มาตรการและกลไกทางกฎหมายในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล

นพดล นิ่มหนู

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
นิติศาสตรดุษฎีบัณฑิต
คณะนิติศาสตร์
สถาบันบัณฑิตพัฒนบริหารศาสตร์
2562

มาตรการและกลไกทางกฎหมายในการคุ้มครองสิทธิ
ในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล
นพดล นิ่มหนู
คณะนิติศาสตร์

ผู้ช่วยศาสตราจารย์ .....อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(ดร.พัชรวรรณ นุชประยูร)

คณะกรรมการสอบวิทยานิพนธ์ ได้พิจารณาแล้วเห็นสมควรอนุมัติให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรนิติศาสตรดุษฎีบัณฑิต

ศาสตราจารย์.....ประธานกรรมการ
(ดร.สุรพล นิติไกรพจน์)

ศาสตราจารย์.....กรรมการ
(ดร.บรรเจิด สิงคะเนติ)

ศาสตราจารย์.....กรรมการ
(ดร.นนทวัชร์ นวตระกูลพิสุทธิ์)

ผู้ช่วยศาสตราจารย์.....กรรมการ
(ดร.อมรรัตน์ กุลสุจริต)

ผู้ช่วยศาสตราจารย์.....กรรมการ
(ดร.พัชรวรรณ นุชประยูร)

รองศาสตราจารย์.....คณบดี
(นเรศร์ เกษะประกร)
กุมภาพันธ์ 2563

บทคัดย่อ

ชื่อวิทยานิพนธ์ มาตรการและกลไกทางกฎหมายในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล

ชื่อผู้เขียน นายนพดล นิ่มหนู

ชื่อปริญญา นิติศาสตรดุษฎีบัณฑิต

ปีการศึกษา 2562

การวิจัยนี้มีวัตถุประสงค์เพื่อ 1) เพื่อศึกษาถึงแนวคิดและทฤษฎีอันเกี่ยวกับสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล 2) เพื่อศึกษาวิเคราะห์ถึงมาตรการและกลไกตามระบบกฎหมายไทยที่เกี่ยวกับคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล 3) เพื่อศึกษาวิเคราะห์และเปรียบเทียบถึงมาตรการและกลไกในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของต่างประเทศเพื่อเป็นแนวทางสำหรับประเทศไทย 4) เพื่อศึกษาและเสนอแนะแนวทางสำหรับการพัฒนามาตรการและกลไกในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลสำหรับประเทศไทยต่อไป ซึ่งวิธีการวิจัยในเรื่องนี้เป็นการศึกษาวิจัยเชิงคุณภาพ (Qualitative Research) ใช้วิธีวิเคราะห์เชิงพรรณนา (Descriptive Analysis) โดยทำการศึกษาจากแนวคิดทฤษฎีและวรรณกรรมที่เกี่ยวข้อง โดยมีการรวบรวมข้อมูลจากเอกสารต่าง ๆ ที่เกี่ยวข้องทั้งที่เป็นภาษาไทยและภาษาต่างประเทศ และใช้วิธีการสัมภาษณ์ (Interview) ด้วยวิธีการสัมภาษณ์แบบเชิงลึก (In-Depth Interview) จากผู้ทรงคุณวุฒิ ผลการวิจัยพบว่า สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลเป็นสิทธิมนุษยชนที่ได้รับการยอมรับจากนานาอารยประเทศซึ่งประเทศไทยนั้นเดิมเรามีเพียงกฎหมายเฉพาะที่ตราขึ้นเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลเพียงบางประเภท แต่ในปัจจุบันได้ตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ซึ่งมีลักษณะเป็นกฎหมายกลางอันเป็นบทบัญญัติทั่วไปที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคลทุกประเภทออกมาใช้บังคับเป็นที่เรียบร้อยแล้ว แต่อย่างไรก็ดียังคงมีปัญหาบางประการที่ต้องเร่งดำเนินการพัฒนาสำหรับมาตรการและกลไกในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ไม่ว่าจะเป็นประเด็นในเรื่องของนิยามความหมาย การกำหนดประเภทของข้อมูล การคุ้มครองข้อมูลส่วนบุคคลของของบุคคลบางประเภทเช่นผู้เยาว์ ผู้มรณะ ผู้ต้องขัง ผู้พิการหรือทุพพลภาพ มาตรการในการคุ้มครองข้อมูลไม่ว่าจะเป็นการเก็บรวบรวม การใช้ การเผยแพร่ และการเก็บรักษา และข้อจำกัด

ต่าง ๆ ของมาตรการ รวมไปถึงบทบาทหน้าที่ขององค์กรผู้ใช้อำนาจรัฐ องค์กรธุรกิจที่เกี่ยวข้อง ทั้งนี้ เพื่อให้เป็นไปตามมาตรฐานสากลที่นานาอารยประเทศยอมรับโดยเฉพาะสหภาพยุโรปอันเป็นการป้องกันปัญหาที่จะนำไปสู่การกีดกันทางการค้าในอนาคต

ABSTARCT

Title of Dissertation The Legal Measures to Protect the Rights to Personal Data Protection

Author Mr.Noppadon Nimnoo

Degree Doctor of Laws

Year 2019

The purposes of this research were 1) to study concepts and theories regarding privacy rights regarding personal information 2) to analyze the measures and mechanisms under the Thai legal system regarding the protection of privacy rights regarding personal information 3) analyze, and compare measures and mechanisms in protecting the privacy rights of foreign personal information in order to be a guideline for Thailand 4)to study the methods for the development of measures and mechanisms for the protection of privacy rights regarding personal information for Thailand. Research methodology was qualitative research that applied descriptive analysis by reviewing theories and related literature in an attempt to analyze a conclusion and propose legal measures. Data were collected from both Thai and English documents. In-depth interviews with experts were conducted.The research found that The right to privacy regarding personal information is a human right recognized by many civilized countries. In the case of Thailand, in the past we had only specific laws enacted to protect the privacy rights of certain types of personal information. But now we have enacted the Personal Data Protection Act. 2019 That has a central law, which is a general provision used to protect all types of personal information has come into force. However, there are still some problems that need to be accelerated in the development of measures and mechanisms for protect this rights. Whether it is a matter of definition or meaning of Personal Data, Data type determination, Rights to data privacy of minors,

prisoners, disabled person and Protection of personal information of the deceased, , Data processing methods such as collection, use, dissemination,storage and limitations of measures . Including the role and duty of the state authority, business organizations. This is to comply with international standards that are accepted by many countries, especially the European Union, in order to prevent problems that will lead to trade barriers in the future.

กิตติกรรมประกาศ

การจัดทำวิทยานิพนธ์ครั้งนี้สำเร็จลุล่วงได้ด้วยดี โดยได้รับความกรุณาจากคณะกรรมการสอบวิทยานิพนธ์ ซึ่งประกอบไปด้วยศาสตราจารย์ ดร.สุรพล นิติไกรพจน์ ประธานกรรมการและคณะกรรมการอันประกอบไปด้วยศาสตราจารย์ ดร.บรรเจิด สิงคะเนติ ศาสตราจารย์ ดร.นนทวัชร์ นวตระกูลพิสุทธิ์ ผู้ช่วยศาสตราจารย์ ดร.อมรรัตน์ กุลสุจริต และโดยเฉพาะอย่างยิ่งผู้ช่วยศาสตราจารย์ ดร.พัชรวรรณ นุชประยูร กรรมการและอาจารย์ที่ปรึกษาวิทยานิพนธ์ ที่ได้กรุณาให้คำแนะนำและช่วยเหลือในประการต่าง ๆ แก่ผู้เขียนจนวิทยานิพนธ์ฉบับนี้ได้สำเร็จลุล่วง ศิษย์จึงขอกราบขอบพระคุณมา ณ โอกาสนี้เป็นอย่างสูง

นอกจากนี้ผู้เขียนขอกราบขอบพระคุณสำนักงานศาลรัฐธรรมนูญ ที่ได้อนุเคราะห์ให้ทุนสนับสนุนในการทำวิจัยครั้งนี้ และ ขอขอบคุณทุกคนในครอบครัวและเพื่อน ๆ ร่วมสถาบันทุกคนที่คอยเป็นกำลังใจให้เป็นอย่างดียิ่งตลอดระยะเวลาในการศึกษา และขอกราบขอบคุณคณาจารย์ทุกท่านที่ได้ประสิทธิประสาทวิชาให้ตลอดหลักสูตร

นพดล นิ่มหนู

กุมภาพันธ์ 2563

สารบัญ

สารบัญตาราง

ตารางที่ **หน้า**

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ด้วยเหตุที่สิทธิมนุษยชน (Human Rights) เป็นแนวคิดที่มาจากความเชื่อ คำสอนทางศาสนา ปรัชญา ศีลธรรมและจริยธรรมของสังคม ซึ่งมีพัฒนาการของแนวความคิดในลักษณะที่กว้างขวางขึ้นไปตามยุคสมัยและสถานการณ์ความเปลี่ยนแปลงของสังคมตั้งแต่อดีตจนถึงปัจจุบัน ก่อให้เกิดสิทธิประเภทหนึ่งขึ้นมาเรียกว่า สิทธิในความเป็นส่วนตัว (Right to Privacy) โดยเฉพาะในมิติของข้อมูลส่วนบุคคล (Personal Data) ซึ่งสิทธิมนุษยชนประเภทนี้เป็นสิทธิที่เกิดขึ้นจากพลวัตทางสังคมที่มีการเปลี่ยนแปลงอย่างฉับพลันและรุนแรงโดยผลของการปฏิวัติอุตสาหกรรมครั้งที่ 3[1] และจากการเข้าสู่ยุคแห่งการปฏิวัติอุตสาหกรรมครั้งที่ 4 ซึ่งเริ่มขึ้นในช่วงเปลี่ยนศตวรรษที่ผ่านมาประกอบกับผลมาจากการปฏิวัติดิจิตอล ทำให้ระบบอินเทอร์เน็ตแพร่หลายขึ้นอย่างมากและเคลื่อนที่ได้ โดยมีตัวเซ็นเซอร์ที่เล็กลงและทรงพลังมากขึ้นแต่ราคาถูกลง รวมไปถึงการพัฒนาปัญญาประดิษฐ์และจักรกลเรียนรู้[2] ทำให้โลกในปัจจุบันกลายเป็นโลกแห่งการเชื่อมต่อ แนวคิดหมู่บ้านโลก (Global Village) ของมาแชลล์ แมคลูฮาน จึงได้กลายเป็นความจริงในช่วงโลกดิจิตอลที่กำลังเบ่งบาน ดังจะเห็นได้จากทุกวันนี้มีผู้ใช้งานอินเทอร์เน็ตทั่วโลกประมาณ 7,000 ล้านคน และมีอุปกรณ์ที่สามารถเชื่อมต่อกับ

---

[1] การปฏิวัติอุตสาหกรรมครั้งแรกกินเวลาตั้งแต่ประมาณ ค.ศ.1760 จนถึงประมาณปี ค.ศ. 1840 เป็นยุคที่มีการสร้างรางรถไฟและการประดิษฐ์เครื่องจักรไอน้ำ การปฏิวัติอุตสาหกรรมครั้งที่สอง เริ่มต้นช่วงปลายศตวรรษที่ 19 และเลยมาจนถึงช่วงต้นศตวรรษที่ 20 ทำให้มีการผลิตเป็นจำนวนมากเนื่องจากผลของการคิดค้นกระแสไฟฟ้าและระบบสายพานการผลิตในโรงงาน การปฏิวัติอุตสาหกรรมครั้งที่สามเริ่มต้นในปี 1960 โดยมักเรียกกันว่าการปฏิวัติดิจิตอลหรือการปฏิวัติคอมพิวเตอร์ เพราะผลจากการพัฒนาสารกึ่งตัวนำ เมนเฟรมคอมพิวเตอร์ คอมพิวเตอร์ส่วนบุคคล และระบบอินเทอร์เน็ต

[2] เคลาส์ ชวาบ, **การปฏิวัติอุตสาหกรรมครั้งที่สี่**, แปลโดย ศรรวริศา เมฆไพบูลย์ (กรุงเทพมหานคร: อมรินทร์ฮาวทู อมรินทร์พริ้นติ้งแอนด์พับลิชชิ่ง, 2561), หน้า 17.

อินเทอร์เน็ตจำนวนมากขึ้น 12,100 ล้านเครื่องในปี ค.ศ.2014 และคาดการได้ว่าตัวเลขนี้จะสูงขึ้นเป็น 50,000 ล้านเครื่อง ในปี ค.ศ.2020[3]

ผลจากการปฏิวัติอุตสาหกรรมก่อให้เกิดความเสี่ยงต่อการคุกคามสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลอย่างหลีกเลี่ยงไม่ได้ การคุกคามในรูปแบบใหม่ ๆ เช่น การปลอมอัตลักษณ์ (Identity Fraud) และการขโมยอัตลักษณ์ (Identity Theft) การเกิดขึ้นของรูปแบบใหม่ ๆ ของอาชญากรรมที่มุ่งหมายต่อข้อมูลส่วนบุคคล การใช้กระแสสังคม(กระแสโซเชียล) กดดัน การกดขี่ข่มเหงที่กระทำโดยวิธีการเผยแพร่ข้อมูลส่วนบุคคลด้วยการกระจายข้อมูลอย่างรวดเร็ว การลักลอบเก็บข้อมูลส่วนบุคคลมาประมวลผลเพื่อประโยชน์ในทางการบริหารจัดการ ฯลฯ ประเด็นต่าง ๆ เหล่านี้ที่เกิดขึ้นยิ่งทวีความรุนแรงมากขึ้นโดยเฉพาะอย่างยิ่งในโลกอนาคต ทั้งนี้เพราะข้อมูลเป็นสิ่งมีความสำคัญ สามารถนำไปใช้ประโยชน์ต่อการวางแผน วางระบบการทำงานและการบริหารจัดการการดำเนินกิจกรรมต่าง ๆ ทำให้ไม่ว่าจะเป็นภาครัฐหรือเอกชนจึงมีความจำเป็นต้องมีข้อมูลไว้ในครอบครองไว้ให้มากที่สุด โดยในข้อมูลข่าวสารจำนวนมากมายมหาศาลที่มีการครอบครองหรือมีการแลกเปลี่ยนหรือแย่งชิงแข่งขันกันครอบครองนี้ ก็จะมีข้อมูลส่วนหนึ่งเป็นข้อมูลส่วนบุคคล ดังนั้นสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลอันเป็นสิ่งเฉพาะตัวของบุคคลแต่ละคนที่สามารถนำไปสู่การพิสูจน์ตัวตนของบุคคลได้ ซึ่งได้แก่ ข้อมูลในเรื่องเกี่ยวกับประวัติส่วนตัวต่าง ๆ ไม่ว่าจะเป็นการศึกษาหรือการทำงาน ข้อมูลเกี่ยวกับการนับถือศาสนา ข้อมูลเกี่ยวกับสุขอนามัยส่วนบุคคล ข้อมูลประวัติอาชญากรหรือการถูกดำเนินคดีอาญา ข้อมูลอันเกี่ยวกับพฤติกรรมการใช้ชีวิต ทัศนคติ รสนิยมการเดินทาง การแสดงออก หรือการใช้บริการต่าง ๆ รวมถึงการทำธุรกรรมของบุคคลไม่ว่าจะเป็นกับทางภาครัฐหรือเอกชน ข้อมูลเหล่านี้จึงเป็นที่ต้องการและถูกล่วงละเมิดเพื่อประโยชน์ของผู้กระทำอย่างแพร่หลายและง่ายดาย

เมื่อพิจารณาถึงการที่องค์กรต่าง ๆ (ไม่ว่าจะเป็นภาครัฐหรือเอกชน) ซึ่งเป็นผู้ครอบครองข้อมูลส่วนบุคคลของปัจเจกชนทั้งหลายจึงอยู่ในฐานะที่เป็นผู้ได้เปรียบ เหมือนกับที่กล่าวกันว่า “ความรู้ คือ อำนาจ” จึงย่อมมีโอกาสที่จะเป็นไปได้ว่าองค์กรเหล่านี้จะมีการกระทำที่มากไปกว่าการส่งต่อข้อมูลอย่างถูกต้องและตรงไปตรงมา แต่จะเป็นการใช้ข้อมูลจัดการกับปัจเจกชนเสียเอง ตัวอย่างของการที่องค์กรใช้ข้อมูลไปในทางที่ผิด เช่น การที่บริษัทเอกชนใช้ข้อมูลส่วนบุคคลที่มีหรือได้มาทำให้ปัจเจกชนที่เป็นประชาชนทั่วไปต้องซื้อสินค้าหรือบริการหรือกระทำการอื่น ๆ โดยที่ไม่เคย

---

[3] ซามูเอล กรีนการ์ด, **อินเทอร์เน็ตแห่งสรรพสิ่ง**, แปลโดย ทีปกร วุฒิพิทยามงคล (กรุงเทพมหานคร: โอเพ่นเวิลด์ส, 2560), หน้า 30.

รู้และไม่เคยคิดอยากทำ โดยที่ไม่รู้ตัว[4] จึงส่งผลให้บรรดาปัจเจกชนก็จะต้องเผชิญกับประเด็นปัญหาการล่วงละเมิดข้อมูลส่วนบุคคลจากบรรดาองค์กรต่าง ๆ ทั้งภาครัฐรัฐและเอกชนด้วยอีกด้านหนึ่ง

ด้วยเหตุต่าง ๆ ข้างต้นนี้ ข้อมูลส่วนบุคคลจึงเป็นสิทธิในความเป็นส่วนตัวอันสำคัญอย่างยิ่งต่อตัวผู้เป็นเจ้าของและเป็นสิทธิขั้นพื้นฐานของมนุษย์ที่นานาอารยประเทศให้การยอมรับ ดังจะเห็นได้จากการบัญญัติรับรองไว้ในปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ.1948 (Universal Declaration of Human Rights 1948) ข้อ 12 ที่ว่า “บุคคลใดจะถูกแทรกแซงตามอำเภอใจในความเป็นส่วนตัว ครอบครัว ที่อยู่อาศัย หรือการสื่อสาร หรือจะถูกลบหลู่เกียรติยศหรือชื่อเสียงมิได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองของกฎหมายต่อการแทรกแซงหรือลบหลู่เช่นนั้น”[5] รวมไปถึงยังมีการรับรองไว้ในกฎหมายหรือกฎเกณฑ์ระหว่างประเทศอีกหลายฉบับ ในระดับองค์การระหว่างประเทศ เช่น องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD) สหภาพยุโรป (EU) แม้กระทั่งกลุ่มความร่วมมือทางเศรษฐกิจเอเชีย-แปซิฟิก (APEC) เอง ก็ให้ความสำคัญโดยการกำหนดกรอบ (Framework) หรือแนวทาง (Guidelines) เพื่อกำหนดมาตรฐานขั้นต่ำให้ประเทศสมาชิกของตนอ้างอิงเป็นฐานในการบัญญัติกฎหมายภายในประเทศของตนเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ซึ่งจะเห็นได้ว่าประเทศต่าง ๆ เช่นประเทศสิงค์โปร์ ประเทศฟิลิปปินส์ รวมไปถึงประเทศมาเลเซียเอง ก็ได้ดำเนินการตรากฎหมายภายในของประเทศของตนให้สอดคล้องกับกติกาสากลเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลเป็นที่เรียบร้อยแล้ว

ส่วนประเทศไทยมีการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ซึ่งเริ่มขึ้นโดยการกำหนดไว้ในรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2535 (แก้ไขเพิ่มเติม พุทธศักราช 2538) โดยได้บัญญัติคุ้มครอง “สิทธิในความเป็นส่วนตัว” ไว้ในมาตรา 47[6] และต่อมามีการนำมา

---

[4] ดอน แทปส์ค็อตต์, **เศรษฐกิจดิจิตอล**, แปลโดย พรศักดิ์ อุรัจฉัทชัยรัตน์ (กรุงเทพมหานคร: แมคกรอ-ฮิล อินเทอร์เนชั่นแนล เอ็นเตอร์ไพรส์ แอลแอลซี, 2559), หน้า 325.

[5] The Universal Declaration of Human Rights 1948. Article 12 “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.” แปลโดยกระทรวงการต่างประเทศ จากเว็บไซต์ http://humanrights.mfa.go.th/upload/pdf/udhr-th-en.pdf

[6] มาตรา 47 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย แก้ไขเพิ่มเติม (ฉบับที่ 5) พ.ศ.2538 “สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัว ย่อมได้รับความคุ้มครอง

บัญญัติไว้ในรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540 มาตรา 34 เพื่อเป็นการกำหนดยืนยันหลักการคุ้มครองสิทธิในความเป็นส่วนตัวว่า “สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัวย่อมได้รับความคุ้มครอง การกล่าวหรือไขข่าว แพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชนอันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัวจะกระทำมิได้ เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณชน” บทบัญญัติมาตรานี้นำไปสู่ความพยายามในการตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลขึ้นทั้งในส่วนที่อยู่ในความครอบครองของทางภาคราชการและภาคเอกชน ซึ่งในส่วนทางภาคราชการได้มีการตราพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 เป็นที่เรียบร้อย แต่สำหรับข้อมูลข่าวสารที่อยู่ในความครอบครองของภาคเอกชนนั้น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพิ่งได้ผ่านการพิจารณาของรัฐสภาในระยะเวลาไม่นานมานี้เอง

เมื่อมองย้อนไปในอดีตแล้ว จึงเห็นว่าประเทศไทยได้มีการตรากฎหมายเฉพาะออกมาหลายฉบับเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในบางเรื่อง เช่น พระราชบัญญัติการประกอบธุรกิจข้อมูลบัตรเครดิต พ.ศ.2544 คุ้มครองสิทธิของเจ้าของข้อมูลเครดิต พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ.2550 คุ้มครองสิทธิของเจ้าของข้อมูลประวัติสุขภาพ หรือพระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ.2544 คุ้มครองสิทธิของเจ้าของข้อมูลในการติดต่อสื่อสารระหว่างกันของบุคคล ฯลฯ เป็นต้น แต่เป็นเพียงมาตรการเฉพาะด้านไม่ได้ครอบคลุมถึงการคุ้มครองสิทธิในความเป็นส่วนตัวของข้อมูลส่วนบุคคลทั้งระบบ อีกทั้งมาตรการคุ้มครองตามกฎหมายฉบับต่าง ๆ ที่มีอยู่นั้นก็ไม่ได้มีมาตรฐานที่เท่าเทียมกัน รวมตลอดถึงยังไม่ได้เป็นไปตามมาตรฐานของกติกาสากลในทุกมิติ แม้ประเทศไทยจะมีการตราพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 โดยกำหนดให้หน่วยงานของรัฐต้องมีมาตรการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลก็ตาม แต่ก็เป็นเพียงข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความครอบครองของภาครัฐ ไม่ได้มีการกำหนดมาตรการคุ้มครองไปถึงข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของภาคเอกชนแต่อย่างใด

ช่วงระยะเวลาที่ประเทศไทยยังไม่มีมาตรการและกลไกอันเป็นกฎหมายกลางที่กำหนดมาตรฐานขั้นต่ำในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนั้น จึงส่งผลให้เกิดปัญหาในหลายด้าน แม้จะมีกฎหมายในระดับรัฐธรรมนูญวางหลักการรับรองสิทธิไว้ แต่โดยเนื้อหาสาระแล้วก็เป็นเพียงการรับรองหลักการไว้เท่านั้น ยังขาดความชัดเจนในเรื่องความหมายและขอบเขต

การกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชน อันเป็นการกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ หรือชื่อเสียงและความเป็นอยู่ส่วนตัวจะกระทำมิได้ เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณชน”

บางประการ ซึ่งอาจเป็นปัญหาต่อไปในอนาคต และเมื่อมองในส่วนของกฎหมายระดับพระราชบัญญัติที่มีการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนั้น จะเห็นว่ามีการบัญญัติไว้อย่างกระจัดกระจายในกฎหมายหลายฉบับ ไม่มีกฎหมายที่มุ่งคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลเป็นการทั่วไปและคุ้มครองสิทธิของเจ้าของข้อมูลได้โดยตรง กฎหมายฉบับต่าง ๆ ที่ตราขึ้นจึงไม่ได้ให้ความคุ้มครองอย่างเป็นระบบ และไม่ได้ให้หลักประกันสิทธิอย่างเพียงพอ และยังไม่ได้เป็นไปตามมาตรฐานสากลที่ได้มีการพัฒนาและยกระดับของการคุ้มครองมากยิ่งขึ้น

นอกจากนี้ในด้านการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนั้น ประเทศไทยยังไม่มีองค์กรที่เป็นเจ้าภาพหลักซึ่งมีอำนาจที่จะมาทำหน้าที่คุ้มครองสิทธินี้ตามรัฐธรรมนูญและกฎหมาย กระบวนการในการบังคับใช้กฎหมาย รวมไปถึงระบบการเยียวยาสิทธิของประชาชนที่ถูกล่วงละเมิดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลก็ยังอาศัยหลักการของกฎหมายอาญาและกฎหมายแพ่งและพาณิชย์เท่านั้น ซึ่งไม่สามารถทำให้เกิดการเยียวยาความเสียหายได้อย่างแท้จริง และการไม่มีมาตรการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลที่มีมาตรฐานทัดเทียมในระดับสากล อาจส่งผลกระทบทำให้เกิดการกำหนดมาตรการกีดกันทางการค้าจากประเทศคู่ค้าโดยเฉพาะอย่างยิ่งประเทศจากสหภาพยุโรป ที่ได้มีการออกข้อบังคับในระดับสหภาพยุโรปที่เรียกว่า General Data Protection Regulation (GDPR) เพื่อเป็นมาตรการในการยกระดับการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประชาชนที่เป็นพลเมืองของยุโรปให้สูงขึ้นกว่าหลักการเดิมที่มีมา อันจะส่งผลให้การดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของประเทศคู่ค้าจะต้องมีมาตรฐานของการคุ้มครองไม่น้อยไปกว่ามาตรฐานนี้ ซึ่งประเด็นนี้ยิ่งทำให้ประเทศไทยจำเป็นที่จะต้องเร่งรีบดำเนินการในการออกมาตรการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลโดยเร็วเพื่อจะไม่ให้เกิดผลกระทบต่อเศรษฐกิจของประเทศ

ด้วยเหตุผลข้างต้นทำให้ในปัจจุบันเมื่อวันที่ 28 กุมภาพันธ์ พ.ศ.2562 ประเทศไทยจึงมีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ซึ่งได้ผ่านการพิจารณาของสภานิติบัญญัติแห่งชาติ โดยมีหลักการและเหตุผลว่าเนื่องจากปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคล เป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว สามารถทำได้โดยง่าย สะดวก และรวดเร็ว รวมทั้งก่อให้เกิด ความเสียหายต่อเศรษฐกิจโดยรวมที่ใช้เทคโนโลยีดิจิทัลอย่างแพร่หลาย แม้ว่าจะได้มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลในบางเรื่อง แต่ก็ยังไม่มีหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไปจึงจำเป็นต้องตราพระราชบัญญัตินี้ ซึ่งเหตุผลของพระราชบัญญัติที่ได้กล่าวมาสะท้อนภาพของปัญหาได้เป็นอย่างดี

อย่างไรก็ดี แม้ว่าประเทศไทยจะได้มีการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ขึ้นมาเป็นกฎหมายกลางแล้วก็ตาม แต่ก็ถือว่ายังเป็นประเด็นใหม่สำหรับสังคมไทย ทำให้ยังมีปัญหาหลายมิติทั้งในด้านเนื้อหาของบทบัญญัติของกฎหมาย การกำหนดข้อยกเว้นทั้งในตัวกฎหมายฉบับนี้และกฎหมายฉบับอื่น ๆ รวมไปถึงการบังคับใช้ จึงเกิดประเด็นที่น่าจะศึกษาว่า ระบบกฎหมายของรัฐไทยโดยเฉพาะกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ตราขึ้นใหม่นี้ จะสามารถวางหลักคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ซึ่งอยู่ภายใต้บริบทแห่งความเปลี่ยนแปลงทางเทคโนโลยีสารสนเทศอย่างรวดเร็วและต่อเนื่องได้หรือไม่ รวมจึงมาตรฐานของการคุ้มครองที่จะได้มีการกำหนดไว้นั้น จะมีมาตรฐานของการคุ้มครองเป็นที่ยอมรับในระดับกติกาสากลหรือไม่ และควรจะมีการพัฒนามาตรการและกลไกทางกฎหมายอย่างไรเพื่อให้สามารถรับมือกับสถานการณ์ดังกล่าวได้ ไม่ว่าจะเป็นเรื่องมาตรการอันเป็นบทบัญญัติกฎหมายที่เหมาะสมในการรับรองและคุ้มครองสิทธิ และ กลไกอันเป็นองค์กรในการขับเคลื่อนและบังคับใช้กฎหมายเพื่อคุ้มครองและดำเนินการเยียวยาสิทธิของผู้ถูกล่วงละเมิด อันจะทำให้สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลได้รับการคุ้มครองอย่างแท้จริงและสอดคล้องกับหลักการสากล

1.2 วัตถุประสงค์ของการศึกษา

1. เพื่อศึกษาถึงแนวคิดและทฤษฎีอันเกี่ยวกับสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล
2. เพื่อศึกษาวิเคราะห์ถึงมาตรการและกลไกตามกฎหมายไทยที่เกี่ยวกับคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล
3. เพื่อศึกษาวิเคราะห์และเปรียบเทียบถึงมาตรการและกลไกในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของต่างประเทศเพื่อเป็นแนวทางสำหรับประเทศไทย
4. เพื่อศึกษาและเสนอแนะแนวทางสำหรับการพัฒนามาตรการและกลไกในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลสำหรับประเทศไทยต่อไป

1.3 สมมติฐานของการศึกษา

สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลถือเป็นสิทธิมนุษยชนอันสำคัญที่ถูกล่วงละเมิดได้โดยง่ายและทวีความรุนแรงมากขึ้น ซึ่งแม้ว่าสิทธินี้จะได้รับการบัญญัติคุ้มครองไว้ในกฎหมายหลายฉบับก็ตามแต่ก็เป็นเพียงการคุ้มครองในลักษณะเฉพาะเรื่องไม่ได้มีลักษณะการคุ้มครองเป็นการทั่วไปอันสามารถครอบคลุมไปทุกมิติ และยังขาดความชัดเจนในเรื่องของนิยามและขอบเขต และ

แม้ว่าปัจจุบันจะได้มีการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ซึ่งเป็นกฎหมายกลางที่เป็นบทบัญญัติทั่วไปขึ้นมาเพื่อคุ้มครองสิทธินี้แล้วก็ตามแต่ก็ยังมีปัญหาหลายมิติทั้งในด้านบทบัญญัติของกฎหมายรวมไปถึงการบังคับใช้จึงสมควรที่จะมีการพัฒนากฎหมายฉบับนี้รวมไปถึงกฎหมายอื่น ๆ ที่เกี่ยวข้องเพื่อให้การคุ้มครองข้อมูลส่วนบุคคลสามารถเกิดขึ้นได้ตามความเป็นจริงตามเจตนารมณ์ของกฎหมายรวมถึงมีความทัดเทียมกับมาตรฐานสากล

1.4 ขอบเขตการศึกษา

ศึกษาวิเคราะห์หลักกฎหมายที่เกี่ยวข้องกับการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศไทย โดยเฉพาะพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และกฎหมายฉบับอื่น ๆ ที่เกี่ยวข้อง รวมไปถึงกฎหมายของต่างประเทศ และกติการะหว่างประเทศที่ฉบับต่าง ๆ ที่เกี่ยวข้อง เพื่อนำมาเปรียบเทียบและประยุกต์สำหรับการพัฒนากฎหมายคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศไทยต่อไป

1.5 วิธีการดำเนินการศึกษา

การศึกษาวิจัยเกี่ยวกับเรื่องนี้จะใช้การดำเนินการวิธีวิจัยเชิงคุณภาพ (Qualitative Research) โดยใช้รูปแบบการวิจัยเอกสาร (Documentary Research) เช่นตำราวิชาการ หนังสือ รายงานการวิจัย วิทยานิพนธ์ตลอดจนเอกสารจากฐานข้อมูลออนไลน์ทั้งในและต่างประเทศ รวมถึงวิธีการสัมภาษณ์เชิงลึก (Indepth-interviews) นักวิชาการและผู้มีประสบการณ์ที่เกี่ยวข้องในประเด็นของงานวิจัยอีกด้วย

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1. ทำให้ทราบถึงถึงแนวคิดและทฤษฎีอันเกี่ยวกับสิทธิในความเป็นส่วนตัว โดยเฉพาะในมิติของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล
2. ทำให้ทราบถึงถึงมาตรการและกลไกที่เกี่ยวกับคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ตามกฎหมายที่เกี่ยวข้องทั้งของประเทศไทยและต่างประเทศ
3. ทำให้ทราบถึงปัญหา และอุปสรรค รวมถึงแนวทางในการกำหนดมาตรการและกลไกเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลทั้งของประเทศไทยและต่างประเทศ

4. ผลที่ได้จากการศึกษาวิจัยจะเป็นแนวทางพัฒนาการตราและการปรับปรุงแก้ไขกฎหมายที่เกี่ยวกับมาตรการและกลไกในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล เพื่อให้สอดคล้องกับหลักการสากลต่อไป

บทที่ 2

ข้อความคิดว่าด้วยสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล

ด้วยเหตุที่สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลถือเป็นสิทธิมนุษยชนอย่างหนึ่งซึ่งบุคคลทั้งหลายพึงได้รับการรับรองและคุ้มครองให้ทั้งจากกฎหมายและกฎเกณฑ์ระหว่างประเทศที่เป็นสากล รวมไปถึงกฎหมายภายในของรัฐ ไม่ว่าจะเป็นระดับของรัฐธรรมนูญรวมไปถึงระบบกฎหมายภายในของรัฐทั้งระบบ ในบทนี้จึงจะได้อธิบายถึงรากฐานในทางความคิดอันเป็นที่มาของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล รวมไปถึงหลักการและมาตรการรวมถึงกลไกในการคุ้มครองสิทธิประเภทนี้ตามหลักการสากล

2.1 แนวคิดทฤษฎีเกี่ยวกับสิทธิเสรีภาพและข้อมูลส่วนบุคคล

ในส่วนนี้จะได้นำเสนอแนวคิดพื้นฐานเกี่ยวกับสิทธิเสรีภาพซึ่งถือเป็นรากฐานสำคัญไม่ว่าจะเป็นความหมาย พัฒนาการ ประเภทของสิทธิเสรีภาพ เพื่อนำไปสู่ความเข้าใจถึง “สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล” ว่ามีฐานะเป็นสิทธิเสรีภาพประเภทใดและมีลักษณะพื้นฐานอย่างไร ซึ่งมีรายละเอียดดังนี้

2.1.1 แนวคิดพื้นฐานเกี่ยวกับสิทธิเสรีภาพ

หลักการพื้นฐานที่สำคัญ 2 ประการซึ่งเป็นหลักในการจัดองค์กรของรัฐเสรีประชาธิปไตย นั่นคือ หลักประชาธิปไตย ประการหนึ่ง และหลักนิติรัฐ อีกประการหนึ่งโดยสาระสำคัญของหลักการทั้งสองนี้จะแตกต่างกันไปตามสภาพของรูปแบบรัฐบาลหรือระบบการปกครองของประเทศนั้น ๆ ตามที่รัฐธรรมนูญกำหนด โดยที่หลักการประชาธิปไตยและหลักนิติรัฐนี้จะมีความเกี่ยวพันซึ่งกันและกัน จนอาจกล่าวได้ว่า หลักประชาธิปไตยเป็นหลักที่เอื้อให้เกิดหลักนิติรัฐ และขณะเดียวกันหลักนิติรัฐก็เป็นหลักที่ส่งเสริมสนับสนุนต่อประชาธิปไตย[7] ซึ่งการปกครองรัฐภายใต้หลักการทั้งสองนี้ให้ความสำคัญ

---

[7] บรรเจิด สิงคะเนติ, **หลักพื้นฐานเกี่ยวกับสิทธิเสรีภาพ และศักดิ์ศรีความเป็นมนุษย์**, พิมพ์ครั้งที่ 3 (กรุงเทพมหานคร: วิญญูชน, 2552), หน้า 17.

กับสิทธิเสรีภาพของประชาชนซึ่งเป็นเจ้าของอำนาจอธิปไตยเป็นอย่างยิ่ง กล่าวได้ว่ารัฐและรัฐบาลจะต้องปฏิบัติตามหลักการพื้นฐานของรัฐธรรมนูญ การออกกฎหมายของรัฐจะต้องมีอยู่บนพื้นฐานของการเปิดเผยให้ประชาชนรับรู้ มีความชัดเจน มีการบังคับใช้เป็นการทั่วไป เป็นที่คาดหมายได้ และมีความแน่นอน โดยรัฐไม่ควรที่จะเข้าไปแทรกแซงสิทธิเสรีภาพของประชาชนโดยพลการหรือตามอำเภอใจ[8] การใช้อำนาจขององค์กรของรัฐทุกองค์กรจะต้องเคารพต่อกฎหมายอันเป็นหลักประกันสิทธิเสรีภาพที่สำคัญของประชาชน เราจึงพบเห็นภาพที่ชัดเจนตลอดมาในรัฐเสรีประชาธิปไตยนั้นคือการตรากฎหมายขึ้นมาเพื่อรับรองและคุ้มครองสิทธิเสรีภาพของประชาชนภายในรัฐของตน ไม่ว่าจะเป็นการบัญญัติรับรองไว้ในกฎหมายรัฐธรรมนูญ พระราชบัญญัติ จนกระทั่งถึงกฎเกณฑ์ลำดับรองลงมาทั้งระบบ อย่างไรก็ดี ระดับของการรับรองและคุ้มครองสิทธิเสรีภาพของรัฐแต่ละรัฐ ก็ย่อมมีความแตกต่างกันไปตามสภาพทางประวัติศาสตร์ สังคม เศรษฐกิจ รวมไปถึงวัฒนธรรมของแต่ละประเทศ แต่เราก็ยังสามารถสรุปแนวคิดพื้นฐานเกี่ยวกับสิทธิเสรีภาพอันเป็นหลักการตามรัฐธรรมนูญที่เป็นหลักสากลร่วมกันซึ่งทุกประเทศให้การยอมรับได้ดังนี้

2.1.1.1 ความหมายของสิทธิเสรีภาพ

สำหรับคำว่า “สิทธิ” ตามความหมายทั่วไป หมายถึง “อำนาจที่กฎหมายรับรองคุ้มครองให้แก่บุคคลในอันที่จะเรียกร้องให้บุคคลอื่นกระทำการอย่างใดอย่างหนึ่ง สิทธิจึงก่อให้เกิดหน้าที่แก่บุคคลอื่นด้วย”[9] แต่คำว่า “สิทธิตามรัฐธรรมนูญ” ถือว่าเป็นสิทธิในทางกฎหมายมหาชน (Das Subjective Oeffenliche Recht) หมายถึง อำนาจตามรัฐธรรมนูญหรือกฎหมายสูงสุดที่ได้บัญญัติให้การรับรองคุ้มครองแก่ปัจเจกชนในอันที่จะกระทำการใดหรือไม่กระทำการใด การให้อำนาจแก่ปัจเจกบุคคลดังกล่าวได้ก่อให้เกิดสิทธิเรียกร้องที่จะไม่ให้บุคคลใดแทรกแซงในสิทธิตามรัฐธรรมนูญของตน โดยเฉพาะอย่างยิ่งเรียกร้องต่อองค์กรของรัฐมิให้แทรกแซงสิทธิตามรัฐธรรมนูญของตน ในบางกรณีการรับรองดังกล่าวได้ก่อให้เกิดสิทธิเรียกร้องให้รัฐดำเนินการอย่างใดอย่างหนึ่ง[10]

ส่วนคำว่า “เสรีภาพ” หมายถึง “สภาพการณ์ที่บุคคลมีอิสระในการที่จะกระทำการอย่างใดอย่างหนึ่งตามความประสงค์ของตน”[11] เสรีภาพจึงหมายถึง อำนาจในการกำหนดตนเองโดยอิสระของบุคคลที่จะกระทำการใดหรือไม่กระทำการใดอันเป็นอำนาจที่มีเหนือตนเอง ความแตกต่าง

---

[8] Steve Foster, **Human Rights and Civil Liberties** (London: Pearson Education, 2003), p. 13.

[9] วรพจน์ วิศรุตพิชญ์, **สิทธิเสรีภาพตามรัฐธรรมนูญ** (กรุงเทพมหานคร: วิญญูชน, 2538), หน้า 21.

[10] บรรเจิด สิงคะเนติ, *เรื่องเดิม*, หน้า 49.

[11] วรพจน์ วิศรุตพิชญ์, **สิทธิเสรีภาพตามรัฐธรรมนูญ,** หน้า 22.

ระหว่างสิทธิและเสรีภาพนี้ จึงอยู่ที่ว่า สิทธิ เป็นอำนาจที่บุคคลมีเพื่อเรียกร้องให้ผู้อื่นกระทำการหรือละเว้นกระทำการอันใดอันหนึ่ง แต่ขณะที่เสรีภาพ เป็นอำนาจที่บุคคลมีเหนือตนเองในการตัดสินใจที่จะกระทำอย่างใดอย่างหนึ่งหรือไม่กระทำการอย่างใดอย่างหนึ่งโดยปราศจากการแทรกแซงหรือครอบงำจากบุคคลอื่น เสรีภาพจึงไม่ก่อให้เกิดหน้าที่ต่อบุคคลอื่นแต่อย่างใด[12]

2.1.1.2 พัฒนาการของสิทธิเสรีภาพ

ต้องยอมรับว่ากำเนิดของสิทธิเสรีภาพมีที่มาจากสังคมตะวันตก โดยมีพื้นฐานมาจากแนวคิดเสรีนิยมและแนวคิดปัจเจกชนนิยม ที่เปลี่ยนมุมมองใหม่จากเดิมมายอมรับและเชื่อมั่นในคุณค่าของความเป็นมนุษย์ โดยผลจากการต่อสู้เรียกร้องระหว่างผู้ใต้ปกครองต่อผู้ปกครองซึ่งเป็นการต่อสู้ทางชนชั้นระหว่างชนชนกลางกับขุนนางและกษัตริย์ นำไปสู่การบังคับให้ผู้ปกครองยอมรับและให้หลักประกันสิทธิเสรีภาพบางประการแก่ประชาชน ดังจะเห็นได้ในกรณีของ Magna Carta ที่มีสาระสำคัญว่า พระมหากษัตริย์ (ในฐานะผู้ปกครอง) จะใช้พระราชอำนาจตามอำเภอใจไม่ได้ และนับจากกรณีนี้ก็ยังมีเอกสารสำคัญอีกหลายฉบับที่มีวัตถุประสงค์ในการจำกัดอำนาจของผู้ปกครอง เช่น Petition of Right, Bill of Right อันเป็นฐานสำคัญให้ประชาชนอ้างถึงสิทธิเสรีภาพของตนได้ โดยต่อมาในศตวรรษที่ 16 แนวความคิดทฤษฎีกฎหมายธรรมชาติ (Natural Law) ก็มีการพัฒนาขึ้นและได้รับการยอมรับอย่างมาก โดยแนวคิดนี้ได้ปฏิเสธการใช้อำนาจตามอำเภอใจและผิดทำนองคลองธรรมของผู้ปกครอง โดยมีการให้การยอมรับและเชื่อมั่นในสิทธิตามธรรมชาติ (Natural Right) ของประชาชนซึ่งนำไปสู่การสร้างหลักกฎหมายขึ้นมายอมรับในสิทธิเสรีภาพของประชาชนที่ว่า “บุคคลทุกคนเกิดมาย่อมมีความเสมอภาคกันและมีสิทธิเสรีภาพ เช่น สิทธิในชีวิต ร่างกาย ทรัพย์สิน ซึ่งเป็นสิทธิที่ติดตัวมาและสิทธินี้ไม่อาจจำหน่ายจ่ายโอนได้” หลักการนี้ได้กลายเป็นหลักสำคัญในคำประกาศสิทธิมนุษยชนและพลเมืองฝรั่งเศส ลงวันที่ 26 สิงหาคม ค.ศ.1789 (Déclaration des droits de l’homme et du citoyen 1789) ซึ่งจุดประสงค์ของการยอมรับสิทธิตามธรรมชาตินี้ก็เพื่อจำกัดอำนาจของผู้ปกครอง ไม่ว่าจะเป็นรัฐหรือผู้มีอำนาจทางปกครองใด ๆ ไม่ให้ใช้อำนาจล่วงละเมิดต่อสิทธิเสรีภาพของประชาชนนั่นเอง

ในกาลต่อมาแนวคิดเรื่องสิทธิเสรีภาพอันมีพื้นฐานมาจากแนวคิดเสรีนิยมและปัจเจกชนนิยม ก็ได้ถูกวิพากษ์วิจารณ์จากแนวคิดทางการเมืองแบบสังคมนิยมแบบมาร์กซิสต์ ว่าการให้เสรีภาพภาพแก่ปัจเจกชนมากเกินไปนำไปสู่ภาวะมือใครยาวสาวได้สาวเอา ทำให้นายทุนซึ่งมีอำนาจทางเศรษฐกิจมากกว่า ฉวยโอกาสและใช้โอกาสจากความมีเสรีนี้เอารัดเอาเปรียบชนชั้นแรงงาน และทำให้เกิดช่องว่างทางสังคม แนวคิดเรื่องสิทธิเสรีภาพนี้ก็เริ่มมีการปรับเปลี่ยนและพัฒนาโดยยอมรับกันว่า นอกจากประชาชนจะมีสิทธิเสรีภาพที่จะจำกัดอำนาจของรัฐและผู้ปกครองแล้ว ประชาชนยังมี

---

[12] บรรเจิด สิงคะเนติ, *เรื่องเดิม*, หน้า 51.

สิทธิเรียกร้องต่อรัฐให้กระทำการอย่างใดอย่างหนึ่งเพื่อเป็นหลักประกันขั้นต่ำให้แก่ตนเพื่อจะสามารถดำรงชีวิตได้อย่างผาสุก รวมทั้งมีโอกาสใช้สิทธิเสรีภาพได้อย่างเท่าเทียมกับผู้อื่น ซึ่งก็คือสิทธิเสรีภาพในทางสังคมและเศรษฐกิจนั่นเอง

ดังนั้น จึงกล่าวได้ว่าในมิติของพัฒนาการของสิทธิและเสรีภาพนี้ เราสามารถแบ่งช่วงระยะเวลาของพัฒนาการออกได้เป็น 4 ช่วงดังนี้[13]

ช่วงที่ 1 เป็นช่วงของพัฒนาการเกี่ยวกับเสรีภาพในทางศาสนา อันเป็นช่วงระยะเวลาที่ทำให้เกิดความมั่นคงต่อความเคารพในความเชื่อที่แตกต่างไปของบุคคลในสังคม (สิทธิเสรีภาพในชีวิต ร่างกาย ก็ได้รับการยอมรับในช่วงระยะเวลานี้)

ช่วงที่ 2 เป็นช่วงของพัฒนาการของสิทธิเสรีภาพในทางเศรษฐกิจ ซึ่งเกี่ยวกับเรื่องกรรมสิทธิ์และเสรีภาพในการทำสัญญา และเสรีภาพในการประกอบอาชีพ

ช่วงที่ 3 เป็นช่วงของการพัฒนาสิทธิในทางประชาธิปไตย อันได้แก่ เสรีภาพในการแสดงความคิดเห็น เสรีภาพของหนังสือพิมพ์ เสรีภาพในการชุมนุม และเสรีภาพในการรวมตัวกันเป็นสมาคม ซึ่งทำให้ชนชั้นกระฎุมพีเข้ามามีบทบาททางการเมืองการปกครองมากขึ้น จนจำเป็นต้องอาศัยสิทธิในทางประชาธิปไตยเป็นเครื่องมือสำคัญในการให้ประชาชนเข้าไปมีส่วนร่วมในการใช้อำนาจของรัฐ

ช่วงที่ 4 เป็นช่วงของพัฒนาการที่นำไปสู่สิทธิพื้นฐานในการดำรงชีพ หรือที่เรียกว่า “สิทธิขั้นพื้นฐานทางสังคม” เพื่อให้ผลประโยชน์โดยรวมของสังคมสามารถดำเนินไปบรรลุเป้าหมาย ไม่ว่าจะเป็นกรณีการมีงานทำ การให้หลักประกันสำหรับอนาคต การให้ความดูแลทางด้านสุขภาพ อาหาร เสื้อผ้า ที่อยู่อาศัย การศึกษา เป็นต้น ซึ่งสิทธิขั้นพื้นฐานเหล่านี้ได้รับการพัฒนาชัดเจนครั้งแรกในศตวรรษที่ 19

จากพัฒนาการที่กล่าวมา จะเห็นได้ว่า แนวคิดในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนั้น เป็นสิทธิที่เกิดขึ้นในช่วงที่ 3 ของพัฒนาการ ที่มีการเกิดขึ้นของรัฐธรรมนูญและมีการรับรองสิทธิเสรีภาพไว้ในรัฐธรรมนูญเพื่อเป็นหลักประกันที่มั่นคง ดังปรากฏตัวอย่างในกรณีของรัฐธรรมนูญของสหรัฐอเมริกาและคำประกาศสิทธิมนุษยชนและพลเมือง ค.ศ. 1789 ซึ่งถึงแม้จะมีการกล่าวถึงการคุ้มครองข้อมูลส่วนบุคคลในฐานะสิทธิส่วนบุคคลยังไม่ปรากฏเด่นชัด แต่กระนั้นก็เป็นจุดเริ่มต้นของพัฒนาการทางความคิดของนักนิติศาสตร์จนสามารถแยกสิทธิส่วนบุคคลออกจากสิทธิเสรีภาพของบุคคลทั่วไปได้[14]

---

[13] *เรื่องเดียวกัน*, หน้า 37-41.

[14] กิตติพงศ์ กมลธรรมวงศ์, **การคุ้มครองข่าวสารส่วนบุคคลในระบบกฎหมายไทย: ปัญหาและแนวทางแก้ไข** (วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2549), หน้า 12-13.

แต่อย่างไรก็ดีประเด็นสำคัญที่ต้องพิจารณาต่อไปก็คือ เมื่อพิจารณาจากธรรมชาติของสิทธิเสรีภาพแล้วจะเห็นว่า เป็นสิ่งที่มีพลวัตไปตามสภาพทางสังคมเศรษฐกิจและการเมืองที่มีการเปลี่ยนแปลงอยู่ตลอดเวลา จึงไม่ใช่เรื่องแปลกที่หลังจากโลกเข้าสู่ยุคแห่งการปฏิวัติอุตสาหกรรมครั้งที่ 4 ซึ่งเริ่มขึ้นในช่วงเปลี่ยนศตวรรษที่ผ่านมาและเป็นผลมาจากการปฏิวัติดิจิตอลตามแนวคิดของเคลาส์ ชวาบ (Mr.Klaus Schwab) นักเศรษฐศาสตร์ชื่อดังของโลก ผู้ก่อตั้งและประธานบริหารของสภาเศรษฐกิจโลก (World Economic Forum) เราจะเห็นภาพของการเปลี่ยนแปลงรูปแบบและสาระสำคัญของสิทธิเสรีภาพต่าง ๆ รวมไปถึงจะพบเห็นการกำเนิดขึ้นของสิทธิใหม่ ๆ เกิดขึ้นอีกหลายสิทธิ ซึ่งตัวอย่างที่ดีที่สุดที่จะนำมาแสดงก็คือการเกิดขึ้นของสิทธิบนโลกอินเทอร์เน็ต อันประกอบด้วยสิทธิต่าง ๆ ดังนี้คือ[15]

1. สิทธิในการเข้าถึงอินเทอร์เน็ต
2. สิทธิที่จะไม่ถูกเลือกปฏิบัติในการเข้าถึง, การใช้และการจัดการอินเทอร์เน็ต
3. สิทธิที่จะมีเสรีภาพและความปลอดภัยบนอินเทอร์เน็ต
4. สิทธิในการพัฒนาผ่านอินเทอร์เน็ต
5. เสรีภาพในการแสดงความคิดเห็นและการรับรู้ข้อมูลข่าวสารบนอินเทอร์เน็ต
6. เสรีภาพทางศาสนาและมโนธรรมความเชื่อบนอินเทอร์เน็ต
7. เสรีภาพในการสมาคมและประกอบธุรกิจออนไลน์
8. สิทธิในความเป็นส่วนตัวบนอินเทอร์เน็ต
9. สิทธิที่จะได้รับการปกป้องข้อมูลดิจิตอลบนอินเทอร์เน็ต
10. สิทธิในการศึกษาบนอินเทอร์เน็ตและการศึกษาเกี่ยวกับอินเทอร์เน็ต
11. สิทธิในทางวัฒนธรรมและการเข้าถึงความรู้เกี่ยวกับอินเทอร์เน็ต
12. สิทธิเด็กเกี่ยวกับอินเทอร์เน็ต
13. สิทธิของคนพิการเกี่ยวกับอินเทอร์เน็ต
14. สิทธิแรงงานเกี่ยวกับอินเทอร์เน็ต
15. สิทธิที่จะมีส่วนร่วมในกิจการสาธารณะผ่านอินเทอร์เน็ต
16. สิทธิผู้บริโภคบนอินเทอร์เน็ต
17. สิทธิได้รับบริการด้านสุขภาพและสังคมบนอินเทอร์เน็ต

---

[15] Marianne Franklin, Robert Bodle and Dixie Hawtin, **The Charter of Human Rights and Principles for the Internet** (S.l.: Internet Rights & Principles Coalition, United Nation, 2018), pp.13-26, Retrieved March 10, 2018 from http://internetrights andprinciples.org/site/wp-content/uploads/2018/01/IRPC_english_5th edition.pdf

18. สิทธิได้รับความเป็นธรรมในการพิจารณาและการเยียวยาทางกฎหมายเกี่ยวกับอินเทอร์เน็ต

19. สิทธิได้รับการวางกฎกติกาทางสังคมและทางระหว่างประเทศที่เหมาะสม

สิทธิต่าง ๆ ที่กล่าวมาข้างต้นนี้เป็นผลมาจากการที่กลุ่มความร่วมมือด้านสิทธิและหลักการอินเทอร์เน็ต (Internet Rights and Principles Dynamic Coalition: IRP) ซึ่งเป็นการรวมกลุ่มของทุกภาคส่วนของผู้มีส่วนเกี่ยวข้องกับอินเทอร์เน็ต ไม่ว่าจากภาครัฐ เอกชน และประชาสังคม เห็นชอบร่วมกันประกาศ “10 สิทธิและหลักการอินเทอร์เน็ต”[16] เมื่อวันที่ 31 มีนาคม 2554 ณ

---

[16] “10 สิทธิและหลักการอินเทอร์เน็ต” ประกอบไปด้วย

1) ความเป็นสากล และ ความเสมอภาค มีสาระสำคัญว่า มนุษย์ทุกคนต่างเกิดมามีอิสระและเสมอกันในศักดิ์ศรีและสิทธิต่าง ๆ ซึ่งจะต้องได้รับความเคารพ ปกป้อง และส่งเสริมในสภาพแวดล้อมออนไลน์

2) สิทธิ และ ความยุติธรรมทางสังคม มีสาระสำคัญว่า อินเทอร์เน็ตเป็นพื้นที่เพื่อการส่งเสริม ปกป้อง และบรรลุสิทธิมนุษยชนและพัฒนาความยุติธรรมทางสังคม เราทุกคนมีหน้าที่ผูกพันในการเคารพสิทธิมนุษยชนของคนอื่น ๆ ทั้งหมด ในสิ่งแวดล้อมออนไลน์

3) ความเข้าถึงได้ มีสาระสำคัญว่า คนทุกคนมีสิทธิเสมอกันในการเข้าถึงและใช้อินเทอร์เน็ตที่ปลอดภัยและเปิดกว้าง

4) การแสดงออก และ การสมาคม มีสาระสำคัญว่า คนทุกคนมีสิทธิในการค้นหา ได้รับและแจ้งข้อมูลข่าวสารอย่างเสรีบนอินเทอร์เน็ต โดยไม่ถูกปิดกั้นหรือรบกวนในทางอื่นใด คนทุกคนยังมีสิทธิในการคบค้าสมาคมกันผ่านอินเทอร์เน็ตและบนอินเทอร์เน็ต เพื่อวัตถุประสงค์ทางสังคม การเมือง วัฒนธรรม และวัตถุประสงค์อื่น ๆ

5) ความเป็นส่วนตัว และ การปกป้องข้อมูล มีสาระสำคัญว่า คนทุกคนมีสิทธิในความเป็นส่วนตัวออนไลน์ ซึ่งสิทธิดังกล่าวนี้รวมถึงเสรีภาพในการที่จะพ้นจากการถูกสอดส่องตรวจตรา สิทธิในการใช้การเข้ารหัส และสิทธิที่จะไม่เปิดเผยตัวตนออนไลน์ คนทุกคนยังมีสิทธิที่จะได้รับการคุ้มครองข้อมูล ซึ่งรวมถึงการควบคุมการรวบรวม การเก็บ การประมวล การกำจัด และการเปิดเผยข้อมูลส่วนบุคคล

6) ชีวิต อิสรภาพ และ ความมั่นคงปลอดภัย มีสาระสำคัญว่า สิทธิที่จะมีชีวิต มีอิสรภาพและมีความมั่นคงปลอดภัย จะต้องได้รับการเคารพ ปกป้อง และส่งเสริมในสภาพแวดล้อมออนไลน์ สิทธิเหล่านี้จะต้องไม่ถูกละเมิด หรือใช้เพื่อละเมิดสิทธิอื่น ในสภาพแวดล้อมออนไลน์

กรุงสตอกโฮล์ม ประเทศสวีเดน เพื่อใช้เป็นหลักการพื้นฐานในการพัฒนาและจัดการดูแลอินเทอร์เน็ต ซึ่งหลักการดังกล่าวมีรากฐานมาจากหลักสิทธิมนุษยชนนั่นเอง โดยในข้อที่ 5 สะท้อนภาพชัดเจนของการยอมรับสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ในมิติของสิทธิในความเป็นส่วนตัวบนอินเทอร์เน็ต และสิทธิที่จะได้รับการปกป้องข้อมูลดิจิตอลบนอินเทอร์เน็ต ดังจะเห็นได้จากข้อความที่ว่า “ความเป็นส่วนตัว และ การปกป้องข้อมูล มีสาระสำคัญว่า คนทุกคนมีสิทธิในความเป็นส่วนตัวออนไลน์ ซึ่งสิทธิดังกล่าวนี้รวมถึงเสรีภาพในการที่จะพ้นจากการถูกสอดส่องตรวจตรา สิทธิในการใช้การเข้ารหัส และสิทธิที่จะไม่เปิดเผยตัวตนออนไลน์ คนทุกคนยังมีสิทธิที่จะได้รับการคุ้มครองข้อมูลซึ่งรวมถึงการควบคุมการรวบรวม การเก็บ การประมวล การกำจัด และการเปิดเผยข้อมูลส่วนบุคคล”

แต่อย่างไรก็ดี หากพิจารณาในทางด้านสิทธิเสรีภาพบนโลกอินเทอร์เน็ตแล้วจะเห็นด้วยพลวัตที่ไม่หยุดยั้งในทางเทคโนโลยีนั้น ลำพังการกำกับดูแลจากภาครัฐโดยอาศัยกฎหมายของรัฐหรือกติการะหว่างประเทศ อาจจะยังไม่เพียงพอต่อการคุ้มครองสิทธิเสรีภาพใหม่ ของโลกที่ทันสมัยเช่นนี้ ดังนั้น การสร้างกฎหมายบนโลกอินเทอร์เน็ต (Internet Law) ควรจะต้องมีพื้นฐานและพัฒนามาจากวัฒนธรรมในทางกติกาบนโลกอินเทอร์เน็ต (Internet Legal Culture) อันเป็นกรอบกติกาใหม่ที่เกี่ยวข้องกับแนวคิดอำนาจอธิปไตยบนโลกอินเทอร์เน็ตอันไม่ได้จำกัดอยู่ภายใต้เขตอำนาจอธิปไตยทางดินแดนของรัฐใดรัฐหนึ่งอีกต่อไป รูปแบบของกติกาเช่นนี้เรียกว่า Lex Informatica ซึ่ง

---

7) ความหลากหลาย มีสาระสำคัญว่า ความหลากหลายทางภาษาและวัฒนธรรมบนอินเทอร์เน็ต จะต้องได้รับการส่งเสริม นวัตกรรมทางเทคโนโลยีและทางนโยบายควรได้รับการสนับสนุนเพื่ออำนวยความเป็นพหุลักษณ์ของการแสดงออก

8) ความเสมอภาคทางโครงข่าย มีสาระสำคัญว่า คนทุกคนจะต้องมีช่องทางเข้าถึงเนื้อหาอินเทอร์เน็ตที่เปิดกว้างและไม่เลือกปฏิบัติ เป็นอิสระจากการถูกจัดลำดับ กรองและควบคุมการจราจรอย่างแบ่งแยก ไม่ว่าจะด้วยเหตุผลทางการค้า การเมือง หรือเหตุผลอื่นใด

9) มาตรฐาน และ การวางข้อกำหนด มีสาระสำคัญว่า สถาปัตยกรรม ระบบสื่อสาร และรูปแบบเอกสารและข้อมูล ของอินเทอร์เน็ต จะต้องอยู่บนฐานของมาตรฐานเปิด ที่จะทำให้แน่ใจได้ว่าคนทุกคนจะสามารถประสานงานระหว่างกันได้อย่างสมบูรณ์ ไม่ถูกกันออกไป และได้รับโอกาสอย่างเท่าเทียมกัน

10) การจัดการดูแล มีสาระสำคัญว่า สิทธิมนุษยชนและความยุติธรรมทางสังคม จะต้องเป็นสิ่งที่ประกอบขึ้นเป็นพื้นฐานทางกฎหมายและแบบแผนปฏิบัติ ซึ่งอินเทอร์เน็ตจะใช้ดำเนินการและถูกจัดการดูแล สิ่งนี้จะต้องเกิดขึ้นอย่างโปร่งใสและเป็นไปในลักษณะพหุภาคี บนหลักการของความเปิดกว้าง การมีส่วนร่วมอย่างครอบคลุม และการให้เหตุผลและรับผิดได้

คำ ๆ นี้ถูกใช้ครั้งแรกโดย W. H. van Boom และ J. H. M. van Erp[17] นอกจากนี้ในช่วงระยะเวลาใกล้เคียงกัน Joel R. Reidenberg[18] ก็ได้เขียนบทความโดยใช้คำนี้เช่นเดียวกัน โดยกล่าวได้ว่า Lex Informatica เป็นหลักการที่เกิดขึ้นคล้ายคลึงกับการเกิดขึ้นของ Lex Mercatoria หรือกฎหมายของกลุ่มพ่อค้า ซึ่งสามารถบังคับกันเองได้ในฐานะที่ทุกฝ่ายเท่าเทียมอยู่ในฐานะระดับเดียวกัน (Horizontal Mechanisms) โดยที่ไม่ต้องอาศัยอำนาจรัฐเข้ามาเกี่ยวข้อง หรือเข้ามาเกี่ยวข้องน้อยที่สุด[19] แต่อย่างไรก็ดี แนวคิดเหล่านี้ยังไม่ได้รับการยอมรับจากทางฝ่ายรัฐเท่าที่ควร ซึ่งในประเด็นนี้เป็นประเด็นที่ต้องรอคอยพลวัตของสังคมกันต่อไป

2.1.1.3 ประเภทของสิทธิเสรีภาพ

เมื่อเรายอมรับว่า สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล เป็นสิทธิประเภทหนึ่งจึงจำเป็นต้องพิจารณาว่าสิทธิเช่นนี้ เป็นสิทธิประเภทใด ดังนั้นในเบื้องต้นจึงต้องทำความเข้าใจว่า หลักเกณฑ์ในการจำแนกหรือแนวคิดในการแบ่งประเภทสิทธินั้นใช้หลักเกณฑ์ในการพิจารณาอย่างไร

สำหรับแนวคิดในการแบ่งแยกสิทธิและเสรีภาพนั้น จะได้อธิบายถึงหลักเกณฑ์ในการแบ่งแยกออกเป็น 2 หลักเกณฑ์คือ หลักเกณฑ์ในการแบ่งแยกสิทธิและเสรีภาพตามแนวความคิดทางการเมือง และ หลักเกณฑ์ในการแบ่งแยกสิทธิและเสรีภาพโดยพิจารณาจากเนื้อหาของสิทธิและเสรีภาพ โดยมีสาระสำคัญดังนี้

1. การแบ่งสิทธิเสรีภาพตามแนวคลาสสิคของเยอรมัน

แนวคิดนี้มีที่มาจาก Georg Jellinek เป็นผู้เสนอแนวคิด โดยได้จำแนกสิทธิเสรีภาพบนพื้นฐานความสัมพันธ์ระหว่างปัจเจกชนกับรัฐไว้ ว่าความสัมพันธ์ดังกล่าวสะท้อนออกมาเป็นสถานะต่าง ๆ 3 ประเภท คือ[20]

---

[17] W. H. van Boom and J. H. M. van Erp, Electronic Highways: on the Road to Liability, In **Emerging Electronic Highways,** V. Bekkers et al., eds. (Netherland: Kluwer Law International, 1996), pp. 153-164.

[18] Joel R. Reidenberg, “Lex Informatica: The Formulation of Information Policy Rules through Technology,” **Texas Law Review** 76 (1998): 554-555.

[19] Radim Polčák and Dan Jerker B. Svantesson, **Information Sovereignty Data Privacy, Sovereign Powers and the Rule of Law** (Massachusetts: Edward Elgar, 2017), p. 114.

[20] บรรเจิด สิงคะเนติ, *เรื่องเดิม*, หน้า 52-55.

ประเภทแรก Status Negativus ซึ่งหมายถึง กลุ่มของสิทธิและเสรีภาพที่การใช้สิทธิและเสรีภาพของปัจเจกบุคคลจะต้องปราศจากการเข้ามาแทรกแซงของรัฐ หรือกล่าวอีกนัยหนึ่ง คือ มีลักษณะเป็นสิทธิในการป้องกัน คือ สิทธิที่ผู้ทรงสิทธิสามารถเรียกร้องให้รัฐงดเว้นกระทำการ ที่ก้าวล่วงแดนแห่งสิทธิของตน เช่น เสรีภาพในการนับถือศาสนา เสรีภาพในเคหสถาน เสรีภาพในการสื่อสาร สิทธิและเสรีภาพในชีวิตและร่างกาย เสรีภาพในการแสดงความคิดเห็น และเสรีภาพในทางวิชาการ ฯลฯ เป็นต้น

ประเภทที่สอง Status Positivus หมายถึงกลุ่มของสิทธิที่การใช้สิทธิและเสรีภาพของปัจเจกบุคคลมิอาจบรรลุความมุ่งหมายได้หากปราศจากการเข้ามาดำเนินการอย่างใดอย่างหนึ่งจากฝ่ายรัฐ สิทธิเสรีภาพประเภทนี้จะแสดงออกมาในลักษณะของสิทธิเรียกร้อง คือ ผู้ทรงสิทธิสามารถเรียกร้องให้รัฐกระทำการในสิ่งที่ให้ประโยชน์แก่ตน เช่น สิทธิในการได้รับการศึกษาขั้นพื้นฐาน สิทธิในการได้รับบริการทางสาธารณสุข สิทธิในการได้รับการเลี้ยงดูและการศึกษาอบรมจากรัฐของเด็กและเยาวชน สิทธิในการได้รับความช่วยเหลือจากรัฐของบุคคลซึ่งมีอายุเกินหกสิบปีบริบูรณ์ สิทธิที่จะได้รับความสะดวกอันเป็นสาธารณะและความช่วยเหลือจากรัฐของผู้พิการ และ สิทธิเรียกร้องให้รัฐคุ้มครองตนเองในทางกฎหมายโดยผ่านสถาบันศาล

ประเภทที่สาม Status Activus หมายถึง กลุ่มของสิทธิที่ปัจเจกบุคคลใช้สิทธิของตนในการเข้าไปมีส่วนร่วมในการสร้างเจตจำนงแห่งรัฐ คือ ผู้ทรงสิทธิสามารถเรียกร้องการเข้ามีส่วนร่วมทางการเมืองได้ หรือสามารถเข้าไปมีส่วนร่วมกับองค์กรของรัฐ สิทธิเสรีภาพประเภทนี้จะมีการบัญญัติรับรองออกมาในรูปสิทธิของพลเมือง อันได้แก่สิทธิของผู้มีสิทธิเลือกตั้ง สิทธิในการสมัครรับราชการ สิทธิในการจัดตั้งพรรคการเมือง ทั้งนี้ สิทธิประเภทนี้มักจะจำกัดให้เฉพาะพลเมืองในชาตินั้น

2. การแบ่งโดยพิจารณาจากผู้ทรงสิทธิ

แนวคิดนี้แยกสิทธิและเสรีภาพโดยพิจารณาจากผู้ซึ่งได้รับสิทธิตามรัฐธรรมนูญหรือบุคคลซึ่งรัฐธรรมนูญมุ่งที่จะให้ความคุ้มครอง ซึ่งอาจแบ่งสิทธิเสรีภาพได้ดังนี้[21]

ประเภทแรกคือ สิทธิมนุษยชนหรือสิทธิของทุกคน (Menschenrdchte หรือ Jedermannrechte)

ประเภทที่สองคือ สิทธิพลเมือง (Buergerrechte)

ซึ่งรายละเอียดจะได้กล่าวในลำดับต่อไป

---

[21] *เรื่องเดียวกัน*.

3. การแบ่งสิทธิและเสรีภาพโดยพิจารณาจากเงื่อนไขการจำกัดสิทธิและเสรีภาพ

เป็นการพิจารณาว่า สิทธิและเสรีภาพนั้น ๆ เป็นสิทธิที่อยู่ภายใต้เงื่อนไขของกฎหมายหรือไม่ หรือหากอยู่ภายใต้เงื่อนไขกฎหมายในการจำกัดสิทธิเสรีภาพแล้วจะอยู่ในเงื่อนไขประเภทใด ซึ่งมีการกำหนดเงื่อนไขของกฎหมายไว้ 3 รูปแบบ คือ[22]

รูปแบบแรก สิทธิและเสรีภาพกับเงื่อนไขของกฎหมายทั่วไป (Grundrechte Mit Einfachem)

กรณีนี้รัฐธรรมนูญเพียงแต่เรียกร้องว่าการจำกัดสิทธิเสรีภาพจะกระทำได้ก็แต่โดยบทบัญญัติของกฎหมาย สิทธิเสรีภาพกับเงื่อนไขของกฎหมายทั่วไปนี้ไม่ได้เรียกร้องเงื่อนไขพิเศษในการจำกัดสิทธิเสรีภาพประการอื่น

รูปแบบที่สอง สิทธิและเสรีภาพกับเงื่อนไขกฎหมายพิเศษ (Grundrerecht Mit Qualifizerterm Gesetzesvorbehalt) กรณีนี้รัฐธรรมนูญจะกำหนดเรียกร้องว่า การแทรกแซงสิทธิและเสรีภาพโดยกฎหมายนั้นต้องผูกพันกับสถานการณ์ใดสถานการณ์หนึ่งหรือต้องผูกพันอยู่กับวัตถุประสงค์ใดวัตถุประสงค์หนึ่ง หรือจะต้องดำเนินการโดยวิธีการที่กำหนดไว้ในรัฐธรรมนูญเท่านั้น

รูปแบบสาม สิทธิและเสรีภาพที่ปราศจากเงื่อนไขของกฎหมาย (Grundrerecht Ohne Qualifizerterm Gesetzesvorbehalt) กรณีที่รัฐธรรมนูญได้กำหนดสิทธิและเสรีภาพนั้นไม่อยู่ภายใต้การจำกัดใด ๆ ทั้งสิ้น

การแบ่งสิทธิเสรีภาพประเภทนี้จะสามารถทำให้เข้าใจถึงประเภทของเงื่อนไขในการจำกัดสิทธิและเสรีภาพ ซึ่งจะเป็นประโยชน์ในการตรวจสอบอำนาจนิติบัญญัติในการบัญญัติกฎหมายเพื่อจำกัดสิทธิต่าง ๆ ว่าเป็นไปตามเงื่อนไขที่รัฐธรรมนูญกำหนดไว้หรือไม่นั่นเอง[23]

ดังนั้นจากที่อธิบายทั้งหมด ประเด็นจึงน่าสนใจว่า สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนั้นจะมีลักษณะเป็นสิทธิเสรีภาพประเภทใด ซึ่งในการนี้ขอนำแนวทางการแบ่งประเภทของสิทธิเสรีภาพ โดยพิจารณาจากผู้ทรงสิทธิ มาเป็นเกณฑ์ในการอธิบาย ภายใต้เกณฑ์ผู้ทรงสิทธินี้จะเห็นว่ามีการแบ่งสิทธิออกเป็น 2 ประเภทดังที่ได้กล่าวไว้แล้วเบื้องต้น กล่าวคือ

1. สิทธิพลเมือง

หมายถึง สิทธิและเสรีภาพในอันที่จะเข้าไปมีส่วนร่วมในกระบวนการสร้างเจตจำนงทางการเมืองของรัฐหรือเข้าไปมีส่วนร่วมในองค์กรของรัฐ สิทธิพลเมืองจึงมีได้เฉพาะแต่เวลาภายหลังที่รัฐได้ถือกำเนิดขึ้นมาแล้วเท่านั้น และรัฐต่าง ๆ มักจะบัญญัติรับรองและคุ้มครองสิทธิประเภทนี้ให้แก่พลเมืองของตนเท่านั้น หากบุคคลใดเข้ามาอยู่ในขอบอำนาจรัฐที่ใช้รัฐธรรมนูญ บุคคลนั้นหาก

---

[22] *เรื่องเดียวกัน*, หน้า 55.

[23] *เรื่องเดียวกัน*.

ไม่ได้เป็นพลเมือง ก็ย่อมไม่ได้รับความคุ้มครอง เพราะผู้ทรงสิทธิ ในกรณีของสิทธิพลเมือง คือ ประชาชนซึ่งเป็นพลเมืองของรัฐ

ดังนั้น สิทธิประเภทนี้ได้แก่ สิทธิที่รัฐธรรมนูญมุ่งที่จะให้ความคุ้มครองเฉพาะบุคคลที่เป็นพลเมืองของรัฐเท่านั้น ถือเป็นสิทธิที่เกี่ยวข้องตามกฎหมายของรัฐ เช่น สิทธิในการออกเสียงเลือกตั้ง สิทธิในการลงสมัครรับเลือกตั้ง สิทธิในการจัดตั้งพรรคการเมือง ฯลฯ เป็นต้น นอกจากนี้ สิทธิพลเมือง อาจปรากฏในรูปของ สิทธิทางสังคม (Social Right) เป็นสิทธิของประชาชนทางสังคมที่จะได้รับบริการจากสังคม ในฐานะที่เป็นสมาชิกของสังคม เช่น สิทธิการเข้าถึงการบริการสาธารณะ เป็นต้น หรือสิทธิในทางสวัสดิการสังคม (Social Welfare Right) เป็นสิทธิของประชาชนทุกคนที่จะได้รับสวัสดิการทางสังคม เช่น สิทธิการได้รับการศึกษา และหมายรวมสิทธิทางวัฒนธรรม (Cultural Right) ได้แก่ สิทธิเข้าร่วมในพิธีกรรม ประเพณีวัฒนธรรม ต่าง ๆ จึงกล่าวได้ว่า สิทธิใดที่รัฐกำหนดไว้ในรัฐธรรมนูญเพื่อมอบความคุ้มครองให้แก่พลเมืองของรัฐของตน ถือเป็นสิทธิพลเมืองทั้งสิ้น

2. สิทธิมนุษยชน

หมายถึง สิทธิและเสรีภาพที่ติดตัวมนุษย์ทุกคนมาตั้งแต่เกิด และไม่อาจถูกพรากไปจากมนุษย์ได้โดยไม่เป็นทำลายความเป็นมนุษย์ของผู้นั้น สิทธิมนุษยชนจึงเป็นคุณลักษณะประจำตัวของมนุษย์ และเป็นสิ่งที่มนุษย์ทุกคนพึงมีในฐานะที่เกิดมาเป็นมนุษย์ มนุษย์ทุกคนจึงมีสิทธิและเสรีภาพนี้อยู่แล้วตั้งแต่ก่อนที่จะมีรัฐเกิดขึ้น ไม่มีมนุษย์ผู้ใดสามารถสละสิทธิและเสรีภาพนี้ได้โดยชอบ และไม่มีผู้ปกครองคนใดหรือคณะใดที่จะมีอำนาจทำลายสิทธิและเสรีภาพเหล่านี้[24] สิทธิมนุษยชนจึงเป็น สิทธิที่รัฐธรรมนูญมุ่งให้ความคุ้มครองแก่ทุก ๆ คน โดยไม่ได้แบ่งแยกว่าบุคคลนั้นจะเป็นคนของชาติใด เชื้อชาติใด หรือศาสนาใด หากบุคคลนั้นเข้ามาอยู่ในขอบเขตอำนาจรัฐ ย่อมได้รับความคุ้มครองของภายใต้รัฐธรรมนูญของประเทศนั้น ๆ ด้วย ดังนั้น สิทธิมนุษยชนจึงเป็นสิทธิและเสรีภาพที่รัฐธรรมนูญมุ่งให้ความคุ้มครองแก่บุคคลทุกคนโดยไม่เลือกปฏิบัติในทุกกรณี หากบุคคลเข้ามาอยู่ในขอบอำนาจรัฐที่ใช้รัฐธรรมนูญของรัฐใดก็ตาม บุคคลดังกล่าวย่อมได้รับความคุ้มครอง[25]

ดังนั้น เราจึงสรุปลักษณะสำคัญที่สุดของสิทธิมนุษยชนได้ ดังต่อไปนี้[26]

ประการแรก สิทธิมนุษยชนนั้นกำเนิดขึ้นบนพื้นฐานของความเคารพต่อศักดิ์ศรีความเป็นมนุษย์และความคุณค่าของมนุษย์แต่ละคน

---

[24] วรพจน์ วิศรุตพิชญ์, **สิทธิและเสรีภาพตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540** (กรุงเทพมหานคร: วิญญูชน, 2543), หน้า 22.

[25] บรรเจิด สิงคะเนติ, *เรื่องเดิม*, หน้า 53.

[26] United Nations, **Human Rights: A Basic Handbook for UN Staff**, p. 3, Retrieved March 10, 2018 from http://www.ohchr.org/Documents/Publications/HR handbooken.pdf

ประการที่สอง สิทธิมนุษยชนมีลักษณะเป็นสากลและเป็นการทั่วไป ซึ่งหมายความว่า สิทธิมนุษยชนนี้จะให้ความคุ้มครองมนุษย์ทุกคนอย่างเท่าเทียมและไม่เลือกปฏิบัติ

ประการที่สาม สิทธิมนุษยชนเป็นสิ่งที่โอนไปไม่ได้

ประการที่สี่ สิทธิมนุษยชนนั้นไม่อาจแบ่งแยก, มีความสัมพันธ์กัน และ อยู่ในลักษณะพึ่งพาอาศัยกัน

เมื่อพิจารณาแล้วในเบื้องต้นจะเห็นว่า สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนั้นถือเป็นประเภทหนึ่งของสิทธิในความเป็นส่วนตัวจึงมีลักษณะเป็นสิทธิมนุษยชน ซึ่งรายละเอียดจะได้กล่าวในหัวข้อถัดไป

2.1.2 สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในฐานะสิทธิมนุษยชน

ในหัวข้อนี้จะได้พิจารณาสถานะทางกฎหมายของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล กล่าวคือ ธรรมชาติของมนุษย์แม้ว่าจะเป็นสัตว์สังคมที่จำเป็นจะต้องอยู่ร่วมกับบุคคลอื่นในลักษณะของการพึ่งพาอาศัยซึ่งกันและกันอย่างซับซ้อนจนมีลักษณะของการเป็นสังคมก็ตาม แต่ทว่าในอีกมิติหนึ่ง มนุษย์แต่ละคนนั้นยังคงมีความต้องการที่จะแยกตัวออกจากสังคมบ้างในบางครั้งคราวหรือบางเรื่องบางกรณี จึงกล่าวได้ว่า โดยแท้จริงแล้วมนุษย์แต่ละคนนั้นยังคงต้องการความเป็นส่วนตัวหรือพื้นที่ส่วนตัวเพื่อแยกตัวเองออกจากสังคม[27] ซึ่งความเป็นส่วนตัวนี้ได้ถูกพัฒนายกระดับขึ้นมาจนกระทั่งได้รับการยอมรับกันในหลายสังคมว่ามีความเป็นสิทธิ คือเป็นคุณค่าที่กฎหมายในหลายประเทศรวมถึงกติการะหว่างประเทศได้ทำการรับรองและคุ้มครองให้ โดยจะเห็นว่าสิทธิในความเป็นส่วนตัวนี้มีพื้นฐานตั้งต้นมาจากสิทธิเสรีภาพในชีวิตและร่างกายที่เรียกร้องให้รัฐหรือผู้อื่นไม่เข้ามาแทรกแซงหรือล่วงละเมิด จนพัฒนาไปสู่การเป็นสิทธิที่จะอยู่ตามลำพัง อันเป็นสิทธิของบุคคลที่จะให้หรือไม่ให้ข้อมูลเกี่ยวกับชีวิตส่วนตัว พฤติกรรมส่วนตัว นิสัยส่วนตัว และความสัมพันธ์ส่วนตัวกับผู้อื่น ดังที่ Samel Warren และ Louis Brandeis ได้อธิบายไว้ว่า สิทธิในความเป็นส่วนตัวนี้ก่อให้เกิดความสงบแก่จิตใจ ซึ่งการล่วงล้ำแทรกแซงความเป็นส่วนตัวนี้จะก่อให้เกิดความเจ็บปวดและทุกข์ใจ (Mental Pain and Distress) แก่เจ้าของสิทธิ[28] ดังนั้น การคุ้มครองสิทธิในความเป็นส่วนตัวนี้จึง

---

[27] Karl Mannheim, **Systematic Sociology: An Introduction to the Study of Society** (New York: Routledge, 2013), p. 61.

[28] Samuel D. Warren and Louis D. Brandeis, “The Right to Privacy,” **Harvard Law Review** 4, 5 (December 15, 1890): 196.

มุ่งเน้นที่จะต้องคุ้มครองสภาพภายในหรือจิตใจของบุคคลเป็นสำคัญ[29] เราจึงจะเห็นว่า สิทธิในความเป็นส่วนตัวนี้ แยกออกได้จากสิทธิในทรัพย์สิน (The Right to Property) และแยกออกได้จากสิทธิในเสรีภาพ (Right to Liberty) นั่นเองเพราะวัตถุแห่งการคุ้มครองไม่ได้อยู่ที่ทรัพย์สินหรือการคุ้มครองอิสระเสรีในขอบเขตอย่างกว้างแต่เป็นการมุ่งเน้นคุ้มครองถึงจิตใจมากกว่าดังที่กล่าวมา

ดังนั้นการกำหนดนิยามของสิทธิในความเป็นส่วนตัวจึงไม่ใช่เรื่องง่าย การตั้งคำถามว่าอะไรคือความเป็นส่วนตัว จึงเป็นคำถามที่อยู่ทั้งในมิติของสหศาสตร์ ไม่ว่าจะเป็นกฎหมาย ปรัชญา สังคมวิทยา รวมไปถึงจิตวิทยาด้วย โดยความเป็นส่วนตัวนี้เชื่อมโยงกับแนวคิดเรื่องศักดิ์ศรีของความเป็นมนุษย์ (Human Dignity) การยอมรับหรือเคารพตัวตน (Autonomy) การเคารพในอัตลักษณ์ของบุคคล (Personhood) ซึ่งการแทรกแซงถือเป็นการล่วงละเมิดต่อคุณค่านี้[30] การยอมรับคุณค่าเช่นนี้จะเป็นหลักการอันเป็นป้อมปราการสำคัญที่จะต่อต้านการแทรกแซงและกดขี่การจากใช้อำนาจตามอำเภอใจ โดยการกำหนดระดับของคุณค่าของความเป็นส่วนตัวขึ้นอยู่กับบริบทของแต่ละศาสตร์ รวมถึงแต่ละสังคม สำหรับในทางด้านกฎหมายการพิจารณาคุณค่าความเป็นส่วนตัวก็ขึ้นอยู่กับระดับของการรับรองสิทธิโดยกฎหมาย

สำหรับสิทธิในความเป็นส่วนตัวที่ได้กล่าวมา มีความเชื่อมโยงมาถึงข้อมูลส่วนบุคคล เพราะข้อมูลส่วนบุคคลถือว่าเป็นสิ่งเฉพาะตัวของเจ้าของข้อมูล ไม่ว่าจะเป็นข้อมูลการศึกษา ฐานะการเงิน อาชีพและประวัติการทำงาน ประวัติสุขภาพ ประวัติอาชญากรรม ฯลฯ เป็นต้นซึ่งสามารถระบุตัวเจ้าของข้อมูลได้ถือว่าเป็นความลับของเจ้าของข้อมูล หากมีการเข้ามาแสวงหาประโยชน์จากข้อมูลโดยมิชอบก็ถือว่าเป็นการกระทำที่แทรกแซงความเป็นส่วนตัวของเจ้าของข้อมูลนั่นเอง ซึ่งประเด็นนี้ Alan Westin ได้อธิบายไว้ในบทความเรื่อง Privacy and Freedom ว่าสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนั้น เป็นสิทธิเรียกร้องของปัจเจกชน กลุ่มบุคคล หรือสถาบัน ที่จะตัดสินใจว่าข้อมูลของตนนั้นจะถูกใช้เมื่อไหร่ อย่างไร หรือจะถูกส่งต่อแค่ไหนและไปยังใคร[31] กล่าวอีกนัยหนึ่งก็คือ เป็นการรับรองให้แก่เจ้าของข้อมูลที่จะมีอำนาจเหนือข้อมูลส่วนบุคคลของตนนั้นเอง และสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนี้ก็ไม่ใช่เป็นเรื่องของกรรมสิทธิ ทั้งนี้เพราะหากเป็นกรรมสิทธิ์เหนือข้อมูล ผู้ที่เป็นผู้เก็บรวบรวมข้อมูลย่อมมีฐานะเป็นเจ้าของ แต่ สิทธิในความเป็น

---

[29] กิตสุรณ สังขสุวรรณ์, “การรับรองและข้อจำกัดสิทธิในความเป็นส่วนตัวภายใต้กฎหมายไทย,” **วารสารกฎหมาย คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย** 36, 2 (กันยายน 2561): 271.

[30] Maria Tzanou, **The Fundamental Right to Data Protection: Nomative Value in the Context of Counter-Terrorism Surveillance** (Oregon: Hart, 2017), p. 8.

[31] *Ibid.,* p. 11.

ส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล เป็นสิทธิในความเป็นส่วนตัวของเจ้าของในเรื่องข้อมูลของตนอันเป็นสิทธิและเสรีภาพของเจ้าของข้อมูล

จากที่กล่าวมาจะเห็นได้ว่า สิทธิในความเป็นส่วนตัวมีลักษณะของการจำกัดการล่วงล้ำ (Limited Access the Self) และสิทธินี้มีความเกี่ยวพันกับข้อมูลส่วนบุคคลที่ถือว่าเป็นความลับของตน โดยสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลจึงเป็นสิทธิเสรีภาพที่มีคุณค่าและมีสถานะในทางกฎหมายสามระดับ คือ เป็นสิทธิอันเกี่ยวกับศักดิ์ศรีความเป็นมนุษย์ เป็นสิทธิเสรีภาพของบุคคลที่ได้รับการรับรองและคุ้มครองตามหลักสากลและกฎเกณฑ์ระหว่างประเทศด้านสิทธิมนุษยชน และเป็นสิทธิเสรีภาพของบุคคลที่ได้รับการรับรองและคุ้มครองตามรัฐธรรมนูญแห่งราชอาณาจักรไทย สถานะทางกฎหมายของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลทั้งสามระดับนี้ นำมาซึ่งผลในทางกฎหมายสำคัญในหลายประการได้แก่[32]

ประการที่หนึ่ง สิทธิเกี่ยวกับข้อมูลส่วนบุคคลเป็นสิทธิและเสรีภาพขั้นพื้นฐานของมนุษย์ที่จะต้อง “ได้รับการเคารพ” จากบุคคลทั้งหลายในอันที่จะต้องไม่กระทำการใด ๆ ที่เป็น “การแทรกแซง” หรือ “ล่วงละเมิด” สิทธิส่วนบุคคลเกี่ยวกับข้อมูลส่วนบุคคลที่เกี่ยวกับตน โดยนัยดังกล่าวนี้ สิทธิเกี่ยวกับข้อมูลส่วนบุคคลจึงต้องได้รับ “การเคารพ” ทั้งจากภาครัฐหรือปัจเจกชน กล่าวคือ ปัจเจกชนด้วยกันจะต้องไม่กระทำการใด ๆ ที่เป็นการแทรกแซงหรือละเมิดสิทธิเกี่ยวกับข้อมูลส่วนบุคคลของปัจเจกชนอื่น ในส่วนของภาครัฐเอง นอกจากองค์กรของรัฐหรือเจ้าหน้าที่ของรัฐจะต้องไม่กระทำการใด ๆ ที่เป็นการแทรกแซงหรือละเมิดสิทธิของบุคคลทั้งหลายเกี่ยวกับข้อมูลส่วนบุคคลของบุคคลนั้นซึ่งเป็น “หน้าที่ละเว้นการกระทำ” เช่นกันแล้ว รัฐหรือองค์กรของรัฐยังมีหน้าที่จะต้องกำหนดกลไกหรือมาตรการทางกฎหมายเพื่อให้ความคุ้มครองสิทธิเกี่ยวกับข้อมูลส่วนบุคคลของบุคคลทั้งหลายซึ่งเป็น “หน้าที่กระทำการ” อีกด้วย นอกจากนี้ บุคคลที่สิทธิในความเป็นส่วนตัวของตนถูกละเมิดโดยไม่ชอบ ยังมีสิทธิได้รับการเยียวยาความเสียหายอย่างแท้จริง (Effective Remedy) อีกด้วย

ประการที่สอง สิทธิในความเป็นส่วนตัวของบุคคล ไม่ใช่ สิทธิเด็ดขาด และรัฐอาจมีความจำเป็นที่จะต้องกำหนดมาตรการหรือกระทำการบางอย่างอันมีผลเป็นการแทรกแซงสิทธิเกี่ยวกับข้อมูลส่วนบุคคลของคนบางกลุ่มบางประเภท อย่างไรก็ตาม รัฐหรือองค์กรของรัฐจะกระทำการหรือกำหนดมาตรการอันมีผลเป็นการแทรกแซงสิทธิเกี่ยวกับข้อมูลส่วนบุคคลได้ก็ต่อเมื่อเป็นไปตามเงื่อนไขต่าง ๆ ทีกำหนดไว้ในกฎหมาย หรือ กฎเกณฑ์ระหว่างประเทศด้านสิทธิมนุษยชนโดยเคร่งครัด โดยตั้งอยู่บนพื้นฐานของ “หลักการสำคัญ” สามประการอันได้แก่ หลักความโปร่งใส (Transparacy)

---

[32] นนทวัชร์ นวตระกูลพิสุทธิ์, “สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลกับมาตรการคุ้มครองตาม ร่าง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....,” **วารสารนิติศาสตร์** 43, 4 (ธันวาคม 2557): 741-742.

หลักประโยชน์สาธารณะ (Public Interest) หลักความจำเป็นและความได้สัดส่วน (Necessity and Proportionality)

ประการที่สาม รัฐหรือองค์กรของรัฐและปัจเจกชนจะต้องเคารพต่อสิทธิเกี่ยวกับข้อมูลส่วนบุคคลของบุคคลอื่นทั้งหลาย และจะต้องละเว้นการกระทำการใด ๆ ที่จะมีผลเป็นการแทรกแซงหรือละเมิดสิทธิเกี่ยวกับข้อมูลส่วนบุคคลของบุคคลต่าง ๆ โดยมิชอบ หากรัฐหรือองค์กรของรัฐสามารถดำเนินการใด ๆ อันจะมีผลเป็นการแทรกแซงสิทธิเกี่ยวกับข้อมูลส่วนบุคคลของบุคคลอื่นได้จะต้องเป็นไปตามเงื่อนไขประการต่าง ๆ ดังกล่าวข้างต้นโดยเคร่งครัด ดังนั้น “ข้อยกเว้น” ของการดำเนินการที่จะมีผลเป็นการแทรกแซงสิทธิเกี่ยวกับข้อมูลส่วนบุคคลของบุคคลอื่นจึง “จำกัด” อยู่เฉพาะแต่กรณีการดำเนินมาตรการของรัฐหรือองค์กรของรัฐเท่านั้น และการดำเนินมาตรการอันเป็นข้อยกเว้นนั้นจะต้องเป็นไปตามหลักและเงื่อนไขของกฎหมายและกฎเกณฑ์ระหว่างประเทศด้านสิทธิมนุษยชนกำหนดไว้โดยเคร่งครัด

โดยนัยดังกล่าว ปัจเจกชนหรือเอกชนด้วยกันจึงมิอาจยกเหตุเกี่ยวกับประโยชน์สาธารณะขึ้นเป็นข้อกล่าวอ้างเพื่อกระทำการใด ๆ อันจะมีผลเป็นการแทรกแซงหรือละเมิดสิทธิเกี่ยวกับข้อมูลส่วนบุคคลของปัจเจกชนหรือบุคคลอื่นได้แต่ประการใด ดังนั้น โดยหลักแล้ว ปัจเจกชนหรือเอกชนจึงมิอาจกระทำการใด ๆ อันมีผลเป็นการแทรกแซงสิทธิเกี่ยวกับข้อมูลส่วนบุคคลของบุคคลอื่น มิฉะนั้นย่อมจะเป็นการกระทำอันเป็นการ “ละเมิดสิทธิมนุษยชน” ของบุคคลที่เกี่ยวข้องกับข้อมูลส่วนบุคคล (หรือเจ้าของข้อมูล) เนื่องจากบุคคลทุกคนย่อมเสมอภาคกันในกฎหมายและได้รับความคุ้มครองตามกฎหมายเท่าเทียมกัน อีกทั้งบุคคลจะใช้สิทธิและเสรีภาพของตนได้เท่าที่ไม่ละเมิดต่อสิทธิเสรีภาพของบุคคลอื่น อย่างไรก็ตาม ปัจเจกชนหรือเอกชนจะกระทำการอันจะมีผลเป็นการแทรกแซงสิทธิเกี่ยวกับข้อมูลส่วนบุคคลของบุคคลอื่นได้ก็ย่อมจะต้องอาศัย “ความสมัครใจ” หรือ “ความยินยอม” ของบุคคลที่เป็นเจ้าของข้อมูลเป็นสำคัญเพียงประการเดียวเท่านั้น[33] ซึ่งหลักการนี้จะเป็นฐานสำคัญในการยกเว้นให้มีการเก็บรวบรวม ใช้ หรือเปิดเผย หรือดำเนินการประการอื่น ๆ เกี่ยวกับข้อมูลส่วนบุคคลได้โดยไม่ผิดหลักการคุ้มครองข้อมูลส่วนบุคคลที่กำหนดไว้ในกฎหมายและกติการะหว่างประเทศซึ่งจะได้กล่าวถึงต่อไป

2.2 แนวคิดและหลักการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล

สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล เป็นส่วนหนึ่งของแนวคิดสิทธิในความเป็นส่วนตัว (Right to Privacy) อันเป็นแนวความคิดที่สำคัญและมีพัฒนาการมาอย่างยาวนานในสังคม

---

[33] *เรื่องเดียวกัน*.

ตะวันตก สำหรับประเทศไทยนั้นยังขาดพัฒนาการในส่วนที่เกี่ยวกับระบบกฎหมายซึ่งจำเป็นจะต้องมีการพัฒนาต่อไปเพื่อให้ทัดเทียมกับนานาอารยะประเทศ ในส่วนนี้จึงจะได้อธิบายถึงนิยามความหมายพัฒนาการ การจำแนกประเภท เพื่อเป็นฐานสำคัญในการวิเคราะห์ต่อไป

2.2.1 ความหมายและวิวัฒนาการทางความคิดเกี่ยวข้อมูลส่วนบุคคล

2.2.1.1 ความหมาย ขอบเขตและลักษณะของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล

“สิทธิในความเป็นส่วนตัว (Privacy)” เป็นคำที่ปรากฏอยู่ในนิยามหนึ่งของสิทธิส่วนบุคคล (Personal Right) เป็นการย้ำให้เห็นถึงความสำคัญที่มนุษย์ทุกคนต้องปฏิบัติต่อความเป็นส่วนตัวของบุคคลในฐานะที่เป็นสาระสำคัญของสิทธิในความเป็นตัวตนของมนุษย์ ในสมัยโบราณความเข้าใจเบื้องต้นเกี่ยวกับ “ความเป็นส่วนตัว” คือ การที่ไม่ร่วมอยู่กับคนอื่น หรือการปลีกตัวออกจากสังคม ดังเช่นในสมัยโรมันแนวความคิดเกี่ยวกับเรื่องส่วนตัว ยอมรับว่าบุคคลแต่ละคนมีเขตแดนของตัวเอง ในเขตแดนดังกล่าวเสมือนเป็นที่พำนักพักพิงไม่เกี่ยวข้องกับกิจกรรมทางสังคมในช่วงเวลาใดเวลาหนึ่ง ภายในดินแดนส่วนตัวนี้เป็นดินแดนเฉพาะตัวของแต่ละบุคคลเท่านั้น และเป็นที่ปราศจากการเข้ามาเกี่ยวข้องของคนในสังคม[34]

มุมมองถึงความหมายของ “สิทธิในความเป็นส่วนตัว” มีในหลายมิติ เช่น มุมมองในทางปรัชญาซึ่งมีทัศนะที่หลากหลาย แต่คำอธิบายที่ได้รับการกล่าวถึงเสมอคือ คำสอนของอริสโตเติ้ล (Aristotle) ซึ่งได้อธิบายว่า ความเป็นส่วนตัว ได้แก่เรื่องที่เกี่ยวกับร่างกายและการดำเนินชีวิตของสมาชิกภายในครอบครัวโดยมีเจ้าบ้านคือผู้เป็นพ่อ หรือผู้ชายที่เป็นผู้อาวุโสที่เป็นเจ้าบ้าน และเป็นผู้ทรงสิทธิในความเป็นส่วนตัวนั้น ซึ่งสถานะของความเป็นส่วนตัวหากมองในแง่ปรัชญา “ความเป็นส่วนตัว” เป็นภาวะพื้นฐานของบุคคลที่ไม่ต้องต่อสู้ ยื้อแย่งและไม่ต้องการข้อพิสูจน์ ความเป็นส่วนตัวเป็นสิทธิขั้นพื้นฐานโดยธรรมชาติของความเป็นมนุษย์ซึ่งแฝงอยู่ในตัวบุคคลนั้น ๆ มาตั้งแต่เกิด[35] หรือมุมมองในทางศาสนาตามที่ปรากฏในคัมภีร์ใบเบิ้ล ในบทคำสอนเกี่ยวกับศีลธรรมของมนุษย์ “ความเป็นส่วนตัว” เกิดจากคำสอนเรื่องการกำเนิดของมนุษย์ อดัมและอีฟ ได้ขโมยกินผลไม้

---

[34] Ellen Alderman and Caroline Kennedy, **The Right to Privacy** (New York: Alfred A. Knopf, 1995), p. xiv อ้างถึงใน นคร เสรีรักษ์, **ความเป็นส่วนตัว: ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย** (กรุงเทพมหานคร: พี. เพรส, 2557), หน้า 62.

[35] นคร เสรีรักษ์, **ความเป็นส่วนตัว: ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย** (กรุงเทพมหานคร: พี. เพรส, 2557), หน้า 62-63.

ต้องห้ามในสวนของพระเจ้า ทำให้ทั้งสองได้สำนึกถึงความอับอายที่ต่างต้องอยู่ในร่างกายที่เปลือยเปล่าโดยปราศจากสิ่งปกปิดร่างกาย จึงได้นำใบไม้มาประดิษฐ์เป็นที่ปิดบังส่วนของร่างกายที่ไม่ต้องการให้คนอื่นเห็น ความเป็นส่วนตัวของบุคคลในคำสอนทางศาสนาจึงได้แก่ สิ่งต่าง ๆ ที่เกี่ยวกับเนื้อตัวร่างกายของบุคคล สิ่งใดหรือเรื่องใดก็ตามที่เกี่ยวกับตัวของบุคคล ถือว่าเป็นเรื่อง "ส่วนตัว" ทั้งสิ้น[36]

แต่สำหรับในมุมมองทางทฤษฎีกฎหมายแล้ว แนวคิดเรื่องสิทธิในความเป็นส่วนตัวถือเป็นสิ่งซึ่งจะได้รับการรับรองและคุ้มครองโดยกฎหมาย ไม่ว่าจะเป็นโดยกฎเกณฑ์ในระบบกฎหมายระหว่างประเทศด้านสิทธิมนุษยชนทั้งหลาย หรือระบบกฎหมายภายในของรัฐ ซึ่งเมื่อพิจารณาความหมายจากการบัญญัติรับรอง “สิทธิในความเป็นส่วนตัว” จะเห็นนิยามตามกฎเกณฑ์ระหว่างประเทศปรากฏดังนี้[37]

1. ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (UDHR) มีการบัญญัติรับรองและคุ้มครอง “สิทธิในความเป็นส่วนตัว” ของบุคคลไว้ในข้อ 12 ความว่า “บุคคลใดจะถูกแทรกแซงตามอำเภอใจในความเป็นส่วนตัว ครอบครัว ที่อยู่อาศัย หรือการสื่อสาร หรือจะถูกลบหลู่เกียรติยศหรือชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองของกฎหมายต่อการลบหลู่เช่นนั้น”

2. กติการะหว่างประเทศว่าด้วยพลเมืองและสิทธิทางการเมือง (ICCPR) ข้อกำหนดเกี่ยวกับการรับรองและคุ้มครอง “สิทธิในความเป็นส่วนตัวของบุคคล” ไว้ใน ข้อ 17 “1. บุคคลใดจะถูกแทรกแซงตามอำเภอใจหรือโดยมิชอบด้วยกฎหมายในความเป็นอยู่ส่วนตัว ครอบครัว ที่อยู่อาศัย หรือการสื่อสาร หรือจะถูกลบหลู่เกียรติยศหรือชื่อเสียงมิได้ และ 2. ทุกคนมีสิทธิที่จะได้รับความคุ้มครองของกฎหมายต่อการแทรกแซงหรือการลบหลู่ดังกล่าวนั้น”

3. อนุสัญญาแห่งยุโรปว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขึ้นพื้นฐาน (EU Convention) รับรอง “สิทธิที่จะได้รับการเคารพในชีวิตส่วนตัวและชีวิตครอบครัว” (Right to Respect for Private and Family Life) ไว้ในข้อ 8

> 1. ทุกคนมีสิทธิที่จะได้รับความเคารพต่อชีวิตส่วนตัวและชีวิตครอบครัว ที่อยู่อาศัย และการสื่อสาร 2. จะต้องไม่มีการแทรกแซงโดยเจ้าหน้าที่ของรัฐในการใช้สิทธิดังกล่าว เว้นแต่ในกรณีเป็นไปตามกฎหมายและความจำเป็นในสังคมประชาธิปไตยเพื่อประโยชน์เกี่ยวกับความมั่นคงแห่งรัฐ ความปลอดภัยสาธารณะ หรือความมั่งคั่งทางเศรษฐกิจของประเทศ เพื่อป้องกันความไม่สงบเรียบร้อยหรือ

---

[36] *เรื่องเดียวกัน*, หน้า 63.

[37] นนทวัชร์ นวตระกูลพิสุทธิ์, *เรื่องเดิม,* หน้า 736-739.

การกระทำความผิดในทางอาญา เพื่อคุ้มครองสุขภาพหรือศีลธรรม หรือเพื่อคุ้มครองสิทธิและเสรีภาพของบุคคลอื่น

อนุสัญญาฯ นี้ ยังได้รับรองและคุ้มครองสิทธิที่จะได้รับการเยียวยาที่แท้จริง (Right to an Effective Remedy) อีกด้วย โดยกำหนดไว้ในข้อ 13 ความว่า “ทุกคนซึ่งสิทธิและเสรีภาพตามที่กำหนดไว้ในอนุสัญญานี้ถูกละเมิด จะต้องได้รับการเยียวยาที่แท้จริงโดยองค์กรของรัฐ แม้ว่าการล่วงละเมิดนั้นจะได้กระทำโดยบุคคลในการปฏิบัติหน้าที่ของตน”

นอกจากนี้ยังมี กฎบัตรสิทธิขั้นพื้นฐานของสหภาพยุโรป (Charter of Fundamental Rights of the European Union) เป็นกฎหมายที่เกี่ยวข้องกับสิทธิทางการเมือง เศรษฐกิจและสังคมของ ประชาชนชาวยุโรป ประกอบไปด้วยทั้งสิ้น 54 ข้อ 7 หมวดใหญ่สำหรับหลักการที่เกี่ยวกับสิทธิในความ เป็นอยู่ส่วนตัวและข้อมูลส่วนบุคคลปรากฏในหมวดที่ 2 ซึ่งครอบคลุมเรื่องเสรีภาพ (Freedom) ความเป็น ส่วนตัว (Article 7) การคุ้มครองข้อมูลส่วนบุคคล (Article 8) ฯลฯ โดยมีหลักการที่สำคัญดังนี้[38]

มาตรา 7 ว่าด้วยชีวิตส่วนบุคคลและครอบครัว วางหลักว่า “บุคคลทุกคนมีสิทธิได้รับการเคารพในชีวิตส่วนบุคคลและครอบครัว ที่อยู่อาศัย และการสื่อสาร”

มาตรา 8 ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล วางหลักว่า “บุคคลทุกคนมีสิทธิที่จะได้รับการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวกับตน ข้อมูลดังกล่าวจะต้องถูกประมวลอย่างเป็นธรรมเพื่อวัตถุประสงค์ที่ระบุไว้และบนพื้นฐานของความยินยอมของบุคคลนั้นหรือด้วยเหตุผลอันชอบด้วยกฎหมายอื่นที่ กฎหมายบัญญัติ บุคคลทุกคนมีสิทธิในการเข้าถึงและแก้ไขข้อมูลเกี่ยวกับตนที่ถูกเก็บรวบรวม การปฏิบัติให้ สอดคล้องกับกฎเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลจะต้องอยู่ภายใต้การควบคุมขององค์กรอิสระ”

จากหลักการดังกล่าวข้างต้น ถือเป็นมาตรฐานขั้นต่ำ กล่าวคือ ประเทศสมาชิกของสหภาพยุโรปอาจกำหนดหลักการคุ้มครองที่สูงกว่าได้ (More Extensive Provision) จะเห็นได้ว่าหลักกฎหมายสิทธิมนุษยชนนอกจากวางหลักทั่วไปในการ คุ้มครองข้อมูลส่วนบุคคลแล้ว ยังกำหนดหลักสำคัญไว้ เช่น หลักความชอบด้วยกฎหมายของการประมวลผลข้อมูล หลักความยินยอม หลักสิทธิของเจ้าของข้อมูล เป็นต้น หลักการเหล่านี้ได้มีการนำไปกำหนดในกฎหมายคุ้มครองข้อมูลส่วนบุคคลของยุโรปฉบับต่าง ๆ นอกจากนี้ ในการปรับใช้และการตีความกฎหมายคุ้มครอง ข้อมูลส่วน

---

[38] คณาธิป ทองวีรวงศ์, **รายงานการวิจัยฉบับสมบูรณ์ เรื่องการปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน** (รายงานการวิจัย เสนอต่อสำนักงานเลขาธิการสภาผู้แทนราษฎร, 2559), หน้า 50-51.

บุคคลของสหภาพยุโรปนั้น ศาลมิได้พิจารณาเฉพาะกฎหมายคุ้มครองข้อมูลส่วนบุคคล แต่จะพิจารณาในบริบทของกฎหมายสิทธิมนุษยชน โดยนำหลักการสิทธิมนุษยชนมาประกอบการวินิจฉัยประเด็น การคุ้มครองข้อมูลด้วย[39]

4. อนุสัญญาแห่งอเมริกาว่าด้วย สิทธิมนุษยชน (USA Convention) ก็ได้รับรองไว้ในข้อ 11 ความว่า

> 1. ทุกคนมีสิทธิที่จะได้รับการเคารพซึ่งเกียรติและยอมรับศักดิ์ศรีของตน 2. บุคคลใดจะเป็นวัตถุแห่งการแทรกแซงตามอำเภอใจหรือโดยมิชอบในชีวิตส่วนตัว ครอบครัว ที่อยู่อาศัย และการสื่อสาร หรือการลบหลู่เกียรติยศหรือชื่อเสียงโดยมิชอบด้วยกฎหมายมิได้ 3. ทุกคนมีสิทธิที่จะได้รับความคุ้มครองของกฎหมายต่อการลบหลู่เช่นนั้น

จากหลักเกณฑ์ต่าง ๆ ที่กล่าวมาสามารถสรุปความหมายของ “สิทธิในความเป็นส่วนตัว” หมายถึงสิทธิและเสรีภาพส่วนตัวของมนุษย์ทุกคนที่จะสามารถกำหนด “การดำรงตน” หรือ “การดำเนินวิถีชีวิตของตน” ตามความพึงพอใจหรือความปรารถนาแห่งตนเองได้ โดยไม่ถูกแทรกแซงหรือรบกวนจากบุคคลอื่น

อย่างไรก็ดี แม้สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลจะได้รับการยอมรับว่าเป็นสิทธิมนุษยชนประเภทหนึ่งแต่สิทธินี้ก็ไม่ใช่สิทธิเด็ดขาด ดังนั้นรัฐย่อมสามารถที่จะออกข้อกำหนดมายกเว้นจำกัดสิทธินี้ได้ในมิติเพื่อประโยชน์สาธารณะ ตัวอย่างเช่นกรณีของ คดี Klass V. Germany ที่รัฐบาลประเทศเยอรมนีได้ตรากฎหมายเกี่ยวกับการรักษาความปลอดภัย หรือ The Act on Restrictions on the Secrecy of Mail, Post and Telecommunications (G 10 Act) โดยรัฐบาลได้อ้างถึงสิทธิในการรักษาความมั่นคงปลอดภัยและการป้องกันอาชญากรรมภายหลังจากประเทศประสบปัญหาภัยคุกคามจากผู้ก่อการร้าย โดยกฎหมายฉบับนี้ได้ให้อำนาจแก่เจ้าหน้าที่ในการที่จะสามารถล่วงละเมิดสิทธิในความเป็นส่วนตัวได้ ไม่ว่าจะเป็นการตรวจสอบจดหมาย ไปรษณียบัตร หรือโทรศัพท์ ฯลฯ เป็นต้น เพื่อที่จะตรวจสอบผู้ต้องสงสัย ทำให้มีการฟ้องคดีต่อศาลแห่งสหภาพยุโรปว่า เป็นการกระทำที่ละเมิดต่อมาตรา 8 ของกฎบัตรสิทธิขั้นพื้นฐานของสหภาพยุโรป (Charter of Fundamental Rights of the European Union) ที่ได้กล่าวไว้แล้วตอนต้น แต่ในที่สุด ศาลแห่งสหภาพยุโรปก็ได้มีคำวินิจฉัยว่าเจ้าพนักงานมีอำนาจใจการตรวจสอบการติดต่อสื่อสารเช่นนี้ได้ เพราะ

---

[39] *เรื่องเดียวกัน*.

เป็นมาตรการที่จำเป็นเพื่อรักษาความสงบเรียบร้อยและความปลอดภัยของประเทศ[40] ดังนั้นจะเห็นได้ว่าขอบเขตของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในประการสำคัญนั้นก็คือ ประโยชน์สาธารณะที่เกี่ยวกับความมั่นคงของรัฐนั่นเอง

โดยสิทธิในความเป็นส่วนตัว อันเป็นสิทธิและเสรีภาพส่วนตัวของมนุษย์ทุกคนที่จะสามารถกำหนด “การดำรงตน” หรือ “การดำเนินวิถีชีวิตของตน” ตามความพึงพอใจหรือความปรารถนาแห่งตนเองได้ โดยไม่ถูกแทรกแซงหรือรบกวนจากบุคคลอื่น ตามที่ได้กล่าวมาข้างต้นนี้ หากพิจารณาในแง่ความเป็นส่วนตัวในประเด็นเรื่อง ความเป็นเจ้าของเรื่องราวส่วนตัว หรือข้อมูลส่วนบุคคลแล้ว จะเห็นว่า มนุษย์ทุกคนก็ย่อมมีสิทธิเสรีภาพเหนือเรื่องราวส่วนหรือข้อมูลเกี่ยวกับตน ที่จะดำเนินการอย่างไรกับข้อมูลนี้ก็ย่อมได้ ดังนั้น สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลจึงเป็นส่วนที่อธิบายลึกลงไปในประเด็นนี้ ซึ่งความหมายของคำว่า ข้อมูลส่วนบุคคลในทางวิชาการแล้วจะประกอบด้วย 2 องค์ประกอบหลักได้แก่ องค์ประกอบด้านเนื้อหา และองค์ประกอบด้านรูปแบบ โดยมีลักษณะดังนี้คือ[41]

ประการแรก องค์ประกอบด้านเนื้อหา จะประกอบด้วยข้อมูล 3 ลักษณะ ดังนี้

1. ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล ตัวอย่างเช่น ชื่อ ที่อยู่ เพศ อาชีพ

2. ข้อมูลที่บ่งให้รู้ตัวบุคคล เช่น รหัสหรือเลขประจำตัวประชาชน ลักษณะทางกายภาพ เช่น ลายพิมพ์นิ้วมือ หรือรหัส DNA หรือสิ่งที่บ่งชี้อย่างอื่น เช่น จดหมายอิเลคทรอนิคส์ (e-Mail Address), หมายเลขโทรศัพท์ส่วนตัว

3. ข้อมูลที่เป็นความลับของบุคคล เช่น เชื้อชาติ ประวัติทางวินัย ประวัติทางการแพทย์หรือสุขอนามัย ประวัติทางอาชญากรรม ข้อมูลทางการเงินหรือหนี้สิน ข้อมูลเชิงทัศนคติของบุคคล เช่น ความเชื่อทางการเมือง การปกครอง การนับถือศาสนา รสนิยมในเรื่องต่าง ๆ

ประการที่สอง องค์ประกอบด้านรูปแบบ จะประกอบด้วยองค์ประกอบ 2 ประการดังนี้

1. ข้อมูลจะเป็นข้อมูลส่วนบุคคล จะต้องมีการจัดเก็บหรือประมวลขึ้นมาอย่างเป็นระบบโดยบุคคลหรือนิติบุคคล และสามารถสื่อเรื่องราวความหมายอย่างใดอย่างหนึ่งได้ ซึ่งตามหลักกฎหมายแต่เดิมถือว่า ผู้ทำหน้าที่จัดเก็บเป็นเจ้าของกรรมสิทธิ์ แต่หลังจากวิวัฒนาการถึงปัจจุบัน ถือ

---

[40] Russell A. Miller, **Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair** (New York: Cambridge University Press, 2017), p. 156.

[41] จันทจิรา เอี่ยมมยุรา, “การคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย,” **วารสารนิติศาสตร์** 34, 4 (ธันวาคม 2547): 636-638.

ว่าองค์กรผู้เก็บรวมรวมมิใช่ผู้เป็นเจ้าของ แต่กลับจะต้องเป็นผู้มีหน้าที่และถูกควบคุมตามกฎหมาย เพื่อมิให้ละเมิดสิทธิของเจ้าของข้อมูลส่วนบุคคลที่แท้จริง

2. ต้องมีวิธีการ ช่องทางหรือสื่อหรือสิ่งที่สื่อความหมายให้รู้เรื่องราวข้อมูลส่วนบุคคล ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งของนั้นเอง หรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้ทำไว้ในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้สื่อความหมายปรากฏออกมาได้

โดยหากไม่ครบองค์ประกอบทั้งสองประการข้างต้น ข้อมูลเช่นนี้จะไม่ถือว่าเป็นข้อมูลส่วนบุคคล อันถือว่าเป็นวัตถุแห่งสิทธิที่จะได้รับการรับรองและคุ้มครองตามกฎหมาย[42]

นอกจากนี้หากพิจารณาถึงลักษณะของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ก็พอจะแบ่งลักษณะของสิทธินี้ได้เป็น 2 รูปแบบ กล่าวคือ สิทธิในความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลที่มีลักษณะเป็นข้อมูลส่วนบุคคลทั่วไป และข้อมูลส่วนบุคคลที่มีความอ่อนไหว โดยลักษณะของข้อมูลทั้งสองประเภทดังนี้[43]

ประเภทแรก ข้อมูลส่วนบุคคลทั่วไป (Non-Sensitive Data) มีลักษณะเป็นข้อมูลใด ๆ ที่เกี่ยวข้องกับบุคคลอันสามารถบ่งชี้เฉพาะตัวบุคคล อันได้แก่ ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ ที่อยู่ทางอิเล็กทรอนิกส์ อายุ วุฒิการศึกษา อาชีพ ตำแหน่งหน้าทีการงาน สถานะและลักษณะทางกายภาพ หรือข้อมูลอื่นใดที่สามารถนำมาประมวลกันเป็นลักษณะบ่งชี้ตัวบุคคลได้ ซึ่งโดยสภาพของข้อมูลประเภทนี้สามารถจะเปิดเผยต่อสาธารณะได้เพราะเป็นเรื่องปกติและไม่กระทบต่อสิทธิในความเป็นส่วนตัวของเจ้าของข้อมูลมากจนเกินสมควร ในลักษณะที่จะทำให้เกิดการล่วงละเมิดสิทธิหรือมีการเลือกปฏิบัติต่อเจ้าของข้อมูล

ประการที่สอง ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) มีลักษณะเป็นข้อมูลส่วนบุคคลที่เป็นเรื่องเฉพาะ (Intimate) ของบุคคลโดยเฉพาะ เป็นข้อมูลซึ่งเป็นความลับหรือเจ้าของข้อมูลไม่พึงประสงค์จะให้มีการเปิดเผย ข้อมูลประเภทนี้ได้แก่ การนับถือศาสนา ปรัชญาการใช้ชีวิต ทัศนะคติหรือลัทธิทางการเมือง รสนิยมทางเพศ ข้อมูลสุขภาพ ข้อมูลเกี่ยวกับการดำเนินคดีอาญาหรือประวัติอาชญากรรม

---

[42] *เรื่องเดียวกัน*, หน้า 638.

[43] ศิริกุล ภู่พันธ์, **ข้อความคิดว่าด้วยข้อมูลข่าวสารส่วนบุคคล** (วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2548), หน้า 83.

โดยสำหรับข้อมูลส่วนบุคคลที่มีความอ่อนไหวนี้ Reymond Wacks ได้แบ่งระดับไว้ 3 ระดับในหนังสือเรื่อง Personal Information: Privacy and The Law โดยพิจารณาจากผลกระทบต่อเจ้าของข้อมูลหากมีการเปิดเผยหรือล่วงรู้ข้อมูลนั้น ดังนี้[44]

1. ข้อมูลส่วนบุคคลที่มีความอ่อนไหวระดับสูง (High Sensitivety) ซึ่งได้แก่ ข้อมูลส่วนบุคคลเกี่ยวกับประวัติทางการแพทย์ ผลการตรวจเลือด ผลการตรวจสุขภาพ ผลการทดสอบทางจิตวิทยา พฤติกรรมและรสนิยมทางเพศ ข้อมูลเกี่ยวกับการดำเนินคดีอาญาหรือประวัติอาชญากรรม หรือข้อเท็จจริงในชีวิตประจำวันที่เป็นเรื่องลับเฉพาะ เป็นต้น

2. ข้อมูลที่มีความอ่อนไหวระดับปานกลาง (Moderate Sensitivity) ข้อมูลประเภทนี้มีความเสี่ยงในแง่ที่อาจทำให้บุคคลอื่นนำไปใช้ประโยชน์ในทางที่ผิด เช่น ข้อมูลเกี่ยวกับรายได้ ทรัพย์สิน หนี้สิน เชื้อชาติ ข้อพิพาทระหว่างสามีภริยา ประวัติการหย่าร้าง พินัยกรรม การชำระภาษี กรมธรรม์ประกันชีวิต ประวัติการใช้ยา ข้อมูลเกี่ยวกับความคิดเห็นของบุคคล ข้อมูลเกี่ยวกับพฤติกรรมส่วนตัว เป็นต้น

3. ข้อมูลที่มีความอ่อนไหวระดับต่ำ (Low Sensitivity) ข้อมูลประเภทนี้เป็นข้อมูลที่เกี่ยวข้องกับบุคคลที่สามารถทำให้ได้มาซึ่งข้อมูลที่มีความอ่อนไหวสูง เช่น สถานะภาพการแต่งงาน ประวัติการทำงาน การถือหุ้น การถือครองที่ดิน สวัสดิการ การใช้อุปกรณ์ทางการแพทย์ เป็นต้น

แต่อย่างไรก็ดี การกำหนดประเภทของข้อมูลส่วนบุคคลว่าจะเป็นข้อมูลส่วนบุคคลทั่วไป หรือเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวนั้น ขึ้นอยู่กับกฎหมายของแต่ละประเทศว่าจะกำหนดอย่างไรโดยอาจจะแตกต่างกันไปตามบริบททางสังคมของประเทศนั้น ๆ

2.2.1.2 วิวัฒนาการทางความคิดของสิทธิในความความเป็นส่วนตัว

นับแต่โบราณพวกกรีกมองว่า ชีวิตที่เป็นส่วนตัว “ด้วยตัวเอง” (Idiom) เป็นชีวิต “แบบคนบ้า” (Idiotic) ในทำนองเดียวกันกับพวกโรมันก็มองว่าความเป็นส่วนตัวนั้นเป็นการลี้ภัยชั่วคราวจากชีวิตสาธารณะ (res publica) ดังที่ Hannah Arendt บรรยายไว้ว่า “ในยุคโบราณลักษณะของความเป็นส่วนตัว (The Private of Privacy) ซึ่งมีความหมายตามตัวอักษร ถือเป็นลักษณะที่มีความสำคัญยิ่ง มันมีความหมายตรงตัวถึงสถานะของการแยกขาด (Deprived) จากอะไรบางอย่างชั่วคราว และการแยกขาดนั้นก็เป็นคุณลักษณะระดับสูงที่มนุษย์พึงมี คนที่มีแต่ชีวิตส่วนตัวนั้นไม่ใช่มนุษย์ที่สมบูรณ์ ดังเช่นที่พวกทาสไม่ได้รับอนุญาตให้เข้าร่วมชีวิตสาธารณะ และพวกคนเถื่อน

---

[44] Raymond Wacks, **Personal Information: Privacy and The Law** (London: Oxford, 1993), pp. 229-238 อ้างถึงใน สุวรรณ ปริญญา, **ปัญหาทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบคุคลบนธุรกรรมทางอิเล็กทรอนิกส์** (สารนิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยกรุงเทพ, 2550), หน้า 17-18.

(Barbarian) ซึ่งเลือกที่จะไม่สถาปนาชีวิตสาธารณะ”จนกระทั่งถึงยุคโรมันตอนปลาย เราจึงเริ่มเห็นการยอมรับว่าความเป็นส่วนตัวมีลักษณะเป็นอาณาบริเวณพื้นที่ส่วนตัว[45]

แนวความคิดที่ยอมรับสิทธิส่วนตัวของบุคคลนั้นเป็นแนวคิดแบบปัจเจกนิยม (Individualism) ที่มีรากฐานทางความคิดมาจากพวกสโตอิค (Stoic) ที่เชื่อว่ามนุษย์ในสภาวะธรรมชาติสมบูรณ์นั้น จะดำรงชีวิตอย่างมี “เหตุผล” และเหตุผลนี้เป็นระบบสากลซึ่งเป็นพื้นฐานของกฎเกณฑ์ที่ธรรมชาติคอยควบคุมอยู่ มนุษย์ก็อยู่ภายใต้กฎเกณฑ์ของจักรวาลนี้[46] เพราะเหตุผลที่แวดล้อมตัวมนุษย์อยู่เป็นกฎเกณฑ์ของจักรวาล ปัจเจกชนที่เกิดมาแล้วจึงมีสิทธิตามธรรมชาติ (Natural Rights) ในฐานะที่เกิดมาเป็นมนุษย์ เป็นสิทธิเฉพาะตัวไม่อาจจำหน่าย จ่ายโอน ยกเลิก เพิกถอน ไม่ว่ากรณีใด ๆ ซึ่งสิทธิตามธรรมชาตินี้เป็นแนวความคิดว่าด้วยสิทธิส่วนตัวของเอกชน ว่าเกิดขึ้นพร้อมกับสภาพบุคคล และหากมีการก้าวล่วงซึ่งสิทธิส่วนตัวย่อมเป็นการหมิ่นศักดิ์ศรีในความเป็นมนุษย์ของผู้นั้น และสิทธิส่วนตัวของบุคคลนี้มักจะถูกใช้กล่าวอ้างเพื่อเป็นข้อเรียกร้องต่อผู้มีอำนาจในการปกครอง ซึ่งนักปรัชญาที่มีแนวคิดสนับสนุนความคิดของพวกสโตอิค (Stoic) ได้แก่[47]

พลาโต (Plato, 429-348 BC) พลาโตเห็นว่า มนุษย์ประกอบด้วยส่วนที่เป็นรูปธรรม (Empirie) คือ ร่างกาย และยังมีอีกส่วนที่เป็นนามธรรม (Idea) คือ วิญญาณหรือจิตของมนุษย์ ซึ่งกฎหมายที่บัญญัติขึ้น (Positive Law) เพื่อกำหนดสิทธิและหน้าที่นั้นมีลักษณะหยาบเกินกว่าที่จะนำมาบังคับใช้กับมนุษย์ที่มีความซับซ้อน จึงมีเพียงกฎหมายธรรมชาติที่มีลักษณะเป็นศีลธรรมมนุษย์จะสำนึกรู้ได้เอง ซึ่งสนับสนุนแนวคิดในเรื่อง "สิทธิส่วนตัว" ที่ว่า มนุษย์มีสำนึกที่จะรู้ว่าตน “มีสิทธิ” ในส่วนของตนแค่ไหนเพียงไร อันเป็นธรรมชาติของความเป็นมนุษย์นั่นเอง

อริสโตเติล (Aristotle, 384-322 BC) อริสโตเติลเป็นศิษย์ของพลาโต อริสโตเติลเห็นด้วยกับความคิดของอาจารย์ แต่เห็นเพิ่มเติมอีกว่านอกจากจะมีนิติรัฐแล้ว ยังต้องมีกฎหมายเป็นเครื่องกำหนดความยุติธรรมที่มีโดยธรรมชาตินั้น เหตุผลของมนุษย์เป็นส่วนหนึ่งของธรรมชาติที่เป็นกฎหมาย ซึ่งธรรมชาติได้ให้ความสามารถในการใช้เหตุผลมาแก่มนุษย์อันแตกต่างจากสัตว์โลกชนิดอื่น ๆ เหตุผลในการที่มนุษย์ระลึกรู้ว่าตนมีขอบเขตในการกระทำเพียงไรในเรื่องหนึ่ง ๆ เป็นสิทธิตามธรรมชาติ ซึ่งสิทธิส่วนตัวของบุคคลหนึ่ง ๆ ที่จะไม่ถูกก้าวล่วงเป็นเรื่องที่มนุษย์รู้ได้ด้วยตนเองจากความมีเหตุผลที่เป็นคุณสมบัติพิเศษในความเป็นมนุษย์นั่นเอง

---

[45] เรย์มอนด์ แวคส์, **ความเป็นส่วนตัว: ความรู้ฉบับพกพา,** แปลโดย อธิป จิตตฤกษ์ และปวรรัตน์ ผลาสิทธุ์ (กรุงเทพมหานคร: โอเพ่นเวิลด์ส, 2556), หน้า 74-75.

[46] ปรีดี เกษมทรัพย์, **นิติปรัชญา** (กรุงเทพมหานคร: มิตรนราการพิมพ์, 2531), หน้า 118-116.

[47] ชื่นอารีย์ มาลีศรีประเสริฐ, **การคุ้มครองสิทธิส่วนตัวกับการสื่อสารสนเทศ** (วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2539), หน้า 16-20.

ซิเซโร (Cicero, 106-43 BC) ซิเซโรได้กล่าวถึงกฎหมายธรรมชาติ ที่รองรับสิทธิธรรมชาติซึ่งหมายรวมถึง “สิทธิส่วนตัว” ไว้อย่างชัดเจนและรัดกุม ดังคำอธิบายที่ว่า

> กฎหมายที่แท้จริง คือ เหตุผลที่ถูกต้อง สอดคล้องกับธรรมชาติ แผ่ซ่านไปในทุกสิ่งทุกอย่าง สม่ำเสมอเป็นนิรันดร ก่อให้เกิดหน้าที่ที่จะต้องทำโดยคำสั่งหรือห้ามไม่ให้กระทำความชั่วโดยข้อห้าม เป็นหน้าที่อันศักดิ์สิทธิ์ที่จะต้องไม่บัญญัติกฎหมายให้ขัดแย้งกับกฎหมายนี้ เราไม่อาจยกเลิกหรือทำให้กฎหมายนี้เสื่อมลงได้ อันที่จริงแล้วไม่ว่าวุฒิสภาหรือมวลชน ก็ไม่มีอำนาจปลดปล่อยเราให้พ้นจากกฎหมายนี้ และเราไม่จำต้องพึ่งบุคคลหรือสิ่งอื่นใด นอกจากตัวเราเอง ที่จะแสดงออกว่ากฎหมายนั้นเป็นอย่างไร หรือตีความว่ากฎหมายนั้นมีความหมายว่าอย่างไร กฎหมายนี้ไม่เป็นอย่างหนึ่งที่กรุงโรมและเป็นอีกอย่างหนึ่งที่กรุงเอเธนส์ เป็นอย่างหนึ่งในสมัยนี้แต่เป็นอีกอย่างหนึ่งในสมัยต่อมา แต่จะยังคงเป็นกฎหมายอันหนึ่งอันเดียวไม่เปลี่ยนแปลงโดยอนันตกาล และผูกพันบังคับทุกชาติ ทุกภาษา ทุกยุค ทุกสมัย

โดยความหมายของคำว่ากฎหมายจากคำกล่าวของซิเซโรคือ กฎหมายที่แท้จริงคือเหตุผลที่ถูกต้อง คำว่า “เหตุผล” ตามความหมายทางปรัชญา หมายถึงระบบที่เป็นระเบียบ ที่มีอยู่เป็นอันหนึ่งอันเดียวกันกับระบบของจักรวาล จะเรียกว่าเป็นเหตุผลสากลก็ได้ ส่วนเหตุผลที่มีอยู่ในจิตใจของมนุษย์ที่ทำให้มนุษย์รู้ผิดชอบชั่วดีก็เป็นส่วนหนึ่งของเหตุผลสากล เมื่อเหตุผลเติบโตเต็มที่หรือและสมบูรณ์ครบถ้วนแล้วก็คือสิ่งที่เรียกกันว่า "ปัญญา" ซึ่งจะทำให้เหตุผลเป็นสามัญเป็นสากลและเป็นเหตุผลอันถูกต้อง

อย่างไรก็ดีในสังคมโบราณและสังคมบุพกาลก็ยังมีทัศนคติต่อความเป็นส่วนตัวแตกต่างกันไปตามสภาพของสังคมและจารีตประเพณี โดย Barrington Moore ผู้แต่งหนังสือ Privacy Rights: Moral and Legal Foundations ได้พิจารณาสถานะของความเป็นส่วนตัวในชุมชนมนุษย์ยุคโบราณโดยเปรียบเทียบจากหลายแห่ง เช่น เอเธนส์ยุคคลาสสิค สังคมชาวยิวที่ปรากฏในคัมภีร์พันธสัญญาเดิม และจีนในยุคโบราณ ในกรณีของจีน เขาได้แสดงให้เห็นว่าแนวทางการแบ่งแยกระหว่างรัฐ (สาธารณะ) และครอบครัว (ส่วนตัว) ตามขนบขงจื๊อ รวมถึงตัวบทโบราณเกี่ยวกับการเกี้ยวพาราสี ครอบครัว และมิตรภาพได้ทำให้แนวคิดเรื่องสิทธิในความเป็นส่วนตัวของสังคมจีนไม่เข้มแข็งมากนัก แต่ในอีกด้านหนึ่ง สังคมเอเธนส์ในศตวรรษที่ 4 ก่อนคริสตกาล สิทธิความเป็นส่วนตัว

ได้รับการคุ้มครองมากกว่า ข้อสรุปของเขาก็คือ สิทธิในความเป็นส่วนตัวในด้านการสื่อสารจะเกิดขึ้นได้เฉพาะในสังคมสลับซับซ้อนที่จารีตแบบเสรีนิยมมีความเข้มแข็ง[48]

อย่างไรก็ดี แนวความคิดเรื่องสิทธิในความเป็นส่วนตัว ซึ่งเป็นส่วนหนึ่งก็แนวความคิดในการเคารพต่อสิทธิเสรีภาพ และศักดิ์ศรีความเป็นมนุษย์ก็ได้ถูกจำกัดและลบเลือนไปในบางยุคสมัย เช่น ในยุคสมัยกลางตอนต้น ที่เรียกว่าเป็นยุคมืด อันเป็นยุคที่บ้านเมืองเต็มไปด้วยความสับสนวุ่นวายและมีการรบพุ่งเพื่อแย่งชิงอำนาจและทรัพย์สมบัติทั่วยุโรป การแตกแยกเป็นแคว้นเล็กแคว้นน้อยทำให้สภาพสังคมไม่สงบสุข ประชาชนตกอยู่ภายใต้ภาวะที่ต้องต่อสู้ดิ้นรนทำมาหากินเพื่อให้มีชีวิตรอดเท่านั้น เรื่องสิทธิเสรีภาพหรือเรื่องศักดิ์ศรีความเป็นมนุษย์ (รวมถึงสิทธิในความเป็นส่วนตัว) ในยุคนี้แทบจะไม่ได้รับการคำนึงถึงเลย[49]

เมื่อเวลาผ่านไปจนถึงยุคต่อมา การเกิดขึ้นของรัฐชาติ ในศตวรรษที่ 16 และทฤษฎีอำนาจอธิปไตยในศตวรรษที่ 17 ทำให้เกิดมโนทัศน์เกี่ยวกับอาณาบริเวณสาธารณะที่ชัดเจน อีกด้านหนึ่งก็คือแนวคิดเรื่องอาณาบริเวณส่วนตัวหรือสิทธิในความเป็นส่วนตัวที่เป็นอิสระจากเงื้อมมือของรัฐก็เกิดขึ้นอันเป็นผลมาจากการกล่าวอ้างอำนาจอันไร้ขีดจำกัดของกษัตริย์และของสภาในเวลาต่อมา กล่าวอีกแง่หนึ่ง การปรากฏตัวของรัฐสมัยใหม่ การกำกับควบคุมกิจกรรมทางสังคมและเศรษฐกิจและการยอมรับการดำรงอยู่ของความเป็นส่วนตัว เป็นเงื่อนไขสำคัญของการแยกระหว่างความเป็นสาธารณะและความเป็นส่วนตัวออกจากกัน[50] ซึ่งนักปรัชญาที่มีอิทธิพลสำคัญต่อพัฒนาการทางความคิดในยุคนี้คือ

จอห์น ล็อค (John Locke, 1632-1704) อธิบายว่า รัฐบาลจะต้องให้ความคุ้มครองสิทธิในทรัพย์สินส่วนตัวของบุคคล ซึ่งเป็นสิ่งที่โอนให้ใครไม่ได้ และปกป้องสิทธิเสรีภาพของบุคคลให้พ้นจากอำนาจทางการเมือง นั่นคือรัฐบาลจะเข้าไปก้าวก่ายสิทธิเสรีภาพส่วนบุคคลเกินกว่าที่ประชาชนได้ยอมสละให้แล้วไม่ได้ ซึ่งสำหรับ “ความเป็นส่วนตัว” นั้น จอห์น ล็อค ได้อธิบายไว้ในหนังสือเรื่อง Second Treatise of Government ในปี 1960 ว่าหมายถึงสถานะของบุคคลที่มีเสรีภาพโดยสมบูรณ์ที่จะกำหนดการกระทำของตนเอง กำหนดการใช้ทรัพย์สินของตนเอง และกำหนดความสัมพันธ์กับบุคคลอื่น ตามที่เขาคิดว่าสมควรภายใต้ขอบเขตของกฎหมายธรรมชาติ[51]

---

[48] เรย์มอนด์ แวคส์, *เรื่องเดิม*, หน้า 75.

[49] ศิริกุล ภู่พันธ์, *เรื่องเดิม*, หน้า 15.

[50] เรย์มอนด์ แวคส์, *เรื่องเดิม*, หน้า 76.

[51] ศิริกุล ภู่พันธ์, *เรื่องเดิม*, หน้า 31.

จอห์น สจ๊วต มิลล์ (John Stuart Mill, 1806-1873) เขียนอธิบาย “หลักการของความอันตราย” (Harm Principle) ไว้ในหนังสือ On Liberty ว่า “มีเพียงเหตุผลเดียวที่มนุษยชาติไม่ว่าในฐานะปัจเจกหรือส่วนรวม จะได้รับอนุญาตให้แทรกแซงชีวิตของมนุษย์คนอื่น เหตุผลนั้นคือการป้องกันตัว มีเป้าหมายเดียวที่จะใช้อำนาจได้อย่างชอบธรรมเหนือเจตจำนงของสมาชิกคนใดก็ตามที่ได้อาศัยอยู่ในชุมชนอันศิวิไลซ์ นั่นคือ การป้องกันไม่ให้เกิดอันตรายกับสมาชิกคนอื่น ๆ ของชุมชน ลำพังแค่ผลประโยชน์ของสมาชิกคนใดคนหนึ่งในสังคม ไม่ว่าจะเป็นผลประโยชน์ทางกายภาพหรือศีลธรรม ไม่ใช่หลักการที่เพียงพอสำหรับการใช้อำนาจในแบบที่กล่าวมา”[52]

ต่อมาในช่วงศตวรรษที่ 18 ถึงต้นศตวรรษที่ 19 แนวความคิดเรื่องสิทธิในความเป็นส่วนตัวเป็นสิทธิขั้นพื้นฐานของมนุษย์ได้รับการพัฒนาอย่างต่อเนื่อง พัฒนาการดังกล่าวแสดงให้เห็นจากบทความจำนวนมาก สำหรับบทความที่โดดเด่นที่สุดดูเหมือนว่าบทความของ Samuel D. Warren และ Louis D. Brandeis ชื่อ “The Right to Privacy” เขียนขึ้นในปี 1890 ได้อธิบายความหมายของสิทธิในความเป็นส่วนตัว ว่าหมายถึง “สิทธิที่จะอยู่โดยลำพัง (Rights to be Let Alone)” และการคุ้มครองสิทธิตามกฎหมายนั้นไม่ควรจะจำกัดแค่เพียงในเรื่องของสิทธิในชีวิตร่างกาย และทรัพย์สินเท่านั้น ควรจะคุ้มครองไปถึงสิทธิที่จะใช้ชีวิตอย่างปกติสุข (Right to Enjoy Life) หรือสิทธิที่จะอยู่โดยลำพัง (Rights to be Let Alone) นั่นเอง[53]

การให้คำจำกัดความของสิทธิในความเป็นส่วนตัวว่าหมายถึงสิทธิที่จะอยู่โดยลำพังเช่นนี้เป็นการมองความเป็นส่วนตัวออกเป็นสองแง่มุม คือ ความเป็นส่วนตัวในแง่นามธรรม ได้แก่การที่บุคคลมีสิทธิและเสรีภาพในการแสดงอารมณ์ความรู้สึกนึกคิดตลอดจนความเชื่อในทางศาสนา ส่วนความเป็นส่วนตัวในทางรูปธรรมคือสิทธิที่จะอยู่โดยลำพังปราศจากการรบกวนและแทรกแซงจากสังคม การอยู่อย่างสันโดษไม่ติดต่อสัมพันธ์กับสังคม ซึ่งภายใต้แนวคิดนี้ ข้อมูลของบุคคลใดก็ตามที่สามารถเก็บรักษาความลับเกี่ยวกับตัวบุคคลย่อมมีสิทธิได้รับการคุ้มครองตามกฎหมายจากการละเมิดของบุคคลอื่น กล่าวคือ นอกจากจะคุ้มครองจากการกระทำของรัฐแล้ว บุคคลควรได้รับการคุ้มครองความเป็นส่วนตัวจากการกระทำของเอกชนด้วย ไม่ว่าจะเป็นเพื่อนบ้าน นายจ้าง หรือแม้แต่นักหนังสือพิมพ์ก็ตาม สิทธิในความเป็นส่วนตัวจึงเป็นสิทธิของคนใดคนหนึ่งในส่วนที่มีลักษณะเฉพาะตัวเพื่อป้องกันตัวเองออกจากสาธารณะ บุคคลมีสิทธิที่จะปฏิเสธข้อมูลอันเป็นความลับของตนต่อสาธารณะได้[54]

---

[52] เรย์มอนด์ แวคส์, *เรื่องเดิม*, หน้า 78.

[53] Samuel D. Warren and Louis D. Brandeis, *op. cit.*, pp. 193-220.

[54] วรรณรัชชา ทรัพย์รดาพัดชา, **ปัญหาการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลระหว่างประเทศกับสหภาพยุโรป: ศึกษาผลกระทบของคดีคำพิพากษาศาลยุติธรรมแห่งสหภาพ**

มาถึงยุคศตวรรษที่ 21 ประเด็นเรื่องสิทธิในความเป็นส่วนตัวยิ่งมีความสำคัญมากขึ้นด้วยเหตุที่เทคโนโลยีใหม่กำลังสร้างความท้าทายและอุปสรรค เมื่อบุคคลต่าง ๆ ต้องเผชิญกับอุปกรณ์เทคโนโลยีจำนวนนับไม่ถ้วนที่ล้วนมีโอกาสที่จะเป็นสาเหตุของการถูกเปิดเผยหรือล่วงละเมิดความเป็นส่วนตัวจากทั้งภาครัฐและเอกชน นานาอารยะประเทศก็ได้เร่งรีบปรับตัวโดยการตราเป็นกฎหมายขึ้นมาคุ้มครองสิทธินี้ ทั้งในระดับของกฎหมายระหว่างประเทศ รวมถึงกฎหมายภายในประเทศ ซึ่งรายละเอียดจะได้กล่าวถึงในบทต่อไป

2.2.1.3 ประเภทของสิทธิในความเป็นส่วนตัว

สิทธิความเป็นส่วนตัว สามารถจำแนกออกได้เป็น 4 ด้าน ดังนี้[55]

1) สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล (Information Privacy)

เป็นสิทธิเหนือข้อมูลส่วนบุคคล ไม่ว่าจะเป็นข้อมูลใด ๆ ที่เกี่ยวข้องกับบุคคลธรรมดาที่อาจโดยทางตรงหรือโดยอ้อมโดยระบุหมายเลขประจำตัวประชาชน (เช่นหมายเลขประกันสังคม) หรืออย่างน้อยหนึ่งองค์ประกอบที่เป็นเอกลักษณ์ของบุคคลนั้น (เช่น ชื่อและนามสกุล , วันเดือนปีเกิด, องค์ประกอบไบโอเมตริกซ์ ลายนิ้วมือ ดีเอ็นเอ ฯลฯ เป็นต้น ซึ่งจะได้รับความคุ้มครองโดยการวางหลักเกณฑ์เกี่ยวกับการเก็บรวบรวมและการบริหารจัดการข้อมูลส่วนบุคคล ทั้งนี้ การคุ้มครองความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลหรือข้อมูลส่วนตัวนั้น มีหลักการสากลที่เป็นกรอบในการคุ้มครองข้อมูลส่วนบุคคล (Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data) ขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD) ซึ่งรายละเอียดจะได้กล่าวในบทต่อไป

2) สิทธิในความเป็นส่วนตัวเกี่ยวกับเนื้อตัวร่างกาย (Bodily Privacy)

ความเป็นส่วนตัวในชีวิตร่างกาย (Bodily Privacy) เป็นการให้ความคุ้มครองในชีวิตร่างกายของบุคคลในทางกายภาพที่จะไม่ถูกดำเนินการใด ๆ อันละเมิดความเป็นส่วนตัว อาทิ การทดลองทางพันธุกรรม การทดลองยา เป็นต้น

ยุโรปในคดี C-362/14 ต่อโครงการเซฟส์ฮาร์เบอร์ (Safe Harbour) (วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2558), หน้า 8-9.

[55] บรรเจิด สิงคะเนติ, นนทวัชร์ นวตระกูลพิสุทธิ์ และเรวดี ขวัญทองยิ้ม, **รายงานการศึกษาวิจัยฉบับสมบูรณ์ เรื่อง ปัญหาและมาตรการทางกฎหมายในการรับรองและคุ้มครองสิทธิในความเป็นส่วนตัว** (รายงานการวิจัย เสนอต่อสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ, 2554), หน้า 6-7.

3) สิทธิในความเป็นส่วนตัวเกี่ยวกับการติดต่อสื่อสาร (Privacy of Communication)

เป็นการให้ความคุ้มครองในความปลอดภัย และความเป็นส่วนตัวในการติดต่อสื่อสารทางจดหมาย โทรศัพท์ ไปรษณีย์อิเล็กทรอนิกส์ หรือวิธีการติดต่อสื่อสารอื่นใดที่ผู้อื่นจะล่วงรู้มิได้

4) สิทธิในความเป็นส่วนตัวเกี่ยวกับการอยู่หรือพักอาศัย (Teritorial Privacy)

เป็นการกำหนดขอบเขตหรือข้อจำกัดที่บุคคลอื่นจะรุกล้ำเข้าไปในอาณาเขตแห่งสถานที่ส่วนตัวมิได้ ทั้งนี้ รวมทั้งการติดกล้องวงจรปิด และการตรวจสอบหมายเลขประจำตัวประชาชนของบุคคลเพื่อการเข้าที่พักอาศัย (ID Checks)

2.2.2 หลักการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล

Hilary Delany และ Eoin Carolan ได้สรุปว่าสิทธิในความเป็นส่วนตัวนี้เป็นสิทธิที่เป็นสากลและมีเหตุผลที่ความความเป็นส่วนตัวควรได้รับการคุ้มครองโดยสรุปจากงานเขียนของ John Craig โดยชี้ว่าเหตุผลนี้จะแสดงให้เห็นประโยชน์ต่อปัจเจกและต่อสังคม ซึ่งเหตุผลนี้มี 6 ประการได้แก่[56]

1. ความเป็นส่วนตัวให้โอกาสกับปัจเจกชนปลีกตัวจากแรงกดดันจากการจับตามองและบรรทัดฐานของสังคม
2. ความเป็นส่วนตัวให้เสรีภาพที่จะไม่ถูกแทรกแซง
3. ความเป็นส่วนตัวสนับสนุนเสรีภาพในการตัดสินใจ (Autonomy)
4. ความเป็นส่วนตัวช่วยป้องกันแรงกดดันจากการบังคับให้ปฏิบัติตามในสิ่งเดียวกันอันเป็นการจำกัดความคิดสร้างสรรค์ (Creativity) ซึ่งนำไปสู่ความหลากหลายในสังคม
5. ความเป็นส่วนตัวมีผลกระทบต่อสุขภาพจิต (Mental Health)
6. ความเป็นส่วนตัวเป็นสิ่งจำเป็นในการสร้างความสัมพันธ์ซึ่งมีความเชื่อมั่นและไว้เนื้อเชื่อใจกันในสังคม

เมื่อพิจารณาในมิติปัจจุบันจะเห็นว่าสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลได้รับการล่วงละเมิดมากขึ้น ด้วยเหตุที่เป็นเรื่องเกี่ยวข้องกับข้อมูลส่วนบุคคลซึ่งมีเป็นจำนวนมาก โดยเฉพาะมีการกระทำในลักษณะของการนำข้อมูลไปแสวงหาประโยชน์หรือนำไปเปิดเผยโดยไม่ได้รับ

---

[56] Hilary Delany, Eoin Carolan and Cliodhna Murphy, **The Right to Privacy: A Doctrinal and Comparative Analysis** (Dublin: Thomson Round Hall, 2008) อ้างถึงใน ชวิน อุ่นภัทร, “ความเป็นส่วนตัวและการคุ้มครองจากการล่วงล้ำของรัฐในประเทศสหรัฐอเมริกา,” **วารสารนิติศาสตร์** 44, 4 (ธันวาคม 2558): 971.

ความยินยอมจากเจ้าของข้อมูล จนเป็นเหตุให้เกิดความเดือดร้อนรำคาญหรือสร้างความเสียหายให้แก่บุคคลผู้เป็นเจ้าของข้อมูล ดังนั้นจึงมีความจำเป็นที่รัฐจะต้องเข้ามาดำเนินการเพื่อคุ้มครองให้สิทธินี้ได้รับความคุ้มครองอย่างแท้จริง กฎหมายที่จะตราออกมาเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลจึงมีความสำคัญยิ่ง กล่าวคือ[57]

ประการแรก ในระดับกฎหมายระหว่างประเทศ การคุ้มครองข้อมูลส่วนบุคคลเป็นสิทธิมนุษยชนขั้นพื้นฐาน อันเป็นมาตรฐานขั้นต่ำในการคุ้มครองสิทธิมนุษยชน ซึ่งในปัจจุบันกฎหมายในระดับระหว่างประเทศได้รับรองและกำหนดเป็นหลักเกณฑ์ในการให้ความคุ้มครองข้อมูลส่วนบุคคลไว้แล้ว เช่น Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ขององค์การความร่วมมือและการพัฒนาเศรษฐกิจ (OECD) หรือ Convention for the Protection of Individuals with Regard to Automatic. Processing of Personal Data ของคณะมนตรีแห่งยุโรป หรือ RESOLUTION on the Protection of the Rights of the Individual in the Face of Technical Developments in Data Processing และ General Data Protection Regulation ของสหภาพยุโรป หรือ Guidelines for the Regulation of Computerized Personal Data Files ของสหประชาชาติ เป็นต้น ซึ่งการยอมรับหลักการคุ้มครองข้อมูลส่วนบุคคลในระดับกฎหมายระหว่างประเทศมีความสำคัญต่อประเทศไทยปัจจุบันและอนาคตอย่างมาก เนื่องจากประเทศในกลุ่มองค์กรระหว่างประเทศต่าง ๆ มักไม่อนุญาตให้มีการถ่ายโอนข้อมูลไปยังประเทศที่ไม่มีมาตรฐานคุ้มครองที่ดีพอนั่นเอง หากประเทศไทยได้เป็นหนึ่งในประเทศที่ได้รับความเชื่อมั่นด้านการคุ้มครองข้อมูลแล้ว จะเป็นการสร้างความเชื่อมั่นให้กับชาวต่างชาติที่จะเข้ามาลงทุน นอกจากนี้ ยังเป็นการสร้างโอกาสให้กับประเทศไทยได้รับรู้ข้อมูลที่เป็นประโยชน์จากต่างประเทศมากยิ่งขึ้น

ประการที่สอง เป็นการแสดงออกถึงความมีพัฒนาการทางการเมือง เนื่องจากมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลเป็นมาตรการที่พัฒนามาเป็นลำดับของการคุ้มครองสิทธิเสรีภาพของประชาชนในระบอบประชาธิปไตย โดยเฉพาะอย่างยิ่งเป็นการแสดงออกถึงการมีส่วนร่วมในทางการเมืองของประชาชนในเชิงรุกในการเข้าถึงข้อมูลของตน มิใช่เพียงการแสดงออกทางการเมืองเฉพาะที่รัฐเปิดโอกาสให้ในการเลือกตั้งหรือลงประชามติเท่านั้น

ประการที่สาม มีความสำคัญต่อเศรษฐกิจแบบเสรี เพราะการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนั้นจำเป็นต่อระบบเศรษฐกิจแบบเสรีที่กำลังเกิดขึ้นในปัจจุบัน และจะยิ่งทวีความจำเป็นและสำคัญมากขึ้นอย่างไร้ขีดจำกัดในอนาคต ไม่ว่าจะเป็นค้าขายผ่านเครือข่ายอินเทอร์เน็ต การใช้บัตรเครดิต ซึ่งเกิดปัญหาอยู่เสมอว่ามีผู้นำข้อมูลส่วนบุคคลไปขายหรือใช้

---

[57] เพชรรัตน์ จงปัญญาประพันธ์, “ความสำคัญของกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล,” **วารสารนิติศาสตร์** 33, 4 (ธันวาคม 2546): 826-829.

ประโยชน์ อันจะสร้างความเสียหายแก่เจ้าของข้อมูล ดังนั้น การมีกฎหมายคุ้มครองสิทธิในข้อมูลส่วนบุคคลจึงเป็นมาตรการป้องกันการล่วงละเมิดและป้องกันปัญหาอื่น ๆ อันยุ่งยากซึ่งจะเกิดขึ้นในอนาคต

ประการที่สี่ การต้องมีกฎหมายให้ทันต่อความเปลี่ยนแปลงและเจริญก้าวหน้าของเทคโนโลยี โดยเฉพาะอย่างยิ่งในปัจจุบัน ความก้าวหน้าทางเทคโนโลยีที่มีมากขึ้น ก็ยิ่งทำให้ความเป็นส่วนตัวหรือสิทธิของบุคคล ล่อแหลมต่อการถูกละเมิดได้อย่างง่ายดายมากขึ้น ทั้งยังแพร่หลายได้โดยไร้ขีดจำกัดในระเวลาอันสั้น ยากที่จะทำการควบคุม ไม่ว่าจะเป็นการลักลอบดู หรือเข้าถึงข้อมูลแบบธรรมดา หรือ การใช้เทคนิคขั้นสูง ซึ่งการมีกฎหมายมาคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลก็จะสร้างความปลอดภัยให้กับข้อมูลได้มากยิ่งขึ้น และเป็นหน้าที่ของผู้ดูแลหรือควบคุมข้อมูลที่จะต้องสร้างความปลอดภัยให้ข้อมูล ทั้งยังไม่อาจเปิดเผยข้อมูลให้แตกต่างไปจากวัตถุประสงค์ที่ได้เก็บรวมรวมข้อมูลมา เว้นแต่เจ้าของข้อมูลจะอนุญาตเท่านั้น

ประการที่ห้า เป็นพื้นฐานสำหรับกฎหมาย หรือแนวปฏิบัติอื่น ๆ กฎหมายคุ้มครองข้อมูลจะเป็นพื้นฐานของกฎหมายหรือแนวปฏิบัติอื่น ๆ

ประการที่หก เป็นการสร้างความเชื่อมั่นให้เกิดขึ้น การคุ้มครองข้อมูลส่วนบุคคล จะทำให้เกิดความเชื่อมั่นว่าแก่บุคคลว่าข้อมูลของตนจะปลอดภัย ก่อนให้เกิดพัฒนาการต่อในด้านต่าง ๆ ไม่ว่าจะเป็นงานศิลปะ ธุรกิจ การลงทุน จะเกิดขึ้นอย่างเสรี โดยกฎหมายคุ้มครองข้อมูลจะมีบทบาทในการดูแล ไม่ว่าจะเป็นการจัดเก็บข้อมูล การควบคุมคุณภาพของข้อมูล การใช้ข้อมูลอย่างจำกัด การรักษาความปลอดภัยของข้อมูล การเปิดเผยข้อมูล การมีตรวจสอบข้อมูลของเจ้าของ และหลักความรับผิดเมื่อมีการละเมิดข้อมูลส่วนบุคคล

2.2.2.1 หลักการพื้นฐานของการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล

ด้วยเหตุที่ปัจจุบันเป็นสังคมแห่งการติดต่อสื่อสารไร้พรมแดนมีการส่งผ่านข้อมูลจำนวนมหาศาลได้ในเวลาอันรวดเร็วและทำได้อย่างง่ายดาย ซึ่งนั่นก็ย่อมก่อให้เกิดการละเมิดต่อสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลได้ง่ายเช่นกัน ฉะนั้นการหามาตรการคุ้มครองจึงเป็นสิ่งจำเป็นอย่างยิ่ง กฎหมายการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลจึงให้ความสำคัญแก่กระบวนการจัดเก็บ ข้อมูลเป็นอย่างมาก ต้องดำเนินการอย่างมีประสิทธิภาพ มีความเป็นธรรมและถูกต้องตามกฎหมาย ซึ่งกระบวนการต่าง ๆ ในการจัดเก็บข้อมูลส่วนบุคคลต้องเป็นไปในแนวทางที่กฎหมายกำหนด ซึ่งได้แก่วิธีการจัดเก็บรวบรวมข้อมูลส่วนบุคคล การเปิดเผยข้อมูลส่วนบุคคลการเข้าถึงข้อมูลส่วนบุคคล การตรวจสอบความถูกต้องของการเก็บรวบรวมข้อมูลและการประมวลผลข้อมูล และการรักษาความปลอดภัยแก่ข้อมูล ซึ่งหลักการดังกล่าวนี้ ถือเป็นพื้นฐานของกฎหมายคุ้มครองข้อมูลส่วนบุคคล และด้วยเหตุนี้ทำให้องค์การเพื่อความร่วมมือทางเศรษฐกิจและ

การพัฒนา (OECD) มีแนวคิดที่จะวางกรอบเพื่อกำหนดให้เป็นแนวทางสำหรับการออกกฎหมายเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล โดยกำหนดให้ถือเป็นอีกสิทธิหนึ่งที่เพิ่มขึ้นจากการคุ้มครองสิทธิโดยทั่วไปที่มีมาตรการและกลไกของรัฐต่าง ๆ คุ้มครองอยู่แล้ว ซึ่งหลักเกณฑ์ในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ได้แก่ Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data ปี ค.ศ.1980 ขององค์การเพื่อความร่วมมือทางเศรษฐกิจ และการพัฒนา (OECD) ซึ่งมีหลักการที่สำคัญ 8 ประการ ดังนี้

1. หลักข้อจำกัดในการเก็บรวบรวมข้อมูล (Collection Limitation Principle) ในการเก็บรวบรวมข้อมูลนั้น ต้องชอบด้วยกฎหมายและต้องใช้วิธีการที่เป็นธรรมและเหมาะสม โดยในการเก็บรวบรวมข้อมูลนั้นต้องให้เจ้าของข้อมูลรู้เห็น รับรู้หรือได้รับความยินยอมจากเจ้าของข้อมูล

2. หลักคุณภาพของข้อมูล (Data Quality and Proportional Principle) ข้อมูลจะต้องถูกต้อง สมบูรณ์ หรือทำให้เป็นปัจจุบันหรือทันสมัยอยู่เสมอ

3. หลักการกำหนดวัตถุประสงค์ในการจัดเก็บ (Purpose Specification Principle) ต้องกำหนดวัตถุประสงค์ว่าข้อมูลที่มีการเก็บรวบรวมนั้น เก็บรวบรวมไปเพื่ออะไร พร้อมทั้งกำหนดระยะเวลาที่เก็บรวบรวมหรือรักษาข้อมูลนั้น ตลอดจนกรณีที่จำเป็นต้องมีการเปลี่ยนแปลงวัตถุประสงค์ในการเก็บรวบรวมข้อมูล เช่นว่านั้นไว้ให้ชัดเจน

4. หลักข้อจำกัดในการนำไปใช้ (Use Limitation Principle) สาระสำคัญ คือ ข้อมูลส่วนบุคคลนั้น จะต้องไม่มีการเปิดเผยทำให้มีหรือปรากฏในลักษณะอื่นใด ซึ่งไม่ได้กำหนดไว้โดยชัดแจ้งในวัตถุประสงค์ของการเก็บรวบรวมข้อมูล เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูล หรือโดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย

5. หลักการรักษาความมั่นคงปลอดภัยข้อมูล (Security Safeguards Principle) สาระสำคัญ คือ จะต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสมเพื่อป้องกันความเสี่ยงภัยใด ๆ ที่อาจจะทำให้ข้อมูลนั้นสูญหาย เข้าถึง ทำลาย ใช้ ดัดแปลงแก้ไข หรือเปิดเผยโดยมิชอบ

6. หลักการเปิดเผยข้อมูล (Openness Principle) สาระสำคัญ คือ ควรมีการประกาศนโยบายฯ ให้ทราบโดยทั่วกัน หากมีการปรับปรุงแก้ไข หรือพัฒนาแนวนโยบายหรือแนวปฏิบัติที่เกี่ยวกับข้อมูล ส่วนบุคคล ก็ควรเปิดเผยหรือประกาศไว้ให้ชัดเจน รวมทั้งให้ข้อมูลใด ๆ ที่สามารถระบุเกี่ยวกับหน่วยงานของรัฐผู้ให้บริการ ที่อยู่ ผู้ควบคุมข้อมูลส่วนบุคคลด้วย

7. หลักการมีส่วนร่วมของบุคคล (Individual Participation Principle) สาระสำคัญ คือ ให้บุคคลซึ่งเป็นเจ้าของข้อมูลได้รับแจ้งหรือยืนยันจากหน่วยงานของรัฐที่เก็บรวบรวมหรือ

จัดเก็บข้อมูลทราบว่า “หน่วยงานของรัฐนั้น ๆ ได้รวบรวมข้อมูลหรือจัดเก็บข้อมูลส่วนบุคคลดังกล่าวหรือไม่ ภายในระยะเวลาที่เหมาะสม”

8. หลักความรับผิดชอบ (Accountability Principle) สาระสำคัญ คือ ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

ต่อมา ในปี ค.ศ.2013 ได้มีการทำการปรับปรุงหลักการและเนื้อหาของ Guidelines on the protection of Privacy and Transborder Data Flows of Personal Data ซึ่งหลักการที่ได้ทำการปรับปรุงแก้ไขใหม่นี้ ได้มีการปรับเปลี่ยนมุมมองในการปกป้องคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล เพื่อให้สามารถเป็นแนวทางในการคุ้มครองสิทธินี้ได้อย่างมีประสิทธิภาพ โดยให้ความสำคัญกับการหลีกเลี่ยงการเข้าถึงข้อมูลโดยไม่มีเหตุผล และการใช้ข้อมูลโดยไม่จำเป็น ซึ่งเรื่องนี้เป็นเรื่องสำคัญอย่างยิ่งต่อ ปัจเจกชน สังคม และระบบเศรษฐกิจ นอกจากนี้ยังมีการยกระดับความรับผิดชอบในการคุ้มครองข้อมูลส่วนบุคคล ทั้งยังมีการปรับปรุงนิยามความหมายของถ้อยคำสำคัญ หลายประการ เช่น คำว่า “การใช้ (Use)” ซึ่งในกรอบปี 1980 นั้น มีการกำหนดนิยามไว้อย่างกว้าง ๆ รวมถึงคำว่า “หลักการใช้ (Use Principle)” ซึ่งได้รับการตีความขยายความไปค่อยข้างมาก ก็ได้รับการจำกัดนิยามให้มีความชัดเจนขึ้น เพื่อจะได้นำไปสู่เป้าหมายดั้งเดิมอันเป็นที่มาของการกำหนดกรอบของ OECD ที่ต้องการสร้างสมดุลระหว่างสิทธิในความเป็นส่วนตัวกับการไหลเวียนของข้อมูลบนฐานของค่านิยมพื้นฐานที่มีการแข่งขัน (“Foundamental but Competing Values” of “Privacy and the Flow of Information”) ซึ่งภายใต้หลักการใหม่ที่มีการปรับปรุงแก้ไขนั้น Fred H. Cate, Peter Cullen และ Viktor Mayer-Schonberger ได้จัดแบ่งกลุ่มของหลักการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลไว้เป็น 3 กลุ่มและอธิบายหลักการพื้นฐานของการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลไว้อย่างน่าสนใจ ดังนี้[58]

กลุ่มที่ 1 หลักเกณฑ์ที่ใช้ในการเก็บรวบรวมข้อมูลส่วนบุคคล (Principle Applicable to the Collection of Personal Data)

1. หลักการเก็บรวมรวมข้อมูล (Collection Principle)

หลักการเก็บรวมรวมข้อมูลที่ได้มีการปรับปรุงนี้ มีการกำหนดหลักเกณฑ์ดังนี้คือ

1) ข้อมูลส่วนบุคคลไม่ควรเก็บรวบรวมโดย

(1) ละเมิดข้อจำกัดที่กำหนดโดยกฎหมาย

(2) ผ่านวิธีการหลอกลวง หรือ

---

[58] Fred H. Cate, Peter Cullen and Viktor Mayer-Schonberger, **Data Protection Principles for the 21st Century**, p. 23, Retrieved February 26, 2018 from https://www.repository.law.indiana.edu/facbooks/23

(3) ปราศจากเหตุผลอันสมควร

1) นอกเหนือจากข้อกำหนดข้างต้นหน่วยงานของรัฐไม่ควรรวบรวมข้อมูล

(1) เกินขอบเขตอำนาจตามกฎหมาย หรือ

(2) โดยมีวัตถุประสงค์อันไม่ชอบด้วยกฎหมาย

จากหลักการนี้อธิบายได้ว่า หลักการเก็บรวบรวมข้อมูล (Collection Principle) ซึ่งกำหนดขึ้นแทนที่หลักการเก็บรวมรวมข้อมูลอย่างจำกัด (Collection Limitation Principle) (ออกในปี 1980) สะท้อนให้เห็นถึงเจตนาที่จะให้ความสำคัญกับการปกป้องข้อมูลส่วนบุคคลมากขึ้น เหตุผลสำหรับเรื่องนี้มีดังต่อไปนี้

1. ผู้ดูแลข้อมูลมักอ้างเหตุผลที่ถูกต้องในการรวบรวมหรือเปิดเผยข้อมูลส่วนบุคคล ดังนั้นการให้ความสำคัญกับการกำหนดขอบเขตของเก็บรวบรวมข้อมูลจึงจำเป็นสำหรับการป้องกัน

2. การพัฒนาอย่างรวดเร็วของเทคโนโลยีสารสนเทศ และอุปกรณ์ตรวจจับต่าง ๆ ได้นำไปสู่การรวบรวมข้อมูลส่วนบุคคลโดยไม่มีความรู้หรือความตระหนักต่อสิทธิของปัจเจกบุคคล

3. ปัญหาเกี่ยวกับการแพร่หลายของเอกสารที่ถูกทำให้มีความหมายและเป็นประโยชน์ซึ่งมีมากขึ้น

4. มีการเพิ่มขึ้นของข้อมูลที่ถูกรวบรวมและจัดเก็บ ซึ่งส่งผลให้ค่าส่งผ่านข้อมูลราคาถูกลง ซึ่งสังคมกำลังค้นพบการใช้ประโยชน์ที่อย่างมีคุณค่ามากขึ้นของข้อมูลส่วนบุคคลเหล่านี้

5. การให้ความสำคัญกับการแจ้งและความยินยอม มีแนวโน้มที่จะเพิ่มความรับผิดชอบในการคุ้มครองข้อมูลแก่เจ้าของข้อมูลส่วนบุคคล การเปลี่ยนไปให้ความสำคัญเช่นนี้ทำให้ผู้ใช้ข้อมูลจะต้องมีความรับผิดชอบเพิ่มขึ้น

หลักการเก็บรวมข้อมูลนี้รวมถึงการปฏิบัติตามข้อจำกัดทางกฎหมายอื่น ๆ ในการเก็บรวบรวม (เช่นกฎหมายห้ามมิให้มีการบุกรุกหรือล่วงละเมิด) และห้ามรวบรวมข้อมูลส่วนบุคคลโดยการหลอกลวงหรือฉ้อโกง โดยต้องสร้างความมั่นใจในความโปร่งใสโดยปราศจากการซุกซ่อนข้อมูล

นี่คือหลักการเดียวที่เน้นเฉพาะกิจกรรมของรัฐบาล สะท้อนให้เห็นถึงความเชื่อมั่นว่านอกเหนือจากบทบัญญัติที่ใช้บังคับกับการเก็บรวบรวมข้อมูลทั้งหมดการเก็บรวบรวมข้อมูลของรัฐบาลควรดำเนินการให้มีความถูกต้องตามกฎหมายทั่วไปและมีวัตถุประสงค์ที่ถูกต้อง

กลุ่มที่ 2 หลักเกณฑ์ที่ใช้บังคับกับการใช้ข้อมูลส่วนบุคคล (Principles Applicable to the Use of Personal Data)

2. หลักการนำไปใช้ (Use Principle)

1) ความถูกต้องของการใช้ข้อมูลส่วนบุคคลควรพิจารณาจากการสร้างความสมดุลระหว่าง

(1) ระดับความเป็นไปได้และผลประโยชน์ที่เกิดจากการใช้ประโยชน์จากข้อมูลดังกล่าว

(2) ระดับความเป็นไปได้ที่จะเกิดความเสียหายจากการใช้ข้อมูลนั้น และ

(3) มาตรการในการป้องกันการละเมิดดังกล่าว

2) การใช้ข้อมูลส่วนบุคคลที่อาจทำให้เกิดผลกระทบ

(1) ไม่ควรให้บุคคลใดได้รับความเสียหายหรือเสียหายน้อยที่สุดโดยได้รับการคุ้มครองขั้นพื้นฐานตามหลักการเหล่านี้

(2) ความเสียหายที่เป็นนัยสำคัญ เช่น การบาดเจ็บทางร่างกายหรือการสูญเสียชีวิตเป็นเรื่องต้องห้าม และ

(3) ความเสียหายอื่น ๆ ควรได้รับความคุ้มครองอย่างเหมาะสมกับความเสี่ยงและระดับของความเสียหาย

3) การให้ทางเลือกแก่บุคคลควรจะต้องเป็นการป้องกันเฉพาะในกรณีที่มีเป้าหมายที่ชัดเจนและจำเป็น โดยต้องมีความชัดเจนใช้เพื่อให้เป็นทางเลือกที่แท้จริง และมีการให้ข้อมูลที่เกี่ยวข้องและให้ความเข้าใจเกี่ยวกับทางเลือกและผลที่ตามมา

4) เมื่อพิจารณาถึงความเป็นส่วนตัวและการไหลเวียนของข้อมูลส่วนบุคคลแต่ละประเทศควรดำเนินการโดยผ่านกระบวนการที่โปร่งใสเพื่อกำหนดวิธีการประเมินผลกระทบจากความเสียหายและผลประโยชน์ การใช้ข้อมูลส่วนบุคคลที่จะได้รับอนุญาต ห้ามหรืออนุญาตเฉพาะกรณีที่มีการป้องกันอันเหมาะสมภายใต้การยินยอมของแต่ละบุคคล องค์การสหประชาชาติสนับสนุนแต่ละประเทศให้ร่วมมือและประสานงานในการกำหนดมาตรการเหล่านี้

หลักการใช้ข้อมูลส่วนบุคคล อธิบายได้ดังนี้คือ ผู้ดูแลข้อมูลจะต้องระมัดระวังในการประเมินผลประโยชน์ ความเสียหาย และเครื่องมือในการบรรเทาความเสียหายที่เหมาะสมในการใช้ข้อมูล ลักษณะของการประเมินและการกำหนดความเสียหาย(และประโยชน์) อาจแตกต่างกันไปในแต่ละประเทศ แต่หลักการใช้ข้อมูลส่วนบุคคลนั้นจะช่วยเพิ่มความสามารถและประสิทธิภาพในการประเมินผลกระทบ โดยการยอมรับเกณฑ์มาตรฐาน หรือคำจำกัดความของ “ความเสียหายและผลประโยชน์” หลักการนี้ยังสนับสนุนให้รัฐบาลของแต่ละประเทศร่วมมือกันในการเข้าถึงข้อกำหนดและในการประสานการปฏิบัติตามกฎหมายต่อไป

ในส่วนคำจำกัดความ “ความเสียหาย” มีความหมายกว้าง ๆ ซึ่งรวมถึงความเสียหายที่เป็นรูปธรรม (เช่นการบาดเจ็บทางร่างกายและการสูญเสียทางการเงิน) ความเสียหายที่เป็นนามธรรม (เช่นความเสียหายต่อชื่อเสียงหรือความปรารถนาหรือการบุกรุกที่มากเกินไปในชีวิตส่วนตัว) รวมไปถึงความเสียหายในลักษณะของภยันตรายทางสังคมในวงกว้าง (เช่นการละเมิดสิทธิมนุษยชนในระดับชาติและระดับนานาชาติ) แต่ละประเทศควรใช้คำจำกัดความและ / หรือประเภท

ของความเสียหายที่เหมาะสมกับสภาพแวดล้อมของตนเองและควรให้แน่ใจว่าคำจำกัดความเหล่านี้สามารถใช้ได้อย่างกว้างขวาง

คำว่า “ประโยชน์” ซึ่งถูกใช้กันอย่างแพร่หลายนั้น แม้ว่าการกำหนดสิ่งที่ถือว่าเป็นประโยชน์อย่างถูกต้องอาจแตกต่างกันไปขึ้นอยู่กับบริบทของประเทศ แต่คำนี้จะรวมถึงผลประโยชน์แก่บุคคลผู้ดูแลข้อมูลและสังคม

หลักการใช้งานที่กำหนดขึ้นนี้จะส่งผลให้การใช้ข้อมูลบางอย่างจะได้รับอนุญาตเป็นประจำ (ตัวอย่างเช่นเพื่อความปลอดภัยของข้อมูล) โดยไม่มีเครื่องมือป้องกันข้อมูลเป็นพิเศษ การใช้ข้อมูลบางอย่างอาจเป็นสิ่งต้องห้ามโดยสิ้นเชิงหรืออาจจำเป็นต้องได้รับการคุ้มครองเป็นพิเศษ และอื่น ๆ อาจใช้มากที่สุดจะต้องมีการประเมินความเสี่ยงตามบริบทเฉพาะและเครื่องมือการป้องกันข้อมูลที่เหมาะสม

หลักการนี้ยอมรับว่าการให้ทางเลือกแก่บุคคลจะเป็นหนึ่งในเครื่องมือที่เหมาะสมได้ แต่ก็ต่อเมื่อทางเลือกดังกล่าวมีความหมาย (ตัวอย่างเช่นได้รับแจ้งข้อมูลในการดำเนินการและไม่อยู่ภายใต้ความแตกต่างที่มากเกินไปของอำนาจต่อรอง) นอกจากนี้เมื่อจำเป็นต้องมีการแจ้งและยินยอมควรมีความชัดเจนให้เป็นตัวเลือกที่แท้จริง (ไม่ใช่อยู่ในสถานการณ์ที่ถูกปล่อยปละละเลยเป็นประจำ) และพร้อมด้วยข้อมูลที่เกี่ยวข้องและความเข้าใจเกี่ยวกับทางเลือก รวมถึงผลที่ตามมา

3. หลักคุณภาพของข้อมูล (Data Quality Principle)

ข้อมูลส่วนบุคคลที่ใช้สำหรับการตัดสินใจอันจะมีผลต่อบุคคลควรมีความเกี่ยวข้องกับวัตถุประสงค์ที่ใช้และในขอบเขตที่จำเป็นสำหรับวัตถุประสงค์เหล่านั้นจะต้องมีความถูกต้องครบถ้วนและเป็นปัจจุบัน

จากหลักการนี้อธิบายได้ว่า หลักคุณภาพของข้อมูล เกือบจะเหมือนกันกับฉบับปี 1980 ยกเว้นว่าจะใช้เฉพาะกับ “ข้อมูลส่วนบุคคลที่ใช้ในการตัดสินใจที่มีผลกระทบต่อบุคคลต่าง ๆ เท่านั้น” ถ้อยคำที่มีการจำกัดนี้ ถูกออกแบบมาเพื่อหลีกเลี่ยงการสูญเสียทรัพยากรในการพยายามประเมินความถูกต้อง, ความครบถ้วนสมบูรณ์และทันเวลาของข้อมูลที่ไม่ได้ใช้ในลักษณะใด ๆ ที่อาจส่งผลกระทบต่อบุคคล นอกจากนี้หลักการยังระบุด้วยว่าการกำหนดความถูกต้อง ครบถ้วน สมบูรณ์และตรงเวลาของข้อมูลจำเป็นต้องรู้เพื่อวัตถุประสงค์ในการใช้ข้อมูล

4. หลักการมีส่วนร่วมของบุคคล (Individual Participation Principle)

1) ผู้ใช้ข้อมูลที่ใช้ข้อมูลส่วนบุคคลในลักษณะใดก็ตามที่มีผลต่อการศึกษา การจ้างงาน สุขภาพร่างกายหรือจิตใจ ฐานะทางการเงิน หรือสิทธิที่ได้รับการคุ้มครองตามกฎหมายของแต่ละบุคคลควรแจ้งให้บุคคลทราบว่ามีการใช้ข้อมูลส่วนบุคคลของเขา และควรให้สิทธิบุคคลเหล่านั้นเข้าถึงของมูลของตน บุคคลโดยไม่มีค่าใช้จ่าย และมีคำอธิบายที่ชัดเจนและเข้าใจง่ายเกี่ยวกับ

(1) ประเภทของข้อมูลส่วนบุคคลที่ใช้

(2) แหล่งข้อมูลส่วนบุคคลที่ใช้

(3) การมีอยู่ของข้อมูลส่วนบุคคลเหล่านั้น หรือข้อมูลเหล่านั้นจะถูกนำมาใช้ และ

(4) สิทธิตามกฎหมายของบุคคลตามหลักการนี้

2) บุคคลควรมีสิทธิในข้อมูลส่วนบุคคลของตนที่ถูกที่ใช้ในลักษณะใดก็ตามอันมีผลต่อการศึกษา การจ้างงาน สุขภาพร่างกายหรือจิตใจ ฐานะทางการเงิน หรือการคุ้มครองสิทธิของบุคคลนั้นตามกฎหมาย เพื่อ

(1) เข้าถึงข้อมูลส่วนบุคคลดังกล่าวที่เกี่ยวข้องกับบุคคลภายในเวลาที่เหมาะสม ที่มีค่าใช้จ่ายถ้ามีซึ่งไม่มากเกินไป ในลักษณะที่สมเหตุสมผล และในรูปแบบที่เข้าใจง่ายแก่บุคคล

(2) โต้แย้งการประมวลผลและความถูกต้องของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตน และหากการโต้แย้งรับฟังได้ ให้มีการแก้ไขข้อมูล โดยการลบ แก้ไขปรับปรุง หรือแก้ไขเพิ่มเติม และ

(3) จะต้องมีการให้เหตุผล เมื่อไม่สามารถปฏิบัติตามสองข้อข้างต้นได้

3. ผู้ดูแลข้อมูลควรแก้ไขข้อมูลส่วนบุคคลที่ไม่ถูกต้องเมื่อมีการร้องขอ หรือจะต้องให้เหตุผลที่ถูกต้องสำหรับความล้มเหลวในการดำเนินการดังกล่าว

หลักการนี้สามารถอธิบายได้ว่า หลักการการมีส่วนร่วมที่ได้มีการแก้ไขแล้วนั้นมีความแข็งแกร่งกว่าฉบับปี 1980 แต่ จำกัดอยู่ในสถานการณ์ที่มีการใช้ข้อมูลส่วนบุคคล “ในลักษณะใดก็ตามที่ส่งผลต่อการศึกษา การจ้างงาน สุขภาพร่างกายหรือจิตใจ ฐานะทางการเงิน หรือสิทธิที่ได้รับการคุ้มครองตามกฎหมายของแต่ละบุคคล” ในสถานการณ์เช่นนี้บุคคลมีสิทธิที่จะสังเกตเห็นว่ามีการใช้ข้อมูลส่วนบุคคลและบุคคลสามารถหาข้อมูลเกี่ยวกับการใช้งานได้อย่างง่ายดาย สำหรับในมิติการเข้าถึงข้อมูลนั้น ต้องให้โอกาสที่จะโต้แย้งการประมวลผลและความถูกต้องของข้อมูล หากมีการเข้าถึงหรือแก้ไขไม่ได้หรือไม่สามารถระงับการเผยแพร่ข้อมูลหรือประมวลผล และต้องให้โอกาสที่จะโต้แย้งเหตุผลเหล่านี้อย่างถูกต้องตามกฎหมาย อย่างไรก็ดี สิทธิการเข้าถึงเหล่านี้นอกเหนือจากสิทธิอื่น ๆ ในการเข้าถึงข้อมูลส่วนบุคคลที่อาจมีอยู่ในกฎหมายอื่นเช่นกฎหมายแรงงานหรือกฎหมายคุ้มครองผู้บริโภค

นอกจากนี้ ในการกำหนดหลักเกณฑ์ ผู้ดูแลข้อมูลมีหน้าที่ในการแก้ไขข้อมูลที่ไม่ถูกต้อง หรือ ให้เหตุผลที่ถูกต้องสำหรับความล้มเหลวในการทำเช่นนั้น สำหรับเหตุผลที่ถูกต้องจะต้องมีการกำหนดภายใต้กฎหมายที่ใช้บังคับและอาจมีความแตกต่างกันไปในแต่ละประเทศ แต่อาจรวมถึง

ปัจจัยต่าง ๆ เช่น ข้อผิดพลาดที่ไม่ก่อให้เกิดความเสียหายต่อผู้เจ้าของข้อมูลโดยเฉพาะอย่างยิ่งหากข้อผิดพลาดเหล่านี้มีราคาแพงหรือมีภาระหนักเกินสมควร

นอกเหนือจากหลักการมีส่วนร่วมของบุคคล บุคคลต่าง ๆ ยังคงมีสิทธิที่จะเพิกถอนการยินยอมในทุกกรณีที่ได้ให้ความยินยอมอย่างชัดแจ้งต่อการประมวลผลข้อมูลส่วนบุคคลโดยเป็นส่วนหนึ่งของกลไกการแจ้งและเลือก

กลุ่มที่ 3 หลักเกณฑ์ที่ใช้ในการรวบรวม, ใช้หรือ การประมวลผลข้อมูลส่วนบุคคลอื่น ๆ (Principles Applicable to the Collection, Use, or Other Processing of Personal Data)

5. หลักการเปิดเผยข้อมูล (Openness Principle)

ควรมีนโยบายเกี่ยวกับแนวปฏิบัติและนโยบายที่เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล

1) ควรมีวิธีการในการสร้างข้อกำหนดทั่วไปในการประมวลผลข้อมูลส่วนบุคคล, ลักษณะพื้นฐานของข้อมูลส่วนบุคคลที่กำลังดำเนินการ โดยต้องมีวิธีการป้องกันข้อมูลดังกล่าว

2) การระบุตัวตน, ที่ตั้ง และข้อมูลการติดต่อ (รวมถึง email address) ของผู้ดูแลข้อมูลควรให้สามารถเข้าถึงได้อย่างง่ายดาย

หลักการนี้อธิบายได้ว่า หลักการเปิดเผยข้อมูลที่ปรับปรุงแล้วมีความคล้ายคลึงกันมากกับหลักการเดิมในปี 1980 แต่มีการกำหนดสาระสำคัญเพื่อให้เกิดความชัดเจนมากขึ้น

6. หลักการรักษาความมั่นคงปลอดภัยข้อมูล (Security Safeguards Principle)

หลักการรักษาความมั่นคงปลอดภัยข้อมูลนั้น กำหนดให้ข้อมูลส่วนบุคคลควรได้รับป้องกันความปลอดภัยที่เหมาะสมจากความเสี่ยงทั้งภายนอกและภายใน ไม่ว่าจะเป็นความเสียหายจากเข้าถึง การทำลาย การใช้ การดัดแปลงแก้ไข หรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

ภายใต้หลักการรักษาความมั่นคงปลอดภัยข้อมูลนี้ เกือบจะเหมือนกันในสาระสำคัญกับฉบับปี 1980 แต่ได้รับการขยายเล็กน้อยเพื่อชี้แจงว่าภาระผูกพันในการปกป้องข้อมูลส่วนบุคคลจะครอบคลุมไปถึงความเสี่ยงทั้งภายในและภายนอก

7. หลักความรับผิดชอบ (Accountability Principle)

1) ทุกคนที่เก็บรวบรวมใช้หรือประมวลผลข้อมูลส่วนบุคคลจะต้องเป็นผู้ดูแลข้อมูลที่รับผิดชอบและด้วยเหตุนี้ ควรทำดังนี้

(1) รับผิดชอบในการปฏิบัติตามมาตรการที่มีผลต่อหลักการเหล่านี้

(2) ดำเนินการแก้ไขที่เหมาะสมกับบุคคลที่โดยให้สอดคล้องกับหลักการนี้

(3) ต้องรับผิดชอบต่อความเสียหายที่อาจคาดหมายได้ เนื่องมาจากความผิดพลาดของผู้ดูแลข้อมูล

(4) ตามคำร้องขอที่สมเหตุสมผลของออกกฎเกณฑ์ ผู้ดูแลข้อมูลต้องแสดงให้เห็นว่าได้พัฒนาและดำเนินการประเมินนโยบายและกระบวนการต่าง ๆ ที่เหมาะสมเพื่อให้เป็นไปตามกฎการประมวลผลข้อมูลที่สอดคล้องกับหลักการเหล่านี้

2) ไม่มีใครสามารถสงวนความรับผิดชอบภายใต้หลักการนี้ สำหรับการกระทำหรือการละเลยเกี่ยวกับข้อมูลส่วนบุคคล

จากหลักการนี้สามารถอธิบายได้ว่า หลักการความรับผิดชอบ ในปี 1980 เป็นไปในลักษณะจำกัดและไม่ชัดเชน ในฉบับที่ได้แก้ไขใหม่จึงกำหนดให้ "ผู้ควบคุมข้อมูลควรมีความรับผิดชอบในการปฏิบัติตามมาตรการที่มีผลต่อหลักการที่กล่าวไว้ข้างต้น" หลักการใหม่นี้กว้างขึ้นและเรียกร้องมากขึ้น ผู้ดูแลข้อมูลไม่เพียงรับผิดชอบต่อการปฏิบัติตามกฎเท่านั้น แต่ต้องสามารถแสดงให้ทราบว่าพวกเขามีเครื่องมือที่จะปฏิบัติตาม นอกจากนี้ภายใต้หลักการความรับผิดชอบใหม่ ผู้ดูแลข้อมูลต้องเยียวยาผู้ที่ได้รับความเสียหายด้วยการชดใช้ และต้องยอมรับรับผิดชอบต่อ "อันตรายที่คาดหมายได้" ซึ่งเกิดจากความผิดพลายในการดำเนินการ การเปลี่ยนแปลงเหล่านี้สอดคล้องกับการยกระดับความรับผิดชอบในการปกป้องข้อมูลของปัจเจกชนไปยังผู้ดูแลข้อมูล

นอกจากนี้หลักการใหม่ยังชี้ให้เห็นถึงความรับผิดชอบที่มุ่งเน้นไปที่ “ข้อมูลส่วนบุคคล” ซึ่งอยู่ภายใต้คำจำกัดความที่รวมถึง “ข้อมูลใด ๆ ที่ระบุถึงบุคคลอันสามารถใช้เพื่อระบุตัวบุคคลได้หรือเชื่อมโยงกับข้อมูลที่ระบุตัวบุคคล และ การใช้ "เชื่อมโยงกับข้อมูลที่ระบุตัวบุคคลและใช้ในลักษณะใด ๆ ที่ส่งผลกระทบต่อบุคคลนั้น” (แม้เป็นความรับผิดชอบตามกฎหมาย) คำจำกัดความนี้ให้หลักการกว้าง ๆ แต่ไม่สามารถบังคับใช้กับข้อมูลที่ไม่มีความเชื่อมโยงกับบุคคลได้

8. หลักการบังคับใช้กฎหมาย (Enforcement Principle)

1) แต่ละประเทศควรมีการเตรียมการด้านกฎระเบียบ หน่วยงาน และงบประมาณและบุคลากรที่เหมาะสมเพื่อให้มั่นใจว่ากฎหมายที่มีผลบังคับตามหลักการเหล่านี้จะมีผลบังคับใช้

2) การบังคับใช้กฎหมายคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลควรกำหนดการปฏิบัติตามหลักการเหล่านี้ และกฎหมายที่ใช้บังคับจะต้องมีประสิทธิภาพโดยสามารถจำกัดการละเมิดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล และควบคุมการไหลเวียนของข้อมูลที่ถูกกฎหมาย

หลักการข้อนี้อธิบายได้ว่า หลักเกณฑ์ของฉบับปี 1980 ไม่ได้มีหลักการบังคับใช้กฎหมาย แต่ประสบการณ์มากกว่า 30 ปีในการบังคับใช้ ได้แสดงให้เห็นถึงความสำคัญในการที่จะต้องทำให้มั่นใจได้ว่า การคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนั้น ไม่ใช่เพียงแต่มีการตรากฎหมายขึ้นรับรองสิทธิเท่านั้น แต่จะต้องมีบังคับใช้อย่างเข้มงวด ซึ่งภายใต้หลักการใหม่นี้ รัฐบาลจำเป็นต้องลงทุนด้านการงบประมาณและทรัพยากรบุคคลเพื่อบังคับใช้กฎหมายให้บรรลุเป้าหมายคือการ “บรรลุการปฏิบัติอย่างมีประสิทธิภาพ” โดยสามารถจำกัดการ

ละเมิดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล และควบคุมการไหลเวียนของข้อมูลที่ถูกกฎหมายได้นั่นเอง

จากหลักการข้างต้น สามารถสรุปได้ดังตารางต่อไปนี้[59]

ตารางที่ 2.1 สรุปหลักการของ Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data ของ OECD

กิจกรรมที่เกี่ยวกับข้อมูล (Data Activity)	**กระบวนการ (Processing)**		
	การจัดเก็บรวมรวม (Collection)	**การใช้ (Use)**	**กระบวนการอื่น (Other Processing)** (รวมถึงการเก็บรักษาและการทำลายข้อมูล)
หลักการ (Principle)	หลักการเก็บรวบรวมข้อมูล (Collection Principle) ; ใช้หลักการพิเศษต่างหากในการเก็บรวมรวมข้อมูลภาครัฐ	หลักการนำไปใช้ (Use Principle) หลักคุณภาพของข้อมูล (Data Quality Principle) หลักการมีส่วนร่วมของบุคคล (Individual Participation Principle) หลักการเปิดเผยข้อมูล (Openness Principle) หลักการรักษาความมั่นคงปลอดภัยข้อมูล (Security Safeguards Principle) หลักความรับผิดชอบ (Accountability Principle) หลักการบังคับใช้กฎหมาย (Enforcement Principle)	

[59] *Ibid.,* p. 15.

จากตารางนี้ จะเห็นว่า หลักการที่ออกมาโดยองค์กรเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD) ได้ออกแนวทางปฏิบัติเกี่ยวกับข้อมูลส่วนบุคคล โดยมีวัตถุประสงค์เพื่อการดูแลการส่งผ่านข้อมูลระหว่างประเทศ (Transborder Flow) และคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล อันมีจุดเริ่มต้นมาจากปัญหาความแตกต่างและไม่เท่าเทียมกันในมาตรฐานของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในแต่ละประเทศ ซึ่งอาจเป็นการขัดขวางการไหลเวียนของข้อมูลอันจะเป็นอุปสรรคต่อการค้าการลงทุน โดยวัตถุประสงค์หลักของแนวทางนี้ก็เพื่อเป็นเครื่องมือในการสร้างความเป็นอันหนึ่งอันเดียวกันของประเทศสมาชิก ทั้งนี้ เพื่อก่อให้เกิดความเชื่อมั่นแก่ภาคเอกชนและผู้ประกอบธุรกิจทั้งหลายในการติดต่อสัมพันธ์ทางการค้า โดยกฎเกณฑ์ของแนวทางต่าง ๆ ข้างต้น ถือเป็นแนวปฏิบัติขั้นต่ำของหลักการเพื่อให้ประเทศสมาชิกได้นำไปปฏิบัติภายในแต่ละประเทศ โดยไม่ได้แยกระหว่างหน่วยงานของรัฐและหน่วยงานเอกชน และหลักการต่าง ๆ นี้ถือเป็นหลักการในการคุ้มครองข้อมูลส่วนบุคคลที่ถูกนำไปพัฒนาปรับปรุงเป็นหลักการสำคัญต่าง ๆ ที่มีผลเป็นการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศต่าง ๆ ทั่วโลกในเวลาต่อมา

2.2.2.2 ข้อจำกัดของการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล

โดยธรรมชาติของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล อาจจะมีการประเด็นของการขัดแย้งกันกับสิทธิเสรีภาพในประการอื่น เช่นการขัดแย้งกับสิทธิเสรีภาพในการแสดงความคิดเห็น, สิทธิในการรับรู้ข้อมูลข่าวสาร ซึ่งเป็นสิทธิเสรีภาพขั้นพื้นฐานตามรัฐธรรมนูญและเป็นหลักการพื้นฐานของระบอบการปกครองแบบประชาธิปไตย นอกจากนี้ สิทธิในความเป็นส่วนตัวอาจขัดแย้งกับคุณค่า (Value) อื่น ๆ ที่รัฐธรรมนูญให้การรับรอง เช่น ประโยชน์สาธารณะในมิติของความมั่นคงของรัฐ รวมถึงความปลอดภัยจากอาชญกรรมของประชาชน ซึ่งคุณค่าเหล่านี้ล้วนแล้วแต่มีลักษณะเป็นประโยชน์สาธารณะอันเป็นภารกิจของรัฐที่จะต้องดำเนินการให้กับประชาชน ดังนั้นเราจะเห็นว่า สิทธิในความเป็นส่วนตัวทุกประเภทรวมถึงสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลจึงไม่ใช่สิทธิเสรีภาพที่เป็นสิทธิโดยสมบูรณ์ แต่เป็นสิทธิที่อาจถูกจำกัดได้ บนพื้นฐานของการคุ้มครองประโยชน์มหาชนหรือประโยชน์สาธารณะ ซึ่งมีหลักการในการดำเนินการดังนี้

1. หลักการคุ้มครองประโยชน์สาธารณะ

ประโยชน์มหาชน หรือสาธารณะประโยชน์นี้ ถือเป็น นิติสมบัติ (Rechtgut) หรือคุณธรรมในทางกฎหมายมหาชน กล่าวคือ เป็นวัตถุหรือสิ่งที่กฎหมายมุ่งที่จะคุ้มครองป้องกันอันมีที่มาจากพื้นฐานของการแยกความต้องการส่วนตัวหรือประโยชน์ส่วนตัวออกจากความต้องการส่วนรวมหรือประโยชน์มหาชนออกจากกันนั่นเอง ซึ่งคุณค่าเช่นนี้ทำให้รัฐมีความชอบธรรมในการใช้อำนาจ

บังคับแก่เอกชนในการดำเนินภารกิจ ซึ่งประเภทของประโยชน์มหาชนนี้ แบ่งได้ออกเป็น 2 ประเภท คือ[60]

ประโยชน์มหาชนทั่วไป เป็นประโยชน์แก่เอกชนทุกคน เช่น ประโยชน์จากการป้องกันประเทศโดยกำลังทหาร การรักษาความปลอดภัยภายในโดยตำรวจ หรือประโยชน์จากหลักการคุ้มครองโดยทางภาษี งานมหาชนหรือบริการสาธารณะที่เป็นประโยชน์ทั่วไปนี้ อยู่ในลักษณะของประโยชน์ทางอ้อม เช่น ประโยชน์จากการคุ้มครองโดยทางภาษี อาจเป็นผลดีแก่พ่อค้าหรือนักอุตสาหกรรมจำนวนมาก แต่ไม่มีผู้ใดผู้หนึ่งได้รับประโยชน์โดยเฉพาะเจาะจงจากการคุ้มครองนี้และไม่ก่อให้เกิดสิทธิโดยตรงแก่เอกชน

ประโยชน์มหาชนเฉพาะ เป็นประโยชน์ที่ตกได้แก่บุคคลโดยเฉพาะเจาะจง ประโยชน์ชนิดนี้คือ สิทธิในทางมหาชนซึ่งมีลักษณะเป็นประโยชน์โดยตรงเฉพาะรายตัวบุคคลเป็นคน ๆ ไป เช่น ประโยชน์จากการจัดการศึกษาของกระทรวงศึกษาธิการย่อมตกแก่ผู้ศึกษา ซึ่งก็คือนักเรียนในโรงเรียนของรัฐ ประโยชน์จากกิจการไปรษณีย์ย่อมก่อให้เกิดประโยชน์แก่ผู้ส่งข่าวสารและผู้รับข่าวสาร การที่รัฐหรือฝ่ายปกครองดำเนินการก่อให้เกิดประโยชน์ตามความปรารถนาของบุคคลแต่ละคนเหล่านี้ คือวิถีทางที่จะทำให้ความเป็นอยู่ของประชาชนมีความสะดวกสบายและเจริญก้าวหน้า จึงต้องนับว่าเป็นงานมหาชนที่เป็นประโยชน์ต่อส่วนรวมด้วยในขณะเดียวกัน

2. ขอบเขตของการคุ้มครองสิทธิในความเป็นส่วนตัว

จากลักษณะของประโยชน์สาธารณะข้างต้น จะเห็นได้ว่า แม้ว่าสิทธิส่วนตัวจะเป็นสิทธิที่ได้รับการรับรองโดยปฏิญญาสากลฯ รวมถึงกฎเกณฑ์กติกาต่าง ๆ ทั้งภายนอกและภายในของแต่ละรัฐ แต่สิทธิความเป็นส่วนตัวนี้มักจะถูกล่วงล้ำโดยมีการอ้างถึงสิทธิที่รับรู้ข้อมูลข่าวสารของประชาชน (People's Right to Know) เพื่อเป็นเหตุสำหรับการเข้าถึงข้อมูลส่วนตัวของบุคคล นอกจากนี้สิทธิส่วนตัวของบุคคลก็อาจถูกล่วงละเมิดได้จากเจ้าหน้าที่ของรัฐ โดยทั่วไปแล้ว การรุกล้ำในความเป็นส่วนตัวเป็นสิ่งที่ไม่สามารถกระทำได้ เว้นแต่จะมีความจำเป็นในเรื่องของความมั่นคงแห่งรัฐ (National Security) ซึ่งความจำเป็นเช่นนี้จะต้องเป็นไปเพื่อความสงบเรียบร้อยของประชาชน

อาจกล่าวได้ว่า สิทธิส่วนตัวมีขอบเขตเท่าที่ไม่เป็นปรปักษ์กับประโยชน์สาธารณะ การกำหนดขอบเขตอันสมควรในเรื่องสิทธิส่วนตัวจึงเป็นความพยายามที่จะสร้างดุลภาพโดยการประสานประโยชน์ที่ขัดแย้งกัน ระหว่างประโยชน์ของบุคคลหนึ่งในชีวิตส่วนตัวกับประโยชน์สังคมส่วนรวม ซึ่งประโยชน์ทั้งสองประการสามารถนำมาประสานกันได้บนรากฐานของการยอมรับที่สมเหตุสมผล เป็นการยอมรับสิทธิส่วนตัวโดยไม่บั่นทอนประโยชน์สาธารณะ ทั้งในมิติของสิทธิเสรีภาพในการแสดงความคิดเห็น สิทธิที่จะรับรู้ข้อมูลข่าวสารของประชาชน รวมไปถึงประเด็น

---

[60] สมยศ เชื้อไทย, **กฎหมายมหาชนเบื้องต้น** (กรุงเทพมหานคร: วิญญูชน, 2560), หน้า 37-38.

ทางด้านความปลอดภัยของประชาชนและความมั่นคงของรัฐ ซึ่งการจะทำให้เกิดดุลยภาพระหว่างสิทธิในความเป็นส่วนตัวและประโยชน์สาธารณะนี้จะต้องอยู่บนพื้นฐานของหลักความได้สัดส่วนซึ่งจะได้กล่าวถึงในลำดับต่อไปนั่นเอง

3. หลักความได้สัดส่วนระหว่างการคุ้มครองสิทธิในความเป็นส่วนตัวกับการคุ้มครองประโยชน์สาธารณะ

หลักความได้สัดส่วน เป็นหลักกฎหมายทั่วไปในทางกฎหมายมหาชนที่สำคัญหลักการหนึ่งกับการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล กล่าวคือ มีความสัมพันธ์ในลักษณะเกื้อกูลกัน เพราะหลักการนี้จะเป็นเครื่องช่วยในการรักษาดุลยภาพระหว่างการคุ้มครองข้อมูลข่าวสารส่วนบุคคลอันเป็นสิทธิเสรีภาพขั้นพื้นฐานด้านหนึ่งกับข้ออ้างในการเข้ามาแทรกแซงสิทธินี้ด้วยอำนาจของฝ่ายรัฐมักจะอ้างถึงประโยชน์สาธารณะที่มีอำนาจเหนือกว่า[61] ซึ่งในระบบกฎหมายของยุโรปยอมรับหลักการนี้มาอย่างยาวนานว่าเป็นหลักการพื้นฐานของความสัมพันธ์ระหว่างผู้ใช้อำนาจ (รัฐ) กับผู้ที่ตกอยู่ภายใต้อำนาจบังคับ (ประชาชน) โดยเป็นหลักให้ผู้ใช้อำนาจต้องใช้อำนาจจำกัดสิทธิเสรีภาพของผู้ตกอยู่ใต้อำนาจอย่างพอเหมาะพอประมาณ[62]

หลักการขั้นพื้นฐานของความสัมพันธ์ระหว่างผู้ใช้อำนาจกับผู้ที่ตกอยู่ภายใต้อำนาจนี้บังคับให้ผู้ใช้อำนาจจำกัดสิทธิและเสรีภาพของผู้ที่ตกอยู่ภายใต้อำนาจของตนอย่างพอเหมาะพอประมาณ (Moderation) ถึงแม้ว่ารัฐธรรมนูญของรัฐเสรีประชาธิปไตยส่วนใหญ่ไม่ได้บัญญัติกำหนดหลักกฎหมายนี้ไว้เป็นลายลักษณ์อักษร แต่ก็ถือกันว่าเป็นหลักรัฐธรรมนูญทั่วไปและมีค่าบังคับเสมอกันกับบทบัญญัติแห่งรัฐธรรมนูญทุกประการ หลักกฎหมายดังกล่าวมีสาระสำคัญประกอบด้วยหลักการย่อย ๆ สามหลักการด้วยกันคือ หลักแห่งความเหมาะสม (Principle of Suitability) หลักแห่งความจำเป็น (Principle of Necessity) และหลักแห่งความได้สัดส่วนในความหมายอย่างแคบ (Principle of Proportionality in the Narrow Sense) ซึ่งในที่นี้จะขอนำเสนอสาระสำคัญของหลักความได้สัดส่วนในกฎหมายปกครองฝรั่งเศสที่มีรายละเอียดดังนี้[63]

---

[61] กิตติพงศ์ กมลธรรมวงศ์, *เรื่องเดิม*, หน้า 73.

[62] Paul Muller, **Le principe de la proportionnalité** (S.l.: s.n., 1978) อ้างถึงในวรพจน์ วิศรุตพิชญ์, **คู่มือศึกษาวิชากฎหมายปกครอง** (กรุงเทพมหานคร: สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา, 2545), หน้า 145.

[63] วรพจน์ วิศรุตพิชญ์, **คู่มือศึกษาวิชากฎหมายปกครอง** (กรุงเทพมหานคร: สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา, 2545), หน้า 85-94.

1. หลักแห่งความเหมาะสม

หลักแห่งความเหมาะสมบังคับว่าในบรรดามาตรการที่กฎหมายเปิดช่องให้ออกมาใช้บังคับแก่ประชาชนได้นั้น ฝ่ายปกครองต้องใช้วิจารณญาณเลือกออกมาตรการที่สามารถดำเนินการให้เจตนารมณ์หรือความมุ่งหมายของกฎหมายสำเร็จลุล่วงไปได้เท่านั้น มาตรการใดก็ตามที่ไม่สามารถทำให้เจตนารมณ์หรือความมุ่งหมายของกฎหมายฉบับที่ให้อำนาจปรากฏเป็นจริงขึ้นมาได้เลย ย่อมเป็นมาตรการที่ขัดต่อหลักการดังกล่าว และดังนั้น จึงไม่มีผลใช้บังคับได้ จะเห็นได้ว่าหลักแห่งความเหมาะสมนี้เรียกร้องความสัมพันธ์เชิงเหตุ (Cause) และผล (Effect) ระหว่างมาตรการที่ฝ่ายปกครองออกมาใช้บังคับกับสิ่งที่กฎหมายฉบับที่ให้อำนาจประสงค์จะให้เกิดขึ้น ทั้งนี้โดยให้มาตรการที่ฝ่ายปกครองออกมาใช้บังคับเป็นเหตุ (Cause) และสิ่งที่กฎหมายฉบับที่ให้อำนาจประสงค์จะให้เกิดขึ้นเป็นผล (Effect) ดังนั้นจึงกล่าวได้ว่า หลักแห่งความเหมาะสมจึงเป็นสิ่งเดียวกันกับสามัญสำนึก (Common Sense) นั่นเอง มาตรการที่ไม่อาจก่อให้เกิดผลตามที่ต้องการจะให้เกิดได้อย่างแน่แท้ หรือมาตรการที่ก่อให้เกิดผลตรงกันข้ามที่ต้องการจะให้เกิด แท้ที่จริงแล้วเป็นมาตรการที่ไร้ความหมายอย่างสิ้นเชิงในสายตาของคนที่มีสติสัมปชัญญะเต็มบริบูรณ์ และเนื่องจากบุคคลที่ได้รับแต่งตั้งให้ดำรงตำแหน่งหน้าที่ทางปกครองล้วนแล้วแต่เป็นคนที่จริตไม่วิกล ดังนั้นหากฝ่ายปกครองออกมาตรการที่ไม่สามารถดำเนินการให้เป็นไปตามเจตนารมณ์หรือความมุ่งหมายของกฎหมายได้อย่างแน่แท้ จึงต้องสันนิษฐานไว้ก่อนว่าฝ่ายปกครองประสงค์จะใช้มาตรการนั้นเป็นเครื่องมือดำเนินการให้เกิดผลอย่างอื่นนอกเหนือไปจากผลที่กฎหมายประสงค์จะให้เกิดขึ้น เข้าข่ายเป็นการใช้อำนาจโดยมิชอบ (Abuse of Power)

2. หลักแห่งความจำเป็น

หลักแห่งความจำเป็น หมายความว่า ในบรรดามาตรการหลาย ๆ มาตรการซึ่งล้วนแต่สามารถทำให้เจตนารมณ์หรือความมุ่งหมายของกฎหมายฉบับที่ให้อำนาจสำเร็จลุล่วงไปได้ แต่ทว่าแต่ละมาตรการมีผลกระทบกระเทือนต่อสิทธิหรือเสรีภาพของประชาชนมากน้อยแตกต่างกัน ฝ่ายปกครองต้องตัดสินใจเลือกออกมาตรการที่มีความรุนแรงน้อยที่สุด ความคิดที่เป็นรากฐานของหลักการนี้มีอยู่ว่า “ในระหว่างสิ่งที่เลวร้ายสองสิ่งที่จำต้องเลือก บุคคลควรเลือกสิ่งที่เลวร้ายน้อยกว่า” ดังนั้น ฝ่ายปกครองจึงมีอำนาจจำกัดสิทธิหรือเสรีภาพของราษฎรได้เพียงเท่าที่จำเป็นแก่การดำเนินการให้เป็นไปตามความประสงค์ของกฎหมายเท่านั้น การจำกัดสิทธิหรือเสรีภาพของราษฎรเกินขอบเขตแห่งความจำเป็นแก่การดำเนินการให้เป็นไปตามความประสงค์ของกฎหมายเป็นสิ่งที่ไม่ชอบธรรม ดังนั้นจะสังเกตได้ว่า องค์ประกอบของหลักแห่งความได้สัดส่วนข้อที่สองนี้จะใช้บังคับได้ก็ต่อเมื่อปรากฏว่า มีมาตรการที่เหมาะสมอยู่หลายมาตรการเท่านั้น ในกรณีที่มีมาตรการที่สามารถดำเนินการให้เจตนารมณ์หรือความมุ่งหมายของกฎหมายสำเร็จลุล่วงไปได้อยู่เพียงมาตรการเดียว

ปัญหาว่าฝ่ายบริหารได้เลือกออกมาตรการที่จำเป็นหรืออีกนัยหนึ่งมาตรการที่รุนแรงน้อยที่สุดแล้วหรือไม่ จะไม่มีทางเกิดขึ้นได้เลย

3. หลักแห่งความได้สัดส่วนในความหมายอย่างแคบ

หลักแห่งความได้สัดส่วนในความหมายอย่างแคบ เป็นหลักการที่เรียกร้องให้เกิดภาวะสมดุลขึ้นระหว่างความเสียหายอันจะเกิดขึ้นแก่เอกชนและ/หรือแก่สังคมโดยส่วนรวมกับประโยชน์อันมหาชนจะพึงรับจากการดำเนินการให้เป็นไปตามมาตรการใดมาตรการหนึ่งที่ฝ่ายปกครองออกมาใช้บังคับ ดังนั้นองค์ประกอบข้อที่สามของหลักแห่งความได้สัดส่วนนี้จึงบังคับให้ฝ่ายปกครองต้องทำการชั่งผลดีและผลเสียของมาตรการแต่ละมาตรการที่ตนตั้งใจจะออกมาใช้บังคับแก่ราษฎร มาตรการใดก็ตามที่เห็นได้ชัดว่าหากได้ลงมือบังคับการให้เป็นไปตามนั้นแล้ว จะยังให้เกิดประโยชน์แก่มหาชนน้อยมากไม่คุ้มกับความเสียหายที่จะเกิดขึ้นแก่เอกชนและ/หรือแก่สังคมโดยส่วนรวม ฝ่ายปกครองต้องห้ามมิให้ออกมาใช้บังคับ ถึงแม้ว่ามาตรการนั้นจะเหมาะสมและจำเป็นแก่การดำเนินการให้ความประสงค์ของกฎหมายสำเร็จลุล่วงไปได้ก็ตาม เมื่อบังคับตามหลักแห่งความได้สัดส่วนในความหมายอย่างแคบกันอย่างเคร่งครัดแล้ว ในกรณีที่มาตรการต่าง ๆ ซึ่งกฎหมายเปิดช่องให้ฝ่ายปกครองออกมาใช้บังคับได้ทุกมาตรการก่อความเสียหายแก่เอกชนและ/หรือสังคมโดยส่วนรวมมากกว่าประโยชน์ที่มหาชนจะพึงได้รับ ฝ่ายปกครองต้องละเว้นจากการใช้อำนาจกระทำการอย่างใด ๆ เลยทีเดียว

ดังนั้นกล่าวโดยสรุปได้ว่า ในกรณีเกิดปัญหาการขัดกันระหว่างสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลกับประโยชน์สาธารณะที่ถูกอ้างโดยฝ่ายรัฐหรือปัจจเจกชนด้วยกันที่ยกการทำหน้าที่เพื่อประโยชน์สาธารณะนั้น จะเห็นว่า การคุ้มครองสิทธิในข้อมูลส่วนบุคคล ที่ฝ่ายรัฐสามารถอ้างประโยชน์สาธารณะเข้ามาแทรกแซงในการเปิดเผยข้อมูลส่วนบุคคล หรือในกรณีการที่มีบุคคลอันเป็นปัจจเจกชนโดยเฉพาะสื่อมวลชนจะอ้างเสรีภาพในการแสดงออกซึ่งความคิดความเห็นล่วงล้ำเข้ามาวิพากษ์วิจารณ์หรือเปิดเผยข้อมูลส่วนบุคคลบางอย่าง เมื่อพิจารณาจากหลักความได้สัดส่วนก็จะพบว่า การล่วงละเมิดข้อมูลส่วนบุคคลจะต้องคำนึงถึงประโยชน์ 2 ประการ ประการแรกได้แก่ ประโยชน์สาธารณะ อันเป็นประโยชน์ส่วนรวมที่ส่วนรัฐมีหน้าที่ดูแลรักษา กับประโยชน์ส่วนบุคคล ซึ่งแบ่งออกเป็นประโยชน์ของผู้ขอให้เปิดเผยข้อมูลด้านหนึ่ง และประโยชน์ของบุคคลที่สามที่ได้รับผลกระทบจากการเปิดเผยข้อมูลข่าวสารดังกล่าวอีกด้านหนึ่ง โดยจะต้องทำการชั่งน้ำหนักของประโยชน์สาธารณะและผลกระทบจากการล่วงละเมิดสิทธิขั้นพื้นฐานอันเป็นสิทธิมนุษยชน ว่าอย่างใดมากกว่ากันเป็นสำคัญ การดำเนินการเพื่อประโยชน์สาธารณะจะต้องเป็นการดำเนินการเพื่อประโยชน์สาธารณะอย่างแท้จริงที่ทำให้คนส่วนใหญ่หรือมหาชนได้รับผลประโยชน์และที่สำคัญการกระทำนั้นจะต้องไม่ได้เป็นการทำลายสาระสำคัญของสิทธิเสรีภาพอันเป็นสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลไปจนเกินสมควร ดุลภาพระหว่างสองสิ่งนี้เป็นสิ่งที่จะต้องคำนึงถึงเสมอ

2.2.3 มาตรการและกลไกในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล

2.2.3.1 มาตรการในการคุ้มครอง

1) มาตรการทางกฎหมาย (State-Regulatory Approach)

(1) บทกฎหมายทั่วไป (Comprehensive Laws)

ในแนวทางนี้เป็นการออกกฎหมายหลักเพียงฉบับเดียวที่ครอบคลุมกรณีการคุ้มครองข้อมูลข่าวสารส่วนบุคคลในลักษณะต่าง ๆ ซึ่งแนวทางการตรากฎหมายเช่นนี้ส่วนใหญ่จะปรากฏอยู่ในประเทศภาคพื้นยุโรป สหราชอาณาจักร และประเทศที่ใช้ระบบประมวลกฎหมาย (Civil Law) ได้แก่ สวีเดน เยอรมัน ฝรั่งเศส เป็นต้น

สำหรับการตรากฎหมายคุ้มครองข้อมูลข่าวสารส่วนบุคคลที่เป็นการทั่วไปนั้น ได้เกิดขึ้นเป็นครั้งแรกในลักษณะที่เป็นกฎหมายระดับมลรัฐ Henssen ซึ่งเป็นรัฐหนึ่งของประเทศเยอรมัน เมื่อปี พ.ศ.1970 ซึ่งถือว่าเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับแรกในโลกหลังจากนั้นได้มีการตรากฎหมายระดับประเทศของเยอรมันขึ้น ในปี ค.ศ.1977 ซึ่งเกิดจากแนวคิดของการออกกฎหมายกลางมาเพื่อคุ้มครองข้อมูลข่าวสารส่วนบุคคลนี้ ก็ได้เป็นต้นแบบให้ประเทศอีกหลายประเทศออกกฎหมายในลักษณะเดียวกันนี้มา เช่น ประเทศสวีเดน ในปี ค.ศ.1973 สหรัฐอเมริกาในปี ค.ศ.1974 และประเทศฝรั่งเศส ในปี ค.ศ.1978 เป็นต้น

อย่างไรก็ตาม ต่อมาภายหลังประเทศต่าง ๆ ในภาคพื้นยุโรปก็ได้มีการบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่มีความสอดคล้องและเป็นไปในทิศทางเดียวกันมากขึ้น เนื่องจากได้มีการพัฒนากรอบนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลในระดับสากลโดยองค์การระหว่างประเทศต่าง ๆ อาทิ การออกแนวปฏิบัติด้านการคุ้มครองความเป็นอยู่ส่วนตัวและการโอนข้อมูลส่วนบุคคลระหว่างประเทศ (Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data) โดยองค์การเพื่อเศรษฐกิจและการพัฒนา (OECD) ในปี ค.ศ.1980 ซึ่งมีวัตถุประสงค์เพื่อให้ข้อเสนอแนะแก่ประเทศสมาชิกในการนำเอาหลักการคุ้มครองข้อมูลส่วนบุคคลดังกล่าวมีทั้งสิ้น 8 ประการ ซึ่งได้กลายเป็นมาตรฐานให้นานาประเทศยึดเป็นหลักเพื่อใช้ในการตรากฎหมายเกี่ยวกับการคุ้มครองข้อมูลข่าวสารส่วนบุคคลขึ้นสำหรับประเทศตน

(2) บทกฎหมายเฉพาะ (Sectoral Laws)

แนวทางนี้จะพบได้ในประเทศสหรัฐอเมริกา ที่แม้จะมีการบังคับใช้กฎหมายคุ้มครองสิทธิส่วนบุคคล (Privacy Act 1974) ซึ่งเป็นกฎหมายหลักคุ้มครองอยู่แล้วก็ตาม แต่

รัฐสภาจะตรากฎหมายเฉพาะออกมาเมื่อ ถึงคราวเกิดปัญหาการป้องกันความลับหรือความเป็นอยู่ส่วนตัวของประชาชนถูกละเมิดขึ้นที่มีลักษณะพิเศษ ก็จะออกกฎหมายเรื่องนั้น ๆ มาแก้ปัญหา เช่น[64]

กรณีการตรากฎหมาย The Driver Privacy Protection Act เนื่องจากว่านักแสดงหญิงชื่อว่า Rebecca Shaeffer ได้ถูกฆาตกรรมที่บ้านของเธอเองเมื่อปี 1988 ซึ่งคนร้ายสามารถสืบหาที่อยู่ของเธอได้โดยการหาข้อมูลจากใบขับขี่ของเธอจาก California Department of Motor Vehicles

กรณีการตรากฎหมายใน The Video Privacy Protection Act เนื่องจากผู้พิพากษา Robert Bork ได้เสนอชื่อให้เป็นผู้ชิงตำแหน่งผู้พิพากษาสูงของสหรัฐอเมริกา และปรากฏว่า มีผู้สื่อข่าวขอและเผยแพร่ข้อมูลการเช่าวีดีโอเทป ของผู้พิพากษาท่านนี้ ปรากกว่ามีรายการวีดีโอเทปเกี่ยวกับหนังโป๊หรือภาพยนตร์ลามกอนาจาร (Pornography) อยู่ด้วย ทำให้มีการวิพากษ์วิจารณ์ถึงความประพฤติของผู้พิพากษาท่านนี้ เป็นเหตุให้ท่านไม่ได้รับการคัดเลือกเป็นผู้พิพากษาศาลสูง

กรณีการตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวกับข้อมูลทางการเงิน เรียกว่า Gramm-Leach-Bliley Financial Modernization Act 1999 เนื่องจากมีบริษัทเอกชนชื่อว่า U.S. Bankcorp ได้เปิดเผยเลขบัญชีของลูกค้าแก่บุคคลภายนอกซึ่งเป็นบุคคลที่สามโดยปราศจากความยินยอมของลูกค้า

นอกเหนือจากกฎหมายสามฉบับที่ยกมาข้างต้นแล้ว ก็ยังมีกฎหมายเฉพาะอื่น ๆ ที่ได้รับการตราขึ้นในสหรัฐอเมริกา เช่น Fair Credit Reporting Act 1970 ซึ่งเป็นกฎหมายที่มีวัตถุประสงค์เพื่อควบคุมการใช้ข้อมูลเครดิตของภาคธุรกิจ โดยการกำหนดหลักเกณฑ์ที่สำคัญ อาทิ ผู้มีสิทธิใช้ข้อมูลเครดิต การจำกัดการเปิดเผยข้อมูลเครดิต ตลอดจนการให้สิทธิแก่ผู้บริโภคในการเข้าถึง หรือแก้ไขข้อมูลเครดิตของตนให้ถูกต้อง กฎหมาย Health Insurance Portability and Accountability Act 1996 ซึ่งตราขึ้นเพื่อคุ้มครองข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวข้องกับการรักษาพยาบาล Children's On line Privacy Protection Act 1998 ซึ่งเป็นกฎหมายที่มีวัตถุประสงค์ห้ามไม่ให้ผู้ประกอบกิจการพาณิชย์อิเล็กทรอนิกส์ และบริการแบบออนไลน์ต่าง ๆ ทำการเก็บรวบรวมข้อมูลจากผู้เยี่ยมชมเวปไซต์หรือผู้ใช้บริการที่เป็นเด็กอายุต่ำกว่า 13 ปี เว้นแต่ผู้ประกอบการที่ได้ใช้กลไกการกำกับดูแลตนเอง ซึ่งได้ผ่านความเห็นชอบจากคณะกรรมาธิการการค้า (FTC) กฎหมาย Financial Modernization act 1999 ซึ่งได้ตราขึ้นเพื่อให้สถาบันการเงินต่าง ๆ เพิ่มระดับการคุ้มครองข้อมูลส่วนบุคคลของผู้บริโภคในกิจกรรมที่เกี่ยวข้องทางการเงินเพิ่มมาก

---

[64] ประสิทธิ์ ปิวาวัฒนาพานิช, “กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกาและประเทศมาเลเซีย,” **วารสารนิติศาสตร์** 43, 4 (ธันวาคม 2557): 537-538.

ขึ้นอาทิ การประกาศนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลให้ลูกค้าทราบ และหน้าที่ในการปฏิบัติตามข้อเรียกร้องของผู้บริโภคที่เกี่ยวกับข้อมูลส่วนบุคคล เป็นต้น

ทั้งนี้แนวคิดของประเทศสหรัฐอเมริกาที่เลือกจะตรากฎหมายคุ้มครองข้อมูลข่าวสารส่วนบุคคลเป็นเรื่อง ๆ นั้น อาจมีเหตุผลจาก ปรัชญาหรือที่มาทางประวัติศาสตร์สร้างชาติของประเทศสหรัฐอเมริกาที่พยายามจะมิให้เจ้าหน้าที่ของรัฐลิดรอนสิทธิเสรีภาพของประชาชน ในขณะเดียวกัน ประชาชนก็มีสิทธิเสรีภาพที่จะดำเนินธุรกิจแบบทุนนิยม หรือ Free enterprise อันเป็นปรัชญาที่ชาวอเมริกันยึดถือมาเป็นเวลานาน ซึ่งโดยทั่วไปแล้วในประเทศสหรัฐอเมริกาไม่มีกฎหมายให้ประชาชนต้องให้ความยินยอมในเรื่องประมวลผลข้อมูล การจัดทำการตลาดและการขายข้อมูลส่วนบุคคลให้กับบุคคลที่สาม ดังนั้น อเมริกาจึงมีบริษัทขนาดใหญ่หลายแห่งที่ทำธุรกิจเกี่ยวกับการจัดเก็บและขายข้อมูลส่วนบุคคลของคนอเมริกัน เช่น บริษัท Catalina Marketing Corporation บริษัท Aristotle Industries บริษัท Winland Service เป็นต้น[65]

นอกจากนั้น ประเทศสหรัฐอเมริกา ยังได้ให้ความสำคัญเกี่ยวกับ Freedom Access มากกว่า Privacy ซึ่งเห็นได้จากบทบัญญัติของกฎหมายหลายฉบับที่รัฐบาลกลางปล่อยให้เอกชนดูแลควบคุมกันเอง ด้วยการให้เอกชนออก Self-Regulations แล้วเจ้าหน้าที่ของรับจะควบคุมอีกทีหนึ่ง เช่น Federal Trade Commission (FTC) ซึ่งการควบคุมกันเองนี้มีข้อดีในเรื่องของความยืดหยุ่นในการสามารถแก้ไขปัญหาได้ทันท่วงทีสอดคล้องกับความเปลี่ยนแปลงด้านเทคโนโลยีที่รวดเร็ว ทั้งนี้ในกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหรัฐอเมริกาหลายฉบับ ยังมีลักษณะพิเศษที่ให้สิทธิเจ้าของข้อมูลที่ถูกละเมิดสามารถดำเนินคดีทางศาลได้อย่างเต็มที่โดยที่ศาลสามารถกำหนดค่าเสียหายในเชิงลงโทษแก่ผู้กระทำละเมิดได้ด้วยซึ่งเรียกว่า Punitive Damages ซึ่งจะเห็นได้ว่า รูปแบบของการตรากฎหมายเพื่อคุ้มครองข้อมูลข่าวสารส่วนบุคคลที่แตกต่างกันนี้ มีเหตุผลที่สามารถวิเคราะห์ได้ว่ามีที่มาจาก แนวคิดพื้นฐานในนิติวิธีที่ต่างกัน โดยประเทศในภาคพื้นยุโรปมองว่า การออกกฎหมายในลักษณะทั่วไปเพียงฉบับเดียว เป็นกฎหมายกลางย่อมจะสามารถปกป้องสิทธิเสรีภาพของประชาชนได้ดีกว่า ขณะที่ในประเทศสหรัฐอเมริกาแม้จะมีกฎหมายหลัก คือ Privacy Act 1974 แต่ก็มีการตรากฎหมายเฉพาะสำหรับการคุ้มครองข้อมูลข่าวสารส่วนบุคคลขึ้นอีกหลายฉบับ ซึ่งมีความเชื่อว่ามีความยืดหยุ่นสอดคล้องกับความเปลี่ยนแปลงในการคุ้มครองข้อมูลส่วนบุคคลในลักษณะต่าง ๆ ที่เกิดขึ้นมาใหม่ตามความเปลี่ยนแปลงของสภาพเศรษฐกิจ สังคม การเมือง และเทคโนโลยีต่าง ๆ[66]

---

[65] *เรื่องเดียวกัน*, หน้า 537-538.

[66] *เรื่องเดียวกัน*, หน้า 537-538.

2) การกำกับดูแลตนเอง (Self-Regulatory Approach)

นอกเหนือจากการคุ้มครองข้อมูลส่วนบุคคลโดยอาศัยกลไกในทางกฎหมายแล้ว ไม่ว่าจะเป็นบทกฎหมายทั่วไป (Comprehensive Laws) หรือ บทกฎหมายเฉพาะ (Sectoral Laws) ยังมีแนวทางที่สามคือ การกำกับดูแลตนเอง ซึ่งมีฐานแนวคิดมาจาก แนวคิด Code ของ Lawrence Lessig มองว่า แนวปฏิบัติที่ดีที่สุดซึ่งจะเป็นเครื่องมืออันมีประสิทธิภาพในการปกครองโดยไม่มีการควบคุมจากรัฐเลย เป็นการควบคุมอุตสาหกรรมโดยบริสุทธิ์ปราศจาการแทรกแซงกำกับดูแลจากภายนอก การกำกับดูแลตนเองนี้เป็นทางเลือกที่ได้รับความนิยมที่สุดในบริบททางด้านการคุ้มครองข้อมูลส่วนบุคคลบนโลกอินเทอร์เน็ต ซึ่งสหรัฐอเมริกายอมรับแนวทางนี้ และอนุญาตให้ภาคเอกชนสามารถปกครองกำกับดูแลกันเองได้ ดังนั้น การกำกับดูแลตนเอง จึงมีลักษณะเป็นการที่กลุ่มผู้ประกอบการ บริษัท หรือปัจเจกชนรวมตัวกันในรูปองค์กรที่มีฐานสมาชิกเพื่อสร้างอำนาจในการควบคุมพฤติกรรมของกันและกัน การเป็นสมาชิกขององค์กรจะต้องเป็นไปด้วยความสมัครใจ และสมาชิกต้องร่วมมือกันสร้างกฎ กติกา มารยาท จรรยาบรรณ หรือข้อกำหนดทางจริยธรรม ตลอดจนแนวทางและมาตรฐานทางเทคโนโลยี ทั้งนี้ สมาชิกมีหน้าที่และความรับผิดชอบโดยตรงในการสอดส่องดูแลและบังคับใช้ให้มีการปฏิบัติตามแนวทางที่ออกร่วมกัน โดยไม่ต้องอาศัยอำนาจตามกฎหมายขององค์กรภาครัฐ แต่ใช้ความสมัครใจและการมีพันธกิจรับผิดชอบร่วมกัน[67]

โดยหากการกำกับดูแลกันเองของผู้ประกอบการ บริษัท รวมถึงผู้ประกอบวิชาชีพที่เกี่ยวข้องกับประมวลผลข้อมูลส่วนบุคคล ไม่ว่าโดยการเก็บรวมรวม ใช้หรือเปิดเผยข้อมูลเกิดขึ้นได้อย่างแท้จริง จะมีส่วนช่วยเป็นอย่างมากในการส่งเสริมการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของบรรดาปัจเจกชนไม่ว่าจะอยู่ในฐานะผู้บริโภค ผู้รับบริการ หรือผู้ที่เกี่ยวข้องกับกิจกรรมทางธุรกิจนั่นเอง ดังนั้น นอกเหนือจากการกำหนดมาตรการกำกับโดยภาครัฐแล้ว ทั้งภาครัฐและเอกชนควรจะร่วมมือกันส่งเสริมให้เกิดการกำกับดูแลกันเองอีกด้วย

2.2.3.2 กลไกในการบังคับใช้กฎหมาย

1) องค์กรที่ทำหน้าที่ในลักษณะกำกับดูแล (Regulatory)

ประเทศที่ได้จัดตั้งองค์กรในลักษณะเช่นนี้ได้แก่ ประเทศสวีเดน และประเทศฝรั่งเศสโดยในกรณีประเทศสวีเดนนั้นก็ได้จัดตั้ง Data Inspection Board and National Commision on Informatics and Liberties ซึ่งมีบทบาทหน้าที่ค่อนข้างกว้างขวางในการกำกับดูแลการประมวลข้อมูลในประเทศ อาทิ อำนาจในการอนุญาตหรือไม่อนุญาตให้มีการประมวลผลข้อมูลทั้งโดยหน่วยงานของรัฐและหน่วยงานภาคเอกชน ส่วนในประเทศฝรั่งเศสก็ได้มีการจัดตั้ง

---

[67] พิรงรอง รามสูต, **การกำกับดูแลเนื้อหาอินเทอร์เน็ต** (กรุงเทพมหานคร: ศูนย์ศึกษานโยบายสื่อ คณะนิเทศศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2556), หน้า 100.

Commission Nationale Informatique Liberte's (CNIL) ซึ่งมีบทบาทหน้าที่ในทำนองเดียวกับประเทศสวีเดน แต่จะแตกต่างกันตรงที่มีการจัดตั้งคณะอนุกรรมการ (Submissions) ขึ้นเพื่อทำหน้าที่ศึกษาวิจัยเกี่ยวกับข้อมูลทางสถิติ (Statistics) การประมวลผลโดยหน่วยงานของรัฐส่วนท้องถิ่น (Local Government) ด้านเทคโนโลยีและการรักษาความปลอดภัย (Technology and Security) ขึ้นเป็นการเฉพาะด้วย อย่างไรก็ตาม การจัดให้องค์กรซึ่งมีโครงสร้างการทำงานที่เป็นอิสระและมีอำนาจหน้าที่กว้างขวางของประเทศสวีเดน และฝรั่งเศสข้างต้น ก็หามีผลให้สามารถคุ้มครองสิทธิความเป็นอยู่ส่วนตัวในข้อมูลส่วนบุคคลของประชาชนได้อย่างมีประสิทธิภาพแต่อย่างใด เนื่องจากมีงบประมาณอย่างจำกัด ในขณะที่มีภาระหน้าที่ซึ่งจะต้องปฏิบัติอยู่เป็นจำนวนมาก ไม่ว่าจะเป็นการรับจดทะเบียนหน่วยงานที่ทำการประมวลผลข้อมูล การไต่สวนข้อร้องเรียน การประชาสัมพันธ์ให้ประชาชนเข้าใจเกี่ยวกับหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคล เป็นต้น[68]

2) องค์กรที่ทำหน้าที่ในลักษณะให้คำปรึกษา (Advisory)

ประเทศที่ได้จัดตั้งองค์กรในลักษณะเช่นนี้ได้แก่ ประเทศเยอรมัน ซึ่งได้มีการจัดตั้งกรรมการคุ้มครองข้อมูลส่วนบุคคล (Federal Data Protection Commissioner) ขึ้นเป็นองค์กรหนึ่งในกระทรวงมหาดไทย (Ministry of the Interior) และอยู่ภายใต้การกำกับดูแลของรัฐมนตรีว่าการกระทรวงมหาดไทย โดยกรรมการคุ้มครองข้อมูลส่วนบุคคลมีบทบาทหน้าที่หลักในการให้คำปรึกษา (Advise) ให้ความช่วยเหลือ (Assist) และว่ากล่าวตักเตือน (Admonish) หน่วยงานต่าง ๆ ในกิจกรรมที่เกี่ยวข้องกับการประมวลผลข้อมูล นอกจากนี้ กรรมการดังกล่าวสามารถยื่นคำร้องเรียนอย่างเป็นทางการ (Formal Complaints) เกี่ยวกับการประมวลผลข้อมูลที่เห็นว่าไม่ถูกต้องไปยังกระทรวงซึ่งมีหน้าที่รับผิดชอบ แต่ไม่มีอำนาจในการออกคำสั่งหรือให้ดำเนินการอย่างหนึ่งอย่างใดโดยอาศัยอำนาจของกรรมการเอง[69]

การจัดองค์กรในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนี้ ไม่ว่ารัฐจะเลือกรูปแบบใด แต่จะเห็นว่าประเด็นสำคัญอยู่ที่การกำหนดให้องค์กรนั้นมีความเป็นอิสระเพื่อดำเนินการบังคับใช้กฎหมายคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลอย่างมีประสิทธิภาพ จะเห็นได้จากตัวอย่างของ การบังคับใช้ General Data Protection Regulation (GDPR) หรือ กฎหมายหลาย ๆ ฉบับของสหภาพยุโรป คือ “การมีองค์กรบังคับใช้กฎหมายที่มีประสิทธิภาพ” เนื่องจากสหภาพยุโรปมีลักษณะเฉพาะประการสำคัญคือให้ความสำคัญกับการบังคับใช้กฎหมายโดยองค์กรของรัฐเพราะถือว่ารัฐมีหน้าที่ต้องปกป้องสิทธิของปัจเจกบุคคล ซึ่งแนวคิดนี้

---

[68] ปฏิวัติ อุ่นเรือน, **ปัญหาการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลระหว่างประเทศ** (สารนิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2547), หน้า 16.

[69] *เรื่องเดียวกัน*, หน้า 17.

ตรงข้ามกับประเทศสหรัฐอเมริกาที่สิทธิของบุคคลได้รับการคุ้มครองผ่านกระบวนการใช้สิทธิเยียวยาทางศาลเป็นหลัก (Private Rights of Action) โดยระบบการพิจารณาแบบกล่าวหา (Adversarial Legal System) โดยจะเห็นว่า GDPR กำหนดเงื่อนไขสำคัญขององค์กรบังคับใช้กฎหมายในรัฐสมาชิกไว้หลายประการเพื่อเป็นหลักประกันของการบังคับใช้กฎหมายอย่างมีประสิทธิภาพ (Article 51-55) โดยเฉพาะการมีคณะกรรมการที่เป็นอิสระและไม่อยู่ภายใต้การครอบงำของบุคคลใด ๆ (Remain Free from External Influence) มีอำนาจหน้าที่ในการไต่สวนและหาข้อเท็จจริงต่าง ๆ เพื่อบังคับให้เป็นไปตามกฎหมาย และต้องไม่กระทำการใด ๆ ที่ขัดหรือแย้งต่อหน้าที่ในการบังคับใช้กฎหมายด้วย และการจะให้กรรมการพ้นจากตำแหน่งได้จะต้องเกิดจากพฤติกรรมที่ไม่เหมาะสมอย่างร้ายแรง (Serious Misconduct) หรือมีคุณสมบัติไม่เป็นไปตามเงื่อนไขของกฎหมายเท่านั้น[70]

ดังนั้น องค์กรที่จะทำหน้าที่สำคัญเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลจึงจำเป็นรัฐจะต้องมีการกำหนดให้องค์กรนั้นมีความเป็นอิสระ ทั้งนี้เพื่อสร้างความเชื่อมั่นและสามารถเป็นหลักประกันที่ได้รับการยอมรับจากประชาชนผู้เป็นเจ้าของสิทธิ รวมถึงนานาอารยะประเทศด้วย

2.3 กรอบสากลว่าด้วยการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล

2.3.1 ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน

เมื่อวันที่ 10 ธันวาคม ค.ศ.1948 ที่ประชุมสมัชชาสหประชาชาติสมัยสามัญ สมัยที่ 3[71] ได้มีข้อมติรับรองปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ซึ่งมีเจตนารมณ์เพื่อรองรับและคุ้มครองสิทธิมนุษยชนของประชาชนทั่วโลกอย่างแท้จริง ปฏิญญาสากลว่าด้วยสิทธิมนุษยชนฉบับนี้ถือว่า เป็นเอกสารที่มีความสำคัญอย่างยิ่งต่อการวางรากฐานด้านสิทธิมนุษยชนระหว่างประเทศอันเป็นมาตรฐานสากลที่ประเทศสมาชิกสหประชาชาติได้ร่วมกันจัดทำขึ้น นอกจากนี้ ยังถือเป็นหลักการพื้นฐานของการตรากฎหมายและการทำข้อตกลงระหว่างประเทศด้านสิทธิมนุษยชนฉบับต่าง ๆ ใน

---

[70] ศุภวัชร์ มาลานนท์, **องค์กรบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล**, ค้นวันที่ 24 ธันวาคม 2562 จาก https://www.kaohoon.com/content/328480?fbclid=IwAR1tk2WV6by81RAy_OV1CMwb_59Z2dRD7iL7CS1EuqQdXLaZ5iL_oKnReog

[71] การประชุมดังกล่าวได้จัดขึ้น ณ กรุงปารีส สาธารณรัฐฝรั่งเศส และปฏิญญาสากลว่าด้วยสิทธิมนุษยชนดังกล่าวได้รบการประกาศในรัฐกิจจานุเบกษาของสาธารณรัฐฝรั่งเศส (Le Journal Officiel) เมื่อวันที่ 19 กุมภาพันธ์ 1949

ระยะเวลาต่อมา โดยเฉพาะอย่างยิ่งอนุสัญญาแห่งยุโรปว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐาน

สิทธิในความเป็นส่วนตัวของบุคคล ได้รับการรับรองและคุ้มครองในฐานะเป็นสิทธิมนุษยชนประการหนึ่ง เป็นครั้งแรกในปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ.1948[72] โดยรับรองและคุ้มครองไว้ในข้อ 12 ความว่า “บุคคลใดจะถูกแทรกแซงตามอำเภอใจในความเป็นส่วนตัว ครอบครัว ที่อยู่อาศัย หรือการสื่อสาร หรือจะถูกลบหลู่เกียรติยศและชื่อเสียงมิได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองของกฎหมายต่อการแทรกแซงสิทธิหรือการลบหลู่ดังกล่าวนั้น”[73]

2.3.2 อนุสัญญายุโรปว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐาน

อนุสัญญาแห่งยุโรปว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานเป็นข้อตกลงที่คณะกรรมาธิการแห่งยุโรปได้จัดทำขึ้นเพื่อใช้บังคับในระหว่างประเทศต่าง ๆ ในสหภาพยุโรป โดยรับแนวความคิดมาจากปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ.1948 ดังที่ได้กล่าวแล้วข้างต้น

อนุสัญญาแห่งยุโรปฉบับนี้ มีเจตนารมณ์เพื่อคุ้มครองและพัฒนาสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานในระหว่างประเทศสมาชิกโดยกำหนดหลักการเบื้องต้นที่มุ่งหมายเพื่อสร้างหลักประกันสิทธิบางประการที่กำหนดไว้ในปฏิญญาสากลว่าด้วยสิทธิมนุษยชนเป็นการเฉพาะ

อนุสัญญาแห่งยุโรปว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐาน ก็ได้รับรองและคุ้มครองสิทธิในความเป็นส่วนตัวของบุคคลไว้โดยชัดแจ้งในข้อ 8 ของอนุสัญญา ความว่า

> 1. บุคคลทุกคนมีสิทธิได้รับการเคารพในชีวิตส่วนตัวและครอบครัว ที่อยู่อาศัยและการสื่อสาร
>
> 2. การแทรกแซงการใช้สิทธิในชีวิตส่วนตัวของบุคคล โดยองค์กรของรัฐจะกระทำได้ก็เฉพาะแต่เมื่อมีกฎหมายบัญญัติให้กระทำได้ และการแทรกแซงดังกล่าวเป็นมาตรการที่จำเป็นในสังคมประชาธิปไตยต่อความปลอดภัยแห่งชาติ

---

[72] ฉบับแปลและเรียบเรียงโดย คณะอนุกรรมการสิทธิมนุษยชนและสันติภาพ องค์การการศึกษา วิทยาศาสตร์ และวัฒนธรรมแห่งสหประชาชาติ (UNESCO) และฉบับแปลและเรียบเรียงโดยกรมองค์การระหว่างประเทศ กระทรวงการต่างประเทศ (กรกฎาคม 2551)

[73] Article 12

No one shall be subjected to arbitrary interference with his privacy family, home or correspondence, nor to attacks upon his honour and reputation, Everyone has the right to the protection of the law against such interference or attacks.

ความมั่นคงของรัฐ ประโยชน์ทางเศรษฐกิจของประเทศ การรักษาความสงบเรียบร้อยและการป้องกันการกระทำความผิดทางอาญา การคุ้มครองสุขภาพหรือจิตใจ หรือการคุ้มครองสิทธิและเสรีภาพของบุคคลอื่น

2.3.3 ข้อบังคับสหภาพยุโรปว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (European Union Directive 95/46/EC) และ General Data Protection Regulation (GDPR: 2016)

ในปี 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” หรือ Directive 95/46/EC ทั้งนี้เพื่อผลักดันให้กฎหมายในกลุ่มประเทศสมาชิกมีความสอดคล้องกันในการให้หลักประกันที่ดีเพียงพอต่อการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของพลเมืองของสหภาพยุโรป และเพื่อทำให้การส่งผ่านข้อมูลส่วนบุคคลภายในประเทศสมาชิกเป็นไปโดยเสรีปราศจากข้อจำกัดที่เกิดจากความแตกต่างกันของกฎหมายหรือกฎเกณฑ์ภายในของประเทศต่าง ๆ

Directive 95/46/EC มีวัตถุประสงค์เพื่อคุ้มครองสิทธิขั้นพื้นฐานและเสรีภาพ ของบุคคลธรรมดาโดยเฉพาะอย่างยิ่งสิทธิในความเป็นอยู่ส่วนตัวอันเนื่องจากการประมวลผลข้อมูลส่วนบุคคลตามที่บัญญัติไว้อย่างชัดเจนในมาตราที่ 1 นอกจากนี้ อารัมภบทที่ 2 ยังได้อธิบายเพิ่มเติมว่า “ระบบประมวลผลข้อมูลนั้นถูกออกแบบมาเพื่ออำนวยประโยชน์แก่มนุษย์ . . . ระบบเหล่านี้ต้องเคารพสิทธิและ เสรีภาพขั้นพื้นฐานของบุคคลธรรมดาโดยไม่เลือกสัญชาติหรือถิ่นที่อยู่ของบุคคลนั้นโดยเฉพาะสิทธิในความเป็นส่วนตัว” และนอกจากนี้ ในอารัมภบทที่ 10 ได้อธิบายว่า “ประมวลกฎหมายภายในประเทศ ว่าด้วยการประมวลข้อมูลส่วนบุคคลมีวัตถุประสงค์เพื่อคุ้มครองสิทธิและเสรีภาพขั้นพื้นฐาน โดยเฉพาะสิทธิในความเป็นส่วนตัว ซึ่งได้รับความเห็นชอบทั้งในมาตราที่ 8 ของอนุสัญญาเพื่อคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานยุโรป และในหลักทั่วไปของกฎหมายประชาคม ด้วยเหตุนั้นการปรับกฎหมายเหล่านี้ให้ สอดคล้องกันจะต้องมิทำให้การคุ้มครองที่พึงได้ของพวกเขานั้นย่อหย่อนลง แต่ในทางกลับกันต้องแสวงหาวิธีที่จะรับรองการคุ้มครองขั้นสูงในประชาคม” ดังนั้นจะเห็นได้ว่า กฎหมายสหภาพยุโรปฉบับนี้มุ่งเน้นให้เกิดความเป็นเอกภาพของกฎหมายคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศในยุโรป[74]

---

[74] คณาธิป ทองวีรวงศ์, **รายงานการวิจัยฉบับสมบูรณ์ เรื่องการปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน**, หน้า 47.

สามารถสรุปสาระสำคัญของหลักเกณฑ์ Directive 95/46/EC ดังกล่าวได้ ดังนี้[75]

1. วัตถุประสงค์
    1) เพื่อให้ประเทศสมาชิกของสหภาพยุโรปมีแนวทางบัญญัติกฎหมายที่สอดคล้องกัน
    2) เพื่อให้มีการส่งผ่านข้อมูลส่วนบุคคลภายในประเทศสมาชิก
2. ขอบเขตการบังคับใช้
    1) การประมวลผลข้อมูลโดยวิธีการปกติ (Manual)
    2) การประมวลผลข้อมูลโดยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอัตโนมัติ (Electronic or Automatic)
3. สาระสำคัญ
    1) การรักษาคุณภาพของข้อมูล
    2) มาตรฐานของการประมวลผลข้อมูลที่ชอบด้วยกฎหมาย
    3) การประมวลผลข้อมูลชนิดพิเศษ
    4) สิทธิในการได้รับแจ้งข้อมูลต่าง ๆ ของเจ้าของข้อมูล
    5) สิทธิในการเข้าถึงข้อมูลของเจ้าของข้อมูล
    6) สิทธิในการคัดค้านการประมวลผลข้อมูลของเจ้าของข้อมูล
    7) การรักษาความปลอดภัยในการประมวลผลข้อมูล
    8) การส่งผ่านข้อมูลส่วนบุคคลไปยังประเทศที่สาม

จากสาระสำคัญที่กล่าวมาข้างต้น จะเห็นได้ว่า Directive 95/46/EC อยู่บนพื้นฐานของหลักการดังต่อไปนี้คือ[76]

1. ข้อมูลส่วนบุคคลต้องถูกประมวลผลอย่างเป็นธรรมและชอบด้วยกฎหมาย
2. ข้อมูลส่วนบุคคลต้องถูกจัดเก็บโดยมีวัตถุประสงค์ที่ชัดเจน แน่นอน และชอบ ด้วยกฎหมาย (Specified, Explicit and Legitimate Purposes) นอกจากนี้ จะต้องไม่มีการประมวลผลของมูลที่ขัดแย้งกับวัตถุประสงค์นั้น เว้นแต่เป็นการประมวลผลข้อมูลที่มีวัตถุประสงค์ทางด้านประวัติศาสตร์ สถิติ หรือวิทยาศาสตร์

---

[75] World Intellectual Propert Organization (WIPO), **European Union Directive 95/46/EC**, Retrieved March 10, 2018 from http://www.wipo.int/wipolex/en/text.jsp?file_id=313007

[76] คณาธิป ทองวีรวงศ์, **รายงานการวิจัยฉบับสมบูรณ์ เรื่องการปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน**, หน้า 47.

3. ข้อมูลส่วนบุคคลต้องมีความเพียงพอ (Adequate) ไม่มากเกินความจำเป็น (Not Excessive) และสอดคล้องกับวัตถุประสงค์ในการจัดเก็บ หรือประมวลผลข้อมูลนั้น

4. ข้อมูลส่วนบุคคลต้องมีความถูกต้องครบถ้วน และในกรณีจำเป็นต้องเป็น ปัจจุบันด้วย

5. ไม่ควรเก็บไว้ในรูปแบบที่สามารถระบุตัวบุคคลผู้เป็นเจ้าของไว้นานเกินไป อีกทั้งต้องใช้มาตรการที่เหมาะสมในการรักษาความปลอดภัยของข้อมูล

6. ข้อมูลชนิดที่มีความอ่อนไหว (Sensitive Data) กฎหมายกำหนดให้เป็นหน้าที่ของผู้ควบคุมการประมวลผลข้อมูลส่วนบุคคลที่ต้องใช้มาตรการทางเทคนิค และการจัดการที่เหมาะสม

นอกจากนี้ สำหรับหลักเกณฑ์เกี่ยวกับการโอนข้อมูลออกไปนอกประเทศสหภาพยุโรปนั้น Directive 95/46/EC ได้วางหลักการไว้ดังนี้คือ เมื่อมีการโอนข้อมูลออกจากประเทศสมาชิกสหภาพยุโรปไปยังประเทศนอกกลุ่ม ซึ่งสามารถจำแนกประเภทการโอนข้อมูลส่วนบุคคลตาม Directive นี้ออกเป็น 2 ประเภท คือ ประเภทแรก การโอนข้อมูลส่วนบุคคลไปยังประเทศที่เป็นสมาชิกของสหภาพยุโรป กรณีนี้สามารถโอนข้อมูลระหว่างกันได้ เช่นเดียวกับการโอนข้อมูลภายในประเทศเดียวกัน เนื่องจากวัตถุประสงค์ของ Directive 95/46/EC ต้องการให้เกิดการถ่ายโอน ข้อมูลส่วนบุคคลภายในกลุ่มประเทศสมาชิกโดยปราศจากอุปสรรคเพื่อส่งเสริมเศรษฐกิจและการค้านั่นเอง และประเภทที่สองคือ การโอนข้อมูลส่วนบุคคลไปยังประเทศนอกสหภาพยุโรป การโอนข้อมูลส่วนบุคคลไปยังประเทศนอกกลุ่มสมาชิกสหภาพยุโรปนั้น มีข้อจำกัดและข้อพิจารณาหลาย ประการ เนื่องจากประเทศเหล่านั้นอาจมีการคุ้มครองข้อมูลส่วนบุคคลในระดับที่ต่ำกว่ามาตรฐานของกฎหมายสหภาพยุโรป ซึ่งหากมีการอนุญาตให้โอนข้อมูลส่วนบุคคลไปยังประเทศที่สามเหล่านั้นได้โดยสะดวกปราศจากข้อจำกัด อาจกระทบสิทธิของเจ้าของข้อมูล ดังนั้นกฎหมายสหภาพยุโรป จึงมีการกำหนดไว้ในมาตรา 25 เพื่อคุ้มครองการโอนข้อมูลส่วนบุคคลไปยังประเทศที่สาม ภายใต้หลักการที่ว่า ประเทศสมาชิกสหภาพยุโรปนั้นจะถ่ายโอนข้อมูลส่วนบุคคลไปยังประเทศที่สาม ได้ก็ต่อเมื่อประเทศที่สามสามารถรับรองระดับการคุ้มครองที่เพียงพอ (Directive 95/46/EC, Article 1) (Adequate Level of Protection) ดังนั้นประเทศสมาชิกสหภาพยุโรปจึงไม่สามารถโอนข้อมูลส่วนบุคคลไปยัง ประเทศที่สามซึ่งมิได้รับรองระดับการคุ้มครองที่เพียงพอเมื่อเปรียบเทียบกับยุโรป[77]

ต่อมาภายหลังจากที่บังคับใช้ Directive 95/46/EC ทางสหภาพยุโรปก็ได้มีการทบทวนและเตรียมการเพื่อปรับปรุงหลักการคุ้มครองข้อมูลส่วนบุคคลตลอดมาเป็นระยะ จนกระทั่งวันที่ 27 พฤษภาคม ค.ศ.2016 ทาง EU Commission ได้ตรากติกาฉบับใหม่และมีการรับรอง General Data Protection Regulation 2016 (Regulation 2016/679) ซึ่งในการร่างกติกาฉบับนี้ใช้เวลาเตรียมการร่างและประชุมปรึกษาหารือกันถึง 4 ปี โดยจะให้มีผลบังคับในวันที่ 25 พฤษภาคม ค.ศ.

---

[77] *เรื่องเดียวกัน*, หน้า 48.

2018 ซึ่งถือเป็นการเปลี่ยนแปลงหลักการครั้งใหญ่ที่สุดในรอบ 20 ปี ทั้งนี้ การกำหนดระยะเวลาในการบังคับใช้ยาวนานถึง 2 ปีนับแต่วันที่กฎหมายผ่านก็เพื่อที่จะให้องค์กรทางธุรกิจต่าง ๆ มีเวลาปรับตัวและเตรียมการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของลูกค้าหรือเจ้าของข้อมูลอย่างถูกต้องตามหลักการอันเป็นมาตรฐานขั้นต่ำใหม่ของ General Data Protection Regulation

สำหรับ General Data Protection Regulation มีหลักการสำคัญดังต่อไปนี้[78]

1. วัตถุประสงค์ของ General Data Protection Regulation

General Data Protection Regulation ถูกกำหนดขึ้นเพื่อให้ประชาชนมีสิทธิควบคุมข้อมูลส่วนบุคคลของตน ซึ่งถือเป็นสิทธิขั้นพื้นฐาน[79] และกำหนดให้สหภาพยุโรปมีมาตรฐานการคุ้มครองข้อมูลที่เป็นอันหนึ่งอันเดียวเพื่อให้เกิดการเคลื่อนย้ายโดยเสรีของข้อมูล[80] กล่าวได้ว่ากฎหมายฉบับนี้ถือเป็นพัฒนาการที่สำคัญยิ่งในอันที่จะเสริมสร้างความแข็งแกร่งให้แก่สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ซึ่งเป็นสิทธิขั้นพื้นฐานของพลเมืองยุคดิจิทัลในปัจจุบัน และยังส่งเสริมและอำนวยความสะดวกแก่ภาคธุรกิจเอกชน โดยทำให้กฎเกณฑ์ต่าง ๆ มีความง่ายขึ้นในทางปฏิบัติสำหรับบริษัทหรือองค์กรธุรกิจที่อยู่ในตลาดร่วมด้านดิจิทัล (digital single market) รวมถึงบริษัทหรือองค์กรธุรกิจอื่น ๆ ที่เกี่ยวข้องอีกด้วย

2. ขอบเขตการบังคับใช้ของ General Data Protection Regulation

มาตรการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนั้น ยังคงบังคับใช้แก่การประมวลผลเช่นเดิม แต่มีขยายขอบเขตการบังคับ (Territorial Scope) โดยกำหนดให้กติกาจะมีผลบังคับต่อบุคคลดังต่อไปนี้

1) ประชาชนและธุรกิจที่จัดตั้งในสหภาพยุโรป ได้รับการคุ้มครองข้อมูลส่วนบุคคลภายใต้กฎหมายนี้ ไม่ว่าการประมวลผลข้อมูลนั้นจะเกิดขึ้นสหภาพยุโรป หรือนอกสหภาพยุโรป เช่นนี้

---

[78] EU, **An Overview of The Main Change Under GDPR And How They Differ from the Previous Directive**, Retrieved March 11, 2018 from https://www.eugdpr.org/key-changes.html

[79] GDPR Preamble (1): “The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8 (1) of the Charter of Fundamental Rights of the European Union ...provide that everyone has the right to protection of personal data concerning him or her.”

[80] GDPR Preamble (3): “. . . harmonisethe protection of fundamental rights and freedom to ensure the free flow of personal data between Member States”

กล่าวได้ว่า แม้ General Data Protection Regulation จะเป็นกฎหมายของสหภาพยุโรป ก็ตาม แต่สภาพบังคับของ General Data Protection Regulation ไม่ได้จำกัดอยู่แค่ภายในสหภาพยุโรป เท่านั้น โดยหากพิจารณาจาก Article 3 ซึ่งเป็นบทบัญญัติที่กำหนดขอบเขตการบังคับใช้เชิงพื้นที่ของ General Data Protection Regulation จะเห็นว่ากฎหมายฉบับนี้จะใช้บังคับกับกรณีต่อไปนี้

(1) การประมวลผลข้อมูลส่วนบุคคลที่อยู่ในบริบทของกิจกรรมของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่ในสหภาพยุโรป ไม่ว่าการประมวลผลดังกล่าว จะเกิดขึ้นในสหภาพยุโรปหรือไม่ (Article. 3 ข้อ 1.) และ

(2) การประมวลผลข้อมูลส่วนบุคคลที่กระทำโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือ ผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่นอกสหภาพยุโรป แต่เจ้าของข้อมูลส่วนบุคคลที่ข้อมูลของตน ถูกประมวลผลนั้นอยู่ในสหภาพยุโรป และการประมวลผลนั้นเป็นการเสนอสินค้าหรือบริการ โดยมิพักต้องคำนึงว่าจะมีการชำระราคากันหรือไม่ หรือเป็นการเฝ้าสังเกตพฤติกรรมของเจ้าของข้อมูลที่เกิดขึ้นในสหภาพยุโรป (Article. 3 ข้อ 2.)

(3) นอกจากนี้ General Data Protection Regulation ยังใช้บังคับกับการประมวลผลข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ไม่ได้ตั้งอยู่ในสหภาพยุโรป แต่อยู่ในสถานที่ซึ่งกฎหมายของประเทศสมาชิกจะต้องนำมาใช้ด้วยโดยผลของกฎหมายมหาชนระหว่างประเทศ (Article. 3 ข้อ 3.)

2) ข้อมูลส่วนบุคคลจะโอนไปยังผู้ประกอบการนอกสหภาพ ยุโรปได้ก็ต่อเมื่อประเทศปลายทางมีระดับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลเทียบเท่าสหภาพยุโรป

3) หากผู้ประมวลผลข้อมูลนอกยุโรปให้บริการหรือขายสินค้าให้กับผู้บริโภคชาว ยุโรป หรือ “มีการสังเกตพฤติกรรม” ของชาวยุโรป ผู้ประกอบการนั้นจะต้องตกอยู่ภายใต้บังคับของกฎหมายฉบับนี้ด้วย

อย่างไรก็ดี แม้ General Data Protection Regulation จะมีขอบเขตการบังคับใช้ขยายออกไปนอกพื้นที่สหภาพยุโรป และมีการกำหนดโทษปรับทางปกครองที่มีโทษสูงสุดเป็นจำนวนที่สูงมาก แต่สำหรับบุคคลธรรมดา ที่ใช้ข้อมูลส่วนบุคคลตามปกติชีวิตประจำวันก็ไม่จำต้องเป็นกังวลกับการปฏิบัติตาม General Data Protection Regulation แต่อย่างใด เนื่องจากกฎหมายนี้ไม่นำมาใช้กับการประมวลผลข้อมูลส่วนบุคคลที่กระทำโดยบุคคลธรรมดาที่เป็น กิจกรรมส่วนตัวหรือเป็นกิจกรรมภายในครัวเรือนโดยแท้ ซึ่งกิจกรรมดังกล่าวอาจรวมไปถึงการ ติดต่อกันทางจดหมาย การเก็บข้อมูลที่อยู่ หรือการใช้โซเชียลเนทเวิร์คและกิจกรรมออนไลน์ต่าง ๆ ที่อยู่ในบริบทของกิจกรรมดังกล่าว นอกจากนี้ General Data Protection Regulation ยังไม่นำมาบังคับใช้กับการดำเนินการโดย เจ้าหน้าที่ของรัฐซึ่งมีอำนาจหน้าที่เพื่อการป้องกัน สอบสวน (Investigation) สืบสวน (Detection)

การดำเนินคดีอาญา การบังคับใช้โทษอาญา รวมทั้งการป้องกันภัยคุกคามต่อความปลอดภัยสาธารณะอีกด้วย (Article. 2)

3. สาระสำคัญในภาพรวมของ General Data Protection Regulation

หากกล่าวถึงภาพรวมของ General Data Protection Regulation ในเบื้องต้นอาจกล่าวได้ว่า General Data Protection Regulation เป็นกฎหมายที่คุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ของบุคคลธรรดาเกี่ยวกับการที่ข้อมูลส่วนบุคคลของเขาจะถูกประมวลผล ทั้งนี้ หากพิจารณาจาก General Data Protection Regulation ทั้งฉบับแล้ว จะพบว่ากฎหมายนี้มีเนื้อหาค่อนข้างยาว ในส่วนของบทนำ (Recital) ก่อนที่จะถึงบทบัญญัติก็มีจำนวนถึง 173 ข้อ สำหรับในส่วนบทบัญญัติของ General Data Protection Regulation เองก็มีจำนวนถึง 99 มาตรา แบ่งออกเป็น 11 หมวด โดยมีการกำหนดเนื้อหาในส่วนต่าง ๆ ที่สำคัญ เช่น

หมวด 2 หลักการทั่วไป เป็นการกำหนดเรื่องต่าง ๆ เช่น หลักการในการประมวลผล ข้อมูลส่วนบุคคล (Article. 5) หลักการประมวลผลที่ชอบด้วยกฎหมาย (Article. 6) เงื่อนไขในการขอความยินยอม (Article. 7) การประมวลผลข้อมูลส่วนบุคคลที่มี ลักษณะพิเศษ (Article. 9) เป็นต้น

หมวด 3 สิทธิของเจ้าของข้อมูลส่วนบุคคล ซึ่งกำหนดสิทธิต่าง ๆ ของเจ้าของ ข้อมูลส่วนบุคคลเอาไว้ เช่น สิทธิที่จะลบ (หรือสิทธิที่จะถูกลืม) (Right to Erasure (Right to be Forgotten)) (Article. 17) หรือสิทธิที่จะโอนย้ายข้อมูล (Data Portability) (Article. 18) เป็นต้น

หมวด 4 ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งกำหนดเรื่องต่าง ๆ เกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผล ข้อมูลส่วนบุคคล เช่น ภาระหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลและ ผู้ประมวลผลข้อมูลส่วนบุคคล (Section 1) ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (Section 2) การประเมินผลกระทบต่อความเป็นส่วนตัว (Section 3) หรือการจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) (Section 4) เป็นต้น

หมวด 5 การโอนข้อมูลส่วนบุคคลไปยังประเทศที่สามหรือองค์การระหว่าง ประเทศ ซึ่งกำหนดหลักเกณฑ์เกี่ยวกับการโอนข้อมูลส่วนบุคคลข้ามดินแดนออกไปนอกสหภาพยุโรปว่าจะสามารถทำได้ในกรณีใดบ้าง และภายใต้เงื่อนไข อย่างไร

หมวด 6 หน่วยงานอิสระที่ทำหน้าที่กำกับดูแล (Independent Supervisory Authorities) หรือ

หมวด 8 การเยียวยา ความรับผิด และโทษ (Remedies, Liability and Penalties) เป็นต้น

ที่กล่าวมาข้างต้นเป็นเพียงบางหมวดของ General Data Protection Regulation เท่านั้น และเนื่องจากเนื้อหาของ General Data Protection Regulation นั้นมีรายละเอียดจำนวนมาก ในส่วนนี้จึงจะกล่าวถึงเนื้อหาสำคัญเพียงบางเรื่อง ซึ่งได้แก่ (1) นิยามศัพท์ที่สำคัญ (2) หลักการในการ

ประมวลผลข้อมูลส่วนบุคคล (3) หลักการประมวลผลที่ชอบด้วยกฎหมาย (4) สิทธิของเจ้าของข้อมูลส่วนบุคคล และ (5) การโอนข้อมูลไปยังประเทศที่สาม

ทั้งนี้ นอกจากเรื่องต่าง ๆ เหล่านี้แล้ว General Data Protection Regulation ก็ยังกำหนดหลักเกณฑ์ในเรื่องอื่น ๆ ที่มีความสำคัญเช่นเดียวกัน เช่น การประมวลผลข้อมูลส่วนบุคคลที่มีลักษณะพิเศษเฉพาะซึ่งการประมวลผลข้อมูลเหล่านี้จะมีหลักเกณฑ์เพิ่มเติม หรือการจัดตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) ในองค์กรเพื่อทำหน้าที่ต่าง ๆ เช่น ดูแลการดำเนินการขององค์กร นั้นให้สอดคล้องกับ General Data Protection Regulation โดยมีบทบาทในการช่วยเหลือผู้ควบคุมข้อมูลส่วนบุคคลในการประเมินความเสี่ยงผลกระทบต่อข้อมูลส่วนบุคคล (Data Protection Impact Assessment) หรือให้ความร่วมมือและประสานงานกับหน่วยงานผู้กำกับดูแล เป็นต้น ซึ่งผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลบางประเภท เช่น หน่วยงานของรัฐ (Public Authorities) องค์กรที่มีกิจกรรมหลักเป็นการเฝ้าติดตามพฤติกรรมของบุคคลเป็นจำนวนมากอย่างเป็นระบบ หรือองค์กรที่ทำการประมวลผลข้อมูลส่วนบุคคลที่มีลักษณะพิเศษเป็นจำนวนมาก จะต้องจัดตั้งให้มีเจ้าหน้าที่คุ้มครองข้อมูล หรือ DPO ขึ้นในองค์กรของตนด้วย เป็นต้น[81]

4. นิยามศัพท์ที่สำคัญ

บทนิยามของ General Data Protection Regulation ปรากฏอยู่ใน Article 4 ซึ่งมีการกำหนดนิยามไว้จำนวนมากถึง 26 คำ ในส่วนนี้จึงจะกล่าวถึงแต่เพียงความหมายของนิยามศัพท์สำคัญเกี่ยวกับการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลเท่านั้น ซึ่งได้แก่

1) ข้อมูลส่วนบุคคล (Personal Data)

ตามบทบัญญัติของ Article 4 (1) ได้ให้ความหมายของ “ข้อมูลส่วนบุคคล” เอาไว้ว่าได้แก่ ข้อมูลใด ๆ ก็ตามที่เกี่ยวข้องกับบุคคลธรรมดาที่ระบุตัว หรืออาจถูกระบุตัวบุคคลผู้นั้นได้ ซึ่งการที่ข้อมูลนั้น “อาจระบุตัวบุคคลได้” จะเป็นโดยทางตรงหรือทางอ้อมก็ได้ โดยอาศัยสิ่งบ่งชี้ (Identifier) ต่าง ๆ ซึ่งอาจเป็น ชื่อ หมายเลขประจำตัวประชาชน ที่อยู่ เอกลักษณ์ออนไลน์ (Online Identifier) หรือเอกลักษณ์ทางร่างกายอย่างใดอย่างหนึ่ง ลักษณะทางกายภาพ พันธุกรรม จิตใจ เศรษฐกิจ วัฒนธรรม หรือสังคมของบุคคล นั้น เป็นต้น

การที่จะพิจารณาว่าข้อมูลนั้นสามารถบ่งชี้หรือระบุตัวบุคคลได้หรือไม่ จะต้องพิจารณาว่าข้อมูลดังกล่าวทำให้สามารถบรรยายถึงบุคคลนั้นในประการที่จะแบ่งแยกบุคคลนั้น ออกจากบุคคลอื่น ๆ และสามารถจดจำบุคคลนั้นในฐานะปัจเจกบุคคลได้หรือไม่ ตัวอย่างที่สำคัญของ สิ่งบ่งชี้อย่าง

---

[81] Article 29 Data Protection Working Party, Guidelines on Data Protection Officers (DPO), p. 4.

หนึ่งคือชื่อของบุคคล ซึ่งชื่อนั้นเป็นสิ่งที่สามารถระบุตัวบุคคลได้โดยตรง[82] นอกจากนี้ หมายเลข IP Address หรือการใช้คุกกี้บนเว็บไซต์ (ข้อมูลขนาดเล็กบนเว็บไซต์ที่ส่งเข้ามาเก็บไว้ในเครื่องคอมพิวเตอร์ของผู้ที่เข้าชมเว็บไซต์นั้น) ก็เป็นสิ่งที่สามารถบ่งชี้ตัวบุคคลได้เช่นเดียวกัน[83] แต่สำหรับข้อมูลที่ไม่ระบุชื่อเจ้าของข้อมูล (Anonymous Information) ซึ่งเป็นข้อมูลที่ไม่เกี่ยวข้องกับบุคคลที่ถูกระบุตัวหรือที่อาจระบุตัวบุคคลได้ หรือข้อมูลไม่ระบุชื่อที่ไม่สามารถระบุตัวเจ้าของข้อมูลได้อีกต่อไป ก็จะไม่อยู่ภายใต้ของหลักการตามกฎหมายนี้ นอกจากนี้ กฎหมายนี้ยังไม่นำมาใช้ บังคับกับข้อมูลของบุคคลที่ถึงแก่กรรมแล้วด้วย

2) การประมวลผล (Processing)

การกำหนดนิยามของคำว่า การประมวลผล ปรากฏอยู่ใน Article 4 (2) โดยได้กำหนดความหมายไว้ให้มีลักษณะของมีขอบเขตที่กว้างมาก โดยหมายความว่า การดำเนินการหรือชุดของการดำเนินการที่ทำต่อข้อมูลส่วนบุคคลหรือชุดของข้อมูลส่วนบุคคล ทั้งนี้ ไม่ว่าการดำเนินการดังกล่าวจะอาศัยวิธีการอัตโนมัติ (Automated Mean) หรือวิธีการไม่อัตโนมัติ (Manual) ก็ตาม เช่น การเก็บ รวบรวม บันทึก จัดกลุ่ม จัดวางโครงสร้าง เก็บ ปรับปรุงหรือเปลี่ยนแปลง การกู้คืน ค้นหา (Consultation) ใช้ เปิดเผยโดยการโอน (Disclosure by Transmission) เผยแพร่หรือทำให้เข้าถึงได้ จัดเรียงหรือควบรวม (Alignment or Combination) จำกัด (Restriction) ลบ (Erasure) หรือทำลาย (Destruction) เป็นต้น ซึ่งหากพิจารณาจากนิยามนี้แล้ว กรณีที่บริษัทได้ทำการเก็บรวบรวมข้อมูลต่าง ๆ ของลูกค้า เช่น ชื่อ เพศ อายุ และรายการสินค้าที่เคยสั่งซื้อไว้ในระบบคอมพิวเตอร์ และนำข้อมูลดังกล่าวมาจัดกลุ่มลูกค้าตาม ความสนใจในสินค้าแต่ละประเภท ก็ถือได้ว่าบริษัทนั้นทำการประมวลผลข้อมูลส่วนบุคคลแล้ว

3) ผู้ควบคุมข้อมูลส่วนบุคคล (Controller) และผู้ประมวลผลข้อมูลส่วนบุคคล (Processor)

การพิจารณาว่าผู้ใดเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้นมีความสำคัญ เนื่องจากบุคคลดังกล่าวจะต้องมีหน้าที่ตาม General Data Protection Regulation

---

[82] European Union Agency for Fundamental Rights (FRA), **Handbook on European Data Protection Law**, p. 89, Retrieved December 12, 2018 from https://www.coe.int/en/web/data-protection/-/the-new-handbook-on-european-data-protection-law-is-out-get-your-copy-

[83] Information Commissioner's Office (ICO), **Guide to the General Data Protection Regulation (GDPR)**, p. 11, Retrieved March 1, 2019 from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

ที่ต้องปฏิบัติแตกต่างกัน เช่น ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่จะต้องเก็บบันทึกกิจกรรมการประมวลผล ข้อมูลของตนเพื่อแสดงว่าตนได้ปฏิบัติตามหน้าที่ที่กำหนดใน General Data Protection Regulation แล้ว (Article 30 (2)) เป็นต้น

ทั้งนี้ Article 4 (7) ได้กำหนดความหมายของ “ผู้ควบคุมข้อมูลส่วนบุคคล” เอาไว้ว่า หมายความถึง ผู้ที่ทำการตัดสินใจเกี่ยวกับวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคล โดยจะเป็นบุคคลธรรมดาหรือนิติบุคคลก็ได้ และอาจเป็นหน่วยงานของรัฐ (Public Authority) เจ้าหน้าที่ (Agency) หรือองค์กรอื่น ๆ (Other Body) ก็ได้

ในขณะที่ “ผู้ประมวลผลข้อมูลส่วนบุคคล” มีการกำหนดความหมายเอาไว้ใน Article 4 (8) ว่าหมายถึง บุคคลธรรมดา หรือนิติบุคคลหน่วยงานของรัฐ (Public Authority) เจ้าหน้าที่ (Agency) หรือองค์กรอื่น ๆ (Other Body) ที่ทำการประมวลผลข้อมูลส่วนบุคคลในนามของผู้ควบคุมข้อมูลส่วนบุคคล (On Behalf of the Controller)

จากนิยามดังกล่าว เราอาจกล่าวได้ว่าผู้ควบคุมข้อมูลส่วนบุคคลจะเป็นผู้ที่ตัดสินใจ ว่าเพราะเหตุใดจึงต้องทำการประมวลผลข้อมูลส่วนบุคคลและจะทำการประมวลผลด้วยวิธีการอย่างไร ในขณะที่ผู้ประมวลผลข้อมูลส่วนบุคคลก็จะเป็นผู้ที่ประมวลผลตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล

5. หลักการในการประมวลผลตาม General Data Protection Regulation

ใน Article 5 ของ General Data Protection Regulation ได้กำหนดหลักการเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลไว้หลายประการ ซึ่งหลักการดังกล่าวได้แก่

1) หลักความชอบด้วยกฎหมาย เป็นธรรม และโปร่งใส (Lawfulness, Fairness And Transparency) กล่าวคือ การประมวลผลข้อมูลส่วนบุคคลจะต้องเป็นไปโดยชอบด้วย กฎหมายอย่างเป็นธรรม และในประการที่โปร่งใส (Article 5 1. (A)) ซึ่งการประมวลผลอย่างไรที่จะถือได้ ว่าชอบด้วยกฎหมาย เป็นธรรม และโปร่งใส ก็จะต้องพิจารณาจากบทบัญญัติอื่น ๆ ของ General Data Protection Regulation ต่อไป

2) หลักข้อจำกัดตามวัตถุประสงค์ (Purpose Limitation) กล่าวคือ การเก็บ รวบรวมข้อมูลส่วนบุคคลต้องเป็นไปเพื่อวัตถุประสงค์ที่เฉพาะเจาะจง แจ้งชัด และชอบด้วยกฎหมาย และข้อมูลดังกล่าวจะไม่ถูกนำไปประมวลผลในวัตถุประสงค์ที่แตกต่างจากวัตถุประสงค์ข้างต้น (Article. 5 1. (B))

3) หลักการใช้ข้อมูลให้น้อยที่สุด (Data Minimalisation) กล่าวคือ ข้อมูลส่วนบุคคลนั้นจะมีได้เท่าที่เพียงพอ (Adequate) เกี่ยวข้อง และจำกัดเฉพาะสิ่งที่จำเป็นตาม วัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลเท่านั้น (Article 5 1. (C))

4) หลักความถูกต้อง (Accuracy) กล่าวคือ ข้อมูลส่วนบุคคลนั้นจะต้อง ถูกต้อง และในกรณีที่จำเป็นก็จะต้องทำให้เป็นปัจจุบัน ทั้งนี้ จะต้องมีการใช้วิธีการตามสมควรเพื่อให้ มั่นใจว่าข้อมูลส่วนบุคคลที่ไม่ถูกต้องตรงตามวัตถุประสงค์ของการประมวลผลจะถูกลบหรือได้รับการ แก้ไขให้ถูกต้องโดยไม่ชักช้า (Article 5 1. (D))

5) หลักการเก็บข้อมูลอย่างจำกัด (Storage Limitation) กล่าวคือ การเก็บข้อมูล ส่วนบุคคลในรูปแบบที่สามารถบ่งชี้ตัวเจ้าของข้อมูลได้นั้น จะเก็บได้ไม่นานเกินกว่าที่จำเป็นเพื่อวัตถุประสงค์ในการประมวลผล (เว้นแต่กรณีที่เป็นไปเพื่อประโยชน์สาธารณะ ทางวิทยาศาสตร์ การวิจัยทางประวัติศาสตร์ หรือในเชิงสถิติ ตาม Article 89 (1) ซึ่งมีรายละเอียดอีกสำหรับข้อยกเว้นเหล่านี้) (Article 5 1. (e))

6) หลักความเชื่อถือได้และการรักษาความลับ (Integrity and Confidentiality) กล่าวคือ ในการประมวลผลข้อมูลส่วนบุคคลจะต้องมีการรักษาความมั่นคงปลอดภัยของข้อมูลที่เหมาะสมจะต้องป้องกันข้อมูลดังกล่าวจากการประมวลผลโดยปราศจากอำนาจหรือโดยไม่ชอบด้วยกฎหมาย และป้องกันข้อมูลจากการสูญหาย ทำลาย หรือเกิดความเสียหายโดยอุบัติเหตุ โดยใช้เทคนิคหรือ กระบวนการจัดข้อมูลที่เหมาะสม (Article 5 1. (f))

7) หลักความรับผิดชอบ (Accountability) กล่าวคือ ผู้ควบคุมข้อมูลส่วน บุคคลมีภาระความรับผิดชอบที่จะต้องแสดงให้เห็นว่าตนสามารถปฏิบัติตามหลักการตามข้อ 1) ถึง 6) ที่ได้กล่าวมาข้างต้นได้ (Article 5 2.)

ทั้งนี้ หลักการเหล่านี้ที่สะท้อนถึงเจตนารมณ์ของการคุ้มครองข้อมูลส่วน บุคคลมากกว่าที่จะเป็นการวางกฎเกณฑ์ที่ชัดเจนตายตัวเอาไว้ ซึ่งการปฏิบัติให้เป็นไปตามหลักการ เหล่านี้จะเป็นพื้นฐานสำคัญสำหรับการสร้างแนวทางปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลที่ดีต่อไป[84]

6. หลักการประมวลผลข้อมูลส่วนบุคคลที่ชอบด้วยกฎหมาย

ตามที่ได้กล่าวไว้แล้วข้างต้นว่า General Data Protection Regulation ได้วางหลักการที่สำคัญสำหรับการประมวลผลข้อมูลส่วนบุคคลเอาไว้ ซึ่งหลักการที่สำคัญประการหนึ่งก็คือ การประมวลผลข้อมูลส่วนบุคคลจะต้องเป็นไปโดยชอบด้วยกฎหมาย (Article 5 1. (a)) ซึ่งปัญหาที่ต้องพิจารณาต่อมา ก็คือ การประมวลผลข้อมูลส่วนบุคคลกรณีใดบ้างที่จะถือว่าสามารถทำได้โดยชอบด้วยกฎหมาย กรณีเช่นนี้ มีการกำหนดเอาไว้ใน Article 6 ซึ่งได้วางหลักการอันเป็นฐานที่ทำให้การประมวลผลข้อมูลส่วนบุคคลชอบด้วยกฎหมายเอาไว้ ดังนั้น ในกรณีที่จะทำการประมวลผลข้อมูลส่วนบุคคลก็จะต้องพิจารณาด้วยว่าการประมวลผลนั้นมีหลักการอันเป็นฐานรองรับตามบทบัญญัตินี้หรือไม่ ไม่เช่นนั้นแล้วการประมวลผลข้อมูลส่วนบุคคลดังกล่าวก็อาจมีผลเป็นการละเมิดต่อหลักการ

---

[84] *Ibid.,* p. 17.

ของ General Data Protection Regulation และนำไปสู่บทบังคับตาม General Data Protection Regulation ได้ ทั้งนี้ ฐานที่ทำให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปโดยชอบด้วยกฎหมายตาม Article 6 ได้แก่

1) ฐานจากความยินยอม กล่าวคือ เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอม สำหรับการประมวลผลข้อมูลส่วนบุคคลของตนเพื่อวัตถุประสงค์ใดวัตถุประสงค์หนึ่งหรือหลาย วัตถุประสงค์ ซึ่งความยินยอมตาม General Data Protection Regulation นั้น หมายความถึงการใด ๆ ที่แสดงถึงความประสงค์ของ เจ้าของข้อมูลส่วนบุคคล ไม่ว่าจะในลักษณะของถ้อยคำแถลง (Statement) หรือเป็นการกระทำที่แสดงการยืนยันอย่างแจ้งชัด (Clear Affirmative Action) ว่าเห็นชอบกับการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวกับตน ซึ่งการให้ความยินยอมนั้นจะต้องเป็นการให้โดยเสรี (Freely Given) อย่างเฉพาะเจาะจง (Specific) ต้องได้รับทราบข้อมูลที่ถูกต้องครบถ้วน (Informed) และไม่คลุมเครือ (Unambiguous) (Article 4 (11))

สำหรับรูปแบบของการให้ความยินยอมนั้น อาจเป็นลายลักษณ์อักษรซึ่งรวมทั้งวิธีการทางอิเล็กทรอนิกส์ หรืออาจเป็นการให้ความยินยอมด้วยถ้อยคำวาจาก็ได้ อย่างไรก็ดี General Data Protection Regulation ไม่ยอมรับวิธีการขอความยินยอมไว้ล่วงหน้าโดยการใช้ช่องให้มีการกาเครื่องหมายให้ความยินยอมเอาไว้ก่อน (Pre-Ticked Opt-In Boxes)

กล่าวโดยสรุปก็คือ การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล จะต้องเป็นไปตามหลักเกณฑ์ทั้ง 4 ข้อ ต่อไปนี้คือ

ประการแรก เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมอย่างเสรี (Freely Given) หมายถึง เจ้าของข้อมูลมีทางเลือกในการตัดสินใจว่าจะให้หรือไม่ให้ข้อมูลส่วนใดบ้าง และการไม่ให้ความยินยอมในส่วนนั้นต้องไม่ทำให้เกิดผลเสียแก่เจ้าของข้อมูลส่วนบุคคล

ประการที่สอง มีวัตถุประสงค์ที่เฉพาะเจาะจงในการขอความยินยอม (Specific) หมายถึง การประมวลผลข้อมูลนต้องเป็นไปเพื่อวัตถุประสงค์ที่แจ้งเจ้าของข้อมูลส่วนบุคคลเท่านั้น

ประการที่สาม แจ้งการประมวลผลข้อมูลให้เจ้าของข้อมูลส่วนบุคคลทราบ (Informed) หมายถึง เจ้าของข้อมูลส่วนบุคคลต้องทราบแล้วว่าจะมีการประมวลผลนั้น ๆ ก่อนให้ความยินยอม

ประการสุดท้าย เจ้าของข้อมูลต้องแสดงความยินยอมอย่างไม่กำกวม (Unambiguous) หรือ เป็นการแสดงออกโดยชัดเจน ต้องปราศจากความลังเลสงสัยในการตีความว่าเป็นการกระทำของเจ้าของข้อมูลหรือไม่ เช่น การกดอัปโหลดภาพบัตรประจำตัวประชาชน การลงลายมือชื่ออิเล็กทรอนิกส์

นอกจากนี้ สำหรับกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ General Data Protection Regulation ได้กำหนดกรณีให้การเสนอบริการที่จัดให้มีขึ้นเพื่อประโยชน์ตอบแทนโดยอาศัยอุปกรณ์ทางอิเล็กทรอนิกส์ (Information Society Services) โดยตรงต่อผู้เยาว์ การประมวลผล

ข้อมูลส่วนบุคคลกรณีนี้จะชอบด้วยกฎหมายก็ต่อเมื่อผู้เยาว์มีอายุอย่างน้อย 16 ปี และหากผู้เยาว์มีอายุต่ำกว่านั้น การให้ความยินยอมของผู้เยาว์จะต้องได้รับการให้ความเห็นชอบโดยผู้มีอำนาจปกครองด้วย (Article 8 1.) อนึ่ง กำหนดอายุ 16 ปีดังกล่าว General Data Protection Regulation ได้เปิดช่องให้ประเทศสมาชิกสามารถเลือกกำหนดอายุขั้นต่ำของเด็กในกรณีนี้ได้เอง แต่จะต้องไม่ต่ำกว่า 13 ปี

2) ฐานจากสัญญา กล่าวคือ หากการประมวลผลนั้นมีความเป็นจำเป็นแก่การปฏิบัติตามสัญญาที่เจ้าของข้อมูลส่วนบุคคลเข้าเป็นคู่สัญญาอยู่ด้วย หรือเพื่อที่จะดำเนินการให้เป็นไปตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนการเข้าทำสัญญา ก็จะทำให้การประมวลผลนั้นชอบด้วยกฎหมาย

3) ฐานจากหน้าที่ตามกฎหมาย กล่าวคือ ถ้าหากการประมวลผลข้อมูลส่วนบุคคลนั้น มีความจำเป็นในการปฏิบัติหน้าที่ตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งฐานแห่งการประมวลผลในข้อนี้ ไม่ได้หมายความว่าจะต้องมีกฎหมายที่กำหนดโดยเฉพาะเจาะจงให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำ การประมวลผล เพียงแค่ผู้ควบคุมข้อมูลส่วนบุคคลมีวัตถุประสงค์ในภาพรวมที่จะต้องปฏิบัติให้เป็นไป ตามหน้าที่ตามกฎหมายก็ถือได้ว่าสามารถอาศัยฐานในข้อนี้ได้แล้ว เช่น หากมีกฎหมายกำหนดหน้าที่ ให้สถาบันการเงินต้องรายงานต่อพนักงานเจ้าหน้าที่เมื่อพบเหตุต้องสงสัยว่ามีบุคคลกระทำการอันเป็นการฟอกเงินเ ช่นนี้ก็ถือได้ว่าเป็นการปฏิบัติหน้าที่ตามกฎหมายแล้ว

4) ฐานจากการคุ้มครองชีวิต (Vital Interests) กล่าวคือ ถ้าหากการประมวลผลข้อมูลส่วนบุคคลนั้นจำเป็นสำหรับการปกป้องชีวิตของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่น เช่น กรณีที่มีบุคคลผู้ประสบอุบัติเหตุทางรถยนต์ซึ่งอาจถึงขั้นเสียชีวิตได้ และโรงพยาบาลมีความจำเป็นที่จะต้องเปิดเผยประวัติทางการแพทย์ของบุคคลนั้นเพื่อรักษาชีวิตของบุคคลนั้น เป็นต้น

5) ฐานจากหน้าที่ต่อสาธารณะ กล่าวคือ การประมวลผลนั้นจำเป็นสำหรับการปฏิบัติงานเพื่อประโยชน์สาธารณะ หรือเป็นการใช้อำนาจรัฐของผู้ควบคุมข้อมูลส่วนบุคคล

6) ฐานจากประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest) กล่าวคือ การประมวลผลนั้นเป็นการจำเป็นเพื่อให้ได้มาซึ่งประโยชน์โดยชอบด้วยกฎหมาย ซึ่งประโยชน์ดังกล่าวอาจเป็นของผู้ควบคุมข้อมูลส่วนบุคคลหรือบุคคลที่สามก็ได้ แต่ประโยชน์ดังกล่าวจะต้องไม่ถูกกลบกลืน (Overridden) โดยประโยชน์หรือสิทธิและเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคลที่จำเป็นต้องได้รับการคุ้มครองข้อมูลส่วนบุคคล ทั้งนี้ ตัวอย่างของประโยชน์โดยชอบด้วยกฎหมายนั้นรวมทั้งประโยชน์ในทางพาณิชย์ ประโยชน์ของปัจเจกบุคคล หรือประโยชน์ต่อสังคมที่กว้างกว่า เป็นต้น ซึ่งจะเห็นได้ว่าฐานของการประมวลผลในข้อนี้มีความยืดหยุ่นมากที่สุดเมื่อเทียบกับฐานอื่น ๆ

การพิจารณาว่าการประมวลผลจะชอบด้วยกฎหมายโดยอาศัยฐานข้อนี้ ได้หรือไม่นั้น มีข้อพิจารณาสามประการ กล่าวคือ 1. บททดสอบโดยหลักเกณฑ์ด้านวัตถุประสงค์ (Purpose Test)

ซึ่งต้องพิจารณาว่าการประมวลผลนั้นเป็นไปเพื่อให้ได้มาซึ่งประโยชน์อันชอบด้วยกฎหมายหรือไม่ 2. บททดสอบโดยหลักเกณฑ์ด้านความจำเป็น (Necessity Test) ซึ่งต้องพิจารณาว่าการประมวลผลข้อมูลนั้นจำเป็นสำหรับวัตถุประสงค์นั้นหรือไม่ และ 3. บททดสอบโดยหลักเกณฑ์การชั่งน้ำหนัก (Balancing Test) ซึ่งต้องพิจารณาว่าสิทธิของเจ้าของ ข้อมูลนั้นเหนือกว่าประโยชน์อันชอบด้วยกฎหมายหรือไม่

ทั้งนี้ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลจะทำการประมวลผลข้อมูลส่วนบุคคล ก็จะต้องพิจารณาว่าตนควรจะประมวลผลโดยอาศัยฐานข้อใดเพื่อให้สอดคล้องกับการประมวลผลแต่ละกรณีที่ตนดำเนินการ ซึ่งอาจจะต้องพิจารณาปัจจัยหลายประการ เช่น วัตถุประสงค์ในการประมวลผล การทำให้บรรลุวัตถุประสงค์นั้นสามารถดำเนินการด้วยวิธีการอื่นนอกจากการประมวลผลข้อมูลส่วนบุคคลได้หรือไม่ มีทางเลือกอื่นที่จะไม่ต้องประมวลผลข้อมูลส่วนบุคคลนั้นหรือไม่ หรือผู้จะประมวลผลนั้นเป็นเจ้าหน้าที่ของรัฐหรือไม่ เป็นต้น และในบางกรณีก็อาจจำเป็นต้องพิจารณาถึงฐานในการประมวลผลข้อมูลส่วนบุคคลไว้หลาย ๆ ฐานด้วย

7. สิทธิของเจ้าของข้อมูลส่วนบุคคล

General Data Protection Regulation ได้กำหนดสิทธิของเจ้าของข้อมูลส่วนบุคคลเอาไว้ในหมวดที่ 3 ซึ่งประกอบไปด้วยสิทธิหลายประการ ซึ่งในที่นี้จะกล่าวถึงแต่ละสิทธิโดยสังเขป ได้แก่

1) สิทธิที่จะได้รับการแจ้ง (The Right to be Informed)

กล่าวคือ บุคคลมีสิทธิที่จะได้รับแจ้งเกี่ยวกับการเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลของตน ซึ่งสิทธินี้มีการกำหนดไว้ใน Article 13 และ Article 14 โดยกำหนดว่าบุคคลมีสิทธิที่จะได้รับแจ้งเกี่ยวกับ “ข้อมูลเกี่ยวกับความเป็นส่วนตัว” (Privacy Information) ซึ่งสำหรับกรณีตาม Article 13 จะเป็นข้อมูลที่ต้องแจ้งให้ทราบในกรณีที่เก็บรวบรวมข้อมูลส่วนบุคคลจากตัวเจ้าของข้อมูลเอง และสำหรับกรณีตาม Article 14 จะเป็นการแจ้งข้อมูลให้ทราบสำหรับกรณีที่ได้รับข้อมูลจากแหล่งอื่นนอกจากเจ้าของข้อมูลส่วนบุคคล ซึ่งตัวอย่างของข้อมูลต่าง ๆ ที่ต้องแจ้งให้ทราบ ก็เช่น ตัวตนของผู้ควบคุมข้อมูลส่วนบุคคลและรายละเอียดสำหรับการติดต่อ วัตถุประสงค์ของการประมวลผลข้อมูลตลอดจนฐานทางกฎหมายในการประมวลผลข้อมูล หรือผู้รับหรือประเภทผู้ที่จะได้รับข้อมูลดังกล่าว ในกรณีที่จะมีการ เปิดเผยข้อมูลนั้นต่อไป เป็นต้น

2) สิทธิที่จะเข้าถึงข้อมูลส่วนบุคคลของตน (The Right of Access) ซึ่งปรากฏอยู่ใน Article 15 โดยเจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะได้รับการยืนยันจากผู้ควบคุมข้อมูลส่วนบุคคลว่ามีการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวกับตนหรือไม่ และถ้าหากมีการประมวลผลดังกล่าว ผู้นั้นก็จะมีสิทธิในการเข้าถึงข้อมูลต่าง ๆ เช่น วัตถุประสงค์ของการประมวลผล ประเภทของข้อมูลส่วนบุคคลที่เกี่ยวข้อง ผู้รับหรือประเภทของผู้จะรับข้อมูลส่วนบุคคลนั้นในกรณีที่มี การเปิดเผยหรือได้รับแจ้งสิทธิในการร้องเรียนต่อหน่วยงานที่ทำหน้าที่กำกับดูแล (Supervisory Authority) เป็นต้น

3) สิทธิที่จะแก้ไขข้อมูลให้ถูกต้อง (The Right to Rectification) โดย Article 16 ได้กำหนดว่าเจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะได้รับการแก้ไขข้อมูลส่วนบุคคลที่เกี่ยวกับตนที่ไม่ถูกต้องโดยไม่ชักช้า ตลอดจนมีสิทธิที่จะขอให้ทำข้อมูลที่ไม่สมบูรณ์ให้มีความสมบูรณ์ขึ้น ซึ่งอาจด้วยวิธีการให้คำอธิบายเพิ่มเติมเกี่ยวกับข้อมูลนั้นก็ได้ ทั้งนี้โดยจะต้องพิจารณาถึงวัตถุประสงค์ของการประมวลผลด้วย

4) สิทธิที่จะถูกลืมหรือสิทธิที่จะลบ (The Right to be Forgotten หรือ The Right to Erasure) ซึ่งปรากฏอยู่ใน Article 17 โดยเจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการลบข้อมูลส่วนบุคคลเกี่ยวกับตนโดยไม่ชักช้า และผู้ควบคุมข้อมูลส่วนบุคคลจะต้องลบข้อมูลดังกล่าวหากเป็นไปตามเงื่อนไขที่มาตรานี้กำหนด เช่น ข้อมูลส่วนบุคคลนั้นไม่มีความจำเป็นอันเกี่ยวเนื่องกับวัตถุประสงค์ที่ได้มีการเก็บรวบรวมหรือประมวลผลอีกต่อไป เจ้าของข้อมูลส่วนบุคคลได้เพิกถอนความยินยอม (ในกรณีที่การประมวลผลมีฐานจากความยินยอม) หรือข้อมูลส่วนบุคคลนั้นถูกประมวลผลโดยไม่ชอบด้วยกฎหมาย เป็นต้น ทั้งนี้ แม้จะเป็นกรณีตามเงื่อนไขที่อาจขอให้ลบข้อมูลได้แล้วก็ตาม สิทธิข้อนี้ก็ยังมีข้อยกเว้นอีกว่า ถ้าหากว่าการประมวลผลข้อมูลส่วนบุคคลนั้น มีความจำเป็นเพื่อกรณีต่าง ๆ ได้แก่ เพื่อการใช้สิทธิเสรีภาพในการแสดงออกและการเข้าถึงข้อมูลข่าวสารเพื่อการปฏิบัติให้เป็นไปตามข้อผูกพันตามกฎหมายเพื่อการสาธารณสุข เพื่อบรรลุวัตถุประสงค์เพื่อประโยชน์สาธารณะ การศึกษาวิจัยทางวิทยาศาสตร์หรือประวัติศาสตร์ หรือทางสถิติ หรือเพื่อก่อตั้งหรือใช้สิทธิทางกฎหมาย หรือต่อสู้คดี

5) สิทธิที่จะจำกัดการประมวลผล (The Right to Restrict Processing) ซึ่งปรากฏตาม Article 18 โดยเจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะให้ผู้ควบคุมข้อมูลส่วนบุคคลจำกัดการประมวลผลในกรณีต่าง ๆ เช่น การประมวลผลนั้นไม่ชอบด้วยกฎหมาย หรือข้อมูลส่วนบุคคลนั้น ไม่มีความจำเป็นสำหรับวัตถุประสงค์ของการประมวลผลอีกต่อไป แต่เจ้าของข้อมูลส่วนบุคคลจำเป็นต้องอาศัยข้อมูลดังกล่าวเพื่อก่อตั้งหรือใช้สิทธิทางกฎหมาย หรือต่อสู้คดี เป็นต้น ทั้งนี้ ในกรณีที่การประมวลผลถูกจำกัดแล้ว ข้อมูลส่วนบุคคลดังกล่าวนอกจากการเก็บแล้วจะถูกนำมาประมวลผลได้ก็แต่โดยความยินยอมของเจ้าของข้อมูลส่วนบุคคล หรือเป็นไปเพื่อการก่อตั้งหรือใช้สิทธิทาง กฎหมาย หรือต่อสู้คดี หรือเป็นไปเพื่อปกป้องคุ้มครองสิทธิของบุคคลธรรมดาหรือนิติบุคคลสำหรับเหตุผลเกี่ยวกับประโยชน์สาธารณะที่สำคัญของสหภาพหรือรัฐสมาชิก เท่านั้น

6) สิทธิที่จะโอนย้ายข้อมูล (The Right to Data Portability) ปรากฏตาม Article 20 โดยเจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะได้รับข้อมูลส่วนบุคคลที่เกี่ยวกับตนที่ให้ไว้แก่ ผู้ควบคุมข้อมูลส่วนบุคคล โดยข้อมูลนั้นอยู่ในสภาพที่มีการจัดหมวดหมู่ และอยู่ในรูปแบบที่สามารถอ่านได้โดยเครื่องคอมพิวเตอร์ (Machine-Readable) นอกจากนี้ ยังมีสิทธิที่จะให้โอนข้อมูลดังกล่าวให้กับผู้

ควบคุมข้อมูลส่วนบุคคลรายอื่นได้ด้วย ทั้งนี้ สิทธินี้จะใช้เฉพาะในกรณีที่การประมวลผลมีฐานมาจากความยินยอม และการประมวลผลนั้นได้ทำโดยวิธีการอัตโนมัติ (Automated Means) เท่านั้น

7) สิทธิที่จะคัดค้าน (The Right to Object) ปรากฏตาม Article 21 โดยเจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะคัดค้านการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวกับตนได้ใน กรณีต่าง ๆ เช่นกรณีที่การประมวลผลนั้นมีฐานมาจากการปฏิบัติงานเพื่อประโยชน์สาธารณะหรือ เป็นการใช้อำนาจรัฐของผู้ควบคุมข้อมูลส่วนบุคคล หรือเป็นการจำเป็นเพื่อให้ได้มาซึ่งประโยชน์โดยชอบด้วยกฎหมาย รวมทั้งกรณีที่เป็นการนำข้อมูลส่วนบุคคลมาใช้ในการวิเคราะห์พฤติกรรมของบุคคลนั้น (Profiling) เป็นต้น ซึ่งหากมีการคัดค้านแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องไม่ประมวลผลข้อมูลนั้นอีกต่อไปเว้นเสียแต่ว่าจะแสดงให้เห็นได้ว่าตนมีฐานที่ชอบด้วยกฎหมายสำหรับการประมวลผลที่เหนือกว่าประโยชน์ สิทธิ และเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือเป็นไปเพื่อการก่อตั้งหรือใช้สิทธิทางกฎหมายหรือต่อสู้คดี เป็นต้น

8) สิทธิเกี่ยวกับการตัดสินใจด้วยวิธีการอัตโนมัติและการใช้ข้อมูลเพื่อการวิเคราะห์พฤติกรรมบุคคล (Profiling) ปรากฏอยู่ใน Article 22 โดยเจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะไม่ถูกตัดสินจากการประมวลผลข้อมูลส่วนบุคคลด้วยวิธีการอัตโนมัติเพียงอย่างเดียวเท่านั้น ซึ่งรวมไปถึงการนำข้อมูลมาใช้ในการวิเคราะห์พฤติกรรมบุคคลนั้น (Profiling) ที่อาจก่อให้เกิดผลทางกฎหมายเกี่ยวกับตนหรือส่งผลที่มีความสำคัญในระดับเดียวกันด้วย อย่างไรก็ตาม สิทธิในข้อนี้มีข้อยกเว้นอยู่กล่าวคือ หากเป็นไปเพื่อการเข้าสู่การทำสัญญาหรือเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคล หรือได้รับความยินยอมของเจ้าของข้อมูลส่วนบุคคลอย่างชัดแจ้งแล้ว เป็นต้น

ทั้งนี้ เจ้าของข้อมูลส่วนบุคคลจะสามารถใช้สิทธิใดของตนตามที่ได้กล่าวข้างต้นได้บ้างนั้น อาจขึ้นอยู่กับฐานในการประมวลผลข้อมูลส่วนบุคคลนั้นด้วย ยกตัวอย่างเช่น ในกรณีที่การประมวลผลข้อมูลส่วนบุคคลมีฐานมาจากการปฏิบัติหน้าที่ตามกฎหมาย เช่นนี้ เจ้าของข้อมูลส่วนบุคคลจะไม่สามารถใช้สิทธิในการลบข้อมูลส่วนบุคคลของตนได้หรือในกรณีที่การ ประมวลผลอาศัยฐานจากสัญญา เช่นนี้ก็จะไม่สามารถใช้สิทธิในการคัดค้านการประมวลผลได้ เป็นต้น

8. การส่งข้อมูลไปยังประเทศที่สาม

นอกจากหลักเกณฑ์ในการประมวลผลข้อมูลส่วนบุคคลและสิทธิของเจ้าของ ข้อมูลส่วนบุคคลแล้ว General Data Protection Regulation ยังได้กำหนดหลักเกณฑ์สำหรับการส่งข้อมูลส่วนบุคคลไปยังประเทศที่สามหรือองค์การระหว่างประเทศเอาไว้ด้วย โดยหากคณะกรรมาธิการ (Commission) พิจารณาเห็นว่า ประเทศที่จะมีการส่งข้อมูลส่วนบุคคลไปหรือดินแดนส่วนหนึ่งของประเทศดังกล่าว มีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ (Article 45) ก็จะทำให้สามารถส่งข้อมูลได้โดยไม่ต้องอาศัยการอนุญาตเป็นการเฉพาะ (Specific Authorisation) แต่สำหรับ

ประเทศที่ไม่มีมาตรฐานการคุ้มครองที่เพียงพอในการส่งข้อมูลก็จะต้องพิจารณาเงื่อนไขอื่นที่ทำให้สามารถส่งข้อมูลระหว่างกันได้ เช่น ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้จัดหามาตรการป้องกันที่เหมาะสม (Appropriate Safeguards) และจะต้องสามารถบังคับตามสิทธิของเจ้าของข้อมูลส่วนบุคคลและ บังคับตามมาตรการเยียวยาตามกฎหมายให้แก่เจ้าของข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพ (Article 46 1.)

สำหรับกรณีที่จะถือได้ว่ามีมาตรการป้องกันที่เหมาะสมนั้น ตาม Article 46 กำหนดไว้ เช่น เป็นการปฏิบัติตามกฎเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร (Binding Corporate Rules) เป็นต้น นอกจากนี้ยังมีข้อยกเว้นอื่น ๆ สำหรับเฉพาะกรณีตาม Article 49 อีก เช่น เจ้าของข้อมูลได้ให้ความยินยอมโดยชัดแจ้งภายหลังจากที่ได้รับทราบข้อมูลความเสี่ยงของการส่งข้อมูลดังกล่าวแล้ว เป็นการส่งข้อมูลที่จำเป็นเพื่อปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคล หรือการส่งข้อมูลมีความจำเป็นสำหรับการก่อตั้งหรือใช้สิทธิทางกฎหมาย หรือต่อสู้คดี เป็นต้น

กล่าวโดยสรุปได้ว่าสาระสำคัญ ของ General Data Protection Regulation ที่โดดเด่นนั้นมีดังนี้[85]

1) ให้ประชาชนเข้าถึงข้อมูลส่วนบุคคลของตนได้ง่ายและไม่มีค่าใช้จ่าย

2) แจ้งให้ทราบถึงวัตถุประสงค์ ต้องมีความโปร่งใสในการรวบรวมข้อมูลส่วนบุคคล

3) เมื่อมีการนำข้อมูลไปประมวลผล จะต้องได้รับความยินยอมที่ชัดเจนจากเจ้าของข้อมูล (Clear and Affirmative Consent)

4) การใช้ข้อมูลควรเป็นไปตามวัตถุประสงค์ที่แจ้งเท่านั้น

5) จัดให้มีระบบการคุ้มครองข้อมูลส่วนบุคคลตั้งแต่ขั้นแรกของการ ออกแบบบริการและให้การตั้งค่าเป็นมิตรต่อการคุ้มครองข้อมูลส่วนบุคคล (Privacy-Friendly Setting)

6) ให้สิทธิประชาชนในการขอข้อมูลส่วนบุคคลของตนจากผู้ประกอบการเพื่อโอนข้อมูลนั้นไปยัง ผู้ประกอบการอื่นได้

7) ให้สิทธิเจ้าของข้อมูลส่วนบุคคลเรียกร้องให้มีการลบข้อมูลของตนออกจากระบบเมื่อไม่มี ความจำเป็นที่ผู้ประกอบการจะต้องเก็บข้อมูลนั้นไว้ หรือเจ้าของข้อมูลไม่ประสงค์ให้นำข้อมูลดังกล่าวไป ประมวลผลอีกต่อไป

เมื่อพิจารณาถึงความแตกต่างระหว่างสาระสำคัญของ General Data Protection Regulation กับ European Union Directive 95/46/EC จะเห็นว่ามีประเด็นความแตกต่างที่น่าสนใจดังต่อไปนี้ คือ[86]

---

[85] EU, *op. cit.*

1) การบังคับใช้กฎหมายนอกอาณาเขต (Extraterritarial Applicability) กล่าวคือ General Data Protection Regulation มีการกำหนดนิยามของข้อมูลข้ามพรมแดนชัดเจน ทำให้ไม่เกิดความสับสนในการจัดการข้อมูลข้ามแดน ทำให้ไม่จำต้องพิจารณาว่าควรใช้กฎหมายฉบับไหนของประเทศใดมาบังคับ เพราะผู้รับข้อมูลไม่ว่าจะอยู่ในอาณาเขตใด ก็จะต้องทำตามหลักการของ General Data Protection Regulation เหมือนกันทั้งสิ้น

2) กำหนดบทลงโทษรุนแรงขึ้น กล่าวคือ หากพบว่ามีการปฏิบัติผิดไปจากหลักการของ General Data Protection Regulation องค์กรที่ฝ่าฝืนจะต้องจ่ายค่าปรับ 4% ของผลประกอบการรายได้ทั่วโลกทั้งหมด หรือสูงถึง 20 ล้านยูโร ซึ่งบทลงโทษนี้จะบังคับใช้ทั้งหน่วยงานผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล

3) กำหนดการขอความยินยอมจากเจ้าของข้อมูล (Consent) จะต้องใช้ภาษาที่ชัดเจน กระชับ และเข้าใจง่าย เช่นเดียวกับกรณีของการถอนความยินยอม

4) กำหนดการแจ้งเตือนเมื่อเกิดเหตุข้อมูลรั่วไหล (Breach Notification) กล่าวคือ หากพบว่าข้อมูลรั่วไหล หน่วยงานผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลต้องแจ้งให้หน่วยงานกำกับดูแลและประชาชนทราบภายใน 72 ชั่วโมง

5) สิทธิในการเข้าถึง (Right to Access) ใน General Data Protection Regulation ได้มีการขยายขอบเขตสิทธิของเจ้าของข้อมูล ที่ผู้ควบคุมข้อมูล ต้องแจ้งเจ้าของข้อมูลว่าข้อมูลถูกใช้เอาไปใช้เพื่อวัตถุประสงค์ใด และต้องจัดทำสำเนาข้อมูลให้กับเจ้าของข้อมูลในรูปแบบอิเล็กทรอนิกส์โดยห้ามเก็บค่าใช้จ่ายเพิ่ม

6) มีการกำหนดสิทธิที่จะถูกลืม (Right to be Forgotten) กล่าวคือเจ้าของข้อมูลสามารถขอให้หน่วยงานควบคุมข้อมูลลบข้อมูลของตัวเองออกได้ นอกจากนั้นข้อมูลที่ไม่มีความเกี่ยวข้องกับจุดประสงค์ของการประมวลผลก็ต้องเอาออกด้วยเช่นกัน

7) มีการกำหนดสิทธิในการโอนย้ายข้อมูลของตนจากผู้ประกอบการหนึ่งไปยังผู้ประกอบการอื่นได้ (Data Portability)

8) กำหนดให้ความสำคัญกับความเป็นส่วนตัวตั้งแต่การออกแบบ (Privacy by Design) คือการให้หน่วยงานควบคุมข้อมูลตระหนักความสำคัญของข้อมูล โดยเริ่มจากการออกแบบบริการที่คำนึงถึงการป้องกันข้อมูลส่วนบุคคลตั้งแต่แรก ไม่ใช่ออกแบบบริการแล้ว จึงค่อยมาเพิ่มเรื่องการป้องกันข้อมูลส่วนบุคคลของผู้รับบริการ และในการนี้จะต้องใช้มาตรการทางเทคนิคที่เหมาะสมและมีประสิทธิภาพในการป้องกันข้อมูลด้วย

---

[86] *Ibid.*

9) กำหนดให้ต้องมีเจ้าหน้าที่คุ้มครองข้อมูล หรือ Data Protection Officers (DPO) จากเดิมที่องค์กรต้องแจ้งกิจกรรมการประมวลผลข้อมูลต่อหน่วยงานท้องถิ่น (Local Data Protection Authority) ซึ่งเป็นหลักการตามกฎหมายเดิม (Data Protection Act 1998) แต่ภายใต้หลักการของ General Data Protection Regulation นี้ไม่ต้องแจ้งอีกต่อไป แต่ทว่าจะต้องมีการว่าจ้างเจ้าหน้าที่คุ้มครองข้อมูล หรือ DPO เข้ามาในบริษัทเพื่อทำหน้าที่ดูแลข้อมูลส่วนบุคคลเลย

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

เมื่อต่อมา General Data Protection Regulation ได้ถูกตราขึ้น ก็จะเห็นว่าเป็นไปเพื่อวัตถุประสงค์ในการยกระดับมาตรฐานคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลให้มีความชัดเจน และคุ้มครองเป็นการทั่วไป (General) รวมไปถึงกำหนดการบังคับใช้ให้เหมือนกันในทุกประเทศสมาชิกของสหภาพยุโรป ซึ่งต่างจากก่อนหน้านี้ ที่ สภาพยุโรปกำหนดเพียงหลักการเบื้องต้นให้ ซึ่งก็แล้วแต่ละประเทศไปดำเนินการร่างกฎหมายและกำหนดบทลงโทษกันเอง และประเด็นสำคัญอีกประการหนึ่งที่ General Data Protection Regulation ถูกกำหนดให้ชัดเจนคือ การส่งข้อมูลระหว่างประเทศ ทำให้ไม่ต้องสับสนอีกต่อไปว่าจะจัดการอย่างไร เพราะระบุชัดเจนว่า ผู้รับข้อมูล ซึ่งอาจจะเป็นบริษัทคลาวด์หรือบริษัทประมวลผลข้อมูล (Data Processer) ที่แม้อยู่ต่างประเทศ นอก

ขอบเขตของประเทศสมาชิก EU ก็ต้องทำตามหลักการของ General Data Protection Regulation ที่ได้วางหลักคุ้มครองสิทธิขั้นพื้นฐานนี้ไว้นั่นเอง

2.3.4 แนวทางการควบคุมข้อมูลส่วนบุคคลที่จัดเก็บด้วยคอมพิวเตอร์ของสหประชาชาติ (Guildlines for the Regulation of Computerized Personal Data Files)

เมื่อวันที่ 14 ธันวาคม พ.ศ.1990 คณะมนตรีเศรษฐกิจและสังคมแห่งสหประชาชาติ (United Nations Economic and Social Council) ได้กำหนดหลักเกณฑ์เกี่ยวกับข้อมูลส่วนบุคคลไว้ในแนวทางการควบคุมข้อมูลส่วนบุคคลที่จัดเก็บด้วยคอมพิวเตอร์ (Guidelines for the Regulation of Computerized Personal Data Files) ซึ่งมีสาระสำคัญดังนี้[87]

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

1) เก็บรวบรวมเพียงเท่าที่เกี่ยวข้องและเหมาะสมกับวัตถุประสงค์ที่ระบุ

2) ข้อมูลส่วนบุคคลจะต้องไม่ถูกใช้หรือเปิดเผย เว้นแต่ได้รับความยินยอมจากบุคคลที่เกี่ยวข้อง

3) ระยะเวลาที่จัดเก็บข้อมูลส่วนบุคคลจะต้องไม่เกินกว่าระยะเวลาที่การดำเนินการตามวัตถุประสงค์ที่ระบุไว้ได้สำเร็จลง

4) หลักการเข้าถึงข้อมูล (Principle of Interested-Person Access) หมายความว่า เจ้าของข้อมูลมีสิทธิที่จะได้รู้ว่ามีการประมวลผลข้อมูลข่าวสารที่เกี่ยวกับตนโดยได้รับข้อมูลในรูปแบบที่เข้าใจได้ในเวลาอันสมควรและปราศจากค่าใช้จ่าย และสามารถขอให้แก้ไขหรือลบในกรณีมีการเก็บ

---

[87] Office of the United Nations High Commissioner for Human Rights, **Guidelines for the Regulation of Computerized Personal Data Files**, Retrieved March 13, 2018 from http://www.refworld.org/pdfid/3ddcafaac.pdf

ข้อมูลโดยไม่ชอบด้วยกฎหมาย ไม่จำเป็น หรือมีการเก็บข้อมูลโดยไม่ถูกต้อง ข้อกำหนดแห่งหลักการนี้ให้บังคับใช้กับบุคคลทุกคนโดยไม่คำนึงถึงสัญชาติหรือถิ่นที่อยู่

5) หลักการไม่เลือกปฏิบัติ (Principle of Non-Discrimination) หมายความว่า ห้ามเก็บรวบรวมข้อมุลซึ่งอาจทำให้เกิดการเลือกปฏิบัติที่ขัดต่อกฎหมาย 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 ต้องมีการรักษาความปลอดภัยข้อมุลที่จัดเก็บ เพื่อป้องกันอันตรายทั้งจากภัยธรรมชาติ การสูญหายหรือเสียหาย การทำลายโดยบุคคล การเข้าถึงโดยปราศจากอำนาจ การใช้ในทางที่ผิด หรือการทำลายโดยไวรัสคอมพิวเตอร์

8) การกำกับดูแล (Supervision of Sanctions) หมายความว่า กฎหมายของประเทศต่าง ๆ จะต้องระบุหน่วยงานที่รับผิดชอบในการควบคุมดูแลและให้คำแนะนำเกี่ยวกับการปฏิบัติตามหลักการนี้

9) การส่งข้อมูลข้ามพรมแดน (Tran Border Data Flows) หมายความว่า การส่งข้อมูลระหว่างประเทศจะสามารถกระทำได้ในกรณีที่ประเทศสองประเทศหรือมากกว่าสองประเทศ มีกลไกในการคุ้มครองสิทธิความเป็นส่วนตัวในระดับเดียวกัน

10) ขอบเขตการใช้ข้อปฏิบัติ (Field of Application) หมายความว่า หลักปฏิบัติดังกล่าวควรได้มีการปฏิบัติใช้สำหรับข้อมูลในภาครับและเอกชนที่จัดเก็บด้วยคอมพิวเตอร์ (Computerized Files) เช่นเดียวกับการจัดเก็บด้วยวิธีการอื่น ๆ ที่มีการปรับปรุงให้เหมาะสมกับเอกสารที่จัดเก็บด้วยมือ (Manual Files)

2.3.5 การคุ้มครองข้อมูลส่วนบุคคลของกลุ่มประเทศเอเปค (APEC Information Privacy Principles)[88]

สำหรับองค์กรความร่วมมือทางเศรษฐกิจเอเชีย–แปซิฟิก (Asia–Pacific Economic Cooperation APE: APEC) ก่อตั้งขึ้นเมื่อ พ.ศ.2532 โดยมีจุดประสงค์มุ่งเน้นความเจริญเติบโตและพัฒนาที่ยั่งยืนของภูมิภาค และผลักดันให้การเจรจาการค้าระหว่างกันประสบผลสำเร็จ ขณะเดียวกัน APEC ก็ ต้องการถ่วงดุลอำนาจทางเศรษฐกิจของกลุ่มเศรษฐกิจต่าง ๆ โดยเฉพาะกลุ่มสหภาพยุโรปอีกด้วย ปัจจุบัน APEC มีสมาชิกทั้งสิ้น 21 เขตเศรษฐกิจ (19 ประเทศ 2 เขตเศรษฐกิจ) ประกอบด้วยประเทศมหาอำนาจ ทางการเมืองและเศรษฐกิจที่สำคัญคือ สหรัฐอเมริกา รัสเซีย สาธารณรัฐประชาชนจีน และญี่ปุ่น รวมทั้ง สมาชิกอาเซียน และประเทศในอเมริกาเหนือและใต้ โดยกลุ่ม APEC ได้จัดการประชุมเชิงปฏิบัติการฯ ในปี พ.ศ.2551 เพื่อหารือแลกเปลี่ยนประสบการณ์ด้านการคุ้มครองข้อมูลส่วนบุคคลระหว่างประเทศ และเสริมสร้างความเข้าใจแก่ สมาชิกในการนำ APEC Privacy Framework ไปปรับใช้ให้เหมาะแต่ละประเทศสมาชิกที่มีความแตกต่าง กันด้านกฎระเบียบและวิธีการดำเนินงาน รวมทั้งเพื่อส่งเสริมการขับเคลื่อนโครงการนำร่อง Data Privacy Pathfinder โดยประเด็นหลักในการหารือคือ การพัฒนาแผนการดำเนินโครงการย่อย 9 โครงการซึ่งประกอบไปด้วยโครงการดังต่อไปนี้[89]

1. CBPR Self–Assessment Guidance for Organization พัฒนามาตรฐาน แนวทางประเมินตนเอง (Self–Assessment) เพื่อช่วยให้ภาคธุรกิจนำแนวทางดังกล่าวไปพัฒนาเป็น แนวทางในการคุ้มครองข้อมูลส่วนบุคคลข้ามพรหมแดน (Cross–Border Privacy Rules: CBPRs) ของตนเองได้สร้างความตระหนักและการรับรู้ในหลักการคุ้มครองข้อมูลส่วนบุคคลภายใต้กรอบ APEC (APEP Privacy Principles) และการคุ้มครองบุคคลข้ามพรมแดน (CBPRs)

2. Guidelines for Trustmark Participating in a CBPR System องค์กรที่ออก Trustmark จะต้องพัฒนาแนวทางที่จะต้องปฏิบัติเพื่อให้เป็นที่ยอมรับในเรื่องของ SBPRs ภายใต้กรอบ APEC

3. Compliance Review of an Organization’s CBPRs พัฒนาแนวทางสำหรับ องค์กรที่ออก Trustmark เพื่อใช้ในการประเมินภาคธุรกิจที่ต้องการนำหลักการคุ้มครองข้อมูลส่วนบุคคลภายใต้กรอบ APEC ไปใช้

---

[88] APEC Secretariat, **APEC Privacy Framework,** Retrieved March 10, 2018 from https://www.apec.org/-/media/APEC/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf

[89] คณาธิป ทองวีรวงศ์, **รายงานการวิจัยฉบับสมบูรณ์ เรื่องการปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน,** หน้า 45.

4. Directory of Compliant Organizations พัฒนาฐานข้อมูลรายชื่อของภาคธุรกิจที่ มี CBPRs และได้รับการรับรองว่าได้ปฏิบัติตามหลักการคุ้มครองข้อมูลส่วนบุคคลภายใต้กรอบ APEC

5. DATA Protection Authority and Privacy Contact Officer Directory พัฒนาฐานข้อมูล ที่เกี่ยวข้องกับอำนาจ หน้าที่ต่าง ๆ ที่เกี่ยวข้องในการคุ้มครองข้อมูล รายชื่อเจ้าหน้าที่ที่ ดูแลในเรื่อง การคุ้มครองข้อมูลส่วนบุคคลในเขตเศรษฐกิจภายใต้กรอบ APEC

6. Template Enforcement Cooperation Arrangements พัฒนารูปแบบ เอกสาร เช่น บันทึกความเข้าใจ (MOU) หรือหนังสือผูกพัน (Letter of Commitment) ซึ่งแสดงถึง ข้อตกลง ร่วมกันระหว่างหน่วยงานที่มีอำนาจในการแลกเปลี่ยนข้อมูลส่งเสริมความร่วมมือระหว่างพรมแดน ใน การสอบสวน และบังคับใช้

7. Template Cross-Border Cooperation Arrangements พัฒนาแบบฟอร์มรับ เรื่อง ร้องเรียนในรูปแบบเดียวกับแบบฟอร์มขอความช่วยเหลือของ OECD (OECD Request for Assistant From) เพื่อสะดวก เป็นที่ยอมรับต่อการจัดการข้อร้องเรียนข้ามพรมแดน และพัฒนาความ ร่วมมือระหว่าง หน่วยงานที่มีอำนาจในการแลกเปลี่ยน สอบสวน บังคับใช้ และให้ความช่วยเหลือ ในทางจำเป็นและเหมาะสม

8. Guidelines and Procedures for Responsive Regulation in a CBPR System พัฒนาแนวทางและขั้นตอน (เช่น แผนผัง) ที่ช่วยในการพิจารณาว่า ขั้นตอนในการจัดการข้อร้องเรียน ข้ามพรมแดนควรจะเป็นเช่นไร และควรจะดำเนินการอย่างไรเพื่อไปยังขั้นตอนถัดไป

9. CBPR International Implementation Pilot Project พัฒนาและทดสอบ โครงการ นำร่องระหว่างเขตเศรษฐกิจที่สนใจเข้าร่วมทดสอบระบบ CBPR การดำเนินโครงการนำร่องฯ มิได้ บังคับให้สมาชิกจะต้องปฏิบัติทุกโครงการย่อย แต่สมาชิกสามารถเลือกดำเนินโครงการใด ก่อนหรือ หลังได้ ตามความสมัครใจ โดยพิจารณาจากความและการดำเนินงานภายในเขตเศรษฐกิจเป็นหลัก ทั้งนี้ เปูาหมาย หลักของการดำเนินโครงการนำร่องเพื่อให้สมาชิกได้ตื่นตัวและเริ่มดำเนินการที่เห็นผล เป็นรูปธรรมของสมาชิก

สำหรับหลักเกณฑ์เกี่ยวกับข้อมูลส่วนบุคคล (APEC Information Privacy Principles) ซึ่งมี สาระสำคัญดังนี้

1. เพื่อเป็นการรักษาผลประโยชน์ของบุคคลในเรื่องสิทธิความเป็นส่วนตัวจึงต้องมีการ กำหนดมาตรการการคุ้มครองข้อมูลส่วนบุคคลเพื่อป้องกันการใช้ข้อมูลโดยมิชอบและป้องกันความ เสียหายที่จะเกิดจากการใช้โดยมิชอบ ไม่ว่าจะเป็นการเก็บ การใช้ และการส่งต่อ

2. ต้องแจ้งเจ้าของข้อมูลอย่างชัดเจนว่า จะมีการเก็บข้อมูลส่วนบุคคล วัตถุประสงค์การเก็บ ประเภทบุคคลหรือองค์กรที่ข้อมูลส่วนบุคคลอาจได้รับการเปิดเผย ต้องแจ้งสิทธิของเจ้าของข้อมูล

และมาตรการที่จะใช้ในการจำกัดการใช้ การเปิดเผย การเข้าถึง และการแก้ไข ทั้งนี้ต้องแจ้งก่อนหรือในขณะที่เก็บ หรือเร็วที่สุดหลังการจัดเก็บ

3. ต้องมีการจัดเก็บอย่างจำกัดเท่าที่เป็นไปตามวัตถุประสงค์ของการเก็บ การเก็บต้องทำโดยวิธีที่ถูกกฎหมาย และวิธีที่เป็นธรรมและเหมาะสม โดยได้แจ้งต่อและได้ขอคำยินยอมจากเจ้าของข้อมูลแล้ว

4. ข้อมูลที่เก็บไว้จะเอาไปใช้ได้เฉพาะตามวัตถุประสงค์ของการเก็บเท่านั้น เว้นแต่ได้รับคำยินยอมจากเจ้าของข้อมูลหรือเป็นไปตามข้อยกเว้นตามที่กฎหมายกำหนด

5. เจ้าของข้อมูลมีสิทธิเลือกว่าจะยินยอมให้มีการเก็บใช้และเปิดเผยข้อมูลส่วนบุคคลของตน

6. ข้อมูลที่จัดเก็บต้องมีความถูกต้อง สมบูรณ์ เป็นปัจจุบัน ตามความจำเป็นและตามวัตถุประสงค์การเก็บ

7. ต้องมีมาตรการคุ้มครองข้อมูลอย่างเหมาะสมเพื่อป้องกันอันตรายที่อาจเกิดขึ้น ไม่ว่าจะเป็นการสูญหาย-เสียหาย-การเข้าถึงข้อมูล ส่วนบุคคลโดยไม่ได้รับอนุญาต การทำลายโดยไม่ได้รับอนุญาต การใช้ปรับเปลี่ยนแก้ไข-เปิดเผยโดยมิชอบ

8. เจ้าของข้อมูลมีสิทธิรับรู้ว่ามีการเก็บข้อมูลส่วนบุคคลของตนหรือไม่ มีสิทธิเข้าถึงข้อมูลของตนเอง และมีสิทธิขอให้ตรวจสอบความถูกต้องและขอให้ปรับปรุง แก้ไข เพิ่มเติม หรือทำลายข้อมูลของตน

9. ผู้เก็บข้อมูลจะต้องรับผิดชอบการจัดมาตรการต่าง ๆ ให้เป็นไปตามหลักเกณฑ์ดังกล่าว การส่งข้อมูลส่วนบุคคลไปยังบุคคลหรือองค์การอื่น ๆ ไม่ว่าภายในประเทศหรือส่งไปยังต่างประเทศจะต้องได้รับคำยินยอมจากเจ้าของข้อมูลและจะต้องมีมาตรการที่เหมาะสมที่ประกันได้ว่าบุคคลหรือองค์กรที่ได้รับข้อมูลไปแล้วจะเก็บรักษาข้อมูลให้เป็นไปตามหลักเกณฑ์ที่กำหนด

เมื่อพิจารณาเปรียบเทียบระหว่าง GDPR และ APEC Framework จะเห็นว่ามีความเหมือนและแตกต่างปรากฏรายละเอียดดังตารางต่อไปนี้[90]

---

[90] Alex Wall, **GDPR Matchup: The APEC Privacy Framework and Cross-Border Privacy Rules**, Retrieved March 17, 2018 from https://iapp.org/news/a/gdpr-matchup-the-apec-privacy-framework-and-cross-border-privacy-rules/

ตารางที่ 2.2 เปรียบเทียบระหว่าง GDPR และ APEC Framework

ประเด็น	APEC Privacy Framework	GDPR
วัตถุประสงค์	เพื่อพัฒนาประสิทธิภาพในการคุ้มครองความเป็นส่วนตัวจากการไหลเวียนของข้อมูล และเพื่อสร้างความเชื่อมั่นต่อระบบเศรษฐกิจการค้าของภูมิภาคอาเซียน	เพื่อให้สามารถเคลื่อนย้ายข้อมูลส่วนบุคคลภายในสหภาพได้อย่างเสรีและสามารถปกป้องสิทธิเสรีภาพขั้นพื้นฐานโดยเฉพาะสิทธิข้อมูลส่วนบุคคล
วัตถุแห่งการบังคับ	บังคับกับบุคคลหรือองค์กรทั้งในภาครัฐและเอกชนที่ครอบครอง, เก็บรวบรวม,ประมวลผล,ใช้,ถ่ายโอนหรือเปิดเผยข้อมูลส่วนบุคคล	บังคับกับการประมวลผลข้อมูลส่วนบุคคลทั้งหมดหรือบางส่วนโดยวิธีอัตโนมัติภายใต้ขอบเขตของกฎหมายของสหภาพยุโรป
ขอบเขตอำนาจ	ใช้ภายในขอบเขตที่กฎหมายของแต่ละประเทศสมาชิกบังคับอยู่	ใช้บังคับกับการประมวลผลที่เกิดขึ้นในสหภาพยุโรป หรือโดยผู้ประมวล ผลที่มีสถานประกอบการในสหภาพยุโรป หรือการประมวลผลที่เกิดขึ้นนอกสหภาพยุโรปแต่กิจกรรมนั้นมีผลไปถึงในสหภาพยุโรป เช่นการซื้อขายสินค้าหรือบริการที่เกี่ยวพันกับสหภาพยุโร (Extraterritorial Applicability)
ความหมายของข้อมูลส่วนบุคคล	ข้อมูลส่วนบุคคลหมายถึงข้อมูลเกี่ยวกับบุคคลที่ระบุหรือระบุตัวได้ (เหมือนกัน)	ข้อมูลส่วนบุคคลหมายถึงข้อมูลใด ๆ ที่เกี่ยวข้องกับบุคคลธรรมดาที่ระบุตัวหรือสามารถระบุตัวได้
ผู้ควบคุมข้อมูล (Data Controller)	หมายถึง บุคคลหรือองค์กรที่ควบคุมการรวบรวมเก็บรวบรวมประมวลผลหรือใช้ข้อมูลส่วนบุคคล	บุคคลธรรมดาหรือนิติบุคคลหรือหน่วยงานของรัฐหรือหน่วยงานอื่น ๆ ที่ดำเนินการหรือร่วมกับผู้อื่นดำเนินการประมวลผลข้อมูลส่วนบุคคล
ผู้ประมวลผลข้อมูล (Data Processors)	APEC Privacy Framework ไม่บังคับใช้กับผู้ประมวลผล คงบังคับใช้กับผู้ควบคุมข้อมูลเท่านั้น	หมายถึงบุคคลธรรมดาหรือหน่วยงานของรัฐหน่วยงานหรือหน่วยงานอื่นที่ประมวลผลข้อมูลส่วนบุคคล

ตารางที่ 2.2 (ต่อ)

ปะเด็น	APEC Privacy Framework	GDPR
การเปิดเผยข้อมูลต่อสาธารณะ	The APEC Privacy Framework มีข้อจำกัด ในการเปิดเผยต่อสาธารณชน โดยจะต้องมีการแจ้งเตือนและการให้ทางเลือก โดยเฉพาะอย่างยิ่งหากเป็นข้อมูลที่ไม่จำเป็นซึ่งข้อมูลเหล่านี้มีอยู่แล้วในที่สาธารณะและผู้ควบคุมข้อมูลส่วนบุคคลไม่ได้รวบรวมข้อมูลโดยตรงจากบุคคลที่เกี่ยว ข้อง	การเปิดเผยข้อมูลส่วนบุคคลต่อสาธารณชนอาจได้รับอนุญาตสำหรับวัตถุประสงค์บางอย่างเพื่อประโยชน์สาธารณะ เช่น ผลการวิจัยทางวิทยาศาสตร์หรือทางประวัติศาสตร์หรือเพื่อวัตถุประสงค์เชิงสถิติ ตราบเท่าที่การแจ้งให้ทราบไม่ได้ก่อให้เกิดความเสียหายร้ายแรง ในกรณีเช่นนี้ผู้ควบคุมต้องใช้มาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูล
หลักการป้องกันการล่วงละเมิด (Preventing Harm Principle)	การปกป้องข้อมูลส่วนบุคคลควรได้รับการออกแบบกระบวนการเพื่อป้องกันการใช้ข้อมูลดังกล่าวในทางที่ผิด	มุ่งเน้นปกป้องสิทธิเสรีภาพขั้นพื้นฐานของบุคคลธรรมดาโดยเฉพาะอย่างยิ่งสิทธิในการปกป้องข้อมูลส่วนบุคคลของปัจเจกชน
การแจ้งเตือน (Notice)	ผู้ควบคุมข้อมูลส่วนบุคคลควรให้ข้อมูลที่ชัดเจนและสามารถเข้าถึงได้ง่ายเกี่ยวกับนโยบายและแนวทางปฏิบัติและต้องดำเนิน การตามขั้นตอนที่สมเหตุ สมผลเพื่อให้มั่นใจว่าได้มีการแจ้งให้ทราบล่วงหน้าก่อนหรือในขณะที่เก็บรวบรวมข้อมูลส่วนบุคคล (หรือแจ้งให้ทราบเร็วที่สุดเท่าที่เป็นไปได้)	ต้องได้รับความยินยอมจากเจ้าของข้อมูลเป็นลายลักษณ์อักษร การขอความยินยอมจะต้องแจ้งในรูปแบบที่ชัดเจนเข้าใจได้ง่าย และสามารถเข้าถึงได้โดยใช้วิธีการที่ชัดเจนและ ภาษาธรรมดา ส่วนการประมวลผลข้อมูลที่เปิดเผยต่อสาธารณชนอาจได้รับอนุญาตสำหรับกรณีที่มีวัตถุประสงค์เพื่อประโยชน์สาธารณะ เช่นผลการวิจัยทางวิทยาศาสตร์หรือทางประวัติศาสตร์หรือเพื่อวัตถุประสงค์เชิงสถิติ ตราบเท่าที่การแจ้งให้ทราบมีแนวโน้มที่ไม่ได้ก่อให้เกิดความเสียหายร้ายแรง ในกรณีเช่นนี้ผู้ควบคุมต้องใช้มาตรการที่เหมาะสมเพื่อ

ตารางที่ 2.2 (ต่อ)

ปะเด็น	APEC Privacy Framework	GDPR
		ปกป้องสิทธิเสรีภาพและผลประโยชน์ของเจ้าของข้อมูล
ข้อจำกัดในการรวบรวมข้อมูลส่วนบุคคล (Collection Limitation)	การจัดเก็บข้อมูลส่วนบุคคล ควรมีข้อจำกัด เฉพาะข้อมูลที่เกี่ยวข้องกับวัตถุประสงค์ในการรวบรวมข้อมูล และควรใช้วิธีการที่ถูกต้องเหมาะสมและเป็นธรรมตามกฎหมาย โดยต้องมีการแจ้งให้ทราบ หรือได้รับความยินยอมจากบุคคลที่เกี่ยวข้อง	ข้อมูลส่วนบุคคลจะถูกเก็บรวบรวมได้ ก็เฉพาะแต่เพื่อวัตถุประสงค์ที่ชัดเจนและถูกต้อง และไม่ได้ถูกนำไปใช้หรือประมวลผลในลักษณะที่ขัดวัตถุประสงค์ของการจัดเก็บ
ข้อจำกัดในการใช้ข้อมูลส่วนบุคคล (Use Limitation)	ข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมนั้น ควรใช้เฉพาะเพื่อให้เป็นไปตามวัตถุประสงค์ของการรวบรวมและวัตถุประสงค์อื่นที่เกี่ยวข้องเท่านั้น เว้นแต่ ก) โดยได้รับความยินยอมจากเจ้าของข้อมูล หรือ ข) เมื่อจำเป็นต้องให้ตามที่ถูกร้องขอ หรือ ค) โดยอำนาจของกฎหมาย	ข้อมูลส่วนบุคคลจะต้องถูกเก็บรวบรวมเพื่อวัตถุประสงค์ที่ระบุอย่างชัดเจนและใช้วิธีการที่ถูกต้องและห้ามนำไปประมวลผลในลักษณะที่ขัดกับวัตถุประสงค์ของการจัดเก็บ
การเปิดโอกาสให้เลือกและการขอความยินยอม (Choice and Consent)	ควรมีกลไกที่ชัดเจนและเข้าใจง่ายและสามารถเข้าถึงได้โดยให้มีค่าใช้จ่ายน้อยที่สุด	อนุญาตให้มีการใช้ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับสุขภาพโดยต้องได้รับความยินยอมอย่างชัดแจ้ง เว้นแต่กรณีที่ได้รับอนุญาตจากสหภาพยุโรปหรือกฎหมายของประเทศสมาชิก “ความยินยอมอย่างชัดแจ้ง” ต้องเป็นไปตามมาตรฐานที่สูงกว่าความยินยอมในการประมวลผลข้อมูลส่วนบุคคลอื่น ๆ บุคคลต้องได้รับการแจ้งอย่างชัดเจนเกี่ยวกับการใช้ข้อมูลของตนและ

ตารางที่ 2.2 (ต่อ)

ปะเด็น	APEC Privacy Framework	GDPR
		ดำเนินการยืนยันเพื่อแสดงความยินยอมจากพวกเขา
ความถูกต้องและสมบูรณ์ของข้อมูล (Data Integrity)	ข้อมูลส่วนบุคคลควรมีความถูกต้องครบถ้วน และเป็นปัจจุบันตามขอบเขตที่จำเป็นเพื่อวัตถุประสงค์ในการใช้งาน	ข้อมูลส่วนบุคคลควรได้รับการดำเนินการในลักษณะที่ช่วยให้มั่นใจได้ถึงความปลอดภัยที่รวมถึงสามารถป้องกันการประมวลผลโดยไม่ได้รับอนุญาตหรือผิดกฎหมายและป้องกันการสูญเสียการทำลายหรือความเสียหายโดยใช้มาตรการด้านเทคนิคและองค์กรที่เหมาะสม
ความปลอดภัยข้อมูลส่วนบุคคล (Security Safeguards)	ผู้ควบคุมข้อมูลควรปกป้องข้อมูลส่วนบุคคลที่ตนถือไว้ โดยมีระบบป้องกันที่เหมาะสม เพื่อป้องกันความเสี่ยง เช่น ความเสียหาย ถูกทำลาย ถูกดัดแปลงแก้ไข ถูกเปิดเผย ถูกใช้ผิดประเภท โดยผลจากการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต ซึ่งการป้องกันดังกล่าวควรเป็นไปได้และมีความเหมาะสมกับบริบทและระดับความรุนแรงของภยันตรายและควรได้รับการทบทวนและประเมินผลใหม่เป็นระยะ	จะต้องมีการดำเนินการด้านความปลอดภัยให้เหมาะสมกับระดับความเสี่ยงของข้อมูล ซึ่งผู้ควบคุมและผู้ประมวลผลจะต้องปฏิบัติตามมาตรการด้านเทคนิคและมีการจัดการที่เหมาะสม
การเข้าถึงข้อมูลและความถูกต้องของข้อมูล (Access and Correction)	บุคคลควรได้รับจากการยืนยันจากผู้ควบคุมข้อมูลส่วนบุคคลว่า ได้มีการจัดเก็บข้อมูลส่วนบุคคลของเขาไว้หรือไม่ และสามารถเข้าถึงข้อมูลที่ถูกจัดเก็บไว้และสามารถตรวจสอบความถูกต้องสมบูรณ์, มี	เจ้าของข้อมูลมีสิทธิที่จะได้รับการยืนยันจากผู้ควบคุมข้อมูลส่วนบุคคลว่าข้อมูลบุคคลของเขากำลังถูกจัดเก็บและดำเนินการอยู่หรือไม่, มีสิทธิเข้าถึงข้อมูลส่วนบุคคลของตน, มีสิทธิในการลบและแก้ไขข้อมูลส่วนบุคคล รวมถึงมีสิทธิใน

ตารางที่ 2.2 (ต่อ)

ประเด็น	APEC Privacy Framework	GDPR
	สิทธิแก้ไขหรือลบข้อมูลส่วนบุคคลของตนได้สิทธิทั้งหมดที่กล่าวมาข้างต้นต้องมีความสมดุลกับภาระหรือค่าใช้จ่ายในการปฏิบัติตามกฎหมายหรือเหตุผลด้านความปลอดภัยในการคุ้มครองข้อมูลทางการค้า หรือการคุ้มครองสิทธิส่วนบุคคลของบุคคลอื่นที่ไม่ใช่บุคคลที่ได้รับผลกระทบ	การยื่นคำร้องต่อองค์กรผู้รับผิดชอบ
หลักความรับผิดชอบ (Accountability)	ผู้ควบคุมข้อมูลส่วนบุคคลต้องรับผิดชอบในการปฏิบัติตามมาตรการที่ระบุข้างต้น	ผู้ควบคุมต้องรับผิดชอบและสามารถแสดงให้เห็นถึงการปฏิบัติตามหลักการของการประมวลผลข้อมูลส่วนบุคคลภายใต้ GDPR
การถ่ายโอนข้อมูลส่วนบุคคลไปยังบุคคลหรือประเทศอื่น (Transfer of Personal Data to Another Person or Country)	เมื่อข้อมูลส่วนบุคคลถูกถ่ายโอนไปยังบุคคลหรือองค์กรอื่นไม่ว่าจะเป็นในประเทศหรือต่าง ประเทศ ผู้ควบคุมข้อมูลส่วนบุคคลควรได้รับความยินยอมและใช้ความระมัดระวังอย่างเหมาะสมรวมถึงทำตามขั้นตอนที่เหมาะสมเพื่อให้มั่นใจว่าผู้รับหรือองค์กรจะปกป้องข้อมูลอย่างสม่ำเสมอและสอดคล้องหลักการเหล่านี้	ข้อมูลส่วนบุคคลสามารถถ่ายโอนไปยังประเทศที่สามนอกสหภาพยุโรปได้ก็ต่อเมื่อได้รับพิจารณาแล้วว่าประเทศนั้นมีกฎหมายที่ให้การป้องกันสิทธิในข้อมูลส่วนบุคคลอย่างเพียงพอ ไม่ต่ำไปกว่ามาตรฐานของสหภาพยุโรป
นิยามของการล่วงละเมิด (Breach Definition)	ไม่มี	การละเมิดข้อมูลส่วนบุคคลหมายถึงการละเมิดความปลอดภัยที่นำไปสู่การทำลาย การสูญหาย การเปลี่ยน แปลง การเปิดเผยหรือการเข้าถึงข้อมูลส่วนบุคคลที่ถูกจัดเก็บหรือประมวลผลอย่าง

ตารางที่ 2.2 (ต่อ)

ปะเด็น	APEC Privacy Framework	GDPR
		อื่นโดยไม่ได้ตั้งใจ
การแจ้งเตือนการละเมิด (Breach Notification)	The APEC Privacy Framework ไม่ได้กล่าวถึงเรื่องนี้ แต่มีหลักการของ CBPRs ที่ประเทศเอเปคต้องผูกมัดกำหนดให้ประเทศสมาชิกออกกฎที่กำหนดให้ผู้ควบคุมข้อมูลต้องทำสัญญาป้องกันข้อมูลโดยให้การแจ้งเตือนโดยผู้ประมวลผลข้อมูลหรือตัวแทนผู้ให้บริการหรือผู้ให้บริการรายอื่น ๆ	ต้องมีการประเมินเหตุการณ์และแจ้งให้ทราบถึงการละเมิดข้อมูล แก่เจ้าของข้อมูลส่วนบุคคล เมื่อมีความเสี่ยงสูงต่อการละเมิดสิทธิเสรีภาพของบุคคล และในส่วนที่เกี่ยวกับหน่วยงานกำกับดูแลให้มีการแจ้งเตือนเมื่อมีการละเมิดซึ่งอาจทำให้เกิดความเสียหาย
การป้องกันข้อมูลส่วนบุคคลตั้งแต่ชั้นออกแบบ (Privacy by Design)	ไม่ชัดเจน	จะต้องมีการกำหนดมาตรการทางเทคนิคที่เหมาะสมและมีประสิทธิ- ภาพในการป้องกันข้อมูลตั้งแต่ชั้นเริ่มต้น

จากตารางข้างต้นจะเห็นว่า ความแตกต่างในระหว่างหลักการคุ้มครองข้อมูลส่วนบุคคลของกลุ่มประเทศสหภาพยุโรป ตาม GDPR นั้น มีรากฐานของการกำเนิดขึ้นมาจากความประสงค์ที่จะคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลอันเป็นสิทธิขั้นพื้นฐานของปัจเจกชนชาวยุโรปเป็นสำคัญ แต่ทว่า การกำเนิดขึ้นของหลักการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลตามกรอบความร่วมมือ APEC Privacy Framework นั้นเกิดขึ้นจากพื้นฐานของความต้องการในด้านเศรษฐกิจการค้าการลงทุนเสียมากกว่าจะเป็นความต้องการคุ้มครองสิทธิของพลเมืองอย่างแท้จริง แต่อย่างไรก็ดี เมื่อพิจารณาเนื้อหาสาระของหลักการคุ้มครองแล้วจะเห็นได้ว่า มีการกำหนดหลักการไว้ใกล้เคียงกัน ทั้งนี้อาจเป็นเพราะอิทธิพลทางการค้าของสหภาพยุโรปส่งผลให้กลุ่มประเทศเอเปคต้องปรับตัว โดยนำหลักการมากำหนดไว้ในแนวทางเดียวกัน แต่อย่างไรก็ดี หลักการของ GDPR จะมีความโดดเด่นกว่ากรอบความร่วมมือ APEC Privacy Framework ในหลายประการ เช่น การกำหนดให้มีการบังคับใช้กฎหมายนอกอาณาเขต (Extraterritorial Applicability), การกำหนดโทษที่รุนแรงกว่าอย่างเห็นได้ชัด , การกำหนดนิยามของการรั่วไหลของข้อมูลอย่างชัดเจน

และมีการกำหนดหลักการปฏิบัติในการแจ้งเตือนเมื่อข้อมูลรั่วไหลอย่างชัดเจนว่าต้องดำเนินการภายใน 72 ชั่วโมง, มีการกำหนดสิทธิในการโอนย้ายข้อมูลไว้อย่างชัดเจน (Data Portibility), มีการกำหนดผู้ประกอบการจะต้องให้ความสำคัญกับการป้องกันข้อมูลส่วนบุคคลตังแต่การออกแบบ (Privacy by Design) ฯลฯ เป็นต้น ดังนั้นจึงกล่าวได้ว่า มาตรฐานของการคุ้มครองข้อมูลของสหภาพยุโรปตาม GDPR นั้น สูงกว่า มาตรฐานของ APEC Privacy Framework อันจะส่งผลให้ต้องมีการปรับปรุงหลักการคุ้มครองข้อมูลส่วนบุคคลให้มีมาตรฐานทัดเทียมกันอย่างรวดเร็วต่อไปในเร็ววันนี้แน่นอน

ดังนั้น จึงกล่าวโดยสรุปได้ว่า สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลจัดได้ว่าเป็นสิทธิมนุษยชนที่สำคัญ โดยเฉพาะอย่างยิ่งในยุคของการเปลี่ยนแปลงอย่างรวดเร็วในทางเทคโนโลยี เช่นปัจจุบันอันเป็นเหตุของการล่วงละเมิดสิทธินี้เป็นอย่างมาก จนทำให้ประเทศต่าง ๆ รวมถึงองค์กรระหว่างประเทศให้ความสำคัญกับการหามาตรการและกลไกเพื่อเป็นกรอบในการคุ้มครอง ซึ่งการคุ้มครองข้อมูลส่วนบุคคลในกฎหมายระหว่างประเทศและข้อตกลงระหว่างประเทศล้วนแต่เป็นกรอบที่ใช้บังคับเกี่ยวกับการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ไม่ว่าจะเป็นในการเก็บรวมรวม และการดำเนินการต่าง ๆ เกี่ยวกับข้อมูลส่วนบุคคล โดยเฉพาะในประเด็นเกี่ยวกับการส่งและรับข้อมูลระหว่างประเทศ หลักการต่าง ๆ เกี่ยวกับการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลเหล่านี้ จะมีผลกระทบไปสู่การที่รัฐสมาชิก รวมถึงรัฐที่ได้รับผลกระทบจากกฎเกณฑ์เหล่านี้จะต้องดำเนินการพัฒนาและปรับปรุงกฎหมายภายในของรัฐตนให้มีมาตรฐานการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลที่ทัดเทียมกัน ผลกระทบต่าง ๆ เช่นนี้ประเทศไทยเองก็หลีกเลี่ยงไม่พ้นในอันที่จะต้องพัฒนาและปรับปรุงหลักกฎหมายที่เกี่ยวกับมาตรการและกลไกคุ้มครองต่าง ๆ ดังที่จะได้กล่าวถึงในบทต่อ ๆ ไป

บทที่ 3

มาตรการและกลไกทางกฎหมายในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของต่างประเทศ

ด้วยเหตุที่สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนั้น มีการพัฒนาแนวความคิดมาอย่างยาวนานในสังคมของต่างประเทศ จนได้มีการพัฒนาหลักการขึ้นมาอย่างเป็นระบบทำให้รัฐได้สร้างมาตรการทางกฎหมายขึ้นมาเพื่อวางระบบในการคุ้มครองสิทธินี้อย่างมีประสิทธิภาพ ในบทนี้จะได้แสดงให้เห็นถึงมาตรการและกลไกในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล โดยจะอธิบายถึงแนวคิดและวิวัฒนาการของการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของต่างประเทศ ไม่ว่าจะเป็นการกำหนดนิยามสิทธิที่จะได้รับความคุ้มครอง การกำหนดหลักการในการจำกัดสิทธิ รวมถึงองคกรและกลไกทางกฎหมายในการคุ้มครองสิทธินี้ ดังจะได้อธิบายต่อไปนี้

3.1 การคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกา

3.1.1 แนวคิดและวิวัฒนาการในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกา

3.1.1.1 ความหมายของข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกา

กฎหมายคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกาใช้ระบบแบ่งเป็นส่วน ๆ ที่เรียกว่า Sectoral Laws กล่าวคือ ไม่มีกฎหมายที่วางหลักเกณฑ์อันมีลักษณะเป็นการทั่วไป ที่เป็นกฎหมายแม่บทหรือกฎหมายกลางซึ่งวางหลักการคุ้มครองสิทธิ แต่จะมีการออกบทกฎหมายเฉพาะที่สภาคองเกรสตราขึ้นเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลเป็นบางกรณี บางเรื่องหรือบางประเภทเมื่อเกิดปัญหาขึ้นแล้ว[91] สำหรับประเทศที่ใช้ระบบนี้ จะมีการกำหนดนิยามความหมายของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูล

---

[91] ประสิทธิ ปิวาวัฒนิช, *เรื่องเดิม,* หน้า 535.

ส่วนบุคคลในความหมายอย่างแคบ[92] อันเป็นสิ่งที่แตกต่างจากประเทศที่ใช้ระบบ Comprehensive ตัวอย่างเช่นประเทศในสหภาพยุโรปที่จะมีการให้นิยามไว้ในความหมายอย่างกว้างโดยผลของการวางหลักการอันมีลักษณะเป็นการทั่วไป

สำหรับกฎหมายที่ได้ให้ความหมายของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในประเทศสหรัฐอเมริกานั้น แต่ละฉบับก็จะให้นิยามความหมายไปตามวัตถุประสงค์ของกฎหมายที่มุ่งหมายหรือต้องการจะคุ้มครองสิทธิในแต่ละเรื่องไป กฎหมายฉบับสำคัญที่ให้นิยามความหมายของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลไว้อย่างน่าสนใจก็คือ Privacy Act 1974 ซึ่งได้กำหนดนิยามความหมายของ “การบันทึกข้อมูลส่วนบุคคล” ว่า การบันทึกใด ๆ การจัดเก็บรวมรวม หรือการจัดกลุ่มข้อมูลเกี่ยวกับบุคคล ซึ่งเก็บรักษาไว้โดยหน่วยงานของรัฐบาลกลาง โดยรวมถึง ข้อมูลเกี่ยวกับการศึกษา ข้อมูลเกี่ยวกับธุรกรรมทางการเงิน ประวัติการแพทย์ และประวัติอาชญากรรม หรือประวัติการทำงาน และข้อมูลนั้นได้ระบุชื่อ หรือหมายเลขประจำตัว สัญลักษณ์ หรือรหัสบ่งชี้อื่น ๆ ที่สามารถแสดงได้ว่าหมายถึงบุคคลใด เช่นลายนิ้วมือ หรือแผ่นบันทึกเสียง หรือภาพถ่าย”[93] ซึ่งนั่นหมายความว่า ในส่วนของข้อมูลส่วนบุคคลนั้น ย่อมหมายถึงข้อมูลที่เกี่ยวกับบุคคลที่มีการจัดเก็บรวบรวม หรือจัดกลุ่มข้อมูล ไม่ว่าจะเป็นข้อมูลที่เกี่ยวกับการศึกษา ข้อมูลเกี่ยวกับธุรกรรมทางการเงิน ประวัติการแพทย์ และประวัติอาชญากรรม หรือประวัติการทำงาน และข้อมูลนั้นได้ระบุชื่อ หรือหมายเลขประจำตัว สัญลักษณ์ หรือรหัสบ่งชี้อื่น ๆ ที่สามารถแสดงได้ว่าหมายถึงบุคคลใดได้นั่นเอง

สำหรับในส่วนนิยามของข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) ก็มีลักษณะเช่นเดียวกันคือมีการกำหนดนิยามไว้ในกฎหมายหลาย ๆ ฉบับ ซึ่งในภาพรวมแล้วพอจะสรุปความหมายได้ว่า หมายถึง ข้อมูลส่วนบุคคลที่เกี่ยวกับทางด้านสุขภาพ ข้อมูลส่วนบุคคลในด้านการเงิน ข้อมูลเครดิตหรือความน่าเชื่อถือของผู้กู้ ข้อมูลส่วนบุคคลของนักเรียน ข้อมูลไบโอเมตริกซ์ ข้อมูลส่วนบุคคลของเด็กอายุต่ำกว่า 13 ปีที่ได้มีการจัดเก็บออนไลน์ ข้อมูลที่สามารถนำไปใช้เพื่อการโจรกรรมหรือฉ้อโกงได้ ก็ถือว่าเป็นข้อมูลที่มีความอ่อนไหวด้วย ยกตัวอย่างเช่น หมายเลขประกันสังคมและหมายเลขประจำตัวประชาชนอื่น ๆ หมายเลขบัตรเครดิตและบัญชีการเงินสุขภาพ

---

[92] ศิริกุล ภู่พันธ์, *เรื่องเดิม*, หน้า 99.

[93] *เรื่องเดียวกัน*, หน้า 100.

หรือข้อมูลทางการแพทย์ ข้อมูลหมายเลขประกันภัย ข้อมูลและบัญชีดิจิทัล ลายเซ็นและ/หรือข้อมูลชีวภาพ[94]

3.1.1.2 สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในฐานะสิทธิขั้นพื้นฐาน

เมื่อพิจารณาถึงสิทธิในความเป็นส่วนตัวอันเกี่ยวกับข้อมูลส่วนบุคคลในประเทศสหรัฐอเมริกาแล้ว จะเห็นได้ว่าเป็นสิทธิขั้นพื้นฐานประการหนึ่งที่ได้รับการรับรองและคุ้มครองให้โดยรัฐธรรมนูญที่ให้ความสำคัญกับหลักการพื้นฐานของแนวความคิดเรื่องสิทธิตามธรรมชาติ ว่ามนุษย์ทั้งหลายเกิดมาเท่าเทียมกัน มนุษย์มีสิทธิบางประการที่ติดตัวมนุษย์มาตั้งแต่เกิดจนกระทั่งถึงแก่ความตาย สิทธิดังกล่าว ได้แก่ สิทธิในชีวิต เสรีภาพในร่างกายสิทธิในทรัพย์สิน และความเสมอภาคซึ่งเป็นสิทธิที่ไม่สามารถโอนให้แก่กันได้ และผู้ใดจะล่วงละเมิดมิได้[95] โดยบทบัญญัติแห่งรัฐธรรมนูญแห่งสหรัฐอเมริกานี้จะทำหน้าที่เป็นหลักประกันอันสำคัญในการคุ้มครองให้แก่ประชาชน อย่างไรก็ดีเมื่อพิจารณาลำพังเนื้อหาของบทบัญญัติแห่งรัฐธรรมนูญ ก็ยังไม่เพียงพอที่จะอธิบายถึงสาระสำคัญของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในฐานะที่เป็นสิทธิขั้นพื้นฐานของประชาชนได้ จำเป็นจะต้องศึกษาควบคู่ไปกับคำวินิจฉัยของศาลสูงสุดของสหรัฐอเมริกา (U.S. Supreme Court) ซึ่งเป็นองค์กรที่มีอำนาจตีความประกอบกันไปด้วย ซึ่งสาระสำคัญของสิทธิในความเป็นส่วนตัว ในเบื้องต้นมีดังจะกล่าวต่อไปนี้ คือ[96]

บทแก้ไขที่ 1 (The First Amendment) ได้วางหลักการรับรองสิทธิเสรีภาพของบุคคลในการแสดงความคิดเห็นและการเลือกรับข้อมูลข่าวสารได้อย่างเสรี แต่ในขณะเดียวกันก็ได้ให้ความคุ้มครองแก่บุคคลที่ถูกเผยแพร่เรื่องราวหรือข้อเท็จจริงอันเกี่ยวกับตนด้วย

บทแก้ไขที่ 4 (The Fourth Amendment) ได้วางหลักการให้ความคุ้มครองสิทธิในความเป็นส่วนตัวไว้ว่า “ประชาชนมีสิทธิที่จะได้รับความปลอดภัยในชีวิต ร่างกาย เคหสถาน เอกสาร และทรัพย์สิ่งของจะถูกตรวจค้นหรือยึดโดยไม่มีเหตุอันชอบด้วยกฎหมายจะกระทำไม่ได้ และจะออกกฎหมายเพื่อกระทำการดังกล่าวมิได้ เว้นแต่มีเหตุผลที่ควรเชื่อถือซึ่งได้รับการยืนยันด้วยคำสาบานหรือคำปฏิญาณ และจะต้องระบุสถานที่ที่จะค้นหรือบุคคลที่จะถูกจับกุมหรือสิ่งที่จะยึดไว้ในหมายนั้นอย่างเฉพาะเจาะจง” ซึ่งจากบทบัญญัตินี้ศาลสูงสุดของสหรัฐอเมริกาได้อาศัยอำนาจในการเป็นผู้ตีความรัฐธรรมนูญโดยตีความคำว่า “การค้นและการยึด” ในความหมายอย่างกว้างและได้กำหนด

---

[94] Data Protection Laws of the World, **Definition of Personal Data**, Retrieved December 12, 2018 from https://www.dlapiperdataprotection.com/index.html?t=definitions&c=US&c2=

[95] บรรเจิด สิงคะเนติ, นนทวัชร์ นวตระกูลพิสุทธิ์ และเรวดี ขวัญทองยิ้ม, *เรื่องเดิม*, หน้า 45.

[96] กิตติพงศ์ กมลธรรมวงศ์, *เรื่องเดิม*, หน้า 139-140.

มาตรฐานคำว่า “ไม่สมเหตุสมผล” (Unreasonable) อย่างเคร่งครัดและเน้นตีความตามเจตนารมณ์โดยมุ่งถึงสิทธิและผลประโยชน์ที่รัฐธรรมนูญต้องการจะคุ้มครอง[97] นอกจากนี้ The Fourth Amendment ยังให้ความคุ้มครองสิทธิเสรีภาพในการตัดสินใจได้ด้วยตนเองของบุคคลเกี่ยวกับขอบเขตการดำเนินชีวิตในครอบครัวของตนหรือรูปแบบของความสัมพันธ์ส่วนตัวของบุคคล[98]

อย่างไรก็ดี แม้ว่ารัฐธรรมนูญแห่งสหรัฐอเมริกาจะได้ทำการรับรองสิทธิในความเป็นส่วนตัว ซึ่งรวมไปถึงสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลไว้ในฐานะเป็นสิทธิเสรีภาพขั้นพื้นฐานที่ประชาชนพึงได้รับความคุ้มครองจากรัฐก็ตาม แต่ทว่า สิทธิในความเป็นส่วนตัวนี้ยังคงมีในหลายกรณีที่ไปขัดกับคุณค่า (Value) ที่กฎหมายให้ความรับรองและคุ้มครองในประการอื่น เช่นกรณีตัวอย่างของการขัดกันระหว่างสิทธิในความเป็นส่วนตัว กับ ความมั่นคง (National Security) ที่หน่วยงาน National Security Agency (NSA) ซึ่งเป็นหน่วยงานด้านความมั่นคงของสหรัฐอเมริกาได้มีคำสั่งเรียกให้ผู้ประกอบการโทรคมนาคมส่งบันทึกข้อมูลเกี่ยวกับการโทรเข้าโทรออกจำนวนมาก (Telephony Metadata) เพื่อนำไปวิเคราะห์สำหรับประโยชน์ในการป้องกันการก่อการร้าย ซึ่งเรื่องดังกล่าวมานี้ได้เป็นคดีขึ้นสู่การพิจารณาของศาลสองศาลในเวลาไล่เลี่ยกันโดยมีประเด็นว่า การเก็บข้อมูลของ NSA และการวิเคราะห์ข้อมูลดังกล่าวเป็นการละเมิดสิทธิในความเป็นส่วนตัวซึ่งได้รับความคุ้มครองโดยรัฐธรรมนูญแห่งสหรัฐอเมริกาหรือไม่? ซึ่งศาลทั้งสองได้มีการตัดสินในประเด็นเดียวกันแตกต่างกันออกไป โดยศาลที่นิวยอร์ค ตัดสินว่า การกระทำของ NSA ไม่ได้เป็นการขัดต่อรัฐธรรมนูญ แต่ศาลที่โคลัมเบีย (District of Columbia) เห็นว่าการกระทำดังกล่าวเป็นการค้นและละเมิดสิทธิในความเป็นส่วนตัวที่ได้รับความคุ้มครองตามรัฐธรรมนูญ[99]

3.1.1.3 วิวัฒนาการในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในประเทศสหรัฐอเมริกา

สำหรับประเทศสหรัฐอเมริกาในอดีตเมื่อย้อนเวลากลับไปประมาณ 30-40 ปีก่อน ยังมีความเข้าใจผิดว่าสิทธิในความเป็นส่วนตัว รวมถึงกฎหมายที่ว่าด้วยความเป็นส่วนตัว (Privacy Law) นั้นเป็นเพียงสาขาหนึ่งของกฎหมายลักษณะละเมิด (Tort) ความจริงแล้วกฎหมายว่าด้วยความเป็นส่วนตัวนั้นกินความไปถึงการจับหรือการค้นภายใต้บทบัญญัติของบทแก้ไขเพิ่มเติมรัฐธรรมนูญ

---

[97] บรรเจิด สิงคะเนติ, นนทวัชร์ นวตระกูลพิสุทธิ์ และเรวดี ขวัญทองยิ้ม, *เรื่องเดิม*, หน้า 46.

[98] กิตติพงศ์ กมลธรรมวงศ์, *เรื่องเดิม*, หน้า 140.

[99] American Civil Liberties Union v. James Clapper (United States District Court for the Southern District of New York, 2013); Klayman v. Obama (United States District Court, District of Columbia, 2013); ชวิน อุ่นภัทร, “ความเป็นส่วนตัวและการคุ้มครองจากการล่วงล้ำของรัฐในประเทศสหรัฐอเมริกา,” **วารสารนิติศาสตร์** 44, 4 (ธันวาคม 2558): 971.

แห่งสหรัฐอเมริกา (The Fourth Amendment) ในกรณีการเฝ้าระวังทางอิเล็กทรอนิกส์ ความเป็นส่วนตัวทางด้านครอบครัวและเพศ และกรณีความเป็นส่วนตัวในโลกไซเบอร์หรือโลกเทคโนโลยีสารสนเทศด้วย กล่าวคือ กฎหมายว่าด้วยความเป็นส่วนตัวนั้นสอดแทรกอยู่ในสาขาต่าง ๆ ที่มีอยู่ก่อนแล้วและได้รับการให้ความสำคัญมากขึ้นในภายหลังทำให้มีการศึกษาค้นคว้ากันมากขึ้นนั่นเอง[100]

เหตุการณ์สำคัญในประวัติศาสตร์ของการคุ้มครองสิทธิในความเป็นส่วนตัวของสหรัฐอเมริกานั้นเกิดขึ้นในปี ค.ศ.1890 ปรากฏในงานเขียนของนักนิติศาสตร์ผู้มีชื่อเสียงสองท่าน คือ Louis D. Brandeis และ Samuel D. Warren ที่ได้เคยกล่าวไว้แล้วในบทก่อน โดยประเด็นสำคัญอยู่ที่ท่านทั้งสองได้เสนอว่า เอกชนมีสิทธิตามกฎหมายที่จะคัดค้านการเผยแพร่หรือการตีพิมพ์ที่มีลักษณะเป็นการล่วงละเมิดต่อความเป็นส่วนตัว และกฎหมายเองก็ไม่ควรที่จำกัดอยู่แค่เพียงการคุ้มครองสิทธิในชีวิตร่างกายและทรัพย์สินเท่านั้น ควรจะคุ้มครองสิทธิที่จะใช้ชีวิตโดยปกติสุข (Right to Enjoy Life) หรือที่เรียกว่าสิทธิที่จะอยู่โดยลำพังก็ต้องได้รับความคุ้มครอง (Right to be Let Alone) ซึ่งภายหลังบทความที่ได้เผยแพร่ผ่านวารสาร Harvrd Law Review ก็นำไปสู่ประเด็นการถกเถียงอย่างกว้างขวางในสังคมยุคนั้นถึง “การมีอยู่” และ “การคุ้มครองสิทธิ” นี้[101] แต่อย่างไรก็ดี Louis D. Brandeis และ Samuel D. Warren ก็ยอมรับว่าการคุ้มครองสิทธิความเป็นส่วนตัว (The Right to Privacy) ยังคงมีข้อจำกัดบางประการ กล่าวคือ การคุ้มครองสิทธิในชีวิตส่วนตัวจะต้องไม่ขัดขวางต่อการเผยแพร่เรื่องราวอันเกี่ยวด้วยประโยชน์สาธารณะ หรือไม่คุ้มครองบุคคลซึ่งได้แสดงเจตนาสละสิทธิที่มีความเป็นอยู่โดยรอดพ้นจากการรับรู้ของสาธารณะ ซึ่งหมายถึงการให้สาธารณะรับรู้ความเป็นอยู่ในชีวิตของตน หรือไม่ขัดขวางต่อการสื่อสารเรื่องราวใด ๆ ซึ่งได้รับเอกสารสิทธิภายใต้กฎหมายเกี่ยวกับการ หมิ่นประมาทแม้จะเป็นเรื่องส่วนตัวก็ตาม และสิทธิในชีวิตส่วนตัวย่อมระงับไปเมื่อมีการเผยแพร่ข้อเท็จจริงโดยบุคคลนั้นเองหรือได้รับความยินยอมจากบุคคลนั้น[102]

ต่อมาในปี ค.ศ.1902 มลรัฐนิวยอร์ก (New York) ในคดี Roberson v. Rochester Folding Box ถือเป็นคดีที่กระตุ้นให้มีการคุ้มครองสิทธิความเป็นส่วนตัว (The Right to Privacy) โดยข้อเท็จจริงปรากฏว่า จำเลยได้ใช้ภาพของโจทก์ซึ่งเป็นเด็กผู้หญิงผู้หนึ่งในการโฆษณาสิ้นค้าแป้งข้าวสาลี โดยมิได้รับอนุญาตจากโจทก์และผู้ปกครองของโจทก์ โจทก์ได้ทำการคัดค้านการกระทำดังกล่าวและเรียกร้องให้มีการชดใช้ค่าเสียหาย ศาลอุทธรณ์แห่งมลรัฐนิวยอร์กได้ลงมติด้วยคะแนน 4 ต่อ 3 เสียง ให้โจทก์ชนะคดีในเรื่องการยักยอกแต่ปฏิเสธการให้มีการชดใช้ค่าเสียหาย โดยไม่ยอมรับ

---

[100] *เรื่องเดียวกัน*, หน้า 970.

[101] กิตติพงศ์ กมลธรรมวงศ์, *เรื่องเดิม*, หน้า 138.

[102] นพมาศ เกิดวิชัย, **การพัฒนากฎหมายเพื่อคุ้มครองสิทธิในความเป็นส่วนตัว** (วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยรังสิต, 2557), หน้า 59.

ว่าสิทธิความเป็นส่วนตัวมีจริงแม้จะมีความเห็นว่าโจทก์ควรได้รับการคุ้มครองในสิทธิความเป็นส่วนตัว ก็ตาม โดยศาลให้เหตุผลว่า กฎหมายเกี่ยวข้องกับสิ่งที่เป็นรูปธรรม ไม่มีเจตนารมณ์ให้มีการชดใช้ค่าเสียหายทางจิตใจ (Mental Damages) สิทธิความเป็นส่วนตัวยังไม่ปรากฏในกฎหมายจารีตประเพณี (Common Law) จึงยังมิได้รับรองสิทธิดังกล่าวแต่ประการใด[103]

สำหรับ คำพิพากษาคำพิพากษาในคดี Roberson v. Rochester Folding Box แสดงให้เห็นว่าศาลใน มลรัฐนิวยอร์กยังไม่ให้การยอมรับว่าสิทธิความเป็นส่วนตัวได้รับความคุ้มครองในกฎหมาย จารีตประเพณี (Common Law) ซึ่งผู้พิพากษา Gray J. ได้ทำการเขียนความเห็นแย้งไว้ โดยกล่าวว่า “สิทธิในความเป็นส่วนตัวเป็นสิทธิเกี่ยวกับบุคคล ซึ่งไม่ใช้เป็นสิทธิอันไม่มีอยู่ในระบบกฎหมาย แต่เป็นสิทธิส่วนเสริมของสิทธิที่เกี่ยวกับการคุ้มครองตัวตนของบุคคล นอกจากนั้นเมื่อสังคมมีการพัฒนาขึ้น การติดต่อสัมพันธ์ของมนุษย์ก็ย่อมมีลักษณะใหม่ ๆ เกิดขึ้นตามมา การให้ความคุ้มครองสิทธิที่เกี่ยวกับตัวบุคคลมีความสำคัญไม่น้อยไปกว่าการคุ้มครองสิทธิในทรัพย์สินของบุคคล”[104] ซึ่งคำพิพากษาดังกล่าวนี้ได้ถูกวิจารณ์อย่างกว้างขวาง และกลายเป็นแรงกระตุ้นให้มลรัฐนิวยอร์กผ่านการรับรองสิทธิความเป็นส่วนตัว (The Right to Privacy)[105]

ต่อมาในปี ค.ศ.1903 มลรัฐนิวยอร์กผ่านการรับรองสิทธิความเป็นส่วนตัว (The Right to Privacy) ในปี ค.ศ.1903 อันถือเป็นกฎหมายฉบับแรกของสหรัฐอเมริกาที่ทำการรับรองสิทธิความเป็นส่วนตัว[106] โดยมีใจความว่าดังนี้

มาตรา 50 "บุคคล บริษัท ที่ใช้ชื่อ ภาพ หรือภาพของบุคคลที่มีชีวิตเพื่อการโฆษณาหรือเพื่อวัตถุประสงค์ในการค้า โดยไม่ได้รับความยินยอมเป็นลายลักษณ์อักษรจากบุคคลดังกล่าวก่อนถือเป็นความผิดอาญา และถ้าเป็นการกระทำแก่ผู้เยาว์ ให้ถือว่าพ่อแม่หรือผู้ปกครองของผู้เยาว์เป็นผู้เสียหายด้วย"[107]

---

[103] *เรื่องเดียวกัน*, หน้า 60.

[104] คณาธิป ทองรวีวงศ์, **มาตรการทางกฎหมายในการคุ้มครองสิทธิของโดยมิได้รับรู้และยินยอม** (รายงานการวิจัย เสนอต่อคณะนิติศาสตร์ มหาวิทยาลัยเซนต์จอห์น, 2550), หน้า 74-75.

[105] วิสาร พันธุนะ, กฎหมายสื่อสารมวลชนในต่างประเทศ, ใน **เอกสารการสอนชุดกฎหมายและจริยธรรมสื่อมวลชน** (นนทบุรี: มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2552), หน้า 789.

[106] นพมาศ เกิดวิชัย, *เรื่องเดิม*, หน้า 60.

[107] Article 50 “A person, firm or corporation that uses for advertising purposes, or for the purposes of trade, the name, portrait or picture of any living person without having first obtained the written consent of such person, or if a minor of his or her parent or guardian, is guilty of a misdemeanor.”

กฎหมายฉบับดังกล่าวปัจจุบันก็คือ N.Y. Civil Rights Law 1921 มาตรา 50 ที่ได้บัญญัติให้การละเมิดสิทธิความเป็นส่วนตัว (Violation of The Right to Privacy) เป็นความผิดทั้งทางอาญาและทางแพ่ง

ต่อมา รัฐแคลิฟอร์เนีย (California) ได้มีการบัญญัติรับรองสิทธิความเป็นส่วนตัว (The Right to Privacy) ในลักษณะเดียวกับมลรัฐนิวยอร์ก (New York) ในประมวลกฎหมายแพ่งว่า “ผู้ใดรู้แล้วใช้ชื่อ เสียง ลายมือชื่อ ภาพถ่าย หรือคุณลักษณะของผู้อื่น เพื่อวัตถุประสงค์ทางการโฆษณา การขายสินค้าหรือการบริการ โดยปราศจากความยินยอมจากบุคคลนั้น หรือกรณีเป็นผู้เยาว์มิได้รับความยินยอมเป็นลายลักษณ์อักษรจากผู้แทนโดยชอบธรรม จะต้องรับผิดชดใช้ค่าสินไหมทดแทนสำหรับการนั้น”

ในปี ค.ศ.1905 มลรัฐจอร์เจีย (Georgia) ในคดี Pavesich v. New England Life Insurance โดยข้อเท็จจริงปรากฏว่า จำเลยได้ใช้รูปภาพของโจทก์ซึ่งเป็นศิลปินในการโฆษณากิจการประกันภัยของจำเลยแม้จำเลยจะมิได้ระบุชื่อโจทก์ในการโฆษณาแต่ทั้งนี้ไม่ปรากฏว่าโจทก์ได้เข้าทำประกันชีวิตกับบริษัทของจำเลยหรือได้ให้ความยินยอมในการใช้ภาพของโจทก์ โจทก์จึงได้ทำการฟ้องจำเลยฐานทำลายชื่อเสียงของโจทก์โดยหมิ่นประมาท (Defamation) และล่วงละเมิดในสิทธิความเป็นส่วนตัวของโจทก์ (Violation of The Right of Privacy)[108]

ศาลสูงแห่งมลรัฐจอร์เจียได้ตระหนักถึงสิทธิความเป็นส่วนตัว (The Right to Privacy)ในฐานะที่เป็นสิทธิเด็ดขาดและเป็นสิทธิที่มีอยู่โดยธรรมชาติ ทำการยอมรับว่าสิทธิความเป็นส่วนตัวของโจทก์ได้ถูกละเมิด และสั่งห้ามมิให้จำเลยกระทำการดังกล่าวโดยให้เหตุผลว่า “กรณีที่ระบบกฎหมายจารีตประเพณี (Common Law) ไม่ได้กล่าวถึง มิได้หมายความว่าไม่มีอยู่ แม้จะไม่มีแบบอย่างบรรทัดฐานก็เป็นที่ยอมรับด้วยกฎหมายธรรมชาติ (Natural Law) และเป็นสิทธิที่มีกฎหมายรัฐธรรมนูญเป็นหลักประกันว่าเสรีภาพย่อมรวมถึงสิทธิที่จะมีชีวิตอยู่ตามที่เขาต้องการ ซึ่งบางคนย่อมอาจต้องการมีชีวิตอยู่ตามลำพัง (Right to be Let Alone)”[109]

ต่อมาในปี ค.ศ.1974 ประเทศสหรัฐอเมริกาได้ตรากฎหมาย The Privacy Act ขึ้น โดยเป็นผลมาจากกรณีของคดีวอเตอร์เกต (Watergate) ที่มีการล้วงข้อมูลจากพรรคการเมืองฝ่ายตรงข้ามโดยเจ้าหน้าที่ของรัฐ อันเป็นผลให้เกิดความวิตกกังวลถึงสิทธิในความเป็นส่วนตัวของปัจเจกชนว่าข้อมูลที่ถูกจัดเก็บโดยเจ้าหน้าที่ของรัฐจะถูกนำไปใช้โดยไม่ชอบหรือโดยมิได้อนุญาตจากเจ้าของ ทำให้สภาคองเกรสของสหรัฐจึงได้ตรากฎหมายนี้ขึ้นและได้รับการลงนามโดยประธานาธิบดีเจอรัลด์ ฟอร์ด

---

[108] ชูชีพ ปิณฑะสิริ, **การละเมิดสิทธิส่วนตัว** (วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2525), หน้า 25.

[109] *เรื่องเดียวกัน*.

ในวันที่ 31 ธันวาคม 1974 และมีผลใช้บังคับในวันที่ 27 กันยายน 1975 โดยเจตนารมณ์ของกฎหมายฉบับนี้ ต้องการสร้างสมดุลระหว่างความจำเป็นของรัฐบาลในการมีไว้หรือได้รับข้อมูลส่วนบุคคลเพื่อประโยชน์สาธารณะกับสิทธิเสรีภาพของปัจเจกชนที่จะได้รับความคุ้มครองสิทธิส่วนบุคคลไม่ให้ถูกล่วงล้ำโดยหน่วยงานของรัฐบาลกลางที่ดำเนินการเกี่ยวกับการจัดเก็บ รักษา ใช้ และเปิดเผยข้อมูลส่วนบุคคล อย่างไรก็ดีกฎหมายฉบับนี้ใช้บังคับเฉพาะภาครัฐเทานั้น[110] ไม่ได้รวมไปถึงข้อมูลส่วนบุคคลที่อยู่กับภาคเอกชนแต่อย่างใด

สำหรับการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในภาคเอกชนนั้น สหรัฐอเมริกาใช้วิธีการให้เอกชนกำกับดูแลกันเอง (Self Regurations) โดยจะมีเจ้าหน้าที่ของรัฐ เช่น Federal Trade Commission (FTC) กำกับดูแลอีกชั้นหนึ่ง โดยอยู่บนพื้นฐานความคิดที่ว่า การกำกับดูแลกันเอง (Self Regurations) มีลักษณะยืดหยุ่นกว่า และสามารถแก้ปัญหาได้ทันท่วงทีมากกว่าโดยเฉพาะหากเป็นเรื่องที่เกี่ยวข้องกับเทคโนโลยี[111]

3.1.2 มาตรการทางกฎหมายในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกา

3.1.2.1 ลักษณะและประเภทของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลที่ได้รับความคุ้มครอง

สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล เป็นประโยชน์ที่กฎหมายรับรองและคุ้มครองให้แก่บุคคลซึ่งเป็นเจ้าของในข้อมูล ซึ่งการกำหนดลักษณะและประเภทของสิทธิในความเป็นส่วนตัวจึงเป็นเรื่องสำคัญสำหรับการดำเนินการเพื่อให้ความคุ้มครองเกิดขึ้น

อย่างไรก็ดี ด้วยเหตุที่ประเทศสหรัฐอเมริกาไม่ได้มีกฎหมายกลางที่กำหนดการคุ้มครองเป็นการทั่วไปมีการตรากฎหมายคุ้มครองสิทธินี้ในลักษณะของ Sectoral Law ทำให้มีการกำหนดนิยามของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลที่จะได้รับความคุ้มครองไว้เฉพาะเจาะจงตามกฎหมายแต่ละฉบับ ตัวอย่างเช่น

The Federal Trade Commission Act (15 U.S.C. §§41-58) (FTC Act) ซึ่งพระราชบัญญัติ FTC นี้ ไม่ได้กำหนดประเภทของข้อมูลโดยเฉพาะเจาะจง แต่จะเป็นการห้ามมิให้มี

---

[110] กิตติพงศ์ กมลธรรมวงศ์, *เรื่องเดิม*, หน้า 139.

[111] ประสิทธิ์ ปิวาวัฒนพานิช, *เรื่องเดิม*, หน้า 538-539.

การกระทำที่ไม่เป็นธรรมหรือหลอกลวงหรือการปฏิบัติที่ไม่สามารถปกป้องข้อมูลส่วนบุคคลของผู้บริโภคได้[112]

The Financial Services Modernization Act (Gramm-Leach-Bliley Act (GLB)) (15 U.S.C. §§6801-6827) คุ้มครองสิทธิในข้อมูลส่วนบุคคลที่ไม่ใช่ข้อมูลซึ่งอยู่ในความครอบครองของฝ่ายรัฐ ซึ่งข้อมูลนี้เป็นข้อมูลที่จัดเก็บโดยสถาบันการเงินที่ได้มาโดยผลจากการให้บริการทางการเงิน

The Health Insurance Portability and Accountability Act (HIPAA) (42 U.S.C. §1301 et seq.) กำหนดหลักการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ซึ่งข้อมูลส่วนบุคคลตามกฎหมายฉบับนี้ จะหมายถึงข้อมูลซึ่งเป็นข้อมูลด้านสุขภาพและข้อมูลทางการแพทย์ที่สามารถระบุตัวตนได้ซึ่งจัดทำหรือส่งโดยผู้มีส่วนได้เสียหรือผู้ร่วมธุรกิจ

ในกรณีของกฎหมายระดับมลรัฐที่มีลักษณะเป็น State Privacy Law ขอยกตัวอย่างกรณีของรัฐแคลิฟอร์เนีย ซึ่งมีการตรากฎหมาย The California Security Breach Notification Law และอีกฉบับคือ The California Online Privacy Protection Act (CalOPPA)[113]

The California Security Breach Notification Law กำหนดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลว่า คือ ข้อมูลส่วนบุคคลซึ่งหมายถึงชื่อ หรือชื่อและนามสกุลของบุคคลรวมไปถึงข้อมูลต่อไปนี้อย่างใดอย่างหนึ่งหรือกว่านั้นคือ หมายเลขประกันสังคม หมายเลขใบอนุญาตขับขี่ หมายเลขบัตรประชาชนแคลิฟอร์เนีย หมายเลขบัญชีหมายเลขบัตรเครดิตหรือเดบิตร่วมกับรหัสความปลอดภัยที่จำเป็นรหัสการเข้าถึงหรือรหัสผ่านที่อนุญาตให้เข้าถึงบัญชีการเงินของแต่ละบุคคล ข้อมูลทางการแพทย์ ข้อมูลการประกันสุขภาพ นอกจากนี้ การกำหนดนิยามตามกฎหมายนี้ยังรวมไปถึงข้อมูลส่วนบุคคลไม่ว่าจะเป็นชื่อผู้ใช้หรือที่อยู่อีเมลร่วมกับรหัสผ่านหรือคำถามและคำตอบเพื่อความปลอดภัยซึ่งจะช่วยให้สามารถเข้าถึงบัญชีออนไลน์ได้ ข้อมูลส่วนบุคคลไม่ได้รวมถึงข้อมูลที่เปิดเผยต่อสาธารณชนที่ได้รับการเผยแพร่ต่อสาธารณชนอย่างถูกต้องตามกฎหมายจากระเบียนของรัฐบาลกลางรัฐหรือท้องถิ่น

---

[112] Ieuan Jolly, **Data Protection in the United States: Overview**, Retrieved May 15, 2018 from https://uk.practicallaw.thomsonreuters.com/6-502-0467?TransitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1

[113] California Online Privacy Protection Act (CalOPPA) เป็นเป็นกฎหมายของมลรัฐฉบับแรกในประเทศสหรัฐอเมริกา ที่กำหนดให้เว็บไซต์ของธุรกิจและบริการต่าง ๆ ต้องเขียนนโยบายคุ้มครองข้อมูลส่วนบุคคลบนเว็บไซต์ของตน โดย CalOPPA นั้นมีผลบังคับใช้ครั้งแรกในปี 2004 และได้มีการแก้ไขอีกครั้งในปี 2013

ส่วน The California Online Privacy Protection Act ซึ่งเป็นกฎหมายที่รู้จักกันในลักษณะของกฎหมายที่บังคับให้ธุรกิจและบริการที่มีการเก็บรวบรวมข้อมูลส่วนบุคคล (PII) ต้องเปิดเผยนโนบายด้านข้อมูลส่วนบุคคลออนไลน์ (Disclosure of their Online Privacy Policy) โดยข้อกำหนดตาม CalOPPA นั้น เจ้าของธุรกิจหรือบริการสามารถเปิดเผยนโยบายข้อมูลส่วนบุคคลได้ 3 วิธีดังนี้คือ ประการที่หนึ่ง โดยการขึ้นนโยบายด้านข้อมูลส่วนบุคคลไว้บนหน้าแรกของเว็บไซต์ ประการที่สอง โดยการใส่ Link บนไอคอนที่มีคำว่า “Privacy” บนหน้าแรกของเว็บไซต์ หรือ ประการที่สาม โดยการใส่ลิงค์ผ่าน Hypertext ที่มีคำว่า PRIVACY ตัวพิมพ์ใหญ่ขนาดใหญ่กว่าหรือเท่ากับข้อความอื่น ๆ ในหน้าแรกของเว็บไซต์นั้น ๆ โดยหากไม่ทำตามข้อกำหนดดังกล่าว องค์กรธุรกิจก็อาจจะสูญเสียโอกาสในการเข้าถึงลูกค้าที่อยู่อาศัยในมลรัฐแคลิฟอร์เนีย

กฎหมาย CalOPPA กำหนดนิยามระบุสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ว่าเป็นสิทธิที่เกี่ยวกับข้อมูลส่วนบุคคล หรือ Personally Identifiable Information (PII) ตาม CalOPPA ซึ่งคำว่าข้อมูลส่วนบุคคลคลนั้น หมายถึง ข้อมูลที่ถูกรวบรวมผ่านทางอินเตอร์เน็ตโดยเป็นข้อมูลที่เกี่ยวกับผู้บริโภคโดยรวมถึง ชื่อ นามสกุล ที่อยู่ อีเมล์ เบอร์โทรศัพท์ หมายเลขประจำตัวตามฐานข้อมูลทะเบียนราษฎร์ สิ่งใด ๆ ที่อาจใช้ในการระบุตัวตนของผู้ใช้ โดยรวมถึงวันเกิด ส่วนสูง น้ำหนัก สีผม ที่ถูกถามและเก็บรวบรวมออนไลน์

ประเด็นคำถามที่น่าสนใจก็คือ ในประเทศสหรัฐอเมริกาได้มีการกำหนดประเภทของข้อมูลส่วนบุคคลไว้ เช่นเดียวกันกับประเทศภาคพื้นยุโรปที่ได้มีการกำหนดประเภทของข้อมูลส่วนบุคคลทั่วไป และข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) ไว้ในกฎหมายกลางหรือไม่ ซึ่งในประเด็นนี้ คำตอบก็คือ แม้ไม่มีกฎหมายกลาง แต่ในกฎหมายเฉพาะบางฉบับของสหรัฐอเมริกาก็มีการกำหนดลักษณะของข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) ตัวอย่างเช่น ในกฎหมาย The Health Insurance Portability and Accountability Act (HIPAA) มีกฎเกณฑ์ระบุเกี่ยวกับการคุ้มครองข้อมูลที่เป็นบันทึกการบำบัดด้วยวิธีการจิตบำบัด ซึ่งจะต้องได้รับอนุญาตตามกฎหมายเป็นลายลักษณ์อักษรก่อนจะเปิดเผยข้อมูลส่วนบุคคลประเภทนี้แม้กระทั่งว่าจะเป็นการเปิดเผยเพื่อวัตถุประสงค์ในทางการแพทย์หรือการชำระเงินค่ารักษาพยาบาลก็ตาม

จึงกล่าวได้ว่าการกำหนดประเภทของข้อมูลส่วนบุคคลมีความแตกต่างกันไปตามแต่ละมลรัฐและตามประเภทของกฎหมาย โดยทั่วไปข้อมูลสุขภาพส่วนบุคคล ข้อมูลทางการเงิน ข้อมูลเกี่ยวกับบัตรเครดิต ข้อมูลนักเรียน, ข้อมูลส่วนบุคคลที่รวบรวมออนไลน์จากเด็กอายุต่ำกว่า 13 ปีและข้อมูลที่สามารถนำไปใช้ในการโจรกรรมข้อมูลหรือการฉ้อฉลถือเป็นเรื่องสำคัญ ตัวอย่างเช่นการแจ้งข้อมูลการละเมิดความปลอดภัยข้อมูลของสหรัฐฯและกฎหมายด้านความปลอดภัยข้อมูลของรัฐมักใช้ชื่อบวกหมายเลขประจำตัวประชาชน, บัญชีการเงินหรือหมายเลขบัตรการชำระเงินและในบางรัฐการ

ประกันสุขภาพทางการแพทย์และ / หรือข้อมูลไบโอเมตริกซ์และชื่อผู้ใช้และรหัสผ่านสำหรับบัญชีออนไลน์

3.1.2.2 หลักการและข้อจำกัดในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล

หลักการคุ้มครองสิทธิความเป็นส่วนตัว (The Right to Privacy) นับแต่บทความเรื่อง The Right to Privacy ของ Louis D. Brandeis และ Samuel D. Warren ก็ได้มีพัฒนาอย่างต่อเนื่อง ในปี ค.ศ.1960 Dean William Prosser ได้ทำการศึกษาแนวคำพิพากษาในคดีต่าง ๆ โดยแบ่งการละเมิดสิทธิความเป็นส่วนตัว (Violation of the Right to Privacy) ออกเป็น 4 ประเภท[114] และต่อมาได้ถูกพัฒนาและทำการรวบรวมจากสถาบันกฎหมายอเมริกัน (American Law Institute) ที่เป็นสถาบันที่ทำการรวบรวมกฎหมายจารีตประเพณี (Common Law) เข้าไว้ด้วยกันและทำการสังเคราะห์ออกเป็นหลักกฎหมายทั่วไปซึ่งมีลักษณะคล้ายประมวลกฎหมาย แม้จะไม่มีผลบังคับใช้แต่ก็ได้รับการอ้างอิงจากศาลทั่วสหรัฐอเมริกา[115]

กฎหมายจารีตประเพณี (Common Law) ที่เกี่ยวกับละเมิดที่ได้รวมเข้าไว้ด้วยกันและทำการสังเคราะห์นี้เรียกว่าบัญญัติเป็นกฎหมายลักษณะละเมิด (The Restatement (Second) of Torts) ซึ่งได้มีการกำหนดหลักทั่วไปของการละเมิดสิทธิความเป็นส่วนตัว (Violation of The Right to Privacy) ไว้ในมาตรา 652A ไว้ว่า[116]

---

[114] กุลพล พลวัน, แนวความคิดเกี่ยวกับเสรีภาพสื่อมวลชนในการแสวงหาข่าวสาร, ใน **เอกสารการสอนชุดวิชากฎหมายและจริยธรรมสื่อสารมวลชน หน่วยที่ 8** (นนทบุรี: มหาวิทยาลัยสุโขทัยธรรมธิราช, 2529), หน้า 4.

[115] คณาธิป ทองรวีวงศ์, **รายงานการวิจัยฉบับสมบูรณ์ เรื่องการปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน**, หน้า 99.

[116] The Restatement (second) of Torts

Article 652A. General Principle

(1) One who invades the right of privacy of another is subject to liability for the resulting harm to the interests of the other.

(2) The right of privacy is invaded by:

(a) unreasonable intrusion upon the seclusion of another, as stated in 652B; or

(b) appropriation of the other's name or likeness, as stated in 652C; or

(1) ผู้ใดทำการก้าวล่วงสิทธิในความเป็นส่วนตัวของผู้อื่นจะต้องรับผิดในความเสียหายที่เกิดขึ้น

(2) การละเมิดสิทธิในความเป็นส่วนตัวมี 4 ประเภท ดังนี้

(a) การแทรกแซงความสันโดษของผู้อื่นโดยปราศจากเหตุผลอันควรตามมาตรา 652B

(b) การแสวงหาประโยชน์จากชื่อหรือลักษณะของผู้อื่นโดยมิได้รับความยินยอมตามมาตรา 652C

(c) การเปิดเผยเรื่องราวส่วนตัวของผู้อื่นต่อสาธารณชน ตามมาตรา 652D

(d) การเผยแพร่ซึ่งทำให้ผู้อื่นเสื่อมเสียในสายตาของสาธารณชน ตามมาตรา 652E

โดยจากหลักการข้างต้นก็ได้มีคำพิพากษาของศาลในระบบคอมมอนลอว์ตัดสินออกมาเป็นบรรทัดฐานในการคุ้มครองสิทธิในความเป็นส่วนตัวมากกมาย แต่อย่างไรก็ดี ในบางกรณีศาลก็ได้ตัดสินวางหลักการว่าสามารถแทรกแซงสิทธิความเป็นส่วนตัวโดยชอบด้วยกฎหมาย

คดี Pavesich v. New England Life Insurance Co. et al. ที่โจทก์ได้ทำการฟ้องบริษัทประกันภัยที่นำภาพถ่ายของโจทก์ไปใช้ในการโฆษณาโดยโจทก์มิได้ยินยอม โดยศาลได้พิพากษาถึงสิทธิความเป็นส่วนตัวย่อมได้รับการยอมรับว่าเป็นสิทธิตามกฎหมายทั้งนี้โดยอยู่ในขอบเขตที่เหมาะสม การนำภาพของผู้อื่นไปพิมพ์โดยมิได้รับความยินยอมเพื่อวัตถุประสงค์ทางการค้าย่อมเป็นการละเมิดสิทธิความเป็นส่วนตัว และยังได้พิพากษาต่อไปว่า สิทธิความเป็นส่วนตัวนั้นอาจสละได้ด้วยเจตนาของผู้เป็นเจ้าของสิทธิ รวมถึงข้อจำกัดของสิทธิความเป็นส่วนตัวไว้ว่า คือ การใช้สิทธิความเป็นส่วนตัวที่ไม่กระทบกระเทือนสิทธิความเป็นส่วนตัวของผู้อื่น และในบางกรณีสิทธิของสาธารณะจะมาก่อนและอยู่เหนือกว่าสิทธิความเป็นส่วนตัวในกรณีที่เกี่ยวกับผลประโยชน์สาธารณะ[117]

(c) unreasonable publicity given to the other's private life, as stated in 652D; or

(d) publicity that unreasonably places the other in a false light before the public, as stated in 652E.

[117] นพมาศ เกิดวิชัย, *เรื่องเดิม*, หน้า 74-75.

3.1.2.3 กลไกทางกฎหมายในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล

สำหรับกลไกทางกฎหมายในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกานั้น ประกอบไปด้วยรัฐธรรมนูญแห่งสหรัฐ บทบัญญัติในระดับมลรัฐ และกฎหมายคอมมอนลอว์ ที่เกี่ยวกับละเมิดที่ได้กล่าวไว้แล้วในหัวข้อก่อน ซึ่งกฎหมายที่ตราขึ้นมาเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนั้นมีรูปแบบการตราดังนี้[118]

1. กฎหมายของรัฐบาลกลาง ที่มีการตราขึ้นหลายฉบับเพื่อใช้ควบคุมการใช้ข้อมูลข่าวสารโดยไม่จำกัดว่าจะต้องเป็นข้อมูลข่าวสารที่มีการจัดเก็บไว้ด้วยเครื่องมืออัตโนมัติหรือไม่

2. การตรากฎหมายเพื่อควบคุมการใช้ข้อมูลข่าวสารแบ่งได้เป็นสองระดับ คือ กฎหมายที่ตราขึ้นเพื่อชี้บังคับกับภาครัฐหรือองค์กรของรัฐบาลกลาง และกฎหมายที่ตราขึ้นเพื่อใช้บังคับกับภาคเอกชน

3. กฎหมายที่ตราขึ้นเพื่อใช้ควบคุมการใช้ข้อมูลส่วนบุคคลที่มีลักษณะการบัญญัติขึ้นโดยแบ่งแยกตามประเภทของกิจการ ดังนั้น บทบัญญัติที่ใช้ควบคุมการใช้ข้อมูลส่วนบุคคลจึงกระจายอยู่ตามกฎหมายซึ่งควบคุมกิจการเป็นเรื่อง ๆ ไป

ดังนั้นจึงกล่าวได้ว่า บ่อเกิดของกฎหมายที่คุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกานั้นประกอบด้วยหลักเกณฑ์โดยสรุปดังนี้[119]

1. รัฐธรรมนูญและคำวินิจฉัยของศาลสูง

แม้บทบัญญัติของรัฐธรรมนูญสหรัฐอเมริกาจะมิได้บัญญัติรับรองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลไว้อย่างชัดเจนเหมือนกับประเทศไทยของเรา แต่อย่างไรก็ดี ศาลสูงของสหรัฐก็ได้ทำให้หน้าที่สร้างหลักการโดยคำพิพากษาเพื่อคุ้มครองสิทธินี้ ตัวอย่างเช่นคดี Whalen & Roe ที่ศาลได้ตัดสินวางหลักการคุ้มครองสิทธิในข้อมูลส่วนบุคคลของคนไข้ ซึ่งกฎหมายของมลรัฐนิวยอร์คได้กำหนดว่า แพทย์ต้องส่งสำเนาเกี่ยวกับใบสั่งยาในการใช้ยาโดยมิชอบของคนไข้แก่รัฐเพื่อทำการประมวลผลในเครื่องคอมพิวเตอร์กลาง ซึ่งศาลสูงได้ตัดสินว่า การกระทำดังกล่าวเป็นการละเมิดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของคนไข้

---

[118] กงจักร โพธิพร้อม, **ปัญหาทางกฎหมายมหาชนบางประการเกี่ยวกับการควบคุมการใช้ข่าวสารโดยเครื่องคอมพิวเตอร์** (วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2529), หน้า 27.

[119] ประสิทธิ ปิวาวัฒนพาณิชย์, *เรื่องเดิม*, หน้า 539-541.

2. กฎหมายของสหพันธรัฐ

ประเทศสหรัฐอเมริกาไม่มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่มีลักษณะเป็นการทั่วไปครอบคลุมเป็นเอกรูปอย่างเช่นสหภาพยุโรป แต่มีลักษณะเป็นกฎหมายเฉพาะเป็นเรื่อง ๆ ไป ไม่มีกฎหมายที่กำหนดมาตรฐานกลางหรือกฎหมายแม่บท ที่วางหลักการคุ้มครองข้อมูลส่วนบุคคลไว้ ดังนั้น กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหรัฐอเมริกาจึงมีอยู่หลายฉบับกระจัดกระจายไปยกตัวอย่างได้ดังนี้

- Privacy Act 1974
- Bank Secrecy Act 1974
- Communication Peivacy Act of 1984 (Cable Act)
- Health Care Quality Improvement Act of 1986
- Children’s online Privacy Act
- Electronic Communication Privacy Act
- Video Privacy Protection Act
- The Driver Privacy Protection Act 1994
- The Computer Matching Protection Act 1988
- The Telephone Consumer Protection Act 1991

3. กฎหมายของมลรัฐ

- Massachusetts Physician Profile Act 1996

4. คำพิพากษาของศาลในคดีละเมิด

- การละเมิดความต้องการอยู่คนเดียวโดยปราศจากการรบกวน
- การเปิดเผยของมูลส่วนตัวต่อสาธารณะ
- การใช้ชื่อหรือสิ่งที่คล้ายคลึงกันโดยมิชอบ

นอกจากหลักการดังกล่าวข้างต้น ประเทศสหรัฐอเมริกายังได้ทำความตกลงกับสหภาพยุโรป ที่เรียกว่า Safe Harbor หรือ Safe Harbor Privacy Principles อันเป็นผลมาจากการที่สหภาพยุโรปได้ประกาศใช้ The European Commission’s Directive on Data Protection เมื่อวันที่ 25 ตุลาคม 1998 อันเป็นการสร้างมาตรฐานในการคุ้มครองสิทธิในความเป็นส่วนตัวอันเกี่ยวกับข้อมูลส่วนบุคคลให้แก่บุคคลซึ่งเป็นพลเมืองของประเทศสมาชิกจากการละเมิดโดยประเทศที่ไม่มีมาตรการเพียงพอ ซึ่งจะมีการกำหนดกลไกสำคัญประการหนึ่งคือ ข้อบังคับนี้เปิดโอกาสให้

ประเทศสมาชิกยับยั้งหรือห้ามมิให้มีการส่งข้อมูลไปยังประเทศที่ไม่มีมาตรฐานหรือไม่มีบทบัญญัติที่ให้การคุ้มครองข้อมูลส่วนบุคคลอย่างเพียงพอ[120]

ในความเป็นจริงทั้งประเทศสหรัฐอเมริกาและประเทศในกลุ่มสหภาพยุโรปนั้น ต่างมีความมุ่งมั่นที่จะคุ้มครองสิทธิในความเป็นส่วนตัวของประชาชนของประเทศตนเช่นเดียวกัน แต่เนื่องจากประเทศสหรัฐอเมริกามีแนวทางการดำเนินการที่แตกต่างจากประเทศยุโรป โดยประเทศสหรัฐอเมริกามีบทบัญญัติคุ้มครองความเป็นส่วนตัวในลักษณะที่แยกเป็นส่วน ๆ กล่าวคือ กฎเกณฑ์การคุ้มครองนั้นกระจัดกระจายไปตามกฎเกณฑ์ ข้อบังคับ หลาย ๆ ฉบับ ที่จำกัดเฉพาะเรื่องที่บทบัญญัติดังกล่าวมีวัตถุประสงค์มุ่งคุ้มครอง ส่วนการควบคุมดูแลนั้น ในประเทศสหรัฐอเมริกานั้นเลือกใช้ระบบการกำกับดูแลตนเอง (Self-Regulation) โดยให้ภาคเอกชนกำกับดูแลและควบคุมกันเองเป็นสำคัญ ซึ่งจะแตกต่างจากประเทศในสหภาพยุโรปที่ใช้ระบบให้มีกฎหมายกลางในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล[121] ซึ่งในการนี้ทำให้ประเทศสหภาพยุโรปมองว่า ประเทศสหรัฐอเมริกาไม่มีกฎหมายกลางที่เป็นมาตรฐานขั้นต่ำสำหรับคุ้มครองอันเป็นมาตรฐานที่เพียงพอตามที่สหภาพยุโรปกำหนด

ความแตกต่างนำมาสู่ความขัดแย้งระหว่างกันอย่างมากเพื่อแก้ปัญหาและบรรเทาความขัดแย้งที่เกิดขึ้นสหรัฐอเมริกา โดยกระทรวงพาณิชย์ได้ประชุมปรึกษาหารือและทำความตกลงกับสภาพยุโรป และได้จัดทำความตกลงเพื่อเป็นกรอบแห่งการปฏิบัติ เรียกว่า Safe Harbor Privacy Principles (Safe Harbor) ซึ่งหลักการดังกล่าวได้มีผลบังคับใช้ในปี 2000

สาระสำคัญของความตกลงดังกล่าวก็คือ จะมีการอนุญาติให้มีการส่งข้อมูลระหว่างกันได้ก็ต่อเมื่อ ผู้ประกอบการภายในประเทศสหรัฐเมริกาได้เข้าร่วมโครงการ Safe Harbor แล้วโดยจะต้องปฏิบัติตามหลักการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนตามที่กำหนดใน Safe Harbor ทุกประการด้วย หรือในกรณีที่ผู้ประกอบการภายในประเทศสหรัฐอเมริกาสามารถแสดงให้เห็นได้ว่าตนเองมีมาตรการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่มีมาตรฐานเพียงพอ โดยการจัดทำนโยบายการคุ้มครองส่วนบุคคลให้สอดคล้องกับหลักเกณฑ์ของ Safe Harbor ซึ่งมี 7 ประการดังนี้[122]

---

[120] นคร เสรีรักษ์, *เรื่องเดิม*, หน้า 165-166.

[121] *เรื่องเดียวกัน*, หน้า 166.

[122] ธนัท สุวรรณปริญญา, **ปัญหาทางกฎหมายเกี่ยวกับการค้มุครองข้อมลูส่วนบคุคลบนธุรกรรมทางอิเล็กทรอนิกส์** (สารนิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยกรุงเทพ, 2550), หน้า 45-49.

1. Notice การแจ้งให้ทราบเกี่ยวกับวัตถุประสงค์ของการจัดเก็บข้อมูลส่วนบุคคล การแจ้ง ให้ทราบเกี่ยวกับวิธีการติดต่อกับผู้ประกอบการเพื่อติดต่อสอบถามหรือเพื่อการทำข้อร้องเรียน การแจ้งข้อมูลเกี่ยวกับประเภทของบุคคลที่สามที่อาจได้รับการเปิดเผยข้อมูลส่วนบุคคล รวมทั้ง ทางเลือกและวิธีการในการจำกัดการใช้หรือการเปิดเผยข้อมูลส่วนบุคคล

2. Choice ผู้ประกอบการจะต้องมีการเสนอทางเลือกให้บุคคลตัดสินใจว่าจะให้ข้อมูลส่วนบุคคลของตน ถูกเปิดเผยต่อบุคคลที่สามหรือถูกนำไปใช้ภายใต้วัตุประสงค์อื่น ๆ และผู้ประกอบการจะต้องจัดเตรียมวิธีการ หรือกลไกที่ชัดเจนที่จะแสดงให้บุคคลสามารถใช้สิทธิในการเลือกให้ข้อมูลส่วนบุคคลได้ โดยเฉพาะในกรณีที่เป็นข้อมูลที่อ่อนไหว (Sensitive) บุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลต้องสามารถที่จะเลือกได้ว่าจะอนุญาตให้ผู้ประกอบการสามารถเปิดเผยต่อบุคคลที่สามได้หรือไม่และเป็นไปเพื่อวัตถุประสงค์ใด

3. Onward Transfer ในการโอนถ่ายข้อมูลส่วนบุคคลไปยังบุคคลที่สามซึ่งผู้ประกอบการจะต้องปฏิบัติตามหลักการ Notice และ Choice อย่างเคร่งครัด การโอนถ่ายข้อมูลไปยังตัวแทนของผู้ประกอบการซึ่งเป็นผู้ถ่ายโอนข้อมูลอาจจะไม่ต้องปฏิบัติตามหลักการ Notice และ Choice ก็ได้ ถ้าหากตัวแทนของผู้ประกอบการนั้น ได้ปฏิบัติตาม Safe Harbor Principles หรือได้ทำสัญญาเป็นลายลักษณะอักษรในเรื่องการคุ้มครองข้อมูลส่วนบุคคลกับผู้ประกอบการนั้นแล้ว

4. Security ผู้ประกอบการที่สร้าง เก็บรักษา ใช้ หรือเผยแพร่ข้อมูลส่วนบุคคลจะต้องมี ระบบรักษาความปลอดภัยที่เหมาะสมเพื่อคุ้มครองข้อมูลส่วนบุคคลไม่ให้สูญหาย ถูกนำไปใช้ผิดวัตถุประสงค์ หรือการเข้าถึงการเปิดเผยข้อมูลโดยปราศจากอำนาจ รวมทั้งการเปลี่ยนแปลง แก้ไข และการทำลายข้อมูลส่วนบุคคลด้วย และผู้ประกอบการจะต้องมีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นพิเศษ

5. Data Integrity การเก็บรักษา ใช้ หรือเผยแพร่ข้อมูลส่วนบุคคลจะต้องเป็นไปเพื่อ และสอดคล้องกับวัตถุประสงค์ที่ผู้ประกอบการได้แจ้งไว้เท่านั้น ผู้ประกอบการจะต้องไม่เก็บรักษา ใช้ หรือเผยแพร่ข้อมูลส่วนบุคคลในลักษณะที่ขัดกับวัตถุประสงค์ในการจัดเก็บ หรือนอกเหนือไปจากที่เจ้าของข้อมูลอนุญาตไว้ ในกรณีที่มีความจำเป็นจะต้องนำข้อมูลส่วนบุคคลไปใช้เพื่อวัตถุประสงค์ต่าง ๆ ผู้ประกอบการจะต้องดำเนินการตามขั้นตอนที่เหมาะสมเพื่อให้แน่ใจว่าข้อมูลนั้นมีความสมบูรณ์ ถูกต้อง เชื่อถือได้ สำหรับนำไปใช้เพื่อวัตถุประสงค์นั้น ๆ

6. Access ผู้ใช้บริการต้องมีวิธีการ และสามารถเข้าถึงข้อมูลส่วนบุคคลของตนได้และสามารถแก้ไข เปลี่ยนแปลงข้อมูลส่วนบุคคลให้ถูกต้องได้ ยกเว้นในกรณีที่มีภาระความเสียง หรือค่าใช้จ่ายที่เกิดขึ้น เนื่องจากการจัดการวิธีการเข้าถึงข้อมูลต่าง ๆ จะมีความเสี่ยงที่จะละเมิดสิทธิของบุคคลอื่นมากกว่า

7. Enforcement ผู้ประกอบการจะต้องมีกลไกการบังคับใช้ที่เหมาะสม จะต้องมีการติดตาม ถึงขั้นตอนการรับนโยบายและกลไกของ Safe Harbor ว่ามีความเหมาะสมและบรรลุผลตาม วัตถุประสงค์ Safe Harbor รวมทั้งจัดให้มีระบบการระงับข้อพิพาทที่เป็นอิสระ เพื่อแก้ปัญหาและข้อร้องเรียนของผู้ใช้บริการ และมีการจัดระบบชดใช้ค่าเสียหาย โดยมีหน้าที่ในการเยียวยาปัญหาจากการ ที่ผู้ประกอบการเองไม่ได้ปฏิบัติตาม Safe Harbor ด้วย

สำหรับการตัดสินของบริษัทผู้ประกอบการหรือองค์กรต่าง ๆ ที่จะเข้าร่วมกับโครงการ Safe Harbour นั้น เป็นไปด้วยความสมัครใจทั้งหมด (Voluntary) โดยบริษัทผู้ประกอบการหรือองค์กรต่าง ๆ สามารถปรับตัวเพื่อให้มีคุณสมบัติเหมาะสมสอดคล้องกับหลักการทั้ง 7 ประการของโครงการ Safe Harbour ได้ด้วยวิธีที่แตกต่างกัน ซึ่งบริษัทผู้ประกอบการหรือองค์กรสามารถเลือกที่จะดำเนินการในทางใดทางหนึ่ง ดังนี้[123]

1. เข้าร่วมโครงการกลไกกำกับดูแลตนเองที่มีหลักการสอดคล้องกับหลักเกณฑ์ของ Safe Harbourเช่น เข้าร่วมเป็นสมาชิกขององค์กรให้บริการเครื่องหมายรับรองการคุ้มครองข้อมูลส่วน บุคคล (Third Party Self–Regulatory Programs) ซึ่งผ่านการรับรองจากคณะกรรมาธิการยุโรปแล้วว่าสามารถบังคับให้มีการปฏิบัติตามกลไกกำกับดูแลตนเองขององค์กรดังกล่าวโดยอย่างมีประสิทธิภาพ อาทิ Trustedและ WEB Trust เป็นต้น

2. จัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของตนเองที่สอดคล้องกับหลักเกณฑ์ของ Safe Harbour

สำหรับข้อยกเว้นของโครงการ Safe Harbour นั้นมีการกำหนดให้องค์กรหรือหน่วยงานต่าง ๆ จะต้องปฏิบัติตามหลักการคุ้มครองข้อมูลส่วนบุคคลของโครงการ Safe Harbour แต่อย่างไรก็ตามโครงการ Safe Harbour ได้กำหนดข้อยกเว้นหรือจำกัด ให้ไม่จำต้องปฏิบัติตามหลักการคุ้มครองข้อมูลส่วนบุคคลได้เอาไว้ใน Safe Harbour Privacy Principles วรรคสาม ซึ่งได้แก่กรณีดังต่อไปนี้[124]

1) มีความจำเป็นสำหรับความมั่นคงของชาติ สาธารณประโยชน์ หรือสอดคล้องกับข้อกำหนดการบังคับใช้กฎหมาย

2) มีพระราชบัญญัติระเบียบของราชการหรือกฎหมายที่มาจากบรรทัดฐาน คำพิพากษาของศาล ซึ่งได้สร้างข้อผูกพันที่ขัดแย้งกับหลักการ Safe Harbour รวมไปถึงการให้อำนาจตามกฎหมายอย่างชัดแจ้ง (Explicit Legal Authorisations) โดยองค์กรต้องแสดงให้เห็นได้ว่าการฝ่า

---

[123] คณาธิป ทองวีรวงศ์, **รายงานการวิจัยฉบับสมบูรณ์ เรื่องการปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน,** หน้า 73-74.

[124] *เรื่องเดียวกัน*, หน้า 75.

ฝืนหลักของโครงการ Safe Harbour ถูกจำกัดอยู่ในขอบเขตที่ไม่ละเมิดผลประโยชน์อันชอบด้วยกฎหมายที่มี ความสำคัญสูงสุดซึ่งเสริมขึ้นมาจากการให้อำนาจนั้น

3) Directive หรือ กฎหมายของประเทศสมาชิกอนุญาตให้มีข้อยกเว้นหรือการหลีกเลี่ยงไม่ทำตามกฎได้ โดยมีเงื่อนไขว่าข้อยกเว้นหรือการหลีกเลี่ยงไม่ทำตามกฎนั้น ๆ ต้องถูกนำมาใช้ในบริบทที่คล้ายกันองค์กรต่าง ๆ ควรมุ่งมั่นที่จะปฏิบัติตามหลักของโครงการ Safe Harbour อย่างเต็มที่และโปร่งใส โดยยังคงเปูาหมายที่จะยกระดับการคุ้มครองความเป็นส่วนตัวอย่างสม่ำเสมอ และระบุในนโยบายคุ้มครองความเป็นส่วนตัวกรณีที่จะมีการนำข้อยกเว้นที่ได้รับความเห็นชอบตามข้อ 2) มาใช้เป็นประจำด้วย

ด้วยเหตุผลเดียวกันในกรณีที่ทางเลือกนั้นสามารถกระทำได้ภายใต้หลักของโครงการ Safe Harbor และ/หรือ กฎหมายสหรัฐ องค์กรนั้น ๆ จะต้องเลือกทางเลือกที่สามารถให้การคุ้มครองข้อมูลส่วนบุคคลได้สูงสุดเท่าที่จะเป็นไปได้[125]

ในส่วนของการบังคับให้เป็นไปตามหลักการ Safe Harbor ดังกล่าวข้างต้นจะมีองค์กรที่ทำหน้าที่รับผิดชอบคือ Federal Trade Commission (FTC) ในการกำกับดูแลและควบคุมให้องค์กร หรือสมาคมต่าง ๆ ในภาคเอกชน ปฏิบัติตาม Self Regulation ของตนอย่างเคร่งครัด ซึ่ง FTC จะเป็นองค์กรของรัฐที่ทำหน้าที่บังคับการให้เป็นไปตาม Safe Harbor Privacy Principles ซึ่งในกรณีที่มีการไม่ปฏิบัติตามหลักการ หรือละเมิดหลักการไม่ว่าทั้งหมดหรือแต่บางส่วน FTC มีอำนาจสั่งให้หยุดหรือระงับการกระทำที่ไม่เป็นธรรมได้ ซึ่งกรณีเหล่านี้จะถูกดำเนินคดีภายใต้กฎหมายแห่งสหรัฐอเมริกาหรือกฎหมายของมลรัฐต่าง ๆ ได้[126]

นอกจาก FTC แล้วในกลไกการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนั้นยังมีองค์กรตรวจสอบอื่น ๆ อีกตามกฎหมายฉบับต่าง ๆ ที่กำหนดการคุ้มครองเป็นเรื่อง ๆ ไป ซึ่งได้แก่องค์กรต่าง ๆ ดังนี้[127]

1. The Office of Management and Budget (OMB) เป็นหน่วยงานที่กำกับดูแล ให้คำอธิบายและแนวทางในการปฏิบัติแก่ส่วนราชการในการบังคับใช้ Privacy Act โดยมีหน้าที่สำคัญคือการออก Guidelines ในการคุ้มครองข้อมูลส่วนบุคคล (โดยเฉพาะอย่างยิ่งในมิติของการบันทึกข้อมูลส่วนบุคคลโดยภาครัฐ) และข้อบังคับต่าง ๆ เพื่อให้หน่วยงานรัฐได้ปฏิบัติตาม และทำหน้าที่ช่วยเหลือและดูแลการปฏิบัติตาม Guidelines ดังกล่าว

---

[125] *เรื่องเดียวกัน*

[126] นคร เสรีรักษ์, *เรื่องเดิม*, หน้า 168-169.

[127] ประสิทธิ์ ปิวาวัฒนพานิช, *เรื่องเดิม*, หน้า 542-543.

2. The National Practitioner Data Bank (NPDB) และThe National Telecommunications and Information Administration (NTIA) เป็นหน่วยงานที่ทำหน้าที่ให้คำปรึกษาแนะนำแก่ผู้ให้บริการโทรคมนาคม (Service Providers) ในการทำ Self-Regurations ไม่ว่าจะเป็นการออกกฎเกณฑ์ แนวปฏิบัติหรือประมวลจริยธรรมเพื่อกำกับดูแลกันเองโดยภาคเอกชนเกี่ยวกับการเปิดเผยข้อมูลส่วนบุคคล

3. The Social Security Administration (SSA) เป็นหน่วยงานที่ดูแลเกี่ยวกับการประกันสังคมจึงมีหน้าที่ในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของผู้ประกันตนภายใต้หลักการของรัฐธรรมนูญและ Privacy Act

4. The Internal Revenue Service (IRS) ทำหน้าที่คุ้มครองและกำกับดูแลสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของผู้เสียภาษีอากร

5. The Federal Reserve Board ทำหน้าที่กำกับดูแลสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประชาชนในกรณีข้อมูลเกี่ยวกับการเงินการธนาคารที่อยู่กับธนาคารพาณิชย์ต่าง ๆ

6. The Office of Consumer Affairs ทำหน้าที่คุ้มครองและกำกับดูแลสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของผู้บริโภค

7. Department of Health and Human Services ทำหน้าที่กำกับดูแลตามข้อมูลส่วนบุคคลเกี่ยวกับการแพทย์ ตามกฎหมาย Health Insurance Portibility and Accountability Act

8. คณะกรรมการย่อยชุดต่าง ๆ ในสภาคองเกรส ซึ่งจะทำหน้าที่กำกับการคุ้มครองข้อมูลส่วนบุคคลของประชาชนในภาพรวม ในฐานะหน่วยงานส่วนหนึ่งของรัฐสภา

นอกเหนือจากองค์กรของฝ่ายบริหารข้างต้นนี้แล้ว องค์กรฝ่ายตุลาการในระดับ District Court ก็มีบทบาทในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในสหรัฐอเมริกาเป็นอย่างมาก ไม่ว่าจะเป็นเรื่องของการลงโทษผู้ที่ละเมิดและกำหนดค่าเสียหายแก่ผู้ที่ละเมิดสิทธิในความเป็นส่วนตัวตามกฎหมายแต่ละฉบับ ซึ่งกฎหมายที่คุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลทุกฉบับยอมรับทั้งค่าเสียหายตามความเป็นจริง และค่าเสียหายเชิงลงโทษไว้ ซึ่งจะเป็นดุลพินิจขององค์กรศาล

อย่างไรก็ดี เนื่องจากโครงการ Safe Harbor มีวัตถุประสงค์เพื่อรองรับการถ่ายโอนข้อมูลจากลุ่มประเทศสมาชิกสหภาพยุโรปเพื่อประโยชน์ในการประกอบธุรกิจการค้าการลงทุนของภาคเอกชนเป็นหลักองค์กรที่มีอำนาจในการบังคับการกรณีที่เกิดการปฏิบัติที่ไม่เป็นไปตามหลักการ Safe Harbour จึงมุ่งเน้นเพื่อการไกล่เกลี่ยและระงับข้อพิพาททางการค้าเป็นหลักกลไกในการแก้ไขข้อพิพาทและการจัดการในกรณีที่องค์กรล้มเหลวในการปฏิบัติตามหลักการโครงการ Safe Harbour ติดต่อกันหลายครั้งนั้นสามารถทำได้หลากหลายรูปแบบ แต่ทั้งหมดนั้นต้องเป็นไปตามข้อกำหนดตาม

หลักการใน FAQ ว่าด้วยการพิสูจน์การปฏิบัติตามกฎองค์กรต่าง ๆ อาจปฏิบัติตามข้อกำหนดเหล่านั้นได้ผ่านวิธีดังต่อไปนี้คือ[128]

1. การปฏิบัติตามแผนงานคุ้มครองความเป็นส่วนตัวที่พัฒนาขึ้นโดยภาคส่วนเอกชนซึ่งได้รวมหลักการของโครงการ Safe Harbour ไว้ในกฎระเบียบของโครงการและมีวิธีการบังคับใช้ที่มีประสิทธิภาพตามที่ได้กำหนดไว้ในหลักการบังคับใช้

2. การร่วมมือกับหน่วยงานควบคุมระเบียบกฎหมายที่จัดเตรียมวิธีรับมือกับ ข้อร้องเรียนจากปัจเจกบุคคลและวิธีการแก้ไขข้อพิพาทให้ได้

3. ข้อผูกมัดที่จะร่วมมือกับหน่วยงานคุ้มครองข้อมูลที่ตั้งอยู่ในสหภาพยุโรป หรือตัวแทนที่มีอำนาจจากหน่วยงานนั้น ๆ

วิธีการข้างต้นนี้เป็นเพียงการยกตัวอย่างให้เห็นภาพเท่านั้น มิใช่วิธีปฏิบัติโดยเคร่งครัด ผู้ประกอบการบริษัทหรือองค์กรเอกชนต่าง ๆ มีสิทธิออกแบบกลไกแบบอื่นในการบังคับใช้ได้โดยอิสระเช่นกัน องค์กรและบริษัทต่าง ๆ นั้น จะอยู่ภายใต้อำนาจของหน่วยงานรัฐบาลสหรัฐอเมริกา 2 หน่วยงานด้วยกัน ได้แก่ คณะกรรมการการค้าแห่งสหรัฐอเมริกา (The Federal Trade Commission) กับกระทรวงการขนส่งแห่งสหรัฐอเมริกา (The US Department of Transportation) โดยหน่วยงานทั้งสองมีอำนาจในการสืบสวนข้อร้องเรียนและระงับการปฏิบัติที่ไม่เป็นธรรมและอาจก่อให้เกิดความหลงผิดรวมไปถึงหากมีการผ่าฝืนหลักการโครงการ Safe Harbour หน่วยงานดังกล่าวสามารถกำหนดให้มีการชดเชยแก้ไขให้แก่ปัจเจกบุคคลได้โดยไม่จำกัดสัญชาติหรือประเทศอันเป็นถิ่นที่อยู่บุคคลนั้น[129]

อย่างไรก็ตาม ในปี ค.ศ.2015 ได้เกิดข้อพิพาทขึ้นเป็นคดีระหว่าง นาย Maximillian Schrems กับ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของยุโรป (Data Protection Commissioner) โดยนาย Schrems ซึ่งเป็นเจ้าของบัญชีผู้ใช้ Facebook เชื่อว่าข้อมูลที่เขาโพสต์ลงใน Facebook ถูกโอนจากสำนักงานสาขาของ Facebook ที่ประเทศไอร์แลนด์ไปยังผู้ให้บริการประมวลผลข้อมูลที่อยู่ในสหรัฐอเมริกา และถูกสอดแนมโดยสำนักงานความมั่นคงแห่งชาติสหรัฐอเมริกาและหน่วยงานข่าวกรองอื่น ๆ ของสหรัฐอเมริกา จึงได้กล่าวหาว่า กฎหมายและแนวปฏิบัติของสหรัฐอเมริกา Safe Habour Privacy Principles ไม่เพียงพอที่จะคุ้มครองประชาชน แต่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของยุโรปสั่งยกคำร้องโดยให้เหตุผลว่ามาตรการของอเมริกาคุ้มครองข้อมูลส่วนบุคคลอย่างเพียงพอแล้ว นาย Schrems จึงนำคดีขึ้นศาลยุติธรรมยุโรป (The European Court of Justice:

---

[128] คณาธิป ทองวีรวงศ์, **รายงานการวิจัยฉบับสมบูรณ์ เรื่องการปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน,** หน้า 75-76.

[129] *เรื่องเดียวกัน*, หน้า 76.

ECJ) ซึ่งในที่สุดตัดสินให้ความตกลง Safe Habour เป็นโมฆะ และศาลยังมีความเห็นเพิ่มเติมว่าเนื่องจากความตกลง Safe Habour ดังกล่าวไม่ใช้บังคับกับการดำเนินการของหน่วยงานภาครัฐของสหรัฐอเมริกา[130]

โดยผลของคดีนี้ที่มีการตัดสินว่า Safe Habour เป็นโมฆะ ทำให้ทั้งประเทศสหรัฐอเมริกาและสหภาพยุโรปจึงเจรจากรอบความคุ้มครองข้อมูลส่วนบุคคลระหว่างกันใหม่ จึงเกิดความตกลงที่เรียกว่า US –EU Privacy Shield Framework Principles (2016) ซึ่ง EU Commission รับรองเมื่อวันที่ 12 กรกฎาคม ค.ศ.2016 โดยมีวัตถุประสงค์ดังนี้[131]

ประการแรก ความตกลงนี้ถูกกำหนดขึ้นเพื่อส่งเสริมการการเคลื่อนย้ายข้อมูลส่วนบุคคลระหว่างสหภาพยุโรปและสหรัฐอเมริกาซึ่งเป็นปัจจัยสำคัญต่อการเจริญเติบโตของเศรษฐกิจ

ประการที่สอง ความตกลงนี้กำหนดขึ้นเพื่อหาทางคุ้มครองข้อมูลส่วนบุคคลจากกรอบกฎหมายที่มีความแตกต่างกันระหว่างประเทศสหรัฐอเมริกาที่ใช้ระบบของการคุ้มครองข้อมูลส่วนบุคคลแบบผสมและใช้ระบบของการกำกับดูแลตนเอง (Mixed Regulation and Self-Regulation) กับประเทศสหภาพยุโรปที่ใช้รูปแบบของมาตรการทางกฎหมาย (Unified Data Protection Rules)

ประการที่สาม ความตกลงนี้มุ่งเน้นให้ผู้ประกอบการของสหรัฐอเมริกาที่รับข้อมูลส่วนบุคคลของยุโรปดำเนินการตามหลักการของ Privacy Shield Principles เพื่อให้ผ่านมาตรฐานการคุ้มครองข้อมูลของยุโรป

ความตกลงตาม US–EU Privacy Shield Framework Principles มีสาระสำคัญดังนี้คือ[132]

1. หน้าที่ของบริษัท (Obligations on Companies) บริษัทต้องรับรองตัวเองว่าเข้ามาตรฐาน (Self-Certify) และต้องปฏิบัติตามหลักการอื่น ๆ (Transparency, Prompt Reply to Complaints, etc.) ที่กำหนด

---

[130] Maximillian Schrems v. Data Protection Commissioner (European Court of Justice, 2015)

[131] **US –EU Privacy Shield Framework Principles**, pp. 1-3, Retrieved March 16, 2018 from https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t000 00004qAg

[132] *Ibid.*, pp. 4-8.

2. การเข้าถึงข้อมูลของรัฐบาลสหรัฐฯ (US Government Access) รัฐบาลของสหรัฐอเมริกาสามารถเข้าถึงข้อมูลส่วนบุคคลได้ จะต้องอยู่ภายใต้เงื่อนไขและวัตถุประสงค์ที่ระบุไว้โดยชัดแจ้งแล้วเท่านั้น เช่น เหตุผลเรื่องความมั่นคง

3. การเยียวยา (Redress) ความตกลงนี้กำหนดช่องทางการใช้สิทธิเพื่อเยียวยาความเสียหายได้โดยสามารถเลือกดำเนินการดังนี้

1) เจ้าของข้อมูลร้องเรียนโดยตรงกับบริษัท

2) ใช้กระบวนการระงับข้อพิพาททางเลือก

3) ร้องเรียนกับ Data Protection Authority (DPA)

4) ร้องเรียนต่อผู้ตรวจการ (Ombudsman) ซึ่งมีหน้าที่การสืบสวนข้อเท็จจริงเพื่อเยียวยาความเสียหาย

5) ใช้สิทธิฟ้องคดีเพื่อบังคับให้เป็นไปตามคำตัดสิน

4. การทบทวน (Review & Monitoring)

รูปแบบของการทบทวนนั้น อาจดำเนินการได้ในสองวิธีคือ วิธีแรกโดยการทบทวนร่วมกันรายปี (Annual Joint Review) และวิธีที่สองคือการเปิดโอกาสให้ภาคส่วนอื่น ๆ ไม่ว่าจะเป็น NGOs หรือผู้มีส่วนได้ส่วนเสียอื่นร่วมแสดงความคิดเห็น

ดังนั้นจึงสามารถสรุปได้ว่า US–EU Privacy Shield Framework Principles มีการกำหนดหลักการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ดังต่อไปนี้คือ[133]

1. หลักทางเลือก (Choice) หลักการของ Privacy Shield มุ่งเน้นรับรองสิทธิเจ้าของ ข้อมูลโดยให้ข้อมูลมีสิทธิเลือกที่จะไม่ถูกประมวลข้อมูลต่อไป หรือหลัก OPT OUT จากการประมวลข้อมูล เช่น เมื่อข้อมูลส่วนบุคคลถูกโอนไปยังบุคคลที่สามหรือเพื่อวัตถุประสงค์ที่แตกต่างจากวัตถุประสงค์ที่เก็บ ข้อมูลนั้นแต่แรก สำหรับในกรณีข้อมูลอ่อนไหวหรือ Sensitive Data นั้นจะใช้หลักการขอความยินยอมก่อนหรือ OPT IN ในการเก็บข้อมูล

2. หลักความปลอดภัยของข้อมูล (Security) บริษัทที่เข้าร่วมโครงการ Privacy Shield จะต้องมีมาตรการที่สมเหตุผลในการคุ้มครองข้อมูลจากการสูญเสีย นำไปใช้โดยมิชอบ การเข้าถึง การเปิดเผย การแก้ไข การทำลาย โดยปราศจากอำนาจตามกฎหมาย

3. หลักบูรณภาพของข้อมูลและการจำกัดวัตถุประสงค์ (Data Integrity and Purpose Limitation) หลักนี้จำกัดการประมวลข้อมูลว่าต้องเป็นกิจกรรมที่เกี่ยวข้องกับวัตถุประสงค์ของการประมวล ที่แจ้งไว้ และหลีกเลี่ยงกิจกรรมที่ขัดแย้งกับวัตถุประสงค์ดังกล่าว

---

[133] คณาธิป ทองวีรวงศ์, **รายงานการวิจัยฉบับสมบูรณ์ เรื่องการปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน,** หน้า 76-78.

4. หลักการเข้าถึง (Access) หลักการนี้รับรองสิทธิของเจ้าของข้อมูลว่าต้องสามารถ เข้าถึงข้อมูลเกี่ยวกับตนซึ่งองค์กรเก็บไว้ รวมทั้งสามารถแก้ไข ลบ ข้อมูลที่ไม่ถูกต้อง (inaccurate) หรือ ประมวลขัดแย้งกับหลักความตกลงนี้

5. หลักการแจ้ง (Notice) สำหรับหลักการแจ้ง ตาม Privacy Shield นั้นมีความเจาะจง รวมทั้งกำหนดข้อมูลรายละเอียดหลายประเด็นซึ่ง กิจการที่จะได้รับการรับรอง Privacy Shield ต้องแจ้งข้อมูล ดังนี้

1) การเข้าร่วมโครงการ Privacy Shield

2) ชนิดข้อมูลส่วนบุคคลที่เก็บ และ หน่วยงาน ตัวแทน ที่เกี่ยวข้องกับองค์กรซึ่งจะต้องปฏิบัติตามหลักการ Privacy Shield

3) ความตกลงที่จะปฏิบัติตามหลักการ Privacy Shield ต่อข้อมูลส่วนบุคคลทั้งหมดที่ได้รับจากสหภาพยุโรป

4) วัตถุประสงค์ของการเก็บและใช้ข้อมูลส่วนบุคคล

5) ระบุถึงบุคคลที่สามซึ่งทำการเปิดเผยข้อมูลส่วนบุคคลและวัตถุประสงค์ของการเปิดเผย

6) สิทธิของบุคลในการเข้าถึงข้อมูล

7) ทางเลือกและวิธีการขององค์กรที่เสนอให้บุคคลเพื่อจำกัดการใช้และเปิดเผยข้อมูลส่วนบุคคลของตน

8) องค์กรระงับข้อพิพาทที่เป็นอิสระซึ่งมีอำนาจในการดำเนินการกับข้อร้องเรียนโดยปราศจากค่าใช้จ่าย

9) การที่จะต้องอยู่ภายใต้การบังคับใช้กฎหมายและการสอบสวนขององค์กรที่มีอำนาจตามกฎหมายสหรัฐ

10) ความเป็นไปได้ของบุคคลในการดำเนินการระงับข้อพิพาททางอนุญาโตตุลาการ

11) ข้อกำหนดให้เปิดเผยข้อมูลส่วนบุคคลที่มีคำขออันชอบด้วยกฎหมายของหน่วยงานรัฐ

12) ความรับผิดชอบในกรณีการส่งต่อข้อมูลไปยังบุคคลที่สาม (Onwards Transfer)

6. หลักการควบคุม Data Processor และ Data Controller ในกรณีการโอนข้อมูลจากผู้ประมวลข้อมูลไปให้บุคคลที่สามทำการประมวลข้อมูลต่อนั้น หลักการใหม่กำหนดควบคุม Onward Transfer โดยบริษัทที่เข้าร่วมโครงการ Privacy Shield จะต้องทำสัญญากับบุคคลที่สามซึ่งตนโอนข้อมูลไปโดยผูกพันบุคคลที่สามที่เป็นผู้ควบคุมข้อมูล (Third Party Controller) อันจะต้องจัด

ให้มีมาตรการคุ้มครองข้อมูลตามหลัก Privacy Shield ด้วย รวมทั้งประมวลข้อมูลภายใต้ข้อจำกัดตามหลักวัตถุประสงค์ หากบริษัทที่ร่วมโครงการ Privacy Shield ประมวลข้อมูลโดยทางบุคคลที่สามซึ่งเป็นตัวแทน (Third Party Agent) จะต้องมีข้อตกลงการประมวลข้อมูลที่สอดคล้องกับหลักคุ้มครองข้อมูลของยุโรป นอกจากนี้ต้องมีการแจ้งให้ทราบกรณีผู้รับโอนข้อมูลซึ่งเป็นบุคคลที่สามไม่สามารถดำเนินการให้มีระดับการคุ้มครองข้อมูลที่เทียบเท่ากับยุโรป (Third–Party Recipient Is Unable to Provide the Same Level of Protection)

7. หลักการบังคับใช้หลักการคุ้มครอง (Enforcement) และการเยียวยา กระบวนการเยียวยา (Redress) ตามข้อตกลงนี้มีหลายระดับ เช่น

1) การเยียวยาโดยตรง กิจการจะต้องตอบสนองต่อคำร้องจากบุคคลธรรมดาภายใน 45 วัน

2) เจ้าของข้อมูลมีสิทธิร้องเรียนโดยตรงต่อองค์กรอิสระ รวมทั้งองค์กรคุ้มครองข้อมูลของยุโรป เช่น คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายภายใน

3) กระทรวงพาณิชย์สหรัฐเข้ามามีบทบาทระงับข้อพิพาทกรณีองค์กรที่ไม่ปฏิบัติ ตามหลัก PRIVACY SHIELD

4) การระงับข้อพิพาททางเลือก (Alternative Dispute Resolution) ต้องจัดให้มี ขึ้นโดยปราศจากค่าใช้จ่าย

5) มีกลไกอนุญาโตตุลาการเป็นที่พึ่งสุดท้าย (Last Resort) โดยมีการจัดตั้ง Privacy Shield Panel ทั้งนี้ เจ้าของข้อมูลที่เป็นฯพลเมืองยุโรปมีสิทธิระงับข้อพิพาทโดยอนุญาโตตุลาการ (Privacy Shield Panel) ประกอบด้วยอย่างน้อย 20 คนที่แต่งตั้งโดยกระทรวงพาณิชย์สหรัฐและกรรมาธิการยุโรป ในกรณีปัญหาการสอดส่องข้อมูลโดยภาครัฐมีกระบวนการพิเศษได้แก่ การจัดตั้งองค์กรอิสระเรียกว่า Privacy Shield Ombudsperson ซึ่งเป็นอิสระจากหน่วยงานเกี่ยวกับข่าวกรองหรือ Intelligent Community เพื่อคุ้มครองการล่วงละเมิดข้อมูลจากภาครัฐ

สำหรับความแตกต่างระหว่างหลักการของ Safe Harbor Privacy Principles กับหลักการของ US–EU Privacy Shield Framework Principles นั้น คณาธิป ทองวีรวงศ์ ได้เปรียบเทียบหลักการที่คล้ายคลึงและแตกต่าง โดยแบ่งเป็นสองกลุ่มดังนี้[134]

กลุ่มแรก เป็นกลุ่มของหลักการที่ยังคงคล้ายคลึงกับ “Safe Harbor” ได้แก่

1. หลักทางเลือก (Choice) หลักการของ Privacy Shield มุ่งเน้นรับรองสิทธิเจ้าของข้อมูลโดยให้ข้อมูลมีสิทธิเลือกที่จะไม่ถูกประมวลข้อมูลต่อไป หรือหลัก OPT OUT จากการประมวล ข้อมูล เช่น เมื่อข้อมูลส่วนบุคคลถูกโอนไปยังบุคคลที่สามหรือเพื่อวัตถุประสงค์ที่แตกต่าง

---

[134] *เรื่องเดียวกัน*, หน้า 168-171.

จากวัตถุประสงค์ที่ เก็บข้อมูลนั้นแต่แรก สำหรับในกรณีข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) นั้นจะใช้หลักการขอความยินยอมก่อนหรือ OPT IN ในการเก็บข้อมูล

2. หลักความปลอดภัยของข้อมูล (Security) บริษัทที่เข้าร่วมโครงการ Privacy shield จะต้องมีมาตรการที่สมเหตุผลในการคุ้มครองข้อมูลจากการสูญเสีย นำไปใช้โดยมิขอบ การเข้าถึง การเปิดเผย การแก้ไข การทำลาย โดยปราศจากอำนาจตามกฎหมายหลักการนี้เป็นหลักการเดิมของ Safe Harbor

3. หลักบูรณภาพของข้อมูลและการจำกัดวัตถุประสงค์ (Data Integrity and Purpose Limitation) หลักนี้จำกัดการประมวลข้อมูลว่าต้องเป็นกิจกรรมที่เกี่ยวข้องกับวัตถุประสงค์ของ การประมวลที่แจ้งไว้ และหลีกเลี่ยงกิจกรรมที่ขัดแย้งกับวัตถุประสงค์ดังกล่าว

4. หลักการเข้าถึง (Access) หลักการนี้รับรองสิทธิของเจ้าของข้อมูลว่า ต้องสามารถเข้าถึงข้อมูลเกี่ยวกับตนซึ่งองค์กรเก็บไว้ รวมทั้งสามารถแก้ไข ลบ ข้อมูลที่ไม่ถูกต้อง (Inaccurate) หรือประมวลผลไม่ถูกต้องขัดแย้งกับหลักการของกฎหมาย

กลุ่มที่สอง เป็นหลักการที่มีความเข้มงวดในการคุ้มครองข้อมูลมากกว่า Safe Harbor ซึ่งได้แก่

1. หลักการแจ้ง (Notice) โดยหลักแล้วผู้ประมวลข้อมูลต้องแจ้งถึงวัตถุประสงค์ของการประมวลข้อมูลให้เจ้าของข้อมูลทราบ ซึ่งหลักการนี้เหมือนกันทั้ง Privacy Shield และ Safe Harbor แต่อย่างไรก็ตาม Privacy Shield มีหลักการแจ้ง ที่มีเข้มงวดกว่า Safe Harbor กล่าวคือ Safe Harbor กำหนดให้หน่วยธุรกิจที่เข้าร่วมโครงการ ต้องให้ข้อมูลทั่วไปเกี่ยวกับการประมวลข้อมูล เช่น วัตถุประสงค์ที่เก็บและประมวล ข้อมูล ผู้รับการโอนข้อมูลซึ่งเป็นบุคคลที่สาม รวมทั้งกำหนดให้มีทางเลือกแก่เจ้าของข้อมูล

สำหรับหลักการแจ้ง ตาม Privacy Shield นั้นมีความเจาะจงมากกว่า รวมทั้งกำหนดข้อมูลรายละเอียดหลายประเด็นซึ่งกิจการที่จะได้รับการรับรอง Privacy Shield ต้องแจ้งข้อมูล ดังนี้

1) การเข้าร่วมโครงการ Privacy Shield

2) ชนิดข้อมูลส่วนบุคคลที่เก็บและ หน่วยงาน ตัวแทน ที่เกี่ยวข้องกับองค์กรซึ่งจะต้องปฏิบัติตามหลักการ Privacy Shield

3) ความตกลงที่จะปฏิบัติตามหลักการ Privach Shield ต่อข้อมูลส่วนบุคคลทั้งหมดที่ได้รับจากสหภาพยุโรป

4) วัตถุประสงค์ของการเก็บและใช้ข้อมูลส่วนบุคคล

5) ระบุถึงบุคคลที่สามซึ่งทำการเปิดเผยข้อมูลส่วนบุคคลและวัตถุประสงค์ของการเปิดเผย

6) สิทธิของบุคลในการเข้าถึงข้อมูล

7) ทางเลือกและวิธีการขององค์กรที่เสนอให้บุคคลเพื่อจำกัดการใช้และเปิดเผยข้อมูล ส่วนบุคคลของตน

8) องค์กรระงับข้อพิพาทที่เป็นอิสระซึ่งมีอำนาจในการดำเนินการกับข้อร้องเรียน โดยปราศจากค่าใช้จ่าย

9) การที่จะต้องอยู่ภายใต้การบังคับใช้กฎหมายและการสอบสวนขององค์กรที่มีอำนาจตามกฎหมายสหรัฐ

10) ความเป็นไปได้ของบุคคลในการดำเนินการระงับข้อพิพาททางอนุญาโตตุลาการ

11) ข้อกำหนดให้เปิดเผยข้อมูลส่วนบุคคลที่มีคำขออันชอบด้วยกฎหมายของหน่วยงานรัฐ

12) ความรับผิดชอบในกรณีการส่งต่อข้อมูลไปยังบุคคลที่สาม (Onwards Transfer)

2. หลักการควบคุม Data Processor และ Data Controller

ในกรณีการโอนข้อมูลจากผู้ประมวลข้อมูลไปให้บุคคลที่สามทำการประมวลข้อมูลต่อนั้น หลักการใหม่กำหนดควบคุมการโอนข้อมูลต่อ (Onward Transfer) โดยองค์กรที่เข้าร่วมโครงการ Privacy Shield จะต้องทำสัญญากับบุคคลที่สามซึ่งตนโอนข้อมูลไป โดยผูกพันบุคคลที่สามที่เป็นผู้ควบคุม ข้อมูล (Third Party Controller) อันจะต้องจัดให้มีมาตรการคุ้มครองข้อมูลตามหลัก Privacy shield ด้วย รวมทั้งประมวลข้อมูลภายใต้ข้อจำกัดตามหลักวัตถุประสงค์

หากองค์กรที่ร่วมโครงการ Privacy Shield ประมวลข้อมูลโดยทางบุคคลที่สาม ซึ่งเป็นตัวแทน (Third Party Agent) จะต้องมีข้อตกลงการประมวลข้อมูลที่สอดคล้องกับหลักคุ้มครองข้อมูลของยุโรป

นอกจากนี้ ต้องมีการแจ้งให้ทราบกรณีผู้รับโอนข้อมูลซึ่งเป็นบุคคลที่สาม ไม่สามารถดำเนินการให้มีระดับการคุ้มครองข้อมูลที่เทียบเท่ากับยุโรป (Third–Party Recipient is Unable to Provide the Same Level of Protection)

3. หลักบูรณภาพของข้อมูลและการจำกัดวัตถุประสงค์ (Data Integrity and Purpose Limitation) โดยทั่วไปหลักการนี้คล้ายคลึงกับ Safe Harbor แต่ Privacy Shield ระบุชัดเจนขึ้นว่า บริษัทที่เข้าร่วมโครงการ Privacy Shield ต้องปฏิบัติตามหลัก Privacy Shield ตราบเท่าที่ยังคงเก็บ ข้อมูลนั้นอยู่แม้ว่าจะไม่ได้รับรองตนเองแล้วก็ตาม (Self Certification Terminated)

4. หลักการบังคับใช้หลักการคุ้มครอง (Enforcement) และการเยียวยา

กระบวนการเยียวยา (Redress) ตามข้อตกลงนี้มีหลายระดับ เช่น การเยียวยาโดยตรง กิจการจะต้องตอบสนองต่อคำร้องจากบุคคลธรรมดาภายใน 45 วัน หรืออาจเป็นกรณีเจ้าของข้อมูลมีสิทธิร้องเรียนโดยตรงต่อองค์กรอิสระ รวมทั้งองค์กรคุ้มครอง ข้อมูลของยุโรป เช่น คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายภายในหรือการกำหนดให้กระทรวงพาณิชย์สหรัฐเข้ามามีบทบาทระงับข้อพิพาทกรณีองค์กรที่ไม่ปฏิบัติตามหลัก Privacy Shield หรืออาจมีการระงับข้อพิพาททางเลือก (Alternative Dispute Resolution) ต้องจัดให้มีขึ้นโดยปราศจากค่าใช้จ่าย รวมไปถึงการมีกลไกอนุญาโตตุลาการที่เป็นทางเลือกสุดท้าย (Last Resort)

จากที่กล่าวมาสรุปได้ว่า ความตกลง Privacy Shield นั้นแม้มีการปรับปรุงเพิ่มเติมหลักการและนโยบายการคุ้มครองข้อมูลส่วนบุคคล แต่หากพิจารณาเปรียบเทียบกับหลักกฎหมายของยุโรปแล้วยังมีอีกหลายประเด็นที่สภาพของระบบกฎหมายและแนวปฏิบัติของหน่วยงานภาครัฐในสหรัฐอเมริกาจะส่งผลกระทบต่อโครงการนี้ อันอาจทำให้ศาลยุโรปตัดสินว่าคำรับรองของคณะกรรมาธิการยุโรปต่อโครงการนี้ใช้ไม่ได้เช่นเดียวกับ Safe Harbor แม้ว่าหลักการคุ้มครองข้อมูลส่วนบุคคลจะมีการปรับปรุงขึ้นหลายหลัก แต่ปัญหาพื้นฐานที่เป็นปัจจัยสำคัญอันทำให้ศาลยุโรปตัดสินว่า Safe Harbor สิ้นผลยังคงอยู่โดยไม่ได้รับการปรับปรุง กล่าวคือ การสอดแนมการสื่อสารของประชาชนโดยรัฐบาลสหรัฐอเมริกาที่ยังอาจไม่สอดคล้องกับหลักการคุ้มครองสิทธิขั้นพื้นฐานของประชาชนนั่นเอง[135]

3.2 การคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศอังกฤษ

3.2.1 แนวคิดและวิวัฒนาการในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศอังกฤษ

3.2.1.1 ความหมายของข้อมูลส่วนบุคคลของประเทศอังกฤษ

สำหรับการกำหนดความหมายของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในประเทศอังกฤษนั้น ย่อมหมายถึง อำนาจหรือประโยชน์ที่ระบบกฎหมายของประเทศอังกฤษรับรองหรือคุ้มครองให้แก่เจ้าของข้อมูลส่วนบุคคล ซึ่งข้อมูลส่วนบุคคลที่ระบบกฎหมายอังกฤษรับรองและคุ้มครองให้นั้นมีความหมายดังต่อไปนี้

---

[135] *เรื่องเดียวกัน*, หน้า 187.

“ข้อมูล” (Data) หมายถึง ข้อมูลซึ่งถูกประมวลผล (Processed) โดยเครื่องมือที่ทำงานโดยอัตโนมัติ เพื่อตอบสนองคำสั่งที่ป้อนเข้าไปเพื่อวัตถุประสงค์นั้นหรือข้อมูลซึ่งถูกบันทึกไว้โดยมีเจตนาที่จะนำไปประมวลผลโดยเครื่องมือที่ทำงานโดยอัตโนมัติ (เช่น ข้อมูลที่บันทึกไว้ในกระดาษที่เตรียมไว้เพื่อนำไปประมวลผลโดยคอมพิวเตอร์ เป็นต้น) หรือข้อมูลซึ่งถูกบันทึกไว้เป็นส่วนหนึ่งของ Relevant Filing System (ระบบจัด เก็บข้อมูลที่เกี่ยวข้อง) หรือ มีเจตนาที่จะนำไปบันทึกไว้เป็นส่วนหนึ่งของ Relevant Filing System หรือข้อมูลซึ่งเป็นส่วนหนึ่งของ Accessible Record

“ข้อมูลส่วนบุคคล” (Personal Data) หมายถึง ข้อมูลที่เกี่ยวข้องกับบุคคลที่ยังมีชีวิตอยู่ซึ่งสามารถบ่งชี้ตัวบุคคลได้ จากข้อมูลนั้นเองและข้อมูลอื่น ๆ ที่อยู่ในความครอบครองของผู้ควบคุมดูแลข้อมูล (Data Controller) หรืออาจอยู่ในความครอบครองของผู้ควบคุมดูแลข้อมูลในอนาคต ทั้งนี้ รวมถึงข้อมูลเกี่ยวกับการแสดงความคิดเห็นเกี่ยวกับตัวบุคคลธรรมดาและการแสดงเจตนาของผู้ควบคุมดูแลข้อมูลหรือบุคคลอื่นที่เกี่ยวกับบุคคลธรรมดานั้นด้วย

3.2.1.2 สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในฐานะสิทธิขั้นพื้นฐาน

เดิมที่ประเทศอังกฤษไม่ให้ความสำคัญกับสิทธิในความเป็นส่วนตัว ทั้งนี้เนื่องจากระบบการเมืองการปกครองของอังกฤษ ให้ความสำคัญกับสิทธิในการปราศรัยแสดงความคิดเห็น กับสิทธิในการรับรู้ข้อมูลข่าวสารอันเป็นพื้นฐานของระบอบประชาธิปไตย ดังคำกล่าวของ Clive Rumbelow ที่กล่าวโดยสรุปได้ว่า สิทธิในความเป็นส่วนตัวไม่ได้รับการยอมรับในระบบกฎหมายของอังกฤษ เพราะสิทธินี้ขัดแย้งโดยตรงกับสิ่งที่สำคัญกว่า นั่นก็คือ สิทธิในการปราศรัยโดยเสรี (Right of Free Speech) ถ้าหากไม่ได้รับอนุญาติให้มีการวิพากษ์วิจารณ์ โดยเหตุผลว่าเป็นเรื่องส่วนบุคคลเช่นนั้นสิทธิปราศรัยโดยเสรีก็จะเสียไป[136] อย่างไรก็ดี ในภายหลังเมื่อเข้าสู่ยุคที่มีการเกิดขึ้นของคอมพิวเตอร์ และเกิดการใช้ข้อมูลโดยมิชอบมากขึ้นทำให้อังกฤษได้พัฒนากฎหมายของตนขึ้นเพื่อคุ้มครองสิทธิในข้อมูลส่วนบุคคลนี้

ต่อมาในภายหลังระบบกฎหมายของอังกฤษยอมรับสิทธิในความเป็นส่วนตัวในฐานะสิทธิขั้นพื้นฐานโดยบรรจุไว้ในกฎหมายที่ตราขึ้นโดยรัฐสภาอังกฤษ นั่นก็คือ Data Protection Act ซึ่งทำให้สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลมีฐานะเป็นสิทธิเสรีภาพที่รับรองโดยระบบกฎหมายรัฐธรรมนูญของอังกฤษ[137]

---

[136] ชื่นอารีย์ มาลีศรีประเสริฐ, *เรื่องเดิม*, หน้า 127.

[137] Anneliese Roos, **The Law of Data (Privacy) Protection: A Comparative And Theoretical Study** (Doctoral dissertation, Doctor of Laws at The University of South Africa 2003), pp. 387-388.

3.2.1.3 วิวัฒนาการในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในประเทศอังกฤษ

ดังที่ได้กล่าวมาแล้วว่า ประเทศอังกฤษในอดีต ไม่มีกฎหมายที่ให้ความคุ้มครองข้อมูลส่วนบุคคลเป็นการเฉพาะเนื่องจากไม่ยอมรับในสิทธิความเป็นส่วนตัวที่จะขัดแย้งกับสิทธิในการปราศรัยโดยเสรี อย่างไรก็ดี ต่อมาเมื่อประเทศมีความเจริญก้าวหน้าทางเทคโนโลยีสารสนเทศมากยิ่งขึ้น ทำให้การจัดเก็บข้อมูล ประมวลผล เรียกใช้ข้อมูลโดยระบบอิเล็กทรอนิกส์สามารถกระทำได้สะดวกรวดเร็วและการเข้าถึงแหล่งข้อมูลต่าง ๆ สามารถกระทำได้จนยากที่จะป้องกันเป็นความลับได้ ส่งผลให้เกิดปัญหาการล่วงละเมิดสิทธิส่วนบุคคลเกี่ยวกับข้อมูลส่วนบุคคลมากขึ้น ประเทศอังกฤษได้ตระหนักถึงปัญหาดังกล่าวจึงเริ่มพัฒนากฎหมายและมีความพยายามที่จะให้ความคุ้มครองแก่สิทธิส่วนบุคคลมากขึ้น

ในปี ค.ศ.1970 รัฐบาลอังกฤษได้จัดตั้งคณะกรรมการขึ้นศึกษาว่ามีความจำเป็นที่จะต้องตรากฎหมายขึ้นคุ้มครองการล่วงละเมิดสิทธิส่วนบุคคลของประชาชนที่เกิดจากการกระทำของผู้อื่นหรือหน่วยงานในภาคเอกชนหรือไม่ซึ่งผลการศึกษาของคณะกรรมการหลายชุดพบว่า ไม่ปรากฏความจำเป็นที่จะต้องตรากฎหมายดังกล่าว ในทางตรงกันข้ามกับประเทศต่าง ๆ ในยุโรปได้มีการบัญญัติกฎหมายให้ความคุ้มครองการเก็บและการใช้ข้อมูลข่าวสารโดยเฉพาะอย่างยิ่งประชาคมเศรษฐกิจยุโรป (European Economic Community) เดิมหรือสหภาพยุโรป (EU) ในปัจจุบันได้ร่วมกันจัดทำอนุสัญญาฉบับหนึ่งขึ้นมีชื่อว่า “Convention for the Protection of Individual with Regard to Automatic Processing of Personal Data” ซึ่งประเทศอังกฤษก็เป็นสมาชิกและได้ให้สัตยาบันต่ออนุสัญญาดังกล่าวเมื่อวันที่ 14 พฤษภาคม ค.ศ.1981 และเพื่ออนุวัติการให้เป็นไปตามอนุสัญญาดังกล่าวประเทศอังกฤษจึงได้ตรากฎหมายเพื่อคุ้มครองสิทธิส่วนบุคคลอันเกี่ยวกับข้อมูลข่าวสารขึ้น คือ พระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลข่าวสาร ค.ศ.1984 (Data Protection Act 1984)

เมื่อได้ประกาศใช้ Data Protection Act 1984 แล้ว มีผลทำให้การจัดเก็บสารสนเทศทุกประเภทที่เกี่ยวกับบุคคล (Personal Data) โดยระบบคอมพิวเตอร์จะต้องดำเนินการให้เป็นไปตามกฎหมายฉบับนี้ ทั้งในภาครัฐและภาคเอกชน โดยข้อมูลข่าวสารนั้นต้องเป็นข้อมูลข่าวสารที่เกี่ยวกับบุคคลธรรมดา ซึ่งสามารถพิสูจน์หรือบ่งชี้ถึงบุคคลหนึ่ง ๆ ได้โดยตัวข้อมูลข่าวสารนั้นเองหรือโดยการตรวจสอบด้วยข้อมูลข่าวสารอื่น ๆ ที่อยู่ในความครอบครองของผู้ใช้ข้อมูล (Data User) และเป็นข้อมูลข่าวสารที่ถูกจัดเก็บไว้ในประเทศอังกฤษ

ต่อมาประเทศอังกฤษได้ออก Data Protection Act 1998 เพื่ออนุวัติการให้เป็นไปตาม The European Data Protection Directive (95/46/EC) หรือ EU Directive (95/46/EC) โดยมีผลบังคับใช้ในครั้งแรกเมื่อวันที่ 16 กรกฎาคม 1998 และได้มีการปรับปรุงจนเป็นฉบับสมบูรณ์

(Fully) ซึ่งมีผลบังคับใช้ตั้งแต่ 1 มีนาคม 2000 กฎหมายฉบับนี้มีความละเอียดและสลับซับซ้อนกว่า Data Protection Act 1984 โดยกฎหมายฉบับนี้มีผลใช้บังคับกับข้อมูลที่ถูกประมวลผลด้วยมือซึ่งถูกจัดเก็บไว้ในแฟ้มข้อมูล และประมวลผลโดยวิธีการอัตโนมัติด้วย รวมทั้งมีการกำหนดเงื่อนไขหรือบรรทัดฐานขึ้นต่ำของการประมวลผลข้อมูลที่จะถือว่าเป็นการประมวลผลข้อมูลที่ชอบด้วยกฎหมาย นอกจากนี้กฎหมายฉบับนี้ยังกำหนดให้มีข้อมูลส่วนบุคคลประเภทข้อมูลที่กระทบต่อความรู้สึก หรือข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) ซึ่งมีผลทำให้ผู้ควบคุมดูแลข้อมูลไม่สามารถประมวลผลข้อมูลประเภทนี้ได้ เว้นแต่จะได้มีการปฏิบัติตามเงื่อนไขหรือข้อยกเว้นที่กำหนดไว้โดยเฉพาะ ทั้งยังได้กำหนดห้ามมิให้ส่งข้อมูลส่วนบุคคลไปยังประเทศที่อยู่นอกสมาชิกของ European Economic Area-EEA อีกด้วย เว้นแต่เป็นไปตามเงื่อนไขที่กำหนดไว้

อย่างไรก็ดี ในวันที่ 23 มิถุนายน ค.ศ.2016 ประเทศอังกฤษได้ทำการลงมติสมาชิกภาพในสหภาพยุโรป โดยฝ่ายที่ต้องการให้ออกจากสหภาพยุโรปเป็นฝ่ายชนะ กรณีนี้ก็จะมีผลทำให้แม้ว่าสหภาพยุโรปจะประกาศใช้ General Data Protection Regulation 2016 กฎเกณฑ์นี้ก็จะมีผลบังคับควบคู่กับกฎหมายภายในของประเทศอังกฤษเพียงชั่วระยะเวลาหนึ่งคือ วันที่ 25 พฤษภาคม ค.ศ.2018 จนกระทั่งถึง 29 มีนาคม ค.ศ.2019 ในกรณีนี้ทำให้ประเทศอังกฤษเตรียมการในเรื่องการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลโดยรัฐสภาอังกฤษได้เตรียมการโดยการร่าง The Data Protection Bill [HL] 2017-19[138]

ร่างกฎหมายฉบับนี้ รัฐสภาของอังกฤษได้ให้เหตุผลในการตราขึ้น โดยมีวัตถุประสงค์ดังนี้[139]

1. ตราขึ้นเพื่อแทนที่ Data Protection Act 1998 โดยจะให้กฎหมายฉบับใหม่มีความทันสมัยและครอบคลุมเพื่อการปกป้องสิทธิในข้อมูลส่วนบุคคลโดยใช้วิธีการลงโทษที่รุนแรงขึ้นสำหรับการผ่าฝืน

---

[138] John Woodhouse and Arabella Lang, **Brexit and Data Protection,** Retrieved March 12, 2018 from http://researchbriefings.files.parliament.uk/documents/CBP-7838/CBP-7838.pdf

[139] Department for Digital, Culture, Media and Sport, **Data Protection Bill Factsheet – Overview**, Retrieved March 12, 2018 from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/685647/2018-03-05_Factsheet01_Bill_overview.pdf

2. กำหนดมาตรฐานใหม่สำหรับการปกป้องข้อมูลทั่วไป ตามข้อกำหนดของGDPR อันจะทำให้ประชาชนผู้เป็นเจ้าของข้อมูลสามารถที่จะควบคุมการใช้ข้อมูลของตนเองได้มากขึ้นและมีสิทธิใหม่ในการย้ายหรือลบข้อมูลส่วนบุคคลของตน

3. รักษาข้อดีตามบทบัญญัติเดิมของ Data Protection Act ไว้ในกฎหมายใหม่ เพื่อให้มั่นใจว่าองค์กรและบริษัทของประเทศอังกฤษจะยังคงสามารถเป็นผู้นำในด้านการวิจัย บริการทางการเงิน สื่อสารมวลชน และการให้บริการทางกฎหมาย

4. จัดทำกรอบการทำงานที่เหมาะในกระบวนการยุติธรรมทางอาญาของหน่วยงานและหน่วยสืบราชการลับเพื่อปกป้องสิทธิของผู้ที่ตกเป็นเหยื่อ, พยานและผู้ต้องสงสัย ในขณะเดียวกันก็ต้องทำให้มั่นใจว่าสามารถจัดการกับการเปลี่ยนแปลงในลักษณะที่เป็นภัยคุกคามจากทั่วโลกซึ่งประเทศอังกฤษต้องเผชิญ

ต่อมาร่างกฎหมาย The Data Protection Bill ก็ได้ผ่านการพิจารณาของรัฐสภาเป็น The Data Protection Act 2018 ซึ่งกฎหมายฉบับนี้ได้มีการลงพระปรมาภิไธยเพื่อประกาศใช้ในวันที่ 23 พฤษภาคม 2018 ถือเป็นพระราชบัญญัติฉบับใหม่ที่ได้มีการพัฒนาปรับปรุงหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับเดิมของประเทศอังกฤษ ตามมาตรฐานของสหภาพยุโรปที่มีการเปิดโอกาสอย่างจำกัดให้ประเทศสมาชิกได้ปรับปรุงหลักการของกฎหมายเพื่อประยุกต์ใช้ในรัฐตนเองได้ และถือเป็นกฎหมายภายในของรัฐที่ได้เติมเต็มให้ General Data Protection Regulation (GDPR) ของสหภาพยุโรปได้มีผลสมบูรณ์ตามเจตนารมณ์ ซึ่งตามหลักการพื้นฐานแล้ว ผู้ที่รับผิดชอบในการใช้ข้อมูลส่วนบุคคลจะต้องปฏิบัติตาม "หลักการปกป้องข้อมูล" อย่างเคร่งครัด โดยจะต้องทำให้แน่ใจว่าข้อมูลนั้นจะต้องมีการดำเนินการดังนี้[140]

1. ได้ใช้อย่างยุติธรรม ถูกต้องตามกฎหมาย และโปร่งใส
2. ใช้เพื่อวัตถุประสงค์ที่ระบุไว้ชัดเจนโดยเฉพาะ
3. ใช้ในลักษณะที่จำกัด ตามความจำเป็น และเหมาะสม เฉพาะในส่วนที่มีความเกี่ยวข้อง
4. ข้อมูลจะต้องถูกต้อง และทันสมัย
5. ไม่จัดเก็บไว้นานเกินความจำเป็น

---

[140] Information Commissioner's Office (ICO), **An Overview of the Data Protection Act 2018,** Retrieved March 1, 2019 from https://ico.org.uk/media/2614158/ico-introduction-to-the-data-protection-bill.pdf

6. การเก็บรักษาข้อมูลจะต้องมีระบบความปลอดภัยที่เหมาะสมและสามารถป้องกันการเข้าถึงหรือการประมวลผลที่ไม่ชอบด้วยกฎหมาย รวมถึงการทำลาย การทำให้เสียหาย หรือสูญหายซึ่งข้อมูลนั้น

สำหรับข้อมูลที่มีความอ่อนไหว (Sensitive Data) จะต้องมีมาตรการทางกฎหมายที่เคร่งครัดกว่า ซึ่งได้แก่ข้อมูลส่วนบุคคลเหล่านี้คือ ข้อมูลเกี่ยวกับเชื้อชาติ ชาติพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนา การเป็นสมาชิกสหภาพแรงงาน พันธุศาสตร์ ข้อมูล Biometrics (ที่ใช้ระบุตัวตนได้) ข้อมูลสุขภาพ รสนิยมทางเพศ และข้อมูลประวัติอาชญากรรม

3.2.2 มาตรการทางกฎหมายในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศอังกฤษ

3.2.2.1 ลักษณะและประเภทของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลที่ได้รับความคุ้มครอง

ลักษณะและประเภทของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลมีการแบ่งแยกออกเป็น 2 ประเภท คือข้อมูลส่วนบุคคลทั่วไป และข้อมูลส่วนบุคคลที่มีความอ่อนไหว

ข้อมูลส่วนบุคคลทั่วไป หมายถึง ข้อมูลใด ๆ ของบุคคลที่เกี่ยวข้องกับความเป็นอยู่ส่วนของบุคคลซึ่งสามารถระบุตัวตนได้จากข้อมูลเหล่านั้นหรือข้อมูลอื่น ๆ ที่อยู่ในความครอบครองภายใต้กฎหมาย DPA “ข้อมูลส่วนบุคคล” จะไม่รวมถึงข้อมูลเกี่ยวกับนิติบุคคล เช่น บริษัท

สำหรับข้อมูลส่วนบุคคลที่มีความอ่อนไหวนั้น ในมาตรา 2 ของ Data Protection Act 1998 ได้มีการกำหนดความหมายว่า หมายถึงข้อมูลดังต่อไปนี้ของเจ้าของข้อมูลส่วนบุคคล

1. ข้อมูลที่เกี่ยวกับเชื้อชาติ หรือเผ่าพันธุ์
2. ข้อมูลเกี่ยวกับความคิดหรือความเห็นในทางการเมือง
3. ข้อมูลเกี่ยวกับความเชื่อในทางศาสนา
4. ข้อมูลการเป็นสมาชิกสมาคมหรือหสภาพแรงงาน
5. ข้อมูลเกี่ยวกับสุขภาพทางกายหรือจิตใจของเจ้าของข้อมูล
6. ข้อมูลอาชญากรรมหรือข้อมูลที่เกี่ยวกับการถูกกล่าวหาว่ากระทำความผิด
7. ข้อมูลที่เกี่ยวกับคดีความ การฟ้องคดีหรือการจำหน่ายคดี และการกำหนดบทลงโทษตามคำพิพากษา

ซึ่งจากข้อมูลเหล่านี้ถือเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว แต่ทว่าในระบบกฎหมายอังกฤษแต่เดิมนั้น ระบบการคุ้มครองสิทธิในข้อมูลก็ใช้หลักการคุ้มครองแบบเดียวกันกับข้อมูลส่วนบุคคลทั่วไป ก่อนที่ภายหลังจะได้รับอิทธิพลจาก GDPR

สำหรับ สิทธิของเจ้าของข้อมูลส่วนบุคคล ตามหลักการเดิมของ Data Protection Act 1998 ได้กำหนดรับรองสิทธิของเจ้าของข้อมูลที่เป็นบุคคลธรรมดาเกี่ยวกับข้อมูลส่วนบุคคลของตนที่อยู่ในความครอบครองของบุคคอื่นหรือผู้ควบคุมดูแลข้อมูลไว้ดังนี้

1. สิทธิในการเข้าถึงข้อมูล

Data Protection Act 1998 มาตรา 7-9 กำหนดให้เจ้าของข้อมูล มีสิทธิที่จะร้องขอให้ผู้ควบคุมดูแลข้อมูลให้ข้อเท็จจริงแก่ตนว่า ผู้ควบคุมดูแลข้อมูลได้ดำเนินการประมวลผลข้อมูลส่วนบุคคลของตนอยู่ หรือไม่อย่างใด โดยเจ้าของข้อมูลจะต้องทำคำร้องขอเป็นลายลักษณ์อักษร (ซึ่งรวมถึงการร้องผ่านทางสื่ออิเล็กทรอนิกส์ด้วย) และอาจต้องเสียค่าธรรมเนียมตามที่ผู้ควบคุมดูแลข้อมูลกำหนดด้วย ทั้งนี้ ผู้ควบคุมดูแลข้อมูลจะต้องทำตามคำร้องขอดังกล่าวภายใน 40 วันนับแต่วันที่ได้รับคำร้องขอจากเจ้าของข้อมูล (กรณีทั่วไป) หากปรากฏว่า ผู้ควบคุมดูแลข้อมูลได้ดำเนินการประมวลผลข้อมูลส่วนบุคคลของผู้ร้องขออยู่ ผู้ร้องขอในฐานะเจ้าของข้อมูล มีสิทธิจะได้รับคำอธิบายเพิ่มเติมเกี่ยวกับข้อมูลส่วนบุคคลของตนที่ผู้ควบคุมดูแลข้อมูลประมวลผลอยู่วัตถุประสงค์ของการประมวลข้อมูล และผู้รับข้อมูลหรือผู้ที่จะได้รับรู้ข้อมูลจากการเปิดเผยข้อมูลส่วนบุคคล

นอกจากนี้ เจ้าของข้อมูลยังมีสิทธิอื่น ๆ ที่เกี่ยวกับการเข้าถึงข้อมูลอีก เช่น สิทธิที่จะขอสำเนาเอกสารเกี่ยวกับข้อมูลส่วนบุคคล สิทธิที่จะรู้ถึงแหล่งที่มาของข้อมูล เป็นต้น หากเจ้าของข้อมูล ร้องขอให้ผู้ควบคุมดูแลข้อมูล ส่งข้อมูลส่วนบุคคลให้แก่ตนแล้ว แต่ผู้ควบคุมดูแลข้อมูลไม่ดำเนินการให้ เจ้าของข้อมูลอาจร้องขอต่อศาลได้ ซึ่งศาลอาจสั่งให้ผู้ควบคุมดูแลข้อมูลเปิดเผยข้อมูลที่เกี่ยวข้องแก่ศาลเพื่อใช้ประกอบการพิจารณาคำร้องขอของเจ้าของข้อมูลได้ (เป็นการเปิดเผยเฉพาะแก่ศาลเท่านั้น) หากศาลพิจารณาแล้วเห็นว่าเจ้าของข้อมูลเป็นผู้มีสิทธิตามกฎหมายที่จะได้รับข้อมูลเหล่านั้น ก็อาจมีคำสั่งให้ผู้ควบคุมดูแลข้อมูลปฏิบัติตามคำร้องขอของเจ้าของข้อมูลได้ ทั้งนี้ขึ้นอยู่กับดุลพินิจของศาล

2. สิทธิในการป้องกันการประมวลผลข้อมูลที่อาจก่อให้เกิดความเสียหายหรือความทุกข์ Data Protection Act 1998 มาตรา 10 ได้กำหนดไว้ว่าหากเจ้าของข้อมูลเห็นว่าการที่ผู้ควบคุมดูแลข้อมูลทำการประมวลผลข้อมูลส่วนบุคคลของตน จะทำให้เกิดความเสียหายหรือความทุกข์และเป็นการไม่สมเหตุสมผล ย่อมมีสิทธิที่จะบอกกล่าวไปยัง ผู้ควบคุม ดูแลข้อมูล เพื่อให้ยุติการประมวลผลข้อมูลดังกล่าวได้ โดยต้องบอกกล่าวเป็นลายลักษณ์อักษร และภายใน 21 วันหลังจากได้รับคำบอกกล่าวแล้ว ผู้ควบคุมดูแลข้อมูลจะต้องดำเนินการอย่างใดอย่างหนึ่งดังต่อไปนี้

1) แจ้งเป็นลายลักษณ์อักษรให้เจ้าของข้อมูลทราบว่า ผู้ควบคุม ดูแลข้อมูลได้ดำเนินการหรือตั้งใจจะดำเนินการตามคำบอกกล่าวของเจ้าของข้อมูล หรือ

2) แจ้งเป็นลายลักษณ์อักษรให้เจ้าของข้อมูลทราบว่าจะได้มีการดำเนินการบางส่วนตามคำบอกกล่าวของเจ้าของข้อมูลแล้ว (หากมี) และอธิบายถึงเหตุผลของผู้ควบคุมดูแลข้อมูลที่เห็นว่าคำบอกกล่าวของเจ้าของข้อมูลไม่มีความชอบธรรมเพราะเหตุใด

3. สิทธิในการป้องกันการประมวลผลข้อมูลเพื่อทำการตลาดแบบตรง Data Protection Act 1998 มาตรา 11 (1) ได้ กำหนดให้เจ้าของข้อมูลมีสิทธิบอกกล่าวเป็นลายลักษณ์อักษรให้ผู้ควบคุมดูแลข้อมูลยุติหรืองดเว้นไม่ดำเนินการประมวลผลข้อมูลของตนเพื่อประโยชน์ในการทำการตลาดแบบตรงได้ โดย Data Protection Act 1998 ไม่ได้กำหนดข้อยกเว้นหรือข้อจำกัดการใช้สิทธิไว้แต่อย่างใด

นอกจากนี้ EU Directive (95/46/EC) Article 14 (b) ยังได้ กำหนดให้เจ้าของข้อมูลมีสิทธิที่จะคัดค้านการประมวลผลข้อมูลส่วนบุคคลของตนซึ่งผู้ควบคุมดูแลข้อมูลคาดว่าจะเป็นกาประมวลผลข้อมูล เพื่อวัตถุประสงค์ในการทำการตลาดแบบตรงต่อไป หรือคัดค้านการเปิดเผยข้อมูลให้แก่บุคคลที่สาม หรือ การใช้ข้อมูล ในนามของบค คลที่สามเพื่อวัตถุประสงค์ในการทำการตลาดแบบตรง

4. สิทธิเกี่ยวกับการตัดสินใจโดยอาศัยการประมวลผลข้อมูลของเครื่องมือซึ่งทำงานโดยอัตโนมัติ Data Protection Act 1998 มาตรา 12 กำหนดให้สิทธิแก่เจ้าของข้อมูลที่จะบอกกล่าวเป็นลายลักษณ์อักษร ไม่ให้ผู้ควบคุมดูแลข้อมูลดำเนินการตัดสินใจใด ๆ ซึ่งจะมีผลกระทบที่สำคัญแก่ตนโดยอาศัยการประมวลผลของเครื่องมือที่ทำงานโดยอัตโนมัติเพียงอย่างเดียวเท่านั้น

5. สิทธิเรียกร้องค่าเสียหายในกรณีที่บุคคลนั้น ได้รับความเสียหายจากการที่ผู้ควบคุมดูแลข้อมูล ปฏิบัติฝ่าฝืน Data Protection Act 1998 มาตรา 13 กำหนดให้บุคคลธรรมดาที่ได้รับความเสียหาย (Damage) หรือความเสียหายและความทุกข์ (Damage and Distress) จากการที่ควบคุมดูแลข้อมูลปฏิบัติฝ่าฝืนบทบัญญัติใน Data Protection Act 1998 มีสิทธิที่จะได้รับการชดเชยความเสียหาย หากผู้ควบคุมดูแลข้อมูลไม่สามารถพิสูจน์ได้ว่าตนได้ใช้ความระมัดระวังตามสมควรแก่ทุกสภาวการณ์เพื่อที่จะปฏิบัติให้เป็นไปตามบทบัญญัติกฎหมายที่เกี่ยวข้องแล้ว

6. สิทธิในการดำเนินการเพื่อแก้ไข ลบ หรือทำลายข้อมูลที่ไม่ถูกต้อง Data Protection Act 1998 มาตรา 14 กำหนดไว้ว่าหากเจ้าของข้อมูลเห็นว่าข้อมูลส่วนบุคคลของตนที่อยู่ในความครอบครองของผู้ควบคุมดูแลข้อมูลไม่เที่ยงตรง แต่ข้อมูลนั้นเป็นข้อมูลที่ผู้ควบคุมดูแลข้อมูลได้บันทึกไว้อย่างถูกต้องตรงตามที่เจ้าของข้อ มูลหรือบุคคลที่สามเปิดเผยให้แก่ผู้ควบคุมดูแลข้อมูลในกรณีนี้ กำหนดให้ศาลมีอำนาจสั่งให้ผู้ควบคุมดูแลข้อมูลแนบถ้อยคาแสดงถึงข้อมูลที่ถูกต้องเที่ยงตรงตามที่ศาลเห็นชอบแล้วไว้เป็นส่วนหนึ่งของข้อมูลเดิมได้แทนที่จะมีคำสั่งให้ผู้ควบคุมดูแลข้อมูล แก้ไขลบหรือทำลายข้อมูล

7. สิทธิในการขอให้ตรวจสอบประเมินผลการปฏิบัติตามกฎหมาย Data Protection Act 1998 มาตรา 42 กำหนด ว่า บุคคลใดเห็นว่าตนได้รับผลกระทบโดยตรงจากการประมวลผลข้อมูลของผู้ควบคุมดูแลข้อมูลมีสิทธิร้องขอให้ Commissioner เข้าตรวจสอบและประเมินผลการปฏิบัติงานของผู้ควบคุมดูแลข้อมูลนั้นว่าได้มีการปฏิบัติฝ่าฝืนกฎหมายหรือไม่ อย่างไร (บุคคลตามมาตรา 42 นี้ รวมถึงนิติบุคคลด้วย)

ต่อเมื่อมีการประกาศใช้ The Data Protection Act 2018 จะเห็นว่ามีสิทธิของเจ้าของข้อมูลส่วนบุคคลยังคงเป็นไปตามหลักการเดิมและมีการเพิ่มเติมในส่วนของ data portability เข้ามาโดยสิทธิตามกฎหมายฉบับใหม่มีโดยสรุปดังนี้คือ [141]

1. สิทธิในการเข้าถึงข้อมูลส่วนบุคคล (Right to Access Personal Data)

2. สิทธิที่จะได้รับการแจ้งเตือนเมื่อจะมีการใช้ข้อมูลส่วนบุคคล (Right to be Informed about How Data is Being Used)

3. สิทธิที่ได้รับการแก้ไขปรับปรุงข้อมูลที่ไม่ถูกต้อง (Right to have Incorrect Data Updated)

4. สิทธิที่จะขอลบข้อมูลส่วนบุคคล (Right to have Data Erased)

5. สิทธิที่จะขอให้หยุดหรือจำกัดการประมวลผลข้อมูลส่วนบุคคล (Right to Stop or Restrict the Processing of Data)

6. สิทธิที่จะขอโอนข้อมูลส่วนบุคคลไปยังผู้ให้บริการรายอื่น (Right to Data Portability (Allowing to Get and Reuse Your Data for Different Services))

7. สิทธิที่จะคัดค้านการประมวลผลข้อมูลส่วนบุคคล (Right to Object to How Data Is Processed in Certain Circumstances)

3.2.2.2 หลักการและข้อจำกัดในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล

ขอบเขตการใช้ Data Protection Act 1998 กำหนดไม่ให้บุคคลผู้ปฏิบัติงานอยู่ในสำนักงานคอมพิวเตอร์หรือตัวแทนของบุคคลดังกล่าวเปิดเผยข้อมูลอันเกี่ยวกับบุคคลโดยปราศจากอำนาจ ถ้าบุคคลใดฝ่าฝืนโดยเจตนาหรือไม่นำพาถึงผลที่จะเกิดขึ้นถือว่า กระทำผิดตามพระราชบัญญัติฉบับนี้

---

[141] Information Commissioner's Office (ICO), **Individual Rights,** Retrieved March 1, 2019 from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

นอกจากนั้นยังได้กำหนดสิทธิของบุคคลผู้ถูกระบุในข้อมูลนั้น ๆ เช่น สิทธิที่จะได้ทราบว่าตนถูกระบุอยู่ในข้อมูลนั้นหรือไม่ สิทธิที่จะเข้าสู่ข้อมูลอันเกี่ยวกับตน สิทธิในการแก้ไขหรือลบล้างข้อมูลที่ผิดพลาด สิทธิที่จะอนุญาตหรือไม่อนุญาตให้มีการเปิดเผยข้อมูล สิทธิในการดำเนินการเรียกร้องค่าเสียหายในกรณีที่บุคคลธรรมดานั้น ได้รับความเสียหายจากการที่ผู้ควบคุมดูแลข้อมูลปฏิบัติฝ่าฝืน เป็นต้น

การกำหนดหลักการคุ้มครองข้อมูลส่วนบุคคลไว้ 8 ข้อ (หรืออาจเรียกว่า “หลักของการจัดการข้อมูลที่ดี”) โดย Data Protection Act 1998 มาตรา 4 ได้กำหนดว่า หลักการคุ้มครองข้อมูลส่วนบุคคลที่อ้างถึงในพระราชบัญญัติฉบับนี้ คือ หลักการที่กำหนดไว้ใน Part I Schedule 1 ซึ่งสาระสำคัญ คือ การกำหนดให้ผู้ควบคุมดูแลข้อมูล ต้องปฏิบัติตามหลักการดังกล่าวเว้น แต่ผู้ควบคุมดูแลข้อมูลจะสามารถอ้างสิทธิจากข้อยกเว้นของหลักต่าง ๆ นั้นได้ อันเป็นการบังคับให้ผู้ควบคุมดูแลข้อมูลต้องปฏิบัติตามหลักการต่าง ๆ นี้ ไม่ว่าผู้ควบคุมดูแลข้อมูลนั้นจะมีหน้าที่ตามกฎหมายที่จะต้องจดแจ้งข้อมูลหรือไม่ก็ตามและเป็นการบังคับใช้กับข้อมูลส่วนบุคคลทั้งหมดที่ถูกประมวลผลโดยผู้ควบคุมดูแลข้อมูล หลักการดังกล่าวได้แก่[142]

หลักประการที่ 1 (The First Principle) คือ ข้อมูลส่วนบุคคลจะต้องถูกประมวลผลอย่างเป็นธรรมและถูกต้องตามกฎหมาย โดยเฉพาะอย่างยิ่งจะถูกประมวลไม่ได้ เว้นแต่เป็นไปตามเงื่อนที่กฎหมายกำหนด

หลักประการที่ 2 (The Second Principle) คือ จะทำการจัดเก็บข้อมูลส่วนบุคคลไว้ได้เพียงเท่าที่ระบุไว้ในวัตถุประสงค์ และจะต้องเป็นวัตถุประสงค์อันชอบด้วยกฎหมายเท่านั้น ทั้งจะต้องไม่มีการประมวลผลที่ไม่สอดคล้องกับวัตถุประสงค์ดังกล่าว

ในการนี้ผู้ควบคุมดูแลข้อมูลจะต้องแจ้งให้เจ้าของข้อมูล และ Commissioner ได้รู้ถึงวัตถุประสงค์ของการจัดเก็บโดยการระบุวัตถุประสงค์ไว้ในเอกสารดังต่อไปนี้

1. หนังสือบอกกล่าวที่ผู้ควบคุมดูแลข้อมูลแจ้งไปยังเจ้าของข้อมูล หรือ
2. ทะเบียนการจดแจ้งข้อมูลของผู้ควบคุมดูแลข้อมูลที่ให้ไว้ต่อ Commissioner

หลักประการที่ 3 (The Third Principle) คือ ข้อมูลส่วนบุคคลจะต้องเพียงพอเกี่ยวข้องและไม่มากเกินไปกว่าวัตถุประสงค์ของการประมวลผลนั้น

หลักการข้อนี้อาจเรียกอีกชื่อหนึ่งได้ว่า “หลักความเพียงพอ (Adequacy Principle)” กล่าวคือ ผู้ควบคุมดูแลข้อมูล จะจัดเก็บข้อมูลส่วนบุคคลเกินกว่า ความจำเป็นตามที่ระบุไว้ในวัตถุประสงค์ของการจัดเก็บมิได้ ดังนั้น เพื่อให้การประมวลผลข้อมูลเป็นไปอย่างถูกต้องและสอดคล้องกับหลักการข้อนี้ ผู้ควบคุมดูแลข้อมูลส่วนบุคคลควรจะทบทวนแบบฟอร์มการกรอกข้อมูล

---

[142] *Ibid.*

เพื่อจัดเก็บข้อมูล เพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลที่จะทำการจัดเก็บมีเพียงพอ เกี่ยวข้องและไม่เกินกว่าวัตถุประสงค์ที่กำหนดไว้ เช่นแบบฟอร์มการสมัครงาน แบบฟอร์มสำหรับรายละเอียดของลูกค้า

หลักประการที่ 4 (The Fourth Principle) คือการจัดเก็บข้อมูลส่วนบุคคลจะต้องทำให้ถูกต้องเที่ยงตรงและทันสมัยอยู่เสมอ

หลักการข้อนี้ เป็นหลักการที่กำหนดถึงหน้าที่ของผู้ควบคุมดูแลข้อมูล กล่าวคือ กำหนดให้ผู้ควบคุมดูแลข้อมูล มีหน้าที่โดยตรงในการทำให้ข้อมูลส่วนบุคคลซึ่งตนได้ทำการประมวลผลไว้ให้มีความเที่ยงตรงและทันสมัยอยู่เสมอ นอกจากนี้ หน้าที่ดังกล่าวยังเป็นหน้าที่ที่ไม่อาจมอบหมายให้คนอื่นทำแทนได้

หลักประการที่ 5 (The Fifth Principle) คือ การเก็บข้อมูลส่วนบุคคลไม่ว่าเพื่อวัตถุประสงค์ใด ๆ จะต้องไม่จัดเก็บไว้นานเกินกว่าความจำเป็นเพื่อวัตถุประสงค์นั้น

การจัดเก็บข้อมูลส่วนบุคคลไว้นานเกินกว่าความจำเป็นตามวัตถุประสงค์ของการประมวลผลข้อมูลนั้น ๆ ถือเป็นการปฏิบัติฝ่าฝืนหลักการในข้อนี้ อีกทั้งใน Data Protection Act 1998 เองก็ไม่ได้กำหนดรายละเอียดหรือหลักเกณฑ์เกี่ยวกับหลักการนี้ไว้ นอกจากนี้แนวทางการบังคับใช้กฎหมายของ Commissioner ในเรื่องนี้ก็มีอยู่อย่างจำกัด ดังนั้นจึงยังไม่ชัดเจนว่าระยะเวลานานเท่าใดจึงจะถือว่าเป็นระยะเวลานานเกินความจำเป็น

ดังนั้น การที่จะปฏิบัติตามหลักการนี้ได้จะต้องพิจารณาข้อเท็จจริงเป็นกรณี ๆ ไป โดยผู้ควบคุมดูแลข้อมูลจะต้องตรวจสอบข้อมูลส่วนบุคคลที่ถูกประมวลผลทั้งหมดและวัตถุประสงค์ของการประมวลผลนั้น และทำการพิจารณาว่าข้อมูลส่วนบุคคลแต่ละข้อมูลต้องจัดเก็บเอาไว้เพื่อวัตถุประสงค์ที่กำหนดไว้เป็นเวลานานเท่าใด โดยอาจกำหนดนโยบายในการเก็บรักษาข้อมูลด้วยการกำหนดระยะเวลาในการเก็บข้อมูลแต่ละประเภทไว้และหากผู้ควบคุมดูแลข้อมูลต้องการเก็บข้อมูลส่วนบุคคลไว้เป็นระยะเวลานานก็ควรมีเอกสารบ่งบอกถึงเหตุผลของการเก็บข้อมูลนั้น ๆ ไว้ในช่วงระยะเวลานั้นด้วย

นอกจากนี้ ผู้ควบคุมดูแลข้อมูลซึ่งมีข้อผูกพันที่จะต้องทำลายข้อมูลต้องจำไว้ว่ากระบวนการทำลายตัวมันเองจะมีค่าเท่ากับเป็นการประมวลผล ดังนั้นผู้ควบคุมดูแลข้อมูลจะต้องดำเนินการตามหลักการข้ออื่น ๆ ด้วย

อนึ่ง ตามหลักทั่วไปข้อมูลส่วนบุคคลควรถูกทำลายเมื่อไม่มีความต้องการข้อมูลนั้นอีก แต่ในบางกรณีอาจมี การกำหนดให้มีการเก็บข้อมูลส่วนบุคคลนั้นได้นานกว่าในกรณีปกติได้โดยการอาศัยอำนาจตามกฎหมายว่า ด้วยการต่อต้านการก่อการร้าย (Anti-Terrorism Crime and Security Act 2001)

หลักประการที่ 6 (The Sixth Principle) คือ จะต้องทำการประมวลผลข้อมูลส่วนบุคคลให้สอดคล้องกับสิทธิของเจ้าของข้อมูลตามที่กำหนดไว้ใน Data Protection Act 1998

Schedule 1 ของ Data Protection Act 1998 วางหลักไว้ว่า หากผู้ประมวลผลข้อมูลกระทำการดังต่อไป ให้ถือว่าเป็นการกระทำที่ฝ่าฝืนหลักการคุ้มครองข้อมูลประการที่หก

1. ละเมิดสิทธิในการเข้าถึงข้อมูลตามที่กำหนดไว้ใน Section 7

2. ไม่ปฏิบัติตามคำร้องขอที่สมเหตุสมผลของเจ้าของข้อมูลที่ให้ยุติการประมวลผลข้อมูลตามที่กำหนดไว้ใน Section 10 หรือไม่ปฏิบัติตามคำร้องนั้นภายใน 21 วันนับแต่วันได้รับคำร้องขอ

3. ไม่ปฏิบัติตามคำร้องขอให้ยุติการประมวลผลข้อมูล เพื่อทำการตลาดแบบตรงตามที่กำหนดไว้ใน Section 11

4. ปฏิบัติฝ่าฝืน Section 13 โดยไม่ปฏิบัติตามคำร้องขอเกี่ยวกับการตัดสินใจโดยอาศัยการประมวลผลของเครื่องมือที่ทางานโดยอัตโนมัติหรือการไม่แจ้งให้เจ้าของข้อมูลทราบถึงการตัดสินใจตามคำร้องนั้น หรือการไม่ตอบกลับไปยังเจ้าของข้อมูลภายใน 21 วันนับแต่วันที่ได้รับคำร้องนั้น

5. ปฏิบัติฝ่าฝืน Section 12 a (สิทธิเฉพาะกาล (Transition Rights)) โดยการไม่ปฏิบัติตามคำบอกกล่าว (Notice) ของ Commissioner ที่ชอบด้วยกฎหมาย

หลัก ประการที่ 7 (The Seventh Principle) คือ ต้องจัดให้มีมาตรการทางเทคนิคและการจัดการที่เหมาะสมในการป้องกันและจัดการกับการประมวลผลข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตหรือไม่ชอบด้วยกฎหมาย และเพื่อป้องกันการสูญหายหรือการทำลายหรือทำให้เสียหายต่อข้อมูลส่วนบุคคล

หลักการข้อนี้ มีรากฐานมาจาก EU Directive (95/46/EC) มีวัตถุประสงค์เพื่อให้ผู้ควบคุมดูแลข้อมูลเกิดความระมัดระวังในการประมวลผลข้อมูล และเป็นการกำหนดมาตรการเพื่อให้เจ้าของข้อมูลเกิดความมั่นใจว่าข้อมูลส่วนบุคคลของตนจะได้รับการดูแลอย่างเหมาะสม

แม้จะมีรากฐานมาจากที่เดียวกัน แต่ก็มีความแตกต่างบางประการ นั่นคือ EU Directive (95/46/EC) กำหนดให้ผู้ควบคุมดูแลข้อมูลต้องกำหนดให้มีมาตรการในการรักษาความปลอดภัยในระดับที่เหมาะสมกับความเสียหายที่อาจเกิดขึ้นจากการประมวลผลและจากลักษณะของข้อมูลนั้น เอง แต่หลักประการที่ 7 นี้ จะเน้นในเรื่องการกำหนดให้ มีมาตรการเพื่อป้องกันไม่ให้เกิดความเสียหายแก่เจ้าของข้อมูลที่อาจจะได้รับผลเสียหายจากการฝ่าฝืนบทบัญญัติในเรื่องการรักษาความปลอดภัย

หลักประการที่ 8 (The Eight Principle) คือข้อมูลส่วนบุคคลจะต้องไม่ถูกส่งออกไปยังประเทศหรือดินแดนที่อยู่นอกเขต European Economic Area (EEA) เว้นแต่ประเทศหรือดินแดนนั้นรับรองว่ามีระดับการคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลที่เพียงพอสำหรับการประมวลผลข้อมูลส่วนบุคคล

การที่ Data Protection Act 1998 กำหนดห้ามมิให้มีการส่งหรือโอนข้อมูลออกไปยังประเทศที่มิใช่สมาชิกของ European Economic Area (EEA) ก็เพื่อให้ความคุ้มครองแก่เจ้าของข้อมูล ทั้งนี้เนื่องจากหากประเทศนอกกลุ่ม EEA ไม่มีกฎหมายที่ให้ความคุ้มครองเกี่ยวกับข้อมูลส่วนบุคคลหรือมีกฎหมายเช่นว่า นี้แต่ไม่ได้ระดับมาตรฐานเดียวกับ EU Directive (95/46/EC) ก็ไม่ถูกผูกพันให้ต้องมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลตามหลักการที่กำหนดใน EU Directive(95/46/EC) แต่เพื่อให้เกิดความคล่องตัวทางการค้า Data Protection Act 1998 จึงได้กำหนดให้หลักประการที่ 8 นี้มีข้อยกเว้นดังนี้

1. กรณีที่ได้รับความยินยอมจากเจ้าของข้อมูล
2. การส่งออกข้อมูลมีความจำเป็น
    1) เพื่อดำเนินการตามสัญญาซึ่งเจ้าของข้อมูลเป็นคู่สัญญา หรือ
    2) เพื่อการดำเนินการตามความประสงค์ของเจ้าของข้อมูล โดยมีความมุ่งหมายเพื่อเข้าทำสัญญา
3. การส่งออกข้อมูลมีความจำเป็น เพื่อประโยชน์ในการลงนามหรือสรุปสัญญาระหว่างผู้ควบคุม ดูแลข้อมูลกับบุคคลที่ไม่ใช่เจ้าของข้อมูลแต่เป็นผู้เข้าทำสัญญาโดยได้รับการร้องขอจากเจ้าของข้อมูลหรือประโยชน์ของเจ้าของข้อมูล
4. การส่งออกข้อมูลมีความจำเป็นเพื่อประโยชน์สำคัญของสาธารณะ
5. การส่งออกข้อมูล
    1) มีความจำเป็นเพื่อวัตถุประสงค์ของหรือที่เกี่ยวข้องกับการดำเนินกระบวนการทางกฎหมาย
    2) มีความจำเป็นเพื่อการได้รับความเห็นทางกฎหมาย
    3) มีความจำเป็นเพื่อการก่อ ใช้ และสงวนไว้ซึ่งสิทธิตามกฎหมาย
6. การส่งออกข้อมูลมีความจำเป็นเพื่อที่จะคุ้มครองประโยชน์สำคัญต่อชีวิตของเจ้าของข้อมูล
7. การส่งข้อมูลส่วนบุคคลที่เป็นส่วนหนึ่งของข้อมูลซึ่งปรากฏอยู่ในทะเบียนสาธารณะ
8. การส่งข้อมูลนั้นกระทำโดยอยู่ภายใต้เงื่อนไขที่ Commissioner ได้ให้ความเห็นชอบแล้ว และเงื่อนไขนั้น ได้มีการกำหนดเงื่อนเวลากับมาตรการในการคุ้มครองสิทธิ และเสรีภาพของเจ้าของข้อมูลอย่างเพียงพอแล้ว
9. การส่งออกข้อมูลนั้นได้รับอนุญาตจาก Commissioner ให้กระทำได้ เนื่องจากมีมาตรการในการคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลอย่างเพียงพอแล้ว

ข้อยกเว้น การคุ้มครองข้อมูลส่วนบุคคลตาม Data Protection Act 1998 กำหนดไว้ 10 กรณีเพื่อเปิดช่องทางให้เข้าถึงข้อมูลส่วนบุคคลได้ ได้แก่

1. กรณีเกี่ยวด้วยความมั่นคงของประเทศ
2. กรณีเกี่ยวด้วยอาชญากรรมและภาษีอากร
3. กรณีเกี่ยวด้วยงานด้านสุขภาพและสังคม
4. กรณีเกี่ยวด้วยการออกกฎระเบียบด้านการบริการทางการเงิน
5. กรณีเกี่ยวด้วยสิทธิพิเศษในการประกอบอาชีพด้านกฎหมายและการพิจารณาพิพากษาของศาล
6. กรณีเกี่ยวด้วยบัญชีเงินเดือนและบัญชีรายรับรายจ่าย
7. กรณีเกี่ยวด้วยข้อมูลส่วนบุคคลที่จัดเก็บไว้เพื่อภายในบ้านของตนหรือเพื่อวัตถุประสงค์อื่นอันจำกัด
8. กรณีเป็นข้อมูลที่จัดเก็บในฐานะที่เป็นสมาชิก
9. กรณีเพื่อการเก็บสถิติหรือการค้นคว้า
10. กรณีเกี่ยวกับคะแนนในการทดสอบ

การเข้าถึงข้อมูลส่วนบุคคล ผู้เป็นเจ้าของข้อมูลมีสิทธิที่จะได้รับสำเนาบันทึก ข้อมูลส่วนบุคคลของตนจากผู้เก็บและใช้ข้อมูลนั้น ๆ หากข้อมูลนั้นอยู่ในรูปแบบหรือถ้อยคำที่ไม่อาจเข้าใจได้ จะต้องมีคำอธิบายประกอบข้อมูลนั้นมาให้พร้อมกับสำเนาข้อมูลซึ่งการร้องขอดังกล่าวจะต้องเป็นไปตามเงื่อนไขที่กำหนดไว้ดังนี้[143]

1. คำร้องจะต้องทำเป็นหนังสือและชำระค่าธรรมเนียมในการร้องขอ (หากไม่ระบุไว้เป็นอย่างอื่น) การร้องขอต้องเป็นไปเพื่อที่จะได้รับการแจ้งให้ทราบว่ามีข้อมูลส่วนบุคคลของตนหรือไม่ ถ้ามีจะได้ขอรับสำเนาข้อมูลนั้นด้วยหากผู้เก็บและใช้ข้อมูล ได้จดทะเบียนการเก็บและใช้ข้อมูลแยกเป็นกรณี จะต้องทาคำร้องขอและชาระค่าธรรมเนียมแยกกัน
2. ผู้ร้องขอจะต้องแสดงหลักฐานประจำตัวและระบุรายละเอียดถึงข้อมูลที่ตนต้องการตามที่ผู้เก็บและผู้ใช้ข้อมูลได้กำหนดไว้ตามสมควร ถ้าเป็นข้อมูลที่เมื่อเปิดเผยแล้วต้องเปิดเผยข้อมูลส่วนบุคคลของบุคคลอื่นด้วย จะต้องขออนุญาตจากบุคคลนั้น ๆ เสียก่อน
3. ผู้เก็บและใช้ข้อมูลจะต้องตอบคำร้องขอภายใน 40 วันหลังจากที่ได้รับคำร้องขอและหลักฐานต่าง ๆ ตามเงื่อนไขที่กำหนดไว้
4. กรณีที่ข้อมูลส่วนบุคคลนั้นเป็นเรื่องของสุขภาพร่างกายรัฐมนตรีว่าการกระทรวงการต่างประเทศมีอำนาจที่จะแก้ไขหรือยกเว้นบทบัญญัติที่เกี่ยวกับการเข้าสู่ข้อมูลของ

---

[143] กิตติพงศ์ กมลธรรมวงศ์, *เรื่องเดิม*, หน้า 168-175.

บุคคลหนึ่ง ๆ ได้ตามสมควร ดังนั้น หากเป็นกรณีข้อมูลทางการแพทย์และการขอเข้าสู่ข้อมูลนั้นโดยตรงจะเป็นผลร้ายต่อบุคคลผู้ร้องขอ รัฐมนตรีว่าการกระทรวงการต่างประเทศย่อมมีอำนาจที่จะออกกฎระเบียบให้การเข้าสู่ข้อมูลในกรณีดังกล่าวเป็นไปโดยทางอ้อม หรือต้องเข้าสู่ข้อมูลนั้นโดยผ่านบุคคลอื่น

การแก้ไขเพิ่มเติมข้อมูลส่วนบุคคล การที่บุคคลหนึ่ง ๆ จะต้องได้รับสิทธิที่จะแก้ไขเพิ่มเติมหรือลบข้อมูลส่วนบุคคลของตนได้ ดังนั้น จึงได้กำหนดให้บุคคลสามารถร้องขอแก้ไขเพิ่มเติมข้อมูลส่วนบุคคลของตนได้เป็น 2 กรณี คือ

กรณีที่ 1 เป็นการร้องขอแก้ไขเพิ่มเติมข้อมูลส่วนบุคคลของตนต่อผู้เก็บและใช้ข้อมูลนั้นโดยตรง

จากหลักการดังกล่าวข้างต้น จึงมีการกำหนดให้ใช้บังคับกับผู้เก็บและใช้ข้อมูลส่วนบุคคลของบุคคลใด ๆ และบุคคลผู้ปฏิบัติงานในสำนักงานคอมพิวเตอร์ซึ่งเก็บและใช้ข้อมูลดังกล่าว ดังนั้น หากบุคคลได้ร้องขอและเข้าสู่ข้อมูลส่วนบุคคลของตนเพื่อตรวจดูและรับสำเนาข้อมูลแล้วพบว่าข้อมูลที่ได้รับจากหน่วยงานหรือผู้เก็บและใช้ข้อมูลมีความผิดพลาดหรือไม่เป็นไปตามที่กฎหมายกำหนดไว้ ก็สามารถร้องขอให้มีการดำเนินการแก้ไขเพิ่มเติมหรือ ลบข้อมูลที่ผิดพลาดหรือบกพร่องนั้น ๆ และหน่วยงานหรือผู้เก็บและใช้ข้อมูลนั้นต้องรีบตรวจสอบและดำเนินการแก้ไขเพื่อให้เป็นไปตามหลักการดังกล่าวข้างต้น

หากหน่วยงานหรือผู้เก็บและใช้ข้อมูลดังกล่าวเพิกเฉยหรือไม่ดำเนินการใด ๆ บุคคลผู้ร้องขออาจยื่นคำร้องต่อ The Commissioner ว่ามีการล่วงละเมิดหลักการคุ้มครองข้อมูลส่วนบุคคลและเจ้าหน้าที่ดังกล่าวก็จะดำเนินการกับผู้ฝ่าฝืนตามที่พระราชบัญญัติฉบับนี้กำหนดไว้หรือหากเข้าเงื่อนไขตามที่กฎหมายกำหนดก็อาจยื่นคำร้องขอต่อศาลให้มีการดำเนินการเช่นนั้น

กรณีที่ 2 เป็นการร้องขอแก้ไขเพิ่มเติมข้อมูลส่วนบุคคลของตนต่อศาล

การที่สิทธิของบุคคลซึ่งได้รับการรับรองคุ้มครองตามกฎหมายถูกล่วงละเมิดบุคคลผู้ได้รับความเสียหายย่อมมีสิทธิที่จะร้องขอต่อศาลเพื่อให้มีการบังคับการตามสิทธิของตนได้ ซึ่งพระราชบัญญัติฉบับนี้ก็ได้ให้การรับรองไว้โดยกำหนดเงื่อนไขที่ จะสามารถร้องขอต่อศาลทั้งยังกำหนดให้ศาลมีอำนาจในการที่จะออกคำสั่งในเรื่องนี้ได้

จากหลักการข้างต้นของ Data Protection Act 1998 เมื่อพิจารณาเปรียบเทียบกับหลักการที่ได้รับการปรับปรุงตาม Data Portection Act 2018 ที่เป็นไปตามหลักการของ General Data Protection Regutation สามารถสรุปความเหมือนและแตกต่างได้ดังตารางต่อไปนี้คือ[144]

ตารางที่ 3.1 เปรียบเทียบ Data Protection Act 1998 และ Data Portection Act 2018

หัวข้อ	DPA 1998	DPA 2018 & GDPR
หลักความชอบด้วยกฎหมาย (Lawfulness)	ข้อมูลส่วนบุคคลจะต้องถูกประมวลผลภายใต้เงื่อนไขของความเป็นธรรมและถูกต้องตามกฎหมาย	การประมวลผลข้อมูลส่วนบุคคลจะต้องเป็นไปโดยชอบด้วยกฎหมายอย่างเป็นธรรมและโปร่งใส
หลักข้อจำกัดตามวัตถุประสงค์ (Purpose)	ข้อมูลส่วนบุคคลจะต้องถูกรวบรวมเพื่อวัตถุประสงค์ที่ถูกต้องตามกฎหมายและจะต้องไม่ถูกประมวลผลในลักษณะที่ไม่สอดคล้องกับวัตถุประสงค์ของข้อมูลส่วนบุคคลนั้น	การเก็บรวบรวมข้อมูลส่วนบุคคลต้องเป็นไปเพื่อวัตถุประสงค์ที่เฉพาะเจาะจง แจ้งชัดและชอบด้วยกฎหมาย ซึ่งข้อมูลดังกล่าวจะไม่ถูกนำไปประมวลผลในวัตถุประสงค์ที่แตกต่างไปจากวัตถุประสงค์ของข้อมูลนั้น
หลักการใช้ข้อมูลให้น้อยที่สุด (Data Minimization)	ข้อมูลส่วนบุคคลจะต้องมีได้เท่าที่เพียงพอ มีความเกี่ยวข้องและไม่มากเกินไปกว่าวัตถุประสงค์ของข้อมูลนั้น	ข้อมูลส่วนบุคคลนั้นจะมีได้เท่าที่เพียงพอ (Adequate) มีความเกี่ยวข้องและจำกัดเฉพาะสิ่งที่จำเป็นตามวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลเท่านั้น
หลักความถูกต้อง (Accuracy)	ข้อมูลส่วนบุคคลนั้น จะต้องมีความถูกต้อง ในกรณีที่จำเป็นก็จะต้องทำให้เป็นปัจจุบัน	ข้อมูลส่วนบุคคลนั้นจะต้องมีความถูกต้อง และในกรณีที่จำเป็นก็จะต้องทำให้เป็นปัจจุบัน ทั้งนี้ จะต้องมีการใช้วิธีการตามสมควรเพื่อให้ มั่นใจว่าข้อมูลส่วนบุคคลที่ไม่ถูกต้องตรงตาม

[144] Practical Law Employment, **Comparisons: DPA 1998 v GDPR and DPA 2018,** Retrieved March 10, 2019 from https://uk.practicallaw.thomsonreuters.com/w-011-6935?transitionTypeDefault&contextDatasc.Default)&firstPagetrue&comp= pluk&bhcp=1

ตารางที่ 3.1 (ต่อ)

หัวข้อ	DPA 1998	DPA 2018 & GDPR
		วัตถุประสงค์ของการประมวลผลจะถูกลบหรือได้รับการแก้ไขให้ถูกต้องโดยไม่ชักช้า
หลักการเก็บข้อมูลอย่างจำกัด (Storage)	ข้อมูลส่วนบุคคลจะไม่ถูกเก็บไว้นานเกินความจำเป็นสำหรับวัตถุประสงค์ในการประมวลผลข้อมูลเหล่านั้น	การเก็บข้อมูลส่วนบุคคลในรูปแบบที่สามารถบ่งชี้ตัวเจ้าของข้อมูลได้นั้น จะเก็บได้ไม่นานเกินกว่าที่จำเป็นเพื่อวัตถุประสงค์ในการประมวลผล (เว้นแต่กรณีที่เป็นไปเพื่อประโยชน์สาธารณะ ทางวิทยาศาสตร์ การวิจัยทางประวัติศาสตร์ หรือในเชิงสถิติ)
หลักการเข้าถึงข้อมูล (Access)	ข้อมูลส่วนบุคคลจะต้องถูกประมวลผลโดยให้เป็นไปตามสิทธิของเจ้าของข้อมูลส่วนบุคคล	ใน GDPR ไม่ได้บัญญัติไว้ในส่วนของหลักการ แต่แยกไปเขียนไว้ในส่วนของสิทธิของเจ้าของข้อมูลส่วนบุคคล
หลักความปลอดภัยของข้อมูล (Security)	จะต้องมีมาตรการทางเทคนิคและองค์กรที่เหมาะสมในการจัดการต่อการประมวล ผลข้อมูลโดยไม่ได้รับอนุญาตหรือผิดกฎหมาย และมีมาตรการต่อต้านการสูญหายหรือถูกทำลายโดยไม่ตั้งใจและความเสียหายต่อข้อมูลส่วนบุคคล	ในการประมวลผลข้อมูลส่วนบุคคลจะต้องมีการรักษาความมั่นคงปลอดภัยของข้อมูลที่เหมาะสม จะต้องป้องกันข้อมูลดังกล่าวจากการประมวลผลโดยปราศจากอำนาจหรือโดยไม่ชอบด้วยกฎหมาย และป้องกันข้อมูลจากการสูญหาย ทำลาย หรือเกิดความเสียหายโดยอุบัติเหตุ โดยใช้เทคนิคหรือกระบวนการจัดข้อมูลที่เหมาะสม
หลักการโอนข้อมูล Overseas transfer	ข้อมูลส่วนบุคคลจะไม่ถูกถ่ายโอนไปยังประเทศหรือดินแดนนอกเขตเศรษฐกิจของสหภาพยุโรปเว้นแต่ว่าประเทศหรือดินแดนนั้นจะมีระดับของการรับประกันการปกป้องสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วน	ใน GDPR ไม่ได้บัญญัติไว้ในส่วนหลักการ แต่แยกไปเขียนไว้ใน Chapter 5 เรื่องการถ่ายโอนข้อมูลส่วนบุคคลไปยังประเทศที่สามหรือองค์กรระหว่างประเทศ โดยกำหนดว่าหากคณะกรรมาธิการ (Commission)

ตารางที่ 3.1 (ต่อ)

หัวข้อ	DPA 1998	DPA 2018 & GDPR
	บุคคลที่เพียงพอ	พิจารณาเห็นว่า ประเทศที่จะมีการส่งข้อมูลส่วนบุคคลไปมีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอก็จะทำให้สามารถส่งข้อมูลได้โดยไม่ต้องอาศัยการอนุญาตเป็นการเฉพาะ (Specific Authorisation) แต่สำหรับประเทศที่ไม่มีมาตรฐานการคุ้มครองที่เพียงพอ ในการส่งข้อมูลก็จะต้องพิจารณาเงื่อนไขอื่นที่ทำให้สามารถส่งข้อมูลระหว่างกันได้ เช่น ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้จัดหามาตรการป้องกันที่เหมาะสม (Appropriate Safeguards) และจะต้องสามารถบังคับตามสิทธิของเจ้าของข้อมูลส่วนบุคคลและบังคับตามมาตรการเยียวยาตามกฎหมายให้แก่เจ้าของข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพ
หลักความรับผิดชอบ Accountability	ไม่มี	ผู้ควบคุมข้อมูลส่วนบุคคลมีภาระความรับผิดชอบที่จะต้องแสดงให้เห็นว่าตนสามารถปฏิบัติตามหลักการของการคุ้มครองข้อมูลส่วนบุคคล

กล่าวโดยสรุปได้ว่า หลักการของ Data Portection Act 2018 ที่ถูกตราขึ้นใหม่ให้มีหลักการสอดคล้องเป็นเช่นเดียวกันกับ GDPR นั้น เป็นกฎหมายที่มีพัฒนาการต่อเนื่องมาจากหลักการของ Data Portection Act 1998 เพื่อให้มีการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วน

บุคคลอย่างมีขอบเขตตามวัตถุประสงค์ของข้อมูล และยังมีการเพิ่มเติมในส่วนของผู้ควบคุมข้อมูลส่วนบุคคลให้ต้องรับผิดชอบในการคุ้มครองข้อมูลอย่างเป็นรูปธรรม

3.2.2.3 กลไกทางกฎหมายในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล

ในสหราชอาณาจักร The Information Commissioner's Office (ICO) รับผิดชอบในการบังคับใช้กฎหมาย ซึ่ง ICO ถือเป็นหน่วยงานอิสระที่ไม่ใช่ส่วนราชการ ซึ่งทำหน้าที่รายงานโดยตรงต่อรัฐสภาของอังกฤษ และได้รับการสนับสนุนในการปฏิบัติหน้าที่จาก กระทรวง Digital, Culture, Media and Sport (DCMS) จึงกล่าวได้ว่า ICO มีฐานะเป็นหน่วยงานกำกับดูแลข้อมูลส่วนบุคคลของรัฐที่เป็นอิสระ ซึ่งคำวินิจฉัยของ ICO สามารถถูกอุทธรณ์ต่อคณะกรรมการอิสระหรือศาลแล้วแต่กรณี อีกทั้ง ICO มีภารกิจในการส่งเสริมการเข้าถึงข้อมูลข่าวสารของทางราชการและขณะเดียวกันก็มีหน้าที่คุ้มครองดูแลสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลด้วย

ในการบังคับใช้กฎหมาย หาก ICO ทราบว่าผู้ควบคุมข้อมูลกระทำการขัดต่อกฎหมายก็สามารถแจ้งประกาศการบังคับใช้บังคับให้ผู้ควบคุมข้อมูลดำเนินการแก้ไขได้ หรือระงับการกระทำได้ ซึ่งหากมีการไม่ปฏิบัติตามประกาศหรือคำสั่งของ ICO ถือเป็นความผิดทางอาญาและสามารถถูกลงโทษด้วยการปรับค่าปรับสูงสุด 5,000 ปอนด์ในศาลแขวง หรือโทษปรับอย่างไม่จำกัดในศาลจังหวัด[145]

โดย ICO สามารถกำหนดค่าปรับได้ถึง 500,000 ปอนด์สเตอร์ลิงสำหรับการละเมิดกฎหมายอย่างร้ายแรง การลงโทษนี้ซึ่งนำมาใช้ในเดือนเมษายน 2010 สามารถกำหนดได้ในแง่ของการละเมิดหลักการปกป้องข้อมูลซึ่ง ได้แก่ กรณีที่มีความร้ายแรงและน่าจะก่อให้เกิดความเสียหายหรือความทุกข์ทรมานอย่างมากและการฝ่าฝืนนั้นเป็นไปโดยเจตนาหรือตัวควบคุมข้อมูลรู้หรือควรรู้ว่ามีความเสี่ยงที่การละเมิดจะเกิดขึ้นและอาจก่อให้เกิดความเสียหายหรือความทุกข์ทรมานอย่างมากแต่ล้มเหลว ทำตามขั้นตอนที่เหมาะสมเพื่อป้องกันไม่ให้เกิดการฝ่าฝืน[146]

จึงกล่าวได้ว่าในส่วนนี้ กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศอังกฤษก็ได้พัฒนาและปรับปรุงหลักการให้เป็นไปในทำนองเดียวกันกับ GDPR นั่นเอง

---

[145] DLA Piper, **Data Protection Laws of the World**, p. 497, Retrieved March 10, 2018 from http://www.dlapiperdataprotection.com

[146] *Ibid.*

3.3 การคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศแคนาดา

3.3.1 แนวคิดและวิวัฒนาการในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศแคนาดา

3.3.1.1 ความหมายของข้อมูลส่วนบุคคลของประเทศแคนาดา

สำหรับประเทศแคนาดานั้น สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลได้รับความคุ้มครองโดยกฎหมาย 3 ประเภท นั้นคือ กฎหมายกลาง (Federal Laws) กฎหมายในระดับมณฑลและเขตปกครองพิเศษ (Provincial and Territorial Laws) และกฎหมายเฉพาะที่บังคับกับภาคธุรกิจที่เกี่ยวกับการคุ้มครองสิทธิในข้อมูลส่วนบุคคล (Sector-Spectfic Legislation) ซึ่งกฎหมายที่สำคัญจะมีอยู่ 2 ฉบับ โดยได้มีการตราขึ้นเป็นกฎหมายกลางและมีการวางหลักการในลักษณะของบทบัญญัติที่เป็นการทั่วไป อันได้แก่ กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดา หรือ The Privacy Act 1980 ซึ่งมีผลบังคับกำหนดแนวทางปฏิบัติในการจัดการข้อมูลส่วนบุคคลของหน่วยงานที่เป็นส่วนราชการของรัฐบาล และ กฎหมายคุ้มครองข้อมูลส่วนบุคคลและเอกสารอิเลคทรอนิกส์ หรือ The Personal Information Protection and Electronic Documents Act 2000 (PIPEDA) ซึ่งมีผลบังคับกำหนดถึงแนวทางการจัดการข้อมูลส่วนบุคคลของภาคเอกชนและธุรกิจต่าง ๆ โดยที่กฎหมายฉบับนี้เกิดจากแรงกดดันและผลกระทบจากสหภาพยุโรป (EU) เช่นเดียวกับประเทศสหรัฐอเมริกาและประเทศอื่น ๆ ที่จะต้องมีการพัฒนากฎหมายให้เทียบเท่ากับมาตรฐานที่กำหนดขึ้นโดยฝ่ายสหภาพยุโรป[147] นอกจากนี้สำหรับกฎหมายเฉพาะ (Sector-Spectfic Legislation) ที่สำคัญ ได้แก่ กฎหมายว่าด้วยสแปมของแคนาดา Canada's Anti–Spam Legislation (CASL)

สำหรับการกำหนดนิยามความหมายของคำว่า “ข้อมูลส่วนบุคคล” นั้น กฎหมายคุ้มครองข้อมูลส่วนบุคคลและเอกสารอิเลคทรอนิกส์ หรือ The Personal Information Protection and Electronic Documents Act 2000 (PIPEDA) ได้กำหนดว่า หมายความรวมถึง ข้อมูลใด ๆ ทั้งที่มีการบันทึกและไม่มีการบันทึกของบุคคลที่สามารถระบุตัวตนได้ ซึ่งได้แก่[148]

---

[147] นคร เสรีรักษ์, *เรื่องเดิม*, หน้า 173

[148] Office of Privacy Commisionner of Canada , **PIPEDA in Brief**, Retrieved February 20, 2019 from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/#_what_is

1. อายุ ชื่อ เลขที่บัตรประชาชน รายได้ เชื่อชาติ หรือหมู่โลหิต

2. ความคิดเห็นหรือทัศนะ การประเมินคุณค่า การแสดงความเห็น สถานะทางสังคม หรือประวัติการต้องโทษหรือถูกดำเนินคดี และ

3. ข้อมูลของลูกจ้างหรือพนักงาน ข้อมูลด้านเครดิต ข้อมูลเกี่ยวกับหนี้สินหรือการกู้ยืม ข้อมูลเกี่ยวกับประวัติทางการแพทย์ ข้อมูลเกี่ยวกับการพิพาทระหว่างผู้บริโภคและผู้ประกอบการ หรือข้อมูลเกี่ยวกับความต้องการ (เช่น การให้ได้มาซึ่งสินค้าหรือบริการ หรือความประสงค์เปลี่ยนงาน)

และนอกจากนี้ยังรวมถึงข้อมูลที่เกี่ยวกับสุขภาพของบุคคล (Personal Dealth Information) ดังต่อไปนี้[149]

1. ข้อมูลที่เกี่ยวกับสุขภาพร่างกายหรือจิตใจของบุคคลธรรมดา

2. ข้อมูลเกี่ยวกับการบริการทางสุขภาพที่บุคคลธรรมดาได้รับ

3. ข้อมูลที่เกี่ยวกับการบริจาคอวัยวะส่วนใดของร่างกายหรือส่วนประกอบใดของร่างกายของบุคคลธรรมดา หรือ ข้อมูลที่ได้รับการทดสอบหรือตรวจสอบอวัยวะส่วนใดของร่างกายหรือส่วนประกอบส่วนใดของร่างกายของบุคคลธรรมดา

4. ข้อมูลที่รวบรวมได้ในการให้บริการทางสุขภาพแก่บุคคลธรรมดา

5. ข้อมูลอื่นที่เกี่ยวข้องที่รวบรวมได้ในการให้บริการทางสุขภาพแก่บุคคลธรรมดา แต่ไม่รวมถึงชื่อ ตำแหน่ง สถานที่ทำงาน (สถานที่ประกอบธุรกิจ) หรือหมายเลขโทรศัพท์ของลูกจ้างในองค์กร

สำหรับข้อมูล IP Address (รวมถึง Mac Adrress) ไม่ได้มีการบัญญัติไว้ชัดแจ้ง แต่อาศัยการตีความ PIPEDA โดยประเทศแคนาดาให้ความคุ้มครองแก่ข้อมูลประเภท IP Address โดยจะถือเป็นข้อมูลส่วนบุคคลเมื่อสามารถเชื่อมโยงไปหาเจ้าของข้อมูลส่วนบุคคลได้ เช่น ในกรณีที่ผู้ให้บริการอินเตอร์เน็ต (Internet Service Provider: ISP) เก็บรวมรวมข้อมูล IP Address ของ

---

[149] สมศักดิ์ นวตระกูลพิสุทธิ์, กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศฝรั่งเศส, ใน **รายงานการวิจัยโครงการจัดทำความเป็นทางวิชาการเพื่อจัดทำรายงานเกี่ยวกับหลักเกณฑ์และแนวทางการพิจารณาและดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และจัดทำคู่มือการปฏิบัติงานเกี่ยวกับข้อมูลส่วนบุคคลภาครัฐตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ.2540** (กรุงเทพมหานคร: สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์, 2547), หน้า 97.

ผู้รับบริการเช่นนี้ ก็จะถือว่าข้อมูล IP Address เป็นข้อมูลส่วนบุคคลเนื่องจากถือว่าผู้ให้บริการมีข้อมูลเพียงพอและสามารถระบุตัวเจ้าของข้อมูลส่วนบุคคลได้นั่นเอง[150]

อย่างไรก็ดี กฎหมายที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดานั้น ไม่ได้มีการบัญญัตินิยามความหมายของข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) ไว้เป็นการเฉพาะ[151]

3.3.1.2 สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในฐานะสิทธิขั้นพื้นฐาน

ภายใต้ระบบกฎหมายรัฐธรรมนูญของประเทศแคนาดา รัฐธรรมนูญของประเทศแคนาดา ฉบับปี ค.ศ.1982 (Constitution Act 1982) หมวด 1 Canadian Charter of Rights and Freedoms ได้มีการบัญญัติรับรองสิทธิตามกฎหมาย (Legal Rights) มาตรา 7 ว่า ทุกคนมีสิทธิในชีวิต เสรีภาพ และความมั่นคงปลอดภัย และสิทธิเหล่านี้จะมีถูกลิดรอนเว้นแต่เป็นไปตามหลักการพื้นฐานของความยุติธรรม และในมาตรา 8 กำหนดว่า ทุกคนมีสิทธิที่จะได้รับความปลอดภัยจากการตรวจตราหรือค้นโดยปราศจากเหตุผล ซึ่งจากหลักการทั้งสองนี้ จะเห็นว่า รัฐธรรมนูญของประเทศแคนาดาก็ได้ให้การยอมรับหลักการเรื่องความเป็นส่วนตัวของประชาชนเอาไว้ แม้ว่าจะไม่ได้เป็นการรับรองสิทธิในความเป็นส่วนตัวไว้โดยตรงก็ตาม แต่ก็เป็นหลักการพื้นฐานสำคัญที่ทำให้ศาลฎีกาของประเทศแคนาดาได้ใช้เป็นหลักการในการตัดสินคดีเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวในอีกหลายคดีต่อ ๆ มา ซึ่งจะเห็นได้ว่า แนวคิดเรื่องสิทธิในความเป็นส่วนตัวนี้ได้ถูกยกระดับให้กลายเป็นสิทธิขั้นพื้นฐานที่รัฐจะต้องให้การรับรองและคุ้มครองให้แก่ประชาชน ซึ่งรายละเอียดจะได้กล่าวในส่วนต่อไป

3.3.1.3 วิวัฒนาการในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในประเทศแคนาดา

สำหรับวิวัฒนาการของการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในประเทศแคนาดานั้น จะเห็นว่า ได้รับอิทธิพลของกระแสความคิดเกี่ยวกับการให้ความเคารพต่อสิทธิในความเป็นส่วนตัวจากฝั่งอเมริกา โดยเฉพาะจากบทความของ Samuel Warren และ Louis Brandeis ที่ลงตีพิมพ์ในวารสารThe Harvard Law Review ในปี 1890 ที่ได้อธิบายว่า สิทธิในความเป็นส่วนตัวนั้นไม่ได้จำกัดอยู่แต่เฉพาะสิทธิในชีวิตร่างกายและทรัพย์สิน แต่จะต้องหมายความไปถึงสิทธิที่จะอยู่โดยลำพัง (The Right to be Let Alone) เป็นสิทธิขั้นพื้นฐานที่จะไม่ถูกคุกคามหรือล่วงละเมิดความเป็นส่วนตัวด้วยวิธีการต่าง ๆ ดังที่ได้กล่าวไว้แล้วในบทก่อน ประกอบกับ

---

[150] อธิพร สิทธิธีรรัตน์, **ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลในบริบทอิเล็กทรอนิกส์** (วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2558), หน้า 108.

[151] DLA Piper, *op. cit.*

สาระสำคัญของกติการะหว่างประเทศไม่ว่าจะเป็น ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน, กติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง, อนุสัญญายุโรปว่าด้วยสิทธิมนุษยชน และอนุสัญญาว่าด้วยสิทธิมนุษยชนแห่งอเมริกา ซึ่งได้ยอมรับสิทธิในความเป็นส่วนตัว ว่าเป็นหนึ่งในสิทธิมนุษยชนที่สำคัญยิ่ง ซึ่งหลักการของกติกาสากลต่าง ๆ เหล่านี้ ประเทศแคนาดาก็ได้ให้การยอมรับโดยเฉพาะอย่างยิ่งแนวทางปฏิบัติตาม OECD Guidelines for the Protection of Privacy and Transborder Flows of Personal Data 1980 โดยในปี 1984 ประเทศแคนาดาได้เข้าร่วมเช่นเดียวกันกับ 22 ประเทศอุตสาหกรรมอื่น ๆ โดยหลักการนี้ได้กลายเป็นจุดเริ่มต้นของกฎหมายคุ้มครองข้อมูลในประเทศต่าง ๆ ทั่วโลกรวมถึงประเทศแคนาดา[152]

การตอบสนองครั้งแรกในระดับรัฐบาล ของประเทศแคนาดาต่อข้อเรียกร้องให้ปกป้องคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป คือการแก้ไขบทบัญญัติให้มีการคุ้มครองข้อมูลในพระราชบัญญัติสิทธิมนุษยชนของแคนาดา (The Canadian Human Rights Act) อย่างไรก็ตามในปี 1982 รัฐสภาแคนาดาก็ได้ผ่านกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดา หรือ The Privacy Act ซึ่งกฎหมายฉบับนี้ได้กำหนดให้มีผลบังคับในปีต่อไป[153] โดยมีสาระสำคัญกำหนดว่าหน่วยงานของรัฐบาลจะต้องจัดการกับข้อมูลส่วนบุคคลของบุคคลบนพื้นฐานของหลักการดังนี้คือ[154]

1. หน่วยงานของรัฐจะต้องไม่เก็บรวบรวมข้อมูลส่วนบุคคล เว้นแต่จะเกี่ยวข้องโดยตรงกับโปรแกรมการปฏิบัติงานหรือกิจกรรมของหน่วยงาน (มาตรา 4)

2. หน่วยงานของรัฐจะต้องแจ้งให้บุคคลใด ๆ ที่หน่วยงานของรัฐได้เก็บรวบรวมข้อมูลส่วนบุคคลของเขาไว้ได้ทราบถึงวัตถุประสงค์ในการรวบรวมข้อมูลส่วนบุคคลนั้น (มาตรา 5 (2))

3. ข้อมูลส่วนบุคคลที่อยู่ภายใต้การควบคุมของหน่วยงานของรัฐจะต้องไม่ถูกนำไปใช้ เว้นแต่จะเป็นไปตามวัตถุประสงค์ของการจัดเก็บข้อมูลนั้น หรือจะได้รับความยินยอมจากบุคคลนั้น (มาตรา 7)

4. ข้อมูลส่วนบุคคลภายใต้การควบคุมของหน่วยงานรัฐ จะต้องไม่ได้รับการเปิดเผยเว้นแต่ได้รับความยินยอมจากบุคคลนั้น (มาตรา 8)

---

[152] Bruce Phillips, **The Evolution of Canada's Privacy Laws, Speaking Notes Prepared for the Canadian Bar Association - Ontario Institute - January 28, 2000**, Retrieved February 8, 2019 from https://www.priv.gc.ca/en/opc-news/speeches/archive/02_05_a_ 000128/

[153] *Ibid.*

[154] **Privacy Act**, Retrieved February 8, 2019 from https://laws-lois.justice.gc.ca/PDF/P-21.pdf

5. พลเมืองแคนาดาหรือผู้มีถิ่นที่อยู่ถาวรทุกคนมีสิทธิที่จะได้รับการเข้าถึงข้อมูลส่วนบุคคลเกี่ยวกับตนภายใต้การควบคุมของหน่วยงานของรัฐได้ตามสมควรและร้องขอการแก้ไขหากข้อมูลไม่ถูกต้อง (มาตรา 12)

6. คณะกรรมการสิทธิความเป็นส่วนตัวแห่งแคนาดา มีอำนาจรับข้อร้องเรียนและตรวจสอบถึงการร้องเรียนว่าบุคคลหนึ่งถูกปฏิเสธการเข้าถึงข้อมูลส่วนบุคคลของเขาที่จัดขึ้นโดยหน่วยงานของรัฐ (มาตรา 29)

ซึ่งบุคคลที่ถูกปฏิเสธการเข้าถึงข้อมูลส่วนบุคคลในที่สุด อาจนำคดีไปฟ้องศาล the Federal Court เพื่อตรวจสอบเรื่องตามมาตรา 41 และศาลอาจสั่งให้หัวหน้าหน่วยงานของรัฐเปิดเผยข้อมูลต่อบุคคล (มาตรา 48 และ 49) ซึ่งคำพิพากษาของศาลอาจถูกอุทธรณ์และฎีกาได้ตามลำดับ

แต่เนื่องจาก Privacy Act ไม่ได้มีผลไปคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในภาคเอกชน ทำให้ต่อมาในปี 2000 จึงได้มีการตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลและเอกสารอิเลคทรอนิกส์ The Personal Information Protection and Electronic Documents Act (PIPEDA) ขึ้นโดยกำหนดหลักการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของภาคเอกชนไม่ว่าจะเป็นเรื่องของ การเก็บรวบรวม การใช้และการเปิดเผยข้อมูลส่วนบุคคลในการดำเนินธุรกิจเชิงพาณิชย์ นอกจากนี้กฎหมายฉบับนี้ยังมีผลบังคับไปถึงการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในรูปแบบของเอกสารอิเล็กทรอนิกส์ด้วย โดยมีผลใช้บังคับในวันที่ 13 เมษายน ค.ศ.2000 ซึ่งสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในฐานะสิทธิของปัจเจกชนตามกฎหมายฉบับนี้ ซึ่งหลักการของกฎหมายฉบับนี้ที่เป็นรายละเอียดจะได้กล่าวถึงในหัวข้อต่อไป

ต่อมาในปี 2014 ประเทศแคนาดาได้ตรากฎหมายเฉพาะสำหรับกรณีของสแปม แยกออกมาเป็นกฎหมายเฉพาะต่างหาก ซึ่งก็คือ Canada's Anti–spam Legislation (CASL) โดยมีวัตถุประสงค์คุ้มครองการพาณิชย์อิเล็กทรอนิกส์และเพิ่มความเชื่อมั่นในการทำธุรกรรมออนไลน์ โดยมีการกำหนดข้อห้ามการส่งข้อความอิเล็กทรอนิกส์ที่ผู้รับมิได้เรียกร้อง (Unsolicited Electronic Messages) ซึ่งมีสาระสำคัญคือการห้ามส่งหรือก่อให้เกิดการส่งข้อความอิเล็กทรอนิกส์ไปยังที่อยู่อิเล็กทรอนิกส์ เว้นแต่ผู้รับให้ความยินยอมในการรับโดยชัดแจ้งหรือปริยาย (Express or Implied) และข้อความนั้นมีลักษณะเป็นข้อมูลนั้นมีการระบุรายละเอียดบ่งชี้ตัวตนของผู้ส่งหรือผู้ที่ทำการส่งในนามของผู้นั้น มีข้อมูลที่ทำให้ผู้รับสามารถติดต่อผู้ส่งได้ และ มีกลไกในการให้บอกเลิก (Unsubscribe)[155] ซึ่งหลักการข้อนี้จะมีผลเป็นการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประชาชนนั้นเอง

---

[155] คณาธิป ทองวีรวงศ์, *เรื่องเดิม*, หน้า 106.

อย่างไรก็ดี กฎหมายฉบับนี้มีการกำหนดข้อยกเว้นไว้ กล่าวคือ ข้อห้ามการส่งข้อความอิเล็กทรอนิกส์ที่ผู้รับมิได้เรียกร้อง (Unsolicited Electronic Messages) ไม่ใช้บังคับกับกรณีต่อไปนี้คือ[156]

1. ข้อความที่เป็นแต่เพียงข้อความอิเล็กทรอนิกส์

2. เสนอราคาหรือประมาณราคาของสินค้า บริการ ที่ดิน หากการเสนอราคานั้นถูกเรียกร้องโดยผู้รับ

3. สนับสนุน ทำให้สมบูรณ์ หรือยืนยัน ธุรกรรมทางพาณิชย์ ซึ่งผู้รับข้อความได้ ตกลงกับผู้ส่ง - ให้ข้อมูลเกี่ยวกับการรับประกัน หรือความปลอดภัย ของสินค้า บริการที่ผู้รับ ข้อความได้ใช้หรือได้ซื้อไป

4. ให้การแจ้งเตือนหรือข้อมูลที่เป็นข้อเท็จจริงเกี่ยวกับกระบวนการต่อเนื่องการใช้หรือการซื้อสินค้าหรือบริการ (Ongoing Use or Purchase) ที่ผู้รับข้อมูลนั้นได้มีความสัมพันธ์กับผู้ส่งข้อความ ภายใต้การสมัครสมาชิก บัญชีเงินกู้ หรือความสัมพันธ์อย่างอื่นในลักษณะคล้ายคลึงกัน

5. ให้ข้อมูลเกี่ยวกับความสัมพันธ์ในการจ้างแรงงานหรือประโยชน์เกี่ยวกับการจ้างแรงงานที่ผู้รับเกี่ยวข้อง

3.3.2 มาตรการทางกฎหมายในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศแคนาดา

3.3.2.1 ลักษณะและประเภทของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลที่ได้รับความคุ้มครอง

สำหรับประเทศแคนาดาไม่ได้มีการแบ่งแยกประเภทของข้อมูลส่วนบุคคล โดยมีการกำหนดนิยามเป็นประเภทของข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) แต่อย่างใด ซึ่งมีเพียงแต่การกำหนดนิยามความหมายของข้อมูลส่วนบุคคลในภาพรวมว่าหมายถึง ข้อมูลใด ๆ ทั้งที่มีการบันทึกและไม่มีการบันทึกของบุคคลที่สามารถระบุตัวตนได้ ดังที่ได้กล่าวไว้แล้วในตอนต้น

สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศแคนนาดาปรากฏตัวในรูปแบบของสิทธิสำคัญอันเกี่ยวกับข้อมูลดังต่อไปนี้คือ[157]

---

[156] *เรื่องเดียวกัน*.

[157] Adam Kardash and Patricia Kosseim, **The International Comparative Legal Guide to: Data Protection 2018**, Retrieved February 8, 2019 from https://www.osler.com/osler/media/Osler/reports/privacy-data/Data-Protection-Laws-in-Canada-2018.pdf

1. สิทธิที่จะเข้าถึงข้อมูลส่วนตัว (Rights to Access)

ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดาภายใต้เงื่อนไขคำร้องขอและข้อยกเว้นตามกฎหมายกำหนด องค์กรจะต้องแจ้งให้บุคคลทราบถึงการมีอยู่ การใช้ และการเปิดเผยข้อมูลส่วนบุคคล และต้องให้เจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึงข้อมูลนั้นได้ รวมถึงแจ้งให้ทราบถึงรายชื่อขององค์กรอื่น (บุคคลที่สาม) ซึ่งมีการแบ่งปันหรือส่งข้อมูลไป

สิทธิในการ “เข้าถึง” นี้ ไม่ได้บังคับให้องค์กรเพียงแค่จัดทำสำเนาบันทึกข้อมูลส่วนบุคคลให้เท่านั้น แต่รวมถึงจะต้องให้มีการเข้าถึงข้อมูลที่รวมไปถึงการเข้าดูบันทึกที่เกี่ยวกับข้อมูลส่วนบุคคลที่สำนักงานขององค์กรด้วย ซึ่งโดยทั่วไปคำขอของแต่ละบุคคลจะต้องเจาะจงอย่างเพียงพอเพื่อให้องค์กรสามารถปฏิบัติตามคำขอได้ และองค์กรต้องตอบสนองภายในระยะเวลาที่กำหนดหรือตามระยะเวลาที่เหมาะสม โดยไม่มีค่าใช้จ่ายและต้องทำให้ข้อมูลส่วนบุคคลนั้นอยู่ในรูปแบบที่สามารถเข้าใจได้โดยทั่วไป

การจำกัดหรือการยกเว้นสิทธิในการเข้าถึงอาจแตกต่างกันไปในกฎหมายแต่ละฉบับ แต่อย่างไรก็ดี การพิจารณาเรื่องการจำกัดหรือยกเว้นสิทธินี้ จำเป็นต้องพิจารณาอย่างรอบคอบ ซึ่งตัวอย่างของการยกเว้นตามกฎหมาย เช่น ข้อมูลที่อยู่ภายใต้การร้องขอของลูกค้านั้นเกี่ยวข้องกับสิทธิดำเนินคดีในเรื่องข้อมูลทางการค้าที่เป็นความลับ ข้อมูลเกี่ยวกับบุคคลอื่น ข้อมูลที่เกี่ยวข้องกับเรื่องความมั่นคงของประเทศและข้อมูลเกี่ยวกับกระบวนการระงับข้อพิพาทในคดี เป็นต้น

2. สิทธิในการแก้ไขข้อมูลส่วนบุคคลที่ไม่ถูกต้องหรือผิดพลาด (Right to Rectification of Errors)

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดาโดยทั่วไป กำหนดว่าเมื่อบุคคลแสดงให้เห็นถึงความไม่ถูกต้องหรือความไม่สมบูรณ์ของข้อมูลส่วนบุคคลของเขา องค์กรจะต้องแก้ไขความไม่ถูกต้องและ / หรือเพิ่มเติมและบันทึกลงในข้อมูลตามความเหมาะสม

3. สิทธิในการลบข้อมูล / สิทธิที่จะถูกลืม (Right to Deletion/Right to be Forgotten)

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดาให้สิทธิแก่บุคคลในการเพิกถอนคำยินยอมและโต้แย้งความถูกต้องครบถ้วนและความทันสมัยเป็นปัจจุบันของข้อมูลส่วนบุคคล เมื่อมีกรณีเช่นนี้ กฎหมายจึงกำหนดให้องค์กรต้อง “ลบ” ข้อมูลส่วนบุคคลนั้น

4. สิทธิในการคัดค้านการประมวลผลข้อมูล (Right to Object to Processing)

แม้ว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดาจะไม่ได้บัญญัติรับรองถึงสิทธิคัดค้านการประมวลผลข้อมูลไว้เป็นการเฉพาะ แต่ก็มีข้อกำหนดห้ามองค์กรไม่ให้มีการกำหนดเงื่อนไขสำหรับการจัดหาผลิตภัณฑ์หรือบริการของข้อมูลส่วนบุคคลของพวกเขานอกเหนือจากสิ่งที่จำเป็นในการบรรลุวัตถุประสงค์ที่ระบุไว้อย่างชัดเจนและถูกต้องตามกฎหมาย นอกจากนี้บุคคล

จะต้องสามารถถอนความยินยอมได้ตลอดเวลาภายใต้เงื่อนไขทางกฎหมายหรือสัญญา และการบอกกล่าวตามสมควร เมื่อบุคคลแจ้งถึงการถอนดังกล่าว องค์กรที่ได้รับการร้องขอการถอนความยินยอมจะต้องดำเนินการให้ตามความประสงค์

5. สิทธิในการโอนข้อมูลระหว่างผู้ควบคุมข้อมูล (Right to Data Portability)

ถึงแม้ว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลของแคนาดามีการรับรองสิทธิในการเข้าถึงข้อมูลส่วนบุคคลดังที่กล่าวไว้ข้างต้น แต่ก็ไม่ได้รวมไปถึงสิทธิในการโอนข้อมูลระหว่างผู้ควบคุมข้อมูล

6. สิทธิในการถอนความยินยอม (Right to Withdraw Consent)

ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดาบุคคล จะต้องสามารถถอนความยินยอมได้ตลอดเวลา ภายใต้ข้อจำกัดทางกฎหมายหรือสัญญาและการบอกกล่าวตามสมควร บุคคลจะต้องได้รับการแจ้งถึงผลของการถอนความยินยอมดังกล่าวด้วย

7. สิทธิปฏิเสธความยินยอมเกี่ยวกับการทำตลาด (Right to Object to Marketing Consent)

สิทธินี้มีความสำคัญสำหรับ การเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคล เพื่อวัตถุประสงค์ในทางการตลาด ซึ่งรูปแบบของความยินยอมที่จำเป็น (Opt-In or Opt-Out) จะแตกต่างกันไปตามสถานการณ์ความอ่อนไหวของข้อมูลและความสมเหตุสมผลของแต่ละบุคคล โดยสิทธิเจ้าของข้อมูลที่จะไม่ให้ข้อมูลของตนถูกประมวลผลต่อไป (Opt Out) จะต้องได้รับการดำเนินการอย่างเหมาะสม โดยบุคคลมีสิทธิรับทราบถึงวัตถุประสงค์ทางการตลาดในช่วงเวลาก่อนการเก็บรวบรวมข้อมูล โดยต้องมีการอธิบายในลักษณะที่ชัดเจนและเข้าใจได้ รวมไปถึงบุคคลจะต้องสามารถยกเลิกการให้ความยินยอมได้โดยสะดวก และการยกเลิกจะต้องมีผลในทันทีและคงอยู่ และข้อมูลที่ถูกเก็บรวบรวมและใช้งานจะต้องถูกทำลายหรือถูกยกเลิกการเข้าถึงหรือประมวลผล อย่างมีประสิทธิภาพและรวดเร็วที่สุด

8. สิทธิในการร้องเรียนไปยังหน่วยงานคุ้มครองข้อมูลที่เกี่ยวข้อง (Right to Complain to the Relevant Data Protection Authority)

ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดา บุคคลมีสิทธิร้องเรียนกับหน่วยงานคุ้มครองข้อมูลที่เกี่ยวข้อง โดยในเบื้องต้นบุคคลจะต้องสามารถได้รับการแก้ไขปัญหาเกี่ยวกับการปกป้องข้อมูลกับบุคคล โดยองค์กรที่รับผิดชอบ (ตามหลักการความรับผิดชอบ) ซึ่งองค์กรต้องมีขั้นตอนที่ง่ายต่อการเข้าถึงและใช้งาน และสามารถตอบสนองต่อข้อร้องเรียนหรือข้อซักถามและจะต้องดำเนินการเพื่อจัดการกับข้อร้องเรียนอย่างมีประสิทธิภาพ

เมื่อพิจารณาแล้วจะเห็นได้ว่า สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศแคนาดานั้น จะมีลักษณะสำคัญโดยสรุปได้ ดังนี้[158]

1. บุคคลย่อมมีสิทธิที่จะรู้ว่าทำไมองค์กรจึงทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของพวกเขา

2. องค์กรจะต้องทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอย่างสมเหตุสมผล และเหมาะสม รวมถึงไม่ใช้ข้อมูลเพื่อจุดประสงค์อื่นใดนอกจากที่ได้รับความยินยอม

3. บุคคลย่อมมีสิทธิที่จะรู้ว่าใครในองค์กรมีหน้าที่รับผิดชอบในการปกป้องข้อมูลส่วนบุคคลของพวกเขา

4. องค์กรจะต้องดำเนินการปกป้องข้อมูลส่วนบุคคลโดยใช้มาตรการความปลอดภัยที่เหมาะสม

5. ข้อมูลส่วนบุคคลที่องค์กรเก็บไว้เป็นข้อมูลที่ถูกต้องสมบูรณ์และทันสมัย

6. บุคคลย่อมมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลและขอแก้ไขข้อมูลได้หากจำเป็น

7. บุคคลย่อมมีสิทธิที่จะร้องเรียนเกี่ยวกับวิธีที่องค์กรจัดการกับข้อมูลส่วนบุคคลของพวกเขาหากพวกเขารู้สึกว่าสิทธิความเป็นส่วนตัวของพวกเขายังไม่ได้รับการเคารพ หรือมีการปฏิบัติที่ไม่ถูกต้อง

และภายใต้สิทธิที่กฎหมาย Personal Information Protection and Electronic Documents Act รับรองไว้เช่นนี้ ได้ก่อให้เกิดหน้าที่แก่องค์กรต่าง ๆ ดังนี้คือ[159]

1. ต้องขอความยินยอมจากเจ้าของข้อมูลทุกครั้งที่จะมีการเก็บรวบรวม ใช้ หรือเปิดเผย

2. ยังคงจัดหาผลิตภัณฑ์หรือบริการให้กับบุคคลตามปกติ แม้ว่าพวกเขาจะไม่ยินยอมให้มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เว้นแต่ว่าข้อมูลนั้นมีความสำคัญต่อการทำธุรกรรม

3. รวบรวมข้อมูลส่วนบุคคลด้วยวิธีการที่ชอบธรรมและถูกกฎหมาย และ

4. กำหนดนโยบายและแนวปฏิบัติเกี่ยวกับข้อมูลส่วนบุคคลที่ชัดเจนเข้าใจง่ายและปฏิบัติได้

---

[158] **Personal Information Protection and Electronic Documents Act**, Retrieved February 8, 2019 from https://laws-lois.justice.gc.ca/PDF/P-8.6.pdf

[159] *Ibid.*

3.3.2.2 หลักการและข้อจำกัดในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล

ภายใต้บังคับของกฎหมายคุ้มครองข้อมูลส่วนบุคคลและเอกสารอิเลคทรอนิกส์ หรือ The Personal Information Protection and Electronic Documents Act 2000 (PIPEDA) ก็จะมีองค์กรสำคัญ คือ สำนักงานคณะกรรมการสิทธิความเป็นส่วนตัวแห่งแคนาดา (Privacy Commissioner of Canada) ทำหน้าที่เป็นเจ้าภาพหลัก โดยจะเป็นองค์กรที่คอยช่วยเหลือ ให้ความรู้และให้คำปรึกษาแก่บุคคลเกี่ยวกับสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลและการคุ้มครองข้อมูลทางอิเล็กทรอนิกส์ที่ได้รับการคุ้มครองตามกฎหมายฉบับนี้ โดยจะมีอำนาจควบคุมบุคคล (Person) และองค์กรต่าง ๆ (Organization) ซึ่งหมายความรวมถึงสมาคม (Association) ห้างหุ้นส่วนนิติบุคคล (Partnership) และสหภาพแรงงาน (Trade Union) ซึ่งเป็นผู้ที่เกี่ยวข้องกับการควบคุม การจัดเก็บ การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลที่อยู่ในความควบคุมหรือครอบครอง โดยกฎหมายนี้ ได้กำหนดไว้ว่า องค์กรทั้งหลายมีภาระหน้าที่ที่กำหนดดังหลักเกณฑ์มาตรฐานแห่งชาติ (National Standard of Canada) ซึ่งมีสาระสำคัญที่ต้องปฏิบัติตามดังนี้[160]

1) หลักความรับผิดชอบ (Accountability)

หน่วยงานหรือองค์กรต้องมีความรับผิดชอบต่อข้อมูลส่วนบุคคลที่อยู่ในความควบคุมของตน และต้องแต่งตั้งบุคคลหนึ่งหรือหลายคนซึ่งรับผิดชอบต่อการปฏิบัติขององค์กรตามหลักปฏิบัติปฏิบัติต่าง ๆ ที่กำหนดในแบบปฏิบัตินี้

องค์กรต้องกำหนดนโยบายและแนวทางปฏิบัติเพื่อให้หลักปฏิบัติต่าง ๆ ที่กำหนดในแบบปฏิบัตินี้บังเกิดผลได้แก่

(1) กำหนดกระบวนการคุ้มครองข้อมูลส่วนบุคคล

(2) กำหนดกระบวนการรับและตอบคำร้อง (Complaints) หรือข้อซักถาม (Inquiries) ต่าง ๆ

(3) ฝึกอบรมพนักงานและแจ้งให้พนักงานที่เกี่ยวข้องทราบเกี่ยวกับนโยบายและแนวทางปฏิบัติในเรื่องนี้ขององค์กร

(4) จัดทำข้อมูลชี้แจงนโยบายและกระบวนการต่าง ๆ ขององค์กร

2) หลักการแจ้งวัตถุประสงค์ (Idenitfying Purpose)

องค์กรต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงวัตถุประสงค์ของการเก็บรวบรวมข้อมูลก่อนหรือในขณะทำการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น ทั้งนี้ การแจ้งอาจกระทำ

---

[160] สมศักดิ์ นวตระกูลพิสุทธิ์, *เรื่องเดิม*, หน้า 97.

ด้วยวาจาหรือเป็นลายลักษณ์อักษรก็ได้ ตามลักษณะของการเก็บรวบรวมข้อมูลนั้น และมีหน้าที่ดำเนินการดังนี้

(1) จัดพิมพ์ประกาศ หรือเอกสารเพื่อแจ้งให้ทราบเกี่ยวกับวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อให้สอดคล้องกับหลักการเปิดเผย และหลักการเข้าตรวจดูข้อมูลของบุคคล

(2) ต้องเก็บรวบรวมข้อมูลส่วนบุคคลแต่เพียงข้อมูลที่จำเป็นตามวัตถุประสงค์ที่ได้แจ้งให้ทราบแล้วเท่านั้น ทั้งนี้เป็นไปตามหลักการเก็บรวบรวมข้อมูลอย่างจำกัด

(3) ในกรณีที่จะนำข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้ไปใช้ประโยชน์เพื่อวัตถุประสงค์อย่างอื่นที่มิได้แจ้งให้ทราบล่วงหน้า องค์กรต้องแจ้งวัตถุประสงค์ใหม่นั้นให้บุคคลนั้นทราบเสียก่อน และจะต้องได้รับความยินยอมก่อนที่จะนำข้อมูลนั้นไปใช้เพื่อประโยชน์ตามวัตถุประสงค์ใหม่นั้น ทั้งนี้ เว้นแต่ วัตถุประสงค์ใหม่นั้นเป็นไปตามที่กฎหมายกำหนด

3) หลักความยินยอม (Consent)

บุคคลที่จะให้ข้อมูลส่วนบุคคลต้องได้รับทราบและให้ความยินยอมแก่การเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลของบุคคลนั้น ทั้งนี้ เว้นแต่ เป็นกรณีที่ไม่สมควรตามที่กำหนดในกฎหมาย

ตามปกติองค์กรจะต้องขอความยินยอมสำหรับการใช้หรือการเปิดเผยข้อมูลในขณะทำการเก็บรวบรวม แต่อย่างไรก็ตาม ในบางสถานการณ์อาจมีการขอความยินยอมนำข้อมูลไปใช้หรือเปิดเผยภายหลังการเก็บรวบรวมข้อมูล แต่ต้องก่อนการนำข้อมูลไปใช้ โดยการขอความยินยอมนั้น องค์กรต้องจัดให้มีการขอความยินยอมโดยวิธีดำเนินการที่เหมาะสมเพื่อให้บุคคลได้รับแจ้งถึงวัตถุประสงค์ของการที่จะนำข้อมูลนั้นไปใช้ และจะต้องไม่ขอความยินยอมในการดำเนินการมากเกินความจำเป็นสำหรับการดำเนินการตามวัตถุประสงค์ที่ชอบด้วยกฎหมายและที่ได้แจ้งให้ทราบ

รูปแบบของความยินยอมอาจแตกต่างกันไปขึ้นอยู่กับสถานการณ์และประเภทของข้อมูล ทั้งนี้ในการกำหนดรูปแบบของความยินยอมองค์กรต้องคำนึงถึงประเภทของข้อมูลโดยเฉพาะอย่างยิ่งข้อมูลส่วนตัวโดยเฉพาะ (Sensitive Data) โดยหากเป็นข้อมูลส่วนตัวโดยเฉพาะควรขอความยินยอมอย่างชัดแจ้งในกรณีที่เป็นข้อมูลส่วนตัวโดยเฉพาะน้อยก็อาจขอความยินยอมโดยปริยายได้ เช่น บันทึกทางการแพทย์และบันทึกรายได้ แต่ข้อมูลที่ไม่ได้ถูกจัดอยู่ในประเภทที่เป็นข้อมูลส่วนตัวโดยเฉพาะก็อาจจะต้องใช้ความระมัดระวังในการแจ้งขอความยินยอม ทั้งนี้ขึ้นอยู่กับบริบทแวดล้อมเช่น ชื่อและที่อยู่ของสมาชิกนิตยสารซึ่งโดยทั่วไปไม่ถือว่าเป็นข้อมูลส่วนบุคคลโดยเฉพาะ แต่หากเป็นชื่อและที่อยู่ของสมาชิกนิตยสารที่มีลักษณะเฉพาะ (Special-Interest Magazines) อาจถือว่าเป็นข้อมูลส่วนตัวโดยเฉพาะก็ได้ ความยินยอมอาจเป็นความยินยอมอย่างชัด

แจ้ง (Express Consent) ความยินยอมโดยปริยาย (Implied Consent) ก็ได้ และบุคคลธรรมดาอาจถอนความยินยอมเมื่อใดก็ได้โดยองค์กรต้องแจ้งกระบวนการถอนความยินยอมให้บุคคลนั้นทราบด้วย

4) หลักการเก็บรวบรวมข้อมูลอย่างจำกัด (limiting Collection)

การเก็บรวบรวมข้อมูลส่วนบุคคลจะต้องจำกัดเฉพาะแต่ข้อมูลที่จำเป็นและเป็นไปเพื่อวัตถุประสงค์ขององค์กรที่ได้แจ้งให้ทราบและต้องเก็บรวบรวมข้อมูลโดยวิธีการที่เป็นธรรมและชอบด้วยกฎหมาย องค์กรจะต้องไม่เก็บรวมรวมข้อมูลโดยวิธีการที่เป็นการเลือกปฏิบัติ และต้องเก็บรวมรวมข้อมูลอย่างจำกัดเพียงเท่าที่จำเป็นต่อวัตถุประสงค์และต้องระบุประเภทของข้อมูลที่เก็บรวบรวมโดยการจัดทำเป็นประกาศ หรือคู่มือเกี่ยวกับนโยบายและแนวทางปฏิบัติขององค์การ แจ้งแก่ผู้เป็นเจ้าของข้อมูล ซึ่งหลักการนี้มีความสัมพันธ์กับหลักการแจ้งวัตถุประสงค์และหลักความยินยอม

5) หลักการจำกัดการใช้ การเปิดเผย และการเก็บรักษา (Limiting Use, Disclosure and Retenion)

องค์การจะต้องไม่นำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยเพื่อวัตถุประสงค์อย่างอื่นนอกเหนือจากวัตถุประสงค์ของการเก็บรวบรวมข้อมูลนั้น เว้นแต่จะได้รับความยินยอมของบุคคลธรรมดาคนนั้นหรือเป็นไปตามที่กฎหมายกำหนด และข้อมูลส่วนบุคคลจะต้องถูกเก็บรักษาไว้ในระยะเวลาเพียงเท่าที่จำเป็นสำหรับการดำเนินการตามวัตถุประสงค์ดังกล่าวเท่านั้น หากมีการใช้ข้อมูลข่าวสารเพื่อวัตถุประสงค์ที่กำหนดขึ้นใหม่จะต้องจัดทำเอกสารเกี่ยวกับวัตถุประสงค์ใหม่แจ้งแก่เจ้าของข้อมูล นอกจากนี้ในการจัดทำข้อมูลตามข้อ 4 ต้องกำหนดกระบวนการเกี่ยวกับการเก็บรักษาข้อมูลส่วนบุคคล และควรกำหนดระยะเวลาต่ำสุดและสูงสุดของการเก็บรักษาข้อมูลนั้นไว้ด้วย

ภายใต้หลักการนี้ ข้อมูลส่วนบุคลที่ไม่ถูกต้องตามวัตถุประสงค์ที่ได้แจ้งหรือได้ใช้เสร็จสิ้นแล้วจะต้องถูกทำลาย ลบทิ้ง หรือทำให้ไม่ปรากฏชื่อของบุคคลนั้น (Anonymous) ทั้งนี้องค์กรจะต้องจัดทำคู่มือแนวทางปฏิบัติและกำหนดกระบวนการเกี่ยวกับการทำลายข้อมูลส่วนบุคคลดังกล่าวด้วย

6) หลักความถูกต้อง (Accuracy)

ข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้จะต้องถูกต้อง (Accurate) สมบูรณ์ (Complete) และเป็นปัจจุบัน (Up-to-Date) ตามความจำเป็นเพื่อวัตถุประสงค์ของการนำข้อมูลนั้นไปใช้ หลักการที่ว่าข้อมูลส่วนบุคคลจะต้องถูกต้อง สมบูรณ์ และเป็นปัจจุบันจะต้องคำนึงถึสัดส่วนของส่วนได้เสียของเจ้าของข้อมูล ทั้งนี้เพื่อที่จะลดความเป็นไปได้ของการนำข้อมูลที่ไม่ถูกต้อง (Inappropriate Information) ไปใช้

องค์การจะต้องไม่ปรับปรุงข้อมูลส่วนบุคคลโดยกระทำในลักษณะที่เป็นงานประจำ (Routinely Update) เว้นแต่กระบวนการเช่นนั้นมีความจำเป็นเพื่อสนองตอบต่อวัตถุประสงค์ของการเก็บรวบรวมข้อมูลนั้น

7) หลักการรักษาความปลอดภัย (Safeguards)

ข้อมูลส่วนบุคคลจะต้องได้รับการรักษาความปลอดภัยที่เหมาะสม การรักษาความจะต้องให้ความคุ้มครองข้อมูลส่วนบุคคลต่อการสูญหายหรือโจรกรรม ตลอดจนการเข้าตรวจดู การเปิดเผย การทำซ้ำ การใช้ หรือการแก้ไขเพิ่มเติมโดยไม่ได้รับอนุญาต ทั้งนี้ ไม่ว่าข้อมูลนั้นจะอยู่ในรูปแบบใด ลักษณะของการรักษาความปลอดภัยจะแตกต่างกันไปขึ้นอยู่กับระดับของความเป็นข้อมูลส่วนตัวโดยเฉพาะ รูปแบบและปริมาณข้อมูลที่เก็บรวบรวม ข้อมูลส่วนบุคคลโดยเฉพาะความได้รับการรักษาความปลอดภัยโดยการให้ความคุ้มครองในระดับที่สูงกว่าข้อมูลธรรมดาหรือข้อมูลข่าวสารทั่ว ๆ ไป

มาตรการในการรักษาความปลอดภัยประกอบด้วยมาตรการคุ้มครองในทางกายภาพ (Physical Measure) เช่น การปิดล็อกตู้เอกสาร มาตรการควบคุมการเข้า-ออกสำนักงาน มาตรการการจัดระบบรักษาความปลอดภัยในองค์กร มาตรการจำกัดการเข้าตรวจดูข้อมูลตามหลักความจำเป็นที่ต้องรู้ (Need-to-Know Basis) และมาตรการทางเทคโนโลยี เช่นการใช้รหัสผ่าน (Password) และการเข้ารหัส (Encryption) เพื่อป้องกันมิให้ผู้ที่ไม่ได้รับอนุญาตเข้าตรวจดูข้อมูลนั้นได้ รวมทั้งการฝึกอบรมและดำเนินการให้พนักงานลูกจ้างตระหนักถึงความสำคัญของการรักษาความลับของข้อมูลส่วนบุคคล หรือการกำจัดหรือการทำลายข้อมูลส่วนบุคคลจะต้องกระทำด้วยความระมัดระวัง

8) หลักการเปิดเผย (Openness)

องค์กรต้องจัดทำนโยบายและแนวทางปฏิบัติขององค์กรในการจัดการข้อมูลส่วนบุคคล กล่าวคือ การจัดการวิธีการเข้าถึงข้อมูลหรือจัดข้อมูลที่ต้องเผยแพร่แก่ประชาชนในสถานที่และวิธีการที่เหมาะสม บุคคลทั่วไปจะต้องสามารถได้รับข้อมูลนั้นได้โดยไม่ลำบากและข้อมูลดังกล่าวจะต้องเปิดเผยในลักษณะที่สามารถเข้าใจได้โดยทั่วไป โดยข้อมูลที่ได้เปิดเผยหรือเผยแพร่อย่างน้อยต้องประกอบด้วยรายการดังต่อไปนี้

(1) ชื่อ ตำแหน่งและที่อยู่ของบุคคลที่รับผิดชอบนโยบายและแนวทางปฏิบัติขององค์กร หรือผู้รับคำร้องหรือข้อซักถามต่าง ๆ

(2) วิธีการเข้าตรวจดูข้อมูลส่วนบุคคลที่อยู่ในความครอบครองขององค์กร

(3) รายละเอียดเกี่ยวกับข้อมูล ประเภทของข้อมูล ตลอดจนรายละเอียดเกี่ยวกับการนำข้อมูลส่วนบุคคลนั้นไปใช้

(4) สำเนาเอกสารแผ่นปลิว หรือข้อมูลอื่นใดเกี่ยวกับนโยบาย มาตรฐาน และประมวลจริยธรรม (Codes) ขององค์การ

(5) ข้อมูลส่วนบุคคลที่จัดหาให้แก่องค์กรที่เกี่ยวข้อง หน่วยงาน สาขา หรือบริษัทในเครือ

9) หลักการเข้าตรวจดูข้อมูลของบุคคล (Individual Access)

เมื่อมีการร้องขอบุคคลผู้เป็นเจ้าของข้อมูลจะต้องได้รับรายงานหรือเข้าตรวจดูเกี่ยวกับการมีอยู่ (Existence) การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคล นอกจากนี้ บุคคลสามารถโต้แย้งหากพบว่า ข้อมูลดังกล่าวไม่ถูกต้องหรือสมบูรณ์ และมีสิทธิเรียกต้องให้มีการแก้ไขเพิ่มเติมข้อมูลนั้นได้ตามความเหมาะสม อย่างไรก็ตาม ในบางสถานการณ์อาจไม่สามารถที่จะให้บุคคลเข้าตรวจดูข้อมูลส่วนบุคคลทั้งหมด แต่ข้อยกเว้นการเข้าตรวจดูนั้นควรมีลักษณะจำกัด ในกรณีที่องค์กรได้ปฏิแสธการขอเข้าตรวจดู องค์กรต้องแจ้งเหตุผลของการปฏิเสธนั้น การปฏิเสธอาจได้แก่ กรณีที่การเข้าตรวจดูข้อมูลส่วนบุคคลต้องมีการเสียค่าใช้จ่ายในการจัดหาข้อมูลดังกล่าวสูงมาก หรือในกรณีที่ข้อมูลนั้น มีข้อมูลส่วนบุคคลของบุคคลอื่นรวมอยู่ด้วย หรือในกรณีข้อมูลส่วนบุคคลที่ไม่สามารถเปิดเผยได้ด้วยเหตุผลทางกฎหมาย ด้านความปลอดภัย หรือทางการค้า

เมื่อบุคคลผู้เป็นเจ้าของข้อมูลส่วนบุคคลขอเข้าถึงข้อมูลข่าวสารของตน องค์กรต้องแจ้งให้บุคคลดังกล่าวทราบว่า องค์กรมีข้อมูลส่วนบุคคลของบุคคลนั้นอยู่ในความครอบครองหรือไม่ ชี้แจงถึงแหล่งที่มาของข้อมูลนั้น ในกรณีที่มีการขอเข้าถึงข้อมูลทางการแพทย์ซึ่งเป็นข้อมูลส่วนบุคคลที่มีลักษณะเป็นข้อมูลส่วนตัวโดยเฉพาะ องค์กรอาจเลือกที่จะเปิดเผยโดยผ่านแพทย์ก็ได้

ในการเปิดเผยข้อมูลข่าวสารที่สามารถทำได้ องค์กรอาจต้องจัดทำบัญชีรายละเอียดเกี่ยวกับการนำข้อมูลไปเปิดเผย ลักษณะของการนำข้อมูลไปใช้ และการจัดทำบัญชีรายชื่อของบุคคลภายนอกที่จะสามารถเข้าถึงข้อมูลส่วนบุคคลดังกล่าวได้ ในการจัดทำบัญชีรายชื่อของบุคคลภายนอกดังกล่าวควรพยายามกำหนดประเภทของบุคคลภายนอกที่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ให้ชัดเจนมากที่สุดเท่าที่จะทำได้

ในการพิจารณาเปิดเผยข้อมูลตามคำขอของผู้ร้อง องค์กรต้องตอบคำร้องขอภายในระยะเวลาที่เหมาะสมโดยที่ผู้ร้องขอไม่ต้องเสียค่าใช้จ่าย หรือเสียค่าใช้จ่ายน้อยที่สุด ข้อมูลที่ได้จัดให้มีการเข้าถึงได้จะต้องจัดให้อยู่ในรูปแบบที่สามารถเข้าถึงและสามารถเข้าใจโดยทั่วไป เช่น ในกรณีที่องค์กรนั้นใช้อักษรย่อหรือรหัสในการบันทึกข้อมูลก็ต้องแนบคำอธิบายที่เกี่ยวข้องกับการใช้คำดังกล่าว

เมื่อบุคคลเห็นว่าข้อมูลส่วนบุคคลของตนที่อยู่ในความครอบครองขององค์กรนั้น ๆ ไม่ถูกต้องหรือไม่สมบูรณ์ และบุคคลได้โต้แย้งให้แก้ไขเปลี่ยนแปลง องค์กรจะต้องทำการแก้ไขเพิ่มเติมข้อมูลดังกล่าวตามที่ร้องขอ ซึ่งอาจกระทำโดยวิธีการแก้ไข การตัดออก หรือการเพิ่มเติม

ข้อมูล แล้วแต่กรณี และหากข้อมูลดังกล่าวไม่ได้รับการแก้ไขให้เป็นที่พอใจตามคำโต้แย้ง ให้องค์กรบันทึกเรื่องที่ไม่ได้ดำเนินการแก้ไขนั้นไว้

10) หลักการโต้แย้งการปฏิบัติขององค์กร (Challenging Compliance)

บุคคลผู้เป็นเจ้าของข้อมูลสามารถทำคำโต้แย้งเกี่ยวกับการดำเนินการเกี่ยวกับข้อมูลข่าวสารที่เกี่ยวกับตนโดยการทำคำโต้แย้งไปยังบุคคลที่ได้รับแต่งตั้งให้เป็นผู้รับผิดชอบการปฏิบัติหน้าที่องค์กรได้

ในการทำคำร้องขอหรือคำโต้แย้ง องค์กรต้องจัดให้มีกระบวนการที่เหมาะสมในการรับคำร้อง ข้อโต้แย้ง หรือข้อซักถามเกี่ยวกับนโยบายและแนวทางปฏิบัติขององค์กรเกี่ยวกับการจัดการข้อมูลส่วนบุคคล ทั้งนี้กระบวนการดังกล่าวต้องทำได้ไม่ยุ่งยากและไม่ซับซ้อน โดยองค์กรจะต้องแจ้งหรืออธิบายให้บุคคลทราบเกี่ยวกับกระบวนการร้องเรียน การรับคำร้อง และการตอบข้อซักถาม และต้องทำการสอบสวนเกี่ยวกับคำร้องทั้งหลาย และในกรณีที่คำร้องนั้นมีเหตุอันสมควร องค์กรจะต้องมีการดำเนินการที่เหมาะสม รวมทั้งการแก้ไขเพิ่มเติม หรือมีมาตรการที่เหมาะสมเกี่ยวกับนโยบายและแนวทางปฏิบัติขององค์กรที่จำเป็น

สำหรับข้อจำกัดนั้น จะเห็นว่าขอบเขตของกฎหมาย PIPEDA ใช้บังคับแก่องค์การทั้งหลาย (Organization) ที่มีการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล ไม่ว่าจะเป็นกรณีในการเก็บรวมรวม ใช้ หรือเปิดเผยเพื่อการประกอบกิจการขององค์กร หรือที่เกี่ยวกับลูกจ้างขององค์กร หรือข้อมูลส่วนบุคคลที่ใช้ในกิจการหรือธุรกิจของสหพันธรัฐ ทั้งนี้ กฎหมายที่ได้กำหนดกฎเกณฑ์ที่ใช้บังคับแก่การเก็บรวมรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลให้ความสำคัญกับการชั่งน้ำหนักระหว่างสิทธิความเป็นส่วนตัวของบุคคล (The Right of Privacy of Individual) ในส่วนที่เกี่ยวกับข้อมูลส่วนบุคคลของบุคคลนั้น กับความจำเป็นขององค์กรในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ซึ่งวิญญูชนเห็นว่าเหมาะสมกับสถานะการณ์[161]

อย่างไรก็ดี กฎหมายฉบับนี้ได้กำหนดให้องค์กรหรือบุคคลต่อไปนี้ไม่ต้องอยู่ภายใต้บังคับของกฎหมาย[162]

1. หน่วยงานของรัฐที่อยู่ภายใต้บังคับของ Privacy Act 1985
2. บุคคลธรรมดาในส่วนที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่บุคคลธรรมดาเก็บรวบรวม ใช้ หรือเปิดเผยเพื่อวัตถุประสงค์ส่วนตัวและมิใช่เพื่อการอย่างอื่น
3. องค์กรใด ๆ ที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการหนังสือพิมพ์ ศิลปะ หรือวรรณกรรม และมิใช่เพื่อการอย่างอื่น

---

[161] *เรื่องเดียวกัน*, หน้า 49-70.

[162] นคร เสรีรักษ์, *เรื่องเดิม*, หน้า 182-183

3.3.2.3 กลไกทางกฎหมายในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล

สำหรับองค์กรที่เป็นองค์กรหลักในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล (National Data Protection Authority) ของประเทศแคนาดาก็คือ สำนักงานคณะกรรมการสิทธิความเป็นส่วนตัวแห่งแคนาดา (Office of the Privacy Commissioner of Canada) ซึ่งมีความเป็นอิสระและทำหน้าที่เป็นตัวแทนของรัฐสภาที่มีภารกิจคือการปกป้องและส่งเสริมสิทธิความเป็นส่วนตัว

อำนาจหน้าที่ขององค์กรคณะกรรมการสิทธิความเป็นส่วนตัวแห่งแคนาดา (Privacy Commissioner) มีอำนาจหน้าที่หลายประการดังนี้[163]

1) รับคำร้องของบุคคลในกรณีที่องค์กรฝ่าฝืนบทบัญญัติ หรือในกรณีที่มีการละเมิดข้อมูลส่วนบุคคล และแจ้งให้องค์กรที่ถูกร้องเรียนทำการสอบสวนและพิจารณาคำร้องดังกล่าว

2) หากคณะกรรมการสิทธิความเป็นส่วนตัวแห่งแคนาดาพิจารณาแล้วเห็นว่ามีเหตุอันสมควรในอันที่จะต้องทำการสอบสวนเรื่องใด ๆ ที่เห็นว่ามีการละเมิดข้อมูลส่วนบุคคล คณะกรรมการฯสามารถนำเรื่องดังกล่าวขึ้นพิจารณาได้

3) เพื่อให้บรรลุวัตถุประสงค์ในการดำเนินการสอบสวน คณะกรรมการสิทธิความเป็นส่วนตัวแห่งแคนาดา อาจใช้อำนาจเรียกให้บุคคลใดมาให้คำชี้แจงหรือเรียกให้ส่งหลักฐานใด ๆ ที่เกี่ยวข้องกับเรื่องที่มีการร้องเรียนนั้น รับหลักฐานและข้อมูลอื่นใดตามที่คณะกรรมการฯ เห็นสมควร เข้าไปในสถานที่ขององค์กรใด ๆ ในเวลาที่เหมาะสม และมีอำนาจซักถามบุคคลในสถานที่นั้นได้ตามสมควร ตลอดจนเจรจาเป็นการส่วนตัวกับบุคคลที่อยู่ในสถานที่ดังกล่าว

4) คณะกรรมการสิทธิความเป็นส่วนตัวแห่งแคนาดาจะต้องจัดทำรายงานผลการพิจารณาและแก้ปัญหา ประกอบด้วยคำวินิจฉัยและคำแนะนำของคณะกรรมการฯ ในคดีต่าง ๆ การระงับข้อโต้แย้งที่คู่กรณีได้ตกลงกัน คำร้องที่องค์กรส่งให้แก่คณะกรรมการฯ คำบอกกล่าวที่เกี่ยวกับการดำเนินการที่ได้กระทำไปแล้ว หรือที่จะกระทำคำแนะนำที่ระบุไว้ในรายงาน หรือเหตุผลที่จะไม่ดำเนินการ และความช่วยเหลือที่ผู้ยื่นคำร้องอาจได้รับตามที่กำหนดในกฎหมาย

โดยภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดา (PIPEDA) คณะกรรมการสิทธิความเป็นส่วนตัวแห่งแคนาดาจะออกรายงานผลการพิจารณาและคำแนะนำ

---

[163] *เรื่องเดียวกัน*, หน้า 183-184

สำหรับการปฏิบัติ (ถ้าหากมี) แม้ว่ารายงานดังกล่าวจะไม่มีผลผูกพัน แต่อาจมีการเปิดเผยต่อสาธารณะตามดุลยพินิจของคณะกรรมการฯ หากว่าจะเป็นประโยชน์ต่อสาธารณะ[164]

ในด้านการพิจารณาคดี ผู้ร้องเรียนซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล หรือคณะกรรมการสิทธิความเป็นส่วนตัวของแคนาดาภายใต้ความยินยอมของเจ้าของข้อมูล สามารถที่จะนำคดีขึ้นสู่การพิจารณาของศาล The Federal Court เพื่อพิจารณาคดีใหม่อีกครั้งหนึ่ง ซึ่งศาลมีอำนาจอย่างกว้างขวางในการสั่งการแก้ไขการปฏิบัติขององค์กร และมีอำนาจลงโทษให้ชดใช้ค่าเสียหายเพื่อเยียวยาความเสียหายให้แก่ผู้ร้องเรียน ซึ่งความเสียหายนี้รวมไปถึงความเสียหายต่อชื่อเสียงเกียรติยศซึ่งได้รับความเดือดร้อนด้วย

สำนักงานคณะกรรมการสิทธิความเป็นส่วนตัวแห่งแคนาดาและองค์กรอาจตกลงทำข้อตกลงเกี่ยวกับการปฏิบัติตามความสมัครใจ โดยถ้าองค์กรรับรองว่าจะปฏิบัติตามคำแนะนำที่ได้ทำไว้ภายใต้กฎหมาย PIPEDA และถ้าผู้ร้องเรียนเห็นชอบด้วย คณะกรรมการฯ จะไม่นำคดีขึ้นสู่ศาลเพื่อพิจารณาคดี หรือจะระงับการยื่นคำร้องต่อศาลที่ค้างอยู่ทั้งหมดก็ได้ เว้นแต่จะมีการละเมิดข้อตกลง และหากต่อมา หากองค์กรไม่สามารถปฏิบัติตามความตกลงของตนในข้อตกลงการปฏิบัติตามสำนักงานคณะกรรมการสิทธิความเป็นส่วนตัวของแคนาดาก็สามารถยื่นคำร้องต่อศาลเพื่อขอให้ศาลสั่งให้องค์กรปฏิบัติตามเงื่อนไขของข้อตกลงได้[165]

สำหรับอัตราโทษในกรณีของการละเมิดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนั้น มีการกำหนดไว้ดังนี้คือ สำหรับกฎหมายระดับมลรัฐ มีการกำหนดข้อหาและโทษทางอาญาไว้ในรัฐควิเบค อัลเบอร์ตา และบริติช โคลัมเบีย คือ บทบัญญัติทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลของรัฐเหล่านี้ ซึ่งหากถูกละเมิดก็ถือเป็นความผิดและส่งผลให้มีการปรับสูงถึง 10,000 ดอลลาร์สำหรับความผิดครั้งแรก และ 20,000 ดอลลาร์สำหรับความผิดที่ตามมาในรัฐควิเบค และ 100,000 ดอลลาร์สำหรับความผิดในอัลเบอร์ตาและบริติชโคลัมเบีย รวมถึงความผิดที่ไม่ปฏิบัติตามคำสั่งของคณะกรรมการสิทธิความเป็นส่วนตัวของแคนาดา[166]

ภายใต้กฎหมาย PIPEDA มีบทบัญญัติทางกฎหมายที่จำกัดมากขึ้น การฝ่าฝืนอาจส่งผลให้ผู้กระทำต้องถูกลงโทษทางอาญา ตัวอย่างเช่น บุคคลใด ๆ ที่มีเจตนาทำลายข้อมูลส่วนบุคคลของบุคคลอื่นซึ่งเป็นสาระสำคัญของการร้องขอเข้าถึงข้อมูลส่วนบุคคล หรือข้อมูลของลูกจ้างผู้แจ้งเบาะแสในการทุจริต หรือขัดขวางการดำเนินการสอบสวนข้อร้องเรียนของคณะกรรมการฯ หรือหลอกลวงหรือบีบบังคับให้มีการเก็บรวบรวมข้อมูลส่วนบุคคลอันเป็นการฝ่าฝืนต่อกฎหมายนี้ หรือไม่

---

[164] Adam Kardash and Patricia Kosseim, *op. cit.*

[165] *Ibid.*

[166] *Ibid.*

ยอมแจ้งเตือนเมื่อมีการละเมิดข้อมูลส่วนบุคคล มีความผิดและต้องระวางโทษปรับ 10,000 ดอลลาร์ ถึง 100,000 ดอลลาร์[167]

3.4 การคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศฝรั่งเศส

3.4.1 แนวคิดและวิวัฒนาการในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศฝรั่งเศส

3.4.1.1 ความหมายของข้อมูลส่วนบุคคลของประเทศฝรั่งเศส

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศฝรั่งเศส ได้แก่ รัฐบัญญัติที่ 78-17 ลงวันที่ 6 มกราคม ค.ศ.1978 ว่าด้วยข้อมูล สารสนเทศ แฟ้มข้อมูล และเสรีภาพ (Loi relative à l'informatique, aux fichiers et aux libertès หรือ The Act on Data Processing Data Files and Individual Liberties) โดยกฎหมายฉบับนี้ เป็นบทบัญญัติทั่วไปฉบับแรกของฝรั่งเศสที่ได้กำหนดได้รับรองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล

โดยข้อมูลส่วนบุคคลตามกฎหมายฉบับนี้ หมายถึง ข้อมูลทั้งหลายที่เกี่ยวข้องกับบุคคลธรรมดาที่ระบุตัวบุคคลนั้น หรือสามารถระบุตัวบุคคลได้ไม่ว่าโดยทางตรงหรือทางอ้อมโดยการอ้างอิงถึงเลขประจำตัวหรือลักษณะอย่างหนึ่งอย่างใดที่เป็นลักษณะเฉพาะของบุคคลนั้น[168]

3.4.1.2 สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในฐานะสิทธิขั้นพื้นฐาน

ประเทศฝรั่งเศสให้ความสำคัญกับสิทธิในการมีชีวิตส่วนตัวและสิทธิในการที่จะได้รับความเคารพในชีวิตส่วนตัวและชีวิต ครอบครัวของประชาชน การให้ความสำคัญกับสิทธิความเป็นส่วนตัวของประเทศฝรั่งเศสนี้ ได้รับอิทธิพลมาจากอนุสัญญาสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานยุโรป โดยเฉพาะอย่างยิ่งมาตรา 8 ของอนุสัญญาสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานยุโรปที่ให้ความคุ้มครองในข้อมูลส่วนบุคคลไม่ให้ถูกละเมิดได้ แม้ว่าจะเป็นการกระทำของเจ้าหน้าที่ของรัฐหรือของฝ่ายปกครองก็ตามที โดยระบุว่า หากฝ่ายปกครองหรือหน่วยงานของรัฐจะเข้าไปแทรกแซงในการใช้สิทธิดังกล่าว การแทรกแซงต้องได้รับการบัญญัติไว้ในรัฐบัญญัติ และการแทรกแซงจะต้องเป็นมาตรการที่จำเป็นต่อความความปลอดภัยของประเทศ (sécurité nationale) ต่อความมั่นคง (sûreté publique) ต่อความปลอดภัยทางเศรษฐกิจของประเทศ (bien-être économique du

---

[167] *Ibid.*

[168] สมศักดิ์ นวตระกูลพิสุทธิ์, *เรื่องเดิม,* หน้า 27-36.

pays) ต่อการรักษาความสงบเรียบร้อยของสังคมและการป้องกันอาชญากรรม (defense de l'ordre et prevention des infractions pénales) ต่อการคุ้มครองสุขภาพและศีลธรรม (protection de la santé ou de la morale) และต่อการคุ้มครองสิทธิและเสรีภาพของผู้อื่น (protection des droits et libertés d'autrui)[169]

3.4.1.3 วิวัฒนาการในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในประเทศฝรั่งเศส

กำเนิดของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศฝรั่งเศส มีที่มาจากการที่ในปี ค.ศ.1970 รัฐบาลฝรั่งเศสได้เสนอร่างกฎหมาย 2 ฉบับบนพื้นฐานของนโยบายที่ต้องการขยายการใช้คอมพิวเตอร์ในภาครัฐ และกฎหมายนี้กำหนดให้อำนาจแก่รัฐในการเก็บรวมรวบและสามารถจัดการเกี่ยวกับข้อมูลส่วนบุคคลของประชาชนได้มากขึ้น ซึ่งต่อมาในปี ค.ศ.1974 หนังสือพิมพ์ของฝรั่งเศส Le Monde ได้นำเสนอบทความข่าวเรื่อง "Safari" ou la chasse aux Français ที่แสดงถึงศักยภาพของคอมพิวเตอร์ที่มีประสิทธิภาพซึ่งสามารถรวบรวมข้อมูลต่าง ๆ รวมถึงข้อมูลส่วนบุคคลของพลเมืองจากทุกพื้นที่ของประเทศได้ และแผน Safari ของรัฐบาลฝรั่งเศสนี้จะดำเนินการผลักดันให้เกิดการรวมศูนย์ข้อมูลที่ถูกจัดเก็บในระบบคอมพิวเตอร์ทั้งหมดที่อยู่ในรูปไฟล์ต่าง ๆ ของรัฐบาลไว้ที่จุดเดียวกัน ซึ่งถือเป็นภัยคุกคามร้ายแรงต่อสิทธิเสรีภาพและอิสรภาพของบุคคลและจะทำลายความสมดุลของอำนาจ ซึ่งข้อโต้แย้งนี้ได้ขยายวงกว้างกลายเป็นประเด็นสาธารณะและนำไปสู่การตั้งคณะกรรมการที่มีชื่อว่า คณะกรรมาธิการด้านสารสนเทศและเสรีภาพ (Commission Informatique et Libertés: CIL) โดยจะการกำหนดมาตรการเพื่อให้แน่ใจว่าการพัฒนาระบบประมวลผลข้อมูลในภาครัฐภาครัฐและเอกชนจะเกิดขึ้นในบริบทของการเคารพต่อชีวิตส่วนตัวเสรีภาพส่วนบุคคลและเสรีภาพสาธารณะ ซึ่ง CIL ชุดนี้ได้ทำการศึกษาและสรุปว่าแม้การใช้เทคโนลียีสารสนเทศจะไม่ส่งผลให้เกิดการละเมิดสิทธิเสรีภาพส่วนบุคคล แต่ก็มีความเสี่ยงที่สำคัญสำหรับอนาคต การเตรียมการเพื่อเพิ่มระดับการควบคุมในทางสังคมต่อปัญหาที่จะเกิดขึ้นจึงเป็นเรื่องสำคัญ โดยผลของรายงานนี้ทำให้ในเวลาต่อมาประเทศฝรั่งเศสจึงได้มีการออกกฎหมาย คือ รัฐบัญญัติที่ 78-17 ลงวันที่ 6 มกราคม ค.ศ.1978 ว่าด้วยข้อมูล สารสนเทศ แฟ้มข้อมูล และเสรีภาพ (Loi relative à l'informatique, aux fichiers et aux libertès หรือ The Act on Data Processing Data Files and Individual Liberties) มาคุ้มครองสิทธิในข้อมูลส่วนบุคคลของประชาชนในที่สุด[170]

---

[169] *เรื่องเดียวกัน*.

[170] Brendan Van Alsenoy, **Regulating Data Protection the Allocation of Responsibility and Risk Among Actors Involved in Personal Data Processing** (Doctoral dissertation, Faculty of Law, Catholic University of Leuven, 2016), pp. 137-148.

อนึ่ง ขอบเขตของกฎหมายฉบับนี้ได้มีการกำหนดรับรองสิทธิของพลเมืองในการได้รับบริการระบบข้อมูลสารสนเทศภายใต้หลักการที่ว่าระบบข้อมูลสารสนเทศนั้นจะต้องไม่ก่อให้เกิดความเสียหายต่อชีวิตส่วนตัวของบุคคลและเสรีภาพส่วนบุคคลหรือสาธารณะ รวมถึงบุคคลทุกคนมีสิทธิที่จะรับทราบและโต้แย้งข้อมูลต่าง ๆ และเหตุผลที่ใช้ในระบบข้อมูลสารสนเทศแบบอัตโนมัติที่มีผลเป็นการโต้แย้งหรือละเมิดสิทธิของบุคคลนั้น รวมไปถึงกฎหมายฉบับนี้ยังได้กำหนดกฎเกณฑ์ควบคุมการจัดทำระบบข้อมูลสารสนเทศแบบอัตโนมัติและไม่อัตโนมัติ โดยมีการกำหนดบทบัญญัติเกี่ยวกับการเก็บรวบรวม การบันทึก และการเก็บรักษาข้อมูล ตลอดจนมีการควบคุมเนื้อหาสาระของข้อมูลในระบบ การใช้ประโยชน์ การแก้ไข การเพิ่มเติม การโอน และการลบทิ้งหรือทำลายข้อมูลส่วนบุคคลซึ่งอยู่ทั้งในอำนาจของฝ่ายปกครองหรือภาครัฐ (les fichiers administratifs ou publics) และในระบบข้อมูลสารสนเทศขององค์กรเอกชน (les fichiers privés) และรับรองสิทธิของบุคคลในการตรวจดูข้อมูลที่ระบุชื่อที่เกี่ยวกับตนในระบบข้อมูลสารสนเทศดังกล่าว สิทธิในการโต้แย้งมิให้เก็บรวบรวมข้อมูลที่ระบุชื่อที่เกี่ยวกับตนไว้ในฐานข้อมูลสารสนเทศ สิทธิในการรับทราบข้อมูลต่าง ๆ ที่เกี่ยวกับการรวบรวมข้อมูลระบุชื่อ สิทธิในการสอบถามหน่วยงานหรือองค์กรว่ามีการเก็บรวบรวมข้อมูลเกี่ยวกับตนหรือไม่[171]

ต่อมาเมื่อวันที่ 7 ตุลาคม 2016 ประเทศฝรั่งเศสได้ตรา รัฐบัญญัติสาธารณรัฐดิจิทัลของฝรั่งเศส (Loi n ° 2016-1321 pour une Républiquenumérique) ให้มีผลบังคับใช้ หลังผ่านกระบวนการพิจารณาอันยาวนานนับปี ซึ่งเริ่มตั้งแต่เดือนธันวาคม 2015 เพื่อแก้ไขกฎหมายสำหรับการกำกับควบคุมเศรษฐกิจดิจิทัลในแง่มุมต่าง ๆ ของฝรั่งเศส กฎหมายฉบับนี้ได้วางหลักการที่เป็นบทบัญญัติใหม่ที่อันจะกำกับควบคุมระบบเศรษฐกิจดิจิทัลในภาพรวม (เช่น ประเด็นการเปิดเผยข้อมูลส่วนบุคคล ประเด็นความร่วมมือทางเศรษฐกิจในโลกออนไลน์ ประเด็นการต่อต่านสื่อลามกอนาจาร และประเด็นสิทธิในการเข้าถึงอินเทอร์เน็ต) สำหรับผลกระทบต่อปัจเจกชนนั้น กฎหมายฉบับนี้มีความสำคัญเนื่องจากจะมีการแก้ไขรัฐบัญญัติการปกป้องข้อมูลของฝรั่งเศสในปี 1978 และกฎหมายอื่น ๆ ในหลายประการ เพื่อให้มีผลก่อนที่ GDPR จะเริ่มมีผลบังคับใช้ในปี 2018 โดยมีสาระสำคัญคือ[172]

---

[171] สมศักดิ์ นวตระกูลพิสุทธิ์, *เรื่องเดิม*, หน้า 27-36.

[172] Olivier Proust and Gaëtan Goossens, **France Adopts Digital Republic Law**, Retrieved February 10, 2019 from https://privacylawblog.fieldfisher.com/2016/france-adopts-digital-republic-law

1. ให้อำนาจ CNIL กำหนดโทษสูงขึ้นกว่าเดิม (Higher Fines Pronounced by CNIL)

กฎหมายฉบับนี้ได้มีการแก้ไข the Data Protection Act โดยให้องค์กร CNIL มีอำนาจกำหนดค่าปรับทางปกครองสูงขึ้น โดยก่อนหน้านี้ถูกนี้ ค่าปรับทางปกครองจำกัดไว้ที่ 150,000 ยูโร แต่ตามหลักการที่แก้ไขใหม่ CNIL จะสามารถกำหนดค่าปรับทางปกครองได้สูงถึง 3 ล้านยูโร ซึ่งในประเด็นนี้ตามรัฐบัญญัติสาธารณรัฐดิจิตอลได้อธิบายว่าเมื่อ GDPR มีผลบังคับใช้ในปี 2018 ก็จะมีผลทำให้ องค์กร CNIL จะสามารถกำหนดค่าปรับทางปกครองได้มากถึง 20 ล้านยูโร หรือ 4% ของมูลค่าการซื้อขายรวมทั่วโลกประจำปี สำหรับการละเมิดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ตามที่กำหนดไว้ในมาตรา 83 ของ GDPR แต่ผู้ควบคุมในประเทศฝรั่งเศสอาจถูกปรับไม่เกิน 3 ล้านยูโร สำหรับการฝ่าฝืน ซึ่งจะไม่เป็นไปตามหลักการของ GDPR ที่มีความสำคัญอย่างยิ่งต่อสิทธิใหม่ของเจ้าของข้อมูลส่วนบุคคล

2. ยกระดับสิทธิของปัจเจกชน (Enhanced Rights for Individuals)

โดยหลังจากที่มีการเริ่มทำ GDPR นั้น รัฐบัญญัติสาธารณะรัฐดิจิตอลที่ประกาศใช้ก็ได้พยายามที่จะยกระดับการคุ้มครองสิทธิของบุคคลภายใต้รัฐบัญญัติคุ้มครองข้อมูลซึ่งเป็นสิทธิพื้นฐานที่ให้แก่เจ้าของข้อมูลส่วนบุคคลที่จะตัดสินใจและควบคุมการใช้ข้อมูลส่วนบุคคลของพวกเขา ตัวอย่างเช่น รัฐบัญญัติสาธารณะรัฐดิจิตอลกำหนดให้ผู้ควบคุมข้อมูลต้องยินยอมให้เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิของเขาผ่านทางระบบอิเล็กทรอนิกส์ได้อย่างชัดเจนทุกครั้งที่มีการรวบรวมข้อมูลทางอิเล็กทรอนิกส์

3. ต้องให้ข้อมูลเพิ่มขึ้นแก่เจ้าของข้อมูลส่วนบุคคล (Additional Information to the Data Subjects)

รัฐบัญญัติสาธารณรัฐดิจิตอลกำหนดให้ผู้ควบคุมข้อมูลต้องแจ้งให้เจ้าของข้อมูลทราบเกี่ยวกับช่วงเวลาที่จะจัดเก็บข้อมูลส่วนบุคคล เว้นแต่กรณีที่ไม่สามารถกระทำได้ในช่วงเวลานั้น

นอกจากนี้ผู้ให้บริการด้านการสื่อสารออนไลน์สาธารณะจะต้องแจ้งให้ผู้ใช้ทราบว่าข้อมูลส่วนบุคคลของพวกเขาจะถูกประมวลผลอย่างไรภายหลังการเสียชีวิต เพื่อประโยชน์ในการใช้สิทธิตัดสินใจ

ในประเด็นเกี่ยวกับการประมวลผลข้อมูลเพื่อวัตถุประสงค์ในการวิจัย หรือทางการแพทย์ รัฐบัญญัติสาธารณะรัฐดิจิตอล กำหนดให้ผู้ปกครองตามกฎหมายของผู้เยาว์อายุต่ำกว่า 18 ปี หรือตัวแทนตามกฎหมายของบุคคลที่อยู่ภายใต้การคุ้มครอง ได้รับทราบข้อมูลเกี่ยวกับการประมวลผลข้อมูล อย่างไรก็ตาม สำหรับการวิจัยทางการแพทย์บางประเภทที่กำหนดไว้ในกฎหมายสาธารณสุข ผู้เยาว์อายุ 15 ปีขึ้นไปอาจคัดค้านบิดามารดาหรือผู้ปกครองตามกฎหมายที่เข้าถึงข้อมูลส่วนบุคคลของพวกเขา อันมาจากการเก็บรวบรวมและดำเนินการในทางการวิจัย หรือทางการแพทย์

ดังกล่าว รวมถึงอาจใช้สิทธิในการเข้าถึงข้อมูล และสิทธิขอแก้ไขข้อมูล รวมถึงสิทธิในการคัดค้านการประมวลผลด้วย

4. สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของผู้ตาย (Post Mortem Right to Privacy)

นับได้ว่าเป็นการสร้างนวัตกรรมเกี่ยวกับสิทธิใหม่ของปัจเจกชน ในการตัดสินใจว่าจะให้มีประมวลผลข้อมูลส่วนบุคคลอย่างไรหลังจากการเสียชีวิตของเขา โดยก่อนตายบุคคลใดบุคคลหนึ่งอาจทำคำสั่งทั่วไปหรือเฉพาะเจาะจงเกี่ยวกับการจัดเก็บการลบหรือการเปิดเผยข้อมูลส่วนบุคคลของ คำสั่งเหล่านี้ถูกเก็บไว้โดยบุคคลที่สามที่ผ่านการรับรองหรือ CNIL ในทางกลับกันบุคคลอาจส่งคำสั่งโดยเฉพาะเจาะจงไปยังผู้ควบคุมข้อมูลให้ผู้ควบคุมนั้นทราบว่าจะใช้ข้อมูลส่วนบุคคลนั้นได้อย่างไรหลังจากการตายของพวกเขา ซึ่งในกรณีที่ผู้ควบคุมได้รับคำสั่งเฉพาะเจาะจงจากบุคคลในการประมวลผลข้อมูลของเขาหลังจากเสียชีวิต การใช้หรือประมวลผลข้อมูลนั้นก็ต้องเป็นไปตามความยินยอมโดยที่ไม่อาจจะกระทำเป็นอย่างอื่นไปได้ ซึ่งกล่าวได้ว่าเจตนารมณ์ของบทบัญญัติใหม่นี้ การกำหนดให้ปัจเจกชนได้รับการลบของมูลส่วนบุคคลของเขาออกไปจากระบบหรือแพลตฟอร์มออนไลน์เสีย ถ้าหากไม่มีคำสั่งไว้ก่อนที่เขาจะเสียชีวิต

5. สิทธิที่จะถูกลืม (Right to be Forgotten)

หลักการนี้คือ เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะขอให้ลบข้อมูลส่วนบุคคลของตนโดยไม่ชักช้าเมื่อข้อมูลดังกล่าวถูกเก็บรวบรวมโดยผู้ให้บริการสื่อสังคมออนไลน์ ในกรณีที่ผู้ควบคุมข้อมูลได้ใช้ข้อมูล หรือมีการแบ่งปัน หรือส่งต่อข้อมูลให้กับผู้ควบคุมข้อมูลรายอื่น (บุคคลที่สาม) กรณีนี้ผู้ควบคุมข้อมูลรายแรกจะต้องดำเนินการตามสมควร รวมถึงใช้มาตรการทางเทคนิคเพื่อแจ้งให้บุคคลที่สามทราบ โดยคำนึงถึงเทคโนโลยีที่มีอยู่และค่าใช้จ่ายตามสมควร และหากผู้ควบคุมข้อมูลไม่ลบข้อมูลหรือไม่สามารถตอบคำขอของเจ้าของข้อมูลส่วนบุคคลได้ภายในหนึ่งเดือนบุคคลนั้นอาจยื่นเรื่องร้องเรียนต่อ CNIL เพื่อจะดำเนินมาตรการต่อไปภายในสามสัปดาห์หลังจากได้รับการร้องเรียน

6. เพิ่มระดับความลับในการติดต่อสื่อสาร (Enhanced Secrecy of Correspondence)

รัฐบัญญัติสาธารณะรัฐดิจิตอลได้กำหนดข้อผูกมัดใหม่สำหรับผู้ให้บริการด้านการสื่อสารโทรคมนาคมและผู้ให้บริการการสื่อสารอิเล็กทรอนิกส์แก่ประชาชนที่เสนอบริการการสื่อสารออนไลน์ (ตัวอย่างเช่นผู้ให้บริการการส่งข้อความออนไลน์) เพื่อรักษาความลับของการติดต่อรวมถึงเนื้อหาของข้อความ ข้อมูลประจำตัวของผู้ส่งและผู้รับและหัวเรื่องและสิ่งที่แนบของข้อความ การประมวลผลอีเมลอัตโนมัติหรือการสื่อสารดิจิทัลประเภทอื่น ๆ เพื่อจุดประสงค์ในการโฆษณา สถิติหรือการปรับปรุงการให้บริการนั้น ในการรักษาความลับของข้อมูล เว้นแต่ว่าจะได้รับความยินยอมอย่างชัดแจ้งก่อนการประมวลผลอย่างน้อยหนึ่งปี นอกจากนี้จะต้องมีความยินยอมเฉพาะสำหรับการประมวลผลข้อมูลแต่ละประเภท อย่างไรก็ตามข้อความอิเล็กทรอนิกส์ยังสามารถวิเคราะห์โดย

อัตโนมัติเพื่อแสดงการเรียงลำดับ หรือส่งข้อความ หรือเพื่อตรวจจับไวรัสหรือมัลแวร์คอมพิวเตอร์ในรูปแบบอื่น ๆ

7. สิทธิในการขอโอนข้อมูลของผู้บริโภค (New Right to Data Portability for Consumers)

รัฐบัญญัติสาธารณะรัฐดิจิตอล กำหนดหลักการใหม่ขึ้นภายใต้ประมวลกฎหมายผู้บริโภคซึ่งให้สิทธิแก่ผู้บริโภคในการกู้คืนและโอนย้ายข้อมูลส่วนบุคคลของพวกเขา หลักการใหม่นี้กำหนดให้ผู้ให้บริการการสื่อสารออนไลน์ทั้งหมดแก่สาธารณะ ต้องยอมให้ผู้บริโภคสามารถกู้คืนข้อมูลรวมถึงไฟล์ข้อมูลข้อมูลทั้งหมดได้ โดยไม่เสียค่าใช้จ่ายและสามารถเข้าถึงได้จากบัญชีออนไลน์ของผู้ใช้และข้อมูลนั้นต้องสามารถนำกลับมาใช้ใหม่โดยผู้ควบคุมข้อมูลอื่นได้อย่างง่ายดาย ซึ่งผู้ควบคุมข้อมูลจะต้องจัดเตรียมข้อมูลในรูปแบบที่สามารถอ่านได้ แต่ถ้าหากไม่สามารถทำได้ผู้ควบคุมข้อมูลจะต้องแจ้งให้ผู้บริโภคทราบถึงข้อจำกัดดังกล่าวและให้วิธีการอื่นสำหรับผู้ใช้ในการกู้คืนข้อมูลของตน

8. ข้อกำหนดสำหรับผู้ให้บริการแพลตฟอร์มออนไลน์ (Online Platform Providers)

รัฐบัญญัติสาธารณรัฐดิจิตอล กำหนดข้อผูกพันเฉพาะสำหรับผู้ให้บริการแพลตฟอร์มออนไลน์ พวกเขาถูกกำหนดให้เป็นธุรกิจที่ให้บริการการสื่อสารออนไลน์แก่ลูกค้าว่า 1) สามารถจัดอันดับหรืออ้างอิงโดยใช้อัลกอริทึมคอมพิวเตอร์ของเนื้อหาสินค้าหรือบริการที่เสนอหรือแสดงออนไลน์โดยบุคคลที่สาม (เช่นเครื่องมือค้นหา) หรือ 2) อนุญาตให้ฝ่ายต่าง ๆ ติดต่อกันเพื่อขายสินค้าเสนอบริการหรือแลกเปลี่ยนหรือแบ่งปันเนื้อหาสินค้าหรือบริการ (เช่นการประมูลออนไลน์หรือเว็บไซต์ช้อปปิ้ง)

ผู้ให้บริการแพลตฟอร์มออนไลน์เหล่านี้จะต้องให้ข้อมูลที่ถูกต้อง ชัดเจนและโปร่งใสแก่ผู้บริโภค เกี่ยวกับ 1) ข้อกำหนดการใช้งานทั่วไปที่ใช้กับแพลตฟอร์มและวิธีการที่ใช้ในการจัดอันดับอ้างอิงหรือยกเลิกการอ้างอิงเนื้อหาสินค้าหรือบริการที่มีอยู่ผ่านแพลตฟอร์มนี้; 2) ไม่ว่าจะมีความผูกพันตามสัญญาหรือค่าตอบแทน ในกรณีที่พวกเขามีส่วนสำคัญต่อการจัดอันดับหรือการอ้างอิงเนื้อหาสินค้าหรือบริการที่มีให้บนแพลตฟอร์มของพวกเขา; และ 3) สิทธิและข้อผูกพันของคู่กรณีในเรื่องทางแพ่งและทางการเงินเมื่อแพลตฟอร์มอนุญาตให้ผู้บริโภคติดต่อผู้เชี่ยวชาญหรือผู้ที่ไม่ใช่มืออาชีพ

9. ยกเลิกข้อจำกัดในการจัดเก็บข้อมูลเฉพาะในสหภาพยุโรป (No Restrictions on Data Storage)

รัฐบัญญัติสาธารณะรัฐดิจิตอล ได้ยกเลิกหลักการที่จะต้องเก็บข้อมูลทั้งหมดในสหภาพยุโรป และห้ามถ่ายโอนข้อมูลไปนอกสหภาพยุโรป ดังนั้น จึงไม่มีกฎการมีถิ่นที่อยู่ของข้อมูล ที่

จะกำหนดให้ธุรกิจจัดเก็บข้อมูลของพวกเขาในฝรั่งเศส และในทางกลับกันธุรกิจสามารถถ่ายโอนข้อมูลส่วนบุคคลนอกยุโรปได้ตราบใดที่พวกเขาเคารพข้อกำหนดการปกป้องข้อมูลของสหภาพยุโรป

10. ผลกระทบในการบังคับใช้กฎหมาย (Practical Implications)

รัฐบัญญัติสาธารณะรัฐดิจิตอลของประเทศฝรั่งเศส ได้กำหนดหลักการที่ชัดเจนในการปกป้องข้อมูลส่วนบุคคลอย่างจริงจังและกระตือรือร้นที่จะสร้างระบบป้องกันที่เข้มแข็งสำหรับการปกป้องข้อมูลส่วนบุคคล กฎหมายฉบับนี้แสดงให้เห็นว่า แม้ต่อมาว่า GDPR จะสร้างระบบการปกป้องข้อมูลที่เป็นอันหนึ่งอันเดียวกันทั่วทั้งสหภาพยุโรป แต่ประเทศสมาชิกสหภาพยุโรปยังสามารถใช้กฎเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลเพิ่มเติมหรือที่เข้มงวดกว่าได้ดังนั้นกฎหมายของแต่ละประเทศจะยังคงใช้ต่อไป ซึ่งหมายความว่าองค์กรธุรกิจยังคงจะต้องปฏิบัติตามกฎหมายภายในของแต่ละประเทศด้วยเมื่อต้องการจะใช้หรือประมวลผลข้อมูลส่วนบุคคลในสหภาพยุโรป

ต่อมาเมื่อสหภาพยุโรปได้มีการประกาศใช้ General Data Protection Regulation (GDPR) แล้ว ทำให้ส่งผลกระทบต่อประเทศฝรั่งเศสที่จะต้องปรับปรุงมาตรการในการคุ้มครองสิทธิให้สอดคล้องกับ GDPR โดยเมื่อวันที่ 21 มิถุนายน พ.ศ.2561 ได้มีการออกกฎหมายฉบับใหม่ (Loi n°2018-493 on the Protection of Personal Data) ซึ่งแก้ไขเพิ่มเติมกฎหมายฉบับเดิม เพื่อให้เป็นไปตามข้อกำหนดที่กำหนดไว้ใน GDPR และ Directive (EU) 2016/680 โดยเฉพาะกฎหมายฉบับใหม่ได้นำหลักการที่กำหนดไว้ใน GDPR มาบัญญัติไว้ในกฎหมาย[173] ซึ่งรายละเอียดจะได้กล่าวในส่วนต่อไป

3.4.2 มาตรการทางกฎหมายในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศฝรั่งเศส

3.4.2.1 ลักษณะและประเภทของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลที่ได้รับความคุ้มครอง

รัฐบัญญัติที่ 78-17 ลงวันที่ 6 มกราคม ค.ศ.1978 ว่าด้วยข้อมูล สารสนเทศ แฟ้มข้อมูล และเสรีภาพ (Loi relative à l'informatique, aux fichiers et aux libertès หรือ The Act on Data Processing Data Files and Individual Liberties) ได้มีให้ความหมายของคำว่าข้อมูลส่วนบุคคลไว้ว่าหมายถึง ข้อมูลใด ๆ ที่เกี่ยวข้องกับบุคคลที่ทำให้สามารถระบุหรือเปิดเผยตัวบุคคลได้ ไม่ว่าโดยตรงหรือโดยอ้อมโดย เช่นข้อมูลที่มีการอ้างอิงถึงหมายเลขประจำตัวประชาชน

---

[173] Olivier Proust and Julien-Alexis Defromont, **Post-GDPR French Data Protection Law Adopted,** Retrieved November 1, 2018 from https://privacylawblog.fieldfisher.com/2018/post-gdpr-french-data-protection-law-adopted

หมายเลขประกันสังคม หรือข้อมูลที่ระบุถึงอัตลักษณ์ทางกายภาพ สรีรวิทยา หรือจิตวิทยา ฐานะเศรษฐกิจวัฒนธรรมหรือสังคมของบุคคล ชื่อและวันเดือนปีเกิด ข้อมูล Biometrics ลายนิ้วมือ รวมถึงดีเอ็นเอ ฯลฯ เป็นต้น[174] ทำให้เราสามารถจำแนกประเภทของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลได้ดังนี้คือ

1. ข้อมูลส่วนบุคคล (Definition of Personal Data)

ข้อมูลส่วนบุคคลที่เปิดเผยโดยตรงหรือโดยอ้อมเชื้อชาติและเชื้อชาติความคิดเห็นทางการเมืองปรัชญาหรือศาสนาหรือสหภาพแรงงานของบุคคลหรือที่เกี่ยวข้องกับสุขภาพหรือชีวิตทางเพศของพวกเขา

2. ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Definition of Sensitive Personal Data)

ข้อมูลใด ๆ ที่เกี่ยวข้องกับบุคคลธรรมดาที่สามารถระบุได้โดยทางตรงหรือโดยทางอ้อมโดยการอ้างอิงถึงหมายเลขประจำตัวหรือปัจจัยหนึ่งหรือหลายอย่างที่เฉพาะเจาะจงเช่นชื่อหมายเลขทะเบียนหรือหมายเลขโทรศัพท์

สำหรับในส่วนของข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) นี้ตามกฎหมายที่ได้มีการแก้ไขเพิ่มเติม (Loi n°2018-493 on the Protection of Personal Data) เมื่อวันที่ 21 มิถุนายน พ.ศ.2561 ได้มีการปรับปรุงเพิ่มเติมความหมายเพื่อให้สอดคล้องกับ GDPR โดยขอบเขตของข้อมูลส่วนบุคคลที่มีความอ่อนไหว ได้รับการขยายความ รวมไปถึง ข้อมูลทางพันธุกรรม ข้อมูลไบโอเมตริกซ์ และข้อมูลเกี่ยวกับการกำหนดพฤติกรรมทางเพศของเจ้าของข้อมูล โดย GDPR สร้างข้อยกเว้นสำหรับข้อห้ามทั่วไปในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว และให้ความยืดหยุ่นแก่ประเทศสมาชิกเพื่อใช้ข้อยกเว้นเพิ่มเติม ทำให้กฎหมายที่แก้ไขใหม่ของประเทศฝรั่งเศสใช้ข้อยกเว้นดังกล่าวในบางประการ เช่น โดยการอนุญาตให้ประมวลผลข้อมูลไบโอเมตริกซ์เมื่อเหตุจำเป็นอย่างยิ่ง[175]

เมื่อพิจารณาถึงการรับรองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ของประเทศฝรั่งเศสแล้ว จะเห็นว่า รัฐบัญญัติที่ 78-17 ลงวันที่ 6 มกราคม ค.ศ.1978 ว่าด้วยข้อมูล สารสนเทศ แฟ้มข้อมูล และเสรีภาพ (Loi relative à l'informatique, aux fichiers et aux

---

[174] Commission Nationale de l'Informatique et des Libertés (CNIL), **Personal Data: Definition**, Retrieved October 1, 2018 from https://www.cnil.fr/en/personal-data-definition

[175] Olivier Proust and Julien-Alexis Defromont, *op. cit.*

libertès หรือ The Act on Data Processing Data Files and Individual Liberties) ได้บัญญัติรับรองสิทธิของบุคคลธรรมดาที่เกี่ยวข้องกับข้อมูลที่ระบุชื่อไว้หลายประการ ได้แก่[176]

1. สิทธิในการสอบถามหน่วยงานของรัฐ หรือ องค์กรเอกชนที่จัดทำระบบข้อมูลสารสนเทศแบบอัตโนมัติ ตามรายชื่อที่ CNIL ได้จัดทำและประกาศต่อสาธารณชนว่าระบบข้อมูลสารสนเทศดังกล่าวมีข้อมูลส่วนบุคคลของตนหรือไม่ และสิทธิในการเข้าตรวจดูข้อมูลนั้นได้ในกรณีที่มีข้อมูลข่าวสารของตนปรากฏอยู่

2. สิทธิในการได้รับการเปิดเผยข้อมูลที่เกี่ยวกับตน ทั้งนี้ ข้อมูลที่เปิดเผยนั้นจะต้องใช้ภาษาที่เข้าใจง่ายและต้องมีเนื้อความเป็นอย่างเดียวกับข้อมูลที่บันทึกไว้

3. สิทธิในการได้รับสำเนาเอกสารข้อมูลที่เกี่ยวกับตน

4. สิทธิในการขอให้ดำเนินการแก้ไขเพิ่มเติมทำให้ชัดเจนขึ้น ปรับปรุงให้ทันสมัย หรือลบทิ้งซึ่งข้อมูลที่เกี่ยวกับตนที่ไม่ถูกต้อง ไม่ครบถ้วนสมบูรณ์ คลุมเครือ ล้าสมัย หรือการเก็บรวบรวม การใช้ การเปิดเผย หรือการเก็บรักษาข้อมูลนั้นเป็นการต้องห้าม

นอกจากที่กล่าวมายังมีสิทธิอีก 2 ประการที่ได้มีการเพิ่มเติมขึ้นในภายหลัง คือ[177]

1. สิทธิในการโต้แย้งคัดค้านการเปิดเผยข้อมูลของตนในกรณีที่มีการนำไปใช้ประโยชน์ในทางการโฆษณาหรือวัตถุประสงค์ในทางการค้า ซึ่งบุคคลอาจคัดค้านการเปิดเผยข้อมูลของเขาต่อบุคคลที่สาม ในกรณีของการกระทำการเพื่อวัตถุประสงค์ดังกล่าวตั้งแต่ในขณะที่มีการเก็บรวบรวมข้อมูล

2. สิทธิที่จะร้องขอต่อ CNIL ให้ตรวจสอบการกระทำที่เป็นการละเมิดข้อมูลส่วนบุคคลของตน

จึงกล่าวได้ว่าในสังคมของประเทศฝรั่งเศส โดยระบบของกฎหมายภายในรัฐนั้น มีการวางหลักการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลไว้อย่างดีอยู่แล้ว ซึ่งเมื่อพิจารณาประกอบการการที่สหภาพยุโรป ได้มีการประกาศใช้ General Data Protection Reguration (GDPR) เพื่อคุ้มครองสิทธินี้อีกด้วยแล้วยิ่งทำให้การคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลยิ่งมีมาตรฐานสูงขึ้น ซึ่งโดยผลของการประกาศใช้นี้ มีผลกระทบทำให้มีการกำหนดสิทธิสำคัญเพิ่มเติมตามหลักการของ GDPR ซึ่งได้แก้สิทธิดังต่อไปนี้คือ[178]

---

[176] สมศักดิ์ นวตระกูลพิสุทธิ์, *เรื่องเดิม*, หน้า 27-36.

[177] Commission Nationale de l'Informatique et des Libertés (CNIL), **Rights and Obligations,** Retrieved March 11, 2018 from https://www.cnil.fr/en/rights-and-obligations

[178] EU, *op. cit.*

1. สิทธิที่จะได้รับการแจ้งเตือนเมื่อเกิดเหตุข้อมูลรั่วไหล (Breach Notification) ภายใน 72 ชั่วโมง

2. สิทธิในการเข้าถึง (Right to Access) ที่ผู้ควบคุมข้อมูล ต้องแจ้งเจ้าของข้อมูลว่าข้อมูลถูกใช้เอาไปใช้เพื่อวัตถุประสงค์ใด และต้องจัดทำสำเนาข้อมูลให้กับเจ้าของข้อมูลในรูปแบบอิเล็กทรอนิกส์ โดยห้ามเก็บค่าใช้จ่ายเพิ่ม

3. สิทธิที่จะถูกลืม (Right to be Forgotten) ซึ่งเจ้าของข้อมูลสามารถขอให้หน่วยงานควบคุมข้อมูลลบข้อมูลของตัวเองออกได้ตามความประสงค์

4. สิทธิในการโอนย้ายข้อมูลของตนจากผู้ประกอบการหนึ่งไปยังผู้ประกอบการอื่นได้ (Data Portability)

นอกจากนี้ ตามกฎหมายที่ได้มีการแก้ไขใหม่นั้น มีหลักการที่มีการเปลี่ยนแปลงอย่างสำคัญที่สุด ก็คือ สิทธิในข้อมูลของผู้เยาว์ โดยกฎหมายฉบับใหม่ได้มีการกำหนดให้ ผู้เยาว์ที่มีอายุต่ำกว่า 15 ปีสามารถใช้สิทธิในการคุ้มครองข้อมูลได้โดยไม่ต้องแจ้งให้บิดามารดาหรือผู้ปกครองตามกฎหมาย เกี่ยวกับการประมวลผลข้อมูลด้านสุขภาพของตนสำหรับการวิจัยทางการแพทย์ การศึกษาหรือการประเมินผลบางประเภท[179]

3.4.2.2 หลักการและข้อจำกัดในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล

กฎหมายฉบับนี้ว่าประกอบไปด้วยสาระสำคัญ 3 ประการ ดังต่อไปนี้[180]

ประการที่ 1 กฎหมายฉบับนี้ได้กำหนดให้มีองค์กรรับผิดชอบ เรียกว่า คณะกรรมการข้อมูลข่าวสารและเสรีภาพแห่งชาติ (National Commission for Data Processing and Licensing หรือ Commission nationale de l'informatiqueet des litertés: CNIL) เป็น องค์กรอิสระซึ่ง ให้คำแนะนำเกี่ยวกับการวางแผนและรับรองการประมวลผลข้อมูลข่าวสารของหน่วยงานหรือองค์กรต่าง ๆ คณะกรรมาธิการมี อำนาจหน้าที่ ในการแนะนำให้ความรู้เกี่ยวกับบทบัญญัติกฎหมายนี้ ในสิทธิและหน้าที่ของบุคคล รวมถึงการตรวจสอบดูแลผู้ประกอบการทางธุรกิจในการดำเนินการประมวลผลข้อมูลส่วนบุคคล นอกจากนี้ คณะกรรมาธิการต้องมีการจัดทำเอกสารเกี่ยวกับการประมวลผลข้อมูลข่าวสารในกิจกรรมต่าง ๆ เพื่อเผยแพร่ และจัดทำรายงานประจำปีเพื่อเสนอต่อนายกรัฐมนตรีและต่อรัฐสภา

คณะกรรมการว่าด้วยข้อมูลข่าวสารและเสรีภาพแห่งชาติ (La commission nationale de l'informatique et des libertés: CNIL) เป็นกรรมการอิสระไม่ อยู่ใต้อำนาจของ

---

[179] Olivier Proust and Julien-Alexis Defromont, *op. cit.*

[180] สมศักดิ์ นวตระกูลพิสุทธิ์, *เรื่องเดิม*, หน้า 27-36.

องค์กรใด โดยองค์กรนี้ประกอบไปด้วยกรรมการ 17 คนมีวาระการดำรงตำแหน่ง 5 ปี โดยมีกรรมการ 2 คน มาจากสมาชิกสภาผู้แทนราษฎร กรรมการ 2 คน มาจากสมาชิกวุฒิสภา กรรมการ 2 คนมาจากสภาเศรษฐกิจและสังคม กรรมการ 2 คน มาจากศาลปกครองสูงสุด กรรมการ 2 คน มาจากศาลฎีกากรรมการ 2 คน มาจากศาลการคลังและภาษี กรรมการผู้ทรงคุณวุฒิ 2 คน มาจากการแต่งตั้งโดยกฤษฎีกาจากการเสนอของประธานวุฒิสภาและประธานสภาผู้แทนราษฎรและกรรมการอีก 3 คน มาจากการแต่งตั้งโดยกฤษฎีกาของที่ประชุมคณะรัฐมนตรี

ประการที่ 2 กฎหมายนี้กำหนดให้มีหลักประกันในการคุ้มครอง (Preventive Guarantees) เพื่อรับรองว่าระบบการประมวลผลข้อมูลข่าวสารได้ปฏิบัติตามแนวทางที่กำหนด

ประการที่ 3 กฎหมายนี้ได้ให้สิทธิในการเข้าถึงข้อมูลข่าวสารและสิทธิในการโต้แย้งหรือเรียกร้องให้มีการแก้ไขเปลี่ยนแปลงข้อมูลส่วนบุคคล

บทบัญญัตินี้อยู่บนพื้นฐานว่าระบบการประมวลผลข้อมูลข่าวสารจะต้องไม่ก่อให้เกิดความเสียหายต่อความเป็นส่วนตัวของบุคคล (Human Identity) สิทธิความเป็นส่วนตัว (Privacy) เสรีภาพส่วนบุคคลหรือสาธารณะ (Individual or Public Liberties) และบุคคลมีสิทธิที่จะรับทราบและโต้แย้งข้อมูลต่าง ๆ และเหตุผลที่ใช้ในระบบประมวลผลข้อมูลข่าวสารแบบอัตโนมัติที่มีผลเป็นการโต้แย้งบุคคลนั้น

กฎหมายได้กำหนดวิธีปฏิบัติเกี่ยวกับการเก็บรวบรวม การบันทึกและการเก็บรักษาข้อมูล ที่ ระบุ ชื่อ โดยกฎหมายนี้ใช้บังคับทั้งในระบบการประมวลผลแบบอัตโนมัติและวิธีการประมวลผลด้วยวิธีธรรมดา ตลอดจนควบคุมเนื้อหาของข้อมูลในระบบ การใช้ประโยชน์ข้อมูล การแก้ไขเปลี่ยนแปลง การลบ การเพิ่มข้อมูล การโอนหรือการทาลายข้อมูลดังกล่าว ทั้งในภาคเอกชนและภาครัฐ

รัฐบัญญัติที่ 78-17 ลงวันที่ 6 มกราคม ค.ศ.1978 ว่าด้วยข้อมูลสารสนเทศแฟ้มข้อมูลและเสรีภาพ มีกรอบของการใช้รัฐบัญญัติฉบับดังกล่าวโดยได้มีการกำหนดไว้ในมาตรา 4 ที่กำหนดว่ารัฐบัญญัติฉบับนี้จะไม่อาจใช้บังคับได้หากว่าเป็น ข้อมูลสารสนเทศที่เกี่ยวกับข้อมูลส่วนบุคคลซึ่งจัด ทำขึ้นเพื่อประโยชน์ของรัฐและเกี่ยวข้องกับประโยชน์สาธารณะ เช่น ความมั่นคงแห่งรัฐ การป้องกัน ประเทศ หรือ ความปลอดภัย ของประชาชน การป้องกัน การค้นหา การพบหรือ การติดตามการกระทำความผิดอาญา การจัดทำระบบข้อมูลสารสนเทศในกรณีต่าง ๆ เหล่านี้จะต้องมีการตราเป็นกฎหมายหรือกฎระเบียบของรัฐมนตรีที่มีอำนาจหน้าที่ที่เกี่ยวข้องแก่การนั้นเป็นการเฉพาะ

นอกจากนี้ กฎหมายได้ กำหนดบทนิยามของคำว่า “ระบบข้อมูลสารสนเทศแบบอัตโนมัติที่เกี่ยวกับข้อมูลที่ระบุชื่อ” ไว้ว่า หมายถึง การดำเนินการในทุกขั้นตอนโดยระบบอัตโนมัติที่เกี่ยวกับการเก็บรวบรวม การบันทึก การจัดทำ การแก้ไข การเก็บรักษาและการทำลายข้อมูลที่ ระบุชื่อ ตลอดจนการดำเนินการทั้งหลายที่เกี่ยวกับการใช้ประโยชน์ซึ่งแฟ้มข้อมูลหรือฐานข้อมูล และ

โดยเฉพาะอย่างยิ่งการเชื่อมเครือข่ายหรือการส่งถึงกัน การตรวจดูหรือการเปิดเผยข้อมูลที่ระบุชื่อ ทั้งนี้ กฎหมายนี้ มีขอบเขตครอบคลุม ระบบข้อมูลข่าวสารทั้งในภาครัฐและภาคเอกชน อย่างไรก็ตาม กฎหมายได้กำหนดมาตรการในการควบคุมสำหรับข้อมูลในภาครัฐและภาคเอกชนไว้แตกต่างกัน

ระบบข้อมูลข่าวสารในภาครัฐ ได้แก่ ระบบข้อมูลข่าวสารที่ดำเนินการเพื่อประโยชน์ของรัฐ องค์การมหาชน องค์กรปกครองส่วนท้องถิ่น หรือนิติบุคคลตามกฎหมายเอกชนที่จัดทำบริการสาธารณะ ส่วนข้อมูลข่าวสารอื่นที่นอกเหนือไปจากข้อมูลข่าวสารที่ใช้ในองค์กรเหล่านี้ถือว่าเป็นระบบข้อมูลข่าวสารในภาคเอกชน

บทบัญญัติของประเทศฝรั่งเศสก็เช่นเดียวกับประเทศอื่น ๆ ในเรื่องของการจำกัดการเก็บข้อมูลประเภทที่เป็นข้อมูลส่วนตัวโดยเฉพาะที่มีความอ่อนไหว (Sensitive Data) เช่น ข้อมูลที่แสดงให้เห็นถึงชาติกำเนิด หรือ ความคิดเห็นทางการเมืองทางปรัชญา หรือทางศาสนา หรือการเป็นสมาชิกสหพันธ์ อย่างไรก็ดี ในข้อยกเว้นในข้อจากัดนี้ เช่น กรณีข้อมูลที่เกี่ยวข้องกับการกระทำความผิด การถูกลงโทษ หรือการถูกกักกัน จะถูกจัดเก็บได้เฉพาะศาลและฝ่ายปกครองที่มีอำนาจ ตลอดจนนิติบุคคลที่จัดทำบริการสาธารณะในกรณีที่ได้รับความเห็นชอบจากคณะกรรมการว่าด้วยข้อมูลข่าวสารและเสรีภาพแห่งชาติ (La commission nationale de l'informatique et des libertés หรือ CNIL) เท่านั้น หรือองค์กรบางแห่ง ได้แก่ องค์กรทางศาสนาหรือกลุ่มกิจกรรมทางศาสนา ปรัชญา การเมือง หรือ สหพันธ์ สามารถเก็บ ข้อมูลเกี่ยวกับ สมาชิก ของตนหรือ บุคคลที่เกี่ยวข้องได้ นอกจากนี้ หน่วยงานอื่นอาจดำเนินการดังกล่าวได้ด้วยเหตุผลเพื่อประโยชน์สาธารณะ ทั้งนี้โดยตราเป็นรัฐกฤษฎีกาที่ผ่านความเห็นชอบของสภาที่ปรึกษาแห่งรัฐ ตามคำเสนอหรือความเห็นชอบของคณะกรรมการว่าด้วยข้อมูลข่าวสารและเสรีภาพแห่งชาติ

กฎหมายนี้กำหนดให้องค์กรผู้จัดทำระบบข้อมูลข่าวสารต้องมีหน้าที่ ดังนี้

1. การจัดทำระบบการประมวลข้อมูลข่าวสารโดยวิธีอัตโนมัติในภาครัฐ

การดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลจะต้องได้รับอนุญาตตามกฎหมาย ซึ่งเป็นไปตามกฎระเบียบที่ออกตามความเห็นของ CNIL โดยกฎระเบียบที่ออกเพื่อ การจัดระบบข้อมูลข่าวสารต้องปรากฏรายละเอียดต่อไปนี้

1) ชื่อและวัตถุประสงค์ของการจัดทำข้อมูลข่าวสาร

2) หน่วยงานหรือ บุคคลใดที่บุคคลผู้เป็นเจ้าของข้อมูลที่ระบุชื่อสามารถใช้สิทธิเข้าตรวจดูข้อมูลตามที่กำหนดในกฎหมาย

3) ประเภทของข้อมูลที่ระบุชื่อที่บันทึกได้ ตลอดจนผู้ที่สามารถเข้าถึงหรือสามารถได้รับข้อมูลนั้น หรือประเภทของผู้ที่ได้รับข้อมูลนั้นที่สามารถตรวจดูข้อมูลนั้นได้

2. การจัดทำระบบการประมวลผลข้อมูลข่าวสารโดยวิธีอัตโนมัติภาคเอกชน

องค์กรเอกชนจะต้องยื่นคำขอต่อคณะกรรมการข้อมูลสารสนเทศและเสรีภาพแห่งชาติล่วงหน้าก่อนการดำเนินการ ทั้งนี้คำขอดังกล่าวถือเป็นข้อผูกพันขององค์กรว่า การจัดทำระบบข้อมูลข่าวสารจะต้องเป็นไปตามเงื่อนไขต่าง ๆ ที่กฎหมายกำหนด และจะต้องได้รับอนุญาตจาก CNIL ก่อนจึงจะดำเนินการได้ ในการทำคำขอจัดทำระบบข้อมูล ข่าวสารต่อ CNIL ต้องปรากฏรายการ ดังนี้[181]

1) ผู้ดำเนินการหรือผู้ควบคุมแฟ้มข้อมูลข่าวสารบุคคล (File controller) หรือบุคคลที่มีอำนาจตัดสินใจจัดทำระบบข้อมูลหรือตัวแทนของบุคคลดังกล่าวในประเทศฝรั่งเศส ในกรณีที่บุคคลนั้นอาศัยอยู่ในต่างประเทศ

2) ลักษณะ วัตถุประสงค์ และชื่อของระบบข้อมูล

3) หน่วยงานที่รับผิดชอบในการดำเนินการจัดทำระบบข้อมูลข่าวสาร

4) หน่วยงานภายในที่บุคคลสามารถใช้สิทธิเข้าตรวจดูข้อมูล ตลอดจนมาตรการต่าง ๆ ที่กำหนดเพื่ออำนวยความสะดวกแก่การใช้สิทธิดังกล่าว

5) ประเภทของบุคคลที่สามารถเข้า ถึงข้อมูล ที่บันทึกได้โดยตรง ทั้งนี้ ตามอำนาจหน้าที่ของบุคคลนั้น หรือตามความจาเป็นของหน่วยงานภายใน

6) การดำเนินงานเกี่ยวกับข้อมูลที่ระบุชื่อ ที่มาของข้อมูล ระยะเวลาของการเก็บรักษามาตรการในการรักษาความปลอดภัย ตลอดจนผู้ได้รับข้อมูลนั้น หรือประเภทของผู้ได้รับข้อมูลนั้นที่จะสามารถตรวจดูข้อมูลนั้นได้

7) การส่งข้อมูลถึงกัน การเชื่อมโยงเครือข่าย หรือการเชื่อมโยงข้อมูลในรูปแบบอื่นใดตลอดจนการโอนข้อมูลแก่บุคคลภายนอก

8) ข้อกำหนดเพื่อรับรองความปลอดภัยของระบบข้อมูล และข้อมูลที่จัดเก็บและการรับรองความลับต่าง ๆ ที่ได้รับการคุ้มครองตามกฎหมาย

9) ข้อแถลงว่าระบบข้อมูลดังกล่าวมีวัตถุประสงค์ในการส่งข้อมูลที่ระบุชื่อระหว่างดินแดนของประเทศฝรั่งเศสและต่างประเทศหรือไม่ ทั้งนี้ ไม่ว่าจะกระทำในรูปแบบใด

อย่างไรก็ตาม คำขอเกี่ยวกับการจัดทำข้อมูลข่าวสารที่เกี่ยวข้องกับความมั่นคงของรัฐ การป้องกันประเทศ และความปลอดภัยสาธารณะ อาจไม่มีรายการบางรายการดังที่กำหนดไว้ข้างต้นก็ได้

สำหรับการจัดทำระบบข้อมูลข่าวสารของหน่วยงานรัฐหรือองค์กรเอกชนในกิจการบางประเภท ซึ่งมิได้ก่อให้เกิดผลกระทบต่อเสรีภาพหรือชีวิตส่วนตัว ให้ CNIL จัดทำหลักเกณฑ์อย่าง

---

[181] *เรื่องเดียวกัน*, หน้า 19-28.

ง่าย โดยเทียบเคียงจากรายการต่าง ๆ ตามที่กำหนดข้างต้น และประกาศหลักเกณฑ์ดังกล่าวให้สาธารณชนทั่วไปได้ทราบเพื่อเป็นแนวทางในการจัดทำระบบข้อมูลข่าวสาร และการจัดทำระบบข้อมูลข่าวสารต้องขออนุญาต CNIL ก่อนตามหลักทั่วไปที่กำหนดไว้ เว้นแต่คณะกรรมการจะมีคำสั่งเป็นพิเศษ เมื่อได้รับคำขอดังกล่าวแล้วผู้ยื่นคำขอจึงสามารถจัดทำระบบข้อมูลข่าวสารได้ การนำแนวทางอย่างง่ายไปใช้สามารถเกิดขึ้นในกิจการ เช่น การเก็บข้อมูลที่ระบุชื่อในระบบภาษี หรือข้อมูลระบุชื่อของห้องสมุด เป็นต้น

อย่างไรก็ดี แนวทางสำหรับกระบวนการจัดทำระบบข้อมูลข่าวสารอย่างง่ายประกอบด้วยรายการ ดังนี้[182]

1. การจัดทำระบบการประมวลผลข้อมูลข่าวสารกระทำเพียงเท่าที่วัตถุประสงค์ที่กำหนดเท่านั้น และเจ้าของข้อมูลต้องสามารถเข้าถึงข้อมูลข่าวสารได้โดยง่าย

2. ระบบการประมวลผลข้อมูลข่าวสารต้องใช้โปรแกรมคอมพิวเตอร์ที่สามารถตรวจสอบข้อมูลข่าวสารได้โดยง่าย

3. การเชื่อมโยงข้อมูลข่าวสารทำได้เท่าที่จำเป็นแก่วัตถุประสงค์และเพียงเท่าที่จำเป็นแก่การใช้เท่านั้น

4. ต้องมีมาตรการในการรักษาความปลอดภัย และมาตรการในการรักษาความลับของข้อมูลข่าวสาร

นอกจากนี้ ยังมีหน้าที่เฉพาะที่สำคัญ เช่น การให้ความเห็นชอบต่อการบันทึกข้อมูลเกี่ยวกับชาติกำเนิด หรือความคิดเห็นทางการเมือง ทางปรัชญา หรือทางศาสนา หรือการเป็นสมาชิกของสหพันธ์ต่าง ๆ และในการใช้อำนาจหน้าที่ในการควบคุม คณะกรรมการมีอำนาจจัดทำหลักเกณฑ์ เพื่อรับรองความปลอดภัยของระบบข้อมูล กำหนดมาตรการด้านความปลอดภัยในสถานการณ์พิเศษ ซึ่งอาจมีขอบเขตไปถึงการทำลายเครื่องมือและอุปกรณ์ต่าง ๆ ที่ใช้ในการจัดเก็บข้อมูล กำกับดูแลมิให้มาตรการต่าง ๆ ที่ดำเนินการเพื่อการใช้สิทธิเข้าตรวจดูข้อมูลและการแก้ไขข้อมูล ก่อให้เกิดอุปสรรคต่อเสรีภาพในการใช้สิทธิดังกล่าว จัดทำรายชื่อระบบข้อมูลข่าวสารและประกาศให้สาธารณชนรับทราบโดยระบบข้อมูลแต่ละระบบต้องประกอบด้วยกฎหมายหรือกฎระเบียบที่กำหนดให้จัดทำระบบข้อมูลชื่อของระบบข้อมูลและวัตถุประสงค์ หน่วยงานภายในที่บุคคลสามารถใช้สิทธิเข้าตรวจดูข้อมูล และประเภทของข้อมูล หรือประเภทของบุคคลที่สามารถเข้าตรวจดูข้อมูลนั้นได้ ประเด็นที่น่าสนใจของกฎหมายฉบับนี้ ก็คือ การอนุญาตให้ใช้ข้อมูลส่วนบุคคล (Consent) ซึ่งการอนุญาตให้มีการเข้าถึงข้อมูลส่วนบุคคลตามรัฐบัญญัติที่ 78-17 ลงวันที่ 6 มกราคม ค.ศ.1978 ว่าด้วยข้อมูลสารสนเทศ แฟ้มข้อมูล และเสรีภาพ นอกจากการได้รับอนุญาตจาก

---

[182] *เรื่องเดียวกัน*.

คณะกรรมการว่าด้วยข้อมูลข่าวสารและเสรีภาพแห่งชาติ (La commission nationale de l'informatique et des libertés: CNIL) หรือเป็นข้อยกเว้นที่เกี่ยวกับประโยชน์ของรัฐและเกี่ยวข้องกับประโยชน์สาธารณะตามมาตรา 26-27 แล้ว ยังจะต้องได้รับการอนุญาตให้มีการเข้าถึงข้อมูลส่วนบุคคลจากเจ้าของข้อมูลด้วย

สำหรับโทษสำหรับการละเมิดต่อข้อมูลส่วนบุคคลนั้น รัฐบัญญัติ ที่ 78-17 ลงวัน ที่ 6 มกราคม ค.ศ.1978 ว่าด้วยข้อมูลสารสนเทศแฟ้มข้อมูลและเสรีภาพ ไม่ได้มีการกำหนดโทษไว้แต่อย่างใด แต่โทษสำหรับการละเมิดต่อข้อมูลส่วนบุคคลถูกกำหนดไว้ในกฎหมายฉบับอื่น ๆ ที่สามารถนำมาใช้สำหรับการละเมิดต่อข้อมูลส่วนบุคคลได้ กล่าวคือ

ประมวลกฎหมายคุ้มครองผู้บริโภคและประมวลกฎหมายว่าด้วยการไปรษณีย์และการโทรคมนาคม ที่กำหนดว่า ผู้ที่ฝ่าฝืนประมวลกฎหมายว่าด้วยการไปรษณีย์และการโทรคมนาคมของฝรั่งเศสจะต้องถูกปรับเป็นเงิน 750 ยูโรต่อข้อความ และอาจได้รับโทษทางอาญา จำคุกสูงสุดไม่เกิน 5 ปี และปรับสูงสุด 300,000 ยูโร หากได้เลขหมายโทรศัพท์มาด้วยวิธีการไม่ชอบด้วยกฎหมาย

ประมวลกฎหมายแพ่งของประเทศฝรั่งเศส มาตรา 1382 ที่กำหนดว่า บุคคลที่ก่อให้เกิดความเสียหายแก่บุคคลอื่นจะต้องรับผิดต่อบุคคลนั้นเพื่อความเสียหายที่เกิดขึ้นแต่การนั้น กล่าวคือมีการกระทำความผิดของบุคคลหนึ่งต่อบุคคลอื่นและการกระทำนั้นก่อให้เกิดความเสียหายแก่ผู้เสียหาย ผู้ที่เป็นต้นเหตุแห่งการกระทำก็ต้องรับผิดต่อผลของความเสียหายที่เกิดขึ้นนั่นเอง

การก่อให้เกิดผลกระทบต่อชีวิตส่วนตัวของบุคคลตามมาตรา 1382 นี้มักจะเป็นการกระทำความผิดโดยจงใจอันมาจากการเลือกที่จะกระทำการนั้นโดยสมัครใจของผู้กระทำ แต่ก็อาจมีกรณีเป็นการกระทำโดยละเว้นได้เช่นกัน เช่น กรณีบรรณาธิการนิตยสารฉบับหนึ่งที่ปล่อยให้มีการตีพิมพ์บทความซึ่งก่อให้เกิดผลกระทบต่อชีวิตส่วนตัวของบุคคลหนึ่ง ทั้ง ๆ ที่ตนควรที่จะคัดค้านการตีพิมพ์บทความดังกล่าวบรรณาธิการนั้นจึงต้องรับผิดร่วมกับบริษัทนิตยสารในการชดใช้ค่าเสียหายแก่ผู้เสียหายเพื่อความเสียหายที่เกิดขึ้นแต่การนั้น เป็นต้น

ประมวลกฎหมายอาญาของประเทศฝรั่งเศสได้ กำหนดบทลงโทษสำหรับการล่วงละเมิดต่อข้อมูลส่วนบุคคลไว้ด้วยกันหลายมาตรา ซึ่งสามารถสรุปได้ว่ามีด้วยกันทั้งสิ้น 3 กรณีด้วยกัน กล่าวคือ[183]

1. ความผิดในการก่อให้เกิดผลกระทบต่อความลับในชีวิตส่วนตัวของบุคคลอื่นโดยเจตนา ถูกกำหนดอยู่ในมาตรา 226-1 วรรคหนึ่ง แห่งประมวลกฎหมายอาญากำหนดว่า การก่อให้เกิดความเสียหายต่อความลับ หรือเกี่ยวกับชีวิตส่วนตัวของบุคคลอื่น โดยการดักฟัง บันทึกหรือส่งต่อคำพูดที่บุคคลได้กล่าวขึ้นในลักษณะเป็นการส่วนตัวหรือเป็นความลับโดยมิได้รับความยินยอม

---

[183] *เรื่องเดียวกัน*.

ของบุคคลนั้น ไม่ว่าจะกระทำโดยใช้เครื่องมืออย่างใด หรือโดยการถ่าย การบันทึกหรือการส่งต่อภาพของบุคคลในสถานที่ส่วนบุคคลโดยมิได้รับความยินยอมของบุคคลนั้น ไม่ว่าจะกระทำโดยใช้เครื่องมืออย่างใด ต้องรับโทษจาคุกหนึ่งปีและปรับเป็นเงินจานวน 45,000 ยูโร

2. ความผิดในการก่อให้เกิดผลกระทบต่อความลับในการประกอบวิชาชีพ ถูกกำหนดอยู่ในมาตรา 226-1 แห่งประมวลกฎหมายอาญา กำหนดว่า การเปิดเผยข้อมูลที่มีลักษณะเป็นความลับ โดยบุคคลหนึ่งซึ่งได้รับข้อมูลนั้น โดยสภาพของเรื่อง หรือ โดยตำแหน่งหน้าที่ หรือ อันเนื่องมาจากการปฏิบัติตามอำนาจหน้าที่เป็นการชั่วคราว ต้องรับโทษจาคุกหนึ่งปีและปรับเป็นเงินจานวน 15,000 ยูโร

3. ความผิดในการก่อให้เกิดผลกระทบต่อความลับในจดหมายของบุคคลอื่น ซึ่งเป็นฐานความผิดที่มีเจตนารมณ์เพื่อคุ้มครองเสรีภาพในการแสดงความคิดเห็นผ่านจดหมายและคุ้มครองความลับในชีวิตส่วนตัวของบุคคลที่ปรากฏอยู่ในจดหมายนั้นถูกกำหนดอยู่ใน มาตรา 226-15 วรรคหนึ่ง แห่งประมวลกฎหมายอาญา กำหนดว่า การเปิด ทำลาย ทำให้ล่าช้า หรือส่ง กลับโดยเจตนาทุจริต ซึ่งจดหมายที่มีถึงบุคคลภายนอกไม่ว่าจะได้มาถึงจุดหมายปลายทางแล้วหรือไม่ก็ตามหรือการอ่านข้อความภายในจดหมายโดยการฉ้อฉล ต้องรับโทษจำคุกหนึ่งปี และปรับเป็นเงิน 45,000 ยูโร

โดยภายหลังที่ประเทศฝรั่งเศสได้มีการแก้ไขเพิ่มเติมกฎหมายให้สอดคล้องกับ GDPR ก็ได้มีการกำหนดมาตรการเพิ่มเติมที่สำคัญคือ มีการกำหนดบทลงโทษรุนแรงขึ้น กล่าวคือ หากพบว่ามีการปฏิบัติผิดไปจากหลักการของ General Data Protection Regulation องค์กรจะต้องจ่ายค่าปรับ 4% ของผลประกอบการรายได้ทั่วโลกทั้งหมด หรือสูงถึง 20 ล้านยูโร ซึ่งบทลงโทษนี้จะบังคับใช้ทั้งหน่วยงานผู้ควบคุมข้อมูล และผู้ประมวลผลข้อมูล ซึ่งบทบัญญัติของกฎหมายฉบับใหม่ที่ได้มีการแก้ไขเพิ่มเติม (Loi n°2018-493 on the Protection of Personal Data) ก็ได้มีการบัญญัติหลักการไว้เช่นเดียวกันกล่าวคือ หากมีการละเมิดข้อมูลส่วนบุคคล ก็จะมีบทลงโทษโดยมีการกำหนดค่าปรับไว้ หรือเพิกถอนการรับรองหรือการให้สิทธิ ซึ่งค่าปรับนี้ถือเป็นโทษปรับในทางปกครองซึ่งตามกฎหมายนี้ CNIL สามารถกำหนดค่าปรับได้ถึง 20 ล้านยูโรหรือคิดเป็นมูลค่าสูงสุด 4% ของมูลค่าผลประกอบการรายได้ทั่วโลกก่อนหน้านึงรอบบัญชี[184]

3.4.2.3 กลไกทางกฎหมายในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล

กลไกทางกฎหมายในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนั้นจะเห็นว่า บทบาทหลักจะอยู่ที่ CNIL ที่เป็นหน่วยงานอิสระของรัฐซึ่งมีหน้าที่ตรวจสอบเพื่อความมั่นใจว่ากฎหมายคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลสามารถมีผลบังคับใช้

---

[184] Olivier Proust and Julien-Alexis Defromont, *op. cit.*

อย่างมีประสิทธิภาพ สถานะของ CNIL ถือเป็นองค์กรกำกับดูแลของรัฐที่มีความเป็นอิสระ แต่มีอำนาจจำกัดภายใต้บทบัญญัติของกฎหมาย และทางด้านงบประมาณได้รับการสนับสนุนจากฝ่ายรัฐ โดย CNIL จะมีภารกิจพื้นฐานดังนี้[185]

1. การแจ้งสิทธิและให้ความรู้แก่ประชาชน

สำหรับในการแจ้งให้ประชาชนชาวฝรั่งเศสทราบถึงสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ซึ่งในการนี้ทำให้ CNIL จะต้องตอบคำถามต่าง ๆ จากประชาชนมากมาย เช่น ในปี ค.ศ.2013 มีโทรศัพท์เข้ามาสอบถามถึง 125,000 สาย

นอกจากนี้ CNIL ได้รณรงค์แคมเปญการรับรู้ที่สิทธิไปสู่สาธารณชนทั่วไปโดยใช้สื่อเว็บไซต์, เครือข่ายทางสังคมและการฝึกอบรมกลุ่มเป้าหมาย ที่เป็นองค์กร บริษัท หรือสถาบันต่าง ๆ หลายแห่ง อีกทั้ง CNIL ยังมีส่วนร่วมในการจัดประชุมสัมมนาและการประชุมเชิงปฏิบัติการเพื่อนำเสนอการรับรู้โดยได้นำกลุ่มองค์กรภาคประชาชนต่าง ๆ กว่า 60 องค์กร เข้ามามีส่วนร่วม

2. การปกป้องสิทธิของพลเมือง

สำหรับภารกิจด้านนี้ จะเห็นได้ชัดว่าในปี 2013 CNIL ได้รับเรื่องร้องเรียนทั้งสิ้น 5,640 ราย จากพลเมืองที่มีปัญหาเกี่ยวกับการล่วงละเมิดข้อมูลส่วนบุคคล และดำเนินการให้พวกเขามั่นใจได้ถึงสิทธิในข้อมูลส่วนบุคคลของตน โดยเรื่องร้องเรียนนั้นตัวอย่างเช่น คำขอลบข้อมูลบนอินเทอร์เน็ต, ขอให้หยุดการประชาสัมพันธ์ทางไปรษณีย์หรือออนไลน์, เรื่องกลไกการเฝ้าระวังเช่น การเฝ้าระวังวิดีโอหรือการล่วงรู้ตำแหน่งยานพาหนะ และประเด็นเกี่ยวกับการเงินและธนาคาร (คัดค้านการลงทะเบียนในแฟ้ม Banque de France)

3. การควบคุมและการให้คำแนะนำ

สำหรับภารกิจด้านนี้ของ CNIL จะมีการออกกฎระเบียบต่าง ๆ เพื่อนำมาใช้เป็นเครื่องมือในการควบคุมดูแลไม่ให้มีการล่วงละเมิดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ดังนี้

ประการแรก คือการออกกฎระเบียบต่าง ๆ ออกมาเพื่อกำกับการอนุมัติในการที่จะดำเนินการประมวลผลข้อมูลส่วนบุคคล อันจะมีผลกระทบต่อสิทธิของบุคคล

ประการที่สอง CNIL มีอำนาจในการอนุญาตในการกำหนดหลักการเกี่ยวกับโดเมนอื่น ๆ

ประการที่สาม จะมีการให้คำแนะนำแก่ผู้ควบคุมข้อมูลและเจ้าหน้าที่ผู้ดูแลข้อมูลส่วนบุคคลตามคำขอที่ส่งเข้ามา

---

[185] Commission Nationale de l'Informatique et des Libertés (CNIL), **The CNIL's Missions ,** Retrieved March 11, 2018 from https://www.cnil.fr/en/cnils-missions

และประการสุดท้าย CNIL จะดำเนินการให้ความคิดเห็นเกี่ยวกับร่างกฎหมายของรัฐบาลที่จะส่งผลกระทบต่อการปกป้องข้อมูลส่วนบุคคล

4. การบังคับให้ผู้ประกอบการดำเนินการตามข้อกำหนด

CNIL มีอำนาจในการให้คำรับรอง (The Certifications) สำหรับผลิตภัณฑ์หรือกระบวนการ ขององค์กรหรือบริษัท ในเรื่องที่เกี่ยวข้องกับการปกป้องข้อมูลส่วนบุคคล ซึ่งการให้คำรับรองนี้ CNILจะช่วยให้ สามารถแยกแยะคุณภาพของบริการในส่วนที่เกี่ยวข้องกับการดูแลคุ้มครองข้อมูลส่วนบุคคลของบริษัทและองค์กรต่าง ๆ อันจะเป็นตัวบ่งชี้ความไว้วางใจในผลิตภัณฑ์และกระบวนการขั้นตอนต่าง ๆ

5. การเตรียมการสำหรับนวัตกรรมใหม่ที่จะเกิดขึ้น

CNIL จะทำการประเมินแนวโน้มของเทคโนโลยีและการใช้ข้อมูลที่จะเกิดขึ้นในอนาคต เพื่อเตรียมการสำหรับมาตรการคุ้มครองข้อมูลส่วนบุคคลในอนาคต ไม่ว่าด้วยวิธีการดำเนินการวิจัย ให้ทุนวิจัย ให้รางวัลสำหรับวิทยานิพนธ์ เป็นต้น

6. การดำเนินการตรวจสอบและการลงโทษ

สำหรับการตรวจสอบภายหลังมีการล่วงละเมิดถือเป็นวิธีการที่ได้รับการยอมรับ โดย CNIL จะเป็นองค์กรที่มีอำนาจตรวจสอบการปฏิบัติตามกฎหมายอย่างเป็นรูปธรรม

นอกจากที่กล่าวมาข้างต้น ต้องยอมรับว่า CNIL จะมีอำนาจควบคุมเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ไม่ว่าจะเป็นการจัดเก็บ หรือ ประมวลผล รวมถึงการใช้แล้วแต่กรณี และสามารถออกคำสั่งเรียกสำเนาเอกสารทุกฉบับที่เห็นว่าเป็นประโยชน์ในแง่ของภารกิจของตน โดยตั้งแต่เดือนมีนาคม 2014 ทาง CNIL มีสิทธิดำเนินการตรวจสอบทางออนไลน์และออกคำสั่งให้ปฏิบัติตามข้อกำหนด แก่ บริษัท ที่ละเมิดกฎหมาย ผู้ควบคุมข้อมูลจะได้รับแจ้งถึงการตรวจสอบ นอกจากนี้เจ้าหน้าที่ของหน่วยงานด้านได้รับอนุญาตให้ทำการสืบสวนภายในขอบเขตของกฎหมายเพื่อรายงานการละเมิดกฎหมายต่อ CNIL นอกจากนี้ CNIL ยังมีอำนาจในการลงโทษ ซึ่งการลงโทษจะแตกต่างกันไปตามความรุนแรงของการละเมิดที่กระทำโดยผู้ควบคุมข้อมูล ซึ่งในการนี้จะมีระดับการดำเนินการดังนี้คือ[186]

ประการแรก คือการออกคำเตือนและประกาศเพื่อให้สอดคล้องกับข้อผูกพันที่กำหนดไว้ในกฎหมายและ

ประการที่สอง ถ้าผู้ควบคุมข้อมูลดำเนินการไม่สอดคล้องกับประกาศแจ้ง CNIL มีอำนาจสั่งให้การลงโทษทางการเงินเป็นสัดส่วนกับความรุนแรงของการละเมิดได้ถึง 3 ล้านยูโร เมื่อ

---

[186] *Ibid.*

พิจารณาจำนวนเงินที่ต้องเสียค่าปรับ CNIL ต้องคำนึงถึงปัจจัยหลายประการซึ่งส่วนใหญ่จะสะท้อนถึงข้อกำหนดที่กำหนดไว้ในระเบียบว่าด้วยการคุ้มครองข้อมูลทั่วไป

ซึ่งนับตั้งแต่เดือนตุลาคมปี 2016 เป็นต้นมา จะเห็นว่า ในกรณีฉุกเฉิน CNIL ก็มีสิทธิที่จะระงับและยกเลิกการแจ้งให้ทราบเพื่อปฏิบัติตามภายใน 24 ชั่วโมง เมื่อคู่กรณีที่ละเมิดไม่ปฏิบัติตาม CNIL อาจออกคำเตือนคำสั่งปรับหรือคำสั่งห้าม และในกรณีที่ฝ่ายละเมิดไม่สามารถปฏิบัติตามกฎหมายได้ CNIL สามารถสั่งปรับค่าปรับได้โดยไม่ต้องแจ้งให้ทราบล่วงหน้าก่อนและหยุดชะงัก (แต่ต้องดำเนินการตามขั้นตอนต่อไป)

และเมื่อพิจารณาถึงอำนาจหน้าที่ ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ที่ได้มีการแก้ไขเพิ่มเติมในฉบับใหม่ (Loi n°2018-493 on the Protection of Personal Data) แล้วจะเห็นได้ว่า มีการนำหลักการสำคัญที่ได้กำหนดใน GDPR มาบัญญัติไว้ โดยได้มีการแก้ไขเพิ่มเติมให้องค์กร CNIL มีอำนาจที่กว้างขวางขึ้นโดยมีการกำหนดเสริมบทบาทขององค์กรที่ทำหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Reinforced Role of the Data Protection Authority) โดย CNIL ได้รับอำนาจเพิ่มขึ้นในการกำกับดูแล ดังจะเห็นได้จากการกำหนดให้เจ้าหน้าที่ของ CNIL สามารถเข้าตรวจสอบสถานที่ควบคุมและเก็บรักษาข้อมูลได้และอาจขอเอกสารทั้งหมดและข้อมูลที่เป็นประโยชน์หรือเหตุผลที่จำเป็นสำหรับการตรวจสอบ และการเปลี่ยนแปลงที่สำคัญที่สุดประการหนึ่งคือการให้อำนาจสืบสวนทางออนไลน์ที่เพิ่มขึ้นมาใหม่[187]

นอกจากนี้ยังมีการกำหนดให้อำนาจแก่ CNIL ในการขอระงับการโอนย้ายข้อมูลระหว่างประเทศชั่วคราว (Temporary Suspension of International Data Transfers at the Request of the CNIL) กล่าวคือ ในประเด็นเกี่ยวกับการถ่ายโอนข้อมูลระหว่างประเทศ ในกรณีที่เห็นว่ามีเหตุจำเป็นเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล CNIL สามารถยื่นคำร้องต่อศาลปกครองสูงสุดของฝรั่งเศส (Conseil d'État) เพื่อระงับการโอนย้ายชั่วคราวนอกเขตสหภาพยุโรปได้[188]

กล่าวโดยสรุปได้ว่า สำหรับประเทศฝรั่งเศสนั้น การคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลได้เริ่มตั้งต้นเป็นรูปธรรมขึ้นเมื่อมีการประกาศใช้รัฐบัญญัติที่ 78-17 ลงวันที่ 6 มกราคม ค.ศ.1978 ว่าด้วยข้อมูล สารสนเทศ แฟ้มข้อมูล และเสรีภาพ (Loi relative à l'informatique, aux fichiers et aux libertès หรือ The Act on Data Processing Data Files and Individual Liberties) ซึ่งเป็นจุดเริ่มต้นของกฎหมายที่มีลักษณะของการวางหลักการทั่วไปเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล และได้มีการจัดตั้งองค์กรสำคัญขึ้นมาทำ

---

[187] Olivier Proust and Julien-Alexis Defromont, *op. cit.*

[188] *Ibid.*

หน้าที่ปกป้องคุ้มครองสิทธินี้ให้เกิดขึ้นตามความเป็นจริง ซึ่งก็คือ องค์กร CNIL นั่นเอง แต่อย่างไรก็ดี ภายใต้กฎหมายฉบับนี้ เป็นกฎหมายที่ถูกสร้างและพัฒนาขึ้นมาบนพื้นฐานของสถานการณ์ที่เริ่มมีการนำเครื่องคอมพิวเตอร์เข้ามาใช้ในมิติต่าง ๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลทั้งในระบบราชการและภาคเอกชน เมื่อต่อมาคอมพิวเตอร์ได้มีการพัฒนาและมีศักยภาพในการเชื่อมโยงมากขึ้นและความแพร่หลายของอินเทอร์เน็ตก็มีมากขึ้นประเทศฝรั่งเศสก็ได้มีการพัฒนากฎหมายคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลอย่างมีนัยสำคัญอีกครั้ง ก็คือการตรา รัฐบัญญัติสาธารณรัฐดิจิตอล (The French Digital Republic Act (Loi n°2016-1321 pour une République numérique)) เพื่อควบคุมกำกับเศรษฐกิจดิจิตอลในภาพรวม และมีส่วนในการพัฒนาหลักการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลมากขึ้นโดยเฉพาะในประเด็นของการเปิดเผยข้อมูลส่วนบุคคล มีการยกระดับของสิทธิของเจ้าของข้อมูลส่วนบุคคลในประการสำคัญคือ ผู้ใดจะนำของมูลของเจ้าของข้อมูลไปใช้ จะต้องได้รับความยินยอมจากเจ้าของข้อมูลเสมอเว้นแต่มีเหตุผลอันยอมรับได้ นอกจากนี้ยังให้ความสำคัญกับการเพิ่มความลับในการสื่อสาร และกำหนดสิทธิต่าง ๆ มากมายให้แก่เจ้าของข้อมูลส่วนบุคคล และมีการเพิ่มเติมอำนาจให้แก่ CNIL ในการที่จะเข้ามาทำหน้าที่ปกป้องคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลอีกด้วย จนกระทั่งถึงปัจจุบัน เมื่อมีการประการใช้ General Data Protection Regulation โดยสหภาพยุโรป ประเทศฝรั่งเศสก็ได้ยอมรับเอาหลักการคุ้มครองสิทธิตามกติกาสากลฉบับนี้มาบังคับในประเทศของตนและบังคับแก่ข้อมูลส่วนบุคคลของพลเมืองของตนไม่ว่าอยู่ ณ ที่ใดในโลก ทำให้การคุ้มครองข้อมูลส่วนบุคคลของพลเมืองฝรั่งเศสยกระดับมาตรฐานขึ้นไปเทียบเท่ากับหลักการของ GDPR ดังที่ได้กล่าวไว้แล้วในตอนต้น

3.5 การคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศเยอรมนี

3.5.1 แนวคิดและวิวัฒนาการในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศเยอรมนี

3.5.1.1 ความหมายของข้อมูลส่วนบุคคลของประเทศเยอรมนี

กฎหมายของประเทศเยอรมนีที่ถูกตราขึ้นมาเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนั้น มีชื่อว่า “กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล” (Bundesdatanschutzgesetz: BDSG) ซึ่งถูกตราขึ้นมาโดยมีวัตถุประสงค์เพื่อคุ้มครองข้อมูลส่วนบุคคล โดยครอบคลุมไปถึงการเก็บรวมรวม การประมวลผล และการใช้ ทั้งในส่วนข้อมูลส่วนบุคคลที่ใช้โดยหน่วยงานของรัฐ และข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานภาคเอกชนซึ่งมี

ไว้เพื่อวัตถุประสงค์ในทางอาชีพหรือในทางธุรกิจ โดยหลักการในการที่จะใช้ประโยชน์จากข้อมูลส่วนบุคคลดังกล่าวจะต้องเป็นไปตามกฎหมายฉบับนี้อนุญาตหรือมีกฎหมายฉบับอื่นอนุญาตให้กระทำได้เท่านั้น[189]

สำหรับความหมายของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนั้น กฎหมายว่าด้วยการคุ้มครองข้อมูล (BDSG) ได้รับรองโดยกำหนดนิยามของคำว่า “ข้อมูลส่วนบุคคล” ไว้ในมาตรา 3 ว่าหมายถึง ข้อมูลอันใดอันหนึ่งที่เกี่ยวกับเรื่องส่วนบุคคลของบุคคลธรรมดาบุคคลใดบุคคลหนึ่ง หรือบุคคลธรรมดาที่อาจระบุตัวได้”

นอกจากความหมายตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลแล้ว ในกฎหมายวิธีปฏิบัติราชการทางปกครอง (Verwaltungsverfahrensgesetz: VwVfg) มาตรา 30 ยังได้กำหนดนิยามของ “ข้อมูลส่วนบุคคล” ว่าหมายรวมถึงข้อมูลส่วนบุคคลอื่น ๆ เช่น ข้อมูลเกี่ยวกับความสัมพันธ์ภายในครอบครัว ข้อมูลเกี่ยวกับเรื่องทรัพย์สินและภาษีของบุคคล ข้อมูลเกี่ยวกับความลับในทางธุรกิจต่าง ๆ ฯลฯ เป็นต้น[190]

3.5.1.2 สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในฐานะสิทธิขั้นพื้นฐาน

ตามหลักการของรัฐธรรมนูญเยอรมนี (Basic Law หรือ Grundgesetz) ถือว่า สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล เป็นสิทธิส่วนบุคคล (Personlichkeitsrecht) อันเป็นสิทธิขั้นพื้นฐาน (Grundrechte) ที่ได้รับการรับรองและคุ้มครองแก่ปัจเจกบุคคลโดยบทบัญญัติของรัฐธรรมนูญ โดยได้กำหนดห้ามมิให้มีการเข้าไปแทรกแซงสิทธิในความเป็นส่วนตัวของบุคคลใด ๆ ไม่ว่าจะเป็นกรณีจดหมาย หรือวัตถุทางไปรษณีย์ และการติดต่อสื่อสาร อย่างไรก็ดี การจะจำกัดสิทธิในความเป็นส่วนตัวนี้ จะกระทำได้ภายใต้บทบัญญัติของกฎหมายบนพื้นฐานเพื่อประโยชน์สาธารณะเท่านั้น

การกำหนดรับรองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศเยอรมนีจึงเป็นการกำหนดประเภทของสิทธินี้ให้อยู่ในกลุ่มของ status negativus อันถือเป็นสิทธิของปัจเจกบุคคลที่จะต้องปราศจากการแทรกแซงใด ๆ ของรัฐรวมถึงบุคคลอื่น ซึ่งเมื่อพิจารณาถึงพื้นฐานของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนี้จะเห็นได้ว่าสิทธินี้มีภารกิจของสิทธิและเสรีภาพในฐานะทำหน้าที่ในการป้องกัน (Abwehrfunktion)[191] อันเป็นการก่อให้เกิดสิทธิในการป้องกันตนเองของปัจเจกบุคคลต่อการแทรกแซง โดยมีความมุ่งหมายเพื่อให้เกิดความมั่งคงหรือ

---

[189] กิตติพงศ์ กมลธรรมวงศ์, *เรื่องเดิม*, หน้า 189.

[190] *เรื่องเดียวกัน*, หน้า 190.

[191] บรรเจิด สิงคะเนติ, *เรื่องเดิม*, หน้า 56.

หลักประกันต่อเสรีภาพ อันจะเกิดผลให้บุคคลผู้ได้รับผลกระทบจากการแทรกแซงสามารถเรียกร้องให้มีการระงับยับยั้งการแทรกแซงสิทธิขั้นพื้นฐานที่ได้รับความคุ้มครอง

3.5.1.3 วิวัฒนาการในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในประเทศเยอรมนี

ในช่วงต้นทศวรรษที่ 1960 แนวคิดในการปกป้องข้อมูลส่วนบุคคลอันเนื่องมาจากพัฒนาการของความก้าวหน้าทางเทคโนโลยีได้เริ่มมีขึ้นในประเทศสหรัฐอเมริกา ดังนั้นจำเป็นต้องมีการเสนอกรอบการกำกับดูแลเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล แนวความคิดนี้ได้มีอิทธิพลมาถึงประเทศเยอรมนี

วิวัฒนาการของการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในประเทศเยอรมนีเกิดขึ้นเป็นครั้งแรก โดยมีการตราเป็นกฎหมายระดับมลรัฐ (State Law) โดยเกิดขึ้นในรัฐเอสเซน (Hessen) ในปี 1970 ซึ่งถือเป็นกฎหมายที่คุ้มครองข้อมูลส่วนบุคคลฉบับแรกของโลก[192] หลังจากนั้นก็ได้มีการตรากฎหมายของรัฐบาลกลางออกมาเพื่อบังคับใช้ในระดับประเทศ โดยมีการเสนอร่างพระราชบัญญัติร่างแรก ในปี ค.ศ.1971 จนกระทั่งวันที่ 1 ม.ค. 1978 กฎหมายจึงมีผลใช้บังคับ กฎหมายฉบับนี้ก็คือ “กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล” (Bundesdatanschutzgesetz: BDSG)

หลังจากกฎหมายมีผลใช้บังคับระยะหนึ่ง ก็ได้เกิดมีประเด็นใหม่จากคำตัดสินคดีการนับประชากร (Volkszaehlungsurteil des BvvrfG) ของศาลรัฐธรรมนูญแห่งสหพันธรัฐเกิดขึ้น กล่าวคือ สภานิติบัญญัติได้มีการออกกฎหมายฉบับใหม่ ที่มีชื่อว่า“กฎหมายว่าด้วยการนับประชากร” ทำให้เกิดภาวะของการพยายามเป็นอย่างมากของภาครัฐที่จะจัดเก็บข้อมูลส่วนบุคคลของประชาชน โดยมีลักษณะของการกระทำของรัฐที่ไม่แยกแยะว่าเป็นมิติการเมืองหรือสังคม และได้ก่อให้เกิดความหวาดกลัวในหมู่ประชาชนเกี่ยวกับการใช้คอมพิวเตอร์ จนเกิดกระแสประท้วงและต่อต้าน และได้มีการนำคดีขึ้นสู่การพิจารณาของศาลรัฐธรรมนูญ จนกระทั่งเมื่อวันที่ 15 ธันวาคม ค.ศ.1983 ศาลรัฐธรรมนูญได้ตัดสินวางหลักการถึงสิทธิในการตัดสินใจเหนือข้อมูลข่าวสาร (Right to Self-Determination of Information) (หลักการตามรัฐธรรมนูญมาตรา 1 และมาตรา 2) โดยคำตัดสินยืนยันว่าข้อมูลส่วนบุคคลนี้ได้รับการคุ้มครองตามรัฐธรรมนูญในเยอรมนี ซึ่งหมายความว่า บุคคลมีอำนาจในการตัดสินใจว่าจะเผยแพร่ข้อมูลส่วนบุคคลเมื่อใดและอย่างไรก็ได้[193] โดยการกระทำใด ๆ ของรัฐจะต้องเคารพสิทธินี้ของประชาชน รัฐจึงต้องเคารพการใช้ข้อมูลของประชาชนโดยจะต้องเน้นในเรื่องของการตรงต่อวัตถุประสงค์ ความรัดกุมของการใช้ข้อมูล และมีระบบการป้องกันข้อมูลที่ดี

---

[192] นคร เสรีรักษ์, *เรื่องเดิม*, หน้า 108.

[193] BVerfGE 65, 1 (41 ff.)

อันทำให้ต่อมาในปี ค.ศ.1990 สภานิติบัญญัติได้แก้ไขกฎหมายคุ้มครองข้อมูลใหม่ให้สอดคล้องกับหลักการตามคำวินิจฉัยของศาลรัฐธรรมนูญ

อย่างไรก็ดี ต่อมาเมื่อคณะรัฐมนตรีแห่งสหภาพยุโรปได้ประกาศใช้ the Data Protection Directive (The Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data หรือ EU Directive (95/46/EC) เมื่อวันที่ 24 ตุลาคม ค.ศ.1995 อันมีการบังคับให้หลักการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลตาม Directive จะต้องถูกเปลี่ยนเป็นกฎหมายภายในของประเทศสมาชิกภายในปี ค.ศ.1998 ส่งผลให้กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (Bundesdatanschutzgesetz: BDSG) ฉบับนี้ได้มีการทบทวนและแก้ไข และได้มีการทบทวนแก้ไขเรื่อยมาจนล่าสุดในปี 2010

ในเวลาต่อมาภายหลังจากที่สหภาพยุโรปได้ประกาศที่จะใช้ General Data Protection Regulation (GDPR) เพื่อแทนที่ EU Directive (95/46/EC) ในปี 2016 โดยจะให้มีผลบังคับใช้ในปี 2018 นั้น ประเทศเยอรมนีเป็นประเทศแรกที่ได้มีการดำเนินการตรากฎหมาย Federal Data Protection Act (BDSG) ฉบับใหม่ขึ้นใช้บังคับภายในของรัฐตน [194] ซึ่งประเด็นสำคัญที่น่าสนใจก็คือว่า GDPR นี้จะแทนที่กฎหมายของรัฐสมาชิกและโดยจะเหลือเพียงพื้นที่จำกัดสำหรับบทบัญญัติแห่งกฎหมายของประเทศเท่านั้น และเป็นที่น่าสังเกตว่าบทบัญญัติส่วนใหญ่ของ BDSG ที่อาจจะมีมาตรฐานการคุ้มครองสิทธิเกินขอบเขตของ GDPR จะส่งผลต่อข้อจำกัดในการปฏิบัติตามกฎหมายนี้ เนื่องจากศาลและเจ้าหน้าที่ของเยอรมันจะต้องไม่ใช้บทบัญญัติของ BDSG หากเห็นว่าขัดต่อกฎหมายยุโรป ซึ่งอย่างไรก็ดี BDSG ฉบับใหม่นี้ยังใช้บังคับกับภาคเอกชนรวมถึงภาครัฐ[195]

องค์ประกอบสำคัญอันโดดเด่นของกฎหมาย BDSG (Key Elements of BDSG) มีดังนี้คือ[196]

ประการแรก มีการกำหนดให้มีเจ้าหน้าที่เพื่อปกป้องข้อมูลส่วนบุคคล (Data protection officer) โดยกฎหมายของเยอรมันเกี่ยวกับหน้าที่ในการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูล

---

[194] Lennart Schüßler and Natallia Karniyevich, **Germany is the First EU Member State to Enact New Data Protection Act to Align with the GDPR** , Retrieved November 1, 2018 from https://www.twobirds.com/en/news/articles/2017/germany/germany-is-the-first-eu-member-state-to-enact-new-data-protection-act-to-align-with-the-gdpr

[195] Tatjana Zrinski, **EU GDPR vs. German Bundesdatenschutzgesetz – Similarities and Differences**, Retrieved November 1, 2018 from https://advisera.com/eugdpracademy/knowledgebase/eu-gdpr-vs-german-bundesdatenschutzgesetz-similarities-and-differences/

[196] *Ibid*.

ส่วนบุคคลเข้มงวดกว่าที่กำหนดไว้ในมาตรา 37 ของ GDPR ซึ่งตาม ตามมาตร 38 ของ BDSG บริษัทที่ดำเนินงานในประเทศเยอรมนี จะต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หากมีพนักงานอย่างน้อย 10 คน ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลโดยอัตโนมัติ

ประการที่สอง ในเรื่องค่าปรับนั้น ตามหลักการของ GDPR กำหนดค่าปรับซึ่งเป็นโทษทางปกครองสูง ถึง 20 ล้านยูโรหรือ 4 เปอร์เซ็นต์ของผลกำไรจากรายได้ทั่วโลก แต่การละเมิดที่เกี่ยวข้องกับข้อกำหนดเฉพาะตามกฎหมายของ BDSG จะถูกจำกัด ไว้ที่การปรับสูงสุด 50,000 ยูโร แต่สถานการณ์นี้จะเป็นเรื่องที่หาได้ยากในทางปฏิบัติและครอบคลุมเฉพาะกรณีที่เฉพาะเจาะจงมาก เช่น กรณีของการละเมิดต่อหน้าที่เกี่ยวกับข้อมูลสินเชื่อผู้บริโภค (Consumer Lones) สำหรับในกรณีอื่น ๆ จะมีการปรับค่าปรับสูงสุดตามที่ได้กำหนดโดย GDPR

ประการสุดท้าย คือ การกำหนดความเสียหายที่มิใช่ตัวเงิน กฎหมาย BDSG ใหม่นี้ได้มาการกำหนดความเสียหายที่มิใช่ตัวเงิน (Non-Monetary Damages) ซึ่งความเสียหายเหล่านี้ไม่สามารถคำนวณหรือวัดคุณค่าในการการเงินได้ เช่น การชดเชยความเจ็บปวดและความทุกข์ทรมานของเจ้าของข้อมูลในกรณีที่มีการล่วงละเมิดข้อมูลส่วนบุคคล กรณีเช่นนี้เจ้าของข้อมูลที่ถูกล่วงละเมิดอาจเรียกร้องค่าเสียหายจากความเสียหายที่มิใช่ตัวเงิน ซึ่งกรณีนี้เป็นความรับผิดใหม่ที่อาจส่งผลให้บริษัทและองค์กรธุรกิจ มีความเสี่ยงทางเศรษฐกิจเพิ่มขึ้นอย่างมาก

เมื่อพิจารณาถึงหลักการเพิ่มเติมของ BDSG ใหม่ซึ่งอยู่ภายใต้กรอบของ GDPR ประเมินได้ว่าองค์กรคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศเยอรมนีจะได้มีการตราแนวปฏิบัติ (Guidelines) ออกมาในอนาคต เพื่อให้ความเชื่อมั่นทางกฎหมายเกี่ยวกับการตีความและการบังคับใช้กฎหมายให้สูงขึ้น และแนวปฏิบัตินี้ควรได้รับการออกโดยคณะกรรมาธิการยุโรปเพื่อให้แน่ใจว่ามีการบังคับใช้และตีความข้อกำหนดของ GDPR อย่างเท่าเทียมกัน[197]

3.5.2 มาตรการทางกฎหมายในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศเยอรมนี

3.5.2.1 ลักษณะและประเภทของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลที่ได้รับความคุ้มครอง

สำหรับลักษณะและประเภทของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลได้มีการแบ่งแยกประเภทของข้อมูลส่วนบุคคลเป็น 2 ประเภท ดังนี้

---

[197] *Ibid.*

ข้อมูลส่วนบุคคล (Personal Data) หมายความว่า ข้อมูลที่เกี่ยวข้องกับบุคคลหรือรายละเอียดใด ๆ ที่สามารถระบุตัวบุคคล (เจ้าของข้อมูลได้) ประกอบด้วย

ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) หมายความว่า ข้อมูลส่วนบุคคลที่มีความอ่อนไหวต่อความรู้สึก ไม่ว่าจะเป็นข้อมูลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความเห็นทางการเมือง ความเชื่อทางศาสนา ลัทธิ ปรัชญา ความเป็นสมาชิกสหภาพแรงงาน สุขภาพและพฤติกรรมทางเพศ

สำหรับนิยามของข้อมูลส่วนบุคคลที่มีความอ่อนไหวนี้ ในกฎหมายที่ได้แก้ไขใหม่ที่ถูกตราขึ้นเพื่อให้สอดคล้องกับหลักการของ GDPR นั้น ได้มีการเพิ่มความหมายให้หมายรวมไปถึง ข้อข้อมูลไบโอเมตริกซ์และข้อมูลทางพันธุกรรมอีกด้วย[198]

3.5.2.2 หลักการและข้อจำกัดในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล

ซึ่งหลักการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนั้น มีหลักการตามกฎหมายดังนี้

ประการแรก การเก็บรวบรวม ใช้ และการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลที่ชอบด้วยกฎหมาย ได้แก่[199]

1. เป็นไปตามกฎหมายนี้หรือกฎหมายอื่นหรือได้รับความยินยอมจากผู้ทรงสิทธิ (The Data Subject) ซึ่งหมายถึงเจ้าของข้อมูลส่วนบุคคล

2. การเก็บรวมรวมข้อมูลโดยปราศจากความยินยอมให้ทำได้ในกรณี

   1) เป็นการปฏิบัติตามกฎหมาย

   2) เป็นอำนาจของฝ่ายปกครอง

   3) การเก็บข้อมูลจากผู้ทรงสิทธิฯ โดยตรงจะทำให้ข้อมูลไม่ถูกต้องและก่อความเสียหายแก่ผู้ทรงสิทธิ

3. เมื่อผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูล จะต้องแจ้งรายละเอียดดังต่อไปนี้ เว้นแต่ผู้ทรงสิทธิฯ จะทราบอยู่แล้ว

   1) ชื่อหรือสิ่งบอกให้รู้ว่า ผู้ควบคุมข้อมูลเป็นใคร

   2) วัตถุประสงค์ของการเก็บรวบรวม การใช้ และการดำเนินการ

   3) แหล่งที่มาของข้อมูลเฉพาะกรณีที่ผู้ทรงสิทธิฯ ไม่รู้ถึงการเปิดเผยข้อมูลนั้น

ประการที่สอง หลักความยินยอม มีสาระสำคัญดังนี้[200]

---

[198] Lennart Schüßler and Natallia Karniyevich, *op. cit.*

[199] นคร เสรีรักษ์, *เรื่องเดิม*, หน้า 108.

1. ความยินยอมต้องมาจากผู้ทรงสิทธิฯ ที่มีอิสระในการตัดสินใจ ซึ่งก่อนตัดสินใจผู้ทรงสิทธิฯ ย่อมขอทราบถึงวัตถุประสงค์ของการเก็บรวมรวม การใช้ และการดำเนินการได้ และความยินยอมจะต้องทำเป็นหนังสือ เว้นแต่จะมีสถานการณ์พิเศษอาจกระทำในรูปแบบอื่นที่เหมาะสมได้

2. ในกรณีของการวิจัยทางวิทยาศาสตร์ จะต้องแจ้งวัตถุประสงค์ของการวิจัยเป็นหนังสือด้วย

3. ในกรณีที่เป็นการเก็บรวมรวม การใช้ หรือการดำเนินการกับข้อมูลที่มีความอ่อนไหว การให้ความยินยอมจะต้องแสดงให้เห็นอย่างชัดแจ้ง

ประการที่สาม การเก็บรวมรวมข้อมูลที่มีความอ่อนไหว ที่ชอบด้วยกฎหมาย จะกระทำได้ต่อเมื่อ[201]

1. กฎหมายให้อำนาจ หรือ จำเป็นเพื่อป้องกันประโยชน์สาธารณะ

2. เจ้าของข้อมูลได้ให้ความยินยอมอย่างชัดแจ้ง

3. เพื่อป้องกันประโยชน์ของเจ้าของข้อมูลหรือบุคคลอื่น ในกรณีที่เจ้าของข้อมูลไม่สามารถให้ความยินยอมได้ ไม่ว่าโดยทางกายภาพหรือนิติกรรมตามกฎหมาย

4. ข้อมูลนั้นได้ถูกเปิดเผยต่อสาธารณะชนโดยเจ้าของข้อมูล

5. เป็นการเก็บรวมรวมข้อมูลเพื่อความปลอดภัยต่อสาธารณะ

6. มีความจำเป็นอย่างเร่งด่วนเพื่อป้องกันความไม่เป็นธรรมแก่ประโยชน์สาธารณะหรือประโยชน์อื่นใดที่เกี่ยวข้องกับเรื่องดังกล่าว

7. มีความจำเป็นเพื่อวัตถุประสงค์ทางการแพทย์ การวินิจฉัยโรค หรือเกี่ยวกับการดูแลรักษาหรือจัดการเกี่ยวกับการบริการทางด้านสุขภาพ หรือข้อมูลนั้นถูกประมวลโดยผู้ประกอบวิชาชีพทางการแพทย์หรือบุคคลอื่นใดที่มีหน้าที่รักษาความลับเทียบเท่ากับผู้ประกอบวิชาชีพทางการแพทย์

8. มีความจำเป็นเพื่อการวิจัยทางวิทยาศาสตร์ หรือเพื่อความสำเร็จในการวิจัยทางวิทยาศาสตร์ ซึ่งมีความจำเป็นอย่างมากที่ต้องใช้ข้อมูลนั้น หากไม่ได้มีการเก็บรวมรวมข้อมูลนั้นจะทำให้การวิจัยไม่ประสบความสำเร็จ และการวิจัยดังกล่าวได้ชั่งน้ำหนักกับผลประโยชน์ที่จะได้รับกับตัวเจ้าของข้อมูลแล้วจะเกิดประโยชนทางด้านวิทยาศาสตร์มากกว่า

9. รัฐมีเหตุจำเป็นต้องป้องกัน หรือทำให้บรรลุเกี่ยวกับการจัดการวิกฤติการณ์หรือความขัดแย้ง หรือการป้องกัน ที่เกี่ยวกับเรื่องของมนุษยชาติ

---

[200] *เรื่องเดียวกัน*.

[201] *เรื่องเดียวกัน*, หน้า 108.

นอกจากนี้ ในหลักกฎหมายที่ได้มีการแก้ไขเพิ่มเติมนั้น ยังได้มีการกำหนดข้อยกเว้นเพิ่มเติมในกรณีของการใช้ประโยชน์จากข้อมูลส่วนบุคคลที่มีความอ่อนไหว ว่าจะสามารถทำได้หากการประมวลผลเป็นสิ่งที่จำเป็นสำหรับวัตถุประสงค์ทางการแพทย์เชิงป้องกัน, การประเมินความสามารถในการทำงานของพนักงานในทางการแพทย์และสาธารณสุข ซึ่งการประมวลผลนี้จะต้องอยู่ภายใต้เงื่อนไขของหลักการของความลับในวิชาชีพแพทย์เพื่อประโยชน์สาธารณะในด้านสาธารณสุข ซึ่งการที่กำหนดเช่นนี้ เพื่อให้มั่นใจว่าการบริการด้านสุขภาพ การดำเนินการเกี่ยวกับเวชกรรมหรือทางการแพทย์จะมีคุณภาพและมีมาตรฐานด้านความปลอดภัยสำหรับประชาชน[202] การกำหนดข้อยกเว้นนี้เป็นไปตามที่หลักการของ GDPR ได้อนุญาต

3.5.2.3 กลไกทางกฎหมายในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล

ผู้ตรวจการด้านการคุ้มครองข้อมูลส่วนบุคคลแห่งสหพันธ์รัฐ (The Federal Commissioner for Data Protection and Freedom of Information (BfDI)) เป็นองค์กรอิสระของรัฐและเป็นองค์กรผู้เชี่ยวชาญในการบังคับการตามกฎหมาย ซึ่งมีอำนาจดังต่อไปนี้คือ[203]

1. ตรวจสอบดูแลการคุ้มครอง การเก็บ การใช้ หรือการประมวลผลข้อมูลของผู้ควบคุมข้อมูล นอกจากนี้ ยังมีอำนาจในการตรวจสอบเหนือองค์กรผู้ประกอบวิชาชีพ หน่วยงานพิเศษในการรักษาความลับของทางราชการ โดยเฉพาะอย่างยิ่งข้อมูลที่เป็นความลับภายใต้บทบัญญัติประมวลกฎหมายภาษีอากร
2. รับเรื่องร้องเรียนและสอบสวนการร้องเรียน
3. ให้คำแนะนำต่อคณะรัฐมนตรีและองค์กรอื่น ๆ ของรัฐ
4. จัดทำรายงานประจำปี

ตำแหน่งผู้ตรวจการด้านการคุ้มครองข้อมูลส่วนบุคคลแห่งสหพันธ์รัฐนี้ จะมีวาระดำรงตำแหน่งได้วาระละ 5 ปี และสามารถดำรงตำแหน่งได้ 2 วาระเท่านั้น

สำหรับการฝ่าฝืนกฎหมายเกี่ยวกับการปกป้องข้อมูลของเยอรมันอาจมีการลงโทษโดยกำหนดค่าปรับไม่เกิน 300,000 ยูโรต่อการละเมิด (โทษทางปกครอง) ในกรณีที่มีพฤติกรรมจงใจหรือดำเนินการเพื่อแลกกับผลประโยชน์ทางการเงิน (ความผิดอาญา) โดยจำคุกไม่เกิน 2 ปีหรือปรับขึ้นอยู่กับความรุนแรงของการละเมิด และอาจถูกริบผลกำไรที่เกิดจากการละเมิดการป้องกันข้อมูล[204]

---

[202] Lennart Schüßler and Natallia Karniyevich, *op. cit.*

[203] นคร เสรีรักษ์, *เรื่องเดิม*, หน้า 209-210.

[204] *เรื่องเดียวกัน*.

นอกจากนี้ ภายหลังจากที่ GDPR มีผลใช้บังคับแล้ว ตามหลักการของมาตรา 84 (1) ของ GDPR กำหนดให้ประเทศสมาชิกจะต้องกำหนดหลักเกณฑ์ในการลงโทษอื่น ๆ ที่ใช้กับการละเมิด GDPR โดยเฉพาะอย่างยิ่งกับการละเมิดที่ไม่อยู่ภายใต้การปรับค่าปรับทางปกครอง ทำให้กฎหมายเกี่ยวกับการปกป้องข้อมูลส่วนบุคคลที่ได้มีการตราขึ้นใหม่ ได้ระบุว่าการกระทำผิดโดยผู้กระทำโดยเจตนาหรือโดยประมาทไม่สามารถจัดการตามคำขอเกี่ยวกับข้อมูลส่วนบุคคลได้อย่างเหมาะสม (ตามสิทธิที่กำหนดใน GDPR และกฎหมาย) หรือไม่แจ้งให้ผู้บริโภคทราบอย่างเต็มที่และถูกต้อง รวมถึงดำเนินการภายในเวลาที่กำหนดไว้จะต้องถูกปรับเป็นเงิน 50,000 ยูโร[205] ซึ่งกรณีนี้จะมีการบังคับใช้อย่างจำกัดเป็นอย่างมาก ในกรณีอื่น ๆ ก็จะต้องบังคับตามโทษที่ได้กำหนดไว้ใน GDPR คือ กำหนดค่าปรับซึ่งเป็นโทษทางปกครองสูง ถึง 20 ล้านยูโรหรือ 4 เปอร์เซ็นต์ของผลกำไรจากรายได้ทั่วโลก

ซึ่งภายใต้หลักการของ GDPR และ BDSG ที่ได้ออกมาให้ทั้งสองฉบับ น่าจะมีผลให้การบังคับใช้กฎหมายเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลมีประสิทธิภาพและมีความเข้างวดในการบังคับใช้ รวมไปถึงการกำหนดอัตราโทษไว้ค่อนข้างสูงน่าจะทำให้การคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลมีผลในทางปฏิบัติมากยิ่งขึ้น

3.6 การคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศมาเลเซีย

3.6.1 แนวคิดและวิวัฒนาการในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศมาเลเซีย

3.6.1.1 ความหมายของข้อมูลส่วนบุคคลของประเทศมาเลเซีย

กฎหมายที่ตราขึ้นเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศมาเลเซีย มีชื่อว่า Personal Data Protection Act 2010 (PDPA) โดยในบทบัญญัติของกฎหมายฉบับนี้ มาตรา 4 ได้มีการกำหนดนิยามความหมายของคำว่าข้อมูลส่วนบุคคลไว้ดังนี้[206]

ข้อมูลส่วนบุคคล หมายความว่า ข้อมูลใด ๆ ที่เกี่ยวกับธุรกรรมในทางพาณิชย์ซึ่งถูกประมวลผลหรือถูกบันทึกหรือจัดเก็บไว้เพื่อการประมวลผล (Process) ซึ่งสามารถระบุตัวบุคคล หรือข้อมูลที่เมื่อนำไปประกอบกับข้อมูลอื่น ๆ ที่มีแล้วทำให้สามารถระบุตัวบุคคลได้

---

[205] Lennart Schüßler and Natallia Karniyevich, *op. cit.*

[206] DLA Piper, *op. cit.,* p. 97.

ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) หมายถึงข้อมูลส่วนบุคคลซึ่งได้แก่ ข้อมูลที่เกี่ยวของกับสุขภาพทั้งร่างกาย จิตใจ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนาหรือ ความเชื่ออื่น ๆ ที่มีลักษณะคลายคลึงกัน หรือข้อมูลอื่น ๆ ที่ คณะกรรมการข้อมูลส่วนบุคคลหรือรัฐมนตรีกระทรวงการสื่อสารและมัลติมีเดียประกาศให้เป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว ซึ่งข้อมูลประเภทนี้ได้รับการคุมครองมากกว่าข้อมูลส่วนบุคคลทั่วไป คือบุคคลไม่สามารถ ประมวลผลข้อมูลได้ หากไม่ได้รับความยินยอมอย่างชัดแจ้ง หรือมีความจำเป็นตามที่กำหนดไว้ใน มาตรา 40 (b) เช่น ความจำเป็นทางการแพทย์และเพื่อการดำเนินงานในกระบวนการยุติธรรม

3.6.1.2 สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในฐานะสิทธิขั้นพื้นฐาน

สิทธิในความเป็นส่วนตัวในฐานะเป็นสิทธิมนุษยชนขั้นพื้นฐานได้รับการยอมรับโดยกฎหมายของประเทศส่วนใหญ่ว่าเป็นคุณค่าพื้นฐานที่ต้องได้รับการปกป้อง ซึ่งตามระบบกฎหมายของแต่ละประเทศจะมีความแตกต่างกันไปในรูปแบบของการรับรองและคุ้มครองสิทธิ สำหรับประเทศมาเลเซียซึ่งใช้ระบบกฎหมายแบบคอมมอนลอว์อย่างอังกฤษ องค์กรศาลมักจะสร้างหลักการคุ้มครองเรื่อง "การบุกรุกความเป็นส่วนตัว (Invasion of Privacy) ในรูปของคำพิพากษา (Case Law) รวมถึงรัฐก็ได้ตราพระราชบัญญัติที่เป็นกฎหมายเฉพาะในการคุ้มครองสิทธินี้ซึ่งก็สอดคล้องตามรัฐธรรมนูญของประเทศมาเลเซีย (Malaysia's Constitution of 1957 with Amendments through 2007) ในหมวด 2 สิทธิเสรีภาพขั้นพื้นฐาน (Part II: Fundamental Liberties) ที่ได้มีการกำหนดว่า สิทธิในชีวิตและเสรีภาพส่วนบุคคลจะถูกลิดรอนไม่ได้ ทั้งนี้ให้เป็นไปตามที่กฎหมายบัญญัติ ซึ่งเสรีภาพส่วนบุคคลในความหมายของรัฐธรรมนูญนั้นหมายรวมถึงสิทธิในความเป็นส่วนตัวด้วย

3.6.1.3 วิวัฒนาการในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในประเทศมาเลเซีย

สำหรับในกลุ่มประเทศอาเซียนนั้น ประเทศมาเลเซียถือเป็นประเทศแรกที่ได้มีการประกาศใช้กฎหมาย Personal Data Protection Act 2010 (PDPA) ซึ่งเป็นกฎหมายที่บัญญัติขึ้นเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล โดยประกาศใช้เมื่อวันที่ 10 มิถุนายน ค.ศ.2010 กำหนดมีคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นผู้ดูแล (The Malaysain Personal Data Protection Commissioner) และกำหนดให้มีผลใช้บังคับอย่างสมบูรณ์ ในวันที่ 15 พฤศจิกายน ค.ศ.2013 (พ.ศ.2556) โดยมีวัตถุประสงค์สำคัญในการคุ้มครองส่วนบุคคลของประชาชน การจัดเก็บ การประมวลผลข้อมูลส่วนบุคคลที่ใช้ในธุรกรรมทางการค้า[207]

---

[207] กิตติพงศ์ กมลธรรมวงศ์ และคณะ, **โครงการศึกษาและพัฒนาแนวทางการคุ้มครองข้อมูลส่วนบุคคลภายใต้ประชาคมอาเซียน** (กรุงเทพมหานคร: สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์, 2558), หน้า 46.

ทั้งนี้การพัฒนากฎหมายคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศมาเลเซียนั้นเกิดจากความต้องการยกระดับในการพัฒนาประเทศ ซึ่งมาเลเซียได้เริ่มนโยบายเศรษฐกิจดิจิทัล ตั้งแต่ปี 2555 โดยการวางเป้าหมายให้นำนโยบายดังกล่าวมาประยุกต์ใช้ในสัดส่วนอย่างน้อย ร้อยละ 17 ของผลิตภัณฑ์มวลรวมภายในประเทศ (Gross Domestic Product: GDP) ของประเทศภายในปี 2563 เพื่อให้เกิดการใช้เทคโนโลยีเพื่อเข้ามาขับเคลื่อนในทุกมิติของสังคมและเศรษฐกิจ เชื่อมโยงมาเลเซียกับสังคมโลกได้อย่างรวดเร็ว อันนำไปสู่การยกระดับรายได้ประชาชาติ (Gross National Income: GNI) การพัฒนาศักยภาพในการแข่งขันและคุณภาพชีวิตที่ดีขึ้นของคนมาเลเซีย การปรับใช้นโยบายดังกล่าวของมาเลเซียสะท้อนอยู่ในมาตรการส่งเสริมการลงทุนธุรกิจเทคโนโลยีการสื่อสาร (ICT) ที่เรียกว่า Multi Media Super Corridor (MSC) นอกจากนี้รัฐบาลมาเลเซียได้ปรับปรุงสาธารณูปโภคพื้นฐานด้านเทคโนโลยีการสื่อสารให้ทันสมัย เทียบเท่ามาตรฐานสากล เพื่อรองรับการขยายตัวของเศรษฐกิจดิจิทัลอีกด้วย ซึ่งนอกจากมาตรฐานการดึงดูดการลงทุนจากต่างประเทศ รัฐบาลมาเลเซียยังคำนึงถึงพลวัตของข้อมูลในยุคโลกาภิวัตน์ซึ่งส่งผลกระทบต่อผู้บริโภคในสังคม จึงบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act 2010: PDPA) เพื่อป้องกันมิให้ผู้ประกอบการนำข้อมูลส่วนบุคคลของผู้บริโภคไปแสวงหาประโยชน์ในทางมิชอบ กฎหมายคุ้มครองข้อมูลส่วนบุคคลจึงมีเป้าหมายในการควบคุมการเก็บรวบรวม เก็บรักษา และเปิดเผยซึ่งข้อมูลส่วนบุคคลที่ได้จากกิจกรรมในเชิงพาณิชย์[208]

ดังนั้นจึงกล่าวได้ว่า เมื่อมาเลเซียมีการกำหนดนโยบายเศรษฐกิจดิจิทัลในการขับเคลื่อนเศรษฐกิจของประเทศ ย่อมมีผลให้การออกกฎหมายคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลจึงมีความสำคัญเป็นอย่างมาก โดยเฉพาะในการสร้างความมั่นใจให้แก่นักลงทุนรวมไปถึงผู้บริโภค และจะยังเพิ่มขีดความสามารถในการแข่งขันของประเทศในตลาดโลก ที่ย่อมจะต้องมีการเคลื่อนย้ายข้อมูลขนาดมหาศาลระหว่างประเทศ ซึ่งในกรณีนี้ทำให้ประเทศคู่ค้าโดยเฉพาะชาติตะวันตกไม่สามารถกีดกันผู้ประกอบการมาเลเซียเพื่อไม่ให้ประกอบกิจการในประเทศของตนหรือกำหนดมาตรกรอื่นในในลักษณะของการกีดกันทางการค้าโดยอ้างมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลได้อีกต่อไป

---

[208] ธนาคารอาคารสงเคราะห์, **หุ้นส่วนประเทศไทย: เศรษฐกิจดิจิตอลกับการพัฒนาดิจิตอลไทยแลนด์**, ค้นวันที่ 20 มีนาคม 2561 จาก http://library.baac.or.th/portal/news_detail.php?id=2934

3.6.2 มาตรการทางกฎหมายในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศมาเลเซีย

3.6.2.1 ลักษณะและประเภทของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลที่ได้รับความคุ้มครอง

จากนิยามของ ข้อมูลส่วนบุคคล ของประเทศมาเลเซียที่ให้ความสำคัญไปที่ข้อมูลในบริบทธุรกรรมทางการค้าที่ถูกประมวลผลหรือจัดเก็บไวเพื่อการประมวลผล (Process) ซึ่งสามารถระบุตัวบุคคล หรือ ข้อมูลที่เมื่อนำไปประกอบกับข้อมูลอื่น ๆ ที่มีแล้วสามารถระบุตัวบุคคลได้ และนิยามข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) ที่หมายถึง ข้อมูลส่วนบุคคลซึ่งประกอบไปด้วย ข้อมูลที่เกี่ยวของกับสุขภาพทั้งร่างกาย จิตใจ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนา หรือ ความเชื่ออื่น ๆ ที่มีลักษณะคล้ายคลึงกัน หรือข้อมูลอื่น ๆ ที่ คณะกรรมการข้อมูลสวนบุคคล (Personal Data Commissioner) หรือรัฐมนตรีจะประกาศให้เป็นข้อมูลส่วนบุคคลโดยเฉพาะ ซึ่งข้อมูลประเภทนี้ได้รับการคุ้มครองมากกว่าข้อมูลส่วนบุคคลทั่วไป คือ บุคคลไม่สามารถ ประมวลผลข้อมูลได้ หากไม่ได้รับความยินยอมอยางชัดแจ้ง หรือมีความจำเป็นตามที่กำหนดไว้ใน มาตรา 40 (b) เช่น ความจำเป็นทางการแพทย์และเพื่อการดำเนินงานในกระบวนการยุติธรรม ซึ่งเป็น ข้อยกเว้นด้านความจำเป็นที่แคบกว่ากรณีของข้อมูลส่วนบุคคลทั่วไป หรือข้อมูลนั้นถูกทำให้เป็นข้อมูลสาธารณะโดยเจตนาของเจ้าข้อมูลเอง กรณีเช่นนี้ ผู้กระทำความผิดจะต้องโทษปรับไม่เกิน 200,000 ริงกิต หรือโทษจำคุกไม่เกิน 2 ปี หรือทั้งจำทั้งปรับ[209]

3.6.2.2 หลักการและข้อจำกัดในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล

หลักการสำคัญของการคุ้มครองข้อมูลข่าวสารส่วนบุคคลในกฎหมายของมาเลเซียอยู่บนพื้นฐานของหลักการดังต่อไปนี้คือ

1. หลักทั่วไป (General)
2. หลักการแจ้งให้ทราบและทางเลือก (Notice and Choice)
3. หลักการเปิดเผย (Disclosure)
4. หลักการเก็บรักษา (Retention)
5. หลักความปลอดภัย (Security)
6. หลักการเข้าถึง (Access)
7. หลักความถูกต้องของข้อมูล (Data Integrity Principle)

---

[209] กิตติพงศ์ กมลธรรมวงศ์ และคณะ, *เรื่องเดิม*, หน้า 46.

จากหลักการข้างต้นนี้ ปรากฏในสาระสำคัญของกฎหมายคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศมาเลเซีย ซึ่งสรุปสาระสำคัญได้ดังนี้[210]

1. การเก็บ การใช้ และการเปิดเผยข้อมูล (Collection, Use and Discloser) มาตรา 6 กำหนดหลักการความยินยอมของเจ้าของข้อมูลส่วนบุคคลในการประมวลผลข้อมูล และกำหนดข้อยกเว้นในบางกรณี เช่น การประมวลผลข้อมูลเพื่อปฏิบัติตามสัญญา ที่ให้ไว้กับเจ้าของข้อมูลนั้นเอง มาตรา 7 กำหนดให้ผู้ใช้ข้อมูล (Data User) ต้องแจ้งเป็นลายลักษณอักษรถึงเจ้าของข้อมูลเมื่อมีการประมวลผลข้อมูล โดยระบุรายละเอียดเกี่ยวกับวัตถุประสงค์ แหล่งที่มาของข้อมูล สิทธิของเจ้าของข้อมูล ลักษณะของบุคคลอื่นที่อาจมีการเปิดเผยข้อมูล และทางเลือกที่เจ้าของข้อมูลสามารถจำกัดการประมวลผลข้อมูลได้ ซึ่งจะต้องแจ้งอย่างเร็วที่สุดเท่าที่สามารถทำได้ (As Soon as Practicable) เมื่อมีการเก็บข้อมูลเป็นครั้งแรก หรือเมื่อจะใช้ข้อมูลเพื่อวัตถุประสงค์อื่น ๆ ที่ไม่ได้แจ้งไว้ในครั้งแรก หรือเมื่อจะเปิดเผยข้อมูลไปยังบุคคลอื่น ซึ่งการแจ้งนี้ จะต้องเป็นไปอย่างชัดแจ้งและเข้าถึงได้โดยง่ายด้วย

2. การส่งข้อมูลไปต่างประเทศ (Transfer) มาตรา 129 กำหนดวางหลักห้ามส่งข้อมูลไปต่างประเทศ ยกเว้นสำหรับประเทศที่ รัฐมนตรีได้มีการออกประกาศตามคำแนะนำของคณะกรรมการข้อมูลส่วนบุคคล ว่ามีระดับมาตรฐานในการคุมครองข้อมูลส่วนบุคคล เช่นเดียวกับกฎหมายฉบับนี้ ยกเว้นในกรณีที่ได้รับความยินยอมจากเจ้าของข้อมูล หรือมีความจำเป็นต้องกระทำเพื่อผลประโยชน์ของเจ้าของข้อมูล หรือได้ดำเนินมาตรการเพื่อรับรองว่าข้อมูลนั้นจะไม่ถูกนำไปประมวลผลในลักษณะที่ผิดกฎหมาย อย่างไรก็ดีปัจจุบัน รัฐบาลมาเลเซียยังไม่ได้ออกประกาศรายชื่อของประเทศที่สามารถส่งข้อมูลไปได้ ดังนั้น ภาคธุรกิจจึงใช้หลักความยินยอมหรือดำเนินมาตรการอื่น ๆ เป็นการเฉพาะเรื่อง เพื่อรับประกันความปลอดภัยและความเป็นส่วนตัวของข้อมูลสวนบุคคล ทำให้เกิดมีเสียงสะท้อนจากภาคธุรกิจว่าควรจะมีการออกประกาศรายชื่อให้เร็วที่สุด เพื่อความคล่องตัวในการประกอบกิจกรรมทางธุรกิจข้ามพรมแดนที่เกี่ยวข้องกับการรับส่งข้อมูลส่วนบุคคล แต่อย่างไรก็ดี ทางฝ่ายคณะกรรมการข้อมูลส่วนบุคคล มีความเห็นว่าถึงแม้จะไม่มีรายชื่อที่ชัดเจน แต่ภาคธุรกิจก็สามารถดำเนินการส่งข้อมูลไปต่างประเทศได้โดยทำตามเงื่อนไขของมาตรา 129

3. การรักษาความปลอดภัยข้อมูล (Security) มาตรา 9 กำหนดให้ผู้ใช้ข้อมูล (Data User) ต้องจัดให้มีมาตรการในการรักษาความปลอดภัยข้อมูลส่วนบุคคลจากความเสียหาย การใช้ผิดวัตถุประสงค์ การปรับแต่ง การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรือจากการทำลายข้อมูล ในกรณีที่ให้บุคคลอื่นประมวลผลข้อมูลให้จะต้องมีมาตรการประกันความปลอดภัยของข้อมูลนั้นอย่างเพียงพอ

---

[210] *เรื่องเดียวกัน*, หน้า 49-50.

4. การเก็บรักษาข้อมูล (Retention) มาตรา 10 กำหนดให้เก็บรักษาข้อมูลไว้เท่าที่จำเป็นตามวัตถุประสงค์เท่านั้น และจะต้องทำลายข้อมูลเมื่อหมดความจำเป็นแล้ว ทั้งมาตรา 11 กำหนดให้ต้องดูแลและปรับปรุง ข้อมูลให้ถูกต้องอยู่เสมอ

5. การเข้าถึงข้อมูล (Access) มาตรา 12 กำหนดให้ต้องเปิดช่องทางให้เจ้าของข้อมูลเข้าถึงและสามารถแก้ไขข้อมูลให้ถูกต้องได้ หากได้รับการปฏิเสธอย่างไม่เป็นธรรมจากผู้ใช้ข้อมูล เจ้าของข้อมูลสามารถร้องเรียนหรือ ขอให้มีการตรวจสอบโดย Advisory Committee ได้

สำหรับข้อยกเว้นของกฎหมายปรากฏในส่วนของ Part III (มาตรา 45-46) กำหนดลักษณะการใช้งานข้อมูลที่ได้รับการยกเว้นไม่ต้องปฏิบัติตามหลักการบางประการของกฎหมายฉบับนี้ คือกรณีที่เป็นไปเพื่อการป้องกันอาชญากรรม การคำนวณภาษี เพื่อดำเนินงานในกระบวนการยุติธรรม การป้องกันอันตรายที่อาจเกิดขึ้นกับสุขภาพ ของผู้ป่วย การเก็บข้อมูลสถิติเพื่อการวิจัยในลักษณะที่ผลการวิจัยจะไม่ถูกเปิดเผยข้อมูลที่ระบุตัวตนได้ และการประมวลผลข้อมูลไปเพื่อวัตถุประสงค์ในเชิงวรรณกรรมและศิลปะ การสื่อสารมวลชน ทั้งนี้ เป็นการยกเว้นเฉพาะเมื่อหากการกิจกรรมต่าง ๆ ที่กล่าวมาไม่สามารถกระทำโดยสอดคลองกับหลักการต่าง ๆ ของกฎหมายนี้ได้เท่านั้น

มีข้อสังเกตที่น่าสนใจ 3 ประการเกี่ยวกับกฎหมายคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของมาเลเซียกล่าวคือ[211]

ประการแรก กฎหมายคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลจำกัดขอบเขตการบังคับใช้เฉพาะข้อมูลส่วนบุคคลที่เกี่ยวกับการทำธุรกรรมเชิงพาณิชย์ หมายความว่าข้อมูลส่วนบุคคลที่ถูกจัดเก็บโดยสถานศึกษาหรือองค์กรไม่แสวงหากำไร (Non-profit organization) จะไม่ได้รับการคุ้มครอง

ประการที่สอง การจัดเก็บข้อมูลส่วนบุคคลโดยหน่วยงานรัฐบาลกลางหรือรัฐบาลท้องถิ่นจะได้รับการยกเว้น ไม่ต้องปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล อันก่อให้เกิดความไม่ชัดเจนของขอบเขตการบังคับใช้ในกรณีรัฐวิสาหกิจ ที่รัฐเป็นผู้ประกอบกิจการในเชิงพาณิชย์ ซึ่งตามหลักการจะต้องอยู่ภายใต้บังคับของกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ประการสุดท้าย กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดหน้าที่ดูแลรักษาข้อมูลส่วนบุคคลแก่ผู้ใช้ข้อมูล (Data User) ซึ่งหมายถึง บุคคลที่เก็บรักษาข้อมูลส่วนบุคคล หรือมีอำนาจควบคุมหรืออนุญาตการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ของผู้ใช้ข้อมูล แม้ว่ากฎหมายจะไม่ได้กำหนดหน้าที่แก่ผู้ประมวลผลข้อมูล (Data Processor) ซึ่งเป็นลูกจ้างของผู้ใช้ข้อมูล แต่ถ้า

---

[211] ปภาวดี ธโนดมเดช, **มาเลเซียกับการคุ้มครองผู้บริโภคในยุค Digital Economy**, ค้นวันที่ 20 มีนาคม 2561 จาก http://www.itd.or.th/wp-content/uploads/2015/05/20150114-ar_malaysia-digi-economy.pdf

ผู้ประมวลผลข้อมูลนำข้อมูลที่เก็บรักษาโดยผู้ใช้ข้อมูลไปแสวงหาประโยชน์ในทางมิชอบ ผู้ประมวลผลข้อมูลก็จะมีสถานะเป็นผู้ใช้ข้อมูลซึ่งมีความรับผิดตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

แม้ว่ากฎหมายคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลไม่ได้ครอบคลุมการคุ้มครองข้อมูลส่วนบุคคลที่องค์กรของรัฐเป็นผู้จัดเก็บ แต่อย่างไรก็ดี กฎหมายฉบับนี้ก็สามารถสะท้อนแนวความคิดของประเทศมาเลเซียถึงปัญหาการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลที่จำเป็นต้องได้รับการคุ้มครองเป็นพิเศษ เนื่องจากความไม่เท่าเทียมกันในการรับรู้ข้อมูลระหว่างฝ่ายผู้ผลิตและผู้ให้บริการกับฝ่ายประชาชนซึ่งถือเป็นผู้บริโภค รวมถึงอำนาจต่อรองของประชาชนซึ่งเป็นผู้บริโภคที่มีน้อยกว่าผู้ประกอบการ อย่างไรก็ตาม กฎหมายฉบับดังกล่าวย่อมสร้างความกังวลให้กับผู้ประกอบการถึงอุปสรรคในการดำเนินธุรกิจและต้นทุนที่ย่อมจะเกิดมีขึ้นโดยผลของการบังคับใช้กฎหมาย ในกรณีที่ประชาชนซึ่งเป็นผู้บริโภคไม่ยินยอมในการเปิดเผยข้อมูลส่วนบุคคล แต่หากพิจารณาในอีกมุมหนึ่ง การที่ผู้ประกอบการเคารพและปฏิบัติตามกฎหมายอย่างเคร่งครัดย่อมแสดงถึงความซื่อสัตย์และความรับผิดชอบขององค์กรต่อสังคมในการดำเนินธุรกิจซึ่งจะสร้างความมั่นใจกับประชาชผู้บริโภครวมถึงประชาสังคมในภาพรวม

3.6.2.3 กลไกทางกฎหมายในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล

หน่วยงานที่รับผิดชอบตามกฎหมายในส่วน Part IV (มาตรา 47-60) ของกฎหมายฉบับนี้ได้กำหนดใหรัฐมนตรีแต่งตั้ง Personal Data Protection Commissioner เป็นผู้บังคับใช้กฎหมายนี้กับภาคเอกชน ให้คำปรึกษาแก่รัฐบาลในประเด็นนโยบายที่เกี่ยวของกับข้อมูลส่วนบุคคล รับการร้องเรียนจากประชาชนผู้ถูกละเมิดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล สืบสวนข้อเท็จจริง และเป็นผู้แทนของรัฐบาลมาเลเซียในความร่วมมือเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในระดับระหว่างประเทศด้วย โดยมี Personal Data Protection Advisory Committee (บัญญัติใน Part VI) คอยทำหน้าที่ให้คำปรึกษา แต่คำปรึกษานั้นไม่ผูกพัน Commissioner และหากบุคคลได้รับความเดือดร้อนจากการวินิจฉัยหรือการใช้อำนาจของ Commissioner เช่น การออกใบรับรองหน่วยงานผู้ใช้ข้อมูล หรือ การปฏิเสธข้อร้องเรียนของเจ้าของข้อมูล บุคคลนั้นสามารถฟ้องร้องต่อ Appeal Tribunal ได้ ซึ่งหน้าที่สำคัญอีกประการของ Commissioner คือการจัดให้มีการขึ้นทะเบียนผู้ใช้ข้อมูลบางประเภท และออกใบรับรอง (Certificate of Registration) ตามมาตรา 13-20 โดยเฉพาะองค์กรที่เกี่ยวข้องกับการสื่อสาร ธนาคารและสถาบันทางการเงิน ธุรกิจประกันภัย ธุรกิจที่เกี่ยวข้องกับสุขภาพ การศึกษา การขายตรง ในการนี้ Commissioner อาจปฏิเสธคำร้องขอขึ้นทะเบียน เพิกถอนใบรับรอง หรือไม่ต่อใบรับรอง ในกรณีที่เอกสารไม่ครบหรือผู้ใช้ข้อมูล (Data User) ไม่ปฏิบัติ ตามกฎหมายฉบับนี้ ซึ่งในทางปฏิบัติแล้ว แทบทุกบริษัทที่มีการเก็บข้อมูลส่วนบุคคลไปใช้เพื่อการทำธุรกรรมทางการค้าจำเป็นจะต้องขึ้นทะเบียน ซึ่งจะเห็นว่าองค์กรด้านการเงิน เช่น

Maybank เป็นหน่วยงานแรก ๆ ที่ยื่นเอกสารคำร้องขอขึ้นทะเบียน นอกจากนี้ยังอาจมีการขึ้นทะเบียน Data User Rorum ซึ่งเป็นการรวมกลุ่มระหว่าง ผู้ใช้ข้อมูลประเภทเดียวกันเพื่อจัดทำ Code of Practice ตามลักษณะของการใช้งานข้อมูลของแต่ละหน่วยงานและเสนอให้ Commissioner รับรอง ซึ่งวิธีการนี้จะทำให้เกิดการนำหลักการที่ระบุไว้ในกฎหมายฉบับนี้ไปใช้ในทางปฏิบัติอย่างเป็นรูปธรรมและสอดคลองกับลักษณะข้อมูลและธรรมชาติของธุรกิจนั้น ๆ [212]

จากที่กล่าวมาในบทนี้ทั้งหมด จะเห็นภาพของมาตรการและกลไกในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของต่างประเทศ ซึ่งในภาพรวมจะเห็นว่าสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนั้นถือว่าเป็นสิทธิขั้นพื้นฐานที่รัฐธรรมนูญของแต่ละประเทศรับรองและคุ้มครองให้แก่ประชาชน และแต่ละประเทศก็จะมีการตรากฎหมายในระดับพระราชบัญญัติออกมาเพื่อคุ้มครองสิทธินี้ ไม่ว่าจะตราออกมาในรูปแบบของกฎหมายบทกฎหมายทั่วไป (Comprehensive Laws) หรือบทกฎหมายเฉพาะ (Sectoral Laws) ก็ตาม แต่จะพบว่ากฎหมายของแทบทุกประเทศจะมีการกำหนดนิยามของคำว่าข้อมูลส่วนบุคคลไว้ เพื่อเป็นฐานในการกำหนดสิทธิตามกฎหมายอันจะมีผลต่อการกำหนดมาตรการและกลไกในการคุ้มครอง แต่อย่างไรก็ดีสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนี้ไม่ได้มีฐานะเป็นสิทธิโดยเด็ดขาด ดังนั้น ภายใต้หลักการเรื่องประโยชน์สาธารณะแล้วจะเห็นว่ารัฐทุกรัฐสามารถออกมาตรการมาจำกัดสิทธินี้ได้ แต่จะต้องอยู่ภายใต้หลักความได้สัดส่วน นอกจากนี้ ในปัจจุบันการที่สหภาพยุโรปได้ตรา GDPR ออกมาให้มีผลบังคับใช้ในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนั้น ได้มีผลกระทบต่อหลักการในการคุ้มครองตามกฎหมายภายในของประเทศต่าง ๆ ให้ต้องมีการปรับปรุงแก้ไขหลักการตามกฎหมายภายในให้มีมาตรฐานของการคุ้มครองไม่ด้อยไปกว่าหลักการของ GDPR นั่นเอง โดยจากหลักการที่กล่าวมานี้ เมื่อพิจารณาเปรียบเทียบกับสถานการณ์ในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลรวมถึงกฎหมายที่เกี่ยวข้องกับการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศไทยแล้วถือเป็นประเด็นที่น่าสนใจว่าประเทศไทยจะดำเนินการปรับปรุงมาตรการและกลไกอย่างไรเพื่อให้มีมาตรฐานทัดเทียมกับนานาอารยประเทศอันจะได้กล่าวในบทต่อ ๆ ไป

---

[212] *เรื่องเดียวกัน*, หน้า 48-49.

บทที่ 4

การคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในประเทศไทย

ในบทนี้จะได้อธิบายถึงสภาพของการรับรองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในประเทศไทย ซึ่งจะแสดงให้เห็นประเด็นสำคัญไม่ว่าจะเป็นเรื่องของแนวคิด นิยามความหมายและขอบเขตของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล มาตรการและองค์กรที่เป็นกลไกในการทำหน้าที่คุ้มครองสิทธิ รวมไปถึงระบบในการเยียวยาผู้ที่ถูกละเมิดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ซึ่งรายละเอียดมีดังนี้คือ

4.1 แนวคิดของการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในระบบกฎหมายของไทย

แนวความคิดของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนั้น จะเห็นว่ามุมมองของประเทศไทยกับต่างประเทศมีการให้ความสำคัญแตกต่างกัน ซึ่งในประเด็นนี้จึงมีผลให้พัฒนาการของการตรากฎหมายเฉพาะขึ้นมาคุ้มครองสิทธิจึงมีความล่าช้าเป็นอย่างมากเมื่อเปรียบเทียบกับนานาอารยประเทศ รวมถึงประเทศเพื่อนบ้านในอาเซียนอย่างมาเลเซีย ฟิลิปปินส์ และสิงคโปร์ ที่ได้มีการออกกฎหมายมาคุ้มครองสิทธินี้เป็นที่เรียบร้อยนานมาแล้ว ในขณะที่ประเทศไทยกฎหมายนั้นเพิ่งได้ตราผ่านทางรัฐสภาไม่นานมานี้เอง

ต้องยอมรับว่าแนวคิดในเรื่องสิทธิในความเป็นส่วนตัวยังต้องถือว่าเป็นเรื่องใหม่สำหรับสังคมไทย แต่สำหรับประเทศตะวันตกที่มีการปกครองในระบอบประชาธิปไตยมาอย่างยาวนานนั้นจะมีการให้ความสำคัญกับสิทธิในความเป็นส่วนตัวนี้เป็นอย่างมาก เพราะถือว่ามีฐานะเป็นสิทธิมนุษยชนอันเป็นหน้าที่สำคัญของรัฐประชาธิปไตยที่จะต้องมีหน้าที่ในการรับรองและคุ้มครองให้ ในฐานะที่เป็นมาตรฐานขั้นต่ำที่มนุษย์จะพึงมีและจะพึงได้รับ เพื่อการดำรงชีวิตที่มีคุณค่าและมีศักดิ์ศรีตั้งแต่เกิดจนกระทั่งถึงตาย สิทธินี้ถือเป็นสิทธิตามธรรมชาติอันปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ซึ่งแนวคิดนี้ถือว่าเป็นข้อผูกพันทางกฎหมายที่บรรดารัฐสมาชิกจะต้องปฏิบัติตาม และเราก็จะเห็นภาพของพัฒนาการของแนวคิดในการคุ้มครองสิทธิในความเป็นส่วนตัวที่ได้รับการนำไปบังคับใช้ทั้งในระดับ

องค์การระหว่างประเทศ ไม่ว่าจะเป็นองค์การเพื่อความร่วมมือและการพัฒนาทางเศรษฐกิจ (OECD), สหภาพยุโรป (EU), เอเปค (APEC) รวมไปถึงในระดับกฎหมายภายในของนานาอารยประเทศ

แนวคิดเรื่องการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลได้ยิ่งทวีความสำคัญมากยิ่งขึ้นในยุคที่มีการพัฒนาอย่างก้าวกระโดดในด้านเทคโนโลยีสารสนเทศ อันมีผลให้การติดต่อสื่อสารและการเผยแพร่ข้อมูลสามารถเชื่อมโยงกันได้โดยไม่จำกัดเวลาและสถานที่ อีกทั้งการประมวลผล การจัดเก็บหรือการเปิดเผยข้อมูลส่วนบุคคลนั้นสามารถกระทำได้โดยง่ายดายสะดวกและรวดเร็ว ก็ยิ่งมีผลทำให้สิทธิของปัจเจกชนสามารถถูกล่วงละเมิดได้โดยง่าย เราจึงจะเห็นว่านานาอารยประเทศที่มีแนวคิดในการคุ้มครองสิทธิมนุษยชนอย่างก้าวหน้าอยู่แล้ว ก็ได้ให้ความสำคัญและพัฒนาหลักกฎหมายเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลเพื่อป้องกันการแทรกแซงและล่วงละเมิด ซึ่งเมื่อย้อนมาพิจารณาแนวคิดนี้ในประเทศไทยของเราจะเห็นพัฒนาการของแนวคิดดังนี้

4.1.1 ช่วงระยะเวลาของการเริ่มต้นคุ้มครองโดยกฎหมายเอกชนและกฎหมายอาญา

ภายใต้ระบบกฎหมายของประเทศไทย ข้อมูลส่วนบุคคล (Personal Data) ถือเป็นวัตถุแห่งสิทธิในประเภทหนึ่งที่จัดรวมอยู่ในเรื่องสิทธิในความเป็นส่วนตัว (Right to Privacy) ซึ่งเรียกได้ว่าสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล (Right to Data Privacy) สำหรับสิทธินี้เมื่อพิจารณาเปรียบเทียบกับแนวคิดของต่างประเทศจะเห็นว่า มีพัฒนาการที่ไม่ยาวนานนักและมีข้อถกเถียงถึงขอบเขตและความหมายในระยะเวลาไม่นานมานี้ ทั้งนี้เป็นเพราะการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลที่ผ่านมาตกอยู่ภายใต้บริบทแห่งปริมณฑลของกฎหมายแพ่งและกฎหมายอาญาเสียมากว่าการคุ้มครองในฐานะเป็นสิทธิตามรัฐธรรมนูญซึ่งเราอาจเรียกได้ว่าเป็นการคุ้มครองแบบดั้งเดิม[213]

การคุ้มครองข้อมูลส่วนบุคคลเช่นนี้ มีลักษณะของการกำหนดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในลักษณะของการเป็นสิทธิในการป้องกัน หรือ Status Negativus อันมีลักษณะของการจัดกลุ่มของสิทธิและเสรีภาพที่การใช้สิทธิและเสรีภาพของปัจเจกบุคคลจะต้องปราศจากการเข้ามาแทรกแซงของรัฐหรือของบุคคลอื่น ถือเป็นสิทธิที่ผู้ทรงสิทธิสามารถเรียกร้องให้ผู้อื่นงดเว้นกระทำการที่ก้าวล่วงแดนแห่งสิทธิของตน และหากมีการกระทำอันเป็นการก้าวล่วงสิทธินี้แล้ว ผู้ทรงสิทธิสามารถใช้สิทธิเรียกร้องเอาจากผู้กระทำให้รับผิดชอบแก้ไขเยียวยาไม่ว่าจะเป็นในทางกฎหมายแพ่งหรือทางกฎหมายอาญา

---

[213] กิตติพงศ์ กมลธรรมวงศ์, *เรื่องเดิม*, หน้า 219

เมื่อวิเคราะห์ถึงการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลแบบดั้งเดิมก่อนที่จะมีการพัฒนาต่อมาโดยการบัญญัติรับรองหลักการของสิทธิไว้ในรัฐธรรมนูญหรือการตราเป็นบทบัญญัติของกฎหมายเฉพาะในปัจจุบันนั้น ต้องยอมรับว่าการคุ้มครองแบบดั้งเดิมนี้เป็นลักษณะเก่าแก่ซึ่งเป็นลักษณะพื้นฐานของระบบกฎหมายไทยที่มุ่งเน้นการคุ้มครองในลักษณะของ “การแก้ไขเยียวยา” เมื่อได้มีการล่วงละเมิดและเกิดความเสียหายเกิดขึ้นแก่สิทธิของผู้ทรงสิทธิแล้ว โดยหลักการสำคัญได้มีการบัญญัติไว้ในประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 420 และมาตรา 423[214] อันเป็นการกำหนดความรับผิดทางละเมิดในทางแพ่ง ซึ่งเป็นกรณีที่บุคคลหนึ่งได้ล่วงละเมิดสิทธิของบุคคลอื่นจนก่อให้เกิดความเสียหายต่อเกียรติยศชื่อเสียงหรือสิทธิอย่างหนึ่งอย่างใดที่เป็นประโยชน์ที่กฎหมายรับรองและคุ้มครองให้ ซึ่งสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลก็ถือว่าเป็นสิทธิอย่างหนึ่งอย่างใดที่เป็นประโยชน์ที่กฎหมายรับรองและคุ้มครองให้นั่นเอง โดยหลักเกณฑ์การพิจารณาว่าการกระทำใดจะเป็นการละเมิดหรือไม่ อาศัยการพิจารณาเช่นเดียวกับหลักการของประมวลกฎหมายแพ่งของประเทศฝรั่งเศส ที่จะต้องประกอบด้วยหลักเกณฑ์ 3 ประการคือ ประการแรก มีความเสียหายเกิดขึ้น (Prejudice) ประการที่สอง มีความผิด (Faute) และประการสุดท้ายคือมีความสัมพันธ์ระหว่างการกระทำและผลแห่งความผิด และความเสียหาย (Relation de cause a effet entre faute et la Prejudice)[215]

สำหรับการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ตามหลักการของกฎหมายอาญาก็จะปรากฏอยู่ใน หมวด 2 ความผิดเกี่ยวกับการเปิดเผยความลับ และหมวด 3 ความผิดเกี่ยวกับการหมิ่นประมาท สำหรับความผิดฐานเปิดเผยความลับนั้นได้มีการบัญญัติหลักการ

---

[214] มาตรา 420 แห่งประมวลกฎหมายแพ่งและพาณิชย์ ผู้ใดจงใจหรือประมาทเลินเล่อ ทำต่อบุคคลอื่นโดยผิดกฎหมายให้เขาเสียหายถึงแก่ชีวิตก็ดี แก่ร่างกายก็ดี อนามัยก็ดี เสรีภาพก็ดี ทรัพย์สินหรือสิทธิอย่างหนึ่งอย่างใดก็ดี ท่านว่าผู้นั้นทำละเมิดจำต้องใช้ค่าสินไหมทดแทนเพื่อการนั้น

มาตรา 423 แห่งประมวลกฎหมายแพ่งและพาณิชย์ ผู้ใดกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความอันฝ่าฝืนต่อความจริง เป็นที่เสียหายแก่ชื่อเสียงหรือเกียรติคุณของบุคคลอื่นก็ดี หรือเป็นที่เสียหายแก่ทางทำมาหาได้หรือทางเจริญของเขาโดยประการอื่นก็ดี ท่านว่าผู้นั้นจะต้องใช้ค่าสินไหมทดแทนให้แก่เขาเพื่อความเสียหายอย่างใด ๆ อันเกิดแต่การนั้น แม้ทั้งเมื่อตนมิได้รู้ว่าข้อความนั้นไม่จริง แต่หากควรจะรู้ได้

ผู้ใดส่งข่าวสารอันตนมิได้รู้ว่าเป็นความไม่จริง หากว่าตนเองหรือผู้รับข่าวสารนั้นมีทางได้เสียโดยชอบในการนั้นด้วยแล้ว ท่านว่าเพียงที่ส่งข่าวสารเช่นนั้นหาทำให้ผู้นั้นต้องรับผิดใช้ค่าสินไหมทดแทนไม่

[215] กิตติพงศ์ กมลธรรมวงศ์, *เรื่องเดิม*, หน้า 220.

ไว้ในมาตรา 322 – 323[216] ซึ่งเป็นประเด็นปัญหาที่เกิดขึ้นบ่อยครั้งสำหรับผู้ที่ประกอบวิชาชีพซึ่งมีหน้าที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่ตามปกติในทางปฏิบัติจะต้องมีการเปิดเผยข้อมูลส่วนบุคคลเพื่อประโยชน์ในทางวิชาชีพ เช่น เพื่อประโยชน์ในการรักษาทางการแพทย์ ที่หากมีการนำข้อมูลที่ล่วงรู้มาจากการประกอบวิชาชีพไปเปิดเผยย่อมเป็นการละเมิดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล[217] แต่หลักการตามมาตรา 323 นี้ยังมีปัญหาที่เป็นจุดบกพร่องที่อาจทำให้ไม่สามารถเอาผิดกับผู้ล่วงละเมิดก็คือ หากมีการนำข้อมูลไปเปิดเผยโดยความยินยอมของเจ้าของข้อมูลผู้กระทำก็จะไม่มีความผิด แม้ว่าการเปิดเผยข้อมูลนั้นจะก่อให้เกิดความเสียหายขึ้นในภายหลังก็ตาม[218]

ดังนั้นกล่าวได้ว่า การคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ภายใต้ระบบกฎหมายไทยแบบดั้งเดิมในอดีต เป็นการดำเนินการตามกรอบการคุ้มครองภายใต้กฎหมายว่าด้วยความรับผิดต่อความเสียหายต่อสิทธิส่วนตัว ซึ่งถือว่าได้รับการพิจารณาอยู่ในขอบเขตการคุ้มครองตามกฎหมายแพ่งและกฎหมายอาญาเป็นหลัก[219] ซึ่งการคุ้มครองสิทธิในความเป็นส่วนตัว

---

[216] มาตรา 322 แห่งประมวลกฎหมายอาญา ผู้ใดเปิดผนึกหรือเอาจดหมาย โทรเลข หรือเอกสารใด ๆ ซึ่งปิดผนึกของผู้อื่นไป เพื่อล่วงรู้ข้อความก็ดี เพื่อนำข้อความในจดหมายโทรเลขหรือเอกสารเช่นว่านั้นออกเปิดเผยก็ดี ถ้าการกระทำนั้นน่าจะเกิดความเสียหายแก่ผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 323 แห่งประมวลกฎหมายอาญา ผู้ใดล่วงรู้หรือได้มาซึ่งความลับของผู้อื่นโดยเหตุที่เป็นเจ้าพนักงานผู้มีหน้าที่ โดยเหตุที่ประกอบอาชีพเป็นแพทย์ เภสัชกร คนจำหน่ายยา นางผดุงครรภ์ ผู้พยาบาล นักบวช หมอความ ทนายความ หรือผู้สอบบัญชีหรือโดยเหตุที่เป็นผู้ช่วยในการประกอบอาชีพนั้นแล้วเปิดเผยความลับนั้นในประการที่น่าจะเกิดความเสียหายแก่ผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

ผู้รับการศึกษาอบรมในอาชีพดังกล่าวในวรรคแรก เปิดเผยความลับของผู้อื่น อันตนได้ล่วงรู้หรือได้มาในการศึกษาอบรมนั้น ในประการที่น่าจะเกิดความเสียหายแก่ผู้หนึ่งผู้ใด ต้องระวางโทษเช่นเดียวกัน

[217] วรรณรัชชา ทรัพย์รดาพัดชา, *เรื่องเดิม*, หน้า 114.

[218] กิตติพันธุ์ เกียรติสุนทร, **มาตรการทางอาญาในการคุ้มครองข้อมูลส่วนบุคคล** (วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2538), หน้า 34.

[219] นคร เสรีรักษ์, *เรื่องเดิม*, หน้า 244.

เกี่ยวกับข้อมูลส่วนบุคคลภายใต้บทบัญญัติของประมวลกฎหมายแพ่งและพาณิชย์และประมวลกฎหมายอาญาที่กล่าวมานั้น มีประเด็นปัญหาในการคุ้มครองดังนี้[220]

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

2. กฎหมายทั้งสองฉบับผลักภาระการพิสูจน์ให้แก่ผู้เสียหาย

3. กฎหมายทั้งสอบฉบับยังขาดบทบัญญัติเกี่ยวกับหลักเกณฑ์ วิธีการ เงื่อนไข และมาตรการที่จำเป็นและเฉพาะเจาะจงเพื่อให้หลักประกันในเรื่องนี้ได้อย่างเพียงพอตามหลักสากล

เมื่อพิจารณาถึงหลักการให้การคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลแบบดั้งเดิมตามหลักการของประมวลกฎหมายแพ่งและพาณิชย์และประมวลกฎหมายอาญาแล้ว จะเห็นว่า หลักการตามประมวลกฎหมายแพ่งและพาณิชย์แม้จะวางหลักการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในฐานะเป็นสิทธิอย่างหนึ่งอย่างใดที่เป็นประโยชน์ที่กฎหมายรับรองและคุ้มครองให้จากการถูกล่วงละเมิดก็ตาม แต่ก็มีลักษณะเป็นเพียงการคุ้มครองในลักษณะของการกำหนดวิธีการเยียวยาความเสียหาย โดยไม่ได้มีการกำหนดหลักการในเรื่องการเก็บรวบรวม การใช้หรือการเปิดเผยแต่อย่างใด มีเพียงแต่เจ้าของข้อมูลส่วนบุคคลผู้ถูกละเมิดสามารถเรียกร้องค่าเสียหายจากผู้เก็บรวมรวมข้อมูลโดยมิชอบหรือการเผยแพร่ข้อมูลอันทำให้เกิดความเสียหายในลักษณะของการละเมิดเท่านั้น นอกจากนี้ ในช่วงระยะเวลาที่ประเทศไทยยังไม่มีกฎหมายออกมาให้ความคุ้มครองสิทธิในข้อมูลส่วนบุคคลเป็นการทั่วไป ทำให้มีการล่วงละเมิดข้อมูลส่วนบุคคลในหลายมิติ โดยเฉพาะ

---

[220] จันทจิรา เอี่ยมมยุรา, กฎหมายเกี่ยวกับข้อมูลส่วนบุคคลในประเทศไทย, ใน **รายงานการวิจัยโครงการจัดทำความเห็นทางวิชาการเพื่อจัดทำรายงานเกี่ยวกับหลักเกณฑ์และแนวทางการพิจารณาและดำเนินการตามกฎหมายคุ้มครองข้อมูลข่าวสารส่วนบุคคล และจัดทำคู่มือการปฏิบัติงานเกี่ยวกับข้อมูลข่าวสารส่วนบุคคลภาครัฐตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ.2540** (กรุงเทพมหานคร: สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์, 2547), หน้า 6.

ข้อมูลส่วนบุคคลประเภทที่ยังไม่มีกฎหมายออกมารับรองไปถึงและเมื่อความคุ้มครองไม่อาจครอบคลุมไปถึงในทุกทุกมิติได้ การเยียวยาความเสียหายจึงไม่อาจเกิดขึ้นได้อย่างเป็นรูปธรรม กล่าวได้ว่า ความรับผิดทางแพ่งอันเกิดจากการล่วงละเมิดข้อมูลส่วนบุคคลย่อมไม่ครอบคลุมเพียงพอ ที่จะคุ้มครองเจ้าของข้อมูลส่วนบุคคลนั้น ภายใต้การคุ้มครองสิทธิตามแนวทางดั้งเดิมนี้ เมื่อเกิดการล่วงละเมิดข้อมูลส่วนบุคคลขึ้น เจ้าของข้อมูลส่วนบุคคลต้องนำเอาบทบัญญัติแห่งประมวลกฎหมายแพ่งและพาณิชย์เรื่องละเมิดมาปรับใช้ในการเยียวยาความเสียหาย ก็จะเป็นภาระแก่เจ้าของข้อมูลผู้เสียหายที่ต้องนำสืบพิสูจน์ถึงองค์ประกอบความผิดทางละเมิด และด้วยเหตุแห่งการพัฒนาอย่างมากในโลกแห่งเทคโนโลยีทำให้ปัจจุบันสามารถโอนถ่ายข้อมูลได้โดยง่าย จึงเป็นการยากที่เจ้าของข้อมูลผู้เสียหายจะนำสืบพิสูจน์การละเมิดต่อสิทธิส่วนบุคคลของตน

ในส่วนของกฎหมายอาญานั้น ด้วยเหตุที่กฎหมายอาญาเป็นกฎหมายที่มีลักษณะเป็นการกำหนดมาตรการปราบปรามผู้กระทำความผิด โดยแม้จะมีการบัญญัติฐานความผิดและกำหนดโทษแก่การล่วงรู้ข้อความในจดหมาย โทรเลข หรือเอกสารใด ๆ หรือการเผยแพร่ความลับ ซึ่งเป็นข้อมูลส่วนบุคคลก็ตาม แต่หากจะฟ้องร้องเพื่อเอาผิดกับผู้กระทำนั้นจะต้องเกิดการกระทำความผิดหรือเกิดความเสียหายจากกระทำความผิดขึ้นก่อน เช่นนี้ จะเห็นว่า เจ้าของข้อมูลส่วนบุคคลไม่สามารถจะดูแลปกป้องหรือควบคุมข้อมูลส่วนบุคคลของตนได้ โดยอาศัยหลักการของกฎหมายอาญา และนอกจากนี้ก็ไม่ได้มีการกำหนดบทบัญญัติที่กล่าวถึงการเก็บรวบรวมข้อมูล กล่าวคือ การเก็บรวบรวมข้อมูลส่วนบุคคล หากไม่ใช่กรณีตามประมวลกฎหมายอาญากำหนดไว้ ในมาตรา 322 ถึง มาตรา 324 ย่อมจะกระทำได้โดยไม่มีความผิดตามกฎหมายตราบเท่าที่ไม่ได้เป็นไปในลักษณะของการหมิ่นประมาทหรือกรณีที่อื่นที่มีการกำหนดไว้ให้เป็นความผิด

จึงกล่าวได้ว่า การคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลแบบดั้งเดิม โดยการอาศัยบทบัญญัติตามประมวลกฎหมายแพ่งและพาณิชย์ หรือประมวลกฎหมายอาญาย่อมไม่เหมาะสมที่จะทำให้สิทธินี้ได้รับความคุ้มครองอย่างแท้จริง ทั้งในมิติของการควบคุมการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคล แต่อย่างไรก็ดี การบัญญัติหลักการไว้ในกฎหมายทั้งสองฉบับนี้ก็ยังพอมีประโยชน์ในแง่ของการเป็นฐานอย่างกว้างในการเรียกร้องสิทธิในกรณีที่ไม่มีกฎหมายอื่นบัญญัติรับรองสิทธิไว้เลยหรือในกรณีที่หากมีบทกฎหมายเฉพาะบัญญัติรับรองสิทธิไว้แต่กำหนดหลักการครอบคลุมไปไม่ถึง

4.1.2 ช่วงระยะเวลาแห่งการสร้างกฎหมายมหาชนเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล

กฎหมายมหาชนเป็นกฎหมายที่กำหนดความสัมพันธ์ระหว่างรัฐไม่ว่าจะเป็นองค์กรของรัฐ หน่วยงานของรัฐ หรือเจ้าหน้าที่ของรัฐด้วยกันเอง หรือกำหนดความสัมพันธ์ระหว่างรัฐกับเอกชน ใน

ฐานะที่รัฐมีอำนาจเหนือกว่าในการที่จะรักษาความสงบเรียบร้อยให้กับสังคม ซึ่งกฎหมายฉบับใดก็ตามที่ตราออกมาให้อำนาจแก่รัฐเพื่อรักษาความสงบเรียบร้อยให้กับสังคมกฎหมายฉบับนั้นก็ย่อมมีฐานะเป็นกฎหมายมหาชน

ประเทศไทยก่อนการประกาศใช้รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช2540 นั้น กล่าวได้ว่า ไม่มีกฎหมายที่กำหนดให้ความคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลเป็นการเฉพาะ โดยกฎหมายที่มีอยู่ก็ได้แก่ ประมวลกฎหมายแพ่งและพาณิชย์ และประมวลกฎหมายอาญา ดั่งที่ได้กล่าวถึงแล้วในหัวข้อก่อนหน้า ซึ่งแม้จะมีบทบัญญัติคุ้มครองสิทธิของบุคคล เช่น เรื่องการทำละเมิด การหมิ่นประมาท และการเปิดเผยความลับของผู้อื่นไว้แล้วก็ตาม แต่ก็ยังไม่เพียงพอที่จะทำให้เกิดการคุ้มครองสิทธิอย่างเป็นระบบและมีประสิทธิภาพ ด้วยเหตุว่า การคุ้มครองแบบดั้งเดิมตามประมวลกฎหมายแพ่งและพาณิชย์และประมวลกฎหมายอาญา เป็นรูปแบบมาตรการเยียวยาเสียมากกว่าจะเป็นมาตรการป้องกันการล่วงละเมิดสิทธิ และโดยเฉพาะอย่างยิ่งหลักเกณฑ์ของกฎหมายทั้งสองนั้นเป็นการกำหนดให้มีขึ้นเพื่อคุ้มครองสิทธิเสรีภาพโดยทั่วไป ไม่ได้ออกแบบมาเพื่อคุ้มครองป้องกันสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลซึ่งมีธรรมชาติแตกต่างจากสิทธิประเภทอื่น ๆ โดยเฉพาะ[221]

ต่อมานับแต่ที่ประเทศไทยได้มีการปฏิรูปการเมืองครั้งสำคัญในบรรยากาศประชาธิปไตยและได้มีการประกาศใช้รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540 ก็ได้ส่งผลให้มีการตราพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ.2540 ออกมาใช้บังคับ ซึ่งกฎหมายฉบับนี้ถือเป็นกฎหมายมหาชนที่สำคัญที่ถูกตราขึ้นโดยมีเจตนารมณ์ดังนี้ คือ ประการแรกเพื่อให้ประชาชนได้รับรู้หรือได้ทราบข้อมูลข่าวสารเกี่ยวกับการดำเนินงานต่าง ๆ ของรัฐ เพื่อสามารถแสดงความคิดเห็นและใช้สิทธิทางการเมืองได้อย่างถูกต้อง รวมทั้งมีส่วนร่วมในกระบวนการการบริหารและตรวจสอบการใช้อำนาจรัฐ อันจะเป็นการส่งเสริมให้มีรัฐบาลที่บริหารบ้านเมืองอย่างมีประสิทธิภาพ โปร่งใส เป็นไปเพื่อประโยชน์ของประชาชนมากยิ่งขึ้น ประการที่สองเพื่อกำหนดหลักเกณฑ์เกี่ยวกับข้อมูลข่าวสารของราชการที่หากเปิดเผยและจะเกิดความเสียหายต่อประเทศชาติหรือต่อประโยชน์ที่สำคัญของเอกชน และประการที่สามเพื่อคุ้มครองการรุกล้ำสิทธิส่วนบุคคลในส่วนที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานรัฐ

ภายใต้หลักการของกฎหมายฉบับนี้ กล่าวได้ว่าเป็นกฎหมายที่ได้มีการเริ่มกำหนดนิยามของคำว่า “ข้อมูลส่วนบุคคล” เอาไว้[222] และได้มีการกำหนดหลักเกณฑ์การจัดการระบบข้อมูลส่วนบุคคล

---

[221] จันทจิรา เอี่ยมมยุรา, “การคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย,” **วารสารนิติศาสตร์,** หน้า 628.

[222] นคร เสรีรักษ์, *เรื่องเดิม*, หน้า 249.

ที่อยู่ในความครอบครองของรัฐเอาไว้ด้วย โดยในมาตรา 4 ของพระราชบัญญัติข้อมูลข่าวสารของทางราชการได้มีการบัญญัติไว้ดังนี้

> ข้อมูลข่าวสารส่วนบุคคล หมายความว่า ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะ การเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้นหรือมีเลขหมาย รหัส หรือ สิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่าย และให้หมายความ รวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย

สาระสำคัญของการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในกฎหมายฉบับนี้ ได้วางหลักการให้ต้องมีการจัดระบบข้อมูลส่วนบุคคลโดยอยู่บนพื้นฐานของความจำเป็นและต้องเก็บเพื่อการดำเนินงานของหน่วยงานรัฐให้สำเร็จตามวัตถุประสงค์ และเมื่อวัตถุประสงค์ได้สำเร็จแล้วจะต้องยกเลิกการจัดระบบข้อมูลดังกล่าวทันทีที่หมดความจำเป็น นอกจากนี้ จะต้องมีการตรวจสอบและแก้ไขข้อมูลข่าวสารส่วนบุคคลให้ถูกต้องอยู่เสมอ มีการจัดระบบรักษาความปลอดภัยให้แก่ข้อมูลเพื่อป้องกันมิให้มีการนำไปใช้โดยไม่เหมาะสมหรือเป็นผลร้ายต่อเจ้าของข้อมูล อีกทั้งในกรณีที่จะมีการเก็บข้อมูลข่าวสารโดยตรงจากเจ้าของข้อมูล หน่วยงานของรัฐจะต้องแจ้งให้เจ้าของข้อมูลทราบล่วงหน้าหรือพร้อมกับการขอข้อมูล และจะต้องแจ้งให้ทราบถึงกรณีที่จะมีการจัดส่งข้อมูลข่าวสารส่วนบุคคลไปยังที่ใด ๆ ซึ่งจะเป็นผลให้บุคคลทั่วไปทราบข้อมูลข่าวสารนั้น[223]

ภายใต้กฎหมายฉบับนี้ ผู้ทรงสิทธิในฐานะเจ้าของข้อมูลส่วนบุคคล (Data Subject) นั้นมีเพียง 2 ประเภทคือ บุคคลผู้มีสัญชาติไทย หรือ บุคคลที่มิได้มีสัญชาติไทย แต่ มีถิ่นที่อยู่ในประเทศไทย ตามหลักการของมาตรา 21 อันทำให้บุคคลสัญชาติไทยไม่ว่าจะมีถิ่นที่อยู่ในประเทศไทยหรือไม่ก็ตามสามารถใช้สิทธิเรียกร้องให้มีการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้ได้ แต่สำหรับบุคคลที่มิได้มีสัญชาติไทยจะกล่าวอ้างสิทธิ ประโยชน์ หรือความคุ้มครองตามพระราชบัญญัตินี้จะต้องเป็นผู้ที่มีถิ่นที่อยู่ในประเทศไทยเท่านั้น[224]

สำหรับประเด็นการจัดเก็บข้อมูลส่วนบุคคลนั้น หลักการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลตาม พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 กำหนดหน้าที่ให้หน่วยงานของรัฐจะต้องปฏิบัติตาม กล่าวคือ ในกรณีที่หน่วยงานของรัฐเก็บข้อมูลข่าวสารโดยตรงจาก

---

[223] มาตรา 23 แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540

[224] อธิพร สิทธิธีรรัตน์, *เรื่องเดิม*, หน้า 129.

เจ้าของข้อมูล หน่วยงานของรัฐต้องแจ้งให้เจ้าของข้อมูลทราบล่วงหน้าหรือพร้อมกับการขอข้อมูลถึงวัตถุประสงค์ที่จะนำข้อมูลมาใช้ลักษณะการใช้ข้อมูลตามปกติและกรณีที่ขอข้อมูลนั้นเป็นกรณีที่อาจให้ข้อมูลได้โดยความสมัครใจหรือเป็นกรณีมีกฎหมายบังคับ ซึ่งภายหลังจากการจัดเก็บแล้วหน่วยงานของรัฐจะต้องดำเนินการจัดการข้อมูลส่วนบุคคลตามหลักการดังนี้[225]

(1) ต้องจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลเพียงเท่าที่เกี่ยวข้องและจำเป็นเพื่อการดำเนินงานของหน่วยงานของรัฐให้สำเร็จตามวัตถุประสงค์เท่านั้น และยกเลิกการจัดให้มีระบบดังกล่าวเมื่อหมดความจำเป็น

(2) พยายามเก็บข้อมูลข่าวสารโดยตรงจากเจ้าของข้อมูลโดยเฉพาะอย่างยิ่งในกรณีที่จะกระทบถึงประโยชน์ได้เสียโดยตรงของบุคคลนั้น

(3) จัดให้มีการพิมพ์ในราชกิจจานุเบกษาและตรวจสอบแก้ไขให้ถูกต้องอยู่เสมอเกี่ยวกับสิ่งดังต่อไปนี้

(ก) ประเภทของบุคคลที่มีการเก็บข้อมูลไว้

(ข) ประเภทของระบบข้อมูลข่าวสารส่วนบุคคล

(ค) ลักษณะการใช้ข้อมูลตามปกติ

(ง) วิธีการขอตรวจดูข้อมูลข่าวสารของเจ้าของข้อมูล

(จ) วิธีการขอให้แก้ไขเปลี่ยนแปลงข้อมูล

(ฉ) แหล่งที่มาของข้อมูล

(4) ตรวจสอบแก้ไขข้อมูลข่าวสารส่วนบุคคลในความรับผิดชอบให้ถูกต้องอยู่เสมอ

(5) จัดระบบรักษาความปลอดภัยให้แก่ระบบข้อมูลข่าวสารส่วนบุคคลตามความเหมาะสมเพื่อป้องกันมิให้มีการนำไปใช้โดยไม่เหมาะสมหรือเป็นผลร้ายต่อเจ้าของข้อมูล

และหน่วยงานของรัฐต้องแจ้งให้เจ้าของข้อมูลทราบ ในกรณีที่มีการให้จัดส่งข้อมูลข่าวสารส่วนบุคคลไปยังที่ใดซึ่งจะเป็นผลให้บุคคลทั่วไปทราบข้อมูลข่าวสารนั้นได้ เว้นแต่เป็นไปตามลักษณะการใช้ข้อมูลตามปกติ

---

[225] มาตรา 23 แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540

สำหรับประเด็นการเปิดเผยข้อมูลส่วนบุคคลนั้น พระราชบัญญัติข้อมูลข่าวสารของราชการกำหนดหลักการไว้ว่า หน่วยงานของรัฐจะเปิดเผยข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความควบคุมดูแลของตนต่อหน่วยงานของรัฐแห่งอื่นหรือผู้อื่นโดยปราศจากความยินยอมเป็นหนังสือของเจ้าของข้อมูลที่ให้ไว้ล่วงหน้าหรือในขณะนั้นมิได้ เว้นแต่เป็นการเปิดเผย ในกรณีดังต่อไปนี้[226]

(1) ต่อเจ้าหน้าที่ของรัฐในหน่วยงานของตนเพื่อการนำไปใช้ตามอำนาจหน้าที่ของหน่วยงานของรัฐแห่งนั้น

(2) เป็นการใช้ข้อมูลตามปกติภายในวัตถุประสงค์ของการจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลนั้น

(3) ต่อหน่วยงานของรัฐที่ทำงานด้านการวางแผนหรือการสถิติหรือสำมะโนต่าง ๆ ซึ่งมีหน้าที่ต้องรักษาข้อมูลข่าวสารส่วนบุคคลไว้ไม่ให้เปิดเผยต่อไปยังผู้อื่น

(4) เป็นการให้เพื่อประโยชน์ในการศึกษาวิจัยโดยไม่ระบุชื่อหรือส่วนที่ทำให้รู้ว่าเป็นข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับบุคคลใด

(5) ต่อหอจดหมายเหตุแห่งชาติ กรมศิลปากร หรือหน่วยงานอื่นของรัฐเพื่อการตรวจดูคุณค่าในการเก็บรักษา

(6) ต่อเจ้าหน้าที่ของรัฐเพื่อการป้องกันการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย การสืบสวน การสอบสวน หรือการฟ้องคดี ไม่ว่าเป็นคดีประเภทใดก็ตาม

(7) เป็นการให้ซึ่งจำเป็นเพื่อการป้องกันหรือระงับอันตรายต่อชีวิตหรือสุขภาพของบุคคล

(8) ต่อศาลและเจ้าหน้าที่ของรัฐหรือหน่วยงานของรัฐหรือบุคคลที่มีอำนาจตามกฎหมายที่จะขอข้อเท็จจริงดังกล่าว

(9) กรณีอื่นตามที่กำหนดในพระราชกฤษฎีกา

จากที่กล่าวมาข้างต้นสรุปหลักการได้ว่า ห้ามหน่วยงานของรัฐเปิดเผยข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความควบคุมดูแลของตนต่อหน่วยงานของรัฐแห่งอื่นหรือผู้อื่นโดยปราศจากความยินยอม เว้นแต่ในกรณีที่เป็นไปเพื่อประโยชน์สาธารณะ ซึ่งหลักการนี้ก็สอดคล้องกับสภาพของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ที่ไม่ได้มีลักษณะของการเป็นสิทธิเด็ดขาด โดยรัฐสามารถออกมาตรการจำกัดสิทธินี้ได้ด้วยเหตุผลเพื่อประโยชน์สาธารณะ

---

[226] มาตรา 24 แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540

หากพิจารณาหลักการของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 นั้นจะพบว่ายังมีปัญหาในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลดังนี้คือ[227]

1. พระราชบัญญัติข้อมูลข่าวสารของราชการไม่ได้กำหนดคุ้มครองระบบการจัดเก็บและการใช้ข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานภาคเอกชน

2. แม้คณะกรรมการข้อมูลข่าวสารของราชการจะมีอำนาจควบคุมดูแลองค์กรประกอบวิชาชีพด้วย แต่ไม่ได้ครอบคลุมถึงอำนาจในการให้ความเห็นชอบประมวลหรือกฎเกณฑ์เกี่ยวกับจริยธรรมในวิชาชีพขององค์กรวิชาชีพที่จัดตั้งขึ้นตามกฎหมาย ในขณะที่กฎหมายของต่างประเทศที่ได้มีการพัฒนาใหม่ มักมีการกำหนดให้องค์กรที่ทำหน้าที่ควบคุมดูแลข้อมูลส่วนบุคคลมีอำนาจให้ความเห็นชอบประมวลจริยธรรมวิชาชีพที่องค์กรหรือหน่วยงานตามกฎหมายควบคุมวิชาชีพจัดทำขึ้นตามกฎหมายนั้น ๆ ด้วย

3. คณะกรรมการข้อมูลข่าวสารของทางราชการไม่มีอำนาจสืบสวนสอบสวนการกระทำที่ฝ่าฝืนการคุ้มครองข้อมูลส่วนบุคคล (Investigation Power) ตัวอย่างเช่นอำนาจของคณะกรรมการ ป.ป.ช. ในเรื่องทุจริตคอร์รัปชั่นในภาครัฐ

นอกจากนี้ ในแง่ของอำนาจจะเห็นได้ว่า คณะกรรมการข้อมูลข่าวสารมีเพียงอำนาจในการเรียกให้บุคคลมาให้ถ้อยคำหรือส่งวัตถุเอกสารหรือพยานหลักฐานมาประกอบการพิจารณาเท่านั้น ถ้าหากมีการฝ่าฝืนก็มีบทลงโทษก็มีเพียงระวางโทษจำคุก ไม่เกิน 3 เดือน หรือปรับไม่เกินห้าพันบาทหรือทั้งจำทั้งปรับเท่านั้น แต่ไม่มีบทลงโทษกรณีหน่วยงานรัฐฝ่าฝืนไม่ปฏิบัติตามกฎหมาย ซึ่งเมื่อพิจารณาจากความซับซ้อนและความเสียหายอันจะเกิดในกรณีเกี่ยวกับการล่วงละเมิดข้อมูลส่วนบุคคล อำนาจของคณะกรรมการข้อมูลข่าวสารของราชการดูจะไม่เพียงพอกับการคุ้มครองสิทธิเสรีภาพของประชาชนในปัจจุบัน[228]

---

[227] จันทจิรา เอี่ยมมยุรา, กฎหมายเกี่ยวกับข้อมูลส่วนบุคคลในประเทศไทย, ใน **รายงานการวิจัยโครงการจัดทำความเห็นทางวิชาการเพื่อจัดทำรายงานเกี่ยวกับหลักเกณฑ์และแนวทางการพิจารณาและดำเนินการตามกฎหมายคุ้มครองข้อมูลข่าวสารส่วนบุคคลและจัดทำคู่มือปฏิบัติงา เกี่ยวกับข้อมูลข่าวสารส่วนบุคคลภาครัฐตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540,** หน้า 9.

[228] นคร เสรีรักษ์, *เรื่องเดิม*, หน้า 254.

การตรากฎหมายขึ้นมาเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศไทยนั้น ไม่ได้มีการตราไว้ในกฎหมายฉบับเดียว แม้ว่าจะมีพระราชบัญญัติข้อมูลข่าวสารของทางราชการเป็นกฎหมายหลัก แต่ก็มีขอบเขตของการคุ้มครองที่จำกัดไม่ได้ครอบคลุมไปถึงข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของภาคเอกชนซึ่งมีปริมาณข้อมูลที่จัดเก็บเป็นจำนวนมากไม่น้อยไปกว่าข้อมูลที่อยู่กับภาครัฐ ไม่ว่าจะเป็นข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของบรรดาธนาคารเอกชน โรงพยาบาลเอกชน โรงแรม ห้างสรรพสินค้า หรือบรรษัทห้างร้านที่จำหน่ายสินค้า ผลิตภัณฑ์ หรือให้บริการที่มีการจัดเก็บข้อมูลของลูกค้าไว้ เมื่อพิจารณาประกอบกับความก้าวหน้าทางด้านเทคโนโลยีอันได้อธิบายมาแล้ว ก็จะทำให้เห็นถึงความเสี่ยงที่จะมีการล่วงละเมิดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลได้โดยง่าย โดยที่ระบบกฎหมายของไทยยังไม่สามารถให้ความคุ้มครองสิทธิได้อย่างมีประสิทธิภาพในช่วงระยะเวลานี้

แต่อย่างน้อยเราก็เห็นได้ถึงความพยายามของรัฐในอันที่จะใช้กฎหมายมหาชนเป็นเครื่องมือในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ซึ่งก็คือ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 ที่รับหลักการมาจากบทบัญญัติของรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540 มาตรา 34[229] และมาตรา 58[230] ซึ่งได้กำหนดหลักการคุ้มครองข้อมูลข่าวสารของบุคคลในฐานะที่เป็นส่วนหนึ่งของสิทธิส่วนบุคคลนั้นเอง

นอกจากพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ.2540 ประเทศไทยก็ยังได้มีการตรากฎหมายมหาชนที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลอีกหลายฉบับ แต่ฉบับที่สำคัญซึ่งควรกล่าวถึงจะมีอยู่ 3 ฉบับ ซึ่งก็คือ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544, พระราชบัญญัติว่าด้วยการประกอบธุรกิจข้อมูลบัตรเครดิต พ.ศ.2545 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ซึ่งสาระสำคัญของกฎหมายมหาชนทั้ง 3 ฉบับเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล สรุปได้ดังนี้

---

[229] มาตรา 34 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย (พ.ศ.2540) สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัวย่อมได้รับความคุ้มครอง

การกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชน อันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัวจะกระทำมิได้ เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณชน

[230] มาตรา 58 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย (พ.ศ.2540) บุคคลย่อมมีสิทธิได้รับทราบข้อมูลหรือข่าวสารสาธารณะในครอบครองของหน่วยราชการ หน่วยงานของรัฐ รัฐวิสาหกิจ หรือราชการส่วนท้องถิ่น เว้นแต่การเปิดเผยข้อมูลนั้นจะกระทบต่อความมั่นคงของรัฐ ความปลอดภัยของประชาชน หรือส่วนได้เสียอันพึงได้รับความคุ้มครองของบุคคลอื่น ทั้งนี้ ตามที่กฎหมายบัญญัติ

1. ข้อมูลส่วนบุคคลที่ได้รับความคุ้มครอง

ข้อมูลส่วนบุคคลที่กฎหมายทั้งสามฉบับกำหนดให้ความคุ้มครองแก่เจ้าของข้อมูลส่วนบุคคลนั้น เป็นลักษณะของข้อมูลส่วนบุคคลเฉพาะเรื่อง รายละเอียดดังจะกล่าวต่อไปนี้คือ

ฉบับแรก พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 ถูกตราขึ้นเพื่อการรองรับสถานะทางกฎหมายของข้อมูลทางอิเล็กทรอนิกส์ให้เสมอกับการทำเป็นหนังสือ หรือหลักฐานเป็นหนังสือ การรับรองวิธีการส่งและรับข้อมูลอิเล็กทรอนิกส์ การใช้ลายมือชื่ออิเล็กทรอนิกส์ ตลอดจนการรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ เพื่อเป็นการส่งเสริมการทำธุรกรรมทางอิเล็กทรอนิกส์ให้น่าเชื่อถือและมีผลในทางกฎหมายเช่นเดียวกับการทำธุรกรรมโดยวิธีการทั่วไปที่เคยปฏิบัติอยู่เดิมนั่นเอง

ส่วนฉบับที่สอง พระราชบัญญัติว่าด้วยการประกอบธุรกิจข้อมูลบัตรเครดิต พ.ศ.2545 กฎหมายฉบับนี้เป็นกฎหมายที่ถูกตราขึ้นเพื่อให้รัฐสามารถกำกับดูแลการประกอบธุรกิจบัตรเครดิตให้เป็นมาตรฐานเดียวกัน โดยกำหนดมาตรการคุ้มครองผู้บริโภคที่เหมาะสมและเป็นธรรม รวมถึงการกำหนดให้การรับส่งข้อมูลธุรกรรมทางอิเล็กทรอนิกส์ภายในประเทศผ่านศูนย์กลางหรือจุดเชื่อมต่อรับส่งข้อมูลรายการชำระเงินทางอิเล็กทรอนิกส์ที่จัดตั้งภายในประเทศ เพื่อลดต้นทุนให้กับผู้ประกอบการและผู้บริโภคในการประกอบกิจการและการใช้บริการบัตรเครดิต ซึ่งตามกฎหมายฉบับนี้ ได้มีการกำหนดความหมายของข้อมูลส่วนบุคคลที่เป็นข้อมูลเฉพาะเรื่อง นั่นก็คือมีการกำหนดความหมายของ “ข้อมูลเครดิต” โดยกฎหมายฉบับนี้กำหนดว่า หมายถึงข้อมูลเกี่ยวกับประวัติการชำระหนี้ของลูกค้า ซึ่งถูกจัดเก็บไว้ในระบบฐานข้อมูลของบริษัทข้อมูลเครดิต และจะปรากฏในรายงานข้อมูลเครดิตเมื่อมีผู้ขอเรียกดู ปัจจุบันข้อมูลเครดิตประกอบด้วยข้อมูล 2 ส่วนคือ

ส่วนแรก ข้อมูลที่บ่งชี้ถึงตัวตนลูกค้าเช่น ชื่อ ที่อยู่ วันเดือนปีเกิด สถานภาพการสมรส อาชีพ เลขที่บัตรประชาชน และกรณีที่เป็นนิติบุคคล จะเป็น ชื่อ สถานที่ตั้ง เลขที่ทะเบียนนิติบุคคล เป็นต้น

ส่วนที่สอง ข้อมูลเกี่ยวกับสินเชื่อที่ได้รับอนุมัติ และประวัติการชำระสินเชื่อ ประวัติการชำระราคาสินค้าหรือบริการโดยบัตรเครดิต รวมทั้งสถานะบัญชี

โดยข้อมูลเครดิตนี้มีความสำคัญคือ จะเป็นข้อมูลที่แสดงถึงประวัติการชำระหนี้ที่สะท้อนถึงพฤติกรรมและวินัยทางการเงินของเจ้าของข้อมูล แสดงถึงความตั้งใจในการชำระหนี้และความน่าเชื่อถือหรือที่เรียกกันว่า “เครดิต” ที่มีความสำคัญต่อการประกอบธุรกิจ สถาบันการเงินจึงใช้ประโยชน์จากรายงานข้อมูลเครดิตเป็นปัจจัยหนึ่งที่ใช้ร่วมกับปัจจัยอื่น ๆ ในการพิจารณาอนุมัติสินเชื่อ เช่น ความสามารถในการหารายได้ ความเป็นไปได้ของธุรกิจ หลักประกัน เป็นต้น ดังนั้น ย่อมกล่าวได้ว่าผู้ที่มีประวัติการชำระหนี้ดีมีโอกาสได้รับสินเชื่อในอัตราที่เหมาะสม

ฉบับที่สาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 กฎหมายฉบับนี้ไม่ได้มีการกำหนดความหมายของข้อมูลส่วนบุคคลเฉพาะ ซึ่งก็คือข้อมูลคอมพิวเตอร์

โดยกำหนดนิยามของ “ข้อมูลคอมพิวเตอร์” ว่าหมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึง ข้อมูลอิเล็กทรอนิกส์ ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ด้วย

จากนิยามของข้อมูลส่วนบุคคลตามกฎหมายทั้งสามฉบับจะเห็นว่า มีลักษณะของการกำหนดข้อมูลส่วนบุคคลเฉพาะ เพื่อเป็นนิยามสำหรับการบังคับใช้กฎหมาย กล่าวอีกนัยหนึ่งก็คือ มีการกำหนดรับรองสิทธิเพื่อให้มีการคุ้มครองข้อมูลส่วนบุคคลเฉพาะเรื่องตามวัตถุประสงค์หรือเจตนารมณ์ของกฎหมายแต่ละฉบับนั้นเอง

2. มาตรการคุ้มครองตามกฎหมายแต่ละฉบับ

สำหรับมาตรการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายแต่ละฉบับ จะเห็นว่าในกฎหมายฉบับแรก ซึ่งก็คือ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 ได้มีการกำหนดมาตรการอันเป็นสาระสำคัญของกฎหมายดังนี้

1) ในกรณีที่กฎหมายกำหนดให้การใดต้องทำเป็นหนังสือ มีหลักฐานเป็นหนังสือหรือมีเอกสารมาแสดง ถ้าได้มีการจัดทำข้อความขึ้นเป็นข้อมูลอิเล็กทรอนิกส์ที่สามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง ให้ถือว่าข้อความนั้นได้ทำเป็นหนังสือ มีหลักฐานเป็นหนังสือหรือมีเอกสารมาแสดงแล้ว (มาตรา 8) และในกรณีที่บุคคลลงลายมือชื่อในหนังสือ ให้ถือว่าข้อมูลอิเล็กทรอนิกส์นั้นมีการลงลายมือชื่อแล้ว ถ้าบุคคลนั้นใช้วิธีการที่สามารถระบุตัวเจ้าของลายมือชื่อได้และสามารถจะแสดงได้ว่าเจ้าของลายมือชื่อนั้นรับรองข้อความในข้อมูลอิเล็กทรอนิกส์ว่าเป็นของตน โดยวิธีดังกล่าวจะต้องเป็นวิธีการที่เชื่อถือได้โดยเหมาะสมกับวัตถุประสงค์ของการสร้างหรือส่งข้อมูลอิเล็กทรอนิกส์โดยคำนึงถึงพฤติการณ์แวดล้อมหรือข้อตกลงของคู่กรณี (มาตรา 9)

2) ในกรณีที่กฎหมายกำหนดให้นำเสนอหรือเก็บรักษาข้อความใดในสภาพที่เป็นมาแต่เดิมอย่างเอกสารต้นฉบับ ถ้าได้นำเสนอหรือเก็บรักษาในรูปข้อมูลอิเล็กทรอนิกส์โดยใช้วิธีการที่เชื่อถือได้ในการรักษาความถูกต้องของข้อความ ความครบถ้วนและไม่มีการเปลี่ยนแปลงใด ๆ ของข้อความ เว้นแต่การรับรองหรือบันทึกเพิ่มเติมหรือการเปลี่ยนแปลงใด ๆ และสามารถที่จะแสดงข้อความนั้นในภายหลังได้แล้ว ให้ถือว่าได้มีการนำเสนอหรือเก็บรักษาเป็นเอกสารต้นฉบับตามกฎหมายแล้ว (มาตรา 10)

3) ห้ามไม่ให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในกระบวนการพิจารณาตามกฎหมายเพียงเพราะเหตุว่าเป็นข้อมูลอิเล็กทรอนิกส์ โดยการพิเคราะห์ถึงความน่าเชื่อถือของข้อมูลดังกล่าวจะพิเคราะห์ถึงลักษณะหรือวิธีการที่ใช้สร้าง เก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์ ลักษณะหรือวิธีการรักษาความครบถ้วนและไม่มีการเปลี่ยนแปลงของข้อความ ลักษณะหรือวิธีการที่ใช้ในการระบุหรือแสดงตัวผู้ส่งข้อมูล รวมทั้งพฤติการณ์ที่เกี่ยวข้องทั้งปวง (มาตรา 11)

4) คำเสนอหรือคำสนองในการทำสัญญาอาจทำเป็นข้อมูลอิเล็กทรอนิกส์ก็ได้ (มาตรา 13) โดยการแสดงเจตนาหรือคำบอกกล่าวอาจทำเป็นข้อมูลอิเล็กทรอนิกส์ได้ (มาตรา 14) และบุคคลใดเป็นผู้ส่งข้อมูลไม่ว่าจะเป็นการส่งโดยวิธีใดให้ถือว่าข้อมูลอิเล็กทรอนิกส์เป็นของผู้นั้น โดยมีหลักเกณฑ์ในการส่งหรือการรับข้อมูลดังนี้คือ

กรณีแรก ในระหว่างผู้ส่งข้อมูลและผู้รับข้อมูล ให้ถือว่าเป็นข้อมูลอิเล็กทรอนิกส์ของผู้ส่งข้อมูล หากข้อมูลอิเล็กทรอนิกส์นั้นได้ส่งโดยบุคคลผู้มีอำนาจกระทำการแทนผู้ส่งข้อมูลเกี่ยวกับข้อมูลอิเล็กทรอนิกส์นั้นหรือระบบข้อมูลที่ผู้ส่งข้อมูลหรือบุคคลผู้มีอำนาจกระทำการแทนผู้ส่งข้อมูลได้กำหนดไว้ล่วงหน้าให้สามารถทำงานได้โดยอัตโนมัติ (มาตรา 15)

กรณีที่สอง ผู้รับข้อมูลชอบที่จะถือว่าข้อมูลอิเล็กทรอนิกส์เป็นของผู้ส่งข้อมูลและชอบที่จะดำเนินการไปตามข้อมูลอิเล็กทรอนิกส์นั้นได้ถ้าผู้รับข้อมูลได้ตรวจสอบโดยสมควรว่าข้อมูลอิเล็กทรอนิกส์นั้นเป็นของผู้ส่งข้อมูล แต่ถ้าในขณะนั้นผู้รับข้อมูลได้รับแจ้งจากผู้ส่งข้อมูลว่าข้อมูลอิเล็กทรอนิกส์ที่ผู้รับข้อมูลได้รับนั้นไม่ใช่ของผู้ส่งข้อมูลและในขณะเดียวกันผู้รับข้อมูลมีเวลาพอสมควรที่จะตรวจสอบข้อเท็จจริงตามที่ได้รับแจ้งนั้น จะถือว่าข้อมูลที่ผู้รับได้รับเป็นของผู้ส่งข้อมูลไม่ได้ อีกกรณีหนึ่งคือ ข้อมูลอิเล็กทรอนิกส์ที่ผู้รับข้อมูลได้รับนั้นเกิดจากการกระทำของบุคคลซึ่งใช้วิธีการที่ผู้ส่งข้อมูลใช้ในการแสดงว่าข้อมูลอิเล็กทรอนิกส์นั้นเป็นของผู้ส่งข้อมูล ซึ่งบุคคลนั้นได้ล่วงรู้โดยอาศัยความสัมพันธ์ระหว่างบุคคลนั้นกับผู้ส่งข้อมูลหรือผู้มีอำนาจกระทำการแทนผู้ส่งข้อมูล ผู้รับข้อมูลจะถือว่าข้อมูลเป็นของผู้ส่งข้อมูลและชอบที่จะดำเนินการไปตามข้อมูลนั้นได้ แต่ถ้าผู้รับข้อมูลได้รู้หรือควรจะได้รู้ว่าข้อมูลนั้นไม่ใช้ข้อมูลของผู้ส่งข้อมูล หากผู้รับข้อมูลได้ใช้ความระมัดระวังตามสมควรหรือดำเนินการตามวิธีการที่ได้ตกลงกันไว้ก่อนแล้ว ผู้รับข้อมูลจะถือว่าข้อมูลนั้นเป็นของผู้ส่งข้อมูลไม่ได้ (มาตรา 11)

5) ในกรณีที่ต้องมีการตอบแจ้งการรับข้อมูลทางอิเล็กทรอนิกส์ ไม่ว่าผู้ส่งข้อมูลได้ร้องขอหรือตกลงกับผู้รับข้อมูลไว้ก่อนหรือขณะที่ส่งข้อมูลอิเล็กทรอนิกส์หรือปรากฏในข้อมูลอิเล็กทรอนิกส์ให้เป็นไปตามหลักเกณฑ์ ดังต่อไปนี้คือ

กรณีแรก ในกรณีที่ผู้ส่งข้อมูลมิได้ตกลงให้ตอบแจ้งการรับข้อมูลอิเล็กทรอนิกส์ในรูปแบบหรือวิธีการใดโดยเฉพาะ การตอบแจ้งการรับอาจทำได้ด้วยการติดต่อสื่อสารจากผู้รับข้อมูล

กรณีที่สอง ในกรณีที่ผู้ส่งข้อมูลกำหนดเงื่อนไขว่าจะถือว่ามีการส่งข้อมูลอิเล็กทรอนิกส์ต่อเมื่อได้รับการตอบแจ้งการรับจากผู้รับข้อมูล ให้ถือว่ายังไม่มีการส่งข้อมูลอิเล็กทรอนิกส์จนกว่าผู้ส่งข้อมูลจะได้รับการตอบแจ้งการรับแล้ว

กรณีที่สาม ในกรณีที่ผู้ส่งข้อมูลมิได้กำหนดเงื่อนไขและผู้ส่งข้อมูลมิได้รับการตอบแจ้งการรับนั้นภายในเวลาที่กำหนดหรือตกลงกัน หรือภายในระยะเวลาอันสมควรในกรณีที่มิได้กำหนดหรือตกลงเวลาไว้ ผู้ส่งข้อมูลอาจส่งคำบอกกล่าวไปยังผู้รับข้อมูลว่าตนยังมิได้รับการตอบแจ้งการรับ

และกำหนดระยะเวลาอันสมควรให้ผู้รับข้อมูลตอบแจ้งการรับและหากผู้ส่งข้อมูลมิได้รับการตอบแจ้งการรับภายในระยะเวลาอันสมควรดังกล่าว เมื่อผู้ส่งข้อมูลบอกกล่าวแก่ผู้รับข้อมูลแล้ว ผู้ส่งข้อมูลชอบที่จะถือว่าข้อมูลอิเล็กทรอนิกส์นั้นมิได้มีการส่งเลยหรือผู้ส่งข้อมูลอาจใช้สิทธิอื่นใดที่ผู้ส่งข้อมูลมีอยู่ได้

6) การส่งข้อมูลอิเล็กทรอนิกส์ให้ถือว่าได้มีการส่งเมื่อข้อมูลอิเล็กทรอนิกส์นั้นได้เข้าสู่ระบบข้อมูลที่อยู่นอกเหนือการควบคุมของผู้ส่งข้อมูล (มาตรา 22) และการรับข้อมูลอิเล็กทรอนิกส์ให้ถือว่ามีผลนับแต่เวลาที่ข้อมูลอิเล็กทรอนิกส์นั้นได้เข้าสู่ระบบข้อมูลของผู้รับข้อมูล หากผู้รับข้อมูลได้กำหนดระบบข้อมูลที่ประสงค์จะใช้ในการรับข้อมูลอิเล็กทรอนิกส์ไว้โดยเฉพาะให้ถือว่าการรับข้อมูลอิเล็กทรอนิกส์มีผลนับแต่เวลาที่ข้อมูลอิเล็กทรอนิกส์นั้นได้เข้าสู่ระบบข้อมูลที่ผู้รับข้อมูลได้กำหนดไว้นั้น

นอกจากนี้ ในกรณีมีการใช้ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์เพื่อสร้างลายมือชื่ออิเล็กทรอนิกส์ที่จะมีผลตามกฎหมาย เจ้าของลายมือชื่อต้องใช้ความระมัดระวังตามสมควรเพื่อไม่ให้มีการใช้ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์โดยไม่ได้รับอนุญาต,แจ้งให้บุคคลที่คาดหมายได้โดยมีเหตุอันควรเชื่อว่าจะกระทำการใดโดยขึ้นอยู่กับลายมือชื่ออิเล็กทรอนิกส์หรือให้บริการเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ทราบโดยไม่ชักช้าเมื่อเจ้าของลายมือชื่อรู้หรือควรได้รู้ว่าข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์นั้นสูญหาย ถูกทำลาย ถูกแก้ไข ถูกเปิดเผยโดยไม่ชอบหรือถูกล่วงรู้โดยไม่สอดคล้องกับวัตถุประสงค์ รวมถึงการที่เจ้าของลายมือชื่อรู้จากสภาพการณ์ที่ปรากฏว่ากรณีมีความเสี่ยงมากพอที่ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์จะสูญหาย ถูกทำลาย ถูกแก้ไข ถูกเปิดเผยโดยไม่ชอบหรือถูกล่วงรู้โดยไม่สอดคล้องกับวัตถุประสงค์,ในกรณีมีการออกใบรับรองสนับสนุนการใช้ลายมือชื่ออิเล็กทรอนิกส์จะต้องใช้ความระมัดระวังตามสมควรให้แน่ใจในความถูกต้องและสมบูรณ์ของการแสดงสาระสำคัญทั้งหมด ซึ่งกระทำโดยเจ้าของลายมือชื่อเกี่ยวกับใบรับรองนั้นตลอดอายุใบรับรองหรือตามที่มีการกำหนดในใบรับรอง (มาตรา 17)

นอกจากที่กล่าวมาข้างต้น ภายใต้กฎหมายฉบับนี้ที่ได้ให้อำนาจแก่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ออก ประกาศฯ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานรัฐ พ.ศ.2553 ซึ่งสาระสำคัญของประกาศฯ ฉบับดังกล่าวที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลมีการกำหนดหลักการออกเป็น 2 ส่วนคือ

ส่วนที่ 1 ให้หน่วยงานของรัฐซึ่งรวบรวม จัดเก็บ ใช้ เผยแพร่ หรือดำเนินการอื่นใดเกี่ยวกับข้อมูลของผู้ใช้บริการ ธุรกรรมทางอิเล็กทรอนิกส์ จัดทำนโยบายในการ คุ้มครองข้อมูลส่วนบุคคลไว้เป็นลายลักษณ์อักษร โดยให้มีสาระสำคัญอย่างน้อย ดังนี้[231]

---

[231] ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวทางการจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ.2553

1) การเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด

2) คุณภาพของข้อมูลส่วนบุคคล

3) การระบุวัตถุประสงค์ในการเก็บรวบรวม

4) ข้อจำกัดในการนำข้อมูลส่วนบุคคลไปใช้

5) การรักษาความมั่นคงปลอดภัย

6) การเปิดเผยเกี่ยวกับการดำเนินการแนวปฏิบัติ และนโยบายที่เกี่ยวกับข้อมูลส่วนบุคคล

7) การมีส่วนร่วมของเจ้าของข้อมูล

8) ความรับผิดชอบของบุคคลซึ่งทำหน้าที่ควบคุมข้อมูล

ส่วนที่ 2 ให้หน่วยงานของรัฐจัดทำข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการ และให้มีรายการ อย่างน้อย ดังนี้

1) ข้อมูลเบื้องต้น

2) การเก็บรวบรวม จัดประเภท และการใช้ข้อมูลส่วนบุคคล

3) การแสดงระบุความเชื่อมโยงให้ข้อมูลส่วนบุคคลกับหน่วยงานหรือองค์กรอื่น

4) การรวมข้อมูลจากที่มาหลาย ๆ แห่ง

5) การให้บุคคลอื่นใช้หรือการเปิดเผยข้อมูลส่วนบุคคล

6) การรวบรวม จัดเก็บ ใช้ และการเปิดเผยข้อมูลเกี่ยวกับผู้ใช้บริการ

7) การเข้าถึง การแก้ไขให้ถูกต้อง และการปรับปรุงให้เป็นปัจจุบัน

8) การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

9) เว็บไซต์ซึ่งให้ข้อมูลแก่ผู้ใช้บริการในการติดต่อกับ หน่วยงานของรัฐต้องจัดให้มีทั้งข้อมูลติดต่อไปยัง สถานที่ทำการงานปกติและข้อมูลติดต่อผ่านทางออนไลน์ด้วย

สำหรับกฎหมายฉบับที่สอง ซึ่งก็คือ พระราชบัญญัติว่าด้วยการประกอบธุรกิจข้อมูลบัตรเครดิต พ.ศ.2545 ได้มีการกำหนดมาตการอันเป็นสาระสำคัญของกฎหมายดังนี้

1) ผู้จัดเก็บข้อมูลและผู้นำส่งข้อมูล สำหรับบริษัทที่จะประกอบธุรกิจข้อมูลเครดิตเพื่อจัดเก็บข้อมูลเครดิตได้ จะต้องได้รับอนุญาตจากรัฐมนตรีว่าการกระทรวงการคลัง ซึ่งปัจจุบันผู้ประกอบธุรกิจข้อมูลเครดิตที่ได้รับอนุญาตมีเพียงแห่งเดียว คือ บริษัทข้อมูลเครดิตแห่งชาติ จำกัด (National Credit Bureau Co.,Ltd.: NCB) ส่วนผู้นำส่งข้อมูลนั้นจะเป็นสถาบันการเงินหรือนิติบุคคลที่ประกอบธุรกิจให้สินเชื่อ ที่เป็นสมาชิกของบริษัทข้อมูลเครดิตแห่งชาติ มีหน้าที่นำส่งข้อมูลเครดิตลูกค้าของตนให้บริษัทข้อมูลเครดิตแห่งชาติ

2) การจัดเก็บข้อมูลและระยะเวลาการจัดเก็บข้อมูล สถาบันการเงินที่เป็นสมาชิกของบริษัทข้อมูลเครดิตมีหน้าที่นำส่งข้อมูลสินเชื่อของลูกค้าแต่ละรายให้บริษัทข้อมูลเครดิตเป็นรายเดือนไปจนกว่าสินเชื่อนั้นจะได้รับการชำระเสร็จสิ้น ในกรณีที่ลูกค้าผิดนัดชำระหนี้และค้างชำระเกิน 90 วัน

สถาบันการเงินจะส่งข้อมูลสินเชื่อคงค้างให้บริษัทข้อมูลเครดิตต่อเนื่องไปอีกเป็นเวลาไม่เกิน 5 ปี นับแต่วันที่ค้างชำระเกิน 90 วัน

บริษัทข้อมูลเครดิตจะเก็บข้อมูลเครดิตที่ได้รับจากสถาบันการเงินไว้ในฐานข้อมูลต่อไปอีกเป็นเวลาไม่เกิน 3 ปี นับจากวันที่บริษัทข้อมูลเครดิตได้รับข้อมูลจากสถาบันการเงิน

3) ในกรณีเจ้าของข้อมูลพบว่าข้อมูลเครดิตไม่ถูกต้อง เจ้าของข้อมูลมีสิทธิยื่นคำขอตรวจสอบและแก้ไขข้อมูลเครดิตของตนได้ที่บริษัทข้อมูลเครดิตและสถาบันการเงินที่เจ้าของข้อมูลเป็นลูกค้า หากสถาบันการเงินตรวจสอบหลักฐานและข้อเท็จจริงพบว่าข้อมูลเครดิตไม่ถูกต้อง สถาบันการเงินจะต้องส่งข้อมูลที่ถูกต้องให้บริษัทข้อมูลเครดิตแก้ไข และแจ้งผลการตรวจสอบให้ทราบภายใน 30 วัน หากเจ้าของข้อมูลเห็นว่ารายงานข้อมูลเครดิตของตนยังมีความไม่ถูกต้องอีก เจ้าของข้อมูลสามารถยื่นคำขอให้บริษัทข้อมูลเครดิตบันทึกข้อโต้แย้งไว้ในรายงานข้อมูลเครดิตของตนเองได้

สำหรับกฎหมายฉบับที่สาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ได้มีการกำหนดมาตรการในการคุ้มครองสิทธิของเจ้าของข้อมูลคอมพิวเตอร์ไว้ดังนี้[232]

1) การเข้าถึงคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์โดยมิชอบ

สำหรับกรณีของ การเข้าถึง (Access) ข้อมูลโดยมิชอบนั้น มีการกำหนดไว้ให้เป็นความผิดตามกฎหมายฉบับนี้ ซึ่งมีอยู่ 2 กรณี คือ กรณีแรก ตามบทบัญญัติของมาตรา 5 ที่มีการกำหนดว่า ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ และในกรณีของบทบัญญัติ มาตรา 7 ที่กำหนดว่า ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ ซึ่งทั้งสองกรณีเป็นมาตรการที่สามารถคุ้มครองการเข้าถึงโดยมิชอบ อันจะเป็นการป้องกันการล่วงละเมิดข้อมูลส่วนบุคคล

2) การเปิดเผยมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์

สำหรับกรณีนี้เป็นไปตามบทบัญญัติของมาตรา 6 ซึ่งเป็นการวางมาตรการป้องกันไว้โดยเฉพาะ หากผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบ ในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

3) การดักรับข้อมูล

ในกฎหมายฉบับนี้ มีการกำหนดความผิดฐานดักรับข้อมูลทางคอมพิวเตอร์ของผู้อื่นโดยมิชอบไว้ในมาตรา 8 โดยหากผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อดัก

---

[232] อธิพร สิทธิธีรรัตน์, *เรื่องเดิม*, หน้า 134-136.

รับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะ หรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

4) ทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติมข้อมูลคอมพิวเตอร์โดยมิชอบ

กรณีนี้มีการกำหนดไว้ในมาตรา 9 โดยกำหนดว่า ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติม ไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่น โดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ ซึ่งวัตถุประสงค์ของมาตรานี้ มีขึ้นเพื่อรักษาความถูกต้องแท้จริงของข้อมูล และเสถียรภาพในการใช้งานข้อมูลคอมพิวเตอร์และโปรแกรมคอมพิวเตอร์เพื่อให้เป็นไปตามปกติ ซึ่งนอกจากความผิดที่ได้กล่าวมาแล้วข้างต้น หากว่าเป็นกรณีซึ่งได้กระทำโดยก่อให้เกิดความเสียหายแก่ประชาชน หรือเป็นกรณีของการกระทำที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ ต้องระวางโทษหนักขึ้น

3. สิทธิของเจ้าของข้อมูลตามกฎหมายแต่ละฉบับ

ในข้อนี้จะได้อธิบายถึงสิทธิของเจ้าของข้อมูล (Data Subject) ตามกฎหมายต่าง ๆ ที่กล่าวมาในตอนต้น โดยเมื่อพิจารณาถึงสิทธิของเจ้าของข้อมูลตามกฎหมายฉบับแรก พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 จากสาระสำคัญของกฎหมายฉบับนี้ที่กล่าวมาแล้ว เมื่อพิจารณาจากสภาพของการทำธุรกรรมทางอิเล็กทรอนิกส์ที่แม้จะส่งผลดีให้เกิดความสะดวกรวดเร็วในการทำธุรกรรม แต่ในทางปฏิบัติของการทำธุรกรรมก็อาจมีปัญหาเกิดขึ้น โดยเฉพาะอย่างยิ่งในเรื่องของความปลอดภัยของข้อมูลส่วนบุคคล ที่อาจเกิดปัญหาการจารกรรมข้อมูล (Theft of Information) ซึ่งเป็นการคัดลอก หรือนำเอาไปซึ่งข้อมูลส่วนบุคคลที่อยู่ในรูปอิเล็กทรอนิกส์โดยไม่มีสิทธิ ไม่ว่าจะเป็นข้อมูลเกี่ยวกับการค้า ข้อมูลการชำระราคา หรือข้อมูลที่มีความมุ่งประสงค์ใช้เฉพาะบุคคลหรือกลุ่มบุคคล เช่น ข้อมูลเกี่ยวกับการรักษาพยาบาล หรือข้อมูลประวัติทางการแพทย์อื่น ๆ เป็นต้น การจารกรรมข้อมูลเช่นนี้ อาจเป็นการทำขึ้นโดยผู้ซึ่งมีหน้าที่ควบคุมดูแลข้อมูลส่วนบุคคลนั้นเอง หรือบุคคลภายนอกเป็นผู้กระทำโดยไม่มีสิทธิก็ได้ หรืออาจจะมีปัญหาในเรื่องของการแก้ไข เปลี่ยนแปลงข้อมูล อันส่งให้เกิดความเสียหายต่อข้อมูลที่แท้จริง รวมไปถึงปัญหาการลบ หรือการทำลายข้อมูลซึ่งก่อให้เกิดความเสียหาย เช่น ไม่สามารถนำข้อมูลนั้นกลับมาใช้ใหม่ได้อีก ซึ่งการลบ หรือทำลายข้อมูลอาจเป็นการกระทำต่อข้อมูลอิเล็กทรอนิกส์โดยตรง หรือเป็นการกระทำต่อสื่ออิเล็กทรอนิกส์ทางกายภาพก็ได้ การทำลายข้อมูลหรือระบบคอมพิวเตอร์มักพบได้ในกรณีของการใช้ไวรัสคอมพิวเตอร์ ก็ได้ ซึ่งจากปัญหาทางปฏิบัติที่กล่าวมานี้ เมื่อพิจารณาจากหลักเกณฑ์ของการคุ้มครองข้อมูลส่วนบุคคล

ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 จะพบว่ามีปัญหาในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล แยกพิจารณาได้ 2 ประการดังนี้

ประการแรก กรณีข้อมูลที่ไม่ใช่ลายมือชื่ออิเล็กทรอนิกส์ เช่น ข้อมูลเกี่ยวกับประวัติสุขภาพและการรักษา ข้อมูลการเงิน ข้อมูลเกี่ยวกับการตกลงทำนิติกรรมสัญญาต่าง ๆ อันอยู่ในรูปอิเล็กทรอนิกส์นั้น กฎหมายฉบับนี้ไม่ได้มีการวางหลักการคุ้มครองความปลอดภัยของข้อมูลแต่อย่างใด โดยไม่ได้มีการกำหนดหน้าที่ให้ผู้เก็บรักษาข้อมูลต้องดำเนินการใด ๆ เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์ ไม่ได้มีการวางหลักเกี่ยวกับการจัดเก็บ การประมวลผล ตลอดจนหลักการเกี่ยวกับการห้ามเปิดเผยข้อมูลต่าง ๆ ดังเช่นกฎหมายของต่างประเทศเช่น สหรัฐอเมริกา ออสเตรเลีย หรือสหภาพยุโรป เป็นต้น ทั้งนี้เนื่องจากพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 มุ่งเน้นการวางหลักเกณฑ์ในการรับรองความมีผลของข้อมูลอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการทำนิติกรรมสัญญาให้มีผลเสมือนการทำธุรกรรมโดยเอกสารหรือกระดาษ แต่ไม่ได้มุ่งเน้นการคุ้มครองความปลอดภัยของข้อมูลในส่วนที่เกี่ยวกับการใช้ การประมวลผล และการจัดเก็บข้อมูลดังกล่าวแต่อย่างใด ด้วยเหตุนี้จึงเกิดช่องว่างทางกฎหมายและทำให้พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 ซึ่งถือเป็นกฎหมายเฉพาะที่เกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ไม่สามารถที่จะเป็นกฎหมายที่วางหลักเกณฑ์ต่าง ๆ ในการทำธุรกรรมอิเล็กทรอนิกส์ได้อย่างครบถ้วนทั้งระบบ กล่าวคือ ขาดการวางหลักการคุ้มครองความปลอดภัยของข้อมูลส่วนบุคคลที่อยู่ในรูปอิเล็กทรอนิกส์

ประการที่สอง กรณีข้อมูลที่เป็นลายมือชื่ออิเล็กทรอนิกส์ ซึ่งจัดเป็นข้อมูลส่วนบุคคลที่สำคัญประการหนึ่งของเจ้าของลายมือชื่อ เนื่องจากเป็นข้อมูลที่สามารถทำให้ระบุตัวตนของบุคคลผู้เป็นเจ้าของลายมือชื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องทั้งทางตรงและทางอ้อมกับข้อมูลอิเล็กทรอนิกส์นั้นได้ โดยพระราชบัญญัติฉบับนี้ได้มีการวางหลักเกณฑ์คุ้มครองความปลอดภัยของข้อมูลส่วนนี้ ดังที่ได้กล่าวมาแล้วในส่วนของสาระสำคัญของกฎหมายข้างต้น อย่างไรก็ตามปัญหาหลักของกฎหมายฉบับนี้ก็คือเป็นการมุ่งเน้นเพื่อวางหลักเกณฑ์คุ้มครองความถูกต้องแท้จริงของลายมือชื่ออิเล็กทรอนิกส์ในระดับของการเกิดขึ้นหรือการสร้างลายมือชื่ออิเล็กทรอนิกส์เท่านั้น โดยไม่ได้มุ่งเน้นการวางหลักคุ้มครองความปลอดภัยของข้อมูลที่เป็นลายมือชื่ออิเล็กทรอนิกส์หลังจากที่ได้เกิดขึ้นแล้ว โดยอาจจะถูกนำไปใช้โดยไม่ได้รับอนุญาตจากเจ้าของข้อมูล ทั้งนี้จะเป็นได้จากหลักกฎหมายนี้มุ่งกำหนดหน้าที่ให้แก่เจ้าของลายมือชื่ออิเล็กทรอนิกส์ดำเนินการต่าง ๆ เพื่อมิให้มีการใช้ข้อมูลสำหรับสร้างลายมือชื่ออิเล็กทรอนิกส์โดยไม่ได้รับอนุญาต แต่หลังจากที่ได้มีการสร้างขึ้นแล้วและถือว่าเป็นข้อมูลอิเล็กทรอนิกส์ประเภทหนึ่ง กฎหมายกลับไม่ได้กำหนดหน้าที่ให้บุคคลหรือองค์กรใด ๆ ที่เกี่ยวข้องกับการจัดเก็บ ประมวลผล หรือเกี่ยวข้องในประการอื่นกับลายมือชื่ออิเล็กทรอนิกส์นั้นให้มีหน้าที่ในการคุ้มครองความปลอดภัยแก่ข้อมูลดังกล่าว นอกจากนี้ แม้ว่ากฎหมายได้กำหนดหน้าที่สำหรับผู้

ให้บริการออกใบรับรองเพื่อสนับสนุนลายมือชื่ออิเล็กทรอนิกส์ให้มีผลทางกฎหมายเสมือนลายมือชื่อ แต่ก็เป็นเพียงการกำหนดหน้าที่เพื่อให้ผู้ให้บริการรับรองได้ดำเนินกระบวนการในการรับรองลายมือชื่ออิเล็กทรอนิกส์นั้นให้มีความถูกต้องแท้จริง โดยไม่ได้มีการกำหนดหน้าที่ในการเก็บรักษาข้อมูลแต่อย่างใด ด้วยเหตุนี้จึงเกิดช่องว่างทางกฎหมายทำให้พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ไม่สามารถเป็นกฎหมายหลักที่วางหลักเกณฑ์ต่าง ๆ ในการทำธุรกรรมทางอิเล็กทรอนิกส์ได้อย่างครบถ้วนทั้งระบบ กล่าวคือ ขาดการวางหลักคุ้มครองความปลอดภัยของลายมือชื่ออิเล็กทรอนิกส์ภายหลังจากที่เจ้าของลายมือชื่อได้สร้างขึ้นแล้ว

สำหรับกฎหมายฉบับที่สอง พระราชบัญญัติว่าด้วยการประกอบธุรกิจข้อมูลบัตรเครดิต พ.ศ. 2545 กำหนดสิทธิให้แก่เจ้าของข้อมูลไว้หลายประการดังนี้คือ

1) สิทธิในการรับรู้ว่าบริษัทข้อมูลเครดิตเก็บรักษาข้อมูลใดของตน

2) สิทธิที่จะตรวจสอบข้อมูลของตน

3) สิทธิที่จะขอแก้ไขข้อมูลที่ไม่ถูกต้อง

4) สิทธิที่จะโต้แย้งเมื่อทราบว่าข้อมูลของตนไม่ถูกต้อง

5) สิทธิที่จะได้รับแจ้งผลการตรวจสอบข้อมูลของตนภายในระยะเวลาที่กำหนด

6) สิทธิที่จะได้รับทราบเหตุแห่งการปฏิเสธคำขอสินเชื่อหรือบริการจากสถาบันการเงินในกรณีที่สถาบันการเงินใช้ข้อมูลของบริษัทข้อมูลบัตรเครดิตมาเป็นเหตุในการปฏิเสธคำขอสินเชื่อหรือบริการ

7) สิทธิที่จะอุทธรณ์ต่อคณะกรรมการ

เมื่อพิจารณาสาระสำคัญของพระราชบัญญัติฉบับนี้แล้ว มีข้อสังเกตและข้อคิดเห็นที่สำคัญดังนี้คือ

1) กฎหมายฉบับนี้แม้ว่าจะครอบคลุมหลักเกณฑ์ วิธีการ และกระบวนการในการคุ้มครองและควบคุมการใช้ข้อมูลส่วนบุคคลของผู้ขอสินเชื่อ ซึ่งควบคุมทั้งหน่วยงานภาครัฐและเอกชนก็ตาม แต่ก็มีฐานะเป็นเพียงกฎหมายที่คุ้มครองเฉพาะเรื่องข้อมูลส่วนบุคคลทางด้านการเงินสินเชื่อเท่านั้น

2) กฎหมายฉบับนี้กำหนดให้ธนาคารแห่งประเทศไทยมีฐานะเป็นผู้เสียหาย ตามประมวลกฎหมายวิธีพิจารณาความอาญาแทนผู้เสียหายที่แท้จริง แต่ไม่ตัดสิทธิบุคคลธรรมดาที่เป็นผู้เสียหายที่แท้จริงในการฟ้องร้องผู้กระทำผิด

3) กฎหมายฉบับนี้บัญญัติความผิดที่กระทำต่อข้อมูลในระบบความจำของคอมพิวเตอร์เป็นพิเศษ แสดงให้เห็นว่า กฎหมายฉบับนี้ให้ความสำคัญกับการประมวลผลข้อมูลด้วยระบบคอมพิวเตอร์ นอกเหนือจากระบบการประมวลผลด้วยมือ

นอกจากนี้ ยังมีประเด็นปัญหาเรื่องของการเปิดเผยข้อมูลเครดิต (ซึ่งเป็นข้อมูลส่วนบุคคล) ตามกฎหมายฉบับนี้อีกด้วย กล่าวคือ หากพิจารณาถึงสาระสำคัญของ พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ.2545 แล้ว จะเห็นว่ามีการกำหนดหลักการอย่างหนึ่งเรียกว่า หลักการในการให้ความยินยอมในการเปิดเผยข้อมูลเครดิตของเจ้าของข้อมูล โดยมีการกำหนดว่า การเปิดเผยข้อมูลเครดิต (ซึ่งถือเป็นข้อมูลส่วนบุคคลชนิดหนึ่ง) ไม่สามารถกระทำได้หากไม่ได้รับความยินยอมจากผู้ที่เป็นเจ้าของข้อมูล (มาตรา 20) จึงมีประเด็นปัญหาสำคัญว่าหากความยินยอมไม่ได้เป็นการเกิดจากอิสระในการตัดสินใจที่แท้จริงของเจ้าของข้อมูล หรือข้อมูลเครดิตที่มีการเปิดเผยนั้น ไม่ได้มีการนำไปใช้เพื่อวัตถุประสงค์ในเรื่องที่เกี่ยวกับสินเชื่อหรือการนำไปวิเคราะห์สินเชื่อแล้ว เจ้าของข้อมูลยังคงจะได้รับความคุ้มครองตามกฎหมายฉบับนี้หรือไม่ ทั้งนี้เพราะพระราชบัญญัติดังกล่าวได้อาศัยอำนาจจากรัฐธรรมนูญแห่งราชอาณาจักรไทยในการออกบทบัญญัติมาจำกัดสิทธิเสรีภาพของบุคคลผู้เป็นเจ้าของข้อมูล แต่กลับไม่มีความชัดเจนในการคุ้มครองสิทธิของเจ้าของข้อมูล อีกทั้งยังจะเห็นได้ชัดเจนในกรณีที่หากว่า เจ้าของข้อมูลเครดิต (ซึ่งเป็นข้อมูลส่วนบุคคล) ไม่ให้ความยินยอมในการที่จะเปิดเผยข้อมูลเครดิตแล้ว เจ้าของข้อมูลส่วนบุคคลนั้นก็ย่อมที่จะถูกปิดกั้นหรือสูญเสียโอกาสในการได้รับการพิจารณาสินเชื่อได้ตามความเป็นจริงในทางปฏิบัติ สะท้อนภาพของการที่เจ้าของข้อมูลไม่มีทางเลือกใด ๆ ในเรื่องการเปิดเผยข้อมูล และในเรื่องการให้ความยินยอม

นอกจากนี้ยังมีประเด็นปัญหาสำคัญอีกประการหนึ่งก็คือ การนำข้อมูลเครดิตไปใช้อย่างผิดวัตถุประสงค์ กล่าวคือ ปัจจุบันได้มีการนำข้อมูลเครดิตไปใช้เพื่อประกอบการพิจารณารับสมัครงาน ซึ่งนายจ้างส่วนใหญ่ก็ได้หาวิธีการต่าง ๆ นานา เพื่อให้เข้าถึงข้อมูลเครดิตนี้ของลูกจ้างให้ได้ โดยอาศัยช่องว่างทางกฎหมายและวิธีการเลี่ยงกฎหมายเพื่อให้สามารถเข้าถึงข้อมูลของลูกจ้างที่จะรับเข้าทำงาน โดยประเด็นนี้ได้สร้างปัญหาให้กับลูกจ้างผู้ซึ่งเป็นเจ้าของข้อมูลเครดิตอย่างมาก กล่าวคือ มีผลกระทบต่อโอกาสในการเข้าทำงานของลูกจ้างมากยิ่งขึ้น การที่ไม่ได้มีการกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลครอบคลุมถึงประเด็นเช่นนี้ก็ก่อให้เกิดช่องว่างที่สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในด้านข้อมูลเครดิตย่อมมีโอกาสถูกล่วงละเมิดได้โดยง่าย

กล่าวโดยสรุปคือ แม้ว่า พระราชบัญญัติการประกอบข้อมูลเครดิต พ.ศ.2545 จะมีบทบัญญัติเกี่ยวกับการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล แต่ก็เป็นเพียงการรับรองโดยจำกัดไว้แต่เพียงการให้ความคุ้มครองในข้อมูลเครดิตเท่านั้น ไม่ได้คุ้มครองแก่ข้อมูลประเภทอื่น ๆ ด้วยแต่อย่างใด นอกจากนี้ในเรื่องของการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายฉบับนี้ก็ยังมีช่องว่างในส่วนของการที่ผู้ประกอบการอาจใช้ความพยายามเข้าถึงข้อมูลตามหลักการของกฎหมายแต่ได้นำข้อมูลไปใช้ประโยชน์อย่างอื่นนอกเหนือไปจากวัตถุประสงค์ของกฎหมายฉบับนี้นั่นเอง

สำหรับสิทธิของเจ้าของข้อมูลตามกฎหมายฉบับที่สามคือ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ซึ่งเป็นกฎหมายที่มีเจตนารมณ์ในการให้ความคุ้มครองแก่

ระบบคอมพิวเตอร์และข้อมูลในระบบคอมพิวเตอร์ โดยในประเด็นสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลจะเห็นว่า มีการวางหลักการคุ้มครองข้อมูลคอมพิวเตอร์ซึ่งส่วนหนึ่งก็ถือว่าเป็นข้อมูลส่วนบุคคล อย่างไรก็ตาม กฎหมายฉบับนี้ไม่ได้กล่าวถึงสิทธิของเจ้าของข้อมูลและไม่ได้มีการวางหลักการเกี่ยวกับการควบคุมการเก็บรวบรวมข้อมูล การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคล โดยจะเห็นได้จากกรณีการที่มีบุคคลเก็บรวบรวมข้อมูลส่วนบุคคลของบุคคลอื่นโดยเก็บรักษาไว้ในรูปแบบของข้อมูลคอมพิวเตอร์ เช่นนี้ กฎหมายถือว่าเป็นทรัพย์สินของผู้เก็บรวบรวม ซึ่งหากภายหลังมีบุคคลทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติมข้อมูลส่วนบุคคลในรูปของข้อมูลคอมพิวเตอร์โดยมิชอบ แม้เจ้าของข้อมูลที่แท้จริงจะได้รับความเสียหาย ก็ไม่ได้รับความคุ้มครองตามกฎหมายฉบับนี้ นอกจากนี้รูปแบบของการวางหลักการตามกฎหมายฉบับนี้เป็นการกำหนดมาตรการปราบปรามกล่าวคือเป็นการเอาผิดกับการกระทำความผิดที่ได้เกิดแก่ข้อมูลส่วนบุคคลและสร้างความเสียหายแล้วมากกว่าจะเป็นการกำหนดมาตรการในการป้องกัน ดังนั้น จึงกล่าวได้ว่า พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ยังไม่เหมาะสมเพียงพอที่จะเป็นหลักในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลอย่างครบถ้วนและเหมาะสม

นอกจากกฎหมายที่ยกมาอธิบายข้างต้นแล้ว ยังมีกฎหมายฉบับต่าง ๆ ที่รัฐได้ตราออกมาในรูปของกฎหมายมหาชนเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยกับข้อมูลส่วนบุคคลอีกหลายฉบับ ซึ่งหากวิเคราะห์แยกแยะกฎหมายที่ได้ตราออกมาในช่วงระยะเวลานี้ จะพบว่ามีกฎหมายมหาชนที่รัฐได้ตราขึ้นมาเป็น 3 กลุ่มใหญ่ ก็คือ[233]

1) กลุ่มของกฎหมายที่บัญญัติรับรองคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลอย่างชัดแจ้ง เช่น ประมวลกฎหมายแพ่งและพาณิชย์, ประมวลกฎหมายอาญา, พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540, พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ.2545, พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ.2544, พระราชบัญญัติการทะเบียนราษฎร พ.ศ.2534 ฯลฯ เป็นต้น

2) กลุ่มของกฎหมายที่บัญญัติยกเว้นหลักประกันสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลอย่างชัดแจ้ง เช่น พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ.2542, พระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ.2519 (แก้ไขเพิ่มเติม พ.ศ.2545) , พระราชบัญญัติการธนาคารพาณิชย์ พ.ศ.2505

3) กลุ่มของกฎหมายที่การคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลไม่ได้ถูกกำหนดไว้อย่างชัดแจ้ง แต่แฝงอยู่ในรูปของแนวปฏิบัติในการประกอบวิชาชีพ เช่น

---

[233] จันทจิรา เอี่ยมมยุรา, “การคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย,” **วารสารนิติศาสตร์**, หน้า 638.

พระราชบัญญัติขายตรงและตลาดแบบขายตรง พ.ศ.2545, พระราชบัญญัติวิชาชีพบัญชี พ.ศ.2547, พระราชบัญญัติทนายความ พ.ศ.2528, พระราชบัญญัติเกี่ยวกับวิชาชีพต่าง ๆ เช่นเวชกรรม ทันตกรรม เภสัชกรรม การพยาบาลและผดุงครรภ์ ฯลฯ เป็นต้น

จากที่ได้กล่าวมาทั้งหมดข้างต้น สรุปได้ว่า รูปแบบกฎหมายต่าง ๆ ที่ตราออกมานั้น ถือกฎหมายคุ้มครองข้อมูลส่วนบุคคลหลายฉบับ เฉพาะเรื่อง เฉพาะกรณี อยู่ในลักษณะของกฎหมายที่ใช้บังคับกับแต่ละภาคส่วน (Sectorial Law) โดยมีการบัญญัติกฎหมายกระจายไปคุ้มครองข้อมูลส่วนบุคคลประเภทต่าง ๆ ตามที่กำหนดนิยามอยู่ตามพระราชบัญญัติแต่ละฉบับดังที่ได้กล่าวมา ดังนั้นในช่วงระยะเวลานี้จึงยังไม่มีกฎหมายกลางที่วางหลักเกณฑ์ทั่วไปในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ซึ่งแม้ว่าช่วงระยะเวลานี้จะมีพระราชบัญญัติข้อมูลข่าวสารของราชการ ซึ่งถือว่าเป็นการบัญญัติหลักการคุ้มครองสิทธินี้ก็ตาม แต่การคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายนี้มุ่งให้ความคุ้มครองในส่วนของข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของภาครัฐเท่านั้น ทำให้ข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของภาคเอกชนไม่ได้รับความคุ้มครองแต่อย่างใด ส่วนกฎหมายฉบับอื่น ๆ ที่ตราออกมาคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลก็ไม่ได้มีความครอบคลุมทั่วถึงสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลทั้งหมดทุกมิติแต่อย่างใด และนอกจากนี้ในยุคนี้ เรายังไม่เห็นภาพของการกำหนดแบ่งแยกข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) ออกมากำหนดให้ความคุ้มครองเป็นพิเศษแตกต่างจากข้อมูลส่วนบุคคลทั่วไปแต่อย่างใด

4.1.3 ช่วงระยะเวลาหลังการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

กฎหมายคุ้มครองข้อมูลส่วนบุคคล เป็นกฎหมายอีกฉบับหนึ่งที่มีระยะเวลาในการเสนอเพื่อให้มีการตรากฎหมายผ่านสภาอย่างยาวนาน กล่าวคือ นับจากระยะเวลาที่เริ่มปรากฏแนวคิดในการรับรองสิทธิในความเป็นส่วนตัว ก็คือ รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช2517 ที่มีการบัญญัติรับรองและคุ้มครองการติดต่อสื่อสารถึงกันโดยทางไปรษณีย์ ได้แก่จดหมาย โทรเลข โทรศัพท์ หรือสิ่งสื่อสารอื่นใดที่บุคคลติดต่อถึงกัน ไว้ในมาตรา 46 และต่อมาในรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2535 (แก้ไขเพิ่มเติม ฉบับที่ 5 พุทธศักราช 2538) ได้มีการบัญญัติรับรองและคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว ไว้ในมาตรา 47 จนกระทั่งถึง รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540 ก็ได้มีการบัญญัติรับรองและคุ้มครองสิทธิในข้อมูลข่าวสารไว้ในมาตรา 34 และมาตรา 58 ดังที่ได้กล่าวไว้ในตอนต้น จนกระทั่งถึงรัฐธรรมนูญฉบับปัจจุบัน คือ รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ก็ยังคงมีการบัญญัติรับรองและคุ้มครองสิทธินี้ กล่าวคือ

> มาตรา 32 บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว การกระทำอันเป็นการละเมิดหรือกระทบต่อสิทธิของบุคคลตามวรรคหนึ่ง หรือการนำข้อมูล ส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใด ๆ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย ที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ

แต่อย่างไรก็ดี ภายใต้หลักการข้างต้นถือเป็นการรับรองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลไว้ในฐานะเป็นสิทธิในความเป็นส่วนตัว ซึ่งเป็นสิทธิเสรีภาพที่รัฐธรรมนูญได้บัญญัติรับรองไว้ จึงเป็นสิทธิที่จะต้องได้รับการเคารพ จากทั้งภาครัฐและปัจเจกชน แต่ทว่าสิทธินี้ไม่ใช่สิทธิเด็ดขาด โดยรัฐสามารถที่จะกำหนดมาตรการหรือกระทำการบางอย่างที่มีลักษณะเป็นการล่วงละเมิดหรือแทรกแซงสิทธินี้ได้บนพื้นฐานของหลักการสำคัญ 3 ประการคือ[234]

ประการแรก หลักความโปร่งใส (Transparency) โดยรัฐหรือองค์กรของรัฐจะดำเนินมาตรการใด ๆ อันมีผลเป็นการแทรกแซงสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลได้ก็ต่อเมื่อมีกฎหมายบัญญัติให้กระทำได้ เพื่อให้ประชาชนผู้เป็นเจ้าของสิทธิจะได้ทราบล่วงหน้าว่าสถานการณ์เช่นไรที่สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของตนจะถูกแทรกแซงโดยรัฐและการดำเนินการเช่นนั้นจะต้องเป็นไปภายใต้เงื่อนไขและหลักเกณฑ์เช่นไร

ประการที่สอง หลักประโยชน์สาธารณะ (Public Interest) โดยการที่รัฐหรือองค์กรของรัฐจะดำเนินมาตรการอันมีผลเป็นการแทรกแซงสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนั้นจะต้องเป็นไปเพื่อประโยชน์สาธารณะเกี่ยวกับความมั่นคงแห่งรัฐ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ เพื่อดูแลความสงบเรียบร้อยหรือการกระทำความผิดอาญา เพื่อคุ้มครองสุขภาพหรือศีลธรรม หรือเพื่อคุ้มครองสิทธิและเสรีภาพของบุคคลอื่น กล่าวอีกนัยหนึ่งก็คือประโยชน์สาธารณะจะต้องมีสถานะเหนือกว่าประโยชน์ส่วนตัวของบุคคล

ประการที่สาม หลักความจำเป็นและความได้สัดส่วน (Necessity and Proportionality) โดยที่มาตรการของรัฐหรือองค์กรของรัฐที่จะดำเนินการและมีผลเป็นการแทรกแซงสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลจะต้องเป็นสิ่งที่จำเป็นเพื่อให้บรรลุวัตถุประสงค์อันเป็นประโยชน์สาธารณะ และจะต้องได้สัดส่วนกันกับผลกระทบที่เกิดขึ้นจากการดำเนินมาตรการดังกล่าว ทั้งนี้เพื่อให้มาตรการเช่นนั้นก่อให้เกิดผลกระทบต่อสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลน้อยที่สุด อีกทั้งจะต้องมีมาตรการเยียวยาความเสียหายแก่บุคคลนั้นในกรณีที่หากว่ามีความเสียหายเกิดขึ้นแก่สิทธิเกินสมควรด้วย

---

[234] นนทวัชร์ นวตระกูลพิสุทธิ์, *เรื่องเดิม,* หน้า 742.

ภายใต้ข้อจำกัดในทางกฎหมายของระบบกฎหมายไทยที่ได้กล่าวมาแล้วในสองช่วงระยะเวลาตอนต้นนั้น จะเห็นว่า แม้มีบทบัญญัติของรัฐธรรมนูญรับรองสิทธิในความเป็นส่วนตัวไว้ก็ตามแต่รัฐธรรมนูญเองก็ได้เปิดโอกาสให้รัฐหรือองค์กรของรัฐสามารถมีการออกกฎหมายหรือมีมาตรการต่าง ๆ มาจำกัดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลได้ หรือแม้ว่าจะมีการตรากฎหมายเฉพาะออกมาคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในบางกรณีหรือเฉพาะเรื่องก็ตาม แต่ลักษณะของการคุ้มครองสิทธิก็ยังมีปัญหาในทางกฎหมายรวมถึงปัญหาในทางปฏิบัติมากมายดังที่ได้กล่าวไว้แล้ว

สำหรับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ซึ่งถือว่าเป็นกฎหมายในลักษณะของบทกฎหมายทั่วไปซึ่งตราขึ้นมารับรองคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในภาพรวมและทุกมิติอันจะมีลักษณะครอบคลุมนั้นได้มีการริเริ่มที่จะตราขึ้นเป็นกฎหมาย นับตั้งแต่ปี พ.ศ.2540 ก็ยังไม่สามารถตราขึ้นเป็นกฎหมายได้รวมระยะเวลากว่า 20 ปี จนกระทั่งเมื่อวันที่ 28 กุมภาพันธ์ พ.ศ.2562 บทบัญญัติแห่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลซึ่งก็คือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ก็ได้ผ่านความเห็นชอบจากสภานิติบัญญัติแห่งชาติด้วยคะแนนเสียงเป็นเอกฉันท์โดยหลักการและเหตุผลของพระราชบัญญัติ มีว่า

> เนื่องจากปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคล เป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคล อันเป็นการล่วงละเมิดดังกล่าวสามารถทำได้โดยง่าย สะดวก และรวดเร็ว รวมทั้งก่อให้เกิด ความเสียหายต่อเศรษฐกิจโดยรวมที่ใช้เทคโนโลยีดิจิทัลอย่างแพร่หลาย แม้ว่าจะได้มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลในบางเรื่อง แต่ก็ยังไม่มีหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป สมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครอง ข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้น จึงจำเป็นต้องตราพระราชบัญญัตินี้

หากวิเคราะห์แล้วจะเห็นว่าเหตุผลสำคัญที่ประเทศไทยมีความจำเป็นมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ ก็คือ

1. ปัจจุบันประเทศไทยยังไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคล ซึ่งทำให้ไม่มีหลักประกันในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ซึ่งเป็นสิทธิมนุษยชนขั้นพื้นฐานในขณะที่นานาอารยประเทศ ไม่ว่าจะเป็นประเทศในแถบยุโรป อเมริกาใต้ ได้มีการตรากฎหมายเพื่อ

มาคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลและวางระบบการเยียวยาความเสียหายอันเกิดจากละเมิดเป็นที่เรียบร้อยแล้ว

2. จัดสร้างกลไกในการปกป้องสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล โดยพยายามรักษาดุลยภาพของการคุ้มครองสิทธิของบุคคลในความเป็นส่วนตัว (Right of Privacy) เสรีภาพในการไหลเวียนของข้อมูลข่าวสาร (Free Flow of Information) และความมั่นคงของประเทศ (National Security) เพื่อเป็นโครงสร้างพื้นฐานสารสนเทศที่มั่นคงในช่วงระยะเวลาแห่งข้อมูลข่าวสาร ภายใต้หลักการปกครองระบอบประชาธิปไตย และหลักนิติรัฐ

3. เพื่อสนับสนุนการทำธุรกรรมทางอิเล็กทรอนิกส์ เนื่องในปัจจุบันการพัฒนาการทางเทคโนโลยีสารสนเทศมีความก้าวหน้าอย่างรวดเร็ว ทำให้มีการนำเอาเทคโนโลยีมาประยุกต์ใช้ให้เกิดประโยชน์กับเศรษฐกิจและสังคมมากมาย โดยเฉพาะการประมวลผลข้อมูลส่วนบุคคลอันสามารถทำได้อย่างสะดวกและรวดเร็ว จึงมีความจำเป็นออกกฎหมายมาคุ้มครองข้อมูลส่วนบุคคล ซึ่งมีการใช้อย่างแพร่หลายในยุคสังคมสารสนเทศ

4. เพื่อปรับตัวให้สอดคล้องกับการออกกติกาของสหภาพยุโรป (EU) ซึ่งก็คือ GDPR อันมีลักษณะของการเป็น Normative Power[235] และมีขอบเขตการบังคับออกไปนอกพื้นที่ของสหภาพยุโรป ส่งผลให้ภาคธุรกิจรวมถึงรัฐที่มีการติดต่อปฏิสัมพันธ์ในทางการค้ากับสหภาพยุโรปต้องเร่งรีบปรับตัวโดยการตรากฎหมายที่มีมาตรฐานของการคุ้มครองข้อมูลส่วนบุคคลไม่ต่ำไปกว่าที่กำหนดโดย GDPR

ดังนั้น พระราชบัญญัติฉบับนี้ มีเป้าหมายเพื่อเป็นการพัฒนาและกำหนดนโยบาย มาตรการ กฎเกณฑ์ด้านการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้ประเทศไทยสามารถมีหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป อันจะช่วยสร้างความเชื่อมั่นให้กับบุคคลที่เกี่ยวข้องทั้งภาครัฐ ภาคเอกชน และภาคประชาชน และเพื่อเป็นการเตรียมการด้านการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย รวมทั้งเตรียมความพร้อมเพื่อรองรับผลกระทบด้านต่าง ๆ ของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศที่มีผลกระทบต่อประเทศไทยอย่างทันท่วงที กล่าวอีกนัยหนึ่งก็คือพระราชบัญญัติฉบับนี้มีเป้าหมายเพื่อทำให้สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประชาชนได้รับการคุ้มครองได้จริง อันจะเป็นผลดีต่อประโยชน์ของปัจเจกบุคคลเองและต่อการยอมรับในระดับสากล

แต่อย่างไรก็ดี สาระสำคัญของ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 นี้ ก็ยังมีประเด็นที่จะต้องพิจารณาอีกหลายประการที่สำคัญ ซึ่งจะได้อธิบายในหัวข้อต่อไปตามลำดับ

---

[235] กันยภัทร รัตนวิลาส, **มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลในฐานะเครื่องมือสร้างบรรทัดฐานของอียู**, ค้นวันที่ 20 กันยายน 2561 จาก https://www.the101.world/gdpr-insight/

4.2 การกำหนดนิยามและขอบเขตของความหมายของคำว่า “สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล” ของประเทศไทย

4.2.1 การกำหนดนิยามความหมายในระบบกฎหมายไทย

สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ถือเป็นสิทธิมนุษยชนของเจ้าของข้อมูลที่มีอยู่เหนือข้อมูลส่วนบุคคลของตน ซึ่งนิยามความหมายและขอบเขตของสิทธินี้จะมีเพียงใดก็ขึ้นอยู่กับการที่ระบบกฎหมายยอมรับว่าความหมายของคำว่า ข้อมูลส่วนบุคคล หรือ Personal Data นั้นมีความหมายเพียงใด โดยยังเป็นประเด็นถกเถียงกันในทางวิชาการอยู่และกฎหมายของแต่ละประเทศก็ได้กำหนดคำนิยามแตกต่างกันออกไปดังที่ได้กล่าวไว้แล้วในบทก่อนหน้า โดยในมิติของการแบ่งความหมายของข้อมูลส่วนบุคคลนั้น

จะเห็นว่าในประเทศที่ไม่ได้มีการบัญญัติกฎหมายกลางในการคุ้มครองข้อมูลส่วนบุคคล จะมีการกำหนดให้ความหมายของข้อมูลส่วนบุคคลในความหมายที่แคบ และจะมีการกำหนดนิยามเป็นเรื่อง ๆ โดยเฉพาะดังจะเห็นได้จากกรณีของประเทศสหรัฐอเมริกา แต่สำหรับประเทศในกลุ่มสหภาพยุโรปและประเทศอื่น ๆ เช่น อังกฤษ ออสเตรเลีย ก็จะมีการให้ความหมายในลักษณะอย่างกว้างเอาไว้ดังจะเห็นตัวอย่างได้ชัดจากกรณีของ EU Directive และ GDPR จะมีการกำหนดให้นิยามไว้ในลักษณะอย่างกว้าง

เมื่อมาพิจารณาในระบบกฎหมายของประเทศไทย จะเห็นรูปแบบของการกำหนดนิยามไว้ทั้งสองลักษณะ คือ มีกฎหมายกลางกำหนดนิยามความหมายของข้อมูลส่วนบุคคลไว้อย่างกว้าง และมีกฎหมายเฉพาะกำหนดนิยามไว้เฉพาะเป็นเรื่อง ๆ หรือกรณี ๆ ไป ดังจะเห็นได้ดังนี้

1. การกำหนดนิยามในลักษณะอย่างกว้างตามกฎหมายกลาง

กรณีนี้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 6 ที่กำหนดบทนิยาม คำว่า “ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

2. การกำหนดนิยามไว้อย่างแคบในกฎหมายเฉพาะฉบับต่าง ๆ

กรณีนี้จะมีการกำหนดในกฎหมายเฉพาะหลายฉบับ ยกตัวอย่างเช่น พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 ได้มีการกำหนดนิยามของข้อมูล โดยกำหนดไว้ให้ คำว่า “ข้อมูลข่าวสาร” หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริง ข้อมูล หรือสิ่งใด ๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้ และคำว่า “ข้อมูล

ข่าวสารส่วนบุคคล” หมายความว่า ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้นหรือมีเลขหมายรหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึก ลักษณะเสียงของคนหรือรูปถ่าย และให้หมายรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ถึงแก่กรรมแล้วด้วย[236]

พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ.2545 ได้กำหนดให้ “ข้อมูล” หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงของข้อมูลเครดิตไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเอง หรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์มการบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้[237]

พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ.2550 แม้ไม่มีการกำหนดนิยามของคำว่า “ข้อมูลด้านสุขภาพไว้” แต่ได้มีการกำหนดหลักการคุ้มครองในมาตรา 7 ว่า ข้อมูลด้านสุขภาพของบุคคลเป็นความลับส่วนบุคคล ผู้ใดจะนำไปเปิดเผยในประการที่น่าจะทำให้บุคคลนั้นเสียหายไม่ได้ เว้นแต่การเปิดเผยนั้นเป็นไปตามความประสงค์ของบุคคลนั้นโดยตรง หรือมีกฎหมายเฉพาะบัญญัติให้ต้องเปิดเผย แต่ไม่ว่าในกรณีใด ๆ ผู้ใดจะอาศัยอำนาจหรือสิทธิตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการหรือกฎหมายอื่นเพื่อขอเอกสารเกี่ยวกับข้อมูลด้านสุขภาพของบุคคลที่ไม่ใช่ของตนไม่ได้ ในกรณีนี้จึงพอจะสรุปความหมายของ “ข้อมูลส่วนบุคคลด้านสุขภาพ” ได้ว่า หมายถึง ข้อมูลส่วนบุคคลที่บันทึกไว้ในเรื่องเกี่ยวกับสุขภาพ ไม่ว่าจะเป็นในทางด้านกายภาพหรือด้านจิตใจของบุคคลซึ่งสามารถระบุตัวบุคคลได้ และมีลักษณะเป็นข้อมูลที่มีความอ่อนไหว นั่นเอง

ประเด็นปัญหาจึงมีว่า หากนิยามของข้อมูลส่วนบุคคล ซึ่งควรจะอยู่ในบังคับของกฎหมายเฉพาะ แต่การกำหนดนิยามของข้อมูลส่วนบุคคลนั้นไปไม่ถึงความหมายตามตัวบทของกฎหมายเฉพาะที่เขียนนิยามไว้ ข้อมูลส่วนบุคคลนั้น ควรจะอยู่ในบังคับความคุ้มครองตามกฎหมายฉบับใด กรณีนี้เห็นว่า ข้อมูลส่วนบุคคลใดอยู่ภายใต้นิยามของกฎหมายเฉพาะ ก็จะได้รับความคุ้มครองตามมาตรฐานที่กำหนดไว้ในกฎหมายเฉพาะ แต่หากข้อมูลส่วนบุคคลใดไม่อยู่ภายใต้นิยามของกฎหมายเฉพาะก็จะได้รับความคุ้มครองตามกฎหมายทั่วไปอันเป็นกฎหมายกลาง

เมื่อพิจารณาถึงบทนิยามต่าง ๆ ที่กล่าวมาข้างต้น เปรียบเทียบกับการกำหนดบทนิยามของคำว่า ข้อมูลส่วนบุคคล ของ GDPR ที่กำหนดว่า หมายถึง ข้อมูลของบุคคลธรรมดาที่ยังมีชีวิตอยู่และทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าโดยทางตรงหรือทางอ้อม ตัวอย่างเช่น ชื่อ หมายเลขประจำตัว

---

[236] มาตรา 4 แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540

[237] มาตรา 3 แห่งพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ.2545

ข้อมูลสถานที่อยู่ การระบุตัวตนออนไลน์ หรือปัจจัยอย่างหนึ่งหรือหลายอย่างที่กล่าวต่อไปนี้อันจะทำให้สามารถระบุลักษณะทางกายภาพ ลักษณะทางพันธุกรรม สภาพจิต เศรษฐกิจ วัฒนธรรม หรือสังคมของบุคคลธรรมดานั้น ก็ให้ถือว่าเป็นข้อมูลส่วนบุคคลทั้งสิ้น[238] จะเห็นว่ามีลักษณะของการกำหนดบทนิยามใกล้เคียงกัน และนอกจากนี้จะเห็นว่า มีการลดและตัดคำนิยามในส่วนของผู้เป็นเจ้าของข้อมูลส่วนบุคคล โดยในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลจะไม่ได้ให้สิทธิแก่ทายาทหรือคู่สมรสในกรณีที่เจ้าของข้อมูลผู้ถึงแก่กรรมแต่อย่างใด

ประเด็นต่อมา เมื่อพิจารณาตามเนื้อหาของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แล้ว จะเห็นว่าเริ่มมีการกำหนดประเภทของข้อมูลที่เรียกว่า ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) ไว้ในระบบกฎหมายไทยอย่างชัดเจน โดยในกฎหมายได้มีการจำแนกข้อมูลส่วนบุคคลเป็น 2 ประเภทคือ ข้อมูลส่วนบุคคลทั่วไป (General Data) และข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) อันเป็นข้อมูลที่มีความละเอียดอ่อนและสุ่มเสี่ยงที่หากมีการเข้าถึงข้อมูลแล้วก็อาจจะมีการนำข้อมูลไปใช้ในลักษณะของการเลือกปฏิบัติหรือการล่วงละเมิดสิทธิหรือก่ออันตรายในประการต่าง ๆ แก่เจ้าของข้อมูล ดังนั้นประเด็นนี้ในมิติของกฎหมายฉบับนี้ก็ได้วางหลักการไปในแนวทางเดียวกันกับหลักการสากลต่าง ๆ ไม่ว่าจะเป็น GDPR หรือกฎหมายของต่างประเทศ กล่าวคือ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลได้กำหนดให้ความคุ้มครองแก่เจ้าของข้อมูลที่เป็นบุคคลธรรมดา และกำหนดหลักการคุ้มครองไว้เป็นพิเศษกว่าข้อมูลธรรมดา โดยมีการกำหนดลักษณะข้อมูลส่วนบุคคลที่มีความอ่อนไหวว่าหมายถึง ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ ฯลฯ เป็นต้น

โดยตามมาตรา 26 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลแล้ว กำหนดความคุ้มครองไว้มากกว่าข้อมูลส่วนบุคคลธรรมดา โดยมีการกำหนดว่า ผู้อื่นจะเก็บข้อมูลเหล่านี้ได้ต้องได้รับ “ความยินยอมโดยชัดแจ้ง” จากเจ้าของข้อมูล แต่อย่างไรก็ดี กฎหมายยังไม่ได้ให้นิยามเอาไว้ว่า ความยินยอมโดยชัดแจ้งต่างจากความยินยอมในกรณีปกติอย่างไร ทั้งนี้เพราะความยินยอมในกรณีปกติก็

---

[238] “personal data” means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

ต้องเป็นความยินยอมที่ทำเป็นหนังสืออยู่แล้ว ดังนั้นประเด็นนี้จึงเป็นรายละเอียดที่จะต้องมีการประกาศหลักเกณฑ์ที่เป็นรายละเอียดออกมาเพื่อความชัดเจนต่อไป

จากที่กล่าวมา แม้ว่าในส่วนของข้อมูลส่วนบุคคลที่มีความอ่อนไหวจะได้รับการกำหนดมาตรการคุ้มครองสิทธิให้แก่เจ้าของข้อมูลมากกว่าข้อมูลส่วนบุคคลทั่วไปก็ตาม แต่เมื่อพิจารณามาตรา 26 และมาตรา 27 และก็จะพบว่าได้มีการกำหนดข้อยกเว้นไว้อีกหลายประการกล่าวคือ การเก็บข้อมูลและใช้ข้อมูลที่มีความอ่อนไหวในกิจการต่อไปนี้ ไม่ต้องขอความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล

1. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล ซึ่งเจ้าของข้อมูลไม่สามารถให้ความยินยอมได้

2. การดำเนินกิจการขององค์กรไม่แสวงหาผลกำไร เช่น มูลนิธิ สมาคม ที่ทำงานด้านการเมือง ศาสนา ปรัชญา สหภาพแรงงาน ให้แก่สมาชิกหรือผู้ที่ติดต่ออย่างสม่ำเสมอ และองค์กรนั้น ๆ ไม่ได้เปิดเผยข้อมูลออกไปภายนอก

3. ข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูล

4. เป็นการจำเป็นเพื่อก่อตั้งสิทธิเรียกร้อง หรือการดำเนินคดี การต่อสู้คดีตามกฎหมาย

5. เป็นการจำเป็นในการปฏิบัติตามกฎหมาย เพื่อประเมินความสามารถของลูกจ้างในการทำงาน การวินิจฉัยโรคทางการแพทย์ การให้บริการสุขภาพ การรักษาทางการแพทย์ การป้องกันโรคติดต่อ การคุ้มครองแรงงาน สวัสดิการรักษาพยาบาล การวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ สถิติ ฯลฯ และเพื่อประโยชน์สาธารณะที่สำคัญ โดยจัดให้มีมาตรการคุ้มครองข้อมูลที่เหมาะสมด้วย

จากข้อเว้นที่กล่าวมา เมื่อพิจารณาตามหลักสากลและกฎหมายของต่างประเทศแล้ว จะเห็นว่า ข้อควรระวัง สำหรับข้อมูลที่มีความอ่อนไหวนั้น ควรได้รับความคุ้มครองเป็นพิเศษที่เข้มข้นมากกว่าข้อมูลอื่น ๆ แต่เมื่อพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล มาตรา 24 (5) กำหนดยกเว้นสำหรับกิจการ “เพื่อประโยชน์สาธารณะที่สำคัญ” ให้สามารถเก็บข้อมูลและใช้ข้อมูลได้โดยไม่ต้องได้รับความยินยอมอย่างชัดแจ้ง ก็เท่ากับเป็นการเปิดช่องให้กิจการของหน่วยงานรัฐทั้งหลาย ยกประโยชน์สาธารณะขึ้นมาอ้างได้ว่า ภารกิจของหน่วยงานของตนนั้น มีความสำคัญในลักษณะเป็นประโยชน์สาธารณะ ซึ่งก็จะมีผลทำให้ข้อมูลที่มีความอ่อนไหว ก็จะไม่ได้รับการคุ้มครองจากการสอดส่องของภาครัฐได้เลย ดังนั้นในการตีความคำว่า “ประโยชน์สาธารณะที่สำคัญ” อันจะเกิดขึ้นต่อไปในอนาคต หน่วยงานที่เกี่ยวข้องกับการตีความบังคับใช้กฎหมายฉบับนี้ ควรจะตระหนักถึงเจตนารมณ์ของกฎหมายและให้ความสำคัญต่อความปลอดภัยของข้อมูลของประชาชนด้วย

4.2.2 ขอบเขตของ “สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล”ที่ได้รับความคุ้มครองในประเทศไทย

ในประเด็นขอบเขตของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล จะเห็นได้ว่า โดยธรรมชาติของสิทธิในความเป็นส่วนตัวในฐานะที่เป็นสิทธิมนุษยชนนั้น สามารถแบ่งได้เป็นในส่วนที่เป็น Status Negativus ที่เป็นข้อห้ามมิได้รัฐหรือบุคคลใด ๆ เข้ามาแทรกแซงหรือล่วงละเมิด อันมีลักษณะของการเป็นสิทธิที่จะอยู่คนเดียว หรือ Right to be Let Alone แต่ในขณะเดียวกันสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลก็มีส่วนที่เป็น Status Positivus ด้วย คือในกรณีของสิทธิในการควบคุมการไหลเวียนของข้อมูลส่วนบุคคลของตนเองนั้น โดยธรรมชาติ เจ้าของข้อมูลย่อมไม่อาจที่จะควบคุมการไหลเวียนได้เอง เพราะข้อมูลส่วนบุคคลไม่ได้อยู่แต่เฉพาะที่ตัวเจ้าของข้อมูลเท่านั้น ดังนั้น กรณีนี้จึงเป็นหน้าที่ของรัฐหรือผู้ควบคุมข้อมูลหรือภาคเอกชนที่เกี่ยวข้องอื่น ๆ จะต้องเป็นผู้ที่มีหน้าที่ และรัฐจะต้องเป็นผู้ทำให้สิทธิในส่วนนี้ได้รับความคุ้มครองอย่างแท้จริง โดยเจ้าของข้อมูลจะต้องทราบ เมื่อข้อมูลส่วนบุคคลไปอยู่ที่ใด เจ้าของข้อมูลก็มีสิทธิที่จะรู้และมีสิทธิควบคุมไม่ให้มีการไหลเวียนได้

อย่างไรก็ดี สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนี้ ไม่ได้มีฐานะเป็นสิทธิโดยสมบูรณ์ (Absolute Right) ที่จะมีการจำกัดไม่ได้ แต่สิทธิสามารถถูกจำกัดได้ภายใต้เงื่อนไขของประโยชน์สาธารณะบนพื้นฐานของหลักความได้สัดส่วนหรือความสมเหตุสมผล ซึ่งในประเด็นนี้จึงจำเป็นจะต้องมีการจำแนกประเภทของข้อมูล และทำความเข้าใจกับประเภทของข้อมูลว่ามีลักษณะเช่นไร เพื่อให้การกำหนดข้อยกเว้นมาจำกัดสิทธินั้นตั้งอยู่บนพื้นฐานของความเข้าใจธรรมชาติของการจัดเก็บ การรวบรวม การประมวลผล และการใช้ข้อมูลในแต่ละประเภท ตัวอย่างเช่น การวางหลักการคุ้มครองรวมถึงการกำหนดข้อจำกัดของ ข้อมูลที่ไม่ได้อ่อนไหว เช่น ข้อมูลทางพันธุกรรม เมื่อผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลจะนำมาใช้ในการวิเคราะห์เพื่อให้เกิดประโยชน์สาธารณะนั้น ก็ไม่จำต้องให้ความคุ้มครองสิทธิในข้อมูลส่วนบุคคลนี้เท่ากับข้อมูลส่วนบุคคลในทางการแพทย์ ซึ่งเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวและมีลักษณะของข้อมูลที่ไม่เหมือนกัน

สำหรับหลักการเบื้องต้นในแง่ของขอบเขตการบังคับใช้กฎหมายก็คือ กฎหมายฉบับนี้จะใช้บังคับแก่การเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลที่เกิดขึ้นในราชอาณาจักร และครอบคลุมถึงกรณีผู้ควบคุมและผู้ประมวลผลอยู่นอกราชอาณาจักร หากมีกิจกรรม ดังนี้คือ ประการแรก เสนอขายสินค้าหรือบริการแก่เจ้าของข้อมูลซึ่งอยู่ในราชอาณาจักรไม่ว่าจะมีการชำระเงินหรือไม่ และประการที่สองก็คือ การเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลที่เกิดขึ้นในราชอาณาจักร

แต่อย่างไรก็ดี กฎหมายฉบับนี้ได้มีการกำหนดข้อจำกัด หรือข้อยกเว้นของการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลไว้ใน มาตรา 4 โดยได้บัญญัติว่าพระราชบัญญัตินี้ไม่ใช้บังคับแก่

1. บุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น โดยมิให้ผู้อื่นใช้ข้อมูลส่วนบุคคล หรือเปิดเผยข้อมูลส่วนบุคคลนั้นต่อผู้อื่น

2. การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐหรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงินหรือนิติวิทยาศาสตร์

3. บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมไว้เฉพาะเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น

4. สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าว ซึ่งเก็บรวมรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมาธิการ แล้วแต่กรณี

5. การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

6. การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

จากหลักการของมาตรา 4 ของพระราชบัญญัตินี้ มีประเด็นที่น่าสนใจ คือ การไม่ให้กฎหมายใช้บังคับกับข้อมูลส่วนบุคคลทั้งหมดในกิจการตามมาตรา 4 วรรค 1 ใน (2) - (6) ซึ่งมีข้อกังวลว่าจะเป็นการยกเว้นที่กว้างขวางเกินไป และไม่เป็นไปตามหลักความได้สัดส่วนและเกินกรณีแห่งความจำเป็น อีกทั้งข้อมูลส่วนบุคคลในกิจการต่าง ๆ ดังกล่าว สามารถอยู่ภายในบังคับกฎหมายฉบับนี้ได้ไม่ต้องยกเว้นไปทั้งหมดในทุกกิจการ นอกจากนี้ยังมีประเด็นที่น่าพิจารณาเพิ่มเติมคือ[239]

1. การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐหรือการรักษาความปลอดภัยของประชาชน ตาม มาตรา 4 (2) มีหลักการอันสอดคล้องกับหลักสากลซึ่งเป็นที่ยอมรับได้ แต่ภาษาที่ใช้อาจไม่ชัดเจนเพียงพอ ซึ่งขอบเขตข้อนี้เป็นข้อใหม่ที่ ในชั้นเป็นร่างพระราชบัญญัติ ในเดือนมกราคม พ.ศ.2561 ยังไม่มีปรากฏ และเพิ่งเพิ่มเนื้อหาเข้ามาใหม่ในร่างพระราชบัญญัติ ที่ปรับปรุงในเดือนกันยายน พ.ศ.2561 ก่อนที่พระราชบัญญัติจะผ่านรัฐสภาออกมา

---

[239] เครือข่ายพลเมืองเน็ต, **ความคิดเห็นต่อร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.... (ก.ย. 2561)**, ค้นวันที่ 12 ธันวาคม 2561 จาก https://thainetizen.org/docs/data-protection-bill-comments-20180920/

ในที่สุด โดยในประเด็นนี้คณะผู้ร่างกฎหมายได้อธิบายระหว่างการนำเสนอในวันที่ 11 กันยายน พ.ศ. 2561 ว่า หากพิจารณาตามกฎหมาย General Data Protection Regulation ของสหภาพยุโรป ใน Article 2 ที่ว่าด้วยขอบเขตสิ่งที่คุ้มครอง (Material Scope)[240] ซึ่งน่าสนใจว่า GDPR Article 2 Material Scope นั้นยกเว้นการบังคับใช้ไว้เพียง 4 ข้อ ดังระบุใน Article 2(2)[241] โดยในส่วนของ Article 2(2) ข้อ d) ซึ่งยกเว้นการประมวลผลข้อมูลส่วนบุคคล “โดยหน่วยงานที่มีอำนาจหน้าที่และความสามารถ เพื่อประโยชน์แห่งการป้องกัน การสืบสวน การตรวจหา หรือการฟ้องคดีอาญา หรือการบังคับคดีทางอาญา รวมถึงการพิทักษ์หรือป้องกันไม่ให้เกิดภัยคุกคามต่อความปลอดภัยของสาธารณะ” (By competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security) ซึ่งข้อนี้มีความใกล้เคียงกับมาตรา 4 (2)

หากพิจารณาตัวอย่างตาม Material Scope ของ General Data Protection Reguration แล้ว จะเห็นได้ว่า ข้อยกเว้นที่ไม่เกี่ยวกับบริบทของสหภาพยุโรปนั้น มีเพียง 2 ข้อ คือข้อยกเว้นเพื่อการใช้ในครัวเรือนและข้อยกเว้นเพื่อความปลอดภัยสาธารณะ ซึ่งคำว่า “Public Security” (ความ

---

[240] กระทรวงดิจิตอลเพื่อเศรษฐกิจและสังคม, **คำชี้แจงร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล**, ค้นวันที่ 30 กันยายน 2561 จาก http://bit.ly/2QkSLSG

[241] Article 2 Material scope

1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Regulation does not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law;

(b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;

(c) by a natural person in the course of a purely personal or household activity;

(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

ปลอดภัยของสาธารณะ) และไม่ใช่ “ความมั่นคงของรัฐ” ดังที่ปรากฏในพระราชบัญญัติที่ผ่านสภาออกมาแต่อย่างใด

2. คำว่า กิจการสื่อมวลชน ตาม มาตรา 4 (3) ไม่จำเป็นต้องได้รับการยกเว้นการบังคับใช้ทั้งกิจการ โดยเหตุผลสองประการคือ ประการแรก สื่อมวลชนสามารถเก็บรวบรวมข้อมูลส่วนบุคคลได้อยู่แล้ว ตามข้อยกเว้นใน มาตรา 24 ซึ่งระบุว่า “(1) เพื่อประโยชน์ที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งเป็นไปเพื่อประโยชน์สาธารณะและได้เก็บข้อมูลส่วนบุคคลเพื่อการนั้นไว้เป็นความลับ” “(5) เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล” และ “(6) เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล” รวมถึงข้อยกเว้นตามมาตรา 25 และ 26 และประการที่สอง สื่อสารมวลชนสามารถใช้และเปิดเผยข้อมูลส่วนบุคคลได้ตามข้อยกเว้นที่ระบุไว้ในมาตรา 27

3. สำหรับกิจการซึ่งเป็น “สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าว” ในมาตรา 4 (4) ไม่จำเป็นต้องได้รับการยกเว้นการบังคับใช้ทั้งกิจการ ทั้งนี้เพราะว่า สภาฯ สามารถเก็บรวบรวมข้อมูลส่วนบุคคลได้อยู่แล้ว ตามข้อยกเว้นในมาตรา 24 ทั้งในข้อ (1) (3) (5) (6) และ “(7) เป็นการปฏิบัติตามกฎหมายหรือการใช้อำนาจรัฐของผู้ควบคุมข้อมูลส่วนบุคคล” รวมถึงข้อยกเว้นตามมาตรา 25 และ 26 นอกจากนี้ กิจการเกี่ยวกับรัฐสภา สามารถใช้และเปิดเผยข้อมูลส่วนบุคคลได้ตามข้อยกเว้นที่ระบุไว้ใน มาตรา 27

4. สำหรับการพิจารณาพิพากษาคดีของศาล และเจ้าหน้าที่ตามกระบวนการยุติธรรมทางอาญา” ในมาตรา 4 (5) และการดำเนินงานตาม “หน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงินหรือนิติวิทยาศาสตร์” ในมาตรา 4 (2) ไม่จำเป็นต้องได้รับการยกเว้นการบังคับใช้ทั้งกิจการ ทั้งนี้เพราะว่า ศาลและเจ้าหน้าที่ในกระบวนการยุติธรรม การป้องกัน การปราบปราม และนิติวิทยาศาสตร์ สามารถเก็บรวบรวมข้อมูลส่วนบุคคลได้อยู่แล้ว ตามข้อยกเว้นในมาตรา 24, 25, และ 26 อีกทั้งศาลและเจ้าหน้าที่ในกระบวนการยุติธรรม สามารถใช้และเปิดเผยข้อมูลส่วนบุคคลได้ตามข้อยกเว้นที่ระบุไว้ในมาตรา 27

5. การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต ในมาตรา 4 (6) ไม่จำเป็นต้องได้รับการยกเว้นการบังคับใช้ทั้งกิจการ ทั้งนี้เพราะเหตุผลดังต่อไปนี้คือ

1) กิจการข้อมูลเครดิตสามารถเก็บรวบรวมข้อมูลส่วนบุคคลได้อยู่แล้ว ตามข้อยกเว้นในมาตรา 24 ซึ่งระบุว่า “(4) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น” “(6) เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล [...] เว้นแต่

ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล” และ “(7) เป็นการปฏิบัติตามกฎหมายหรือการใช้อำนาจรัฐของผู้ควบคุมข้อมูลส่วนบุคคล” รวมถึงข้อยกเว้นตามมาตรา 25 และ 26

2) กิจการข้อมูลเครดิตสามารถใช้และเปิดเผยข้อมูลส่วนบุคคลได้ตามข้อยกเว้นที่ระบุไว้ในมาตรา 24 อาศัยอำนาจตามมาตรา 27 เช่น การส่งข้อมูลให้กับหน่วยงานปราบปรามการฟอกเงินก็สามารถใช้ข้อยกเว้นตามมาตรา 24 (7) (ประกอบกับมาตรา 20 ของพระราชบัญญัติประกอบธุรกิจข้อมูลเครดิต) หรือการนำข้อมูลไปสร้างแบบจำลองด้านเครดิต ก็สามารถใช้ข้อยกเว้นตามมาตรา 24 (6) (ประกอบกับมาตรา 20/1 ของพระราชบัญญัติประกอบธุรกิจข้อมูลเครดิต) ได้ ซึ่งสถาบันการเงินซึ่งเป็นสมาชิกของบริษัทข้อมูลเครดิตนั้น หมายถึงนิติบุคคลผู้ประกอบการใน 9 ประเภทธุรกิจ คือ ธนาคารพาณิชย์ บริษัทเงินทุน บริษัทหลักทรัพย์ บริษัทเครดิตฟองซิเอร์ บริษัทประกันวินาศภัย บริษัทประกันชีวิต นิติบุคคลที่ให้บริการบัตรเครดิต นิติบุคคลที่มีกฎหมายเฉพาะจัดตั้งขึ้นเพื่อดำเนินการทางการเงิน และนิติบุคคลอื่นที่ประกอบกิจการให้สินเชื่อเป็นทางการค้าปกติตามที่คณะกรรมการประกาศกำหนด

เมื่อมีการประกาศใช้มาตรา 4 (6) ดังที่ปรากฏ จะมีผลให้การดำเนินการกับข้อมูลในกิจการทั้งหมด 9 ประเภทนี้ ซึ่งมีข้อมูลส่วนบุคคลในหลายมิติและเกี่ยวข้องกับชีวิตของประชาชนจำนวนมาก และมีแนวโน้มจะเกี่ยวข้องกับชีวิตของประชาชนทุกคนในอนาคต ตามยุทธศาสตร์ชาติและแผนพัฒนาเศรษฐกิจดิจิทัล จะไม่อยู่ในการบังคับของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ซึ่งการกำหนดเช่นนี้จะส่งผลให้มาตรฐานการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลไม่ได้ครอบคลุมไปทุกมิติอย่างที่ควรจะเป็น

6. ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล มีกำหนดเรื่องของการยกเว้นการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลดั่งนี้ คือ “มาตรา 4 วรรคสอง การยกเว้นไม่ให้นำบทบัญญัติแห่งพระราชบัญญัตินี้ทั้งหมดหรือแต่บางส่วนมาใช้บังคับแก่ผู้ควบคุมข้อมูลส่วนบุคคลในลักษณะใด กิจการใด หรือหน่วยงานใดทำนองเดียวกับผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง หรือเพื่อประโยชน์สาธารณะอื่นใด ให้ตราเป็นพระราชกฤษฎีกา”

ในประเด็นการตรากฎหมายเพื่อยกเว้นไม่ให้มีการคุ้มครองสิทธิ หรือการตรากฎหมายขึ้นมาเพื่อจำกัดสิทธินี้ จะต้องตราเป็นพระราชบัญญัติที่ผ่านการพิจารณาของรัฐสภาเท่านั้น หรืออย่างน้อยหากเห็นสมควรให้ใช้การตราเป็นพระราชกฤษฎีกา โดยจะต้องต้องกำหนดกรอบสำหรับการบัญญัติข้อยกเว้นเพิ่มเติมดังกล่าวเอาไว้ในพระราชบัญญัติที่เป็นกฎหมายแม่บท ซึ่งเป็นหลักการพื้นฐานตามรัฐธรรมนูญ

มาตรา 4 วรรคสอง จึงอาจไม่สอดคล้องกับหลักการตามรัฐธรรมนูญแห่งราชอาณาจักรไทย ทั้งนี้เพราะ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ได้ถูกตราขึ้นเพื่อกำหนดหลักเกณฑ์และวิธีการที่

ชัดเจนในการใช้สิทธิและเสรีภาพตามเจตนารมณ์ของรัฐธรรมนูญ อันหมายความว่าสิทธิและเสรีภาพนั้นมีอยู่ก่อนแล้วและได้รับการคุ้มครองตามรัฐธรรมนูญแม้ยังไม่มีการตรากฎหมายขึ้นใช้บังคับเป็นการเฉพาะ ซึ่งสิทธิและเสรีภาพดังกล่าวเช่น “บุคคลย่อมมีสิทธิและเสรีภาพในชีวิตและร่างกาย” “บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว การกระทำอันเป็นการละเมิดหรือกระทบต่อสิทธิในความเป็นอยู่ส่วนตัว หรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใด ๆ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ” “บุคคลย่อมมีเสรีภาพในการติดต่อสื่อสารถึงกันไม่ว่าในทางใด ๆ การตรวจ การกัก หรือการเปิดเผยข้อมูลที่บุคคลสื่อสารถึงกัน รวมทั้งการกระทำด้วยประการใด ๆ เพื่อให้ล่วงรู้หรือได้มาซึ่งข้อมูล” “การเลือกปฏิบัติโดยไม่เป็นธรรมต่อบุคคล ไม่ว่าด้วยเหตุความแตกต่างในเรื่องถิ่นกำเนิด เชื้อชาติ ภาษา เพศ อายุ ความพิการ สภาพทางกายหรือสุขภาพ สถานะของบุคคล ฐานะทางเศรษฐกิจหรือสังคม ความเชื่อทางศาสนา การศึกษาอบรม หรือความคิดเห็นทางการเมือง จะกระทำมิได้” ฯลฯ เป็นต้น การยกเว้นการคุ้มครองสิทธิและเสรีภาพตามที่กำหนดไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล เท่ากับเป็นการจำกัดมาตรการคุ้มครองสิทธิและเสรีภาพของบุคคล หากจำเป็นต้องบัญญัติการยกเว้นดังกล่าว ต้องตราเป็นกฎหมายที่มีลำดับศักดิ์เทียบเท่าหรือสูงกว่าพระราชบัญญัติที่ผ่านการรับรองโดยรัฐสภา

ดังนั้น จึงสมควรมีการกำหนดกรอบเอาไว้ว่าการบัญญัติข้อยกเว้นเพิ่มเติมนั้น จะต้องระบุอย่างน้อยถึง ลักษณะผู้ควบคุมข้อมูลที่จะได้รับการยกเว้น จุดประสงค์การเก็บรวมรวม ใช้ หรือเปิดเผยที่จะได้รับการยกเว้น และเงื่อนไขหรือหลักเกณฑ์ที่จะทำให้ได้รับการยกเว้น โดยให้คำนึงถึงหลักความจำเป็นและได้สัดส่วนของกฎหมาย และสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลซึ่งจะสูญเสียไปจากการขยายข้อยกเว้นดังกล่าว

จากการพิจารณาในเบื้องต้นจะเห็นได้ว่า สำหรับการกำหนดนิยามของ GDPR กับ นิยามของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มีเนื้อหาสอดคล้องกัน แต่การกำหนดนิยามของข้อมูลส่วนบุคคลของ GDPR จะมีความชัดเจนกว่า เนื่องจากมีการระบุตัวอย่างมาเพื่อความชัดเจน ไม่ได้วางหลักการเปิดช่องให้มีการตราพระราชกฤษฎีกามาจำกัดสิทธิอย่างกว้างขวาง เหมือนเช่นกรณีของประเทศไทย

และประการสุดท้าย ในส่วนของการกำหนดข้อยกเว้น ควรจะมีการเพิ่มเติม “ประเภทประโยชน์โดยชอบด้วยกฎหมาย” (Legitimate Interest) ไปในข้อยกเว้นให้ชัดเจนขึ้น ทั้งนี้ เพราะการอนุญาตให้ประมวลผลข้อมูลได้เพื่อประโยชน์โดยชอบธรรมของผู้ควบคุมข้อมูลหรือของบุคคลที่สาม เป็นสิ่งที่ทั้ง Data Protection Directive และ GDPR อนุญาตให้ทำได้ต่อเมื่อประโยชน์ดังกล่าวไม่ขัดกับประโยชน์ที่จะมีต่อสิทธิและเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูล การอนุญาตในกรณีนี้จึง

เป็นการอนุญาตที่จะทำได้ก็ต่อเมื่อมีการทำ “Balancing Test” ชั่งน้ำหนักประโยชน์ต่าง ๆ เป็นรายกรณี[242]

4.3 องค์กรที่ทำหน้าที่คุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศไทย

4.3.1 รูปแบบขององค์กร

องค์กรที่ทำหน้าที่คุ้มครองข้อมูลส่วนบุคคลนั้น ถือเป็นกลไกอันสำคัญในการที่จะทำให้การคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลเป็นไปได้อย่างมีประสิทธิภาพ สำหรับในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลได้มีการกำหนดให้มีการจัดตั้งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลขึ้น ดังนั้นเพื่อให้องค์กรที่อยู่ในรูปของคณะกรรมการนี้สามารถทำงานคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพ จึงจำเป็นต้องออกแบบโครงสร้างขององค์กรให้มีรูปแบบที่สามารถรับประกันความเป็นอิสระในการทำงานของคณะกรรมการ

และนอกจากนี้ คณะกรรมการจะต้องมีอำนาจตามกฎหมายที่เพียงพอที่อันที่จะทำงานตามหน้าที่ที่ได้รับมอบหมายได้อย่างมีประสิทธิภาพ ซึ่งเรื่องนี้ต้องรวมไปถึงคณะกรรมการฯ จำเป็นจะต้องมีบุคคลากรและทรัพยากรเป็นขององค์กรตนเองในปริมาณที่เหมาะสมกับภาระงานด้วย

เมื่อพิจารณาจากโครงสร้างขององค์กรตามพระราชบัญญัติ แล้วมีลักษณะดังนี้

1. โครงสร้างขององค์กร จะถูกกำหนดให้อยู่ในรูปของคณะกรรมการ โดยอยู่ภายใต้โครงสร้างกระทรวง ดิจิตอลเพื่อเศรษฐกิจและสังคม

2. องค์ประกอบของคณะกรรมการ ประกอบด้วย

1) ประธานคณะกรรมการ 1 คน

2) รองประธานคณะกรรมการโดยตำแหน่ง 1 คน คือ ปลัดกระทรวงดิจิตอลเพื่อเศรษฐกิจและสังคม

3) กรรมการโดยตำแหน่ง จำนวน 5 คน คือ เลขาธิการคณะกรรมการกฤษฎีกา, อัยการสูงสุด, เลขาธิการคณะกรรมการคุ้มครองผู้บริโภค, อธิบดีกรมคุ้มครองสิทธิและเสรีภาพ และผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

---

[242] อาทิตย์ สุริยะวงศ์กุล, **ข้อมูลประกอบการนำเสนอความเห็นและข้อเสนอแนะแนวทางแก้ไขหรือปรับปรุงร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....**, ค้นวันที่ 1 ตุลาคม 2561 จาก https://thainetizen.org/docs/data-protection-bill-comments-20180920/

4) กรรมการผู้ทรงคุณวุฒิ จำนวน 9 คน ซึ่งสรรหาและแต่งตั้งจากผู้มีความรู้ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์ในด้านการคุ้มครองข้อมูลส่วนบุคคล ด้านการคุ้มครองผู้บริโภค ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านสังคมศาสตร์ ด้านกฎหมาย ด้านสุขภาพ หรือด้านอื่น ทั้งนี้ต้องเกี่ยวข้องและเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคล

3. ที่มากรรมการ เมื่อพิจารณาจะเห็นว่าคณะรัฐมนตรี ซึ่งจัดเป็นฝ่ายการเมือง มีอำนาจโดยตรงและทางอ้อมในการเลือกกรรมการ และตำแหน่งประธานคณะกรรมการฯ แต่งตั้งและให้ออกโดยคณะรัฐมนตรี, กรรมการโดยตำแหน่ง 5 คน เป็นผู้บริหารของส่วนราชการหรือองค์กรในกำกับของรัฐ, กรรมการผู้ทรงคุณวุฒิ 9 คน แต่งตั้งโดยคณะรัฐมนตรี

4. ภาระงานอาจมีประเด็นเรื่องการขัดประโยชน์ กล่าวคือกรรมการไม่ได้ทำงานเต็มเวลาและอาจทำงานให้องค์กรรัฐหรือภาคเอกชนอื่น ๆ ด้วย

5. ทรัพยากร ประเด็นนี้ จะเห็นว่าในระยะแรก คณะกรรมการฯ ไม่มีสำนักงานเฉพาะเป็นของตัวเอง ต้องพึ่งพาทรัพยากรและบุคลากรของ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ในการปฏิบัติงาน

4.3.2 อำนาจขององค์กร

เมื่อพิจารณาอำนาจขององค์กรตามกฎหมายแล้ว จะเห็นว่าภาระงานของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและสำนักงานฯจะมีปริมาณมาก เนื่องจากครอบคลุมทุกกิจการและมีอำนาจหน้าที่จำนวนมาก ซึ่งรวมถึงการทำแผนยุทธศาสตร์ การออกประกาศ การเสนอแนะต่อคณะรัฐมนตรี และการวินิจฉัยชี้ขาดปัญหาที่เกิดจากการบังคับใช้กฎหมาย หากทรัพยากรในการทำงานไม่เพียงพอหรือมีขั้นตอนลำดับชั้นในการปฏิบัติงานที่ยุ่งยากเกินความจำเป็น จะทำให้งานล่าช้าและยิ่งสะสม จนอาจกระทบสิทธิผู้เกี่ยวข้องและเสียโอกาสทางธุรกิจได้

ดังนั้น เพื่อให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ปฏิบัติงานได้อย่างมีประสิทธิภาพและทันต่อสถานการณ์ ควรพิจารณากำหนดให้กรรมการทุกคนต้องปฏิบัติหน้าที่เต็มเวลา หรือหากเห็นว่าจำเป็นอย่างยิ่งที่จะต้องมีกรรมการโดยตำแหน่งซึ่งไม่สามารถทำงานเต็มเวลาได้ ก็อาจกำหนดให้มีกรรมการโดยตำแหน่งที่ทำหน้าที่ไม่เต็มเวลาได้ แต่โดยที่กรรมการที่เหลือต้องปฏิบัติหน้าที่เต็มเวลาอย่างน้อยที่สุดตำแหน่งประธานกรรมการฯ และกรรมการผู้ทรงคุณวุฒิอย่างน้อยอีกครึ่งหนึ่ง ควรทำงานเต็มเวลา

จากที่กล่าวมาเมื่อพิจารณาเปรียบเทียบกับ GDPR จะเห็นว่า GDPR กำหนดหลักเกณฑ์ในทางสารบัญญัติจำนวนมากว่าด้วยสิทธิต่าง ๆ ของเจ้าของข้อมูลส่วนบุคคล หน้าที่และความรับผิดของผู้ควบคุมและผู้ประมวลผลข้อมูลส่วนบุคคลแล้ว ส่วนที่สำคัญที่สุดของการบังคับใช้ GDPR หรือกฎหมายหลาย ๆ ฉบับของสหภาพยุโรปอย่างมีประสิทธิภาพในการคุ้มครองสิทธิของปัจเจกชนคือ

“การมีองค์กรบังคับใช้กฎหมายที่มีประสิทธิภาพ” ดังที่ได้กล่าวไว้แล้วในบทที่ 2 ทั้งนี้เนื่องจากสหภาพยุโรปมีลักษณะเฉพาะประการสำคัญคือให้ความสำคัญกับการบังคับใช้กฎหมายโดยองค์กรของรัฐเพราะถือว่ารัฐมีหน้าที่ต้องปกป้องสิทธิของปัจเจกบุคคล ดังนั้นจะเห็นว่า GDPR กำหนดเงื่อนไขสำคัญขององค์กรบังคับใช้กฎหมายในรัฐสมาชิกไว้หลายประการเพื่อเป็นหลักประกันของการบังคับใช้กฎหมายอย่างมีประสิทธิภาพ (Article 51-55) โดยเฉพาะใน Article 52[243] กำหนดหลักการเรื่องความเป็นอิสระไว้อย่างชัดเจน โดยเฉพาะอย่างยิ่งใน อนุมาตรา (2) มีการกำหนดให้คณะกรรมการมีความเป็นเป็นอิสระและไม่อยู่ภายใต้การครอบงำของบุคคลใด ๆ (Remain Free From External Influence) มีอำนาจหน้าที่ในการไต่สวนและหาข้อเท็จจริงต่าง ๆ เพื่อบังคับให้เป็นไปตามกฎหมาย และต้องไม่กระทำการใด ๆ ที่ขัดหรือแย้งต่อหน้าที่ในการบังคับใช้กฎหมายด้วย

---

[243] GDPR - Article 52 Independence

Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.

The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.

Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.

Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.

เมื่อพิจารณาต่อไปถึงรูปแบบขององค์กรเช่นนี้ สำหรับประเทศที่ให้ความสำคัญในการคุ้มครองข้อมูลส่วนบุคคลที่ได้ยกตัวอย่างมาในบทที่ 3 จะเห็นว่า องค์กรที่ทำหน้าที่คุ้มครองข้อมูลส่วนบุคคลของประเทศเหล่านั้น ล้วนแล้วแต่มีลักษณะเป็นองค์กรที่มีความเป็นอิสระทั้งสิ้น ตัวอย่างเช่น The Federal Commissioner for Data Protection and Freedom of Information (BfDI) ของประเทศเยอรมนี เป็นองค์กรอิสระ, Commission Nationale Informatique Liberte's (CNIL) ของประเทศฝรั่งเศสเป็นหน่วยงานอิสระ,The Information Commissioner's Office (ICO) ของสหราชอาณาจักรเป็นหน่วยงานอิสระไม่ใช่ส่วนราชการแต่ขึ้นตรงกับรัฐสภา, The Office of the Privacy Commissioner of Canada (OPC) ของประเทศแคนาดาเป็นหน่วยงานอิสระขึ้นตรงกับรัฐสภา ฯลฯ การกำหนดเช่นนี้เป็นการสอดคล้องกับหลักการของ GDPR ดังที่ได้กล่าวมานั่นเอง

เมื่อพิจารณา รูปแบบขององค์กรของประเทศไทย จะพบว่าประกอบด้วยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลจำนวน 17 คน ทำหน้าที่ในเชิงนโยบายและกำหนดหลักเกณฑ์ที่สำคัญในการบังคับใช้กฎหมาย และมีคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอีกจำนวน 10 คน ทำหน้าที่กำกับดูแลด้านการบริหารงานบุคคลของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โดยมีปลัดกระทรวงดิจิทัลฯ และเลขาธิการสำนักงานฯ เป็นกรรมการโดยตำแหน่งในทั้งสองชุด โดยในส่วนของกรรมการผู้ทรงคุณวุฒิของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และกรรมการในคณะกรรมการผู้เชี่ยวชาญนั้น ไม่มีข้อกฎหมายกำหนดห้ามมิให้เป็นข้าราชการหรือเจ้าหน้าที่ในหน่วยงานของรัฐอื่น หรือลูกจ้าง พนักงาน หรือผู้บริหารของรัฐวิสาหกิจหรือองค์กรเอกชนเป็นกรรมการ อีกทั้งตามกฎหมายยังมิใช่การปฏิบัติงานเต็มเวลา โดยให้ได้รับเบี้ยประชุมและประโยชน์ตอบแทนอื่นตามที่กำหนดเท่านั้น ดังนั้น ตามโครงสร้างของกฎหมาย กรรมการผู้ทรงคุณวุฒิหรือกรรมการในคณะกรรมการผู้เชี่ยวชาญจึงอาจเป็นข้าราชการประจำหรือตัวแทนของภาคเอกชนก็ได้ ซึ่งเมื่อเปรียบเทียบกับ GDPR จึงอาจจะขัดหรือแย้งกับหลักการเรื่องความเป็นอิสระ ข้อสังเกตประการสำคัญคือกรรมการเหล่านี้จะไม่มีเวลาในการทำงานในหน้าที่ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลอย่างเต็มที่[244]

จากที่กล่าวมา องค์กรบังคับใช้กฎหมายซึ่งก็คือ คณะกรรมการคุ้มครองของมูลส่วนบุคคลนั้นถือเป็นองค์กรสำคัญที่ทำหน้าที่ในการบังคับใช้กฎหมาย เพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล การนำหลักการของ GDPR มาเป็นแนวทางในการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 นั้น ส่วนหนึ่งที่อาจไม่ได้รับการพิจารณามากนักคือ การกำหนดโครงสร้างขององค์กรบังคับใช้กฎหมายที่เหมาะสม อาจจะเนื่องจากเหตุผลว่าด้วยระบบกฎหมายของ

---

[244] ศุภวัชร์ มาลานนท์, *เรื่องเดิม*.

การจัดองค์กรของภาครัฐในประเทศไทย หรืออาจจะด้วยไม่ได้ให้ความสำคัญกับโครงสร้างขององค์กรบังคับใช้กฎหมายที่เป็นอิสระมากนัก ความน่ากังวลของการมีกฎหมายบัญญัติรับรองสิทธิแต่ปราศจากหน่วยงานการบังคับใช้หรือกลไกที่มีประสิทธิภาพ ย่อมทำให้กฎหมายไม่สามารถเป็นเครื่องมือในการคุ้มครองสิทธินี้ได้อย่างทั่วถึงและมีประสิทธิภาพเพียงพอ ดังนั้นในประการนี้จึงสมควรที่ในอนาคตจะได้มีการกำหนดให้มีองค์ประกอบของคณะกรรมการใหม่ โดยให้มีที่มาจากภาคประชาชน หรือภาคประชาสังคม รวมถึงองค์กรสื่อสารมวลชน เข้ามาเป็นกรรมการด้วย รวมไปถึงการกำหนดให้ผู้ที่เข้ามาดำรงตำแหน่งคณะกรรมการนั้น ควรจะได้ทำงานเต็มเวลาและไม่เป็นผู้ที่ดำรงตำแหน่งอื่น ในองค์กรอื่นด้วยในขณะเดียวกันเพื่อป้องกันปัญหาเรื่องการขัดกันแห่งผลประโยชน์และอิสระในการทำหน้าที่

4.4 มาตรการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศไทย

4.4.1 การคุ้มครองข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้ หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น เว้นแต่บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้[245] โดยหลักการสำคัญกล่าวอีกนัยหนึ่งก็คือ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้น จะต้องมีการขอความยินยอม และการขอความยินยอมต้องมีความชัดเจน ไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิด โดยการขอความยินยอมต้องทำเป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เว้นแต่โดยสภาพไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้ ส่วนการถอนความยินยอมนั้นเจ้าของข้อมูลอาจถอนความยินยอมเมื่อใดก็ได้ เว้นแต่มีข้อจำกัดตามที่กฎหมายกำหนด

ข้อยกเว้นตามกฎหมายที่จะสามารถดำเนินการโดยไม่ต้องขอความยินยอมนั้น กฎหมายไว้วางหลักการไว้ดังนี้คือ[246]

1. เพื่อประโยชน์ที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งเป็นไปเพื่อประโยชน์สาธารณะและได้เก็บข้อมูลส่วนบุคคลเพื่อการนั้นไว้เป็นความลับ
2. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

---

[245] มาตรา 19 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

[246] มาตรา 24 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

3. เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยตรงหรือโดยปริยาย ของเจ้าของข้อมูลส่วนบุคคล

4. เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคล เป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

5. เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล

6. เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูล ส่วนบุคคล หรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

7. เป็นการปฏิบัติตามกฎหมายหรือการใช้อำนาจรัฐของผู้ควบคุมข้อมูลส่วนบุคคล

หลักการขอความยินยอมนั้น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลได้กำหนดหลักการไว้ในมาตรา 19 วรรคสอง ถึงวรรคหก โดยมีหลักการดังนี้คือ การขอความยินยอมต้องทำเป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เว้นแต่โดยสภาพไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้

ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล ต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไปด้วย และการขอความยินยอมนั้นต้องชัดเจน และไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิด ในวัตถุประสงค์ดังกล่าว ทั้งนี้ คณะกรรมการจะให้ผู้ควบคุมข้อมูลส่วนบุคคลขอความยินยอม จากเจ้าของข้อมูลส่วนบุคคลตามแบบและข้อความที่คณะกรรมการประกาศกำหนดก็ได้

เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเสียเมื่อใดก็ได้ เว้นแต่มีข้อจำกัดสิทธิในการถอนความยินยอมโดยกฎหมายหรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล

ในกรณีที่การถอนความยินยอมส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลในเรื่องใด ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงผลกระทบจากการถอน ความยินยอมนั้น

การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลที่ไม่เป็นไปตามที่กำหนดไว้ในหมวดนี้ ไม่มีผลผูกพันเจ้าของข้อมูลส่วนบุคคล และไม่ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้

เมื่อพิจารณาหลักการตามกฎหมายฉบับนี้ของประเทศไทยเปรียบเทียบกับหลักการของ GDPR ที่กำหนดหลักความยินยอมไว้ว่า การขอความยินยอมต้องเป็นลายลักษณ์อักษร โดยวิธีการทางอิเล็กทรอนิกส์ หรือทางวาจาก็ได้ แต่ต้องมีการยืนยันที่ชัดเจน มีความเฉพาะเจาะจง ไม่คลุมเครือ ทั้งจะต้องแจ้งให้เจ้าของข้อมูลทราบ และเจ้าของข้อมูลต้องให้ความยินยอมนั้นโดยอิสระ จะเห็นว่าหลักการมีความเหมือนกัน

สำหรับในส่วนของข้อยกเว้นหลักความยินยอมนั้น GDPR รวมไปถึงกฎหมายของต่างประเทศดังกล่าวมาแล้ว ได้กำหนดข้อยกเว้นไว้มีความคล้ายคลึงกับของประเทศไทย กล่าวคือ เพื่อปฏิบัติตามสัญญา, เพื่อผลประโยชน์อันชอบธรรมที่กระทำโดยผู้ควบคุมข้อมูลหรือโดยบุคคลที่สาม, เพื่อป้องกันประโยชน์อย่างยิ่งยวดของเจ้าของข้อมูล, เพื่องานที่ดำเนินการเพื่อประโยชน์ของสาธารณะ หรือเพื่อปฏิบัติตามหน้าที่ตามกฎหมาย นั่นเอง

4.4.2 การเก็บรวบรวมข้อมูลส่วนบุคคล

สำหรับการเก็บรวมรวมข้อมูลส่วนบุคคลนั้น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดหลักการห้ามไม่ให้ผู้ควบคุมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลไม่ว่าจะเก็บโดยตรงหรือจากแหล่งอื่นใด โดยเจ้าของข้อมูลไม่ได้ให้ความยินยอม ดังที่ได้กล่าวไว้แล้วในข้อก่อนหน้านี้ นอกจากนี้ การเก็บรวบรวมข้อมูลส่วนบุคคลจะต้องมีการเก็บรวบรวมได้เท่าที่จำเป็น ภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล[247]

และยังมีการวางหลักการแจ้งให้ผู้เป็นเจ้าของข้อมูลทราบไว้เพิ่มเติมอีกด้วย กล่าวคือ ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียด ดังต่อไปนี้[248]

1. วัตถุประสงค์ของการเก็บรวบรวม
2. ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม
3. ประเภทของบุคคลหรือหน่วยงานที่ซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย
4. ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อ ในกรณีที่มีตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลให้แจ้งข้อมูล สถานที่ติดต่อ และวิธีการติดต่อของตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย

และวิธีการเก็บรวบรวมข้อมูลนั้น กฎหมายฉบับนี้ก็ได้มีการวางหลักการไว้ ดังนี้คือ ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่[249]

---

[247] มาตรา 22 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

[248] มาตรา 23 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

[249] มาตรา 25 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

1. ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลโดยได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

2. เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอม ตามมาตรา 24 หรือมาตรา 26 ให้นำบทบัญญัติเกี่ยวกับการแจ้งวัตถุประสงค์ใหม่ตามมาตรา 21 และการแจ้งรายละเอียดตามมาตรา 23 มาใช้บังคับกับการเก็บรวบรวมข้อมูลส่วนบุคคลที่ต้องได้รับความยินยอมตามวรรคหนึ่งโดยอนุโลม เว้นแต่กรณีดังต่อไปนี้

1) เจ้าของข้อมูลส่วนบุคคลทราบวัตถุประสงค์ใหม่หรือรายละเอียดนั้นอยู่แล้ว

2) ผู้ควบคุมข้อมูลส่วนบุคคลพิสูจน์ได้ว่าการแจ้งวัตถุประสงค์ใหม่หรือรายละเอียดดังกล่าวไม่สามารถทำได้หรือจะเป็นอุปสรรคต่อการใช้และการเปิดเผยข้อมูลส่วนบุคคลโดยเฉพาะอย่างยิ่งเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ ในกรณีนี้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิ เสรีภาพ และประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

3) การใช้หรือการเปิดเผยข้อมูลส่วนบุคคลต้องกระทำโดยเร่งด่วนตามที่กฎหมายกำหนดซึ่งได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

4) เมื่อผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้ซึ่งล่วงรู้หรือได้มาซึ่งข้อมูลส่วนบุคคล จากหน้าที่หรือจากการประกอบอาชีพหรือวิชาชีพและต้องรักษาวัตถุประสงค์ใหม่หรือรายละเอียดบางประการตามมาตรา 23 ไว้เป็นความลับตามที่กฎหมายกำหนด

นอกจากนี้ ในส่วนของข้อมูลส่วนบุคคลที่มีความอ่อนไหวนั้น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลก็ได้วางหลักการคุ้มครองข้อมูลไว้เป็นการเฉพาะ ในมาตรา 26 กล่าวคือ ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

1. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม

2. เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงานให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิ สมาคม หรือ

องค์กรที่ไม่แสวงหากำไรตามวัตถุประสงค์ดังกล่าวโดยไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรนั้น

3. เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล

4. เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

5. เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ

1) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ ทั้งนี้ ในกรณีที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์

2) ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพ จากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสม และเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

3) การคุ้มครองแรงงาน การประกันสังคม หรือการคุ้มครองทางสังคม ซึ่งการเก็บรวบรวมข้อมูลส่วนบุคคลเป็นสิ่งจำเป็นในการปฏิบัติตามสิทธิหรือหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคล โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

4) การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น ทั้งนี้ ต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น และได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล รวมทั้งต้องใช้มาตรการทางเทคนิคและมาตรการในองค์กรเพื่อให้เป็นไปตามหลักการลดการใช้ข้อมูลส่วนบุคคลลงให้มากที่สุด การใช้นามสมมุติหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ และห้ามใช้ข้อมูลส่วนบุคคลเมื่อหมดความจำเป็นตามวัตถุประสงค์โดยมีมาตรการเพื่อลดผลกระทบต่อสิทธิของเจ้าของข้อมูลส่วนบุคคล

5) ประโยชน์สาธารณะที่สำคัญ โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

กล่าวโดยสรุปได้ว่าหลักการสำคัญเรื่องนี้ก็เป็นไปทิศทางเดียวกันกับหลักการของ GDPR ที่วางหลักการไว้ว่า ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับถิ่นกำเนิด เชื้อชาติ หรือชาติพันธุ์ ความเห็นทางการเมือง ความเชื่อทางศาสนา หรือปรัชญา การเป็นสมาชิกสหภาพทางการค้า ข้อมูลพันธุกรรม ข้อมูลชีวภาพสุขภาพ ชีวิตหรือรสนิยมทางเพศ เว้นแต่ จะได้รับความยินยอมอันแจ้งชัดจากเจ้าของข้อมูล หรือกรณีต่อไปนี้คือ 1) จำเป็นเพื่อวัตถุประสงค์ในการปฏิบัติตามและการใช้สิทธิเฉพาะเจาะจงของผู้ควบคุมข้อมูล หรือของเจ้าของข้อมูลในขอบเขตของการจ้างงานและตามกฎหมายความมั่นคงปลอดภัยทางสั่งคม และกฎหมายการป้องกันความมั่นคงปลอดภัยต่อสังคม 2) จำเป็นเพื่อปกป้องประโยชน์อันยิ่งยวดของเจ้าของข้อมูลหรือผู้อื่น 3) ในกระบวนการของกิจกรรมอันชอบด้วยกฎหมายของการใช้ข้อมูลโดยมีการป้องกันอันเหมาะสม 4) เป็นข้อมูลที่ถูกแสดงเป็นสาธารณะแล้วโดยเจ้าของข้อมูล 5) เป็นการสร้าง ใช้ หรือแก้ต่างข้อเรียกร้องทางกฎหมายหรือ โดยศาล 6) เพื่อเหตุผลด้านผลประโยชน์สาธารณะตามกฎสหภาพยุโรปโดยได้สัดส่วนกับวัตถุประสงค์ 7) เพื่อประโยชน์สาธารณะอันสำคัญในการสาธารณสุขหรือการระงับการแพร่ระบาดของโรค 8) เพื่อการป้องกันและชีวอนามัย การตรวจความสามารถในการทำงานของลูกจ้าง การวินิจฉัยทางการแพทย์ การให้บริการทางสุขภาพ หรือการรักษา หรือการดูแลทางสังคมหรือการจัดการบริการด้านสุขภาพ หรือ 9) เพื่อวัตถุประสงค์สำหรับประโยชน์สาธารณะในทางการวิจัยทางวิทยาศาสตร์ หรือประวัติศาสตร์ซึ่งต้องเป็นไปตามหลักความได้สัดส่วน

4.4.3 การใช้และการเปิดเผยข้อมูลส่วนบุคคล

หลักการในการใช้หรือเปิดเผยข้อมูลส่วนบุคคลนั้น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 27 ได้วางหลักการว่า ห้ามมิให้ผู้ควบคุมใช้ข้อมูลส่วนบุคคลที่อยู่ในความครอบครองโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล เว้นแต่เป็นกรณีข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26

นอกจากนี้ บุคคลหรือนิติบุคคลที่ได้รับข้อมูลส่วนบุคคลมาจากการเปิดเผยตามวรรคหนึ่งจะต้องไม่ใช้หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลส่วนบุคคลในการขอรับข้อมูลส่วนบุคคลนั้น

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้และเปิดเผยข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอม ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกการใช้และการเปิดเผยนั้นไว้ในรายการตามที่กฎหมายกำหนดด้วย

นอกจากที่กล่าวมา สำหรับกรณีของการเปิดเผยข้อมูลไปนอกราชอาณาจักรนั้น มาตรา 28 ได้กำหนดหลักการไว้ว่า ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ประเทศปลายทางหรือองค์การระหว่างประเทศที่ได้รับข้อมูลส่วนบุคคลต้องมีมาตรฐาน

การคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ตามที่คณะกรรมการข้อมูลส่วนบุคคลได้ออกประกาศกำหนด เว้นแต่ ในกรณีต่อไปนี้

1. เป็นการปฏิบัติตามกฎหมาย
2. ได้รับความยินยอมจากเจ้าของข้อมูลโดยได้แจ้งเจ้าของข้อมูลส่วนบุคคลทราบถึงมาตรการการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลแล้ว
3. เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น
4. เป็นการกระทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่นเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล
5. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้
6. เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ

ในกรณีที่มีปัญหาเกี่ยวกับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคล ก็จะเป็นอำนาจของคณะกรรมการข้อมูลส่วนบุคคลที่จะเป็นผู้วินิจฉัย

จากหลักการที่กล่าวมาจะเห็นว่า หลักการในส่วนของการใช้และการเปิดเผยข้อมูลส่วนบุคคลที่กำหนดไว้ใน พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 นั้นก็ถือว่าเป็นไปในทิศทางและมาตรฐานเดียวกันกับกฎหมายของต่างประเทศและหลักการที่ GDPR กำหนดนั่นเอง

4.4.4 การเก็บรักษาข้อมูลส่วนบุคคล

เพื่อเป็นการปกป้องสิทธิของเจ้าของข้อมูลส่วนบุคคลในด้านความปลอดภัยของข้อมูลส่วนบุคคล พระราชบัญญัติฉบับนี้จึงกำหนดหลักการในการเก็บรักษาข้อมูลส่วนบุคคลว่า ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย การเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ทั้งนี้ ต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม[250]

---

[250] มาตรา 36 (1) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

4.4.5 การกำหนดสิทธิให้แก่เจ้าของข้อมูลส่วนบุคคล

สำหรับสิทธิของเจ้าของข้อมูลส่วนบุคคลนั้น ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ได้วางหลักการไว้ในหลายมาตราดังต่อไปนี้คือ

มาตรา 30 เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอม

ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามคำขอตามวรรคหนึ่ง จะปฏิเสธคำขอได้เฉพาะในกรณีดังต่อไปนี้

1. เป็นการขัดหรือแย้งกับบทบัญญัติแห่งกฎหมาย หรือปฏิบัติตามคำสั่งศาล
2. มีผลต่อการสืบสวนสอบสวนของพนักงานเจ้าหน้าที่ตามกฎหมาย
3. การเปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลนั้นอาจจะเป็นอันตรายต่อสิทธิ และเสรีภาพของบุคคลอื่น
4. กรณีอื่นตามที่กำหนดในกฎกระทรวง

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธคำขอตามวรรคหนึ่ง ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกการปฏิเสธคำขอดังกล่าวพร้อมด้วยเหตุผลไว้ในรายการตามมาตรา 38

เมื่อเจ้าของข้อมูลส่วนบุคคลมีคำขอตามวรรคหนึ่งและเป็นกรณีที่ไม่อาจปฏิเสธคำขอได้ตามวรรคสอง ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามคำขอภายในสามสิบวันนับแต่วันที่ได้รับคำขอ

มาตรา 31 เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอรับข้อมูลส่วนบุคคลที่เกี่ยวกับตนจากผู้ควบคุมข้อมูลส่วนบุคคลได้ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้ทำให้ข้อมูลส่วนบุคคลนั้นอยู่ในรูปแบบที่สามารถอ่านหรือใช้งานโดยทั่วไปได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติและสามารถใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ด้วยวิธีการอัตโนมัติ รวมทั้งมีสิทธิดังต่อไปนี้

1. ขอให้ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลในรูปแบบดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นเมื่อสามารถทำได้ด้วยวิธีการอัตโนมัติ
2. ขอรับข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลในรูปแบบดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นโดยตรง เว้นแต่โดยสภาพทางเทคนิคไม่สามารถทำได้

ข้อมูลส่วนบุคคลตามวรรคหนึ่งต้องเป็นข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลตามหลักเกณฑ์แห่งพระราชบัญญัตินี้ หรือเป็นข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 (4)

การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามวรรคหนึ่งจะใช้กับการส่งหรือโอนข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะหรือเป็นการปฏิบัติหน้าที่ตามกฎหมายไม่ได้ หรือการใช้สิทธินั้นต้องไม่ละเมิดสิทธิหรือเสรีภาพของบุคคลอื่น ทั้งนี้

ในกรณีที่ควบคุมข้อมูลส่วนบุคคลปฏิเสธคำขอด้วยเหตุผลดังกล่าว ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกการปฏิเสธคำขอพร้อมด้วยเหตุผลไว้ในรายการตามมาตรา 38

มาตรา 32 เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตนเมื่อใดก็ได้ ดังต่อไปนี้

1. กรณีที่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอ ความยินยอมตามมาตรา 24 (5) หรือ (6) เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลพิสูจน์ได้ว่า

1) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นเป็นไปโดยผลของการบังคับใช้กฎหมายที่สำคัญยิ่งกว่า

2) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

2. กรณีที่เป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง

3. กรณีที่เป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ เว้นแต่เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล

ในกรณีที่เจ้าของข้อมูลส่วนบุคคลใช้สิทธิคัดค้านตามวรรคหนึ่ง ผู้ควบคุมข้อมูล ส่วนบุคคลไม่สามารถเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นต่อไปได้ ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติโดยชัดแจ้งในทันทีเมื่อเจ้าของข้อมูลส่วนบุคคลได้แจ้งการคัดค้านให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบ

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธการคัดค้านด้วยเหตุผลตาม (1) (ก) หรือ (ข) หรือ (3) ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกการปฏิเสธการคัดค้านพร้อมด้วยเหตุผลไว้ในรายการตามมาตรา 38

มาตรา 33 ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่ปฏิบัติตามหลักเกณฑ์แห่งพระราชบัญญัตินี้ เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบ หรือทำลาย ระงับการใช้ชั่วคราว หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล ที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

การขอให้ระงับการใช้ชั่วคราวนอกจากกรณีตามวรรคหนึ่ง เจ้าของข้อมูลส่วนบุคคลอาจขอให้ระงับการใช้ชั่วคราวได้ ในกรณีดังต่อไปนี้ด้วย

1. เมื่อผู้ควบคุมข้อมูลส่วนบุคคลอยู่ในระหว่างการตรวจสอบตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอให้ดำเนินการตามมาตรา 35

2. เมื่อพ้นกำหนดระยะเวลาการเก็บรักษาไว้ตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล แต่เจ้าของข้อมูลส่วนบุคคลมีความจำเป็นต้องขอให้เก็บรักษาไว้เพื่อใช้ในการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

3. เมื่อผู้ควบคุมข้อมูลส่วนบุคคลอยู่ในระหว่างการพิสูจน์ตามมาตรา 32 (1) หรือตรวจสอบตามมาตรา 32 (3) เพื่อปฏิเสธการคัดค้านของเจ้าของข้อมูลส่วนบุคคลตาม มาตรา 32 วรรคสาม

กรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามวรรคหนึ่งหรือวรรคสอง เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมข้อมูล ส่วนบุคคลดำเนินการได้

คณะกรรมการอาจประกาศกำหนดหลักเกณฑ์ในการลบหรือทำลาย ระงับการใช้ชั่วคราว หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูล ส่วนบุคคลตามวรรคหนึ่งก็ได้

จากบทบัญญัติที่กล่าวมาข้างต้น จะเห็นว่า สิทธิของเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ที่สำคัญจะมีดังนี้คือ เจ้าของข้อมูลส่วนบุคลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตน, มีสิทธิขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลที่ตนไม่ได้ให้ความยินยอม, มีสิทธิในการเคลื่อนย้ายข้อมูล และมีสิทธิโต้แย้งคัดค้านตลอดจนมีสิทธิการระงับใช้ข้อมูลส่วนบุคคลของตนได้ ซึ่งจะเห็นว่าเป็นสิทธิสำคัญและสอดคล้องกับหลักการของ GDPR แต่อย่างไรก็ดี สิทธิสำคัญบางประการที่ได้มีการกำหนดไว้ใน GDPR นั้น กฎหมายของไทยฉบับนี้ไม่ได้มีการรับรองไว้ ซึ่งจะได้กล่าวในบทต่อไป

4.5 ระบบการเยียวยาผู้ถูกละเมิดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศไทย

ในอดีตด้วยเหตุที่ประเทศไทยยังไม่มีกฎหมายกลางที่บัญญัติจัดตั้งองค์กรให้ความคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลเป็นการเฉพาะมาก่อน ทำให้แต่เดิมเมื่อประชาชนผู้ถูกละเมิดสิทธิก็จะใช้สิทธิเรียกร้องให้มีการเยียวยาความเสียหายบนฐานของกฎหมายแพ่งและพาณิชย์ ลักษณะละเมิด และประมวลกฎหมายอาญา เป็นสำคัญ แต่อย่างไรก็ดี การดำเนินคดีบนฐานของกฎหมายทั้งสองฉบับนี้ ย่อมต้องจะต้องมีต้นทุนเสมอ ดังนั้น ประชาชนส่วนหนึ่งจึงเลี่ยงที่จะไม่ใช้สิทธิของตนในการฟ้องร้องหรือดำเนินคดีในทางศาล เมื่อกรณีเป็นเช่นนี้ย่อมจะส่งผลให้ผู้ล่วงละเมิดสิทธิในข้อมูลส่วนบุคคลย่อมได้รับประโยชน์ นอกจากนี้ ในมิติของการเรียกค่าเสียหายโดยเหตุละเมิดนั้น ประชาชนซึ่งเป็นผู้ฟ้องคดีจะมีภาระในการพิสูจน์ให้ศาลเชื่อว่าผู้ก่อให้เกิดความเสียหายนั้นจงใจ

หรือประมาท กระทำการผิดกฎหมายเป็นเหตุให้ได้รับความเสียหาย ซึ่งในทางปฏิบัติค่อนข้างยากที่ผู้เสียหายโดยเฉพาะอย่างยิ่งประชาชนซึ่งมักจะเป็นผู้ใช้บริการรายย่อยทั่วไปที่จะสามารถพิสูจน์ได้ตามเงื่อนไขที่กฎหมายกำหนด จึงเป็นอุปสรรคที่ทำให้ผู้เสียหายไม่อยากดำเนินคดี

ทว่า อุปสรรคนี้เหล่านี้จะหมดไปหากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลมีผลบังคับใช้อย่างเต็มรูปแบบ เนื่องจากในกฎหมายดังกล่าวมีบทกำหนดความรับผิดทางแพ่งโดยเด็ดขาดให้ผู้ควบคุมข้อมูลส่วนบุคคลที่ทำให้เกิดความเสียหายจะต้องรับผิดต่อเจ้าของข้อมูลไม่ว่าการดำเนินการนั้นจะเกิดจากการกรทำโดยจงใจหรือประมาทเลินเล่อก็ตาม เว้นแต่จะพิสูจน์ได้ว่าความเสียหายดังกล่าวเกิดจากเหตุสุดวิสัย การปฏิบัติตามคำสั่งของเจ้าหน้าที่หรือการปฏิบัติตามกฎหมาย หรือเป็นไปเพื่อการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

นอกจากนั้น ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ได้มีการกำหนดมาตรการไว้ในกฎหมาย ผ่านการบังคับใช้โดยคณะกรรมการข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการข้อมูลส่วนบุคคล โดยมีการกำหนดทั้งในส่วนของโทษทางอาญา และโทษทางปกครอง รวมไปถึงมีการกำหนดความรับผิดในทางแพ่งไว้ในร่างพระราชบัญญัติ

โดยมีการกำหนดกระบวนการร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญที่ได้รับการพิจารณาแต่งตั้งจากคณะกรรมการข้อมูลส่วนบุคคล โดยให้คณะกรรมการชุดนี้มีอำนาจดังต่อไปนี้คือ[251]

1. พิจารณาเรื่องร้องเรียนตามพระราชบัญญัตินี้
2. ตรวจสอบการกระทำใด ๆ ของผู้ควบคุมข้อมูลส่วนบุคคลหรือลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลเกี่ยวกับข้อมูลส่วนบุคคลที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคล
3. ไกล่เกลี่ยข้อพิพาทเกี่ยวกับข้อมูลส่วนบุคคล
4. ปฏิบัติการอื่นใดตามที่พระราชบัญญัติกำหนด

โดยการยื่นเรื่องร้องเรียน การไม่รับเรื่อง การยุติเรื่อง และวิธีพิจารณาคำร้องเรียน นั้นร่างกฎหมายได้กำหนดให้เป็นไปตามระเบียบที่คณะกรรมการประกาศกำหนด

---

[251] มาตรา 70 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

แต่อย่างไรก็ดี ในส่วนของการกำหนดค่าเสียหายหรือค่าสินไหมทดแทนนั้น กฎหมายได้มีการกำหนดให้ศาลเป็นผู้มีอำนาจ[252] ซึ่งรูปแบบของการกำหนดค่าเสียหายหรือค่าสินไหมทดแทนนี้จะอยู่ในลักษณะของค่าเสียหายเชิงลงโทษ (Punitive Damages) ทั้งนี้เพื่อจะให้เป็นมาตรการในการสร้างหลักประกันแก่การคุ้มครองสิทธินี้ให้เกิดผลขึ้นอย่างแท้จริง ซึ่งหลักการของการกำหนดความรับผิดในทางแพ่งนั้น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ได้กำหนดหลักการไว้ในมาตรา 75 ซึ่งมีสาระสำคัญคือ ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลอันเป็นการฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติแห่งพระราชบัญญัตินี้ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้นแก่เจ้าของข้อมูลส่วนบุคคล ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่ก็ตาม เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้นจะพิสูจน์ได้ว่า

1. ความเสียหายนั้นเกิดจากเหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั้นเอง

2. เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามหน้าที่และอำนาจตามกฎหมาย

ค่าสินไหมทดแทนตามวรรคหนึ่ง ให้หมายความรวมถึงค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย

นอกจากความรับผิดในทางแพ่งที่ได้กล่าวมาแล้ว พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ยังได้วางมาตรการความรับผิดในทางอาญาไว้ในมาตรา 77 กล่าวคือ หากผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 27 วรรคหนึ่งหรือ วรรคสอง หรือไม่ปฏิบัติตามมาตรา 28 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 26 โดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดู

---

[252] มาตรา 76 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ให้ศาลมีอำนาจสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูล ส่วนบุคคลจ่ายค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มขึ้นจากจำนวนค่าสินไหมทดแทนที่แท้จริงที่ศาล กำหนดได้ตามที่ศาลเห็นสมควร แต่ไม่เกินสองเท่าของค่าสินไหมทดแทนที่แท้จริงนั้น ทั้งนี้ โดยคำนึงถึงพฤติการณ์ต่าง ๆ เช่น ความร้ายแรงของความเสียหายที่เจ้าของข้อมูลส่วนบุคคลได้รับ ผลประโยชน์ที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้รับ สถานะทางการเงิน ของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล การที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือ ผู้ประมวลผลข้อมูลส่วนบุคคลได้บรรเทาความเสียหายที่เกิดขึ้น หรือการที่เจ้าของข้อมูลส่วนบุคคล มีส่วนในการก่อให้เกิดความเสียหายด้วย

หมิ่นถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ

ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 27 วรรคหนึ่งหรือวรรคสอง หรือไม่ปฏิบัติตามมาตรา 28 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 26 เพื่อแสวงหาประโยชน์ ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งล้านบาท หรือทั้งจำทั้งปรับ แต่อย่างไรก็ดี ความผิดตามมาตรา77 นี้ถูกกำหนดให้เป็นความผิดอันยอมความได้

ดังนั้นเมื่อพิจารณาโดยภาพรวมแล้ว จะเห็นได้ว่าโดยสาระสำคัญของกฎหมายฉบับใหม่ที่ได้ตราขึ้นนี้ ในแง่ประโยชน์ที่จะได้รับนั้น กฎหมายฉบับนี้จะก่อให้เกิดประโยชน์ประการแรก คือในด้านประโยชน์ส่วนบุคคล (Individual Interest) กล่าวคือ เป็นกฎหมายเพื่อใช้ในการป้องกันข้อมูลส่วนบุคคลจากการเก็บ รวบรวม ใช้ เปิดเผยผิดวัตถุประสงค์ โดยมีกลไกการจัดการข้อมูลส่วนบุคคลที่เหมาะสมและเพื่อให้เจ้าของข้อมูลส่วนบุคคลได้รับความคุ้มครอง สามารถตรวจสอบและควบคุมผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของตน และประการที่สองคือประโยชน์ด้านเศรษฐกิจ (Economic Interest) กล่าวคือ กฎหมายฉบับนี้จะสร้างความเชื่อมั่นให้แก่นานาชาติว่าประเทศไทยมีมาตรฐานการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลเป็นการทั่วไปที่เพียงพอและอำนวยความสะดวกสำหรับการส่งหรือโอนข้อมูลส่วนบุคคลข้ามพรมแดนได้อย่างมีมาตรฐานนั่นเอง

บทที่ 5

วิเคราะห์มาตรการและกลไกทางกฎหมายในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล

ในบทนี้จะได้ทำการวิเคราะห์ถึงมาตรการและกลไกทางกฎหมายในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล โดยพิจารณาตั้งแต่ผลของกติการะหว่างประเทศที่กระทบต่อการกำหนดมาตรการและกลไกในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล การวางรูปแบบ (Form) ของกฎหมายที่ถูกตราขึ้นเพื่อรับรองและคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล การกำหนดนิยามและขอบเขตรวมถึงการกำหนดประเภทของสิทธิที่มอบให้แก่เจ้าของข้อมูลส่วนบุคคลตามกฎหมาย ข้อจำกัดของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล รวมถึงการกำหนดรูปแบบขององค์กรและวิธีการเยียวยาอันเป็นกลไกในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล โดยจะได้เรียงลำดับในการวิเคราะห์เพื่ออธิบายดังต่อไปนี้

5.1 วิเคราะห์มาตรการในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล

ในส่วนแรกนี้จะได้ทำการวิเคราะห์ถึงมาตรการอันเป็นกฎหมายในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล โดยจะได้เรียงลำดับการวิเคราะห์คือ รูปแบบของกฎหมายที่กำหนดเพื่อคุ้มครองสิทธิ การกำหนดนิยามและขอบเขตของข้อมูลส่วนบุคคลที่จะได้รับความคุ้มครองตามมาตรการทางกฎหมาย การกำหนดสิทธิให้กับเจ้าของข้อมูลส่วนบุคคลและการวางข้อจำกัดสิทธิของเจ้าของข้อมูลส่วนบุคคลโดยพิจารณาจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลและกฎหมายสำคัญต่าง ๆ ของประเทศไทยที่เกี่ยวข้อง โดยพิจารณาเปรียบเทียบกับหลักการของกฎหมายต่างประเทศ และกติการะหว่างประเทศอันสำคัญที่มีผลกระทบอย่างมากต่อการวางมาตรการและกลไกคุ้มครองข้อมูลส่วนบุคคลของไทยในปัจจุบันซึ่งก็คือ General Data Protection Regulation (GDPR) โดยจะเรียงลำดับในการอธิบายดังนี้

5.1.1 วิเคราะห์รูปแบบของกฎหมายเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล

5.1.1.1 กติการะหว่างประเทศที่มีผลกระทบต่อการคุ้มครองสิทธิ

สำหรับประเทศไทยต้องยอมรับว่าการกำเนิดขึ้นของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนั้น ไม่ได้ถือกำเนิดขึ้นในบ้านเมืองหรือประเทศของเราแต่แรกเริ่ม หากแต่เป็นการยอมเอาแนวคิดจากประเทศที่มีความก้าวหน้ามากกว่าในทางกฎหมายเข้ามา เช่นเดียวกับมาตรการและกลไกในทางกฎหมายที่จะใช้เป็นเครื่องมือในทางสังคมเพื่อปกป้องและคุ้มครองสิทธินี้ก็ได้มีการยอมรับและมีการนำเอาหลักการของกฎหมายต่างประเทศมาเป็นแนวทางเช่นเดียวกัน แม้จะไม่ถึงขนาดเป็นการรับกฎหมาย (Reception of Law) อันเป็นกระบวนการที่รัฐหนึ่งได้ยอมรับเอากฎหมายของอีกรัฐหนึ่งเข้ามาเป็นส่วนหนึ่งหรือมีอิทธิพลในระบบกฎหมายของตน ไม่ว่าทั้งหมดหรือบางส่วน เพื่อตอบสนองเหตุผลหรือความจำเป็นในบางประการของรัฐนั้น ๆ แต่ภายใต้เหตุผลแรงกดดันในทางเศรษฐกิจระหว่างประเทศก็ทำให้ประเทศไทยหลีกเลี่ยงไม่ได้ที่จะต้องดำเนินการยอมรับและพัฒนามาตรการและกลไกทางกฎหมายขึ้นมาให้ทัดเทียมกันกับหลักการของนานาอารยประเทศ

จากที่ได้กล่าวมาข้างต้น จะเห็นได้ว่า การที่สหภาพยุโรปได้มีการพัฒนาหลักการเกี่ยวกับสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล รวมถึงพัฒนามาตรการและกลไกทางกฎหมายเพื่อปกป้องและคุ้มครองสิทธิเช่นว่านี้ ได้มีผลกระทบต่อหลักการของกฎหมายทั่วโลกที่จะต้องปรับหลักการของกฎหมายภายในของประเทศตนให้มีความสอดคล้องกับหลักการที่สหภาพยุโรปได้กำหนดไว้ ซึ่งหลักการของกฎหมายสหภาพยุโรปที่ว่านี้ก็คือ General Data Protection Regulation (GDPR) ที่มีผลบังคับใช้วันที่ 25 พฤษภาคม พ.ศ.2561 ที่ผ่านมา

วัตถุประสงค์ของ General Data Protection Regulation นั้นได้กล่าวไว้แล้วในบทก่อน ๆ ซึ่งสรุปได้ว่าเป็นหลักเกณฑ์ที่ถูกกำหนดขึ้นเพื่อให้ประชาชนของสหภาพยุโรปมีสิทธิควบคุมข้อมูลส่วนบุคคลของตนซึ่งถือเป็นสิทธิมนุษยชนขั้นพื้นฐาน และกำหนดมาตรการและกลไกเพื่อให้สหภาพยุโรปมีมาตรฐานการคุ้มครองข้อมูลที่เป็นอันหนึ่งอันเดียวในอันที่จะทำให้เกิดการเคลื่อนย้ายโดยเสรีของข้อมูล โดยหลักการสำคัญของ General Data Protection Regulation นั้นถือเป็นการยกระดับของการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลให้เพิ่มมากขึ้นกว่าหลักการเดิมที่ยุโรปเคยบังคับใช้อย่างเข้มแข็งอยู่แล้ว ซึ่งสาระสำคัญของหลักการในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลตั้งอยู่บนพื้นฐานคือ

ประการแรก หน่วยงานควบคุมข้อมูลที่เจ้าของข้อมูลรับบริการ (Data Controller) ต้องได้รับความยินยอมจากเจ้าของข้อมูล (Data Subject) ในการจัดเก็บข้อมูล รวมทั้งต้องกำหนดขอบเขต วัตถุประสงค์ในการประมวลผลข้อมูลที่ชัดเจน

ประการที่สอง ประเทศซึ่งเป็นชาติสมาชิกสหภาพยุโรปจะต้องให้การคุ้มครองอย่างเคร่งครัดต่อข้อมูลที่อ่อนไหวเป็นพิเศษ เช่น ความคิดทางการเมือง ความเชื่อทางศาสนาหรือลัทธิ พฤติกรรมสุขภาพ รสนิยมหรือพฤติกรรมทางเพศ การเป็นสมาชิกสหภาพหรือสหพันธ์แรงงาน ประวัติอาชญากรรม ฯลฯ เป็นต้น

ประการที่สาม ในการส่งข้อมูลไปต่างประเทศ หรือบริษัทที่อยู่ต่างประเทศ ผู้รับข้อมูลต้องมีการคุ้มครองข้อมูลมาตรฐานเดียวกับบริษัทในยุโรป

และประการที่สี่ หน่วยงานควบคุมข้อมูลต้องกำหนดขอบเขต ระยะเวลาในการประมวลผล และมีมาตรการรักษาความปลอดภัยข้อมูลอย่างรัดกุม

การมีผลใช้บังคับของ GDPR นั้น ส่งผลกระทบไปยังประเทศต่าง ๆ ก็คือ ขอบเขตการบังคับใช้เชิงพื้นที่ของ GDPR นั้นให้บังคับใช้ในทุกหน่วยงานที่มีการประมวลผลข้อมูลส่วนบุคคลของพลเมืองที่อาศัยอยู่ในสหภาพยุโรป ไม่ว่าองค์กร องค์กรธุรกิจหรือบริษัทจะตั้งอยู่ที่ไหน กล่าวคือ GDPR บังคับใช้กับผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลในสหภาพยุโรป ไม่ว่าการประมวลผลจะได้กระทำในสหภาพยุโรปหรือไม่ก็ตาม โดยจะบังคับใช้กับทุกกิจกรรมที่เป็นการจำหน่ายสินค้าและบริการแก่พลเมืองของสหภาพยุโรปและทุกกิจกรรมที่มีลักษณะการติดตามพฤติกรรมของพลเมืองที่เกิดขึ้นในสหภาพยุโรปหากเป็นธุรกิจของประเทศอื่นที่ไม่ใช่สมาชิกของสหภาพยุโรป (Non-EU Business) ก็ต้องดำเนินการแต่งตั้งผู้แทนในสหภาพยุโรปด้วย

สำหรับประเทศไทย แม้ไม่ได้เป็นสมาชิกสหภาพยุโรป แต่ไม่อาจหลีกเลี่ยงผลกระทบจากการประกาศใช้ General Data Protection Regulation ทั้งนี้เพราะการค้าระหว่างประเทศระหว่างไทยและประเทศในสหภาพยุโรปมีมูลค่าทางเศรษฐกิจสูงมาก และในการดำเนินกิจกรรมทางการค้าส่วนหนึ่งจะมีการดำเนินธุรกิจผ่านระบบอิเล็กทรอนิกส์ จะมีการแลกเปลี่ยนข้อมูลระหว่างผู้ประกอบการตลอดเวลา โดยปริมาณการรับส่งข้อมูลมีจำนวนมหาศาล ในบรรดาข้อมูลเหล่านี้ย่อมรวมถึงข้อมูลส่วนบุคคลที่เกี่ยวข้องจำนวนมาก ทั้งข้อมูลพลเมืองของประเทศผู้ซื้อและประเทศผู้ขายสินค้าและบริการ โดยยกตัวอย่าง หากพิจารณาจากภาคธุรกิจการท่องเที่ยวและบริการเพียงส่วนเดียวจะพบว่านักท่องเที่ยวจากยุโรปเป็นกลุ่มใหญ่ที่สุดที่ทำรายได้ให้กับประเทศไทย ซึ่งแน่นอนว่า ข้อมูลส่วนบุคคลของนักท่องเที่ยวเหล่านี้จะต้องมีการรับ ส่ง และแลกเปลี่ยน กับผู้ให้บริการในประเทศไทยอย่างหลีกเลี่ยงไม่ได้ ทำให้บริษัทและหน่วยงานในประเทศเราน่าจะมีผลกระทบจาก General Data Protection Regulation จำนวนมาก ไม่ว่าจะเป็นประเด็นนับตั้งแต่การเก็บข้อมูลการเดินทางเข้าออกประเทศ ธุรกิจสายการบิน บริษัทท่องเที่ยว โรงแรมที่พัก โรงพยาบาลหรือสถานบริการสุขภาพ สถาบันการเงิน ธุรกิจการเงิน การแลกเปลี่ยนเงินตรา บัตรเครดิต การประกันชีวิต การประกันภัย บริษัทโทรคมนาคม บริษัทที่ดำเนินธุรกิจธุรกรรมออนไลน์ และ E-commerce ฯลฯ เป็นต้น นอกจากนี้ ด้วยความใหญ่โตของฐานข้อมูลส่วนบุคคลในผู้ประกอบการด้านการเงินการธนาคาร ธุรกิจ

การติดต่อสื่อสารโทรคมนาคม และโดยเฉพาะธุรกิจที่เกี่ยวข้องกับข้อมูลโดยตรง ไม่ว่าจะเป็นผู้ประกอบการด้านการประมวลผลข้อมูล Big Data Cloud รวมทั้งธุรกิจตลาดหลักทรัพย์ ธุรกิจบริการด้านสุขภาพ จะมีความเชื่อมโยงสัมพันธ์กันในทางข้อมูลอยู่ตลอดเวลา นั่นหมายความว่าทุกหน่วยงานที่จะทำหน้าที่เป็นผู้ควบคุมข้อมูล หรือเป็น ผู้ประมวลผลข้อมูล ที่จะเก็บและประมวลผลข้อมูลส่วนบุคคลของพลเมืองจากประเทศในกลุ่มสหภาพยุโรป จะต้องคำนึงถึงการปฏิบัติให้สอดคล้องกับมาตรการ GDPR ด้วยความระมัดระวังอย่างมาก

ประเด็นนี้ ได้สร้างความกังวลจากหลายฝ่ายที่เริ่มตระหนักถึงความสำคัญของ GDPR โดยมองว่าถึงแม้ผู้ประกอบการไทยอาจไม่โดนดำเนินคดีทางกฎหมายจากการไม่ปฏิบัติตามหรือปฏิบัติขัดกับหลักการ GDPR แต่โดยที่ธรรมชาติของการติดต่อธุรกิจระหว่างประเทศต้องมีการแลกเปลี่ยนข้อมูลระหว่างกันอยู่แล้ว หากฝ่ายผู้ประกอบการทางยุโรปเห็นว่าบริษัทคู่ค้าของไทยไม่สามารถปฏิบัติตาม GDPR บริษัท EU ก็จะไม่สามารถแลกเปลี่ยนข้อมูลกับบริษัทในไทย ซึ่งก็จะส่งผลให้ไม่สามารถทำธุรกิจธุรกรรมกันได้ในที่สุด นอกจากนี้ สหภาพยุโรปอาจใช้มาตรการแทรกแซงทางการค้าอื่น ๆ ในลักษณะเช่นเดียวกับใช้มาตรการตอบโต้ทางการค้า หรือการให้ “ใบเหลือง” แก่ประเทศไทยจากกรณีปัญหา Illegal, Unreported and Unregulated Fishing (IUU) เมื่อเดือนเมษายน 2558 โดยระบุว่าเป็นประเทศที่ไม่ให้ความร่วมมือในการต่อต้านการทำประมงที่ผิดกฎหมาย ซึ่งสหภาพยุโรปได้ใช้มาตรการคว่ำบาตรการนำเข้าอาหารทะเลจากประเทศที่เพิกเฉยต่อการแก้ไขปัญหา นั่นหมายความว่าในประเด็นเรื่องสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนี้ ประเทศไทยจึงจะต้องให้ความสนใจเป็นพิเศษเช่นเดียวกัน

จากที่กล่าวมาจะเห็นได้ว่า ผลกระทบจาก GDPR ย่อมเป็นปัจจัยสำคัญประการหนึ่งที่ทำให้กระบวนการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ได้ผ่านการพิจารณาออกมาได้ ทั้ง ๆ ที่มีความพยายามต่อสู้โดยนักวิชาการและภาคประชาสังคมเพื่อเรียกร้องให้มีการออกกฎหมายคุ้มครองข้อมูลส่วนบุคคลมาอย่างยาวนานนับสิบปีแต่ไม่ประสบความสำเร็จ ทว่าเมื่อเกิดภาวะกดดันในเรื่องประเด็นผลประโยชน์ทางการค้าการลงทุนข้างต้น กฎหมายคุ้มครองข้อมูลส่วนบุคคลกลับสามารถผ่านการพิจารณาออกมาได้อย่างรวดเร็ว

5.1.1.2 ระบบกฎหมายภายในที่กำหนดมาตรการคุ้มครองสิทธิ

ในส่วนนี้จะได้พิจารณาถึงระบบกฎหมายของประเทศไทยภายหลังจากที่ได้มีการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ออกมาให้มีผลบังคับใช้แล้ว ว่าจะทำให้ระบบกฎหมายภายในของประเทศไทยมีรูปแบบการคุ้มครองข้อมูลส่วนบุคคลเช่นใด เมื่อเปรียบเทียบกับรูปแบบของต่างประเทศ

ในเบื้องต้นนี้จะเห็นว่ารูปแบบของการบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ได้เคยกล่าวไว้แล้วในบทก่อนสามารถจำแนกได้โดยสรุปดังนี้

รูปแบบที่หนึ่ง การบัญญัติกฎหมายในลักษณะกฎหมายกลางที่มีหลักการคุ้มครองข้อมูลส่วนบุคคลครอบคลุมภาคส่วนต่าง ๆ ไว้ในกฎหมายฉบับหลักฉบับเดียว ดังจะเห็นได้จากกรณีของประเทศภาคพื้นยุโรป

รูปแบบที่สอง การบัญญัติกฎหมายในลักษณะเฉพาะภาคส่วน (Target or Specific or Sectoral Legislation) หรืออาจเรียกว่าการคุ้มครองข้อมูลส่วนบุคคลกระจัดกระจายใน กฎหมายหลายฉบับ โดยไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะในลักษณะกฎหมายกลาง การบัญญัติกฎหมายแนวทางนี้จะประกอบด้วยกฎหมายหลายฉบับที่มีขอบเขตใช้บังคับกับภาคส่วนต่าง ๆ เช่น ภาคธุรกิจโทรคมนาคม การบริการสาธารณสุข การเงินการธนาคาร เป็นต้น ดังจะเห็นได้จากกรณีของประเทศเช่นสหรัฐอเมริกา

รูปแบบที่สาม ไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะรวมทั้งไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลเฉพาะภาคส่วนต่าง ๆ แต่มีกฎหมายอื่นที่อาจนำมาปรับใช้กับการคุ้มครองข้อมูลส่วนบุคคลเหมือนเช่นในยุคต้นของพัฒนาการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยที่อาศัยกฎหมายแพ่งและกฎหมายอาญา

จากที่กล่าวมาข้างต้น จะเห็นว่าปัจจุบันนั้น ประเทศไทยใช้รูปแบบทั้งการบัญญัติกฎหมายในลักษณะกฎหมายกลางที่มีหลักการคุ้มครองข้อมูลส่วนบุคคลครอบคลุมภาคส่วนต่าง ๆ ไว้ในกฎหมายฉบับหลัก คือมีการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ออกมาใช้บังคับเป็นที่เรียบร้อยแล้ว และยังมีการบัญญัติกฎหมายในลักษณะเฉพาะภาคส่วน (Target or Specific or Sectoral Legislation) เพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลเฉพาะเรื่อง เช่น กรณีของข้อมูลส่วนบุคคลเกี่ยวกับเครดิต ก็จะมีพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ.2545 หรือกรณีของข้อมูลส่วนบุคคลในด้านสุขภาพ ก็จะมีพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ.2550 หรือกรณีของข้อมูลส่วนบุคคลที่อยู่ในความควบคุมของภาครัฐก็จะมีพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 ฯลฯ เป็นต้น

โดยการคุ้มครองตามกฎหมายเฉพาะต่าง ๆ นั้น ก็อยู่ภายใต้หลักการของมาตรา 3 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ที่กำหนดว่า ในกรณีที่มีกฎหมายว่าด้วยการใดบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในลักษณะใด กิจการใด หรือหน่วยงานใดไว้โดยเฉพาะแล้ว ให้บังคับไปตามบทบัญญัติแห่งกฎหมายว่าด้วยการนั้น แต่อย่างไรก็ดี บทบัญญัติมาตรา 3 นี้ ได้กำหนดข้อยกเว้นไว้ว่าอย่างไรก็จะต้องนำหลักการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลไปใช้บังคับในกรณีดังนี้

ประการแรก คือ บทบัญญัติเกี่ยวกับการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคล และตามบทบัญญัติเกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคล รวมทั้ง บทกำหนดโทษที่

เกี่ยวข้องกำหนดให้บังคับตามพระราชบัญญัตินี้เป็นการเพิ่มเติม ไม่ว่าจะซ้ำกับบทบัญญัติว่าด้วยการนั้นหรือไม่'[253]

ประการที่สอง คือ บทบัญญัติเกี่ยวกับการร้องเรียน, บทบัญญัติที่ให้อำนาจแก่คณะกรรมการผู้เชี่ยวชาญออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคล และบทบัญญัติเกี่ยวกับอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ รวมทั้งบทกำหนดโทษที่เกี่ยวข้อง ให้บังคับตามบทบัญญัติแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ในกรณีที่กฎหมายนั้นไม่มีบทบัญญัติเกี่ยวกับการร้องเรียน หรือ ในกรณีที่กฎหมายนั้นมีบทบัญญัติให้อำนาจแก่เจ้าหน้าที่ผู้มีอำนาจพิจารณาเรื่องร้องเรียนแต่อำนาจของเจ้าหน้าที่ตามกฎหมายนั้นไม่เพียงพอเท่ากับอำนาจของคณะกรรมการผู้เชี่ยวชาญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล และเจ้าหน้าที่นั้นได้ร้องขอต่อคณะกรรมการผู้เชี่ยวชาญหรือเจ้าของข้อมูลส่วนบุคคลผู้เสียหายยื่นคำร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญแล้วแต่กรณี[254]

ดังนั้น จึงสรุปได้ว่า ประเทศไทยใช้รูปแบบของระบบกฎหมายแบบผสม กล่าวคือ ในกรณีที่มีการกำหนดหลักการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลเรื่องใดหรือกรณีใดไว้โดยเฉพาะแล้วก็บังคับไปตามกฎหมายฉบับนั้น แต่หากไม่มีหรือมีแต่มาตรฐานของการคุ้มครองสิทธินั้นไม่ทัดเทียมกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 แล้วก็ต้องบังคับตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ซึ่งถือเป็นกฎหมายกลางนั่นเอง

เมื่อพิจารณาถึงสาระสำคัญของกฎหมายกลาง หรือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 เปรียบเทียบกับ หลักการตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ที่ได้วางหลักการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลไว้เป็นสิทธิพื้นฐานของประชาชนชาวไทย ตามที่ปรากฏในมาตรา 32 ว่า

> บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว การกระทำอันเป็นการละเมิดหรือกระทบต่อสิทธิของบุคคลตามวรรคหนึ่ง หรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใด ๆ จะกระทำมิได้ เว้นแต่ โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ

---

[253] มาตรา 3 (1) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

[254] มาตรา 3 (2) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

ซึ่งจากหลักการนี้สามารถสรุปสาระสำคัญได้ คือ[255]

1. การคุ้มครองข้อมูลส่วนบุคคล คือ สิทธิความเป็นส่วนตัวประการหนึ่งที่ได้รับการคุ้มครองในฐานะที่เป็นสิทธิขั้นพื้นฐานตามรัฐธรรมนูญแห่งราชอาณาจักรไทย

2. การกระทำอันเป็นการละเมิดหรือกระทบต่อสิทธิของบุคคล หรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใด ๆ จะกระทำมิได้เว้นแต่จะมีอำนาจตามกฎหมาย

3. การจะนำข้อมูลส่วนบุคคลไปใช้ประโยชน์จะกระทำได้ต่อเมื่ออาศัยอำนาจตามบทบัญญัติของกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นและต้องเพื่อประโยชน์สาธารณะเท่านั้น

จะเห็นว่าหลักการมีความสอดคล้องกัน โดยหลักการของรัฐธรรมนูญได้ถูกอธิบายรายละเอียดของการคุ้มครองไว้ในกฎหมายกลางหรือพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไว้ ให้การคุ้มครองสิทธิมีความชัดเจนเป็นรูปธรรมมากขึ้น

นอกจากนี้ เมื่อพิจารณาถึงความสัมพันธ์ระหว่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กับกฎหมายฉบับอื่น โดยเฉพาะอย่างยิ่งกับพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 ซึ่งเป็นกฎหมายที่ตราออกมาก่อนหน้า และเป็นกฎหมายที่มีการวางหลักการคุ้มครองสิทธิในความความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลซึ่งอยู่ในความครอบครองของภาครัฐไว้แต่เดิมแล้ว จะเห็นว่า พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 ซึ่งเป็นกฎหมายกลางที่ออกมารองรับ “สิทธิที่จะได้รู้” ของประชาชน โดยมีหลักการพื้นฐานในเรื่องของการเปิดเผยข้อมูลของราชการให้กับประชาชนได้รับทราบ โดยกำหนดให้เป็นหน้าที่ของหน่วยงานของรัฐและเจ้าหน้าที่ของรัฐที่ต้องปฏิบัติให้เป็นไปตามกฎหมายเพื่อรองรับและคุ้มครองสิทธิของประชาชนภายใต้แนวคิดที่ว่า “เปิดเผยเป็นหลัก ปกปิดเป็นข้อยกเว้น” ควบคู่ไปกับความเป็นกฎหมายกลางที่กำหนดหลักเกณฑ์และวิธีการคุ้มครองข้อมูลส่วนบุคคลของประชาชนที่อยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐ ภายใต้แนวคิดที่ว่า “ปกปิดเป็นหลัก เปิดเผยเป็น ข้อยกเว้น” โดยในหลักการพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 จะมีบทบัญญัติรับรองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของข้อมูลที่อยู่ในความครอบครองของหน่วยงานของรัฐไว้ใน ซึ่งเมื่อพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ผ่านการพิจารณาของรัฐสภาให้มีผลใช้

---

[255] วิริยะ รามสมภพ, **เอกสารวิชาการ เรื่องความสัมพันธ์ระหว่างร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... กับ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540,** หน้า 16-18, ค้นวันที่ 19 กรกฎาคม 2562 จาก http://www.oic.go.th/web2017/iwebform_viewer.asp?i=21111%2E22213705112112151111211

บังคับเป็นกฎหมายแล้ว จะมีผลต่อพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 โดยเฉพาะหมวด 3 ข้อมูลข่าวสารส่วนบุคคล ในมาตรา 21 - 25 โดยจะพบประเด็นปัญหาดังนี้[256]

ประการแรก ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล มาตรา 3 กำหนดว่า ในกรณีที่มีกฎหมายว่าด้วยการใดบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในลักษณะใด กิจการใดหรือหน่วยงานใดไว้โดยเฉพาะแล้ว ให้บังคับตามบทบัญญัติแห่งกฎหมายว่าด้วยการนั้น เว้นแต่

1. บทบัญญัติเกี่ยวกับการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคล และบทบัญญัติเกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคล รวมทั้งบทกำหนดโทษที่เกี่ยวข้องให้บังคับตามบทบัญญัติแห่งพระราชบัญญัตินี้เป็นการเพิ่มเติม ไม่ว่าจะซ้ำกับบทบัญญัติแห่งกฎหมายว่าด้วยการนั้นหรือไม่ก็ตาม

2. บทบัญญัติเกี่ยวกับการร้องเรียนบทบัญญัติที่ให้อำนาจแก่คณะกรรมการผู้เชี่ยวชาญออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคล และบทบัญญัติเกี่ยวกับอำนาจหน้าที่ของพนักงานเจ้าหน้าที่รวมทั้งบทกำหนดโทษที่เกี่ยวข้อง ให้บังคับตามบทบัญญัติแห่งพระราชบัญญัตินี้ ในกรณีดังต่อไปนี้

1) ในกรณีที่กฎหมายว่าด้วยการนั้นไม่มีบทบัญญัติเกี่ยวกับการร้องเรียน

2) ในกรณีที่กฎหมายว่าด้วยการนั้นมีบทบัญญัติที่ให้อำนาจแก่เจ้าหน้าที่ผู้มีอำนาจ พิจารณาเรื่องร้องเรียนตามกฎหมายดังกล่าวออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคล แต่ไม่ เพียงพอเท่ากับอำนาจของคณะกรรมการผู้เชี่ยวชาญตามพระราชบัญญัตินี้และเจ้าหน้าที่ผู้มีอำนาจตามกฎหมายดังกล่าวร้องขอต่อคณะกรรมการผู้เชี่ยวชาญหรือเจ้าของข้อมูลส่วนบุคคลผู้เสียหายยื่นคำร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญตามพระราชบัญญัตินี้แล้วแต่กรณี

ในกรณีนี้จะเห็นว่า มาตรา 3 (1) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลจะมีผลกระทบกับการปฏิบัติตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 ในส่วนที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานของรัฐ เนื่องจากการเก็บรวมรวม การใช้ การเปิดเผยข้อมูลส่วนบุคคล บทกำหนดโทษที่เกี่ยวข้องและการร้องเรียน หากหน่วยงานของรัฐต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล จะส่งผลกระทบต่อการปฏิบัติหน้าที่โดยเฉพาะคณะกรรมการข้อมูลข่าวสารของราชการ (กขร.) ซึ่งมีอำนาจหน้าที่พิจารณาและให้ความเห็นเรื่องร้องเรียน กรณีที่มีผู้ร้องเรียนว่าหน่วยงานของรัฐไม่ปฏิบัติตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 ในเรื่องที่เกี่ยวกับข้อมูลข่าวสารส่วนบุคคล (มาตรา 21 - มาตรา 25) และการปฏิบัติหน้าที่ของ คณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสาร (กวฉ.) ในการพิจารณาวินิจฉัยอุทธรณ์คำสั่งของหน่วยงานของรัฐที่ปฏิเสธไม่ดำเนินการแก้ไขข้อมูลส่วนบุคคล

---

[256] *เรื่องเดียวกัน*, หน้า 183-185.

ตามที่เจ้าของข้อมูลข่าวสารส่วนบุคคลร้องขอ (ตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มาตรา 25 วรรคสี่ กำหนดเป็นอำนาจหน้าที่ของ กวฉ.) เนื่องจากตามพระราชบัญญัติคุ้มครอง ข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 72 (1) บัญญัติให้คณะกรรมการผู้เชี่ยวชาญมีหน้าที่และอำนาจในการพิจารณาเรื่องร้องเรียน ประกอบกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลดังกล่าวนี้ มี บทบัญญัติเกี่ยวกับความรับผิดทางแพ่ง โทษอาญา และโทษทางปกครอง กับผู้ควบคุมข้อมูลส่วน บุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลด้วย แต่ในพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 ไม่มีบทบัญญัติความรับผิดทางแพ่ง โทษอาญา และโทษทางปกครอง กับหน่วยงานของรัฐ และเจ้าหน้าที่ของรัฐ ที่รับผิดชอบในการเก็บรวมรวม การใช้ การเปิดเผยข้อมูลส่วนบุคคล และ การควบคุมดูแลข้อมูลส่วนบุคคลไว้แต่อย่างใด

ประการที่สอง สำหรับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 4 กำหนดหลักการว่า พระราชบัญญัตินี้ไม่ใช้บังคับแก่

1. การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลที่ทำการเก็บรวมรวมเพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น

2. การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ หรือ การรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์

3. บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมไว้เฉพาะเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น

4. สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดย สภาดังกล่าว ซึ่งเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามหน้าที่และ อำนาจของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมาธิการ แล้วแต่กรณี

5. การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

6. การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

การยกเว้นไม่ให้นำบทบัญญัติแห่งพระราชบัญญัตินี้ทั้งหมดหรือแต่บางส่วนมาใช้บังคับ แก่ผู้ควบคุมข้อมูลส่วนบุคคลในลักษณะใด กิจการใด หรือหน่วยงานใดทำนองเดียวกับผู้ควบคุม ข้อมูลส่วนบุคคลตามวรรคหนึ่งหรือเพื่อประโยชน์สาธารณะอื่นใด ให้ตราเป็นพระราชกฤษฎีกา

เมื่อพิจารณาแล้วจะเห็นว่า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล เป็นกฎหมายกลาง ซึ่งจะต้องเป็นหลักในการให้การดูแลและให้ความคุ้มครองข้อมูลส่วนบุคคลของประชาชนอย่างแท้จริง การมีบทยกเว้นมิให้นำกฎหมายนี้ไปใช้บังคับกับหน่วยงานใดต้องมีเหตุผลที่มีน้ำหนักเพียงพอที่รับฟังได้ กรณีของ มาตรา 4 (4) ยกเว้นไม่ใช้บังคับกับสภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึง คณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าว ซึ่งเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในการ พิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมาธิการแล้วแต่กรณี จึงเป็นเรื่องที่ไม่เหมาะสม เพราะเกิดประเด็นคำถามตามมาว่า หน่วยงานของรัฐแห่งอื่นที่มีหน้าที่และอำนาจในการพิจารณาในลักษณะเดียวกันถึงไม่ได้รับการพิจารณายกเว้นมิให้ใช้บังคับ และนอกจากนี้ กรณีมาตรา 4 (6) ยกเว้นไม่ใช้บังคับกับการดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิก ตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต เนื่องจากเมื่อพิจารณาจากพระราชบัญญัติการประกอบธุรกิจข้อมูล เครดิต พ.ศ.2545 คำว่า “สถาบันการเงิน” หมายความว่า นิติบุคคลที่ได้รับอนุญาตให้ประกอบธุรกิจหรือดำเนินกิจการในราชอาณาจักร ดังนี้ (1) ธนาคารพาณิชย์ (2) บริษัทเงินทุน (3) บริษัท หลักทรัพย์ (4) บริษัทเครดิตฟองซิเอร์ (5) บริษัทประกันวินาศภัย (6) บริษัทประกันชีวิต (7) นิติบุคคลที่ให้บริการบัตรเครดิต (8) นิติบุคคลที่มีกฎหมายเฉพาะจัดตั้งขึ้นเพื่อดำเนินการทางการเงิน (9) นิติบุคคลอื่นที่ประกอบกิจการให้สินเชื่อเป็นทางการค้าปกติตามที่คณะกรรมการประกาศกำหนด และคำว่า “สมาชิก” หมายความว่า สถาบันการเงินที่บริษัทข้อมูลเครดิตรับเข้าเป็นสมาชิก ซึ่งในการยกเว้นไม่ใช้บังคับกับการดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต เป็นการยกเว้นให้กับภาคสถาบันการเงิน และบริษัทประกันภัยซึ่งเป็นภาคธุรกิจที่มีขนาดใหญ่มากและในระยะเวลาที่ผ่านมาภาคธุรกิจกลุ่มนี้มีการละเมิดข้อมูลส่วนบุคคลจำนวนมาก จะเห็นได้จากกรณีที่มีบริษัทประกันภัยโทรศัพท์ติดต่อหรือส่งเมล์หรือเอาข้อมูลส่วนบุคคลของผู้อื่นมาใช้ประโยชน์เพื่อการขายประกันอยู่เป็นประจำ จึงเป็นเรื่องที่ไม่เหมาะสมหากยกเว้นไม่ใช้บังคับกับการดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต เช่นนี้

ประการที่สาม มาตรา 6 ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลนี้ “ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคล นั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ ซึ่งคำว่า“บุคคล” จึงหมายความว่า บุคคลธรรมดา เช่นนี้จะเห็นว่า นิยามคำว่า “ข้อมูลส่วนบุคคล” ดังกล่าว มีความหมายไม่ชัดเจน อาจมีปัญหา ในการตีความ และการทำความเข้าใจของประชาชนและหน่วยงานผู้ปฏิบัติได้ จึงควรที่จะใช้นิยามในลักษณะเดียวกับคำว่า “ข้อมูลข่าวสารส่วนบุคคล” ตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 ที่หมายความว่า ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะ การเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้น

หรือมี เลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่าย และให้หมายความรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย โดยการกำหนดนิยามเช่นเดียวกันเช่นนี้น่าจะมีความหมายที่ชัดเจนและเข้าใจได้ง่ายกว่า นอกจากนี้ ข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ก็ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม ซึ่งในหลักการสมควรที่จะให้ความคุ้มครองด้วย เพราะหากมีการนำข้อมูลส่วนบุคคลของผู้ที่ถึงแก่กรรมไปเปิดเผยอาจทำให้เกิดผลกระทบและสร้างความเสียหายแก่ผู้ที่ถึงแก่กรรมซึ่งเป็นเจ้าของข้อมูล รวมถึงบรรดาทายาทของผู้ที่ถึงแก่กรรมแล้วด้วย ในหลักจึงสมควรที่จะกำหนดนิยามให้ครอบคลุมถึงข้อมูลส่วนบุคคลของผู้ที่ถึงแก่กรรมแล้วด้วย เช่นเดียวกับพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540

ประการที่สี่ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล มาตรา 26 ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติ อาชญากรรม ข้อมูลสุขภาพ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่ ตามที่บัญญัติไว้ใน (1) - (5) เห็นว่า ตามหลักการของมาตรา 26 เป็นเรื่องการห้ามเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) เนื่องจากเป็นข้อมูลข่าวสารที่จะทำให้เกิดมีการเลือกปฏิบัติอย่างหนึ่งอย่างใดกับ เจ้าของข้อมูลส่วนบุคคลนั้น ๆ ได้ ในหลักการจึงห้ามไม่ให้มีการจัดเก็บข้อมูลที่มีความอ่อนไหวต่อความรู้สึกของประชาชน เว้นแต่จะได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลก่อน แต่การที่พระราชบัญญัตินี้มีข้อยกเว้นที่จัดเก็บได้โดยไม่ต้องได้รับความยินยอมในมาตรา 26 (1) - (5) นั้น น่าจะเป็นข้อยกเว้นที่มากเกินความจำเป็นอันจะทำให้ข้อมูลส่วนบุคคลที่มีความอ่อนไหวไม่ได้รับความคุ้มครองเท่าที่ควร สำหรับพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 ไม่มีบทบัญญัติเกี่ยวกับการห้ามเก็บรวบรวมข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) แต่อย่างใด เช่นนี้จึงสมควรที่จะต้องมีการกำหนดหลักการเรื่องนี้ไว้ในพระราชบัญญัติข้อมูลข่าวสารของราชการด้วย

ประการที่ห้า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล มาตรา 41 บัญญัติให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Privacy Data Officer) มีหน้าที่ ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งประสานงานและให้ความร่วมมือ กับสำนักงานในกรณีที่มีปัญหาเกี่ยวกับการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคล

หรือผู้ประมวลผลข้อมูลส่วนบุคคลในการปฏิบัติตามพระราชบัญญัตินี้ และรักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่

เมื่อพิจารณาแล้วจะเห็นว่า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล กำหนดให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล มีหน้าที่ตามที่กล่าวไว้ในมาตรา 41 ซึ่งเป็นเรื่องที่มีความสำคัญต้องอาศัย ผู้ที่มีความรู้และประสบการณ์ในการปฏิบัติหน้าที่ดังกล่าว แต่พระราชบัญญัตินี้มิได้มีการบัญญัติ ในเรื่องคุณวุฒิหรือคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไว้แต่อย่างใด จึงสมควรที่จะได้มีการกำหนดคุณวุฒิ หรือคุณสมบัติ และประสบการณ์ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไว้ด้วย ซึ่งเมื่อพิจารณาเปรียบเทียบกับ พระราชบัญญัติข้อมูลข่าวสารของราชการแล้ว ก็เห็นว่าไม่ได้มีการกำหนดตำแหน่งหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไว้แต่อย่างใด เช่นนี้ เพื่อให้กฎหมายคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลเป็นไปในทิศทางเดียวกัน จึงสมควรที่จะได้มีการแก้ไข พระราชบัญญัติข้อมูลข่าวสารของราชการให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย

5.1.2 วิเคราะห์การกำหนดนิยามและขอบเขตของข้อมูลส่วนบุคคล

5.1.2.1 วิเคราะห์นิยามของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และกฎหมายอื่น

ด้วยเหตุที่ประเทศไทยปัจจุบัน ใช้รูปแบบการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลโดยการบัญญัติกฎหมายในลักษณะกฎหมายกลางที่มีหลักการคุ้มครองข้อมูลส่วนบุคคลครอบคลุมภาค ไว้ในกฎหมายฉบับหลัก และจะมีการบัญญัติกฎหมายในลักษณะเฉพาะภาคส่วน เพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลเฉพาะเรื่องอีกด้วย การทำความเข้าใจกับนิยามของคำว่าข้อมูลส่วนบุคคล จึงจะต้องพิจารณาจากทั้งนิยามของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นกฎหมายฉบับหลัก และนิยามตามกฎหมายฉบับอื่น ๆ ประกอบด้วยกล่าวคือ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 6 กำหนดนิยามคำว่า “ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 มาตรา 4 กำหนดนิยามคำว่า “ข้อมูลข่าวสารส่วนบุคคล” หมายความว่า ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะ การเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้นหรือมีเลขหมาย รหัสหรือ สิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่น

บันทึกลักษณะเสียงของคนหรือรูปถ่าย และให้หมายความ รวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย

พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ.2545 มาตรา 3 กำหนดนิยามคำว่า “ข้อมูลเครดิต” หมายความว่า ข้อเท็จจริงเกี่ยวกับลูกค้าที่ขอสินเชื่อ ดังต่อไปนี้

(1) ข้อเท็จจริงที่บ่งชี้ถึงตัวลูกค้า และคุณสมบัติของลูกค้าที่ขอสินเชื่อ

(ก) กรณีบุคคลธรรมดา หมายถึง ชื่อ ที่อยู่ วันเดือนปีเกิด สถานภาพการสมรส อาชีพ เลขที่บัตรประจำตัวประชาชน หรือบัตรประจำตัวเจ้าหน้าที่ของรัฐ หรือหนังสือเดินทาง และเลขประจำตัวผู้เสียภาษีอากร (ถ้ามี)

(ข) กรณีนิติบุคคล หมายถึง ชื่อ สถานที่ตั้ง เลขที่ทะเบียนการจัดตั้งนิติบุคคล หรือเลขประจำตัวผู้เสียภาษีอากร

(2) ประวัติการขอและการได้รับอนุมัติสินเชื่อ และการชำระสินเชื่อของลูกค้าที่ขอ

สินเชื่อ รวมทั้งประวัติการชำระราคาสินค้าหรือบริการโดยบัตรเครดิต

พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ.2550 ไม่มีการกำหนดนิยามของคำว่า “ข้อมูลด้านสุขภาพไว้” แต่ได้มีการกำหนดหลักการคุ้มครองในมาตรา 7 ว่า ข้อมูลด้านสุขภาพของบุคคลเป็นความลับส่วนบุคคล ผู้ใดจะนำไปเปิดเผยในประการที่น่าจะทำให้บุคคลนั้นเสียหายไม่ได้ เว้นแต่การเปิดเผยนั้นเป็นไปตามความประสงค์ของบุคคลนั้นโดยตรง หรือมีกฎหมายเฉพาะบัญญัติให้ต้องเปิดเผย แต่ไม่ว่าในกรณีใด ๆ ผู้ใดจะอาศัยอำนาจหรือสิทธิตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการหรือกฎหมายอื่นเพื่อขอเอกสารเกี่ยวกับข้อมูลด้านสุขภาพของบุคคลที่ไม่ใช่ของตนไม่ได้

อย่างไรก็ตาม ในประเด็นนี้ จึงทำให้เกิดปัญหาไม่สามารถกำหนดความหมายและขอบเขตการคุ้มครองสิทธิเกี่ยวกับข้อมูลส่วนบุคคลด้านสุขภาพที่ชัดเจน ทำให้เกิดความสับสนในการตีความ และการใช้บังคับกฎหมายที่เกี่ยวข้องในทางปฏิบัติ[257] นอกจากนี้ ยังพบปัญหาอีกประการหนึ่งก็คือ ความไม่ชัดเจนของบทบัญญัติเกี่ยวกับการคุ้มครองข้อมูลด้านสุขภาพของบุคคลและความขัดแย้งกันเองของบทบัญญัติ เนื่องจากบทบัญญัติมาตรา 7 แห่งพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 มีถ้อยคำว่า “ผู้ใดจะนำไปเปิดเผยในประการที่น่าจะทำให้บุคคลนั้นเสียหายไม่ได้” จึงไม่ชัดเจนว่า ต้องใช้เกณฑ์การวินิจฉัยอย่างวิญญูชน และเป็นพฤติการณ์ประกอบการกระทำอันจะทำให้การ

---

[257] หทัยชนก หร่ายวงศ์, **ปัญหาเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลด้านสุขภาพ** (วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2548), หน้า 116.

คุ้มครองตามบทบัญญัตินี้ไม่ครอบคลุมการเปิดเผยที่ไม่น่าจะเกิดความเสียหายแก่เจ้าของข้อมูลด้วยหรือไม่ ก่อให้เกิดความสับสนในการตีความบทบัญญัติ แม้บทบัญญัติดังกล่าวกำหนดกรณียกเว้นตามที่ได้กล่าวมาข้างต้น แต่ภายใต้บทบัญญัติเดียวกันกลับบัญญัติตอนท้ายว่า “แต่ไม่ว่าในกรณีใด ๆ ผู้ใดจะอาศัยอำนาจหรือสิทธิตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการหรือกฎหมายอื่นเพื่อขอเอกสารเกี่ยวกับข้อมูลด้านสุขภาพของบุคคลที่ไม่ใช่ของตนไม่ได้” ย่อมมีนัยเป็นการปฏิเสธการใช้อำนาจและสิทธิตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการและกฎหมายอื่นเพื่อขอเอกสารเกี่ยวกับข้อมูลส่วนบุคคลด้านสุขภาพที่ผู้ขอมิใช่เจ้าของข้อมูลในทุก ๆ กรณี แม้ผู้ขอได้รับความยินยอมจากเจ้าของข้อมูลซึ่งเป็นกรณีที่บทบัญญัตินั้นกำหนดรับรองในตอนต้นแล้วก็ตาม จากความขัดแย้งกันเองของบทบัญญัติดังกล่าว ก่อให้เกิดความสับสนในการตีความ และการใช้บังคับกฎหมายของเจ้าหน้าที่ หน่วยงาน และบุคคลที่เกี่ยวข้อง[258] ซึ่งประเด็นทั้งสองนี้ สมควรที่จะได้มีการปรับปรุงแก้ไขกฎหมายต่อไป

ตารางที่ 5.1 เปรียบเทียบนิยามของข้อมูลส่วนบุคคลตามกฎหมายฉบับต่าง ๆ ของประเทศไทย

	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562	**พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540**	**พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ.2545**	**พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ.2550**
นิยาม	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ	ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้นหรือมีเลขหมาย	ข้อเท็จจริงเกี่ยวกับลูกค้าที่ขอสินเชื่อดังต่อไปนี้ (1) ข้อเท็จจริงที่บ่งชี้ถึงตัวลูกค้า และคุณสมบัติของลูกค้าที่ขอสินเชื่อ (ก) กรณีบุคคลธรรมดา หมายถึง ชื่อ ที่อยู่ วันเดือนปี	ไม่มี

[258] *เรื่องเดียวกัน*, หน้า 110-111.

ตารางที่ 5.1 (ต่อ)

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562	พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540	พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ.2545	พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ.2550
	รหัสหรือ สิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่าย และให้หมายความรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย	เกิด สถานภาพ การสมรส อาชีพ เลขที่บัตรประจำตัวประชาชน หรือบัตรประจำตัวเจ้าหน้าที่ของรัฐ หรือหนังสือเดินทาง และเลขประจำตัวผู้เสียภาษีอากร (ถ้ามี) (ข) กรณีนิติบุคคล หมายถึง ชื่อ สถานที่ตั้ง เลขที่ทะเบียนการจัดตั้งนิติบุคคล หรือเลขประจำตัวผู้เสียภาษีอากร (2) ประวัติการขอและการได้รับอนุมัติสินเชื่อ และการชำระสินเชื่อของลูกค้าที่ขอสินเชื่อ รวมทั้งประวัติการชำระราคาสินค้าหรือบริการโดยบัตรเครดิต	

เมื่อพิจารณาเปรียบเทียบกันระหว่างกฎหมายฉบับต่าง ๆ ที่ถูกตราขึ้นมาเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ในประเด็นเรื่องของนิยามศัพท์แล้วจะเห็นว่า นิยามของคำว่า “ข้อมูลส่วนบุคคล” นั้นถือเป็นถ้อยคำสำคัญของกฎหมายทุกฉบับที่กล่าวมา ทั้งนี้เพราะข้อมูลส่วนบุคคลนี้ถือเป็นวัตถุแห่งสิทธิ ที่กฎหมายมุ่งจะรับรองและคุ้มครองให้แก่เจ้าของข้อมูลส่วนบุคคลซึ่งถือเป็นผู้ทรงสิทธิตามกฎหมาย ซึ่งเมื่อได้พิจารณานิยามของคำว่าข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ซึ่งถือเป็นกฎหมายกลางที่วางหลักการในการคุ้มครองข้อมูลส่วนบุคคลในทุกประเภทแล้ว จะเห็นได้ว่าถ้อยคำมีความหมายทำนองเดียวกันกับ “ข้อมูลข่าวสารส่วนบุคคล” อันเป็นข้อมูลส่วนบุคคลที่ได้มีการบัญญัติรับรองไว้ในพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 ซึ่งอาจกล่าวได้ว่านิยามของข้อมูลส่วนบุคคลตามตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 น่าจะยกร่างมาจากนิยามของข้อมูลข่าวสารส่วนบุคคลตามพระราชบัญญัติข้อมูลข่าวสารของราชการฯ ดังนั้น การกำหนดนิยามของคำว่า “ข้อมูลส่วนบุคคล” ในพระราชบัญญัติข้อมูลส่วนบุคคลฯ ก็ย่อมมีเจตนารมณ์เพื่อให้ถ้อยคำทั้งสองมีความหมายอย่างเดียวกัน แม้จะใช้ถ้อยคำอธิบายหรือถ้อยคำเรียกแตกต่างกันเล็กน้อยก็ตาม และเพื่อไม่ให้เกิดความสับสนแก่บุคคลทุกฝ่ายที่มีหน้าที่จะต้องปฏิบัติและบังคับการให้เป็นไปตามกฎหมายทั้งสองฉบับ[259]

ตารางที่ 5.2 เปรียบเทียบนิยามข้อมูลส่วนบุคคลตามกฎหมายไทยและต่างประเทศ

	นิยาม
GDPR	ข้อมูลใด ๆ ก็ตามที่เกี่ยวข้องกับบุคคลธรรมดาที่ระบุตัว หรืออาจทำให้ระบุตัวบุคคลผู้นั้นได้ ซึ่งการที่ข้อมูลนั้น “อาจระบุตัวบุคคลได้” จะเป็นโดยทางตรงหรือทางอ้อมก็ได้ โดยอาศัยสิ่งบ่งชี้ (Identifier) ต่าง ๆ ซึ่งอาจเป็น ชื่อ หมายเลขประจำตัวประชาชน ที่อยู่ เอกลักษณ์ออนไลน์ (Online Identifier) หรือเอกลักษณ์ทางร่างกายอย่างใดอย่างหนึ่ง ลักษณะทางกายภาพ พันธุกรรม จิตใจ เศรษฐกิจ วัฒนธรรม หรือสังคมของบุคคล นั้น เป็นต้น
ประเทศฝรั่งเศส	ข้อมูลส่วนบุคคลที่เปิดเผยโดยตรงหรือโดยอ้อมเชื้อชาติและเชื้อชาติความคิดเห็นทางการเมืองปรัชญาหรือศาสนาหรือสหภาพแรงงานของบุคคลหรือที่เกี่ยวข้องกับสุขภาพหรือชีวิตทางเพศของพวกเขา

[259] นนทวัชร์ นวตระกูลพิสุทธิ์, *เรื่องเดิม,* หน้า 746-747.

ตารางที่ 5.2 (ต่อ)

	นิยาม
ประเทศเยอรมนี	หมายรวมถึงข้อมูลส่วนบุคคลอื่น ๆ เช่น ข้อมูลเกี่ยวกับความสัมพันธ์ภายในครอบครัว ข้อมูลเกี่ยวกับเรื่องทรัพย์สินและภาษีของบุคคล ข้อมูลเกี่ยวกับความลับในทางธุรกิจต่าง ๆ ฯลฯ เป็นต้น
ประเทศสหรัฐอเมริกา	นิยามแตกต่างกันไปตามแต่ละมลรัฐหรือกฎหมายแต่ละฉบับ เช่น กฎหมายของมลรัฐ California กำหนดนิยามข้อมูลส่วนบุคคลว่าหมายถึง “ชื่อบุคคล ชื่อสกุล ซึ่งเมื่อพิจารณารวม กับข้อมูลอื่น ๆ เช่น ข้อมูลเลขหมายประกันสังคม ข้อมูลใบขับขี่ ข้อมูลบัญชี บัตรเครดิต และเมื่อใช้ร่วมกับ รหัสผ่านหรือรหัสเพื่อความปลอดภัยแล้วสามารถทำให้เข้าถึงบัญชีการเงินของบุคคลนั้น” (California Civil Code section 1798.82) โดยต่อมามีการเพิ่มเติมข้อมูลการรักษาพยาบาลและประกันสุขภาพด้วย (California Civil Code section 1798.29 (e) (4) – (5)) มลรัฐ Wisconsin และ Iowa กำหนดนิยามรวมถึง “ข้อมูลชีวภาพ ลายนิ้วมือ เสียง ม่านตา” ส่วนมลรัฐ New York นิยามไว้กว้าง รวมถึงข้อมูลใด ๆ เกี่ยวกับบุคคลธรรมดา เช่น ชื่อ เลข หมายประจำตัว สัญลักษณ์ เครื่องหมาย หรือเครื่องบ่งชี้อื่น ซึ่งอาจระบุตัวของบุคคลนั้นได้ (New York General Business Law section 899–aa(1)(a)) เป็นต้น
ประเทศอังกฤษ	ข้อมูลที่เกี่ยวข้องกับบุคคลที่ยังมีชีวิตอยู่ซึ่งสามารถบ่งชี้ตัวบุคคลได้ จากข้อมูลนั้นเองและข้อมูลอื่น ๆ ที่อยู่ในความครอบครองของผู้ควบคุมดูแลข้อมูล (Data Controller) หรืออาจอยู่ในความครอบครองของผู้ควบคุมดูแลข้อมูลในอนาคต ทั้งนี้ รวมถึงข้อมูลเกี่ยวกับการแสดงความคิดเห็นเกี่ยวกับตัวบุคคลธรรมดาและการแสดงเจตนาของผู้ควบคุมดูแลข้อมูลหรือบุคคลอื่นที่เกี่ยวกับบุคคลธรรมดานั้นด้วย
ประเทศแคนาดา	ข้อมูลใด ๆ ทั้งที่มีการบันทึกและไม่มีการบันทึกของบุคคลที่สามารถระบุตัวตนได้ ซึ่งได้แก่ 1. อายุ ชื่อ เลขที่บัตรประชาชน รายได้ เชื้อชาติ หรือหมู่โลหิต 2. ความคิดเห็นหรือทัศนะ การประเมินคุณค่า การแสดงความเห็นสถานะทางสังคม หรือประวัติการต้องโทษหรือถูกดำเนินคดี และ 3. ข้อมูลของลูกจ้างหรือพนักงาน ข้อมูลด้านเครดิต ข้อมูลเกี่ยวกับ

ตารางที่ 5.2 (ต่อ)

	นิยาม
	หนี้สินหรือการกู้ยืม ข้อมูลเกี่ยวกับประวัติทางการแพทย์ ข้อมูลเกี่ยวกับการพิพาทระหว่างผู้บริโภคและผู้ประกอบการ หรือข้อมูลเกี่ยวกับความต้องการ (เช่น การให้ได้มาซึ่งสินค้าหรือบริการ หรือความประสงค์เปลี่ยนงาน)
ประเทศมาเลเซีย	ข้อมูลส่วนบุคคล หมายความว่า ข้อมูลใด ๆ ที่เกี่ยวกับธุรกรรมในทางพาณิชย์ซึ่งถูกประมวลผลหรือถูกบันทึกหรือจัดเก็บไว้เพื่อการประมวลผล (Process) ซึ่งสามารถระบุตัวบุคคล หรือ ข้อมูลที่เมื่อนำไปประกอบกับข้อมูลอื่น ๆ ที่มีแล้วทำให้สามารถระบุตัวบุคคลได้
ประเทศไทย	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

เมื่อพิจารณาการกำหนดนิยามของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 เปรียบเทียบกับกฎหมายต่างประเทศและกติกาสากลฉบับต่าง ๆ โดยเฉพาะ GDPR จะเห็นว่า นิยามความหมายของคำว่าข้อมูลส่วนบุคคลมีความสอดคล้องกันบางส่วน กล่าวคือ ตามหลักการของ GDPR คำว่า ข้อมูลส่วนบุคคล นั้น เป็นข้อมูลใด ๆ ก็ตามที่เกี่ยวข้องกับบุคคลธรรมดาที่ระบุตัว หรืออาจทำให้ระบุตัวบุคคลผู้นั้นได้ ซึ่งการที่ข้อมูลนั้น “อาจระบุตัวบุคคลได้” จะเป็นโดยทางตรงหรือทางอ้อมโดยจะต้องเป็นข้อมูลของบุคคลธรรมดาที่ยังคงมีชีวิตอยู่ แต่อย่างไรก็ตามใน GDPR จะมีความหมายที่ชัดเจนกว่า เนื่องจากมีการระบุเป็นตัวอย่างไว้ด้วยว่า หมายเลข ชื่อ หมายเลขประจำตัว ข้อมูลสถานที่อยู่ การระบุตัวตนทางออนไลน์หรือปัจจัยหนึ่งหรือหลายอย่างที่กล่าวถึงอันทำให้สามารถระบุลักษณะทางกายภาพ ลักษณะทางพันธุกรรม สภาพทางจิต เศรษฐกิจ วัฒนธรรม หรือสังคมของบุคคลธรรมดานั้น ก็ล้วนถือว่าเป็นข้อมูลส่วนบุคคลทั้งสิ้น อีกทั้งตาม GDPR ข้อมูลส่วนบุคคลที่ถูกทำให่ม่ (De-Identified) ข้อมูลที่ถูกเข้ารหัส (Encrypted) หรือการใช้นามแฝง (Pseudonymised) แต่สามารถประมวลผลและระบุตัวเจ้าของข้อมูลส่วนบุคคลได้ ก็ถือว่าอยู่ในบทนิยามของคำว่าข้อมูลส่วนบุคคลที่สามารถระบุตัวบุคคลนั้นได้และต้องอยู่ภายใต้บังคับกฎหมาย แต่ในส่วนของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ไม่ได้มีการยกตัวอย่างให้ชัดเจนในส่วนนี้ ซึ่งอาจทำให้มีผลในทางปฏิบัติเมื่อมีการบังคับใช้กฎหมายและจะต้องตีความนิยามดังกล่าวนี้

นอกจากนี้ยังมีประเด็นปัญหาในส่วนของนิยามศัพท์ที่จะสร้างความวิตกกังวลให้กับผู้ประกอบการต่าง ๆ ไม่เฉพาะผู้ประกอบการอินเทอร์เน็ตเท่านั้นแต่ รวมถึงผู้ประกอบการหรือผู้ที่มีส่วนเกี่ยวข้องกับระบบสารสนเทศทั้งหมดในประเทศไทย รวมถึงผู้ให้บริการธนาคาร สถาบันการเงิน ระบบสื่อสารโทรคมนาคม และระบบขนส่งสาธารณะต่าง ๆ ด้วยกล่าวคือ การกำหนดนิยามเช่นนี้ในมุมมองของผู้ประกอบการอาจจะเห็นว่ากว้างขวางเกินไป ควรให้คำจำกัดความในส่วนของข้อมูลที่ไม่ได้มีความเชื่อมโยงไปถึงตัวเจ้าของข้อมูลส่วนบุคคลนั้นได้ถ้ามีการใช้มาตรการทางเทคนิคหรือเทคโนโลยีที่มีความก้าวหน้าเพียงพอที่จะสามารถลดความเสี่ยงไม่ให้มีการระบุตัวตนของผู้เป็นเจ้าของข้อมูลได้ ข้อมูลเช่นนี้ ไม่ควรกำหนดให้เป็นข้อมูลส่วนบุคคลตามนิยามความหมายของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

5.1.2.2 วิเคราะห์ขอบเขตของข้อมูลส่วนบุคคล

1) ประเด็นข้อมูลส่วนบุคคลของผู้เสียชีวิต

จะเห็นได้ว่า การกำหนดนิยามศัพท์คำว่าข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ดังที่ได้กล่าวมาแล้วข้างต้น ไม่ได้หมายความรวมถึงข้อมูลส่วนบุคคลของผู้ถึงแก่กรรมโดยเฉพาะ ซึ่งในประเด็นนี้ มีความเห็นคัดค้านมาตั้งแต่ในช่วงระยะเวลาของการรับฟังความคิดเห็นร่างพระราชบัญญัติฯ โดยมีการให้ความเห็นว่าข้อมูลผู้เสียชีวิต ควรต้องได้รับคุ้มครอง กล่าวคือข้อมูลของผู้ถึงแก่กรรมควรได้รับการคุ้มครองเช่นเดียวกับบุคคลที่ยังมีชีวิต ดังนั้นในการการเก็บรวบรวมข้อมูลของผู้ถึงแก่กรรมอาจทำได้เมื่อมีความจำเป็นเพื่อประโยชน์สาธารณะตามข้อยกเว้นของกฎหมาย โดยการใช้และการเปิดเผยข้อมูลของผู้ถึงแก่กรรมสามารถทำได้ตามที่เคยได้รับความยินยอมจากเจ้าของข้อมูลเมื่อตอนที่ยังมีชีวิต รวมถึงการส่งหรือโอนข้อมูลของผู้ถึงแก่กรรมไปยังต่างประเทศสามารถทำได้ ตามข้อยกเว้นที่กฎหมายกำหนดอนุญาต แต่ถ้าหากว่ามีข้อมูลที่บุคคลแสดงความประสงค์เมื่อตอนที่ยังมีชีวิตอยู่ว่าไม่ให้เปิดเผย ก็ควรไม่เปิดเผยต่อไปตามความประสงค์ของเจ้าของข้อมูล แม้เจ้าของข้อมูลจะถึงแก่กรรมแล้วก็ตาม ส่วนในการกำหนดการเปิดเผยข้อมูลของผู้ถึงแก่กรรม อาจเปิดเผยถึงข้อมูลส่วนบุคคลของบุคคลอื่นที่ยังมีชีวิตอยู่ด้วย เช่น ญาติที่ยังมีชีวิตอยู่ แพทย์ผู้ทำการรักษา หรืออาจเปิดเผยถึงข้อมูลทั่วไปที่สามารถใช้ระบุบุคคลอื่น การพิจารณาเปิดเผยข้อมูลส่วนบุคคลของผู้ถึงแก่กรรมจึงจำเป็นต้องคำนึงถึงบุคคลที่ยังมีชีวิตอยู่ด้วย[260]

---

[260] เครือข่ายพลเมืองเน็ต, **ความคิดเห็นต่อร่าง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (2 ก.พ. 2561),** ค้นวันที่ 23 พฤษภาคม 2562 จาก https://thainetizen.org/docs/data-protection-bill-2018-comments/

อย่างไรก็ตาม หากพิจารณาหลักการของพระราชบัญญัติข้อมูลส่วนบุคคลฯ กับ General Data Protection Regulation ในเรื่องข้อมูลส่วนบุคคลของผู้ถึงแก่กรรมนั้นจะเห็นว่าอยู่บนพื้นฐานของหลักการเดียวกันกล่าวคือ ตาม Recital 27 ของ General Data Protection Regulation กล่าวว่า ระเบียบนี้ไม่สามารถใช้กับข้อมูลส่วนบุคคลของผู้เสียชีวิต แต่ประเทศสมาชิกอาจจัดให้มีกฎระเบียบเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลของผู้เสียชีวิตได้ นอกจากนี้ข้อมูลที่เกี่ยวกับผู้ทำพินัยกรรมที่จัดขึ้นโดยตัวแทนและผู้ที่ทำหน้าที่แทนนั้น จะไม่อยู่ภายใต้ข้อผูกพันของ GDPR[261] จากหลักการนี้จะเห็นว่า เมื่อผู้ถึงแก่กรรมนั้นไม่สามารถเป็นผู้ทรงสิทธิตาม GDPR แล้ว การคุ้มครองข้อมูลส่วนบุคคลจึงไม่อาจมีขึ้นได้ ซึ่งหลักการในเรื่องนี้ก็เป็นหลักการเช่นเดียวกันกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของอีกหลายประเทศ

สำหรับประเทศฝรั่งเศส นับแต่ปี 2016 มีการบัญญัติรับรองหลักการเรื่องสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของผู้ตาย (Post Mortem Right to Privacy) ไว้ในมาตรา 40 (1) รัฐบัญญัติสาธารณรัฐดิจิตอล (The French Digital Republic Act (Loi n°2016-1321 pour une République numérique)) ซึ่งเป็นกฎหมายหลักในการคุ้มครองข้อมูลส่วนบุคคลของฝรั่งเศส โดยกำหนดให้ บุคคลมีสิทธิที่จะควบคุมการประมวลผลข้อมูลส่วนบุคคลของพวกเขาหลังจากการตาย โดยบุคคลสามารถให้ข้อมูลแก่ผู้ควบคุมข้อมูลทั่วไปหรือข้อบ่งชี้เฉพาะเกี่ยวกับการเก็บรักษา การลบและการเปิดเผยหรือส่งผ่านข้อมูลส่วนบุคคลของเขาหลังจากการเสียชีวิตได้ ภายใต้คำสั่งเช่นนั้น ในกรณีที่ผู้ควบคุมได้รับคำสั่งเฉพาะเจาะจงจากบุคคลในการประมวลผลข้อมูลของเขาหลังจากเสียชีวิต การใช้หรือประมวลผลข้อมูลนั้นก็ต้องเป็นไปตามความยินยอมโดยที่ไม่อาจจะกระทำเป็นอย่างอื่นไปได้

ในด้านของประเทศเยอรมนี ก็ได้มีคำพิพากษาของศาลสูงของประเทศเยอรมนี (The German Federal Supreme Court (Bundesgerichtshof – “BGH”) มีคำพิพากษาในคดี Case no.III ZR 183/17 โดยตัดสินให้ Facebook จะต้องยอมให้แม่ซึ่งมีฐานะเป็นทายาทมีสิทธิเข้าถึงบัญชี (User Account) ของลูกสาวที่เสียชีวิต โดยศาลได้ตัดสินว่า สัญญาที่ลูกสาวซึ่งเสียชีวิตทำไว้กับ Facebook ควรถือเป็นส่วนหนึ่งของมรดกและควรตกแก่ทายาทโดยธรรม โดยสัญญาที่ครอบคลุมบัญชีผู้ใช้กับเครือข่ายสังคมออนไลน์ใด ๆ ก็ตามจะต้องถูกโอนถ่ายไปยังทายาทของเจ้าของบัญชีดั้งเดิมนั้น และแม่ซึ่งเป็น ทายาทมีสิทธิอย่างสมบูรณ์ที่จะเข้าถึงบัญชี Facebook ของลูกสาวที่เสียชีวิต รวมทั้งมีสิทธิในข้อมูลส่วนบุคคลที่ลูกสาวซึ่งเสียชีวิตได้โพสต์ลงใน Facebook

---

[261] Recital 27 “This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons.”

และข้อมูลส่วนตัวอื่น ๆ ทุกอย่าง[262] ซึ่งจากคำพิพากษาของศาลสูงในคดีนี้สะท้อนให้เห็นการยอมรับในสิทธิในข้อมูลส่วนบุคคลของผู้เสียชีวิตได้เป็นอย่างดี

ดังนั้น สำหรับประเทศไทยเรา แม้หลักการสากลยังมีประเด็นถกเถียงกันในเรื่องนี้อยู่จนยังไม่ได้ข้อยุติเป็นแนวทางเดียวกันก็ตาม แต่ในอนาคตก็มีแนวโน้มที่สหภาพยุโรปซึ่งเป็นสังคมที่ให้ความสำคัญกับสิทธิเสรีภาพเป็นอย่างมาก อาจปรับหลักกฎหมายของสหภาพให้เป็นไปในทิศทางเดียวกันกับประเทศฝรั่งเศสและศาลสูงของประเทศเยอรมนีก็เป็นไปได้อย่างมาก เราจึงควรที่จะเตรียมการแก้ไขหลักการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ในประเด็นนี้ต่อไปในอนาคตเพื่อขยายการคุ้มครองสิทธิในข้อมูลส่วนบุคคลของผู้เสียชีวิตต่อไป

2) ประเด็นข้อมูลส่วนบุคคลของผู้เยาว์

ในส่วนของสภาพสังคมในปัจจุบัน ผู้เยาว์ก็อาจถูกล่วงละเมิดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลได้เช่นเดียวกัน ไม่ว่าจะเป็นในลักษณะของการ เก็บรวบรวม ประมวล และ ส่งต่อ ทั้งในสภาพแวดล้อมทางกายภาพ เช่น เอกสาร และสภาพแวดล้อมทางอิเล็กทรอนิกส์ โดยเฉพาะ อย่างยิ่งการใช้งานสื่อออนไลน์ ทำให้เกิดการนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลส่วนบุคคลรูปแบบต่าง ๆ ของเด็ก เช่น ชื่อตัว ชื่อสกุล ที่อยู่ ที่อยู่จดหมายอิเล็กทรอนิกส์ หมายเลขโทรศัพท์ ภาพถ่ายที่มีข้อมูล เชื่อมโยงกับชื่อของเด็ก รวมทั้งข้อมูลอันอาจบ่งระบุตัวตนอื่น ๆ (Personally Identifiable Information) ข้อมูลเหล่านี้อาจอยู่ในความครอบครองของผู้ให้บริการต่าง ๆ ทางอินเทอร์เน็ต เช่น ผู้ให้บริการเว็บไซต์ที่ เก็บข้อมูลผู้สมัครสมาชิกที่เป็นผู้เยาว์ ผู้ให้บริการเครือข่ายสังคม หรือเครือข่ายการสนทนาออนไลน์ ข้อมูล เหล่านี้อาจเป็นต้นเหตุนำไปสู่การกระทำละเมิดต่อสิทธิในความเป็นส่วนตัวเกี่ยวกับส่วนบุคคลของเด็ก หรืออาจนำไปสู่การประกอบอาชญากรรมอื่น ๆ เช่น การเฝ้าติดตามคุกคามทางอินเทอร์เน็ต (Cyberstalking) การนำข้อมูลเชิงเอกลักษณ์ไปใช้โดยมิชอบ (Identity Theft) ก็ได้[263]

---

[262] Alexander Hardinghaus, Ramona Kimmich and Philipp Süss, **German Federal Supreme Court: Facebook Account Passes to Heirs,** Retrieved April 22, 2018 from https://www.technologylawdispatch.com/2018/07/in-the-courts/german-federal-supreme-court-facebook-account-passes-to-heirs/

[263] คณาธิป ทองรวีวงศ์, “มาตรการทางกฎหมายในการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว: ศึกษากรณีการ รบกวนสิทธิในความเป็นอยู่ส่วนตัวจากการใช้เว็บไซต์เครือข่ายสังคม,” **วารสารวิชาการสมาคม สถาบันอุดมศึกษาเอกชนแห่งประเทศไทย (สสอท.)** 18, 2 (2555): 39-51.

สำหรับในประเด็นนี้ เมื่อพิจารณาจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป General Data Protection Regulation (GDPR) มีหลักเกณฑ์ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของเด็กดังนี้

ประการแรก หลักการประมวลข้อมูลที่ชอบด้วยกฎหมายนั้น มีหลักว่า การประมวลข้อมูล นั้นมีความจำเป็นเพื่อปกป้องประโยชน์ของเจ้าของข้อมูลหรือบุคคลธรรมดาอื่น (GDPR Article 6 (1) (d)) ซึ่งอาจรวมถึงเด็ก

ประการที่สอง การประมวลข้อมูลมีความจำเป็นในกรณีผู้ประมวลข้อมูลกระทำไปเพื่อประโยชน์อันชอบด้วยกฎหมาย (Legitimate Interests) เว้นแต่กรณีที่ผลประโยชน์ของผู้ควบคุมข้อมูล จะต้องอยู่ภายใต้สิทธิหรือเสรีภาพของเจ้าของข้อมูล โดยเฉพาะอย่างยิ่งกรณีเจ้าของข้อมูลเป็นเด็ก (GDPR article 6 (1) (f))

ในทางด้านของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกานั้น กฎหมายเกี่ยวกับการคุ้มครองเด็กในบริบทของการสื่อสารออนไลน์นั้นมีจำนวนหลายฉบับ แต่ในส่วนของกฎหมายที่วางหลักเกี่ยวข้องกับการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวของเด็ก ได้แก่ กฎหมายคุ้มครองความเป็นอยู่ส่วนตัวของเด็กออนไลน์ (Children's Online Privacy Protection Act: COPPA)

โดยหลักสำคัญของกฎหมาย COPPA ซึ่งอยู่ในรูปแบบของกฎหมายลายลักษณ์อักษรที่วางหลักคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว (Right of Privacy) ของเด็ก ได้แก่ กฎหมายคุ้มครองความเป็นอยู่ส่วนตัวของเด็กออนไลน์ (Children's Online Privacy Protection Act: COPPA) โดยสาระสำคัญของกฎหมาย COPPA คือ ให้สิทธิแก่ผู้ปกครองในการควบคุมข้อมูลส่วนบุคคลที่บ่งระบุตัวตนของ เด็กทางอินเทอร์เน็ต (Personally Identifiable Information) โดยกำหนดว่าผู้ให้บริการเว็บไซต์หรือ ผู้ให้บริการออนไลน์อื่น ๆ ที่มีการเก็บข้อมูลส่วนบุคคลของผู้ใช้งานที่เป็นเด็ก จะต้องได้รับความยินยอมจาก ผู้ปกครอง (Parental Consent) ก่อนการเก็บรวบรวม ใช้และเปิดเผยข้อมูลของเด็กซึ่งมีอายุไม่เกิน 13 ปี (16 C.F.R., section 312.5 (a)) กล่าวคือ ผู้ให้บริการเว็บไซต์ที่จะเก็บข้อมูลหรือใช้ข้อมูลของเด็กจะต้อง แจ้งไปยังผู้ปกครองว่าจะทำการดังกล่าว นอกจากนี้ผู้ให้บริการเว็บไซต์จะต้องมีประกาศ (Notice) แจ้งว่า จะมีการเก็บข้อมูลใดของผู้ใช้งานที่เป็นเด็ก วัตถุประสงค์ในการเก็บข้อมูลนั้น ตลอดจนแจ้งให้ทราบว่าข้อมูล ดังกล่าวจะถูกนำไปใช้อย่างไร (15 U.S.C.A., Section 6502 (B)(1)(A)(i)–(ii)) ข้อมูลส่วนบุคคลที่บ่งระบุ ตัวตนของ

เด็กได้นั้น หมายความรวมถึงข้อมูลเช่น ชื่อตัว ชื่อสกุล ที่อยู่ ที่อยู่จดหมายอิเล็กทรอนิกส์ หมายเลขโทรศัพท์ ภาพถ่ายที่มีข้อมูลเชื่อมโยงกับชื่อของเด็กนั้น (15 U.S.C.A., section 312.2)[264]

กฎหมาย COPPA ให้อำนาจคณะกรรมาธิการการค้าสหรัฐ (Federal Trade Commission) หรือ FTC ออกกฎเกณฑ์กำหนดรายละเอียดของหลักกฎหมายตาม COPPA ได้ ทั้งนี้ คณะกรรมาธิการ FTC ออกกฎเกณฑ์กำหนดรายละเอียดต่าง ๆ เช่น หลักการให้ความยินยอมจากผู้ปกครอง ของเด็ก (FTC Children's Online Privacy Protection Rule, 1999) ซึ่งอาจทำได้ด้วยวิธีต่าง ๆ เช่น การส่งโทรสาร (Fax) นอกจากนี้ยังกำหนดให้เว็บไซต์ที่จะเก็บข้อมูลเด็กต้องจัดให้มีหมายเลขโทรศัพท์ไม่ เสียค่าบริการ (toll free) สำหรับผู้ปกครองในการติดต่อให้ความยินยอมในการเก็บข้อมูลดังกล่าว รวมทั้ง การแสดงความยินยอมทางอิเล็กทรอนิกส์ (16 C.F.R., section 312.5(b)(2)) สำหรับการบังคับใช้กฎหมายทาง คณะกรรมาธิการ FTC มีอำนาจดำเนินคดีกับผู้ฝ่าฝืนโดยมีอำนาจกำหนดค่าปรับทางแพ่งได้ (15 U.S.C.A., section 6505 (a))[265] กล่าวได้ว่ากลไกสำคัญในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของเด็กตามหลักการของกฎหมาย COPPA นั้นมีลักษณะเป็นการกำหนดหน้าที่ร่วมกันระหว่างผู้ให้บริการกับผู้ปกครอง กล่าวคือ ผู้ให้บริการเว็บไซต์หรือกิจกรรมออนไลน์อื่น ๆ จะต้องได้รับความยินยอมของผู้ปกครองก่อนจึงจะเก็บข้อมูลส่วนบุคคลของเด็กได้นั่นเอง

สำหรับประเทศไทย พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ก็ได้บัญญัติรับรองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของเด็กหรือผู้เยาว์ไว้เช่นเดียวกัน โดยในชั้นของการร่างกฎหมายนั้นได้นำเอาแนวคิดและหลักการของต่างประเทศที่กล่าวมาข้างต้นใช้เป็นกรอบในการยกร่างกฎหมาย ซึ่งในบทบัญญัติของมาตรา 20 มีการบัญญัติสาระสำคัญไว้ว่า ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ซึ่งยังไม่บรรลุนิติภาวะโดยการสมรสหรือไม่มีฐานะเสมือนดังบุคคลซึ่งบรรลุนิติภาวะแล้ว การขอความยินยอมจากเจ้าของของมูลส่วนบุคคลในการที่จะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้น จะต้องดำเนินการดังต่อไปนี้

1. ในกรณีที่การให้ความยินยอมของผู้เยาว์ไม่ใช่การใด ๆ ซึ่งผู้เยาว์อาจให้ความยินยอมโดยลำพังได้ตามที่บัญญัติไว้ในมาตรา 22 มาตรา 23 หรือมาตรา 24 แห่งประมวลกฎหมายแพ่งและพาณิชย์ ต้องได้รับความยินยอมจากผู้ใช้อานาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ด้วย

---

[264] คณาธิป ทองรวีวงศ์, **รายงานการวิจัยฉบับสมบูรณ์ เรื่องการปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน**, หน้า 258.

[265] *เรื่องเดียวกัน*, หน้า 259.

2. ในกรณีที่ผู้เยาว์มีอายุเกินไม่เกินสิบปี ให้ขอความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์

โดยหลักการขอความยินยอมนี้นำมาใช้บังคับกับการถอนความยินยอมของเจ้าของข้อมูลส่วนบุคคล, การแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ, การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล, การร้องเรียนของเจ้าของข้อมูลส่วนบุคคล และการอื่นใดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ด้วย[266]

จากที่กล่าวมานั้นจะเห็นว่าหลักการของกฎหมายไทยตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มีความสอดคล้องกันกับหลักการของ General Data Protection Regulation ของสหภาพยุโรป และ กฎหมาย COPPA ของประเทศสหรัฐอเมริกา ซึ่งสามารถสรุปสาเหตุของการที่ต้องกำหนดการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของเด็กหรือผู้เยาว์ไว้เป็นกรณีพิเศษในกรณีของการขอความยินยอมเพราะว่าหากไม่ได้มีการกำหนดหลักการไว้เป็นการเฉพาะสำหรับกรณีของเด็กหรือผู้เยาว์นั้นอาจก่อให้เกิดปัญหาบางประการ กล่าวคือ[267]

ประการแรก การคุ้มครองข้อมูลส่วนบุคคลในกรณีของเด็กหรือผู้เยาว์นั้นจำเป็นต้องมีความเข้มงวดมากกว่าผู้ใหญ่ เช่น กฎหมายสหภาพยุโรปแม้มีข้อยกเว้นสำหรับกรณีที่ผู้ควบคุมข้อมูลสามารถประมวลข้อมูลโดยไม่ต้องขอความยินยอมเจ้าของข้อมูล แต่ข้อยกเว้นดังกล่าวก็ยังมีข้อจำกัดกรณีที่เจ้าของข้อมูลเป็นเด็กหรือผู้เยาว์ ทั้งนี้เนื่องจากกฎหมายให้ความสำคัญกับความอ่อนไหวของข้อมูลส่วนบุคคลของเด็กหรือผู้เยาว์เป็นพิเศษ จึงต้องกำหนดให้มีหลักบางประการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของเด็กเพิ่มเติมขึ้นมาจากกรณีของผู้ใหญ่ หรืออาจกล่าวได้ว่าแม้ว่าการคุ้มครองข้อมูลส่วนบุคคลจะอยู่ภายใต้กฎหมายฉบับเดียวกับผู้ใหญ่แต่มีหลักการพิเศษเพิ่มขึ้นมาสำหรับกรณีเด็กหรือผู้เยาว์นั่นเอง

ประการที่สอง หลักการสำคัญของการคุ้มครองข้อมูลส่วนบุคคลบางประการอาจไม่เหมาะสมที่จะนำมาใช้บังคับกับบุคคลทุกคนโดยไม่คำนึงถึงความแตกต่างด้านอายุ เช่น หลักความยินยอม ซึ่งโดยหลักแล้วบุคคล ทั่วไปให้ความยินยอมเกี่ยวกับข้อมูลส่วนบุคคลของตนได้เอง แต่สำหรับกรณีของเด็กหรือผู้เยาว์แล้ว มีประเด็นว่า หลักการดังกล่าวอาจไม่เหมาะสมทำให้ต้องมีการกำหนดหลักการเฉพาะขึ้นมา คือ กฎหมายคุ้มครองข้อมูลส่วนบุคคลวางหลักเกณฑ์เกี่ยวกับรายละเอียดของความยินยอมในกรณีของเด็กที่แตกต่างจากผู้ใหญ่ โดยวางเงื่อนไขว่าเด็กไม่สามารถให้

---

[266] มาตรา 20 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ใช้บังคับกับกรณีเจ้าของข้อมูลส่วนบุคคลเป็นคนไร้ความสามารถหรือคนเสมือนไร้ความสามารถด้วย

[267] คณาธิป ทองรวีวงศ์, **รายงานการวิจัยฉบับสมบูรณ์ เรื่องการปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน**, หน้า 265-266.

ความ ยินยอมได้เอง แต่ต้องขอความยินยอมจากผู้ใหญ่ที่เป็นผู้ปกครอง (Parental Consent) ดังจะเห็นได้จากกฎหมาย COPPA ของสหรัฐอเมริกา ดังนั้น หลักความยินยอมในกรณีของเด็กจึงใช้หลักการเดียวกับผู้ใหญ่ ซึ่งอาจทำให้ไม่เหมาะสมสำหรับกรณีที่เด็กยังไม่สามารถเข้าใจสภาพหรือสาระของความยินยอมและผลกระทบที่จะเกิดขึ้น เช่น การที่เด็กคลิกปุ่มยินยอมตกลงในการเก็บข้อมูลของผู้ให้บริการต่าง ๆ ทางอินเทอร์เน็ตโดยไม่รู้ถึงข้อเท็จจริงและผลกระทบของการเก็บข้อมูลนั้น ในประเด็นนี้หากนำหลักกฎหมายทั่วไป เช่น หลักกฎหมายแพ่งเกี่ยวกับการแสดงเจตนาทำนิติกรรมมาปรับใช้ โดยถือว่าเป็นการแสดงเจตนา ของผู้เยาว์ซึ่งต้องได้รับความยินยอมจากผู้ปกครอง แต่ก็อาจมีปัญหาการตีความว่า การแสดงเจตนายินยอม ให้เก็บข้อมูลจะถือเป็นนิติกรรมหรือไม่ หรือปัญหาการตีความตามกฎหมายแพ่งว่าการให้ความยินยอม เกี่ยวกับการเก็บข้อมูลนั้นเป็นกรณีที่ผู้เยาว์สามารถทำได้เองหรือต้องอยู่ในอำนาจของผู้ใช้อำนาจปกครอง ดังนั้น เพื่อแก้ไขปัญหาการนำกฎหมายทั่วไปมาตีความและปรับใช้ โดยคำนึงถึงสภาพการเก็บข้อมูลทางอิเล็กทรอนิกส์ที่อาจแตกต่างจากการแสดงเจตนาทำนิติกรรม กฎหมายคุ้มครองข้อมูลส่วนบุคคลจึงอาจกำหนดรายละเอียดเกี่ยวกับการให้ความยินยอมในกรณีเด็กไว้โดยเฉพาะ ดังนั้น หากกฎหมายคุ้มครองข้อมูลไม่ได้กำหนดหลักการสำหรับความยินยอมในกรณีของเด็กเป็นการเฉพาะแล้ว ก็จะไม่สามารถกำหนดรายละเอียดเกี่ยวกับการให้ความยินยอมโดยผู้ปกครอง ซึ่งจะต้องนำกฎหมายอื่นที่อยู่บนพื้นฐานหลักการที่แตกต่างกันมาปรับใช้ดังกล่าว

ดังนั้น หากพิจารณาจากสถานการณ์ปัจจุบันในมิติทางเทคโนโลยี หรือสภาพทางปฏิบัติของการใช้งาน โดยเฉพาะอย่างยิ่งการใช้งานบริการออนไลน์ต่าง ๆ ที่เด็กอาจสามารถเข้าถึงและใช้การได้เอง รวมทั้งเพื่อเหตุผลของความยืดหยุ่นและความรวดเร็วในทางปฏิบัติ แต่เพื่อสร้างความสมดุลกับการคุ้มครองข้อมูลของเด็ก การกำหนดหลักการเรื่องความยินยอม ในกรณีของเจ้าของข้อมูลส่วนบุคคลเป็นเด็กหรือผู้เยาวน์นี้จึงควรจำแนกความยินย อมเป็นสองกรณี ได้แก่ กรณีที่เด็กสามารถยินยอมได้เอง และกรณีที่เด็กต้องขอความยินยอมจากผู้ใหญ่

โดยในส่วนของการที่จะกำหนดให้ผู้เยาว์สามารถตัดสินใจยินยอมด้วยตนเอง ก็จะต้องมีการวางเงื่อนไขเพื่อคุ้มครองเด็ก ว่าแม้อาจให้ความยินยอมเกี่ยวกับข้อมูลส่วนบุคคลของตนเองได้ โดยการขอความยินยอมนั้นต้องอยู่ภายใต้เงื่อนไข เช่น ผู้เยาว์มีความเข้าใจในวัตถุประสงค์ ผลกระทบ ของการเก็บประมวลผล และใช้ข้อมูลส่วนบุคคล นอกจากนี้ ยังต้องพิจารณาว่าผู้เยาว์อยู่ภายใต้แรงกดดันหรืออิทธิพลใดหรือไม่ ดังนั้นจะเห็นได้ว่า ในอนาคตหากจะต้องมีการพิจารณาปรับปรุงแก้ไขพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ประเด็นเรื่องนี้จึงจะเป็นประเด็นที่สมควรจะได้พัฒนาหลักการของมาตรา 20 โดยควรกำหนดเพิ่มเติมไปด้วยว่า แม้ผู้เยาว์จะสามารถให้ความยินยอมได้เองในกรณีที่อาจให้ความยินยอมโดยลำพังได้ตามที่บัญญัติไว้ในมาตรา 22 มาตรา 23 หรือมาตรา 24 แห่งประมวลกฎหมายแพ่งและพาณิชย์ แต่ผู้เยาว์จะต้องไม่ได้อยู่ภายใต้

แรงกดดันหรืออิทธิพลใด ๆ และมีความเข้าใจในวัตถุประสงค์ ผลกระทบ ของการเก็บประมวลผลและใช้ข้อมูลส่วนบุคคลของตนด้วย

3) ประเด็นข้อมูลส่วนบุคคลของผู้พิการหรือทุพพลภาพ

ตามหลักการของ GDPR Recital 35 เรื่อง ข้อมูลเกี่ยวกับสุขภาพ (Health Data) อธิบายว่า ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับสุขภาพ ควรหมายรวมถึงข้อมูลทั้งหมดที่เกี่ยวข้องเจ้าของข้อมูลส่วนบุคคล ซึ่งจะเปิดเผยให้ทราบถึงเรื่องที่เกี่ยวข้องกับสุขภาพกายหรือจิตใจ ทั้งในอดีต ปัจจุบันหรืออนาคต ซึ่งรวมถึงข้อมูลของบุคคลธรรมดาที่เก็บรวบรวมในระหว่างการลงทะเบียนหรือการให้บริการด้านสุขภาพตามที่กำหนดใน Directive 2011/24/EU ไม่ว่าจะเป็น หมายเลข สัญลักษณ์ที่ได้รับโดยเฉพาะเพื่อวัตถุประสงค์ด้านสุขภาพ ข้อมูลที่ได้จากการทดสอบหรือตรวจสอบส่วนของร่างกายหรือสารทางร่างกาย รวมถึงข้อมูลทางพันธุกรรมและตัวอย่างข้อมูลทางชีวภาพ และข้อมูลใด ๆ เกี่ยวข้อง เช่น โรค ความพิการ ความเสี่ยงของโรค ประวัติทางการแพทย์ การรักษาทางคลินิก หรือข้อมูลทางสรีรวิทยาหรือชีวการแพทย์ที่เป็นอิสระจากแหล่งที่มา ตัวอย่างเช่น จากแพทย์หรือผู้เชี่ยวชาญด้านสุขภาพอื่น ๆ หรือจากโรงพยาบาล หรือจากการทดสอบ การวินิจฉัยภายนอกด้วยอุปกรณ์ทางการแพทย์[268]

ฉะนั้นจะเห็นว่า ข้อมูลที่เกี่ยวกับความพิการนั้น ถือเป็นข้อมูลที่เป็นข้อมูลด้านสุขภาพและถือเป็นข้อมูลที่มีความอ่อนไหว (Sensitive Data) ที่พึงได้รับการคุ้มครอง โดยเฉพาะอย่างยิ่งในกรณีของ บุคคลซึ่งเป็นผู้พิการหรือทุพพลภาพในฐานะที่เขาเป็นเจ้าของข้อมูลส่วนบุคคล

---

[268] Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

นั้น หากมีการล่วงละเมิดข้อมูลส่วนบุคคลของเขา ย่อมเป็นเรื่องยากที่เขาจะใช้สิทธิเรียกร้องในฐานะผู้เป็นเจ้าของข้อมูลส่วนบุคคล เช่นนี้โดยหลักการสมควรวางระบบการเยียวยาแก่เจ้าของข้อมูลส่วนบุคคลที่มีปัญหาและอุปสรรคในการใช้สิทธิเป็นกรณีพิเศษ

ประเด็นต่อมาคือ หากข้อมูลความพิการ เป็นข้อมูลที่อยู่ในความครอบครองดูแลของหน่วยงานราชการ ตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 จะเห็นว่าไม่ได้มีบทบัญญัติคุ้มครองสิทธิเหนือข้อมูลที่มีความอ่อนไหวไว้แต่อย่างใด และเมื่อพิจารณาถึงพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 จะเห็นว่ามีการกำหนดให้ ข้อมูลความพิการนี้เป็นข้อมูลที่มีความอ่อนไหวเป็นพิเศษ โดยหลักการของมาตรา 26 และมาตรา 27 จึงห้ามทำการเก็บรวมรวม ใช้ หรือเปิดเผยข้อมูลความพิการนี้โดยปราศจากความยินยอม ประเด็นปัญหาในส่วนนี้ที่ตามมาก็คือ ผู้พิการจะแสดงออกซึ่งความยินยอมหรือไม่ยินยอมนั้น หากบุคคลอยู่ในฐานะที่ไม่สามารถแสดงออกซึ่งความยินยอมแล้ว การพิจารณาในเรื่องขอความยินยอมจะดำเนินการอย่างไร

นอกจากนี้ ประเด็นปัญหาที่สำคัญของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ในเรื่องนี้ก็คือ ในส่วนของข้อมูลส่วนบุคคลที่มีความอ่อนไหวนั้น ตามหลักของมาตรา 26 และ 27 ก็ได้กำหนดข้อยกเว้นไว้หลายประการว่า การเก็บข้อมูล ใช้และเปิดเผยข้อมูลที่มีความอ่อนไหวในกิจการต่อไปนี้ ไม่ต้องขอความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล ในกรณีต่าง ๆ เหล่านี้

1. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลไม่สามารถให้ความยินยอมได้

2. การดำเนินกิจการขององค์กรไม่แสวงหาผลกำไร เช่น มูลนิธิ สมาคม ที่ทำงานด้านการเมือง ศาสนา ปรัชญา สหภาพแรงงาน ให้แก่สมาชิกหรือผู้ที่ติดต่ออย่างสม่ำเสมอ และองค์กรนั้น ๆ ไม่ได้เปิดเผยข้อมูลออกไปภายนอก

3. ข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูล

4. เป็นการจำเป็นเพื่อก่อตั้งสิทธิเรียกร้อง หรือการดำเนินคดี การต่อสู้คดีตามกฎหมาย

5. เป็นการจำเป็นในการปฏิบัติตามกฎหมาย เพื่อประเมินความสามารถของลูกจ้างในการทำงาน การวินิจฉัยโรคทางการแพทย์ การให้บริการสุขภาพ การรักษาทางการแพทย์ การป้องกันโรคติดต่อ การคุ้มครองแรงงาน สวัสดิการรักษาพยาบาล การวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ สถิติ ฯลฯ และเพื่อประโยชน์สาธารณะที่สำคัญ โดยต้องจัดให้มีมาตรการคุ้มครองข้อมูลที่เหมาะสมด้วย

จากหลักการข้างต้น สำหรับกิจการ “เพื่อประโยชน์สาธารณะที่สำคัญ” ให้สามารถเก็บข้อมูลและใช้ข้อมูลได้โดยไม่ต้องได้รับความยินยอมอย่างชัดแจ้ง ก็เท่ากับเปิดช่องให้กิจการของหน่วยงานรัฐทั้งหลายหยิบขึ้นมาอ้างได้ว่าภารกิจของหน่วยงานของตนนั้นสำคัญ จนข้อมูลที่มีความอ่อนไหวอาจแทบไม่เหลือพื้นที่ที่จะถูกคุ้มครอง โดยอาจมีผลคุ้มครองได้เพียงจากภาคธุรกิจบางประเภทเท่านั้น และนอกจากนี้ คำว่า “มาตรการที่คุ้มครองข้อมูลที่เหมาะสม” จะพิจารณาอย่างไรจึงจะถือว่ามีความเหมาะสม กรณีเช่นนี้ก็ยังขึ้นอยู่กับหลักเกณฑ์ในรายละเอียดที่จะประกาศออกมา และการตีความที่จะเกิดขึ้นต่อไปในอนาคต ดังนั้น คณะกรรมการข้อมูลส่วนบุคคลซึ่งหน่วยงานที่เกี่ยวข้องกับการตีความบังคับใช้กฎหมายนี้จึงมีความสำคัญต่อความปลอดภัยของข้อมูลของประชาชนอย่างมาก สมควรที่จะได้กำหนดหลักเกณฑ์ในเรื่องนี้ออกมาให้ชัดเจนต่อไป

อย่างไรก็ดีประเด็นปัญหาที่สำคัญที่สุดเกี่ยวกับการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวก้บข้อมูลส่วนบุคคลของผู้พิการหรือทุพพลภาพนั้น อยู่ที่เรื่องของการเข้าถึงสิทธิในฐานะเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ โดยสภาพของร่างกายหรือจิตใจของบุคคลประเภทนี้ทำให้เป็นการยากมากที่จะสามารถเข้าถึงสิทธิได้อย่างเต็มที่ แม้ว่าระบบกฎหมายจะมีการพัฒนาจนสามารถให้ความคุ้มครองสิทธิและวางระบบการเยียวยาสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลดีเพียงใดก็ตาม แต่หากว่าเจ้าของข้อมูล (Data Subject) มีปัญหาเรื่องความสามารถในการเข้าถึงสิทธิระบบและกลไกการเยียวยาก็ไม่สามารถที่จะเกิดประสิทธิภาพและประสิทธิผลได้ กรณีเช่นนี้ จึงสมควรที่จะได้มีการกำหนดมาตรการต่าง ๆ โดยเฉพาะอย่างยิ่งในระบบของการเยียวยา ควรจะส่งเสริมให้บุคคลผู้ด้อยโอกาสที่เป็นผู้พิการหรือทุพพลภาพ สามารถเข้าถึงสิทธิเช่นนี้ได้อย่างแท้จริง

4) ประเด็นข้อมูลส่วนบุคคลของผู้ต้องขัง

สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของผู้กระทำความผิดในทางอาญานั้น ตราบใดที่ศาลยังไม่ได้มีคำพิพากษาถึงที่สุดให้เป็นผู้กระทำความผิด บุคคลนั้นก็ยังถือว่าเป็นผู้บริสุทธิ์อยู่ตามกฎหมาย กรณีบุคคลนั้นย่อมจะมีสิทธิโดยสมบูรณ์อยู่ตามกฎหมายเช่นเดียวกับบุคคลทั่วไป ในส่วนนี้ข้อมูลส่วนบุคคลของเขาที่เป็นประวัติในการถูกดำเนินคดีอาญา ไม่ว่าในชั้นพนักงานสอบสวน พนักงานอัยการ และชั้นศาล ย่อมถือว่าเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) และจะได้รับความคุ้มครองตามหลักการของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ตามหลักการของมาตรา 26 และมาตรา 27 กล่าวคือ ห้ามการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลที่เป็นประวัติอาชญากรรมโดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลผู้นั้น

แต่อย่างไรก็ดี ถ้าผู้กระทำความผิดในทางอาญา ถูกคำพิพากษาถึงที่สุดให้เป็นผู้กระทำผิด โดยเฉพาะในกรณีที่ต้องคำพิพากษาถึงที่สุดให้ลงโทษจำคุก ฐานะของบุคคลนั้นจะกลายเป็นผู้ต้องขัง และอยู่ภายใต้กฎหมายอีกฉบับก็คือ พระราชบัญญัติราชทัณฑ์ พ.ศ.2560 ที่ตรา

ขึ้นมาใหม่โดยพยายามยกระดับของระบบการบังคับโทษเพื่อให้เป็นการแก้ไข บำบัด ฟื้นฟู และพัฒนาพฤตินิสัยของผู้ต้องขัง และขณะเดียวกันก็วางหลักการปฏิบัติให้สอดคล้องตามมาตรฐานสากลต่าง ๆ อาทิ ข้อกำหนดมาตรฐานขั้นต่ำสำหรับปฏิบัติต่อผู้ต้องขัง (Standard Minimum Rules for the Treatment of Prisoners / SMR) หรือ ข้อกำหนดกรุงเทพ (Bangkok Rules)

แต่ทว่าในประเด็นเรื่องการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนั้นในพระราชบัญญัติราชทัณฑ์ฉบับใหม่ก็ไม่ได้มีการกำหนดห้ามเจ้าหน้าที่ราชทัณฑ์ หรือเรือนจำที่เป็นหน่วยงานในสังกัด ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ต้องขังแต่อย่างใด ประเด็นข้อน่ากังวลจึงอยู่ที่ว่า แม้พระราชบัญญัติราชทัณฑ์ พ.ศ.2560 จะมุ่งเน้นการปฏิบัติต่อผู้ต้องขังไปในทิศทางที่จะแก้ไข บำบัด ฟื้นฟู และพัฒนาพฤตินิสัย อันจะทำให้มีการส่งเสริมในการฝึกอบรมต่าง ๆ แก่ผู้ต้องขังทั้งในและนอกเรือนจำ ซึ่งอาจจะมีการออกประกาศนียบัตรเพื่อรับรองคุณวุฒิทางวิชาการหรือวิชาชีพให้ กรณีเช่นนี้หากในใบรับรองคุณวุฒิได้มีการเขียนข้อความไว้ในทำนองว่าเป็นการฝึกอบรมในฐานะผู้ต้องขัง หรือฝึกอบรมในเรือนจำแล้ว ย่อมเป็นการเปิดเผยข้อมูลส่วนบุคคลของผู้ต้องขังทันที และกรณีนี้ สิทธิของผู้ต้องขังอันเป็นสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลย่อมไม่ได้รับความคุ้มครอง ทั้งจาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่ไม่ใช้บังคับกับการดำเนินงานตามกระบวนการยุติธรรมทางอาญา[269] อีกทั้งยังไม่ได้รับความคุ้มครองจากพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 ที่ไม่ได้บัญญัติรับรองสิทธิไปถึงกรณีนี้

ในประเด็นนี้จึงสมควรที่จะได้มีการกำหนดมาตรการเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของผู้กระทำความผิดในทางอาญาที่อยู่ในฐานะผู้ต้องขังต่อไป

5) ประเด็นข้อมูลส่วนบุคคลและเสรีภาพของสื่อมวลชน

วัตถุประสงค์พื้นฐานของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ถูกตราขึ้นมาให้สอดคล้องกับรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 มาตรา 32 รับรองสิทธิในความเป็นส่วนตัวของบุคคล โดยกฎหมายฉบับนี้มีเป้าหมายเพื่อยังให้เกิดการรับรองสิทธิและให้ความคุ้มครองข้อมูลส่วนบุคคล ที่อาจถูกเก็บรวมรวม ประมวลผล เปิดเผยหรือเผยแพร่ถึงบุคคล

---

[269] มาตรา 4 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 พระราชบัญญัตินี้ไม่ใช้บังคับแก่

(5) การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

จำนวนมากได้ในระยะเวลาอันรวดเร็วโดยอาศัยความก้าวหน้าทางเทคโนโลยีในปัจจุบัน จนอาจก่อให้เกิดการนำข้อมูลนั้นไปใช้ในทางมิชอบ อันเป็นการละเมิดต่อเจ้าของข้อมูล ทั้งนี้ โดยคำนึงถึงการรักษาดุลยภาพระหว่างสิทธิขั้นพื้นฐานในความเป็นส่วนตัวในมิติของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล, เสรีภาพในการติดต่อสื่อสารและเสรีภาพในการแสดงความคิดเห็น รวมไปถึงเรื่องของความมั่นคงของรัฐ อันเป็นมิติของประโยชน์สาธารณะ

จากหลักการในข้างต้น จึงเกิดประเด็นตามมาว่า เมื่อมีการรับรองและคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลแล้ว การรับรองสิทธินี้จะไปขัดหรือแย้งกับการทำหน้าที่นำเสนอข้อมูลข่าวสารต่อสาธารณะอันเป็นหน้าที่ของบรรดาสื่อมวลชนภายใต้หลักเสรีภาพของสื่อมวลชน หรือไม่

กรณีนี้เห็นว่า การคุ้มครองข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล และ เสรีภาพของสื่อมวลชนนั้น รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 มาตรา 35 บัญญัติรับรองไว้ว่า “บุคคลซึ่งประกอบวิชาชีพสื่อมวลชนย่อมมีเสรีภาพในการเสนอข่าวสาร หรือการแสดงความคิดเห็นตามจริยธรรมแห่งวิชาชีพ” ทั้งสองส่วนนี้ เป็นคุณค่า (Value) ที่รัฐธรรมนูญให้การรับรอง และไม่ได้มีความขัดแย้งกันในหลักการ กล่าวคือ เมื่อพิจารณาตามบทบัญญัติของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กำหนดข้อยกเว้นการบังคับใช้สำหรับกิจการสื่อมวลชน ในมาตรา 4 (3) ที่ว่า บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมไว้เฉพาะเพื่อกิจการสื่อมวลชนอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะ ซึ่งหลักการข้อนี้จะเห็นว่า หลักการคุ้มครองข้อมูลส่วนบุคคลจะไม่ได้เป็นไปในลักษณะขัดขวางการทำงานของสื่อมวลชนที่อยู่บนฐานของการปฏิบัติหน้าที่ของตนอย่างมีจริยธรรม แต่อย่างไรก็ดี ผู้ควบคุมข้อมูลส่วนบุคคลของฝ่ายสื่อมวลชน จะต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานด้วย

แต่อย่างไรก็ตาม จากข้อยกเว้นข้างต้น ก็อาจก็ให้เกิดประเด็นคำถามต่อมาประการแรกคือ ลักษณะ รูปแบบ และประเภทของกิจการอะไรบ้าง ที่ถือเป็นกิจการสื่อมวลชน

และคำถามในประการที่สองคือ สื่อมวลชนที่ได้รับยกเว้นเฉพาะเพื่อกิจการสื่อมวลชนอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น ซึ่งจากข้อความของมาตรา 4 (3) นี้ ย่อมนำมาซึ่งคำถามสำคัญว่าอะไรคือ “จริยธรรมแห่งการประกอบวิชาชีพ” หรือ “ประโยชน์สาธารณะ” เพราะหากไม่ต้องด้วยข้อยกเว้น สื่อมวลชนก็ต้องดำเนินการตามเงื่อนไขของกฎหมายในการกระทำต่อข้อมูลส่วนบุคคล อาทิ การเปิดเผยชื่อและรูปหรือภาพถ่ายของผู้ถูกกล่าวหาว่ากระทำความผิดต่อสาธารณะโดยไม่ได้รับความยินยอมจะกระทำได้หรือไม่ ถ้าทำได้ใช้กฎหมายใดเป็นข้อยกเว้น นอกจากนี้สื่อมวลชนยังมีหน้าที่ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานด้วย ซึ่งมาตรฐานดังกล่าวคืออะไร และมีเนื้อหา

อย่างไรซึ่งประเด็นปัญหาทั้งสองกรณีนี้ยังไม่มีความชัดเจน จึงจำเป็นที่องค์กรซึ่งมีอำนาจนั่นก็คือคณะกรรมการข้อมูลส่วนบุคคลจะต้องออกประกาศหรือระเบียบมาเพื่ออธิบายให้ชัดเจนต่อไปในอนาคต

5.1.3 วิเคราะห์การกำหนดสิทธิของเจ้าของข้อมูล (Data Subject)

5.1.3.1 สิทธิของเจ้าของข้อมูลโดยทั่วไป

หลักการสำคัญของกฎหมายคุ้มครองข้อมูลส่วนบุคคลก็คือการรับรองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในประการต่าง ๆ ของเจ้าของข้อมูลส่วนบุคคล (Right) ไว้ในกฎหมาย ซึ่งเมื่อพิจารณาจากกฎหมายระหว่างประเทศและกฎหมายต่างประเทศจะเห็นว่าหลักกฎหมายที่มีการรับรองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลไว้อย่างชัดเจนที่สุดก็คือ General Data Protection Reguration ของสหภาพยุโรปนั่นเอง ในส่วนนี้จึงจะได้นำหลักการของ General Data Protection Reguration ในเรื่องสิทธิของเจ้าของข้อมูลส่วนบุคคลมาพิจารณาเปรียบเทียบกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย ซึ่งสามารถสรุปดังตารางข้างล่างนี้

ตารางที่ 5.3 เปรียบเทียบสิทธิของเจ้าของข้อมูลส่วนบุคคลระหว่าง GDPR และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

สิทธิของเจ้าของข้อมูลส่วนบุคคล (Rights of Data Subject)	**GDPR**	**พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562**
The Right to be Informed	เจ้าของข้อมูลมีสิทธิที่จะได้รับแจ้งเกี่ยวกับ “ข้อมูลเกี่ยวกับความเป็นส่วนตัว” (Privacy Information) (Article 13 และ Article 14) ซึ่งสำหรับกรณีตาม Article 13 จะเป็นข้อมูลที่ต้องแจ้งให้ทราบในกรณีที่เก็บรวบรวมข้อมูลส่วนบุคคลจากตัวเจ้าของข้อมูลเอง	มาตรา 23

ตารางที่ 5.3 (ต่อ)

สิทธิของเจ้าของข้อมูลส่วนบุคคล (Rights of Data Subject)	GDPR	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562
	และสำหรับกรณีตาม Article 14 จะเป็นการแจ้งข้อมูลให้ทราบสำหรับกรณีที่ได้รับข้อมูลจากแหล่งอื่นนอกจากเจ้าของข้อมูลส่วนบุคคล ซึ่งตัวอย่างของข้อมูลต่าง ๆ ที่ต้องแจ้งให้ทราบ ก็เช่น ตัวตนของผู้ควบคุมข้อมูลส่วนบุคคลและรายละเอียดสำหรับการติดต่อ วัตถุประสงค์ของการประมวลผลข้อมูล ตลอดจนฐานทางกฎหมายในการประมวลผลข้อมูล หรือผู้รับหรือประเภทผู้ที่จะได้รับข้อมูลดังกล่าวในกรณีที่จะมีการ เปิดเผยข้อมูลนั้นต่อไป เป็นต้น	
The Right of Access	เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะได้รับการยืนยันจากผู้ควบคุมข้อมูลส่วนบุคคลว่ามีการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวกับตนหรือไม่ และถ้าหากมีการประมวลผลดังกล่าว ผู้นั้นก็จะมีสิทธิในการเข้าถึงข้อมูลต่าง ๆ เช่น วัตถุประสงค์ของการประมวลผล ประเภทของข้อมูลส่วนบุคคลที่เกี่ยวข้อง ผู้รับหรือประเภทของผู้จะรับข้อมูลส่วนบุคคลนั้นในกรณีที่มี	มาตรา 30

ตารางที่ 5.3 (ต่อ)

สิทธิของเจ้าของข้อมูลส่วนบุคคล (Rights of Data Subject)	GDPR	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562
	การเปิดเผยหรือได้รับแจ้งสิทธิในการร้องเรียนต่อหน่วยงานที่ทำหน้าที่กำกับดูแล (Supervisory Authority) เป็นต้น (Article 16)	
The Right to Rectification	เจ้าของข้อมูลมีสิทธิเรียกร้องให้ แก้ไขข้อมูลที่ไม่ถูกต้อง (Article 5 (1) (d) และ Article 16)	มาตรา 36
The Right to be Forgotten/ The Right to Erasure	เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการลบข้อมูลส่วนบุคคลเกี่ยวกับตนโดยไม่ชักช้า และผู้ควบคุมข้อมูลส่วนบุคคลจะต้องลบข้อมูลดังกล่าวหากเป็นไปตามเงื่อนไข เช่น ข้อมูลส่วนบุคคลนั้นไม่มีความจำเป็นอันเกี่ยวเนื่องกับวัตถุประสงค์ที่ได้มีการเก็บรวบรวมหรือประมวลผลอีกต่อไป เจ้าของข้อมูลส่วนบุคคลได้เพิกถอนความยินยอม (ในกรณีที่การประมวลผลมีฐานจากความยินยอม) หรือข้อมูลส่วนบุคคลนั้นถูกประมวลผลโดยไม่ชอบด้วยกฎหมาย เป็นต้น (Article 17)	มาตรา 33
The Right to Restrict Processing	เจ้าของข้อมูลมีสิทธิจำกัดการประมวลข้อมูล หากโต้แย้งว่าข้อมูลนั้นไม่ถูกต้อง/การประมวล	มาตรา 34

ตารางที่ 5.3 (ต่อ)

สิทธิของเจ้าของข้อมูลส่วนบุคคล (Rights of Data Subject)	GDPR	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562
	ข้อมูลนั้นไม่ชอบด้วยกฎหมาย หรือผู้ควบคุมข้อมูลไม่มีความจำเป็นเกี่ยวกับข้อมูลนั้นแต่ยังคงเก็บข้อมูลไว้เพื่อดำเนินการตามกฎหมาย (Article 18)	
The Right to Data Portability	เจ้าของข้อมูลมี สิทธิได้รับสำเนา ข้อมูลในรูปแบบ ที่อ่านได้โดยทั่วไปและ โอนข้อมูลส่วน บุคคลจากผู้ควบคุมข้อมูล หนึ่งไปยังผู้ควบคุมข้อมูลอื่น (Article 20)	มาตรา 31
The Right to Object	เจ้าของข้อมูลมี สิทธิคัดค้านใน กรณีที่การ ประมวลข้อมูล นั้นสืบเนื่องจาก ผลประโยชน์สาธารณะหรือ ประโยชน์อื่นของ ผู้ควบคุมข้อมูล เว้นแต่ผู้ควบคุม ข้อมูลแสดงได้ว่า ประโยชน์ตาม กฎหมายในการ ประมวลข้อมูล นั้นมีมากกว่าสิทธิ เสรีภาพของ เจ้าของข้อมูลหรือ มีความ จำเป็นเพื่อการ ใช้สิทธิหรือ ดำเนินคดีตาม กฎหมาย (Article 21)	มาตรา 32
Rights in Relation to Automated Decision Making and Profiling.	เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะคัดค้านการตัดสินใจโดยอิงจากการประมวลผลโดยอัตโนมัติ รวมถึงการนำข้อมูลมาใช้ในการ	ไม่มี

ตารางที่ 5.3 (ต่อ)

สิทธิของเจ้าของข้อมูลส่วนบุคคล (Rights of Data Subject)	GDPR	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562
	วิเคราะห์พฤติกรรมบุคคล (Profiling) ซึ่งมีผลทางกฎหมายหรือส่งผลกระทบอย่างยิ่งยวดต่อเจ้าของข้อมูล ยกเว้นในบางกรณี เช่น การตัดสินใจนั้นจำเป็นต่อการปฏิบัติตามข้อสัญญา การตัดสินใจนั้นได้รับอนุญาตจากกฎหมายของสหภาพยุโรปหรือรัฐสมาชิก หรือได้รับความยินยอมที่ชัดเจนจากเจ้าของข้อมูล (Article 22)	

จากที่กล่าวมาจะเห็นว่า General Data Protection Reguration มุ่งเน้นให้ความสำคัญกับสิทธิของเจ้าของข้อมูล แม้ว่ากฎหมายจะกำหนดว่าผู้ควบคุมข้อมูลอาจเก็บข้อมูลหรือประมวลข้อมูลได้ด้วยเหตุ ต่าง ๆ ที่ไม่ต้องอาศัยความยินยอมของเจ้าของข้อมูล เช่น ในกรณีที่การประมวลข้อมูลนั้นสืบเนื่องจากผลประโยชน์สาธารณะ หรือประโยชน์อื่นของผู้ควบคุมข้อมูลกฎหมายก็ยังให้สิทธิเจ้าของข้อมูลคัดค้านการประมวลข้อมูลที่อาศัยเหตุดังกล่าวได้ หรือในกรณีการประมวลข้อมูลส่วนบุคคลสืบเนื่องจากเหตุผลเกี่ยวกับ สถิติ วิทยาศาสตร์ ประวัติศาสตร์ ซึ่งเป็นข้อยกเว้นที่อาจประมวลข้อมูลได้โดยไม่ต้องขอความยินยอม แต่กฎหมายก็ยังให้สิทธิเจ้าของข้อมูลคัดค้านการประมวลข้อมูลด้วยเหตุเหล่านั้นเช่นกัน นอกจากนี้ยังมีการให้สิทธิเจ้าของข้อมูลคัดค้านการประมวลข้อมูลโดยเฉพาะกรณีการประมวลข้อมูลที่อาศัยข้อยกเว้นของกฎหมายโดยไม่ต้องขอความยินยอม เช่น การที่ผู้ควบคุมข้อมูลอาศัยเหตุเกี่ยวกับการประมวลข้อมูลที่เกี่ยวกับประโยชน์ตามกฎหมายของผู้ควบคุมข้อมูล หรืออาศัยเหตุเกี่ยวกับการประมวลข้อมูลเพื่อเหตุด้านประวัติศาสตร์ วิทยาศาสตร์

สถิติ[270] สำหรับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ก็ได้มีการกำหนดให้สิทธิคัดค้านการประมวลข้อมูลภายใต้หลักการเช่นเดียวกันกับ General Data Protection Reguration ของสหภาพยุโรป

อย่างไรก็ตามประเทศไทยนั้น ในระดับรัฐธรรมนูญได้มีการรับรองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลไว้สอดคล้องกับรัฐธรรมนูญของต่างประเทศรวมไปถึงหลักการระหว่างประเทศข้างต้น โดยในมาตรา 32 ได้บัญญัติรับรองไว้อันมีสาระโดยสรุปคือ

ประการแรก สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล เป็นสิทธิในความเป็นส่วนตัวประการหนึ่งที่พึงได้รับความคุ้มครองในฐานะที่เป็นสิทธิเสรีภาพขั้นพื้นฐานตามรัฐธรรมนูญแห่งราชอาณาจักรไทย

ประการที่สอง การกระทำอันมีลักษณะเป็นการละเมิด การนำข้อมูลส่วนบุคคลไปใช้หรือดำเนินเนินการที่กระทบกระเทือนสาระสำคัญแห่งสิทธิประเภทนี้ในทางใด ๆ จะกระทำไม่ได้ เว้นแต่มีอำนาจตามกฎหมาย

ประการที่สาม การจะนำข้อมูลส่วนบุคคลของเจ้าของข้อมูลไปใช้ประโยชน์ในทางใด ๆ จะกระทำได้ต่อเมื่อได้อาศัยอำนาจตามกฎหมายที่ตราขึ้นเพียงจำเป็นและเพื่อประโยชน์สาธารณะเท่านั้น

โดยเมื่อเปรียบเทียบกับหลักการระหว่างรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550 จะเห็นว่ามีความแตกต่างกัน กล่าวคือ ในรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550 มาตรา 35 บัญญัติว่า “บุคคลย่อมมีสิทธิที่จะได้รับความคุ้มครองจากการแสวงหาประโยชน์โดยมิชอบจากข้อมูลส่วนบุคคลเกี่ยวกับตน ทั้งนี้ตามที่กฎหมายบัญญัติ” แต่รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ไม่ได้มีบทบัญญัติในส่วนนี้ ดังนั้นจะเห็นความแตกต่างในลักษณะของการบัญญัติ กล่าวคือ รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550 เป็นลักษณะการบัญญัติที่มุ่งคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล โดยให้เป็นไปตามหลักเกณฑ์และวิธีการที่กฎหมายบัญญัติไว้ ในขณะที่รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 เป็นการบัญญัติในลักษณะของหลักการคุ้มครองข้อมูลส่วนบุคคลที่จะได้รับการคุ้มครองไม่ให้นำไปใช้ประโยชน์ โดยมีการกำหนดข้อยกเว้นที่อาจกระทำได้ หากเป็นการใช้อำนาจตามกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นและเพื่อประโยชน์สาธารณะ

เมื่อพิจารณาถึงสิทธิของเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลแล้ว จะเห็นว่ามีการกำหนดหลักการให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคล โดยมีการกำหนด

---

[270] คณาธิป ทองรวีวงศ์, **รายงานการวิจัยฉบับสมบูรณ์ เรื่องการปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน**, หน้า 136.

สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลไว้ให้เป็นสิทธิเชิงลบ (Negative Rights) กล่าวคือ เป็นสิทธิในความเป็นส่วนตัวที่กำหนดห้ามผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล หากเจ้าของข้อมูลส่วนบุคคล ไม่ยินยอมไว้ก่อนหรือในขณะนั้น (เว้นแต่กฎหมายบัญญัติให้กระทำได้)

นอกจากนี้ ยังได้กำหนดให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงข้อมูล, สิทธิขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตน, สิทธิขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลที่ตนไม่ได้ให้ความยินยอม, สิทธิโต้แย้งคัดค้าน หรือสิทธิระงับใช้ข้อมูล รวมถึงมีสิทธิถอนความยินยอม สิทธิ ขอให้ลบ หรือสิทธิทำลายข้อมูลได้ หากถูกนำไปใช้ในทางมิชอบด้วยกฎหมาย และเจ้าของข้อมูลส่วนบุคคลยังมีสิทธิได้รับการดูแลความปลอดภัยของข้อมูล กล่าวคือ ผู้เก็บรวบรวมข้อมูลต้องรักษาความมั่นคงปลอดภัยของข้อมูล ไม่ให้มีการเปลี่ยนแปลงแก้ไขหรือมีผู้ใดเข้าถึงข้อมูลได้โดยมิชอบ

และเพื่อให้การคุ้มครองสิทธิสิทธิเกิดขึ้นได้ในความเป็นจริง กฎหมายจึงได้จัดตั้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เพื่อกำหนดมาตรฐานการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และทำหน้าที่เป็นองค์กรหลักในการคุ้มครองสิทธินี้

แต่อย่างไรก็ดี ประเทศไทยยังไม่ได้มีการบัญญัติรับรองสิทธิในการคัดค้านการตัดสินใจแทนโดยอัตโนมัติ (Right on Automated Individual Decision-Making, Including Profiling) ที่วางหลักให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะคัดค้านการตัดสินใจโดยอิงจากการประมวลผลโดยอัตโนมัติรวมถึงการนำข้อมูลมาใช้ในการวิเคราะห์พฤติกรรมบุคคล (Profiling) ซึ่งมีผลทางกฎหมายหรือส่งผลกระทบอย่างยิ่งยวดต่อเจ้าของข้อมูล ยกเว้นในบางกรณี เช่น การตัดสินใจนั้นจำเป็นต่อการปฏิบัติตามข้อสัญญาการตัดสินใจนั้นได้รับอนุญาตตามกฎหมาย หรือได้รับความยินยอมที่ชัดเจนจากเจ้าของข้อมูล ซึ่งประเด็นนี้คงเป็นประเด็นที่นำไปสู่การพิจารณาเพิ่มเติมและปรับปรุงหลักการในเรื่องสิทธิของเจ้าของข้อมูลให้มีความสอดคล้องและทัดเทียมกับ General Data Protection Reguration ต่อไป

สำหรับการบัญญัติรับรองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล มีลักษณะของการบัญญัติให้เป็นกฎหมายกลางอันเป็นการกำหนดสิทธิเสรีภาพขั้นพื้นฐานที่สอดคล้องกับบทบัญญัติแห่งรัฐธรรมนูญ แต่ในขณะเดียวกันประเทศไทยก็ได้มีการบัญญัติรับรองสิทธิของเจ้าของข้อมูลส่วนบุคคลไว้เป็นการเฉพาะเรื่องตามประเภทของข้อมูลส่วนบุคคล โดยจะมีการกำหนดมาตรการเฉพาะในการคุ้มครองสิทธิแตกต่างกันไปตามประเภทของข้อมูลของกฎหมายแต่ละฉบับ ซึ่งในส่วนนี้จะได้อธิบายในหัวข้อ 5.2 ต่อไป

5.1.3.2 สิทธิที่จะถูกลืม (Rights to be Forgotten)

สำหรับสิทธิที่จะถูกลืม (Rights to be Forgotten) เป็นหลักการที่มีมาตั้งแต่สหภาพยุโรปได้ประกาศใช้ The European Data Protection Directive (95/46/EC) หรือ EU

Directive (95/46/EC) ตั้งแต่วันที่ 13 ธันวาคม ค.ศ.1998 โดยบัญญัติไว้ในมาตรา 12(2) มีสาระสำคัญว่า เจ้าของข้อมูลมีสิทธิที่จะขอให้ผู้ควบคุมข้อมูลทำการลบข้อมูลของตนเองได้ ถ้าข้อมูลนั้นถูกประมวลผลโดยวิธีการที่ไม่เป็นไปตามหลักเกณฑ์ที่ Data Protection Officer (OPD) กำหนดไว้ โดยเฉพาะกรณีที่ข้อมูลมีความไม่สมบูรณ์และไม่ถูกต้อง

อย่างไรก็ดี แนวคิดเรื่องของสิทธิที่จะถูกลืม ไม่ได้รับความเห็นชอบจากทางประเทศสหรัฐอเมริกา โดยเจ้าหน้าที่ในกระบวนการยุติธรรมอ้างว่าสิทธิดังกล่าวทำให้เกิดความยากลำบากในการจัดการกับอาชญากรรมและการปกป้องความปลอดภัยของสังคม โดยมีข้อสังเกตว่า ความเห็นดังกล่าวน่าจะมีเหตุผลอยู่เบื้องหลังก็คือ เพื่อปกป้องผลประโยชน์ของผู้ประกอบการให้บริการออนไลน์รายใหญ่ซึ่งส่วนใหญ่เป็นนิติบุคคลสัญชาติอเมริกัน เช่น Facebook และ Google นอกจากนี้บริษัทต่าง ๆ ก็แสดงความเห็นว่าสิทธิที่จะถูกลืมนี้กระทบต่อเสรีภาพในการแสดงความคิดเห็นบนโลกออนไลน์ รวมไปถึงผู้ประกอบวิชาชีพกฎหมาย เช่นทนายความที่มีความเชี่ยวชาญด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคลก็ให้ความเห็นว่าสิทธิดังกล่าวนี้จะทำให้เกิดความยุ่งยากต่อผู้ให้บริการ ที่จะต้องดำเนินการตามคำร้องขอมากมายจากเจ้าของข้อมูล ในการที่จะลบข้อมูลที่เจ้าของได้นำเข้าสู่ระบบออนไลน์และจะต้องแจ้งแก่บุคคลที่สามที่ได้นำข้อมูลนั้นไปประมวลผลทราบถึงการเรียกร้องของเจ้าของข้อมูลอีกด้วย[271]

ในส่วนของแวดวงวิชาการหรือวงการอื่น ๆ ที่เกี่ยวข้อง แม้กระทั้งคณะกรรมาธิการยุโรปเอง ประเด็นเรื่องสิทธิที่จะถูกลืมก็เป็นประเด็นข้อข้อถกเถียงกันมาโดยตลอด จนกระทั่งในที่สุดคณะกรรมธิการยุโรปได้เสนอสิทธิหลักของเจ้าของข้อมูล 3 ประการ กล่าวคือ[272]

ประการแรก ประชาชนมีสิทธิที่จะได้รับการแจ้งถึงกระบวนการประเมินการประมวลผลข้อมูลของตนเป็นภาษาที่ง่าย ชัดเจน ผู้ใช้อินเทอร์เน็ตจะต้องได้รับการแจ้งว่าข้อมูลใดที่จะถูกรวบรวมเพื่อวัตถุประสงค์ใดและจะถูกเก็บเป็นเวลานานเท่าใด พวกเขาจำเป็นจะต้องทราบว่าข้อมูลอาจถูกใช้โดยฝ่ายที่สามอย่างไร พวกเขาต้องทราบสิทธิของตนและองค์กรใดสามารถร้องเรียนได้บ้างหากเกิดการเมิดขึ้น

ประการที่สอง เมื่อใดก็ตามที่ผู้ใช้จะดำเนินการประมวลผลข้อมูล นั่นหมายความว่าจะต้องได้รับความยินยอมอย่างชัดแจ้งและเฉพาะเจาะจง

---

[271] อัญธิกา ณ พิบูลย์, “ปัญหาการบังคับใช้สิทธิที่จะลบข้อมูลส่วนบุคคลในโลกออนไลน์: ศึกษากรณีกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป,” **วารสารนิติพัฒน์นิด้า** 7, 2 (กรกฎาคม-ธันวาคม 2561): 44-45.

[272] ฉัตรชัย เอมราช, “สิทธิที่จะถูกลืม,” **วารสารนิติศาสตร์** 45, 2 (มิถุนายน 2559): 419-420.

ประการที่สาม การปฏิรูปจะทำให้การควบคุมข้อมูลส่วนบุคคลมีประสิทธิภาพมากขึ้น รวมถึงการเข้าถึงข้อมูลส่วนบุคคลของเจ้าของข้อมูลจะง่ายกว่าเดิมตามหลักการของกฎเกณฑ์ใหม่ โดยบุคคลจะต้องสามารถนำข้อมูลส่วนบุคคลของตนไปมอบให้แก่ผู้จัดเก็บอื่นได้โดยง่าย หรือจัดให้มีการลบข้อมูลเมื่อพวกเขาไม่ต้องการให้ข้อมูลดังกล่าวถูกใช้อีกต่อไป

จากหลักที่กล่าวมาจะเห็นว่ากรรมาธิการยุโรป เห็นว่าหนทางสำคัญประการหนึ่งที่จะทำให้บุคคลสามารถควบคุมข้อมูลของตนเองได้ คือการกำหนดสิทธิที่จะถูกลืม ซึ่งบุคคลไม่ควรมีแต่เพียงสิทธิที่จะให้ความยินยอมในกระบวนการประมวลผลเท่านั้น ต้องกำหนดให้เขาหากว่าไม่ประสงค์จะให้ข้อมูลส่วนบุคคลของตนถูกจัดเก็บหรือถูกประมวลผลโดยผู้ควบคุมข้อมูล หรือว่าไม่มีสาเหตุอันชอบด้วยกฎหมายในการที่จะเก็บข้อมูลส่วนบุคคลของเขาเอาไว้อีกต่อไป ข้อมูลส่วนบุคคลนั้นก็ควรถูกลบออกจากระบบไปเสีย[273] จากแนวคิดนี้นำไปสู่การประกาศใช้หลักการในเรื่องสิทธิที่จะถูกลืมตามกฎหมายคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลฉบับใหม่ของสหภาพยุโรป ซึ่งก็คือ General Data Protection Regulation (GDPR) ที่มีการกำหนดหลักการในเรื่องสิทธิที่จะถูกลืมไว้ใน มาตรา 17 อันมีสาระสำคัญดังนี้คือ[274]

1. เจ้าของข้อมูลมีสิทธิที่จะได้รับจากผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลในการลบข้อมูลส่วนบุคคลต่าง ๆ ที่เกี่ยวข้องกับตนเองโดยมิชักช้า และผู้ควบคุมข้อมูลมีหน้าที่ที่จะต้องลบข้อมูลดังกล่าวโดยไม่ชักช้า เมื่อ

1) ข้อมูลส่วนบุคคลนั้น ไม่มีความจำเป็นที่จะต้องถูกเก็บหรือถูกประมวลผลแล้ว

2) เจ้าของข้อมูลส่วนบุคคลถอนความยินยอมในการประมวลผลข้อมูลส่วนบุคคลนั้น

3) เจ้าของข้อมูลส่วนบุคคลคัดค้านการประมวลผลข้อมูลส่วนบุคคลของตนเองตามพฤติการณ์ที่กฎหมายกำหนด

4) ข้อมูลส่วนบุคคลถูกประมวลผลโดยมิชอบด้วยกฎหมาย

5) ข้อมูลส่วนบุคคลจำต้องถูกลบเพื่อให้เป็นไปตามกฎหมายของประเทศสมาชิก โดยผู้ควบคุมข้อมูลตกอยู่ภายใต้บังคับของกฎหมายดังกล่าว

6) ข้อมูลส่วนบุคคลถูกเก็บไว้ตามข้อเสนอของการให้บริการสังคมเกี่ยวกับข้อมูล

2. ในกรณีที่ผู้ควบคุมข้อมูลได้มีการเผยแพร่ข้อมูลดังกล่าวสู่สาธารณะ และมีหน้าที่ต้องลบข้อมูลดังกล่าวตามคำเรียกร้องของเจ้าของข้อมูล ผู้ควบคุมนั้นจะดำเนินการดังกล่าวอย่างเป็น

---

[273] *เรื่องเดียวกัน*, หน้า 420.

[274] อัญธิกา ณ พิบูลย์, *เรื่องเดิม*, หน้า 46.

เหตุเป็นผล โดยคำนึงถึงวิธีการทางเทคนิคที่เกี่ยวข้อง และค่าใช้จ่ายต่าง ๆ รวมถึงต้องแจ้งผู้ควบคุมข้อมูลคนอื่น ๆ ที่ได้มีการทำสำเนา ทำซ้ำซึ่งข้อมูลที่เจ้าของข้อมูลได้ร้องขอให้ลบ และทราบถึงคำร้องขอเช่นนั้นด้วย

3. ข้อ 1 และ ข้อ 2 จะไม่ใช้บังคับในกรณีที่

1) เพื่อเป็นการใช้สิทธิเกี่ยวกับเสรีภาพในการแสดงความคิดเห็นหรือแสดงข้อมูล

2) เพื่อเป็นการปฏิบัติตามกฎหมายของประเทศสมาชิก ซึ่งผู้ควบคุมข้อมูลนั้นอยู่ภายใต้บังคับต้องปฏิบัติตามเพื่อประโยชน์สาธารณะ

3) เพื่อประโยชน์สาธารณะในด้านสุขภาพ

4) เพื่อบรรลุวัตถุประสงค์ในส่วนของประโยชน์สาธารณะ การทำวิจัยทางด้านวิทยาศาสตร์ ประวัติศาสตร์และสถิติ

5) เพื่อเป็นข้อต่อสู้ทางกฎหมาย

จากสาระสำคัญของ General Data Protection Regulation ในเรื่องสิทธิที่จะถูกลืมที่กล่าวมาจะเห็นได้ว่า วัตถุประสงค์ของการกำหนดสิทธิที่จะถูกลืมไว้ในกติกายุโรปเรื่องนี้นั้น มีเป้าหมายเพื่อมุ่งสนับสนุนให้ผู้ทรงสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในฐานะเป็นเจ้าของข้อมูลได้มีอำนาจในการควบคุมข้อมูลของตนได้อย่างแท้จริง เป็นการกำหนดให้อำนาจแก่ผู้ทรงสิทธิอย่างเต็มที่ที่จะตัดสินใจว่าข้อมูลของตนนั้นควรจะได้รับการปฏิบัติอย่างไร หรือจะส่งมอบหรือมอบหมายให้ผู้ใดทำการเก็บรักษา

อย่างไรก็ดี สิทธิที่จะถูกลืมนี้ มีการกำหนดข้อยกเว้นไว้นอกจากที่ได้กล่าวไว้ในสาระสำคัญข้างต้นแล้ว General Data Protection Regulation ได้กำหนดหลักการไว้ว่า รัฐสมาชิกสามารถที่จะออกกฎหมายยกเว้นสิทธิของเจ้าของข้อมูลส่วนบุคคลซึ่งรวมถึงสิทธิที่จะถูกลืมได้ สำหรับการประมวลผลข้อมูลส่วนบุคคลที่มีวัตถุประสงค์เฉพาะเพื่อการประกอบกิจการหนังสือพิมพ์ หรือเพื่อวัตถุประสงค์ทางศิลปะหรือวรรณคดี เพื่อความสอดคล้องของสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลกับสิทธิเสรีภาพในการแสดงความคิดเห็นภายใต้หลักเกณฑ์ของกฎหมาย[275]

นอกจากนี้แล้ว หากพิจารณาถึงสภาพบังคับของสิทธิที่จะถูกลืมแล้วจะเห็นว่า General Data Protection Regulation กำหนดว่าในกรณีที่มีการฝ่าฝืนไม่ปฏิบัติตาม ผู้ฝ่าฝืนอาจได้รับสภาพบังคับ ดังนี้คือ ได้รับการตักเตือนเป็นหนังสือในกรณีที่มีการฝ่าฝืนครั้งแรกและไม่ได้เป็นการฝ่าฝืนโดยจงใจ หรือจะถูกตรวจสอบในเรื่องการคุ้มครองข้อมูลเป็นระยะ หรือถูกปรับเป็นจำนวน

---

[275] General Data Protection Regulation, Article 80.

เงินไม่เกิน 1,000,000,000 ยูโร หรือไม่เกินร้อยละห้าของรายได้จากการประกอบกิจการทั่วโลกตลอดปีในกรณีที่ผู้ฝ่าฝืนเป็นองค์กรธุรกิจทั้งนี้แล้วแต่ว่าจำนวนไหนจะมากกว่ากัน[276]

จากหลักการที่กล่าวมา เมื่อพิจารณาถึงพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ของประเทศไทย จะเห็นว่ามีการบัญญัติรับรองสิทธิที่จะถูกลืมนี้ไว้ ในมาตรา 33 โดยวางหลักการว่า “ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่ปฏิบัติตามหลักเกณฑ์แห่งพระราชบัญญัตินี้ เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบ หรือทำลาย ระงับการใช้ชั่วคราว หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล ที่เป็นเจ้าของข้อมูลส่วนบุคคลได้” แต่ทว่าการบัญญัติรับรองหลักการเรื่องสิทธิที่จะถูกลืมของประเทศไทยมีประเด็นข้อสังเกตที่อาจเป็นปัญหาในทางปฏิบัติต่อไปดังนี้คือ

ประการแรก การบัญญัติรับรองสิทธิที่จะถูกลืมไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนส่วนบุคคล พ.ศ.2562 ไม่ได้มีการกำหนดเงื่อนไขการใช้สิทธิไว้อย่างชัดเจนเหมือนเช่นกรณีของ General Data Protection Regulation ที่มีการกำหนดเงื่อนไขการใช้สิทธิตามมาตรา 17 ว่าเจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลลบข้อมูลส่วนบุคคลของตนได้ในกรณีดังต่อไปนี้ คือ

1. ข้อมูลส่วนบุคคลนั้น ไม่มีความจำเป็นที่จะต้องถูกเก็บหรือถูกประมวลผลแล้ว
2. เจ้าของข้อมูลส่วนบุคคลถอนความยินยอมในการประมวลผลข้อมูลส่วนบุคคลนั้น
3. เจ้าของข้อมูลส่วนบุคคลคัดค้านการประมวลผลข้อมูลส่วนบุคคลของตนเองตามพฤติการณ์ที่กฎหมายกำหนด
4. ข้อมูลส่วนบุคคลถูกประมวลผลโดยมิชอบด้วยกฎหมาย
5. ข้อมูลส่วนบุคคลจำต้องถูกลบเพื่อให้เป็นไปตามกฎหมายของประเทศสมาชิกโดยผู้ควบคุมข้อมูลตกอยู่ภายใต้บังคับของกฎหมายดังกล่าว
6. ข้อมูลส่วนบุคคลถูกเก็บไว้ตามข้อเสนอของการให้บริการสังคมเกี่ยวกับข้อมูล

การไม่ได้มีการกำหนดเงื่อนไขการใช้สิทธิที่จะถูกลืมอย่างชัดเจนนี้ ในอนาคตจะส่งผลต่อการใช้และการตีความ มาตรา 33 ว่าผู้ทรงสิทธิสามารถจะใช้สิทธิได้ในทุกเมื่อและทุกกรณี โดยไม่จำเป็นต้องคำนึงถึงสิทธิอื่น ๆ เกี่ยวข้องกันหรือไม่ เช่น สิทธิที่เข้าถึงข้อมูลข่าวสาร ,สิทธิเสรีภาพที่จะแสดงความคิดเห็น หรือสิทธิอันเกี่ยวเนื่องจากประโยชน์สาธารณะอื่น ๆ

ประการที่สอง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ของประเทศไทยไม่ได้มีการกำหนดข้อยกเว้นของการใช้สิทธิที่จะถูกลืมไว้อย่างชัดเจนเหมือนกับกรณีของ General Data Protection Regulation ที่มีการกำหนดข้อยกเว้นไว้อย่างชัดเจนในกรณีที่ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลมีความจำเป็นด้วยเหตุต่าง ๆ ดังนี้คือ

---

[276] General Data Protection Regulation, Article 79.

1. เพื่อเป็นการใช้สิทธิเกี่ยวกับเสรีภาพในการแสดงความคิดเห็นหรือแสดงข้อมูล

2. เพื่อเป็นการปฏิบัติตามกฎหมายของประเทศสมาชิก ซึ่งผู้ควบคุมข้อมูลนั้นอยู่ภายใต้บังคับต้องปฏิบัติตามเพื่อประโยชน์สาธารณะ

3. เพื่อประโยชน์สาธารณะในด้านสุขภาพ

4. เพื่อบรรลุวัตถุประสงค์ในส่วนของประโยชน์สาธารณะ การทำวิจัยทางด้านวิทยาศาสตร์ ประวัติศาสตร์และสถิติ

5. เพื่อเป็นข้อต่อสู้ทางกฎหมาย

นอกจากนั้น การไม่ได้มีการกำหนดข้อจำกัดการใช้สิทธิที่จะถูกลืมอย่างชัดเจนนี้ ในอนาคตจะส่งผลต่อการใช้และการตีความ มาตรา 33 เช่นเดียวกับประการก่อนหน้านี้คือ ผู้ทรงสิทธิสามารถจะใช้สิทธิได้ในทุกเมื่อและทุกกรณี โดยไม่จำเป็นต้องคำนึงถึงสิทธิอื่น ๆ เกี่ยวข้องกันหรือไม่ เช่น สิทธิที่เข้าถึงข้อมูลข่าวสาร, สิทธิเสรีภาพที่จะแสดงความคิดเห็น หรือสิทธิอันเกี่ยวเนื่องจากประโยชน์สาธารณะอื่น ๆ

ประการที่สาม หลักการเรื่องสิทธิที่จะถูกลืมตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ยังขาดสภาพบังคับทางกฎหมายที่เหมาะและชัดเจน ในกรณีที่มีการฝ่าฝืนสิทธิของเจ้าของข้อมูลส่วนบุคคลที่มีการร้องขอให้ลบหรือทำลายข้อมูลส่วนบุคคลของตน กล่าวคือ แม้ในบทบัญญัติของกฎหมายฉบับนี้จะมีการกำหนดไว้ในมาตรา 75 ที่วางหลักว่าถ้าผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลอันเป็นการฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติแห่งพระราชบัญญัตินี้ ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ต้องชดใช้ค่าสินไหมทดแทน เพื่อการนั้นแก่เจ้าของข้อมูลส่วนบุคคล ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่ก็ตาม ซึ่งกรณีนี้ถือว่าเป็นการกำหนดความรับผิดในทางแพ่งไว้แต่เพียงด้านเดียวเท่านั้น

แต่ทว่าในกรณีของบทกำหนดโทษในทางอาญาและโทษทางปกครองไม่ได้มีการกำหนดแก่กรณีของการกระทำที่เป็นการฝ่าฝืนสิทธิที่จะถูกลืมไว้แต่อย่างใด ซึ่งสภาพบังคับทั้งทางอาญาและทางปกครองนี้ถือเป็นกลไกขับเคลื่อนที่สำคัญในอันที่จะทำให้สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ในมิติของสิทธิที่จะถูกลืมสามารถเกิดผลสำเร็จได้จริงในทางปฏิบัติ ซึ่งการกำหนดมาตรการในการคุ้มครองสิทธินั้น ควรจะมีการกำหนดไว้หลายระดับเพื่อให้สอดคล้องกับความรุนแรงของการฝ่าฝืนอย่างเช่นกรณีของ General Data Protection Regulation ที่มีการกำหนดมาตราไว้ถึง 3 แนวทางตามระดับของความรุนแรงดังที่ได้กล่าวมาแล้วตอนต้น

5.1.3.3 สิทธิที่จะย้ายหรือถ่ายโอนข้อมูล (Rights to Data Portability)

General Data Protection Regulation กำหนดยอมรับสิทธินี้ไว้ ปรากฏตาม Article 20 โดยเจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะได้รับข้อมูลส่วนบุคคลที่เกี่ยวกับตนที่ให้ไว้แก่

ผู้ควบคุมข้อมูลส่วนบุคคล โดยข้อมูลนั้นอยู่ในสภาพที่มีการจัดหมวดหมู่ และอยู่ในรูปแบบที่สามารถอ่านได้โดยเครื่องคอมพิวเตอร์ (Machine-Readable) นอกจากนี้ ยังมีสิทธิที่จะให้โอนข้อมูลดังกล่าวให้กับผู้ควบคุมข้อมูลส่วนบุคคลรายอื่นได้ด้วย ทั้งนี้ สิทธินี้จะใช้เฉพาะในกรณีที่การประมวลผลมีฐานมาจากความยินยอม และการประมวลผลนั้นได้ทำโดยวิธีการอัตโนมัติ (Automated Means) เท่านั้น

สำหรับรัฐบัญญัติสาธารณะรัฐดิจิตอล ของประเทศฝรั่งเศสก็ได้กำหนดหลักการใหม่ให้สิทธิแก่ผู้บริโภคในการกู้คืนและโอนย้ายข้อมูลส่วนบุคคลของพวกเขา หลักการใหม่นี้กำหนดให้ผู้ให้บริการการสื่อสารออนไลน์ทั้งหมดแก่สาธารณะ ต้องยอมให้ผู้บริโภคสามารถกู้คืนข้อมูลรวมถึงไฟล์ข้อมูลข้อมูลทั้งหมดได้ โดยไม่เสียค่าใช้จ่ายและสามารถเข้าถึงได้จากบัญชีออนไลน์ของผู้ใช้ และข้อมูลนั้นต้องสามารถนำกลับมาใช้ใหม่โดยผู้ควบคุมข้อมูลอื่นได้อย่างง่ายดาย ซึ่งผู้ควบคุมข้อมูลจะต้องจัดเตรียมข้อมูลในรูปแบบที่สามารถอ่านได้ แต่ถ้าหากไม่สามารถทำได้ผู้ควบคุมข้อมูลจะต้องแจ้งให้ผู้บริโภคทราบถึงข้อจำกัดดังกล่าวและให้วิธีการอื่นสำหรับผู้ใช้ในการกู้คืนข้อมูลของตน

นอกจากนั้นหลักการนี้ยังปรากฏอยู่ใน The Data Protection Act 2018 ของประเทศอังกฤษเช่นเดียวกัน

สำหรับประเทศไทย ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคล พ.ศ.2562 ได้มีการบัญญัติรับรองสิทธิที่จะย้ายหรือถ่ายโอนข้อมูล (Rights to Data Portability) นี้ไว้ในมาตรา 31 (1) โดยบัญญัติว่า เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลในรูปแบบดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นเมื่อสามารถทำได้ด้วยวิธีการอัตโนมัติ ซึ่งจะเห็นว่าการกำหนดหลักการนั้นก็เป็นไปในแนวทางเดียวกันกับกติการะหว่างประเทศและกฎหมายระหว่างประเทศที่ได้กล่าวมาข้างต้น

5.1.4 วิเคราะห์ข้อจำกัดในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล

5.1.4.1 ข้อจำกัดของการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

การคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลที่สำคัญก็คือ การควบคุมการเก็บรวมรวม การใช้ การเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูล โดยเฉพาะอย่างยิ่งการควบคุมการประมวลผลข้อมูลส่วนบุคคลนั้นมีความสำคัญมาก ตัวอย่าง ดังจะเห็นได้จากการที่ GDPR ได้วางหลักการที่สำคัญสำหรับการประมวลผล[277]ข้อมูลส่วนบุคคลเอาไว้ ซึ่งหลักการที่สำคัญ

---

[277] การประมวลผล (Processing) ในความหมายของ GDPR หมายถึง การดำเนินการหรือชุดของการ ดำเนินการที่ทำต่อข้อมูลส่วนบุคคลหรือชุดของข้อมูลส่วนบุคคล ทั้งนี้ ไม่ว่าการดำเนินการดังกล่าวจะ อาศัยวิธีการอัตโนมัติ (Automated Mean) หรือวิธีการไม่อัตโนมัติ (Manual) ก็ตาม เช่น

ประการหนึ่งก็คือ การประมวลผลข้อมูลส่วนบุคคลจะต้องเป็นไปโดยชอบด้วยกฎหมาย ดังนั้น ในกรณีที่จะทำการประมวลผลข้อมูลส่วนบุคคลก็จะต้องพิจารณาด้วยว่าการประมวลผลนั้นมีฐานรองรับตามกฎหมายหรือไม่ ไม่เช่นนั้นแล้วการประมวลผลข้อมูลส่วนบุคคลดังกล่าวอาจมีผลเป็นการละเมิด

ข้อยกเว้นที่ทำให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปโดยชอบด้วยกฎหมาย ตามหลักการ Article 6 GDPR สรุปได้ดังต่อไปนี้คือ[278]

1. ฐานความยินยอม กล่าวคือ เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมสำหรับการประมวลผลข้อมูลส่วนบุคคลของตนเพื่อวัตถุประสงค์ใดวัตถุประสงค์หนึ่งหรือหลาย วัตถุประสง์

2. ฐานจากสัญญา กล่าวคือ หากการประมวลผลนั้นมีความเป็นจำเป็นแก่การปฏิบัติตามสัญญาที่เจ้าของข้อมูลส่วนบุคคลเข้าเป็นคู่สัญญาอยู่ด้วย หรือเพื่อที่จะดำเนินการให้เป็นไปตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนการเข้าทำสัญญา ก็จะทำให้การประมวลผลนั้นชอบด้วยกฎหมาย

3. ฐานจากหน้าที่ตามกฎหมาย กล่าวคือ การประมวลผลนั้นมีความจำเป็นในการปฏิบัติหน้าที่ตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งฐานแห่งการประมวลผลในข้อนี้ไม่ได้หมายความว่าจะต้องมีกฎหมายที่กำหนดโดยเฉพาะเจาะจงให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำการประมวลผล เพียงแค่ผู้ควบคุมข้อมูลส่วนบุคคลมีวัตถุประสงค์ในภาพรวมที่จะต้องปฏิบัติให้เป็นไปตามหน้าที่ตามกฎหมายก็ถือได้ว่าสามารถอาศัยฐานในข้อนี้ได้แล้ว

4. ฐานจากการคุ้มครองชีวิต (Vital Interests) กล่าวคือ การประมวลผลนั้นจำเป็นสำหรับการปกป้องชีวิตของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่น

5. ฐานจากหน้าที่ต่อสาธารณะ กล่าวคือ การประมวลผลนั้นจำเป็นสำหรับการปฏิบัติงานเพื่อประโยชน์สาธารณะ หรือเป็นการใช้อำนาจรัฐของผู้ควบคุมข้อมูลส่วนบุคคล

6. ฐานจากประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest) กล่าวคือ การประมวลผลนั้นเป็นการจำเป็นเพื่อให้ได้มาซึ่งประโยชน์โดยชอบด้วยกฎหมาย ซึ่งประโยชน์ดังกล่าว

การเก็บ รวบรวม บันทึก จัดกลุ่ม จัดวางโครงสร้าง เก็บ ปรับปรุงหรือเปลี่ยนแปลง การกู้คืน ค้นหา (Consultation) ใช้ เปิดเผยโดยการโอน (Disclosure by Transmission) เผยแพร่หรือทำให้เข้าถึงได้ จัดเรียงหรือควบรวม (Alignment or Combination) จำกัด (Restriction) ลบ (Erasure) หรือทำลาย (Destruction) เป็นต้น

[278] รักไท เทพปัญญา, **ข้อมูลเบื้องต้นเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (The General Data Protection Regulation (GDPR)),** ค้นวันที่ 1 พฤษภาคม 2562 จาก https://lawforasean.com/blog/2018/07/-the-general-data-protection-regulation-gdpr?lang=th

อาจเป็นของผู้ควบคุมข้อมูลส่วนบุคคลหรือบุคคลที่สามก็ได้ แต่ประโยชน์ดังกล่าวจะต้องไม่ถูกกลบกลืน (Overridden) โดยประโยชน์หรือสิทธิและเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคลที่ จำเป็นต้องได้รับการคุ้มครองข้อมูลส่วนบุคคล

เมื่อพิจารณาเปรียบเทียบกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 จะเห็นได้ว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยได้นำเอาหลักการของ GDPR มากำหนดในในตัวบทบัญญัติซึ่งปรากฏดังตารางข้างล่างนี้

ตารางที่ 5.4 ข้อยกเว้นที่ทำให้การประมวลผลข้อมูลเป็นไปโดยชอบด้วยกฎหมายเปรียบเทียบระหว่าง GDPR กับ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

ข้อยกเว้น	**GDPR**	**พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562**
ฐานความยินยอม	ความยินยอม (Consent) เป็นปัจจัยที่ทำให้การ ประมวลข้อมูลนั้นชอบด้วย กฎหมาย (มาตรา 6 (1))	มาตรา 27 ประกอบมาตรา 24(3)
ฐานจากสัญญา	การประมวล ข้อมูลที่จำเป็น เพื่อการทำ สัญญา ปฏิบัติ ตามสัญญากับ เจ้าของข้อมูล (มาตรา 6 (1) (b)	มาตรา 27 ประกอบมาตรา 24(3)
ฐานจากหน้าที่ตามกฎหมาย	การประมวล ข้อมูลนั้นมีความจำเป็นเพื่อปฏิบัติ ตามกฎหมาย (มาตรา 6 (1) (c)	มาตรา 27 ประกอบมาตรา 24(6)
ฐานจากการคุ้มครองชีวิต (Vital Interests)	การประมวล ข้อมูลนั้นมีความจำเป็นเพื่อ ปกป้องประโยชน์ ของเจ้าของ ข้อมูลหรือบุคคล ธรรมดาอื่น (มาตรา 6 (1) (d)	มาตรา 27 ประกอบมาตรา 24(2)
ฐานจากหน้าที่ต่อสาธารณะ	การประมวลข้อมูลที่จำเป็นเพื่อการปฏิบัติการที่เป็นไปเพื่อประโยชน์สาธารณะ	มาตรา 27 ประกอบมาตรา 24 (1)(4)

ตารางที่ 5.4 (ต่อ)

ข้อยกเว้น	GDPR	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562
ฐานจากประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest)	การประมวลผลนั้นเป็นการจำเป็นเพื่อให้ได้มาซึ่งประโยชน์โดยชอบด้วยกฎหมายซึ่งประโยชน์ดังกล่าวอาจเป็นของผู้ควบคุมข้อมูลส่วนบุคคลหรือบุคคลที่สามก็ได้ แต่ประโยชน์ดังกล่าวจะต้องไม่ถูกกลบกลืน (Overridden) โดยประโยชน์หรือสิทธิและเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคลที่จำเป็นต้องได้รับการคุ้มครองข้อมูลส่วนบุคคล	มาตรา 27 ประกอบมาตรา 24(5)

5.1.4.2 ข้อจำกัดการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายฉบับอื่น

1) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562

สำหรับเจตนารมณ์ของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 เป็นกฎหมายที่ถูกตราขึ้นโดยเหตุผลจากความก้าวหน้าทางเทคโนโลยีสารสนเทศซึ่งถูกนำมาใช้ประโยชน์ในการทำธุรกรรมหรือการติดต่อสื่อสาร จึงก่อให้เกิดสภาพแวดล้อมที่เอื้ออำนวยต่อภัยคุกคามและการก่ออาชญากรรมทางไซเบอร์ที่สามารถส่งผลกระทบในวงกว้างได้อย่างรวดเร็วและปัจจุบันยิ่งทวีความรุนแรงมากขึ้น สร้างความเสียหายทั้งในระดับบุคคลและระดับประเทศ การป้องกันหรือรับมือกับภัยคุกคามหรือความเสี่ยงบนไซเบอร์จึงต้องอาศัยความรวดเร็วและการประสานงานกับทุกหน่วยงานที่เกี่ยวข้องเพื่อป้องกันและรับมือได้ทันสถานการณ์ และมีการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง ดังนั้น เพื่อให้ประเทศไทยสามารถปกป้อง ป้องกัน หรือรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบหรืออาจก่อให้เกิดความเสี่ยงต่อการ ให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียม ซึ่งกระทบต่อความมั่นคงของชาติในมิติต่าง ๆ อันครอบคลุมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจได้อย่างเหมาะสม มีการ

ดำเนินการที่รวดเร็ว และมีความเป็นเอกภาพ สมควรกำหนดให้มีคณะกรรมการขึ้นเพื่อกำหนดมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ ให้เป็นไปอย่างมีประสิทธิภาพและเกิดผลสัมฤทธิ์[279]

โดยสาระสำคัญของกฎหมายฉบับนี้กล่าวโดยสรุปได้ดังนี้ คือ

ประการแรก มีการกำหนดนิยามความหมายของคำว่า ภัยคุกคามทางไซเบอร์ ไว้ในมาตรา 3 โดยให้หมายถึงการกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลที่เกี่ยวข้อง

ประการที่สอง กฎหมายฉบับนี้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ไว้ในมาตรา 60 โดยแบ่งออกเป็น 3 ระดับ คือ

1) ภัยคุกคามไซเบอร์ระดับไม่ร้ายแรง หมายถึงภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงอย่างมีนัยสำคัญถึงระดับที่ทำให้คอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศหรือการให้บริการของรัฐด้อยประสิทธิภาพลง

2) ภัยคุกคามไซเบอร์ในระดับร้ายแรง หมายถึง ภัยคุกคามที่มีลักษณะเป็นการเพิ่มขึ้นอย่างมีนัยสำคัญของการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์โดยมุ่งหมายเพื่อโจมตีโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศและการโจมตีดังกล่าวมีผลทำให้ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานที่สำคัญของประเทศ ความมั่นคงของรัฐ ความสัมพันธ์ระหว่างประเทศ การป้องกันประเทศ เศรษฐกิจ สาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชนเสียหายจนไม่สามารถทำงานหรือให้บริการได้

3) ภัยคุกคามระดับวิกฤต หมายถึง ภัยคุกคามทางไซเบอร์ในระดับวิกฤติที่มีลักษณะดังต่อไปนี้

(1) เป็นภัยคุกคามทางไซเบอร์ที่เกิดจากการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ในระดับที่สูงกว่าภัยคุกคามทางไซเบอร์ในระดับร้ายแรงโดยส่งผลกระทบรุนแรงต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศในลักษณะที่เป็นวงกว้าง จนทำให้การทำงานของหน่วยงานรัฐหรือการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชนล้มเหลวทั้งระบบ จนรัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้ หรือการใช้

---

[279] หลักการและเหตุผลของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562

มาตรการเยียวยาตามปกติในการแก้ไขปัญหาภัยคุกคามไม่สามารถแก้ไขปัญหาได้และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ ของประเทศซึ่งอาจทำให้บุคคลจำนวนมากเสียชีวิต หรือระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างระดับประเทศ

(2) เป็นภัยคุกคามทางไซเบอร์อันกระทบหรืออาจกระทบความสงบเรียบร้อยของประชาชนหรือเป็นภัยต่อความมั่นคงของรัฐหรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขันหรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือการสงคราม ซึ่งจำเป็นต้องมีมาตรการเร่งด่วนเพื่อรักษาไว้ซึ่งการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญแห่งราชอาณาจักรไทย เอกราชและบูรณภาพแห่งอาณาเขต ผลประโยชน์ของชาติ การปฏิบัติตามกฎหมาย ความปลอดภัยของประชาชน การดำรงชีวิตโดยปกติสุขของประชาชน การคุ้มครองสิทธิเสรีภาพ ความสงบเรียบร้อยหรือประโยชน์ส่วนรวม หรือการป้องปัดหรือเยียวยาความเสียหายจากภัยพิบัติสาธารณะอันมีมาอย่างฉุกเฉินและร้ายแรง

ประการที่สาม เพื่อเป็นการกำกับการรับมือกับภัยคุกคามทางไซเบอร์ในประการที่สองที่กล่าวมา กฎหมายฉบับนี้จึงมีการจัดตั้งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช. หรือ NCSC) โดยมีนายกรัฐมนตรี เป็นประธานกรรมการ และมีกรรมการโดยตำแหน่ง ประกอบด้วยรัฐมนตรีว่าการกระทรวงกลาโหม รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ปลัดกระทรวงการคลัง ปลัดกระทรวงยุติธรรม ผู้บัญชาการตำรวจแห่งชาติ เลขาธิการสภาความมั่นคงแห่งชาติ (สมช.) นอกจากนั้น คณะกรรมการฯ ยังจะมีกรรมการผู้ทรงคุณวุฒิไม่เกินเจ็ดคนที่คณะรัฐมนตรีแต่งตั้งจากผู้มีความรู้ ความเชี่ยวชาญและประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เทคโนโลยีสารสนเทศและการสื่อสาร การคุ้มครองข้อมูลส่วนบุคคล วิทยาศาสตร์ วิศวกรรมศาสตร์ กฎหมาย หรืออื่น ๆ ที่เกี่ยวข้อง

โดยคณะกรรมการจะมีหน้าที่โดยสรุปคือ เสนอนโยบาย แผนว่าด้วยการรักษาความมั่นคงไซเบอร์ ส่งเสริม สนับสนุน การรักษาความมั่นคงไซเบอร์ ทำแผนปฏิบัติการรักษาความมั่นคงไซเบอร์ ให้คณะรัฐมนตรีให้ความเห็นชอบ กำหนดนโยบายการบริหารจัดการให้กับหน่วยงานรัฐ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ไปจนถึงมอบหมายการควบคุมและกำกับดูแล กรอบการดำเนินงานด้านความมั่นคงไซเบอร์ให้หน่วยงานควบคุมหรือกำกับดูแล และติดตามประเมินผลการปฏิบัติตามนโยบาย และให้ข้อเสนอแนะแก่คณะรัฐมนตรีหรือกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

นอกจากคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งเป็นองค์กรที่เปรียบเสมือนร่มใหญ่ในการดูแลในภาพรวมแล้ว กฎหมายฉบับนี้ ยังให้มีคณะกรรมการ

กำกับดูแลด้านความมั่นคงไซเบอร์ ที่มีชื่อว่า คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) มีนายกรัฐมนตรี และรัฐมนตรีกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นประธานกรรมการ มีผู้บัญชาการทหารสูงสุด ปลัดกระทรวงต่าง ๆ คือ กระทรวงการต่างประเทศ กระทรวงคมนาคม กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมกระทรวงพลังงาน กระทรวงมหาดไทย กระทรวงสาธารณสุข เป็นกรรมการและมีผู้บัญชาการตำรวจแห่งชาติ เลขาธิการสภาความมั่นคงแห่งชาติ ผู้อำนวยการสำนักข่าวกรองแห่งชาติ ผู้ว่าการธนาคารแห่งประเทศไทย เลขาธิการสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ เลขาธิการคณะกรรมการกิจการการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) เป็นกรรมการโดยตำแหน่ง และกรรมการทรงคุณวุฒิอีกสี่คน ให้เลขาธิการเป็นกรรมการและเลขานุการ

คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) มีหน้าที่โดยสรุป กล่าวคือ ติดตามการดำเนินงานตามที่คณะกรรมการฯ กมช. ได้วางเอาไว้ ดูแลและดำเนินการรับมือกับภัยคุกคามไซเบอร์ระดับร้ายแรง กำหนดกรอบมาตรฐานการรักษาความมั่นคงไซเบอร์ ที่จะใช้เป็นข้อกำหนดขั้นต่ำ กำหนดระดับภัยคุกคามทางไซเบอร์ และรายละเอียดมาตรการป้องกัน รับมือ ประเมิน ปราบปราบ ระงับภัยเพื่อเสนอต่อคณะกรรมการฯ กมช. ไปจนถึงวิเคราะห์สถานการณ์ ประเมินผลกระทบจากภัยเพื่อเสนอให้คณะกรรมการพิจารณาสั่งการเมื่อมีภัยระดับร้ายแรง

ประการที่สี่ มาตรการที่สำคัญของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 คือ เมื่อปรากฏแก่คณะกรรมการฯ กกม. ว่าเกิด หรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ระดับร้ายแรง คณะกรรมการฯ กกม. สามารถออกคำสั่งให้สำนักงานดำเนินการรวบรวมข้อมูล ให้ความช่วยเหลือ ป้องกัน แจ้งเตือนและประสานงาน ทั้งนี้ มาตรา 61 อำนวยความสะดวกให้สำนักงาน โดยให้เลขาธิการมีอำนาจสั่งให้เจ้าหน้าที่ดำเนินการได้ต่อไปนี้

1. มีหนังสือขอความร่วมมือจากคนที่เกี่ยวข้องเพื่อมาให้ข้อมูล
2. มีหนังสือขอข้อมูล เอกสาร หรือสำเนาข้อมูลในความครอบครองผู้อื่น
3. ถามบุคคลผู้มีความรู้ ความเข้าใจสถานการณ์ ข้อเท็จจริง
4. เข้าไปในอสังหาริมทรัพย์หรือสถานประกอบการที่เกี่ยวข้อง หรือคาดว่ามีส่วนเกี่ยวข้องโดยได้รับความยินยอมจากผู้ครอบครองสถานที่นั้น

จะเห็นว่า แม้กฎหมายฉบับนี้จะใช้คำว่าขอความร่วมมือ แต่หากพิจารณามาตรา 73 ว่าด้วยบทลงโทษ ได้มีการบัญญัติไว้ว่า ผู้ใดไม่ปฏิบัติตามหนังสือเรียกของพนักงานเจ้าหน้าที่ หรือไม่ส่งข้อมูลให้พนักงานเจ้าหน้าที่ตามมาตรา 61 (1) (2) โดยไม่มีเหตุอันสมควรแล้วแต่กรณี ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท กรณีเช่นนี้ก็ถือเป็นลักษณะของการใช้อำนาจทางกฎหมายในการบังคับนั่นเอง

นอกจากนี้ คณะกรรมการฯ กกม. ยังมีอำนาจตาม มาตรา 64 ให้อำนาจในการออกคำสั่งต่อไปนี้เพื่อรับมือและบรรเทาความเสียหายจากภัยคุกคามระดับร้ายแรง

1. เฝ้าระวังคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ในช่วงเวลาใดเวลาหนึ่ง
2. ตรวจสอบคอมพิวเตอร์ หรือระบบคอมพิวเตอร์เพื่อหาข้อบกพร่อง
3. กำจัดข้อบกพร่อง หรือชุดคำสั่งไม่พึงประสงค์
4. รักษาสถานะข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ด้วยวิธีการใด ๆ เพื่อดำเนินการทางนิติวิทยาศาสตร์ทางคอมพิวเตอร์
5. เข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่เกี่ยวข้องเฉพาะเท่าที่จำเป็น

จากที่กล่าวถึงสาระสำคัญของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ในข้างต้น เมื่อวิเคราะห์แล้วจะเห็นว่า

ประการแรกกฎหมายฉบับนี้เป็นกฎหมายที่มีการให้อำนาจแก่รัฐที่จะเข้ามาล่วงละเมิดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลโดยอาศัยการอ้างอิงประโยชน์สาธารณะในด้านความมั่นคงปลอดภัยของรัฐเป็นพื้นฐาน ทำให้แม้ว่าประเทศไทยจะมีการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 เพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลให้กับประชาชนแล้วก็ตาม แต่สิทธินี้ก็อาจถูกรัฐอาศัยอำนาจตามกฎหมายฉบับนี้ล่วงละเมิดได้โดยการอ้างประโยชน์สาธารณะตามกฎหมาย

ประการที่สอง การกำหนดคำนิยามที่ปรากฏในพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ฯ มีความไม่ชัดเจนแน่นอน ส่งผลให้เกิดข้อกังวลของภาคประชาสังคม อีกทั้งการให้คำนิยามนั้นยังมีลักษณะเป็นการเขียนกว้าง ๆ เหมือนกับกฎหมายความมั่นคงฉบับอื่น ๆ เช่น พระราชบัญญัติกฎอัยการศึกษา พ.ศ.2457 พระราชกำหนดบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ.2548 หรือพระราชบัญญัติการรักษาความมั่นคงภายในราชอาณาจักร พ.ศ.2551 ซึ่งมีปัญหาในทางปฏิบัติมาแล้วทั้งสิ้นในเรื่องการใช้อำนาจของเจ้าหน้าที่รัฐฝ่ายความมั่นคง

โดยเฉพาะอย่างยิ่งในส่วนของคำว่า “ความมั่นคงปลอดภัยไซเบอร์” ตามมาตรา 3 วรรคหนึ่ง ที่กำหนดให้หมายความว่า “มาตรการหรือการดำเนินที่กำหนดขึ้นเพื่อป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามไซเบอร์ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ” ซึ่งการกำหนดเช่นนี้มีลักษณะของการเขียนไว้กว้าง ๆ ทำให้ประชาชนทั่วไปอ่านแล้วเข้าใจได้ยาก จึงอาจเป็นการเปิดโอกาสให้เจ้าหน้าที่ใช้ดุลพินิจในการปฏิบัติงานได้อย่างกว้างขวาง นอกจากนั้นในส่วนของคำว่า “ภัยคุกคาม” ตามมาตรานี้ ก็มีความกำกวม เพราะไม่ได้ระบุให้ชัดเจน

ว่าเป็นภัยคุกคามในเชิงเทคนิคที่มีต่อตัวระบบเท่านั้น หรือจะหมายรวมไปถึงการเผยแพร่เนื้อหาที่เจ้าหน้าที่เห็นว่ากระทบต่อความมั่นคงด้วยหรือไม่

ประการต่อมา พระราชบัญญัติฉบับนี้ได้มีการกำหนดอำนาจให้แก่หน่วยงานด้านความมั่นคงมาก โดยจะเห็นว่า คำว่า “ภัยคุกคามไซเบอร์” กับ “ความมั่นคงทางทหาร” ไม่มีนิยามใด ๆ ในกฎหมายฉบับนี้ มีแต่นิยามคำว่า “การรักษาความมั่นคงปลอดภัยไซเบอร์” ดังที่ได้กล่าวไว้แล้วประการก่อน โดยสิ่งที่อันตรายอย่างยิ่ง ก็คือ ลำพังสถานการณ์ที่ “อาจก่อให้เกิดความเสี่ยง” ก็เพียงพอให้เจ้าหน้าที่ใช้อำนาจละเมิดสิทธิความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลได้แล้ว อันเป็นการผิดหลักสากลที่ว่า กฎหมายที่ลิดรอนสิทธิประชาชนนั้นจะต้องลิดรอนสิทธิเท่าที่ “จำเป็นและได้ส่วน” (Necessary and Proportionate) อย่างชัดเจน นอกจากนี้พระราชบัญญัตินี้ยังมีลักษณะที่น่ากังวลเพราะให้อำนาจเจ้าหน้าที่ตรวจสอบการสื่อสารของประชาชนโดยทุกช่องทางและไม่มีกระบวนการตรวจสอบใด ๆ เลย คล้ายกับการให้อำนาจเจ้าหน้าที่ทหารอย่างเต็มเวลาที่ประกาศใช้กฎอัยการศึก และ เป็นการมอบอำนาจให้กับหน่วยงานความมั่นคงอย่างมหาศาลในทางที่ขาดกลไกตรวจสอบถ่วงดุลต่าง ๆ[280] จึงทำให้ถูกมองว่าเป็นกฎหมายที่จะส่งผลกระทบต่อสิทธิเสรีภาพของประชาชนคนไทยทุกคน เนื่องจากอาจถูกล่วงละเมิดข้อมูลส่วนบุคคลและความลับขององค์กรโดยเจ้าหน้าที่รัฐ

ดังนั้น แม้ว่าประเทศไทยเราจะได้มีการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ออกมา แต่ในขณะเดียวกันรัฐก็ได้ตราพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ออกมาคู่กัน ซึ่งเมื่อพิจารณาหลักการพื้นฐานของกฎหมายทั้งสองฉบับแล้ว พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล กำหนดหลักการสำคัญคือ การห้ามทำการเก็บข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอม ในขณะที่พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ให้อำนาจรัฐเกี่ยวกับในการตรวจสอบและเข้าถึง ซึ่งก็คือการเก็บข้อมูลที่อาจจะเกี่ยวข้องกับภัยคุกคามไซเบอร์จึงรวมถึงข้อมูลส่วนบุคคลที่อยู่ในระบบได้ ประกอบการที่ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลเองก็ได้วางหลักการยกเว้นให้สามารถทำการเก็บรวบรวมข้อมูลโดยไม่ต้องขอความยินยอมได้ในกรณีที่เป็นประโยชน์สาธารณะ หรือตามกฎหมายอื่นที่อนุญาตให้ทำได้ ซึ่งในการบัญญัติเช่นนี้เท่ากับเป็นการเปิดช่องให้กิจการของหน่วยงานรัฐทั้งหลายยกประโยชน์สาธารณะขึ้นมาอ้างได้ว่าภารกิจของหน่วยงานของตนนั้นมีความสำคัญในลักษณะเป็นประโยชน์สาธารณะนั่นเอง ซึ่งจะมีผลกระทบต่อผลในทางปฏิบัติของการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลเป็นอย่างมาก

---

[280] สฤณี อาชวานันทกุล, **“เศรษฐกิจดิจิตอล” เพื่อใคร? อันตรายของชุดกฎหมายไซเบอร์,** ค้นวันที่ 25 เมษายน 2562 จาก https://thaipublica.org/2015/01/dangers-new-cyber-laws/

จากที่กล่าวมาทั้งหมด จึงสรุปได้ว่าแม้ประเทศไทยเราจะมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลออกมาแล้ว แต่ในมิติของการคุ้มครองนั้นแม้ว่าจะเป็นหลักการสำคัญที่จะป้องกันการล่วงละเมิดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลจากบุคคลอื่น ๆ ก็ตาม แต่สำหรับการคุ้มครองข้อมูลส่วนบุคคลจากฝ่ายรัฐ ดูเหมือนจะเป็นปัญหาที่ไม่สามารถปกป้องสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลจากฝ่ายรัฐที่อ้างอิงประโยชน์สาธารณะมาเป็นเหตุผลของการสอดแนม หรือล่วงละเมิดในประการอื่น ๆ ในประเด็นนี้เป็นเรื่องสำคัญกล่าวคือ ถ้าเราพิจารณาในแง่ของ GDPR ที่ได้มีการกำหนดห้ามโอนข้อมูลของพลเมืองยุโรปไปยังประเทศที่มีมาตรฐานการคุ้มครองข้อมูลที่ต่ำกว่านั้น ประเด็นที่รัฐไทยจะต้องพิจารณาก็คือ กฎหมายคุ้มครองข้อมูลส่วนบุคคลนั้นไม่ใช่แค่การมีกฎหมายคุ้มครองข้อมูลแล้วจะถือว่าได้มาตรฐาน จะต้องพิจารณาถึงเนื้อสาระและมาตรฐานในการคุ้มครองตามความเป็นจริงด้วย ไม่เช่นนั้น เราอาจสูญเสียผลประโยชน์ทางการค้าจากสหภาพยุโรป เช่นเดียวกันกับกรณี Safe Harbor ซึ่งเป็นมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่มีผลบังคับใช้ในสหรัฐอเมริกาดังได้กล่าวไว้ในบทก่อน ๆ นั้น ได้กำหนดให้ผู้ประกอบการที่เข้าร่วมโครงการนี้ยอมปฏิบัติตามหลักที่คล้ายคลึงกับกฎหมายยุโรป แต่ต่อมามีการฟ้องศาลยุโรปอ้างข้อมูลว่า รัฐบาลสหรัฐอเมริกามีพฤติกรรมไม่น่าวางใจในการสอดส่องข้อมูลผู้ใช้โทรคมนาคมอย่างกว้าง ทำให้ศาลยุโรปจึงตัดสินในปี ค.ศ.2015 ว่า ความตกลงโอนข้อมูลระหว่างยุโรปกับสหรัฐฯ ไม่ชอบด้วยกฎหมายนั่นเอง

2) พระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ.2562

สำหรับพระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ.2562 ถูกตราขึ้นด้วยเหตุผลที่ว่า เนื่องจากกฎหมายว่าด้วยข่าวกรองแห่งชาติได้ใช้บังคับมาเป็นเวลานาน เนื้อหาและหลักเกณฑ์บางส่วนไม่สอดคล้องกับสถานการณ์ภัยคุกคามความมั่นคงและเทคโนโลยีที่เปลี่ยนแปลงไป นอกจากนี้ ยังมีแนวโน้มของภัยคุกคามรูปแบบใหม่ด้วยวิธีการที่หลากหลายซับซ้อนขยายตัวมากขึ้น ฉะนั้น เพื่อเสริมสร้างสภาวะแวดล้อมให้เอื้อต่อการปฏิบัติการข่าวกรองของชาติ เพิ่มขีดความสามารถในการปฏิบัติงานของเจ้าหน้าที่ และทำให้ภารกิจของรัฐด้านกิจการการข่าวกรองมีประสิทธิภาพยิ่งขึ้น สามารถรองรับสถานการณ์ภัยคุกคามความมั่นคงทุกรูปแบบได้อย่างเหมาะสมและทันท่วงทีจึงจำเป็นต้องตราพระราชบัญญัตินี้ โดยให้สำนักข่าวกรองแห่งชาติจัดให้มีศูนย์ประสานข่าวกรองแห่งชาติ เรียกโดยย่อว่า “ศป.ข.” เป็นหน่วยงานภายในเพื่อทำหน้าที่เป็นหน่วยงานกลางในการประสานกิจการการข่าวกรอง การต่อต้านข่าวกรอง และการรักษาความปลอดภัยฝ่ายพลเรือนร่วมกับหน่วยข่าวกรองอื่นภายในประเทศ ตลอดจนแก้ไขเพิ่มเติมบทนิยาม หน้าที่และอำนาจของสำนักข่าวกรองแห่งชาติ เพื่อให้ทันกับภูมิทัศน์ด้านต่าง ๆ ที่เปลี่ยนแปลงไป ในการนี้ ได้กำหนดให้ผู้อำนวยการสำนักข่าวกรองแห่งชาติมีอำนาจแต่งตั้งข้าราชการพลเรือนสามัญในสำนักข่าวกรองแห่งชาติที่มีความรู้ความสามารถและมีประสบการณ์ด้านการข่าวกรอง การต่อต้านข่าวกรอง การข่าวกรองทางการ

สื่อสาร หรือการรักษาความปลอดภัยฝ่ายพลเรือน เป็นผู้ปฏิบัติงานข่าวกรองเพื่อปฏิบัติหน้าที่ในงานด้านการข่าวกรองของสำนักข่าวกรองแห่งชาติ และเพื่อรักษาความมั่นคงและผลประโยชน์แห่งรัฐและความสงบเรียบร้อยของประชาชน[281] ภายใต้บทบัญญัติของกฎหมายฉบับนี้ ภาครัฐได้อ้างว่าจะทำให้ประชาชนได้ประโยชน์ในด้านความมั่นคง คือ ทำให้มีกลไกที่ชัดเจนเพื่อเพิ่มขีดความสามารถในการปฏิบัติงานของสำนักข่าวกรองแห่งชาติและเจ้าหน้าที่ในสำนักข่าวกรองแห่งชาติ รวมถึงหน่วยการข่าวอื่น ๆ ซึ่งจะทำให้ภารกิจของรัฐด้านกิจการการข่าวกรองมีประสิทธิภาพยิ่งขึ้น

เมื่อพิจารณสาระสำคัญของกฎหมายฉบับนี้แล้วจะเห็นว่ามีสาระสำคัญโดยสรุปดังนี้คือ

ประการแรก กฎหมายฉบับนี้กำหนดนิยามสำคัญไว้ดังนี้คือ[282]

“การข่าวกรอง” หมายความว่า การดำเนินการเพื่อให้ทราบถึงความมุ่งหมาย กำลังความสามารถและความเคลื่อนไหว รวมทั้งวิถีทางของบุคคล กลุ่มบุคคล หรือองค์การใด ทั้งภายในประเทศและต่างประเทศ ที่อาจกระทำการอันเป็นพฤติการณ์เป็นภัยคุกคาม ทั้งนี้เพื่อรักษาความมั่นคงหรือประโยชน์แห่งรัฐและให้รัฐบาลนำมาประกอบการพิจารณาในการกำหนดนโยบายแห่งชาติ

“การต่อต้านข่าวกรอง” หมายความว่า การดำเนินการเพื่อต่อต้านการกระทำของต่างชาติ บุคคลกลุ่มบุคคล หรือองค์การใด ที่มุ่งหมายจะให้ได้ไปซึ่งความลับของชาติ หรือทำลายความมั่นคงแห่งชาติโดยการจารกรรม การบ่อนทำลาย การก่อวินาศกรรม และการก่อการร้าย หรือการอื่นใดอันเป็นภัยคุกคามเพื่อรักษาความมั่นคงหรือประโยชน์แห่งรัฐ

“การข่าวกรองทางการสื่อสาร” หมายความว่า การใช้เทคนิคและการดำเนินกรรมวิธีทางเทคโนโลยีและเครื่องมือสื่อสาร เพื่อให้ได้มาซึ่งข้อมูลข่าวสารเกี่ยวกับความเคลื่อนไหวในการข่าวกรองและการต่อต้านข่าวกรอง

“การรักษาความปลอดภัยฝ่ายพลเรือน” หมายความว่า การให้คำแนะนำช่วยเหลือและกำกับดูแลส่วนราชการฝ่ายพลเรือน รัฐวิสาหกิจ และหน่วยงานอื่นของรัฐ ในการดำเนินการเพื่อรักษาความปลอดภัยแก่เจ้าหน้าที่ สถานที่ ข้อมูลข่าวสาร และสิ่งของอื่น ๆ ของทางราชการให้พ้นจากการจารกรรม การบ่อนทำลาย การก่อวินาศกรรม และการก่อการร้าย

ประการที่สอง ภายใต้อำนาจที่ได้รับจากกฎหมายฉบับนี้ ทำให้สำนักข่าวกรองแห่งชาติอาจสั่งให้หน่วยงานของรัฐหรือบุคคลใดส่งข้อมูลหรือเอกสารที่มีผลกระทบต่อความมั่นคงแห่งชาติภายในระยะเวลาที่ผู้อำนวยการกำหนด หากหน่วยงานของรัฐหรือบุคคลดังกล่าวไม่ส่ง

---

[281] หลักการและเหตุผลของพระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ.2562

[282] มาตรา 4 แห่งพระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ.2562

ข้อมูลหรือเอกสารภายในกำหนดเวลาโดยไม่มีเหตุอันสมควร ให้สำนักข่าวกรองแห่งชาติรายงานต่อนายกรัฐมนตรี เพื่อพิจารณาสั่งการตามที่เห็นสมควรต่อไป

โดยในกรณีที่มีความจำเป็นต้องได้มาซึ่งข้อมูลหรือเอกสารอันเกี่ยวกับการข่าวกรอง การต่อต้านข่าวกรอง การข่าวกรองทางการสื่อสาร หรือการรักษาความปลอดภัยฝ่ายพลเรือน สำนักข่าวกรองแห่งชาติ อาจดำเนินการด้วยวิธีการใด ๆ รวมทั้งอาจใช้เครื่องมืออิเล็กทรอนิกส์ เครื่องมือทางวิทยาศาสตร์ เครื่องโทรคมนาคม หรือเทคโนโลยีอื่นใด เพื่อให้ได้มาซึ่งข้อมูลหรือเอกสารดังกล่าวได้

กล่าวได้ว่า เป็นการเปิดช่องให้สำนักงานข่าวกรองแห่งชาติ สามารถใช้เครื่องมืออิเล็กทรอนิกส์ ล้วงข้อมูลบุคคลได้โดยไม่ผิดกฎหมาย เพื่อป้องกันภัยคุมคามที่นำมาซึ่งความมั่นคงของชาติ และข้อมูลข่าวสารที่ได้มาไม่จำเป็นต้องเปิดเผย เว้นแต่เป็นการเปิดเผยต่อหน่วยข่าวกรอง หน่วยงานความมั่นคง นายกรัฐมนตรี หรือตามคำสั่งศาลเท่านั้น

ข้อกฎหมายตามพระราชบัญญัตินี้ทำให้เกิดข้อถกเถียงมากมาย ซึ่งมีข้อสังเกตประการสำคัญต่อการบังคับใช้ ดังนี้[283]

1. การให้สำนักข่าวกรองแห่งชาติมีอำนาจใช้เครื่องมืออิเล็กทรอนิกส์ เครื่องมือทางวิทยาศาสตร์ เครื่องโทรคมนาคม หรือเทคโนโลยีอื่นใด เพื่อให้ได้มาซึ่งข้อมูลหรือเอกสาร โดยเป็นไปตามระเบียบที่ผู้อำนวยการสำนักข่าวกรองแห่งชาติกำหนดโดยความเห็นชอบของนายกรัฐมนตรี ซึ่งไม่ได้ผ่านกระบวนการในการกลั่นกรองและตรวจสอบการใช้อำนาจจากองค์กรอื่นในลักษณะที่เป็นสากล เช่น จากองค์กรศาล แต่เป็นการใช้อำนาจในลักษณะที่เป็นการเสนอ และตรวจสอบควบคุม ภายในหน่วยงานเดียวกันเอง ทั้งที่เป็นเรื่องที่เกี่ยวข้องกับการคุ้มครองสิทธิเสรีภาพของประชาชนโดยตรงนี้ จะสุ่มเสี่ยงต่อการใช้อำนาจที่ไม่สุจริตและไม่ชอบธรรม และการใช้อำนาจเกินสมควรแก่เหตุ อันเป็นการละเมิดสิทธิเสรีภาพของประชาชนที่รัฐธรรมนูญให้ความคุ้มครองหรือไม่

2. การที่พระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ.2562 มาตรา 6 วรรคสาม บัญญัติให้ความคุ้มครองการดำเนินการเพื่อให้ได้มาซึ่งข้อมูลหรือเอกสาร ที่กระทำไปตามอำนาจหน้าที่โดยสุจริตตามสมควรแก่เหตุ และเพื่อประโยชน์ด้านความมั่นคงหรือการป้องกันภัยสาธารณะให้ถือว่าเป็นการกระทำโดยชอบด้วยกฎหมาย แม้จะมีข้อดีในการให้ความคุ้มครองเจ้าหน้าที่ที่ปฏิบัติหน้าที่โดยสุจริต แต่ก็อาจจะเป็นเหรียญสองด้าน โดยอีกด้านอาจจะเป็นการอ้างและใช้ประโยชน์จากบทบัญญัติกฎหมายในการคุ้มครองการปฏิบัติหน้าที่ไม่สุจริตชอบธรรมของเจ้าหน้าที่รัฐได้

---

[283] ธนกฤต วรธนัชชากุล, **ข้อสังเกตต่อการบังคับใช้ พ.ร.บ.ข่าวกรองแห่งชาติฉบับใหม่**, ค้นวันที่ 27 เมษายน 2562 จาก https://www.isranews.org/isranews-article/75704-aticle-75704.html

3. การใช้อำนาจหน้าที่ของสำนักข่าวกรองแห่งชาติในการได้มาซึ่งข้อมูลหรือเอกสารดังกล่าว จะเป็นการขัดกับรัฐธรรมนูญ มาตรา 3 วรรคสอง ที่บัญญัติให้หน่วยงานของรัฐต้องปฏิบัติหน้าที่ให้เป็นไปตามรัฐธรรมนูญและหลักนิติธรรมหรือไม่

4. การใช้อำนาจหน้าที่ของสำนักข่าวกรองแห่งชาติในการได้มาซึ่งข้อมูลหรือเอกสารตามกฎหมายนี้จะเป็นการละเมิดสิทธิเสรีภาพของประชาชนที่รัฐธรรมนูญคุ้มครองหรือไม่ โดยรัฐธรรมนูญ มาตรา 25 วรรคสาม บัญญัติให้บุคคลซึ่งถูกละเมิดสิทธิเสรีภาพที่ได้รับความคุ้มครองตามรัฐธรรมนูญสามารถยกบทบัญญัติแห่งรัฐธรรมนูญเพื่อใช้สิทธิทางศาลได้ และรัฐธรรมนูญ มาตรา 213 บัญญัติให้บุคคลซึ่งถูกละเมิดสิทธิหรือเสรีภาพที่รัฐธรรมนูญคุ้มครองมีสิทธิยื่นคำร้องต่อศาลรัฐธรรมนูญเพื่อให้ศาลมีคำวินิจฉัยว่า การกระทำนั้นขัดหรือแย้งกับรัฐธรรมนูญได้

5. การใช้อำนาจหน้าที่ของสำนักข่าวกรองแห่งชาติในการได้มาซึ่งข้อมูลหรือเอกสารตามกฎหมายนี้ อาจจะนำไปสู่

1) การขอให้ศาลรัฐธรรมนูญพิจารณาความชอบด้วยรัฐธรรมนูญของพระราชบัญญัติข่าวกรองแห่งชาติ ตามพระราชบัญญัติประกอบรัฐธรรมนูญว่าด้วยวิธีพิจารณาของศาลรัฐธรรมนูญ พ.ศ.2561 มาตรา 41 และมาตรา 7 (1)

2) การยื่นคำร้องต่อศาลรัฐธรรมนูญโดยบุคคลผู้ถูกละเมิดสิทธิเสรีภาพตามที่รัฐธรรมนูญคุ้มครอง เพื่อขอให้ศาลวินิจฉัยว่า มีการกระทำที่ขัดหรือแย้งต่อรัฐธรรมนูญหรือ พ.ร.บ.ข่าวกรองแห่งชาติฉบับใหม่นี้ขัดหรือแย้งกับรัฐธรรมนูญ ตามพระราชบัญญัติประกอบรัฐธรรมนูญว่าด้วยวิธีพิจารณาของศาลรัฐธรรมนูญ มาตรา 46 และมาตรา 48 ทั้งนี้ เป็นไปตามหลักเกณฑ์และขั้นตอนที่กฎหมายกำหนดไว้

ภายใต้ข้อสังเกตที่กล่าวมาเราจะเห็นได้ว่าภายใต้กฎหมายฉบับนี้ มีการให้อำนาจตามกฎหมายของรัฐที่จะเข้ามาล่วงละเมิดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลเป็นอย่างมาก ภายใต้เงื่อนไขของการอ้างประโยชนสาธารณะเช่นเดียวกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ฯ นั่นเอง

3) กฎหมายฉบับอื่น ๆ

นอกจากกฎหมาย 2 ฉบับ คือพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 และพระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ.2562 ที่ได้กล่าวมา ยังมีกฎหมายอีกหลายฉบับที่มีบทบัญญัติให้อำนาจรัฐที่จะล่วงละเมิดข้อมูลส่วนบุคคลได้ โดยอาศัยการอ้างอิงประโยชน์สาธารณะ ยกตัวอย่างเช่น

(1) พระราชบัญญัติป้องกันและปราบปรามยาเสพติดให้โทษ พ.ศ.2519

ใน พระราชบัญญัติฉบับนี้ มาตราที่ 14 จัตวา บัญญัติว่า ในกรณีที่มีเหตุอันควรเชื่อได้ว่า เอกสารหรือข้อมูลข่าวสารอื่นใด ซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์หรือสื่อทางเทคโนโลยีสารสนเทศใด ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดเกี่ยวกับยาเสพติด เจ้าพนักงานซึ่งได้รับอนุมัติจากเลขาธิการเป็นหนังสือจะยื่นคำขอฝ่ายเดียวต่ออธิบดีผู้พิพากษาศาลอาญาเพื่อมีคำสั่งอนุญาตให้เจ้าพนักงานได้มาซึ่งข้อมูลข่าวสารดังกล่าวได้

ตาม พระราชบัญญัติฉบับนี้ ถูกใช้ในการหาข้อมูลข่าวสารที่ “เชื่อได้ว่า” ถูกใช้ในการค้ายาเสพติด สามารถได้มาซึ่งข้อมูลที่เกี่ยวข้องกับยาเสพติด และไม่มีวิธีการอื่นใดเหมาะสม ก็สามารถเลือกใช้เปิดทางให้บังคับใช้กฎหมายข้อนี้ได้ แต่ใน พระราชบัญญัติเดียวกันนี้ พอที่จะมีการควบคุมไม่ให้ข้อมูลที่ได้มารั่วไหลออกไปโดย

มาตรา 16/1 ผู้ใดรู้หรือได้มาซึ่งข้อมูลข่าวสารที่ได้มาตามมาตรา 14 จัตวา กระทำด้วยประการใด ๆ ให้ผู้อื่นรู้หรืออาจรู้ข้อมูลข่าวสารดังกล่าว ต้องระวางโทษจำคุกไม่เกินห้าปีหรือปรับไม่เกินหนึ่งแสนบาท เว้นแต่เป็นการเปิดเผยในการปฏิบัติหน้าที่หรือตามกฎหมาย

(2) พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ.2542

โดย พระราชบัญญัติฉบับนี้ มาตราที่ 46 บัญญัติไว้ว่า ในกรณีที่มีพยานหลักฐานตามสมควรว่าบัญชีลูกค้าของสถาบันการเงิน เครื่องมือหรืออุปกรณ์ในการสื่อสาร หรือเครื่องคอมพิวเตอร์ใด ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดฐานฟอกเงิน พนักงานเจ้าหน้าที่ซึ่งเลขาธิการมอบหมายเป็นหนังสือจะยื่นคำขอฝ่ายเดียวต่อศาลแพ่ง เพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่เข้าถึงบัญชีข้อมูลทางการสื่อสารหรือ ข้อมูลคอมพิวเตอร์เพื่อให้ได้มาซึ่งข้อมูลดังกล่าวนั้นก็ได้

(3) พระราชกำหนดการบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ.2548

เมื่อวันที่ 11 กรกฎาคม พ.ศ.2548 ได้มีการประกาศใช้ พระราชกำหนดการบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ.2548 ซึ่งได้มีการระบุเหตุผลด้านความมั่นคง ให้สามารถล้วงข้อมูลได้เช่นกัน โดยระบุไว้ใน มาตรา 11 (5) กล่าวคือ ประกาศให้พนักงานเจ้าหน้าที่มีอำนาจออกคำสั่งตรวจสอบจดหมาย หนังสือ สิ่งพิมพ์ โทรเลข โทรศัพท์หรือการสื่อสารด้วยวิธีการอื่นใด ตลอดจนการสั่งระงับหรือยับยั้งการติดต่อ หรือ การสื่อสารใด เพื่อป้องกันหรือระงับเหตุการณ์ร้ายแรง โดยต้องปฏิบัติตามหลักเกณฑ์ที่กำหนดไว้ในกฎหมายว่าด้วยการสอบสวนคดีพิเศษโดยอนุโลม

แต่ทว่าในพระราชกำหนด มิได้เอ่ยถึงการดำเนินการป้องกัน หรือปกป้องข้อมูล กรณีเมื่อข้อมูลที่ได้มาหลุดออกมาสู่ภายนอกแต่อย่างใด

(4) พระราชบัญญัติป้องกันและปราบปรามการค้ามนุษย์ พ.ศ.2551

มีการบัญญัติไว้ใน มาตรา 30 ว่า ในกรณีที่มีเหตุอันควรเชื่อได้ว่าเอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือหรืออุปกรณ์ในการสื่อสารสื่ออิเล็กทรอนิกส์หรือสื่อสารสนเทศอื่นใด ถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิดฐานค้ามนุษย์ พนักงานเจ้าหน้าที่ซึ่งได้รับอนุมัติเป็นหนังสือจากผู้บัญชาการตำรวจแห่งชาติ อธิบดีกรมสอบสวนคดีพิเศษ หรือผู้ว่าราชการจังหวัด แล้วแต่กรณี จะยื่นคำขอฝ่ายเดียวต่อศาลอาญาหรือศาลจังหวัดที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ได้มาซึ่งเอกสาร หรือข้อมูลข่าวสารดังกล่าวก็ได้ ทั้งนี้ ตามหลักเกณฑ์และวิธีการที่กำหนดในข้อบังคับประธานศาลฎีกา

โดยใน พระราชบัญญัติฉบับนี้ ระบุเหตุผลไว้ว่า สามารถบังคับใช้มาตรา 30 เมื่อเชื่อได้ว่า มีความผิดฐานการค้ามนุษย์ เชื่อว่าจะได้มาซึ่งข้อมูลที่เกี่ยวข้องกับการค้ามนุษย์ และไม่มีทางเลือกอื่นใดในการได้มาซึ่งข้อมูลดังกล่าวแล้ว

(5) พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ.2556

ในมาตรา 17 บัญญัติไว้ว่า ในกรณีที่มีเหตุอันควรเชื่อว่า เอกสารหรือข้อมูลข่าวสารซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีใด ถูกใช้หรืออาจถูกใช้ เพื่อให้ได้รับประโยชน์จากการกระทำความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พนักงานสอบสวนซึ่งได้รับอนุมัติจากอัยการสูงสุด ผู้บัญชาการตำรวจแห่งชาติ หรือผู้ซึ่งได้รับมอบหมาย แล้วแต่กรณี อาจยื่นคำขอฝ่ายเดียวต่ออธิบดีผู้พิพากษาศาลอาญาเพื่อมีคำสั่งอนุญาตให้ได้มาซึ่งเอกสารหรือข้อมูลข่าวสารดังกล่าวก็ได้

โดยใน พระราชบัญญัติ ฉบับนี้ ระบุไว้ตอนท้ายของมาตรา 17 ไว้คล้ายกับ พ.ร.บ.ป้องกันและปราบปรามการค้ามนุษย์ ปี 2551 เช่นกันคือ จะบังคับใช้เมื่อเชื่อว่ามีการกระทำที่เกี่ยวข้องกับการกระทำความผิด เชื่อว่าจะทำให้ได้มาซึ่งข้อมูลที่เกี่ยวข้องกับการกระทำความผิด และไม่มีวิธีการอื่นใดที่ให้ได้มาซึ่งข้อมูลดังกล่าวแล้ว

(6) พระราชบัญญัติประกอบรัฐธรรมนูญว่าด้วยการป้องกันและปราบปรามการทุจริต พ.ศ.2561

มาตรา 34 ในการปฏิบัติหน้าที่ตามพระราชบัญญัติประกอบรัฐธรรมนูญนี้ ให้คณะกรรมการ ป.ป.ช. มีอำนาจ

(1) มีคำ สั่งให้ข้าราชการ พนักงาน หรือลูกจ้างของหน่วยราชการ หน่วยงานของรัฐรัฐวิสาหกิจ หรือราชการส่วนท้องถิ่น มาให้ถ้อยคำหรือส่งมอบเอกสารหรือหลักฐานที่เกี่ยวข้องมาเพื่อประโยชน์ในการไต่สวน

(2) ให้บุคคลใดมาให้ถ้อยคำ หรือส่งบัญชี เอกสาร หรือหลักฐานใด ๆ มาเพื่อประโยชน์ในการไต่สวน

มาตรา 38 ในกรณีที่คณะกรรมการ ป.ป.ช. ดำเนินการตรวจสอบหรือไต่สวนเพื่อมีความเห็นหรือวินิจฉัยเกี่ยวกับการกระทำของบุคคลใด และมีความจำเป็นต้องได้ข้อมูลเกี่ยวกับธุรกรรมทางการเงินของบุคคลนั้นหรือบุคคลที่เกี่ยวข้อง ให้คณะกรรมการ ป.ป.ช. มีอำนาจขอข้อมูลดังกล่าวจากสำนักงานป้องกันและปราบปรามการฟอกเงินได้ตามที่จำเป็น และให้สำนักงานป้องกันและปราบปรามการฟอกเงินส่งมอบข้อมูลดังกล่าวให้คณะกรรมการ ป.ป.ช. และให้ถือว่าการส่งมอบดังกล่าวเป็นการดำเนินการที่ชอบด้วยกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงินแล้ว

จากบทบัญญัติกฎหมายต่าง ๆ ที่กล่าวมาข้างต้น ก็เป็นกฎหมายที่เกี่ยวกับประโยชน์สาธารณะอันจะเป็นเหตุผลให้แม้ว่าเราจะมีการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลแล้วก็ตาม แต่สิทธิเหล่านี้ของปัจจเจกชนก็อาจถูกอ้างประโยชน์สาธารณะมาเป็นข้อยกเว้นเพื่อล่วงละเมิดข้อมูลส่วนบุคคลโดยภาครัฐได้ ซึ่งเป็นไปตามหลักการของมาตรา 4 ที่กำหนดว่าพระราชบัญญัตินี้ไม่ใช้บังคับแก่ (2) การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์ และ (5) การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดีการบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

ซึ่งหลักการนี้ เป็นประเด็นในการให้อำนาจรัฐโดยองค์กร หน่วยงาน หรือเจ้าหน้าที่ต่าง ๆ ตามกฎหมายที่ได้กล่าวมา ไม่ว่าจะเป็น ป.ป.ช., ปปง. หรือพนักงานสอบสวน เข้าไปล่วงละเมิดสิทธิในข้อมูลส่วนบุคคล ไม่ว่าจะเป็นการดำเนินการในลักษณะของการเก็บรวมรวม ใช้ หรือเปิดเผย เพื่อประโยชน์ในการดำเนินการตามวัตถุประสงค์ตามภารกิจของตน

แต่อย่างไรก็ดี เมื่อองค์กร หน่วยงาน หรือเจ้าหน้าที่ได้ดำเนินการกับข้อมูลส่วนบุคคลจนเสร็จสิ้นหรือจบภารกิจเกี่ยวกับข้อมูลนั้นแล้ว ไม่ว่าจะเป็นกรณีการสอบสวนหรือไต่ส่วนหรือรวบรวมพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลเสร็จสิ้น การบริหารจัดการข้อมูลส่วนบุคคลที่ได้รับมาควรจะต้องดำเนินการอย่างไรต่อ ในเรื่องนี้เห็นว่า กฎหมายฉบับต่าง ๆ ที่ได้กล่าวมาไม่ได้มีการบัญญัติถึงหลักการไว้โดยอาจจะมีระเบียบภายในองค์กร หรือหน่วยงาน อันมีฐานะเป็นกฎหมายลำดับรองกำหนดวิธีการในการบริหารจัดการข้อมูลส่วนบุคคลที่ได้รับมานั้น แต่ต้องไม่ลืมว่า

กฎหมายลำดับรองต่าง ๆ ไม่ได้มีฐานะเทียบเท่ากับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในฐานะที่เป็นกฎหมายกลางกำหนดหลักการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล และต้องอยู่ภายใต้บังคับพระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ.2540 ที่วางหลักการควบคุมข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานรัฐ

ดังนั้น ในการบริหารจัดการข้อมูลส่วนบุคคลที่ได้รับมาองค์กร หน่วยงาน หรือเจ้าหน้าที่ตามกฎหมายที่ได้กล่าวมา จึงจำเป็นจะต้องตระหนักและดำเนินการให้เป็นไปตามเจตนารมณ์ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ในฐานะที่เป็นบทกฎหมายทั่วไปนั่นเอง โดยควรมีการกำหนดนโยบายการปกป้องข้อมูลส่วนบุคคลและจัดทำระบบบริหารจัดการเพื่อการปกป้องข้อมูลส่วนบุคคลด้วย เพื่อเป็นการส่งเสริมให้มาตรฐานของการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลมีประสิทธิภาพมากยิ่งขึ้นอันจะเป็นประโยชน์ต่อสิทธิเสรีภาพของประชาชนในภาพรวม

5.2 วิเคราะห์มาตรการคุ้มครองข้อมูลส่วนบุคคลภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และกฎหมายอื่นที่เกี่ยวข้อง

ในหัวข้อนี้จะได้แยกวิเคราะห์ออกเป็น 2 ส่วนคือ มาตรการคุ้มครองข้อมูลส่วนบุคคลภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และมาตรการคุ้มครองตามกฎหมายอื่นที่เกี่ยวข้อง โดยจะได้พิจารณาเปรียบเทียบกับหลักการคุ้มครองตามกติกาสากลดังจะได้กล่าวต่อไปนี้คือ

5.2.1 วิเคราะห์มาตรการคุ้มครองข้อมูลส่วนบุคคลภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

หลักกฎหมายคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลไม่ว่าของ OECD, GDPR หรือกฎหมายของต่างประเทศนั้น จะประกอบด้วยหลักการต่าง ๆ มากมาย ดังนั้นในการวิเคราะห์จึงจะได้นำหลักการสำคัญของกฎหมายคุ้มครองข้อมูลมาเป็นเกณฑ์ในการพิจารณา โดยจะถือหลักกฎหมายของ General Data Protection Regulation หรือ GDPR มาเป็นเกณฑ์หลักในการวิเคราะห์เปรียบเทียบ โดยในส่วนของมาตรการในการควบคุมการประมวลผลข้อมูลส่วนบุคคลนั้นอาจแสดงผลการเปรียบเทียบได้ดังตารางต่อไปนี้

ตารางที่ 5.5 เปรียบเทียบหลักการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ตาม GDPR และ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

หลักการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล	**GDPR**	**พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562**
หลักการประมวลข้อมูลต้องหลักความชอบด้วยกฎหมาย เป็นธรรม และโปร่งใส (Lawfulness, Fairness and Transparency)	การประมวลข้อมูลส่วนบุคคลต้องชอบด้วยกฎหมาย เป็นธรรมและโปร่งใส (Article 5 (1) (a))	การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล จะกระทำไม่ได้หากเจ้าของข้อมูลไม่ได้ให้ความยินยอม หรือมีอำนาจกระทำได้ตามกฎหมาย โดยการขอความยินยอมจะต้องดำเนินการอย่างโปร่งในและเป็นธรรม (มาตรา 19)
หลักวัตถุประสงค์ที่จำกัด (Purpose Limitation)	ข้อมูลส่วนบุคคลจะถูกเก็บได้เฉพาะเพื่อวัตถุประสงค์ที่ชัดแจ้งและชอบด้วยกฎหมาย และจะต้องไม่ถูก ประมวลในลักษณะที่ไม่สอดคล้องกับวัตถุประสงค์ (Article 5 (1) (b)) ยกเว้นกรณีเพื่อประโยชน์สาธารณะ เพื่อวัตถุประสงค์ทางประวัติศาสตร์ วิทยาศาสตร์ หรือสถิติตาม (Article 89 (1))	การเก็บรวบรวมข้อมูลส่วนบุคคลจะเก็บได้เท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมาย (มาตรา 22) โดยมีข้อยกเว้นเพื่อประโยชน์สาธารณะ วัตถุประสงค์ทางประวัติศาสตร์ การศึกษาวิจัย หรือสถิติ (มาตรา 24)
หลักการประมวลข้อมูลที่น้อยที่สุด (Data Minimization) ข้อมูลส่วนบุคคลนั้นจะมีได้เท่าที่เพียงพอ (Adequate) เกี่ยวข้อง และจำกัดเฉพาะ	การประมวลข้อมูลส่วนบุคคลต้องอยู่ภายใต้เงื่อนไขความเพียงพอ ความเกี่ยวข้อง และต้องจำกัดเฉพาะเท่าที่จำเป็นบรรลุวัตถุประสงค์ของการประมวลข้อมูลนั้น (Article 5 (1)	การเก็บรวบรวมข้อมูลให้เก็บรวบรวมได้เท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมาย (มาตรา 21)

ตารางที่ 5.5 (ต่อ)

หลักการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล	GDPR	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562
สิ่งที่จำเป็นตามวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลเท่านั้น	(c))	
หลักความถูกต้อง (Accuracy)	ข้อมูลส่วนบุคคลจะต้องมีความถูกต้อง และเป็นปัจจุบัน (Accurate and Up to Date) ส่วนข้อมูลที่ไม่ ถูกต้องจะต้องถูกลบหรือแก้ไขโดยไม่ชักช้า (Article 5 (1) (d))	ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด (มาตรา 35)
หลักการเก็บข้อมูล (Data Retention) หรือหลักการเก็บข้อมูลอย่างจำกัด (Storage Limitation)	ข้อมูลส่วนบุคคลจะต้องไม่เก็บไว้ในลักษณะที่อาจทำให้ระบุตัวเจ้าของ ข้อมูลได้ และในระยะเวลาเกินความจำเป็นตามวัตถุประสงค์ของการประมวลข้อมูลนั้น (Article 5 (1) (e)) ยกเว้นกรณีเพื่อประโยชน์สาธารณะ เพื่อวัตถุประสงค์ทางประวัติศาสตร์ วิทยาศาสตร์ หรือสถิติตาม (Article 89 (1))	เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวเจ้าของข้อมูลได้ ในกรณีหมดความจำเป็นในการเก็บรักษาตามวัตถุประสงค์ (มาตรา 33)
หลักความเชื่อถือได้และการรักษาความลับ (Integrity and Confidentiality) หรือหลักความปลอดภัยของข้อมูล (Data Security)	ข้อมูลส่วนบุคคลต้องมีความปลอดภัย โดยมีการป้องกันจากการประมวลข้อมูลโดยปราศจากอำนาจ รวมถึงป้องกันการสูญหายหรือถูกทำลายจากอุบัติเหตุ โดยจะต้องใช้	กำหนดหน้าที่ไว้ตามมาตรา 37 แก่ผู้ควบคุมข้อมูล และ มาตรา 40 (2) แก่ผู้ประมวลผลข้อมูล

ตารางที่ 5.5 (ต่อ)

หลักการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล	GDPR	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562
	มาตรการทางเทคโนโลยีและมาตรการเชิงองค์กรที่เหมาะสม (Article 5(1)(f), 24(1), 25(1)–(2), 28, 39, 32)	
หลักความรับผิดชอบ (Accountability)	ผู้ควบคุมข้อมูลส่วนบุคคลมีภาระความรับผิดชอบที่จะต้องแสดงให้เห็นว่าตนสามารถปฏิบัติตามหลักการคุ้มครองข้อมูลตาม GDPR	ไม่ชัดเจน มีเพียงการกำหนดโทษในกรณีฝ่าฝืน

จากหลักการที่ได้ยกมาเปรียบเทียบดังตาราง แสดงให้เห็นชัดเจนว่า หลักการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยนั้นมีมาตรฐานไม่แตกต่างไปจากหลักการของกติการะหว่างประเทศแต่อย่างใด

นอกจากนี้ยังมีมาตรการสำคัญอีกประเด็นหนึ่งก็คือ มาตรการในการคุ้มครองข้อมูลส่วนบุคคลในกรณีข้อมูลรั่วไหล โดยภายใต้สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนั้น การคุ้มครองข้อมูลส่วนบุคคลให้มีความปลอดภัยจากการล่วงละเมิดนั้น เป็นหน้าที่ในประการสำคัญของทั้งผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่ต้องปฏิบัติภายใต้หลักความเชื่อถือได้และการรักษาความลับ (Integrity and Confidentiality) หรือ หลักความปลอดภัยของข้อมูล (Data Security) ที่ถูกกำหนดไว้ทั้งในกรอบ OECD, GDPR, กฎหมายต่างประเทศและรวมถึงพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยด้วย

ทั้งนี้เพราะการรั่วไหลของข้อมูลส่วนบุคคลเป็นปัญหาที่สำคัญอันส่งผลกระทบทั้งความเป็นอยู่ส่วนตัวของเจ้าของข้อมูล ตลอดจนส่งผลกระทบในทางธุรกิจและเศรษฐกิจของประเทศ โดยการรั่วไหลของข้อมูลอาจจะเกิดจากการละเมิดในรูปแบบดังนี้

ประการแรก เป็นการละเมิดความพร้อมใช้ของข้อมูล (Availability Breach) โดยมีลักษณะเป็นการทำลายข้อมูลส่วนบุคคลที่ไม่ไปเป็นตามกฎหมายหรือเกิดเหตุสุดวิสัย อันทำให้ข้อมูลเสียหาย

ประการที่สอง เป็นการละเมิดความครบถ้วนสมบรูณ์ของข้อมูล (Integrity Breach) การเปลี่ยนแปลงข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย

ประการสุดท้าย เป็นการละเมิดความลับของข้อมูล (Confidentiality Breach) การเปิดเผยหรือเข้าถึงโดยไม่มีสิทธิของข้อมูลส่วนบุคคล

เมื่อพิจารณาถึงกฎหมายคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลที่มีการกำหนดมาตรการและกลไกเพื่อรับมือในปัญหาเรื่องนี้ คณาธิป ทองรวีวงศ์ ได้ทำการศึกษาและแบ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดหน้าที่และความรับผิดของผู้ควบคุมข้อมูล (Data Controller) ที่เกี่ยวข้องกับกรณีข้อมูลรั่วไหล โดยจำแนกหลักกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลและหน้าที่ของผู้ควบคุมข้อมูลออกเป็นสองขั้นตอนได้ดังนี้[284]

1. ขั้นตอนก่อนการรั่วไหลของข้อมูล

ในช่วงก่อนที่จะเกิดการรั่วไหลของข้อมูล แต่ข้อมูลอาจอยู่ในสภาพแวดล้อมหรืออยู่ในการควบคุมดูแลที่มีความเสี่ยง ความเปราะบาง ต่อการรั่วไหลอันอาจเกิดขึ้นจึงนำไปสู่ประเด็นทางกฎหมายที่จะต้องพิจารณาว่า กฎหมายเข้ามาเกี่ยวข้องกับการป้องกัน ในช่วงระยะเวลาก่อนการรั่วไหลของข้อมูลอย่างไร กฎหมายจะกำหนดหน้าที่และความรับผิดสำหรับบุคคลที่เกี่ยวข้องกับการเก็บรักษาข้อมูลอย่างไร

2. ขั้นตอนหลังการรั่วไหลของข้อมูล

การรั่วไหลของข้อมูลอาจนำไปสู่อาชญากรรม ประเภทต่าง ๆ เช่น การโจรกรรมข้อมูลเชิงเอกลักษณ์ การฉ้อโกงหลอกลวงทางอินเทอร์เน็ต ฯลฯ จึงมีประเด็นทางกฎหมายว่า กฎหมายจะกำหนดมาตรการในการป้องกันก่อนเกิดอาชญากรรมที่กระทำต่อข้อมูลนั้นอย่างไร จะเห็นได้ว่าแม้เกิดการรั่วไหลของข้อมูลแล้ว กฎหมายยังอาจวางกลไกเชิงป้องกันอีกชั้นหนึ่ง ซึ่งไม่ใช่การป้องกันการรั่วไหล แต่เป็นการป้องกันเพื่อมิให้การรั่วไหลที่เกิดขึ้นนำไปสู่ผลกระทบอื่นต่อไปอีก

ประเด็นที่ต้องพิจารณาในประการแรกก็คือ เมื่อพิจารณาในกรณีการกำหนดมาตรการในกรณีก่อนการรั่วไหลของข้อมูลนั้น จะเห็นว่า กฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับเดิม (Directive 95/46/EC) วางหลักว่าผู้ควบคุมข้อมูลต้องจัดให้มีมาตรการทางเทคนิคและทางองค์กรสำหรับการรักษาความมั่นคง ปลอดภัยอย่างเหมาะสมเพื่อป้องกันข้อมูลส่วนบุคคลจากการถูกทำลาย หรือสูญเสีย หรือถูกแก้ไข เปลี่ยนแปลง โดยอุบัติเหตุหรือโดยมิชอบการเข้าถึงและการเปิดเผยข้อมูลโดยปราศจากอำนาจ (Directive 95/46/EC Article.17(1)) ต่อมาเมื่อมีการประกาศใช้ General Data Protection Regulation ก็ได้มีการแก้ไขปรับปรุงหลักการ โดยได้วางหลักเกี่ยวกับความปลอดภัยใน

---

[284] คณาธิป ทองรวีวงศ์, **รายงานการวิจัยฉบับสมบูรณ์ เรื่องการปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน**, หน้า 274.

การประมวลข้อมูลส่วนบุคคล (Security of Processing) โดยกำหนดหน้าที่ของผู้กระทำการเกี่ยวข้องกับข้อมูลส่วนบุคคล (Article 32) ดังนี้[285]

1. ผู้ควบคุมข้อมูล (Data Controller) และผู้ประมวลข้อมูล (Data Processor) จะต้องจัดให้มีมาตรการทางเทคนิคและมาตรการทางองค์กร (Technical and Organizational Measure) ที่เหมาะสมในการรักษาระดับความมั่นคงปลอดภัยเพื่อป้องกันความเสี่ยง ซึ่งรวมถึง การเข้ารหัสข้อมูล (Encryption) ความสามารถในการรักษาความลับ บูรณภาพ ความพร้อมใช้ (Confidentiality, Integrity and Availability) ในการประมวลผลและบริการ ความสามารถในการแก้ไขความพร้อมใช้และการเข้าถึงข้อมูล ในเวลาอันสมควรสำหรับกรณีที่เกิดเหตุการณ์ทางกายภาพหรือทางเทคนิค กระบวนการในการทดสอบอย่าง สม่ำเสมอ เกี่ยวกับประสิทธิภาพของมาตรการทางเทคนิคหรือมาตรการทางองค์กรเพื่อให้มั่นใจในความ ปลอดภัยของการประมวลข้อมูล

2. ในการประเมินความเหมาะสมของระดับการรักษาความปลอดภัย นั้นจะต้องนำปัจจัยต่างเกี่ยวกับความเสี่ยงมาพิจารณา เช่น การถูกทำลาย หรือ สูญเสีย หรือถูกแก้ไข เปลี่ยนแปลง โดยอุบัติเหตุหรือโดยมิชอบ การเข้าถึง และการเปิดเผยโดยปราศจากอำนาจซึ่งข้อมูลที่ส่งหรือเก็บรักษาไว้

3. ผู้ควบคุมข้อมูลและผู้ประมวลข้อมูลต้องดำเนินการเพื่อทำให้มั่นใจ ว่าบุคคลธรรมดาที่กระทำการที่มีอำนาจกระทำการเกี่ยวกับการประมวลข้อมูลนั้นจะไม่ทำการประมวล ข้อมูลเว้นแต่เป็นการกระทำตามคำสั่งของผู้ควบคุมข้อมูล

นอกจากนี้ จะเห็นว่าในประเด็นนี้ กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศอังกฤษก็ได้กำหนดหลักการไว้ในทำนองเดียวกัน โดย Data Protection Act ได้กำหนดว่า[286]

1. ต้องจัดให้มีมาตรการที่เหมาะสมตามลักษณะของข้อมูลนั้น ในการป้องกันภัยอันอาจเกิดจากการประมวลข้อมูลโดยปราศจากอำนาจหรือไม่ชอบด้วยกฎหมาย การสูญเสีย การทำลาย หรือเสียหายโดยอุบัติเหตุ

2. ในกรณีที่การประมวลข้อมูลทำขึ้นโดยผู้ประมวลข้อมูลที่กระทำในนามผู้ควบคุมข้อมูล ผู้ควบคุมข้อมูลต้องเลือกผู้ประมวลข้อมูลที่สามารถให้การรับรองถึงมาตรการความปลอดภัยที่เพียงพอในการประมวลข้อมูล และ ใช้วิธีการที่สมเหตุผลในการดำเนินการให้สอดคล้องกับมาตรการดังกล่าว

3. ในกรณีที่การประมวลข้อมูลส่วนบุคคลกระทำโดยผู้ประมวลข้อมูล ที่กระทำในนามผู้ควบคุมข้อมูลผู้ควบคุมข้อมูลจะต้องจัดให้การประมวลข้อมูลนั้นกระทำภายใต้สัญญา ซึ่งทำเป็นลายลักษณ์อักษร และกำหนดให้ผู้ประมวลข้อมูลต้องกระทำการตามคำสั่งของผู้ควบคุมข้อมูล นอกจากนี้

---

[285] *เรื่องเดียวกัน*, หน้า 275.

[286] *เรื่องเดียวกัน*.

สัญญาดังกล่าวต้องกำหนดให้ผู้ประมวลข้อมูลต้องดำเนินการให้สอดคล้องกับหน้าที่ซึ่งเทียบเท่า กับหน้าที่ของผู้ควบคุมข้อมูลที่กฎหมายนี้กำหนดไว้

เช่นเดียวกับหลักการของประเทศมาเลเซีย ก็ได้มีการกำหนดหลักคุ้มครองข้อมูลส่วนบุคคลในเรื่องนี้ไว้ตาม PERSONAL DATA PROTECTION ACT 2010 มาตรา 9 กล่าวคือ[287]

1. ผู้ใช้ข้อมูลส่วนบุคคล ต้องดำเนินขั้นตอนเพื่อปกป้องข้อมูลจากการสูญหาย การใช้ในทางที่มิชอบ การแก้ไขเปลี่ยนแปลง การเข้าถึง เปิดเผย แก้ไขหรือทำลายโดยปราศจากอำนาจ ทั้งนี้จะต้องนำปัจจัยต่าง ๆ มาพิจารณาด้วย เช่น ลักษณะของข้อมูลส่วนบุคคลและผลกระทบอันอาจเกิดจากการสูญหาย ใช้ในทางที่มิชอบ การแก้ไขเปลี่ยนแปลง การเข้าถึง เปิดเผย แก้ไข หรือทำลาย โดยปราศจากอำนาจ สถานที่หรือที่ตั้งซึ่งข้อมูลส่วนบุคคลนั้นถูกเก็บรักษาไว้ มาตรการรักษา ความปลอดภัยที่เกี่ยวข้องกับอุปกรณ์เก็บข้อมูลนั้น มาตรการที่นำมาใช้เพื่อทำให้เกิดความเชื่อถือในข้อมูลบูรณภาพ และความสามารถในการเข้าถึงข้อมูลนั้น และมาตรการที่ใช้เพื่อความปลอดภัยในการโอนหรือส่งต่อข้อมูลนั้น

2. ในกรณีที่ข้อมูลส่วนบุคคลถูกประมวลโดยผู้ประมวลข้อมูลที่กระทำในนามผู้ใช้ข้อมูล ผู้ใช้ข้อมูลต้องทำให้มั่นใจว่าผู้ประมวลข้อมูลจัดให้มีมาตรการที่เพียงพอทั้งมาตรการทางเทคนิคและมาตรการเชิงองค์กรในการรักษาความปลอดภัยในการประมวลข้อมูลนั้น และ ดำเนินการตามขั้นตอนเพื่อให้สอดคล้องกับมาตรการเพื่อความปลอดภัยดังกล่าว

สำหรับประเทศไทย ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ได้มีการกำหนดหลักการนี้ไว้ในบทบัญญัติมาตรา 37 (1) และ (2) โดยกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ดังต่อไปนี้

1. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบด้วย และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อมีเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม

2. ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโยปราศจากอำนาจหรือโดยมิชอบ

เห็นได้ว่า หลักการคุ้มครองก่อนเกิดเหตุข้อมูลรั่วไหลที่กล่าวมานั้น กฎหมายที่ กำหนดมาตรการหรือกลไกในเชิงป้องกันคือ การวางหลักกำหนดหน้าที่ให้ผู้ควบคุมข้อมูลต้องจัดให้มีมาตรการรักษาความปลอดภัยของข้อมูล อย่างไรก็ตาม มาตรการรักษาความปลอดภัยแต่เพียงอย่าง

---

[287] *เรื่องเดียวกัน*, หน้า 277.

เดียวยังอาจไม่เพียงพอ ทั้งนี้จะเห็นได้ว่ารูปแบบของการละเมิดโดยเฉพาะอย่างยิ่งกรณีของอาชญากรรมคอมพิวเตอร์ได้มีการพัฒนาเทคนิควิธีการและสามารถทำให้เกิดการรั่วไหลแม้แต่ในองค์กรขนาดใหญ่หรือประเทศที่เจริญแล้วก็อาจถูกละเมิดได้ตลอดเวลา ซึ่งหากพิจารณาหลักการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Principles) จะเห็นว่ามีหลักการคุ้มครองข้อมูลส่วนบุคคลประการอื่นที่อาจนำมาใช้ในขั้นตอนก่อนการรั่วไหลของข้อมูลอีกด้วย เช่น หลักเกี่ยวกับการจัดเก็บข้อมูลเท่าที่จำเป็น (Necessity) หรือหลักการจัดเก็บข้อมูลที่น้อยที่สุด (Data Minimization) ซึ่งปรากฏโดดเด่นใน General Data Protection สหภาพยุโรป สำหรับประเทศไทยเองก็มีการบัญญัติรับรองหลักการนี้ไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล เช่นเดียวกัน

อย่างไรก็ดี ใน General Data Protection มีการกำหนดหลักการให้ผู้ควบคุมข้อมูลควรพิจารณาเลือกจัดเก็บข้อมูลเท่าที่จำเป็นตามวัตถุประสงค์ของการใช้ที่แจ้งให้กับเจ้าของข้อมูลทราบ โดยไม่ควรเก็บข้อมูลมากเกินไป (Excessive) โดยจะมีการกำหนดหน้าที่ให้ผู้ควบคุมข้อมูลมีหน้าที่บูรณาการหลักการคุ้มครองข้อมูลทั้งในขั้นวางแผนและขั้นปฏิบัติการ (Privacy by Design หรือ Data Protection by Design)

หลักการ Privacy by Design คือ ฝ่ายผู้ควบคุมข้อมูลต้องคำนึงถึงสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลตั้งแต่ขั้นออกแบบ คงไว้ตลอดกระบวนการที่ตามมา ซึ่งสามารถประยุกต์ใช้ได้ทั้งในบริบทของการพัฒนาระบบ ผลิตภัณฑ์ บริการ แผนธุรกิจ ฯลฯ โดยเรื่อง Privacy by Design นี้มีอยู่ในกระบวนการทางวิศวกรรมบางสาขาและปฏิบัติกันมานานพอสมควรแล้ว แต่ไม่เคยมีการบัญญัติไว้เป็นกฎหมายแน่ชัดมาก่อนจนกระทั่งกฎหมาย GDPR มีผลบังคับใช้ แม้ GDPR ไม่ได้กล่าวถึงหน้าที่ผู้ประมวลผลข้อมูลในหลักการ Privacy by Design อย่างแน่ชัด แต่ก็มีการระบุว่าผู้ควบคุมข้อมูลต้องเลือกผู้ประมวลผลข้อมูลที่ปฏิบัติตามมาตรการทางเทคนิคและทางการจัดการองค์กรที่เหมาะสมและเพียงพอต่อการคุ้มครองความเป็นส่วนตัวของเจ้าของข้อมูล และเมื่อกล่าวถึง Privacy by Design นักพัฒนาระบบจำนวนมากมักอ้างอิงถึงหลักการพื้นฐาน 7 ประการ ดังนี้[288]

ประการแรก กันไว้ดีกว่าแก้ (Proactive not Reactive; Preventative not Remedial) ผู้ออกแบบต้องป้องกันมากกว่าแก้ไข คือ คาดคะเนถึงเหตุการณ์ที่ไม่พึงประสงค์และสุ่มเสี่ยงต่อความเป็นส่วนตัวของผู้ใช้ แล้วดำเนินมาตรการการป้องกันไว้ก่อนที่จะเกิดขึ้นจริง เริ่มต้นจากการตระหนักถึงคุณประโยชน์ของการปฏิบัติตามนโยบายความเป็นส่วนตัวที่เข้มข้น ยึดมั่นในการใช้มาตรการสูงสุดในการคุ้มครองความเป็นส่วนตัว

---

[288] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.), **กฎหมาย GDPR ฉบับรวบรัด,** ค้นวันที่ 25 เมษายน 2562 จาก https://www.etda.or.th/content/gdpr-in-a-nutshell?fbclid=IwAR2MXf7Q1YnAjZEdX9xuz6ez7ZNWvVWcCmq9r0XMVDug2hMAG8J3HqEmwOM

ประการที่สอง ตั้งเป็นค่าตั้งต้น (Privacy as the Default Setting) การคุ้มครองข้อมูลส่วนบุคคลจะต้องเป็นไปโดยอัตโนมัติและยังคงอยู่แม้ผู้ใช้ไม่ได้กระทำการใดเพิ่มเติม หากระบุการใช้ข้อมูลส่วนบุคคลไว้ไม่ชัดเจน จะต้องใช้มาตรการคุ้มครองขั้นสูงสุดเป็นมาตรฐานตั้งต้น

ประการที่สาม ฝังอยู่ในแม่แบบ (Privacy Embedded into Design) มาตรการความเป็นส่วนตัวจะต้องรวมอยู่ในแม่แบบและสถาปัตยกรรมอย่างกลมกลืน มิใช่เพียงอุปกรณ์เสริมในภายหลังเพื่อสอดคล้องกับกฎหมาย

ประการที่สี่ ยังคงเต็มประสิทธิภาพ (Full Functionality — Positive-Sum, not Zero-Sum) นอกจากความเป็นส่วนตัวที่ออกแบบจะเป็นไปตามข้อกำหนดทางกฎหมายแล้ว จะต้องไม่ลดทอนประสิทธิภาพการทำงานของระบบ ผู้ใช้ไม่ต้องเลือกสิทธิประโยชน์ประการใดประการหนึ่งอาทิ ระหว่างความเป็นส่วนตัวกับความปลอดภัย ในขณะที่สามารถได้รับสิทธิประโยชน์ทั้งสองได้

ประการที่ห้า จากต้นจรดปลาย (End-to-End Security — Lifecycle Protection) ความเป็นส่วนตัวต้องฝังตัวอยู่ในระบบ เริ่มใช้งานตั้งแต่ก่อนเก็บข้อมูล และมีผลต่อเนื่องตลอดอายุการเก็บรักษาข้อมูล เพื่อสร้างความมั่นใจว่าข้อมูลทั้งหมดได้รับการคุ้มครองและถูกทำลายทิ้งเมื่อสิ้นสุดการใช้งาน

ประการที่หก ประจักษ์และโปร่งใส (Visibility and Transparency — Keep it Open) ผู้มีส่วนได้ส่วนเสียทุกคนจะต้องได้รับแจ้งถึงมาตรการทางธุรกิจและเทคโนโลยีที่ใช้เพื่อให้บรรลุวัตถุประสงค์ที่แจ้งไว้ และอนุญาตให้ขอตรวจสอบได้ กรรมวิธีทั้งหมดต้องโปร่งใสทั้งต่อผู้ใช้และผู้ให้บริการ

ประการสุดท้าย ผู้ใช้คือศูนย์กลาง (Respect for User Privacy — Keep it User-Centric) ผู้ออกแบบและผู้ให้บริการต้องให้ความสำคัญต่อความเป็นส่วนตัวของผู้ใช้เป็นสำคัญ โดยมีมาตรการเช่น แจ้งเตือนตามความเหมาะสม และจัดสรรตัวเลือกความเป็นส่วนตัว (Privacy Option) ที่ใช้งานง่าย

โดยหลักการ Privacy by Design เรื่องนี้เป็นประเด็นที่ไม่ได้มีการกำหนดไว้ชัดเจนในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย ซึ่งหากในอนาคตถ้ามีการแก้ไขพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ก็สมควรอย่างยิ่งที่จะมีการกำหนดหน้าที่ให้ผู้ควบคุมข้อมูลเพิ่มเติม กล่าวคือนอกจากจะต้องมีหน้าที่รักษาความปลอดภัยแก่ข้อมูลที่เก็บรักษาไว้แล้ว รวมถึงมีหน้าที่ในการการจัดเก็บข้อมูลเท่าที่จำเป็น (Necessity) แล้วจะต้องมีการบัญญัติหลักการเรื่อง Privacy by Design ไว้ในบทบัญญัติด้วย เพื่อกำหนดหน้าที่ผู้ควบคุมข้อมูลส่วนบุคคลให้มีหน้าที่ในบูรณาการหลักการคุ้มครองข้อมูลตั้งแต่ในขั้นวางแผนและขั้นปฏิบัติการ เพื่อเป็นการสร้างความมั่นใจให้แก่เจ้าของข้อมูลส่วนบุคคลว่าจะได้มีมาตรการและกลไกป้องกันข้อมูลส่วนบุคคลของเขาไม่ให้มีการรั่วไหลนั้นเอง

ประเด็นที่ต้องพิจารณาในประการต่อมาก็คือ มาตรการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในขั้นตอนหลังการรั่วไหลของข้อมูล จะเห็นในประเด็นนี้ ประเทศไทยได้นำ

หลักการแจ้งเตือนข้อมูล รั่วไหล (Data Breach Notification) ทีมีการกำหนดไว้ในหลักการสากลไม่ว่าจะเป็น GDPR หรือกฎหมายของต่างประเทศที่สำคัญมากำหนดไว้ในกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย ซึ่งหลักการสำคัญในระดับสากลในเรื่องนี้นั้น ยกตัวอย่างได้คือ

GDPR กำหนดหลักการแจ้งเตือนกรณีข้อมูลส่วนบุคคลรั่วไหล โดยกำหนดหน้าที่ให้ผู้ควบคุมข้อมูลให้ดำเนินการแจ้งเตือนเมื่อเกิดเหตุข้อมูลรั่วไหล (Breach Notification) โดยถ้าหากพบว่าข้อมูลรั่วไหล ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลต้องแจ้งให้หน่วยงานของรัฐที่กำกับดูแล และประชาชนทราบ

สำหรับในกรณีการแจ้งให้หน่วยงานของรัฐนั้นจะมีหลักสองประการคือ ประการแรก มีการกำหนดหน้าที่ของผู้ควบคุมข้อมูล (Data Controller) ว่าเมื่อมีเหตุการณ์รั่วไหลของข้อมูล ผู้ควบคุมข้อมูลต้องแจ้งเหตุรั่วไหลต่อหน่วยงาน ของรัฐที่มีอำนาจโดยไม่ชักช้า และภายในเวลาไม่เกิน 72 ชั่วโมงหลังจากทราบถึงเหตุรั่วไหล เว้นแต่การรั่วไหลนั้นอาจไม่ส่งผลในแง่ความเสี่ยงต่อสิทธิและเสรีภาพของบุคคลธรรมดา หากมิได้มีการแจ้งภายในเวลาดังกล่าวจะต้องมีการชี้แจงเหตุผลถึงความล่าช้าด้วย และประการที่สองกำหนดหน้าที่ของผู้ประมวลข้อมูล (Data Processor) โดยผู้ประมวลข้อมูลต้องแจ้งให้ผู้ควบคุมข้อมูลทราบโดยไม่ชักช้าหลังจากทราบถึงการรั่วไหลของข้อมูลส่วนบุคคล การแจ้งนั้นอย่างน้อยต้องประกอบด้วยข้อมูลต่อไปนี้ บรรยายลักษณะ ของการรั่วไหล รวมทั้งประเภทและจำนวนโดยประมาณของเจ้าของข้อมูลที่เกี่ยวข้อง แจ้งชื่อ ที่ติดต่อของ เจ้าหน้าที่คุ้มครองข้อมูลขององค์กรนั้น บรรยายถึงผลกระทบอันอาจเกิดกับข้อมูลที่รั่วไหล บรรยายถึงมาตรการที่ได้ใช้หรือจะใช้ในการตอบสนองต่อการรั่วไหล เช่น มาตรการลดผลกระทบในทางลบอันอาจเกิดขึ้น

นอกจากหน้าที่ในการแจ้งหน่วยงานของรัฐแล้ว GDPR ยังได้กำหนดหน้าที่ให้ต้องมีการแจ้งแก่เจ้าของข้อมูลด้วย กล่าวคือ เมื่อการรั่วไหลของข้อมูลอาจส่งผลให้เกิดความเสี่ยงสูงต่อสิทธิและเสรีภาพของบุคคลธรรมดา ผู้ควบคุมข้อมูลต้องแจ้งให้เจ้าของข้อมูลทราบถึงการรั่วไหลโดยไม่ชักช้า โดยในการแจ้งให้เจ้าของข้อมูลทราบต้องทำโดยใช้ภาษาที่ง่ายและชัดเจนถึงลักษณะการรั่วไหลและมีข้อมูลประกอบด้วย ชื่อ ที่ติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลขององค์กรนั้น บรรยายถึงผลกระทบอันอาจเกิดกับข้อมูลที่รั่วไหล บรรยายถึงมาตรการที่ได้ใช้หรือจะใช้ในการตอบสนอง ต่อการรั่วไหล เช่น มาตรการลดผลกระทบในทางลบอันอาจเกิดขึ้น

สำหรับประเทศสหรัฐอเมริกาก็ได้มีการกำหนดหลักการในเรื่องนี้ไว้เช่นกันโดยมีการกำหนดหลักการไว้แตกต่างกันไปในกฎหมายแต่ละมลรัฐ ตัวอย่างเช่น มลรัฐ California กำหนดว่าในกรณีที่มีการรั่วไหลหรือล่วงละเมิดว่า เป็นกรณีการเข้าถึงโดยมิชอบ (Unauthorized Access) หรือการได้มาโดยมิชอบ (Unauthorized Acquisition) ผู้ประกอบการหรือผู้ควบคุมข้อมูลมีหน้าที่แจ้งในทันที ซึ่งรูปแบบนี้มีลักษณะเป็นการกำหนดหน้าที่แบบความรับผิดเด็ดขาด (Strict Liability Model) หรือ

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของบางรัฐเช่น Alaska, Arkansas Florida วางหลักว่า ผู้ประกอบการต้องแจ้งเตือนเมื่อได้ทำการตรวจสอบประเมินความเสี่ยงอย่างเหมาะสมและมีเหตุผลแสดงว่าการรั่วไหลนั้นอาจส่งผลกระทบต่อเจ้าของข้อมูล ซึ่งรูปแบบการแจ้งแบบนี้เป็นรูปแบบการประเมินความเสี่ยง (Risk Assessment Model)[289]

เมื่อพิจารณาถึงหลักการนี้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 แล้วจะเห็นว่าประเทศไทยเลือกใช้หลักการตามแนวทางของสหภาพยุโรป โดยจะเห็นได้ว่า มีการบัญญัติหลักการกำหนดหน้าที่ให้กับผู้ควบคุมข้อมูลส่วนบุคคล ไว้ในมาตรา 37 (4) โดยกำหนดให้ผู้ควบคุมข้อมูลต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุเท่าที่สามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะกระทบต่อสิทธิและเสรีภาพของบุคคลให้แจ้งเหตุการละเมิดให้แก่เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางเยียวยาโดยไม่ชักช้าด้วย ซึ่งการกำหนดเช่นนี้เป็นการนำหลักการของ GDPR มาประยุกต์และกำหนดไว้ในกฎหมายไทยโดยมีการปรับเปลี่ยนแต่เพียงถ้อยคำเท่านั้นแต่สาระสำคัญก็เป็นไปในทำนองเดียวกัน

5.2.2 วิเคราะห์มาตรการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายอื่นที่เกี่ยวข้อง

นอกจากมาตรการในการคุ้มครองข้อมูลส่วนบุคคลตามที่ได้กำหนดไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 แล้ว ประเทศไทยยังมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่ได้บัญญัติไว้ในกฎหมายเฉพาะอีกมากมายหลายฉบับ โดยมีลักษณะของการกำหนดเป็นการเฉพาะเรื่องเฉพาะกรณีตามประเภทของข้อมูลส่วนบุคคล ดังจะยกตัวอย่างนอกเหนือจากที่ได้กล่าวไว้แล้วในบทที่ 4 ดังต่อไปนี้

ตัวอย่างแรก ข้อมูลส่วนบุคคลที่เป็นข้อมูลประวัติราษฎร ตามพระราชบัญญัติการทะเบียนราษฎร พ.ศ.2534 กำหนดนิยามข้อมูลส่วนบุคคลประเภทนี้ในมาตรา 4 ว่า

> ข้อมูลทะเบียนประวัติราษฎร” หมายความว่า ข้อมูลส่วนบุคคลเกี่ยวกับชื่อ สกุล เพศ วันเดือนปีเกิดและตาย สัญชาติ ศาสนา ภูมิลำเนา สถานการณ์สมรส วุฒิการศึกษา ชื่อบิดามารดาหรือผู้รับบุตรบุญธรรม ชื่อคู่สมรส และชื่อบุตร และข้อมูลอื่นที่จำเป็นเพื่อการดำเนินงานทะเบียนต่าง ๆ ตามพระราชบัญญัตินี้

---

[289] คณาธิป ทองรวีวงศ์, **รายงานการวิจัยฉบับสมบูรณ์ เรื่องการปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน,** หน้า 281-282.

โดยในกฎหมายฉบับนี้ ได้กำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลเป็นการเฉพาะไว้ในมาตรา 17 ว่า ข้อมูลทะเบียนประวัติราษฎรต้องถือเป็นความลับ และให้นายทะเบียนเป็นผู้เก็บรักษาและใช้เพื่อการปฏิบัติตามที่ได้บัญญัติไว้ในพระราชบัญญัตินี้เท่านั้น ห้ามมิให้ผู้ใดเปิดเผยข้อความหรือตัวเลขนั้นแก่บุคคลใด ๆ ซึ่งไม่มีหน้าที่ปฏิบัติการตามพระราชบัญญัตินี้ หรือแก่สาธารณชน เว้นแต่ผู้มีส่วนได้เสียขอทราบเกี่ยวกับสถานภาพทางครอบครัวของผู้ที่ตนจะมีนิติสัมพันธ์ด้วยหรือเมื่อมีความจำเป็นเพื่อประโยชน์แก่การสถิติ หรือเพื่อประโยชน์แก่การรักษาความมั่นคงของรัฐ หรือการดำเนินคดีและการพิจารณาคดีหรือการปฏิบัติหน้าที่ตามกฎหมายและไม่ว่าในกรณีใดจะนำข้อมูลทะเบียนประวัติราษฎรไปใช้เป็นหลักฐานที่อาจก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลมิได้

ตัวอย่างที่สอง ข้อมูลพยาน ตามพระราชบัญญัติคุ้มครองพยาน พ.ศ.2546 กำหนดมีการคุ้มครองข้อมูลส่วนบุคคลของพยานเกี่ยวกับชื่อตัว ชื่อสกุล และหลักฐานทางทะเบียนที่สามารถระบุตัวพยาน โดยกำหนดไว้ในมาตรา 10 (3) ให้สำนักงานคุ้มครองพยานดำเนินการประสานงานกับหน่วยงานที่เกี่ยวข้องเพื่อดำเนินการเปลี่ยนชื่อตัว ชื่อสกุลและหลักฐานทางทะเบียนเช่นว่า โดยให้ถือว่าข้อมูลดังกล่าวนี้เป็นความลับ และห้ามมิให้หน่วยงานเปิดเผยข้อมูล เว้นแต่จะได้รับอนุญาตจากรัฐมนตรีว่าการกระทรวงยุติธรรม โดยกำหนดโทษทางอาญาของการฝ่าฝืนไว้ในมาตรา 21 ว่า ห้ามผู้ใดเปิดเผยความลับที่เกี่ยวกับสถานที่อยู่ ชื่อ สกุล ที่อยู่ ภาพ หรือข้อมูลอย่างอื่นที่สามารถระบุตัวพยาน สามี ภรรยา ผู้บุพการี ผู้สืบสันดาน หรือบุคคลที่มีสัมพันธ์ใกล้ชิดกับพยานที่ได้รับการคุ้มครองตามมาตราการต่าง ๆ ของกฎหมายฉบับนี้ จนน่าจะเป็นเหตุให้บุคคลเหล่านี้ได้รับความไม่ปลอดภัย ถ้าฝ่าฝืนก็จะมีโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 2 หมื่นบาทหรือทั้งจำทั้งปรับ

ตัวอย่างที่สาม ข้อมูลที่ได้จากการดำเนินการเกี่ยวกับสถิติ ตามพระราชบัญญัติสถิติ พ.ศ. 2550 กำหนดให้มีการคุ้มครองข้อมูลสถิติอันเป็นข้อมูลส่วนบุคคลไว้ในมาตรา 15 ว่า บรรดาข้อมูลเฉพาะบุคคลหรือเฉพาะรายที่ได้มาตามพระราชบัญญัตินี้ ต้องถือเป็นความลับเคร่งครัด ห้ามมิให้ผู้ปฏิบัติหน้าที่ตามพระราชบัญญัตินี้หรือผู้มีหน้าที่เก็บรักษาเปิดเผยข้อมูลแก่บุคคลใด เว้นแต่ (1) เป็นการเปิดเผยเพื่อประโยชน์แก่การสอบสวนหรือพิจารณาคดีที่ต้องหาว่ากระทำความผิดตามพระราชบัญญัตินี้ หรือ (2) เป็นการเปิดเผยต่อหน่วยงานเพื่อประโยชน์ในการจัดทำสถิติ วิเคราะห์หรือวิจัย ทั้งนี้ เท่าที่ไม่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูล และต้องไม่ระบุหรือเปิดเผยถึงเจ้าของข้อมูล

นอกจากสามตัวอย่างนี้ ยังมีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่มีลักษณะเฉพาะกรณีอีกมากมายหลายฉบับ โดยหากพิจารณาตามหลักการของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ซึ่งเป็นกฎหมายกลาง ได้วางหลักการไว้ในมาตรา 3 โดยกำหนดไว้ว่า “ในกรณีที่มีกฎหมายว่าด้วยการใดบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในลักษณะใด กิจการใด หรือหน่วยงานใด

ไว้โดยเฉพาะแล้ว ให้บังคับตามบทบัญญัติแห่งกฎหมายว่าด้วยการนั้น เว้นแต่ (1) บทบัญญัติเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และบทบัญญัติเกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคล รวมทั้งบทกำหนดโทษที่เกี่ยวข้อง ให้บังคับตามบทบัญญัติแห่งพระราชบัญญัตินี้ เป็นการเพิ่มเติม ไม่ว่าจะซ้ำกับบทบัญญัติแห่งกฎหมายว่าด้วยการนั้นหรือไม่ก็ตาม” ดังนั้นหมายความว่าไม่ว่ากรณีจะเป็นประการใด ในเรื่องของการคุ้มครองข้อมูลส่วนบุคคลในมิติของการเก็บรวบรวม การใช้หรือการเปิดเผยข้อมูลส่วนบุคคล ประการที่หนึ่ง ในเรื่องสิทธิของเจ้าของข้อมูลส่วนบุคคลเป็นประการที่สอง และบทกำหนดโทษที่เกี่ยวข้องเป็นประการที่สาม จะต้องบังคับตามพระราชบัญญัติข้อมูลส่วนบุคคลด้วยเสมอเพื่อเป็นการยกระดับมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปในแนวทางเดียวกันทั้งระบบ

หากพิจารณาถึงกฎหมายเฉพาะที่กำหนดรับรองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลเป็นการเฉพาะที่สำคัญก็คือ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 ซึ่งได้อธิบายถึงสาระสำคัญไว้แล้วในบทที่ 4 จะเห็นว่ากฎหมายฉบับนี้ถือว่าเป็นกฎหมายที่มีการกำหนดคุ้มครองสิทธิในความเป็นส่วนตัวตัวเกี่ยวกับข้อมูลส่วนบุคคลไว้เป็นการเฉพาะสำหรับข้อมูลประเภทที่เป็นข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความครอบครองของทางราชการ ซึ่งสามารถเปรียบเทียบหลักการของกฎหมายทั้งสองฉบับได้ดังนี้คือ

ประการแรก วัตถุประสงค์ของกฎหมาย จะเห็นว่า พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 มีวัตถุประสงค์สำคัญต้องการให้ประชาชนได้รับทราบข้อมูลข่าวสารเกี่ยวกับการดำเนินการต่าง ๆ ของรัฐ และคุ้มครองสิทธิส่วนบุคคลในเรื่องของข้อมูลของประชาชนที่อยู่ในความครอบครองดูแลของหน่วยงานรัฐ โดยกำหนดให้เป็นหน้าที่ของหน่วยงานรัฐและเจ้าหน้าที่ของรัฐที่จะต้องปฏิบัติให้เป็นไปตามกฎหมายเพื่อรับรองและคุ้มครองสิทธิที่จะได้รู้ (Right to Know) ของประชาชน ภายใต้แนวคิดที่ว่า “เปิดเผยข้อมูลเป็นหลัก ปกปิดเป็นข้อยกเว้น” ส่วนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 เป็นกฎหมายที่ถูกสร้างขึ้นมาเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ทั้งนี้เพราะประเทศไทยยังไม่มีกฎหมายที่กำหนดคุ้มครองข้อมูลส่วนบุคคลในภาพรวมทุกชนิดทุกประเภท ดังนั้นวัตถุประสงค์หลักของกฎหมายฉบับนี้คือ “ปกปิดข้อมูลเป็นหลัก เปิดเผยเป็นข้อยกเว้น”

ประการที่สอง การกำหนดนิยามของข้อมูลส่วนบุคคลตามกฎหมาย จะเห็นว่า พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 มาตรา 4 ได้กำหนดนิยามของคำว่า “ข้อมูลข่าวสารส่วนบุคคล” หมายความว่า “ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้นหรือมีเลขหมายรหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึก ลักษณะเสียงของคนหรือรูปถ่าย และให้หมายรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ถึงแก่กรรมแล้ว

ด้วย” ส่วน พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 6 ได้กำหนดนิยามของคำว่า “ข้อมูลส่วนบุคคล” หมายความว่า “ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ” ในประเด็นนี้เห็นว่า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลไม่ได้ให้ความคุ้มครองไปถึงข้อมูลส่วนบุคคลของผู้ถึงแก่กรรม ซึ่งหากเกิดกรณีของการที่มีการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ถึงแก่กรรมโดยมิชอบ โดยประการที่น่าจะก่อให้เกิดความเสียหายแก่ตัวผู้ถึงแก่กรรม หรือทายาท กรณีเช่นนี้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลในฐานะที่เป็นกฎหมายกลางก็ไม่ได้คุ้มครองไปถึง

ประการที่สาม การกำหนดตัวบุคคลผู้ได้รับความคุ้มครอง จะเห็นว่า พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 มาตรา 21 ได้กำหนดตัวบุคคลผู้ได้รับความคุ้มครองว่า ต้องเป็นบุคคลธรรมดาที่มีสัญชาติไทย และบุคคลธรรมดาที่ไม่มีสัญชาติไทย แต่มีถิ่นที่อยู่ในประเทศไทยเท่านั้น ส่วนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 6 กำหนดตัวบุคคลว่าหมายถึงบุคคลธรรมดา โดยพระราชบัญญัติทั้งสองฉบับไม่ได้ให้ความคุ้มครองไปถึงข้อมูลของนิติบุคคล ซึ่งสอดคล้องกับหลักการสากล โดยหากพิจารณาคำว่า ข้อมูลส่วนบุคคล (Personal Data) ที่หมายถึงข้อมูลใด ๆ อันสามารถชี้เฉพาะตัวบุคคลที่เกี่ยวข้องกับตัวบุคคลซึ่งหมายถึง บุคคลธรรมดา (Natural Person) ที่เป็นเจ้าของข้อมูล (Data Subject) นั่นเอง

ประการที่สี่ การกำหนดหน้าที่ความรับผิดชอบ จะเห็นว่า ตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 กำหนดหน้าที่ความรับผิดชอบของหน่วยงานรัฐ ไว้ดังนี้คือ

1. ต้องจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลเท่าที่เกี่ยวข้องและจำเป็นเพื่อการดำเนินงานของหน่วยงานรัฐสำเร็จลุล่วงตามวัตถุประสงค์เท่านั้น และต้องยกเลิกการจัดให้มีระบบดังกล่าวเมื่อหมดความจำเป็น (มาตรา 23(1))

2. การจัดเก็บข้อมูล ให้พยายามจัดเก็บจากเจ้าของข้อมูลโดยตรง (มาตรา 23(2)) และในการจัดเก็บข้อมูลจะต้องแจ้งวัตถุประสงค์ให้เจ้าของข้อมูลทราบล่วงหน้า หรือพร้อมกับการขอข้อมูลด้วยว่าจะนำข้อมูลนั้นมาใช้เพื่อการอันใด และลักษณะของการใช้ข้อมูลตามปกติ (มาตรา 23 วรรคสอง)

3. จัดให้มีการพิมพ์ในราชกิจานุเบกษาและตรวจสอบแก้ไขให้ถูกต้องอยู่เสมอเกี่ยวกับประเภทข้อมูลที่มีการเก็บไว้ ประเภทของข้อมูลข่าวสารส่วนบุคคล ลักษณะการใช้ตามปกติ วิธีการขอตรวจดูข้อมูลข่าวสารของเจ้าของข้อมูล วิธีการขอให้แก้ไขเปลี่ยนแปลงข้อมูล แหล่งที่มาของข้อมูล (มาตรา 23(3))

4. ตรวจสอบแก้ไขข้อมูลข่าวสารส่วนบุคคลในความรับผิดชอบให้ถูกต้องอยู่เสมอ (มาตรา 23(4))

5. จัดระบบรักษาความปลอดภัยให้แก่ระบบข้อมูลข่าวสารส่วนบุคคล ตามความเหมาะสมเพื่อป้องกันมิให้มีการนำไปใช้โดยไม่เหมาะสมหรือเป็นผลร้ายต่อเจ้าของข้อมูล (มาตรา 23(5))

6. ต้องแจ้งให้เจ้าของข้อมูลทราบในกรณีมีการให้จัดส่งข้อมูลข่าวสารส่วนบุคคลไปยังที่ใด ซึ่งจะเป็นผลให้บุคคลทั่วไปทราบข้อมูลข่าวสารนั้นได้ เว้นแต่เป็นไปตามลักษณะการใช้ข้อมูลตามปกติ (มาตรา 23 วรรคสาม)

ส่วนตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กำหนดหน้าที่ความรับผิดชอบไว้แก่ผู้ควบคุมข้อมูล และผู้ประมวลผลข้อมูล ซึ่งนับว่าเป็นผู้มีส่วนเกี่ยวข้องกับข้อมูลส่วนบุคคลแตกต่างกัน กฎหมายจึงกำหนดหน้าที่และความรับผิดของสองนี้ไว้แตกต่างกันด้วย โดยจะกำหนดหน้าที่และความรับผิดสำหรับผู้ควบคุมข้อมูลไว้ค่อนข้างมาก เพราะถือว่าเป็นผู้ที่รับผิดชอบโดยตรง ตัวอย่างเช่น ผู้ควบคุมข้อมูลจะมีหน้าที่ในการจัดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่ตนจัดเก็บไว้ เพื่อป้องกันการสูญหาย เข้าถึง หรือแก้ไขโดยปราศจากอำนาจ รวมถึงจะต้องจัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบ หรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา รวมถึงมีหน้าที่แจ้งเหตุ กล่าวคือ หน้าที่ในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลให้แก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า โดยจะต้องไม่เกิน 72 ชั่วโมง และหากการละเมิดดังกล่าวมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล ก็จะต้องแจ้งเหตุแห่งการละเมิดพร้อมแนวทางการเยียวยาดังกล่าวให้เจ้าของข้อมูลทราบโดยไม่ชักช้า ในส่วนผู้ประมวลผลข้อมูล มีการกำหนดหน้าที่ในการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลเท่านั้น ไม่มีหน้าที่ในการจัดให้มีระบบตรวจสอบเพื่อดำเนินการลบข้อมูล รวมถึงมีหน้าที่ในการแจ้งให้ผู้ควบคุมข้อมูลทราบเมื่อเกิดเหตุละเมิดข้อมูล

สำหรับในประเด็นนี้ จะเห็นว่า สำหรับหน่วยงานของรัฐนั้น ถือว่าอยู่ในฐานะเทียบได้กับผู้ควบคุมข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 โดยมีกำหนดหน้าที่ไว้อย่างใกล้เคียงกัน แต่จะเห็นว่า ในส่วนของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 นั้นไม่ได้มีการกำหนดหน้าที่ในการปฏิบัติต่อข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นพิเศษ (Sensitive Data) เหมือนเช่นที่มีการกำหนดไว้ใน พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ประเด็นนี้จึงสมควรที่จะได้มีการกำหนดหน้าที่ของหน่วยงานรัฐตาม พระราชบัญญัติข้อมูลข่าวสารของราชการให้สอดคล้องกันกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลต่อไป

ประการที่ห้า การเปิดเผยข้อมูลส่วนบุคคล ตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 มาตรา 24 กำหนดว่า หน่วยงานของรัฐจะเปิดเผยข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความควบคุมดูแลของตนต่อหน่วยงานของรัฐแห่งอื่นหรือผู้อื่น โดยปราศจากความยินยอมเป็นหนังสือของเจ้าของข้อมูลที่ให้ไว้ล่วงหน้าหรือในขณะนั้นมิได้ เว้นแต่เป็นการเปิดเผยดังต่อไปนี้

1. ต่อเจ้าหน้าที่ของรัฐในหน่วยงานของตน เพื่อการนำไปใช้ตามอำนาจหน้าที่ของหน่วยงานของรัฐแห่งนั้น

2. เป็นการใช้ข้อมูลตามปกติภายในวัตถุประสงค์ของการจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลนั้น

3. ต่อหน่วยงานของรัฐที่ทำงานด้วยการวางแผน หรือการสถิติ หรือสำมะโนต่าง ๆ ซึ่งมีหน้าที่ต้องรักษาข้อมูลข่าวสารส่วนบุคคลไว้ไม่ให้เปิดเผยต่อไปยังผู้อื่น

4. เป็นการให้เพื่อประโยชน์ในการศึกษาวิจัย โดยไม่ระบุชื่อหรือส่วนที่ทำให้รู้ว่าเป็นข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับบุคคลใด

5. ต่อหอจดหมายเหตุแห่งชาติ กรมศิลปากร หรือหน่วยงานอื่นของรัฐตามมาตรา 26 วรรคหนึ่ง เพื่อการตรวจดูคุณค่าในการเก็บรักษา

6. ต่อเจ้าหน้าที่ของรัฐ เพื่อการป้องกันการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย การสืบสวน การสอบสวน หรือการฟ้องคดี ไม่ว่าเป็นคดีประเภทใดก็ตาม

7. เป็นการให้ซึ่งจำเป็น เพื่อการป้องกันหรือระงับอันตรายต่อชีวิตหรือสุขภาพของบุคคล

8. ต่อศาล และเจ้าหน้าที่ของรัฐหรือหน่วยงานของรัฐหรือบุคคลที่มีอำนาจตามกฎหมายที่จะขอข้อเท็จจริงดังกล่าว

9. กรณีอื่นตามที่กำหนดในพระราชกฤษฎีกา

ในส่วนของ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 27 กำหนดหลักการว่า ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอม เว้นแต่กรณีที่ไม่ต้องขอความยินยอมตาม มาตรา 24 หรือ มาตรา 26 ซึ่งก็ได้แก่กรณีดังนี้

1. เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

2. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

3. เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคล เป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

4. เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล

5. เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูล ส่วนบุคคล หรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

6. เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

โดยจะเห็นได้ว่า พระราชบัญญัติทั้งสองฉบับมีหลักการเป็นไปในทำนองเดียวกันในประเด็นนี้

ประการที่หก สิทธิของเจ้าของข้อมูลส่วนบุคคล ตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 บัญญัติให้สิทธิสำคัญแก่เจ้าของข้อมูลข่าวสารส่วนบุคคลคือ มีสิทธิขอตรวจสอบข้อมูลข่าวสารส่วนบุคคลของตนได้ ตามมาตรา 25 โดยเมื่อบุคคลนั้นมีคำขอเป็นหนังสือ หน่วยงานของรัฐที่ควบคุมดูแลข้อมูลข่าวสารนั้นจะต้องให้บุคคลนั้นหรือผู้กระทำการแทนบุคคลนั้นได้ตรวจดูหรือได้รับสำเนาข้อมูลข่าวสารส่วนบุคคลส่วนที่เกี่ยวกับบุคคลนั้น นอกจากนี้ ถ้าบุคคลใดเห็นว่าข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับตนส่วนใดไม่ถูกต้องตามที่เป็นจริง ให้มีสิทธิยื่นคำขอเป็นหนังสือให้หน่วยงานของรัฐที่ควบคุมดูแลข้อมูลข่าวสารแก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสารส่วนนั้นได้

ส่วนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มีการกำหนดให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลในลักษณะที่มากและกว้างขวางกว่า โดยเจ้าของข้อมูลส่วนบุคคลมีสิทธิ

1. สิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอม

2. สิทธิขอรับข้อมูลส่วนบุคคลที่เกี่ยวกับตนจากผู้ควบคุมข้อมูลส่วนบุคคลได้ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้ทำให้ข้อมูลส่วนบุคคลนั้นอยู่ในรูปแบบที่สามารถอ่านหรือใช้งานโดยทั่วไปได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติและสามารถใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ด้วยวิธีการอัตโนมัติ

3. สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตนเมื่อใดก็ได้

4. สิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

5. สิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการใช้ข้อมูลส่วนบุคคลได้

6. สิทธิขอให้ข้อมูลส่วนบุคคลถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด โดยในกรณีที่เจ้าของข้อมูลส่วนบุคคลร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด หากผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามคำร้องขอ ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกคำร้องขอของเจ้าของข้อมูลส่วนบุคคลพร้อมด้วยเหตุผลไว้

ซึ่งสิทธิของเจ้าของข้อมูลส่วนบุคคลตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้น มีการกำหนดรับรองสิทธิไว้มากมายและกว้างขวาง และสอดคล้องกับหลักการสากล เช่น สิทธิที่จะได้รับการแจ้ง (The Right to be Informed), สิทธิที่จะเข้าถึงข้อมูลส่วนบุคคลของตน (The Right of Access), สิทธิที่จะแก้ไขข้อมูลให้ถูกต้อง (The Right to Rectification), สิทธิที่จะถูกลืมหรือสิทธิที่จะลบ (The Right to be Forgotten/ The Right to Erasure), สิทธิที่จะจำกัดการ

ประมวลผล (The Right to Restrict Processing), สิทธิที่จะโอนย้ายข้อมูล (The Right to Data Portability) และสิทธิที่จะคัดค้าน (The Right to Object)

ประการสุดท้าย ประเด็นเรื่องบทกำหนดโทษ จะเห็นว่าในพระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ.2540 มิได้มีบทกำหนดโทษไว้สำหรับกรณีที่หน่วยงานของรัฐ และเจ้าหน้าที่ของรัฐ ไม่ปฏิบัติให้เป็นไปตามหลักการคุ้มครองข้อมูลข่าวสารส่วนบุคคล คงมีแต่บทบัญญัติกำหนดคุ้มครองเจ้าหน้าที่ตามมาตรา 20 โดยกำหนดว่า การเปิดเผยข้อมูลข่าวสารใดแม้จะเข้าข่ายต้องมีความรับผิดตามกฎหมายใด ให้ถือว่าเจ้าหน้าที่ของรัฐไม่ต้องรับผิดหากเป็นการกระทำโดยสุจริต ใน 2 กรณีคือ การปฏิบัติที่ถูกต้องตามกฎหมายว่าด้วยการรักษาความลับ และกรณีที่ใช้ดุลพินิจเปิดเผยข้อมูลข่าวสารโดยสมควรแก่เหตุเพื่อรักษาประโยชน์ที่สำคัญกว่า

ในส่วนของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2560 มีบทกำหนดโทษไว้อย่างรุนแรง ดังที่ได้กล่าวไว้แล้วในบทก่อน

จากที่ได้วิเคราะห์มาทั้งหมด สามารถสรุปข้อเปรียบเทียบเป็นตารางแสดงความแตกต่างได้ดังต่อไปนี้

ตารางที่ 5.6 เปรียบเทียบความแตกต่างระหว่าง พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ในประเด็นสำคัญ

ประเด็น	พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562
วัตถุประสงค์ของกฎหมายเกี่ยวกับสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล	เปิดเผยข้อมูลเป็นหลัก ปกปิดเป็นข้อยกเว้น	ปกปิดข้อมูลเป็นหลัก เปิดเผยเป็นข้อยกเว้น
นิยามของข้อมูลส่วนบุคคล	ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้นหรือมีเลขหมายรหัส หรือสิ่งบอก	ข้อมูลส่วนบุคคล” หมายความว่า “ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

ตารางที่ 5.6 (ต่อ)

ประเด็น	พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562
	ลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่าย และให้หมายรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ถึงแก่กรรมแล้วด้วย	
ผู้ได้รับความคุ้มครอง	บุคคลธรรมดาที่มีสัญชาติไทย และบุคคลธรรมดาที่ไม่มีสัญชาติไทยแต่มีถิ่นที่อยู่ในประเทศไทย	บุคคลธรรมดา
การกำหนดหน้าที่ความรับผิดชอบ	หน้าที่ของหน่วยงานรัฐ (ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล) จะต้อง 1. จัดระบบข้อมูลข่าวสารส่วนบุคคล เท่าที่เกี่ยวข้องและจำเป็นตามวัตถุประสงค์ และต้องยกเลิกเมื่อหมดความจำเป็น 2. การจัดเก็บข้อมูลให้พยายามจัดเก็บจากเจ้าของโดยตรง 3. จัดให้มีการตรวจสอบและแก้ไขข้อมูลให้ถูกต้องอยู่เสมอ 4. จัดระบบการรักษาความปลอดภัยให้แก่ระบบข้อมูลเพื่อป้องกันมิให้มีการนำไปใช้โดยไม่เหมาะสมหรือเป็นผลร้ายกับเจ้าของข้อมูล 5. แจ้งให้เจ้าของข้อมูลทราบในกรณีมีการให้จัดส่งข้อมูลข่าวสารส่วนบุคคลไปยังที่ใดซึ่งจะเป็นผล	ผู้ควบคุมข้อมูลส่วนบุคคล จะต้อง 1. จะทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้ หากเจ้าของข้อมูลไม่ได้ให้ความยินยอม และมีการกำหนดหลักการห้ามเก็บข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นพิเศษ 2. จัดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่ตนจัดเก็บไว้เพื่อป้องกันการสูญหาย เข้าถึงหรือแก้ไขโดยปราศจากอำนาจ 3.จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบ หรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา 4. หน้าที่แจ้งเหตุ กล่าวคือ หน้าที่ในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

ตารางที่ 5.6 (ต่อ)

ประเด็น	พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562
	ให้บุคคลทั่วไปทราบข้อมูลข่าวสารนั้นได้	
การเปิดเผยข้อมูลส่วนบุคคล	หน่วยงานของรัฐจะเปิดเผยข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความควบคุมดูแลของตนต่อหน่วยงานของรัฐแห่งอื่นหรือผู้อื่น โดยปราศจากความยินยอมเป็นหนังสือของเจ้าของข้อมูลที่ให้ไว้ล่วงหน้าหรือในขณะนั้นมิได้ เว้นแต่ มีเหตุตามมาตรา 24 (1) - (9) ให้มีการจัดทำบัญชีแสดงการเปิดเผยกำกับไว้กับข้อมูลข่าวสารนั้น	ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอม เว้นแต่กรณีที่ไม่ต้องขอความยินยอมตาม มาตรา 24 หรือมาตรา 26
สิทธิของเจ้าของข้อมูล	สิทธิสำคัญแก่เจ้าของข้อมูลข่าวสารส่วนบุคคลคือ มีสิทธิขอตรวจสอบข้อมูลข่าวสารส่วนบุคคลของตน และมีสิทธิขอให้แก้ไขเปลี่ยนแปลงให้ถูกต้อง	มีการกำหนดรับรองสิทธิไว้มากมายและกว้างขวาง และสอดคล้องกับหลักการสากล เช่น สิทธิที่จะได้รับการแจ้ง (The Right to be Informed), สิทธิที่จะเข้าถึงข้อมูลส่วนบุคคลของตน (The Right of Access), สิทธิที่จะแก้ไขข้อมูลให้ถูกต้อง (The Right to Rectification), สิทธิที่จะถูกลืมหรือสิทธิที่จะลบ (The Right to Be Forgotten/ The Right to Erasure), สิทธิที่จะจำกัดการประมวลผล (The Right to Restrict Processing), สิทธิที่จะโอนย้ายข้อมูล (The Right to

ตารางที่ 5.6 (ต่อ)

ประเด็น	พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562
		Data Portability) และสิทธิที่จะคัดค้าน (The Right to Object)
บทกำหนดโทษ	ไม่มีบทกำหนดโทษที่ชัดเจน	มีบทกำหนดโทษ

5.3 วิเคราะห์กลไกการเยียวยาผู้ถูกละเมิดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล

สำหรับกลไกการเยียวยาผู้ถูกละเมิดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกา นั้นมีกลไกการเยียวยา (Redress) หลายระดับซึ่งเป็นไปตามกรอบข้อตกลง EU-U.S. Privacy Shield ซึ่งสรุปได้ดังนี้คือ

ประการแรก การเยียวยาโดยตรง กิจการจะต้องตอบสนองต่อคำร้องจากบุคคลธรรมดาภายใน 45 วัน

ประการที่สอง เจ้าของข้อมูลใช้สิทธิร้องเรียนโดยตรงต่อองค์กรอิสระ รวมทั้งองค์กรคุ้มครองข้อมูลของยุโรป เช่น คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายภายใน

ประการที่สาม กระทรวงพาณิชย์สหรัฐเข้ามามีบทบาทระงับข้อพิพาทกรณีองค์กรที่ไม่ปฏิบัติตามหลัก PRIVACY SHIELD

ประการที่สี่ การระงับข้อพิพาททางเลือก (Alternative Dispute Resolution) ต้องจัดให้มีขึ้นโดยปราศจากค่าใช้จ่าย

ประการที่ห้า มีกลไกอนุญาโตตุลาการเป็นที่พึ่งสุดท้าย (Last Resort) โดยมีการจัดตั้ง PRIVACY SHIELD Panel ทั้งนี้ เจ้าของข้อมูลที่เป็นฯพลเมืองยุโรปมีสิทธิระงับข้อพิพาทโดยอนุญาโตตุลาการ (Privacy Shield Panel) ประกอบด้วยอย่างน้อย 20 คนที่แต่งตั้งโดยกระทรวงพาณิชย์สหรัฐและกรรมาธิการยุโรป ในกรณีปัญหาการสอดส่องข้อมูลโดยภาครัฐมีกระบวนการพิเศษได้แก่ การจัดตั้งองค์กรอิสระเรียกว่า Privacy Shield Ombudsperson ซึ่งเป็นอิสระจากหน่วยงานเกี่ยวกับข่าวกรองหรือ Intelligent Community เพื่อคุ้มครองการล่วงละเมิดข้อมูลจากภาครัฐ

สำหรับประเทศแคนาดา กลไกการเยียวยานั้น มีการกำหนดให้ผู้ร้องเรียนซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล หรือ คณะกรรมการสิทธิความเป็นส่วนตัวของแคนาดาภายใต้ความยินยอมของ

เจ้าของข้อมูล สามารถที่จะนำคดีขึ้นสู่การพิจารณาของศาล The Federal Court เพื่อพิจารณาคดีใหม่อีกครั้งหนึ่ง ซึ่งศาลมีอำนาจอย่างกว้างขวางในการสั่งการแก้ไขการปฏิบัติขององค์กร และมีอำนาจลงโทษให้ชดใช้ค่าเสียหายเพื่อเยียวยาความเสียหายให้แก่ผู้ร้องเรียน ซึ่งความเสียหายนี้รวมไปถึงความเสียหายต่อชื่อเสียงเกียรติยศซึ่งได้รับความเดือดร้อนด้วย นอกจากนี้ สำนักงานคณะกรรมการสิทธิความเป็นส่วนตัวแห่งแคนาดาและองค์กรอาจตกลงทำข้อตกลงเกี่ยวกับการปฏิบัติตามความสมัครใจ โดยถ้าองค์กรรับรองว่าจะปฏิบัติตามคำแนะนำที่ได้ทำไว้ภายใต้กฎหมาย PIPEDA และถ้าผู้ร้องเรียนเห็นชอบด้วย คณะกรรมการฯ จะไม่นำคดีขึ้นสู่ศาลเพื่อพิจารณาคดี หรือจะระงับการยื่นคำร้องต่อศาลที่ค้างอยู่ทั้งหมดก็ได้ เว้นแต่จะมีการละเมิดข้อตกลง และหากต่อมา หากองค์กรไม่สามารถปฏิบัติตามความตกลงของตนในข้อตกลงการปฏิบัติตามสำนักงานคณะกรรมการสิทธิความเป็นส่วนตัวของแคนาดาก็สามารถยื่นคำร้องต่อศาลเพื่อขอให้ศาลสั่งให้องค์กรปฏิบัติตามเงื่อนไขของข้อตกลงได้

ในส่วนประเทศทางฝั่งสหภาพยุโรปนั้น ในส่วนของ GDPR วางหลักการในเรื่องกลไกการเยียวยาไว้โดยกำหนดให้สิทธิแก่ผู้ที่ถูกล่วงละเมิดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลมีสิทธิดังต่อไปนี้คือ

ประการแรก ผู้ถูกล่วงละเมิดมีสิทธิในการยื่นเรื่องร้องเรียนกับหน่วยงานกำกับดูแล (Right to Lodge a Complaint with a Supervisory Authority) โดยเมื่อหน่วยงานกำกับดูแลได้รับเรื่องร้องเรียนแล้วจะต้องแจ้งให้ผู้ร้องเรียนทราบถึงความคืบหน้าและผลของการร้องเรียน รวมถึงความเป็นไปได้ในการแก้ไขปัญหาโดยอาศัยกระบวนการทางศาล (Article 77)

ซึ่งในเรื่องนี้ หากองค์กรกำกับดูแลปฏิบัตหน้าที่ไม่ถูกต้องหรือละเลยการปฏิบัติหน้าที่หรือปฏิบัติหน้าที่ล้าช้า เช่นนี้ ผู้ถูกล่วงเมิดมีสิทธิได้รับการเยียวยาอย่างมีประสิทธิภาพจากฝ่ายตุลาการต่อหน่วยงานกำกับดูแล (Right to an Effective Judicial Remedy Against a Supervisory Authority) ในกรณีที่หน่วยงานกำกับดูแลไม่จัดการเรื่องร้องเรียนหรือไม่แจ้งข้อมูลเรื่องภายในสามเดือนเกี่ยวกับความคืบหน้าหรือผลลัพธ์ของการร้องเรียน (Article 78)

ประการที่สอง สิทธิในการดำเนินคดีอย่างมีประสิทธิภาพต่อผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูล (Right to an Effective Judicial Remedy Against a Controller or Processor) โดยไม่กระทบกระเทือนต่อถึงบริหารจัดการหรือการเยียวยาหรือสิทธิยื่นเรื่องร้องเรียนต่อหน่วยงานกำกับดูแลตาม Article 77 ในประการแรก เจ้าของข้อมูลส่วนบุคคลที่ถูกล่วงละเมิดมีสิทธิในการได้รับการพิจารณาคดีที่มีประสิทธิภาพ เมื่อผู้ถูกล่วงละเมิดเห็นว่าตนถูกละเมิดอันเป็นผลมาจากการประมวลผลข้อมูลส่วนบุคคลหรือในการไม่ปฏิบัติตาม GDPR เขาย่อมมีสิทธิที่จะใช้สิทธิในทางศาล (Article 79)

ภายใต้สิทธิในสองประการก่อน (สิทธิตาม Article 77-79) เจ้าของข้อมูลส่วนบุคคลที่ถูกล่วงละเมิดอาจมอบหมายให้องค์กรหรือสมาคมที่ไม่แสวงหาผลกำไรทำหน้าที่เป็นผู้แทนของตนในการใช้สิทธิได้ (Article 80)

ประการที่สาม เจ้าของข้อมูลส่วนบุคคลที่ถูกล่วงละเมิดมีสิทธิได้รับการชดเชยและค่าเสียหาย (Right to Compensation and Liability) โดย GDPR วางหลักการว่า บุคคลใดก็ตามที่ได้รับความเดือดร้อนหรือความเสียหายอันเป็นผลมาจากการละเมิดกฎข้อบังคับนี้ จะมีสิทธิได้รับค่าชดเชยจากผู้ควบคุมหรือผู้ประมวลผลสำหรับความเสียหายที่ได้รับความเดือดร้อน ซึ่งขั้นตอนในการใช้สิทธิทางศาลเพื่อเรียกร้องค่าชดเชยจะต้องดำเนินการต่อศาลที่มีอำนาจตามกฎหมายของแต่ละประเทศสมาชิก (Article 82)

ภายใต้กลไกการเยียวยาที่กล่าวมา หากมีการพบว่า เจ้าของข้อมูลส่วนบุคคลถูกล่วงละเมิดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลจริงและเกิดความเสียหายแล้ว จะเห็นว่า GDPR ได้มีการกำหนดความรับผิดสำหรับการฝ่าฝืนบทบัญญัติ เอาไว้ ปรากฏอยู่ในหมวด 8 ว่าด้วยการเยียวยา ความรับผิด และโทษ (Remedies, Liability and Penalties)

โดยมาตรการบังคับสำหรับการฝ่าฝืนนั้น มีทั้งกรณีที่ผู้ฝ่าฝืนจะต้องชดใช้ค่าสินไหมทดแทนสำหรับความเสียหายที่เจ้าของข้อมูลส่วนบุคคลได้รับ (Article 82 1.) และกรณีที่ผู้ฝ่าฝืนจะต้องชำระค่าปรับทางปกครอง (Administrative Fine) ซึ่งการฝ่าฝืนบทบัญญัติบางกรณีมีโทษปรับทางปกครองโดยโทษปรับสูงสุดเป็นจำนวนเงินสูงถึงไม่เกิน 10 ล้านยูโร หรือไม่เกินร้อยละ 2 ของรายได้รวมจากทั่วโลกในรอบปี (Worldwide Annual Turnover) แล้วแต่ว่าจำนวนใดจะสูงกว่ากัน (Article 83 4.) และกรณีการละเมิดที่มีความร้ายแรง ก็มีโทษปรับทางปกครอง โดยปรับสูงสุดเป็นจำนวนเงินถึงไม่เกิน 20 ล้านยูโร หรือไม่เกินร้อยละ 4 ของรายได้รวมจากทั่วโลกในรอบปี แล้วแต่ว่าจำนวนใดจะสูงกว่ากัน (Article 83 5.)

อย่างไรก็ดี ในทางปฏิบัติก็ยังมีประเด็นที่ต้องพิจารณาว่าสำหรับกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลอยู่นอกสหภาพยุโรปแล้ว ทางสหภาพยุโรปจะทำการบังคับอย่างไร ซึ่งคงต้องรอแนวทางปฏิบัติต่อไป

จากหลักกฎหมายต่างประเทศที่กล่าวมาข้างต้น เมื่อพิจารณาจากกลไกเยียวยาผู้ถูกละเมิดสิทธิตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 แล้วจะเห็นว่า ได้มีการกำหนดมาตรการไว้ในกฎหมายผ่านการบังคับใช้โดยคณะกรรมการข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการข้อมูลส่วนบุคคล โดยมีการกำหนดทั้งในส่วนของโทษทางอาญา และโทษทางปกครอง รวมไปถึงมีการกำหนดความรับผิดในทางแพ่งไว้ด้วย

มีการกำหนดกระบวนการให้ต้องร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญที่ได้รับการพิจารณาแต่งตั้งจากคณะกรรมการข้อมูลส่วนบุคคล ซึ่งคณะกรรมการชุดนี้จะมีอำนาจในการตรวจสอบและออกคำสั่งตามที่มีการร้องเรียน

โดยให้สิทธิร้องเรียนแก่เจ้าของข้อมูลที่ถูกล่วงละเมิด กล่าวคือ เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ฝ่าฝืน หรือไม่ปฏิบัติตามพระราชบัญญัตินี้ กฎกระทรวงหรือประกาศที่ออกตามพระราชบัญญัตินี้

นอกจากนี้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลยังได้มีการให้สิทธิแก่เจ้าของข้อมูลที่จะดำเนินคดีทางแพ่งสำหรับผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลส่วนบุคคล สำหรับความรับผิดในทางแพ่งนั้น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ได้มีการกำหนดหลักการไว้ซึ่งเมื่อพิจารณาเปรียบเทียบกับหลักการของ GDPR แล้วจะเห็นความแตกต่างดังต่อไปนี้

ตารางที่ 5.7 แสดงความรับผิดทางแพ่งตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

หัวข้อ	**ความรับผิด ตามพระราชบัญญัติฯ**	**ความรับผิด ตาม GDPR**
พฤติการณ์ของการล่วงละเมิด	ผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูลดำเนินการใด ๆ เกี่ยวกับข้อมูลอันเป็นการฝ่าฝืนต่อบทบัญญัติ ไม่ว่าจะเป็นโดยจงใจหรือประมาทเลินเล่อ	ผู้ควบคุมข้อมูลจะรับผิดชอบต่อความเสียหายที่เกิดจากการดำเนินการที่ไม่สอดคล้องกับ GDPR; ผู้ประมวลผลต้องรับผิดต่อความเสียหายที่เกิดขึ้นจากการดำเนินการใด ๆ ที่เป็นการละเมิดข้อผูกพันที่กำหนดไว้โดยเฉพาะใน GDPR หรือเกิดจากการดำเนินการที่อยู่นอกขอบเขตหรือขัดต่อคำแนะนำที่ชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

ตารางที่ 5.7 (ต่อ)

หัวข้อ	ความรับผิด ตามพระราชบัญญัติฯ	ความรับผิด ตาม GDPR
ข้อยกเว้นไม่ต้องรับผิด	(1) ความเสียหายเกิดจากเหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั้นเอง (2) เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามหน้าที่	--
การชดใช้ค่าสินไหมทดแทน	ค่าสินไหมทดแทนรวมถึงค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลได้ใช้จ่ายไปตามความเป็นจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้น หรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย ศาลมีอำนาจกำหนดค่าสินไหมทดแทนเพิ่มขึ้นจากจำนวนค่าสินไหมทดแทนที่แท้จริงที่ศาลกำหนดได้ตามที่เห็นสมควร แต่ไม่เกินสองเท่าของค่าสินไหมทดแทนที่แท้จริงนั้น โดยคำนึงถึงพฤติการณ์ต่าง ๆ ประกอบเช่น ความร้ายแรงของความเสียหาย ผลประโยชน์และสถานะทางการเงินที่ผู้ล่วงละเมิดได้รับ การบรรเทาความเสียหายให้แก่	GDPR เพียงแต่กำหนดให้บุคคลใดก็ตามที่ได้รับความเดือดร้อนหรือความเสียหายอันเป็นผลมาจากการละเมิด จะมีสิทธิได้รับค่าชดเชยจากผู้ควบคุมหรือผู้ประมวลผลสำหรับความเสียหายที่ได้รับความเดือดร้อน ซึ่งกระบวนการ รูปแบบ และขั้นตอนในการใช้สิทธิทางศาลเพื่อเรียกร้องค่าชดเชยจะต้องดำเนินการต่อศาลที่มีอำนาจตามกฎหมายของแต่ละประเทศสมาชิก ซึ่งค่าเสียหายนี้มีทั้งค่าเสียหายที่เป็นอาจคำนวณราคาเป็นเงินและไม่อาจคำนวณราคาเป็นตัวเงิน

ตารางที่ 5.7 (ต่อ)

หัวข้อ	ความรับผิด ตามพระราชบัญญัติฯ	ความรับผิด ตาม GDPR
	เจ้าของข้อมูล หรือการที่เจ้าของข้อมูลมีส่วนร่วมในการก่อความเสียหาย	
อายุความ	ขาดอายุความเมื่อพ้น 3 ปีนับแต่วันที่รู้ถึงความเสียหายและรู้ตัวผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูล หรือเมื่อพ้น 10 ปีนับแต่วันที่มีการละเมิดข้อมูลส่วนบุคคล	เป็นไปตามกฎหมายของแต่ละประเทศสมาชิก

เมื่อพิจารณาแล้วจะเห็นว่า แม้ว่าตามหลักการของ GDPR และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลจะมีการกำหนดให้หน่วยงานคุ้มครองข้อมูลส่วนบุคคล มีอำนาจในวงกว้างโดยเฉพาะอำนาจทางปกครอง แต่ก็ยังอาจจะไม่เพียงพอที่จะแก้ไขเยียวยาความเสียหายที่เกิดขึ้น ดังนั้น จึงจำเป็นจะต้องมีกลไกเยียวยาที่มีลักษณะการบังคับใช้สิทธิของเจ้าของข้อมูลเป็นการส่วนตัวและอิสระการกำหนดสิทธิเรียกร้องค่าเสียหายในทางแพ่ง จึงเป็นรูปแบบของกลไกเยียวยาความเสียหายที่จะมาเติมเต็มและอุดช่องว่างในการใช้มาตรการบังคับทางปกครองของหน่วยงานคุ้มครองข้อมูลส่วนบุคคลได้เป็นอย่างดี ซึ่งหลักการเรียกร้องค่าเสียหายในทางแพ่งของ GDPR นั้น อยู่บนพื้นฐานของการกำหนดให้เป็นสิทธิแก่เจ้าของข้อมูล โดยกำหนดให้มีกลไกการเยียวยา 2 ประเภท กล่าวคือ ประเภทแรก เป็นสิทธิในการได้รับชดเชยค่าเสียหายจากผู้ควบคุมหรือผู้ประมวลผล สำหรับความเสียหายที่เกิดจากการละเมิดกฎข้อบังคับ และประเภทที่สอง คือ สิทธิในการแก้ไขที่มีประสิทธิภาพในรูปแบบของความต้องการที่จะดำเนินการเฉพาะ (เป็นไปตามหลักการของ Article. 82) ซึ่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยก็ได้มีการกำหนดหลักการไว้ในลักษณะเช่นเดียวกัน

แต่อย่างไรก็ดี ในลักษณะของการกำหนดกลไกเยียวยาความเสียหายนั้น GDPR ยังมีการกำหนดให้สามารถมีตัวแทน (Representative Bodies) มาดำเนินการให้แก่เจ้าของข้อมูลส่วนบุคคลที่ได้รับความเสียหายได้ ซึ่งเรื่องนี้ไม่มีการกำหนดไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล โดยภายใต้หลักการของ GDPR จะมีการให้สิทธิแก่ตัวแทนซึ่งทำหน้าที่ในนามของเจ้าของข้อมูลส่วนบุคคลเพื่อยื่นเรื่องร้องเรียนกับหน่วยงานกำกับดูแล หรือดำเนินการฟ้องร้องเพื่อเรียกร้องการเยียวยาทางศาล โดยองค์กรที่ได้รับการยอมรับให้ทำหน้าที่เป็นตัวแทนของเจ้าของข้อมูลนั้นจะต้องอยู่บนพื้นฐาน คือ ต้องเป็นองค์กรหรือสมาคมที่ไม่แสวงหาผลกำไร และมีประกอบการหรือดำเนินการอย่างถูกต้องตามกฎหมายของประเทศสมาชิก โดยจะต้องมีวัตถุประสงค์ตามกฎหมายที่เป็นประโยชน์ต่อสาธารณะ และมีการดำเนินกิจกรรมทางด้านการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ซึ่งการกำหนดหลักการเช่นนี้ของ GDPR เป็นการส่งเสริมให้มีการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลสำหรับพลเมืองชาวยุโรปอย่างแท้จริงนั้นเอง

นอกจากการกำหนดให้สิทธิแก่เจ้าของข้อมูลที่จะใช้ช่องทางการเยียวยาโดยอาศัยหลักการทางแพ่งฟ้องเรียกร้องค่าเสียหายสำหรับการทำละเมิดของผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลส่วนบุคคลแล้ว ในแง่อำนาจรัฐที่กำหนดเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลยังมีการกำหนดโทษแก่ผู้ที่ล่วงละเมิดสิทธินี้ด้วย ทั้งในรูปแบบของโทษอาญาและโทษทางปกครอง ซึ่งสำหรับโทษนั้น มีการกำหนดไว้ทั้งโทษทางอาญา กล่าวคือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล มาตรา 77 กำหนดสาระสำคัญในเรื่องโทษทางอาญาว่า ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนโดยใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ หรือ ทำการเก็บรวบรวมข้อมูลส่วนบุคคลอันเกี่ยวกับข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) โดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่นถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ หรือหากเป็นกรณีผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนกระทำการดังที่กล่าวมา แต่เป็นการกระทำเพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น ต้องระวางโทษหนักขึ้น คือ จำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งล้านบาท หรือทั้งจำทั้งปรับ ซึ่งพิจารณาได้จากตารางต่อไปนี้

ตารางที่ 5.8 แสดงโทษทางอาญาตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

ความผิด	โทษตามพระราชบัญญัติฯ
1. ผู้ควบคุมข้อมูลซึ่งเป็นบุคคลหรือนิติบุคคลได้ใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลฯ หรือเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่แจ้งไว้ โดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย	ระวางโทษจำคุกไม่เกิดหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ
2. ผู้ควบคุมข้อมูลซึ่งเป็นบุคคลหรือนิติบุคคลได้ส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศโดยประเทศปลายทางไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ โดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย	ระวางโทษจำคุกไม่เกิดหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ
3. ผู้ควบคุมข้อมูลซึ่งเป็นบุคคลหรือนิติบุคคลได้ใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลฯ หรือเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่แจ้งไว้ เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น	ระวางโทษจำคุกไม่เกินหนึ่งปีหรือปรับไม่เกินหนึ่งล้านบาท หรือทั้งจำทั้งปรับ
4. ผู้ควบคุมข้อมูลซึ่งเป็นบุคคลหรือนิติบุคคลได้ส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศโดยประเทศปลายทางไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น	ระวางโทษจำคุกไม่เกินหนึ่งปีหรือปรับไม่เกินหนึ่งล้านบาท หรือทั้งจำทั้งปรับ

สำหรับโทษในทางอาญาไม่ได้มีเขียนไว้ใน GDPR แต่ในส่วนกฎหมายภายในของรัฐสมาชิกจะพบว่ามีการกำหนดฐานความผิดทางอาญาไว้สำหรับกรณีการล่วงละเมิดข้อมูลส่วนบุคคล ตัวอย่างเช่น ในกรณีของประเทศฝรั่งเศส ปรากฏตามมาตรา 50-52 ของ รัฐบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของประเทศฝรั่งเศส ที่ผ่านรัฐสภาเมื่อวันที่ 20 มิถุนายน 2561 ได้มีการกำหนดฐานความผิดและโทษทางอาญาไว้สำหรับกรณีดังนี้

กรณีแรกเป็นบทลงโทษระบุไว้ในมาตรา 226-16 to 226-24 and ในมาตรา R. 625-10 ถึง R. 625-13 ของประมวลกฎหมายอาญาฝรั่งเศส (ตัวอย่างเช่น การรวบรวมข้อมูลส่วนบุคคลด้วยวิธีการฉ้อโกง ไม่เป็นธรรมหรือผิดกฎหมาย ประมวลผลหมายเลขประจำตัวประชาชนโดยไม่ได้รับอนุญาตตามกฎหมาย หรือการไม่แจ้งเตือนในกรณีมีการละเมิดข้อมูล ฯลฯ เป็นต้น)

กรณีที่สองเป็นการกำหนดโทษสำหรับการกระทำใด ๆ ที่เป็นการขัดขวางการดำเนินงานของ CNIL

สำหรับประเทศเยอรมนี ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (BDSG) มีการกำหนดโทษจำคุกหรือปรับในกรณี (1) การโอน หรือการเข้าถึงข้อมูลส่วนบุคคลที่โดยมิชอบด้วยกฎหมายของบุคคลจำนวนมากเพื่อวัตถุประสงค์ทางการค้า (2) การประมวลผลข้อมูลส่วนบุคคลที่มิใช่ข้อมูลสาธารณะที่โดยมิชอบด้วยกฎหมาย หากทำเพื่อหากำไรหรือด้วยความตั้งใจที่เพิ่มคุณค่าให้กับตนเองหรือบุคคลที่สาม หรือทำลายบุคคลอื่น (3) การได้มาซึ่งข้อมูลส่วนบุคคลที่ไม่สามารถเข้าถึงได้โดยมิชอบด้วยกฎหมาย หากกระทำเพื่อหากำไร หรือด้วยเจตนาที่จะเพิ่มคุณค่าให้กับตนเองหรือบุคคลที่สาม หรือสร้างความเสียหายให้กับบุคคลอื่น

สำหรับในประเทศอังกฤษ The Data Protection Act มีการกำหนดโทษทางอาญาสำหรับกรณีดังต่อไปนี้

1. กระทำการโดยเจตนาหรือประมาท

1) ในการเก็บรวบรวมหรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากผู้ควบคุมข้อมูล

2) เปิดเผยข้อมูลส่วนบุคคลให้กับบุคคลอื่นโดยไม่ได้รับความยินยอมจากผู้ควบคุมข้อมูล

3) หลังจากได้รับข้อมูลส่วนบุคคลและเก็บข้อมูลส่วนบุคคลนั้นไว้โดยไม่ได้รับความยินยอมจากบุคคลที่เป็นผู้ควบคุมที่เกี่ยวข้อง

4) ขายข้อมูลหากได้รับมาจากกรณีที่มีการกระทำความผิดตามสามข้อข้างต้น (S170)

2. จงใจหรือประมาทเลินเล่อ นำกลับมาหรือระบุข้อมูลส่วนบุคคลที่ถูกลบโดยไม่ได้รับความยินยอมจากผู้ควบคุมที่รับผิดชอบ (S171)

3. ทำการแก้ไข, ลบล้าง, บล็อก, ลบ, ทำลาย หรือปกปิดข้อมูลด้วยความตั้งใจที่จะป้องกันการเปิดเผยข้อมูลตามคำขอเข้าถึงของเจ้าของข้อมูล (S173)

4. ทำลายหรือการปลอมแปลงเอกสาร หรืออนุญาตให้ทำลายหรือปลอมแปลงเอกสารด้วยความตั้งใจที่จะขัดขวางคณะกรรมการข้อมูลส่วนบุคคลฯ หลังจากได้รับข้อมูลหรือการแจ้งการประเมิน

ส่วนโทษทางปกครองนั้น กล่าวคือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล วางบทกำหนดโทษทางปกครองที่สำคัญแก่ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลไว้ในกรณีที่ไม่ดำเนินการให้ถูกต้องตามพระราชบัญญัตินี้ โดยปรากฏดังตารางดังต่อไปนี้

ตารางที่ 5.9 แสดงโทษทางปกครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

ความผิด	**โทษตามพระราชบัญญัติฯ**
1. ผู้ควบคุมข้อมูลเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่แจ้งเจ้าของข้อมูลทราบ หรือ เมื่อเจ้าของข้อมูลมีคำขอเพื่อเข้าถึงข้อมูลส่วนบุคคลแล้วผู้ควบคุมไม่ปฏิบัติตามคำขอ โดยการปฏิบัติล่าช้าหรือเกิน 30 วันนับแต่ได้รับคำขอ หรือ ไม่บันทึกรายการสำคัญอันจะทำให้เจ้าของข้อมูลหรือสำนักงานคณะกรรมการข้อมูลส่วนบุคคลฯ ไม่สามารถตรวจสอบข้อมูลส่วนบุคคลได้ หรือไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด หรือไม่สนับสนุนการทำงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลออกจากงานเพราะได้ปฏิบัติตามกฎหมายนี้ หรือไม่ขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลให้ชัดเจนในกรณีจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล	โทษปรับทางปกครอง ไม่เกิน 1 ล้านบาท

ตารางที่ 5.9 (ต่อ)

ความผิด	โทษตามพระราชบัญญัติฯ
หรือไม่แจ้งผลกระทบจากการถอนความยินยอมให้แก่เจ้าของข้อมูลทราบ หรือไม่แจ้งให้เจ้าของข้อมูลทราบในกรณีที่จะกระทำการเก็บรวบรวมข้อมูลของเจ้าของข้อมูลจากแหล่งอื่นที่ไม่ใช่มาจากเจ้าของข้อมูลโดยตรง (มาตรา 82)	
2. ผู้ควบคุมข้อมูลเก็บรวมรวมข้อมูล ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลผิดวัตถุประสงค์ หรือ เก็บรวบรวมข้อมูลเกินความจำเป็นหรือไม่อยู่ภายใต้วัตถุประสงค์โดยชอบด้วยกฎหมาย หรือ เก็บรวบรวมข้อมูลจากแหล่งอื่นที่ไม่ใช่มาจากเจ้าของข้อมูลโดยตรง หรือ ใช้ หรือเปิดเผยข้อมูลโดยไม่ได้รับความยินยาม หรือตามวัตถุประสงค์อื่นผิดไปจากที่แจ้งแก่เจ้าของข้อมูล หรือ ส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ โดยประเทศปลายทางไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ เมื่อเจ้าของข้อมูลส่วนบุคคลใช้สิทธิคัดค้านการเก็บรวบรวม ใช้ เหรือเปิดเผยข้อมูลแล้ว ยังคงเก็บรวมรวม ใช้ หรือเปิดเผยข้อมูลนั้นต่อไป หรือไม่จัดให้มีมาตรฐานการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม หรือ ขอความยินยอมโดยการหลอกลวง หรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ในการที่จะเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลนั้น	โทษปรับทางปกครอง ไม่เกิน 3 ล้านบาท

ตารางที่ 5.9 (ต่อ)

ความผิด	โทษตามพระราชบัญญัติฯ
(มาตรา 83)	
3. ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวม ใช้ เปิดเผย ส่งออกหรือโอนไปยังต่างประเทศ ซึ่งข้อมูลส่วนบุคคลที่มีความอ่อนไหว โดยไม่ชอบด้วยกฎหมายนี้	โทษปรับทางปกครอง ไม่เกิน 5 ล้านบาท
(มาตรา 84)	
4. ผู้ประมวลผลข้อมูลส่วนบุคคล ไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด หรือไม่สนับสนุนการทำงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลออกจากงานเพราะได้ปฏิบัติตามกฎหมายนี้	โทษปรับทางปกครอง ไม่เกิน 1 ล้านบาท
(มาตรา 85)	
5. ผู้ประมวลผลข้อมูลส่วนบุคคล ไม่ปฏิบัติหน้าที่ให้ถูกต้องในเรื่องการเก็บรวบรวม ใช้ เปิดเผย รักษาความปลอดภัยของข้อมูล จัดทำหรือบันทึกรายการกิจกรรมการประมวลผล หรือส่งหรือโอนข้อมูลไปต่างประเทศโดยมิชอบ หรือ ไม่แต่งตั้งตัวแทนไว้ในราชอาณาจักรสำหรับธุรกิจที่มีการเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่อยู่ราชอาณาจักร	โทษปรับทางปกครอง ไม่เกิน 3 ล้านบาท
(มาตรา 86)	
6. ผู้ประมวลผลข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลที่มีความอ่อนไหวไปยังต่างประเทศโดยมิชอบ	โทษปรับทางปกครอง ไม่เกิน 5 ล้านบาท
(มาตรา 87)	

สำหรับ GDPR ในกรณีที่ไม่ได้ปฏิบัติตามหลักการจะมีการกำหนดโทษปรับทางปกครองไว้ 2 ระดับ[290]

สำหรับระดับแรก เป็นระดับโทษรุนแรง (Severe Penalties)

กล่าวคือ โทษปรับทางปกครองสูงสุดถึง 10,000,000 EUR หรือปรับมากถึง 2% ของมูลค่าการซื้อขายรวมทั่วโลกประจำปีของปีงบประมาณก่อน

ในกรณีที่ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลไม่ปฏิบัติหน้าที่ตาม GDPR ตัวอย่างเช่นเรื่องต่อไปนี้คือ

1. ไม่ขอความยินยอมจากเจ้าของข้อมูลให้ถูกต้องในกรณีที่เจ้าของข้อมูลเป็นผู้เยาว์
2. ประมวลผลข้อมูลส่วนบุคคลโดยไม่แจ้งวัตถุประสงค์ให้เจ้าของข้อมูลทราบ
3. ไม่ดำเนินการจัดให้มีการคุ้มครองข้อมูลส่วนบุคคล ในรูปแบบ Data Protection by Design and by Default, ไม่มีการแต่งตั้งตัวแทนของผู้ประมวลผลไว้ในสหภาพยุโรป, ไม่มีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ฯลฯ เป็นต้น

ระดับที่สอง เป็นระดับโทษรุนแรงมาก (Very Severe Penalties)

กล่าวคือ โทษปรับทางปกครองสูงสุดถึง 20,000,000 EUR หรือปรับมากถึง 4% ของมูลค่าการซื้อขายรวมทั่วโลกประจำปีของปีงบประมาณก่อน สำหรับกรณีของการฝ่าฝืนหลักการดังต่อไปนี้

ประการแรก หลักการพื้นฐานสำหรับการประมวลผลข้อมูลส่วนบุคคลตามที่กำหนดใน GDPR รวมถึงข้อกำหนดในการให้ความยินยอม (หลักการประมวลผลข้อมูล หลักการประมวลผลข้อมูลโดยชอบด้วยกฎหมาย หลักความยินยอม และหลักการประมวลผลข้อมูลส่วนตัวประเภทพิเศษหรือข้อมูลส่วนบุคคลที่มีความอ่อนไหว)

ประการที่สอง การฝ่าฝืนหรือละเมิดสิทธิของเจ้าของข้อมูลส่วนบุคคล (หลักความโปร่งใสและสิทธิในการเข้าถึงข้อมูลส่วนบุคคล สิทธิในการแก้ไขข้อมูล และสิทธิคัดค้านการประมวลผลข้อมูลส่วนบุคคลโดยอัตโนมัติ)

ประการที่สาม หลักการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้รับในประเทศที่สามหรือองค์กรระหว่างประเทศ

เมื่อพิจารณาแล้วจะเห็นว่า การกำหนดโทษทางปกครองแก่ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลส่วนบุคคลตามหลักการของกฎหมายระดับสากลจะเห็นว่า มีการกำหนดโทษไว้อย่างรุนแรงและมีอัตราค่าปรับที่สูงมาก เมื่อเปรียบเทียบกับกฎหมายของประเทศไทย ทั้งนี้สะท้อนภาพของการให้ความสำคัญแก่สิทธิ ในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลที่ถือว่าเป็นเรื่องที่สำคัญมากในสังคมตะวันตกนั่นเอง แต่โดยภาพรวมแล้ว ถือว่าการกำหนดโทษไม่ว่าในทางอาญา ในทางปกครอง

---

[290] Article. 83 GDPR - General conditions for imposing administrative fines

หรือในทางแพ่งนั้น ถือว่าประเทศไทยเราก็ได้ยอมรับเอาแนวคิดนี้มากำหนดไว้พอสมควรดังจะเห็นได้จากที่กล่าวมาในข้างต้น

ดังนั้น มาตรการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยในปัจจุบันนั้น มีลักษณะรูปแบบทั้งที่เป็นกฎหมายกลางที่มีหลักการคุ้มครองข้อมูลส่วนบุคคลทั่วไปในทุกมิติ นอกจากนี้ ยังมีการบัญญัติคุ้มครองไว้ในกฎหมายเฉพาะภาคส่วนอีกด้วย แต่ทว่ายังขาดการส่งเสริมให้มีการใช้รูปแบบการควบคุมกันเองของภาคธุรกิจ โดยเมื่อพิจารณาแล้วจะเห็นได้ว่าหลักการในการคุ้มครองข้อมูลส่วนบุคคลนั้น ได้รับอิทธิพลมาจากหลักสิทธิมนุษยชนตามกติการะหว่างประเทศและหลักการของกฎหมายต่างประเทศ โดยเฉพาะอย่างยิ่ง GDPR ที่สหภาพยุโรปได้ออกมาให้มีผลบังคับใช้ล่าสุด ซึ่งกติกาและหลักการที่กล่าวมาส่งผลต่อการกำหนดนิยามของคำว่าข้อมูลส่วนบุคคล ที่ไม่ได้มีการกำหนดไปถึงข้อมูลส่วนบุคคลของผู้ถึงแก่กรรมโดยเฉพาะซึ่งเป็นประเด็นปัญหาดังที่ได้กล่าวมาแล้วในตอนต้นซึ่งจะนำไปสู่การพัฒนาและปรับปรุงหลักการต่อไป นอกจากนี้ในประเด็นการกำหนดมาตรการตามกฎหมายก็ยังมีปัญหาอีกหลายประการทั้งในประเด็นการกำหนดสิทธิของเจ้าของข้อมูลหรือข้อจำกัดสิทธิของเจ้าของข้อมูลก็ยังมีประเด็นปัญหาที่จะต้องปรับปรุงแก้ไขต่อไป รวมไปถึงระบบการเยียวยาสิทธิของเจ้าของข้อมูลส่วนบุคคลที่ถูกล่วงละเมิดเช่นเดียวกัน ซึ่งจากสภาพเช่นนี้จะต้องยกระดับมาตรการและกลไกตามกฎหมายของเราให้ทัดเทียมกับกติกาสากล ดังที่จะได้ทำการเสนอแนะในบทต่อไป

นอกจากนี้ ประเด็นที่ต้องพิจารณาต่อมาคือ กลไกการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลที่กล่าวมาแล้วนี้ จะถูกดำเนินการบังคับใช้โดยองค์กรหลักตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ซึ่งก็คือคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ประเด็นสำคัญที่ควรพิจารณาต่อไปก็คือ ปัญหาความเป็นอิสระขององค์กรนั่นเอง เพราะคณะกรรมการชุดนี้ ถือเป็นองค์กรสำคัญที่ทำหน้าที่ในการบังคับใช้กฎหมายเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล การนำหลักการของ GDPR มาเป็นแนวทางในการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 นั้น ดังที่ได้กล่าวไว้ในบทที่ 4 แล้วว่า ส่วนหนึ่งที่อาจไม่ได้รับการพิจารณามากนักคือ การกำหนดโครงสร้างขององค์กรบังคับใช้กฎหมายที่เหมาะสม เนื่องจากระบบกฎหมายของการจัดองค์กรของภาครัฐในประเทศไทย ประกอบกับการไม่ได้ให้ความสำคัญกับโครงสร้างขององค์กรบังคับใช้กฎหมายที่เป็นอิสระ เช่นนี้ ย่อมทำให้กฎหมายไม่สามารถเป็นเครื่องมือในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลได้อย่างทั่วถึงและมีประสิทธิภาพ ดังนั้นในประการนี้จึงสมควรที่ในอนาคตจะได้มีการกำหนดให้มีองค์ประกอบของคณะกรรมการใหม่ โดยให้มีที่มาจากภาคประชาชน หรือภาคประชาสังคม รวมถึงองค์กรสื่อสารมวลชน เข้ามาเป็นกรรมการด้วย รวมไปถึงการกำหนดให้ผู้ที่เข้ามาดำรงตำแหน่ง

คณะกรรมการนั้น ควรจะได้ทำงานเต็มเวลาและไม่เป็นผู้ที่ดำรงตำแหน่งอื่น ในองค์กรอื่นด้วยในขณะเดียวกันเพื่อป้องกันปัญหาเรื่องการขัดกันแห่งผลประโยชน์และอิสระในการทำหน้าที่

จึงกล่าวโดยสรุปได้ว่า มาตรฐานของมาตรการและกลไกในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศไทย ที่ได้ยอมรับเอาหลักการต่าง ๆ ของต่างประเทศโดยเฉพาะกติกาสากลอันสำคัญ คือ GDPR นั้น ในภาพรวมถือว่าเป็นการยกระดับมาตรฐานได้ดีขึ้นพอสมควรแต่อย่างไรก็ดี ยังมีประเด็นที่ยังเป็นปัญหาอยู่บางเรื่องจึงสมควรที่จะได้มีการพัฒนามาตรการและกลไกในประเด็นเหล่านั้นต่อไป ซึ่งรายละเอียดจะกล่าวโดยสรุปและเสนอแนะในบทต่อไป

บทที่ 6

บทสรุปและข้อเสนอแนะ

6.1 บทสรุป

สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ถือเป็นสิทธิที่ก้าวผ่านมุมมองของการเป็นกรรมสิทธิเหนือข้อมูล ที่มองว่าผู้เก็บข้อมูลย่อมมีฐานะเป็นเจ้าของกรรมสิทธิในข้อมูล แต่ถือว่าสิทธินี้เป็นสิทธิในความเป็นส่วนตัวของเจ้าของข้อมูลในอันที่จะให้เปิดเผยหรือไม่ให้เปิดเผยเรื่องราวต่าง ๆ ของตน สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลจึงถือเป็นสิทธิมนุษยชนขั้นพื้นฐานที่มีความสำคัญเป็นอย่างยิ่ง โดยได้รับการรับรองและคุ้มครองโดยกฎหมายทั้งในระดับกติกาสากลและระบบกฎหมายภายในของประเทศไทยเองนับตั้งแต่ระดับกฎหมายรัฐธรรมนูญลงมา โดยธรรมชาติของสิทธิมนุษยชนประเภทนี้ มีลักษณะเป็นทั้งสิทธิในเชิงลบ (Status Nagativus) ที่ถือว่าสิทธิในความเป็นส่วนตัวนั้นจะต้องไม่ถูกแทรกแซงหรือล่วงละเมิดโดยรัฐหรือเอกชนบุคคลอื่น ๆ ในลักษณะของสิทธิที่จะอยู่โดยลำพัง (Right to be Let Alone) และชณะเดียวกันก็ถือว่าเป็นสิทธิในเชิงบวก (Status Positivus) คือ เจ้าของข้อมูลส่วนบุคคลผู้ซึ่งเป็นประธานแห่งสิทธินี้ย่อมที่จะมีอำนาจควบคุมข้อมูลส่วนบุคคลของตนได้ โดยจะต้องมีสิทธิที่จะทราบว่าข้อมูลส่วนบุคคลของตนนั้น ถูกเก็บรวมรวม ใช้ เปิดเผย หรือประมวลผลโดยใคร เพื่อวัตถุประสงค์ใด และจะต้องมีสิทธิที่จะคัดค้านการดำเนินการหากว่าเป็นการกระทำที่ไม่ถูกต้องหรือตนไม่ยินยอมให้กระทำการดังที่กล่าวมา รวมไปถึงเจ้าของข้อมูลจะต้องมีสิทธิในการควบคุมการไหลเวียนของข้อมูลส่วนบุคคลของตนด้วย และภายใต้ความเป็นสิทธิเชิงบวกเช่นนี้ รัฐจึงจะต้องเข้ามาดำเนินการให้มีการคุ้มครองสิทธิให้แก่ประชาชน แต่อย่างไรก็ดีสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลไม่ใช่สิทธิเด็ดขาด นั่นหมายความว่าในกรณีที่มีความจำเป็นเพื่อประโยชน์สาธารณะ รัฐย่อมสามารถออกมาตรการหรือกฎหมายมาจำกัดสิทธินี้ได้ภายใต้หลักความได้สัดส่วนและตามกรอบของบทบัญญัติแห่งรัฐธรรมนูญ

กล่าวได้ว่า ภายหลังการปฏิวัติอุตสาหกรรมครั้งที่ 4 สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลยิ่งทวีความสำคัญมากขึ้น ดังที่กล่าวกันว่าความรู้คืออำนาจ นั่นก็คือใครที่สามารถมีข้อมูลมากกว่าย่อมได้เปรียบในการบริหารจัดการ การค้าขาย และการพัฒนาด้านต่าง ๆ กล่าวได้ว่า ความมั่งคั่งในยุคโบราณ มาจากการที่ผู้มั่งคั่งสามารถสะสมทรัพยากรที่ดินได้มาก พอถึงยุคต่อมาหลังการ

ปฏิวัติอุตสาหกรรมครั้งแรกใครที่มีเครื่องจักรมากว่าและมีคุณภาพดีกว่าผู้นั้นย่อมเป็นผู้มั่งคั่งที่สุด แต่ในยุคปัจจุบันใครมีข้อมูลมากว่าหรือสามารถรวบรวมข้อมูลได้มากกว่า ผู้นั้นคือ ผู้ที่จะมั่งคั่งที่สุดนั่นเอง เราจึงเห็นภาพว่าในยุคแห่งการพัฒนาการอย่างก้าวหน้าและรวดเร็วเช่นนี้ จึงมีการแข่งขันและแก่งแย่งกันเพื่อครอบครองข้อมูลส่วนบุคคล ซึ่งภาวะเช่นนี้ย่อมทำให้เกิดการล่วงละเมิดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลกันมากยิ่งขึ้นทวีคูณ

จากการศึกษาพบว่า ด้วยเหตุข้างต้นนี้ นานาอารยประเทศจึงได้มีการพัฒนาหลักการเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลขึ้น แต่เนื่องจากความแตกต่างกันทั้งทางด้านแนวคิดและระบบกฎหมายทำให้หลักเกณฑ์ในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของแต่ละประเทศมีความแตกต่างกัน กรณีเช่นนี้ทำให้องค์กรเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD) ได้ริเริ่มออกหลักการคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นหลักการทั่วไปขึ้นมา ซึ่งก็คือ Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data โดยมีวัตถุประสงค์เพื่อให้ประเทศสมาชิกได้ใช้ดูแลการส่งหรือโอนข้อมูลระหว่างประเทศ การคุ้มครองข้อมูลส่วนบุคคลและการคุ้มครองสิทธิในความเป็นส่วนตัว เพื่อแก้ปัญหาความไม่เท่าเทียมกันของหลักการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของแต่ละประเทศซึ่งจะยังผลให้เป็นอุปสรรคขัดขวางการไหลเวียนของข้อมูลระหว่างประเทศ และเพื่อสร้างความเป็นหนึ่งเดียวกันของหลักการคุ้มครองข้อมูลส่วนบุคคลของประเทศสมาชิก โดยมีการกำหนดหลักการพื้นฐานไว้ดังนี้คือ 1) หลักข้อจำกัดในการเก็บรวบรวมข้อมูล 2) หลักคุณภาพของข้อมูล 3) หลักการกำหนดวัตถุประสงค์ในการจัดเก็บ 4) หลักข้อจำกัดในการนำไปใช้ 5) หลักการรักษาความมั่นคงปลอดภัยข้อมูล 6) หลักการเปิดเผยข้อมูล 7) หลักการมีส่วนร่วมของบุคคล 8) หลักความรับผิดชอบ ซึ่งรายละเอียดได้อธิบายไว้แล้วในตอนต้น

จากหลักการของ OECD ถือเป็นจุดเริ่มต้นสำคัญของนานาอารยประเทศในการออกมาตรการและกลไกทางกฎหมายขึ้นมาเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ต่อมาเมื่อสหภาพยุโรปได้มีการตรา Directive 95/46/EC ขึ้นมา กติกาสากลฉบับนี้ก็ได้มีผลกระทบเป็นอย่างมากต่อระบบการคุ้มครองสิทธิของประเทศต่าง ๆ ทั่วโลก รวมไปถึงประเทศมหาอำนาจอย่างประเทศสหรัฐอเมริกาก็ได้รับผลกระทบในเรื่องนี้ด้วยจนถึงขึ้นที่ต้องทำความตกลงกับสหภาพยุโรปในเรื่องของการโอนข้อมูลส่วนบุคคลระหว่างประเทศ และเมื่อต่อมาหลักการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปได้รับการพัฒนาอีกครั้งเป็น General Data Protection Regulation หรือ GDPR อันเป็นกติการะหว่างประเทศที่มีผลกระทบเป็นอย่างยิ่งไปยังทุกประเทศทั่วโลก

General Data Protection Regulation เป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลของพลเมืองที่อาศัยอยู่ในเขตสหภาพยุโรป ถูกพัฒนาขึ้นเพื่อตอบรับกระแสของการใช้อินเทอร์เน็ต ธุรกิจอี-คอมเมิร์ซ การโฆษณาและการตลาดออนไลน์ รวมถึงธุรกรรมต่าง ๆ ทุกประเภทในโลกยุคดิจิทัล

โดย General Data Protection Regulation ได้รวบรวมและพัฒนาหลักการขึ้นมาจากกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลของผู้บริโภคหลายฉบับ แต่เพิ่มบทลงโทษที่รุนแรงขึ้นกว่าเดิม เช่น การเสียค่าปรับที่มีจำนวนเงินสูงถึง 20 ล้านยูโร ดังที่ได้กล่าวไว้แล้ว นอกจากนี้ ยังระบุให้องค์กรหรือบริษัทที่เก็บรวบรวมข้อมูลของพลเมืองในสหภาพยุโรปต้องรายงานหรือแจ้งเหตุการณ์การล่วงละเมิด (Data Breach) ที่เกิดขึ้นต่อหน่วยงานกำกับดูแลที่เกี่ยวข้องและเจ้าของข้อมูลส่วนบุคคล รวมไปถึงแจ้งให้ทราบหรือตอบคำถามเกี่ยวกับการนำข้อมูลของเจ้าของข้อมูลส่วนบุคคลไปใช้หรือประมวลผลในลักษณะใด ๆ ก็ตาม ที่สำคัญคือ General Data Protection Regulation ทำให้ประเทศสมาชิกใช้กฎหมายการคุ้มครองข้อมูลส่วนบุคคลฉบับเดียวกัน ซึ่งช่วยให้เกิดความสะดวกต่อแนวปฏิบัติในการคุ้มครองสิทธิและต่อการดำเนินธุรกิจระหว่างกลุ่มประเทศสมาชิกอีกด้วย

จุดสำคัญของ General Data Protection Regulation ที่ส่งผลกระทบให้ประเทศไทยจะต้องมีการปรับปรุงกฎหมายคุ้มครองข้อมูลส่วนบุคคลก็คือ มีการกำหนดการใช้อำนาจนอกอาณาเขต (Extraterritorial Jurisdiction) คือ ข้อมูลส่วนบุคคลของสหภาพยุโรปอยู่ภายใต้ความคุ้มครองไม่ว่าจะอยู่ในที่ใดในโลก ซึ่งจะส่งผลให้ General Data Protection Regulation สามารถใช้บังคับไปถึงภายนอกอาณาเขตของสหภาพยุโรป รวมไปถึงประเทศไทยนั้นเอง

จากการศึกษาถึงพัฒนาการของการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย พบว่า การคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลเริ่มมีการกำหนดไว้ในรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2535 (แก้ไขเพิ่มเติม พุทธศักราช 2538) โดยได้บัญญัติรับรองสิทธิในความเป็นส่วนตัว” ในมาตรา 47 “สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัว ย่อมได้รับความคุ้มครอง” แต่ยุคแรกเริ่มนี้ ก็ไม่ได้มีการตรากฎหมายเฉพาะขึ้นมาคุ้มครองสิทธิแต่อย่างใด ลักษณะของการคุ้มครองสิทธิจึงอาศัยหลักการของประมวลกฎหมายแพ่งและพาณิชย์ในเรื่องละเมิด และหลักการของประมวลกฎหมายอาญาในส่วนของความผิดเกี่ยวกับการเปิดเผยความลับ เป็นกฎหมายหลักในการคุ้มครอง

ต่อมาภายหลังประเทศไทยประกาศใช้รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540 ก็ได้มีการบัญญัติรับรองสิทธิในความเป็นส่วนตัวไว้ในบทบัญญัติของรัฐธรรมนูญ มาตรา 34 “สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัว ย่อมได้รับความคุ้มครอง” และได้มีการตราพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 ออกมาเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลโดยมุ่งเน้นการคุ้มครองไปที่ข้อมูลส่วนบุคคลที่อยู่ในภาครัฐเท่านั้น แต่ไม่ได้มีการกำหนดให้อำนาจที่จะเข้าไปดูแลหรือคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในภาคเอกชนแต่อย่างใด และแม้ว่าจะมีการตรากฎหมายในลักษณะของกฎหมายมหาชนขึ้นมาอีกหลายฉบับเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ที่สำคัญก็เช่น พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544, พระราชบัญญัติว่าด้วยการประกอบธุรกิจข้อมูลบัตรเครดิต

พ.ศ.2545 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ฯลฯ เป็นต้น แต่ทว่า กฎหมายฉบับต่าง ๆ เหล่านี้มีลักษณะของการวางหลักการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลเฉพาะเรื่อง หรือเฉพาะประเภทของข้อมูลส่วนบุคคลเท่านั้น ไม่ได้มีลักษณะของการวางหลักการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในลักษณะทั่วไป หรือเป็นกฎหมายกลาง ที่ตราขึ้นเพื่อคุ้มครองสิทธิในข้อมูลทุกประเภทแต่อย่างใด

จนกระทั่งถึงวันที่ 28 กุมภาพันธ์ 2562 ที่ผ่านมา พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ได้ผ่านการพิจารณาของสภานิติบัญญัติแห่งชาติ โดยมีหลักการและเหตุผลว่า “เนื่องจากปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคล เป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว สามารถทำได้โดยง่าย สะดวก และรวดเร็ว รวมทั้งก่อให้เกิด ความเสียหายต่อเศรษฐกิจโดยรวมที่ใช้เทคโนโลยีดิจิทัลอย่างแพร่หลาย แม้ว่าจะได้มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลในบางเรื่อง แต่ก็ยังไม่มีหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป สมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้น จึงจำเป็นต้องตราพระราชบัญญัตินี้” ซึ่งเหตุผลของพระราชบัญญัตินี้สะท้อนภาพของปัญหาที่กล่าวมาข้างต้นได้เป็นอย่างดี

แต่อย่างไรก็ตาม เมื่อพิจารณาถึงสาระสำคัญมาตรการและกลไกในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ตามพระราชบัญญัติฉบับนี้รวมไปถึงกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับอื่น ๆ ที่เกี่ยวข้อง พบว่ามีประเด็นปัญหาสำคัญที่จะนำไปสู่ข้อเสนอแนะเพื่อปรับปรุงแก้ไขดังต่อไปนี้คือ

1. ประเด็นปัญหาเรื่องการกำหนดนิยามของคำว่า “ข้อมูลส่วนบุคคล” จะเห็นว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ของประเทศไทย ได้มีการนำหลักการของ General Data Protection Regulation มาใช้เป็นแนวทางในการกำหนดนิยามความหมายของคำว่าข้อมูลส่วนบุคคล ซึ่งมีการกำหนดให้หมายความว่า “ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ” ซึ่งการกำหนดนิยามที่ไม่ให้รวมถึงข้อมูลส่วนบุคคลของผู้ถึงแก่กรรมนั้น แม้จะสอดคล้องกับหลักการของ General Data Protection Regulation แต่มีผลทำให้สิทธิของผู้ถึงแก่กรรมในข้อมูลส่วนบุคคล รวมไปถึงทายาทนั้นจะไม่ได้รับความคุ้มครอง

ซึ่งประเด็นนี้ ในประเทศเยอรมนีก็ได้มีคำพิพากษาของศาลสูงของประเทศเยอรมนี (The German Federal Supreme Court (Bundesgerichtshof – “BGH”) ตัดสินในคดี Case no.III ZR 183/17 โดยตัดสินให้ Facebook ต้องยอมรับในสิทธิในข้อมูลส่วนบุคคลของผู้เสียชีวิต และ ใน

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศฝรั่งเศส ก็มีการบัญญัติรับรองหลักการเรื่องสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของผู้ตาย (Post Mortem Right to Privacy) ไว้ในมาตรา 40 (1) ของรัฐบัญญัติสาธารณรัฐดิจิตอล (The French Digital Republic Act ("Loi n°2016-1321 pour une République numérique")) โดยกำหนดให้ บุคคลมีสิทธิที่จะควบคุมการประมวลผลข้อมูลส่วนบุคคลของพวกเขาหลังจากการตาย โดยบุคคลสามารถให้ข้อมูลแก่ผู้ควบคุมข้อมูลทั่วไปหรือข้อบ่งชี้เฉพาะเกี่ยวกับการเก็บรักษา การลบและการเปิดเผยหรือส่งผ่านข้อมูลส่วนบุคคลของเขาหลังจากการเสียชีวิตได้ ภายใต้คำสั่งเช่นนั้น ในกรณีที่ผู้ควบคุมได้รับคำสั่งเฉพาะเจาะจงจากบุคคลในการประมวลผลข้อมูลของเขาหลังจากเสียชีวิต การใช้หรือประมวลผลข้อมูลนั้นก็ต้องเป็นไปตามความยินยอมโดยที่ไม่อาจจะกระทำเป็นอย่างอื่นไปได้

จากที่กล่าวมาจึงสมควรที่จะได้แก้ไขมาตรการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 เพื่อขยายของเขตนิยามของคำว่าข้อมูลส่วนบุคคลให้ครอบคลุมไปถึงสิทธิในความเป็นส่วนตัวของผู้ตายหรือผู้เสียชีวิตต่อไป

2. ประเด็นเรื่องข้อมูลที่มีความอ่อนไหว ไม่ว่าจะเป็นข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็น ทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลซึ่งตามหลักการสากลควรได้รับความคุ้มครองเป็นพิเศษที่เข้มข้นมากกว่าข้อมูลอื่น ๆ แต่เมื่อพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล และมีเพียงการกำหนดให้ต้องมีการขอความยินยอมจากเจ้าของข้อมูล ซึ่งในการขอความยินยอมนั้นก็ยังไม่ได้มีการกำหนดรายเอียดอันเป็นแนวปฏิบัติออกมาว่าจะแตกต่างจากการขอความยินยอมในกรณีข้อมูลส่วนบุคคลทั่วไปอย่างไร นอกจากนี้ในมาตรา 26 (5) (จ) ได้กำหนดหลักการยกเว้นสำหรับกิจการ "เพื่อประโยชน์สาธารณะที่สำคัญ โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล" ให้สามารถเก็บข้อมูลและใช้ข้อมูลได้โดยไม่ต้องได้รับความยินยอมอย่างชัดแจ้ง ก็เท่ากับเป็นการเปิดช่องให้กิจการของหน่วยงานรัฐทั้งหลาย ยกประโยชน์สาธารณะขึ้นมาอ้างได้ว่า ภารกิจของหน่วยงานของตนนั้น มีความสำคัญในลักษณะเป็นประโยชน์สาธารณะ ซึ่งก็จะมีผลทำให้ข้อมูลที่มีความอ่อนไหว ก็จะไม่ได้รับการคุ้มครองจากการสอดส่องของภาครัฐได้เลย ดังนั้นในการตีความคำว่า “ประโยชน์สาธารณะที่สำคัญ” อันจะเกิดขึ้นต่อไปในอนาคตนั้น คณะกรรมการข้อมูลส่วนบุคคล ซึ่งเป็นหน่วยงานที่เกี่ยวข้องกับการตีความบังคับใช้กฎหมายฉบับนี้ ควรจะตระหนักถึงเจตนารมณ์ของกฎหมายและให้ความสำคัญต่อความปลอดภัยของข้อมูลของประชาชนด้วยในการออกประกาศมาอธิบายขยายความในประเด็นนี้ ว่า อย่างไรถือเป็นประโยชน์สาธารณะที่สำคัญ และอย่างไรถือว่าเป็นมาตรการที่เหมาะสมเพื่อคุ้มครอง

นอกจากนี้ ในส่วนของข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) ที่อยู่ในความครอบครองของหน่วยงานราชการนั้น สมควรที่จะได้มีการแก้ไขพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 วางหลักการคุ้มครองเป็นการเฉพาะเพื่อให้เป็นมาตรฐานเดียวกันกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ต่อไป

3. ประเด็นปัญหาในเรื่องสิทธิในข้อมูลส่วนบุคคลของผู้เยาว์ จากการศึกษาพบว่า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ได้บัญญัติรับรองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของเด็กหรือผู้เยาว์ไว้เช่นเดียวกับหลักการสากลและหลักกฎหมายของต่างประเทศ โดยในชั้นของการร่างกฎหมายนั้นได้นำเอาแนวคิดและหลักการนี้มาใช้เป็นกรอบในการยกร่างกฎหมาย โดยในบทบัญญัติของมาตรา 20 มีการบัญญัติสาระสำคัญไว้ว่า ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ซึ่งยังไม่บรรลุนิติภาวะโดยการสมรสหรือไม่มีฐานะเสมือนดังบุคคลซึ่งบรรลุนิติภาวะแล้ว การขอความยินยอมจากเจ้าของของมูลส่วนบุคคลในการที่จะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้น จะต้องดำเนินการดังต่อไปนี้

1) ในกรณีที่การให้ความยินยอมของผู้เยาว์ไม่ใช่การใด ๆ ซึ่งผู้เยาว์อาจให้ความยินยอมโดยลำพัง การนั้นจะต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ด้วย

2) ในกรณีที่ผู้เยาว์มีอายุเกินไม่เกินสิบปี ให้ขอความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์

ซึ่งหลักการขอความยินยอมนี้นำมาใช้บังคับกับการถอนความยินยอมของเจ้าของข้อมูลส่วนบุคคล, การแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ, การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล, การร้องเรียนของเจ้าของข้อมูลส่วนบุคคล และการอื่นใดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ด้วย

ในประเด็นนี้ หากพิจารณาจากสถานการณ์ปัจจุบันในมิติทางเทคโนโลยี หรือสภาพทางปฏิบัติของการใช้งาน โดยเฉพาะอย่างยิ่งการใช้งานบริการออนไลน์ต่าง ๆ ที่ผู้เยาว์อาจเข้าถึงและใช้การได้เอง รวมทั้งเพื่อเหตุผลของความยืดหยุ่นและความรวดเร็วในทางปฏิบัติ แต่เพื่อสร้างความสมดุลกับการคุ้มครองข้อมูลของผู้เยาว์การกำหนดหลักการเรื่องความยินยอม ในกรณีของเจ้าของข้อมูลส่วนบุคคลเป็นเด็กหรือผู้เยาวน์นี้จึงควรจำแนกความยินยอมเป็นสองกรณี ได้แก่ กรณีที่เด็กสามารถยินยอมได้เอง และกรณีที่เด็กต้องขอความยินยอมจากผู้ใหญ่

โดยเฉพาะในส่วนของการที่จะกำหนดให้ผู้เยาว์สามารถตัดสินใจยินยอมด้วยตนเอง ก็จะต้องมีการวางเงื่อนไขเพื่อคุ้มครองเด็ก ว่าแม้อาจให้ความยินยอมเกี่ยวกับข้อมูลส่วนบุคคลของตนเองได้ โดยการขอความยินยอมนั้นต้องอยู่ภายใต้เงื่อนไข เช่น ผู้เยาว์มีความเข้าใจในวัตถุประสงค์ ผลกระทบของการเก็บประมวลผล และใช้ข้อมูลส่วนบุคคล นอกจากนี้ ยังต้องพิจารณาว่าผู้เยาว์อยู่ภายใต้แรงกดดันหรืออิทธิพลใดหรือไม่ ดังนั้นจะเห็นได้ว่า ในอนาคตหากจะต้องมีการพิจารณาปรับปรุงแก้ไข

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ประเด็นเรื่องนี้จึงจะเป็นประเด็นที่สมควรจะได้พัฒนาหลักการของมาตรา 20 โดยควรกำหนดเพิ่มเติมไปด้วยว่า แม้ผู้เยาว์จะสามารถให้ความยินยอมได้เองในกรณีที่อาจให้ความยินยอมโดยลำพังได้ตามที่บัญญัติไว้ในมาตรา 22 มาตรา 23 หรือมาตรา 24 แห่งประมวลกฎหมายแพ่งและพาณิชย์ แต่ผู้เยาว์จะต้องไม่ได้อยู่ภายใต้แรงกดดันหรืออิทธิพลใด ๆ และมีความเข้าใจในวัตถุประสงค์ ผลกระทบ ของการเก็บประมวลผล และใช้ข้อมูลส่วนบุคคลของตนด้วย

4. ประการที่สี่ประเด็นปัญหาการคุ้มครองข้อมูลส่วนบุคคลของผู้ต้องขัง

สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของผู้กระทำความผิดในทางอาญาโดยเฉพาะผู้ที่ถูกคำพิพากษาถึงที่สุดให้เป็นผู้กระทำผิดและให้ลงโทษจำคุก ฐานะของบุคคลนั้นจะกลายเป็นผู้ต้องขัง และอยู่ภายใต้กฎหมายอีกฉบับก็คือ พระราชบัญญัติราชทัณฑ์ พ.ศ.2560 ที่ตราขึ้นมาใหม่โดยมีวัตถุประสงค์ในการบังคับโทษเป็นสำคัญ และแม้ว่ามีความพยายามยกระดับของระบบการบังคับโทษเพื่อให้เป็นการแก้ไข บำบัด ฟื้นฟู และพัฒนาพฤตินิสัยของผู้ต้องขัง ให้เป็นไปตามหลักการสากลดังที่ได้กล่าวไว้แล้วก็ตาม แต่ ประเด็นเรื่องการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนั้น ก็ไม่ได้มีการกำหนดห้ามเจ้าหน้าที่ราชทัณฑ์ หรือเรือนจำที่เป็นหน่วยงานในสังกัด ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ต้องขังแต่อย่างใด ประเด็นข้อน่ากังวลจึงอยู่ที่ว่า แม้พระราชบัญญัติราชทัณฑ์ พ.ศ.2560 จะมุ่งเน้นการปฏิบัติต่อผู้ต้องขังไปในทิศทางที่จะแก้ไข บำบัด ฟื้นฟู และพัฒนาพฤตินิสัย อันจะทำให้มีการส่งเสริมในการฝึกอบรมต่าง ๆ แก่ผู้ต้องขังทั้งในและนอกเรือนจำ ซึ่งอาจจะมีการออกประกาศนียบัตรเพื่อรับรองคุณวุฒิทางวิชาการหรือวิชาชีพให้ กรณีเช่นนี้หากในใบรับรองคุณวุฒิได้มีการเขียนข้อความไว้ในทำนองว่าเป็นการฝึกอบรมในฐานะผู้ต้องขัง หรือฝึกอบรมในเรือนจำแล้ว ย่อมเป็นการเปิดเผยข้อมูลส่วนบุคคลของผู้ต้องขังทันที และกรณีนี้ สิทธิของผู้ต้องขังอันเป็นสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลย่อมไม่ได้รับความคุ้มครอง ทั้งจาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ที่ไม่ใช้บังคับกับการดำเนินงานตามกระบวนการยุติธรรมทางอาญา อีกทั้งยังไม่ได้รับความคุ้มครองจากพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 ที่ไม่ได้บัญญัติรับรองสิทธิไปถึงกรณีนี้

ในประเด็นนี้จึงสมควรที่จะได้มีการกำหนดมาตรการเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของผู้กระทำความผิดในทางอาญาที่อยู่ในฐานะผู้ต้องขังต่อไป

5. ประการที่ห้าประเด็นปัญหาในเรื่องมาตรการคุ้มครองข้อมูลส่วนบุคคลนั้นจะเห็นได้ว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ได้นำเอามาตรการต่าง ๆ ของ GDPR มากำหนดไว้ในกฎหมาย แต่อย่างไรก็ดี สำหรับมาตรการที่เรียกว่า Privacy by Design หรือ การกำหนดหน้าที่

ให้ผู้ควบคุมข้อมูลมีหน้าที่บูรณาการหลักการคุ้มครองข้อมูลทั้งในขั้นวางแผนและขั้นปฏิบัติการ นั้น กฎหมายของประเทศไทยเราไม่ได้มีการกำหนดหลักการนี้ไว้

กล่าวคือ ใน General Data Protection ที่ได้มีการพัฒนาต่อมาจาก EU Directive 95/46/EC มีการกำหนดหลักการใหม่ขึ้นมาเพิ่มเติมเพื่อให้การคุ้มครองข้อมูลส่วนบุคคลนั้นสามารถก้าวทันยุคสมัยของการเปลี่ยนแปลงทางเทคโนโลยีดิจิตอล นั้นคือ มีการกำหนดหลักการให้ผู้ควบคุมข้อมูลควรพิจารณาเลือกจัดเก็บข้อมูลเท่าที่จำเป็นตามวัตถุประสงค์ของการใช้ที่แจ้งให้กับเจ้าของข้อมูลทราบโดยไม่ควรเก็บข้อมูลมากเกินไป (Excessive) โดยจะมีการกำหนดหน้าที่ให้ผู้ควบคุมข้อมูลมีหน้าที่บูรณาการหลักการคุ้มครองข้อมูลทั้งในขั้นวางแผนและขั้นปฏิบัติการ (Privacy by Design หรือ Data Protection by Design) กล่าวคือ จะต้องให้ความสำคัญกับสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของเจ้าของข้อมูลตั้งแต่ในชั้นของการออกแบบเทคโนโลยีที่เกี่ยวข้องกับการเก็บรวมรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลแล้ว โดยหน่วยงานหรือองค์กรที่เกี่ยวข้องกับข้อมูลส่วนบุคคลจะต้องตระหนักในความสำคัญของข้อมูล โดยเริ่มจากการออกแบบบริการ ที่คิดคำนึงถึงการป้องกันข้อมูลตั้งแต่แรก ไม่ใช่ออกแบบบริการแล้วจึงค่อยมาคิดเพิ่มเติมในเรื่องการปกป้องคุ้มครองข้อมูลส่วนบุคคล และนอกจากนี้ ในการออกแบบบริการที่ต้องคำนึงถึงสิทธิในข้อมูลส่วนบุคคลนั้นจะต้องมีการใช้มาตรการทางเทคนิคที่เหมาะสม ทันสมัย และมีประสิทธิภาพในการปกป้องข้อมูลส่วนบุคคลด้วย

หลักการเรื่องนี้ ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ของประเทศไทยไม่ได้มีการกำหนดไว้หรือกล่าวถึง ดังนั้น อาจเป็นเหตุที่ทำให้สหภาพยุโรปมองกว่ากฎหมายของประเทศไทยไม่มีมาตรฐานการคุ้มครองข้อมูลที่ทัดเทียมหรือเทียบเท่า อันจะนำไปสู่เหตุแห่งการออกมาตรการต่าง ๆ มากระทบต่อประเทศไทยในโอกาสข้างหน้าก็ได้ ดังนั้นจึงสมควรที่จะมีการเพิ่มเติมหลักการเรื่องนี้ไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลต่อไป

6. ประการที่หก แม้ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ได้มีการกำหนดให้สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคลก็ตาม แต่ทว่าไม่ได้มีการเขียนให้ชัดเจนลงไปว่าหมายความรวมถึงการค้ดค้านการประมวลผลข้อมูลโดยอัตโนมัติด้วย ซึ่งอาจจะเป็นประเด็นปัญหาที่ต้องตีความกันต่อไป

สำหรับหลักการคัดค้านการประมวลผลข้อมูลโดยอัตโนมัตินี้ ถือเป็นสิทธิเกี่ยวกับการตัดสินใจด้วยวิธีการอัตโนมัติและการใช้ข้อมูลเพื่อการวิเคราะห์พฤติกรรมบุคคล (Profiling) ปรากฏอยู่ใน General Data Protection Article 22 โดยเจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะไม่ถูกประมวลผลข้อมูลส่วนบุคคลของตนด้วยวิธีการอัตโนมัติเพียงอย่างเดียวเท่านั้น ซึ่งรวมไปถึงการนำข้อมูลมาใช้ในการวิเคราะห์พฤติกรรมบุคคลนั้น (Profiling) ที่อาจก่อให้เกิดผลทางกฎหมายเกี่ยวกับตนหรือส่งผลที่มีความสำคัญในระดับเดียวกันด้วย อย่างไรก็ตาม สิทธิในข้อนี้มีข้อยกเว้นอยู่ กล่าวคือ

หากเป็นไปเพื่อการเข้าสู่การทำสัญญาหรือเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคล หรือได้รับความยินยอมของเจ้าของข้อมูลส่วนบุคคลอย่างชัดแจ้งแล้ว เป็นต้น ในประเด็นนี้จึงสมควรที่ประเทศไทยจะได้มีการแก้ไขเพิ่มเติมหลักการคัดค้านการประมวลผลข้อมูลโดยอัตโนมัตินี้ให้ชัดเจนลงในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ต่อไป

7. ประเด็นปัญหาในเรื่องหลักความรับผิดชอบ (Accountability) กล่าวคือ ผู้ควบคุมข้อมูลส่วนบุคคล เป็นผู้ที่มีภาระความรับผิดชอบที่จะต้องแสดงให้เห็นว่าตนสามารถปฏิบัติตามหลักการคุ้มครองส่วนบุคคลได้ ทั้งนี้ หลักการข้อนี้สะท้อนถึงเจตนารมณ์ของการคุ้มครองข้อมูลส่วนบุคคลมากกว่าที่จะเป็นการวางกฎเกณฑ์ที่ชัดเจนตายตัวเอาไว้ แต่เป็นหลักการที่เรียกร้องให้มีการปฏิบัติให้เป็นไปตามหลักการอันจะเป็นพื้นฐานสำคัญสำหรับการสร้างแนวทางปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลที่ดีต่อไป หลักการนี้เป็นหลักการที่มีอยู่ทั้งใน OECD Guildeline และ GDPR รวมถึงกฎหมายของต่างประเทศที่สำคัญดังที่ได้กล่าวมาแล้ว แต่สำหรับประเทศไทยไม่ได้มีการบัญญัติหลักการนี้ไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กรณีจึงสมควรที่จะได้มีการแก้ไขเพิ่มเติมหลักการนี้ต่อไป เพื่อให้กฎหมายไทยได้มาตรฐานการยอมรับว่าทัดเทียมและเทียบเท่ากับการคุ้มครองข้อมูลส่วนบุคคลของนานาประเทศ

8. ประเด็นปัญหาความไม่สอดประสานกันในส่วนของกฎหมายเฉพาะที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย ตัวอย่างเช่น พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 หรือ พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ.2550 เช่นนี้ควรจะได้มีการกำหนดหลักการให้สอดคล้องกันกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ทั้งในด้านของการกำหนดนิยามความหมาย รวมถึงมาตรการในการจัดการข้อมูลส่วนบุคคลที่เป็นการคุ้มครองสิทธิ เพื่อให้ระบบของการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของทั้งกฎหมายกลางและกฎหมายเฉพาะเป็นไปในทิศทางเดียวกัน ตัวอย่างเช่น

1) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กำหนดให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล มีหน้าที่ตามที่กล่าวไว้ในมาตรา 41 ซึ่งเป็นเรื่องที่มีความสำคัญต้องอาศัย ผู้ที่มีความรู้และประสบการณ์ในการปฏิบัติหน้าที่ดังกล่าว ซึ่งเมื่อพิจารณาเปรียบเทียบกับพระราชบัญญัติข้อมูลข่าวสารของราชการแล้ว เห็นว่าไม่ได้มีการกำหนดตำแหน่งหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไว้แต่อย่างใด

แม้ว่า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 41 นั้น จะได้มีการกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของตน ในกรณี (1) ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นหน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด

แต่ประเด็นปัญหาก็คือ ประการแรกยังไม่ได้มีการออกประการกำหนดออกมาจึงยังไม่ชัดเจนว่าหน่วยงานใดบ้างที่จะต้องมีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และประการที่สอง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลนั้น กำหนดไว้ในมาตรา 4 ว่าไม่ได้ใช้บังคับไปถึงการดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมไปถึง การดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดีการบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา นั่นหมายความว่า แม้จะมีการออกประกาศกำหนดออกมา ก็ไม่ครอบคลุมไปถึง หน่วยงานราชการ ที่ไม่ได้อยู่ใต้บังคับของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 จึงไม่ต้องปฏิบัติตามนั่นเอง

ส่วนคำว่า “หน่วยงานของรัฐ” ตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 หมายความว่า ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ ส่วนราชการสังกัดรัฐสภา ศาลเฉพาะในส่วนที่ไม่เกี่ยวกับการพิจารณาพิพากษาคดี องค์กรควบคุมการประกอบวิชาชีพ หน่วยงานอิสระของรัฐและหน่วยงานอื่นตามที่กำหนด ดังนั้น การกำหนดให้ต้องระบุให้ส่วนราชการต้องมีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล จึงจะทำให้ภาครัฐ ต้องกำหนดให้มีตำแหน่งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้ครอบคลุมหน่วยงานมากกว่าอันจะทำให้สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ที่อยู่ในความครอบครองของรัฐมีมาตรฐานในการคุ้มครองมากขึ้น เช่นนี้ จึงสมควรที่จะได้มีการแก้ไขพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 ให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในการทำหน้าที่คุ้มครองข้อมูลข่าวสารส่วนบุคคลที่อยู่ในภาครัฐด้วย

2) ในส่วนของพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ.2550 ยังไม่ได้มีการบัญญัตินิยามของข้อมูลส่วนบุคคลเกี่ยวกับสุขภาพไว้ จึงทำให้เกิดปัญหาไม่สามารถกำหนดความหมายและขอบเขตการคุ้มครองสิทธิเกี่ยวกับข้อมูลส่วนบุคคลด้านสุขภาพที่ชัดเจน ซึ่งอาจทำให้เกิดความสับสนในการตีความและการใช้บังคับกฎหมาย ดังนั้น จึงควรแก้ไขเพิ่มเติมพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 โดยกำหนดคำนิยามของคำว่า “ข้อมูลส่วนบุคคลเกี่ยวกับสุขภาพ” ไว้ให้ชัดเจน

9. ประเด็นปัญหาเรื่องข้อจำกัดการคุ้มครองข้อมูลส่วนบุคคล กล่าวคือ แม้ประเทศไทยจะมีการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ออกมาเป็นกฎหมายกลาง ที่กำหนดหลักการคุ้มครองข้อมูลส่วนบุคคลในทุกประเภท อันถือได้ว่าเป็นการยกระดับมาตรฐานของการคุ้มครองข้อมูลส่วนบุคคลให้มีมาตรฐานทัดเทียมและเทียบเท่ากับนานาอารยประเทศแล้วก็ตาม แต่ทว่า ในช่วงระยะเวลาใกล้เคียงกัน สภานิติบัญญัติแห่งชาติ (สนช.) ก็ได้ผ่านกฎหมายเกี่ยวกับความมั่นคงออกมาอีกหลายฉบับ อันมีกฎหมายที่สำคัญซึ่งให้อำนาจแก่รัฐในอันที่จะสามารถใช้อำนาจล่วงละเมิดข้อมูลส่วนบุคคลได้ ได้แก่ พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 โดย

กฎหมายฉบับนี้ฝ่ายรัฐอ้างว่าเป็นกฎหมายความสำคัญที่จะช่วยสร้างความพร้อมให้กับประเทศไทยในการรับมือความเสี่ยงและภัยคุกคามทางไซเบอร์ยุคใหม่ จากความก้าวหน้าของเทคโนโลยีดิจิทัลที่อาจส่งผลกระทบสร้างความเสียหายต่อความมั่นคงประเทศและเศรษฐกิจโดยรวม ตลอดจนถึงการคุ้มครองข้อมูลประชาชนทั่วไป อีกทั้งจะช่วยสร้างความมั่นใจในการใช้เทคโนโลยีดิทัล หนุนการขับเคลื่อนประเทศไทยเปลี่ยนผ่านสู่ยุคดิจิทัลอย่างมีเข้มแข็งและยั่งยืน

แต่อย่างไรก็ดี กฎหมายฉบับนี้มีปัญหาเกี่ยวกับการให้อำนาจแก่เจ้าหน้าที่ในการดำเนินการตรวจสอบภัยคุกคามทางไซเบอร์โดยทันทีและไม่ต้องยื่นคำร้องต่อศาล โดยมีการกำหนดนิยามของคำว่าภัยคุกคามไซเบอร์ไว้ไม่ชัดเจน และมีลักษณะของการเปิดโอกาสให้มีการตีความอย่างกว้างขวางและมีการให้อำนาจแก่เจ้าหน้าที่อย่างกว้างขวางเช่นกันในอันที่จะจัดการกับภัยคุกคามนั้น ซึ่งหมายความว่า เจ้าหน้าที่ตามกฎหมายสามารถอ้างอำนาจตามกฎหมายฉบับนี้ล่วงละเมิดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลได้นั่นเอง

นอกจากพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ฯ แล้ว สภานิติบัญญัติแห่งชาติยังได้ผ่านพระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ.2562 ซึ่งเป็นกฎหมายที่ให้อำนาจแก่เจ้าหน้าที่และหน่วยงานของรัฐ (สำนักข่าวกรองแห่งชาติ) มีอำนาจใช้เครื่องมืออิเล็กทรอนิกส์ เครื่องมือทางวิทยาศาสตร์ เครื่องโทรคมนาคม หรือเทคโนโลยีอื่นใด เพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคล

โดยลักษณะของการกำหนดอำนาจตามกฎหมายฉบับนี้ ให้แก่สำนักข่าวกรองแห่งชาตินั้นเป็นการมอบอำนาจให้ตามกฎหมายที่ไม่ได้ผ่านกระบวนการในการกลั่นกรองและตรวจสอบการใช้อำนาจจากองค์กรอื่นในลักษณะที่เป็นสากล เช่น องค์กรศาล แต่เป็นการใช้อำนาจในลักษณะที่เป็นการเสนอ และตรวจสอบควบคุม ภายในหน่วยงานเดียวกันเอง ทั้งที่เป็นเรื่องที่เกี่ยวข้องกับการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล นอกจากนี้ยังจะสุ่มเสี่ยงต่อการใช้อำนาจที่ไม่สุจริตและไม่ชอบธรรม และการใช้อำนาจเกินสมควรแก่เหตุ อันเป็นการละเมิดสิทธิเสรีภาพของประชาชน

ประเด็นสำคัญอยู่ที่ว่า หากประเทศไทย โดยเจ้าหน้าที่ของรัฐหรือหน่วยงานของรัฐในด้านความมั่นคงใช้อำนาจตามกฎหมายที่กล่าวมาข้างต้น ไปล่วงละเมิดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลแล้ว หากบุคคลนั้นเป็นพลเมืองของสหภาพยุโรปที่ได้รับความคุ้มครองนอกอาณาเขตโดยหลักการของ GDPR หรือแม้ว่าบุคคลนั้นจะเป็นประชาชนชาวไทยที่ได้รับความคุ้มครองภายใต้หลักการของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ที่ประเทศไทยตราขึ้นเพื่อให้มีมาตรฐานการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลทัดเทียมและเท่ากับมาตรฐานของ GDPR แต่ถูกล่วงละเมิดข้อมูลส่วนบุคคลโดยเจ้าหน้าที่ของรัฐหรือหน่วยงานของรัฐตามกฎหมายที่เกี่ยวข้องกับความมั่นคงข้างต้น กรณีอาจเกิดปัญหาเช่นเดียวกันกับการที่สหภาพยุโรปไม่ยอมรับหลักการคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกา ในกรณีของการตัดสินว่า Safe Harbour

ไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เทียบเท่าสหภาพยุโรป ทั้งนี้เป็นเพราะรัฐได้ดำเนินการสอดส่องข้อมูลส่วนบุคคลของประชาชนนั่นเอง ประเด็นนี้จึงสมควรที่ผู้บังคับใช้กฎหมายข้างต้นจะต้องระมัดระวัง ไม่เช่นนั้นอาจสร้างความเสียหายแก่ผลประโยชน์ทางการค้ามหาศาลก็เป็นได้

10. ปัญหาความเป็นอิสระขององค์กรที่ทำหน้าที่สำคัญในการบังคับใช้กฎหมาย โดยในการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 นั้น ประเด็นที่อาจไม่ได้รับการพิจารณามากนักคือประเด็นการกำหนดโครงสร้างขององค์กรบังคับใช้กฎหมายที่เหมาะสม เนื่องจากเหตุผลว่าด้วยระบบกฎหมายของการจัดองค์กรของภาครัฐในประเทศไทยหรืออาจจะเหตุไม่ได้ให้ความสำคัญกับโครงสร้างขององค์กรบังคับใช้กฎหมายที่เป็นอิสระมากนัก จึงทำให้สัดส่วนของคณะกรรมการไม่ได้มีภาคประชาสังคมเข้าไปมีส่วนร่วมอย่างชัดเจน อีกทั้งคณะกรรมการยังมีที่มาจากฝ่ายรัฐเสียเป็นส่วนใหญ่ ทำให้เกิดความน่ากังวลของการมีกฎหมายบัญญัติรับรองสิทธิแต่ปราศจากหน่วยงานการบังคับใช้หรือกลไกที่มีอิสระ จนอาจทำให้การคุ้มครองสิทธินี้ ไม่ได้เป็นไปอย่างทั่วถึงและมีประสิทธิภาพเพียงพอ ดังนั้นจึงสมควรที่ในอนาคตจะได้มีการกำหนดให้มีองค์ประกอบของคณะกรรมการใหม่ โดยให้มีที่มาจากภาคประชาชน หรือภาคประชาสังคม รวมถึงองค์กรสื่อสารมวลชน หรือองค์กรอื่น ๆ ที่จะสะท้อนได้ถึงการมีส่วนร่วมของประชาชน ให้เข้ามาเป็นกรรมการด้วย รวมไปถึงการกำหนดให้ผู้ที่เข้ามาดำรงตำแหน่งคณะกรรมการนั้น ควรจะได้ทำงานเต็มเวลาและไม่เป็นผู้ที่ดำรงตำแหน่งอื่น ในองค์กรอื่นด้วยในขณะเดียวกันเพื่อป้องกันปัญหาเรื่องการขัดกันแห่งผลประโยชน์และอิสระในการทำหน้าที่

11. ประเด็นปัญหาเรื่องกลไกการเยียวยาสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของผู้พิการหรือทุพพลภาพ

ในประเด็นนี้จะเห็นว่า กลไกการเยียวยาผู้ถูกละเมิดสิทธิตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ได้มีการกำหนดมาตรการไว้ในกฎหมายผ่านการบังคับใช้โดยคณะกรรมการข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการข้อมูลส่วนบุคคล โดยมีการกำหนดทั้งในส่วนของโทษทางอาญา และโทษทางปกครอง รวมไปถึงมีการกำหนดความรับผิดในทางแพ่งไว้ด้วย นอกจากนี้ยังมีการกำหนดกระบวนการให้ต้องร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญที่ได้รับการพิจารณาแต่งตั้งจากคณะกรรมการข้อมูลส่วนบุคคล ซึ่งคณะกรรมการชุดนี้จะมีอำนาจในการตรวจสอบและออกคำสั่งตามที่มีการร้องเรียน

โดยให้สิทธิร้องเรียนแก่เจ้าของข้อมูลที่ถูกล่วงละเมิด กล่าวคือ เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ฝ่าฝืน หรือไม่ปฏิบัติตามพระราชบัญญัตินี้ กฎกระทรวงหรือประกาศที่ออกตามพระราชบัญญัติ

อย่างไรก็ดี จากกรณีข้างต้น ประเด็นปัญหาจึงมีว่า สิทธิของผู้พิการหรือทุพพลภาพ ซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล อาจจะมีปัญหาเรื่องของการเข้าถึงสิทธิอันเป็นกลไกการเยียวยานี้ เช่นนี้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 จึงควรที่จะมีการวางหลักการในการส่งเสริมการเข้าถึงสิทธิของบุคคลเหล่านี้ด้วย

6.2 ข้อเสนอแนะ

1. ควรมีการแก้ไขพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 เพื่อขยายขอบเขตนิยามของคำว่าข้อมูลส่วนบุคคลให้ครอบคลุมไปถึงสิทธิในความเป็นส่วนตัวของผู้ตายหรือผู้เสียชีวิตด้วย โดยควรให้มีการแก้ไขเพิ่มเติม มาตรา 6 ให้มีข้อความดังนี้

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม และให้หมายรวมถึงข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย”

2. ประเด็นข้อมูลที่มีความอ่อนไหว ควรได้รับความคุ้มครองเป็นพิเศษที่เข้มข้นมากกว่าข้อมูลอื่น ๆ แต่เมื่อพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล 26 (5) (จ) กำหนดยกเว้นสำหรับกิจการ "เพื่อประโยชน์สาธารณะที่สำคัญ" ให้สามารถเก็บข้อมูลและใช้ข้อมูลได้โดยไม่ต้องได้รับความยินยอมอย่างชัดแจ้ง ก็เท่ากับเป็นการเปิดช่องให้กิจการของหน่วยงานรัฐทั้งหลาย ยกประโยชน์สาธารณะขึ้นมาอ้างได้ว่าภารกิจของหน่วยงานของตนนั้น มีความสำคัญในลักษณะเป็นประโยชน์สาธารณะ ซึ่งก็จะมีผลทำให้ข้อมูลที่มีความอ่อนไหว ก็จะไม่ได้รับการคุ้มครองจากการสอดส่องของภาครัฐได้เลย ดังนั้นในการบังคับใช้กฎหมายฉบับนี้ จึงควรตีความคำว่า “ประโยชน์สาธารณะที่สำคัญ” บนพื้นฐานของการตระหนักถึงเจตนารมณ์ของกฎหมายและให้ความสำคัญต่อความปลอดภัยของข้อมูลส่วนบุคคลของประชาชนเป็นสำคัญ

นอกจากนี้ ในส่วนของข้อมูลที่มีความอ่อนไหวที่อยู่ภายใต้อำนาจของหน่วยงานราชการตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 ซึ่งไม่ได้มีการกำหนดมาตรฐานในการคุ้มครองไว้เป็นพิเศษ กรณีเช่นนี้ สมควรที่จะได้มีการแก้ไขเพิ่มเติม ในมาตรา 24/1 ว่า

> ในการจัดระบบข้อมูลข่าวสารตามมาตรา 23 และ การเปิดเผยข้อมูลข่าวสารตามมาตรา 24 แห่งพระราชบัญญัตินี้ หากข้อมูลข่าวสารนั้นเป็นข้อมูลข่าวสารส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด

ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกัน ให้หน่วยงานของรัฐกระทำโดยระมัดระวังและจะให้เกิดผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลอย่างร้ายแรงเกินสมควรมิได้

3. ในประเด็นเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของผู้เยาว์ควรมีการแก้ไขพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 20 (1) โดยให้มีการเพิ่มข้อความว่า

“สำหรับกรณีที่ผู้เยาว์อาจให้ความยินยอมได้เอง จะต้องเป็นกรณีที่ผู้เยาว์ต้องไม่อยู่ภายใต้แรงกดดันหรืออิทธิพลใด ๆ และมีความเข้าใจในวัตถุประสงค์ ผลกระทบ ของการเก็บประมวลผลและใช้ข้อมูลส่วนบุคคลของตน” เพื่อให้เกิดความชัดเจนและเป็นการปกป้องสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของผู้เยาว์

4. ในประเด็นสิทธิในความเป็นส่วนตัวของผู้ต้องขัง ในประเด็นนี้สมควรที่จะกำหนดมาตรการให้การแก้ไขฟื้นฟูผู้ต้องโทษ โดยฝึกอบรมและพัฒนาพฤตินิสัยในรูปแบบที่มีการมอบประกาศนียบัตรเพื่อรับรองคุณวุฒิทางวิชาการหรือวิชาชีพนั้นจะต้องไม่มีการระบุข้อความที่เป็นการเปิดเผยว่า ได้รับการฝึกอบรมในเรือนจำ หรือได้รับการฝึกอบรมในขณะต้องโทษ เพราะเป็นการเปิดเผยข้อมูลส่วนบุคคลซึ่งถือเป็นข้อมูลที่มีความอ่อนไหว โดยในประเด็นนี้ อาจมีการออกระเบียบโดยอาศัยอำนาจตามพระราชบัญญัติราชทัณฑ์ พ.ศ.2560 มาตรา 42 เพื่อวางหลักเกณฑ์อันเป็นกฎหมายลำดับรองต่อไป

5. ควรมีการแก้ไขเพิ่มเติมหลักการ Privacy by Design หรือ การกำหนดหน้าที่ให้ผู้ควบคุมข้อมูลมีหน้าที่บูรณาการหลักการคุ้มครองข้อมูลทั้งในขั้นวางแผนและขั้นปฏิบัติการ ไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 โดยควรแก้ไขเพิ่มเติมมาตรา 37 ให้มีอนุมาตราเพิ่มเติม และมีข้อความดังนี้

(6) ผู้ควบคุมข้อมูลต้องเลือกผู้ประมวลผลข้อมูลที่ปฏิบัติตามมาตรการทางเทคนิคและทางการจัดการองค์กรที่เหมาะสมและเพียงพอต่อการคุ้มครองความเป็นส่วนตัวของเจ้าของข้อมูลตั้งแต่ขั้นแรกเริ่มในการวางแผนออกแบบผลิตภัณฑ์และในขั้นปฏิบัติการจำหน่ายสินค้าหรือให้บริการ

6. ควรมีการแก้ไขเพิ่มเติมหลักการคัดค้านการประมวลผลข้อมูลโดยอัตโนมัตินี้ให้ชัดเจนลงในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 โดยอาจจะเพิ่มเติมเป็นมาตรา 32/1 โดยให้มีข้อความว่า

เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะไม่ถูกประมวลผลข้อมูลส่วนบุคคลของตนด้วยวิธีการอัตโนมัติเพียงอย่างเดียวเท่านั้น ซึ่งรวมไปถึงการนำข้อมูลมาใช้ในการวิเคราะห์พฤติกรรมบุคคลนั้น (Profiling) ที่อาจก่อให้เกิดผลทางกฎหมายเกี่ยวกับตนหรือส่งผลที่มีความสำคัญในระดับเดียวกันด้วย

7. ควรที่จะได้มีการแก้ไขเพิ่มเติมหลักความรับผิดชอบ (Accountability) ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 เพื่อให้กฎหมายไทยได้มาตรฐานการยอมรับว่าทัดเทียมและเทียบเท่ากับการคุ้มครองข้อมูลส่วนบุคคลของนานาประเทศ โดยหลักการในเรื่องนี้เป็นหลักการที่กำหนดหน้าที่ให้แก่ผู้ควบคุมข้อมูล (Data Controller) จึงควรแก้ไขเพิ่มเติม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 37 ซึ่งเป็นมาตราที่กำหนดหน้าที่ให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล โดยอาจจะเพิ่มเติมอนุมาตรา ให้มีข้อความดังต่อไปนี้

(6) ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องรับผิดชอบในอันที่จะแสดงให้เห็นว่าตนสามารถปฏิบัติตามแผนแม่บท นโยบาย ยุทธศาสตร์ หรือแผนระดับชาติ รวมไปถึงกฎระเบียบต่าง ๆ ที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

8. ควรจะได้มีการกำหนดหลักการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนให้สอดคล้องกัน ระหว่างกฎหมายกลาง คือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และกฎหมายเฉพาะฉบับต่าง ๆ ทั้งในด้านของการกำหนดนิยามความหมาย รวมถึงมาตรการในการจัดการข้อมูลส่วนบุคคลที่เป็นการคุ้มครองสิทธิ เพื่อให้ระบบของการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของทั้งกฎหมายกลางและกฎหมายเฉพาะเป็นไปในทิศทางเดียวกัน โดย

1) สมควรที่จะได้มีการแก้ไขพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 ให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในการทำหน้าที่คุ้มครองข้อมูลข่าวสารส่วนบุคคลที่อยู่ในภาครัฐด้วย

2) ในส่วนของพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ.2550 ยังไม่ได้มีการบัญญัตินิยามของข้อมูลส่วนบุคคลเกี่ยวกับสุขภาพไว้ จึงทำให้เกิดปัญหาไม่สามารถกำหนดความหมายและขอบเขตการคุ้มครองสิทธิเกี่ยวกับข้อมูลส่วนบุคคลด้านสุขภาพที่ชัดเจน ซึ่งอาจทำให้เกิดความสับสนในการตีความและการใช้บังคับกฎหมาย ดังนั้น จึงควรแก้ไขโดยกำหนดคำนิยามของคำว่า “ข้อมูลส่วนบุคคลเกี่ยวกับสุขภาพ” ไว้ให้ชัดเจน โดยอาจทำการแก้ไขพระราชบัญญัติสุขภาพแห่งชาติ พ.ศ.2550 มาตรา 3 โดยอาจกำหนดให้มีข้อความดังนี้

ข้อมูลด้านสุขภาพของบุคคล หมายถึงข้อมูลใด ๆ ด้านสุขภาพทั้งหลายในทางด้านร่างกาย จิตใจ ปัญญา พฤติกรรม หรือสังคมของบุคคลธรรมดา และข้อมูลดังกล่าวเกี่ยวกับสิ่งเฉพาะตัวของบุคคล หรือเป็นสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ ทั้งนี้ ข้อมูลด้านสุขภาพของบุคคลให้หมายรวมถึงบุคคลซึ่งถึงแก่ความตายแล้วด้วย

9. ในการบังคับใช้กฎหมายเกี่ยวกับความมั่นคง ไม่ว่าจะเป็นพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 พระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ.2562 รวมไปถึงกฎหมายที่เกี่ยวข้องกับความมั่นคงหรือมีการเปิดโอกาสให้รัฐเข้าล่วงละเมิดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนั้น จะต้องมีการจำกัดขอบเขตของการใช้กฎหมายให้ชัดเจนและบังคับใช้ด้วยความระมัดระวังไม่ให้ไปล่วงละเมิดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประชาชน ไม่เช่นนั้น อาจจะสร้างปัญหาทางด้านเศรษฐกิจการค้าการลงทุนกับประเทศในสหภาพยุโรป ดังเช่นที่ประเทศสหรัฐอเมริกาเคยประสบในกรณีของ Safe Harbour ก็เป็นได้

10. ควรกำหนดให้องค์กร “คณะกรรมการข้อมูลส่วนบุคคล” มีความเป็นอิสระมากขึ้น โดยการแก้ไขพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 หมวด 1 ที่ว่าด้วยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โดยควรกำหนดแก้ไขสัดส่วนของคณะกรรมการและกระบวนการสรรหาที่จะทำให้สะท้อนถึงการมีส่วนร่วมของภาคประชาสังคมมากขึ้นต่อไป

11. ควรแก้ไขพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 โดยเพิ่มเติมหน้าที่ของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ให้มีหน้าที่ในการส่งเสริมการเข้าถึงสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่ง สิทธิในการได้รับการเยียวยาของเจ้าของข้อมูลส่วนบุคคลที่เป็นผู้พิการหรือทุพพลภาพ ซึ่งย่อมจะมีปัญหาในการใช้สิทธิของตน กรณีเช่นนี้ แม้ว่า ในตัวพระราชบัญญัติจะได้กำหนดหลักการคุ้มครองสิทธิของเจ้าของข้อมูลไว้ ไม่ว่าจะเป็นการกำหนดโทษทางอาญา โทษทางปกครองและ สภาพบังคับในทางแพ่ง ไว้ดีเพียงใดก็ตาม แต่หากผู้เป็นเจ้าของสิทธิมีปัญหาในการเข้าถึงระบบและกลไกการเยียวยาแล้ว ย่อมทำให้การคุ้มครองสิทธิของบุคคลไม่อาจเกิดประสิทธิภาพและประสิทธิผลได้ เช่นนี้จึงสมควรที่จะได้แก้ไข มาตรา 16 โดยเพิ่มเติมอนุมาตรา (14) ให้มีข้อความว่า “มาตรา 16 คณะกรรมการมีหน้าที่และอำนาจ ดังต่อไปนี้ (14) ออกมาตรการหรือแนวทางการดำเนินงาน หรือข้อปฏิบัติในการส่งเสริมการเข้าถึงสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของเจ้าของข้อมูลที่อยู่ในฐานะผู้ด้อยโอกาส เช่น ผู้พิการหรือทุพพลภาพ”

12. ควรจะมีการกำหนดให้มีการสนับสนุน และส่งเสริม ให้เกิดกลไกการกำกับดูแลกันเอง (Self Regulation) โดยภาคเอกชนไว้ในกฎหมายอย่างชัดเจน หรือไม่เช่นนั้นอย่างน้อยก็ควรจะมีการนำแนวคิดนี้ ไปบรรจุในแผนแม่บทการดำเนินงานด้านการส่งเสริมและการคุ้มครองข้อมูลส่วนบุคคล

ที่สอดคล้องกับนโยบาย ยุทธศาสตร์ชาติ และแผนระดับชาติที่เกี่ยวข้อง เพื่อเสนอต่อคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติตามกฎหมายว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม ในส่วนการจัดทำแผนนี้เป็นอำนาจของคณะกรรมการข้อมูลส่วนบุคคลที่กำหนดไว้ในมาตรา 16 (1) ซึ่งจะได้มีการดำเนินการจัดทำในอนาคตอันใกล้นี้ ตัวอย่างเช่นการส่งเสริมให้มีการจัดตั้งองค์กรวิชาชีพเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เป็นต้น

โดยจากข้อเสนอแนะต่าง ๆ ที่กล่าวมา สามารถทำเป็นตารางสรุปได้ดังนี้

ตารางที่ 6.1 สรุปข้อเสนอแนะ

ข้อเสนอแนะเพื่อพัฒนา			
มาตรการทางกฎหมาย	1. พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562	ประเด็นนิยาม	ควรแก้ไข มาตรา 6 “ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม และให้หมายรวมถึงข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย”
		ประเด็นการให้ความยินยอมของผู้เยาว์	ควรแก้ไข มาตรา 20 (1) “สำหรับกรณีที่ผู้เยาว์อาจให้ความยินยอมได้เอง จะต้องเป็นกรณีที่ผู้เยาว์ต้องไม่อยู่ภายใต้แรงกดดันหรืออิทธิพลใด ๆ และมีความเข้าใจในวัตถุประสงค์ ผลกระทบ ของการเก็บประมวลผล และใช้ข้อมูลส่วนบุคคลของตน” เพื่อให้เกิดความชัดเจนและเป็นการปกป้องสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของผู้เยาว์
		ประเด็น Privacy by Design	ควรแก้ไข มาตรา 37 (6) “ผู้ควบคุมข้อมูลต้องเลือกผู้ประมวลผลข้อมูลที่ปฏิบัติตามมาตรการทางเทคนิคและทางการจัดการองค์กรที่เหมาะสมและเพียงพอต่อการคุ้มครองความเป็นส่วนตัวของเจ้าของข้อมูลตั้งแต่ขั้นแรกเริ่มในการวางแผนออกแบบผลิตภัณฑ์และในขั้นปฏิบัติการจำหน่ายสินค้าหรือให้บริการ”

ตารางที่ 6.1 (ต่อ)

ข้อเสนอแนะเพื่อพัฒนา			
		ประเด็นหลักการคัดค้านการประมวลผลข้อมูลโดยอัตโนมัติ (Profiling)	ควรแก้ไข มาตรา 32/1 “เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะไม่ถูกประมวลผลข้อมูลส่วนบุคคลของตนด้วยวิธีการอัตโนมัติเพียงอย่างเดียวเท่านั้น ซึ่งรวมไปถึงการนำข้อมูลมาใช้ในการวิเคราะห์พฤติกรรมบุคคลนั้น (Profiling) ที่อาจก่อให้เกิดผลทางกฎหมายเกี่ยวกับตนหรือส่งผลที่มีความสำคัญในระดับเดียวกันด้วย”
		หลักความรับผิดชอบ (Accountability)	ควรแก้ไข มาตรา 37 (6) “ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องรับผิดชอบในอันที่จะแสดงให้เห็นว่าตนสามารถปฏิบัติตามแผนแม่บท นโยบาย ยุทธศาสตร์ หรือแผนระดับชาติ รวมไปถึงกฎระเบียบต่าง ๆ ที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล”
		ประเด็นข้อยกเว้นเรื่องการคุ้มครองข้อมูลส่วนบุคคลที่มีความอ่อนไหว	ควรตีความ มาตรา 26 (5) (จ) “เพื่อประโยชน์สาธารณะที่สำคัญ” บนพื้นฐานของการตระหนักถึงเจตนารมณ์ของกฎหมายและให้ความสำคัญต่อความปลอดภัยของข้อมูลส่วนบุคคลของประชาชนเป็นสำคัญ
	2.พ.ร.บ.ข้อมูลข่าวสารของราชการ พ.ศ. 2540	ประเด็นการคุ้มครองข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data)	ควรแก้ไข มาตรา 24/1 ว่า “ในการจัดระบบข้อมูลข่าวสารตามมาตรา 23 และ การเปิดเผยข้อมูลข่าวสารตามมาตรา 24 แห่งพระราชบัญญัตินี้ หากข้อมูลข่าวสารนั้นเป็นข้อมูลข่าวสารส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของ

ตารางที่ 6.1 (ต่อ)

ข้อเสนอแนะเพื่อพัฒนา		
		ข้อมูลส่วนบุคคลในทำนองเดียวกัน ให้หน่วยงานของรัฐกระทำโดยระมัดระวังและจะให้เกิดผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลอย่างร้ายแรงเกินสมควรมิได้”
3. พ.ร.บ. สุขภาพแห่งชาติ พ.ศ. 2550	ประเด็นนิยามข้อมูลสุขภาพ	ควรแก้ไข มาตรา 3 “ข้อมูลด้านสุขภาพของบุคคล หมายถึงข้อมูลใด ๆ ด้านสุขภาพทั้งหลายในทางด้านร่างกาย จิตใจ ปัญญา พฤติกรรม หรือสังคมของบุคคลธรรมดา และข้อมูลดังกล่าวเกี่ยวกับสิ่งเฉพาะตัวของบุคคล หรือเป็นสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ ทั้งนี้ ข้อมูลด้านสุขภาพของบุคคลให้หมายรวมถึงบุคคลซึ่งถึงแก่ความตายแล้วด้วย”
3.พ.ร.บ. ราชทัณฑ์ พ.ศ.2560	ประเด็นสิทธิของผู้ต้องขัง	ควรอาศัยอำนาจตาม มาตรา 42 เพื่อวางหลักเกณฑ์อันเป็นกฎหมายลำดับรองกำหนดให้การมอบประกาศนียบัตรทางวิชาชีพต่าง ๆ ที่ได้จากการฝึกอบรมต้องไม่ระบุว่าเป็นการฝึกอบรมในเรือนจำหรือระหว่างถูกลงโทษ เพื่อไม่ให้เป็นการเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหว
4. พ.ร.บ.ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และ พ.ร.บ.ข่าวกรองแห่งชาติ พ.ศ.2562	ประเด็นข้อยกเว้นการคุ้มครองข้อมูลส่วนบุคคล	การบังคับใช้และการตีความ กฎหมายเกี่ยวกับความมั่นคง ไม่ว่าจะเป็นพระราช-บัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 พระราชบัญญัติข่าวกรองแห่ง ชาติ พ.ศ.2562 รวมไปถึงกฎหมายที่เกี่ยวข้องกับความมั่นคง หรือมีการเปิดโอกาสให้รัฐเข้าล่วงละเมิดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนั้น จะต้องมีการจำกัดขอบเขตของการใช้กฎหมายให้ชัดเจนและบังคับใช้ด้วยความระมัดระวัง

ตารางที่ 6.1 (ต่อ)

ข้อเสนอแนะเพื่อพัฒนา			
			ไม่ให้ไปล่วงละเมิดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประชาชน ไม่เช่นนั้น อาจจะสร้างปัญหาทางด้านเศรษฐกิจการค้าการลงทุน
กลไกทางกฎหมาย	1. พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562	ประเด็นความเป็นอิสระขององค์กรที่ทำหน้าที่ในการบังคับใช้กฎหมาย	ควรแก้ไข ให้องค์กร“คณะกรรมการข้อมูลส่วนบุคคล” มีความเป็นอิสระมากขึ้น โดยการแก้ไขพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 หมวด 1 โดยควรกำหนดแก้ไขสัดส่วนของคณะกรรมการและกระบวนการสรรหาที่จะทำให้สะท้อนถึงการมีส่วนร่วมของภาคประชาสังคมมากขึ้น
		ประเด็นการเยียวยา	ควรแก้ไขเพิ่มเติม “มาตรา 16 คณะกรรมการมีหน้าที่และอำนาจ ดังต่อไปนี้ (14) ออกมาตรการ หรือแนวทางการดำเนินงาน หรือข้อปฏิบัติในการส่งเสริมการเข้าถึงสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของเจ้าของข้อมูลที่อยู่ในฐานะผู้ด้อยโอกาส เช่น ผู้พิการหรือทุพพลภาพ”
		ประเด็นส่งเสริมการกำกับดูแลตนเอง (Self Regulation)	ควรจะมีการกำหนดให้มีการสนับสนุน และส่งเสริม ให้เกิดกลไกการกำกับดูแลกันเอง (Self Regulation) โดยภาคเอกชนไว้ในกฎหมายอย่างชัดเจน หรือไม่เช่นนั้นอย่างน้อยก็ควรจะมีการนำแนวคิดนี้ ไปบรรจุในแผนแม่บทการดำเนินงานด้านการส่งเสริมและการคุ้มครองข้อมูลส่วนบุคคล ซึ่งอยู่ในอำนาจของคณะกรรรมการคุ้มครองข้อมูลส่วนบุคคล ตัวอย่างเช่น การส่งเสริมให้มีการจัดตั้งองค์กรวิชาชีพเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เป็นต้น

บรรณานุกรม

กงจักร โพธิพร้อม. **ปัญหาทางกฎหมายมหาชนบางประการเกี่ยวกับการควบคุมการใช้ข่าวสารโดยเครื่องคอมพิวเตอร์**. วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2529.

กระทรวงดิจิตอลเพื่อเศรษฐกิจและสังคม. **คำชี้แจงร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล**. ค้นวันที่ 30 กันยายน 2561 จาก http://bit.ly/2QkSLSG

กรีนการ์ด, ซามูเอล. **อินเทอร์เน็ตแห่งสรรพสิ่ง.** แปลโดย ทีปกร วุฒิพิทยามงคล. กรุงเทพมหานคร: โอเพ่นเวิลด์ส, 2560.

กันยภัทร รัตนวิลาส. **มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลในฐานะเครื่องมือสร้างบรรทัดฐานของอียู**. ค้นวันที่ 20 กันยายน 2561 จาก https://www.the101.world/gdpr-insight/

กิตติพงศ์ กมลธรรมวงศ์. **การคุ้มครองข่าวสารส่วนบุคคลในระบบกฎหมายไทย: ปัญหาและแนวทางแก้ไข**. วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2549.

กิตติพงศ์ กมลธรรมวงศ์ และคณะ. **โครงการศึกษาและพัฒนาแนวทางการคุ้มครองข้อมูลส่วนบุคคลภายใต้ประชาคมอาเซียน**. กรุงเทพมหานคร: สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์, 2558.

กิตติพันธุ์ เกียรติสุนทร. **มาตรการทางอาญาในการคุ้มครองข้อมูลส่วนบุคคล**. วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2538.

กิตสุรณ สังขสุวรรณ์. การรับรองและข้อจำกัดสิทธิในความเป็นส่วนตัวภายใต้กฎหมายไทย. **วารสารกฎหมาย คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย**. 36, 2 (กันยายน 2561): 267-292.

กุลพล พลวัน. แนวความคิดเกี่ยวกับเสรีภาพสื่อมวลชนในการแสวงหาข่าวสาร. ใน **เอกสารการสอนชุดวิชากฎหมายและจริยธรรมสื่อสารมวลชน หน่วยที่ 8.** นนทบุรี: มหาวิทยาลัยสุโขทัยธรรมธิราช, 2529.

ข้อมูลบัตรเครดิตแห่งชาติ. **ข้อมูลเครดิตคืออะไร สำคัญอย่างไร: ข้อมูลจากคณะกรรมการคุ้มครองข้อมูลเครดิต.** ค้นวันที่ 7 กุมภาพันธ์ 2562 จาก https://www.ncb.co.th/ncb-article/ข้อมูลเครดิตคืออะไร-สำค

คณาธิป ทองรวีวงศ์. **มาตรการทางกฎหมายในการคุ้มครองสิทธิของโดยมิได้รับรู้และยินยอม.** รายงานการวิจัย เสนอต่อคณะนิติศาสตร์ มหาวิทยาลัยเซนต์จอห์น, 2550.

คณาธิป ทองรวีวงศ์. มาตรการทางกฎหมายในการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว: ศึกษากรณีการรบกวนสิทธิในความเป็นอยู่ส่วนตัวจากการใช้เว็บไซต์เครือข่ายสังคม. **วารสารวิชาการสมาคมสถาบันอุดมศึกษาเอกชนแห่งประเทศไทย (สสอท.).** 18, 2 (2555): 39-51.

คณาธิป ทองวีรวงศ์. **รายงานการวิจัยฉบับสมบูรณ์ เรื่องการปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน.** รายงานการวิจัย เสนอต่อสำนักงานเลขาธิการสภาผู้แทนราษฎร, 2559.

เครือข่ายพลเมืองเน็ต. **ความคิดเห็นต่อร่าง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล (2 ก.พ. 2561).** ค้นวันที่ 23 พฤษภาคม 2562 จาก https://thainetizen.org/docs/data-protection-bill-2018-comments/

เครือข่ายพลเมืองเน็ต. **ความคิดเห็นต่อร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ก.ย. 2561).** ค้นวันที่ 12 ธันวาคม 2562 จาก https://thainetizen.org/docs/data-protection-bill-comments-20180920/

จันทจิรา เอี่ยมมยุรา. กฎหมายเกี่ยวกับข้อมูลส่วนบุคคลในประเทศไทย. ใน **รายงานการวิจัย โครงการจัดทำความเห็นทางวิชาการเพื่อจัดทำรายงานเกี่ยวกับหลักเกณฑ์และแนวทางการพิจารณาและดำเนินการตามกฎหมายคุ้มครองข้อมูลข่าวสารส่วนบุคคล และจัดทำคู่มือการปฏิบัติงานเกี่ยวกับข้อมูลข่าวสารส่วนบุคคลภาครัฐตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ.2540.** กรุงเทพมหานคร: สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์, 2547.

จันทจิรา เอี่ยมมยุรา. การคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย. **วารสารนิติศาสตร์.** 34, 4 (ธันวาคม 2547): 627-652.

ฉัตรชัย เอมราช. สิทธิที่จะถูกลืม. **วารสารนิติศาสตร์.** 45, 2 (มิถุนายน 2559): 408-430.

ชวาบ, เคลาส์. **การปฏิวัติอุตสาหกรรมครั้งที่สี่.** แปลโดย ศรรวริศา เมฆไพบูลย์. กรุงเทพมหานคร: อมรินทร์ฮาวทู อมรินทร์พริ้นติ้งแอนด์พับลิชชิ่ง, 2561.

ชวิน อุ่นภัทร. ความเป็นส่วนตัวและการคุ้มครองจากการล่วงล้ำของรัฐในประเทศสหรัฐอเมริกา. **วารสารนิติศาสตร์.** 44, 4 (ธันวาคม 2558): 968-1005.

ชื่นอารีย์ มาลีศรีประเสริฐ. **การคุ้มครองสิทธิส่วนตัวกับการสื่อสารสนเทศ**. วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2539.

ชูชีพ ปิณฑะสิริ. **การละเมิดสิทธิส่วนตัว.** วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2525.

แทปส์ค็อตต์, ดอน. **เศรษฐกิจดิจิตอล**. แปลโดย พรศักดิ์ อุรัจฉัทชัยรัตน์. กรุงเทพมหานคร: แมคกรอ-ฮิล อินเทอร์เนชั่นแนล เอ็นเตอร์ไพรส์ แอลแอลซี, 2559.

ธนกฤต วรธนัชชากุล. **ข้อสังเกตต่อการบังคับใช้ พ.ร.บ.ข่าวกรองแห่งชาติฉบับใหม่**. ค้นวันที่ 27 เมษายน 2562 จาก https://www.isranews.org/isranews-article/75704-aticle-75704.html

ธนัท สุวรรณปริญญา. **ปัญหาทางกฎหมายเกี่ยวกับการค้มุครองข้อมลูส่วนบคุคลบนธุรกรรมทางอิเล็กทรอนิกส์**. สารนิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยกรุงเทพ, 2550.

ธนาคารอาคารสงเคราะห์. **หุ้นส่วนประเทศไทย: เศรษฐกิจดิจิตอลกับการพัฒนาดิจิตอลไทยแลนด์.** ค้นวันที่ 20 มีนาคม 2561 จาก http://library.baac.or.th/portal/news_detail.php?id=2934

นคร เสรีรักษ์. **ความเป็นส่วนตัว: ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย**. กรุงเทพมหานคร: พี. เพรส, 2557.

นนทวัชร์ นวตระกูลพิสุทธิ์. สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลกับมาตรการคุ้มครองตาม ร่าง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... . **วารสารนิติศาสตร์.** 43, 4 (ธันวาคม 2557): 732-771.

นพมาศ เกิดวิชัย. **การพัฒนากฎหมายเพื่อคุ้มครองสิทธิในความเป็นส่วนตัว**. วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยรังสิต, 2557.

บรรเจิด สิงคะเนติ. **หลักพื้นฐานเกี่ยวกับสิทธิเสรีภาพ และศักดิ์ศรีความเป็นมนุษย์.** พิมพ์ครั้งที่ 3. กรุงเทพมหานคร: วิญญูชน, 2552.

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

ปฏิวัติ อุ่นเรือน. **ปัญหาการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลระหว่างประเทศ**. สารนิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2547.

ปภาวดี ธโนดมเดช. **มาเลเซียกับการคุมครองผูบริโภคในยุค Digital Economy.** ค้นวันที่ 20 มีนาคม 2561 จาก http://www.itd.or.th/wp-content/uploads/2015/05/20150114-ar_malaysia-digi-economy.pdf

ประสิทธิ์ ปิวาวัฒนาพานิช. กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกาและประเทศมาเลเซีย. **วารสารนิติศาสตร์.** 43, 4 (ธันวาคม 2557): 537-538.

ปรีดี เกษมทรัพย์. **นิติปรัชญา.** กรุงเทพมหานคร: มิตรนราการพิมพ์, 2531.

พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ.2545. **ราชกิจจานุเบกษา.** 119, 114ก (13 พฤศจิกายน 2545).

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562. **ราชกิจจานุเบกษา.** 136, 69ก (27 พฤษภาคม 2562).

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540. **ราชกิจจานุเบกษา.** 114, 46ก (10 กันยายน 2540).

พระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ.2562. **ราชกิจจานุเบกษา.** 136, 50ก (16 เมษายน 2562).

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562. **ราชกิจจานุเบกษา.** 136, 69ก (27 พฤษภาคม 2562).

พิรงรอง รามสูต. **การกำกับดูแลเนื้อหาอินเทอร์เน็ต**. กรุงเทพมหานคร: ศูนย์ศึกษานโยบายสื่อ คณะนิเทศศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2556.

เพชรรัตน์ จงปัญญาประพันธ์. ความสำคัญของกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล. **วารสารนิติศาสตร์.** 33, 4 (ธันวาคม 2546): 821-830.

รักไท เทพปัญญา. **ข้อมูลเบื้องต้นเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (The General Data Protection Regulation (GDPR)).** ค้นวันที่ 1 พฤษภาคม 2562 จาก https://lawforasean.com/blog/2018/07/-the-general-data-protection-regulation-gdpr?lang=th.

รัฐธรรมนูญแห่งราชอาณาจักรไทย แก้ไขเพิ่มเติม (ฉบับที่ 5) พุทธศักราช 2538. **ราชกิจจานุเบกษา.** 112, 7ก (10 กุมภาพันธ์ 2538).

รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2540. **ราชกิจจานุเบกษา.** 114, 55ก (11 ตุลาคม 2540).

วรพจน์ วิศรุตพิชญ์. **คู่มือศึกษาวิชากฎหมายปกครอง**. กรุงเทพมหานคร: สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา, 2545.

วรพจน์ วิศรุตพิชญ์. **สิทธิเสรีภาพตามรัฐธรรมนูญ.** กรุงเทพมหานคร: วิญญูชน, 2538.

วรพจน์ วิศรุตพิชญ์. **สิทธิและเสรีภาพตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540**. กรุงเทพมหานคร: วิญญูชน, 2543.

วรรณรัชชา ทรัพย์รดาพัดชา. **ปัญหาการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลระหว่างประเทศกับสหภาพยุโรป: ศึกษาผลกระทบของคดีคำพิพากษาศาลยุติธรรมแห่งสหภาพยุโรปในคดี C-362/14 ต่อโครงการเซฟฮาร์เบอร์ (Safe Harbour)**. วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2558.

วิริยะ รามสมภพ. **เอกสารวิชาการ เรื่องความสัมพันธ์ระหว่างร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... กับ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540.** ค้นวันที่ 19 กรกฎาคม 2562 จาก http://www.oic.go.th/web2017/iwebform_viewer.asp?i=21111%2E22213705112112151111211

วิสาร พันธุนะ. กฎหมายสื่อสารมวลชนในต่างประเทศ. ใน **เอกสารการสอนชุดกฎหมายและจริยธรรมสื่อมวลชน**. นนทบุรี: มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2552.

แวคส์, เรย์มอนด์. **ความเป็นส่วนตัว: ความรู้ฉบับพกพา.** แปลโดย อธิป จิตตฤกษ์ และปวรรัตน์ ผลาสิทธุ์. กรุงเทพมหานคร: โอเพ่นเวิลด์ส, 2556.

ศิริกุล ภู่พันธ์. **ข้อความคิดว่าด้วยข้อมูลข่าวสารส่วนบุคคล**. วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2548.

ศิริลักษณ์ ศรีโชละ. ปัญหาทางกฎหมายเกี่ยวกับข้อมูลบัตรเครดิต ศึกษาเฉพาะกรณีการนำข้อมูลเครดิตไปใช้ผิดวัตถุประสงค์. **วารสารนิติศาสตร์ปรีดีพนมยงค์.** 4, 1 (1 สิงหาคม 2558-มกราคม 2559): 101-116.

ศุภวัชร์ มาลานนท์. **องค์กรบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล**. ค้นวันที่ 24 ธันวาคม 2562 จาก https://www.kaohoon.com/content/328480?fbclid=IwAR1tk2WV6by81RAy_OV1CMwb_59Z2dRD7iL7CS1EuqQdXLaZ5iL_oKnReog

สฤณี อาชวานันทกุล. **เศรษฐกิจดิจิตอล" เพื่อใคร? อันตรายของชุดกฎหมายไซเบอร์.** ค้นวันที่ 25 เมษายน 2562 จาก https://thaipublica.org/2015/01/dangers-new-cyber-laws/

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.). **กฎหมาย GDPR ฉบับรวบรัด**. ค้นวันที่ 25 เมษายน 2562 จาก https://www.etda.or.th/content/gdpr-in-a-nutshell?fbclid=IwAR2MXf7Q1YnAjZEdX9xuz6ez7ZNWvVWcCmq9r0XMVDug2hMAG8J3HqEmwOM

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.). **คุ้มครองข้อมูลส่วนบุคคล: ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวทางการจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ.2553.** ค้นวันที่ 25 เมษายน 2562 จาก https://ictlawcenter.etda.or.th/laws/detail/ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์-เรื่อง-แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ-พศ2553

สมยศ เชื้อไทย. **กฎหมายมหาชนเบื้องต้น.** กรุงเทพมหานคร: วิญญูชน, 2560.

สมศักดิ์ นวตระกูลพิสุทธิ์. กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศฝรั่งเศส. ใน **รายงานการวิจัยโครงการจัดทำความเป็นทางวิชาการเพื่อจัดทำรายงานเกี่ยวกับหลักเกณฑ์และแนวทางการพิจารณาและดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และจัดทำคู่มือการปฏิบัติงานเกี่ยวกับข้อมูลส่วนบุคคลภาครัฐตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ.2540**. กรุงเทพมหานคร: สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์, 2547.

สุวรรณ ปริญญา. **ปัญหาทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบคุคลบนธุรกรรมทางอิเล็กทรอนิกส์**. สารนิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยกรุงเทพ, 2550.

หทัยชนก หร่ายวงศ์. **ปัญหาเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลด้านสุขภาพ**. วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2548.

อธิพร สิทธิธีรรัตน์. **ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลในบริบทอิเล็กทรอนิกส์.** วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์. 2558.

อัครเดช มณีภาค. ปัญหาทางกฎหมายพระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 ในการคุ้มครองข้อมูลส่วนบุคคลเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์. **วารสารจันทรเกษมสาร.** 16, 31 (กรกฎาคม-ธันวาคม 2553).

อัญธิกา ณ พิบูลย์. ปัญหาการบังคับใช้สิทธิที่จะลบข้อมูลส่วนบุคคลในโลกออนไลน์: ศึกษากรณีกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป. **วารสารนิติพัฒน์นิด้า.** 7, 2 (กรกฎาคม-ธันวาคม 2561): 41-50.

อาทิตย์ สุริยะวงศ์กุล. **ข้อมูลประกอบการนำเสนอความเห็นและข้อเสนอแนะแนวทางแก้ไขหรือปรับปรุงร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....** . ค้นวันที่ 1 ตุลาคม 2561 จาก https://thainetizen.org/docs/data-protection-bill-comments-20180920/

Alderman, Ellen and Kennedy, Caroline. **The Right to Privacy**. New York: Alfred A. Knopf, 1995 อ้างถึงใน นคร เสรีรักษ์. **ความเป็นส่วนตัว: ความคิด ความรู้ ความจริงและพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย**. กรุงเทพมหานคร: พี. เพรส, 2557.

Alsenoy, Brendan Van. **Regulating Data Protection the Allocation of Responsibility and Risk Among Actors Involved in Personal Data Processing**. Doctoral dissertation, Faculty of Law, Catholic University of Leuven, 2016.

APEC Secretariat. **APEC Privacy Framework.** Retrieved March 10, 2018 from https://www.apec.org/-/media/APEC/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf

Boom, W. H. van and Erp, J. H. M. van. Electronic Highways: On The Road to Liability. In **Emerging Electronic Highways.** V. Bekkers et al., eds. Netherland: Kluwer Law International, 1996. Pp. 153-164.

Cate, Fred H.; Cullen, Peter and Mayer-Schonberger, Viktor. **Data Protection Principles for the 21st Century.** Retrieved February 26, 2018 from https://www.repository.law.indiana.edu/facbooks/23

Commission Nationale de l'Informatique et des Libertés (CNIL). **Personal Data: Definition**. Retrieved October 1, 2018 from https://www.cnil.fr/en/personal-data-definition

Commission Nationale de l'Informatique et des Libertés (CNIL). **Rights and Obligations.** Retrieved March 11, 2018 from https://www.cnil.fr/en/rights-and-obligations

Commission Nationale de l'Informatique et des Libertés (CNIL). **The CNIL's Missions.** Retrieved March 11, 2018 from https://www.cnil.fr/en/cnils-missions

Data Protection Laws of the World. **Definition of Personal Data.** Retrieved December 12, 2018 from https://www.dlapiperdataprotection.com/index.html?t= definitions&c=US&c2=

Delany, Hilary; Carolan, Eoin and Murphy, Cliodhna. **The Right to Privacy: A Doctrinal and Comparative Analysis.** Dublin: Thomson Round Hall, 2008 อ้างถึงใน ชวิน อุ่นภัทร. ความเป็นส่วนตัวและการคุ้มครองจากการล่วงล้ำของรัฐในประเทศสหรัฐอเมริกา. **วารสารนิติศาสตร์.** 44, 4 (ธันวาคม 2558): 968-1005.

Department for Digital, Culture, Media and Sport. **Data Protection Bill Factsheet – Overview.** Retrieved March 12, 2018 from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/685647/2018-03-05_Factsheet01_Bill_overview.pdf

DLA Piper. **Data Protection Laws of the World.** Retrieved March 10, 2018 from http://www.dlapiperdataprotection.com

EU. Retrieved March 11, 2018 from https://www.eugdpr.org/

EU. **An Overview of the Main Change under GDPR and How They Differ from the Previous Directive**. Retrieved March 11, 2018 from https://www.eugdpr.org/key-changes.html

European Union Agency for Fundamental Rights (FRA). **Handbook on European Data Protection Law**. Retrieved December 12, 2018 from https://www.coe.int/en/web/data-protection/-/the-new-handbook-on-european-data-protection-law-is-out-get-your-copy-

Foster, Steve. **Human Rights and Civil Liberties.** London: Pearson Education, 2003.

Franklin, Marianne; Bodle, Robert and Hawtin, Dixie. **The Charter of Human Rights and Principles for the Internet**. S.l.: Internet Rights & Principles Coalition, United Nation, 2018. Retrieved March 10, 2018 from http://internetrightsandprinciples.org/site/wp-content/uploads/2018/01/IRPC_ english_5th edition.pdf

Hardinghaus, Alexander; Kimmich, Ramona and Süss, Philipp. **German Federal Supreme Court: Facebook Account Passes to Heirs.** Retrieved April 22, 2018 from https://www.technologylawdispatch.com/2018/07/in-the-courts/german-federal-supreme-court-facebook-account-passes-to-heirs/

Information Commissioner's Office (ICO). **Guide to the General Data Protection Regulation (GDPR).** Retrieved March 1, 2019 from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

Information Commissioner's Office (ICO). **Individual Rights.** Retrieved March 1, 2019 from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

Information Commissioner's Office (ICO). **An Overview of the Data Protection Act 2018.** Retrieved March 1, 2019 from https://ico.org.uk/media/2614158/ico-introduction-to-the-data-protection-bill.pdf

Jolly, Ieuan. **Data Protection in the United States: Overview.** Retrieved May 15, 2018 from https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1

Kardash, Adam and Kosseim, Patricia. **The International Comparative Legal Guide to: Data Protection 2018**. Retrieved February 8, 2019 from https://www.osler.com/osler/media/Osler/reports/privacy-data/Data-Protection-Laws-in-Canada-2018.pdf

Mannheim, Karl. **Systematic Sociology: An Introduction to the Study of Society.** New York: Routledge, 2013.

Miller, Russell A. **Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair.** New York: Cambridge University Press, 2017.

Muller, Paul. **Le principe de la proportionnalité**. S.l.: s.n., 1978 อ้างถึงใน วรพจน์ วิศรุตพิชญ์. **คู่มือศึกษาวิชากฎหมายปกครอง.** กรุงเทพมหานคร: สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา, 2545.

Office of Privacy Commisionner of Canada. **PIPEDA in Brief.** Retrieved February 20, 2019 from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/#_what_is

Office of the United Nations High Commissioner for Human Rights. **Guidelines for the Regulation of Computerized Personal Data Files.** Retrieved March 13, 2018 from http://www.refworld.org/pdfid/3ddcafaac.pdf

Personal Information Protection and Electronic Documents Act. Retrieved February 8, 2019 from https://laws-lois.justice.gc.ca/PDF/P-8.6.pdf

Phillips, Bruce. **The Evolution of Canada's Privacy Laws, Speaking Notes Prepared for the Canadian Bar Association - Ontario Institute - January 28, 2000**. Retrieved February 8, 2019 from https://www.priv.gc.ca/en/opc-news/speeches/archive/02_05_a_000128/

Polčák, Radim and Jerker B. Svantesson, Dan. **Information Sovereignty Data Privacy, Sovereign Powers and the Rule of Law.** Massachusetts: Edward Elgar, 2017.

Practical Law Employment. **Comparisons: DPA 1998 v GDPR and DPA 2018.** Retrieved March 10, 2019 from https://uk.practicallaw.thomsonreuters.com/w-011-6935?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1

Privacy Act. Retrieved February 8, 2019 from https://laws-lois.justice.gc.ca/PDF/P-21.pdf

Proust, Olivier and Defromont, Julien-Alexis. **Post-GDPR French Data Protection Law adopted** Retrieved November 1, 2018 from https://privacylawblog.fieldfisher.com/2018/post-gdpr-french-data-protection-law-adopted

Proust, Olivier and Goossens, Gaëtan. **France Adopts Digital Republic Law.** Retrieved February 10, 2019 from https://privacylawblog.fieldfisher.com/2016/france-adopts-digital-republic-law

Reidenberg, Joel R. Lex Informatica: The Formulation of Information Policy Rules through Technology. **Texas Law Review**. 76 (1998): 553-584.

Roos, Anneliese. **The Law of Data (Privacy) Protection: A Comparative and Theoretical Study.** Doctoral dissertation, Doctor of Laws at the University of South Africa, 2003.

Schüßler, Lennart and Karniyevich, Natallia. **Germany is the First EU Member State to Enact New Data Protection Act to Align with the GDPR.** Retrieved November 1, 2018 from https://www.twobirds.com/en/news/articles/2017/germany/germany-is-the-first-eu-member-state-to-enact-new-data-protection-act-to-align-with-the-gdpr

Tzanou, Maria. **The Fundamental Right to Data Protection: Nomative Value in the Context of Counter-Terrorism Surveillance**. Oregon: Hart, 2017.

United Nations. **Human Rights: A Basic Handbook for UN Staff.** Retrieved March 10, 2018 from http://www.ohchr.org/Documents/Publications/HRhandbooken.pdf

US–EU Privacy Shield Framework Principles (2016). Retrieved March 16, 2018 from https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg

Wacks, Raymond. **Personal Information: Privacy and The Law**. London: Oxford, 1993 อ้างถึงใน สุวรรณ ปริญญา. **ปัญหาทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบคุคลบนธุรกรรมทางอิเล็กทรอนิกส์**. สารนิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยกรุงเทพ, 2550.

Wall, Alex. **GDPR Matchup: The APEC Privacy Framework and Cross-Border Privacy Rules.** Retrieved March 17, 2018 from https://iapp.org/news/a/gdpr-matchup-the-apec-privacy-framework-and-cross-border-privacy-rules/

Warren, Samuel D. and Brandeis, Louis D. The Right to Privacy. **Harvard Law Review**. 4 (December 15, 1890): 194-220.

Woodhouse, John and Lang, Arabella. **Brexit and Data Protection.** Retrieved March 12, 2018 from http://researchbriefings.files.parliament.uk/documents/CBP-7838/CBP-7838.pdf

World Intellectual Property Organization (WIPO). **European Union Directive 95/46/EC.** Retrieved March 10, 2018 from http://www.wipo.int/wipolex/en/text.jsp?file_id=31

Zrinski, Tatjana. **EU GDPR vs. German Bundesdatenschutzgesetz – Similarities and Differences**. Retrieved November 1, 2018 from https://advisera.com/eugdpracademy/knowledgebase/eu-gdpr-vs-german-bundesdatenschutzgesetz-similarities-and-differences/

ภาคผนวก

พระราชบัญญัติ
คุ้มครองข้อมูลส่วนบุคคล
พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ
พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๒๔ พฤษภาคม พ.ศ. ๒๕๖๒
เป็นปีที่ ๔ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ พระวชิรเกล้าเจ้าอยู่หัว มีพระบรมราชโองการโปรดเกล้าฯ ให้ประกาศว่า

โดยที่เป็นการสมควรมีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

พระราชบัญญัตินี้มีบทบัญญัติบางประการเกี่ยวกับการจำกัดสิทธิและเสรีภาพของบุคคล ซึ่งมาตรา ๒๖ ประกอบกับมาตรา ๓๒ มาตรา ๓๓ และมาตรา ๓๗ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย บัญญัติให้กระทำได้โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย

เหตุผลและความจำเป็นในการจำกัดสิทธิและเสรีภาพของบุคคลตามพระราชบัญญัตินี้ เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพและเพื่อให้มีมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคลที่มีประสิทธิภาพ ซึ่งการตราพระราชบัญญัตินี้สอดคล้องกับเงื่อนไขที่บัญญัติไว้ในมาตรา ๒๖ ของรัฐธรรมนูญแห่งราชอาณาจักรไทยแล้ว

จึงทรงพระกรุณาโปรดเกล้าฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของสภานิติบัญญัติแห่งชาติทำหน้าที่รัฐสภา ดังต่อไปนี้

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า “พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒”

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป เว้นแต่บทบัญญัติในหมวด ๒ หมวด ๓ หมวด ๕ หมวด ๖ หมวด ๗ และความในมาตรา ๙๕ และมาตรา ๙๖ ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ในกรณีที่มีกฎหมายว่าด้วยการใดบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในลักษณะใด กิจการใด หรือหน่วยงานใดไว้โดยเฉพาะแล้ว ให้บังคับตามบทบัญญัติแห่งกฎหมายว่าด้วยการนั้น เว้นแต่

(๑) บทบัญญัติเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และบทบัญญัติเกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคล รวมทั้งบทกำหนดโทษที่เกี่ยวข้อง ให้บังคับตามบทบัญญัติแห่งพระราชบัญญัตินี้เป็นการเพิ่มเติม ไม่ว่าจะซ้ำกับบทบัญญัติแห่งกฎหมายว่าด้วยการนั้นหรือไม่ก็ตาม

(๒) บทบัญญัติเกี่ยวกับการร้องเรียน บทบัญญัติที่ให้อำนาจแก่คณะกรรมการผู้เชี่ยวชาญออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคล และบทบัญญัติเกี่ยวกับอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ รวมทั้งบทกำหนดโทษที่เกี่ยวข้อง ให้บังคับตามบทบัญญัติแห่งพระราชบัญญัตินี้ ในกรณีดังต่อไปนี้

(ก) ในกรณีที่กฎหมายว่าด้วยการนั้นไม่มีบทบัญญัติเกี่ยวกับการร้องเรียน

(ข) ในกรณีที่กฎหมายว่าด้วยการนั้นมีบทบัญญัติที่ให้อำนาจแก่เจ้าหน้าที่ผู้มีอำนาจพิจารณาเรื่องร้องเรียนตามกฎหมายดังกล่าวออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคล แต่ไม่เพียงพอเท่ากับอำนาจของคณะกรรมการผู้เชี่ยวชาญตามพระราชบัญญัตินี้และเจ้าหน้าที่ผู้มีอำนาจตามกฎหมายดังกล่าวร้องขอต่อคณะกรรมการผู้เชี่ยวชาญหรือเจ้าของข้อมูลส่วนบุคคลผู้เสียหายยื่นคำร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญตามพระราชบัญญัตินี้ แล้วแต่กรณี

มาตรา ๔ พระราชบัญญัตินี้ไม่ใช้บังคับแก่

(๑) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น

(๒) การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์

(๓) บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมไว้เฉพาะเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น

(๔) สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าว ซึ่งเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมาธิการ แล้วแต่กรณี

(๕) การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

(๖) การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

การยกเว้นไม่ให้นำบทบัญญัติแห่งพระราชบัญญัตินี้ทั้งหมดหรือแต่บางส่วนมาใช้บังคับแก่ผู้ควบคุมข้อมูลส่วนบุคคลในลักษณะใด กิจการใด หรือหน่วยงานใดทำนองเดียวกับผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง หรือเพื่อประโยชน์สาธารณะอื่นใด ให้ตราเป็นพระราชกฤษฎีกา

ผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง (๒) (๓) (๔) (๕) และ (๖) และผู้ควบคุมข้อมูลส่วนบุคคลของหน่วยงานที่ได้รับยกเว้นตามที่กำหนดในพระราชกฤษฎีกาตามวรรคสอง ต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานด้วย

มาตรา ๕ พระราชบัญญัตินี้ให้ใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่าการเก็บรวบรวม ใช้ หรือเปิดเผยนั้น ได้กระทำในหรือนอกราชอาณาจักรก็ตาม

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่นอกราชอาณาจักร พระราชบัญญัตินี้ให้ใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักรโดยการดำเนินกิจกรรมของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าว เมื่อเป็นกิจกรรม ดังต่อไปนี้

(๑) การเสนอสินค้าหรือบริการให้แก่เจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่าจะมีการชำระเงินของเจ้าของข้อมูลส่วนบุคคลหรือไม่ก็ตาม

(๒) การเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักร

มาตรา ๖ ในพระราชบัญญัตินี้

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

“บุคคล” หมายความว่า บุคคลธรรมดา

“คณะกรรมการ” หมายความว่า คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

“พนักงานเจ้าหน้าที่” หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

“เลขาธิการ” หมายความว่า เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

“รัฐมนตรี” หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้

มาตรา ๗ ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรักษาการตามพระราชบัญญัตินี้ และให้มีอำนาจแต่งตั้งพนักงานเจ้าหน้าที่ เพื่อปฏิบัติการตามพระราชบัญญัตินี้

หมวด ๑
คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

มาตรา ๘ ให้มีคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ประกอบด้วย

(๑) ประธานกรรมการ ซึ่งสรรหาและแต่งตั้งจากผู้มีความรู้ ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์ในด้านการคุ้มครองข้อมูลส่วนบุคคล ด้านการคุ้มครองผู้บริโภค ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านสังคมศาสตร์ ด้านกฎหมาย ด้านสุขภาพ ด้านการเงิน หรือด้านอื่น ทั้งนี้ ต้องเกี่ยวข้องและเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคล

(๒) ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นรองประธานกรรมการ

(๓) กรรมการโดยตำแหน่ง จำนวนห้าคน ได้แก่ ปลัดสำนักนายกรัฐมนตรี เลขาธิการคณะกรรมการกฤษฎีกา เลขาธิการคณะกรรมการคุ้มครองผู้บริโภค อธิบดีกรมคุ้มครองสิทธิและเสรีภาพ และอัยการสูงสุด

(๔) กรรมการผู้ทรงคุณวุฒิ จำนวนเก้าคน ซึ่งสรรหาและแต่งตั้งจากผู้มีความรู้ ความเชี่ยวชาญและประสบการณ์เป็นที่ประจักษ์ในด้านการคุ้มครองข้อมูลส่วนบุคคล ด้านการคุ้มครองผู้บริโภค ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านสังคมศาสตร์ ด้านกฎหมาย ด้านสุขภาพ ด้านการเงิน หรือด้านอื่น ทั้งนี้ ต้องเกี่ยวข้องและเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคล

ให้เลขาธิการเป็นกรรมการและเลขานุการ และให้เลขาธิการแต่งตั้งพนักงานของสำนักงานเป็นผู้ช่วยเลขานุการได้ไม่เกินสองคน

หลักเกณฑ์และวิธีการสรรหาบุคคลเพื่อแต่งตั้งเป็นประธานกรรมการและกรรมการผู้ทรงคุณวุฒิ รวมทั้งการสรรหาประธานกรรมการและกรรมการผู้ทรงคุณวุฒิเพื่อดำรงตำแหน่งแทนผู้ที่พ้นจากตำแหน่งก่อนวาระตามมาตรา ๑๓ ให้เป็นไปตามที่คณะรัฐมนตรีประกาศกำหนด ทั้งนี้ ต้องคำนึงถึงความโปร่งใสและความเป็นธรรมในการสรรหา

มาตรา ๙ ให้มีคณะกรรมการสรรหาคณะหนึ่งจำนวนแปดคนทำหน้าที่คัดเลือกบุคคลที่สมควรได้รับการแต่งตั้งเป็นประธานกรรมการตามมาตรา ๘ (๑) หรือกรรมการผู้ทรงคุณวุฒิตามมาตรา ๘ (๔) ประกอบด้วย

(๑) บุคคลซึ่งนายกรัฐมนตรีแต่งตั้งจำนวนสองคน

(๒) บุคคลซึ่งประธานรัฐสภาแต่งตั้งจำนวนสองคน

(๓) บุคคลซึ่งผู้ตรวจการแผ่นดินแต่งตั้งจำนวนสองคน และ

(๔) บุคคลซึ่งคณะกรรมการสิทธิมนุษยชนแห่งชาติแต่งตั้งจำนวนสองคน

ในกรณีที่ผู้มีอำนาจแต่งตั้งตาม (๒) (๓) หรือ (๔) ไม่สามารถแต่งตั้งกรรมการสรรหาในส่วนของตนได้ภายในสี่สิบห้าวันนับแต่วันที่ได้รับแจ้งจากสำนักงาน ให้สำนักงานเสนอชื่อให้นายกรัฐมนตรีพิจารณาแต่งตั้งบุคคลที่เหมาะสมเป็นกรรมการสรรหาแทนผู้มีอำนาจแต่งตั้งนั้น

ให้คณะกรรมการสรรหาเลือกกรรมการสรรหาคนหนึ่งเป็นประธานกรรมการสรรหาและเลือกกรรมการสรรหาอีกคนหนึ่งเป็นเลขานุการคณะกรรมการสรรหา และให้สำนักงานปฏิบัติหน้าที่เป็นหน่วยธุรการของคณะกรรมการสรรหา

ในกรณีที่ตำแหน่งกรรมการสรรหาว่างลง ให้ดำเนินการเพื่อให้มีกรรมการสรรหาแทนในตำแหน่งนั้นโดยเร็ว ในระหว่างที่ยังไม่ได้กรรมการสรรหาใหม่ ให้คณะกรรมการสรรหาประกอบด้วยกรรมการสรรหาเท่าที่มีอยู่

กรรมการสรรหาไม่มีสิทธิได้รับการเสนอชื่อเป็นประธานกรรมการตามมาตรา ๘ (๑) หรือกรรมการผู้ทรงคุณวุฒิตามมาตรา ๘ (๔)

มาตรา ๑๐ ในการสรรหาประธานกรรมการตามมาตรา ๘ (๑) หรือกรรมการผู้ทรงคุณวุฒิตามมาตรา ๘ (๔) ให้คณะกรรมการสรรหาคัดเลือกบุคคลผู้มีคุณสมบัติตามมาตรา ๘ (๑) หรือตามมาตรา ๘ (๔) แล้วแต่กรณี รวมทั้งมีคุณสมบัติและไม่มีลักษณะต้องห้ามตามมาตรา ๑๑ และยินยอมให้เสนอชื่อเข้ารับคัดเลือกเท่ากับจำนวนประธานกรรมการตามมาตรา ๘ (๑) หรือกรรมการผู้ทรงคุณวุฒิตามมาตรา ๘ (๔) ที่จะได้รับแต่งตั้ง

เมื่อได้คัดเลือกบุคคลเป็นประธานกรรมการตามมาตรา ๘ (๑) หรือกรรมการผู้ทรงคุณวุฒิตามมาตรา ๘ (๔) ครบจำนวนแล้ว ให้คณะกรรมการสรรหาแจ้งรายชื่อประธานกรรมการตามมาตรา ๘ (๑) หรือกรรมการผู้ทรงคุณวุฒิตามมาตรา ๘ (๔) พร้อมหลักฐานแสดงคุณสมบัติและการไม่มีลักษณะต้องห้าม รวมทั้งความยินยอมของบุคคลดังกล่าวต่อคณะรัฐมนตรีเพื่อแต่งตั้งเป็นประธานกรรมการตามมาตรา ๘ (๑) หรือกรรมการผู้ทรงคุณวุฒิตามมาตรา ๘ (๔)

ให้นายกรัฐมนตรีประกาศรายชื่อประธานกรรมการตามมาตรา ๘ (๑) หรือกรรมการผู้ทรงคุณวุฒิตามมาตรา ๘ (๔) ซึ่งได้รับแต่งตั้งจากคณะรัฐมนตรีในราชกิจจานุเบกษา

มาตรา ๑๑ ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิต้องมีคุณสมบัติและไม่มีลักษณะต้องห้าม ดังต่อไปนี้

(๑) มีสัญชาติไทย

(๒) ไม่เป็นบุคคลล้มละลายหรือเคยเป็นบุคคลล้มละลายทุจริต

(๓) ไม่เป็นคนไร้ความสามารถหรือคนเสมือนไร้ความสามารถ

(๔) ไม่เคยต้องคำพิพากษาถึงที่สุดให้จำคุกไม่ว่าจะได้รับโทษจำคุกจริงหรือไม่ เว้นแต่เป็นโทษสำหรับความผิดที่ได้กระทำโดยประมาทหรือความผิดลหุโทษ

(๕) ไม่เคยถูกไล่ออก ปลดออก หรือให้ออกจากราชการ หน่วยงานของรัฐ หรือรัฐวิสาหกิจ หรือจากหน่วยงานของเอกชน เพราะทุจริตต่อหน้าที่หรือประพฤติชั่วอย่างร้ายแรง

(๖) ไม่เคยถูกถอดถอนออกจากตำแหน่งตามกฎหมาย

(๗) ไม่เป็นผู้ดำรงตำแหน่งทางการเมือง สมาชิกสภาท้องถิ่น หรือผู้บริหารท้องถิ่น กรรมการหรือผู้ดำรงตำแหน่งซึ่งรับผิดชอบการบริหารพรรคการเมือง ที่ปรึกษาพรรคการเมือง หรือเจ้าหน้าที่พรรคการเมือง

มาตรา ๑๒ ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิมีวาระการดำรงตำแหน่งคราวละสี่ปี

เมื่อครบกำหนดตามวาระในวรรคหนึ่ง หากยังมิได้มีการแต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิขึ้นใหม่ ให้ประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งตามวาระนั้นอยู่ในตำแหน่งเพื่อดำเนินงานต่อไปจนกว่าประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิซึ่งได้รับแต่งตั้งใหม่เข้ารับหน้าที่

ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งตามวาระอาจได้รับแต่งตั้งอีกได้ แต่จะดำรงตำแหน่งเกินสองวาระไม่ได้

มาตรา ๑๓ นอกจากการพ้นจากตำแหน่งตามวาระตามมาตรา ๑๒ ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่ง เมื่อ

(๑) ตาย

(๒) ลาออก

(๓) คณะรัฐมนตรีให้ออก เพราะบกพร่องต่อหน้าที่ มีความประพฤติเสื่อมเสีย หรือหย่อนความสามารถ

(๔) ขาดคุณสมบัติหรือมีลักษณะต้องห้ามตามมาตรา ๑๑

ในกรณีที่ประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่งก่อนวาระ ให้ผู้ที่ได้รับแต่งตั้งแทนตำแหน่งที่ว่างนั้นดำรงตำแหน่งได้เท่ากับวาระที่เหลืออยู่ของประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิซึ่งตนแทน เว้นแต่วาระที่เหลืออยู่ไม่ถึงเก้าสิบวันจะไม่แต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิแทนก็ได้

ในกรณีที่ประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่งก่อนวาระ ให้คณะกรรมการประกอบด้วยกรรมการทั้งหมดเท่าที่มีอยู่จนกว่าจะมีการแต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิตามวรรคสอง และในกรณีที่ประธานกรรมการพ้นจากตำแหน่งก่อนวาระ ให้รองประธานกรรมการทำหน้าที่ประธานกรรมการเป็นการชั่วคราว

มาตรา ๑๔ การประชุมคณะกรรมการ ต้องมีกรรมการมาประชุมไม่น้อยกว่ากึ่งหนึ่งของจำนวนกรรมการที่มีอยู่ จึงจะเป็นองค์ประชุม

ให้ประธานกรรมการเป็นประธานในที่ประชุม ในกรณีที่ประธานกรรมการไม่มาประชุมหรือไม่อาจปฏิบัติหน้าที่ได้ ให้รองประธานกรรมการทำหน้าที่เป็นประธานในที่ประชุม ในกรณีที่ประธานกรรมการและรองประธานกรรมการไม่มาประชุมหรือไม่อาจปฏิบัติหน้าที่ได้ ให้กรรมการซึ่งมาประชุมเลือกกรรมการคนหนึ่งเป็นประธานในที่ประชุม

การวินิจฉัยชี้ขาดของที่ประชุมให้ถือเสียงข้างมาก กรรมการคนหนึ่งให้มีเสียงหนึ่งในการลงคะแนน ถ้าคะแนนเสียงเท่ากัน ให้ประธานในที่ประชุมออกเสียงเพิ่มขึ้นอีกเสียงหนึ่งเป็นเสียงชี้ขาด

การประชุมของคณะกรรมการอาจกระทำได้โดยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นได้ตามที่คณะกรรมการกำหนด

มาตรา ๑๕ กรรมการผู้ใดมีส่วนได้เสียไม่ว่าโดยตรงหรือโดยอ้อมในเรื่องที่ที่ประชุมพิจารณา ให้แจ้งการมีส่วนได้เสียของตนให้คณะกรรมการทราบล่วงหน้าก่อนการประชุม และห้ามมิให้ผู้นั้นเข้าร่วมประชุมพิจารณาในเรื่องดังกล่าว

มาตรา ๑๖ คณะกรรมการมีหน้าที่และอำนาจ ดังต่อไปนี้

(๑) จัดทำแผนแม่บทการดำเนินงานด้านการส่งเสริม และการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับนโยบาย ยุทธศาสตร์ชาติ และแผนระดับชาติที่เกี่ยวข้อง เพื่อเสนอต่อคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติตามกฎหมายว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม

(๒) ส่งเสริมและสนับสนุนหน่วยงานของรัฐและภาคเอกชน ดำเนินกิจกรรมตามแผนแม่บทตาม (๑) รวมทั้งจัดให้มีการประเมินผลการดำเนินงานตามแผนแม่บทดังกล่าว

(๓) กำหนดมาตรการหรือแนวทางการดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามพระราชบัญญัตินี้

(๔) ออกประกาศหรือระเบียบเพื่อให้การดำเนินการเป็นไปตามพระราชบัญญัตินี้

(๕) ประกาศกำหนดหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ

(๖) ประกาศกำหนดข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลเป็นแนวทางให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลปฏิบัติ

(๗) เสนอแนะต่อคณะรัฐมนตรีให้มีการตราหรือปรับปรุงกฎหมายหรือกฎที่ใช้บังคับอยู่ในส่วนที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

(๘) เสนอแนะต่อคณะรัฐมนตรีในการตราพระราชกฤษฎีกาหรือทบทวนความเหมาะสมของพระราชบัญญัตินี้อย่างน้อยทุกรอบห้าปี

(๙) ให้คำแนะนำและคำปรึกษาเกี่ยวกับการดำเนินการใด ๆ เพื่อให้ความคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐและภาคเอกชนในการปฏิบัติตามพระราชบัญญัตินี้

(๑๐) ตีความและวินิจฉัยชี้ขาดปัญหาที่เกิดจากการบังคับใช้พระราชบัญญัตินี้

(๑๑) ส่งเสริมและสนับสนุนให้เกิดทักษะการเรียนรู้และความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้แก่ประชาชน

(๑๒) ส่งเสริมและสนับสนุนการวิจัย เพื่อพัฒนาเทคโนโลยีที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

(๑๓) ปฏิบัติการอื่นใดตามที่พระราชบัญญัตินี้หรือกฎหมายอื่นกำหนดให้เป็นหน้าที่และอำนาจของคณะกรรมการ

มาตรา ๑๗ ให้ประธานกรรมการ รองประธานกรรมการ และกรรมการได้รับเบี้ยประชุมและประโยชน์ตอบแทนอื่นตามหลักเกณฑ์ที่คณะรัฐมนตรีกำหนด

ประธานอนุกรรมการ อนุกรรมการ ประธานกรรมการผู้เชี่ยวชาญ และกรรมการผู้เชี่ยวชาญที่คณะกรรมการแต่งตั้ง ให้ได้รับเบี้ยประชุมและประโยชน์ตอบแทนอื่นตามหลักเกณฑ์ที่คณะกรรมการกำหนดโดยความเห็นชอบของกระทรวงการคลัง

มาตรา ๑๘ คณะกรรมการมีอำนาจแต่งตั้งคณะอนุกรรมการเพื่อพิจารณาหรือปฏิบัติการอย่างใดอย่างหนึ่งตามที่คณะกรรมการมอบหมายได้

การประชุมคณะอนุกรรมการ ให้นำความในมาตรา ๑๔ และมาตรา ๑๕ มาใช้บังคับโดยอนุโลม

หมวด ๒
การคุ้มครองข้อมูลส่วนบุคคล

ส่วนที่ ๑
บททั่วไป

มาตรา ๑๙ ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น เว้นแต่บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้

การขอความยินยอมต้องทำโดยชัดแจ้ง เป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เว้นแต่โดยสภาพไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้

ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไปด้วย และการขอความยินยอมนั้นต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน มีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ รวมทั้งใช้ภาษาที่อ่านง่าย และไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ดังกล่าว ทั้งนี้ คณะกรรมการจะให้ผู้ควบคุมข้อมูลส่วนบุคคลขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามแบบและข้อความที่คณะกรรมการประกาศกำหนดก็ได้

ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องคำนึงอย่างถึงที่สุดในความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม ทั้งนี้ ในการเข้าทำสัญญาซึ่งรวมถึงการให้บริการใด ๆ ต้องไม่มีเงื่อนไขในการให้ความยินยอมเพื่อเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่มีความจำเป็นหรือเกี่ยวข้องสำหรับการเข้าทำสัญญาซึ่งรวมถึงการให้บริการนั้น ๆ

เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเสียเมื่อใดก็ได้โดยจะต้องถอนความยินยอมได้ง่ายเช่นเดียวกับการให้ความยินยอม เว้นแต่มีข้อจำกัดสิทธิในการถอนความยินยอมโดยกฎหมายหรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล ทั้งนี้ การถอนความยินยอมย่อมไม่ส่งผลกระทบต่อการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมไปแล้วโดยชอบตามที่กำหนดไว้ในหมวดนี้

ในกรณีที่การถอนความยินยอมส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลในเรื่องใด ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงผลกระทบจากการถอนความยินยอมนั้น

การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลที่ไม่เป็นไปตามที่กำหนดไว้ในหมวดนี้ ไม่มีผลผูกพันเจ้าของข้อมูลส่วนบุคคล และไม่ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถทำการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้

มาตรา ๒๐ ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ซึ่งยังไม่บรรลุนิติภาวะโดยการสมรสหรือไม่มีฐานะเสมือนดังบุคคลซึ่งบรรลุนิติภาวะแล้วตามมาตรา ๒๗ แห่งประมวลกฎหมายแพ่งและพาณิชย์ การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลดังกล่าว ให้ดำเนินการ ดังต่อไปนี้

(๑) ในกรณีที่การให้ความยินยอมของผู้เยาว์ไม่ใช่การใด ๆ ซึ่งผู้เยาว์อาจให้ความยินยอมโดยลำพังได้ตามที่บัญญัติไว้ในมาตรา ๒๒ มาตรา ๒๓ หรือมาตรา ๒๔ แห่งประมวลกฎหมายแพ่งและพาณิชย์ ต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ด้วย

(๒) ในกรณีที่ผู้เยาว์มีอายุไม่เกินสิบปี ให้ขอความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์

ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นคนไร้ความสามารถ การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลดังกล่าว ให้ขอความยินยอมจากผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถ

ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นคนเสมือนไร้ความสามารถ การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลดังกล่าว ให้ขอความยินยอมจากผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ

ให้นำความในวรรคหนึ่ง วรรคสอง และวรรคสาม มาใช้บังคับกับการถอนความยินยอมของเจ้าของข้อมูลส่วนบุคคล การแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล การร้องเรียนของเจ้าของข้อมูลส่วนบุคคล และการอื่นใดตามพระราชบัญญัตินี้ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นผู้เยาว์ คนไร้ความสามารถ หรือคนเสมือนไร้ความสามารถ โดยอนุโลม

มาตรา ๒๑ ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือในขณะที่เก็บรวบรวม

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่แตกต่างไปจากวัตถุประสงค์ที่ได้แจ้งไว้ตามวรรคหนึ่งจะกระทำมิได้ เว้นแต่

(๑) ได้แจ้งวัตถุประสงค์ใหม่นั้นให้เจ้าของข้อมูลส่วนบุคคลทราบและได้รับความยินยอมก่อนเก็บรวบรวม ใช้ หรือเปิดเผยแล้ว

(๒) บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้

ส่วนที่ ๒
การเก็บรวบรวมข้อมูลส่วนบุคคล

มาตรา ๒๒ การเก็บรวบรวมข้อมูลส่วนบุคคล ให้เก็บรวบรวมได้เท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

มาตรา ๒๓ ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียด ดังต่อไปนี้ เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว

(๑) วัตถุประสงค์ของการเก็บรวบรวมเพื่อการนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยซึ่งรวมถึงวัตถุประสงค์ตามที่มาตรา ๒๔ ให้อำนาจในการเก็บรวบรวมได้โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

(๒) แจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือสัญญาหรือมีความจำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา รวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล

(๓) ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม

(๔) ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย

(๕) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อในกรณีที่มีตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ให้แจ้งข้อมูล สถานที่ติดต่อ และวิธีการติดต่อของตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย

(๖) สิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา ๑๙ วรรคห้า มาตรา ๓๐ วรรคหนึ่ง มาตรา ๓๑ วรรคหนึ่ง มาตรา ๓๒ วรรคหนึ่ง มาตรา ๓๓ วรรคหนึ่ง มาตรา ๓๔ วรรคหนึ่ง มาตรา ๓๖ วรรคหนึ่ง และมาตรา ๗๓ วรรคหนึ่ง

มาตรา ๒๔ ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(๑) เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ตามที่คณะกรรมการประกาศกำหนด

(๒) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

(๓) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

(๔) เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

(๕) เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

(๖) เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

มาตรา ๒๕ ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่

(๑) ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า แต่ต้องไม่เกินสามสิบวันนับแต่วันที่เก็บรวบรวมและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

(๒) เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา ๒๔ หรือมาตรา ๒๖

ให้นำบทบัญญัติเกี่ยวกับการแจ้งวัตถุประสงค์ใหม่ตามมาตรา ๒๑ และการแจ้งรายละเอียดตามมาตรา ๒๓ มาใช้บังคับกับการเก็บรวบรวมข้อมูลส่วนบุคคลที่ต้องได้รับความยินยอมตามวรรคหนึ่งโดยอนุโลม เว้นแต่กรณีดังต่อไปนี้

(๑) เจ้าของข้อมูลส่วนบุคคลทราบวัตถุประสงค์ใหม่หรือรายละเอียดนั้นอยู่แล้ว

(๒) ผู้ควบคุมข้อมูลส่วนบุคคลพิสูจน์ได้ว่าการแจ้งวัตถุประสงค์ใหม่หรือรายละเอียดดังกล่าวไม่สามารถทำได้หรือจะเป็นอุปสรรคต่อการใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ ในกรณีนี้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิ เสรีภาพ และประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

(๓) การใช้หรือการเปิดเผยข้อมูลส่วนบุคคลต้องกระทำโดยเร่งด่วนตามที่กฎหมายกำหนด ซึ่งได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

(๔) เมื่อผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้ซึ่งล่วงรู้หรือได้มาซึ่งข้อมูลส่วนบุคคลจากหน้าที่หรือจากการประกอบอาชีพหรือวิชาชีพและต้องรักษาวัตถุประสงค์ใหม่หรือรายละเอียดบางประการตามมาตรา ๒๓ ไว้เป็นความลับตามที่กฎหมายกำหนด

การแจ้งรายละเอียดตามวรรคสอง ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบภายในสามสิบวันนับแต่วันที่เก็บรวบรวมตามมาตรานี้ เว้นแต่กรณีที่นำข้อมูลส่วนบุคคลไปใช้เพื่อการติดต่อกับเจ้าของข้อมูลส่วนบุคคลต้องแจ้งในการติดต่อครั้งแรก และกรณีที่จะนำข้อมูลส่วนบุคคลไปเปิดเผย ต้องแจ้งก่อนที่จะนำข้อมูลส่วนบุคคลไปเปิดเผยเป็นครั้งแรก

มาตรา ๒๖ ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(๑) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม

(๒) เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงานให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรตามวัตถุประสงค์ดังกล่าวโดยไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรนั้น

(๓) เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล

(๔) เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

(๕) เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ

(ก) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ ทั้งนี้ ในกรณีที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์

(ข) ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

(ค) การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองทางสังคม ซึ่งการเก็บรวบรวมข้อมูลส่วนบุคคลเป็นสิ่งจำเป็นในการปฏิบัติตามสิทธิหรือหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคล โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

(ง) การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น ทั้งนี้ ต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น และได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ตามที่คณะกรรมการประกาศกำหนด

(จ) ประโยชน์สาธารณะที่สำคัญ โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

ข้อมูลชีวภาพตามวรรคหนึ่งให้หมายถึงข้อมูลส่วนบุคคลที่เกิดจากการใช้เทคนิคหรือเทคโนโลยีที่เกี่ยวข้องกับการนำลักษณะเด่นทางกายภาพหรือทางพฤติกรรมของบุคคลมาใช้ทำให้สามารถยืนยันตัวตนของบุคคลนั้นที่ไม่เหมือนกับบุคคลอื่นได้ เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองม่านตา หรือข้อมูลจำลองลายนิ้วมือ

ในกรณีที่เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมต้องกระทำภายใต้การควบคุมของหน่วยงานที่มีอำนาจหน้าที่ตามกฎหมาย หรือได้จัดให้มีมาตรการคุ้มครองข้อมูลส่วนบุคคลตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด

ส่วนที่ ๓
การใช้หรือเปิดเผยข้อมูลส่วนบุคคล

มาตรา ๒๗ ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา ๒๔ หรือมาตรา ๒๖

บุคคลหรือนิติบุคคลที่ได้รับข้อมูลส่วนบุคคลมาจากการเปิดเผยตามวรรคหนึ่ง จะต้องไม่ใช้หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลส่วนบุคคลในการขอรับข้อมูลส่วนบุคคลนั้น

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกการใช้หรือเปิดเผยนั้นไว้ในรายการตามมาตรา ๓๙

มาตรา ๒๘ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ทั้งนี้ ต้องเป็นไปตามหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลตามที่คณะกรรมการประกาศกำหนดตามมาตรา ๑๖ (๕) เว้นแต่

(๑) เป็นการปฏิบัติตามกฎหมาย

(๒) ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลแล้ว

(๓) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

(๔) เป็นการกระทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่นเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

(๕) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้

(๖) เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ

ในกรณีที่มีปัญหาเกี่ยวกับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคล ให้เสนอต่อคณะกรรมการเป็นผู้วินิจฉัย ทั้งนี้ คำวินิจฉัยของคณะกรรมการอาจขอให้ทบทวนได้เมื่อมีหลักฐานใหม่ทำให้เชื่อได้ว่าประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลมีการพัฒนาจนมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ

มาตรา ๒๙ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักรได้กำหนดนโยบายในการคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ต่างประเทศและอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน หากนโยบายในการคุ้มครองข้อมูลส่วนบุคคลดังกล่าวได้รับการตรวจสอบและรับรองจากสำนักงาน การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศที่เป็นไปตามนโยบายในการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับการตรวจสอบและรับรองดังกล่าวให้สามารถกระทำได้โดยได้รับยกเว้นไม่ต้องปฏิบัติตามมาตรา ๒๘

นโยบายในการคุ้มครองข้อมูลส่วนบุคคล ลักษณะของเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน และหลักเกณฑ์และวิธีการตรวจสอบและรับรองตามวรรคหนึ่งให้เป็นไปตามที่คณะกรรมการประกาศกำหนด

ในกรณีที่ยังไม่มีคำวินิจฉัยของคณะกรรมการตามมาตรา ๒๘ หรือยังไม่มีนโยบายในการคุ้มครองข้อมูลส่วนบุคคลตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอาจส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศได้โดยได้รับยกเว้นไม่ต้องปฏิบัติตามมาตรา ๒๘ เมื่อผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้จัดให้มีมาตรการคุ้มครองที่เหมาะสมสามารถบังคับตามสิทธิของเจ้าของข้อมูลส่วนบุคคลได้ รวมทั้งมีมาตรการเยียวยาทางกฎหมายที่มีประสิทธิภาพตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

หมวด ๓
สิทธิของเจ้าของข้อมูลส่วนบุคคล

มาตรา ๓๐ เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอม

ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามคำขอตามวรรคหนึ่ง จะปฏิเสธคำขอได้เฉพาะในกรณีที่เป็นการปฏิเสธตามกฎหมายหรือคำสั่งศาล และการเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลนั้นจะส่งผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธคำขอตามวรรคหนึ่ง ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกการปฏิเสธคำขอดังกล่าวพร้อมด้วยเหตุผลไว้ในรายการตามมาตรา ๓๙

เมื่อเจ้าของข้อมูลส่วนบุคคลมีคำขอตามวรรคหนึ่งและเป็นกรณีที่ไม่อาจปฏิเสธคำขอได้ตามวรรคสอง ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามคำขอโดยไม่ชักช้า แต่ต้องไม่เกินสามสิบวันนับแต่วันที่ได้รับคำขอ

คณะกรรมการอาจกำหนดหลักเกณฑ์เกี่ยวกับการเข้าถึงและการขอรับสำเนาตามวรรคหนึ่ง รวมทั้งการขยายระยะเวลาตามวรรคสี่หรือหลักเกณฑ์อื่นตามความเหมาะสมก็ได้

มาตรา ๓๑ เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอรับข้อมูลส่วนบุคคลที่เกี่ยวกับตนจากผู้ควบคุมข้อมูลส่วนบุคคลได้ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้ทำให้ข้อมูลส่วนบุคคลนั้นอยู่ในรูปแบบที่สามารถอ่านหรือใช้งานโดยทั่วไปได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติและสามารถใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ด้วยวิธีการอัตโนมัติ รวมทั้งมีสิทธิ ดังต่อไปนี้

(๑) ขอให้ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลในรูปแบบดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นเมื่อสามารถทำได้ด้วยวิธีการอัตโนมัติ

(๒) ขอรับข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลในรูปแบบดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นโดยตรง เว้นแต่โดยสภาพทางเทคนิคไม่สามารถทำได้

ข้อมูลส่วนบุคคลตามวรรคหนึ่งต้องเป็นข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามหลักเกณฑ์แห่งพระราชบัญญัตินี้ หรือเป็นข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา ๒๔ (๓) หรือเป็นข้อมูลส่วนบุคคลอื่นที่กำหนดในมาตรา ๒๔ ตามที่คณะกรรมการประกาศกำหนด

การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามวรรคหนึ่งจะใช้กับการส่งหรือโอนข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะหรือเป็นการปฏิบัติหน้าที่ตามกฎหมายไม่ได้ หรือการใช้สิทธินั้นต้องไม่ละเมิดสิทธิหรือเสรีภาพของบุคคลอื่น ทั้งนี้ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธคำขอด้วยเหตุผลดังกล่าว ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกการปฏิเสธคำขอพร้อมด้วยเหตุผลไว้ในรายการตามมาตรา ๓๙

มาตรา ๓๒ เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตนเมื่อใดก็ได้ ดังต่อไปนี้

(๑) กรณีที่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา ๒๔ (๔) หรือ (๕) เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลพิสูจน์ได้ว่า

(ก) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้น ผู้ควบคุมข้อมูลส่วนบุคคลได้แสดงให้เห็นถึงเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า

(ข) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

(๒) กรณีที่เป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง

(๓) กรณีที่เป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ เว้นแต่เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล

ในกรณีที่เจ้าของข้อมูลส่วนบุคคลใช้สิทธิคัดค้านตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นต่อไปได้ ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติโดยแยกส่วนออกจากข้อมูลอื่นอย่างชัดเจนในทันทีเมื่อเจ้าของข้อมูลส่วนบุคคลได้แจ้งการคัดค้านให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบ

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธการคัดค้านด้วยเหตุผลตาม (๑) (ก) หรือ (ข) หรือ (๓) ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกการปฏิเสธการคัดค้านพร้อมด้วยเหตุผลไว้ในรายการตามมาตรา ๓๙

มาตรา ๓๓ เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ในกรณีดังต่อไปนี้

(๑) เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

(๒) เมื่อเจ้าของข้อมูลส่วนบุคคลถอนความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคลไม่มีอำนาจตามกฎหมายที่จะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นได้ต่อไป

(๓) เมื่อเจ้าของข้อมูลส่วนบุคคลคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา ๓๒ (๑) และผู้ควบคุมข้อมูลส่วนบุคคลไม่อาจปฏิเสธคำขอตามมาตรา ๓๒ (๑) (ก) หรือ (ข) ได้ หรือเป็นการคัดค้านตามมาตรา ๓๒ (๒)

(๔) เมื่อข้อมูลส่วนบุคคลได้ถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยไม่ชอบด้วยกฎหมายตามที่กำหนดไว้ในหมวดนี้

ความในวรรคหนึ่งมิให้นำมาใช้บังคับกับการเก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น การเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา ๒๔ (๑) หรือ (๔) หรือมาตรา ๒๖ (๕) (ก) หรือ (ข) การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้ทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่เปิดเผยต่อสาธารณะและผู้ควบคุมข้อมูลส่วนบุคคลถูกขอให้ลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลต้องเป็นผู้รับผิดชอบดำเนินการทั้งในทางเทคโนโลยีและค่าใช้จ่ายเพื่อให้เป็นไปตามคำขอนั้น โดยแจ้งผู้ควบคุมข้อมูลส่วนบุคคลอื่น ๆ เพื่อให้ได้รับคำตอบในการดำเนินการให้เป็นไปตามคำขอ

กรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามวรรคหนึ่งหรือวรรคสาม เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการได้

คณะกรรมการอาจประกาศกำหนดหลักเกณฑ์ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลตามวรรคหนึ่งก็ได้

มาตรา ๓๔ เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการใช้ข้อมูลส่วนบุคคลได้ ในกรณีดังต่อไปนี้

(๑) เมื่อผู้ควบคุมข้อมูลส่วนบุคคลอยู่ในระหว่างการตรวจสอบตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอให้ดำเนินการตามมาตรา ๓๖

(๒) เมื่อเป็นข้อมูลส่วนบุคคลที่ต้องลบหรือทำลายตามมาตรา ๓๓ (๔) แต่เจ้าของข้อมูลส่วนบุคคลขอให้ระงับการใช้แทน

(๓) เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล แต่เจ้าของข้อมูลส่วนบุคคลมีความจำเป็นต้องขอให้เก็บรักษาไว้เพื่อใช้ในการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

(๔) เมื่อผู้ควบคุมข้อมูลส่วนบุคคลอยู่ในระหว่างการพิสูจน์ตามมาตรา ๓๒ (๑) หรือตรวจสอบตามมาตรา ๓๒ (๓) เพื่อปฏิเสธการคัดค้านของเจ้าของข้อมูลส่วนบุคคลตามมาตรา ๓๒ วรรคสาม

กรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามวรรคหนึ่ง เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการได้

คณะกรรมการอาจประกาศกำหนดหลักเกณฑ์ในการระงับการใช้ตามวรรคหนึ่งก็ได้

มาตรา ๓๕ ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด

มาตรา ๓๖ ในกรณีที่เจ้าของข้อมูลส่วนบุคคลร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามมาตรา ๓๕ หากผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามคำร้องขอ ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกคำร้องขอของเจ้าของข้อมูลส่วนบุคคลพร้อมด้วยเหตุผลไว้ในรายการตามมาตรา ๓๙

ให้นำความในมาตรา ๓๔ วรรคสอง มาใช้บังคับโดยอนุโลม

มาตรา ๓๗ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(๑) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด

(๒) ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

(๓) จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น

การเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา ๒๔ (๑) หรือ (๔) หรือมาตรา ๒๖ (๕) (ก) หรือ (ข) การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย ทั้งนี้ ให้นำความในมาตรา ๓๓ วรรคห้า มาใช้บังคับกับการลบหรือทำลายข้อมูลส่วนบุคคลโดยอนุโลม

(๔) แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

(๕) ในกรณีที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา ๕ วรรคสอง ต้องแต่งตั้งตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลเป็นหนังสือซึ่งตัวแทนต้องอยู่ในราชอาณาจักรและตัวแทนต้องได้รับมอบอำนาจให้กระทำการแทนผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่มีข้อจำกัดความรับผิดใด ๆ ที่เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ของผู้ควบคุมข้อมูลส่วนบุคคล

มาตรา ๓๘ บทบัญญัติเกี่ยวกับการแต่งตั้งตัวแทนตามมาตรา ๓๗ (๕) มิให้นำมาใช้บังคับแก่ผู้ควบคุมข้อมูลส่วนบุคคล ดังต่อไปนี้

(๑) ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นหน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด

(๒) ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งประกอบอาชีพหรือธุรกิจในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่มีลักษณะตามมาตรา ๒๖ และไม่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการประกาศกำหนดตามมาตรา ๔๑ (๒)

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา ๕ วรรคสอง มีผู้ประมวลผลข้อมูลส่วนบุคคล ให้นำความในมาตรา ๓๗ (๕) และความในวรรคหนึ่ง มาใช้บังคับแก่ผู้ประมวลผลข้อมูลส่วนบุคคลนั้นโดยอนุโลม

มาตรา ๓๙ ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกรายการ อย่างน้อยดังต่อไปนี้ เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานสามารถตรวจสอบได้ โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้

(๑) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม

(๒) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท

(๓) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล

(๔) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

(๕) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น

(๖) การใช้หรือเปิดเผยตามมาตรา ๒๗ วรรคสาม

(๗) การปฏิเสธคำขอหรือการคัดค้านตามมาตรา ๓๐ วรรคสาม มาตรา ๓๑ วรรคสาม มาตรา ๓๒ วรรคสาม และมาตรา ๓๖ วรรคหนึ่ง

(๘) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา ๓๗ (๑)

ความในวรรคหนึ่งให้นำมาใช้บังคับกับตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา ๕ วรรคสอง โดยอนุโลม

ความใน (๑) (๒) (๓) (๔) (๕) (๖) และ (๘) อาจยกเว้นมิให้นำมาใช้บังคับกับผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด เว้นแต่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือมิใช่กิจการที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว หรือมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา ๒๖

มาตรา ๔๐ ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(๑) ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้

(๒) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

(๓) จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

ผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งไม่ปฏิบัติตาม (๑) สำหรับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลใด ให้ถือว่าผู้ประมวลผลข้อมูลส่วนบุคคลเป็นผู้ควบคุมข้อมูลส่วนบุคคลสำหรับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้น

การดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีข้อตกลงระหว่างกัน เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามพระราชบัญญัตินี้

ความใน (๓) อาจยกเว้นมิให้นำมาใช้บังคับกับผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด เว้นแต่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือมิใช่กิจการที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว หรือมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา ๒๖

มาตรา ๔๑ ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของตน ในกรณีดังต่อไปนี้

(๑) ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นหน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด

(๒) การดำเนินกิจกรรมของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในการเก็บรวบรวม ใช้ หรือเปิดเผย จำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอโดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการประกาศกำหนด

(๓) กิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา ๒๖

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกันตามที่คณะกรรมการประกาศกำหนดตามมาตรา ๒๙ วรรคสอง ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าวอาจจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลร่วมกันได้ ทั้งนี้ สถานที่ทำการแต่ละแห่งของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันดังกล่าวต้องสามารถติดต่อกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้โดยง่าย

ความในวรรคสองให้นำมาใช้บังคับแก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งเป็นหน่วยงานของรัฐตาม (๑) ซึ่งมีขนาดใหญ่หรือมีสถานที่ทำการหลายแห่งโดยอนุโลม

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลตามวรรคหนึ่งต้องแต่งตั้งตัวแทนตามมาตรา ๓๗ (๕) ให้นำความในวรรคหนึ่งมาใช้บังคับแก่ตัวแทนโดยอนุโลม

ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานทราบ ทั้งนี้ เจ้าของข้อมูลส่วนบุคคลสามารถติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้ได้

คณะกรรมการอาจประกาศกำหนดคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้ โดยคำนึงถึงความรู้หรือความเชี่ยวชาญเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจเป็นพนักงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลหรือเป็นผู้รับจ้างให้บริการตามสัญญากับผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลก็ได้

มาตรา ๔๒ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(๑) ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้

(๒) ตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามพระราชบัญญัตินี้

(๓) ประสานงานและให้ความร่วมมือกับสำนักงานในกรณีที่มีปัญหาเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในการปฏิบัติตามพระราชบัญญัตินี้

(๔) รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้

ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลต้องสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยจัดหาเครื่องมือหรืออุปกรณ์อย่างเพียงพอ รวมทั้งอำนวยความสะดวกในการเข้าถึงข้อมูลส่วนบุคคลเพื่อการปฏิบัติหน้าที่

ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลจะให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลออกจากงานหรือเลิกสัญญาการจ้างด้วยเหตุที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ไม่ได้ ทั้งนี้ ในกรณีที่มีปัญหาในการปฏิบัติหน้าที่ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องสามารถรายงานไปยังผู้บริหารสูงสุดของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลโดยตรงได้

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจปฏิบัติหน้าที่หรือภารกิจอื่นได้ แต่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลต้องรับรองกับสำนักงานว่าหน้าที่หรือภารกิจดังกล่าวต้องไม่ขัดหรือแย้งต่อการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้

หมวด ๔
สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

มาตรา ๔๓ ให้มีสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลมีวัตถุประสงค์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งส่งเสริมและสนับสนุนให้เกิดการพัฒนาด้านการคุ้มครองข้อมูลส่วนบุคคลของประเทศ

สำนักงานเป็นหน่วยงานของรัฐมีฐานะเป็นนิติบุคคล และไม่เป็นส่วนราชการตามกฎหมายว่าด้วยระเบียบบริหารราชการแผ่นดิน หรือรัฐวิสาหกิจตามกฎหมายว่าด้วยวิธีการงบประมาณหรือกฎหมายอื่น

กิจการของสำนักงานไม่อยู่ภายใต้บังคับแห่งกฎหมายว่าด้วยการคุ้มครองแรงงาน กฎหมายว่าด้วยแรงงานสัมพันธ์ กฎหมายว่าด้วยแรงงานรัฐวิสาหกิจสัมพันธ์ กฎหมายว่าด้วยการประกันสังคม และกฎหมายว่าด้วยเงินทดแทน แต่พนักงานและลูกจ้างของสำนักงานต้องได้รับประโยชน์ตอบแทนไม่น้อยกว่าที่กำหนดไว้ในกฎหมายว่าด้วยการคุ้มครองแรงงาน กฎหมายว่าด้วยการประกันสังคม และกฎหมายว่าด้วยเงินทดแทน

ให้สำนักงานเป็นหน่วยงานของรัฐตามกฎหมายว่าด้วยความรับผิดทางละเมิดของเจ้าหน้าที่

มาตรา ๔๔ นอกจากหน้าที่และอำนาจในการดำเนินการให้เป็นไปตามวัตถุประสงค์ตามมาตรา ๔๓ วรรคหนึ่ง ให้สำนักงานมีหน้าที่ปฏิบัติงานวิชาการและงานธุรการให้แก่คณะกรรมการ คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล คณะกรรมการผู้เชี่ยวชาญ และคณะอนุกรรมการ รวมทั้งให้มีหน้าที่และอำนาจ ดังต่อไปนี้

(๑) จัดทำร่างแผนแม่บทการดำเนินงานด้านการส่งเสริม และการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับนโยบาย ยุทธศาสตร์ชาติ และแผนระดับชาติที่เกี่ยวข้อง รวมทั้งร่างแผนแม่บทและมาตรการแก้ไขปัญหาอุปสรรคการปฏิบัติการตามนโยบาย ยุทธศาสตร์ชาติ และแผนระดับชาติดังกล่าว เพื่อเสนอต่อคณะกรรมการ

(๒) ส่งเสริมและสนับสนุนการวิจัย เพื่อพัฒนาเทคโนโลยีที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

(๓) วิเคราะห์และรับรองความสอดคล้องและความถูกต้องตามมาตรฐานหรือตามมาตรการหรือกลไกการกำกับดูแลที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งตรวจสอบและรับรองนโยบายในการคุ้มครองข้อมูลส่วนบุคคลตามมาตรา ๒๙

(๔) สำรวจ เก็บรวบรวมข้อมูล ติดตามความเคลื่อนไหวของสถานการณ์ด้านการคุ้มครองข้อมูลส่วนบุคคล และแนวโน้มการเปลี่ยนแปลงด้านการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งวิเคราะห์และวิจัยประเด็นทางด้านการคุ้มครองข้อมูลส่วนบุคคลที่มีผลต่อการพัฒนาประเทศเพื่อเสนอต่อคณะกรรมการ

(๕) ประสานงานกับส่วนราชการ รัฐวิสาหกิจ ราชการส่วนท้องถิ่น องค์การมหาชน หรือหน่วยงานอื่นของรัฐเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

(๖) ให้คำปรึกษาแก่หน่วยงานของรัฐและหน่วยงานของเอกชนเกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้

(๗) เป็นศูนย์กลางในการให้บริการทางวิชาการหรือให้บริการที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลแก่หน่วยงานของรัฐ หน่วยงานของเอกชน และประชาชน รวมทั้งเผยแพร่และให้ความรู้ความเข้าใจในเรื่องการคุ้มครองข้อมูลส่วนบุคคล

(๘) กำหนดหลักสูตรและฝึกอบรมการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ลูกจ้าง ผู้รับจ้าง หรือประชาชนทั่วไป

(๙) ทำความตกลงและร่วมมือกับองค์การหรือหน่วยงานทั้งในประเทศและต่างประเทศในกิจการที่เกี่ยวกับการดำเนินการตามหน้าที่และอำนาจของสำนักงาน เมื่อได้รับความเห็นชอบจากคณะกรรมการ

(๑๐) ติดตามและประเมินผลการปฏิบัติตามพระราชบัญญัตินี้

(๑๑) ปฏิบัติหน้าที่อื่นตามที่คณะกรรมการ คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล คณะกรรมการผู้เชี่ยวชาญ หรือคณะอนุกรรมการมอบหมาย หรือตามที่กฎหมายกำหนด

มาตรา ๔๕ ในการดำเนินงานของสำนักงาน นอกจากหน้าที่และอำนาจตามที่บัญญัติในมาตรา ๔๔ แล้ว ให้สำนักงานมีหน้าที่และอำนาจทั่วไป ดังต่อไปนี้ด้วย

(๑) ถือกรรมสิทธิ์ มีสิทธิครอบครอง และมีทรัพยสิทธิต่าง ๆ

(๒) ก่อตั้งสิทธิ หรือทำนิติกรรมทุกประเภทผูกพันทรัพย์สิน ตลอดจนทำนิติกรรมอื่นใดเพื่อประโยชน์ในการดำเนินกิจการของสำนักงาน

(๓) จัดให้มีและให้ทุนเพื่อสนับสนุนการดำเนินกิจการของสำนักงาน

(๔) เรียกเก็บค่าธรรมเนียม ค่าบำรุง ค่าตอบแทน หรือค่าบริการในการดำเนินงานต่าง ๆ ตามวัตถุประสงค์ของสำนักงาน ทั้งนี้ ตามหลักเกณฑ์และอัตราที่สำนักงานกำหนดโดยความเห็นชอบของคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

(๕) ปฏิบัติการอื่นใดที่กฎหมายกำหนดให้เป็นหน้าที่และอำนาจของสำนักงาน หรือตามที่คณะกรรมการ คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล คณะกรรมการผู้เชี่ยวชาญ หรือคณะอนุกรรมการมอบหมาย

มาตรา ๔๖ ทุนและทรัพย์สินในการดำเนินงานของสำนักงานประกอบด้วย

(๑) ทุนประเดิมที่รัฐบาลจัดสรรให้ตามมาตรา ๙๔ วรรคหนึ่ง

(๒) เงินอุดหนุนทั่วไปที่รัฐบาลจัดสรรให้ตามความเหมาะสมเป็นรายปี

(๓) เงินอุดหนุนจากหน่วยงานของรัฐทั้งในประเทศและต่างประเทศ หรือองค์การระหว่างประเทศระดับรัฐบาล

(๔) ค่าธรรมเนียม ค่าบำรุง ค่าตอบแทน ค่าบริการ หรือรายได้อันเกิดจากการดำเนินการตามหน้าที่และอำนาจของสำนักงาน

(๕) ดอกผลของเงินหรือรายได้จากทรัพย์สินของสำนักงาน

เงินและทรัพย์สินของสำนักงานตามวรรคหนึ่ง ต้องนำส่งคลังเป็นรายได้แผ่นดิน

มาตรา ๔๗ บรรดาอสังหาริมทรัพย์ที่สำนักงานได้มาจากการซื้อหรือแลกเปลี่ยนจากรายได้ของสำนักงานตามมาตรา ๔๖ (๔) หรือ (๕) ให้เป็นกรรมสิทธิ์ของสำนักงาน

มาตรา ๔๘ ให้มีคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ประกอบด้วยประธานกรรมการซึ่งสรรหาและแต่งตั้งจากผู้มีความรู้ ความเชี่ยวชาญ และประสบการณ์ในด้านการคุ้มครองข้อมูลส่วนบุคคล ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และเลขาธิการคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ เป็นกรรมการ และกรรมการผู้ทรงคุณวุฒิจำนวนหกคนซึ่งสรรหาและแต่งตั้งจากผู้มีความรู้ ความเชี่ยวชาญ และประสบการณ์ในด้านการคุ้มครองข้อมูลส่วนบุคคลอย่างน้อยสามคน และด้านอื่นที่เกี่ยวข้องอันเป็นประโยชน์ต่อการดำเนินงานของสำนักงาน

ให้เลขาธิการเป็นกรรมการและเลขานุการ และให้เลขาธิการแต่งตั้งพนักงานของสำนักงานเป็นผู้ช่วยเลขานุการได้ไม่เกินสองคน

ให้นำความในมาตรา ๑๑ และมาตรา ๑๓ มาใช้บังคับกับประธานกรรมการและกรรมการผู้ทรงคุณวุฒิโดยอนุโลม

มาตรา ๔๙ ให้มีคณะกรรมการสรรหาคณะหนึ่งประกอบด้วยบุคคลซึ่งคณะกรรมการแต่งตั้งจำนวนแปดคนทำหน้าที่คัดเลือกบุคคลที่สมควรได้รับการแต่งตั้งเป็นประธานกรรมการและกรรมการผู้ทรงคุณวุฒิตามมาตรา ๔๘

ให้คณะกรรมการสรรหาเลือกกรรมการสรรหาคนหนึ่งเป็นประธานกรรมการสรรหาและเลือกกรรมการสรรหาอีกคนหนึ่งเป็นเลขานุการคณะกรรมการสรรหา และให้สำนักงานปฏิบัติหน้าที่เป็นหน่วยธุรการของคณะกรรมการสรรหา

ในกรณีที่ตำแหน่งกรรมการสรรหาว่างลง ให้ดำเนินการเพื่อให้มีกรรมการสรรหาแทนในตำแหน่งนั้นโดยเร็ว ในระหว่างที่ยังไม่ได้กรรมการสรรหาใหม่ ให้คณะกรรมการสรรหาประกอบด้วยกรรมการสรรหาเท่าที่มีอยู่

กรรมการสรรหาไม่มีสิทธิได้รับการเสนอชื่อเป็นประธานกรรมการและกรรมการผู้ทรงคุณวุฒิตามมาตรา ๔๘

หลักเกณฑ์และวิธีการสรรหาให้เป็นไปตามที่คณะกรรมการกำหนด ทั้งนี้ ต้องคำนึงถึงความโปร่งใสและความเป็นธรรมในการสรรหา

มาตรา ๕๐ ในการสรรหาประธานกรรมการและกรรมการผู้ทรงคุณวุฒิตามมาตรา ๔๘ ให้คณะกรรมการสรรหาคัดเลือกบุคคลผู้มีคุณสมบัติตามมาตรา ๔๘ วรรคหนึ่ง รวมทั้งมีคุณสมบัติและไม่มีลักษณะต้องห้ามตามมาตรา ๔๘ วรรคสาม และยินยอมให้เสนอชื่อเข้ารับคัดเลือกเท่ากับจำนวนประธานกรรมการและกรรมการผู้ทรงคุณวุฒิตามมาตรา ๔๘ ที่จะได้รับแต่งตั้ง

เมื่อได้คัดเลือกบุคคลเป็นประธานกรรมการและกรรมการผู้ทรงคุณวุฒิตามมาตรา ๔๘ ครบจำนวนแล้ว ให้คณะกรรมการสรรหาแจ้งรายชื่อประธานกรรมการและกรรมการผู้ทรงคุณวุฒิตามมาตรา ๔๘ พร้อมหลักฐานแสดงคุณสมบัติและการไม่มีลักษณะต้องห้าม รวมทั้งความยินยอมของบุคคลดังกล่าวต่อคณะกรรมการเพื่อแต่งตั้งเป็นประธานกรรมการและกรรมการผู้ทรงคุณวุฒิตามมาตรา ๔๘

ให้คณะกรรมการประกาศรายชื่อประธานกรรมการและกรรมการผู้ทรงคุณวุฒิตามมาตรา ๔๘ ซึ่งได้รับแต่งตั้งในราชกิจจานุเบกษา

มาตรา ๕๑ ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิตามมาตรา ๔๘ มีวาระการดำรงตำแหน่งคราวละสี่ปี

เมื่อครบกำหนดตามวาระในวรรคหนึ่ง ให้ดำเนินการแต่งตั้งประธานกรรมการและกรรมการผู้ทรงคุณวุฒิขึ้นใหม่ภายในหกสิบวัน ในระหว่างที่ยังมิได้มีการแต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิขึ้นใหม่ ให้ประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งตามวาระนั้นอยู่ในตำแหน่งเพื่อดำเนินงานต่อไปจนกว่าประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิซึ่งได้รับแต่งตั้งใหม่เข้ารับหน้าที่

ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งตามวาระอาจได้รับแต่งตั้งอีกได้ แต่จะดำรงตำแหน่งเกินสองวาระไม่ได้

มาตรา ๕๒ ในกรณีที่ประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิตามมาตรา ๔๘ พ้นจากตำแหน่งก่อนวาระ ให้คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกอบด้วยกรรมการทั้งหมดเท่าที่มีอยู่จนกว่าจะมีการแต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิแทน และในกรณีที่ประธานกรรมการพ้นจากตำแหน่งก่อนวาระ ให้ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมทำหน้าที่ประธานกรรมการเป็นการชั่วคราว

ให้ดำเนินการแต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิแทนตำแหน่งที่ว่างภายในหกสิบวันนับแต่วันที่ตำแหน่งว่างลง และให้ผู้ที่ได้รับแต่งตั้งให้ดำรงตำแหน่งแทนอยู่ในตำแหน่งเท่ากับวาระที่เหลืออยู่ของผู้ซึ่งตนแทน เว้นแต่วาระของประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิเหลือไม่ถึงเก้าสิบวันจะไม่แต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิแทนก็ได้

มาตรา ๕๓ การประชุมคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลต้องมีกรรมการมาประชุมไม่น้อยกว่ากึ่งหนึ่งของจำนวนกรรมการที่มีอยู่ จึงจะเป็นองค์ประชุม

ให้ประธานกรรมการเป็นประธานในที่ประชุม ถ้าประธานกรรมการไม่มาประชุมหรือไม่อาจปฏิบัติหน้าที่ได้ ให้กรรมการซึ่งมาประชุมเลือกกรรมการคนหนึ่งเป็นประธานในที่ประชุม

การวินิจฉัยชี้ขาดของที่ประชุมให้ถือเสียงข้างมาก กรรมการคนหนึ่งให้มีเสียงหนึ่งในการลงคะแนน ถ้าคะแนนเสียงเท่ากัน ให้ประธานในที่ประชุมออกเสียงเพิ่มขึ้นอีกเสียงหนึ่งเป็นเสียงชี้ขาด

กรรมการที่มีส่วนได้เสียในเรื่องที่มีการพิจารณาจะเข้าร่วมประชุมมิได้

การประชุมของคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอาจกระทำโดยวิธีการทางอิเล็กทรอนิกส์ตามที่คณะกรรมการกำหนดก็ได้

มาตรา ๕๔ คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลมีหน้าที่และอำนาจ ดังต่อไปนี้

(๑) กำหนดนโยบายการบริหารงาน และให้ความเห็นชอบแผนการดำเนินงานของสำนักงาน

(๒) ออกข้อบังคับว่าด้วยการจัดองค์กร การเงิน การบริหารงานบุคคล การบริหารงานทั่วไป การตรวจสอบภายใน รวมตลอดทั้งการสงเคราะห์และสวัสดิการต่าง ๆ ของสำนักงาน

(๓) อนุมัติแผนการดำเนินงาน แผนการใช้จ่ายเงินและงบประมาณรายจ่ายประจำปีของสำนักงาน

(๔) ควบคุมการบริหารงานและการดำเนินการของสำนักงานและเลขาธิการให้เป็นไปตามพระราชบัญญัตินี้และกฎหมายอื่นที่เกี่ยวข้อง

(๕) แต่งตั้งคณะกรรมการสรรหาเลขาธิการ

(๖) วินิจฉัยอุทธรณ์คำสั่งทางปกครองของเลขาธิการในส่วนที่เกี่ยวกับการบริหารงานของสำนักงาน

(๗) ประเมินผลการดำเนินการของสำนักงาน และการปฏิบัติงานของเลขาธิการ

(๘) ปฏิบัติหน้าที่อื่นตามที่พระราชบัญญัตินี้หรือกฎหมายอื่นกำหนดให้เป็นหน้าที่และอำนาจของคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือตามที่คณะกรรมการหรือคณะรัฐมนตรีมอบหมาย

ข้อบังคับตาม (๒) ถ้ามีการจำกัดอำนาจเลขาธิการในการทำนิติกรรมกับบุคคลภายนอก ให้ประกาศในราชกิจจานุเบกษา

มาตรา ๕๕ คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลมีอำนาจแต่งตั้งคณะอนุกรรมการ เพื่อปฏิบัติหน้าที่หรือกระทำการอย่างหนึ่งอย่างใดตามที่คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลมอบหมายได้

คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอาจแต่งตั้งบุคคลซึ่งมีความเชี่ยวชาญหรือประสบการณ์ที่จะเป็นประโยชน์ในการปฏิบัติหน้าที่ของคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เป็นที่ปรึกษาคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้

การปฏิบัติหน้าที่และจำนวนของคณะอนุกรรมการตามวรรคหนึ่งหรือบุคคลตามวรรคสอง ให้เป็นไปตามที่คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

การประชุมคณะอนุกรรมการ ให้นำความในมาตรา ๕๓ มาใช้บังคับโดยอนุโลม

มาตรา ๕๖ ให้ประธานกรรมการและกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ที่ปรึกษาคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ประธานอนุกรรมการและอนุกรรมการที่คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแต่งตั้ง ได้รับเบี้ยประชุมหรือค่าตอบแทนตามหลักเกณฑ์ที่คณะกรรมการกำหนดโดยความเห็นชอบของกระทรวงการคลัง

มาตรา ๕๗ ให้สำนักงานมีเลขาธิการคนหนึ่งซึ่งคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแต่งตั้ง มีหน้าที่บริหารกิจการของสำนักงาน

การแต่งตั้งเลขาธิการตามวรรคหนึ่ง ให้เป็นไปตามหลักเกณฑ์และวิธีการสรรหาตามที่คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

มาตรา ๕๘ ผู้ที่จะได้รับการแต่งตั้งเป็นเลขาธิการต้องมีคุณสมบัติ ดังต่อไปนี้

(๑) มีสัญชาติไทย

(๒) อายุไม่ต่ำกว่าสามสิบห้าปีแต่ไม่เกินหกสิบปี

(๓) เป็นผู้มีความรู้ ความสามารถ และประสบการณ์ในด้านที่เกี่ยวกับภารกิจของสำนักงานและการบริหารจัดการ

มาตรา ๕๙ ผู้มีลักษณะอย่างใดอย่างหนึ่งดังต่อไปนี้ ต้องห้ามมิให้เป็นเลขาธิการ

(๑) เป็นบุคคลล้มละลายหรือเคยเป็นบุคคลล้มละลายทุจริต

(๒) เป็นคนไร้ความสามารถหรือคนเสมือนไร้ความสามารถ

(๓) เคยต้องคำพิพากษาถึงที่สุดให้จำคุกไม่ว่าจะได้รับโทษจำคุกจริงหรือไม่ เว้นแต่เป็นโทษสำหรับความผิดที่ได้กระทำโดยประมาทหรือความผิดลหุโทษ

(๔) เป็นข้าราชการ พนักงาน หรือลูกจ้าง ของส่วนราชการหรือรัฐวิสาหกิจหรือหน่วยงานอื่นของรัฐหรือของราชการส่วนท้องถิ่น

(๕) เป็นหรือเคยเป็นข้าราชการการเมือง ผู้ดำรงตำแหน่งทางการเมือง สมาชิกสภาท้องถิ่นหรือผู้บริหารท้องถิ่น เว้นแต่จะได้พ้นจากตำแหน่งมาแล้วไม่น้อยกว่าหนึ่งปี

(๖) เป็นหรือเคยเป็นกรรมการหรือผู้ดำรงตำแหน่งอื่นในพรรคการเมืองหรือเจ้าหน้าที่ของพรรคการเมือง เว้นแต่จะได้พ้นจากตำแหน่งมาแล้วไม่น้อยกว่าหนึ่งปี

(๗) เคยถูกไล่ออก ปลดออก หรือให้ออกจากราชการ หรือออกจากงานจากหน่วยงานที่เคยปฏิบัติหน้าที่ เพราะทุจริตต่อหน้าที่หรือประพฤติชั่วอย่างร้ายแรง หรือเคยถูกถอดถอนจากตำแหน่ง

(๘) เคยถูกให้ออกเพราะไม่ผ่านการประเมินผลการปฏิบัติงานตามมาตรา ๖๒ (๔)

(๙) เป็นผู้มีส่วนได้เสียในกิจการที่เกี่ยวข้องกับสำนักงานไม่ว่าโดยทางตรงหรือทางอ้อม

มาตรา ๖๐ เลขาธิการมีวาระการดำรงตำแหน่งคราวละสี่ปี และอาจได้รับแต่งตั้งอีกได้ แต่จะดำรงตำแหน่งเกินสองวาระไม่ได้

ก่อนครบกำหนดตามวาระการดำรงตำแหน่งของเลขาธิการเป็นเวลาไม่น้อยกว่าสามสิบวันแต่ไม่เกินหกสิบวัน หรือภายในสามสิบวันนับแต่วันที่เลขาธิการพ้นจากตำแหน่งก่อนครบวาระ ให้คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแต่งตั้งคณะกรรมการสรรหาเพื่อสรรหาเลขาธิการคนใหม่ ทั้งนี้ ให้คณะกรรมการสรรหาเสนอรายชื่อบุคคลที่เหมาะสมไม่เกินสามคนต่อคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

มาตรา ๖๑ ในแต่ละปีให้มีการประเมินผลการปฏิบัติงานของเลขาธิการ ทั้งนี้ ให้เป็นไปตามระยะเวลาและวิธีการที่คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

มาตรา ๖๒ นอกจากการพ้นจากตำแหน่งตามวาระตามมาตรา ๖๐ เลขาธิการพ้นจากตำแหน่ง เมื่อ

(๑) ตาย

(๒) ลาออก

(๓) ขาดคุณสมบัติตามมาตรา ๕๘ หรือมีลักษณะต้องห้ามตามมาตรา ๕๙

(๔) คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลให้ออก เพราะไม่ผ่านการประเมินผลการปฏิบัติงาน มีความประพฤติเสื่อมเสีย บกพร่องหรือไม่สุจริตต่อหน้าที่ หรือหย่อนความสามารถ

มาตรา ๖๓ ให้เลขาธิการมีหน้าที่และอำนาจ ดังต่อไปนี้

(๑) บริหารงานของสำนักงานให้เกิดผลสัมฤทธิ์ตามภารกิจของสำนักงาน และตามนโยบายและแผนระดับชาติ แผนยุทธศาสตร์ นโยบายของคณะรัฐมนตรี คณะกรรมการ และคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และระเบียบ ข้อบังคับหรือมติของคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

(๒) วางระเบียบเกี่ยวกับการดำเนินงานของสำนักงานโดยไม่ขัดหรือแย้งกับกฎหมาย มติของคณะรัฐมนตรี และระเบียบ ข้อบังคับ ข้อกำหนด นโยบาย มติ หรือประกาศที่คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

(๓) เป็นผู้บังคับบัญชาพนักงานและลูกจ้างของสำนักงาน และประเมินผลการปฏิบัติงานของพนักงานและลูกจ้างของสำนักงานตามระเบียบหรือข้อบังคับของสำนักงาน

(๔) แต่งตั้งรองเลขาธิการและผู้ช่วยเลขาธิการโดยความเห็นชอบของคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเพื่อเป็นผู้ช่วยปฏิบัติงานของเลขาธิการตามที่เลขาธิการมอบหมาย

(๕) บรรจุ แต่งตั้ง เลื่อน ลด ตัดเงินเดือนหรือค่าจ้าง ลงโทษทางวินัยพนักงาน และลูกจ้างของสำนักงาน ตลอดจนให้พนักงานและลูกจ้างของสำนักงานออกจากตำแหน่ง ทั้งนี้ ตามระเบียบหรือข้อบังคับที่คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

(๖) ปฏิบัติการอื่นใดตามระเบียบ ข้อบังคับ ข้อกำหนด นโยบาย มติ หรือประกาศของคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ให้เลขาธิการรับผิดชอบในการบริหารงานของสำนักงานขึ้นตรงต่อคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

มาตรา ๖๔ ในกิจการของสำนักงานที่เกี่ยวกับบุคคลภายนอก ให้เลขาธิการเป็นผู้แทนของสำนักงาน เพื่อการนี้ เลขาธิการจะมอบอำนาจให้บุคคลใดปฏิบัติงานเฉพาะอย่างแทนก็ได้ แต่ต้องเป็นไปตามข้อบังคับที่คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

มาตรา ๖๕ ให้คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นผู้กำหนดอัตราเงินเดือนและประโยชน์ตอบแทนอื่นของเลขาธิการตามหลักเกณฑ์ที่คณะรัฐมนตรีกำหนด

มาตรา ๖๖ เพื่อประโยชน์ในการบริหารงานของสำนักงาน เลขาธิการอาจขอให้ข้าราชการ พนักงาน เจ้าหน้าที่ หรือลูกจ้างของส่วนราชการ หน่วยงานของรัฐ รัฐวิสาหกิจ ราชการส่วนท้องถิ่น องค์การมหาชน หรือหน่วยงานอื่นของรัฐ มาปฏิบัติงานเป็นพนักงานหรือลูกจ้างเป็นการชั่วคราวได้ ทั้งนี้ เมื่อได้รับอนุมัติจากผู้บังคับบัญชาหรือนายจ้างของผู้นั้น และมีข้อตกลงที่ทำไว้ในการอนุมัติ และในกรณีที่เจ้าหน้าที่ของรัฐได้รับอนุมัติให้มาปฏิบัติงานเป็นพนักงานหรือลูกจ้างเป็นการชั่วคราว ให้ถือว่าเป็นการได้รับอนุญาตให้ออกจากราชการหรือออกจากงานไปปฏิบัติงานใด ๆ

เมื่อสิ้นสุดระยะเวลาที่ได้รับอนุมัติให้มาปฏิบัติงานในสำนักงาน ให้เจ้าหน้าที่ของรัฐตามวรรคหนึ่งมีสิทธิได้รับการบรรจุและแต่งตั้งให้ดำรงตำแหน่งและรับเงินเดือนในส่วนราชการหรือหน่วยงานเดิมไม่ต่ำกว่าตำแหน่งและเงินเดือนเดิมตามข้อตกลงที่ทำไว้ในการอนุมัติ

ในกรณีที่เจ้าหน้าที่ของรัฐผู้นั้นกลับมาบรรจุและได้รับแต่งตั้งในส่วนราชการหรือหน่วยงานเดิมตามวรรคสองแล้ว ให้นับระยะเวลาของเจ้าหน้าที่ของรัฐผู้นั้นระหว่างที่มาปฏิบัติงานในสำนักงานสำหรับการคำนวณบำเหน็จบำนาญหรือประโยชน์ตอบแทนอื่นทำนองเดียวกันเสมือนอยู่ปฏิบัติราชการหรือปฏิบัติงานเต็มเวลาดังกล่าว แล้วแต่กรณี

มาตรา ๖๗ ข้าราชการหรือเจ้าหน้าที่ของรัฐซึ่งอยู่ระหว่างการปฏิบัติงานชดใช้ทุนการศึกษาที่ได้รับจากส่วนราชการหรือหน่วยงานของรัฐ ที่ได้ย้ายมาปฏิบัติหน้าที่ที่สำนักงานโดยได้รับความเห็นชอบจากผู้บังคับบัญชาต้นสังกัด ให้ถือเป็นการชดใช้ทุนตามสัญญา และให้นับระยะเวลาการปฏิบัติงานในสำนักงานเป็นระยะเวลาในการชดใช้ทุน

ในกรณีที่หน่วยงานของรัฐแห่งใดประสงค์จะขอให้พนักงานของสำนักงานซึ่งอยู่ระหว่างการปฏิบัติงานชดใช้ทุนการศึกษาที่ได้รับจากสำนักงานไปเป็นข้าราชการหรือเจ้าหน้าที่ของรัฐในหน่วยงานของรัฐแห่งนั้น ต้องได้รับความเห็นชอบจากเลขาธิการก่อน และให้ถือว่าการไปปฏิบัติงานในหน่วยงานของรัฐแห่งนั้นเป็นการชดใช้ทุนตามสัญญา และให้นับระยะเวลาการปฏิบัติงานในหน่วยงานของรัฐแห่งนั้นเป็นระยะเวลาในการชดใช้ทุน

มาตรา ๖๘ การบัญชีของสำนักงานให้จัดทำตามหลักสากล ตามแบบและหลักเกณฑ์ที่คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

มาตรา ๖๙ ให้สำนักงานจัดทำงบการเงินและบัญชี แล้วส่งผู้สอบบัญชีภายในหนึ่งร้อยยี่สิบวันนับแต่วันสิ้นปีบัญชี

ให้สำนักงานการตรวจเงินแผ่นดินหรือผู้สอบบัญชีรับอนุญาตที่สำนักงานการตรวจเงินแผ่นดินให้ความเห็นชอบเป็นผู้สอบบัญชีของสำนักงาน และประเมินผลการใช้จ่ายเงินและทรัพย์สินของสำนักงานทุกรอบปีแล้วทำรายงานผลการสอบบัญชีเสนอต่อคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเพื่อรับรอง

มาตรา ๗๐ ให้สำนักงานจัดทำรายงานการดำเนินงานประจำปีเสนอคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและรัฐมนตรีภายในหนึ่งร้อยแปดสิบวันนับแต่วันสิ้นปีบัญชี และเผยแพร่รายงานนี้ต่อสาธารณชน

รายงานการดำเนินงานประจำปีตามวรรคหนึ่ง ให้แสดงรายละเอียดของงบการเงินที่ผู้สอบบัญชีให้ความเห็นแล้ว พร้อมทั้งผลงานของสำนักงานและรายงานการประเมินผลการดำเนินงานของสำนักงานในปีที่ล่วงมาแล้ว

การประเมินผลการดำเนินงานของสำนักงานตามวรรคสอง จะต้องดำเนินการโดยบุคคลภายนอกที่คณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลให้ความเห็นชอบ

หมวด ๕
การร้องเรียน

มาตรา ๗๑ ให้คณะกรรมการแต่งตั้งคณะกรรมการผู้เชี่ยวชาญขึ้นคณะหนึ่งหรือหลายคณะก็ได้ตามความเชี่ยวชาญในแต่ละเรื่องหรือตามที่คณะกรรมการเห็นสมควร

คุณสมบัติและลักษณะต้องห้าม วาระการดำรงตำแหน่ง การพ้นจากตำแหน่ง และการดำเนินงานอื่นของคณะกรรมการผู้เชี่ยวชาญให้เป็นไปตามที่คณะกรรมการประกาศกำหนด

มาตรา ๗๒ คณะกรรมการผู้เชี่ยวชาญมีหน้าที่และอำนาจ ดังต่อไปนี้

(๑) พิจารณาเรื่องร้องเรียนตามพระราชบัญญัตินี้

(๒) ตรวจสอบการกระทำใด ๆ ของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับข้อมูลส่วนบุคคลที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคล

(๓) ไกล่เกลี่ยข้อพิพาทเกี่ยวกับข้อมูลส่วนบุคคล

(๔) ปฏิบัติการอื่นใดตามที่พระราชบัญญัตินี้กำหนดให้เป็นหน้าที่และอำนาจของคณะกรรมการผู้เชี่ยวชาญหรือตามที่คณะกรรมการมอบหมาย

มาตรา ๗๓ เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัติหรือประกาศที่ออกตามพระราชบัญญัตินี้

การยื่น การไม่รับเรื่อง การยุติเรื่อง การพิจารณา และระยะเวลาในการพิจารณาคำร้องเรียนให้เป็นไปตามระเบียบที่คณะกรรมการประกาศกำหนดโดยคำนึงถึงการกำหนดให้ไม่รับเรื่องร้องเรียนหรือยุติเรื่องในกรณีที่มีผู้มีอำนาจพิจารณาในเรื่องนั้นอยู่แล้วตามกฎหมายอื่นด้วย

มาตรา ๗๔ ในกรณีที่ผู้ร้องเรียนไม่ได้ปฏิบัติให้ถูกต้องตามระเบียบที่กำหนดไว้ในมาตรา ๗๓ วรรคสอง หรือเป็นเรื่องร้องเรียนที่ระเบียบนั้นได้กำหนดไม่ให้รับไว้พิจารณา ให้คณะกรรมการผู้เชี่ยวชาญไม่รับเรื่องร้องเรียนไว้พิจารณา

เมื่อคณะกรรมการผู้เชี่ยวชาญพิจารณาเรื่องร้องเรียนตามมาตรา ๗๒ (๑) หรือตรวจสอบการกระทำใด ๆ ตามมาตรา ๗๒ (๒) แล้วรับฟังได้ว่า เรื่องร้องเรียนหรือการกระทำนั้นไม่มีมูล ให้คณะกรรมการผู้เชี่ยวชาญมีคำสั่งยุติเรื่อง

ในกรณีที่คณะกรรมการผู้เชี่ยวชาญพิจารณาหรือตรวจสอบตามวรรคสองแล้วรับฟังได้ว่าเรื่องร้องเรียนหรือการกระทำนั้นเป็นกรณีซึ่งอาจไกล่เกลี่ยได้และคู่กรณีประสงค์จะให้ไกล่เกลี่ย ให้คณะกรรมการผู้เชี่ยวชาญดำเนินการไกล่เกลี่ย แต่หากเรื่องร้องเรียนหรือการกระทำนั้นไม่อาจไกล่เกลี่ยได้ หรือไกล่เกลี่ยไม่สำเร็จ ให้คณะกรรมการผู้เชี่ยวชาญมีอำนาจออกคำสั่ง ดังต่อไปนี้

(๑) สั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลปฏิบัติหรือดำเนินการแก้ไขการกระทำของตนให้ถูกต้องภายในระยะเวลาที่กำหนด

(๒) สั่งห้ามผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลกระทำการที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลหรือให้กระทำการใดเพื่อระงับความเสียหายนั้นภายในระยะเวลาที่กำหนด

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลไม่ยอมดำเนินการตามคำสั่งตามวรรคสาม (๑) หรือ (๒) ให้นำบทบัญญัติเกี่ยวกับการบังคับทางปกครองตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองมาใช้บังคับโดยอนุโลม ทั้งนี้ ในกรณีที่ต้องมีการยึด อายัด หรือขายทอดตลาดทรัพย์สินของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเพื่อบังคับตามหลักเกณฑ์ที่กำหนดไว้ในกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครอง ให้คณะกรรมการผู้เชี่ยวชาญเป็นผู้มีอำนาจสั่งยึด อายัด หรือขายทอดตลาดทรัพย์สินเพื่อการนั้น

การจัดทำคำสั่งตามวรรคหนึ่ง วรรคสอง หรือวรรคสาม (๑) หรือ (๒) ให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

คำสั่งของคณะกรรมการผู้เชี่ยวชาญ ให้ประธานกรรมการผู้เชี่ยวชาญเป็นผู้ลงนามแทน

คำสั่งของคณะกรรมการผู้เชี่ยวชาญตามมาตรานี้ให้เป็นที่สุด

ในการดำเนินการตามมาตรานี้ เมื่อผลการพิจารณาเป็นประการใด ให้คณะกรรมการผู้เชี่ยวชาญแจ้งให้ผู้ร้องเรียนทราบพร้อมด้วยเหตุผล และในกรณีที่ไม่รับเรื่องร้องเรียนหรือยุติเรื่องที่มีผู้มีอำนาจพิจารณาในเรื่องนั้นอยู่แล้วตามกฎหมายอื่น ให้แจ้งผู้ร้องเรียนทราบ หากผู้ร้องเรียนประสงค์จะให้ส่งเรื่องให้ผู้มีอำนาจพิจารณาในเรื่องนั้นตามกฎหมายอื่น ให้ดำเนินการตามความประสงค์ดังกล่าว และให้ถือว่าผู้มีอำนาจพิจารณาได้รับเรื่องร้องเรียนนับแต่วันที่คณะกรรมการผู้เชี่ยวชาญได้รับเรื่องร้องเรียนนั้น

มาตรา ๗๕ คณะกรรมการผู้เชี่ยวชาญมีอำนาจสั่งให้บุคคลใดส่งเอกสารหรือข้อมูลเกี่ยวกับเรื่องที่มีผู้ร้องเรียน หรือเรื่องอื่นใดที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้ รวมทั้งจะสั่งให้บุคคลใดมาชี้แจงข้อเท็จจริงด้วยก็ได้

มาตรา ๗๖ ในการปฏิบัติการตามพระราชบัญญัตินี้ พนักงานเจ้าหน้าที่มีหน้าที่และอำนาจดังต่อไปนี้

(๑) มีหนังสือแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล หรือผู้ใดมาให้ข้อมูลหรือส่งเอกสารหรือหลักฐานใด ๆ เกี่ยวกับการดำเนินการหรือการกระทำความผิดตามพระราชบัญญัตินี้

(๒) ตรวจสอบและรวบรวมข้อเท็จจริง แล้วรายงานต่อคณะกรรมการผู้เชี่ยวชาญ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล หรือผู้ใดได้กระทำผิดหรือทำให้เกิดความเสียหายเพราะฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัติหรือประกาศที่ออกตามพระราชบัญญัตินี้

ในการดำเนินการตาม (๒) หากมีความจำเป็นเพื่อคุ้มครองประโยชน์ของเจ้าของข้อมูลส่วนบุคคลหรือเพื่อประโยชน์สาธารณะ ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่เข้าไปในสถานที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ใดเกี่ยวกับการกระทำความผิดตามพระราชบัญญัตินี้ ในระหว่างเวลาพระอาทิตย์ขึ้นถึงพระอาทิตย์ตกหรือในเวลาทำการของสถานที่นั้น เพื่อตรวจสอบและรวบรวมข้อเท็จจริง ยึดหรืออายัดเอกสารหลักฐาน หรือสิ่งอื่นใดที่เกี่ยวกับการกระทำความผิด หรือมีเหตุอันควรเชื่อได้ว่ามีไว้หรือใช้เพื่อกระทำความผิด

ในการแต่งตั้งพนักงานเจ้าหน้าที่ ให้รัฐมนตรีพิจารณาแต่งตั้งจากข้าราชการหรือเจ้าหน้าที่อื่นของรัฐซึ่งดำรงตำแหน่งไม่ต่ำกว่าข้าราชการพลเรือนระดับปฏิบัติการหรือเทียบเท่าและมีคุณสมบัติตามที่คณะกรรมการประกาศกำหนด

ในการปฏิบัติหน้าที่ของพนักงานเจ้าหน้าที่ตามมาตรานี้ ต้องแสดงบัตรประจำตัวต่อผู้ที่เกี่ยวข้องและให้ผู้ที่เกี่ยวข้องอำนวยความสะดวกตามสมควร

บัตรประจำตัวพนักงานเจ้าหน้าที่ ให้เป็นไปตามแบบที่คณะกรรมการประกาศกำหนด

หมวด ๖
ความรับผิดทางแพ่ง

มาตรา ๗๗ ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลอันเป็นการฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติแห่งพระราชบัญญัตินี้ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้นแก่เจ้าของข้อมูลส่วนบุคคล ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่ก็ตาม เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้นจะพิสูจน์ได้ว่า

(๑) ความเสียหายนั้นเกิดจากเหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั้นเอง

(๒) เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามหน้าที่และอำนาจตามกฎหมาย

ค่าสินไหมทดแทนตามวรรคหนึ่ง ให้หมายความรวมถึงค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย

มาตรา ๗๘ ให้ศาลมีอำนาจสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลจ่ายค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มขึ้นจากจำนวนค่าสินไหมทดแทนที่แท้จริงที่ศาลกำหนดได้ตามที่ศาลเห็นสมควร แต่ไม่เกินสองเท่าของค่าสินไหมทดแทนที่แท้จริงนั้น ทั้งนี้ โดยคำนึงถึงพฤติการณ์ต่าง ๆ เช่น ความร้ายแรงของความเสียหายที่เจ้าของข้อมูลส่วนบุคคลได้รับ ผลประโยชน์ที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้รับ สถานะทางการเงินของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล การที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้บรรเทาความเสียหายที่เกิดขึ้น หรือการที่เจ้าของข้อมูลส่วนบุคคลมีส่วนในการก่อให้เกิดความเสียหายด้วย

สิทธิเรียกร้องค่าเสียหายอันเกิดจากการละเมิดข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้เป็นอันขาดอายุความเมื่อพ้นสามปีนับแต่วันที่ผู้เสียหายรู้ถึงความเสียหายและรู้ตัวผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ต้องรับผิด หรือเมื่อพ้นสิบปีนับแต่วันที่มีการละเมิดข้อมูลส่วนบุคคล

หมวด ๗
บทกำหนดโทษ

ส่วนที่ ๑
โทษอาญา

มาตรา ๗๙ ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา ๒๗ วรรคหนึ่งหรือวรรคสอง หรือไม่ปฏิบัติตามมาตรา ๒๘ อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา ๒๖ โดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ

ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา ๒๗ วรรคหนึ่งหรือวรรคสอง หรือไม่ปฏิบัติตามมาตรา ๒๘ อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา ๒๖ เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งล้านบาท หรือทั้งจำทั้งปรับ

ความผิดตามมาตรานี้เป็นความผิดอันยอมความได้

มาตรา ๘๐ ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ถ้าผู้นั้นนำไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ

ความในวรรคหนึ่ง มิให้นำมาใช้บังคับแก่การเปิดเผย ในกรณีดังต่อไปนี้

(๑) การเปิดเผยตามหน้าที่

(๒) การเปิดเผยเพื่อประโยชน์แก่การสอบสวน หรือการพิจารณาคดี

(๓) การเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย

(๔) การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล

(๕) การเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่าง ๆ ที่เปิดเผยต่อสาธารณะ

มาตรา ๘๑ ในกรณีที่ผู้กระทำความผิดตามพระราชบัญญัตินี้เป็นนิติบุคคล ถ้าการกระทำความผิดของนิติบุคคลนั้นเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ ด้วย

ส่วนที่ ๒
โทษทางปกครอง

มาตรา ๘๒ ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา ๒๓ มาตรา ๓๐ วรรคสี่ มาตรา ๓๙ วรรคหนึ่ง มาตรา ๔๑ วรรคหนึ่ง หรือมาตรา ๔๒ วรรคสองหรือวรรคสาม หรือไม่ขอความยินยอมตามแบบหรือข้อความที่คณะกรรมการประกาศกำหนดตามมาตรา ๑๙ วรรคสาม หรือไม่แจ้งผลกระทบจากการถอนความยินยอมตามมาตรา ๑๙ วรรคหก หรือไม่ปฏิบัติตามมาตรา ๒๓ ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา ๒๕ วรรคสอง ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท

มาตรา ๘๓ ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา ๒๑ มาตรา ๒๒ มาตรา ๒๔ มาตรา ๒๕ วรรคหนึ่ง มาตรา ๒๗ วรรคหนึ่งหรือวรรคสอง มาตรา ๒๘ มาตรา ๓๒ วรรคสอง หรือมาตรา ๓๗ หรือขอความยินยอมโดยการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ หรือไม่ปฏิบัติตามมาตรา ๒๑ ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา ๒๕ วรรคสอง หรือส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่เป็นไปตามมาตรา ๒๙ วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษปรับทางปกครองไม่เกินสามล้านบาท

มาตรา ๘๔ ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา ๒๖ วรรคหนึ่งหรือวรรคสาม หรือฝ่าฝืนมาตรา ๒๗ วรรคหนึ่งหรือวรรคสอง หรือมาตรา ๒๘ อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา ๒๖ หรือส่งหรือโอนข้อมูลส่วนบุคคลตามมาตรา ๒๖ โดยไม่เป็นไปตามมาตรา ๒๙ วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษปรับทางปกครองไม่เกินห้าล้านบาท

มาตรา ๘๕ ผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา ๔๑ วรรคหนึ่ง หรือมาตรา ๔๒ วรรคสองหรือวรรคสาม ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท

มาตรา ๘๖ ผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา ๔๐ โดยไม่มีเหตุอันควรหรือส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่เป็นไปตามมาตรา ๒๙ วรรคหนึ่งหรือวรรคสาม หรือไม่ปฏิบัติตามมาตรา ๓๗ (๕) ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา ๓๘ วรรคสอง ต้องระวางโทษปรับทางปกครองไม่เกินสามล้านบาท

มาตรา ๘๗ ผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดส่งหรือโอนข้อมูลส่วนบุคคลตามมาตรา ๒๖ วรรคหนึ่งหรือวรรคสาม โดยไม่เป็นไปตามมาตรา ๒๙ วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษปรับทางปกครองไม่เกินห้าล้านบาท

มาตรา ๘๘ ตัวแทนผู้ควบคุมข้อมูลส่วนบุคคลหรือตัวแทนผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา ๓๙ วรรคหนึ่ง ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา ๓๙ วรรคสองและมาตรา ๔๑ วรรคหนึ่ง ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา ๔๑ วรรคสี่ ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท

มาตรา ๘๙ ผู้ใดไม่ปฏิบัติตามคำสั่งของคณะกรรมการผู้เชี่ยวชาญหรือไม่มาชี้แจงข้อเท็จจริงตามมาตรา ๗๕ หรือไม่ปฏิบัติตามมาตรา ๗๖ (๑) หรือไม่อำนวยความสะดวกแก่พนักงานเจ้าหน้าที่ตามมาตรา ๗๖ วรรคสี่ ต้องระวางโทษปรับทางปกครองไม่เกินห้าแสนบาท

มาตรา ๙๐ คณะกรรมการผู้เชี่ยวชาญมีอำนาจสั่งลงโทษปรับทางปกครองตามที่กำหนดไว้ในส่วนนี้ ทั้งนี้ ในกรณีที่เห็นสมควรคณะกรรมการผู้เชี่ยวชาญจะสั่งให้แก้ไขหรือตักเตือนก่อนก็ได้

ในการพิจารณาออกคำสั่งลงโทษปรับทางปกครอง ให้คณะกรรมการผู้เชี่ยวชาญคำนึงถึงความร้ายแรงแห่งพฤติกรรมที่กระทำผิด ขนาดกิจการของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล หรือพฤติการณ์ต่าง ๆ ประกอบด้วย ทั้งนี้ ตามหลักเกณฑ์ที่คณะกรรมการกำหนด

ในกรณีที่ผู้ถูกลงโทษปรับทางปกครองไม่ยอมชำระค่าปรับทางปกครอง ให้นำบทบัญญัติเกี่ยวกับการบังคับทางปกครองตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองมาใช้บังคับโดยอนุโลม และในกรณีที่ไม่มีเจ้าหน้าที่ดำเนินการบังคับตามคำสั่ง หรือมีแต่ไม่สามารถดำเนินการบังคับทางปกครองได้ ให้คณะกรรมการผู้เชี่ยวชาญมีอำนาจฟ้องคดีต่อศาลปกครองเพื่อบังคับชำระค่าปรับ ในการนี้ ถ้าศาลปกครองเห็นว่าคำสั่งให้ชำระค่าปรับนั้นชอบด้วยกฎหมาย ให้ศาลปกครองมีอำนาจพิจารณาพิพากษา และบังคับให้มีการยึดหรืออายัดทรัพย์สินขายทอดตลาดเพื่อชำระค่าปรับได้

คำสั่งลงโทษปรับทางปกครองและคำสั่งในการบังคับทางปกครอง ให้นำความในมาตรา ๗๔ วรรคหก มาใช้บังคับโดยอนุโลม และให้นำความในมาตรา ๗๔ วรรคสี่ มาใช้บังคับกับการบังคับทางปกครองตามวรรคสามโดยอนุโลม

บทเฉพาะกาล

มาตรา ๙๑ ในวาระเริ่มแรก ให้คณะกรรมการประกอบด้วยกรรมการตามมาตรา ๘ (๒) (๓) และให้เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นกรรมการและเลขานุการ เพื่อปฏิบัติหน้าที่เท่าที่จำเป็นไปพลางก่อนแต่ไม่เกินเก้าสิบวันนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ และให้รองประธานกรรมการทำหน้าที่ประธานกรรมการเป็นการชั่วคราว

ให้สำนักงานดำเนินการให้มีการแต่งตั้งประธานกรรมการตามมาตรา ๘ (๑) และกรรมการผู้ทรงคุณวุฒิตามมาตรา ๘ (๔) ภายในเก้าสิบวันนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ

มาตรา ๙๒ ให้ดำเนินการเพื่อให้มีคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายในเก้าสิบวันนับแต่วันที่ได้มีการแต่งตั้งประธานกรรมการ และกรรมการผู้ทรงคุณวุฒิตามมาตรา ๙๑

ให้ดำเนินการแต่งตั้งเลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้ให้แล้วเสร็จภายในเก้าสิบวันนับแต่วันที่จัดตั้งสำนักงานแล้วเสร็จตามมาตรา ๙๓

มาตรา ๙๓ ให้ดำเนินการจัดตั้งสำนักงานให้แล้วเสร็จเพื่อปฏิบัติงานตามพระราชบัญญัตินี้ภายในหนึ่งปีนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ

หน้า ๙๓
เล่ม ๑๓๖ ตอนที่ ๖๙ ก ราชกิจจานุเบกษา ๒๗ พฤษภาคม ๒๕๖๒

ในระหว่างที่การดำเนินการจัดตั้งสำนักงานยังไม่แล้วเสร็จ ให้สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมทำหน้าที่สำนักงานตามพระราชบัญญัตินี้ และให้รัฐมนตรีแต่งตั้งรองปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมคนหนึ่งทำหน้าที่เลขาธิการจนกว่าจะมีการแต่งตั้งเลขาธิการตามมาตรา ๙๒ วรรคสอง

มาตรา ๙๔ ในวาระเริ่มแรก ให้คณะรัฐมนตรีจัดสรรทุนประเดิมให้แก่สำนักงานตามความจำเป็น

ให้รัฐมนตรีเสนอต่อคณะรัฐมนตรีเพื่อพิจารณาให้ข้าราชการ พนักงาน เจ้าหน้าที่ หรือผู้ปฏิบัติงานอื่นใดในหน่วยงานของรัฐ มาปฏิบัติงานเป็นพนักงานของสำนักงานเป็นการชั่วคราวภายในระยะเวลาที่คณะรัฐมนตรีกำหนด

ให้ถือว่าข้าราชการ พนักงาน เจ้าหน้าที่ หรือผู้ปฏิบัติงานอื่นใดในหน่วยงานของรัฐที่มาปฏิบัติงานในสำนักงานเป็นการชั่วคราวตามวรรคสองไม่ขาดจากสถานภาพเดิมและคงได้รับเงินเดือนหรือค่าจ้างแล้วแต่กรณี จากสังกัดเดิม ทั้งนี้ คณะกรรมการอาจกำหนดค่าตอบแทนพิเศษให้แก่ข้าราชการ พนักงาน เจ้าหน้าที่ หรือผู้ปฏิบัติงานอื่นใดในหน่วยงานของรัฐตามวรรคสอง ในระหว่างปฏิบัติงานในสำนักงานด้วยก็ได้

ภายในหนึ่งร้อยแปดสิบวันนับแต่วันที่จัดตั้งสำนักงานแล้วเสร็จ ให้สำนักงานดำเนินการคัดเลือกข้าราชการ พนักงาน เจ้าหน้าที่ หรือผู้ปฏิบัติงานอื่นใดในหน่วยงานของรัฐตามวรรคสองเพื่อบรรจุเป็นพนักงานของสำนักงานต่อไป

ข้าราชการ พนักงาน เจ้าหน้าที่ หรือผู้ปฏิบัติงานอื่นใดในหน่วยงานของรัฐผู้ใดได้รับการคัดเลือกและบรรจุตามวรรคสี่ ให้มีสิทธินับระยะเวลาทำงานที่เคยทำงานอยู่ในสังกัดเดิมต่อเนื่องรวมกับระยะเวลาทำงานในสำนักงานตามพระราชบัญญัตินี้

มาตรา ๙๕ ข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลได้เก็บรวบรวมไว้ก่อนวันที่พระราชบัญญัตินี้ใช้บังคับ ให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวมรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปได้ตามวัตถุประสงค์เดิม ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลต้องกำหนดวิธีการยกเลิกความยินยอมและเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวมรวมและใช้ข้อมูลส่วนบุคคลดังกล่าวสามารถแจ้งยกเลิกความยินยอมได้โดยง่าย

การเปิดเผยและการดำเนินการอื่นที่มิใช่การเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลตามวรรคหนึ่งให้เป็นไปตามบทบัญญัติแห่งพระราชบัญญัตินี้

หน้า ๙๔
เล่ม ๑๓๖ ตอนที่ ๖๙ ก ราชกิจจานุเบกษา ๒๗ พฤษภาคม ๒๕๖๒

มาตรา ๙๖ การดำเนินการออกระเบียบ และประกาศตามพระราชบัญญัตินี้ ให้ดำเนินการให้แล้วเสร็จภายในหนึ่งปีนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ หากไม่สามารถดำเนินการได้ให้รัฐมนตรีรายงานเหตุผลที่ไม่อาจดำเนินการได้ต่อคณะรัฐมนตรีเพื่อทราบ

ผู้รับสนองพระบรมราชโองการ
พลเอก ประยุทธ์ จันทร์โอชา
นายกรัฐมนตรี

หน้า ๙๕
เล่ม ๑๓๖ ตอนที่ ๖๙ ก ราชกิจจานุเบกษา ๒๗ พฤษภาคม ๒๕๖๒

หมายเหตุ :- เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ เนื่องจากปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวก และรวดเร็ว ก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวม สมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้น เพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป จึงจำเป็นต้องตราพระราชบัญญัตินี้

ประวัติผู้เขียน

ชื่อ ชื่อสกุล	นายนพดล นิ่มหนู
ประวัติการศึกษา	นิติศาสตรบัณฑิต จุฬาลงกรณมหาวิทยาลัย ปีที่สำเร็จการศึกษา พ.ศ.2543
	นิติศาสตรมหาบัณฑิต จุฬาลงกรณมหาวิทยาลัย ปีที่สำเร็จการศึกษา พ.ศ.2548
	เนติบัณฑิตไทย สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา ปีที่สำเร็จการศึกษา พ.ศ.2549
ประสบการณ์ทำงาน	พ.ศ.2544-2545 นิติกร (เจ้าพนักงานพิทักษ์ทรัพย์) สำนักฟื้นฟูกิจการของลูกหนี้ กรมบังคับคดี
	พ.ศ.2547-2553 อาจารย์ประจำวิทยาลัยการเมืองการปกครอง มหาวิทยาลัยมหาสารคาม
	พ.ศ.2557-ปัจจุบัน อาจารย์ประจำคณะนิติศาสตร์ มหาวิทยาลัยมหาสารคาม