

### บทที่ 3

## กฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย ระหว่างประเทศ ต่างประเทศ และประเทศไทย

การคุ้มครองข้อมูลส่วนบุคคลเป็นผลผลิตมาจากแนวคิดของการปกครองระบอบประชาธิปไตย แนวคิดเกี่ยวกับหลักนิติรัฐและหลักนิติธรรม แนวคิดเกี่ยวกับสิทธิเสรีภาพ แนวคิดเกี่ยวกับสิทธิส่วนบุคคลและการคุ้มครองข้อมูลส่วนบุคคล ตลอดจนทฤษฎีการจำกัดสิทธิและเสรีภาพของประชาชนดังได้กล่าวถึงแล้วในบทที่ 2 ในบทนี้ผู้เขียนจะนำเสนอกฎหมายที่เกิดจากแนวคิดดังกล่าวที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายระหว่างประเทศ โดยเริ่มจากการคุ้มครองข้อมูลส่วนบุคคลขององค์การสหประชาชาติที่ประกาศใช้กติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง และการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป กฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลของประเทศในระบบคอมมอนลอว์ (Common Law) และระบบซีวิลลอว์ (Civil Law) และกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยตามลำดับดังต่อไปนี้

#### 3.1 กฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายระหว่างประเทศ

การให้ความสำคัญคุ้มครองข้อมูลส่วนบุคคลถือว่าเป็นสิ่งที่มีความสำคัญเป็นอย่างมาก นอกจากการบัญญัติเป็นกฎหมายที่ใช้บังคับภายในประเทศแล้วยังมีกฎหมายระหว่างประเทศที่ได้บัญญัติรับรองในเรื่องที่เกี่ยวกับการให้ความสำคัญคุ้มครองข้อมูลส่วนบุคคลไว้ด้วย

ในส่วนกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายระหว่างประเทศนี้ผู้เขียนได้ทำการแบ่งการอธิบายออกเป็น 2 เรื่องด้วยกัน คือ 1. การคุ้มครองข้อมูลส่วนบุคคลขององค์การสหประชาชาติและ 2. การคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป โดยมีรายละเอียดดังต่อไปนี้

### 3.1.1 การคุ้มครองข้อมูลส่วนบุคคลขององค์การสหประชาชาติ

สหประชาชาติเป็นองค์การระหว่างประเทศระดับโลก ได้ประกาศใช้กติการะหว่างประเทศที่เรียกว่า กติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง<sup>1</sup> มีผลใช้บังคับเมื่อวันที่ 23 มีนาคม 2519 และประเทศไทยได้เข้าเป็นภาคีกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมืองโดยการภาคยานุวัติ เมื่อวันที่ 27 ตุลาคม 2539 และมีผลใช้บังคับกับประเทศไทย เมื่อวันที่ 30 มกราคม 2540 ซึ่งมีสาระสำคัญกล่าวถึงพันธกรณีของรัฐด้านสิทธิมนุษยชนตามกฎบัตรสหประชาชาติ รวมทั้งหน้าที่ของบุคคลที่จะส่งเสริมและคุ้มครองสิทธิมนุษยชนและได้รับสิทธิทั้งด้านพลเมือง การเมือง เศรษฐกิจ สังคม และวัฒนธรรมอย่างเท่าเทียมกันและบทบัญญัติ 53 ข้อ ซึ่งแบ่งเป็น 6 ส่วน คือ

ส่วนที่ 1 กล่าวถึงสิทธิในการกำหนดเจตจำนงของตนเอง กำหนดสถานะทางการเมือง รวมทั้งการดำเนินการพัฒนาเศรษฐกิจ สังคม และวัฒนธรรม ตลอดจนการจัดการโรคภัยไข้เจ็บและทรัพยากรธรรมชาติของตนเองได้อย่างเสรี<sup>2</sup>

ส่วนที่ 2 กล่าวถึงพันธกรณีของรัฐภาคีที่รับรองจะเคารพและประกันสิทธิของบุคคล รวมถึงการห้ามการเลือกปฏิบัติ ไม่ว่าจะด้วยเหตุผลทางเชื้อชาติ สีผิว เพศ ภาษา ศาสนา ความคิดเห็นทางการเมืองหรือความคิดเห็นอื่นใด สัญชาติ สถานะทางเศรษฐกิจ สังคม ถิ่นกำเนิด หรือสภาพอื่นใด โดยจะดำเนินการให้เกิดผลในทางปฏิบัติภายในประเทศ ประกันว่าบุคคลที่ถูกละเมิดจะได้รับการเยียวยาไม่ว่าบุรุษหรือสตรีจะได้รับสิทธิพลเมืองและการเมืองอย่างเท่าเทียมกัน การลิดรอนสิทธิในสถานการณ์ฉุกเฉินและการห้ามการตีความกติกาในอันที่จะไปจำกัดสิทธิและเสรีภาพอื่น ๆ<sup>3</sup>

ส่วนที่ 3 กล่าวถึงสาระของสิทธิในส่วนที่เป็นสิทธิพลเมืองและสิทธิทางการเมือง ได้แก่ สิทธิในการมีชีวิตอยู่ เสรีภาพจากการถูกทรมาน การห้ามบุคคลมิให้ตกอยู่ในภาวะเยี่ยงทาส การห้ามบุคคลมิให้ถูกจับกุมตามอำเภอใจ การปฏิบัติต่อผู้ถูกลิดรอนเสรีภาพอย่างมีมนุษยธรรม การห้ามบุคคลถูกจำคุกด้วยเหตุที่ไม่สามารถชำระหนี้ตามสัญญาได้ เสรีภาพในการโยกย้ายถิ่นฐาน ความเสมอภาคของบุคคลภายใต้กฎหมาย การห้ามมิให้มีการบังคับใช้กฎหมายอาญาย้อนหลัง

<sup>1</sup> จาก *หลักกฎหมายระหว่างประเทศทั่วไปเกี่ยวกับสนธิสัญญาด้านสิทธิมนุษยชน กติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง UN International Covenant on Civil and Political Rights (ICCPR)* (น. 15-20), โดย คณะกรรมการสิทธิมนุษยชน. กรุงเทพฯ: สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ

<sup>2</sup> กติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง, ข้อ 1.

<sup>3</sup> กติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง, ข้อ 2-5.

สิทธิการได้รับรองเป็นบุคคลตามกฎหมาย การห้ามแทรกแซงความเป็นส่วนตัว การคุ้มครองเสรีภาพทางความคิด เสรีภาพในการแสดงความคิดเห็นและการแสดงออก การห้ามการโฆษณาชวนเชื่อเพื่อการสงครามหรือก่อให้เกิดความเกลียดชังทางเชื้อชาติ สิทธิที่จะชุมนุมอย่างสันติ การรวมกันเป็นสมาคม สิทธิของชายหญิงที่อยู่ในวัยที่เหมาะสมในการมีครอบครัว การคุ้มครองสิทธิเด็ก และการที่พลเมืองทุกคนมีสิทธิที่จะมีส่วนร่วมในกิจการสาธารณะ การรับรองว่าบุคคลทั้งปวงย่อมเสมอภาคกันตามกฎหมายและได้รับการคุ้มครองอย่างเท่าเทียมกัน การรับรองสิทธิของชนกลุ่มน้อยทางเผ่าพันธุ์ ศาสนา และภาษาภายในรัฐ

ส่วนที่ 4 กล่าวถึงการจัดตั้งคณะกรรมการสิทธิมนุษยชน ซึ่งมีหน้าที่รับผิดชอบในการตรวจสอบการปฏิบัติตามพันธกรณีที่กำหนดไว้ในกติกา รวมถึงพันธกรณีในการเสนอรายงานของรัฐภาคี การยอมรับอำนาจของคณะกรรมการสิทธิมนุษยชน และขั้นตอนการพิจารณาข้อร้องเรียน

ส่วนที่ 5 ห้ามการตีความไปในทางขัดกับกฎหมายระหว่างประเทศอื่น ๆ รวมทั้งการมิให้ตีความในการที่จะลดทอนสิทธิที่จะใช้ประโยชน์จากทรัพยากรธรรมชาติ

ส่วนที่ 6 กล่าวถึงการเข้าเป็นภาคี และการแก้ไขเพิ่มเติมกติกา

จะเห็นได้ว่ากติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมืองได้ให้ความคุ้มครองความเป็นส่วนตัวไว้ในส่วนที่ 3 ข้อ 17 การห้ามแทรกแซงความเป็นส่วนตัว โดยกำหนดว่า “บุคคลจะถูกแทรกแซงความเป็นส่วนตัว ครอบครัว เคหสถานหรือการติดต่อสื่อสารโดยพลการหรือไม่ชอบด้วยกฎหมายมิได้ และจะถูกกลบหลู่เกียรติและชื่อเสียงโดยไม่ชอบด้วยกฎหมายมิได้”

หากพิจารณาจากกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมืองแล้ว จะเห็นได้ว่าสิทธิความเป็นส่วนตัวเป็นที่มีความสำคัญเป็นอย่างมาก ข้อมูลส่วนบุคคลก็เป็นสิทธิความเป็นส่วนตัวประเภทหนึ่ง ดังนั้นข้อมูลส่วนบุคคลย่อมได้รับความคุ้มครองในฐานะของสิทธิความเป็นส่วนตัวตามมาตรา 17 ของกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมืองด้วยเช่นกัน

### 3.1.2 การคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป

สหภาพยุโรปซึ่งเป็นองค์การระหว่างประเทศได้ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลมากมายหลายประเทศ เมื่อพิจารณาความเป็นมาแล้วจะเห็นได้จากพัฒนาการตั้งแต่องค์การเพื่อความร่วมมือทางด้านเศรษฐกิจและการพัฒนา (The Organization for Economic Cooperation and Development) ได้ออก Guidelines governing the protection of privacy and transporter data

flows of personal data ในปี ค.ศ. 1980 ซึ่งเป็นหลักการขั้นพื้นฐานในการให้ความคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในรูปอิเล็กทรอนิกส์ที่หลายประเทศยอมรับ

ต่อมา ค.ศ. 1995 สหภาพยุโรปได้ออกหลักเกณฑ์ที่สำคัญ “Directive 95/46/EC on the protection of Individuals with regard to the processing of personal data and on the free movement of such data” ทั้งนี้ เพื่อผลักดันให้กฎหมายในกลุ่มประเทศสมาชิกมีความสอดคล้องกันในการให้หลักประกันที่ดีเพียงพอต่อการคุ้มครองความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของพลเมืองของสหภาพยุโรปและเพื่อให้การส่งผ่านข้อมูลส่วนบุคคลภายในประเทศสมาชิกเป็นไปโดยเสรีปราศจากข้อจำกัดที่เกิดจากความแตกต่างกันของกฎหมายหรือกฎเกณฑ์ภายในของประเทศต่าง ๆ<sup>4</sup> โดยให้เป็นไปตามที่กำหนดไว้ใน Directive ภายในปี 1998

Directive 95/49/EC มีวัตถุประสงค์เพื่อกำหนดแนวทางในการบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลก็เพื่อให้ประเทศสมาชิกของสหภาพยุโรปมีแนวทางในการบัญญัติกฎหมายให้สอดคล้องกัน โดยคำนึงถึงการคุ้มครองสิทธิขั้นพื้นฐานและเสรีภาพของบุคคล (Fundamental rights and free of natural persons) โดยเฉพาะอย่างยิ่งความเป็นส่วนตัวของบุคคล (Right to privacy) โดยมีขอบเขตมุ่งใช้กับการประมวลผลข้อมูลส่วนบุคคลทั้งหมดหรือแต่บางส่วน โดยวิธีอัตโนมัติหรือโดยวิธีการอื่นใด โดยที่ข้อมูลส่วนบุคคลนั้นเป็นส่วนหนึ่งของระบบการจัดเก็บข้อมูล แต่ไม่ใช่บังคับกับการประมวลผลข้อมูลที่เกี่ยวข้องกับความสงบเรียบร้อย (Public security) ความมั่นคงของรัฐ (State security) การบังคับตามกฎหมายอาญา และการประมวลผลโดยบุคคลธรรมดา ในเรื่องส่วนตัวหรือเรื่องภายในครอบครัว

ข้อกำหนดของ Directive 95/49/EC ได้กำหนดนิยามศัพท์ที่สำคัญ ดังนี้

“ข้อมูลส่วนบุคคล (Personal data)” หมายถึง ข้อความที่เกี่ยวกับการระบุตัวบุคคลไม่ว่าโดยทางตรงหรือทางอ้อม เช่น เลขบัตรประจำตัวประชาชน หรือข้อมูลเกี่ยวกับลักษณะทางร่างกายจิตใจ ฐานะ เอกสิทธิ์ทางวัฒนธรรมและสังคม

“การประมวลผลข้อมูล (Processing)” หมายถึง การดำเนินการหรือชุดการดำเนินการซึ่งใช้กับข้อมูลส่วนบุคคลไม่ว่าจะทำขึ้นโดยวิธีการอัตโนมัติหรือไม่ เช่น การเก็บรวบรวม

<sup>4</sup> จาก *กฎหมายคุ้มครองข้อมูลส่วนบุคคล* (เอกสารประกอบการบรรยาย), โดย ไพโรจน์ วายุภาพ. (อ้างถึงใน *ปัญหาและมาตรการทางกฎหมายในการรับรองและคุ้มครองสิทธิในความเป็นส่วนตัว (Right to privacy)* (รายงานผลการวิจัย) (น. IV), โดย บรรเจิด สิงคะเนติ และคณะ, 2554, กรุงเทพฯ: สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ.

<sup>5</sup> สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ. (2546). *The EU Directive 95/46/EC*. สืบค้น 10 มิถุนายน 2558, จาก [www.ecommerce.or.th/ictlaw](http://www.ecommerce.or.th/ictlaw)

การบันทึก การจัดเรียง การเก็บรักษา การแก้ไขเพิ่มเติม การนำกลับมา การหาหรือ การใช้ การเปิดเผย โดยการส่ง การเผยแพร่ หรือวิธีการอื่น ๆ ที่ทำให้เข้าถึงข้อมูลได้ การจัดเก็บ หรือการรวมข้อมูล การจัดวาง การลบ หรือการทำลายข้อมูล

“ผู้ควบคุมข้อมูล (Controller)” หมายถึง บุคคลธรรมดา นิติบุคคล หน่วยงานของรัฐ องค์กรหรือหน่วยงานอื่นใด ไม่ว่าจะ เป็นหน่วยงานเดียวหรือร่วมกับหน่วยงานอื่น ซึ่งมีหน้าที่ กำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคล

“ผู้ประมวลผลข้อมูล (Processor)” หมายถึง บุคคลธรรมดา นิติบุคคล หน่วยงานของรัฐ องค์กรหรือหน่วยงานอื่นใด ซึ่งประมวลผลข้อมูลส่วนบุคคลในนามของผู้ควบคุมข้อมูล

“ความยินยอมของเจ้าของข้อมูล (The data subject’s consent)” หมายถึง การแสดงเจตนาโดยเฉพาะของเจ้าของข้อมูลในการตกลงให้ข้อมูลส่วนบุคคลของตนประมวลผลได้

EU Directive ของกลุ่มสหภาพยุโรปมีการกำหนดขอบเขตของกฎหมายและการบังคับใช้ไว้ในมาตรา 3 โดยใช้บังคับกับการประมวลผลทั้งวิธีการอิเล็กทรอนิกส์อัตโนมัติ และวิธีอื่นใด ที่มีใช้วิธีการอิเล็กทรอนิกส์อัตโนมัติหากเป็นไปเพื่อการทำระบบ Filing ทั้งนี้ EU Directive จะไม่ใช้บังคับกับการประมวลผลข้อมูลส่วนบุคคลที่ไม่อยู่ภายใต้กิจกรรมของ Community การประมวลผลข้อมูลส่วนบุคคลของรัฐสมาชิกที่เป็นไปเพื่อการรักษาความมั่นคงและการดำเนินการตามกฎหมายอาญาและการประมวลผลโดยบุคคลธรรมดาที่เป็นไปเพื่อกิจกรรมส่วนตัว

จากคำอธิบายกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่นำเสนอมาข้างต้น จะพบว่าจุดประสงค์ของบทบัญญัตินี้ในท้ายที่สุดแล้วก็เพื่อให้ความคุ้มครองความเป็นส่วนตัวของบุคคลในระดับของข้อมูลส่วนบุคคล ซึ่งอยู่บนพื้นฐานของหลักความยินยอม (Consent) เป็นสำคัญ แต่ถึงแม้บทบัญญัติดังกล่าวจะมีความแตกต่างกันเพียงใดจากการศึกษาสามารถสรุปสาระสำคัญของบทบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลได้ ดังนี้<sup>6</sup>

#### 1) หลักความรับผิดชอบ

กล่าวคือ ผู้จัดเก็บข้อมูล ผู้ครอบครองข้อมูลหรือผู้ประมวลผลข้อมูลจะต้องมีความรับผิดชอบในการปฏิบัติตามหลักการหรือมาตรการต่าง ๆ ให้ครบถ้วนทุกประการอย่างเคร่งครัด หากมีการฝ่าฝืนหรือละเลยแล้วมีผลให้เกิดความเสียหายแก่ข้อมูลส่วนบุคคล ผู้จัดเก็บข้อมูล ผู้ครอบครองข้อมูล หรือผู้ประมวลผลข้อมูลจะต้องรับผิดชอบทั้งทางแพ่งและทางอาญา นอกจากนี้

<sup>6</sup> จาก มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลจากการใช้บริการเครือข่ายสังคมออนไลน์ (วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ) (น. 50-57), โดย นรินทร์ จุ่มศรี, 2555, กรุงเทพฯ: มหาวิทยาลัยธุรกิจบัณฑิต.

ยังจะต้องรับผิดชอบค่าใช้จ่ายที่เกิดขึ้นเพื่อทำการแก้ไขข้อมูลให้ถูกต้อง ลบ หรือทำลายข้อมูลส่วนบุคคล รวมทั้งเยียวยาความเสียหาย แล้วแต่กรณี

## 2) หลักการแจ้งวัตถุประสงค์

การกำหนดจุดมุ่งหมายในการเก็บข้อมูลต้องชัดเจนในช่วงเวลาที่มีการเก็บรวบรวมข้อมูล และการใช้จะต้องตรงตามจุดมุ่งหมายและถ้ามีการเปลี่ยนแปลงจุดมุ่งหมายต้องมีการแจ้งทุกครั้งที่เปลี่ยนแปลง

ข้อมูลส่วนบุคคลไม่ควรเปิดเผยหรือนำไปใช้ทั่วไปโดยไม่ตรงกับจุดมุ่งหมายที่ระบุไว้ นอกเหนือจากการที่ได้รับอนุญาตจากเจ้าของข้อมูลหรือการได้รับสิทธิตามกฎหมาย

## 3) หลักความยินยอม

EU Directive ของกลุ่มสหภาพยุโรปมีการบัญญัติไว้ในมาตรา 9 ว่ารัฐสมาชิกต้องกำหนดข้อยกเว้นสำหรับกรณีตาม Chapter IV โดยไม่ใช้บังคับกับข้อมูลส่วนบุคคลที่ทำเพื่อวัตถุประสงค์ในการเขียนข่าวเพียงเท่าที่จำเป็นในการรักษาสมดุลระหว่างสิทธิความเป็นส่วนตัวและหลักเกณฑ์เกี่ยวกับเสรีภาพในการแสดงออก

ในการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูล ผู้ควบคุมข้อมูลต้องขอความยินยอมจากเจ้าของข้อมูลก่อนเก็บรวบรวมข้อมูล และต้องแจ้งแก่เจ้าของข้อมูลว่าข้อมูลได้ถูกเก็บรวบรวม รวมถึงรายละเอียดอื่น ๆ เช่น ลักษณะของผู้ควบคุมข้อมูลและตัวแทนของผู้ควบคุมข้อมูล (The identity of the controller and of his representative) วัตถุประสงค์ของการประมวลผลข้อมูล เป็นต้น และในกรณีที่ไม่ได้ข้อมูลมาจากเจ้าของข้อมูลผู้ควบคุมข้อมูลต้องแจ้งแก่เจ้าของข้อมูลในเวลาที่ได้ดำเนินการใด ๆ กับข้อมูลนั้นหรือได้มีการเปิดเผยข้อมูลนั้นต่อบุคคลที่สาม

Directive 95/49/EC กำหนดให้ผู้ประมวลผลจะประมวลผลได้ในกรณีดังต่อไปนี้<sup>7</sup>

1. เจ้าของข้อมูลให้ความยินยอมโดยชัดแจ้ง
2. การประมวลผลเป็นการปฏิบัติตามสัญญาที่เจ้าของข้อมูลเป็นคู่สัญญาหรือเจ้าของข้อมูลร้องขอให้ประมวลผลก่อนมีการเข้าทำสัญญา
3. การประมวลผลเป็นหน้าที่ตามกฎหมายของผู้ควบคุมข้อมูล
4. การประมวลผลเพื่อคุ้มครองชีวิตของเจ้าของข้อมูล

<sup>7</sup> จาก ปัญหาทางกฎหมายเกี่ยวกับ การคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์  
กรณีศึกษา: การจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของธนาคาร สถาบันการเงิน และผู้ประกอบการธุรกิจบัตรเครดิตในประเทศไทย (วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ) (น. 40), โดย ธนัท สุวรรณปริญญา, 2550, กรุงเทพฯ: มหาวิทยาลัยกรุงเทพ.

5. การประมวลผลเป็นการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะหรือการปฏิบัติตามหน้าที่ของเจ้าหน้าที่ผู้มีอำนาจของผู้ควบคุมข้อมูลหรือของบุคคลที่สามที่ได้รับข้อมูลนั้น

6. การประมวลผลเป็นไปตามวัตถุประสงค์ที่ชอบด้วยกฎหมายซึ่งปฏิบัติการ โดยผู้ควบคุมข้อมูล หรือบุคคลที่สามหรือคู่สัญญาที่ได้รับข้อมูลนั้น เว้นแต่การประมวลผลเป็นการขัดกับสิทธิขั้นพื้นฐานและเสรีภาพของเจ้าของข้อมูล

4) หลักการเก็บรวบรวมข้อมูลอย่างจำกัด

ในกรณีที่เป็นข้อมูลส่วนบุคคลชนิดพิเศษหรือข้อมูลที่มีความอ่อนไหว (Special categories of data) ได้แก่ ข้อมูลที่เกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ศาสนา ความเชื่อในลัทธิ สมาชิกของสมาคมการค้าหรือสหภาพแรงงาน สุขภาพหรือพฤติกรรมทางเพศนั้น ห้ามมิให้มีการประมวลผล เว้นแต่ในกรณีดังต่อไปนี้

1. เจ้าของข้อมูลให้ความยินยอมโดยชัดแจ้ง

2. การประมวลผลโดยมีวัตถุประสงค์เป็นการปฏิบัติตามสิทธิหน้าที่ของผู้ควบคุมข้อมูลตามกฎหมายแรงงาน

3. การประมวลผลเพื่อคุ้มครองชีวิตของเจ้าของข้อมูลหรือบุคคลอื่น ในกรณีที่เจ้าของข้อมูลไม่สามารถให้ความยินยอมได้

4. การประมวลผลโดยชอบด้วยกฎหมายและรับรองโดยมูลนิธิ องค์กร หรือหน่วยงานที่ไม่มุ่งหวังผลกำไร โดยมีจุดประสงค์ในทางการเมือง ลัทธิ ศาสนาหรือสมาคมการค้าหรือสหภาพแรงงานและการประมวลผลดังกล่าวต้องเกี่ยวข้องกับสมาชิกของหน่วยงานหรือบุคคลที่มีการติดต่อกับหน่วยงานนั้นเป็นการปฏิบัติตามวัตถุประสงค์ของหน่วยงานและข้อมูลนั้นต้องไม่ถูกเปิดเผยต่อบุคคลที่สามโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล

5. การประมวลผลข้อมูลที่เจ้าของข้อมูลทำให้เป็นสาธารณะโดยชัดแจ้ง หรือการประมวลผลเพื่อฟ้องร้อง ดำเนินการ หรือแก้ต่างคดี

6. การประมวลผลโดยมีวัตถุประสงค์เพื่อป้องกันการให้ยา การวินิจฉัยโรค การรักษาพยาบาล หรือการดำเนินงานของสถานพยาบาล หรือของแพทย์ ภายใต้กฎหมายเกี่ยวกับความลับทางวิชาชีพ

7. การประมวลผลข้อมูลที่เกี่ยวข้องกับการกระทำความผิดทางอาญา คำตัดสินการกระทำความผิดทางอาญา หรือวิธีการเพื่อความปลอดภัย กระทำได้ภายใต้การควบคุมของเจ้าพนักงานผู้มีอำนาจและการประมวลผลข้อมูลที่เกี่ยวข้องกับการลงโทษทางปกครอง หรือคำตัดสินในคดีแพ่ง กระทำได้ภายใต้การควบคุมของเจ้าพนักงานผู้มีอำนาจ

8. การประมวลผลข้อมูลโดยมีวัตถุประสงค์ในการเขียนข่าวศิลปะหรือการประพันธ์เฉพาะในกรณีที่ไม่ขัดแย้งกับสิทธิความเป็นส่วนตัวของเจ้าของข้อมูล

5) หลักการจำกัดการใช้ การเปิดเผย และการเก็บรักษา

การประมวลผลข้อมูลส่วนบุคคลตาม Directive 95/46/EC ได้รับการยกเว้นในกรณีที่ดำเนินการเพื่อวัตถุประสงค์ดังต่อไปนี้ ความมั่นคงของชาติ การป้องกันประเทศ ความปลอดภัยของสาธารณะ การป้องกัน การสืบสวนและสอบสวน การดำเนินคดีอาญา จรรยาบรรณของวิชาชีพ ประโยชน์ทางด้านเศรษฐกิจของประเทศ รวมถึงการเงิน งบประมาณและภาษี องค์กรที่มีหน้าที่ดูแลตรวจสอบตามที่กฎหมายกำหนด การคุ้มครองเจ้าของข้อมูล หรือสิทธิเสรีภาพของบุคคลอื่น

6) หลักความถูกต้อง

ข้อมูลส่วนบุคคลจะต้องมีการจัดเก็บไปตามจุดมุ่งหมายของการนำไปใช้ของข้อมูลเหล่านี้ จะต้องเก็บเท่าที่มีความจำเป็นจะต้องใช้งาน เป็นข้อมูลที่ถูกต้องสมบูรณ์และทันสมัย นอกจากนี้ การประมวลผลข้อมูลส่วนบุคคลจะต้องเป็นการประมวลผลข้อมูลที่มีคุณภาพ โดยจะต้องปฏิบัติตามดังต่อไปนี้

1. ข้อมูลส่วนบุคคลต้องถูกประมวลผลอย่างเป็นธรรมและชอบด้วยกฎหมาย
2. ข้อมูลส่วนบุคคลต้องถูกจัดเก็บโดยมีวัตถุประสงค์ที่ชัดเจน แน่นนอนและชอบด้วยกฎหมาย นอกจากนี้จะต้องไม่มีการประมวลผลข้อมูลที่ขัดแย้งกับวัตถุประสงค์นั้น เว้นแต่การประมวลผลข้อมูลที่มีวัตถุประสงค์ทางด้านประวัติศาสตร์ สถิติหรือวิทยาศาสตร์
3. ข้อมูลส่วนบุคคลต้องมีความเพียงพอ ไม่มากเกินไปและสอดคล้องกับวัตถุประสงค์ในการจัดเก็บหรือประมวลผลข้อมูลนั้น
4. ข้อมูลส่วนบุคคลต้องมีความถูกต้อง และเก็บเป็นปัจจุบัน (Kept up to Date) ข้อมูลส่วนบุคคลที่ไม่ถูกต้องหรือไม่ครบถ้วนตามวัตถุประสงค์ของการจัดเก็บ หรือการประมวลผลต้องลบทิ้งหรือแก้ไขให้ถูกต้อง
5. ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับลักษณะเฉพาะของเจ้าของข้อมูล (Identification of Data Subject) ต้องไม่ถูกเก็บไว้ยาวนานเกินความจำเป็นตามวัตถุประสงค์ของการเก็บหรือการประมวลผล และประเทศสมาชิกต้องกำหนดมาตรการที่เหมาะสมสำหรับข้อมูลที่ใช้ทางด้านประวัติศาสตร์ สถิติ หรือวิทยาศาสตร์ที่ต้องเก็บไว้เป็นเวลานาน

7) หลักการรักษาความปลอดภัย

ในปี ค.ศ. 1995 สหภาพยุโรปได้ออกหลักเกณฑ์ที่มีชื่อว่า “Directive 95/46/EC on the Protection of Individuals with regard to the processing of Personal data and on the free movement of such data” เพื่อผลักดันให้กฎหมายในหมู่ประเทศสมาชิกมีความสอดคล้องกันในการให้

หลักประกันที่ดีพอต่อการคุ้มครองข้อมูลส่วนบุคคลของพลเมืองของ EU โดยปราศจากข้อจำกัดที่เกิดจากความแตกต่างกันของกฎหมาย กฎเกณฑ์ทางสังคมและวัฒนธรรม โดยให้เป็นไปตามที่กำหนดไว้ใน Directive ดังกล่าว และในปี ค.ศ. 2002 สหภาพยุโรปก็ได้ออกหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลเพิ่มเติมอีก คือ “Directive 2002/58/EC concerning the processing of Personal Data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)” โดยกำหนดรายละเอียดให้ผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารทางอิเล็กทรอนิกส์ต้องมีมาตรการในการคุ้มครองข้อมูลส่วนบุคคล เช่น จัดให้มีมาตรการรักษาความปลอดภัยและความลับของข้อมูลที่ส่งหรือการลบข้อมูลเมื่อหมดความจำเป็น

ทั้งนี้ Directive 95/49/EC กำหนดห้ามบุคคลใดทำการประมวลผลข้อมูลส่วนบุคคลเว้นแต่ภายใต้คำสั่งของผู้ควบคุมข้อมูล (Instructions from the controller) หรือกฎหมายอนุญาตให้ประมวลผลได้เท่านั้น และผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลมีหน้าที่จะต้องปฏิบัติดังต่อไปนี้

1. ผู้ควบคุมข้อมูลต้องใช้เทคนิคหรือวิธีการที่เหมาะสมในการคุ้มครองข้อมูลส่วนบุคคลจากการทำลาย สูญหาย เปลี่ยนแปลง การเปิดเผยหรือการเข้าถึงโดยปราศจากอำนาจ โดยเฉพาะอย่างยิ่งการส่งผ่านข้อมูลนอกเครือข่าย รวมทั้งการประมวลผลข้อมูลที่ผิดกฎหมาย วิธีการคุ้มครองที่เหมาะสมนั้นพิจารณาจากความเสี่ยงที่เกิดจากการประมวลผลและชนิดของข้อมูลที่ต้องการคุ้มครอง

2. ผู้ควบคุมข้อมูลต้องเลือกผู้ประมวลผลข้อมูลที่มีเทคนิคหรือวิธีการรักษาความปลอดภัยที่เพียงพอและเหมาะสม

3. การประมวลผลของผู้ประมวลผลข้อมูลต้องกระทำโดยมีสัญญาผูกพัน ผู้ประมวลผลข้อมูลกับผู้ควบคุมข้อมูลและในสัญญาต้องกำหนดว่าผู้ประมวลผลต้องกระทำภายในคำสั่งของผู้ควบคุมดูแลและผู้ประมวลผลข้อมูลมีหน้าที่ตามข้อ 1

4. สัญญาที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและวิธีการที่ต้องปฏิบัติตาม ข้อ 1 ต้องทำเป็นลายลักษณ์อักษร เพื่อประโยชน์ในการพิสูจน์พยานหลักฐาน

#### 8) หลักการเปิดเผย

จะต้องมีการประกาศนโยบายในการประมวลผลข้อมูลส่วนบุคคล เพื่อให้บุคคลที่เกี่ยวข้องทราบถึงกระบวนการจัดเก็บ รวบรวมนำไปใช้ ฯลฯ นอกจากนี้ จะต้องมีการแสดงให้เห็นถึงความมีอยู่และประเภทของข้อมูลส่วนบุคคล วัตถุประสงค์ของการใช้ข้อมูลส่วนบุคคล ตลอดจนข้อ สถานที่จัดตั้ง และรายละเอียดของผู้ที่ทำหน้าที่เก็บรักษาข้อมูล ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลให้เจ้าของข้อมูลทราบ

### 9) หลักการเข้าตรวจดูข้อมูลของบุคคล

Directive 95/46/EC ได้กำหนดสิทธิของเจ้าของข้อมูลในการเข้าถึงข้อมูลของเจ้าของข้อมูล เจ้าของข้อมูลมีสิทธิได้รับการยืนยันจากผู้ควบคุมข้อมูลว่าข้อมูลที่เกี่ยวข้องกับเจ้าของข้อมูล ได้ถูกประมวลผลหรือไม่ และรายละเอียดเกี่ยวกับวัตถุประสงค์ในการประมวลผล ประเภทของข้อมูล และผู้รับข้อมูล เจ้าของข้อมูลมีสิทธิเรียกร้องให้ผู้ควบคุมข้อมูล ส่งข้อมูลที่ได้มีการประมวลผลแก่เจ้าของข้อมูลและให้ผู้ควบคุมข้อมูลแจ้งเหตุผลของการประมวลผลข้อมูลอัตโนมัติแก่เจ้าของข้อมูล ทั้งนี้โดยปราศจากข้อจำกัดเรื่องเวลา (Constraint at reasonable intervals) การประวิงเวลาและค่าใช้จ่ายที่มากเกินไป นอกจากนี้เจ้าของข้อมูลยังมีสิทธิที่จะแก้ไขข้อมูลให้ถูกต้อง ลบข้อมูลหรือขัดขวางการประมวลผลที่ไม่ได้ปฏิบัติตามแนวทางนี้ และผู้ควบคุมข้อมูลต้องแจ้งแก่บุคคลที่สามที่ได้รับข้อมูลถึงการแก้ไขข้อมูล การลบ หรือการขัดขวางการประมวลผลข้อมูลดังกล่าวด้วย

### 10) หลักการโต้แย้งการปฏิบัติขององค์กร

Directive 95/46/EC ได้กำหนดสิทธิของเจ้าของข้อมูลในการคัดค้านการประมวลผลข้อมูลของตน ในกรณีที่ถูกกฎหมายบัญญัติให้สิทธิแก่เจ้าของข้อมูลในการคัดค้าน รวมถึงในกรณีที่ผู้ควบคุมข้อมูล ประมวลผลข้อมูลโดยมีวัตถุประสงค์เพื่อการตลาด (Purposes of direct marketing) หรือกรณีที่มีการเปิดเผยข้อมูลโดยมีวัตถุประสงค์เพื่อการตลาด เจ้าของข้อมูลมีสิทธิได้รับแจ้งก่อนมีการเปิดเผยข้อมูลต่อบุคคลที่สามและมีสิทธิคัดค้านการเปิดเผยข้อมูลนั้น

นอกจากนี้ Directive 95/46/EC ยังกำหนดให้สิทธิบุคคลที่จะไม่ต้องอยู่ภายใต้การตัดสินใจใด ๆ ที่ได้มาจากการประมวลผลข้อมูลอัตโนมัติ โดยมีจุดมุ่งหมายที่จะประเมินลักษณะส่วนบุคคล เช่น การทำงาน ความน่าเชื่อถือ ความน่าไว้วางใจ การกระทำอื่น ๆ เป็นต้น เว้นแต่การตัดสินใจที่เป็นไปเพื่อเข้าทำ หรือปฏิบัติตามสัญญา หรือเจ้าของข้อมูลร้องขอเพื่อเข้าทำหรือปฏิบัติตามสัญญา

ในกรณีที่มีการล่วงละเมิดเกี่ยวกับสิทธิข้อมูลส่วนบุคคล Directive 95/46/EC ได้วางแนวทางให้สภานิติบัญญัติของแต่ละประเทศควรกำหนดให้มีการเยียวยาโดยใช้สิทธิทางศาล โดยอาจกำหนดไว้ในกฎหมายเฉพาะหรือกฎหมายทั่วไปก็ได้

### 11) หลักการไม่เลือกปฏิบัติ

การจัดเก็บหรือรวบรวมข้อมูลส่วนบุคคลจะต้องไม่ทำให้เกิดการเลือกปฏิบัติต่อบุคคลที่แตกต่างกัน เช่น ข้อมูลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ สีผิว พฤติกรรมทางเพศ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนา ปรัชญา ความเชื่อเกี่ยวกับลัทธิทางการเมือง หรือความเชื่ออื่นใด รวมถึงความเป็นสมาชิกสหภาพการค้า เป็นต้น ข้อมูลที่กล่าวมาเป็นข้อมูลส่วนบุคคลประเภทที่เรียกว่า

“Sensitive Data” (ข้อมูลส่วนบุคคลที่มีผลกระทบต่อความรู้สึก/ข้อมูลส่วนบุคคลที่ต้องให้ความสำคัญเป็นพิเศษ/ข้อมูลละเอียดอ่อน) ดังนั้น จึงอาจกล่าวได้ว่าเป็นหลักการที่ห้ามมิให้จัดเก็บข้อมูลส่วนบุคคลประเภท Sensitive Data

#### 12) หลักข้อจำกัดในการส่งหรือโอนข้อมูลส่วนบุคคล

หลักการนี้กำหนดห้ามมิให้มีการส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศซึ่งมิได้มีบทบัญญัติในการให้ความคุ้มครองข้อมูลส่วนบุคคลในระดับที่เท่าเทียมกันในสาระสำคัญ เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูลหรือจำเป็นเพื่อชำระหนี้ตามความผูกพันที่เป็นผลของสัญญา หรือทำเพื่อประโยชน์ของบุคคลซึ่งไม่สามารถให้ความยินยอมได้

#### 3.1.3 กรอบในการคุ้มครองข้อมูลส่วนบุคคลขององค์การร่วมมือและพัฒนาทางเศรษฐกิจ (OECD: The Organization for Economic Cooperation and Development)

The Organization for Economic Cooperation and Development เป็นเวทีแลกเปลี่ยนข้อคิดเห็นระหว่างประเทศสมาชิกเกี่ยวกับการจัดการปัญหาต่าง ๆ ในยุคโลกาภิวัตน์บนพื้นฐานของการศึกษาวิจัยอย่างรอบคอบและเป็นกลาง เพื่อนำไปสู่ข้อสรุปร่วมระดับนโยบายในลักษณะที่เป็น Guidelines for Best Practices และการปรับเปลี่ยนนโยบายภายในประเทศสมาชิกให้สอดคล้องกับ Guidelines เหล่านั้นในที่สุด<sup>8</sup>

หลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลขึ้นอย่างเป็นรูปธรรมและเป็นหลักเกณฑ์ที่ประเทศส่วนใหญ่ให้การยอมรับคือ Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder flows of Personal Data โดย OECD (Organization for Economic Cooperation and Development) ภายใต้อาณัติของ Guidelines ฉบับนี้ได้กลายเป็นที่ยอมรับกันโดยทั่วไปว่าเป็นหลักเกณฑ์พื้นฐานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่สำคัญประเทศส่วนใหญ่ในโลกต่างรับและนำไปปฏิบัติเป็นกฎหมายภายในของตน

หลักการภายใต้ Guidelines on the protection of Privacy and Transborder Data Flows of Personal Data ขององค์การเพื่อเศรษฐกิจและการพัฒนา (OECD) ซึ่งมีหลักการที่สำคัญจำนวน 8 ประการ ดังนี้<sup>9</sup>

<sup>8</sup> จาก แนวทางการคุ้มครองข้อมูลใน Big Data: ศึกษาประเด็นความเป็นส่วนตัวและความมั่นคงปลอดภัยของข้อมูล (น. 75-76), โดย ปิยะภัสร์ โรจน์รัตนวาณิชย์, 2556, กรุงเทพฯ.

<sup>9</sup> ปัญหาและมาตรการทางกฎหมายในการรับรองและคุ้มครองสิทธิในความเป็นส่วนตัว (Right to privacy) (รายงานผลการวิจัย) (น. 30). น. III-IV.

1. หลักข้อจำกัดในการเก็บรวบรวมข้อมูล ในการเก็บรวบรวมข้อมูลนั้น ต้องชอบด้วยกฎหมายและต้องใช้วิธีการที่เป็นธรรมและเหมาะสม โดยในการเก็บรวบรวมข้อมูลนั้นต้องให้เจ้าของข้อมูลรู้เห็น รับรู้ หรือได้รับความยินยอมจากเจ้าของข้อมูล

2. หลักคุณภาพของข้อมูล ข้อมูลที่เก็บรวบรวมนั้น ต้องเกี่ยวข้องกับวัตถุประสงค์ที่กำหนดขึ้นว่า “จะนำไปใช้ทำอะไร” และเป็นไปตามอำนาจหน้าที่และวัตถุประสงค์ในการดำเนินงานของหน่วยงานตามที่กฎหมายกำหนดนอกจากนั้นข้อมูลดังกล่าวจะต้องถูกต้อง สมบูรณ์ หรือทำให้เป็นปัจจุบันหรือทันสมัยอยู่เสมอ

3. หลักการกำหนดวัตถุประสงค์ในการจัดเก็บต้องกำหนดวัตถุประสงค์ว่าข้อมูลที่มีการเก็บรวบรวมนั้น เก็บรวบรวมไปเพื่ออะไร พร้อมทั้งกำหนดระยะเวลาที่เก็บรวบรวมหรือรักษาข้อมูลนั้น ตลอดจนกรณีที่จะต้องมีการเปลี่ยนแปลงวัตถุประสงค์ในการเก็บรวบรวมข้อมูล เช่นว่านั้น ไว้ให้ชัดเจน

4. หลักข้อจำกัดในการนำไปใช้ข้อมูลส่วนบุคคลนั้น จะต้องไม่มีการเปิดเผยทำให้มีหรือปรากฏในลักษณะอื่นใด ซึ่งไม่ได้กำหนดไว้โดยชัดแจ้งในวัตถุประสงค์ของการเก็บรวบรวมข้อมูล เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูล หรือโดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย

5. หลักการรักษาความมั่นคงปลอดภัยข้อมูลจะต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม เพื่อป้องกันความเสี่ยงภัยใด ๆ ที่อาจจะทำให้ข้อมูลนั้นสูญหาย เข้าถึง ทำลาย ใช้ ดัดแปลงแก้ไข หรือเปิดเผยโดยมิชอบ

6. หลักการเปิดเผยข้อมูล ควรมีการประกาศนโยบายให้ทราบโดยทั่วกัน หากมีการปรับปรุงแก้ไขหรือพัฒนาแนวนโยบายหรือแนวปฏิบัติที่เกี่ยวกับข้อมูลส่วนบุคคล ก็ควรเปิดเผยหรือประกาศไว้ให้ชัดเจน รวมทั้งให้ข้อมูลใด ๆ ที่สามารถระบุเกี่ยวกับหน่วยงานของรัฐผู้ให้บริการที่อยู่ผู้ควบคุมข้อมูลส่วนบุคคลด้วย

7. หลักการมีส่วนร่วมของบุคคล ให้บุคคลซึ่งเป็นเจ้าของข้อมูลได้รับแจ้งหรือยืนยันจากหน่วยงานของรัฐที่เก็บรวบรวมหรือจัดเก็บข้อมูลทราบว่า “หน่วยงานของรัฐนั้น ๆ ได้รวบรวมข้อมูลหรือจัดเก็บข้อมูลส่วนบุคคลดังกล่าวหรือไม่ภายในระยะเวลาที่เหมาะสม”

8. หลักความรับผิดชอบ ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

หลังจากที่มีการตกลงในเวที The Organization for Economic Cooperation and Development แต่ละประเทศก็เริ่มที่จะมีการนำเอาหลักการภายใต้ Guidelines on the protection of Privacy and Transborder Data Flows of Personal Data ขององค์การเพื่อเศรษฐกิจและการพัฒนา (OECD)

ไปบัญญัติเป็นกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลหรือสิทธิส่วนบุคคลภายในประเทศนั่นเอง

เมื่อได้ทราบรายละเอียดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในส่วนที่เป็นกฎหมายระหว่างประเทศแล้ว ในส่วนต่อไปผู้เขียนจะทำการอธิบายให้ทราบถึงการคุ้มครองข้อมูลส่วนบุคคลในส่วนที่เป็นกฎหมายในต่างประเทศต่อไป

### 3.2 กฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศ

การคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศอาจจำเป็นต้องย้อนไปตั้งแต่หลังสงครามโลกครั้งที่ 2 ประเทศต่าง ๆ ได้ร่วมกันก่อตั้งองค์การสหประชาชาติ และได้มีการจัดทำกฎบัตรสหประชาชาติ ซึ่งเป็นเอกสารสำคัญที่ยอมรับถึงสิทธิมนุษยชนขึ้น กฎบัตรนี้เป็นจุดเริ่มต้นที่สำคัญของการยอมรับสิทธิมนุษยชนในระดับโลก อย่างไรก็ตามแม้จะมีบทบัญญัติที่แสดงถึงภารกิจที่สำคัญของสหประชาชาติในการส่งเสริมสิทธิมนุษยชน แต่ก็มีได้บัญญัติถึงสิทธิมนุษยชนไว้ในรายละเอียดและไม่ได้จำแนกประเภทต่าง ๆ ของสิทธิมนุษยชนไว้

ต่อมาได้มีการตั้งคณะกรรมการสิทธิมนุษยชนและจัดทำร่างปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ. 1948 ซึ่งที่ประชุมสมัชชาแห่งสหประชาชาติได้ลงมติยอมรับเป็นเอกฉันท์เมื่อวันที่ 10 ธันวาคม ค.ศ. 1948 (Universal Declaration of Human Rights หรือ UDHR) ปฏิญญาสากลว่าด้วยสิทธิมนุษยชนซึ่งรับรองโดยสมัชชาใหญ่สหประชาชาติ (Universal Declaration of Human Rights) เกิดขึ้นมาด้วยวัตถุประสงค์ที่จะให้มีองค์กรหนึ่งทำหน้าที่ในการปกป้องสิทธิมนุษยชนในระดับระหว่างประเทศ อย่างไรก็ตามปฏิญญาสากลดังกล่าวมิได้ก่อพันธะทางกฎหมายผูกพันรัฐสมาชิก การคุ้มครองสิทธิความเป็นอยู่ส่วนตัวก็ยังคงขึ้นอยู่กับการออกกฎหมายภายในของรัฐต่าง ๆ ในการคุ้มครองสิทธิดังกล่าว แต่ปฏิญญาสากลนี้นับได้ว่าเป็นแนวทางสำหรับการที่รัฐต่าง ๆ นำไปพิจารณาเพื่อออกกฎหมายของตนต่อไป

ทั้งนี้ เมื่อพิจารณาโดยเนื้อหาของปฏิญญาแล้วถือเป็นเอกสารลายลักษณ์อักษรฉบับแรกที่บัญญัติคุ้มครองสิทธิของบุคคลในอันที่จะไม่ถูกรบกวนโดยบัญญัติไว้ในข้อ 12 ว่า

“บุคคลใดจะถูกแทรกแซงตามอำเภอใจในความเป็นส่วนตัว ครอบครัว ที่อยู่อาศัยหรือการสื่อสาร หรือจะถูกหลอกลวงเกียรติยศและชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองของกฎหมายต่อการแทรกแซงสิทธิหรือการหลอกลวงดังกล่าวนี้”

ต่อจากนั้นสนธิสัญญาแห่งสหภาพยุโรปว่าด้วยสิทธิมนุษยชน (The European Convention on Human Rights หรือ ECHR) ซึ่งมีวัตถุประสงค์มุ่งคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานในยุโรป สนธิสัญญานี้จัดตั้งศาลสิทธิมนุษยชนยุโรป โดยให้สิทธิบุคคลใด ๆ ที่ถูกละเมิดสิทธิ

มนุษยชนโดยรัฐสมาชิกสามารถนำคดีขึ้นสู่ศาลนี้ได้ แม้ว่าคำตัดสินจะไม่มีผลผูกพันทางกฎหมายโดยอัตโนมัติ แต่ศาลมีอำนาจกำหนดค่าเสียหายได้ แนวคิดทางกฎหมายของการจัดตั้งศาลนี้นับเป็นพัฒนาการอีกขั้นหนึ่งเนื่องจากให้สิทธิปัจเจกชนนำคดีขึ้นสู่ศาลได้ อันเป็นแนวคิดที่แตกต่างจากเดิมซึ่งรัฐเท่านั้นจักเป็นบุคคลตามกฎหมายระหว่างประเทศ<sup>10</sup>

เมื่อพิจารณาสนธิสัญญาแห่งสหภาพยุโรปว่าด้วยสิทธิมนุษยชนจะพบว่า มาตรา 8 ซึ่งบัญญัติว่า

1. บุคคลทุกคนมีสิทธิที่จะได้รับการเคารพในชีวิตส่วนตัว ชีวิตครอบครัว ที่อยู่อาศัย และการติดต่อสื่อสาร

2. รัฐไม่ควรเข้าไปแทรกแซงสิทธิดังกล่าว เว้นแต่เป็นเรื่องที่เกี่ยวกับกฎหมายและความจำเป็นในสังคมประชาธิปไตย เพื่อผลประโยชน์ทางความมั่นคงของชาติ ความปลอดภัยของสาธารณะหรือความผาสุกทางเศรษฐกิจของประเทศ เพื่อป้องกันการจลาจล หรืออาชญากรรม เพื่อป้องกันสุขภาพ หรือศีลธรรม หรือเพื่อป้องกันซึ่งเสรีภาพของผู้อื่น

จะเห็นได้ว่าในต่างประเทศให้ความสำคัญกับการคุ้มครองสิทธิในความเป็นส่วนตัวอย่างยิ่ง และมีการบัญญัติไว้เป็นลายลักษณ์อักษรของเอกสารในระดับกฎหมายระหว่างประเทศ ซึ่งอิทธิพลของสนธิสัญญาดังกล่าวข้างต้นมีผลต่อกฎหมายของประเทศต่าง ๆ และทำให้เกิดพัฒนาการในระบบกฎหมายภายในของหลาย ๆ ประเทศ และกระตุ้นให้มีการเริ่มให้ความสำคัญกับการคุ้มครองสิทธิในความเป็นส่วนตัวมากยิ่งขึ้น โดยเฉพาะอย่างยิ่งการให้ความสำคัญคุ้มครองข้อมูลส่วนบุคคล

ในส่วนนี้ ผู้เขียนจะได้กล่าวถึงการคุ้มครองข้อมูลส่วนบุคคลของประเทศระบบคอมมอนลอว์ (Common Law) ได้แก่ ประเทศอังกฤษและประเทศแคนาดา ประเทศในระบบ (Civil Law) ได้แก่ ประเทศอิตาลี ประเทศฝรั่งเศสและประเทศญี่ปุ่น โดยมีรายละเอียดดังต่อไปนี้

3.2.1 กฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลของประเทศในระบบคอมมอนลอว์ (Common Law)

สำหรับในส่วนของกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลของประเทศในระบบคอมมอนลอว์ (Common Law) ผู้เขียนได้ทำการศึกษาการคุ้มครองข้อมูลส่วนบุคคลของประเทศอังกฤษและการคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดา โดยมีรายละเอียดดังต่อไปนี้

<sup>10</sup> จาก มาตรการทางกฎหมายในการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว: ศึกษากรณีการรบกวนสิทธิในความเป็นอยู่ส่วนตัวจากการใช้เว็บไซต์เครือข่ายสังคม (วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ) (น. 33-26), โดย คณาธิป ทองรวีวงศ์, 2553, กรุงเทพฯ: มหาวิทยาลัยเซนตจอร์จส์.

### 3.2.1.1 การคุ้มครองข้อมูลส่วนบุคคลของประเทศอังกฤษ

ประเทศอังกฤษในอดีตไม่มีกฎหมายที่ให้ความคุ้มครองข้อมูลส่วนบุคคลเป็นการเฉพาะ ต่อมาเมื่อประเทศมีความเจริญก้าวหน้าทางเทคโนโลยีสารสนเทศมากยิ่งขึ้น ทำให้การจัดเก็บข้อมูล ประมวลผล เรียกใช้ข้อมูล โดยระบบอิเล็กทรอนิกส์สามารถกระทำได้สะดวกรวดเร็ว และการเข้าถึงแหล่งข้อมูลต่าง ๆ สามารถกระทำได้จนยากที่จะป้องกันเป็นความลับได้ ส่งผลให้เกิดปัญหาการล่วงละเมิดสิทธิส่วนบุคคลเกี่ยวกับข้อมูลส่วนบุคคลมากขึ้น ประเทศอังกฤษได้ตระหนักถึงปัญหาดังกล่าวจึงเริ่มพัฒนากฎหมายและมีความพยายามที่จะให้ความคุ้มครองแก่สิทธิส่วนบุคคลมากขึ้น

ในปี ค.ศ. 1970 รัฐบาลอังกฤษได้จัดตั้งคณะกรรมการขึ้นศึกษาว่ามีความจำเป็นที่จะต้องตรากฎหมายขึ้นคุ้มครองการล่วงละเมิดสิทธิส่วนบุคคลของประชาชนที่เกิดจากการกระทำของผู้อื่นหรือหน่วยงานในภาคเอกชนหรือไม่ ซึ่งผลการศึกษาของคณะกรรมการหลายชุดไม่ปรากฏความจำเป็นที่จะต้องตรากฎหมายดังกล่าว<sup>11</sup> 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 และเพื่ออนุวัติการให้เป็นไปตามอนุสัญญาดังกล่าวประเทศอังกฤษจึงได้ตรากฎหมาย เพื่อคุ้มครองสิทธิส่วนบุคคลอันเกี่ยวกับข้อมูลข่าวสารขึ้น คือ พระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลข่าวสาร ค.ศ. 1984 (Data Protection Act 1984)

เมื่อได้ประกาศใช้ Data Protection Act 1984 แล้ว มีผลทำให้การจัดเก็บสารสนเทศทุกประเภทที่เกี่ยวกับบุคคล (Personal Data) โดยระบบคอมพิวเตอร์จะต้องดำเนินการให้เป็นไปตามกฎหมายฉบับนี้ ทั้งในภาครัฐและภาคเอกชน โดยข้อมูลข่าวสารนั้นต้องเป็นข้อมูลข่าวสารที่เกี่ยวกับบุคคลธรรมดา ซึ่งสามารถพิสูจน์หรือบ่งชี้ถึงบุคคลหนึ่ง ๆ ได้โดยตัวข้อมูลข่าวสารนั่นเองหรือโดยการตรวจสอบด้วยข้อมูลข่าวสารอื่น ๆ ที่อยู่ในความครอบครองของผู้ใช้ข้อมูล (Data User) และเป็นข้อมูลข่าวสารที่ถูกจัดเก็บไว้ในประเทศอังกฤษ<sup>12</sup>

<sup>11</sup> จาก *มาตรการทางอาญาในการคุ้มครองข้อมูลข่าวสาร* (วิทยานิพนธ์ปริญญาโท) (น. 102), โดย กิตติพันธุ์ เกียรติสุนทร, 2538, กรุงเทพฯ: จุฬาลงกรณ์มหาวิทยาลัย.

<sup>12</sup> จาก *การเปิดเผยข้อมูลส่วนบุคคลตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540* (วิทยานิพนธ์ปริญญาโท) (น. 53-55), โดย วีระพงษ์ บึงไกร, 2543, กรุงเทพฯ: จุฬาลงกรณ์มหาวิทยาลัย.

ต่อมาประเทศอังกฤษ ได้ออก 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 โดยกฎหมายฉบับนี้มีผลใช้บังคับกับข้อมูลที่ถูกประมวลผลด้วยมือซึ่งถูกจัดเก็บไว้ในแฟ้มข้อมูลและประมวลผลโดยวิธีการอัตโนมัติด้วย รวมทั้งมีการกำหนดเงื่อนไขหรือบรรทัดฐานขั้นต่ำของการประมวลผลข้อมูลที่จะถือว่าเป็นการประมวลผลข้อมูลที่ชอบด้วยกฎหมาย นอกจากนี้กฎหมายฉบับนี้ยังกำหนดให้มีข้อมูลส่วนบุคคลประเภทข้อมูลที่กระทบต่อความรู้สึก (Sensitive Data) ซึ่งมีผลทำให้ผู้ควบคุมดูแลข้อมูลไม่สามารถประมวลผลข้อมูลประเภทนี้ได้ เว้นแต่จะได้มีการปฏิบัติตามเงื่อนไขหรือข้อยกเว้นที่กำหนดไว้โดยเฉพาะ ทั้งยังได้กำหนดห้ามมิให้ส่งข้อมูลส่วนบุคคลไปยังประเทศที่อยู่นอกสมาชิกของ European Economic Area-EEA อีกด้วย เว้นแต่เป็นไปตามเงื่อนไขที่กำหนดไว้

นิยามศัพท์ที่สำคัญใน Data Protection Act 1998 ได้แก่<sup>13</sup>

“Data” (ข้อมูล) หมายถึง ข้อมูลซึ่งถูกประมวลผล (Processed) โดยเครื่องมือที่ทำงานโดยอัตโนมัติ เพื่อตอบสนองคำสั่งที่ป้อนเข้าไปเพื่อวัตถุประสงค์นั้นหรือข้อมูลซึ่งถูกบันทึกไว้โดยมีเจตนาที่จะนำไปประมวลผลโดยเครื่องมือที่ทำงานโดยอัตโนมัติ (เช่น ข้อมูลที่บันทึกไว้ในกระดาษที่เตรียมไว้เพื่อนำไปประมวลผลโดยคอมพิวเตอร์ เป็นต้น) หรือข้อมูลซึ่งถูกบันทึกไว้เป็นส่วนหนึ่งของ Relevant filing system (ระบบจัดเก็บข้อมูลที่เกี่ยวข้อง) หรือมีเจตนาที่จะนำไปบันทึกไว้เป็นส่วนหนึ่งของ Relevant filing system หรือข้อมูลซึ่งเป็นส่วนหนึ่งของ Accessible Record

“Personal Data” (ข้อมูลส่วนบุคคล) หมายถึง ข้อมูลที่เกี่ยวข้องกับบุคคลที่ยังมีชีวิตอยู่ซึ่งสามารถบ่งชี้ตัวบุคคลได้จากข้อมูลนั้นเองและข้อมูลอื่น ๆ ที่อยู่ในความครอบครองของผู้ควบคุมดูแลข้อมูล (Data Controller) หรืออาจอยู่ในความครอบครองของผู้ควบคุมดูแลข้อมูลในอนาคต ทั้งนี้ รวมถึงข้อมูลเกี่ยวกับการแสดงความคิดเห็นเกี่ยวกับตัวบุคคลธรรมดาและการแสดงเจตนาของผู้ควบคุมดูแลข้อมูลหรือบุคคลอื่นที่เกี่ยวข้องกับบุคคลธรรมดานั้นด้วย

<sup>13</sup> จาก การคุ้มครองข้อมูลส่วนบุคคล (วิทยานิพนธ์ปริญญาโท) (น. 83), โดย จิราวัฒน์ วรวัฒน์ธีรารัง, 2548, กรุงเทพฯ: มหาวิทยาลัยรามคำแหง.

“Relevant filing system” (ระบบจัดเก็บข้อมูลที่เกี่ยวข้องกัน) หมายถึง กลุ่มของข้อมูลเกี่ยวกับบุคคลธรรมดาซึ่งแม้จะไม่ได้ถูประมวลผลโดยเครื่องมืออัตโนมัติ แต่กลุ่มของข้อมูลนั้นได้มีการจัดวางโครงสร้างโดยอ้างอิงถึงตัวบุคคลหรือเฉพาะอย่างที่เกี่ยวข้องกับตัวบุคคลหนึ่งได้

“Accessible record” หมายถึง บันทึกสุขภาพ ซึ่งประกอบด้วย ข้อมูลที่บ่งบอกถึงสุขภาพทางกายหรือสุขภาพจิตหรือภาวะของบุคคลธรรมดาข้อมูลเกี่ยวกับการศึกษาหรือข้อมูลสาธารณะที่สามารถเข้าถึง

“Sensitive personal data” (ข้อมูลที่กระทบต่อความรู้สึก) หมายถึง ข้อมูลส่วนบุคคลซึ่งประกอบด้วยข้อมูลเกี่ยวกับเชื้อชาติหรือเผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนาหรือความเชื่ออื่น ๆ ที่มีลักษณะเดียวกัน การเป็นสมาชิกของสมาคมหรือสหภาพแรงงาน สุขภาพทางกายและจิตใจ พฤติกรรมทางเพศ การกระทำผิดหรือการถูกกล่าวหาว่ากระทำผิดกฎหมาย การดำเนินคดีหรือถูกดำเนินคดี การจำหน่ายคดี หรือการถูกลงโทษตามคำพิพากษาของศาลของเจ้าของข้อมูล

“Data Controller” (ผู้ควบคุมดูแลข้อมูล) หมายถึง บุคคลซึ่งเป็นผู้ตัดสินใจ (อาจเป็นการตัดสินใจโดยลำพังหรือตัดสินใจร่วมกับบุคคลอื่นก็ได้) ที่จะดำเนินการประมวลผลข้อมูลเพื่อวัตถุประสงค์ใดและในลักษณะใด อาจเป็นบุคคลธรรมดาหรือนิติบุคคลก็ได้ เช่น ห้างหุ้นส่วนบริษัทจำกัด สมาคม มูลนิธิ ฯลฯ หรืออาจเป็นหน่วยงานของรัฐก็ได้

“Data Processor” (ผู้ประมวลผลข้อมูล) หมายถึงบุคคลที่ประมวลผลข้อมูลในนามของผู้ควบคุมดูแลข้อมูลนอกเหนือจากลูกจ้างหรือพนักงานของผู้ควบคุมดูแลข้อมูล

“Processing” (การประมวลผล) หมายถึง การได้รับการบันทึก การครอบครองข้อมูลหรือการดำเนินการปฏิบัติการอย่างหนึ่งหรือหลายอย่างเกี่ยวกับข้อมูล ซึ่งรวมถึงการเก็บรวบรวม การตัดแปลง การแก้ไขข้อมูล การกู้ การพิจารณา การใช้ข้อมูล การเปิดเผยข้อมูลโดยการส่งผ่านทางสื่อ การเผยแพร่ การจัดวาง การประกอบ การกีดกันยับยั้ง การลบหรือการทำลายข้อมูล

ขอบเขตการใช้ Data Protection Act 1998 กำหนดไม่ให้บุคคลผู้ปฏิบัติงานอยู่ในสำนักงานคอมพิวเตอร์หรือตัวแทนของบุคคลดังกล่าวเปิดเผยข้อมูลอันเกี่ยวกับบุคคลโดยปราศจากอำนาจ ถ้าบุคคลใดฝ่าฝืนโดยเจตนาหรือไม่นำพาถึงผลที่จะเกิดขึ้น ถือว่ากระทำผิดตามพระราชบัญญัติฉบับนี้<sup>14</sup>

<sup>14</sup> มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลจากการใช้บริการเครือข่ายสังคมออนไลน์ (วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ) (น. 150). เล่มเดิม.

นอกจากนั้นยังได้กำหนดสิทธิของบุคคลผู้ถูกระบุในข้อมูลนั้น ๆ เช่น สิทธิที่จะได้ทราบว่าคุณถูกระบุอยู่ในข้อมูลนั้นหรือไม่ สิทธิที่จะเข้าสู่ข้อมูลอันเกี่ยวกับตน สิทธิในการแก้ไขหรือลบล้างข้อมูลที่ผิดพลาด สิทธิที่จะอนุญาตหรือไม่อนุญาตให้มีการเปิดเผยข้อมูล สิทธิในการดำเนินการเรียกร้องค่าเสียหายในกรณีที่คุณถูกระบุในข้อมูลนั้น ได้รับความเสียหายจากการที่ผู้ควบคุมดูแลข้อมูลปฏิบัติฝ่าฝืน เป็นต้น

การกำหนดหลักการคุ้มครองข้อมูลส่วนบุคคลไว้ 8 ข้อ (หรืออาจเรียกว่า “หลักของการจัดการข้อมูลที่ดี”) โดย Data Protection Act 1998 มาตรา 4 ได้กำหนดว่า หลักการคุ้มครองข้อมูลส่วนบุคคลที่อ้างอิงในพระราชบัญญัติฉบับนี้ คือ หลักการที่กำหนดไว้ใน Part I Schedule 1 ซึ่งสาระสำคัญ คือ การกำหนดให้ผู้ควบคุมดูแลข้อมูลต้องปฏิบัติตามหลักการดังกล่าว เว้นแต่ผู้ควบคุมดูแลข้อมูลจะสามารถอ้างสิทธิจากข้อยกเว้นของหลักต่าง ๆ นั้นได้ อันเป็นการบังคับให้ผู้ควบคุมดูแลข้อมูลต้องปฏิบัติตามหลักการต่าง ๆ นี้ ไม่ว่าผู้ควบคุมดูแลข้อมูลนั้นจะมีหน้าที่ตามกฎหมายที่จะต้องจัดแจ้งข้อมูลหรือไม่ก็ตามและเป็นการบังคับใช้กับข้อมูลส่วนบุคคลทั้งหมดที่ถูกประมวลผลโดยผู้ควบคุมดูแลข้อมูล หลักการดังกล่าว ได้แก่<sup>15</sup>

หลักการที่ 1 (The First principle) คือ ข้อมูลส่วนบุคคลจะต้องถูกประมวลผลอย่างเป็นธรรมและถูกต้องตามกฎหมาย โดยเฉพาะอย่างยิ่งจะถูกประมวลไม่ได้ เว้นแต่เป็นไปตามเงื่อนไขที่กฎหมายกำหนด

หลักการที่ 2 (The Second principle) คือ จะทำการจัดเก็บข้อมูลส่วนบุคคลไว้ได้เพียงเท่าที่ระบุไว้ในวัตถุประสงค์ และจะต้องเป็นวัตถุประสงค์อันชอบด้วยกฎหมายเท่านั้น ทั้งจะต้องไม่มีการประมวลผลที่ไม่สอดคล้องกับวัตถุประสงค์ดังกล่าว

ในการนี้ ผู้ควบคุมดูแลข้อมูลจะต้องแจ้งให้เจ้าของข้อมูลและ Commissioner ได้รู้ถึงวัตถุประสงค์ของการจัดเก็บโดยการระบุวัตถุประสงค์ไว้ในเอกสารดังต่อไปนี้

- (1) หนังสือบอกกล่าวที่ผู้ควบคุมดูแลข้อมูลแจ้งไปยังเจ้าของข้อมูล หรือ
- (2) ทะเบียนการจดแจ้งข้อมูลของผู้ควบคุมดูแลข้อมูลที่ให้ไว้ต่อ Commissioner

หลักการที่ 3 (The Third principle) คือ ข้อมูลส่วนบุคคลจะต้องเพียงพอเกี่ยวข้องกับและไม่มากเกินไปกว่าวัตถุประสงค์ของการประมวลผลนั้น

หลักการข้อนี้อาจเรียกอีกชื่อหนึ่งได้ว่า “หลักความเพียงพอ (Adequacy Principle)” กล่าวคือ ผู้ควบคุมดูแลข้อมูลจะจัดเก็บข้อมูลส่วนบุคคลเกินกว่าความจำเป็นตามที่ระบุไว้ใน

<sup>15</sup> จาก มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลกับการประกันชีวิต (วิทยานิพนธ์ปริญญาโท มหบัณฑิต) (น. 130), โดย กิตติศักดิ์ จันเส, 2553, กรุงเทพฯ: มหาวิทยาลัยธุรกิจบัณฑิต.

วัตถุประสงค์ของการจัดเก็บมิได้ ดังนั้น เพื่อให้การประมวลผลข้อมูลเป็นไปอย่างถูกต้องและสอดคล้องกับหลักการข้อนี้ ผู้ควบคุมดูแลข้อมูลส่วนบุคคลควรจะทบทวนแบบฟอร์มการกรอกข้อมูลเพื่อจัดเก็บข้อมูล เพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลที่จะทำการจัดเก็บมีเพียงพอ เกี่ยวข้องและไม่เกินกว่าวัตถุประสงค์ที่กำหนดไว้ เช่นแบบฟอร์มการสมัครงาน แบบฟอร์มสำหรับรายละเอียดของลูกค้า

หลักการที่ 4 (The Fourth principle) คือการจัดเก็บข้อมูลส่วนบุคคลจะต้องทำให้ถูกต้องเที่ยงตรงและทันสมัยอยู่เสมอ

หลักการข้อนี้เป็นหลักการที่กำหนดถึงหน้าที่ของผู้ควบคุมดูแลข้อมูล กล่าวคือ กำหนดให้ผู้ควบคุมดูแลข้อมูลมีหน้าที่โดยตรงในการทำให้ข้อมูลส่วนบุคคลซึ่งตนได้ทำการประมวลผลไว้ให้มีความเที่ยงตรงและทันสมัยอยู่เสมอ นอกจากนี้ หน้าที่ดังกล่าวยังเป็นหน้าที่ที่ไม่อาจมอบหมายให้คนอื่นทำแทนได้

หลักการที่ 5 (The Fifth principle) คือ การเก็บข้อมูลส่วนบุคคลไม่ว่าเพื่อวัตถุประสงค์ใด ๆ จะต้องไม่จัดเก็บไว้นานเกินกว่าความจำเป็นเพื่อวัตถุประสงค์นั้น

การจัดเก็บข้อมูลส่วนบุคคลไว้นานเกินกว่าความจำเป็นตามวัตถุประสงค์ของการประมวลผลข้อมูลนั้น ๆ ถือเป็น การปฏิบัติฝ่าฝืนหลักการในข้อนี้ อีกทั้งใน Data Protection Act 1998 เองก็ไม่ได้กำหนดรายละเอียดหรือหลักเกณฑ์เกี่ยวกับหลักการนี้ไว้ นอกจากนี้แนวทางการบังคับใช้กฎหมายของ Commissioner ในเรื่องนี้มีอยู่อย่างจำกัด ดังนั้นจึงยังไม่ชัดเจนว่าระยะเวลาที่นานเท่าใดจึงจะถือว่าเป็นระยะเวลานานเกินความจำเป็น

ดังนั้น การที่จะปฏิบัติตามหลักการนี้ได้จะต้องพิจารณาข้อเท็จจริงเป็นกรณี ๆ ไป โดยผู้ควบคุมดูแลข้อมูลจะต้องตรวจสอบข้อมูลส่วนบุคคลที่ถูกประมวลผลทั้งหมดและวัตถุประสงค์ของการประมวลผลนั้นและทำการพิจารณาว่าข้อมูลส่วนบุคคลแต่ละข้อมูลต้องจัดเก็บเอาไว้เพื่อวัตถุประสงค์ที่กำหนดไว้เป็นเวลานานเท่าใด โดยอาจกำหนดนโยบายในการเก็บรักษาข้อมูลด้วยการกำหนดระยะเวลาในการเก็บข้อมูลแต่ละประเภทไว้และหากผู้ควบคุมดูแลข้อมูลต้องการเก็บข้อมูลส่วนบุคคลไว้เป็นระยะเวลานานก็ควรมีเอกสารบ่งบอกถึงเหตุผลของการเก็บข้อมูลนั้น ๆ ไว้ในช่วงระยะเวลานั้นด้วย

นอกจากนี้ ผู้ควบคุมดูแลข้อมูลซึ่งมีข้อผูกพันที่จะต้องทำลายข้อมูลต้องจำไว้ว่ากระบวนการทำลายตัวมันเองจะมีค่าเท่ากับเป็นการประมวลผล ดังนั้นผู้ควบคุมดูแลข้อมูลจะต้องดำเนินการตามหลักการข้ออื่น ๆ ด้วย

อนึ่ง ตามหลักทั่วไปข้อมูลส่วนบุคคลควรถูกทำลายเมื่อไม่มีความต้องการข้อมูลนั้นอีก แต่ในบางกรณีอาจมีการกำหนดให้มีการเก็บข้อมูลส่วนบุคคลนั้นได้นานกว่าในกรณีปกติได้ โดยการอาศัยอำนาจตามกฎหมายว่าด้วยการต่อต้านการก่อการร้าย (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 หากผู้ประมวลผลข้อมูลกระทำการดังต่อไปนี้ ให้ถือว่าเป็นการกระทำที่ฝ่าฝืนหลักการคุ้มครองข้อมูลประการที่หก

- (1) ละเมิดสิทธิในการเข้าถึงข้อมูลตามที่กำหนดไว้ใน Section 7
- (2) ไม่ปฏิบัติตามคำร้องขอที่สมเหตุสมผลของเจ้าของข้อมูลที่ยุติการประมวลผลข้อมูลตามที่กำหนดไว้ใน Section 10 หรือไม่ปฏิบัติตามคำร้องนั้นภายใน 21 วันนับแต่วันได้รับคำร้องขอ
- (3) ไม่ปฏิบัติตามคำร้องขอให้ยุติการประมวลผลข้อมูลเพื่อทำการตลาดแบบตรงตามที่กำหนดไว้ใน Section 11
- (4) ปฏิบัติฝ่าฝืน Section 13 โดยไม่ปฏิบัติตามคำร้องขอเกี่ยวกับการตัดสินใจโดยอาศัยการประมวลผลของเครื่องมือที่ทำงานโดยอัตโนมัติหรือการไม่แจ้งให้เจ้าของข้อมูลทราบถึงการตัดสินใจตามคำร้องนั้น หรือการไม่ตอบกลับไปยังเจ้าของข้อมูลภายใน 21 วันนับแต่วันที่ได้รับคำร้องนั้น
- (5) ปฏิบัติฝ่าฝืน Section 12 a (สิทธิเฉพาะกาล (Transition Rights)) โดยการไม่ปฏิบัติตามคำบอกกล่าว (Notice) ของ Commissioner ที่ขอด้วยกฎหมาย

หลักประการที่ 7 (The Seventh Principle) คือ ต้องจัดให้มีมาตรการทางเทคนิคและการจัดการที่เหมาะสมในการป้องกันและจัดการกับการประมวลผลข้อมูลส่วนบุคคล โดยไม่ได้รับอนุญาตหรือไม่ชอบด้วยกฎหมาย และเพื่อป้องกันการสูญหายหรือการทำลายหรือทำให้เสียหายต่อข้อมูลส่วนบุคคล

หลักการข้อนี้มีรากฐานมาจาก EU Directive (95/46/EC) มีวัตถุประสงค์เพื่อให้ผู้ควบคุมดูแลข้อมูลเกิดความระมัดระวังในการประมวลผลข้อมูล และเป็นการกำหนดมาตรการเพื่อให้เจ้าของข้อมูลเกิดความมั่นใจว่าข้อมูลส่วนบุคคลของตนจะได้รับการดูแลอย่างเหมาะสม

แม้จะมีรากฐานมาจากที่เดียวกัน แต่ก็มีความแตกต่างบางประการ นั่นคือ EU Directive (95/46/EC) กำหนดให้ผู้ควบคุมดูแลข้อมูลต้องกำหนดให้มีมาตรการในการรักษาความปลอดภัยในระดับที่เหมาะสมกับความเสียหายที่อาจเกิดขึ้นจากการประมวลผลและจากลักษณะของข้อมูล

นั่นเอง แต่หลักประการที่ 7 นี้จะเน้นในเรื่องการกำหนดให้มีมาตรการเพื่อป้องกันไม่ให้เกิดความเสียหายแก่เจ้าของข้อมูลที่จะได้รับผลเสียหายจากการฝ่าฝืนบทบัญญัติในเรื่องการรักษาความปลอดภัย<sup>16</sup>

หลักประการที่ 8 (The Eight principle) คือข้อมูลส่วนบุคคลจะต้องไม่ถูกส่งออกไปยังประเทศหรือดินแดนที่อยู่นอกเขต European Economic Area (EEA) เว้นแต่ประเทศหรือดินแดนนั้นรับรองว่ามีระดับการคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลเพียงพอสำหรับการประมวลผลข้อมูลส่วนบุคคล

การที่ Data Protection Act 1998 กำหนดห้ามมิให้มีการส่งหรือโอนข้อมูลออกไปยังประเทศที่มีใช้สมาชิกของ European Economic Area (EEA) ก็เพื่อให้ความคุ้มครองแก่เจ้าของข้อมูล ทั้งนี้เนื่องจากหากประเทศนอกกลุ่ม EEA ไม่มีกฎหมายที่ให้ ความคุ้มครองเกี่ยวกับข้อมูลส่วนบุคคล หรือมีกฎหมายเช่นนี้แต่ไม่ได้ระดับมาตรฐานเดียวกับ EU Directive (95/46/EC) ก็ไม่ถูกผูกพันให้ต้องมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลตามหลักการที่กำหนดใน EU Directive (95/46/EC)

แต่เพื่อให้เกิดความคล่องตัวทางการค้า Data Protection Act 1998 จึงได้กำหนดให้หลักประการที่ 8 นี้มีข้อยกเว้นดังนี้<sup>17</sup>

1. กรณีที่ได้รับความยินยอมจากเจ้าของข้อมูล
2. การส่งออกข้อมูลมีความจำเป็น
  - 1) เพื่อดำเนินการตามสัญญาซึ่งเจ้าของข้อมูลเป็นคู่สัญญา หรือ
  - 2) เพื่อการดำเนินการตามความประสงค์ของเจ้าของข้อมูล โดยมีความมุ่งหมายเพื่อเข้าทำสัญญา
3. การส่งออกข้อมูลมีความจำเป็นเพื่อประโยชน์ในการลงนามหรือสรุปสัญญา ระหว่างผู้ควบคุมดูแลข้อมูลกับบุคคลที่ไม่ใช่เจ้าของข้อมูลแต่เป็นผู้เข้าทำสัญญา โดยได้รับการร้องขอจากเจ้าของข้อมูลหรือประโยชน์ของเจ้าของข้อมูล
4. การส่งออกข้อมูลมีความจำเป็นเพื่อประโยชน์สำคัญของสาธารณะ
5. การส่งออกข้อมูล
  - 1) มีความจำเป็นเพื่อวัตถุประสงค์ของหรือที่เกี่ยวข้องกับการดำเนินกระบวนการทางกฎหมาย

<sup>16</sup> แหล่งเดิม

<sup>17</sup> จาก แนวทางการคุ้มครองข้อมูลใน Big Data: ศึกษาประเด็นความเป็นส่วนตัวและความมั่นคงปลอดภัยของข้อมูล (น. 66-67), โดย ปิยะกัศร์ โรจนรัตน์วานิชย์, 2556, กรุงเทพฯ.

- 2) มีความจำเป็นเพื่อการได้รับความเห็นทางกฎหมาย
- 3) มีความจำเป็นเพื่อการก่อสร้างและสงวนไว้ซึ่งสิทธิตามกฎหมาย
6. การส่งออกข้อมูลมีความจำเป็นเพื่อที่จะคุ้มครองประโยชน์สำคัญต่อชีวิตของเจ้าของข้อมูล
7. การส่งข้อมูลส่วนบุคคลที่เป็นส่วนหนึ่งของข้อมูลซึ่งปรากฏอยู่ในทะเบียนสาธารณะ
8. การส่งข้อมูลนั้นกระทำโดยอยู่ภายใต้เงื่อนไขที่ Commissioner ได้ให้ความเห็นชอบแล้วและเงื่อนไขนั้นได้มีการกำหนดเงื่อนไขเวลากับมาตรการในการคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลอย่างเพียงพอแล้ว
9. การส่งออกข้อมูลนั้นได้รับอนุญาตจาก Commissioner ให้กระทำได้ เนื่องจากมีมาตรการในการคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลอย่างเพียงพอแล้ว

สิทธิของเจ้าของข้อมูลส่วนบุคคล ตาม Data Protection Act 1998 ได้กำหนดถึงสิทธิของเจ้าของข้อมูลที่เป็นบุคคลธรรมดาเกี่ยวกับข้อมูลส่วนบุคคลของตนที่อยู่ในความครอบครองของบุคคลอื่นหรือผู้ควบคุมดูแลข้อมูลไว้ดังนี้<sup>18</sup>

#### 1. สิทธิในการเข้าถึงข้อมูล

Data Protection Act 1998 มาตรา 7-9 กำหนดให้เจ้าของข้อมูลมีสิทธิที่จะร้องขอให้ผู้ควบคุมดูแลข้อมูลให้ข้อเท็จจริงแก่ตนว่า ผู้ควบคุมดูแลข้อมูลได้ดำเนินการประมวลผลข้อมูลส่วนบุคคลของตนอยู่หรือไม่อย่างไร โดยเจ้าของข้อมูลจะต้องทำคำร้องขอเป็นลายลักษณ์อักษร (ซึ่งรวมถึงการร้องผ่านทางสื่ออิเล็กทรอนิกส์ด้วย) และอาจต้องเสียค่าธรรมเนียมตามที่ผู้ควบคุมดูแลข้อมูลกำหนดด้วย ทั้งนี้ ผู้ควบคุมดูแลข้อมูลจะต้องทำตามคำร้องขอดังกล่าวภายใน 40 วันนับแต่วันที่ได้รับคำร้องขอจากเจ้าของข้อมูล (กรณีทั่วไป) หากปรากฏว่า ผู้ควบคุมดูแลข้อมูลได้ดำเนินการประมวลผลข้อมูลส่วนบุคคลของผู้ร้องขอยู่ ผู้ร้องขอในฐานะเจ้าของข้อมูลมีสิทธิจะได้รับคำอธิบายเพิ่มเติมเกี่ยวกับข้อมูลส่วนบุคคลของตนที่ผู้ควบคุมดูแลข้อมูลประมวลผลอยู่วัตถุประสงค์ของการประมวลผลข้อมูล และผู้รับข้อมูลหรือผู้ที่จะได้รับรู้ข้อมูลจากการเปิดเผยข้อมูลส่วนบุคคล

นอกจากนี้ เจ้าของข้อมูลยังมีสิทธิอื่น ๆ ที่เกี่ยวกับการเข้าถึงข้อมูลอีก เช่น สิทธิที่จะขอสำเนาเอกสารเกี่ยวกับข้อมูลส่วนบุคคล สิทธิที่จะรู้ถึงแหล่งที่มาของข้อมูล เป็นต้น หากเจ้าของข้อมูลร้องขอให้ผู้ควบคุมดูแลข้อมูลส่งข้อมูลส่วนบุคคลให้แก่ตนแล้ว แต่ผู้ควบคุมดูแลข้อมูลไม่ดำเนินการให้ เจ้าของข้อมูลอาจร้องขอต่อศาลได้ ซึ่งศาลอาจสั่งให้ผู้ควบคุมดูแลข้อมูลเปิดเผย

<sup>18</sup> จาก *กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของประเทศสหราชอาณาจักร* (รายงานผลการวิจัย) (น. 102-107), โดย พงศ์ศักดิ์ ยอดมณี, 2548, กรุงเทพฯ: สำนักงานคณะกรรมการกฤษฎีกา.

ข้อมูลที่เกี่ยวข้องแก่ศาลเพื่อใช้ประกอบการพิจารณาคำร้องขอของเจ้าของข้อมูลได้ (เป็นการเปิดเผยเฉพาะแก่ศาลเท่านั้น) หากศาลพิจารณาแล้วเห็นว่าเจ้าของข้อมูลเป็นผู้มีสิทธิตามกฎหมายที่จะได้รับข้อมูลเหล่านั้น ก็อาจมีคำสั่งให้ผู้ควบคุมดูแลข้อมูลปฏิบัติตามคำร้องขอของเจ้าของข้อมูลได้ ทั้งนี้ขึ้นอยู่กับดุลพินิจของศาล

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

1) แจ้งเป็นลายลักษณ์อักษรให้เจ้าของข้อมูลทราบว่าผู้ควบคุมดูแลข้อมูลได้ดำเนินการหรือตั้งใจจะดำเนินการตามคำบอกกล่าวของเจ้าของข้อมูล หรือ

2) แจ้งเป็นลายลักษณ์อักษรให้เจ้าของข้อมูลทราบว่าจะได้มีการดำเนินการบางส่วนตามคำบอกกล่าวของเจ้าของข้อมูลแล้ว (หากมี) และอธิบายถึงเหตุผลของผู้ควบคุมดูแลข้อมูลเห็นว่าคำบอกกล่าวของเจ้าของข้อมูลไม่มีความชอบธรรมเพราะเหตุใด

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

นอกจากนี้ EU Directive (95/46/EC) Article 14 (b) ยังได้กำหนดให้เจ้าของข้อมูลมีสิทธิที่จะคัดค้านการประมวลผลข้อมูลส่วนบุคคลของตนซึ่งผู้ควบคุมดูแลข้อมูลคาดว่าจะเป็นการประมวลผลข้อมูลเพื่อวัตถุประสงค์ในการทำการตลาดแบบตรงต่อไป หรือคัดค้านการเปิดเผยข้อมูลให้แก่บุคคลที่สาม หรือการใช้ข้อมูลในนามของบุคคลที่สามเพื่อวัตถุประสงค์ในการทำการตลาดแบบตรง

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

5. สิทธิเรียกร้องค่าเสียหายในกรณีที่บุคคลนั้นได้รับความเสียหายจากการที่ผู้ควบคุมดูแลข้อมูลปฏิบัติฝ่าฝืน Data Protection Act 1998 มาตรา 13 กำหนดให้บุคคลธรรมดาที่ได้รับความเสียหาย (Damage) หรือความเสียหายและความทุกข์ (Damage and Distress) จากการที่ผู้ควบคุมดูแลข้อมูลปฏิบัติฝ่าฝืนบทบัญญัติใน Data Protection Act 1998 มีสิทธิที่จะได้รับการชดเชยความเสียหาย หากผู้ควบคุมดูแลข้อมูลไม่สามารถพิสูจน์ได้ว่าคนได้ใช้ความระมัดระวังตามสมควรแก่ทุกสถานการณ์เพื่อที่จะปฏิบัติให้เป็นไปตามบทบัญญัติกฎหมายที่เกี่ยวข้องแล้ว

6. สิทธิในการดำเนินการเพื่อแก้ไข ลบ หรือทำลายข้อมูลที่ไม่ถูกต้อง Data Protection Act 1998 มาตรา 14 กำหนดไว้ว่าหากเจ้าของข้อมูลเห็นว่าข้อมูลส่วนบุคคลของตนที่อยู่ในความครอบครองของผู้ควบคุมดูแลข้อมูลไม่เที่ยงตรง แต่ข้อมูลนั้นเป็นข้อมูลที่ถูกควบคุมดูแลข้อมูลได้บันทึกไว้อย่างถูกต้องตรงตามที่เจ้าของข้อมูลหรือบุคคลที่สามเปิดเผยให้แก่ผู้ควบคุมดูแลข้อมูลในกรณีนี้ กำหนดให้ศาลมีอำนาจสั่งให้ผู้ควบคุมดูแลข้อมูลแนบถ้อยคำแสดงถึงข้อมูลที่ถูกต้องเที่ยงตรงตามที่ศาลเห็นชอบแล้วไว้เป็นส่วนหนึ่งของข้อมูลเดิมได้แทนที่จะมีคำสั่งให้ผู้ควบคุมดูแลข้อมูล แก้ไข ลบ หรือทำลายข้อมูล

7. สิทธิในการขอให้ตรวจสอบประเมินผลการปฏิบัติตามกฎหมาย Data Protection Act 1998 มาตรา 42 กำหนดว่า บุคคลใดเห็นว่าตนได้รับผลกระทบโดยตรงจากการประมวลผลข้อมูลของผู้ควบคุมดูแลข้อมูลมีสิทธิร้องขอให้ Commissioner เข้าตรวจสอบและประเมินผลการปฏิบัติงานของผู้ควบคุมดูแลข้อมูลนั้นว่า ได้มีการปฏิบัติฝ่าฝืนกฎหมายหรือไม่ อย่างไร (บุคคลตามมาตรา 42 นี้ รวมถึงนิติบุคคลด้วย)

ข้อยกเว้นการคุ้มครองข้อมูลส่วนบุคคลตาม Data Protection Act 1998 กำหนดไว้ 10 กรณีเพื่อเปิดช่องทางให้เข้าถึงข้อมูลส่วนบุคคลได้ ได้แก่<sup>19</sup>

1. กรณีเกี่ยวกับความมั่นคงของประเทศ
2. กรณีเกี่ยวกับอาชญากรรมและภาษีอากร
3. กรณีเกี่ยวกับงานด้านสุขภาพและสังคม
4. กรณีเกี่ยวกับการออกกฎระเบียบด้านการบริการทางการเงิน
5. กรณีเกี่ยวกับสิทธิพิเศษในการประกอบอาชีพด้านกฎหมายและการพิจารณา

พิพากษาของศาล

6. กรณีเกี่ยวกับบัญชีเงินเดือนและบัญชีรายรับรายจ่าย

<sup>19</sup> มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลจากการใช้บริการเครือข่ายสังคมออนไลน์ (วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ) (น. 155). เล่มเดิม.

7. กรณีเกี่ยวข้องกับข้อมูลส่วนบุคคลที่จัดเก็บไว้เพื่อภายในบ้านของคุณหรือเพื่อวัตถุประสงค์อื่นอันจำกัด

8. กรณีเป็นข้อมูลที่จัดเก็บในฐานะที่เป็นสมาชิก

9. กรณีเพื่อการเก็บสถิติหรือการค้นคว้า

10. กรณีเกี่ยวกับคะแนนในการทดสอบ

การเข้าถึงข้อมูลส่วนบุคคล ผู้เป็นเจ้าของข้อมูลมีสิทธิที่จะได้รับสำเนาบันทึกข้อมูลส่วนบุคคลของคุณจากผู้เก็บและใช้ข้อมูลนั้น ๆ หากข้อมูลนั้นอยู่ในรูปแบบหรือถ้อยคำที่ไม่อาจเข้าใจได้ จะต้องมีคำอธิบายประกอบข้อมูลนั้นมาให้พร้อมกับสำเนาข้อมูลซึ่งการร้องขอดังกล่าวจะต้องเป็นไปตามเงื่อนไขที่กำหนดไว้ดังนี้<sup>20</sup>

1. คำร้องจะต้องทำเป็นหนังสือและชำระค่าธรรมเนียมในการร้องขอ (หากไม่ระบุไว้เป็นอย่างอื่น) การร้องขอต้องเป็นไปเพื่อที่จะได้รับการแจ้งให้ทราบว่ามีส่วนข้อมูลส่วนบุคคลของคุณหรือไม่ ถ้ามีจะได้ขอรับสำเนาข้อมูลนั้นด้วยหากผู้เก็บและใช้ข้อมูลได้จดทะเบียนการเก็บและใช้ข้อมูลแยกเป็นกรณี จะต้องทำคำร้องขอและชำระค่าธรรมเนียมแยกกัน

2. ผู้ร้องขอจะต้องแสดงหลักฐานประจำตัวและระบุรายละเอียดถึงข้อมูลที่ตนต้องการตามที่ผู้เก็บและผู้ใช้ข้อมูลได้กำหนดไว้ตามสมควร ถ้าเป็นข้อมูลที่เมื่อเปิดเผยแล้วต้องเปิดเผยข้อมูลส่วนบุคคลของบุคคลอื่นด้วย จะต้องขออนุญาตจากบุคคลนั้น ๆ เสียก่อน

3. ผู้เก็บและใช้ข้อมูลจะต้องตอบคำร้องขอภายใน 40 วันหลังจากที่ได้รับคำร้องขอและหลักฐานต่าง ๆ ตามเงื่อนไขที่กำหนดไว้

4. กรณีที่ข้อมูลส่วนบุคคลนั้นเป็นเรื่องของสุขภาพร่างกายรัฐมนตรีว่าการกระทรวงการต่างประเทศมีอำนาจที่จะแก้ไขหรือยกเว้นบทบัญญัติที่เกี่ยวกับการเข้าสู่ข้อมูลของบุคคลหนึ่ง ๆ ได้ตามสมควร ดังนั้น หากเป็นกรณีข้อมูลทางการแพทย์และการขอเข้าสู่ข้อมูลนั้น โดยตรงจะเป็นผลร้ายต่อบุคคลผู้ร้องขอ รัฐมนตรีว่าการกระทรวงการต่างประเทศย่อมมีอำนาจที่จะออกกฎระเบียบให้การเข้าสู่ข้อมูลในกรณีดังกล่าวเป็นไปโดยทางอ้อม หรือต้องเข้าสู่ข้อมูลนั้นโดยผ่านบุคคลอื่น

การแก้ไขเพิ่มเติมข้อมูลส่วนบุคคล การที่บุคคลหนึ่ง ๆ จะต้องได้รับสิทธิที่จะแก้ไขเพิ่มเติมหรือลบข้อมูลส่วนบุคคลของคุณได้ ดังนั้น จึงได้กำหนดให้บุคคลสามารถร้องขอแก้ไขเพิ่มเติมข้อมูลส่วนบุคคลของคุณได้เป็น 2 กรณี คือ

<sup>20</sup> มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลกับการประกันชีวิต (วิทยานิพนธ์ปริญญาโท) (น. 132-134). เล่มเดิม.

กรณีที่ 1 เป็นการร้องขอแก้ไขเพิ่มเติมข้อมูลส่วนบุคคลของตนต่อผู้เก็บและใช้ข้อมูลนั้นโดยตรง

จากหลักการดังกล่าวข้างต้น จึงมีการกำหนดให้ใช้บังคับกับผู้เก็บและใช้ข้อมูลส่วนบุคคลของบุคคลใด ๆ และบุคคลผู้ปฏิบัติงานในสำนักงานคอมพิวเตอร์ซึ่งเก็บและใช้ข้อมูลดังกล่าว ดังนั้น หากบุคคลได้ร้องขอและเข้าสู่ข้อมูลส่วนบุคคลของตนเพื่อตรวจสอบและรับสำเนาข้อมูลแล้วพบว่าข้อมูลที่ได้รับจากหน่วยงานหรือผู้เก็บและใช้ข้อมูลมีความผิดพลาดหรือไม่เป็นไปตามที่กฎหมายกำหนดไว้ ก็สามารถร้องขอให้มีการดำเนินการแก้ไขเพิ่มเติมหรือลบข้อมูลที่ผิดพลาดหรือบกพร่องนั้น ๆ และหน่วยงานหรือผู้เก็บและใช้ข้อมูลนั้นต้องรีบตรวจสอบและดำเนินการแก้ไขเพื่อให้เป็นไปตามหลักการดังกล่าวข้างต้น

หากหน่วยงานหรือผู้เก็บและใช้ข้อมูลดังกล่าวเพิกเฉยหรือไม่ดำเนินการใด ๆ บุคคลผู้ร้องขออาจยื่นคำร้องต่อ The Commissioner ว่ามีการล่วงละเมิดหลักการคุ้มครองข้อมูลส่วนบุคคล และเจ้าหน้าที่ดังกล่าวก็จะดำเนินการกับผู้ฝ่าฝืนตามที่พระราชบัญญัติฉบับนี้กำหนดไว้หรือหากเข้าใจผิดตามที่กฎหมายกำหนดก็อาจยื่นคำร้องต่อศาลให้มีการดำเนินการเช่นนั้น

กรณีที่ 2 เป็นการร้องขอแก้ไขเพิ่มเติมข้อมูลส่วนบุคคลของตนต่อศาล

การที่สิทธิของบุคคลซึ่งได้รับการรับรองคุ้มครองตามกฎหมายถูกล่วงละเมิด บุคคลผู้ได้รับความเสียหายย่อมมีสิทธิที่จะร้องขอต่อศาลเพื่อให้มีการบังคับการตามสิทธิของตนได้ ซึ่งพระราชบัญญัติฉบับนี้ได้ให้การรับรองไว้โดยกำหนดเงื่อนไขที่จะสามารถร้องขอต่อศาล ทั้งยังกำหนดให้ศาลมีอำนาจในการที่จะออกคำสั่งในเรื่องนี้ได้

### 3.2.1.2 การคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดา

กฎหมายคุ้มครองข้อมูลข่าวสารของแคนาดา คือ Personal Information Protection and Electronic Documents Act 2000 (PIPEDA) เกิดจากแรงกดดันหรือได้รับผลกระทบจาก European Union (EU) เช่นเดียวกับประเทศสหรัฐอเมริกาและประเทศอื่น ๆ ที่ต้องมีการพัฒนากฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้เทียบเท่า EU Personal Information Protection and Electronic Documents Act 2000<sup>21</sup>

หลักเกณฑ์และแนวทางการพิจารณาและการดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ของประเทศแคนาดามีขอบเขตของกฎหมายฉบับนี้ใช้บังคับแก่องค์กรทั้งหลาย (Organizations) ที่มีการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล ในการเก็บรวบรวม ใช้ หรือเปิดเผย

<sup>21</sup> จาก มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลของเด็กบนเครือข่ายอินเทอร์เน็ต (วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ) (น. 66), โดย พนิดา พูลสวัสดิ์, 2556, กรุงเทพฯ: สถาบันบัณฑิตพัฒนบริหารศาสตร์.

เพื่อการประกอบกิจการขององค์กร หรือที่เกี่ยวกับลูกจ้างขององค์กรหรือข้อมูลส่วนบุคคลที่ใช้ในกิจการหรือธุรกิจของสหพันธรัฐ ทั้งนี้ กฎหมายได้กำหนดกฎเกณฑ์ที่ใช้บังคับแก่การเก็บรวบรวมการใช้ และการเปิดเผยข้อมูลส่วนบุคคล โดยให้ความสำคัญกับการชั่งน้ำหนักระหว่างสิทธิความเป็นส่วนตัวของบุคคล (The right of privacy of individuals) ในส่วนที่เกี่ยวกับข้อมูลส่วนบุคคลของบุคคลนั้น กับความจำเป็นขององค์กรในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ซึ่งวิญญูชนเห็นว่าเหมาะสมกับสถานการณ์<sup>22</sup>

กฎหมายแคนาดากำหนดค่านิยมของข้อมูลส่วนบุคคลว่าหมายถึง ข้อมูลที่เกี่ยวกับบุคคลธรรมดาคนหนึ่งซึ่งสามารถกำหนดตัวบุคคลได้ และรวมถึงข้อมูลที่เกี่ยวข้องกับสุขภาพของบุคคล (Personal Health Information) ไม่ว่าจะมีชีวิตอยู่หรือถึงแก่ความตายแล้ว ดังต่อไปนี้<sup>23</sup>

1. ข้อมูลที่เกี่ยวกับสุขภาพร่างกายหรือจิตใจของบุคคลธรรมดาคนนั้น
2. ข้อมูลเกี่ยวกับการบริการทางสุขภาพที่บุคคลธรรมดาคนนั้นได้รับ
3. ข้อมูลเกี่ยวกับการบิรจาคอวัยวะส่วนใดของร่างกายหรือส่วนประกอบใดของร่างกายของบุคคลธรรมดาคนนั้น หรือข้อมูลที่ได้รับจากการทดสอบหรือตรวจสอบ อวัยวะส่วนใดของร่างกายหรือส่วนประกอบส่วนใดของร่างกายของบุคคลธรรมดาคนนั้น
4. ข้อมูลที่รวบรวมได้ในการให้บริการทางสุขภาพแก่บุคคลธรรมดาคนนั้น
5. ข้อมูลอื่นที่เกี่ยวข้องที่รวบรวมได้ในการให้บริการทางสุขภาพแก่บุคคลธรรมดาคนนั้น แต่ไม่รวมถึงชื่อ ตำแหน่ง สถานที่ทำงาน (สถานที่ประกอบธุรกิจ) หรือหมายเลขโทรศัพท์ของลูกจ้างในองค์กร

องค์กรหรือบุคคลที่ไม่อยู่ภายใต้บังคับของกฎหมายนี้ กล่าวคือ กฎหมายนี้ไม่ใช้บังคับแก่องค์กรหรือบุคคลบางประเภทหรือได้รับการยกเว้นไม่ต้องปฏิบัติตามกฎหมายนี้<sup>24</sup>

<sup>22</sup> จาก *กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดา*, โครงการจัดทำความเห็นทางวิชาการเพื่อจัดทำรายงานเกี่ยวกับหลักเกณฑ์และแนวทางการพิจารณาและดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และจัดทำคู่มือการปฏิบัติงานเกี่ยวกับข้อมูลส่วนบุคคลภาครัฐตาม พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 (รายงานผลการวิจัย) (น. 49-70), โดย สมศักดิ์ นวตระกูลพิสุทธิ์, 2547, กรุงเทพฯ: สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์.

<sup>23</sup> แหล่งเดิม.

<sup>24</sup> จาก *การศึกษาและพัฒนาแนวทางการคุ้มครองข้อมูลส่วนบุคคลภายใต้ประชาคมอาเซียน* (น. 29-30), โดย อุดม รัฐอมฤต และคณะ, 2557, กรุงเทพฯ.

1. หน่วยงานของรัฐ ที่อยู่ภายใต้บังคับของ Privacy Act 1985
2. บุคคลธรรมดาในส่วนที่เกี่ยวกับข้อมูลส่วนบุคคลที่บุคคลธรรมดาเก็บรวบรวม ใช้ หรือเปิดเผยเพื่อวัตถุประสงค์ส่วนตัวและมีใช้เพื่อการอย่างอื่น
3. องค์กรใด ๆ ที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการหนังสือพิมพ์ ศิลปะ หรือวรรณกรรม และมีใช้เพื่อการอย่างอื่น

ดังที่ได้กล่าวแล้วข้างต้นว่ากฎหมายฉบับนี้ได้กำหนดให้มีองค์กรที่ทำหน้าที่ควบคุมและบังคับการให้เป็นไปตามกฎหมาย คือ กรรมการสิทธิความเป็นส่วนตัว (Privacy Commissioner) ซึ่งมีอำนาจหน้าที่สำคัญหลายประการ ดังนี้

- 1) การรับคำร้องของบุคคล ในกรณีที่ต้องคุ้มครองฝ่าฝืนบทบัญญัติ หรือในกรณีที่มีการละเมิดข้อมูลส่วนบุคคลและแจ้งให้องค์กรที่ถูกร้องเรียนทำการสอบสวนและพิจารณาคำร้องดังกล่าว

- 2) หากคณะกรรมการพิจารณาแล้วเห็นว่ามีความผิดอันสมควรในอันที่จะต้องทำการสอบสวนเรื่องใด ๆ ที่เห็นว่าการละเมิดข้อมูลส่วนบุคคล กรรมการสามารถนำเรื่องดังกล่าวขึ้นมาพิจารณาได้

- 3) เพื่อให้บรรลุวัตถุประสงค์ในการดำเนินการสอบสวน กรรมการอาจใช้อำนาจเรียกให้บุคคลใดมาให้คำชี้แจงหรือเรียกให้ส่งหลักฐานใด ๆ ที่เกี่ยวข้องกับเรื่องที่มีการร้องเรียนนั้นรับหลักฐานและข้อมูลอื่นใดตามที่คณะกรรมการเห็นสมควร เข้าไปในสถานที่ขององค์กรใด ๆ ในเวลาที่เหมาะสม และมีอำนาจซักถามบุคคลในสถานที่นั้นได้ตามที่เห็นสมควร ตลอดจนเจรจาเป็นการส่วนตัวกับบุคคลที่อยู่ในสถานที่ดังกล่าว

- 4) คณะกรรมการต้องจัดทำรายงานผลการพิจารณาและแก้ไขปัญหาประกอบด้วย คำวินิจฉัยและคำแนะนำของคณะกรรมการในคดีต่าง ๆ การระงับข้อโต้แย้งที่คู่กรณีได้ตกลงกัน คำร้องที่องค์กรส่งให้แก่คณะกรรมการ คำบอกกล่าวเกี่ยวกับการดำเนินการที่ได้กระทำไปแล้ว หรือที่จะกระทำตามคำแนะนำที่ระบุไว้ในรายงาน หรือเหตุผลที่ไม่ดำเนินการหรือไม่ดำเนินการ และความช่วยเหลือที่ผู้ยื่นคำร้องอาจได้รับตามที่กำหนดในกฎหมาย

ภายใต้กฎหมายนี้กำหนดให้มีการจัดตั้งสำนักงานกรรมการสิทธิความเป็นส่วนตัวแห่งแคนาดา (Office of the Privacy Commissioner of Canada) เป็นองค์กรที่คอยช่วยเหลือให้คำปรึกษาแก่บุคคลเกี่ยวกับสิทธิในความเป็นส่วนตัวและความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและการคุ้มครองข้อมูลทางอิเล็กทรอนิกส์ที่ได้รับการคุ้มครองภายใต้กฎหมายฉบับนี้ โดยกฎหมายนี้มีอำนาจควบคุมองค์กรต่าง ๆ (Organization) ซึ่งหมายความรวมถึง สมาคม ห้างหุ้นส่วนนิติบุคคล และสหภาพแรงงาน กฎหมายได้กำหนดไว้ว่าองค์กรทั้งหลายมีภาระหน้าที่ที่

กำหนดไว้ในเอกสาร 1 แบบท้ายกฎหมาย ซึ่งเป็นแบบปฏิบัติเพื่อการคุ้มครองข้อมูลส่วนบุคคล (Model Code for the Protection of Personal Information) ตามหลักเกณฑ์มาตรฐานแห่งชาติ แคนาดา (National Standard of Canada) ดังนี้

### 1) หลักความรับผิดชอบ

หน่วยงานหรือองค์กรต้องมีความรับผิดชอบต่อข้อมูลส่วนบุคคลที่อยู่ในความควบคุมของตน และต้องแต่งตั้งบุคคลหนึ่งหรือหลายคนซึ่งรับผิดชอบต่อการปฏิบัติขององค์กรตามหลักปฏิบัติต่าง ๆ ที่กำหนดในแบบปฏิบัตินี้

องค์กรต้องกำหนดนโยบายและแนวทางปฏิบัติเพื่อหลักปฏิบัติต่าง ๆ ที่กำหนดในแบบปฏิบัตินี้บังเกิดผล ซึ่งได้แก่ การกำหนดกระบวนการคุ้มครองข้อมูลส่วนบุคคล การกำหนดกระบวนการรับและตอบคำร้อง (Complaints) หรือข้อซักถาม (Inquiries) ต่าง ๆ การฝึกอบรมพนักงานและแจ้งให้พนักงานที่เกี่ยวข้องทราบเกี่ยวกับนโยบายและแนวทางปฏิบัติในเรื่องนี้ขององค์กร การจัดทำข้อมูลชี้แจงนโยบายและกระบวนการต่าง ๆ ขององค์กร<sup>25</sup>

### 2) หลักการแจ้งวัตถุประสงค์

องค์กรต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงวัตถุประสงค์ของการเก็บรวบรวมข้อมูลก่อนหรือในขณะที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น ทั้งนี้การแจ้งอาจกระทำด้วยวาจาหรือเป็นลายลักษณ์อักษรก็ได้ตามลักษณะของการเก็บรวบรวมข้อมูลนั้น และมีหน้าที่ต้องดำเนินการ ดังนี้

1. องค์กรต้องจัดพิมพ์ประกาศหรือเอกสารเพื่อแจ้งให้รับทราบเกี่ยวกับวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อให้สอดคล้องกับหลักการเปิดเผย และหลักการเข้าตรวจสอบข้อมูลของบุคคล

2. องค์กรต้องเก็บรวบรวมข้อมูลส่วนบุคคลแต่เพียงข้อมูลที่จำเป็นต่อวัตถุประสงค์ที่ได้แจ้งให้ทราบแล้วเท่านั้น ทั้งนี้เป็นไปตามหลักการเก็บรวบรวมข้อมูลอย่างจำกัด

3. ในกรณีที่องค์กรจะนำข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้ไปใช้ประโยชน์เพื่อวัตถุประสงค์อย่างอื่นซึ่งมิได้แจ้งให้ทราบล่วงหน้า องค์กรต้องแจ้งวัตถุประสงค์ใหม่นั้นให้บุคคลนั้นทราบเสียก่อน และจะต้องได้รับความยินยอมก่อนที่จะนำข้อมูลนั้นไปใช้ประโยชน์ตามวัตถุประสงค์ใหม่นั้น ทั้งนี้ เว้นแต่วัตถุประสงค์ใหม่นั้นเป็นไปตามที่กฎหมายกำหนด

<sup>25</sup> กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดา, โครงการจัดทำความเห็นทางวิชาการเพื่อจัดทำรายงานเกี่ยวกับหลักเกณฑ์และแนวทางการพิจารณาและดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และจัดทำคู่มือการปฏิบัติงานเกี่ยวกับข้อมูลส่วนบุคคลภาครัฐตาม พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 (รายงานผลการวิจัย) (น. 97). เล่มเดิม.

### 3) หลักความยินยอม

บุคคลที่ให้ข้อมูลส่วนบุคคลต้องได้รับทราบและให้ความยินยอมแก่การเก็บรวบรวม การใช้หรือการเปิดเผยข้อมูลส่วนบุคคลของบุคคลนั้น ทั้งนี้ เว้นแต่เป็นกรณีที่ไม่สมควรตามที่กำหนดในกฎหมาย

องค์กรหรือผู้ที่อยู่ภายใต้บังคับของกฎหมายฉบับนี้จะต้องได้รับความยินยอมจากเจ้าของข้อมูลในกรณีที่มีการจัดเก็บ การใช้ และการเปิดเผยข้อมูลส่วนบุคคล โดยเจ้าของข้อมูลมีสิทธิที่จะเข้าถึงข้อมูลของตนที่อยู่ในความควบคุมหรือภายใต้การครอบครองขององค์กร ภาคเอกชนตลอดจนมีสิทธิในการเรียกร้องให้ปรับปรุงแก้ไขข้อมูลของตนให้มีความถูกต้องในกรณีที่เป็น ซึ่งการได้รับความยินยอมจากเจ้าของข้อมูลนั้น เจ้าของข้อมูลอาจแสดงออกซึ่งความยินยอมในรูปแบบที่ชัดเจนเป็นลายลักษณ์อักษรหรือด้วยวาจา หรือโดยไม่ชัดเจนจากการตีความจากการดำเนินการหรือการไม่ดำเนินการของบุคคลผู้เป็นเจ้าของข้อมูล

องค์กรธุรกิจหรือองค์กรภาคเอกชนสามารถนำข้อมูลส่วนบุคคลไปใช้เพื่อวัตถุประสงค์ตามที่ระบุไว้เท่านั้น สำหรับกรณีที่มีการใช้ข้อมูลดังกล่าวเพื่อวัตถุประสงค์อื่นนอกเหนือจากที่ได้ระบุไว้ นั้น จำเป็นที่จะต้องได้รับความยินยอมจากผู้เป็นเจ้าของข้อมูลดังกล่าวเป็นรายกรณีอีกครั้ง ทั้งนี้ บุคคลผู้เป็นเจ้าของข้อมูลจะต้องมั่นใจได้ว่าข้อมูลส่วนบุคคลของตนได้รับการคุ้มครองภายใต้มาตรการปกป้องข้อมูลที่เหมาะสม อาทิ การเก็บรักษาในสถานที่ที่ปลอดภัย การมีระบบรหัสผ่าน หรือการถอดรหัสเพื่อคุ้มครองข้อมูล เป็นต้น<sup>26</sup>

โดยทั่วไปแล้ว องค์กรมีหน้าที่ที่จะต้องขอความยินยอมสำหรับการใช้หรือการเปิดเผยข้อมูลนั้นในขณะทำการเก็บรวบรวม แต่อย่างไรก็ตามในบางสถานการณ์อาจมีการขอความยินยอม นำข้อมูลไปใช้หรือเปิดเผยภายหลังการเก็บรวบรวมข้อมูลแต่ต้องก่อนการนำข้อมูลนั้นไปใช้ โดยการขอความยินยอมนั้นองค์กรต้องจัดให้มีการขอความยินยอมโดยวิธีการดำเนินการที่เหมาะสมเพื่อให้บุคคลได้รับแจ้งถึงวัตถุประสงค์ของการที่จะนำข้อมูลนั้นไปใช้ และจะต้องไม่ขอความยินยอมในการดำเนินการมากเกินไปจนความจำเป็นสำหรับการดำเนินการตามวัตถุประสงค์ที่ชอบด้วยกฎหมายและที่ได้แจ้งให้ทราบ

รูปแบบของความยินยอมอาจแตกต่างกันไปขึ้นอยู่กับสถานการณ์และประเภทของข้อมูล ทั้งนี้ในการกำหนดรูปแบบของความยินยอมองค์กรต้องคำนึงถึงประเภทของข้อมูล โดยเฉพาะอย่างยิ่งข้อมูลส่วนตัว โดยเฉพาะ (Sensitive data) โดยหากเป็นข้อมูลส่วนตัว โดยเฉพาะ

<sup>26</sup> การศึกษาและพัฒนาแนวทางการคุ้มครองข้อมูลส่วนบุคคลภายใต้ประชาคมอาเซียน (น. 29).  
เล่มเดิม.

ควรขอความยินยอมอย่างชัดแจ้ง ในกรณีที่มีความเป็นข้อมูลส่วนตัวโดยเฉพาะอย่างน้อยก็อาจขอความยินยอมโดยปริยายได้ เช่น บันทึกรทางการแพทย์ และบันทึกรายได้ แต่ข้อมูลที่ไม่ได้ถูกจัดอยู่ในข้อมูลประเภทที่เป็นข้อมูลส่วนตัวโดยเฉพาะก็อาจต้องใช้ความระมัดระวังในการแจ้งขอความยินยอมขึ้นอยู่กับบริบทแวดล้อม เช่น ชื่อและที่อยู่ของสมาชิกนิตยสารซึ่งโดยทั่วไปจะไม่ถือว่าเป็นข้อมูลส่วนตัวโดยเฉพาะ แต่หากเป็นชื่อและที่อยู่ของสมาชิกนิตยสารที่มีลักษณะเฉพาะ (Special-Interest magazines) อาจถือว่าเป็นข้อมูลส่วนตัวโดยเฉพาะก็ได้ ความยินยอมอาจเป็นความยินยอมอย่างชัดแจ้ง (Express Consent) ความยินยอมโดยปริยาย (Implied Consent) ก็ได้และบุคคลธรรมดาอาจถอนความยินยอมเมื่อใดก็ได้โดยองค์กรต้องแจ้งกระบวนการถอนความยินยอมให้บุคคลนั้นทราบด้วย

#### 4) หลักการเก็บรวบรวมข้อมูลอย่างจำกัด

การเก็บรวบรวมข้อมูลส่วนบุคคลจะต้องจำกัดเฉพาะแต่ข้อมูลที่จำเป็นและเป็นไปตามวัตถุประสงค์ขององค์กรที่ได้แจ้งให้ทราบและต้องเก็บรวบรวม โดยวิธีการที่เป็นธรรมและชอบด้วยกฎหมายขององค์กรจะต้องไม่เก็บรวบรวมข้อมูลส่วนบุคคลโดยวิธีที่เป็นการเลือกปฏิบัติ (Indiscriminately) และต้องเก็บรวบรวมข้อมูลอย่างจำกัดเพียงเท่าที่จำเป็นต่อวัตถุประสงค์และต้องระบุประเภทของข้อมูลที่เก็บรวบรวมโดยการจัดทำเป็นประกาศ หรือคู่มือเกี่ยวกับนโยบายและแนวทางปฏิบัติขององค์กร แจ้งแก่ผู้เป็นเจ้าของข้อมูล ซึ่งหลักการนี้มีความสัมพันธ์อย่างใกล้ชิดกับหลักการแจ้งวัตถุประสงค์และหลักความยินยอม<sup>27</sup>

#### 5) หลักการจำกัดการใช้ การเปิดเผย และการเก็บรักษา

องค์กรจะต้องไม่นำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยเพื่อวัตถุประสงค์อย่างอื่นนอกเหนือจากวัตถุประสงค์ของการเก็บรวบรวมข้อมูลนั้น เว้นแต่จะได้รับความยินยอมของบุคคลธรรมดาคนนั้นหรือเป็นไปตามที่กฎหมายกำหนด และข้อมูลส่วนบุคคลจะต้องถูกเก็บรักษาไว้ในระยะเวลาเพียงเท่าที่จำเป็นสำหรับการดำเนินการตามวัตถุประสงค์ดังกล่าวเท่านั้น หากมีการใช้ข้อมูลข่าวสารเพื่อวัตถุประสงค์ที่กำหนดขึ้นใหม่ต้องจัดเอกสารเกี่ยวกับวัตถุประสงค์ใหม่แจ้งแก่เจ้าของข้อมูล นอกจากนี้ในการจัดทำคู่มือตามหลักข้อ 4 ต้องกำหนดกระบวนการเกี่ยวกับการเก็บรักษาข้อมูลส่วนบุคคล และควรกำหนดระยะเวลาต่ำสุดและสูงสุดของการเก็บรักษาข้อมูลไว้ด้วย

<sup>27</sup> กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดา, โครงการจัดทำความเห็นทางวิชาการเพื่อจัดทำรายงานเกี่ยวกับหลักเกณฑ์และแนวทางการพิจารณาและดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และจัดทำคู่มือการปฏิบัติงานเกี่ยวกับข้อมูลส่วนบุคคลภาครัฐตาม พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 (รายงานผลการวิจัย) (น. 101). เล่มเดิม.

ภายใต้หลักการนี้ข้อมูลส่วนบุคคลที่ไม่ต้องตรงกับวัตถุประสงค์ที่ได้แจ้งหรือได้ใช้เสร็จสิ้นแล้วต้องถูกทำลาย ลบทิ้ง หรือทำให้ไม่ปรากฏชื่อของบุคคลนั้น (Anonymous) ทั้งนี้องค์กรจะต้องจัดทำคู่มือแนวทางปฏิบัติและกำหนดกระบวนการเกี่ยวกับการทำลายข้อมูลส่วนบุคคลดังกล่าวด้วย<sup>28</sup>

#### 6) หลักความถูกต้อง

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

องค์กรจะต้องไม่ปรับปรุงข้อมูลส่วนบุคคลโดยกระทำในลักษณะเป็นงานประจำ (Routinely Update) เว้นแต่กระบวนการเช่นนั้นมีความจำเป็นเพื่อสนองตอบต่อวัตถุประสงค์ของการเก็บรวบรวมข้อมูลนั้น

#### 7) หลักการรักษาความปลอดภัย

ข้อมูลส่วนบุคคลจะต้องได้รับการรักษาความปลอดภัยที่เหมาะสมกับข้อมูลส่วนบุคคล โดยเฉพาะการรักษาความปลอดภัยจะต้องให้ความคุ้มครองข้อมูลส่วนบุคคลต่อการสูญหายหรือการโจรกรรม ตลอดจนการเข้าตรวจดู การเปิดเผย การทำซ้ำ การใช้ หรือการแก้ไขเพิ่มเติมโดยไม่ได้รับอนุญาต ทั้งนี้ไม่ว่าข้อมูลนั้นจะอยู่ในรูปแบบใด ลักษณะของการรักษาความปลอดภัยจะแตกต่างกันไปขึ้นอยู่กับระดับความเป็นข้อมูลส่วนตัว โดยเฉพาะ รูปแบบและปริมาณข้อมูลที่เก็บรวบรวม ข้อมูลส่วนตัวโดยเฉพาะมากกว่าควรได้รับการรักษาความปลอดภัยโดยให้การคุ้มครองในระดับที่สูงกว่าข้อมูลธรรมดาหรือข้อมูลข่าวสารทั่วไป

มาตรการในการรักษาความปลอดภัยประกอบไปด้วยมาตรการคุ้มครองในทางกายภาพ (Physical Measure) เช่น การปิดล็อกตู้เอกสาร มาตรการที่เคร่งครัดในการเข้า-ออกสำนักงาน มาตรการการจัดระบบรักษาความปลอดภัยภายในองค์กร มาตรการจำกัดการเข้าตรวจดูข้อมูลตามหลักความจำเป็นที่ต้องรู้ (Need-to-Know Basis) และมาตรการทางเทคโนโลยี เช่น การใช้รหัสผ่าน (Passwords) และการใส่รหัส (Encryption) เพื่อป้องกันมิให้ผู้ไม่ได้รับอนุญาตสามารถเข้าตรวจดูข้อมูลนั้นได้ รวมถึงการฝึกอบรมและดำเนินการให้พนักงานลูกจ้างของตนตระหนักถึงความสำคัญ

<sup>28</sup> แหล่งเดิม.

ของการรักษาความลับของข้อมูลส่วนบุคคล และการจำกัดหรือทำลายข้อมูลส่วนบุคคลจะต้องกระทำด้วยความระมัดระวัง

#### 8) หลักการเปิดเผย

องค์กรต้องจัดทำนโยบายและแนวทางปฏิบัติขององค์กรในการจัดการข้อมูลส่วนบุคคล กล่าวคือ การจัดการวิธีการเข้าถึงข้อมูลหรือจัดข้อมูลที่ต้องเผยแพร่แก่ประชาชนในสถานที่และวิธีการที่เหมาะสม บุคคลทั่วไปจะต้องสามารถได้รับข้อมูลนั้นได้โดยไม่ลำบากและข้อมูลดังกล่าวจะต้องเปิดเผยในลักษณะที่สามารถเข้าใจได้โดยทั่วไป โดยข้อมูลที่เปิดเผยหรือเผยแพร่อย่างน้อยต้องประกอบไปด้วยรายการดังต่อไปนี้<sup>29</sup>

1. ชื่อ ตำแหน่งและที่อยู่ของบุคคลที่รับผิดชอบบนนโยบายและแนวทางปฏิบัติขององค์กรหรือผู้รับคำร้องหรือข้อซักถามต่าง ๆ
2. วิธีการเข้าตรวจสอบข้อมูลส่วนบุคคลที่อยู่ในความครอบครองขององค์กร
3. รายละเอียดเกี่ยวกับข้อมูล ประเภทของข้อมูล ตลอดจนรายละเอียดเกี่ยวกับการนำข้อมูลส่วนบุคคลนั้นไปใช้
4. สำเนาเอกสารแผ่นปลิว หรือข้อมูลอื่นใดเกี่ยวกับนโยบาย มาตรฐาน และประมวลจริยธรรม (Codes) ขององค์กร
5. ข้อมูลส่วนบุคคลที่จัดหาให้แก่องค์กรที่เกี่ยวข้อง หน่วยงานสาขาหรือบริษัทในเครือ

#### 9) หลักการเข้าตรวจสอบข้อมูลของบุคคล (Individual Access)

เมื่อมีการร้องขอ บุคคลผู้เป็นเจ้าของข้อมูลจะต้องได้รับการรายงานหรือเข้าตรวจสอบเกี่ยวกับการมีอยู่ (Existence) การใช้หรือการเปิดเผยข้อมูลส่วนบุคคลของตน นอกจากนี้ บุคคลสามารถโต้แย้งหากพบว่าข้อมูลดังกล่าวไม่ถูกต้องหรือสมบูรณ์ และมีสิทธิเรียกร้องให้มีการแก้ไขเพิ่มเติมข้อมูลนั้นได้ตามความเหมาะสม อย่างไรก็ตาม ในบางสถานการณ์อาจไม่สามารถที่จะให้บุคคลเข้าตรวจสอบข้อมูลส่วนบุคคลทั้งหมด แต่ข้อยกเว้นการเข้าตรวจสอบนั้นควรมีลักษณะจำกัดในกรณีที่องค์กรได้ปฏิเสธการเข้าขอตรวจสอบ องค์กรต้องแจ้งเหตุผลของการปฏิเสธนั้น การปฏิเสธอาจได้แก่กรณีที่การเข้าตรวจสอบข้อมูลต้องมีการเสียค่าใช้จ่ายในการจัดหาข้อมูลดังกล่าวสูงมากหรือในกรณีที่ข้อมูลนั้นมีข้อมูลที่เกี่ยวข้องกับบุคคลอื่นรวมอยู่ด้วย กรณีของข้อมูลซึ่งไม่สามารถเปิดเผยได้ด้วยเหตุผลทางกฎหมาย ด้านความปลอดภัย หรือทางการค้า

<sup>29</sup> การศึกษาและพัฒนาแนวทางการคุ้มครองข้อมูลส่วนบุคคลภายใต้ประชาคมอาเซียน (น. 31).  
เล่มเดิม.

เมื่อบุคคลผู้เป็นเจ้าของข้อมูลเข้าถึงข้อมูลข่าวสารของตน องค์กรต้องแจ้งให้บุคคลดังกล่าวทราบว่าองค์กรมีข้อมูลส่วนบุคคลของบุคคลนั้นอยู่ในความครอบครองหรือไม่ ซึ่งแจ้งถึงแหล่งที่มาของข้อมูลนั้น ในกรณีที่มีการขอเข้าถึงข้อมูลทางการแพทย์ซึ่งเป็นข้อมูลที่เป็นข้อมูลส่วนตัวโดยเฉพาะ องค์กรอาจเลือกที่จะเปิดเผยโดยผ่านแพทย์ก็ได้

ในการเปิดเผยข้อมูลข่าวสารที่สามารถเปิดเผยได้ องค์กรอาจต้องจัดทำบัญชีรายละเอียดเกี่ยวกับการนำข้อมูลไปเปิดเผย ลักษณะของการนำข้อมูลไปใช้และจัดทำบัญชีรายชื่อของบุคคลภายนอกที่จะสามารถเข้าถึงข้อมูลส่วนบุคคลดังกล่าวได้ ในการจัดทำบัญชีรายชื่อของบุคคลภายนอกดังกล่าวควรพยายามกำหนดประเภทของบุคคลภายนอกที่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ให้ชัดเจนมากที่สุดเท่าที่จะทำได้

ในการพิจารณาการเปิดเผยข้อมูลตามคำขอของผู้ร้อง องค์กรต้องตอบคำร้องขอภายในระยะเวลาที่เหมาะสม โดยที่ผู้ร้องขอไม่ต้องเสียค่าใช้จ่ายหรือเสียค่าใช้จ่ายน้อยที่สุด ข้อมูลที่ได้จัดให้มีการเข้าถึงได้ต้องจัดให้อยู่ในรูปแบบที่สามารถเข้าถึงและสามารถเข้าใจได้โดยทั่วไป ในกรณีที่องค์กรนั้นใช้อักษรย่อหรือรหัสในการบันทึกข้อมูลก็ต้องแนบคำอธิบายที่เกี่ยวข้องกับการใช้คำดังกล่าว

เมื่อบุคคลเห็นว่าข้อมูลข่าวสารของตนที่อยู่ในความครอบครองขององค์กรนั้น ๆ ไม่ถูกต้องหรือไม่สมบูรณ์และบุคคลได้โต้แย้งให้แก้ไขเปลี่ยนแปลง องค์กรจะต้องแก้ไขเพิ่มเติมข้อมูลดังกล่าวตามที่ร้องขอ ซึ่งอาจกระทำโดยการแก้ไข การตัดออก หรือการเพิ่มเติมข้อมูล แล้วแต่กรณี และหากข้อมูลดังกล่าวไม่ได้รับการแก้ไขให้เป็นที่พอใจตามคำโต้แย้ง ให้องค์กรบันทึกเรื่องที่ไม่น่าดำเนินการแก้ไขนั้นไว้

#### 10) หลักการโต้แย้งการปฏิบัติขององค์กร

บุคคลผู้เป็นเจ้าของข้อมูลสามารถทำคำโต้แย้งเกี่ยวกับการดำเนินการเกี่ยวกับข้อมูลข่าวสารที่เกี่ยวกับตน โดยการทำคำโต้แย้งไปยังบุคคลที่ได้รับแต่งตั้งให้เป็นผู้รับผิดชอบการปฏิบัติหน้าที่ขององค์กรได้

ในการทำคำร้องขอหรือคำโต้แย้ง องค์กรต้องจัดให้มีกระบวนการที่เหมาะสมในการรับคำร้อง ข้อโต้แย้ง หรือข้อซักถามเกี่ยวกับนโยบายและแนวทางปฏิบัติขององค์กรเกี่ยวกับการจัดการข้อมูลส่วนบุคคล ทั้งนี้ กระบวนการดังกล่าวต้องทำได้ไม่ยุ่งยากและไม่ซับซ้อน โดยองค์กรจะต้องแจ้งหรืออธิบายให้บุคคลทราบเกี่ยวกับกระบวนการร้องเรียน การรับคำร้อง และการตอบข้อซักถาม และต้องทำการสอบสวนเกี่ยวกับคำร้องทั้งหลาย และในกรณีที่คำร้องนั้นมี

เหตุอันสมควร องค์กรจะต้องมีการดำเนินการที่เหมาะสม รวมทั้งการแก้ไขเพิ่มเติม หรือมีมาตรการที่เหมาะสมเกี่ยวกับนโยบายและแนวทางปฏิบัติขององค์กรที่จำเป็น<sup>30</sup>

3.2.2 กฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลของประเทศระบบซีวิลลอว์ (Civil Law)

สำหรับในส่วนของกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลของประเทศระบบซีวิลลอว์ (Civil Law) ผู้เขียนได้ทำการศึกษาศึกษาการคุ้มครองข้อมูลส่วนบุคคลของประเทศอิตาลี การคุ้มครองข้อมูลส่วนบุคคลของประเทศฝรั่งเศสและการคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่น โดยมีรายละเอียดดังต่อไปนี้

### 3.2.2.1 การคุ้มครองข้อมูลส่วนบุคคลของประเทศอิตาลี

ประเทศอิตาลีมีรัฐบัญญัติคุ้มครองข้อมูลส่วนบุคคล หรือที่เรียกว่า Protection of Individuals and Other Subjects with Regard to the Processing of Personal Data Act no.675 of 31.12.1996 กฎหมายฉบับนี้ให้มีผลใช้บังคับเมื่อพ้นกำหนด 120 วัน นับแต่วันประกาศในราชกิจจานุเบกษา<sup>31</sup>

รัฐบัญญัติคุ้มครองข้อมูลส่วนบุคคลหรือที่เรียกว่า Protection of Individuals and Other Subjects with Regard to the Processing of Personal Data Act no.675 of 31.12.1996 เป็นกฎหมายที่มีเพื่ออนุวัติการให้เป็นไปตาม EU Directive (95/46EC)

รัฐบัญญัติฉบับนี้ได้มีการบัญญัติคำนิยามศัพท์ขึ้นมาเพื่อใช้เป็นคำศัพท์ที่มีความหมายเฉพาะและมีความแตกต่างไปจากคำนิยามศัพท์ทั่วไป โดยได้มีการบัญญัติไว้ในมาตรา 1 ว่าด้วยบทนิยามและความหมายของคำศัพท์ (Purposes and Definitions) โดยกำหนดว่ารัฐบัญญัติฉบับนี้มีขึ้นเพื่อให้เกิดความแน่ใจว่าการประมวลผลของข้อมูลส่วนบุคคลที่จะดำเนินการต้องเคารพสิทธิและเสรีภาพขั้นพื้นฐานและศักดิ์ศรีของบุคคล โดยเฉพาะอย่างยิ่งในเรื่องเกี่ยวกับความเป็นส่วนตัวและอัตลักษณ์ส่วนบุคคล อันจะก่อให้เกิดการคุ้มครองสิทธิของบุคคลตามกฎหมาย

<sup>30</sup> กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดา, โครงการจัดทำความเห็นทางวิชาการเพื่อจัดทำรายงานเกี่ยวกับหลักเกณฑ์และแนวทางการพิจารณาและดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และจัดทำคู่มือการปฏิบัติงานเกี่ยวกับข้อมูลส่วนบุคคลภาครัฐตาม พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 (รายงานผลการวิจัย) (น. 108). เล่มเดิม.

<sup>31</sup> การเปิดเผยข้อมูลส่วนบุคคลตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 (วิทยานิพนธ์ปริญญาโท) (น. 77). เล่มเดิม.

ตามรัฐธรรมนูญฉบับนี้ให้ความหมายของคำนิยามศัพท์ที่มีความหมายดังต่อไปนี้

“คลังข้อมูล (Data Bank)” หมายความว่า ชุดข้อมูลส่วนบุคคลซึ่งอาจจัดเก็บเป็นหน่วยเดียวหรือหลายหน่วย ไม่ว่าจะจัดเก็บอยู่ ณ สถานที่แห่งเดียวหรือหลายแห่ง โดยมีการจัดหมวดหมู่เพื่อวัตถุประสงค์อย่างใดอย่างหนึ่ง เช่น เพื่อประโยชน์ต่อการประมวลผล

“การประมวลผลข้อมูล (Processing)” หมายความว่า การดำเนินการใด ๆ ไม่ว่าจะกระทำโดยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอัตโนมัติหรือไม่ก็ตาม อันเกี่ยวกับการรวบรวมการบันทึกการจัดหมวดหมู่ การจัดเก็บ การให้รายละเอียดข้อมูล การเปลี่ยนแปลงแก้ไข การเลือกสรร การเรียกข้อมูลจากระบบ การเปรียบเทียบ การใช้ประโยชน์ การเชื่อมโยง การระงับใช้ชั่วคราว การเปิดเผยโดยเฉพาะเจาะจง การเปิดเผยโดยทั่วไป การลบข้อมูล และการทำลายข้อมูล

“ข้อมูลส่วนบุคคล (Personal Data)” หมายความว่า ข้อมูลที่มีความสัมพันธ์กับบุคคลธรรมดาหรือนิติบุคคล องค์กร สมาคม และสามารถระบุถึงบุคคลหรือหน่วยงานเหล่านั้นได้โดยตรงหรือโดยอ้อม เช่น การอ้างอิงข้อความอื่น ๆ กับหมายเลขบัตรสำคัญประจำตัว

“ผู้ควบคุมข้อมูล (Controller)” หมายความว่า บุคคลธรรมดา นิติบุคคล หน่วยงานของรัฐ องค์กร สมาคม หรือหน่วยงานอื่นใด ซึ่งมีหน้าที่ในการตัดสินใจเกี่ยวกับวัตถุประสงค์และวิธีการประมวลผลข้อมูลส่วนบุคคล

“ผู้ประมวลผลข้อมูล (Processor)” หมายความว่า บุคคลธรรมดา นิติบุคคล หน่วยงานของรัฐ องค์กร สมาคม หรือหน่วยงานอื่นใด ซึ่งมีหน้าที่ในการประมวลผลข้อมูลส่วนบุคคลในนามของผู้ควบคุมข้อมูล

“เจ้าของข้อมูล (Data Subject)” หมายถึง บุคคลธรรมดาหรือนิติบุคคล องค์กรหรือสมาคมซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล

“การเปิดเผยโดยเฉพาะเจาะจง (Communication)” หมายถึงการเปิดเผยข้อมูลส่วนบุคคลแก่บุคคลอื่นซึ่งระบุตัวไว้และไม่ได้เป็นเจ้าของข้อมูลไม่ว่าในรูปแบบใดก็ตาม รวมถึงการกระทำอื่นใดที่ทำให้บุคคลอื่นได้รับหรือสามารถค้นหาข้อมูลนั้นได้ด้วย

“การเปิดเผยโดยทั่วไป (Dissemination)” หมายถึงการเปิดเผยข้อมูลส่วนบุคคลให้แก่บุคคลอื่น ซึ่งไม่ได้ระบุตัวไว้ไม่ว่าในรูปแบบใดก็ตามรวมถึงการกระทำอื่นใดที่ทำให้บุคคลอื่นได้รับหรือสามารถค้นหาข้อมูลนั้นได้ด้วย

“ข้อมูลซึ่งไม่เปิดเผยชื่อ (Anonymous Data)” หมายถึงข้อมูลใด ๆ ซึ่งเป็นข้อมูลดิบหรือข้อมูลที่มีการประมวลผลแล้วซึ่งไม่สามารถระบุบุคคลผู้เป็นเจ้าของข้อมูลได้

“การระงับใช้ชั่วคราว (Blocking)” หมายถึงการจัดเก็บข้อมูลส่วนบุคคล โดยพักการประมวลผลไว้ชั่วคราว

“คณะกรรมการ (Garate)” หมายถึง หน่วยงานผู้ควบคุมดูแลซึ่งจัดตั้งขึ้นตามกฎหมายนี้ ในด้านการคุ้มครองสิทธิของเจ้าของข้อมูล กฎหมายฉบับนี้ทำให้สิทธิไว้หลายประการ โดยสามารถจำแนกเป็นหลักเกณฑ์ใหญ่ ๆ ดังนี้<sup>32</sup>

1) หลักความรับผิดชอบ

รัฐบัญญัติคุ้มครองข้อมูลส่วนบุคคล หรือที่เรียกว่า Protection of Individuals and Other Subjects with Regard to the Processing of Personal Data Act no.675 of 31.12.1996 กำหนดให้มีกลุ่มบุคคลขึ้นมาเพื่อทำหน้าที่ให้การคุ้มครองข้อมูลส่วนบุคคลที่เรียกว่า คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (Guarantee for the Protection of Personal Data)<sup>33</sup> คณะกรรมการประกอบด้วยกรรมการผู้ทรงคุณวุฒิจำนวน 4 คน โดยการคัดเลือกจาก Chamber of Deputies จำนวน 2 คน และจากการลงคะแนนเลือกของวุฒิสภาอีกจำนวน 2 คน ทั้งนี้กฎหมายกำหนดให้กรรมการผู้ได้รับเลือกทั้ง 4 คน ประชุมและเลือกกันเองให้คนหนึ่งเป็นประธานกรรมการ โดยประธานกรรมการ มีสิทธิออกเสียงชี้ขาดในกรณีที่การออกเสียงของกรรมการมีคะแนนเสียงเท่ากัน นอกจากนี้กฎหมายยังกำหนดให้ผู้ดำรงตำแหน่งกรรมการมีความเป็นอิสระ เป็นผู้ที่มีความรู้และประสบการณ์ ในด้านนิติศาสตร์หรือด้านคอมพิวเตอร์

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (Guarantee for the Protection of Personal Data) ทำหน้าที่กำกับดูแลและคุ้มครองข้อมูลส่วนบุคคลในการประมวลผลข้อมูลส่วนบุคคลตามที่กฎหมายกำหนดไว้ ทั้งนี้ คณะกรรมการดังกล่าวสามารถปฏิบัติหน้าที่ได้โดยอิสระ

อำนาจหน้าที่ของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (Guarantee for the Protection of Personal Data) ตามรัฐบัญญัติคุ้มครองข้อมูลส่วนบุคคล หรือ Protection of Individuals and Other Subjects with Regard to the Processing of Personal Data Act no.675 of 31.12.1996 เป็นไปตาม มาตรา 31<sup>34</sup> โดยแบ่งออกเป็นอำนาจหน้าที่ทั่วไป และอำนาจหน้าที่ต่อรัฐสภาและคณะรัฐมนตรี ดังนี้<sup>35</sup>

<sup>32</sup> การเปิดเผยข้อมูลส่วนบุคคลโดยธนาคารไทยพาณิชย์กับมาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคล (วิทยานิพนธ์ปริญญาโท) (น. 79-80). เล่มเดิม.

<sup>33</sup> Protection of Individuals and Other Subjects with Regard to the Processing of Personal Data Act no.675 of 31.12.1996, Article 30.

<sup>34</sup> Protection of Individuals and Other Subjects with Regard to the Processing of Personal Data Act no.675 of 31.12.1996, Article 31.

<sup>35</sup> มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลกับการประกันชีวิต (วิทยานิพนธ์ปริญญาโท) (น. 136). เล่มเดิม.

1. อำนาจหน้าที่ทั่วไป ได้แก่ จัดตั้งหน่วยงานเพื่อทำหน้าที่ในการรับจดทะเบียนการประกอบกรรมผลข้อมูล รับรายงานและคำร้องต่าง ๆ ให้คำแนะนำและให้ข้อมูลต่อสาธารณะ ออกประกาศกำหนดหลักเกณฑ์ต่าง ๆ ออกคำสั่งห้ามประมวลผลส่วนบุคคล ควบคุมและตรวจสอบการประมวลผลข้อมูลส่วนบุคคล เรียกบุคคลมาให้ข้อมูลหรือเอกสาร สอบสวนบุคคล

2. อำนาจหน้าที่ต่อรัฐสภาและคณะรัฐมนตรี ได้แก่ ให้คำปรึกษานายกรัฐมนตรีและรัฐมนตรีในการใช้อำนาจหรือมาตรการทางปกครองที่มีส่วนเกี่ยวข้องกับกฎหมายนี้ให้คำแนะนำ คณะรัฐมนตรีในการออกกฎหมายที่เกี่ยวข้อง จัดทำรายงานเสนอต่อรัฐสภาและคณะรัฐมนตรีปีละ 1 ครั้ง

### 2) หลักการแจ้งวัตถุประสงค์

กฎหมายกำหนดสิทธิให้เจ้าของข้อมูลและบุคคลใดก็ตามที่ได้รับการร้องขอให้เป็นผู้ให้ข้อมูลส่วนบุคคลจะต้องได้รับการแจ้งให้ทราบล่วงหน้าเกี่ยวกับรายการตามที่กฎหมายกำหนด ไม่ว่าโดยวาจาหรือลายลักษณ์อักษร เช่น วัตถุประสงค์และรูปแบบการประมวลผล การให้ข้อมูลนั้นเป็นหน้าที่หรือความสมัครใจและผลที่จะได้รับในกรณีที่ไม่ให้ข้อมูลส่วนบุคคลตามที่ร้องขอ บุคคล ประเภทของบุคคล หรือบริเวณที่อาจได้รับการเปิดเผยข้อมูลส่วนบุคคลนั้น สิทธิของเจ้าของข้อมูล ชื่อ ภูมิลำเนา สถานที่ทำการงานของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล เป็นต้น และในกรณีที่มิได้มีการรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลเองโดยตรง จะต้องแจ้งข้อความดังกล่าวให้แก่เจ้าของข้อมูลทราบทันทีที่ได้มีการบันทึกข้อมูลส่วนบุคคลนั้นหรือก่อนที่มีการเปิดเผยข้อมูลส่วนบุคคลนั้นเป็นครั้งแรก

### 3) หลักความยินยอม

การประมวลผลข้อมูลส่วนบุคคลโดยภาคเอกชนหรือภาครัฐที่มีวัตถุประสงค์เพื่อแสวงหากำไร ให้ถือว่าได้กระทำโดยชอบด้วยกฎหมายหากได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลโดยสมัครใจและเป็นลายลักษณ์อักษร และเจ้าของข้อมูลได้รับแจ้งข้อมูลที่จำเป็นตามที่กฎหมายกำหนดในขณะที่มีการรวบรวมข้อมูลส่วนบุคคลนั้นแล้ว ซึ่งเจ้าของข้อมูลจะให้ความยินยอมต่อกระบวนการทั้งหมดหรือเฉพาะบางส่วนของประมวลผลข้อมูลก็ได้

แม้ว่ากฎหมายจะกำหนดให้การประมวลผลข้อมูลส่วนบุคคลต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล แต่ก็ได้กำหนดข้อยกเว้นสำหรับบางกรณีที่ไม่ต้องได้รับความยินยอมจากเจ้าของข้อมูลไว้ด้วย เช่น ข้อมูลที่ต้องมีการรวบรวมและจัดเก็บตามที่กำหนดไว้ในกฎหมายอื่น การประมวลผลข้อมูลอันเกิดจากความผูกพันตามสัญญา กระบวนการประมวลผลข้อมูลของภาครัฐที่เปิดเผยต่อสาธารณะ การประมวลผลข้อมูลที่เกี่ยวข้องกับการวิจัยทางวิทยาศาสตร์ สถิติ การประมวลผลข้อมูลเกี่ยวกับกิจกรรมทางเศรษฐกิจ ซึ่งไม่กระทบต่อหลักการในการรักษาความลับทางธุรกิจหรือ

อุตสาหกรรม การประมวลผลข้อมูลที่เป็นต่อการคุ้มครองชีวิตของเจ้าของข้อมูลหรือบุคคลอื่น และเจ้าของข้อมูลไม่สามารถให้ความยินยอมได้เนื่องจากความพิการทางกายหรือเป็นบุคคลไร้ความสามารถหรือมีจิตฟั่นเฟือน การประมวลผลข้อมูลที่เป็นต่อการสืบสวนและสอบสวน<sup>36</sup>

กรณีเจ้าของข้อมูลได้รับความเสียหายอันเนื่องมาจากการประมวลผลข้อมูล กฎหมายกำหนดให้บุคคลใดก็ตามที่ทำให้ผู้อื่นได้รับความเสียหายอันเนื่องมาจากการประมวลผลข้อมูลต้องชดเชยค่าเสียหายตามหลักเกณฑ์ที่กำหนดไว้ในประมวลกฎหมายแพ่งและพาณิชย์ และยังกำหนดโทษทางอาญาเท่าที่จำเป็น และโทษปรับทางปกครอง ทั้งนี้ เพื่อให้กฎหมายมีความยืดหยุ่นและไม่เคร่งครัดมากเกินไป ซึ่งจากการศึกษากฎหมายต่างประเทศที่มีการบัญญัติโทษปรับทางปกครองพบว่า การกระทำความผิดที่เป็นพื้นฐานอันนำมาสู่การลงโทษปรับทางปกครองนั้นมักเป็นการกระทำที่ไม่ได้กระทบต่อความสงบเรียบร้อย แต่กระทบต่อความเป็นระเบียบของสังคม โดยมีฐานที่มาจาก การฝ่าฝืนคำสั่งทางปกครอง ทั้งนี้ เพื่อให้เจ้าหน้าที่สามารถดำเนินการลงโทษปรับได้เองและลดขั้นตอนกระบวนการพิจารณาของศาลอันทำให้คดีมีความรวดเร็วมากขึ้น

การประมวลผลข้อมูลส่วนบุคคลโดยภาคเอกชนหรือภาครัฐ ที่มีวัตถุประสงค์เพื่อแสวงหากำไร ให้ถือว่าได้กระทำโดยชอบด้วยกฎหมายหากได้รับความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลโดยสมัครใจและเป็นลายลักษณ์อักษร และเจ้าของข้อมูลได้รับแจ้งข้อมูลที่เป็นไปตามที่กฎหมายกำหนดในขณะที่มีการรวบรวมข้อมูลส่วนบุคคลนั้นแล้ว ซึ่งเจ้าของข้อมูลจะให้ความยินยอมต่อกระบวนการทั้งหมด หรือเฉพาะบางส่วนของ การประมวลผลข้อมูลก็ได้

แม้ว่ากฎหมายจะกำหนดให้ การประมวลผลข้อมูลส่วนบุคคลต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล แต่การให้ความยินยอมของเจ้าของข้อมูลส่วนบุคคลตามรัฐธรรมนูญคุ้มครองข้อมูลส่วนบุคคล หรือที่เรียกว่า Protection of Individuals and Other Subjects with Regard to the Processing of Personal Data Act no.675 of 31.12.1996 นี้มีข้อยกเว้นที่ไม่จำเป็นต้องได้รับความยินยอมจากเจ้าของข้อมูล 8 ประการ คือ

1. การประมวลผลข้อมูลซึ่งข้อมูลนั้นมีการเก็บรวบรวมและเก็บรักษาตามที่กำหนดไว้ในกฎหมาย กฎ ข้อบังคับ หรือข้อบัญญัติท้องถิ่น
2. การประมวลผลข้อมูลซึ่งจำเป็นต่อการปฏิบัติการชำระหนี้อันเป็นผลมาจากการที่เจ้าของข้อมูลเป็นคู่สัญญา

<sup>36</sup> จาก *มาตรการทางกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคล: ศึกษาเฉพาะกรณีการแยกแยะประเภทข้อมูลส่วนบุคคล* (วิทยานิพนธ์ปริญญาโท) (น. 1109), โดย สกต อติสรประเสริฐ, 2553, กรุงเทพฯ: มหาวิทยาลัยธุรกิจบัณฑิต.

3. การประมวลผลข้อมูลซึ่งเป็นข้อมูลที่นำมาจากทะเบียนสาธารณะ บัญชี เอกสาร หรือบันทึกต่าง ๆ ซึ่งสามารถเปิดเผยต่อสาธารณะได้

4. การประมวลผลข้อมูลที่เกี่ยวข้องกับการวิจัยทางวิทยาศาสตร์ หรือทางสถิติ และการปฏิบัติตามประมวลจริยธรรมของความประพฤติและวิชาชีพตามที่กฎหมายกำหนด

5. การประมวลผลข้อมูลที่กระทำภายในขอบเขตของวิชาชีพหนังสือพิมพ์

6. การประมวลผลข้อมูลที่เกี่ยวข้องกับกิจกรรมทางเศรษฐกิจซึ่งไม่กระทบต่อหลักเกณฑ์ในการรักษาความลับทางธุรกิจและอุตสาหกรรม

7. การประมวลผลข้อมูลที่ทำเป็นต่อการคุ้มครองชีวิตหรือร่างกายของเจ้าของข้อมูล หรือบุคคลอื่น และเจ้าของข้อมูลไม่สามารถให้ความยินยอมได้เนื่องจากความพิการทางกายหรือเป็นบุคคลไร้ความสามารถหรือมีจิตฟั่นเฟือน

8. การประมวลผลข้อมูลที่ทำเป็นต่อการสืบสวนและสอบสวน

4) หลักการเก็บรวบรวมข้อมูลอย่างจำกัด

การสิ้นสุดการประมวลผลข้อมูลส่วนบุคคล การประมวลผลข้อมูลสิ้นสุดลงเมื่อผู้ประมวลผลข้อมูลหยุดการประมวลผลข้อมูลไม่ว่าด้วยเหตุผลใดก็ตาม และผู้ควบคุมข้อมูลได้แจ้งให้คณะกรรมการทราบล่วงหน้าแล้ว ซึ่งผู้ควบคุมข้อมูลสามารถดำเนินการได้ ดังต่อไปนี้

1. ทำลายข้อมูลที่มีการประมวลผลแล้วนั้น

2. โอนข้อมูลนั้นให้แก่ผู้ควบคุมข้อมูลรายอื่นที่มีวัตถุประสงค์ของการประมวลผลข้อมูลในขณะที่มีการรวบรวมข้อมูลทำนองเดียวกัน

3. จัดเก็บข้อมูลนั้น โดยมีวัตถุประสงค์เพื่อใช้ส่วนตัวโดยไม่เปิดเผยข้อมูลนั้นไม่ว่าโดยทั่วไปหรือเฉพาะเจาะจง

4. จัดเก็บ หรือโอนข้อมูลให้แก่ผู้ควบคุมข้อมูลรายอื่นเพื่อวัตถุประสงค์ในการวิจัยทางประวัติศาสตร์ วิทยาศาสตร์ และสถิติ

อย่างไรก็ตาม การโอนข้อมูลให้แก่ผู้ควบคุมข้อมูลรายอื่นที่มีได้มีวัตถุประสงค์ของการประมวลผลข้อมูลในขณะที่มีการรวบรวมข้อมูลทำนองเดียวกัน หรือฝ่าฝืนบทบัญญัติอื่นที่เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล เป็นโมฆะ และต้องได้รับโทษตามที่กฎหมายกำหนดไว้ด้วย

การชดใช้ค่าเสียหายอันเนื่องมาจากการประมวลผลข้อมูล: กฎหมายกำหนดให้บุคคลใดก็ตามที่ทำให้ผู้อื่นได้รับความเสียหายอันเนื่องมาจากการประมวลผลข้อมูลต้องชดใช้ค่าเสียหายตามหลักเกณฑ์ที่กำหนดไว้ในประมวลกฎหมายแพ่งและพาณิชย์

#### 5) หลักการจำกัดการใช้ การเปิดเผย และการเก็บรักษา

จะต้องไม่นำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยเพื่อวัตถุประสงค์อย่างอื่น นอกเหนือจากวัตถุประสงค์ของการเก็บรวบรวมข้อมูลนั้น และข้อมูลส่วนบุคคลจะต้องถูกเก็บรักษาไว้ในระยะเวลาเพียงเท่าที่จำเป็นสำหรับการดำเนินการตามวัตถุประสงค์ดังกล่าวเท่านั้น ข้อมูลส่วนบุคคลที่ไม่ต้องตรงกับวัตถุประสงค์ที่ได้แจ้งหรือได้ใช้เสร็จสิ้นแล้วต้องถูกทำลาย ลบทิ้ง หรือทำให้ไม่ปรากฏชื่อของบุคคลนั้น (Anonymous)

การสิ้นสุดการประมวลผลข้อมูลส่วนบุคคล การประมวลผลข้อมูลสิ้นสุดลงเมื่อผู้ประมวลผลข้อมูลหยุดการประมวลผลข้อมูลไม่ว่าด้วยเหตุผลใดก็ตาม และผู้ควบคุมข้อมูลได้แจ้งให้คณะกรรมการทราบล่วงหน้าแล้ว ซึ่งผู้ควบคุมข้อมูลสามารถดำเนินการได้ ดังต่อไปนี้

1. ทำลายข้อมูลที่มีการประมวลผลแล้วนั้น
2. โอนข้อมูลนั้นให้แก่ผู้ควบคุมข้อมูลรายอื่นที่มีวัตถุประสงค์ของการประมวลผลข้อมูลในขณะที่มีการรวบรวมข้อมูลทำนองเดียวกัน
3. จัดเก็บข้อมูลนั้นโดยมีวัตถุประสงค์เพื่อใช้ส่วนตัวโดยไม่เปิดเผยข้อมูลนั้นไม่ว่าโดยทั่วไปหรือเฉพาะเจาะจง
4. จัดเก็บ หรือโอนข้อมูลให้แก่ผู้ควบคุมข้อมูลรายอื่นเพื่อวัตถุประสงค์ในการวิจัยทางประวัติศาสตร์ วิทยาศาสตร์ และสถิติ

#### 6) หลักความถูกต้อง

รูปแบบของการรวบรวมและคุณภาพของข้อมูลส่วนบุคคล: กฎหมายกำหนดให้ข้อมูลส่วนบุคคลที่จะมีการประมวลผลนั้นจะต้องมีการประมวลผลโดยชอบด้วยกฎหมายและเป็นธรรม มีการรวบรวมและบันทึกตามวัตถุประสงค์ที่ได้ระบุไว้โดยชัดแจ้งหรือที่กำหนดขึ้นเป็นพิเศษและชอบด้วยกฎหมาย ข้อมูลนั้นจะต้องมีความถูกต้องและได้มีการปรับแก้ให้ถูกต้องอยู่เสมอ และที่สำคัญคือ จะต้องดำเนินการประมวลผลข้อมูลส่วนบุคคลเพียงเท่าที่เหมาะสมและไม่เกินกรอบวัตถุประสงค์ของการรวบรวมและประมวลผลข้อมูลนั้น นอกจากนี้จะต้องมีการกำหนดระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคลดังกล่าวไว้ด้วย

#### 7) หลักการรักษาความปลอดภัย

การประมวลผลข้อมูลส่วนบุคคล สิ่งสำคัญประการหนึ่งที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศอิตาลีกำหนดไว้ คือ ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลจะต้องดำเนินการจัดเก็บและควบคุมข้อมูลส่วนบุคคลที่มีการประมวลผล โดยคำนึงถึงวัฒนธรรมทางเทคโนโลยีและลักษณะเฉพาะในการประมวลผลข้อมูลนั้น ๆ รวมถึงมาตรการความปลอดภัยที่เหมาะสม เพื่อป้องกันการทำลายข้อมูลหรือทำให้ข้อมูลเสียหาย การเข้าถึงข้อมูลโดยปราศจาก

อำนาจ หรือการนำมาสู่การประมวลผลที่ไม่ชอบด้วยกฎหมายหรือไม่เป็นไปตามวัตถุประสงค์ที่กำหนดขึ้นในขณะที่มีการรวบรวมข้อมูล นอกจากนี้ กฎหมายยังบังคับให้มีการกำหนดมาตรฐานขั้นต่ำสำหรับใช้เป็นมาตรฐานความปลอดภัยของข้อมูลส่วนบุคคลโดยจะต้องกำหนดให้มีขึ้นภายใน 180 วันนับจากวันที่พระราชบัญญัตินี้มีใช้บังคับ และจะต้องปรับปรุงมาตรฐานความปลอดภัยดังกล่าวให้มีความทันสมัยตามความก้าวหน้าทางเทคโนโลยีอย่างน้อยทุก ๆ 2 ปี<sup>37</sup>

#### 8) หลักการเปิดเผย

กฎหมายกำหนดหลักการเกี่ยวกับการเปิดเผยข้อมูลส่วนบุคคลไว้ว่า บุคคลหรือหน่วยงานภาคเอกชนหรือภาครัฐที่แสวงหากำไรเปิดเผยข้อมูลส่วนบุคคลไม่ว่าโดยทั่วไปหรือโดยเฉพาะเจาะจงได้ก็ต่อเมื่อได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล

อย่างไรก็ตาม ก็ได้กำหนดข้อยกเว้นของการเปิดเผยข้อมูลส่วนบุคคลไม่ว่าโดยทั่วไปหรือโดยเฉพาะเจาะจงไว้หลายประการ ดังนี้

1. เป็นการเปิดเผยข้อมูลตามปกติภายในวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลนั้น
2. เป็นข้อมูลที่นำมาจากเอกสารมหาชน การลงทะเบียน เอกสารหรือบันทึกใด ๆ ซึ่งมีอยู่ทั่วไป โดยไม่ฝ่าฝืนบทบัญญัติแห่งกฎหมาย
3. เป็นการเปิดเผยตามบทบัญญัติกฎหมาย
4. เป็นการเปิดเผยภายในขอบเขตวิชาชีพหนังสือพิมพ์ โดยไม่ฝ่าฝืนบทบัญญัติว่าเสรีภาพสิ่งพิมพ์ หรือมีผลกระทบต่อการใช้ความคุ้มครองความเป็นส่วนตัวหรือประโยชน์สาธารณะ
5. ฝ่าฝืนกฎหมายว่าด้วยธุรกิจและอุตสาหกรรม
6. เป็นการจำเป็นหรือเพื่อป้องกันหรือระงับอันตรายต่อชีวิตหรือสุขภาพของเจ้าของข้อมูลหรือบุคคลอื่น ในกรณีที่เจ้าของข้อมูลไม่สามารถให้ความยินยอมได้ อันเนื่องมาจากเป็นบุคคลไร้ความสามารถ การพิการ หรือจิตฟั่นเฟือน
7. เป็นการจำเป็นเพื่อการสืบสวน สอบสวน หรือฟ้องร้องคดี ตามประมวลกฎหมายวิธีพิจารณาความอาญา
8. เป็นไปตามวัตถุประสงค์ของการรวบรวมข้อมูลภายในกลุ่มธนาคารด้วยกันตามกฎหมายว่าด้วยการเงินการธนาคารหรือระหว่างกลุ่มบริษัทตามประมวลกฎหมายแพ่งและพาณิชย์

<sup>37</sup> Protection of Individuals and Other Subjects with Regard to the Processing of Personal Data Act no.675 of 31.12.1996 Article 15. (อ้างถึงใน *มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลกับการประกันชีวิต* (วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ) (น. 138). เล่มเดิม).

นอกจากนี้ กฎหมายยังได้กำหนดข้อยกเว้นอีกประการหนึ่งเฉพาะกรณีการเปิดเผยข้อมูล โดยเฉพาะเจาะจง คือ ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลสามารถเปิดเผยข้อมูลส่วนบุคคลให้แก่บุคคลที่ดำเนินการประมวลผลข้อมูลนั้นภายใต้บังคับบัญชาของผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลโดยตรงได้<sup>38</sup>

9) หลักการเข้าตรวจดูข้อมูลของบุคคล

การประมวลผลข้อมูลส่วนบุคคล เจ้าของข้อมูลมีสิทธิ ดังต่อไปนี้

1. มีสิทธิที่จะได้รับแจ้งเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลและมีสิทธิที่จะเข้าถึงข้อมูลโดยไม่ต้องเสียค่าใช้จ่าย

2. มีสิทธิที่ได้รับแจ้งเกี่ยวกับชื่อ ภูมิลำเนา สถานที่ทำงานของผู้ควบคุมดูแลข้อมูลและผู้ประมวลผลข้อมูลและการเปิดเผยข้อมูลไม่ว่าโดยทั่วไปหรือโดยเฉพาะเจาะจง

นอกจากนี้ ยังมีสิทธิที่จะได้รับทราบข้อมูล หรือให้ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลดำเนินการโดยไม่ชักช้าในกรณีต่อไปนี้

(1) ยืนยันเกี่ยวกับข้อมูลส่วนบุคคลของตน และวัตถุประสงค์ในการประมวลผลข้อมูลนั้น

(2) ลบ ระงับการใช้ชั่วคราว หรือแปลงข้อมูลให้อยู่ในรูปแบบที่ไม่เปิดเผยตัวบุคคล ผู้เป็นเจ้าของข้อมูล ในกรณีที่มีการประมวลผลโดยมิชอบหรือฝ่าฝืนบทบัญญัติของกฎหมายหรือกรณีที่มีการจัดเก็บข้อมูลไว้เกินความจำเป็น

(3) ตรวจสอบและแก้ไขข้อมูลให้ถูกต้องอยู่เสมอ

(4) แจ้งการดำเนินการตาม (2) และ (3) ไปยังบุคคลที่ได้มีการเปิดเผยข้อมูลให้ทราบ เว้นแต่การดำเนินการนั้นจะกระทบถึงประโยชน์ได้เสียของบุคคลผู้เป็นเจ้าของข้อมูลโดยตรง

10) หลักการโต้แย้งการปฏิบัติขององค์กร

เจ้าของข้อมูลมีสิทธิที่จะโต้แย้งคัดค้านเมื่อเห็นว่าข้อมูลของตนไม่ถูกต้อง ทั้งนี้เจ้าของข้อมูลมีสิทธิยื่นคำร้องคัดค้านต่อคณะกรรมการได้ด้วยหรือโต้แย้งคัดค้านการประมวลผลข้อมูลทั้งหมดหรือบางส่วนแม้ว่าจะดำเนินการประมวลผลข้อมูลนั้นโดยชอบด้วยกฎหมาย อย่างไรก็ตาม การใช้สิทธิดังกล่าวของเจ้าของข้อมูลก็มีข้อจำกัดในบางกรณี เช่น กรณีที่มีการประมวลผล ข้อมูลเกี่ยวกับการเงิน หรือการชำระหนี้สำหรับหน่วยงานของรัฐซึ่งมีวัตถุประสงค์เพื่อแสวงหากำไร

<sup>38</sup> Protection of Individuals and Other Subjects with Regard to the Processing of Personal Data Act no.675 of 31.12.1996 Article 19. (อ้างถึงใน *มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลกับการประกันชีวิต* (วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ) (น. 139). เล่มเดิม).

การกำกับดูแลบริษัทหลักทรัพย์และเครดิตฟองซิเออร์ ตามที่กำหนดไว้ในกฎหมายอื่นที่บัญญัติขึ้นเป็นพิเศษ การสืบสวนสอบสวน เป็นต้น

### 3.2.2.2 การคุ้มครองข้อมูลส่วนบุคคลของประเทศฝรั่งเศส

ประเทศฝรั่งเศสเป็นประเทศหนึ่งที่ทำให้ความสำคัญกับสิทธิในการมีชีวิตส่วนตัวและสิทธิในการที่จะได้รับความเคารพในชีวิตส่วนตัวและชีวิตครอบครัวของประชาชน การให้ความสำคัญกับสิทธิความเป็นส่วนตัวของประเทศฝรั่งเศสนี้ได้รับอิทธิพลมาจากอนุสัญญาสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานยุโรป<sup>39</sup> โดยเฉพาะอย่างยิ่งมาตรา 8 ของอนุสัญญาสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานยุโรป<sup>39</sup> ที่ให้ความสำคัญคุ้มครองในข้อมูลส่วนบุคคลไม่ให้ถูกละเมิดได้ แม้ว่าจะเป็นการกระทำของเจ้าหน้าที่ของรัฐหรือของฝ่ายปกครองก็ตามที่ โดยระบุว่า หากฝ่ายปกครองหรือหน่วยงานของรัฐจะเข้าไปแทรกแซงในการใช้สิทธิดังกล่าว การแทรกแซงต้องได้รับการบัญญัติไว้ในรัฐบัญญัติ และการแทรกแซงจะต้องเป็นมาตรการที่จำเป็นต่อความความปลอดภัยของประเทศ (sécurité nationale) ต่อความมั่นคง (sûreté publique) ต่อความปลอดภัยทางเศรษฐกิจของประเทศ (bien-être économique du 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)<sup>40</sup>

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศฝรั่งเศส ได้แก่ รัฐบัญญัติที่ 78-17 ลงวันที่ 6 มกราคม ค.ศ. 1978 ว่าด้วยข้อมูลสารสนเทศ เพิ่มข้อมูลและเสรีภาพ (Loi relative à l'informatique, aux fichiers et aux libertés หรือ The Act on Data Processing Data Files and Individual Liberties)<sup>41</sup> โดยรัฐบัญญัติที่ 78-17 ลงวันที่ 6 มกราคม ค.ศ. 1978 ว่าด้วยข้อมูลสารสนเทศ เพิ่มข้อมูลและเสรีภาพ ได้ให้ความหมายของข้อมูลส่วนบุคคล ว่าหมายถึงข้อมูลทั้งหลายที่เกี่ยวข้องกับบุคคลธรรมดาที่ระบุตัวบุคคลนั้นหรือสามารถระบุตัวบุคคลได้ไม่ว่า

<sup>39</sup> pub-law.net. (2547). *คดีการดักฟังโทรศัพท์และสิทธิในการมีชีวิตส่วนตัว* โดยนางสาวพิมพ์ดาว จันทร์ขันธ์. สืบค้น 31 ตุลาคม 2558, จาก <http://www.pub-law.net/publaw/view.aspx?id=560>

<sup>40</sup> แหล่งเดิม

<sup>41</sup> *กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดา*, โครงการจัดทำความเห็นทางวิชาการเพื่อจัดทำรายงานเกี่ยวกับหลักเกณฑ์และแนวทางการพิจารณาและดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และจัดทำคู่มือการปฏิบัติงานเกี่ยวกับข้อมูลส่วนบุคคลภาครัฐตาม พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 (รายงานผลการวิจัย) (น. 27-36). เล่มเดิม.

โดยทางตรงหรือทางอ้อมโดยการอ้างอิงถึงเลขประจำตัวหรือลักษณะอย่างหนึ่งอย่างใดที่เป็นลักษณะเฉพาะของบุคคลนั้น<sup>42</sup>

สมศักดิ์ นวตระกูลพิสุทธิ์ ได้อธิบายกฎหมายฉบับนี้ว่าประกอบไปด้วยสาระสำคัญ 3 ประการ<sup>43</sup> ดังนี้

ประการที่ 1 กฎหมายฉบับนี้ได้กำหนดให้มีองค์กรรับผิดชอบ เรียกว่า คณะกรรมการข้อมูลข่าวสารและเสรีภาพแห่งชาติ (National Commission for Data Processing and Licensing หรือ Commission nationale de l'informatique et des libertés : CNIL) เป็นองค์กรอิสระซึ่งให้คำแนะนำเกี่ยวกับการวางแผนและรับรองการประมวลผลข้อมูลข่าวสารของหน่วยงานหรือองค์กรต่าง ๆ คณะกรรมาธิการมีอำนาจหน้าที่ในการแนะนำให้ความรู้เกี่ยวกับบทบัญญัติกฎหมายนี้ในสิทธิและหน้าที่ของบุคคล รวมถึงการตรวจสอบดูแลผู้ประกอบการทางธุรกิจในการดำเนินการประมวลผลข้อมูลส่วนบุคคล นอกจากนี้คณะกรรมาธิการต้องมีการจัดทำเอกสารเกี่ยวกับการประมวลผลข้อมูลข่าวสารในกิจกรรมต่าง ๆ เพื่อเผยแพร่ และจัดทำรายงานประจำปีเพื่อเสนอต่อนายกรัฐมนตรีและต่อรัฐสภา

คณะกรรมการว่าด้วยข้อมูลข่าวสารและเสรีภาพแห่งชาติ (La commission nationale de l'informatique et des libertés หรือ CNIL) เป็นกรรมการอิสระไม่อยู่ใต้อำนาจขององค์กรใด โดยองค์กรนี้ประกอบไปด้วยกรรมการ 17 คนมีวาระการดำรงตำแหน่ง 5 ปี โดยมีกรรมการ 2 คนมาจากสมาชิกสภาผู้แทนราษฎร กรรมการ 2 คนมาจากสมาชิกวุฒิสภา กรรมการ 2 คนมาจากสภาเศรษฐกิจและสังคม กรรมการ 2 คนมาจากศาลปกครองสูงสุด กรรมการ 2 คนมาจากศาลฎีกา กรรมการ 2 คนมาจากศาลการคลังและภาษี กรรมการผู้ทรงคุณวุฒิ 2 คน มาจากการแต่งตั้งโดยกฤษฎีกาจากการเสนอของประธานวุฒิสภาและประธานสภาผู้แทนราษฎรและกรรมการอีก 3 คน มาจากการแต่งตั้งโดยกฤษฎีกาของที่ประชุมคณะรัฐมนตรี<sup>44</sup>

<sup>42</sup> ปัญหาและมาตรการทางกฎหมายในการรับรองและคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว (Right to privacy) (รายงานผลการวิจัย) (น. 35). เล่มเดิม.

<sup>43</sup> กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดา, โครงการจัดทำความเห็นทางวิชาการเพื่อจัดทำรายงานเกี่ยวกับหลักเกณฑ์และแนวทางการพิจารณาและดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และจัดทำคู่มือการปฏิบัติงานเกี่ยวกับข้อมูลส่วนบุคคลภาครัฐตาม พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 (รายงานผลการวิจัย).

<sup>44</sup> เกรียงไกร เจริญธนาวัฒน์. (2548). *รวมบทความกฎหมายมหาชน*, จาก [www.pub-law.net](http://www.pub-law.net) เล่ม 4. (น. 324).

ประการที่ 2 กฎหมายนี้กำหนดให้มีหลักประกันในการคุ้มครอง (Preventive guarantees) เพื่อรับรองว่าระบบการประมวลผลข้อมูลข่าวสารได้ปฏิบัติตามแนวทางที่กำหนด

ประการที่ 3 กฎหมายนี้ได้ให้สิทธิในการเข้าถึงข้อมูลข่าวสารและสิทธิในการโต้แย้งหรือเรียกร้องให้มีการแก้ไขเปลี่ยนแปลงข้อมูลส่วนบุคคล

บทบัญญัตินี้อยู่บนพื้นฐานว่าระบบการประมวลผลข้อมูลข่าวสารจะต้องไม่ก่อให้เกิดความเสียหายต่อความเป็นส่วนตัวของบุคคล (Human identity) สิทธิความเป็นส่วนตัว (Privacy) เสรีภาพส่วนบุคคลหรือสาธารณะ (Individual or Public liberties)<sup>45</sup> และบุคคลมีสิทธิที่จะรับทราบและโต้แย้งข้อมูลต่าง ๆ และเหตุผลที่ใช้ในระบบประมวลผลข้อมูลข่าวสารแบบอัตโนมัติที่มีผลเป็นการโต้แย้งบุคคลนั้น

กฎหมายได้กำหนดวิธีปฏิบัติเกี่ยวกับการเก็บรวบรวม การบันทึกและการเก็บรักษาข้อมูลที่ระบุชื่อ โดยกฎหมายนี้ใช้บังคับทั้งในระบบการประมวลผลแบบอัตโนมัติและวิธีการประมวลผลด้วยวิธีธรรมดา ตลอดจนควบคุมเนื้อหาของข้อมูลในระบบ การใช้ประโยชน์ข้อมูล การแก้ไขเปลี่ยนแปลง การลบ การเพิ่มข้อมูล การโอนหรือการทำลายข้อมูลดังกล่าว ทั้งในภาคเอกชนและภาครัฐ

รัฐบัญญัติที่ 78-17 ลงวันที่ 6 มกราคม ค.ศ. 1978 ว่าด้วยข้อมูลสารสนเทศ แฟ้มข้อมูล และเสรีภาพ มีกรอบของการใช้รัฐบัญญัติฉบับดังกล่าวโดยได้มีการกำหนดไว้ในมาตรา 4 ที่กำหนดว่า รัฐบัญญัติฉบับนี้จะไม่อาจใช้บังคับได้หากว่าเป็นข้อมูลสารสนเทศที่เกี่ยวกับข้อมูลส่วนบุคคลซึ่งจัดทำขึ้นเพื่อประโยชน์ของรัฐและเกี่ยวข้องกับประโยชน์สาธารณะ เช่น ความมั่นคงแห่งรัฐ การป้องกันประเทศ หรือความปลอดภัยของประชาชน การป้องกัน การค้นหา การพบหรือการติดตามการกระทำ ความผิดอาญา การจัดทำระบบข้อมูลสารสนเทศในกรณีต่าง ๆ เหล่านี้จะต้องมีการตราเป็นกฎหมายหรือกฎระเบียบของรัฐมนตรีที่มีอำนาจหน้าที่ที่เกี่ยวข้องแก่การนั้นเป็นการเฉพาะ<sup>46</sup>

นอกจากนี้ กฎหมายได้กำหนดบทนิยามของคำว่า “ระบบข้อมูลสารสนเทศแบบอัตโนมัติที่เกี่ยวกับข้อมูลที่ระบุชื่อ” ไว้ว่า หมายถึง การดำเนินการในทุกขั้นตอนโดยระบบอัตโนมัติที่เกี่ยวกับการเก็บรวบรวม การบันทึก การจัดทำ การแก้ไข การเก็บรักษาและการทำลายข้อมูลที่ระบุชื่อ ตลอดจนการดำเนินการทั้งหลายที่เกี่ยวข้องกับการใช้ประโยชน์ซึ่งแฟ้มข้อมูลหรือ

<sup>45</sup> CNIL. สืบค้น 31 ตุลาคม 2558, จาก <http://www.cnil.fr/index.php?id=4>

<sup>46</sup> Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés Article 26-27 (อ้างถึงใน ปัญหาและมาตรการทางกฎหมายในการรับรองและคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว (Right to privacy) (รายงานผลการวิจัย) (น. 35). เล่มเดิม).

ฐานข้อมูล และโดยเฉพาะอย่างยิ่งการเชื่อมต่อเครือข่ายหรือการส่งถึงกัน การตรวจดูหรือการเปิดเผยข้อมูลที่ระบุชื่อ ทั้งนี้กฎหมายนี้มีขอบเขตครอบคลุมระบบข้อมูลข่าวสารทั้งในภาครัฐ และภาคเอกชน อย่างไรก็ตามกฎหมายได้กำหนดมาตรการในการควบคุมสำหรับข้อมูลในภาครัฐและภาคเอกชนไว้แตกต่างกัน

ระบบข้อมูลข่าวสารในภาครัฐ ได้แก่ ระบบข้อมูลข่าวสารที่ดำเนินการเพื่อประโยชน์ของรัฐ องค์กรมหาชน องค์กรปกครองส่วนท้องถิ่น หรือนิติบุคคลตามกฎหมายเอกชนที่จัดทำบริการสาธารณะ<sup>47</sup> ส่วนข้อมูลข่าวสารอื่นที่นอกเหนือไปจากข้อมูลข่าวสารที่ใช้ในองค์กรเหล่านี้ถือว่าเป็นระบบข้อมูลข่าวสารในภาคเอกชน

บทบัญญัติของประเทศฝรั่งเศสก็เช่นเดียวกับประเทศอื่น ๆ ในเรื่องของการจำกัดการเก็บข้อมูลประเภทที่เป็นข้อมูลส่วนตัวโดยเฉพาะ (Sensitive Data) เช่น ข้อมูลที่แสดงให้เห็นถึงชาติกำเนิด หรือความคิดเห็นทางการเมือง ทางปรัชญา หรือทางศาสนา หรือการเป็นสมาชิกสหพันธ์ อย่างไรก็ตามในข้อยกเว้นในข้อจำกัดนี้ เช่น กรณีข้อมูลที่เกี่ยวข้องกับการกระทำความผิด การถูกลงโทษ หรือการถูกกักกัน จะถูกจัดเก็บได้เฉพาะศาลและฝ่ายปกครองที่มีอำนาจ ตลอดจนนิติบุคคลที่จัดทำบริการสาธารณะในกรณีที่ได้รับความเห็นชอบจากคณะกรรมการว่าด้วยข้อมูลข่าวสารและเสรีภาพแห่งชาติ (La commission nationale de l'informatique et des libertés หรือ CNIL) เท่านั้น หรือองค์กรบางแห่ง ได้แก่ องค์กรทางศาสนาหรือกลุ่มกิจกรรมทางศาสนา ปรัชญา การเมือง หรือสหพันธ์ สามารถเก็บข้อมูลเกี่ยวกับสมาชิกของตนหรือบุคคลที่เกี่ยวข้องได้นอกจากนี้ หน่วยงานอื่นอาจดำเนินการดังกล่าวได้ด้วยเหตุผลเพื่อประโยชน์สาธารณะ ทั้งนี้โดยตราเป็นรัฐกฤษฎีกาที่ผ่านความเห็นชอบของสภาที่ปรึกษาแห่งรัฐ ตามคำเสนอหรือความเห็นชอบของคณะกรรมการว่าด้วยข้อมูลข่าวสารและเสรีภาพแห่งชาติ<sup>48</sup>

กฎหมายนี้กำหนดให้องค์กรผู้จัดทำระบบข้อมูลข่าวสารต้องมีหน้าที่ ดังนี้

1) การจัดทำระบบการประมวลข้อมูลข่าวสารโดยวิธีอัตโนมัติในภาครัฐ

การดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลจะต้องได้รับอนุญาตตามกฎหมาย ซึ่งเป็นไปตามกฎระเบียบที่ออกตามความเห็นของ CNIL โดยกฎระเบียบที่ออกเพื่อการจัดระบบข้อมูลข่าวสารต้องปรากฏรายละเอียดต่อไปนี้

<sup>47</sup> แหล่งเดิม.

<sup>48</sup> นันทวัฒน์ บรมานันท์. (2553). รวมบทความกฎหมายมหาชน. จาก [www.pub-law.net](http://www.pub-law.net). เล่ม 9 (น. 486).

1. ชื่อและวัตถุประสงค์ของการจัดทำข้อมูลข่าวสาร
2. หน่วยงานหรือบุคคลใดที่บุคคลผู้เป็นเจ้าของข้อมูลที่ระบุชื่อสามารถใช้สิทธิเข้าตรวจสอบข้อมูลตามที่กำหนดในกฎหมาย
3. ประเภทของข้อมูลที่ระบุชื่อที่บันทึกได้ ตลอดจนผู้ที่สามารถเข้าถึงหรือสามารถได้รับข้อมูลนั้น หรือประเภทของผู้ที่ได้รับข้อมูลนั้นที่สามารถตรวจสอบข้อมูลนั้นได้
- 2) การจัดทำระบบการประมวลผลข้อมูลข่าวสารโดยวิธีอัตโนมัติภาคเอกชน  
องค์กรเอกชนจะต้องยื่นคำขอต่อคณะกรรมการข้อมูลสารสนเทศและเสรีภาพแห่งชาติล่วงหน้าก่อนการดำเนินการ ทั้งนี้คำขอดังกล่าวถือเป็นข้อผูกพันขององค์กรว่า การจัดทำระบบข้อมูลข่าวสารจะต้องเป็นไปตามเงื่อนไขต่าง ๆ ที่กฎหมายกำหนด และจะต้องได้รับอนุญาตจาก CNIL ก่อนจึงจะดำเนินการได้ ในการทำคำขอจัดทำระบบข้อมูลข่าวสารต่อ CNIL ต้องปรากฏรายการ ดังนี้<sup>49</sup>
  1. ผู้ดำเนินการหรือผู้ควบคุมแฟ้มข้อมูลข่าวสารบุคคล (File controller) หรือบุคคลที่มีอำนาจตัดสินใจจัดทำระบบข้อมูลหรือตัวแทนของบุคคลดังกล่าวในประเทศฝรั่งเศส ในกรณีที่บุคคลนั้นอาศัยอยู่ในต่างประเทศ
  2. ลักษณะ วัตถุประสงค์ และชื่อของระบบข้อมูล
  3. หน่วยงานที่รับผิดชอบในการดำเนินการจัดทำระบบข้อมูลข่าวสาร
  4. หน่วยงานภายในที่บุคคลสามารถใช้สิทธิเข้าตรวจสอบข้อมูล ตลอดจนมาตรการต่าง ๆ ที่กำหนดเพื่ออำนวยความสะดวกแก่การใช้สิทธิดังกล่าว
  5. ประเภทของบุคคลที่สามารถเข้าถึงข้อมูลที่บันทึกได้โดยตรง ทั้งนี้ตามอำนาจหน้าที่ของบุคคลนั้น หรือตามความจำเป็นของหน่วยงานภายใน
  6. การดำเนินงานเกี่ยวกับข้อมูลที่ระบุชื่อ ที่มาของข้อมูล ระยะเวลาของการเก็บรักษา มาตรการในการรักษาความปลอดภัย ตลอดจนผู้ได้รับข้อมูลนั้น หรือประเภทของผู้ได้รับข้อมูลนั้น ที่จะสามารถตรวจสอบข้อมูลนั้นได้
  7. การส่งข้อมูลถึงกัน การเชื่อมโยงเครือข่าย หรือการเชื่อมโยงข้อมูลในรูปแบบอื่นใด ตลอดจนการโอนข้อมูลแก่บุคคลภายนอก

<sup>49</sup> กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดา, โครงการจัดทำความเห็นทางวิชาการเพื่อจัดทำรายงานเกี่ยวกับหลักเกณฑ์และแนวทางการพิจารณาและดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และจัดทำคู่มือการปฏิบัติงานเกี่ยวกับข้อมูลส่วนบุคคลภาครัฐตาม พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 (รายงานผลการวิจัย).

8. ข้อกำหนดเพื่อรับรองความปลอดภัยของระบบข้อมูลและข้อมูลที่จัดเก็บและการรับรองความลับต่าง ๆ ที่ได้รับการคุ้มครองตามกฎหมาย

9. ข้อตกลงว่าระบบข้อมูลดังกล่าวมีวัตถุประสงค์ในการส่งข้อมูลที่ระบุชื่อระหว่างดินแดนของประเทศฝรั่งเศสและต่างประเทศหรือไม่ ทั้งนี้ ไม่ว่าจะกระทำในรูปแบบใด

อย่างไรก็ตาม คำขอเกี่ยวกับการจัดทำข้อมูลข่าวสารที่เกี่ยวข้องกับความมั่นคงของรัฐ การป้องกันประเทศ และความปลอดภัยสาธารณะ อาจไม่มีรายการบางรายการดังที่กำหนดไว้ข้างต้นก็ได้

สำหรับการจัดทำระบบข้อมูลข่าวสารของหน่วยงานรัฐหรือองค์กรเอกชนในกิจการบางประเภท ซึ่งมีได้ก่อให้เกิดผลกระทบต่อเสรีภาพหรือชีวิตส่วนตัว ให้ CNIL จัดทำหลักเกณฑ์อย่างง่าย โดยเทียบเคียงจากรายการต่าง ๆ ตามที่กำหนดข้างต้น และประกาศหลักเกณฑ์ดังกล่าวให้สาธารณชนทั่วไปได้ทราบเพื่อเป็นแนวทางในการจัดทำระบบข้อมูลข่าวสาร และการจัดทำระบบข้อมูลข่าวสารต้องขออนุญาต CNIL ก่อนตามหลักทั่วไปที่กำหนดไว้ เว้นแต่คณะกรรมการจะมีคำสั่งเป็นพิเศษ เมื่อได้รับคำขอดังกล่าวแล้วผู้ยื่นคำขอจึงสามารถจัดทำระบบข้อมูลข่าวสารได้ การนำแนวทางอย่างง่ายไปใช้สามารถเกิดขึ้นในกิจการ เช่น การเก็บข้อมูลที่ระบุชื่อในระบบภาษีหรือข้อมูลระบุชื่อของห้องสมุด<sup>50</sup> เป็นต้น

อย่างไรก็ดี แนวทางสำหรับกระบวนการจัดทำระบบข้อมูลข่าวสารอย่างง่ายประกอบด้วยรายการ ดังนี้

1. การจัดทำระบบการประมวลผลข้อมูลข่าวสารกระทำเพียงเท่าที่วัตถุประสงค์ที่กำหนดเท่านั้น และเจ้าของข้อมูลต้องสามารถเข้าถึงข้อมูลข่าวสารได้โดยง่าย

2. ระบบการประมวลผลข้อมูลข่าวสารต้องใช้โปรแกรมคอมพิวเตอร์ที่สามารถตรวจสอบข้อมูลข่าวสารได้โดยง่าย

3. การเชื่อมโยงข้อมูลข่าวสารทำได้เท่าที่จำเป็นแก่วัตถุประสงค์และเพียงเท่าที่จำเป็นแก่การใช้เท่านั้น

4. ต้องมีมาตรการในการรักษาความปลอดภัยและมาตรการในการรักษาความลับของข้อมูลข่าวสาร

กฎหมายได้บัญญัติรับรองสิทธิของบุคคลธรรมดาที่เกี่ยวข้องกับข้อมูลที่ระบุชื่อไว้หลายประการ ได้แก่<sup>51</sup>

<sup>50</sup> CNIL. สืบค้นจาก <http://www.cnil.fr/index.php?id=4>

<sup>51</sup> ปัญหาและมาตรการทางกฎหมายในการรับรองและคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว (*Right to privacy*) (รายงานผลการวิจัย) (น. 34). เล่มเดิม.

1. สิทธิในการสอบถามหน่วยงานของรัฐหรือองค์กรเอกชนที่จัดทำระบบข้อมูลสารสนเทศแบบอัตโนมัติ ตามรายชื่อที่ CNIL ได้จัดทำและประกาศต่อสาธารณชนว่าระบบข้อมูลสารสนเทศดังกล่าวมีข้อมูลส่วนบุคคลของตนหรือไม่ และสิทธิในการเข้าตรวจสอบข้อมูลนั้นได้ในกรณีที่มีข้อมูลข่าวสารของตนปรากฏอยู่

2. สิทธิในการได้รับการเปิดเผยข้อมูลที่เกี่ยวข้องกับตน ทั้งนี้ ข้อมูลที่เปิดเผยนั้นจะต้องใช้ภาษาที่เข้าใจง่ายและต้องมีเนื้อความเป็นอย่างเดียวกับข้อมูลที่บันทึกไว้

3. สิทธิในการได้รับสำเนาเอกสารข้อมูลที่เกี่ยวข้องกับตน

4. สิทธิในการขอให้ดำเนินการแก้ไขเพิ่มเติมทำให้ชัดเจนขึ้น ปรับปรุงให้ทันสมัยหรือลบทิ้ง ซึ่งข้อมูลที่เกี่ยวข้องกับตนที่ไม่ถูกต้อง ไม่ครบถ้วนสมบูรณ์ คลุมเครือ ล้าสมัย หรือการเก็บรวบรวม การใช้ การเปิดเผย หรือการเก็บรักษาข้อมูลนั้นเป็นการต้องห้าม

นอกจากนี้ ยังมีหน้าที่เฉพาะที่สำคัญ เช่น การให้ความเห็นชอบต่อการบันทึกข้อมูลเกี่ยวกับชาติกำเนิด หรือความคิดเห็นทางการเมือง ทางปรัชญา หรือทางศาสนา หรือการเป็นสมาชิกของสหพันธ์ต่าง ๆ และในการใช้อำนาจหน้าที่ในการควบคุม คณะกรรมการมีอำนาจจัดทำหลักเกณฑ์เพื่อรับรองความปลอดภัยของระบบข้อมูล กำหนดมาตรการด้านความปลอดภัยในสถานการณ์พิเศษ ซึ่งอาจมีขอบเขตไปถึงการทำลายเครื่องมือและอุปกรณ์ต่าง ๆ ที่ใช้ในการจัดเก็บข้อมูล กำกับดูแลมิให้มาตรการต่าง ๆ ที่ดำเนินการเพื่อการใช้สิทธิเข้าตรวจสอบข้อมูลและการแก้ไขข้อมูล ก่อให้เกิดอุปสรรคต่อเสรีภาพในการใช้สิทธิดังกล่าว จัดทำรายชื่อระบบข้อมูลข่าวสารและประกาศให้สาธารณชนรับทราบโดยระบบข้อมูลแต่ละระบบต้องประกอบด้วยกฎหมายหรือกฎระเบียบที่กำหนดให้จัดทำระบบข้อมูลชื่อของระบบข้อมูลและวัตถุประสงค์ หน่วยงานภายในที่บุคคลสามารถใช้สิทธิเข้าตรวจสอบข้อมูล และประเภทของข้อมูล หรือประเภทของบุคคลที่สามารถเข้าตรวจสอบข้อมูลนั้นได้

การอนุญาตให้ใช้ข้อมูลส่วนบุคคล (Consent)

การอนุญาตให้มีการเข้าถึงข้อมูลส่วนบุคคลตามรัฐบัญญัติที่ 78-17 ลงวันที่ 6 มกราคม ค.ศ. 1978 ว่าด้วยข้อมูลสารสนเทศ แฟ้มข้อมูลและเสรีภาพ นอกจากการได้รับอนุญาตจากคณะกรรมการว่าด้วยข้อมูลข่าวสารและเสรีภาพแห่งชาติ (La commission nationale de l'informatique et des libertés หรือ CNIL) หรือเป็นข้อยกเว้นที่เกี่ยวกับประโยชน์ของรัฐและเกี่ยวข้องกับประโยชน์สาธารณะตามมาตรา 26-27 แล้ว ยังจะต้องได้รับการอนุญาตให้มีการเข้าถึงข้อมูลส่วนบุคคลจากเจ้าของข้อมูลด้วย<sup>52</sup>

<sup>52</sup> Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, Article 33.

### โทษสำหรับการละเมิดต่อข้อมูลส่วนบุคคล

สำหรับโทษสำหรับการละเมิดต่อข้อมูลส่วนบุคคลนั้นรัฐบัญญัติที่ 78-17 ลงวันที่ 6 มกราคม ค.ศ. 1978 ว่าด้วยข้อมูลสารสนเทศเพิ่มข้อมูลและเสรีภาพ ไม่ได้มีการกำหนดโทษไว้แต่อย่างใด แต่โทษสำหรับการละเมิดต่อข้อมูลส่วนบุคคลถูกกำหนดไว้ในกฎหมายฉบับอื่น ๆ ที่สามารถนำมาใช้สำหรับการละเมิดต่อข้อมูลส่วนบุคคลได้ กล่าวคือ

ประมวลกฎหมายคุ้มครองผู้บริโภคและประมวลกฎหมายว่าด้วยการไปรษณีย์และการโทรคมนาคม ที่กำหนดว่า ผู้ที่ฝ่าฝืนประมวลกฎหมายว่าด้วยการไปรษณีย์และการโทรคมนาคมของฝรั่งเศสจะต้องถูกปรับเป็นเงิน 750 ยูโรต่อข้อความ และอาจได้รับโทษทางอาญา จำคุกสูงสุดไม่เกิน 5 ปี และปรับสูงสุด 300,000 ยูโร หากได้เลขหมายโทรศัพท์มาด้วยวิธีการไม่ชอบด้วยกฎหมาย<sup>53</sup>

ประมวลกฎหมายแพ่งของประเทศฝรั่งเศส มาตรา 1382 ที่กำหนดว่า บุคคลที่ก่อให้เกิดความเสียหายแก่บุคคลอื่นจะต้องรับผิดชอบต่อบุคคลนั้นเพื่อความเสียหายที่เกิดขึ้นแต่การนั้น กล่าวคือมีการกระทำความผิดของบุคคลหนึ่งต่อบุคคลอื่นและการกระทำนั้นก่อให้เกิดความเสียหายแก่ผู้เสียหาย ผู้ที่เป็นต้นเหตุแห่งการกระทำก็ต้องรับผิดชอบต่อผลของความเสียหายที่เกิดขึ้นนั่นเอง<sup>54</sup>

การก่อให้เกิดผลกระทบต่อชีวิตส่วนตัวของบุคคลตามมาตรา 1382 นี้มักจะเป็นการกระทำความผิดโดยจงใจอันมาจากการเลือกที่จะกระทำการนั้นโดยสมัครใจของผู้กระทำ แต่ก็อาจมีกรณีเป็นการกระทำโดยละเว้นได้เช่นกัน เช่น กรณีบรรณาธิการนิตยสารฉบับหนึ่งที่ปล่อยให้มีการตีพิมพ์บทความซึ่งก่อให้เกิดผลกระทบต่อชีวิตส่วนตัวของบุคคลหนึ่ง ทั้ง ๆ ที่ตนควรที่จะคัดค้านการตีพิมพ์บทความดังกล่าวบรรณาธิการนั้นจึงต้องรับผิดชอบร่วมกับบริษัทนิตยสารในการชดเชยค่าเสียหายแก่ผู้เสียหายเพื่อความเสียหายที่เกิดขึ้นแต่การนั้น เป็นต้น<sup>55</sup>

ประมวลกฎหมายอาญาของประเทศฝรั่งเศสได้กำหนดบทลงโทษสำหรับการล่วงละเมิดต่อข้อมูลส่วนบุคคลไว้ด้วยกันหลายมาตรา ในส่วนนี้ผู้เขียนได้ทำการศึกษาพบว่ามีความเกี่ยวเนื่องกัน 3 กรณีด้วยกัน กล่าวคือ 1. ความผิดในการก่อให้เกิดผลกระทบต่อความลับในชีวิตส่วนตัว

<sup>53</sup> mycomputerlaw.in.th. (2554). *ข้อความขยะ...อะไรคือมาตรการ “เลือกรับ” และ “เลือกไม่รับ”?*. สืบค้น 31 ตุลาคม 2558, จาก <http://mycomputerlaw.in.th/2011/07/spam-sms-opt-in-opt-out/>

<sup>54</sup> *ปัญหาและมาตรการทางกฎหมายในการรับรองและคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว (Right to privacy)* (รายงานผลการวิจัย) (น. 30). เล่มเดิม.

<sup>55</sup> Civ. 2, 9 juillet 1980, Bull. II, n° 179; Paris, 1ère Ch. A, 19 juin 1989, F. c/ L., D. 1989, I.R., 240. (อ้างถึงใน *ปัญหาและมาตรการทางกฎหมายในการรับรองและคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว (Right to privacy)* (รายงานผลการวิจัย) (น. 30). เล่มเดิม).

ของบุคคลอื่นโดยเจตนา 2. ความผิดในการก่อให้เกิดผลกระทบต่อความลับในการประกอบวิชาชีพ และ 3. ความผิดในการก่อให้เกิดผลกระทบต่อความลับในจดหมายของบุคคลอื่น โดยมีรายละเอียด ดังต่อไปนี้<sup>56</sup>

1. ความผิดในการก่อให้เกิดผลกระทบต่อความลับในชีวิตส่วนตัวของบุคคลอื่น โดยเจตนา ถูกกำหนดอยู่ในมาตรา 226-1 วรรคหนึ่ง แห่งประมวลกฎหมายอาญากำหนดว่า การก่อให้เกิดความเสียหายต่อความลับหรือเกี่ยวกับชีวิตส่วนตัวของบุคคลอื่น โดยการดักฟัง บันทึกหรือส่งต่อคำพูดที่บุคคลได้กล่าวขึ้นในลักษณะเป็นการส่วนตัวหรือเป็นความลับ โดยมีได้รับความยินยอมของบุคคลนั้น ไม่ว่าจะกระทำโดยใช้เครื่องมืออย่างใด หรือโดยการถ่าย การบันทึกหรือการส่งต่อภาพของบุคคลในสถานที่ส่วนบุคคล โดยมีได้รับความยินยอมของบุคคลนั้น ไม่ว่าจะกระทำโดยใช้เครื่องมืออย่างใด ต้องรับโทษจำคุกหนึ่งปีและปรับเป็นเงินจำนวน 45,000 ยูโร

2. ความผิดในการก่อให้เกิดผลกระทบต่อความลับในการประกอบวิชาชีพ ถูกกำหนดอยู่ในมาตรา 226-1 แห่งประมวลกฎหมายอาญากำหนดว่า การเปิดเผยข้อมูลที่มีลักษณะเป็นความลับโดยบุคคลหนึ่งซึ่งได้รับข้อมูลนั้นโดยสภาพของเรื่องหรือโดยตำแหน่งหน้าที่หรืออันเนื่องมาจากการปฏิบัติตามอำนาจหน้าที่เป็นการชั่วคราว ต้องรับโทษจำคุกหนึ่งปีและปรับเป็นเงินจำนวน 15,000 ยูโร

3. ความผิดในการก่อให้เกิดผลกระทบต่อความลับในจดหมายของบุคคลอื่น ซึ่งเป็นฐานความผิดที่มีเจตนารมณ์เพื่อคุ้มครองเสรีภาพในการแสดงความคิดเห็นผ่านจดหมายและคุ้มครองความลับในชีวิตส่วนตัวของบุคคลที่ปรากฏอยู่ในจดหมายนั้นถูกกำหนดอยู่ใน มาตรา 226-15 วรรคหนึ่ง แห่งประมวลกฎหมายอาญากำหนดว่า การเปิด ทำลาย ทำให้ล่าช้า หรือส่งกลับโดยเจตนาทุจริต ซึ่งจดหมายที่มีถึงบุคคลภายนอกไม่ว่าจะได้มาถึงจุดหมายปลายทางแล้วหรือไม่ก็ตาม หรือการอ่านข้อความภายในจดหมายโดยการฉ้อฉล ต้องรับโทษจำคุกหนึ่งปี และปรับเป็นเงิน 45,000 ยูโร

---

<sup>56</sup> ปัญหาและมาตรการทางกฎหมายในการรับรองและคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว (*Right to privacy*) (รายงานผลการวิจัย) (น. 32). เล่มเดิม.

### 3.2.2.3 การคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่น

ประเทศญี่ปุ่นเป็นประเทศหนึ่งที่มีความก้าวหน้าในเทคโนโลยี นอกจากนี้ยังเป็นประเทศที่ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลของประชาชนเป็นอย่างมาก จึงมีแนวคิดในการจัดทำกฎหมายเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคล ในปี ค.ศ. 1999 โดยกฎหมายฉบับดังกล่าวอาศัยหลักการพื้นฐาน 5 ประการ คือ<sup>57</sup>

1. จะต้องมีการกำหนดวัตถุประสงค์ในการจัดเก็บข้อมูลให้ชัดเจนและจัดระบบข้อมูลตามวัตถุประสงค์ที่ได้ประกาศไว้
2. การจัดเก็บข้อมูลส่วนบุคคลจะต้องกระทำโดยชอบด้วยกฎหมายและใช้วิธีการที่เหมาะสม
3. การเก็บรักษาและการปรับปรุงข้อมูลให้แน่นอนถูกต้องและทันสมัยอยู่เสมอ
4. จัดระบบรักษาความปลอดภัยให้กับข้อมูลที่จัดเก็บ
5. จัดระบบการจัดเก็บและใช้ข้อมูลภายใต้หลักความโปร่งใส

นอกจากนี้ร่างกฎหมายดังกล่าวยังมุ่งกำหนดให้หน่วยงานเอกชนมีหน้าที่เปิดเผยข้อมูลที่ตนเก็บไว้แก่เจ้าของข้อมูลนั้น และแจ้งให้เจ้าของข้อมูลทราบว่าหน่วยงานเอกชนนั้น ๆ จัดเก็บข้อมูลไว้เพื่อวัตถุประสงค์ใด และกฎหมายยังห้ามไม่ให้หน่วยงานเอกชนที่จัดเก็บข้อมูลส่วนบุคคลโอนข้อมูลแก่บุคคลภายนอกหรือยินยอมให้บุคคลภายนอกมารวมใช้ข้อมูลนั้นด้วย

ต่อวันที่ 30 พฤษภาคม ค.ศ. 2003 ได้มีการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2003 หรือ Act on Protection of Personal Information 2003 ขึ้นมาบังคับใช้ใน ประเทศญี่ปุ่น กฎหมายฉบับนี้มุ่งคุ้มครองข้อมูลส่วนบุคคลทั้งในความควบคุมดูแลของหน่วยงานของรัฐ หน่วยงานเอกชนและหน่วยงานอิสระของรัฐ โดยมุ่งจะวางหลักกฎหมายทั่วไปเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ทั้งนี้ โดยคำนึงถึงความจำเป็นในการเอื้ออำนวยให้การประกอบการค้า และธุรกิจในยุคข้อมูลข่าวสารเป็นไปได้ และยังวางหลักกว้าง ๆ ในกฎหมายว่า การดำเนินการใด ๆ ต่อข้อมูลส่วนบุคคลจะต้องกระทำด้วยความเคารพต่อสิทธิในบุคคลภาพของเอกชนแต่ละคน และจะต้องใช้วิธีที่ชอบและแน่นอนถูกต้อง<sup>58</sup>

<sup>57</sup> จาก กฎหมายคุ้มครองข้อมูลข่าวสารส่วนบุคคลในประเทศญี่ปุ่น, โดย กิตติศักดิ์ ปรกติ, 2547, ธันวาคม), *วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์*, 34(4), น. 525.

<sup>58</sup> Act on Protection of Personal Information 2003, Article 1. (อ้างถึงใน *ปัญหาทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ กรณีศึกษา: การจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล (privacy policy) ของธนาคาร สถาบันการเงิน และผู้ประกอบการธุรกิจบัตรเครดิตในประเทศไทย (วิทยานิพนธ์ปริญญาโท)* (น. 49), เล่มเดิม).

ทั้งนี้ กฎหมายกำหนดให้คณะรัฐมนตรีเป็นผู้มีอำนาจหน้าที่ในการบังคับการให้เป็นไปตามกฎหมายนี้ โดยกำหนดแนวนโยบายพื้นฐานเพื่อส่งเสริมมาตรการการคุ้มครองข้อมูลส่วนบุคคลตามความมุ่งหมายของกฎหมายนี้ และรัฐมนตรีที่รับผิดชอบมีอำนาจหลักเกณฑ์แนวปฏิบัติแก่เอกชน และกำหนดให้รัฐบาลกลางมีหน้าที่สนับสนุนช่วยเหลือองค์กรปกครองท้องถิ่น และให้องค์กรปกครองท้องถิ่นวางมาตรการที่จำเป็นเพื่อส่งเสริมความช่วยเหลือแก่ผู้ประกอบการในเขตท้องที่ของตน และมีหน้าที่คอยเป็นสื่อกลาง โกล่เกลี่ยข้อขัดแย้งหรือบรรเทาอุปสรรคในการปฏิบัติตามกฎหมายนี้ด้วย

กฎหมายได้วางข้อยกเว้นไม่ใช้บังคับแก่บุคคล 5 ประเภท ได้แก่<sup>59</sup>

1. สื่อสารมวลชน หากการดำเนินการเกี่ยวกับข้อมูลข่าวสารส่วนบุคคลนั้นเกี่ยวข้องกับกิจการของสื่อสารมวลชน ทั้งนี้ ได้มีการกำหนดค่านิยมความหมายของสื่อมวลชนไว้ด้วยว่า หมายถึง การไขข่าวเกี่ยวกับข้อเท็จจริงไปยังบุคคลที่ไม่เฉพาะเจาะจงจำนวนมาก รวมทั้งการแสดงความคิดเห็นที่อาศัยข้อเท็จจริงเหล่านั้น

2. นักเขียน ในส่วนที่เกี่ยวกับการดำเนินงานเขียนของตน

3. มหาวิทยาลัยหรือสถาบันที่มุ่งศึกษาวิจัยทางวิชาการ และบุคลากรขององค์การเหล่านั้นเฉพาะกิจการที่เกี่ยวกับการศึกษาวิจัย

4. องค์กรศาสนา ในส่วนที่เกี่ยวกับการดำเนินกิจกรรมทางศาสนา

5. องค์กรทางการเมือง ในส่วนที่เกี่ยวกับการดำเนินกิจกรรมทางการเมือง

แต่ทั้งนี้บุคคลที่เข้าข่ายได้รับยกเว้นจะต้องวางมาตรการในการคุ้มครองข้อมูลส่วนบุคคลและป้องกันการนำไปเปิดเผยโดยไม่สมควรด้วย

สำหรับการจัดเก็บข้อมูลนั้นพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2003 หรือ Act on Protection of Personal Information 2003 ได้กำหนดเป็นหลักการเบื้องต้นว่า ผู้ประกอบการเอกชนที่จัดระบบข้อมูลส่วนบุคคลจะต้องระมัดระวังประสงคในการจัดระบบข้อมูลส่วนบุคคลในความควบคุมดูแลของตนให้ชัดเจน และจะต้องไม่นำข้อมูลส่วนบุคคลนั้น ไปใช้นอกเหนือจากการใช้ตามปกติภายในขอบเขตวัตถุประสงค์ที่ได้ระบุไว้ นอกจากนี้ผู้ประกอบการต้องไม่จัดเก็บหรือรวบรวมข้อมูลส่วนบุคคลเป็นอย่างอื่น ผู้ประกอบการนั้นจะต้องแจ้งให้เจ้าของข้อมูลทราบหรือประกาศโฆษณาต่อสาธารณชนด้วย<sup>60</sup>

<sup>59</sup> มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลจากการใช้บริการเครือข่ายสังคมออนไลน์ (วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ) (น. 197). เล่มเดิม.

<sup>60</sup> กฎหมายคุ้มครองข้อมูลข่าวสารส่วนบุคคลในประเทศญี่ปุ่น (น. 530). เล่มเดิม.

การที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2003 หรือ Act on Protection of Personal Information 2003 ไม่ได้มีการกำหนดให้ผู้ประกอบการต้องขอความยินยอมจากเจ้าของข้อมูลเป็นรายบุคคล นี้ถือได้ว่าเป็นลักษณะที่มีความพิเศษกว่ากฎหมายของประเทศอื่น ๆ โดยเฉพาะกฎหมายในแถบประเทศยุโรป เพราะว่าประเทศในแถบยุโรปนั้นลักษณะของกฎหมายจะกำหนดให้ต้องแจ้งแก่เจ้าของข้อมูลส่วนบุคคลทุกคน แต่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2003 หรือ Act on Protection of Personal Information 2003 กำหนดการแจ้งไว้โดยให้แจ้งเจ้าของข้อมูลทราบนับตั้งแต่เมื่อเริ่มจัดเก็บข้อมูลส่วนบุคคลหรือโดยโฆษณาต่อสาธารณชนก็ได้ โดยต้องแจ้งวัตถุประสงค์ของการจัดเก็บ การใช้ข้อมูลร่วมกับบุคคลอื่น เพื่อให้เจ้าของข้อมูลมีโอกาสปฏิเสธหรือคัดค้านได้ ทั้งนี้ จะต้องแจ้งหรือกำหนดวิธีบอกกล่าวปฏิเสธหรือโต้แย้งมายังผู้ประกอบการให้เป็นไปโดยสะดวก โดยหลักการดังกล่าวถูกกำหนดไว้ในมาตรา 18(1) และ มาตรา 24 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2003 หรือ Act on Protection of Personal Information 2003<sup>61</sup>

#### หลักความยินยอม (Consent)

การเก็บรวบรวมข้อมูลส่วนบุคคลต้องได้รับความยินยอมหรือมีการแจ้งเจ้าของข้อมูล (Data Subject) ก่อนหรือในขณะที่มีการเก็บรวบรวมข้อมูล ในกรณีที่ไม่สามารถขอความยินยอมจากเจ้าของข้อมูลได้ ผู้ดำเนินการเก็บรวบรวมข้อมูลส่วนบุคคลต้องแจ้งขอความยินยอมจากเจ้าของข้อมูลในเวลาใด ๆ ที่สามารถทำได้ และการนำข้อมูลส่วนบุคคลไปใช้แต่ละครั้งต้องมีการแจ้งต่อเจ้าของข้อมูลทุกครั้งและต้องใช้เท่าที่จำกัดเฉพาะตามวัตถุประสงค์ที่ได้แจ้งไว้เท่านั้น

หลักทั่วไปในกฎหมายคุ้มครองข้อมูลส่วนบุคคลคือการคุ้มครองข้อมูลส่วนบุคคล คือ การคุ้มครองไม่ให้เปิดเผยหรือโอนข้อมูลส่วนบุคคลไปยังบุคคลภายนอก โดยเจ้าของข้อมูลมิได้รับรู้หรือยินยอมไว้ล่วงหน้า เว้นแต่จะเข้าข้อยกเว้นที่กฎหมายกำหนด ข้อยกเว้นดังกล่าวมีหลายประการ เช่น เมื่อมีเหตุจำเป็นเพื่อป้องกันภัยอันตราย หรือเป็นการเปิดเผยต่อเจ้าหน้าที่ผู้มีอำนาจโดยชอบ ที่สำคัญข้อยกเว้นดังกล่าวนี้รวมถึง กรณีเปิดเผยแก่คู่สัญญาผู้ได้รับมอบหมายให้เป็นผู้ให้บริการเครือข่ายแก่ผู้ประกอบการ หรือผู้รับสัญญาช่วงจากคู่สัญญา และผู้ประกอบการเข้าร่วมหรือผู้ประกอบการอื่นซึ่งมีสิทธิใช้ข้อมูลส่วนบุคคลนั้น เช่น ในกรณีมีการ โอนหรือควบกิจการเข้าด้วยกัน เป็นต้น ทั้งนี้เพราะในกรณีเหล่านี้กฎหมายไม่ถือว่าเป็นการเปิดเผยข้อมูลต่อบุคคลภายนอก<sup>62</sup>

<sup>61</sup> Act on Protection of Personal Information 2003, Article 18(1) and Article 24.

<sup>62</sup> กฎหมายคุ้มครองข้อมูลข่าวสารส่วนบุคคลในประเทศญี่ปุ่น (น. 532). เล่มเดิม.

### หลักการเก็บรวบรวมข้อมูลอย่างจำกัด

ในการจัดเก็บข้อมูลส่วนบุคคลในหลายประเทศส่วนใหญ่ต้องมีการบอกกล่าวหรือแจ้งต่อองค์กรที่มีอำนาจกำกับดูแล หรือในบางกรณีหมายถึงการแจ้งต่อนายทะเบียนที่มีอำนาจของรัฐ ซึ่งผู้ดำเนินการเก็บรวบรวมข้อมูลส่วนบุคคลจะได้รับใบอนุญาตให้ดำเนินการได้ และผู้ดำเนินการเก็บรวบรวมข้อมูลส่วนบุคคลต้องปฏิบัติตามหลักเกณฑ์ข้อบังคับที่เจ้าหน้าที่ผู้มีอำนาจกำหนด หากมีการฝ่าฝืนอาจถูกถอดถอนใบอนุญาตชั่วคราวหรือเป็นการถาวรแล้วแต่กรณี

### หลักการจำกัดการใช้ การเปิดเผยและการเก็บรักษา

ผู้ประกอบการยังมีหน้าที่ในการจัดให้มีระเบียบและหลักเกณฑ์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและแจ้งให้เจ้าของข้อมูลหรือประกาศต่อสาธารณะชนและในกรณีที่มีการเก็บรวบรวมหรือการจัดเก็บเป็นส่วนหนึ่งของการปฏิบัติตามสัญญาหรือเป็นส่วนหนึ่งของการจัดทำข้อมูลข่าวสารหรือเอกสารในรูปแบบข้อมูลข่าวสารอิเล็กทรอนิกส์ ผู้ประกอบการจะต้องแจ้งให้เจ้าของข้อมูลรู้ล่วงหน้าด้วย อย่างไรก็ตามกฎหมายได้วางข้อยกเว้นไว้ว่า ผู้ประกอบการไม่ต้องแจ้งให้เจ้าของข้อมูลทราบหากการแจ้งหรือการโฆษณาต่อสาธารณะชนนั้นจะเป็นเหตุให้ผู้ประกอบการต้องเสียประโยชน์อันพึงได้โดยชอบ<sup>63</sup>

### การรักษาความปลอดภัย

หลักการรักษาความปลอดภัยนี้ถูกกำหนดอยู่ใน Act on Protection of Personal Information 2003 Article 20<sup>64</sup> ที่กำหนดให้ผู้ประกอบการมีหน้าที่วางมาตรการต่าง ๆ เพื่อรักษาความปลอดภัยแก่ข้อมูลส่วนบุคคลและระบบฐานข้อมูลในความควบคุมดูแลของตนไม่ให้เกิดสูญหาย หรือมีผู้นำเอาไปเปิดเผยโดยไม่ได้รับอนุญาต โดยผู้ประกอบการมีหน้าที่วางมาตรการต่าง ๆ เพื่อรักษาความปลอดภัยแก่ข้อมูลส่วนบุคคลและระบบฐานข้อมูลในความควบคุมดูแลของตนไม่ให้เกิดความสูญหาย หรือมีผู้นำเอาไปเปิดเผยโดยมิชอบนอกจากนี้ ยังต้องกำกับดูแลลูกจ้างของตนในการเข้าถึงข้อมูลส่วนบุคคลให้ปฏิบัติหน้าที่เกี่ยวกับข้อมูลส่วนบุคคลอย่างถูกวิธี และสามารถรักษาความปลอดภัยแก่ข้อมูลและระบบฐานข้อมูลได้ นอกจากนี้กฎหมายยังกำหนดให้ผู้ว่าจ้างต้องมีหน้าที่รับผิดชอบทำนองเดียวกัน คือ แม้ว่าจ้างให้ผู้รับจ้างไปดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล ผู้ว่าจ้างก็ต้องวางมาตรการรักษาความปลอดภัยไม่ให้ข้อมูลสูญหาย หรือมีผู้นำไปเปิดเผยในทางไม่สมควร

<sup>63</sup> แหล่งเดิม.

<sup>64</sup> Act on Protection of Personal Information 2003 Article 20. (อ้างถึงใน ปัญหาทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ กรณีศึกษา: การจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล (privacy policy) ของธนาคาร สถาบันการเงิน และผู้ประกอบการธุรกิจบัตรเครดิตในประเทศไทย (วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ) (น. 49). เล่มเดิม).

โดยนัยนี้กฎหมายได้ขยายขอบเขตความรับผิดชอบทางสัญญาและทางละเมิดของผู้ประกอบการให้กว้างขึ้นด้วย

#### การเปิดเผยข้อมูลส่วนบุคคล

โดยหลักแล้วการให้ความคุ้มครองข้อมูลส่วนบุคคลจะมีหลักที่สำคัญก็คือ การเก็บรักษาข้อมูลส่วนบุคคลไม่ให้บุคคลภายนอกได้ล่วงรู้โดยที่บุคคลผู้เป็นเจ้าของข้อมูลไม่ได้รับรู้หรือยินยอมไว้ล่วงหน้าแต่อย่างใด โดยเรื่องดังกล่าวมีการกำหนดไว้ในมาตรา 22 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2003 หรือ Act on Protection of Personal Information 2003

แม้ว่าโดยหลักของการให้ความคุ้มครองข้อมูลส่วนบุคคลจะห้ามไม่ให้มีการเปิดเผยข้อมูลส่วนบุคคลก่อนที่จะได้รับอนุญาตหรือได้มีการอนุญาตไว้ล่วงหน้าแล้วก็ตาม แต่ข้อห้ามดังกล่าวก็ไม่ใช่ข้อห้ามที่เด็ดขาด มีการยกเว้นไว้ในมาตรา 23(1) ของพระราชบัญญัติฉบับเดียวกัน กล่าวคือ<sup>65</sup>

1. กรณีที่การจัดการข้อมูลส่วนบุคคลอยู่บนพื้นฐานของกฎหมาย
2. กรณีที่การจัดการข้อมูลส่วนบุคคลเป็นสิ่งที่จำเป็นสำหรับการป้องกันชีวิตร่างกายหรือทรัพย์สินของบุคคลที่จำเป็นในขณะนั้นและเป็นเรื่องยากที่จะได้รับความยินยอมจากบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลนั้น
3. กรณีของการจัดการข้อมูลส่วนบุคคลจำเป็นต่อการป้องกันเกี่ยวกับโรคติดต่อที่มีผลต่ออนามัยของประชาชนและหากต้องรอคำอนุญาตของผู้เป็นเจ้าของข้อมูลส่วนบุคคลจะก่อให้เกิดความเสียหายในวงกว้าง
4. กรณีการให้ความยินยอมของบุคคลผู้เป็นเจ้าของข้อมูลส่วนบุคคลจะก่อให้เกิดอุปสรรคของการปฏิบัติงานของเจ้าหน้าที่รัฐ

หากเข้าข้อยกเว้นอย่างใดอย่างหนึ่งใน 4 ข้อที่ถูกกำหนดอยู่ในมาตรา 23(1) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2003 หรือ Act on Protection of Personal Information 2003 จะใช้ข้อมูลส่วนบุคคลของเจ้าของข้อมูลก็จะได้รับการยกเว้นไม่ต้องรับผิดชอบ<sup>66</sup>

#### หลักการเข้าตรวจดูข้อมูลของบุคคล

เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการเข้าถึงข้อมูลข่าวสารของตน สิทธิในการเรียกร้องให้ตรวจสอบและแก้ไขเปลี่ยนแปลง ปรับปรุง ข้อมูลข่าวสารเกี่ยวกับตนให้ถูกต้องและทันสมัย

<sup>65</sup> Act on Protection of Personal Information 2003, Article 23(1).

<sup>66</sup> Act on Protection of Personal Information 2003, Article 23(1).

สิทธิที่จะรู้ว่าใครบ้างที่สามารถเข้าถึงข้อมูลส่วนบุคคลของตน สิทธิในการรับรู้ถึงกระบวนการหรือวิธีการต่าง ๆ ในการใช้ การประมวลผล เผยแพร่ข้อมูลเกี่ยวกับตน<sup>67</sup>

บทลงโทษของผู้ที่ทำการฝ่าฝืนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2003

บทลงโทษของผู้ที่ทำการฝ่าฝืนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2003

ถูกกำหนดอยู่ในหมวดที่ 6 ว่าด้วย Penal Provisions มาตรา 56 ถึงมาตรา 59 โดยมีรายละเอียดดังต่อไปนี้

กรณีที่ 1 เป็นการลงโทษแก่นิติบุคคลผู้ที่เป็นผู้ดูแลข้อมูลส่วนบุคคลแล้วมีการนำเอาข้อมูลส่วนบุคคลไปจำหน่ายหรือเปิดเผยให้กับบุคคลภายนอกทราบ เช่น หมายเลขโทรศัพท์ เป็นต้น หากมีการฝ่าฝืนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2003 หรือ Act on Protection of Personal Information 2003 มาตรา 56 กำหนดให้มีโทษจำคุกผู้ที่มีอำนาจกำกับดูแลนิติบุคคลนั้น ไม่เกินหกเดือนหรือปรับไม่เกินกว่า 300,000 เยน<sup>68</sup>

กรณีที่ 2 เป็นการลงโทษแก่การไม่ทำรายงานหรือทำรายงานข้อมูลส่วนบุคคลเท็จ หากมีการฝ่าฝืนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2003 หรือ Act on Protection of Personal Information 2003 มาตรา 57 กำหนดให้มีโทษสำหรับการไม่ทำรายงานหรือทำรายงานข้อมูลส่วนบุคคลเท็จ คือ ปรับไม่เกินกว่า 300,000 เยน<sup>69</sup>

กรณีที่ 3 เป็นการลงโทษกิจการที่ตกอยู่ภายใต้ข้อใดข้อหนึ่งของรายการต่อไปนี้ ต้องระวางโทษปรับไม่เกินกว่า 100,000 เยน ตามมาตรา 59<sup>70</sup>

1. กิจการที่ไม่ได้ทำรายงานที่จำเป็นตามวรรค 1 ของมาตรา 40 หรือที่ได้ทำรายงานเท็จ
2. กิจการฝ่าฝืนบทบัญญัติของมาตรา 45 กล่าวคือ เป็นกิจการที่ไม่ได้รับอนุญาตให้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล

---

<sup>67</sup> มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลจากการใช้บริการเครือข่ายสังคมออนไลน์ (วิทยานิพนธ์ปริญญาโทมหาบัณฑิต) (น. 201). เล่มเดิม.

<sup>68</sup> Act on Protection of Personal Information 2003, Article 56.

<sup>69</sup> Act on Protection of Personal Information 2003, Article 57.

<sup>70</sup> Act on Protection of Personal Information 2003, Article 59.

ตารางที่ 3.1 เปรียบเทียบกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศ

สาระสำคัญ	สหภาพ ยุโรป	ประเทศ อังกฤษ	ประเทศ แคนาดา	ประเทศ อิตาลี	ประเทศ ฝรั่งเศส	ประเทศ ญี่ปุ่น
1. หลักความรับผิดชอบ (Accountability)	√	-	√	√	-	√
2. หลักการแจ้งวัตถุประสงค์ (Identifying Purposes)	√	√	√	√	√	√
3. หลักความยินยอม (Consent)	√	-	√	√	√	√
4. หลักการเก็บรวบรวมข้อมูล อย่างจำกัด (Limiting Collection)	√	√	√	√	√	√
5. หลักการจำกัดการใช้ การเปิดเผย และการเก็บรักษา	√	√	√	√	-	√
6. หลักความถูกต้อง (Accuracy)	√	√	√	√	√	√
7. หลักการรักษาความปลอดภัย (Safeguards)	√	√	√	√	√	√
8. หลักการเปิดเผย (Openness)	√	-	√	√	-	√
9. หลักการเข้าตรวจสอบข้อมูลของ บุคคล (Individual Access)	√	√	√	√	√	√
10. หลักการโต้แย้งการปฏิบัติ ขององค์กร (Challenging Compliance)	√	√	√	√	-	√
11. หลักการไม่เลือกปฏิบัติ	√	-	-	-	-	-
12. หลักข้อจำกัดในการส่งหรือ โอนข้อมูลส่วนบุคคล	√	√	-	-	-	-

### 3.3 กฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย

การคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยได้รับการบัญญัติรับรองไว้ในกฎหมายทั้งในระดับรัฐธรรมนูญแห่งราชอาณาจักรไทยและกฎหมายระดับพระราชบัญญัติ โดยมีรายละเอียดดังต่อไปนี้

#### 3.3.1 รัฐธรรมนูญแห่งราชอาณาจักรไทย

การคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยได้รับการบัญญัติรับรองไว้ในรัฐธรรมนูญแห่งราชอาณาจักรไทย 3 ฉบับ คือ รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2534 รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540 และรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550 โดยในรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2534 และรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540 ยังมิได้มีการกล่าวถึงการคุ้มครองข้อมูลส่วนบุคคลไว้เป็นการเฉพาะ มีเพียงการกล่าวถึงสิทธิความเป็นอยู่ส่วนตัวเท่านั้น โดยมีรายละเอียดดังต่อไปนี้

##### 3.3.1.1 รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2534

รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2534 ได้บัญญัติในภาพรวมไว้อย่างกว้างในการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว โดยมีการบัญญัติไว้ในมาตรา 44 ว่าสิทธิของบุคคลในครอบครัว เกียรติยศหรือชื่อเสียงและความเป็นอยู่ส่วนตัว ย่อมได้รับความคุ้มครอง เท่านั้น โดยยังหาได้มีบทบัญญัติที่เป็นการคุ้มครองข้อมูลส่วนบุคคลแต่อย่างใด

##### 3.3.1.2 รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540

รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540 ได้พัฒนาการให้ความคุ้มครองสิทธิความเป็นอยู่ส่วนตัวของเจ้าของข้อมูลไว้เพิ่มเติมจากรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2534 แต่ก็ยังหาได้มีการกำหนดให้มีการคุ้มครองข้อมูลส่วนบุคคลไว้เป็นการเฉพาะ ดังเช่นรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550 แต่อย่างใดไม่ ซึ่งแต่เดิมมีการบัญญัติเพียงว่า “สิทธิของบุคคลในครอบครัว เกียรติยศหรือชื่อเสียง และความเป็นอยู่ส่วนตัว ย่อมได้รับความคุ้มครอง” แต่ในรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540 มีการเพิ่มเติมบทบัญญัติในวรรคที่สองของมาตรา 34 ดังนี้ “การกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชน อันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัว จะกระทำมิได้ เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณชน”

ความในวรรคสองของมาตรา 34 ที่บัญญัติเพิ่มเติมขึ้นมานั้น มีเจตนารมณ์ในการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวของบุคคล โดยคณะทำงานคณะกรรมการยกร่างรัฐธรรมนูญชี้แจงว่าถ้าไม่มีการบัญญัติไว้จะมีการกล่าวอ้างได้ง่าย ๆ ว่า “เพื่อประโยชน์สาธารณะ” ตัวอย่างเช่น

กรณีที่สื่อถ่ายภาพเปลือยของดาราส่งถ่ายไว้ดูเอง ไม่ได้เผยแพร่มาตีพิมพ์ นอกจากนี้ ความในวรรคสองนี้ มิได้หมายความเฉพาะการกระทำของสื่อมวลชนเท่านั้น แต่รวมถึงการกระทำอื่น ๆ ด้วย เช่น ใบปลิวโจมตีบุคคล การปล่อยข่าวลือต่าง ๆ<sup>71</sup>

การบัญญัติข้อความเพิ่มเติมใหม่นี้ถือได้ว่าเป็นหลักประกันสิทธิความเป็นอยู่ส่วนตัว ประเภทหนึ่งที่มีความชัดเจนแน่นอนนั่นเอง นอกจากมาตรา 34 แล้ว รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540 ยังมีการบัญญัติการให้ความคุ้มครองในสิทธิความเป็นอยู่ส่วนตัวไว้ในมาตรา 39<sup>72</sup> เรื่องของเสรีภาพในการแสดงความคิดเห็น การพูด การเขียน การพิมพ์ การโฆษณา และการสื่อความหมายโดยวิธีอื่น แต่ห้ามบุคคลไม่ให้มีเสรีภาพในการแสดงความคิดเห็น การพูด การเขียน การพิมพ์ การโฆษณา และการสื่อความหมายโดยวิธีอื่นที่จะไปกระทบต่อความเป็นอยู่ส่วนตัวของบุคคลอื่น

คณะกรรมการสิทธิการยกร่างรัฐธรรมนูญชี้แจงว่าความในมาตรา 39 มีเจตนารมณ์ ในการคุ้มครองเสรีภาพในการแสดงความคิดเห็น โดยจะหมายความว่า การห้ามทำการพิมพ์ การห้าม เสนอข่าวทางหนังสือพิมพ์ สถานีวิทยุกระจายเสียง หรือสถานีวิทยุโทรทัศน์หรือโดยทางอื่น โดย คำพิพากษาของศาลจะกระทำได้ตามกฎหมายเฉพาะเพื่อการคุ้มครองสิทธิ เสรีภาพ เกียรติยศ ชื่อเสียง สิทธิในครอบครัวหรือความเป็นอยู่ส่วนตัวของบุคคลอื่นเท่านั้น ซึ่งเป็นไปตามปณิญา สากลว่าด้วยสิทธิพลเมือง ข้อ 17 กำหนดว่า บุคคลจะถูกแทรกแซงความเป็นอยู่ส่วนตัวในครอบครัว เคหสถาน ฯลฯ โดยไม่ชอบด้วยกฎหมายไม่ได้<sup>73</sup>

<sup>71</sup> จาก เจตนารมณ์ของรัฐธรรมนูญ รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540 (น. 99), โดย มนตรี รูปสุวรรณ และคณะ, 2542, กรุงเทพฯ: วิญญูชน.

<sup>72</sup> รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540 มาตรา 39 บุคคลย่อมมีเสรีภาพในการแสดงความคิดเห็น การพูด การเขียน การพิมพ์ การโฆษณา และการสื่อความหมายโดยวิธีอื่น

การจำกัดเสรีภาพตามวรรคหนึ่งจะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย เฉพาะเพื่อรักษาความมั่นคงของรัฐ เพื่อคุ้มครองสิทธิ เสรีภาพ เกียรติยศ ชื่อเสียง สิทธิในครอบครัวหรือ ความเป็นอยู่ส่วนตัวของบุคคลอื่น เพื่อรักษาความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน หรือเพื่อป้องกัน หรือระงับความเสื่อมทรามทางจิตใจหรือสุขภาพของประชาชน.

<sup>73</sup> เจตนารมณ์ของรัฐธรรมนูญ รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540 (น. 106). เล่มเดิม.

### 3.3.1.3 รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550

รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550 ถือเป็นรัฐธรรมนูญแห่งราชอาณาจักรไทยฉบับแรกที่ได้กำหนดการคุ้มครองข้อมูลส่วนบุคคลไว้ โดยได้มีการจัดทำเป็นหมวดเฉพาะในหมวดที่ 3 ส่วนที่ 3 ว่าด้วยสิทธิและเสรีภาพส่วนบุคคล และบทบัญญัติอื่น ๆ โดยมีรายละเอียดดังต่อไปนี้

#### (1) การคุ้มครองข้อมูลส่วนบุคคล

รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550 ได้ประกันการคุ้มครองข้อมูลส่วนบุคคลไว้ในมาตรา 35<sup>74</sup> ของรัฐธรรมนูญฉบับดังกล่าว โดยมีการกำหนดให้สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง ตลอดจนความเป็นอยู่ส่วนตัว ย่อมได้รับความคุ้มครอง การกระทำที่เป็นการกล่าวหาหรือไขข่าวแพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชน อันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัว จะกระทำมิได้ ยกเว้นหากเป็นกรณีที่เป็นประโยชน์ต่อสาธารณะจึงจะสามารถกระทำได้

นอกจากนี้ยังได้มีการบัญญัติการคุ้มครองข้อมูลส่วนบุคคลจากการแสวงประโยชน์โดยมิชอบจากข้อมูลส่วนบุคคลที่เกี่ยวข้องกับเจ้าของข้อมูลอีกด้วยในวรรคที่สามของมาตราเดียวกันที่บัญญัติว่า บุคคลย่อมมีสิทธิได้รับความคุ้มครองจากการแสวงประโยชน์โดยมิชอบจากข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตน ทั้งนี้ ตามที่กฎหมายบัญญัติ

#### (2) การประกันสิทธิในข้อมูลส่วนบุคคล

ตามปกติแล้วประชาชนทั่วไปย่อมมีสิทธิได้รับทราบและเข้าถึงข้อมูลหรือข่าวสารสาธารณะในครอบครองของหน่วยราชการ หน่วยงานของรัฐ รัฐวิสาหกิจ หรือราชการส่วนท้องถิ่น แต่สิทธิดังกล่าวก็หาได้กว้างขวางไร้ขอบเขตแต่อย่างใด การที่ประชาชนทั่วไปจะอ้างบทบัญญัติดังกล่าวเพื่อเข้าไปรบกวนข้อมูลส่วนบุคคลของผู้อื่นเป็นเรื่องที่รัฐธรรมนูญแห่งราชอาณาจักรไทย

---

<sup>74</sup> รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550 มาตรา 35 สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง ตลอดจนความเป็นอยู่ส่วนตัว ย่อมได้รับความคุ้มครอง

การกล่าวหาหรือไขข่าวแพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชน อันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัว จะกระทำมิได้ เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณะ

บุคคลย่อมมีสิทธิได้รับความคุ้มครองจากการแสวงประโยชน์โดยมิชอบจากข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตน ทั้งนี้ ตามที่กฎหมายบัญญัติ.

พุทธศักราช 2550 ห้ามไม่ได้กระทำตามบทบัญญัติของมาตรา 56<sup>75</sup> ตอนที่บัญญัติว่า “เว้นแต่การเปิดเผยข้อมูลหรือข่าวสารนั้นจะกระทบต่อความมั่นคงของรัฐ ความปลอดภัยของประชาชน หรือส่วนได้เสียอันพึงได้รับความคุ้มครองของบุคคลอื่น หรือเป็นข้อมูลส่วนบุคคล”

แต่การประกันสิทธิในข้อมูลส่วนบุคคลดังกล่าวที่ห้ามไม่ให้มีการเปิดเผยข้อมูลส่วนบุคคลนั้นก็หาได้เป็นข้อห้ามที่เด็ดขาดแต่อย่างใด ข้อมูลส่วนบุคคลของผู้เป็นเจ้าของข้อมูลส่วนบุคคลจะสามารถเปิดเผยได้ก็แต่โดยอาศัยอำนาจของบทบัญญัติแห่งกฎหมายเท่านั้น

(3) การกำหนดให้รัฐมีหน้าที่ดำเนินการจัดทำหรือปรับปรุงกฎหมายในเรื่องกฎหมายว่าด้วยข้อมูลส่วนบุคคลตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550 มาตรา 56 ภายในหนึ่งปีนับแต่วันที่แถลงนโยบายต่อรัฐสภา

รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550 มาตรา 303 ว่าด้วยบทเฉพาะกาลได้กำหนดให้รัฐมีหน้าที่ดำเนินการจัดทำหรือปรับปรุงกฎหมายที่เกี่ยวกับการกำหนดรายละเอียดเพื่อส่งเสริมและคุ้มครองสิทธิในข้อมูลข่าวสารและการร้องเรียน รวมทั้งกฎหมายว่าด้วยข้อมูลส่วนบุคคลตามมาตรา 56

### 3.3.2 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

แม้ว่าในประเทศไทยจะไม่มีบทบัญญัติแห่งกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล มีเพียงพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 เท่านั้น ดังนั้นกฎหมายที่ว่าด้วยข้อมูลข่าวสารส่วนบุคคลจึงได้รับการบัญญัติรับรองไว้ในพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 หมวด 3

#### 3.3.2.1 หลักการและเหตุผลของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มีหลักการสำคัญประการหนึ่งในการคุ้มครองข้อมูลข่าวสารส่วนบุคคล ดังที่ปรากฏในหลักการและเหตุผลของพระราชบัญญัติข้อมูลข่าวสารของราชการ ว่า “ในระบอบประชาธิปไตย การให้ประชาชนมีโอกาสดูวงกว้างในการได้รับข้อมูลข่าวสารเกี่ยวกับการดำเนินการต่าง ๆ ของรัฐเป็นสิ่งจำเป็น เพื่อที่ประชาชนจะสามารถแสดงความคิดเห็นและใช้สิทธิทางการเมืองได้โดยถูกต้องกับความจริงอันเป็นการส่งเสริมให้มีความเป็นรัฐบาลโดยประชาชนมากยิ่งขึ้นสมควรกำหนดให้ประชาชนมีสิทธิได้รับรู้ข้อมูล

<sup>75</sup> รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550 มาตรา 56 บุคคลย่อมมีสิทธิได้รับทราบและเข้าถึงข้อมูลหรือข่าวสารสาธารณะในครอบครองของหน่วยราชการ หน่วยงานของรัฐ รัฐวิสาหกิจ หรือราชการส่วนท้องถิ่น เว้นแต่การเปิดเผยข้อมูลหรือข่าวสารนั้นจะกระทบต่อความมั่นคงของรัฐ ความปลอดภัยของประชาชน หรือส่วนได้เสียอันพึงได้รับความคุ้มครองของบุคคลอื่น หรือเป็นข้อมูลส่วนบุคคล ทั้งนี้ ตามที่กฎหมายบัญญัติ.

ข่าวสารของราชการ โดยมีข้อยกเว้นอันไม่ต้องเปิดเผยที่แจ้งชัดและจำกัดเฉพาะข้อมูลข่าวสารที่ หากเปิดเผยแล้วจะเกิดความเสียหายต่อประเทศชาติหรือต่อประโยชน์ที่สำคัญของเอกชน ทั้งนี้ เพื่อพัฒนาระบบประชาธิปไตยให้มั่นคงและจะยังผลให้ประชาชนมีโอกาสรู้ถึงสิทธิหน้าที่ของตน อย่างเต็มที่ เพื่อที่จะปกป้องรักษาประโยชน์ของตนประการหนึ่งกับสมควรคุ้มครองสิทธิส่วนบุคคล ในส่วนที่เกี่ยวข้องกับข้อมูลข่าวสารของราชการไปพร้อม อีกประการหนึ่ง”

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ได้กำหนดความหมายของข้อมูล ข่าวสารส่วนบุคคลไว้ว่า ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้นหรือมีเลขหมายรหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคน หรือรูปถ่าย และให้หมายความรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย<sup>76</sup>

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ได้วางหลักเกณฑ์ไว้โดยเฉพาะ เกี่ยวกับข้อมูลข่าวสารส่วนบุคคลเพื่อป้องกันมิให้เกิดการกระทบต่อสิทธิในความเป็นอยู่ส่วนตัว ของบุคคล เพราะปกติคนเราจะเป็นส่วนตัวในการดำรงชีวิตระดับหนึ่งที่ไม่ต้องการให้ผู้อื่น นำไปเปิดเผยต่อสาธารณชน ซึ่งอาจทำให้เกิดความไม่สบายใจหรือรำคาญใจ รวมทั้งเป็นเรื่องศักดิ์ศรี ความเป็นมนุษย์ที่พึงได้รับความคุ้มครองความเป็นส่วนตัวด้วย โดยหลักการหน่วยงานของรัฐ จะนำไปเปิดเผยโดยที่เจ้าของข้อมูลไม่ยินยอมนั้นไม่ได้ ส่วนความยินยอมสามารถจัดทำไว้ล่วงหน้า หรือจะมาเป็นครั้งคราวที่จะเปิดเผยก็ได้ขึ้นอยู่กับลักษณะของข้อมูลข่าวสาร ทั้งนี้ มีข้อยกเว้น ให้หน่วยงานของรัฐสามารถเปิดเผยข้อมูลข่าวสารส่วนบุคคลโดยไม่ต้องขอความยินยอมได้ในบาง กรณีตามที่กฎหมายกำหนด

### 3.3.2.2 สิทธิของเจ้าของข้อมูลข่าวสารส่วนบุคคล

1. เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอตรวจสอบข้อมูลข่าวสาร กรณีที่บุคคลใด บุคคลหนึ่งมีเหตุอันควรสงสัย หรือตรวจสอบพบว่าข้อมูลข่าวสารส่วนบุคคลของตนที่หน่วยงาน ของรัฐรวบรวมเก็บไว้มีข้อความส่วนใดที่ไม่ถูกต้องอยู่ด้วย พระราชบัญญัติข้อมูลข่าวสาร ของราชการ พ.ศ. 2540 นี้ ได้ให้เจ้าของข้อมูลมีสิทธิที่จะขอตรวจสอบข้อมูลข่าวสารที่เกี่ยวกับ ตนได้ เพราะกฎหมายมีเจตนารมณ์เพื่อมิให้หน่วยงานของรัฐ จัดเก็บและนำข้อมูลข่าวสาร ที่ผิดพลาดไปใช้ให้บังเกิดผลร้ายแก่บุคคล นอกจากนี้ บุคคลยังมีสิทธิสำเนาข้อมูลข่าวสารนั้นได้ด้วย ถ้าข้อมูลข่าวสารนั้นเป็นความลับหน่วยงานของรัฐอาจปฏิเสธไม่ให้ตรวจสอบได้ ทั้งนี้หน่วยงานของ

<sup>76</sup> พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540, มาตรา 4.

รัฐต้องตรวจสอบข้อมูลข่าวสารส่วนบุคคลที่จัดเก็บไว้ให้ตรงกับความเป็นจริงอยู่เสมอและพยายามเก็บข้อมูลจากเจ้าของข้อมูลโดยตรง

2. เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอแก้ไขข้อมูลข่าวสารส่วนบุคคลของตน ถ้าบุคคลใดพบว่าข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับตนส่วนใดไม่ถูกต้อง ผู้นั้นมีสิทธิทำคำขอเป็นหนังสือให้หน่วยงานของรัฐแก้ไขข้อมูลข่าวสาร นั้น ซึ่งหน่วยงานของรัฐจะต้องพิจารณาและแจ้งผลให้ผู้ยื่นทราบโดยไม่ชักช้า

3. เจ้าของข้อมูลส่วนบุคคลมีสิทธิอุทธรณ์คำสั่งไม่แก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสารส่วนบุคคลของตน ในกรณีที่หน่วยงานของรัฐไม่ยอมปฏิบัติตามคำขอแก้ไขผู้มีคำขออาจอุทธรณ์ต่อคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสาร ได้ภายในสามสิบวันนับแต่วันที่ได้รับแจ้ง ซึ่งถ้ากรรมการวินิจฉัย ฯ ได้ วินิจฉัยเช่นใดหน่วยงานของรัฐต้องปฏิบัติตาม

4. เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้หน่วยงานของรัฐหมายเหตุคำขอแก้ไขเปลี่ยนแปลงข้อมูลข่าวสารส่วนบุคคลของตนแนบไว้กับข้อมูลส่วนบุคคลนั้นได้ ไม่ว่าจะมีการอุทธรณ์คำสั่งของหน่วยงานของรัฐหรือไม่ หรือผลการพิจารณาอุทธรณ์จะเป็นเช่นใด เจ้าของผู้มีสิทธิขอให้หน่วยงานของรัฐหมายเหตุคำขอของตนแนบไว้กับข้อมูลส่วนบุคคลนั้นได้ ทั้งนี้ การให้หมายเหตุไว้เป็นวิธีการสุดท้ายกรณีที่ผู้ขอแก้ไขไม่สามารถพิสูจน์ความถูกต้องได้ชัดเจนและหน่วยงานยืนยันว่าข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความครอบครองนั้นถูกต้องสมบูรณ์แล้ว เพื่อจะเตือนให้ผู้จะนำข้อมูลข่าวสารส่วนบุคคลนั้นมาใช้ได้ตระหนักและใช้ดุลพินิจโดยระมัดระวังว่าที่ถูกต้องเป็นเช่นใด สำหรับการเปิดเผยข้อมูลข่าวสาร โดยปราศจากความยินยอมของเจ้าของข้อมูล จะทำได้ต่อเมื่อเข้าข้อยกเว้นตามที่บัญญัติไว้ในมาตรา 24 เท่านั้น เช่น การเปิดเผยต่อเจ้าหน้าที่ของรัฐในหน่วยงานของตนเพื่อนำไปใช้ตามอำนาจหน้าที่การใช้ข้อมูลตามปกติเพื่อประโยชน์ในการศึกษาวิจัยต่อหोजดหมายเหตุแห่งชาติ เพื่อป้องกันการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย เพื่อการป้องกันหรือระงับอันตรายต่อชีวิตหรือสุขภาพของบุคคลและต่อศาลและเจ้าหน้าที่ของรัฐ/หน่วยงานของรัฐรวมทั้งบุคคลที่มีอำนาจตามกฎหมายในการขอซื้อเท็จจริง เป็นต้น

### 3.3.2.3 หน้าที่ของหน่วยงานของรัฐในการคุ้มครองข้อมูลข่าวสารส่วนบุคคล

หน่วยงานของรัฐต้องปฏิบัติเกี่ยวกับการจัดระบบข้อมูลข่าวสารส่วนบุคคล ดังนี้

1. ต้องจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลเพียงเท่าที่เกี่ยวข้องและจำเป็นเพื่อการดำเนินงานของหน่วยงานของรัฐให้สำเร็จตามวัตถุประสงค์เท่านั้น และยกเลิกการจัดให้มีระบบดังกล่าวเมื่อหมดความจำเป็น

2. พยายามเก็บข้อมูลข่าวสารโดยตรงจากเจ้าของข้อมูล โดยเฉพาะอย่างยิ่งในกรณีที่จะกระทบถึงประโยชน์ได้เสียโดยตรงของบุคคลนั้น โดยในการจัดเก็บจากเจ้าของข้อมูล หน่วยงานของรัฐต้องแจ้งให้ผู้นั้นทราบถึงวัตถุประสงค์ที่จะนำข้อมูลมาใช้ ลักษณะการใช้ข้อมูลตามปกติ และต้องแจ้งให้ทราบด้วยว่าการขอข้อมูลข่าวสารนั้นเป็นการบังคับหรือไม่ เพื่อที่เจ้าของข้อมูลจะได้ทราบถึงผลกระทบจากการให้ข้อมูลข่าวสารและขอบเขตที่จะนำข้อมูลข่าวสารนั้นไปใช้ รวมทั้งให้เจ้าของข้อมูลมีอิสระที่จะตัดสินใจว่าควรให้ข้อมูลข่าวสารหรือไม่

3. จัดให้มีการพิมพ์ในราชกิจจานุเบกษาและตรวจสอบแก้ไขให้ถูกต้องอยู่เสมอเกี่ยวกับสิ่งดังต่อไปนี้

- (1) ประเภทของบุคคลที่มีการเก็บข้อมูลไว้
- (2) ประเภทของระบบข้อมูลข่าวสารส่วนบุคคล
- (3) ลักษณะการใช้ข้อมูลตามปกติ
- (4) วิธีการตรวจสอบข้อมูลข่าวสารของเจ้าของข้อมูล
- (5) วิธีการขอให้แก้ไขเปลี่ยนแปลงข้อมูล
- (6) แหล่งที่มาของข้อมูล

4) ตรวจสอบแก้ไขข้อมูลข่าวสารส่วนบุคคลในความรับผิดชอบให้ถูกต้องอยู่เสมอ

5) จัดระบบรักษาความปลอดภัยให้แก่ระบบข้อมูลข่าวสารส่วนบุคคลตามความเหมาะสมเพื่อป้องกันมิให้การนำไปใช้โดยไม่เหมาะสมหรือเป็นผลร้ายต่อเจ้าของข้อมูล

#### 3.3.2.4 การเปิดเผยข้อมูลข่าวสารส่วนบุคคล

ในการเปิดเผยข้อมูลข่าวสารส่วนบุคคลซึ่งถือหลักว่า “ปกปิดเป็นหลัก เปิดเผยเป็นข้อยกเว้น” นั้น อาจแยกพิจารณาได้ 2 กรณี คือ

กรณีที่ 1 เป็นการเปิดเผยข้อมูลข่าวสารส่วนบุคคลเป็นการเฉพาะตัวของผู้ที่เกี่ยวข้องโดยตรง

บุคคลย่อมมีสิทธิที่จะได้รู้ถึงข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับตน และเมื่อบุคคลนั้นมีคำขอเป็นหนังสือ หน่วยงานของรัฐที่ควบคุมดูแลข้อมูลข่าวสารนั้นจะต้องให้บุคคลนั้น หรือผู้กระทำการแทนบุคคลนั้น ได้ตรวจสอบหรือได้รับสำเนาข้อมูลข่าวสารส่วนบุคคลส่วนที่เกี่ยวกับบุคคลนั้น

กรณีที่ 2 เป็นการเปิดเผยข้อมูลข่าวสารส่วนบุคคลของผู้ซึ่งอาจได้รับผลกระทบจากการเปิดเผยข้อมูลข่าวสาร (บุคคลที่สาม) มีเงื่อนไข ดังนี้

เงื่อนไขแรกหากว่าหน่วยงานของรัฐจะเปิดเผยข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความควบคุมดูแลของตนต่อหน่วยงานของรัฐแห่งอื่นหรือผู้อื่น โดยปราศจากความยินยอมเป็นหนังสือของเจ้าของข้อมูลที่ให้ไว้ล่วงหน้าหรือในขณะนั้นมีได้

เงื่อนไขที่สองหากเจ้าหน้าที่ของรัฐเห็นว่า การเปิดเผยข้อมูลข่าวสารของราชการใด อาจกระทบถึงประโยชน์ได้เสียของผู้ใด ให้เจ้าหน้าที่ของรัฐแจ้งให้ผู้นั้นเสนอคำคัดค้านภายในเวลาที่กำหนด แต่ต้องให้เวลาอันสมควรที่ผู้นั้นอาจเสนอคำคัดค้านได้ ซึ่งต้องไม่น้อยกว่า 15 วัน นับแต่วันที่ได้รับแจ้ง โดยหลักแล้วหน่วยงานของรัฐจะเปิดเผยข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความควบคุมดูแลของตนต่อหน่วยงานของรัฐแห่งอื่นหรือผู้อื่น โดยปราศจากความยินยอมของเจ้าของข้อมูลที่ให้ไว้ล่วงหน้าหรือในขณะนั้นมีได้ แต่อย่างไรก็ตาม การเปิดเผยข้อมูลข่าวสารส่วนบุคคล โดยไม่ต้องได้รับความยินยอมจากผู้เป็นเจ้าของข้อมูลก่อนมีข้อยกเว้นในกรณีดังต่อไปนี้

1. เป็นการเปิดเผยต่อเจ้าหน้าที่ของรัฐในหน่วยงานของตน เพื่อการนำไปใช้ตามอำนาจหน้าที่ของหน่วยงานของรัฐแห่งนั้น
  2. เป็นการใช้ข้อมูลตามปกติภายในวัตถุประสงค์ของการจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลนั้น
  3. เป็นการเปิดเผยต่อหน่วยงานของรัฐที่ทำงานด้านการวางแผน หรือการสถิติหรือสำมะโนต่าง ๆ ซึ่งมีหน้าที่ต้องรักษาข้อมูลข่าวสารส่วนบุคคลไว้ไม่ให้เปิดเผยต่อไปยังผู้อื่น
  4. เป็นการให้เพื่อประโยชน์ในการศึกษาวิจัยโดยไม่ระบุชื่อหรือส่วนที่ทำให้รู้ว่าเป็นข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับบุคคลใด
  5. เป็นการเปิดเผยต่อหอจดหมายเหตุแห่งชาติ กรมศิลปากร หรือหน่วยงานอื่นของรัฐตามที่กำหนดในพระราชกฤษฎีกา เพื่อการตรวจสอบคุณค่าในการเก็บรักษา
  6. เป็นการเปิดเผยต่อเจ้าหน้าที่ของรัฐเพื่อการป้องกันการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย การสืบสวน การสอบสวน หรือการฟ้องคดี ไม่ว่าเป็นคดีประเภทใดก็ตาม
  7. เป็นการให้ซึ่งจำเป็นเพื่อการป้องกันหรือระงับอันตรายต่อชีวิตหรือสุขภาพของบุคคล
  8. เป็นการเปิดเผยต่อศาลและเจ้าหน้าที่ของรัฐหรือหน่วยงานของรัฐหรือบุคคลที่มีอำนาจตามกฎหมายที่จะขอข้อเท็จจริงดังกล่าว
  9. กรณีอื่นตามที่กำหนดในพระราชกฤษฎีกา
- กรณีต่าง ๆ ที่กฎหมายบัญญัติเป็นข้อยกเว้นไว้ล้วนแต่เป็นกรณีที่มีความสำคัญ เช่น เป็นการรักษาประโยชน์สาธารณะ หรือเป็นการรักษาสุขภาพหรือชีวิตของบุคคล ฯลฯ และแม้ว่ากฎหมายจะอนุญาตให้เจ้าหน้าที่ของรัฐเปิดเผยข้อมูลข่าวสารส่วนบุคคลดังกล่าวได้ แต่การ

เปิดเผยดังกล่าวก็ต้องคำนึงถึงการคุ้มครองประโยชน์ส่วนบุคคลด้วย กล่าวคือ จะต้องทำให้มีผลกระทบกระเทือน อันเกิดจากการเปิดเผยข้อมูลข่าวสารดังกล่าวแก่บุคคลให้น้อยที่สุด สรุปลักษณะสำคัญของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ปรากฏตามตารางที่ 2

ตารางที่ 3.2 หลักการสำคัญของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

ที่	หลัก	พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540
1	<p>หลักความรับผิดชอบ (Accountability)</p> <p>หน่วยงานหรือองค์กรต้องมีความรับผิดชอบต่อข้อมูลส่วนบุคคลที่อยู่ในความควบคุมของตน และต้องแต่งตั้งบุคคลหนึ่งหรือหลายคนซึ่งรับผิดชอบต่อการปฏิบัติขององค์กรตามหลักปฏิบัติต่าง ๆ ที่กำหนดในรูปแบบปฏิบัติ</p> <p>การกำหนดกระบวนการคุ้มครองข้อมูลส่วนบุคคล การกำหนดกระบวนการรับและตอบคำร้อง หรือข้อซักถาม</p>	<p>มาตรา 23 ได้รับการบัญญัติรับรองหลักความรับผิดชอบต่อไว้โดยได้กำหนดแนวทางปฏิบัติของหน่วยงานของรัฐในการจัดระบบข้อมูลข่าวสารส่วนบุคคลว่าหน่วยงานของรัฐต้องจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลเพียงพอที่เกี่ยวกับการดำเนินงานตามหน้าที่และเพียงพอที่จำเป็นเพื่อการดำเนินงานของหน่วยงานของรัฐให้สำเร็จตามวัตถุประสงค์เท่านั้น และดำเนินงานแล้วเสร็จหรือหมดความจำเป็นแล้วต้องยกเลิกการจัดให้มีระบบดังกล่าว</p> <p>นอกจากนี้หน่วยงานของรัฐยังต้องมีการประกาศกำหนดประเภทของบุคคลที่มีการเก็บข้อมูลประเภทของระบบข้อมูลข่าวสารส่วนบุคคล ลักษณะการใช้ข้อมูลตามปกติ วิธีการขอตรวจดูข้อมูลข่าวสารของเจ้าของข้อมูล วิธีการขอให้แก้ไขเปลี่ยนแปลงข้อมูล และ แหล่งที่มาของข้อมูล โดยการประกาศในราชกิจจานุเบกษา</p>

## ตารางที่ 3.2 (ต่อ)

ที่	หลัก	พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540
2	<p>หลักการแจ้งวัตถุประสงค์ (Identifying Purposes)</p> <p>องค์กรต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงวัตถุประสงค์ของการเก็บรวบรวมข้อมูลก่อนหรือในขณะทำการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น</p>	<p>มาตรา 23 วรรคสอง ได้รับการบัญญัติรับรองหลักการแจ้งวัตถุประสงค์โดยการกำหนดว่าในกรณีที่หน่วยงานของรัฐจะดำเนินการจัดเก็บข้อมูลข่าวสารส่วนบุคคลโดยตรงจากเจ้าของข้อมูล หน่วยงานของรัฐต้องแจ้งให้เจ้าของข้อมูลทราบล่วงหน้าหรือพร้อมกับการขอข้อมูล โดยหน่วยงานของรัฐต้องแจ้งให้เจ้าของข้อมูลทราบถึงวัตถุประสงค์ที่จะนำข้อมูลมาใช้ ลักษณะการใช้ข้อมูลตามปกติ และกรณีที่ขอข้อมูลนั้นเป็นกรณีที่อาจให้ข้อมูลได้โดยความสมัครใจหรือเป็นกรณีมีกฎหมายบังคับ</p>
3	<p>หลักความยินยอม (Consent)</p> <p>บุคคลที่ให้ข้อมูลส่วนบุคคลต้องได้รับทราบและให้ความยินยอมแก่การเก็บรวบรวมการใช้หรือการเปิดเผยข้อมูลส่วนบุคคลของบุคคลนั้น ทั้งนี้ เว้นแต่เป็นกรณีที่ไม่สมควรตามที่กำหนดในกฎหมายรูปแบบของความยินยอมอาจแตกต่างกันไปขึ้นอยู่กับสถานการณ์และประเภทของข้อมูล</p>	<p>มาตรา 23 ได้บัญญัติให้หน่วยงานของรัฐต้องปฏิบัติเกี่ยวกับการจัดระบบข้อมูลข่าวสารส่วนบุคคล โดยกำหนดให้พยายามเก็บข้อมูลข่าวสารโดยตรงจากเจ้าของข้อมูล โดยเฉพาะอย่างยิ่งในกรณีที่กระทบถึงประโยชน์ได้เสียโดยตรงของบุคคลนั้น</p> <p>และมาตรา 23 วรรคสาม ยังได้บัญญัติว่าหน่วยงานของรัฐต้องแจ้งให้เจ้าของข้อมูลทราบในกรณีมีการให้จัดส่งข้อมูลข่าวสารส่วนบุคคลไปยังที่ใดซึ่งจะเป็นผลให้บุคคลทั่วไปทราบข้อมูลข่าวสารนั้นได้ เว้นแต่เป็นไปตามลักษณะการใช้ข้อมูลตามปกติ</p> <p>นอกจากนี้ มาตรา 24 ยังได้บัญญัติว่าหน่วยงานของรัฐจะเปิดเผยข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความควบคุมดูแลของตนต่อหน่วยงานของรัฐแห่งอื่นหรือผู้อื่น โดยปราศจากความยินยอมเป็นหนังสือของเจ้าของข้อมูลที่ให้ไว้ล่วงหน้าหรือในขณะนั้นมีได้ เว้นแต่เป็นการเปิดเผยตามที่กฎหมายบัญญัติไว้</p>

## ตารางที่ 3.2 (ต่อ)

ที่	หลัก	พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540
4	<p>หลักการเก็บรวบรวมข้อมูลอย่างจำกัด</p> <p>การเก็บรวบรวมข้อมูลส่วนบุคคลจะต้องจำกัดเฉพาะแต่ข้อมูลที่จำเป็นและเป็นไปตามวัตถุประสงค์ขององค์กรที่ได้แจ้งให้ทราบและต้องเก็บรวบรวมโดยวิธีการที่เป็นธรรม และขอด้วยกฎหมายขององค์กรจะต้องไม่เก็บรวบรวมข้อมูลส่วนบุคคลโดยวิธีที่เป็นการเลือกปฏิบัติ</p>	<p>มาตรา 23 วรรคหนึ่ง (1) บัญญัติว่าหน่วยงานของรัฐต้องจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลเพียงเท่าที่เพียงพอ และจำเป็นเพื่อการดำเนินงานของหน่วยงานของรัฐให้สำเร็จตามวัตถุประสงค์เท่านั้น และยกเลิกการจัดให้มีระบบดังกล่าวเมื่อหมดความจำเป็น</p>
5	<p>หลักการจำกัดการใช้ การเปิดเผย และการเก็บรักษา</p> <p>องค์กรจะต้องไม่นำข้อมูลส่วนบุคคลไปใช้ หรือเปิดเผย เพื่อวัตถุประสงค์ อย่างอื่นนอกเหนือจากวัตถุประสงค์ของการเก็บรวบรวมข้อมูลนั้น เว้นแต่จะได้รับความยินยอมของบุคคลธรรมดาคนนั้นหรือเป็นไปตามที่กฎหมายกำหนด และข้อมูลส่วนบุคคลจะต้องถูกเก็บรักษาไว้ ในระยะเวลาเพียงเท่าที่จำเป็น สำหรับการดำเนินการตามวัตถุประสงค์ดังกล่าวเท่านั้น</p>	<p>มาตรา 24 บัญญัติว่า หน่วยงานของรัฐจะเปิดเผยข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความควบคุมดูแลของตนต่อหน่วยงานของรัฐแห่งอื่นหรือผู้อื่นโดยปราศจากความยินยอมเป็นหนังสือของเจ้าของข้อมูลที่ให้ไว้ล่วงหน้าหรือในขณะนั้นมิได้ เว้นแต่เป็นการเปิดเผยดังต่อไปนี้</p> <p>(1) เป็นการเปิดเผยต่อเจ้าหน้าที่ของรัฐในหน่วยงานของตน เพื่อการนำไปใช้ตามอำนาจหน้าที่ของหน่วยงานของรัฐแห่งนั้น</p> <p>(2) เป็นการ ใช้ข้อมูลตามปกติภายใน วัตถุประสงค์ของการจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลนั้น</p> <p>(3) เป็นการเปิดเผยต่อหน่วยงานของรัฐที่ทำงานด้านการวางแผน หรือการสถิติหรือสำมะโนต่าง ๆ ซึ่งมีหน้าที่ต้องรักษาข้อมูลข่าวสารส่วนบุคคลไว้ไม่ให้เปิดเผยต่อไปยังผู้อื่น</p>

## ตารางที่ 3.2 (ต่อ)

ที่	หลัก	พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540
		<p>(4) เป็นการให้เพื่อประโยชน์ในการศึกษาวิจัย โดยไม่ระบุชื่อหรือส่วนที่ทำให้รู้ว่าเป็นข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับบุคคลใด</p> <p>(5) เป็นการเปิดเผยต่อหอจดหมายเหตุแห่งชาติ กรมศิลปากร หรือหน่วยงานอื่นของรัฐตามที่กำหนดในพระราชกฤษฎีกา เพื่อการตรวจคุณค่าในการเก็บรักษา</p> <p>(6) เป็นการเปิดเผยต่อเจ้าหน้าที่ของรัฐเพื่อการป้องกันการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย การสืบสวน การสอบสวน หรือการฟ้องคดี ไม่ว่าเป็นคดีประเภทใดก็ตาม</p> <p>(7) เป็นการให้ซึ่งจำเป็นเพื่อการป้องกันหรือระงับอันตรายต่อชีวิตหรือสุขภาพของบุคคล</p> <p>(8) เป็นการเปิดเผยต่อศาลและเจ้าหน้าที่ของรัฐ หรือหน่วยงานของรัฐหรือบุคคลที่มีอำนาจตามกฎหมายที่จะขอข้อเท็จจริงดังกล่าว</p> <p>(9) กรณีอื่นตามที่กำหนดในพระราชกฤษฎีกา</p>

## ตารางที่ 3.2 (ต่อ)

ที่	หลัก	พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540
6	<p>หลักความถูกต้อง (Accuracy)</p> <p>ข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้จะต้องถูกต้อง สมบูรณ์ และเป็นปัจจุบันตามความจำเป็นเพื่อวัตถุประสงค์ของการนำข้อมูลนั้นไปใช้ หลักการที่ว่าข้อมูลส่วนบุคคลต้องถูกต้อง สมบูรณ์ และเป็นปัจจุบันต้องคำนึงถึงสัดส่วนของส่วนได้เสียของเจ้าของข้อมูล ทั้งนี้เพื่อที่จะลดความเป็นไปได้ของการนำข้อมูลที่ไม่ถูกต้องไปใช้</p>	<p>มาตรา 23 วรรคหนึ่ง (3) บัญญัติว่าหน่วยงานของรัฐต้องจัดให้มีการพิมพ์ในราชกิจจานุเบกษา และตรวจสอบแก้ไขให้ถูกต้องอยู่เสมอเกี่ยวกับสิ่งดังต่อไปนี้</p> <ol style="list-style-type: none"> <li>(1) ประเภทของบุคคลที่มีการเก็บข้อมูลไว้</li> <li>(2) ประเภทของระบบข้อมูลข่าวสารส่วนบุคคล</li> <li>(3) ลักษณะการใช้ข้อมูลตามปกติ</li> <li>(4) วิธีการขอตรวจดูข้อมูลข่าวสารของเจ้าของข้อมูล</li> <li>(5) วิธีการขอให้แก้ไขเปลี่ยนแปลงข้อมูล</li> <li>(6) แหล่งที่มาของข้อมูล</li> </ol> <p>และมาตรา 23 วรรคหนึ่ง (4) บัญญัติว่าหน่วยงานของรัฐต้องตรวจสอบแก้ไขข้อมูลข่าวสารส่วนบุคคลในความรับผิดชอบให้ถูกต้องอยู่เสมอ</p>
7	<p>หลักการรักษาความปลอดภัย (Safeguards)</p> <p>ข้อมูลส่วนบุคคลจะต้องได้รับการรักษาความปลอดภัยที่เหมาะสมกับข้อมูลส่วนบุคคล โดยเฉพาะการรักษาความปลอดภัยจะต้องให้ความคุ้มครองข้อมูลส่วนบุคคลต่อการสูญหายหรือการโจรกรรม ตลอดจนการเข้าตรวจดู การเปิดเผย การทำซ้ำ การใช้ หรือการแก้ไขเพิ่มเติมโดยไม่ได้รับอนุญาต</p>	<p>มาตรา 23 วรรคหนึ่ง (5) บัญญัติว่าหน่วยงานของรัฐต้องจัดระบบรักษาความปลอดภัยให้แก่ระบบข้อมูลข่าวสารส่วนบุคคล ตามความเหมาะสม เพื่อป้องกันมิให้มีการนำไปใช้โดยไม่เหมาะสมหรือเป็นผลร้ายต่อเจ้าของข้อมูล</p>

## ตารางที่ 3.2 (ต่อ)

ที่	หลัก	พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540
8	<p>หลักการเปิดเผย (Openness)</p> <p>องค์กรต้องจัดทำนโยบายและแนวทางปฏิบัติขององค์กรในการจัดการข้อมูลส่วนบุคคล กล่าวคือ การจัดการวิธีการเข้าถึงข้อมูลหรือจัดข้อมูลที่ต้องเผยแพร่แก่ประชาชนในสถานที่และวิธีการที่เหมาะสม บุคคลทั่วไปจะต้องสามารถได้รับข้อมูลนั้นได้โดยไม่ลำบากและข้อมูลดังกล่าวจะต้องเปิดเผยในลักษณะที่สามารถเข้าใจได้โดยทั่วไป</p>	<p>มาตรา 25 บัญญัติรับรองสิทธิของบุคคลในการจะรับรู้ถึงข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับตน และเมื่อบุคคลนั้นมีคำขอเป็นหนังสือ หน่วยงานของรัฐที่ควบคุมดูแลข้อมูลข่าวสารนั้นจะต้องให้บุคคลนั้นหรือผู้กระทำการแทนบุคคลนั้นได้ตรวจดูหรือได้รับสำเนาข้อมูลข่าวสารส่วนบุคคลส่วนที่เกี่ยวกับบุคคลนั้น</p>
9	<p>หลักการเข้าตรวจดูข้อมูลของบุคคล (Individual Access)</p> <p>เมื่อมีการร้องขอ บุคคลผู้เป็นเจ้าของข้อมูลจะต้องได้รับการรายงานหรือเข้าตรวจดูเกี่ยวกับการมีอยู่การใช้หรือการเปิดเผยข้อมูลส่วนบุคคลของตน นอกจากนี้ บุคคลสามารถโต้แย้งหากพบว่าข้อมูลดังกล่าวไม่ถูกต้องหรือสมบูรณ์ และมีสิทธิเรียกร้องให้มีการแก้ไขเพิ่มเติมข้อมูลนั้นได้ตามความเหมาะสม</p>	<p>มาตรา 25 บัญญัติรับรองสิทธิของบุคคลในการจะรับรู้ถึงข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับตน และเมื่อบุคคลนั้นมีคำขอเป็นหนังสือ หน่วยงานของรัฐที่ควบคุมดูแลข้อมูลข่าวสารนั้นจะต้องให้บุคคลนั้นหรือผู้กระทำการแทนบุคคลนั้นได้ตรวจดูหรือได้รับสำเนาข้อมูลข่าวสารส่วนบุคคลส่วนที่เกี่ยวกับบุคคลนั้น</p> <p>และในวรรคสามบัญญัติว่า ถ้าบุคคลใดเห็นว่าข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับตนส่วนใดไม่ถูกต้องตามที่ป็นจริง ให้มีสิทธิยื่นคำขอเป็นหนังสือให้หน่วยงานของรัฐที่ควบคุมดูแลข้อมูลข่าวสารแก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสารส่วนนั้นได้ ซึ่งหน่วยงานของรัฐจะต้องพิจารณาคำขอดังกล่าว และแจ้งให้บุคคลนั้นทราบโดยไม่ชักช้า</p>

## ตารางที่ 3.2 (ต่อ)

ที่	หลัก	พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540
10	<p>หลักการโต้แย้งการปฏิบัติขององค์กร บุคคลผู้เป็นเจ้าของข้อมูลสามารถ ทำคำโต้แย้งเกี่ยวกับการดำเนินการ เกี่ยวกับข้อมูลข่าวสารที่เกี่ยวกับตน โดยการทำคำโต้แย้งไปยังบุคคลที่ ได้รับแต่งตั้งให้เป็นผู้รับผิดชอบการ ปฏิบัติหน้าที่ขององค์กรได้</p> <p>โดยองค์กรจะต้องแจ้งหรืออธิบาย ให้บุคคลทราบเกี่ยวกับกระบวนการ ร้องเรียน การรับคำร้อง และการตอบ ข้อซักถาม และต้องทำการสอบสวน เกี่ยวกับคำร้องทั้งหลาย และในกรณีที่ คำร้องนั้นมีเหตุอันสมควร องค์กร จะต้องมีการดำเนินการที่เหมาะสม รวมทั้งการแก้ไขเพิ่มเติม หรือมี มาตรการที่เหมาะสมเกี่ยวกับนโยบาย และแนวทางปฏิบัติขององค์กรที่ จำเป็น</p>	<p>มาตรา 33 บัญญัติว่า ในกรณีที่หน่วยงานของ รัฐปฏิเสธว่าไม่มีข้อมูลข่าวสารตามที่มิคำขอไม่ว่า จะเป็นกรณีมาตรา 11 หรือมาตรา 25 ถ้าผู้มีคำขอไม่ เชื่อว่าเป็นความจริงและร้องเรียนต่อคณะกรรมการ ตามมาตรา 13 ให้คณะกรรมการมีอำนาจเข้า ดำเนินการตรวจสอบข้อมูลข่าวสารของราชการที่ เกี่ยวข้องกับได้ และแจ้งผลการตรวจสอบให้ผู้ร้องเรียน ทราบ</p> <p>หน่วยงานของรัฐหรือเจ้าหน้าที่ของรัฐต้อง ยินยอมให้คณะกรรมการหรือผู้ซึ่งคณะกรรมการ มอบหมายเข้าตรวจสอบข้อมูลข่าวสารที่อยู่ในความ ครอบครองของตนได้ ไม่ว่าจะเป็ข้อมูลข่าวสารที่ เปิดเผยได้หรือไม่ก็ตาม</p>

## 3.3.3 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 เป็นกฎหมายอีกฉบับหนึ่ง  
ที่มีเนื้อหาเกี่ยวข้องกับข้อมูลส่วนบุคคลของประชาชน ในส่วนนี้ผู้เขียนจะทำการอธิบายให้ทราบถึง  
รายละเอียดของพระราชบัญญัติฉบับดังกล่าวที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของประชาชนโดยมี  
รายละเอียดดังต่อไปนี้

### 3.3.3.1 หลักการและเหตุผลของพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

โดยที่การทำธุรกรรมในปัจจุบันมีแนวโน้มที่จะปรับเปลี่ยนวิธีการในการติดต่อสื่อสารที่อาศัยการพัฒนาเทคโนโลยีทางอิเล็กทรอนิกส์ซึ่งมีความสะดวก รวดเร็วและมีประสิทธิภาพ แต่เนื่องจากการทำธุรกรรมทางอิเล็กทรอนิกส์ดังกล่าวมีความแตกต่างจากวิธีการทำธุรกรรมซึ่งมีกฎหมายรองรับอยู่ในปัจจุบันเป็นอย่างมาก อันส่งผลให้ต้องมีการรองรับสถานะทางกฎหมายของข้อมูลทางอิเล็กทรอนิกส์ให้เสมือนกับการทำเป็นหนังสือ หรือหลักฐานเป็นหนังสือ การรับรองวิธีการส่งและรับข้อมูลอิเล็กทรอนิกส์ การใช้ลายมือชื่ออิเล็กทรอนิกส์ ตลอดจนการรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ เพื่อเป็นการส่งเสริมการทำธุรกรรมทางอิเล็กทรอนิกส์ให้น่าเชื่อถือ และมีผลในทางกฎหมายเช่นเดียวกับการทำธุรกรรมโดยวิธีการทั่วไปที่เคยปฏิบัติอยู่เดิมควรกำหนดให้มีคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ทำหน้าที่วางนโยบายกำหนดหลักเกณฑ์เพื่อส่งเสริมการทำธุรกรรมทางอิเล็กทรอนิกส์ ติดตามดูแลการประกอบธุรกิจเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ รวมทั้งมีหน้าที่ในการส่งเสริมการพัฒนาการทางเทคโนโลยีเพื่อติดตามความก้าวหน้าของเทคโนโลยี ซึ่งมีการเปลี่ยนแปลงและพัฒนาศักยภาพตลอดเวลาให้มีมาตรฐานน่าเชื่อถือ ตลอดจนเสนอแนะแนวทางแก้ไขปัญหาและอุปสรรคที่เกี่ยวข้อง อันจะเป็นการส่งเสริมการใช้ธุรกรรมทางอิเล็กทรอนิกส์ทั้งภายในประเทศและระหว่างประเทศ ด้วยการมีกฎหมายรองรับในลักษณะที่เป็นเอกกรูปร่าง และสอดคล้องกับมาตรฐานที่นานาประเทศยอมรับ

### 3.3.3.2 ขอบเขตการใช้บังคับพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

ขอบเขตการใช้บังคับพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 เป็นไปตามมาตรา 3 แห่งพระราชบัญญัติดังกล่าว กล่าวคือ พระราชบัญญัตินี้ใช้บังคับแก่ธุรกรรมในทางแพ่งและพาณิชย์ที่ดำเนินการโดยใช้ข้อมูลอิเล็กทรอนิกส์<sup>77</sup> ได้แก่ คำขอการอนุญาต การจดทะเบียน คำสั่งทางปกครอง การชำระเงิน การประกาศหรือการดำเนินการใด ๆ ตามกฎหมายกับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ ถ้าได้กระทำในรูปของข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่กำหนดโดยพระราชกฤษฎีกา ให้นำพระราชบัญญัตินี้มาใช้บังคับและให้ถือว่า มีผลโดยชอบด้วยกฎหมายเช่นเดียวกับการดำเนินการตามหลักเกณฑ์และวิธีการที่กฎหมายในเรื่องนั้นกำหนด<sup>78</sup>

<sup>77</sup> พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544, มาตรา 3.

<sup>78</sup> พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544, มาตรา 35.

ข้อยกเว้นของการนำเอาพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 คือธุรกรรมที่มีพระราชกฤษฎีกากำหนดมิให้นำพระราชบัญญัตินี้ทั้งหมดหรือแต่บางส่วนมาใช้ บังคับและกฎหมายหรือกฎใดที่กำหนดขึ้นเพื่อคุ้มครองผู้บริโภค

3.3.3.3 การคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

การคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 นั้น ปรากฏตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553 เพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานของรัฐมีความมั่นคงปลอดภัย ความน่าเชื่อถือ และมีการคุ้มครองข้อมูลส่วนบุคคลที่เป็นไปตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงได้กำหนดแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐให้มีมาตรฐานเดียวกัน โดยอาศัยอำนาจตามความในมาตรา 6 แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 ซึ่งบัญญัติว่า “ในกรณีที่หน่วยงานของรัฐมีการรวบรวม จัดเก็บ ใช้ หรือเผยแพร่ข้อมูลหรือข้อเท็จจริงที่ทำให้สามารถระบุตัวบุคคล ไม่ว่าจะโดยตรงหรือโดยอ้อมให้หน่วยงานของรัฐจัดทำแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล”

ดังนั้น คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงออก “ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553” เพื่อให้หน่วยงานของรัฐให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลด้วยการจัดทำแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553 เป็นกฎหมายที่ถูกตราขึ้นมาโดยอาศัยอำนาจของพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ที่กำหนดมาตรการคุ้มครองสิทธิของบุคคลในฐานะที่เป็นผู้ใช้บริการโทรคมนาคม โดยกำหนดให้หน่วยงานของรัฐซึ่งเป็นผู้รวบรวม จัดเก็บ ใช้ เผยแพร่ หรือดำเนินการอื่นใดเกี่ยวกับข้อมูลของผู้ใช้บริการต้องมีการจัดทำนโยบายในการคุ้มครองข้อมูลส่วนบุคคลไว้เป็นลายลักษณ์อักษร โดยมีสาระสำคัญ ดังนี้

### 1) ขอบเขตของการรวบรวมข้อมูลส่วนบุคคล

การเก็บรวบรวมข้อมูลส่วนบุคคลต้องเป็นการกระทำอย่างจำกัด โดยต้องกำหนดให้มีขอบเขตสำหรับการจัดเก็บข้อมูลอย่างจำกัด และการจัดเก็บข้อมูลนั้นต้องใช้วิธีการที่ชอบด้วยกฎหมายและเป็นธรรม อีกทั้งยังต้องแจ้งให้เจ้าของข้อมูลทราบหรือได้รับความยินยอมจากเจ้าของข้อมูลด้วย โดยข้อมูลที่จัดเก็บนั้น ต้องเป็นข้อมูลที่มีคุณภาพของ กล่าวคือ ต้องเป็นข้อมูลส่วนบุคคลที่มีความถูกต้องและต้องรวบรวมจัดเก็บให้เป็นไปตามอำนาจหน้าที่โดยชอบด้วยกฎหมายของผู้จัดเก็บข้อมูลดังกล่าวด้วย

### 2) วัตถุประสงค์ในการเก็บข้อมูลส่วนบุคคล

การจัดเก็บข้อมูลส่วนบุคคลนั้นต้องมีการระบุวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลด้วย โดยต้องมีการบันทึกวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลในขณะที่มีการรวบรวมในปัจจุบันและหากมีการนำเอาข้อมูลส่วนบุคคลที่ได้มีการรวบรวมไว้ไปใช้ในภายหลังก็จำเป็นที่จะต้องมีการบันทึกให้ทราบถึงวัตถุประสงค์ที่จะนำไปใช้ด้วย

### 3) ข้อจำกัดของการนำข้อมูลส่วนบุคคลไปใช้

สำหรับข้อจำกัดในการนำข้อมูลส่วนบุคคล ไปใช้นั้นประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553 กำหนดห้ามมิให้มีการเปิดเผย หรือแสดง หรือทำให้ปรากฏในลักษณะอื่นใดซึ่งข้อมูลส่วนบุคคลที่ไม่สอดคล้องกับวัตถุประสงค์ของการรวบรวมและจัดเก็บข้อมูล เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูล หรือเป็นกรณีที่มีกฎหมายกำหนดให้กระทำได้

### 4) การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

การรักษาความมั่นคงปลอดภัยให้มีมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสมเพื่อป้องกันการสูญหาย การเข้าถึง ทำลาย รั่วไหล แคล้ง แก้ไขหรือเปิดเผยข้อมูลโดยมิชอบ โดยให้หน่วยงานของรัฐซึ่งรวบรวมข้อมูลส่วนบุคคลผ่านทางเว็บไซต์ จัดให้มีวิธีการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคลที่รวบรวมและจัดเก็บไว้ให้เหมาะสมกับการรักษาความลับของข้อมูลส่วนบุคคล เพื่อป้องกันการเปลี่ยนแปลงแก้ไขข้อมูลดังกล่าวโดยมิชอบ รวมถึงการป้องกันการกระทำใดที่จะมีผลทำให้ข้อมูลไม่อยู่ในสภาพพร้อมใช้งาน ซึ่งหน่วยงานของรัฐพึงดำเนินการ ดังนี้

1. สร้างเสริมความสำนึกในการรับผิดชอบด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้แก่บุคลากร พนักงาน หรือลูกจ้างของหน่วยงานด้วยการเผยแพร่ข้อมูลข่าวสาร ให้ความรู้ จัดสัมมนา หรือฝึกอบรมในเรื่องดังกล่าวให้แก่บุคลากรในองค์กรเป็นประจำ

2. กำหนดสิทธิและข้อจำกัดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของบุคลากร พนักงาน หรือลูกจ้างของตนในแต่ละลำดับชั้นให้ชัดเจน และให้มีการบันทึกรวมทั้งการทำสำรองข้อมูลของการเข้าถึงหรือการเข้าใช้งานข้อมูลส่วนบุคคลไว้ในระยะเวลาที่เหมาะสมหรือตามระยะเวลาที่กฎหมายกำหนด

3. ตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของเว็บไซต์หรือของระบบสารสนเทศทั้งหมดอย่างน้อยปีละ 1 ครั้ง

4. กำหนดให้มีการใช้มาตรการที่เหมาะสมและเป็นการเฉพาะสำหรับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่มีความสำคัญยิ่งหรือเป็นข้อมูลที่อาจกระทบต่อความรู้สึก ความเชื่อ ความสงบเรียบร้อย และศีลธรรมอันดีของประชาชนซึ่งเป็นผู้ใช้บริการของหน่วยงานของรัฐ หรืออาจก่อให้เกิดความเสียหาย หรือมีผลกระทบต่อสิทธิเสรีภาพของผู้เป็นเจ้าของข้อมูลอย่างชัดเจน เช่น หมายเลขบัตรเดบิต หรือบัตรเครดิต หมายเลขประจำตัวประชาชน หรือหมายเลขประจำตัวบุคคล เชื้อชาติ ศาสนา ความเชื่อ ความคิดเห็นทางการเมือง สุขภาพ พฤติกรรมทางเพศ เป็นต้น

5. ควรจัดให้มีมาตรการที่รอบคอบในการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคลของบุคคลซึ่งอายุไม่เกินสิบแปดปีโดยใช้วิธีการ โดยเฉพาะและเหมาะสม

5) การมีส่วนร่วมของเจ้าของข้อมูลส่วนบุคคล

การมีส่วนร่วมของเจ้าของข้อมูลส่วนบุคคล ประกาศฉบับนี้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งถึงความมีอยู่ หรือรายละเอียดของข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลเมื่อได้รับคำร้องขอภายในระยะเวลาอันสมควรตามวิธีการในรูปแบบ รวมถึงค่าใช้จ่ายตามสมควร และห้ามไม่ให้ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธ ที่จะให้คำชี้แจงหรือให้ข้อมูลแก่เจ้าของข้อมูล ผู้สืบสิทธิ์ ทายาท ผู้แทนโดยชอบธรรม หรือผู้พิทักษ์ตามกฎหมาย โดยให้ผู้ควบคุมข้อมูลจัดทำบันทึกคำคัดค้าน การจัดเก็บ ความถูกต้อง หรือการกระทำใด ๆ เกี่ยวกับข้อมูลของเจ้าของข้อมูลไว้เป็นหลักฐานด้วย

6) การแสดงระบุมความเชื่อมโยงให้ข้อมูลส่วนบุคคลกับหน่วยงานหรือองค์กรอื่น

การเก็บรวบรวมข้อมูลผ่านทางเว็บไซต์ของหน่วยงานของรัฐและเว็บไซต์ดังกล่าวที่มีการเชื่อมโยงให้ข้อมูลแก่หน่วยงานหรือองค์กรอื่น ให้หน่วยงานของรัฐแสดงไว้อย่างชัดเจนถึงชื่อผู้เก็บรวบรวมข้อมูลผ่านทางเว็บไซต์ หรือชื่อผู้มีสิทธิในข้อมูลที่ได้มีการเก็บรวบรวม (Data Subject) และชื่อเป็นผู้มีสิทธิเข้าถึงข้อมูลดังกล่าวทั้งหมด รวมถึงประเภทของข้อมูลที่จะใช้ร่วมกับหน่วยงานหรือองค์กรนั้น ๆ ตลอดจนชื่อผู้มีหน้าที่ปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้ผู้ใช้บริการทราบ ให้หน่วยงาน

ของรัฐแจ้งให้ผู้ใช้บริการทราบและให้ความยินยอมล่วงหน้าก่อนทำการเปลี่ยนแปลงการเชื่อมโยงข้อมูลตามวรรคแรกกับหน่วยงานหรือองค์กรอื่น

7) การรวมข้อมูลจากที่มาหลาย ๆ แห่ง

ให้หน่วยงานของรัฐที่ซึ่งได้รับข้อมูลมาจากผู้ใช้บริการเว็บไซต์ และจะนำไปรวมเข้ากับข้อมูลของบุคคลดังกล่าวที่ได้รับจากที่มาแห่งอื่น ระบุไว้ในนโยบายคุ้มครองข้อมูลส่วนบุคคลถึงเจตนารมณ์การรวมข้อมูลดังกล่าวด้วย เช่น เว็บไซต์ได้รับข้อมูลที่เป็นชื่อและที่อยู่ของการส่งจดหมายอิเล็กทรอนิกส์จากผู้ใช้บริการ โดยการกรอกข้อมูลตามแบบสอบถามผ่านทางเว็บไซต์ และจะนำข้อมูลดังกล่าวไปรวมเข้ากับข้อมูลเกี่ยวกับประวัติของผู้ใช้บริการที่ได้รับจากที่มาแห่งอื่น

สำหรับการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ โดยในประกาศฯ ต้องมีสาระสำคัญอย่างน้อยประกอบด้วย 2 ส่วน ได้แก่

1) นโยบายการคุ้มครองข้อมูลส่วนบุคคล

การจัดทำนโยบายในการคุ้มครองข้อมูลส่วนบุคคล มีวัตถุประสงค์เพื่อเป็นการแจ้งให้กับผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐกับหน่วยงานได้ทราบว่า หน่วยงานมีแนวทางในการบริหารจัดการข้อมูลส่วนบุคคลของผู้ใช้บริการซึ่งเป็นเจ้าของข้อมูลอย่างไร เพื่อให้ผู้ใช้บริการทราบและสามารถตัดสินใจได้ว่าสมควรให้ข้อมูลส่วนบุคคลของตนหรือไม่ เพื่อให้สอดคล้องเป็นไปตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553

ในส่วนของนโยบายฯ จะต้องมีหัวข้อหลักที่เป็นสาระสำคัญอย่างน้อย 8 ข้อ ดังนี้

1. การเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด
  2. คุณภาพของข้อมูลส่วนบุคคล
  3. การระบุวัตถุประสงค์ในการเก็บรวบรวม
  4. ข้อจำกัดในการนำข้อมูลส่วนบุคคลไปใช้
  5. การรักษาความมั่นคงปลอดภัย
  6. การเปิดเผยเกี่ยวกับการดำเนินการแนวปฏิบัติและนโยบายที่เกี่ยวกับข้อมูลส่วนบุคคล
  7. การมีส่วนร่วมของเจ้าของข้อมูล
  8. ความรับผิดชอบของบุคคลซึ่งทำหน้าที่ควบคุมข้อมูล
- 2) แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

การจัดทำแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลมีวัตถุประสงค์เพื่อเป็นการประกาศให้กับบุคลากรในหน่วยงานปฏิบัติตามนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการ ทั้งนี้ แนวปฏิบัติต้องแสดงถึงขั้นตอนและวิธีการดำเนินการเพื่อให้

บุคลากรซึ่งเป็นผู้ปฏิบัติสามารถปฏิบัติได้อย่างถูกต้อง เพื่อให้สอดคล้องเป็นไปตามประกาศคณะกรรมการฯ จะต้องมีความเข้าใจหลักที่เป็นสาระสำคัญใน แนวปฏิบัติอย่างน้อย 9 ข้อ ดังนี้

1. ข้อมูลเบื้องต้น
2. การเก็บรวบรวม จัดประเภท และการใช้ข้อมูลส่วนบุคคล
3. การแสดงระบุมความเชื่อมโยงให้ข้อมูลส่วนบุคคลกับหน่วยงานหรือองค์กรอื่น
4. การรวมข้อมูลจากที่มาหลาย ๆ แห่ง
5. การให้บุคคลอื่นใช้หรือการเปิดเผยข้อมูลส่วนบุคคล
6. การรวบรวม จัดเก็บ ใช้และการเปิดเผยข้อมูลเกี่ยวกับผู้ใช้บริการ
7. การเข้าถึง การแก้ไขให้ถูกต้อง และการปรับปรุงให้เป็นปัจจุบัน
8. การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล
9. การติดต่อกับเว็บไซต์

กรอบในการคุ้มครองข้อมูลส่วนบุคคลที่นิยมของสากลประเทศและประเทศไทย ใช้นามอ้างอิงเป็นแนวทางในการดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลที่อยู่ในรูปของข้อมูล อิเล็กทรอนิกส์ซึ่งข้อมูลส่วนบุคคลต้องได้รับการคุ้มครองที่เหมาะสมในทุกขั้นตอนตั้งแต่ การเก็บ รวบรวม การเก็บรักษา และการเปิดเผย คือ กรอบในการคุ้มครองข้อมูลขององค์การร่วมมือและ พัฒนาทางเศรษฐกิจ (OECD : The Organization for Economic Cooperation and Development) ในเรื่อง Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data มีหลักการพื้นฐาน 8 ประการ<sup>79</sup> ดังปรากฏในตารางที่ 3

ตารางที่ 3.3 กรอบในการคุ้มครองข้อมูลของ OECD

ที่	กรอบ OECD	สาระสำคัญ
1	หลักข้อจำกัดในการเก็บรวบรวมข้อมูล	ในการเก็บรวบรวมข้อมูลนั้น ต้องชอบด้วย กฎหมายและต้องใช้วิธีการที่เป็นธรรมและ เหมาะสม โดยในการเก็บรวบรวมข้อมูลนั้นต้อง ให้เจ้าของข้อมูลรู้เห็นรับรู้หรือได้รับความ ยินยอมจากเจ้าของข้อมูล

<sup>79</sup> คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์. (ม.ป.ป.). การคุ้มครองข้อมูลส่วนบุคคล (Data Privacy). สืบค้น 24 มีนาคม 2559, จาก <http://www.etcommission.go.th/files/article/article-dp.pdf>

ตารางที่ 3.3 (ต่อ)

ที่	กรอบ OECD	สาระสำคัญ
2	หลักคุณภาพของข้อมูล	ข้อมูลที่เกี่ยวข้องกับวัตถุประสงค์ที่กำหนดขึ้นว่า “จะนำไปใช้ทำอะไร” และเป็นไปตามอำนาจหน้าที่และวัตถุประสงค์ในการดำเนินงานของหน่วยงานตามที่กฎหมายกำหนด นอกจากนั้นข้อมูลดังกล่าวจะต้องถูกต้อง สมบูรณ์หรือทำให้เป็นปัจจุบันหรือทันสมัยอยู่เสมอ
3	หลักการกำหนดวัตถุประสงค์ในการจัดเก็บ	ต้องกำหนดวัตถุประสงค์ว่าข้อมูลที่มีการเก็บรวบรวมนั้นเก็บรวบรวมไปเพื่ออะไร พร้อมทั้งกำหนดระยะเวลาที่เก็บรวบรวมหรือรักษาข้อมูลนั้น ตลอดจนกรณีที่ต้องมีการเปลี่ยนแปลงวัตถุประสงค์ในการเก็บรวบรวมข้อมูลเช่นว่านั้นไว้ให้ชัดเจน
4	หลักข้อจำกัดในการนำไปใช้	ข้อมูลส่วนบุคคลนั้น จะต้องไม่มีการเปิดเผยทำให้มีหรือปรากฏในลักษณะอื่นใดซึ่งไม่ได้กำหนดไว้โดยชัดแจ้งในวัตถุประสงค์ของการเก็บรวบรวมข้อมูล เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลหรือ โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย
5	หลักการรักษาความมั่นคงปลอดภัยข้อมูล	จะต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม เพื่อป้องกันความเสี่ยงภัยใด ๆ ที่อาจจะทำให้ข้อมูลนั้นสูญหายเข้าถึง ทำลายใช้ตัดแปลงแก้ไข หรือเปิดเผยโดยมิชอบ

## ตารางที่ 3.3 (ต่อ)

ที่	กรอบ OECD	สาระสำคัญ
6	หลักการเปิดเผยข้อมูล	ควรมีการประกาศนโยบายให้ทราบโดยทั่วกัน หากมีการปรับปรุงแก้ไขหรือพัฒนาแนวนโยบาย หรือแนวปฏิบัติที่เกี่ยวกับข้อมูลส่วนบุคคลก็ ควรเปิดเผยหรือประกาศไว้ให้ชัดเจน รวมทั้งให้ ข้อมูลใด ๆ ที่สามารถระบุเกี่ยวกับหน่วยงาน ของรัฐผู้ให้บริการที่อยู่ผู้ควบคุมข้อมูลส่วนบุคคลด้วย
7	หลักการมีส่วนร่วมของบุคคล	ให้บุคคลซึ่งเป็นเจ้าของข้อมูลได้รับแจ้งหรือ ยืนยันจากหน่วยงานของรัฐที่เก็บรวบรวมหรือ จัดเก็บข้อมูลทราบว่า “หน่วยงานของรัฐนั้น ๆ ได้รวบรวมข้อมูลหรือจัดเก็บข้อมูลส่วนบุคคล ดังกล่าวหรือไม่ภายในระยะเวลาที่เหมาะสม”
8	หลักความรับผิดชอบ	ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตาม นโยบายและแนวปฏิบัติในการคุ้มครองข้อมูล ส่วนบุคคล

## 3.3.4 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

เมื่อสังคมมีการพัฒนามากขึ้น มีการใช้เทคโนโลยีในชีวิตประจำวันมากขึ้น ปัจจุบัน สังคมมนุษย์มีการนำเอาคอมพิวเตอร์เข้ามาเกี่ยวข้องกับการทำงาน จึงมีการจัดทำกฎหมายขึ้นมา เพื่อเข้าควบคุมและดูแลการความผิดเกี่ยวกับคอมพิวเตอร์ จึงได้มีการจัดทำพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ขึ้นมา ซึ่งพระราชบัญญัตินี้เป็นกฎหมาย อีกฉบับหนึ่งที่มีเนื้อหาเกี่ยวข้องกับข้อมูลส่วนบุคคลของประชาชน ในส่วนนี้ผู้เขียนจะทำการ อธิบายให้ทราบถึงรายละเอียดของพระราชบัญญัตินี้ฉบับดังกล่าวที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของ ประชาชน โดยมีรายละเอียดดังต่อไปนี้

### 3.3.4.1 หลักการและเหตุผลของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

เหตุผลในการประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เนื่องจากปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ หากมีผู้กระทำความผิดด้วยประการใด ๆ ให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะอันลามกอนาจาร ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน สมควรกำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำความผิดดังกล่าว

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีวัตถุประสงค์เพื่อป้องกันและปราบปรามการกระทำความผิดกับบุคคลที่ใช้คอมพิวเตอร์กระทำความผิด ไม่ว่าจะเป็นการทำให้ระบบคอมพิวเตอร์ไม่ทำงานตามคำสั่งที่กำหนดไว้ หรือระบบได้ทำตามคำสั่งผิดพลาดไป อีกทั้งการใช้วิธีการอันใด ๆ ที่เป็นการเข้าระบบคอมพิวเตอร์ แก้ไข หรือทำลายข้อมูลในระบบคอมพิวเตอร์ของบุคคลอื่น รวมถึงเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือเป็นข้อมูลที่มีลักษณะลามกอนาจาร อันส่งผลให้เกิดความเสียหายต่อสังคม เศรษฐกิจ ความมั่นคงของรัฐและความสงบสุขหรือศีลธรรมอันดีของประชาชน ทั้งนี้ ไม่ว่าจะตัวผู้กระทำความผิดจะอยู่นอกราชอาณาจักร ไม่ว่าจะเป็นคนไทยหรือเป็นคนต่างชาติ ถ้าผู้เสียหายมีการร้องขอให้ลงโทษ ผู้กระทำความผิดต้องรับโทษภายในราชอาณาจักรไทย

### 3.3.4.2 ขอบเขตการบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

พระราชบัญญัติฉบับนี้ประกาศในราชกิจจานุเบกษาเมื่อวันที่ 18 มิถุนายน 2550 ดังนั้นจึงมีผลบังคับใช้ตั้งแต่วันที่ 18 กรกฎาคม 2550 เป็นต้นไป โดยให้ความหมายคำว่า “ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

“ข้อมูลคอมพิวเตอร์” หมายถึงข้อมูลทุกอย่างที่อยู่ในระบบคอมพิวเตอร์ รวมทั้งชุดคำสั่งด้วยหากอยู่ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ นอกจากนั้นยังให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

โดยที่คำว่า “ข้อมูลอิเล็กทรอนิกส์” ตามที่บัญญัติไว้ในพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ได้ให้ความหมายคำว่า “ข้อมูลอิเล็กทรอนิกส์” ไว้ว่า “ข้อความที่ได้สร้าง ส่ง เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร” ดังนั้น ความหมายจึงกว้างรวมออกไปถึง โทรเลข โทรพิมพ์ โทรสาร อย่างไรก็ตามองค์ประกอบความผิดตามพระราชบัญญัตินี้ส่วนใหญ่จะเชื่อมโยงองค์ประกอบความผิด “ข้อมูลคอมพิวเตอร์” กับ “ระบบคอมพิวเตอร์” เข้าด้วยกัน ดังนั้นกรณีของ โทรเลข โทรพิมพ์ หรือ โทรสารหากเป็นความผิดที่ต้องเชื่อมโยงกับระบบคอมพิวเตอร์ เช่นการดักจับไว้ซึ่งข้อมูลคอมพิวเตอร์โดยมิชอบตามมาตรา 8 นั้นจะต้องเป็นกรณีที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ เป็นต้น ดังนั้นการดักจับ โทรเลข โทรพิมพ์หรือโทรสารที่ไม่ได้ส่งในระบบคอมพิวเตอร์ย่อมไม่เป็นความผิดตามมาตราดังกล่าว เป็นต้น

“ข้อมูลจราจรทางคอมพิวเตอร์” หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น หมายถึงข้อมูลที่แสดงรายการให้เห็นถึงการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์ซึ่งจะแสดงถึงแหล่งกำเนิด เช่น IP address ของเครื่อง ชื่อที่อยู่ของผู้ใช้บริการที่มีการลงทะเบียน ข้อมูลของผู้ให้บริการ (Service Provider) ลักษณะของการให้บริการว่าผ่านระบบใดหรือเครือข่ายใด วันเวลาของการส่งข้อมูล และข้อมูลทุกประเภทที่เกิดจากการสื่อสาร (Communication) ผ่าน “ระบบคอมพิวเตอร์”

3.3.4.3 การคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีสาระสำคัญโดยสรุป ดังนี้<sup>80</sup> (โปรดดูตารางที่ 4 ประกอบ)

1) การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ (มาตรา 5)

“การเข้าถึง” ตรงกับคำภาษาอังกฤษว่า “Access” หมายถึง การเข้าถึงทั้งในระดับกายภาพ เช่น กรณีที่มีการกำหนดรหัสผ่านเพื่อป้องกันมิให้บุคคลอื่นใช้เครื่องคอมพิวเตอร์ และผู้กระทำความผิดดำเนินการด้วยวิธีใดวิธีหนึ่งเพื่อให้ได้รหัสนั้นมาและสามารถใช้เครื่องคอมพิวเตอร์นั้นได้โดยนั่งอยู่หน้าเครื่องคอมพิวเตอร์นั่นเอง และหมายความรวมถึงการเข้าถึงระบบคอมพิวเตอร์หรือเข้าถึง

<sup>80</sup> พรเพชร วิชิตชลชัย. (ม.ป.ป.). คำอธิบาย พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550. สืบค้นจาก <http://www.chandra.ac.th>

ข้อมูลคอมพิวเตอร์ แม้ตัวบุคคลที่เข้าถึงจะอยู่ห่างโดยระยะทางกับเครื่องคอมพิวเตอร์ แต่สามารถเจาะเข้าไปในระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่ตนต้องการได้

นอกจากนี้ยังหมายถึงการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ทั้งหมดหรือแต่บางส่วนก็ได้ ดังนั้นจึงอาจหมายถึง การเข้าถึงฮาร์ดแวร์ หรือส่วนประกอบต่าง ๆ ของคอมพิวเตอร์ ข้อมูลที่ถูกบันทึกเก็บไว้ในระบบเพื่อใช้ในการส่งหรือโอนถึงอีกบุคคลหนึ่ง เช่น ข้อมูลจราจรทางคอมพิวเตอร์ เป็นต้น

ส่วนวิธีการเข้าถึงนั้นรวมทุกวิธีการไม่ว่าจะเข้าถึงโดยผ่านทางเครือข่ายสาธารณะ เช่น อินเทอร์เน็ตอันเป็นการเชื่อมโยงระหว่างเครือข่ายหลาย ๆ เครือข่ายเข้าด้วยกัน และยังหมายถึงการเข้าถึงโดยผ่านระบบเครือข่ายเดียวกันด้วยก็ได้ เช่น ระบบ LAN (Local Area Network) อันเป็นเครือข่ายที่เชื่อมต่อคอมพิวเตอร์ที่ตั้งอยู่ในพื้นที่ใกล้เคียง ๆ เข้าด้วยกัน นอกจากนี้ยังหมายความรวมถึงการเข้าถึงโดยการติดต่อสื่อสารแบบไร้สาย (Wireless Communication) อีกด้วย

“การเข้าถึง” ซึ่งถือว่าเป็นความผิดฐานนี้ จะต้องเป็นการเข้าถึงโดยปราศจากสิทธิโดยชอบธรรม (Without Right) ด้วย ซึ่งหมายความว่าหากผู้ทำการเข้าถึงนั้นเป็นบุคคลที่มีสิทธิเข้าถึงไม่ว่าด้วยถือสิทธิตามกฎหมายหรือได้รับอนุญาตจากเจ้าของระบบ ย่อมไม่มีความผิด ตัวอย่างเช่น การเข้าถึงเพื่อดูแลระบบของผู้ดูแลเว็บ (Webmaster) อยุ่อย่างไรก็ตาม หากผู้ได้รับอนุญาตให้ทำการเข้าถึงนั้นได้เข้าถึงระบบหรือข้อมูลคอมพิวเตอร์เกินกว่าที่ตนได้รับอนุญาต ในกรณีนี้บุคคลดังกล่าวก็ย่อมต้องรับผิดเช่นเดียวกัน

2) การเปิดเผยมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะโดยมิชอบ (มาตรา 6)

ระบบคอมพิวเตอร์นั้นมีมาตรการการเข้าถึง เช่นมีการลงทะเบียน username และ password หรือมีวิธีการอื่นใดที่จัดขึ้นเป็นการเฉพาะ การที่จะเป็นความผิดตามมาตรานี้ต้องเป็นเรื่องที่ผู้กระทำล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ และนำมาตรการนั้นเปิดเผยแก่ผู้หนึ่งผู้ใด โดยการเปิดเผยนั้นอยู่ในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น

3) การเข้าถึงข้อมูลคอมพิวเตอร์ (มาตรา 7)

ผู้ใดเข้าถึงซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตนโดยมิชอบถือว่าเป็นความผิด โดยเจตนาารมณ์ของการบัญญัติความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ ซึ่งหมายถึงข้อมูลนั้นเป็นการเก็บหรือส่งด้วยวิธีการทางคอมพิวเตอร์หรือวิธีการทางอิเล็กทรอนิกส์ ดังนั้นจึงไม่น่าจะหมายความรวมถึงข้อมูลที่บรรจุไว้ใน

แผ่นซีดี หรือแผ่นดิสเกตต์ อย่างไรก็ตามเมื่อใดที่มีการนำซีดีหรือแผ่นดิสเกตต์นั้นเล่นผ่านระบบคอมพิวเตอร์ก็จะอยู่ในความหมายของข้อมูลคอมพิวเตอร์ทันที

#### 4) การคัดกรับข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ (มาตรา 8)

ผู้ใดกระทำความผิดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อคัดกรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมีได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ ถือว่าเป็นการคัดกรับข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ

การคัดกรับข้อมูลในมาตรานี้หมายถึง การคัดกรับโดยวิธีการทางเทคนิค (Technical Means) เพื่อลักลอบดักฟัง (Listen) ตรวจสอบ (Monitoring) หรือติดตามเนื้อหาสาระของข่าวสาร (surveillance) ที่สื่อสารถึงกันระหว่างบุคคล หรือเป็นการกระทำเพื่อให้ได้มาซึ่งเนื้อหาของข้อมูลโดยตรงหรือโดยการเข้าถึงและใช้ระบบคอมพิวเตอร์ หรือการทำให้ได้มาซึ่งเนื้อหาของข้อมูลโดยทางอ้อมด้วยการแอบบันทึกข้อมูลสื่อสารถึงกันด้วยอุปกรณ์อิเล็กทรอนิกส์ โดยไม่คำนึงว่าอุปกรณ์อิเล็กทรอนิกส์ที่ใช้บันทึกข้อมูลดังกล่าวจะต้องเชื่อมต่อเข้ากับสายสัญญาณสำหรับส่งผ่านข้อมูลหรือไม่เพราะบางกรณีอาจใช้อุปกรณ์เช่นว่านั้นเพื่อบันทึกการสื่อสารข้อมูลที่ส่งผ่านด้วยวิธีการแบบไร้สายก็ได้ เช่น การติดต่อผ่านทางโทรศัพท์เคลื่อนที่ การติดต่อโดยใช้เทคโนโลยีไร้สายประเภท wireless LAN เป็นต้น ซึ่งนอกจากการใช้อุปกรณ์อิเล็กทรอนิกส์เพื่อบันทึกข้อมูลที่มีการส่งผ่านกันแล้วยังรวมถึงกรณีการใช้ซอฟต์แวร์หรือรหัสผ่านต่าง ๆ เพื่อทำการแอบบันทึกข้อมูลที่ส่งผ่านถึงกันด้วย

การกระทำความผิดตามมาตรานี้ผู้กระทำได้กระทำได้ไป “โดยมิชอบ” ด้วย ซึ่งหมายถึงการไม่มีอำนาจกระทำ ดังนั้น ถ้าผู้กระทำมีอำนาจที่จะกระทำได้ไม่ว่าโดยกฎหมายหรือโดยการอนุญาตของเจ้าของสิทธิ ผู้กระทำย่อมไม่มีความผิด

การคัดกรับข้อมูลคอมพิวเตอร์ของผู้อื่นนี้จะต้องเป็นข้อมูลที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ ดังนั้นจึงไม่หมายความรวมถึงข้อมูลคอมพิวเตอร์ที่จัดเก็บในรูปแบบซีดีหรือดิสเกตต์

การพิจารณาว่าข้อมูลคอมพิวเตอร์ได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้หรือไม่ ต้องพิจารณาจากข้อเท็จจริงว่าลักษณะการส่งข้อมูลคอมพิวเตอร์ดังกล่าวนี้ผู้ส่งต้องการให้เป็นเรื่องเฉพาะตนไม่ได้ต้องการให้เปิดเผยข้อมูลนั้นแก่ผู้ใดหรือไม่

การพิจารณาว่าข้อมูลคอมพิวเตอร์ใดมีไว้เพื่อประโยชน์สาธารณะจึงต้องพิจารณาจากการมีการเข้ารหัสการเข้าถึงข้อมูลคอมพิวเตอร์ดังกล่าวเพียงใด ดังนั้นจึงไม่ใช่เรื่องที่จะพิจารณาจากเนื้อหาของข้อมูลว่าเป็นความลับหรือไม่ เช่น เนื้อหาของข้อมูลอาจเป็นเรื่องความลับทางการค้า แต่หากผู้ส่งใช้วิธีการส่งที่ไม่มีมาตรการป้องกันการเข้าถึงข้อมูลนั้น ผู้ที่คัดกรับย่อมไม่มีความผิด

5) การทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติมข้อมูลคอมพิวเตอร์โดยมิชอบ (มาตรา 9)

ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ถือว่าเป็นการกระทำความผิดเป็นการรบกวนข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ

ความผิดตามมาตรา 9 มุ่งจะคุ้มครองความถูกต้องของข้อมูล (Integrity) ความถูกต้องแท้จริง (Authentication) และเสถียรภาพหรือความพร้อมในการใช้งานหรือการใช้ข้อมูลคอมพิวเตอร์ หรือ โปรแกรมคอมพิวเตอร์ที่บันทึกเก็บไว้บนสื่อคอมพิวเตอร์ได้อย่างเป็นปกติจึงเป็นการกำหนดขึ้นเพื่อให้ข้อมูลคอมพิวเตอร์และ โปรแกรมคอมพิวเตอร์ได้รับความคุ้มครองเช่นเดียวกับสิ่งของที่สามารจับต้องได้ (Corporeal Object)

ตัวอย่างของการกระทำความผิดตามมาตรา 9 ได้แก่ การป้อน โปรแกรมที่มีไวรัสทำลายข้อมูลหรือ โปรแกรมคอมพิวเตอร์ หรือการป้อน Trojan Horse เข้าไปในระบบเพื่อขโมยรหัสผ่านของผู้ใช้คอมพิวเตอร์สำหรับเพื่อเข้าไปลบ เปลี่ยนแปลงแก้ไขข้อมูลหรือกระทำการใด ๆ อันเป็นการรบกวนข้อมูล เป็นต้น

การกระทำความผิดตามมาตรา 9 นี้มีองค์ประกอบความผิดที่สำคัญคือ “โดยมิชอบ” ดังนั้น หากเป็นการกระทำของบุคคลผู้มีสิทธิโดยชอบก็จะไม่เป็นความผิด เช่น การเปลี่ยนแปลงข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) เพื่อประโยชน์ในการสื่อสารแบบไม่ระบุชื่อ ตัวอย่างเช่น การสื่อสารผ่านระบบ Anonymous Remailer System หรือการเปลี่ยนแปลงข้อมูลเพื่อการรักษาความลับและความปลอดภัยของการสื่อสาร อาทิ การเข้ารหัสข้อมูล (Encryption) เป็นต้น

6) ตกแต่งข้อมูลคอมพิวเตอร์ที่เป็นภาพของบุคคล (มาตรา 16)

ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ถือเป็นการกระทำความผิด

ผู้กระทำได้มีการกระทำความผิดเป็นการนำข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น หมายถึงการแสดงผลข้อมูลคอมพิวเตอร์นั้นออกเป็นภาพของบุคคล และภาพนั้นอาจเกิดจากการสร้างขึ้นใหม่ หรือเป็นภาพที่มีอยู่แต่ได้มีการตัดต่อ เติมหรือดัดแปลง ซึ่งเป็นการทำด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด เข้าสู่ระบบคอมพิวเตอร์ และระบบคอมพิวเตอร์นั้นเป็นระบบที่ประชาชนทั่วไปอาจเข้าถึงได้ ถ้าเป็นระบบคอมพิวเตอร์ของตนเองก็ไม่เป็นความผิด

ตารางที่ 3.4 หลักการสำคัญของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ที่	หลัก	พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
1	<p>หลักความยินยอม (Consent)</p> <p>บุคคลที่ให้ข้อมูลส่วนบุคคลต้องได้รับทราบและให้ความยินยอมแก่การเก็บรวบรวมการใช้หรือการเปิดเผยข้อมูลส่วนบุคคลของบุคคลนั้น ทั้งนี้ เว้นแต่เป็นกรณีที่ไม่สมควรตามที่กำหนดในกฎหมาย</p> <p>รูปแบบของความยินยอมอาจแตกต่างกันไปขึ้นอยู่กับสถานการณ์และประเภทของข้อมูล</p>	<p>การกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จะต้องเป็นการกระทำโดยปราศจากสิทธิโดยชอบธรรม ซึ่งหมายความว่าหากผู้ทำการกระทำความผิด เช่น การเข้าถึงโดยเป็นบุคคลที่มีสิทธิเข้าถึงไม่ว่าด้วยถือสิทธิตามกฎหมายหรือได้รับอนุญาตจากเจ้าของระบบ ตัวอย่างเช่น การเข้าถึงเพื่อดูแลระบบของผู้ดูแลเว็บ (Webmaster) ย่อมไม่มีความผิด</p> <p>อย่างไรก็ตาม หากผู้ได้รับอนุญาตให้ทำการเข้าถึงนั้นได้เข้าถึงระบบหรือข้อมูลคอมพิวเตอร์เกินกว่าที่ตนได้รับอนุญาต ในกรณีนี้บุคคลดังกล่าวก็ย่อมต้องรับผิดชอบเช่นเดียวกัน</p> <p>หรือกรณีกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อดักจับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ หากผู้กระทำมีอำนาจที่จะกระทำได้ไม่ว่าโดยกฎหมายหรือโดยการอนุญาตของเจ้าของสิทธิ ผู้กระทำย่อมไม่มีความผิด</p>

ตารางที่ 3.4 (ต่อ)

ที่	หลัก	พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
2	<p>หลักการจำกัดการใช้ การเปิดเผย และการเก็บรักษา</p> <p>องค์กรจะต้องไม่นำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยเพื่อวัตถุประสงค์อย่างอื่นนอกเหนือจากวัตถุประสงค์ของการเก็บรวบรวมข้อมูลนั้น เว้นแต่จะได้รับความยินยอมของบุคคลธรรมดาคนนั้นหรือเป็นไปตามที่กฎหมายกำหนด และข้อมูลส่วนบุคคลจะต้องถูกเก็บรักษาไว้ในระยะเวลาเพียงพอที่จำเป็นสำหรับการดำเนินการตามวัตถุประสงค์ดังกล่าวเท่านั้น</p>	<p>ผู้กระทำความผิดรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะและนำมาตรการนั้นเปิดเผยแก่ผู้หนึ่งผู้ใด โดยการเปิดเผยนั้นอยู่ในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น หรือเข้าถึงซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตนโดยมิชอบถือว่าเป็นความผิด</p>
3	<p>หลักความถูกต้อง (Accuracy)</p> <p>ข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้จะต้องถูกต้อง สมบูรณ์ และเป็นปัจจุบัน ตามความจำเป็นเพื่อวัตถุประสงค์ของการนำข้อมูลนั้นไปใช้ หลักการที่ว่าข้อมูลส่วนบุคคลต้องถูกต้อง สมบูรณ์ และเป็นปัจจุบันต้องคำนึงถึงสัดส่วนของส่วนได้เสียของเจ้าของข้อมูล ทั้งนี้เพื่อที่จะลดความเป็นไปได้ของการนำข้อมูลที่ไม่ถูกต้องไปใช้</p>	<p>ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบถือว่าเป็นการกระทำอันเป็นการรบกวนข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ความผิดตามมาตรา 9 มุ่งจะคุ้มครองความถูกต้องของข้อมูล (Integrity) ความถูกต้องแท้จริง (Authentication) และเสถียรภาพหรือความพร้อมในการใช้งานหรือการใช้ข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ที่บันทึกเก็บไว้บนสื่อคอมพิวเตอร์ได้อย่างเป็นปกติ</p>

ตารางที่ 3.4 (ต่อ)

ที่	หลัก	พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
4	<p>หลักการรักษาความปลอดภัย (Safeguards)</p> <p>ข้อมูลส่วนบุคคลจะต้องได้รับการรักษาความปลอดภัยที่เหมาะสมกับข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความปลอดภัยจะต้องให้ความคุ้มครองข้อมูลส่วนบุคคลต่อการสูญหายหรือการโจรกรรม ตลอดจนการเข้าตรวจดู การเปิดเผย การทำซ้ำ การใช้ หรือการแก้ไขเพิ่มเติมโดยไม่ได้รับอนุญาต</p>	<p>ระบบคอมพิวเตอร์นั้นมีมาตรการการเข้าถึง เช่น มีการลงทะเบียน username และ password หรือมีวิธีการอื่นใดที่จัดขึ้นเป็นการเฉพาะ การที่ล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะและนำมาใช้นั้นเปิดเผยแก่ผู้หนึ่งผู้ใด โดยการเปิดเผยนั้นอยู่ในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นถือเป็นความผิด</p>

3.3.5 ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....<sup>81</sup>

ตามที่กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ได้เสนอร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ต่อคณะรัฐมนตรี โดยที่ร่างพระราชบัญญัตินี้ดังกล่าว มีหลักการเพื่อให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล เนื่องจากความก้าวหน้าของเทคโนโลยีสารสนเทศ รวมทั้งระบบสื่อสาร ทำให้การเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลสามารถทำได้โดยง่าย สะดวก และรวดเร็ว อันอาจนำมาซึ่งความเดือดร้อน รำคาญ หรือความเสียหายในกรณีที่มีการนำไปแสวงหาประโยชน์หรือเปิดเผยโดยไม่ได้รับความยินยอมหรือแจ้งล่วงหน้า ซึ่งแม้ว่าจะได้มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลในบางเรื่อง แต่ก็ยังไม่มีหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป โดยคณะรัฐมนตรีได้มีมติอนุมัติหลักการร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... เมื่อวันที่ 6 มกราคม 2558 และส่งให้สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณา โดยให้รับ

<sup>81</sup> เว็บไซต์สำนักงานคณะกรรมการคุ้มครองสิทธิเสรีภาพ (ม.ป.ป.). ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... สืบค้น 24 มีนาคม 2559, จาก <http://www.etcommission.go.th>

ข้อสังเกตของส่วนราชการที่เกี่ยวข้อง ไปประกอบการพิจารณาด้วย แล้วส่งให้คณะกรรมการประสานงานสภานิติบัญญัติแห่งชาติพิจารณา ก่อนเสนอสภานิติบัญญัติแห่งชาติต่อไป โดยคณะกรรมการกฤษฎีกา (คณะที่ 11) ได้พิจารณาตรวจร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... เสร็จเรียบร้อยแล้ว โดยมีรายละเอียดดังต่อไปนี้

โครงสร้างของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ประกอบด้วย

1. บททั่วไป (มาตรา 1 - มาตรา 6)

หมวด 1 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (มาตรา 7 – มาตรา 16)

หมวด 2 การคุ้มครองข้อมูลส่วนบุคคล

ส่วนที่ 1 บททั่วไป (มาตรา 17 – มาตรา 18)

ส่วนที่ 2 การเก็บรวบรวมข้อมูลส่วนบุคคล (มาตรา 19 – มาตรา 23)

ส่วนที่ 3 การใช้หรือเปิดเผยข้อมูลส่วนบุคคล (มาตรา 24 – มาตรา 25)

หมวด 3 สิทธิของเจ้าของข้อมูลส่วนบุคคล (มาตรา 26 – มาตรา 30)

หมวด 4 ข้อปฏิบัติในการคุ้มครองข้อมูล (มาตรา 31 – มาตรา 34)

หมวด 5 การร้องเรียน (มาตรา 35 – มาตรา 41)

หมวด 6 ความรับผิดชอบทางแพ่ง (มาตรา 42)

หมวด 7 บทกำหนดโทษ (มาตรา 43 – มาตรา 49)

บทเฉพาะกาล (มาตรา 50 – มาตรา 53)

การคุ้มครองข้อมูลส่วนบุคคล ตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... สรุปสาระสำคัญ ดังนี้

1. เป็นกฎหมายกลางในการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป (มีขอบเขตการใช้บังคับกับหน่วยงานของรัฐด้วย)

2. หากมีกฎหมายว่าด้วยการใดบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในลักษณะใด กิจการใด หรือหน่วยงานใดไว้โดยเฉพาะแล้วให้เป็นไปตามกฎหมายนั้น (มาตรา 3) เว้นแต่

3. บทบัญญัติเกี่ยวกับการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคล และบทกำหนดโทษที่เกี่ยวข้อง จะต้องนำบทบัญญัติแห่งพระราชบัญญัตินี้ไปใช้บังคับเป็นการเพิ่มเติมไม่ว่า จะซ้ำกับกฎหมายนั้นหรือไม่ก็ตาม

4. บทบัญญัติในเรื่องการร้องเรียน บทบัญญัติที่ให้อำนาจแก่คณะกรรมการผู้เชี่ยวชาญออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคล และบทบัญญัติเกี่ยวกับอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ รวมทั้งบทกำหนดโทษที่เกี่ยวข้อง ให้บังคับตามพระราชบัญญัตินี้ เฉพาะในกรณีที่มีกฎหมายว่าด้วยการนั้น ไม่มีบทบัญญัติเกี่ยวกับการร้องเรียน

5. สำหรับข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล มาตรา 31 ได้กำหนดให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นผู้ทำประกาศกำหนดข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลเพื่อเป็นแนวทางให้ผู้ควบคุมข้อมูลส่วนบุคคลปฏิบัติ

มาตรา 42 กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการใด ๆ อันทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้น เว้นแต่จะพิสูจน์ได้ว่า (1) ความเสียหายนั้นเกิดจากเหตุสุดวิสัย (2) เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติตามอำนาจหน้าที่ตามกฎหมาย และ (3) เป็นการปฏิบัติตามถ้วนตามข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนดตามมาตรา 31

จากการศึกษากฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายระหว่างประเทศ ต่างประเทศ และประเทศไทยพบว่า สหประชาชาติซึ่งเป็นองค์การระหว่างประเทศได้ประกาศใช้กติการะหว่างประเทศว่าด้วยสิทธิพลเมือง และสิทธิทางการเมือง เพื่อให้ความคุ้มครองความเป็นอยู่ส่วนตัว ส่วนสหภาพยุโรปได้ออกหลักเกณฑ์ที่สำคัญ “Directive 95/46/EC on the protection of Individuals with regard to the processing of personal data and on the free movement of such data” เพื่อผลักดันให้กฎหมายในหมู่ประเทศสมาชิกมีความสอดคล้องกันในการให้หลักประกันที่ดีพอต่อการคุ้มครองข้อมูลส่วนบุคคลของพลเมืองของ EU โดยปราศจากข้อจำกัดที่เกิดจากความแตกต่างกันของกฎหมายกฎเกณฑ์ทางสังคมและวัฒนธรรมโดยให้เป็นไปตามที่กำหนดไว้ใน Directive ภายในปี 1998 และต่อมาในปี ค.ศ. 2002, EU ได้ออกหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลเพิ่มเติมคือ “Directive 2002/58/EC concerning the processing of personal data and protection of privacy in the electronic communication sector (Directive on privacy and electronic communication)” โดยกำหนดรายละเอียดให้ผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารทางอิเล็กทรอนิกส์ต้องมีมาตรการให้ความคุ้มครองข้อมูลส่วนบุคคล เช่น จัดให้มีมาตรการรักษาความปลอดภัยและความลับของข้อมูลที่ส่ง หรือการลบข้อมูลจราจรเมื่อหมดความจำเป็น

ในขณะที่ประเทศในระบบคอมมอนลอว์ (Common Law) ได้แก่ ประเทศอังกฤษได้ตรากฎหมายเพื่อคุ้มครองสิทธิส่วนบุคคลอันเกี่ยวกับข้อมูลข่าวสาร คือ พระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลข่าวสาร ค.ศ. 1984 (Data Protection Act 1984) มีผลทำให้การจัดเก็บสารสนเทศทุกประเภทที่เกี่ยวกับบุคคลโดยระบบคอมพิวเตอร์จะต้องดำเนินการให้เป็นไปตามที่กฎหมายกำหนดต่อมาได้ตรา 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 และประเทศแคนาดาได้ตรากฎหมายคุ้มครองข้อมูลข่าวสาร คือ Personal

Information Protection and Electronic Documents Act 2000 เกิดจากแรงกดดันหรือได้รับผลกระทบจาก European Union (EU) เช่นเดียวกับประเทศสหรัฐอเมริกาและประเทศอื่น ๆ ที่ต้องมีการพัฒนากฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้เทียบเท่า EU Personal Information Protection and Electronic Documents Act 2000 (PIPEDA)

ส่วนประเทศในระบบซีวิลลอว์ (Civil Law) ได้แก่ ประเทศอิตาลีได้ตรารัฐบัญญัติคุ้มครองข้อมูลส่วนบุคคลหรือที่เรียกว่า Protection of Individuals and Other Subjects with Regard to the Processing of Personal Data Act no.675 of 31.12.1996 เป็นกฎหมายที่มีเพื่ออนุวัติการให้ เป็นไปตาม EU Directive (95/46EC) ประเทศฝรั่งเศสได้ตรารัฐบัญญัติที่ 78-17 ลงวันที่ 6 มกราคม ค.ศ. 1978 ว่าด้วยระบบประมวลข่าวสารและเสรีภาพ (Loi relative à l'informatique, aux fichiers et aux libertés หรือ The Act on Data Processing Data Files and Individual Liberties) ปัจจุบันได้มีการร่างรัฐบัญญัติว่าด้วยการคุ้มครองบุคคลธรรมดาในด้านการจัดทำระบบข้อมูลที่มีลักษณะ ส่วนตัว และมีการแก้ไขรัฐบัญญัติที่ 78-17 ลงวันที่ 6 มกราคม ค.ศ. 1978 โดยการออก Projet de caractère personnel et loi 78-17 du janvier 1978 ประเทศญี่ปุ่นได้ตรากฎหมายว่าด้วยการคุ้มครอง ข้อมูลส่วนบุคคลในฐานะเป็นกฎหมายทั่วไป พร้อมกับกฎหมายเฉพาะ 4 ฉบับ ได้แก่ กฎหมาย เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในการครอบครองดูแลของหน่วยงานฝ่ายปกครอง กฎหมาย เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในการครอบครองดูแลขององค์กรอิสระและองค์กรมหาชน อื่น ๆ กฎหมายเกี่ยวกับการจัดตั้งคณะกรรมการวินิจฉัยการเปิดเผยและการคุ้มครองข้อมูล ส่วนบุคคล และกฎหมายว่าด้วยการเตรียมการบังคับการให้ เป็นไปตามกฎหมายคุ้มครองข้อมูล ส่วนบุคคลในความครอบครองดูแลของหน่วยงานฝ่ายปกครอง เมื่อวันที่ 23 พฤษภาคม ค.ศ. 2003 และต่อมาได้ตรากฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นหลักทั่วไป และกฎหมาย ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในความควบคุมดูแลของหน่วยงานรัฐ และหน่วยงานปกครอง ท้องถิ่น รวมตลอดถึงหน่วยงานและองค์กรอิสระอื่น ๆ มีผลใช้บังคับ เมื่อวันที่ 30 พฤษภาคม ค.ศ. 2003

สำหรับประเทศไทยไม่มีบทบัญญัติแห่งกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล มีเพียงพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 เท่านั้น ดังนั้น กฎหมายที่ว่าด้วยข้อมูล ข่าวสารส่วนบุคคลจึงได้รับการบัญญัติรับรองไว้ในพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 โดยมีหลักการสำคัญประการหนึ่งในการคุ้มครองข้อมูลข่าวสารส่วนบุคคล ดังที่ปรากฏ ในหลักการและเหตุผลของพระราชบัญญัติข้อมูลข่าวสารของราชการ ว่า “ในระบอบประชาธิปไตย การให้ประชาชนมีโอกาสดูข่าวสารในการได้รับข้อมูลข่าวสารเกี่ยวกับการดำเนินการต่าง ๆ ของรัฐเป็นสิ่งจำเป็น เพื่อที่ประชาชนจะสามารถแสดงความคิดเห็นและใช้สิทธิทางการเมืองได้โดย

ถูกต้องกับความจริงอันเป็นการส่งเสริมให้มีความเป็นรัฐบาลโดยประชาชนมากยิ่งขึ้นสมควรกำหนดให้ประชาชนมีสิทธิได้รับข้อมูลข่าวสารของราชการ โดยมีข้อยกเว้นอันไม่ต้องเปิดเผยที่แจ้งชัดและจำกัดเฉพาะข้อมูลข่าวสารที่หากเปิดเผยแล้วจะเกิดความเสียหายต่อประเทศชาติหรือต่อประโยชน์ที่สำคัญของเอกชน ทั้งนี้เพื่อพัฒนาระบบประชาธิปไตยให้มั่นคงและจะยังผลให้ประชาชนมีโอกาสดูถึงสิทธิหน้าที่ของตนอย่างเต็มที่ เพื่อที่จะปกป้องรักษาประโยชน์ของตนประการหนึ่งกับสมควรคุ้มครองสิทธิส่วนบุคคลในส่วนที่เกี่ยวข้องกับข้อมูลข่าวสารของราชการไปพร้อม อีกประการหนึ่ง”