารถทำให้หน่วยงานนั้นสามารถเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นได้โดยชอบด้วยกฎหมายเพื่อ วัตถุประสงค์ในการเสนอขายสินค้าและบริการให้กับเจ้าของข้อมูลส่วนบุคคลแล้ว ผลการศึกษาวิจัยพบว่าการติดต่อขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เพื่อให้เป็นไปตามหลักเกณฑ์ที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดไว้เป็นเรื่องที่ค่อนข้างยาก และมีความเป็นไปได้สูงที่เจ้าของข้อมูลจะปฏิเสธที่จะให้ความยินยอม

(2) ประเด็นเกี่ยวกับการกำหนดสถานะ หน้าที่ และความรับผิดของผู้ที่เกี่ยวข้องกับการประผลข้อมูลส่วนบุคคล กล่าวคือ เนื่องจากเส้นทางการเคลื่อนไหวของข้อมูลในบริบทของเมืองอัจฉริยะนั้นค่อนข้างมีความซับซ้อน จึงอาจทำให้มีหน่วยงานต่าง ๆ ที่สามารถเข้าถึงข้อมูลส่วนบุคคลดังกล่าวได้อย่างหลากหลาย และหากการเข้าถึงนั้นเกิดขึ้นจากการที่หน่วยงานเหล่านั้นแบ่งปันข้อมูลกันเอง หรือการแบ่งปันนั้นเกิดขึ้นเองโดยระบบอัตโนมัติจากการทำงานของเทคโนโลยีต่าง ๆ แล้ว การควบคุมการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในกรณีดังกล่าวจึง

[66] สุวิทย์ วงศ์รุจิราวาณิชย์, “Smart City เมืองอัจฉริยะ เชื่อมสังคมขับเคลื่อนเศรษฐกิจผ่านเทคโนโลยี,” สืบเมื่อค้นวันที่ 28 มกราคม 2563, จาก https://www.asaexpo.org/single-post/smartcity.

เป็นไปได้ยาก เหตุการณ์ดังกล่าวทำให้เกิดความยากลำบากในการกำหนดสถานะ หน้าที่ในการปฏิบัติตามกฎหมาย และความรับผิดของผู้ที่เกี่ยวข้อง

จากประเด็นความท้าทายทางกฎหมายทั้งสองประการ งานวิจัยนี้ จึงได้เสนอแนะแนวทางที่เป็นไปได้ในการจัดการกับความท้าทายดังกล่าว ทั้งนี้เพื่อเป็นการคุ้มครองความปลอดภัยของข้อมูลส่วนบุคคลและสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคล โดยที่ไม่เป็นการการกีดกันการนำข้อมูลไปใช้ในบริบทของเมืองอัจฉริยะเพื่อการพัฒนาอย่างยั่งยืน ดังต่อไปนี้

(1) กำหนดนโยบายให้หน่วยงานต่าง ๆ ที่จะได้รับข้อมูลส่วนบุคคลโดยตรงจากเจ้าของข้อมูลไม่ว่าจะได้รับมาโดยฐานของสัญญา หรือฐานของความยินยอมจากเจ้าของข้อมูลส่วนบุคคล พยายามระบุวัตถุประสงค์ ในการใช้งานข้อมูลส่วนบุคคลให้ครอบคลุมทุกกิจกรรมที่จะเกิดขึ้นและที่อาจจะเกิดขึ้น รวมทั้งระบุลักษณะและพฤติการณ์ที่อาจเกิดขึ้นกับข้อมูลดังกล่าว โดยระบุในสัญญาหรือแบบคำขอความยินยอม (Consent Form) และนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของหน่วยงาน[67] ทั้งนี้เพื่อให้เจ้าของข้อมูลส่วนบุคคลได้รับทราบและมีข้อมูลเพียงพอที่จะตัดสินใจได้ว่าจะตกลงยินยอมให้หน่วยงานดังกล่าว เก็บรวบรวม ใช้หรือเปิดเผยข้อมูลของตนเองต่อหน่วยงานอื่น ๆ เพื่อให้สามารถกระทำการตามวัตถุประสงค์ที่แจ้งไว้ได้หรือไม่ และในขณะเดียวกันควรแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงการเปิดเผยข้อมูลดังกล่าวต่อบุคคลที่สาม พร้อมทั้งกำหนดมาตรการที่ปลอดภัยในการเปิดเผยข้อมูลส่วนบุคคลที่ชัดเจน ยกตัวอย่าง เช่น ต้องมีการทำสัญญาประมวลผลข้อมูลส่วนบุคคล (data processing agreement) หรือสัญญาแบ่งปันข้อมูลส่วนบุคคล (data sharing agreement) กับบุคคลที่สาม เพื่อให้การเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลที่สามนั้นเป็นไปตามวัตถุประสงค์ที่ได้ตกลงไว้กับเจ้าของข้อมูล และเพื่อเป็นการควบคุมบุคคลที่สามให้ปฏิบัติตามกฎหมายอย่างเคร่งครัด

(2) กำหนดหลักเกณฑ์เกี่ยวกับการแลกเปลี่ยนข้อมูลส่วนบุคคลระหว่างหน่วยงานที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของประชาชนในบริบทของเมืองอัจฉริยะ โดยเฉพาะอย่างยิ่งควรกำหนดมาตรการไว้โดยเฉพาะสำหรับข้อมูลที่ได้รับมาจากระบบการทำงานอัตโนมัติของเทคโนโลยีต่าง ๆ[68] และควรจัดทำแบบบันทึก (มีแนวคิดคล้ายกับแบบบันทึกการประมวลผลข้อมูลตามที่กำหนดไว้ในมาตรา 39 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562) ในฐานะเป็นเอกสาร สำคัญของหน่วยงานเพื่อยืนยันรายละเอียดต่าง ๆ เกี่ยวกับวิธีการได้มา ซึ่งข้อมูลส่วนบุคคลของ เจ้าของข้อมูลแต่ละรายพร้อมแนบหลักฐานประกอบ (เช่น สัญญาหรือแบบความยินยอม) รวมทั้งระบุลักษณะการใช้งานข้อมูลส่วนบุคคลดังกล่าว อาทิ เช่น วิธีการในการเก็บรวบรวม ใช้และเปิดเผยข้อมูลส่วนบุคคล ทั้งนี้เพื่อทำให้สามารถกำหนด สถานะ หน้าที่และความรับผิดของแต่ละหน่วยงานได้อย่างชัดเจน ซึ่งจะเป็นประโยชน์ต่อเจ้าของข้อมูลโดยเฉพาะ เมื่อมีการละเมิดข้อมูลส่วนบุคคลเกิดขึ้นและถือเป็นการสนับสนุนหลักความโปร่งใสอันเป็นหลักการพื้นฐานที่สำคัญของกฎหมายคุ้มครองข้อมูลส่วนบุคคล

(3) หน่วยงานทั้งภาครัฐและภาคเอกชนต่าง ๆ ควรใช้มาตรการ ในการรักษาความปลอดภัยของข้อมูลที่เหมาะสมกับข้อมูลแต่ละประเภท (ข้อมูลส่วนบุคคลหรือข้อมูลอ่อนไหว) โดยอาจเป็นการใช้มาตรการเฉพาะของหน่วยงาน อาทิ เช่น การกำหนดลำดับขั้นการเข้าถึงข้อมูลร่วมกับมาตรการทางเทคนิคในรูปแบบต่าง ๆ ยกตัวอย่าง เช่น “Anonymization” ซึ่งก็คือ การทำให้ข้อมูลส่วนบุคคลไม่สามารถใช้ในการระบุตัวตนของบุคคลดังกล่าวได้อีกต่อไป โดยใช้วิธีการต่าง ๆ เช่น Generalising หรือ Adding noise[69] นอกจากนั้น ยังมีวิธีการที่เรียกกันว่า

---

[67] Article 29 Working Party, “Opinion 8/2014 on the Recent developments on the Internet of Things, WP 223 (2014),” p.7.

[68] Lilian Edwards, “Privacy, Security and Data Protection in Smart Cities : A Critical EU Law Perspective,” European Data Protection Law Review. 2: 1. (2016).

[69] Article 29 Working Party, “Opinion 05/2014 on Anonymisation Techniques, WP 216 (2014),” Retrieved on January 20, 2020, from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. p.11 – 13.

Pseudonymisation คือ การใช้ตัวเลขหรือรหัสแทนที่ข้อมูลส่วนบุคคลส่งผลให้ข้อมูลนั้นไม่สามารถระบุตัวตนของเจ้าของข้อมูลได้โดยตรง เช่น encryption with secret key หรือ hash function[70]

แต่อย่างไรก็ตาม ในบริบทของเมืองอัจฉริยะข้อมูลเหล่านี้จะถูกนำเข้าสู่ระบบ การทำงานอัตโนมัติของเทคโนโลยีต่าง ๆ จึงทำให้เกิดการเชื่อมโยงกันระหว่างฐานข้อมูลที่หลากหลาย และสุดท้ายอาจนำไปสู่สถานการณ์ที่ทำให้สามารถระบุตัวตนของเจ้าของข้อมูลได้จากข้อมูลดังกล่าวได้ นักวิชาการเรียกกันว่า Quasi - Identifier ซึ่งก็คือแนวคิดของข้อมูลที่ไม่สามารถใช้ เพื่อระบุตัวตนของบุคคลได้จากตัวของข้อมูลเอง แต่ข้อมูลดังกล่าวสามารถใช้ระบุตัวตนของบุคคลได้หากถูกนำไปรวมหรือเชื่อมโยงกับข้อมูลอื่น[71]

ดังนั้น จึงได้มีการเสนอวิธีการรักษาความปลอดภัยของข้อมูลส่วนบุคคลในบริบท Internet of Things ไว้ว่า ให้มีการลบข้อมูลดิบที่รวบรวม โดยเครื่องมือเครื่องใช้อิเล็กทรอนิกส์ โดยให้ผู้ให้บริการ ลบข้อมูลดิบทันทีที่ได้มีการดึงข้อมูลที่จำเป็นสำหรับการประมวลผลข้อมูล ซึ่งตามหลักการแล้วการลบควรเกิดขึ้น ณ จุดรวบรวมข้อมูลดิบที่ใกล้ที่สุด (เช่น จากอุปกรณ์เดียวกันหลังจากประมวลผล)[72] นอกจากนั้น มีการนำเสนอแนวทางในจัดการกับความเสี่ยงในกรณีข้อมูลรั่วไหวในระบบการทำงานของ Machine Learning โดยการปรับปรุงลักษณะของการทำงานของของระบบให้ไม่มีการจดจำข้อมูลที่มีการเรียนรู้ ทั้งนี้ เพื่อเป็นการป้องกันการรวบรวมข้อมูลส่วนบุคคลเข้าสู่ระบบการประมวลผลและมีการแลกเปลี่ยนกันเอง โดยอัตโนมัติในระบบ ซึ่งจะเป็นขั้นตอนที่ทำให้การควบคุมความปลอดภัยของข้อมูลทำได้ยากขึ้น[73]

นอกจากนั้น การพัฒนาโปรแกรมใหม่ๆขึ้นมาเพื่อช่วยควบคุมดูแลการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในบริบทของเมืองอัจฉริยะก็เป็นแนวคิดที่น่าสนใจ ยกตัวอย่างเช่น เมืองปัมโปลนา ประเทศสเปน มีการพัฒนาพลังงานอัจฉริยะเพื่อบูรณาการเข้ากับเขตเมือง โดยมีพัฒนาซอฟต์แวร์สำหรับการปกป้องคุ้มครองข้อมูลอัจฉริยะของเมืองมาใช้ภายใต้การดูแลของเจ้าหน้าที่คุ้มครองข้อมูลเพื่อปกป้องข้อมูลส่วนบุคคลพลเมืองซึ่งผู้เชี่ยวชาญของมหาวิทยาลัยซาเกร็บ Goran Vojkovic ได้กล่าวถึงแนวคิด และลักษณะการทำงานของซอฟต์แวร์ดังกล่าวว่า “นับตั้งแต่วินาทีที่เมืองอัจฉริยะต้องการ ใช้ข้อมูลส่วนบุคคลที่เก็บรวบรวมในที่สาธารณะก็จะเกิดภาระหน้าที่ในการแปลงข้อมูล ส่วนบุคคล ให้เป็นข้อมูลที่ไม่สามารถระบุตัวตนได้ เพื่อเป็นการปกป้องคุ้มครองสิทธิของประชาชน”[74]

(4) ให้ความรู้แก่หน่วยงานทั้งภาครัฐและภาคเอกชนทุกรายที่มีบทบาทในเมืองอัจฉริยะ ในฐานะผู้ให้บริการประเภทต่าง ๆ ให้ตระหนักถึงความสำคัญในการรักษาความปลอดภัยของข้อมูลส่วนบุคคลและการคุ้มครองสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลอันเป็นสิทธิขั้นพื้นฐานของประชาชนทุกคน ตลอดจนชี้แจงให้มีความเข้าใจถึงหลักเกณฑ์ในการเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคลให้เป็นไปตามหลักเกณฑ์ที่ได้กำหนดไว้ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล นอกจากนั้นควรจัดให้มีการให้ความรู้แก่ประชาชนทุกคนในฐานะเป็นผู้ใช้บริการในการ

---

[70] *Ibid*, p.20.

[71] Rubinstein, Ira and Hartzog, Woodrow, Anonymization and Risk (August 17, 2015). 91 Washington Law Review 703 (2016) ; NYU School of Law, Public Law Research Paper No.1536. from https: //ssrn.com/abstract=2646185.

[72] Himani Verma, Shraddha Ugalmugale, Mrunmayee Godse and Nasim Shah, “Prevention of Duplication of Encrypted Big Data in Cloud,” 2nd International Conference on Advances in Science & Technology (ICAST) by K J Somaiya Institute of Engineering & Information Technology, Mumbai, India, April, 8-9, 2019, from https://ssrn.com/abstract=3370214.

[73] Yinzhi Cao and Junfeng Yang, “Towards Making Systems Forget with Machine Unlearning,” in Proceedings of the 2015 IEEE Symposium on Security and Privacy, Washington, DC, USA, (May 2015).

[74] Lorenzo Dalla Corte, Bastiaan van Loenen and Colette Cuijpers, “Personal Data Protection as a Nonfunctional Requirement in the Smart City's Development,” in Proceedings of the 13th International Conference on Internet, organized by Law & Politics, Universitat Oberta de Catalunya, Barcelona, June 29 - 30, 2017.

เลือกใช้บริการจากผู้ให้บริการที่มีมาตรการในการดูแล และคุ้มครองความปลอดภัยของข้อมูลที่เหมาะสม รวมทั้งให้ความรู้แก่ประชาชนเกี่ยวกับมาตรการทางเทคนิคต่าง ๆ ในการปกป้องความปลอดภัยของข้อมูล และสนับสนุนให้ประชาชนมีส่วนร่วมในการปรับใช้มาตรการทางเทคนิคดังกล่าวในการรักษาความปลอดภัยของ ข้อมูลส่วนบุคคลของตนเอง

บรรณานุกรม

เอกสารอื่น ๆ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

BOOKS

Andrew G. Psaltis. Streaming Data : Understanding the Real - time Pipeline. New York : Manning Publications Co,. 2017.

Rob Kitchin. Tracey P. Lauriault and Matthew W. Wilson. Understanding Spatial Media. London : Sage Publications Ltd,. 2017.

Vlasios Tsiatsis. Stamatis Karnouskos. Jan Holler. David Boyle and Catherine Mulligan. Internet of Things : Technologies and Applications for a New Age of Intelligence. 2nd edition. Academic Press. 2018.

Zhu Han. Mingyi Hong and Dan Wang. Signal Processing and Networking for Big Data Applications. Cambridge University Press. 2017.

ARTICLES

A. Michael Froomkin. “Big Data : Destroyer of Informed Consent.” Yake Journal of Health Policy, Law, and Ethics. Forthcoming ; University of Miami Legal Studies Research Paper Forthcoming. https://ssrn.com/abstract=3405482. (September 2019).

Arthur P.B. Laudrain. “Smart-city Technologies, Government Surveillance and Privacy: Assessing the Potential for Chilling Effects and Existing Safeguards in the ECHR.” Leiden Law School Research Paper. https://ssrn.com/abstract=3437216. (August 2019).

Christian Iaione. Elena de Nictolis and Anna Berti Suman. “The Internet of Humans (IoH) : Human Rights and Co-Governance to Achieve Tech Justice in the City.” Law and Ethics of Human Rights. Forthcoming. https://ssrn.com/abstract=3315437. (January 2019).

Daniela Popescul and Laura Diana Radu. “Data Security in Smart Cities : Challenges and Solutions.” Informatică Economică. 20:1. (2016).

Fang Yang and Jian Xu. “Privacy Concerns in China's Smart City Campaign: The Deficit of China's Cybersecurity Law.” Asia & the Pacific Policy Studies. 5:3. (2018).

Janine S. Hiller and Jordan M. Blanke. “Smart Cities, Big Data, and the Resilience of Privacy.” Hastings Law Journal. 68: 2. (2017).

Jesse W. Woo. “Smart Cities Pose Privacy Risks and Other Problems, But that Doesn't Mean We Shouldn't Build Them.” University of Missouri - Kansas City Law Review. 83:4. (2017).

Karl M. Manheim and Lyric Kaplan. “Artificial Intelligence: Risks to Privacy and Democracy.” 21 Yale Journal of Law and Technology 106 ; Loyola Law School, Los Angeles Legal Studies Research Paper No. 2018 - 37. https://ssrn.com/abstract=3273016. (2019).

Liesbet van Zoonen. “Privacy Concerns in Smart Cities.” Government Information Quarterly. 33:3. (2016).

Lilian Edwards. “Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective.” European Data Protection Law Review. 2: 1. (2016).

Mahmoud Elkhodr and Zuhaib Bari Mufti. “On the Challenges of Data Provenance in the Internet of Things.” International Journal of Wireless & Mobile Networks (IJWMN). 11:3. (2019).

Manick Wadhwa. “Understanding the Impact of Smart Cities and the Need for Smart Regulations.” SSRN Electronic Journal. https://ssrn.com/abstract=2908299. (July 2015).

Masa Galic. “Surveillance. Privacy and Public Space in the Stratumseind Living Lab : The Smart City Debate. Beyond Data.” Ars Aequi. special issue July - August. (2019).

Nora Ni Loideain. “Cape Town as a Smart and Safe City : Implications for Governance and Data Privacy.” International Data Privacy Law. 7:4. (2017).

R. Sumithra and R. Parameswari. “Security, Privacy Issues and Challenges in Big Data and Cloud Security: A Survey (2018).” International Journal of Advanced Studies of Scientific Research. 3:10. https://ssrn.com/abstract=3319251. (2018).

Zaheer Allam and Zaynah A. Dhunny. “On Big data, Artificial Intelligence and Smart Cities in Cities.” Cities 89. (January 2019).

OTHER DOCUMENTS

Ewa Luger and Tom Rodden. “An Informed View on Consent for Ubicomp.” in Proceedings of UbiComp (Adjunct), Zurich, Switzerland, http://dx.doi.org/10.1145/2493432.249344. September 8 – 12, 2013.

Himani Verma. Shraddha Ugalmugale. Mrunmayee Godse and Nasim Shah. “Prevention of Duplication of Encrypted Big Data in Cloud.” 2nd International Conference on Advances in Science & Technology (ICAST) by K J Somaiya Institute of Engineering & Information Technology, Mumbai, India. https://ssrn.com/abstract=3370214. April 8 - 9, 2019.

Ira Rubinstein. “Big Data: The End of Privacy or a New Beginning?.” International Data Privacy Law (2013 Forthcoming), NYU School of Law, Public Law Research Paper No.12 - 56. http://dx.doi.org/10.2139/ssrn.2157659.

Mark Lizar and Mary Hodder. “Usable Consents : Tracking and Managing Use of Personal Data with Consent Transaction Receipts.” in Proceedings of UbiComp (Adjunct), Seattle, WA, USA, http://dx.doi.org/10.1145/2638728.2641681. September 13 - 17, 2014.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation

Yinzhi Cao and Junfeng Yang. “Towards Making Systems Forget with Machine Unlearning.” in Proceedings of the 2015 IEEE Symposium on Security and Privacy, Washington, DC, USA. May, 2015.