มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคล ในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐ

Legal Measures of Personal Data Protection for e-Government

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
นิติศาสตร์มหาบัณฑิต มหาวิทยาลัยกรุงเทพ
ปีการศึกษา 2554

มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคล ในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐ

Legal Measures of Personal Data Protection for e-Government

สัญญา วิริยะอมรพันธุ์

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
นิติศาสตร์มหาบัณฑิต มหาวิทยาลัยกรุงเทพ
ปีการศึกษา 2554

ชื่องานวิจัย :	มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ภาครัฐ
ชื่อผู้วิจัย :	นายสัญญา วิริยะอมรพันธุ์
ชื่อคณะและสถาบัน :	คณะนิติศาสตร์ มหาวิทยาลัยกรุงเทพ
สาขา :	กฎหมายธุรกิจระหว่างประเทศและธุรกรรมอิเล็กทรอนิกส์
รายชื่อที่ปรึกษา :	ผู้ช่วยศาสตรจารย์ ดร. อรรยา สิงห์สงบ
ปีการศึกษา :	2554
คำสำคัญ :	มาตรการคุ้มครองข้อมูลส่วนบุคคล, ธุรกรรมอิเล็กทรอนิกส์, รัฐบาลอิเล็กทรอนิกส์

บทคัดย่อ

เนื่องจากในปัจจุบันมีการนำธุรกรรมอิเล็กทรอนิกส์มาใช้ในภาคเอกชน ส่งผลให้การติดต่อสื่อสารและทำธุรกรรมต่าง ๆ บนโลกได้เปลี่ยนแปลงไปอย่างสิ้นเชิง จากผลลัพธ์ดังกล่าวซึ่งได้ส่งผลกระทบในด้านลบด้วย โดยเทคโนโลยีที่ทันสมัยทำให้เกิดการกระความผิดในรูปแบบใหม่ คือ การกระทำความผิดโดยอาศัยระบบคอมพิวเตอร์และระบบอินเตอร์เน็ตเพื่อทำลายข้อมูลหรือขโมยข้อมูลไปใช้ในทางทุจริต ซึ่งเป็นปัญหาใหญ่ที่เกิดขึ้นกับภาคเอกชนและส่งผลกระทบในวงกว้าง ขณะที่ในปัจจุบันภาครัฐของประเทศไทยได้มีการนำการทำธุรกรรมอิเล็กทรอนิกส์มาใช้ในการบริหารจัดการภาครัฐและให้บริการกับประชาชนหรือที่เรียกว่า “รัฐบาลอิเล็กทรอนิกส์”ได้ไม่นาน ดังนั้น จึงมีความจำเป็นอย่างยิ่งที่ภาครัฐจะต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่ดีพอ เนื่องจากหน่วยงานของรัฐเป็นผู้มีอำนาจในการเก็บข้อมูลที่สำคัญของบุคคล ดังนั้น ภาครัฐจึงต้องพัฒนากลไกการจัดเก็บรักษาข้อมูลให้มีความมั่นคงปลอดภัยและเป็นสากลเพื่อให้ประชาชนมีความมั่นใจในการทำธุรกรรมทางอิเล็กทรอนิกส์กับภาครัฐซึ่งมีความแตกต่างจากการทำธุรกรรมอิเล็กทรอนิกส์ทั่วไป

ทั้งนี้ สืบเนื่องจากในปัจจุบัน ปัญหาการละเมิดข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐในประเทศไทยยังไม่ปรากฏข้อเท็จจริงที่สามารถนำมาเป็นกรณีศึกษาได้ อีกทั้งในทางปฏิบัติเป็นการยากที่หน่วยงานของรัฐจะเปิดเผยถึงข้อผิดพลาดและความเสียหายในการจัดเก็บข้อมูลส่วนบุคคล ตลอดจนมาตรการการคุ้มครองข้อมูลส่วนบุคคลโดยละเอียด เพราะหากแม้มีกรณีที่เกิดขึ้นจริง การเปิดเผยถึงข้อผิดพลาดในมาตรการคุ้มครองข้อมูลส่วนบุคคลหรือข้อมูลอื่นของหน่วยงานรัฐ อาจส่งผลกระทบต่อบุคคลที่เกี่ยวข้องรวมถึงหน่วยงานและอาจทำให้ภาพลักษณ์ขององค์กรหรือหน่วยงานเสื่อมเสียซึ่งอาจทำให้ความเชื่อมั่นในการทำธุรกรรมอิเล็กทรอนิกส์ของประชาชนลดลง

บัณฑิตวิทยาลัย
มหาวิทยาลัยกรุงเทพ

สารนิพนธ์

โดย

นายสัญญา วิริยะอมรพันธุ์

เรื่อง

มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐ

ได้รับการตรวจสอบและอนุมัติให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
นิติศาสตรมหาบัณฑิต

อาจารย์ที่ปรึกษา [redacted]
(ผู้ช่วยศาสตราจารย์ ดร.อรรยา สิงห์สงบ)

อาจารย์ที่ปรึกษาร่วม [redacted]
(ดร.ใจรัก เอื้อชูเกียรติ)

กรรมการผู้ทรงคุณวุฒิ [redacted]
(อาจารย์ชวลิต อัตถศาสตร์)

ซึ่งจากการศึกษาพบว่า ประเทศไทยมีความจำเป็นที่จะต้องมีการกำหนดมาตรการหรือปรับปรุงมาตราการเดิมให้ครอบคลุมถึงความคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ของภาครัฐไว้เป็นการเฉพาะเจาะจง เพื่อให้แต่ละหน่วยงานหรือองค์กรของรัฐมีระเบียบแบบแผนและวิธีปฏิบัติในการให้ความคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐที่สอดคล้องกัน ตลอดจนเร่งให้มีองค์กรหรือหน่วยงานของรัฐที่ทำหน้าที่ในการออกกฎเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์กับภาครัฐ รวมถึงเร่งให้มีหน่วยงานที่ทำหน้าที่กำกับดูแลการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของหน่วยงานรัฐตลอดจนมีการออกเครื่องหมายรับรองความน่าเชื่อถือ เพื่อให้มีการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ของภาครัฐที่เข้มแข็งและมีมาตรการที่มีประสิทธิภาพ ซึ่งมีความสอดคล้องกับการคุ้มครองข้อมูลส่วนบุคคลในต่างประเทศซึ่งมีการพัฒนาด้านการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ของภาครัฐอย่างจริงจัง

Title : Legal Measures of Personal Data Protection for e-Government

Author : Mr.Sanya Wiriya-amornphan

School : Law, Bangkok University

Major : International Business Law and Electronic Transaction

Advisor : Asst.Prof.Dr. Aunya Singsangob

Academic Year : 2011

Keywords : Privacy Law, Data Protection Law, e-Government, Electronic Transaction, Electronic Government

Abstracts

Due to electronic transaction are widely used in private sector, These result significant changes in ways of communication, including adverse effects. Modern technologies cause new forms of offenses from the use of computer and internet systems to cause damages or loss of information occurred by illegal acts. This has widely effected as a major problem in a private sector. On the other hand, Thai government has recently implemented the electronic transactions in the administrative public service, know as “e-Government”. Therefore, it is necessary for the government to have the effective personal data prevention measures because government agencies are authorized to maintain personal records. In addition, the government has to develop the system of data maintenance for the security and internationality purposes in order to ensure the public confidence in using electronic transactions with the government which is different from electronic transactions in general.

Nowadays, the problems of personal data intrusion for electronic transactions in Thai government sector have no study case. In practical ways, it is difficult to ask the state agency to disclose in detail about mistake and damages about personal data collection and personal data prevention measures thoroughly. Otherwise, the disclosure of those errors and damages of personal data prevention measure of government sector may cause adverse effects to relevant parties including the agency itself. Negative images of the agency may reduce the level of public confidence in doing electronic transactions.

This research, finds that Thailand should specifically create or improve the existing procedures on personal data protection for e-government to be more comprehensive in order for each government's agencies to have coherent regulations and practices. In additions, it is suggested that the governmental organizations or agencies should take responsibilities enact laws to regulations on personal data protection in electronic transactions of e-government and to urge the establishment of an agency whose function is to take care of personal data for e-government including the endorsement of the Trust Mark standards for privacy protection. This will lead to the strength and effectiveness of personal data protection procedures in Thailand in consistence with international measures which have been gradually and seriously developed.

กิตติกรรมประกาศ

การจัดทำสารนิพนธ์ฉบับนี้ จะสำเร็จลุล่วงมิได้เลยหากขาดผู้ให้การสนับสนุน ผู้ให้คำแนะนำ และผู้ให้กำลังใจทุกท่านในการจัดทำสารนิพนธ์ฉบับนี้

ข้าพเจ้าขอกราบขอบพระคุณท่านอาจารย์ ผศ.ดร.อรรยา สิงห์สงบ อาจารย์ที่ปรึกษา และท่านอาจารย์ ดร.ใจรัก เอื้อชูเกียรติ อาจารย์ที่ปรึกษาร่วมเป็นอย่างสูงที่ให้เกียรติและได้สละเวลาอันมีค่าในการให้คำปรึกษาและให้คำชี้แนะตลอดจนความช่วยเหลือต่าง ๆ ที่เป็นประโยชน์อย่างยิ่งอันทำให้การจัดทำสารนิพนธ์ฉบับนี้สำเร็จลงได้ด้วยความบริบูรณ์และข้าพเจ้าขอกราบขอบพระคุณท่านคณะกรรมการสอบสารนิพนธ์ทุกท่านโดยเฉพาะอย่างยิ่งท่านอาจารย์ชวลิต อัตถศาสตร์ ที่ได้ให้เกียรติในการเป็นกรรมการสอบสารนิพนธ์และได้ให้คำชี้แนะในการแก้ไขปรับปรุงสารนิพนธ์ฉบับนี้จนเสร็จโดยสมบูรณ์

ข้าพเจ้าได้หวังเป็นอย่างยิ่งว่าสารนิพนธ์ฉบับนี้ พอจะเป็นประโยชน์แก่ผู้อื่นอยู่บ้างไม่มากก็น้อย โดยข้าพเจ้าขอยกประโยชน์และความดีงามทั้งมวลให้แก่ผู้มีพระคุณดังข้างต้นทุกท่าน ส่วนข้อบกพร่องประการใดในการจัดทำสารนิพนธ์ฉบับนี้ ข้าพเจ้าขอกราบขออภัยและขอน้อมรับความผิดพลาดนั้นไว้แต่เพียงผู้เดียว

และที่สำคัญข้าพเจ้าขอกราบขอบพระคุณท่านบิดาและมารดาที่คอยให้ความรักให้กำลังใจและให้การสนับสนุนแก่ข้าพเจ้าด้วยดีเสมอมา และขอขอบคุณทุกคนในครอบครัว ญาติสนิทมิตรสหาย ตลอดรวมถึงบุคคลอื่นที่มิได้เอ่ยนาม ที่ได้คอยให้การสนับสนุนและให้กำลังใจกันเสมอมาและข้าพเจ้าหวังเป็นอย่างยิ่งว่าสารนิพนธ์ฉบับนี้จะมีประโยชน์แก่ผู้ศึกษาและผู้สนใจทุกท่าน

สัญญา วิริยะอมรพันธุ์

สารบาญ

หน้า

สารบาญ(ต่อ)

หน้า

สารบาญ(ต่อ)

หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

โลกยุคปัจจุบันมีการพัฒนาเทคโนโลยีทางด้านต่าง ๆ อยู่ตลอดเวลาเพื่อตอบสนองความต้องการที่ไม่มีขอบเขตจำกัดของมนุษย์ อันทำให้สังคมมีลักษณะเป็นสังคมที่มีความเป็นพลวัต(Dynamic)โดยการพัฒนาทางด้านเทคโนโลยีสารสนเทศ(Information Technology : IT) เป็นอีกสิ่งหนึ่งที่มีความสำคัญในสังคมโลกยุคปัจจุบันเพื่อเป็นการยกระดับคุณภาพชีวิตและเป็นการอำนวยความสะดวกด้านการติดต่อสื่อสาร(Communication)ระหว่างผู้คนซึ่งอยู่ในสถานที่ต่าง ๆ ทั่วทุกมุมโลกให้ได้รับความสะดวกและรวดเร็วมากขึ้น ดังนั้น มนุษย์จึงมีการพัฒนาทางด้านเทคโนโลยีสารสนเทศอยู่ตลอดเวลา โดยการพัฒนาดังกล่าวมักเป็นการพัฒนาในรูปแบบของการทำการแลกเปลี่ยนข้อมูลทางคอมพิวเตอร์หรือข้อมูลอิเล็กทรอนิกส์(Electronic Data)ระหว่างกัน ซึ่งในการแลกเปลี่ยนข้อมูลนั้นจำเป็นที่จะต้องมีการรวบรวมและบันทึกข้อมูลสำคัญต่าง ๆ ลงในระบบคอมพิวเตอร์เพื่อให้มีการนำข้อมูลออกมาใช้ได้โดยสมบูรณ์เมื่อมีความจำเป็นที่จะต้องใช้ข้อมูลดังกล่าวโดยมีอินเตอร์เน็ต(Internet) เป็นสื่อกลางสำคัญในการเชื่อมโยงเครือข่ายและทำการรับและส่งข้อมูลระหว่างกัน

ทั้งนี้ ประเทศไทยซึ่งเปรียบเสมือนตัวแสดงหนึ่งในเวทีสังคมโลก จึงหลีกเลี่ยงมิได้เลยที่จะต้องมีการปรับตัวเพื่อเร่งให้มีการสนับสนุนการพัฒนาด้านเทคโนโลยีสารสนเทศในประเทศไทยอย่างจริงจังทั้งในส่วนของภาคเอกชนและในส่วนของภาครัฐ ด้วยเหตุดังกล่าวรัฐบาลจึงได้ออกนโยบายเทคโนโลยีสารสนเทศและการสื่อสาร ระยะ พ.ศ. 2544-2553 ของประเทศไทยหรือ IT2010 (Information Technology 2010) เพื่อกำหนดกุลยุทธ์ในการพัฒนาประเทศสู่สังคมแห่งภูมิปัญญาและการเรียนรู้ไว้ 5 ด้าน ได้แก่ e-Industry , e-Commerce , e-Government , e-Education และ e-Society ซึ่งเป็นนโยบายของรัฐบาลที่ออกมาเพื่อพัฒนาระบบเทคโนโลยีสารสนเทศในประเทศไทยจนเป็นที่มาของ “รัฐบาลอิเล็กทรอนิกส์” หรือ (Electronics Government : e-Government) ซึ่งได้ถูกพัฒนาขึ้นเพื่อเป็นการสนับสนุนให้มีการพัฒนาเทคโนโลยีสารสนเทศอย่างต่อเนื่อง โดยโครงการรัฐบาลอิเล็กทรอนิกส์เป็นวิธีการบริหารจัดการภาครัฐในรูปแบบใหม่ของรัฐบาลโดยใช้เทคโนโลยีสารสนเทศเป็นสื่อกลางในการบริหารงานและการให้บริการกับประชาชน ซึ่งจะส่งผลให้การบริหารราชการแผ่นดินมีความเป็นธรรมาภิบาล(Good Governance)และมีความโปร่งใส(Transparency)มากขึ้น อันเนื่องมาจากการเปิดเผยข้อมูลข่าวสารและประชาชนสามารถทำการตรวจสอบได้ตลอดเวลา โดยรัฐบาลอิเล็กทรอนิกส์จะมีการทำธุรกรรมอิเล็กทรอนิกส์ในหลายระดับทั้งจากระดับภาครัฐสู่ภาครัฐด้วยกัน(Government to Government : G2G) ระดับภาครัฐสู่ภาคธุรกิจ(Government to

Business : G2B)และระดับภาครัฐสู่ประชาชน(Government to Citizen : G2C)[1]ซึ่งหน่วยงานของรัฐต้องมีระบบรักษาความปลอดภัยของข้อมูลที่มีความมั่นคงและปลอดภัยเพื่อให้การแลกเปลี่ยนข้อมูลระหว่างหน่วยงานของรัฐและประชาชนเกิดประสิทธิภาพสูงสุด โดยโครงการรัฐบาลอิเล็กทรอนิกส์ยังได้ถูกพัฒนาอย่างต่อเนื่องซึ่งในปัจจุบันอยู่ภายใต้กรอบนโยบายเทคโนโลยีสารสนเทศและการสื่อสาร ระยะ พ.ศ. 2554-2563 ของประเทศไทย หรือ IT2020[2]

จากนโยบายดังกล่าว ส่งผลให้ในปัจจุบันภาครัฐของไทยมีการดำเนินงานในการพัฒนาการทำธุรกรรมอิเล็กทรอนิกส์(Electronic Transaction : e-Transaction)ของภาครัฐซึ่งเริ่มตั้งแต่นโยบาย IT2000 และ IT2010 จนกระทั่งได้พัฒนาเป็นนโยบาย IT2020 ในปัจจุบันให้อยู่ภายใต้ระบบการทำธุรกรรมทางอิเล็กทรอนิกส์มากขึ้นเพื่อตอบสนองต่อการเปลี่ยนแปลงของโลกในยุคปัจจุบันที่มีการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์และมีการพัฒนาข้อมูลอิเล็กทรอนิกส์อยู่ตลอดเวลา และเพื่อเป็นการลดช่องว่างตลอดจนลดความเหลื่อมล้ำในการเข้าถึงข้อมูลและการให้บริการของภาครัฐ

ในขณะที่ปัจจุบันรัฐบาลของหลายประเทศ ต่างมีการสนับสนุนและส่งเสริมให้ประชาชนของประเทศตนได้ทำธุรกรรมในรูปแบบอิเล็กทรอนิกส์มากขึ้น เช่น ดังปรากฏในกรณีของประเทศเดนมาร์ก โดยรัฐบาลเดนมาร์กได้มีการจัดตั้งหน่วยงานที่ชื่อ Digital Task Force ซึ่งเป็นหน่วยงานปฏิบัติการเฉพาะกิจสังกัดกระทรวงการคลัง(Danish Ministry of Finance)โดยมีวัตถุประสงค์เพื่อเป็นการสนับสนุนและส่งเสริมในการนำกลยุทธ์ด้านรัฐบาลอิเล็กทรอนิกส์มาปรับใช้ในหน่วยงานภาครัฐทุกระดับชั้น โดยมีการบริหารงานแบบบูรณาการโดยการรวมตัวในแนวดิ่ง(Vertical Integration)[3]และมีการรวมตัวในเชิงกายภาพ(Physical Integration)[4]ซึ่งเป็นการรวมฮาร์ดแวร์(Hardware)และซอฟต์แวร์(Software)หรืออุปกรณ์ที่ใช้ในการติดต่อสื่อสารให้สามารถทำงานร่วมกันเพื่อให้ส่วนที่สนับสนุนการทำงานต่าง ๆ สามารถใช้งานได้อย่างมีประสิทธิภาพและมีการแบ่งปันข้อมูลโดยทำการเชื่อมโยงกับหมายเลขประจำตัวส่วนบุคคล

---

[1] รัฐบาลอิเล็กทรอนิกส์, **e-Government คืออะไร**[online], 4 มิถุนายน 2555. แหล่งที่มา http://www. dld. go.th/ict/article/egov/e-gev02.html.

[2] กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร**, กรอบนโยบายเทคโนโลยีสารสนเทศและการสื่อสาร ระยะ พ.ศ.2554-2563 ของประเทศไทย**, (ม.ป.พ., 2554), 79.

[3] Vertical Integration เป็นคำศัพท์ทางการตลาด หมายถึง การที่บริษัทควบคุมในทุกขั้นตอนการผลิตที่แตกต่างกัน เช่น บริษัทกลั่นปิโตรเลียมเป็นเจ้าของโรงเก็บปิโตรเลียมและสถานีบริการน้ำมัน ซึ่งเป็นธุรกิจปลายน้ำ ในขณะเดียวกันก็เป็นเจ้าของบ่อน้ำมันดิบและท่อขนส่งซึ่งเป็นธุรกิจต้นน้ำ ซึ่งหากเปรียบเทียบกับระบบราชการ อาจหมายถึง การควบคุมโดยหน่วยงานเดียวในขั้นตอนที่แตกต่างกันตามลำดับชั้น

[4] Physical Integration หมายถึง การรวมฮาร์ดแวร์(Hardware)และซอฟต์แวร์(Software)หรืออุปกรณ์ในการติดต่อสื่อสาร ให้สามารถทำงานร่วมกันได้เพื่อทำให้ส่วนสนับสนุนต่าง ๆ ในการการทำงาน สามารถใช้งานได้อย่างมีประสิทธิภาพและสอดคล้องกัน

ในปัจจุบันและจะทำการเชื่อมโยงเข้ากับลายมือชื่ออิเล็กทรอนิกส์(e-Signature)ในอนาคต ภายใต้มาตรการคุ้มครองทางกฎหมายในด้านของความเป็นส่วนตัวที่เข้มงวดในการป้องกันในการส่งผ่านข้อมูลส่วนบุคคล[5]ซึ่งในปัจจุบันยังพบอุปสรรคในการนำลายมือชื่ออิเล็กทรอนิกส์มาใช้สำหรับประชาชนและเจ้าหน้าที่ของรัฐ เช่น กรณีที่จะทำอย่างไรให้ประชาชนเกิดความไว้วางใจและเชื่อถือหน่วยงานของรัฐในการคุ้มครองข้อมูลส่วนบุคคลมิให้ถูกนำไปใช้ผิดวัตถุประสงค์หรือผิดกฎหมาย ตลอดจนการนำหมายเลขประจำตัวส่วนบุคคลมาใช้ในหน่วยงานของภาครัฐซึ่งยังถือเป็นอุปสรรคสำคัญ เนื่องจากการทำรัฐบาลอิเล็กทรอนิกส์ได้เปลี่ยนรากฐานของการระบุตัวตนไปอย่างสิ้นเชิง

ในขณะที่ปัจจุบันภาครัฐของไทยมีการใช้และเก็บข้อมูลทางอิเล็กทรอนิกส์ได้ไม่นาน และยังไม่มีกฎหมายที่ให้ความคุ้มครองข้อมูลส่วนบุคคลบังคับใช้เป็นการเฉพาะ ทั้งที่การมีกฎหมายบังคับใช้อย่างเฉพาะเจาะจงนั้นมีความจำเป็นอย่างมาก อันเนื่องจากการทำธุรกรรมของรัฐบาลอิเล็กทรอนิกส์(e-Government)เป็นการทำธุรกรรมระหว่างหน่วยงานของรัฐกับเอกชนตลอดจนเป็นการทำธุรกรรมระหว่างหน่วยงานของรัฐกับหน่วยงานของรัฐด้วยกันเอง ซึ่งในบางครั้งหน่วยงานของรัฐมีอำนาจในการจัดเก็บข้อมูลที่สำคัญของบุคคล ดังนั้น ภาครัฐจึงต้องพัฒนากลไกการจัดเก็บรักษาข้อมูลให้มีความมั่นคงปลอดภัยและเป็นสากลเพื่อให้ประชาชนมีความมั่นใจในการทำธุรกรรมทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ ซึ่งจะเห็นได้ว่ามีความแตกต่างจากการทำธุรกรรมอิเล็กทรอนิกส์ทั่วไปที่เป็นการทำธุรกรรมระหว่างเอกชนกับเอกชนที่สามารถใช้หลักความยินยอมของผู้ถูกเก็บข้อมูลหรือโดยอาศัยบทบัญญัติของกฎหมายในการควบคุมดูแลการทำธุรกรรมทางอิเล็กทรอนิกส์ระหว่างเอกชนด้วยกันเอง มาควบคุมดูแลอยู่แล้ว

อนึ่ง การที่ภาครัฐของไทยจะให้บริการกับประชาชนผ่านทางอิเล็กทรอนิกส์ได้นั้น จำเป็นจะต้องมีการเก็บข้อมูลที่สำคัญต่าง ๆ ของประชาชนเอาไว้ เช่น ชื่อ-นามสกุล ที่อยู่ หมู่โลหิต ศาสนา ข้อมูลการเสียภาษี ตลอดจนข้อมูลการรักษาพยาบาล และข้อมูลทางคดีความ เป็นต้น ดังนั้น ย่อมเกิดเป็นความเสี่ยงที่จะมีข้อผิดพลาดในการจัดเก็บรักษาข้อมูลส่วนบุคคล (Personal Data)ของประชาชนที่หน่วยงานของรัฐมีอยู่ ซึ่งอาจส่งผลเสียและเกิดความเสียหายต่อประชาชนหรือหน่วยงานของรัฐได้หากเกิดกรณีมีข้อผิดพลาดเกิดขึ้น เช่น มีผู้ปลอมแปลงข้อมูลหรือมีผู้นำฐานข้อมูล(Database)ไปใช้ผิดวัตถุประสงค์ก็อาจส่งผลเสียต่อผู้ให้ข้อมูลเป็นอย่างมาก ซึ่งเหมือนกับกรณีที่เกิดขึ้นกับการทำธุรกรรมอิเล็กทรอนิกส์ในภาคเอกชน เช่น

---

[5] Adam Lebech, **Privacy and e-government Enterprise Challenges for Danish Government**, Danish ministry of Finance, IBM Privacy Technology Summit 9-10 July 2003 [online], 1 May 2012. Available from http://www.zurich.ibm.com/pdf/privacysummit/Lebech.pdf.

ตัวอย่างในกรณีบริษัท Epsilon Data Management ซึ่งเป็นบริษัทการตลาดออนไลน์ (Online)[6]ของประเทศสหรัฐอเมริกาซึ่งถูกแฮกเกอร์(Hacker)เจาะระบบเข้าไปขโมยข้อมูลส่วนตัวของผู้บริโภคที่บริษัท Epsilon เก็บรักษาไว้ เนื่องจากปรากฏว่าส่วนหนึ่งของข้อมูลที่ถูกขโมยไปนั้นเป็นข้อมูลชื่อและจดหมายอิเล็กทรอนิกส์(Electronics Mail : E-mail)ของลูกค้าของที่เป็นองค์กรขนาดใหญ่ในสหรัฐอเมริกามากกว่า 50 แห่ง ซึ่งทำให้ในขณะนี้ บริษัทต่าง ๆ ตลอดจนสถาบันการเงิน ร้านค้าปลีก และบริษัทเอกชนขนาดใหญ่ในประเทศสหรัฐอเมริกา เช่น JP Morgan, ChaseKroger , TiVo , Best Buy , Walgreen , Capital One และบริษัทอื่น ๆ เริ่มทำการประกาศเตือนภัยลูกค้าของตนเองให้ระวังภัยจากการล่อลวงในจดหมายอิเล็กทรอนิกส์ เนื่องจากข้อมูลที่เกี่ยวกับชื่อและจดหมายอิเล็กทรอนิกส์ของลูกค้าบางส่วนได้ถูกขโมยไป ทั้งนี้ บริษัท Epsilon ซึ่งได้ถูกเจาะระบบนั้นเป็นบริษัทรับจ้างบริษัทภายนอกมาทำงาน(Out Source)ในการบริการส่งจดหมายอิเล็กทรอนิกส์(E-Mail)แทนองค์กรต่าง ๆ ในสหรัฐอเมริกามากกว่า 2,500 แห่ง[7]

หรือตัวอย่างในกรณีของ American Life Insurance Company (ALICO) ซึ่งเป็นบริษัทประกันภัยในประเทศญี่ปุ่นและเป็นบริษัทในเครือของ American Life International Group (AIG) ได้เปิดเผยว่าข้อมูลบัตรเครดิตของลูกค้าราว 110,000 รายการ อาจรั่วไหลและอาจมีการนำข้อมูลในบัตรเครดิตไปใช้โดยทุจริตเพื่อซื้อสินค้ากว่า 1,000 รายการ ซึ่งบริษัท ALICO ได้รับแจ้งจากบริษัทบัตรเครดิตที่สงสัยว่าอาจเกิดปัญหาข้อมูลบัตรเครดิตของผู้ถือกรมธรรม์รั่วไหล โดยคนร้ายได้นำข้อมูลเหล่านั้นไปใช้ในการซื้อสินค้าทางอินเทอร์เน็ต ซึ่งบริษัท ALICO ยังไม่สามารถระบุได้ว่าข้อมูลรั่วไหลไปได้อย่างไร และยังไม่สามารถประเมินมูลค่าความเสียหายได้[8]

หรือตัวอย่างในกรณีจากการเปิดเผยของกรรมการผู้จัดการมูลนิธิเพื่อผู้บริโภคว่ามูลนิธิเพื่อผู้บริโภคได้รับการร้องเรียนและมีข้อเรียกร้องจากชมรมหนี้บัตรเครดิต(Credit Card) และสินเชื่อส่วนบุคคลที่มีสมาชิกประมาณ 3,700 ราย ให้สำนักงานประกันสังคม(สปส.)ทำการแก้ปัญหาการขายข้อมูลส่วนบุคคลให้แก่บริษัทบัตรเครดิตและผู้ประกอบการสินเชื่อบุคคล ซึ่งขณะนี้ยังไม่มีข้อมูลด้านตัวเลขที่ชัดเจนว่าผู้ถูกละเมิดสิทธิในส่วนนี้มีจำนวนเท่าไร นอกจากนี้ ยังมีกรณีบริษัทบัตรเครดิตทำการขายข้อมูลให้แก่บริษัทอื่นอีก เช่น กรณีที่ผู้บริโภครายหนึ่งติดต่อเรื่องซื้อบ้านกับธนาคารแห่งหนึ่ง แต่กลับมีธนาคารอีกแห่งทราบข้อมูลลูกค้าที่ซื้อบ้าน เป็นต้น ซึ่งในปัจจุบันข้อมูลส่วนบุคคลของลูกหนี้ไม่ได้ถูกนำไปใช้ให้เป็นประโยชน์

---

[6] Online หมายถึง การทำงานของระบบคอมพิวเตอร์ในขณะที่มีการเชื่อมต่อระบบอินเตอร์เน็ต

[7] ASTVผู้จัดการออนไลน์, **50 องค์กรมะกันป่วน ถูกขโมยข้อมูลลูกค้า** [online], 29 มีนาคม 2555. แหล่งที่มา http://www.manager.co.th/Cyberbiz/ViewNews.aspx?NewsID=9540000043136.

[8] สำนักข่าวไทย, **อลิโค ญี่ปุ่นทำข้อมูลบัตรเครดิตลูกค้ารั่วไหล** [online], 31 พฤษภาคม 2555. แหล่งที่มา http://news.mcot.net/bidnews/inside.php?nid=105865&ntype=text.

ทางกรรมการผู้จัดการมูลนิธิเพื่อผู้บริโภคจึงไม่เห็นด้วยกับการเก็บข้อมูลส่วนบุคคลเพราะถือว่าเป็นการละเมิดสิทธิส่วนบุคคล[9]

จากเหตุการณ์ดังกล่าวข้างต้น ย่อมแสดงให้เห็นว่าสถานการณ์การกระทำความผิดต่อข้อมูลส่วนบุคคลในการธุรกรรมอิเล็กทรอนิกส์ในภาคเอกชนมีผู้ได้รับผลกระทบเป็นจำนวนมาก ซึ่งก่อให้เกิดความเสียหายเป็นวงกว้างและเป็นการยากในประเมินมูลค่าของความเสียหายและจำนวนที่ผู้ได้รับผลกระทบเป็นจำนวนที่แน่นอน ประกอบกับการทำธุรกรรมอิเล็กทรอนิกส์ได้มีการพัฒนามาจากภาคเอกชนก่อนที่จะมีการนำมาใช้ในภาครัฐ ดังนั้น หน่วยงานของรัฐในประเทศต่าง ๆ รวมถึงประเทศไทยซึ่งได้มีการนำธุรกรรมอิเล็กทรอนิกส์มาใช้ในการให้บริการกับประชาชนจะต้องตระหนักถึงผลกระทบและความเสียหายที่อาจเกิดขึ้นได้หากมีกรณีที่มีการกระทำความผิดข้อมูลส่วนบุคคลเกิดขึ้นกับหน่วยงานของรัฐซึ่งจัดเก็บและดูแลข้อมูลส่วนบุคคลอยู่ และจากปัญหาดังกล่าว หน่วยงานของรัฐจึงต้องมีมาตรการที่เหมาะสมในการดูแลและให้ความคุ้มครองข้อมูลส่วนบุคคล เพื่อเป็นการสร้างความมั่นใจให้กับประชาชนผู้ใช้บริการและต้องมีบทลงโทษแก่ผู้กระทำผิดเพื่อให้เกิดความยำเกรงต่อกฎหมาย

นอกจากนี้ ในปัจจุบันหลายประเทศทั่วโลกต่างให้ความสำคัญกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลโดยได้มีการออกกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลเพื่อบังคับใช้และเป็นหลักประกันให้กับประชาชนว่าข้อมูลส่วนบุคคลของประชาชนจะได้รับความคุ้มครองในความเป็นส่วนตัวจากหน่วยงานของรัฐ เช่น

- ค.ศ. 1974 ประเทศสหรัฐอเมริกาเป็นประเทศแรกในการประกาศใช้ Privacy Act
- ค.ศ. 1974 ประเทศสวีเดน ประกาศใช้ The Data Act
- ค.ศ. 1988 ประเทศออสเตรเลียประกาศใช้ Privacy Protection Act
- ค.ศ. 1997 ประเทศเยอรมันได้ออกกฎหมายชื่อ Tele-services Data Protection Act
- ค.ศ. 1998 ประเทศอังกฤษได้ออกกฎหมายชื่อ Data Protection Act 1998[10]

ในกรณีสำหรับประเทศไทยนั้น ได้มีการกระทำความผิดที่เกี่ยวข้องกับข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์เกิดขึ้นหลายกรณี เช่น การซื้อขายฐานข้อมูล(Database)ของลูกค้าบริษัทเอกชน การถอดรหัส(Decode)บัตรเครดิตของบุคคลอื่นมาใช้โดยทุจริตเพื่อให้ได้มาซึ่งข้อมูลหรือทรัพย์สินของบุคคลนั้น เป็นต้น ซึ่งในเวลาต่อมาประเทศไทยจึงได้มีการเสนอร่าง

---

[9] มูลนิธิเพื่อนผู้บริโภค, **ลูกหนี้บัตรเครดิตโวยถูกขายข้อมูลส่วนตัว สปส.เต้นขู่เชือด พนง**. [online], 29 มีนาคม 2555. แหล่งที่มา http://old.consumerthai.org/cms/index.php?option=com_content&task=view&id=357&Itemid=73.

[10] วรรณศรี ทิวแพ, **การกำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคล : ศึกษาเฉพาะกรณีบัตรประจำตัวประชาชนแบบอเนกประสงค์**, (การค้นคว้าอิสระ รัฐประศาสนศาสตร์มหาบัณฑิต สาขาวิชานโยบายสาธารณะ มหาวิทยาลัยศรีนครินทรวิโรฒ, 2550), 2.

พระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล[11]โดยเป็นร่างกฎหมายที่ให้ความคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะ ซึ่งจะบังคับใช้กับข้อมูลส่วนบุคคลเป็นการทั่วไปเป็นฉบับแรก แต่ร่างพระราชบัญญัติดังกล่าวในปัจจุบันยังอยู่ระหว่างการพิจารณาร่างกฎหมายในกระบวนการนิติบัญญัติเพื่อทำการตีความกฎหมายและศึกษาถึงผลกระทบในการประกาศใช้พระราชบัญญัติดังกล่าว

ดังนั้น จะเห็นได้ว่าการมีมาตรการหรือกฎหมายที่กำหนดหลักเกณฑ์และแนวทางในการปฏิบัติงานให้หน่วยงานของรัฐปฏิบัติตามในเรื่องของความคุ้มครองข้อมูลส่วนบุคคล(Personal Data Protection)ที่ดีนั้นมีความจำเป็นอย่างยิ่ง เพื่อเป็นการสนับสนุนให้รัฐดำเนินงานตามแนวทางรัฐบาลอิเล็กทรอนิกส์(e-Government)ได้อย่างมีประสิทธิภาพและเพื่อเป็นการสร้างความเชื่อมั่นให้กับประชาชนในการแจ้งข้อมูลที่ถูกต้องและเป็นจริงให้กับภาครัฐ

1.2 วัตถุประสงค์ของการวิจัย

(1) เพื่อทราบถึงสภาพปัญหาทางด้านการละเมิดข้อมูลส่วนบุคคลและมาตรการในการให้ความคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐของไทย

(2) ศึกษามาตรการหรือกฎหมายที่รัฐไทยบังคับใช้อยู่ว่ามีความเหมาะสมหรือไม่ ถ้าการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐของไทยยังไม่ครอบคลุมเพียงพอ ควรจะมีมาตรการใดมาเพิ่มเติม

(3) ศึกษาเปรียบเทียบมาตรการหรือกฎหมายที่รัฐบังคับใช้อยู่ว่ามีความเหมาะสมหรือไม่ ถ้าการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐของไทยยังไม่ครอบคลุมเพียงพอ ควรจะมีมาตรการใดมาเพิ่มเติม

1.3 ขอบเขตของการทำวิจัย

ทำการศึกษาโดยวิธีการค้นคว้าวิจัยเกี่ยวกับมาตรการคุ้มครองข้อมูลส่วนบุคคลจากเอกสารวิชาการ ตำรา ตลอดจนข้อมูลทางอินเตอร์เน็ต ทั้งแหล่งข้อมูลของต่างประเทศและแหล่งข้อมูลภายในประเทศ โดยทำการศึกษาจากมาตรการคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกา สหภาพยุโรป และของประเทศไทย

[11] ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ..., ร่างพระราชบัญญัติที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้ว เรื่องเสร็จที่ 515/2552.

1.4 คำถามของการวิจัย

ประเทศไทยมีมาตรการหรือกฎหมายที่ให้ความคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐที่มีความเหมาะสมหรือไม่ ถ้ายังไม่มีมาตรการหรือกฎหมายที่เหมาะสม เห็นควรที่จะมีมาตรการใดมาเพิ่มเติม

1.5 ประโยชน์ที่คาดว่าจะได้รับจากการวิจัย

(1) ทราบถึงสภาพปัญหาทางด้านการละเมิดข้อมูลส่วนบุคคลและมาตรการการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐของไทยในปัจจุบัน

(2) ทราบถึงมาตรการหรือกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐของไทยว่าควรจะมีมาตรการใดมาเพิ่มเติม

(3) ทราบถึงมาตรการหรือกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐของสหรัฐอเมริกาและสหภาพยุโรปว่ามีมาตรการใดที่แตกต่างไปจากมาตรการหรือกฎหมายคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐที่ประเทศไทยบังคับใช้อยู่

1.6 นิยามศัพท์

“ข้อมูลข่าวสารส่วนบุคคล” หมายความว่า ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงานบรรดาที่มีชื่อของผู้นั้นหรือมีเลขหมายรหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ(Fingerprint) แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่าย และให้หมายความรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย[12]

“ธุรกรรมทางอิเล็กทรอนิกส์” หมายความว่า ธุรกรรมที่กระทำขึ้นโดยใช้วิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือแต่บางส่วน[13]

“รัฐบาลอิเล็กทรอนิกส์” หมายความว่า การนำเทคโนโลยีสารสนเทศและการสื่อสารมาใช้เป็นเครื่องมือในการบริหารจัดการ และบูรณาการการปฏิบัติงานของหน่วยงานภาครัฐเพื่อเพิ่มศักยภาพในการให้บริการประชาชน[14]

---

[12] พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540, มาตรา 4.

[13] เรื่องเดียวกัน.

[14] พระราชกฤษฎีกาจัดตั้งสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ. 2554, มาตรา 3.

“เครื่องหมายรับรองความน่าเชื่อถือ(Trust Mark)” หมายความว่า เครื่องหมายที่รับรองว่าหน่วยงานดังกล่าวมีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลของประชาชนในการทำธุรกรรมทางอิเล็กทรอนิกส์ซึ่งออกโดยหน่วยงานหรือองค์กรที่จัดตั้งโดยชอบด้วยกฎหมายเพื่อทำหน้าที่ในการตรวจสอบและรับรองการออกทรัสต์มาร์คให้กับผู้ขอรับการรับรอง[15]

[15] ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของประเทศด้านสารสนเทศของหน่วยงานรัฐ พ.ศ. 2553, ข้อ 3 วรรค 2.

บทที่ 2
ลักษณะทั่วไปของการคุ้มครองข้อมูลส่วนบุคคลและการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐในประเทศไทย

2.1 ความเป็นมาและแนวคิดในการนำมาตรการคุ้มครองข้อมูลส่วนบุคคลมาใช้ในประเทศไทย

สิทธิในความเป็นส่วนตัว ถือได้ว่าเป็นสิ่งสำคัญอย่างยิ่งอันเป็นสิทธิที่มนุษย์ตามหลักแนวความคิดในเรื่องกฎหมายธรรมชาติ(Natural Law)ซึ่งเป็นสิทธิของมนุษย์ที่มีอยู่ตามธรรมชาติ (Natural Rights)เพราะว่ามนุษย์นั้นเปรียบเสมือนสัตว์ที่จะต้องทำการป้องกันร่างกายและป้องกันทรัพย์สินของตนเอง ดังนั้น กฎหมายโดยแท้จริงแล้วมาจากสิทธิต่าง ๆ เหล่านี้ มิใช่ได้มาจากบทบัญญัติของรัฐ[1] ทั้งนี้ สิทธิในความเป็นส่วนตัวถือเป็นสิทธิขั้นพื้นฐานของมนุษย์ที่พึงมี แต่การที่มนุษย์มาอยู่ร่วมกันเป็นสังคมขนาดใหญ่มีผู้คนจากต่างเชื้อชาติ ต่างวัฒนธรรมและต่างศาสนามาอาศัยอยู่รวมกันนั้น ย่อมมีโอกาสที่บุคคลใดจะได้รับการละเมิดสิทธิในความเป็นส่วนตัวจากบุคคลอื่นไม่ว่าจะโดยตั้งใจหรือมิได้ตั้งใจก็ตาม ด้วยเหตุดังกล่าวหลายประเทศทั่วโลกจึงได้ให้ความสำคัญและได้มีการพัฒนาแนวความคิดเรื่องการคุ้มครองสิทธิในความเป็นส่วนตัวมาบัญญัติเป็นกฎหมายขึ้น เพื่อบังคับใช้เป็นหลักประกันสิทธิขั้นพื้นฐานในการเป็นพลเมืองของประเทศตนเองรวมถึงประเทศไทยซึ่งเห็นได้จากการที่บัญญัติเอาไว้ในรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550 เป็นต้น

ในขณะที่ประเทศสหรัฐอเมริกา ได้เริ่มมีการพัฒนาแนวความคิดในเรื่องการใช้กฎหมายคุ้มครองสิทธิในความเป็นส่วนตัว โดยการพัฒนาแนวความคิดดังกล่าวเริ่มเห็นได้อย่างชัดเจนภายหลังจากที่บทความทางวิชาการของ Samuel D. Warren และ Louis D. Brandies ได้ถูกทำการเผยแพร่ออกไปในปี ค.ศ. 1890 ซึ่งบทความนี้แม้ได้ถูกเผยแพร่ในยุคที่ยังไม่มีการแพร่หลายของเทคโนโลยีสารสนเทศดังเช่นในปัจจุบัน แต่ผู้เขียนทั้งสองได้เล็งเห็นถึงการละเมิดสิทธิในความเป็นส่วนตัวและได้ระบุไว้ในงานเขียนเรื่อง “The Right to Privacy”[2]โดยมีสาระสำคัญซึ่งกล่าวถึงการพัฒนาของกฎหมายในช่วงแรกนั้น ได้ให้การเยียวยาเพียงการคุกคามทางร่างกายที่กระทำต่อชีวิต ทรัพย์สิน และสิทธิที่จะมีชีวิตอยู่(Right of Life)เท่านั้น ซึ่งกฎหมายได้ถูกใช้เพื่อคุ้มครองบุคคลจากการทำร้ายในรูปแบบต่าง ๆ ต่อมาจึงเริ่มมีการพัฒนาแนวความคิดโดยให้มีความคุ้มครองครอบคลุมถึงสภาพจิตใจของบุคคลรวมถึงความรู้สึกและสติปัญญาของมนุษย์ ซึ่งจะเห็นได้ว่ากฎหมายได้ขยายขอบเขตครอบคลุมถึงสิทธิต่างๆ มากขึ้นทีละน้อย โดยเริ่มจากสิทธิที่จะมี

---

[1] James A. Donald, **Natural Law and Natural Right** [online], 3 July 2012 Available from http://jim.com/rights.html.

[2] Ben Bratman, **"The Right to Privacy and the Birth of the Right to Privacy"**, Tennessee Law Review, University of Pittsburgh Legal Studies Research Paper, (Vol. 69, 2002), 623.

ชีวิตอยู่จนกระทั่งได้กลายมาเป็นสิทธิในการดำรงชีวิตอย่างมีความสุขหรือสิทธิในการที่จะอยู่เพียงลำพัง(The right to be let alone)โดยเป็นการขยายความหมายให้ครอบคลุมถึงการคุ้มครองทั้งในแบบนามธรรมและรูปธรรม[3]ซึ่งอาจหมายความรวมถึงการคุ้มครองสิทธิในความเป็นส่วนตัวในข้อมูลส่วนบุคคลด้วย

นอกจากนี้ บทความดังกล่าวยังได้ให้คำจำกัดความถึงขอบเขตในการให้ความคุ้มครองสิทธิส่วนบุคคลว่าเป็นสิทธิขั้นพื้นฐานอันเป็นเสรีภาพส่วนบุคคล เนื่องจากในยุคปัจจุบันหน่วยงานของรัฐและองค์กรต่าง ๆ ได้มีการพัฒนาการบริหารจัดการหน่วยงานหรือองค์กรให้มีประสิทธิภาพ มากขึ้น ดังนั้น จึงมีโอกาสมากขึ้นที่หน่วยงานเหล่านั้นจะเข้ามาลุกล้ำกิจกรรมส่วนบุคคลที่ครั้งหนึ่งเคยเป็นสิ่งที่ไม่อาจเข้าถึงได้ ด้วยเหตุดังกล่าวจึงมีความจำเป็นที่จะต้องพัฒนากฎหมายและมาตรการคุ้มครองข้อมูลส่วนบุคคลเพื่อตอบสนองต่อการเปลี่ยนแปลงทางเทคโนโลยีที่เกิดขึ้นอย่างรวดเร็ว ซึ่งข้อห้ามที่เกี่ยวข้องกับการล่วงล้ำ การดูหมิ่น การต่อต้าน และการกระทำซึ่งเป็นการรุกรานแบบเดิม ๆ เป็นมาตรการที่ใช้ได้เพียงกับยุคก่อนแต่ไม่สามารถที่จะใช้เพื่อปกป้องบุคคลจากผู้ครอบครองอุปกรณ์ที่ทันสมัยในยุคปัจจุบันได้[4]

ทั้งนี้ ในปัจจุบันปัญหาการละเมิดสิทธิในความเป็นส่วนตัวมีมากขึ้น โดยเฉพาะอย่างยิ่งการละเมิดสิทธิความเป็นส่วนตัวโดยการใช้เทคโนโลยีสารสนเทศและการสื่อสารซึ่งเกิดขึ้นได้ทั่วทุกมุมโลก โดยมักเป็นการขโมยข้อมูลที่สำคัญรวมถึงข้อมูลส่วนบุคคลโดยอาศัยระบบอินเตอร์เน็ต(Internet)หรืออาศัยการเชื่อมต่อของระบบคอมพิวเตอร์(Computer)ในรูปแบบต่าง ๆ เป็นสื่อกลางในการกระทำความผิดต่อข้อมูล

ดังนั้น จากแนวความคิดในการให้ความคุ้มครองด้านสิทธิมนุษยชนหรือสิทธิในความเป็นส่วนตัว ส่งผลให้สหประชาชาติ(United Nations)ได้ให้ความสำคัญและตระหนักถึงความจำเป็นในการมีหลักเกณฑ์หรือกฎหมายที่ให้ความคุ้มครองทางด้านสิทธิมนุษยชน จึงได้มีการออกปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ. 1984(Universal Declaration of Human Right 1984)[5]เพื่อใช้เป็นแนวทางให้ประเทศต่าง ๆ ได้นำไปปรับใช้เพื่อเป็นแนวทางในการพัฒนาด้านการคุ้มครองสิทธิมนุษยชนในประเทศของตนให้สอดคล้องกับปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ. 1984 ดังนั้น จึงมีความจำเป็นที่จะต้องทำความเข้าใจกับสิทธิในความเป็นส่วนตัว ซึ่งในปัจจุบันย่อม

---

[3] Samuel D. Warren & Louis D. Brandies, **The Right to Privacy**, Harvard Law Review (Vol. 4, 1890), 5.

[4] Samuel D. Warren & Louis D. Brandies, **Context of The Right to Privacy** [Online], Harvard Law Review. Available from 1 June 2012 from http://faculty.uml.edu/sgallagher/Harvard__law_review.htm

[5] The Universal Declaration of Human Rights 1948.

หมายความรวมถึงสิทธิที่จะได้รับความคุ้มครองในข้อมูลส่วนบุคคล ซึ่งถือเป็นพัฒนาการของกฎหมายในปัจจุบันที่ให้ความคุ้มครองครอบคลุมถึงความเสียหายในเชิงนามธรรมด้วย

2.1.1. ความหมายของคำว่าข้อมูลส่วนบุคคล

นักวิชาการหลายท่าน รวมถึงบทบัญญัติในกฎหมายฉบับต่าง ๆ ได้มีการให้คำนิยามความหมายของคำว่า “ข้อมูลส่วนบุคคล” แตกต่างกันออกไป เช่น

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อความใดๆ อันระบุตัว หรืออาจระบุตัวบุคคลได้[6]

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อความใดๆ ที่เกี่ยวกับบุคคลธรรมดาอันระบุตัวหรืออาจระบุตัวบุคคลนั้นได้ ซึ่งบุคคลที่อาจถูกระบุตัวได้ไม่ว่าโดยตรงหรือโดยอ้อมนี้อาจทำได้โดยการอ้างอิงจากหมายเลขเฉพาะของบุคคล(Identification Number)หรือจากปัจจัยอื่น ๆ ที่มีลักษณะเฉพาะในทางร่างกาย จิตใจ ฐานะทางเศรษฐกิจ เอกลักษณ์ทางวัฒนธรรมและสังคมของบุคคลนั้นเป็นต้น[7]

ทั้งนี้ แม้ว่านิยามของคำว่า ข้อมูลส่วนบุคคลจะอธิบายไว้แตกต่างกันออกไป แต่จะเห็นได้ว่ามีความหมายในลักษณะที่ใกล้เคียงกัน โดยแนวความคิดเรื่องการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยได้รับแนวความคิดและแนวทางการพัฒนามาจากข้อตกลงระหว่างประเทศที่สำคัญ ดังต่อไปนี้

(1) ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ.1948(The Universal Declaration of Human Rights 1948)ซึ่งถือเป็นมติที่สำคัญของสมัชชาใหญ่แห่งสหประชาชาติและเป็นกฎหมายแม่บทด้านสิทธิมนุษยชน ซึ่งถือเป็นจารีตประเพณีระหว่างประเทศและเป็นรากฐานของความร่วมมือด้านสิทธิมนุษยชนฉบับต่าง ๆ ในภายหลัง ซึ่งในบทบัญญัติ Article 12. กำหนดไว้ว่า

“บุคคลใดจะถูกแทรกแซงโดยพลการในความเป็นอยู่ส่วนตัวในครอบครัว ในเคหสถานหรือในการสื่อสารหรือจะถูกดูหมิ่นในเกียรติยศและชื่อเสียงไม่ได้และบุคคลดังกล่าวมีสิทธิที่จะได้รับความคุ้มครองของกฎหมายต่อการแทรกแซงหรือการดูหมิ่นดังกล่าวด้วย”[8]

---

[6] Organization for Economic Co-operation and Development, **Guidelines on the protection of Privacy and Transborder Data Flows of Personal Data**, Article 1 b).

[7] **DIRECTIVE 95/46/EC of THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data**, Article 2 (a).

[8] The Universal Declaration of Human Rights 1948, Article 12.

(2) องค์กรเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (Organization for Economic Co-operation and Development : OECD)[9]ซึ่งเป็นองค์กรระหว่างประเทศที่จัดตั้งขึ้นในปี ค.ศ. 1961 โดยพัฒนามาจาก (Organization for European Economic Co-operation : OEEC) ซึ่งจัดตั้งขึ้นในปี ค.ศ. 1948 เพื่อบริหารเงินช่วยเหลือจากสหรัฐอเมริกาและแคนาดาภายใต้แผนการมาร์แชล(Marshall Plan)เพื่อทำการบูรณะฟื้นฟูสภาพเศรษฐกิจและสังคมของยุโรปภายหลังสงครามโลก ครั้งที่ 2 ซึ่ง OECD มีบทบาทสำคัญในการเสริมสร้างความแข็งแกร่งทางเศรษฐกิจให้แก่ประเทศสมาชิก โดยทำการปรับปรุงประสิทธิภาพการบริหารจัดการตลอดจนส่งเสริมการค้าเสรี และให้ความช่วยเหลือเพื่อการพัฒนาทั้งในประเทศอุตสาหกรรมและประเทศกำลังพัฒนา ซึ่งต่อมาในปัจจุบันภารกิจของ OECD ได้มีการเปลี่ยนแปลงไปจากเดิมที่เน้นการตรวจสอบนโยบายในด้านต่าง ๆ ของประเทศสมาชิกไปสู่การวิเคราะห์แนวทางที่จะนำนโยบายไปใช้ได้โดยสามารถมีปฏิสัมพันธ์ร่วมกันระหว่างประเทศสมาชิกภายในกลุ่มและกับประเทศภายนอกกลุ่ม โดยเฉพาะในประเด็นปัญหาข้ามชาติต่าง ๆ อันเกิดจากกระแสโลกาภิวัตน์ (Globalization) ซึ่งในปัจจุบัน OECD ถือเป็นองค์กรวิจัยที่มีคุณภาพที่สุดองค์กรหนึ่งของโลก เป็นแหล่งรวมข้อมูลวิจัยด้านต่างๆ ให้แก่ประเทศสมาชิกโดยสามารถปรึกษา ค้นคว้า รวมทั้งขอข้อเสนอแนะเกี่ยวกับแนวปฏิบัติอันเป็นเลิศในด้านต่าง ๆ[10] ซึ่งรวมถึงกรอบในการคุ้มครองข้อมูลส่วนบุคคล (Guidelines on the protection of Privacy and Transborder Data Flows of Personal Data แห่ง OECD) ซึ่งประกอบด้วยหลักการที่สำคัญ 8 ประการ ได้แก่

(ก) หลักข้อจำกัดในการเก็บรวบรวมข้อมูล (Collection Limitation Principle)

(ข) หลักคุณภาพของข้อมูล (Data Quality Principle)

(ค) หลักการกำหนดวัตถุประสงค์ในการจัดเก็บ (Purpose Specification Principle)

(ง) หลักข้อจำกัดในการนำไปใช้ (Use Limitation Principle)

(จ) หลักการรักษาความมั่นคงปลอดภัยข้อมูล (Security Safeguards Principle)

(ฉ) หลักการเปิดเผยข้อมูล (Openness Principle)

(ช) หลักการมีส่วนร่วมของบุคคล (Individual Participation Principle)

(ซ) หลักความรับผิดชอบ (Accountability Principle)

---

[9] ศูนย์บริการข้อมูลเศรษฐกิจระหว่างประเทศ. กรมเศรษฐกิจระหว่างประเทศ. กระทรวงการต่างประเทศ. **กรอบความร่วมมือเศรษฐกิจระหว่างประเทศ** [online], 10 เมษายน 2555. แหล่งที่มา http://www.mfa.go.th/business/2026.php.

[10] เรื่องเดียวกัน.

ต่อมาจึงได้มีการนำแนวความคิดด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคลมาใช้ในประเทศไทย โดยบัญญัติเอาไว้ในรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550 มาตรา 35 ซึ่งบัญญัติว่า “สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง ตลอดจนความเป็นอยู่ส่วนตัวย่อมได้รับความคุ้มครอง

การกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชนอันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัวจะกระทำมิได้ เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณะ

บุคคลย่อมมีสิทธิได้รับความคุ้มครองจากการแสวงประโยชน์โดยมิชอบจากข้อมูลส่วนบุคคลที่เกี่ยวกับตน ทั้งนี้ ตามที่กฎหมายบัญญัติ”[11]

ดังนั้น จะเห็นได้ว่าประเทศไทยได้รับแนวความคิดในเรื่องการคุ้มครองข้อมูลส่วนบุคคลมาจากปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ.1948 เป็นลำดับแรก จากนั้นได้มีการพัฒนาแนวคิดเรื่อยมาจนกระทั่งมีการบัญญัติเอาไว้ในรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550 ซึ่งหมายถึง ประชาชนไทยย่อมได้รับความคุ้มครองสิทธิส่วนบุคคลตามสมควร

อย่างไรก็ดี แม้ว่าในปัจจุบันประเทศไทยจะยังไม่มีกฎหมายที่ให้ความคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะมาบังคับใช้เป็นการทั่วไป แต่คณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติได้แต่งตั้งคณะอนุกรรมการเฉพาะกิจเพื่อยกร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลขึ้นเพื่อบังคับใช้ โดยในปัจจุบันได้มีการปรับเปลี่ยนแนวทางการยกร่างจำนวน 2 ครั้ง คือ

<u>ครั้งที่หนึ่ง</u> ได้มีการยกร่างขึ้นตามแนวทาง Directive 95/46/EC of the European Parliament and of the Council of 24 October1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ของสหภาพยุโรป(European Union : EU) เป็นหลัก[12]

<u>ครั้งที่สอง</u> เนื่องจากการให้ความคุ้มครองข้อมูลส่วนบุคคลที่ได้รับผลกระทบจากการพัฒนาทางเทคโนโลยีเป็นเรื่องที่ค่อนข้างใหม่สำหรับประเทศไทย ดังนั้น การที่จะนำกลไกที่เข้มงวดมาบัญญัติเป็นกฎหมายเพื่อบังคับใช้ อาจก่อให้เกิดปัญหาในทางปฏิบัติในการบังคับใช้กฎหมายได้ ด้วยเหตุดังกล่าวจึงได้มีปรับเปลี่ยนแนวทางการยกร่างกฎหมายโดยมีการศึกษา

---

[11] รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2550, มาตรา 35.

[12] สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์, **แนวทางการจัดทำกฎหมายคุ้มครองข้อมูลส่วนบุคคล**, (ม.ป.พ, 2546), 12.

กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของประเทศอื่นมาเพิ่มเติมนอกเหนือจากประเทศภาคพื้นยุโรป กล่าวคือ กฎหมายของประเทศออสเตรเลีย นิวซีแลนด์ และเขตปกครองพิเศษฮ่องกง ซึ่งแม้ว่าประเทศต่าง ๆ เหล่านี้จะมีหลักการในการให้ความคุ้มครองข้อมูลส่วนบุคคลใกล้เคียงกับกฎหมายของสหภาพยุโรปก็ตาม แต่กฎหมายของประเทศเหล่านี้มีหลักการในการให้ความคุ้มครองข้อมูลส่วนบุคคลในอีกรูปแบบหนึ่งที่สำคัญ คือ การกำกับดูแลตนเอง (Self Regulation)ซึ่งเป็นมาตรการที่กำหนดให้ผู้ที่เก็บหรือรวบรวมข้อมูลส่วนบุคคลสามารถที่จะกำหนดหรือวางหลักเกณฑ์ในทางปฏิบัติที่สอดคล้องกับการดำเนินงานของตนเองได้ ซึ่งการบัญญัติกฎหมายในแนวที่ค่อนข้างมีความยืดหยุ่นและน่าจะเหมาะสมกับประเทศไทยซึ่งยังอยู่ในช่วงเริ่มต้นของการพัฒนาแนวความคิดในเรื่องการให้ความคุ้มครองสิทธิในความเป็นส่วนตัวในเรื่องข้อมูลส่วนบุคคล[13]

2.1.2. ประเภทของข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล เป็นสิ่งที่มีความสำคัญซึ่งผู้เก็บข้อมูลหรือผู้ควบคุมข้อมูลต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่ดีพอ ซึ่งหากทำการจำแนกข้อมูลส่วนบุคคลแล้วอาจแบ่งประเภทของข้อมูลส่วนบุคคลได้จากลักษณะของข้อมูลส่วนบุคคลซึ่งมีเป็น 2 ประเภท ดังนี้

(1) ข้อมูลส่วนบุคคลที่เปิดเผยได้หรือข้อมูลส่วนบุคคลทั่วไป(Non-sensitive)[14]

หมายถึง ข้อมูลส่วนบุคคลที่มักจะเป็นข้อมูลที่เกี่ยวข้องกับบุคคลใดอันเป็นข้อมูลที่นำมาประมวลผลรวมกันเป็นข้อเท็จจริงที่สามารถบ่งชี้ลักษณะเฉพาะตัวของบุคคลได้ เช่น ชื่อ นามสกุล ที่อยู่ อายุ ระดับการศึกษา ตำแหน่งหน้าที่การงาน ตลอดจนหมายเลขโทรศัพท์ที่ทำงาน เป็นต้น ซึ่งข้อมูลดังกล่าวโดยสภาพของข้อมูลเหล่านี้อาจเป็นข้อมูลข่าวสารส่วนบุคคลที่สามารถเปิดเผยต่อสาธารณะได้

(2) ข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นพิเศษ (Sensitive Data)[15]

หมายถึง ข้อมูลส่วนบุคคลที่ไม่สามารถเปิดเผยต่อสาธารณชนได้ เนื่องจากเป็นเรื่องส่วนบุคคลโดยเฉพาะ ซึ่งเจ้าของข้อมูลส่วนบุคคลมีความประสงค์ที่จะปกปิดไว้เพื่อ

---

[13] เรื่องเดียวกัน, 13.

[14] วรรณศรี ทิวแพ, **การกำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคล : ศึกษาเฉพาะกรณีบัตรประจำตัวประชาชนแบบอเนกประสงค์**, (การค้นคว้าอิสระ : รัฐประศาสนศาสตรมหาบัณฑิต สาขาวิชานโยบายสาธารณะ มหาวิทยาลัยศรีนครินทรวิโรฒ, 2550), 9.

[15] เรื่องเดียวกัน.

ความเป็นส่วนตัวของบุคคลของผู้เป็นเจ้าของข้อมูล เช่น การดำเนินชีวิตส่วนตัว ทัศนคติ ความเชื่อทางศาสนา ลัทธิการเมือง ความพิการทางร่างกาย พฤติกรรมทางเพศ หรือบทสนทนาทางโทรศัพท์ เป็นต้น ซึ่งข้อมูลเหล่านี้เป็นข้อมูลที่มีความอ่อนไหวเป็นพิเศษกว่าข้อมูลข่าวสารทั่วไปซึ่งหากคำนึงถึงความรู้สึกของวิญญูชนโดยทั่วไปแล้ว การเปิดเผยของข้อมูลประเภทนี้อาจกระทบถึงความรู้สึกไปในทางลบต่อชื่อเสียงและเกียรติคุณได้ ซึ่งในบางกรณีการเปิดเผยข้อมูลส่วนบุคคลก็อาจเกิดเป็นความเสี่ยงที่จะเกิดอันตรายต่อบุคคลนั้นได้ เช่น การแสดงออกถึงเชื้อชาติในสถานที่หรือช่วงเวลาไม่เหมาะสมอาจทำให้บุคคลนั้นอยู่ในภาวะอันตรายต่อชีวิตได้ ดังปรากฏในกรณีเรื่องความแตกแยกทางด้านเผ่าพันธุ์ระหว่างชนเผ่าตุดซี(Tusi)และชนเผ่าฮูตู (Hutu)ในประเทศราวันดา(Rwanda)ซึ่งมีความขัดแย้งทางเชื้อชาติรุนแรงถึงขั้นเป็นสงครามกลางเมือง โดยมีการฆ่าล้างเผ่าพันธุ์กันอย่างรุนแรงในช่วงปี พ.ศ. 2527[16]ส่งผลให้ประชาชนของประเทศราวันดาในช่วงเวลาดังกล่าวต้องปิดบังเชื้อชาติเผ่าพันธุ์ของตนเองไว้เพื่อความปลอดภัยของชีวิต หรืออาจศึกษาได้ในกรณีการแสดงออกถึงเชื้อชาติและทัศนะคติทางการเมือง ซึ่งอาจทำให้เกิดอันตรายต่อชีวิตจากฆ่าล้างเผ่าพันธุ์ในประเทศกัมพูชาในช่วงประมาณปี พ.ศ. 2518 - 2522 ซึ่งกลุ่มชาวกัมพูชาที่เรียกตนเองว่า“กองทัพแห่งชาติกัมพูชาประชาธิปไตย” หรือ “เขมรแดง” (Khmer Rouge) มีความต้องการให้ประเทศกัมพูชาเป็นประเทศที่มีผู้คนเพียงเชื้อสายเดียวเท่านั้น คือ คนเชื้อสายกัมพูชา ดังนั้น ชนกลุ่มน้อยอย่างชาวเวียดนามและชาวจีนจึงถูกฆ่าล้างเผ่าพันธุ์ตลอดรวมถึงคนกัมพูชาด้วยกันเอง ซึ่งจากการประเมินคาดว่ามีผู้เสียชีวิตประมาณ 1.5 - 2 ล้านคน ซึ่งถือเป็นการฆ่าล้างเผ่าพันธุ์ที่เลวร้ายที่สุดของกัมพูชา[17]

จากกรณีศึกษาดังกล่าว แม้จะไม่ใช่กรณีที่เป็นเรื่องของการเปิดเผยข้อมูลส่วนบุคคลและนำไปใช้ในทางทุจริตก็ตาม แต่ก็ทำให้ตระหนักได้ว่าข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นพิเศษนั้น เป็นข้อมูลที่ไม่ควรบันทึกจัดเก็บไว้หากไม่มีความจำเป็นและในการบันทึกข้อมูลนั้นจะต้องมีมาตรการคุ้มครองในระดับที่สูงกว่าข้อมูลส่วนบุคคลทั่วไป ด้วยเหตุดังกล่าวหลายประเทศทั่วโลกจึงเคร่งครัดกับข้อมูลส่วนบุคคลประเภทนี้มากกว่าข้อมูลส่วนบุคคลทั่วไป โดยอาจมีมาตรการในการห้ามเก็บบันทึก ห้ามใช้ และห้ามประมวลผลข้อมูลประเภทนี้ไม่ว่ากรณีใด เว้นแต่กฎหมายบัญญัติไว้เป็นการเฉพาะ เป็นต้น

อย่างไรก็ตาม คำว่า “ความเป็นส่วนตัว”(Privacy)เป็นคำที่มีความหมายค่อนข้างกว้างครอบคลุมได้หลายกรณี โดยในปัจจุบันได้มีกฎหมายคุ้มครองความเป็นส่วนตัวจำนวน

---

[16] United Human Right Council, **Genocide in Rwanda** [online], 1 June 2012. Available from http://www.unitedhumanrights.org/genocide/genocide_in_rwanda.htm

[17] Yale University, **The Cambodian Genocide Program** [online], 1 June 2012. Available from http://www.yale.edu/cgp/thai/index.html.

หลายฉบับ ซึ่งอาจสะท้อนถึงการคุ้มครองความเป็นส่วนตัวที่ปรากฏให้เห็นได้ในกฎหมายแตกต่างกัน โดยในส่วนของความเป็นส่วนตัวเกี่ยวกับข้อมูลข่าวสาร(Information Privacy)[18]ซึ่งหมายถึง สิทธิของมนุษย์ในการได้รับความคุ้มครองในเรื่องของข้อมูลส่วนบุคคลซึ่งไม่ประสงค์ที่จะเปิดเผยให้ผู้ใดรับรู้ เช่น การให้ความคุ้มครองข้อมูลส่วนบุคคลโดยการวางหลักเกณฑ์ที่เกี่ยวข้องกับการจัดเก็บรวบรวมและการบริหารจัดการข้อมูลส่วนบุคคลหรือเป็นที่รู้จักกันภายใต้คำว่า “Data Protection” เช่น พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล เป็นต้น

2.1.3. รูปแบบของการให้ความคุ้มครองข้อมูลส่วนบุคคล

การมีมาตรการคุ้มครองสิทธิในความเป็นส่วนตัวซึ่งหมายความรวมถึงข้อมูลส่วนบุคคลด้วยนั้นมีความสำคัญเป็นอย่างยิ่ง เนื่องจากในปัจจุบันเทคโนโลยีสารสนเทศได้มีการพัฒนาให้ความทันสมัยมากยิ่งขึ้น ดังนั้น การละเมิดสิทธิในความเป็นส่วนตัวย่อมอาจเกิดขึ้นได้ด้วยวิธีการแบบใหม่ ส่งผลให้ข้อมูลซึ่งถือว่าเป็นสื่อกลางสำคัญที่ใช้แลกเปลี่ยนในการใช้เทคโนโลยีในปัจจุบันมีความเสี่ยงมากยิ่งขึ้น จึงต้องมีการเร่งพัฒนามาตรการในการให้ความคุ้มครองข้อมูลส่วนบุคคลให้มีประสิทธิภาพเท่าทันต่อสถานการณ์ในปัจจุบัน ซึ่งอาจแบ่งพิจารณาได้เป็น 3 รูปแบบ ดังต่อไปนี้

(1) รูปแบบที่เป็นบัญญัติเป็นกฎหมายทั่วไป

การบัญญัติมาตรการคุ้มครองข้อมูลส่วนบุคคลขึ้นเป็นกฎหมายทั่วไปมีความจำเป็นซึ่งจะส่งผลให้เป็นการบังคับใช้กฎหมายอย่างกว้างเพื่ออุดช่องว่างของกฎหมายในกรณีที่ไม่มีบทบัญญัติใดมาเทียบเคียงได้ อีกทั้งยังเป็นการประกันสิทธิเสรีขั้นพื้นฐานในการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศนั้นด้วย ซึ่งแต่ละประเทศอาจบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลแตกต่างกันออกไป ตามแต่ความเหมาะสมของแต่ละประเทศ

(2) รูปแบบที่บัญญัติเป็นกฎหมายคุ้มครองแต่ละเรื่องไว้โดยเฉพาะ

การบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลขึ้นบังคับใช้ในแต่ละเรื่องเป็นกรณีเฉพาะเจาะจงนั้น เป็นกรณีที่มีความจำเป็นที่จะต้องให้ความคุ้มครองกับข้อมูลส่วนบุคคลในกรณีโดยเฉพาะ เช่น การคุ้มครองข้อมูลในการทำธุรกรรมกับธนาคารและสถาบัน

---

[18] สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์, **แนวทางการจัดทำกฎหมายคุ้มครองข้อมูลส่วนบุคคล**, (ม.ป.พ, 2546), 19.

การเงิน หรือการทำธุรกรรมที่เกี่ยวข้องกับบัตรอิเล็กทรอนิกส์ เป็นต้น ซึ่งแต่ละกรณีอาจมีความแตกต่างกันตามแต่ความเหมาะสม และความจำเป็นในการคุ้มครองข้อมูลส่วนบุคคลในเรื่องนั้น

(3) รูปแบบที่เป็นการกำกับดูแลตนเอง

นอกจากมาตรการในทางกฎหมายซึ่งรัฐได้บัญญัติขึ้นในกรณีบังคับใช้เป็นการทั่วไปและเป็นการเฉพาะแล้วนั้น ยังมีการให้ความคุ้มครองข้อมูลส่วนบุคคลในอีกรูปแบบหนึ่ง ซึ่งเรียกว่า การกำกับดูแลตนเอง(Self-Regulation) กล่าวคือ การที่หน่วยงานหรือองค์กรได้ทำการกำหนดแบบแผน วิธีปฏิบัติ หรือประมวลจริยธรรมขึ้นเพื่อบังคับใช้ในหน่วยงานหรือองค์กรของตนเอง โดยหน่วยงานหรือองค์กรดังกล่าวมีหน้าที่ที่จะต้องดูแลให้บุคลากรของตนมีการปฏิบัติตามแบบแผนหรือแนวนโยบายที่กำหนดไว้โดยสอดคล้องกัน

2.2 การทำธุรกรรมทางอิเล็กทรอนิกส์ของภาครัฐในประเทศไทย

ภายใต้ยุคสมัยที่เทคโนโลยีสารสนเทศได้มีการพัฒนาไปอย่างรวดเร็วนั้น การทำธุรกรรมอิเล็กทรอนิกส์ในประเทศไทยได้มีการพัฒนาและนำมาปรับใช้กับภาคเอกชนก่อน หลังจากนั้นภาครัฐจึงได้มีการพัฒนาและนำมาปรับใช้กับการทำธุรกรรมอิเล็กทรอนิกส์ในหน่วยงานหรือองค์กรของรัฐ ซึ่งได้ตระหนักถึงความจำเป็นในการพัฒนาระบบการบริหารงานและระบบการให้บริการของหน่วยงานรัฐให้มีประสิทธิภาพและมีความทันสมัยมากขึ้น เพื่อเป็นการเพิ่มขีดความสามารถในการให้บริการประชาชนให้ได้รับความสะดวก รวดเร็ว ทั่วถึงและเป็นธรรมมากยิ่งขึ้น กระทั่งได้จัดตั้งโครงการรัฐบาลอิเล็กทรอนิกส์ หรือ e-Government ภายใต้กรอบนโยบายเทคโนโลยีสารสนเทศของประเทศไทยเป็นฉบับที่ 2 หรือ IT2010[19]ซึ่งจะครอบคลุมเป็นระยะเวลา 10 ปี (ระหว่าง พ.ศ. 2544-2553) โดยได้รับความเห็นชอบจากคณะรัฐมนตรีในวันที่ 19 มีนาคม พ.ศ. 2545[20]และพัฒนาต่อเนื่องมาจนถึงปัจจุบันซึ่งอยู่ภายใต้กรอบนโยบายเทคโนโลยีสารสนเทศและการสื่อสาร ระยะ พ.ศ.2554-2563 ของประเทศไทยหรือนโยบาย IT2020 ซึ่งได้รับความเห็นชอบจากคณะรัฐมนตรี เมื่อวันที่ 22 มีนาคม พ.ศ. 2554[21]เพื่อเป็นการให้ความสำคัญ

---

[19] ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, **กรอบนโยบายเทคโนโลยีสารสนเทศและการสื่อสารระยะ พ.ศ.2544-2553** [online], 22 มีนาคม 2555. แหล่งที่มา http://www.nectec.or.th/pld/it 2010/index.html.

[20] เรื่องเดียวกัน.

[21] สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, **บทสรุปผู้บริหาร : แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร (ฉบับที่ 2) ของประเทศไทย พ.ศ. 2552-2556**, (ม.ป.พ., 2544), 1.

ต่อบทบาทของเทคโนโลยีสารสนเทศและการสื่อสารที่มีต่อการพัฒนาเศรษฐกิจและสังคม โดยมุ่งเน้นการยกระดับคุณภาพชีวิตของประชาชนและสังคมไทยให้มุ่งไปสู่สังคมแห่งภูมิปัญญาและการเรียนรู้[22]

ทั้งนี้ การทำธุรกรรมที่เพิ่มมากขึ้นของหน่วยงานรัฐในปัจจุบัน ส่งผลให้การบริหารงานและการจัดเก็บข้อมูลของหน่วยงานราชการต่างมีความสลับซับซ้อนมากขึ้น จึงมีความจำเป็นที่จะต้องเก็บข้อมูลในแบบดิจิตอล(Digital)เพื่อความสะดวก รวดเร็ว และประหยัดงบประมาณ จึงได้มีการนำการทำธุรกรรมทางอิเล็กทรอนิกส์มาใช้กับหน่วยงานของรัฐ ไม่ว่าจะเป็นการเชื่อมต่อข้อมูลระหว่างหน่วยงานของรัฐด้วยกันเองและการเชื่อมต่อข้อมูลระหว่างหน่วยงานของรัฐกับประชาชนผู้ใช้บริการ โดยเฉพาะอย่างยิ่งกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งเป็นหน่วยงานหลักในการพัฒนาและประยุกต์เทคโนโลยีสารสนเทศเข้ามาใช้ในการบริหารจัดการและการดำเนินงานของภาครัฐให้มีประสิทธิภาพตลอดจนมีความต่อเนื่องและเป็นรูปธรรมมากขึ้น ซึ่งภายหลังจากที่ได้ดำเนินการตามแนวทางของแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารมาได้ระยะหนึ่ง พบว่ามีอุปสรรคที่สำคัญประการหนึ่งในการดำเนินงานด้านรัฐบาลอิเล็กทรอนิกส์ คือ การขาดแคลนบุคลากรผู้เชี่ยวชาญในการดำเนินงาน ดังนั้น คณะรัฐมนตรีจึงมีมติวันที่ 25 พฤศจิกายน พ.ศ. 2553[23]เห็นควรให้มีการจัดตั้ง “สำนักงานรัฐบาลอิเล็กทรอนิกส์” โดยเป็นองค์การมหาชนซึ่งอยู่ในกำกับดูแลของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้มีระบบการบริหารงานที่เป็นอิสระจากระบบราชการ ซึ่งจะส่งผลให้การบริหารจัดการองค์กรมีความเป็นอิสระ คล่องตัว และมีประสิทธิภาพ โดยมีการประกาศในราชกิจจานุเบกษาเป็นพระราชกฤษฎีกาจัดตั้งสำนักงานรัฐบาลอิเล็กทรอนิกส์(องค์การมหาชน) ลงวันที่ 21 กุมภาพันธ์ พ.ศ. 2554 และมีผลบังคับตั้งแต่วันที่ 22 กุมภาพันธ์ พ.ศ. 2554 เป็นต้นมา[24]โดยมีวัตถุประสงค์เพื่อการพัฒนาการบริหารจัดการ ศึกษา วิจัย พัฒนา ให้คำปรึกษาด้านรัฐบาลอิเล็กทรอนิกส์ ตลอดจน ส่งเสริม สนับสนุน และจัดอบรมเพื่อยกระดับทักษะความรู้ความสามารถด้านรัฐบาลอิเล็กทรอนิกส์[25]เพื่อให้การดำเนินงานดังกล่าวมีประสิทธิภาพมากยิ่งขึ้น โดยในระยะเริ่มต้นของสำนักงานรัฐบาลอิเล็กทรอนิกส์ ได้ทำการโอนย้ายบุคลากรและกิจการมาจากสำนักบริการเทคโนโลยีสารสนเทศภาครัฐ(สบทร.) ซึ่งเป็นโครงการที่จัดตั้งขึ้นเพื่อพัฒนาเครือข่ายข้อมูลข่าวสารภาครัฐ(Government Information Network : GINet) และดำเนินกิจกรรมอื่นที่สนับสนุน

---

[22] เรื่องเดียวกัน, 3.

[23] **สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์กรมหาชน) (สรอ.)** [online], 24 พฤษภาคม 2555. แหล่งที่มา http://www.ega.or.th/Content.aspx?m_id=23.

[24] พระราชกฤษฎีกาจัดตั้งสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ. 2554.

[25] เรื่องเดียวกัน, มาตรา 7.

การใช้เทคโนโลยีสารสนเทศในภาครัฐโดยให้เริ่มดำเนินโครงการตั้งแต่ปีงบประมาณ พ.ศ. 2541 ภายใต้สังกัดกระทรวงวิทยาศาสตร์ เทคโนโลยีและสิ่งแวดล้อมในเวลานั้น

จากข้อมูลดังกล่าว จะเห็นได้ว่าเป็นการบริหารราชการแผ่นดินของรัฐบาลเพื่อทำการให้บริการสาธารณะในรูปแบบใหม่ซึ่งเป็นการผสมผสานเทคโนโลยีในการส่งผ่านข้อมูลผ่านการทำธุรกรรมอิเล็กทรอนิกส์ซึ่งได้มีการใช้กับภาคเอกชนก่อนแล้วจึงนำมาใช้กับภาครัฐ กระทั่งเกิดเป็นรัฐบาลอิเล็กทรอนิกส์ หรือ e-Government เป็นสิ่งที่จำเป็นที่รัฐบาลในหลายประเทศต้องจัดให้มีการให้บริการดังกล่าวโดยเร็ว ภายใต้สภาพแวดล้อมของสังคมโลกที่มีการพัฒนาอยู่ตลอดเวลา ในขณะที่สหประชาชาติ(United Nation)ก็ได้ตระหนักถึงความจำเป็นดังกล่าวจึงได้มีการจัดตั้งแผนกที่ว่าด้วยการจัดการสาธารณะและการพัฒนาการจัดการ(Division for Public Administration and Development Management : DPADM)ซึ่งอยู่ภายใต้การควบคุมและดูแลของหน่วยงานด้านเศรษฐกิจและสังคมสหประชาชาติ(United Nation Department of Economic and Social Affiars : UNDESA) เนื่องจากประเทศสมาชิกได้เล็งเห็นถึงความสำคัญในการจัดการงานสาธารณะในประเทศที่กำลังพัฒนาและเพื่อความก้าวหน้าด้านการบริหารงานภาครัฐในอนาคต จึงได้มีความพยายามที่จะกำหนดแนวทางภายใต้วัตถุประสงค์ให้รัฐบาลของประเทศกำลังพัฒนาได้ดำเนินการพัฒนาด้านการบริหารจัดการภาครัฐให้มีความปลอดภัยโดยมีการใช้เทคโนโลยีใหม่ ๆ เพื่อพัฒนาประสิทธิภาพและความโปร่งใสของการบริหารงานรัฐ เช่น การบริหารงานภาครัฐเชิงอิเล็กทรอนิกส์และเคลื่อนที่(Electronic and Mobile Government)ตลอดจนต้องการให้ประชาชนมีส่วนร่วมในการพัฒนาการบริหารงาน เช่น การศึกษาการดำเนินงานของภาครัฐหรือการร่วมมือระหว่างภาครัฐและเอกชนภายใต้กรอบความร่วมมือด้านต่าง ๆ เป็นต้น อีกทั้งต้องการให้ประชาชนมีสิทธิที่เข้าถึงข้อมูลของภาครัฐ(Open Government Data) ทั้งนี้ เพื่อให้เกิดความโปร่งใสและความน่าเชื่อถือในการดำเนินงานของภาครัฐ[26]

โดยในปัจจุบัน ภายหลังจากที่รัฐบาลได้มีนโยบายที่เป็นการส่งเสริมและผลักดันให้หน่วยงานต่างของรัฐนำการทำธุรกรรมทางอิเล็กทรอนิกส์มาใช้ภายในองค์กรเพื่ออำนวยความสะดวกในการจัดเก็บข้อมูลและประมวลผลข้อมูล และเพื่อเป็นการอำนวยความสะดวกให้แก่ประชาชนที่จะได้รับบริการที่มีประสิทธิภาพและรวดเร็วจากหน่วยงานของรัฐ เช่น กรณีกรมสรรพากร ให้บริการยื่นภาษีเงินได้ผ่านทางระบบออนไลน์ หรืออาจเป็นกรณีกรมพัฒนาธุรกิจการค้า ให้บริการจดทะเบียนจัดตั้งห้างหุ้นส่วนหรือบริษัทผ่านทางระบบออนไลน์ เป็นต้น

---

[26] Haiyan Qian, Division for Public administration and Development Management, **Future government : A Global Perspective Connection to Open Government** [online], 2 July 2012. แหล่งที่มา http://www.slideshare.net/undesapublicadmin/future-governmenta-global-perspective-in-connection-to-open-government.

ดังนั้น หน่วยงานของรัฐต่างต้องเร่งพัฒนาการทำธุรกรรมทางอิเล็กทรอนิกส์ในหน่วยงานของตนเองให้มีประสิทธิภาพมากขึ้น โดยมีแนวทางพัฒนาการทำธุรกรรมทางอิเล็กทรอนิกส์มาจากพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 ซึ่งเป็นการกำหนดแนวทางให้หน่วยงานหรือองค์กรต่างๆ ของรัฐมีการพัฒนาการทำธุรกรรมทางอิเล็กทรอนิกส์ให้เป็นไปในแนวทางเดียวกัน[27]เพื่อประโยชน์ในการเก็บรักษาข้อมูลและแลกเปลี่ยนข้อมูลระหว่างกัน

โดยมีคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งจัดตั้งขึ้นตามพระราชบัญญัติธุรกรรมอิเล็กทรอนิกส์ พ.ศ. 2544[28]ได้อาศัยอำนาจตามมาตรา 7 วรรค 1 แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 ทำการออกหลักเกณฑ์ในการพิจารณาแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งหากหน่วยงานของรัฐหน่วยงานใดทำการจัดทำแผนการดำเนินงานด้านสารสนเทศเสร็จสิ้นแล้วต้องทำรายงานเพื่อแสดงรายละเอียดของมาตรการในการให้ความคุ้มครองข้อมูลในด้านต่าง ๆ ให้แก่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ หลังจากนั้นคณะกรรมการธุรกรรมอิเล็กทรอนิกส์จะทำการประกาศรายชื่อหน่วยงานภาครัฐที่จัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยได้ผ่านความเห็นชอบจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์แล้ว ซึ่งถือเป็นการรับรองมาตรฐานขั้นต่ำในการลดความเสี่ยงจากภัยคุกคามของระบบสารสนเทศเพื่อก่อให้เกิดความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ โดยในปัจจุบันมีหน่วยงานของรัฐที่ผ่านการรับรองการดำเนินการตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของประเทศด้านสารสนเทศของหน่วยงานรัฐ พ.ศ.2553 แล้วจำนวน 25 แห่ง[29] ซึ่งหน่วยงานของรัฐจะต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงอย่างสม่ำเสมอเพื่อให้ระบบสารสนเทศมีความมั่นคงปลอดภัยในทางปฏิบัติ และอาจปรับปรุงมาตรการเพื่อรักษาความมั่นคงปลอดภัยตามความเหมาะสม

---

[27] พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549.

[28] พระราชบัญญัติธุรกรรมอิเล็กทรอนิกส์ พ.ศ. 2544, มาตรา 36.

[29] สำนักงานคณะกรรมการอิเล็กทรอนิกส์, **ประกาศรายชื่อหน่วยงานที่จัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและผ่านความเห็นชอบจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์** [online], 3 พฤษภาคม 2555. แหล่งที่มาhttp://www.etcommission.go.th/index.php?option=com_content&view=article&id=178%3A2011-03-02-04-43-58&catid=117%3A2009-09-22-09-49-49&Itemid=182&lang=th.

2.3 ปัญหาที่เกิดขึ้นกับการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ของภาครัฐ

2.3.1 กรณีศึกษา กองหนังสือเดินทาง สังกัดกรมการกงสุล กระทรวงการต่างประเทศ

การให้บริการและการทำธุรกรรมอิเล็กทรอนิกส์ของหน่วยงานหรือองค์กรของรัฐในประเทศไทยได้รับการพัฒนารูปแบบการให้บริการอย่างต่อเนื่องและได้ขยายการให้บริการครอบคลุมหลายหน่วยงานมากขึ้น โดยรวมถึงกองหนังสือเดินทางซึ่งเป็นอีกหน่วยงานหนึ่งที่มีการให้บริการการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐเช่นกัน

(1) หน้าที่และความสำคัญของกองหนังสือเดินทาง

ในการบริหารราชการแผ่นดินของประเทศไทยในปัจจุบัน รัฐบาลได้ทำการจำแนกงานและแบ่งส่วนราชการออกเป็นหน่วยงานต่าง ๆ ตามความเชี่ยวชาญเฉพาะด้านซึ่งในปัจจุบันได้อาศัยอำนาจตามพระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม พ.ศ. 2545 ซึ่งได้บัญญัติให้มีการแบ่งส่วนราชการโดยมีกระทรวงการต่างประเทศ ซึ่งมีอำนาจหน้าที่เกี่ยวกับการราชการต่างประเทศและราชการอื่นตามกฎหมายกำหนด[30]และให้ทำการแบ่งส่วนราชการกระทรวงการต่างประเทศออกเป็นกรมต่าง ๆ ซึ่งรวมถึงกรมการกงสุลด้วย[31]หลังจากนั้นจึงได้มีการออกพระราชกฤษฎีกาแบ่งส่วนราชการกรมการกงสุล กระทรวงการต่างประเทศ พ.ศ. 2541 โดยบัญญัติให้มีการแบ่งส่วนราชการกรมการกงสุลออกเป็นหน่วยงานระดับกองซึ่งรวมถึงกองหนังสือเดินทางด้วย[32]และได้บัญญัติให้กองหนังสือเดินทางมีอำนาจและหน้าที่ในการดำเนินการเกี่ยวกับเอกสารและหนังสือเดินทางให้แก่บุคคลสัญชาติไทย ตลอดจนปฏิบัติงานร่วมกับหน่วยงานอื่นที่เกี่ยวข้องหรือที่ได้รับมอบหมาย[33]

ทั้งนี้ กรมการกงสุล เป็นหน่วยงานที่มีภารกิจในการรับผิดชอบเรื่องที่เกี่ยวข้องกับการออกหนังสือเดินทางและเอกสารเดินทาง ตลอดจนการคุ้มครองดูแลผลประโยชน์ของชาวไทยในต่างประเทศ ซึ่งในทางปฏิบัติกรมการกงสุลเป็นหน่วยงานราชการที่รับรองงานด้านการบริการประชาชน โดยประสานกับหน่วยงานด้านการปกครองและทะเบียนราษฎรทั้งในประเทศและนอกประเทศ และยังมีหน้าที่ในการพัฒนาหนังสือเดินทางหรือเอกสารเดินทางของ

---

[30] พระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม พ.ศ.2545, มาตรา 12.

[31] เรื่องเดียวกัน, มาตรา 13 (3).

[32] พระราชกฤษฎีกาแบ่งส่วนราชการกรมการกงสุล กระทรวงการต่างประเทศ พ.ศ. 2541, ข้อ 2 (5).

[33] เรื่องเดียวกัน, ข้อ 3 (5) .

ประเทศไทย ตลอดจนเอกสารการตรวจลงตรา(Visa)ของประเทศไทยให้มีความทันสมัยและทัดเทียมกับมาตรฐานสากล เพื่อให้ประเทศไทยเป็นที่ยอมรับในประชาคมระหว่างประเทศ[34]

ดังนั้น กรมการกงสุลจึงได้มีการแบ่งส่วนราชการออกเป็นหลายกองซึ่งมีอำนาจและหน้าที่แตกต่างกันไป ซึ่งรวมถึงกองหนังสือทางที่มีอำนาจและหน้าที่ในการดำเนินการเกี่ยวกับหนังสือเดินทางและเอกสารเดินทางให้แก่บุคคลสัญชาติไทย โดยในปัจจุบันได้มีการแบ่งส่วนราชการออกเป็น 8 ฝ่าย ได้แก่ ฝ่ายอำนวยการ ฝ่ายหนังสือเดินทางธรรมดา ฝ่ายหนังสือเดินทางทูตและราชการ ฝ่ายตรวจสอบประวัติ ฝ่ายผลิตเล่มหนังสือเดินทาง ฝ่ายบันทึกและแก้ไขหนังสือเดินทาง ฝ่ายจ่ายเล่มหนังสือเดินทางและไปรษณีย์ และฝ่ายหนังสือเดินทางไทยในต่างประเทศ[35]

นอกจากนี้ เพื่อเป็นการอำนวยความสะดวกและยกระดับในการให้บริการแก่ประชาชน กองหนังสือเดินทางจึงได้จัดหน่วยให้ให้บริการประชาชนในการทำเอกสารเกี่ยวกับหนังสือเดินทางอยู่ที่สำนักงานกรมการกงสุลและได้จัดตั้งสำนักงานชั่วคราวเพื่อให้บริการแก่ประชาชนในกรุงเทพมหานคร และยังจัดให้มีสำนักงานหนังสือเดินทางชั่วคราวในส่วนภูมิภาคซึ่งตั้งอยู่ในหลายจังหวัดอีกด้วย[36]

(2) ความหมายของหนังสือเดินทาง

หนังสือเดินทาง คือ เอกสารสำคัญประจำตัวที่รัฐบาลประเทศหนึ่งออกให้แก่พลเมืองหรือคนชาติของตนเพื่อใช้ในการแสดงตนในการเดินทางไปต่างประเทศ ซึ่งในทางปฏิบัติประเทศเจ้าของหนังสือเดินทางจะต้องทำการร้องขอให้ประเทศต่าง ๆ ให้ความสะดวก ให้ความปลอดภัย หรือให้ความช่วยเหลือและให้ความคุ้มครองทางกฎหมายในขณะที่พลเมืองของประเทศตนอยู่ในประเทศนั้น ๆ โดยหนังสือเดินทางต้องได้รับการประทับการตรวจลงตราหรือวีซ่า (Visa)จากหน่วยงานของประเทศที่จะเดินทางไปเยือน เว้นแต่จะมีความตกลงยกเว้นการตรวจลงตราระหว่างประเทศเอาไว้[37]

---

[34] กรมการกงสุล. กระทรวงการต่างประเทศ, **หน่วยงานในกรม**, 4 พฤษภาคม 2555 แหล่งที่มา http://www.consular.go.th/modules.php?name=Content&pa=showpage&pid=7

[35] เรื่องเดียวกัน.

[36] กรมการกงสุล. กระทรวงการต่างประเทศ, **งานกองหนังสือเดินทาง**, 4 พฤษภาคม 2555. แหล่งที่มา http://www.consular.go.th/modules.php?name=Content&pa=showpage&pid=56.

[37] กรมการกงสุล. กระทรวงการต่างประเทศ, **วิวัฒนาการของหนังสือเดินทางไทย**, 4 พฤษภาคม 2555. แหล่งที่มา http://www.consular.go.th/modules.php?name=Content&pa=showpage&pid=72.

(3) การให้บริการของกองหนังสือเดินทาง

กองหนังสือเดินมีภารกิจหลัก คือ การให้การบริการกับประชาชนในส่วนที่เกี่ยวข้องกับหนังสือเดินทาง(Passport)ซึ่งในปัจจุบันกองหนังสือเดินทางได้จัดให้มีการใช้หนังสือเดินทางอิเล็กทรอนิกส์(Electronic Passport : e-Passport)โดยได้เริ่มใช้ตั้งแต่เดือนสิงหาคม พ.ศ. 2548 เป็นต้นมา

ทั้งนี้ กองหนังสือเดินในปัจจุบัน ทำการแบ่งประเภทของหนังสือเดินทางออกเป็น 5 ประเภท ได้แก่ หนังสือเดินทางบุคคลธรรมดา หนังสือเดินทางทูต หนังสือเดินทางราชการ หนังสือเดินทางพระภิกษุและหนังสือเดินทางเพื่อประกอบพิธีฮัจญ์ โดยหนังสือเดินทางแบบอิเล็กทรอนิกส์เป็นหนังสือเดินทางซึ่งมีคุณลักษณะพิเศษเฉพาะทางเทคนิคตามข้อกำหนดขององค์การการบินพลเรือนระหว่างประเทศ(International Civil Aviation Organization : ICAO) ซึ่งแตกต่างจากหนังสือเดินทางแบบเดิม คือ ได้มีการบันทึกข้อมูลทางด้านชีวภาพ(Biometric Data) เช่น รูปใบหน้า และหรือลายนิ้วมือ และหรือม่านตา โดยทำการบันทึกเอาไว้ในอุปกรณ์อิเล็กทรอนิกส์ขนาดเล็กซึ่งมีชื่อว่า Contactless Integrated Circuit หรือ IC ที่ฝังอยู่ภายในเล่มของหนังสือเดินทาง นอกจากนี้ ยังมีการเข้ารหัสข้อมูลเพื่อทำการตรวจสอบความถูกต้องแท้จริงของหนังสือเดินทางฉบับนั้น โดยหนังสือเดินทางแบบอิเล็กทรอนิกส์มีข้อดีกว่าหนังสือเดินทางแบบเดิม คือ สามารถป้องกันการปลอมแปลงได้สูง ซึ่งถือเป็นมาตรการที่สำคัญในการสกัดกั้นขบวนการก่อการร้ายข้ามชาติและการลักลอบเข้าเมือง เป็นต้น[38]

ทั้งนี้ หนังสือเดินทางอิเล็กทรอนิกส์ยังสามารถทำการตรวจสอบเพื่อพิสูจน์ตัวบุคคลได้อย่างถูกต้องแม่นยำและมีความรวดเร็ว ซึ่งถือเป็นการอำนวยความสะดวกต่อการเดินทางการเข้าเมือง(Immigration)อันเป็นส่งเสริมการท่องเที่ยวและทำให้หนังสือเดินทางของประเทศไทยมีความน่าเชื่อถือและได้รับการยอมรับในระดับสากลซึ่งจะส่งผลดีต่อการท่องเที่ยวของประเทศไทยให้มีความก้าวหน้า ตลอดจนมีความปลอดภัยและมีความสะดวกสบายมากยิ่งขึ้นซึ่งจะส่งผลให้เศรษฐกิจการค้าและการลงทุนของประเทศมีการพัฒนามากขึ้นเป็นลำดับ ทั้งนี้ หนังสือเดินทางในระบบแบบเดิม ซึ่งกองหนังสือเดินทางได้ออกให้กับประชาชนก่อนเดือนสิงหาคม พ.ศ. 2548 ยังคงใช้ได้ตราบจนวันสิ้นอายุตามที่ปรากฏในเล่มหนังสือเดินทางแต่จะไม่สามารถต่ออายุได้อีก ซึ่งหมายความว่า ผู้ที่ทำหนังสือเดินทางภายหลังเดือนสิงหาคม พ.ศ. 2548 จะได้รับหนังสือเดินทางอิเล็กทรอนิกส์ หรือ e-Passport เท่านั้น[39]

---

[38] กรมการกงสุล. กระทรวงการต่างประเทศ, **หนังสือเดินทางอิเล็กทรอนิกส์**, 4 พฤษภาคม 2555. แหล่งที่มา http://www.consular.go.th/modules.php?name=Content&pa=showpage&pid=59.

[39] เรื่องเดียวกัน.

นอกจากนี้ กองหนังสือเดินทางยังได้รับเอาข้อมูลส่วนบุคคลจากหน่วยงานอื่นมาใช้ในการให้บริการกับประชาชนด้วย เช่น การเชื่อมโยงในฐานะผู้ขอใช้ข้อมูลโดยมีการเชื่อมโยงข้อมูลทะเบียนราษฎร เช่น ข้อมูลบัตรประชาชนหรือข้อมูลทะเบียนบ้าน จากกรมการปกครอง กระทรวงมหาดไทย ซึ่งได้มีการทำบันทึกข้อตกลง(Memorandum of Understanding : MOU) ตามบันทึกความตกลงมาตรฐานของกระทรวงมหาดไทย ตลอดจนมีการเชื่อมโยงในฐานะผู้ให้ข้อมูลโดยทำการเชื่อมโยงข้อมูลให้กับกรมสอบสวนคดีพิเศษ ซึ่งมีการลงนามในบันทึกข้อตกลงระหว่างกัน และการส่งผ่านข้อมูลการทำหนังสือเดินทาง และข้อมูลกรณีที่หนังสือเดินทางหายหรือถูกโจรกรรมให้กับสำนักงานตรวจคนเข้าเมือง เป็นต้น[40]

(4) ข้อมูลที่จัดเก็บหรือปรากฏบนหนังสือเดินทาง

ในการทำหนังสือเดินทางประเภทต่าง ๆ กองหนังสือเดินทางมีความจำเป็นที่จะต้องใช้เอกสารหรือข้อมูลส่วนบุคคลที่แตกต่างกันออกไป เพื่อพิจารณาและจำแนกเหตุผลของการเดินทางไปต่างประเทศของบุคคลนั้น โดยในปัจจุบันการขอทำหนังสือเดินทางแต่ละประเภทกองหนังสือเดินทางมีความต้องการเอกสารหรือข้อมูลที่สำคัญ ดังต่อไปนี้

(4.1) เอกสารสำคัญที่ระบุตัวตนของผู้ขอทำหนังสือเดินทาง เช่น

บัตรประจำตัวประชาชน บัตรประจำตัวที่ใช้แทนได้ตามกฎกระทรวงมหาดไทย สูติบัตรฉบับจริงหากเป็นสำเนาต้องได้รับการรับรองจากอำเภอหรือเขต หรือบัตรประจำตัวข้าราชการที่ปรากฏเลขประจำตัวประชาชน 13 หลัก เป็นต้น

(4.2) เอกสารสำคัญที่บ่งบอกสถานะสำคัญในทางทางกฎหมายที่เกี่ยวข้องกับผู้ขอทำหนังสือเดินทาง เช่น เอกสารหลักฐานการรับรองบุตรหรือรับบุตรบุญธรรม ใบสำคัญการสมรส ทะเบียนหย่า คำสั่งศาลกรณีระบุผู้มีอำนาจปกครองแทนบิดาหรือมารดา เป็นต้น

---

[40] กองหนังสือเดินทาง. กรมการกงสุล. กระทรวงการต่างประเทศ, **หนังสือเดินทางอิเล็กทรอนิกส์กับการคุ้มครองข้อมูลส่วนบุคคล**[online], เอกสารประกอบการสัมนา“ธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐกับการคุ้มครองข้อมูลส่วนบุคคล”, 28 พฤษภาคม 2555. แหล่งที่มา http://www.etcommission.go.th/index.php?option=com_content&view=article&id=170&Itemid=8&lang=th.

(4.3) เอกสารสำคัญที่ใช้ยืนยันการแก้ไขข้อมูลส่วนบุคคล เช่น

เอกสารการเปลี่ยนชื่อ-นามสกุลของผู้ขอทำหนังสือเดินทาง เอกสารแก้ไขวันเดือนปีเกิด(กรณีที่วันเดือนปีเกิดที่ปรากฏบนบัตรประจำตัวประชาชนไม่ถูกต้อง) และเอกสารเปลี่ยนชื่อ-นามสกุลของบิดาหรือมารดา เป็นต้น

(4.4) เอกสารสำคัญอื่นซึ่งแยกตามประเภทของหนังสือเดินทาง เช่น

(4.4.1) ในกรณีที่ขอทำหนังสือเดินทางบุคคลธรรมดาซึ่งเป็นผู้เยาว์ต้องมีหนังสือยินยอมให้ผู้เยาว์เดินทางไปต่างประเทศซึ่งได้รับการรับรองจากสำนักงานเขต

(4.4.2) ในกรณีที่ขอทำหนังสือเดินทางราชการ จะต้องมีหนังสือนำจากหน่วยงานต้นสังกัดซึ่งลงนามโดยปลัดกระทรวงต้นสังกัด แจ้งขอให้กระทรวงต่างประเทศออกหนังสือเดินทาง พร้อมระบุวัตถุประสงค์ที่จะเดินทาง เป็นต้น

(4.4.3) ในกรณีที่ขอทำหนังสือเดินทางฑูต ต้องมีหนังสือนำจากหน่วยงานต้นสังกัดซึ่งลงนามโดยปลัดกระทรวง แจ้งขอให้กระทรวงต่างประเทศออกหนังสือเดินทาง พร้อมระบุวัตถุประสงค์ที่จะเดินทางและหนังสือบันทึกจากกลุ่มพัฒนาระบบกลุ่มบริหารกระทรวงการต่างประเทศถึงผู้อำนวยการกองหนังสือเดินทางให้ออกหนังสือเดินทางไปรับตำแหน่งพร้อมครอบครัว เป็นต้น

(4.4.5) ในกรณีที่ขอทำหนังสือเดินทางพระ ทั้งนี้ เนื่องจากพระภิกษุอยู่มีสถานะต่างกับบุคคลธรรมดาทั่วไป ดังนั้น เอกสารที่ใช้ในการเดินทางไปต่างประเทศรวมถึงขั้นตอนในการเดินทางไปต่างประเทศ จึงต้องมีความแตกต่างออกไป เช่น เอกสารแสดงการได้รับอนุญาตให้เดินทางไปต่างประเทศ หรือหนังสืออนุมัติจากสำนักงานพระพุทธศาสนาแห่งชาติ หนังสือสุทธิ ทะเบียนบ้านและทะเบียนวัดและเอกสารประกอบ เช่น ใบตราตั้งสัญญาบัตร ใบฐานานุกรม ใบตราตั้งเจ้าอาวาส ใบตราตั้งเจ้าคณะตำบล เป็นต้น ตลอดจนหนังสือรับรองความประพฤติจากเจ้าอาวาสซึ่งใช้ในกรณีสามเณรมีอายุไม่ครบ 20 ปีบริบูรณ์ โดยต้องระบุข้อความยินยอมให้เดินทางไปต่างประเทศเพื่อปฏิบัติศาสนกิจในต่างประเทศมาแสดง เป็นต้น

(4.4.6) ในกรณีที่ขอทำหนังสือเดินทางเพื่อไปประกอบพิธีฮัจญ์ จะต้องมีหนังสือซึ่งได้รับการรับรองจากสำนักจุฬาราชมนตรีหรือหนังสือรับรองจากคณะกรรมการอิสลามประจำจังหวัดซึ่งรับรองการประกอบพิธีฮัจญ์ เป็นต้น

(4.4.7) ในกรณีที่เป็นนักเรียนทุนรัฐบาลหรือเป็นข้าราชการซึ่งลาศึกษาฝึกอบรมไปยังต่างประเทศ ยื่นคำร้องขอต่ออายุหนังสือเดินทางธรรมดาสำหรับข้าราชการหรือนักเรียนทุนรัฐบาล จะต้องขอรับหนังสือรับรองจากสำนักงานผู้ดูแลนักเรียนไทยในต่างประเทศและเอกสารเพิ่มเติมที่จำเป็นแล้วแต่กรณี เป็นต้น[41]

ทั้งนี้ การทำหนังสือเดินทางอิเล็กทรอนิกส์ กองหนังสือเดินทางมีความจำเป็นจะต้องใช้ข้อมูลส่วนบุคคลที่สำคัญในการทำธรุกรรรมอิเล็กทีอนิกส์ ซึ่งการบันทึกข้อมูลส่วนบุคคลที่ถูกจัดเก็บไว้ในหนังสือเดินทางอิเล็กทีทรอนิกส์ อาจแบ่งได้ออกเป็น 2 ประเภท ได้แก่ ข้อมูลทั่วไปและข้อมูลชีวภาพ(Biometric Data) ซึ่งมีรายละเอียด ดังต่อไปนี้

(ก) ข้อมูลทั่วไป เช่น

- คำนำหน้านาม ชื่อ และนามสกุล
- วันเดือนปีเกิด และสถานที่เกิด
- สถานที่ หรือที่อยู่จริงที่ติดต่อได้
- หมายเลขโทรศัพท์ และโทรศัพท์มือถือ
- บุคคลที่ใกล้ชิด ติดต่อได้ในกรณีฉุกเฉินจำนวน 2 คน

(ข) ข้อมูลชีวภาพ(Biometric Data) ได้แก่

- รูปใบหน้า ลายนิ้วมือนิ้วชี้สองข้าง และม่านตา[42]

โดยในการเก็บข้อมูลชีวภาพจะถูกจัดเก็บไว้ใน Contactless Integrated Circuit ซึ่งเป็นอุปกรณ์อิเล็กทรอนิกส์ขนาดเล็กที่ฝังอยู่ในเล่มของหนังสือเดินทางแบบอิเล็กทรอนิกส์ทุกเล่ม

(5) สภาพปัญหาในการคุ้มครองข้อมูลส่วนบุคคลของกองหนังสือเดินทาง

เนื่องจากกองหนังสือเดินมีภารกิจหลักที่จะต้องให้บริการแก่ประชาชนในการจัดทำหนังสือเดินทาง ซึ่งมีความจำเป็นที่จะต้องมีการเก็บรวบรวมข้อมูลส่วนบุคคลที่จำเป็น เช่น ชื่อ นามสกุล วันเกิด สถานที่เกิด อายุ และที่อยู่ โดยเฉพาะอย่างข้อมูลที่เป็นข้อมูลชีวภาพ (Biometric Data)ซึ่งมีการบันทึกลายนิ้วมือ ม่านตา และภาพถ่ายเพื่อใช้ในการให้บริการธุรกรรม

---

[41] สำนักงานผู้ดูแลนักเรียนไทยในประเทศฝรั่งเศส, สำนักงานคณะกรรมการข้าราชการพลเรือน, **ต้องต่อหนังสือเดินทางที่ใด**[online], 21 กรกฎาคม 2555 แหล่งที่มา http://oeaparis.online.fr/article.php3?id_Article=1&id_section=1.

[42] กรมการกงสุล. กระทรวงการต่างประเทศ, **สาระน่ารู้เกี่ยวกับหนังสือเดินทาง ตอนที่ 2**, 4 พฤษภาคม 2555. แหล่งที่มา http://www.consular.go.th/modules.php?name=Content&pa=showpage&pid=46.

ทางอิเล็กทรอนิกส์ของภาครัฐ โดยกองหนังสือเดินทางต้องมีการเก็บรวบรวมและประมวลผลข้อมูลส่วนบุคคลเป็นจำนวนมาก ซึ่งจากสถิติการให้บริการหนังสือเดินทางในปีงบประมาณ พ.ศ. 2553(ระหว่าง 1 ต.ค. 2552 - 30 ก.ย. 2553) มีการออกหนังสือเดินทางประเภทต่าง ๆ ภายในประเทศรวมทั้งสิ้นจำนวน 1,210,625 ราย[43]ซึ่งยังคงประสบปัญหาในการบริหารจัดการและคุ้มครองข้อมูลส่วนบุคคลดังกล่าว ดังนี้

(5.1) ปัญหาในแง่กฎหมาย เช่น มีกฎหมายใดในการให้อำนาจกับกรมการกงสุลในการอนุญาตให้หน่วยราชการอื่นได้เข้ามาเชื่อมโยงข้อมูลส่วนบุคคลดังกล่าว

(5.2) ปัญหาในการให้ข้อมูลกับสถานทูตในต่างประเทศ เช่น ข้อมูลการขอหนังสือเดินทางและข้อมูลส่วนบุคคลในความครอบครองของกองหนังสือเดินทาง ซึ่งเกิดขึ้นในกรณีมีผู้ขอหนังสือเดินทางไปยื่นคำร้องขอรับการตรวจลงตรา(Visa)กับสถานทูตต่างประเทศ

(5.3) แนวทางการพัฒนาในอนาคต เช่น เรื่องของความร่วมมือกับต่างประเทศเรื่องการแบ่งปัน(Share)ข้อมูลส่วนบุคคลในกรณีที่หนังสือเดินทางสูญหายหรือถูกโจรกรรมซึ่งสามารถให้ข้อมูลได้เพียงใด ตลอดจนการออกหลักเกณฑ์ในการทำการเชื่อมโยงที่เป็นปัจจุบัน(Realtime Online)ซึ่งจะทำการเชื่อมโยงข้อมูลกับต่างประเทศ รวมถึงสำนักงานตำรวจสากล(INTERPOL)[44]เป็นต้น

(5.4) การศึกษาและพิจารณารายละเอียดของการดำเนินการจัดเก็บข้อมูลส่วนบุคคลของกรมการกงสุลว่ามีความสอดคล้องกับกฎหมายและพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549 หรือประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์หรือไม่[45]

(6) มาตรการคุ้มครองข้อมูลส่วนบุคคลที่กองหนังสือเดินทางบังคับใช้

(6.1) พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540

กองหนังสือเดินทาง ซึ่งมีสถานะเป็นหน่วยงานของรัฐซึ่งมีทั้งข้อมูลข่าวสารของราชการและข้อมูลส่วนบุคคลที่สำคัญอยู่ในความควบคุมดูแล ซึ่งในปัจจุบันต้องนำ

---

[43] กองหนังสือเดินทาง. กรมการกงสุล. กระทรวงการต่างประเทศ, **รายงานประจำปีงบประมาณ 2553,** 2.

[44] International Police Organization, **About INTERPOL**[online], 22 July 2012 Available from http://www.interpol.int/About-INTERPOL/Overview.

[45] กองหนังสือเดินทาง. กรมการกงสุล. กระทรวงการต่างประเทศ, **หนังสือเดินทางอิเล็กทรอนิกส์กับการคุ้มครองข้อมูลส่วนบุคคล**, เอกสารประกอบการสัมนา“ธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐกับการคุ้มครองข้อมูลส่วนบุคคล”, 28 พฤษภาคม 2555. แหล่งที่มาhttp://www.etcommission.go.th/index.php?Option=com_content&view=article&id=170&Itemid=8&lang=th.

บทบัญญัติตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มาบังคับใช้ภายในหน่วยงานซึ่งมีหลักเกณฑ์เป็นไปตามที่พระราชบัญญัติกำหนด

(6.2) พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549

ทั้งนี้ กองหนังสือเดินทาง ในฐานะหน่วยงานของรัฐซึ่งทำการจัดเก็บทั้งข้อมูลข่าวสารของราชการและข้อมูลส่วนบุคคลที่สำคัญและเป็นหน่วยงานที่ต้องให้บริการต่อบุคคลทั้งภายในและภายนอกประเทศ ตลอดจนต้องมีการควบคุมมาตรฐานการให้บริการด้านหนังสือเดินทางให้เป็นไปตามมาตรฐานในระดับสากล จึงมีความจำเป็นที่ต้องพัฒนาระบบสารสนเทศให้มีความมั่นคงปลอดภัยเพื่อที่ประชาชนจะได้เกิดความเชื่อมั่นในการเข้าใช้บริการ ดังนั้น กองหนังสือเดินทางจึงได้ดำเนินการตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549 โดยมีมาตรการที่สำคัญ ดังต่อไปนี้

(ก) มีมาตรการลงทะเบียนผู้ใช้งานระบบ และกำหนดตัวบุคคลผู้ใช้งานระบบโดยทำการกำหนดบุคคลที่สามารถเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศเอาไว้

(ข) มีมาตรการในการควบคุมและจำกัดสิทธิของผู้ใช้งานระบบอย่างจำกัดและมีความเหมาะสมเพื่อให้ความคุ้มครองข้อมูลส่วนบุคคล

(ค) มีมาตรการโดยกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งานระบบ

(ง) มีมาตรการในการจัดให้มีระบบสารสนเทศ และระบบสำรองในกรณีที่การใช้งานระบบออนไลน์(Online System)ตามปกติเกิดเหตุขัดข้องไม่สามารถใช้งานได้และมีความจำเป็นอย่างยิ่งที่จะดำเนินการภายใต้ระบบออฟไลน์(Offline System)[46]

(จ) มีมาตรการควบคุมดูแลและทำการตรวจสอบบุคคลผู้ใช้งานและเข้าถึงระบบของงานให้เป็นไปโดยถูกต้อง[47]

จากมาตรการดังกล่าว จะเห็นได้ว่ากองหนังสือเดินทางได้มีมาตรการคุ้มครองข้อมูลส่วนบุคคลตามที่รัฐบาลกำหนด ซึ่งเป็นการดำเนินมาตรการตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของประเทศด้านสารสนเทศของหน่วยงานรัฐ พ.ศ.2553 ซึ่งกำหนดให้หน่วยงานของรัฐปฏิบัติตามหากหน่วยงาน

---

[46] Offline หมายถึง การทำงานของระบบคอมพิวเตอร์ในขณะที่ไม่มีการเชื่อมต่อระบบอินเตอร์เน็ต

[47] กองหนังสือเดินทาง. กรมการกงสุล. กระทรวงการต่างประเทศ, **หนังสือเดินทางอิเล็กทรอนิกส์กับการคุ้มครองข้อมูลส่วนบุคคล**, เอกสารประกอบการสัมนา"ธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐกับการคุ้มครองข้อมูลส่วนบุคคล", 28 พฤษภาคม 2555. แหล่งที่มา http://www.etcommission.go.th/index.php?option=com_content&view=article&id=170&Itemid=8&lang=th.

ใดผ่านการรับรองตามประกาศของคณะกรรมการธุรกรรมอิเล็กทรอนิกส์แล้วนั้น ให้ถือว่าหน่วยงานดังกล่าวผ่านมาตรฐานขั้นต่ำในการดำเนินงานภายใต้ระบบสารสนเทศที่กำหนด

ทั้งนี้ กรณีศึกษากองหนังสือเดินทางดังที่กล่าวข้างต้น เป็นการศึกษาเพื่อแสดงให้เห็นถึงกระบวนการทำงานและการนำมาตรการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐมาใช้ในสถานการณ์ปัจจุบัน เนื่องจากในปัจจุบันภาครัฐของไทยมีการนำเทคโนโลยีสนเทศมาปรับใช้ในการให้บริการแก่ประชาชนได้ไม่นาน ดังนั้น ปัญหาการกระทำความผิดต่อข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐในประเทศไทย จึงยังไม่ปรากฏข้อเท็จจริงที่สามารถนำมาเป็นกรณีศึกษาได้อย่างชัดเจน อีกทั้งในทางปฏิบัติเป็นการยากที่หน่วยงานของรัฐจะเปิดเผยถึงข้อผิดพลาดและความเสียหายในการจัดเก็บข้อมูลส่วนบุคคลตลอดจนมาตรการคุ้มครองข้อมูลส่วนบุคคลโดยละเอียด เพราะหากแม้มีกรณีที่เกิดขึ้นจริงในปัจจุบันความเสียหายอาจยังไม่ได้รับการเปิดเผย เนื่องจากการเปิดเผยถึงข้อผิดพลาดในมาตรการคุ้มครองข้อมูลส่วนบุคคลหรือข้อมูลอื่นของหน่วยงานรัฐ อาจส่งผลกระทบต่อบุคคลและเจ้าหน้าที่ที่เกี่ยวข้องหลายฝ่ายรวมถึงหน่วยงานของรัฐ และอาจทำให้ภาพลักษณ์ขององค์กรเสื่อมเสียซึ่งอาจทำให้ความเชื่อมั่นในการทำธุรกรรมอิเล็กทรอนิกส์กับภาครัฐลดลงได้ ดังเช่นที่เกิดขึ้น ในกรณีของเว็บไซต์(Website)Wikileaks ซึ่งได้ทำการระบุตนเองว่าเป็นองค์กรอาสาสมัครซึ่งตั้งอยู่บริเวณแถบสแกนดิเนเวีย ซึ่งถูกพัฒนาขึ้นโดยกลุ่มผู้ที่ไม่เห็นด้วยกับการดำเนินงานของรัฐบาลแห่งสาธารณรัฐประชาชนจีน[48]และจากข้อมูลที่ปรากฏบนเว็บไซต์ Wikileaks ในปี พ.ศ. 2553 ซึ่งได้มีการเผยแพร่ภาพปฏิบัติการโจมตีทางอากาศต่อกรุงแบกแดก (Bagdad)ประเทศอิรัก[49]โดยกองทัพสหรัฐอเมริกา ส่งผลให้มีพลเรือนชาวอิรักเสียชีวิตเป็นจำนวนมาก หลังจากนั้นในยังได้มีการเผยแพร่เอกสารลับต่าง ๆ ที่ไม่เคยถูกเผยแพร่เกี่ยวกับปฏิบัติการทางการทหารของสหรัฐอเมริกาในประเทศอัฟกานิสถานและได้มีการเผยแพร่เอกสารลับเกี่ยวกับเอกสารปกปิดทางการทูตของกระทรวงการต่างประเทศของสหรัฐอเมริกาอีกจำนวนมาก ส่งผลให้รัฐมนตรีว่าการกระทรวงการต่างประเทศของสหรัฐอเมริกาได้ทำการออกแถลงการณ์เพื่อประณามเว็บไซต์ Wikileaks จนกระทั่งตำรวจสากล(INTERPOL)ได้มีการออกหมายจับจูเลียน อาสซานจ์(Julian Assange)[50]ซึ่งเป็นหนึ่งในผู้ก่อตั้งเว็บไซต์ดังกล่าว

---

[48] China Electronic and Governance, **Wikileaks Releases Unsurprising China**[online], 18 July 2012. from Cableshttp://chinaelectionsblog.net/?p=11043.

[49] Cable News Network (CNN), **Leaked video reveals chaos of Baghdad Attack**[online], 18 July 2012. from http://edition.cnn.com/2010/WORLD/meast/04/06/iraq.journalists.killed/index.html.

[50] Cable News Network (CNN), **Interpol puts Assange on Most-Wanted List**[online], 18 July 2012. from http://edition.cnn.com/2010/WORLD/europe/11/30/sweden.interpol.assange/index.html.

ดังนั้น จะเห็นได้ว่าแม้กรณีดังกล่าวข้างต้น จะไม่ใช่ความเสียหายที่เกิดขึ้นกับการกระทำความผิดต่อข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐ แต่ก็เป็นการแสดงให้เห็นถึงความสำคัญในการที่หน่วยงานของรัฐจะต้องมีมาตรการในการควบคุมดูแลข้อมูลที่หน่วยงานของรัฐจัดเก็บอยู่มีความสำคัญเป็นอย่างมาก ดังนั้น หน่วยงานของรัฐจำเป็นต้องจัดเตรียมระบบหรือมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เข้มงวดเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นได้

อย่างไรก็ตาม ในเรื่องของการทำหนังสือเดินทางอิเล็กทรอนิกส์ ได้มีผู้ทำการศึกษาไว้ในต่างประเทศ ถึงผลกระทบและความเสี่ยงในการนำเทคโนโลยีมาใช้ในการทำหนังสือเดินทางอิเล็กทรอนิกส์ ซึ่งรายงานดังกล่าวได้ระบุว่า สำหรับหนังสือเดินทางอิเล็กทรอนิกส์นั้นในบริเวณส่วนปกของหนังสือเดินทางอิเล็กทรอนิกส์โดยทั่วไปมักจะมีการฝังแผงวงจรอิเล็กทรอนิกส์ที่มีขนาดเล็กเอาไว้ซึ่งเรียกว่า RFID Tag ซึ่งเป็นระบบฉลากที่ได้ถูกพัฒนามาตั้งแต่ปี ค.ศ. 1980 ภายใต้เทคโนโลยี RFID ซึ่งถือเป็นหนึ่งในเทคโนโลยีที่หลายประเทศให้ความสำคัญในการพัฒนาอย่างจริงจัง เนื่องจากเทคโนโลยี RFID เริ่มเข้ามามีบทบาทสำคัญในชีวิตประจำวันมากขึ้นในรูปแบบการใช้งานที่หลากหลาย เช่น บัตรโดยสารรถไฟฟ้าใต้ดิน บัตรพนักงาน และสติ๊กเกอร์ RFID Tag ที่ใช้ในการป้องกันสินค้าสูญหายซึ่งสามารถพบได้ตามศูนย์การค้าขนาดใหญ่ เป็นต้น จากข้อมูลดังกล่าวข้างต้นทำให้สามารถคาดการณ์ได้ว่าเทคโนโลยีดังกล่าว จะต้องเข้ามามีบทบาทสำคัญต่อการดำเนินชีวิตในอนาคต ซึ่งจะมีส่วนในการเปลี่ยนแปลงสังคมของประเทศไทยให้เข้าสู่สังคมสารสนเทศโดย RFID ย่อมาจากคำว่า “Radio Frequency Identification”ซึ่งเป็นเทคโนโลยีที่ถูกประดิษฐ์ขึ้นโดย Leon Theremin โดยได้สร้างเทคโนโลยีนี้ให้กับรัฐบาลของประเทศรัสเซีย(Russia)ในช่วงปี ค.ศ. 1945 ซึ่งได้ใช้เป็นระบบในการชี้เฉพาะอัตโนมัติ(Auto-Identification)ที่มีการทำงานแบบไร้สาย(Wireless)โดยทำการระบุเอกลักษณ์ของวัตถุหรือตัวบุคคลโดยใช้คลื่นความถี่วิทยุ ซึ่งต่างจากเทคโนโลยีอื่น เช่น บาร์โค้ด(Barcode)ที่อาศัยคลื่นแสงหรือโดยการสแกน(Scan)ลายนิ้วมือ เป็นต้น แต่ทั้งนี้ ในการทำงานของระบบ RFID จะมีประสิทธิภาพเพียงไรนั้นยังคงต้องคำนึงถึงข้อจำกัดในการใช้งานไม่ว่าจะเป็นเรื่องของสนามแม่เหล็กไฟฟ้า(Electromagnetic Field : EMF)ในสภาพแวดล้อมหรือกฎหมายที่เกี่ยวข้องกับระเบียบการใช้คลื่นความถี่วิทยุและกำลังส่งของแต่ละประเทศด้วย[51]

อนึ่ง เทคโนโลยี RFID ในปัจจุบันได้ถูกพัฒนาให้มีลักษณะเป็นแผ่นป้ายอิเล็กทรอนิกส์หรือ RFID Tag ที่สามารถอ่านข้อมูลได้โดยผ่านคลื่นวิทยุจากระยะไกล เพื่อทำการตรวจติดตามบันทึกข้อมูลที่ติดอยู่กับ RFID Tag ซึ่งนำไปติดไว้กับวัตถุต่าง ๆ เช่น ผลิตภัณฑ์ กล่อง หรือ

---

[51] สถาบันส่งเสริมความเป็นเลิศทางเทคโนโลยี RFID แห่งประเทศไทย, **คำแนะนำเทคโนโลยี RFID** [online], 15 มิถุนายน 2555. from http://www.rfid.or.th/th/technology/know.asp.

สิ่งของใดให้สามารถติดตามบันทึกข้อมูลของวัตถุชิ้นว่า วัตถุชิ้นนั้นคืออะไร ผลิตที่ไหน และใครเป็นผู้ผลิต รวมถึงข้อมูลอื่นที่ผู้ผลิตต้องใส่ลงไปใน RFID Tag เพื่อที่จำทำการระบุตัวตนของวัตถุชิ้นนั้น รวมถึงตำแหน่งที่ตั้งของวัตถุนั้นว่าอยู่ที่ใดโดยไม่จำเป็นต้องอาศัยการสัมผัส (Contact-Less)หรือต้องเห็นวัตถุนั้นก่อน ซึ่งมีกระบวนการทำงานโดยใช้เครื่องอ่านที่สื่อสารกับ RFID Tag ด้วยคลื่นวิทยุ ดังนั้น หนังสือเดินทางอิเล็กทรอนิกส์มีซึ่งมีการติดตั้ง RFID Tag อยู่ภายในเล่มอาจทำให้เกิดการติดตามตัวบุคคลได้ในบางสถานการณ์ได้ เช่น การลักลอบติดตั้งเครื่องอ่านข้อมูล RFID Tag บนขอบประตูเพื่อลักลอบอ่านข้อมูลใน RFID Tag เป็นต้น[52]

จากกรณี ดังกล่าวข้างต้น แม้จะไม่ใช่เอกสารที่เกิดการทำธุรกรรมทางอิเล็กทรอนิกส์ที่ออกโดยรัฐบาลไทย แต่หนังสือเดินทางอิเล็กทรอนิกส์ของต่างประเทศก็มีสถานะเป็นเอกสารราชการของต่างประเทศซึ่งรัฐบาลออกให้ภายใต้ระบบอิเล็กทรอนิกส์เช่นกัน ย่อมมีโอกาสที่ผู้ที่ถือหนังสือเดินทางอิเล็กทรอนิกส์ดังกล่าว จะนำหนังสือเดินทางอิเล็กทรอนิกส์เข้ามาใช้ในประเทศไทยซึ่งมีผู้คนเดินทางเข้าและออกนอกประเทศอยู่ตลอดเวลา โดยข้อมูลดังกล่าวเป็นข้อมูลส่วนบุคคลที่มีความสำคัญที่รัฐจะต้องมีมาตรการคุ้มครองขอมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์กับภาครัฐให้มีความมั่นคงปลอดภัยและมีมาตรฐานในระดับสากล

ทั้งนี้ ประเทศไทยซึ่งเป็นประเทศหนึ่งที่มีการนำหนังสือเดินทางอิเล็กทรอนิกส์มาใช้ในการให้บริการกับประชาชนจึงต้องมีการกำหนดมาตรการเฝ้าระวังอย่างใกล้ชิด มิให้มีผู้กระทำความผิดทำการลักลอบนำข้อมูลในหนังสือเดินทางอิเล็กทรอนิกส์ไปใช้โดยทุจริต ซึ่งอาจทำให้ประชาชนได้รับความเสียหาย และทำให้ภาพลักษณ์ของหน่วยงานของรัฐหรือความน่าเชื่อถือของประเทศไทยลดลงได้ ซึ่งหากปราศจากความเชื่อมั่นในการดำเนินงานของหน่วยงานของรัฐแล้ว การลงทุน การพัฒนา และการค้ากับต่างประเทศย่อมสะดุดลง อันส่งผลกระทบต่อการพัฒนาประเทศในทุกด้านอย่างหลีกเลี่ยงไม่ได้

---

[52] Eleni Kosta, Martin Meints, Marit Hansen & Mark Gasson, **An analysis of security and privacy issuesrelating to RFID enabled ePassports** [online]. 5 June 2012 Available from ihttp:// www.few.vu.nl/~mconti/teaching/ATCNS2010/ATCS/RFIDpassport/kosta.pdf.

บทที่ 3
มาตรากรการคุ้มครองข้อมูลส่วนบุคคลในการการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐ

สังคมโลกยุคปัจจุบัน เราไม่สามารถปฏิเสธได้เลยว่าเทคโนโลยีสารสนเทศได้มีบทบาทอย่างมากในชีวิตประจำวันอย่างหลีกเลี่ยงไม่ได้ เนื่องจากการติดต่อสื่อสารระหว่างกันของมนุษย์ได้มีการพัฒนารูปแบบอยู่ตลอดเวลา ดังนั้น รัฐบาลจึงต้องจัดให้มีการปรับปรุงและพัฒนาแนวนโยบายทั้งในด้านการบริหารและในด้านกฎหมายให้ทันต่อสภาพสังคมที่เปลี่ยนแปลงไปอย่างรวดเร็ว ซึ่งรวมถึงการพัฒนามาตรการคุ้มครองสิทธิเสรีภาพของประชาชนให้สอดคล้องกับบริบทของสังคมที่เริ่มนำการทำธุรกรรมทางอิเล็กทรอนิกส์ซึ่งเคยใช้กับภาคเอกชนมาใช้กับภาครัฐ เพื่อให้สามารถตอบสนองต่อการให้บริการกับประชาชนได้อย่างทั่วถึงและเป็นธรรม ทั้งนี้ หากหน่วยงานของรัฐมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่หน่วยของรัฐควบคุมดูแลที่มีประสิทธิภาพเพียงพอ ก็จะเป็นการสร้างความเชื่อมั่นให้กับประชาชนในการเข้ารับบริการจากภาครัฐและมีความไว้วางใจที่จะให้ข้อมูลที่เป็นจริง โดยในแต่ละประเทศซึ่งรวมถึงประเทศไทยต่างได้มีมาตรการคุ้มครองข้อมูลส่วนบุคคลในการธุรกรรมอิเล็กทรอนิกส์ของหน่วยงานของรัฐที่แตกต่างกันออกไปตามบริบทของสังคมของประเทศตนเอง ซึ่งอาจทำการศึกษาได้โดยมีสาระสำคัญ ดังนี้

3.1 กฎหมายและมาตรการคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศ

ในแต่ละประเทศต่างเร่งพัฒนามาตรการและกฎหมายในการให้ความคุ้มครองข้อมูลส่วนบุคคลเพื่อให้สอดคล้องกับสภาพสังคมของประเทศตนเอง โดยมีสหรัฐอเมริกาและสหภาพยุโรปเป็นผู้นำในการพัฒนามาตรการต่าง ๆ ในการให้ความคุ้มครองข้อมูลส่วนบุคคล ซึ่งรวมถึงประเทศไทย ที่ได้มีการวางกรอบการพัฒนากฎหมายคุ้มครองข้อมูลส่วนบุคคลตามแนวทางที่สหภาพยุโรปบังคับใช้ ซึ่งอาจทำการศึกษาได้ดังต่อไปนี้

3.1.1 แนวทางด้านการคุ้มครองความเป็นอยู่ส่วนตัวและการโอนข้อมูลส่วนบุคคลระหว่างประเทศ (Guidelines on the protection of Privacy and Transborder Data Flows of Personal Data แห่ง OECD)

แนวทางด้านการคุ้มครองความเป็นอยู่ส่วนตัวและการโอนข้อมูลส่วนบุคคลระหว่างประเทศ เป็นแนวทางในระดับสากลซึ่งเป็นการพัฒนาขึ้นโดยองค์การระหว่างประเทศ

คือ องค์การเพื่อเศรษฐกิจและการพัฒนา[1](Organization for Economic Cooperation and Development : OECD)ซึ่งเป็นองค์กรที่มีวัตถุประสงค์เพื่อให้ข้อเสนอแนะด้านเศรษฐกิจและการพัฒนาแก่ประเทศภาคีสมาชิก ซึ่งรวมถึงการนำเอาหลักการคุ้มครองข้อมูลส่วนบุคคลขั้นพื้นฐาน(Basic Principles)ไปปรับใช้ในกลุ่มประเทศภาคีสมาชิกหรือในประเทศที่มีความสนใจ ซึ่งอาจอยู่ในรูปของการบัญญัติเป็นกฎหมาย(Legislative)หรือมาตรการ(Messurement)อื่นใดที่มีสภาพบังคับหรือการเป็น Best Practice[2] ซึ่งเป็นทางปฏิบัติของภาคเอกชนที่ได้รับความนิยมค่อนข้างมาก โดยเฉพาะอย่างยิ่งในกลุ่มประเทศที่มีอัตราประชากรในการเข้าใช้ระบบอินเตอร์เน็ตในการทำธุรกรรมทางอิเล็กทรอนิกส์ที่ค่อนข้างสูง โดยมีหลักการสำคัญทั้งสิ้น 8 ประการ ดังต่อไปนี้

(1) หลักข้อจำกัดในการเก็บรวบรวมข้อมูล (Collection Limitation Principle)

มีสาระสำคัญ คือ ในการเก็บรวบรวมข้อมูลส่วนบุคคลจะต้องดำเนินการโดยชอบด้วยกฎหมายและต้องใช้วิธีการที่เหมาะสมและเป็นธรรม โดยในการเก็บรวบรวมข้อมูลนั้นจะต้องให้แจ้งเจ้าของข้อมูลรับรู้ หรือได้รับความยินยอมจากเจ้าของข้อมูลก่อน[3]

(2) หลักคุณภาพของข้อมูล (Data Quality Principle)

มีสาระสำคัญ คือ ข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวม จะต้องเป็นไปตามวัตถุประสงค์ที่กำหนดขึ้นและเป็นไปตามอำนาจหน้าที่ในการดำเนินงานของหน่วยงานตามที่กฎหมายกำหนด และต้องมีการตรวจสอบข้อมูล ให้ถูกต้องและมีการปรับปรุงข้อมูลส่วนบุคคลให้เป็นปัจจุบันอยู่เสมอ[4]

(3) หลักการกำหนดวัตถุประสงค์ (Purpose Specification Principle)

มีสาระสำคัญ คือ ในการเก็บข้อมูลส่วนบุคคล ผู้เก็บข้อมูลจะต้องทำการแจ้งวัตถุประสงค์ของการรวบรวมข้อมูลให้เจ้าของข้อมูลได้ทราบก่อนการรวบรวมข้อมูล อีกทั้งจะต้องใช้ข้อมูลส่วนบุคคลภายในวัตถุประสงค์ที่แจ้งไว้ดังกล่าวด้วย[5]

---

[1] สำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์(องค์กรมหาชน), **หลักเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคลของผู้บริโภค ตามแนวทางขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา**, 1 พฤษภาคม 2555. แหล่งที่มา http://www.etda.or.th/main/contents/display/337.

[2] Best Practice หมายถึง วิธีการทำงานที่ซึ่งอาจไม่วิธีดีที่สุดในเรื่องนั้น แต่เป็นวิธีที่ทำให้ผลงานบรรลุเป้าหมายระดับสูงสุด ซึ่งอาจจะเป็นระบบบริหาร เทคนิค(Technical) หรือวิธีการใดก็ได้

[3] Organization for Economic Co-operation and Development, **OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data**, Article 7.

[4] ibid, Article 8.

[5] ibid, Article 9.

(4) หลักข้อจำกัดในการนำไปใช้ (Use Limitation Principle)

มีสาระสำคัญ คือ ข้อมูลส่วนบุคคลซึ่งเก็บรวบรวมมานั้น จะต้องไม่มีการเปิดเผยหรือทำให้ปรากฏในลักษณะอื่นใดที่มิได้กำหนดไว้โดยชัดแจ้งในวัตถุประสงค์ของการเก็บรวบรวมข้อมูล เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลหรือโดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย[6]

(5) หลักการรักษาความมั่นคงปลอดภัยข้อมูล (Security Safeguards Principle)

มีสาระสำคัญ คือ การกำหนดให้หน่วยงานจะต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสมเพื่อป้องกันความเสี่ยงภัยใดที่อาจทำให้ข้อมูลส่วนบุคคลนั้นสูญหาย ถูกเข้าถึง ถูกทำลาย ถูกใช้ ดัดแปลงแก้ไข หรือเปิดเผยโดยมิชอบ[7]

(6) หลักการเปิดเผยข้อมูล (Openness Principle)

มีสาระสำคัญ คือ หน่วยงานควรมีการประกาศนโยบายให้ทราบโดยทั่วกันในกรณีที่มีการปรับปรุงแก้ไขหรือพัฒนาแนวนโยบายหรือแนวปฏิบัติที่เกี่ยวกับข้อมูลส่วนบุคคล และควรเปิดเผยหรือประกาศไว้ให้ชัดเจน รวมทั้งให้แจ้งข้อมูลใดที่สามารถระบุเกี่ยวกับหน่วยงานผู้ให้บริการและที่อยู่ผู้ควบคุมข้อมูลส่วนบุคคลด้วย[8]

(7) หลักการมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation Principle)

มีสาระสำคัญ คือ ควรกำหนดให้เจ้าของข้อมูลมีสิทธิในการได้รับการยืนยันจากผู้ควบคุมข้อมูลว่าผู้ควบคุมข้อมูลมีข้อมูลที่เกี่ยวข้องกับเจ้าของข้อมูลหรือไม่เพียงใด และต้องได้รับทราบผลการยืนยันภายในเวลาอันสมควร[9]

ทั้งนี้ ผู้ควบคุมข้อมูลอาจคิดค่าใช้จ่ายในการดำเนินการได้ในอัตราที่เหมาะสม และในกรณีที่ไม่สามารถดำเนินการตามที่เจ้าของข้อมูลร้องขอข้างต้น ผู้ควบคุมข้อมูลจะต้องแจ้งเหตุผลให้เจ้าของข้อมูลทราบ รวมทั้งต้องบอกกล่าวให้เจ้าของข้อมูลทราบถึงสิทธิในการโต้แย้งในการไม่ปฏิบัติตามคำร้องขอดังกล่าว และหากต่อมาปรากฏว่าข้อโต้แย้งจากเจ้าของข้อมูลสามารถรับฟังได้ เจ้าของข้อมูลย่อมมีสิทธิที่จะขอให้ผู้ควบคุมข้อมูลทำการลบ แก้ไขปรับปรุงหรือดำเนินการใดให้ข้อมูลมีความสมบูรณ์ได้

---

[6] ibid, Article 10.

[7] ibid, Article 11.

[8] ibid, Article 12.

[9] ibid, Article 13.

(8) หลักความรับผิดชอบ (Accountability Principle)

มีสาระสำคัญ คือ ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด[10]

จากบทบัญญัติดังกล่าว จะเห็นได้ว่า Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data แห่ง OECD เป็นเพียงข้อตกลงระหว่างประเทศซึ่งกำหนดหลักการคุ้มครองข้อมูลส่วนบุคคลอย่างกว้าง เพื่อให้ประเทศภาคีสมาชิกหรือประเทศที่นำแนวของข้อตกลงฉบับนี้ไปปรับใช้สามารถปฏิบัติได้โดยสอดคล้องกัน โดยมิได้มีการกำหนดโทษหรือรายละเอียดในการให้ความคุ้มครองข้อมูลส่วนบุคคลอย่างเป็นขั้นตอน ทั้งนี้เพื่อให้แต่ละประเทศนำแนวทางการปฏิบัติดังกล่าวไปปรับใช้ให้เหมาะสมกับสภาพเศรษฐกิจและสังคมของประเทศตนเอง

3.1.2 DIRECTIVE 95/46/EC of The European Parliament and of The Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

ในช่วงปี ค.ศ. 1995 สหภาพยุโรป(European Union : EU)ได้ออกหลักเกณฑ์เกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่สำคัญฉบับหนึ่ง คือ 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[11] เพื่อเป็นการสนับสนุนและผลักดันให้ประเทศภาคีสมาชิกได้มีแนวทางของกฎหมายบังคับใช้คุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกัน ในการให้ความคุ้มครองข้อมูลส่วนบุคคลของพลเมืองสหภาพยุโรป และเพื่อเป็นการทำให้การไหลเวียนของข้อมูลส่วนบุคคลในประเทศภาคีสมาชิกเป็นไปได้โดยเสรีปราศจากข้อจำกัดที่เกิดจากความแตกต่างกันของกฎหมายหรือกฎเกณฑ์ใด ๆ ซึ่งส่งผลให้ประเทศภาคีสมาชิกสหภาพยุโรปได้มีการตรากฎหมายตามแนวทางที่ 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 ซึ่งได้บัญญัติไว้ เพื่อให้ความคุ้มครองข้อมูลส่วนบุคคลครอบคลุมถึงประเทศอื่น ๆ ที่มิใช่ภาคีสมาชิกสหภาพยุโรปด้วย และในเวลาต่อมาหลักเกณฑ์ดังกล่าวได้รับการยอมรับว่าเป็นการวางพื้นฐานของการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปที่ซึ่งประเทศต่าง ๆ ในสหภาพยุโรปได้ยึดเป็นแนวทางในการออกกฎหมายภายในของประเทศตน ทั้งนี้ ตามบัญญัติของ Directive 95/46/EC on the Protection of Individuals

---

[10] ibid, Article 14.

[11] European Union, **EUR-Lex Access to European Union Law** [online], 4 June 2012. Available from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0087:en:NOT.

with regard to the processing of Personal Data and on the free movement of such data มีหลักการที่สำคัญ 8 ประการ ดังต่อไปนี้

(1) หลักเกณฑ์มาตรฐานในการรักษาคุณภาพของข้อมูล
(Principles Relating to Data Quality)[12]

(2) หลักเกณฑ์มาตรฐานในการทำให้การใช้ข้อมูลถูกต้องตามกฎหมาย
(Criteria for Making Data Processing Legitimate)[13]

(3) หลักเกณฑ์มาตรฐานในการใช้ข้อมูลในหมวดพิเศษ
(Special Categories of Processing)[14]

(4) หลักเกณฑ์มาตรฐานของข้อมูลที่จะให้แก่เจ้าของข้อมูล[15]
(Information to be Given to the Data Subject)

(5) หลักเกณฑ์มาตรฐานของสิทธิในการเข้าถึงข้อมูลของเจ้าของข้อมูล[16]
(The Data Subject's Right of Access to Data)

(6) หลักเกณฑ์มาตรฐานของสิทธิในการคัดค้านการประมวลผลข้อมูลของเจ้าของข้อมูล
(Exemtionp and Restrictions)[17]

(7) หลักเกณฑ์มาตรฐานของสิทธิในการคัดค้านของเจ้าของข้อมูล
(The Data Subject's Right to Object)[18]

(8) หลักเกณฑ์มาตรฐานในการรักษาความลับและความปลอดภัยในการใช้ข้อมูล
(Confidentialty and Security of Processing)[19]

ทั้งนี้ จากหลักการสำคัญทั้ง 8 ประการของ 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 จะเห็นได้ว่ามีลักษณะคล้ายคลึงกันกับ Guidelines on the protection of Privacy and Transborder Data Flows of Personal Data แห่ง OECD โดยสาระสำคัญของ Directive 95/46/EC on the Protection of Individuals with regard to the processing of Personal

---

[12] 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, Section I.

[13] ibid, Article Section II.

[14] ibid, Section III.

[15] ibid, Section IV.

[16] ibid, Section V.

[17] ibid, Section VI.

[18] ibid, Section VII.

[19] ibid, Section VIII.

Data and on the free movement of such data ได้ทำการอธิบายไว้ในบทที่ 4 ของสารนิพนธ์ฉบับนี้แล้ว

3.2 กฎหมายและมาตรการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย

การทำธุรกรรมในรูปทางอิเล็กทรอนิกส์ไม่ว่าจะเป็นการดำเนินงานในหน่วยงานของเอกชนหรือหน่วยงานของรัฐ ล้วนแต่มีความจำเป็นที่จะต้องบันทึกหลักฐานแห่งการทำธุรกรรมอิเล็กทรอนิกส์นั้นไว้ในรูปแบบของข้อมูล(File)ซึ่งรวมถึงข้อมูลส่วนบุคคลที่มีความสำคัญด้วย ดังนั้น จะเห็นได้ว่าในโลกปัจจุบันข้อมูลเป็นสิ่งที่มีค่า ซึ่งหน่วยงานของรัฐจะต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่มั่นคงปลอดภัยเพื่อสร้างความมั่นใจให้กับประชาชนในการเข้าทำธุรกรรมอิเล็กทรอนิกส์กับภาครัฐ แม้ว่าประเทศไทยจะยังไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลบังคับใช้เป็นกรณีทั่วไป แต่ก็มีกฎหมายบางฉบับที่ให้ความคุ้มครองสิทธิส่วนบุคคลซึ่งรวมถึงการให้ความคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมกับภาครัฐเป็นการเฉพาะบังคับใช้อยู่ซึ่งมีสาระสำคัญดังต่อไปนี้

3.2.1 รัฐธรรมนูญแห่งราชอาณาจักรไทย

รัฐธรรมนูญจัดเป็นกฎหมายลำดับสูงที่สุดของประเทศไทย ซึ่งเปรียบเสมือนเป็นกฎหมายแม่บทที่วางหลักเกณฑ์และการให้ความคุ้มครองสิทธิเสรีภาพขั้นพื้นฐานของประชาชน โดยในปัจจุบันอยู่ภายใต้การบังคับใช้ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550 ซึ่งได้บัญญัติเรื่องการคุ้มครองสิทธิเสรีภาพส่วนบุคคลไว้เป็นแนวทางอย่างกว้างในมาตรา 35 ซึ่งบัญญัติไว้ว่า

“สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง ตลอดจนความเป็นอยู่ส่วนตัวย่อมได้รับความคุ้มครอง

การกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชนอันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัวจะกระทำมิได้ เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณะ

บุคคลย่อมมีสิทธิได้รับความคุ้มครองจากการแสวงหาประโยชน์โดยมิชอบจากข้อมูลส่วนบุคคลที่เกี่ยวกับตน ทั้งนี้ ตามที่กฎหมายบัญญัติ”[20]

จากบทบัญญัติข้างต้น มีข้อสังเกตว่ารัฐธรรมนูญได้บัญญัติรับรองถึงการให้ความคุ้มครองสิทธิในความเป็นส่วนตัว ซึ่งอาจทำการตีความตามเจตนารมย์ของกฎหมายซึ่งให้หมายความรวมถึงการคุ้มครองข้อมูลส่วนบุคคลได้เช่นเดียวกับที่ปรากฏในปฏิญญาสากลว่า

[20] รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2550, มาตรา 32.

ด้วยสิทธิมนุษยชนของสหประชาชาติ เพียงแต่ในปัจจุบันประเทศไทยยังไม่มีการบัญญัติกฎหมายรองรับสิทธิความเป็นส่วนตัวในเรื่องของการคุ้มครองข้อมูลส่วนบุคคลไว้การทั่วไปซึ่งอาจให้ความคุ้มครองครอบคลุมถึงข้อมูลส่วนบุคคลที่รัฐเก็บรักษาไว้ด้วย มีเพียงแต่รัฐธรรมนูญซึ่งเป็นเสมือนกฎหมายกลางที่บัญญัติให้นำแนวทางการคุ้มครองสิทธิส่วนบุคคลไปใช้ในการออกกฎหมาย หรือมีมาตรการใดเพื่อคุ้มครองสิทธิในข้อมูลส่วนบุคคลเท่านั้น จึงเห็นได้ว่าข้อมูลส่วนบุคคลเป็นสิ่งสำคัญประการหนึ่งซึ่งรัฐธรรมนูญได้ให้ความคุ้มครองเอาไว้

3.2.2 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

ในปัจจุบันประเทศไทย มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่บังคับใช้อยู่ แต่เป็นการคุ้มครองข้อมูลส่วนบุคคลเฉพาะหน่วยงานของรัฐเท่านั้น ซึ่งกฎหมายดังกล่าว คือ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ซึ่งได้ประกาศใช้เมื่อวันที่ 2 กันยายน พ.ศ. 2540[21]โดยมีเหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ เป็นการเปิดโอกาสให้ประชาชนได้รับข้อมูลข่าวสารเกี่ยวกับการดำเนินงานของรัฐ ซึ่งเป็นสิ่งจำเป็นในการปกครองระบอบประชาธิปไตย เพื่อที่ประชาชนจะสามารถแสดงความคิดเห็นและใช้สิทธิทางการเมืองได้โดยถูกต้องกับความเป็นจริง อันเป็นการส่งเสริมให้รัฐบาลมีความเป็นรัฐบาลของประชาชนมากยิ่งขึ้น จึงสมควรให้ประชาชนมีสิทธิได้รู้ข้อมูลข่าวสารของราชการโดยมีข้อยกเว้นอันไม่ต้องเปิดเผย ซึ่งจำกัดเฉพาะข้อมูลข่าวสารที่หากเปิดเผยแล้วจะเกิดความเสียหายต่อประเทศชาติหรือต่อประโยชน์ที่สำคัญของเอกชน ทั้งนี้ เพื่อให้ประชาชนได้มีโอกาสรู้ถึงสิทธิหน้าที่ของตนอย่างเต็มที่และเพื่อที่จะปกป้องรักษาประโยชน์ของตนได้อีกประการหนึ่งด้วย ประกอบกับสมควรคุ้มครองสิทธิส่วนบุคคลในส่วนที่เกี่ยวข้องกับข้อมูลข่าวสารของราชการไปพร้อมกันจึงจำเป็นต้องตราพระราชบัญญัติฉบับนี้ขึ้น[22]เพื่อบังคับใช้โดยได้บัญญัติเรื่องของการคุ้มครองข้อมูลส่วนบุคคลไว้โดยมีสาระ สำคัญ ดังนี้

(1) ขอบเขตการบังคับใช้พระราชบัญญัติฉบับนี้

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ได้กำหนดขอบเขตในการใช้บังคับกฎหมายกับหน่วยงานของรัฐ รัฐวิสาหกิจ องค์กรควบคุมการประกอบวิชาชีพและหน่วยงานอิสระของรัฐทุกหน่วยงานที่มีข้อมูลข่าวสารของราชการอยู่ในความครอบครองไม่ว่าจะเป็นข้อมูลที่เกี่ยวกับการดำเนินงานของรัฐหรือการดำเนินงานของเอกชน[23]เว้นแต่เป็นหน่วยงานที่มีความจำเป็นในการกำหนดหลักเกณฑ์เพิ่มเติมเป็นพิเศษ หรือหน่วยงานใดที่ไม่สามารถนำพระราชบัญญัติ

---

[21] พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540.

[22] เรื่องเดียวกัน.

[23] เรื่องเดียวกัน, มาตรา 4.

ฉบับนี้ไปใช้บังคับได้ เนื่องจากเป็นอุปสรรคอย่างร้ายแรงต่อการดำเนินงาน ซึ่งอาจกระทำได้โดยได้รับความเห็นชอบคณะกรรมการข้อมูลส่วนบุคคล[24]ทั้งนี้ พระราชบัญญัติฉบับนี้ได้บัญญัติให้ความคุ้มข้อมูลข่าวสารส่วนบุคคล[25]แยกต่างหากไว้จากข้อมูลข่าวสารของราชการ[26]ซึ่งในส่วนของการคุ้มครองข้อมูลส่วนบุคคลบทบัญญัติแห่งกฎหมายได้ให้ความคุ้มครองถึง “บุคคล” ซึ่งหมายถึง บุคคลธรรมดาที่มีสัญชาติไทยและบุคคลธรรมดาที่ไม่มีสัญชาติไทยแต่มีถิ่นที่อยู่ในประเทศไทย[27]เท่านั้น

(2) การเก็บรวบรวมข้อมูลตามพระราชบัญญัติฉบับนี้

พระราชบัญญัติฉบับนี้ ได้กำหนดหลักเกณฑ์ในการเก็บรวบรวมข้อมูลส่วนบุคคลไว้โดยหน่วยงานของรัฐต้องจัดให้มีการปฏิบัติเกี่ยวกับการจัดระบบข้อมูลส่วนบุคคลซึ่งอยู่ในความดูแลหรืออยู่ในการจัดเก็บของหน่วยรัฐ โดยมีสาระสำคัญดังต่อไปนี้[28]

(2.1) ให้หน่วยงานของรัฐพยายามเก็บข้อมูลส่วนบุคคลโดยตรงจากเจ้าของข้อมูล[29]เพียงเท่าที่จำเป็นเพื่อการดำเนินงานตามวัตถุประสงค์ และให้ยกเลิกการจัดระบบดังกล่าวเมื่อหมดความจำเป็น[30]โดยในการเก็บข้อมูลส่วนบุคคลให้หน่วยงานของรัฐทำการแจ้งให้เจ้าของข้อมูลทราบล่วงหน้า หรือพร้อมกับการขอข้อมูลเพื่อให้ทราบถึงวัตถุประสงค์และลักษณะการใช้ข้อมูลตามปกติ และให้แจ้งให้เจ้าของข้อมูลทราบด้วยว่าเป็นการให้ข้อมูล โดยความสมัครใจหรือมีกฎหมายบังคับ[31]และให้หน่วยงานของรัฐแจ้งให้เจ้าของข้อมูลส่วน บุคคลทราบ หากเป็นกรณีที่จะมีการจัดส่งข้อมูลส่วนบุคคลไปยังที่ใดก็ตามซึ่งจะทำให้บุคคลทั่วไปทราบข้อมูลนั้น เว้นแต่เป็นไปตามลักษณะการใช้ข้อมูลตามปกติ[32]

(2.2) ให้หน่วยงานของรัฐจัดให้มีการพิมพ์ประเภทของบุคคล[33]ประเภทของระบบจัดเก็บข้อมูลส่วนบุคคล[34]ลักษณะการใช้ข้อมูล[35]วิธีการขอตรวจดูข้อมูล[36]และวิธีการขอแก้ไขเปลี่ยนแปลงข้อมูลของเจ้าของข้อมูล[37]ตลอดจนแหล่งที่มาของข้อมูล[38]ลงในราชกิจจานุเบกษา[39]

---

[24] เรื่องเดียวกัน, มาตรา 22.

[25] เรื่องเดียวกัน, หมวด 3.

[26] เรื่องเดียวกัน, หมวด 1.

[27] เรื่องเดียวกัน, มาตรา 21.

[28] เรื่องเดียวกัน, มาตรา 23.

[29] เรื่องเดียวกัน, มาตรา 23 (2).

[30] เรื่องเดียวกัน, มาตรา 23 (1).

[31] เรื่องเดียวกัน, มาตรา 23 วรรค 2.

[32] เรื่องเดียวกัน, มาตรา 23 วรรค 3.

[33] เรื่องเดียวกัน, มาตรา 23 วรรค 3 (ก).

[34] เรื่องเดียวกัน, มาตรา 23 วรรค 3 (ข).

(2.3) ให้หน่วยงานของรัฐทำการตรวจสอบแก้ไขข้อมูลข่าวสารส่วนบุคคลให้มีความถูกต้องอยู่เสมอ[40]และต้องจัดระบบรักษาความปลอดภัยให้แก่ระบบจัดเก็บข้อมูลส่วนบุคคลเพื่อป้องกันมิให้มีการนำเอาข้อมูลไปใช้โดยไม่เหมาะสม[41]

(3) การเปิดเผยข้อมูลส่วนบุคคลตามพระราชบัญญัติฉบับนี้

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ได้บัญญัติให้หน่วยงานของรัฐสามารถเปิดเผยข้อมูลส่วนบุคคลได้ในกรณี ดังต่อไปนี้

(3.1) กรณีที่การเปิดเผยข้อมูลข่าวสารโดยได้รับความยินยอม

เป็นกรณีที่หน่วยงานของรัฐเปิดเผยข้อมูลส่วนบุคคลต่อบุคคลที่สามโดยได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลที่ได้ให้ไว้ล่วงหน้าหรือให้ในขณะนั้น[42]

(3.2) กรณีที่การเปิดเผยข้อมูลส่วนบุคคลเป็นการเฉพาะตัว

เป็นกรณีที่กฎหมายกำหนดให้บุคคลมีสิทธิที่จะได้รู้ถึงข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวข้องกับตนได้ โดยมีคำขอเป็นหนังสือซึ่งหน่วยงานของรัฐที่ควบคุมดูแลข้อมูลนั้น จะต้องอนุญาตให้ตรวจดูหรือได้รับสำเนาข้อมูลส่วนบุคคลส่วนที่เกี่ยวกับบุคคลนั้น[43] เว้นแต่ เป็นกรณีที่เป็นการเปิดเผยรายงานการแพทย์ที่เกี่ยวกับบุคคลใด ซึ่งมีเหตุอันควรเจ้าหน้าที่ของรัฐจะเปิดเผยต่อเฉพาะแพทย์ที่บุคคลนั้นมอบหมายก็ได้[44]

(4) ข้อยกเว้นในการเปิดเผยข้อมูลส่วนบุคคลโดยไม่ต้องขอความยินยอม

พระราชบัญญัติข้อมูลข่าวสารส่วนบุคคล พ.ศ. 2540 ได้บัญญัติถึงข้อยกเว้นว่าหน่วยงานของรัฐสามารถทำการเปิดเผยข้อมูลส่วนบุคคลโดยไม่ต้องรับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก็ได้ แต่ต้องเป็นกรณีดังต่อไปนี้

---

[35] เรื่องเดียวกัน, มาตรา 23 วรรค 3 (ค).

[36] เรื่องเดียวกัน, มาตรา 23 วรรค 3 (ง).

[37] เรื่องเดียวกัน, มาตรา 23 วรรค 3 (จ).

[38] เรื่องเดียวกัน, มาตรา 23 วรรค 3 (ฉ).

[39] เรื่องเดียวกัน, มาตรา 23 (3).

[40] เรื่องเดียวกัน, มาตรา 23 (4).

[41] เรื่องเดียวกัน, มาตรา 23 (5).

[42] เรื่องเดียวกัน, มาตรา 24.

[43] เรื่องเดียวกัน, มาตรา 25.

[44] เรื่องเดียวกัน, มาตรา 25 วรรค 2.

(4.1) กรณีการเปิดเผยข้อมูลข่าวสารส่วนบุคคลต่อบุคคลที่สาม

หน่วยงานของรัฐสามารถเปิดเผยข้อมูลส่วนบุคคลต่อบุคคลที่สามได้โดยไม่ต้องได้รับยินยอมเป็นหนังสือจากเจ้าของข้อมูล แต่จะต้องเป็นการเปิดเผยข้อมูลส่วนบุคคลซึ่งเป็นกรณี ดังต่อไปนี้[45]

(4.1.1) เป็นการเปิดเผยต่อเจ้าหน้าที่ของรัฐในหน่วยงานของตนเพื่อการนำไปใช้ตามอำนาจหน้าที่ของหน่วยงานของรัฐแห่งนั้น[46]

(4.1.2) เป็นการเปิดเผยเพื่อการใช้ข้อมูลตามปกติภายในวัตถุประสงค์ของการจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลนั้น[47]

(4.1.3) เป็นการเปิดเผยต่อหน่วยงานของรัฐที่ทำงานด้านการวางแผนหรือการสถิติ หรือสำมะโนต่าง ๆ ซึ่งมีหน้าที่ต้องรักษาข้อมูลข่าวสารส่วนบุคคลนั้นไว้ไม่ให้เปิดเผยต่อไปยังผู้อื่น[48]

(4.1.4) เป็นการเปิดเผยเพื่อประโยชน์ในการศึกษาวิจัยโดยไม่ระบุชื่อหรือส่วนใดที่ทำให้รู้ว่าเป็นข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับบุคคลใด[49]

(4.1.5) เป็นการเปิดเผยต่อหอจดหมายเหตุแห่งชาติ กรมศิลปากรหรือหน่วยงานอื่นของรัฐตามที่กำไว้ในมาตรา 26 เพื่อการตรวจดูคุณค่าในการเก็บรักษา[50]

(4.1.6) เป็นการเปิดเผยต่อเจ้าหน้าที่ของรัฐเพื่อการป้องกันการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย การสืบสวน การสอบสวน หรือการฟ้องคดี[51]

(4.1.7) เป็นการเปิดเผยโดยจำเป็นเพื่อการป้องกันหรือระงับอันตรายต่อชีวิตหรือสุขภาพของบุคล[52]

(4.1.8) เป็นการเปิดเผยต่อศาล และเจ้าหน้าที่ของรัฐหรือหน่วยงานของรัฐหรือบุคคลที่มีอำนาจตามกฎหมายที่จะขอข้อเท็จจริงดังกล่าว[53]

(4.1.9) เป็นการเปิดเผยในกรณีอื่นตามที่กำหนดในพระราชกฤษฎีกา[54]

---

[45] เรื่องเดียวกัน, มาตรา 24.

[46] เรื่องเดียวกัน, มาตรา 24 (1).

[47] เรื่องเดียวกัน, มาตรา 24 (2).

[48] เรื่องเดียวกัน, มาตรา 24 (3).

[49] เรื่องเดียวกัน, มาตรา 24 (4).

[50] เรื่องเดียวกัน, มาตรา 24 (5).

[51] เรื่องเดียวกัน, มาตรา 24 (6).

[52] เรื่องเดียวกัน, มาตรา 24 (7).

[53] เรื่องเดียวกัน, มาตรา 24 (8).

[54] เรื่องเดียวกัน, มาตรา 24 (9).

(5) ข้อมูลข่าวสารที่ห้ามมิให้เปิดเผย

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ได้บัญญัติให้หน่วยงานของรัฐไม่อาจทำการเปิดเผยข้อมูลข่าวสารที่หน่วยงานของรัฐเก็บรักษาอยู่ได้ ซึ่งบัญญัติไว้ในหมวด 2 เช่น กรณีที่เป็นการเปิดเผยข้อมูลข่าวสารซึ่งจะอาจก่อให้ความเสียหายสถาบันพระมหากษัตริย์[55]เป็นต้น แต่เนื่องจากข้อห้ามดังกล่าวเป็นข้อห้ามที่ใช้กับข้อมูลข่าวสารของราชการเท่านั้นไม่รวมถึงข้อมูลส่วนบุคคล แต่มีข้อยกเว้นเพียงกรณีเดียวที่ระบุถึงข้อห้ามหน่วยงานรัฐในการเปิดเผยข้อมูลส่วนบุคคล คือ กรณีที่ห้ามเปิดรายงานทางการแพทย์หรือข้อมูลข่าวสารส่วนบุคคลซึ่งการเปิดเผยนั้นจะเป็นการรุกล้ำสิทธิส่วนบุคคลโดยไม่สมควร[56]

(6) การขอแก้ไขข้อมูลข่าวสารส่วนบุคคลตามพระราชบัญญัติฉบับนี้

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ได้บทบัญญัติถึงการแก้ไขข้อมูลส่วนบุคคล โดยบุคคลใดที่เห็นว่าข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตนส่วนใดไม่ถูกต้องให้ทำการยื่นคำขอเป็นหนังสือต่อหน่วยงานของรัฐที่ควบคุมดูแลข้อมูลข่าวสารนั้น เพื่อให้หน่วยงานของรัฐดำเนินการแก้ไขเปลี่ยนแปลงข้อมูลให้ถูกต้องหรือลบข้อมูลส่วนนั้นได้

ทั้งนี้ หน่วยงานของรัฐต้องรับพิจารณาคำขอและแจ้งให้บุคคลนั้นทราบโดยไม่ชักช้า[57] หากหน่วยงานของรัฐไม่แก้ไขข้อมูลให้ถูกต้อง บุคคลผู้นั้นมีสิทธิอุทธรณ์ต่อคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารภายใน 30 วัน นับแต่วันได้รับแจ้งคำสั่งไม่ยินยอมแก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสาร โดยทำการยื่นอุทธรณ์ต่อคณะกรรมการ นอกจากนี้เจ้าของข้อมูลมีสิทธิร้องขอให้หน่วยงานของรัฐหมายเหตุคำขอของตนแนบไว้กับข้อมูลส่วนบุคคลที่เกี่ยวข้องได้ด้วย[58]

(7) คณะกรรมการข้อมูลข่าวสารของราชการ

ตามที่พระราชบัญญัติข้อมูลข่าวสารส่วนบุคคล พ.ศ. 2540 ได้มีการกำหนดให้คณะรัฐมนตรีทำการแต่งตั้งคณะกรรมการมูลข่าวสารของราชการ จากบุคคลซึ่งมาจากแขนงความรู้ต่าง ๆ ซึ่งปฏิบัติงานภายใต้สำนักงานคณะกรรมข้อมูลข่าวสารของราชการ โดยมีอำนาจหน้าที่ ซึ่งมีสาระสำคัญดังต่อไปนี้[59]

---

[55] เรื่องเดียวกัน, มาตรา 14.

[56] เรื่องเดียวกัน, มาตรา 15 (5).

[57] เรื่องเดียวกัน, มาตรา 25 วรรค 3.

[58] เรื่องเดียวกัน, มาตรา 25 วรรค 4.

[59] เรื่องเดียวกัน, มาตรา 28.

(7.1) ให้คำปรึกษา[60]สอดส่องดูแลและให้คำแนะนำเกี่ยวกับการดำเนินงานของเจ้าหน้าที่ของรัฐและหน่วยงานของรัฐในการปฏิบัติตามพระราชบัญญัตินี้[61]

(7.2) ให้ข้อเสนอแนะในการออกกฎหมายที่เกี่ยวข้อง[62]จัดทำรายงานเกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้เสนอคณะรัฐมนตรี[63]ตลอดจนดำเนินการเรื่องอื่นตามที่คณะรัฐมนตรีหรือนายกรัฐมนตรีมอบหมาย[64]หรือตามที่กำหนดในพระราชบัญญัตินี้[65]

(7.3) พิจารณาและให้ความเห็นเรื่องร้องเรียนตามมาตรา 13

(7.4) มีอำนาจในการเรียกให้บุคคลใดมาให้ถ้อยคำ หรือให้ส่งวัตถุเอกสารหรือพยานหลักฐานมาประกอบการพิจารณาของคณะกรรมการข้อมูลข่าวสารของราชการได้[66]

นอกจากนี้ ในกรณีที่หน่วยงานของรัฐปฏิเสธว่าไม่มีข้อมูลข่าวสารตามที่มีคำขอไม่ว่ากรณีใด ให้คณะกรรมการมีอำนาจตรวจสอบข้อมูลข่าวสารของราชการที่เกี่ยวข้องที่อยู่ในความครอบครองของหน่วยงานของรัฐหรือเจ้าหน้าที่ของรัฐและให้แจ้งผลการตรวจสอบให้ผู้ร้องเรียนทราบ[67]

(8) คณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสาร

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 ได้กำหนดให้มีการแต่งตั้งคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสาร ตามคำแนะนำของคณะกรรมการข้อมูลข่าวสารของราชการ ซึ่งเสนอให้คณะรัฐมนตรีแต่งตั้งบุคคลตามสาขาความเชี่ยวชาญเฉพาะด้านของข้อมูลข่าวสารของราชการ โดยมีอำนาจหน้าที่ ซึ่งมีสาระสำคัญ คือ พิจารณาวินิจฉัยอุทธรณ์คำสั่ง เช่น คำสั่งมิให้เปิดเผยข้อมูลข่าวสารตามมาตรา 14 หรือมาตรา 15 หรือคำสั่งไม่รับฟังคำคัดค้านตามมาตรา 17 และคำสั่งไม่แก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสารส่วนบุคคลตามที่กำหนดไว้ในมาตรา 25[68] แต่ทั้งนี้ ในการพิจารณาเกี่ยวกับข้อมูลข่าวสารของหน่วยงานของรัฐแห่งใด คณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารซึ่งมาจากหน่วยงานของรัฐแห่งนั้นจะเข้าร่วมพิจารณาด้วยไม่ได้[69]

---

[60] เรื่องเดียวกัน, มาตรา 28 (2).

[61] เรื่องเดียวกัน, มาตรา 28 (1).

[62] เรื่องเดียวกัน, มาตรา 28 (3).

[63] เรื่องเดียวกัน, มาตรา 28 (5).

[64] เรื่องเดียวกัน, มาตรา 28 (7).

[65] เรื่องเดียวกัน, มาตรา 28 (6).

[66] เรื่องเดียวกัน, มาตรา 32.

[67] เรื่องเดียวกัน, มาตรา 33.

[68] เรื่องเดียวกัน, มาตรา 35.

[69] เรื่องเดียวกัน, มาตรา 36.

(9) บทกำหนดโทษ

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ได้มีการบัญญัติเกี่ยวกับบทลงโทษตามพระราชบัญญัตินี้ ซึ่งอาจแบ่งออกได้เป็น 2 กรณี ดังนี้

(9.1) ผู้ใดไม่ปฏิบัติตามคำสั่งของคณะกรรมการที่สั่งตามมาตรา 32 ต้องระวางโทษจำคุกไม่เกิน 3 เดือน หรือโทษปรับไม่เกิน 5,000 บาท หรือทั้งจำทั้งปรับ[70]

(9.2) ผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามข้อจำกัดหรือเงื่อนไขที่เจ้าหน้าที่ของรัฐกำหนดตามมาตรา 20 ต้องระวางโทษจำคุกไม่เกิน 1 ปี หรือโทษปรับไม่เกิน 20,000 บาท หรือทั้งจำทั้งปรับ[71]

จากบทบัญญัติดังกล่าว จะเห็นได้ว่าพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ซึ่งเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลในหน่วยงานของรัฐฉบับสำคัญที่ประเทศไทยได้ใช้บังคับอยู่นั้น ยังมิได้มีการบัญญัติไว้โดยละเอียดว่าหน่วยงานของรัฐต้องมีมาตรการอย่างไรในการรักษาข้อมูลส่วนบุคคล เพื่อที่จะให้แต่ละหน่วยมีหลักเกณฑ์การปฏิบัติที่สอดคล้องกัน อีกทั้ง พระราชบัญญัติฉบับนี้ ยังได้มุ่งเน้นที่จะคุ้มครองข้อมูลข่าวสารทั่วไปและข้อมูลข่าวสารที่เป็นความลับของราชการที่หน่วยงานของรัฐได้เก็บรักษาข้อมูลไว้มากกว่าข้อมูลส่วนบุคคล ประกอบกับช่วงเวลาดังกล่าวการกระทำความผิดต่อข้อมูลส่วนบุคคลที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ยังไม่แพร่หลายเท่าในปัจจุบัน ทำให้กฎหมายไม่อาจคุ้มครองครอบคลุมถึงการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐในปัจจุบันได้อย่างเหมาะสม

3.2.3 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

พระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ พ.ศ. 2544 ได้มีการประกาศใช้เมื่อวันที่ 2 ธันวาคม พ.ศ. 2544[72] เนื่องจากในช่วงเวลานั้น ประเทศไทยยังไม่มีกฎหมายรองรับการทำธุรกรรมอิเล็กทรอนิกส์ จึงมีความจำเป็นต้องมีกฎหมายการรองรับสถานะทางกฎหมายของข้อมูลทางอิเล็กทรอนิกส์ให้เสมอกับการทำเป็นหนังสือหรือหลักฐานเป็นหนังสือ รวมถึงการรับรองวิธีการส่งและรับข้อมูลทางอิเล็กทรอนิกส์และการใช้ลายมือชื่ออิเล็กทรอนิกส์ ตลอดจนการรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์[73] นอกจากนี้ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2554 ยังได้บัญญัติเรื่องการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐเอาไว้

---

[70] เรื่องเดียวกัน, มาตรา 40.

[71] เรื่องเดียวกัน, มาตรา 41.

[72] พระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ พ.ศ. 2544.

[73] เรื่องเดียวกัน.

ในมาตรา 35 หมวด 4 ซึ่งกำหนดให้การดำเนินการใดตามกฎหมายกับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ เช่น คำขอ การอนุญาต การจดทะเบียน และคำสั่งทางปกครอง ถ้าหากได้ทำในรูปแบบของข้อมูลอิเล็กทรอนิกส์ซึ่งมีเงื่อนไขตามหลักเกณฑ์ที่กำหนดโดยพระราชกฤษฎีกาแล้ว ให้นำพระราชบัญญัตินี้มาใช้บังคับและให้ถือว่ามีผลโดยชอบด้วยกฎหมายเช่นเดียวกับการดำเนินการตามหลักเกณฑ์ที่กฎหมายกำหนดในเรื่องนั้น[74]

นอกจากนี้ พระราชบัญญัติฉบับนี้ยังกำหนดให้มีคณะทำงานเพื่อทำหน้าที่กำกับดูแลและกำหนดนโยบายในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐและภาคเอกชน โดยเรียกว่า“คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์”[75]ซึ่งปัจจุบันได้ปฏิบัติหน้าที่ภายใต้สำนักงานคณะกรรมการธุรกรรมอิเล็กทรอนิกส์ โดยเป็นเจ้าพนักงานตามประมวลกฎหมายอาญา[76] ซึ่งมีอำนาจดำเนินการ ดังมีสาระสำคัญดังต่อไปนี้

(1) ให้ข้อเสนอแนะ[77]หรือให้คำปรึกษาต่อคณะรัฐมนตรีเพื่อใช้ในการออกกฎหมาย[78] หลักเกณฑ์ หรือวางนโยบายการส่งเสริมและพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ หรือลายมือชื่ออิเล็กทรอนิกส์[79]ตลอดจนการแก้ไขปัญหาและอุปสรรคที่เกี่ยวข้อง

(2) ติดตามดูแลการประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์[80]และปฏิบัติการอื่นใดเพื่อให้เป็นไปตามที่พระราชบัญญัตินี้กำหนด[81]

นอกจากนี้ ภายใต้อำนาจแห่งคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ซึ่งได้ให้คำแนะนำแก่คณะรัฐมนตรีให้ตระหนักถึงความสำคัญในการบริหารจัดการการทำธุรกรรมอิเล็กทรอนิกส์ให้ครอบคลุมทั้งภาครัฐและภาคเอกชน จึงได้มีการจัดตั้งหน่วยงานที่มีรูปแบบการบริหารจัดการที่คล่องตัว[82]และสามารถประสานการทำงานกับสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ได้ คือ คณะกรรมการพัฒนาธุรกรรมทางอิเล็กทรอนิกส์(Electronic Transactions Commission)ซึ่งได้ปฏิบัติงานภายใต้สำนักงานคณะกรรมการพัฒนาธุรกรรมอิเล็กทรอนิกส์

---

[74] เรื่องเดียวกัน, มาตรา 35.

[75] เรื่องเดียวกัน, มาตรา 36.

[76] เรื่องเดียวกัน, มาตรา 37.

[77] เรื่องเดียวกัน, มาตรา 36 (1).

[78] เรื่องเดียวกัน, มาตรา 36 (3).

[79] เรื่องเดียวกัน, มาตรา 36 (4).

[80] เรื่องเดียวกัน, มาตรา 36 (2).

[81] เรื่องเดียวกัน, มาตรา 36 (5).

[82] สำนักงานคณะกรรมการพัฒนาธุรกรรมอิเล็กทรอนิกส์(องค์การมหาชน), **เกี่ยวกับ สพธอ.[**online]. 2 มิถุนายน 2555, จาก http://www.etda.or.th/main/contents/display/35.

(องค์การมหาชน)หรือ(สพธอ.)(Electronic Transactions Development Agency : ETDA)[83]โดยเป็นองค์การมหาชน ซึ่งเป็นส่วนราชการสังกัดสำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ที่จัดตั้งขึ้นโดยพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)พ.ศ. 2554 โดยมีวัตถุประสงค์ ดังต่อไปนี้[84]

(1) เพื่อทำการพัฒนา ส่งเสริม และสนับสนุนการทำธุรกรรมทางอิเล็กทรอนิกส์ของประเทศ[85]รวมถึงภาคอุตสาหกรรมและวิสาหกิจชุมชน[86]ตลอดจนดำเนินการเผยแพร่ความรู้เกี่ยวกับเทคโนโลยีสารสนเทศและธุรกรรมทางอิเล็กทรอนิกส์ นอกจากนี้ยังต้องดำเนินการฝึกอบรมเพื่อยกระดับทักษะเกี่ยวกับมาตรฐาน ความมั่นคงปลอดภัย หรือกรณีอื่นใดเกี่ยวกับเทคโนโลยีสารสนเทศและธุรกรรมทางอิเล็กทรอนิกส์อีกด้วย[87]

(2) เพื่อศึกษาความต้องการด้านโครงสร้างพื้นฐานของสารสนเทศเพื่อรองรับการทำธุรกรรมทางอิเล็กทรอนิกส์ในด้านต่างๆ เพื่อจัดทำข้อเสนอแนะเกี่ยวกับการพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ของประเทศ[88]ตลอดจนทำการวิจัยและพัฒนาเพื่อจัดทำข้อเสนอแนะเกี่ยวกับมาตรฐานเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์[89]

จากพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2554 จะเห็นได้ว่าแม้บทบัญญัติฉบับนี้ จะไม่ได้กำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐไว้เป็นการเฉพาะ แต่บทบัญญัติดังกล่าวได้ให้ความสำคัญกับการทำธุรกรรมทางอิเล็กทรอนิกส์ โดยบัญญัติเอาไว้ให้การดำเนินการใดตามกฎหมายกับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ ถ้าได้กระทำในรูปของข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่กำหนดโดยพระราชกฤษฎีกา ให้นำพระราชบัญญัติ ฉบับนี้มาใช้บังคับ ซึ่งถือเป็นการยอมรับการทำธุรกรรมทางอิเล็กทรอนิกส์ของภาครัฐและให้อำนาจคณะกรรมการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เป็นผู้กำกับดูแลในการกำหนดแนวทางในการออกกฎระเบียบต่าง ๆ มาใช้ควบคุมและคุ้มครองความเสียหาย ซึ่งอาจเกิดขึ้นได้จากการทำธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานของรัฐ

---

[83] พระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)พ.ศ. 2554, มาตรา 5.

[84] เรื่องเดียวกัน, มาตรา 7.

[85] เรื่องเดียวกัน, มาตรา 7 (1).

[86] เรื่องเดียวกัน, มาตรา 7 (2).

[87] เรื่องเดียวกัน, มาตรา 7 (5).

[88] เรื่องเดียวกัน, มาตรา 7 (3).

[89] เรื่องเดียวกัน, มาตรา 7 (4).

3.2.4 พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

พระราชกฤษฎีกาฉบับนี้ ได้ออกโดยการอาศัยอำนาจตามความในมาตรา 35 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 เนื่องจากในปัจจุบันประเทศไทยได้มีการพัฒนาการทำธุรกรรมทางอิเล็กทรอนิกส์มาใช้กับหน่วยงานของรัฐมากขึ้น จึงเห็นควรสนับสนุนให้หน่วยงานของรัฐมีการประยุกต์ใช้เทคโนโลยีสารสนเทศเข้ามาใช้ในการบริหารจัดการ เพื่อที่จะให้บริการประชาชนได้อย่างมีประสิทธิภาพ ทั่วถึงและเป็นธรรม ซึ่งหน่วยงานของรัฐจะต้องพัฒนาการทำธุรกรรมทางอิเล็กทรอนิกส์ของภาครัฐให้อยู่ภายใต้มาตรฐานและมีแนวทางเดียวกัน ซึ่งเป็นไปตามมาตรา 55 วรรค 1 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ซึ่งกำหนดให้การดำเนินการใดตามกฎหมายกับหน่วยงานของรัฐ ถ้าได้กระทำในรูปของข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่กำหนดโดยพระราชกฤษฎีกาแล้วให้ถือว่ามีผลโดยชอบด้วยกฎหมาย[90]จึงจำเป็นต้องตราพระราชกฤษฎีกานี้ขึ้นบังคับใช้[91] โดยมีสาระสำคัญ ดังนี้

(1) ให้หน่วยงานของรัฐจะต้องจัดให้มีระบบเอกสารอิเล็กทรอนิกส์[92]ในรูปแบบที่เหมาะสม[93]และสามารถอ้างอิงเพื่อใช้ในภายหลังได้โดยยังคงความครบถ้วนของข้อมูลอิเล็กทรอนิกส์ พร้อมกับกำหนดระยะเวลาเริ่มต้นและระยะเวลาสิ้นสุดในการยื่นเอกสารที่ได้ทำในรูปแบบอิเล็กทรอนิกส์[94]และต้องกำหนดวิธีการที่ทำให้สามารถระบุตัวเจ้าของลายมืออิเล็กทรอนิกส์เพื่อที่จะแสดงได้ว่าเจ้าของลายมือชื่อรับรองข้อความในข้อมูลอิเล็กทรอนิกส์[95]ตลอดจนต้องกำหนดวิธีการแจ้งการตอบรับด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใดด้วย[96]

นอกจากนี้ พระราชกฤษฎีกาฉบับนี้ ยังกำหนดให้หน่วยงานของรัฐที่จัดทำกระบวนการพิจารณาทางปกครองโดยวิธีการทางอิเล็กทรอนิกส์ อาจกำหนดเงื่อนไขให้คู่กรณียินยอมตกลงและยอมรับการดำเนินการพิจารณาทางปกครองของหน่วยงานของรัฐด้วยวิธีการ

---

[90] พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544, มาตรา 55 วรรค 1.

[91] พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549.

[92] เรื่องเดียวกัน, มาตรา 3.

[93] เรื่องเดียวกัน, มาตรา 3 (1).

[94] เรื่องเดียวกัน, มาตรา 3 (2).

[95] เรื่องเดียวกัน, มาตรา 3 (3).

[96] เรื่องเดียวกัน, มาตรา 3 (4).

ทางอิเล็กทรอนิกส์ได้[97]แต่ต้องจัดให้มีระบบเอกสารที่อิเล็กทรอนิกส์ซึ่งมีลักษณะตามที่พระราชกฤษฎีกาฉบับนี้กำหนด เว้นแต่จะมีกฎหมายกำหนดไว้เป็นอย่างอื่น[98]

(2) ให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้[99]โดยแนวนโยบายและแนวปฏิบัติอย่างน้อยต้องประกอบด้วยเนื้อต่าง ๆ เช่น การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ[100]การจัดให้มีระบบสารสนเทศสำรองซึ่งอยู่ในสภาพพร้อมใช้งานกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ได้ตามปกติ[101]ตลอดจนต้องการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ[102]

(3) ให้หน่วยงานของรัฐที่มีการรวบรวม จัดเก็บ ใช้ หรือมีการเผยแพร่ข้อมูลส่วนบุคคล ต้องจัดทำแนวนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล[103]เป็นประกาศและต้องได้รับความเห็นชอบจากคณะกรรมการก่อนประกาศดังกล่าวจึงมีผลใช้บังคับได้[104]โดยอาจเพิ่มเติมรายละเอียดที่เกี่ยวข้องกับแนวนโยบายและแนวปฏิบัติได้ หากหน่วยงานของรัฐแห่งนั้นมีความจำเป็นโดยไม่ขัดต่อกฎหมาย ทั้งนี้ กระบวนการทั้งหมดต้องคำนึงถึงความถูกต้องครบถ้วน ความน่าเชื่อถือ สภาพความพร้อมใช้งาน และความมั่นคงปลอดภัยของระบบและข้อมูลส่วนบุคคลอิเล็กทรอนิกส์[105]

จากบทบัญญัติตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 จะเห็นได้ว่าคณะกรรมการธุรกรรมอิเล็กทรอนิกส์ต้องการให้หน่วยงานของรัฐที่ควบคุมดูแลข้อมูลส่วนบุคคลและมีการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐ ต้องเร่งดำเนินการตามพระราชกฤษฎีกากำหนด โดยหน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการคุ้มครอง

---

[97] เรื่องเดียวกัน, มาตรา 4 (2).

[98] เรื่องเดียวกัน, มาตรา 4.

[99] เรื่องเดียวกัน, มาตรา 5.

[100] เรื่องเดียวกัน, มาตรา 5 (1).

[101] เรื่องเดียวกัน, มาตรา 5 (2).

[102] เรื่องเดียวกัน, มาตรา 5 (3).

[103] เรื่องเดียวกัน, มาตรา 6.

[104] เรื่องเดียวกัน, มาตรา 7 วรรค 1.

[105] เรื่องเดียวกัน, มาตรา 8.

ข้อมูลส่วนบุคคลเพื่อให้หน่วยงานของรัฐที่ได้ปฏิบัติตามหลักเกณฑ์ของพระราชกฤษฎีกาฉบับนี้เป็นหน่วยงานที่มีข้อมูลอิเล็กทรอนิกส์ที่มีผลโดยชอบด้วยกฎหมาย

3.2.5 พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553

ตามที่พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553 ซึ่งได้ประกาศใช้เมื่อวันที่ 23 สิงหาคม พ.ศ. 2553[106]โดยมีวัตถุประสงค์เพื่อเป็นการส่งเสริมให้มีการบริหารจัดการและการรักษาความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศในการทำธุรกรรมอิเล็กทรอนิกส์ เพื่อให้มีการยอมรับในข้อมูลอิเล็กทรอนิกส์มากยิ่งขึ้น ประกอบมาตรา 25 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 บัญญัติให้ธุรกรรมทางอิเล็กทรอนิกส์ใดที่ได้กระทำตามวิธีการแบบปลอดภัยที่กำหนดในพระราชกฤษฎีกาแล้วให้สันนิษฐานว่าเป็นวิธีการที่เชื่อถือได้[107]จึงมีความจำเป็นที่จะต้องตราพระราชกฤษฎีกานี้ โดยได้กำหนดภารกิจสำคัญที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จะต้องเร่งดำเนินการไว้ 3 เรื่อง ได้แก่

(1) ให้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนดประเภทหรือหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามมาตรา 5 (1) ซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด ระดับกลาง หรือระดับพื้นฐาน[108]แล้วแต่กรณี ทั้งนี้ การกำหนดให้หน่วยงานใดใช้มาตรการในระดับใดนั้น ต้องประเมินจากความเสี่ยงต่อความคงไว้ซึ่งปลอดภัยของระบบสารสนเทศหรือความร้ายแรงของผลกระทบ[109]

(2) ให้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ทำประกาศกำหนดรายชื่อหรือประเภทของหน่วยงานที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศตามมาตรา 5 (2) ซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด ระดับกลาง หรือระดับพื้นฐาน แล้วแต่กรณี[110]

---

[106] พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553.

[107] พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544, มาตรา 25.

[108] พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553, มาตรา 4.

[109] เรื่องเดียวกัน, มาตรา 5.

[110] เรื่องเดียวกัน, มาตรา 6 วรรค 2.

(3) ให้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ กำหนดมาตรฐานในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่เหมาะสมกับวิธีการแบบปลอดภัย ตามมาตรา 4 ในแต่ละระดับ[111]ซึ่งอย่างน้อยจะต้องมีหลักเกณฑ์ตามที่พระราชกฤษฎีกาฉบับนี้กำหนด เช่น การสร้างความมั่นคงปลอดภัยด้านการบริหารจัดการ[112]การบริหารจัดการทรัพย์สินสารสนเทศ[113]การควบคุมการเข้าถึงเครือข่ายคอมพิวเตอร์[114]และการบริหารจัดการสถานการณ์ด้านความมั่นคงที่ไม่พึงประสงค์[115]ตลอดจนการตรวจสอบและประเมินผลการปฏิบัติตามนโยบาย[116]เป็นต้น

จากบทบัญญัติข้างต้น จะเห็นได้ว่าพระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553 นั้น เป็นการออกมาตรการเพื่อเป็นการเตรียมความพร้อม เพื่อให้หน่วยงานของรัฐออกหลักเกณฑ์ในการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศให้สอดคล้องพระราชกฤษฎีฉบับนี้

3.2.6 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของประเทศด้านสารสนเทศของหน่วยงานรัฐ พ.ศ. 2553

ตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ได้ออกประกาศ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของประเทศด้านสารสนเทศของหน่วยงานรัฐ พ.ศ. 2553 โดยอาศัยอำนาจตามมาตรา 5 , 7 และ 8 แห่งพระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2553 โดยมีวัตถุประสงค์เพื่อใช้เป็นแนวทางเบื้องต้นให้หน่วยงานของรัฐใช้ในการกำหนดนโยบาย และข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งประกาศฉบับนี้กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานตนเอง เพื่อให้การดำเนินธุรกรรมด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ ซึ่งถือเป็นเสิ่งที่สำคัญในการปฏิบัติงานและการบริหารราชการ โดยมีสาระสำคัญ ดังต่อไปนี้[117]

---

[111] เรื่องเดียวกัน, มาตรา 7.

[112] เรื่องเดียวกัน, มาตรา 7 (1).

[113] เรื่องเดียวกัน, มาตรา 7 (3).

[114] เรื่องเดียวกัน, มาตรา 7 (7).

[115] เรื่องเดียวกัน, มาตรา 7 (9).

[116] เรื่องเดียวกัน, มาตรา 7 (11).

[117] ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของประเทศด้านสารสนเทศของหน่วยงานรัฐ พ.ศ. 2553.

(1) หน่วยงานของรัฐจำเป็นที่จะต้องจัดให้มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานซึ่งสอดคล้องกันกับนโยบายหน่วยงาน[118]และต้องประกาศนโยบายและข้อปฏิบัติให้ผู้เกี่ยวข้องทั้งหมดทราบ[119]พร้อมทั้งผู้รับผิดชอบตามนโยบายและข้อปฏิบัติให้ชัดเจน[120]และต้องมีการปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ[121]

(2) หน่วยงานของรัฐจำเป็นต้องมีข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control) เช่น มีการควบคุมการเข้าถึงข้อมูล มีการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง และหน่วยงานของรัฐต้องกำหนดเกี่ยวกับประเภทของข้อมูลและทำการลำดับความสำคัญของข้อมูล ลำดับการเข้าถึงข้อมูล เป็นต้น

(3) ให้มีข้อกำหนดในการเข้าถึงและควบคุมการใช้งานสานเทศ(Access Control) ของหน่วยงานของรัฐ[122]เช่น การกำหนดสิทธิ หรือการอนุญาตให้เข้าถึงข้อมูล เป็นต้น

(4) ให้มีการบริหารจัดการในการเข้าถึงของผู้ใช้งาน(User Access Management)[123]เพื่อเป็นการควบควบคุมการเข้าถึงสารสนเทศของหน่วยงานรัฐได้เฉพาะผู้ที่ได้รับอนุญาตแล้ว เช่น ผู้ผ่านการฝึกอบรม หรือการลงทะเบียนผู้ใช้งาน(User Registration)[124]เป็นต้น

(5) ให้หน่วยงานของรัฐมีการกำหนดความรับผิดชอบของผู้ใช้งาน เช่น การป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรือการป้องกันการลักลอบขโมยข้อมูล เป็นต้น[125]

ทั้งนี้ จากการที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ออกประกาศว่าด้วย เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของประเทศด้านสารสนเทศของหน่วยงานรัฐ พ.ศ. 2553 นั้น ได้มีการกำหนดถึงหลักเกณฑ์และวิธีการรักษาความปลอดภัยด้านสารสนเทศของหน่วยงานรัฐ ซึ่งจะเห็นได้ว่าเป็นการบังคับใช้เป็นการทั่วไปกับข้อมูลข่าวสารอื่นซึ่งหน่วยงานของรัฐครอบครองข้อมูลดังกล่าวอยู่ ซึ่งมิได้เป็นการบัญญัติเพื่อ

---

[118] เรื่องเดียวกัน, ข้อ 3 (1).

[119] เรื่องเดียวกัน, ข้อ 3 (2).

[120] เรื่องเดียวกัน, ข้อ 3 (3).

[121] เรื่องเดียวกัน, ข้อ 3 (4).

[122] เรื่องเดียวกัน, ข้อ 5.

[123] เรื่องเดียวกัน, ข้อ 7.

[124] เรื่องเดียวกัน, ข้อ 7 (2).

[125] เรื่องเดียวกัน, ข้อ 8.

คุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐโดยเฉพาะเจาะจงและบทบัญญัติ ดังกล่าวก็ไม่ได้มีบทกำหนดโทษในกรณีที่หน่วยงานของรัฐไม่สามารถปฏิบัติตามที่เงื่อนไขในประกาศฉบับนี้กำหนดได้

3.2.7 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553

คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ อาศัยอำนาจตามมาตรา 37แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2554 ในการเสนอแนวทางและกำหนดมาตรการในการคุ้มครองข้อมูลส่วนบุคคลของภาครัฐ โดยการออกเป็นประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของประเทศด้านสารสนเทศของหน่วยงานรัฐ พ.ศ.2553 ซึ่งประกาศไว้ ณ วันที่ 1 ตุลาคม พ.ศ. 2553[126] โดยมีสาระสำคัญ ดังนี้

(1) ให้หน่วยงานของรัฐซึ่งรวบรวม จัดเก็บ ใช้ เผยแพร่ หรือดำเนินการอื่นใดเกี่ยวกับข้อมูลของผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ จัดทำนโยบายในการคุ้มครองข้อมูลส่วนบุคคลไว้เป็นลายลักษณ์อักษร โดยให้มีสาระสำคัญอย่างน้อย ดังต่อไปนี้[127]

(1.1) หลักการเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด[128]

หมายถึง การจัดเก็บรวบรวมข้อมูลส่วนบุคคลต้องให้มีขอบเขตจำกัดและมีกระบวนการเก็บรวบรวมข้อมูลที่ชอบด้วยกฎหมายและเป็นธรรม โดยต้องมีการแจ้งให้เจ้าของข้อมูลทราบหรือได้รับความยินยอมจากเจ้าของข้อมูลตามแต่กรณี

(1.2) หลักคุณภาพของข้อมูลส่วนบุคคล[129]

หมายถึง ข้อมูลส่วนบุคคลที่หน่วยงานของรัฐทำการรวบรวมและจัดเก็บจะต้องเป็นไปตามอำนาจหน้าที่และวัตถุประสงค์ในการดำเนินงานของหน่วยงานของรัฐที่ทำการรวบรวมและจัดเก็บข้อมูลตามกฎหมาย

---

[126] ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553.

[127] เรื่องเดียวกัน, ข้อ 2.

[128] เรื่องเดียวกัน, ข้อ 1 (1).

[129] เรื่องเดียวกัน, ข้อ 1 (2).

(1.3) หลักการระบุวัตถุประสงค์ในการเก็บรวบรวม[130]

หมายถึง ให้หน่วยงานของรัฐทำการบันทึกวัตถุประสงค์ของการจัดเก็บและรวบรวมข้อมูลส่วนบุคคลในขณะที่มีการรวบรวมและจัดเก็บข้อมูล รวมถึงการนำข้อมูลส่วนบุคคลนั้นไปใช้ในภายหลัง และหากมีการเปลี่ยนแปลงวัตถุประสงค์ของการเก็บรวบรวมข้อมูลให้มีการจัดทำบันทึกแก้ไขเพิ่มเติมไว้เป็นหลักฐานด้วย

(1.4) หลักข้อจำกัดในการนำข้อมูลส่วนบุคคลไปใช้[131]

หมายถึง ห้ามมิให้หน่วยงานของรัฐที่ทำการจัดเก็บและรวบรวมข้อมูลส่วนบุคคล มีการเปิดเผยหรือทำให้ปรากฏในลักษณะอื่นใดซึ่งข้อมูลส่วนบุคคลที่ไม่สอดคล้องกับวัตถุประสงค์ของการรวบรวมและจัดเก็บข้อมูล เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลหรือเป็นกรณีที่มีกฎหมายกำหนดให้กระทำได้

(1.5) หลักการรักษาความมั่นคงปลอดภัย[132]

หมายถึง ให้หน่วยงานของรัฐที่ทำการจัดเก็บและรวบรวมข้อมูลส่วนบุคคลจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสมเพื่อป้องกันการสูญหาย การเข้าถึง ทำลาย ใช้ ดัดแปลง แก้ไข หรือเปิดเผยข้อมูลโดยส่วนบุคคลมิชอบ

(1.6) หลักการเปิดเผยที่เกี่ยวกับการดำเนินการ แนวปฏิบัติ และนโยบายที่เกี่ยวข้องกับข้อมูลส่วนบุคคล[133]

หมายถึง ให้หน่วยงานของรัฐที่ทำการจัดเก็บและรวบรวมข้อมูลส่วนบุคคลมีการเปิดเผยการดำเนินการ แนวปฏิบัติ และนโยบายที่เกี่ยวกับข้อมูลส่วนบุคคลและจัดให้มีวิธีการที่สามารถตรวจดูความมีอยู่ของข้อมูล ลักษณะของข้อมูล วัตถุประสงค์ของการนำข้อมูลไปใช้ ตลอดจนสถานที่ทำการของผู้ควบคุมข้อมูลและผู้ควบคุมข้อมูล

(1.7) หลักการมีส่วนร่วมของเจ้าของข้อมูล[134]

หมายถึง ให้หน่วยงานของรัฐที่ทำการจัดเก็บและรวบรวมข้อมูลส่วนบุคคลมีมาตรการให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งถึงความมีอยู่ของข้อมูลส่วนบุคคลพร้อมรายละเอียดของข้อมูลแก่เจ้าของข้อมูลส่วนบุคคล และเมื่อหน่วยงานของรัฐได้รับคำร้องขอภายใน

---

[130] เรื่องเดียวกัน, ข้อ 1 (3).

[131] เรื่องเดียวกัน, ข้อ 1 (4).

[132] เรื่องเดียวกัน, ข้อ 1 (5).

[133] เรื่องเดียวกัน, ข้อ 1 (6).

[134] เรื่องเดียวกัน, ข้อ 1 (7).

ระยะเวลาอันสมควร รวมถึงค่าใช้จ่าย(ถ้ามี) และห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธที่จะให้คำชี้แจงหรือให้ข้อมูลแก่เจ้าของข้อมูล และให้ผู้ควบคุมข้อมูลจัดทำบันทึกคำคัดค้านการจัดเก็บความถูกต้องหรือการกระทำใดเกี่ยวกับข้อมูลของเจ้าของข้อมูลไว้เป็นหลักฐาน

(1.8) ความรับผิดชอบของบุคคลซึ่งทำหน้าที่ควบคุมข้อมูล[135]

หมายถึง ให้ผู้ควบคุมข้อมูลส่วนบุคคลปฏิบัติตามมาตรการที่กำหนดไว้ข้างต้น เพื่อให้การดำเนินงานตามแนวนโยบายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเป็นไปตามมาตรฐานของประกาศฉบับนี้

จากข้อ (1.1) - (1.8) จะเห็นได้ว่าหลักการในการให้ความคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐ ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของประเทศด้านสารสนเทศของหน่วยงานรัฐ พ.ศ.2553 ข้อ 1 ซึ่งรัฐบาลไทยได้กำหนดขึ้นมาเป็นแนวทางในการที่จะให้องค์กรหรือหน่วยงานของรัฐต้องปฏิบัติตามนั้น เป็นหลักการที่สำคัญ 8 ประการ ที่ได้รับอิทธิพลมาจากหลักการคุ้มครองข้อมูลส่วนบุคคลของ OECD ตามที่ปรากฏใน Part Two แห่ง Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

(2) ให้หน่วยงานของรัฐที่ทำการจัดเก็บและรวบรวมข้อมูลส่วนบุคคล โดยจัดทำข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการและให้มีรายการอย่างน้อยตามที่ปรากฏใน ข้อ 2 ของประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553 ซึ่งมีสาระสำคัญดังนี้

(2.1) ข้อมูลเบื้องต้นซึ่งประกอบด้วยรายละเอียดต่าง ๆ เช่น ชื่อนโยบายการคุ้มครองข้อมูลส่วนบุคคล หน่วยงานที่กำกับดูแล ตลอดจนขอบเขตของการบังคับใช้และหากมีการเปลี่ยนแปลงวัตถุประสงค์หรือนโยบายการคุ้มครองข้อมูลส่วนบุคคลต้องมีการแจ้งให้เจ้าของข้อมูลทราบ และขอความยินยอมก่อนทุกครั้ง[136]โดยให้มีความชัดเจนว่าหน่วยงานของรัฐจะขอความยินยอมในการจัดเก็บและรวบรวมข้อมูลส่วนบุคคลไปเพื่อวัตถุประสงค์ใด[137]เช่น การแจ้งล่วงหน้าก่อน 15 วันให้เจ้าของข้อมูลทราบทางจดหมายอิเล็กทรอนิกส์หรือประกาศไว้ในหน้าแรกของเว็บไซต์ เว้นแต่กฎหมายกำหนดไว้เป็นอย่างอื่น[138] และหน่วยงานของรัฐต้องทำการ

---

[135] เรื่องเดียวกัน, ข้อ 1 (8).

[136] เรื่องเดียวกัน, ข้อ 2 (1) (ค).

[137] เรื่องเดียวกัน, ข้อ 2 (1) วรรคท้าย.

[138] เรื่องเดียวกัน, ข้อ 2 (1).

กำหนดชื่อนโยบายการให้ความคุ้มครองข้อมูลส่วนบุคคลไว้ให้ชัดเจน และในกรณีที่มีการปรับปรุงนโยบาย ให้ระบุวัน เวลา และปี ที่จะมีการปรับปรุงหรือเปลี่ยนแปลงนโยบายดังกล่าวด้วย[139]

(2.2) ให้หน่วยงานของรัฐที่มีการทำธุรกรรมทางอิเล็กทรอนิกส์และได้มีการเก็บรวบรวมข้อมูลส่วนบุคคลผ่านทางเว็บไซต์ ต้องจัดทำรายละเอียดตามที่กฎหมายกำหนดไว้ในข้อ 2 วรรค 3 (ก) - (จ) แห่งประกาศฉบับนี้ เช่น[140]การติดต่อไปยังผู้ใช้บริการด้วยวิธีการทางอิเล็กทรอนิกส์ต้องทำการแจ้งให้ผู้ใช้บริการทราบล่วงหน้า[141]หรือในเรื่องที่เกี่ยวข้องกับการใช้คุกกี้(Cookies)[142]การเก็บข้อมูลสถิติเกี่ยวกับประชากร(Demographic Information)[143]และการเก็บบันทึกผู้เข้าชมเว็บ(Log Files)[144] ตลอดจนการกำหนดให้หน่วยงานของรัฐจัดเตรียมช่องทางอื่นในการติดต่อสื่อสารสำหรับผู้ใช้บริการที่ไม่ประสงค์จะให้ข้อมูลผ่านทางเว็บไซต์[145]เป็นต้น

(2.3) ในกรณีที่การเก็บรวบรวมข้อมูลผ่านทางเว็บไซต์ของหน่วยงานของรัฐมีการเชื่อมโยงข้อมูลให้แก่หน่วยงานอื่น ให้หน่วยงานของรัฐต้องแสดงการระบุความเชื่อมโยงโดยมีรายการตามที่กำหนดไว้ใน ตามข้อ 2 (3) ของประกาศฉบับนี้ เช่น ชื่อผู้เก็บรวบรวมข้อมูล ชื่อผู้มีสิทธิในข้อมูลและมีสิทธิเข้าถึงข้อมูล ชื่อผู้มีหน้าที่ปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล ตลอดจนประเภทของข้อมูลที่จะใช้ร่วมกับหน่วยงานนั้น ๆ เพื่อให้ผู้ใช้บริการทราบ[146]

(3) ให้หน่วยงานของรัฐที่มีการรวม หรือมีการให้บุคคลอื่นใช้ หรือการเปิดเผยข้อมูลจากที่มาหลายแห่ง ให้หน่วยงานของรัฐระบุไว้ในนโยบายคุ้มครองข้อมูลส่วนบุคคลถึงเจตนารมณ์ในการ

---

[139] เรื่องเดียวกัน, ข้อ 4.

[140] เรื่องเดียวกัน, ข้อ 2 (2) วรรค 2.

[141] เรื่องเดียวกัน, ข้อ 2 (2) (ก).

[142] Cookies หมายถึง คุกกี้หรือไฟล์(File)ข้อมูลขนาดเล็กที่เว็บเซอร์เวอร์(Web Server) จะทำการเก็บไว้ในเครื่องคอมพิวเตอร์ของผู้ใช้ซึ่งเตรียมไว้ใช้ในอนาคต ซึ่งคุกกี้จะฝังตัวอยู่ในส่วนของคำสั่ง html โดยมีการรับและส่งจากทั้งเครื่องเซอร์ฟเวอร์และเครื่องคอมพิวเตอร์ของผู้ใช้

[143] ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553, ข้อ 2 (2) (ค).

[144] Log File หมายถึง ข้อมูลจราจรคอมพิวเตอร์ ซึ่งเป็นข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ที่แสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลาและชนิดของบริการหรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์

[145] เรื่องเดียวกัน, ข้อ 2 (2) (จ).

[146] เรื่องเดียวกัน, ข้อ 2 (3).

รวมข้อมูลที่ได้รับจากที่มาจากแห่งอื่น[147]หรือระบุถึงการที่บุคคลอื่นจะเข้าถึงหรือใช้ข้อมูลภายข้อกำหนดตามกฎหมายของหน่วยงานของรัฐด้วย[148]แล้วแต่กรณี

(4) ให้หน่วยงานของรัฐที่ประสงค์จะนำข้อมูลส่วนบุคคลไปดำเนินการอย่างอื่นนอกเหนือไปจากวัตถุประสงค์ที่ได้ระบุไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคล หน่วยงานของรัฐต้องระบุสิทธิผู้ใช้บริการไว้ในนโยบาย เช่น จะให้หน่วยงานของรัฐรวบรวม จัดเก็บหรือไม่ให้จัดเก็บ ใช้หรือไม่ให้ใช้ และเปิดเผยหรือไม่เปิดเผยข้อมูลดังกล่าว เป็นต้น เพื่อให้ผู้ใช้บริการได้มีสิทธิเลือก[149]

(5) การกำหนดให้หน่วยงานของรัฐซึ่งได้มีการจัดเก็บ รวบรวม หรือใช้ข้อมูลส่วนบุคคลต้องกำหนดวิธีการที่ผู้ใช้บริการเว็บไซต์สามารถเข้าถึงและแก้ไขข้อมูลส่วนบุคคลให้ถูกต้องได้ตลอดจนหน่วยงานของรัฐต้องมีการปรับปรุงข้อมูลให้เป็นปัจจุบัน[150]และมีวิธีการรักษาความมั่นคงปลอดภัยให้เหมาะสม เพื่อป้องกันการเปลี่ยนแปลงแก้ไขข้อมูลโดยมิชอบ ตลอดจนเป็นการป้องการกระทำใดที่จะมีผลทำให้ข้อมูลไม่อยู่ในสภาพพร้อมใช้งานซึ่งหน่วยงานของรัฐต้องดำเนินการดังต่อไปนี้ เช่น[151]การสร้างเสริมความสำนึกในการรับผิดชอบด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้แก่บุคลากร[152]การกำหนดสิทธิและข้อจำกัดสิทธิในการเข้าถึงข้อมูล การทำสำรองข้อมูล[153]การตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของของระบบสารสนเทศ[154]ตลอดจนการกำหนดมาตรการที่เป็นการเฉพาะสำหรับข้อมูลส่วนบุคคลที่มีอ่อนไหวเป็นพิเศษ(Sensitive Data)[155]และข้อมูลส่วนบุคคลของบุคคลซึ่งอายุไม่เกิน 18 ปี[156]และหากมีการติดต่อกับเว็บไซต์ที่ให้ข้อมูลแก่ผู้ใช้บริการในการติดต่อกับหน่วยงานของรัฐต้องจัดให้มีทั้งข้อมูลติดต่อไปยังสถานที่ทำการงานปกติและข้อมูลติดต่อผ่านทางออนไลน์ด้วย[157]

---

[147] เรื่องเดียวกัน, ข้อ 2 (4).

[148] เรื่องเดียวกัน, ข้อ 2 (5).

[149] เรื่องเดียวกัน, ข้อ 2 (6).

[150] เรื่องเดียวกัน, ข้อ 2 (7).

[151] เรื่องเดียวกัน, ข้อ 2 (8).

[152] เรื่องเดียวกัน, ข้อ 2 (8) (ก).

[153] เรื่องเดียวกัน, ข้อ 2 (8) (ข).

[154] เรื่องเดียวกัน, ข้อ 2 (8) (ค).

[155] เรื่องเดียวกัน, ข้อ 2 (8) (ง).

[156] เรื่องเดียวกัน, ข้อ 2 (8) (จ).

[157] เรื่องเดียวกัน, ข้อ 2 (9).

(6) ให้หน่วยงานของรัฐจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลภายใต้หลักการตามข้อ 1 และข้อ 2 ของประกาศฉบับนี้ สำหรับหน่วยงานของรัฐที่ได้รับเครื่องหมายรับรองความหน้าเชื่อถือหรือทรัสต์มาร์ค(Trust Mark)จากหน่วยงานหรือองค์กรที่ทำหน้าที่ออกเครื่องหมายรับรอง และให้หน่วยงานของรัฐนั้นแสดงนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับการรับรอง ดังกล่าวต่อคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์[158]

จากบทบัญญัติข้างต้น จะเห็นได้ว่าประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ว่าประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553 เป็นกฎหมายที่บัญญัติให้หน่วยงานของรัฐนำแนวทางการปฏิบัติในการเก็บรักษาข้อมูลส่วนบุคคลไปปรับใช้ในแต่ละหน่วยงานหรือองค์กรซึ่งมิได้มีรายละเอียดในการแสดงขั้นตอนหรือวิธีการการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่ชัดเจนและไม่มีส่วนใดที่บัญญัติถึงการกำหนดโทษแก่ผู้ทำละเมิดข้อต่อข้อมูลส่วนบุคคล

3.2.8 ประมวลกฎหมายอาญา

ตามประมวลกฎหมายอาญาของประเทศไทยได้มีบัญญัติถึงความผิดฐานเปิดเผยความลับไว้ในหมวดที่ 2 ดังนี้

(1) ความผิดฐานเปิดเผยความลับโดยการเปิดผนึก

เป็นความผิดที่ได้บัญญัติไว้ในมาตรา 322 ซึ่งมีสาระสำคัญ คือ ผู้ใดเปิดผนึกหรือเอาจดหมาย หรือเอกสารใดซึ่งปิดผนึกของผู้อื่นไป เพื่อล่วงรู้ข้อความ หรือเพื่อนำข้อความออกเปิดเผย ถ้าการกระทำนั้นน่าจะเกิดความเสียหายแก่ผู้หนึ่งผู้ใด ต้องระวางโทษ...[159]

(2) ความผิดฐานเปิดเผยความลับโดยเจ้าพนักงานผู้มีหน้าที่

เป็นความผิดที่ได้บัญญัติไว้ในมาตรา 323 ซึ่งมีสาระสำคัญ คือ ผู้ใดล่วงรู้หรือได้มาซึ่งความลับของผู้อื่น โดยเหตุที่เจ้าพนักงานผู้หน้าที่ หรือโดยเหตุที่ประกอบอาชีพเป็นแพทย์ เภสัชกร คนจำหน่ายยา นางผดุงครรภ์ ผู้พยาบาลนักบวช หมอความ ทนายความหรือผู้สอบบัญชีหรือโดยเหตุที่เป็นผู้ช่วยในการประกอบอาชีพนั้น หรือเป็นผู้รับการฝึกอบรมใน

---

[158] เรื่องเดียวกัน, ข้อ 3.

[159] ประมวลกฎหมายอาญา(ฉบับแก้ไขเพิ่มเติม พ.ศ.2551), มาตรา 322.

อาชีพดังกล่าวและได้ล่วงรู้หรือได้มาในการศึกษาอบรมนั้น แล้วเปิดเผยความลับนั้นในประการที่น่าจะเกิดความเสียหายแก่ผู้หนึ่งผู้ใด ต้องระวางโทษ...[160]

อย่างไรก็ตาม ความผิดตามประมวลกฎหมายอาญา มาตรา 322 และ 323 ล้วนแต่เป็นความผิดอันยอมความได้[161] และจะเห็นได้ว่าประมวลกฎหมายอาญาให้ความคุ้มครองข้อมูลส่วนบุคคลโดยนั้นความสำคัญที่ ความเป็นวิชาชีพ หรือการเป็นเจ้าพนักงานซึ่งปฏิบัติหน้าที่และได้นำความลับที่ได้มาเปิดเผย ตลอดจนความผิดในการเปิดผนึกจดหมายเท่านั้น ซึ่งไม่สามารถให้ความคุ้มครองครอบคลุมถึงการกระทำผิดต่อข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐได้

3.2.9 ประมวลกฎหมายแพ่งและพาณิชย์

ประมวลกฎหมายแพ่งและพาณิชย์ของประเทศไทย ได้มีการบัญญัติถึงความผิดฐานกระทำละเมิด ซึ่งอาจนำความเสียหายที่เกิดจากการเปิดเผยข้อมูลส่วนบุคคลมาปรับใช้ได้ โดยกฎหมายได้กำหนดให้การกระทำดังกล่าวมีความรับผิดตามที่ได้บัญญัติไว้ในมาตรา 420 ซึ่งมีสาระสำคัญ คือ ผู้ใดจงใจหรือประมาทเลินเล่อ กระทำต่อบุคคลอื่นโดยผิดกฎหมาย ให้เขาเสียหายถึงแก่ชีวิต ร่างกาย อนามัย เสรีภาพ ทรัพย์สิน หรือสิทธิอย่างใดอย่างหนึ่ง ถือว่าผู้นั้นกระทำละเมิดต้องใช้ค่าสินไหมทดแทนเพื่อการนั้น[162]

อย่างไรก็ตาม ความผิดตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 420 แม้จะระบุไว้ว่าการกระทำต่อบุคคลอื่นโดยผิดกฎหมายอันเป็นการละเมิด แต่ก็ไม่ได้ครอบคลุมถึงความคุ้มครองในเรื่องข้อมูลส่วนบุคคลเอาไว้อย่างชัดเจน และหากเป็นการได้ข้อมูลส่วนบุคคลโดยมิได้เกิดความเสียหายอย่างชัดแจ้ง ก็ไม่เป็นความผิดตามมาตรานี้ อีกทั้งไม่มีโทษทางอาญาเพื่อลงโทษให้ผู้กระทำผิดเข็ดหลาบอีกด้วย

---

[160] เรื่องเดียวกัน, มาตรา 323.

[161] เรื่องเดียวกัน, มาตรา 325.

[162] ประมวลกฎหมายแพ่งและพาณิชย์(ฉบับแก้ไขเพิ่มเติม พ.ศ.2551), มาตรา 420.

3.2.10 ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...

ปัจจุบันในประเทศไทยมีกฎหมายบังคับเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเป็นการเฉพาะกรณีไป ซึ่งยังไม่ครอบคลุมเพียงพอต่อการคุ้มครองข้อมูลส่วนบุคคลทั้งหมด แม้ว่าพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ซึ่งเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับหลักที่ประเทศไทยใช้บังคับอยู่ แต่ก็มีความครอบคลุมเฉพาะข้อมูลส่วนบุคคลที่อยู่ในครอบครองของหน่วยงานของรัฐเท่านั้น ซึ่งยังไม่ครอบคลุมถึงข้อมูลส่วนบุคคลที่อยู่ความครอบครองของเอกชนไว้เป็นการเฉพาะ อีกทั้งในปัจจุบันได้เกิดปัญหากับการคุ้มครองข้อมูลส่วนบุคคลในภาคเอกชนเป็นจำนวนมาก โดยเฉพาะการนำข้อมูลส่วนบุคคลไปแสวงหาประโยชน์หรือเปิดเผยโดยไม่ได้รับความยินยอมจากบุคคลซึ่งเป็นเจ้าของข้อมูล จนสร้างความเดือดร้อนรำคาญหรือเกิดความเสียหายให้แก่บุคคลซึ่งเป็นเจ้าของข้อมูล จึงสมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป เพื่อป้องกันจากการแสวงประโยชน์โดยมิชอบจากข้อมูลส่วนบุคคลจึงจำเป็นต้องตราพระราชบัญญัตินี้ขึ้นเพื่อบังคับใช้ โดยในปัจจุบันกฎหมายฉบับนี้ยังอยู่ในระหว่างการพิจารณาเพื่อศึกษาผลกระทบและตีความข้อกฎหมาย[163]

ทั้งนี้ ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลได้ยกร่างขึ้นโดยอาศัยแนวทางขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (Organization for Economic Cooperation and Development) หรือ OECD และ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ของสหภาพยุโรป ซึ่งในเวลาต่อมาจึงได้มีการอาศัยเทียบเคียงกับกฎหมายของอีกหลายประเทศ เช่น เยอรมัน อังกฤษ ออสเตรียเลีย เขตปกครองพิเศษฮ่องกง เป็นต้น[164] โดยในปัจจุบันร่างพระราชบัญญัตินี้ซึ่งอยู่ระหว่างการศึกษาและพิจารณาอยู่นั้น มีสาระสำคัญ ดังนี้

(1) ขอบเขตการใช้บังคับ

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ให้ใช้บังคับกับหน่วยงาน หรือองค์กรทั้งภาครัฐและเอกชนทั้งหมดเป็นการทั่วไป ซึ่งเป็นเรื่องที่ยังไม่มีกฎหมายคุ้มตรองข้อมูลส่วนบุคคลมาใช้บังคับเป็นการเฉพาะ[165]ก็ให้ใช้พระราชบัญญัติฉบับนี้บังคับใช้แทน[166]โดยมีข้อยกเว้นไว้ว่า พระราชบัญญัตินี้ไม่ให้ใช้บังคับแก่ กรณีดังต่อไปนี้

---

[163] บันทึกหลักการและเหตุผลประกอบร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ...,

[164] สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, **รายงานการประเมินผลนโยบายเทคโนโลยีสารสนเทศ IT2000**, (ม.ป.พ., 2544), 12.

[165] บันทึกหลักการและเหตุผลประกอบร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ...,

[166] เรื่องเดียวกัน, มาตรา 4 วรรค 2.

(1.1) หน่วยงานของรัฐที่อยู่ภายใต้บังคับพระราชบัญญัติข้อมูลข่าวสารของราชการ

(1.2) บุคคลหรือนิติบุคคลที่เก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตนโดยมิได้ให้ผู้อื่นใช้ข้อมูลส่วนบุคคล หรือเปิดเผยข้อมูลส่วนบุคคลนั้นต่อผู้อื่น

(1.3) บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมไว้เพื่อการสื่อสารมวลชน งานศิลปกรรม หรืองานวรรณกรรม[167]

(2) นิยามศัพท์ที่สำคัญ

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ได้มีการกำหนดนิยามศัพท์ที่สำคัญอันมีความเฉพาะในพระราชบัญญัติฉบับนี้ โดยมีสาระสำคัญดังต่อไปนี้

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของบุคคลนั้นหรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะที่ทำให้รู้ตัวบุคคลนั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคน หรือรูปถ่าย และให้หมายความรวมถึงข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย[168]

“เจ้าของข้อมูลส่วนบุคคล” ให้หมายความรวมถึง ทายาทหรือคู่สมรสของเจ้าของข้อมูลส่วนบุคคลในกรณีที่เจ้าของข้อมูลส่วนบุคคลนั้นถึงแก่ความตาย หรือผู้ซึ่งมีหน้าที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลตามที่กำหนดในกฎกระทรวง

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า ผู้ซึ่งมีหน้าที่รับผิดชอบในการเก็บรวบรวม ควบคุมการใช้และการเปิดเผยข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้

(3) การเก็บรวบรวมข้อมูลส่วนบุคคลตามพระราชบัญญัติฉบับนี้

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ได้มีการกำหนดหลักเกณฑ์เรื่องการเก็บรวบรวมข้อมูลส่วนบุคคลได้ ซึ่งอาจแบ่งพิจารณาได้เป็น 2 กรณี ได้แก่ การเก็บรวบรวมข้อมูลส่วนบุคคลเป็นกรณีทั่วไป และการเก็บรวบรวมข้อมูลส่วนบุคคลอันมีลักษณะต้องห้ามโดยมีสาระสำคัญ ดังนี้

---

[167] เรื่องเดียวกัน, มาตรา 5.

[168] บันทึกหลักการและเหตุผลประกอบร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ..., มาตรา 3.

(3.1) การเก็บรวบรวมข้อมูลส่วนบุคคลเป็นกรณีทั่วไป

(3.1.1) การเก็บรวบรวมข้อมูลส่วนบุคคลต้องเป็นการเก็บโดยตรงจากเจ้าของข้อมูลส่วนบุคคล หากจะเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น ต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลนั้นทราบหลังจากเก็บข้อมูลแล้ว[169]และต้องเป็นกรณีดังต่อไปนี้

(ก) ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล[170]

(ข) เป็นสิ่งซึ่งได้จากการสังเกตการณ์ จากการปรากฏตัวของบุคคลผู้ถูกเก็บข้อมูลโดยสมัครใจและเป็นกิจกรรมที่เปิดเผยต่อสาธารณะ[171]

(ค) เป็นสิ่งจำเป็นในการพิจารณาการตัดสินการจะได้รับรางวัลเกียรติยศหรือผลประโยชน์อื่นในลักษณะคล้ายคลึงกัน[172]

(ง) เป็นการปฏิบัติตามสัญญาที่ทำกับเจ้าของข้อมูลส่วนบุคคลหรือตามมาตรการที่เจ้าของข้อมูลส่วนบุคคลร้องขอเพื่อให้เป็นไปตามสัญญา[173]

(จ) เป็นการเก็บรวบรวมข้อมูลโดยได้รับยกเว้นให้เก็บได้โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามมาตรา 18[174]ซึ่งต้องเป็นการใช้เพื่อปฏิบัติตามกฎหมาย[175]การใช้เพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคลซึ่งไม่อาจขอความยินยอมได้ในเวลานั้น[176]การใช้เพื่อประโยชน์เกี่ยวกับชีวิตหรือสุขภาพหรือความปลอดภัยของเจ้าของข้อมูล[177] การใช้เพื่อประโยชน์ในการสอบสวนและพิจารณาคดี[178]ตลอดจนการใช้เพื่อประโยชน์ในการศึกษาวิจัยหรือสถิติ[179]และการเปิดเผยในกรณีอื่นตามกฎกระทรวง[180]แต่ทั้งนี้จะต้องเป็นไปตามเงื่อนไขที่มาตรา 18 กำหนดไว้

(ฉ) เป็นการเก็บรวบรวมโดยมีความจำเป็นอื่นใด ตามที่คณะกรรมการประกาศกำหนด[181]

---

[169] เรื่องเดียวกัน, มาตรา 21.

[170] เรื่องเดียวกัน, มาตรา 21 (1).

[171] เรื่องเดียวกัน, มาตรา 21 (2).

[172] เรื่องเดียวกัน, มาตรา 21 (3).

[173] เรื่องเดียวกัน, มาตรา 21 (4).

[174] เรื่องเดียวกัน, มาตรา 21 (5).

[175] เรื่องเดียวกัน, มาตรา 18 (1).

[176] เรื่องเดียวกัน, มาตรา 18 (2).

[177] เรื่องเดียวกัน, มาตรา 18 (3).

[178] เรื่องเดียวกัน, มาตรา 18 (4).

[179] เรื่องเดียวกัน, มาตรา 18 (5).

[180] เรื่องเดียวกัน, มาตรา 18 (6).

[181] เรื่องเดียวกัน, มาตรา 21 (6).

(3.2) การเก็บรวบรวมข้อมูลส่วนบุคคลอันมีลักษณะต้องห้าม[182]

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ได้มีการกำหนดหลักเกณฑ์เรื่องการเก็บรวบรวมข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลอันมีลักษณะต้องห้าม โดยมีหลักเกณฑ์ต่างหากจากการเก็บรวบรวมข้อมูลทั่วไป โดยมีสาระสำคัญ ดังนี้

(3.2.1) ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลที่เกี่ยวข้องกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ประวัติสุขภาพ หรือข้อมูลอื่นใดซึ่งกระทบความรู้สึกของผู้อื่นหรือประชาชน[183]

(3.2.2) ข้อมูลที่อาจเป็นผลร้ายทำให้เสื่อมเสียชื่อเสียงหรืออาจก่อให้เกิดความรู้สึกเกี่ยวกับการเลือกปฏิบัติโดยไม่เป็นธรรมหรือความไม่เท่าเทียมกันแก่บุคคลใด[184]

(3.2.3) ข้อมูลอื่นตามที่กำหนดในกฎกระทรวง

(3.3) ข้อยกเว้นในเก็บรวบรวมข้อมูลส่วนบุคคลอันมีลักษณะต้องห้าม[185]

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ได้มีการกำหนดหลักเกณฑ์เรื่องการเก็บรวบรวมข้อมูลส่วนบุคคลไว้ ซึ่งการเก็บรวบรวมข้อมูลส่วนบุคคลอันเป็นข้อมูลส่วนบุคคลอันมีลักษณะต้องห้ามได้ จะต้องเป็นกรณีดังต่อไปนี้

(3.3.1) เป็นการเก็บรวบรวมข้อมูลโดยได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลส่วนบุคคล[186]

(3.3.2) เป็นการเก็บรวบรวมเพื่อวัตถุประสงค์ทางการแพทย์ซึ่งเป็นความลับ[187]

(3.3.3) เป็นการเก็บรวบรวมโดยได้รับยกเว้น ให้ไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามมาตรา 18[188]ซึ่งต้องเป็นการใช้เพื่อปฏิบัติตามกฎหมาย[189]การใช้เพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคลซึ่งไม่อาจขอความยินยอมได้ในเวลานั้น[190]การใช้เพื่อประโยชน์เกี่ยวกับชีวิตหรือสุขภาพหรือความปลอดภัยของเจ้าของข้อมูล[191]การใช้เพื่อประโยชน์ในการสอบสวนและ

---

[182] เรื่องเดียวกัน, มาตรา 22.

[183] เรื่องเดียวกัน, มาตรา 22 (1).

[184] เรื่องเดียวกัน, มาตรา 22 (2).

[185] เรื่องเดียวกัน, มาตรา 22 วรรค 2.

[186] เรื่องเดียวกัน, มาตรา 22 วรรค 2 (1).

[187] เรื่องเดียวกัน, มาตรา 22 วรรค 2 (2).

[188] เรื่องเดียวกัน, มาตรา 22 วรรค 2 (3).

[189] เรื่องเดียวกัน, มาตรา 18 (1).

[190] เรื่องเดียวกัน, มาตรา 18 (2).

[191] เรื่องเดียวกัน, มาตรา 18 (3).

พิจารณาคดี[192]การใช้เพื่อประโยชน์ในการศึกษาวิจัยหรือสถิติ[193]และเปิดเผยในกรณีอื่นตามกฎกระทรวง[194]แต่ทั้งนี้จะต้องเป็นไปตามเงื่อนไขที่มาตรา 18 กำหนดไว้

(3.3.4) เป็นการเก็บรวบรวมโดยมีความจำเป็นอื่นใด ตามที่คณะกรรมการได้ประกาศกำหนด[195]

(3.4) การแจ้งรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคล

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ได้มีการกำหนดหลักเกณฑ์เรื่องการเก็บรวบรวมข้อมูลส่วนบุคคลไว้ ซึ่งการเก็บรวบรวมข้อมูลส่วนบุคคลไม่ว่าในกรณีใด ผู้ที่ทำการเก็บรวบรวมข้อมูลต้องแจ้งข้อมูลดังต่อไปนี้ ก่อนทำการเก็บรวบรวมข้อมูลหรือขณะทำการเก็บรวบรวมข้อมูลก็ได้ มิเช่นนั้นจะถือว่าจะเป็นการเก็บข้อมูลส่วนบุคคลโดยมิชอบ[196]

(3.4.1) ให้แจ้งชื่อ สถานที่ทำการ และสถานภาพของผู้ควบคุมข้อมูลว่าเป็นบุคคลธรรมดาหรือนิติบุคคลและเป็นหน่วยงานหรือประกอบกิจการในเชิงพาณิชย์ใด[197]

(3.4.2) ให้แจ้งเจ้าของข้อมูลส่วนบุคคลก่อนทำการเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคล ทั้งนี้ หลักเกณฑ์ให้เป็นไปตามที่กำหนดในมาตรา 17[198]และต้องแจ้งให้เจ้าของข้อมูลทราบว่าเป็นข้อมูลอันมีลักษณะต้องห้าม ตามมาตรา 22 หรือไม่[199]

(3.4.3) ให้แจ้งกำหนดระยะเวลาในการเก็บรักษาข้อมูล[200]และแจ้งสิทธิในการขอตรวจสอบข้อมูล สิทธิในการได้รับแจ้งข้อมูล สิทธิในการระงับข้อมูล สิทธิในการลบทำลายข้อมูลและสิทธิในการขอให้เปิดเผยแหล่งที่มาของข้อมูล ซึ่งบัญญัติไว้ในมาตรา 42[201]ตลอดจนให้แจ้งละเอียดอื่นตามที่คณะกรรมกำหนด[202]

---

[192] เรื่องเดียวกัน, มาตรา 18 (4).

[193] เรื่องเดียวกัน, มาตรา 26 (5).

[194] เรื่องเดียวกัน, มาตรา 26 (6).

[195] เรื่องเดียวกัน, มาตรา 22 วรรค 2 (4).

[196] เรื่องเดียวกัน, มาตรา 23.

[197] เรื่องเดียวกัน, มาตรา 23 (1).

[198] เรื่องเดียวกัน, มาตรา 23 (2).

[199] เรื่องเดียวกัน, มาตรา 23 (3).

[200] เรื่องเดียวกัน, มาตรา 23 (4).

[201] เรื่องเดียวกัน, มาตรา 23 (5).

[202] เรื่องเดียวกัน, มาตรา 23 (5).

(4) การเปิดเผยข้อมูลส่วนบุคคลและข้อยกเว้นการเปิดเผยข้อมูลส่วนบุคคล

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ได้มีการกำหนดหลักเกณฑ์เรื่องการเปิดเผยข้อมูลส่วนบุคคลแตกต่างไปจากพระราชบัญญัติข้อมูลข่าวสารของราชการ ซึ่งบัญญัติถึงเรื่องการเปิดเผยข้อมูลเพียงอย่างเดียว แต่ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลได้บัญญัติถึงเรื่องการเปิดเผยและการใช้ข้อมูลแยกออกจากกัน โดยหลักเกณฑ์ในการเปิดเผยข้อมูลแห่งพระราชบัญญัติฉบับนี้ อาจแบ่งออกได้เป็น 4 กรณี ได้แก่ ข้อยกเว้นในเปิดเผยข้อมูลส่วนบุคคลกรณีทั่วไป ข้อยกเว้นในเปิดเผยข้อมูลส่วนบุคคลไปนอกราชอาณาจักรและข้อยกเว้นในการเปิดเผยข้อมูลส่วนบุคคลไปยังประเทศที่มีการคุ้มครองข้อมูลส่วนบุคคลในระดับต่ำกว่าและข้อยกเว้นในการเปิดเผยข้อมูลส่วนบุคคลอันมีลักษณะต้องห้าม โดยมีสาระสำคัญ คือ หน่วยงานของรัฐจะทำการเปิดเผยข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของตนเองได้เฉพาะที่เกี่ยวข้องกับเจ้าของข้อมูลโดยตรงตามเท่าที่จำเป็นและเหมาะสม[203]โดยมีข้อยกเว้นดังต่อไปนี้

(4.1) ข้อยกเว้นในเปิดเผยข้อมูลส่วนบุคคลกรณีทั่วไป[204]

(4.1.1) เป็นการเปิดเผยข้อมูลส่วนบุคคลโดยได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลส่วนบุคคล[205]

(4.1.2) เป็นการเปิดเผยต่อทนายความของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งได้รับแต่งตั้งให้ว่าความแทนในคดีใดคดีหนึ่งหรือได้รับมอบอำนาจทั่วไปให้กระทำการแทนผู้ควบคุมข้อมูลส่วนบุคคล[206]

(4.1.3) เป็นการเปิดเผยเพื่อวัตถุประสงค์ในการเรียกเก็บหนี้ซึ่งเจ้าของข้อมูลส่วนบุคคลจะต้องชำระให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล[207]

(4.1.4) เป็นการเปิดเผยให้แก่หน่วยงานใดซึ่งที่มีหน้าที่รักษาข้อมูลไว้เป็นประวัติศาสตร์[208]

(4.1.5) เป็นการเปิดเผยเมื่อเจ้าหน้าที่รัฐร้องขอโดยมีเหตุอันควรสงสัยว่าข้อมูลส่วนบุคคลนั้นเกี่ยวข้องกับความมั่นคงของประเทศ หรือกิจการระหว่างประเทศ[209]

(4.1.6) เป็นการเปิดเผยข้อมูลที่รวบรวมได้จากการสังเกตการณ์จากการปรากฏตัวของบุคคลผู้ถูกเก็บข้อมูลโดยสมัครใจและเป็นกิจกรรมที่เปิดเผยต่อสาธารณะตามมาตรา 21 (2)[210]

---

[203] เรื่องเดียวกัน, มาตรา 26 วรรค 2.

[204] เรื่องเดียวกัน, มาตรา 26.

[205] เรื่องเดียวกัน, มาตรา 26 (1).

[206] เรื่องเดียวกัน, มาตรา 26 (2).

[207] เรื่องเดียวกัน, มาตรา 26 (3).

[208] เรื่องเดียวกัน, มาตรา 26 (4).

[209] เรื่องเดียวกัน, มาตรา 26 (5).

(4.1.7) เป็นการเปิดเผยข้อมูลที่รวบรวมไว้เพื่อสิ่งจำเป็นในการพิจารณาตัดสินการได้รับรางวัล หรือผลประโยชน์อื่นในลักษณะคล้ายคลึงกันตามมาตรา 21 (3)[211]

(4.1.8) เป็นการเปิดเผยมีความจำเป็นอื่นตามที่กฎหมายกำหนด[212]

(4.2) ข้อยกเว้นในเปิดเผยข้อมูลส่วนบุคคลไปนอกราชอาณาจักร[213]

(4.2.1) เป็นการเปิดเผยโดยได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลส่วนบุคคล[214]ซึ่งการขอความยินยอมต้องเป็นไปตามหลักเกณฑ์ที่คณะกรรมการกำหนด[215]

(4.2.2) เป็นการเปิดเผยเพื่อการดำเนินคดีนอกราชอาณาจักร[216]

(4.2.3) เป็นการเปิดเผยซึ่งเป็นการปฏิบัติตามสัญญาที่ทำกับเจ้าของข้อมูลส่วนบุคคล หรือตามมาตรการที่เจ้าของข้อมูลส่วนบุคคลร้องขอให้เป็นไปตามสัญญานั้น[217]

(4.2.4) เป็นการเปิดเผยโดยเป็นผลจากการปฏิบัติตามสัญญาที่ทำกับผู้อื่นเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล[218]

(4.2.5) เป็นการเปิดเผยข้อมูลส่วนบุคคล ซึ่งได้รับยกเว้นให้เก็บรวบรวม ใช้ หรือเปิดเผยได้ โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามมาตรา 18[219] ในเรื่องของเปิดเผยเพื่อปฏิบัติตามกฎหมาย[220]หรือเพื่อประโยชน์เกี่ยวกับชีวิตหรือสุขภาพหรือความปลอดภัยของเจ้าของข้อมูล[221]แต่ทั้งนี้จะต้องเป็นไปตามเงื่อนไขที่มาตรา 18 กำหนดไว้[222]

(4.2.6) เป็นการเปิดเผยโดยความจำเป็นตามที่คณะกรรมการกำหนด[223]

---

[210] เรื่องเดียวกัน, มาตรา 26 (6).

[211] เรื่องเดียวกัน, มาตรา 26 (6).

[212] เรื่องเดียวกัน, มาตรา 26 (7).

[213] เรื่องเดียวกัน, มาตรา 29.

[214] เรื่องเดียวกัน, มาตรา 29 (1).

[215] เรื่องเดียวกัน, มาตรา 29 วรรค 2.

[216] เรื่องเดียวกัน, มาตรา 29 (2).

[217] เรื่องเดียวกัน, มาตรา 29 (3).

[218] เรื่องเดียวกัน, มาตรา 29 (4).

[219] เรื่องเดียวกัน, มาตรา 18 (1).

[220] เรื่องเดียวกัน, มาตรา 18 (2).

[221] เรื่องเดียวกัน, มาตรา 18 (3).

[222] เรื่องเดียวกัน, มาตรา 29 (5).

[223] เรื่องเดียวกัน, มาตรา 29 (6).

(4.3) ข้อยกเว้นในการเปิดเผยข้อมูลส่วนบุคคลไปยังประเทศที่มีการคุ้มครองข้อมูลส่วนบุคคลในระดับต่ำกว่า

ทั้งนี้ ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ได้บัญญัติห้ามมิให้มีการส่งข้อมูลส่วนบุคคลไปยังประเทศใดที่มีระดับมาตรการคุ้มครองข้อมูลส่วนบุคคลที่ต่ำกว่าพระราชบัญญัติฉบับนี้ แต่มีข้อยกเว้นให้เปิดเผยได้ในกรณี ดังต่อไปนี้[224]

(4.3.1) เป็นการเปิดเผยโดยได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลส่วนบุคคล[225] ทั้งนี้ การขอความยินยอมและการพิจารณาว่ากฎหมายประเทศใดมีระดับต่ำกว่าให้มีหลักเกณฑ์เป็นไปตามที่คณะกรรมการกำหนด[226]

(4.3.2) เป็นการเปิดเผยข้อมูลส่วนบุคคล ซึ่งได้รับยกเว้นให้เก็บรวบรวม ใช้ หรือเปิดเผยได้โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามมาตรา 18[227]ในเรื่องของการเปิดเผยเพื่อปฏิบัติตามกฎหมาย[228]หรือเพื่อประโยชน์เกี่ยวกับชีวิตหรือสุขภาพหรือความปลอดภัยของเจ้าของข้อมูล[229] ซึ่งจะต้องเป็นไปตามเงื่อนไขที่มาตรา 18 กำหนดไว้[230]

(4.3.3) เป็นการเปิดเผยโดยความจำเป็นตามที่คณะกรรมการกำหนด[231]

(4.4) ข้อยกเว้นการเปิดเผยข้อมูลส่วนบุคคลอันมีลักษณะต้องห้าม[232]

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ได้มีการกำหนดหลักเกณฑ์ในการเปิดเผยข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลส่วนบุคคลอันมีลักษณะต้องห้ามตามมาตรา 22 ซึ่งกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้ข้อมูลส่วนบุคคลอันมีลักษณะต้องห้ามที่อยู่ในความครอบครองหรือควบคุมดูแลของตนเองมิได้ เว้นแต่มีกรณีดังต่อไปนี้[233]

---

[224] เรื่องเดียวกัน, มาตรา 30.

[225] เรื่องเดียวกัน, มาตรา 30 (1).

[226] เรื่องเดียวกัน, มาตรา 30 วรรค 2.

[227] เรื่องเดียวกัน, มาตรา 18 (1).

[228] เรื่องเดียวกัน, มาตรา 18 (2).

[229] เรื่องเดียวกัน, มาตรา 18 (3).

[230] เรื่องเดียวกัน, มาตรา 30 (2).

[231] เรื่องเดียวกัน, มาตรา 30 (3).

[232] เรื่องเดียวกัน, มาตรา 27.

[233] เรื่องเดียวกัน, มาตรา 27 วรรค 2.

(4.4.1) เป็นการเปิดเผยโดยได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลส่วนบุคคล[234]

(4.4.2) เป็นการเปิดเผยโดยเก็บข้อมูลส่วนบุคคลเพื่อการนั้นไว้เป็นความลับและเป็นการใช้ข้อมูลส่วนบุคคลซึ่งได้รับยกเว้นแม้เป็นข้อมูลส่วนบุคคลอันมีลักษณะต้องห้าม ซึ่งได้ใช้เพื่อวัตถุประสงค์ทางการแพทย์หรือการรักษาพยาบาลจากบุคคลใดและได้เก็บข้อมูลส่วนบุคคลเพื่อการนั้นไว้เป็นความลับ[235]

(4.4.3) เป็นการเปิดเผยโดยได้รับยกเว้นให้ให้ได้โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามมาตรา 18[236]ในเรื่องของการใช้เพื่อปฏิบัติตามกฎหมาย[237] การใช้เพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคลซึ่งไม่อาจขอความยินยอมได้ในเวลานั้น[238] เพื่อประโยชน์เกี่ยวกับชีวิตหรือสุขภาพหรือความปลอดภัยของเจ้าของข้อมูล[239]เพื่อประโยชน์ในการสอบสวนและพิจารณาคดี [240]เพื่อประโยชน์ในการศึกษาวิจัยหรือสถิติ[241]และการใช้ในกรณีอื่นตามกฎกระทรวง[242]แต่ทั้งนี้จะต้องเป็นไปตามเงื่อนไขที่มาตรา 18 กำหนดไว้[243]

(4.4.4) เป็นการใช้โดยความจำเป็นตามที่คณะกรรมการกำหนด[244]

(5) การใช้ข้อมูลส่วนบุคคลและข้อยกเว้นการใช้ข้อมูลส่วนบุคคล

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ได้มีการกำหนดหลักเกณฑ์เรื่องการใช้ข้อมูลส่วนบุคคลต่างหากจากการเปิดเผยข้อมูลส่วนบุคคล ซึ่งอาจแบ่งได้เป็น 2 กรณี ได้แก่ ข้อยกเว้นการใช้ข้อมูลส่วนบุคคลกรณีทั่วไปและข้อยกเว้นการใช้ข้อมูลส่วนบุคคลที่เป็นข้อมูลต้องห้าม โดยมีสาระสำคัญดังต่อไปนี้

(5.1) ข้อยกเว้นการใช้ข้อมูลส่วนบุคคลกรณีทั่วไป

ในกรณีนี้ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลจะใช้ข้อมูลส่วนบุคคลที่อยู่ในความครอบครองหรือควบคุมดูแลของตนเอง เว้นแต่มีกรณีดังต่อไปนี้[245]

---

[234] เรื่องเดียวกัน, มาตรา 27 (1).

[235] เรื่องเดียวกัน, มาตรา 27 (2).

[236] เรื่องเดียวกัน, มาตรา 18.

[237] เรื่องเดียวกัน, มาตรา 18 (1).

[238] เรื่องเดียวกัน, มาตรา 18 (2).

[239] เรื่องเดียวกัน, มาตรา 18 (3).

[240] เรื่องเดียวกัน, มาตรา 18 (4).

[241] เรื่องเดียวกัน, มาตรา 26 (5).

[242] เรื่องเดียวกัน, มาตรา 26 (6).

[243] เรื่องเดียวกัน, มาตรา 27 (2).

[244] เรื่องเดียวกัน, มาตรา 27 (3).

(5.1.1) เป็นการใช้ข้อมูลโดยได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลส่วนบุคคล[246]

(5.1.2) เป็นการใช้ข้อมูลส่วนบุคคล ซึ่งได้รับยกเว้นให้เก็บรวบรวม ใช้ หรือเปิดเผยได้โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามมาตรา 18[247]ในเรื่องของการใช้เพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคลซึ่งไม่อาจขอความยินยอมได้ในเวลานั้น[248]เกี่ยวกับชีวิตหรือสุขภาพหรือความปลอดภัยของเจ้าของข้อมูล[249]เพื่อประโยชน์ในการสอบสวนและพิจารณาคดี[250]เพื่อประโยชน์ในการศึกษาวิจัยหรือสถิติ[251]แต่ทั้งนี้จะต้องเป็นไปตามเงื่อนไขที่มาตรา 18 กำหนดไว้[252]

(5.1.3) เป็นการใช้โดยความจำเป็นตามที่คณะกรรมการกำหนด[253]

(5.2) ข้อยกเว้นการใช้ข้อมูลส่วนบุคคลที่เป็นข้อมูลต้องห้าม

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ได้มีการกำหนดหลักเกณฑ์ในการใช้ข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลส่วนบุคคลอันมีลักษณะต้องห้ามตามมาตรา 22 ซึ่งกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้ข้อมูลส่วนบุคคลอันมีลักษณะต้องห้ามที่อยู่ในความครอบครองหรือควบคุมดูแลของตนเองไม่ได้ เว้นแต่เป็นกรณีที่มีข้อยกเว้นตามที่กำหนดไว้ในมาตรา 25 ซึ่งมีสาระสำคัญเช่นเดียวกันกับข้อยกเว้นการใช้ข้อมูลส่วนบุคคลอันมีลักษณะต้องห้ามตามมาตรา 27[254]ซึ่งได้อธิบายรายละเอียดแล้วในข้อ (3.4)

(6) การให้ความคุ้มครองข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ได้มีการบัญญัติถึงการให้การคุ้มครองข้อมูลส่วนบุคคลซึ่งภาคเอกชนหรือหน่วยงานของรัฐต้องดำเนินการโดยมีสาระสำคัญ ดังต่อไปนี้

---

[245] เรื่องเดียวกัน, มาตรา 24.

[246] เรื่องเดียวกัน, มาตรา 24 (1).

[247] เรื่องเดียวกัน, มาตรา 18 (1).

[248] เรื่องเดียวกัน, มาตรา 18 (2).

[249] เรื่องเดียวกัน, มาตรา 18 (3).

[250] เรื่องเดียวกัน, มาตรา 18 (4).

[251] เรื่องเดียวกัน, มาตรา 26 (5).

[252] เรื่องเดียวกัน, มาตรา 24 (2).

[253] เรื่องเดียวกัน, มาตรา 24 (3).

[254] เรื่องเดียวกัน, มาตรา 27.

(6.1) ผู้ควบคุมข้อมูลส่วนบุคคลจะทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้ เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือมีกฎหมายยกเว้นไว้[255]

(6.2) การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยสุจริต[256]ทั้งนี้การแจ้งจะต้องเป็นวิธีการเปิดเผยและโดยชัดแจ้ง[257]

(6.3) การเพิกถอนความยินยอมเจ้าของข้อมูลส่วนบุคคลจะเพิกถอนความยินยอมเมื่อใดก็ได้ หากไม่มีกฎหมายหรือสัญญาใดจำกัดสิทธิในการเพิกถอนไว้[258]

(6.4) ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ดูแลรักษาข้อมูลส่วนบุคคลให้มีความถูกต้องเป็นปัจจุบันไม่ให้สูญหาย ถูกแก้ไข หรือถูกเปลี่ยนแปลง[259]

(6.5) ห้ามมิให้ผู้ควบคุมข้อมูลทำการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลผิดไปจากวัตถุประสงค์ที่แจ้งเจ้าของข้อมูล[260]เว้นแต่ได้แจ้งวัตถุประสงค์ใหม่ และได้รับความยินยอมจากเจ้าของข้อมูลแล้ว[261]หรือเป็นกรณีที่กฎหมายบัญญัติให้กระทำได้[262]

(7) การตรวจสอบข้อมูลและกระบวนการขอแก้ไขข้อมูล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลได้มีการบัญญัติถึงกระบวนการตรวจสอบและขอแก้ไขข้อมูลไว้ ซึ่งมีสาระสำคัญ คือ การกำหนดสิทธิให้แก่เจ้าของข้อมูลในตรวจดูข้อมูลส่วนบุคคลโดยสามารถขอสำเนาข้อมูลได้[263]และมีสิทธิที่จะขอให้หน่วยงานหรือองค์กรแจ้งถึงการมีอยู่ การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวข้อง[264]และมีสิทธิขอแก้ไขข้อมูลให้ถูกต้อง[265]และมีสิทธิขอให้ระงับการใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวข้องที่ไม่ถูกต้อง[266]และมีสิทธิในการขอให้ลบหรือทำลายข้อมูลส่วนบุคคลที่เกี่ยวข้องเมื่อพ้นกำหนดเวลาการเก็บรวบรวม หรือหมดความจำเป็นตามวัตถุประสงค์[267]ตลอดจนมีสิทธิในการขอให้เปิดเผยข้อมูล

---

[255] เรื่องเดียวกัน, มาตรา 15 วรรค (1).

[256] เรื่องเดียวกัน, มาตรา 15 วรรค (2).

[257] เรื่องเดียวกัน, มาตรา 17 วรรค 2.

[258] เรื่องเดียวกัน, มาตรา 15 วรรค (3).

[259] เรื่องเดียวกัน, มาตรา 16.

[260] เรื่องเดียวกัน, มาตรา 17.

[261] เรื่องเดียวกัน, มาตรา 17 วรรค 1.

[262] เรื่องเดียวกัน, มาตรา 17 วรรค 2.

[263] เรื่องเดียวกัน, มาตรา 42 (1).

[264] เรื่องเดียวกัน, มาตรา 42 (2).

[265] เรื่องเดียวกัน, มาตรา 42 (3).

[266] เรื่องเดียวกัน, มาตรา 42 (4).

[267] เรื่องเดียวกัน, มาตรา 42 (5).

ส่วนบุคคลที่ไม่ได้ให้ความยินยอมในการเก็บข้อมูล[268]อันเป็นการบัญญัติไว้โดยชัดแจ้งถึงสิทธิของบุคคลในการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของตนเอง ดังมีสาระสำคัญ ดังต่อไปนี้

(7.1) ในกรณีที่เจ้าของข้อมูลส่วนบุคคลที่ได้รับความเสียหาย มีสิทธิที่จะร้องเรียนต่อคณะกรรมการในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคล ที่ไม่ปฏิบัติตามพระราชบัญญัตินี้[269]โดยยื่นคำร้องเรียนให้คณะกรรมการตรวจสอบข้อมูลส่วนบุคคล ซึ่งมีหลักเกณฑ์และวิธีพิจารณาตามที่คณะกรรมการกำหนด[270]

(7.2) ในกรณีที่เรื่องร้องเรียนไม่ได้รับการปฏิบัติให้ถูกต้องหรือได้รับการปฏิเสธการรับเรื่องร้องเรียนไว้พิจารณา ให้หน่วยงานมีหนังสือแจ้งให้คณะกรรมการทราบ[271]และให้คณะกรรมการตรวจสอบเรื่องร้องเรียนดังกล่าว หากเห็นว่าการกระทำนั้นไม่เป็นความจริงให้มีคำสั่งยุติเรื่อง[272]หากเห็นว่าเป็นความจริงให้ดำเนินการตามหลักเกณฑ์ที่กำหนดต่อไป[273]

(8) การเก็บรักษาและการแก้ไขเปลี่ยนแปลงข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลได้มีการบัญญัติถึงมาตรการในการเก็บรักษาและขอการแก้ไขเปลี่ยนแปลงข้อมูลส่วนบุคคลไว้ โดยในการเก็บรวบรวม ใช้ เปิดเผย แก้ไขเปลี่ยนแปลง ลบ หรือกระทำการใดต่อข้อมูลส่วนบุคคลจะสามารถดำเนินการได้ต่อเมื่อได้ปฏิบัติตามหลักเกณฑ์ที่ได้บัญญัติไว้ในพระราชบัญญัตินี้เท่านั้น ซึ่งมีสาระสำคัญ ดังต่อไปนี้

(8.1) ผู้ควบคุมข้อมูลส่วนบุคคลสามารถทำการเก็บรักษาข้อมูลเอาไว้ได้เพียงระยะเวลาที่กำหนดหรือเท่าที่จำเป็นตามวัตถุประสงค์ของการเก็บรวบรวม[274]และเมื่อพ้นกำหนดระยะเวลาหรือหมดความจำเป็นในการเก็บรวบรวม หรือเจ้าของข้อมูลส่วนบุคคลเพิกถอนความยินยอมแล้วนั้น ให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำลายข้อมูลนั้น หรือทำให้ข้อมูลนั้นไม่ปรากฏชื่อหรือสิ่งบอกลักษณะใดที่สามารถทำให้รู้ตัวเจ้าของข้อมูลส่วนบุคคลได้ภายใน 30 วัน นับแต่วันที่ครบกำหนดระยะเวลาหรือหมดความจำเป็นหรือได้รับแจ้งการเพิกถอนความยินยอม แล้วแต่กรณี[275]

---

[268] เรื่องเดียวกัน, มาตรา 42 (6).

[269] เรื่องเดียวกัน, มาตรา 47.

[270] เรื่องเดียวกัน, มาตรา 47 วรรค 2.

[271] เรื่องเดียวกัน, มาตรา 48 วรรค 1.

[272] เรื่องเดียวกัน, มาตรา 48 วรรค 2.

[273] เรื่องเดียวกัน, มาตรา 48 วรรค 3.

[274] เรื่องเดียวกัน, มาตรา 31 วรรคแรก.

[275] เรื่องเดียวกัน, มาตรา 31 วรรค 2.

เว้นแต่ กรณีที่มีความจำเป็นเพื่อประโยชน์ในการดำเนินการของผู้ควบคุมข้อมูลที่ต้องเก็บรวบรวมข้อมูลส่วนบุคคลไว้เพื่อเป็นสถิติหรือการศึกษาวิจัย ผู้ควบคุมข้อมูลส่วนบุคคลจะไม่ดำเนินการทำลายข้อมูลส่วนบุคคลนั้นก็ได้ แต่ต้องมีหนังสือแจ้งเจ้าของข้อมูลส่วนบุคคลนั้นเพื่อขอความยินยอมเป็นหนังสือ[276]

(8.2) ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีระบบรักษาความปลอดภัยให้แก่ข้อมูลส่วนบุคคลตามความเหมาะสม เพื่อป้องกันมิให้มีการนำข้อมูลส่วนบุคคลไปใช้ หรือเปิดเผยโดยไม่เหมาะสม หรือเป็นผลร้ายต่อเจ้าของข้อมูลส่วนบุคคล แต่หากเป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่อันมีลักษณะห้ามตามมาตรา 22 ให้ผู้ควบคุมข้อมูลต้องจัดให้มีระบบรักษาความปลอดภัยในระดับที่สูงขึ้นเพื่อป้องกันการสูญหาย ทำลาย ถูกสืบค้น หรือถูกเชื่อมโยง ใช้ เปิดเผย ทำสำเนา หรือเปลี่ยนแปลงโดยไม่มีสิทธิหรือมิชอบด้วยกฎหมาย ซึ่งอย่างน้อยต้องมีมาตรการดังต่อไปนี้[277]เช่น ห้ามมิให้ผู้ที่ไม่มีส่วนเกี่ยวข้องเข้าไปในสถานที่ที่ใช้เก็บรักษาข้อมูลส่วนบุคคล[278]มีมาตรการจำกัดบุคคลที่สามารถเรียกดูหรือใช้ซึ่งข้อมูลส่วนบุคคลนั้น[279]และมีการกำหนดรหัสผ่านเพื่อดูหรือใช้ข้อมูลอิเล็กทรอนิกส์นั้น เป็นต้น แต่ทั้งนี้ คณะกรรมการจะประกาศกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีระบบรักษาความปลอดภัยอื่นใดที่เหมาะสมให้แก่ข้อมูลส่วนบุคคลก็ได้[280]

(8.3) ในการแก้ไขเปลี่ยนแปลงข้อมูลส่วนบุคคล เจ้าของข้อมูลส่วนบุคคลต้องร้องขอเป็นหนังสือ[281]และให้ผู้ควบคุมข้อมูลที่มีหน้าที่ในการแก้ไขเปลี่ยนแปลงข้อมูลส่วนบุคคลที่อยู่ในความครอบครองให้มีความถูกต้อง ครบถ้วน และเป็นปัจจุบันตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ โดยอาจขอให้จัดส่งเอกสารที่เกี่ยวข้องเพื่อประกอบการพิจารณาแก้ไขก็ได้ ทั้งนี้ หากเป็นกรณีที่ต้องใช้วิธีการลบหรือทำลายเพื่อเก็บรวบรวมข้อมูลส่วนบุคคลดังกล่าวใหม่เพื่อความสะดวกหรือโดยเหตุอื่นที่จำเป็นก็ให้ใช้วิธีนั้นได้ แต่จะต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล[282]

---

[276] เรื่องเดียวกัน, มาตรา 31 วรรค 3.

[277] เรื่องเดียวกัน, มาตรา 32.

[278] เรื่องเดียวกัน, มาตรา 32 (1).

[279] เรื่องเดียวกัน, มาตรา 32 (2).

[280] เรื่องเดียวกัน, มาตรา 32 (3).

[281] เรื่องเดียวกัน, มาตรา 33.

[282] เรื่องเดียวกัน, มาตรา 33 วรรค 3.

(9) คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลได้มีการบัญญัติให้มีคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล[283]ซึ่งอำนาจหน้าที่ในการกำหนดนโยบาย มาตรการหรือแนวทางการดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามพระราชบัญญัตินี้และมีหน้าที่ให้คำปรึกษา กำหนดหลักเกณฑ์ และจัดทำรายงานหรือแต่งตั้งคณะอนุกรรมการเพื่อดำเนินการใดตามอำนาจแห่งพระราชบัญญัตินี้[284]

(10) บทกำหนดโทษ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลได้มีการบัญญัติถึงบทกำหนดโทษเอาไว้ 3 กรณี ดังมีสาระสำคัญ ดังนี้

(10.1) การลงโทษทางปกครอง ให้ผู้อำนวยการต้องมีการคำนึงถึงความร้ายแรงแห่งพฤติกรรมที่กระทำผิดและความเสียหายที่เกิดจากการกระทำนั้น[285]

(10.2) การลงโทษทางอาญา ผู้ใดที่ไม่ได้มาให้ถ้อยคำหรือส่งวัตถุ ตลอดจนเอกสารหรือพยานหลักฐานแก่คณะกรรมการตรวจสอบข้อมูลข่าวสารส่วนบุคคลหรือคณะอนุกรรมการตามต้องระวางโทษจำคุก หรือปรับ หรือทั้งจำทั้งปรับ[286]

(10.3) การลงโทษทางแพ่ง หากผู้ใดที่ได้รับโทษตามพระราชบัญญัตินี้เป็นนิติบุคคลให้กรรมการผู้จัดการ ผู้จัดการ หรือบุคคลใดซึ่งเป็นผู้รับผิดชอบในการดำเนินงานของนิติบุคคลนั้นต้องระวางโทษตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ เว้นแต่จะพิสูจน์ได้ว่าตนมิได้รู้เห็นหรือยินยอมในการกระทำความผิดของนิติบุคคลนั้น[287]

จากบทบัญญัติดังกล่าว จะเห็นได้ว่าร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลได้ขยายขอบเขตการบังคับใช้จากเฉพาะหน่วยงานราชการตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 ให้ครอบคลุมถึงทั้งภาครัฐและภาคเอกชนเป็นกรณีทั่วไป เว้นแต่หน่วยงานใดมีกฎหมายเฉพาะมาใช้บังคับอยู่แล้ว ซึ่งแสดงให้เห็นว่ากฎหมายฉบับนี้ให้ความสำคัญกับข้อมูลส่วนบุคคลตลอดจนมีการพัฒนากลไกในการบังคับใช้ให้ครอบคลุมมากกว่ากฎหมายฉบับเดิม

---

[283] เรื่องเดียวกัน, มาตรา 7.

[284] เรื่องเดียวกัน, มาตรา 11.

[285] เรื่องเดียวกัน, มาตรา 56.

[286] เรื่องเดียวกัน, มาตรา 60.

[287] เรื่องเดียวกัน, มาตรา 55.

แต่ทั้งนี้ เนื่องจากกฎหมายฉบับนี้ มีผลบังคับได้ทั้งกับภาครัฐซึ่งมีประโยชน์สาธารณะเป็นจุดมุ่งหมายสูงสุดในการดำเนินงาน และภาคเอกชนซึ่งมีผลตอบแทนหรือกำไรเป็นจุดหมายสูงสุดในการดำเนินงาน ดังนั้น กฎหมายฉบับนี้จะสามารถรักษาสมดุลในการบังคับใช้กฎหมายได้อย่างไร ซึ่งอาจต้องทำการศึกษาถึงผลกระทบให้ดีก่อนมีการนำพระราชบัญญัติฉบับนี้มาประกาศใช้ เพราะหากมีผลเสียอาจจะส่งกระทบในวงกว้างครอบคลุมหลายภาคส่วน แต่อย่างไรก็ดี การเร่งให้มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลมาบังคับใช้ก็เป็นสิ่งที่พึงปรารถนาเพื่อที่ประชาชนและผู้บริโภคจะได้รับความคุ้มครองในสิทธิส่วนบุคคลที่มีประสิทธิภาพมากยิ่งขึ้น

บทที่ 4
ศึกษาเปรียบเทียบมาตรการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐในประเทศสหรัฐอเมริกาและสหภาพยุโรป

4.1 การคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐในประเทศสหรัฐอเมริกา

ในประเทศสหรัฐอเมริกาเริ่มมีแนวความคิดในการนำมาตรการการคุ้มครองข้อมูลส่วนบุคคลมาใช้ภายหลังจากที่บทความวิชาการที่ชื่อ“The Right to Privacy” ของ Samuel D.Warren และ Louis D.Brandies ได้ถูกเผยแพร่ออกไปในปี ค.ศ. 1890 ซึ่งถือเป็นจุดเริ่มต้นของการสร้างกระแสในการพัฒนากฎหมายคุ้มครองข้อมูลส่วนบุคคลในสหรัฐอเมริกาให้ขยายขอบเขตครอบคลุมสิทธิต่าง ๆ ของมนุษย์มากขึ้นจากเดิมซึ่งเป็นเพียงสิทธิที่จะมีชีวิตอยู่จนกลายเป็นสิทธิในการดำรงชีวิตอย่างมีความสุข หรือสิทธิในการที่จะอยู่เพียงลำพัง(The right to be let alone) อันเป็นการขยายความหมายโดยรวมถึงการคุ้มครองทั้งในแบบรูปธรรมและนามธรรมตามที่ D. Warren และ Louis D. Brandies ระบุไว้ในหนังสือดังกล่าว

ทั้งนี้ เนื่องจากสภาพสังคม เศรษฐกิจ และวัฒนธรรมในประเทศสหรัฐอเมริกาซึ่งได้มีการเปลี่ยนแปลงและพัฒนาอยู่ตลอดเวลา กระทั่งได้มีการนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารงานและให้บริการกับประชาชนในรูปแบบของรัฐบาลอิเล็กทรอนิกส์ ทำให้ประชาชนชาวอเมริกัน(American)ซึ่งถือว่าเป็นผู้ที่อาศัยอยู่ในสังคมที่มีการติดต่อเชื่อมโยงทางระบบอินเตอร์เน็ตที่มีการพัฒนาถึงขีดสุดได้อย่างมีประสิทธิภาพ โดยสามารถเข้าถึงการให้บริการได้ตลอด 24 ชั่วโมงต่อวันและ 7 วันต่อสัปดาห์ และมากกว่า 60 เปอร์เซนต์ของผู้ใช้อินเตอร์เน็ตในสหรัฐอเมริกาได้มีการติดต่อกับเว็บไซต์หน่วยงานของรัฐ[1] ดังนั้น จะเห็นได้ว่ามาตรการคุ้มครองข้อมูลส่วนบุคคลมีความสำคัญอย่างมากในการให้ความคุ้มครองข้อมูลส่วนบุคคลของประชาชนหรือผู้บริโภคให้มีความปลอดภัย เพื่อสร้างความเชื่อมั่นให้แก่ประชาชนหรือผู้บริโภคในการให้ข้อมูลที่เป็นจริงในการทำธุรกรรมต่าง ๆ ซึ่งรวมถึงการทำธุรกรรมทางอิเล็กทรอนิกส์ของภาครัฐด้วย โดยในประเทศสหรัฐอเมริกาได้ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลเป็นอย่างมาก เนื่องจากรัฐบาลสหพันธรัฐแห่งสหรัฐอเมริกา(Federal Government of the United States)มีความจำเป็นที่จะต้องรวบรวมข้อมูลส่วนบุคคลในการบริหารจัดการเพื่อประโยชน์ของประชาชนซึ่งอาจกล่าวได้ว่า เริ่มเก็บรวบรวมข้อมูลส่วนบุคคลตั้งแต่การจัดเก็บภาษีเรื่อยไปจนถึงส่วนของการเก็บข้อมูลเพื่อใช้ในการเอาชนะสงครามการก่อการร้าย(Terrorism War)

---

[1] Executive Office of The President Office Of Management and Budget, **E-Government Strategy**[online], 2 June 2012. Available from http://www.usa.gov/Topics/Includees/reference/egov_strategy.pdf.

ด้วยเหตุดังกล่าว จึงนำมาซึ่งความเสี่ยงในเรื่องของความเป็นส่วนตัวที่อาจเกิดขึ้นจากการใช้ข้อมูล คุณภาพของข้อมูล ความปลอดภัยของข้อมูล และรวมถึงสิทธิของประชาชนในการตรวจสอบข้อมูลที่เกี่ยวข้องกับตนเอง รัฐบาลสหพันธรัฐแห่งสหรัฐอเมริกาจึงได้มีการใช้มาตรการคุ้มครองความเป็นส่วนตัวพร้อมกับการรวบรวมข้อมูล และใช้ข้อมูลโดยหน่วยงานของรัฐอย่างมีประสิทธิภาพ คือ การคำนึงถึงความเป็นส่วนตัวในระหว่างการพัฒนาโครงการเพื่อที่สิ่งเหล่านี้จะได้ถูกให้ความสำคัญและเตรียมพร้อมไว้ล่วงหน้าโดยเรียกกระบวนการนี้ว่า“ความเป็นส่วนตัวที่กำหนดได้เอง”(Privacy by Design)[2]เนื่องจากหลายหน่วยงานอาจพบปัญหาของความเป็นส่วนตัวภายหลังจากการนำระบบมาใช้ จึงเป็นการยากที่จะทำการแก้ไขข้อมูลหรือระบบเหล่านั้นให้ถูกต้องเหมาะสม ดังนั้น เพื่อความมั่นใจว่าความเป็นส่วนตัวจะได้รับการให้ความสำคัญบริษัทหลายแห่งและหน่วยงานของรัฐจึงมีการจัดตั้งตำแหน่งเจ้าหน้าที่ความเป็นส่วนตัว(Chief Privacy Officer Position)[3]ซึ่งเป็นตำแหน่งที่คอยทำหน้าที่ในการดูแลข้อมูลส่วนบุคคลและมีส่วนร่วมในทุกกระบวนการที่เกี่ยวข้องกับการรวบรวมข้อมูลส่วนบุคคล

อย่างไรก็ตาม ในช่วงแรกของการพัฒนากฎหมายคุ้มครองข้อมูลส่วนบุคคลในสหรัฐอเมริกายังไม่มีบทบัญญัติกฎหมายใดใช้บังคับกับข้อมูลส่วนบุคคลโดยเฉพาะ ซึ่งมีเพียงแต่พระราชบัญญัติเสรีภาพแห่งข้อมูลข่าวสาร(The Freedom of Information Act of 1967 : FOIA)ซึ่งเป็นกฎหมายที่บัญญัติถึงการให้สิทธิกับประชาชนในการเข้าถึงข้อมูลข่าวสารจากรัฐบาลแห่งสหพันธรัฐ ซึ่งมีผลบังคับใช้เมื่อปี ค.ศ. 1966 โดยพระราชบัญญัติเสรีภาพแห่งข้อมูลข่าวสาร(FOIA)ได้บัญญัติให้ประชาชนมีสิทธิที่จะทำการร้องเรียนต่อศาลเพื่อให้ได้มาซึ่งการเข้าถึงข้อมูลของหน่วยงานของสหพันธรัฐเว้นแต่ข้อมูลดังกล่าวถูกเก็บไว้มิให้เผยแพร่ ซึ่งจะเห็นได้ว่าเป็นเพียงสิทธิในการเข้าถึงข้อมูลข่าวสารของรัฐเท่านั้น มิใช่กฎหมายที่มีเจตนารมณ์ในการให้ความคุ้มครองสิทธิส่วนบุคคล

ด้วยเหตุกล่าว รัฐบาลสหพันธรัฐแห่งสหรัฐอเมริกา โดยกระทรวงความมั่นคงแห่งมาตุภูมิ(Department of Homeland Security : DHS)[4]ซึ่งเป็นหน่วยงานที่ทำหน้าที่ในการจัดหาตำแหน่งเจ้าหน้าที่ฝ่ายความเป็นส่วนตัว จึงมีความพยายามที่จะผลักดันให้แนวทางดังกล่าวให้ได้รับการยอมรับอย่างแพร่หลาย และเพื่อเป็นแบบอย่างแก่หน่วยงานอื่นเพื่อนำไปใช้ทั่วทั้งรัฐ นอกจากนี้กระทรวงความมั่นคงแห่งมาตุภูมิยังทำการเผยแพร่การประเมินผลกระทบของความเป็นส่วนตัว(Privacy Impact Assessments : PIAs)โดยกฎหมายคุ้มครองความเป็นส่วนตัวจะเป็นสิ่งที่สนับสนุนให้หน่วยงานของรัฐในประเทศสหรัฐอเมริกาทำการประเมินผลกระทบความเป็น

---

[2] James X. Dempsey, Paige Anderson & Ari Schwartz, **Privacy and E-Government**, A Report to the United Nations Department of Economic and Social Affairs as background for the World Public Sector Report : E-Government, 2.

[3] ibid, 3.

[4] United states of America, **Department of Homeland Security**[online], 24 May 2012. Available from http://www.dhs.gov/index.shtm.

ส่วนตัวในทุกครั้งที่มีข้อมูลข่าวสารใหม่เกิดขึ้น หรือเมื่อมีการเริ่มรวบรวมข้อมูลส่วนบุคคลขึ้น[5] ซึ่งต่อมาในปี ค.ศ.1974 รัฐสภาแห่งสหรัฐอเมริกาได้ผ่านร่างพระราชบัญญัติกฎหมายเกี่ยวกับความเป็นส่วนตัว “The Privacy Act of 1974” โดยกฎหมายดังกล่าวบัญญัติถึงการคุ้มครองความเป็นส่วนตัว ซึ่งประกาศใช้เพื่อเป็นการรวบรวมข้อมูลและการใช้ข้อมูลส่วนบุคคลโดยหน่วยงานของสหพันธรัฐ ซึ่งบุคคลใดที่เห็นว่าความเป็นส่วนตัวของตนเองถูกคุกคามโดยหน่วยงานของรัฐให้สามารถทำการฟ้องคดีต่อศาลได้

นอกจากนี้ ในการบริหารราชการแผ่นดินของประสหรัฐอเมริกา ได้มีการจัดตั้งสำนักงานบริหารของประธานาธิบดี(Executive Office of the President : EOP)[6]ซึ่งมีลักษณะการทำงานคล้ายคลึงกับสำนักนายกรัฐมนตรี[7]ของประเทศไทยและทำการมอบหมายให้สำนักงานการบริหารจัดการและงบประมาณ(Office of Management and Budget : OMB)[8]เป็นผู้รับผิดชอบในการพัฒนาและนำนโยบายตลอดจนโครงการต่างๆ ของประธานาธิบดีแห่งสหรัฐอเมริกามาบังคับใช้ภายใต้บทบัญญัติข้อ (v) แห่ง The Privacy Act of 1974 ซึ่งกำหนดให้สำนักงานการบริหารจัดการและงบประมาณ ทำหน้าที่ในการพัฒนากฎหมาย และต้องมีการเปิดโอกาสแก่ประชาชนในการแสดงความเห็น[9]เพื่อใช้ในการการกำหนดแนวทางข้อบังคับสำหรับหน่วยงานต่าง ๆ ที่จะนำ The Privacy Act มาบังคับใช้ โดยมีแนวการปฏิบัติในทิศทางที่สอดคล้องกัน[10]

4.1.1 The Privacy Act of 1974

พระราชบัญญัติกฎหมายเกี่ยวกับความเป็นส่วนตัวของสหรัฐอเมริกาได้รับการประกาศใช้ในปี ค.ศ. 1974 ทั้งนี้ เนื่องจากรัฐบาลสหพันธรัฐมีข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลอยู่เป็นจำนวนมาก เช่น หากบุคคลใดเคยทำงานในหน่วยงานของรัฐ หรือเคยลงชื่อเพื่อรับผลประโยชน์ใดจากหน่วยงานของรัฐ ทางหน่วยงานของรัฐบาลก็จะมีการบันทึกข้อมูลที่เกี่ยวข้องกับบุคคลดังกล่าวเก็บไว้ ดังนั้น จะเห็นได้ว่าไม่ว่าบุคคลใดจะมีนิติสัมพันธ์ในรูปแบบใด

---

[5] James X. Dempsey, Paige Anderson & Ari Schwartz, **Privacy and E-Government**, A Report to the United Nations Department of Economic and Social Affairs as background for the World Public Sector Report : E-Government, 3.

[6] **Executive Office of the President** [online], 4 June 2012. Available from http://www.whitehouse.gov/administration/eop.

[7] พระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม พ.ศ. 2545, มาตรา 5 (1).

[8] Office of Management and Budget, **Office of Management and Budget**[online], 4 June 2012. Available from http://www.whitehouse.gov/omb.

[9] Public Law 93-579, The Privacy Acts of 1974, (v) (1).

[10] ibid, (v) (2).

กับหน่วยงานของรัฐไม่ว่าที่ไหนหรือเวลาใด หน่วยงานของรัฐก็จะมีข้อมูลทุกอย่างที่เกี่ยวข้องกับบุคคลดังกล่าว ดังนั้น The Privacy Act ซึ่งได้ผ่านสภาครองเกรสเมื่อปี ค.ศ.1974 จึงได้ถูกบัญญัติขึ้นเพื่อใช้ในการควบคุมการจัดเก็บข้อมูล การรวบรวมข้อมูลและการใช้ข้อมูลส่วนบุคคลของรัฐบาลสหพันธรัฐ ซึ่งมีประเด็นที่สำคัญ คือ สิทธิที่จะทำการตรวจสอบข้อมูลส่วนบุคคลของตนเองโดยมิได้ขัดกับข้อยกเว้น และสิทธิที่จะแก้ไขบันทึกข้อมูลที่ไม่ถูกต้อง ไม่เกี่ยวข้อง หรือไม่เป็นปัจจุบัน ตลอดจนสิทธิที่จะฟ้องร้องหน่วยงานของรัฐที่กระทำความผิดต่อ The Privacy Act[11]

ซึ่งหากบุคคลใดต้องการทราบว่าหน่วยงานของรัฐมีข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตนเองอยู่หรือไม่สามารถแจ้งความประสงค์ไปยังเจ้าหน้าที่ในหน่วยงานที่เก็บรักษาข้อมูลพร้อมให้ข้อมูลเบื้องต้นสำหรับตรวจสอบว่ามีข้อมูลส่วนบุคคลที่เกี่ยวข้องอยู่หรือไม่ ซึ่งทางหน่วยงานจะต้องทำการรายงานถึงสถานภาพการมีอยู่ของข้อมูลส่วนบุคคลที่เกี่ยวข้องในระบบทั้งหมดให้กับสำนักงานทะเบียนแห่งรัฐ(The Office of the Federal Register)และหน่วยงานจะต้องจัดให้มีโปรแกรมทางอินเตอร์เน็ตในแต่ละส่วนของหน่วยงานที่จะสามารถเชื่อมโยงข้อมูลระหว่างกันได้ โดยในการบังคับใช้กฎหมายในส่วนที่ให้ความคุ้มครองเกี่ยวกับความเป็นส่วนตัวของประเทศสหรัฐอเมริกาในส่วนของ The Privacy Act มีสาระสำคัญ ดังนี้

(1) ขอบเขตการบังคับใช้พระราชบัญญัติฉบับนี้

The Privacy Act จะบังคับใช้กับการบันทึกข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมโดยหน่วยงานฝ่ายบริหารของรัฐบาลสหพันธรัฐ และจะบังคับใช้กับข้อมูลในกรณีที่อยู่ใน “ระบบบันทึกข้อมูล” เท่านั้น ซึ่งหมายความว่า ข้อมูลจะถูกดึงเข้ามาจากชื่อของบุคคล หมายเลขประกันสังคม(Social Security Number) หรือข้อมูลระบุตัวตนอื่น ๆ อีกด้วย

(2) นิยามศัพท์ที่สำคัญ

“บุคคล” หมายถึง ประชาชนของประเทศสหรัฐอเมริกา หรือคนต่างด้าวที่ได้รับการอนุญาตให้เข้ามาพำนักในอาณาจักรอย่างถูกต้องตามกฎหมาย[12]

“บันทึก” หมายถึง สิ่งใดๆ การเก็บรวบรวม หรือการจัดหมวดหมู่ของข้อมูลข่าวสารเกี่ยวกับบุคคลที่ได้เก็บรักษาไว้โดยหน่วยงาน เช่น การศึกษา ประวัติทางการแพทย์ หรือการจ้างงาน ที่ซึ่งมีชื่อของบุคคล หรือหมายเลขระบุตัวตน สัญลักษณ์ รวมถึง สิ่งที่ระบุตัวตนอื่น ๆ ที่กำหนดไว้โดยบุคคลนั้น เช่น ลายนิ้วมือ หรือบันทึกภาพและเสียง[13]

---

[11] United States Government Printing Office, **About Privacy Act Issuances**[online]. 3 June 2012. Available from http://www.gpo.gov/help/index.html#about_privacy_act_issuances.htm.

[12] ibid, (a) (2).

[13] ibid, (a) (2).

(3) การเก็บรวบรวมข้อมูล

แม้ว่า The Privacy Act of 1974 จะไม่มีการกำหนดหมวดข้อกฎหมายที่เกี่ยวข้องกับการเก็บรวบรวมข้อมูลส่วนบุคคลไว้เป็นการเฉพาะ แต่ได้มีการบัญญัติเรื่องการเก็บรวบรวมข้อมูลส่วนบุคคลไว้ในข้อ (e) ซึ่งมีสาระสำคัญ คือ การเก็บรวบข้อมูลจะต้องเป็นการเก็บข้อมูลที่สามารถนำไปใช้ได้เพื่อเป็นประโยชน์สูงสุดโดยตรงจากเจ้าของข้อมูลส่วนบุคคลนั้น[14]และในการเก็บข้อมูลส่วนบุคคลหน่วยงานจะต้องมีการแจ้งถึงข้อกำหนดลงในแบบเอกสาร(form)[15]ซึ่งในแบบเอกสารดังกล่าว ได้ระบุถึงที่มาของอำนาจในการทำการเก็บข้อมูลว่ามาจากกฎหมายหรือมาจากคำสั่งของประธานาธิบดี[16]ตลอดจนวัตถุประสงค์ในการใช้ข้อมูล[17]ลักษณะของการใช้ข้อมูลเป็นประจำ[18]และผลกระทบต่อเจ้าของข้อมูลจากการที่ไม่ยินยอมให้ข้อมูลที่ร้องขอ[19]ทั้งนี้ เป็นไปเพื่อการขอให้มีการแสดงความยินยอมในการเปิดเผยข้อมูลว่าเจ้าของข้อมูลให้เปิดเผยข้อมูลโดยสมัครใจหรือโดยคำสั่ง[20]

(4) การเปิดเผยข้อมูลและข้อยกเว้นการเปิดเผยข้อมูล[21]

The Privacy Act of 1974 บัญญัติให้หน่วยงานของรัฐ ไม่อาจเปิดเผยข้อมูลส่วนบุคคลใดที่ถูกเก็บไว้ในระบบการบันทึกข้อมูลให้กับบุคคลหรือหน่วยงานอื่นใด เว้นแต่ มีคำร้องขอเป็นลายลักษณ์อักษร หรือเป็นการที่เจ้าของข้อมูลส่วนบุคคลให้ความยินยอมที่เป็นลายลักษณ์อักษรไว้ล่วงหน้า เว้นแต่ว่าการเปิดเผยข้อมูลนั้นจะเป็น กรณีดังต่อไปนี้[22]

(4.1) เป็นการเปิดเผยต่อเจ้าหน้าที่และพนักงานของหน่วยงานที่รักษาบันทึกข้อมูลหรือผู้ที่มีความจำเป็นในบันทึกข้อมูลนั้นเพื่อการปฏิบัติงานตามหน้าที่[23]

(4.2) เป็นการเปิดเผยในกรณีมีความจำเป็นตามที่กฎหมายกำหนด[24]

(4.3) เป็นการเปิดเผยเพื่อการใช้ข้อมูลส่วนบุคคลในวัตถุประสงค์ใดที่สอดคล้องกับวัตถุประสงค์ที่ได้เก็บรวบรวมข้อมูลมา[25]

---

[14] ibid, (e) (2).

[15] ibid, (e) (3).

[16] ibid, (e) (3) (a).

[17] ibid, (e) (3) (b).

[18] ibid, (e) (3) (c).

[19] ibid, (e) (3) (d).

[20] ibid, (e) (3) (a).

[21] ibid, (b).

[22] ibid, (b) paragraph 1.

[23] ibid, (b) (1).

[24] ibid, (b) (2).

(4.4) เป็นการเปิดเผยแก่สำนักงานสำมะโนประชากรเพื่อวัตถุประสงค์ในการวางแผนหรือการสำรวจสำมะโนประชากร หรือทำกิจกรรมอื่นใดตามที่กฎหมายกำหนด[26]

(4.5) เป็นการเปิดเผยแก่ผู้รับข้อมูลที่ได้ให้การรับรองที่เป็นลายลักษณ์อักษรแก่หน่วยงานว่า บันทึกนี้จะนำไปใช้ในทางการวิจัยหรือการรายงานทางสถิติเท่านั้น และบันทึกดังกล่าวจะถูกส่งผ่านไปในรูปแบบที่ไม่สามารุระบุตัวตนส่วนบุคคลได้[27]

(4.6) เป็นการเปิดเผยแก่องค์การบริหารจดหมายเหตุและบันทึกแห่งชาติว่าเป็นบันทึกที่มีข้อมูลทางประวัติศาสตร์หรือควรค่าแก่การสงวนรักษาไว้โดยรัฐบาล[28]

(4.7) เป็นการเปิดเผยแก่หน่วยงานอื่นในขอบข่ายอำนาจของรัฐบาลเพื่อการบังคับใช้กฎหมายทางแพ่งและอาญาที่กฎหมายได้ให้อำนาจไว้ และให้หัวหน้าของหน่วยงานที่ขอบันทึกข้อมูลได้ทำการร้องขอเป็นลายลักษณ์อักษรแก่หน่วยงานที่เก็บรักษาบันทึกข้อมูลและให้บันทึกข้อมูลได้โดยเฉพาะในส่วนที่ต้องการหรือกฎหมายกำหนดไว้[29]

(4.8) เป็นการเปิดเผยแก่บุคคลในกรณีมีความจำเป็นตามสถานการณ์บังคับที่ส่งผลกระทบต่อสุขภาพหรือความปลอดภัยของบุคคล หากการเปิดเผยข้อมูลนั้นได้ถูกส่งผ่านไปยังภูมิลำเนาสุดท้ายที่ปรากฏของบุคคลนั้น[30]

(4.9) เป็นการเปิดเผยต่อรัฐสภา หรือเพื่อขยายความในประเด็นที่อยู่ในขอบอำนาจตามกฎหมายแก่คณะกรรมาธิการ หรือคณะอนุกรรมการตามที่กฎหมายกำหนด[31]

(4.10) เป็นการเปิดเผยแก่ผู้อำนวยการตรวจสอบด้านการเงินและด้านการบัญชีและผู้มีอำนาจกระทำแทน ในกรณีที่เกี่ยวกับการปฏิบัติงานตามหน้าที่ของสำนักงานตรวจเงินแผ่นดิน[32]

(4.11) เป็นการเปิดเผยโดยปฏิบัติตามตามคำสั่งของศาล[33]

(4.12) เป็นการเปิดเผยแก่ผู้ใช้ข้อมูลที่ได้รายงานความจำเป็นในการขอใช้ข้อมูลต่อหน่วยงานตามที่กฎหมายกำหนด[34]

---

[25] ibid, (b) (3).

[26] ibid, (b) (4).

[27] ibid, (b) (5).

[28] ibid, (b) (6).

[29] ibid, (b) (7).

[30] ibid, (b) (8).

[31] ibid, (b) (9).

[32] ibid, (b) (10).

[33] ibid, (b) (11).

[34] .ibid, (b) (12).

(5) การเข้าถึงบันทึกข้อมูล[35]

ตามบทบัญญัติแห่ง The Privacy Act of 1974 ได้กำหนดให้แต่ละหน่วยงานที่เก็บรักษาบันทึกข้อมูลส่วนบุคคลจะต้องกำหนดหลักเกณฑ์ในการเข้าถึงบันทึกข้อมูล เมื่อผู้ที่เกี่ยวข้องกับบันทึกข้อมูลได้ร้องขอเพื่อเข้าถึงบันทึกข้อมูลที่ถูกเก็บไว้ในระบบ โดยหน่วยงานจะต้องอนุญาตให้บุคคลผู้ที่ร้องขอได้ดูบันทึกข้อมูลและทำสำเนาไว้ทั้งหมดหรือแต่บางส่วน เว้นแต่ว่า หน่วยงานดังกล่าวต้องการให้บุคคลเขียนข้อความเป็นลายลักษณ์อักษรเพื่อขออนุญาตให้มีการสนทนาเกี่ยวกับบันทึกของบุคคลนั้นก็ได้[36]นอกจากนี้ หน่วยงานที่ทำการจัดเก็บบันทึกข้อมูลจะต้องมีมาตรการความคุ้มครองรายชื่อและที่อยู่ของผู้ที่ได้รับข้อมูล ซึ่งชื่อและที่อยู่ของบุคคลจะต้องไม่ถูกนำไปขายหรือให้เช่าโดยหน่วยงานอื่น เว้นเสียแต่ว่าการกระทำดังกล่าวได้รับอนุญาตตามกฎหมายแล้ว ทั้งนี้ ข้อกำหนดดังกล่าวจะไม่ถูกตีความรวมถึงบันทึกข้อมูลที่ใช้เพื่อการปิดกั้นข้อมูลที่จะต้องถูกเปิดเผยต่อสู่สาธารณะชน[37]

(6) การขอแก้ไขข้อมูล

ตามบทบัญญัติแห่ง The Privacy Act of 1974 ได้กำหนดให้แต่ละหน่วยงานต้องกำหนดให้ผู้ที่เกี่ยวข้องกับบันทึกข้อมูลส่วนบุคลได้มีโอกาสการแก้บันทึกข้อมูลที่ไม่สมบูรณ์ หรือไม่เป็นปัจจุบัน ซึ่งอาจแบ่งการแก้ไขตามพระราชบัญญัติฉบับนี้ ออกเป็น 2 กรณี ได้แก่

(6.1) การแก้ไขกรณีที่มีบุคคลได้ร้องขอให้หน่วยงานทำการแก้ไขบันทึกข้อมูลที่เกี่ยวข้องกับบุคลดังกล่าว ให้ทำการร้องขอเป็นลายลักษณ์อักษร และให้หน่วยงานดังกล่าวทำการแก้ไขบันทึกข้อมูลให้ถูกต้องภายใน 10 วันทำการ นับหลังจากวันที่ได้รับคำร้อง[38]

(6.2) การแก้ไขกรณีที่หน่วยงานทราบถึงความไม่ถูกต้อง ไม่เป็นปัจจุบัน หรือไม่สมบูรณ์ของบันทึกข้อมูลด้วยตนเอง ซึ่งหน่วยอาจงานแก้ไขบันทึกข้อมูลได้ทันที[39]

ในกรณีที่หน่วยงานไม่รับแก้ไขบันทึกข้อมูลใด ต้องทำการแจ้งให้ผู้ร้องขอทราบถึงการปฏิเสธแก้ไขข้อมูล พร้อมระบุถึงเหตุผลในการปฏิเสธตลอดจนเจ้าหน้าที่และหน่วยงานที่เกี่ยวข้องในการปฏิเสธคำขอแก้ไขข้อมูลดังกล่าวด้วย[40]

และในกรณีที่หน่วยงานทำการปฏิเสธการแก้ไขบันทึกข้อมูลและได้ทำการชี้แจงตามที่กฎหมายกำหนดแล้วนั้น หากผู้ร้องขอไม่เห็นด้วยกับการได้รับปฏิเสธการแก้ไขบันทึกข้อมูลสามารถยื่นคำร้องขอดูการปฏิเสธนั้นได้ภายใน 30 วันทำการ นับจากวันที่ยื่นคำร้องนั้น

---

[35].ibid, (d).

[36].ibid, (d) (1).

[37].ibid, (n).

[38].ibid, (d) (2) (A).

[39].ibid, (d) (2) (B).

[40].ibid, (d) (2) (B) (ii).

และกฎหมายได้กำหนดให้เจ้าหน้าที่ต้องทำการทบทวนและลงความเห็นอีกครั้งซึ่งภายหลังจากได้ทบทวนคำสั่งอีกครั้งหนึ่งแล้ว หากเจ้าหน้าที่ยังคงยืนยันการปฏิเสธที่จะให้แก้ไขบันทึกข้อมูลตามเดิมให้เจ้าหน้าที่อนุญาตให้ผู้ร้องขอสามารถยื่นคำร้องกับหน่วยงานโดยชี้แจงให้ชัดเจนถึงเหตุผลขอการไม่เห็นด้วยกับการปฏิเสธ[41]

แต่ทั้งนี้ หากหน่วยงานจะทำการเปิดเผยบันทึกข้อมูลใดซึ่งเจ้าหน้าได้ที่รายงานว่าบันทึกข้อมูลดังกล่าว เคยมีผู้ยื่นคำร้องขอแก้ไขบันทึกข้อมูลและหน่วยงานได้มีการปฏิเสธการขอแก้ไขบันทึกข้อมูลนั้น ให้หน่วยงานบันทึกข้อความอย่างชัดเจนลงในส่วนใดของบันทึกข้อมูลที่มีการพิพาท และให้สำเนาของคำร้องที่ชัดเจนถึงเหตุผลของหน่วยงานที่ไม่ทำการแก้ไขที่ได้ร้องขอไปแก่บุคคลหรือหน่วยงานอื่นที่ซึ่งบันทึกข้อมูลพิพาทได้ถูกเปิดเผย[42]

(7) ข้อกำหนดและมาตรการคุ้มครองข้อมูลส่วนบุคล

The Privacy Act of 1974 ได้กำหนดให้แต่ละหน่วยงานที่มีการเก็บรักษาระบบบันทึกข้อมูลส่วนบุคคลจะต้องทำการประกาศกฎระเบียบที่สอดคล้องกันกับกฎหมายฉบับนี้ และต้องมีการกำหนดหลักเกณฑ์ให้บุคคลสามารถทำการยื่นคำร้องเพื่อขอตรวจสอบข้อมูลส่วนบุคคลที่เกี่ยวข้องได้[43]ตลอดจนให้หน่วยงานต้องออกมาตรการในการระบุตัวตนของผู้ร้องขอข้อมูลตามความเหมาะสม ก่อนที่หน่วยงานจะอนุญาตให้ผู้ร้องขอข้อมูลสามารถเข้าถึงบันทึกข้อมูลดังกล่าวได้[44]และหากการขอเข้าถึงบันทึกข้อมูลนั้นเป็นข้อมูลทางการแพทย์หรือทางจิตวิทยาที่เกี่ยวข้องกับบุคคลนั้น ให้หน่วยงานที่จัดเก็บรวบรวมข้อมูลนั้นอาจมีการกำหนดมาตรการที่เป็นขั้นตอนพิเศษเพิ่มเติมก็ได้[45]

ทั้งนี้ ในกรณีที่บุคคลร้องขอให้มีการดำเนินการใดเกี่ยวกับข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตนและหน่วยงานดังกล่าวได้ทำการปฏิเสธการร้องขอ หรืออาจเป็นกรณีที่หน่วยงานได้ทำการตัดสินใจใดเพื่อดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลที่เกี่ยวข้อง ซึ่งส่งผลให้เกิดผลกระทบแก่ผู้ร้องขอในทางลบ ให้หน่วยงานดังกล่าวกำหนดขั้นตอนสำหรับตรวจดูคำร้องจากผู้ร้องขอแก้ไขบันทึกข้อมูล หรือข้อมูลที่เกี่ยวข้องการตัดสินใจที่มีผลกระทบในทางลบกับผู้ร้องขอเพื่อที่จะให้ยื่นอุทธรณ์ต่อหน่วยงาน ตลอดจนอาจมีการกำหนดมาตรการใดเพิ่มเติมที่มีความจำเป็นสำหรับบุคคลเพื่อที่จะได้ใช้สิทธิของตนอย่างเต็มที่[46]ซึ่งในการดำเนินการดังกล่าวข้างต้น หน่วยงานอาจกำหนดให้มีค่าใช้จ่ายในการทำสำเนาข้อมูลได้ แต่ไม่รวมถึงค่าใช้จ่ายใน

---

[41] ibid, (d) (3) (B).

[42] ibid, (d) (4) (B).

[43] ibid, (f) (1).

[44] ibid, (f) (2).

[45] ibid, (f) (3).

[46] ibid, (f) (4).

การค้นหาหรือตรวจดูบันทึกข้อมูล[47]และให้หน่วยงานต้องทำการรวบรวมกฎระเบียบที่เกี่ยวข้องกับพระราชบัญญัตินี้ ให้สำนักงานทะเบียนแห่งสหพันธรัฐทำการรวบรวมทุก 2 ปีและเผยแพร่กฎระเบียบที่นั้นตามลักษณะที่กฎหมายกำหนด โดยให้ประชาชนเข้าถึงได้ในราคาที่ต่ำ[48]

อนึ่ง การเผยแพร่กฎระเบียบหรือการปรับปรุงประกาศที่มีอยู่ต้องดำเนินการประกาศลงในทะเบียนหลักของสหพันธรัฐ ซึ่งจะต้องมีข้อมูลดังนี้ ได้แก่[49]ชื่อและตำแหน่งของบุคคลที่บันทึกข้อมูลไว้[50]ประเภทของบันทึกข้อมูล[51]และแหล่งข้อมูล[52]วัตถุประสงค์และลักษณะการใช้ประจำของบันทึกข้อมูล[53]ข้อปฏิบัติของหน่วยงานเกี่ยวกับการจัดการบันทึกข้อมูล[54]ตำแหน่งและที่อยู่ที่ทำงานของเจ้าหน้าที่ผู้รับผิดชอบ[55]ขั้นตอนในการได้รับแจ้งตามคำร้องขอในกรณีที่ระบบบันทึกข้อมูลมีข้อมูลที่เกี่ยวกับบุคคลนั้น[56]ตลอดจนขั้นตอนของหน่วยงานที่ซึ่งบุคคลสามารถได้รับแจ้งตามคำร้องขอถึงวิธีการที่จะเข้าถึงข้อมูลที่เกี่ยวข้องและวิธีที่บุคคลนั้นที่จะสามารถคัดค้านเนื้อหาในบันทึกข้อมูลนั้นได้[57]

นอกจากนี้ มาตรการดังกล่าวข้างต้นแล้ว พระราชบัญญัติฉบับนี้ยังกำหนดให้หน่วยงานต้องทำการรักษาบันทึกข้อมูลทั้งหมด ให้มีความถูกต้อง เป็นปัจจุบัน และมีความสมบูรณ์ตามความจำเป็นและเหมาะสมเพื่อรับรองความชอบธรรมของบุคคลในการตัดสินใจใดเกี่ยวกับบันทึกข้อมูลที่เกี่ยวข้องกับตน[58]และก่อนที่จะเผยแพร่บันทึกข้อมูลใดที่เกี่ยวกับบุคคลหนึ่งแก่บุคคลใดนอกเหนือจากหน่วยงานนั้น ให้ทำการรับรองก่อนว่าบันทึกข้อมูลนั้นถูกต้องสมบูรณ์เป็นปัจจุบัน และเกี่ยวข้องกับวัตถุประสงค์ของหน่วยงาน[59]

ทั้งนี้ หน่วยงานจะต้องจัดตั้งกฎระเบียบในการดำเนินงานสำหรับบุคคลทั้งที่เกี่ยวข้องในการปฏิบัติงานและที่เกี่ยวการพัฒนาระบบบันทึกข้อมูล และมีบทลงโทษสำหรับการไม่ปฏิบัติตามกฎระเบียบ[60]ตลอดจนต้องมีมาตรการคุ้มครองทางการบริหารที่เหมาะสมเพื่อรับรองความ

---

[47] ibid, (f) (5).

[48] ibid, (f) paragraph 2.

[49] ibid, (e) (4).

[50] ibid, (e) (4) (a).

[51] ibid, (e) (4) (b).

[52] ibid, (e) (4) (j).

[53] ibid, (e) (4) (c).

[54] ibid, (e) (4) (d).

[55] ibid, (e) (4) (e).

[56] ibid, (e) (4) (f).

[57] ibid, (e) (4) (i).

[58] ibid, (e) (5).

[59] ibid, (e) (6).

[60] ibid, (e) (9).

ปลอดภัยและการรักษาความลับของบันทึกข้อมูลและเพื่อป้องกันข้อผิดพลาดและความเสี่ยงที่อาจเกิดขึ้นต่อความปลอดภัยที่อาจส่งผลผลเสียที่รุนแรงต่อบุคคลที่ข้อมูลนั้นมีอยู่[61]

ทั้งนี้ ในกรณีที่เป็นการเผยแพร่บันทึกข้อมูลซึ่งได้ใช้เป็นประจำ ให้หน่วยงานต้องทำการประกาศลงในทะเบียนหลักของสหพันธรัฐ(The Federal Register Notice)ถึงการใช้บันทึกข้อมูลอย่างน้อย 30 วันก่อนการเผยแพร่ข้อมูล และให้โอกาสแก่บุคคลเพื่อส่งข้อโต้แย้งให้กับหน่วยงาน[62]และถ้าหน่วยงานดังกล่าวเป็นหน่วยงานที่เป็นผู้รับข้อมูลหรือหน่วยงานที่เป็นแหล่งข้อมูลในโปรแกรมจับคู่ข้อมูลกับหน่วยงานที่มิใช่สหพันธรัฐ ให้หน่วยงานนั้นทำการประกาศลงในทะเบียนหลักของสหพันธรัฐอย่างน้อย 30 วันก่อนการทำโปรแกรมดังกล่าว[63]

(8) ข้อยกเว้นในการไม่ใช้พระราชบัญญัติฉบับนี้

The Privacy Act of 1974 ได้บัญญัติข้อยกเว้นในการไม่นำพระราชบัญญัติฉบับนี้มาใช้บังคับบันทึกข้อมูลส่วนบุคคล ซึ่งอาจแบ่งได้เป็น 2 กรณี ดังต่อไปนี้

(8.1) ข้อยกเว้นทั่วไป[64]

ข้อยกเว้นกรณีทั่วไป หมายถึง ข้อมูลส่วนบุคคลนั้นได้ถูกเก็บรักษาโดยหน่วยสืบราชการลับกลางแห่งสหรัฐอเมริกา(Central Intelligence Agency : CIA)หรือได้ถูกเก็บรักษาโดยหน่วยงานของรัฐที่เกี่ยวข้องกับการบังคับใช้กฎหมายอาญา และการดำเนินการตามกระบวนของศาล เช่น กรมราชทัณฑ์ กรมคุมประพฤติ การอภัยโทษ หรือผู้มีอำนาจอภัยโทษภายใต้มาตรการที่เหมาะสม เป็นต้น

(8.2) ข้อยกเว้นเฉพาะ[65]

The Privacy Act of 1974 ได้บัญญัติเรื่องของการกำหนดข้อยกเว้นไว้เป็นการเฉพาะ โดยให้เป็นอำนาจของหัวหน้าหน่วยงานผู้เก็บรักษาบันทึกข้อมูลส่วนบุคคลซึ่งอาจประกาศใช้กฎระเบียบที่สอดคล้องกับกฎหมายฉบับนี้ โดยกำหนดเป็นให้ข้อยกเว้นโดยเฉพาะได้ในกรณีดังต่อไปนี้

(ก) บันทึกข้อมูลนั้น[66]เป็นการเปิดเผยต่อเจ้าหน้าที่และพนักงานของหน่วยงานที่รักษาบันทึกข้อมูล หรือผู้ที่มีความจำเป็นเพื่อการทำงานตามหน้าที่[67]

---

[61] ibid, (e) (10).

[62] ibid, (e) (11).

[63] ibid, (e) (12).

[64] ibid, (j).

[65] ibid, (k).

[66] ibid, (k) (1)

[67] ibid, (b) (1).

(ข) เป็นบันทึกข้อมูลที่มีลักษณะเป็นข้อเท็จจริงทางการสืบสวนที่เกี่ยวข้องกับวัตถุประสงค์ในการบังคับใช้กฎหมาย[68]

(ค) เป็นบันทึกข้อมูลที่ได้ถูกเก็บไว้เพื่อเชื่อมโยงกับมาตรการคุ้มครองแก่ประธานาธิบดีแห่งสหรัฐอเมริกา หรือการให้บริการบุคคลอื่นตามที่กฎหมายกำหนด[69]

(ง) เป็นบันทึกข้อมูลที่ถูกบังคับใช้โดยกฎหมายเพื่อใช้ในทางสถิติ[70]

(จ) เป็นบันทึกข้อมูลที่เป็นข้อเท็จจริงทางการสืบสวนตามวัตถุประสงค์ของการกำหนดคุณสมบัติ สำหรับการว่าจ้างงานของสหพันธรัฐ[71]หรือเพื่อใช้ตรวจสอบคุณสมบัติส่วนบุคคลสำหรับการแต่งตั้งหรือการเลื่อนขั้นในการบริการของสหพันธรัฐ[72]

(9) การเยียวยาทางแพ่ง[73]

ตามบทบัญญัติแห่ง The Privacy Act ได้มีกำหนดให้บุคคลผู้ได้รับความเสียหายจากการเปิดเผยบันทึกข้อมูลได้รับการเยียวยาทางแพ่งไว้ โดยสามารถทำการฟ้องร้องได้ภายใน 2 ปี หลังจากที่พบการเปิดเผยบันทึกข้อมูล แต่ไม่อนุญาตให้มีการฟ้องเรียกค่าเสียหายทางแพ่งซึ่งเป็นความเสียหายที่เกิดขึ้นจากการเปิดเผยบันทึกข้อมูลก่อนวันที่ 27 กันยายน ค.ศ. 1975[74] ซึ่งอาจแบ่งกรณีการเรียกร้องการเยียวยาทางแพ่งได้เป็น 4 กรณี ดังต่อไปนี้

(9.1) กรณีที่หน่วยงานมีการตัดสินใจเกี่ยวกับ[75]การอนุญาตให้บุคคลที่ไม่เห็นด้วยในการปฏิเสธของหน่วยงานในการแก้ไขบันทึกข้อมูลสามารถยื่นคำร้องที่จะขอดูการปฏิเสธ[76] และไม่แก้ไขบันทึกข้อมูลส่วนตัวของบุคคลตามคำร้องขอ หรือล้มเหลวที่จะทำการตรวจดูความสอดคล้องกันของบันทึกข้อมูล ซึ่งหากมีการดำเนินคดีทางแพ่งศาลอาจสั่งให้หน่วยงานแก้ไขบันทึกข้อมูลของบุคคลโดยสอดคล้องกับคำร้องขอของบุคคลนั้นหรือในทางอื่นใดที่ศาลสั่ง ในกรณีนี้ ศาลจะกำหนดวิธีใหม่อีกครั้ง[77]

---

[68] ibid, (k) (2).

[69] ibid, (k) (3).

[70] ibid, (k) (4).

[71] ibid, (k) (5).

[72] ibid, (k) (6).

[73] ibid, (g).

[74] ibid, (g) (5).

[75] ibid, (g) (1).

[76] ibid, (d) (3).

[77] ibid, (g) (2) (A).

(9.2) กรณีที่หน่วยงานได้ปฏิเสธที่จะปฏิบัติตามคำร้องขอของบุคคล[78]โดยผู้มีสิทธิซึ่งได้มีการร้องขอเพื่อเข้าถึงบันทึกข้อมูลที่ถูกเก็บไว้ในระบบซึ่งหน่วยงานจะต้องอนุญาตให้บุคคลผู้ที่ร้องขอได้ดูบันทึกข้อมูลและทำสำเนาไว้ทั้งหมดหรือแต่บางส่วน[79]และหากมีการดำเนินคดีทางแพ่งศ าลอาจสั่งห้ามมิให้หน่วยงานทำการปิดกั้นบันทึกข้อมูลต่าง ๆ ได้[80]

(9.3) กรณีที่หน่วยงานล้มเหลวที่จะเก็บรักษาบันทึกข้อมูลใดที่เกี่ยวกับความถูกต้องความเป็นปัจจุบันและความสมบูรณ์ของข้อมูล ซึ่งผลที่ตามมาจากการตัดสินใจเป็นไปในทางลบกับบุคคลนั้น[81]และหากมีการดำเนินคดีทางแพ่ง ศาลอาจกำหนดให้หน่วยงานที่กระทำไปโดยเจตนา ต้องมีความรับผิดทางแพ่งตามกฎหมายต่อบุคคลที่เสียหายได้[82]

(9.4) กรณีที่หน่วยงานล้มเหลวที่จะปฏิบัติตามข้อกำหนดของการเยียวยาทางแพ่งหรือกฎใดที่ประกาศไว้ในทางที่จะเป็นผลในทางลบต่อบุคคลนั้น บุคคลที่ได้รับผลในทางลบอาจฟ้องร้องทางแพ่งต่อศาลชั้นต้นได้[83]และหากมีการดำเนินคดีทางแพ่ง ศาลอาจกำหนดให้หน่วยงานที่กระทำไปโดยเจตนา ต้องมีความรับผิดทางแพ่งตามกฎหมายต่อบุคคลที่เสียหายได้[84]

(10) บทกำหนดโทษ[85]

(10.1) เจ้าหน้าที่ของหน่วยงานของรัฐใด หรือผู้ซึ่งโดยอาศัยอำนาจตามตำแหน่งหน้าที่หรืออำนาจตามกฎหมาย ในการครอบครองหรือเข้าถึงข้อมูลส่วนบุคคลของหน่วยงานของรัฐ ซึ่งได้เปิดเผยข้อมูลส่วนบุคคลที่ต้องห้ามเปิดเผยโดยทุจริต หรือไม่เหตุสมควร ถือว่าเป็นการกระทำความผิดลหุโทษ และมีโทษปรับไม่เกิน 5,000 ดอลลาร์สหรัฐอเมริกา[86]

(10.2) เจ้าหน้าที่ของหน่วยงานของรัฐใดที่เจตนาที่จะเก็บรักษาระบบบันทึกข้อมูลโดยปราศจากข้อกำหนดที่ประกาศไว้ ถือว่าเป็นการกระทำความผิดลหุโทษ และมีโทษปรับไม่เกิน 5,000 ดอลลาร์สหรัฐอเมริกา[87]

---

[78] ibid, (g) (2).

[79] ibid, (d) (1).

[80] ibid, (g) (3) (A).

[81] ibid, (g) (1) (C).

[82] ibid, (g) (4).

[83] ibid, (g) (1) (D).

[84] ibid, (g) (4).

[85] ibid, (i).

[86] ibid, (i) (1).

[87] ibid, (i) (2).

(10.3) ผู้ขอข้อมูลบุคคลใดโดยทุจริต ได้ร้องขอหรือได้รับข้อมูลที่เกี่ยวกับบุคคลจากหน่วยงานของรัฐ ถือว่าเป็นการกระทำความผิดลหุโทษ และมีโทษปรับไม่เกิน 5,000 ดอลลาร์สหรัฐอเมริกา[88]

(11) โปรแกรมจับคู่ข้อมูล(Data-Matching Program)

นอกจากบทบัญญัติที่เป็นข้อกำหนดในการบริหารจัดการข้อมูลส่วนบุคคลในหน่วยงานของรัฐแล้ว The Privacy Act of 1974 ยังได้บัญญัติถึงโปรแกรมจับคู่ข้อมูล(Data-Matching Program)ซึ่งเป็นมาตรการสำคัญที่หน่วยงานของรัฐพัฒนาขึ้น โดยเป็นโปรแกรมที่ทำหน้าที่จับคู่ข้อมูลส่วนบุคคลเพื่อทำการเปรียบเทียบข้อมูลด้านคอมพิวเตอร์ของระบบบันทึกข้อมูลสองหรือมากกว่าสองระบบซึ่งอาจรวมถึงระบบบันทึกข้อมูลที่มีใช่ของสหพันธรัฐด้วย โดยข้อมูลส่วนบุคคลจะอยู่ในรูปแบบของบันทึกข้อมูลอัตโนมัติหรือถูกทำให้เปลี่ยนไปเป็นรูปแบบการบันทึกข้อมูลอัตโนมัติ เพื่อใช้ทำการจับคู่ข้อมูลของแต่ละหน่วยงานที่ใช้โปรแกรมจับคู่ข้อมูลด้วยกัน ซึ่งการทำงานของโปรแกรมจับคู่ข้อมูลจะอยู่ภายใต้พระราชบัญญัติ The Computer Matching and Privacy Protection Act of 1988 อันเป็นพระราชบัญญัติที่แก้ไขเพิ่มเติมจาก The Privacy Act of 1974 เพื่อวัตถุประสงค์ในการจัดการกับปัญหาด้านระบบบันทึกข้อมูลอัตโนมัติและการใช้โปรแกรมจับคู่ข้อมูล โดยผู้อำนวยการของสำนักงานการบริหารจัดการและงบประมาณ(Office of Management and Budget : OMB)[89]จะเป็นผู้มีหน้าที่รับผิดชอบในการกำกับดูแลการใช้งานโปรแกรมตามข้อกำหนดของการใช้โปรแกรมจับคู่ข้อมูลใน The Privacy Act of 1974 ซึ่งสำนักงานกิจการสัมพันธ์แห่งรัฐและการเปิดเผยข้อมูล จะมีหน้าที่ให้คำแนะนำและให้ความช่วยเหลือทางเทคนิคในการพัฒนาข้อตกลงการจับคู่ข้อมูล และการแจ้งเรื่องการจับคู่ข้อมูล ตลอดจนรายงานอื่นที่เกี่ยวข้อง เป็นต้น

ทั้งนี้ หน่วยงานที่มีการใช้โปรแกรมจับคู่ข้อมูล กฎหมายได้กำหนดให้ทำการแต่งตั้งเจ้าหน้าที่ในหน่วยงานเป็นคณะกรรมการความสอดคล้องกันของข้อมูล(Data Integrity Board)[90] เพื่อคอยกำกับดูแลตลอดจนการออกกฎเกณฑ์ให้ทุกภาคส่วนในองค์กรให้มีการดำเนินงานที่สอดคล้องกัน และให้คณะกรรมการความสอดคล้องกันของข้อมูล ทำหน้าที่ในการตรวจทาน ทบทวน อนุมัติ และดำเนินการอย่างใดเกี่ยวกับบันทึกข้อมูลในโปรแกรมจับคู่ข้อมูล[91]นอกจากนี้หน่วยงานที่ใช้โปรแกรมจับคู่ข้อมูลจะต้องมีการทำข้อตกลงการจับคู่ข้อมูล(Matching Agreement) ซึ่งเป็นข้อตกลงที่เป็นลายอักษรระหว่างหน่วยงานซึ่งเป็นแหล่งที่มาของข้อมูลและหน่วยงานผู้รับข้อมูลรวมถึงหน่วยงานที่มิใช่สหพันธรัฐ โดยระบุถึงขอบเขตและเงื่อนไขของโปรแกรมจับคู่

---

[88] ibid, (i) (3).

[89] Public Law 93-579, The Privacy Acts of 1974, (u) (1).

[90] ibid, (u) (1).

[91] ibid, (u) (3) (a).

ข้อมูลระหว่างกัน ว่าแต่ละหน่วยงานที่ใช้โปรแกรมจับคู่ข้อมูลจะต้องทำการส่งรายงานชี้แจ้งรายละเอียดการใช้โปรแกรมดังกล่าวต่อสำนักงานการบริหารจัดการและงบประมาณ(Office of Management and Budget : OMB)และรัฐสภาแห่งสหพันธรัฐโดยผ่านสำนักงานกิจสัมพันธ์แห่งรัฐและการเปิดเผยข้อมูลและคณะกรรมการความสอดคล้องกันของข้อมูล(Data Integrity Board)

นอกจากนี้ ในประเทศสหรัฐอเมริกายังมีคณะกรรมการ The Privacy and Civil Liberties Oversight Board (PCLOB)ซึ่งได้ก่อตั้งครั้งแรกในปี ค.ศ. 2004 โดยเป็นหน่วยงานของผู้บริหารระดับสูง สังกัดสำนักงานบริหารของประธานาธิบดี(Executive Office of the President : EOP) ซึ่งเป็นหน่วยงานสำคัญที่ทำหน้าที่ควบคุมดูแลการรวบรวมและการใช้ข้อมูลส่วนบุคคลตลอดจนกำหนดหลักเกณฑ์เกี่ยวกับการจัดการข้อมูลส่วนบุคคลภายในประเทศสหรัฐอเมริกา[92] ในขณะที่กระทรวงกลาโหม(Department of Defense : DOD)แห่งประเทศสหรัฐอเมริกา ได้มีการจัดตั้งหน้าที่ของหน่วยงานป้องกันความเป็นส่วนตัวและเสรีภาพของประชาชน(Defense Privacy and Civil Liberties Office : DPCLO)[93]เพื่อทำหน้าที่จัดทำโครงการของหน่วยงานผ่านการปรึกษา ควบคุมดูแล รายงาน และการฝึกอบรมและมีหน้าที่รับผิดชอบต่อโปรแกรมที่เกี่ยวข้องกับด้านความเป็นส่วนตัวของกระทรวงกลาโหม(Department of Defense Privacy Program) โดยโครงการดังกล่าวจะมีโครงสร้างที่ครอบคลุมวิธีการ และเวลาที่กระทรวงกลาโหมจะรวบรวม รักษาหรือใช้ ตลอดจนเผยแพร่ข้อมูลส่วนบุคคล โดยมีวัตถุประสงค์ของโครงการเพื่อเป็นการสร้างสมดุลของความต้องการข้อมูลของหน่วยงานกับผลประโยชน์ด้านความเป็นส่วนตัวและการคำนึงถึงสิทธิความเป็นส่วนตัวของบุคคล

จากข้อมูลดังกล่าวข้างต้น จะเห็นได้ว่าประเทศสหรัฐอเมริกา ได้มีการพัฒนาด้านการให้ความคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของหน่วยงานรัฐอย่างจริงจัง โดยส่วนหนึ่งเป็นผลมาจากการได้ประกาศบังคับใช้พระราชบัญญัติรัฐบาลอิเล็กทรอนิกส์ หรือ The E-Government Act of 2002 เนื่องจากสหรัฐอเมริกาได้ตระหนักว่าในโลกที่มีความก้าวหน้าทางเทคโนโลยีสารสนเทศและการโทรคมนาคมนั้น ยังมีความจำเป็นที่จะต้องแตกแขนงมาตรการที่ให้ความคุ้มครองข้อมูลส่วนบุคคลเอาไว้โดยเฉพาะออกไปอีก[94]ดังนั้น Section 208 แห่ง E-Government Act of 2002 จึงบัญญัติบังคับให้หน่วยงานแห่งสหพันธรัฐทั้งหมดที่ได้พัฒนาหรือผลิตเทคโนโลยีข้อมูลข่าวสารใดที่เกี่ยวกับการรวบรวมข้อมูล รักษา หรือเผยแพร่ข้อมูลในรูปแบบการระบุตัวตน ต้องทำการเปลี่ยนแปลงเทคโนโลยีข้อมูลข่าวสารที่ใช้ในการจัดการ

---

[92] Techfreedom, **Today's Approval of PCLOB Nominations a Long-Overdue Victory for Privacy and the Rule of Law** [online], 1 July 2012. Available from http://techfreedom.org/node/175.

[93] Defense Privacy and Civil Liberties Office, **About the Office** [online], 1 July 2012. Available from http://dpclo.defense.gov/privacy/About_The_Office/about_the_office.html.

[94] The United States Department of Justice. **E-Government Act 2002** [online], 7 June 2012 Available from http://www.justice.gov/opcl/e-govt-act-2002.html.

ข้อมูลดังกล่าว[95]ซึ่งรวมถึงการทำการประเมินผลกระทบด้านความเป็นส่วนตัว(Privacy Impact Assessments : PIAs)อันเป็นการวิเคราะห์วิธีการดำเนินงานของหน่วยงานของรัฐซึ่งได้กระทำกับข้อมูลในรูปแบบการระบุตัวตน ดังนั้น E-Government Act of 2002 จึงบัญญัติให้หน่วยงานของรัฐทำการประเมินผลกระทบความเป็นส่วนตัว(PIAs)ต่อสาธารณะ เว้นแต่หน่วยงานดังกล่าวมีดุลยพินิจพิเศษที่จะให้การมีประเมินผลกระทบความเป็นส่วนตัวในกรณีที่เป็นเรื่องเกี่ยวกับด้านความความมั่นคงของชาติ หรือเป็นข้อมูลที่อ่อนไหวที่อาจทำให้เกิดความเสียหายแก่ผลประโยชน์ของชาติ หรือการบังคับใช้กฎหมาย[96]

ทั้งนี้ นอกจากรัฐบาลแห่งสหพันรัฐจะให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์กับหน่วยงานของรัฐเป็นอย่างมากแล้ว ยังปรากฏรายงานว่าชาวอเมริกันมีความพึงพอใจเป็นอย่างมากต่อการให้บริการในการทำธุรกรรมอิเล็กทรอนิกส์กับหน่วยงานของรัฐ ซึ่งปรากฏในไตรมาสที่ 4 ของดัชนีการสำรวจความพึงพอใจของชาวอเมริกัน American Customer Satisfaction Index (ACSI)[97]โดยดัชนีความพึงพอใจในรัฐบาลอิเล็กทรอนิกส์แสดงให้เห็นว่าผู้ใช้บริการมีความพึงพอใจในการให้บริการเว็บไซต์ของรัฐบาลสหพันธรัฐซึ่งใกล้จะถึงจุดสูงสุดซึ่งเลยระดับความพึงพอใจโดยรวมไปแล้วนั้น โดย ACSI แสดงให้เห็นถึงความพึงพอใจในการให้บริการของหน่วยงานของรัฐในรูปแบบรัฐบาลอิเล็กทรอนิกส์ในช่วงท้ายปี ค.ศ. 2011 ซึ่งได้รับคะแนนสูงถึง 75.1 คะแนน จากคะแนนเต็มจำนวน 100 คะแนน โดยประชาชนยังมีความพอใจเมื่อได้ติดต่อประสานงานกับรัฐบาลผ่านระบบออนไลน์ ซึ่งรัฐบาลของประธานาธิบดีบารัค โอบามา(Barack Obama)ได้ให้ความสำคัญกับดำเนินงานด้านรัฐบาลอิเล็กทรอนิกส์เป็นอย่างมาก โดยประธานาธิบดีได้สั่งให้มีการบริหารงานภาครัฐแบบเปิดเพื่อเพิ่มความโปร่งใสและความน่าเชื่อถือ โดยได้มีการตั้งตำแหน่งหัวหน้าเจ้าหน้าเทคนิค(Chief Technical Office) เพื่อการดำเนินงานของรัฐบาลอิเล็กทรอนิกส์มีประสิทธิภาพมากและเพื่อที่จะเป็นการส่งเสริมความพึงพอใจและสร้างความเชื่อมั่นต่อการให้บริการของรัฐบาลอิเล็กทรอนิกส์ หรือ e-Government

---

[95] Public Law 107–347, E-Government Act of 2002, Section 208.

[96] The United States Department of Justice. E-Government Act 2002[online], 7 June 2012 Available from http://www.justice.gov/opcl/e-govt-act-2002.html.

[97] ACSI หรือ The American Customer Satisfaction Index คือ การวัดความพึงพอใจในการบริการที่ดีในทุกภาคส่วนในประเทศอเมริกา โดยในปี ค.ศ.1999 รัฐบาลสหพันธรัฐได้เลือก ACSI เป็นมาตรฐานในการวัดความพึงพอใจของประชาชน โดยมีกว่า 100 หน่วยงานของสหพันธรัฐที่ใช้ ACSI เพื่อวัดค่าความพึงพอใจ ซึ่งดัชนีจะทำขึ้นที่มหาวิทยาลัยมิชิแกน(Michigan's Ross School of Business) โดยมี LLC. ForeSee เป็นผู้สนับสนุนในการทำดัชนีวัดค่าความพึงพอใจ e-Government

ให้สูงยิ่งขึ้น[98]ซึ่งจะเห็นได้ว่าประเทศสหรัฐอเมริกานอกจากจะมีมาตรการในการให้ความคุ้มครองข้อมูลส่วนบุคคลและมีกลไกในการบริหารจัดการทางด้านข้อมูลส่วนบุคคลที่มีประสิทธิภาพแล้ว ยังมีการเชื่อมโยงการดำเนินงานภายใต้กรอบรัฐบาลอิเล็กทรอนิกส์อย่างเป็นระบบอีกด้วย เช่น

กรณี ของกระทรวงแรงงานแห่งสหรัฐอเมริกา[99](United States Department of Labor : DOL)ซึ่งมีความพยายามในการจัดเก็บและรักษาข้อมูลส่วนบุคคลภายในหน่วยงานให้มีประสิทธิภาพ โดยทำการพัฒนาระบบอิเล็กทรอนิกส์ที่เกี่ยวข้องกับด้านความมั่นคงขึ้น เพื่อให้สอดคล้องกับกฎระเบียบและนโยบายของสหพันธรัฐและพระราชบัญญัติการจัดการความมั่นคงด้านข้อมูลแห่งสหพันธรัฐ[100](Federal Information Security Management Act of 2002 : FISMA) ตลอดจน Title III แห่ง the E-Government Act of 2002 ว่าด้วยเรื่อง ความมั่นคงปลอดภัยของข้อมูล (Information Security)[101]รวมถึงพระราชบัญญัติความเป็นส่วนตัว The Privacy Act of 1974[102]จนกระทั่งประสบความประสบความสำเร็จในการนำการทำธุรกรรมอิเล็กทรอนิกส์มาปรับใช้ในองค์กรในหลายรูปแบบเพื่อเป็นการพัฒนาระบบการให้บริการกับประชาชน เช่น มาตรการใช้ระบบป้องกันข้อมูลการสื่อสารผ่านเครือข่ายอินเตอร์เน็ต(Public Key Infrastructure : PKI)[103]ตลอดจนการนำลายมือชื่ออิเล็กทรอนิกส์มาใช้ทั่วทั้งองค์กร โดยระบบ PKI จะต้องถูกนำมาใช้แทนวิธีพิสูจน์ตัวตนที่มีอยู่ตลอดจนสนับสนุนให้มีการใช้สมาร์ทการ์ด(Smart Card)เพื่อเป็นที่เก็บข้อมูลและหลักฐานต่าง ๆ ในการทำธุรกรรมทางอิเล็กทรอนิกส์เพื่อตอบสนองความต้องการของหน่วยงานของรัฐได้อย่างมีประสิทธิภาพตามแนวทางในการจัดทำรัฐบาลอิเล็กทรอนิกส์

จากข้อมูลดังกล่าวข้างต้นจะเห็นได้ว่า ประเทศสหรัฐอเมริกาได้ให้ความสำคัญต่อการคุ้มครองสิทธิในความเป็นส่วนตัวซึ่งครอบคลุมถึงการคุ้มครองข้อมูลส่วนบุคคลเป็นอย่างมาก แม้กระทั่งในยุคปัจจุบันที่มีความเจริญก้าวหน้าทางเทคโนโลยีสารสนเทศและการโทรคมนาคมอย่างต่อเนื่อง

---

[98] United Nations Public Administration Network Public Administration News. **USA : Satisfaction With e-Government Reaches New Highs Under Obama but is Stalling, According to ForeSee** [online], 7 June 2012 Avalible from http://www.unpan.org/PublicAdministrationNews/tabid/118/mctl/ArticleView/ModuleID/1473/articleId/29498/default.aspx

[99] Public Law 426-62, An Act to Create a Department of Labor.

[100] Federal Information Security Management Act of 2002.

[101] Public Law 107–347, E-Government Act of 2002, Title III.

[102] The United States of Labor. **U.S. Department of Labor E-Government Strategic Plan** [online], 7 June 2012. Available from http://www.dol.gov/_sec/e_government_plan/p23_security_privacy.htm

[103] PKI หรือ Public Key Infrastructure หมายถึง โครงสร้างพื้นฐานกุญแจสาธารณะซึ่งเป็นเทคโนโลยีที่อาศัยระบบรหัสแบบกุญแจสาธารณะ(Public Key Cryptography) ที่ประกอบด้วยกุญแจส่วนตัว (Private Key)และกุญแจสาธารณะ(Public Key) เพื่อใช้ในการพิสูจน์ตัวตนจริง(Authentication) รวมทั้งการรักษาความลับของข้อมูล (Data Confidentiality) ความครบถ้วนของข้อมูล (Data Integrity) และการห้ามปฏิเสธความรับผิด (Non-repudiation)

แต่รัฐบาลสหพันธรัฐแห่งสหรัฐอเมริกาก็ได้มีความพยายามที่จะพัฒนามาตรการและกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลซึ่งครอบคลุมไปถึงการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐหรือ e-Government เพื่อให้เกิดความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่หน่วยงานของรัฐจัดเก็บหรือดูแลอยู่ และยังเป็นการเสริมสร้างความเชื่อมั่นให้แก่ประชาชนในการให้ข้อมูลที่เป็นจริงกับหน่วยงานของรัฐอีกด้วย

4.2 การคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐในสหภาพยุโรป

สหภาพยุโรป(European Union : EU) เป็นองค์การด้านความร่วมมือระหว่างประเทศซึ่งก่อตั้งขึ้นเมื่อวันที่ 7 กุมภาพันธ์ ค.ศ. 1992 ภายใต้สนธิสัญญาว่าด้วยสหภาพยุโรป(The Treaty on European Union : TEU) หรือเป็นที่รู้จักกันอย่างแพร่หลายในชื่อสนธิสัญญามาสทริชต์ (Maastricht Treaty) โดยเป็นองค์กรเพื่อสนับสนุนความร่วมมือทางเศรษฐกิจ ซึ่งปัจจุบันประกอบด้วยรัฐสมาชิก 27 ประเทศ โดยประเทศส่วนใหญ่อยู่ในทวีปยุโรปซึ่งมีการรวมตัวและก่อตั้งแทนที่ประชาคมเศรษฐกิจยุโรป (European Economic Community : EEC) ทั้งนี้ สหภาพยุโรปมีอิทธิพลอย่างมากต่อเวทีโลก เนื่องด้วยมีประชากรกว่า 500 ล้านคน[104]และมีผลิตภัณฑ์มวลรวมภายในประเทศคิดเป็นกว่า 30% ของโลก โดยมีสำนักงานใหญ่ตั้งอยู่ที่กรุงบรัสเซลส์ ประเทศเบลเยี่ยม ซึ่งการดำเนินงานของสหภาพยุโรปประกอบด้วยสถาบันหลัก 3 สถาบัน ได้แก่

(1) คณะกรรมาธิการยุโรป(European Commission)[105]ซึ่งเปรียบเสมือนเป็นตัวแทนของผลประโยชน์แห่งสหภาพยุโรป ซึ่งมีการดำเนินงานที่เป็นอิสระจากรัฐบาลของแต่ละประเทศสมาชิก โดยประกอบไปด้วยคณะกรรมาธิการ(Commissioner)จากประเทศสมาชิกตามความเชี่ยวชาญ ซึ่งจะต้องทำงานร่วมกับข้าราชการประจำ(Officials)โดยมีผู้บริหาร คือ ประธานคณะกรรมาธิการ ซึ่งจะได้รับการเลือกจากรัฐบาลของประเทศสมาชิกและจะต้องได้รับการรับรองจากรัฐสภายุโรป นอกจากนี้ คณะกรรมาธิการยุโรป(European Commission)ยังทำหน้าที่เป็นผู้สอดส่องดูแลการนำกฎหมายแห่งสหภาพยุโรป(Directive)ไปใช้ในแต่ละประเทศ โดยจะมีการประชุมกันระหว่างประเทศสมาชิกถึงการบังคับใช้กฎหมายของประเทศสมาชิกเพื่อความสอดคล้องกับ Directive

---

[104] Department of Economic and Social Affairs. Population Division, United Nations, **World Population Prospects : The 2010 Revision**[online], 6 June 2012 Available from http:// www.irs. gov/irs/article/0,,id=183728,00.html.

[105] European Union, European Commission [online], 1 July 2012. Available from http://ec.europa.eu/index_en.htm.

โดยประเทศสมาชิกจะจัดทำรายงานของสภาพการณ์ในปัจจุบันและรับข้อเสนอแนะที่เป็นไปในทิศทางเดียวกับที่คณะกรรมาธิการยุโรปกำหนด

(2) สภายุโรป(European Parliament)[106]เป็นองค์กรที่สมาชิกแห่งสภายุโรปซึ่งจะได้รับการเลือกตั้งโดยตรงทุก 5 ปีจากแต่ละประเทศสมาชิก โดยมีภารกิจหลักในการประสานงานและตัดสินใจในการดำเนินงานเรื่องใด ๆ กับคณะมนตรี เช่น การร่วมพิจารณาร่างกฎหมายของสหภาพยุโรปที่คณะกรรมาธิการเสนอ เป็นต้น

(3) คณะมนตรีแห่งสหภาพยุโรป (Council of the European Union หรือ Council of Ministers) เป็นองค์กรหลักในด้านกระบวนการนิติบัญญัติและด้านการตัดสินใจชี้ขาดของสหภาพยุโรป โดยจะทำหน้าที่ประสานงานกับรัฐสภายุโรปในการพิจารณาร่างกฎหมายและยังเป็นผู้รับผิดชอบในด้านนโยบายต่างประเทศและความมั่นคงร่วม(Common Foreign and Security Policy : CFSP หรือ CONSILIUM)[107]แห่งสหภาพยุโรปอีกด้วย

ทั้งนี้ ในช่วงปี ค.ศ. 1961 สหภาพยุโรป(EU)ในขณะที่ยังเป็นประชาคมเศรษฐกิจยุโรป (European Economic Community : EEC)อยู่นั้นได้มีการก่อตั้งองค์กรเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา(Organization for Economic Cooperation and Development : OECD) ขึ้นเมื่อวันที่ 30 กันยายน พ.ศ. 1961 ซึ่งเป็นการพัฒนามาจาก OEEC (Organization for European Economic Co-operation)ที่จัดตั้งขึ้นในปี ค.ศ. 1948 โดยมีวัตถุประสงค์เพื่อเป็นองค์กรในการบริหารเงินช่วยเหลือจากสหรัฐอเมริกาและแคนาดาภายใต้แผนมาร์แชล(Marshall Plan)เพื่อบูรณะฟื้นฟูสภาพเศรษฐกิจและสภาพสังคมของยุโรปภายหลังสงครามโลก ครั้งที่ 2 โดยประกอบไปด้วยประเทศสมาชิกจากหลายประเทศซึ่งอยู่ในทวีปยุโรป ซึ่งได้ตระหนักถึงผลกระทบจากกระทำความผิดต่อสิทธิในความเป็นส่วนตัวขั้นพื้นฐานในการใช้ข้อมูลส่วนบุคคลอย่างผิดกฎหมายหรือจากการเก็บข้อมูลส่วนบุคคลที่ไม่ถูกต้อง ตลอดจนการเปิดเผยข้อมูลส่วนบุคคลโดยมิได้รับอนุญาต จึงได้มีการกำหนดแนวทางร่วมกันในการสร้างมาตรการคุ้มครองข้อมูลส่วนบุคคล (Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Transborders Flows of Personal Data)[108]ซึ่งเปรียบเสมือนตัวแทนของความคิดเห็นที่เกี่ยวข้องกับการจัดเก็บรวบรวมและการจัดการข้อมูลส่วนบุคคลที่ได้กำหนดขึ้น เป็นหลักการ

---

[106] European Union, European Parliament [online], 1 July 2012. Available from http://www.europarl.europa.eu/.

[107] European Union, Council of the European Union [online], 1 July 2012. Available from http://www.consilium.europa.eu/homepage?lang=en.

[108] Organization for Economic Co-operation and Development, **OECD Council Recommendation** [online], 4 June 2012. Available from http://www.oecd.org/document/18/0,3746,en_2649_34223_1815186_1_1_1_1,00.html.

เพื่อที่จะสนับสนุนและช่วยให้ภาครัฐ และภาคเอกชน ตลอดจนภาคส่วนอื่นในสหภาพยุโรปได้ร่วมกันนำมาตรการคุ้มครองข้อมูลส่วนบุคคลมาใช้โดยสอดคล้องกัน

ต่อมาในช่วงปี ค.ศ. 1995 เนื่องจากกฎหมายของหลายประเทศภาคีสมาชิกในสหภาพยุโรปมีความแตกต่างกันมาก ซึ่งอาจเป็นอุปสรรคต่อการส่งผ่านข้อมูลส่วนบุคคลภายในสหภาพยุโรป ดังนั้น สหภาพยุโรปจึงได้มีการกำหนดหลักเกณฑ์ที่มีชื่อว่า 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 ซึ่งเป็นมาตรการในการให้ความคุ้มครองข้อมูลส่วนบุคคลแก่ประเทศที่เป็นภาคีสมาชิกให้มีแนวทางของกฎหมายที่สอดคล้องกันเพื่อเป็นการทำให้การไหลเวียนของข้อมูลส่วนบุคคลในประเทศภาคีสมาชิกเป็นไปได้โดยเสรีปราศจากข้อจำกัดที่เกิดจากความแตกต่างกันของกฎหมายหรือกฎเกณฑ์ใด ๆ ที่แต่ละประเทศภาคีสมาชิกพึงมีและใช้บังคับอยู่

4.2.1 DIRECTIVE 95/46/EC of The European Parliament and of The Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

ตามบัญญัติแห่ง 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 แห่งสหภาพยุโรป มีหลักการที่สำคัญ 8 ประการ ดังต่อไปนี้

(1) หลักเกณฑ์มาตรฐานในการรักษาคุณภาพของข้อมูล(Principles Relating to Data Quality)[109]ซึ่งมีสาระสำคัญ ดังนี้

ข้อมูลส่วนบุคคลจะต้องได้รับการดำเนินการ[110]อย่างถูกต้องเหมาะสมและชอบด้วยกฎหมาย[111]โดยในการเก็บรวบรวมและการนำข้อมูลไปใช้จะต้องไม่เกินขอบวัตถุประสงค์ที่แจ้งไว้[112]เว้นแต่ เป็นการนำไปใช้เพื่อวัตถุประสงค์ในทางประวัติศาสตร์ สถิติและวิทยาศาสตร์[113] ซึ่งประเทศสมาชิกต้องให้การคุ้มครองที่เหมาะสมสำหรับการเก็บรักษาข้อมูลในระยะเวลาที่ยาวนานเพื่อไว้ใช้ในทางประวัติศาสตร์ ทางสถิติ และทางวิทยาศาสตร์นั้น[114]ตลอดจนต้องมีการ

---

[109] 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, Section I.

[110] ibid, Article 6 paragraph 1.

[111] ibid, Article 6 paragraph 1. (a).

[112] ibid, Article 6 paragraph 1. (c).

[113] ibid, Article 6 paragraph 1. (b).

[114] ibid, Article 6 1. (e).

ตรวจสอบข้อมูล ให้มีความถูกต้องและเป็นปัจจุบัน ซึ่งข้อมูลที่ไม่ถูกต้องจะต้องถูกลบ หรือได้รับการแก้ไขให้ถูกต้องเมื่อจะมีการนำข้อมูลไปใช้[115]และข้อมูลนั้นจะต้องถูกเก็บไว้ในรูปแบบที่สามารถอนุญาตให้มีการระบุตัวตนของเจ้าของมูลได้เท่าที่จำเป็น

(2) หลักเกณฑ์มาตรฐานในการทำให้การใช้ข้อมูลถูกต้องตามกฎหมาย (Criteria for Making Data Processing Legitimate)[116]ซึ่งมีสาระสำคัญ ดังนี้

(2.1) การนำข้อมูลมาใช้จะต้องอยู่ภายใต้เงื่อนไข ดังต่อไปนี้[117]

(ก) เจ้าของข้อมูลได้ให้ความยินยอมโดยชัดแจ้ง หรือ[118]

(ข) การใช้ข้อมูลมีความจำเป็นในผลของสัญญาที่ซึ่งเจ้าของข้อมูลได้มีส่วนเกี่ยวข้อง หรือเพื่อใช้ดำเนินการตามที่เจ้าของข้อมูลเรียกร้องก่อนที่จะทำสัญญา หรือ[119]

(ค) การใช้ข้อมูลมีความจำเป็นเพื่อการดำเนินการใดที่มีความสอดคล้องกับข้อบังคับทางกฎหมาย ทั้งนี้ ต้องอยู่ภายใต้การกำกับดูแลของผู้ควบคุมข้อมูล หรือ[120]

(ง) การใช้ข้อมูลมีความจำเป็นเพื่อประโยชน์สาธารณะหรือโดยการกระทำของเจ้าหน้าที่ผู้มีอำนาจตามกฎหมาย หรือ[121]

(จ) การใช้ข้อมูลมีความจำเป็นเพื่อวัตถุประสงค์ซึ่งเป็นผลประโยชน์ในทางกฎหมายซึ่งชักจูงโดยผู้ควบคุม หรือบุคคลที่สาม หรือผู้อื่นที่ข้อมูลได้รับการเปิดเผย ยกเว้นในกรณีที่ผลประโยชน์ดังกล่าว เป็นการคุกคามต่อสิทธิและเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลที่พึงจะได้รับการคุมครองภายใต้ มาตราที่ 1(1)[122]

(3) หลักเกณฑ์มาตรฐานในการใช้ข้อมูลในหมวดพิเศษ (Special Categories of Processing)[123]ซึ่งมีสาระสำคัญ ดังนี้

(3.1) ห้ามมีการเปิดเผยข้อมูลส่วนบุคคลที่เป็นการเหยียดเผ่าพันธุ์ ชาติพันธ์ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนา ปรัชญา ข้อมูลทางการแพทย์ หรือชีวิตทางเพศ เว้นแต่มี กรณีดังต่อไปนี้

---

[115] ibid, Article 6 paragraph 1. (d).

[116] ibid, Section II.

[117] ibid, Article 7 (a).

[118] ibid, Article 7 (b).

[119] ibid, Article 7 (c).

[120] ibid, Article 7 (d).

[121] ibid, Article 7 (e).

[122] ibid, Article 7 (f).

[123] ibid, Section III.

(ก) เจ้าของข้อมูลได้ให้ความยินยอมเอาไว้โดยชัดแจ้ง เว้นแต่กฎหมายของประเทศสมาชิกระบุว่าความยินยอมของเจ้าของข้อมูลไม่อาจใช้ได้ หรือ

(ข) การนำข้อมูลไปใช้ในวัตถุประสงค์เพื่อการดำเนินการตามข้อบังคับและสิทธิจำเพาะของผู้ควบคุม ซึ่งได้รับการรับรองโดยกฎหมายของประเทศที่มีการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ หรือ

(ค) การนำข้อมูลไปใช้โดยความจำเป็นเพื่อคุ้มครองผลประโยชน์ชีวิตของเจ้าของข้อมูลหรือบุคคลอื่น ซึ่งเจ้าของข้อมูลไม่มีความสามารถในทางร่างกายหรือในทางกฎหมายที่จะให้ความยินยอม หรือ

(ง) การนำข้อมูลไปใช้ในทางกฎหมายที่มีการรับรองอย่างเหมาะสมโดยมูลนิธิ สมาคม หรือองค์ไม่แสวงหากำไรอื่น ๆ ภายใต้เงื่อนไขที่ว่าการนำข้อมูลไปใช้จะต้องไม่เปิดเผยต่อบุคคลที่สามโดยไม่ได้รับการยินยอมจากเจ้าของข้อมูล หรือ

(จ) การนำข้อมูลไปใช้โดยเปิดเผยต่อสาธารณะโดยเจ้าของข้อมูล หรือมีความจำเป็นในการก่อตั้ง กระทำ หรือป้องกันการกล่าวหาทางกฎหมาย

(3.2) การไม่นำข้อห้ามใดมาบังคับใช้กับการใช้ข้อมูลส่วนบุคคลเพื่อความจำเป็นทางการแพทย์ แต่ต้องอยู่ภายใต้กฎหมายของประเทศ หรือข้อบังคับที่ตั้งขึ้นโดยหน่วยงานที่มีอำนาจเข้าถึงความลับในการประกอบวิชาชีพ

(3.3) ต้องมีมาตรการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม ซึ่งหากเป็นการดำเนินงานเพื่อประโยชน์สาธารณะ ประเทศสมาชิกอาจกำหนดข้อยกเว้นเพิ่มเติมได้

(3.4) การนำข้อมูลไปใช้ในส่วนที่เกี่ยวข้องกับโทษทางอาญา หรือมาตรการด้านความปลอดภัย ซึ่งอาจกระทำขึ้นภายใต้การควบคุมของเจ้าหน้าที่ผู้มีอำนาจ หรือภายใต้การคุ้มครองที่เฉพาะภายใต้กฎหมายของประเทศ

(3.5) ประเทศสมาชิกจะต้องระบุเงื่อนไขไว้ใต้หมายเลขระบุตัวตน

(3.6) การใช้ข้อมูลส่วนบุคคลซึ่งเป็นเสรีภาพในการแสดงออก ประเทศภาคีสมาชิกต้องกำหนดข้อยกเว้นในการใช้ข้อมูลเพื่อวัตถุประสงค์ในการตีพิมพ์ หรือการแสดงออกทางศิลปะหรือวรรณกรรม[124]

(4) หลักเกณฑ์มาตรฐานของข้อมูลที่จะให้แก่เจ้าของข้อมูล[125](Information to be Given to the Data Subject) ซึ่งมีสาระสำคัญ ดังนี้

ตามหลักเกณฑ์มาตรฐานของข้อมูลที่จะให้แก่เจ้าของข้อมูลซึ่งกำหนดว่าประเทศสมาชิกต้องให้การรับรองว่าผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งเจ้าของข้อมูลให้ทราบ

---

[124] ibid, Article 9.

[125] ibid, Section IV.

ในขณะที่ทำการบันทึกข้อมูลส่วนบุคคลหรือเมื่อมีการเปิดเผยข้อมูลแก่บุคคลที่สามเป็นครั้งแรก ถึงการระบุตัวตนของผู้ควบคุมข้อมูลและตัวแทน[126]และวัตถุประสงค์ในการนำข้อมูล ไปใช้[127] ตลอดจนข้อมูลอื่นที่จำเป็น เช่น รายละเอียดของผู้รับข้อมูล และสิทธิของเจ้าของข้อมูลส่วนบุคคล ในการเข้าถึงข้อมูลและแก้ไขข้อมูลที่เกี่ยวข้อง[128]เว้นแต่ว่าบุคคลนั้นมีข้อมูลแล้ว[129]

ทั้งนี้ มีข้อยกเว้นว่าไม่นำข้อห้ามของกฎหมายมาบังคับใช้ เมื่อมีการนำข้อมูลไปใช้เพื่อวัตถุประสงค์ทางสถิติ ทางประวัติศาสตร์ หรือวิทยาศาสตร์ แต่ต้องอยู่ภายใต้หลักเกณฑ์ที่กำหนดไว้โดยกฎหมาย และต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม[130]

(5) หลักเกณฑ์มาตรฐานของสิทธิในการเข้าถึงข้อมูลของเจ้าของข้อมูล[131] (The Data Subject's Right of Access to Data) ซึ่งมีสาระสำคัญ ดังนี้

ตามหลักหลักสิทธิในการเข้าถึงข้อมูลของเจ้าของข้อมูลซึ่งกำหนดให้เจ้าของข้อมูลมีสิทธิเข้าถึงข้อมูลจากผู้ควบคุมข้อมูลตามความเหมาะสมเพื่อการขอแก้ไข การลบ หรือการจำกัดการใช้ข้อมูล[132]โดยปราศจากข้อจำกัด ค่าใช้จ่าย หรือความล่าช้าจนเกินไป[133]ตลอดจนต้องมีการแจ้งให้บุคคลที่สามที่ข้อมูลถูกเปิดเผยได้ทราบถึงการแก้ไข การลบ หรือการจำกัดการใช้ข้อมูล เว้นแต่การเปิดเผยข้อมูลจะพิสูจน์ได้ว่าอาจเกิดความไม่เหมาะสม[134]

(6) หลักเกณฑ์มาตรฐานของสิทธิในการคัดค้านการประมวลผลข้อมูลของเจ้าของข้อมูล[135] (Exemption and Restrictions) ซึ่งมีสาระสำคัญ ดังนี้

(6.1) ประเทศภาคีสมาชิกอาจใช้มาตรการทางกฎหมายเพื่อจำกัดขอบเขตของข้อยกเว้นต่าง ๆ ได้ต่อเมื่อมีมาตรการการคุ้มครองข้อมูลตามความจำเป็น[136]หรือเพื่อประโยชน์ใดที่สำคัญ เช่น การตรวจสอบข้อเท็จจริง การสืบสวนและการดำเนินคดีทางอาญา การละเมิดหลักจริยธรรมวิชาชีพ[137]หรือเพื่อประโยชน์ที่มีความสำคัญทางเศรษฐกิจหรือทางการเงินของประเทศ

---

[126] ibid, Article 10 (a).

[127] ibid, Article 10 (b).

[128] ibid, Article 10 (c).

[129] ibid, Article 11.

[130] ibid, Article 10 paragraph 2.

[131] ibid, Article V.

[132] ibid, Article 12 (b).

[133] ibid, Article 12 (a).

[134] ibid, Article 12 (c).

[135] ibid, Article VI.

[136] ibid, Article 13 paragraph 1.

[137] ibid, Article 13 (a).

สมาชิก[138]หรือการดูแลตรวจสอบระเบียบควบคุมเป็นบางครั้งโดยเจ้าหน้าที่มีผู้มีอำนาจ[139] ตลอดจนการป้องกันเจ้าของข้อมูลหรือสิทธิและเสรีภาพของผู้อื่น[140]

(6.2) ข้อมูลส่วนบุคคลที่ได้ถูกนำไปใช้เพื่อวัตถุประสงค์ในการวิจัยทางวิทยาศาสตร์ หรือถูกเก็บไว้ในรูปแบบที่เป็นส่วนตัวเพื่อวัตถุประสงค์ในทางสถิติ จะต้องมีช่วงระยะเวลาที่จัดเก็บเท่าที่จำเป็น และต้องมีการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม[141]

(7) หลักเกณฑ์มาตรฐานของสิทธิในการคัดค้านของเจ้าของข้อมูล(The Data Subject's Right to Object)[142] ซึ่งมีสาระสำคัญ คือ

(7.1) ต้องให้สิทธิในการทำคัดค้านข้อมูลส่วนบุคคลของเจ้าของข้อมูลอย่างน้อยในกรณีที่มีการใช้ข้อมูลนั้นมีความจำเป็นเพื่อประโยชน์สาธารณะ หรือเพื่อประโยชน์ในทางกฎหมาย โดยในการคัดค้านการใช้ข้อมูลส่วนบุคคลนั้นจะต้องมีเหตุอันชอบด้วยกฎหมายที่เกี่ยวข้องกับบุคคลนั้นโดยเฉพาะ และเมื่อมีการแสดงการคัดค้านการใช้ข้อมูลแล้วผู้ควบคุมอาจจะไม่สามารถใช้ข้อมูลเหล่านั้นได้อีกต่อไป[143]

(7.2) ผู้ควบคุมข้อมูลจะต้องให้สิทธิในการคัดค้านข้อมูลส่วนบุคคลของเจ้าของข้อมูลโดยไม่เสียค่าใช้จ่าย และให้เจ้าของข้อมูลได้รับการแจ้งก่อนที่ข้อมูลจะถูกเปิดเผยแก่บุคคลที่สามหรือใช้เพื่อเป็นส่วนหนึ่งของการตลาดทางตรง[144]

(8) หลักเกณฑ์มาตรฐานของการรักษาความลับและความปลอดภัยในการใช้ข้อมูล (Confidentialty and Security of Processing)[145] ซึ่งมีสาระสำคัญ คือ

หลักเกณฑ์ในข้อนี้ ได้กำหนดให้บุคคลใดที่กระทำการภายใต้อำนาจของผู้ควบคุมข้อมูลส่วนบุคคลที่สามารถเข้าถึงข้อมูลส่วนบุคคลได้จะต้องมิใช้ข้อมูลดังกล่าว เว้นแต่จะได้รับคำสั่งจากผู้ควบคุมข้อมูลหรือมีความจำเป็นต้องกระทำตามกฎหมาย[146]โดยมีมาตรการที่

---

[138] ibid, Article 13 (b).

[139] ibid, Article 13 (c).

[140] ibid, Article 13 (c).

[141] ibid, Article 13.

[142] ibid, Article VII.

[143] ibid, Article 14 (a).

[144] ibid, Article 14 (b).

[145] ibid, Section VIII.

[146] ibid, Article 16.

เหมาะสมเพื่อปกป้องข้อมูลจากการทำลาย การสูญหายโดยมิได้เจตนา การใช้งานที่ผิดกฎหมาย ตลอดจนการเปิดเผย หรือการเข้าถึงข้อมูลโดยมิได้รับอนุญาต[147]

นอกจากหลักการสำคัญ 8 ประการดังกล่าวของ 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 ซึ่งได้รับอิทธิพลมาจาก Guidelines on the protection of Privacy and Transborder Data Flows of Personal Data แห่ง OECD แล้วนั้น ยังได้มีการกำหนดแนวทางในการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลให้แก่ประเทศสมาชิกอีกด้วย โดยมีสาระสำคัญดังนี้

(1) วัตถุประสงค์ของการใช้ข้อมูลส่วนบุคคลจะต้องชอบด้วยกฎหมายและมีความยุติธรรมต่อบุคคลผู้เป็นเจ้าของข้อมูล ซึ่งจะต้องไม่ใช้ข้อมูลส่วนบุคคลที่ไม่ตรงกับวัตถุประสงค์ที่ระบุเอาไว้ในการจัดเก็บข้อมูล[148]และเป็นสิ่งสำคัญที่ประเทศสมาชิกต้องจัดหาผู้ดูแลการใช้มาตรการคุ้มครองข้อมูลส่วนบุคคลที่มีอำนาจเป็นอิสระ[149]

(2) ความแตกต่างของระดับการคุ้มครองข้อมูลส่วนบุคคล และสิทธิเสรีภาพของบุคคลของแต่ละประเทศภาคีสมาชิก อาจเป็นอุปสรรคสำคัญต่อการส่งผ่านข้อมูลส่วนบุคคล[150] ดังนั้น การที่จะขจัดอุปสรรคเหล่านั้น ประเทศภาคสมาชิกควรมีระดับความคุ้มครองข้อมูลส่วนบุคคลในระดับเดียวกัน โดยจะต้องได้รับความร่วมมือจากประเทศภาคีสมาชิกทุกประเทศซึ่งหลักการคุ้มครองสิทธิส่วนบุคคลดังกล่าวจะต้องสอดคล้องกับหลักกฎหมายภายในประเทศของตนเองด้วย[151]และต้องห้ามมิให้ส่งผ่านข้อมูลส่วนบุคคลไปสู่ประเทศที่สาม ถ้าพบว่าประเทศนั้นไม่ได้มีการรับรองต่อระดับความคุ้มครองข้อมูลส่วนบุคคลที่พึงพอ[152]

(3) ในการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมายภายในของแต่ละประเทศภาคีสมาชิก แต่หากผู้ใช้ข้อมูลได้กระทำขึ้นที่ใดก็ให้บังคับใช้กฎหมาย

---

[147] ibid, Article 17 paragraph 2.

[148] ibid, (28).

[149] ibid, (56).

[150] ibid, (7).

[151] ibid, (8).

[152] ibid, (56).

ตามประเทศนั้น[153]ถ้าผู้ใช้ข้อมูลได้กระทำหลายในประเทศ ก็ให้บังคับใช้กฎหมายตามแต่ละการกระทำในประเทศนั้นที่บังคับใช้อยู่[154]

(4) ข้อมูลส่วนบุคคลที่สามารถทำการเปิดเผยต่อบุคคลที่สามได้ แต่เจ้าของข้อมูลควรได้รับแจ้งเมื่อข้อมูลถูกบันทึก หรือได้รับการเปิดเผยต่อบุคคลที่สามเป็นครั้งแรก[155]

(5) ให้ถือว่าการใช้ข้อมูลส่วนบุคคล โดยอำนาจของหน่วยงานราชการเพื่อบรรลุวัตถุประสงค์ตามที่ระบุไว้ในกฎหมายรัฐธรรมนูญ กฎหมายระหว่างประเทศแผนกคดีเมือง หรือสมาคมทางศาสนาที่เป็นที่รู้จัก ให้ถือว่าเป็นไปเพื่อประโยชน์ของสาธรณชน[156]

(6) เมื่อเกิดการใช้ข้อมูลส่วนบุคคล ประเทศสมาชิกควรจัดหาผู้มีอำนาจที่จะทำการแนะนำหรือเป็นผู้ควบคุมการใช้ข้อมูลส่วนบุคคล เพื่อตรวจสอบกระบวนการใช้ข้อมูลส่วนบุคคลก่อนที่จะทำการใช้ข้อมูล[157]และผู้ควบคุมการใช้ข้อมูลจะต้องรับผิดชอบหากเกิดความเสียหายขึ้นจากการใช้ข้อมูลส่วนบุคคล เว้นแต่พิสูจน์ได้ว่าตนมิได้มีความรับผิดชอบต่อการใช้ข้อมูลดังกล่าว[158]

(7) เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะได้รับรู้ว่าข้อมูลของตนนั้น ได้มีการนำไปใช้ในกระบวนใด แต่ทั้งนี้ สิทธิดังกล่าวไม่ควรกระทบต่อความลับทางการค้า ตลอดจนทรัพย์สินทางปัญญาหรือลิขสิทธิ์[159]

จากบทบัญญัติข้างต้น จะเห็นได้ว่าบทบัญญัติ 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 เป็นข้อตกลงที่เป็นแนวทางในการปฏิบัติ(Guildline)ที่ชัดเจนเพื่อประเทศภาคีสมาชิกสหภาพยุโรปและประเทศที่นำบทบัญญัติดังกล่าวไปปรับใช้และได้จัดให้มีมาตรการคุ้มครองข้อมูลส่วนบุคคลซึ่งมีลักษณะการบังคับใช้กฎหมายตลอดมีวัตถุประสงค์ที่สอดคล้องกันกับบทบัญญัติข้างต้น ซึ่งจะเป็นการส่งผลให้สิทธิเสรีภาขั้นพื้นฐานของพลเมืองสหภาพยุโรป

---

[153] ibid, (18).

[154] ibid, (19).

[155] ibid, (39).

[156] ibid, (35).

[157] ibid, (54).

[158] ibid, (55).

[159] ibid, (41).

ได้รับการคุ้มครองในสิทธิความเป็นส่วนตัวที่เป็นมาตรฐานเดียวกันในแต่ละประเทศสมาชิกเท่านั้น

อย่างไรก็ตาม นอกเหนือจากมาตรการและกฎหมายทั่วไปเพื่อคุ้มครองข้อมูลส่วนบุคคล ซึ่งรวมถึงการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐด้วยตาม 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 และหลักการปฏิบัติตามแนวทางด้านการคุ้มครองความเป็นอยู่ส่วนตัวและการโอนข้อมูลส่วนบุคคลระหว่างประเทศ (Guidelines on the protection of Privacy and Transborder Data Flows of Personal Data แห่ง OECD ซึ่งกลุ่มประเทศสหภาพยุโรปได้ถือปฏิบัติกันอย่างแพร่หลายแล้ว อาจไม่เพียงพอต่อการคุ้มครองข้อมูลส่วนบุคคล ดังนั้น หลายประเทศในสหภาพยุโรปจึงมีความพยายามที่จะสร้างมาตรการที่มีความเหมาะสมกับสภาพการบริหารราชการแผ่นดินของรัฐบาลประเทศนั้นๆ โดยสอดคล้องกับหลักการทั่วไปตามที่ปรากฏใน 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 และGuidelines on the protection of Privacy and Transborder Data Flows of Personal Data ซึ่งเรียกว่า Best Practices ซึ่งหมายถึง วิธีปฏิบัติที่เป็นเลิศในการดำเนินงานเรื่องใด ซึ่งอาจไม่ใช่วิธีที่ดีและถูกต้องที่สุด แต่เป็นวิธีที่ปฏิบัติแล้วบรรลุวัตถุประสงค์ในการปฏิบัติงานสูงสุด

ทั้งนี้ อาจศึกษาได้จากโครงการ e-PRODAT ซึ่งเป็นโครงการหนึ่งของสหภาพยุโรป โดยมีวัตถุประสงค์เพื่อเป็นการส่งเสริมในการแลกเปลี่ยนความรู้และประสบการณ์ระหว่างหน่วยงานและองค์กรต่าง ๆ ของภาครัฐที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลที่ใช้งาน โดยภาครัฐตลอดจนการบริหารงานของของภาคส่วนราชการ เพื่อวัตถุประสงค์ในการให้บริการสาธารณะที่เกี่ยวข้องกับการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐ หรือ e-Government โดยมีพื้นฐานเกี่ยวกับการใช้ระบบอินเตอร์เน็ตและการเผยแพร่วิธีปฏิบัติที่เป็นเลิศ(Best Practice)อันจะส่งผลลัพธ์ที่ดีและสามารถนำไปใช้เป็นมาตรฐานต่อไป ซึ่งนอกจากหน่วยงานหรือองค์กรของรัฐในประเทศต่าง ๆ ของสหภาพยุโรปจะต้องปฏิบัติตามกฎหมายและแนวทางปฏิบัติข้างต้นแล้ว หน่วยงานหรือองค์ของรัฐของประเทศเหล่านั้น ยังต้องพยายามที่จะหาวิธีทางที่คุ้มค่าและก่อให้เกิดผลลัพธ์ที่ดีที่สุดในทางปฏิบัติ โดยมีความสอดคล้องกับหลักการคุ้มครองข้อมูลซึ่งผ่านการนำเสนอแนวทางที่สามารถปฏิบัติได้จริง[160] เช่น ปรากฏในกรณี ดังต่อไปนี้

---

[160] Francisco J. López Carmona, **Data Protection Best Practices in E-Government : Real Experience** [online], 1 July 2012. Available from http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/74.

ในประเทศเยอรมนี มีโครงการ Quasi-Niere[161]ซึ่งเป็นโครงการของรัฐบาลแห่งเยอรมนี โดยกระทรวงสาธารณสุข เพื่อทำการรักษาและบำบัดการเปลี่ยนผ่านไตของผู้ป่วยภายนอกและผู้ป่วยภายใน โดยผู้ป่วยสามารถที่จะมีบัตร Quasi-Nere ซึ่งบรรจุข้อมูลส่วนตัวทางการแพทย์ของบุคคลดังกล่าว แต่ไม่ระบุนามของผู้ป่วยและแพทย์ในการผ่าตัดปลูกถ่ายไต[162]

ในประเทศสวิตเซอร์แลนด์มีบริการท่าเรือและการขนถ่ายสินค้า(Swissport Checkport) ด่านตรวจและสายการบินสวิสแอร์ไลน์(Swiss Airlines)ซึ่งได้มีระบบการคุ้มครองข้อมูลการระบุตัวตนทางชีวภาพของผู้โดยสาร รวมถึง ระบบ การจัดเก็บข้อมูลทางชีวภาพแบบแยกส่วนโดยสมาทการ์ด(Smart Card)[163]

ในประเทศกรีซ มีการใช้ระบบ Awgen-Net[164]ซึ่งเป็นระบบการกระจายข้อมูลและโครงสร้างการสื่อสารทางไกลโดยใช้เทคโนโลยี(Telecommunication)ที่เป็นเอกลักษณ์ เช่น การเข้าถึงข้อมูลและบริการอิเล็กทรอนิกส์โดยผ่านสมาร์ทการ์ด(Smart Card)และเทคโนโลยี PKI (Public Key Infrastructure)ซึ่งเป็นระบบป้องกันข้อมูลในการสื่อสารผ่านเครือข่ายอินเตอร์เน็ต โดยมีหลักการทำงานในการใช้ระบบกุญแจคู่(Key Pairs) เพื่อทำการเข้ารหัสและถอดรหัสข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐ นอกจากนี้ ประเทศกรีซยังมีการให้บริการ e-Vehicles ในส่วนของการรักษาความปลอดภัยในการสื่อสารอิเล็กทรอนิกส์ระหว่างประชาชนและรัฐบาล ไว้สำหรับการลงทะเบียนยานพาหนะอีกด้วย[165]

จากกรณีศึกษาดังกล่าวข้างต้น จะเห็นได้ว่าแม้ว่ามาตรการหรือกฎหมายในการให้ความคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์กับภาครัฐ จะเป็นเพียงแนวปฏิบัติหรือหลักการให้ความคุ้มครองอย่างกว้าง แต่หลายประเทศในสหภาพยุโรปได้นำหลักการต่าง ๆ ไปประยุกต์ใช้ให้มีความเหมาะสมกับสภาพเศรษฐกิจและสังคม ตลอดจนความพร้อมของประชาชนของประเทศตนเองในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐ ซึ่งอาจแตกต่างกันในรายละเอียด ซึ่งแต่ละหน่วยงานหรือองค์กรได้รวบรวมแนวปฏิบัติที่ดีและมีประสิทธิภาพไว้เป็น

---

[161] ibid.

[162] Information Technology Telecommunications and Electronics Association, **Quality Assurance in Renal Care The QuaSi-Niere Card** [online], 1 July 2012. Available from http://www.intellectuk.org/Index.php?option=com_docman&task=doc_download&gid=411.

[163] Francisco J. López Carmona, **Data Protection Best Practices in E-Government : Real Experience** [online], 1 July 2012. Available from http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/74.

[164] ibid.

[165] Ibid.

Best Practice เพื่อการบริหารงานมีประสิทธิภาพสูงสุดและยังสามารถใช้เป็นแบบอย่างให้แก่หน่วยงานอื่นได้อีกด้วย

อย่างไรก็ตาม ภายใต้แนวปฏิบัติทางเทคนิคควรกระทำด้วยความระมัดระวังและต้องพิจารณาในเชิงของของกฎหมายและวัฒธรรมในท้องถิ่นนั้นด้วย ซึ่งถือเป็นการพัฒนารัฐบาลอิเล็กทรอนิกส์ หรือ e-Government ในส่วนที่อยู่นอกเหนือจากแผนการดำเนินงานหลักทั่วไป ตลอดจนต้องมีมาตรการในการประเมินผลกระทบในเรื่องของความเป็นส่วนตัวซึ่งมีความจำเป็นอย่างมาก เนื่องสิ่งเหล่านี้จะช่วยสร้างสมดุลระหว่างเสรีภาพและการคุ้มครองข้อมูลเพื่อให้การใช้รัฐบาลอิเล็กทรอนิกส์ e-Government มีประสิทธิภาพและถูกต้องตามหลักจริยธรรมมากยิ่งขึ้น[166]

จากการศึกษามาตรการคุ้มครองข้อมูลส่วนบุคคลในการทำธุกรรมอิเล็กทรอนิกส์ภาครัฐของสหรัฐอเมริกาและสหภาพยุโรป จะเห็นได้ว่าแม้รายละเอียดของกฎหมาย เช่น ในเรื่องของการเก็บข้อมูลส่วนบุคคล การเปิดเผยข้อมูลส่วนบุคคล การคัดค้านหรือยืนยันข้อมูลส่วนบุคคล ตลอดจนบทกำหนดโทษ อาจมีความแตกต่างกันในส่วนของรายละเอียดที่แต่ละประเทศได้บัญญัติขึ้นเพื่อให้สอดคล้องกับสภาพเศรษฐกิจและสังคมภายในประเทศตนเอง แต่หากวิเคราะห์สาระสำคัญของมาตรการและกฎหมายแล้วจะพบได้ว่าทั้ง The Privacy of 1974 ของประเทศสหรัฐอเมริกาและ DIRECTIVE 95/46/EC of The European Parliament and of The Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ของสหภาพยุโรป ได้มีสาระสำคัญซึ่งเป็นแนวความคิดจาก Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data แห่ง OECD ทั้งสิ้น เพียงแต่สหรัฐอเมริกาและสหภาพยุโรป มีวิธีการนำมาตรการหรือกฎหมายไปปรับใช้ในทางปฏิบัติที่แตกต่างกัน โดยประเทศสหรัฐอเมริกาจะมีการออกกฎหมายที่มีความละเอียดครอบคลุมในหลายกรณี ประกอบกับนำเทคโนโลยีที่ทันสมัยมาใช้เพื่อทำให้การคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐให้มีความปลอดภัยและมีประสิทธิภาพมากยิ่งขึ้น เช่น การใช้โปรแกรมจับคู่ข้อมูล เป็นต้น ประกอบกับรัฐบาลของสหรัฐอเมริกามีการสนับสนุนการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐอย่างต่อเนื่องและเป็นรูปธรรมจนประสบความสำเร็จกระทั่งได้รับความไว้วางใจจากประชาชนในการเข้าทำธุรกรรมอิเล็กทรอนิกส์กับหน่วยงานของรัฐอย่างแพร่หลาย ซึ่งถือเป็นความสำเร็จของรัฐบาลสหรัฐอเมริกาในการดำเนินนโยบายรัฐบาลอิเล็กทรอนิกส์

---

[166] Luciano Batista, Journal of Information, Law & Technology, The Open University Business School, **Information sharing in e-government initiatives: Freedom of Information and Data Protection issues concerning local government**[online], 21 July 2012. Available from http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2009_2/bc/bc.pdf.

ในขณะที่สหภาพยุโรป ได้มีการนำมาตรการและกฎหมายมาใช้เพื่อให้ประเทศภาคีสมาชิกนำบทบัญญัติไปปรับใช้ให้สอดคล้องกับประเทศของตนเอง แต่เนื่องจากแต่ละประเทศมีระเบียบหรือวิธีปฏิบัติในการใช้มาตรการทางกฎหมายซึ่งเกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐที่แตกต่างกัน ดังนั้น รัฐบาลแต่ละประเทศหรือหน่วยงานต่าง ๆ ของรัฐ จึงได้มีการรวบรวมแนวปฏิบัติที่เป็นเลิศหรือ Best Pratice ซึ่งเป็นการรวบรวมวิธีการปฏิบัติที่ดีที่สุดซึ่งสอดคล้องกับตามมาตรการหรือกฎหมายที่บังคับใช้อยู่ เพื่อให้บังเกิดผลในทางปฏิบัติที่มีประสิทธิภาพในการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์กับหน่วยงานของรัฐ

ดังนั้น จากการศึกษามาตรการและกฎหมายในการให้ความคุ้มครองส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐของประเทศสหรัฐอเมริกาและสหภาพยุโรปแล้ว จะเห็นได้ว่าการนำมาตรการและกฎหมายซึ่งเป็นหลักสากลระหว่างประเทศไปปรับใช้ให้เหมาะสมกับสภาพเศรษฐกิจและสังคมของประเทศตนเอง อาจไม่เพียงพอต่อการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐที่มีประสิทธิภาพ ในขณะที่ประเทศต่าง ๆ ยังต้องกำหนดมาตรการอื่นเป็นการเสริมเพื่อให้การดำเนินงานที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐมีประสิทธิภาพสูงสุด

นอกจากมาตรการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของหน่วยงานรับของซึ่งประเทศสหรัฐอเมริกาและประเทศในสหภาพยุโรปใช้บังคับแล้วนั้น ยังมีมาตรการคุ้มครองข้อมูส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ที่ได้รับความนิยมอีกวิธีหนึ่ง คือ การใช้เครื่องหมายรับรองความน่าเชื่อถือ หรือ Trust Mark ซึ่งเป็นสัญลักษณ์ที่ปรากฏอยู่บนหน้าเว็บไซต์หรือหน่วยงานเพื่อแสดงระดับการรับรองของการคุ้มครองสิทธิในเรื่องความเป็นส่วนตัวของบุคคล โดยเครื่องหมายรับรองความน่าเชื่อถือที่ได้รับความนิยมสูงสุด คือ “TRUSTe” ซึ่งมีสมาชิกมากกว่า 5000 เว็บไซต์ในปัจจุบัน[167]โดยTRUSTe Company เป็นองค์กรเอกชนที่ก่อตั้งขึ้นในประเทศสหรัฐอเมริกา ซึ่งทำการเออกครื่องหมายรับรองความน่าเชื่อถือโดยไม่แสวงหากำไรให้แก่เว็ปไซต์ที่มีมาตรคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ที่ได้รับมาตรฐาน ซึ่งต่อมาได้เปลี่ยนแนวทางมาเป็นองค์แสวงหากำไรในภายหลัง[168]

---

[167] TRUSTe, **About TRUSTe** [online], 21 July 2012. Available from http://www.truste.com/about-TRUSTe/.

[168] Chris Connolly, **Trustmark Schemes Struggle to Protect Privacy**[online], 21 July 2012. Available from http://www.galexia.com/public/research/assets/trustmarks_struggle_20080926/trustmarks_struggle_public.pdf.

ทั้งนี้ TRUSTe Company มีความพยายามที่จะทำการยกระดับมาตรการคุ้มครองข้อมูลส่วนบุคคลให้มีประสิทธิภาพมากยิ่งขึ้น จึงได้ร่วมกับกระทรวงพาณิชย์ของสหรัฐอเมริกา (Department of Commerce : DOC)[169]และสหภาพยุโรปเพื่อทำการพัฒนาโปรแกรม TRUSTe EU Safe Harbour Privacy Seal เพื่อทำการรับรองเครื่องหมายรับรองความน่าเชื่อถือให้สอดคล้องกับแนวทางตาม DIRECTIVE 95/46/EC of The European Parliament and of The Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[170]ได้บัญญัติเอาไว้ โดยในทางปฏิบัติ TRUSTe ในระยะแรกเริ่มได้ใช้เครื่องหมายรับรองความน่าเชื่อถือ เรื่องความเป็นส่วนตัวเอาไว้ 3 สี ซึ่งบ่งชี้การเก็บข้อมูลหรือการเปิดเผยข้อมูลส่วนบุคคล โดยมีแนวคิดเริ่มแรกว่าให้เว็บไซต์นำเสนอ 3 สัญลักษณ์ ว่ามีมาตรฐานความเป็นส่วนตัวในระดับคุณภาพดี คุณภาพปานกลาง หรือคุณภาพแย่ ซึ่งแนวคิดนี้ได้กลายเป็นปัญหาโดยที่เว็บไซต์ส่วนใหญ่ไม่ต้องการแสดงสัญลักษณ์ดังกล่าวว่ามาตรฐานคุ้มครองของเว็บไซต์ตนเองอยู่ในระดับใด ดังนั้น จึงเห็นควรที่จะมีสัญลักษณ์ เครื่องหมายรับรองความน่าเชื่อถือเรื่องความเป็นส่วนตัวแบบเดียวที่สมาชิกทุกเว็บไซต์ใช้ได้เหมือนกัน ซึ่งหมายความว่าทุกเว็บไซต์มีนโยบายด้านความเป็นส่วนตัว ซึ่งทำให้การบังคับใช้มีประสิทธิภาพมากกว่า

ดังนั้นจะเห็นได้ว่า นอกเหนือจากหน่วยงานรัฐที่พยายามให้ความคุ้มครองกับข้อมูลส่วนบุคคลที่รัฐกำกับดูแลอยู่ซึ่งหมายความรวมถึงข้อมูลในการทำธุรกรรมอิเล็กทรอนิกส์ของหน่วยงานรัฐด้วยนั้น ภาคเอกชนก็ได้ให้ความสำคัญกับการป้องกันปัญหาต่าง ๆ ที่จะเกิดขึ้นกับมการใช้ข้อมูลส่วนบุคคลด้วยวิธีการทางอิเล็กทรอนิกส์ ซึ่งเป็นสิ่งสำคัญที่ทุกหน่วยงานทุกภาคส่วนทั้งภาครัฐและภาคเอกชนจะต้องร่วมมือกันต่อไป

---

[169] Department of Commerce, United States of America, **Media Contacts**[online], 21 July 2012. Available from http://www.commerce.gov/contact/media-contacts.

[170] TRUSTe, **Pan to Europe the Right Way** [online], 21 July 2012. Available from http://www.truste.com/products-and-services/enterprise-privacy/eu-safe-harbor-seal.

บทที่ 5
บทสรุปและข้อเสนอแนะ

5.1 บทสรุป

ในปัจจุบันภาครัฐของไทยเริ่มมีการนำเทคโนโลยีสนเทศมาปรับใช้ในการให้บริการแก่ประชาชนเพื่อเป็นการอำนวยความสะดวก และเป็นการเปิดโอกาสให้ประชาชนได้รับการบริการจากหน่วยงานของรัฐอย่างทั่วถึงและเป็นธรรม ซึ่งเป็นไปตามโครงการรัฐบาลอิเล็กทรอนิกส์ (e-Government)แต่ปัญหาการกระทำความผิดที่เกี่ยวข้องกับข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของหน่วยงานของรัฐของประเทศไทย ยังไม่ปรากฏข้อเท็จจริงที่สามารถนำมาเป็นกรณีศึกษาได้ อีกทั้งในทางปฏิบัติเป็นการยากที่หน่วยงานของรัฐจะเปิดเผยถึงข้อผิดพลาดและความเสียหายในการจัดเก็บข้อมูลส่วนบุคคลตลอดจนมาตรการคุ้มครองข้อมูลส่วนบุคคลโดยละเอียด เพราะหากแม้มีกรณีที่เกิดขึ้นจริง ความเสียหายอาจยังไม่ได้รับการเปิดเผย เนื่องจากการเปิดเผยถึงข้อผิดพลาดในมาตรการคุ้มครองข้อมูลส่วนบุคคลหรือข้อมูลอื่นของหน่วยงานรัฐอาจส่งผลกระทบต่อบุคคลและเจ้าหน้าที่ที่เกี่ยวข้องหลายฝ่ายรวมถึงหน่วยงานและอาจทำให้ภาพลักษณ์ขององค์กรเสื่อมเสีย ซึ่งอาจทำให้ความเชื่อมั่นในการทำธุรกรรมอิเล็กทรอนิกส์และธุรกรรมอื่นของประชาชนลดลง

ดังนั้น จะเห็นได้ว่า ข้อมูลหรือข้อมูลส่วนบุคคลซึ่งอยู่ในความดูแลของหน่วยงานของรัฐมีความสำคัญเป็นอย่างมาก หน่วยงานของรัฐจำเป็นต้องแบ่งแยกประเภทของหน่วยงานที่มีข้อมูลส่วนบุคคล ตามระดับของผลกระทบหรือระดับความเสียหายที่อาจเกิดขึ้นหากมีการกระทำความผิดต่อข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของหน่วยงานรัฐเกิดขึ้นจริง โดยเฉพาะอย่างยิ่งหน่วยงานที่ทำการจัดเก็บข้อมูลส่วนบุคคลมีความสำคัญและมีความอ่อนไหวเป็นพิเศษ เช่น สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ กระทรวงกลาโหม กระทรวงการต่างประเทศ ธนาคารแห่งประเทศไทย และธนาคารพาณิชย์ที่เป็นรัฐวิสาหกิจ เป็นต้น ซึ่งหน่วยงานของรัฐจะต้องจัดเตรียมระบบหรือมาตรการในการให้ความคุ้มครองข้อมูลส่วนบุคคลที่มีความเข้มงวดมากขึ้น

สารนิพนธ์ฉบับนี้ จึงเป็นการนำเสนอมาตรการในการให้ความคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของหน่วยงานของรัฐ ซึ่งประเทศสหรัฐอเมริกาและประเทศกลุ่มสหภาพยุโรปได้บังคับใช้อยู่ในปัจจุบันและยังไม่ได้มีการนำมาตรการดังกล่าวมาใช้ในประเทศไทย ตลอดจนเป็นการศึกษาเพื่อเฝ้าระวังการกระทำความผิดต่อข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ที่หน่วยงานของรัฐควบคุมหรือดูแลอยู่ ซึ่งอาจจะเกิดขึ้นได้ในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐ เนื่องจากการทำธุรกรรมอิเล็กทรอนิกส์ได้ถูกพัฒนาและได้มีการใช้ในการทำธุรกรรมของภาคเอกชนก่อน ต่อมารัฐบาลของหลายประเทศจึงได้มีการนำการทำธุรกรรมอิเล็กทรอนิกส์มาใช้ในการให้บริการกับประชาชนของประเทศตน ซึ่งจะเห็นได้ว่าการทำธุรกรรมอิเล็กทรอนิกส์ของภาคเอกชนได้มีปัญหาเกิดขึ้นหลายกรณี เช่น การนำฐานข้อมูลส่วนบุคคลของลูกค้าไปขายเพื่อประโยชน์ทางการตลาด ตลอดจนการนำข้อมูลทางบัตรอิเล็กทรอนิกส์ไปใช้โดยมิชอบ เป็นต้น ซึ่งที่ตลอดระยะเวลาที่ผ่านมาระบบการป้องกันข้อมูลและระบบการทำงานขององค์กรเอกชนขนาดใหญ่ ค่อนข้างจะมีประสิทธิภาพในการทำงานและสามารถปกป้องข้อมูลที่เก็บรักษาไว้ได้ดีกว่าหน่วยงานของรัฐ เช่น สถาบันการเงินขนาดใหญ่ เป็นต้น แต่หน่วยงานของภาคเอกชนหลายแห่งก็ไม่สามารถปกป้องข้อมูลต่าง ๆ ในความครอบครองดูแลของตนให้พ้นจากผู้กระทำความผิดได้ ดังนั้น การที่หน่วยงานของรัฐนำการทำธุรกรรมอิเล็กทรอนิกส์มาใช้ในการให้บริการกับประชาชน จำเป็นต้องมีมาตรการและกฎหมายที่มีความรัดกุมและมีประสิทธิภาพในการบังคับใช้ เพื่อความไม่ประมาทในการดำเนินงานของภาครัฐ

ทั้งนี้ ปัญหาดังกล่าว ล้วนแต่เป็นปัญหาสำคัญที่ส่งผลกระทบต่อประชาชนในหลายประเทศทั่วโลก ดังนั้น การที่รัฐบาลได้นำเอาการทำธุรกรรมอิเล็กทรอนิกส์มาใช้กับหน่วยงานของรัฐ มีความจำเป็นอย่างยิ่งที่จะต้องตระหนักและทำความเข้าใจถึงปัญหาที่อาจเกิดขึ้นกับหน่วยของรัฐในการให้บริการกับประชนดังที่เคยเกิดขึ้นกับภาคเอกชน ดังนั้น การคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ของภาครัฐมีความจำเป็นที่จะต้องมีมาตรการป้องกันที่ดีและมีการเฝ้าระวังปัญหาที่อาจจะเกิดขึ้นได้ ดังนั้น จึงได้นำเสนอมาตรการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐของประเทศสหรัฐอเมริกา สหภาพยุโรปและประเทศไทย เนื่องจากประเทศสหรัฐอเมริกาได้มีการนำธุรกรรมอิเล็กทรอนิกส์มาใช้กับภาครัฐเป็นประเทศแรก ๆ และประเทศสหรัฐอเมริกาก็เป็นหนึ่งหลายประเทศที่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ดีที่สุด อีกทั้ง สหภาพยุโรปได้มีแนวทางการคุ้มครองข้อมูลส่วน

บุคคลที่ดีและมีประสิทธิภาพ ซึ่งหลายประเทศทั่วโลกได้นำไปเป็นแนวทางในการปรับใช้ให้เหมาะสมกับกฎหมายภายในและสภาพสังคมของประเทศตนเอง

ทั้งนี้ เพื่อแสวงหาแนวทางการพัฒนามาตรการและกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐของไทยให้มีประสิทธิภาพและมีมาตรฐานในระดับสากลมากยิ่งขึ้น เนื่องจาก ในปัจจุบันมาตรการและกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลของภาครัฐของไทยยังไม่มีมาตรการที่รัดกุมเพียงพอ ซึ่งยังต้องพัฒนาในเรื่องของการตรวจสอบแหล่งที่มาของข้อมูลส่วนบุคคลและการคุ้มครองข้อมูลส่วนบุคคลที่หน่วยงานของรัฐกำกับดูแลอยู่ ตลอดจนต้องพัฒนาการตรวจสอบข้อมูลส่วนบุคคลก่อนมีการประมวลผลให้มีความถูกต้องและเป็นปัจจุบัน รวมถึงต้องหามาตรการเสริมในทางปฏิบัติเพื่อให้การบังคับใช้กฎหมายและมาตรการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ให้มีประสิทธิภาพและสามารถบังคับใช้ได้จริงโดยสอดคล้องกับหลักเกณฑ์ที่กำหนดไว้

5.2 ข้อเสนอแนะ

5.2.1 เห็นควรให้ประเทศไทยทำการจัดตั้งหน่วยงานหรือองค์กรซึ่งอยู่ภายใต้การกำกับดูแลโดยภาครัฐและทำหน้าที่เป็นหน่วยงานกลางในการออกหลักเกณฑ์เพื่อกำกับดูแลในการคุ้มครองข้อมูลส่วนบุคคลให้มีประสิทธิภาพและมีความมั่นคงปลอดภัย และเพื่อให้หน่วยงานต่าง ๆ ทั้งภาครัฐและภาคเอกชนได้นำหลักเกณฑ์ที่กำหนดขึ้นไปปรับใช้ในหน่วยงานหรือองค์กรของตนให้สอดคล้องกับหลักเกณฑ์ที่หน่วยงานกลางกำหนดไว้ ซึ่งหมายความรวมถึงหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐด้วย โดยอาจให้มีมาตรการในการออกเครื่องหมายรับรองความน่าเชื่อถือ(Trust Marks)ให้แก่หน่วยงานของรัฐหรือเอกชนที่มีมาตรการคุ้มครองข้อมูลส่วนบุคคลและมีมาตรการรักษาความปลอดภัยในระบบสารสนเทศที่เหมาะสมตามหลักเกณฑ์ที่หน่วยงานดังกล่าวกำหนด โดยเครื่องหมายรับรองความน่าเชื่อถือ(Trust Marks)จะเป็นสิ่งยืนยันว่าหน่วยงานดังกล่าวผ่านมาตรฐานในระดับปลอดภัยและให้ความมั่นใจกับประชาชนในการเข้าทำธุรกรรมทางอิเล็กทรอนิกส์กับภาครัฐได้ ไม่ใช่เพียงแค่เป็นการผ่านการประเมินในระดับมาตรฐานขั้นต่ำซึ่งหน่วยงานใดผ่าน

การรับรองความน่าเชื่อถือจากคณะกรรมการแล้วจะได้รับสิทธิในการแสดงเครื่องหมายรับรองความน่าเชื่อถือให้ประชาชนได้รับรู้ซึ่งหากประชาชนสามารถรับรู้และทำความเข้าใจกับเครื่องหมายในเชิงสัญลักษณ์(Symbolic)ได้มากกว่าการติดตามข้อมูลข่าวสารทางราชการจากประกาศเป็นเอกสารหรือข้อความต่าง ๆ ทั้งนี้ เพื่อเป็นการสร้างความเชื่อมั่นให้กับประชาชนผู้ใช้บริการให้มีความมั่นใจในการให้ข้อมูลที่แท้จริงกับรัฐ เพื่อประโยชน์สูงสุดในการให้บริการกับประชาชน

5.2.2 เห็นควรให้ประเทศไทยมีการรวบรวมวิธีการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์กับหน่วยงานของรัฐ ซึ่งอาจไม่ใช่เป็นบทบัญญัติของกฎหมายก็ได้ แต่เป็นมาตรการหรือวิธีการทางเทคนิค(Technical)ที่ดีและมีประสิทธิภาพไว้เหมือนดังที่สหภาพยุโรปมีการจัดทำ Best practice ในโครงการ e-PRODAT ซึ่งจะต้องทำการรวบรวมไว้ให้ประชาชนหรือหน่วยงานของรัฐสามารถทำการศึกษาได้ แม้ว่าวิธีการปฏิบัติที่เป็นเลิศของแต่ละหน่วยงานหรือองค์กรอาจจะไม่สามารถใช้ได้เหมือนกัน แต่ก็เป็นการรวบรวมสิ่งที่ดีซึ่งปฏิบัติแล้วมีประสิทธิภาพในการดำเนินงาน เพื่อให้ใช้เป็นแนวทางในการศึกษาและปรับปรุงมาตรการต่าง ๆ ให้เหมาะสมกับหน่วยงานของตนเองต่อไป

5.2.3 นอกจากความรับผิดทางอาญาแก่ผู้กระทำความผิดต่อข้อมูลส่วนบุคคลไม่ว่าจะกระทำโดยเจตนาหรือมิได้มีเจตนาแล้ว เห็นควรให้มีการเยียวยาทางแพ่งในกรณีที่เกิดความเสียหายอันเนื่องมาจากการประมวลผลข้อมูลส่วนบุคคลของหน่วยงานของรัฐไม่ว่าเพื่อวัตถุประสงค์ใด ตลอดจนความเสียหายอันเกิดจากความล้มเหลวของระบบรักษาความปลอดภัยในการรักษาคุ้มครองข้อมูลส่วนบุคคล เหมือนดังที่ The Privacy Act of 1974 แห่งสหรัฐอเมริกา ตามมาตรา (g) ที่ได้บัญญัติให้ กรณีที่บุคคลได้รับความเสียหายจากการปฏิเสธการแก้ไขข้อมูลจากหน่วยงานของรัฐ หรือกรณีที่บุคคลได้รับความเสียหายอันเกิดจากการได้รับการปฏิเสธการขอเข้าถึงข้อมูลส่วนบุคคลของหน่วยงานของรัฐ หรือในกรณีบุคคลได้รับความเสียหายจากการที่หน่วยงานของรัฐประสบความล้มเหลวของระบบรักษาความปลอดภัยในการรักษาคุ้มครองข้อมูลส่วนบุคคล ตลอดจนบุคคลที่ได้รับความเสียหายจากหน่วยงานของรัฐที่ล้มเหลวที่จะปฏิบัติตามข้อกำหนดของการเยียวยาทางแพ่ง ทั้งนี้ ความเสียหายจะต้องครอบคลุมถึงความ

เสียหายที่เป็นนามธรรมและรูปธรรม โดยคำนึงฐานะทางสังคม ตลอดจนชื่อเสียง และหน้าที่การงานของผู้เสียหายในการประเมินความเสียหายด้วย

5.2.4 เห็นควรให้หน่วยงานของรัฐมีการปรับปรุงแนวทางการปฏิบัติงานด้านการรักษาความปลอดภัยของระบบสารสนเทศและข้อมูลที่สำคัญต่าง ๆ ให้มีความเป็นสากลและเหมาะสมกับการพัฒนาในประเทศ ไม่ว่าจะเป็นการทำธุรกรรมระหว่างหน่วยงานของรัฐด้วยกันเองหรือระหว่างหน่วยงานของรัฐกับเอกชน ซึ่งตามความในมาตรา 4 แห่งพระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553 ได้ทำการแบ่งระดับของวิธีการแบบปลอดภัยเอาไว้ 3 ระดับ ได้แก่ ระดับเคร่งครัด ระดับกลาง และระดับพื้นฐาน โดยเห็นควรให้มีการกำหนดมาตรฐานกลางว่าวิธีการแบบปลอดภัยระดับใด ควรมีขั้นตอนในดำเนินงานและมีมาตรการใดคุ้มครองข้อมูลดังกล่าวอย่างไรจึงจะเหมาะสม แล้วจึงทำการจำแนกหน่วยงานต่าง ๆ ของรัฐเป็นกลุ่มซึ่งเรียงตามลำดับความร้ายแรงแห่งผลกระทบที่อาจจะเกิดขึ้นหากมีกรณีที่มีความเสียหายต่อข้อมูลส่วนบุคคลซึ่งหน่วยงานของรัฐนั้นดูแลอยู่ เช่น กลุ่มที่ข้อมูลมีความอ่อนไหวเป็นพิเศษ(Sensitive Data) เช่น ธนาคารของรัฐหรือกระทรวงกลาโหม เป็นต้น แล้วจึงนำระดับการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมมาปรับใช้กับกลุ่มหน่วยงานดังกล่าวในเบื้องต้น ซึ่งหากมีความจำเป็นหน่วยงานใดของรัฐอาจออกกฎเกณฑ์เพิ่มเติมก็ได้ ทั้งนี้ เพื่อให้ประชาชนไม่เกิดความสับสนในการขอตรวจสอบข้อมูลส่วนบุคคลในเบื้องต้น เพราะ แต่ละหน่วยงานมีพื้นฐานทางด้านมาตรการรักษาความปลอดภัยที่สอดคล้องกันซึ่งจะไม่เป็นการปิดกั้นข้อมูลระหว่างหน่วยงานของรัฐด้วยกันเอง

5.2.5 การขอความยินยอมเป็นหนังสือจากเจ้าของข้อมูลส่วนบุคคลซึ่งได้ขอความยินยอมก่อนหรือขณะมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลนั้น เห็นควรบัญญัติให้ครอบคลุมถึงวิธีการอื่นด้วย เนื่องจากการทำธุรกรรมเป็นหนังสือ(กระดาษ) อาจขัดต่อการสนับสนุนการใช้การทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐซึ่งมีการสนับสนุนให้ใช้ระบบเทคโนโลยีสารสนแทนการใช้เอกสารแบบเดิม

5.2.6. ทั้งนี้ เพื่อความมีประสิทธิภาพในการบริการจัดการเห็นควรแบ่งระดับข้อมูลออกเป็นข้อมูลทั่วไป เช่น ชื่อ นามสกุล ที่อยู่ เพศ และอายุ เป็นต้น ซึ่งข้อมูลดังกล่าวเป็นข้อมูลทั่วไปซึ่งสามารถเปิดเผยและทำการส่งข้อมูลระหว่างหน่วยงานได้โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูล แต่ทั้งนี้ แม้ว่าจะไม่ต้องขอความยินยอมจากเจ้าของข้อมูล แต่ก็มีการแจ้งให้เจ้าของข้อมูลทราบเมื่อมีการประมวลผลข้อมูลส่วนบุคคลนั้นเสมอ ไม่ว่าจะใช้ในวัตถุประสงค์ใด

นอกจากนี้ ต้องแบ่งข้อมูลออกเป็นข้อมูลที่มีความอ่อนไหวเป็นพิเศษ(Sensitive Data) เช่น เชื้อชาติ โรคประจำตัว และข้อมูลด้านอาชญากร เป็นต้น ซึ่งหน่วยงานของรัฐจะต้องขอความยินยอมจากประชาชนผู้ให้ข้อมูลโดยตรง เท่านั้น นอกจากนี้หน่วยงานของรัฐต้องทำการแจ้งหรือประกาศถึงวัตถุประสงค์ในการเก็บข้อมูล และลักษณะการนำข้อมูลไปใช้ว่าจะมีการส่งต่อข้อมูลหรือเปิดเผยข้อมูลหรือไม่อย่างไร เพื่อให้ประชาชนได้ทราบก่อนหรือทราบขณะทำธุรกรรมใดกับหน่วยงานของรัฐ ซึ่งหมายความรวมถึงการทำธุรกรรมทางอิเล็กทรอนิกส์ด้วย

5.2.7 เห็นควรให้หน่วยงานของรัฐเร่งให้มีมาตรการทางกฎหมายที่ให้ความคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปซึ่งมีความครอบคลุมที่กว้างกว่ากฎหมายเฉพาะ เช่น กรณีพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ซึ่งบังคับใช้อยู่ในปัจจุบัน ทั้งนี้ เพื่อให้ความคุ้มครองเป็นหลักเกณฑ์พื้นฐานในการกระทำใดเกี่ยวกับข้อมูลส่วนบุคคล เว้นแต่ หน่วยงานใดมีความจำเป็นพิเศษในการดำเนินงานก็อาจออกกฎเกณฑ์เป็นข้อยกเว้นได้ตามความจำเป็น ทั้งนี้ อาจเป็นร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... ซึ่งในปัจจุบันอยู่ระหว่างกระบวนการนิติบัญญัติ

ทั้งนี้ เนื่องจากร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... มีผลบังคับใช้ได้ทั้งหน่วยงานของภาครัฐซึ่งมีประโยชน์สาธารณะเป็นจุดมุ่งหมายสูงสุดในการดำเนินงานและหน่วยงานภาคเอกชนซึ่งมีผลตอบแทนหรือกำไรเป็นจุดหมายสูงสุดในการดำเนินงาน ดังนั้นกฎหมายฉบับนี้จะสามารถรักษาสมดุลในการบังคับใช้กฎหมายได้อย่างไร ซึ่งอาจต้องทำการศึกษาถึงผลกระทบให้ดีก่อนมีการนำพระราชบัญญัติฉบับนี้มาประกาศใช้ เพราะหากมีผลเสียอาจจะส่งกระทบในวงกว้างครอบคลุมหลายภาคส่วน อย่างไรก็ตาม การเร่งให้มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลมาบังคับใช้ก็เป็นสิ่งที่พึงปรารถนา เพื่อที่ประชาชนและผู้บริโภคจะได้รับความคุ้มครองในสิทธิส่วนบุคคลที่มีประสิทธิภาพมากยิ่งขึ้น

5.2.8 จากการศึกษาและพิจารณาพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ตลอดจนมาตรการคุ้มครองมูลส่วนบุคคลของประเทศไทยที่ปรากฏในสารนิพนธ์ฉบับนี้ ยังไม่พบมาตรการในการยืนยันความถูกต้องของข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมว่าผู้ให้ข้อมูลส่วนบุคคลนั้น ได้ให้ข้อมูลที่ถูกต้องตามความเป็นจริงหรือไม่ ซึ่งหากไม่มีกระบวนการตรวจสอบข้อมูลนำเข้าให้มีประสิทธิภาพ อาจเกิดผลกระทบและเกิดความเสียหายเหมือนดังกรณีที่ร้านขายสินค้าทำการยื่นเสียภาษีเงินได้บุคคลธรรมดาโดยใช้ชื่อของบุคคลอื่นจำนวนหลายคนโดยทุจริต เพื่อทำการหลีกเลี่ยงการชำระภาษีในจำนวนมาก ซึ่งผู้เสียหายบางรายอาจไม่ทราบถึงข้อเท็จจริงดังกล่าวเลย หรืออาจทราบแต่กว่าที่จะมีการดำเนินกระบวนพิจารณาตามขั้นตอนต้องใช้เวลาและค่าใช้จ่ายจำนวนมาก ซึ่งก่อให้เกิดความเสียหายอันเนื่องมาจากการไม่มีมาตรการยืนยันความถูกต้องข้อมูลส่วนบุคคลในขณะนำข้อมูลเข้าสู่ระบบการให้บริการอิเล็กทรอนิกส์ของหน่วยงานของรัฐ

บรรณานุกรม

กรมการกงสุล. กระทรวงการต่างประเทศ. (ม.ป.ป.). ค้นเมื่อ 4 พฤษภาคม 2555, จาก http://www.consular.go.th.

กองหนังสือเดินทาง. กรมการกงสุล. กระทรวงการต่างประเทศ. (ม.ป.ป.). หนังสือเดินทางอิเล็กทรอนิกส์กับการคุ้มครองข้อมูลส่วนบุคคล. เอกสารประกอบการสัมนา“ธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐกับการคุ้มครองข้อมูลส่วนบุคคล”. ค้นเมื่อ 28 พฤษภาคม 2555, จาก http://www.etcommission.go.th/index.php?option=com_content&view=article&id=170&Itemid=8&lang=th.

กองหนังสือเดินทาง. กรมการกงสุล. กระทรวงการต่างประเทศ. (ม.ป.ป.). รายงานประจำปีงบประมาณ 2553. ค้นเมื่อ 4 พฤษภาคม 2555, จาก http://www.consular.go.th.

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. (ม.ป.ป.). ค้นเมื่อ 22 มีนาคม 2555, จาก http://www.mict.go.th/.

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. (2554). กรอบนโยบายเทคโนโลยีสารสนเทศและการสื่อสารระยะ พ.ศ.2554-2563 ของประเทศไทย (ICT2020). ค้นเมื่อ 2 พฤษภาคม 2555 จาก www.ict2020.in.th.

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553. ค้นเมื่อ 4 พฤษภาคม 2555, จาก http://www.etcommission.go.th.

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของประเทศด้านสารสนเทศของหน่วยงานรัฐ พ.ศ. 2553, ค้นเมื่อ 4 พฤษภาคม 2555, จาก http://www.etcommission.go.th.

ประมวลกฎหมายอาญา. แก้ไขเพิ่มเติมฉบับที่ 21 พ.ศ. 2551. ค้นเมื่อ 7 มิถุนายน 2555, จาก http://www.krisdika.go.th.

ประมวลกฎหมายแพ่งและพาณิชย์. แก้ไขเพิ่มเติมฉบับที่ 19 พ.ศ. 2551. ค้นเมื่อ 7 มิถุนายน 2555, จาก http://www.krisdika.go.th.

พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549. ค้นเมื่อ 5 มิถุนายน 2555, จาก http://www.krisdika.go.th.

พระราชกฤษฎีกาจัดตั้งสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ. 2554. ค้นเมื่อ 5 มิถุนายน 2555, จาก www.opdc.go.th/uploads/files/PO/30.pdf.

พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553. ค้นเมื่อ 5 มิถุนายน 2555, จาก http://www.etcommission.go.th.

พระราชกฤษฎีกาแบ่งส่วนราชการกรมการกงสุล กระทรวงการต่างประเทศ พ.ศ. 2541. ค้นเมื่อ 4 พฤษภาคม 2555, จาก www.lawreform.go.th.

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540. ค้นเมื่อ 27 พฤษภาคม 2555, จาก http://www.krisdika.go.th.

พระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544. ค้นเมื่อ 5 มิถุนายน 2555, จาก http://www.krisdika.go.th.

พระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม พ.ศ. 2545. ค้นเมื่อ 9 พฤษภาคม 2555, จาก http:// www.office.mict.go.th/file/law.pdf

รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550. ค้นเมื่อ 7 พฤษภาคม 2555, จาก http://www.krisdika.go.th.

ร่างพระราชบัญญัติข้อมูลส่วนบุคคล พ.ศ.... ร่างที่สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้ว เรื่องเสร็จที่ 515/2552. ค้นเมื่อ 27 พฤษภาคม 2555, จาก http://www.krisdika.go.th.

มูลนิธิเพื่อนผู้บริโภค. (ม.ป.ป.). ลูกหนี้บัตรเครดิตโวยถูกขายข้อมูลส่วนตัว สปส.เต้นขู่เชือด พนง.. ค้นเมื่อ 29 มีนาคม 2555, จาก http://old.consumerthai.org.

รัฐบาลอิเล็กทรอนิกส์. (ม.ป.ป.). e-Government คืออะไร. ค้นเมื่อ 4 มิถุนายน 2555, จาก http://www.dld.go.th/ict/article/egov/e-gev02.html.

วรรณศรี ทิวแพ. (2550). **การกำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคล : ศึกษาเฉพาะกรณีบัตรประจำตัวประชาชนแบบอเนกประสงค์**. การค้นคว้าอิสระ. ปริญญามหาบัณฑิต, มหาวิทยาลัยศรีนครินทรวิโรฒ.

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ. (ม.ป.ป.). กรอบนโยบายเทคโนโลยีสารสนเทศและ การสื่อสารระยะ พ.ศ.2544-2553. ค้นเมื่อ 22 มีนาคม 2555, จาก http://www.nectec.or.th.

ศูนย์บริการข้อมูลเศรษฐกิจระหว่างประเทศ. กรมเศรษฐกิจระหว่างประเทศ. กระทรวงการต่างประเทศ. (ม.ป.ป.). กรอบความร่วมมือเศรษฐกิจระหว่างประเทศ. ค้นเมื่อ 10 เมษายน 2555, จาก http://www.mfa.go.th/business/2026.php.

สถาบันส่งเสริมความเป็นเลิศทางเทคโนโลยี RFID แห่งประเทศไทย. (ม.ป.ป.). คำแนะนำเทคโนโลยี RFID. ค้นเมื่อ 15 มิถุนายน 2555, จาก http://www.rfid.or.th/th/technology/know.asp.

สำนักข่าวไทย. (ม.ป.ป.). อลิโคญี่ปุ่นทำข้อมูลบัตรเครดิตลูกค้ารั่วไหล. ค้นเมื่อ 31 พฤษภาคม 2555, จาก http://news.mcot.net.

สำนักงานคณะกรรมการอิเล็กทรอนิกส์. (ม.ป.ป.). ประกาศรายชื่อหน่วยงานที่จัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและผ่านความเห็นชอบจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์. ค้นเมื่อ 3 พฤษภาคม 2555, จาก http://www.etcommission.go.th.

สำนักงานคณะกรรมการพัฒนาธุรกรรมอิเล็กทรอนิกส์(องค์การมหาชน). (ม.ป.ป.). เกี่ยวกับ สพธอ. ค้นเมื่อ 2 มิถุนายน 2555, จาก http://www.etda.or.th/main/contents/display/35.

สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. (2552). **บทสรุปผู้บริหาร : แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร (ฉบับที่ 2) ของประเทศไทย พ.ศ. 2552-2556**, (ม.ป.พ.). 1-3.

สำนักงานผู้ดูแลนักเรียนไทยในประเทศฝรั่งเศส. (ม.ป.ป.). สำนักงานคณะกรรมการข้าราชการพลเรือน. ต้องต่อหนังสือเดินทางที่ใด. ค้นเมื่อ 21 กรกฎาคม 2555, จาก http://oeaparis.online.fr/article.php3?id_article=1&id_section=1.

สำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์(องค์กรมหาชน). (ม.ป.ป.). หลักเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคลของผู้บริโภคตามแนวทางขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา. ค้นเมื่อ 1 พฤษภาคม 2555, จาก http://www.etda.or.th/main/contents/display/337.

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์กรมหาชน)(สรอ.). (ม.ป.ป.). ประวัติความเป็นมา. ค้นเมื่อ 24 พฤษภาคม 2555, จาก http://www.ega.or.th.

สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์. (2546). **แนวทางการจัดทำกฎหมายคุ้มครองข้อมูลส่วนบุคคล**, (ม.ป.พ.). ค้นเมื่อ 20 พฤษภาคม 2555, จาก www.lawreform.go.th.

สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ. **รายงานการประเมินผลนโยบายเทคโนโลยีสารสนเทศ IT2000**, (ม.ป.พ.). ค้นเมื่อ 20 พฤษภาคม 2555, จาก www.nectec.or.th/pld/documents_pris/IT2000%20Report.pdf

ASTV ผู้จัดการออนไลน์. (ม.ป.ป.). 50 องค์กรมะกันป่วน ถูกขโมยข้อมูลลูกค้า. ค้นเมื่อ 29 มีนาคม 2555, จาก http://www.manager.co.th.

Adam Lebech. (n.d.). Privacy and e-government Enterprise Challenges for Danish Government. Danish ministry of Finance. IBM Privacy Technology Summit 9-10 July 2003. Retrieved May, 1, 2012, from http://www.zurich.ibm.com/pdf/privacysummit/Lebech.pdf.

Ben Bratman. (2002). The Right to Privacy and the Birth of the Right to Privacy". (Vol. 69). Tennessee Law Review. University of Pittsburgh Legal Studies Research Paper. 623. Retrieved May, 1, 2012, from http://papers.ssrn.com/sol3/papers.cfm?abstract_id =1334296

Cable News Network (CNN). (n.d.). Interpol Puts Assange on Most-Wanted List. Retrieved July, 18, 2012, from http://edition.cnn.com/2010/WORLD/europe/11/30 /sweden.interpol.assange/index.html.

Cable News Network (CNN). (n.d.). Leaked video reveals chaos of Baghdad attack. Retrieved July, 18, 2012, from http://edition.cnn.com/2010/WORLD/meast/04/06 /iraq.journalists.killed/index.html.

China Electronic and Governance. (n.d.). Wikileaks Releases Unsurprising China. Retrieved July, 18, 2012, from Cableshttp://chinaelectionsblog.net/?p=11043.

Chris Connolly. (n.d.). Trustmark Schemes Struggle to Protect Privacy. Retrieved July, 21, 2012, from http://www.galexia.com/public/research/assets/trustmarks_str uggle_20080926/trustmarks_struggle_public.pdf.

Department of Homeland Security. United States of America. (n.d.). Media Contacts. Retrieved May, 24, 2012, from http://www.commerce.gov/contact/media-contacts.

Department of Economic and Social Affairs. (n.d.). Population Division. United Nations. World Population Prospects : The 2010 Revision. Retrieved June, 6, 2012, from http:// www.irs.gov/irs/article/0,,id=183728,00.html.

Defense Privacy and Civil Liberties Office. (n.d.). About the Office. Retrieved July, 1, 2012, from http://dpclo.defense.gov/privacy/about_The_Office/about_the_office.html.

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. Retrieved June, 6, 2012, from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

Eleni K., Martin M., Marit H. & Mark G. (n.d.). An analysis of security and privacy issues relating to RFID enabled ePassports. Retrieved June, 5, 2012, from ihttp://www.few.vu.nl/~mconti/teaching/ATCNS2010/ATCS/RFIDpassport/kosta.pdf.

European Union. (n.d.). Council of the European Union. Retrieved July, 1, 2012, from http://www.consilium.europa.eu/homepage?lang=en.

European Union. (n.d.). European Commission. Retrieved July, 1, 2012, from http://ec.europa.eu/index_en.htm.

European Union. (n.d.). European Parliament. Retrieved July, 1, 2012, from http://www.europarl.europa.eu/.

European Union. (n.d.). EUR-Lex Access to European Union Law. Retrieved June, 4, 2012, from http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0087:en:NOT.

Executive Office of the President. (n.d.). Retrieved June, 4, 2012, from http://www.whitehouse.gov/administration/eop.

Executive Office of The President Office Of Management and Budget. (n.d.). E-Government Strategy. Retrieved June, 2, 2012, from http://www.usa.gov/Topics/Includees/reference/egov_strategy.pdf.

Haiyan Qian. (n.d.). Division for Public administration and Development Management. Future government : A Global Perspective Connection to Open Government. Retrieved 2, July, 2012, from http://www.slideshare.net/undesapublicadmin/future-governmenta-global-perspective-in-connection-to-open-government.

Information Technology Telecommunications and Electronics Association. (n.d.). Quality Assurance in Renal Care The QuaSi-Niere Card. Retrieved July, 1, 2012, from http://www.intellectuk.org/index.php?option=com_docman&task=doc_download&gid=411.

International Police Organization. (n.d.). About INTERPOL. Retrieved July, 22, 2012 Available from http://www.interpol.int/About-INTERPOL/Overview.

James A. Donald. (n.d.). Natural Law and Natural Right. Retrieved July, 3, 2012, from http://jim.com/rights.html.

James X. D., Paige A. & Ari S. (n.d.). Privacy and E-Government. A Report to the United Nations Department of Economic and Social Affairs as background for the World Public Sector Report : E-Government, Retrieved June, 4, 2012, from http://www.internetpolicy.net/privacy/20030523cdt.pdf.

Luciano Batista. (n.d.). Journal of Information Law & Technology. The Open University Business School. Information sharing in e-government initiatives : Freedom of Information and Data Protection issues concerning local government, Retrieved July, 21, 2012, from http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2009_2/bc/bc.pdf.

Office of Management and Budget. (n.d.). Office of Management and Budget. Retrieved June, 4, 2012, from Available from http://www.whitehouse.gov/omb.

Organization for Economic Co-operation and Development. (n.d.). Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data.

Organization for Economic Co-operation and Development. (n.d.). OECD Council Recommendation. Retrieved June, 4, 2012, from http://www.oecd.org/document/18/0,3746,en_2649_34223_1815186_1_1_1_1,00.html.

Public Law 93-579. The Privacy Acts of 1974. Retrieved June, 9, 2012, from http://epic.org/privacy/1974act/.

Public Law 107–347. E-Government Act of 2002. Retrieved June, 9, 2012, from http://www.access.gpo.gov/.

Public Law 426-62. (1913). An Act to Create a Department of Labor. Retrieved July, 1, 2012, fromhttp://www.dol.gov.

Samuel D. Warren & Louis D. Brandies. (1890). The Right to Privacy. Harvard Law Review. (Vol. 4). 5.

Samuel D. Warren & Louis D. Brandies. (n.d.). Context of The Right to Privacy. Harvard Law Review. Retrieved June, 1, 2012, from http://faculty.uml.edu/Sgallagher/Harvard__law_review.htm.

Techfreedom. (n.d.). Today's Approval of PCLOB Nominations a Long-Overdue Victory for Privacy and the Rule of Law. Retrieved July, 1, 2012, from http://techfreedom.org/node/175.

The United States Department of Labor. (n.d.). U.S. Department of Labor E-Government Strategic Plan. Retrieved June, 7, 2012, from http://www.dol.gov/_sec/e_government_plan/p23_security_privacy.htm.

The United States Department of Justice. (n.d.). E-Government Act 2002. Retrieved June, 7, 2012, from http://www.justice.gov/opcl/e-govt-act-2002.html.

The Universal Declaration of Human Rights 1948. (n.d.). from http://www.un.org/en/documents/udhr/index.shtml.

TRUSTe. (n.d.). About TRUSTe. Retrieved July, 21, 2012, from http://www.truste.com/about-TRUSTe/

TRUSTe. (n.d.). Pan to Europe the Right Way. Retrieved July, 21, 2012, from http://www.truste.com/products-and-services/enterprise-privacy/eu-safe-harbor-seal

United Human Right Council. (n.d.). Genocide in Rwanda. Retrieved June, 4, 2012, from http://www.unitedhumanrights.org/genocide/genocide_in_rwanda.htm

United Nations Public Administration Network Public Administration News. (n.d.). USA : Satisfaction With e-Government Reaches New Highs Under Obama but is Stalling, According to ForeSee. Retrieved June, 7, 2012, from http://www.unpan.org/PublicAdministrationNews/tabid/118/mctl/ArticleView/ModuleID/1473/articleId/29498/default.aspx.

United States Government Printing Office. (n.d.). About Privacy Act Issuances. Retrieved June, 3, 2012, from http://www.gpo.gov/help/index.html#about_Privacy_act_issuances.ht.

Yale University. (n.d.). The Cambodian Genocide Program. Retrieved June, 1, 2012, from http://www.yale.edu/cgp/thai/index.htmlm.

ประวัติผู้เขียน

ชื่อ-สกุล : นายสัญญา วิริยะอมรพันธุ์

วัน-เดือน-ปีเกิด : วันที่ 2 กรกฎาคม พ.ศ. 2529

วุฒิการศึกษา : ปี 2552 จบการศึกษาระดับปริญญาตรี
นิติศาสตร์บัณฑิต มหาวิทยาลัยเชียงใหม่ จังหวัดเชียงใหม่

ปี 2547 จบการศึกษาระดับมัธยมศึกษาตอนปลาย
โรงเรียนบดินทรเดชา(สิงห์ สิงหเสนีย์) จังหวัดกรุงเทพมหานคร

ประสบการณ์การทำงาน : ปี 2554 ตำแหน่ง นิติกร สังกัด ฝ่ายกฎหมายและวินัย
องค์การค้าของสำนักงานคณะกรรมการส่งเสริมสวัสดิการและ
สวัสดิภาพครูและบุคลากรทางการศึกษา (องค์การค้าของคุรุสภา)

มหาวิทยาลัยกรุงเทพ

ข้อตกลงว่าด้วยการอนุญาตให้ใช้สิทธิในวิทยานิพนธ์/สารนิพนธ์

วันที่ 25 เดือน สิงหาคม พ.ศ. 2555

ข้าพเจ้า (นาย/นาง/นางสาว) นายสัญญา วิริยะอมรพันธุ์ อยู่บ้านเลขที่ 503

ซอย ลาดพร้าว 80/3 ถนน ลาดพร้าว ตำบล/แขวง วังทองหลาง

อำเภอ/เขต วังทองหลาง จังหวัด กรุงเทพมหานคร รหัสไปรษณีย์ 10310

เป็นนักศึกษาของมหาวิทยาลัยกรุงเทพ รหัสประจำตัว 7530400089

ระดับปริญญา ☐ ตรี ☑ โท ☐ เอก

หลักสูตร นิติศาสตรมหาบัณฑิต สาขาวิชา กฎหมายธุรกิจระหว่างประเทศและธุรกรรมทางอิเล็กทรอนิกส์

คณะ บัณฑิตวิทยาลัย ซึ่งต่อไปนี้เรียกว่า **"ผู้อนุญาตให้ใช้สิทธิ"** ฝ่ายหนึ่ง และ

มหาวิทยาลัยกรุงเทพ ตั้งอยู่เลขที่ 119 ถนนพระราม 4 แขวงพระโขนง เขตคลองเตย กรุงเทพมหานคร 10110 ซึ่งต่อไปนี้เรียกว่า **"ผู้ได้รับอนุญาตให้ใช้สิทธิ"** อีกฝ่ายหนึ่ง

ผู้อนุญาตให้ใช้สิทธิ และ ผู้ได้รับอนุญาตให้ใช้สิทธิ ตกลงทำสัญญากันโดยมีข้อความดังต่อไปนี้

ข้อ 1. ผู้อนุญาตให้ใช้สิทธิขอรับรองว่าเป็นผู้สร้างสรรค์และเป็นผู้มีสิทธิแต่เพียงผู้เดียวในงานสารนิพนธ์/วิทยานิพนธ์ หัวข้อ มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ของภาครัฐ

Legal Measures of Personal Data Protection for e-Government

ซึ่งถือเป็นส่วนหนึ่งของการศึกษาตามหลักสูตร นิติศาสตรมหาบัณฑิต ของมหาวิทยาลัยกรุงเทพ (ต่อไปนี้เรียกว่า **"สารนิพนธ์/วิทยานิพนธ์"**)

ข้อ 2. ผู้อนุญาตให้ใช้สิทธิตกลงยินยอมให้ผู้ได้รับอนุญาตให้ใช้สิทธิโดยปราศจากค่าตอบแทนและไม่มีกำหนดระยะเวลาในการนำสารนิพนธ์/วิทยานิพนธ์ ซึ่งรวมถึงแต่ไม่จำกัดเพียงการทำซ้ำ ดัดแปลง เผยแพร่ต่อสาธารณชน ให้เช่าต้นฉบับหรือสำเนางาน ให้ประโยชน์อันเกิดจากลิขสิทธิ์แก่ผู้อื่น อนุญาตให้ผู้อื่นใช้สิทธิโดยจะกำหนดเงื่อนไขอย่างหนึ่งอย่างใดด้วยหรือไม่ก็ได้ ไม่ว่าทั้งหมดหรือเพียงบางส่วน หรือการกระทำอื่นใดในลักษณะทำนองเดียวกัน

สัญญานี้ทำขึ้นสองฉบับ มีข้อความเป็นอย่างเดียวกัน คู่สัญญาได้อ่านและเข้าใจข้อความในสัญญานี้โดยละเอียดแล้ว จึงได้ลงลายมือชื่อให้ไว้เป็นสำคัญต่อหน้าพยาน และเก็บรักษาไว้ฝ่ายละฉบับ

ลงชื่อ.....[redacted]...ผู้อนุญาตให้ใช้สิทธิ

(สัญญา วิริยาอมรพันธุ์)

ลงชื่อ.....[redacted]...ผู้ได้รับอนุญาตให้ใช้สิทธิ

(ดร.ชนัฌนา ชอบสุทธิ)

ผู้อำนวยการสำนักหอสมุด

ลงชื่อ.....[redacted].....พยาน

(ผู้ช่วยศาสตราจารย์ ดร. ศิวพร หวังพิพัฒน์วงศ์)

คณบดีบัณฑิตวิทยาลัย

ลงชื่อ.....[redacted]...พยาน

(จินตนา แสงมาลา)