ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลในบริบทอิเล็กทรอนิกส์

โดย

นางสาวอธิพร สิทธิธีรรัตน์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
นิติศาสตรมหาบัณฑิต
สาขาการค้าระหว่างประเทศ
คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์
ปีการศึกษา 2558

ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลในบริบทอิเล็กทรอนิกส์

โดย

นางสาวอธิพร สิทธิธีรรัตน์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
นิติศาสตรมหาบัณฑิต
สาขาการค้าระหว่างประเทศ
คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์
ปีการศึกษา 2558

LEGAL PROBLEMS CONCERNING ELECTRONIC PERSONAL DATA PROTECTION

BY

Ms. Athiporn Sitthitheerarut

A THESISSUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OFMASTER OF LAWS

INTERNATIONAL TRADE REGULATION

FACULTY OF LAW

THAMMASAT UNIVERSITY

ACADEMIC YEAR 2015

มหาวิทยาลัยธรรมศาสตร์
คณะนิติศาสตร์

วิทยานิพนธ์

ของ

นางสาวอธิพร สิทธิธีรรัตน์

เรื่อง

ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลในบริบทอิเล็กทรอนิกส์

ได้รับการตรวจสอบและอนุมัติให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
นิติศาสตรมหาบัณฑิต

เมื่อวันที่ 11 สิงหาคม พ.ศ. 2559

ประธานกรรมการสอบวิทยานิพนธ์ _____
(ศาสตราจารย์ ดร. เสาวนีย์ อัศวโรจน์)

กรรมการและอาจารย์ที่ปรึกษาวิทยานิพนธ์ _____
(รองศาสตราจารย์ ดร. พินัย ณ นคร)

กรรมการสอบวิทยานิพนธ์ _____
(ผู้ช่วยศาสตราจารย์ ดร. วีรวัฒน์ จันทโชติ)

กรรมการสอบวิทยานิพนธ์ _____
(ผู้ช่วยศาสตราจารย์ ดร. ต่อพงศ์ กิตติยานุพงศ์)

คณบดี _____
(ศาสตราจารย์ ดร. อุดม รัฐอมฤต)

หัวข้อวิทยานิพนธ์	ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลในบริบทอิเล็กทรอนิกส์
ชื่อผู้เขียน	นางสาวอธิพร สิทธิธีรรัตน์
ชื่อปริญญา	นิติศาสตรมหาบัณฑิต
สาขาวิชา/คณะ/มหาวิทยาลัย	กฎหมายการค้าระหว่างประเทศ นิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์	รองศาสตราจารย์ ดร.พินัย ณ นคร
ปีการศึกษา	2558

บทคัดย่อ

วิทยานิพนธ์ฉบับนี้มุ่งศึกษาถึงความจำเป็นในการมีกฎหมายคุ้มครองข้อมูลส่วนบุคคล ซึ่งมีบทบัญญัติคุ้มครองถึงข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์ และศึกษาแนวทางการให้ความคุ้มครองความเป็นส่วนตัวของประเทศต่างๆโดยเฉพาะอย่างยิ่งในประเทศสหรัฐอเมริกา และสหภาพยุโรปเนื่องจากในปัจจุบันเทคโนโลยีต่างๆโดยเฉพาะอย่างยิ่งอินเตอร์เน็ตได้ก้าวเข้ามาเป็นส่วนสำคัญในชีวิตของทุกคนในทุกเพศทุกวัย ไม่ว่าจะเป็นการติดต่อสื่อสาร การสืบค้นข้อมูล หรือพาณิชย์อิเล็กทรอนิกส์ แต่หลายๆคนกลับมิได้ตระหนักถึงการละเมิดความเป็นส่วนตัวที่เทคโนโลยีดังกล่าวอาจกระทำได้

เทคโนโลยีในปัจจุบันนี้สามารถก่อให้เกิดการละเมิดความเป็นส่วนตัวได้ง่าย กล่าวคือข้อมูลเกี่ยวกับอุปกรณ์อิเล็กทรอนิกส์ได้แก่Mac Address และ IP Address สามารถนำมาใช้เพื่อติดตามการกระทำของเจ้าของอุปกรณ์ทราบผู้ให้บริการอินเตอร์เน็ตของเจ้าของอุปกรณ์ หรือทราบพื้นที่ที่มีการเชื่อมต่ออินเตอร์เน็ตได้ ความก้าวหน้าของเทคโนโลยีทำให้เจ้าของข้อมูล Pseudonymous หรือ Anonymous อาจถูกค้นพบได้ในด้านการทำ Profiling และการตัดสินใจโดยระบบอัตโนมัติซึ่งเป็นการติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลจะก่อให้เกิดความรำคาญแก่เจ้าของข้อมูลส่วนบุคคลและทำให้เกิดการเลือกปฏิบัติต่อเจ้าของข้อมูลส่วนบุคคลได้ นอกจากนี้เทคโนโลยีไบโอเมตริก (Biometric) ซึ่งนำมาใช้ทางการค้าเพื่อยืนยันตัวเจ้าของข้อมูลส่วนบุคคล เช่น การชำระเงิน เป็นต้น ทำให้ข้อมูลไบโอเมตริก (Biometric) ถูกเก็บรวบรวมได้ง่ายจึงอาจละเมิดความส่วนตัวของเจ้าของข้อมูลส่วนบุคคล ที่มากไปกว่านั้นเนื่องจากข้อมูลส่วนบุคคลมักถูกเก็บรวบรวมในรูปแบบอิเล็กทรอนิกส์และเป็นสิ่งที่มีค่าจึงควรเปิดโอกาสให้เจ้าของข้อมูลส่วนบุคคลสามารถใช้

ประโยชน์จากข้อมูลส่วนบุคคลของตนโดยการโอนข้อมูลส่วนบุคคลของตนไปยังผู้ประกอบการอื่น (Right to data portability) ได้ย่อมทำให้เจ้าของข้อมูลส่วนบุคคลสามารถเปลี่ยนผู้ให้บริการได้ง่าย อันเป็นการส่งเสริมการแข่งขันทางการค้าอีกด้วย

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... มีบทบัญญัติควบคุมการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ภายใต้ร่างพระราชบัญญัติดังกล่าวผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลและต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลในเวลาทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล การนำข้อมูลส่วนบุคคลไปใช้เป็นประการอื่นนอกจากที่ได้แจ้งไว้จะกระทำมิได้เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หากผู้ควบคุมข้อมูลส่วนบุคคลเปลี่ยนแปลงวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล นอกจากนี้เจ้าของข้อมูลส่วนบุคคลมีสิทธิเพิกถอนความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้เว้นแต่มีกฎหมายหรือสัญญาซึ่งให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคลห้ามไว้

จากการศึกษาร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ประกอบกับกฎหมายของต่างประเทศแล้วจะเห็นได้ว่าร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ยังมิได้ครอบคลุมไปถึงเทคโนโลยีในปัจจุบัน คือ ข้อมูล Mac Address หรือ IP Address ข้อมูล Pseudonymous ข้อมูลไบโอเมตริก (Biometric) การทำ Profiling รวมถึงการตัดสินใจโดยระบบอัตโนมัติ และสิทธิในการโอนข้อมูลส่วนบุคคล ทำให้ต้องอาศัยการตีความร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... เพื่อให้ครอบคลุมถึงเทคโนโลยีเหล่านี้ การตีความดังกล่าวนำมาซึ่งปัญหาความไม่แน่นอนและทำให้ความเป็นส่วนตัวของประชาชนอาจไม่ได้รับความคุ้มครองอย่างครอบคลุมได้ นอกจากนี้ยังมีข้อบกพร่องของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... เช่น เนื่องจากการติดต่อสื่อสารและการทำธุรกรรมสามารถเกิดขึ้นไม่ว่าอยู่ ณ ที่ใดในโลก ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลที่อยู่ต่างประเทศสามารถเก็บรวบรวมข้อมูลส่วนบุคคลของคนไทยได้ แต่ร่างพระราชบัญญัติดังกล่าว ไม่สามารถนำมาบังคับใช้แก่ผู้ควบคุมข้อมูลส่วนบุคคลที่อยู่ในต่างประเทศแต่ได้เก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลของประชาชนภายในประเทศ ด้วยเหตุนี้ร่างพระราชบัญญัติดังกล่าว ควรกำหนดบทบัญญัติให้ครอบคลุมถึงเทคโนโลยีที่นำมาใช้บนอินเตอร์เน็ตและแก้ไขข้อบกพร่องเพื่อให้สามารถคุ้มครองความเป็นส่วนตัวของประชาชนได้อย่างดีที่สุด

คำสำคัญ:ข้อมูลส่วนบุคคล, การคุ้มครองข้อมูลส่วนบุคคลในบริบทอิเล็กทรอนิกส์, ข้อมูลส่วนบุคคลในบริบทอิเล็กทรอนิกส์

Thesis Title	LEGAL PROBLEMS CONCERNING ELECTRONIC PERSONAL DATA PROTECTION
Author	Ms. Athiporn Sitthitheerarut
Degree	Master of Laws
Major Field/Faculty/University	International Trade Regulation Law Law Thammasat University
Thesis Advisor	Associate Professor Pinai Na Nakorn, Ph.D.
Academic Year	2015

ABSTRACT

This dissertation aims to study the necessity of enacting personal data protection law which includes the provisions thatprotect electronic personal data and to study the principles of privacy protection in foreign countries, especially those of the United States of America and European Union. Nowadays, technologies, particularly the Internet, are one of the important parts in all ages, but not many people are aware of privacy violation by these technologies.

Today's technologies are prone to privacy violation – that is to say the information about electronic devices such as Mac Address and IP Address can be used for owner's behavioral tracking, knowing an internet service provider or knowing the place where the owner connect to the Internet. An advance of technologies can reveal the owner of pseudonymous data or anonymous data. Also, the profiling and automated decisions which are used to track the data subject's behavior cause annoyance to the data subject and sometimes result in discrimination against the data subject. Other than the technologies stated above, biometrictechnologyplays its large role in commerce to identify a data subject. Since biometric data is easy to gather, it poses big privacy risks. Moreover, personal data is valuable, and most of the data controllers store it in electronic format. Thus, the data subject should gain benefitfrom

its data through the right to data portability. This right helps the data subject switch the provider easily and promotes the trade competition.

The Personal Data Protection Bill B.E. .... has provisions that control the collection, use and disclosure of personal data. Under this bill, the data controller must provide the purpose or purposes for which the data are intended to be processed to the data subject and obtain consent from the data subject at the time of obtaining that data. The data controller shall not use or disclose the collected personal data for any purpose other than those indicated at the time it was collected. If the data controller is willing to use the personal data for a new purpose, it must obtain the permission from the data subject. Furthermore, the data subject has the right to revoke its consent to collect, use or disclose its personal data unless prohibited by law or contract from which the data subject gains profit.

Having studied the Personal Data Protection Bill B.E. .... along with the foreign data protection laws, the study shows that thePersonal Data Protection Bill B.E. .... does not cover such new technologies as Mac Address, IP Address, pseudonymous data, biometric data, profiling, automated decisions and the right to data portability. To cover all these technologies, we have to interpret the bill boarder, and this will result in uncertainty as well as hindrances to the protection of privacy. In addition, the bill has some drawbacks, for example,given that transaction or contact can be madeelsewhere, but the bill cannot protect the data subject whose data was collected used or disclosed by the data controller situated outside Thailand. As a result, it is recommended by this research that the bill should be amended to cover the technologies and eviscerate weaknesses found in the bill with a view to better protection of privacy rights.

Keywords: personal data, electronic personal data protection, electronic personal data

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จได้เนื่องด้วยความช่วยเหลือและความกรุณาอย่างยิ่งของบุคคลหลายท่านซึ่งไม่สามารถนำมากล่าวในที่นี้ได้ทั้งหมด ผู้มีพระคุณท่านแรกที่ผู้เขียนขอกราบขอพระคุณเป็นอย่างยิ่งคือ รองศาสตราจารย์ ดร. พินัย ณ นคร ที่ได้ให้ความกรุณาสละเวลาอันมีค่ารับเป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ พร้อมทั้งได้สละเวลาอันมีค่าอย่างยิ่งเพื่อให้ความรู้ คำแนะนำ และแนวทางอันเป็นประโยชน์ต่อการศึกษาค้นคว้าในการทำวิทยานิพนธ์นี้ จนกระทั่งวิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้ด้วยดี

นอกจานี้ผู้เขียนขอกราบขอบพระคุณอย่างสูงต่อศาสตราจารย์ ดร. เสาวนีย์ อัศวโรจน์ ผู้ช่วยศาสตราจารย์ ดร. วีรวัฒน์ จันทโชติ และผู้ช่วยศาสตราจารย์ ดร. ต่อพงศ์ กิตติยานุพงศ์ ที่ได้กรุณาสละเวลาอันมีค่าอย่างยิ่งในการเป็นคณะกรรมการสอบวิทยานิพนธ์ รวมถึงให้คำแนะนำในการตรวจสอบและแก้ไขวิทยานิพนธ์นี้

สุดท้ายนี้ผู้เขียนขอกราบขอบพระคุณบิดา มารดา ผู้ซึ่งให้ความรักและกำลังใจแก่ผู้เขียนมาโดยตลอด และขอบคุณเพื่อนร่วมรุ่นปริญญาโทที่ให้คำปรึกษา เป็นกำลังใจ และให้ความช่วยเหลืออยู่ตลอด

นางสาวอธิพร สิทธิธีรรัตน์

สารบัญ

สารบัญตาราง

สารบัญภาพ

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

สิทธิในความเป็นอยู่ส่วนบุคคลหรือสิทธิในความเป็นส่วนตัว (Right to Privacy) หมายความว่าสถานะที่บุคคลจะรอดพ้นจากการสังเกต การรู้ การสืบความลับ การรบกวนต่างๆและความมีสันโดษ โดยไม่ติดต่อสัมพันธ์กับสังคม โดยทั้งนี้ขอบเขตที่บุคคลควรได้รับการคุ้มครองและการเคารพสิทธิในสิทธิส่วนบุคคลก็คือการดำรงชีวิตอย่างเป็นอิสระ มีการพัฒนาบุคลิกลักษณะตามที่ต้องการ สิทธิที่จะแสวงหาความสุขในชีวิตตามวิถีทางที่อาจเป็นไปได้และเป็นความพอใจตราบเท่าที่ไม่ขัดต่อกฎหมาย ไม่ขัดต่อความสงบเรียบร้อยและศีลธรรมอันดีของประชาชนและไม่เป็นการล่วงละเมิดสิทธิเสรีภาพของผู้อื่น[1] สิทธิดังกล่าวมีความสำคัญอย่างมากโดยจะเห็นได้จากการที่นานาอารยประเทศให้ความสำคัญโดยพยายามคุ้มครองสิทธิดังกล่าว เช่น ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ.1948 (Universal Declaration of Human Rights of 1949)[2]อนุสัญญาแห่งยุโรปว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐาน (European Convention for theProtection of Human Rights and Fundamental Freedoms)[3] รวมทั้งรัฐธรรมนูญแห่งราช

---

[1] เกรียงไกร เจริญธนาวัฒน์, “สิทธิของผู้เล่นเกมส์ออนไลน์”,สืบค้นเมื่อ 15 มกราคม 2559, http://www.pub-law.net/publaw/view.aspx?ID=609

[2] **Universal Declaration of Human Rights of 1949**

Article 12

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

[3] **European Convention for the Protection of Human Rights and Fundamental Freedoms**

ARTICLE 8 Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

อาณาจักรไทย พ.ศ. 2550 มาตรา 35[4] ได้ให้ความคุ้มครองแก่สิทธิในความเป็นอยู่ส่วนตัวเช่นกัน

แม้สิทธิส่วนบุคคลมีความสำคัญแต่ในอดีตนั้นการละเมิดสิทธิส่วนบุคคลยังค่อนข้างจำกัดอยู่ในวงแคบ การเก็บรวบรวมข้อมูลส่วนบุคคลยังคงทำได้อย่างจำกัด แต่เมื่อมีการพัฒนาคอมพิวเตอร์ขึ้นใช้ทำให้การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลสามารถทำได้ง่ายมากขึ้นและสามารถเก็บรักษาข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์ได้ยาวนานขึ้นโดยมีค่าใช้จ่ายน้อยลง โดยเทคโนโลยีที่กระทบต่อความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลได้เพิ่มความสำคัญขึ้นอย่างเด่นชัดในระยะเวลาไม่นานมานี้ได้แก่ ข้อมูล Mac AddressและIP Address ข้อมูล Pseudonymous การทำ Profiling และ ข้อมูล Biometric

เทคโนโลยีดังกล่าวสามารถถูกนำมาใช้เพื่อติดตามตัวเจ้าของข้อมูลส่วนบุคคลได้โดยอาศัยการทำ Profiling หรือการใช้ Mac Address หรือ IP Address และในหลายๆครั้งข้อมูลที่ผู้ควบคุมข้อมูลส่วนบุคคลได้รับจากข้อมูลทั้งสามประเภทดังกล่าวเป็นข้อมูลหรือพฤติกรรมที่เจ้าของข้อมูลส่วนบุคคลไม่ประสงค์จะเปิดเผยเนื่องจากการเปิดเผยอาจก่อผลเสียแก่เจ้าของข้อมูลส่วนบุคคลได้ ในด้านข้อมูล Pseudonymous สามารถถูกนำมาใช้เพื่อหลีกเลี่ยงการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลได้ และข้อมูล Biometric เป็นข้อมูลที่ได้ถูกพัฒนามาใช้เพื่อการยืนยันตัวเจ้าของ

---

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[4]**รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550**

มาตรา 35

สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง ตลอดจนความเป็นอยู่ส่วนตัวย่อมได้รับความคุ้มครองการกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชน อันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัวจะกระทำมิได้ เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณะ

บุคคลย่อมมีสิทธิได้รับความคุ้มครองจากการแสวงหาประโยชน์โดยมิชอบจากข้อมูลส่วนบุคคลที่เกี่ยวกับตน ทั้งนี้ ตามที่กฎหมายบัญญัติ

ข้อมูลส่วนบุคคลมากขึ้นไม่ และยังสามารถถูกเก็บรวบรวมได้ง่าย นอกจากนี้ข้อมูล Biometric ยังสามารถบอกถึงสภาพต่างๆของเจ้าของข้อมูลส่วนบุคคลได้เป็นอย่างดี

ความสามารถของเทคโนโลยีเหล่านี้ก่อให้เกิดความพยายามแก้ไขกฎหมายคุ้มครองข้อมูลส่วนบุคคลในสหภาพยุโรปให้มีความทันสมัยเพื่อมิให้เทคโนโลยีดังกล่าวละเมิดความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคล เช่น การเพิ่มสิทธิในการขอให้ลบข้อมูลของตน (Right to be forgotten) การเพิ่มความคุ้มครองแก่ข้อมูล Pseudonymous การเพิ่มการคุ้มครองในการเก็บรวบรวมและวิเคราะห์ข้อมูลส่วนบุคคล (Profiling) และการเพิ่มความคุ้มครองในการเก็บข้อมูลเด็ก เป็นต้น นอกจากนี้ในทางสหรัฐอเมริกาเองก็มีความพยายามผลักดันกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลในลักษณะเช่นเดียวกัน เช่น Do Not Track Me Online Bill

สำหรับประเทศไทยเองยังไม่มีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล คงปรากฏเพียงร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลหลายฉบับซึ่งร่างโดยไม่สอดรับกับเทคโนโลยีที่พัฒนาขึ้นในปัจจุบันจึงยังมิได้ครอบคลุมถึงการละเมิดความเป็นส่วนตัวที่อาจเกิดขึ้นจากการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยเทคโนโลยีดังกล่าวและอาจก่อให้เกิดปัญหาการละเมิดข้อมูลส่วนบุคคลได้อย่างง่ายดาย การปราศจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลใช้บังคับเป็นการทั่วไปย่อมก่อให้เกิดผลเสียทั้งในทางสังคมและเศรษฐกิจของประเทศ กล่าวคือ ประชาชนย่อมไม่ได้รับความคุ้มครองต่อสิทธิในความเป็นอยู่ส่วนตัวอย่างพอเพียงและในด้านเศรษฐกิจย่อมทำให้ธุรกิจพาณิชย์อิเล็กทรอนิกส์ดำเนินไปไม่เต็มศักยภาพ บุคคลทั้งในประเทศและต่างประเทศไม่กล้าที่จะทำธุรกิจกับบริษัทหรือห้างร้านในประเทศไทยอีกด้วย

1.2 วัตถุประสงค์ของการศึกษา

1.2.1เพื่อให้เกิดความเข้าใจในหลักการและแนวคิดของความจำเป็นในการมีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

1.2.2 เพื่อศึกษาถึงรูปแบบในการได้มาซึ่งข้อมูลส่วนบุคคลและการละเมิดข้อมูลส่วนบุคคล

1.2.3 เพื่อศึกษาเปรียบเทียบกฎหมาย การบังคับใช้กฎหมาย และแนวความคิดในการคุ้มครองข้อมูลส่วนบุคคลในต่างประเทศ

1.2.4 เพื่อเป็นแนวทางในการพัฒนากฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยให้มีหลักเกณฑ์ที่สามารถคุ้มครองประชาชนได้จริง

1.3 สมมติฐานของการศึกษา

แม้ประเทศไทยมีกฎหมายที่จะนำมาบังคับใช้เพื่อคุ้มครองข้อมูลส่วนบุคคลอยู่บ้าง เช่น พ.ร.บ.ข้อมูลข่าวสารราชการ พ.ศ.2540 หรือ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 หรือพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 เป็นต้น ซึ่งกฎหมายดังกล่าวก็หาเป็นกฎหมายที่มีวัตถุประสงค์ในการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป อันหาพอเพียงแก่การนำมาบังคับใช้ในการคุ้มครองความเป็นส่วนตัวและการเก็บข้อมูลส่วนบุคคลไม่ อย่างไรก็ตามแม้ประเทศไทยมีแนวความคิดและความพยายามในการร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ดังเห็นได้จากมีการพยายามเสนอร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... โดยองค์กรต่างๆเรื่อยมา เช่น สมาชิกสมาผู้แทนราษฎร สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ หรือโดยกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เป็นต้นแต่ร่างพระราชบัญญัติดังกล่าวยังไม่ครอบคลุมเพียงพอในการคุ้มครองประชาชน ทั้งยังไม่สอดรับกับเทคโนโลยีที่ถูกพัฒนาขึ้นใหม่อีกด้วย ด้วยเหตุนี้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ดังกล่าวจึงยังคงขาดประสิทธิภาพเมื่อนำมาบังคับใช้จริง

1.4 ขอบเขตการศึกษา

การศึกษานี้มุ่งศึกษาการเก็บข้อมูลส่วนบุคคลโดยอาศัยเทคโนโลยีทางอิเล็กทรอนิกส์และการละเมิดข้อมูลส่วนบุคคล นอกจากนี้ยังศึกษาหลักเกณฑ์รวมถึงมาตรการในการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปทั้งระเบียบที่ใช้บังคับอยู่ (Directive 95/46/EC) และกฎหมายที่จะมีขึ้นใหม่ (General Data Protection Regulation) รวมทั้งศึกษากฎหมายในประเทศสหรัฐอเมริกา แคนาดา และประเทศสิงคโปร์ เพื่อนำมาวิเคราะห์เปรียบเทียบกับร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ของประเทศไทย เพื่อทราบถึงแนวความคิด หลักเกณฑ์ ทางปฏิบัติและปัญหา โดยมีวัตถุประสงค์เพื่อนำมาพัฒนากฎหมายของประเทศไทยต่อไป

1.5 การดำเนินการศึกษา

การศึกษานี้เป็นการศึกษาวิจัยทางเอกสาร มุ่งศึกษาเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลโดยรวบรวบข้อมูลและค้นคว้าวิจัยจากตำรา เอกสาร บทความ วารสาร วิทยานิพนธ์ สาระ

นิพนธ์ เอกสารทางวิชาการของนักวิชาการไทยและต่างประเทศ กฎหมายที่เกี่ยวข้องของประเทศไทยและในต่างประเทศ รวมถึงข้อมูลบนอินเตอร์เน็ต

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1.6.1มีความรู้ความเข้าใจในหลักการ แนวคิด และความสำคัญของการมีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

1.6.2 ได้ทราบถึงรูปแบบในการได้มาซึ่งข้อมูลส่วนบุคคลและการละเมิดข้อมูลส่วนบุคคลในต่างประเทศ

1.6.3 ได้ทราบถึงกฎหมาย การบังคับใช้กฎหมาย หลักการ และแนวคิดในการคุ้มครองข้อมูลส่วนบุคคลในต่างประ

1.6.4 ทราบถึงข้อบกพร่องของกฎหมายประเทศไทยที่มีอยู่หรือจะมีขึ้นต่อไปเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล และนำไปสู่แนวทางการแก้ไขข้อบกพร่องดังกล่าว

บทที่ 2
แนวความคิดและการคุ้มครองข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์

2.1 ความเป็นมาของการคุ้มครองข้อมูลส่วนบุคคล

สิทธิมนุษยชน (Human Right) มาจากคำว่าสิทธิรวมกับคำว่ามนุษยชน โดย สิทธิ หมายถึง อำนาจอันชอบธรรมที่บุคคลแต่ละคนพึงมีโดยมิได้ไปเบียดเบียนผู้อื่น เป็นอำนาจซึ่งกฎหมายให้การรับรองแก่บุคคลผู้เป็นเจ้าของสิทธิเพื่อให้สามารถเรียกร้องให้ผู้อื่นกระทำการบางอย่างแก่ผู้เป็นเจ้าของสิทธินั้น สิทธิมีปรากฏอยู่ในหลายๆด้าน เช่น สิทธิในชีวิต ร่างกายหรือทรัพย์สิน เป็นต้น สำหรับ “สิทธิมนุษยชน” นั้นมีการให้ความหมายในหลายที่ได้แก่

ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights หรือ UDHR) ข้อ 1[1] ระบุว่า มนุษย์ทั้งปวงเกิดมามีอิสระและเสมอภาคกันในศักดิ์ศรีและสิทธิ ต่างในตนมีเหตุผลและมโนธรรม และควรปฏิบัติต่อกันด้วยจิตวิญญาณแห่งภารดรภาพ และข้อ 2[2] ระบุว่า ทุกคนย่อมมีสิทธิและอิสรภาพทั้งปวงตามที่กำหนดไว้ในปฏิญญานี้ โดยปราศจากการแบ่งแยกไม่ว่าชนิดใด อาทิ เชื้อชาติ ผิว เพศ ภาษา ศาสนา ความคิดเห็นทางการเมืองหรือทางอื่น พื้นเพทางชาติหรือสังคม

---

[1]**Universal Declaration of Human Rights**

Article 1

All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood.

[2]**Universal Declaration of Human Rights**

Article 2

Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. Furthermore, no distinction shall be made on the basis of the political, jurisdictional or international status of the country or territory to which a person belongs, whether it be independent, trust, non-self-governing or under any other limitation of sovereignty.

ทรัพย์สิน การเกิดหรือสถานะอื่น นอกเหนือจากนี้ จะไม่เกิดการแบ่งแยกใดบนพื้นฐานของสถานะทางการเมือง ทางกฎหมายหรือทางการระหว่างประเทศของประเทศ หรือดินแดนที่บุคคลสังกัด ไม่ว่าดินแดนนี้จะเป็นเอกราชอยู่ในความพิทักษ์ มิได้ปกครองตนเอง หรืออยู่ภายใต้การจำกัดอธิปไตยอื่นใด

คณะกรรมการสิทธิมนุษยชนแห่งสหประชาชาติได้ให้ความหมายของสิทธิมนุษยชนไว้ดังนี้ สิทธิมนุษยชน คือ สิทธิที่มนุษย์ทุกคนพึงมี โดยไม่คำนึงถึงเชื้อชาติ ถิ่นที่อยู่ เพศ ชาติพันธุ์ สีผิว ศาสนา ภาษา หรือสถานะอื่นใด ภายใต้สิทธิมนุษยชนทุกๆคนมีสิทธิอย่างเท่าเทียมกันโดยไม่ถูกแบ่งแยก[3]

พระราชบัญญัติคณะกรรมการสิทธิมนุษยชนแห่งชาติ พ.ศ. 2542 มาตรา 3 ให้ความหมายของสิทธิมนุษยชน หมายถึง ศักดิ์ศรีความเป็นมนุษย์ สิทธิเสรีภาพ ความเสมอภาคของบุคคลที่ได้รับการรับรองหรือคุ้มครองตามรัฐธรรมนูญแห่งราชอาณาจักรไทย หรือตามกฎหมายไทย หรือตามสนธิสัญญาที่ประเทศไทยมีพันธกรณีที่จะต้องปฏิบัติตาม

สิทธิมนุษยชน คือ สิ่งจำเป็นสำหรับคนทุกคนที่ต้องได้รับในฐานะที่เป็นคน เพื่อทำให้คนนั้นๆมีชีวิตอยู่รอดได้และมีการพัฒนา สิทธิมนุษยชนจึงมี 2 ระดับ[4]

ระดับแรก สิทธิที่ติดตัวทุกคนมาแต่เกิด ไม่สามารถถ่ายโอนให้แก่กันได้ อยู่เหนือกฎหมายและอำนาจใดๆของรัฐทุกรัฐ สิทธิเหล่านี้ได้แก่ สิทธิในชีวิต ห้ามฆ่าหรือทำร้ายต่อชีวิต ห้ามการค้ามนุษย์ ห้ามทรมานอย่างโหดร้าย คนทุกคนมีสิทธิในความเชื่อมโนธรรมหรือลัทธิทางศาสนา ทางการเมือง มีเสรีภาพในการแสดงความคิดเห็นและแสดงออกหรือการสื่อความหมายโดยวิธีอื่น สิทธิมนุษยชนเหล่านี้ไม่จำเป็นต้องมีกฎหมายมารองรับ สิทธิเหล่านี้ก็ดำรงอยู่ซึ่งอย่างน้อยอยู่ในมโนธรรมสำนึกถึงบาปบุญคุณโทษที่อยู่ในตัวของแต่ละคน เช่น แม้ไม่มีกฎหมายบัญญัติว่าการฆ่าคนเป็นความผิดตามกฎหมาย แต่คนทุกคนมีสำนึกรู้ได้เองว่าการฆ่าคนนั้นเป็นสิ่งต้องห้าม เป็นบาปในทางศาสนา เป็นต้น

---

[3]United Nations Human Rights office of the High Commissioner for Human Rights, “What are human rights?”,Accedssed 1 Feubulary2016, http://www.ohchr.org/EN/Issues/Pages/WhatareHumanRights.aspx

[4] กองส่งเสริมสิทธิและเสรีภาพ กรมคุ้มครองสิทธิและเสรีภาพ กระทรวงยุติธรรม, “ชุดความรู้สิทธิมนุษยชน สิทธิและเสรีภาพตามรัฐธรรมนูญ สนธิสัญญาหลักระหว่างประเทศด้านสิทธิมนุษยชนที่ประเทศไทยเป็นภาคี”, สืบค้นวันที่ 15 มกราคม 2559,www.rlpd.go.th/rlpdnew/images/rlpd_1/HRC/nhr.pdf

ระดับที่สอง เป็นสิทธิที่ต้องได้รับการรับรองในรูปของกฎหมายหรือต้องได้รับการคุ้มครองโดยรัฐบาล ได้แก่ การได้รับสัญชาติ การมีงานทำ การได้รับความคุ้มครองแรงงาน ความเสมอภาคของหญิงชาย สิทธิของเด็ก เยาวชน ผู้สูงอายุ และคนพิการ การได้รับการศึกษาขั้นพื้นฐาน การประกันการว่างงาน การได้รับบริการทางด้านสาธารณสุข การสามารถแสดงออกทางด้านวัฒนธรรมอย่างอิสระ สามารถได้รับความเพลิดเพลินจากศิลปะ วัฒนธรรมในกลุ่มของต้น เป็นต้น สิทธิมนุษยชนระดับที่สองนี้ต้อง เขียนรับรองไว้ในกฎหมายหรือรัฐธรรมนูญหรือแนวนโยบายพื้นฐานของรัฐแต่ละประเทศ เพื่อเป็นหลักประกันว่าคนทุกคนที่อยู่ในรัฐ นั้นจะได้รับความคุ้มครองชีวิตความเป็นอยู่ให้มีความเหมาะสมแก่ความเป็นมนุษย์

โดยสรุปแล้ว สิทธิมนุษยชน คือ สิทธิขั้นพื้นฐานที่มนุษย์ทุกคนพึงได้รับอย่างเท่าเทียมกัน โดยไม่คำนึงถึงเชื้อชาติ สีผิว เพศ อายุ ภาษา ศาสนา หรือสถานะทางกายภาพหรือสุขภาพอนามัย เป็นสิทธิสากลซึ่งติดตัวบุคคลแต่ละคนไม่สามารถโอนแก่กันได้ ซึ่งสิทธิมนุษยชนนี้สามารถแบ่งออกได้เป็น 5 ประเภทตาม Universal Declaration of Human Rights[5] คือ สิทธิพลเมือง เช่น สิทธิในชีวิตและร่างกาย หรือสิทธิที่จะได้รับการปกป้องจากการจับกุมหรือคุมขังโดยมิชอบ เป็นต้น สิทธิทางการเมือง เช่น สิทธิในการเลือกตั้ง หรือสิทธิในการแสดงความคิดเห็นทางการเมือง เป็นต้น สิทธิในทางเศรษฐกิจ เช่น สิทธิในการเป็นเจ้าของทรัพย์สิน หรือสิทธิในการเลือกทำงานอย่างอิสระ เป็นต้น สิทธิทางสังคม เช่น สิทธิในการศึกษา หรือสิทธิในการได้รับหลักประกันทางสุขภาพ เป็นต้น และ สิทธิทางวัฒนธรรม เช่น สิทธิในการปฏิบัติตามประเพณีท้องถิ่นของตน หรือการปฏิบัติตามความเชื่อทางศาสนา เป็นต้น

เมื่อพูดถึงการคุ้มครองข้อมูลส่วนบุคคลแล้ว การคุ้มครองข้อมูลส่วนบุคคลนั้นมีแนวความคิดพื้นฐานมาจากสิทธิในความเป็นส่วนตัว (Privacy) อันเป็นส่วนหนึ่งของสิทธิมนุษยชนซึ่งได้รับการรับรองใน ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights หรือ UDHR) ข้อ 12[6] ความว่า บุคคลใดจะถูกแทรกแซงตามอำเภอใจในความเป็นส่วนตัว ครอบครัว

---

[5] อฤตา สายคูณ, “โครงงานสิทธิมนุษยชน” สืบค้นวันที่ 23 มีนาคม 2559,http://arueta.blogspot.com/2014/02/blog-post_18.html

[6] **Universal Declaration of Human Rights**

Article 12

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation.

ที่อยู่อาศัย หรือการสื่อสาร หรือจะถูกลบหลู่เกียรติยศและชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองของกฎหมายต่อการแทรกแซงสิทธิหรือการลบหลู่ดังกล่าวนั้น สิทธิในความเป็นส่วนตัว คือ สิทธิที่แต่ละบุคคลตัดสินใจไม่ทำการติดต่อสัมพันธ์กับสังคมเพื่อปิดกั้นตนเองให้รอดพ้นจากการสังเกต การรู้เห็น การสืบความลับ หรือการรบกวนในรูปแบบต่างๆ สิทธิดังกล่าวเช่น สิทธิของแต่ละบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัว เป็นต้น

สำหรับความเป็นมาของแนวความคิดในการปกป้องสิทธิส่วนบุคคลนั้นมิใช่แนวความคิดที่เกิดขึ้นใหม่หากแต่แนวความคิดนี้ได้เริ่มต้นมาตั้งแต่โบราณ ในสมัยโรมันแม้การยอมรับในสิทธิในความเป็นส่วนตัวจะมิได้มีบัญญัติเอาไว้เป็นลายลักษณ์อักษรให้เห็นชัดแจ้งแต่ก็มีแนวความคิดในการยอมรับว่าบุคคลแต่ละคนมีเขตแดนของตนเอง เป็นเสมือนที่พักพิงไม่เกี่ยวข้องกับกิจกรรมทางสังคมในช่วงเวลาหนึ่ง ภายในดินแดนนี้เป็นดินแดนเฉพาะตัวของแต่ละบุคคลเท่านั้นและเป็นที่ปราศจากการเข้ามาเกี่ยวข้องของคนในสังคม นอกเหนือจากหลักนี้แล้วการคุ้มครองความเป็นส่วนตัวยังมีปรากฏให้เห็นในหลักการชดเชยความเสียหายแก่บุคคลคือ Actio iniuriarum ซึ่งเป็นหลักกฎหมายมีขึ้นเพื่อปกป้องตัวบุคคล ชื่อเสียง และศักดิ์ศรีของบุคคลในโรมัน หลักดังกล่าวเป็นหลักในการชดเชยความเสียหาย โดยให้ผู้เสียหายสามารถเรียกค่าสินไหมทดแทนเพื่อความเสียหายที่เกิดขึ้นโดยการกระทำละเมิดซึ่งเกิดขึ้นอย่างจงใจ วัตถุประสงค์ของหลักนี้เป็นการปกป้องโจทก์จากการกระทำที่ผิดกฎหมายและตั้งใจให้เกิดความเสียหายต่อประโยชน์ส่วนบุคคล ซึ่งความเสียหายดังกล่าวอาจเป็นได้ทั้งความเสียหายต่อร่างกาย ชื่อเสียงและศักดิ์ศรี

แต่อย่างไรก็ตามสิทธิในความเป็นส่วนตัวเดิมมิใช่สิทธิที่จะได้รับความคุ้มครองมากนัก เนื่องจากมนุษย์อาศัยอยู่ร่วมกันเป็นครอบครัวขยายมิได้มีห้องนอนเป็นส่วนตัว ภายใต้สภาพการณ์เช่นนี้ทำให้แต่ละคนต่างรู้ข้อมูลข่าวสารของกันและกัน และไม่มีเหตุผลใดๆที่คนเหล่านี้ต้องสนใจติดตามข้อมูลข่าวสารของบุคคลที่มิใช่คนใกล้ตัวคนอื่นอย่างไรก็ตามการปฏิบัติอุตสาหกรรมทำให้เกิดการเปลี่ยนแปลงในบริเทนและยุโรปตะวันตก โดยในยุคปฏิวัติอุตสาหกรรมนี้เป็นการรวมคนนับพันเข้าในโรงงานหรือในสำนักงาน การใช้ชีวิตในยุคปฏิบัติอุตสาหกรรมนี้จึงเปลี่ยนไปจากยุคกสิกรรม

ในยุคอุตสาหกรรมจากครอบครัวขยายเริ่มเปลี่ยนเป็นครอบครัวเดี่ยว คนในต่างจังหวัดเริ่มเข้าเมืองเพื่อหางานและเริ่มติดต่อกับครอบครัวเดิมน้อยลงเรื่อยๆ ซึ่งทำให้คนเริ่มต้องการความเป็นส่วนตัวมากขึ้น ประกอบกับเริ่มมีการแบ่งระดับชั้นทางสังคมทำให้เมื่อคนจำนวนหนึ่งซึ่งมีพื้นหลังและวัฒนธรรมต่างกันมาอยู่ร่วมกันย่อมจะทำให้คนบางส่วนรู้สึกไม่ปลอดภัย ดังจะเห็นได้จากคนที่มี

Everyone has the right to the protection of the law against such interference or attacks.

ฐานะเริ่มสร้างห้องรับแขกเพื่อจำกัดพื้นที่สำหรับผู้มาเยือน ซึ่งในยุคนี้นั่งเองที่การคุ้มครองความเป็นส่วนตัวก็ได้เริ่มต้นขึ้น[7]

2.2 ความหมายของข้อมูลส่วนบุคคล

2.2.1 ข้อมูลส่วนบุคคล

ข้อมูล เป็นกลุ่มอักขระไม่ว่าตัวเลข ตัวอักษร รูปภาพ เสียงหรือสัญลักษณ์ใดๆที่นำมารวมกันแล้วก่อให้เกิดความหมายอย่างใดอย่างหนึ่งอันเป็นข้อเท็จจริงหรือเรื่องราวที่เกี่ยวข้องกับสิ่งต่างๆ เช่น คน สิ่งของ สัตว์ ข้อมูลเป็นรูปแบบที่ใช้สำหรับการสื่อสาร การแปลความหมายและการประมวลผลข้อมูล โดยการประมวลผลนั้นอาจทำได้จากการสังเกต การรวบรวม การวัด หรือการประมวลผลโดยคอมพิวเตอร์ เป็นต้น ข้อมูลเป็นสิ่งที่อยู่รอบๆตัวเรามีประโยชน์ในการดำรงชีวิตไม่ว่าจะเป็นการสื่อสาร การเรียน หรือการตัดสินใจ ข้อมูลสามารถแบ่งออกได้เป็นหลายประเภท กล่าวคือ หากจำแนกตามแหล่งที่มาสามารถแบ่งได้เป็น 2 ประเภท[8] คือ ข้อมูลปฐมภูมิ (Primary Data) อันเป็นข้อมูลที่เก็บจากแหล่งกำเนิดโดยตรง และข้อมูลทุติยภูมิ (Secondary Data) เป็นข้อมูลที่ผู้อื่นเก็บรวบรวมไว้ สามารถนำมาใช้ได้โดยไม่จำต้องเก็บรวบรวมเอง หากแบ่งตามลักษณะของข้อมูลสามารถแบ่งออกได้เป็น 2 ประเภท คือ ข้อมูลเชิงปริมาณ (Quantitative Data) คือข้อมูลที่แสดงออกเป็นตัวเลข แสดงความแตกต่างในเรื่องของปริมาณหรือขนาด เช่น อายุ ผมสัมฤทธิ์ผลในการเรียน หรือคะแนนความถนัดในด้านต่างๆ เป็นต้น และ ข้อมูลเชิงคุณลักษณะหรือเชิงคุณภาพ (Qualitative Data) เป็นข้อมูลซึ่งมิได้แสดงออกเป็นตัวเลข แต่แสดงถึงลักษณะของนั้นๆ เช่น เพศหญิง หรือชาย ศาสนา หรือฐานะทางเศรษฐกิจ เป็นต้น หากแบ่งตามสภาพของข้อมูลที่เกี่ยวข้องกับกลุ่มตัวอย่างสามารถแบ่งออกได้เป็น 3 ประเภท คือ ข้อมูลส่วนบุคคล (Personal Data) ข้อมูลสิ่งแวดล้อม (Environmental Data) และข้อมูลพฤติกรรม (Behavioral Data) นอกจากนี้ข้อมูลยังสามารถถูกจำแนกตามการนำไปใช้กับคอมพิวเตอร์ได้ 5 ประเภท คือ ข้อมูลตัวเลข (Numeric Data) ข้อมูล

---

[7] Henderson, H., Privacy in the information age, (New York: Oxford university press), 1993 p. 3

[8] สำนักงานสถิติแห่งชาติ, “แหล่งที่มาของข้อมูล”, สืบค้นวันที่ 15 กุมภาพันธ์ 2559 ,http://service.nso.go.th/nso/nsopublish/know/estat1_4.html

ตัวอักษร (Text Data) ข้อมูลเสียง (Audio Data) ข้อมูลภาพ (Images Data) และข้อมูลภาพเคลื่อนไหว (Video Data) อีกด้วย[9]

สำหรับข้อมูลส่วนบุคคล (Personal Data) นั้นเป็นประเภทหนึ่งของข้อมูล โดยเป็นข้อมูลที่เกี่ยวข้องกับตัวบุคคลผู้เป็นเจ้าของข้อมูลโดยตรงหรือทำให้สามารถเชื่อมโยงไปยังเจ้าของข้อมูลได้ง่าย เช่น ชื่อ ที่อยู่ อายุ อาชีพ หมายเลขบัตรประจำตัวประชาชน หรืออีเมล์ เป็นต้น เมื่อพิจารณาถึงข้อมูลส่วนบุคคลแล้วอาจก่อให้เกิดความสงสัยว่ามีความครอบคลุมถึงข้อมูลเกี่ยวกับตัวบุคคลมากน้อยเพียงใด จะจำกัดไว้เพียงเฉพาะชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ หรืออีเมล์ของเจ้าของข้อมูลหรือไม่ หากพิจารณาตาม Directive 95/46/EC ได้ให้ความหมายข้อมูลส่วนบุคคลใน Article 2[10] ว่า เป็นข้อมูลใดๆซึ่งเชื่อมโยงไปยังบุคคลที่เป็นเจ้าของข้อมูลหรือเป็นข้อมูลที่อาจระบุตัวบุคคลผู้เป็นเจ้าของข้อมูลได้ไม่ว่าโดยทางตรงหรือทางอ้อม เช่น หมายเลขบัตรประจำตัวประชาชน หรือปัจจัยทางกายภาพที่ทำให้สามารถระบุตัวได้ อย่างไรก็ตามข้อมูลส่วนบุคคลตามความหมายของ Directive 95/46/EC นี้ให้หมายถึงข้อมูลของปัจเจกบุคคลเท่านั้นจึงทำให้ไม่รวมไปถึงข้อมูลของนิติบุคคล

ประเทศอังกฤษได้ให้ความหมายของข้อมูลส่วนบุคคลไว้ใน The Data Protection Act 1998Section 1(1)[11] ว่าหมาถึงข้อมูลซึ่งสามารถระบุตัวเจ้าของข้อมูลนั้นได้โดยอาศัยข้อมูลนั้นเอง

---

[9] นางสาวปรานิสา ทองอ่อน, “ความหมายและประเภทของข้อมูลสารสนเทศ”, สืบค้นวันที่ 15 กุมภาพันธ์ 2559,http://www.seekan.ac.th/it_com/lesson_01_1.html

[10] **DIRECTIVE 95/46/EC**

Article 2

For the purposes of this Directive:

(a) “personal data” shall mean any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological mental, economic, cultural or social identity;

[11] **Data Protection Act 1991**

Section 1 (1)

“personal data” means data which relate to a living individual who can be identified-

หรืออาศัยข้อมูลนั้นประกอบกับข้อมูลอื่นที่อยู่ในความครอบครองขอบผู้ควบคุมข้อมูลหรือข้อมูลที่ผู้ควบคุมข้อมูลมีโอกาสในการได้รับ รวมไปถึงการแสดงความคิดเห็นเกี่ยวกับเจ้าของข้อมูลหรือการแสดงความคิดเห็นเกี่ยวกับเจ้าของข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือบุคคลอื่น

ประเทศแคนาดาได้ให้ความหมายของข้อมูลส่วนบุคคลไว้ใน The Personal Information Protection and Electronic Document Act ว่าหมายถึง ข้อมูลเกี่ยวกับบุคคลที่อาจถูกระบุตัวได้แต่ไม่รวมถึงชื่อ ตำแหน่ง ที่อยู่ทางธุรกิจ หรือเบอร์โทรศัพท์ของลูกจ้างในองค์กร

นอกจากความหมายตามที่ระบุไว้ใน Directive 95/46/EC ประเทศอังกฤษ และประเทศแคนาดาดังที่ได้กล่าวมาแล้วยังมีองค์การที่น่าสนใจคือ องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (Organisation for Economic Co-operation and Development หรือ OECD) ซึ่งได้ให้ความหมายของข้อมูลส่วนบุคคลในแนวทางปฏิบัติเกี่ยวกับข้อมูลส่วนบุคคลโดยระบุไว้ใน Guidelines Governing the Protection of Privacy and Transborder flows of Personal Data หมายถึง ข้อมูลซึ่งเกี่ยวข้องกับตัวบุคคล หรือข้อมูลซึ่งสามรถระบุตัวบุคคลได้

สำหรับประเทศไทยร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ได้ให้ความหมายของข้อมูลส่วนบุคคลไว้ในมาตรา 5 โดยหมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าในทางตรงหรือทางอ้อม แต่ไม่รวมถึงการระบุเฉพาะชื่อ ตำแหน่ง สถานที่ทำงาน หรือที่อยู่ทางธุรกิจของผู้ถึงแก่กรรมโดยเฉพาะ และในพระราชบัญญัติข้อมูลข่าวสารของราชการ มาตรา 3 กำหนดให้ข้อมูลข่าวสารส่วนบุคคล หมายความว่า ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อบรรดาที่มีชื่อของผู้นั้นหรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึก ลักษณะเสียงของคนหรือรูปถ่าย และให้หมายความรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย

(a) From those data, or

(b) From those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

And includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual

จะเห็นได้ว่าข้อมูลส่วนบุคคลนั้นมิได้หมายถึงเพียงชื่อ ที่อยู่ หรือเบอร์โทรศัพท์ของเจ้าของข้อมูลส่วนบุคคลเท่านั้น แต่ยังหมายรวมถึงข้อมูลอื่นๆที่สามารถเชื่อมโยงไปยังเจ้าของข้อมูลส่วนบุคคลได้ไม่ว่าทางตรงหรือทางอ้อม เช่น ลักษณะทางกายภาพ หรือความคิดเห็นทางการเมือง เป็นต้น

2.2.2 ข้อมูลของอุปกรณ์อิเล็กทรอนิกส์

เนื่องจากความหมายของข้อมูลส่วนบุคคลในหลายๆประเทศดังที่กล่าวมามีความครอบคลุมข้อมูลต่างๆที่เกี่ยวกับตัวบุคคลในวงกว้างเมื่อนำมาพิจารณากับเทคโนโลยีคอมพิวเตอร์ที่ก้าวหน้าเป็นอย่างมากในปัจจุบันจนกระทั่งทำให้หลายๆครั้งบุคคลที่ใช้คอมพิวเตอร์นั้นสามารถูกระบุตัวตนได้จากเพียง IP Addressเท่านั้น จึงควรนำปัญหาว่าข้อมูล IP Addressเป็นข้อมูลส่วนบุคคลด้วยหรือไม่มาพิจารณา IP Address นั้นเป็นคำย่อมาจากคำว่า Internet Protocol Address คือ หมายเลขประจำเครื่องคอมพิวเตอร์แต่ละเครื่องในระบบเครือข่าย IP Address แสดงค่าเป็นชุดตัวเลขแบ่งออกเป็น 4 ส่วนโดยมีเครื่องหมายจุดขั้นระหว่างแต่ละส่วนมีค่าตั้งแต่ 0 จนถึง 225 เช่น 192.168.1.1 หรือ 113.53.15.162 เป็นต้น IP Address นี้สามารถแบ่งออกได้เป็น 5 คลาส[12] คือ Class A เป็นคลาสซึ่งมีไว้สำหรับองค์กรขนาดใหญ่ Class B เป็นคลาสซึ่งมีไว้สำหรับองค์กรขนาดกลาง Class C มีไว้สำหรับองค์กรขนาดเล็กและใช้กับเครื่องคอมพิวเตอร์ส่วนใหญ่ในเครือข่าย Class D มีไว้เพื่อการใช้ในเครือข่ายแบบ Multicast เท่านั้น และ Class E ในปัจจุบันยังมิได้มีการนำมาใช้งาน แต่ Class ที่ถูกนำมาใช้งานทั่วไปมีเพียง Class A Class B และ Class C เท่านั้น ซึ่งเราสามารถแบ่งประเภทของ IP Address ออกเป็น 2 ประเภท ดังนี้

(1) Dynamic IP Address คือ การกำหนด IP Address โดยเซิฟเวอร์หรืออุปกรณ์ Dynamic Host Configuration Protocol Sever (หรือ DHCP) ซึ่งผู้ใช้บริการจะได้รับจากผู้ให้บริการอินเตอร์เน็ต (Internet Service Provider หรือ ISP) เมื่อมีการเชื่อมต่ออินเตอร์เน็ต โดย Dynamic IP Address นี้จะเปลี่ยนแปลงทุกครั้งที่มีการเชื่อมต่ออินเตอร์เน็ต

(2) Static IP Address คือ การกำหนด IP Address แบบถาวรโดยผู้ให้บริการอินเตอร์เน็ต (Internet Service Provider หรือ ISP) แก่ผู้ใช้บริการอินเตอร์เน็ต

---

[12]Thai Windows Administrator Blog, พื้นฐาน Protocol TCP/IP และ IP Address, สืบค้นวันที่ 20 กุมภาพันธ์ 2559,http://thaiwinadmin.blogspot.com/2007/12/kb-122007-01.html

ในการคุ้มครองข้อมูลส่วนบุคคลนั้นสำหรับ Static IP Address ย่อมถือเป็นข้อมูลส่วนบุคคลอย่างไม่มีข้อสงสัย เนื่องจาก IP Address ประเภทดังกล่าวสามารถบ่งชี้ไปถึงตัวบุคคลได้ แต่สำหรับ IP Address ประเภท Dynamic แล้วอาจเกิดปัญหาขึ้นว่าจะถือเป็นข้อมูลส่วนบุคคลหรือไม่ เนื่องจาก IP Address ประเภทดังกล่าวมีการเปลี่ยนแปลงทุกครั้งเมื่อผู้ใช้บริการทำการเชื่อมต่ออินเตอร์เน็ตจึงทำให้การระบุตัวบุคคลจาก IP Address ประเภทดังกล่าวต้องอาศัยความร่วมมือจากบุคคลที่สามด้วย

กรณีดังกล่าวศาลยุติธรรมแห่งสหภาพยุโรป (Court of Justice of the European Union หรือ CJEU) ในคดี Scarlet Extnded SA V. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)[13]ซึ่งเกิดขึ้นในประเทศเบลเยี่ยมโดย SABAM เป็นบริษัทรับจัดการทำการเป็นตัวแทนของนักแสดง นักประพันธ์หรือบรรณาธิการเกี่ยวกับการอนุญาตให้ใช้ลิขสิทธิ์ในงานเพลง และ Scarlet เป็นผู้ให้บริการอินเตอร์เน็ต (Internet Service Provider) โดยมิได้มีการให้บริการประเภทอื่นประกอบด้วย ในคดีดังกล่าว SABAM กล่าวอ้างว่าผู้ใช้บริการอินเตอร์เน็ตของ Scarlet ทำการดาวน์โหลดเพลงของ SABAM โดยมิได้รับอนุญาตและไม่มีการจ่ายค่าลิขสิทธิ์ด้วยวิธีการ peer-to-peer ในวันที่ 24 มิถุนายน ค.ศ. 2004 SABAM จึงฟ้อง Scarlet ต่อศาลชั้นต้น ณ กรุงบรัสเซลส์กล่าวอ้างว่าลิขสิทธิ์ในงานเพลงที่อยู่ในครอบครองของ SABAM นั้นถูกละเมิดโดยเฉพาะอย่างยิ่งสิทธิในการทำซ้ำและสิทธิในการเผยแพร่ต่อสาธารณะเนื่องมากจากการแบ่งปันเพลงซึ่งอยู่ในรูปไฟล์อิเล็กทรอนิกส์ (Electronic File) ด้วยวิธีการ peer-to-peer โดยมิได้รับอนุญาตผ่านเครือข่ายของ Scarlet และขอให้ Scarlet ทำการบล็อกการกระทำที่ผิดกฎหมายดังกล่าวหรือทำให้ผู้ใช้บริการไม่สามารถทำการส่งหรือรับไฟล์เพลงผ่านวิธีการ peer-to-peer โดยไม่ได้รับอนุญาตจากเจ้าของลิขสิทธิ์ได้ ในคดีนี้ศาลชั้นต้น ณ กรุงบรัสเซลส์มีคำสั่งให้ Scarlet ดำเนินการมิให้ผู้ใช้บริการของตนสามารถส่งหรือรับไฟล์เพลงที่ SABAM มีลิขสิทธิ์โดยวิธีการ peer-to-peer ได้ Scarlet อุทธรณ์โดยอ้างเหตุผลหลายประการซึ่งหนึ่งในเหตุผลที่ Scarlet อ้างนั้นคือ การติดตั้งระบบตัวกรองนั้นขัดต่อกฎหมายของสหภาพยุโรปว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเนื่องจากตัวกรองดังกล่าวมีการประมวลผล IP Address ซึ่งถือเป็นข้อมูลส่วนบุคคล ศาลอุทธรณ์แห่งกรุงบรัสเซลส์จึงได้ตัดสินให้มีการเลื่อนคดีและส่งข้อซักถามไปยังศาลยุติธรรมแห่งสหภาพยุโรป

ศาลยุติธรรมแห่งสหภาพยุโรปพิจารณาว่าการใช้ตัวกรองดังกล่าวนี้เกี่ยวกับการวิเคราะห์เนื้อหาและการเก็บรวบรวมและการระบุ IP Address ของผู้ใช้บริการซึ่งกระทำการละเมิด

---

[13]Case C-70/10

ลิขสิทธิ์บนเครือข่ายอินเตอร์เน็ต โดย IP Address ดังกล่าวได้รับความคุ้มครองในฐานะเป็นข้อมูลส่วนบุคคลเนื่องจากสามารถระบุตัวบุคคลผู้ใช้บริการได้

สำหรับประเทศแคนาดา The Office of the Privacy Commissioner of Canada ได้ให้ความเห็นเกี่ยวกับ IP Address ว่าการรับรู้ถึงข้อมูล IP Address เป็นจุดเริ่มต้นของการเก็บรวบรวมกิจกรรมออนไลน์ของบุคคลซึ่งสามารถทำให้ทราบได้ถึงผู้ให้บริการอินเตอร์เน็ตของบุคคลนั้น ความสนใจของเจ้าของ IP Address โดยพิจารณาจากเว็บไซต์ที่เข้าเยี่ยมชม และการติดต่อกับองค์กรต่างๆ นอกจากนี้ข้อมูลดังกล่าวยังสามารถบอกสิ่งต่างๆได้อีกหลายประการ เช่น การเรียนรู้ของเจ้าของข้อมูล บุคคลที่เจ้าของข้อมูลติดต่อสื่อสารด้วย และสถานที่ที่เจ้าของข้อมูลไป เป็นต้น พร้อมกันนั้นข้อมูลต่างๆที่ได้รับมาจาก IP Address นี้ เช่น การติดต่อสื่อสารกับบุคคลอื่น หรือสถานที่ที่เจ้าของข้อมูลไป เป็นต้น ยังสามารถนำมาใช้เพื่อแสวงหาข้อมูลอื่นๆเกี่ยวกับเจ้าของข้อมูลได้อีกด้วย ด้วยเหตุนี้หาก IP Address ดังกล่าวมีข้อมูลที่สามารถเชื่อมโยงไปยังเจ้าของข้อมูลได้ IP Address นี้ถือเป็นข้อมูลส่วนบุคคล[14]

นอกจาก IP Address ดังที่ได้กล่าวมาแล้วคอมพิวเตอร์แต่ละเครื่องได้ถูกบรรจุหมายเลข Media access control address หรือ Mac Address ซึ่งเป็นหมายเลขประจำตัวของอุปกรณ์ไม่ว่าจะเป็นคอมพิวเตอร์ หรือสมาร์ทโฟน เป็นค่าที่ใช้อ้างอิงที่อยู่กายภาพของการ์ดแลนด์และการ์ดไวไฟ ถูกกำหนดโดยผู้ผลิตซึ่งแต่ละการ์ดนั้นจะมีค่าไม่ซ้ำกันและจะไม่มีการเปลี่ยนแปลง การแสดงค่าจะแสดงค่าเป็นตัวเลขฐาน 16 จำนวน 6 ชุด เช่น 00-04-23-75-03-DF หรือ 00-08-CA-E7-5B-E0 เป็นต้น Mac Address สามารถนำไปใช้ประโยชน์ได้หลายประการ เช่น ใช้เพื่อการเชื่อมต่ออินเตอร์เน็ต หรือ ใช้เพื่อการตรวจสอบการใช้งาน เป็นต้น สำหรับ Mac Address นั้นยังคงมีข้อโต้เถียงกันว่าจะถือเป็นข้อมูลส่วนบุคคลหรือไม่ ซึ่งหากมองโดยผิวเผินแล้ว Mac Address ย่อมเป็นเพียงข้อมูลที่เชื่อมโยงไปยังเครื่องคอมพิวเตอร์หรือสมาร์ทโฟนเครื่องใดเครื่องหนึ่งเท่านั้น มิใช่ข้อมูลเกี่ยวกับบุคคล แต่ Mac Address นั้นสามารถบ่งชี้ได้ถึงกิจกรรมที่เจ้าของคอมพิวเตอร์หรือสมาร์ทโฟนใช้งาน และ Mac Address ยังสามารถใช้ในการติดตามอุปกรณ์คอมพิวเตอร์หรือสมาร์ทโฟนได้ เช่น จากการเชื่อมต่อสัญญา Wi-Fi ผ่านจุดส่งสัญญาณต่างๆ

Mac Address นี้ ตามความเห็นของArticle 29Data protection working party ในเรื่องการให้บริการการบอกตำแหน่งบนสมาร์ทโฟน เห็นว่า Mac Address สามารถใช้ในการระบุ

---

[14]Technology Analysis Branch of the Office Privacy Commissioner of Canada, “What an IP Address Can Reveal About You”, Accedssed 15 January 2016,https://www.priv.gc.ca/information/research-recherche/2013/ip_201305_e.asp

ตำแหน่งของเครื่องได้จาการคำนวณจุดที่เครื่องพบหรือเชื่อมต่อกับ Wi-Fi จึงทำให้ Mac Address นี้เข้าข่ายเป็นข้อมูลส่วนบุคคล

เมื่อพิจารณาแล้วข้อมูลที่เกี่ยวกับเครื่องคอมพิวเตอร์หรือสมาร์ทโฟน ได้แก่ Mac Address ซึ่งถือเป็นข้อมูลส่วนบุคคลเนื่องจากไม่มีการเปลี่ยนแปลง สามารถเก็บรวบรวมและประมวลผลเพื่อเชื่อมโยงไปยังเจ้าของข้อมูลส่วนบุคคลได้ง่าย สำหรับ IP Address ประเภท Static มีลักษณะเช่นเดียวกับข้อมูล Mac Address จึงเป็นข้อมูลส่วนบุคคล แต่ข้อมูล IP Address ประเภท Dynamic จะถือเป็นข้อมูลส่วนบุคคลก็ต่อเมื่อผู้เก็บรวบรวมข้อมูลมีข้อมูลอย่างอื่นประกอบทำให้สามารถเชื่อมโยงไปยังเจ้าของคอมพิวเตอร์หรือสมาร์ทโฟนเครื่องนั้นๆได้

2.3 ประเภทของข้อมูลส่วนบุคคล

ในการให้ความคุ้มครองข้อมูลส่วนบุคคลสามารถแบ่งความคุ้มครองแก่ข้อมูลออกเป็นสองประเภทแตกต่างกัน คือ ข้อมูลทั่วไป (Non-Sensitive Data) และข้อมูลประเภทที่มีความอ่อนไหว (Sensitive Data) โดยข้อมูลแต่ละประเภทมีลักษณะดังนี้

(1) ข้อมูลทั่วไป (Non-Sensitive Data) คือ ข้อมูลเกี่ยวกับบุคคลผู้เป็นเจ้าของข้อมูลซึ่งสามารถบ่งชี้เฉพาะเจาะจงไปยังเจ้าของข้อมูลได้ เช่น ชื่อ ที่อยู่ อาชีพ อายุ เบอร์โทรศัพท์ การศึกษา สถานภาพในการสมรส ตำแหน่งหน้าที่ทางการงาน หรือลักษณะทางกายภาพของบุคคล เป็นต้น ข้อมูลประเภทดังกล่าวเป็นข้อมูลซึ่งมิได้มีความละเอียดอ่อนจนอาจนำมาสู่ปัญหาต่างๆได้ จึงทำให้ข้อมูลดังกล่าวเป็นข้อมูลที่อาจเก็บรวบรวม เปิดเผย หรือใช้ได้ ทั้งนี้ภายใต้หลักเกณฑ์ที่กฎหมายกำหนดไว้

(2) ข้อมูลประเภทที่มีความอ่อนไหว (Sensitive Data) คือ ข้อมูลของบุคคลซึ่งถือเป็นเรื่องเฉพาะตัวของตัวบุคคล เป็นข้อมูลซึ่งมีความละเอียดอ่อนสูง กล่าวคือข้อมูลประเภทดังกล่าวเป็นข้อมูลซึ่งหากมีการเปิดเผยอาจก่อให้เกิดผลกระทบที่ไม่พึงประสงค์ตามมา เช่น กระทบต่อความรู้สึกของเจ้าของข้อมูลหรือประชาชนทั่วไป เป็นข้อมูลที่ก่อให้เกิดความขัดแย้งได้ ก่อให้เกิดผลกระทบต่อชื่อเสียงหรือเกียรติคุณของเจ้าของข้อมูล หรือเป็นข้อมูลซึ่งหากมีการเปิดเผยอาจก่อให้เกิดการตั้งข้อรังเกียจหรือเลือกปฏิบัติหรือเกิดอันตรายต่อเจ้าของข้อมูล เป็นต้น โดยข้อมูลประเภทดังกล่าวเจ้าของข้อมูลประสงค์ที่จะเก็บข้อมูลประเภทนี้ไว้เป็นความลับหรือไม่ประสงค์ให้มีการเปิดเผยข้อมูล เช่น ข้อมูลเกี่ยวกับเชื้อชาติ เผาพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อเกี่ยวกับลัทธิ ศาสนา พฤติกรรมทางเพศ ประวัติสุขภาพ ประวัติอาชญากรรม หรือ สถานะทางการเงิน เป็นต้น

สำหรับหลักเกณฑ์ในการให้ความคุ้มครองต่อข้อมูลทั้งสองประเภทดังกล่าวมีความแตกต่างกัน เนื่องจากการเก็บรวบรวม เปิดเผย หรือใช้ข้อมูลส่วนบุคคลประเภทที่มีความอ่อนไหว (Sensitive Data) อาจนำมาซึ่งปัญหาต่างๆดังที่ได้กล่าวมาแล้ว ดังนั้น ในหลายๆประเทศข้อมูลประเภทที่มีความอ่อนไหว (Sensitive Data) จึงถูกกำหนดให้เป็นข้อมูลที่ห้ามทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลโดยเด็ดขาด เว้นแต่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล หรือเป็นกรณีอื่นตามที่กฎหมายกำหนดไว้ เช่น เป็นการปฏิบัติตามกฎหมาย หรือเป็นการจำเป็นเพื่อการดำเนินคดี เป็นต้น แต่ข้อมูลประเภทข้อมูลทั่วไปนั้น (Non-Sensitive Data) กฎหมายกำหนดให้สามารถทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลได้ หากได้รับความยินยอมจากเจ้าของข้อมูล

นอกจากนี้ยังสามารถแบ่งประเภทของข้อมูลส่วนบุคคลในประเด็นเกี่ยวกับความอ่อนไหวที่อาจส่งผลกระทบต่อผู้เป็นเจ้าของข้อมูลส่วนบุคคลหากมีการเปิดเผยหรือล่วงรู้ข้อมูลนั้นได้เป็น 3 ระดับ[15] ดังนี้

(1) ข้อมูลข่าวสารประเภทที่มีความอ่อนไหวในระดับต่ำ (Low-sensitivity) ข้อมูลประเภทนี้เป็นข้อมูลที่เกี่ยวข้องกับบุคคลเป็นข้อมูลที่มีความอ่อนไหวเนื่องจากข้อมูลเหล่านี้ทำให้มีโอกาสได้มาซึ่งข้อมูลที่มีระดับความอ่อนไหวสูงขึ้น

(2) ข้อมูลข่าวสารประเภทที่มีความอ่อนไหวระดับปานกลาง (Moderate-sensitivity) ข้อมูลประเภทนี้เป็นข้อมูลที่มีความอ่อนไหวมาก กล่าวคือที่มีโอกาสอย่างมากที่จะก่อให้เกิดความเสียหายเมื่อข้อมูลถูกนำไปใช้ในทางที่ผิด ข้อมูลประเภทนี้ครอบคลุมถึงข้อมูลประเภทที่เกี่ยวความคิดเห็นของบุคคล ซึ่งมีความครอบคลุมในทุกเรื่องของชีวิต ข้อมูลที่มีความอ่อนไหวระดับปานกลางนี้สำคัญเช่นเดียวกันกับข้อมูลที่มีความอ่อนไหวระดับสูงและไม่ควรถูกเก็บรวบรวมโดยสิ้นเชิง

(3) ข้อมูลข่าวสารประเภทที่มีความอ่อนไหวระดับสูง (High-sensitivity) ข้อมูลประเภทนี้ ได้แก่ ข้อมูลรายละเอียดส่วนตัวของบุคคลที่เกี่ยวกับประวัติทางการแพทย์ พฤติกรรมทางเพศ หรือข้อเท็จจริงด้านอื่นๆของชีวิตของบุคคล โดยส่วนใหญ่แล้วนับว่าเป็นเรื่องเป็นเรื่องส่วนตัวหรือลับเฉพาะ ข้อมูลประเภทที่มีความอ่อนไหวสูงนี้จึงมีความสำคัญและไม่ควรถูกเก็บรวบรวมโดยสิ้นเชิงเช่นเดียวกันกับข้อมูลข่าวสารที่มีความอ่อนไหวระดับปานกลาง

---

[15] นรินทร์ จุ่มศรี, “มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลจากการใช้บริการเครือข่ายสังคมออนไลน์”, (วิทยานิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยธุรกิจบัณฑิตย์, 2555), น. 31.

2.4 หลักการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

เนื่องจากข้อมูลส่วนบุคคลเป็นสิ่งสำคัญในการพัฒนาเศรษฐกิจ การดำเนินธุรกิจล้วนอาศัยข้อมูลเป็นปัจจัยสำคัญ ดังนั้นประเทศต่างๆจึงให้ความคุ้มครองแก่ข้อมูลส่วนบุคคลโดยนำหลักการทั่วไปในการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งหลักการขององค์การต่างๆ เช่น องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (Organization for Economic Co-operation and Development หรือ OECD) หรือองค์การสหประชาชาติ เป็นต้น มาเป็นแนวทางในการร่างกฎหมายเพื่อที่จะสามารถทำความเข้าใจกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลของนานาประเทศได้ดีจึงควรศึกษาหลักการทั่วไป และหลักการขององค์การต่างๆ ซึ่งมีรายละเอียดดังนี้

2.4.1 หลักการทั่วไป

หลักการพื้นฐานของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในระดับสากลนั้นมีหลักการสำคัญซึ่งเป็นหัวใจของเรื่องอยู่ 9 ประการ ได้แก่[16]

2.4.1.1 หลักการจัดเก็บข้อมูลส่วนบุคคลอย่างจำกัด (Collection Limitation Principle)

หลักการดังกล่าวกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องเก็บรวบรวมและประมวลผลข้อมูลส่วนบุคคลอย่างจำกัดเพียงเท่าที่จำเป็นเท่านั้น และการเก็บรวบรวมข้อมูลส่วนบุคคลต้องกระโดยวิธีการที่เป็นธรรมและชอบด้วยกฎหมาย นอกจากนี้ต้องกระทำภายใต้ความรับรู้และความยินยอมจากบุคคลผู้เป็นเจ้าของข้อมูลส่วนบุคคลด้วย

2.4.1.2 หลักการประมวลผลข้อมูลส่วนบุคคลอย่างมีคุณภาพและได้สัดส่วน (Data Quality and Proportional Principle)

หลักการดังกล่าวกำหนดให้ข้อมูลส่วนบุคคลที่ทำการประมวลผลนั้นต้องมีความเกี่ยวข้อง เพียงพอ และได้สัดส่วนหรือเกี่ยวเนื่องกับวัตถุประสงค์ที่ได้แจ้งไว้แก่เจ้าของข้อมูลส่วนบุคคล นอกจากนี้ข้อมูลส่วนบุคคลนั้นต้องมีถูกต้องสมบูรณ์และมีการปรับปรุงให้ทันสมัยอยู่ตลอดเวลาเมื่อผู้ควบคุมข้อมูลส่วนบุคคลจะทำการประมวลผลและใช้ข้อมูลส่วนบุคคลนั้น อย่างไรก็ดีหลักการนี้ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลนั้นจัดเก็บและประมวลผลข้อมูลส่วนบุคคลประเภทที่มีความ

---

[16] จันทจิรา เอี่ยมมยุรา. “แนวคิดและหลักการยกร่างกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย”, วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, หน้า 653-657,(ธันวาคม 2547).

อ่อนไหว (Sensitive Data) เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยชัดแจ้งซึ่งข้อมูลประเภทที่มีความอ่อนไหว เช่น ข้อมูลเกี่ยวกับชาติกำเนิด ความเชื่อทางศาสนา หรือความเชื่อทางปรัชญา เป็นต้น

2.4.1.3 หลักการระบุวัตถุประสงค์และระยะเวลาในการใช้ข้อมูลส่วนบุคคล (Purpose Specification Principle)

หลักการดังกล่าวกำหนดให้ต้องมีการระบุวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลก่อนหรือในขณะที่ทำการประมวลผลข้อมูลส่วนบุคคล การประมวลผลข้อมูลส่วนบุคคลภายหลังสามารถกระทำได้หากเป็นเพียงเพื่อให้สำเร็จตามวัตถุประสงค์ หรือเพื่อการอื่นที่ไม่ขัดหรือแย้งกับวัตถุประสงค์ที่ได้แจ้งไว้ อย่างไรก็ตามหากมีการเปลี่ยนแปลงวัตถุประสงค์ ผู้ควบคุมข้อมูลส่วนบุคคลต้องระบุวัตถุประสงค์การใช้ที่เปลี่ยนแปลงไปนั้นทุกคราวด้วย นอกจากนี้การเก็บและใช้ข้อมูลส่วนบุคคลนั้นต้องไม่เกินกว่าระยะเวลาที่จำเป็นเพื่อให้วัตถุประสงค์ที่ได้แจ้งไว้สำเร็จลุล่วง

2.4.1.4 หลักการใช้ข้อมูลส่วนบุคคลอย่างจำกัด (Use Limitation Principle)

หลักการดังกล่าวห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลเปิดเผยทำให้สามารถเข้าถึงได้ หรือนำข้อมูลส่วนบุคคลไปใช้เพื่อการอย่างอื่นนอกจากจากวัตถุประสงค์อื่นซึ่งไม่ขัดหรือแย้งกับวัตถุประสงค์ที่ได้แจ้งไว้ เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือเป็นการใช้อำนาจตามบทบัญญัติของกฎหมายเพื่อความมั่นคงของประเทศ ความสงบเรียบร้อยของสังคม ประโยชน์สาธารณะ เพื่อการปฏิบัติตามกฎหมาย หรือเพื่อประโยชน์มหาชนอื่นๆ

นอกจากนี้ยังกำหนดให้บุคคลใดซึ่งมิใช่ผู้จัดเก็บข้อมูลส่วนบุคคลจะนำข้อมูลส่วนบุคคลนั้นไปเปิดเผยโดยเจ้าของมิได้ยินยอมมิได้ แม้ทั้งการเปิดเผยนั้นจะมิได้ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลเลยก็ตาม นอกจากนี้เมื่อเจ้าของข้อมูลส่วนบุคคลอนุญาตให้มีการเปิดเผยแล้ว เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการเพิกถอนความยินยอมเพื่อยุติการเผยแพร่ข้อมูลส่วนบุคคลนั้นได้ตลอดเวลา

2.4.1.5 หลักการป้องกันรักษาความปลอดภัยของข้อมูลส่วนบุคคล (Security Safeguard Principle)

หลักการนี้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีระบบการป้องกันรักษาความปลอดภัยของข้อมูลเพื่อมิให้ข้อมูลส่วนบุคคลนั้นสูญหาย ถูกเข้าถึง ถูกทำลาย มีการใช้หรือเปลี่ยนแปลงแก้ไข หรือมีการเปิดเผยข้อมูลโดยบุคคลซึ่งปราศจากอำนาจ

2.4.1.6 หลักเปิดเผยโปร่งใส (Openness Principle)

หลักการดังกล่าวกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องประกาศนโยบายในการประมวลผลข้อมูลส่วนบุคคล โดยมีวัตถุประสงค์เพื่อให้ผู้ที่เกี่ยวข้องทราบถึงการจัดเก็บหรือการ

รวบรวมข้อมูลส่วนบุคคล หรือการนำข้อมูลส่วนบุคคลนั้นไปใช้ ระบบการประมวลผลข้อมูลส่วนบุคคลต้องสามารถแสดงให้เห็นถึงความมีอยู่และประเภทของข้อมูลส่วนบุคคล วัตถุประสงค์ของการใช้ข้อมูลส่วนบุคคล รวมทั้งชื่อและสถานที่ตั้งของนายทะเบียนผู้ทำหน้าที่ในการประมวลผลข้อมูลส่วนบุคคล

2.4.1.7 หลักการมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation Principle)

หลักการดังกล่าวกำหนดสิทธิให้แก่เจ้าของข้อมูลส่วนบุคคลซึ่งเป็นปัจเจกบุคคล ดังต่อไปนี้

(1) ได้รับแจ้งหรือยืนยันจากนายทะเบียนว่าได้ทำการประมวลผล ใช้ หรือโอนข้อมูลส่วนบุคคลของตนหรือไม่

(2) ได้รับการติดต่อจากนายทะเบียนเกี่ยวกับข้อมูลส่วนบุคคลของตน

(2.1) ภายในเวลาอันสมควร

(2.2) อาจมีค่าใช้จ่ายได้แต่ต้องไม่เกินสมควร

(2.3) โดยวิธีที่เหมาะสม

(2.4) โดยรูปแบบที่เจ้าของข้อมูลส่วนบุคคลสามารถเข้าใจได้

(3) ได้รับเหตุผลเมื่อคำร้องตามข้อ (1) และ (2) ถูกปฏิเสธและมีสิทธิในการอุทธรณ์การปฏิเสธนั้น

(4) คัดค้านการประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับตน และหากการโต้แย้งนั้นรับฟังได้มีสิทธิขอให้ลบหรือทำลายข้อมูลส่วนบุคคล ปรับปรุงหรือแก้ไขเพิ่มเติมเพื่อให้ข้อมูลส่วนบุคคลนั้นถูกต้องและสมบูรณ์

2.4.1.8 หลักข้อจำกัดในการส่งหรือโอนข้อมูลส่วนบุคคลให้แก่บุคคลอื่นข้ามพรมแดน (Restriction on Onward Opposition)

หลักการดังกล่าวมีวัตถุประสงค์เพื่อป้องกันมิให้มีการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้รับที่อยู่ในประเทศซึ่งปราศจากกฎหมายและวิธีปฏิบัติที่สามารถเป็นหลักประกันการคุ้มครองข้อมูลส่วนบุคคลอย่างเพียงพอ เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือมีสัญญาส่งโอนข้อมูลส่วนบุคคลระหว่างกันที่ให้หลักประกันอย่างเพียงพอ

2.4.1.9 หลักความรับผิดชอบของนายทะเบียน (Accountability Principle)

ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามหลักการที่ (1) ถึง (8) อย่างเคร่งครัด หากฝ่าฝืนหลักการดังกล่าวและก่อให้เจ้าของข้อมูลส่วนบุคคลได้รับความเสียหาย ควบคุมข้อมูลส่วนบุคคลต้องรับผิดทั้งในทางแพ่งและทางอาญา และรับผิดในค่าใช้จ่ายเพื่อแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง รวมไปถึงต้องลบหรือทำลายข้อมูลส่วนบุคคลอีกด้วย

2.4.2 Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data

องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (Organization for Economic Co-operation and Development หรือ OECD) ได้ออกแนวปฏิบัติ OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data มีขึ้นเพื่อดูแลการส่งผ่านข้อมูลระหว่างประเทศ การคุ้มครองข้อมูลส่วนบุคคลและการคุ้มครองสิทธิความเป็นส่วนตัว จุดเริ่มต้นของแนวปฏิบัติดังกล่าวเกิดจากคามไม่เท่าเทียมกันของบทบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในประเทศต่างๆอันอาจนำมาซึ่งการขัดขวางการไหลเวียนของข้อมูลระหว่างประเทศ แนวปฏิบัติดังกล่าวเป็นแนวปฏิบัติขั้นต่ำของหลักการเพื่อให้ประเทศสมาชิกได้นำไปปฏิบัติโดยมิได้แบ่งแยกระหว่างหน่วยงานของรัฐและหน่วยงานเอกชน และมีวัตถุประสงค์เพื่อเป็นเครื่องมือในการสร้างความเป็นอันหนึ่งอันเดียวกันของประเทศสมาชิก OECD เพื่อก่อให้เกิดความเชื่อมั่นแก่ภาคเอกชนและผู้ประกอบธุรกิจในการติดต่อสัมพันธ์ทางการค้า ภายใต้ Section 1[17] ของแนวปฏิบัติข้อมูลส่วนบุคคล (Personal Data) หมายถึง ข้อมูลใดๆที่เกี่ยวข้องเฉพาะตัวบุคคลหรือสามารถชี้ให้เห็นลักษณะเฉพาะของตัวบุคคลผู้เป็นเจ้าของข้อมูลได้ แนวปฏิบัติดังกล่าวมีหลักการที่สำคัญกล่าวคือ

(1) หลักการเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด (Collection Limitation Principle)

---

[17]**Guidelines governing the protection of privacy and transborder flows of personal data**

1.For the purposes of these Guidelines:

a) “Personal Data” means any information relating to an identified or identifiable individual (data subject)

หลักการดังกล่าวกำหนดให้ต้องมีการจำกัดการจัดเก็บรวบรวมข้อมูลส่วนบุคคล และข้อมูลส่วนบุคคลดังกล่าวต้องได้มาโดยวิธีที่ชอบด้วยกฎหมาย และควรได้รับมาภายใต้ความยินยอมหรือความรับรู้ของเจ้าของข้อมูลส่วนบุคคล

(2) หลักคุณภาพของข้อมูล (Data Quality Principle)

หลักการดังกล่าวกำหนดให้ข้อมูลส่วนบุคคลนั้นต้องเกี่ยวข้องกับวัตถุประสงค์ในการจัดเก็บรวบรวมข้อมูลส่วนบุคคล และข้อมูลส่วนบุคคลนั้นต้องถูกต้อง สมบูรณ์ และเป็นปัจจุบัน

(3) หลักการกำหนดวัตถุประสงค์ (Purpose Specification Principle)

หลักการดังกล่าวกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลในเวลาที่จัดเก็บรวบรวมข้อมูลนั้น และการนำข้อมูลส่วนบุคคลที่จัดเก็บนั้นไปใช้ต้องเป็นไปเพียงเพื่อให้บรรลุวัตถุประสงค์ที่ได้แจ้งไว้ หรือหากผู้ควบคุมข้อมูลส่วนบุคคลต้องการใช้ข้อมูลส่วนบุคคลนั้นเพื่อวัตถุประสงค์อื่นซึ่งไม่ขัดต่อวัตถุประสงค์ที่ได้แจ้งไว้ในขณะทำการเก็บรวบรวมต้องมีการการแจ้งวัตถุประสงค์ที่เปลี่ยนแปลงไปให้เจ้าของข้อมูลทราบ

(4) หลักการใช้ข้อมูลส่วนบุคคลอย่างจำกัด (Use Limitation Principle)

หลักการดังกล่าวกำหนดห้ามมิให้ผู้เก็บรวบรวมข้อมูลส่วนบุคคลทำการเปิดเผยข้อมูลส่วนบุคคล ทำให้บุคคลอื่นสามารถใช้ได้ หรือใช้เพื่อวัตถุประสงค์อื่นนอกจากวัตถุประสงค์ที่ได้แจ้งไว้ขณะเก็บรวบรวมข้อมูล เว้นแต่

1. ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือ
2. เป็นการปฏิบัติตามบทบัญญัติกฎหมาย

(5) หลักการรักษาความปลอดภัย (Security Safeguards Principle)

หลักการดังกล่าวกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องมีหลักเกณฑ์ในการรักษาความปลอดภัยที่เหมาะสมแก่ข้อมูลส่วนบุคคลเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นจากการสูญหาย การเข้าถึงโดยมิได้รับอนุญาต การทำลาย การใช้ การเปลี่ยนแปลง หรือการเปิดเผยข้อมูลส่วนบุคคลดังกล่าว

(6) หลักการเปิดเผย (Openness Principle)

หลักการดังกล่าวกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องกำหนดวิธีการทั่วไปเกี่ยวกับการการเปิดเผยถึงการนำไปใช้ แนวทางปฏิบัติ และนโยบายเกี่ยวกับข้อมูลส่วนบุคคล การเปิดเผยดังกล่าวต้องแสดงถึงความมีอยู่ของข้อมูลส่วนบุคคล ลักษณะของข้อมูลส่วนบุคคล และ

วัตถุประสงค์ในการนำข้อมูลส่วนบุคคลไปใช้ รวมไปถึงชื่อของผู้เก็บรวบรวมข้อมูลส่วนบุคคลและที่ทำการของผู้ควบคุมข้อมูลส่วนบุคคล

(7) หลักการมีส่วนร่วมของปัจเจกบุคคล (Individual Participation Principle)

ภายใต้หลักการดังกล่าวปัจเจกบุคคลมีสิทธิ

a) ได้รับการบอกกล่าวจากผู้ควบคุมข้อมูลส่วนบุคคลเพื่อยืนยันถึงการมีอยู่ซึ่งข้อมูลส่วนบุคคลของปัจเจกบุคคลนั้น

b) ได้รับการแจ้งถึงข้อมูลส่วนบุคคลของตนโดย

i ภายในระยะเวลาพอสมควร

ii มีค่าใช้จ่ายไม่เกินสมควร

iii โดยวิธีการที่เหมาะสม

iv ในรูปแบบซึ่งเจ้าของข้อมูลสามารถเข้าใจได้

c) ได้รับการแจ้งถึงเหตุผลหากการร้องขอตามข้อ a) และข้อ b) ถูกปฏิเสธ และมีสิทธิในการอุทธรณ์การปฏิเสธดังกล่าว

d) มีสิทธิคัดค้านข้อมูลส่วนบุคคลเกี่ยวกับตน หากคำคัดค้านมีเหตุผลเจ้าของข้อมูลมีสิทธิขอให้ลบข้อมูล ทำให้สมบูรณ์ แก้ไขหรือปรับปรุงข้อมูลนั้น

(8) หลักความเชื่อถือได้ (Accountability Principle)

หลักการดังกล่าวกำหนดให้ผู้ควบคุมข้อมูลต้องปฏิบัติตามหลักการข้อ (1) ถึง (7) โดยผู้ควบคุมข้อมูลต้องจัดให้มีแผนในการจัดการเกี่ยวกับความเป็นส่วนตัวซึ่งมีลักษณะ 6 ประการ คือ

1. แผนในการจัดการเกี่ยวกับความเป็นส่วนตัวต้องจัดให้มีแนวปฏิบัติเกี่ยวกับข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของตน

2. แผนในการจัดการเกี่ยวกับความเป็นส่วนตัวต้องเหมาะสมต่อโครงสร้าง ขนาด ปริมาณ และความอ่อนไหวของการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคล

3. แผนในการจัดการเกี่ยวกับความเป็นส่วนตัวต้องกำหนดให้มีมาตรการป้องกันที่เหมาะสมโดยพิจารณาจากการประเมินความเสี่ยงในด้านความเป็นส่วนตัว

4. แผนในการจัดการเกี่ยวกับความเป็นส่วนตัวต้องถูกรวมอยู่ในโครงสร้างการกำกับดูและแลจัดให้มีองค์กรกำกับดูแลภายใน

5. แผนในการจัดการเกี่ยวกับความเป็นส่วนตัวต้องระบุถึงแผนการจัดการกรณีที่เกิดเหตุไม่คาดฝัน

6. แผนในการจัดการเกี่ยวกับความเป็นส่วนตัวต้องได้รับการปรับปรุงให้เป็นไปตามการตรวจสอบและการประเมิน

ผู้ควบคุมข้อมูลส่วนบุคคลต้องสามารถแสดงแผนในการจัดการความเป็นส่วนตัวให้แก่หน่วยงานที่กำกับดูแลได้ ทั้งต้องแจ้งแก่หน่วยงานที่มีหน้าที่กำกับดูแลหากมีการฝ่าฝืนความปลอดภัยอย่างมีนัยสำคัญซึ่งกระทบต่อข้อมูลส่วนบุคคล และหากการฝ่าฝืนนั้นอาจก่อให้เกิดผลร้ายต่อเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งแก่เจ้าของข้อมูลที่อาจได้รับความเสียหายอีกด้วย

2.4.3 Guidelines for the Regulation of Computerized Personal Data Files 1990 (United Nations 1990)

ในปี 1990 องค์การสหประชาชาติได้บังคับใช้ Guidelines for the Regulation of Computerized Personal Data Files (United Nations 1990) การบังคับใช้แนวปฏิบัติดังกล่าวแสดงว่าองค์การสหประชาชาติได้เล็งเห็นถึงความสำคัญในการคุ้มครองข้อมูลส่วนบุคคลมิใช่เพียงในประเทศที่พัฒนาแล้วแต่ต้องรวมไปถึงทุกประเทศทั่วโลก อย่างไรก็ตามมีข้อน่าสังเกตว่าแนวปฏิบัตินี้เป็นเพียงข้อแนะนำแก่ประเทศต่างๆเพื่อการร่างกฎหมายและแก่องค์การระหว่างประเทศเท่านั้น โดยมิได้มีสถานะเป็นกฎหมายในอันที่จะบังคับประเทศต่างๆหรือองค์การต่างๆได้ โดย Guidelines for the Regulation of Computerized Personal Data Files 1990 มีหลักการ ดังนี้

(1) หลักความชอบด้วยกฎหมายและความเป็นธรรม (Principle of lawfulness and fairness)

หลักการดังกล่าวกำหนดให้ข้อมูลซึ่งเกี่ยวกับบุคคลต้องถูกเก็บรวบรวมและถูกประมวลผลอย่างเป็นธรรมและโดยวิธีซึ่งชอบด้วยกฎหมาย โดยการนำข้อมูลไปใช้ต้องไม่ขัดกับวัตถุประสงค์และหลักการของกฎบัตรสหประชาชาติ

(2) หลักความถูกต้อง (Principle of accuracy)

หลักการดังกล่าวกำหนดให้บุคคลซึ่งมีหน้าที่ในการรวบรวมข้อมูลหรือบุคคลซึ่งมีหน้าที่ในการเก็บข้อมูลมีหน้าในการตรวจสอบความถูกต้องและความเกี่ยวข้องกับวัตถุประสงค์ของข้อมูลที่ทำการเก็บรวบรวม และต้องทำให้มั่นใจว่าข้อมูลที่ทำการเก็บรวบรวมนั้นสมบูรณ์เพื่อหลีกเลี่ยงความผิดพลาด และต้องทำให้มั่นใจว่าได้ทำข้อมูลนั้นให้เป็นปัจจุบันเสมอๆ หรือตราบเท่าที่ข้อมูลนั้นยังถูกใช้ในการประมวลผล

(3) หลักการกำหนดวัตถุประสงค์ (Principle of the purpose-specification)

หลักการดังกล่าวกำหนดให้ต้อมีการระบุวัตถุประสงค์ในเก็บรวบรวมข้อมูลส่วนบุคคลและระบุการนำข้อมูลส่วนบุคคลตามวัตถุประสงค์นั้นไปใช้ โดยวัตถุประสงค์ดังกล่าวต้องชอบด้วยกฎหมาย และเมื่อได้มีการระบุวัตถุประสงค์ดังกล่าวและระบุการนำข้อมูลส่วนบุคคลไปใช้แล้ว ต้องทำการเผยแพร่หรือแจ้งให้บุคคลซึ่งเกี่ยวข้อทราบ เพื่อก่อให้เกิดความมั่นใจว่า

ก. ข้อมูลส่วนบุคคลทั้งหมดที่ถูกเก็บรวบรวมและบันทึกยังคงเกี่ยวข้องและเหมาะสมสำหรับวัตถุประสงค์ที่ได้กำหนดไว้

ข. ข้อมูลส่วนบุคคลนั้นจะไม่ถูกใช้หรือเปิดเผยเพื่อใช้สำหรับวัตถุประสงค์อื่นซึ่งขัดกันกับวัตถุประสงค์ที่ได้แจ้งไว้ เว้นแต่ได้รับความยินยอมจากบุคคลที่เกี่ยวข้อง

ค. ระยะเวลาในการเก็บรวบรวมข้อมูลส่วนบุคคลต้องไม่เกินกำหนดเวลาเพื่อการทำวัตถุประสงค์ที่ได้แจ้งไว้ให้สำเร็จลุล่วง

(4) หลักการเข้าถึงของผู้มีส่วนได้เสีย (Principle of interested-person access)

หลักการดังกล่าวกำหนดให้บุคคลซึ่งได้แสดงตนว่าเป็นเจ้าของข้อมูลส่วนบุคคลมีสิทธิในการรับทราบว่าข้อมูลส่วนบุคคลของตนได้ถูกประมวลผลหรือไม่ ผู้เก็บรวบรวมข้อมูลส่วนบุคคลต้องแจ้งแก่เจ้าของข้อมูลส่วนบุคคลในรูปแบบที่เจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึงได้โดยไม่ชักช้าหรือมีค่าใช้จ่ายเกินสมควร ในกรณีนี้เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอแก้ไขหรือลบข้อมูลส่วนบุคคลของตน ในกรณีที่ข้อมูลนั้นไม่ถูกต้อง การเก็บรวบรวมไม่ชอบด้วยกฎหมาย หรือเกินความจำเป็น ค่าใช้จ่ายในการแก้ไขข้อมูลนั้นตกแก่ผู้เก็บรวบรวมข้อมูลส่วนบุคคล หลักการเข้าถึงของผู้มีส่วนได้เสียนี้นำมาบังคับใช้แก่ทุกคนโดยไม่คำนึงถึงสัญญาหรือถิ่นที่อยู่

(5) หลักการไม่เลือกปฏิบัติ (Principle of non-discrimination)

หลักการดังกล่ากำหนดห้ามมิให้เก็บรวบรวมข้อมูลซึ่งอาจก่อให้เกิดการเลือกปฏิบัติซึ่งไม่ชอบด้วยกฎหมายหรือปราศจากเหตุผล รวมไปถึงข้อมูลเกี่ยวกับเชื้อชาติ ชาติพันธุ์ แหล่งกำเนิด สีผิว พฤติกรรมทางเพศ ความคิดเห็นทางการเมือง ศาสนา ความเชื่อทางปรัชญาหรือความเชื่ออื่นๆ รวมไปถึงข้อมูลเกี่ยวกับการเป็นสมาชิกของสมาคมหรือสหภาพแรงงาน เว้นแต่ตกอยู่ภายใต้ข้อยกเว้นตามหลักการกำหนดข้อยกเว้น (Power to make exceptions)

(6) หลักการกำหนดข้อยกเว้น (Power to make exceptions)

หลักการดังกล่าวกำหนดให้ข้อยกเว้นหลักการที่ 1 ถึง 4 สามารถกำหนดได้เพียงเฉพาะในกรณีที่ข้อยกเว้นนั้นเป็นการจำเป็นเพื่อรักษาความมั่นคงของประเทศ รักษาความสงบเรียบร้อยของประชาชน รักษาสุขอนามัยของประชาชน รักษาศีลธรรมอันดีของประชาชน รวมไปถึงสิทธิและเสรีภาพของบุคคลอื่น โดยข้อกำหนดดังกล่าวต้องระบุชัดแจ้งถึงข้อยกเว้นและการป้องกันที่เหมาะสม นอกจากนี้ต้องประกาศเป็นกฎหมายหรือกฎเกณฑ์อื่นซึ่งมีค่าเท่าเทียมกับกฎหมาย

อย่างไรก็ตามข้อยกเว้นของหลักการที่ 5 เกี่ยวกับการไม่เลือกปฏิบัติสามารถกำหนดได้ภายใต้ข้อจำกัดซึ่งระบุโดยปฏิญญาสากลว่าด้วยสิทธิมนุษยชนและตราสารอื่นที่เกี่ยวข้องในด้านการคุ้มครองสิทธิมนุษยชนและการป้องกันการเลือกปฏิบัติ

(7) หลักความปลอดภัย (Principle of Security)

หลักการดังกล่าวกำหนดให้ผู้เก็บรวบรวมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการในการป้องกันข้อมูลจากภยันตรายที่เกิดขึ้นโดยธรรมชาติ เช่น ความสูญหายโดยอุบัติเหตุ หรือการทำลาย หรือภยันตรายที่เกิดจากบุคคล เช่น การเข้าถึงโดยไม่ได้รับอนุญาต การนำข้อมูลไปใช้ในทางหลอกลวง หรือการถูกโจมตีจากไวรัสคอมพิวเตอร์

(8) หลักการกำกับดูแล (Supervision and sanction)

หลักการดังกล่าวกำหนดให้กฎหมายของประเทศต่างๆต้องตั้งหน่วยงานซึ่งมีหน้าที่ในการกำกับดูแลสังเกตการณ์เกี่ยวกับหลักการต่างๆที่กล่าวมา ในกรณีที่มีการฝ่าฝืนข้อกำหนดของกฎหมายระหว่างประเทศซึ่งบัญญัติขึ้นเพื่อบังคับใช้หลักการต่างๆที่กล่าวมาจะต้องมีมาตรการทางอาญาหรือมาตรลงโทษอื่นรวมถึงต้องมีการชดเชยที่เหมาะสมแก่เจ้าของข้อมูลส่วนบุคคลด้วย

(9) หลักการโอนข้อมูลข้ามแดน (Transborder data flows)

หลักการดังกล่าวกำหนดให้การโอนข้อมูลข้ามแดนสามารถทำได้อย่างเสรีหากประเทศที่มีการโอนหรือการรับโอนนั้นมีมาตรการในการคุ้มครองความเป็นส่วนตัวที่เท่าเทียมกัน

(10) หลักขอบเขตการบังคับใช้ (Field of application)

หลักการต่างๆที่กล่าวมาต้องถูกนำมาบังคับใช้ต่อข้อมูลทางคอมพิวเตอร์ทั้งที่เป็นสาธารณะและส่วนตัว และข้อมูลที่จัดเก็บด้วยมือ อาจมีการกำหนดบทบัญญัติที่เฉพาะเจาะจงเพื่อขยายขอบเขตของหลักการต่างๆให้คลอบคลุมถึงข้อมูลเกี่ยวกับนิติบุคคล โดยเฉพาะอย่างยิ่งในกรณีที่ข้อมูลเหล่านั้นมีข้อมูลบางส่วนซึ่งเกี่ยวข้องกับบุคคลธรรมดา

2.4.4 กรอบการคุ้มครองข้อมูลส่วนบุคคลของ Asia-Pacific Economic Cooperation (APEC Privacy Framework)

กรอบการคุ้มครองข้อมูลส่วนบุคคลของ Asia-Pacific Economic Cooperation หรือ APEC มีวัตถุประสงค์ในการคุ้มครองความเป็นส่วนตัวเพื่อส่งเสริมความเชื่อมั่นแก่ผู้บริโภคในด้านความปลอดภัยของข้อมูลให้แก่ธุรกิจพาณิชย์อิเล็กทรอนิกส์เพื่อให้ดำเนินไปได้อย่างเต็มศักยภาพและเพื่อส่งเสริมให้การโอนถ่ายข้อมูลระหว่างประเทศใน Asia-Pacific เกิดขึ้นได้อย่างเสรี โดยข้อมูลและเทคโนโลยีในการสื่อสารนั้นรวมไปถึงเทคโนโลยีบนโทรศัพท์เคลื่อนที่ซึ่งสามารถเชื่อมโยงกับอินเตอร์เน็ตได้และสามารถที่จะทำการเก็บรวบรวมข้อมูลส่วนบุคคล รักษาหรือเข้าถึงได้

จากที่ใดๆก็ตามทั่วโลก แม้เทคโนโลยีดังกล่าวนี้มีประโยชน์ทั้งต่อสังคมและเศรษฐกิจ ไม่ว่าจะเป็นภาคธุรกิจ หรือปัจเจกบุคคล อย่างไรก็ตามเทคโนโลยีดังกล่าวเมื่อนำมาใช้แก่การเก็บรวบรวมข้อมูลส่วนบุคคลของปัจเจกบุคคลปัจเจกบุคคลย่อมไม่อาจทราบได้ทำให้ไม่อาจควบคุมข้อมูลส่วนบุคคลของตนเองได้จนก่อให้เกิดความวิตกกังวลว่าจะมีการนำข้อมูลส่วนบุคคลของตนไปใช้โดยมิชอบ ดังนั้นจึงต้องมีการวางแนวปฏิบัติเกี่ยวกับข้อมูลส่วนบุคคลทั้งออนไลน์และออฟไลน์เพื่อเพิ่มความเชื่อมั่นให้แก่ทั้งปัจเจกบุคคลและภาคธุรกิจ หลักเกณฑ์ของกรอบการคุ้มครองข้อมูลส่วนบุคคลของ Asia-Pacific Economic Cooperation (APEC Privacy Framework) มีดังต่อไปนี้

(1) หลักการป้องกันความเสียหาย (Preventing Harm)

หลักการป้องกันความเสียหายคำนึงถึงประโยชน์ของปัจเจกบุคคลในอันที่จะคาดหวังถึงความเป็นส่วนตัวของตนจึงกำหนดให้การคุ้มครองข้อมูลส่วนบุคคลต้องถูกออกแบบให้ป้องกันการนำข้อมูลดังกล่าวไปใช้ในทางที่มิชอบ ต้องมีการกำหนดมาตรการในการป้องกันความเสียหายที่อาจเกิดขึ้นจากการนำข้อมูลส่วนบุคคลไปใช้ในทางที่มิชอบ และมาตรการในการเยียวยาต้องได้สัดส่วนกับโอกาสและความร้ายแรงที่จะเกิดความเสียหายขึ้นในการเก็บรวบรวม ใช้และโอนข้อมูลส่วนบุคคล

(2) หลักการแจ้งเตือน (Notice)

หลักการดังกล่าวกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีรายงานซึ่งชัดแจ้งและสามารถเข้าถึงได้ง่ายเกี่ยวกับแนวปฏิบัติและนโยบายเกี่ยวกับข้อมูลส่วนบุคคล ทั้งนี้ต้องประกอบด้วยข้อมูลดังต่อไปนี้

1. เหตุผลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคล
2. วัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล
3. ข้อมูลส่วนบุคคลนั้นอาจถูกเปิดเผยให้แก่บุคคลหรือองค์กรในลักษณะใด
4. แสดงตัวตนของผู้เก็บรวบรวมข้อมูลส่วนบุคคลและที่อยู่ รวมถึงวิธีในการติดต่อผู้เก็บรวบรวมข้อมูลส่วนบุคคล
5. แสดงถึงวิธีการในการที่เจ้าของข้อมูลส่วนบุคคลสามารถจำกัดการใช้และการเปิดเผยข้อมูลของตน วิธีการในการเข้าถึงและแก้ไขข้อมูลส่วนบุคคลของตน

โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งข้อมูลดังกล่าวก่อนหรือในเวลาที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคล หรือโดยเร็วที่สุดเท่าที่สามารถเป็นไปได้ อย่างไรก็ตามผู้ควบคุมข้อมูลส่วนบุคคลไม่จำเป็นต้องแจ้งถึงการเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลซึ่งได้ถูกเปิดเผยไว้เป็นสาธารณะ

(3) หลักข้อจำกัดการเก็บรวบรวมข้อมูลส่วนบุคคล (Collection Limitation)

หลักการดังกล่าวกำหนดให้การเก็บรวบรวมข้อมูลส่วนบุคคลทำได้เพียงเท่าที่เกี่ยวข้องกับวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคล และข้อมูลนั้นต้องได้รับมาโดยวิธีที่เป็นธรรม ชอบด้วยกฎหมาย และได้แจ้งหรือได้รับความยินยอมจากบุคคลที่เกี่ยวข้อง

(4) หลักการใช้ข้อมูลส่วนบุคคล (Uses of Personal Information)

หลักการดังกล่าวกำหนดให้การใช้ข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมมาสามารถทำได้เพียงเพื่อให้สำเร็จตามวัตถุประสงค์ของการเก็บรวบรวม หรือวัตถุประสงค์อื่นที่สอดคล้องกับวัตถุประสงค์ในการเก็บรวบรวมหรือเป็นวัตถุประสงค์ที่เกี่ยวข้องกัน เว้นแต่

1. ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

2. เป็นกรณีจำเป็นเพื่อการจัดเตรียมการบริการหรือจัดเตรียมสินค้าตามคำขอของเจ้าของข้อมูลส่วนบุคคล

3. เป็นการเปิดเผยต่อหน่วยงานรัฐผู้มีอำนาจหรือตามกฎหมายอื่นหรือเป็นผลในทางกฎหมาย

(5) หลักตัวเลือก (Choice)

หลักการดังกล่าวกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดเตรียมวิธีการที่ชัดแจ้ง เข้าใจง่าย เข้าถึงได้และมีค่าใช้จ่ายไม่เกินสมควรเพื่อให้เจ้าของข้อมูลส่วนบุคคลให้ความยินยอมเกี่ยวกับการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล แต่หากเป็นข้อมูลส่วนบุคคลซึ่งได้ถูกเปิดเผยเป็นสาธารณะผู้ควบคุมข้อมูลส่วนบุคคลไม่จำต้องจัดเตรียมวิธีการดังกล่าว

(6) หลักความสมบูรณ์ของข้อมูลส่วนบุคคล (Integrity of Personal Information)

หลักการดังกล่าวกำหนดให้ข้อมูลส่วนบุคคลต้องถูกต้อง สมบูรณ์และเป็นปัจจุบัน

(7) หลักความปลอดภัย (Security Safeguards)

หลักการดังกล่าวกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องมีมาตรการรักษาความปลอดภัยข้อมูลส่วนบุคคลซึ่งอยู่ในความครอบครองของตนจากภัยทั้งปวง เช่น การสูญหาย การเข้าถึงโดยไม่ได้รับอนุญาต การทำลายหรือการใช้หรือการเปลี่ยนแปลงข้อมูลส่วนบุคคลโดยปราศจากอำนาจ หรือการเปิดเผยข้อมูลส่วนบุคคล หรือการใช้โดยมิชอบประการอื่น มาตรการในการป้องกันดังกล่าวต้องได้สัดส่วนกันกับโอกาสและความร้ายแรงที่อาจเกิดความเสียหาย และมาตรการนี้ควรได้รับการประเมินและการปรับปรุงเสมอๆ

(8) หลักการเข้าถึงและการแก้ไข (Access and Correction)

หลักการดังกล่าวกำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิดังต่อไปนี้

1. ได้รับการยืนยันจากผู้ควบคุมข้อมูลส่วนบุคคลถึงความยืออยู่ในครอบครองซึ่งข้อมูลส่วนบุคคลของตน

2. ภายหลังจากที่ได้ตรวจสอบตัวตนของเจ้าของข้อมูลส่วนบุคคลแล้ว เจ้าของข้อมูลส่วนบุคคลมีสิทธิได้รับแจ้งถึงข้อมูลเกี่ยวกับตน

i. ภายในเวลาอันสมควร

ii อาจมีค่าใช้จ่ายได้แต่ต้องไม่เกินสมควร

iii ในรูปแบบที่เหมาะสม

iv ในรูปแบบซึ่งสามารถเข้าใจได้

3. มีสิทธิในการคัดค้านความถูกต้องของข้อมูลส่วนบุคคลของตน และได้รับการแก้ไข ทำให้ถูกต้อง ทำให้สมบูรณ์ หรือลบในกรณีที่เป็นการเหมาะสมและสามารถกระทำได้

หากคำขอตามข้อ 1 2 และ 3 ถูกปฏิเสธ เจ้าของข้อมูลส่วนบุคคลมีสิทธิอุทธรณ์การปฏิเสธนั้นได้ อย่างไรก็ตามการเข้าถึงและการแก้ไขดังกล่าวจะได้รับการยกเว้นในกรณีดังต่อไปนี้

ก. ภาระหน้าที่หรือค่าใช้จ่ายในการดำเนินการดังกล่าวไม่ได้สัดส่วนกันกับความเสี่ยงต่อความปลอดภัยของข้อมูลส่วนบุคคล

ข. ข้อมูลส่วนบุคคลนั้นถูกเปิดเผยตามบทบัญญัติของกฎหมาย หรือเหตุผลด้านความปลอดภัย หรือเพื่อปกป้องความลับข้อมูลทางการค้า

ค. อาจมีการละเมิดความเป็นส่วนตัวต่อเจ้าของข้อมูลส่วนบุคคลอื่น

(9) หลักความน่าเชื่อถือ (Accountability)

หลักการดังกล่าวกำหนดให้ผู้เก็บรวบรวมข้อมูลส่วนบุคคลต้องปฏิบัติตามหลักการตามข้อ 1 ถึง 8 ที่กล่าวมาข้างต้น หากจะต้องโอนข้อมูลส่วนบุคคลแก่บุคคลหรือองค์กรอื่นไม่ว่าอยู่ในหรือต่างประเทศ ผู้ควบคุมข้อมูลส่วนบุคคลต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล และต้องทำเท่าที่สามารถทำได้เพื่อให้มั่นใจว่าบุคคลหรือองค์กรผู้รับโอนข้อมูลส่วนบุคคลนั้นจะรักษาข้อมูลส่วนบุคคลตามหลักการของกรอบการคุ้มครองข้อมูลส่วนบุคคลของ Asia-Pacific Economic Cooperation (APEC Privacy Framework)

2.5 เทคโนโลยีเกี่ยวกับข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์

ในปัจจุบันนี้เทคโนโลยีต่างๆมีความล้ำหน้าเป็นอย่างมากและมีการนำมาใช้บนโลกอินเตอร์เน็ตโดยมีวัตถุประสงค์แตกต่างกันไป บางองค์กรนำเทคโนโลยีมาใช้เพื่อพัฒนาเว็บไซต์ของตน

เพียงเท่านั้นโดยมิได้มีวัตถุประสงค์อย่างอื่น บางองค์กรนำมาใช้เพื่อวัตถุประสงค์ในทางธุรกิจ หรือแม้กระทั่งบางองค์กรได้นำเทคโนโลยีเหล่านี้มาใช้เพื่อติดตามผู้กระทำความผิดอีกด้วย ซึ่งเทคโนโลยีที่ถูกนำมาใช้บนอินเตอร์เน็ตที่สำคัญในปัจจุบันมีดังต่อไปนี้

2.5.1 ข้อมูลซึ่งไม่สามารถรู้ตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

เมื่อจำแนกข้อมูลส่วนบุคคลตามความสามารถในการบ่งชี้ตัวบุคคลผู้เป็นเจ้าของข้อมูลแล้วสามารถจำแนกออกได้ 3 ประเภท[18] คือ (1) ข้อมูลประเภท Anonymous (2) ข้อมูลส่วนบุคคล (Personal Data) และ (3) ข้อมูลประเภท Pseudonymous โดยข้อมูลส่วนบุคคลเป็นข้อมูลซึ่งเกี่ยวข้องกับบุคคลธรรมดาประกอบด้วยข้อมูลต่างๆที่สามารถบ่งชี้ตัวบุคคลผู้เป็นเจ้าของข้อมูลได้ อาทิ ชื่อ ที่อยู่ เบอร์โทรศัพท์ อีเมล หรือข้อมูลอื่นซึ่งสามารถระบุตัวบุคคลผู้เป็นเจ้าของข้อมูลได้ ข้อมูลส่วนบุคคลดังกล่าวในบางครั้งเมื่อมีการนำมาใช้แล้วอาจก่อให้เกิดปัญหาต่อความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคล รวมถึงในยุคที่เทคโนโลยีมีราคาถูกเจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึงบริการอินเตอร์เน็ตได้อย่างง่ายดายและเจ้าของข้อมูลส่วนบุคคลมักไม่ตระหนักถึงอันตรายที่อาจเกิดจากการที่บุคคลอื่นมีข้อมูลส่วนบุคคลของตน กอปรกับการที่ผู้ประกอบการเองสามารถที่จะเก็บข้อมูลส่วนบุคคลได้มากขึ้นและวิเคราะห์ประมวลผลข้อมูลนั้นเพื่อประโยชน์ของตนได้ง่ายขึ้นจึงทำให้มีโอกาสในการละเมิดความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลได้มาก การนำข้อมูลประเภท Anonymous มาใช้จึงเป็นแก้ไขปัญหาดังกล่าว

ข้อมูลประเภท Anonymous นี้มีขึ้นเนื่องจากคือการเก็บรวบรวม เปิดเผย และการนำมาใช้ซึ่งข้อมูลส่วนบุคคลในหลายๆครั้งอาจกระทบต่อสิทธิในความเป็นส่วนตัวของเจ้าของข้อมูลอีกทั้งการเก็บรักษาข้อมูลส่วนบุคคลไว้เป็นเวลานานอาจก่อให้เกิดการรั่วไหลของข้อมูลไม่ว่าเป็นความจงใจหรือความประมาทเลินเล่อของบุคคลในองค์กรของผู้ควบคุมข้อมูลส่วนบุคคล นอกจากนี้ข้อมูลต่างๆสามารถถูกเก็บรวบรวมและทำการประมวลผลเพื่อเชื่อมโยงไปยังข้อมูลอื่นๆได้ง่ายขึ้นเนื่องจากราคาอุปกรณ์ทางอิเล็กทรอนิกส์นั้นถูกลงและมีความล้ำหน้ามากขึ้น จึงทำให้มีการนำ

---

[18] Thomas Schauf, “The Concept of Pseudonymous Data”,Accedssed15 January 2016, https://www.google.co.th/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0ahUKEwj7vrqfw8zKAhUEG44KHbEFAe0QFggyMAI&url=http%3A%2F%2Fwww.w3.org%2F2011%2Ftracking-protection%2Fmit%2Fbvdw_w3c_pseud-data_20130211.pptx.pdf&usg=AFQjCNHl0lMGNlZFd6BXou1Tj4C3imX5Ow

ข้อมูล Anonymous มาใช้เพื่อแก้ไขปัญหาในเรื่องความเป็นส่วนตัวและการรั่วไหลของข้อมูลส่วนบุคคล โดยข้อมูล Anonymous เป็นข้อมูลซึ่งไม่สามารถรู้ตัวบุคคลผู้เป็นเจ้าของข้อมูลได้ โดยการตัดออกหรือเปลี่ยนแปลงข้อมูลต่างๆเกี่ยวกับเจ้าของข้อมูลส่วนบุคคลหรือข้อมูลที่มีลักษณะพิเศษจนอาจทำให้สามารถระบุตัวบุคคลผู้เป็นเจ้าของข้อมูลส่วนบุคคลนั้นได้ อาทิ ชื่อ ที่อยู่ โรคประจำตัวหรือลักษณะทางกายภาพ เป็นต้นโดยมีวัตถุประสงค์เพื่อมิให้สามารถระบุตัวเจ้าของข้อมูลส่วนบุคคลจากข้อมูลนั้นเองหรือการนำข้อมูลนั้นประกอบกับข้อมูลอื่นซึ่งผู้ควบคุมข้อมูลส่วนบุคคลมีอยู่หรือเข้าถึงได้หรืออาจเข้าถึงได้ วิธีการที่นิยมใช้ในการนำข้อมูลส่วนบุคคลมาแปลงเป็นข้อมูล Anonymous มี 2 วิธี กล่าวคือ

(1) k-Anonymity วิธีการดังกล่าวถูกนำเสนอโดย Samarati และ Sweeney ในปี ค.ศ. 1998 เพื่อแก้ไขปัญหาในเรื่องของการเปิดเผยข้อมูลส่วนบุคคลโดยเฉพาะอย่างยิ่งข้อมูลทางการแพทย์ซึ่งเป็นข้อมูลที่มีความอ่อนไหว ด้วยเหตุนี้จึงมีการคิดค้นวิธีทางคณิตศาสตร์เพื่อทำให้ไม่สามารถเชื่อมโยงข้อมูลนั้นไปยังเจ้าของข้อมูลส่วนบุคคลได้ ในการแทนข้อมูลส่วนบุคคลโดยวิธีการ k-Anonymity นี้มีการแทนค่าข้อมูลโดยวิธีการ Suppression โดยการนำข้อมูลมาแทนค่าเป็นเครื่องหมาย * เช่น การแทนชื่อเจ้าของข้อมูลส่วนบุคคลด้วยเครื่องหมาย * หรือใช้วิธี Generalization ด้วยการแทนค่าข้อมูลโดยข้อมูลที่มีขนาดกว้างมากขึ้น เช่น เจ้าของข้อมูลอายุ 19 ปี อาจมีการแทนค่าด้วย ≤20 หรือ 15 <Age ≤ 25 เป็นต้น

<u>ตัวอย่าง</u>ข้อมูล Anonymous โดยวิธี k-anonymity

ตารางที่ 2.1

<u>Raw Medical Data Set</u>

	Non-Sensitive			Sensitive
	Zip code	**Age**	**Nationality**	**Condition**
1	13053	28	Russian	Heart Disease
2	130568	29	American	Heart Disease
3	13068	21	Japanese	Viral Infection
4	13053	23	American	Viral Infection
5	14853	50	Indian	Cancer
6	14853	55	Russian	Heart Disease

7	14850	47	American	Viral Infection
8	14850	49	American	Viral Infection
9	13053	31	American	Cancer
10	13053	37	Indian	Cancer
11	13068	36	Japanese	Cancer
12	13068	35	American	Cancer

Anonymous Data Set

	Non-Sensitive			**Sensitive**
	Zip code	**Age**	**Nationality**	**Condition**
1	130**	<30	*	Heart Disease
2	130**	<30	*	Heart Disease
3	130**	<30	*	Viral Infection
4	130**	<30	*	Viral Infection
5	1485*	≥40	*	Cancer
6	1485*	≥40	*	Heart Disease
7	1485*	≥40	*	Viral Infection
8	1485*	≥40	*	Viral Infection
9	130**	3*	*	Cancer
10	130**	3*	*	Cancer
11	130**	3*	*	Cancer
12	130**	3*	*	Cancer

หมายเหตุ จาก Machanavajjhala, A., Kifer, D., Gehrke, J., Venkitasubramaniam, M., l-Diversity: Privacy Beyond K-Anonymity, ACM Transactions on Knowledge Discovery from Data (TKDD) Volume 1 Issue 1, March 2007 Article No. 3 Accedssed 17January 2016.

(2) l-Diversity วิธีดังกล่าเกิดขึ้นเนื่องจากวิธี k-anonymity มีข้อบกพร่องใน2กรณี[19] กล่าวคือ กรณีข้อมูลส่วนบุคคลมีความเหมือนกัน กล่าวคือ ตามตารางที่แสดงไว้ด้านบน หาก A ต้องการทราบข้อมูลของ B โดยทราบว่า B มีอายุประมาณ 31 ปี และเป็นบุคคลที่มีข้อมูลแสดงไว้ในตารางดังกล่าว A จะสามารถทราบได้ทันทีว่า B เป็นมะเร็ง และกรณีที่บุคคลซึ่งประสงค์เชื่อมโยงข้อมูลไปยังเจ้าของข้อมูลส่วนบุคคลทราบประวัติข้อมูลบางอย่างเกี่ยวกับเจ้าของข้อมูลส่วนบุคคล กล่าคือ หาก A ทราบว่า B เป็นบุคคลซึ่งถูกแสดงข้อมูลในตาราง มีอายุ 21 ปี และไม่มีโรคหัวใจ A จะทราบข้อมูลได้ทันทีว่า B เป็นผู้ติดเชื้อไวรัส จึงมีการสร้าง l-Diversityขึ้นโดยให้เป็นฟังชั่นที่ปกปิดเจ้าของข้อมูลส่วนบุคคลและแก้ไขข้อบกพร่องของวิธี k-anonymity

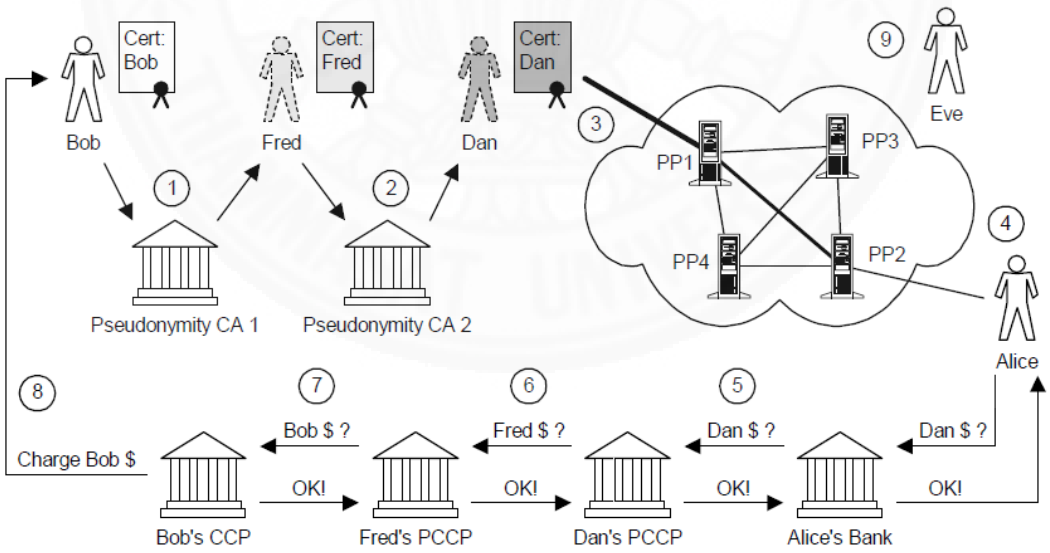
ข้อมูลประเภท Pseudonymous เป็นข้อมูลที่อยู่กึ่งกลางระหว่างข้อมูลส่วนบุคคลและข้อมูลประเภท Anonymous โดยข้อมูล Pseudonymous มีความคล้ายคลึงกับข้อมูลประเภท Anonymous กล่าวคือ เป็นข้อมูลซึ่งไม่สามารถรู้ตัวบุคคลผู้เป็นเจ้าของข้อมูลส่วนบุคคลได้ เว้นแต่ผู้ที่ทราบถึงวิธีการเข้ารหัสข้อมูลนั้น ความแตกต่างระหว่างข้อมูลทั้งสองประเภท คือ ข้อมูลประเภท Pseudonymous ยังคงไว้ซึ่งข้อมูลบางประการทำให้สามารถที่เข้ารหัสเพื่อจะสืบกลับไปยังเจ้าของข้อมูลส่วนบุคคลได้ วิธีการดังกล่าวนับเป็นวิธีการที่สำคัญในทางการแพทย์เพื่อที่จะรักษาความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลโดยป้องกันมิให้ตัวเจ้าของข้อมูลส่วนบุคคลนั้นถูกเปิดเผย ในปัจจุบันข้อมูล Pseudonymous ได้ถูกนำมาใช้อย่างกว้างขวางทั้งในด้านการวิจัยทางแพทย์ การประเมินผลทางสุขภาพ หรือในทางการตลาด การแปลงข้อมูลให้เป็นประเภทนี้ คือการแทนค่าข้อมูลส่วนบุคคล เช่น ชื่อ ที่อยู่ อีเมล หรือเบอร์โทรศัพท์ ด้วยข้อมูลอื่นหรือด้วยข้อมูลซึ่งถูกสมมติขึ้นมา (Pseudo-ID) เช่น A อายุ 30 ปี สามารถแปลงได้เป็น Z อายุ 30 ปี หรือ 1234 อายุ 30 ปี เป็นต้น โดยวิธีการ Pseudonymous นี้สามารถที่จะแทนที่ข้อมูลส่วนบุคคลของบุคคลคนเดียวกันโดย Pseudo-ID เดียวกันได้

---

[19]Machanavajjhala, A., Kifer, D., Gehrke, J., Venkitasubramaniam, M., “l-Diversity: Privacy Beyond K-Anonymity, ACM Transactions on Knowledge Discovery from Data”, Accedssed17 January 2016, https://www.google.co.th/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwiaw9PJsuXLAhVOWI4KHQGdAmoQFggmMAE&url=https%3A%2F%2Fwww.truststc.org%2Fpubs%2F465%2FL%2520Diversity%2520Privacy.pdf&usg=AFQjCNHdEQaN68mCp2zbWJk_lA8sbJnvKQ&sig2=Wf1miHJqXCKbbRJRa6wsFw&bvm=bv.117868183,d.c2E

ในปัจจุบันได้มีการให้บริการโครงข่าย Pseudonymity เพื่อนำมาใช้ในธุรกรรมการชำระเงินโดยประกอบด้วย 3 ส่วนที่สำคัญ คือ โครงข่าย Pseudonymity (Pseudonymous Network) หน่วยงานซึ่งรับผิดชอบในการออก Pseudonym (Pseudonymous Certificate Authority หรือ PCA) และธุรกรรมที่เป็น Pseudonymous โดยเมื่อผู้ซื้อได้ทำการร้องขอ Pseudo-ID จากหน่วยงานซึ่งรับผิดชอบในการออก Pseudonym แล้วโครงข่าย Pseudonymous นี้จะทำการปกปิดตัวผู้ซื้อจากร้านค้าทั้งในระหว่างการเลือกซื้อสินค้าและการชำระเงิน เมื่อมีการชำระเงินระบบจะส่ง Pseudo-ID ไปยังร้านค้าปลายทางและร้านค้าจะส่งข้อมูลดังกล่าวต่อไปยังธนาคาร ธนาคารจะส่งข้อมูลที่ได้รับต่อไปยังผู้ให้บริการบัตรเครดิตแบบ Pseudonymous (Pseudonymity Credit Card Provider หรือ PCCP) เพื่อทำการยืนยันการชำระเงินผ่านบัตรเครดิตดังกล่าวและส่งข้อมูลกลับไปยังธนาคาร และธนาคารส่งข้อมูลดังกล่าวต่อไปยังร้านค้า ภายใต้วิธีการชำระเงินดังกล่าวนี้ร้านค้าจะไม่สามารถทราบถึงผู้ซื้อที่แท้จริงได้ การทำงานของโครงข่าย Pseudonymous สามารถแสดงได้ตามรูปภาพดังกล่าว

<u>ตัวอย่าง</u> รูปภาพแสดงการทำงานของโครงข่าย Pseudonymous



ภาพที่ 2.1 จาก Rafarli, S., Rennhard, M., Mathy, L.,"An Architecture for Pseudomymous e-Commerce, AISB'01 Symposium on Information Agents for Electronic Commerce", Accedssed2 Feubuary 2016, https: / / ww w.google.co.th/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=0ahUKEwjSorPM2tnKAhWOG44 KHW3 D7 8 QFggjMAA&url= https% 3 A% 2 F% 2 Forbi. ulg. ac. be% 2 Fbitstream% 2 F2 2 6 8 % 2 F1 6 8 0 1 9 % 2F1%2FAISB2001.pdf&usg=AFQjCNFfUL2kurCESVPMiiimVhBSWz4VfA

วัตถุประสงค์ของการแปลงข้อมูลให้เป็นข้อมูลประเภท Pseudonymous คือ เพื่อไม่ให้สามารถเชื่อมโยงข้อมูลส่วนบุคคลที่ถูกแปลงไปยังเจ้าของข้อมูลส่วนบุคคลได้และยังมีประโยชน์ต่อผู้ต้องการใช้ข้อมูลในแง่ของการได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เนื่องจากเมื่อมีการแปลงข้อมูลให้เป็นข้อมูล Pseudonymous แล้ว เจ้าของข้อมูลส่วนใหญ่พิจารณาว่าข้อมูลที่ถูกแปลงนี้จะไม่สามารถเชื่อมโยงมายังตนได้และยินยอมให้นำข้อมูลนั้นๆไปใช้ต่อไป

การนำข้อมูล Anonymous และ Pseudonymous มาใช้นั้นมีวัตถุประสงค์เดียวกันคือการปกปิดตัวบุคคลผู้เป็นเจ้าของข้อมูลส่วนบุคคล โดยมีความแตกต่างกันในเรื่องของความสามารถในการสืบค้นกลับไปยังตัวเจ้าของข้อมูลส่วนบุคคล กล่าวคือ ข้อมูลประเภท Anonymous จะมีการใช้ขั้นตอนหรือวิธีการที่ทำให้ไม่สามารถสืบค้นข้อมูลกลับไปยังตัวเจ้าของข้อมูลส่วนบุคคลหรือทำให้เป็นไปไปได้น้อยที่สุด แต่ข้อมูล Pseudonymous นี้ยังคงไว้ซึ่งข้อเท็จจริงหรือข้อมูลบางประการที่เปิดโอกาสให้สามารถสืบกลับไปยังเจ้าของข้อมูลส่วนบุคคลได้ ข้อมูลทั้ง Anonymous และ Pseudonymous นิยมนำมาใช้ในการทำวิจัยทั้งในทางการแพทย์และทางการตลาด และเริ่มมีการนำมาใช้กับเทคโนโลยีอินเตอร์เน็ตในปัจจุบันเพื่อปกปิดตัวผู้ใช้งานจากบุคคลต่างๆโดยเฉพาะอย่างยิ่งจากการทำการเก็บรวบรวมข้อมูลของผู้ใช้และทำการประมวลผลข้อมูลนั้นเพื่อให้ได้ผลลัพธ์บางประการอันเป็นประโยชน์ต่อผู้เก็บรวบรวมข้อมูลนั้น

2.5.2 Profiling

Profile คือ การจัดทำทะเบียนประวัติของบุคคลแต่ละบุคคลโดยการรวบรวมประวัติ หรือข้อมูลเกี่ยวกับการทำงาน ข้อมูลสุขภาพ หรือข้อมูลประเภทอื่นไว้ เดิมในการทำทะเบียนประวัตินี้ผู้ทำมักได้รับข้อมูลจากเจ้าของข้อมูลส่วนบุคคลโดยตรง หรือหากมีการติดตามเจ้าของข้อมูลส่วนบุคคล เช่น การทำวิจัยในทางการแพทย์ หรือการติดตามพฤติกรรมของผู้บริโภค ผู้ติดตามต้องมีการแจ้งและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเสียก่อน

อย่างไรก็ตามในปัจจุบันนี้ความก้าวหน้าของเทคโนโลยีได้เปิดโอกาสให้แก่ผู้ติดตามสามารถทำการ Profiling ผู้ใช้งานบนอินเตอร์เน็ตได้ง่ายมากขึ้น การ Profiling หรือเรียกอีกอย่างหนึ่งว่า Behavioural Tracking คือการติดตามพฤติกรรมของบุคคลใดบุคคลหนึ่งผ่านทางอินเตอร์เน็ตโดยที่ผู้ถูกติดตามไม่รู้ตัวและสร้างเป็นทะเบียนประวัติของบุคคลนั้น เมื่อได้ข้อมูลต่างๆมาแล้วผู้ติดตามจะนำข้อมูลเหล่านั้นมาวิเคราะห์ประมวลผลโดยระบบอัตโนมัติให้เกิดผลลัพธ์ตามที่ตนเองต้องการและอาจมีการนำไปเปรียบเทียบกับข้อมูลของบุคคลอื่นๆได้ ในปัจจุบันการทำ Profiling นี้ถูกนำมาใช้มากในด้านโฆษณาบนอินเตอร์เน็ตเพื่อใช้ในการจัดกลุ่มผู้ใช้งานตามความสนใจของผู้ใช้ ลักษณะการทำ Profiling ในด้านโฆษณา คือเมื่อผู้ใช้มีการค้นหาข้อมูลหรือสินค้าบาง

ประการไม่ว่าผู้ใช้จะซื้อสินค้านั้นหรือไม่ก็ตามการค้นหานี้จะถูกเก็บรวบรวมโดยเครื่องมือที่ถูกติดตั้งไว้บนคอมพิวเตอร์ของผู้ใช้โดยผู้ใช้ไม่รู้ตัว และนำมาใส่ไว้ในรายการสินค้าหรือบริการซึ่งอยู่ในความสนใจของผู้ใช้ ต่อมาโฆษณาต่างๆที่ถูกแสดงบนเว็บไซต์รวมถึงบนโซเชียลมีเดียที่ผู้ใช้เข้าชมจะแสดงสินค้าหรือบริการซึ่งเกี่ยวข้องกับรายการที่อยู่ในความสนใจของผู้ใช้โดยอาจมีการแสดงการลดราคาเพื่อจูงใจให้ผู้ใช้ซื้อสินค้าหรือบริการนั้นหรือในทางตรงกันข้ามอาจมีการเพิ่มราคาขึ้นเพื่อแสดงให้ผู้ใช้เห็นว่าสินค้าหรือบริการนั้นมีจำนวนจำกัดและรีบทำการซื้อสินค้าหรือบริการนั้น ทั้งนี้ความสนใจในสินค้าหรือบริการของผู้ใช้และนโยบายของของเว็บไซต์ซึ่งทำการติดตามผู้ใช้มีส่วนสำคัญในการเพิ่มขึ้นหรือลดลงของราคาสินค้าหรือบริการ

เครื่องมือที่ใช้ในการทำ Profiling นั้นส่วนใหญ่มักเป็นการติดตามผู้ใช้ผ่านทางเว็บไซต์ เช่น การติดตามผู้ใช้ในการเข้าชมเว็บไซต์แต่ละครั้ง หรือการติดตามการเยี่ยมชมเว็บไซต์อื่นๆของผู้ใช้ ซึ่งในการเก็บรวบรวมข้อมูลนั้นผู้ติดตามจะทำการเก็บทั้งเว็บไซต์ที่ผู้ใช้เข้าชม ระยะเวลาในการเข้าชม และความสม่ำเสมอในการเข้าชม การทำ Profiling นั้นมีองค์ประกอบสำคัญ คือ IP Address ของแต่ละเครื่องเพื่อจดจำผู้ใช้ และ เครื่องมือเพื่อเก็บรวบรวมข้อมูลการใช้งาน เช่น Cookies นอกจากนี้องค์ประกอบที่เริ่มมีความสำคัญอย่างเห็นได้เด่นชัดมากขึ้นในการทำ Profiling คือ การบอกตำแหน่ง (Location) และการใช้งานสมาร์ทโฟน เนื่องจากสมาร์ทโฟนมีเซ็นเซอร์ที่ก้าวหน้ามากขึ้นทำให้สามารถทราบพฤติกรรมการใช้งานของผู้ใช้ได้มากขึ้น สำหรับเครื่องมือที่มักนำมาใช้ในการทำ Profiling ได้แก่[20]

(1) คุกกี้ (Cookies)

คุกกี้ หรือ HTTP Cookies เป็นข้อมูลตัวอักษร (text) ขนาดเล็กที่ถูกเก็บไว้ในคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์อื่นๆที่สามารถเชื่อมต่ออินเตอร์เน็ตได้ คุกกี้จะทำการฝังตัวไว้ในส่วนของคำสั่ง HTML โดยมีการรับและส่งจากคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ของผู้ใช้และเว็บเซิฟเวอร์ (Web Server) ซึ่งคุกกี้อนุญาตให้ผู้ใช้กำหนดข้อมูลบางประการเองได้ เช่น การเก็บค่าข้อมูลสินค้า เป็นต้น การทำงานของคุกกี้เกิดขึ้นเมื่อผู้ใช้ได้ทำการเข้าเยี่ยมชมเว็บไซต์และรับ

---

[20] ENISA, “Privacy Considerations of Online Behavioural Tracking”,Accedssed17 January 2016, www.enisa.europa.eu%2Factivities%2Fidentity-andtrust%2Flibrary%2Fdel iverables%2Fprivacy-considerations-of-online-behavioural-tracking&ei=XDl vVZKQOZHguQT3xoDgAQ&usg=AFQjCNF-7Jw2i8Kcf_hiGFkZr0OTdm2vzg&s ig2=jjtbDWM_l-JPlK9eJUw0dA&bvm=bv.94911696,d.c2E

คุกกี้มาคุกกี้จะทำการฝังตัวในบราวเซอร์และทำการจดจำการใช้งานของผู้ใช้ เมื่อผู้ใช้ออกจากเว็บไซต์นั้นไปและกลับเข้ามาใหม่อีกครั้งหนึ่งบราวเซอร์จะทำการประมวลผลคุกกี้เพื่อตรวจสอบผู้ใช้เคยเข้าไปในเว็บไซต์ที่มีการเก็บข้อมูลในคุกกี้หรือไม่ เมื่อตรวจพบว่าเป็นเว็บไซต์ที่ผู้ใช้เคยเข้าไปใช้งานแล้ว บราวเซอร์จะทำการปรับปรุง Header ของ HTTP ให้มีข้อมูลคุกกี้แนบไปกับ Header Request เพื่อเซอเวอร์ (Web Server) จะสามารถจดจำได้ว่าผู้ใช้เป็นใคร

คุกกี้สามารถแบ่งออกได้เป็น คุกกี้แบบชั่วคราว (Session Cookies) และคุกกี้แบบถาวร (Persistent Cookies) โดยคุกกี้แบบชั่วคราวนั้นมักใช้ในการเก็บข้อมูลที่เป็นตัวเลือก เช่น สินค้าที่ผู้ใช้เลือกไว้ในตะกร้า เป็นต้น หรือใช้เพื่อการเชื่อมโยงไปยังที่อื่นๆ คุกกี้แบบชั่วคราวนี้จะถูกตั้งค่าจากผู้ให้บริการเมื่อผู้ใช้เข้าใช้งานและจะถูกลบออกเมื่อผู้ใช้ออกจากระบบ สำหรับคุกกี้แบบถาวร (Persistent Cookies) มักถูกนำมาใช้งานเพื่อการเก็บข้อมูลเกี่ยวกับตัวผู้ใช้ เช่น ความชอบหรือเพื่อยืนยันตัวผู้ใช้งาน คุกกี้ประเภทนี้จะยังคงฝังตัวอยู่ในคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ของผู้ใช้จนกว่าจะถูกลบหรือหมดอายุ คุกกี้ประเภทนี้นอกจากจะส่งข้อมูลของผู้ใช้งานเว็บไซต์นั้นๆ แล้วยังสามารถทำการติดตามผู้ใช้เมื่อผู้ใช้เข้าเยี่ยมชมเว็บไซต์อื่นๆได้อีกด้วย

โดยปกติแล้ว Cookies จะสามารถอ่านโดยเว็บไซต์ซึ่งเป็นคนสร้างคุกกี้นั้นขึ้นหรือโดยเซอร์เวอร์ที่มีโดเมนเดียวกันเท่านั้นซึ่งเรียกว่า First Party Cookies อย่างไรก็ตามมีคุกกี้ซึ่งมีชื่อเรียกว่า Third Party Cookies เป็นคุกกี้ที่สามารถเก็บไว้บนเซอร์เวอร์ของโดเมนอื่นซึ่งมิได้เป็นคนสร้างคุกกี้นั้นได้ คุกกี้ประเภทนี้นิยมนำมาใช้มากโดยเฉพาะในบริษัทโฆษณาเพื่อติดตามผู้ใช้งานผ่านเว็บไซต์อื่นๆ กล่าวคือบริษัทโฆษณาสามารถที่จะติดตามผู้ใช้ได้จากเว็บไซต์ที่มีการติดตั้งโฆษณาไว้ ซึ่งการติดตามนี้มีประโยชน์ต่อบริษัทโฆษณาในแง่ของการทราบเว็บไซต์ที่ผู้ใช้เข้าเยี่ยมชมเพื่อทำการวิเคราะห์ความชอบและทำการโฆษณาสินค้าหรือบริการให้ตรงตามความชอบของผู้ใช้

(2) JavaScript

Javascript คือภาษาคอมพิวเตอร์เพื่อการเขียนโปรแกรม ใช้ในการสร้างและพัฒนาเว็บไซต์โดยใช้ร่วมกันกับ HTML (Hypertext Markup Language) เพื่อทำให้เว็บไซต์สามารถตอบโต้กับผู้ใช้งานได้ Javascript ถูกนำไปใช้บนเว็บไซต์ต่างๆเช่น Facebook และ Twitter นำ Javascript มาใช้ในการอัพเดทเหตุการณ์ต่างๆ Javascript สามารถใช้ในการดูข้อมูลหรือการขโมยข้อมูลส่วนบุคคล นอกจากนี้ยังมีกระจายอยู่ทั่วไปสามารถใช้ได้บนเว็บไซต์ต่างๆนอกจากเว็บไซต์ของผู้สร้าง เมื่อผู้ใช้ได้รับ Javascript จากการเยี่ยมชมเว็บไซต์แล้ว Javascript จะทำการกระตุ้นคุกกี้และส่งข้อมูลไปยังเซิฟเวอร์ แม้Javascript มีข้อจำกัดในการเข้าถึงข้อมูลส่วนบุคคล แต่อย่างไรก็ตาม Javscript ยังสามารถเข้าถึงข้อมูลที่ถูกเก็บไว้บนเว็บไซต์ รวมถึง Cache และประวัติของการเข้าชมเว็บไซต์

Javascript เมื่อถูกติดตั้งแล้วยังสามารถติดตามการใช้งานของผู้ใช้ได้โดย งานวิจัย[21]ซึ่งศึกษาข้อมูลตัวอย่างจากการใช้ Facebook ของผู้ใช้จำนวนห้าล้านคนในประเทศสหรัฐอเมริกาและอังกฤษ มุ่งศึกษาถึงความถี่ที่บุคคลเขียนข้อความในกล่องข้อความบน Facebook และจบลงด้วยการลบข้อความทิ้งก่อนที่จะมีการโพสข้อความนั้นบน Facebook ผู้ศึกษาวิจัยได้ทำงานวิจัยนี้โดยติดตั้ง Javascript ในกล่องโพสข้อความของ Facebook เพื่อติดตามผู้ใช้ การศึกษานี้ทำให้เห็นได้ชัดว่า Javascript สามารถนำมาใช้เพื่อติดตามผู้ใช้งานได้ นอกจากนี้ Javascript ยังสามารถติดตามผู้ใช้ผ่านปุ่มต่างๆที่แสดงบนเว็บไซต์หรือโซเชียลเน็ตเวิร์ค[22] เช่นปุ่มถูกใจ (Like) บน Facebook ได้อีกด้วยซึ่งการติดตามจะกระทำเมื่อผู้ใช้มีการดาวน์โหลดเว็บไซต์โดยไม่ว่าผู้ใช้จะได้คลิกปุ่มนั้นหรือไม่ก็ตาม

(3) Flash Cookies

Flash Cookies เป็นคุกกี้ประเภท Supercookies ถูกพัฒนาขึ้นเนื่องจากการใช้คุกกี้ที่มีความแพร่หลายมากขึ้นทำให้ผู้ใช้จำนวนมากสามารถหลบเลี่ยงการติดตามจากคุกกี้เหล่านี้ได้ทำให้จำเป็นต้องมีการพัฒนาคุกกี้เพื่อการติดตามการใช้งานของผู้ใช้บนอินเตอร์เน็ตเพื่อให้มีประสิทธิภาพมากขึ้น Flash Cookies ถูกสร้างขึ้นโดยปลั๊กอินของ Adobe Flash ซึ่งเป็นส่วนหนึ่งของแอพพลิเคชั่น Flash ที่ติดตั้งในเว็บเพจ Flash Cookies ไม่ได้ถูกเก็บไว้ในบราวเซอร์เหมือนคุกกี้

---

[21]Lee, J.,“3 Ways JavaScript Can Breach Your Privacy&Security”,Accedssed17 January 2016,https://www.google.co.th/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwi-uqL8vt7KAhXOv44KHYLdDSIQFggdMAA&url=http%3A%2F%2Fwww.makeuseof.com%2Ftag%2F3-ways-javascript-can-used-breach-privacy-security%2F&usg=AFQjCNFn_PZA3NV4m5reg8sRXJyBMJ9K1A&bvm=bv.113370389,d.c2E

[22] Lee, J. “4 Seemingly Innocent Online Activities That Track Your Behavior”,Accedssed17 January 2016, https://www.google.co.th/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjtksHpvt7KAhUBjo4KHeYVDsYQFggbMAA&url=http%3A%2F%2Fwww.makeuseof.com%2Ftag%2F4-seemingly-innocent-online-activities-track-behavior%2F&usg=AFQjCNF72TlumPkMvSjr1MfTWOgLd2hZXw

ประเภทอื่นจึงทำให้บราวเซอร์ไม่สามารถที่จะเรียกดู จัดการหรือลบ Flash Cookies ได้และคุกกี้ประเภทนี้ไม่มีหมดอายุ นอกจากนี้ผู้ใช้เองก็ไม่สามารถรับรู้ได้ถึงการติดตั้ง Flash Cookies บนคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ของตน

การทำงานของ Flash Cookies สามารถติดตามผู้ใช้ได้เช่นเดียวกันกับคุกกี้แบบ HTTP (HTTP Cookies) และจะถูกเรียกขึ้นมาเมื่อผู้ใช้เข้าใช้งานเว็บไซต์ที่มีการติดตั้งโปรแกรม Flash ไว้ ประโยชน์ของ Flash Cookies ดังกล่าวทำให้หลายๆเว็บไซต์นำมาใช้งานเพื่อหลบหลีกการตั้งค่าความเป็นส่วนตัวและการจำกัดการใช้คุกกี้บนบราวเซอร์ของผู้ใช้ เช่น เมื่อเว็บไซต์ได้มีการนำคุกกี้แบบ HTTP มาใช้ประกอบกับ Flash Cookies หากผู้ใช้งานการลบคุกกี้แบบ HTTP หรือคุกกกี้แบบ HTTP หมดอายุ แต่มีการกลับไปใช้งานเว็บไซต์นั้นอีกครั้ง Flash Cookies จะทำการติดตั้งคุกกี้แบบ HTTPเนื่องจากผู้ใช้ไม่สามารถลบ Flash Cookies ออกได้และ Flash Cookies ก็ไม่มีวันหมดอายุ

(4) EverCookies

EverCookies เป็นคุกกี้ที่ถูกสร้างขึ้นโดยการใช้ภาษา JavaScript เป็นคุกกี้ถาวรแบบหนึ่งซึ่งถูกลบได้ยาก คุกกี้ประเภทนี้ถูกพัฒนาขึ้นโดยสามารถทำการติดตามผู้ใช้ได้อย่างดีเยี่ยม EverCookies นี้จะทำการเชื่อมโยงและกระตุ้นคุกกี้ประเภทอื่นๆให้กลับมาใช้งานได้อีกครั้งและยังสามารถที่จะระบุตัวผู้ใช้แม้เมื่อผู้ใช้ลบคุกกี้แบบ HTTP และ Flash Cookies

(5) Stateless Tracking (Browser Fingerprinting)

บราวเซอร์สามารถที่จะทำการระบุตัวได้อย่างแม่นยำโดยไม่จำเป็นต้องมีคุกกี้หรือเทคโนโลยีในการติดตามอื่นๆ เว็บบราวเซอร์สามารถให้ข้อมูลต่างๆแก่เว็บไซต์ได้อย่างมากมาย เช่น ข้อมูลเกี่ยวกับ User Agent[23] รูปแบบตัวอักษร หรือความละเอียดของหน้าจอ เป็นต้น ซึ่งแม้ข้อมูลดังกล่าวจะไม่สามารถที่จะระบุตัวได้เพียงลำพังแต่หากนำมาประกอบกันก็จะทำให้สามารถระบุตัวได้ Browser Fingerprinting นี้เอกลักษณ์เพียงพอที่จะระบุบราวเซอร์หนึ่งแยกออกจากบราวเซอร์อื่นๆได้ เมื่อนำ Browser Fingerprinting มาใช้ประกอบกับข้อมูล IP Address คุกกี้ และ Supercookies แล้วจะทำให้เป็นเครื่องมือที่สามารถติดตามผู้ใช้ได้อย่างดีเยี่ยม

(6) Location Tracking

---

[23] User Agent คือ software ที่ทำงานแทนผู้ใช้โดยมีหน้าที่ในการส่งและรับ Session Initialtion Protocol (SIP) ซึ่งเป็นโปรโตคอลที่ใช้งานในด้านมีเดีย ข้อมูลจาก What’s a Browser User Agent,Accedssed4 February 2016, http://www.howtogeek.com/114937/htg-explains-whats-a-browser-user-agent/

เนื่องจากในปัจจุบันมีเทคโนโลยีในการระบุพิกัดที่แพร่หลาย มีราคาถูก ใช้งานได้ง่าย สามารถติดตามผู้ใช้และเก็บรวบรวมข้อมูลนั้นได้ โดยเว็บบราวเซอร์เองก็ได้รองรับเทคโนโลยีดังกล่าว เช่น Firefox Opera และ Google Chrome เป็นต้น นอกจากนี้เทคโนโลยีดังกล่าวยังได้ถูกติดตั้งบนสมาร์ทโฟนอีกด้วย เทคโนโลยี Location Tracking สามารถนำมาใช้เพื่อการติดตามได้ โดยเมื่อผู้ใช้อนุญาตให้เว็บไซต์ทำการใช้งานเครื่องมือเพื่อระบุตำแหน่งของผู้ใช้แล้ว เว็บไซต์จะมีการส่งข้อมูล IP Address Mac Address ของอุปกรณ์ที่ใช้เชื่อมต่อ และเครือข่าย GSM หรือ CDMA ทำให้การระบุพิกัดดังกล่าวมีความแม่นยำมาก การเปิดเผยพิกัดที่อยู่ของบุคคลนี้อาจทำให้พิกัดนั้นถูกจดจำไว้และทำให้บุคคลนั้นสูญเสียความเป็นส่วนตัวในการเคลื่อนไหวโดยอิสระ[24]

เทคโนโลยี Profiling รวมกับเทคโนโลยีที่ก้าวหน้าในปัจจุบันนี้ทำให้สามารถติดตามบุคคลซึ่งสามารถเข้าถึงอินเตอร์เน็ตได้ไม่ว่าอยู่ ณ แห่งหนใด วัตถุประสงค์การทำ Profiling นั้นแตกต่างกันไปตั้งแต่เพื่อการนำเสนอสินค้าหรือบริการ กระทั่งถึงเพื่อการปกป้องสาธารณประโยชน์ การทำ Profiling ในบางครั้งได้ถูกนำมาใช้เพื่อให้ทราบข้อมูลต่างๆของเจ้าของข้อมูล[25] เช่น ความคิดเห็นทางการเมือง ความสัมพันธ์หรือความเชื่อมโยงของแต่ละบุคคล ความเชื่อทางศาสนา หรือลักษณะการใช้ชีวิตส่วนตัว เป็นต้น ในบางครั้งนายจ้างยังนำการทำ Profiling มาใช้เพื่อทราบถึงลักษณะการทำงาน ความขยันหมั่นเพียร หรือความเอาใจใส่ในงานของลูกจ้างได้อีกด้วย นอกจากนี้การทำ Profiling สามารถทำให้ทราบถึงตัวบุคคลที่ถูกแสดงข้อมูลในรูป Pseudonymous เนื่องจาก

---

[24] Blumberg, A.,&Eckersley, P.,“On location privacy, and how to avoid losing it forever”,Accedssed17 January 2016, https://www.eff.org/wp/locational-privacy

[25] Skouma, G., Léonard, L.,“Online Behavioral Tracking : What May Change After the Legal Regorm on Personal Data Protection”,Accedssed17 January 2016, https://www.google.co.th/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjP0q-rqd7KAhXPno4KHfd5CqcQFggeMAA&url=http%3A%2F%2Fwww.springer.com%2Fcda%2Fcontent%2Fdocument%2Fcda_downloaddocument%2F9789401793841-c2.pdf%3FSGWID%3D0-0-45-1491988-p176890444&usg=AFQjCNGcJdBgL96uo-2z2ILWGM01jOVUPQ

การ Profiling ทำให้มีข้อมูลที่มากเพียงพอที่จะสืบค้นกลับไปยังตัวเจ้าของข้อมูลส่วนบุคคลนั้นได้ เมื่อพูดถึงการทำ Profiling บนอินเตอร์เน็ตแล้วมีมากในทางการตลาดเพื่อค้นหากลุ่มความสนใจของผู้ใช้และทำการโฆษณาให้ตรงตามความสนใจนั้น ซึ่งการกระทำในลักษณะดังกล่าวเป็นการประหยัดเวลาและมีประสิทธิภาพมากกว่าการโฆษณาโดยมิได้คำนึงถึงความสนใจของผู้ใช้งาน

2.5.3 ข้อมูลไบโอเมตริก (Biometric)

เทคโนโลยีไบโอเมตริก (Biometric) หรือเทคโนโลยีชีวภาพ มาจากคำว่า ไบโอ (Bio) หรือ Bios ในภาษากรีกซึ่งมีความหมายว่าชีวิต และคำว่า เมตริก (Metric) ซึ่งหมายถึง คุณลักษณะที่อาจถูกวัด หรือประเมินได้ ดังนั้น ไบโอเมตริกจึงหมายถึง เทคโนโลยีซึ่งนำมาใช้กับพฤติกรรมหรือคุณลักษณะบางประการของสิ่งมีชีวิต ซึ่งคุณลักษณะหรือพฤติกรรมนั้นมีความเป็นเอกลักษณ์จนสามารถเทียบวัดหรือนับจำนวนได้ และนำการวัดหรือการนับนั้นมาผนวกเข้ากับหลักการทางสถิติเพื่อแยกแยะหรือจดจำบุคคลแต่ละบุคคล[26]

เทคโนโลยีไบโอเมตริกเป็นเทคโลยีซึ่งประกอบด้วยอุปกรณ์เพื่อใช้ในการอ่านค่าเกี่ยวกับบุคคลและระบบซึ่งใช้ในการเชื่อต่อกับอุปกรณ์ที่บันทึกข้อมูลไบโอเมตริกเกี่ยวกับบุคคลนั้นเพื่อทำการระบุตัวบุคคล หรือยืนยันตัวบุคคล ระบบนี้จะทำการวัดค่าหรือวิเคราะห์คุณลักษณะของบุคคล เช่น รูปหน้า รูปแบบของเสียง ลายนิ้วมือง ลายมือ หรือม่านตา เป็นต้น โดยเทคโนโลยีไบโอเมตริกเป็นเทคโนโลยีซึ่งผสมผสานกับเทคโนโลยีอื่นๆ เช่น เทคโนโลยีด้านการแพทย์ เทคโนโลยีทางคอมพิวเตอร์ สถิติ วิทยาศาสตร์ หรือคณิตศาสตร์ เป็นต้น ข้อมูลเกี่ยวกับร่างกายของบุคคลซึ่งจะถือว่าเป็นข้อมูลไบโอเมตริกซ์ได้เมื่อข้อมูลนั้นมีลักษณะ[27]คือ 1. มีความเป็นสามัญโดยเป็นสิ่งที่บุคคลทุก

---

[26] เอกรินทร์ ซื่อธานุวงศ์, ระบบตรวจสอบลายนิ้วมือฝังตัว, (วิทยานิพนธ์วิศวกรรมศาสตรมหาบัณฑิต สาขาวิศวกรรมคอมพิวเตอร์, มหาวิทยาลัยสงขลานครินทร์, 2548), น. 9

[27] Babich, A.,“Biometric Authentication. Types of biometric identifiers, Bachelor’s Thesis, Degree Programme in Business Information Technology 2012”, Accedssed17 January 2016, https://www.google.co.th/url?sa=t&rct=j&q=&esrc=s&source=web&cd=11&cad=rja&uact=8&ved=0ahUKEwj7r5mt_ODKAhXCA44KHYu3CLcQFghQMAo&url=https%3A%2F%2Fwww.theseus.fi%2Fxmlui%2Fbitstream%2Fhandle%2F10024%2F44684%2FBabich_Aleksandra.pdf%3Fsequence%3D1&usg=AFQjCNF9vP2JZkYFP5DcRRPy_rgZD9RRZg&bvm=bv.113370389,d.c2E

คนมีเหมือนๆกัน 2. มีลักษณะเฉพาะต้องสามารถแยกบุคคลนั้นออกจากบุคคลอื่นได้ 3.มีลักษณะถาวรโดยต้องไม่เปลี่ยนแปลงได้ง่าย 4.สามารถที่จะวัดและเก็บข้อมูลได้โดยไม่มีค่าใช้จ่ายและเวลาที่เกิดสมควร 5. มีประสิทธิภาพ กล่าวคือ มีความรวดเร็วและแม่นยำ 6. มีความน่าเชื่อถือ 7. ทำการปลอแปลงได้ยาก

เทคโนโลยีไบโอเมตริกสามารถแบ่งตามการตรวจพิสูจน์ได้สองแบบ[28] คือ การตรวจสอบลักษณะทางกายภาพ (Physical Characteristics) และ การตรวจสอบทางพฤติกรรม (Behaviors) เทคโนโลยีไบโอเมตริกสามารถแบ่งออกได้หลายรูปแบบโดยมีสาระสำคัญดังนี้[29]

(1) การตรวจลายพิมพ์ดีเอ็นเอ (DNA Matching)

ลายพิมพ์ดีเอ็นเอในบุคคลใดบุคคลหนึ่งมีลักษณะเฉพาะ เนื่องจากการได้รับดีเอ็นเอจากบิดาและมารดาฝั่งละครึ่งหนึ่ง จึงทำให้บุคคลแต่ละคนมีลายพิมพ์ดีเอ็นเอที่ไม่เหมือนกัน[30] และไม่เปลี่ยนแปลงไปตามวัย การตรวจลายพิมพ์ดีเอ็นเอจึงสามารถระบุตัวบุคคลได้อย่างแม่นยำ

(2) ลักษณะของใบหู (Ear)

ลักษณะของใบหูแต่ละคนมีความแตกต่างกันและเมื่อบุคคลโตเต็มวัยแล้วลักษณะของใบหูจะมีการเปลี่ยนแปลงเพียงเล็กน้อยเท่านั้น ดังนั้นลักษณะของใบหูจึงสามารถนำมาใช้ในการระบุตัวบุคคลได้ดีเช่นเดียวกันกับการใช้รูปหน้า ในปัจจุบันได้เริ่มมีการนำลักษณะของใบหูมาใช้เพื่อระบุตัวบุคคล เช่น ในประเทศสหรัฐอเมริกา United States Immigration and Naturalization Service (INS) ได้กำหนดรูปแบบในการถ่ายรูปบุคคลให้ต้องเห็นรูปใบหูด้านขวา

(3) การรู้จำม่านตา (Iris Recognition)

การจดจำม่านตาเป็นเทคโนโลยีชีวิภาพอาศัยการสแกนดวงตาและอ่านสีและลายของม่านตาเทียบกับการอ่านค่าจากครั้งก่อนที่ได้ทำการจัดเก็บไว้ หากผลของการอ่านสีและลายของม่านตานั้นตรงกันหรือมีความแตกต่างเพียงเล็กน้อยย่อมจะถือบุคคลนั้นเป็นเจ้าของม่านตาที่ถูกเก็บข้อมูลไว้ การจดจำม่านตานี้มีความแม่นยำสูงเนื่องจากคนเราเมื่อเติบโตจนสมบูรณ์แล้วลายม่านตาจะไม่มีการเปลี่ยนแปลงและยังทำการปลอมแปลงได้ยาก

---

[28] ไม่ปรากฏผู้แต่ง, “เครื่องสแกนลายนิ้วมือ (Finger Scan)”, สืบค้นวันที่ 6 ก.พ. 2559, http://fingerscan.in.th/fingerprint-scanner/2-finger-scan

[29]Anonymous, “Types of Biometric”,Accedssed17 January 2016, http://www.biometricsinstitute.org/pages/types-of-biometrics.html

[30] “ลายพิมพ์ “ดีเอ็นเอ” สิ่งที่ทุกคนในโลกมีไม่ซ้ำกัน”, สืบวันที่ 17 มกราคม 2559, http://www.myfirstbrain.com/student_view.aspx?ID=66171

(4) การรู้จำใบหน้า (Face Recognition)

ใบหน้าของแต่ละคนมีองค์ประกอบซึ่งมีตำแหน่งแตกต่างกันในแต่ละคน ใบหน้าจึงถูกนำมาสร้างเป็นระบบเพื่อใช้ยืนยันตัวบุคคลอีกระบบหนึ่ง โดยระบบการรู้จำใบหน้านี้จะทำการตรวจจับใบหน้าของบุคคล นำข้อมูลที่ได้นั้นไปวิเคราะห์และเปรียบเทียบกับข้อมูลตัวอย่างที่ได้มีการบันทึกไว้ ซึ่งอาจเป็นการเปรียบเทียบทั้งใบหน้าหรือเพียงบางส่วนก็ได้ ด้วยเทคโนโลยีทางกล้องซึ่งมีความละเอียดสูงและให้ภาพที่คมชัดแม้อยู่ในระยะห่างจากวัตถุโฟกัสทำให้การรู้จำใบหน้าสามารถทำได้แม้อยู่ในระยะไกลออกไปจนในบางครั้งบุคคลอาจถูกตรวจสอบโดยไม่รู้ตัว อย่างไรก็ตามการรู้จำใบหน้าอาจมีข้อผิดพลาดได้ เช่น ภาพที่แปรปรวน การโฟกัสของกล้องไม่ตรงกับหน้า หรือการเปลี่ยนแปลงของใบหน้าเนื่องจากอายุที่มากขึ้น เป็นต้น

(5) การรู้จำลายนิ้วมือ (Fingerprint Recognition)

ลายนิ้วมือของคนเราประกอบด้วยเส้น (Ridge)ซึ่งเกิดจากการนูนของผิวหนังส่วนนอกและร่อง (Valley หรือ Furrow) มีลักษณะเป็นรอยลึกอยู่ต่ำกว่าระดับของเส้นอยู่เป็นจำนวนมาก ในการจดจำลายนิ้วมือของบุคคลเพื่อยืนยันตัวบุคคลนั้นอาศัยลักษณะเฉพาะของเส้นลายนิ้วมือเป็นสำคัญ โดยจะมีการเก็บตำแหน่งและทิศทางที่มีลักษณะพิเศษ ลักษณะเฉพาะของเส้นลายนิ้วมือสามารถแบ่งออกเป็นสองประเภท คือ เส้นจบ ซึ่งเป็นตำแหน่งปลายของเส้นลายนิ้วมือ และเส้นแตก ซึ่งเป็นเส้นที่แตกลักษณะแยกออกเป็นสองทาง การจำแนกเส้นลายนิ้วมือแล้วโดยพื้นฐานอาจแบ่งได้เป็น 3 ประเภท[31] คือ โค้ง (Arch) เป็นเส้นที่มาจากด้านหนึ่งด้านใดของนิ้วมือและเพิ่มจำนวนขึ้นตรงกลางก่อให้เกิดความโค้งและสิ้นสุดลงในอีกด้านหนึ่งก้นหอย (Whorl) เป็นเส้นซึ่งมีลักษณะเป็นวงล้อมรอบจุดกึ่งกลาง และ มัดหวาย (Loop) เป็นเส้นซึ่งมีจุดกำเนิดจากด้านใดด้านหนึ่งของนิ้วมือ และสร้างเส้นโค้งจนกระทั่งสิ้นสุดแล้วจึงกลับมาที่ด้านเดิม การพิสูจน์ลายนิ้วมือเพื่อยืนยันตัวเจ้าของนั้นจะทำโดยดูจาก 2 ลักษณะใหญ่ๆ[32] กล่าวคือ ลักษณะโดยรวม (Global Feature) อันเป็นลักษณะของลายนิ้วมือที่สามารถมองเห็นได้ด้วยตาเปล่าซึ่งประกอบไปด้วยองค์ประกอบ ได้แก่ แบบแผนลายเส้นพื้นฐาน (Basic ridge) พื้นที่ของแบบแผนลายเส้น (Pattern area) จุดใจกลาง (Core Area) สามาเหลี่ยมเดลต้าหรือสันดอน (Delta, Triradius) ชนิดของเส้น (Typelines) จำนวนเส้นลายนิ้วมือ (Ridge Count) และลักษณะเฉพาะที่ (Local Feature) ซึ่งเป็นลักษณะของจุดสิ้นสุด

---

[31]Fingtrack, “การรู้จำลายนิ้วมือ”, สืบค้นวันที่ 17 มกราคม 2559, http://fingerscan.in.th/fingerprint-scanner/83-fingerprint-recognition

[32] องค์การรักษาความปลอดภัยฝ่ายพลเรือน, “ความรู้ทั่วไปเกี่ยวกับลายนิ้วมือ ฝ่ามือ ฝ่าเท้า”, สืบค้นวันที่ 18 มกราคม 2559,http://www.secnia.go.th/2016/01/18/38500/

ของเส้นหรือจุดที่เส้นลายนิ้วมือแตกออกไป และมีความสำคัญเป็นอย่างมากเนื่องจากการรู้จำลายนิ้วอาศัยรูปแบบ 3 รูปแบบ คือ จุดสิ้นสุด จุดแยกเป็นจุดที่เส้นลายนิ้วมือแตกแขนงออกไป และจุดซึ่งเป็นลายเส้นที่มีขนาดสั้นที่สุดสำหรับลายพิมพ์นิ้วมือนั้นถือว่าเป็นเอกลักษณ์เฉพาะของบุคคลแต่ละคน แม้ว่าบุคคลนั้นจะมีความสัมพันธ์ในทางสายเลือด เช่น เป็นบิดา มารดา หรือพี่น้อง ก็ไม่อาจมีลายพิมพ์นิ้วมือที่เหมือนกันได้ นอกจากนี้การปลอมแปลงลายพิมพ์นิ้วมือนั้นทำได้ยาก ลายพิมพ์นิ้วมือจึงถูกนำมาใช้ในการยืนยันตัวบุคคลอย่างกว้างขวางไม่ว่าภาครัฐหรือเอกชน เช่น ในการทำบัตรประชาชน หรือการแสกนนิ้วมือเพื่อเข้าทำงานเป็นต้น

(6) การเดิน (Gait)

การเดินได้ถูกนำมาใช้ในการยืนยันตัวบุคคลจากการวิเคราะห์ลักษณะการเดินของบุคคลนั้น โดยสามรถทำได้แม้ตัวผู้ถูกระบุจะไม่ทราบหรือให้ความร่วมมือแก่การยืนยันตัวบุคคลเลยก็ตาม นอกจากนี้ยังสามารถทำได้แม้ตัวผู้ถูกยืนยันระบุจะอยู่ห่างออกไปจากผู้ทำการวิเคราะห์ โดยมีแนวความคิดที่จะนำการวิเคราะห์การเดินนี้มาใช้ในการระบุตัวผู้กระทำความผิด และยังอาจนำมาใช้ในทางการแพทย์เพื่อประโยชน์ในการระบุโรคบางชนิดแต่ระยะแรกเริ่ม เช่น พาร์กินสัน หรือเส้นโลหิตตีบตัน เป็นต้น ในปัจจุบันเทคโนโลยีทางการวิเคราะห์การเดินมี 2 ลักษณะ คือ ประเภทแรก คือ การวิเคราะห์โดยระบบอัตโนมัติผ่านการบันทึกทางวีดีโอ และประเภทที่สอง คือ การใช้ระบบเรดาร์ซึ่งเป็นระบบเดียวกันกับกล้องตรวจจับความเร็วบนท้องถนน โดยเรดาร์นี้จะบันทึกลักษณะการเคลื่อนไหวของบุคคลและนำมาวิเคราะห์เปรียบเทียบกับลักษณะที่ได้มีการบันทึกไว้ครั้งก่อนๆเพื่อการยืนยันตัวบุคคล

(7) ลักษณะของมือ (Hand Geometry)

ลักษณะของมือถูกนำมาใช้ในการยืนยันตัวบุคคลโดยการวัดขนาดของมือ เช่น ความยาว ความกว้างของนิ้วหรือฝ่ามือ หรือความหนาของฝ่ามือ เป็นต้น และวิเคราะห์เปรียบเทียบกับข้อมูลที่ได้ทำการบันทึกไว้ กระบวนการโดยทั่วไปจะทำการเก็บข้อมูลของมือทั้งด้านบนและด้านข้างโดยกล้องและจะทำการเก็บภาพอย่างน้อยสองภาพเพื่อใช้ในการเปรียบเทียบ ข้อบกพร่องของการนำลักษณะของมือมาใช้ในการยืนยันตัวบุคคล คือ ความไม่มีลักษณะเฉพาะที่มากเพียงพอและข้อจำกัดของระบบที่จำกัดไว้เพียงการยืนยันลักษณะของมือเท่านั้น[33]

---

[33]Federal Bureau of Investigation, “Hand Geometry”,Accedssed 18 January 2016,https://www.google.co.th/url?sa=t&rct=j&q=&esrc=s&source=web&cd=9&cad=rja&uact=8&ved=0ahUKEwiY94biqejKAhUGGY4KHYprD9gQFgg_MAg&url=https%3A%2F%2

(8) กลิ่น (Odor)

การวิจัยของคณะวิจัยแห่ง Universidad Politécnica de Madrid ได้พบว่าบุคคลแต่ละคนมีกลิ่นที่มีลักษณะเฉพาะและไม่เปลี่ยนแปลง ซึ่งทำให้สามารถนำกลิ่นมาใช้เพื่อระบุตัวบุคคลได้โดยมีความแม่นยำมากถึง 85 เปอร์เซ็นต์ และแม้กลิ่นของบุคคลอาจมีการเปลี่ยนแปลงตามการกระทำ เช่น การเปลี่ยนแปลงการรับประทานอาหาร การเปลี่ยนแปลงของอารมณ์ หรือการเกิดโรค เป็นต้น แต่ผลวิจัยได้พบว่าการวิเคราะห์กลิ่นของบุคคลจำนวน 13 คนในการทดลอง 28 ครั้ง พิสูจน์ให้เห็นว่าการใช้กลิ่นในการยืนยันตัวบุคคลมีความผิดพลาดเพียง 15 เปอร์เซ็นต์[34]

(9) การรู้จำลายเซ็น (Signature Recognition)

บุคคลแต่ละคนมีเอกลักษณ์เฉพาะในการเซ็นลายเซ็น การนำลายเซ็นมาใช้ในการยืนยันตัวบุคคลจะทำโดยการพิจารณารูปทรงและลักษณะของเส้นที่ประกอบเป็นของลายเซ็นนั้น อย่างไรก็ตามการรู้จำลายเซ็นเป็นการตรวจสอบทางพฤติกรรมของบุคคล (Behavioral Biometric) ที่อาจมีการเปลี่ยนแปลงได้ภายใต้องค์ประกอบบางประการ เช่น เวลา หรืออารมณ์เป็นต้น นอกจากนี้ลายเซ็นอาจมีการปลอมแปลงได้ง่ายการรู้จำลายเซ็นสามารถแบ่งออกได้เป็น 2 แบบ คือ แบบคงที่ (Static) ซึ่งเป็นกรณีที่ผู้ถูกตรวจสอบเซ็นลายเซ็นในกระดาษ ต่อมาจึงนำกระดาษที่มีลายเซ็นมาสแกนโดยสแกนเนอร์หรือกล้อง และจึงนำมาวิเคราะห์รูปร่างโดยระบบและแบบพลวัต (Dynamic) เป็นกรณีที่ผู้ถูกตรวจสอบเซ็นลายเซ็นในอุปกรณ์อิเล็กทรอนิกส์ เช่น คอมพิวเตอร์ สมาร์ทโฟน หรือแท็ปเล็ต เป็นต้น และจึงนำลายเซ็นนั้นมาวิเคราะห์โดยระบบเพื่อเปรียบเทียบลายเซ็นนั้นกับลายเซ็นที่ถูกจดจำไว้

Fwww.fbi.gov%2Fabout-us%2Fcjis%2Ffingerprints_biometrics%2Fbiometric-center-of-excellence%2Ffiles%2Fhand-geometry.pdf%2Fat_download%2Ffile&usg=AFQjCNH1Yh_pLokt1wGyXfCS7Sc47xaCfg&bvm=bv.113370389,d.c2E

[34] Hill, G.,"Body Odor Biometrics for Identity Verification",Accedssed18 January 2016,https://securitytoday.com/articles/2014/02/21/body-odor-biometrics-for-identity-verification.aspx?admgarea=ht.monitoring.

(10) การรู้จำเสียง (Voice Recognition)

การรู้จำเสียง เป็นการประมวลผลโดยวิธีการแปลงเสียงพูด (Audio File) ให้อยู่ในรูปของคำ (Text) ที่มีการเรียงลำดับต่อเนื่องกันด้วยอัลกอรึธึ่งที่ใช้ในโปรแกรมคอมพิวเตอร์[35] เทคโนโลยีได้ถูกพัฒนาขึ้นโดยหน่วยงานวิจัยของเนคเทค เพื่อการลดข้อจำกัดของการเข้าถึงเทคโนโลยี หลักการทำงานของการรู้จำเสียงคือ เมื่อบุคคลพูดสิ่งใดสิ่งหนึ่งออกไปยังไมโครโฟนซึ่งติดตั้งไว้บนคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ประเภทอื่น ระบบจะทำการประมวลผลวัดความถี่และขนาดของคลื่นเสียง และนำไปเปรียบเทียบกับเสียงที่เคยบันทึกไว้ก่อนหน้าเพื่อทำการยืนยันตัวบุคคล การรู้จำเสียงสามารถแบ่งออกได้เป็น 3 ประเภท[36] คือ 1. การรู้จำเสียงพูดจากสัญญาณเสียงพูดแบบคำโดด (Isolated Speech) เป็นการป้อนคำพูดเพียงสั้นๆหรือเป็นคำสั่งไม่กี่คำ 2. การรู้จำเสียงพูดแบบต่อเนื่อง (Continous Speech) เป็นการป้อนคำพูดที่มีความยาวมากขึ้นจากการป้อนแบบคำโดด โดยอาจมีการป้อนเป็นประโยคก็ได้และ 3. การรู้จำเสียงพูดแบบคำอุทาน (Spontaneous Speech) เป็นการป้อนคำพูดที่มีคำอุทานอยู่ด้วย เพื่อให้ระบบเข้าใจเนื้อหาสำคัญของคำพูดนั้น การรู้จำเสียงอาจเกิดข้อผิดพลาดได้บ้างทั้งนี้อาจเกิดขึ้นจากตัวผู้ถูกระบุเอง เช่น การใช้เสียงตะโกน หรือการใช้เสียงกรีดร้อง เป็นต้น หรือเกิดจากปัจจัยภายนอก เช่น เสียงรบกวนรอบข้าง เป็นต้น

โดยเทคโนโลยีไบโอเมตริกซ์มีความแพร่หลายมากเนื่องจากสาเหตุหลายประการ กล่าวคือ ประการแรกเทคโนโลยีนี้สามารถทำการระบุตัวบุคคลได้อย่างแม่นยำผ่านลักษณะของร่างกายมนุษย์มากกว่าการใช้รหัสซึ่งสามารถถูกปลอมแปลงได้ง่ายกว่า ประการที่สองเทคโนโลยีดังกล่าวมีความปลอดภัยสูง เนื่องจากไบโอเมตริกนั้นไม่สามารถที่ถูกคาดเดาได้ทั้งยังปลอมแปลงได้ยาก และประการที่สามการนำไบโอเมตริกมาใช้ก่อให้เกิดความสะดวก รวดเร็วและประหยัดในการนำมาใช้งานโดยผู้ถูกระบุตัวไม่จำต้องพกพาอุปกรณ์ในการระบุตัวตน เช่น สมาร์ทการ์ด หรือท่องจำรหัสผ่าน แต่การระบุตัวตนจากไบโอเมตริกจะคงอยู่กับตัวผู้ถูกระบุตลอดเวลาไม่อาจที่จะหายหรือถูกขโมยได้ นอกจากนี้การพัฒนาของเทคโนโลยีในปัจจุบันทำให้การประมวลผลไบโอเมตริกซ์เพื่อเทียบกับข้อมูลที่ได้ถูกจัดเก็บไว้ทำได้อย่างรวดเร็วและมีความแม่นยำสูง

---

[35] สมชัย สิริวัฒนวงศ์ชัย, “การสร้างโมเดลคำหลักแบบอัตโนมัติ สำหรับระบบค้นหาคำหลักจากเสียงพูดแบบหลายโดเมน”, (วิทยานิพนธ์ วิทยาศาสตรมหาบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์ ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยธรรมศาสตร์ 2549),น. 7

[36]Hill, G., อ้างแล้วใน 34

จากเทคโนโลยีไบโอเมตริกที่ได้กล่าวมาทั้งหมด เทคโนโลยีที่สามารถพบเห็นได้มากคือการรู้จำลายนิ้วมือซึ่งถูกนำมาใช้อย่างแพร่หลายในการควบคุมการเข้าออกสถานที่ หรือการใช้ตรวจสอบเวลาทำงาน อย่างไรก็ตามเนื่องจากความแม่นยำในการระบุตัวตน ความยากในการปลอมแปลง ความรวดเร็วในการประมวลผล และจุดอ่อนของการใช้พาสเวิร์ดซึ่งมีข้อเสียคือถูกคาดเดาหรือปลอมแปลงได้ง่ายและในหลายๆครั้งผู้ใช้ลืมพาสเวิร์ดที่ตนเองตั้งไว้ ทำให้เริ่มมีการพัฒนาเทคโนโลยีไบโอเมตริกมาใช้บนอินเตอร์เน็ต บริษัทวิจัย Gartner ได้กล่าวว่าในปี 2016 การใช้งานอินเตอร์เน็ตจะมีการนำไบโอเมตริกมาใช้งานเพื่อเปิดอุปกรณ์อิเล็กทรอนิกส์ถึง 20 เปอร์เซ็นต์ และเชื่อว่าในอนาคตจะมีการนำเทคโนโลยีดังกล่าวมาใช้เพิ่มเติมมากขึ้นคาดว่าในปี 2018 จะมีการใช้งานมากถึง 500 ล้านอุปกรณ์[37] สิ่งที่ยืนยันคำพูดดังกล่าวเป็นอย่างดีคือการเพิ่มเซ็นเซอร์ในการสแกนลายนิ้วมือของค่ายบริษัทผลิตสมาร์ทโฟนยักษ์ใหญ่อย่าง Apple ได้ติดตั้งเซ็นเซอร์สแกนลายนิ้วมือบน iPhone 5S และ Samsung ได้ติดตั้งเซ็นเซอร์ดังกล่าวบน Samsung Galaxy S5 เช่นกัน ความคิดในการนำเซ็นเซอร์สแกนลายนิ้วมือมาติดตั้งบนสมาร์ทโฟนเริ่มต้นขึ้นโดยบริษัท Motorola ต่อมาบริษัท Apple จึงได้นำเทคโนโลยีนี้มาติดตั้งบน iPhone 5Sในปี 2013 และในปี 2014 Samsung จึงทำการออก Galaxy S5 จุดเริ่มต้นนี้ทำให้บริษัทผลิตสมาร์ทโฟนต้องหันมาเติมเซ็นเซอร์สแกนลายนิ้วมือลงบนผลิตภัณฑ์ของตนเอง เช่น Lenovo VIBE P1, Huawei Honor7, Oppo R7 Plus และ Asus คาดว่าจะใส่เซ็นเซอร์นี้ลงใน Zenfone3 เป็นต้น

นอกจากเครื่องสแกนลายพิมพ์นิ้วมือจะได้ถูกติดตั้งบนสมาร์ทโฟนดังที่ได้กล่าวมาแล้ว เทคโนโลยีนี้ยังได้ถูกนำมาใช้ในการชำระเงิน โดย MasterCard ซึ่งเป็นเครือข่ายในการให้บริการการทำธุรกรรมผ่านบัตรเครดิตได้ร่วมมือกับบริษัท Zwipe นำเทคโนโลยีไบโอเมตริก คือการแสกนลายนิ้วมือมาใช้ในการชำระเงินผ่านบัตรเครดิต โดยเมื่อมีการชำระเงินผ่านบัตรเครดิตเจ้าของบัตรเครดิตต้องวางนิ้วมือบนเซ็นเซอร์ที่ใช้สำหรับการสแกนลายนิ้วมือและแกว่งผ่านเครื่องรูดบัตรเครดิต เครื่องสแกนลายนิ้วมือจะทำการอ่านลายนิ้วมือของเจ้าของบัตรและเปรียบเทียบกับข้อมูลลายนิ้วมือที่ได้ถูกเก็บไว้ในบัตรนั้น เมื่อเห็นว่าลายนิ้วมือนั้นตรงกับลายนิ้วมือที่ได้ถูกเก็บไว้ในบัตรจึงจะส่งข้อมูลเพื่อทำการชำระเงินต่อไป[38] ไบโอเมตริกถือว่าเป็นหนึ่งในเทคโนโลยีที่กำลังก้าวเข้ามี

---

[37] Sarah Le, “Biometrics to Secure the Internet of things”,Accedssed18 January 2016, http://www.engadget.com/2015/10/08/biometrics-to-secure-the-internet-of-things/

[38]Zwipe, “Mastercard and Zwipe announce the launch of the world’s first biometric contactless payment card with integrated fingerprint

บทบาทสำคัญในชีวิตเรา ในอนาคตนั้นอาจมีการนำเทคโนโลยีไบโอเมตริกประเภทอื่น เช่น การสแกนม่านตา การวัดอัตราการเต้นของหัวใจ หรือการรู้จำเสียง เป็นต้น มาใช้เพื่อเป็นทางเลือกในการยืนยันตัวบุคคลอีกด้วย

2.5.4สิทธิการโอนข้อมูลส่วนบุคคลที่อยู่ในรูปแบบอิเล็กทรอนิกส์ (Right to Data Portability)

สิทธิในการโอนข้อมูลส่วนบุคคลซึ่งอยู่ในรูปแบบอิเล็กทรอนิกส์(Right to data portability) มีแนวความคิดพื้นฐานจากสิทธิในการเข้าถึงข้อมูลส่วนบุคคล สิทธิดังกล่าวเป็นสิทธิซึ่งให้แก่เจ้าของข้อมูลส่วนบุคคลทำให้สามารถโอนข้อมูลส่วนบุคคลของตนไปยังผู้ประกอบการหรือแอพพลิเคชั่นอื่นๆในรูปแบบที่สามารถใช้งานได้ การโอนข้อมูลส่วนบุคคลนี้ช่วยให้เจ้าของข้อมูลส่วนบุคคลสามารถจัดการกับข้อมูลที่แสดงเอกลักษณ์ หรือข้อมูลอื่นๆของตนเอง เช่น รูปภาพ หรือวีดีโอ เป็นต้น ความคิดในการโอนข้อมูลส่วนบุคคลระหว่างผู้ประกอบการหรือแอพพลิเคชั่นนั้นเริ่มต้นขึ้นโดย The DataPortability Project ซึ่งก่อตั้งโดยคนกลุ่มหนึ่งที่รวมตัวกันในเดือนพฤศจิกายน ค.ศ. 2007 และในปี ค.ศ. 2008 ก็ได้รับการสนับสนุนจากผู้ประกอบการยักษ์ใหญ่ด้านโซเชียลมีเดีย เช่น Facebook และ Google

สิทธิในการโอนข้อมูลส่วนบุคคล(Right to data portability)มีความเกี่ยวข้องกับโครงการที่กำลังดำเนินการอยู่ในหลายประเทศในสหภาพยุโรป ซึ่งโครงการดังกล่าวเป็นจุดเริ่มต้นของสิทธิในการโอนข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์(Right to data portability) โครงการนี้มีวัตถุประสงค์เพื่อให้ปัจเจกบุคคลสามารถร้องขอข้อมูลส่วนบุคคลที่สามารถโอนได้และอยู่ในรูปแบบอิเล็กทรอนิกส์จากผู้ประกอบการ เช่น ประเทศอังกฤษ มีโครงการชื่อว่า MiData[39]เริ่มขึ้นในปี ค.ศ.

---

sensor",Accedssed18 January 2016,http://zwipe.com/news/mastercard-and-zwipe-announce-the-launch-of-the-worlds-first-biometric-contactless-payment-card-with-integrated-fingerprint-sensor

[39] Bapat, A.,"The new right to data portability", Pdpjournal, Voulme 13, issue 3,Accedssed19 January 2016, https://www.google.co.th/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwj4-uCG-e7KAhXEA44KHcTjBNUQFggfMAE&url=https%3A%2F%2Fwww.hunton.com%2Ffiles%2FPublication%2Fc924a1bc-b27e-420f-ada4-

2011และเป็นจุดเริ่มต้นของการให้สิทธิในการเข้าถึงข้อมูลส่วนบุคคลหรือโอนข้อมูลส่วนบุคคลของผู้บริโภคในรูปแบบอิเล็กทรอนิกส์ในประเทศอื่นๆ MiData เป็นการแบ่งปันข้อมูลระหว่างองค์กรและผู้บริโภคของตน มีวัตถุประสงค์ให้ผู้บริโภคสามารถเข้าถึงข้อมูลส่วนบุคคลเกี่ยวกับการบริโภคของตัวเองได้เพื่อให้ทราบถึงลักษณะและพฤติกรรมการบริโภคของตนเอง สามารถนำข้อมูลนั้นไปพัฒนากับการจับจ่ายซื้อสินค้าหรือการบริโภคของตนเองให้ดีขึ้น สามารถจัดการตนเองได้อย่างมีประสิทธิภาพ และสามารถที่จะเลือกบริการหรือผลิตภัณฑ์ที่ตรงต่อความต้องการของตนเองได้ ต่อมาจึงเกิดโครงการในสหรัฐอเมริกาชื่อว่า Smart Disclosure โดยมีแนวคิดริเริ่มจากโครงการ MiData[40]

Smart Disclosure เป็นโครงการซึ่งให้สิทธิแก่ผู้บริโภคในการเข้าถึงข้อมูลส่วนบุคคลของตนที่เกี่ยวกับการตัดสินใจของผู้บริโภคคนนั้น เช่น สินค้าที่ผู้บริโภคซื้อ และสามารถที่จะนำข้อมูลนั้นไปเปรียบเทียบกับตัวเลือกอื่นๆได้[41] และในประเทศฝรั่งเศสมีโครงการ Mesinfos ซึ่งให้สิทธิผู้บริโภคผู้เป็นเจ้าของข้อมูลในการจัดการและควบคุมข้อมูลของตนเอง วัตถุประสงค์ของโครงการนี้คือ เพิ่มความรู้เกี่ยวกับตัวเอง ประเมินการตัดสินใจที่ผ่านมาของตนเอง เพิ่มตัวเลือกแก่ผู้บริโภค เกิดความร่วมมือและแบ่งปันข้อมูลส่วนบุคคลแก่บุคคลอื่นๆ และเพื่อให้การดำรงชีวิตง่ายขึ้น[42]

6635d6c9ab4a%2FPresentation%2FPublicationAttachment%2Fd4ce9cda-8229-4778-bdf3-
73eb9a9c3f70%2FThe_new_right_to_data_portability_Bapat.pdf&usg=AFQjCNEN5_bpbZXWc1wNsGYw_FGUK7q7dg&bvm=bv.113943164,d.c2E

[40]Cabinet office behavioural insights team, “Midata 2012 review and consultation”,Accedssed19 January 2016, https://www.google.co.th/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwjsgsO0qe_KAhWJj44KHZfYB4IQFgghMAE&url=https%3A%2F%2Fwww.gov.uk%2Fgovernment%2Fuploads%2Fsystem%2Fuploads%2Fattachment_data%2Ffile%2F32687%2F12-943-midata-2012-review-and-consultation.pdf&usg=AFQjCNFQEkVe50zJbgbO_swGMN52wnfjLg

[41] Howard, A.,“What is smart disclosure?”,Accedssed19 January 2016, http://radar.oreilly.com/2012/04/what-is-smart-disclosure.html

[42] Mesinfors, “The goal of the “Mesinfo” project”,Accedssed19 January 2016,http://mesinfos.fing.org/english/

เมื่อพิจารณาสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของผู้บริโภคที่นำมาใช้ในประเทศต่างๆ เช่น ประเทศอังกฤษ สหรัฐอเมริกา และประเทศฝรั่งเศส ดังที่ได้กล่าวมาแล้ว จะเห็นได้มีวัตถุประสงค์ที่เหมือนกัน กล่าวคือ ต้องการให้ผู้บริโภคสามารถนำข้อมูลนั้นมาพิจารณาและวิเคราะห์ลักษณะการบริโภคของตนเพื่อพัฒนาการบริโภคของตนให้ดีขึ้น สามารถนำข้อมูลการบริโภคของตนมาวิเคราะห์เปรียบเทียบกับสินค้าหรือบริการของบริษัทห้างร้านหรือผู้ให้บริการอื่นๆเพื่อผู้บริโภคสามารถคัดเลือกสินค้าหรือบริการที่ให้ประโยชน์สูงสุดแก่ตนเองได้ แต่สำหรับสิทธิในการโอนข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์(Right to data portability)นั้นมีข้อได้เปรียบสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของผู้บริโภคซึ่งเป็นที่มาของสิทธินี้ กล่าวคือ นอกจากสิทธิในการโอนข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์(Right to data portability)จะให้สิทธิแก่ผู้บริโภคในการเข้าถึงข้อมูลการบริโภคของตนเพื่อนำมาวิเคราะห์และปรับปรุงการบริโภคของตนแล้ว สิทธิดังกล่าวยังทำให้ผู้บริโภคสามารถควบคุมข้อมูลส่วนบุคคลของตนและขอให้ผู้ประกอบการโอนข้อมูลนั้นไปยังผู้ประกอบการหรือผู้ให้บริการอื่นๆ อันเป็นการส่งเสริมการแข่งขันทางการค้า ลดการผูกขาดทางการค้าของผู้ประกอบการยักษ์ใหญ่ เป็นการส่งเสริมให้ผู้ประกอบการพัฒนาสินค้าหรือบริการของตนและให้ผู้บริโภคได้ใช้สินค้าหรือบริการที่มีราคาไม่สูงเกินสมควรอีกด้วย

สิทธิในการโอนข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์(Right to data portability)นี้ทำให้ผู้บริโภคสามารถเปลี่ยนผู้ให้บริการได้ง่ายซึ่งช่วยให้ผู้ใช้บริการไม่ถูกผูกขาดโดยผู้ให้บริการรายเดียว[43] ยกตัวอย่างเช่น การเปลี่ยนผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ หรือการเปลี่ยนผู้ให้บริการอินเตอร์เน็ต เป็นต้น โดยผู้บริโภคสามารถร้องขอให้ผู้ให้บริการเดิมทำการโอนข้อมูลซึ่งผู้ให้บริการเดิมได้รับจากผู้บริโภคหรือเป็นข้อมูลที่ผู้ให้บริการเดิมได้เก็บรวบรวมไว้ไปยังผู้ประกอบการอีกรายหนึ่ง หรือในกรณีโซเชียลเน็ตเวิร์ค แทนที่ผู้ใช้บริการ Facebook ซึ่งต้องการจะเปลี่ยนหรือเพิ่มเติมผู้ให้บริการ Google+ ต้องทำการดาวน์โหลดข้อมูลจาก Facebook และอัพโหลดไปยัง Google+ ด้วยตนเอง ผู้ใช้บริการ Facebook สามารถร้องขอให้ Facebook โอนข้อมูลส่วนบุคคลของตนไปยัง Google+ โดยตรงได้

อย่างไรก็ตามสิทธิในการโอนข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์(Right to data portability)นี้ยังมีปัญหาบางประการ กล่าวคือ ผู้ประกอบการอาจเก็บข้อมูลส่วนบุคคลโดย

---

[43]Grafe, I.,“Data portability series: At the crossroads of data protection & competition policy”,Accedssed20 January 2016, blogs.lse.ac.uk/mediapolicyproject/2014/04/11/data-portability-series-at-the-crossroads-of-protection-and-competition-policy/

อาศัยรูปแบบทางอิเล็กทรอนิกส์ที่แตกต่างกันทำให้ข้อมูลอิเล็กทรอนิกส์อาจไม่สามารถนำไปใช้กับผู้ประกอบการรายอื่นได้ จึงจำเป็นต้องกำหนดรูปแบบของข้อมูลส่วนบุคคลที่เก็บในรูปแบบของอิเล็กทรอนิกส์ให้เป็นแบบเดียวกันเพื่อให้ผู้ประกอบการรายอื่นสามารถใช้ข้อมูลนั้นๆได้ด้วย การกำหนดรูปแบบของการเก็บข้อมูลนี้ก่อให้เกิดปัญหาขึ้นว่าผู้ประการรายย่อยอย่าง SME (Small and medium-sized enterprises) อาจไม่มีทรัพยากรเพียงพอที่จะนำมาพัฒนาโปรแกรมเช่นเดียวกันกับบริษัทยักษ์ใหญ่ที่มีพร้อมทั้งกำลังคนและทรัพย์ ส่งผลให้ SME อาจต้องออกจากการเป็นผู้เล่นในตลาดไป ในท้ายที่สุดผลเสียย่อมจะเกิดขึ้นแก่ผู้บริโภค[44] สำหรับผู้เขียนแล้วเห็นว่าแม้การพัฒนาโปรแกรมขึ้นมาแม้อาจมีค่าใช้จ่ายสูงและอาจก่อให้เกิดความยากลำบากแก่ SME บ้างในช่วงแรก แต่กลับจะส่งผลดีต่อ SME ในเวลาต่อมา กล่าวคือ หาก SME มีศักยภาพที่เพียงพอย่อมดึงดูดกลุ่มผู้บริโภคที่ไม่พอใจการให้บริการของบริษัทยักษ์ใหญ่และทำการโอนข้อมูลส่วนบุคคลของตนมายัง SME ได้ง่าย

2.6 การละเมิดความเป็นส่วนตัวจากการใช้ข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์

แม้เทคโนโลยีที่เกี่ยวกับข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์จะมีประโยชน์มหาศาลในการนำมาใช้ แต่เทคโนโลยีดังกล่าวก็ยังมีจุดอ่อนทำให้ง่ายต่อการละเมิดข้อมูลส่วนบุคคล กล่าวคือ

2.6.1 ข้อมูลของอุปกรณ์อิเล็กทรอนิกส์ (Mac Address หรือ IP Address)

ข้อมูล Mac Address สามารถใช้เพื่อยืนยันคอมพิวเตอร์เครื่องใดเครื่องหนึ่งได้ แม้ว่าคอมพิวเตอร์นั้นอาจมิใช่ตัวบุคคลแต่การเก็บข้อมูล Mac Address ทำให้เห็นความเคลื่อนไหวของเจ้าของเครื่องได้และอาจนำไปสู่ตัวเจ้าของเครื่องคอมพิวเตอร์ในที่สุด กล่าวคือ เมื่อคอมพิวเตอร์แทปเล็ต สมาร์ทโฟน หรืออุปกรณ์อื่นซึ่งมีลักษณะคล้ายกันได้เชื่อมต่อกับ Wi-Fi ณ จุดเชื่อมต่อจะมี

---

[44]Swire, P., Lagos, Y.,“Why the right to data portability likely reduces consumer welfare: antitrust and privacy critique, Maryland law review”,Accedssed20 January 2016, https://www.google.co.th/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwi55Or5r-_KAhWBCo4KHbISDdYQFggjMAE&url=http%3A%2F%2Fdigitalcommons.law.umaryland.edu%2Fcgi%2Fviewcontent.cgi%3Farticle%3D3550%26context%3Dmlr&usg=AFQjCNFkIw5MKgCSQHt5Re1HXLA9c5nObg&bvm=bv.113943164,d.c2E

การส่งข้อมูล Mac Address ไป ทำให้ผู้ที่สามารถเข้าถึงข้อมูลเหล่านี้ได้สามารถทราบพิกัดที่มีการเชื่อมต่อ หาก ณ พิกัดใดมีการเชื่อมต่อบ่อยๆผู้ที่ทราบข้อมูลเหล่านี้ย่อมสามารถจำกัดพื้นที่การใช้งานของเจ้าของคอมพิวเตอร์ แทปเล็ต สมาร์ทโฟน หรืออุปกรณ์ซึ่งมีลักษณะคล้ายกันได้

สำหรับข้อมูล IP Address ไม่ว่าจะเป็นประเภท Dynamic หรือ Static สามารถคุกคามความเป็นส่วนตัวของบุคคลได้โดยผู้ที่มีข้อมูล IP Address สามารถนำข้อมูลนั้นไปตรวจสอบเพื่อทราบว่าผู้ใช้อยู่ในประเทศใดและจังหวัดใด สำหรับเว็บไซต์ที่สามารถตรวจสอบได้ เช่น http://whatismyipaddress.com/ เมื่อทำการสืบค้น IP Address เว็บไซต์ดังกล่าวจะแจ้งถึงผู้ให้บริการ (Internet Service Provider) จังหวัดและประเทศของผู้ใช้งาน ซึ่งในบางครั้งการสืบค้น IP Address เช่นนี้อาจบอกถึงสถานที่ทำงานของผู้ใช้งานเครื่องได้อีกด้วย การนำ IP Address ไปสืบค้นสามารถบอกถึงโครงข่ายการใช้งานแบบ P2P (peer-to-peer) เช่น แบ่งปันไฟล์ หรือการใช้งานต่างๆ ซึ่งการกระทำบางอย่างสามารถบ่งชี้ถึงพฤติกรรม ความคิดหรือรสนิยมของเจ้าของข้อมูล IP Address ได้ นอกจากนี้การใช้ IP Address ยังสามารถติดตามการใช้งานของบุคคลบนอินเตอร์เน็ตได้ เช่น เมื่อเจ้าของ IP Address เปิดอ่านไฟล์เอกสารใดเอกสารหนึ่งบนเว็บไซต์ เว็บไซต์ดังกล่าวจะสามารถทราบได้ว่าเจ้าของ IP Address นี้อ่านเอกสารใดบนเว็บไซต์ของตน[45]

2.6.2 ข้อมูลซึ่งไม่สามารถรู้ตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

ข้อมูลซึ่งไม่สามารถรู้ตัวบุคคลผู้เป็นเจ้าของข้อมูลได้เป็นข้อมูลที่ถูกลบหรือแทนค่าชื่อหรือข้อมูลอื่นของเจ้าของข้อมูลส่วนบุคคลเพื่อมิให้สามารถรู้ตัวเจ้าของข้อมูลได้โดยสามารถแบ่งออกได้ 2 ระดับ คือ ข้อมูลประเภท Anonymous ซึ่งเป็นข้อมูลที่ทำการสืบกลับไปยังเจ้าของข้อมูลส่วนบุคคลได้ยากหรือแทบจะเป็นไปไม่ได้เลย และข้อมูลประเภท Pseudonymousซึ่งเป็นข้อมูลที่ยังมีร่องรอยบางประการให้สืบกลับไปยังเจ้าของข้อมูลส่วนบุคคลได้ แม้เมื่อพิจารณาโดยผิวเผินแล้วข้อมูลประเภท Anonymous และ Pseudonymous อาจไม่ส่งผลกระทบต่อเจ้าของข้อมูล แต่เมื่อพิจารณาโดยลึกซึ้งแล้วข้อมูลทั้งสองประเภทนี้ยังอาจส่งผลให้เจ้าของข้อมูลถูกละเมิดความเป็นส่วนตัวได้ โดยงานวิจัยในปี ค.ศ. 1997 ได้รวบรวมข้อมูลของคนไข้จำนวนมากจากประวัติคนไข้ซึ่งได้มีการลบรหัสไปรษณีย์และวันเกิดของคนไข้ทั้งหมดเพื่อมิให้สามารถสืบกลับไปยังเจ้าของข้อมูลได้ แต่งานวิจัยดังกล่าวยังแสดงให้เห็นว่าข้อมูลที่เหลืออยู่สามารถบ่งชี้ไปยังตัวคนไข้ผู้เป็นเจ้าขอข้อมูลได้

---

[45] Office of the privacy commissioner of Canada, “What an IP Address can reveal about you”, Accedssed20 January 2016,https://www.priv.gc.ca/information/research-recherche/2013/ip_201305_e.pdf

และในปี ค.ศ. 2006 ได้มีงานวิจัยงานวิจัยเกี่ยวกับ Netflix ซึ่งเป็นเว็บไซต์ให้บริการดูหนังออนไลน์ งานวิจัยดังกล่าวได้ให้ผู้ใช้บริการได้ทำการให้คะแนนเพื่อประเมินความพอใจ แม้การให้คะแนนหนังนี้จะไม่ปรากฏว่าผู้ให้คะแนนเป็นใคร แต่หากผู้ให้คะแนนคนหนึ่งคนใดได้ให้คะแนนหนังเพียงจำนวน 6 เรื่องก็จะทำให้สามารถระบุตัวผู้ใช้บริการถูกต้องได้ถึง 99 เปอร์เซ็นต์[46]

สำหรับข้อมูล Pseudonymous นี้สามารถทำการสืบกลับไปยังเจ้าของข้อมูลส่วนบุคคลได้ง่ายกว่าข้อมูล Anonymous กล่าวคือ วัตถุประสงค์ของการแปลงข้อมูลส่วนบุคคลให้เป็นข้อมูลประเภท Anonymous นี้เพื่อลบร่องรอยหรือข้อมูลต่างๆมิให้บุคคลใดๆสืบกลับไปยังเจ้าของข้อมูลส่วนบุคคลได้ แต่ข้อมูลประเภท Pseudonymous ยังทิ้งร่องรอยบางประการเอาไว้เกี่ยวกับตัวเจ้าของข้อมูลส่วนบุคคลเพื่อให้ผู้ควบคุมข้อมูลซึ่งเป็นผู้แปลงข้อมูลส่วนบุคคลให้เป็นข้อมูล Pseudonymous สืบกลับไปยังเจ้าของข้อมูลส่วนบุคลได้เพื่อประโยชน์บางประการ เช่น การทำวิจัย เป็นต้น ทำให้ในการแปลงข้อมูลส่วนบุคคลให้อยู่ในรูปข้อมูล Pseudonymous อาจก่อให้เจ้าของข้อมูลส่วนบุคคลถูกละเมิดจากผู้ไม่หวังดีได้ นอกจากนี้การแปลงข้อมูลส่วนบุคคลให้เป็นข้อมูลประเภท Pseudonymous ยังอาจถูกนำมาใช้ในการหลีกเลี่ยงกฎหมายการคุ้มครองข้อมูลส่วนบุคคล เช่น หลีกเลี่ยงการห้ามเก็บข้อมูลส่วนบุคคลไว้นานเกินกว่าความจำเป็นในประเทศที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลไม่ครอบคลุมถึงข้อมูลประเภทดังกล่าว

2.6.3Profiling

การทำการรวบรวมและนำข้อมูลส่วนบุคคลมาวิเคราะห์นอกจากจะก่อให้เกิดความรำคาญแก่เจ้าของข้อมูลส่วนบุคคล และทำให้ทราบถึงตัวเจ้าของข้อมูลส่วนบุคคลที่อยู่ในรูปของ Anonymous และ Pseudonymous ดังที่ได้กล่าวมาได้แล้ว การทำการ Profiling ยังก่อให้เกิดผลเสียงต่อเจ้าของข้อมูลส่วนบุคคลอีกหลายประการ กล่าวคือ ประการแรก การทำการ Profiling นี้เป็นเสมือนการรุกล้ำความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลด้วยการเก็บรวบรวมการกระทำ พฤติกรรม ลักษณะนิสัย หรือความชอบของเจ้าของข้อมูลส่วนบุคคลทุกๆการกระทำที่เจ้าของข้อมูลส่วนบุคคลได้กระทำบนอินเตอร์เน็ต และทำให้เจ้าของข้อมูลส่วนบุคคลตกอยู่ภายใต้การพิจารณาของระบบอัตโนมัติคือ โปรแกรมคอมพิวเตอร์ ซึ่งผลลัพธ์ของการประมวลผลนี้อาจไม่มีความถูกต้องเสมอไป ส่งผลให้เจ้าของข้อมูลส่วนบุคคลอาจต้องรับผลลัพธ์ที่เกิดจากการประมวลผลผิดๆของระบบอัตโนมัติโดยตนเองไม่มีสิทธิโต้แย้ง

---

[46] EDRi, “An introduction to data protection”,Accedssed20 January 2016,https://edri.org/files/paper06_**data**p.pdf

ประการที่สอง การทำ Profiling ทำให้เจ้าของข้อมูลส่วนบุคคลถูกติดตามซึ่งอาจเป็นการติดตามโดยรัฐบาลเพื่อความปลอดภัยของประเทศ หรือเพื่อวัตถุประสงค์ในทางการเมือง หรือเป็นการติดตามโดยผู้ประกอบการเพื่อวัตถุประสงค์ทางการค้า ซึ่งโดยปกติแล้วผู้ประกอบการเหล่านี้มักทำการติดตามผู้บริโภคโดยมีวัตถุประสงค์คือให้ทราบถึงความเปลี่ยนแปลงที่เกิดขึ้นในตลาดผู้บริโภคและพัฒนาตนเองเพื่อเจาะกลุ่มผู้บริโภคเหล่านั้น ซึ่งการติดตามนี้แต่เดิมมักทำโดยวิธีการที่หลากหลายซึ่งมีความแม่นยำไม่มากนักและผู้บริโภคเองก็สามารถหลบเลี่ยงได้ง่าย เช่น การสำรวจการทำแบบสอบถาม หรือการซื้อสินค้าหรือบริการผ่านบัตรเครดิต เป็นต้น แต่เมื่อมีเทคโนโลยี Profiling เข้ามาทำให้การติดตามพฤติกรรมของกลุ่มผู้บริโภคสามารถทำได้ง่ายขึ้น สะดวกมากขึ้นและมีความแม่นยำสูงยากที่ผู้บริโภคจะหลบเลี่ยงการติดตามเหล่านี้ได้ เช่น บางบริษัทสามารถติดตามพฤติกรรมของผู้บริโภคที่เปลี่ยนแปลงได้อย่างทันทีโดยการนำแบบจำลองที่ใช้ในการคาดการณ์มาประยุกต์ใช้ แบบจำลองนี้สามารถทำให้บริษัทบอกได้อย่างทันทีว่าผู้บริโภครายนั้นกำลังมีปัญหาเรื่องการหย่าร้าง หรือกำลังตั้งครรภ์[47] เป็นต้น

ประการที่สาม การทำ Profiling ก่อให้เกิดการเลือกปฏิบัติต่อผู้บริโภคได้ ทั้งนี้ขึ้นอยู่กับนโยบายของผู้ขายสินค้าหรือผู้ให้บริการแต่ละราย กล่าวคือ การทำ Profiling เป็นการเปิดโอกาสให้แก่ผู้ประกอบการทราบถึงพฤติกรรม รสนิยม และความชอบส่วนตัวของบุคคลแต่ละคน ทำให้ผู้ขายสินค้าหรือบริการอาจใช้ราคา หรือจำนวนสินค้ามาเป็นตัวเร่งรัดการตัดสินใจของผู้บริโภคได้ หรือในบางครั้งอาจมีการแสดงราคาสินค้าแก่ผู้บริโภคที่มีความสนใจสินค้าประเภทนั้นมากสูงกว่าราคาสินค้าที่แสดงแก่ผู้บริโภคคนอื่นๆ

ประการที่สี่ การทำ Profiling ก่อให้ผู้บริโภคเสียโอกาสในการรับรู้สินค้าหรือโปรโมชั่นอื่นๆ กล่าวคือเมื่อทำ Profiling และทราบถึงความชอบของผู้บริโภคแล้ว เว็บไซต์ต่างๆ รวมถึงโฆษณาบนเว็บไซต์จะทำการแสดงสินค้าหรือบริการประเภทเดียวกันกับความชอบของผู้บริโภคคนนั้น โดยระบบจะไม่แสดงสินค้าหรือบริการอื่น ทั้งนี้เนื่องจากการทำการแสดงข้อมูลตามความชอบของผู้บริโภคทำให้ผู้ประกอบการได้รับความสนใจมากกว่าข้อมูลที่แสดงโดยไม่คำนึงถึงความชอบของผู้บริโภค เช่น เมื่อผู้บริโภคค้นหาและซื้อไม้แบตผ่านอินเตอร์เน็ต ระบบจะทำการจดจำและบันทึกว่าความชอบของผู้บริโภครายนี้คือไม้แบต ภายหลังจากนั้นโฆษณาซึ่งอยู่บนเว็บไซต์ต่างๆที่ผู้บริโภคคนดังกล่าวเข้าชมจะทำการแสดงไม้แบตหลากหลายยี่ห้อรวมถึงส่วนลดเพื่อจูงใจให้ผู้บริโภคคนนั้นทำ

---

[47] Duhigg, G.,“How companies learn your secrets”,Accedssed20 January 2016, http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all&_r=0

การสั่งซื้อ แต่จะไม่ทำการแสดงสินค้าประเภทเสื้อ กางเกง หรือรองเท้ากีฬา ในขณะที่ผู้บริโภคคนดังกล่าวเมื่อได้ทำการซื้อไม้แบตเรียบร้อยแล้วและกำลังมองหารองเท้ากีฬาลดราคาจะไม่มีโอกาสทราบจากโฆษณาเหล่านี้ว่ากำลังมีการลดราคารองเท้ากีฬาอยู่ด้วย

ประการที่ห้า การทำ Profiling อาจเป็นการเปิดเผยตัวตนของเจ้าของข้อมูลส่วนบุคคลให้บุคคลอื่นรู้ กล่าวคือ เนื่องจากการทำ profiling ทำให้สามารถแสดงข้อมูลเกี่ยวกับความสนใจของเจ้าของข้อมูลส่วนบุคคลนั้นจากผู้ให้บริการ เช่น การที่บริษัททำการโฆษณาตามความชอบของผู้บริโภคโดยอาศัยข้อมูลจากการทำ Profiling ซึ่งเมื่อมีผู้เห็นโฆษณานี้ย่อมทำทราบว่าเจ้าของข้อมูลส่วนบุคคลนั้นชอบสินค้าประเภทไหน หรือมีความเปลี่ยนแปลงของผู้บริโภคเช่นไร เช่น พ่อทราบว่าลูกสาวของตนซึ่งยังเป็นวัยรุ่นตั้งครรภ์เนื่องจากได้รับคูปองอาหารเด็กจากร้านค้าในประเทศสหรัฐอเมริกา โดยวัยรุ่นคนนี้ได้ถูกระบบอัตโนมัติจัดเป็นผู้ตั้งครรภ์เนื่องจากสินค้าที่วัยรุ่นคนดังกล่าวซื้อ เนื่องจากระบบตั้งค่าให้สินค้าบางประเภทเมื่อซื้อร่วมกันแล้วแสดงว่าผู้ซื้อมีโอกาสตั้งครรภ์สูงง[48]

2.6.4 ข้อมูลไบโอเมตริก (Biometric)

เนื่องจากข้อมูลไบโอเมตริก (Biometric)เป็นข้อมูลที่มีความสำคัญเพิ่มมากขึ้น นอกจากนี้ยังสามารถทำการเก็บรวบรวมได้ง่ายกล่าวคือ ข้อมูลไบโอเมตริก (Biometric) เป็นข้อมูลเกี่ยวกับชีววิทยาของเจ้าของข้อมูลส่วนบุคคล ติดอยู่กับเจ้าของข้อมูลส่วนบุคคลตลอดเวลาและยากที่เจ้าของข้อมูลส่วนบุคคลจะระมัดระวังมิให้ทิ้งร่องรอยบางประการเกี่ยวกับข้อมูลไบโอเมตริก (Biometric) ของตน เช่นเมื่อเจ้าของข้อมูลส่วนบุคคลจับสิ่งของไม่ว่าจะเป็นเหล็กหรือแก้ว เจ้าของข้อมูลส่วนบุคคลได้ทิ้งร่องรอยลายนิ้วมือของตนเอาไว้บนพื้นผิวของสิ่งของนั้น หรือแม้กระทั่งเวลาเจ้าของข้อมูลส่วนบุคคลเดินผ่านกล้องวีดีโอ กล้องดังกล่าวสามารถจับลักษณะท่าทางการเดินรวมถึงรูปหน้าของเจ้าของข้อมูลส่วนบุคคลได้ หรือในเวลาที่เจ้าของข้อมูลส่วนบุคคลพูดเจ้าของข้อมูลส่วนบุคคลอาจถูกเก็บข้อมูลเสียงของตนได้

จากที่ได้กล่าวมาแสดงให้เห็นว่าข้อมูลไบโอเมตริก (Biometric) เป็นข้อมูลที่สามารถถูกเก็บรวบรวมได้โดยเจ้าขอข้อมูลส่วนบุคคลไม่จำต้องเป็นผู้มอบข้อมูลให้ ส่งผลให้การนำข้อมูลไบโอเมตริก (Biometric) ไปใช้โดยปราศจากความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก็สามารถเกิดขึ้นได้ง่ายเช่นเดียวกัน นอกจากนี้การนำข้อมูลไบโอเมตริก (Biometric) ยังทำให้เจ้าของ

---

[48] Lubin, G.,“The incredible story of how target exposed a teen girl’s pregnancy”,Accedssed20January 2016,http://www.businessinsider.com/the-incredible-story-of-how-target-exposed-a-teen-girls-pregnancy-2012-2

ข้อมูลไบโอเมตริก (Biometric) ถูกตรวจสอบ ควบคุม และจดจำ ที่มากไปกว่านั้นข้อมูลไบโอเมตริก (Biometric)ยังสามารถบอกถึงสิ่งต่างๆเกี่ยวกับเจ้าของข้อมูลส่วนบุคคลได้

ข้อมูลไบโอเมตริก (Biometric) เมื่อทำการเก็บรวบรวมแล้วสามารถที่จะบอกถึงสภาพของเจ้าของข้อมูลส่วนบุคคลได้เป็นอย่างดี สาเหตุมาจากข้อมูลไบโอเมตริก (Biometric) เป็นข้อมูลที่เก็บจากลักษณะ ท่าทาง หรือร่างกายของเจ้าของข้อมูลส่วนบุคคล เมื่อนำข้อมูลนี้ไปประมวลผลแล้วสามารถที่จะแสดงสภาพความเป็นอยู่ อาชีพ บุคลิกหรือโรคประจำตัวได้ ดังนั้นหากมีการเก็บรวบรวมข้อมูลไบโอเมตริก (Biometric) แล้วผู้ควบคุมข้อมูลแอบทำการประมวลผลต่อไปย่อมจะเป็นการละเมิดสิทธิของเจ้าของข้อมูลไบโอเมตริก (Biometric)

บทที่ 3
กฎหมายต่างประเทศที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์

3.1 กฎหมายของประเทศสหรัฐอเมริกา

เนื่องจากในปัจจุบันนี้ประเทศสหรัฐอเมริกายังมิได้มีกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลใช้บังคับเป็นการทั่วไป จึงทำให้การคุ้มครองความเป็นส่วนตัวในประเทศสหรัฐอเมริกาอาศัยรัฐธรรมนูญแห่งประเทศสหรัฐอเมริกา กฎหมายของมลรัฐต่างๆ และกฎหมายว่าด้วยความรับผิดในทางละเมิด ส่งผลให้ผู้เก็บรวบรวมข้อมูลส่วนบุคคลในประเทศสหรัฐอเมริกาหากไม่ตกอยู่ภายใต้บังคับแห่งกฎหมายของมลรัฐที่ตนตั้งอยู่หรือไม่ตกอยู่ภายใต้กฎหมายเฉพาะแล้วย่อมจะไม่ตกอยู่ภายในบังคับใดๆเลย อีกทั้งเจ้าของข้อมูลส่วนบุคคลไม่สามารถใช้สิทธิใดๆเกี่ยวกับข้อมูลส่วนบุคคลของตนได้ เช่น สิทธิในการขอแก้ไขข้อมูลส่วนบุคคล สิทธิในการเข้าถึงข้อมูลส่วนบุคคล หรือสิทธิในการเพิกถอนความยินยอม เป็นต้น โดยเหตุที่ไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลนี้ทำให้ข้อมูลทุกประเภทไม่ว่าจะเป็นข้อมูลส่วนบุคคลธรรมดาหรือข้อมูลประเภทที่มีความอ่อนไหวล้วนสามารถถูกเก็บรวบรวมได้ทั้งนั้น และไม่มีกำหนดเวลาในการเก็บรวบรวมข้อมูลส่วนบุคคล นอกจากนี้ประเทศสหรัฐอเมริกาเองก็ยังมิได้มีองค์กรที่ตั้งขึ้นโดยเฉพาะเพื่อให้มีหน้าที่ดูแลควบคุมเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

อย่างไรก็ตามแม้ประเทศสหรัฐอเมริกายังมิได้มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลออกมาใช้บังคับเป็นการทั่วไป แต่ประเทศสหรัฐอเมริกายังมีกฎหมายเฉพาะซึ่งมีบทบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลแทรกอยู่ด้วยโดยนำมาบังคับใช้แก่องค์กรหรือหน่วยงานที่เกี่ยวข้องเท่านั้น เช่น Health Insurance Portability and Accountability Act of 1996 (HIPAA หรือรู้จักในอีกชื่อหนึ่งว่า Kennedy-Kassebaum Health Insurance Portability and Accountability Act) ซึ่งเป็นกฎหมายเกี่ยวกับการคุ้มครองความเป็นส่วนตัวและความปลอดภัยของข้อมูลด้านสุขภาพทั้งในแบบกระดาษและแบบอิเล็กทรอนิกส์ ซึ่งจะนำมาบังคับใช้แก่องค์กรหรือหน่วยงานด้านสุขภาพเท่านั้น The Financial Services Modernization Act of 1999 (Gramm-Leach-Billey Actหรือ GLB) เป็นกฎหมายที่เกี่ยวกับความปลอดภัยและความเป็นส่วนตัวของข้อมูลทางการเงินส่วนบุคคลซึ่งจะนำมาใช้บังคับแก่สถาบันการเงินเท่านั้น หรือ The Fair Credit Reporting Act เป็นกฎหมายเกี่ยวกับการรายงานข้อมูลเครดิตของผู้บริโภค โดยกฎหมายฉบับนี้จะนำมาบังคับใช้แก่ Consumer Reporting Agencies และบุคคลซึ่งใช้ประโยชน์ในข้อมูลนั้น นอกจากกฎหมายแล้วยังมีแนวปฏิบัติ

(Guidelines) แนวปฏิบัติในการกำกับดูและตนเอง (Self-regulatory guidelines) และกรอบในการกำกับดูแลตนเอง (Self-regulatory framework) ซึ่งก็จะนำมาบังคับใช้แก่เพียงบางหน่วยงานหรือองค์กรเช่นเดียวกัน

สำหรับองค์กรในการกำกับดูแลด้านการคุ้มครองข้อมูลส่วนบุคคลในประเทศสหรัฐอเมริกา สืบเนื่องจากที่ประเทศสหรัฐอเมริกายังมิได้มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลใช้บังคับเป็นการทั่วไป ทำให้ยังไม่มีองค์กรหลักซึ่งมีหน้าที่ในการกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคล แต่จะมีเพียงองค์กรซึ่งมีหน้าที่กำกับดูแลตามกฎหมายเฉพาะ เช่น Department of Health and Human Services มีหน้าที่กำกับดูแลตามกฎหมาย Health Insurance Portability and Accountability Act of 1996 เป็นต้น และยังมีองค์กร Federal Trade Commission (FTC) ซึ่งมีหน้าที่สองประการ ได้แก่ การคุ้มครองผู้บริโภค และการส่งเสริมการแข่งขัน กล่าวคือ ในด้านการคุ้มครองผู้บริโภค FTCทำโดยหยุดการกระทำที่เป็นการเอารัดเอาเปรียบ ฉ้อโกง หรือหลอกลวงในตลาดการค้า FTC มีหน้าที่ในการสืบสวนสอบสวน ดำเนินคดีต่อบริษัทรวมไปถึงบุคคลธรรมดาที่ละเมิดกฎหมาย พัฒนากฎหมายเพื่อให้ตลาดการค้าสามารถดำเนินไปอย่างราบรื่น และให้ความรู้แก่ผู้บริโภคและธุรกิจเกี่ยวกับสิทธิและหน้าที่ของตน และในด้านการส่งเสริมการแข่งขัน FTC มีบทบาทในการทำให้ตลาดในประเทศสหรัฐอเมริกาเป็นไปอย่างเสรีและไม่ปิดกั้นผู้ค้ารายใหม่โดยการออกกฎหมายป้องกันการผูกขาดทางการค้า ซึ่ง FTC ก็ได้ใช้อำนาจของตนเพื่อป้องกันมิให้เกิดการละเมิดความเป็นส่วนตัวของผู้บริโภค โดยเฉพาะอย่างยิ่งในกรณีที่ผู้ค้าให้ข้อมูลที่เป็นการหลอกลวงหรือไม่เป็นธรรมแก่ผู้บริโภค โดยกฎหมายของประเทศสหรัฐอเมริกาที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลในด้านอิเล็กทรอนิกส์ มีดังต่อไปนี้

3.1.1 Privacy Act 1974

เนื่องจากรัฐธรรมนูญของประเทศสหรัฐอเมริกามีบทบัญญัติคุ้มครองความเป็นส่วนตัวของประชาชน โดยเฉพาะอย่างยิ่ง Fourth Amendment ได้รับรองว่าบุคคลมีสิทธิที่จะได้รับความปลอดภัยในร่างกาย เคหสถาน เอกสาร และทรัพย์สินจากการค้น ยึดและจับกุมโดยปราศจากเหตุอันสมควร ซึ่งเคหสถานและทรัพย์สินของบุคคลที่ได้รับความคุ้มครองนั้นรวมไปถึงการสนทนาทางโทรศัพท์ด้วย ในขณะที่การเก็บรวบรวมข้อมูล ใช้ และเปิดเผยส่วนบุคคลโดยองค์กรของรัฐบาลกลับไม่มีข้อจำกัด รัฐบาลได้รวบรวมข้อมูลของประชาชนจำนวนมากมายทั้งข้อมูลทั่วไปและข้อมูลที่มีความอ่อนไหว เช่น ภาษีรายได้ ประกันสังคม หรือข้อมูลที่ได้จากการสำรวจเพื่อทำวิจัย เป็นต้น ซึ่งหากรัฐบาลมีข้อมูลเกี่ยวกับประชาชนมากเท่าไรก็ย่อมก่อให้เกิดผลเสียต่อประชาชนผู้เป็นเจ้าของข้อมูลส่วนบุคคลมากขึ้นเท่านั้น โดยเฉพาะอย่างยิ่งเทคโนโลยีทางคอมพิวเตอร์ที่ถูกนำมาใช้เพื่อการเก็บ

รวบรวมและเปิดเผยข้อมูลส่วนบุคคลย่อมทำให้กระทำได้ง่ายขึ้น ดังนั้น Privacy Act จึงได้ถูกนำมาใช้บังคับเพื่อกำหนดกฎเกณฑ์ควบคุมการเก็บรวบรวม การเก็บรักษา การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลโดยหน่วยงานของรัฐ ซึ่งในบางครั้งถูกเรียกว่า แนวปฏิบัติเกี่ยวกับสารสนเทศที่เป็นธรรม (Code of fair information practices)

บุคคลที่จะได้รับความคุ้มครองตาม Privacy Act ได้แก่ บุคคลซึ่งมีสัญชาติอเมริกัน หรือบุคคลซึ่งมีภูมิลำเนาถาวรถูกต้องตามกฎหมายในประเทศสหรัฐอเมริกา บุคคลอื่นใดนอกจากนี้ไม่สามารถอ้างความคุ้มครองตามพระราชบัญญัติฉบับนี้ได้ โดย Privacy Act จะกำหนดหลักเกณฑ์เกี่ยวกับการรักษา การเก็บรวบรวม การใช้ หรือการเผยแพร่ข้อมูลส่วนบุคคล นำมาบังคับใช้แก่หน่วยงานของรัฐ คือ หน่วยงานด้านการบริหาร หน่วยงานทางทหาร รัฐวิสาหกิจ บริษัทที่รัฐบาลมีอำนาจในควบคุม เช่น U.S. Postal Service พระราชบัญญัตินี้ให้ความหมายของข้อมูลส่วนบุคคลไว้ใน 5 U.S.C.§ 552a(a)(4)[1]ว่า “บันทึก” หมายถึง สิ่งใดๆ ชุดหรือกลุ่มของข้อมูลเกี่ยวกับบุคคลซึ่งการเก็บรวบรวม การเก็บรักษา ใช้ หรือเปิดเผยโดยหน่วยงานของรัฐ ซึ่งให้รวมไปถึงการศึกษา ธุรกรรมการเงิน ประวัติการรักษาพยาบาล ประวัติอาชญากรรม ประวัติการทำงาน ซึ่งมีชื่อของบุคคลนั้น หรือเลขบัตรประจำตัวประชาชน สัญลักษณ์หรือสิ่งอื่นใดที่สามารถระบุตัวบุคคลนั้นได้ เช่น ลายพิมพ์นิ้วมือ หรือลายพิมพ์เสียง หรือรูปภาพ และ ใน 5 U.S.C.§ 552a(a)(5)[2] กำหนดให้ “ระบบการบันทึก” หมายถึง กลุ่มของการบันทึกซึ่งควบคุมโดยหน่วยงานของรัฐโดยข้อมูลนั้นเรียกคืนด้วยชื่อของบุคคลนั้น หรือด้วยเลขบัตรประชาชน สัญลักษณ์ หรือสิ่งอื่นที่ระบุถึงตัวบุคคลนั้น

---

[1] **5 U.S.C. § 552a(a)** For purposes of this section

(4) the term “record” means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph

[2] **5 U.S.C.§ 552a(a)** For purposes of this section

(5) the term “system of records” means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual

การเก็บรวบรวมข้อมูลส่วนบุคคลภายใต้ Privacy Act หน่วยงานของรัฐจะต้องได้รับข้อมูลนั้นมาจากบุคคลผู้เกี่ยวข้องโดยตรง โดยต้องแจ้งกฎหมายหรือคำสั่งที่ให้อำนาจแก่หน่วยงานรัฐในการเก็บรวบรวมข้อมูล แจ้งให้ทราบถึงลักษณะของข้อมูล ต้องระบุว่าข้อมูลนั้นจะถูกนำไปใช้เพื่อวัตถุประสงค์ใด หน่วยงานของรัฐต้องเก็บข้อมูลเพียงเท่าที่จำเป็นและเกี่ยวข้องกับวัตถุประสงค์ และหากข้อมูลนั้นอาจก่อให้เกิดผลเสียแก่เจ้าของข้อมูลส่วนบุคคล เช่น กระทบต่อสิทธิหรือประโยชน์ของเจ้าของข้อมูลส่วนบุคคล หน่วยงานของรัฐต้องพยายามเก็บรวบรวมข้อมูลนั้นจากเจ้าของข้อมูลโดยตรง

Privacy Act กำหนดให้หน่วยงานของรัฐที่มีหน้าที่ดูแลระบบการบันทึกต้องยินยอมให้เจ้าของข้อมูลส่วนบุคคลเข้าถึงข้อมูลส่วนบุคคลของตน โดยเจ้าของข้อมูลส่วนบุคคลสามารถที่จะตรวจสอบความถูกต้องและขอสำเนาข้อมูลส่วนบุคคลของตนได้ หากพบว่าข้อมูลของตนไม่ถูกต้องสามารถที่จะขอแก้ไขข้อมูลนั้นได้ เมื่อมีคำขอแก้ไขข้อมูลส่วนบุคคลแล้วหน่วยงานของรัฐจะต้องพิจารณาและตอบรับคำขอของเจ้าของข้อมูลส่วนบุคคลภายใน 10 วันทำการ หากหน่วยงานของรัฐปฏิเสธคำขอ หน่วยงานของรัฐต้องแจ้งเหตุผลในการปฏิเสธ และแจ้งหน่วยงานที่เจ้าของข้อมูลส่วนบุคคลสามารถอุทธรณ์คำสั่งได้

ในกรณีของการเปิดเผยข้อมูลส่วนบุคคล Privacy Act ห้ามมิให้หน่วยงานของรัฐที่มีข้อมูลส่วนบุคคลเปิดเผยข้อมูลส่วนบุคคลนั้น เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือเป็นการเปิดเผยตามที่ Privacy Act บัญญัติยกเว้นไว้ซึ่งมีจำนวน 12 กรณี เช่น เป็นการเปิดเผยตาม Freedom of Information Act เป็นการเปิดเผยแก่บุคคลซึ่งได้แจ้งแก่หน่วยงานของรัฐล่วงหน้าว่าบันทึกนั้นจะถูกใช้เพื่อการศึกษาทางสถิติหรือรายงานและบันทึกนั้นจะถูกโอนถ่ายโดยปราศจากข้อมูลที่สามารถระบุตัวเจ้าของข้อมูลส่วนบุคคลได้ เป็นการเปิดเผยแก่หน่วยงานของรัฐภายใต้อำนาจของรัฐบาลใดๆซึ่งอยู่ภายใต้การควบคุมของประเทศสหรัฐอเมริกาเพื่อการบังคับตามกฎหมายแพ่งหรืออาญาและโดยมีคำขอเป็นหนังสือจากหัวหน้าของหน่วยงานนั้น หรือเป็นการเปิดเผยภายใต้สถานการณ์จำเป็นที่กระทบต่อสุขภาพหรือความปลอดภัยของบุคคลใดและบุคคลซึ่งได้รับผลกระทบต่อสุขภาพหรือความปลอดภัย เป็นต้น

เมื่อมีการเปิดเผยข้อมูลส่วนบุคคลแล้ว หน่วยงานของรัฐต้องทำรายงานข้อมูลเกี่ยวกับวันเวลา บุคคลที่ได้รับการเปิดเผยข้อมูล ข้อมูลเกี่ยวกับการติดต่อบุคคลหรือองค์กรที่ได้รับข้อมูลส่วนบุคคลนั้น โดยจะต้องเก็บรายงานดังกล่าวไว้เป็นเวลา 5 ปี หรือตลอดอายุของบันทึกระยะเวลาใดยาวกว่าให้ถือระยะเวลานั้น ซึ่งหากเจ้าของข้อมูลส่วนบุคคลร้องขอหน่วยงานของรัฐต้องเปิดเผยรายงานนี้แก่เจ้าของข้อมูลส่วนบุคคลเว้นแต่เป็นการเปิดเผยเพื่อการบังคับตามกฎหมาย

3.1.2 The Computer Fraud and Abuse Act 1986

The Computer Fraud and Abuse Act หรือ CFAA เป็นบัญญัติอยู่ใน 18 U.S. Code § 1030 ตราขึ้นโดยสภาคองเกรสในปี ค.ศ. 1986กล่าวถึงการกระทำความผิดต่อคอมพิวเตอร์ มีวัตถุประสงค์เพื่อป้องกันบุคคลหรือองค์กรของรัฐจากการบุกรุกคอมพิวเตอร์ การคุกคามทางคอมพิวเตอร์ การก่อความเสียหาย การจารกรรม หรือการนำคอมพิวเตอร์ไปใช้เพื่อการฉ้อโกง เช่น 18 U.S. Code § 1030 (a)(3)[3] กำหนดให้การตั้งใจเข้าถึงคอมพิวเตอร์ของหน่วยงานของรัฐบาลซึ่งมิได้มีไว้เพื่อสาธารณะโดยไม่ได้รับอนุญาต หรือเข้าถึงคอมพิวเตอร์ของหน่วยงานรัฐบาลซึ่งมีไว้เพื่อรัฐบาลของประเทศสหรัฐอเมริกาเท่านั้น หรือในกรณีที่คอมพิวเตอร์นั้นมิได้มีไว้เพื่อรัฐบาลของประเทศสหรัฐอเมริกาเท่านั้นแต่ได้ถูกนำมาใช้โดยหรือใช้เพื่อรัฐบาลของประเทศสหรัฐอเมริกา และการเข้าถึงนั้นส่งผลต่อการใช้คอมพิวเตอร์โดยหรือใช้เพื่อรัฐบาลของประเทศสหรัฐอเมริกาเป็นความผิด ผู้กระทำการดังกล่าวต้องรับโทษตามที่กำหนดไว้ในพระราชบัญญัตินี้ เป็นต้น FCAA นี้ให้ความคุ้มครองทั้งคอมพิวเตอร์ของบุคคลธรรมดาและคอมพิวเตอร์ของรัฐบาลซึ่งรัฐบาลมีประโยชน์ได้เสียอยู่ด้วย อาทิ คอมพิวเตอร์ที่ใช้โดยองค์กรของรัฐบาล คอมพิวเตอร์ซึ่งใช้โดยสถาบันการเงิน และเป็นคอมพิวเตอร์ที่ใช้โดยหรือใช้เพื่อสถาบันการเงินหรือรัฐบาล

18 U.S. Code § 1030 (e) ได้กำหนดความหมายของคำต่างๆไว้ซึ่งในที่นี้จะนำมาพิจารณาเพียงบางประการ ได้แก่

“คอมพิวเตอร์” หมายถึง อุปกรณ์อิเล็กทรอนิกส์ อุปกรณ์ทางแม่เหล็ก อุปกรณ์ทางสายตา หรืออุปกรณ์ความเร็วสูงซึ่งใช้ในการประมวลผลทางตรรกะ คณิตศาสตร์ หรือเก็บรวบรวมข้อมูล รวมไปถึงสิ่งซึ่งอำนวยความสะดวกในการเก็บข้อมูลหรือสิ่งอำนวยความสะดวกทางการสื่อสารซึ่งเกี่ยวข้องโดยตรงหรือทำงานร่วมกับอุปกรณ์ดังกล่าว แต่คอมพิวเตอร์ไม่ให้รวมถึงเครื่องพิมพ์ดีดอัตโนมัติหรือเครื่องเรียงพิมพ์ เครื่องคิดเลขพกพาขนาดเล็ก หรืออุปกรณ์อื่นซึ่งมีลักษณ์เดียวกัน

“คอมพิวเตอร์ที่มีมาตรการป้องกัน” หมายถึง คอมพิวเตอร์ซึ่ง

---

[3] **18 U.S. Code § 1030 (a)** Whoever

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(1) ใช้เฉพาะเพื่อสถาบันการเงินหรือรัฐบาลแห่งประเทศสหรัฐอเมริกา หรือในกรณีที่คอมพิวเตอร์นั้นมิได้ใช้เฉพาะเพื่อสถาบันการเงินหรือรัฐบาลแห่งประเทศสหรัฐอเมริกาแต่คอมพิวเตอร์นั้นถูกใช้โดยหรือใช้เพื่อสถาบันการเงินหรือรัฐบาลแห่งประเทศสหรัฐอเมริกา และการกระทำความผิดนั้นส่งผลกระทบต่อการใช้คอมพิวเตอร์โดยหรือใช้เพื่อสถาบันการเงินหรือรัฐบาลแห่งประเทศสหรัฐอเมริกา

(2) ซึ่งถูกใช้ในหรือเกี่ยวข้องกับการค้าระหว่างมลรัฐหรือระหว่างประเทศ หรือการติดต่อสื่อสาร รวมถึงคอมพิวเตอร์ซึ่งตั้งอยู่นอกประเทศสหรัฐอเมริกาซึ่งถูกใช้ในลักษณะที่กระทบต่อต่อการค้าระหว่างมลรัฐหรือการค้าระหว่างประเทศหรือการติดต่อสื่อสารในประเทศสหรัฐอเมริกา

“เกินกว่าที่ได้รับอนุญาต” หมายถึง เข้าถึงคอมพิวเตอร์โดยได้รับอนุญาตและอาศัยการเข้าถึงนั้นเพื่อให้ได้มาหรือเปลี่ยนแปลงข้อมูลเกี่ยวกับคอมพิวเตอร์ โดยผู้เข้าถึงไม่มีสิทธิในการได้มาหรือการเปลี่ยนแปลงนั้น

“บุคคล” หมายถึง บุคคลธรรมดา บริษัท นิติบุคคล สถาบันทางการศึกษา สถาบันการเงิน หน่วยงานรัฐบาล หรือหน่วยงานทางกฎหมายหรือหน่วยงานอื่น

บทบัญญัติซึ่งเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลตาม FCAA มีดังต่อไปนี้

18 U.S. Code § 1030 (a)(2)(C)[4] กำหนดให้บุคคลซึ่งเจตนาเข้าถึงคอมพิวเตอร์โดยไม่ได้รับอนุญาตหรือเกินกว่าที่ได้รับอนุญาตและได้รับไปซึ่งข้อมูลจากคอมพิวเตอร์ที่มีมาตรการป้องกัน โดยข้อมูลตาม 18 U.S. Code § 1030 (a)(2)(C) นี้หมายรวมถึงข้อมูลซึ่งเก็บโดยไม่มีรูปร่าง เช่น ข้อมูลอิเล็กทรอนิกส์ วัตถุประสงค์ของมาตรานี้คือเพื่อป้องกันการจารกรรมข้อมูลระหว่างมลรัฐหรือระหว่างประเทศโดยอาศัยคอมพิวเตอร์ เพื่อให้เกิดความมั่นใจว่าการจารกรรมข้อมูลที่อยู่ในรูปแบบอิเล็กทรอนิกส์ซึ่งไม่มีตัวตนจะได้รับความคุ้มครองเช่นเดียวกันกับการขโมยทรัพย์ซึ่งมีรูปร่าง การกระทำความผิดทั้งสองกรณีดังที่กล่าวมามีโทษตาม 18 U.S. Code § 1030 (c) ซึ่งผู้กระทำความผิดอาจต้องโทษปรับหรือจำคุก หรือทั้งจำและปรับ

18 U.S. Code § 1030 (a)(5)[5] กำหนดให้บุคคลใด 1. โดยเจตนาก่อให้เกิดการส่งโปรแกรม ข้อมูล รหัส หรือคำสั่ง และการกระทำนั้นเจตนาให้เกิดผลเสียหายโดยไม่รับอนุญาตแก่

---

[4] **U.S. Code § 1030** (a) whoever-

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains–

(C) information from any protected computer;

[5] **18 U.S. Code § 1030** (a) whoever –

คอมพิวเตอร์ซึ่งมีมาตรการป้องกัน2. ตั้งใจเข้าถึงคอมพิวเตอร์ที่มีมาตรการป้องกันโดยไม่ได้รับอนุญาต และด้วยความประมาทส่งผลให้เกิดความเสียหายจากการกระทำนั้น 3. ตั้งใจเข้าถึงคอมพิวเตอร์ที่มีมาตรการป้องกันโดยไม่ได้รับอนุญาต และก่อให้เกิดความเสียหายหรือสูญหายจากการกระทำนั้นซึ่งผู้กระทำความผิดอาจต้องโทษปรับหรือจำคุก หรือทั้งจำและปรับ

นอกจากการกระทำความผิดตามพระราชบัญญัตินี้จะนำผู้กระทำความผิดไปสู่โทษทัณฑ์ทางอาญาแล้ว ผู้กระทำความผิดอาจต้องรับผิดในทางแพ่งด้วยเช่นเดียวกัน โดย 18 U.S. Code § 1030 (g) แห่ง FCAA เปิดโอกาสให้ผู้ที่ได้รับความเสียหายหรือสูญหายจากการกระทำความผิดตามพระราชบัญญัตินี้คงไว้ซึ่งสิทธิในการฟ้องร้องทางแพ่งเพื่อความเสียหายที่เกิดขึ้น การชดเชย การคุ้มครองชั่วคราว หรือการบรรเทาทุกข์อื่นๆ

3.1.3 Electronic Communications Privacy Act 1986

Electronic Communications Privacy Act (ECPA) หรือที่รู้จักกันในชื่อ Wiretap Actใช้บังคับในปี ค.ศ. 1986 บัญญัติไว้ใน 18 U.S. Code §2510-2522 กฎหมายฉบับดังกล่ามีวัตถุประสงค์ในการห้ามการดักฟังทางโทรศัพท์รวมไปถึงการดักรับข้อมูลที่ส่งโดยทางอิเล็กทรอนิกส์ผ่านทางคอมพิวเตอร์ ECPA ถูกนำมาใช้เพื่อเป็นการแก้ไข Omnibus Crime Control and Safe Streets Act of 1986 โดยกฎหมาย Wiretap ฉบับแรกได้มีขึ้นเพื่อป้องกันการเปิดเผยความลับของรัฐบาลในระหว่างสงครามโลกครั้งที่ 1 ในปัจจุบัน ECPA มีบทบัญญัติเกี่ยวกับการเข้าถึง การเปิดเผย การดักจับ และคุ้มครองความเป็นส่วนตัวในการสื่อสารผ่านทางสื่ออิเล็กทรอนิกส์ กฎหมายฉบับนี้ครอบคลุมบุคคลหลายประเภท อาทิ หน่วยงานของรัฐ ลูกจ้าง บุคคลธรรมดา บริษัท หุ้นส่วน หรือทรัสต์ เป็นต้น โดย ECPA ได้ให้นิยามของคำต่างๆไว้ใน 18 U.S. Code §2510 มีรายละเอียดที่น่าสนใจ ดังนี้

---

(5)

(A) knowingly causes the transmission of a program, information, code or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

“การดักจับ” หมายถึง การฟังหรือการได้รับมาโดยวิธีอื่นซึ่งเนื้อหาของการสื่อสารผ่านทางสาย อิเล็กทรอนิกส์หรือการพูดคุย โดยใช้อุปกรณ์ทางอิเล็กทรอนิกส์ เครื่องมือหรืออุปกรณ์อื่นใด

“บุคคล” หมายถึง ลูกจ้าง หรือหน่วยงานของรัฐ หรือหน่วยงานย่อยของรัฐหรือหน่วยงานย่อยทางการเมือง และรวมถึงบุคคลธรรมดา หุ้นส่วน สมาคม บริษัทร่วมทุน ทรัสต์ หรือบริษัท

“เนื้อหา” เมื่อใช้ร่วมกับคำว่าสาย การพูดคุย หรือการสื่อสารทางอิเล็กทรอนิกส์ให้รวมถึงข้อมูลใดๆเกี่ยวกับสาระสำคัญ ข้อความหรือความหมายของการสื่อสาร

“การติดต่อสื่อสารทางอิเล็กทรอนิกส์” หมายถึง การส่งสัญลักษณ์ สัญญา หนังสือ รูปภาพ เสียง ข้อมูล หรือข่าวกรองซึ่งถูกส่งทั้งหมดหรือบางส่วนผ่านทางสาย วิทยุ แม่เหล็กไฟฟ้า Photoelectronic หรือ ระบบ Photooptical ซึ่งส่งผลต่อการค้าระหว่างประเทศหรือระหว่างมลรัฐ แต่ไม่รวมถึง

1. การสื่อสารใดๆผ่านทางสายหรือผ่านทางการพูดคุย
2. การสื่อสารใดๆซึ่งกระทำผ่านทางอุปกรณ์เสียงเพียงอย่างเดียว
3. การสื่อสารใดๆจากอุปกรณ์ในการติดตาม
4. ข้อมูลการโอนเงินผ่านระบบอิเล็กทรอนิกส์ซึ่งเก็บรวบรวมโดยสถาบันการเงินในระบบการสื่อสารซึ่งใช้เพื่อการเก็บรวบรวมทางอิเล็กทรอนิกส์และการโอนเงิน

“ระบบการสื่อสารทางอิเล็กทรอนิกส์” หมายถึง อุปกรณ์เกี่ยวกับสาย วิทยุ แม่เหล็กไฟฟ้า Photooptical หรือ Photoelectronic ซึ่งใช้เพื่อการส่งผ่านการสื่อสารทางสาย หรืออิเล็กทรอนิกส์ และอุปกรณ์เกี่ยวกับคอมพิวเตอร์หรือเกี่ยวกับอุปกรณ์ทางอิเล็กทรอนิกส์ซึ่งใช้เพื่อการเก็บรวบรวมข้อมูลการสื่อสารทางอิเล็กทรอนิกส์

“ผู้บุกรุกคอมพิวเตอร์” หมายถึง

1. หมายถึงบุคคลซึ่งเข้าถึงคอมพิวเตอร์ที่มีมาตรการป้องกันโดยมิได้รับอนุญาตและปราศจากเหตุอันสมควรที่จะคาดหมายถึงสิทธิในความเป็นส่วนตัวโดยชอบด้วยกฎหมายในการสื่อสารที่ส่งจากหรือผ่านคอมพิวเตอร์ที่มีระบบป้องกันนั้น

2. แต่ไม่หมายรวมถึงบุคคลซึ่งผู้ให้บริการหรือเจ้าของคอมพิวเตอร์ได้ทราบอยู่แล้วว่ามีสัญญากับผู้ให้บริการหรือเจ้าของคอมพิวเตอร์ในการเข้าถึงทั้งหมดหรือบางส่วนของคอมพิวเตอร์ที่มีมาตรการป้องกัน

ECPA มีบทบัญญัติเกี่ยวกับการคุ้มครองการดักจับและการเปิดเผยการสื่อสารผ่านทางสาย การพูดคุย และอิเล็กทรอนิกส์ใน 18 U.S. Code §2511 กำหนดให้การกระทำดังต่อไปนี้เป็นความผิด

1. บุคคลซึ่งเจตนาดักจับ หรือพยายามดักจับ หรือจัดหาบุคคลเพื่อการดักจับหรือพยายามดักจับการสื่อสารผ่านทางสาย การพูดคุย หรือผ่านทางอิเล็กทรอนิกส์

2. บุคคลซึ่งเจตนาใช้ หรือพยายามใช้ หรือจัดหาบุคคลอื่นใดเพื่อใช้หรือพยายามใช้อุปกรณ์ทางอิเล็กทรอนิกส์ เครื่องมือ หรืออุปกรณ์อื่นเพื่อดักจับการสื่อสาร หาก

2.1 อุปกรณ์นั้นติดต่อหรือส่งสัญญาผ่านทางสาย สายเคเบิล หรือการเชื่อมต่ออื่นซึ่งมีลักษณะเดียวกันซึ่งใช้ในการสื่อสารทางสายหรือ

2.2 อุปกรณ์นั้นส่งการสื่อสารผ่านทางวิทยุ หรือรบกวนการส่งการสื่อสารนั้นหรือ

2.3 บุคคลนั้นรู้ หรือมีเหตุผลอันควรรู้ได้ว่าอุปกรณ์นั้นหรือส่วนประกอบของอุปกรณ์นั้นถูกส่งโดยพัสดุหรือถูกขนส่งในการค้าระหว่างประเทศหรือระหว่างมลรัฐ

2.4 การใช้หรือการพยายามใช้นั้น 1. เกิดขึ้นโดยอาจส่งผลกระทบต่อการค้าระหว่างรัฐหรือระหว่างมลรัฐ หรือ 2. ได้รับหรือมีวัตถุประสงค์เพื่อให้ได้รับข้อมูลเกี่ยวกับการดำเนินงานของธุรกิจหรือห้างร้างอื่นซึ่งอาจส่งผลกระทบต่อการค้าระหว่างรัฐหรือระหว่างมลรัฐหรือ

2.5 บุคคลดังกล่าวรวมถึงบุคคลที่ได้กระทำในโคลอมเบีย เปอร์โตริโก หรือดินแดนหรือดินแดนซึ่งอยู่สมบัติของประเทศสหรัฐอเมริกา

3. ตั้งใจเปิดเผย หรือพยายามเปิดเผยแก่บุคคลอื่นซึ่งเนื้อหาเกี่ยวกับการสื่อสารทางสาย ทางการพูดคุย หรือทางอิเล็กทรอนิกส์ โดยรู้หรือมีเหตุอันควรรู้ว่าการสื่อสารนั้นได้มาจากการดักจับผ่านทางสาย การพูดคุย หรือทางอิเล็กทรอนิกส์

4. เจตนาใช้หรือพยายามใช้เนื้อหาการสื่อสารทางสาย ทางการพูดคุย หรืออิเล็กทรอนิกส์ โดยรู้หรือมีเหตุอันควรรู้ว่าการสื่อสารนั้นได้รับจากการดักจับผ่านทางสาย การพูดคุย หรือทางอิเล็กทรอนิกส์

5. เจตนาเปิดเผย หรือพยายามเปิดเผยแก่บุคคลใดๆซึ่งเนื้อหาของการสื่อสารทางสาย การพูดคุย หรืออิเล็กทรอนิกส์ซึ่งได้มาโดยวิธีการที่ไม่ชอบ

3.1.4 Consumer Privacy Bill of Right 2015

ร่างกฎหมาย Consumer Privacy Bill of Right ถูกเสนอครั้งแรกในปี ค.ศ. 2012 โดยรัฐบาลบารัค โอบามา และได้ถูกนำเสนอใหม่อีกครั้งหนึ่งในวันที่ 27 กุมภาพันธ์ ค.ศ. 2015

โดยบารัค โอบามา ซึ่ง Consumer Privacy Bill of Right นี้จะเป็นกฎหมายควบคู่ไปกันกับ Data Security and Breach Notification Act of 2015 ที่มีบทบัญญัติกำหนดให้องค์กรต้องเปิดเผยเมื่อมีการละเมิดข้อมูลส่วนบุคคลในทันทีเพื่อบรรเทาความเสียหายที่จะเกิดขึ้น โดย Consumer Privacy Bill of Right มีบทบัญญัติควบคุมการเก็บรวบรวมและการเปิดเผยข้อมูลของผู้บริโภค ให้สิทธิแก่ผู้บริโภคในการควบคุมข้อมูลส่วนบุคคลของตนเอง ในขณะเดียวกันก็กำหนดหน้าที่และความรับผิดชอบแก่บริษัทหรือผู้ค้าซึ่งเป็นผู้เก็บรวบรวมข้อมูลส่วนบุคคลให้มีความชัดเจน

ภายใต้ Consumer Bill of Right ข้อมูลส่วนบุคคล หมายถึง ข้อมูลใดๆรวมถึงกลุ่มของข้อมูลซึ่งเชื่อมโยงไปยังบุคคลใดบุคคลหนึ่ง และรวมถึงข้อมูลเกี่ยวกับคอมพิวเตอร์หรืออุปกรณ์ในลักษณะอื่น หลักการสำคัญของกฎหมายฉบับดังกล่าวประกอบด้วยหลัก 7 ประการ กล่าวคือ

1. หลักการควบคุมข้อมูลส่วนบุคคลของเจ้าของข้อมูล

ผู้บริโภคซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิในการควบคุมข้อมูลของตนซึ่งบริษัทได้เก็บรวบรวมจากผู้บริโภค บริษัทต้องมีการควบคุมที่เหมาะสมต่อข้อมูลส่วนบุคคลที่ผู้บริโภคแบ่งปันแก่บุคคลอื่นและมีการควบคุมการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยบริษัทต้องจัดเตรียมวิธีการให้ผู้บริโภคสามารถเข้าถึงข้อมูลส่วนบุคคลของตนเองได้โดยง่าย และต้องมีการแจ้งผู้บริโภคถึงวิธีการที่เข้าถึงและสามารถใช้สิทธิได้ง่ายเพื่อการเพิกถอนหรือจำกัดความยินยอม

2. หลักความโปร่งใส

กำหนดให้บริษัทจะต้องจัดให้มีการแจ้งอย่างชัดเจนถึงข้อมูลที่ทำการเก็บรวบรวม เหตุผลที่ทำการเก็บรวบรวม การนำข้อมูลส่วนบุคคลไปใช้ เวลาที่จะทำลายข้อมูลนั้นหรือทำให้ข้อมูลนั้นไม่สามารถเชื่อมโยงไปยังผู้บริโภคผู้เป็นเจ้าของข้อมูลได้ และบริษัทเปิดเผยหรือจะเปิดเผยข้อมูลนั้นแก่บุคคลอื่นหรือไม่พร้อมด้วยวัตถุประสงค์ในการเปิดเผยข้อมูลส่วนบุคคล

3. หลักเคารพต่อบริบท

เว้นแต่กฎหมายจะบัญญัติไว้เป็นอย่างอื่นบริษัทจะต้องจำกัดการใช้งานและการเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ที่สอดคล้องกับทั้งความสัมพันธ์ที่บริษัทมีต่อผู้บริโภคและบริบทที่ผู้บริโภคยินยอมเปิดเผยข้อมูลส่วนบุคคลแก่บริษัท หากภายหลังการเก็บรวบรวมข้อมูลส่วนบุคคล บริษัทต้องการใช้หรือเปิดเผยข้อมูลส่วนบุคคลในลักษณะที่ขัดกับบริบทที่ข้อมูลนั้นถูกเก็บรวบรวม บริษัทต้องจัดให้มีมาตรการเกี่ยวกับความโปร่งและให้สิทธิแก่ผู้บริโภคในการตัดสินใจ บริษัทต้องปฏิบัติหน้าที่ภายใต้หลักการนี้โดยคำนึงถึงอายุและวิสัยของบุคคลนั้น ซึ่งเด็กและวัยรุ่นอาจได้รับความคุ้มครองมากขึ้น

4. หลักความปลอดภัย

บริษัทจะต้องประเมินความเสี่ยงในความเป็นส่วนตัวและความปลอดภัยของแนวปฏิบัติเกี่ยวกับข้อมูลส่วนบุคคลของตน และคงไว้ซึ่งการป้องกันที่เหมาะสมเพื่อที่จะควบคุมความเสี่ยง เช่น การสูญหาย การเข้าถึงโดยไม่ได้รับอนุญาต การใช้ การทำลาย หรือการเปลี่ยนแปลง หรือการเปิดเผยที่ไม่ถูกต้อง

5. หลักการเข้าถึงและความถูกต้อง

บริษัทต้องใช้มาตรการที่เหมาะสมเพื่อคงไว้ซึ่งความถูกต้องของข้อมูลส่วนบุคคล บริษัทต้องให้สิทธิแก่ผู้บริโภคในการเข้าถึงข้อมูลส่วนบุคคลของผู้บริโภคที่บริษัทได้เก็บหรือรักษาไว้ และมีวิธีการที่เหมาะสมเพื่อให้แก้ไขข้อมูลที่ผิดพลาดหรือขอให้ลบข้อมูลหรือใช้สิทธิในการจำกัดการใช้ข้อมูลส่วนบุคคลของผู้บริโภค

6. หลักคำนึงถึงการเก็บรวบรวม

บริษัทต้องเก็บรวบรวมข้อมูลส่วนบุคคลได้เพียงเท่าที่จำเป็นเพื่อบรรลุวัตถุประสงค์ตามที่ระบุไว้ในหลักเคารพต่อบริบท บริษัทต้องทำลายหรือทำให้ข้อมูลส่วนบุคคลนั้นไม่สามารถสืบกลับไปยังผู้เป็นเจ้าของข้อมูลส่วนบุคคลได้เมื่อข้อมูลนั้นไม่จำเป็นอีกต่อไป เว้นแต่มีกฎหมายกำหนดไว้เป็นอย่างอื่น

7. หลักความเชื่อถือได้

บริษัทมีหน้าที่ต้องปฏิบัติตามหลักการที่ 1 – 6 ทั้งให้พนักงานปฏิบัติตามหลักการดังกล่าวด้วย โดยต้องจัดอบรมพนักงานตามที่เหมาะสมเพื่อให้สามารถปฏิบัติตามหลักการคุ้มครองข้อมูลส่วนบุคคลดังกล่าวได้ และหากบริษัทได้เปิดเผยข้อมูลส่วนบุคคลแก่บุคคลอื่น บริษัทต้องดำเนินการเพื่อให้มั่นใจว่าผู้รับข้อมูลส่วนบุคคลนั้นได้ปฏิบัติตามหลักการทั้งหมดที่กล่าวมาได้ เว้นแต่มีกฎหมายบัญญัติไว้เป็นอย่างอื่น

หลักการทั้งหมดของ Comsumer Privacy Bill of Right ดังที่กล่าวมา มีความสอดคล้องกับหลักการของ OECD และหลักการของ APEC นอกจากนี้ Consumer Privacy Bill of Right ยังเปิดโอกาสให้บริษัทสามารถกำหนดแนวปฏิบัติของตนเองได้ทั้งนี้แนวปฏิบัติดังกล่าวต้องได้รับความเห็นชอบจาก FTC ด้วย

3.1.5 Do Not Track Online Bill 2015

จุดเริ่มต้นของร่างกฎหมายฉบับดังกล่าวเริ่มขึ้นในวันที่ 1 ธันวาคม ค.ศ. 2010 โดย FTC ได้ออกรายงานเกี่ยวกับสิทธิของผู้บริโภคที่จะปกป้องตนเองจากเว็บไซต์ซึ่งทำการติดตามพฤติกรรมของผู้บริโภค โดย FTC พิจารณาว่าในปัจจุบันมีการละเมิดความเป็นส่วนตัวของผู้บริโภค

โดยการเก็บรวบรวมข้อมูลส่วนบุคคล ต่อมาในปี ค.ศ. 2011 มีการเสนอร่างพระราชบัญญัติโดยหากมีผลใช้บังคับจะชื่อว่า The Do Not Track Me Online Act of 2011 เป็นร่างกฎหมายมีเนื้อหาให้อำนาจแก่ FTC ในการกำหนดมาตรฐานการนำวิธี Opt-Out มาใช้เพื่อให้ผู้บริโภคสามารถปฏิเสธไม่ให้ผู้ประกอบธุรกิจทำการเก็บรวบรวมข้อมูลส่วนบุคคลของตน และกำหนดให้ผู้ประกอบธุรกิจต้องปฏิบัติตามหลักเกณฑ์เกี่ยวกับการให้อำนาจแก่ผู้บริโภคในการตัดสินใจเกี่ยวกับการเก็บรวบรวมหรือการใช้ข้อมูลของตน ซึ่งร่างพระราชบัญญัติ Do Not Track Online 2011 นี้ถูกเปรียบเทียบว่าเป็นเวอร์ชั่นหนึ่งของกฎหมาย Do Not Calls ซึ่งห้ามผู้ประกอบการทำการตลาดทางโทรศัพท์หากผู้บริโภคไม่ประสงค์จะรับข่าวสารเกี่ยวกับโฆษณาผ่านทางโทรศัพท์ เพียงแต่ Do Not Track Online 2011 นำมาใช้ในทางออนไลน์ในขณะที่ Do Not Calls ใช้กับโทรศัพท์เท่านั้น นอกจากการให้สิทธิแก่ผู้บริโภคในการตัดสินใจเกี่ยวกับการใช้หรือการเก็บรวบรวมข้อมูลส่วนบุคคลแล้ว Do Not Track Online 2011 ยังกำหนดหน้าที่ให้ผู้ประกอบการต้องเปิดเผยข้อมูลส่วนบุคคลที่ตนเก็บรวบรวมไว้แก่ผู้บริโภคและเปิดเผยบุคคลที่ข้อมูลนั้นได้ถูกโอนไป ต่อมาจึงมีการเสนอร่างพระราชบัญญัติ Do Not Track Online 2015

Do Not Track Online 2015 ถูกเสนอเข้าสู่สภาคองเกสเมื่อวันที่ 15 ธันวาคม ค.ศ. 2015 โดยสมาชิกวุฒิสภา Richard Blumenthal วัตถุประสงค์คือควบคุมการเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลที่ได้รับจากการติดตามกิจกรรมอนไลน์ ซึ่งตาม Section 2(d)[6]กำหนดให้ข้อมูลส่วนบุคคลหมายรวมถึงตัวบ่งชี้ถาวร (Persistent Identifiers) เช่น Internet Protocol Address (IP Address) Media Access Contorl (MAC Address) หรือตัวบ่งชี้ซึ่งมีลักษณะเฉพาะอื่นโดยให้ FTC ออกหลักเกณฑ์เพื่อใช้ในการกำกับดูแลภายใน 1 ปีนับแต่วันที่ร่างพระราชบัญญัติดังกล่าวมีผลใช้บังคับ

โดยกฎเกณฑ์ที่ FTC กำหนดนี้ต้องให้บุคคลธรรมดาสามารถใช้สิทธิแสดงเจตนาได้ง่ายว่าต้องการให้ข้อมูลส่วนบุคคลของตนถูกเก็บรวบรวมโดยผู้ให้บริการทางออนไลน์ รวมถึงผู้ให้บริการทางโทรศัพท์เคลื่อนที่ และกฎเกณฑ์ดังกล่าวต้องกำหนดห้ามมิให้ผู้ให้บริการปฏิเสธไม่

---

[6] **Do Not Track Online Bill 2015**

Section 2

(c) PERSONAL INFORMATION. – In this section, the term “personal information” includes persistent identifiers such as Internet Protocol (IP) address, media access control (MAC) address, and other unique device identifiers.

ให้บริการแก่บุคคลที่แสดงเจตนาไม่ประสงค์ให้ข้อมูลส่วนบุคคลของตนเองถูกเก็บรวบรวม และมิให้ผู้ให้บริการเลือกปฏิบัติต่อบุคคลซึ่งแสดงเจตจำนงไม่ประสงค์ให้เก็บรวบรวมข้อมูลส่วนบุคคลของตน

ร่างพระราชบัญญัติดังกล่าวได้กำหนดข้อยกเว้นในการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลแม้ว่าบุคคลนั้นจะแสดงเจตจำนงไม่ให้ทำการเก็บรวบรวมข้อมูลส่วนบุคคลของตนไว้ 2 กรณี คือ 1. เป็นการจำเป็นเพื่อจัดเตรียมบริการซึ่งถูกร้องขอโดยบุคคลนั้น หรือ 2. บุคคลนั้นได้รับการแจ้งโดยชัดเจน ปราศจากความคลุมเครือและถูกต้องระบุว่าจะทำการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้น และได้รับความยินยอมในการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคล

ในกรณีที่มีการฝ่าฝืนโดยทำการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลซึ่งเจ้าของข้อมูลแสดงเจตจำนงมิให้เก็บรวบรวมและใช้ หรือมีการเลือกปฏิบัติต่อบุคคลดังกล่าว ให้ถือว่าเป็นการกระทำที่ไม่เป็นธรรมและหลอกหลวงอันเป็นความผิดตามข้อกำหนดภายใต้ Section 18(a)(1)(B) แห่ง Federal Trade Commision Act (15 U.S.C. 57a(a)(1)(B)) และในกรณีที่มีการละเมิดดังกล่าวเกิดขึ้นตัวบุคคลผู้ถูกละเมิดสามารถที่จะนำคดีไปสู่ศาลด้วยตนเองได้ และมีสิทธิเรียกร้องค่าสินไหมทดแทนเพื่อความเสียหายที่เกิดขึ้นจริงจากการละเมิดนั้น หรือค่าเสียหายจำนวน $500 เพื่อการละเมิดแต่ละครั้ง ทั้งนี้แล้วแต่จำนวนใดจะมากกว่า และหากศาลพบว่าผู้กระทำความผิดเจตนาหรือรู้อยู่แล้วว่าเป็นการกระทำละเมิด ศาลมีอำนาจใช้ดุลพินิจเพิ่มค่าสินไหมทดแทนไม่เกิน 3 เท่าของค่าเสียหายที่แท้จริง

3.1.6 โครงการ Smart Disclosure

โครงการ Smart Disclosure ได้รับแนวความคิดมาจากโครงการ MiData ของประเทศอังกฤษ Smart Disclosure เกิดขึ้นเนื่องจากข้อมูลส่วนบุคคลจำนวนมากที่ได้รับจากประชาชนนั้นมีค่าทางเศรษฐกิจอย่างมากแต่ประชาชนซึ่งเป็นผู้บริโภคกลับมิได้รับประโยชน์ดังกล่าวเลย โครงการดังกล่าวจึงมีขึ้นเพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึงข้อมูลการบริโภคของตนเองซึ่งอยู่ในรูปที่สามารถอ่านได้โดยเครื่อง (Machine Readable Format) ผู้บริโภคสามารถนำข้อมูลดังกล่าวไปเปรียบเทียบกับผลิตภัณฑ์หรือบริการอื่นๆอันจะช่วยให้ผู้บริโภคให้สามารถตัดสินใจและได้รับประโยชน์จากผลิตภัณฑ์หรือบริการได้ดีขึ้น Smart Disclosure ได้ถูกนำมาใช้ในกรณีใหญ่ๆ 4 กรณี[7] คือ

[7]Howard, A.,“What is smart disclosure? “Choice engines” are helping consumers make smarter decisions through personal and government

1.เมื่อรัฐบาลได้ออกข้อมูลเกี่ยวกับสินค้าหรือบริการ เช่น การจัดลำดับโรงพยาบาลของกระทรวงสาธารณสุข

2. เมื่อรัฐบาลได้เปิดเผยข้อมูลส่วนบุคคลของพลเมือง

3. เมื่อบริษัทเอกชนออกข้อมูลเกี่ยวกับสินค้าหรือบริการในรูปแบบซึ่งสามารถอ่านได้โดยเครื่อง

4.เมื่อบริษัทเอกชนได้เปิดเผยแก่บุคคลใดบุคคลหนึ่งซึ่งข้อมูลส่วนบุคคลเกี่ยวกับการใช้งาน เช่น บริษัทพลังงานให้ข้อมูลแก่ครัวเรือนหนึ่งเกี่ยวกับการใช้พลังงาน

3.1.7 ข้อความคิดบางประการเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกา

เนื่องด้วยประเทศสหรัฐอเมริกาไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลบังคับใช้เป็นการทั่วไปต่อภาคเอกชน ทำให้กฎระเบียบเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกามักอยู่ในแนวปฏิบัติขององค์กรหรือเป็นประกาศของคณะกรรมการของแต่ภาคส่วน หรืออยู่ภายใต้ความควบคุมของกฎหมายมลรัฐ ซึ่งผู้เก็บรวบรวมข้อมูลส่วนบุคคลจะตกตกอยู่ภายใต้หลักเกณฑ์ใดๆหรือไม่ต้องพิจารณาจากกฎหมายของแต่ละมลรัฐหรือกฎหรือระเบียบของคณะกรรมการดังที่กล่าวมา สำหรับหน่วยงานที่มีบทบาทอย่างมากในด้านข้อมูลของผู้บริโภคคือ FTC ซึ่งสอดส่องดูแลและเอาผิดกับบริษัทที่บริษัทที่ละเมิดข้อตกลงกับผู้บริโภคไม่เก็บรักษาข้อมูลส่วนบุคคลของผู้บริโภคให้ปลอดภัย หรือละเมิดสิทธิในความเป็นส่วนตัวของผู้บริโภคโดยอาศัยมาตรา 5 แห่ง Federal Trade Commission Act

ในด้านข้อมูล Pseudonymous FTC มีความเห็นว่าข้อมูลดังกล่าวสามารถเชื่อมโยงไปยังเจ้าของข้อมูลส่วนบุคคลได้ โดยเฉพาะอย่างยิ่งเมื่อนำมาใช้กับเทคโนโลยี Profiling โดยงานวิจัยของ AOL ได้แปลงข้อมูลผู้ใช้งานเว็บไซต์ให้เป็นข้อมูล Pseudonymous ด้วยการแทนค่าโดยตัวเลข เช่น 4417749 จากการแทนค่าดังกล่าวนี้ New York Times สามารถที่จะสืบค้นกลับไปได้ว่าเจ้าของข้อมูลที่ถูกแทนค่าโดยตัวเลขเป็นใคร[8] ดังนั้นการให้ความคุ้มครองแก่ข้อมูล Pseudonymous

---

data.",Accedssed 25 January 2016,http://radar.oreilly.com/2012/04/what-is-smart-disclosure.html

[8]Felten, E.,"Are pseudonymous "anonymous"?",Accedssed25 January 2016, https://www.ftc.gov/news-events/blogs/techftc/2012/04/are-pseudonyms-anonymous

ซึ่งถือได้ว่าเป็นข้อมูลส่วนบุคคลจึงแตกต่างไปจากข้อมูล Anonymous กรณีของการ Profiling แล้ว FTC แนะนำให้ผู้ให้บริการนำเทคนิค Do Not Track มาใช้ กล่าวคือ ผู้ให้บริการต้องมีวิธีการให้เจ้าของข้อมูลส่วนบุคคลซึ่งเป็นปัจเจกบุคคลสามารถแสดงเจตนาได้ว่าต้องการให้ติดตามและแสดงโฆษณาแก่ตนหรือไม่[9]

จากที่กล่าวมาแม้สหรัฐอเมริกาจะยังมิได้มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลบังคับใช้เป็นการทั่วไป แต่ก็มีหน่วยงาน FTC ที่พยายามให้ความคุ้มครองแก่ผู้บริโภคโดยอาศัยมาตรา 5 แห่งพระราชบัญญัติ Federal Trade Commission อย่างไรก็ตามสหรัฐอเมริกาได้เล็งเห็นถึงความสำคัญแก่การคุ้มครองข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมผ่านอิเล็กทรอนิกส์ดังจะเห็นได้จากความพยายามในการผลักดันกฎหมาย Consumer Privacy Bill of Right ซึ่งมีบทบัญญัติเกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล และ Do Not Track Me Online Bill ซึ่งมีบทบัญญัติเกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคลผ่านอิเล็กทรอนิกส์โดยอาศัยวิธี Profiling ทั้งยังกำหนดให้ข้อมูล Mac Address และ IP Address เป็นข้อมูลส่วนบุคคลตามร่างพระราชบัญญัตินี้อีกด้วย

3.2 กฎเกณฑ์ของสหภาพยุโรป

สหภาพยุโรปเป็นสหภาพทางเศรษฐกิจและการเมือง ประกอบด้วยสมาชิกจำนวน 28 ประเทศ โดยการออกกฎหมายของสหภาพยุโรปสามารถแบ่งออกได้ 2 ระดับ กล่าวคือ ระดับสหภาพยุโรป และระดับประเทศสมาชิก ซึ่งการออกกฎหมายในระดับสหภาพยุโรปสามารถแบ่งย่อยได้ 3 ประเภท[10] คือ

1.กฎหมายขั้นปฐมภูมิ (Primary Legislation) ได้แก่ สนธิสัญญาต่างๆ

---

[9] Federal Trade Commission, “Do Not Track”,Accedssed25 January 2016, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/do-not-track

[10] กรมวิชาการเกษตร, “ระเบียบสุขอนามัยพืชของสหภาพยุโรป ระเบียบว่าด้วยมาตรการป้องกันการนำสิ่งมีชีวิตที่เป็นอันตรายต่อพืชและผลิตภัณฑ์จากพืชเข้าสู่ประชาคมและมาตรการป้องกันการแพร่ระบาดของสิ่งมีชีวิตที่เป็นอันตรายภายในประชาคม (Council Directive 2002/29/EC)”, สืบค้นเมื่อวันที่ 14 มีนาคม 2559, http://www.doa.go.th/psco/images/EU/translation.complete_regulation.pdf

2.กฎหมายขั้นทุติยภูมิ (Secondary Legislation) ได้แก่Regulation Directive Decision Recommendation และ Opinion

3.ข้อตกลงระหว่างประเทศ (International Agreement) ได้แก่ ข้อตกลงที่สหภาพยุโรปได้ทำกับประเทศที่สาม

โดยในสหภาพยุโรปมีคณะกรรมการซึ่งตั้งขึ้นเพื่อดูแลเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเป็นการเฉพาะ คือ Article 29 Data Protection Working Party และกฎเกณฑ์สำคัญของสหภาพยุโรปเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่จะกล่าวถึงต่อไป คือ Directive 2002/58 Directive 95/46/EC และ General Data Protection Regulation ความแตกต่างระหว่าง Directive และ Regulation คือRegulation มีผลใช้บังคับเสมือนเป็นกฎหมายของประเทศสมาชิกโดยประเทศสมาชิกไม่จำต้องออกกฎหมายอนุวัติการตาม Regulation นี้ส่วน Directive เป็นกฎที่เสนอโดยคณะกรรมาธิการยุโรปและได้รับความเห็นชอบจากคณะมนตรีแห่งสหภาพยุโรป Directive นี้จะกำหนดกรอบการดำเนินงานเพื่อให้ประเทศสมาชิกมีการปฏิบัติที่สอดคล้องกันโดยประเทศต่างๆ ต้องดำเนินการออกกฎหมายในเรื่องนั้นๆ[11]สำหรับ Directive 2002/58 Directive 95/46/EC และ General Data Protection Regulation มีสาระสำคัญดังนี้

3.2.1 Directive 2002/58 on Privacy and Electronic Communications

Directive 2002/58 onPrivacy and Electronic Communications หรือ ePrivacy Directive ถูกนำมาบังคับใช้เมื่อวันที่ 12 กรกฎาคม ค.ศ. 2002 และมีการแก้ไขเพิ่มเติมเรื่อยมาซึ่งการแก้ไขครั้งล่าสุดมีขึ้นเมื่อวันที่ 6 เมษายน 2015 ePrivacy Directive นี้เป็นบทบัญญัติเกี่ยวกับการคุ้มครองข้อมูลและความเป็นส่วนตัวในยุคดิจิตอล ซึ่งมีสาระสำคัญหลายประการเช่น การคุ้มครองข้อมูลซึ่งเป็นความลับ รวมถึงการคุ้มครองการเก็บรวบรวมข้อมูลจากแสปมหรือคุกกี้ สาเหตุประการหนึ่งของการบังคับใช้ ePrivacy Directive นี้มาจากการติดตามพฤติกรรมของบุคคลบนอินเตอร์เน็ต ซึ่งสาระสำคัญของกฎเกณฑ์ฉบับดังกล่าว มีดังต่อไปนี้

เมื่อระบุถึงคำต่างๆใน ePrivacy Directive ที่จะกล่าวต่อไปให้มีความหมายดังต่อไปนี้

“การสื่อสาร” หมายถึง ข้อมูลใดๆที่ถูกแลกเปลี่ยน หรือถ่ายโอนระหว่างกลุ่มบุคคลซึ่งมีจำนวนจำกัดโดยผ่านบริการสื่อสารอิเล็กทรอนิกส์สาธารณะ แต่ไม่รวมถึงข้อมูลซึ่งถ่ายโอน

---

[11] European commission, “legislation”, Accedssed14 March 2016,http://ec.europa.eu/legislation/index_en.htm

โดยเป็นส่วนหนึ่งของการบริการทางโปรแกรม เว้นแต่ข้อมูลนั้นสามารถเชื่อมโยงไปยังสมาชิกหรือผู้ใช้ที่อาจถูกระบุตัวได้จากการรับข้อมูลนั้น

“ผู้ให้บริการการสื่อสาร” มีความหมายซึ่งให้ไว้ตาม Section 405 ของ Communication Act 2003(c) ซึ่ง Communication Act 2003(c) ได้ให้ความหมายไว้ว่าหมายถึง บุคคลซึ่งให้บริการการเครือข่ายการสื่อสารทางอิเล็กทรอนิกส์ หรือให้บริการการสื่อสารทางอิเล็กทรอนิกส์

“เครือข่ายการสื่อสารทางอิเล็กทรอนิกส์” มีความหมายตามที่กำหนดใน section 32 ของ Communications Act 2003(b) ซึ่ง Communication Act 2003(b) ได้ให้ความหมายไว้ว่าหมายถึง 1. ระบบการสื่อสารเพื่อการถ่ายโอนสัญญาณโดยวิธีอิเล็กทรอนิกส์ หรือแม่เหล็ก หรือพลังแม่เหล็กไฟฟ้า และ 2. บุคคลซึ่งจัดเตรียมระบบหรือเกี่ยวข้องกับระบบนั้นได้ใช้สิ่งดังต่อไปนี้เพื่อการถ่ายโอนสัญญาณคือ อุปกรณ์ซึ่งประกอบอยู่ในระบบ อุปกรณ์ซึ่งใช้เพื่อการสลับหรือจัดเส้นทางของสัญญาณ และซอร์ฟแวร์และข้อมูลที่ได้ถูกจัดเก็บไว้

“บริการการสื่อสารทางอิเล็กทรอนิกส์” มีความหมายตามที่กำหนดใน section 32 ของ Communications Act 2003 ซึ่ง Communication Act 2003 ได้ให้ความหมายไว้ว่าหมายถึงบริการซึ่งมีหรือประกอบด้วยลักษณะการส่งสัญญาณทางเครือข่ายการสื่อสารอิเล็กทรอนิกส์ เว้นแต่เป็นการให้บริการทางเนื้อหา

“อีเมล” หมายถึง ตัวอักษรใดๆ เสียงพูด เสียง หรือข้อความรูปภาพที่ถูกส่งบนเครือข่ายการสื่อสารอิเล็กทรอนิกส์สาธารณะซึ่งสามารถที่จะถูกเก็บรักษาบนเครือข่ายหรือบนอุปกรณ์ปลายทางของผู้รับจนกระทั่งผู้รับได้รับ รวมถึงข้อความที่ถูกส่งโดยอาศัยบริการข้อความสั้น

“บุคคล” หมายถึง ปัจเจกบุคคล และรวมถึงหน่วยงานซึ่งยังมิได้จดทะเบียนของบุคคลดังกล่าว

“Location data” หมายถึง ข้อมูลใดๆซึ่งถูกประมวลในเครือข่ายการสื่อสารอิเล็กทรอนิกส์หรือโดยบริการการสื่อสารอิเล็กทรอนิกส์ระบุถึงตำแหน่งทางภูมิศาสตร์ของอุปกรณ์ปลายทางของผู้ใช้บริการการสื่อสารอิเล็กทรอนิกส์สาธารณะ โดยให้รวมถึงข้อมูลดังต่อไปนี้

1. ละติจูด ลองติจูด หรือระดับความสูงของอุปกรณ์ปลายทาง
2. ทิศทางการเดินทางของผู้ใช้
3. เวลาซึ่งข้อมูล location ได้ถูกบันทึกไว้

“การละเมิดข้อมูลส่วนบุคคล” หมายถึง การละเมิดความปลอดภัยซึ่งนำไปสู่การทำลาย การสูญหาย การเปลี่ยนแปลง การเปิดเผยโดยไม่ได้รับอนุญาต หรือการเข้าถึงข้อมูลส่วนบุคคล การถ่ายโอน การเก็บรักษา หรือการประมวลผลโดยประการอื่นตามบทบัญญัติเกี่ยวกับบริการ

สื่อสารอิเล็กทรอนิกส์สาธารณะ ทั้งนี้ไม่ว่าการกระทำดังกล่าวจะเกิดขึ้นโดยอุบัติเหตุหรือการกระทำโดยจงใจก็ตาม

“ผู้ให้บริการการสื่อสารสาธารณะ” หมายถึง ผู้ให้บริการการเครือข่ายการสื่อสารอิเล็กทรอนิกส์สาธารณะ หรือผู้ให้บริการการสื่อสารอิเล็กทรอนิกส์สาธารณะ

“ผู้ให้บริการเครือข่ายอิเล็กทรอนิกส์สาธารณะ” ให้มีความหมายตามที่กำหนดใน section 151 ของ Communication Act 2003(g) ซึ่ง Communication Act 2003(g) ได้ให้ความหมายไว้ว่าหมายถึง บริการสื่อสารอิเล็กทรอนิกส์สาธารณะใดๆซึ่งสามารถใช้ได้โดยสาธารณะ

“เครือข่ายการสื่อสารอิเล็กทรอนิกส์สาธารณะ” ให้มีความหมายตามที่กำหนดใน section 151 ของ Communication Act 2003 ซึ่ง Communication Act 2003 ได้ให้ความหมายไว้ว่า เครือข่ายบริการสื่อสารอิเล็กทรอนิกส์ซึ่งให้บริการทั้งหมดหรือโดยหลักเพื่อวัตถุประสงค์เพื่อให้บริการการสื่อสารอิเล็กทรอนิกส์สาธารณะสามารถเข้าถึงได้โดยสาธารณะ

“สมาชิก” หมายถึง บุคคลซึ่งเป็นคู่สัญญากับผู้ให้บริการสื่อสารอิเล็กทรอนิกส์สาธารณะเพื่อการให้บริการดังกล่าว

“Traffic Data” หมายถึง ข้อมูลซึ่งถูปะมวลผลเพื่อวัตถุประสงค์ในการถ่ายโอนการสื่อสารทางเครือข่ายการสื่อสารอิเล็กทรอนิกส์ หรือเพื่อการเรียกเก็บเงินเกี่ยวกับการสื่อสารนั้น รวมถึงข้อมูลเกี่ยวกับการกำหนดเส้นทาง ระยะเวลา หรือเวลาในการสื่อสาร

“ผู้ใช้” หมายถึง บุคคลใดๆซึ่งใช้บริการสื่อสารอิเล็กทรอนิกส์สาธารณะ

ePrivacy Direvtive ได้กำหนดให้ผู้ให้บริการสื่อสารอิเล็กทรอนิกส์สาธารณะต้องมีมาตรการทางเทคนิคและมาตรการในทางองค์กรเพื่อรักษาความปลอดภัยของการให้บริการ มาตรการดังกล่าวต้องก่อให้เกิดความมั่นใจว่าข้อมูลส่วนบุคคลนั้นจะถูกเข้าถึงได้เพียงเฉพาะบุคคลที่ได้รับอนุญาตและเพื่อวัตถุประสงค์ที่ชอบด้วยกฎหมายเท่านั้น และมาตรการนี้ต้องป้องกันข้อมูลส่วนบุคคลที่ถูกเก็บรักษาหรือถูกโอนมิให้ถูกทำลายโดยอุบัติเหตุหรือโดยมิชอบด้วยกฎหมาย การสูญหายโดยอุบัติเหตุ หรือการเปลี่ยนแปลงหรือการเก็บรักษาโดยบุคคลซึ่งไม่มีอำนาจหรือไม่ชอบด้วยกฎหมาย การประมวลผล การเข้าถึงหรือการเปิดเผย หากภายหลังการบังคับใช้มาตรการดังกล่าวแล้วยังมีความเสี่ยงที่มีนัยสำคัญต่อความปลอดภัยของบริการสื่อสารอิเล็กทรอนิกส์สาธารณะ ผู้ให้บริการต้องแจ้งให้สมาชิกทราบถึงลักษณะของความเสี่ยง มาตรการที่เหมาะสมซึ่งสมาชิกอาจได้รับเพื่อป้องกันความเสี่ยงและค่าใช้จ่ายที่อาจเกิดขึ้นต่อสมาชิกในการใช้มาตรการดังกล่าว

ในกรณีที่มีการละเมิดข้อมูลส่วนบุคคลผู้ให้บริการต้องแจ้งการละเมิดต่อ Information Commissioner โดยไม่ชักช้าโดยจะต้องแจ้งถึงลักษณะของการละเมิด ผลจากการละเมิด และมาตรการที่ถูกใช้หรือจะใช้เพื่อแจ้งการละเมิด และหากการละเมิดนั้นน่าจะก่อให้เกิด

ผลกระทบต่อข้อมูลส่วนบุคคลหรือความเป็นส่วนตัวของสมาชิกหรือผู้ใช้ ผู้ให้บริการต้องแจ้งการละเมิดนั้นแก่สมาชิกหรือผู้ใช้โดยไม่ช้าซึ่งการแจ้งดังกล่าวต้องระบุถึงลักษณะของการละเมิด ข้อมูลเพื่อให้สมาชิกหรือผู้ใช้สามารถติดต่อผู้ให้บริการเพื่อข้อมูลเพิ่มเติม และคำแนะนำเกี่ยวกับมาตรการเพื่อให้สมาชิกบรรเทาผลกระทบที่อาจเกิดขึ้นจากการละเมิดนั้น อย่างไรก็ตามผู้ให้บริการได้รับการยกเว้นไม่ต้องแจ้งเตือนสมาชิกหรือผู้ใช้ในกรณีที่ผู้ให้บริการมีมาตรการเทคโนโลยีป้องกันที่เหมาะสมซึ่งก่อให้บุคคลผู้ไม่ได้รับอนุญาตให้เข้าถึงข้อมูลนั้นไม่สามารไม่สามารถเข้าใจข้อมูลนั้นได้ และมาตรการนั้นได้ถูกนำมาใช้แก่ข้อมูลที่ถูกละเมิด

การให้ความคุ้มครองแก่การเก็บรวบรวมหรือการเข้าถึงข้อมูลส่วนบุคคล ePrivacy Directive ได้กำหนดว่านอกจากจะเป็นการเก็บรวบรวมหรือการเข้าถึงข้อมูลส่วนบุคคลโดยมีวัตถุประสงค์เพื่อการถ่ายโอนข้อมูลการสื่อสารผ่านเครือข่ายการสื่อสารอิเล็กทรอนิกส์หรือการเก็บรวบรวมหรือการสื่อสารนั้นจำเป็นอย่างยิ่งเพื่อข้อกำหนดของบริการสังคมข้อมูลข่าวสารซึ่งร้องขอโดยสมาชิกหรือผู้ใช้ บุคคลจะต้องไม่ทำการเก็บรักษาหรือเข้าถึงข้อมูลส่วนบุคคลซึ่งถูกเก็บรักษาไว้ในอุปกรณ์ปลายทางของสมาชิกหรือผู้ใช้ เว้นแต่สมาชิกหรือผู้ใช้ได้รับข้อมูลที่ชัดแจ้งและเข้าใจได้เกี่ยวกับวัตถุประสงค์ของการเก็บรวบรวมหรือการเข้าถึงข้อมูลนั้น

ในกรณีของการประมวลผลข้อมูลส่วนบุคคล ePrivacy Directive ข้อ 7 กำหนดให้ Traffic data ของสมาชิกหรือผู้ใช้ซึ่งถูกประมวลผลหรือเก็บรักษาโดยผู้ให้บริการสื่อสารสาธารณะหากข้อมูลนั้นไม่จำเป็นอีกต่อไป ผู้ให้บริการสื่อสาธารณะจะต้องลบหรือทำการแก้ไขเปลี่ยนแปลงข้อมูลนั้นเพื่อไม่ให้สามารถเชื่อมโยงตัวเจ้าของได้ สำหรับความคุ้มครอง location data ได้ถูกกำหนดไว้ในข้อ 14 เรื่องข้อจำกัดของการประมวลผล location data โดยกำหนดห้ามผู้ประกอบการสื่อสารอิเล็กทรอนิกส์หรือผู้ให้บริการเครือข่ายการสื่อสารอิเล็กทรอนิกส์ประมวลผลข้อมูลเกี่ยวกับ location data ของสมาชิกหรือผู้ใช้ โดยมีข้อยกเว้นให้สามารถทำการประมวลผลได้หากสมาชิกหรือผู้ใช้ไม่สามารถถูกระบุตัวโดยข้อมูลนั้นหรือเป็นการจำเป็นแก่การให้บริการเสริม (Value added service) โดยได้รับความยินยอมจากผู้ใช้

นอกจากที่กล่าวมา ePrivacy Directive ยังมีบทบัญญัติเกี่ยวกับการทำการตลาดแบบตรงผ่านโทรศัพท์ โทรสาร และอีเมล โดยในที่นี้จะขอกล่าวถึงกฎเกณฑ์เกี่ยวกับการทำการตลาดแบบตรงผ่านอีเมลเท่านั้น ซึ่งในกรณีดังกล่าว ePrivacy Directive ได้กำหนดห้ามบุคคลทำการส่งหรือสนับสนุนการส่งการสื่อสารที่ไม่พึงประสงค์ซึ่งมีวัตถุประสงค์เพื่อการตลาดผ่านทางอีเมล เว้นแต่จะได้รับความยินยอมจากผู้รับไว้ล่วงหน้า

3.2.2 Directive 95/46/EC on the Protection of Personal Data

Directive 95/46/EC of the Protection of Personal ใช้บังคับเมื่อวันที่ 24 ตุลาคม ค.ศ. 1995 บัญญัติขึ้นเพื่อเป็นแนวทางเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของ EU เพื่อกำหนดให้ประเทศสมาชิกให้ความคุ้มครองข้อมูลส่วนบุคคลในระดับที่เท่าทียมกันในยุโรป Directive 95/46/EC นั้นนำมาบังคับใช้แก่การประมวลผลข้อมูลส่วนบุคคลทั้งหมดหรือบางส่วนโดยวิธีอัตโนมัติ แต่จะไม่นำมาบังคับใช้แก่การประมวลผลข้อมูลส่วนบุคคลซึ่งมิได้ตกอยู่ภายใต้กฎหมายแห่งประชาคมยุโรป Directive 95/46/EC ได้ให้ความหมายของคำต่างๆไว้ในมาตรา 2 ซึ่งมีสาระสำคัญดังต่อไปนี้

“ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลใดๆที่เกี่ยวข้องกับบุคคลที่ถูกระบุตัวหรือบุคคลที่อาจถูกระบุตัวได้ โดยบุคคลซึ่งถูกระบุตัวได้ คือบุคคลที่สามารถถูกระบุตัวได้โดยตรงหรือโดยอ้อม โดยเฉพาะอย่างยิ่งจากการอ้างอิงโดยเลขบัตรประชาชน หรือปัจจัยหนึ่งหรือหลายปัจจัยซึ่งบ่งเฉพาะทางร่างกาย สรีรวิทยา จิตใจ เศรษฐกิจ วัฒนธรรม หรืออัตลักษณ์ทางสังคม

“การประมวลผลข้อมูลส่วนบุคคล” หมายถึง การดำเนินการต่างๆหรือชุดของการดำเนินการซึ่งกระทำต่อข้อมูลส่วนบุคคล ไม่ว่าจะเป็นไปโดยวิธีอัตโนมัติหรือไม่ก็ตาม เช่น การเก็บรวบรวม การบันทึก การจัดระเบียบ การเก็บรักษา การเปลี่ยนแปลงหรือปรับปรุง การกู้คืน การใช้ การเปิดเผยโดยการส่ง การเผยแพร่ หรือการทำให้สามารถเข้าถึงได้โดยประการอื่น การจัดหรือการรวม การปิดกั้น การลบหรือการทำลาย

“ผู้ควบคุม” หมายถึง บุคคลธรรมดาหรือนิติบุคคล หน่วยงานรัฐ ตัวแทนหรือหรือบุคคลอื่นใดไม่ว่าโดยตนเองหรือโดยร่วมกับบุคคลอื่นกำหนดวัตถุประสงค์และวิธีในการประมวลผลข้อมูลส่วนบุคคล ในกรณีที่วัตถุประสงค์และวิธีในการประมวลผลข้อมูลส่วนบุคคลกำหนดโดยกฎหมายหรือกฎของประเทศหรือประชาคม ผู้ควบคุมข้อมูลส่วนบุคคลหรือหลักเกณฑ์เฉพาะเพื่อการแต่งตั้งผู้ควบคุมข้อมูลให้กำหนดโดยกฎหมายของประเทศหรือประชาคม

“ความยินยอมของเจ้าของข้อมูลส่วนบุคคล” หมายถึง การแสดงเจตนาโดยอิสระมีลักษณะเฉพาะเจาะจงและบ่งบอกถึงวัตถุประสงค์ที่เจ้าของข้อมูลส่วนบุคคลแสดงถึงความยินยอมให้ทำการประมวลผลข้อมูลส่วนบุคคล

การบังคับใช้ Directive 95/46/EC กำหนดให้รัฐสมาชิกต้องนำบทบัญญัติแห่ง Directive นี้มาใช้บังคับแก่การประมวลผลข้อมูลส่วนบุคคลซึ่งผู้ควบคุมข้อมูลตั้งอยู่ในดินแดนของรัฐสมาชิก ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลตั้งอยู่ในหลายดินแดนของรัฐสมาชิก ผู้ควบคุมข้อมูลต้องปฏิบัติตามกฎหมายของแต่ละประเทศด้วย หรือผู้ควบคุมข้อมูลส่วนบุคคลมิได้ตั้งอยู่ในดินแดนของรัฐสมาชิกแต่กฎหมายของรัฐสมาชิกนั้นถูกนำมาใช้บังคับต่อผู้ควบคุมข้อมูลส่วนบุคคล และในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลอยู่นอกดินแดนของสหภาพยุโรปแต่วัตถุประสงค์ในการประมวลผลข้อมูล

ส่วนบุคคลใช้อุปกรณ์โดยอาจเป็นระบบอัตโนมัติหรือไม่ก็ตามซึ่งตั้งอยู่ในดินแดนแห่งรัฐสมาชิก เว้นแต่อุปกรณ์นั้นใช้เพื่อวัตถุประสงค์ในการส่งข้อมูลข้ามดินแดนเท่านั้น ซึ่งในกรณีดังกล่าวผู้ควบคุมข้อมูลส่วนบุคคลต้องตั้งตัวแทนในดินแดนของรัฐสมาชิก

ประเภทของข้อมูลส่วนบุคคลตาม Directive 95/46/EC สามารถแบ่งออกได้ 2 ประเภท คือ ข้อมูลส่วนบุคคล และข้อมูลพิเศษ ซึ่งการประมวลผลข้อมูลพิเศษนี้ต้องเป็นไปตามมาตรา 9 กล่าวคือ ห้ามทำการประมวลข้อมูลที่เปิดเผยเชื้อชาติ หรือแหล่งกำเนิดทางชาติพันธุ์ ความเห็นทางการเมือง ความเชื่อทางศาสนา ความเป็นสมาชิกของสหภาพแรงงาน และการประมวลข้อมูลเกี่ยวกับสุขภาพหรือความประพฤติทางเพศ โดยมีข้อยกเว้นคือ ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่กฎหมายกำหนดห้ามมิให้เจ้าของข้อมูลส่วนบุคคลให้ความยินยอม หรือเป็นการจำเป็นในการปฏิบัติหน้าที่หรือสิทธิพิเศษของเจ้าของข้อมูลส่วนบุคคลในด้านกฎหมายแรงงานตราบเท่าที่ไม่ขัดต่อกฎหมายของประเทศนั้นๆ หรือเป็นการจำเป็นเพื่อปกป้องผลประโยชน์ที่สำคัญของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่นในกรณีที่เจ้าของข้อมูลไม่สามารถให้ความยินยอมได้ไม่ว่าทางพายภาพหรือทางกฎหมาย หรือการประมวลผลได้ทำขึ้นโดยชอบด้วยกฎหมายและมีหลักประกันที่เหมาะสมจากมูลนิธิ องค์กร หรือบุคคลซึ่งไม่แสวงหากำไร ซึ่งมีวัตถุประสงค์ในทางการเมือง ปรัชญา ศาสนา หรือสหภาพแรงงาน โดยการประมวลผลนั้นต้องเกี่ยวข้องกับสมาชิกของบุคคลหรือองค์นั้นเท่านั้น และข้อมูลต้องไม่ถูกเปิดเผยไปยังบุคคลที่สามโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล หรือ การประมวลผลนั้นเป็นข้อมูลที่ถูกทำให้เป็นสาธารณะโดยเจ้าของข้อมูลส่วนบุคคลหรือจำเป็นในการก่อตั้ง การใช้สิทธิ หรือการต่อสู้คดี

สำหรับในด้านของข้อมูลส่วนบุคคลการประมวลผลข้อมูลส่วนบุคคลจะสามารถกระทำได้ใน 6 กรณี คือ 1. ได้กระทำต่อเมื่อได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล 2. เป็นการจำเป็นเพื่อปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาในสัญญานั้น หรือเป็นการปฏิบัติตามขั้นตอนก่อนมีการเข้าทำสัญญาโดยคำร้องขอของเจ้าของข้อมูลส่วนบุคคล 3. การประมวลผลเป็นการจำเป็นเพื่อปฏิบัติหน้าที่ตามกฎหมาย 4. การประมวลผลเป็นการจำเป็นเพื่อการปกป้องผลประโยชน์สำคัญของเจ้าของข้อมูลส่วนบุคคล 5. การประมวลผลจำเป็นเพื่อการปฏิบัติหน้าที่อันเป็นประโยชน์สาธารณะหรือเป็นการใช้อำนาจขององค์กรรัฐต่อผู้ควบคุมข้อมูลส่วนบุคคลหรือบุคคลที่สามซึ่งข้อมูลนั้นถูกเปิดเผย หรือ 6. การประมวลผลเป็นการจำเป็นเพื่อวัตถุประสงค์เกี่ยวกับผลประโยชน์ที่ชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือบุคคลที่สาม เว้นแต่ประโยชน์นี้ทับซ้อนกับประโยชน์เกี่ยวกับสิทธิและเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคลซึ่งต้องได้รับการคุ้มครอง

มาตรา 6 กำหนดเรื่องคุณภาพของข้อมูลถูกกำหนดไว้โดยกำหนดให้ข้อมูลส่วนบุคคลต้องประมวลผลโดยชอบด้วยกฎหมายหรือเป็นธรรม การเก็บรวบรวมข้อมูลส่วนบุคคลต้องมีวัตถุประสงค์ที่ชัดแจ้ง ชอบด้วยกฎหมาย และต้องไม่ประมวลผลนอกเหนือจากวัตถุประสงค์ที่ระบุไว้ แต่การประมวลเพื่อประวัติศาสตร์ สถิติ หรือวิทยาศาสตร์ ไม่ถือเป็นการขัดกับวัตถุประสงค์หากรัฐสมาชิกมีหลักการคุ้มครองที่เพียงพอ ข้อมูลส่วนบุคคลนั้นต้องเกี่ยวข้อง และไม่เกินความจำเป็นต่อวัตถุประสงค์ซึ่งข้อมูลส่วนบุคคลนั้นถูกเก็บรวบรวมและ/หรือประมวลผลในภายหน้า นอกจากนี้ข้อมูลส่วนบุคคลนั้นต้องถูกต้อง เป็นปัจจุบันและมีมาตรการเพื่อทำให้แน่ใจว่าข้อมูลที่ไม่ถูกต้องหรือไม่สมบูรณ์จะถูกทำลายหรือแก้ไขให้ถูกต้องหรือสมบูรณ์ และการเก็บรักษาข้อมูลนั้นต้องเก็บไว้เท่าระยะเวลาที่จำเป็นเพื่อการประมวลผลตามวัตถุประสงค์ที่ข้อมูลนั้นถูกเก็บรวบรวมมา

เมื่อมีการเก็บรวบรวมข้อมูลส่วนบุคคลแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งแก่เจ้าของข้อมูลส่วนบุคคลว่าได้ข้อมูลนั้นมาจากบุคคลใด รวมทั้งต้องแจ้งถึงตัวผู้ควบคุมข้อมูลและตัวแทน(ถ้ามี) วัตถุประสงค์ในการประมวลข้อมูล และข้อมูลอื่นๆ เช่น ผู้รับหรือประเภทของผู้รับข้อมูลส่วนบุคคล สิทธิในการเข้าถึงและแก้ไขข้อมูล หากข้อมูลส่วนบุคคลนั้นผู้ควบคุมข้อมูลส่วนบุคคลมิได้เก็บรวบรวมโดยตรงจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งเจ้าของข้อมูลส่วนบุคคลถึงตัวผู้ควบคุมข้อมูลส่วนบุคคลและตัวแทน(ถ้ามี) วัตถุประสงค์ในการประมวลผลข้อมูล และข้อมูลอื่นๆ เช่น ประเภทของข้อมูล ประเภทหรือบุคคลที่จะได้รับข้อมูลนั้น สิทธิในการเข้าถึง และสิทธิในการแก้ไขข้อมูลส่วนบุคคล

สำหรับสิทธิของเจ้าของข้อมูลส่วนบุคคล Directive 95/46/EC ได้กำหนดไว้สองประการ ได้แก่สิทธิในการเข้าถึงข้อมูลส่วนบุคคล และสิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล โดยสิทธิในการเข้าถึงข้อมูลส่วนบุคคลกำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิได้รับแจ้งจากผู้ควบคุมข้อมูลภายในเวลาอันควรโดยค่าใช้จ่ายไม่เกินสมควร ยืนยันถึงการมีอยู่ของข้อมูลส่วนบุคคลและการประมวลผลข้อมูลนั้น พร้อมทั้งบอกถึงวัตถุประสงค์ในการประมวลผล ประเภทของข้อมูลและบุคคลหรือประเภทของบุคคลที่ข้อมูลนั้นจะถูกเปิดเผย ซึ่งการแจ้งดังกล่าวต้องอยู่ในรูปแบบที่บุคคลนั้นสามารถเข้าใจได้ นอกจากนี้ Directive 95/46/EC ยังกำหนดสิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคลสามารถแบ่งออกได้สองกรณี คือสิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคลและสิทธิในการคัดค้านการประมวลผลโดยระบบอัตโนมัติ

สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล ให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลคัดค้านเรื่องความชอบด้วยกฎหมายในกรณีที่เกิดสถานการณ์พิเศษในการประมวลผลข้อมูลส่วนบุคคลของตนเมื่อข้อมูลส่วนบุคคลของตนถูกประมวลผลเพื่อประโยชน์สาธารณะหรือเกี่ยวกับประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลที่สาม และให้สิทธิแก่

เจ้าของข้อมูลส่วนบุคคลคัดค้านในกรณีที่เห็นว่าการประมวลผลข้อมูลส่วนบุคคลนั้นทำเพื่อการตลาด โดยการคัดค้านนี้ต้องปราศจากค่าใช้จ่าย สำหรับสิทธิในการคัดด้านการประมวลผลโดยระบบอัตโนมัติให้สิทธิแก่เจ้าของข้อมูลคัดค้านการประมวลผลโดยระบบอัตโนมัติที่ก่อให้เกิดผลทางกฎหมายหรือส่งผลเสียต่อเจ้าของข้อมูลส่วนบุคคล หรือเป็นความเห็นของระบบอัตโนมัติเทานั้น เช่น การประเมินความน่าเชื่อถือ ความประพฤติ หรือความสามารถในการทำงาน

3.2.3 General Data Protection Regulation

General data Protection Regulation หรือ GDPR เป็นกฎเกณฑ์ของสหภาพยุโรปซึ่งจะถูกนำมาบังคับใช้แทน Directive 95/46/EC on the Protection of Personal Data ความคิดในการแก้ไขกฎหมายคุ้มครองข้อมูลส่วนบุคคลเริ่มต้นขึ้นเมื่อวันที่ 25 มกราคม ค.ศ. 2012 โดย GDPR มีวัตถุประสงค์เพื่อเพิ่มความคุ้มครองแก่เจ้าของข้อมูลส่วนบุคคลซึ่งเป็นปัจเจกบุคคลให้เจ้าของข้อมูลส่วนบุคคลสามารถควบคุมข้อมูลของตนได้ นอกจากนี้ GDPR นำมาบังคับใช้แก่การประมวลผลข้อมูลส่วนบุคคลซึ่งเป็นระบบอัตโนมัติด้วย ทั้งยังมีบทบัญญัติเกี่ยวกับการโอนข้อมูลส่วนบุคคลไปนอกสหภาพยุโรป

ขอบเขตการบังคับใช้ GPDR ได้ถูกกำหนดไว้ในมาตรา 3 โดยให้นำมาใช้บังคับกับการประมวลผลข้อมูลส่วนบุคคลซึ่งกระทำโดยผู้ควบคุมข้อมูลส่วนบุคคลที่ตั้งอยู่ในสหภาพยุโรป หรือใช้กับการประมวลผลข้อมูลส่วนบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลนั้นอยู่ในสหภาพยุโรป หรือแม้ตัวผู้ควบคุมข้อมูลส่วนบุคคลจะมิได้ตั้งอยู่ในดินแดนของรัฐสมาชิกในสหภาพยุโรปแต่มีการประมวลผลข้อมูลเพื่อเสนอขายสินค้าหรือบริการให้แก่เจ้าของข้อมูลส่วนบุคคลที่อยู่ในดินแดนแห่งรัฐสมาชิกของสหภาพยุโรปไม่ว่าการเสนอขายสินค้าหรือบริการนั้นจะมีค่าใช้จ่ายหรือไม่ก็ตาม หรือเป็นการสังเกตพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลซึ่งพฤติกรรมนั้นเกิดขึ้นในดินแดนแห่งรัฐสมาชิกของสหภาพยุโรป หรือในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่ตกอยู่ภายใต้บังคับแห่ง GDPR ในกรณีทั้งหมดที่กล่าวมาแต่บทบัญญัติว่าด้วยกฎหมายขัดกันให้นำ GDPR มาใช้ ผู้ควบคุมข้อมูลส่วนบุคคลนั้นต้องปฏิบัติตาม GDPR ด้วย

GDPR ได้กำหนดความหมายของคำสำคัญต่างๆไว้ ดังนี้

“ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งสามารถถูกระบุตัวได้หรืออาจถูกระบุตัวได้ ไม่ว่าโดยทางตรงหรือทางอ้อมจากข้อมูลนั้น โดยเฉพาะอย่างยิ่งจากการอ้างอิงจากสิ่งพิสูจน์เอกลักษณ์ เช่น ชื่อ เลขบัตรจำตัวประชาชน ข้อมูลที่อยู่ เอกลักษณ์ทางออนไลน์ หรือเอกลักษณ์อย่างใดอย่างหรือหลายอย่างเกี่ยวกับร่างกาย สรีรวิทยา พันธุกรรม จิตใจ เศรษฐกิจ วัฒนธรรมหรือสังคมของบุคคลนั้น

“การจำกัดการประมวลผล” หมายถึง การทำเครื่องหมายข้อมูลส่วนบุคคลที่ได้รับมาโดยมีวัตถุประสงค์เพื่อจำกัดการประมวลผลในอนาคต

“ข้อมูล Pseudonymous” หมายถึง การประมวลผลข้อมูลส่วนบุคคลในลักษณะที่ข้อมูลนั้นไม่สามารถบ่งชี้ไปยังเจ้าของข้อมูลส่วนบุคคลได้ หากมิได้มีการใช้ข้อมูลอื่นเพิ่มเติม ตราบเท่าที่ข้อมูลดังกล่าวได้ถูกเก็บไว้แยกต่างหาก และมีมาตรการทางเทคนิคและมาตรการทางองค์ในการทำให้มั่นใจว่าจะไม่เชื่อมโยงไปยังเจ้าของข้อมูลส่วนบุคคล

“ข้อมูลทางพันธุกรรม” หมายถึง ข้อมูลส่วนบุคคลที่เกี่ยวกับพันธุกรรมของบุคคลธรรมดาซึ่งได้รับหรือสืบทอดมา โดยข้อมูลนี้นี้มีเอกลักษณ์พิเศษเกี่ยวกับสรีรวิทยาหรือสุขภาพของบุคคลนั้น โดยแสดงผลจากการวิเคราะห์ตัวอย่างทางชีวภาพของบุคคลนั้น

“ข้อมูลไบโอเมตริก (Biometric)” หมายถึง ข้อมูลส่วนบุคคลเกิดจากการประมวลผลโดยใช้เทคนิคเฉพาะเกี่ยวกับกายภาพ หรือความประพฤติของบุคคลนั้น ซึ่งทำให้บ่งชี้ลักษณะเฉพาะของบุคคล เช่น รูปหน้า หรือ ลายนิ้วมือ

“Profiling” หมายถึง การประมวลผลข้อมูลโดยระบบอัตโนมัติโดยการใช้ข้อมูลเหล่านั้นประเมินมุมมองของบุคคล โดยเฉพาะอย่างยิ่งการวิเคราะห์และประเมินประสิทธิภาพเกี่ยวกับการทำงาน สถานะทางเศรษฐกิจ สุขภาพ ความชอบ ความสนใจ ความน่าไว้วางใจ พฤติกรรมหรือการเคลื่อนไหว

GDPR ได้แบ่งข้อมูลส่วนบุคคลออกเป็น 2 ประเภท คือข้อมูลส่วนบุคคล และข้อมูลพิเศษ ซึ่งข้อมูลส่วนบุคคลได้แก่ข้อมูลทั่วไปเกี่ยวกับบุคคลผู้เป็นเจ้าของข้อมูลส่วนบุคคล ซึ่งมีหลักเกณฑ์ในการเก็บรวบรวม ใช้ หรือเปิดเผยแตกต่างไปจากข้อมูลที่มีลักษณะพิเศษซึ่งจะกล่าวต่อไป โดยข้อมูลที่มีลักษณะพิเศษนี้เป็นข้อมูลซึ่งมีความอ่อนไหว GDPR กำหนดให้ห้ามทำการประมวลผลข้อมูลที่เปิดเผยถึงเชื้อชาติ แหล่งกำเนิดชาติพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนาหรือปรัชญา การเป็นสมาชิกสภาพแรงงาน และการประมวลผลข้อมูลเกี่ยวกับพันธุกรรมและข้อมูลไบโอเมตริก (Biometric) หรือข้อมูลเกี่ยวกับสุขภาพหรือพฤติกรรมทางเพศ โดยมีข้อยกเว้น 10 ประการ คือ

1. เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมโดยชัดแจ้ง เว้นแต่การให้ความยินยอมนั้นต้องห้ามโดยกฎหมาย

2. การประมวลผลเป็นการจำเป็นเพื่อวัตถุประสงค์ในการปฏิบัติตามหน้าที่หรือใช้สิทธิเฉพาะเจาะจงของผู้ควบคุมข้อมูลส่วนบุคคล หรือของเจ้าของข้อมูลส่วนบุคคลเกี่ยวกับการจ้างงาน ประกันสังคม ทั้งนี้เท่าที่ชอบด้วยกฎหมายของประเทศนั้นๆ

3. การประมวลผลจำเป็นในการปกป้องประโยชน์ของเจ้าของข้อมูลส่วนบุคคลหรือของบุคคลอื่นในกรณีที่เจ้าของข้อมูลส่วนบุคคลไม่สมารถให้ความยินยอมทางทางกายภาพหรือตามกฎหมายได้

4. การประมวลผลนั้นเป็นกิจกรรมที่ชอบด้วยกฎหมายและมีมาตรการป้องกันโดยองค์กร สมาคม หรือบุคคลซึ่งไม่แสวงหากำไร โดยมีวัตถุประสงค์ในทางการเมือง ปรัชญา ศาสนา หรือสหภาพแรงงาน ภายใต้เงื่อนไขว่าต้องเป็นการประมวลผลข้อมูลของสมาชิกหรือบุคคลที่เคยเป็นสมาชิกและไม่เปิดเผยข้อมูลนั้น

5. เป็นข้อมูลส่วนบุคคลที่ถูกเปิดเผยไว้เป็นสาธารณะโดยเจ้าของข้อมูลส่วนบุคคล

6. การประมวลผลนั้นจำเป็นเพื่อการก่อตั้ง การใช้สิทธิหรือการต่อสู้คดี หรือเป็นการปฏิบัติหน้าที่ของศาล

7. การประมวลผลนั้นจำเป็นเพื่อวัตถุประสงค์ในทางประโยชน์สาธารณะโดยประเทศต้องมีมาตรการป้องกันประโยชน์ของเจ้าของข้อมูลด้วย

8. การประมวลผลนั้นจำเป็นเพื่อวัตถุประสงค์ทางการแพทย์

9. การประมวลนั้นจำเป็นเพื่อประโยชน์สาธารณะเกี่ยวกับสุขภาพของประชาชน เช่น การป้องกันอันตรายร้ายแรงที่ข้ามพรมแดนหรือเพื่อให้มีมาตรฐานความปลอดภัยและคุณภาพทางสาธารณสุขที่สูง

10. การประมวลผลจำเป็นเพื่อประโยชน์สาธารณะ เช่น ประวัติศาสตร์ สถิติ วิทยาศาสตร์ โดยมีมาตรการป้องกันความปลอดภัยของรัฐ

และในการประมวลผลข้อมูลเกี่ยวกับความผิดอาญา GDPR ได้กำหนดให้สามารถกระทำได้โดยองค์กรของรัฐ ซึ่งต้องมีมาตรการป้องกันความปลอดภัยด้วย

ในเรื่องของการประมวลผลข้อมูลส่วนบุคคล GDPR กำหนดให้การเก็บรวบรวมผู้ควบคุมข้อมูลส่วนบุคคลต้องทำโดยระบุวัตถุประสงค์ที่ชัดแจ้งและชอบด้วยกฎหมาย ซึ่งวัตถุประสงค์ดังกล่าวต้องพอเหมาะ เกี่ยวข้องและไม่เกินสมควรเมื่อพิจารณาถึงวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลและต้องนำข้อมูลส่วนบุคคลไปใช้ตามวัตถุประสงค์นั้น เว้นแต่เป็นการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์สาธารณะหรือวิทยาศาสตร์ หรือวัตถุประสงค์ทางประวัติศาสตร์ การประมวลผลต้องทำโดยชอบด้วยกฎหมาย เป็นธรรมและโปร่งใส และมีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม ผู้เก็บรวบรวมข้อมูลส่วนบุคคลต้องทำให้ข้อมูลนั้นถูกต้องเป็นปัจจุบัน และทำทุกวิถีทางเพื่อให้ข้อมูลส่วนบุคคลที่ไม่ถูกต้องถูกลบ หรือแก้ไขโดยไม่ชักช้า ทั้งนี้เมื่อพิจารณาถึงวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล การเก็บรักษาข้อมูลส่วนบุคคลที่ยัง

สามารถแสดงให้เห็นตัวเจ้าของข้อมูลจะต้องทำเพียงเท่าเวลาที่จำเป็นเพื่อวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลนั้นเท่านั้น

ภายใต้มาตรา 6 กำหนดให้การประมวลจะถือว่าชอบด้วยกฎหมายในกรณีใดกรณีหนึ่งดังต่อไปนี้

1. เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมโดยชัดแจ้งในการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์หนึ่งหรือหลายวัตถุประสงค์

2. การประมวลผลเป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนการเข้าทำสัญญา

3. การประมวลผลเพื่อการปฏิบัติตามหน้าที่ตามกฎหมาย

4. การประมวลผลเป็นการจำเป็นเพื่อปกป้องผลประโยชน์สำคัญของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่น

5. การประมวลเป็นการจำเป็นเพื่อการปฏิบัติภารกิจอันเกี่ยวกับสาธารณประโยชน์หรือเป็นการใช้อำนาจรัฐเหนือผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวทับซ้อนกับประโยชน์หรือสิทธิเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคลซึ่งได้รับการคุ้มครองตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะอย่างยิ่งเมื่อเจ้าของข้อมูลส่วนบุคคลเป็นเด็ก

การประมวลผลในภายภาคหน้าต้องสอดคล้องกับวัตถุประสงค์ที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคล โดยการประมวลผลนั้นจะสอดคล้องกับวัตถุประสงค์หรือไม่ผู้ควบคุมข้อมูลส่วนบุคคลต้องพิจารณากรณีดังต่อไปนี้ เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

1. มีความเชื่อมโยงระหว่างวัตถุประสงค์ที่ข้อมูลนั้นถูกเก็บรวบรวม และวัตถุประสงค์ที่จะทำการประมวลผลต่อไป

2. บริบทที่ข้อมูลส่วนบุคคลนั้นถูกเก็บรวบรวม

3. ลักษณะของข้อมูลส่วนบุคคลที่จะทำการประมวลผลโดยเฉพาะอย่างยิ่งข้อมูลที่มีลักษณะพิเศษ

4. ผลที่อาจเกิดจากกาประมวลที่จะทำต่อไปอันจะส่งผลต่อเจ้าของข้อมูลส่วนบุคคล

5. มีมาตรการป้องกันที่เหมาะสม

อย่างไรก็ตามหากข้อมูลส่วนบุคคลที่จะทำการประมวลผลต่อไปขัดกับวัตถุประสงค์ในตอนแรกที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลคนเดียวกัน การประมวลผลต่อไปนั้นอย่างน้อยต้องมีหลักการตามที่กล่าวมาอย่างน้อยหนึ่งข้อ การ

ประมวลผลเพื่อประโยชน์ของผู้ควบคุมข้อมูลส่วนบุคคลหรือบุคคลที่สามซึ่งขัดกับวัตถุประสงค์ในตอนแรกจะถือว่าชอบด้วยกฎหมายต่อเมื่อประโยชน์นั้นสำคัญกว่าประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

สำหรับการให้ความยินยอม GDPR ได้กำหนดไว้ในมาตรา 7 โดยในกรณีที่มีการประมวลผลข้อมูลส่วนบุคคลและข้อมูลลักษณะพิเศษภายใต้ความยินยอมของเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลต้องสามารถแสดงว่าเจ้าของข้อมูลส่วนบุคคลมีการให้ความยินยอมโดยชัดแจ้ง ในกรณีที่ความยินยอมต้องทำเป็นลายลักษณ์อักษรซึ่งมีเรื่องอื่นๆรวมอยู่ด้วย การขอความยินยอมต้องแยกออกมาอย่างเด่นชัดจากเรื่องอื่นๆ และอยู่ในรูปแบบที่สามารถเข้าใจได้ เข้าถึงได้ง่าย และใช้ภาษาที่ง่ายและชัดเจน นอกจากนี้เจ้าของข้อมูลส่วนบุคคลมีสิทธิเพิกถอนความยินยอมไม่ว่าในเวลาใดๆ โดยการเพิกถอนนั้นจะไม่กระทบความชอบด้วยกฎหมายในการประมวลผลข้อมูลก่อนมีการเพิกถอนความยินยอม ทั้งนี้ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งสิทธิในการเพิกถอนความยินยอมแก่เจ้าของข้อมูลด้วย

ในด้านการประมวลผลข้อมูล Pseudonymous หากการประมวลผลข้อมูลนั้นไม่จำเป็นต้องระบุตัวเจ้าของข้อมูลส่วนบุคคลอีกต่อไป ผู้ควบคุมข้อมูลส่วนบุคคลต้องไม่เก็บรักษาหรือหาข้อมูลเพิ่มเติมหรือไม่จำต้องประมวลผลเพิ่มเติมเพียงเพื่อจะปฏิบัติตามกฎเกณฑ์ฉบับนี้ หากผู้ควบคุมข้อมูลส่วนบุคคลได้ทำการหาข้อมูลเพิ่มเติมก่อให้สามารถระบุตัวเจ้าของข้อมูลส่วนบุคคลได้ เจ้าของข้อมูลส่วนบุคคลนั้นมีสิทธิตามที่กำหนดไว้ในกฎเกณฑ์นี้

เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถควบคุมข้อมูลของตนเองได้ GDPR ได้กำหนดสิทธิของเจ้าของข้อมูลส่วนบุคคลไว้หลายประการ ดังนี้

<u>1. สิทธิในการขอเข้าถึงข้อมูลส่วนบุคคล</u>

สิทธิดังกล่าวกำหนดไว้ในมาตรา 15 กำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิได้รับการยืนยันจากผู้ควบคุมข้อมูลส่วนบุคคลภายในเวลาอันสมควรโดยไม่มีค่าใช้จ่ายแสดงว่าข้อมูลส่วนบุคคลนั้นได้ถูกประมวลผลหรือไม่ ได้ถูกประมวลผลที่ใด และมีสิทธิเข้าถึงข้อมูล ดังต่อไปนี้

1.วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล

2. ผู้รับหรือบุคคลที่ข้อมูลนั้นอาจถูกเปิดเผยโดยเฉพาะอย่างยิ่งผู้รับซึ่งอยู่ในประเทศที่สามหรือเป็นองค์การระหว่างประเทศ

3. หากเป็นไปได้ให้บอกระยะเวลาในการเก็บรักษาข้อมูลนั้น

4. สิทธิในการขอให้แก้ไขหรือลบข้อมูลส่วนบุคคลหรือสิทธิในการคัดค้านการประมวลผล

5. สิทธิในการร้องเรียนต่อเจ้าหน้าที่

6. ในกรณีที่ข้อมูลนั้นมิได้ได้รับมาโดยตรงจากเจ้าของข้อมูลส่วนบุคคล ต้องบอกถึงที่มาของข้อมูลนั้น

7. ในกรณีที่มีการตัดสินใจโดยระบบอัตโนมัติ รวมถึงการทำ Profiling ต้องบอกข้อมูลที่เป็นเหตุผลที่เกี่ยวข้อง รวมถึงผลที่อาจเกิดจากการประมวลผลด้วย

2. สิทธิในการแก้ไขข้อมูลส่วนบุคคล

ในกรณีที่ข้อมูลส่วนบุคคลนั้นไม่ถูกต้อง หรือไม่เป็นปัจจุบัน เจ้าของข้อมูลมีสิทธิร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการแก้ไขข้อมูลให้ถูกต้องโดยไม่ชักช้า โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งการแก้ไขให้แก่บุคคลอื่นซึ่งข้อมูลส่วนบุคคลนั้นถูกเปิดเผย เว้นแต่ไม่สามารถกระทำได้หรือเป็นการใช้ความพยายามเกินสมควร

3. สิทธิในการขอให้ลบข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ในการลบข้อมูลโดยไม่ชักช้า โดยเฉพาะข้อมูลที่เก็บรวบรวมในขณะที่เจ้าของข้อมูลส่วนบุคคลเป็นเด็ก และเจ้าของข้อมูลมีสิทธิขอให้ผู้ควบคุมข้อมูลลบข้อมูลในกรณีดังต่อไปนี้ด้วย

1. ข้อมูลนั้นไม่จำเป็นอีกต่อไปเมื่อพิจารณาถึงวัตถุประสงค์ที่ทำการเก็บรวบรวมหรือ

2. เจ้าของข้อมูลส่วนบุคคลเพิกถอนความยินยอมและไม่มีพื้นฐานกฎหมายรองรับการประมวลผลอีกต่อไปหรือ

3. เจ้าของข้อมูลส่วนบุคคลคัดค้านการประมวลผลข้อมูลตามมาตรา 19(1) และไม่มีเหตุอันชอบด้วยกฎหมายที่สำคัญกว่าในการประมวลผลต่อไป หรือเจ้าของข้อมูลคัดค้านการประมวลผลตามมาตรา 19(2)หรือ

4. ข้อมูลถูกประมวลผลโดยไม่ชอบด้วยกฎหมายหรือ

5. ข้อมูลนั้นจำเป็นต้องถูกลบเพื่อปฏิบัติตามกฎหมายที่ควบคุมผู้ควบคุมข้อมูลส่วนบุคคล

เมื่อเจ้าของข้อมูลส่วนบุคคลขอใช้สิทธิแล้วผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งการขอใช้สิทธิลบข้อมูลให้แก่บุคคลอื่นซึ่งข้อมูลส่วนบุคคลนั้นถูกเปิดเผย เว้นแต่ไม่สามารถกระทำได้หรือเป็นการใช้ความพยายามเกินสมควร

4. สิทธิในการยับยั้งการประมวลผลข้อมูลส่วนบุคคล

สิทธิดังกล่าวกำหนดไว้ในมาตรา 17a ให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิได้รับการยังยั้งการประมวลผลข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลใน 3 กรณี กล่าวคือ 1. เจ้าของข้อมูลส่วนบุคคลคัดค้านความถูกต้องของข้อมูลส่วนบุคคล กรณีเช่นนี้ผู้ควบคุมข้อมูลส่วนบุคคลต้องยับยั้งการประมวลผลข้อมูลนั้นภายในกำหนดเวลาสำหรับการตรวจสอบความถูกต้องของข้อมูลนั้น หรือ 2. ผู้ควบคุมข้อมูลส่วนบุคคลไม่จำเป็นต้องมีข้อมูลส่วนบุคคลนั้นเพื่อการประมวลผล

แต่เป็นการจำเป็นสำหรับเจ้าของข้อมูลเพื่อการก่อตั้ง ใช้สิทธิ หรือต่อสู้คดี หรือ 3. เป็นกรณีที่เจ้าของข้อมูลส่วนบุคคลคัดค้านวัตถุประสงค์ของการประมวลผลตามมาตรา 19(1) ผู้ควบคุมข้อมูลส่วนบุคคลต้องยับยั้งการประมวลข้อมูลนั้นจนกระทั่งมีการยืนยันว่าเหตุผลอันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลเหนือกว่าเจ้าของข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งการจำกัดการประมวลผลให้แก่บุคคลอื่นซึ่งข้อมูลส่วนบุคคลนั้นถูกเปิดเผย เว้นแต่ไม่สามารถกระทำได้หรือเป็นการใช้ความพยายามเกินสมควร

5. สิทธิในการโอนข้อมูลส่วนบุคคล (Right to data portability)

สิทธิดังกล่าวก่อให้เจ้าของข้อมูลส่วนบุคคลสามารถรับข้อมูลเกี่ยวกับตนซึ่งได้ให้ไว้แก่ผู้ควบคุมข้อมูลส่วนบุคคลในรูปแบบที่เป็นแบบแผน ใช้งานได้ และสามารถอ่านได้โดยเครื่อง (machine-readable) และมีสิทธิที่จะโอนข้อมูลนั้นไปยังผู้ควบคุมข้อมูลอื่น เว้นแต่ การประมวลผลนั้นเป็นความยินยอมของเจ้าของข้อมูลส่วนบุคคล หรือเป็นไปตามสัญญา หรือเป็นการประมวลผลโดยวิธีอัตโนมัติ แต่หากการใช้สิทธินี้นำมาซึ่งการละเมิดลิขสิทธิ์ในการประมวลผลข้อมูลส่วนบุคคล เจ้าของข้อมูลส่วนบุคคลไม่สามารถใช้นี้ได้

6. สิทธิในการคัดค้าน

สิทธิดังกล่าวกำหนดไว้ในมาตรา 19 ให้เจ้าของบุคคลมีสิทธิคัดค้านเมื่อมีสถานการณ์พิเศษต่อเจ้าของข้อมูลส่วนบุคคลในการประมวลผลข้อมูลส่วนบุคคลที่เป็นการจำเป็นเพื่อการปฏิบัติภารกิจอันเกี่ยวกับสาธารณประโยชน์หรือเป็นการใช้อำนาจรัฐเหนือผู้ควบคุมข้อมูลส่วนบุคคล หรือเป็นการประมวลผลซึ่งจำเป็นโดยมีวัตถุประสงค์เพื่อประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือบุคคลที่สาม โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องไม่ประมวลผลข้อมูลนั้น เว้นแต่แสดงได้ว่ามีกฎหมายบังคับซึ่งเหนือกว่าประโยชน์หรือสิทธิเสรีภาพของเจ้าของของมูลเพื่อการก่อตั้ง ใช้สิทธิ หรือการต่อสู้คดี

หากข้อมูลส่วนบุคคลนั้นถูกประมวลผลเพื่อการตลาด เจ้าของข้อมูลมีสิทธิคัดค้านและหากมีการคัดค้านดังนั้นแล้วผู้ควบคุมข้อมูลส่วนบุคคลต้องไม่ประมวลผลต่อไป ในกรณีที่ข้อมูลส่วนบุคคลนั้นถูกประมวลผลเพื่อวัตถุประสงค์ทางประวัติศาสตร์ สถิติ หรือวิทยาศาสตร์ เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านได้ เว้นแต่การประมวลผลนั้นจำเป็นเพื่อประโยชน์สาธารณะ

7. สิทธิเกี่ยวกับการตัดสินใจโดยวิธีอัตโนมัติ

บทบัญญัติเกี่ยวกับการตัดสินใจโดยวิธีอัตโนมัติถูกกำหนดไว้ในมาตรา 20 เป็นการคุ้มครองเจ้าของข้อมูลมิให้ตกอยู่ภายใต้การตัดสินใจโดยระบบอัตโนมัติเพียงอย่างเดียว ซึ่งรวมถึงการทำ Profiling โดยเฉพาะอย่างยิ่งเมื่อการประมวลผลนั้นอาจทำให้เกิดผลทางกฎหมายอย่างมีนัยสำคัญแก่บุคคลดังกล่าว อย่างไรก็ตามการตัดสินใจโดยวิธีอัตโนมัตินี้มีข้อยกเว้น 3 กรณี คือ

1. เป็นการจำเป็นเพื่อการเข้าทำสัญญาหรือการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคล และผู้ควบคุมข้อมูลส่วนบุคคล

2. ได้รับอนุญาตตามกฎหมายของสหภาพยุโรปหรือกฎหมายของรัฐสมาชิกซึ่งต้องมีมาตรการคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลที่เหมาะสม

3. เป็นการกระทำภายใต้ความยินยอมโดยัดแจ้งของเจ้าของข้อมูลส่วนบุคคล

3.2.4 ข้อความคิดบางประการเกี่ยวกับกฎเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป

สหภาพยุโรได้ตระหนักถึงเทคโนโลยีที่เปลี่ยนแปลงไปทำให้ความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลอาจถูกละเมิดได้ง่ายขึ้น ดังนั้นจะเห็นได้ว่า General Data Protection Regulation ได้แก้ไขเพิ่มเติม Directive 49/56/EC ให้มีความสอดคล้องกับเทคโนโลยีในปัจจุบันมากขึ้นไม่ว่าจะเป็นการกำหนดให้กฎเกณฑ์ดังกล่าวมีผลใช้บังคับต่อบุคคลซึ่งตั้งอยู่ในสหภาพยุโรปแต่ได้ใช้ข้อมูลหรือเสนอขายสินค้าหรือบริการไม่ว่าจะมีค่าใช้จ่ายหรือไม่ก็ตามให้แก่ปัจเจกบุคคลที่อยู่ในสหภาพยุโรป การกำหนดให้ผู้ควบคุมข้อมูลต้องแยกเรื่องข้อมูลส่วนบุคคลออกมาจากเรื่องอื่นๆให้เด่นชัดในเวลาขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เพิ่มสิทธิแก่เจ้าของข้อมูลส่วนบุคคลให้สามารถเพิกถอนความยินยอมที่ได้ให้ไว้แล้วได้ มีการเพิ่มสิทธิแก่เจ้าของข้อมูลส่วนบุคคล คือ สิทธิในการขอให้ลบข้อมูล สิทธิในการยับยั้งการประมวลผลข้อมูลส่วนบุคคล สิทธิในการโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่น(Right to data portability) ทั้งยังกำหนดหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งผู้ควบคุมข้อมูลส่วนบุคคลอื่นที่ได้ตนได้เปิดเผยข้อมูลส่วนบุคคลไปเมื่อเจ้าของข้อมูลส่วนบุคคลขอใช้สิทธิลบ หรือแก้ไขข้อมูลส่วนบุคคล

นอกจากนี้ยังกำหนดให้ข้อมูล Pseudonymous ได้รับความคุ้มครองเสมือนเป็นข้อมูลส่วนบุคคลเนื่องจากยังอาจอาจนำไปสู่การระบุเจ้าของข้อมูลส่วนบุคคลได้ หากมีบุคคลใดสามารถใช้ข้อมูล Pseudonymous เชื่อมโยงไปยังเจ้าของข้อมูลส่วนบุคคลได้ เจ้าของข้อมูลส่วนบุคคลมีสิทธิตาม GDPR และเพิ่มความคุ้มครองแก่ข้อมูลไบโอเมตริก (Biometric) และ Genetic ซึ่งเป็นข้อมูลที่มีความอ่อนไหวอาจก่อให้เกิดการเลือกปฏิบัติ สำหรับข้อมูลไบโอเมตริก (Biometric) นั้นต่อไปอาจถูกนำมาใช้ในการยืนยันตัวบุคคลแทนรหัสผ่านหากยินยอมให้ทำการเก็บรวบรวมโดยง่ายอาจก่อให้เกิดปัญหาการแอบใช้รหัสผ่านขึ้นได้

GDPR ให้ความคุ้มครองแก่การทำ Profiling และการตัดสินใจโดยวิธีอัตโนมัติเพื่อมิให้เจ้าของข้อมูลส่วนบุคคลต้องตกอยู่ภายใต้การตัดสินใจที่ผิดพลาด ทั้งยังให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลสามารถที่จะขอให้ผู้ควบคุมข้อมูลส่วนบุคคลโอนข้อมูลของตนไปยังผู้ควบคุมข้อมูล

ส่วนบุคคลอื่นอันเป็นการส่งเสริมการแข่งขันเสรีทำให้เจ้าของข้อมูลส่วนบุคคลสามารถเปลี่ยนแปลงผู้ให้บริการได้ง่ายขึ้น นอกจากนี้ยังเพิ่มสิทธิแก่เจ้าของข้อมูลส่วนบุคคลให้สามารถขอแก้ไขข้อมูลส่วนบุคคลของตนได้ มีสิทธิในการยับยั้งการประมวลผลข้อมูล และสิทธิในการเพิกถอนความยินยอมอีกด้วย

ในกรณีของการเก็บรวบรวมข้อมูล IP Address หรือ Mac Address Article 29 Data Protection Working Party เห็นว่าควรให้ถือเป็นข้อมูลส่วนบุคคล[12]เนื่องจากข้อมูล IP Address และ Mac Address นี้สามารถเชื่อมโยงไปยังเจ้าของได้ง่ายไม่ว่าด้วยการนำข้อมูลนี้ไปประกอบกับข้อมูลที่ผู้ควบคุมข้อมูลส่วนบุคคลมีอยู่หรือได้รับมาจากเจ้าของข้อมูลส่วนบุคคล หรือนำไปประกอบกับข้อมูลอื่นที่เจ้าของข้อมูลได้เปิดเผยไว้เป็นสาธารณะ และการประมวลผลข้อมูลส่วนบุคคลเพื่อการตลาดทั้ง Directive 95/46/EC และ General Data Protection Regulation เห็นว่าเป็นสิ่งที่รบกวนความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคล กฎเกณฑ์ทั้งสองฉบับจึงให้สิทธิในการคัดค้านการประมวลผลข้อมูลเพื่อการตลาด

3.3 กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศอังกฤษ

ประเทศอังกฤษมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลคือ The Data protectionAct 1998 หรือ DPAมีขึ้นเพื่อเป็นการอนุวัติการให้เป็นตาม The European Data Protection Directive หรือ Directive 95/46/ECโดยได้รวบรวมกฎหมายคุ้มครองข้อมูลส่วนบุคคลทั้งหลายที่มีอยู่เข้าด้วยกันและร่างขึ้นเพื่อทดแทนกฎหมายอื่นๆ เช่น The data protection Act 1984 และ The Access to Personal Files Act 1987 เป็นต้น The Data protection Act 1998 มีผลใช้บังคับในวันที่ 1 มีนาคม 2000 พร้อมด้วยข้อยกเว้นให้บทบัญญัติบางมาตรามีผลบังคับใช้ในเดือนตุลาคม 2001วัตถุประสงค์ของ The data protection Act 1984 คือเพื่อควบคุมการจัดการข้อมูลส่วนบุคคลและเพื่อให้สิทธิแก่ประชาชนซึ่งเป็นเจ้าของข้อมูลที่ถูกเก็บรวบรวม

พระราชบัญญัติฉบับดังกล่าวใน Section 1[13]ให้ความคุ้มครองแก่ข้อมูลซึ่งถูกจัดเก็บโดยเครื่องมืออัตโนมัติเพื่อวัตถุประสงค์ดังที่ได้แจ้งไว้ หรือถูกจัดเก็บโดยมีวัตถุประสงค์เพื่อการดำเนินการ

---

[12] Aricle 29 Data Protection Working Party, “Opinion 4/2007 on the concept of personal data”,Accedssed 1 February 2016, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

[13]**Data Protection Act 1991**

โดยเครื่องมืออัตโนมัติดังกล่าว หรือถูกจัดเก็บเป็นส่วนหนึ่งของระบบการจัดเก็บข้อมูลที่เกี่ยวข้อง (Relevant filing system) หรือโดยมีวัตถุประสงค์เพื่อให้ข้อมูลดังกล่าวเป็นส่วนหนึ่งของระบบการจัดเก็บข้อมูลที่เกี่ยวข้อง หรือเป็นข้อมูลซึ่งสามารถเข้าถึงได้ตามที่ระบุไว้ในมาตรา 68 โดยข้อมูลที่ได้รับความคุ้มครองภายใต้พระราชบัญญัติดังกล่าวได้แก่ข้อมูลที่ถูกจัดเก็บโดยทางคอมพิวเตอร์ หรือข้อมูลซึ่งได้รับมาในรูปของแผ่นกระดาษโดยผู้ประมวลผลข้อมูลประสงค์จัดเก็บในรูปของข้อมูลทางคอมพิวเตอร์ย่อมได้รับความคุ้มครองเช่นกัน[14] DPA กำหนดหลักการในการคุ้มครองข้อมูลส่วนบุคคลไว้ 8 ประการ ดังนี้

1. ข้อมูลส่วนบุคคลจะต้องถูกประมวลผลอย่างเป็นธรรมและชอบด้วยกฎหมาย และโดยเฉพาะอย่างยิ่งข้อมูลนั้นต้องไม่ถูกประมวลผล เว้นแต่

a. เป็นไปตามเงื่อนไขข้อใดข้อหนึ่งของ Schedule 2 กล่าวคือ

a.1 เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมในการประมวลผล

a.2การประมวลผลนั้นจำเป็น

(a) เพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือ

(b) เพื่อปฏิบัติตามคำขอของเจ้าของข้อมูลส่วนบุคคลเกี่ยวกับความคิดเห็นในการเข้าทำสัญญา

a.3 การประมวลผลนั้นจำเป็นเพื่อปฏิบัติหน้าที่ตามกฎหมายซึ่งใช้บังคับต่อผู้ควบคุมข้อมูลส่วนบุคคล หรือหน้าที่อื่นตามที่ระบุในสัญญา

Section 1 (1)

"Data" means information which-

(a) Is being processed by means of equipment operating automatically in response to instructions given for that purpose,

(b) Is recorded with the intention that it should be processed by means of such equipment,

(c) Is recorded as part of a relevant filing system or with the intention that it should form part of relevant filing system,

(d) Is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d)

[14] ICO, "The guide to data protection",Accedssed4 February 2016, https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/

a.4 การประมวลผลนั้นเป็นการจำเป็นเพื่อรักษาผลประโยชน์สำคัญของเจ้าของข้อมูลส่วนบุคคล

a.5 การประมวลผลนั้นเป็นการจำเป็น

(a) เพื่อกระบวนการยุติธรรม

(aa) เพื่อการปฏิบัติหน้าที่ของสภาผู้แทนราษฎร

(b) เพื่อการปฏิบัติหน้าที่ของบุคคลตามกฎหมาย

(c) เพื่อการปฏิบัติหน้าที่ของกษัตริย์ หรือ Minister of the Crown หรือหน่วยงานรัฐบาล

(d) เพื่อเป็นการปฏิบัติหน้าที่ของบุคคลใดๆเพื่อประโยชน์สาธารณะ

และ

b. หากเป็นข้อมูลที่มีความอ่อนไหว ต้องเป็นไปตามเงื่อนไขข้อใดข้อหนึ่งของ Schedule 3 กล่าวคือ

b.1 เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมโดยชัดแจ้ง

b.2 การประมวลผลนั้นเป็นการจำเป็นเพื่อวัตถุประสงค์ในการใช้สิทธิหรือหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลตามกฎหมายเกี่ยวกับการจ้างงาน

b.3 การประมวลผลนั้นเป็นการจำเป็น

(a) เพื่อปกป้องประโยชน์สำคัญของเจ้าของข้อมูลส่วนบุคคลไม่อาจขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลได้ หรือผู้ควบคุมข้อมูลส่วนบุคคลเห็นว่าอาจไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือ

(b) เพื่อปกป้องผลประโยชน์สำคัญของบุคคลอื่นเมื่อเจ้าของข้อมูลส่วนบุคคลเพิกถอนความยินยอมอย่างไม่มีเหตุผล

b.4 การประมวลผลนั้น

(a) ได้กระทำโดยเป็นกิจกรรมที่ชอบด้วยกฎหมายขององค์กรหรือบุคคลนั้นซึ่งมิได้กระทำเพื่อแสวงหากำไรและมีขึ้นเพื่อวัตถุประสงค์ทางการเมือง ปรัชญา ศาสนา หรือสหภาพแรงงาน

(b) ได้กระทำเพื่อป้องกันสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

(c) เกี่ยวกับปัจเจกบุคคลซึ่งเป็นสมาชิกของบุคคลหรือสมาคมหรือมีความสัมพันธ์พิเศษเกี่ยวกับวัตถุประสงค์ของบุคคลหรือสมาคมนั้น

(d) ไม่เปิดเผยข้อมูลนั้นต่อบุคคลที่สามโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

b.5 ข้อมูลซึ่งได้ถูกเปิดเผยไว้เป็นสาธารณะภายใต้การตัดสินใจของเจ้าของข้อมูลส่วนบุคคล

b.6 การประมวลผลนั้น

(a) จำเป็นเพื่อวัตถุประสงค์ในการดำเนินคดี

(b) จำเป็นเพื่อการขอคำปรึกษาทางกฎหมาย

(c) จำเป็นเพื่อการก่อตั้ง ใช้ หรือต่อสู้ทางกฎหมาย

b.7 การประมวลผลนั้นจำเป็น

(a) เพื่อกระบวนการยุติธรรม

(aa) เพื่อการปฏิบัติหน้าที่ของสภาผู้แทนราษฎร

(b) เพื่อการปฏิบัติหน้าที่ของบุคคลตามกฎหมาย

(c) เพื่อการปฏิบัติหน้าที่ของกษัตริย์ หรือ Minister of the Crown หรือหน่วยงานรัฐบาล

b.8การประมวลผลนั้น

(a) เป็นการเปิดเผยข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลที่มีความอ่อนไหวโดยบุคคลที่เป็นสมาชิกขององค์กรต่อต้านการทุจริต

(b) เป็นการจำเป็นเพื่อป้องกันการทุจริต

b.9 การประมวลผลนั้นเป็นการจำเป็นเพื่อวัตถุประสงค์ทางการแพทย์

2. ข้อมูลส่วนบุคคลนั้นต้องได้รับมาเพื่อวัตถุประสงค์ที่ได้ระบุไว้และชอบด้วยกฎหมายและต้องไม่ประมวลผลเพิ่มเติมอันเป็นการขัดกับวัตถุประสงค์ที่ได้ระบุไว้

3. ข้อมูลส่วนบุคคลต้องเพียงพอ เกี่ยวข้องและไม่เกินกว่าที่จำเป็นเพื่อวัตถุประสงค์ที่ข้อมูลนั้นจะถูกประมวลผล

4. ข้อมูลส่วนบุคคลต้องถูกต้อง และในกรณีจำเป็นข้อมูลส่วนบุคคลนั้นต้องเป็นปัจจุบัน

5. ข้อมูลส่วนบุคคลที่ถูกประมวลผลเพื่อวัตถุประสงค์ใดวัตถุประสงค์หนึ่งต้องไม่ถูกเก็บไว้เกินกว่าเวลาที่จำเป็น

6. ข้อมูลส่วนบุคคลต้องถูกประมวลผลโดยคำนึงถึงสิทธิของเจ้าของข้อมูลส่วนบุคคลตามที่บัญญัติไว้ในพระราชบัญญัตินี้

7. ต้องมีมาตรการทางเทคนิคและทางองค์กรที่เหมาะสมเพื่อป้องกันการประมวลผลที่ไม่มีอำนาจหรือไม่ชอบด้วยกฎหมาย และป้องกันข้อมูลส่วนบุคคลจากการสูญหาย การทำลาย หรือความเสียหาย

8. ข้อมูลส่วนบุคคลนั้นต้องไม่ถูกโอนไปยังประเทศหรือดินแดนอื่นนอกเขตเศรษฐกิจยุโรป เว้นแต่ประเทศหรือดินแดนนั้นมีระดับการในการคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลที่เพียงพอ

DPA ได้กำหนดคำนิยามไว้ในมาตรา 1 ซึ่งมีสาระสำคัญดังนี้

“ข้อมูล” หมายถึงข้อมูลซึ่ง

a. ถูกประมวลผลโดยเครื่องมือที่ทำงานโดยอัตโนมัติเป็นการตอบสนองต่อคำสั่งตามวัตถุประสงค์นั้น

b. ถูกบันทึกเพื่อวัตถุประสงค์ที่จะประมวลผลข้อมูลโดยเครื่องมืออัตโนมัตินั้น

c. ถูกบันทึกโดยถือเป็นส่วนหนึ่งของระบบการจัดเก็บที่เกี่ยวข้องโดยมีวัตถุประสงค์เพื่อให้เป็นส่วนหนึ่งของระบบจัดเก็บนั้น

d. มิใช่กรณีตามข้อ a. b. หรือ c. แต่เป็นส่วนหนึ่งของบันทึกที่สามารถเข้าถึงได้ตามที่ระบุในมาตรา 68

e. ข้อมูลที่ถูกบันทึกโดยหน่วยงานของรัฐและมิใช่กรณีตามข้อ a. ถึง d.

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายถึง บุคคลซึ่งไม่ว่าจะเป็นบุคคลเพียงคนเดียวหรือเป็นกลุ่มบุคคล ตัดสินใจเกี่ยวกับวัตถุประสงค์และวิธีซึ่งข้อมูลส่วนบุคคลนั้นถูกประมวลผลหรือจะถูกประมวลผล

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายถึง บุคคลใดๆนอกจากลูกจ้างของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งประมวลผลข้อมูลนั้นในนามของผู้ควบคุมข้อมูลส่วนบุคคล

“เจ้าของข้อมูลส่วนบุคคล” หมายถึง ปัจเจกบุคคลธรรมดาซึ่งข้อมูลส่วนบุคคลเป็นเรื่องของบุคคลนั้น

“ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลซึ่งเกี่ยวข้องกับปัจเจกบุคคลซึ่งยังมีชีวิตอยู่ซึ่งสามารถถูกระบุตัวได้

a. จากข้อมูลนั้น หรือ

b. ข้อมูลนั้นและข้อมูลอื่นซึ่งอยู่ในความครอบครองหรืออาจเข้ามาอยู่ในความครอบครองของผู้ควบคุมข้อมูลส่วนบุคคล

และให้รวมถึงการแสดงความเห็นเกี่ยวกับปัจเจกบุคคลและการแสดงเจตจำนงใดๆของผู้ควบคุมข้อมูลส่วนบุคคลหรือบุคคลอื่นเกี่ยวกับปัจเจกบุคคลนั้น

นอกจากนี้ในมาตรา 2 กำหนดให้ “ข้อมูลส่วนบุคคลซึ่งซึ่งมีความอ่อนไหว” หมายถึงข้อมูลส่วนบุคคลซึ่งประกอบด้วยข้อมูลดังต่อไปนี้

a. เชื้อชาติ หรือชาติพันธุ์กำเนิดของเจ้าของข้อมูลส่วนบุคคล

b. ความคิดเห็นทางการเมืองของเจ้าของข้อมูลส่วนบุคคล

c. ความเชื่อในทางศาสนา หรือความเชื่ออื่นซึ่งมีลักษณะเช่นเดียวกันของเจ้าของข้อมูลส่วนบุคคล

d. เจ้าของข้อมูลส่วนบุคคลเป็นสมาชิกของสหภาพแรงงานหรือไม่

e. สุขภาพกายหรือสุขภาพจิตใจหรืออาการป่วยของเจ้าของข้อมูลส่วนบุคคล

f. รสนิยมทางเพศของเจ้าของข้อมูลส่วนบุคคล

g. การกระทำความผิดหรือถูกกล่าวหาว่ากระทำความผิดของเจ้าของข้อมูลส่วนบุคคล

h. การดำเนินคดีในความผิดใดๆที่กระทำหรือถูกกล่าวหาว่ากระทำโดยเจ้าของข้อมูลส่วนบุคคล การยกเลิกการดำเนินคดี หรือคำตัดสินของศาลในการดำเนินคดี

โดยพระราชบัญญัติดังกล่าวมีสาระสำคัญดังนี้

1. ผลบังคับใช้

พระราชบัญญัติดังกล่าวใช้บังคับแก่ผู้ควบคุมข้อมูลส่วนบุคคลในกรณีที่

1. ผู้ควบคุมข้อมูลส่วนบุคคลนั้นตั้งอยู่ในประเทศอังกฤษและข้อมูลส่วนบุคคลถูกประมวลผลในประเทศอังกฤษ หรือ

2. ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งมิได้ตั้งขึ้นในประเทศอังกฤษหรือเขตเศรษฐกิจยุโรป (EEA) แต่ได้ใช้เครื่องมือในประเทศอังกฤษเพื่อประมวลผลข้อมูลส่วนบุคคลนั้นอันมิได้มีวัตถุประสงค์เพียงโอนข้อมูลผ่านประเทศอังกฤษเท่านั้น ในกรณีดังกล่าวผู้ควบคุมข้อมูลส่วนบุคคลต้องตั้งตัวแทนในประเทศอังกฤษ

โดยผู้ควบคุมข้อมูลจะถูกถือว่าตั้งอยู่ในประเทศอังกฤษในกรณีดังต่อไปนี้คือ

a. ปัจเจกบุคคลซึ่งมีถิ่นที่อยู่ในประเทศอังกฤษ

b. นิติบุคคลซึ่งตั้งตามกฎหมายของประเทศอังกฤษ

c. ห้างหุ้นส่วนหรือสมาคมซึ่งมิใช่นิติบุคคลตั้งขึ้นตามกฎหมายของประเทศอังกฤษ

d. บุคคลใดๆซึ่งมิใช่กรณีตาม a. b. หรือ c. แต่มีสำนักงาน สาขา หรือตัวแทนซึ่งดำเนินกิจกรรม หรือมีวิธีปฏิบัติเป็นปกติในประเทศอังกฤษ

2. สิทธิของเจ้าของข้อมูลส่วนบุคคล

2.1สิทธิในการเข้าถึงข้อมูลส่วนบุคคลของตน

เมื่อเจ้าของข้อมูลร้องขอเป็นหนังสือเจ้าของข้อมูลส่วนบุคคลมีสิทธิได้รับการแจ้งถึงการประมวลผลข้อมูลส่วนบุคคลของตนโดยองค์กร โดยต้องแจ้งถึงข้อมูลซึ่งเกี่ยวกับเจ้าของข้อมูลส่วนบุคคล วัตถุประสงค์ซึ่งข้อมูลส่วนบุคคลนั้นจะถูกประมวลผลหรืออาจถูกประมวลผล และผู้รับหรือประเภทของผู้รับซึ่งข้อมูลส่วนบุคคลนั้นอาจถูกเปิดเผยนอกจากนี้การแจ้งนั้นต้องอยู่ใน

รูปแบบซึ่งเจ้าของข้อมูลส่วนบุคคลสามารถเข้าใจได้ถึงข้อมูลส่วนบุคคลซึ่งเกี่ยวกับตนและข้อมูลเกี่ยวกับแหล่งที่มาของข้อมูลส่วนบุคคลซึ่งผู้ควบคุมข้อมูลส่วนบุคคลมีอยู่ทั้งนี้ผู้ควบคุมข้อมูลส่วนบุคคลอาจร้องขอให้เจ้าของข้อมูลส่วนบุคคลส่งเอกสารหรือหลักฐานเพิ่มเติมได้เพื่อยืนยันตัวเจ้าของข้อมูลส่วนบุคคล และผู้ควบคุมข้อมูลส่วนบุคคลไม่จำต้องแจ้งถึงข้อมูลนั้นจนกว่าเจ้าของข้อมูลส่วนบุคคลจะได้ส่งเอกสารหรือหลักฐานตามที่ถูกร้องขอ

หากการเปิดเผยข้อมูลส่วนบุคคลนั้นอาจทำให้ข้อมูลส่วนบุคคลของปัจเจกบุคคลของผู้อื่นถูกเปิดเผย ผู้ควบคุมข้อมูลไม่จำเป็นต้องให้ข้อมูลแก่เจ้าของข้อมูลส่วนบุคคลตามที่ร้องขอ เว้นแต่ปัจเจกบุคคลอื่นได้ให้ความยินยอมในการเปิดเผยข้อมูลส่วนบุคคลแก่บุคคลที่ร้องขอ หรือมีเหตุผลอันสมควรที่จะปฏิบัติตามคำร้องขอของเจ้าของข้อมูลส่วนบุคคลโดยปัจเจกบุคคลอื่นมิได้ให้ความยินยอมในการเปิดเผยซึ่งในกรณีเช่นนี้ผู้ควบคุมข้อมูลส่วนบุคคลต้องพิจารณาถึง

1. หน้าที่ในการรักษาข้อมูลอันผู้ควบคุมข้อมูลส่วนบุคคลมีต่อปัจเจกบุคคลอื่น

2. กระบวนการซึ่งผู้ควบคุมข้อมูลส่วนบุคคลกระทำเพื่อขอความยินยอมจากปัจเจกบุคคลอื่น

3. ปัจเจกบุคคลอื่นสามารถให้ความยินยอมได้หรือไม่ และ

4. ปัจเจกบุคคลอื่นได้ปฏิเสธการให้ความยินยอมหรือไม่

ในกรณีที่ข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลถูกประมวลผลโดยวิธีอัตโนมัติเพื่อวัตถุประสงค์ในการประเมินข้อเท็จจริงเกี่ยวกับเจ้าของข้อมูลส่วนบุคคล เช่น ประสิทธิภาพในการทำงาน ความน่าเชื่อถือทางเครดิต ความน่าไว้วางใจหรือความประพฤติของเจ้าของข้อมูลส่วนบุคคล ซึ่งการประเมินข้อเท็จจริงดังกล่าวเพื่อประเมินข้อเท็จจริงใดๆและอาจส่งผลกระทบอย่างมีนัยสำคัญแก่เจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งแก่เจ้าของข้อมูลส่วนบุคคลถึงเหตุผลที่ใช้ในการประเมินนั้น

เมื่อผู้ควบคุมข้อมูลส่วนบุคคลได้แจ้งข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลตามคำขอแล้ว หากเจ้าของข้อมูลส่วนบุคคลมีการร้องขอเช่นเดียวกันหรือคล้ายกันอีกผู้ควบคุมข้อมูลส่วนบุคคลไม่จำต้องดำเนินการตามคำขอภายหลังเว้นแต่ระยะเวลาจะได้ผ่านไปพอสมควรแล้ว โดยระยะเวลาผ่านไปพอสมควรนั้นให้พิจารณาถึงลักษณะของข้อมูลส่วนบุคคล วัตถุประสงค์ซึ่งข้อมูลส่วนบุคคลนั้นถูกประมวลผล และความถี่ซึ่งข้อมูลส่วนบุคคลนั้นถูกแก้ไข

2.2 สิทธิในการคัดค้านการประมวลผลที่อาจก่อให้ความเสียหายหรือความวิตกกังวลอย่างรุนแรง

ปัจเจกบุคคลมีสิทธิแจ้งเป็นหนังสือไปยังผู้ควบคุมข้อมูลส่วนบุคคลไม่ว่าในเวลาใดๆ เรียกร้องให้ผู้ควบคุมข้อมูลส่วนบุคคลหยุดหรือไม่เริ่มการประมวลผลหรือไม่ประมวลผลเพื่อ

วัตถุประสงค์ที่ได้ระบุไว้ หรือโดยวิธีการที่ระบุไว้ภายในเวลาอันสมควรในสองกรณี คือ การประมวลผลข้อมูลนั้น หรือการประมวลผลเพื่อวัตถุประสงค์หรือโดยวิธีที่ระบุไว้นั้นก่อให้เกิดหรืออาจก่อให้เกิดความเสียหายที่มีนัยสำคัญหรือความวิตกกังวลอย่างรุนแรงแก่บุคคลนั้นหรือบุคคลอื่น และความเสียหายหรือความวิตกกังวลนั้นไม่สมควรเกิดขึ้น

เมื่อผู้ควบคุมข้อมูลส่วนบุคลได้รับการแจ้งเป็นหนังสือแล้ว ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งเป็นหนังสือแก่เจ้าของข้อมูลส่วนบุคคลภายใน 20 วันระบุถึง

1. ผู้ควบคุมข้อมูลส่วนบุคคลกระทำตามหรือมีเจตนากระทำตามหนังสือแจ้งของเจ้าของข้อมูลส่วนบุคคล หรือ

2. ถึงเหตุผลของผู้ควบคุมข้อมูลส่วนบุคคลเกี่ยวกับหนังสือแจ้งของเจ้าของข้อมูลส่วนบุคคลในส่วนที่ไม่สมเหตุผลและส่วนที่ผู้ควบคุมข้อมูลส่วนบุคคลจะดำเนินการตามหรือมีเจตนาดำเนินการตามหนังสือนั้น

2.3 สิทธิในการคัดค้านการประมวลผลเพื่อวัตถุประสงค์ทางการตลาดแบบตรง

ปัจเจกบุคคลมีสิทธิไม่ว่าในเวลาใดๆแจ้งเป็นหนังสือไปยังผู้ควบคุมข้อมูลส่วนบุคคลเรียกร้องให้ผู้ควบคุมข้อมูลส่วนบุคคลหยุดหรือไม่เริ่มต้นซึ่งการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลนั้นเพื่อวัตถุประสงค์ทางการตลาดแบบตรงภายในเวลาอันสมควร ทั้งนี้การตลาดแบบตรง หมายถึงการสื่อสารไม่ว่าโดยวิธีใดๆซึ่งสื่อโฆษณาหรือสื่อการตลาดมุ่งโดยตรงไม่ยังปัจเจกบุคคลคนใดหนหนึ่งโดยเฉพาะ

2.4 สิทธิในการคัดค้านการประมวลผลโดยวิธีอัตโนมัติ

ปัจเจกบุคคลมีสิทธิไม่ว่าในเวลาใดๆแจ้งเป็นหนังสือไปยังผู้ควบคุมข้อมูลส่วนบุคคลเพื่อร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลยืนยันว่าจะไม่มีการตัดสินใจเกี่ยวกับหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลที่อาจส่งผลกระทบอย่างมีนัยสำคัญต่อปัจเจกบุคคลนั้นอันได้กระทำโดยอาศัยการประมวลผลโดยวิธีอัตโนมัติเท่านั้น โดยที่การประมวลผลดังกล่าวเกี่ยวกับการประเมินสิ่งต่างๆเกี่ยวกับเจ้าของข้อมูลส่วนบุคคล เช่น ประสิทธิภาพในการทำงาน ความน่าเชื่อถือทางเครดิต ความน่าชื่อถือหรือความประพฤติของเจ้าของข้อมูลส่วนบุคคล เป็นต้น

2.5 สิทธิเกี่ยวกับการตัดสินใจโดยวิธีอัตโนมัติ

ปัจเจกบุคคลมีสิทธิแจ้งเป็นหนังสือไปยังผู้ควบคุมข้อมูลส่วนบุคคลไม่ว่าในเวลาใดๆเพื่อเรียกร้องให้ผู้ควบคุมข้อมูลส่วนบุคคลทำให้มั่นใจว่าจะไม่มีการตัดสินใจที่มีพื้นฐานบนการประมวลผลโดยวิธีอัตโนมัติเพียงอย่างเดียวซึ่งกระทำโดยหรือกระทำในนามของผู้ควบคุมข้อมูลส่วนบุคคลอันจะส่งผลกระทบต่อปัจเจกบุคคลโดยการประมวลผลดังกล่าวนี้มีวัตถุประสงค์เพื่อประเมินสิ่งต่างๆเกี่ยวกับปัจเจกบุคคลนั้น เช่น ประสิทธิภาพในการทำงานของบุคคลนั้น ความน่าเชื่อถือด้าน

เครดิต หรือความประพฤติของบุคคลนั้น อย่างไรก็ตามหากมิได้มีหนังสือแจ้งของปัจเจกบุคคลและเมื่อมีการตัดสินใจที่ส่งผลกระทบอย่างมีนัยสำคัญโดยมีพื้นฐานจากการประมวลผลโดยวิธีอัตโนมัติเพียงอย่างเดียวผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งไปยังเจ้าของข้อมูลส่วนบุคคลถึงการตัดสินใจนั้นโดยเร็วและปัจเจกบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลพิจารณาการตัดสินใจหรือขอให้ตัดสินใจใหม่โดยต้องแจ้งเป็นหนังสือไปยังผู้ควบคุมข้อมูลส่วนบุคคลภายใน 20 วันนับแต่วันที่ได้รับแจ้งการตัดสินใจจากผู้ควบคุมข้อมูลส่วนบุคคล

เมื่อมีการแจ้งเป็นหนังสือจากปัจเจกบุคคลให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการตัดสินใจใหม่หรือพิจารณาการตัดสินใจนั้น ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งเป็นหนังสือไปยังเจ้าของข้อมูลส่วนบุคคลภายใน 20 วันนับแต่วันที่ได้รับแจ้งเป็นหนังสือจากปัจเจกบุคคลระบุวิธีการที่ผู้ควบคุมข้อมูลส่วนบุคคลจะดำเนินการตามคำขอ แต่หากผู้ควบคุมข้อมูลส่วนบุคคลได้รับภายใต้บทบัญญัติเรื่องการตัดสินใจที่ได้รับยกเว้นซึ่งกำหนดไว้ในมาตรา 12(4) ปัจเจกบุคคลไม่มีสิทธิห้ามผู้ควบคุมข้อมูลส่วนบุคคลมิให้ทำการตัดสินใจนั้น

ข้อยกเว้นในการตัดสินใจหมายถึง การตัดสินใจซึ่ง

a. เป็นการตัดสินใจอัน

a.1 ได้กระทำเป็นส่วนหนึ่งของขั้นตอนเพื่อ

i เพื่อวัตถุประสงค์ในการพิจารณาว่าจะเข้าทำสัญญากับปัจเจกบุคคลนั้นหรือไม่

ii มีการแสดงความคิดเห็นเกี่ยวกับการเข้าทำสัญญา หรือ

iii เพื่อปฏิบัติตามสัญญา หรือ

a.2เป็นกรณีซึ่งกฎหมายอนุญาตหรือบังคับไว้

นอกจากนี้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถอ้างข้อยกเว้นในกรณีดังกล่าวได้ต่อเมื่อผลของการตัดสินใจคือเพื่อทำตามคำร้องขอของปัจเจกบุคคล หรือเป็นกระบวนการซึ่งได้กระทำเพื่อปกป้องประโยชน์อันชอบด้วยกฎหมายของเจ้าของข้อมูลส่วนบุคคล

b. เป็นการตัดสินใจซึ่งได้กระทำในสถานการณ์อื่นๆตามคำสั่งของรัฐมนตรีว่าการกระทรวงกิจการการรัฐธรรมนูญ (Secretary of State for Constitutional Affairs)

หากปัจเจกบุคคลได้รับความเสียหายจากการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่ปฏิบัติตามบทบัญญัตินี้ ปัจเจกบุคคลมีสิทธิได้รับค่าสินไหมทดแทนเพื่อความเสียหายจากผู้ควบคุมข้อมูลส่วนบุคคล และหากศาลเห็นว่าข้อมูลที่เกี่ยวกับเจ้าของข้อมูลส่วนบุคคลไม่ถูกต้อง ศาลมีอำนาจสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลแก้ไข ลบ หรือทำลายข้อมูลส่วนซึ่งอยู่ในความครอบครองของผู้ควบคุมข้อมูลส่วนบุคคลและใช้ข้อมูลส่วนบุคคลนั้นในการให้เหตุผลเกี่ยวกับเจ้าของข้อมูลส่วนบุคคลนั้นได้

3. หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลในการขึ้นทะเบียนเป็นผู้ควบคุมข้อมูลส่วนบุคคล

เมื่อกล่าวถึง “รายการที่ต้องจดทะเบียน” ซึ่งเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคลในหัวข้อนี้ให้มีความหมายถึง

a. ชื่อและที่อยู่ของผู้ควบคุมข้อมูลส่วนบุคล

b. ชื่อและที่อยู่ของตัวแทน ในกรณีผู้ควบคุมข้อมูลส่วนบุคลได้แต่ตั้งตัวแทนตามที่บัญญัติไว้ในพระราชบัญญัตินี้

c. คำอธิบายถึงลักษณะของข้อมูลส่วนบุคคลที่ถูกหรือจะถูกประมวลผลโดยหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล และบอกถึงประเภทของข้อมูลส่วนบุคคล

d. การบรรยายถึงลักษณะของผู้รับคนหนึ่งหรือหลายคนซึ่งผู้ควบคุมข้อมูลส่วนบุคคลมีเจตจำนงเปิดเผยข้อมูลส่วนบุคคลนั้น

e. ชื่อ หรือคำบรรยายถึงประเทศหรือดินแดนซึ่งอยู่นอกเขตเศรษฐกิจยุโรปซึ่งผู้ควบคุมข้อมูลส่วนบุคคลจะโอนข้อมูลส่วนบุคคลนั้นไปไม่ว่าโดยทางตรงหรือทางอ้อม หรือผู้ควบคุมข้อมูลส่วนบุคคลมีเจตจำนงโอนข้อมูลนั้นไปไม่ว่าทางตรงหรือทางอ้อม

นอกจากนี้เมื่อพูดถึงที่อยู่ของผู้ควบคุมข้อมูลส่วนบุคคลหากผู้ควบคุมข้อมูลส่วนบุคคลเป็นนิติบุคคลให้หมายถึงที่อยู่ตามที่นิติบุคคลนั้นได้จดทะเบียนไว้ และหากผู้ควบคุมข้อมูลส่วนบุคคลเป็นบุคคลซึ่งประกอบธุรกิจและมิใช่บริษัทจดทะเบียนให้ที่อยู่ของบุคคลดังกล่าวหมายถึงสถานประกอบธุรกิจอันเป็นสำนักงานใหญ่ที่ตั้งอยู่ในประเทศอังกฤษ

ในการขึ้นทะเบียนผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งไปยังคณะกรรมการผู้มีหน้าที่รับผิดชอบในการขึ้นทะเบียนและเสียค่าธรรมเนียมตามที่ได้กำหนดไว้ในข้อบังคับ โดยการแจ้งดังกล่าวต้องระบุรายการที่ต้องจดทะเบียนและคำบรรยายถึงมาตรการที่จะใช้เพื่อปฏิบัติตามหลักการในการคุ้มครองข้อมูลส่วนบุคคลทั้ง 7 ประการ เมื่อมีการขึ้นทะเบียนแล้วคณะกรรมการจะต้องเก็บรักษาไว้ซึ่งบัญชีของบุคลที่ได้ขึ้นทะเบียนและจัดทำการลงทะเบียนในบัญชีอันประกอบไปด้วย 1. รายการที่ต้องจดทะเบียน และ 2. ข้อมูลอื่นๆตามที่คณะกรรมการกำหนด ข้อมูลเกี่ยวกับการขึ้นทะเบียนนี้จะถูกจัดเก็บไว้ไม่เกินสิบสองเดือนหรือกำหนดเวลาอื่นตามข้อบังคับเว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลได้เสียค่าธรรมเนียมตามข้อบังคับ

คณะกรรมการจะต้องจัดให้ประชาชนสามารถตรวจสอบบัญชีข้อมูลการลงทะเบียนได้โดยไม่เสียค่าใช้จ่าย และอาจมีการอำนวยความสะดวกอื่นๆเพื่อให้ประชาชนสามารถตรวจสอบข้อมูลนั้นได้โดยไม่เสียค่าใช้จ่ายทั้งนี้ตามที่คณะกรรมการเห็นสมควร หากมีการเปลี่ยนแปลงรายการที่ต้องจดทะเบียน ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งแก่คณะกรรมการ ซึ่งวัตถุประสงค์ของการแจ้งการเปลี่ยนแปลง คือ

1. ให้การลงทะเบียนนั้นมีข้อมูลที่เป็นปัจจุบันเกี่ยวกับชื่อที่อยู่ แนวปฏิบัติที่ใช้อยู่ในปัจจุบัน หรือเจตจำนงของผู้ควบคุมข้อมูลส่วนบุคคลเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลและ

2. ได้มีการจัดเตรียมคำบรรยายถึงมาตรการเพื่อปฏิบัติตามหลักการในการคุ้มครองข้อมูลส่วนบุคคลทั้ง 7 ประการอันได้ใช้อยู่ในปัจจุบันแก่คณะกรรมการ

หากผู้ควบคุมข้อมูลส่วนบุคคลมิได้ขึ้นทะเบียนเป็นผู้ควบคุมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลนั้นไม่สามารถประมวลผลข้อมูลส่วนบุคคลได้อย่างไรก็ตามข้อยกเว้นของการขึ้นทะเบียนมีทั้งหมด 3 ประการ กล่าวคือ

a. เมื่อรัฐมนตรีว่าการกระทรวงกิจการการรัฐธรรมนูญ (Secretary of State for Constitutional Affairs) เห็นว่าการประมวลผลนั้นไม่กระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

b. เป็นการประมวลผลซึ่งมีวัตถุประสงค์เพียงเพื่อการยืนยันการจดทะเบียน

c. ข้อมูลส่วนบุคคลนั้นไม่ตกอยู่ภายใต้ความหมายของข้อมูลตามพระราชบัญญัตินี้

4. ข้อยกเว้น

DPA ได้กำหนดให้การเก็บรวบรวมข้อมูลส่วนบุคคล การประมวลผลและการเปิดเผยข้อมูลนั้นต้องเป็นไปตามหลักการคุ้มครองข้อมูลส่วนบุคคลและ Schedule 2 หรือ Schedule 3 แล้วแต่กรณี และได้กำหนดข้อยกเว้นไว้สำหรับข้อมูลบางประเภทซึ่งผู้ควบคุมข้อมูลส่วนบุคคลไม่จำเป็นต้องดำเนินการตามหลักการคุ้มครองข้อมูลส่วนบุคคลและ Schedule 2 หรือ Schedule 3 ได้แก่ การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลเพื่อเหตุผลทางความมั่นคงของประเทศ เพื่อเหตุผลทางอาชญากรรรมหรือภาษีอากร เพื่อสุขภาพ การศึกษาและสังคมสงเคราะห์ เพื่อการเขียนข่าว การประพันธ์หรือศิลปะ และเพื่อการวิจัย ประวัติศาสตร์หรือสถิติ นอกจากนี้ DPA ยังกำหนดให้ข้อมูลส่วนบุคคลที่ถูกประเมินผลโดยปัจเจกบุคคลเพื่อวัตถุประสงค์เกี่ยวกับงานบ้าน ครอบครัว หรือส่วนตัว รวมถึงนันทนาการเป็นข้อมูลที่ได้รับการยกเว้นอีกด้วย

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของอังกฤษมีหลักเกณฑ์เช่นเดียวกันกับ Directive 95/46/EC เนื่องจากเป็นการออกกฎหมายมาเพื่ออนุวัตการให้เป็นไปตามDirective 95/46/EC โดย DPA กำหนดให้ข้อมูลส่วนบุคคลนอกจากจะหมายถึงข้อมูลที่สามารถระบุตัวเจ้าของข้อมูลส่วนบุคคลได้แล้วยังให้หมายรวมถึงข้อมูลที่เมื่อนำไปประกอบกับข้อมูลอื่นซึ่งผู้ควบคุมข้อมูลส่วนบุคคลมีอยู่หรืออาจเข้าถึงได้เป็นข้อมูลส่วนบุคคล การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องทำการขึ้นทะเบียนเป็นผู้ควบคุมข้อมูลส่วนบุคคลต่อคณะกรรมคุ้มครองข้อมูลส่วนบุคคลเสียก่อนจึงจะสามารถทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้ และยังให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลในการคัดค้าน

การประมวลผลที่อาจก่อให้ความเสียหายหรือความวิตกกังวลอย่างรุนแรง สิทธิในการยับยั้งการประมวลผล สิทธิในการคัดค้านการประมวลผลเพื่อการตลาดแบบตรง รวมถึงสิทธิในกาคัดค้านการประมวลผลโดยวิธีอัตโนมัติและการตัดสินใจโดยวิธีอัตโนมัติ

สำหรับข้อมูล Mac Address และ IP Address ยังมิได้มีการบัญญัติไว้โดยชัดแจ้ง แต่มีการตีความว่า Mac Address และ IP Address ประเภท Static เป็นข้อมูลส่วนบุคคลซึ่งผู้เก็บรวบรวมข้อมูลดังกล่าวต้องปฏิบัติตาม DPA แต่สำหรับ IP Address ประเภท Dynamic จะเป็นข้อมูลส่วนบุคคลต่อเมื่อผู้ควบคุมข้อมูลส่วนบุคคลมีข้อมูลอื่นประกอบซึ่งอาจบ่งชี้ไปยังเจ้าของข้อมูลส่วนบุคคลได้[15] นอกจากนี้หากผู้ควบคุมข้อมูลส่วนบุคคลทำการ Profiling เพื่อการโฆษณา เช่น โฆษณาโดยอาศัยข้อมูลจากการเยี่ยมชมเว็บไซต์ หรือสินค้าที่เจ้าของข้อมูลส่วนบุคคลเคยสั่งซื้อ ผู้โฆษณาต้องปฏิบัติ DPA นี้ แต่หากการโฆษณานั้นมิได้อาศัยข้อมูลจากเจ้าของข้อมูลส่วนบุคคลผู้โฆษณานั้นไม่จำเป็นต้องปฏิบัติตาม DPA[16]

นอกจากการคุ้มครองข้อมูลส่วนบุคคลของประเทศอังกฤษดังที่กล่าวมาแล้วประเทศอังกฤษยังให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลในการเข้าถึงข้อมูลของตนโดยใช้ชื่อโครงการว่า MiData โครงการนี้เริ่มต้นขึ้นในปี ค.ศ. 2011 เพื่อเพิ่มความคุ้มครองแก่เจ้าของข้อมูลส่วนบุคคลซึ่งเป็นผู้บริโภคให้ตระหนักถึงนิสัยในการใช้จ่ายและตัดสินใจเลือกในสิ่งที่คุ้มค่าที่สุด ภายใต้โครงการดังกล่าวเจ้าของข้อมูลส่วนบุคคลมีสิทธิดาวน์โหลดไฟล์ข้อมูลส่วนบุคคลซึ่งจะเก็บไว้ตามแบบมาตรฐานของ Midata เจ้าของข้อมูลส่วนบุคคลสามารถส่งไฟล์ดังกล่าวไปยังองค์กรที่ให้บริการการเปรียบเทียบ

---

[15] Information Commissioner's Office, "Data Protection Good Practice Note",Accedssed9 February 2016,https://www.google.co.th/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwijof62nMfLAhXGCI4KHWLFDpkQFggaMAA&url=http%3A%2F%2Fec.europa.eu%2Fjustice%2Fdata-protection%2Fdocument%2Fnational-policy%2Ffiles%2Fuk_outsourcing_guide_for_small_and_medium_businesses_en.pdf&usg=AFQjCNFGJxwa1b7lbKlkK1hSC70DfpUYzg&sig2=hqxOvbSdPsJehvRUUt0cbQ

[16] Information Commissioner's Office, "Direct Marketing Data protection Act Privacy and Electronic Communications Regulations",Accedssed9 February 2016,https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf

ลักษณะธุรกรรมและให้คำแนะนำเกี่ยวกับการบริโภคนั้นแก่เจ้าของข้อมูลส่วนบุคคลซึ่งอาจรวมไปถึงการเปลี่ยนผู้ให้บริการด้วย

3.4 กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดา

ประเทศแคนาดามีกฎหมายคุ้มครองข้อมูลส่วนบุคคลคือ The Personal Information Protection and Electronic Document Act หรือเรียกอีกอย่างว่า PIPEDA หรือ PIPED Act พระราชบัญญัติดังกล่าวมีผลใช้บังคับเมื่อวันที่ 13 เมษายน ค.ศ.2000 โดยมีวัตถุประสงค์เพื่อกำหนดกฎเกณฑ์เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเปิดเผยข้อมูลส่วนบุคคลในยุคที่เทคโนโลยีสามารถอำนวยความสะดวกในการเผยแพร่และแลกเปลี่ยนข้อมูลข่าวสาร โดยกฎเกณฑ์ดังกล่าวตระหนักถึงสิทธิในความเป็นส่วนตัวของบุคคลในด้านข้อมูลส่วนบุคคล และความจำเป็นขององค์กรในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ที่วิญญูชนเห็นว่าเหมาะสมแก่สถานการณ์นั้นๆ โดยพระราชบัญญัติดังกล่าวกำหนดความหมายของคำต่างๆไว้ซึ่งจะกล่าวถึงเพียงเฉพาะสาระสำคัญเท่านั้น ดังนี้

“กิจกรรมทางการค้า” หมายถึง ธุรกรรมเฉพาะกิจใดๆ การกระทำหรือการประพฤติหรือทางปฏิบัติปกติซึ่งมีลักษณะทางการค้า รวมถึงการขาย การแลกเปลี่ยน หรือการลิสซิ่ง (Leasing) รายชื่อผู้บริจาค สมาชิกหรือการระดมทุน

“องค์กร” รวมถึง สมาคม ห้างหุ้นส่วน บุคคล และสหภาพแรงงาน

“ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลเกี่ยวกับบุคคลที่อาจถูกระบุตัวได้ แต่ไม่รวมถึงชื่อ คำนำหน้า หรือที่อยู่ทางธุรกิจ หรือเบอร์โทรศัพท์ของลูกจ้างหรือองค์กร

“บันทึก” รวมถึง จดหมายใดๆ บันทึก หนังสือ แผนการ แผนที่ ภาพวาด แผนภาพ งานที่เกี่ยวกับรูปภาพหรือกราฟิก การบันทึกเสียง วีดีโอเทป บันทึกซึ่งสามารถอ่านได้โดยเครื่อง หรือข้อมูลเอกสารอื่นไม่ว่าอยู่ในรูปใดหรือลักษณะใด และให้หมายรวมถึงการทำซ้ำของสิ่งเหล่านั้นด้วย

อย่างไรก็ตามประเทศแคนาดากำลังพยายามแก้ไขข้อมูลส่วนบุคคลซึ่งไม่รวมถึงชื่อดังกล่าวโดยแยกข้อมูลส่วนบุคคลออกจากข้อมูลเพื่อการติดต่อทางธุรกิจ ซึ่งข้อมูลเพื่อการติดต่อทางธุรกิจ หมายถึง ชื่อปัจเจกบุคคล ตำแหน่ง ที่อยู่ที่ทำงาน เบอร์โทรศัพท์ที่ของทำงาน เบอร์แฟ็กซ์ของที่ทำงาน อีเมลของที่ทำงาน และข้อมูลอื่นใดเกี่ยวกับปัจเจกบุคคลนี้ PIPEDA จะไม่นำมาใช้แก่ข้อมูลเพื่อการติดต่อทางธุรกิจนี้ตราบเท่าที่ข้อมูลดังกล่าวมีเพื่อการติดต่อสื่อสาร การอำนวยความสะดวกแก่

การติดต่อสื่อสารกับปัจเจกบุคคลเกี่ยวกับการจ้างงาน อาชีพ หรือธุรกิจ[17] สำหรับหลักการคุ้มครองข้อมูลส่วนบุคคล PIPEDA ตั้งอยู่บนหลักการ 10 ประการ กล่าวคือ

1. หลักความเชื่อถือได้ (Accountability)

องค์กรมีความรับผิดชอบต่อข้อมูลส่วนบุคคลที่อยู่ในความครอบครองขอตน และต้องแต่งตั้งบุคคลซึ่งมีหน้าที่รับผิดชอบดำเนินการให้องค์การปฏิบัติตามหลักการอื่นๆที่จะกล่าวต่อไป องค์กรมีความรับผิดชอบต่อข้อมูลส่วนบุคคลซึ่งอยู่ในความครอบครองหรือการดูแลของตน รวมถึงข้อมูลที่ถูกส่งไปยังบุคคลที่สามเพื่อการประมวลผลโดยองค์กรต้องอาศัยพันธะตามสัญญา หรือด้วยวิธีอื่นใดเพื่อให้มีระดับการป้องกันที่เท่าเทียมกันแก่ข้อมูลที่ถูกประมวลผลนั้น องค์กรต้องกำหนดให้มีนโยบายและแนวปฏิบัติเพื่อให้หลักการอื่นๆดังที่จะกล่าวต่อไปนี้เกิดผลจริงซึ่งรวมถึง

i กำหนดให้มีกระบวนการในการคุ้มครองข้อมูลส่วนบุคคล

ii จัดให้มีกระบวนการเพื่อรับและตอบปัญหาและข้อร้องเรียน

iii ฝึกหัดพนักงานและแจ้งให้พนักงานทราบถึงนโยบายและแนวปฏิบัติขององค์กร และ

iiii จัดให้มีข้อมูลซึ่งอธิบายนโยบายและกระบวนการขององค์กร

2. หลักการกำหนดวัตถุประสงค์ (Identifying Purpose)

องค์กรต้องจัดให้มีการระบุวัตถุประสงค์ที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลก่อนหรือขณะเวลาทำการเก็บรวบรวมข้อมูลส่วนบุคคล โดยองค์กรต้องทำเอกสารแสดงวัตถุประสงค์ซึ่งข้อมูลส่วนบุคคลนั้นถูกเก็บรวบรวม ทั้งนี้เพื่อให้เป็นไปตามหลักการที่ 8 คือหลักเปิดเผยโปร่งใส (Openess Principle) การระบุวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลก่อนหรือขณะทำการเก็บรวบรวมรวมช่วยให้องค์กรสามารถตัดสินใจเกี่ยวกับข้อมูลส่วนบุคคลที่จะทำการเก็บรวบรวมเพื่อให้บรรลุวัตถุประสงค์นั้น อย่างไรก็ตามหลักการจำกัดการเก็บรวม (Limiting Collection Principle) อันเป็นหลักการที่ 4 ห้ามมิให้องค์กรเก็บรวบรวมข้อมูลส่วนบุคคลเกินกว่าความจำเป็นเพื่อดำเนินการตามวัตถุประสงค์ที่ได้ระบุไว้ให้สำเร็จลุล่วง

นอกจากนี้องค์กรต้องมีการแจ้งวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลให้แก่เจ้าของข้อมูลทราบก่อนหรือขณะทำการเก็บรวบรวมข้อมูลส่วนบุคคล ซึ่งอาจกระทำโดยวาจา

---

[17] Office of the privacy commissioner of Canada, “Bill S-4, An act to amend the personal information protection and electronic documents act and to make a consequential amendment to another act”,Accedssed10 March 2016, https://www.priv.gc.ca/parl/2014/parl_sub_140604_sen_e.asp

หรือโดยลายลักษณ์อักษร ทั้งนี้ขึ้นกับวิธีในการเก็บรวบรวมข้อมูลส่วนบุคคล หากผู้เก็บรวบรวมข้อมูลส่วนบุคคลประสงค์นำข้อมูลนั้นไปใช้เพื่อวัตถุประสงค์อื่นที่มิได้แจ้งไว้ ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์นั้นแก่เจ้าของข้อมูลส่วนบุคคลก่อนการนำข้อมูลไปใช้ โดยต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลด้วย เว้นแต่เป็นกรณีที่กฎหมายกำหนดไว้เป็นอย่างอื่น และองค์กรซึ่งทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคล ต้องสามารถอธิบายวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลได้

3. หลักความยินยอม (Consent)

หลักความยินยอมนี้กำหนดให้ในการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเสียก่อน เว้นแต่ในกรณีที่ไม่อาจเป็นไปได้ โดยในบางครั้งข้อมูลส่วนบุคคลอาจถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยไม่ได้รับความยินยอมได้ เช่น เป็นกรณีที่กฎหมายกำหนดไว้ เป็นเหตุผลทางการแพทย์ หรือเพื่อเหตุผลในด้านความปลอดภัย ซึ่งการให้ความยินยอมนั้นอาจเป็นไปไม่ได้หรือเป็นไปได้ยาก หรือในกรณีที่องค์กรไม่มีความสัมพันธ์ใดๆกับเจ้าของข้อมูลส่วนบุคคลอาจไม่สามารถขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลได้ เช่น องค์กรเพื่อการกุศล หรือบริษัทที่ทำการตลาดแบบตรงอาจไม่สามารถขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามบัญชีรายชื่อที่ตนได้รับมาได้ ในกรณีเช่นนี้องค์กรผู้มอบบัญชีข้อมูลส่วนบุคคลแก่องค์กรเพื่อการกุศล หรือบริษัททำการตลาดแบบตรงนี้ต้องขออนุญาตเจ้าของข้อมูลส่วนบุคคลเสียก่อนทำการเปิดเผยข้อมูลนั้น

ในการขอความยินยอมองค์กรต้องดำเนินการในเวลาการเก็บรวบรวมข้อมูลส่วนบุคคล อย่างไรก็ตามในบางกรณีอาจขอความยินยอมในภายหลังเก็บรวบรวมข้อมูลส่วนบุคคลได้ แต่ต้องทำการขอความยินยอมก่อนใช้หรือเปิดเผยข้อมูลส่วนบุคคลนั้น เช่น ในกรณีที่องค์กรต้องการใช้ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกจากที่ได้ระบุไว้ในขณะเก็บรวบรวมข้อมูลส่วนบุคคล โดยความยินยอมดังกล่าวองค์กรต้องใช้ความพยายามตามสมควรเพื่อให้มั่นใจว่าเจ้าของข้อมูลส่วนบุคคลได้รับแจ้งวัตถุประสงค์ในการนำข้อมูลไปใช้ และการแจ้งดังกล่าวต้องใช้ภาษาที่เข้าใจง่ายเพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถเข้าใจวัตถุประสงค์ได้ดี

นอกจากนี้องค์กรต้องไม่บังคับให้เจ้าของข้อมูลส่วนบุคคลให้ความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอันเกินกว่าที่จำเป็นในการดำเนินการตามวัตถุประสงค์ที่กำหนดไว้โดยชัดแจ้งและชอบด้วยกฎหมายด้วยการละเว้นไม่ให้บริการแก่เจ้าของข้อมูลส่วนบุคคล ในการขอความยินยอมนี้องค์กรต้องคำนึงถึงความคาดหวังของเจ้าของข้อมูลส่วนบุคคลด้วย กล่าวคือหากเจ้าของข้อมูลส่วนบุคคลได้ให้ข้อมูลแก่องค์กรเพื่อบอกรับการเป็นสมาชิกของหนังสือพิมพ์ขององค์กรใดองค์กรหนึ่ง องค์กรนั้นอาจนำข้อมูลส่วนบุคคลมาใช้เพื่อการเรียกเก็บค่าบริการ หรือการ

เสนอขายสิ่งพิมพ์อื่นที่มีความเกี่ยวข้องได้ แต่จะนำข้อมูลไปมอบแก่บริษัทซึ่งขายสินค้าทางสุขภาพมิได้ เนื่องจากเจ้าของข้อมูลส่วนบุคคลได้ให้ข้อมูลแก่องค์กรไว้เพื่อคาดหวังการบริการเกี่ยวกับสิ่งพิมพ์ โดยมิได้คาดหวังเกี่ยวกับสินค้าหรือการบริการทางสุขภาพ

การให้ความยินยอมอาจทำได้หลายวิธี เช่น แบบฟอร์มการขอความยินยอม การให้ความยินยอมด้วยวาจา หรือการให้ความยินยอมโดยการ Opt-In เป็นต้น ทั้งนี้เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการเพิกถอนความยินยอมได้ไม่ว่าในเวลาใดๆ โดยในบางกรณีอาจตกอยู่ภายใต้ข้อจำกัดแห่งบทบัญญัติของกฎหมาย หรือข้อกำหนดตามสัญญา และองค์กรต้องแจ้งเจ้าของข้อมูลส่วนบุคคลถึงผลกระทบที่อาจเกิดขึ้นจากการเพิกถอนความยินยอมด้วย

4. หลักการจำกัดการเก็บรวบรวมข้อมูลส่วนบุคคล (Limiting Collection)

หลักการดังกล่าวกำหนดให้การเก็บรวบรวมข้อมูลส่วนบุคคลต้องจำกัดไว้เพียงเท่าที่จำเป็นตามวัตถุประสงค์ซึ่งองค์กรได้กำหนดไว้ โดยข้อมูลส่วนบุคคลนี้ต้องถูกเก็บรวบรวมโดยวิธีที่เป็นธรรม ชอบด้วยกฎหมาย และต้องไม่เลือกปฏิบัติ จำนวนและประเภทของข้อมูลที่ถูกเก็บรวบรวมต้องจำกัดไว้เพียงเพื่อความจำเป็นในการทำให้บรรลุวัตถุประสงค์ตามที่ได้กำหนดไว้ องค์กรจะต้องระบุประเภทของข้อมูลส่วนบุคคลให้เป็นส่วนหนึ่งของนโยบายและทางปฏิบัติในการจัดการข้อมูลส่วนบุคคลตามหลักการเปิดเผยโปร่งใส (Openess Principle) ซึ่งวัตถุประสงค์ของการกำหนดให้ข้อมูลส่วนบุคคลต้องเก็บรวบรวมโดยวิธีที่เป็นธรรมและชอบด้วยกฎหมาย เพื่อป้องกันมิให้องค์กรเก็บรวบรวมข้อมูลส่วนบุคคลโดยวิธีที่ทำให้เจ้าของข้อมูลส่วนบุคคลเกิดความเข้าใจผิดในวัตถุประสงค์หรือเป็นการลวงเจ้าของข้อมูลส่วนบุคคล

5. หลักข้อจำกัดในการใช้ เปิดเผยและเก็บรักษาข้อมูลส่วนบุคคล (Limiting Use, Disclosure, and Retention Principle)

หลักการนี้กำหนดให้ข้อมูลส่วนบุคคลต้องไม่ถูกใช้ หรือเปิดเผยเพื่อวัตถุประสงค์อื่นใดนอกจากวัตถุประสงค์ที่ข้อมูลส่วนบุคคลนั้นถูกเก็บรวบรวม และข้อมูลส่วนบุคคลนั้นต้องถูกเก็บรักษาไว้เพียงเท่าเวลาที่จำเป็นเพื่อให้บรรลุวัตถุประสงค์เท่านั้น องค์กรต้องพัฒนาแนวปฏิบัติเพื่อจัดให้มีกระบวนการเกี่ยวกับการเก็บรักษาข้อมูลส่วนบุคคล โดยแนวปฏิบัตินี้ต้องระบุระยะเวลาขั้นต่ำสุดและขั้นสูงสุดในการเก็บรักษาข้อมูลส่วนบุคคล หากข้อมูลส่วนบุคคลใดถูกนำไปใช้เพื่อการตัดสินใจเกี่ยวกับเจ้าของข้อมูลส่วนบุคคล ข้อมูลนั้นต้องถูกเก็บรักษาไว้ภายหลังที่การตัดสินใจดังกล่าวเสร็จสิ้นนานเท่าที่จะให้เจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึงข้อมูลนั้นได้ ข้อมูลส่วนบุคคลใดไม่จำเป็นต้องใช้เพื่อการบรรลุวัตถุประสงค์ที่ได้ให้ไว้ในขณะทำการเก็บรวบรวมข้อมูลส่วนบุคคลอีกต่อไป ข้อมูลที่ไม่จำเป็นนั้นต้องถูกทำลาย ลบ หรือทำให้เป็นข้อมูลประเภท Anonymous ทั้งนี้องค์กรต้องออกปฏิบัติเพื่อกำหนดกระบวนการเกี่ยวกับการทำลายข้อมูลส่วนบุคคล

6. หลักความถูกต้อง (Accuracy Principle)

หลักการดังกล่าวกำหนดให้ข้อมูลส่วนบุคคลจะต้องถูกต้อง สมบูรณ์ และเป็นปัจจุบันทั้งนี้เพียงเท่าที่จำเป็นเพื่อการทำวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลให้สำเร็จลุล่วง ข้อมูลส่วนบุคคลนั้นต้องถูกต้อง สมบูรณ์และเป็นปัจจุบันเพียงไรขึ้นกับการใช้ข้อมูลส่วนบุคคลโดยคำนึงประโยชน์ของเจ้าของข้อมูลส่วนบุคคลด้วย นอกจากนี้ข้อมูลส่วนบุคคลนั้นต้องถูกต้องสมบูรณ์และเป็นปัจจุบันเพียงพอที่จะลดโอกาสในการนำข้อมูลส่วนบุคคลที่ไม่เหมาะสมไปใช้ในการตัดสินใจเกี่ยวกับเจ้าของข้อมูลส่วนบุคคล องค์กรจะต้องไม่พยายามปรับปรุงข้อมูลส่วนบุคคลให้ทันสมัยเป็นประจำเว้นแต่การปรับปรุงนั้นจำเป็นเพื่อให้วัตถุประสงค์ที่เก็บรวบรวมข้อมูลส่วนบุคคลสำเร็จลุล่วง อย่างไรก็ตามหากข้อมูลส่วนบุคคลรวมถึงข้อมูลส่วนบุคคลที่ถูกเปิดเผยแก่บุคคลที่สามที่ถูกใช้ต่อเนื่องกันไปจะต้องถูกต้องและเป็นปัจจุบัน

7. หลักการป้องกัน (Safeguards Principle)

หลักการดังกล่าวกำหนดให้องค์กรมีมาตรการรักษาความปลอดภัยเพื่อคุ้มครองข้อมูลส่วนบุคคลนั้นจากการสูญหาก การขโมย รวมถึงการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การคัดลอก การใช้ หรือการเปลี่ยนแปลง โดยองค์กรต้องรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่ถูกเก็บรักษาไว้ไม่ว่าจะอยู่ในรูปแบบใดๆ อย่างไรก็ตามลักษณะของมาตรการรักษาความปลอดภัยอาจแตกต่างกันไปตามความอ่อนไหวของข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวม จำนวน การโอนไปยังบุคคลอื่น และรูปแบบของข้อมูลส่วนบุคคล โดยวิธีการเก็บรักษาข้อมูลส่วนบุคคลที่มีความอ่อนไหวมากต้องมีมาตรการในการรักษาความปลอดภัยที่สูง

มาตรการในการรักษาความปลอดภัยต้องรวมถึงกรณีดังต่อไปนี้ด้วย

i มาตรการในทางปฏิบัติ เช่น การใส่กุญแจตู้ที่เก็บรักษาข้อมูลส่วนบุคคล และการจำกัดการเข้าสำนักงาน

ii มาตรการทางองค์กร เช่น การรักษาความปลอดภัยและการจำกัดการเข้าถึงซึ่งเป็นไปตามหลัก need-to-know

iii มาตรการทางเทคโนโลยี เช่น การใช้ password เพื่อการเข้ารหัส

นอกจากนี้องค์กรต้องทำให้ลูกจ้างของตนตระหนักถึงความสำคัญในการเก็บรักษาความลับของข้อมูลส่วนบุคคล และต้องใช้ความระมัดระวังในการกำจัดหรือทำลายข้อมูลส่วนบุคคลเพื่อป้องกันมิให้บุคคลที่ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลส่วนบุคคลได้

8. หลักการเปิดเผยโปร่งใส (Openess Principle)

หลักการดังกล่าวกำหนดให้องค์กรต้องเตรียมนโยบายและแนวปฏิบัติของตนเกี่ยวกับการจัดการข้อมูลส่วนบุคคลให้พร้อมเพื่อที่เจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึงได้ เจ้าของ

ข้อมูลส่วนบุคคลสามารถที่จะร้องขอข้อมูลเกี่ยวกับนโยบายและแนวปฏิบัติขององค์กรเกี่ยวกับการจัดการข้อมูลส่วนบุคคลได้ ซึ่งในการให้ข้อมูลดังกล่าวแก่เจ้าของข้อมูลส่วนบุคคลองค์กรต้องจัดให้อยู่ในรูปแบบที่สามารถเข้าใจได้ง่าย โดยข้อมูลที่องค์กรต้องเปิดเผยรวมถึงข้อมูลดังต่อไปนี้ด้วย

i ชื่อ คำนำหน้า และที่อยู่ของบุคคลซึ่งมีหน้าที่รับผิดชอบเกี่ยวกับนโยบายและแนวปฏิบัติขององค์กร และบุคคลที่เจ้าของข้อมูลส่วนบุคคลสามารถที่จะร้องเรียนหรือขอข้อมูลเพิ่มเติม

ii วิธีการที่จะเข้าถึงข้อมูลส่วนบุคคลซึ่งอยู่ในความครอบครองขององค์กร

iii บรรยายประเภทของข้อมูลส่วนบุคคลที่เก็บรักษาไว้โดยองค์กร

iv สำเนาโบชัวร์หรือข้อมูลที่อธิบายถึงนโยบาย มาตรฐาน และหลักเกณฑ์ขององค์กร

v ข้อมูลส่วนบุคคลใดที่จะถูกเปิดเผยแก่องค์กรที่เกี่ยวข้อง เช่น สาขา

ในการเปิดเผยนโยบายและแนวปฏิบัติขององค์กร องค์กรอาจทำได้หลายวิธีโดยต้องคำนึงถึงลักษณะของธุรกิจและเหตุผลด้านอื่นๆด้วย เช่น องค์กรอาจเลือกที่จะเปิดเผยนโยบายและแนวปฏิบัติของตนผ่านโบชัวร์ซึ่งแจกในสำนักงานขององค์กรนั้น หรือส่งอีเมลไปยังลูกค้าของตน หรือให้เข้าถึงได้โดยทางอินเตอร์เน็ต หรือแจ้งผ่านทางโทรศัพท์ซึ่งไม่เสียค่าใช้จ่าย

9. หลักการเข้าถึงของเจ้าของข้อมูลส่วนบุคคล (Individual Access Principle)

หลักการดังกล่าวกำหนดให้เมื่อมีคำร้องขอของเจ้าของข้อมูลส่วนบุคคล องค์กรต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงการมีอยู่ การใช้ และการเปิดเผยถึงข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล นอกจากนี้เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านความถูกต้องและความสมบูรณ์ของข้อมูลนั้นได้ และมีสิทธิได้รับการแก้ไขข้อมูลนั้นให้ถูกต้องหรือสมบูรณ์ได้ อย่างไรก็ตามในบางสถานการณ์องค์กรอาจไม่สามารถให้เจ้าของข้อมูลส่วนบุคคลเข้าถึงข้อมูลส่วนบุคคลของตนที่องค์กรมีอยู่ทั้งหมดได้ ในกรณีเช่นนี้ถือเป็นข้อยกเว้นของหลักการเข้าถึงของเจ้าของข้อมูลส่วนบุคคล องค์กรต้องแจ้งเหตุผลในการปฏิเสธการเข้าถึงแก่เจ้าของข้อมูลส่วนบุคคล ข้อยกเว้นในการเข้าถึงของเจ้าของข้อมูลส่วนบุคคล เช่น ข้อมูลที่เชื่อมโยงไปยังเจ้าของข้อมูลส่วนบุคคลอื่น ข้อมูลส่วนบุคคลซึ่งไม่สามารถเปิดเผยได้เนื่องจากบทบัญญัติแห่งกฎหมาย ความปลอดภัย เป็นเหตุผลทางกรรมสิทธิ์ทางการค้า เป็นข้อมูลเกี่ยวกับทนายความและลูกความ หรือเป็นข้อมูลอันเกี่ยวกับเอกสิทธิ์ในการดำเนินคดี

เมื่อมีคำร้องขอของเจ้าของข้อมูลส่วนบุคคล องค์กรต้องแจ้งเจ้าของข้อมูลส่วนบุคคลว่าองค์กรมีข้อมูลส่วนบุคคลนั้นไว้ในความครอบครองหรือไม่ โดยองค์กรจะต้องแจ้งถึงแหล่งข้อมูล และแจ้งถึงกรณีที่ได้ใช้ข้อมูลส่วนบุคคลหรือกรณีที่ข้อมูลส่วนบุคคลนั้นจะถูกนำไปใช้และข้อมูลเกี่ยวกับบุคคลที่สามที่ข้อมูลส่วนบุคคลนั้นจะถูกเปิดเผย เจ้าของข้อมูลส่วนบุคคลซึ่งขอเข้าถึงข้อมูลส่วนบุคคลของตนอาจถูกร้องขอให้จัดเตรียมเอกสารหลักฐานได้แต่องค์กรจะนำหลักฐาน

นั้นไปใช้เพื่อการอื่นมิได้ การแจ้งถึงบุคคลที่สามที่ข้อมูลส่วนบุคคลนั้นถูกเปิดเผย องค์กรต้องพยายามระบุให้ชัดแจ้งที่สุดเท่าที่จะเป็นไปได้ ในกรณีที่องค์กรไม่อาจแจ้งถึงบุคคลที่สามที่ข้อมูลนั้นถูกเปิดเผยให้องค์กรแจ้งถึงบุคคลที่สามที่อาจได้รับข้อมูลส่วนบุคคลนั้น

ในกรณีหากมีคำขอของเจ้าของข้อมูลส่วนบุคคล องค์กรต้องตอบรับคำขอภายในเวลาอันสมควร และโดยมีค่าใช้จ่ายน้อยที่สุดหรือไม่มีค่าใช้จ่าย และข้อมูลที่ถูกร้องขอนั้นต้องเปิดเผยแก่เจ้าของข้อมูลส่วนบุคคลในลักษณะที่สามารถเข้าใจได้ง่าย เช่น หากองค์กรมีการใช้คำย่อหรือตัวย่อหรือรหัสในการบันทึกข้อมูลส่วนบุคคล องค์กรต้องอธิบายตัวย่อ คำย่อ หรือรหัสนั้นแก่เจ้าของข้อมูลส่วนบุคคลด้วย หากเจ้าของข้อมูลส่วนบุคคลได้แสดงว่าข้อมูลส่วนบุคคลนั้นไม่ถูกต้องหรือไม่สมบูรณ์ องค์กรต้องทำการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้องหรือสมบูรณ์ ซึ่งการแก้ไขนี้ให้รวมถึงการแก้ไขเปลี่ยนแปลง การทำลาย หรือการเพิ่มเติมข้อมูลด้วย หากองค์กรไม่ดำเนินการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้องหรือสมบูรณ์ตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ องค์กรต้องบันทึกเหตุที่ไม่แก้ไขไว้ด้วย

10. หลักการคัดค้านการไม่ปฏิบัติตามหลักการที่ 1 ถึง 9 (Challenging Compliance Principle)

หลักการดังกล่าวกำหนดให้เจ้าของข้อมูลส่วนบุคคลต้องสามารถอุทธรณ์ข้อร้องเรียนเกี่ยวกับหลักการที่ 1 ถึง 9 ที่ได้กล่าวมาไปยังบุคคลหรือกลุ่มบุคคลที่ได้รับการแต่งตั้งให้มีหน้าที่รับผิดชอบการร้องเรียนองค์กร องค์กรต้องมีมาตรการในการรับและตอบข้อร้องเรียนหรือคำถามเกี่ยวกับนโยบายและแนวปฏิบัติเกี่ยวกับการจัดการข้อมูลส่วนบุคคล กระบวนการในการร้องเรียนนี้ต้องสามารถเข้าถึงและใช้งานได้ง่าย

องค์กรต้องแจ้งแก่เจ้าของข้อมูลส่วนบุคคลซึ่งส่งคำถามหรือข้อร้องเรียนถึงการมีอยู่ของกระบวนการในการร้องเรียนดังกล่าว เช่น หน่วยงานกำกับดูแลบางหน่วยงานอาจรับข้อร้องเรียนเกี่ยวกับแนวปฏิบัติในการจัดการข้อมูลส่วนบุคคลข้อมูลส่วนบุคคลขององค์กรซึ่งหน่วยงานมีหน้าที่กำกับดูแล โดยองค์กรต้องสอบสวนตามข้อร้องเรียนนั้น หากข้อร้องเรียนนั้นฟังได้ องค์กรต้องมีมาตรการที่เหมาะสม ซึ่งให้รวมถึงการแก้ไขนโยบายและแนวปฏิบัติขององค์กร

ในด้านการบังคับใช้ PIPEDA กำหนดให้บทบัญญัติเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลแก่ทุกองค์กรซึ่งเกี่ยวข้องกับข้อมูลส่วนบุคคล โดยนำมาใช้บังคับแม้ว่าจะมีบทบัญญัติอื่นหรือบทบัญญัติใดๆที่บัญญัติขึ้นภายหลังกฎหมาย PIPEDA มีผลใช้บังคับ เว้นแต่กฎหมายอื่นนั้นจะกล่าวไว้โดยชัดแจ้งเป็นประการอื่น ในกรณีดังต่อไปนี้

1. องค์กรเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อกิจกรรมทางการค้า หรือ

2. เป็นข้อมูลส่วนบุคคลเกี่ยวกับลูกจ้างขององค์กรและองค์กรเก็บรวบรวม ใช้ หรือเปิดเผยเกี่ยวกับการดำเนินงานของรัฐ การกระทำหรือธุรกิจ

อย่างไรก็ตาม PIPEDA ในเรื่องการคุ้มครองข้อมูลส่วนบุคคลจะไม่นำมาใช้บังคับแก่กรณีดังต่อไปนี้

i หน่วยงานของรัฐบาลที่อยู่ภายใต้กฎหมาย Privacy Act

ii บุคคลใดๆที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลหรือเพื่อวัตถุประสงค์ส่วนตัว และข้อมูลส่วนบุคคลนั้นมิได้เก็บรักษา ใช้ หรือเปิดเผยเพื่อวัตถุประสงค์ประการอื่น

iii องค์กรใดๆที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการเขียนข่าว วัตถุประสงค์ทางวรรณคดี หรือวัตถุประสงค์ทางศิลปะ และมิได้เก็บรวบรวม ใช้ หรือเปิดเผยเพื่อวัตถุประสงค์อื่น

PIPEDA กำหนดให้องค์กรต้องปฏิบัติตามหลักการที่ 1 ถึง 10 อย่างเคร่งครัด องค์กรต้องเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพียงเพื่อวัตถุประสงค์ที่วิญญูชนพิจารณาว่าเหมาะสมในสถานการณ์นั้นๆ การที่องค์กรแต่งตั้งบุคคลซึ่งมีหน้าที่รับผิดชอบดำเนินการให้องค์การปฏิบัติตามหลักการคุ้มครองข้อมูลส่วนบุคคลไม่ทำให้องค์กรหลุดพ้นจากหน้าที่ในการปฏิบัติตามหลักการที่ 1 ถึง 10

ในการเก็บรวบรวมข้อมูลส่วนบุคคล องค์กรต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

a. การเก็บรวบรวมนั้นเห็นได้ชัดว่าเป็นไปเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคลไม่อาจให้ความยินยอมได้ในเวลานั้น

b. มีเหตุผลอันสมควรเชื่อว่าการเก็บรวบรวมข้อมูลส่วนบุคคลโดยความรู้หรือความยินของเจ้าของข้อมูลส่วนบุคคลอาจทำให้ได้ข้อมูลส่วนบุคคลไม่ครบถ้วนหรือไม่ถูกต้อง และการเก็บรวบรวมนั้นมีเหตุอันสมควรเพื่อวัตถุประสงค์เกี่ยวกับการสืบสวนการผิดข้อตกลง หรือการฝ่าฝืนกฎหมายของประเทศแคนาดา หรือของมลรัฐ

c. การเก็บรวบรวมนั้นมีวัตถุประสงค์เพื่อการเขียนข่าว หรือวัตถุประสงค์ทางศิลปะ หรือวัตถุประสงค์ทางวรรณคดี

d. ข้อมูลนั้นถูกเปิดเผยไว้เป็นสาธารณะและถูกกำหนดไว้ตามบทบัญญัติของกฎหมาย หรือ

e. การเก็บรวบรวมข้อมูลส่วนบุคคลนั้นมีวัตถุประสงค์เพื่อการเปิดเผย

e.1แก่องค์กรของรัฐเกี่ยวกับข้อมูลความปลอดภัยของประเทศแคนาดา การป้องกันประเทศ หรือความสัมพันธ์ระหว่างประเทศ หรือ

e.2 เป็นการเปิดเผยแก่องค์กรหรือบุคคลที่มีหน้าที่สืบสวน หรือองค์กรของรัฐเมื่อมีข้อสงสัยว่าข้อมูลนั้นเกี่ยวข้องกับความมั่นคงของประเทศ การป้องกันประเทศ หรือความสัมพันธ์ระหว่างประเทศ

การนำข้อมูลส่วนบุคคลไปใช้ภายใต้ PIPEDA กำหนดให้องค์กรต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล อย่างไรก็ตาม PIPEDA ได้กำหนดข้อยกเว้นไว้ในบางกรณี เช่น เป็นข้อมูลที่เป็นประโยชน์อย่างมากในการสืบสวนการฝ่าฝืนบทบัญญัติแห่งกฎหมายของประเทศแคนาดาหรือของมลรัฐ หรือใช้เพื่อวัตถุประสงค์ที่ฉุกเฉินต่อชีวิต สุขภาพ หรือความปลอดภัยของบุคคล หรือเป็นข้อมูลที่ได้เปิดเผยไว้เป็นสาธารณะ เป็นต้น

ในด้านการเปิดเผยข้อมูลส่วนบุคคล PIPEDA กำหนดให้องค์กรต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเช่นเดียวกับการนำข้อมูลส่วนบุคคลไปใช้ ทั้งนี้มีข้อยกเว้นบางประการที่องค์กรอาจไม่จำต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เช่น เป็นการเปิดเผยเพื่อการเรียกเก็บหนี้ที่บุคคลนั้นมีต่อองค์กร หรือเป็นการเปิดเผยตามหมายศาล หรือหมายหรือคำสั่งของศาล หรือเป็นการเปิดเผยแก่บุคคลซึ่งจำเป็นต้องอาศัยข้อมูลนั้นเนื่องจากเป็นกรณีฉุกเฉินต่อชีวิต สุขภาพ หรือความปลอดภัยของบุคคลนั้น และในกรณีเช่นนี้หากเจ้าของข้อมูลส่วนบุคคลยังมีชีวิตอยู่ องค์กรต้องแจ้งเป็นหนังสือให้เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้าถึงการเปิดเผยข้อมูลส่วนบุคคลนั้น เป็นต้น

การใช้สิทธิในการเข้าถึงข้อมูลส่วนบุคคลของตนต้องทำเป็นลายลักษณ์อักษร เมื่อมีคำขอดังกล่าวแล้วองค์กรต้องตอบคำขอดังกล่าวโดยสุจริตและไม่ช้ากว่า 30 วันนับแต่วันที่ได้รับคำขอนั้น แต่ระยะเวลาดังกล่าวอาจขยายได้ในกรณีดังต่อไปนี้

a. ไม่เกิน 30 วัน หาก

1. กำหนดเวลานั้นอาจกระทบต่อกิจกรรมขององค์กร หรือ

2. จำเป็นต้องใช้เวลาในการปรึกษาหารือที่จำเป็นเพื่อการตอบคำขอของเจ้าของข้อมูลส่วนบุคคล และไม่อาจกระทำได้ภายในเวลาที่กำหนดไว้

b. เพื่อความจำเป็นในการแปลงข้อมูลส่วนบุคคลให้อยู่ในรูปที่ผู้บกพร่องทางการรับรู้สามารถเข้าถึงได้

ในกรณีทั้งสองดังกล่าวองค์กรต้องแจ้งไปยังเจ้าของข้อมูลส่วนบุคคลถึงการขยายเวลานั้นภายใน 30วัน นับแต่วันที่ได้รับคำขอจากเจ้าของข้อมูลส่วนบุคคล โดยต้องบอกกำหนดเวลาใหม่ เหตุผลในการขยายกำหนดเวลานั้น และสิทธิในการร้องเรียนไปยังคณะกรรมการผู้รับผิดชอบเกี่ยวกับการขยายกำหนดเวลา หากองค์กรไม่อาจตอบเจ้าของข้อมูลส่วนบุคคลภายในกำหนดเวลาดังกล่าวได้ ให้ถือว่าองค์กรปฏิเสธคำขอนั้น

ในกรณีที่องค์กรปฏิเสธคำขอของเจ้าของข้อมูลส่วนบุคคล องค์กรต้องแจ้งเจ้าของข้อมูลส่วนบุคคลเป็นหนังสือถึงการปฏิเสธ เหตุผลในการปฏิเสธ และความช่วยเหลือที่เจ้าของข้อมูลส่วนบุคคลมีสิทธิได้รับตามบทบัญญัติแห่งกฎหมาย นอกจากนี้หากการอนุญาตให้เจ้าของข้อมูลส่วนบุคคลเข้าถึงข้อมูลของตนอาจก่อให้ข้อมูลส่วนบุคคลของผู้อื่นถูกเปิดเผยได้ องค์กรจะปฏิเสธคำขอนั้นก็ได้ หรือเป็นข้อยกเว้นตามกฎหมายในบางกรณี เช่น ข้อมูลส่วนบุคคลนั้นถูกปกป้องไว้เพื่อสิทธิประโยชน์ของทนายความและลูกความ หรือการเปิดเผยนั้นอาจทำให้ความลับทางการค้าถูกเปิดเผยได้ หรือการเปิดเผยนั้นอาจก่อให้เกิดอันตรายต่อชีวิตหรือความปลอดภัยของบุคคลอื่น

ประเทศแคนาดาให้ความคุ้มครองแก่ข้อมูลส่วนบุคคลโดยกำหนดหลักการการคุ้มครองไว้ถึง 10 ประการซึ่งทำให้เจ้าของข้อมูลส่วนบุคคลได้รับความคุ้มครองเป็นอย่างดี ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ต่อเมื่อได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล นอกจากนี้ยังให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของตนโดยทำคำร้องขอเป็นหนังสือต่อเจ้าของข้อมูลส่วนบุคคล

สำหรับข้อมูล Mac Address และ IP Address มิได้บัญญัติไว้โดยชัดแจ้งแต่อาศัยการตีความ PIPEDA โดยประเทศแคนาดาได้กำหนดความคุ้มครองแก่ข้อมูลประเภท IP Address จะถือเป็นข้อมูลส่วนบุคคลเมื่อสามารถเชื่อมโยงไปยังเจ้าของข้อมูลส่วนบุคคลได้ เช่น ในกรณีที่ผู้ให้บริการอินเตอร์เน็ต (Internet Service Provider หรือ ISP) เก็บรวบรวมข้อมูล IP Address ในกรณีนี้ข้อมูล IP Address จะถือว่าเป็นข้อมูลส่วนบุคคลเนื่องจากผู้ให้บริการอินเตอร์เน็ตมีข้อมูลอื่นๆเพียงพอที่จะระบุตัวเจ้าของข้อมูลส่วนบุคคล[18]และ Mac Address เป็นหมายเลขของอุปกรณ์ที่บ่งชี้ไปยังอุปกรณ์เครื่องใดเครื่องหนึ่งโดยเฉพาะจึงถือเป็นข้อมูลส่วนบุคคล[19]การทำ Profilingหรือ Online Tracking

---

[18] Office of the Privacy Comissioner of Canada, “Interpretation Bulletin”,Accedssed 10 February 2016,https://www.priv.gc.ca/leg_c/interpretations_02_e.asp#fn50

[19] Office of the Privacy Comissioner of Canada, “Report of findings investigationinto personal information handling practives of WhatsApp Inc.”,Accedssed10 February 2016, https://www.google.co.th/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwj_g5_Ov-XLAhUUW44KHSFnAeAQFggdMAA&url=https%3A%2F%2Fautoriteitpersoonsgegevens.

ยังมิได้มีการกำหนดไว้ชัดเจนว่าผู้ควบคุมข้อมูลส่วนบุคคลสามารถทำได้มากน้อยเพียงไร เพียงแต่มีความเห็นของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลถือข้อมูลที่ได้จากการ Profiling เป็นข้อมูลที่สามารถเชื่อมโยงไปยังเจ้าของข้อมูลส่วนบุคคลได้ง่าย ดังนั้นผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตาม PIPEDA[20]

ในกรณีของข้อมูลไบโอเมตริก (Biometric) ถือเป็นข้อมูลส่วนบุคคลตาม PIPEDA ซึ่งยังมิได้มีหลักเกณฑ์ที่กำหนดขึ้นเฉพาะเพื่อควบคุมการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลไบโอเมตริก (Biometric) แต่อย่างไรก็ตามคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดาได้ตระหนักถึงความอ่อนไหวของข้อมูลไบโอเมตริก (Biometric) จึงได้แนะนำให้องค์กรต้องพิจารณาให้ถี่ถ้วนเสียก่อนจะทำการเก็บรวบรวมข้อมูลไบโอเมตริก (Biometric) และควรเก็บรวบรวมเพื่อการยืนยันตัวบุคคลเท่านั้น[21]

3.5 กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสิงคโปร์

เนื่องจากในปัจจุบันมีการเก็บรวบรวมข้อมูลส่วนบุคคลตลอดเวลาและนำข้อมูลดังกล่าวมาใช้หรือมีการถ่ายโอนข้อมูลจากสถาบันหรือองค์กรหนึ่งไปยังอีกสถาบันหรือองค์กรหนึ่ง ประเทศสิงคโปร์จึงออกกฎหมายคุ้มครองข้อมูลส่วนบุคคล คือ Personal Data Protection Act 2012 (PDPA) เพื่อควบคุมการเก็บรวบรวมและการจัดการข้อมูลของผู้ควบคุมข้อมูลในยุคปัจจุบัน พระราชบัญญัติดังกล่าวมีผลใช้บังคับเมื่อวันที่ 2 กรกฎาคม 2014 มีวัตถุประสงค์เพื่อควบคุมการเก็บ

---

nl%2Fsites%2Fdefault%2Ffiles%2Fdownloads%2Frapporten%2Frap_2013-whatsapp-opc-final-report-of-findings.pdf&usg=AFQjCNH-Dp3xmYI3cQy7QSdJaUhEzFF5-w&sig2=DZx5ev-Fj7MjWJDyatB9fw&bvm=bv.117868183,d.c2E

[20] Office of the Privacy Commissioner of Canada, “Repert on the 2010 office of the privacy commissioner of canada’s consultations on online tracking, profiling and targeting, and cloud computing”,Accedssed10 February 2016, https://www.priv.gc.ca/resource/consultations/report_201105_e.pdf

[21] Office of the Privacy Comissioner of Canada, “OPC Guidance Documents Data at your fingertips Biometrics and the challenges to privacy”,Accedssed10 February 2016, https://www.priv.gc.ca/information/pub/gd_bio_201102_e.asp

รวบรวม ใช้ เปิดเผย และเก็บรักษาข้อมูลส่วนบุคคลโดยองค์กรต่างๆในลักษณะที่สร้างความสมดุลระหว่างการคุ้มครองข้อมูลส่วนบุคคล เช่นการให้สิทธิเข้าถึงข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคล และความจำเป็นขององค์กรต่างๆในการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ซึ่งวิญญูชนเห็นว่าเป็นการเหมาะสมแก่สถานการณ์นั้นๆ[22] นอกจากนี้พระราชบัญญัติฉบับดังกล่าวจัดตั้งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Commission)ซึ่งเป็นหน่วยงานของรัฐบาลมีวัตถุประสงค์ในการสนับสนุนและบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลเพื่อที่จะก่อให้เกิดความน่าเชื่อถือระหว่างภาคธุรกิจและผู้บริโภค ซึ่งคณะกรรมการดังกล่าวจะเป็นผู้กำหนดนโยบายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล รวมไปถึงการกำหนดหลักเกณฑ์และคำแนะนำอันเป็นแนวทางปฏิบัติ เพื่อให้องค์กรต่างๆดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

Personal Data Protection Act 2012 มีลักษณะเด่นคือการแบ่งความคุ้มครองข้อมูลส่วนบุคคลออกเป็นสองประการ ได้แก่

1. หลักเกณฑ์เกี่ยวกับ Do Not Call ซึ่งมีผลใช้บังคับในวันที่ 2 มกราคม 2014
2. หลักเกณฑ์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล มีผลใช้บังคับเมื่อวันที่ 2 กรกฎาคม 2014

ซึ่งในที่นี้จะกล่าวถึงหลักเกณฑ์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเท่านั้นโดย PDPA กำหนดความหมายของคำซึ่งใช้ในกฎหมายดังกล่าวไว้ในมาตรา 2 โดยมีสาระสำคัญ ดังนี้

“ธุรกิจ” ให้รวมถึงกิจกรรมใดๆขององค์กร ไม่ว่าจะกระทำโดยมีวัตถุประสงค์เพื่อกำไรหรือเป็นการกระทำปกติ ซ้ำๆหรือต่อเนื่อง แต่ไม่รวมถึงการที่บุคคลธรรมดากระทำโดยอาศัยความสามารถของตน

---

[22]**Personal Data Protection Act 2012**

Section3

The purpose of this Act is to govern the collection, use and disclosure of personal data by organization in a manner that regcognises both the right of individuals to protect their personal data and the need of organizations to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances.

“ข้อมูลการติดต่อทางธุรกิจ” หมายถึง ชื่อปัจเจกบุคคล ตำแหน่ง เบอร์โทรศัพท์ซึ่งใช้ในทางธุรกิจ ที่อยู่ซึ่งใช้ในทางธุรกิจ อีเมล เบอร์แฟ็กซ์ซึ่งใช้ทางธุรกิจ หรือข้อมูลอื่นที่มีลักษณะเช่นเดียวกันอันเกี่ยวกับปัจเจกบุคคล ซึ่งมิได้ถูกจัดเตรียมโดยบุคคลนั้นเพียงเพื่อวัตถุประสงค์ส่วนตัว

“คนกลางทางข้อมูล” หมายถึง องค์กรซึ่งประมวลผลข้อมูลส่วนบุคคลในนามขององค์กรอีกองค์กรหนึ่งแต่ไม่รวมถึงลูกจ้างขององค์กรอื่น

“เอกสาร” ให้รวมถึงข้อมูลซึ่งถูกบันทึกไม่ว่าในรูปแบบใดๆ

“วัตถุประสงค์เพื่อการประมวลผล” หมายถึง

a. เพื่อวัตถุประสงค์ในการตัดสินใจเกี่ยวกับความเหมาะสม หรือคุณสมบัติของบุคคลซึ่งข้อมูลนั้นเกี่ยวข้องในกรณีดังต่อไปนี้

i เพื่อการจ้างงาน

ii เพื่อการเลื่อนตำแหน่งในการจ้างงานหรือเพื่อการจ้างงานต่อ

iii เพื่อการเลิกจ้าง

iv เพื่อการรับเข้าศึกษา

v เพื่อการเข้าทำสัญญา ให้รางวัล ให้ทุนการศึกษา หรือให้ประโยชน์อื่นในลักษณะเช่นเดียวกัน

vi เพื่อการคัดเลือกนักกีฬา หรือวัตถุประสงค์ทางศิลปะ

vii เพื่อการให้ความช่วยเหลือทางการเงินหรือทางสังคม หรือการให้บริการทางสุขภาพที่เหมาะสมตามแผนการบริหารของหน่วยงานรัฐ

b. เพื่อวัตถุประสงค์ในการตัดสินใจในการดำเนินต่อไป การเปลี่ยนแปลง หรือการยกเลิกซึ่งสัญญา รางวัล ทุนการศึกษา ทุนเล่าเรียน เกียรติบัตร หรือประโยชน์อื่นที่มีลักษณะเช่นเดียวกัน

c. เพื่อวัตถุประสงค์ในการตัดสินใจให้การรับประกันชีวิตหรือประกันภัยทรัพย์สินดำเนินต่อไป หรือต่ออายุการประกันภัยนั้น

d เพื่อวัตถุประสงค์อื่นซึ่งกำหนดโดยรัฐมนตรี

“ปัจเจกบุคคล” หมายถึง บุคคลธรรมดาไม่ว่ายังมีชีวิตอยู่หรือไม่ก็ตาม

“ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลไม่ว่าจะถูกต้องหรือไม่ก็ตามเกี่ยวกับบุคคลซึ่งอาจถูกระบุตัวได้โดย

a. จากข้อมูลนั้น หรือ

b. จากข้อมูลนั้นและข้อมูลอื่นซึ่งองค์กรมีอยู่หรือมีโอกาสเข้าถึงได้

“ประมวลผล” หมายถึง การดำเนินการหรือชุดของการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล และให้รวมถึง

a. การบันทึก

b. การครอบครอง

c. การจัดเรียง การปรับปรุงหรือการเปลี่ยนแปลง

d. การกู้คืน

e. การรวม

f. การเผยแพร่

g. การลบหรือการทำลาย

เมื่อพิจารณาถึงความหมายของข้อมูลส่วนบุคคลแล้วจะเห็นได้ว่าหมายถึงข้อมูลที่สามารถระบุตัวเจ้าของข้อมูลได้โดยข้อมูลนั้นเอง หรือจากการนำข้อมูลมาประกอบกับข้อมูลนั้น ทำให้ภายใต้ PDPA ของประเทศสิงคโปร์จะถือว่า IP Address เป็นข้อมูลส่วนบุคคลต่อเมื่อข้อมูลนั้นสามารถเชื่อมโยงไปยังเจ้าของข้อมูลได้[23] ในกรณีของการบังคับใช้ PDPA มีผลบังคับใช้ต่อหน่วยงานหรือองค์กรทุกองค์กรแต่จะไม่นำมาบังคับใช้แก่บางกรณี อาทิ บุคคลซึ่งกระทำเป็นการส่วนตัวหรือโดยอาศัยความสามารถของตนเพียงลำพัง หรือลูกจ้างซึ่งกระทำในทางการที่จ้าง หรือหน่วยงานของรัฐ องค์กรซึ่งกระทำในนามของหน่วยงานรัฐเกี่ยวกับการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลหรือองค์กรอื่นหรือข้อมูลส่วนบุคคล หรือประเภทขององค์กรหรือข้อมูลส่วนบุคคลตามที่บัญญัติไว้ในบทบัญญัตินี้ โดยองค์กรจะต้องแต่ตั้งบุคคลคนหนึ่งหรือหลายคนให้มีหน้าที่รับผิดชอบการปฏิบัติตามพระราชบัญญัตินี้ขององค์กร ต้องมีการออกนโยบายแนวปฏิบัติซึ่งจำเป็นเพื่อให้องค์กรปฏิบัติหน้าที่ตามบทบัญญัตินี้ มีกระบวนการในการรับและตอบข้อร้องเรียนที่อาจเกิดขึ้นจากการบังคับใช้พระราชบัญญัตินี้ และหากมีการร้องขอองค์กรต้องเปิดเผยนโยบายและแนวปฏิบัติเพื่อให้องค์กรปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ และกระบวนการในการร้องเรียนสาระสำคัญของพระราชบัญญัติดังกล่าวพิจารณาได้ ดังนี้

---

[23] Personal Data Protection Commission Singapore, “factsheetAccedssed20 February 2016,https://www.pdpc.gov.sg/docs/default-source/public-consultation/factsheet-pdpc_public_consultation_(5feb2013).pdf?sfvrsn=2

1. ความยินยอม

ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล PDPA กำหนดให้องค์กรสามารถทำได้ใน 3 กรณี คือ 1. ได้รับความยินยอมจากปัจเจกบุคคล 2. ถือว่าปัจเจกบุคคลนั้นได้ให้ความยินยอมในการเก็บรวบรวม ใช้ หรือ 3. เปิดเผยแล้ว หรือเป็นกรณีที่สามารถกระทำได้โดยไม่จำต้องได้รับความยินยอมจากปัจเจกบุคคล โดยในการขอความยินยอมจะไม่ถือว่าปัจเจกบุคคลให้ความยินยอมจนกว่าองค์กรจะแจ้งถึงวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และปัจเจกบุคคลนั้นได้ให้ความยินยอม PDPA ห้ามองค์กรพยายามเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยการให้ข้อมูลผิดหรือก่อให้เกิดความเข้าใจผิดเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล หรือกระทำการหลอกลวงหรือก่อให้เกิดความเข้าใจผิด และหากความยินยอมจำเป็นเพื่อการให้บริการองค์กรต้องไม่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเกี่ยวกับปัจเจกบุคคลเกินไปกว่าที่จำเป็นเพื่อการให้บริการ

หากปัจเจกบุคคลนั้นได้จัดเตรียมข้อมูลส่วนบุคคลให้แก่องค์กรเพื่อวัตถุประสงค์นั้นๆ และมีเหตุผลเชื่อว่าปัจเจกบุคคลนั้นเต็มใจที่จะจัดเตรียมข้อมูลให้แก่องค์กร ถือว่าปัจเจกบุคคลได้ให้ความยินยอมแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลหาก เมื่อปัจเจกบุคคลให้ความยินยอมหรือถือว่าได้ให้ความยินยอมแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลแล้ว ปัจเจกบุคคลมีสิทธิเพิกถอนความยินยอมได้หรือถือว่าได้ให้ความยินยอมได้โดยการแจ้งแก่องค์กร เมื่อองค์กรได้รับการแจ้งแล้วต้องบอกปัจเจกบุคคลถึงผลกระทบที่อาจเกิดขึ้นจากการเพิกถอนความยินยอมนั้น ทั้งนี้องค์กรต้องไม่ขัดขวางปัจเจกบุคคลในการเพิกถอนความยินยอม ในกรณีเช่นนี้องค์รวมถึงคนกลางทางข้อมูลและตัวแทนต้องหยุดเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เว้นแต่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นอาจถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยไม่จำต้องได้รับความยินยอมจากปัจเจกบุคคลหรือเป็นกรณีตามที่กฎหมายบัญญัติไว้

2. วัตถุประสงค์

องค์กรอาจเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเกี่ยวกับปัจเจกบุคคลได้เพื่อวัตถุประสงค์ซึ่งวิญญูชนพิจารณาว่าเหมาะสมสำหรับสถานการณ์นั้นและองค์กรได้แจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลแก่ปัจเจกบุคคลแล้ว ซึ่งในการแจ้งวัตถุประสงค์แก่ปัจเจกบุคคลนี้องค์กรต้องแจ้งถึง

1. วัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลก่อนหรือขณะทำการเก็บรวบรวมข้อมูลส่วนบุคคล

2. หากจะนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยเพื่อวัตถุประสงค์อื่นซึ่งมิได้แจ้งปัจเจกบุคคล องค์กรต้องแจ้งวัตถุประสงค์ใหม่นี้แก่ปัจเจกบุคคลก่อทำการใช้หรือเปิดเผยข้อมูลส่วนบุคคลนั้น

3. หากมีการร้องขอโดยปัจเจกบุคคล องค์กรต้องแจ้งถึงข้อมูลการติดต่อทางธุรกิจของบุคคลซึ่งสามารถตอบคำถามของปัจเจกบุคคลในนามขององค์กรเกี่ยงกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

หากองค์กรเก็บรวบรวมข้อมูลส่วนบุคคลจากองค์กรอื่นซึ่งมิได้ขอความยินยอมจากปัจเจกบุคคล องค์กรต้องจัดเตรียมข้อมูลเกี่ยวกับวัตถุประสงค์การเก็บรวบรวมก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคล เพื่อให้องค์กรอื่นพิจารณาว่าการเปิดเผยจะเป็นไปตามบทบัญญัติแห่งกฎหมายนี้หรือไม่

3. การเข้าถึงข้อมูลส่วนบุคคล

ปัจเจกบุคคลมีสิทธิขอเข้าถึงข้อมูลส่วนบุคคลของตนได้ และองค์กรต้องจัดเตรียมข้อมูลตามที่ร้องขอแก่ปัจเจกบุคคลภายในเวลาอันสมควรซึ่งได้แก่ ข้อมูลส่วนบุคคลเกี่ยวกับปัจเจกบุคคลนั้นซึ่งอยู่ในความครอบครองหรืออยู่ภายใต้การควบคุมขององค์กร และข้อมูลเกี่ยวกับเกี่ยวกับกรณีซึ่งองค์กรนำข้อมูลส่วนบุคคลนั้นไปใช้หรือเปิดเผยภายในหนึ่งปีก่อนวันที่มีการร้องขอเข้าถึงข้อมูลส่วนบุคคล อย่างไรก็ตามในบางกรณีองค์กรอาจได้รับยกเว้นไม่จำต้องเปิดเผยข้อมูลส่วนบุคคลได้โดยข้อยกเว้นดังกล่าวได้กำหนดไว้ใน Fifth Schedule ซึ่งประกอบด้วยข้อยกเว้นหลายประการ อาทิ ข้อมูลส่วนบุคคลเกี่ยวกับผู้รับประโยชน์ในทรัสต์ซึ่งถูกเก็บรักษาเพียงเพื่อวัตถุประสงค์ในการจัดการกองทรัสต์ หรือข้อมูลส่วนบุคคลนั้นเก็บรักษาโดยสถาบันอนุญาโตตุลาการหรือศูนย์ประนอมข้อพิพาทเพียงเพื่อวัตถุประสงค์เกี่ยวกับอนุญาโตตุลาการหรือการประนอมข้อพิพาทที่จัดการโดยสถาบันอนุญาโตตุลาการหรือศูนย์ประนอมข้อพิพาทนั้น ข้อมูลส่วนบุคคลที่ตกอยู่ภายใต้เอกสิทธิ์ตามกฎหมาย หรือข้อมูลส่วนบุคคลซึ่งหากมีการเปิดเผยแล้วอาจก่อให้ความลักทางการค้าถูกเปิดเผยซึ่งตามความรู้สึกของวิญญูชนอาจกระทบต่อสถานะการแข่งขันขององค์กรนั้น

องค์กรต้องไม่จัดเตรียมข้อมูลส่วนบุคคลของปัจเจกบุคคลหรือข้อมูลอื่นให้แก่ปัจเจกบุคคลตามที่ร้องขอหากข้อมูลส่วนบุคคลนั้นหรือข้อมูลอื่นอาจก่อให้เกิดกรณีดังต่อไปนี้

1. คุกคามต่อความปลอดภัย สุขภาพร่างกาย หรือสุขภาพจิตใจของปัจเจกบุคคลซึ่งมิใช่ผู้ร้องขอเข้าถึงข้อมูลส่วนบุคคลนั้น

2. ก่อให้เกิดอันตรายร้ายแรงหรือเฉียบพลันเกี่ยวกับความปลอดภัยของสุขภาพร่ายกายหรือสุขภาพจิตใจของปัจเจกบุคคลซึ่งร้องขอเข้าถึงข้อมูลส่วนบุคคลนั้น

3. เป็นการเปิดเผยข้อมูลส่วนบุคคลของปัจเจกบุคคลอื่น

4. เปิดเผยถึงลักษณะเฉพาะของปัจเจกบุคคลซึ่งให้ข้อมูลส่วนบุคคลเกี่ยวกับบุคคลอื่นและปัจเจกบุคคลซึ่งให้ข้อมูลส่วนบุคคลนั้นมิได้ให้ความยินยอมในการเปิดเผยลักษณะเฉพาะของตน

5. เป็นการขัดต่อผลประโยชน์ของประเทศ

ในกรณีที่องค์กรต้องเปิดเผยข้อมูลส่วนบุคคลตามบทบัญญัติแห่งกฎหมายหากการเปิดเผยนั้นจำเป็นเพื่อบริการทางกฎหมายโดยองค์กรหรือเป็นการเปิดเผยที่จำเป็นเพื่อการใช้บริการทางกฎหมายขององค์กร หรือข้อมูลส่วนบุคคลถูกเปิดเผยแก่เจ้าหน้าที่รัฐโดยมีหนังสือลงนามโดยหัวหน้าหน่วยงานนั้นรับรองว่าข้อมูลส่วนบุคคลนั้นจำเป็นเพื่อวัตถุประสงค์ในการดำเนินการหรือเป็นหน้าที่ของเจ้าหน้าที่นั้น องค์กรไม่จำต้องแจ้งแก่เจ้าของข้อมูลส่วนบุคคลถึงการเปิดเผยนั้น

หากปัจเจกบุคคลพบความบกพร่องของข้อมูลส่วนบุคคลปัจเจกบุคคลอาจร้องขอให้องค์กรทำการแก้ไขความบกพร่องหรือความไม่สมบูรณ์ของข้อมูลส่วนบุคคลซึ่งอยู่ในความครอบครองหรือภายใต้การควบคุมขององค์กรได้ ในกรณีเช่นนี้หากองค์กรมิได้รับการยกเว้นตามบทบัญญัติแห่งกฎหมายหรือไม่มีเหตุอันสมควรในการไม่แก้ไขข้อมูลส่วนบุคคลนั้น องค์กรจะต้องดำเนินการดังต่อไปนี้

1. แก้ไขข้อมูลส่วนบุคคลโดยเร็วเท่าที่จะสามารถกระทำได้ และ

2. ส่งการแก้ไขข้อมูลส่วนบุคคลนั้นให้แก่องค์กรอื่นซึ่งข้อมูลส่วนบุคคลนั้นถูกเปิดเผยโดยองค์กรภายในหนึ่งปีก่อนที่มีการร้องขอแก้ไขข้อมูลส่วนบุคคลของปัจเจกบุคคล เว้นแต่องค์กรได้รับการยกเว้นไม่จำต้องแก้ไขข้อมูลส่วนบุคคลตามที่ปัจเจกบุคคลร้องขอเนื่องจากเหตุผลทางกฎหมายหรือทางธุรกิจ

ในกรณีที่เจ้าของข้อมูลส่วนบุคคลยินยอม องค์กรอาจส่งการแก้ไขข้อมูลส่วนบุคคลนั้นไปยังองค์กรที่ข้อมูลส่วนบุคคลนั้นถูกเปิดเผยภายใน 1 ปีก่อนที่จะมีการร้องขอแก้ไขข้อมูลส่วนบุคคลนั้น และเมื่อองค์กรที่ได้รับข้อมูลส่วนบุคคลมาได้รับแจ้งถึงการแก้ไขข้อมูลส่วนบุคคลองค์กรนั้นจะต้องแก้ไขข้อมูลส่วนบุคคลที่อยู่ในความครอบครองหรือความควบคุมของตน เว้นแต่ได้รับยกเว้นตามบทบัญญัติกฎหมายหรือมีเหตุผลประการอื่น

<u>4.การเก็บรักษาข้อมูลส่วนบุคคล</u>

องค์กรต้องใช้ความพยายามตามสมควรเพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมโดยองค์กรหรือถูกเก็บรวบรวมในนามขององค์กรนั้นถูกต้องและสมบูรณ์ หากข้อมูลส่วนบุคคลนั้นอาจถูกใช้โดยองค์กรเพื่อการตัดสินใจซึ่งกระทบต่อปัจเจกบุคคลซึ่งเกี่ยวข้องกับข้อมูลนั้นหรือข้อมูลนั้นอาจถูกเปิดเผยโดยองค์กรไปยังองค์กรอื่น

ในการเก็บรักษาข้อมูลส่วนบุคคลองค์กรต้องป้องกันข้อมูลส่วนบุคคลซึ่งอยู่ในความครอบครองหรือความควบคุมขององค์กรโดยจัดให้มีการรักษาความปลอดภัยตามสมควรเพื่อป้องกันมิ

ให้ข้อมูลส่วนบุคคลนั้นถูกเข้าถึงโดยไม่ได้รับอนุญาต แก้ไข ใช้ เปิดเผย คัดลอก เปลี่ยนแปลง ทำลาย หรือความเสี่ยงอื่นที่มีลักษณะเช่นเดียวกัน

และในการเก็บรักษาข้อมูลส่วนบุคคลนั้น PDPA กำหนดให้องค์กรต้องไม่เก็บรักษาเอกสารซึ่งมีข้อมูลส่วนบุคคล หรือต้องลบวิธีการซึ่งข้อมูลส่วนบุคคลนั้นสามารถเชื่อมโยงไปยังปัจเจกบุคคลได้ เมื่อมีกรณีดังต่อไปนี้

1. การเก็บรักษาข้อมูลส่วนบุคคลนั้นไม่สามารถใช้เพื่อวัตถุประสงค์ซึ่งข้อมูลส่วนบุคคลนั้นถูกเก็บรวบรวมอีกต่อไป

2. การเก็บรักษาข้อมูลส่วนบุคคลนั้นไม่จำเป็นเพื่อวัตถุประสงค์ทางกฎหมายหรือทางธุรกิจอีกต่อไป

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสิงคโปร์มีผลใช้บังคับเมื่อเดือนกรกฎาคม ค.ศ. 2014 ซึ่งนับถึงปัจจุบันเป็นเวลาไม่ถึงสองปี โดย Personal Data Protection Act แยกความคุ้มครองระหว่างข้อมูลเกี่ยวกับปัจเจกบุคคลซึ่งใช้ในการติดต่อทางธุรกิจออกจากข้อมูลเกี่ยวกับปัจเจกบุคคลทั่วไปเพื่อมิให้เป็นอุปสรรคต่อการเก็บรวบรวมข้อมูลส่วนบุคคลซึ่งใช้ในการติดต่อทางธุรกิจและช่วยให้การดำเนินธุรกิจเป็นไปได้สะดวกขึ้น นอกจากนี้ยังให้ความหมายของข้อมูลส่วนบุคคลรวมถึงข้อมูลที่องค์กรมีอยู่และอาจระบุตัวปัจเจกบุคคลได้โดยอาศัยข้อมูลข้อมูลอื่นซึ่งองค์กรมีอยู่หรือมีโอกาสเข้าถึงได้

สำหรับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล Personal Data Protection Act กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเสียก่อน และกำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของตนเอง หากเห็นว่าข้อมูลส่วนบุคคลของตนไม่ถูกต้อง ครบถ้วน หรือเป็นปัจจุบัน เจ้าของข้อมูลส่วนบุคคลสามารถขอให้ผู้ควบคุมข้อมูลส่วนบุคลแก้ไขได้ ในกรณีเช่นนี้ผู้ควบคุมข้อมูลส่วนบุคคลต้องแก้ไขข้อมูลส่วนบุคคลโดยเร็วเท่าที่จะสามารถกระทำได้ และส่งการแก้ไขข้อมูลส่วนบุคคลนั้นให้แก่องค์กรอื่นซึ่งได้รับการเปิดเผยข้อมูลส่วนบุคคลนั้น และในด้านข้อมูล IP Address จะถือเป็นข้อมูลส่วนบุคคลต่อเมื่อข้อมูลนั้นสามารถเชื่อมโยงไปยังเจ้าของข้อมูลได้

ตารางที่ 3.1

สรุปกฎหมายต่างประเทศที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลในบริบทอิเล็กทรอนิกส์

	เรื่อง	ประเทศสหรัฐอเมริกา	สหภาพยุโรป	ประเทศอังกฤษ	ประเทศแคนาดา	ประเทศสิงคโปร์
	ชื่อกฎหมาย	Consumer Privacy Bill of Right 2015 และ Do Not Track Online Bill 2015	General Data Protection Regulation	The Data Protection Act 1998	The Personal Information Protection and Electronic Document Act 2000	Personal Data Protection Act 2012
1.	ข้อมูล Mac Address หรือ IP Address	ถือเป็นข้อมูลส่วนบุคคล	หากสามารถเชื่อมโยงไปยังเจ้าของข้อมูลส่วนบุคคลได้ถือเป็นข้อมูลส่วนบุคคล	หากสามารถเชื่อมโยงไปยังเจ้าของข้อมูลส่วนบุคคลได้ถือเป็นข้อมูลส่วนบุคคล	หากสามารถเชื่อมโยงไปยังเจ้าของข้อมูลส่วนบุคคลได้ถือเป็นข้อมูลส่วนบุคคล	หากสามารถเชื่อมโยงไปยังเจ้าของข้อมูลส่วนบุคคลได้ถือเป็นข้อมูลส่วนบุคคล
2.	ข้อมูล Pseudonymous	ไม่ปรากฏความคุ้มครอง	- เป็นข้อมูลส่วนบุคคล - ผู้ควบคุมข้อมูลส่วนบุคคลต้องไม่ประมวลผลเพิ่มเติมเพื่อทราบเจ้าของข้อมูลส่วนบุคคลเพียงเพื่อปฏิบัติตามกฎหมายฉบับนี้	ไม่ปรากฏความคุ้มครองตาม The Data Protection Act 1998	ถือเป็นข้อมูลที่สามารถเชื่อมโยงไปยังเจ้าของข้อมูลส่วนบุคคลได้จึงเป็นข้อมูลส่วนบุคคล	ไม่ปรากฏความคุ้มครองตาม Personal Data Protection Act 2012

	เรื่อง	ประเทศสหรัฐอเมริกา	สหภาพยุโรป	ประเทศอังกฤษ	ประเทศแคนาดา	ประเทศสิงคโปร์
			- เมื่อการระบุตัวเจ้าของข้อมูลส่วนบุคคลไม่จำเป็นอีกต่อไป ผู้ควบคุมข้อมูลส่วนบุคคลต้องลบข้อมูลอื่นที่ทำให้สามารถเชื่อมโยงไปยังเจ้าของข้อมูลส่วนบุคคลได้			
3.	การทำProfiling และการตัดสินใจโดยระบบอัตโนมัติ	ไม่ปรากฏความคุ้มครอง	- เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านการทำ Profiling และ การตัดสินใจโดยระบบอัตโนมัติ - ในกรณีที่มีการทำ Profiling และการตัดสินใจโดยระบบอัตโนมัติ ผู้ควบคุมข้อมูลส่วนบุคคลต้องแต่งตั้งบุคคลธรรมดา	- การทำ Profiling หากใช้ข้อมูลจากปัจเจกบุคคล ถือเป็นข้อมูลส่วนบุคคล - เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านการตัดสินใจโดยระบบอัตโนมัติ	เป็นข้อมูลที่สามารถเชื่อมโยงไปยังปัจเจกบุคคลได้ จึงเป็นข้อมูลส่วนบุคคล	ไม่ปรากฏความคุ้มครองตาม Personal Data Protection Act 2012

	เรื่อง	ประเทศสหรัฐอเมริกา	สหภาพยุโรป	ประเทศอังกฤษ	ประเทศแคนาดา	ประเทศสิงคโปร์
			เพื่อดูแลควบคุมการทำงานของระบบอัติโนมัตินั้น - เจ้าของข้อมูลส่วนบุคคลมีสิทธิให้ความเห็นเกี่ยวกับผลลัพธ์ที่ได้จากระบบอัตโนมัตินั้น			
4.	ข้อมูล Biometric	ถือเป็นข้อมูลส่วนบุคคล	เป็นข้อมูลที่มีความอ่อนไหว ห้ามมิให้เก็บรวบรวม ประมวลผล หรือเปิดเผย เว้นแต่เป็นไปตามข้อยกเว้น	ถือเป็นข้อมูลส่วนบุคคล	ถือเป็นข้อมูลส่วนบุคคล โดยมีคำแนะนำของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้อย่างระมัดระวัง	ไม่ปรากฏความคุ้มครองตาม Personal Data Protection Act 2012
5.	สิทธิในการโอนข้อมูลส่วนบุคคล (Right to data portability)	มีโครงการ Smart Disclosure ให้สิทธิเจ้าของข้อมูลส่วนบุคคลสามารถนำข้อมูลของตนเองไป	ให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลโอนข้อมูลของตนไปยังผู้ประกอบการอื่นได้	มีโครงการ MiData ให้สิทธิเจ้าของข้อมูลส่วนบุคคลสามารถนำข้อมูลของตนไปวิเคราะห์การใช้จ่ายเพื่อตัด	ไม่ปรากฏสิทธิในการโอนข้อมูลส่วนบุคคล (Right to data portability)ตาม The Personal	ไม่ปรากฏสิทธิในการโอนข้อมูลส่วนบุคคล (Right to data portability) ตาม Personal Data

	เรื่อง	ประเทศสหรัฐอเมริกา	สหภาพยุโรป	ประเทศอังกฤษ	ประเทศแคนาดา	ประเทศสิงคโปร์
		วิเคราะห์เพื่อเลือกสินค้าหรือบริการให้เหมาะสมกับตนมากที่สุด และตัดค่าใช้จ่ายที่ไม่จำเป็น		ค่าใช้จ่ายที่ไม่จำเป็น และสามารถเลือกสินค้าและบริการให้ตรงตามความต้องการของตนมากที่สุด	Information Protection and Electronic Document Act 2000	Protection Act 2012

บทที่ 4
กฎหมายไทยที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลและปัญหาในการคุ้มครองข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์

4.1 ภาพรวมของกฎหมายไทยกับการคุ้มครองข้อมูลส่วนบุคคล

การคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยมีมายาวนานภายใต้กฎหมายทั่วไปซึ่งมิได้บัญญัติขึ้นเพื่อควบคุมการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล สามารถแบ่งได้เป็น 3 ประการ คือ กฎหมายรัฐธรรมนูญ ประมวลกฎหมายแพ่งและพาณิชย์ และประมวลกฎหมายอาญา

(1) กฎหมายรัฐธรรมนูญ

ประเทศไทยได้กล่าวถึงข้อมูลส่วนบุคคลในฐานเป็นสิทธิมนุษยชนขั้นพื้นฐานอันได้รับความคุ้มครองตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช2550 ในมาตรา 4 และมาตรา 35 และมาตรา 36 ความว่า

“**มาตรา 4** ศักดิ์ศรีความเป็นมนุษย์ สิทธิเสรีภาพ และความเสมอภาคของบุคคลย่อมได้รับความคุ้มครอง” และ

“**มาตรา 35** สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง ตลอดจนความเป็นอยู่ส่วนตัวย่อมได้รับความคุ้มครอง

การกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชนอันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัวจะกระทำมิได้ เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณะ

บุคคลย่อมมีสิทธิได้รับความคุ้มครองจากการแสวงประโยชน์โดยมิชอบจากข้อมูลส่วนบุคคลที่เกี่ยวกับตน ทั้งนี้ตามที่กฎหมายบัญญัติ”

“**มาตรา 36** บุคคลย่อมมีเสรีภาพในการสื่อสารถึงกันโดยทางที่ชอบด้วยกฎหมาย

การตรวจ การกัก หรือการเปิดเผยสิ่งสื่อสารที่บุคคลมีติดต่อถึงกัน รวมทั้งการกระทำด้วยประการอื่นใดเพื่อให้ล่วงรู้ถึงข้อความในสิ่งสื่อสารทั้งหลายที่บุคคลติดต่อถึงกันจะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายเฉพาะเพื่อรักษาความมั่นคงของรัฐ หรือเพื่อรักษาความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน”

ด้วยเหตุนี้ปวงชนชาวไทยจึงได้รับความคุ้มครองในเกียรติยศ ชื่อเสียง และความเป็นอยู่ส่วนตัว ผู้ใดจะทำการกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความหรือภาพไปยังสาธารณะชนอันมิได้เป็นไปเพื่อประโยชน์สาธารณะซึ่งการละเมิดหรือกระทบต่อเกียรติยศ ชื่อเสียง หรือความเป็นอยู่

ส่วนตัวของบุคคลอื่นมิได้ นอกจากนี้รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช2550 ยังได้ให้ความคุ้มครองแก่การสื่อสาร และห้ามมิให้ทำการตรวจ กัก หรือเปิดเผยสิ่งสื่อสารที่บุคคลติดต่อกัน รวมถึงห้ามกระทำการใดๆเพื่อให้รู้ข้อความที่บุคคลติดต่อสื่อสารกันด้วย เว้นแต่การกระทำ การตรวจ กัก หรือเปิดเผยนั้นได้เป็นไปเพื่อรักษาความมั่นคงของรัฐ หรือความสงบเรียบร้อยของประชาชน

ต่อมาเมื่อเกิดการัฐประหารขึ้นในประเทศไทยเมื่อวันที่ 22 พฤษภาคม 2557 รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช2550 ก็ได้ถูกยกเลิก ทำให้ในขณะนี้ประไทยยังมิได้มีรัฐธรรมนูญใช้บังคับอย่างเป็นการถาวร คงมีเพียงรัฐธรรมนูญ(ฉบับชั่วคราว) พุทธศักราช 2557 บังคับใช้ ซึ่งรัฐธรรมนูญชั่วคราวฉบับดังกล่าวแตกต่างจากรัฐธรรมนูญฉบับก่อนหน้าที่มีบทบัญญัติหลายมาตราครอบคลุมถึงสิทธิ เสรีภาพของประชาชน แต่รัฐธรรมนูญชั่วคราวฉบับนี้มีเพียงมาตรา 4 เท่านั้นที่บัญญัติถึงศักดิ์ศรีความเป็นมนุษย์ สิทธิ เสรีภาพและความเสมอภาคของประชาชน โดยมาตรา 4 บัญญัติไว้ ดังนี้

“**มาตรา 4** ภายใต้บังคับบทบัญญัติแห่งรัฐธรรมนูญนี้ ศักดิ์ศรีความเป็นมนุษย์ สิทธิ เสรีภาพ และความเสมอภาค บรรดาที่ชนชาวไทยเคยได้รับการคุ้มครองตามประเพณีการปกครองประเทศไทยในระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขและตามพันธกรณีระหว่างประเทศที่ประเทศไทยมีอยู่แล้ว ย่อมได้รับความคุ้มครองตามรัฐธรรมนูญนี้”

แม้มาตรา 4 แห่งรัฐธรรมนูญ (ฉบับชั่วคราว) พุทธศักราช 2557 จะบัญญัติไว้โดยมิได้มีข้อความยืดยาวนัก แต่ก็ให้ใจความครอบคลุมถึงสิทธิเสรีภาพอย่างกว้าง กล่าวคือ มาตราดังกล่าวได้รับรองศักดิ์ศรีความเป็นมนุษย์ สิทธิ เสรีภาพและความเสมอภาคตามประเพณีการปกครองไทยในระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขและตามพันธกรณีระหว่างประเทศที่ประเทศไทยมีอยู่แล้ว จึงก่อให้เป็นเสมือนการยอมรับบทบัญญัติเกี่ยวกับสิทธิเสรีภาพที่เคยมีมาในอดีตตามที่ได้มีการรับรองไว้ในรัฐธรรมนูญฉบับก่อนๆ ทั้งยังรับรองครอบคลุมไปถึงสิทธิเสรีภาพตามพันธกรณีที่ประเทศไทยได้ผูกพันไว้อีกด้วยแต่อย่างไรก็ตามมาตรา 4 คงบัญญัติว่าภายใต้บังคับแห่งรัฐธรรมนูญฉบับนี้ ดังนั้นการรับรองศักดิ์ศรีความเป็นมนุษย์ สิทธิ เสรีภาพและความเสมอภาคอาจไม่ทัดเทียมกับรัฐธรรมนูญฉบับก่อนๆ จากที่กล่าวมาจะเห็นได้ว่ากฎหมายรัฐธรรมนูญมิได้พูดถึงหลักเกณฑ์เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เพียงแต่มีบทบัญญัติอันเป็นหลักการว่าประเทศไทยมีการคุ้มครองความเป็นส่วนตัวเท่านั้น

(2) ประมวลกฎหมายแพ่งและพาณิชย์

ประมวลกฎหมายแพ่งและพาณิชย์มีบทบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลประมวลกฎหมายแพ่งและพาณิชย์มาตรา 18 ความว่า

“**มาตรา 18** สิทธิของบุคคลในการที่จะใช้นามอันชอบที่จะใช้ได้นั้น ถ้ามีบุคคลอื่นโต้แย้งก็ดี หรือบุคคลผู้เป็นเจ้าของนามนั้นต้องเสื่อมเสียประโยชน์เพราะการที่มีผู้อื่นมาใช้นามเดียวกันโดยมิได้รับอำนาจให้ใช้ก็ดี บุคคลผู้เป็นเจ้าของนามจะเรียกให้บุคคลนั้นระงับความเสียหายก็ได้ ถ้าและเป็นที่วิตกว่าจะต้องเสียหายอยู่สืบไป จะร้องขอต่อศาลให้สั่งห้ามก็ได้”

บทบัญญัตินี้เป็นการคุ้มครองสิทธิของบุคคลในการใช้นาม หากมีบุคคลโต้แย้งการใช้นามหรือมีบุคคลอื่นใช้นามเดียวกันจนก่อความเสื่อเสียประโยชน์แก่เจ้าของนามโดยมิได้รับความยินยอมให้ใช้ บุคคลผู้เป็นเจ้าของนามนั้นสามารถเรียกให้ผู้ใช้นามโดยมิได้รับความยินยอมระงับความเสียหายนั้นได้ และนอกจากมาตรา 18 แล้วยังมีบทบัญญัติเกี่ยวกับการคุ้มครองชื่อเสียงของบุคคลไว้ในเรื่องละเมิดในมาตรา 423 ความว่า

“**มาตรา 423** ผู้ใดกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความอันฝ่าฝืนต่อความจริงเป็นที่เสียหายแก่ชื่อเสียงหรือเกียรติคุณของบุคคลอื่นก็ดี หรือเป็นที่เสียหายแก่ทางทำมาหาได้หรือทางเจริญของเขาโดยประการอื่นก็ดี ท่านว่าผู้นั้นจะต้องใช้ค่าสินไหมทดแทนให้แก่เขาเพื่อความเสียหายอย่างใดๆอันเกิดแต่การนั้น แม้ทั้งเมื่อตนมิได้รู้ว่าข้อความนั้นไม่จริงแต่หากควรจะรู้ได้

ผู้ใดส่งข่าวสาส์นอันตนมิได้รู้ว่าเป็นความไม่จริง หากว่าตนหรือผู้รับข่าวสาส์นนั้นมีทางได้เสียโดยชอบในการนั้นด้วยแล้ว ท่านว่าเพียงที่ส่งข่าวสาส์นเช่นนั้นหาทำให้ผู้นั้นต้องรับผิดใช้ค่าสินไหมทดแทนไม่”

บทบัญญัติดังกล่าวเป็นเรื่องการหมิ่นประมาทในทางแพ่ง โดยกำหนดให้ผู้กล่าวหรือไขข่าวแพร่หลายซึ่งข้อความอันเป็นความเท็จ และก่อให้เกิดความเสียหายแก่ชื่อเสียงเกียรติคุณของผู้เป็นเจ้าของข้อมูล หรือก่อให้เกิดความเสียหายแก่ทางทำมาหาได้หรือทางเจริญของบุคคลอื่นต้องรับผิดใช้ค่าสินไหมทดแทนเพื่อความเสียหายใดๆอันเกิดแก่ผู้อื่นนั้น ทั้งนี้บุคคลภายนอกผู้รับรู้ข่าวสารนั้นหมายถึงบุคคลซึ่งมิใช่ผู้กล่าวหรือไขข่าวเอง มิใช่ตัวผู้ถูกพาดพิงถึง มิใช่ผู้ร่วมกระทำความผิด มิใช่สามีหรือภรรยาของผู้กล่าวหรือไขข่าว และมิใช่คนที่เข้ามารับรู้การกล่าวหรือไขข่าวนั้นโดยบังเอิญ[76] อย่างไรก็ตามประมวลกฎหมายแพ่งและพาณิชย์ก็ได้กำหนดข้อยกเว้นไว้ในวรรค 2 แห่งมาตราดังกล่าว กล่าวคือหากผู้กล่าวหรือไขข่าวแพร่หลายนั้นมีส่วนได้เสียโดยชอบในข่าวสารนั้นและกระทำไปโดยสุจริต คือมิได้รู้ว่าข่าวสารนั้นไม่เป็นความจริง ผู้กล่าวหรือไขข่าวแพร่หลายไม่ต้องรับผิดในความเสียหายที่เกิดขึ้น

---

[76] ศนันท์กรณ์ (จำปี) โสตถิพันธุ์, “คำอธิบายกฎหมายลักษณะละเมิด จัดการงานนอกสั่งและลาภมิควรได้”, กรุงเทพมหานคร, สำนักพิมพ์วิญญูชน, 2550 หน้า 88

จากที่กล่าวมาจะเห็นได้ว่าประมวลกฎหมายแพ่งและพาณิชย์มิได้มุ่งหมายเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล หากแต่เมื่อมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจนก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคล หรือเป็นการหมิ่นประมาทในทางแพ่ง เจ้าของข้อมูลส่วนบุคคลนั้นสามารถเรียกร้องค่าสินไหมทดแทนโดยอาศัยบทบัญญัติว่าด้วยละเมิดได้

(3) ประมวลกฎหมายอาญา

ประมวลกฎหมายอาญาเป็นกฎหมายที่บัญญัติว่าการกรทำหรือไม่กระทำอย่างใดเป็นความผิดและกำหนดโทษที่จะลงแก่ผู้กระทำความผิดไว้ โดยมุ่งควบคุมความประพฤติของบุคคลให้สังคมมีความสงบเรียบร้อย ซึ่งประมวลกฎหมายอาญาบัญญัติคุ้มครองความเป็นส่วนตัวของบุคคลไว้ในลักษณะ 11 ว่าด้วยความผิดเกี่ยวกับเสรีภาพและชื่อเสียงซึ่งมีมาตราที่น่าสนใจจำนวน 5มาตรา คือ มาตรา 322 มาตรา 323 มาตรา 324 มาตรา 326 และ มาตรา 328 ซึ่งมีรายละเอียด ดังนี้

1) มาตรา 322

“**มาตรา 322** ผู้ใดเปิดผนึกหรือเอาจดหมาย โทรเลข หรือเอกสารใดๆซึ่งปิดผนึกของผู้อื่นไป เพื่อล่วงรู้ข้อความก็ดี เพื่อนำข้อความในจดหมาย โทรเลข หรือเอกสารใดๆซึ่งปิดผนึกของผู้อื่นไป เพื่อล่วงรู้ข้อความก็ดี เพื่อนำข้อความในจดหมาย โทรเลขหรือเอกสารเช่นว่านั้นออกเปิดเผยก็ดี ถ้าการกระทำนั้นน่าจะเกิดความเสียหายแก่ผู้หนึ่งผู้ใดต้อระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งพันบาท หรือทั้งจำทั้งปรับ”

ภายใต้มาตราดังกล่าวบุคคลใดกระทำโดยเจตนาด้วยการเปิดผนึกหรือเอาจดหมาย โทรเลข หรือเอกสารใดๆซึ่งปิดผนึกของผู้อื่นไป เพื่อล่วงรู้ข้อความหรือเพื่อนำข้อความในจดหมาย โทรเลข หรือเอกสารนั้นออกเปิดเผย โดยผู้กระทำต้องมีเจตนาพิเศษเพื่อล่วงรู้ข้อความในจดหมาย โทรเลข หรือเอกสารนั้น หรือเพื่อนำข้อความนั้นออกเปิดเผย ทั้งนี้ความผิดจะสำเร็จเมื่อมีการเปิดผนึกหรือมีการเอาไปแม้ผู้กระทำความผิดจะยังไม่ทันล่วงรู้ข้อความในจดหมาย โทรเลข หรือเอกสารนั้นหรือยังไม่ทันได้นำข้อความเหล่านั้นออกเปิดเผยก็ตาม และการกระทำดังกล่าวน่าจะเกิดความเสียหายแก่ผู้หนึ่งผู้ใด กล่าวคือ หากการกระทำนั้นน่าจะก่อความเสียหายแก่ผู้เป็นเจ้าของจดหมาย โทรเลข หรือเอสารใดๆหรือแก่ผู้ใดผู้หนึ่งก็ย่อมเป็นความผิดตามมาตรานี้ โดยความเสียหายดังกล่าวอาจเป็น ความเสียหายต่อชื่อเสียง เกียรติคุณหรือการงานก็ได้

2) มาตรา 323

“**มาตรา 323** ผู้ใดล่วงรู้หรือได้มาซึ่งความลับของผู้อื่น โดยเหตุที่เป็นเจ้าพนักงานผู้มีหน้าที่ โดยเหตุที่ประกอบอาชีพเป็นแพทย์ เภสัชกร คนจำหน่ายยา นางผดุงครรภ์ ผู้พยาบาล นักบวช หมอความ ทนายความ หรือผู้สอบบัญชี หรือโดยเหตุที่เป็นผู้ช่วยในการประกอบ

อาชีพนั้น แล้วเปิดเผยความลับนั้นในประการที่น่าจะเกิดความเสียหายแก่ผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งพันบาท หรือทั้งจำทั้งปรับ

ผู้รับการศึกษาอบรมในอาชีพดังกล่าวในวรรคแรก เปิดเผยความลับของผู้อื่นอันตนได้ล่วงรู้หรือได้มาในการศึกษาอบรม ในประการที่น่าจะเกิดความเสียหายแก่ผู้หนึ่งผู้ใดต้องระวางโทษเช่นเดียวกัน”

ความผิดตามมาตรา 323 วรรคแรก ได้กำหนดวิชาชีพของบุคคลที่จะกระทำความผิดตามมาตรานี้ได้ ดังนี้บุคคลอื่นใดซึ่งมิได้มีวิชาชีพตามที่มาตรา 323 วรรคแรกระบุไว้แม้จะกระทำความผิดครบองค์ประกอบของมาตรา 323 วรรคแรกก็ไม่มีความผิดตามมาตรานี้ โดยบุคคลผู้กระทำความผิดอันจะต้องรับโทษตามมาตรานี้ต้องเป็นเจ้าพนักงานผู้มีหน้าที่ หรือประกอบวิชาชีพแพทย์ เภสัชกร คนจำหน่ายยา นางผดุงครรภ์ ผู้พยาบาล นักบวช หมอความ ทนายความ ผู้สอบบัญชี หรือเป็นผู้ช่วยในการประกอบอาชีพนั้น ล่วงรู้หรือได้มาซึ่งความลับของผู้อื่น และเจตนาทำการเปิดเผยความลับนั้นไม่ว่าด้วยวิธีใดๆ เช่นการบอกกล่าวด้วยวาจา ด้วยลายลักษณ์อักษร หรือเปิดเผยให้เห็นเอง ซึ่งการกระทำนั้นน่าจะเกิดความเสียหายแก่ผู้ใดผู้หนึ่ง กล่าวคือ การเปิดเผยความลับนั้นน่าจะทำให้ผู้ใดผู้หนึ่งได้รับความเสียหายไม่ว่าความเสียหายนั้นจะเกิดขึ้นต่อเจ้าของความลับหรือต่อผู้อื่นที่เกี่ยวข้องก็ได้

ความผิดตามมาตรา 323 วรรคสองมีลักษณะคล้ายกับความผิดตามมาตรา 323 วรรคแรก แต่แตกต่างกันในแง่ของผู้กระทำความผิด กล่าวคือผู้ที่จะกระทำความผิดตามมาตรา 323 วรรคสองได้ต้องเป็นผู้รับการศึกษาอบรมในอาชีพตามมาตรา 323 วรรคแรกได้ล่วงรู้ความลับของผู้อื่นจากการศึกษาอบรวม และทำการเปิดเผยความลับนั้นโดยเจตนาในประการที่น่าจะเกิดความเสียหายแก่ผู้หนึ่งผู้ใด

3) มาตรา 324

“มาตรา 324 ผู้ใดโดยเหตุที่ตนมีตำแหน่งหน้าที่ วิชาชีพ หรืออาชีพอันเป็นที่ไว้วางใจ ล่วงรู้หรือได้มาซึ่งความลับของผู้อื่นเกี่ยวกับอุตสาหกรรม การค้นพบ หรือการนิมิตในทางวิทยาศาสตร์ เปิดเผยหรือใช้ความลับนั้น เพื่อประโยชน์ของตนเองหรือผู้อื่น ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งพันบาท หรือทั้งจำทั้งปรับ”

ประมวลกฎหมายอาญา มาตรา 324 กำหนดให้บุคคลซึ่งมีตำแหน่งหน้าที่วิชาชีพ หรืออาชีพอันเป็นที่ไว้วางใจได้ เช่น เป็นนักเคมี หรือเป็นพนักงานผสมสูตรสินค้า ล่วงรู้หรือได้มาซึ่งความลับของผู้อื่นเกี่ยวกับอุตสาหกรรม การค้นพบ หรือการนิมิตใจวิทยาศาสตร์ หมายความว่าความผิดตามมาตรานี้ผู้กระทำเป็นผู้ล่วงรู้หรือได้มาซึ่งความลับเฉพาะที่เกี่ยวกับอุตสาหกรรม การค้นพบในทางวิทยาศาสตร์ หรือการนิมิตในทางวิทยาศาสตร์ เช่น ความลับของการผลิตสินค้า หรือ

ความลับในการค้นพบยาใหม่ เป็นต้น และโดยเจตนาเปิดเผยความลับนั้นให้ผู้อื่นทราบหรือใช้ความลับของผู้อื่นนั้นนอกเหนือจากหน้าที่การงาน ซึ่งการเปิดเผยหรือการใช้ได้กระทำไปเพื่อประโยชน์ตนเองหรือผู้อื่น กล่าวคือ การเปิดเผยหรือการใช้ความลับนั้นผู้กระทำมีเจตนาพิเศษเพื่อประโยชน์ของตนเองหรือประโยชน์ของผู้อื่น เช่น นำไปผลิตเพื่อขายสินค้านั้นเอง หรือนำสูตรลับไปเปิดเผยแก่พี่น้องเพื่อผลิตสินค้าออกมาขาย เป็นต้น

4) มาตรา 326 และ มาตรา 328

“มาตรา 326ผู้ใดใส่ความผู้อื่นต่อบุคคลที่สาม โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง ผู้นั้นกระทำความผิดฐานหมิ่นประมาท ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาทหรือทั้งจำทั้งปรับ”

“**มาตรา 328** ถ้าความผิดฐานหมิ่นประมาทได้กระทำโดยการโฆษณา ด้วยเอกสาร ภาพวาด ภาพระบายสี ภาพยนตร์ ภาพหรือตัวอักษรที่ทำให้ปรากฏด้วยวิธีใดๆ แผ่นเสียงหรือสิ่งบันทึกเสียง บันทึกภาพ หรือบันทึกอักษร กระทำโดยการกระจายเสียง หรือกระจายภาพ หรือโดยกระทำการป่าวประกาศด้วยวิธีอื่น ผู้กระทำต้องระวางโทษจำคุกไม่เกินสองปีและปรับไม่เกินสองแสนบาท”

ประมวลกฎหมายอาญามาตรา 326 และมาตรา 328 เป็นความผิดฐานหมิ่นประมาทและหมิ่นประมาทด้วยการโฆษณา วัตถุประสงค์ของทั้งสองมาตราคือปกป้องบุคคลให้พ้นจากการถูกผู้อื่นใส่ความ โดยองค์ประกอบความผิดของประมวลกฎหมายอาญา มาตรา 326 มีดังต่อไปนี้ 1. ผู้ใด 2. ใส่ความผู้อื่น 3. ต่อบุคคลที่สาม 4. โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่นหรือถูกเกลียดชัง และ 5. เจตนา

การใส่ความผู้อื่นหมายถึงการแสดงข้อเท็จจริงพาดพิงถึงบุคคลอื่นไม่ว่าข้อเท็จจริงนั้นจะเป็นจริงหรือไม่ก็ตาม หรือเป็นข้อเท็จจริงในอดีตหรือปัจจุบัน และไม่ว่าจะเป็นการแสดงข้อเท็จจริงนั้นด้วยวาจา ลายลักษณ์อักษร ท่าทาง หรือรูปภาพก็ได้ ซึ่งการแสดงข้อความนี้จะเป็นความผิดต่อเมื่อผู้แสดงได้มีการยืนยันข้อเท็จจริงนั้นต่อบุคคลที่สามซึ่งมิใช่ผู้ที่ถูกพาดพิงเองอันน่าจะทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง อย่างไรก็ตามหากคำกล่าวถึงบุคคลที่สามนั้นไม่อาจทำให้คนฟังเชื่อว่าเป็นเช่นนั้นได้ เป็นเพียงการแสดงความคิดเห็น เป็นเพียงการคาดคะเน เป็นเพียงการวิจารณ์การทำงาน หรือเป็นเพียงคำเปรียบเทียบที่ไม่สุภาพเท่านั้น ผู้กล่าวไม่มีความผิดฐานหมิ่นประมาท

และสำหรับประมวลกฎหมายอาญามาตรา 328 เป็นเหตุฉกรรจ์ของความผิดมาตรา 326 อันเป็นการกระทำความผิดฐานหมิ่นประมาทซึ่งได้กระทำโดยการโฆษณาด้วยเอกสาร

ภาพวาด ภาพระบายสี ภาพยนตร์ ภาพหรือตัวอักษรที่ทำให้ปรากฏไม่ว่าด้วยวิธีใด แผ่นเสียงหรือสิ่งบันทึกอย่างอื่น หรือการกระจายเสียงหรือโดยการป่าวประกาศด้วยวิธีใดๆ

การให้ความคุ้มครองตามประมวลกฎหมายอาญาเป็นไปเพื่อป้องปรามมิให้เกิดการกระทำความผิดเพื่อรักษาความสงบเรียบร้อยในสังคม มิได้มีเจตนากำหนดวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ทำให้เจ้าของข้อมูลส่วนบุคคลไม่อาจอาศัยบทบัญญัติแห่งประมวลกฎหมายอาญาเพื่อควบคุมข้อมูลส่วนบุคคลของตนเองได้

เมื่อพิจารณาถึงการให้ความคุ้มครองแก่ความเป็นส่วนตัวตามรัฐธรรมนูญแห่งราชอาณาจักรไทย ประมวลกฎหมายแพ่งและพาณิชย์ และประมวลกฎหมายอาญาดังที่ได้กล่าวมาแล้ว จะเห็นได้ว่าแม้กฎหมายรัฐธรรมนูญจะมีบทบัญญัติคุ้มครองความเป็นส่วนตัว แต่ก็เป็นเพียงบทบัญญัติที่แสดงให้เห็นหลักการของประเทศไทยถึงการให้ความสำคัญและคุ้มครองความเป็นส่วนตัวเท่านั้น โดยมิได้มีบทบัญญัติชัดเจนถึงหลักเกณฑ์หรือวิธีการในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

สำหรับประมวลกฎหมายแพ่งและพาณิชย์แม้จะให้ความคุ้มครองแก่การใช้นามของบุคคลและชื่อเสียงของบุคคลก็ตาม แต่ก็เป็นกฎหมายที่มุ่งเยียวยาผู้ที่ได้รับความเสียหาย โดยมิได้กล่าวถึงหลักการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ภายใต้ประมวลกฎหมายแพ่งและพาณิชย์มิได้ห้ามผู้ใดเก็บรวบรวมข้อมูลส่วนบุคคลโดยมิได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เพียงแต่เจ้าของข้อมูลส่วนบุคคลสามารถเอาผิดแก่ผู้เก็บรวบรวมข้อมูลส่วนบุคคลตามบทบัญญัติว่าด้วยละเมิดหากมีการนำข้อมูลไปใช้ หรือเผยแพร่ข้อมูลนั้นจนเกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคล

ในด้านของประมวลกฎหมายอาญาซึ่งเป็นกฎหมายที่มุ่งป้องปรามการกระทำความผิดแม้จะมีบทบัญญัติเอาโทษกับการล่วงรู้ข้อความในจดหมาย โทรเลข หรือเอกสารใดๆหรือการเผยความลับ การหมิ่นประมาทผู้อื่นก็ตาม แต่จะฟ้องร้องเอาผิดกับผู้กระทำดังกล่าวได้ต้องปรากฏว่ามีความเสียหายหรือน่าจะก่อให้เกิดความเสียหายเสียก่อน ทำให้เจ้าของข้อมูลส่วนบุคคลไม่สามารถควบคุมข้อมูลส่วนบุคคลของตนเองได้โดยอาศัยบทบัญญัติแห่งประมวลกฎหมายอาญา ทั้งมิได้มีบทบัญญัติเกี่ยวกับกล่าวถึงการเก็บรวบรวมข้อมูลส่วนบุคคล กล่าวคือ การเก็บรวบรวมข้อมูลส่วนบุคคลหากมิใช่กรณีตามมาตรา 322-324 ย่อมสามารถทำได้โดยไม่มีความผิด การใช้หรือการเปิดเผยข้อมูลที่ได้เก็บรวบรวมมาสามารถทำได้ตามความประสงค์ของผู้ควบคุมข้อมูลส่วนบุคคลตาบเท่าที่ไม่เป็นความผิดฐานหมิ่นประมาทตามมาตรา 326 และมาตรา 328 โดยเจ้าของข้อมูลส่วนบุคคลไม่อาจ

ควบคุมได้ ดังนั้นทั้งกฎหมายรัฐธรรมนูญ ประมวลกฎหมายแพ่งและพาณิชย์ และประมวลกฎหมายอาญาจึงไม่เหมาะที่จะนำมาใช้แก่การควบคุมการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

4.2 กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย

ดังที่ได้กล่าวมาแล้วมาว่ารัฐธรรมนูญแห่งราชอาณาจักรไทย ประมวลกฎหมายแพ่งและพาณิชย์ และประมวลกฎหมายอาญามิได้ให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลเพียงพอที่จะควบคุมข้อมูลส่วนบุคคลของตนเองได้ ดังนั้นจึงจำเป็นต้องพิจารณากฎหมายอื่นๆของประเทศไทยที่มีความเกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลมากกว่ากฎหมายทั้ง 3 ฉบับดังกล่าวมา โดยกฎหมายที่นำมาศึกษาในที่นี้ ได้แก่

1. พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540
2. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
3.พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
4. พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545และ
5. ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....

โดยมีสาระสำคัญ ดังนี้

4.2.1 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

วัตถุประสงค์ของพระราชบัญญัตินี้ คือต้องการเปิดโอกาสให้ประชาชนได้รับรู้ข้อมูลข่าวสารเกี่ยวกับการดำเนินงานของรัฐจึงกำหนดมาตรการต่างๆ เช่น การนำข้อมูลข่าวสารตามที่กำหนดลงพิมพ์ในราชกิจจานุเบกษา หรือกำหนดให้หน่วยงานของรัฐรวบรวมข้อมูลข่าวสารเพื่อให้ประชาชนสามารถตรวจดูได้ เป็นต้น โดยตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540กำหนดความหมายของข้อมูลข่าวสารไว้ในมาตรา 4 ความว่า

“ข้อมูลข่าวสาร” หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริง ข้อมูล หรือสิ่งใดๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใดๆ และไม่ว่าจะได้จัดทำไว้ในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้”

ดังนั้นข้อมูลข่าวสารจึงมีความหมายค่อนข้างกว้างไม่ว่าเป็นข้อมูลข่าวสารเกี่ยวกับการดำเนินงานของรัฐหรือข้อมูลข่าวสารส่วนบุคคล เช่น ฐานะทางการเงิน การศึกษา หรือ

ประวัติสุขภาพเป็นต้น โดยข้อมูลข่าวสารส่วนบุคคลได้ถูกกำหนดความหมายไว้ในมาตรา 4 เช่นกันซึ่งหมายถึง

"ข้อมูลข่าวสารส่วนบุคคล" หมายความว่า ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้น หรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่าย และให้หมายความรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย"

สำหรับความคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้กำหนดไว้ในหมวด 3 ตั้งแต่มาตรา 21 ถึง 25 โดยในมาตรา 21 กำหนดให้บุคคลในหมวดนี้หมายถึงบุคคลธรรมดาที่มีสัญชาติไทย และบุคคลธรรมดาที่ไม่มีสัญชาติไทยแต่มีถิ่นที่อยู่ในประเทศไทย ด้วยเหตุนี้ผู้ที่จะสามารถใช้สิทธิในฐานเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ได้มีเพียง 2 ประเภท เท่านั้น คือ 1. มีสัญชาติไทย หรือ 2. มิได้มีสัญชาติไทยแต่มีถิ่นที่อยู่ในประเทศไทย ส่งผลให้บุคคลสัญชาติไทยไม่ว่าจะอยู่ในประเทศไทยหรือไม่ก็ตามสามารถที่จะเรียกร้องสิทธิตามพระราชบัญญัตินี้ได้ แต่สำหรับบุคคลซึ่งมิได้มีสัญชาติไทยจะกล่าวอ้างสิทธิ ประโยชน์ หรือความคุ้มครองตามพระราชบัญญัตินี้ได้ต้องเป็นบุคคลที่อยู่ในประเทศไทยเท่านั้น

โดยหน่วยงานของรัฐ[77]ที่จะต้องปฏิบัติตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 นี้ครอบครองคลุมกว้างขวาง เช่นราชการส่วนกลาง ราชการส่วนภูมิภาค หรือราชการส่วนท้องถิ่น เป็นต้น อย่างไรก็ตามในมาตรา 22 ได้กำหนดให้สำนักข่าวกรองแห่งชาติ สำนักงานสภาความมั่นคงแห่งชาติ และหน่วยงานของรัฐแห่งอื่นตามที่กำหนดในกฎกระทรวงซึ่งการเปิดเผยข้อมูลข่าวสารส่วนบุคคลจะเป็นอุปสรรคร้ายแรงต่อการดำเนินการของหน่วยงานดังกล่าวอาจออกระเบียบโดยความเห็นชอบของคณะกรรมการกำหนดหลักเกณฑ์ เงื่อนไข ที่เกี่ยวกับข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานดังกล่าว กำหนดยกเว้นให้หน่วยงานนั้นไม่ต้องดำเนินการการพิมพ์ในราชกิจจานุเบกษา และตรวจสอบแก้ไขให้ถูกต้องเสมอเกี่ยวกับประเภท

---

[77] **พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540**

มาตรา 4

"หน่วยงานของรัฐ" หมายความว่า ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ ส่วนราชการสังกัดรัฐสภา ศาลเฉพาะในส่วนที่ไม่เกี่ยวกับการพิจารณาพิพากษาคดี องค์กรควบคุมการประกอบวิชาชีพ หน่วยงานอิสระของรัฐและหน่วยงานอื่นตามที่กำหนดในกฎกระทรวง

ของข้อมูลส่วนบุคคลที่มีการเก็บไว้ ประเภทของระบบข้อมูลข่าวสารส่วนบุคคล ลักษณะการใช้ข้อมูลตามปกติ วิธีการขอตรวจดูข้อมูลข่าวสารของเจ้าของข้อมูล วิธีการขอให้แก้ไขเปลี่ยนแปลงข้อมูล และแหล่งที่มาของข้อมูล นอกจากหน่วยงานที่ได้กล่าวมานี้ หน่วยงานอื่นๆของรัฐต้องปฏิบัติตามหลักเกณฑ์ในการคุ้มครองข้อมูลข่าวสารส่วนบุคคลตามที่กำหนดในพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ซึ่งมีสาระสำคัญดังต่อไปนี้

หน่วยงานของรัฐมีหน้าที่ตามที่กำหนดไว้ในมาตรา 23 โดยในกรณีที่หน่วยงานของรัฐเก็บข้อมูลข่าวสารโดยตรงจากเจ้าของข้อมูล หน่วยงานของรัฐแจ้งให้เจ้าของข้อมูลทราบถึงวัตถุประสงค์ที่จะนำข้อมูลมาใช้ ลักษณะการใช้ข้อมูลตามปกติ และกรณีที่ขอข้อมูลนั้นเป็นกรณีที่มีกฎหมายบังคับให้เจ้าของข้อมูลต้องยินยอมหรือเจ้าของข้อมูลมีสิทธิตัดสินใจให้ความยินยอมหรือไม่ให้ความยินยอมได้ ล่วงหน้าหรือพร้อมกับการขอข้อมูล หน่วยงานของรัฐมีหน้าที่ต้องปฏิบัติเกี่ยวกับการจัดการข้อมูลข่าวสารส่วนบุคคล ดังต่อไปนี้

(1) หน่วยงานของรัฐต้องมีระบบข้อมูลข่าวสารส่วนบุคคลเพียงเท่าที่เกี่ยวข้องและจำเป็นต่อการดำเนินงานของหน่วยงานรัฐนั้นให้สำเร็จตามวัตถุประสงค์ และต้องยกเลิกระบบข้อมูลส่วนบุคคลนั้นเมื่อหมดความจำเป็น

(2) หน่วยงานของรัฐต้องพยายามเก็บข้อมูลข่าวสารโดยตรงจากเจ้าของข้อมูลโดยเฉพาะอย่างยิ่งในกรณีที่จะกระทบถึงประโยชน์ได้เสียโดยตรงของบุคคลนั้น

(3) จัดพิมพ์ในราชกิจจานุเบกษา และตรวจสอบแก้ไขให้ถูกต้องเสมอเกี่ยวกับ

3.1 ประเภทของบุคคลที่มีการเก็บข้อมูลไว้

3.2 ประเภทของระบบข้อมูลข่าวสารส่วนบุคคล

3.3 ลักษณะการใช้ข้อมูลตามปกติ

3.4 วิธีการขอตรวจดูข้อมูลข่าวสารของเจ้าของข้อมูล

3.5 วิธีการขอให้แก้ไขเปลี่ยนแปลงข้อมูล

3.6 แหล่งที่มาของข้อมูล

(4) ตรวจสอบแก้ไขข้อมูลข่าวสารส่วนบุคคลในความรับผิดชอบของหน่วยงานรัฐนั้นให้ถูกต้องอยู่เสมอ

(5) จัดระบบรักษาความปลอดภัยให้แก่ระบบข้อมูลข่าวสารส่วนบุคคลตามความเหมาะสมเพื่อป้องกันมิให้มีการนำไปใช้โดยไม่เหมาะสมหรือเป็นผลร้ายต่อเจ้าของข้อมูล

นอกจากนี้หน่วยงานของรัฐต้องแจ้งให้เจ้าของข้อมูลทราบหากมีการจัดส่งข้อมูลข่าวสารส่วนบุคคลไปยังที่ใดอันเป็นผลให้บุคคลทั่วไปทราบข้อมูลข่าวสารนั้นได้ เว้นแต่เป็นการใช้ข้อมูลตามปกติ

สำหรับการเปิดเผยข้อมูลข่าวสารส่วนบุคคล หน่วยงานของรัฐจะเปิดเผยข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความควบคุมดูแลของตนต่อหน่วยงานของรัฐแห่งอื่นหรือผู้อื่น โดยปราศจากความยินยอมเป็นหนังสือของเจ้าของข้อมูลที่ให้ไว้ล่วงหน้า หรือขณะทำการเปิดเผยมิได้ เว้นแต่เป็นกรณีใดกรณีหนึ่งใน 9 กรณีดังต่อไปนี้

1. ต่อเจ้าหน้าที่ของรัฐในหน่วยงานของตน เพื่อการนำไปใช้ตามอำนาจหน้าที่ของหน่วยงานของรัฐแห่งนั้น

2. เป็นการใช้ข้อมูลตามปกติภายในวัตถุประสงค์ของการจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลนั้น

3. ต่อหน่วยงานของรัฐที่ทำงานด้วยการวางแผน หรือสถิติ หรือสำมะโนต่างๆซึ่งมีหน้าที่ต้องรักษาข้อมูลข่าวสารส่วนบุคคลไว้ไม่ให้เปิดเผยต่อไปยังผู้อื่น

4. เป็นการให้เพื่อประโยชน์ในการศึกษาวิจัย โดยไม่ระบุชื่อหรือส่วนที่ทำให้รู้ว่าเป็นข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับบุคคลใด

5. ต่อหอจดหมายเหตุแห่งชาติ กรมศิลปากร หรือหน่วยงานอื่นของรัฐตามมาตรา 26 วรรคหนึ่ง

6. ต่อเจ้าหน้าที่ของรัฐเพื่อการป้องกันการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย การสืบสวน การสอบสวน หรือการฟ้องคดี ไม่ว่าเป็นคดีประเภทใดก็ตาม

7. เป็นการให้ซึ่งจำเป็นเพื่อการป้องกันหรือระงับอันตรายต่อชีวิตหรือสุขภาพของบุคคล

8. ต่อศาล และเจ้าหน้าที่ของรัฐหรือหน่วยงานของรัฐหรือบุคคลที่มีอำนาจตามกฎหมายที่จะขอข้อเท็จจริงดังกล่าว

9. กรณีอื่นตามที่กำหนดในพระราชกฤษฎีกา

ในด้านสิทธิของเจ้าของข้อมูลข่าวสารส่วนบุคคลภายใต้พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 กำหนดให้บุคคลมีสิทธิที่จะได้รู้ข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับตน โดยเมื่อบุคคลนั้นมีคำขอเป็นหนังสือหน่วยงานของรัฐที่ควบคุมดูแลข้อมูลข่าวสารนั้นต้องให้บุคคลนั้นหรือผู้กระทำการแทนบุคคลนั้นได้ตรวจดูหรือได้รับสำเนาข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับบุคคลนั้น หากการเปิดเผยนั้นเป็นการเปิดเผยรายงานการแพทย์ เจ้าหน้าที่ของรัฐจะเปิดเผยต่อเฉพาะแพทย์ที่บุคคลนั้นมอบหมายก็ได้ อย่างไรก็ตามการเปิดเผยข้อมูลข่าวสารส่วนบุคคลแก่เจ้าของข้อมูลข่าวสาร

ส่วนบุคคลนั้นมีข้อยกเว้นตามมาตรา 14[78] และมาตรา 15[79] ซึ่งเป็นกรณีที่อาจก่อให้เกิดความเสียหายต่อสถาบันพระมหากษัตริย์ หรือกระทบต่อความมั่นคงของรัฐ หรือกระทบต่อบุคคลอื่น

---

[78]**พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540**

มาตรา 14

ข้อมูลข่าวสารของราชการที่อาจก่อให้เกิดความเสียหายต่อสถาบันพระมหากษัตริย์จะเปิดเผยมิได้

[79]**พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540**

มาตรา 14

ข้อมูลข่าวสารของราชการที่มีลักษณะอย่างหนึ่งอย่างใดดังต่อไปนี้ หน่วยงานของรัฐหรือเจ้าหน้าที่ของรัฐอาจมีคำสั่งมิให้เปิดเผยก็ได้ โดยคำนึงถึงการปฏิบัติหน้าที่ตามกฎหมายของหน่วยงานของรัฐ ประโยชน์สาธารณะ และประโยชน์ของเอกชนที่เกี่ยวข้องประกอบกัน

(1) การเปิดเผยจะก่อให้เกิดความเสียหายต่อความมั่นคงของประเทศ ความสัมพันธ์ระหว่างประเทศ และความมั่นคงในทางเศรษฐกิจหรือการคลังของประเทศ

(2) การเปิดเผยจะทำให้การบังคับใช้กฎหมายเสื่อมประสิทธิภาพ หรือไม่อาจสำเร็จตามวัตถุประสงค์ได้ ไม่ว่าจะเกี่ยวกับการฟ้องคดี การป้องกัน การปราบปราม การทดสอบ การตรวจสอบ หรือการรู้แหล่งที่มาของข้อมูลข่าวสารหรือไม่ก็ตาม

(3) ความเห็นหรือคำแนะนำภายในหน่วยงานของรัฐในการดำเนินการเรื่องใด แต่ทั้งนี้ไม่รวมถึงรายงานทางวิชาการ รายงานข้อเท็จจริง หรือข้อมูลข่าวสารที่นำมาใช้ในการทำความเห็นหรือคำแนะนำภายในดังกล่าว

(4) การเปิดเผยจะก่อให้เกิดอันตรายต่อชีวิตหรือความปลอดภัยของบุคคลหนึ่งบุคคลใด

(5) รายงานการแพทย์หรือข้อมูลข่าวสารส่วนบุคคลซึ่งการเปิดเผยจะเป็นการรุกล้ำสิทธิส่วนบุคคลโดยไม่สมควร

(6) ข้อมูลข่าวสารของราชการที่มีกฎหมายคุ้มครองมิให้เปิดเผย หรือข้อมูลข่าวสารที่มีผู้ให้มาโดยไม่ประสงค์ให้ทางราชการนำไปเปิดเผยต่อผู้อื่น

(7) กรณีอื่นตามที่กำหนดในพระราชกฤษฎีกา

คำสั่งมิให้เปิดเผยข้อมูลข่าวสารของราชการจะกำหนดเงื่อนไขอย่างใดก็ได้ แต่ต้องระบุไว้ด้วยว่าที่เปิดเผยไม่ได้เพราะเป็นข้อมูลข่าวสารประเภทใดและเพราะเหตุใด และให้ถือว่าการมีคำสั่งเปิดเผยข้อมูลข่าวสารของราชการเป็นดุลพินิจโดยเฉพาะของเจ้าหน้าที่ของรัฐตามลำดับสายการ

เมื่อเจ้าของข้อมูลข่าวสารส่วนบุคคลเห็นว่าข้อมูลข่าวสารส่วนบุคคลของตนไม่ถูกต้องตามที่เป็นจริง เจ้าของข้อมูลข่าวสารส่วนบุคคลมีสิทธิยื่นคำขอเป็นหนังสือให้หน่วยงานของรัฐที่ควบคุมดูแลข้อมูลข่าวสารของตนแก้ไขเปลี่ยนแปลง หรือลบข้อมูลข่าวสารส่วนบุคคลนั้นได้ โดยหน่วยงานของรัฐต้องพิจารณาคำขอดังกล่าวและแจ้งให้บุคคลนั้นทราบโดยไม่ชักช้า หากหน่วยงานของรัฐไม่แก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสารส่วนบุคคลตามคำขอของเจ้าของข้อมูลข่าวสารส่วนบุคคล เจ้าของข้อมูลข่าวสารส่วนบุคคลมีสิทธิอุทธรณ์ต่อคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารภายใน 30 วันนับแต่วันที่ได้รับแจ้งคำสั่งไม่แก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสารส่วนบุคคล

เมื่อพิจารณาพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 แล้วจะเห็นได้ว่าแม้จะมีบทบัญญัติเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอยู่บ้าง แต่ยังขาดหลักเกณฑ์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลบางประการ เช่น ยังมิได้บัญญัติถึงการนำข้อมูลข่าวสารส่วนบุคคลไปประมวลผลเพื่อวัตถุประสงค์อื่นนอกจากที่ระบุไว้ในขณะทำการเก็บรวบรวมว่าจะสามารถกระทำได้หรือไม่เพียงไร หรือเจ้าของข้อมูลส่วนบุคคลสามารถเพิกถอนความยินยอมได้หรือไม่ในกรณีที่การเก็บรวบรวมข้อมูลส่วนบุคคลนั้นมิใช่กรณีที่มีกฎหมายบังคับไว้เป็นต้น นอกจากนี้พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มีผลบังคับต่อหน่วยงานของรัฐเท่านั้นมิอาจนำไปบังคับใช้แก่เอกชนได้ ดังนั้นพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 จึงยังไม่อาจคุ้มครองประชาชนจากการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของภาคเอกชนได้

4.2.2 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

การจัดทำพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กระทรวงเทคโนโลยีและการสื่อสารได้นำอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ (Convention on Cyber crime) ของคณะมนตรีแห่งยุโรป (The Council of Europe) มาเป็นแนวทางในการศึกษายกร่าง[80] โดยเหตุผลในการประกาศใช้พระราชบัญญัตินี้ เนื่องจากระบบคอมพิวเตอร์เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ หากมีผู้กระทำให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้ หรือทำงานผิดพลาดไปจากคำสั่งที่ได้

บังคับบัญชา แต่ผู้ขออาจอุทธรณ์ต่อคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารได้ตามที่กำหนดในพระราชบัญญัตินี้

[80] ปกรณ์ มงคลประสิทธิ์, “การคุ้มครองความปลอดภัยของข้อมูลส่วนบุคคลในการดำเนินธุรกรรมทางอิเล็กทรอนิกส์ : กรณีศึกษาตามร่างพระราชบัญญัติข้อมูลส่วนบุคคล” , นิติศาสตรมหาบัณฑิต, มหาวิทยาลัยรามคำแหง, 2551 หน้า 103

กำหนดไว้ หรือใช้วิธีการใดๆเพื่อล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะลามกอนาจาร ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน จึงเห็นสมควรให้ตราพระราชบัญญัตินี้ขึ้นเพื่อป้องกันและปราบปรามการกระทำดังกล่าว โดยในมาตรา 3 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2540 ได้บัญญัติไว้ ดังนี้

“**มาตรา 3** ในพระราชบัญญัตินี้

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่งหรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ขุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

“ข้อมูลจราจรทางคอมพิวเตอร์” หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแดสงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่นๆที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

“ผู้ให้บริการ” หมายความว่า

(1) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ไม่ว่าจะเป็นการให้บริการในนามของตนเองหรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

(2) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

“ผู้ใช้บริการ หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าจะต้องเสียค่าใช้บริการหรือไม่ก็ตาม”

สำหรับความคุ้มครองเกี่ยวกับข้อมูลส่วนบุคคลตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีดังต่อไปนี้

<u>1) การเข้าถึงคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์โดยมิชอบ</u>

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้กำหนดให้ผู้ที่เข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการป้องกันนั้นมิได้มีไว้สำหรับตน ผู้นั้นมีความผิดต้องระวางโทษตามที่บัญญัติไว้โดยการเข้าถึงโดยมิชอบซึ่งข้อมูลทางคอมพิวเตอร์ที่มีมาตรการป้องกันจะมีโทษหนักกว่าการ

เข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกัน กรณีดังกล่าวเป็นกรณีที่เจ้าของคอมพิวเตอร์มิได้ยินยอมให้ผู้ใดเข้าถึงคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ของตน โดยเจ้าของคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ได้สร้างมาตรการเพื่อป้องกันมิให้บุคคลอื่นเข้าถึง เช่น การเข้ารหัสป้องกันเครื่องคอมพิวเตอร์ หากมีบุคคลใดเข้าถึงโดยมิชอบซึ่งคอมพิวเตอร์ที่มีมาตรการป้องกันนั้นโดยดำเนินการด้วยวิธีใดๆเพื่อให้ได้รหัสป้องกันเครื่องหรือข้อมูลมา เช่น การเจาะระบบจนกระทั่งสามารถเข้าใช้คอมพิวเตอร์หรือเข้าถึงข้อมูลคอมพิวเตอร์นั้นได้โดยไม่คำนึงว่าบุคคลผู้เข้าถึงระบบคอมพิวเตอร์โดยมิชอบนั้นจะอยู่ใกล้หรือไกลคอมพิวเตอร์เครื่องนั้น

2) การเปิดเผยมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์

ความผิดนี้ได้บัญญัติไว้ในมาตรา 6 กำหนดให้ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านำมาตรการดังกล่าวไปเปิดเผยโดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ การกระทำความผิดตามมาตรานี้ผู้กระทำความผิดต้องล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ไม่ว่าผู้นั้นจะได้ล่วงรู้มาโดยวิธีที่ชอบหรือไม่ชอบก็ตาม และได้ทำการเปิดเผยมาตรการนั้นโดยมิชอบซึ่งการเปิดเผยดังกล่าวนี้แม้จะเปิดเผยแก่บุคคลเพียงคนเดียวหรือแม้ผู้ที่ได้รับข้อมูลการเปิดเผยนั้นจะไม่สนใจนำไปใช้เลยก็ตามก็ย่อมเป็นความผิดตามมาตรานี้ หากการกระทำนั้นน่าจะเกิดความเสียหายแก่ผู้อื่น

3) การดักรับข้อมูล

ความผิดฐานดักรับข้อมูลทางคอมพิวเตอร์ของผู้อื่นโดยมิชอบกำหนดไว้ในมาตรา 8 โดยผู้กระทำความผิดได้กระทำด้วยประการใดๆโดยมิชอบโดยอาศัยวิธีทางอิเล็กทรอนิกส์เพื่อดักรับข้อมูลทางคอมพิวเตอร์ที่อยู่ในระหว่างการส่งในระบบ อาทิ ดักฟัง ตรวจสอบ หรือติดตามและข้อมูลนั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้

มีข้อน่าสังเกตว่าความผิดตามมาตรานี้จะต้องเป็นการดักรับข้อมูลทางคอมพิวเตอร์ที่อยู่ในระหว่างการส่งในระบบ ดังนั้นข้อมูลคอมพิวเตอร์ที่ถูกจัดเก็บในคอมพิวเตอร์โดยมิได้มีการส่ง หรือข้อมูลที่อยู่ในรูปแบบอื่นเช่นแผ่นซีดี หรือ USB ย่อมไม่อยู่ในความหมายของมาตรานี้

4) ทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติมข้อมูลคอมพิวเตอร์โดยมิชอบ

ตามมาตรา 9 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กำหนดให้ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่า

ทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

วัตถุประสงค์ของมาตรา 9 นี้มีขึ้นเพื่อคุ้มครองความถูกต้อง ความแท้จริงของข้อมูล และเสถียรภาพในการใช้งาน ข้อมูลคอมพิวเตอร์ และโปรแกรมคอมพิวเตอร์เพื่อให้ใช้ได้เป็นปกติ การกระทำความผิดตามมาตรานี้ เช่น การส่ง Trojanเข้าสู่ระบบเพื่อบันทึกรหัสผ่านของผู้ใช้งานคอมพิวเตอร์ และนำรหัสนั้นมาใช้ทำการแก้ไขเปลี่ยนแปลง หรือลบข้อมูลคอมพิวเตอร์

นอกจานี้ผู้กระทำความผิดจะต้องรับโทษหนักขึ้นหากการกระทำตามมาตรา 9 เป็นกรณีซึ่ง

1. ก่อให้เกิดความเสียหายแก่ประชาชนไม่ว่าความเสียหายนั้นจะเกิดขึ้นในทันทีหรือภายหลัง และไม่ว่าจะเกิดขึ้นพร้อมกันหรือไม่ ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับเกินสองแสนบาท หรือทั้งจำทั้งปรับ หรือ

2. เป็นการกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศหรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

เมื่อพิจารณาพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แล้วจะเห็นได้ว่าเป็นกฎหมายที่มุ่งให้ความคุ้มครองแก่ระบบคอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ โดยในด้านความคุ้มครองข้อมูลคอมพิวเตอร์ พระราชบัญญัตินี้ให้ความสำคัญแก่ข้อมูลทางคอมพิวเตอร์แต่มิได้กล่าวถึงสิทธิของเจ้าของข้อมูลส่วนบุคคล กล่าวคือ นอกจากพระราชบัญญัตินี้จะมิได้มีบทบัญญัติควบคุมการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลแล้ว พระราชบัญญัตินี้มิได้มุ่งให้ความคุ้มครองแก่เจ้าของข้อมูลส่วนบุคคลโดยเห็นได้จากหากมีผู้เก็บรวบรวมข้อมูลส่วนบุคคลจากบุคคลอื่นโดยเก็บรักษาไว้ในรูปแบบข้อมูลคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์นี้ย่อมถือว่าเป็นทรัพย์สินของผู้เก็บรวบรวมข้อมูลส่วนบุคคล หากภายหลังมีบุคคลทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติมข้อมูลคอมพิวเตอร์โดยมิชอบ แม้เจ้าของข้อมูลส่วนบุคคลจะได้รับความเสียหายแต่ก็ไม่ได้รับความคุ้มครองตามพระราชบัญญัตินี้ นอกจากนี้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ยังมีลักษณะเป็นการเอาโทษต่อผู้กระทำความผิดภายหลังที่ความผิดได้เกิดขึ้นแล้ว ดังนี้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จึงมีลักษณะไม่เหมาะสมที่จะนำมาใช้แก่การคุ้มครองข้อมูลส่วนบุคคล

4.2.3 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์เป็นกฎหมายที่มีขึ้นเพื่อรองรับในเรื่องตราประทับอิเล็กทรอนิกส์ อันเป็นสิ่งซึ่งสามารถระบุตัวผู้ทำธุรกรรมทางอิเล็กทรอนิกส์ได้เช่นเดียวกันกับลายมือชื่อ โดยหากจะให้เอกสารทางอิเล็กทรอนิกส์ต้องมีการประทับตราในหนังสือย่อมก่อให้เกิดอุปสรรคอย่างมาก นอกจากนี้พระราชบัญญัติดังกล่าวยังได้กำหนดเรื่องต้นฉบับให้สามารถนำเอกสารซึ่งเป็นสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์มาใช้แทนต้นฉบับหรือเป็นพยานหลักฐานในศาลได้ โดยในเรื่องเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ได้อาศัยอำนาจตามตามมาตรา 6[81] มาตรา 7[82]และ มาตรา 8[83] แห่งพระราชกฤษฎีกา

---

[81]**พระรากฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549**

มาตรา 6

ในกรณีที่หน่วยงานของรัฐมีการรวบรวม จัดเก็บ ใช้ หรือเผยแพร่ข้อมูล หรือข้อเท็จจริงที่ทำให้สามารถระบุตัวบุคคลไม่ว่าโดยทางตรงหรือโดยอ้อม ให้หน่วยงานของรัฐจัดทำแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

[82]**พระรากฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549**

มาตรา 7

แนวนโยบายและแนวปฏิบัติตามมาตรา 5 และมาตรา 6 ให้หน่วยงานของรัฐจัดทำเป็นประกาศ และต้องได้รับความเห็นชอบจากคณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมาย จึงมีผลใช้บังคับได้

หน่วยงานของรัฐต้องปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่ได้แสดงไว้ และให้จัดให้มีการตรวจสอบแนวปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่กำหนดไว้อย่างสม่ำเสมอ

[83]**พระรากฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549**

มาตรา 8

ให้คณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมายจัดทำแนวนโยบายและแนวปฏิบัติหรือการอื่นอันเกี่ยวกับการดำเนินการตามพระราชบัญญัตินี้ ไว้เป็นตัวอย่างเบื้องต้นสำหรับการดำเนินการของหน่วยงานของรัฐในการปฏิบัติตามพระราชกฤษฎีกานี้ และหากหน่วยงานของรัฐแห่งใดมีการปฏิบัติงานตามกฎหมายที่แตกต่างเป็นการเฉพาะแล้ว หน่วยงานของรัฐแห่งนั้น

กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 ออกประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานรัฐ พ.ศ. 2553 โดยประกาศดังกล่าวสามารถแบ่งสาระสำคัญออกเป็นสองส่วนมีรายละเอียด ดังนี้

1) เพื่อให้ผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐทราบว่าหน่วยงานมีนโยบายในการจัดการข้อมูลส่วนบุคคลอย่างไร และเพื่อให้ผู้ใช้บริการสามารถตัดสินใจเกี่ยวกับข้อมูลส่วนบุคคลของตนเองได้ ประกาศดังกล่าวจึงกำหนดให้หน่วยงานของรัฐซึ่งรวบรวม จัดเก็บ ใช้ เผยแพร่ หรือดำเนินการอื่นใดเกี่ยวกับข้อมูลของผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ ต้องจัดทำนโยบายในการคุ้มครองข้อมูลส่วนบุคคลไว้เป็นลายลักษณ์อักษร และต้องมีสาระสำคัญที่จะกล่าวดังต่อไปนี้

1.1 การจัดเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด โดยหน่วยงานของรัฐต้องใช้ใช้วิธีที่ชอบด้วยกฎหมายและเป็นธรรม และได้รับความยินยอมหรือได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบแล้วแต่กรณี

1.2 การจัดเก็บข้อมูลส่วนบุคคลต้องเป็นไปตามวัตถุประสงค์ในการดำเนินงานและตามอำนาจหน้าที่ของหน่วยงานรัฐนั้น

1.3 หน่วยงานของรัฐต้องบันทึกวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลในเวลาที่มีการจัดเก็บและรวบรวม รวมถึงการนำข้อมูลไปใช้ภายหลัง ในกรณีที่หน่วยงานของรัฐเปลี่ยนแปลงวัตถุประสงค์ให้หน่วยงานของรัฐต้องทำบันทึกแก้ไขเพิ่มเติมไว้เป็นหลักฐาน

1.4 ห้ามหน่วยงานของรัฐเปิดเผย แสดง หรือทำให้ปรากฏโดยประการอื่นซึ่งข้อมูลส่วนบุคคลที่ไม่สอดคล้องกับวัตถุประสงค์ในการเก็บรวบรวมและจัดเก็บข้อมูลส่วนบุคคล เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือเป็นกรณีที่มีกฎหมายกำหนดไว้

1.5 หน่วยงานของรัฐต้องมีมาตรการในการรักษาความปลอดภัยของข้อมูลส่วนบุคคลเพื่อป้องกันมิให้ข้อมูลนั้นสูญหาย ถูกการเข้าถึง ถูกทำลาย ใช้ แปลง หรือแก้ไข หรือถูกเปิดเผยโดยมิชอบ

1.6 หน่วยงานของรัฐต้องดำเนินการให้มีการเปิดเผยการดำเนินการ แนวปฏิบัติ และนโยบายเกี่ยวกับข้อมูลส่วนบุคคล รวมถึงวิธีการที่สามารถตรวจดูความมีอยู่ ลักษณะของ

อาจเพิ่มเติมรายละเอียดการปฏิบัติงานตามกฎหมายที่แตกต่างนั้นได้โดยออกเป็นระเบียบ ทั้งนี้ โดยให้คำนึงถึงความถูกต้อง ครบถ้วน ความน่าเชื่อถือ สภาพความพร้อมใช้งาน และความมั่นคงปลอดภัยของระบบและข้อมูลคอมพิวเตอร์

ข้อมูลส่วนบุคคล วัตถุประสงค์ของการนำข้อมูลไปใช้ ผู้ควบคุมและสถานที่ทำการของผู้ควบคุมข้อมูลส่วนบุคคล

1.7 เมื่อเจ้าของข้อมูลส่วนบุคคลมีคำขอหน่วยงานของรัฐต้องแจ้งถึงผู้ควบคุมข้อมูลส่วนบุคคลความมีอยู่ หรือรายละเอียดของข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลเมื่อได้รับคำร้องขอจากเจ้าของข้อมูลส่วนบุคคลภายในเวลาอันสมควร

1.8 ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามมาตรการที่ได้กล่าวมาแล้วเพื่อให้การดำเนินตามนโยบายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเป็นไปตามมาตรฐานของประกาศฉบับนี้

2) หน่วยงานของรัฐต้องจัดให้มีแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล โดยมีวัตถุประสงค์เพื่อให้บุคคลากรของหน่วยงานนั้นปฏิบัติตาม โดยแนวปฏิบัตินี้ต้องมีสาระสำคัญดังต่อไปนี้ด้วย

2.1 ข้อมูลเบื้องต้นประกอบด้วย ชื่อนโยบายการคุ้มครองข้อมูลส่วนบุคคล รายละเอียดการบังคับใช้นโยบายการคุ้มรองข้อมูลส่วนบุคคลนั้น และหากมีการเปลี่ยนแปลงวัตถุประสงค์หรือนโยบายการคุ้มครองข้อมูลส่วนบุคคลให้หน่วยงานของรัฐแจ้งการเปลี่ยนแปลงให้เจ้าของข้อมูลทราบ และขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนทุกครั้ง

2.2 การเก็บรวบรวม จัดประเภท และการใช้ข้อมูลส่วนบุคคล

2.3 การแสดงระบุความเชื่อมโยงข้อมูลส่วนบุคคลกับหน่วยงานอื่น

2.4หากหน่วยงานของรัฐได้รวบรวมรวมข้อมูลส่วนบุคคลมาจากหลายแหล่ง หน่วยงานของรัฐต้องระบุในนโยบายคุ้มครองข้อมูลส่วนบุคคลถึงเจตนารมณ์การรวมข้อมูล

2.5 หากมีบุคคลอื่นใช้หรือเปิดเผยข้อมูลแก่บุคคลอื่น หน่วยงานของรัฐต้องระบุว่ามีบุคคลอื่นที่จะเข้าถึงหรือใช้ข้อมูลนั้นได้ และต้องระบุว่าการเข้าถึง ใช้ หรือเปิดเผยนั้นสอดคล้องกับข้อกำหนดตามกฎหมายของหน่วยงานรัฐที่ดำเนินการดังกล่าวอีกด้วย

2.6 ระบุถึงสิทธิของผู้ใช้บริการที่จะสามารถเลือกว่าจะให้หน่วยงานของรัฐรวบรวม จัดเก็บหรือไม่จัดเก็บ ใช้หรือไม่ให้ใช้ และเปิดเผยหรือไม่ให้เปิดเผยข้อมูลของตนในกรณีที่มีการนำข้อมูลไปใช้เพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ของการเก็บรวบรวม

2.7 หน่วยงานของรัฐต้องกำหนดวิธีการให้ผู้ใช้สามารถเข้าถึงและแก้ไขหรือปรับปรุงข้อมูลเกี่ยวกับตนเองที่หน่วยงานรวบรวม และจัดเก็บในเว็บไซต์ให้ถูกต้อง

2.8 หน่วยงานของรัฐต้องจัดให้มีมาตรรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

2.9 หน่วยงานของรัฐต้องระบุข้อมูลติดต่อที่ผู้ใช้บริการสามารถติดต่อกับหน่วยงานของรัฐได้ ซึ่งอย่างน้อยต้องประกอบด้วยข้อมูลดังต่อไปนี้

- ชื่อและที่อยู่
- หมายเลขโทรศัพท์
- หมายเลขโทรสาร
- ที่อยู่จดหมายอิเล็กทรอนิกส์

เมื่อพิจารณาถึงประกาศของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์แล้วจะเห็นได้ว่ามีหลักการที่สามารถคุ้มครองเจ้าของข้อมูลส่วนบุคคลได้ แต่ประกาศฉบับดังกล่าวมีผลบังคับใช้ต่อเพียงหน่วยงานของรัฐโดยมิอาจนำมาบังคับใช้แก่ภาคเอกชนได้ ดังนั้นประชาชนย่อมไม่อาจได้รับความคุ้มครองความเป็นส่วนตัวของตนจากภาคเอกชนโดยอาศัยประกาศฉบับดังกล่าว

4.2.4 พระราชบัญญัติว่าด้วยการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545

พระราชบัญญัตินี้มีวัตถุประสงค์เพื่อให้ผู้บริโภคได้รับบริการสินเชื่อสอดคล้องกับศักยภาพในการชำระหนี้คืน ซึ่งส่งผลต่อความมั่นคงของระบบเศรษฐกิจและสภาบันการเงิน พระราชบัญญัติจึงเปิดโอกาสให้บริษัทข้อมูลเครดิตสามารถคำนวณคะแนนเครดิต และจัดทำรายงานเชิงสถิติได้ โดยข้อมูลเครดิต หมายถึงสิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงของข้อมูลเครดิต หรือคะแนนเครดิต ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใดๆ คะแนนเครดิต หมายถึง ตัวชี้วัดความน่าจะเป็นในการชำระคืนหนี้โดยใช้วิธีการทางสถิติในการประมวลผลข้อมูลโดยบริษัทข้อมูลเครดิต โดยข้อมูลเครดิต หมายถึงข้อเท็จจริงเกี่ยวกับลูกค้าที่ข้อสินเชื่อ ดังต่อไปนี้

1. ข้อเท็จจริงที่บ่งชี้ถึงตัวลูกค้า และคุณสมบัติของลูกค้าที่ของสินเชื่อ

1.1 กรณีบุคคลธรรมดา หมายถึง ชื่อ ที่อยู่ วันเดือนปีเกิด สถานภาพ การสมรส อาชีพ เลขที่บัตรประจำตัวประชาชน หรือบัตรประตัวเจ้าหน้าที่ของรัฐ หรือหนังสือเดินทาง และเลขประจำตัวผู้เสียภาษีอากร (ถ้ามี)

1.2 กรณีนิติบุคคล หมายถึง ชื่อ สถานที่ตั้ง เลขที่ทะเบียนการจัดตั้งนิติบุคคล หรือเลขประจำตัวผู้เสียภาษีอากร

2. ประวัติการขอและการได้รับอนุมัติสินเชื่อ และการชำระสินเชื่อของลูกค้าที่ขอสินเชื่อรวมทั้งประวัติการชำระราคาสินค้าหรือบริการโดยบัตรเครดิต

โดยตามพระราชบัญญัตินี้มีสาระสำคัญเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล คือ ภายใต้พระราชบัญญัตินี้บริษัทข้อมูลเครดิตมีหน้าที่ต้องทำการประมวลผลข้อมูลจากสมาชิกหรือจากแหล่งข้อมูลที่เชื่อถือได้ โดยต้องกำหนดให้มีระบบและข้อกำหนดคือ

1. ระบบจำแนกข้อมูลทีเก็บรักษาไว้

2. ระบบการแก้ไขข้อมูลให้มีความถูกต้องสมบูรณ์และทันสมัยอยู่เสมอ

3. ระบบรักษาความลับและความปลอดภัยของข้อมูล

4. ระบบการขอใช้ข้อมูลและระบบการรายงานข้อมูลตามปกติ

5. ระบบการตรวจสอบและแก้ไขข้อมูลของเจ้าของข้อมูล

6. ระบบบันทึกและรายงานผลเมื่อมีผู้เข้าถึงข้อมูล

7. ระบบการทำลายข้อมูลที่มีอายุเกินกว่าที่คณะกรรมการกำหนด

8. ระบบหรือข้อกำหนดอื่นใดตามที่คณะกรรมการประกาศกำหนด

นอกจากนี้เมื่อสมาชิกส่งข้อมูลของลูกค้าแก่บริษัทข้อมูลเครดิตที่ตนเป็นสมาชิกแล้ว บริษัทนั้นต้องแจ้งให้ลูกค้าของตนทราบเกี่ยวกับข้อมูลที่ส่งไปเป็นหนังสือ หรือโดยวิธีอื่นตามที่ตกลงกันภายในสามสิบวัน นอกจากนี้บริษัทข้อมูลเครดิตสามารถเปิดเผยหรือให้ข้อมูลแก่สมาชิกหรือผู้ใช้บริการที่ประสงค์ใช้ข้อมูลเพื่อประโยชน์ในการวิคเราะห์สินเชื่อ และการออกบัตรเครดิตโดยต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนทุกครั้ง เว้นแต่เจ้าของข้อมูลได้ให้ความยินยอมไว้เป็นอย่างอื่น

ในด้านของสิทธิของเจ้าของข้อมูลส่วนบุคคล พระราชบัญญัตินี้กำหนดสิทธิแก่เจ้าของข้อมูลส่วนบุคคลไว้ในมาตรา 25 จำนวน 7 ประการ กล่าวคือ

1. สิทธิในการรับรู้ว่าบริษัทข้อมูลเครดิตเก็บรักษาข้อมูลใดของตน

2. สิทธิที่จะตรวจสอบข้อมูลของตน

3. สิทธิที่จะขอแก้ไขข้อมูลที่ไม่ถูกต้อง

4. สิทธิที่จะโต้แย้งเมื่อทราบว่าข้อมูลของตนไม่ถูกต้อง

5. สิทธิที่จะได้รับแจ้งผลการตรวจสอบข้อมูลของตนภายในระยะเวลาที่กำหนด

6. สิทธิที่จะได้รับทราบเหตุแห่งการปฏิเสธคำขอสินเชื่อหรือบริการจากสถาบันการเงิน ในกรณีที่สถาบันการเงินใช้ข้อมูลของบริษัทข้อมูลเครดิตมาเป็นเหตุแห่งการปฏิเสธคำขอสินเชื่อหรือบริการ

7. สิทธิที่จะอุทธรณ์ต่อคณะกรรมการตามมาตรา 27[84]

---

[84]**พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545**

มาตรา 27

ในกรณีที่มีข้อโต้แย้งระหว่างเจ้าของข้อมูลกับบริษัทข้อมูลเครดิตเกี่ยวกับความถูกต้องของข้อมูลและไม่อาจหาข้อยุติได้ ให้บริษัทข้อมูลเครดิตบันทึกข้อโต้แย้งพร้อมหลักฐาน

โดยเมื่อเจ้าของข้อมูลขอใช้สิทธิในการตรวจสอบหรือแก้ไขข้อมูลที่มีอยู่กับบริษัทข้อมูลเครดิตหรือสมาชิก ให้บริษัทข้อมูลเครดิตหรือสมาชิกนั้นพิจารณาคำขอและตรวจสอบข้อมูลโดยเร็ว และให้แจ้งผลการตรวจสอบหรือแก้ไขข้อมูลของตนพร้อมเหตุผลให้เจ้าองข้อมูลทราบภายในสามสิบวันนับแต่วันที่ได้รับคำขอ จากที่กล่าวมาจะเห็นได้ว่าแม้พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 มีบทบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล แต่ก็จำกัดอยู่เพียงการให้ความคุ้มครองแก่ข้อมูลเครดิตเท่านั้น มิได้ครอบคลุมถึงข้อมูลส่วนบุคคลประเภทอื่นๆ

4.2.5 ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .....

ประเทศไทยได้ปรากฏร่างพระราชบัญญัติหลายฉบับ เช่น ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... คณะรัฐมนตรีและสมาชิกสภาผู้แทนราษฎรเป็นผู้เสนอหรือร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... เสนอโดยสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ (สขร.) เป็นต้นโดยร่างพระราชบัญญัติฉบับล่าสุดเป็นร่างพระราชบัญญัติที่เสนอโดยกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารและส่งให้สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณา โดยร่างพระราชบัญญัติดังกล่าวได้ให้เหตุผลในบันทึกหลักการและเหตุผลประกอบร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ไว้ ความว่า

ประกอบของเจ้าของข้อมูลไว้ในระบบข้อมูลของเจ้าของข้อมูล ในการจัดทำรายงานข้อมูลเพื่อให้บริการแก่สมาชิกหรือผู้ใช้บริการ บริษัทข้อมูลเครดิตต้องระบุในรายงานดังกล่าวด้วยว่ามีข้อโต้แย้งของเจ้าของข้อมูลในเรื่องใดบ้าง ในการนี้ เจ้าของข้อมูลอาจอุทธรณ์ข้อโต้แย้งนั้นต่อคณะกรรมการเพื่อวินิจฉัยชี้ขาด

หากมีข้อโต้แย้งเกิดขึ้นระหว่างสถาบันการเงิน สมาชิก หรือผู้ใช้บริการกับบริษัทข้อมูลเครดิตหรือกับเจ้าของข้อมูลและไม่อาจหาข้อยุติได้ ให้บริษัทข้อมูลเครดิต สถาบันการเงิน สมาชิก หรือผู้ใช้บริการบันทึกข้อโต้แย้งนั้นในระบบข้อมูลของเจ้าของข้อมูลนั้น พร้อมกับแจ้งให้บุคคลที่เกี่ยวข้องทราบด้วย ในการนี้ เจ้าของข้อมูลอาจอุทธรณ์ข้อโต้แย้งนั้นต่อคณะกรรมการเพื่อวินิจฉัยชี้ขาดก็ได้

การอุทธรณ์ข้อโต้แย้งต่อคณะกรรมการตามวรรคหนึ่งและวรรคสอง ให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

เมื่อมีคำวินิจฉัยชี้ขาดของคณะกรรมการตามวรรคหนึ่งและวรรคสอง ให้บริษัทข้อมูลเครดิต สถาบันจการเงิน สมาชิก และผู้ใช้บริการ ปฏิบัติตามคำวินิจฉัยชี้ขาดนั้น

> “เนื่องจากในปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคลประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าวสามารถทำได้โดยง่าย สะดวก และรวดเร็ว รวมทั้งก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวมที่ใช้เทคโนโลยีดิจิทัลอย่างแพร่หลาย แม้ว่าจะได้มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลในบางเรื่อง แต่ก็ยังไม่มีหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป สมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้น”

บันทึกหลักการและเหตุผลของร่างพระราชบัญญัติดังกล่าวแสดงให้เห็นว่าประเทศไทยตระหนักถึงปัญหาในการละเมิดข้อมูลส่วนบุคคลและให้ความสำคัญต่อการคุ้มครองข้อมูลส่วนบุคคล และตามร่างพระราชบัญญัติฉบับนี้ได้มีการตั้งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลขึ้นมีอำนาจหน้าที่หลายประการ เช่น จัดทำแผนยุทธศาสตร์การดำเนินงานด้านการส่งเสริมและการคุ้มครองข้อมูลส่วนบุคคล หรือกำหนดมาตรการหรือแนวทางการดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามร่างพระราชบัญญัตินี้ หรือออกประกาศหรือระเบียบเพื่อให้การดำเนินการเป็นไปตามร่างพระราชบัญญัตินี้ เป็นต้น โดยร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... มีสาระสำคัญ ดังนี้

(1) ผลบังคับใช้

ในกรณีที่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลบัญญัติไว้เป็นการเฉพาะในเรื่องใดให้ปฏิบัติตามกฎหมายนั้น เว้นแต่การเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลและบทกำหนดโทษให้บังคับใช้ตามร่างพระราชบัญญัตินี้เป็นการเพิ่มเติมแม้ว่าจะเป็นการซ้ำกับกฎหมายเฉพาะนั้นก็ตาม และในกรณีที่กฎหมายนั้นไม่มีบทบัญญัติเรื่องการร้องเรียนหรือไม่มีบทบัญญัติให้อำนาจเจ้าหน้าที่ออกคำสั่งเพื่อให้ความคุ้มครองแก่เจ้าของข้อมูลได้ทัดเทียมกับความคุ้มครองตามร่างพระราชบัญญัตินี้และเจ้าหน้าที่หรือเจ้าของข้อมูลส่วนบุคคลนั้นยื่นคำร้องต่อคณะกรรมการให้นำร่างพระราชบัญญัตินี้มาใช้บังคับนอกจากนี้มาตรา 4 แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... กำหนดกิจกรรมบางประเภทที่ไม่นำร่างพระราชบัญญัตินี้มาใช้บังคับ ได้แก่

1. บุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตนของบุคคลนั้นเท่านั้น โดยมิให้ผู้อื่นใช้ข้อมูลส่วนบุคคลนั้น หรือเปิดเผยข้อมูลส่วนบุคคลนั้นต่อผู้อื่น

2. บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมไว้เฉพาะเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น

3. สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมไปถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าว ซึ่งเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามอำนาจหน้าที่ของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมาธิการ แล้วแต่กรณี

4. การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดีและการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

5. การดำเนินกิจการทางศาสนาขององค์การทางศาสนา

6. การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

(2)การเก็บรวบรวม ใช้ หรือการเปิดเผยข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงการระบุเฉพาะชื่อ ตำแหน่ง สถานที่ทำงาน หรือที่อยู่ทางธุรกิจและข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ และผู้ควบคุมข้อมูลส่วนบุคคลหมายถึงบุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยในการเก็บรวบรวมข้อมูลส่วนบุคคลผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวมได้เท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมาย และภายใต้ข้อยกเว้นตามมาตรา 22[85] ข้อมูลนั้นต้องเป็นการเก็บรวบรวมจากเจ้าของข้อมูลส่วนบุคคลโดยตรง ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้

---

[85]**ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....**

มาตรา 22

ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่

(1) ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ชักช้า

(2) เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลจากการใช้และการเปิดเผยที่ได้รับยกเว้นตามมาตรา 24

(3) เป็นข้อมูลที่เปิดเผยต่อสาธารณะ

เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลถึงรายละเอียดต่างๆตามมาตรา 20[86] เช่น วัตถุประสงค์ของการเก็บรวบรวม ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวม หรือประเภทของบุคคลหรือหน่วยงานที่ซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย เป็นต้น

สำหรับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นผู้ควบคุมข้อมูลส่วนบุคคลต้องได้รับความยินยอมเป็นหนังสือหรือโดยผ่านระบบอิเล็กทรอนิกส์จากเจ้าของข้อมูลก่อนหรือในขณะนั้นเว้นแต่มีกฎหมายอื่นบัญญัติให้กระทำได้ ในการขอความยินยอมผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบ และการขอความยินยอมนั้นต้องไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ โดยในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องกระทำตามวัตถุประสงค์ที่ได้แจ้งไว้ก่อนหรือในขณะเก็บรวบรวม การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลแตกต่างไปจากวัตถุประสงค์ที่ได้แจ้งไว้นั้นกระทำมิได้ เว้นแต่ ได้แจ้งวัตถุประสงค์ใหม่แก่เจ้าของข้อมูลส่วนบุคคลและได้รับความยินยอมก่อนเก็บรวบรวม ใช้ หรือเปิดเผยแล้ว หรือบทบัญญัติตามร่างพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้

อย่างไรก็ตามผู้ควบคุมข้อมูลส่วนบุคคลอาจเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลได้ใน 5 กรณีคือ เพื่อประโยชน์ที่เกี่ยวการศึกษาวิจัยหรือสถิติและได้เก็บข้อมูลส่วนบุคคลเพื่อการนั้นไว้เป็นความลับ หรือเพื่อป้องกันหรือระงับอันตรายต่อชีวิต

---

[86]**ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....**

มาตรา 20

ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียด ดังต่อไปนี้

(1) วัตถุประสงค์ของการเก็บรวบรวม

(2) ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวม

(3) ประเภทของบุคคลหรือหน่วยงานที่ซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย

(4) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อและวิธีการติดต่อ

(5) สิทธิของเจ้าของข้อมูลตามมาตรา 26 มาตรา 27 และมาตรา 28

กรณีมีเหตุที่ไม่อาจแจ้งรายละเอียดตามวรรคหนึ่งให้แก่เจ้าของข้อมูลส่วนบุคคลตามกำหนดเวลาในวรรคหนึ่ง ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งรายละเอียดตามวรรคหนึ่งแก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า

ร่างกายหรือสุขภาพของบุคคล หรือเป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยตรงหรือโดยปริยายของเจ้าของข้อมูลส่วนบุคคล หรือเป็นการปฏิบัติตามกฎหมาย หรือกรณีอื่นตามกฎกระทรวง

การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเว้นแต่เป็นการเปิดเผยตามมาตรา 21[87] หรือ 23[88] หรือเป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้ตามมาตรา 22(3)[89] และบุคคลซึ่งได้รับข้อมูลจากการเปิดเผยนั้นต้องไม่ใช้หรือเปิดเผย

---

[87]**ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....**

มาตรา 21

ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(1) เพื่อประโยชน์ที่เกี่ยวกับการศึกษาวิจัยหรือสถิติและได้เก็บข้อมูลส่วนบุคคลเพื่อการนั้นไว้เป็นความลับ

(2) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุภาพของบุคคล

(3) เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยตรงหรือโดยปริยายของเจ้าของข้อมูลส่วนบุคคล

(4) เป็นการปฏิบัติตามกฎหมาย

(5) กรณีอื่นตามที่กำหนดในกฎกระทรวง

[88]**ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....**

มาตรา23

ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อความรู้สึกของประชาชนตามที่คณะกรรมการประกาศกำหนดโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(1) ได้รับยกเว้นตามมาตรา 21(2) หรือ (4)

(2) กรณีอื่นตามที่กำหนดในกฎกระทรวง

[89]**ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....**

มาตรา 22

ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่

ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกจากวัตถุประสงค์ที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลส่วนบุคคลในการขอรับข้อมูลส่วนบุคคลนั้น

(3) ข้อมูลซึ่งห้ามมิให้ทำการเก็บรวบรวม ใช้หรือเปิดเผย

ข้อมูลบางประเภทเป็นข้อมูลที่มีความอ่อนไหว ร่างพระราชบัญญัตินี้จึงกำหนดให้เป็นข้อมูลที่ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมโดยมิได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ได้แก่ ข้อมูลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ หรือข้อมูลอื่นซึ่งกระทบต่อความรู้สึกของประชาชนตามที่คณะกรรมการประกาศกำหนด เว้นแต่เป็นการเก็บรวบรวมเพื่อการศึกษาวิจัยหรือสถิติและได้เก็บข้อมูลส่วนบุคคลนั้นไว้เป็นความลับ หรือเป็นการปฏิบัติตามกฎหมาย หรือเป็นกรณีอื่นตามที่กำหนดในกฎกระทรวง

(4) สิทธิของเจ้าของข้อมูลส่วนบุคคล

เจ้าของข้อมูลมีสิทธิถอนความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของตน เว้นแต่ถูกจำกัดสิทธิโดยกฎหมายหรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคลและหากการถอนความยินยอมส่งผลกระทบต่อเจ้าของข้อมูลผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงผลกระทบจากการถอนความยินยอมนั้น นอกจากสิทธิในการเพิกถอนความยินยอมแล้วภายใต้ร่างพระราชบัญญัติฉบับดังกล่าวเจ้าของข้อมูลส่วนบุคคลยังมีสิทธิขอเข้าถึงข้อมูลส่วนบุคคลเกี่ยวกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอมทั้งยังมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลทำให้ข้อมูลของตนถูกต้อง เป็นปัจจุบัน สมบูรณ์และไม่ก่อให้เกิดความเข้าใจผิด

และหากผู้ควบคุมข้อมูลส่วนบุคคลไม่ปฏิบัติตามหลักเกณฑ์แห่งร่างพระราชบัญญัตินี้ เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบ หรือทำลายหรือระงับการใช้ชั่วคราว หรือแปลงข้อมูลส่วนบุคคลให้อยู่ในรูปแบบข้อมูลที่ไม่สามารถรู้ตัวผู้เป็นเจ้าของข้อมูลได้

(5) หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้องเป็นปัจจุบัน สมบูรณ์และไม่ก่อให้เกิดความเข้าใจผิด หากเจ้าของข้อมูลส่วนบุคคลขอให้ผู้ควบคุมข้อมูลส่วนบุคคลแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง เป็นปัจจุบัน สมบูรณ์และไม่ก่อให้เกิดความเข้าใจผิด ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการตามคำร้องขอนั้น หากเจ้าของข้อมูลส่วนบุคคลขอเข้าถึง

---

(3) เป็นข้อมูลที่เปิดเผยต่อสาธารณะ

ข้อมูลส่วนบุคคลของตนผู้ควบคุมข้อมูลส่วนบุคคลต้องยินยอมให้เจ้าของข้อมูลส่วนบุคคลใช้สิทธิดังกล่าว อย่างไรก็ตามผู้ควบคุมข้อมูลส่วนบุคคลมีสิทธิปฏิเสธการเข้าถึงได้ในกรณีที่เป็นการขัดหรือแย้งกับบทบัญญัติแห่งกฎหมายหรือปฏิบัติตามคำสั่งศาล หรือมีผลต่อการสืบสวนสอบสวนของพนักงานเจ้าหน้าที่ตามกฎหมาย หรือการเปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลนั้นอาจเป็นอันตรายต่อสิทธิและเสรีภาพของบุคคลอื่น หรือกรณีอื่นตามที่กำหนดในกฎกระทรวงและผู้ควบคุมข้อมูลต้องทำบันทึกรายการตามมาตรา 30 เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถตรวจสอบได้

นอกจากหน้าที่ที่ได้กล่าวไปข้างต้นแล้วผู้ควบคุมข้อมูลส่วนบุคคลยังมีหน้าที่อีก 4 ประการตามมาตรา 29 คือ 1. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมเพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

2. ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่น ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

3. ทำลายข้อมูลส่วนบุคคลเมื่อพ้นระยะเวลาในการเก็บรักษา หรือเมื่อข้อมูลส่วนบุคคลนั้นไม่เกี่ยวข้อง หรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือเมื่อเจ้าของข้อมูลส่วนบุคคลเพิกถอนความยินยอม เว้นแต่เป็นการเก็บรักษาเพื่อวัตถุประสงค์ในการพิสูจน์ หรือการตรวจสอบ

4. แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้า หากการละเมิดข้อมูลส่วนบุคคลนั้นเกินจำนวนตามที่คณะกรรมการประกาศกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งการละเมิดและแนวทางการเยียวยาแก่คณะกรรมการโดยไม่ชักช้า

4.3 วิเคราะห์ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... และปัญหาที่อาจเกิดขึ้นจากการคุ้มครองข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์

จากที่กล่าวมาจะเห็นได้ว่าประเทศไทยมีความจำเป็นอย่างยิ่งที่จะต้องออกพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลมาใช้บังคับเพื่อให้ความคุ้มครองแก่ความเป็นส่วนตัวของประชาชนได้อย่างจริงจัง เนื่องจากพระราชบัญญัติอื่น อาทิ ประมวลกฎหมายแพ่งและพาณิชย์ และประมวลกฎหมายอาญา ซึ่งมิได้บัญญัติขึ้นเพื่อให้มีวัตถุประสงค์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ซึ่งใช้บังคับแก่หน่วยงานราชการเท่านั้น หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งก็มิได้ครอบคลุมถึงการ

เก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลทั้งมิใช่บทบัญญัติที่ร่างขึ้นเพื่อให้เป็นกฎหมายซึ่งบังคับใช้เกี่ยวกับข้อมูลส่วนบุคคลเป็นการทั่วไป ดังนั้นกฎหมายดังกล่าวจึงไม่อาจให้ความคุ้มครองแก่เจ้าของข้อมูลส่วนบุคคลได้อย่างครอบคลุมครบถ้วน

ความสำคัญของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลนอกจากจะเป็นกฎหมายที่ให้ความคุ้มครองแก่ความเป็นส่วนตัวของประชาชนชาวไทยแล้วพระราชบัญญัติดังกล่าวสามารถส่งเสริมในด้านการค้าทั้งในและระหว่างประเทศ กล่าวคือ การที่มีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลมีหลักเกณฑ์ครบถ้วนสามารถให้ความคุ้มครองแก่เจ้าของข้อมูลส่วนบุคคลได้อย่างแท้จริงทัดเทียมกับสากล โดยเฉพาะอย่างยิ่งในยุคที่เทคโนโลยีสามารถเก็บรวบรวมและติดตามเจ้าของข้อมูลส่วนบุคคลได้สะดวกรวดเร็วซึ่งส่งผลให้เกิดการละเมิดความเป็นส่วนตัวได้ง่ายย่อมช่วยให้บุคคลหรือหน่วยงานที่อยู่ในต่างประเทศเชื่อมั่นในความคุ้มครองของประเทศไทยและทำธุรกรรมหรือโอนข้อมูลกับประเทศไทย ทั้งนี้สิ่งหนึ่งที่แสดงให้เห็นชัดเจนว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลที่มีหลักเกณฑ์ความคุ้มครองทัดเทียมกับสากลย่อมส่งผลต่อการค้าหรือการโอนข้อมูลระหว่างประเทศ คือ หลักเกณฑ์ของประเทศต่างๆเกี่ยวกับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศมักกำหนดให้มีการโอนข้อมูลได้เมื่อประเทศผู้รับข้อมูลมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ทัดเทียมกับประเทศผู้ส่ง สำหรับร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ของประเทศไทยนั้นเมื่อนำมาวิเคราะห์ประกอบกับทำการเปรียบเทียบกับกฎหมายต่างประเทศแล้วมีข้อน่าพิจารณาดังนี้

4.3.1 หลักการคุ้มครองข้อมูลส่วนบุคคล

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลมีหลักการในการคุ้มครองข้อมูลส่วนบุคคลทั้งสิ้น 9 ประการ กล่าวคือ

หลักการแรก หลักการจัดเก็บข้อมูลส่วนบุคคลอย่างจำกัด (Collection Limitation Principle) กำหนดไว้ในมาตรา 17 โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลซึ่งต้องไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ดังกล่าว มาตรา 19 กำหนดให้การเก็บรวบรวมข้อมูลส่วนบุคคลให้เก็บรวบรวมได้เท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมาย และมาตรา 22 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นนอกจากเจ้าของข้อมูลส่วนบุคคลโดยตรง

หลักการที่สอง หลักการประมวลผลข้อมูลส่วนบุคคลอย่างมีคุณภาพและได้สัดส่วน (Data Quality and Proportional Principle) กำหนดไว้ในมาตรา 18 ให้ผู้ควบคุมข้อมูล

ส่วนบุคคลต้องทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งไว้ก่อนหรือขณะเก็บรวบรวม และผู้ควบคุมข้อมูลส่วนบุคคลจะนำข้อมูลส่วนบุคคลไปใช้ หรือเปิดเผยโดยแตกต่างจากวัตถุประสงค์ที่ได้แจ้งไว้มิได้ เว้นแต่มีทบบัญญัติแห่งกฎหมายให้สิทธิแก่ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ควบคุมข้อมูลส่วนบุคคลได้แจ้งวัตถุประสงค์ใหม่แก่เจ้าของข้อมูลส่วนบุคคลและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

หลักการที่สาม หลักการระบุวัตถุประสงค์และระยะเวลาในการใช้ข้อมูลส่วนบุคคล (Purpose Specification Principle)หลักการดังกล่าวกำหนดไว้ในมาตรา 17 โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ในการขอเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลซึ่งต้องไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ดังกล่าว อย่างไรก็ตามร่างพระราชบัญญัติฉบับนี้มิได้พูดถึงระยะเวลาในการเก็บรักษาและใช้ข้อมูลส่วนบุคคลซึ่งควรกำหนดไว้มิให้เกินกว่าระยะเวลาที่จำเป็นเพื่อให้วัตถุประสงค์ที่ได้แจ้งไว้สำเร็จลุล่วง

หลักการที่สี่ หลักการใช้ข้อมูลส่วนบุคคลอย่างจำกัด (Use Limitation Principle) ระบุไว้ในมาตรา 24 ซึ่งกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลจะทำการเปิดเผย หรือใช้ข้อมูลส่วนบุคคลได้ต่อเมื่อได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

หลักการที่ห้า หลักการป้องกันรักษาความปลอดภัยของข้อมูลส่วนบุคคล (Security Safeguard Principle)กำหนดไว้ในมาตรา 24 ให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องมีมาตรการรักษาความปลอดภัยข้อมูลส่วนบุคคลที่เหมาะสม เพื่อป้องกันมิให้ข้อมูลส่วนบุคคลนั้นสูญหาย ถูกเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

หลักการที่หก หลักเปิดเผยโปร่งใส (Openness Principle) กำหนดไว้ในมาตรา 20 โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องระบุรายละเอียดดังต่อไปนี้ในเวลาแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงการเก็บรวบรวมข้อมูลส่วนบุคคล

1. วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคล
2. ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวม
3. ประเภทของบุคคลหรือหน่วยงานที่ซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย
4. ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการในการติดต่อ
5. สิทธิของเจ้าของข้อมูลส่วนบุคคลในการขอเข้าถึงข้อมูลส่วนบุคคล หรือสิทธิในการขอให้ผู้ควบคุมข้อมูลส่วนบุคคล ลบ หรือทำลาย ระงับการใช้ชั่วคราว หรือแปลงข้อมูลส่วนบุคคลให้อยู่ในรูปแบบข้อมูลที่ไม่สามารถรู้ตัวบุคคลที่เป็น

เจ้าของข้อมูลส่วนบุคคลได้เมื่อผู้ควบคุมข้อมูลส่วนบุคคลไม่ปฏิบัติตามร่างพระราชบัญญัตินี้ หรือ สิทธิในการขอให้ผู้ควบคุมข้อมูลส่วนบุคคลทำให้ข้อมูลของตนเป็นปัจจุบัน สมบูรณ์และไม่ก่อให้เกิดความเข้าใจผิด

หลักการที่เจ็ด หลักการมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation Principle) กำหนดไว้ในมาตรา 26 โดยเจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงข้อมูลของตนซึ่งอยู่ในความครอบครองของผู้ควบคุมข้อมูลส่วนบุคคล และมาตรา 27 กำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคล ลบ หรือทำลาย ระงับการใช้ชั่วคราว หรือแปลงข้อมูลส่วนบุคคลให้อยู่ในรูปแบบข้อมูลที่ไม่สามารถรู้ตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้เมื่อผู้ควบคุมข้อมูลส่วนบุคคลไม่ปฏิบัติตามร่างพระราชบัญญัตินี้

หลักการที่แปด หลักข้อจำกัดในการส่งหรือโอนข้อมูลส่วนบุคคลให้แก่บุคคลอื่นข้ามพรมแดน (Restriction on Onward Opposition) กำหนดไว้ในมาตรา 25 โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามหลักเกณฑ์ที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนดเมื่อผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคล อย่างไรก็ตามในปัจจุบันเมื่อร่างพระราชบัญญัติดังกล่าวยังมิได้ตราขึ้นเป็นพระราชบัญญัติจึงยังมิได้มีคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลผู้ซึ่งจะออกประกาศตามที่บัญญัติไว้ในมาตรา 25

หลักการที่เก้า หลักความรับผิดชอบของนายทะเบียน (Accountability Principle) กำหนดไว้ใน หมวด7 อันเป็นบทกำหนดโทษผู้ควบคุมข้อมูลส่วนบุคคลที่มิได้ปฏิบัติตามร่างพระราชบัญญัตินี้

เมื่อพิจารณาหลักการคุ้มครองข้อมูลส่วนบุคคลตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ดังที่ได้กล่าวมาแล้วจะเห็นได้ว่าร่างพระราชบัญญัตินี้มีหลักการคุ้มครองข้อมูลส่วนบุคคลที่ครบถ้วนตามหลักพื้นฐานซึ่งเป็นหัวใจของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในระดับสากล

4.3.2 การบังคับใช้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....

เมื่อพิจารณาถึงการนำร่างพระราชบัญญัติดังกล่าวมาบังคับใช้มีข้อน่าสังเกตดังต่อไปนี้

1) ความหมายของข้อมูลส่วนบุคคล

ภายใต้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ได้ให้ความหมายของ “ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวข้องกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงการระบุเฉพาะชื่อ ตำแหน่ง สถานที่ทำงาน หรือที่

อยู่ทางธุรกิจและข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ จากความหมายดังกล่าวจะเห็นได้ว่าชื่อของบุคคลไม่ได้รวมอยู่ในความหมายของข้อมูลส่วนบุคคล ส่งผลให้การเก็บรวบรวม ใช้ หรือเปิดเผยชื่อของบุคคลนั้นไม่ต้องดำเนินการตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... อาทิ ผู้เก็บรวบรวมไม่ต้องได้รับความยินยอมจากเจ้าของชื่อ ผู้เก็บรวบรวมไม่ต้องแจ้งการเก็บรวบรวมและวัตถุประสงค์ของการเก็บรวบรวมแก่เจ้าของชื่อ หรือผู้เก็บรวบรวมชื่อไม่มีหน้าที่ต่อเจ้าของชื่อนั้นในการใช้สิทธิเข้าถึงข้อมูลของตนที่อยู่ในความครอบครองของผู้เก็บรวบรวมนั้น กล่าวคือ หากผู้เก็บรวบรวมชื่อเก็บรวบรวมเพียงชื่อของบุคคล ผู้เก็บรวบรวมไม่มีหน้าที่ต้องตอบเจ้าของชื่อถึงวัตถุประสงค์ในการเก็บรวบรวมชื่อ รวมทั้งการใช้และการเปิดเผยชื่อเหล่านั้น โดยชื่อของบุคคลสามารถที่จะบ่งชี้ถึงเจ้าของชื่อได้อย่างง่ายดายควรให้ความคุ้มครองตามร่างพระราชบัญญัตินี้

อย่างไรก็ตามเมื่อพิจารณาต่อไปจะเห็นได้ว่าตำแหน่ง สถานที่ทำงาน หรือที่อยู่ทางธุรกิจนั้นได้ถูกบัญญัติยกเว้นไว้ไม่ถือเป็นข้อมูลส่วนบุคคลเช่นกัน กรณีเช่นนี้พอจะคาดคะเนได้ว่าผู้ร่างประสงค์มิให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลกระทบต่อการติดต่อหรือการดำเนินธุรกิจหรือการค้า เช่นเดียวกันกับการบัญญัติของกฎหมาย Personal Data Protection Act 2012 ของประเทศสิงคโปร์ และ Personal Information Protection and Electronic Act ของประเทศแคนาดา เนื่องจากหากกำหนดให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลการติดต่อทางธุรกิจหรือการค้าต้องได้รับความยินยอมจากเจ้าของข้อมูลนั้นเสมอย่อมจะทำให้เกิดความลำบากในการทำธุรกิจหรือกาค้าได้ แต่ในขณะเดียวกันชื่อของปัจเจกบุคคลซึ่งมิใช่ผู้ติดต่อทางธุรกิจหรือการค้าก็ควรได้รับความคุ้มครองตามร่างพระราชบัญญัตินี้ ดังนั้นจึงควรมีการบัญญัติให้ชัดแจ้งแยกชื่อหรือข้อมูลการติดต่อทางธุรกิจหรือการค้าออกจากชื่อหรือข้อมูลของปัจเจกบุคคล

2) การบังคับใช้ร่างพระราชบัญญัติดังกล่าวกับผู้ควบคุมข้อมูลส่วนบุคคลซึ่งตั้งอยู่ในต่างประเทศ

กฎหมายของประเทศใดย่อมใช้บังคับแก่ประเทศนั้นเท่านั้น อย่างไรก็ตามมีข้อยกเว้นบางประการที่จะนำกฎหมายของต่างประเทศมาบังคับใช้ เช่น กฎหมายขัดกัน เป็นต้น สำหรับกฎหมายของประเทศไทยย่อมนำมาใช้บังคับแก่ราชอาณาจักรไทยเท่านั้น ซึ่งได้แก่ พื้นดินของประเทศไทย ทะเลอาณาเขต และอากาศเหนือพื้นดินและทะเลอาณาเขต ดังนั้นร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... จึงนำมาบังคับใช้แก่บุคคลซึ่งอยู่ในราชอาณาจักรไทยเท่านั้น อย่างไรก็ตามเมื่อพิจารณาถึงเทคโนโลยีในปัจจุบันนี้ที่สามารถทำการติดต่อกันได้ทุกที่ทุกเวลา มิได้จำกัดเพียงราชอาณาจักรไทยหรือไม่ ดังนี้คนต่างประเทศก็สามารถทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลของประชาชนชาวไทยได้ซึ่งมักเกิดขึ้นในกรณีการเสนอขายสินค้าหรือบริการ ในทางกลับกันประชาชนชาวไทยคนใดคนหนึ่งก็อาจทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลซึ่ง

อยู่ในต่างประเทศได้ สำหรับกรณีหลังนี้คงมิใช่ปัญหาเนื่องจากชาวไทยคนใดที่ประสงค์เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลซึ่งอยู่ต่างประเทศต้องปฏิบัติตามหลักเกณฑ์ที่กำหนดไว้ในร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... แต่ในกรณีคนต่างประเทศประสงค์ทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของประชาชนชาวไทยกลับไม่อาจนำร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ไปใช้บังคับได้

กรณีเช่นนี้ในกฎหมายของต่างประเทศเช่น ประเทศอังกฤษ และกฎหมายของสหภาพยุโรป คือ General Data Protection Regulation ได้กำหนดให้บุคคลซึ่งตั้งในต่างประเทศแต่ได้เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของคนในดินแดนตนต้องปฏิบัติตามกฎหมายของตนด้วย เมื่อพิจารณาตามบทบัญญัติแห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ซึ่งไม่มีบทบัญญัติดังกล่าวแล้วอาจก่อให้ประชาชนชาวไทยที่ประสงค์จะติดต่อกับต่างประเทศ เช่น การซื้อสินค้าหรือบริการซึ่งจำเป็นต้องให้ข้อมูลส่วนบุคคลแก่ผู้ขายหรือผู้ให้บริการ อาจได้รับความคุ้มครองไม่เต็มที่โดยเฉพาะอย่างยิ่งหากประเทศผู้ขายหรือผู้ให้บริการมิได้มีกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือมีแต่หลักเกณฑ์ของกฎหมายดังกล่าวต่ำกว่าหลักเกณฑ์ของประเทศไทย ส่งผลให้เจ้าของข้อมูลส่วนบุคคลถูกละเมิดความเป็นส่วนตัวได้ง่าย ในกรณีเช่นนี้จึงสมควรกำหนดให้บุคคลซึ่งอยู่ในต่างประเทศแต่ได้ใช้ข้อมูลส่วนบุคคลของประชาชนชาวไทย หรือเสนอขายสินค้าหรือบริการแก่ประชาชนชาวไทยไม่ว่าจะเสียค่าบริการหรือไม่ก็ตามต้องปฏิบัติตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ดังกล่าวและแต่งตั้งผู้แทนในประเทศไทยเพื่อให้มั่นใจว่าบุคคลดังกล่าวได้ปฏิบัติตามร่างพระราชบัญญัตินี้

4.3.3 หลักเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคล

1) การให้ความยินยอม

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลจะทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้ต่อเมื่อได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ความยินยอมดังกล่าวต้องทำเป็นหนังสือ หรือทำผ่านระบบอิเล็กทรอนิกส์ ในกรณีดังกล่าวจะเห็นได้ว่าหากผู้ควบคุมข้อมูลส่วนบุคคลประสงค์จะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจากเจ้าของข้อมูล เจ้าของข้อมูลส่วนบุคคลจะต้องให้ความยินยอมแก่ผู้ควบคุมข้อมูลส่วนบุคคลเป็นหนังสือหรือทำผ่านระบบอิเล็กทรอนิกส์ กรณีเช่นนี้อาจไม่สอดคล้องกับความเป็นจริงและก่อให้เกิดปัญหาแก่ผู้ควบคุมข้อมูลส่วนบุคคลได้โดยเฉพาะอย่างยิ่งในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลเก็บข้อมูลโดยการสอบถามหรือผู้ควบคุมข้อมูลส่วนบุคคลประสงค์เก็บรวบรวมข้อมูลเพื่อประโยชน์ทางการค้าของตนเท่านั้น และข้อมูลที่ทำการเก็บรวบรวมอาจมิใช่ข้อมูล

ที่มีความสำคัญอันจะส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลได้ หากกำหนดให้เจ้าของข้อมูลส่วนบุคคลต้องลงนามในหนังสือเพื่อให้ความยินยอมอาจทำให้เจ้าของข้อมูลส่วนบุคคลเกิดความกังวลและตัดสินใจไม่มอบข้อมูลให้แก่ผู้เก็บรวบรวมข้อมูลได้ เมื่อเกิดกรณีเช่นนี้อาจส่งผลถึงการพัฒนาสินค้าหรือบริการของประเทศได้ดังนั้นร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... จึงไม่ควรกำหนดให้การให้ความยินยอมต้องทำเป็นหนังสือ อย่างไรก็ตามในกรณีข้อมูลซึ่งมีความสำคัญมีโอกาสถูกนำไปใช้ในทางที่ก่อให้เกิดผลร้ายแก่เจ้าของข้อมูลส่วนบุคคลได้ เช่น เลขบัตรประจำตัวประชาชน เป็นต้น ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลอาจกำหนดให้การเก็บรวบรวมข้อมูลเหล่านี้ต้องทำเป็นหนังสือ

นอกจากนี้ในการให้ความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในบางครั้งอาจถูกรวมเข้าไว้กับเรื่องอื่นๆ ยกตัวอย่างเช่น ในกรณีที่เจ้าของข้อมูลส่วนบุคคลเข้าทำสัญญาซื้อขายสินค้ากับบริษัทใดบริษัทหนึ่ง สัญญาดังกล่าวอาจระบุเรื่องต่างๆไว้ อาทิ ลักษณะของสินค้า การส่งสินค้า การคืนสินค้า การเลิกสัญญา รวมทั้งข้อกำหนดให้บริษัทดังกล่าวสามารถใช้หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ซื้อให้แก่บริษัทลูกหรือบริษัทในเครือได้ ทำให้เจ้าของข้อมูลส่วนบุคคลซึ่งเป็นผู้ซื้ออาจมิได้อ่านสัญญาอย่างระมัดระวังและเข้าทำสัญญากับบริษัทผู้ขายโดยไม่ทราบถึงข้อสัญญายินยอมให้บริษัทใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ ด้วยเหตุนี้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... จึงควรกำหนดให้หากการขอความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลมีเรื่องอื่นๆประกอบอยู่ด้วย ผู้ควบคุมข้อมูลส่วนบุคคลต้องแยกส่วนที่เป็นเรื่องเกี่ยวกับข้อมูลส่วนบุคคลออกต่างหากจากเรื่องอื่นๆ

2) การเพิกถอนความยินยอม

เมื่อเจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมแก่ผู้ควบคุมข้อมูลส่วนบุคคลในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลแล้ว ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลยังได้ให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลในอันที่จะเพิกถอนความยินยอมของตนไว้ในมาตรา มาตรา 17ซึ่งกำหนดให้เจ้าของข้อมูลส่วนบุคคลจะเพิกถอนความยินยอมเสียเมื่อใดก็ได้ เว้นแต่มีข้อจำกัดสิทธิในการถอนความยินยอมโดยกฎหมายหรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล ในกรณีเช่นนี้จะเห็นได้ว่าเจ้าของข้อมูลส่วนบุคคลไม่อาจเพิกถอนความยินยอมได้หากมีกฎหมายหรือสัญญาซึ่งให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคลกำหนดห้าม โดยกรณีที่อาจนำมาซึ่งปัญหาได้คือข้อสัญญาที่ห้ามเจ้าของข้อมูลส่วนบุคคลเพิกถอนความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล กล่าวคือ การเปิดโอกาสให้คู่สัญญาสามารถใส่ข้อกำหนดห้ามเพิกถอนความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคลในสัญญาอาจเป็นช่องว่าที่คู่สัญญาฝ่ายใดฝ่ายหนึ่งนำมาใช้เพื่อมิให้คู่สัญญาอีกฝ่ายหนึ่งใช้สิทธิเพิกถอนความยินยอมได้ โดยเฉพาะอย่าง

ยิ่งในกรณีที่คู่สัญญาฝ่ายนั้นมีอำนาจต่อรองที่สูงกว่า ส่งผลให้คู่สัญญาอีกฝ่ายหนึ่งไม่สามารถต่อรองได้และต้องยอมรับข้อสัญญานั้น ด้วยเหตุนี้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... จึงไม่ควรจำกัดสิทธิของเจ้าของข้อมูลส่วนบุคคลเกี่ยวกับการเพิกถอนความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไว้ตามข้อสัญญา

3) ระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล ระยะเวลาในการเก็บรักษาข้อมูลนี้มาตรา 30 กำหนดให้เป็นหนึ่งในรายการที่ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำเพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถตรวจสอบได้ โดยไม่ปรากฏว่ามีบทบัญญัติเรื่องระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคลกำหนดควบคุมให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวมข้อมูลส่วนบุคคลนั้นไว้ได้นานเพียงใด เมื่อพิจารณามาตรา 30 ประกอบกับการที่ร่างพระราชบัญญัตินี้มิได้พูดถึงระยะเวลาที่ผู้ควบคุมข้อมูลส่วนบุคคลอาจเก็บรักษาข้อมูลไว้ได้ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้กำหนดระยะเวลาในการรักษาข้อมูลส่วนบุคคลได้เอง เหตุนี้อาจก่อให้เกิดช่องว่างในการตีความกฎหมายได้ว่าแม้ข้อมูลส่วนบุคคลนั้นถูกใช้ตามวัตถุประสงค์ที่ได้แจ้งไว้ในขณะเก็บรวบรวมเป็นที่เรียบร้อยแล้วจนกระทั่งวัตถุประสงค์นั้นได้สำเร็จลุล่วงแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลยังสามารถเก็บรักษาข้อมูลส่วนบุคคลนั้นไว้ต่อไปได้หรือไม่อย่างไร สำหรับในต่างประเทศในกรณีเช่นนี้กฎหมายของต่างประเทศกำหนดให้เมื่อผู้ควบคุมข้อมูลส่วนบุคคลใช้ข้อมูลนั้นสำเร็จตามวัตถุประสงค์แล้ว ผู้ควบคุมข้อมูลส่วนบุคคลต้องลบ หรือทำลายข้อมูลนั้น สำหรับในบางประเทศอาจยินยอมให้ผู้ควบคุมข้อมูลส่วนบุคคลแปลงข้อมูลให้เป็นข้อมูลที่ไม่สามารถสืบกลับไปยังเจ้าของข้อมูลส่วนบุคคลอันเป็นข้อมูลประเภท Anonymous Data ได้

ในกรณีของประเทศไทยแล้วผู้เขียนมีความเห็นว่าควรกำหนดหลักการเบื้องต้นเกี่ยวกับกำหนดเวลาในการเก็บรักษาข้อมูลส่วนบุคคล เพื่อมิให้ผู้ควบคุมข้อมูลส่วนบุคคลนำช่องว่างของกฎหมายดังกล่าวมากำหนดระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคลไว้เกินกว่าที่จำเป็น โดยกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องลบหรือทำลายข้อมูลส่วนบุคคลเมื่อวัตถุประสงค์ที่ข้อมูลส่วนบุคคลถูกเก็บรวบรวม ใช้ หรือเปิดเผยได้สำเร็จลุล่วงแล้ว

4) การขอแก้ไขข้อมูลส่วนบุคคล

มาตรา 28 แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... กำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลทำให้ข้อมูลส่วนบุคคลของตนถูกต้อง สมบูรณ์ หรือเป็นปัจจุบัน อย่างไรก็ตามข้อมูลส่วนบุคคลนี้ผู้ควบคุมข้อมูลส่วนบุคคล

สามารถที่จะเปิดเผยแก่ผู้ควบคุมข้อมูลส่วนบุคคลอื่นได้ทั้งนี้เมื่อได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล แต่กลับไม่ปรากฏหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลที่เปิดเผยข้อมูลไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นในการแจ้งการแก้ไขนั้น

หากมิได้กำหนดหน้าที่ดังกล่าวไว้อาจก่อให้ผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการแจ้งการแก้ไขแก่ผู้ควบคุมข้อมูลส่วนบุคคลอื่นเนื่องจากเห็นว่าเป็นการเสียเวลาและอาจมีค่าใช้จ่าย ซึ่งการไม่แจ้งผู้ควบคุมข้อมูลส่วนบุคคลอื่นดังกล่าวอาจนำความเดือดร้อนหรือความเสียหายมาสู่เจ้าของข้อมูลส่วนบุคคลได้ กล่าวคือ เจ้าของข้อมูลส่วนบุคคลอาจต้องดำเนินการแจ้งการแก้ไขข้อมูลส่วนบุคคลของตนที่ไม่ถูกต้องต่อผู้ควบคุมข้อมูลส่วนบุคคลอื่นด้วยตนเอง โดยในบางครั้งเจ้าของข้อมูลส่วนบุคคลอาจมิได้มีสัมพันธ์ใดๆกับผู้ควบคุมข้อมูลส่วนบุคคลอื่นก่อให้การขอแก้ไขข้อมูลส่วนบุคคลมีความยากลำบากมากขึ้น ด้วยเหตุนี้ผู้เขียนจึงเห็นสมควรว่าร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ควรกำหนดหน้าที่แก่ผู้ควบคุมข้อมูลส่วนบุคคลในกรณีที่มีการเปิดเผยข้อมูลส่วนบุคคลแก่ผู้ควบคุมข้อมูลส่วนบุคคลอื่น ต้องแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลอื่นทำการเปลี่ยนแปลงหรือแก้ไขข้อมูลส่วนบุคคลให้สมบูรณ์และถูกต้อง

4.3.4 ปัญหาการคุ้มครองข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์ที่อาจเกิดขึ้นภายใต้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....

1) ข้อมูล Mac Address และ ข้อมูล IP Address

ข้อมูล Mac Address และ IP Address เมื่อพิจารณาตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... แล้วยังมีความไม่ชัดเจนว่าจะถือเป็นข้อมูลส่วนบุคคลหรือไม่ เนื่องจากข้อมูลทั้งสองประเภทนี้เป็นข้อมูลที่เชื่อมโยงไปยังคอมพิวเตอร์เครื่องใดเครื่องหนึ่งเท่านั้น มิใช่เป็นการเชื่อมโยงไปยังเจ้าของข้อมูลส่วนบุคคลโดยตรง อย่างไรก็ตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ระบุให้ข้อมูลที่สามารถระบุตัวบุคคลได้โดยอ้อมเป็นข้อมูลส่วนบุคคลด้วย ดังนั้น หากผู้ควบคุมข้อมูลส่วนบุคคลมีข้อมูล Mac Address หรือ IP Address และข้อมูลอื่นๆมาประกอบกันเพื่อสามารถระบุตัวเจ้าของข้อมูลส่วนบุคคลได้ ข้อมูล Mac Address หรือ IP Address ย่อมถือเป็นข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....

อย่างไรก็ตามอาจมีกรณีเกิดขึ้นได้ว่าผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวมเพียง IP Address เท่านั้น หรือได้รับข้อมูล Mac Address หรือ IP Address มาก่อนได้รับข้อมูลอื่นๆ ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติต่างร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... หรือไม่ กล่าวคือ ผู้ควบคุมข้อมูลส่วนบุคคลต้องขอความยินยอมจากเจ้าของ Mac Address หรือ IP Address

ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลหรือไม่ ในขณะที่ข้อมูล Mac Address หรือ IP Addressสามารถใช้ในการติดตามเจ้าของข้อมูลส่วนบุคคลได้เป็นอย่างดี

กรณีเช่นนี้ในสหภาพยุโรปคณะกรรมการ Article 29 Data Protection Working Partyเห็นว่าควรกำหนดให้ความคุ้มครองแก่ IP Address เป็นข้อมูลส่วนบุคคล สำหรับประเทศไทยแล้วผู้เขียนเห็นว่าควรกำหนดให้ชัดเจนว่า Mac Address และ IP Address เป็นข้อมูลส่วนบุคคลที่ได้รับความคุ้มครองเช่นเดียวกับข้อมูลส่วนบุคคลอื่นๆเพื่อมิให้เกิดความคลุมเครือและต้องมีการตีความว่าข้อมูลส่วนบุคคลตามร่างพระราชบัญญัตินี้หมายรวมถึงข้อมูล Mac Address และ IP Address หรือไม่

2) ข้อมูล Pseudonymousและ ข้อมูล Anonymous

ข้อมูล Pseudonymous และ ข้อมูล Anonymous ต่างเป็นข้อมูลที่ไม่แสดงให้เห็นบุคคลผู้เป็นเจ้าของข้อมูลส่วนบุคคลโดยมีข้อแตกต่างกันคือ ข้อมูล Pseudonymous ผู้ควบคุมข้อมูลส่วนบุคคลยังเก็บรักษาไว้ซึ่งข้อมูลแฝงที่สามารถสืบกลับไปยังเจ้าของข้อมูลส่วนบุคคลได้ ในทางกลับกันข้อมูล Anonymous เป็นข้อมูลที่ผู้ควบคุมข้อมูลส่วนบุคคลจงใจทำลายข้อมูลที่อาจระบุถึงผู้เป็นเจ้าของข้อมูลส่วนบุคคลได้ โดยกฎหมายของประเทศต่างๆให้ความคุ้มครองแก่ข้อมูล Anonymous และ Pseudonymous ต่างกัน

สืบเนื่องจากร่องรอยที่ข้อมูล Pseudonymous ยังคงรักษาไว้เพื่อสืบค้นกลับไปยังเจ้าของข้อมูลส่วนบุคคลทำให้กฎหมายของต่างประเทศโดยเฉพาะ General Data Protection Regulation กำหนดให้ข้อมูล Pseudonymous เป็นข้อมูลส่วนบุคคลได้รับความคุ้มครองตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล แต่สำหรับข้อมูลประเภท Anonymous จะไม่ถือเป็นข้อมูลส่วนบุคคล ในกรณีของประเทศไทยเมื่อพิจารณาข้อมูล Pseudonymous และ Anonymous ตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... แล้วจะเห็นได้ว่าข้อมูลPseudonymous เป็นข้อมูลที่สามารถระบุตัวบุคคลได้โดยอ้อม กล่าวคือ ผู้ที่จะระบุตัวเจ้าของข้อมูลส่วนบุคคลจากข้อมูล Pseudonymous ต้องทราบวิธีในการแปลงหรือเข้ารหัสข้อมูลนั้นเสียก่อนจึงจะสามารถทราบถึงตัวเจ้าของข้อมูลส่วนบุคคลได้ แต่สำหรับข้อมูล Anonymous ย่อมมิใช่ข้อมูลส่วนบุคคลตามความหมายของร่างพระราชบัญญัติดังกล่าว เนื่องจากมิใช่ข้อมูลที่สามารถบ่งชี้ไปยังเจ้าของข้อมูลส่วนบุคคลได้โดยตรงหรือโดยอ้อมแต่ผู้เขียนเห็นว่าร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ควรกำหนดให้ชัดแจ้งว่าข้อมูล Pseudonymousเป็นข้อมูลส่วนบุคคล เพื่อหากข้อมูลดังกล่าวตกไปอยู่ในมือของบุคลซึ่งไม่ทราบการเข้ารหัส บุคคลดังกล่าวย่อมไม่สามารถอ้างได้ว่าข้อมูล Pseudonymous นี้เป็นข้อมูลที่ไม่สามารถระบุเจ้าของข้อมูลส่วนบุคคลได้

นอกจากนี้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... มาตรา 27 กำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลลบหรือทำลาย ระงับการใช้ชั่วคราว หรือแปลงข้อมูลส่วนบุคคลให้อยู่ในรูปแบบข้อมูลที่ไม่สามารถรู้ตัวบุคคลผู้เป็นเจ้าของข้อมูลส่วนบุคคลได้ เมื่อผู้ควบคุมข้อมูลส่วนบุคคลไม่ปฏิบัติตามหลักเกณฑ์แห่งร่างพระราชบัญญัตินี้ ซึ่งร่างพระราชบัญญัติดังกล่าวมิได้กำหนดว่าข้อมูลที่ไม่สามารถรู้ตัวบุคคลผู้เป็นเจ้าของข้อมูลส่วนบุคคลได้นี้เป็นข้อมูลระดับ Pseudonymous หรือ Anonymous แต่เมื่อพิจารณาโดยรวมแล้วทำให้เข้าใจได้ว่าบทบัญญัติดังกล่าวมีเจตนารมณ์มิให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถนำข้อมูลนั้นไปใช้หรือเปิดเผยได้อีกต่อไปทำให้การแปลงข้อมูลดังกล่าวควรเป็นข้อมูลประเภท Anonymous อันเป็นการแปลงข้อมูลส่วนบุคคลที่ทำให้ไม่สามารถสืบกลับไปยังเจ้าของข้อมูลส่วนบุคคลได้ หรือการสืบกลับไปยังเจ้าของข้อมูลส่วนบุคคลเป็นการยากต้องใช้ความพยายามอย่างมาก

อย่างไรก็ตามดังที่ได้กล่าวมาแล้วข้อมูลประเภท Anonymous นี้มิใช่ข้อมูลที่ไม่สามารถสืบกลับไปยังเจ้าของข้อมูลส่วนบุคคลได้ดังเช่นที่ผ่านมา เนื่องจากความก้าวหน้าของเทคโนโลยีช่วยให้การค้นหาเจ้าของข้อมูลส่วนบุคคลจากข้อมูล Anonymous เป็นเรื่องที่ทำได้ไม่ยากนัก ดังจะเห็นได้จากงานวิจัยเกี่ยวกับข้อมูลของคนไข้ และงานวิจัยเกี่ยวกับ Netflix ซึ่งได้กล่าวไว้แล้วในบทที่สอง แม้ข้อมูลนั้นจะไม่ปรากฏว่าเจ้าของข้อมูลส่วนบุคคลเป็นใคร แต่เมื่อผู้ควบคุมข้อมูลส่วนบุคคลสามารถรวบรวมข้อมูลอื่นได้มากเพียงพอซึ่งข้อมูลดังกล่าวอาจมิใช่ข้อมูลที่สามารถสืบกลับไปยังเจ้าของข้อมูลส่วนบุคคลได้ก็ตาม แต่เมื่อนำข้อมูลเหล่านั้นมาประกอบกันแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลยังสามารถระบุตัวเจ้าของข้อมูลส่วนบุคคลได้

นอกจากนี้ข้อมูลประเภท Anonymous ยังมีความเสี่ยงต่อการถูกเปิดเผยหรือเข้าถึงโดยผู้เข้าถึงเป็นผู้ไม่มีสิทธิ เนื่องจากข้อมูลประเภทนี้ผู้ควบคุมข้อมูลส่วนบุคคลอาจเห็นว่าไม่สามารถสืบกลับไปยังเจ้าของข้อมูลส่วนบุคคลได้จึงมิได้ให้ความสำคัญในการดูแลรักษาและจัดมาตรการป้องกันความปลอดภัยเช่นเดียวกับข้อมูลส่วนบุคคลอีกด้วย จากเหตุผลที่กล่าวมาผู้เขียนจึงเห็นว่าการเปิดโอกาสให้แปลงข้อมูลส่วนบุคคลให้เป็นข้อมูลประเภท Anonymous อาจทำให้สิทธิในความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลเสี่ยงต่อการถูกละเมิดได้ ประกอบกับพฤติการณ์ของผู้ควบคุมข้อมูลส่วนบุคคลที่เพิกเฉยหรือละเลยไม่ปฏิบัติตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... อันเป็นการไม่ใยดีต่อผลเสียที่อาจเกิดต่อเจ้าของข้อมูลส่วนบุคคล ผู้เขียนจึงเห็นว่าในกรณีเช่นนี้ไม่ควรเปิดโอกาสให้ผู้ควบคุมข้อมูลส่วนบุคคลแปลงข้อมูลให้อยู่ในรูปที่ไม่สามารถรู้ตัวบุคคลผู้เป็นเจ้าของข้อมูลส่วนบุคคลได้ มิเช่นนั้นแล้วอาจนำมาซึ่งความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล และควรกำหนดให้เจ้าของข้อมูลส่วนบุคคลที่ถูกเชื่อมโยงข้อมูล Anonymous หรือ Pseudonymous กับตนได้ มีสิทธิตามที่กำหนดในร่างพระราชบัญญัตินี้

3) การทำ Profiling และการตัดสินใจโดยระบบอัตโนมัติ

การทำ Profiling คือการติดตามและเก็บรวบรวมข้อมูลเกี่ยวกับเจ้าขอข้อมูลส่วนบุคคล และนำมาวิเคราะห์ประมวลผลและตัดสินใจโดยเครื่องอัตโนมัติเพื่อบอกถึงพฤติการณ์ต่างๆเกี่ยวกับเจ้าของข้อมูลส่วนบุคคล เช่น ลักษณะนิสัย ความชอบส่วนตัว ความประพฤติ หรือความสามารถในการทำงาน เป็นต้น เดิมการทำ Profiling นิยมทำกันมากเพื่อบอกถึงความสามารถในการทำงานของเจ้าของข้อมูลส่วนบุคคล แต่ในปัจจุบันนี้เริ่มแพร่หลายในด้านการโฆษณา มีวิธีการคือผู้ควบคุมข้อมูลส่วนบุคคลจะทำการเก็บรวบรวมข้อมูลการใช้งานของเจ้าของคอมพิวเตอร์โดยอาศัยเครื่องมือต่างๆ เช่น Cookies Stateless Tracking (Browse Fingerprint) หรือ Deep Packet Inspection (DPI) เป็นต้น นำข้อมูลที่ได้มาประมวลผลเพื่อและแสดงเป็นโฆษณาตามเว็บไซต์ต่างๆ ข้อเสียของการทำ Profiling มีหลายประการดังที่ได้กล่าวมาแล้วในบทที่สอง เช่น ก่อให้เกิดการเลือกปฏิบัติในด้านราคาต่อ เป็นการปิดกั้นโอกาสของเจ้าของข้อมูลส่วนบุคคลในการเข้าถึงสินค้าประเภทอื่น หรืออาจทำให้ข้อมูลเกี่ยวกับเจ้าของข้อมูลส่วนบุคคลถูกเปิดเผย เป็นต้น

จากลักษณะของการทำ Profiling และการตัดสิจในโดยระบบอัตโนมัติที่กล่าวมาแล้วกฎหมายของต่างประเทศคือ General Data Protection Regulation จึงให้ความคุ้มครองแก่การกระทำดังกล่าวเมื่อพิจารณาลักษณะของการทำ Profiling โดยเฉพาะอย่างยิ่งในด้านโฆษณาตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... แล้วจะเห็นได้ว่าข้อมูลที่ได้จากการเก็บรวบรวมนี้ถือเป็นข้อมูลส่วนบุคคล เนื่องจากผู้ควบคุมข้อมูลส่วนบุคคลสามารถระบุตัวเจ้าของข้อมูลนั้นโดยอาศัยเครื่องมือที่ตนใช้ในการเก็บข้อมูลส่วนบุคคล ส่งผลให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนหรือในขณะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นโดยต้องแจ้งวัตถุประสงค์ให้เจ้าของข้อมูลทราบด้วย

อย่างไรก็ตามแม้จะได้มีการแจ้งถึงวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลแล้ว การทำ Profiling ยังอาจก่อให้เกิดผลเสียแก่เจ้าของข้อมูลส่วนบุคคลได้ เช่น ข้อมูลที่ได้รับไม่ถูกต้องหรือไม่ครบถ้วน ทั้งเป็นการไม่แน่ว่าระบบอัตโนมัติดังกล่าวจะตัดสินใจได้ถูกต้องตรงต่อความจริง ดังนั้นกฎหมายในต่างประเทศโดยเฉพาอย่างยิ่ง General Data Protection Regulation จึงเห็นสมควรกำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิในการคัดค้าการ Profiling และการตัดสินใจโดยระบบอัตโนมัติ นอกจากนี้ยังกำหนดให้ในกรณีที่มีการตัดสินใจด้วยระบบอัตโนมัติ ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีบุคคลธรรมดารวมอยู่ด้วยมิใช่ให้ระบบอัตโนมัติประมวลผลเพียงอย่างเดียว และให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลที่จะสามารถแสดงความคิดเห็นเกี่ยวกับการตัดสินใจนั้นได้

สำหรับประเทศไทยร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... มิได้กล่าวถึงการตัดสินใจโดยระบบอัตโนมัติ หรือการทำ Profiling ซึ่งจะส่งผลให้เจ้าของข้อมูลส่วน

บุคคลไม่สามารถคัดค้านการประมวลผลโดยระบบอัตโนมัติหรือการทำ Profiling ได้ และมิอาจแสดงความเห็นหรือคัดค้านผลลัพธ์ที่เกิดจากการทำ Profiling หรือการตัดสินใจโดยวิธีอัตโนมัติได้ แม้ทั้งเจ้าของข้อมูลส่วนบุคคลอาจตระหนักว่าการทำ Profiling นั้นส่งผลเสียต่อตนก็ตาม

เนื่องด้วยการทำ Profiling หรือการใช้ระบบอัตโนมัติในการตัดสินใจนี้ได้ถูกนำมาใช้เพิ่มมากขึ้นเนื่องจากเป็นการ สะดวก รวดเร็ว และประหยัดค่าใช้จ่ายและแรงงาน ดังนั้นประเทศไทยจึงควรกำหนดให้ความคุ้มครองเจ้าของข้อมูลส่วนบุคคลจากการทำ Profiling และการนำระบบอัตโนมัติมาใช้ในการตัดสินใจโดยให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำ Profiling หรือใช้ระบบอัตโนมัติตัดสินใจเกี่ยวกับตน ทั้งในกรณีที่เจ้าของข้อมูลส่วนบุคคลยินยอมหรือมีความจำเป็นต้องทำ Profiling หรือใช้ระบบอัตโนมัติในการตัดสินใจควรกำหนดให้มีบุคคลธรรมดาซึ่งเป็นเจ้าหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลเข้ามาเกี่ยวข้องด้วยเพื่อตรวจสอบความถูกต้องของการประมวลผลนั้น และควรให้สิทธิแก่เจ้าของข้อมูลในอันที่จะแสดงความคิดเห็นหรือคัดค้านผลลัพธ์ที่เกิดขึ้นจากการทำ Profiling หรือใช้ระบบอัตโนมัติในการตัดสินใจได้ เนื่องจากระบบอัตโนมัติอาจได้รับข้อมูลที่ไม่ถูกต้อง ไม่ครบถ้วน หรือไม่ตรงต่อความจริง หรือเป็นการผิดพลาดของระบบก่อให้ผลลัพธ์ที่ได้ผิดไปจากความเป็นจริงและส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล

4) ข้อมูลไบโอเมตริก (Biometric)

ข้อมูลไบโอเมตริก (Biometric)เป็นข้อมูลเกี่ยวกับชีววิทยาของเจ้าของข้อมูลส่วนบุคคล โดยผู้ควบคุมข้อมูลส่วนบุคคลจะเก็บตัวอย่างข้อมูลไว้และนำข้อมูลนั้นมาใช้เปรียบเทียบกับข้อมูลที่ได้มาในภายหลังเพื่อยืนยันว่าบุคคลนั้นเป็นเจ้าของข้อมูลไบโอเมตริก (Biometric)ที่ได้เก็บรักษาไว้ แม้ข้อมูลไบโอเมตริก (Biometric)บางประเภทอาจมีความสามารถในการระบุตัวเจ้าของข้อมูลส่วนบุคคลให้แม่นยำได้ไม่ถึง 100% เนื่องจากอาจมีบุคคลอื่นที่มีข้อมูลในลักษณะคล้ายกัน หรือเกิดจากความเปลี่ยนแปลงของเจ้าของข้อมูลส่วนบุคคล เช่น รูปหน้าที่เปลี่ยนไปตามวัยของเจ้าของข้อมูลส่วนบุคคล หรืออาจทำศัลยกรรมตกแต่งใบหน้า เป็นต้น แต่ข้อมูลไบโอเมตริก (Biometric)ที่นิยมนำมาใช้กันอย่างแพร่หลายเป็นข้อมูลแบบที่มีความแม่นยำสูงในการระบุตัวเจ้าของข้อมูลส่วนบุคคล เช่น ลายพิมพ์นิ้วมือ การแสกนม่านตา หรือลายพิมพ์ DNA เป็นต้น

เดิมข้อมูลไบโอเมตริก (Biometric)จำกัดการใช้อยู่ในวงแคบเพื่อการยืนยันตัวเจ้าของข้อมูลไบโอเมตริก (Biometric)ในการทำงานหรือการทำนิติกรรมเท่านั้น แต่ในปัจจุบันนี้เทคโนโลยีช่วยให้สามารถพัฒนาอุปกรณ์ตรวจสอบข้อมูลไบโอเมตริก (Biometric)ให้มีขนาดเล็กลงและมีความแม่นยำในการเปรียบเทียบ ข้อมูลไบโอเมตริก (Biometric)จึงได้ถูกนำมาใช้เพื่อการค้าหรือการยืนยันตัวเจ้าของข้อมูลส่วนบุคคลมากขึ้น อาทิ บริษัท Mastercard ได้ผลิตบัตรเครดิตซึ่งใช้

ลายพิมพ์นิ้วมือของเจ้าของบัตรเพื่ออนุมัติการจ่ายเงินแทนการลงลายมือชื่อซึ่งเป็นเพียงการยืนยันตัวเจ้าของบัตรเท่านั้น หรือการนำเครื่องตรวจสอบลายพิมพ์นิ้วมือติดตั้งไว้ในสมาร์ทโฟนเพื่อยืนยันตัวผู้มีสิทธิใช้งานสมาร์ทโฟน กรณีดังกล่าวแสดงให้เห็นชัดแจ้งว่าข้อมูลไบโอเมตริก (Biometric) ได้ถูกนำใช้งานอย่างแพร่หลายมากขึ้น ในขณะที่ข้อมูลไบโอเมตริก (Biometric)นี้กลับสามารถเป็นชนวนให้เกิดการละเมิดความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลได้อย่างง่ายดาย

โดยที่การเก็บรวบรวมข้อมูลไบโอเมตริก (Biometric)สามารถทำได้ง่ายไม่จำกัดว่าต้องได้รับความยินยอมจากเจ้าของข้อมูลส่าวนบุคคลหรือไม่ หรือแม้กระทั่งมีการเก็บรวบรวมโดยเจ้าของข้อมูลส่วนบุคคลมิได้รับรู้เลยก็ได้ เช่น ลายพิมพ์นิ้วมืออาจถูกเก็บรวบรวมได้เมื่อเจ้าของข้อมูลส่วนบุคคลได้สัมผัสวัตถุต่างๆ อาทิ เหล็ก ไม้หรือแก้ว หรือรูปหน้าหรือท่าทางการเคลื่อนไหวของเจ้าของข้อมูลส่วนบุคคลสามารถบันทึกโดยกล้อง เป็นต้น นอกจากนี้ข้อมูลไบโอเมตริก (Biometric)ยังสามารถแสดงให้เห็นถึงสภาพของเจ้าของข้อมูลส่วนบุคคลได้ กล่าคือ ข้อมูลไบโอเมตริก (Biometric)เป็นข้อมูลที่เก็บรวบรวมจากลักษณะทางชีววิทยาของบุคคล ซึ่งเมื่อร่างกายของคนเรามีความผิดปกติ บกพร่อง มีความเครียด หรือเป็นผู้ทำงานหนัก ร่างกายจะทำการปรับตัวและแสดงออกมา ยกตัวอย่างเช่น สีของตาสามารถแสดงถึงโรคต่างๆได้ หรือหน้าตาที่เคร่งเครียดสามารถบอกความรู้สึกของเจ้าของใบหน้าได้ และแม้กระทั่งมือที่หยาบกร้านสามารถแสดงให้เห็นได้ว่าบุคคลนั้นทำงานอย่างหนัก

จากความอ่อนไหวของข้อมูลไบโอเมตริก (Biometric)ที่นอกจากจะสามารถนำมาใช้กับการยืนยันตัวบุคคล และทำการเก็บรวบรวมได้ง่ายแล้ว ยังสามารถสื่อถึงสภาพของเจ้าของข้อมูลส่วนบุคคลได้ เหตุนี้ทำให้สหภาพยุโรปตระหนักถึงปัญหาที่อาจเกิดขึ้นตามมาหากนำหลักเกณฑ์การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลมาใช้กับข้อมูลไบโอเมตริก (Biometric)จึงได้กำหนดใน General Data Protection Regulation ที่จะใช้บังคับแทน Directive 95/46/EC กำหนดให้ข้อมูลไบโอเมตริก (Biometric)เป็นข้อมูลที่มีความอ่อนไหวซึ่งการเก็บรวบรวม ใช้ และเปิดเผยจะมีหลักเกณฑ์และข้อจำกัดที่เคร่งครัดกว่าการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลทั่วไป

สำหรับประเทศไทยแล้วข้อมูลไบโอเมตริก (Biometric)แม้เป็นข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้โดยตรงจึงเป็นข้อมูลส่วนบุคคลได้รับความคุ้มครองต่างร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ก็ตาม แต่จากเหตุผลที่ได้กล่าวมาแล้วการใช้หลักเกณฑ์ทั่วไปเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลแก่ข้อมูลไบโอเมตริก (Biometric)มีลักษณะไม่เหมาะสมกับสภาพความอ่อนไหวของข้อมูล ดังนั้นประเทศไทยจึงควรกำหนดให้ข้อมูลไบโอเมตริก (Biometric)เป็นข้อมูลที่มีความอ่อนไหวอันจะได้รับความคุ้มครองเป็นพิเศษกว่าข้อมูลส่วนบุคคลทั่วไป

5) สิทธิในการโอนข้อมูลส่วนบุคคล(Right to data portability)

ในปัจจุบันผู้เก็บรวบรวมข้อมูลส่วนบุคคลส่วนใหญ่มักเก็บรวบรวมข้อมูลไว้ในรูปแบบอิเล็กทรอนิกส์ โดยอาจมีความแตกต่างกันไปในโปรแกรมสำหรับใช้อ่านข้อมูลเหล่านั้น กรณีที่ผู้เก็บรวบรวมข้อมูลส่วนบุคคลเป็นผู้เสนอขายสินค้าหรือบริการ และเจ้าของข้อมูลส่วนบุคคลเป็นผู้บริโภค หากยินยอมให้เจ้าของข้อมูลส่วนบุคคลสามารถนำข้อมูลเหล่านี้มาใช้วิเคราะห์ถึงลักษณะของการบริโภคของตนและเปรียบเทียบสินค้าหรือบริการที่ตนเลือกใช้กับสินค้าหรือบริการของผู้ประกอบการรายอื่น หรือมีการยินยอมให้โอนข้อมูลเหล่านั้นในระหว่างผู้เก็บรวบรวมข้อมูลส่วนบุคคลซึ่งเป็นผู้ประกอบการย่อมเป็นการเอื้อต่อการแข่งขันเสรีทำให้ผู้บริโภคสามารถเปลี่ยนผู้ให้บริการได้ง่าย

การเข้าถึงหรือโอนข้อมูลส่วนบุคคลสำหรับในต่างประเทศขณะนี้มีโครงการเพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถนำข้อมูลของตนไปวิเคราะห์ถึงลักษณะการบริโภคและเปรียบเทียบกับสินค้าหรือบริการของผู้ประกอบการรายอื่น เช่น โครงการ MiData ในประเทศอังกฤษ โครงการ Smart Disclosure ในประเทศสหรัฐอเมริกา หรือสิทธิในการโอนข้อมูลส่วนบุคคล(Right to data portability)ของ General Data Protection Regulation

สำหรับประเทศไทยผู้เขียนเห็นว่าควรกำหนดให้มีสิทธิในการโอนข้อมูลส่วนบุคคล (Right to data portability)เช่นกัน เนื่องจากสิทธิดังกล่าวจะทำให้ผู้บริโภคสามารถทราบได้ว่าการใช้จ่ายของตนส่วนใหญ่ได้เสียไปกับสิ่งจำเป็นหรือกับสินค้าฟุ่มเฟือยและสามารถประหยัดการใช้จ่ายของตนได้ ทั้งทำให้ผู้บริโภคสามารถเปลี่ยนผู้ให้บริการได้โดยไม่ต้องเสียเวลาไปกับการให้ข้อมูลส่วนบุคคลแก่ผู้ประกอบการใหม่ อย่างไรก็ตามเมื่อให้สิทธิแก่ผู้บริโภคในการโอนข้อมูลส่วนบุคคลแล้วควรมีการกำหนดรูปแบบการเก็บรักษาข้อมูลส่วนบุคคลเพื่อให้ผู้ประกอบกาเก็บรักษาข้อมูลส่วนบุคคลไว้ในรูปแบบเดียวกันซึ่งเมื่อโอนข้อมูลยังผู้ปกระกอบการอื่นแล้ว ผู้ประกอบการที่รับโอนสามารถนำข้อมูลส่วนบุคคลไปใช้ได้จริง อย่างไรก็ตามการเปลี่ยนแปลงรูปแบบการเก็บรักษาข้อมูลส่วนบุคคลในเบื้องต้นอาจก่อภาระค่าใช้จ่ายแก่ผู้ประกอบการในการลงทุนพัฒนาระบบเก็บรักษาข้อมูลส่วนบุคคล แต่เมื่อพิจารณาให้ถี่ถ้วนแล้วจะเห็นได้ว่าหากผู้ประกอบการรายนั้นมีสินค้าหรือบริการที่ตรงตามความต้องการของผู้บริโภค ย่อมทำให้ผู้บริโภคเปลี่ยนมาใช้สินค้าหรือบริการของตนมากขึ้น

บทที่ 5
บทสรุปและข้อเสนอแนะ

5.1 บทสรุป

ข้อมูลส่วนบุคคล (Personal Information) เป็นข้อมูลเกี่ยวกับเจ้าของข้อมูลส่วนบุคคล ทำให้สามารถเชื่อมโยงไปยังเจ้าของข้อมูลส่วนบุคคลได้ไม่ว่าทางตรงหรือทางอ้อม เช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์ ข้อมูลทางกายภาพ หรือความคิดเห็นทางการเมือง เป็นต้น นอกจากนี้ข้อมูลของอุปกรณ์อิเล็กทรอนิกส์ ได้แก่ Mac Addressและ IP Address หากสามารถเชื่อมโยงไปยังเจ้าของได้ย่อมถือว่าเป็นข้อมูลส่วนบุคคลได้ อย่างไรก็ตามข้อมูล IP Address สามารถแบ่งออกได้เป็น 2 ประเภทได้แก่ Static IP Address และ Dynamic IP Address โดยข้อมูลทั้งสองนี้ประกอบด้วยกลุ่มตัวเลขลักษณะเดียวกันแตกต่างกันที่ Static IP Address จะมีตัวเลขคงเดิมทุกครั้งที่มีการเชื่อมต่ออินเตอร์เน็ต ในขณะที่ข้อมูล Dynamic IP Address นี้จะมีการเปลี่ยนแปลงเสมอเมื่อเชื่อมต่ออินเตอร์ใหม่ โดยที่ข้อมูลทั้งสองประเภทนี้มีลักษณะเช่นเดียวกันจึงก่อให้เกิดความลำบากในการพิจารณาว่าข้อมูล IP Address ใดเป็นข้อมูลประเภท Static หรือเป็น Dynamic ดังนั้นจึงควรพิจารณาให้ความคุ้มครอง IP Address ทั้งสองในลักษณะเดียวกัน

ประเภทของข้อมูลส่วนบุคคลสามารถแบ่งออกได้เป็นสองประเภท คือ ข้อมูลทั่วไป เป็นข้อมูลเกี่ยวกับบุคคลผู้เป็นเจ้าของข้อมูลที่สามารถชี้เฉพาะไปยังเจ้าของข้อมูลส่วนบุคคลได้ และข้อมูลที่มีความอ่อนไหว คือ ข้อมูลที่มีความละเอียดอ่อนสูง หากมีการเปิดเผยอาจก่อให้เกิดผลกระทบที่ไม่พึงประสงค์ต่อเจ้าของข้อมูลส่วนบุคคลได้ กล่าวคือ กระทบต่อความรู้สึกของเจ้าของข้อมูลหรือประชาชนทั่วไป หรือเป็นข้อมูลที่ก่อให้เกิดความขัดแย้งได้ เช่น ความคิดเห็นทางการเมือง ข้อมูลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความเชื่อเกี่ยวกับลัทธิ ศาสนา ประวัติอาชญากรรม หรือประวัติสุขภาพ เป็นต้น

สำหรับกฎหมายการคุ้มครองข้อมูลส่วนบุคคลมักวางอยู่บนหลักพื้นฐานทั้งหมด 9 ประการ ได้แก่

1. หลักการจัดเก็บข้อมูลส่วนบุคคลอย่างจำกัด
2. หลักการประมวลผลข้อมูลส่วนบุคคลอย่างมีคุณภาพและได้สัดส่วน
3. หลักการระบุวัตถุประสงค์และระยะเวลาในการใช้ข้อมูลส่วนบุคคล
4. หลักการใช้ข้อมูลส่วนบุคคลอย่างจำกัด
5. หลักการป้องกันรักษาความปลอดภัยของข้อมูลส่วนบุคคล

6. หลักเปิดเผยโปร่งใส

7. หลักการมีส่วนร่วมของเจ้าของข้อมูลส่วนบุคคล

8. หลักข้อจำกัดในการส่งหรือโอนข้อมูลส่วนบุคคลให้แก่บุคคลอื่นข้ามพรมแดน

9. หลักความรับผิดชอบของนายทะเบียน

นอกจากนี้ยังมีหลักการขององค์การต่างๆที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลอีก เช่น Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data ของ OECD หรือ Guidelines for the Regulation of Computerized Personal Data Files 1990 (United Nations 1990) เป็นต้น

โดยในปัจจุบันเทคโนโลยีมีความก้าวหน้าอย่างมากและถูกนำมาใช้งานอย่างแพร่หลาย โดยมีอินเตอร์เน็ตเป็นส่วนหนึ่งที่จำเป็นในชีวิตประจำวันของเด็กและผู้ใหญ่ไม่ว่าจะเป็นเพื่อใช้ในการสื่อสาร การทำธุรกรรม การค้นคว้าหาความรู้ หรือการพักผ่อนหย่อนใจ นอกจากนี้ก่อนตัดสินใจซื้อสินค้าหรือบริการอย่างใดอย่างหนึ่งหลายๆคนหันมาใช้อินเตอร์เน็ตในการค้นคว้ารวมถึงปรึกษาข้อดีข้อเสียของสินค้าหรือบริการนั้น และในหลายๆครั้งคนเหล่านี้ตัดสินใจสั่งซื้อสินค้าผ่านทางออนไลน์ ซึ่งแต่ละการกระทำบนโลกอินเตอร์เน็ตของพวกเขาเหล่านั้นไม่ว่าจะเป็นการค้นหาสินค้าหรือบริการหรือเป็นไปเพียงเพื่อความบันเทิงมักจะถูกจับตามองโดยเครื่องมือที่ของผู้ประกอบการโดยที่พวกเขาไม่รู้ตัว สำหรับเทคโนโลยีทางอิเล็กทรอนิกส์ที่มีผลกระทบต่อสิทธิในความเป็นอยู่ส่วนตัว ดังที่ได้ศึกษามามีดังต่อไปนี้

1) ข้อมูล Mac Address หรือ IP Address

ข้อมูลMac Address หรือ IP Address เป็นชุดของตัวเลขประกอบกันขึ้นโดยมีจุดขั้นกลางเพื่อใช้ในการสื่อสารระหว่างคอมพิวเตอร์ Mac Address เป็นชุดของตัวเลขกำหนดไว้ตายตัวสำหรับคอมพิวเตอร์แต่ละเครื่องและไม่มีการเปลี่ยนแปลง แตกต่างไปจาก IP Address ซึ่งจะถูกแจกจ่ายแก่เครื่องคอมพิวเตอร์โดยผู้ให้บริการอินเตอร์เน็ต (Internet Service Provider) สามารถแบ่งได้ 2 ประเภท คือ Static IP Address มีลักษณะคล้าย Mac Address คือเป็นชุดของตัวเลขที่ตายตัวไม่มีการเปลี่ยนแปลง และ Dynamic IP Address เป็นชุดของตัวเลขที่เปลี่ยนแปลงทุกครั้งเมื่อผู้ใช้เชื่อมต่อกับอินเตอร์เน็ต โดยชุดของตัวเลยเหล่านี้สามารถเชื่อมโยงไปยังคอมพิวเตอร์เครื่องใดเครื่องหนึ่งโดยเฉพาะและการเชื่อมโยงจะง่ายขึ้นสำหรับข้อมูล Mac Address และ Static IP Address ซึ่งเป็นชุดตัวเลขที่ไม่มีการเปลี่ยนแปลงและถูกกำหนดไว้ตายตัวสำหรับเครื่องคอมพิวเตอร์เครื่องใดเครื่องหนึ่งเท่านั้น ข้อมูล Mac Address และ IP Address เหล่านี้ทำให้ผู้ที่มีข้อมูลเหล่านี้ไว้ในความครอบครองสามารถสืบค้นข้อมูลต่างๆที่เจ้าของข้อมูลทิ้งร่องรอยไว้บนอินเตอร์เน็ต เช่น ผู้

ให้บริการเครือข่ายอินเตอร์เน็ต (Internet Service Provider) หรือ ตำแหน่งของเจ้าของข้อมูล รวมถึงสถานที่ทำงานของผู้เป็นเจ้าของข้อมูลได้

2) ข้อมูลที่ไม่สามารถรู้ตัวเจ้าของข้อมูลส่วนบุคคลได้

ข้อมูลประเภทนี้เป็นข้อมูลที่มีการกระทำบางอย่าง เช่น การเข้ารหัสเพื่อปกปิด หรือลบข้อมูลที่ทำให้ค้นหาเจ้าของข้อมูลส่วนบุคคลได้ ถูกนำมาใช้เพื่อปกปิดตัวเจ้าของข้อมูลส่วนบุคคล เพื่อมิให้เกิดการละเมิดความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลได้ สามารถแบ่งได้สองประเภท คือ ข้อมูล Anonymous และข้อมูล Pseudonymous โดยข้อมูลทั้งสองประเภทโดยตัวของข้อมูลเองแล้วจะไม่สามารถทราบเจ้าของข้อมูลส่วนบุคคลได้ แต่มีความแตกต่างกันในระหว่างข้อมูลทั้งสองประเภท กล่าวคือ ข้อมูล Anonymous เป็นข้อมูลที่มีการใช้โปรแกรมหรือการเข้ารหัสเพื่อทำให้ไม่สามารถเชื่อมโยงไปยังเจ้าของข้อมูลส่วนบุคคลได้เลยหรือการเชื่อมโยงไปยังเจ้าของข้อมูลส่วนบุคคลเป็นไปได้ยาก แต่ข้อมูล Pseudonymous เป็นข้อมูลที่มีการแทนค่าข้อมูลที่สามารถเชื่อมโยงไปยังเจ้าของข้อมูลส่วนบุคคลได้ซึ่งหากมีบุคคลที่ทราบการแทนค่าหรือผู้ที่ทราบวิธีการเข้ารหัสข้อมูลจะสามารถสืบค้นกลับไปหาเจ้าของข้อมูลส่วนบุคคลได้

อย่างไรก็ตามแม้ข้อมูลทั้งสองประเภทเป็นข้อมูลที่ตั้งใจปกปิดมิให้สืบค้นเจ้าของข้อมูลส่วนบุคคล แต่ความก้าวหน้าของเทคโนโลยีในปัจจุบันกลับทำให้ข้อมูลทั้งสองประเภทนี้สามารถเชื่อมโยงไปยังเจ้าของข้อมูลส่วนบุคคลได้โดยเฉพาอย่างยิ่งเมื่อประกอบกับการทำ Profiling จึงเป็นเหตุให้ผู้เป็นเจ้าของข้อมูลส่วนบุคคลทั้งสองประเภทนี้คงมิอาจแน่ใจอีกต่อไปว่าตนจะไม่ถูกค้นพบโดยหากมีการแปลงข้อมูลให้เป็นข้อมูล Pseudonymous หรือ Anonymousตัวอย่างที่สามารถแสดงได้ชัดเจนว่าข้อมูลทั้งสองประเภทนี้ยังสามารถสืบกลับไปยังเจ้าของข้อมูลได้คืองานวิจัยของ Netflix ซึ่งเป็นเว็บไซต์ให้บริการดูหนังออนไลน์ งานวิจัยนี้ทำโดยให้ผู้ใช้บริการให้คะแนนหนังที่ตนได้ดูเพื่อประเมินความพอใจในหนังเรื่องนั้น ปรากฏว่าเมื่อผู้ใช้งานประเมินหนังเพียงจำนวน 6 เรื่องก็จะทำให้สามารถระบุตัวผู้ใช้ได้แม่นยำถึง 99 เปอร์เซ็นต์

3) Profiling

Profiling หรือเรียกอีกอย่างหนึ่งว่า Behavioral Tracking เป็นเทคโนโลยีที่แพร่หลายมากขึ้นในช่วงที่ผ่านมาโดยเฉพาะอย่างยิ่งนิยมนำมาใช้โดยบริษัทโฆษณา ลักษณะของการทำ Profiling คือการใช้เครื่องมือ เช่น Cookies,Javascript ,Stateless Tracking หรือ Location Tracking เพื่อติดตามพฤติกรรมของบุคคลใดบุคคลหนึ่ง และนำพฤติกรรมนั้นมาสร้างเป็น Profile ซึ่งในหลายๆครั้งข้อมูลเหล่านี้ถูกนำมาใช้เพื่อการตัดสินใจโดยวิธีอัตโนมัติ ข้อมูลที่ได้จากการทำ Profiling จะถูกนำมาใช้เพื่อประโยชน์ต่างๆโดยเฉพาะอย่างยิ่งเพื่อทราบข้อมูลของเจ้าของข้อมูลส่วน

บุคคล เช่นเพื่อทำการโฆษณาให้ตรงตามความสนใจของเจ้าของข้อมูลส่วนบุคคล เพื่อประเมินพฤติกรรม หรือทัศนคติของผู้เป็นเจ้าของข้อมูลส่วนบุคคล เป็นต้น

การทำ Profiling นี้ทำให้เจ้าของข้อมูลส่วนบุคคลถูกติดตามโดยไม่รู้ตัวและสูญเสียความเป็นส่วนตัว เจ้าของข้อมูลอาจมิได้ระมัดระวังการกระทำของตนมากนักทำให้ข้อมูลที่ตนประสงค์จะปกปิดไว้ถูกเปิดเผยโดยเฉพาะอย่างยิ่งเมื่อข้อมูลนั้นเป็นข้อมูลที่มีความอ่อนไหวอาจก่อให้เกิดผลกระทบร้ายแรงต่อเจ้าของข้อมูลส่วนบุคคล นอกจานี้หากถูกนำไปใช้ในการโฆษณาอาจก่อให้เกิดการเลือกปฏิบัติในด้านราคาเพื่อจูงใจให้เจ้าของข้อมูลส่วนบุคคลต้องรีบตัดสินใจซื้อสินค้าหรือบริการทั้งยังเป็นปิดกั้นโอกาสของเจ้าของข้อมูลส่วนบุคคลในการเข้าถึงข้อมูลอื่นๆ นอกจากนี้เจ้าของข้อมูลส่วนบุคคลอาจตกอยู่ภายใต้การตัดสินใจโดยวิธีอัตโนมัติซึ่งเป็นการไม่แน่ว่าผลลัพธ์ที่เกิดขึ้นจากการตัดสินใจโดยวิธีอัตโนมัตินั้นจะถูกต้องหรือไม่อีกด้วย

4) ข้อมูลไบโอเมตริก (Biometric)

ข้อมูลไบโอเมตริก (Biometric) มาจากคำว่าไบโอ และคำว่าเมตริก เป็นเทคโนโลยีที่นำมาใช้กับพฤติกรรมหรือคุณลักษณะบางประการของสิ่งมีชีวิตอันเป็นคุณลักษณะที่สามารถนับหรือวัดได้และนำการวัดหรือการนนับนั้นมาผนวกเข้ากับหลักการทางสถิติเพื่อแยกแยะหรือจดจำบุคคลแต่ละบุคคล เทคโนโลยีดังกล่าวอาศัยการเก็บข้อมูลจากร่างกายของบุคคลเพื่อเป็นข้อมูลตัวอย่างและนำไปเปรียบเทียบกับข้อมูลที่ได้รับในภายหลัง เดิมข้อมูลไบโอเมตริก (Biometric) ไม่ได้นิยมใช้กันอย่างแพร่หลายนัก แต่เนื่องด้วยความก้าวหน้าของเทคโนโลยีปัจจุบันสามารถพัฒนาให้อุปกรณ์ที่เกี่ยวกับการประมวลผลข้อมูลไบโอเมตริก (Biometric) มีขนาดเล็กลงและมีค่าใช้จ่ายไม่สูงมาก จึงได้นิยมนำมาใช้เพื่อระบุตัวเจ้าของข้อมูลส่วนบุคคลอย่างแพร่หลายมากขึ้นจะเห็นได้จากสมาร์ทโฟนได้นำเครื่องแสกนลายพิมพ์นิ้วมือมาบรรจุไว้ และบัตรเครดิตอย่าง Mastercard ได้นำเทคโนโลยีการแสกนลายพิมพ์นิ้วมือมาใช้แทนการลงลายมือชื่อ ข้อมูลไบโอเมตริก (Biometric) มีหลายประเภท เช่น การตรวจลายพิมพ์ดีเอ็นเอ การรู้จำม่านตา การรู้จำใบหน้า หรือ การรู้จำลายนิ้วมือ เป็นต้น

เนื่องจากข้อมูลไบโอเมตริก (Biometric) เป็นข้อมูลเกี่ยวกับร่างกายของมนุษย์ทำให้สามารถเก็บรวบรวมได้ง่าย ยากที่เจ้าของข้อมูลไบโอเมตริก (Biometric) จะระมัดระวังตัวได้ อาทิ การเก็บท่าทางการเดินจากกล้องถ่ายรูปหรือกล้องวงจรปิด การเก็บตัวอย่างเสียงจากเครื่องบันทึกเสียง หรือแม้กระทั่งการเก็บตัวอย่างลายพิมพ์นิ้วมือจากสิ่งของที่เจ้าของไบโอเมตริก (Biometric) จับต้อง เป็นต้น และเมื่อความนิยมในการนำข้อมูล Biometric มาใช้ในการยืนยันตัวบุคคลมาขึ้น ทำให้บุคคลที่มีข้อมูลไบโอเมตริก (Biometric) ของผู้อื่นสามารถที่จะนำมาใช้เพื่อแสดงตนเป็นเจ้าของข้อมูล Biometric ได้ นอกจากนี้ข้อมูลไบโอเมตริก (Biometric) ยังสามารถบอกถึงสภาพของเจ้าของข้อมูลส่วนบุคคลได้ เช่น ดวงตาสามารถบอกถึงโรคประจำตัวของเจ้าของข้อมูลไบโอ

เมตริก (Biometric) ได้ ดังนั้นจากสาเหตุที่กล่าวมาจึงเห็นได้ว่าข้อมูล Biometric เป็นข้อมูลที่อ่อนไหวสามารถนำมาละเมิดความเป็นส่วนตัวของเจ้าของข้อมูลได้ทุกเมื่อ

5) การโอนข้อมูลส่วนบุคคล

เนื่องจากผู้เก็บรวบรวมข้อมูลส่วนบุคคลนิยมเก็บข้อมูลในรูปแบบอิเล็กทรอนิกส์ จึงทำให้ข้อมูลเหล่านี้สามารถถ่ายโอนกันได้ ซึ่งหากกำหนดให้มีการโอนข้อมูลส่วนบุคคลระหว่างผู้ประกอบการได้ย่อมทำให้ผู้ประกอบการเร่งพัฒนาตนเองเสนอสินค้าที่คุณภาพสูงสุดเพื่อมิให้ผู้บริโภคเปลี่ยนผู้ให้บริการ และเพื่อให้เจ้าของข้อมูลส่วนบุคคลของตนสามารถเข้าถึงข้อมูลการบริโภคของตนเองได้เพื่อทำการวิเคราะห์และคัดสรรสิ่งที่ดีที่สุดสำหรับตน ความคิดในการโอนข้อมูลส่วนบุคคลจึงเกิดขึ้นมาเพื่อให้ผู้บริโภคสามารถขอให้ผู้ควบคุมข้อมูลส่วนบุคคลโอนข้อมูลที่อยู่ในความครอบครองไปยังผู้ให้บริการอื่น

ในด้านของกฎหมายประเทศต่างๆแม้จะยังมิได้ให้ความคุ้มครองแก่เทคโนโลยีที่กล่าวมาอย่างครบถ้วน เนื่องจากเป็นเทคโนโลยีพัฒนาขึ้นมาเป็นเวลาไม่นานนัก ประเทศส่วนใหญ่มักอาศัยการตีความกฎหมายคุ้มครองข้อมูลส่วนบุคคลให้ครอบคลุมต่อการใช้เทคโนโลยีดังกล่าวให้มากที่สุดเท่าที่จะทำได้ อย่างไรก็ตามในสหภาพยุโรปและประเทศสหรัฐอเมริกามีพัฒนาที่สำคัญเกี่ยวกับเทคโนโลยีเหล่านี้ โดยประเทศสหรัฐอเมริกาแม้ยังมิได้มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลใช้บังคับเป็นการทั่วไป ทำให้ในหลายๆครั้งผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้โดยไม่ต้องปฏิบัติตามกฎหมายใดๆ อย่างไรก็ตามผู้ควบคุมข้อมูลส่วนบุคคลอาจตกอยู่ภายใต้กฎหมายของมลรัฐหรือกฎหมายพิเศษได้ เช่น Health Insurance Portability and Accountability Act of 1996 หรือ The Financial Services Modernization Act of 1999 เป็นต้น แต่ถึงแม้ประเทศสหรัฐอเมริกาจะยังมิได้มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลใช้บังคับเป็นการทั่วไปแต่ก็ได้ตระหนักถึงความสำคัญของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งเมื่อเป็นการกระทำผ่านทางอิเล็กทรอนิกส์ จึงได้มีการพยายามผลักดันกฎหมายสองฉบับ คือ Consumer Privacy Bill of Right และ Do Not Track Me Online ซึ่งมีบทบัญญัติเกี่ยวกับการควบคุมการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและป้องกันมิให้บุคคลถูกติดตามโดยอาศัยเครื่องมือทางอิเล็กทรอนิกส์ พร้อมทั้งยังมีโครงการ Smart Disclosure เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึงข้อมูลส่วนบุคคลของตนเองได้

ในด้านของสหภาพยุโรปในปัจจุบันการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคลเป็นไปตาม Directive 95/46/EC กล่าวคือผู้ควบคุมข้อมูลส่วนบุคคลต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ซึ่งต้องมีการแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลก่อนมีการเก็บรวบรวม ใช้ หรือ

เปิดเผยข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลในขณะทำการเก็บรวบรวมด้วย หากผู้ควบคุมข้อมูลส่วนบุคคลเปลี่ยนวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลหรือประสงค์นำข้อมูลส่วนบุคคลไปใช้โดยประการอื่นนอกจากที่ได้แจ้งไว้ ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลด้วย อย่างไรก็ตาม Directive 95/46/EC มีผลใช้บังคับมาเป็นเวลานานพอสมควรแล้วจึงไม่สามารถครอบคลุมเทคโนโลยีที่ถูกพัฒนาขึ้นใหม่ได้ เหตุนี้สหภาพยุโรปจึงมีการปรับปรุงแก้ไขกฎเกณฑ์ดังกล่าวโดยจะนำ General Data Protection Regulation (GDPR) มาใช้บังคับแทน โดย GDPR ดังกล่าวยังคงหลักการคุ้มครองตาม Directive 95/46/EC ไว้ และเพิ่มความคุ้มครองแก่เทคโนโลยีใหม่ๆพร้อมทั้งเพิ่มหลักเกณฑ์ความคุ้มครองเดิมให้เข้มงวดขึ้น กล่าวคือ GDPR เพิ่มความคุ้มครองแก่ข้อมูล Pseudonymous ให้เป็นข้อมูลส่วนบุคคล นอกจากนี้ยังคุ้มครองเจ้าของขอมูล Pseudonymous เมื่อมีบุคคลสามารถเชื่อมโยงไปยังเจ้าของข้อมูลส่วนบุคคลได้ GDPR มีบทบัญญัติคุ้มครองเจ้าของข้อมูลส่วนบุคคลจากการทำ Profiling และการตัดสินใจโดยระบบอัตโนมัติ โดยให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านได้ และหากมีการทำโดยอาศัยเทคโนโลยีทั้งสองดังกล่าว เจ้าของข้อมูลส่วนบุคคลมีสิทธิให้ความเห็นหรือคัดค้านได้ ในกรณีของข้อมูลไบโอเมตริก (Biometric) GDPR ได้ให้ความคุ้มครองโดยถือเป็นข้อมูลที่มีความอ่อนไหว และในกรณีของข้อมูล Mac Address และ IP Address มีการตีความให้ถือเป็นข้อมูลส่วนบุคคล นอกจากความคุ้มครองที่กล่าวมา GDPR ยังเพิ่มสิทธิแก่เจ้าของข้อมูลส่วนบุคคลอีกหลายประการ เช่น สิทธิในการยับยั้งการประมวลผลข้อมูลส่วนบุคคล สิทธิในการขอให้ลบเจ้าของข้อมูลส่วนบุคคล สิทธิในการโอนข้อมูลส่วนบุคคล(Right to data portability) หรือสิทธิในการเพิกถอนความยินยอม เป็นต้น

สำหรับกฎหมายของประเทศอังกฤษ กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้บัญญัติขึ้นเพื่ออนุวัติการให้เป็นไปตาม Directive 95/46/EC ดังนั้นกฎหมายของประเทศอังกฤษจึงให้ความคุ้มครองแก่เจ้าของข้อมูลส่วนบุคคลเช่นเดียวกันกับ Directive 95/46/EC สำหรับเทคโนโลยีต่างๆที่มีการพัฒนาขึ้นในช่วงเวลาไม่นานมานี้ ประเทศอังกฤษจึงยังมิได้มีกฎหมายที่ครอบคลุมเทคโนโลยีเหล่านี้ทำให้ต้องอาศัยการตีความกฎหมายเพื่อให้ครอบคลุมเทคโนโลยีในปัจจุบัน กล่าวคือ ข้อมูล Mac Address และ IP Address จะถือเป็นข้อมูลส่วนบุคคลต่อเมื่อสามารถเชื่อมโยงไปยังเจ้าของข้อมูลส่วนบุคคลได้ ข้อมูล Pseudonymous ถือเป็นข้อมูลที่สามารถเชื่อมโยงไปยังเจ้าของข้อมูลส่วนส่วนบุคคลจึงเป็นข้อมูลส่วนบุคคลเช่นเดียวกัน ในกรณีของการทำ Profiling ถือเป็นการเก็บรวบรวมข้อมูลส่วนบุคคลทำให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล แต่สำหรับข้อมูลไบโอเมตริก (Biometric) ประเทศอังกฤษยังถือเป็นข้อมูลส่วนบุคคลเท่านั้นมิได้ถือเป็น

ข้อมูลที่มีความอ่อนไหว นอกจากนี้ประเทศอังกฤษยังมีโครงการ MiData เพื่อให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลสามารถใช้ข้อมูลการบริโภคของตนวิเคราะห์และปรับปรุงการบริโภคของตนเองได้

ประเทศแคนาดามีกฎหมายคุ้มครองข้อมูลส่วนบุคคลคือ The Personal Information Protection and Electronic Document Act (PIPEDA) มีหลักการคุ้มครองข้อมูลส่วนบุคคล คือ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล โดยต้องมีการแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลในขณะทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลด้วย การนำข้อมูลส่วนบุคคลไปใช้ต้องเป็นไปตามวัตถุประสงค์ที่ได้แจ้งไว้ หากประสงค์นำข้อมูลส่วนบุคคลไปใช้โดยประการอื่นนอกจากวัตถุประสงค์ทีได้แจ้งไว้ หรือมีการเปลี่ยนแปลงวัตถุประสงค์ ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล สำหรับเทคโนโลยีในปัจจุบัน PIPEDA ยังมิได้มีบทบัญญัติครอบคลุมถึงเทคโนโลยีดังกล่าวจึงต้องอาศัยการตีความ PIPEDA เพื่อคุ้มครองความเป็นส่วนตัวของประชาชนจากเทคโนโลยีเหล่านี้

นอกจากประเทศต่างๆที่กล่าวมาแล้วกฎหมายของอีกประเทศหนึ่งที่น่านำมาพิจารณาคือประเทศสิงคโปร์ซึ่งเป็นประเทศเพื่อบ้านของไทย สำหรับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสิงคโปร์คือ Personal Data Protection Act ซึ่งมีผลบังคับใช้มาไม่นานนักโดยกำหนดให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในขณะทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยสำหรับเทคโนโลยีทางอิเล็กทรอนิกส์กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสิงคโปร์ยังมิได้ครอบคลุมไปถึง จึงทำให้ต้องอาศัยการตีความกฎหมายเพื่อให้ครอบคลุมเทคโนโลยีดังกล่าว

สำหรับประเทศไทยมีร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ซึ่งให้ความคุ้มครองแก่ข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลในการเพิกถอนความยินยอม สิทธิในการขอเข้าถึงข้อมูลส่วนบุคคลของตนและมีสิทธิขอแก้ไขข้อมูลของตนที่ไม่ถูกต้องได้ นอกจากนี้ยังกำหนดหน้าที่แก่ผู้ควบคุมข้อมูลส่วนบุคคลไว้หลายประการ เช่น ต้องทำให้ข้อมูลส่วนบุคคลนั้นถูกต้อง เป็นปัจจุบัน และไม่ก่อให้เกิดความเข้าใจผิด ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการในการรักษาความปลอดภัยข้อมูลส่วนบุคคล และต้องแจ้งแก่เจ้าของข้อมูลส่วนบุคคลเมื่อมีละเมิดข้อมูลส่วนบุคคล อย่างไรก็ตามแม้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ของไทยจะมีหลักเกณฑ์ที่สามารถให้ความคุ้มครองเจ้าของข้อมูลส่วนบุคคลได้ดี แต่ก็ยังปรากฏข้อบกพร่องบางประการ เช่น ยังไม่ครอบคลุมถึงผู้เก็บรวบรวมข้อมูลส่วนบุคคลที่ตั้งอยู่ใน

ต่างประเทศ ยังมิได้กำหนดหน้าที่แก่ผู้ควบคุมข้อมูลส่วนบุคคลในการแจ้งผู้ควบคุมข้อมูลส่วนบุคคลอื่นถึงการแก้ไขข้อมูลส่วนบุคคล และยังมิได้ครอบคลุมเทคโนโลยีที่นำมาใช้ในทางอิเล็กทรอนิกส์ในปัจจุบัน เป็นต้น ซึ่งหากประเทศไทยมีการกำหนดบทบัญญัติของกฎหมายให้ครอบคลุมในส่วนที่ยังบกพร่องอยู่ย่อมก่อให้ประชาชนได้รับการคุ้มครองความเป็นส่วนตัวที่ดีเยี่ยมและเป็นการส่งเสริมการค้า โดยเฉพาะอย่างยิ่งพาณิชย์อิเล็กทรอนิกส์ อีกด้วย

5.2 ข้อเสนอแนะ

เมื่อพิจารณาร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย พ.ศ. .... แล้วจะเห็นได้ว่ายังคงมีข้อบกพร่องบางประการและไม่สอดรับกับเทคโนโลยีที่ถูกพัฒนาขึ้นใหม่ ประเทศไทยควรพิจารณาให้ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลครอบคลุมในเรื่องดังกล่าวด้วย เนื่องจากนอกจากจะเป็นการให้ความคุ้มครองแก่ประชาชนแล้ว ยังเป็นการส่งเสริมการค้าระหว่างประเทศ ซึ่งจากที่ได้ศึกษามามีข้อเสนอแนะดังต่อไปนี้

1) ความหมายของข้อมูลส่วนบุคคลควรให้ความคุ้มครองแก่ชื่อของปัจเจกบุคคลซึ่งมิได้ใช้ในการติดต่อทางธุรกิจด้วย โดยแยกชื่อซึ่งใช้ในการติดต่อทางธุรกิจออกจากชื่อปัจเจกบุคคลดังกล่าวเพื่อมิให้เกิดอุปสรรคต่อการทำธุรกิจของประเทศไทย

2) ควรกำหนดให้ร่างพระราชบัญญัติดังกล่าวใช้บังคับกับผู้ควบคุมข้อมูลส่วนบุคคลซึ่งตั้งอยู่ในต่างประเทศเนื่องจากหากผู้ควบคุมข้อมูลส่วนบุคคลมิได้ตั้งอยู่ในประเทศไทยแต่มีการเสนอขายสินค้าหรือบริการในประเทศไทย อาจทำให้ประชาชนไทยไม่ได้รับความคุ้มครองความเป็นส่วนตัวอย่างเต็มที่โดยเฉพาะอย่างยิ่งในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลตั้งอยู่ในประเทศที่ไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลหรือมีหลักเกณฑ์ของกฎหมายดังกล่าวต่ำกว่าหลักเกณฑ์ของประเทศไทย จึงสมควรกำหนดให้บุคคลซึ่งอยู่ในต่างประเทศแต่ได้ใช้ข้อมูลส่วนบุคคลของประชาชนชาวไทย หรือเสนอขายสินค้าหรือบริการแก่ประชาชนชาวไทยไม่ว่าจะเสียค่าบริการหรือไม่ก็ตามต้องปฏิบัติตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ดังกล่าวและแต่งตั้งผู้แทนในประเทศไทยเพื่อให้มั่นใจว่าบุคคลดังกล่าวได้ปฏิบัติตามร่างพระราชบัญญัตินี้

3) การให้ความยินยอมต้องทำเป็นหนังสืออาจไม่สอดคล้องกับความเป็นจริงโดยเฉพาะอย่างยิ่งในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลเก็บข้อมูลโดยการสอบถามหรือผู้ควบคุมข้อมูลส่วนบุคคลประสงค์เก็บรวบรวมข้อมูลเพื่อประโยชน์ทางการค้าของตนเท่านั้น หากต้องให้เจ้าของข้อมูลส่วนบุคคลลงลายมือชื่อยินยอมเป็นหนังสือย่อมมีโอกาสที่เจ้าของข้อมูลส่วนบุคคลปฏิเสธไม่ทำเป็นหนังสือและส่งผลต่อการพัฒนาสินค้าของบริการหรือการค้าของประเทศได้ดังนั้นจึงไม่ควรกำหนดให้การให้

ความยินยอมต้องทำเป็นหนังสือ อย่างไรก็ตามในกรณีข้อมูลซึ่งมีความสำคัญมีโอกาสถูกนำไปใช้ในทางที่ก่อให้เกิดผลร้ายแก่เจ้าของข้อมูลส่วนบุคคลได้ เช่น เลขบัตรประจำตัวประชาชน เป็นต้น ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลอาจกำหนดให้การเก็บรวบรวมข้อมูลเหล่านี้ต้องทำเป็นหนังสือ และกำหนดให้หากการขอความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลมีเรื่องอื่นๆประกอบอยู่ด้วย ผู้ควบคุมข้อมูลส่วนบุคคลต้องแยกส่วนที่เป็นเรื่องเกี่ยวกับข้อมูลส่วนบุคคลออกต่างหากจากเรื่องอื่นๆ

4) การเพิกถอนความยินยอมไม่ควรจำกัดไว้ที่สัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล เนื่องจากจะเป็นการเปิดโอกาสแก่ผู้ควบคุมข้อมูลส่วนบุคคลที่มีอำนาจต่อรองสูงกว่าใช้ช่องว่านี้ห้ามมิให้เจ้าของข้อมูลส่วนบุคคลเพิกถอนความยินยมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

5) ควรกำหนดกรอบระยะเวลาเบื้องต้นในการเก็บรักษาข้อมูลส่วนบุคคลโดยเมื่อพิจารณาร่างพระราชบัญญัติดังกล่าวซึ่งกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องลบข้อมูลเมื่อพ้นระยะเวลาในการเก็บรักษาประกอบกับการที่ร่างพระราชบัญญัตินี้มิได้พูดถึงระยะเวลาที่ผู้ควบคุมข้อมูลส่วนบุคคลอาจเก็บรักษาข้อมูลไว้ได้ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้กำหนดระยะเวลาในการรักษาข้อมูลส่วนบุคคลได้เอง จึงอาจทำให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรักษาข้อมูลส่วนบุคคลไว้เกินกว่าที่จำเป็นเพื่อทำให้วัตถุประสงค์ที่รวบรวมมาสำเร็จได้

6) ในกรณีที่เจ้าของข้อมูลส่วนบุคคลขอใช้สิทธิในการขอแก้ไขข้อมูลส่วนบุคคลควรกำหนดหน้าที่แก่ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลอื่นทำการเปลี่ยนแปลงหรือแก้ไขข้อมูลส่วนบุคคลให้สมบูรณ์และถูกต้องในกรณีที่มีการเปิดเผยข้อมูลส่วนบุคคลแก่ผู้ควบคุมข้อมูลส่วนบุคคลอื่น

7) ควรกำหนดให้ชัดเจนว่า Mac Address และ IP Address เป็นข้อมูลส่วนบุคคลที่ได้รับความคุ้มครองเช่นเดียวกับข้อมูลส่วนบุคคลอื่นๆเพื่อมิให้เกิดความคลุมเครือและต้องมีการตีความว่าข้อมูลส่วนบุคคลตามร่างพระราชบัญญัตินี้หมายรวมถึงข้อมูล Mac Address และ IP Address หรือไม่

8) ควรกำหนดให้ความคุ้มรองแก่ข้อมูล Pseudonymous ให้เป็นข้อมูลส่วนบุคคลอย่างชัดแจ้งและกำหนดให้บุคคลซึ่งมีข้อมูลPseudonymous หรือ Anonymous หากมีการประมวลผลเพิ่มเติมเพื่อทราบเจ้าของข้อมูลส่วนบุคคลแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลนั้นต้องปฏิบัติตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ทั้งนี้ไม่ควรเปิดโอกาสให้มีการแปลงข้อมูลส่วนบุคคลให้อยู่ในรูปแบบข้อมูลที่ไม่สามารถรู้ตัวบุคคลผู้เป็นเจ้าของข้อมูลส่วนบุคคลได้

9) ควรกำหนดให้ความคุ้มครองประชาชนจากกการทำ Profiling และการตัดสินใจโดยระบบอัตโนมัติโดยกำหนดให้สิทธิในการคัดค้านการทำProfiling และการตัดสินใจโดยระบบอัตโนมัติหากต้องมีการกระทำดังกล่าวต้องให้ปัจเจกบุคคลมีส่วนร่วมในกระบวนการนั้นด้วย และกำหนดให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลในการคัดค้านผลลัพธ์ที่เกิดจากการทำProfiling และการตัดสินใจโดยระบบอัตโนมัติ เนื่องจากProfiling และการตัดสินใจโดยระบบอัตโนมัติทำให้บุคคลสูญเสียความเป็นส่วนตัวเพราะการเฝ้ามองพฤติกรรมคลอดเวลาและถูกตัดสินใจโดยเครื่องซึ่งอาจให้ผลลัพธ์ที่ไม่ถูกต้องได้

10) ควรกำหนดให้ข้อมูลไบโอเมตริก (Biometric)เป็นข้อมูลที่มีความอ่อนไหว เนื่องจากถูกเก็บรวบรวมได้ง่าย และมีความสำคัญมากขึ้นในการนำมาใช้ในการยืนยันตัวบุคคล นอกจากนี้ข้อมูลไบโอเมตริก (Biometric) ยังสามารถแสดงสภาพของเจ้าของข้อมูลส่วนบุคคลได้ เช่น โรคประจำตัว หรืออาชีพ เป็นต้น

11) ควรให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลในการโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นได้ เนื่องจากในปัจจุบันผู้เก็บรวบรวมข้อมูลส่วนบุคคลส่วนใหญ่มักเก็บรวบรวมข้อมูลไว้ในรูปแบบอิเล็กทรอนิกส์ทำให้การโอนข้อมูลทำได้ง่ายขึ้น และเป็นการส่งเสริมการแข่งขันทางการค้าทำให้ผู้ประกอบการต้องพยายามพัฒนาสินค้าหรือบริการของตนเพื่อดึงดูดผู้บริโภคมิให้ย้ายไปใช้บริการของผู้ประกอบการรายอื่น

บรรณานุกรม

หนังสือและวารสาร

เกรียงไกร เจริญธนาวัฒน์. หลักกฎหมายว่าด้วยสิทธิเสรีภาพ. กรุงเทพมหานคร : วิญญูชน, 2547.

จรัญ โฆษณานันท์. สิทธิมนุษยชนไร้พรมแดน. กรุงเทพมหานคร: วิญญูชน, 2556.

ไพจิตร สวัสดิสาร. การใช้คอมพิวเตอร์ทางกฎหมายและกฎหมายที่เกี่ยวกับคอมพิวเตอร์. พิมพ์ครั้งที่ 4, กรุงเทพมหานคร: บริษัท ชวนพิมพ์ 50 จำกัด, 2550.

บุญเพราะ แสงเทียน. กฎหมายอาญา 3 ภาคความผิดและภาคลหุโทษแนวประยุกต์. กรุงเทพมหานคร : วิญญูชน, 2551.

ปทีป เมธคุณวุฒิ, อภิรัตน์ เพ็ชรศิริ. การวิจัยเรื่องแนวทางในการออกกฎหมายคุ้มครองข้อมูลและสารสนเทศส่วนบุคคลในประเทศไทย, สำนักคณะกรรมการการวิจัยแห่งชาติ, 2539.

ศนันกรณ์ (จำปี) โสตถิพันธุ์. คำอธิบายนิติกรรมสัญญา. พิมพ์ครั้งที่ 13. กรุงเทพมหานคร : วิญญูชน, 2551

วิทยานิพนธ์

กิตติพงศ์ กมลธรรมวงศ์, “การคุ้มครองข้อมูลข่าวสารส่วนบุคคลในระบบกฎหมายไทย : ปัญหาและแนวทางการแก้ไข”. วิทยานิพนธ์ปริญญามหาบัณฑิต, คณะนิติศาสตร์, มหาวิทยาลัยธรรมศาสตร์, 2549.

ปกรณ์ มงคลประสิทธิ์, “การคุ้มครองความปลอดภัยของข้อมูลส่วนบุคคลในการดำเนินธุรกรรมทางอิเล็กทรอนิกส์ : กรณีศึกษาตามร่างพระราชบัญญัติข้อมูลส่วนบุคคล”, นิติศาสตรมหาบัณฑิต , มหาวิทยาลัยรามคำแหง, 2551

นรินทร์ จุ่มศรี, “มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลจากการใช้บริการเครือข่ายสังคมออนไลน์”, วิทยานิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยธุรกิจบัณฑิตย์, 2555.

สมชัย สิริวัฒนวงศ์ชัย, “การสร้างโมเดลคำหลักแบบอัตโนมัติ สำหรับระบบค้นหาคำหลักจากเสียงพูดแบหลายโดเมน”, วิทยานิพนธ์ วิทยาศาสตรมหาบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์ ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยธรรมศาสตร์ 2549.

เอกรินทร์ ซื่อธานุวงศ์, “ระบบตรวจสอบลายนิ้วมือฝังตัว”, วิทยานิพนธ์วิศวกรรมศาสตรมหาบัณฑิต สาขาวิศวกรรมคอมพิวเตอร์, มหาวิทยาลัยสงขลานครินทร์, 2548.

บทความ

ชั่งทอง โอภาสศิริวิทย์. “ความคุ้มครองข้อมูลส่วนบุคคลและความเป็นส่วนตัวในประเทศไทย : ปัจจุบันและอนาคต.” วารสารนิติศาสตร์มหาวิทยาลัยธรรมศาสตร์ (613). เล่มที่ 4 ปีที่ 34. (2547).

จันจิรา เอี่ยมมยุรา. “การคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย.” วารสารนิติศาสตร์มหาวิทยาลัยธรรมศาสตร์ (627). เล่มที่ 4 ปีที่ 34. (2547).

_____ “แนวคิดและหลักการยกร่างกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย.” วารสารนิติศาสตร์มหาวิทยาลัยธรรมศาสตร์ (653). เล่มที่ 4, ปีที่ 34. (2547).

เพชรรัตน์ จงปัญญาประพันธ์. “ความสำคัญของกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล.” วารสารนิติศาสตร์มหาวิทยาลัยธรรมศาสตร์ (821). เล่มที่ 4. ปีที่ 33. (2546).

Books

Koops, B., Lips, M., Prins, C., Schellekens, M.. Starting Points for ICT Regulation. T·M·C Asser Press, 2006.

Christoffel, T., Teret, P.S.. Protecting the public. New York: Oxford University Press, 1993.

Clark, Martin P.. Data network, IP and the Internet : protocols, design and operation. Chichester : John Willey and sons, 2003.

Henderson, H.. Privacy in the information age. New York: Facts on file, 1999.

Hill, G.D.. Data protection : governance, risk management, and compliance. Florida: CRC Press, 2009.

Schumann, W. D. , Thorson, E. Internet Advertising. London: Lawrence Erlbaum associates, 2007.

Kozyris, J.P.. Regulating Internet Abuses Invasion of Privacy. Kluwe Law International.

เอกสารอิเล็กทรอนิกส์

กรมวิชาการเกษตร, “ระเบียบสุขอนามัยพืชของสหภาพยุโรป ระเบียบว่าด้วยมาตรการป้องกันการนำสิ่งมีชีวิตที่เป็นอันตรายต่อพืชและผลิตภัณฑ์จากพืชเข้าสู่ประชาคมและมาตรการป้องกันการแพร่ระบาดของสิ่งมีชีวิตที่เป็นอันตรายภายในประชาคม (Council Directive

2002/29/EC)",http://www.doa.go.th/psco/images/EU/translation.complete_regulation.pdf, 14 มีนาคม 2559

กองส่งเสริมสิทธิและเสรีภาพ กรมคุ้มครองสิทธิและเสรีภาพ กระทรวงยุติธรรม, "ชุดความรู้สิทธิมนุษยชน สิทธิและเสรีภาพตามรัฐธรรมนูญ สนธิสัญญาหลักระหว่างประเทศด้านสิทธิมนุษยชนที่ประเทศไทยเป็นภาคี". www.rlpd.go.th/rlpdnew/images/rlpd_1/HRC/nhr.pdf

เครือข่ายพลเมืองเน็ต, "การละเมิดความเป็นส่วนตัวออนไลน์ในสังคมไทย พ.ศ.2556", httpswww.google.co.thurlsa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact= 8 &ved= 0 CB4 QFjAA&url= https% 3 A% 2 F% 2 Fthainetizen. org% 2 Fwp-content% 2 Fuploads% 2 F2 0 1 4 % 2 F0 3 % 2 Fthainetizen- privacy- report-2013.pdf&ei=rC5vVafeEo_buQSXsIL4Bw&usg=AFQjCNE

นาวิก นำเสียง. (2549). "ความเป็นส่วนตัวบนโลกอินเตอร์เน็ต", http://www.crminaction.com/article/7/42/%E0%B8%84%E0%B8%A7%E0%B8%B2%E0%B8%A1%E0%B9%80%E0%B8%9B%E0%B9%87%E0%B8%99%E0%B8%AA%E0%B9%88%E0%B8%A7%E0%B8%99%E0%B8%95%E0%B8%B1%E0%B8%A7%E0%B8%9A%E0%B8%99%E0%B9%82%E0%B8%A5%E0%B8%81%E0%B8%AD%E0%B8%B4%E0%B8%99%E0%B9%80%E0%B8%95%E0%B8%AD%E0%B8%A3%E0%B9%8C%E0%B9%80%E0%B8%99%E0%B9%87%E0%B8%95.html.

รองศาสตราจารย์ ดร. เกรียงไกร เจริญธนาวัฒน์, "สิทธิของผู้เล่นเกมส์ออนไลน์", http://www.pub-law.net/publaw/view.aspx?ID=609

องค์การรักษาความปลอดภัยฝ่ายพลเรือน, "ความรู้ทั่วไปเกี่ยวกับลายนิ้วมือ ฝ่ามือ ฝ่าเท้า", http://www.secnia.go.th/2016/01/18/38500/,18 มกราคม 2559

Fingtrack, "การรู้จำลายนิ้วมือ",http://fingerscan.in.th/fingerprint-scanner/83-fingerprintrecognition, 17 มกราคม 2559

Media Electronics

Aricle 29 Data Protection Working Party, "Opinion 4/2007 on the concept of personal data",

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf, 1 February 2016

Babich, A., “Biometric Authentication. Types of biometric identifiers, Bachelor’s Thesis, Degree Programme in Business Information Technology 2012”, https://www.google.co.th/url?sa=t&rct=j&q=&esrc=s&source=web&cd=11&cad=rja&uact=8&ved=0ahUKEwj7r5mt_ODKAhXCA44KHYu3CLcQFghQMAo&url=https%3A%2F%2Fwww.theseus.fi%2Fxmlui%2Fbitstream%2Fhandle%2F10024%2F44684%2FBabich_Aleksandra.pdf%3Fsequence%3D1&usg=AFQjCNF9vP2JZkYFP5DcRRPy_rgZD9RRZg&bvm=bv.113370389,d.c2E, 17 January 2016

Bapat, A., “The new right to data portability”, Pdpjournal, Voulme 13, issue 3,https://www.google.co.th/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwj4-uCG-e7KAhXEA44KHcTjBNUQFggfMAE&url=https%3A%2F%2Fwww.hunton.com%2Ffiles%2FPublication%2Fc924a1bc-b27e-420f-ada4-6635d6c9ab4a%2FPresentation%2FPublicationAttachment%2Fd4ce9cda-8229-4778-bdf3-73eb9a9c3f70%2FThe_new_right_to_data_portability_Bapat.pdf&usg=AFQjCNEN5_bpbZXWc1wNsGYw_FGUK7q7dg&bvm=bv.113943164,d.c2E, 10 February 2016.

Blumberg, A., &Eckersley, P., “On location privacy, and how to avoid losing it forever”, https://www.eff.org/wp/locational-privacy, 17January 2016

Cabinet office behavioural insights team, “Midata 2012 review and consultation”, https://www.google.co.th/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwjsgsO0qe_KAhWJj44KHZfYB4IQFgghMAE&url=https%3A%2F%2Fwww.gov.uk%2Fgovernment%2Fuploads%2Fsystem%2Fuploads%2Fattachment_data%2Ffile%2F32687%2F12-943-midata-2012-review-and-consultation.pdf&usg=AFQjCNFQEkVe50zJbgbO_swGMN52wnfjLg, 19 มกราคม 2559

Data protection in United States, Practical law.,http://uk.practicallaw.com/6-502-0467**,** 19 January 2016

DLA PIPER, Data Protection laws of the world., http://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw/functions/export.pdf?country=all, 19 January 2016.

Duhigg, G., “How companies learn your secrets”, http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all&_r=0, 20 January 2016

EDRi, An introduction to data protection., https://edri.org/files/paper06_datap.pdf, 20 January 2016

ENISA, Privacy Considerations of Online Behavioural Tracking., www.enisa.europa.eu%2Factivities%2Fidentity-andtrust%2Flibrary%2Fdeliverables%2Fprivacy-considerations-of-online-behavioural-tracking&ei=XDlvVZKQOZHguQT3xoDgAQ&usg=AFQjCNF-7Jw2i8Kcf_hiGFkZr0OTdm2vzg&sig2=jjtbDWM_l-JPlK9eJUw0dA&bvm=bv.94911696,d.c2E, 20 January 2016

European commission, “legislation”, http://ec.europa.eu/legislation/index_en.htm, 14 March 2016

Federal Bureau of Investigation, “Hand Geometry”, https://www.google.co.th/url?sa=t&rct=j&q=&esrc=s&source=web&cd=9&cad=rja&uact=8&ved=0ahUKEwiY94biqejKAhUGGY4KHYprD9gQFgg_MAg&url=https%3A%2F%2Fwww.fbi.gov%2Fabout-us%2Fcjis%2Ffingerprints_biometrics%2Fbiometric-center-of-excellence%2Ffiles%2Fhand-geometry.pdf%2Fat_download%2Ffile&usg=AFQjCNH1Yh_pLokt1wGyXfCS7Sc47xaCfg&bvm=bv.113370389,d.c2E, 18 January 2016

Federal Trade Commission, “Do Not Track”, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/do-not-track, 25 January 2016

Felten, E., “Are pseudonymous “anonymous”?”, https://www.ftc.gov/news-events/blogs/techftc/2012/04/are-pseudonyms-anonymous, 25 January 2016.

Grafe, I., “Data portability series: At the crossroads of data protection & competition policy”, blogs.lse.ac.uk/mediapolicyproject/2014/04/11/data-portability-series-at-the-crossroads-of-protection-and-competition-policy/, 20 January 2016

Howard, A., “What is smart disclosure?”, http://radar.oreilly.com/2012/04/what-is-smart-disclosure.html, 19 January 2016.

ICO, “The guide to data protection”,https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/, 19 January 2016

ICO, “The guidance on the rules on use of cookies and similar technologies”,https://ico.org.uk/media/for…/1545/cookies_guidance.pdf, 19 January 2016.

Information Commissioner’s Office, “Data Protection Good Practice Note”,https://www.google.co.th/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwijof62nMfLAhXGCI4KHWLFDpkQFggaMAA&url=http%3A%2F%2Fec.europa.eu%2Fjustice%2Fdata-protection%2Fdocument%2Fnational-policy%2Ffiles%2Fuk_outsourcing_guide_for_small_and_medium_businesses_en.pdf&usg=AFQjCNFGJxwa1b7lbKIkK1hSC70DfpUYzg&sig2=hqxOvbSdPsJehvRUUt0cbQ, 9 February 2016.

Information Commissioner’s Office, “Direct Marketing Data protection Act Privacy and Electronic Communications Regulations”, https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf, 9 February 2016.

Lee, J., “3 Ways JavaScript Can Breach Your Privacy&Security”, https://www.google.co.th/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwi-uqL8vt7KAhXOv44KHYLdDSIQFggdMAA&url=http%3A%2F%2Fwww.makeuseof.com%2Ftag%2F3-ways-javascript-can-used-breach-privacy-security%2F&usg=AFQjCNFn_PZA3NV4m5reg8sRXJyBMJ9K1A&bvm=bv.113370389,d.c2E,17 January 2016.

Lee, J. “4 Seemingly Innocent Online Activities That Track Your Behavior”, https://www.google.co.th/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjtksHpvt7KAhUBjo4KHeYVDsYQFggbMAA&url=http%3A%2F%2Fwww.makeuseof.com%2Ftag%2F4-seemingly-innocent-online-

activities-track-behavior%2F&usg=AFQjCNF72TlumPkMvSjr1MfTWOgLd2hZXw, 17 January 2016

Lubin, G., “The incredible story of how target exposed a teen girl’s pregnancy”, http://www.businessinsider.com/the-incredible-story-of-how-target-exposed-a-teen-girls-pregnancy-2012-2,20 January 2016

Machanavajjhala, A., Kifer, D., Gehrke, J., Venkitasubramaniam, M., “l-Diversity: Privacy Beyond K-Anonymity, ACM Transactions on Knowledge Discovery from Data”, https://www.google.co.th/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwiaw9PJsuXLAhVOWI4KHQGdAmoQFggmMAE&url=https%3A%2F%2Fwww.trustst c.org%2Fpubs%2F465%2FL%2520Diversity%2520Privacy.pdf&usg=AFQjCNHdEQaN68mCp2zbWJk_lA8sbJnvKQ&sig2=Wf1miHJqXCKbbRJRa6wsFw&bvm=bv.117868183,d.c2E, 1 February 2016.

Mesinfors, “The goal of the “Mesinfo” project”,http://mesinfos.fing.org/english/, 19 January 2016.

Nick Nikiforakis, “Browse Fingerprinting”, www.ieee-security.orgTCSP2014postersKIMDA.pdf, 15 February 2016

Office of the Privacy Commissioner of Canada, “Legal information related Personal PIPEDA”, https://www.priv.gc.ca/leg_c/p_principle_e.asp, 15 February 2016.

Office of the privacy commissioner of Canada, “What an IP Address can reveal about you”, https://www.priv.gc.ca/information/research-recherche/2013/ip_201305_e.pdf, 20 January 2016.

Office of the Privacy Comissioner of Canada, “Report of findings investigationinto personal information handling practives of WhatsApp Inc.”, https://www.google.co.th/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwj_g5_Ov-XLAhUUW44KHSFnAeAQFggdMAA&url=https%3A%2F%2Fautoriteitpersoonsgegevens.nl%2Fsites%2Fdefault%2Ffiles%2Fdownloads%2Frapporten%2Frap_2013-whatsapp-opc-final-report-of-findings.pdf&usg=AFQjCNH-Dp3xmYI3cQy7QSdJaUhEzFF5-w&sig2=DZx5ev-Fj7MjWJDyatB9fw&bvm=bv.117868183,d.c2E, 10 February 2016.

Office of the Privacy Comissioner of Canada, “Interpretation Bulletin”, https://www.priv.gc.ca/leg_c/interpretations_02_e.asp#fn50, 10 February 2016

Office of the Privacy Comissioner of Canada, “OPC Guidance Documents Data at your fingertips Biometrics and the challenges to privacy”, https://www.priv.gc.ca/information/pub/gd_bio_201102_e.asp, 10 February 2016.

Office of the Privacy Commissioner of Canada, “Repert on the 2010 office of the privacy commissioner of canada’s consultations on online tracking, profiling and targeting, and cloud computing”, https://www.priv.gc.ca/resource/consultations/report_201105_e.pdf, 10 February 2016

Personal Data Protection Commission Singapore, “factsheet”, https://www.pdpc.gov.sg/docs/default-source/public-consultation/factsheet-pdpc_public_consultation_(5feb2013).pdf?sfvrsn=2, 20 February 2016.

Skouma, G., Léonard, L., “Online Behavioral Tracking : What May Change After the Legal Regorm on Personal Data Protection”, https://www.google.co.th/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjP0q-rqd7KAhXPno4KHfd5CqcQFggeMAA&url=http%3A%2F%2Fwww.springer.com%2Fcda%2Fcontent%2Fdocument%2Fcda_downloaddocument%2F9789401793841-c2.pdf%3FSGWID%3D0-0-45-1491988-p176890444&usg=AFQjCNGcJdBgL96uo-2z2ILWGM01jOVUPQ, 17 January 2016

Swire, P., Lagos, Y., “Why the right to data portability likely reduces consumer welfare: antitrust and privacy critique, Maryland law review”,https://www.google.co.th/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwi55Or5r-_KAhWBCo4KHbISDdYQFggjMAE&url=http%3A%2F%2Fdigitalcommons.law.umaryland.edu%2Fcgi%2Fviewcontent.cgi%3Farticle%3D3550%26context%3Dmlr&usg=AFQjCNFkIw5MKgCSQHt5Re1HXLA9c5nObg&bvm=bv.113943164,d.c2E, 20 January 2016

Technology Analysis Branch of the Office Privacy Commissioner of Canada, “What an IP Address Can Reveal About You”, https://www.priv.gc.ca/information/research-recherche/2013/ip_201305_e.asp, 15 January 2016.

Thomas Schauf, “The Concept of Pseudonymous Data”,https://www.google.co.th/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0ahUKEwj7vrqfw8zKAhUEG44KHbEFAe0QFggyMAI&url=http%3A%2F%2Fwww.w3.org%2F2011%2Ftracking-protection%2Fmit%2Fbvdw_w3c_pseud-data_20130211.pptx.pdf&usg=AFQjCNHl0lMGNlZFd6BXou1Tj4C3imX5Ow, 15 January 2016.

United Nations Human Rights office of the High Commissioner for Human Rights, “What are human rights?”, http://www.ohchr.org/EN/Issues/Pages/WhatareHumanRights.aspx, 15 January 2016.

Zwipe, “Mastercard and Zwipe announce the launch of the world’s first biometric contactless payment card with integrated fingerprint sensor”, http://zwipe.com/news/mastercard-and-zwipe-announce-the-launch-of-the-worlds-first-biometric-contactless-payment-card-with-integrated-fingerprint-sensor/, 18 January 2016.

ภาคผนวก

ภาคผนวก ก
ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....

ร่างฯ ที่ สคก. ตรวจพิจารณาแล้ว
เรื่องเสร็จที่ ๑๑๓๕/๒๕๕๘

บันทึกหลักการและเหตุผล
ประกอบร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล
พ.ศ. ....

หลักการ

ให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

เหตุผล

เนื่องจากปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว สามารถทำได้โดยง่าย สะดวก และรวดเร็ว รวมทั้งก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวมที่ใช้เทคโนโลยีดิจิทัลอย่างแพร่หลาย แม้ว่าจะได้มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลในบางเรื่อง แต่ก็ยังไม่มีหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป สมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้น จึงจำเป็นต้องตราพระราชบัญญัตินี้

ร่าง
พระราชบัญญัติ
คุ้มครองข้อมูลส่วนบุคคล
พ.ศ. ....

.....
.....
.....

.....
.....

โดยที่เป็นการสมควรมีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

.....
.....

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า “พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....”

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งร้อยแปดสิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ในกรณีที่มีกฎหมายว่าด้วยการใดบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในลักษณะใด กิจการใด หรือหน่วยงานใดไว้โดยเฉพาะแล้ว ให้บังคับตามบทบัญญัติแห่งกฎหมายว่าด้วยการนั้น เว้นแต่

(๑) บทบัญญัติเกี่ยวกับการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคล และบทกำหนดโทษที่เกี่ยวข้อง ให้บังคับตามบทบัญญัติแห่งพระราชบัญญัตินี้เป็นการเพิ่มเติม ไม่ว่าจะซ้ำกับบทบัญญัติแห่งกฎหมายว่าด้วยการนั้นหรือไม่ก็ตาม

(๒) บทบัญญัติเกี่ยวกับการร้องเรียน บทบัญญัติที่ให้อำนาจแก่คณะกรรมการผู้เชี่ยวชาญออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคล และบทบัญญัติเกี่ยวกับอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ รวมทั้งบทกำหนดโทษที่เกี่ยวข้อง ให้บังคับตามบทบัญญัติแห่งพระราชบัญญัตินี้ในกรณีดังต่อไปนี้

(ก) ในกรณีที่กฎหมายว่าด้วยการนั้นไม่มีบทบัญญัติเกี่ยวกับการร้องเรียน

(ข) ในกรณีที่กฎหมายว่าด้วยการนั้นมีบทบัญญัติที่ให้อำนาจแก่เจ้าหน้าที่ผู้มีอำนาจพิจารณาเรื่องร้องเรียนตามกฎหมายดังกล่าวออกคำสั่งเพื่อคุ้มครองเจ้าของข้อมูลส่วนบุคคล แต่ไม่เพียงพอเท่ากับอำนาจของคณะกรรมการผู้เชี่ยวชาญตามพระราชบัญญัตินี้และเจ้าหน้าที่ผู้มี

อำนาจตามกฎหมายดังกล่าวร้องขอต่อคณะกรรมการผู้เชี่ยวชาญหรือเจ้าของข้อมูลส่วนบุคคล ผู้เสียหายยื่นคำร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญตามพระราชบัญญัตินี้ แล้วแต่กรณี

มาตรา ๔ พระราชบัญญัตินี้ไม่ใช้บังคับแก่

(๑) บุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตนของบุคคลนั้นเท่านั้น โดยมิให้ผู้อื่นใช้ข้อมูลส่วนบุคคลนั้น หรือเปิดเผยข้อมูลส่วนบุคคลนั้นต่อผู้อื่น

(๒) บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมไว้เฉพาะเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น

(๓) สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าว ซึ่งเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามอำนาจหน้าที่ของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมาธิการ แล้วแต่กรณี

(๔) การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

(๕) การดำเนินกิจการทางศาสนาขององค์การทางศาสนา

(๖) การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

การยกเว้นไม่ให้นำบทบัญญัติแห่งพระราชบัญญัตินี้ทั้งหมดหรือแต่บางส่วนมาใช้บังคับแก่ผู้ควบคุมข้อมูลส่วนบุคคลในลักษณะใด กิจการใด หรือหน่วยงานใดทำนองเดียวกับผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง หรือเพื่อประโยชน์สาธารณะอื่นใด ให้ตราเป็นพระราชกฤษฎีกา

มาตรา ๕ ในพระราชบัญญัตินี้

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงการระบุเฉพาะชื่อ ตำแหน่ง สถานที่ทำงาน หรือที่อยู่ทางธุรกิจ และข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“เจ้าของข้อมูลส่วนบุคคล” ให้หมายความรวมถึง

(๑) ผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์

(๒) ผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถ หรือ

(๓) ผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ

“บุคคล” หมายความว่า บุคคลธรรมดา

“คณะกรรมการ” หมายความว่า คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

“พนักงานเจ้าหน้าที่” หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

"เลขาธิการ" หมายความว่า เลขาธิการสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

"รัฐมนตรี" หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้

มาตรา ๖ ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรักษาการตามพระราชบัญญัตินี้ และให้มีอำนาจออกกฎกระทรวงเพื่อปฏิบัติการตามพระราชบัญญัตินี้

กฎกระทรวงนั้น เมื่อได้ประกาศในราชกิจจานุเบกษาแล้ว ให้ใช้บังคับได้

หมวด ๑
คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

มาตรา ๗ ให้มีคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ประกอบด้วย

(๑) ประธานกรรมการ ซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้มีความรู้ ความเชี่ยวชาญและประสบการณ์เป็นที่ประจักษ์ในด้านการคุ้มครองข้อมูลส่วนบุคคล ด้านการคุ้มครองผู้บริโภค ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านสังคมศาสตร์ ด้านกฎหมาย ด้านสุขภาพ หรือด้านอื่นที่เกี่ยวข้องและเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคล

(๒) กรรมการโดยตำแหน่ง จำนวนเจ็ดคน ได้แก่ ปลัดสำนักนายกรัฐมนตรี ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เลขาธิการคณะกรรมการคุ้มครองผู้บริโภค อธิบดีกรมคุ้มครองสิทธิและเสรีภาพ ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ผู้แทนสภาหอการค้าแห่งประเทศไทย และผู้แทนสมาคมธนาคารไทย

(๓) กรรมการผู้ทรงคุณวุฒิ จำนวนห้าคน ซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้มีความรู้ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์ในด้านการคุ้มครองข้อมูลส่วนบุคคล ด้านการคุ้มครองผู้บริโภค ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านสังคมศาสตร์ ด้านกฎหมาย ด้านสุขภาพ หรือด้านอื่นที่เกี่ยวข้องและเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคล

ให้เลขาธิการเป็นกรรมการและเลขานุการ และให้เลขาธิการแต่งตั้งเจ้าหน้าที่ของสำนักงานเป็นผู้ช่วยเลขานุการได้ไม่เกินสองคน

หลักเกณฑ์และวิธีการสรรหาบุคคลเพื่อแต่งตั้งเป็นประธานกรรมการและกรรมการผู้ทรงคุณวุฒิ รวมทั้งการสรรหากรรมการผู้ทรงคุณวุฒิเพื่อดำรงตำแหน่งแทนผู้ที่พ้นจากตำแหน่งก่อนวาระตามมาตรา ๑๐ ให้เป็นไปตามระเบียบที่รัฐมนตรีประกาศกำหนด

มาตรา ๘ ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิต้องมีคุณสมบัติและไม่มีลักษณะต้องห้าม ดังต่อไปนี้

(๑) มีสัญชาติไทย

(๒) ไม่เป็นบุคคลล้มละลายหรือเคยเป็นบุคคลล้มละลายทุจริต

(๓) ไม่เป็นคนไร้ความสามารถหรือคนเสมือนไร้ความสามารถ

(๔) ไม่เคยได้รับโทษจำคุกโดยคำพิพากษาถึงที่สุดให้จำคุก เว้นแต่เป็นโทษสำหรับความผิดที่ได้กระทำโดยประมาทหรือความผิดลหุโทษ

มาตรา ๙ ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิมีวาระการดำรงตำแหน่งคราวละสามปี

เมื่อครบกำหนดตามวาระในวรรคหนึ่ง หากยังมิได้มีการแต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิขึ้นใหม่ ให้ประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งตามวาระนั้นอยู่ในตำแหน่งเพื่อดำเนินงานต่อไปจนกว่าประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิซึ่งได้รับแต่งตั้งใหม่เข้ารับหน้าที่

ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งตามวาระอาจได้รับแต่งตั้งอีกได้

มาตรา ๑๐ นอกจากการพ้นจากตำแหน่งตามวาระตามมาตรา ๙ ประธานกรรมการและกรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่งเมื่อ

(๑) ตาย

(๒) ลาออก

(๓) คณะรัฐมนตรีให้ออก เพราะบกพร่องต่อหน้าที่ มีความประพฤติเสื่อมเสีย หรือหย่อนความสามารถ

(๔) ขาดคุณสมบัติหรือมีลักษณะต้องห้ามตามมาตรา ๘

ในกรณีที่ประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่งก่อนวาระ ให้ผู้ที่ได้รับแต่งตั้งแทนตำแหน่งที่ว่างนั้นดำรงตำแหน่งได้เท่ากับวาระที่เหลืออยู่ของประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิซึ่งตนแทน เว้นแต่วาระที่เหลืออยู่ไม่ถึงเก้าสิบวันจะไม่แต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิแทนก็ได้

ในกรณีที่ประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่งก่อนวาระ ให้คณะกรรมการประกอบด้วยกรรมการทั้งหมดเท่าที่มีอยู่จนกว่าจะมีการแต่งตั้งประธานกรรมการหรือกรรมการผู้ทรงคุณวุฒิตามวรรคสอง และในกรณีที่ประธานกรรมการพ้นจากตำแหน่งก่อนวาระ ให้กรรมการที่เหลือเลือกกรรมการคนหนึ่งทำหน้าที่ประธานกรรมการเป็นการชั่วคราว

มาตรา ๑๑ การประชุมคณะกรรมการ ต้องมีกรรมการมาประชุมไม่น้อยกว่ากึ่งหนึ่งของจำนวนกรรมการทั้งหมด จึงจะเป็นองค์ประชุม

ให้ประธานกรรมการเป็นประธานในที่ประชุม ในกรณีที่ประธานกรรมการไม่มาประชุมหรือไม่อาจปฏิบัติหน้าที่ได้ ให้กรรมการซึ่งมาประชุมเลือกกรรมการคนหนึ่งเป็นประธานในที่ประชุม

การวินิจฉัยชี้ขาดของที่ประชุมให้ถือเสียงข้างมาก กรรมการคนหนึ่งให้มีเสียงหนึ่งในการลงคะแนน ถ้าคะแนนเสียงเท่ากัน ให้ประธานในที่ประชุมออกเสียงเพิ่มขึ้นอีกเสียงหนึ่งเป็นเสียงชี้ขาด

การประชุมของคณะกรรมการอาจกระทำได้โดยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นได้ตามที่คณะกรรมการกำหนด

มาตรา ๑๒ กรรมการผู้ใดมีส่วนได้เสียไม่ว่าโดยตรงหรือโดยอ้อมในเรื่องที่ที่ประชุมพิจารณา ให้แจ้งการมีส่วนได้เสียของตนให้คณะกรรมการทราบล่วงหน้าก่อนการประชุม และห้ามมิให้ผู้นั้นเข้าร่วมประชุมพิจารณาในเรื่องดังกล่าว

มาตรา ๑๓ คณะกรรมการมีอำนาจหน้าที่ ดังต่อไปนี้

(๑) จัดทำแผนยุทธศาสตร์การดำเนินงานด้านการส่งเสริม และการคุ้มครองข้อมูลส่วนบุคคล ที่สอดคล้องกับนโยบายและแผนระดับชาติที่เกี่ยวข้อง รวมทั้งเสนอแผนยุทธศาสตร์และมาตรการแก้ไขปัญหาอุปสรรคการปฏิบัติการตามนโยบายและแผนระดับชาติดังกล่าว

(๒) ส่งเสริมและสนับสนุนหน่วยงานของรัฐและภาคเอกชน ดำเนินกิจกรรมตามแผนยุทธศาสตร์ตาม (๑) รวมทั้งจัดให้มีการประเมินผลการดำเนินงานตามแผนยุทธศาสตร์ดังกล่าว เพื่อเสนอต่อคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติตามกฎหมายว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

(๓) กำหนดมาตรการหรือแนวทางการดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามพระราชบัญญัตินี้

(๔) ออกประกาศหรือระเบียบเพื่อให้การดำเนินการเป็นไปตามพระราชบัญญัตินี้

(๕) ประกาศกำหนดหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ

(๖) เสนอแนะต่อคณะรัฐมนตรีให้มีการตราหรือปรับปรุงกฎหมายหรือกฎที่ใช้บังคับอยู่ในส่วนที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

(๗) เสนอแนะต่อคณะรัฐมนตรีหรือรัฐมนตรีในการตราพระราชกฤษฎีกาหรือออกกฎกระทรวงตามพระราชบัญญัตินี้

(๘) ให้คำแนะนำและคำปรึกษาเกี่ยวกับการดำเนินการใด ๆ เพื่อให้ความคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐและภาคเอกชนในการปฏิบัติตามพระราชบัญญัตินี้

(๙) ส่งเสริมและสนับสนุนให้เกิดทักษะการเรียนรู้และความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้แก่ประชาชน

(๑๐) ส่งเสริมและสนับสนุนการวิจัย เพื่อพัฒนาเทคโนโลยีที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

(๑๑) ปฏิบัติการอื่นใดตามที่พระราชบัญญัตินี้หรือกฎหมายอื่นกำหนดให้เป็นอำนาจหน้าที่ของคณะกรรมการ

มาตรา ๑๔ ให้กรรมการได้รับเบี้ยประชุมและประโยชน์ตอบแทนอื่นตามหลักเกณฑ์ที่คณะรัฐมนตรีกำหนด

อนุกรรมการและกรรมการผู้เชี่ยวชาญที่คณะกรรมการแต่งตั้ง ให้ได้รับเบี้ยประชุมและประโยชน์ตอบแทนอื่นตามหลักเกณฑ์ที่คณะกรรมการกำหนด

มาตรา ๑๕ คณะกรรมการมีอำนาจแต่งตั้งคณะอนุกรรมการเพื่อพิจารณาหรือปฏิบัติการอย่างใดอย่างหนึ่งตามที่คณะกรรมการมอบหมายได้

การประชุมคณะอนุกรรมการ ให้นำความในมาตรา ๑๑ มาใช้บังคับโดยอนุโลม

มาตรา ๑๖ ให้สำนักงานมีหน้าที่ปฏิบัติงานวิชาการและงานธุรการให้แก่คณะกรรมการ คณะกรรมการผู้เชี่ยวชาญ และคณะอนุกรรมการ รวมทั้งให้มีอำนาจหน้าที่ ดังต่อไปนี้

(๑) ประสานงานกับส่วนราชการ รัฐวิสาหกิจ องค์การมหาชน และหน่วยงานอื่นของรัฐเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

(๒) ให้คำปรึกษาแก่หน่วยงานของรัฐและภาคเอกชนเกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้

(๓) กำหนดหลักสูตรและฝึกอบรมการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ลูกจ้าง ผู้รับจ้าง หรือประชาชนทั่วไป

(๔) ติดตามและประเมินผลการปฏิบัติตามพระราชบัญญัตินี้

(๕) ปฏิบัติการอื่นใดตามที่พระราชบัญญัตินี้หรือกฎหมายอื่นกำหนดให้เป็นอำนาจหน้าที่ของสำนักงาน

หมวด ๒
การคุ้มครองข้อมูลส่วนบุคคล

ส่วนที่ ๑
บททั่วไป

มาตรา ๑๗ ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยซึ่งข้อมูลส่วนบุคคลไม่ได้หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น เว้นแต่บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้

การขอความยินยอมต้องทำเป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เว้นแต่โดยสภาพไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้

ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยซึ่งข้อมูลส่วนบุคคลไปด้วย และการขอความยินยอมนั้นต้องไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ดังกล่าว ทั้งนี้ คณะกรรมการจะให้ผู้ควบคุมข้อมูลส่วนบุคคลขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามแบบและข้อความที่คณะกรรมการประกาศกำหนดก็ได้

เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเสียเมื่อใดก็ได้ เว้นแต่มีข้อจำกัดสิทธิในการถอนความยินยอมโดยกฎหมายหรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล

ในกรณีที่การถอนความยินยอมส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลในเรื่องใด ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงผลกระทบจากการถอนความยินยอมนั้น

มาตรา ๑๘ ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือในขณะที่เก็บรวบรวม

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่แตกต่างไปจากวัตถุประสงค์ที่ได้แจ้งไว้ตามวรรคหนึ่งจะกระทำมิได้ เว้นแต่

(๑) ได้แจ้งวัตถุประสงค์ใหม่นั้นให้เจ้าของข้อมูลส่วนบุคคลทราบและได้รับความยินยอมก่อนเก็บรวบรวม ใช้ หรือเปิดเผยแล้ว

(๒) บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้

ส่วนที่ ๒
การเก็บรวบรวมข้อมูลส่วนบุคคล

มาตรา ๑๙ การเก็บรวบรวมข้อมูลส่วนบุคคล ให้เก็บรวบรวมได้เท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

มาตรา ๒๐ ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียดดังต่อไปนี้

(๑) วัตถุประสงค์ของการเก็บรวบรวม

(๒) ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวม

(๓) ประเภทของบุคคลหรือหน่วยงานที่ซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย

(๔) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อ

(๕) สิทธิของเจ้าของข้อมูลตามมาตรา ๒๖ มาตรา ๒๗ และมาตรา ๒๘

กรณีมีเหตุที่ไม่อาจแจ้งรายละเอียดตามวรรคหนึ่งให้แก่เจ้าของข้อมูลส่วนบุคคลตามกำหนดเวลาในวรรคหนึ่ง ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งรายละเอียดตามวรรคหนึ่งแก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า

มาตรา ๒๑ ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(๑) เพื่อประโยชน์ที่เกี่ยวกับการศึกษาวิจัยหรือสถิติและได้เก็บข้อมูลส่วนบุคคลเพื่อการนั้นไว้เป็นความลับ

(๒) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

(๓) เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยตรงหรือโดยบริยายของเจ้าของข้อมูลส่วนบุคคล

(๔) เป็นการปฏิบัติตามกฎหมาย

(๕) กรณีอื่นตามที่กำหนดในกฎกระทรวง

มาตรา ๒๒ ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่

(๑) ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ชักช้า

(๒) เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลจากการใช้และเปิดเผยที่ได้รับการยกเว้นตามมาตรา ๒๔

(๓) เป็นข้อมูลที่เปิดเผยต่อสาธารณะ

มาตรา ๒๓ ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ หรือข้อมูลอื่นใดซึ่งกระทบความรู้สึกของประชาชนตามที่คณะกรรมการประกาศกำหนด โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(๑) ได้รับยกเว้นตามมาตรา ๒๑ (๒) หรือ (๔)

(๒) กรณีอื่นตามที่กำหนดในกฎกระทรวง

ส่วนที่ ๓
การใช้หรือเปิดเผยข้อมูลส่วนบุคคล

มาตรา ๒๔ ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา ๒๑ หรือมาตรา ๒๓ หรือเป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้ตามมาตรา ๒๒ (๓) แล้วแต่กรณี

บุคคลหรือนิติบุคคลที่ได้รับข้อมูลส่วนบุคคลมาจากการเปิดเผยตามวรรคหนึ่ง จะต้องไม่ใช้หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลส่วนบุคคลในการขอรับข้อมูลส่วนบุคคลนั้น

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้และเปิดเผยข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกการใช้และการเปิดเผยนั้นไว้ในรายการตามมาตรา ๓๐

มาตรา ๒๕ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศต้องเป็นไปตามหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลตามที่คณะกรรมการประกาศกำหนดตามมาตรา ๑๓ (๕) เว้นแต่

(๑) เป็นการปฏิบัติตามกฎหมาย

(๒) ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

(๓) เป็นการปฏิบัติตามสัญญาที่ทำระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ควบคุมข้อมูลส่วนบุคคล

(๔) เป็นการกระทำเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคลซึ่งไม่สามารถให้ความยินยอมในขณะนั้นได้

(๕) เป็นการโอนไปยังผู้ซึ่งได้รับเครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลตามมาตรา ๓๒ หรือมาตรา ๓๔

(๖) กรณีอื่นตามที่กำหนดในกฎกระทรวง

หมวด ๓
สิทธิของเจ้าของข้อมูลส่วนบุคคล

มาตรา ๒๖ เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงข้อมูลส่วนบุคคลที่เกี่ยวกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอม

ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามคำขอตามวรรคหนึ่ง จะปฏิเสธคำขอได้เฉพาะในกรณีดังต่อไปนี้

(๑) เป็นการขัดหรือแย้งกับบทบัญญัติแห่งกฎหมาย หรือปฏิบัติตามคำสั่งศาล

(๒) มีผลต่อการสืบสวนสอบสวนของพนักงานเจ้าหน้าที่ตามกฎหมาย

(๓) การเปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลนั้นอาจจะเป็นอันตรายต่อสิทธิและเสรีภาพของบุคคลอื่น

(๔) กรณีอื่นตามที่กำหนดในกฎกระทรวง

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธคำขอตามวรรคหนึ่ง ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกการปฏิเสธคำขอดังกล่าวพร้อมด้วยเหตุผลไว้ในรายการตามมาตรา ๓๐

เมื่อเจ้าของข้อมูลส่วนบุคคลมีคำขอตามวรรคหนึ่งและเป็นกรณีที่ไม่อาจปฏิเสธคำขอได้ตามวรรคสอง ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามคำขอภายในสามสิบวันนับแต่วันที่ได้รับคำขอ ทั้งนี้ คณะกรรมการจะประกาศกำหนดระยะเวลาในการดำเนินการตามคำขอให้เร็วขึ้นหรือขยายระยะเวลาดังกล่าวหรือกำหนดหลักเกณฑ์อื่นตามความเหมาะสมก็ได้

มาตรา ๒๗ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่ปฏิบัติตามหลักเกณฑ์แห่งพระราชบัญญัตินี้ เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย ระงับการใช้ชั่วคราว หรือแปลงข้อมูลส่วนบุคคลให้อยู่ในรูปแบบข้อมูลที่ไม่สามารถรู้ตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

กรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามวรรคหนึ่ง เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการได้

คณะกรรมการอาจประกาศกำหนดหลักเกณฑ์ในการลบหรือทำลาย ระงับการใช้ชั่วคราว หรือแปลงข้อมูลส่วนบุคคลให้อยู่ในรูปแบบข้อมูลที่ไม่สามารถรู้ตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลตามวรรคหนึ่งก็ได้

มาตรา ๒๘ ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้องเป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด

ในกรณีที่เจ้าของข้อมูลส่วนบุคคลร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามวรรคหนึ่ง หากผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามคำร้องขอ ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกคำร้องขอของเจ้าของข้อมูลส่วนบุคคลและเหตุผลที่ไม่ดำเนินการตามวรรคหนึ่งไว้ในรายการตามมาตรา ๓๐

มาตรา ๒๙ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(๑) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

(๒) ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

(๓) ทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการพิสูจน์หรือการตรวจสอบ ทั้งนี้ ให้นำความในมาตรา ๒๗ วรรคสาม มาใช้บังคับกับการทำลายข้อมูลส่วนบุคคลโดยอนุโลม

(๔) แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้า ถ้าเป็นกรณีการละเมิดข้อมูลส่วนบุคคลเกินจำนวนบุคคลที่คณะกรรมการประกาศกำหนด ให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลและแนวทางการเยียวยาแก่คณะกรรมการโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

มาตรา ๓๐ ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกทำรายการดังต่อไปนี้ เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถตรวจสอบได้

(๑) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม

(๒) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท

(๓) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล

(๔) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

(๕) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น

(๖) การใช้และการเปิดเผยตามมาตรา ๒๔ วรรคสาม

(๗) การปฏิเสธคำขอตามมาตรา ๒๖ วรรคสาม และมาตรา ๒๘ วรรคสอง

หมวด ๔
ข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

มาตรา ๓๑ ให้คณะกรรมการประกาศกำหนดข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลเป็นแนวทางให้ผู้ควบคุมข้อมูลส่วนบุคคลปฏิบัติ

มาตรา ๓๒ ให้มีเครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลที่ได้รับใบรับรองจากสำนักงานมีสิทธิใช้หรือแสดงเครื่องหมายดังกล่าว

ผู้ควบคุมข้อมูลส่วนบุคคลที่ประสงค์จะมีสิทธิใช้หรือแสดงเครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล ให้ยื่นคำขอรับใบรับรองต่อสำนักงานตามหลักเกณฑ์และวิธีการที่สำนักงานประกาศกำหนด

ในการพิจารณาคำขอตามวรรคสอง ให้สำนักงานประเมินผลการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคล หากผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลเป็นไปตามข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่คณะกรรมการประกาศกำหนดตามมาตรา ๓๑ ให้สำนักงานออกใบรับรองแก่ผู้ควบคุมข้อมูลส่วนบุคคลนั้น

ลักษณะและรายละเอียดของเครื่องหมายรับรองมาตรฐาน การใช้หรือการแสดงเครื่องหมาย วิธีการประเมินผล การตรวจติดตามผล อัตราค่าธรรมเนียมการประเมินผลหรือการตรวจติดตามผล และการเพิกถอนใบรับรองให้เป็นไปตามที่คณะกรรมการประกาศกำหนด

ในกรณีที่สำนักงานเพิกถอนใบรับรองของผู้ควบคุมข้อมูลส่วนบุคคลใด ให้ผู้ควบคุมข้อมูลส่วนบุคคลนั้นคืนใบรับรองให้แก่สำนักงานภายในสิบห้าวันนับแต่วันที่ได้รับแจ้งการเพิกถอน

คณะกรรมการจะประกาศกำหนดให้หน่วยงานอื่นของรัฐหรือหน่วยงานของเอกชนทั้งในประเทศหรือต่างประเทศเป็นผู้ประเมินผลและตรวจติดตามผลการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลเพื่อขอรับใบรับรองจากสำนักงานตามวรรคสามด้วยก็ได้

ห้ามมิให้ผู้ใดใช้หรือแสดงเครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลเว้นแต่เป็นผู้ควบคุมข้อมูลส่วนบุคคลที่ได้รับใบรับรองจากสำนักงาน

มาตรา ๓๓ มาตรฐานของผู้ประเมินผลและตรวจติดตามผล การตรวจสอบมาตรฐานและอัตราค่าธรรมเนียมการตรวจสอบมาตรฐานสำหรับหน่วยงานของเอกชน รวมทั้งการเพิกถอนรายชื่อจากประกาศตามมาตรา ๓๒ วรรคหก ให้เป็นไปตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด

มาตรา ๓๔ คณะกรรมการจะประกาศยอมรับเครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานต่างประเทศหรือองค์การระหว่างประเทศก็ได้ หากปรากฏว่า การคุ้มครองข้อมูลส่วนบุคคลดังกล่าวมีข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลเป็นไปตามที่คณะกรรมการประกาศกำหนดตามมาตรา ๓๑

๑๒

หมวด ๕
การร้องเรียน

มาตรา ๓๕ ให้คณะกรรมการแต่งตั้งคณะกรรมการผู้เชี่ยวชาญขึ้นคณะหนึ่งหรือหลายคณะก็ได้ตามความเชี่ยวชาญในแต่ละเรื่องหรือตามที่คณะกรรมการเห็นสมควร

คุณสมบัติและลักษณะต้องห้าม วาระการดำรงตำแหน่ง การพ้นจากตำแหน่ง และการดำเนินงานอื่นของคณะกรรมการผู้เชี่ยวชาญให้เป็นไปตามที่คณะกรรมการประกาศกำหนด

มาตรา ๓๖ คณะกรรมการผู้เชี่ยวชาญมีอำนาจหน้าที่ ดังต่อไปนี้

(๑) พิจารณาเรื่องร้องเรียนตามพระราชบัญญัตินี้

(๒) ตรวจสอบการกระทำใด ๆ ของผู้ควบคุมข้อมูลส่วนบุคคลหรือลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลเกี่ยวกับข้อมูลส่วนบุคคลที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคล

(๓) ไกล่เกลี่ยข้อพิพาทเกี่ยวกับข้อมูลส่วนบุคคล

(๔) ปฏิบัติการอื่นใดตามที่พระราชบัญญัตินี้กำหนดให้เป็นอำนาจหน้าที่ของคณะกรรมการผู้เชี่ยวชาญ

มาตรา ๓๗ เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคล หรือลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัตินี้ กฎกระทรวงหรือประกาศที่ออกตามพระราชบัญญัตินี้

การยื่น การไม่รับเรื่อง การยุติเรื่อง และวิธีพิจารณาคำร้องเรียน ให้เป็นไปตามระเบียบที่คณะกรรมการประกาศกำหนด

มาตรา ๓๘ ในกรณีที่ผู้ร้องเรียนตามมาตรา ๓๗ ไม่ได้ปฏิบัติให้ถูกต้องตามระเบียบที่กำหนดไว้ในมาตรา ๓๗ วรรคสอง หรือเป็นเรื่องร้องเรียนที่ระเบียบนั้นได้กำหนดไม่ให้รับไว้พิจารณา ให้คณะกรรมการผู้เชี่ยวชาญไม่รับเรื่องร้องเรียนไว้พิจารณา

เมื่อคณะกรรมการผู้เชี่ยวชาญพิจารณาเรื่องร้องเรียนตามมาตรา ๓๖ (๑) หรือตรวจสอบการกระทำใด ๆ ตามมาตรา ๓๖ (๒) แล้วรับฟังได้ว่า เรื่องร้องเรียนหรือการกระทำนั้นไม่มีมูล ให้คณะกรรมการผู้เชี่ยวชาญมีคำสั่งยุติเรื่อง

ในกรณีที่คณะกรรมการผู้เชี่ยวชาญพิจารณาหรือตรวจสอบตามวรรคสองแล้วรับฟังได้ว่า เรื่องร้องเรียนหรือการกระทำนั้นเป็นกรณีที่มิได้เป็นความผิดอาญาซึ่งดำเนินการไกล่เกลี่ยได้ และคู่กรณีประสงค์จะให้ไกล่เกลี่ย ให้คณะกรรมการผู้เชี่ยวชาญดำเนินการไกล่เกลี่ย แต่หากเรื่องร้องเรียนหรือการกระทำนั้นเป็นกรณีที่ไม่อาจไกล่เกลี่ยได้ หรือเป็นกรณีที่ไกล่เกลี่ยไม่สำเร็จ ให้คณะกรรมการผู้เชี่ยวชาญมีอำนาจออกคำสั่ง ดังต่อไปนี้

(๑) สั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลปฏิบัติหรือดำเนินการแก้ไขการกระทำของตนให้ถูกต้องภายในระยะเวลาที่กำหนด

(๒) สั่งห้ามผู้ควบคุมข้อมูลส่วนบุคคลกระทำการที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลหรือให้กระทำการใดเพื่อระงับความเสียหายนั้นภายในระยะเวลาที่กำหนด

ในกรณีผู้ควบคุมข้อมูลส่วนบุคคลไม่ยอมดำเนินการตามคำสั่งตามวรรคสาม (๑) หรือ (๒) ให้นำบทบัญญัติเกี่ยวกับการบังคับทางปกครองตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองมาใช้บังคับโดยอนุโลม ทั้งนี้ ในกรณีที่ต้องมีการยึด อายัด หรือขายทอดตลาดทรัพย์สินของผู้ควบคุมข้อมูลส่วนบุคคลเพื่อบังคับตามหลักเกณฑ์ที่กำหนดไว้ในกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครอง ให้คณะกรรมการผู้เชี่ยวชาญเป็นผู้มีอำนาจสั่งยึด อายัด หรือขายทอดตลาดทรัพย์สินเพื่อการนั้น

การจัดทำคำสั่งตามวรรคหนึ่ง วรรคสอง หรือวรรคสาม (๑) หรือ (๒) ให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

คำสั่งของคณะกรรมการผู้เชี่ยวชาญ ให้ประธานกรรมการผู้เชี่ยวชาญเป็นผู้ลงนามแทน

มาตรา ๓๙ คำสั่งไม่รับเรื่องร้องเรียนไว้พิจารณาตามมาตรา ๓๘ วรรคหนึ่ง หรือยุติเรื่องตามมาตรา ๓๘ วรรคสอง หรือคำสั่งตามมาตรา ๓๘ วรรคสาม (๑) หรือ (๒) ให้เป็นที่สุด

มาตรา ๔๐ ให้คณะกรรมการผู้เชี่ยวชาญมีอำนาจสั่งให้บุคคลหนึ่งบุคคลใดส่งเอกสารหรือข้อมูลเกี่ยวกับเรื่องที่มีผู้ร้องเรียน หรือเรื่องอื่นใดที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้ รวมทั้งจะเรียกให้บุคคลใดมาชี้แจงข้อเท็จจริงด้วยก็ได้

มาตรา ๔๑ ในการปฏิบัติการตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่มีอำนาจหน้าที่ ดังต่อไปนี้

(๑) มีหนังสือแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ใดมาให้ข้อมูลหรือส่งเอกสารหรือหลักฐานใด ๆ เกี่ยวกับการดำเนินการหรือการกระทำความผิดตามพระราชบัญญัตินี้

(๒) ตรวจสอบและรวบรวมข้อเท็จจริง แล้วรายงานต่อคณะกรรมการผู้เชี่ยวชาญในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ใดได้กระทำผิดหรือทำให้เกิดความเสียหายเพราะฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัตินี้ กฎกระทรวงหรือประกาศที่ออกตามพระราชบัญญัตินี้

ในการดำเนินการตาม (๒) หากมีความจำเป็นเพื่อคุ้มครองประโยชน์ของเจ้าของข้อมูลส่วนบุคคลหรือเพื่อประโยชน์สาธารณะ ให้พนักงานเจ้าหน้าที่มีอำนาจเข้าไปในสถานที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ใดเกี่ยวกับการกระทำความผิดตามพระราชบัญญัตินี้ ในระหว่างเวลาพระอาทิตย์ขึ้นจนถึงพระอาทิตย์ตกหรือในเวลาทำการของสถานที่นั้น เพื่อตรวจสอบและรวบรวมข้อเท็จจริง และยึดหรืออายัดเอกสารและหลักฐาน รวมถึงสิ่งอื่นใดที่เกี่ยวกับการกระทำความผิดหรือสงสัยว่ามีไว้หรือใช้เพื่อกระทำความผิด

ในการปฏิบัติหน้าที่ของพนักงานเจ้าหน้าที่ตามมาตรานี้ ให้ผู้ที่เกี่ยวข้องอำนวยความสะดวกตามสมควร

หมวด ๖
ความรับผิดทางแพ่ง

มาตรา ๔๒ ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลอันทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้นแก่เจ้าของข้อมูลส่วนบุคคล ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อของผู้ควบคุมข้อมูลส่วนบุคคลหรือไม่ก็ตาม เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลนั้นจะพิสูจน์ได้ว่า

(๑) ความเสียหายนั้นเกิดจากเหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั้นเอง

(๒) เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามอำนาจหน้าที่ตามกฎหมาย

(๓) เป็นการปฏิบัติครบถ้วนตามข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่คณะกรรมการประกาศกำหนดตามมาตรา ๓๑

ค่าสินไหมทดแทนตามวรรคหนึ่ง ให้หมายความรวมถึงค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย

หมวด ๗
บทกำหนดโทษ

มาตรา ๔๓ ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา ๒๐ มาตรา ๒๖ วรรคสี่ มาตรา ๓๐ หรือมาตรา ๓๒ วรรคห้า หรือไม่ขอความยินยอมตามแบบหรือข้อความที่คณะกรรมการประกาศกำหนดตามมาตรา ๑๗ วรรคสาม หรือไม่แจ้งผลกระทบจากการถอนความยินยอมตามมาตรา ๑๗ วรรคห้า ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

มาตรา ๔๔ ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา ๑๘ มาตรา ๑๙ มาตรา ๒๑ มาตรา ๒๒ มาตรา ๒๔ วรรคหนึ่งหรือวรรคสอง มาตรา ๒๕ หรือมาตรา ๒๙ หรือขอความยินยอมโดยการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ หรือผู้ใดฝ่าฝืนมาตรา ๓๒ วรรคเจ็ด ต้องระวางโทษปรับไม่เกินสามแสนบาท

การกระทำตามความในวรรคหนึ่ง หากเป็นการกระทำเพื่อให้ตนเองหรือผู้อื่นได้รับประโยชน์อันมิควรได้ หรือเพื่อให้เกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๔๕ ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา ๒๓ ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ

การกระทำตามความในวรรคหนึ่ง หากเป็นการกระทำเพื่อให้ตนเองหรือผู้อื่นได้รับประโยชน์อันมิควรได้ หรือให้เกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสองล้านบาท หรือทั้งจำทั้งปรับ

การฝ่าฝืนตามมาตรา ๒๔ วรรคหนึ่งหรือวรรคสอง หรือมาตรา ๒๕ เกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา ๒๓ ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ

การฝ่าฝืนตามวรรคสาม หากเป็นการกระทำเพื่อให้ตนเองหรือผู้อื่นได้รับประโยชน์อันมิควรได้ หรือให้เกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสองล้านบาท หรือทั้งจำทั้งปรับ

มาตรา ๔๖ ผู้ใดไม่ปฏิบัติตามคำสั่งของคณะกรรมการผู้เชี่ยวชาญหรือไม่มาชี้แจงข้อเท็จจริงตามมาตรา ๔๐ หรือไม่อำนวยความสะดวกแก่พนักงานเจ้าหน้าที่ตามมาตรา ๔๑ วรรคสาม ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

มาตรา ๔๗ ผู้ใดต่อสู้หรือขัดขวางพนักงานเจ้าหน้าที่ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๔๘ ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ถ้าผู้นั้นนำไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ

ความในวรรคหนึ่ง มิให้นำมาใช้บังคับแก่การเปิดเผยในกรณีดังต่อไปนี้

(๑) การเปิดเผยตามหน้าที่

(๒) การเปิดเผยเพื่อประโยชน์แก่การสอบสวน หรือการพิจารณาคดี

(๓) การเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย

(๔) การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล

(๕) การเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่าง ๆ ที่เปิดเผยต่อสาธารณะ

มาตรา ๔๙ บรรดาความผิดตามพระราชบัญญัตินี้ ให้คณะกรรมการมีอำนาจเปรียบเทียบได้ และคณะกรรมการอาจมอบอำนาจให้คณะอนุกรรมการใช้อำนาจดังกล่าวด้วยก็ได้

เมื่อผู้กระทำความผิดได้เสียค่าปรับตามที่เปรียบเทียบแล้ว ให้ถือว่าคดีเลิกกันตามประมวลกฎหมายวิธีพิจารณาความอาญา

๑๖

บทเฉพาะกาล

มาตรา ๕๐ ในวาระเริ่มแรก ให้คณะกรรมการประกอบด้วยกรรมการตามมาตรา ๗ (๒) และกรรมการตามวรรคสองเพื่อปฏิบัติหน้าที่เท่าที่จำเป็นไปพลางก่อนแต่ไม่เกินเก้าสิบวันนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ และให้กรรมการดังกล่าวเลือกกรรมการคนหนึ่งทำหน้าที่ประธานกรรมการเป็นการชั่วคราว

ให้สำนักงานดำเนินการให้มีการแต่งตั้งประธานกรรมการตามมาตรา ๗ (๑) และกรรมการผู้ทรงคุณวุฒิตามมาตรา ๗ (๓) ภายในเก้าสิบวันนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ

มาตรา ๕๑ ในวาระเริ่มแรกที่ยังไม่มีเลขาธิการตามพระราชบัญญัตินี้ ให้ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ปฏิบัติหน้าที่เลขาธิการตามพระราชบัญญัตินี้เป็นการชั่วคราวจนกว่าจะมีเลขาธิการตามพระราชบัญญัตินี้

ในกรณีที่ยังไม่มีผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ตามวรรคหนึ่ง ให้ผู้ดำรงตำแหน่งผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ตามพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ. ๒๕๕๔ ปฏิบัติหน้าที่ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์และเลขาธิการตามพระราชบัญญัตินี้เป็นการชั่วคราวจนกว่าจะมีผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์หรือเลขาธิการตามพระราชบัญญัตินี้ แล้วแต่กรณี

มาตรา ๕๒ ในวาระเริ่มแรกที่ยังไม่มีสำนักงานตามพระราชบัญญัตินี้ ให้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ปฏิบัติหน้าที่สำนักงานตามพระราชบัญญัตินี้เป็นการชั่วคราวจนกว่าจะมีสำนักงานตามพระราชบัญญัตินี้

มาตรา ๕๓ ผู้ใดเป็นผู้ควบคุมข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้อยู่ก่อนวันที่พระราชบัญญัตินี้ใช้บังคับ ให้ปฏิบัติตามบทบัญญัติแห่งพระราชบัญญัตินี้ กฎกระทรวงหรือประกาศที่ออกตามพระราชบัญญัตินี้ เว้นแต่การปฏิบัติตามมาตรา ๒๙ (๑) ให้ปฏิบัติตามบทบัญญัติดังกล่าวภายในเก้าสิบวันนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ

ผู้รับสนองพระบรมราชโองการ

.....

นายกรัฐมนตรี

ประวัติผู้เขียน

ชื่อ	นางสาวอธิพร สิทธิธีรรัตน์
วุฒิการศึกษา	ปีการศึกษา 2555 : นิติศาสตรบัณฑิต (เกียรตินิยมอันดับ 1) จุฬาลงกรณ์มหาวิทยาลัย