พัฒนาการของการคุ้มครองสิทธิในความเป็นส่วนตัว เกี่ยวกับข้อมูลส่วนบุคคลในประเทศไทย

นพดล นิ่มหนู *

(วันรับบทความ: 19 กรกฎาคม 2563/ วันแก้ไขบทความ: 3 ตุลาคม 2563/ วันตอบรับบทความ: 16 ตุลาคม 2563)

บทคัดย่อ

พัฒนาการของการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศไทยเป็นไปอย่างล่าช้า โดยแต่เดิมในยุคแรกประเทศไทยใช้รูปแบบการคุ้มครองสิทธินี้บนพื้นฐานของกฎหมายแพ่งในลักษณะละเมิดและกฎหมายอาญา ในความผิดฐานเปิดเผยความลับและฐานหมิ่นประมาท ต่อมายุคที่สองได้มีการสร้างกฎหมายมหาชนขึ้นมาเพื่อคุ้มครองสิทธินี้ ไม่ว่าจะเป็นระดับของบทบัญญัติตามรัฐธรรมนูญ และกฎหมายเฉพาะต่าง ๆ เช่นพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540, พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545, พระราชบัญญัติการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 ฯลฯ เป็นต้น ซึ่งมีลักษณะของการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลที่เป็นการเฉพาะเรื่องและเฉพาะประเภทของข้อมูลบางชนิดเท่านั้น แต่ยังไม่ได้มีบทบัญญัติที่มีลักษณะเป็นกฎหมายกลางอันเป็นบทบัญญัติทั่วไปที่สามารถกำหนดคุ้มครองข้อมูลส่วนบุคคลในทุกกรณี จนกระทั่งถึงยุคของการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่ถือว่าประเทศไทยได้มีการกำหนดมาตรการในการคุ้มครองข้อมูลส่วนบุคคลในลักษณะของกฎหมายกลางที่เป็นบทบัญญัติทั่วไปออกมาภายใต้กระแสแห่งการเปลี่ยนแปลงอย่างรุนแรงของเทคโนโลยีสารสนเทศและแรงกดดันจากกติการะหว่างประเทศที่สำคัญนั่นคือ General Data Protection Regulation ของสหภาพยุโรป กรณีเช่นนี้จึงทำให้ไทยจำเป็นที่จะต้องดำเนินการพัฒนาทั้งหลักการของกฎหมาย รวมถึงกระบวนการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลให้มีมาตรฐานที่ทัดเทียมกับนานาอารยประเทศต่อไปเพื่อป้องกันการนำเป็นเรื่องนี้มาเป็นข้ออ้างในการกีดกันทางการค้าในอนาคต

คำสำคัญ: พัฒนาการ, สิทธิในความเป็นส่วนตัว, การคุ้มครองข้อมูลส่วนบุคคล

---

* *อาจารย์ประจำคณะนิติศาสตร์ มหาวิทยาลัยมหาสารคาม*

Development of Rights to Data Privacy in Thailand

Noppadon Nimnoo*

(Received Date: July 19, 2020, Revised Date: October 3, 2020, Accepted Date: October 16, 2020)

Abstract

The development of Thai Personal Data Protection has been slow due to the lack of specific law that can generally applied to all situation. At first, Thailand applied this form of protection only on rules of tort in both civil law and criminal law for violating disclosed secrets and defamation. Consequently, public law was introduced to protect the rights, including the constitutional provisions and others laws such as, the Official Information Act 2540, Credit information Business Act B.E.2545, Computer Crime Act B.E.2550, etc., which has the characteristics to protect some specific personal data at some certain types. However, there is no general law that can applied to all kind of personal data protection. Not until the upcoming of the promulgation of the Personal Data Protection Act B.E. 2562. This is the first time that Thailand has established the personal data protection law in the form of general law. Notwithstanding, because of the rapid change of new information technology and the General Data Protection Regulation of the European Union. Therefore, Thailand needs to develop both the principles of law and the process of enforcement. The personal data protection need to be international standard in order to cope with the possible pressure from the new international rules and regulation that may be the cause of accusation of an unfavourable law that possible cause trade barriers in the future.

Keywords: Development, Rights to Privacy, Data Protection

---

* *Lecturer, Faculty of Law, Mahasarakham University*

บทนำ

เหตุที่ว่า ข้อมูลมีความสำคัญอย่างยิ่งในสังคมสมัยใหม่ยุคปัจจุบันที่เป็นสังคมแห่งข้อมูลข่าวสารและเป็นสังคมแห่งการติดต่อสื่อสาร ข้อมูลมีความสำคัญทั้งต่อการวางแผน ระบบการทำงานและการบริหารจัดการ การดำเนินกิจกรรมต่าง ๆ ไม่ว่าจะเป็นภาครัฐหรือเอกชน ดังนั้นจึงส่งผลให้เกิดความจำเป็นที่องค์กรต่าง ๆ ต้องมีข้อมูลไว้ในครอบครองไว้ให้มากที่สุด ซึ่งในข้อมูลข่าวสารจำนวนมากมายมหาศาลที่มีการครอบครอง หรือมีการแลกเปลี่ยน หรือแย่งชิงแข่งขันกันครอบครองนี้ มีข้อมูลส่วนหนึ่งเป็นข้อมูลส่วนบุคคล ซึ่งถือเป็นสิทธิมนุษยชนของผู้ที่เป็นเจ้าของข้อมูล ดังนั้น รูปแบบของสิทธิในความเป็นอยู่ส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลอันเป็นสิ่งเฉพาะตัวของบุคคลแต่ละคน ซึ่งสามารถนำไปสู่การพิสูจน์ตัวตนของบุคคลได้ อันได้แก่ ข้อมูลในเรื่องเกี่ยวกับประวัติส่วนตัวต่าง ๆ ไม่ว่าจะเป็นการศึกษาหรือการทำงาน ข้อมูลเกี่ยวกับการนับถือศาสนา ข้อมูลเกี่ยวกับสุขอนามัยส่วนบุคคล ข้อมูลประวัติอาชญากรหรือการถูกดำเนินคดีอาญา ข้อมูลอันเกี่ยวกับพฤติกรรมการใช้ชีวิต ทัศนคติ รสนิยม การเดินทาง การแสดงออก หรือการใช้บริการต่าง ๆ รวมถึงการทำธุรกรรมของบุคคลไม่ว่าจะเป็นกับทางภาครัฐหรือเอกชน ข้อมูลเหล่านี้จึงเป็นที่ต้องการและถูกล่วงละเมิดเพื่อประโยชน์ของผู้กระทำอย่างแพร่หลายและง่ายดาย ภายใต้การพัฒนาอย่างต่อเนื่องและก้าวกระโดดของเทคโนโลยีสารสนเทศ (information technology) ที่ทำให้การติดต่อสื่อสารผ่านระบบการสื่อสารอิเล็กทรอนิกส์และอินเตอร์เน็ตรวมไปถึงการสื่อสารรูปแบบใหม่ ๆ มีความรวดเร็ว และสามารถรองรับปริมาณข้อมูลได้อย่างมหาศาล การล่วงละเมิดความเป็นอยู่ส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลจึงสามารถกระทำได้อย่างง่ายดาย นานาอารยะประเทศจึงได้มีการพัฒนาหลักการขึ้นมาเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนี้

จึงถือเป็นที่ยอมรับว่าข้อมูลส่วนบุคคลเป็นสิทธิในความเป็นส่วนตัว อันสำคัญอย่างยิ่งต่อตัวผู้เป็นเจ้าของและเป็นสิทธิมนุษยชนขั้นพื้นฐานของมนุษย์ที่นานาอารยประเทศให้การยอมรับ ดังจะเห็นได้จากการบัญญัติรับรองไว้ในปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ.1948 (Universal Declaration of Human Rights 1948) ข้อ 12 ที่ว่า “บุคคลใดจะถูกแทรกแซงตามอำเภอใจในความเป็นส่วนตัว ครอบครัว ที่อยู่อาศัย หรือการสื่อสาร หรือจะถูกลบหลู่เกียรติยศหรือชื่อเสียงมิได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองของกฎหมายต่อการแทรกแซงหรือลบหลู่เช่นนั้น” รวมไปถึงยังมีการรับรองไว้ในกฎหมายหรือกฎเกณฑ์ระหว่างประเทศอีกหลายฉบับ ในระดับองค์การระหว่างประเทศ เช่น องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD) , สหภาพยุโรป (EU) แม้กระทั่งกลุ่มความร่วมมือทางเศรษฐกิจเอเชีย-แปซิฟิก (APEC) เอง ก็ให้ความสำคัญโดยการกำหนดกรอบ (framework) หรือแนวทาง (guidelines) เพื่อกำหนดมาตรฐานขั้นต่ำให้ประเทศสมาชิกของตนอ้างอิงเป็นฐานในการบัญญัติกฎหมายภายในประเทศของตนเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล รวมไปถึงกฎหมายของประเทศต่าง ๆ ก็ได้พัฒนาหลักการขึ้นมาเพื่อคุ้มครองสิทธิประเภทนี้

สำหรับประเทศไทย การคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลเริ่มมีการกำหนดไว้ในรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2535 (แก้ไขเพิ่มเติม พ.ศ. 2538) โดยได้บัญญัติคุ้มครอง “สิทธิในความเป็นส่วนตัว”ไว้ในมาตรา 47 และต่อมามีการนำมาบัญญัติไว้ในรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 มาตรา 34 เพื่อเป็นการกำหนดยืนยันหลักการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวว่า “สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียงหรือความเป็นอยู่ส่วนตัวย่อมได้รับความคุ้มครอง การกล่าวหรือไขข่าว แพรหลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชนอันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัวจะกระทำมิได้ เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณชน” บทบัญญัติมาตรานี้นำไปสู่ความพยายามตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลขึ้นทั้งในส่วนที่อยู่ในความครอบครองของทางภาคราชการและภาคเอกชน ซึ่งในส่วนทางภาคราชการได้มีการตรา พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 โดยช่วงระยะเวลาในระหว่างที่ประเทศไทยยังไม่มีกฎหมายกลางนั้น ประเทศไทยก็ได้มีการตรากฎหมายเฉพาะอื่น ๆ ออกมาหลายฉบับเพื่อคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในบางเรื่อง (ในรูปแบบกฎหมายเฉพาะ) เช่น พระราชบัญญัติการประกอบธุรกิจข้อมูลบัตรเครดิต พ.ศ. 2545 คุ้มครองสิทธิของเจ้าของข้อมูลเครดิต, พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 คุ้มครองสิทธิของเจ้าของข้อมูลประวัติสุขภาพ หรือพระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544 คุ้มครองสิทธิของเจ้าของข้อมูลในการติดต่อสื่อสารระหว่างกันของบุคคล ฯลฯ เป็นต้น

จนกระทั่งถึงวันที่ 28 พฤษภาคม พ.ศ. 2562 ก็ได้มีการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ออกมาใช้บังคับในที่สุด ซึ่งจะเห็นได้ว่าพัฒนาการทางกฎหมายที่จะกำหนดหลักการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลมีพัฒนาการที่ล่าช้ามากเมื่อเปรียบเทียบกับต่างประเทศ รวมถึงเมื่อเปรียบเทียบกับพัฒนาการทางเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็วนั้น การที่ประเทศไทยเพิ่งมีกฎหมายกลางที่จะมากำหนดคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลออกมาใช้บังคับอาจทำให้การบังคับใช้กฎหมายอาจต้องใช้ระยะเวลาในการปรับตัวอีกพอสมควร ทั้งทางด้านหลักการของกฎหมายและหลักการปฏิบัติรวมถึงความสามารถของผู้มีหน้าที่บังคับใช้กฎหมายเป็นต้น ประเด็นจึงน่าสนใจที่จะศึกษาว่า สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนี้ มีแนวคิดและพัฒนาการอย่างไร และมีพัฒนาการของการคุ้มครองสิทธินี้อย่างไรในประเทศไทย รวมไปถึงเราจะพัฒนาแนวคิดในเรื่องสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนี้อย่างไรต่อไป

วัตถุประสงค์ในการวิจัย

1. เพื่อศึกษาถึงแนวคิดและทฤษฎีอันเกี่ยวกับสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล
2. เพื่อศึกษาพัฒนาการในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของต่างประเทศ
3. เพื่อศึกษาวิเคราะห์พัฒนาการในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศไทยเพื่อเป็นแนวทางในการพัฒนากฎหมายต่อไป

ขอบเขตการวิจัย

ศึกษาวิเคราะห์หลักกฎหมายที่เกี่ยวข้องกับการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ตั้งแต่บทบัญญัติของรัฐธรรมนูญแห่งราชอาณาจักรไทยรวมถึงกฎหมายที่เกี่ยวข้องกับการรับรองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล โดยเฉพาะพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และกฎหมายฉบับอื่น ๆ รวมไปถึงกฎหมายของต่างประเทศ และกติการะหว่างประเทศที่เกี่ยวข้อง เพื่อนำมาเปรียบเทียบสำหรับการพัฒนากฎหมายคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศไทยต่อไป

วิธีการวิจัย

การศึกษาวิจัยเกี่ยวกับเรื่องนี้จะใช้การดำเนินการวิธีวิจัยเชิงคุณภาพ (qualitative research) โดยใช้รูปแบบการวิจัยเอกสาร (documentary research) เช่นตำราวิชาการ หนังสือ รายงานการวิจัย วิทยานิพนธ์ตลอดจนเอกสารจากฐานข้อมูลออนไลน์ทั้งในและต่างประเทศ รวมถึง วิธีการสัมภาษณ์เชิงลึก (Indepth-interviews) นักวิชาการและผู้มีประสบการณ์ที่เกี่ยวข้องในประเด็นของงานวิจัยอีกด้วย

ผลการวิจัย

สิทธิในความเป็นส่วนตัว เป็นสิทธิมนุษยชนที่ได้รับการยอมรับจากนานาอารยประเทศ และได้มีการบัญญัติรับรองไว้ในปฏิญญาสากลว่าด้วยสิทธิมนุษยชน มาตรา 12 โดยวางหลักการรับรองสิทธิความเป็นส่วนตัวนี้ไว้ว่า บุคคลใดจะถูกแทรกแซงตามอำเภอใจในความเป็นส่วนตัว ครอบครัว ที่อยู่อาศัยหรือการสื่อสาร หรือจะถูกลบหลู่เกียรติยศ และชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับการคุ้มครองของกฎหมายจากการแทรกแซงสิทธิหรือการลบหลู่ดังกล่าวนั้น

สิทธิในความเป็นส่วนตัว สามารถแบ่งแยกได้เป็น 4 ประเภท (บรรเจิด สิงคะเนติ, 2554, น.6-7) ดังนี้

1. สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล (information privacy)

เป็นสิทธิเหนือข้อมูลส่วนบุคคล ไม่ว่าจะเป็นข้อมูลใด ๆ ที่เกี่ยวข้องกับบุคคลธรรมดาที่อาจโดยทางตรงหรือโดยอ้อมโดยระบุหมายเลขประจำตัวประชาชน (เช่นหมายเลขประกันสังคม) หรืออย่างน้อยหนึ่งองค์ประกอบที่เป็นเอกลักษณ์ของบุคคลนั้น (เช่น ชื่อและนามสกุล, วันเดือนปีเกิด, ข้อมูลไบโอเมตริกซ์ ลายนิ้วมือ ดีเอ็นเอ ฯลฯ เป็นต้น)

2. สิทธิในความเป็นส่วนตัวเกี่ยวกับเนื้อตัวร่างกาย (bodily privacy)

ความเป็นส่วนตัวในชีวิตร่างกาย เป็นการให้ความคุ้มครองในชีวิตร่างกายของบุคคลในทางกายภาพที่จะไม่ถูกดำเนินการใด ๆ อันละเมิดความเป็นส่วนตัว อาทิ การทดลองทางพันธุกรรม การทดลองยา เป็นต้น

3. สิทธิในความเป็นส่วนตัวเกี่ยวกับการติดต่อสื่อสาร (privacy of communication)

เป็นการให้ความคุ้มครองในความปลอดภัย และความเป็นส่วนตัวในการติดต่อสื่อสารทางจดหมาย โทรศัพท์ ไปรษณีย์อิเล็กทรอนิกส์ หรือวิธีการติดต่อสื่อสารอื่นใดที่ผู้อื่นจะล่วงรู้มิได้

4 .สิทธิในความเป็นส่วนตัวเกี่ยวกับการอยู่หรือพักอาศัย (territorial privacy)

เป็นการกำหนดขอบเขตหรือข้อจำกัดที่บุคคลอื่นจะรุกล้ำเข้าไปในอาณาเขตแห่งสถานที่ส่วนตัวมิได้ ทั้งนี้ รวมทั้งการติดกล้องวงจรปิด และการตรวจสอบหมายเลขประจำตัวประชาชนของบุคคลเพื่อการเข้าที่พักอาศัย (ID Checks)

โดยในปัจจุบันสิทธิในความเป็นส่วนตัวประเภทแรก คือ สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนั้นประสบปัญหาในการถูกล่วงละเมิดเป็นอย่างมาก ทั้งนี้เพราะ ปัจจุบันข้อมูล (data) ถือเป็นสิ่งสำคัญ โดยเฉพาะอย่างยิ่งในยุคแห่งข้อมูลข่าวสารและยุคแห่งการติดต่อสื่อสารข้อมูลต่าง ๆ ซึ่งรวมไปถึงข้อมูลส่วนบุคคลจึงมีความสำคัญทั้งต่อการวางแผน ระบบการทำงานและการบริหารจัดการ การดำเนินกิจกรรมต่าง ๆ ไม่ว่าจะเป็นภาครัฐหรือเอกชน ดังนั้นจึงส่งผลให้เกิดความจำเป็นที่องค์กรต่าง ๆ ต้องมีข้อมูลไว้ในครอบครองไว้ให้มากที่สุด ซึ่งในข้อมูลข่าวสารจำนวนมากมายมหาศาลที่มีการครอบครอง หรือมีการแลกเปลี่ยน หรือแย่งชิงแข่งขันกันครอบครองจนเกิดภาวะของการล่วงละเมิดสิทธิในความเป็นส่วนตัวประเภทนี้อย่างแพร่หลายทั้งโดยที่เจ้าของข้อมูลรู้ตัวและไม่รู้ตัว

ด้วยเหตุผลข้างต้นทำให้นานาอารยประเทศจึงได้ให้ความสำคัญกับสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลเป็นอย่างยิ่ง จนได้มีการกำหนดมาตรการทางกฎหมายออกมาเพื่อคุ้มครองสิทธิ ไม่ว่าจะเป็นกฎหมายในระดับกติการะหว่างประเทศรวมถึงกฎหมายภายในรัฐของตน โดยกติการะหว่างประเทศที่สำคัญและมีพัฒนาการอย่างต่อเนื่องก็คือ

กรอบในการคุ้มครองข้อมูลขององค์การความร่วมมือและพัฒนาทางเศรษฐกิจ หรือ OECD (Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data (1980-2013) ของ (OECD: The Organization for Economic Cooperation and Development) ซึ่งมีหลักพื้นฐาน 8 ในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล 8 ประการ ดังนี้ (นคร เสรีรักษ์, 2557, น.147-149)

1) หลักข้อจำกัดในการเก็บรวบรวมข้อมูล
2) หลักคุณภาพของข้อมูล
3) หลักการกำหนดวัตถุประสงค์ในการจัดเก็บ
4) หลักข้อจำกัดในการนำไปใช้
5) หลักการรักษาความมั่นคงปลอดภัยข้อมูล 6) หลักการเปิดเผยข้อมูล
7) หลักการมีส่วนร่วมของบุคคล
8) หลักความรับผิดชอบ

นอกจากนี้ คณะมนตรีเศรษฐกิจและสังคมแห่งสหประชาชาติ (United Nations Economic and Social Council) ได้กำหนดหลักเกณฑ์เกี่ยวกับข้อมูลส่วนบุคคลไว้ในแนวทางการควบคุมข้อมูลส่วนบุคคลที่จัดเก็บด้วยคอมพิวเตอร์ (Guidelines for the Regulation of Computerized Personal Data Files) ซึ่งมีสาระสำคัญดังนี้

1) หลักความชอบด้วยกฎหมายและความเป็นธรรม (Principle of lawfulness and fairness) หมายความว่า ข้อมูลส่วนบุคคลจะต้องไม่ถูกเก็บรวบรวมหรือประมวลผลด้วยวิธีการที่ไม่เป็นธรรมหรือไม่ชอบด้วยกฎหมายและการใช้ข้อมูลส่วนบุคคลจะต้องไม่ขัดกับวัตถุประสงค์และหลักการของกฎบัตรสหประชาชาติ

2) หลักความถูกต้อง (principle of accuracy) หมายความว่า ในการเก็บรวบรวมข้อมูลส่วนบุคคล จะต้องมีการตรวจสอบอย่างสม่ำเสมอว่ากระทำด้วยความถูกต้อง ข้อมูลมีความสมบูรณ์ทันสมัยอยู่เสมอ และเก็บได้ภายในระยะเวลาเท่าที่จะมีการประมวลผลหรือใช้ข้อมูลเหล่านั้น

3) หลักการระบุวัตถุประสงค์โดยเฉพาะเจาะจง (Principle of the purpose specification) หมายความว่า ในการจัดเก็บข้อมูลต้องมีการระบุวัตถุประสงค์ในการจัดเก็บและเงื่อนไขของการใช้ประโยชน์ของข้อมูลที่เก็บตามวัตถุประสงค์ซึ่งชอบด้วยกฎหมายโดย

3.1) เก็บรวบรวมเพียงเท่าที่เกี่ยวข้องและเหมาะสมกับวัตถุประสงค์ที่ระบุ

3.2) ข้อมูลส่วนบุคคลจะต้องไม่ถูกใช้หรือเปิดเผย เว้นแต่ได้รับความยินยอมจากบุคคลที่เกี่ยวข้อง

3.3) ระยะเวลาที่จัดเก็บข้อมูลส่วนบุคคลจะต้องไม่เกินกว่าระยะเวลาที่การดำเนินการตามวัตถุประสงค์ที่ระบุไว้ได้สำเร็จลง

4) หลักการเข้าถึงข้อมูล (principle of interested-person access) หมายความว่า เจ้าของข้อมูลมีสิทธิที่จะได้รู้ว่ามีการประมวลผลข้อมูลข่าวสารที่เกี่ยวกับตนโดยได้รับข้อมูลในรูปแบบที่เข้าใจได้ในเวลาอันสมควรและปราศจากค่าใช้จ่าย และสามารถขอให้แก้ไขหรือลบในกรณีมีการเก็บข้อมูลโดยไม่ชอบด้วยกฎหมาย ไม่จำเป็น หรือมีการเก็บข้อมูลโดยไม่ถูกต้อง ข้อกำหนดแห่งหลักการนี้ให้บังคับใช้กับบุคคลทุกคนโดยไม่คำนึงถึงสัญชาติหรือถิ่นที่อยู่

5) หลักการไม่เลือกปฏิบัติ (principle of non-discrimination) หมายความว่า ห้ามเก็บรวบรวมข้อมูลซึ่งอาจทำให้เกิดการเลือกปฏิบัติที่ขัดต่อกฎหมาย เช่น ข้อมูลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ สีผิว พฤติกรรมทางเพศ ความคิดเห็นทางการเมือง การนับถือศาสนา ความเชื่อทางปรัชญาหรือความเชื่ออื่น ๆ รวมทั้งข้อมูลการเป็นสมาชิกสหภาพ หรือสมาคมทางการค้า

6) การกำหนดข้อยกเว้น (Power to make exceptions) หมายความว่า ข้อยกเว้นจากหลักการข้อที่ 1 ถึงข้อที่ 4 อาจกำหนดได้ในกรณีจำเป็นเพื่อรักษาความมั่นคงของชาติ ระเบียบสังคม สาธารณสุข หลักคุณธรรม และสิทธิและเสรีภาพของบุคคลอื่น

ข้อยกเว้นจากหลักการข้อที่ 5 อาจเป็นกรณีเพื่อการป้องกันการเลือกปฏิบัติ ภายใต้ข้อบัญญัติของปฏิญญาสากลว่าด้วยสิทธิมนุษยชนหรือกลไกของกฎหมายอื่น ๆ ที่เกี่ยวกับการคุ้มครองสิทธิมนุษยชนและการป้องกันการเลือกปฏิบัติ

7) หลักการรักษาความปลอดภัย (Principle of security) หมายความว่า ต้องมีการรักษาความปลอดภัยข้อมูลที่จัดเก็บ เพื่อป้องกันอันตรายทั้งจากภัยธรรมชาติ การสูญหายหรือเสียหาย การทำลายโดยบุคคล การเข้าถึงโดยปราศจากอำนาจ การใช้ในทางที่ผิด หรือการทำลายโดยไวรัสคอมพิวเตอร์

8) การกำกับดูแล (supervision of sanctions) หมายความว่า กฎหมายของประเทศต่าง ๆ จะต้องระบุหน่วยงานที่รับผิดชอบในการควบคุมดูแลและให้คำแนะนำเกี่ยวกับการปฏิบัติตามหลักการนี้

9) การส่งข้อมูลข้ามพรมแดน (tran border data flows) หมายความว่า การส่งข้อมูลระหว่างประเทศจะสามารถกระทำได้ในกรณีที่ประเทศสองประเทศหรือมากกว่าสองประเทศมีกลไกในการคุ้มครองสิทธิความเป็นส่วนตัวในระดับเดียวกัน

10) ขอบเขตการใช้ข้อปฏิบัติ (field of application) หมายความว่า หลักปฏิบัติดังกล่าวควรได้มีการปฏิบัติใช้สำหรับข้อมูลในภาครับและเอกชนที่จัดเก็บด้วยคอมพิวเตอร์ (computerized files) เช่นเดียวกับการจัดเก็บด้วยวิธีการอื่น ๆ ที่มีการปรับปรุงให้เหมาะสมกับเอกสารที่จัดเก็บด้วยมือ (manual files)

แต่ในส่วนของพัฒนาการในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลที่โดยเด่นและมีผลกระทบต่อประเทศไทยอย่างมาก ก็คือ หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ลำดับของการตราออกมาหลายฉบับไม่ว่าจะเป็น EU’s Data Protection Directive (Directive 95/46/EC 1995) จนกระทั่งถึงฉบับล่าสุดก็คือ General Data Protection Regulation (GDPR)

เมื่อพิจารณากติกาฉบับต่าง ๆ ของสหภาพยุโรปแล้วจะเห็นพัฒนาการของหลักการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลดังนี้ กล่าวคือในปี ค.ศ. 1995 สหภาพยุโรปได้ออกหลักเกณฑ์ฉบับหนึ่งเรียกว่า "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of person data and on the free movement of such data" ทั้งนี้เพื่อผลักดันให้กฎหมายในกลุ่มประเทศสมาชิกมีความสอดคล้องกัน ในการให้หลักประกันที่ดีเพียงพอต่อการคุ้มครองความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของพลเมืองของสหภาพยุโรป และเพื่อทำให้การส่งผ่านข้อมูลส่วนบุคคลภายในประเทศสมาชิกเป็นไปโดยเสรีปราศจากข้อจำกัดที่เกิดจากความแตกต่างกันของกฎหมายหรือกฎเกณฑ์ภายในของประเทศต่าง ๆ ซึ่งสามารถสรุปสาระสำคัญของหลักเกณฑ์ในการคุ้มครองข้อมูลได้ดังนี้ คือ

1) ต้องมีการรักษาคุณภาพของข้อมูล
2) ต้องมีมาตรฐานของการประมวลผลข้อมูลที่ชอบด้วยกฎหมาย
3) การประมวลผลข้อมูลชนิดพิเศษต้องมีการดูแลเป็นพิเศษ
4) ต้องมีการกำหนดสิทธิในการได้รับแจ้งข้อมูลต่าง ๆ ของเจ้าของข้อมูล
5) ต้องมีการกำหนดสิทธิในการเข้าถึงข้อมูลของเจ้าของข้อมูล
6) ต้องมีการกำหนดสิทธิในการคัดค้านการประมวลผลข้อมูลของเจ้าของข้อมูล
7) ต้องมีการรักษาความปลอดภัยในการประมวลผลข้อมูล
8) การส่งผ่านข้อมูลส่วนบุคคลไปยังประเทศที่สามต้องมีมาตรฐานในการคุ้มครองข้อมูล

ต่อมาได้มีการทบทวนและเตรียมการเพื่อปรับปรุงหลักการคุ้มครองข้อมูลส่วนบุคคลตลอดมาจนกระทั่งวันที่ 27 พฤษภาคม ค.ศ. 2016 ทาง EU Commission ได้รับรอง General Data Protection Regulation 2016 (Regulation 2016/679) ซึ่งร่างกติกาฉบับนี้ใช้เวลาเตรียมการร่างและประชุมปรึกษาหารือกันถึง 4 ปี โดยจะให้มีผลบังคับในวันที่ 25 พฤษภาคม ค.ศ. 2018 ซึ่งถือเป็นการเปลี่ยนแปลงหลักการครั้งใหญ่ที่สุดในรอบ 20 ปี ซึ่งทั้งนี้ การกำหนดระยะเวลาในการบังคับใช้ยาวนานถึง 2 ปีนับแต่วันที่กฎหมายผ่านก็เพื่อที่จะให้องค์กรทางธุรกิจต่าง ๆ มีเวลาปรับตัวและเตรียมการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของลูกค้าหรือเจ้าของข้อมูลอย่างถูกต้องตามหลักการอันเป็นมาตรฐานขั้นต่ำใหม่ของ General Data Protection Regulation ไม่เช่นนั้นจะถูกลงโทษเป็นค่าปรับในอัตราที่สูงมากคือ 20 ล้านยูโร ซึ่ง General Data Protection Regulation 2016 มีสาระสำคัญดังต่อไปนี้

ก. วัตถุประสงค์

General Data Protection Regulation 2016 ถูกกำหนดขึ้นเพื่อให้ประชาชนมีสิทธิควบคุมข้อมูลส่วนบุคคลของตน ซึ่งถือเป็นสิทธิขั้นพื้นฐาน และกำหนดให้สหภาพยุโรปมีมาตรฐานการคุ้มครองข้อมูลที่เป็นอันหนึ่งอันเดียวเพื่อให้เกิดการเคลื่อนย้ายโดยเสรีของข้อมูล

ข. ขอบเขตการบังคับใช้

มาตรการคุ้มครองสิทธินั้นยังคงบังคับใช้แก่การประมวลผลเช่นเดิม แต่มีขยายขอบเขตการบังคับ (territorial scope) โดยกำหนดให้กติกาจะมีผลบังคับต่อบุคคลดังต่อไปนี้

1. ประชาชนและธุรกิจที่จัดตั้งใน EU ได้รับการคุ้มครองข้อมูลส่วนบุคคลภายใต้กฎหมายนี้ไม่ ว่าการประมวลผลข้อมูลนั้นจะเกิดขึ้นใน EU หรือนอก EU

2. ข้อมูลส่วนบุคคลจะโอนไปยังผู้ประกอบการนอกสหภาพ ยุโรปได้ก็ต่อเมื่อประเทศปลายทางมีระดับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลเทียบเท่าสหภาพยุโรป

3. หากผู้ประมวลผลข้อมูลนอกยุโรปให้บริการหรือขายสินค้าให้กับผู้บริโภคชาว ยุโรป หรือ “สังเกตพฤติกรรม” ของชาวยุโรป ผู้ประกอบการจะต้องตกอยู่ภายใต้บังคับของกฎหมายฉบับนี้ด้วย

ค. สาระสำคัญ

สำหรับสาระสำคัญ ของ General Data Protection Regulation 2016 มีดังนี้

1) ให้ประชาชนเข้าถึงข้อมูลส่วนบุคคลของตนได้ง่ายและไม่มีค่าใช้จ่าย

2) แจ้งให้ทราบถึงวัตถุประสงค์ ต้องมีความโปร่งใสในการรวบรวมข้อมูลส่วนบุคคล

3) เมื่อมีการนำข้อมูลไปประมวลผล จะต้องได้รับความยินยอมที่ชัดเจนจากเจ้าของข้อมูล (clear and affirmative consent)

4) การใช้ข้อมูลควรเป็นไปตามวัตถุประสงค์ที่แจ้งเท่านั้น

5) จัดให้มีระบบการคุ้มครองข้อมูลส่วนบุคคลตั้งแต่ขั้นแรกของการ ออกแบบบริการ และให้การตั้งค่าเป็นมิตรต่อการคุ้มครองข้อมูลส่วนบุคคล (privacy-friendly setting)

6) ให้สิทธิประชาชนในการขอข้อมูลส่วนบุคคลของตนจากผู้ประกอบการเพื่อโอนข้อมูลนั้นไปยัง ผู้ประกอบการอื่นได้

7) ให้สิทธิเจ้าของข้อมูลส่วนบุคคลเรียกร้องให้มีการลบข้อมูลของตนออกจากระบบเมื่อไม่มี ความจำเป็นที่ผู้ประกอบการจะต้องเก็บข้อมูลนั้นไว้ หรือเจ้าของข้อมูลไม่ประสงค์ให้นำข้อมูลดังกล่าวไป ประมวลผลอีกต่อไป

ซึ่งความเปลี่ยนแปลงที่กล่าวมาข้างต้นนี้ มีประเด็นความแตกต่างที่น่าสนใจก็คือ

1. การบังคับใช้กฎหมายนอกอาณาเขต (extraterritorial applicability) กล่าวคือ เมื่อมีการกำหนดนิยามของข้อมูลข้ามพรมแดนชัดเจน ทำให้ไม่เกิดความสับสนในการจัดการข้อมูลข้ามแดน ไม่จำต้องพิจารณาว่าควรใช้กฎหมายฉบับไหนของประเทศใดมาบังคับ เพราะผู้รับข้อมูลต้องทำตามหลักการของ General Data Protection Regulation เหมือนกันทั้งสิ้น

2. กำหนดบทลงโทษรุนแรงขึ้น กล่าวคือ หากพบว่ามีการปฏิบัติผิดไปจากหลักการของ General Data Protection Regulation องค์กรจะต้องจ่ายค่าปรับ 4% ของผลประกอบการรายได้ทั่วโลกทั้งหมด หรือสูงถึง 20 ล้านยูโร ซึ่งบทลงโทษนี้จะบังคับใช้ทั้งหน่วยงานผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล

3. กำหนดการขอความยินยอมจากเจ้าของข้อมูล (consent) จะต้องใช้ภาษาที่ชัดเจน กระชับ และเข้าใจง่าย เช่นเดียวกับกรณีของการถอนความยินยอม

4. กำหนดการแจ้งเตือนเมื่อเกิดเหตุข้อมูลรั่ว (breach notification) กล่าวคือ หากพบว่าข้อมูลรั่วไหล หน่วยงานผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลต้องแจ้งให้หน่วยงานกำกับดูแล และประชาชนทราบภายใน 72 ชั่วโมง

5. สิทธิในการเข้าถึง (right to access) ใน General Data Protection Regulation ได้มีการขยายขอบเขตสิทธิของเจ้าของข้อมูล ที่ผู้ควบคุมข้อมูล ต้องแจ้งเจ้าของข้อมูลว่าข้อมูลถูกใช้เอาไปใช้เพื่อวัตถุประสงค์ใด และต้องจัดทำสำเนาข้อมูลให้กับเจ้าของข้อมูลในรูปแบบอิเล็กทรอนิกส์ โดยห้ามเก็บค่าใช้จ่ายเพิ่ม

6. มีการกำหนดสิทธิที่จะถูกลืม (right to be forgotten) กล่าวคือเจ้าของข้อมูลสามารถขอให้หน่วยงานควบคุมข้อมูลลบข้อมูลของตัวเองออกได้ นอกจากนั้นข้อมูลที่ไม่มีความเกี่ยวข้องกับจุดประสงค์ของการประมวลผลก็ต้องเอาออกด้วยเช่นกัน

7. มีการกำหนดสิทธิในการโอนย้ายข้อมูลของตนจากผู้ประกอบการหนึ่งไปยังผู้ประกอบการอื่นได้ (data portability)

8. กำหนดให้ความสำคัญกับความเป็นส่วนตัวตั้งแต่การออกแบบ (Privacy by Design) คือการให้หน่วยงานควบคุมข้อมูลตระหนักความสำคัญของข้อมูล โดยเริ่มจากการออกแบบบริการที่คิดถึงการป้องกันข้อมูลตั้งแต่แรกเลย ไม่ใช่ออกแบบแล้ว ค่อยมาเพิ่มเรื่องการป้องกันข้อมูล และใช้มาตรการทางเทคนิคที่เหมาะสมและมีประสิทธิภาพในการป้องกันข้อมูล

9. กำหนดให้ต้องมีเจ้าหน้าที่คุ้มครองข้อมูล หรือ Data Protection Officers (DPO) จากเดิมที่องค์กรต้องแจ้งกิจกรรมการประมวลผลข้อมูลต่อหน่วยงานท้องถิ่น (local data protection authority) ที่เป็นข้อบังคับตามกฎหมายเดิม (Data Protection Act 1998) ภายใต้หลักการของ General Data Protection Regulation นี้ไม่ต้องแจ้งอีกแล้วแล้ว แต่ต้องมีการว่าจ้างเจ้าหน้าที่คุ้มครองข้อมูล หรือ DPO เข้ามาในบริษัทเลย

เมื่อพิจารณาแล้วจะเห็นว่า General Data Protection Regulation ไม่ได้ตราขึ้นในลักษณะที่เป็นการยกเลิกหลักการเดิม เพียงแต่มีการกำหนดขยายความคุ้มครองข้อมูลส่วนบุคคลให้ชัดเจนมากขึ้นและให้เป็นมาตรฐานเดียวกันทั่วยุโรป และมีประเด็นที่สำคัญก็คือ มีการกำหนดคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประชาชนซึ่งเป็นพลเมืองของสหภาพยุโรป ไม่ว่าข้อมูลนั้นจะอยู่ที่ทวีปใดหรือส่วนใด ๆ ของโลกก็ตาม สิทธิเหนือข้อมูลนั้นก็ยังคงได้รับความคุ้มครอง

ต้องยอมรับว่าแต่เดิม สหภาพยุโรปมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่มีมาตรฐานในการคุ้มครองสิทธิสูงมากอยู่แล้ว ซึ่งจะตั้งอยู่บนพื้นฐานร่วมกันเหล่านี้คือ

ประการแรก หน่วยงานควบคุมข้อมูลที่เจ้าของข้อมูลรับบริการ (data controller) ต้องได้รับความยินยอมจากเจ้าของข้อมูล (data subject) ในการจัดเก็บข้อมูล รวมทั้งต้องกำหนดขอบเขต วัตถุประสงค์ในการประมวลผลข้อมูลที่ชัดเจน

ประการที่สอง ทุกประเทศในสหภาพยุโรปต้องให้การคุ้มครองอย่างเคร่งครัดต่อข้อมูลที่อ่อนไหวเป็นพิเศษ เช่น ความคิดทางการเมือง ศาสนา ลัทธิ พฤติกรรมสุขภาพ พฤติกรรมทางเพศ การเป็นสมาชิกสหพันธ์ ประวัติอาชญากรรม ฯลฯ เป็นต้น

ประการที่สาม การส่งข้อมูลไปต่างประเทศ หรือบริษัทที่อยู่ต่างประเทศ ผู้รับข้อมูลต้องมีการคุ้มครองข้อมูลมาตรฐานเดียวกับบริษัทในยุโรป

ประการที่สี่ หน่วยงานควบคุมข้อมูลต้องกำหนดขอบเขต ระยะเวลาในการประมวลผล และมีมาตรการรักษาความปลอดภัยข้อมูลอย่างรัดกุม

กล่าวได้ว่า General Data Protection Regulation ถูกตราขึ้นมาเพื่อวัตถุประสงค์ในการยกระดับมาตรฐานคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลให้มีความชัดเจนและคุ้มครองเป็นการทั่วไป (general) รวมไปถึงกำหนดการบังคับใช้ให้เหมือนกันในทุกประเทศสมาชิกของสหภาพยุโรป ซึ่งต่างจากก่อนหน้านี้ ที่ สภาพยุโรปกำหนดเพียงหลักการเบื้องต้นให้ซึ่งก็แล้วแต่ละประเทศไปดำเนินการร่างกฎหมายและกำหนดบทลงโทษกันเอง และประเด็นสำคัญอีกประการหนึ่งที่ General Data Protection Regulation ถูกกำหนดให้ชัดเจนคือ การส่งข้อมูลระหว่างประเทศ ไม่ต้องสับสนอีกต่อไปว่าจะจัดการอย่างไร เพราะระบุชัดเจนว่า ผู้รับข้อมูลซึ่งอาจจะเป็นบริษัทคลาวด์หรือบริษัทประมวลผลข้อมูล (data Processer) ที่แม้อยู่ต่างประเทศนอกขอบเขตของประเทศสมาชิก EU ก็ต้องทำตามหลักการของ General Data Protection Regulation ที่ได้วางหลักคุ้มครองสิทธิขั้นพื้นฐานนี้ไว้

เมื่อย้อนมาพิจารณาแนวคิดนี้ในประเทศไทยของเราจะเห็นพัฒนาการของแนวคิดดังนี้

1. ช่วงระยะเวลาของการเริ่มต้นคุ้มครองโดยกฎหมายเอกชนและกฎหมายอาญา

การคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ภายใต้ระบบกฎหมายไทยในอดีตเป็นการดำเนินการตามกรอบการคุ้มครองภายใต้กฎหมายว่าด้วยความรับผิดต่อความเสียหายต่อสิทธิส่วนตัว ซึ่งถือว่าได้รับการพิจารณาอยู่ในขอบเขตการคุ้มครองตามกฎหมายแพ่งและกฎหมายอาญา ไม่ว่าจะเป็นการคุ้มครองสิทธิของบุคคลไม่ให้ผู้อื่นล่วงละเมิดบนฐานมาตรา 420 ของประมวลกฎหมายแพ่งและพาณิชย์ รวมถึงฐานความผิดต่อความเป็นส่วนตัวฐานต่าง ๆ ตามประมวลกฎหมายอาญา ซึ่งการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลภายใต้บทบัญญัติของประมวลกฎหมายแพ่งและพาณิชย์และประมวลกฎหมายอาญานั้นยังมีประเด็นปัญหาในการคุ้มครองดังนี้ (กิตติพงศ์ กมลธรรมวงศ์, 2549, น.250-252)

1. ประมวลกฎหมายแพ่งและพาณิชย์และประมวลกฎหมายอาญาเป็นกฎหมายที่คุ้มครองสิทธิในข้อมูลส่วนบุคคลในฐานะที่เป็นสิทธิในความเป็นส่วนตัวทั่วไป เช่นเดียวกับสิทธิอื่น ๆ เช่น สิทธิในทรัพย์สิน ร่างกาย อนามัย ฯลฯ โดยไม่ได้มุ่งคุ้มครองเฉพาะสิทธิในความเป็นส่วนตัวที่เกี่ยวกับข้อมูลส่วนบุคคลอันเป็นเรื่องเฉพาะข้อมูลส่วนบุคคลโดยตรง ทั้งที่สาระสำคัญของสิทธินี้มีความแตกต่างจากสิทธิอื่น ๆ ซึ่งสิทธิของบุคคลตามประมวลกฎหมายแพ่งและพาณิชย์และประมวลกฎหมายอาญานั้นจะได้รับการคุ้มครองก็ต่อเมื่อได้เกิดมีความเสียหายขึ้นแล้ว การชดใช้ค่าเสียหายที่เกิดขึ้นจึงเป็นมาตรการในการ “เยียวยา” มากกว่าที่จะเป็นการ “ป้องกัน” ซึ่งขัดแย้งกับหลักการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลที่มุ่งจะให้ความคุ้มครองในลักษณะของการป้องกัน

2. กฎหมายทั้งสองผลักภาระการพิสูจน์ให้แก่ผู้เสียหาย

3. กฎหมายทั้งสองขาดบทบัญญัติเกี่ยวกับหลักเกณฑ์ วิธีการ เงื่อนไข และมาตรการที่จำเป็นและเฉพาะเจาะจงเพื่อให้หลักประกันในเรื่องนี้ได้อย่างเพียงพอตามหลักสากล

2. ช่วงระยะเวลาแห่งการสร้างกฎหมายมหาชนขึ้นมาเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล

นับแต่ที่ประเทศไทยได้มีการประกาศใช้รัฐธรรมนูญ พ.ศ. 2540 ซึ่งได้รับการยอมรับว่าเป็นรัฐธรรมนูญที่มีความเป็นประชาธิปไตยมากที่สุดฉบับหนึ่งของประเทศ ก็ได้มีการตราพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 ออกมาใช้บังคับ ซึ่งกล่าวได้ว่าเป็นเพียงกฎหมายฉบับเดียว ในขณะนี้ที่ได้มีการกำหนดนิยามของคำว่า “ข้อมูลส่วนบุคคล” เอาไว้ และได้มีการกำหนดหลักเกณฑ์การจัดการระบบข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของรัฐเอาไว้ด้วย โดยในมาตรา 4 ของพระราชบัญญัติข้อมูลข่าวสารของทางราชการได้มีการบัญญัติไว้ดังนี้

“ข้อมูลข่าวสารส่วนบุคคล หมายความว่า ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะ การเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้นหรือมีเลขหมาย รหัสหรือ สิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่าย และให้หมายความ รวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย”

สาระสำคัญของการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในกฎหมายฉบับนี้ ได้วางหลักการให้ต้องมีการจัดระบบข้อมูลส่วนบุคคลโดยอยู่บนพื้นฐานของความจำเป็นและต้องเก็บเพื่อการดำเนินงานของหน่วยงานรัฐให้สำเร็จตามวัตถุประสงค์ และเมื่อวัตถุประสงค์ได้สำเร็จแล้วจะต้องยกเลิกการจัดระบบข้อมูลดังกล่าวทันทีที่หมดความจำเป็น นอกจากนี้จะต้องมีการตรวจสอบและแก้ไขข้อมูลข่าวสารส่วนบุคคลให้ถูกต้องอยู่เสมอ มีการจัดระบบรักษาความปลอดภัยให้แก่ข้อมูลเพื่อป้องกันมิให้มีการนำไปใช้โดยไม่เหมาะสมหรือเป็นผลร้ายต่อเจ้าของข้อมูล อีกทั้งในกรณีที่จะมีการเก็บข้อมูลข่าวสารโดยตรงจากเจ้าของข้อมูล หน่วยงานของรัฐจะต้องแจ้งให้เจ้าของข้อมูลทราบล่วงหน้าหรือพร้อมกับการขอข้อมูล และจะต้องแจ้งให้ทราบถึงกรณีที่จะมีการจัดส่งข้อมูลข่าวสารส่วนบุคคลไปยังที่ใด ๆ ซึ่งจะเป็นผลให้บุคคลทั่วไปทราบข้อมูลข่าวสารนั้น

นอกจากนี้กฎหมายฉบับนี้ยังได้กำหนดสาระสำคัญคือ ห้ามหน่วยงานของรัฐเปิดเผยข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความควบคุมดูแลของตนต่อหน่วยงานของรัฐแห่งอื่นหรือผู้อื่นโดยปราศจากความยินยอม เว้นแต่ในกรณีที่เป็นไปเพื่อประโยชน์สาธารณะ

จากหลักการของพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 ยังมีปัญหาในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลดังนี้คือ

1. พระราชบัญญัติข้อมูลข่าวสารของทางราชการไม่ได้กำหนดคุ้มครองระบบการจัดเก็บและการใช้ข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานภาคเอกชน

2. แม้คณะกรรมการข้อมูลข่าวสารของราชการจะมีอำนาจควบคุมดูแลองค์กรประกอบวิชาชีพด้วย แต่ไม่ได้ครอบคลุมถึงอำนาจในการให้ความเห็นชอบประมวลหรือกฎเกณฑ์เกี่ยวกับจริยธรรมในวิชาชีพขององค์กรวิชาชีพที่จัดตั้งขึ้นตามกฎหมาย ในขณะที่กฎหมายของต่างประเทศที่ได้มีการพัฒนาใหม่ มักมีการกำหนดให้องค์กรที่ทำหน้าที่ควบคุมดูแลข้อมูลส่วนบุคคลมีอำนาจให้ความเห็นชอบประมวลจริยธรรมวิชาชีพที่องค์กรหรือหน่วยงานตามกฎหมายควบคุมวิชาชีพจัดทำขึ้นตามกฎหมายนั้น ๆ ด้วย

3. คณะกรรมการข้อมูลข่าวสารของทางราชการไม่มีอำนาจสืบสวนสอบสวนการกระทำที่ฝ่าฝืนการคุ้มครองข้อมูลส่วนบุคคล (investigation power) ตัวอย่างเช่นอำนาจของคณะกรรมการ ป.ป.ช. ในเรื่องทุจริตคอร์รัปชั่นในภาครัฐ

นอกจากนี้ ในแง่ของอำนาจจะเห็นได้ว่า คณะกรรมการข้อมูลข่าวสารมีเพียงอำนาจในการเรียกให้บุคคลมาให้ถ้อยคำหรือส่งวัตถุเอกสารหรือพยานหลักฐานมาประกอบการพิจารณาเท่านั้น ถ้าหากมีการฝ่าฝืนก็มีบทลงโทษก็มีเพียงระวางโทษจำคุก ไม่เกิน 3 เดือน หรือปรับไม่เกินห้าพันบาท หรือทั้งจำทั้งปรับเท่านั้น แต่ไม่มีบทลงโทษกรณีหน่วยงานรัฐฝ่าฝืนไม่ปฏิบัติตามกฎหมาย ซึ่งเมื่อพิจารณาจากความซับซ้อนและความเสียหายอันจะเกิดในกรณีเกี่ยวกับการล่วงละเมิดข้อมูลส่วนบุคคล อำนาจของคณะกรรมการข้อมูลข่าวสารของราชการดูจะไม่เพียงพอกับการคุ้มครองสิทธิเสรีภาพของประชาชนในปัจจุบัน

นอกจากนี้ การตรากฎหมายขึ้นมาเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศไทย ไม่ได้มีการตราไว้ในกฎหมายฉบับเดียว แม้ว่าจะมีพระราชบัญญัติข้อมูลข่าวสารของทางราชการเป็นกฎหมายหลัก แต่ก็มีขอบเขตของการคุ้มครองที่จำกัดไม่ได้ครอบคลุมไปถึงข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของภาคเอกชนซึ่งมีปริมาณข้อมูลที่จัดเก็บเป็นจำนวนมากไม่น้อยไปกว่าข้อมูลที่อยู่กับภาครัฐ ไม่ว่าจะเป็นข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของบรรดาธนาคารเอกชน โรงพยาบาลเอกชน โรงแรม ห้างสรรพสินค้า หรือบรรษัทห้างร้านที่จำหน่ายสินค้า ผลิตภัณฑ์ หรือให้บริการที่มีการจัดเก็บข้อมูลของลูกค้าไว้ เมื่อพิจารณาประกอบกับความก้าวหน้าทางด้านเทคโนโลยีอันได้อธิบายมาแล้ว ก็จะทำให้เห็นถึงความเสี่ยงที่จะมีการล่วงละเมิดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลได้โดยง่าย โดยที่ระบบกฎหมายของไทยยังไม่สามารถให้ความคุ้มครองได้อย่างมีประสิทธิภาพ

แต่อย่างไรก็ดี อย่างน้อยเราก็เห็นได้ถึงความพยายามของรัฐในอันที่จะใช้กฎหมายมหาชนเป็นเครื่องมือในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ซึ่งก็คือพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ที่รับหลักการมาจากบทบัญญัติของรัฐธรรมนูญ พ.ศ. 2540 มาตรา 34 และมาตรา 58 ซึ่งได้กำหนดหลักการคุ้มครองข้อมูลข่าวสารของบุคคลในฐานะที่เป็นส่วนหนึ่งของสิทธิส่วนบุคคลนั้นเอง

3. ช่วงระยะเวลาของการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

กฎหมายคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล เป็นกฎหมายอีกฉบับหนึ่งที่มีระยะเวลาในการเสนอเพื่อให้มีการตรากฎหมายผ่านสภาอย่างยาวนานมาก กล่าวคือ นับจากระยะเวลาที่เริ่มปรากฏแนวคิดในการรับรองสิทธิในความเป็นส่วนตัว ก็คือ รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2517 ที่มีการบัญญัติรับรองและคุ้มครองการติดต่อสื่อสารถึงกันโดยทางไปรษณีย์ ได้แก่จดหมาย โทรเลข โทรศัพท์ หรือสิ่งสื่อสารอื่นใดที่บุคคลติดต่อถึงกัน ไว้ในมาตรา 46 และต่อมาในรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2535 (แก้ไขเพิ่มเติม ฉบับที่ 5 พ.ศ. 2538) ได้มีการบัญญัติรับรองและคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว ไว้ในมาตรา 47 จนกระทั่งถึงรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2540 ก็ได้มีการบัญญัติรับรองและคุ้มครองสิทธิในข้อมูลข่าวสารไว้ในมาตรา 34 และมาตรา 58 จนกระทั่งถึงรัฐธรรมนูญฉบับปัจจุบัน คือ รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2560 ก็ยังคงมีการบัญญัติรับรองและคุ้มครองสิทธินี้ไว้ในมาตรา 32

แต่อย่างไรก็ดี พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลที่ได้มีการริเริ่มที่จะตราขึ้นเป็นกฎหมาย นับตั้งแต่ปี พ.ศ. 2540 กว่าจะตราขึ้นเป็นกฎหมายได้รวมระยะเวลากว่า 20 ปี จนกระทั่งเมื่อวันที่ 27 พฤษภาคม 2562 ราชกิจจานุเบกษาเผยแพร่ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ พระราชบัญญัติข้อมูลส่วนบุคคลฯ ซึ่งผ่านการพิจารณาโดยสภานิติบัญญัติแห่งชาติ (สนช.) ในช่วง "สุดท้าย" ก่อนที่สภาแต่งตั้งจะหมดอายุลง ซึ่งกฎหมายฉบับที่ผ่านในยุคของรัฐบาลโดยแม้จะมีการวางหลักการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลไว้ แต่ก็มีการวางข้อยกเว้นไว้อย่างกว้างขวาง โดยเฉพาะการยกเว้นไม่คุ้มครองข้อมูลในกิจการของหน่วยงานความมั่นคง และแทบจะยกเว้นให้กิจการของรัฐไม่ต้องทำตามกฎหมาย ดังนั้นการบังคับใช้กฎหมายฉบับนี้จึงมุ่งเน้นไปที่ผู้ประกอบการภาคธุรกิจเป็นหลัก

โดยหลักการและเหตุผลของร่างพระราชบัญญัติ ที่ได้นำเสนอต่อคณะรัฐมนตรีนั้นมีว่า “เนื่องจากปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคล เป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว สามารถทำได้โดยง่าย สะดวก และรวดเร็ว รวมทั้งก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวมที่ใช้เทคโนโลยีดิจิทัลอย่างแพร่หลาย แม้ว่าจะได้มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลในบางเรื่อง แต่ก็ยังไม่มีหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป สมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครอง ข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้น จึงจำเป็นต้องตราพระราชบัญญัตินี้”

จากหลักการและเหตุผลข้างต้น จะเห็นได้ว่า เหตุผลสำคัญที่ประเทศไทยต้องตรากฎหมายคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวข้อมูลส่วนบุคคลฉบับนี้ ก็คือ

1. ก่อนหน้านี้ประเทศไทยยังไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคล ซึ่งทำให้ไม่มีหลักประกันในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ซึ่งเป็นสิทธิมนุษยชนขั้นพื้นฐาน ในขณะที่นานาอารยประเทศ ไม่ว่าจะเป็นประเทศในแถบยุโรป อเมริกาใต้ ได้มีการตรากฎหมายเพื่อมาคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลและวางระบบการเยียวยาความเสียหายอันเกิดจากละเมิดเป็นที่เรียบร้อยแล้ว

2. จัดสร้างกลไกในการปกป้องสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล โดยพยายามรักษาดุลยภาพของการคุ้มครองสิทธิของบุคคลในความเป็นส่วนตัว (right of privacy) เสรีภาพในการไหลเวียนของข้อมูลข่าวสาร (free flow of Information) และความมั่นคงของประเทศ (national security) เพื่อเป็นโครงสร้างพื้นฐานสารสนเทศที่มั่นคงในช่วงระยะเวลาแห่งข้อมูลข่าวสาร ภายใต้หลักการปกครองระบอบประชาธิปไตยและหลักนิติรัฐ

3. เพื่อสนับสนุนการทำธุรกรรมทางอิเล็กทรอนิกส์ เนื่องในปัจจุบันการพัฒนาการทางเทคโนโลยีสารสนเทศมีความก้าวหน้าอย่างรวดเร็ว ทำให้มีการนำเอาเทคโนโลยีมาประยุกต์ใช้ให้เกิดประโยชน์กับเศรษฐกิจและสังคมมากมาย โดยเฉพาะการประมวลผลข้อมูลส่วนบุคคลอันสามารถทำได้อย่างสะดวกและรวดเร็ว จึงมีความจำเป็นออกกฎหมายมาคุ้มครองข้อมูลส่วนบุคคลซึ่งมีการใช้อย่างแพร่หลายในยุคสังคมสารสนเทศ

4. เพื่อปรับตัวให้สอดคล้องกับการออกกติกาของสหภาพยุโรป (EU) ซึ่งก็คือ GDPR อันมีลักษณะของการเป็น Normative Power และมีขอบเขตการบังคับออกไปนอกพื้นที่ของสหภาพยุโรป ส่งผลให้ภาคธุรกิจ รวมถึงรัฐที่มีการติดต่อปฏิสัมพันธ์ในทางการค้ากับสหภาพยุโรปต้องเร่งรีบปรับตัวโดยการตรากฎหมายที่มีมาตรฐานของการคุ้มครองข้อมูลส่วนบุคคลไม่ต่ำไปกว่าที่กำหนดโดย GDPR

เมื่อพิจารณาสาระสำคัญของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พบว่ามีสาระสำคัญ ดังนี้คือ

1. การเก็บข้อมูล ใช้ข้อมูล เปิดเผยข้อมูล ซึ่งเป็นการกระทำที่กระทบต่อสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของเจ้าของข้อมูลจะต้องได้รับความยินยอมเสมอ

หลักการทั่วไปนี้เขียนไว้ชัดเจนในมาตรา 19 ที่ว่า "ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้ หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น เว้นแต่บทบัญญัติ แห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้"

โดยกฎหมายฉบับนี้ได้กำหนดให้การกระทำใด ๆ กับข้อมูลส่วนบุคคลของผู้อื่นโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล จะมีโทษปรับทางปกครองไว้ สูงสุดไม่เกิน 3,000,000 บาท ตามบทบัญญัติมาตรา 83

ในส่วน ข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นพิเศษ เช่น ข้อมูลเรื่องเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ ฯลฯ มาตรา 26 กำหนดว่า ต้องได้รับ "ความยินยอมโดยชัดแจ้ง" จากเจ้าของข้อมูล การเก็บข้อมูลที่มีความอ่อนไหวโดยไม่ได้รับความยินยอมโดยชัดแจ้ง และน่าจะทำให้เจ้าของข้อมูลเสียหาย มาตรา 79 วรรคสอง กำหนดโทษจำคุกไม่เกิน 1 ปี ปรับไม่เกิน 1,000,000 บาท

นอกจากนี้ การเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอม และน่าจะทำให้เจ้าของข้อมูลเสียหาย มาตรา 79 กำหนดโทษจำคุกไม่เกิน 6 เดือน ปรับไม่เกิน 500,000 บาท ถ้าผู้ประกอบการเปิดเผยข้อมูลเพื่อแสวงหาประโยชน์ที่มิควรได้ โดยไม่ได้รับความยินยอม มาตรา 79 วรรคสอง กำหนดโทษจำคุกไม่เกิน 1 ปี ปรับไม่เกิน 1,000,000 บาท

2. การดำเนินการขอความยินยอม ต้องทำเป็นหนังสือหรือผ่านระบบออนไลน์ตามแบบที่กำหนดไว้ ดั่งที่ระบุไว้ในมาตรา 19 วรรคสอง ที่ว่า "การขอความยินยอมต้องทำโดยชัดแจ้งเป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เว้นแต่ โดยสภาพไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้"

ในการขอความยินยอม ต้องแจ้งวัตถุประสงค์ของการเก็บข้อมูล การใช้ข้อมูล การเปิดเผยข้อมูล และเพื่อไม่ให้ผู้ประกอบการแอบวางข้อความขอความยินยอมไว้เล็ก ๆ ไม่ให้เจ้าของข้อมูลสังเกตเห็น มาตรา 19 วรรคสาม จึงกำหนดว่า การขอความยินยอมต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน มีข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ ใช้ภาษาที่อ่านง่าย ซึ่งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอาจออกประกาศกำหนดแบบของเอกสารขอความยินยอม ผู้ประกอบการจึงต้องติดตามประกาศที่จะออกตามมาอย่างใกล้ชิด

นอกจากนี้ ในการขอความยินยอมผู้ประกอบการต้องให้อิสระในการตัดสินใจแก่เจ้าของข้อมูล ต้องไม่ถือเอาความยินยอมในการเก็บและใช้ข้อมูลเป็นเงื่อนไขในการเข้าทำสัญญาหรือการให้บริการต่าง ๆ โดยเจ้าของข้อมูลที่ให้ความยินยอมไปแล้วหากเปลี่ยนใจก็มีสิทธิจะถอนความยินยอมเมื่อใดก็ได้ ผู้ประกอบการต้องจัดช่องทางไว้ให้ถอนความยินยอมได้โดยง่ายเช่นเดียวกับการให้ความยินยอม หากการขอความยินยอมทำไม่ถูกต้องตามที่กฎหมายเขียนไว้ ก็จะไม่ทำให้ผู้ประกอบการมีสิทธิเก็บข้อมูลหรือนำข้อมูลไปใช้ได้

โดยกฎหมายกำหนดให้การกระทำใด ๆ กับข้อมูลส่วนบุคคลของผู้อื่นโดยไม่ได้ผ่านการขอความยินยอมตามรูปแบบที่ถูกต้อง มาตรา 82 กำหนดโทษปรับทางปกครองไว้ สูงสุดไม่เกิน 1,000,000 บาท

3. การเก็บข้อมูล ต้องแจ้งรายละเอียดและแจ้งสิทธิต่อเจ้าของข้อมูล

บทบัญญัติ มาตรา 23 กำหนดว่า แม้จะได้รับความยินยอมให้เก็บข้อมูลแล้วก็ตาม แต่ในการเก็บข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลทราบถึงรายละเอียดที่เกี่ยวข้อง ได้แก่ วัตถุประสงค์ของการเก็บรวบรวมข้อมูล ข้อมูลที่จะเก็บรวบรวมและระยะเวลาที่คาดหมายได้ว่าจะเก็บข้อมูลไว้ บุคคลหรือหน่วยงานที่ข้อมูลอาจจะถูกเปิดเผย ข้อมูลของผู้ประกอบการและตัวแทนที่เป็นผู้เก็บข้อมูล สถานที่ติดต่อ และวิธีการติดต่อ

นอกจากนี้ยังต้องแจ้งสิทธิของเจ้าของข้อมูลให้ทราบด้วย เช่น สิทธิเข้าถึงและขอสำเนาข้อมูล สิทธิคัดค้านการเก็บข้อมูลและการใช้ข้อมูล สิทธิขอให้ลบหรือทำลายข้อมูล สิทธิขอให้แก้ไขข้อมูลให้ถูกต้อง สิทธิร้องเรียนว่า มีการละเมิดข้อมูลส่วนบุคคลตามกฎหมายนี้ ฯลฯ

การกระทำใด ๆ กับข้อมูลส่วนบุคคลของผู้อื่นโดยไม่ได้แจ้งวัตถุประสงค์ แจ้งรายละเอียดและแจ้งสิทธิของเจ้าของข้อมูล มาตรา 82 กำหนดโทษปรับทางปกครองไว้ สูงสุดไม่เกิน 1,000,000 บาท

4. สำหรับวิธีการเก็บข้อมูลส่วนบุคคลจะต้องเก็บข้อมูลจากเจ้าของข้อมูลเท่านั้น ห้ามเก็บจากแหล่งอื่น เว้นแต่จะได้แจ้งเจ้าของข้อมูล

แม้จะได้รับความยินยอมจากเจ้าของข้อมูลแล้วก็ตาม แต่มาตรา 25 กำหนดว่า การเก็บข้อมูลต้องเก็บจากเจ้าของข้อมูลเท่านั้น กล่าวคือ ต้องให้เจ้าของข้อมูลเป็นผู้กรอกข้อมูลและมอบให้โดยตรง ผู้ประกอบการไม่สามารถเก็บข้อมูลจากแหล่งอื่นได้ เช่น ไม่สามารถค้นหาข้อมูลจากอินเทอร์เน็ตและบันทึกไว้เอง ไม่สามารถซื้อข้อมูลต่อมาจากผู้ประกอบการรายอื่น แม้จะได้รับความยินยอมแล้วก็ตาม

อย่างไรก็ตาม หลักการนี้มีข้อยกเว้นอยู่มากมาย ผู้ประกอบการยังสามารถเก็บข้อมูลจากแหล่งอื่นได้ ถ้าหากเมื่อเก็บข้อมูลแล้วได้แจ้งให้เจ้าของข้อมูลทราบพร้อมกับแจ้งสิทธิต่อเจ้าของข้อมูลโดยไม่ชักช้า หรือภายใน 30 วัน และได้รับความยินยอมจากเจ้าของข้อมูลให้เก็บข้อมูลจากแหล่งอื่นได้ แต่ผู้ประกอบการอาจจะไม่ต้องแจ้งให้เจ้าของข้อมูลทราบและขอความยินยอมใหม่เลย หากเป็นกรณีที่เจ้าของข้อมูลทราบอยู่แล้ว หรือต้องกระทำโดยเร่งด่วนตามที่กฎหมายกำหนด หรือกฎหมายกำหนดให้รายละเอียดบางประการเป็นความลับ

การเก็บข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ได้จากเจ้าของข้อมูลโดยตรง โดยไม่มีข้อยกเว้นให้เก็บข้อมูลได้ มาตรา 83 กำหนดโทษปรับทางปกครองไว้ สูงสุดไม่เกิน 3,000,000 บาท

5. กฎหมายฉบับใหม่นี้กำหนดให้ องค์กรธุรกิจขนาดใหญ่ ต้องมี "เจ้าหน้าที่คุ้มครองข้อมูล" อยู่ประจำหน่วยงานของตน

กฎหมายกำหนดหลักการว่า กรณีที่ผู้เก็บข้อมูลเป็นหน่วยงานของรัฐ หรือเป็นผู้ประกอบการที่มีข้อมูลส่วนบุคคลเป็นจำนวนมาก หรือผู้ประกอบการที่กิจกรรมหลักเป็นการเก็บข้อมูล การใช้ข้อมูล หรือการเปิดเผยข้อมูล ต้องจัดให้มี "เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล" เป็นของตัวเอง ซึ่งอาจเป็นพนักงานของผู้ประกอบการนั้น ๆ หรือเป็นผู้รับจ้างให้บริการหรือ outsource ก็ได้

โดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีหน้าที่ให้คำแนะนำและตรวจสอบการดำเนินการของผู้ประกอบการให้เป็นไปโดยถูกต้องตามกฎหมายนี้ ผู้ประกอบการจะต้องสนับสนุนการทำงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ต้องให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลรายงานปัญหาไปยังผู้บริหารสูงสุดได้ และต้องไม่ไล่เจ้าหน้าที่ออกจากงานหรือเลิกจ้างเพราะการทำหน้าที่คุ้มครองข้อมูลตามกฎหมายนี้ ขณะเดียวกันเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งข้อมูลของตัวเองและวิธีการติดต่อให้กับเจ้าของข้อมูลและให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ

ผู้ประกอบการที่ไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล มาตรา 85 กำหนดโทษปรับทางปกครองไว้ สูงสุดไม่เกิน 1,000,000 บาท

6. การเก็บและใช้ข้อมูลนั้นจะถูกตรวจสอบโดยคณะกรรมการผู้เชี่ยวชาญ

ตามมาตรา 71 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลจะแต่งตั้งคณะกรรมการผู้เชี่ยวชาญขึ้นมาเพื่อพิจารณาเรื่องร้องเรียนและตรวจสอบการกระทำของผู้ประกอบการเมื่อเจ้าของข้อมูลเห็นว่า มีการเก็บข้อมูล ใช้ข้อมูล หรือเปิดเผยข้อมูลของตัวเองโดยปฏิบัติไม่ถูกต้องตามกฎหมายนี้ เช่น ไม่ได้ขอความยินยอมก่อน หรือไม่ได้แจ้งรายละเอียดให้เจ้าของข้อมูลทราบ ก็สามารถร้องเรียนไปยังคณะกรรมการผู้เชี่ยวชาญได้

หากคณะกรรมการผู้เชี่ยวชาญพิจารณาแล้วเห็นว่า มีการปฏิบัติที่ไม่ถูกต้องจริง อาจให้มีการไกล่เกลี่ยกัน และมีอำนาจสั่งให้ผู้ประกอบการแก้ไขให้ถูกต้อง หรือสั่งห้ามกระทำการที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลได้ มาตรา 90 ให้อำนาจกับคณะกรรมการผู้เชี่ยวชาญสามารถสั่งปรับได้ โดยคำนึงถึงความร้ายแรงของการกระทำความผิด และขนาดของกิจการ หรืออาจจะสั่งเพียงแค่ให้แก้ไขและตักเตือนก่อนก็ได้

7. สำหรับข้อมูลส่วนบุคคลของผู้มรณะนั้น กฎหมายไม่คุ้มครองไปถึง

ตามมาตรา 6 กำหนดนิยามของ "ข้อมูลส่วนบุคคล" ไว้ว่า "ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ" ดังนั้น ข้อมูลที่เกี่ยวข้องกับผู้ที่เสียชีวิตแล้ว จึงไม่อยู่ภายใต้การคุ้มครองของกฎหมายนี้ การเก็บข้อมูล การใช้ข้อมูล และการเปิดเผยข้อมูลของผู้ที่เสียชีวิตแล้วสามารถทำได้โดยไม่ต้องขอความยินยมจากทายาทก่อน

8. บริษัทต่างชาติก็ไม่รอด! คุ้มครองข้อมูลของคนในประเทศ ไม่ว่าบริษัทตั้งอยู่ที่ใด

โดยหลักการทั่วไป กฎหมายของไทยที่ประกาศใช้ออกมาจะมีผลใช้บังคับเฉพาะกับการกระทำที่เกิดขึ้นในประเทศไทยเท่านั้น แต่ด้วยโลกยุคปัจจุบันการติดต่อสื่อสาร การส่งข้อมูล การเก็บข้อมูล และการใช้ข้อมูล เกิดขึ้นข้ามพรมแดนตลอดเวลา กฎหมายนี้จึงเขียนขอบเขตอำนาจการบังคับใช้ไว้กว้างขึ้นเป็นพิเศษ ตามมาตรา 5 พระราชบัญญัติข้อมูลส่วนบุคคลฯ จะใช้บังคับกับผู้ประกอบการที่อยู่ในประเทศไทย ไม่ว่า การเก็บข้อมูล การใช้ข้อมูลหรือการเปิดเผยข้อมูลจะเกิดขึ้นในประเทศหรือต่างประเทศก็ตาม

และพระราชบัญญัติฉบับนี้ ยังใช้บังคับกับ การเสนอขายสินค้าหรือบริการให้แก่คนที่อยู่ในประเทศไทย หรือการเฝ้าติดตามพฤติกรรมของคนที่อยู่ในประเทศไทยด้วย ไม่ว่าผู้ประกอบการที่เก็บข้อมูล หรือใช้ข้อมูล หรือเปิดเผยข้อมูลจะอยู่ในประเทศหรือต่างประเทศก็ตาม

9. ฝ่าฝืนกฎหมายฉบับนี้ จะถูกบังคับ "ค่าเสียหายเชิงลงโทษ" โดยต้องจ่ายสองเท่าตามหลักการของมาตรา 77 ที่กำหนดว่า ผู้ประกอบการที่ฝ่าฝืนหลักการที่กฎหมายฉบับนี้กำหนด ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลต้องชดใช้ค่าเสียหายแก่เจ้าของข้อมูล เว้นแต่เป็นเหตุสุดวิสัย หรือความเสียหายเกิดจากการกระทำของเจ้าของข้อมูลเอง หรือเป็นการปฏิบัติตามคำสั่งตามกฎหมายของเจ้าหน้าที่

กรณีที่ศาลตัดสินให้ผู้ประกอบการต้องจ่ายค่าเสียหายแก่เจ้าของข้อมูล ตามมาตรา 78 ศาลมีอำนาจสั่งให้ผู้ประกอบการจ่าย "ค่าเสียหายเชิงลงโทษ" เพิ่มขึ้นจากจำนวนค่าเสียหายที่แท้จริงได้ตามที่ศาลกำหนด แต่ไม่เกินสองเท่าของค่าเสียหายที่แท้จริง ค่าเสียหายเชิงลงโทษ ในที่นี้เป็นเงินที่ต้องจ่ายเพิ่มจากความเสียที่เกิดขึ้นจริง ซึ่งเป็นมาตรการเพื่อ "ป้องปราม" ไม่ให้ผู้ประกอบการกล้ากระทำความผิดอีก โดยศาลอาจกำหนดให้จ่ายค่าเสียหายโดยคำนึงถึงความร้ายแรงของความเสียหาย ผลประโยชน์ที่ผู้ประกอบการได้รับจากข้อมูลส่วนบุคคล สถานะทางการเงินของผู้ประกอบการ ฯลฯ

แต่อย่างไรก็ดี เมื่อพิจารณาพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลแล้ว มีข้อสังเกตเพิ่มเติมดังนี้ คือ สำหรับหลักการของกฎหมายฉบับนี้จะมีหลักการสำคัญอยู่ที่การวางหลักคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป มีผลคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในข้อมูลทุกประเภท แต่ลำพังเพียงการพิจารณาเฉพาะกฎหมายฉบับนี้แล้วตัดสินว่า จะมีการคุ้มครองข้อมูลส่วนบุคคลได้ตามความเป็นจริงหรือไม่นั้น จะต้องพิจารณาจากทั้งการวางข้อยกเว้นไว้ในกฎหมายฉบับนี้เอง และกฎหมายฉบับอื่น ๆ ซึ่ง ในการผ่านกฎหมายคุ้มครองข้อมูลส่วนบุคคลออกมาโดยสภานิติบัญญัติแห่งชาตินั้น ก็ได้มีการผ่านกฎหมายคู่แฝดออกมาอีกฉบับหนึ่งที่สำคัญนั่นก็คือ พระราชบัญญัติการรักษาความปลอดภัยมั่นคงไซเบอร์ พ.ศ. 2562 อันเป็นกฎหมายที่ให้อำนาจรัฐกำหนดมาตรการหรือการดำเนินการต่าง ๆ เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคาม ทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ ดังนั้นเพื่อให้สามารถป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที

ดังนั้น จึงกล่าวได้ว่า ในมิติของการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนั้น ปัจจุบันแม้จะได้มีการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลมาเป็นกฎหมายหลักในการคุ้มครองแล้ว ก็การกำหนดข้อยกเว้นต่าง ๆ ไว้ ไม่ว่าจะโดยกฎหมายคุ้มครองข้อมูลส่วนบุคคลเอง หรือกฎหมายฉบับอื่น ๆ ที่เกี่ยวกับการคุ้มครองประโยชน์สาธารณะ ตัวอย่างเช่น กฎหมายความมั่นคงปลอดภัยไซเบอร์ที่ได้กล่าวมาเป็นต้น

บทสรุปและข้อเสนอแนะ

เมื่อพิจารณาจากพัฒนาการของการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศไทยที่ค่อยข้างเป็นไปอย่างล่าช้า เมื่อเปรียบเทียบกับพัฒนาการของนานาอารยะกประเทศ และแม้ว่าในปัจจุบันเราจะได้มีการตรากฎหมายกลางที่มีลักษณะเป็นบทบัญญัติทั่วไปออกมาเพื่อเป็นหลักประกันในการคุ้มครองสิทธิประเภทนี้แล้วก็ตาม แต่กฎหมายนี้ยังมีปัญหาอีกหลายประการที่จะต้องทำการปรับปรุง โดยผู้วิจัยขอเสนอแนะแนวทางในการปรับปรุงดังต่อไปนี้คือ

1. ควรมีการแก้ไขพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ เพื่อขยายของเขตนิยามของคำว่าข้อมูลส่วนบุคคลให้ครอบคลุมไปถึงสิทธิในความเป็นส่วนตัวของผู้ตายหรือผู้เสียชีวิตต่อไป

2. ในการบังคับใช้กฎหมายเกี่ยวกับความมั่นคง ไม่ว่าจะเป็นพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ. 2562 รวมไปถึงกฎหมายที่เกี่ยวข้องกับความมั่นคงหรือมีการเปิดโอกาสให้รัฐเข้าล่วงละเมิดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนั้น จะต้องมีการจำกัดขอบเขตของการใช้กฎหมายให้ชัดเจน และบังคับใช้ด้วยความระมัดระวังไม่ให้ไปล่วงละเมิดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประชาชน ไม่เช่นนั้น อาจจะสร้างปัญหาทางด้านเศรษฐกิจการค้าการลงทุนกับประเทศในสหภาพยุโรปก็เป็นได้

3. ในส่วนของกฎหมายเฉพาะที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย ตัวอย่างเช่น พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 หรือ พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 ควรจะได้มีการกำหนดหลักการให้สอดคล้องกันกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ทั้งในด้านของการกำหนดนิยามความหมาย รวมถึงมาตรการในการจัดการข้อมูลส่วนบุคคลที่เป็นการคุ้มครองสิทธิ เพื่อให้ระบบของการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของทั้งกฎหมายกลางและกฎหมายเฉพาะเป็นไปในทิศทางเดียวกัน

บรรณานุกรม

กิตติพงศ์ กมลธรรมวงศ์. (2549). *การคุ้มครองข่าวสารส่วนบุคคลในระบบกฎหมายไทย: ปัญหาและแนวทางแก้ไข.* (วิทยานิพนธ์ปริญญามหาบัณฑิต). คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์.

นคร เสรีรักษ์. (2557). *ความเป็นส่วนตัว: ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย.* กรุงเทพฯ: พี.เพรส.

นพมาศ เกิดวิชัย. (2557). *การพัฒนากฎหมายเพื่อคุ้มครองสิทธิในความเป็นส่วนตัว.* (วิทยานิพนธ์ปริญญามหาบัณฑิต). คณะนิติศาสตร์ มหาวิทยาลัยรังสิต.

บรรเจิด สิงคะเนติ, นนทวัชร์ นวตระกูลพิสุทธิ์, และเรวดี ขวัญทองยิ้ม. (2554). *รายงานการศึกษาวิจัยฉบับสมบูรณ์ เรื่อง ปัญหาและมาตรการทางกฎหมายในการรับรองและคุ้มครองสิทธิในความเป็นส่วนตัว.* รายงานการศึกษาวิจัย เสนอต่อสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ.

ปฏิวัติ อุ่นเรือน. (2547). *ปัญหาการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลระหว่างประเทศ.* (สาระนิพนธ์ปริญญามหาบัณฑิต). คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์.