แนวทางการคุ้มครองข้อมูลใน Big Data:
ศึกษาประเด็นความเป็นส่วนตัวและความมั่นคงปลอดภัยของข้อมูล

Guideline for Data Protection in Big Data: Privacy and Data Security

แนวทางการคุ้มครองข้อมูลใน Big Data:
ศึกษาประเด็นความเป็นส่วนตัวและความมั่นคงปลอดภัยของข้อมูล

Guideline for Data Protection in Big Data: Privacy and Data Security

ปิยะภัสร์ โรจน์รัตนวาณิชย์

การค้นคว้าอิสระเป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
นิติศาสตรมหาบัณฑิต
มหาวิทยาลัยกรุงเทพ
ปีการศึกษา 2556

บัณฑิตวิทยาลัย มหาวิทยาลัยกรุงเทพ
อนุมัติให้การค้นคว้าอิสระเป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
นิติศาสตรมหาบัณฑิต

เรื่อง แนวทางการคุ้มครองข้อมูลใน Big Data: ศึกษาประเด็นความเป็นส่วนตัวและความมั่นคงปลอดภัยของข้อมูล

ผู้วิจัย ปิยะภัสร์ โรจน์รัตนวาณิชย์

ได้พิจารณาเห็นชอบโดย

อาจารย์ที่ปรึกษา _____
(ผู้ช่วยศาสตราจารย์ ดร.อรรยา สิงห์สงบ)

อาจารย์ที่ปรึกษาร่วม _____
(อาจารย์วินิจฉัย แจ่มแจ้ง)

ผู้เชี่ยวชาญ _____
(อาจารย์สุรางคณา วายุภาพ)

_____
(ผู้ช่วยศาสตราจารย์ ดร.อรรยา สิงห์สงบ)
รองอธิการบดีฝ่ายวิชาการ
รักษาการคณบดีบัณฑิตวิทยาลัย
10 กันยายน 2557

ปิยะภัสร์ โรจน์รัตนวาณิชย์. ปริญญานิติศาสตรมหาบัณฑิต, กันยายน 2557, บัณฑิตวิทยาลัย มหาวิทยาลัยกรุงเทพ.
แนวทางการคุ้มครองข้อมูลใน Big Data: ความเป็นส่วนตัวและความมั่นคงปลอดภัยของข้อมูล (121 หน้า)
อาจารย์ที่ปรึกษา: ผู้ช่วยศาสตราจารย์ ดร.อรรยา สิงห์สงบ

บทคัดย่อ

ปัจจุบันเทคโนโลยีสารสนเทศได้เข้ามาเป็นส่วนหนึ่งในชีวิตประจำวันโดยการสื่อสานผ่านทางอินเทอร์เน็ตซึ่งถูกใช้กันอย่างแพร่หลายในการดำเนินการทางธุรกิจ ซึ่งในขณะนี้นวัตกรรมใหม่ที่มีความสำคัญและกำลังจะเติบโตอย่างต่อเนื่องในปี 2014 นี้ ได้แก่ Big Data บริษัทขนาดใหญ่ของโลกที่ทรงอิทธิพลที่สุด คือ บริษัทด้านเทคโนโลยีสารสนเทศ เช่น Google, Apple และ Microsoft บริษัทผู้ให้บริการเหล่านี้มี Big Data ที่มีข้อมูลส่วนบุคคลเป็นจำนวนมาก ซึ่งเป็นข้อมูลที่ได้มาจากผู้ใช้บริการทั่วโลกส่งผ่านถึงกันตลอดเวลาในเครือข่ายทางสังคม ยกตัวอย่างเช่น การเพิ่มขึ้นของจำนวนประชากร และอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกันทางเครือข่ายสังคมในขณะนี้ได้มีความสามารถในการสร้าง สื่อสาร แบ่งปัน และเข้าถึงข้อมูลกันอย่างรวดเร็ว ข้อมูลที่ถูกสร้างขึ้นนี้มีมูลค่ามากมหาศาลสำหรับเศรษฐกิจโลก เนื่องจากสามารถถูกใช้เพื่อผลักดันนวัตกรรมใหม่ ๆ และการผลิตให้มีประสิทธิภาพยิ่งขึ้น บางเครือข่ายใช้ Big Data วิเคราะห์ข้อมูลโดยความต้องการเป็นมืออาชีพ ในขณะที่บางเครือข่ายใช้เพื่อความสะดวกสบาย ใช้วิเคราะห์แนวโน้มต่าง ๆ ของโลก จึงเป็นผลให้การใช้ Big Data นั้น มีประเด็นปัญหาเกี่ยวกับความเป็นส่วนตัว และความมั่นคงปลอดภัยของข้อมูลเกิดขึ้นเป็นจำนวนมาก การวิจัยนี้แสดงให้เห็นว่ามีการละเมิดความเป็นส่วนตัวเป็นจำนวนมาก และหนึ่งในประเด็นทางกฎหมายที่สำคัญที่สุดก็คือ การละเมิดความเป็นส่วนตัวของข้อมูลส่วนบุคคลและความมั่นคงปลอดภัยของข้อมูล

สำหรับกรณีของประเทศไทยนั้น หลักจากที่ได้ทำการศึกษากฎหมายต่าง ๆ เกี่ยวกับการคุ้มครองสิทธิความเป็นอยู่ส่วนตัวและความมั่นคงปลอดภัยของข้อมูลที่มีผลใช้บังคับอยู่ในปัจจุบัน ได้แก่ รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550 ประมวลกฎหมายแพ่งและพาณิชย์ ประมวลกฎหมายอาญา พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 รวมถึงร่างกฎหมายที่กำลังอยู่ในระหว่างการพิจารณาของรัฐสภา ซึ่งก็คือ ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...

จากการศึกษาพบว่ายังไม่กฎหมายที่บัญญัติขึ้นเป็นการเฉพาะเรื่องความเป็นส่วนตัว รวมถึงการรักษาความมั่นคงปลอดภัยของข้อมูลของผู้ใช้บริการต่าง ๆ แม้ว่าจะมีการนำกฎหมายที่มีผลบังคับใช้ในปัจจุบันไปใช้ในกรณีการละเมิดความเป็นส่วนตัวจากการใช้ Big Data ก็ตาม แต่ก็ยังไม่ได้บัญญัติไว้ครอบคลุมถึงการคุ้มครองความเป็นส่วนตัว และความปลอดภัยของข้อมูลในกรณี Big Data ดังนั้น ผู้เขียนจึงมีความเห็นว่าควรเร่งให้มีการออกกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลที่มีอยู่ในความครอบครองของภาคเอกชนเป็นการทั่วไป และเพื่อเป็นการวางมาตรการในเชิงป้องกันการละเมิดความเป็นส่วนตัวในข้อมูลส่วนบุคคล และความปลอดภัยของข้อมูล และเพื่อระบุถึงสิทธิหน้าที่ของผู้ที่เกี่ยวข้องกับ Big Data ให้มีความชัดเจนแน่นอน ผู้เขียนเห็นว่าควรจะพยายามตีความกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลให้ครอบคลุมมาถึงความเป็นส่วนตัวและความมั่นคงปลอดภัยของข้อมูลกรณี Big Data ด้วย แล้วอาศัยอำนาจแห่งกฎหมายดังกล่าวออกกฎหมายลำดับรองเพื่อวางแนวทางในการคุ้มครองความเป็นส่วนตัวและความมั่นคงปลอดภัยของข้อมูลกรณี Big Data เป็นการเฉพาะ

คำสำคัญ: Big Data, ข้อมูลส่วนบุคคล, ความเป็นส่วนตัว, ความมั่นคงปลอดภัยของข้อมูล

Rojratanavanich, P. LL.M., September 2014, Graduate school, Bangkok University.
Guideline for Data Protection in Big Data: Privacy and Data Security (121 pp.)
Advisor: Asst.Prof.AunyaSingsangob, S.J.D.

ABSTRACT

Nowadays, information technology of telecommunication via internet was being used widely in the business operation. Big Data was the new and important innovation in 2014. There were many social network sites or companies such as Google, Apple and Microsoft. These companies had a lot of Big Data that included personal information. In addition, increasing number of people, devices, and sensor that were now connected by social networks has revolutionized the ability to generate, communicate, share and access data. Data created enormous value for the world economy, driving innovation, productivity, efficiency and growth. Some networks targeted professional context while others primarily aimed at leisurely contact. Some network focused on text based interactions while others tended towards multimedia. Big Data caused many privacy and data security issues. The research indicated that there were several issues relating to the invasion of privacy of Big Data. One of the most important legal issues was the privacy of personal information.

In case of Thailand, this research studied various laws relating to right of privacy. There were laws which were enforced including the following: Constitution of the Kingdom of Thailand, B.E. 2550 (2007), the Criminal Code, the Civil and Commercial Code, the Official Information Act, B.E. 2540 (1997), the Electronic Transaction Act, B.E. 2544 (2001), the Credit Information Business Act, B.E. 2545 (2002) and the Computer-Related Crimes Act, B.E. 2550 (2007). Not only a study of currently enforceable laws, but this research also considered a bill on Personal Information Protection which was in process of passing into laws. The research found that there were no specific laws in recent Thai legal system to protect the private information and data security for Big Data. Although there were various laws which can be applied to the case of invasion of privacy from the utilization of Big Data, they are

incomprehensive. The writer would like to recommend that a bill on Personal Information Protection should be enacted into enforceable law as soon as possible. Such a law should be supportive. Besides, this Personal Information Protection law should be applied to all technologies, including Big Data. Moreover, for the purpose of clarification it might therefore be necessary to provide detailed guidelines or codes of conduct on practical implementation of Big Data.

Keywords: Big Data, Data Protection, Privacy, Data Security

กิตติกรรมประกาศ

สารนิพนธ์ฉบับนี้สำเร็จได้ด้วยความกรุณาของ ผู้ช่วยศาสตราจารย์ ดร.อรรยา สิงห์สงบ อาจารย์ที่ปรึกษาหลัก และอาจารย์วินิจฉัย แจ่มแจ้ง อาจารย์ที่ปรึกษาร่วม ซึ่งท่านอาจารย์ทั้งสองได้ให้คำปรึกษา เสนอข้อคิดเห็น ข้อชี้แนะ พร้อมทั้งช่วยวางแผนและให้ความช่วยเหลือในหลายสิ่งหลายอย่างจนกระทั่งสารนิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้ด้วยดี ผู้วิจัยขอกราบขอบพระคุณเป็นอย่างสูงมา ณ ที่นี้

ผู้วิจัยขอขอบพระคุณ อาจารย์สุรางคณา วายุภาพ ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) และ ดร.สรณันท์ จิวะรัตน์ ผู้อำนวยการสำนักความมั่นคงปลอดภัย ที่ให้โอกาสผู้วิจัยได้เข้าร่วมศึกษา เข้าถึงแหล่งข้อมูลที่สำคัญ ให้คำปรึกษาทางด้านความมั่นคงปลอดภัย อีกทั้งสละเวลา ให้คำแนะนำและช่วยเหลือผู้วิจัย จนงานวิจัยฉบับนี้สำเร็จลุล่วง

ผู้วิจัยขอขอบคุณ ดร.นิตย์ โรจน์รัตนวาณิชย์ ผู้ช่วยปลัดกระทรวงศึกษาธิการ ผู้ทรงคุณวุฒิด้านหลักการและวิธีการในการทำวิจัย และให้คำแนะนำ คำปรึกษาในด้านการจัดการความรู้ ซึ่งผู้วิจัยขอขอบคุณเป็นอย่างสูง

ผู้วิจัยยังได้รับคำแนะนำจาก ทนายความภูชิชย์ สุรรัตน์ ที่ปรึกษากฎหมายทรัพย์สินทางปัญญาและการวางแผนธุรกิจ ซึ่งเป็นผู้มีความรู้ และความเชี่ยวชาญทางด้านกฎหมายทรัพย์สินทางปัญญาและกฎหมายทั่วไป คุณพลอยพชร โชไชย ผู้มีประสบการณ์ทางด้านกฎหมายธุรกรรมทางอิเล็กทรอนิกส์ และคุณณภาภัช ไชยบุดดี ซึ่งท่านทั้งสามให้ความรู้ คำแนะนำ และช่วยเหลือผู้วิจัยเป็นอย่างดียิ่ง

สุดท้ายนี้ กราบขอบพระคุณ คุณสมพงษ์ โรจน์รัตนวาณิชย์ และคุณนิตย์ โรจน์รัตนวาณิชย์ บุพการีผู้ให้โอกาสทางการศึกษา พร้อมทั้งให้การสนับสนุนทางด้านกำลังทรัพย์ คอยเป็นกำลังใจ และให้การช่วยเหลือในทุก ๆ ด้านกับผู้วิจัย

ปิยะภัสร์ โรจน์รัตนวาณิชย์

สารบัญ

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญภาพ

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันเทคโนโลยีสารสนเทศได้เข้ามาเป็นส่วนหนึ่งในชีวิตประจำวัน จนเกิดเป็นสังคมใหม่เรียกว่า สังคมสารสนเทศ จากผลสำรวจรายงานประจำปีดัชนีชี้วัดสังคมสารสนเทศปี พ.ศ. 2557 พบว่าประเทศไทยเป็นประเทศที่มีพัฒนาการใช้งานอินเทอร์เน็ตความเร็วสูงมากที่สุดในโลก ซึ่งในปี พ.ศ. 2555 อยู่ในลำดับที่ 105 และในปี พ.ศ. 2557 ได้ขึ้นมา 34 อันดับ เป็นลำดับที่ 71[1] จากปัจจัยการจัดสรรคลื่นความถี่ IMT ย่าน 2.1 GHz และการใช้ Mobile Internet ที่เพิ่มสูงขึ้น ส่งผลให้ลำดับดัชนีชี้วัดระดับและพัฒนาการของระบบ ICT หรือ IDI (ICT Development Index) ของประเทศไทย ก้าวขึ้นมาอยู่ลำดับที่ 81 ในปี พ.ศ. 2556 จาก 166 ประเทศทั่วโลก สูงขึ้นจากเดิม 10 อันดับ ยกระดับการพัฒนาการระบบ ICT ของประเทศไทยอยู่ในระดับค่าเฉลี่ยโลก ติด Top 10 ของกลุ่มประเทศเอเชียแปซิฟิก จากปี พ.ศ. 2555 ที่อยู่ในกลุ่มประเทศกำลังพัฒนา แสดงให้เห็นถึงศักยภาพการสื่อสารของไทยที่พัฒนาขึ้นอย่างรวดเร็ว

Big Data ถือเป็นนวัตกรรมที่มีความสำคัญและกำลังจะเติบโตอย่างต่อเนื่องในปี ค.ศ. 2014 แม้กระทั่งในประเทศไทย หลายภาคส่วนของธุรกิจและองค์กรขนาดใหญ่ได้เริ่มให้ความสำคัญกับ Big Data เพื่อเป็นกลยุทธ์ที่สำคัญในการเอาชนะคู่แข่งทางธุรกิจในโลกของอินเทอร์เน็ต ปัจจุบันมีบริษัทใหญ่ของโลกที่ทรงอิทธิพลที่สุด คือ บริษัทผู้ให้บริการ เช่น Google, Apple และ Microsoft บริษัทเหล่านี้มี Big Data ซึ่งมีข้อมูลส่วนบุคคลเป็นจำนวนมากและเป็นข้อมูลที่ได้มาจากผู้บริโภคทั่วโลกส่งผ่านถึงกันตลอดเวลา ผ่านเครื่องมือสื่อสาร หรือช่องทางการสื่อสารทางเทคโนโลยีสารสนเทศ โดยบริษัทผู้ให้บริการที่มีชื่อเสียง และมีผู้เข้าใช้เป็นจำนวนมากที่สุดนั้น คือ Google จากยุคแรกเริ่ม Google นำเสนอโฆษณา โดยกำหนดให้ตรงกับคำค้น (Keyword) ที่ผู้เข้าใช้ใช้ค้นหาบน Search Engine (Google Adwords) และให้ตรงกับเนื้อหาของเว็บไซต์ที่ผู้ใช้เข้าชม (Google Adsense) ต่อมา Google ได้นำเสนอนวัตกรรม Google AdChoices ที่กำหนดโฆษณาให้ตรงกับพฤติกรรมของผู้เข้าใช้โดยตรง ซึ่งเป็นข้อมูลของผู้เข้าใช้ที่ Google ได้เก็บสะสม ซึ่งรวมถึงพฤติกรรมในการเข้าชมเว็บไซต์ต่าง ๆ และอาจรวมถึงสิ่งที่ผู้เข้าใช้ได้กระทำระหว่างที่เข้าชมเว็บไซต์เหล่านั้น นอกจากนี้ยังอาจมีการใช้ข้อมูลอื่น ๆ เช่น ตำแหน่งสถานที่ของผู้เข้าใช้ อุปกรณ์ในการเข้าถึง เป็นต้น ซึ่ง Google มีระบบวิเคราะห์ข้อมูลที่สามารถประมวลข้อมูลที่เกี่ยวข้องกับผู้เข้าใช้อย่างแม่นยำและอัตโนมัติ การที่

[1] ผลสำรวจรายงานประจำปีดัชนีชี้วัดสังคมสารสนเทศปี 2557, **สหภาพโทรคมนาคมระหว่างประเทศ (ITU)** [Online], 2557. แหล่งที่มา http://www.innnews.co.th/shownews/show?newscode=581921.

Google ได้เก็บสะสมพฤติกรรมของผู้เข้าเข้าชมเว็บไซต์ต่าง ๆ จึงถือว่าเป็นข้อมูลส่วนบุคคลที่จำเป็นต้องมีมาตรการคุ้มครอง ทั้งนี้ อาจกล่าวได้ว่าบริษัทผู้ให้บริการดังกล่าวมีการเก็บรวบรวมข้อมูลในลักษณะ Big Data ซึ่งประเด็นที่มีปัญหา คือ การละเมิดข้อมูลส่วนบุคคล การกระทำเหล่านั้นอาจส่งผลกระทบต่อวิถีชีวิตความเป็นส่วนตัวของประชาคมโลก เช่น ข้อมูลที่เกี่ยวข้องกับความสัมพันธ์ในครอบครัว ข้อมูลที่เป็นประวัติส่วนบุคคล รวมถึงข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากร ซึ่งข้อมูลดังกล่าวได้มีการเผยแพร่และเปิดเผยต่อสาธารณชนด้วยผลของเทคโนโลยีการสื่อสารที่พัฒนาไปอย่างรวดเร็ว ส่งผลให้มีทั้งผลดีและผลเสียในเวลาเดียวกัน ทั้งนี้ เนื่องจากบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลนั้นอาจไม่ประสงค์ที่จะเปิดเผยข้อมูลส่วนบุคคลในบางประเภทให้สาธารณชนได้รับรู้ เพราะอาจส่งผลกระทบต่อความปลอดภัย ชื่อเสียง ทรัพย์สิน ความสัมพันธ์ของคนในครอบครัว ชีวิตสมรส รวมถึงหน้าที่การงานของเจ้าของข้อมูลนั้นด้วย เพราะฉะนั้น การเปิดเผยข้อมูลส่วนบุคคลของบุคคลอื่นจึงถือได้ว่าเป็นเรื่องที่ละเอียดอ่อนของแต่ละบุคคลและขึ้นอยู่กับประเภทของข้อมูลส่วนบุคคลที่ได้มีการเปิดเผยออกไป

ดังนั้น การละเมิดข้อมูลส่วนบุคคลที่นำมาเผยแพร่ไว้ในเว็บไซต์เครือข่ายสังคม ซึ่งรวมถึงการนำข้อมูลไปใช้โดยมิได้รับรู้และยินยอม การคุกคามโดยการส่งข้อความ ข้อมูลต่าง ๆ เข้ามาในระบบเว็บไซต์เครือข่ายสังคม อันเป็นการรบกวนความเป็นส่วนตัวของเจ้าของข้อมูลในเว็บไซต์เครือข่ายสังคม จากสภาพปัญหาดังกล่าว ผู้ศึกษามีความเห็นว่า มีความจำเป็นต้องศึกษาแนวทางการคุ้มครอง Big Data ในกรณีความเป็นส่วนตัวและความมั่นคงปลอดภัยของข้อมูล

โดยการวิเคราะห์ระบบกฎหมายไทยในปัจจุบัน พร้อมทั้งศึกษาวิเคราะห์กฎหมายของประเทศสหรัฐอเมริกา และประเทศอังกฤษตามแนวทางของสหภาพยุโรปที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลใน Big Data เพื่อวิเคราะห์เปรียบเทียบกับกฎหมายไทยในปัจจุบัน และเพื่อเป็นแนวทางในการพัฒนามาตรการทางกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยต่อไป ผู้ศึกษาจึงดำเนินการศึกษาครั้งนี้

1.2 วัตถุประสงค์ของการศึกษา

1.2.1 เพื่อศึกษาวิเคราะห์ปัญหา และผลกระทบของการใช้ข้อมูลใน Big Data ที่เกี่ยวข้องกับความเป็นส่วนตัว และความมั่นคงปลอดภัยของข้อมูล

1.2.2 เพื่อศึกษาวิเคราะห์กฎหมายไทยที่เกี่ยวข้องกับ Big Data เรื่องความเป็นส่วนตัว และความมั่นคงปลอดภัยของข้อมูล

1.2.3 เพื่อเปรียบเทียบกฎหมายประเทศสหรัฐอเมริกา และประเทศอังกฤษตามแนวทางของสหภาพยุโรปที่เกี่ยวข้องกับ Big Data เรื่องความเป็นส่วนตัว และความมั่นคงปลอดภัยของข้อมูล อันจะนำมาสู่การวิเคราะห์เปรียบเทียบกับกฎหมายไทยที่เป็นอยู่ในปัจจุบัน

1.2.4 เพื่อเสนอมาตรการทางกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับความเป็นส่วนตัว และความมั่นคงปลอดภัยของข้อมูลใน Big Data

1.3 สมมติฐานของการศึกษา

การศึกษาแนวทางในการคุ้มครอง Big Data ในประเด็นที่เกี่ยวข้องกับความเป็นส่วนตัวและความมั่นคงปลอดภัยของข้อมูลนี้ จะทำให้ทราบถึงปัญหาของ Big Data พร้อมทั้งช่วยพัฒนากฎหมายไทยให้ครอบคลุมถึงปัญหาดังกล่าว และสามารถนำมาปรับใช้เพื่อเป็นแนวทางของกฎหมายคุ้มครองข้อมูลส่วนบุคคล ตลอดจนเพื่อให้สามารถแก้ไขปัญหาเรื่องการละเมิดข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพ และเพื่อมิให้เกิดปัญหาในทางปฏิบัติของผู้ที่ต้องปฏิบัติตามกฎหมายดังกล่าวอันเนื่องมาจากบทบัญญัติทางกฎหมายไม่ชัดเจน

1.4 ขอบเขตของการศึกษา

1.4.1 ขอบเขตด้านเนื้อหา

การศึกษานี้เป็นการศึกษาปัญหาของ Big Data และวิเคราะห์กฎหมายไทยในปัจจุบันที่เกี่ยวข้องกับความเป็นส่วนตัว และความมั่นคงปลอดภัยของข้อมูลใน Big Data รวมทั้งวิเคราะห์ปัญหาและผลกระทบจากการใช้ข้อมูลใน Big Data ศึกษากฎหมายของประเทศสหรัฐอเมริกา และประเทศอังกฤษตามแนวทางของสหภาพยุโรปที่เกี่ยวข้องกับความเป็นส่วนตัว ความมั่นคงปลอดภัยของข้อมูล และการคุ้มครองข้อมูลส่วนบุคคล อันจะนำมาสู่การวิเคราะห์เปรียบเทียบ และพัฒนากฎหมายไทย

1.4.2 ขอบเขตด้านแหล่งข้อมูล

แหล่งข้อมูลทุติยภูมิ ประกอบด้วย เอกสาร บทความ วารสาร ตำราวิชาการ แนวคิดทฤษฎีที่เกี่ยวข้องกับความเป็นส่วนตัว ความมั่นคงปลอดภัยของข้อมูล การคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย ข้อตกลงระหว่างประเทศ ประเทศสหรัฐอเมริกา และประเทศอังกฤษตามแนวทางของสหภาพยุโรป

1.5 วิธีการดำเนินการศึกษา

สารนิพนธ์ฉบับนี้ดำเนินการศึกษาโดยการค้นคว้าจากตำรากฎหมาย วิเคราะห์ข้อมูลจากหนังสือ บทความ เอกสารทางวิชาการของผู้ทรงคุณวุฒิต่าง ๆ ที่เกี่ยวข้อง รวมถึงวิทยานิพนธ์ ข้อมูลจากเว็บไซต์ โดยสืบค้นจากแหล่งข้อมูลทั้งของประเทศไทยและต่างประเทศที่เกี่ยวข้องกับความเป็นส่วนตัว ความมั่นคงปลอดภัยของข้อมูล และการคุ้มครองข้อมูลส่วนบุคคล โดยดำเนินการตามขั้นตอนดังนี้

1.5.1 ศึกษาวิเคราะห์ปัญหา และผลกระทบของการใช้ข้อมูลใน Big Data ที่เกี่ยวข้องกับความเป็นส่วนตัว และความมั่นคงปลอดภัยของข้อมูล โดยการวิเคราะห์เอกสาร

1.5.2 ศึกษาวิเคราะห์กฎหมายไทยที่เกี่ยวข้องกับ Big Data เรื่องความเป็นส่วนตัว และความมั่นคงปลอดภัยของข้อมูล โดยการวิเคราะห์เอกสาร

1.5.3 ศึกษากฎหมายต่างประเทศที่เกี่ยวข้องกับ Big Data เรื่องความเป็นส่วนตัว และความมั่นคงปลอดภัยของข้อมูล อันจะนำมาสู่การวิเคราะห์เปรียบเทียบกับกฎหมายไทยที่เป็นอยู่ในปัจจุบัน โดยการวิเคราะห์เอกสาร

1.5.4 เสนอแนวทางพัฒนามาตรการทางกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับความเป็นส่วนตัว และความมั่นคงปลอดภัยของข้อมูล กรณี Big Data โดยการรวบรวมผลการวิเคราะห์จากเอกสารทั้งหมด

1.6 ประโยชน์ที่คาดว่าจะได้รับจากการศึกษา

1.6.1 ทำให้ได้ข้อมูลเกี่ยวกับปัญหา และผลกระทบของการใช้ข้อมูลใน Big Data ที่เกี่ยวข้องกับความเป็นส่วนตัว และความมั่นคงปลอดภัยของข้อมูล

1.6.2 ทำให้ได้ข้อมูลเกี่ยวกับกฎหมายไทยที่เกี่ยวข้องกับ Big Data ในเรื่องความเป็นส่วนตัว และความมั่นคงปลอดภัยของข้อมูล

1.6.3 ทำให้ได้ข้อมูลเกี่ยวกับกฎหมายต่างประเทศที่เกี่ยวข้องกับ Big Data ในเรื่องความเป็นส่วนตัว และความมั่นคงปลอดภัยของข้อมูล อันจะนำมาสู่การศึกษาเปรียบเทียบกับกฎหมายไทยที่เป็นอยู่ในปัจจุบัน

1.6.4 หน่วยงานที่เกี่ยวข้องและประเทศไทยมีแนวทางในการพัฒนามาตรการทางกฎหมายคุ้มครองข้อมูลส่วนบุคคล ที่เกี่ยวข้องกับความเป็นส่วนตัว และความมั่นคงปลอดภัยของข้อมูล กรณี Big Data

1.6.5 หน่วยงานที่เกี่ยวข้องสามารถนำมาตรการทางกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับความเป็นส่วนตัว และความมั่นคงปลอดภัยของข้อมูลใน Big Data ไปปรับใช้ได้อย่างกว้างขวาง

บทที่ 2
ลักษณะ และบทบาทที่เกี่ยวข้องกับ Big Data

ปัจจุบันการพัฒนาด้านเทคโนโลยีได้นำโลกไปสู่ยุคไซเบอร์ที่มีการใช้ทั้งคอมพิวเตอร์ อินเทอร์เน็ต และระบบเครือข่ายเพื่อเป็นตัวขับเคลื่อนการดำเนินการต่าง ๆ ทั้งภายในและภายนอกประเทศ เช่น การพาณิชย์อิเล็กทรอนิกส์ การทำธุรกรรมอิเล็กทรอนิกส์ การใช้ระบบควบคุมบังคับบัญชาทางทหาร การสื่อสาร และโทรคมนาคม ซึ่งล้วนแล้วแต่เป็นกุญแจสำคัญต่อการพัฒนาขีดความสามารถทางเศรษฐกิจ สังคม และความมั่นคงของประเทศชาติ ซึ่งสิ่งสำคัญสำหรับการใช้คอมพิวเตอร์ อินเทอร์เน็ต และระบบเครือข่าย ก็คือข้อมูล (Data) เดิมข้อมูลในอินเทอร์เน็ต (Data in Internet) อาจจะเป็นข้อมูลที่มีโครงสร้างชัดเจน หรืออาจไม่มีโครงสร้างที่ใหญ่มากนัก จึงมีมาตรการทางกฎหมายที่สามารถเข้าไปควบคุมดูแลข้อมูลในอินเทอร์เน็ตได้ แต่ในปัจจุบันนี้คุณลักษณะของข้อมูลในอินเทอร์เน็ตกลายเป็น Big Data ซึ่งมีคุณลักษณะทั้งเชิงปริมาตร เชิงปริมาณ และมีกลไกในการกำกับ เป็นทั้งข้อมูลที่มีโครงสร้าง และไม่มีโครงสร้าง จึงยากต่อการเข้าไปควบคุมดูแลข้อมูลใน Big Data ดังนั้น ประเทศไทยจึงมีความจำเป็นอย่างยิ่งที่จะต้องเสริมสร้างความแข็งแกร่งด้านความมั่นคงปลอดภัยไซเบอร์ ความเป็นส่วนตัว และความมั่นคงปลอดภัยของข้อมูลใน Big Data ด้วยการสร้างเครือข่ายความร่วมมือในทุกภาคส่วนทั้งภาครัฐ ภาคเอกชน ภาคโทรคมนาคม และภาคอุตสาหกรรม รวมไปถึงมิตรประเทศ ในการสร้างความพร้อมของบุคลากร เครื่องมือ และกระบวนการทำงานในการรับมือการโจมตีในไซเบอร์ด้วยการวางระบบรักษาความมั่นคงปลอดภัยในการเก็บรักษาข้อมูลใน Big Data และเรื่องความเป็นส่วนตัว

ดังนั้น ผู้ศึกษาจึงเห็นว่าการศึกษานี้มีความจำเป็น เพื่อหาแนวทางการคุ้มครองข้อมูลใน Big Data ในเรื่องความเป็นส่วนตัว และความมั่นคงปลอดภัยของข้อมูลใน Big Data ตลอดจนกฎหมายที่เกี่ยวข้องเพื่อให้ทุกภาคส่วนได้เล็งเห็น และตระหนักถึงปัญหาในโลกไซเบอร์ที่เกิดขึ้น และสามารถเตรียมความพร้อมในการรับมือได้อย่างมีประสิทธิภาพ

2.1 ความหมายของคำว่า Big Data

2.1.1 ความหมายของ Big Data

สำหรับบุคคลทั่วไปอาจบอกว่า คำว่า Big Data เป็นข้อมูลขนาดใหญ่มหาศาล หรือบางคนอาจนึกถึง Google, Facebook, Twitter เป็นต้น ซึ่งนั่นเป็นมุมมองหนึ่งแต่มันยังไม่ใช่ทุกมิติทุกมุมของ Big Data เมื่อต้องทำงานกับข้อมูลขนาดใหญ่ เทคโนโลยีที่ใช้จัดการกับข้อมูลแบบเดิมคงไม่

เหมาะสมอีกต่อไป จึงต้องมีการคิดค้นเทคโนโลยีใหม่ ๆ ที่สามารถจัดการข้อมูลขนาดใหญ่ หรือ Big Data นี้ได้ ทั้งในด้านการจัดเก็บข้อมูล การสืบค้นข้อมูล และการวิเคราะห์ข้อมูล

มีผู้ให้คำนิยาม ของคำว่า Big Data คล้ายคลึงกัน คือ คำว่า Big Data นั้นถ้าแปลเป็นภาษาไทย[1] อาจได้ความหมายว่า “อภิมหาข้อมูล หรือ ข้อมูลที่มากมายมหาศาล” ซึ่งในปัจจุบันด้วยพัฒนาการของเทคโนโลยีและระบบต่าง ๆ ทำให้องค์กรที่มีการเก็บข้อมูลต่าง ๆ อย่างมากมายมหาศาล และองค์กรที่ให้ความสำคัญกับข้อมูลเหล่านี้ ก็ย่อมรู้จักที่จะนำ Big Data มาใช้ในการตัดสินใจเพื่อให้เกิดประโยชน์ต่อองค์กร มีงานวิจัยระบุว่าองค์กรที่ให้ความสำคัญกับข้อมูลในการตัดสินใจ หรือเป็นลักษณะชุดข้อมูล (Data-Driven) นั้นจะมีผลการดำเนินงานที่ดีกว่าองค์กรที่ไม่ได้ให้ความสำคัญแก่ Big Data ขององค์กรต่าง ๆ นั้นมาจากบรรดาตัวชี้วัด หรือตัววัดผลประสิทธิภาพการทำงาน (KPI) ต่าง ๆ ที่องค์กรเกือบทุกแห่งต่างเก็บกันไว้ในช่วงกว่า 10 ปีที่ผ่านมา ทำให้องค์กรได้มีข้อมูลใน Big Data ในด้านต่าง ๆ อย่างมากมาย นอกจากนี้ข้อมูลที่องค์กรทุกแห่งเก็บเป็นปกติอยู่แล้ว ไม่ว่าจะเป็นตัวเลขทางด้านการเงิน ตัวเลขทางด้านการดำเนินงาน ข้อมูลเกี่ยวกับลูกค้า ข้อมูลเกี่ยวกับพนักงาน หรือข้อมูลในระบบ ERP (Enterprise Resource Planning) ระบบฐานข้อมูล ระบบ Warehouse ฯลฯ ล้วนแล้วแต่เป็นแหล่งสำคัญของ Big Data ทั้งสิ้น ที่สำคัญคือปริมาณของข้อมูลเหล่านี้กลับทวีปริมาณมากขึ้นทุกขณะ ในปี 2012 ข้อมูลจำนวน 2.5 Exabytes ถูกสร้างขึ้นมาในแต่ละวัน (1 Exabyte เทียบเท่ากับ 1,000 ล้าน Gigabytes)[2]

ในขณะที่ ณรงค์ฤทธิ์ มโนมัยพิบูลย์[3] ให้คำจำกัดความว่า Big Data หมายถึง ปริมาณข้อมูลที่มีขนาดใหญ่มหาศาลเกินกว่าขีดความสามารถในการประมวลผลของระบบฐานข้อมูลธรรมดาที่จะรองรับได้ปริมาณข้อมูลที่มีขนาดใหญ่มาก ๆ จะมีอัตราการเพิ่มข้อมูลได้อย่างรวดเร็วมากและจะมีรูปแบบที่ไม่โครงสร้างหรือกึ่งโครงสร้าง ซึ่งไม่สามารถอยู่ในระบบฐานข้อมูลที่จะจัดเก็บข้อมูลได้[4]

---

[1] ชูชาติ หฤไชยะศักดิ์, **What is Big Data?** [Online], 7 กุมภาพันธ์ 2557. แหล่งที่มา http://www.datamininginnovation.com/wp-content/uploads/2014/02/What_is_big_data.pdf.

[2] พสุ เดชะรินทร์, **Big Data หรืออภิมหาข้อมูล** [Online], 2556. แหล่งที่มา http://library.acc.chula.ac.th/PageController.php?page=FindInformation/ArticleACC/2556/Pasu/BangkokBiznews/B2901131.

[3] ณรงค์ฤทธิ์ มโนมัยพิบูลย์, **“Big Data” is (now) all around Big Data** [Online], 2556. แหล่งที่มา http://www.g-able.com/portal/page/portal/g-able/thai/it_talks/Y2013/it_talks_V34_02/G-Magz_V34_2.pdf.

[4] Dumbill, E., **What is a Big Data?: An introduction to the big data landscape** [Online], 2012. Available from http://radar.oreilly.com/2012/01/what-is-big-data.html.

Big Data เป็นการจัดเก็บรวบรวมและวิเคราะห์ข้อมูลอย่างแม่นยำและรวดเร็ว ทั้งภาพ เสียง ตัวอักษร ตัวเลข และอื่น ๆ ที่มีความหลากหลาย และมากมายจนระบบฐานข้อมูลเดิมไม่สามารถจัดการได้ ตลอดจนเป็นข้อมูลที่มาจากแหล่งต่าง ๆ ทั้ง Internet, Social Network, Smart phone, Tablet แม้กระทั่งข้อมูลเวชระเบียน หรือพาณิชย์อิเล็กทรอนิกส์ขนาดใหญ่ รวมถึง มีการจัดเก็บข้อมูลชนิดที่มีระบบทดแทน เป็นการให้บริการแบบกระจาย การประมวลผลข้อมูลเป็นแบบขนาน ประมวลผลข้อมูลข่าวสารที่มีขีดความสามารถแบบ Map Reduce (การแบ่งข้อมูลเป็นส่วน ๆ ในขนาดที่เท่า ๆ กัน) หรือเทียบเท่า มีการบริหารจัดการแบบรวมศูนย์และเป็นระบบผสานการทำงานกับทรัพยากรประมวลผลต่าง ๆ สามารถในการเข้าถึงข้อมูลและใช้งานง่าย มีความพร้อมของข้อมูลอยู่เสมอ และมีขีดความสามารถในการให้บริการจะต้องสามารถแปรผันไปตามความต้องการใช้งานเสมอ ซึ่งองค์ประกอบหลักในการประมวลผลมี 2 องค์ประกอบ ได้แก่

1) เครื่องมือที่ช่วยในการวิเคราะห์ (Analytics) ประกอบด้วย ซอฟต์แวร์ สำหรับวิเคราะห์และเชื่อมต่อ (Tools) และเทคโนโลยีในการประมวลผลข้อมูล (Engine) ที่ทันสมัย

2) นักวิเคราะห์ข้อมูล (Data Scientist) ที่มีความรอบรู้เกี่ยวกับข้อมูลแต่ละประเภท เข้าใจความสัมพันธ์ และสามารถประมวลผลข้อมูลได้อย่างละเอียด

สรุปได้ว่า Big Data ที่อยู่ในงานวิจัยฉบับนี้ หมายถึง ข้อมูลขนาดใหญ่ที่อยู่ในเครือข่าย เป็นข้อมูลที่มีหลายรูปแบบ ไม่ได้มีเพียงรูปแบบเดียว เป็นข้อมูลที่มีที่มาจากแหล่งที่หลากหลาย เช่น ข้อมูลจากในองค์กร ข้อมูลจาก Social Media ข้อมูลจาก Web E-Commerce ข้อมูลจาก Smart phone หรือข้อมูลจาก Sensor Device เป็นต้น ซึ่งข้อมูลเหล่านี้สามารถรวบรวม และนำมาวิเคราะห์ได้ เป็นทั้งข้อมูลที่มีโครงสร้าง และไม่มีโครงสร้าง และในเมื่อ Big Data เป็นข้อมูลขนาดใหญ่ที่มีหลายรูปแบบ อยู่ในหลายผู้ให้บริการ จึงทำให้ไม่สามารถจัดการได้ เพราะฉะนั้นโอกาสที่จะใช้เครื่องมือใดเครื่องมือหนึ่งเข้าไปจัดการ Big Data เพื่อให้มีการคุ้มครองข้อมูลจึงเป็นไปได้ยาก

ในมุมมองของผู้ใช้บริการ ผู้ให้บริการอาศัยความยินยอมของผู้ใช้บริการเป็นสำคัญ ซึ่งทำให้ผู้ให้บริการสามารถนำข้อมูลของผู้ใช้บริการไปใช้วิเคราะห์ได้ ซึ่งแนวทางการคุ้มครองข้อมูลใน Big Data นั้น ผู้ศึกษาเห็นว่าควรที่จะออกกฎหมายเพื่อกำหนดกฎเกณฑ์ให้เป็นมาตรฐานเป็นการเฉพาะเพื่อกำกับดูแลผู้ให้บริการในการดูแลข้อมูลในส่วนนี้ และในหลาย ๆ ส่วน ที่เรียกว่า ข้อมูลที่เปิดเผยเป็นสาธารณะ ซึ่งเป็นข้อมูลที่บุคคลทั่วไปสามารถเข้าถึงได้

2.1.2 ลักษณะของ Big Data

Gregory Piatetsky[5] หนึ่งในผู้ก่อตั้ง KDDConference และ KDnuggets (เครื่องมือที่ใช้ในการวิเคราะห์ Big Data) ให้คำนิยามว่า “Data is big when data size becomes part of the problem” จากข้อความดังกล่าวให้ข้อสังเกตเกี่ยวกับ Big Data ว่า หากข้อมูลที่มีอยู่ในองค์กรไม่สามารถจัดการได้ด้วยเทคโนโลยีที่มีอยู่แล้ว หรือเริ่มมีปัญหาเกี่ยวกับการจัดการข้อมูล คือ ข้อมูลขนาดใหญ่ หลากหลาย เปลี่ยนแปลงรวดเร็ว ยากต่อการนำมาประมวลผลและวิเคราะห์ เมื่อนั้นคุณเริ่มเผชิญกับปัญหา Big Data แล้ว ปัญหาที่เกิดขึ้นอาจจะเป็นระบบจัดเก็บข้อมูล (Storage) ที่มีอยู่เริ่มไม่พอ Speed ที่ใช้ในการประมวลผลมีประสิทธิภาพแย่ลง เป็นต้น

ภาพที่ 2.1: คุณลักษณะของ Big Data[6]

ที่มา: Orlova, A. (2014). *Telcos Gain Valuable Insight with “Big Data”*. Retrieved from http://blog.azoft.com/telcos-gain-valuable-insight-with-big-data/.

1) ปริมาตร (Volume) คือ ปริมาณข้อมูลจะมีขนาดใหญ่ตั้งแต่ระดับ Terabytes (1 TB = 10^{12} bytes) Petabytes (1 PB = 10^{15} bytes) ไปจนถึง Zettabytes (1 ZB = 10^{21} bytes) ยกตัวอย่างเช่น ข้อมูล Google ที่มีปริมาณมหาศาล

---

[5] Fayyad, U., Piatetsky-Shapiro, G., & Smyth, P., **From Data Mining to Knowledge Discovery in Databases** [Online], 1996. Available from http://www.csd.uwo.ca/faculty/ling/cs435/fayyad.pdf.

[6] Laney, D., **3D Data Management: Controlling Data Volume, Velocity, and Variety** [Online], 6 February 2013. Available from http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf.

2) ความเร็ว (Velocity) มีการให้ความสำคัญ ความน่าสนใจกับข้อมูลประเภท Real Time อย่างมากว่าจะนำมาใช้ประโยชน์ได้อย่างไร แต่ก็ไม่ได้ละเลยข้อมูลประเภทอื่น เช่น Tweeter เป็นต้น

3) ความจริง (Variety) ชนิดของข้อมูลที่มีความหลากหลายไม่ว่าจะเป็นข้อมูลที่มีโครงสร้าง (Structured Data) หรือ ข้อมูลที่ไม่มีโครงสร้าง (Unstructured Data) โดยเฉพาะ Unstructured Data ซึ่งเป็นข้อมูลที่ถูกพูดถึงพร้อม Big Data เช่น ข้อมูล Text Video Image Links ที่มีการผสมผสานหลายรูปแบบ

เมื่อกล่าวถึง Big Data ตามนิยามแรกเริ่มเดิมทีของ Doug Laney (Vice President ของบริษัท Gartner) จะมี 3 มุม หรือ 3Vs แต่ IBM[7] เสนอมุมมองอีกเรื่องคือความไม่แน่นอนของข้อมูลเป็นอีกมิติที่ควรพิจารณาเมื่อต้องทำงานกับข้อมูล Big Data

1) Volume (Scale of Data) หมายถึง ขนาดของข้อมูล เช่น Terabytes Zettabytes

2) Velocity (Analysis of Streaming Data) หมายถึง การเปลี่ยนแปลง การเคลื่อนไหวของข้อมูล

3) Variety (Different form of Data) หมายถึง ความหลากหลายของข้อมูล มีการผสมผสานของข้อมูลหลาย ๆ ประเภท เช่น ข้อความ Video Streaming ภาพ เสียง Sensor เป็นต้น

4) Veracity (Uncertainty of Data) หมายถึง ความไม่แน่นอนของข้อมูลที่เข้ามา

เนื่องจากข้อมูลที่เราใช้ อาจมาจากหลายแหล่งข้อมูล ซึ่งแต่ละแหล่งข้อมูลนั้นอาจจะมีการนิยามลักษณะข้อมูลที่ต่างกัน หรือข้อมูลมีลักษณะไม่เหมือนกันแต่มีความหมายเดียวกัน เป็นต้น สิ่งเหล่านี้อาจจะเกิดจากความตั้งใจของผู้ให้ข้อมูล เช่น ใช้นามแฝง ตัวย่อ แทนชื่อจริง หรือเกิดจากการพิมพ์ข้อมูลผิด ซึ่งลักษณะ Noise ที่เกิดขึ้นเหล่านี้ มีโอกาสพบมากในแหล่งข้อมูลที่สามารถให้ผู้ใช้งานระบุข้อมูลเองได้ เช่น ข้อมูลจาก Twitter ข้อมูล Comment หรือ Review จากเว็บไซต์ เป็นต้น ดังนี้

จึงอาจแบ่ง Big Data ออกเป็น 2 แบบใหญ่ ๆ คือ

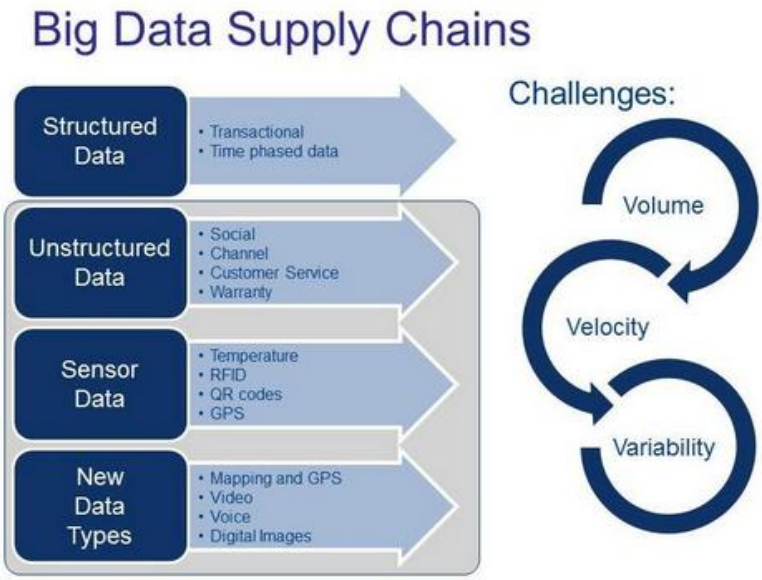
1) ข้อมูลที่มีโครงสร้าง (Structured Data) อาจเป็นข้อมูล Transaction ซื้อขาย ที่บันทึกได้จาก Point of Sales (POS) ข้อมูลจาก Log (การใช้อินเทอร์เน็ต) ข้อมูล Banking (การทำธุรกรรมทางการเงิน) ข้อมูล Financial Stock Market (ตลาดหุ้น) ข้อมูลการใช้งานโทรศัพท์ ข้อมูลจาก Sensor (ตำแหน่ง) เป็นต้น

---

[7] Melodia, M., & Smith, R., “Defending BIG DATA”, **LTN LAW TECHNOLOGY NEWS** [Online], (October 2012): 3. Available from http://www.reedsmith.com/files/News/f6b538a3-7681-40a2-b2bd-ab653940bab5/Presentation/NewsAttachment/f55071a4-b28a-49df-a396-ac3f4403205c/LTN%20October%202012%20-%20Data%20Privacy.pdf.

2) ข้อมูลที่ไม่มีโครงสร้าง (Unstructured Data) ก็พวกข้อมูล Text ที่มาจาก Twitter หรือ Facebook ข้อมูล Email ข้อมูลสอบถามหรือร้องเรียนจาก Call Center ข้อมูลรูปภาพ ข้อมูลข่าว หรือแม้แต่พวกไฟล์เสียง วีดีโอ จาก YouTube เป็นต้น ซึ่งเทคโนโลยีที่ใช้ในการวิเคราะห์ข้อมูลเหล่านี้ก็คือ Text Mining

ภาพที่ 2.2: Big Data Supply Chains (ห่วงโซ่อุปทานของ Big Data)



ที่มา: Big Data Supply Chains: Volume, Variety, Velocity and Veracity. (n.d.). Retrieved from http://www.rosebt.com/blog/big-data-supply-chains-volume-variety-velocity-and-veracity.

สุดท้ายผลลัพธ์ที่ได้จากการวิเคราะห์อาจถูกนำเสนอในรูปแบบของรายงาน Dashboard Visualization ต่าง ๆ ซึ่งเป็นการรวบรวม และเสนอสารสนเทศให้ง่ายต่อการอ่าน เช่น การเสนอลูกบาศก์หลายมิติสู่ภาพเสมือนจริง Strategy ทางการตลาด หรือ Application นั่นเอง โดย 88% ของข้อมูล Transaction ในองค์กรจะถูกนำมาวิเคราะห์ เช่น การหารูปแบบการซื้อสินค้า (Association Rule) หรือการจัดกลุ่มลูกค้า (Customer Segmentation) เพื่องานทางด้านการตลาด ส่วน 73% ของข้อมูล Log (การใช้อินเทอร์เน็ต)[8] ถูกนำมาใช้ในการวิเคราะห์พฤติกรรม หรือความสนใจสินค้า เช่น ใน Amazon มีการติดตามพฤติกรรมการเลือกชม และซื้อสินค้า ส่วนข้อมูล

[8] Ibid, 2.

E-mail ถูกนำมาวิเคราะห์น้อยมาก เนื่องจากข้อมูล E-mail แตกต่างจากข้อมูลสองประเภทข้างต้น โดยข้อมูล E-mail เป็นลักษณะของข้อมูลที่ไม่เป็นโครงสร้าง จึงยากต่อการนำไปวิเคราะห์นั่นเอง รวมทั้งข้อมูลที่ได้จากเว็บไซต์ หรือ Social Media ของบริษัทหรือองค์กรเอง ก็ถูกนำมาใช้ในการวิเคราะห์น้อยอยู่ เนื่องจากเป็นข้อมูลแบบไม่มีโครงสร้างเช่นกัน[9]

ตารางที่ 2.1: ตารางแสดงคุณลักษณะของ Big Data

TABLE 1: CHARACTERISTICS OF BIG DATA

Characteristic	Description	Attribute	Driver
Volume	The sheer amount of data generated or data intensity that must be ingested, analyzed, and managed to make decisions based on complete data analysis	According to IDC's Digital Universe Study, the world's "digital universe" is in the process of generating 1.8 Zettabytes of information - with continuing exponential growth – projecting to 35 Zettabytes in 2020	Increase in data sources, higher resolution sensors
Velocity	How fast data is being produced and changed and the speed with which data must be received, understood, and processed	• Accessibility: Information when, where, and how the user wants it, at the point of impact • Applicable: Relevant, valuable information for an enterprise at a torrential pace becomes a real-time phenomenon • Time value: real-time analysis yields improved data-driven decisions	• Increase in data sources • Improved thru-put connectivity • Enhanced computing power of data generating devices
Variety	The rise of information coming from new sources both inside and outside the walls of the enterprise or organization creates integration, management, governance, and architectural pressures on IT	• Structured – 15% of data today is structured, row, columns • Unstructured – 85% is unstructured or human generated information • Semistructured – The combination of structured and unstructured data is becoming paramount. • Complexity – where data sources are moving and residing	• Mobile • Social Media • Videos • Chat • Genomics • Sensors
Veracity	The quality and provenance of received data	The quality of Big Data may be good, bad, or undefined due to data inconsistency & incompleteness, ambiguities, latency, deception, model approximations	Data-based decisions require traceability and justification

ที่มา: Demystifying BIG DATA., (n.d.). *TechAmerican Foundation: Federal Big Data Commission*, 11. Retrieved from https://www304.ibm.com/industries/ publicsector/ fileserve?contentid=239170.

[9] Ibid.

จากตารางสามารถสรุปลักษณะของ Big Data ได้ดังนี้

1) ปริมาตร (Volume) หมายถึง ข้อมูลที่มีปริมาณมหาศาลซึ่งโครงสร้างข้อมูลของระบบฐานข้อมูลไม่สามารถจัดเก็บข้อมูลได้ปริมาณข้อมูลมหาศาลมีประโยชน์เพื่อเป็นข้อมูลที่ใช้ในการตัดสินใจ หรือทำนายอนาคต หรือเพื่อเตรียมการวางแผนการทำงานเชิงรุกทางธุรกิจ

การประมวลผลปริมาณของข้อมูลที่มีขนาดใหญ่กว่าการจัดการโดยโครงสร้างพื้นฐานของฐานข้อมูลเชิงสัมพันธ์ (Relational Database) ใช้สถาปัตยกรรมของการประมวลผลของกลุ่มข้อมูลที่มีขนาดมหาศาล โดยจะทำไปพร้อม ๆ กันระหว่างคลังข้อมูล (Data Warehouse) หรือฐานข้อมูล (Database) และซอฟต์แวร์ Hadoop ซึ่งเป็นเทคโนโลยีที่สามารถเก็บข้อมูลขนาดใหญ่ และสามารถนำมาประมวลผลได้

2) ความเร็ว (Velocity) หมายถึง อัตราการเพิ่มขึ้นของข้อมูล ข้อมูลที่เข้าสู่ระบบฐานข้อมูลจะมีอัตราการเพิ่มขึ้นอย่างรวดเร็ว เช่น ข้อมูลที่เกิดขึ้นจากโทรศัพท์เคลื่อนที่ที่ผู้ใช้นำขึ้นเก็บเป็นข้อมูลภาพถ่าย ข้อมูลการพิมพ์การสนทนา ข้อมูลการอัดภาพวิดีโอหรือข้อมูลการอัดเสียงหรือแม้กระทั่งข้อมูลการสั่งซื้อสินค้าการขนส่ง และการบริการต่าง ๆ ก็สามารถนำข้อมูลเหล่านั้นเข้าสู่ระบบฐานข้อมูลได้อย่างรวดเร็ว

จากการที่เทคโนโลยีได้พัฒนาก้าวไกลในโลกออนไลน์และถูกนำมาใช้ในธุรกิจและการดำเนินชีวิตประจำวันทำให้ปริมาณข้อมูลที่ผ่านเข้ามาทางเทคโนโลยีต่าง ๆ เหล่านั้น เข้าสู่ระบบฐานข้อมูลได้ง่าย รวดเร็ว และเพิ่มปริมาณข้อมูลมากขึ้น และทำให้การประมวลผลทำได้อย่างยากลำบากดังนั้นจึงต้องหาวิธีประมวลผลข้อมูลให้มีผลดีและถูกต้อง เพื่อหาผลลัพธ์ที่ต้องการหรือมีการพิจารณาการประมวลผลในขณะที่ข้อมูลนั้นไหลเข้าสู่ระบบฐานข้อมูล

การพิจารณาประมวลผลข้อมูลที่ไหลเข้ามา (Streaming Processing) มี 2 หลักการ หลักการแรก คือ เมื่อข้อมูลเข้ามาสู่ระบบฐานข้อมูลอย่างรวดเร็วจะมีการจัดลำดับข้อมูลเข้าไปในการจัดเก็บข้อมูลตามความต้องการ และปฏิบัติตามลำดับของการวิเคราะห์ที่เกิดขึ้นจากการเคลื่อนย้ายของข้อมูล ในที่สุดก็จะมีการจัดการในการจัดเก็บข้อมูล โดยจะไม่เก็บข้อมูลที่ไม่ต้องการนั้นลงไปในฐานข้อมูล ส่วนหลักการที่สอง คือพิจารณาการเคลื่อนย้ายของข้อมูลแอพพลิเคชั่น (Application) ที่สามารถใช้สร้างปฏิสัมพันธ์กับข้อมูลทันที เช่น Mobile Application (โปรแกรมประยุกต์บนอุปกรณ์สื่อสารที่ใช้ในการพกพา) และเกมออนไลน์ เป็นต้น ประเภทของผลิตภัณฑ์ที่ใช้เกี่ยวกับการทำงานของข้อมูลที่ไหลเข้ามา (Streaming Data) อาทิ IBM’s Info Sphere Stream Twitter’s Storm และ Yahoo S4 เป็นต้น

3) รูปแบบที่หลากหลาย (Variety) หมายถึง รูปแบบมีความหลากหลายของรูปแบบข้อมูลซึ่งอาจจะเป็นรูปแบบที่มีโครงสร้างไม่มีโครงสร้าง และกึ่งมีโครงสร้าง เป็นต้น รูปแบบที่ไม่มีโครงสร้าง

หรือกึ่งโครงสร้างจะไม่เหมือนข้อมูลที่เราจัดเก็บไว้ในระบบฐานข้อมูล เช่น ข้อความ E-mail รูปภาพ วิดีโอ และเสียง เป็นต้น ซึ่งข้อมูลเหล่านี้มีความซับซ้อน และเชื่อมโยงกัน

4) ความจริง (Veracity) หมายถึง คุณภาพของข้อมูลขนาดใหญ่จะดีหรือไม่ดีนั้น อาจเกิดจากการไม่สอดคล้องของข้อมูล ข้อมูลไม่สมบูรณ์ หรือในรูปแบบที่ใกล้เคียงกัน

2.2 บทบาทของ Big Data[10]

การนำ Big Data เข้ามามีส่วนร่วมในชีวิตประจำวันของเราในด้านต่าง ๆ ยกตัวอย่างเช่น ด้านสุขภาพ ด้านระบบการขนส่ง อุตสาหกรรม Logistics การปฏิรูประบบการทำงานรัฐบาล และการโทรคมนาคม เป็นต้น ซึ่งอธิบายได้ดังต่อไปนี้

2.2.1 บทบาทของ Big Data ด้านสุขภาพ[11]

ด้านสุขภาพและสาธารณสุข ใช้ข้อมูลใน Big Data ประกอบการรักษาผู้ป่วย เช่น ข้อมูลประวัติผู้ป่วย ประวัติการรักษาพยาบาล ประวัติการแพ้ยา หรือข้อมูลประวัติครอบครัวที่ใช้ประกอบการวิเคราะห์ ผู้ผลิตยาและเวชภัณฑ์ ใช้ข้อมูลมากและหลากหลายเพื่อหาสาเหตุของการเจ็บป่วยที่แท้จริง การวิเคราะห์เพื่อจำเพาะเจาะจงกลุ่มผู้ป่วยที่จะทดลองและติดตามผลของการรักษาจากยาและเวชภัณฑ์ที่พัฒนาขึ้นใหม่ และเพื่อการพัฒนากลยุทธ์ด้านการตลาดของยานั้น ๆ ใช้การวิเคราะห์ลักษณะรูปแบบการแพร่เชื้อ เพื่อใช้ในงานวิจัยทางการแพทย์ วิเคราะห์คุณภาพในการดูแลรักษาผู้ป่วย เป็นต้น

แบบจำลองการคาดการณ์ (Prediction Model) ช่วยวิเคราะห์ข้อมูลใน Big Data จากข้อร้องเรียนของคนไข้ ใบสั่งยา และสำมะโนประชากร เพื่อหาว่าสมาชิกคนใดของโรงพยาบาลหรือที่ทำประกันไว้มีโอกาสที่จะต้องเข้าใช้บริการห้องฉุกเฉิน ซึ่งแน่นอนมีค่าใช้จ่ายที่สูง จากข้อมูลเดิมที่มีอยู่เป็นพื้นฐานสร้างเครื่องมือให้เป็นมาตรฐานในการคาดการณ์การเข้าใช้บริการด้านสุขภาพในอนาคตได้

อย่างไรก็ตามทางผู้ให้บริการประกันภัยเพิ่มข้อมูลประกอบมากขึ้นเพื่อปรับปรุงแบบจำลองด้วยข้อมูลใน Big Data จากรายได้ของครอบครัว ระดับการศึกษา สถานภาพการสมรส เชื้อชาติ จำนวนเด็กในบ้าน และจำนวนรถยนต์ เป็นต้น สิ่งที่กล่าวมาดูจะเป็นข้อมูลเบื้องต้นที่เรามักเห็นได้ทั่วไป แต่การนำเอาข้อมูลการสั่งซื้อของให้ส่งถึงบ้าน การใช้อินเทอร์เน็ต ดูเป็นข้อมูลใหม่ที่แตกต่าง

---

[10] Ibid, 13-15.

[11] **The Big data revolution in healthcare: Accelerating value and innovation** [Online], January 2013. Available from http://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/ healthcare %20systems%20and%20services/pdfs/the_big_data_revolution_in_healthcare.ashx.

จากที่เราคุ้นเคยมา แน่นอนย่อมมีการปรับให้เหมาะสม การสั่งของขนาดใหญ่มาส่งถึงบ้าน หรือการอาศัยอยู่ในบริเวณที่การสัญจรเข้าออกได้ยาก ปัจจัยเหล่านี้ย่อมต้องนำมาพิจารณาปรับเปลี่ยนให้เหมาะสมด้วย

นอกจากนี้ การวิเคราะห์ Big Data[12] เข้ามาช่วยให้สามารถจัดกลุ่มคนไข้ได้ดีขึ้น และมอบหมายผู้ประสานงานด้านสุขภาพเฉพาะเข้าดูแลกลุ่มที่มีความเสี่ยงสูง ซึ่งอาจเป็นโรคเรื้อรังอยู่และรับการรักษาอย่างไม่เหมาะสมเท่าที่ควร การได้ปรึกษาแพทย์ด้วยการยื่นมือเข้าไปจัดการได้ก่อน ย่อมดีกว่าการรอให้ระเบิดเวลาทำงาน เพราะไม่ทราบว่าจะเกิดขึ้นเมื่อไร อาทิเช่น การช่วยแยกแยะหาผู้ที่มีความเสี่ยงเป็นโรคหอบหืด ที่ยังไม่มีอุปกรณ์ช่วยหายใจ การบริหารจัดการได้ก่อนที่จะต้องส่งมาห้องฉุกเฉินด้วยอาการเฉียบพลัน ซึ่งจากการวิเคราะห์ข้อมูลใน Big Data อาจพบว่าผู้ป่วยรายใด เข้าข่ายมีความเสี่ยงจะเกิดโรค ก็สามารถส่งข้อความชักจูงให้มารับคำปรึกษาได้เพิ่มเติม ก่อนที่จะเจ็บป่วยไปมากกว่าที่ควรจะเป็น ผลจากการวิเคราะห์ข้อมูลใน Big Data สามารถแสดงความน่าจะเป็นว่าคนไข้รายใดมีโอกาสเป็นโรคที่มีคนเป็นกันมาก เช่น เบาหวาน หรือการที่จะต้องกลับเข้ามารักษาซ้ำอีกครั้ง ซึ่งเป็นเหตุการณ์ที่ไม่พึงประสงค์ของทุกฝ่าย เครื่องมือทางไอที เข้ามาช่วยหาคนไข้รายที่มีโอกาสต้องกลับเข้ามารักษาใหม่อีกครั้ง และทำการปรับการรักษาให้เหมาะสมมากยิ่งขึ้น

2.2.2 บทบาทของ Big Data ทางด้านระบบการขนส่ง และอุตสาหกรรม Logistics[13]

ด้านระบบการขนส่ง ใช้ข้อมูลการจราจรในขณะนั้น ว่าไปทางไหนจะเปลืองพลังงานมากกว่าเปลืองเวลามากกว่า เนื่องจากผู้ใช้ถนนสามารถแบ่งปันข้อมูลแบบ Real Time ใน Big Data ว่าการจราจรหนาแน่นที่ไหน อีกทั้งยังสามารถช่วยลดอุบัติเหตุได้อีกด้วย

อุตสาหกรรม Logistics ได้ใช้การวิเคราะห์ข้อมูลจาก Big Data เพื่อได้ให้ข้อมูลภาพรวมเกี่ยวกับปัญหาที่คาดว่าจะเกิดขึ้นในระบบห่วงโซ่อุปทาน (Supply Chain) ของลูกค้าได้ล่วงหน้า ระบบวิเคราะห์ข้อมูลใน Big Data (Big Data Analytics) ก่อให้เกิดประโยชน์ด้านเศรษฐกิจต่ออุตสาหกรรม Supply Chain อย่างแท้จริง การรวบรวมข้อมูลและการประเมินผลจะช่วยปกป้องและเพิ่มประสิทธิภาพให้แก่ระบบ Supply Chain ส่งผลให้ธุรกิจสามารถปฏิบัติงานได้อย่างราบรื่น รวมถึงสร้างความพึงพอใจให้แก่ลูกค้าได้อย่างเต็มประสิทธิภาพและยั่งยืน ซึ่งระบบวิเคราะห์ข้อมูลใน Big

---

[12] **Telecom and innovation journal** [Online], 2013. Available from http://www.telecomjournalthailand.com/.

[13] **BIG DATA IN LOGISTICS: A DHL perspective on how to move beyond the hype** [Online], December 2013. Available from http://www.dhl.com/content/dam/downloads/g0/about_us/logistics_insights/DHL_Logistics-TrendRadar_2014.pdf.

Data (Big Data Analytics) สามารถนำมาใช้ประโยชน์ได้ถึง 2 ด้าน คือ เพิ่มประสิทธิภาพการดำเนินงาน และมีศักยภาพในการนำมาประยุกต์ใช้สร้างสรรค์แบบจำลองธุรกิจใหม่ ๆ

2.2.3 บทบาทของ Big Data ต่อการปฏิรูประบบการทำงานรัฐบาล[14]

มีความเป็นไปได้อย่างมากในอนาคตที่หน่วยงานรัฐบาลสหรัฐฯจะใช้ Big Data เพื่อรองรับการเติบโตของข้อมูล ความสามารถในการรับข้อมูลเชิงลึก และสร้างสรรค์นวัตกรรมรูปแบบใหม่ ซึ่งบทบาทของ Big Data ต่อรัฐบาลสหรัฐอเมริกา มีรายละเอียดดังต่อไปนี้

1) การเสริมสร้างการรักษาความปลอดภัยและป้องกันการทุจริต

ในเดือนพฤษภาคม ค.ศ. 2012 The multi-agency Medicare Fraud Strike Force ได้เปิดเผยถึงการปราบปรามทุจริตครั้งประวัติศาสตร์ของระบบประกันสุขภาพสหรัฐฯ โดยมีการเรียกเก็บเงินที่เป็นเท็จจำนวน 452 ล้านเหรียญสหรัฐฯ ซึ่งเจ้าหน้าที่ FBI David Welker กล่าวว่า งบประมาณของระบบประกันสุขภาพรายปีที่มีมูลค่ากว่า 2.5 ล้านล้านเหรียญสหรัฐฯ จำนวนร้อยละ 3 ถึงร้อยละ 10 มีการทุจริต

ดังนั้น Big Data จะสามารถเข้ามาช่วยในการตรวจสอบทุจริต โดยจะมีผู้เชี่ยวชาญที่คอยใช้ข้อมูลใน Big Data เพื่อวิเคราะห์รูปแบบและกิจกรรมที่ผิดปกติ เพื่อป้องกันภัยคุกคามได้อย่างทันการณ์ รวมถึงคอยระวังพฤติกรรมที่น่าสงสัยโดยอาศัยการวิเคราะห์ข้อมูลการทุจริตในอดีต

นอกจากนี้ Big Data ยังถูกใช้เพื่อวิเคราะห์และโต้ตอบต่อภัยคุกคามอย่างทันท่วงที เช่น ศูนย์บัญชาการกระทรวงความมั่นคงแห่งมาตุภูมิสหรัฐฯ ใช้ Big Data ในการวิเคราะห์และตรวจสอบสินค้าที่เข้าออกประเทศ

2) การพัฒนาการให้บริการและการตอบสนองแบบฉับพลัน

Big Data ช่วยส่งเสริมให้หน่วยงานรัฐบาลสามารถทำงานได้อย่างเต็มประสิทธิภาพอย่างชาญฉลาด และมีความคล่องตัวมากขึ้น ในระดับมลรัฐและท้องถิ่น Big Data ช่วยในการตรวจสอบระบบการขนส่งที่ซับซ้อน การวิเคราะห์แบบฉับพลันช่วยให้เจ้าหน้าที่สามารถคาดการณ์และป้องกันปัญหาที่อาจมีผลกระทบต่อระบบการคมนาคมของประเทศ และสามารถบรรเทาการแออัดของจราจรและปัญหาของการขนส่งอื่น ๆ นอกจากนี้ รัฐบาลยังสามารถนำ Big Data มาพัฒนา ระบบการขึ้นเรื่องร้องทุกข์ (โทร 311) และการแจ้งเหตุร้ายฉุกเฉิน (โทร 911) โดยวิเคราะห์ข้อมูลที่เกิดจากการส่งข้อความ การติดต่อทางโทรศัพท์ และการพิมพ์ข้อมูลบน Social Network เพื่อให้รัฐบาลสามารถตอบสนองและเตรียมการต่อเหตุร้ายได้ทันท่วงที รวมถึงพัฒนากลไกการเก็บข้อมูลและกระบวนการในการแจ้งเหตุ

---

[14] Cull, B., **3 ways big data is transforming government** [Online], 25 September 2013. Available from http://fcw.com/articles/2013/09/25/big-data-transform-government.aspx.

3) การสร้างความเป็นประชาธิปไตยทางข้อมูล

อาทิ การแจ้งเหตุร้ายฉุกเฉิน (โทร 911) ที่เป็นระบบที่เปิดเผยข้อมูลสู่สาธารณะ ดังนั้น ข้อมูลใน Big Data เหล่านั้น เปรียบเสมือนแหล่งข้อมูลที่สำคัญของนักพัฒนาและกลุ่มคนต่าง ๆ ที่ต้องการสร้างโปรแกรมประยุกต์ให้แก่รัฐบาล

เมื่อเร็ว ๆ นี้ รัฐบาลของประธานาธิบดีโอบามา ใช้ระบบ Open-Data Executive Order ในการพัฒนาระบบทางความคิด และการแนะแนวทางในการทำงานแก่หน่วยงานราชการต่าง ๆ นอกจากนี้ ยังเป็นแบบอย่างที่ดีต่อหน่วยงานอื่น ๆ ของภาครัฐ ยกตัวอย่างเช่น ในอุตสาหกรรมการบริการสุขภาพ เริ่มมีการเปิดเผยข้อมูลใน Big Data มากขึ้น ซึ่งประชาชนสามารถเข้าไปศึกษาว่าโรงพยาบาลแต่ละแห่งมีความเชี่ยวชาญในด้านอะไร และมีการจัดเก็บค่าบริการประมาณเท่าไร เพื่อให้สามารถเข้ารับการรักษาในโรงพยาบาลที่เหมาะสมที่สุด ทั้งในด้านประสิทธิภาพและราคา

การที่รัฐบาลพยายามขยายการใช้ Big Data ซึ่งจะทำให้การเปิดเผยข้อมูลเป็นเรื่องปกติ เนื่องจาก ประชาชน ภาคธุรกิจ และผู้ออกกฎหมายได้ร่วมค้นหาวิธีการ และพัฒนาการปกครองประเทศ ถึงแม้ว่าอำนาจตัดสินใจจะขึ้นอยู่กับรัฐบาลแต่ประชาชนจะมีบทบาทร่วมในการตัดสินใจว่าจะใช้ข้อมูลใน Big Data อย่างไรเพื่อทำให้รัฐบาลมีความปลอดภัย มีประสิทธิภาพ และเปิดเผย

2.2.4 บทบาทของ Big Data ต่อการโทรคมนาคม[15]

หลังจากติดตั้งเครื่องมือการวิเคราะห์ข้อมูลใน Big Data (Big Data Analytics) ผู้ให้บริการระบบโทรคมนาคมจะมีขีดความสามารถใหม่ ๆ ที่จะเพิ่มรายได้ และสร้างความพึงพอใจแก่ลูกค้า อีกทั้งลดค่าใช้จ่าย ขีดความสามารถนี้ประกอบด้วย

1) การให้บริการด้านตำแหน่งทางภูมิศาสตร์ (Location-based Services)

ผู้ให้บริการสามารถบ่งบอกตำแหน่งที่อยู่ของลูกค้าได้อย่างแม่นยำในลักษณะข้อมูล Real ธ Time ใน Big Data ซึ่งจะช่วยให้สามารถส่งมอบหรือนำเสนอโปรโมชั่นของบริการใหม่ ๆ ได้ทันที ณ ตำแหน่งที่อยู่ปัจจุบันของลูกค้า ขณะที่ยังคำนึงถึงความเป็นส่วนตัวของลูกค้าอีกด้วย อีกทั้งยังบริการข้อมูลแสดงตำแหน่งที่อยู่ของลูกค้าจากโทรศัพท์มือถือ รวมทั้งข้อมูลเกี่ยวกับตำแหน่งที่อยู่จาก GPS

2) การรณรงค์การตลาดที่ชาญฉลาด (Intelligent Marketing Campaigns)

เครื่องมือสำหรับการวิเคราะห์ Big Data (Big Data Analytics) จะช่วยให้ผู้ให้บริการโทรคมนาคม มีความเข้าใจในลูกค้าได้ดีขึ้น และยังสามารถพัฒนาประวัติของสมาชิกผู้ใช้บริการ ซึ่งยังประโยชน์ ต่อการสร้างการรณรงค์ทางการตลาดได้ดียิ่งขึ้น ตัวอย่างเช่น ใช้การบอกตำแหน่งทางด้าน

---

[15] Informatica, **Big Data for the Telecommunications Industry: Minimize Data Cost, Maximize Data Value** [Online], 2012. Available from http://www.informatica.com/Images/02190_big-data-telecommunications_eb_en-US.pdf.

ภูมิศาสตร์ (Location Based Service) เพื่อจัดเก็บข้อมูลเกี่ยวกับตำแหน่งที่อยู่ของลูกค้าในแต่ละวัน จากนั้นทำการวิเคราะห์การใช้ชีวิตตั้งแต่อยู่ในที่ทำงานไปจนถึงกลับบ้านทุกวันบนเส้นทางต่าง ๆ รวมทั้งการดำเนินชีวิตในวันหยุดสุดสัปดาห์ ข้อมูลเหล่านี้ถูกจัดเก็บใน Big Data ในประวัติของลูกค้า โดยผู้ให้บริการสามารถนำไปใช้เพื่อสร้างบริการ (Service) ใหม่มานำเสนอต่อไป การรณรงค์การตลาดที่ชาญฉลาดจะใช้เครื่องมือการวิเคราะห์ Big Data (Big Data Analytics) เพื่อปรับปรุงผลลัพธ์จากการส่งเสริมทางการตลาด เพื่อเพิ่มรายได้และป้องกันลูกค้าหนีหาย

3) การติดตาม Social media และข้อมูลเชิงลึก (Social Media Monitoring and Insights)

ผู้ให้บริการสามารถใช้เครื่องมือวิเคราะห์ Big Data เพื่อติดตามและวิเคราะห์การตอบสนอง รวมถึงความรู้สึกของผู้ใช้บริการได้อย่างรวดเร็วจากสื่อสังคมออนไลน์อย่างเช่น Twitter, Facebook, Youtube รวมทั้ง Message Board ตลอดจน สถานที่ออนไลน์อื่น ๆ ที่ซึ่งลูกค้าใช้เป็นที่สนทนา รวมทั้งบันทึกการติดต่อและแลกเปลี่ยน E-mail กับผู้ใช้บริการ ขีดความสามารถนี้จะช่วยให้สามารถประเมินว่าการโฆษณาการตลาดใหม่ ๆ รวมทั้งผลิตภัณฑ์และบริการจะให้ผลลัพธ์ออกมาอย่างไร และยังสามารถระบุภูมิศาสตร์และกลุ่มเป้าหมายผู้ใช้ผลิตภัณฑ์ที่ตอบสนองเชิงบวก และใช้ข้อมูลใน Big Data นี้เพื่อเพิ่มการขายและลดการตอบสนองเชิงลบ

4) การดูแลระบบเครือข่าย (Network Intelligence)

การเพิ่มความพึงพอใจแก่ลูกค้า และลดการสูญเสียลูกค้า โดยการเพิ่มประสิทธิภาพการให้บริการของเครือข่าย ผู้ให้บริการสามารถใช้เครื่องมือวิเคราะห์ Big Data เพื่อพิสูจน์ทราบปัญหา รวมทั้งการหาจุดเสียแบบเรียลไทม์ ซึ่งจะช่วยปรับปรุงประสิทธิภาพของเครือข่ายและลดค่าใช้จ่ายการปฏิบัติงาน การวิเคราะห์แบบ Real Time จะให้ข้อมูลที่รวดเร็วและชาญฉลาดแก่ผู้ให้บริการอย่างรวดเร็วเพื่อการพิสูจน์ ทราบจุดบริการที่มีปัญหาเพื่อปรับแต่งแก้ไขทันการณ์

5) การป้องกันการทุจริตที่รวดเร็ว (High-velocity Fraud Detection)

การใช้ Smartphone หรืออุปกรณ์อื่น ๆ อย่างเช่น Laptop หรือ Tablet เพื่อสร้าง Hotspot ปลอมโดยมีจุดประสงค์เพื่อแอบเชื่อมต่อกับผู้ใช้งานหลาย ๆ คน กิจกรรมแบบนี้จะทำให้มีการแผ่ข้อมูลออกมามากมาย ทำให้ผู้ให้บริการสูญเสียรายได้ ระบบสามารถพิสูจน์ทราบการเกิดฉ้อโกง หรือความไม่ตั้งใจใช้งานซึ่งละเมิดต่อข้อตกลงการใช้บริการระบบไร้สายของสมาชิก และทีมงานผู้ให้บริการลูกค้า สามารถติดต่อกับสมาชิกผู้ใช้บริการเพื่อลดกิจกรรมเหล่านี้หรืออัพเกรดสัญญาของเขา

2.2.5 กรณีศึกษา Big Data (Big Data Case Studies)

ในยุคปัจจุบัน ขณะที่ความรวดเร็วในการเชื่อมกับโลกเป็นสิ่งที่จำเป็นจึงก่อให้เกิดความคาดหวังที่เพิ่มขึ้นเรื่อย ๆ ระหว่างลูกค้า และบริษัทที่กระทำธุรกิจด้วยกัน ซึ่งเกิดเป็นความท้าทายโดยเฉพาะอย่างยิ่งเมื่อผู้ตัดสินใจภายในองค์กรต้องใช้เวลานานในการคัดกรองข้อมูลที่สำคัญจำนวนหลายพันเทระไบต์ (TB) ภายในองค์กร ดังนั้นเพื่อความรวดเร็วของธุรกิจ เทคโนโลยีที่สามารถช่วยในการตัดสินใจได้อย่างเร่งด่วนพร้อมกับปริมาณของข้อมูลที่น้อยลง ดังนั้น แต่ละบริษัทจึงได้คิดค้นเทคโนโลยีต่าง ๆ ออกมาเพื่อรองรับ และจัดการกับข้อมูลขนาดใหญ่อย่าง Big Data ดังนี้

ตารางที่ 2.2: กรณีศึกษา Big Data

บริษัท	ผลิตภัณฑ์	เทคโนโลยี	ประโยชน์
ออราเคิล Oracle	Oracle Big Data Appliance	Apache Hadoop (CDH)	- จัดสรรระบบที่มีความพร้อมใช้งานสูงและปรับขนาดได้อย่างยืดหยุ่นเพื่อบริหารจัดการข้อมูลจำนวนมหาศาลได้อย่างรวดเร็ว - นำเสนอแพลตฟอร์มประสิทธิภาพสูงสำหรับการประมวลผลและวิเคราะห์ Big Data ในระบบ Hadoop - สามารถใช้ Oracle R Enterprise ซึ่งเป็นสภาพแวดล้อมสำหรับR Statistical Package ในการวิเคราะห์ข้อมูล - ควบคุมค่าใช้จ่ายด้านไอทีด้วยการผนวกรวมส่วนประกอบฮาร์ดแวร์และซอฟต์แวร์ทั้งหมดไว้ใน Big Data Solutions เดียวกันซึ่งจะช่วยเสริมสร้างระบบคลังข้อมูลภายในองค์กร (IT News, 2555)

(ตารางมีต่อ)

ตารางที่ 2.2 (ต่อ): กรณีศึกษา Big Data

บริษัท	ผลิตภัณฑ์	เทคโนโลยี	ประโยชน์
เดลล์ (Dell)	- Dell Big Data Analytics Solution - Dell Crowbar	Cloudera Hadoop	- ช่วยวิเคราะห์ข้อมูลที่ซับซ้อน - ลดค่าใช้จ่ายของการเก็บข้อมูลได้สูงสุดร้อยละ 80 - ทำให้มีการเข้าถึงข้อมูลที่รวดเร็ว และปรับโครงสร้างของข้อมูลได้ตลอดเวลา - รับรองเรื่องความยืดหยุ่นและเสถียรภาพของระบบ (MK, 2555)
ไอบีเอ็ม (IBM)	InfoSpher BigInsights Infosphere Streams	Apache Hadoop	- ช่วยให้เข้าถึงข้อมูลเชิงลึกที่อยู่ทั่วไปในกระบวนการทางธุรกิจได้รวดเร็วยิ่งขึ้น - ช่วยวิเคราะห์ข้อมูลทั้งแบบมีโครงสร้างและไม่มีโครงสร้าง ทำให้เกิดการตัดสินใจได้รวดเร็วขึ้น - สามารถวิเคราะห์ข้อมูลภายในองค์กร และเพื่อตรวจสอบข้อมูลในทุกการเปลี่ยนแปลงทำให้องค์กรใช้ข้อมูลเชิงลึกในการตัดสินใจได้อย่างเหมาะสม - สามารถประมวลผลขนาดใหญ่มากแบบทันที (OSTC, MEXT & NSF, 2555)
SAS	SASVisualAnalytics	Apache Hadoop	- ช่วยให้ผู้ใช้วิเคราะห์ข้อมูลขนาดใหญ่และทำให้มีการตัดสินใจที่ดีขึ้น - สามารถนำผลการวิเคราะห์ข้อมูลมาช่วยตอบคำถามที่ซับซ้อนได้เร็วขึ้น - ทำให้เกิดการปรับปรุงการแบ่งปันข้อมูลและการทำงานร่วมกัน

2.3 ประเด็นปัญหา และความท้าท้ายที่เกี่ยวข้องกับ Big Data

ในปัจจุบัน Big Data มีปัญหาหลายอย่างที่สังคมกำลังเผชิญอยู่ โดยเฉพาะปัญหาที่ในปัจจุบันเรายังไม่สามารถหาวิธีแก้ไขได้ ซึ่งพลังของ Big Data ขึ้นอยู่กับความสามารถในการวิเคราะห์ข้อมูลปริมาณมหาศาลของนักวิทยาศาสตร์ แพทย์ วิศวกร นักวางผังเมือง นักการศึกษา นักวิชาการ และผู้เชี่ยวชาญอื่น ๆ เพื่อแก้ปัญหาสังคม ดังนั้น Big Data จึงเป็นสิ่งที่น่าค้นหา แต่การจะนำ Big Data มาใช้ประโยชน์ได้นั้น เราต้องเผชิญกับความท้าทายในเรื่องความเป็นส่วนตัวและการคุ้มครองข้อมูล โดยเราต้องสนับสนุนเสรีภาพในการนำข้อมูลเหล่านี้มาใช้ แต่ในขณะเดียวกันก็ต้องใช้ข้อมูลอย่างมีความรับผิดชอบด้วย ซึ่งปัญหาดังกล่าวคือ[16] ปัญหาในการเก็บรวบรวมข้อมูล เนื่องจากการเก็บรวบรวมข้อมูล ถือเป็นขั้นตอนที่มีความสำคัญ เพื่อให้ได้มาซึ่งข้อมูลที่ตอบสนองวัตถุประสงค์ และสอดคล้องกับกรอบแนวความคิด สมมุติฐาน เทคนิคการวัด และการวิเคราะห์ข้อมูล ซึ่งหมายรวมทั้งการเก็บข้อมูล (Data Collection) คือ การเก็บข้อมูลขึ้นมาใหม่ และการรวบรวมข้อมูล (Data Compilation) คือการนำเอาข้อมูลต่าง ๆ ที่ผู้อื่นได้เก็บไว้แล้วมาทำการศึกษาวิเคราะห์ต่อ ซึ่งประเด็นปัญหาในการเก็บรวบรวมข้อมูลนั้น ได้แก่ การเก็บรักษาความลับข้อมูล การยินยอมของผู้ให้ข้อมูล การรับรู้ของผู้ให้ข้อมูลต่อการมีอยู่ของฐานข้อมูล การรับรู้ของผู้ให้ข้อมูลต่อการใช้ฐานข้อมูล รวมถึงปัญหาการใช้ฐานข้อมูล ได้แก่ การใช้ข้อมูลที่ไม่ถูกต้องหรือมีความผิดพลาด ความเกี่ยวข้องของข้อมูล ความยินยอมของผู้ให้ข้อมูลต่อการใช้ข้อมูลดังกล่าว และการรับรู้ของผู้ให้ข้อมูลต่อการใช้ข้อมูล และปัญหาในการแลกเปลี่ยนข้อมูล ได้แก่ การเชื่อมโยงฐานข้อมูลที่ต่างกันการรวมศูนย์และการวิเคราะห์ฐานข้อมูล รวมไปถึงการส่งข้อมูลข้ามพรหมแดนระหว่างประเทศอีกด้วย

2.3.1 ผู้มีส่วนได้เสีย (Stakeholders) จาก Big Data

ผู้มีส่วนได้เสีย (Stakeholders) หมายความว่า กลุ่มต่าง ๆ ที่ได้รับผลกระทบ หรืออาจได้รับผลกระทบจากการดำเนินงาน หรือความสำเร็จจาก Big Data ซึ่งก็คือ

1) เจ้าของข้อมูลส่วนบุคคล คือ บุคคลธรรมดา คณะบุคคล ซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล รวมถึงทายาทหรือคู่สมรสของเจ้าของข้อมูลส่วนบุคคลในกรณีที่เจ้าของข้อมูลส่วนบุคคลนั้นถึงแก่ความตายด้วย

2) ผู้ประมวลผลข้อมูลส่วนบุคคล คือ บุคคลธรรมดา คณะบุคคล นิติบุคคล หรือหน่วยงานของรัฐ ซึ่งดำเนินการประมวลผลข้อมูลเอง หรือดำเนินการในนามหรือแทนผู้ควบคุมข้อมูล หรือผู้ทำหน้าที่กำกับการประมวลผลข้อมูล

---

[16] Moed, H., **Research Trends: Special Issue on Big Data** [Online], 30 September 2012. Available from http://www.researchtrends.com/wp-content/uploads /2012/09/ Research_Trends_Issue30.pdf.

3) ผู้ควบคุมข้อมูลส่วนบุคคล คือ ผู้ซึ่งมีหน้าที่รับผิดชอบในการเก็บรวบรวม ควบคุมการใช้และการเปิดเผยข้อมูลส่วนบุคคล

2.3.2 ปัญหาที่เกิดจาก Big Data

Big Data มีความหมายไม่ได้ชัดเจนมากนัก แต่ Big Data ได้ถูกใช้ในลักษณะที่เป็นการสะสมข้อมูลเพิ่มมากขึ้นเรื่อย ๆ[17] เมื่อ 2 ปี ที่ผ่านมา ผู้คนมุ่งความสนใจไปที่คำถามที่ว่า “ทำไมข้อมูลของฉันถึงหาย?” “ทำไมคุณถึงมีข้อมูลของฉัน?” “ทำไมคุณไม่บอกฉันว่าคุณนำข้อมูลของฉันไปใช้ทำอะไร?” แต่ว่าในปัจจุบันนี้คำถามเหล่านั้นได้เปลี่ยนไปแล้ว ยกตัวอย่างเช่น “ผู้คนคาดหวังอะไรจากความเป็นส่วนตัว”[18] “Big Data จำเป็นต้องใช้ข้อมูลส่วนบุคคล และความเป็นส่วนตัวทั้งหมดเลยหรือไม่”[19] “ถ้าคุณใช้ข้อมูลส่วนบุคคล คุณสามารถทำให้เป็นข้อมูลที่ไม่เจาะจงบุคคลได้หรือไม่” เป็นต้น

ดังนั้น ประเด็นปัญหาของ Big Data คือ เรื่องความเป็นส่วนตัว ซึ่งหลักการในเรื่องความเป็นส่วนตัวที่ใช้กันมานานยังคงใช้ได้กับ Big Data หลักการเหล่านี้ คือ ความโปร่งใส (Transparency) ซึ่งการที่ผู้ให้บริการมีความโปร่งใสจะทำให้ผู้ใช้บริการเชื่อมั่นในวิธีที่ผู้ให้บริการเก็บข้อมูลรวมถึงข้อมูลที่ผู้ให้บริการเก็บ ฉะนั้นการขอความยินยอม (Consent) จากผู้ใช้บริการหรือเจ้าของข้อมูลจึงเป็นสิ่งสำคัญ นอกจากนี้ การเก็บข้อมูลควรจะคำนึงถึงความเสี่ยงที่เกี่ยวข้อง การเก็บข้อมูลบางอย่างอาจนำไปสู่ประโยชน์ แต่ก็อาจมีความเสี่ยงต่อปัจเจกบุคคล การเก็บข้อมูลเหล่านี้จึงต้องคำนึงถึงสิทธิของปัจเจกบุคคลด้วย

ในเรื่องหลักการชี้แจงถึงจุดประสงค์ของการเก็บข้อมูล (Purpose Specification) นั้น ปัญหาคือ ผู้ให้บริการจะชี้แจงถึงจุดประสงค์ และความหมายการใช้ข้อมูลที่เหมาะสมได้อย่างไร เนื่องจากไม่สามารถรับรู้ได้ว่าข้อมูลใน Big Data นั้นจะก่อให้เกิดประโยชน์ด้านใดในอนาคต ยกตัวอย่างเช่น ข้อมูลที่เก็บในวันนี้อาจช่วยให้นักวิทยาศาสตร์ในรุ่นต่อไปค้นพบวิธีการรักษาโรคได้ เป็นต้น ฉะนั้น ผู้ให้บริการจึงต้องมีความระมัดระวังเมื่อจะนิยามจุดประสงค์ของการเก็บข้อมูล ไม่สามารถบอกได้ว่าข้อมูลนั้นอาจช่วยไขความลับอะไรในอนาคตข้างหน้า

ความมั่นคงปลอดภัยของข้อมูล (Data Security) ใน Big Data ยังคงเป็นประเด็นที่สำคัญมากเมื่อพูดถึง Big Data อุตสาหกรรมจำเป็นต้องมีนโยบายคุ้มครองความเป็นส่วนตัว และความมั่นคง

---

[17] Ibid, 4.

[18] Ibid, 4-5.

[19] ICO Information Commissioner’s Office, **Big Data and data protection** [Online], 17 October 2014. Available from http://ico.org.uk/news/latest_news/2014/~/media/documents/library/Data_Protection/Practical_application/big-data-and-data-protection.pdf.

ปลอดภัยของข้อมูล ตลอดจนส่งเสริมให้เกิดวิธีการปฏิบัติที่ดี และทำให้การปฏิบัติเหล่านั้นกลายเป็นมาตรฐาน นอกจากนี้ความรับผิด (Accountability) ยังเป็นเครื่องมือพื้นฐานที่สำคัญมากเช่นกันในยุคของ Big Data

ในยุคของ Big Data และอินเทอร์เน็ตของสรรพสิ่ง (Internet of Things–IoT) ที่มีอุปกรณ์จำนวนมากสร้างและเก็บข้อมูลอยู่ตลอดเวลานั้น จุดร่วมกันระหว่างกฎหมายคุ้มครองข้อมูล และ Big Data/ IoT มีอยู่ใน 2 ประเด็นสำคัญด้วยกัน ประเด็นแรกคือเรื่องของความมั่นคงปลอดภัยของข้อมูล (Data Security) กฎหมายของประเทศส่วนใหญ่กำหนดให้ทุกองค์กรต้องมีวิธีการทั้งทางการบริหารจัดการและวิธีทางเทคนิคที่เหมาะสมในการคุ้มครองความมั่นคงปลอดภัยของข้อมูล ซึ่งเป็นสิ่งจำเป็นมากสำหรับ Big Data และ IoT

ประเด็นที่สอง คือ เรื่องของการเคลื่อนย้ายข้อมูลข้ามพรมแดนประเทศ (Cross-border Data Transfer) ในปี ค.ศ. 1995 ประเทศในกลุ่มสหภาพยุโรปได้มีการเซ็นสัญญาร่วมกันเรื่องการรับรองสิทธิมนุษยชน ซึ่งยอมรับว่าคนทุกคนมีสิทธิในความเป็นส่วนตัว และสิทธิดังกล่าวจะต้องได้รับการปกป้อง สหภาพยุโรปจึงมีกฎออกมาควบคุมการจัดการข้อมูลใน Big Data ทั้งการเก็บข้อมูล การนำข้อมูลไปใช้ หรือสิทธิของเจ้าของข้อมูล ซึ่งแม้ว่าแต่ละประเทศในกลุ่ม EU จะมีกฎหมายควบคุมข้อมูลแตกต่างกันออกไปบ้าง แต่ก็มีกรอบใหญ่ร่วมกันอยู่ ซึ่งกฎหนึ่งที่สำคัญคือ EU มีการกำหนดว่าหากมีการเคลื่อนย้ายข้อมูลข้ามพรมแดน จะต้องทำให้แน่ใจว่าประเทศที่จะส่งออกข้อมูลไปนั้นมีกฎหมายคุ้มครองข้อมูลที่ทัดเทียมกัน (Equivalent)

แต่สำหรับข้อมูลดิจิทัล ข้อมูลใน Big Data รูปแบบดังกล่าวเป็นสิ่งที่ไม่มีพรมแดน และหากประเทศหนึ่งตั้งกฎหมายเพื่อกำกับดูแลข้อมูลขึ้นมา แต่ไม่ได้คำนึงถึงเวลาที่ข้อมูลข้ามพรมแดนออกไป กฎหมายที่ตั้งขึ้นมานั้นก็จะไม่มีความหมาย ซึ่งสำหรับการเคลื่อนย้ายข้อมูลระหว่างประเทศใน EU ด้วยกันเองอาจไม่มีปัญหามากนัก เนื่องจากกฎที่กำกับเรื่องนี้มีความคล้ายคลึงกันในระดับหนึ่ง แต่สำหรับประเทศในเอเชีย กฎหมายที่กำกับการคุ้มครองข้อมูลมีความแตกต่างกันมาก เนื่องจากกฎหมายดังกล่าวในเอเชียมีที่มาต่างกันออกไป ยกตัวอย่างเช่นประเทศสิงคโปร์[20] ในการออกกฎหมายคุ้มครองข้อมูลของสิงคโปร์นั้น รัฐบาลสิงคโปร์ไม่ได้พูดถึงเรื่องสิทธิมนุษยชนเลย แต่รัฐมองว่าภาคธุรกิจข้อมูลเป็นภาคเศรษฐกิจที่สำคัญของประเทศ การที่สิงคโปร์จะมีการลงทุนทางด้านนี้ สิงคโปร์จำเป็นต้องทำให้ประเทศยุโรป และบริษัทข้ามชาติสามารถนำข้อมูลเข้ามาไว้ในประเทศได้ สิงคโปร์จึงจำเป็นต้องมีกฎหมายคุ้มครองข้อมูลที่เท่าเทียมกับ EU

---

[20] Internet Society & International Institute of Communications, **ความเป็นส่วนตัวในโลกอินเทอร์เน็ตของสรรพสิ่ง** [Online], 15 ธันวาคม 2557. แหล่งที่มา http://trpc.biz/isoc-trpc-iic-thailand-roundtable/.

เมื่อมองกฎหมายคุ้มครองข้อมูลใน Big Data ของสิงคโปร์อย่างผิวเผินจะพบว่าสิงคโปร์มีกฎหมายคุ้มครองข้อมูลคล้ายกับประเทศในกลุ่ม EU แต่ที่จริงแล้ววิธีการของสิงคโปร์คือการจัดให้มีการคุ้มครองข้อมูลในระดับที่มีความยืดหยุ่นที่สุดเท่าที่จะเป็นไปได้ เพียงเพื่อจะให้สามารถส่งผ่านข้อมูลจากประเทศในกลุ่ม EU และบรรษัทข้ามชาติเข้ามายังสิงคโปร์ได้

ข้อหนึ่งที่เห็นได้ชัด คือ การที่กฎการคุ้มครองข้อมูลดังกล่าวไม่รวมข้อมูลที่อยู่กับรัฐบาลสิงคโปร์ เพราะรัฐบอกว่าเป็นข้อตกลงกันของภาคธุรกิจ ไม่เกี่ยวกับรัฐ เป็นต้น ขณะที่มาเลเซียนั้นนำกฎหมายบางข้อมาจากสหราชอาณาจักรโดยไม่ได้คำนึงถึงบริบทของประเทศตัวเอง ส่วนเกาหลีใต้ก็มีกฎหมายคุ้มครองข้อมูลที่ต่างออกไปจากประเทศอื่น ๆ ในเอเชีย โดยนับได้ว่าเป็นประเทศที่กฎดังกล่าวมีความเข้มงวดที่สุด การที่แต่ละประเทศในเอเชียมีกฎหมายคุ้มครองข้อมูลที่แตกต่างกันมากเช่นนี้เป็นเรื่องที่สำคัญ เพราะสิ่งนี้จะเป็นอุปสรรคต่อการประกอบธุรกิจเกี่ยวกับ Big Data

2.3.2.1 ความเป็นส่วนตัว (Privacy) คือ สิทธิที่อยู่ตามลำพังและสิทธิที่เป็นอิสระจากการถูกรบกวนโดยไม่มีเหตุอันควร

ความเป็นส่วนตัว[21] หมายถึง “สิทธิที่จะอยู่โดยลำพัง” (The right to be let alone) “ความเป็นส่วนตัว” หรือ “Privacy” เป็นสิทธิมนุษยชนขั้นพื้นฐานของมนุษย์ ที่สังคมยุคใหม่เกือบทุกประเทศให้ความสำคัญอย่างมาก ดังจะเห็นได้จากการรับรองหลักการดังกล่าวไว้ในรัฐธรรมนูญหรือแม้บางประเทศจะไม่ได้บัญญัติรับรองไว้โดยตรง ในรัฐธรรมนูญ แต่ก็ได้ตราบทบัญญัติรับรองไว้ในกฎหมายเฉพาะ “ความเป็นส่วนตัว” ได้รวมถึงการคุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นการตีความคำว่า “ความเป็นส่วนตัว” ในด้านการจัดการข้อมูลส่วนบุคคล ความเป็นส่วนตัวเกี่ยวกับข้อมูล (Information Privacy) เป็นการให้ความคุ้มครองข้อมูลส่วนบุคคลโดยการวางหลักเกณฑ์เกี่ยวกับการเก็บรวบรวมและการบริหารจัดการข้อมูลส่วนบุคคล

- **การละเมิดความลับส่วนบุคคล**[22]

ปัญหาที่สำคัญของการละเมิดความลับส่วนบุคคลใน Big Data กลับมิใช่ข้อมูลที่สามารถสังเกตได้โดยตรง แต่เป็นข้อมูลที่สามารถคาดคะเนทางอ้อมได้ด้วยหลักสถิติ นั่นคือข้อมูลใน Big Data นั่นเอง เนื่องจากในขณะที่แต่ละบุคคลควรที่จะระมัดระวังไม่เปิดเผยข้อมูลที่เป็นความลับที่สามารถสังเกตได้โดยตรง แต่การที่แต่ละบุคคลจะสามารถควบคุมการใช้ชีวิตในโลกดิจิทัล

---

[21] Samuel, D., Warren, D., Louis, D., & Brandeis, L., **The Right to Privacy** [Online], 15 December 1890. Available from http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

[22] Agrawal, D., **Challenges and Opportunities with Big Data** [Online], February 2012. Available from http://www.purdue.edu/discoverypark/cyber/assets/pdfs/BigDataWhitePaper.pdf.

ของตน เพื่อที่จะมิให้เกิดเป็นรูปแบบที่สามารถนำไปคำนวณด้วยหลักสถิติ เป็นสิ่งที่ยากมาก ซึ่งอาจจะเกิดขึ้นได้ต่อเมื่อบุคคลผู้นั้นเลือกที่จะไม่ใช้อุปกรณ์ในยุคดิจิทัลเลยเท่านั้น เนื่องจากพฤติกรรมต่าง ๆ ในโลกดิจิทัลที่ทำให้เกิดเป็นรูปแบบนั้น สามารถเกิดขึ้นได้ในขณะที่บุคคลผู้นั้นย่อมไม่รู้ตัว และในบางครั้งการวิเคราะห์ Big Data อาจสามารถทำให้ล่วงรู้ความลับส่วนบุคคลที่บุคคลผู้นั้นอาจมิเคยรู้เกี่ยวกับตัวเองด้วย

ในยุคดิจิทัลไร้พรมแดนระหว่างประเทศ ผู้ที่มีประสิทธิภาพสูงสุด ที่จะสามารถนำ Big Data มาใช้ เพื่อการวิเคราะห์ Big Data ในประเทศไทยกลับเป็นธุรกิจข้ามชาติ ได้แก่ ผู้ให้บริการ Search Engine, Social Network เป็นต้น ซึ่งผู้ให้บริการเหล่านี้มีความล้ำหน้ากว่าธุรกิจภายในประเทศ ทั้งในด้านของเทคโนโลยี บุคลากร และกำลังทุน และยังสามารถให้บริการในประเทศไทยได้โดยสามารถหลีกเลี่ยงการกำกับดูแล การคุ้มครองข้อมูลใน Big Data ภายใต้กฎหมายไทย เนื่องจากไม่จำเป็นต้องมีนิติบุคคลในประเทศ ตัวอย่างที่สำคัญคือ กรณีของ Line ซึ่งเป็นโปรแกรมสำหรับส่งข้อความที่มีผู้ใช้กว่า 18 ล้านคนในประเทศ ผู้ให้บริการ Line ซึ่งอยู่ในประเทศญี่ปุ่น สามารถมองเห็นการส่งข้อความระหว่างกันของคนไทยกว่า 18 ล้านคน ในขณะเดียวกัน สามารถปฏิเสธที่จะให้ความร่วมมือกับหน่วยงานรัฐของไทย เพราะว่า Line อยู่ภายใต้การกำกับดูแลของกฎหมายญี่ปุ่น แต่เนื่องจากประเทศญี่ปุ่นเป็นประเทศหนึ่งที่ให้ความสำคัญกับการรักษาความลับส่วนบุคคล กฎระเบียบและประเพณีปฏิบัติในประเทศล้วนมีพัฒนาการที่สูงกว่ากฎระเบียบและประเพณีปฏิบัติในประเทศไทย ประเทศเหล่านี้จึงมีมาตรการคุ้มครองข้อมูล และรักษาความลับส่วนบุคคล

ในขณะที่หลายฝ่ายกำลังให้ความสำคัญกับการวิเคราะห์ Big Data เพื่อแสวงหาความได้เปรียบในเชิงธุรกิจ หลายฝ่ายอีกเช่นกัน โดยเฉพาะผู้ที่มีอำนาจกำกับดูแลก็ให้ความสำคัญกับการรักษาความลับส่วนบุคคล โดยเฉพาะอย่างยิ่ง ควรมีการกำหนดจรรยาบรรณของการวิเคราะห์ Big Data เนื่องจากสามารถเข้าถึงความลับส่วนบุคคลได้ทั้งทางตรงและทางอ้อม โดยจะมีผลต่อประชากรไทยอย่างกว้างขวาง อีกประการหนึ่งที่มีความสำคัญ คือ การกำกับดูแลธุรกิจข้ามชาติที่มิได้อยู่ภายใต้กฎหมายไทย แต่เป็นผู้ที่มีประสิทธิภาพสูงสุดในการประยุกต์ใช้ Big Data ให้เกิดประโยชน์ ยิ่งไปกว่านั้น Big Data ยังสามารถเป็นเครื่องมือเพื่อการดักฟัง ฯลฯ เพื่อความได้เปรียบด้านความมั่นคงระหว่างประเทศ ซึ่งประเทศไทยในปัจจุบัน อาจยังไม่ได้มีการป้องกัน[23]

[23] อธิป อัศวานันท์, **ความเข้าใจที่ผิด ๆ เกี่ยวกับ Big Data และ Analytics** [Online], กันยายน 2557. แหล่งที่มา http://www.bangkokbiznews.com/home/details/business/ceo-blogs/atip/20140930/607999/Big-Data -Analytics-(1).html.

– **ความท้าทายของ Big Data (Challenges of Big Data)**[24]

ความเป็นส่วนตัว และเรื่องทางกฎหมายที่เกี่ยวข้องกับ Big Data เป็นประเด็นที่เป็นความเสี่ยง โดยผู้เชี่ยวชาญที่เกี่ยวกับความเป็นส่วนตัวชี้ว่าในขณะนี้เรื่องความเป็นส่วนตัวเป็นเรื่องที่คนทั่วไปเริ่มที่จะทราบถึงผลกระทบและปัญหา ซึ่งในปี ค.ศ. 2013 ได้มีการพูดถึงผลเสียของ Big Data กันมาก เนื่องจากผลกระทบจากการที่ผู้ให้บริการนำข้อมูลของผู้ใช้บริการไปทำการวิเคราะห์ในทางธุรกิจ ซึ่งโดยปกติแล้วธุรกิจหรือองค์กรจะทำตามคำแนะนำจากผู้เชี่ยวชาญทางกฎหมายว่าผู้เชี่ยวชาญด้านกฎหมายได้คาดการณ์สิ่งที่กำลังจะเกิดในอนาคตไว้ในทิศทางใด เพื่อที่จะเตรียมความพร้อมในทุก ๆ ด้าน จากนั้นทำการประเมินในด้านที่เกี่ยวกับการประชาสัมพันธ์ ทำความเข้าใจและศึกษาการตลาดเพื่อสร้างความเชื่อมั่นและไว้วางใจให้กับผู้ใช้บริการ แต่ในปัจจุบัน ธุรกิจหรือองค์กรได้ใช้ Big Data เป็นตัวขับเคลื่อนในการตัดสินใจ โดยผู้ให้บริการอาศัยความยินยอมของผู้ใช้บริการเป็นสำคัญ ซึ่งทำให้ผู้ให้บริการสามารถนำข้อมูลของผู้ใช้บริการใน Big Data ไปใช้วิเคราะห์ได้ และด้วยความก้าวหน้าทางเทคโนโลยีที่เกิดขึ้น ทำให้กฎหมายล้าหลัง ไม่มีบทบัญญัติที่ครอบคลุมถึงการกระทำดังกล่าว ดังนั้นจึงควรที่จะออกกฎหมายเพื่อกำหนดกฎเกณฑ์ให้เป็นมาตรฐานเป็นการเฉพาะ เพื่อกำกับดูแลผู้ให้บริการในการดูแลข้อมูลในส่วนนี้ และในหลาย ๆ ส่วน ที่เรียกว่า ข้อมูลที่เปิดเผยเป็นสาธารณะ ซึ่งเป็นข้อมูลที่บุคคลทั่วไปสามารถเข้าถึงได้ โดยสามารถนำมาประยุกต์ใช้ในกรณีการคุ้มครองข้อมูลใน Big Data ได้

2.3.2.2 ความมั่นคงปลอดภัยของข้อมูล (Data Security)

การนำคอมพิวเตอร์และระบบข้อมูลสารสนเทศเข้ามาใช้ การเก็บรวบรวมข้อมูลสารสนเทศขององค์กรก็เปลี่ยนรูปแบบไป ข้อมูลและสารสนเทศจะถูกเก็บเป็นไฟล์เอกสาร และมีการจัดทำระบบข้อมูลส่วนกลางขององค์กรในรูปของ Big Data เพื่อให้การนำข้อมูลไปใช้งานง่าย และสะดวกมากขึ้น เมื่อระบบเสียหายหรือไม่สามารถทำงานได้ตามปกติ เวลาและค่าใช้จ่ายที่ต้องใช้ในการแก้ปัญหาก็สูงตามไปด้วย นอกจากนี้เมื่อทุกคนทั้งในและนอกองค์กรสามารถเข้าถึงระบบข้อมูลได้โดยผ่านทางระบบเครือข่ายคอมพิวเตอร์ เป็นเหตุให้ระบบข้อมูลถูกบุกรุกจากผู้ไม่ประสงค์ดีได้ง่าย นอกจากนี้ระบบคอมพิวเตอร์ยังต้องเผชิญกับภัยคุกคาม (Threat) ต่าง ๆ ได้ง่ายกว่าข้อมูลในรูปแบบเอกสารอีกด้วย

---

[24] Cambridge, **Big Data Privacy Workshop: Advancing the state of the art in technology and practice** [Online], 3 March 2014. Available from http://web.mit.edu/bigdata-priv/images/MITBigDataPrivacyWorkshop2014_final05142014.pdf.

การรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security) หมายถึง การป้องกันข้อมูลในบริบทของการรักษาความลับ ความมั่นคง ความถูกต้อง และความพร้อมใช้งานของข้อมูล ซึ่งสามารถใช้แทน การรักษาความมั่นคงปลอดภัยของสารสนเทศได้ ซึ่งหมายความรวมถึง การป้องกันอันตรายในโลกออนไลน์ ที่มีผลกระทบต่อตัวผู้ใช้งานและทรัพย์สิน (ข้อมูล) ซึ่งในปัจจุบันมีผู้ใช้งานออนไลน์ทั่วโลกเพิ่มมากขึ้น ทั้งนี้เนื่องมาจากปัจจัยหลาย ๆ ด้าน ไม่ว่าเป็นอัตราค่าบริการที่ถูกลง หรือการเพิ่มขึ้นของอุปกรณ์พกพาต่าง ๆ เช่น Smartphone และ Tablet PC ซึ่งประเทศไทย Smartphone และ Tablet กลายเป็นอุปกรณ์ที่ได้รับความนิยมกันอย่างแพร่หลาย จึงปฏิเสธไม่ได้ว่าโทรศัพท์มือถือได้กลายมาเป็นช่องทางใหม่ในการติดต่อสื่อสารผ่านโลกออนไลน์ ทุกคนสามารถใช้งานและเข้าถึงข้อมูลที่เชื่อมต่อบนเครือข่ายของโลกอินเทอร์เน็ตได้ทุกที่ทุกเวลาอย่างง่ายดาย แต่ด้วยความง่ายดายนี้เอง จึงทำให้มีบริษัทมากมายอาจเข้ามาหาผลประโยชน์ หรือทำการเก็บรวบรวมข้อมูลจากการรับบริการทางอินเทอร์เน็ตได้ ถ้าหากผู้ใช้ไม่มีความระมัดระวัง ไม่ตระหนักรู้ถึงความสำคัญในเรื่องนี้ ก็อาจจะต้องพบกับความสูญเสียและตกเป็นเหยื่อได้โดยไม่รู้ตัว เพราะเหตุนี้ การรักษาความมั่นคงปลอดภัยของข้อมูลใน Big Data จึงเป็นสิ่งสำคัญที่ผู้ประกอบการและบุคคลทั่วไปเป็นอย่างยิ่ง

จึงอาจกล่าวได้ว่า ความมั่นคงปลอดภัยของระบบฐานข้อมูลใน Big Data เป็นการป้องกันผู้ไม่มีสิทธิเข้าใช้หรือแก้ไขข้อมูล การควบคุมความพร้อมกันในการเรียกใช้ข้อมูลเดียวกัน รวมถึงการรักษาความถูกต้องครบถ้วนสมบูรณ์ของข้อมูล โดยมีวัตถุประสงค์เพื่อ

1) รักษาความลับของข้อมูล (Secrecy)
2) ข้อมูลมีความถูกต้องสมบูรณ์ (Integrity)
3) มีฐานข้อมูลพร้อมใช้งานเสมอ (Availability)
4) ลดความเสี่ยง (Risk Assessment)

ปัญหาทางความมั่นคงปลอดภัยของข้อมูลใน Big Data ที่เกิดขึ้นในปัจจุบันมีผู้มีส่วนได้ส่วนเสียโดยตรง คือ ผู้ใช้บริการทั้งหน่วยงานของรัฐและเอกชนที่จำเป็นจะต้องใช้ระบบเทคโนโลยีสารสนเทศ ซึ่งยังมีจุดอ่อนที่ยังไม่มีมาตรการที่จะพัฒนากฎหมายเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูล ในกรณีของผู้ให้บริการที่เก็บสะสมข้อมูลจากผู้ใช้บริการในรูปแบบของ Big Data

ผลการวิจัยตลาดซึ่งได้ทำการสำรวจองค์กรทั่วโลกกว่า 2,000 แห่ง โดยสำรวจบุคลากรขององค์กรเอกชนและองค์กรมหาชนขนาดกลางจำนวน 2,038 คนจาก 11 ภูมิภาคทั่วโลกและข้ามอุตสาหกรรม เพื่อให้เกิดการวิเคราะห์ในเชิงลึกลงในระดับอุตสาหกรรมหรือภูมิภาค การสำรวจจัดทำขึ้นระหว่างวันที่ 15 กรกฎาคม พ.ศ. 2557 ถึงวันที่ 2 กันยายน พ.ศ. 2557[25] พบว่าการ

[25] Dell Global Technology Adoption Index, **Revealing decision points around technology adoption, use and benefits in organizations** [Online], 2014. Available from https://kapost-files-

รักษาความมั่นคงปลอดภัยของข้อมูลใน Big Data นับเป็นความกังวลใจใหญ่ที่สุดสำหรับการนำ Big Data มาใช้ จากดัชนีการนำเทคโนโลยีมาใช้ทั่วโลก พบว่าผู้มีอำนาจตัดสินใจด้านไอทียังคงพิจารณาว่าความมั่นคงปลอดภัยของข้อมูลเป็นอุปสรรคที่ใหญ่ที่สุดในการขยับขยายไปใช้ Big Data (35 เปอร์เซ็นต์) ในขณะที่ความกังวลใจเรื่องความมั่นคงปลอดภัยของข้อมูลใน Big Data เป็นตัวเหนี่ยวรั้งไม่ให้องค์กรลงทุนเทคโนโลยีหลัก การขาดข้อมูลเรื่องการรักษาความมั่นคงปลอดภัยของข้อมูลใน Big Data ที่พร้อมมือก็เหมือนเป็นการเหนี่ยวรั้ง ทำให้องค์กรไม่มีความพร้อมในระหว่างที่เกิดช่องโหว่ความมั่นคงปลอดภัยของข้อมูลใน Big Data ได้เช่นกัน มีเพียง 30 เปอร์เซ็นต์ของผู้ที่ตอบการสำรวจที่กล่าวว่าตนมีข้อมูลที่ถูกต้องไว้ช่วยตัดสินใจเกี่ยวกับความเสี่ยง และมีเพียงหนึ่งในสี่ขององค์กรที่สำรวจเท่านั้นที่มีแผนงานรองรับช่องโหว่ความมั่นคงปลอดภัยทุกรูปแบบ

จากผลสำรวจดังกล่าวพบสิ่งที่เหมือนกัน คือองค์กรไม่ทราบว่าจะจัดการอย่างไรกับ Big Data ในขณะที่ 61 เปอร์เซ็นต์ของผู้ตอบการสำรวจทั่วโลกกล่าวว่า องค์กรของตนมี Big Data แต่ไม่สามารถนำมาวิเคราะห์ได้ และมีแค่ 39 เปอร์เซ็นต์ ที่เข้าใจว่าจะสามารถนำคุณค่าของ Big Data มาใช้ต่ออย่างไร[26]

ในขณะที่ Big Data ได้พิสูจน์ให้เห็นถึงผลประโยชน์ในเชิงการตลาด ค่าใช้จ่ายด้านระบบโครงสร้างพื้นฐาน (35 เปอร์เซ็นต์) และระบบรักษาความมั่นคงปลอดภัยของข้อมูลใน Big Data (35 เปอร์เซ็นต์) ก็ดูจะเป็นอุปสรรคสำคัญต่อการติดตั้งเพื่อใช้ Big Data ผู้ตอบการสำรวจยังแจงว่าขาดค่าใช้จ่ายในการวิเคราะห์และในส่วนปฏิบัติการ (34 เปอร์เซ็นต์) การขาดการสนับสนุนจากผู้บริหาร (22 เปอร์เซ็นต์) และขาดความชำนาญด้านเทคนิค (21 เปอร์เซ็นต์) ยังเป็นอุปสรรคต่อกลยุทธ์เรื่อง Big Data และเมื่อพูดถึงความกังวลเรื่องความมั่นคงปลอดภัยของข้อมูลใน Big Data องค์กรส่วนใหญ่จึงมีการใช้ Cloud ส่วนตัว (43 เปอร์เซ็นต์) หรือใช้เซิร์ฟเวอร์แบบเดิม ๆ (24 เปอร์เซ็นต์) แทนการใช้ Cloud สาธารณะ (11 เปอร์เซ็นต์) ในการจัดเก็บ Big Data และองค์กรโดยเฉลี่ย รู้สึกว่าได้ข้อมูลเชิงลึกที่มีประโยชน์เพียง 53 เปอร์เซ็นต์ จากข้อมูลใน Big Data ที่มีอยู่[27]

ประเด็นปัญหาเรื่องความมั่นคงปลอดภัยของข้อมูล (Data Security) ใน Big Data มีดังนี้

---

prod.s3.amazonaws.com/uploads/direct/1415199563-23-1043/Executive_Summary_Global_Technology_Adoption_Index.PDF.

[26] Ibid.

[27] Ibid.

1) การรักษาความลับ (Confidentiality) เช่น การส่งข้อความที่ปกปิดหรือเป็นความลับผ่านเครือข่าย ผู้ส่งจะมั่นใจได้อย่างไรว่าบุคคลที่ประสงค์จะส่งถึงหรือที่ได้รับอนุญาตเท่านั้นที่สามารถอ่านข้อความได้

2) การระบุตัวบุคคล (Authentication) เช่น การได้รับข้อความที่ส่งมาผ่านทางเครือข่าย ผู้รับจะมั่นใจได้อย่างไรว่าเป็นข้อความที่ส่งมาจากบุคคลที่อ้างว่าเป็นผู้ส่งนั้นจริง

3) ความถูกต้องของข้อมูล (Integrity) เช่น การได้รับข้อความที่ส่งมาผ่านทางเครือข่าย ผู้รับจะมั่นใจได้อย่างไรว่าข้อความที่ได้รับเป็นข้อความที่ถูกต้องแท้จริง ไม่ได้ถูกเปลี่ยนแปลงแก้ไขระหว่างทาง

4) การห้ามปฏิเสธความรับผิด (Non-repudiation) เช่น การได้รับข้อความทางเครือข่ายเกี่ยวกับการดำเนินการอย่างใดอย่างหนึ่งหรือเป็นข้อผูกพันทางสัญญา แต่ต่อมาผู้ส่งปฏิเสธว่าไม่ได้ส่งข้อความนั้น ผู้รับจะสามารถใช้สิ่งใดอ้างอิงเพื่อไม่ให้ผู้ส่งปฏิเสธ

องค์กรที่เกี่ยวข้องกับความมั่นคงปลอดภัยระบบสารสนเทศที่มีในปัจจุบัน ซึ่งทำหน้าที่ช่วยเหลือผู้ใช้อินเทอร์เน็ตที่พบปัญหาด้านความมั่นคงปลอดภัยของข้อมูลใน Big Data โดยให้คำปรึกษาเมื่อเกิดปัญหาด้านความมั่นคงปลอดภัย มีดังต่อไปนี้

- **CERT (Computer Emergency Response Team)/ FIRST (Forum of Incident Response and Security Teams)**

CERT[28] หรือ Computer Emergency Response Team เป็นหน่วยงานที่ได้รับทุนสนับสนุนโดยกระทรวงกลาโหมสหรัฐอเมริกาดูแล และจัดการโดยนักวิชาการของมหาวิทยาลัยคาร์เนกี้เมลอน (CMU) ทำหน้าที่ช่วยเหลือผู้ใช้อินเทอร์เน็ตที่พบปัญหาด้านความมั่นคงปลอดภัยของข้อมูลใน Big Data โดยให้คำปรึกษาด่วนตลอด 24 ชั่วโมง และให้ข้อมูลเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลในระบบตลอดจนประกาศข่าวเตือนในกลุ่มข่าว comp.security.announce เมื่อมีปัญหาความมั่นคงปลอดภัยของข้อมูลเกิดขึ้นในเครือข่าย โดยวิเคราะห์ถึงปัญหาและสาเหตุรวมทั้งวิธีการป้องกันแก้ไข

FIRST[29] หรือ Forum of Incident Response and Security Teams เป็นองค์กรไม่หวังผลกำไร ซึ่งรวมเอาทีมผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยระบบสารสนเทศจาก

---

[28] Computer Emergency Response Team, **About Us** [Online], 1988. Available from http://www.cert.org/about/.

[29] Patthakarn, **Cybersecurity วาระแห่งชาติ** [Online], 8 กรกฎาคม 2556. แหล่งที่มา http://www3.senate.go.th/security/index.php?option=com_content&view=article&id=541:cybersecurity-.

กว่า 311 หน่วยงาน[30] ทั่วโลกเข้าด้วยกัน

สมาชิกของ FIRST มีทั้งบริษัทเอกชนต่าง ๆ หน่วยงานภาครัฐ มหาวิทยาลัย และสถาบันต่าง ๆ ทั่วโลกที่เป็นที่รู้จักกันดี เช่น Google, Adobe, CISCO, Microsoft, TREND MICRO, eBay, Facebook, US-CERT (หน่วยงานประเภทเซิร์ตของสหรัฐอเมริกา) และ JPCERT (หน่วยงานประเภทเซิร์ตของญี่ปุ่น) เป็นต้น ในการทำงานของสมาชิก “FIRST” นั้น จะมีการเข้ารวมกลุ่มกันทำงานตามความสนใจ เช่น กลุ่ม CVSS SIG/CVSS Special Interest Group ซึ่งจัดทำมาตรฐานการให้คะแนนความรุนแรงของช่องโหว่ระบบสารสนเทศ กลุ่ม Malware Analysis SIG ซึ่งส่งเสริมการเผยแพร่เครื่องมือและวิธีการวิเคราะห์โปรแกรมไม่พึงประสงค์ (Malware) และกลุ่ม Metrics SIG ซึ่งจัดทำแนวทางการประเมินผลการรับมือภัยคุกคามของหน่วยงาน เป็นต้น โดย “FIRST” มีเป้าหมายสำคัญในการสนับสนุนให้หน่วยงานสมาชิกสามารถรับมือกับภัยคุกคามได้อย่างมีประสิทธิภาพ รวมถึงความเป็นส่วนตัว และความมั่นคงปลอดภัยของข้อมูลใน Big Data ด้วย โดยอาศัยหลักปฏิบัติ เครื่องมือ และช่องทางการสื่อสารที่มั่นคงปลอดภัย

ประเทศไทยมีศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT) มีภาระหน้าที่หลักเพื่อตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยคอมพิวเตอร์ (Incident Response) และให้การสนับสนุนที่จำเป็นและคำแนะนำในการแก้ไขภัยคุกคามความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์ ซึ่งในที่นี้สามารถนำมาประยุกต์ใช้กับ Big Data ได้ รวมทั้งติดตามและเผยแพร่ข่าวสารและเหตุการณ์ทางด้านความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์ต่อสาธารณชน ตลอดจนทำการศึกษาและพัฒนาเครื่องมือและแนวทางต่าง ๆ ในการปฏิบัติเพื่อเพิ่มความมั่นคงปลอดภัยในการใช้คอมพิวเตอร์และเครือข่ายอินเทอร์เน็ต และในฐานะที่เป็นสมาชิกขององค์กรด้านการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ทั้งในระดับภูมิภาค (APCERT/Asia Pacific Computer Emergency Response Team) และระดับสากล (FIRST/Forum of Incident Response and Security Teams) ThaiCERT จึงมีบทบาทในการประสานงานระหว่างหน่วยงานต่างประเทศที่เป็นสมาชิกขององค์กรเหล่านี้ กับหน่วยงานในประเทศ ทั้งภาครัฐ เอกชน มหาวิทยาลัย ผู้ให้บริการอินเทอร์เน็ต หรือผู้เกี่ยวข้องในการตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยที่ได้รับแจ้ง[31]

---

[30] FIRST, **Alphabetical list of FIRST Members** [Online], 2014. Available from http://www.first.org/members/teams.

[31] ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต), **เกี่ยวกับไทยเซิร์ต** [Online], 2543. แหล่งที่มา https://www.thaicert.or.th/about.html.

ภารกิจของ ThaiCERT ได้แก่[32]

– ตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยคอมพิวเตอร์ (Incident Response)

– ให้การสนับสนุนที่จำเป็นและคำแนะนำในการแก้ไขภัยคุกคามความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์

– ติดตามและเผยแพร่ข่าวสารและเหตุการณ์ทางด้านความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์ต่อสาธารณชน

– ศึกษาและพัฒนาเครื่องมือและแนวทางต่าง ๆ ในการปฏิบัติเพื่อเพิ่มความมั่นคงปลอดภัยในการใช้คอมพิวเตอร์และเครือข่ายอินเทอร์เน็ต

ปัจจุบันการกำหนดแผนหรือนโยบายความมั่นคงปลอดภัยไซเบอร์ของประเทศต่าง ๆ ซึ่งรวมถึงความมั่นคงปลอดภัยของข้อมูลใน Big Data นั้นอยู่บนพื้นฐานของ Availability (การรักษาสภาพพร้อมใช้งาน) Integrity (การรักษาความครบถ้วน) และ Confidentiality (การรักษาความลับ) ที่เชื่อมโยงกับกฎหมายและการบังคับใช้กฎหมาย การจัดตั้ง CERT เพื่อเป็นหน่วยงานหลักในทางปฏิบัติของแต่ละประเทศ การดำเนินงานจะครอบคลุมทั้งภาคเอกชน ภาครัฐ และประชาชน การกำหนดนโยบายที่ส่งเสริมการแบ่งปันข้อมูลระหว่างหน่วยงานที่เกี่ยวข้องเพื่อช่วยในการวางแผนรับมือกับภัยได้ทันท่วงที การกำหนดกลุ่มธุรกิจ Critical Infrastructure ที่ชัดเจน และมีนโยบายเฉพาะเพื่อรองรับแผนการพัฒนาบุคลากรจะควบคู่ไปกับการสร้างความตระหนักรู้ และการสนับสนุนการวิจัย และพัฒนาด้านความมั่นคงปลอดภัยของข้อมูลใน Big Data ด้วย[33]

นอกจากนี้ อนาคตของ Cyber Security ไทยนั้นจะต้องมีการผลักดัน National Cyber Security Governance หรือการวางโครงสร้างการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศที่มีความชัดเจนในบทบาทหน้าที่ การปรับปรุงกฎหมายให้สอดคล้องกับบทบาทอำนาจหน้าที่ของผู้รับผิดชอบหลัก และสอดคล้องกับหลักกฎหมาย รวมถึงแนวปฏิบัติสากลการจัดตั้งศูนย์บัญชาการด้านความมั่นคงปลอดภัยของประเทศ (Cyber Security Center of

---

[32] ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย, **การตรวจจับภัยคุกคามและอาชญากรรมไซเบอร์ในประเทศไทย (กรณีศึกษา ThaiCERT)** [Online], 27 มีนาคม 2556. แหล่งที่มา http://ict.moph.go.th/response/admin/file/20130327_ThaiCERT_.

[33] สุรางคณา วายุภาพ, **ทิศทาง Cyber Security ของไทย และบทบาท National CERT** [Online], 13 มิถุนายน 2557 ก. แหล่งที่มา https://www.etda.or.th/etda_website/content/etda-cybersecurity-national-cert.html.

Command) โดยยกระดับ ThaiCERT ให้เป็น National CERT ระดับประเทศและนานาชาติ การรณรงค์สร้างความตระหนักรู้ด้านความมั่นคงปลอดภัย ทั้งในระดับผู้บริหารประเทศและประชาชนทั่วไป รวมทั้งการพัฒนาบุคลากรในบทบาทต่าง ๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์[34] ซึ่งหมายความรวมถึงการรักษาความมั่นคงปลอดภัยของข้อมูลใน Big Data ด้วย

– **ITU (International Telecommunication Union)**

ITU (International Telecommunication Union) หรือ สหภาพโทรคมนาคมระหว่างประเทศ เป็นหน่วยงานระดับนานาชาติเฉพาะทาง (Specialized Agencies) ที่อยู่ภายใต้สหประชาชาติ โดยมีศักดิ์ฐานะเท่ากับองค์กรอื่น ๆ เช่น UNESCO, IMF, WHO หรือ FAO

ITU มีหน้าที่ในการพัฒนามาตรฐาน และกฎระเบียบ สำหรับการสื่อสารวิทยุ และโทรคมนาคมระหว่างประเทศ การกำหนดแถบคลื่นความถี่วิทยุ (Allocation of the Radio Spectrum) และบริหารจัดการ กรณีที่จำเป็นสำหรับการเชื่อมโยงโครงข่ายระหว่างประเทศ เช่น บริการโทรศัพท์ระหว่างประเทศ อันเป็นภารกิจในเชิงโทรคมนาคม ในลักษณะเดียวกับการปฏิบัติงานของสหภาพสากลไปรษณีย์ ในกรณีของงานบริการไปรษณีย์

ITU เป็นองค์การชำนาญพิเศษของสหประชาชาติ ซึ่งนับเป็นองค์การสากลที่เก่าแก่มากที่สุดอันดับสอง ที่ยังคงดำเนินการอยู่ โดยในระยะแรกเริ่ม ใช้ชื่อว่า สหภาพโทรเลขระหว่างประเทศ (International Telegraph Union) จัดตั้งขึ้นที่กรุงปารีส ประเทศฝรั่งเศส เมื่อวันที่ 17 พฤษภาคม ค.ศ. 1865 (พ.ศ. 2408) ปัจจุบัน มีสำนักงานใหญ่ตั้งอยู่ที่ นครเจนีวา ประเทศสวิสเซอร์แลนด์ ใกล้กับสำนักงานสหประชาชาติ[35] ซึ่งชาติสมาชิกของ ITU แบ่งเป็น 5 ภูมิภาค ได้แก่ เอเชียแปซิฟิก (APT) ประเทศไทยอยู่ในกลุ่มนี้, ยุโรป (RCC), แอฟริกา, อเมริกา และกลุ่มประเทศอาหรับ

สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติร่วมกับกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร และสำนักงานส่งเสริมการจัดประชุมและนิทรรศการ (องค์การมหาชน) เป็นเจ้าภาพจัดงาน ITU Telecom World 2013 ระหว่างวันที่ 19-22 พฤศจิกายน พ.ศ. 2556 จัดขึ้นเพื่อระดมความคิดเห็น แลกเปลี่ยนข้อมูลในระดับ

---

[34] สุรางคณา วายุภาพ, **ETDA ร่วมเวที “ไซเบอร์: ภัยคุกคามต่อความมั่นคงของชาติ” เผยแนวโน้มและทิศทาง Cybersecurity ของไทย และบทบาท National CERT** [Online], 13 มิถุนายน 2557 ข. แหล่งที่มา https://www.etda.or.th/etda_website/content/etda-cybersecurity-national-cert.html.

[35] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์กรมหาชน), **ITU: International Telecommunication Union** [Online], ธันวาคม 2554. แหล่งที่มา https://www.etda.or.th/etda_website/mains/display/319.

นโยบายที่เกี่ยวข้องกับการปกป้องผู้บริโภคจากภัยรูปแบบต่าง ๆ ที่เกิดขึ้นในโลกไซเบอร์ปัจจุบันในงานสัมมนาวิชาการ “ความท้าทายความมั่นคงปลอดภัยในโลกไร้สายของประชาคมอาเซียน-การปกป้องผู้บริโภค” หรือ Mobile Security Challenges and Policy in the ASEAN Community: Consumer Protection Perspectives ซึ่งมีการนำเสนอความก้าวหน้าของแผนแม่บท USO Zoning Concept ที่มีเป้าหมายสำคัญคือ การลดความเหลื่อมล้ำในการเข้าถึงโทรคมนาคมและสารสนเทศอย่างทั่วถึง ครอบคลุมบริการโทรคมนาคม ทางเสียงและข้อมูล ในมิติเชิงพื้นที่และเชิงสังคม โดยคำนึงถึงนโยบายความเป็นส่วนตัว และความมั่นคงปลอดภัยของข้อมูลใน Big Data รวมถึงการยกระดับคุณภาพการให้บริการของหน่วยงานภาครัฐต่อประชาชนผ่านเครือข่ายโทรคมนาคมความเร็วสูงได้อย่างครบวงจรมากขึ้น ซึ่งได้พูดถึงความเป็นส่วนตัวและความมั่นคงปลอดภัยของข้อมูลว่าควรทำให้ประชาชนตระหนักรู้ถึงถึงความสำคัญของข้อมูลส่วนบุคคล ระมัดระวังไม่เปิดเผยข้อมูลที่เป็นลับ การป้องกันไม่ให้ผู้ที่ไม่สิทธิเข้าถึงข้อมูล หรือแก้ไขข้อมูลส่วนบุคคลได้ และการควบคุมความพร้อมให้สามารถใช้งานได้เสมอ ซึ่งหลักการดังกล่าวนี้สามารถนำมาใช้เป็นบทวิเคราะห์ได้[36]

2.3.2.3 ธรรมาภิบาล (Governance)[37]

ธรรมาภิบาล (Governance) คือ การปกครอง การบริหาร การจัดการ การควบคุมดูแล กิจการต่าง ๆ ให้เป็นไปในครรลองธรรม นอกจากนี้ยังหมายถึงการบริหารจัดการที่ดี ซึ่งสามารถนำไปใช้ได้ทั้งภาครัฐและเอกชน ธรรมที่ใช้ในการบริหารงานนี้ มีความหมายอย่างกว้างกล่าวคือ หาได้มีความหมายเพียงหลักธรรมทางศาสนาเท่านั้น แต่รวมถึง ศีลธรรม คุณธรรม จริยธรรม และความถูกต้องชอบธรรมทั้งปวง ซึ่งวิญญูชนพึงมีและพึงประพฤติปฏิบัติ อาทิ ความโปร่งใสตรวจสอบได้ การปราศจากการแทรกแซงจากองค์กรภายนอก เป็นต้น

ธรรมาภิบาล เป็นหลักการที่นำมาใช้บริหารงานในปัจจุบันอย่างแพร่หลาย ด้วยเหตุเพราะช่วยสร้างสรรค์และส่งเสริมองค์กรให้มีศักยภาพและประสิทธิภาพ อาทิ พนักงานต่างทำงานอย่างซื่อสัตย์สุจริตและขยันหมั่นเพียร ทำให้ผลประกอบการขององค์กรธุรกิจนั้นขยายตัว นอกจากนี้แล้วยังทำให้บุคคลภายนอกที่เกี่ยวข้อง ศรัทธาและเชื่อมั่นในองค์กรนั้น ๆ อันจะทำให้เกิดการพัฒนาอย่างต่อเนื่อง เช่น องค์กรที่โปร่งใส ย่อมได้รับความไว้วางใจในการร่วมทำธุรกิจ รัฐบาลที่โปร่งใส

---

[36] สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ, **ความท้าทายความมั่นคงปลอดภัยในโลกไร้สายของประชาคมอาเซียน-การปกป้องผู้บริโภค** [Online], พฤศจิกายน 2556. แหล่งที่มา http://www.nbtc.go.th/.

[37] สภาหอการค้าแห่งประเทศไทย, **หลักการสากลของธรรมาภิบาล** [Online], 2556. แหล่งที่มา http://www.thaichamber.org/scripts/detail.asp?nNEWSID=1220.

ตรวจสอบได้ ย่อมสร้างความเชื่อมั่นให้แก่นักลงทุนและประชาชน ตลอดจนส่งผลดีต่อเสถียรภาพของรัฐบาลและความเจริญก้าวหน้าของประเทศ เป็นต้น

ตัวอย่างองค์กรที่นำหลักธรรมาธิบาลไปใช้ เช่น องค์การสหประชาชาติได้กำหนดหลักการทั่วไปของธรรมาภิบาล ไว้ 8 หลักการ ดังนี้

1) การมีส่วนร่วม

การมีส่วนร่วมของสมาชิกทั้งชายหญิงคือการตัดสินใจที่สำคัญในสังคมและสร้างความสามัคคีให้เกิดกับประชาชน การมีส่วนร่วมสามารถทำได้โดยอิสระไม่มีการบังคับ สมาชิกเต็มใจให้ความร่วมมือด้วยตนเองหรือมีส่วนร่วมผ่านหน่วยงาน สถาบัน หรือผู้แทนตามระบอบประชาธิปไตย

2) การปฏิบัติตามกฎ

ธรรมาภิบาลต้องการความถูกต้องตามกรอบของกฎหมาย ไม่เลือกปฏิบัติไม่ลำเอียง มีการปฏิบัติอย่างเสมอภาคและเป็นธรรมกับประชาชนโดยเท่าเทียมกัน ทุกคนในสังคมอยู่ภายใต้ข้อกำหนดของกฎหมายเดียวกัน

3) ความโปร่งใส

ความโปร่งใสเป็นการตรวจสอบความถูกต้อง มีการเปิดเผยข้อมูลอย่างตรงไปตรงมา สิ่งนี้ช่วยแก้ปัญหาการทุจริตและคอรัปชั่นได้ทั้งในภาครัฐและเอกชน สื่อจะเข้ามีบทบาทอย่างมากในการตรวจสอบและรายงานผลงานดำเนินงานโดยการนำเสนอ ข่าวสารให้แก่สังคมได้รับทราบ

4) ความรับผิดชอบ

ความรับผิดชอบเป็นการพยายามให้คนทุกฝ่ายทำหน้าที่ของตนให้ดีที่สุดในการทำงาน กล้าที่จะตัดสินใจและรับผิดชอบต่อผลการตัดสินใจนั้น ๆ

5) ความสอดคล้อง

ความสอดคล้องต้องกันเป็นการกำหนดความต้องการของคนในสังคม ซึ่งมีความแตกต่างอย่างมาก โดยพยายามหาจุดสนใจร่วมกันและความต้องการที่สอดคล้องต้องกันของสังคมมาเป็น ข้อปฏิบัติเพื่อลดปัญหาความขัดแย้งในสังคม การจะพัฒนาสังคมได้ ต้องทราบความต้องการที่สอดคล้องต้องกันของสังคมนั้น ๆ ด้วยวิธีการเรียนรู้ วัฒนธรรมของสังคมนั้น ๆ ก่อน

6) ความเสมอภาค

ความเสมอภาคเป็นสิทธิขั้นพื้นฐานที่ประชาชนทุกคนพึงได้รับจากรัฐบาล ทั้งการบริการด้านสวัสดิการ ตลอดจนสาธารณูปโภคด้านอื่น ๆ

7) หลักประสิทธิภาพและประสิทธิผล

เป็นวิธีการจัดการทรัพยากรที่มีอยู่ โดยการผลิตและจำหน่ายเพื่อให้ได้ผลตอบแทนที่มีคุ้มค่ากับเงินที่ลงทุนหรือ การใช้ทรัพยากรให้ได้ประโยชน์สูงที่สุดต่อมวลมนุษยชาติ โดยมีการพัฒนากระบวนการเพิ่มผลผลิตอย่างต่อเนื่องและยั่งยืน

8) การมีเหตุผล

การมีเหตุผลเป็นความต้องการในทุกสังคม ประชาชนทุกคนต้องตัดสินใจและความรับผิดชอบต่อการกระทำของตนเองด้วยเหตุด้วยผลที่สมเหตุสมผล การมีเหตุผลไม่สามารถกระทำได้ถ้าปราศจากการปฏิบัติตามกฎหมายและความโปร่งใส

หลักการของธรรมาภิบาลที่นำมาประยุกต์ใช้กับการคุ้มครองข้อมูล คือ หลักความโปร่งใส เนื่องจากต้องมีการเปิดเผยข้อมูล อย่างถูกต้อง รวมถึงต้องมีการรักษาความมั่นคงปลอดภัยของข้อมูลใน Big Data ด้วย

อีกตัวอย่างหนึ่งที่นำหลักธรรมาภิบาลไปใช้ คือ กลุ่มประเทศ OECD (Organization for Economic Co-operation and Development) ได้กำหนดหลักการกำกับดูแลกิจการที่ดีที่ได้รับการยอมรับ และถูกนำไปใช้เป็น กรอบในการพัฒนาหลักการกำกับดูแลกิจการของประเทศต่าง ๆ โดยยึดประเด็นสำคัญของการมี Corporate Governance[38] โดยมีหลักการดังนี้

1) หลักพื้นฐานของการกำกับดูแลกิจการ (Ensuring the Basis for an Effective Corporate Governance Framework)

2) สิทธิและหน้าที่หลักของผู้ถือหุ้น (The Rights of Shareholders and Key Ownership Functions)

3) การปฏิบัติต่อผู้ถือหุ้นอย่างเท่าเทียมกัน (The Equitable Treatment of Shareholders)

4) บทบาทของผู้มีสวนได้เสียในการกำกับดูแลกิจการ (The Role of Stakeholders in Corporate Governance)

5) การเปดเผยข้อมูลและความโปรงใส (Disclosure and Transparency)

6) ความรับผิดชอบของคณะกรรมการ (The Responsibilities of the Board)

[38] **OECD Principles of Corporate Governance** [Online], 2004. Available from www.oecd.org.

หลักการดังกล่าวนี้เป็นหลักการที่นำมาใช้บริหารงานในปัจจุบันให้มีประสิทธิภาพ ซึ่งสามารถนำมาประยุกต์ใช้ได้กับความมั่นคงปลอดภัยของข้อมูลใน Big Data ได้โดยนำหลักการสิทธิและหน้าที่มาประยุกต์ใช้กับผู้ให้บริการ และผู้ใช้บริการ กำหนดกฎเกณฑ์ การปฏิบัติกับผู้ใช้บริการอย่างเท่าเทียม รวมถึงการเปิดเผยข้อมูลใน Big Data ด้วย

– **IGF (Internet Governance Forum)**

IGF (Internet Governance Forum) หรือ การประชุมว่าด้วยเรื่องการจัดการปกครองอินเทอร์เน็ตเป็นการประชุมเกี่ยวกับนโยบายสาธารณะที่เกี่ยวข้องกับอินเทอร์เน็ต โดยถือเป็นหนึ่งในกลไกขององค์การสหประชาชาติด้านอินเทอร์เน็ต นอกเหนือไปจากเวทีหรือการประชุมปกติ เช่น กลไก ITU เป็นต้น

IGF ถูกก่อตั้งขึ้นในปี 2006 จากมติของที่ประชุม World Summit on the Information Society ปี 2005 ซึ่งเป็นการประชุมด้านเทคโนโลยีและการสื่อสารขององค์การสหประชาชาติ ซึ่งจัดขึ้น 2 ครั้ง คือปี 2003 ที่นครเจนีวา สมาพันธรัฐสวิส และ ปี 2005 ที่กรุงตูนิส ประเทศตูนิเซีย

IGF มีวัตถุประสงค์ในการเป็นพื้นที่ให้กับผู้มีส่วนได้เสีย (Stakeholder) เข้ามาพูดคุยถึงแนวนโยบายสาธารณะของอินเทอร์เน็ตเป็นหลัก ทั้งนี้ IGF เป็นการประชุมที่ไม่มีภาคีชาติสมาชิก เพราะเป็นการประชุมแบบทั่วไป ไม่มีการลงนามในข้อตกลงหรือการจัดตั้งองค์กรใหม่ แม้ว่า IGF จะมีสถานะเป็นการประชุม แต่ก็ถือเป็นส่วนหนึ่งขององค์การสหประชาชาติ เพราะก่อตั้งขึ้นจากการประชุมของสหประชาชาติ ดังนั้นแล้วการบริหารงานหลายอย่างจึงยังคงอยู่ภายใต้การกำกับขององค์การสหประชาชาติ โดยมีสำนักงานเลขาธิการตั้งอยู่ภายในอาคารที่ทำการขององค์การสหประชาชาติ ณ นครเจนีวา สมาพันธรัฐสวิส และมีคณะกรรมการที่ปรึกษา ซึ่งแต่งตั้งโดยเลขาธิการองค์การสหประชาชาติ ทำหน้าที่ช่วยดูแลและจัดการประชุม[39]

ในงานประชุมอินเทอร์เน็ตระหว่างรัฐบาลต่าง ๆ ทั่วโลกประจำปี ค.ศ. 2014 ได้ใช้คำว่า “Trust” หรือความไว้ใจเป็นแกนกลางในการพัฒนานโยบายส่งเสริมการพัฒนาเทคโนโลยีสารสนเทศ โดยเฉพาะตัวแทนจากบริษัทผู้ประกอบการด้านไอทีของโลกอย่าง Google ซึ่งได้กล่าวเพื่อสร้างความเข้าใจและแสดงออกถึงความกระตือรือร้นด้านการสร้างความเชื่อมั่นให้กับผู้ใช้อินเทอร์เน็ต หรือผู้ใช้บริการ โดยประเด็นเรื่องความเชื่อมั่นถือเป็นสาระสำคัญหลักของงานประชุมครั้งนี้ นับจากที่มีจุดเปลี่ยนสำคัญทางประวัติศาสตร์ของการใช้อินเทอร์เน็ตเมื่อเกิดการเปิดเผย

[39] The Evolution of the Internet Governance Forum (IGF), **Internet Society webinar** [Online], 14 February 2014. Available from http://isoc-ny.org/p2/6303.

ความลับโดย เอ็ดเวิร์ด สโนวเด้นส์ ถึงโครงการใหญ่ของสภาความมั่นคงแห่งชาติในการดักเก็บข้อมูลผู้ใช้อินเทอร์เน็ตทั่วโลก เพื่อสร้างฐานข้อมูลในการขุดค้นประวัติการใช้และนำไปประกอบการจารกรรมทั่วโลก โดย เอ็ดเวิร์ด สโนวเด้นส์ อดีตเจ้าหน้าที่ฝ่ายคอมพิวเตอร์ของซีไอเอ ได้เปิดเผยโครงการลับสุดยอดที่ใช้ชื่อรหัสว่า “Prism”[40] โดยโครงการนี้สามารถจารกรรมข้อมูลส่วนตัวของชาวอเมริกันและผู้ที่เข้าไปตั้งถิ่นฐานในประเทศนี้ ด้วยการเจาะเข้าไปในระบบคอมพิวเตอร์แม่ข่ายหรือเซิร์ฟเวอร์ของบริษัทยักษ์ใหญ่ในวงการเทคโนโลยีของสหรัฐฯ 9 แห่ง ได้แก่ Microsoft, Google, Yahoo, Facebook, Apple, AOL, Paltalk, Skype และ Youtube ซึ่งยินยอมพร้อมใจเปิดช่องทางพิเศษนี้ให้เจ้าหน้าที่เข้าไปค้นหาข้อมูลทุกชนิด ไม่ว่าจะเป็น E-mail ภาพถ่าย คลิปเสียง หรือคลิปภาพเคลื่อนไหว ไม่นับรวมไปถึงการดักฟังโทรศัพท์ของชาวอเมริกันกว่า 10 ล้านคน ตลอดจนการดักฟังเสียง วีดีโอ ข้อความ Chat และการถ่ายโอนข้อมูล ต่าง ๆ ของ Skype หรือโปรแกรมติดต่อสื่อสารระหว่างกันผ่านอินเทอร์เน็ตด้วยข้อความพร้อมเสียงและภาพจากกล้อง Webcam เพื่อสืบหาข้อมูลทุกอย่างที่ถือว่าเป็นภัยต่อความมั่นคงของประเทศ รวมทั้งอาจเป็นเบาะแสนำไปสู่การจับกุมกับผู้ก่อการร้าย เรียกได้ว่าเป็นการละเมิดสิทธิเสรีภาพส่วนบุคคลรวมทั้งเสรีภาพในการแสดงความคิดเห็นของประชาชนครั้งใหญ่สุดเป็นประวัติการณ์ จากเอกสารลับหลายชิ้นเผยว่า เพียงแค่ 1 เดือน สามารถรวบรวมข้อมูลข่าวสารอิเล็กทรอนิกส์เกือบ 3,000 ล้านชิ้นจากการจารกรรมข้อมูลส่วนตัวครั้งนี้ และประเด็นที่มีคนให้ความสำคัญมากที่สุดอีกประเด็นหนึ่ง คือ การคุ้มครองข้อมูลส่วนบุคคล สิทธิมนุษยชน ความเป็นส่วนตัว และความมั่นคงในโลกออนไลน์ รวมถึงประเด็นความมั่นคงปลอดภัยของข้อมูลใน Big Data ด้วย โดยภาคธุรกิจยังให้ความสำคัญกับเรื่องการสร้างนโยบายและกฎหมายด้านเทคโนโลยีสารสนเทศโดยมีเรื่อง “ความเป็นส่วนตัวในกรณี Big Data” “การสื่อสารโดยได้รับการปกป้องเป็นนิรนาม” “ความมั่นคงปลอดภัยของข้อมูลใน Big Data” และ “การสร้างความชัดเจนเรื่องการร่วมมือกับรัฐ”[41]

---

[40] อิสรนันท์, **เอ็ดเวิร์ด สโนว์เดน กับการเปิดโปง “พริซึมเกต”** [Online], 25 มิถุนายน 2013. แหล่งที่มา http://thaipublica.org/2013/06/edward-snowden-prism/.

[41] ทศพล ทรรศนกุลพันธ์, **ไทยคือรัฐตัวอย่างระดับโลก: งานประชุมอินเทอร์เน็ตระหว่างรัฐบาลประจำปี 2557 (IGF 2014)** [Online], 17 กันยายน 2557. แหล่งที่มา http://www.prachatai.com/journal/2014/09/55568.

บทที่ 3
กฎหมายที่เกี่ยวข้องกับประเด็น Big Data ของไทย และต่างประเทศ

กฎหมายเทคโนโลยีสารเทศมีบทบาทที่ช่วยเสริมโครงสร้างพื้นฐานที่เกื้อหนุนให้สมบูรณ์ได้ เป็นองค์ประกอบที่สำคัญของโครงสร้างพื้นฐานที่เกื้อหนุน โดยกฎหมายสามารถเป็นเครื่องมือหนึ่งใน การผลักดันโครงสร้างพื้นฐานอื่น ๆ ให้เกิดขึ้นได้ในทางปฏิบัติ โดยการนำสิ่งเหล่านั้นมาเขียนเป็น กฎหมายเพื่อให้เกิดการบังคับใช้ และเกิดเป็นระบบหรือมาตรฐานในทางปฏิบัติที่ชัดเจน ซึ่งเป็นการ เสริมให้โครงสร้างพื้นฐานที่เกื้อหนุนสมบูรณ์ยิ่งขึ้น และเป็นปัจจัยให้เกิดความเชื่อมั่นและความ น่าเชื่อถือในการทำธุรกรรมทางอิเล็กทรอนิกส์ที่เพิ่มมากขึ้น ซึ่งสามารถจำแนกตามบทบาทได้เป็น 3 ลักษณะ คือ

1) เป็นกฎหมายที่กำหนดในลักษณะของการรับรองกิจกรรมต่าง ๆ ที่ทำในทางอิเล็กทรอนิกส์ ให้มีผลผูกพันตามกฎหมาย เช่น การรับรองผลทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ เป็นต้น หรือ กำหนดเงื่อนไขที่จำเป็นที่หน่วยงานหรือผู้ประกอบการที่ดำเนินงานหรือให้บริการด้านธุรกรรมทาง อิเล็กทรอนิกส์ต้องปฏิบัติตาม เช่น การกำหนดให้หน่วยงานต้องมีแนวนโยบายรักษาความมั่นคง ปลอดภัยในระบบสารสนเทศ เป็นต้น ทั้งนี้ก็เพื่อสร้างความเชื่อมั่นต่อผู้ที่ต้องการทำธุรกรรมผ่านทาง อิเล็กทรอนิกส์ว่าสิ่งที่ตนเองทำอยู่นั้นมีกฎหมายรองรับ และระบบที่ตนเองกำลังใช้งานหรือใช้บริการ อยู่เป็นระบบที่น่าเชื่อถือและมีความปลอดภัยนั่นเอง

โดยได้แบ่งกฎหมายออกเป็น 3 ฉบับ ได้แก่ กฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ และกฎหมายเกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์ อย่างไรก็ตาม ในภายหลังได้รวมหลักการของกฎหมายทั้ง 3 ฉบับไว้ในพระราชบัญญัติว่าด้วยธุรกรรม ทางอิเล็กทรอนิกส์ พ.ศ. 2544 ฉบับเดียว ซึ่งต่อมามีการแก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วย ธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551

นอกจากนี้ ยังได้มีการออกกฎหมายลำดับรองภายใต้พระราชบัญญัติว่าด้วยธุรกรรมทาง อิเล็กทรอนิกส์อีกหลายฉบับ เพื่อกำหนดเงื่อนไขในรายละเอียดต่าง ๆ ให้ชัดเจนยิ่งขึ้น ได้แก่ พระราช กฤษฎีกากำหนดประเภทธุรกรรมในทางแพ่งและพาณิชย์ที่ยกเว้นมิให้นำกฎหมายว่าด้วยธุรกรรมทาง อิเล็กทรอนิกส์มาใช้บังคับ พ.ศ. 2549 พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำ ธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 พระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการ การชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551 และพระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการ ทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553 รวมทั้งอนุบัญญัติในลำดับประกาศอีกจำนวน 11 ฉบับ ด้วยกัน

2) เป็นกฎหมายที่มีบทบาทหรือทำงานในลักษณะการป้องปราม แก้ไขปัญหาและอุปสรรค รวมทั้งลดความเสี่ยง ภัยคุกคาม หรือความเสียหายใด ๆ จากการประยุกต์ใช้เทคโนโลยีสารสนเทศและการสื่อสารในทางมิชอบ หรือการละเมิดความเป็นส่วนตัว อันประกอบด้วยกฎหมายจำนวน 2 ฉบับ ได้แก่ กฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ และกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

สำหรับกฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ หรือชื่ออย่างเป็นทางการคือ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จะอยู่ในความรับผิดชอบของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร และภายใต้กฎหมายฉบับนี้ได้มีการจัดทำกฎหมายลำดับรองเพื่อกำหนดหลักเกณฑ์ในทางปฏิบัติต่าง ๆ ทั้งกฎกระทรวง ประกาศ และระเบียบ รวมจำนวน 5 ฉบับ และมีการจัดทำประกาศเรื่องแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เพิ่มเติมด้วย

ส่วนกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ในขณะนี้ยังไม่มีกฎหมายเฉพาะที่ว่าเรื่องการคุ้มครองข้อมูลส่วนบุคคลออกมาใช้บังคับ แต่จริง ๆ แล้วหลักการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลปัจจุบันก็มีแฝงอยู่ในกฎหมายหลายฉบับ เช่น พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ที่กำหนดหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในการครอบครองของหน่วยงานรัฐ หรือพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 ที่กำหนดการคุ้มครองข้อมูลส่วนบุคคลอยู่ในการครอบครองของสถาบันการเงิน เป็นต้น แต่ในภาพรวมแล้วยังไม่ครอบคลุมหน่วยงานทั้งหมดที่มีการจัดเก็บข้อมูลส่วนบุคคล รวมถึงกลไกการคุ้มครองข้อมูลส่วนบุคคลก็ยังไม่ชัดเจนหรือไม่มีมาตรฐานตามแนวทางสากล ดังนั้นคงต้องรอกฎหมายเฉพาะว่าจะอุดช่องว่างหรือแก้ปัญหาเหล่านี้ได้ดีเพียงใด ซึ่งเท่าที่ทราบมาขณะนี้อยู่ระหว่างการเสนอพิจารณาต่อสภาและเป็นกฎหมายที่บังคับใช้กับหน่วยงานเอกชน

3) เป็นกฎหมายที่ยกระดับคุณภาพชีวิตของประชาชนให้มีความเท่าเทียมกันในการเข้าถึงสารสนเทศ สำหรับกฎหมายที่ทำหน้าที่ในบทบาทนี้ได้แก่ กฎหมายลำดับรองของรัฐธรรมนูญ ตามมาตรา 78 เกี่ยวกับการพัฒนาโครงสร้างพื้นฐานสารสนเทศให้ทั่วถึงและเท่าเทียมกัน ซึ่งรัฐบาลและกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารก็ได้มีการผลักดันให้มีการดำเนินนโยบายทางปฏิบัติแทนการออกเป็นกฎหมายที่ใช้บังคับ[1]

[1] คัชชิดา มีท่อธาร และณัฐวรรธน์ สุขวงศ์ตระกูล, **บทบาทของกฎหมายเทคโนโลยีสารสนเทศ** [Online], 22 พฤศจิกายน 2555. แหล่งที่มา https://www.etda.or.th/etda_website/mains/display/1493.

3.1 กฎหมายไทยที่เกี่ยวข้องกับ Big Data

กฎหมายไทยที่เกี่ยวข้องกับ Big Data ได้แก่ กฎหมายคุ้มครองข้อมูลส่วนบุคคล ซึ่งมีวิวัฒนาการที่ไม่ยาวมากนัก เดิมจะมีบัญญัติอยู่ในประมวลกฎหมายแพ่งและพาณิชย์ และประมวลกฎหมายอาญา โดยเป็นการคุ้มครองสิทธิความเป็นส่วนตัวในลักษณะของการแก้ไขเยียวยา เมื่อเกิดความเสียหายต่อสิทธิความเป็นส่วนตัวของบุคคลแล้ว ผู้เสียหายย่อมมีสิทธิฟ้องคดีต่อศาลเพื่อปกป้องสิทธิของแต่ละบุคคลเป็นการส่วนตัว ซึ่งการคุ้มครองในลักษณะนี้ยังใช้อยู่จนถึงทุกวันนี้

3.1.1 กฎหมายที่เกี่ยวข้องกับความเป็นส่วนตัว (Privacy) และความมั่นคงปลอดภัยของข้อมูล (Data Security)

กฎหมายที่เกี่ยวข้องกับสิทธิความเป็นอยู่ส่วนตัวกรณี Big Data ในประเทศไทยได้รับการคุ้มครองตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 420, 422 และ 423 ซึ่งเป็นเรื่องความรับผิดว่าด้วยละเมิดในทางแพ่ง อันเป็นกรณีที่บุคคลหนึ่งได้ล่วงละเมิดสิทธิของบุคคลอื่น จนก่อให้เกิดความเสียหายในเกียรติยศ ชื่อเสียง หรือสิทธิอื่นใดตามที่กฎหมายบัญญัติรับรองและคุ้มครองให้ ส่วนทางกฎหมายอาญาก็มีบัญญัติไว้อย่างชัดแจ้งในการคุ้มครองข้อมูลข่าวสารส่วนบุคคลในลักษณะความผิดฐานเปิดเผยความลับ ตามประมวลกฎหมายอาญา มาตรา 322-323

หากพิจารณาถึงบทบัญญัติของกฎหมายในเรื่องการคุ้มครองข้อมูลข่าวสารส่วนบุคคลที่อยู่ในประมวลกฎหมายแพ่งและพาณิชย์ และประมวลกฎหมายอาญาแล้วจะเห็นได้ว่า ยังไม่มีการบัญญัติถ้อยคำที่ชัดเจนถึงการคุ้มครองข้อมูลข่าวสารส่วนบุคคลโดยเฉพาะเป็นเรื่อง ๆ แต่กล่าวไว้อย่างรวม ๆ ส่วนการคุ้มครองในทางกฎหมายอาญาก็มีเฉพาะการคุ้มครองในเรื่องการเปิดเผยข้อมูลข่าวสารในการติดต่อสื่อสารระหว่างบุคคล และการเปิดเผยความลับโดยพนักงานหรือบุคคลที่ได้ข้อมูลนั้นมาในทางการประกอบวิชาชีพอย่างใดอย่างหนึ่ง หรือเป็นผู้ศึกษาในสาขาวิชาชีพนั้น เช่น แพทย์ เภสัชกร ผู้สอบบัญชี หรือทนายความ เป็นต้น ซึ่งการเปิดเผยทั้งสองกรณีดังกล่าวต้องก่อให้เกิดความเสียหายแก่บุคคลผู้เป็นเจ้าของข้อมูลด้วย จึงจะครบองค์ประกอบความผิดทางอาญา

การรักษาความมั่นคงปลอดภัยของข้อมูลคือสิ่งที่ผู้ดูแลต้องให้ความสำคัญต่อระบบข้อมูล กล่าวคือ การป้องกันสิ่งที่เกิดขึ้นกับระบบ เช่น การลบข้อมูลโดยไม่ตั้งใจ ระบบเกิดการผิดพลาด หรือเหตุการณ์ทางธรรมชาติ เช่น ไฟดับ เป็นต้น ซึ่งการรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security) ประกอบด้วย

- การรักษาความมั่นคงปลอดภัยของขยะข้อมูล (Secured Waste)
- การควบคุมในระบบคอมพิวเตอร์ (Internal Controls)
- การตรวจสอบ (Auditor Checks)
- การตรวจสอบประวัติผู้สมัครงาน (Applicant Screening)
- การใช้รหัสผ่าน (Passwords)

- ตัวป้องกันในซอฟต์แวร์ (Built-in Software Protection)

หลักการแก้ปัญหาโดยใช้กฎหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ได้แก่ การสร้างจริยธรรมในหมู่สมาชิกในสังคมจึงถูกต้องและยั่งยืนที่สุด เพื่อให้สังคมได้สร้างกลไกบังคับในรูปของวัฒนธรรมประเพณีที่ดีงาม และต้องตรากฎ ระเบียบ ข้อบังคับในลักษณะต่าง ๆ รวมถึงกฎหมาย โดยรัฐจะต้องพัฒนาเศรษฐกิจท้องถิ่นและระบบสาธารณูปโภค ตลอดจนโครงสร้างพื้นฐานสารสนเทศให้ทั่วถึงและเท่าเทียมกันทั่วประเทศ

ในปัจจุบันประเทศไทยมีกฎหมายเกี่ยวกับความเป็นส่วนตัว (Privacy) และกฎหมายเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security) ซึ่งสามารถนำมาประยุกต์ใช้กับกรณีความเป็นส่วนตัว และความมั่นคงปลอดภัยของข้อมูลใน Big Data ได้ กฎหมายดังกล่าวมีดังต่อไปนี้

3.1.1.1 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

สำหรับการคุ้มครองตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 ซึ่งในพระราชบัญญัติข้อมูลข่าวสารได้กล่าวถึง คำว่าข้อมูลข่าวสารไว้ว่า “ข้อมูลข่าวสาร”[2] หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริง ข้อมูลหรือสิ่งใด ๆ ไม่ว่าการสื่อความหมายนั้น จะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่ายฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้ และคำว่าข้อมูลข่าวสารราชการ คือ “ข้อมูลข่าวสารของราชการ”[3] หมายความว่า ข้อมูลข่าวสารที่อยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐ ไม่ว่าจะเป็นข้อมูลข่าวสารเกี่ยวกับการดำเนินงานของรัฐหรือข้อมูลข่าวสารเกี่ยวกับเอกชนและให้ความหมายของคำว่า “ข้อมูลข่าวสารส่วนบุคคล”[4] หมายความว่า ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้นหรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่าย และให้หมายความรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย ซึ่งในพระราชบัญญัตินี้ได้ให้ความหมายในเรื่องของข้อมูลประเภทต่าง ๆ โดยลำดับและมีการกล่าวถึงการคุ้มครองข้อมูลส่วนบุคคลโดยได้กล่าวถึงคำว่าข้อมูลส่วนบุคคลใน มาตรา 4 แล้ว ยังได้อธิบายให้ชัดเจนอีกว่า คำว่าบุคคลคืออะไร โดยบัญญัติว่า

---

[2] มาตรา 4 พระราชบัญญัติข้อมูลข่าวสารทางราชการ พ.ศ. 2540.

[3] เรื่องเดียวกัน.

[4] เรื่องเดียวกัน.

มาตรา 21[5] เพื่อประโยชน์แห่งหมวดนี้ “บุคคล” หมายความว่า บุคคลธรรมดาที่มีสัญชาติไทย และบุคคลธรรมดาที่ไม่มีสัญชาติไทยแต่มีถิ่นที่อยู่ในประเทศไทยและได้บัญญัติหน่วยงานของรัฐต้องปฏิบัติเกี่ยวกับการจัดระบบข้อมูลข่าวสารส่วนบุคคลดังนี้

มาตรา 23 หน่วยงานของรัฐต้องปฏิบัติเกี่ยวกับการจัดระบบข้อมูลข่าวสารส่วนบุคคลดังต่อไปนี้

(1) ต้องจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลเพียงเท่าที่เกี่ยวข้อง และจำเป็นเพื่อการดำเนินงานของหน่วยงานของรัฐให้สำเร็จตามวัตถุประสงค์เท่านั้น และยกเลิกการจัดให้มีระบบดังกล่าวเมื่อหมดความจำเป็น

(2) พยายามเก็บข้อมูลข่าวสารโดยตรงจากเจ้าของข้อมูล โดยเฉพาะอย่างยิ่งในกรณีที่จะกระทบถึงประโยชน์ได้เสียโดยตรงของบุคคลนั้น

(3) จัดให้มีการพิมพ์ในราชกิจจานุเบกษา และตรวจสอบแก้ไขให้ถูกต้องอยู่เสมอเกี่ยวกับสิ่งดังต่อไปนี้

(ก) ประเภทของบุคคลที่มีการเก็บข้อมูลไว้

(ข) ประเภทของระบบข้อมูลข่าวสารส่วนบุคคล

(ค) ลักษณะการใช้ข้อมูลตามปกติ

(ง) วิธีการขอตรวจดูข้อมูลข่าวสารของเจ้าของข้อมูล

(จ) วิธีการขอให้แก้ไขเปลี่ยนแปลงข้อมูล

(ฉ) แหล่งที่มาของข้อมูล

(4) ตรวจสอบแก้ไขข้อมูลข่าวสารส่วนบุคคลในความรับผิดชอบให้ถูกต้องอยู่เสมอ

(5) จัดระบบรักษาความมั่นคงปลอดภัยให้แก่ระบบข้อมูลข่าวสารส่วนบุคคลตามความเหมาะสม เพื่อป้องกันมิให้มีการนำไปใช้โดยไม่เหมาะสมหรือเป็นผลร้ายต่อเจ้าของข้อมูล

ในกรณีที่เก็บข้อมูลข่าวสารโดยตรงจากเจ้าของข้อมูล หน่วยงานของรัฐต้องแจ้งให้เจ้าของข้อมูลทราบล่วงหน้าหรือพร้อมกับการขอข้อมูลถึงวัตถุประสงค์ที่จะนำข้อมูลมาใช้ ลักษณะการใช้ข้อมูลตามปกติ และกรณีที่ขอข้อมูลนั้นเป็นกรณีที่อาจให้ข้อมูลได้โดยความสมัครใจหรือเป็นกรณีมีกฎหมายบังคับ

หน่วยงานของรัฐต้องแจ้งให้เจ้าของข้อมูลทราบในกรณีมีการให้จัดส่งข้อมูลข่าวสารส่วนบุคคลไปยังที่ใดซึ่งจะเป็นผลให้บุคคลทั่วไปทราบข้อมูลข่าวสารนั้นได้ เว้นแต่เป็นไปตามลักษณะการใช้ข้อมูลตามปกติและยังได้มีบทบัญญัติห้ามมิให้หน่วยงานรัฐที่ควบคุมดูแลเปิดเผยข้อมูลส่วนบุคคลแก่หน่วยงานอื่นโดยเจ้าของข้อมูลไม่ยินยอมแต่มีข้อยกเว้นตาม มาตรา 24 และมาตรา 25 ดังนี้

---

[5] มาตรา 21 พระราชบัญญัติข้อมูลข่าวสารทางราชการ พ.ศ. 2540.

มาตรา 24 หน่วยงานของรัฐจะเปิดเผยข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความควบคุมดูแลของตนต่อหน่วยงานของรัฐแห่งอื่นหรือผู้อื่นโดยปราศจากความยินยอมเป็นหนังสือของเจ้าของข้อมูลที่ให้ไว้ล่วงหน้าหรือในขณะนั้นมิได้ เว้นแต่เป็นการเปิดเผยดังต่อไปนี้

(1) ต่อเจ้าหน้าที่ของรัฐในหน่วยงานของตน เพื่อการนำไปใช้ตามอำนาจหน้าที่ของหน่วยงานของรัฐแห่งนั้น

(2) เป็นการใช้ข้อมูลตามปกติภายในวัตถุประสงค์ของการจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลนั้น

(3) ต่อหน่วยงานของรัฐที่ทำงานด้วยการวางแผน หรือการสถิติ หรือสำมะโนต่าง ๆ ซึ่งมีหน้าที่ต้องรักษาข้อมูลข่าวสารส่วนบุคคลไว้ไม่ให้เปิดเผยต่อไปยังผู้อื่น

(4) เป็นการให้เพื่อประโยชน์ในการศึกษาวิจัย โดยไม่ระบุชื่อหรือส่วนที่ทำให้รู้ว่าเป็นข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับบุคคลใด

(5) ต่อหอจดหมายเหตุแห่งชาติ กรมศิลปากร หรือหน่วยงานอื่นของรัฐตามมาตรา 26 วรรคหนึ่ง เพื่อการตรวจดูคุณค่าในการเก็บรักษา

(6) ต่อเจ้าหน้าที่ของรัฐ เพื่อการป้องกันการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย การสืบสวน การสอบสวน หรือการฟ้องคดี ไม่ว่าเป็นคดีประเภทใดก็ตาม

(7) เป็นการให้ซึ่งจำเป็น เพื่อการป้องกันหรือระงับอันตรายต่อชีวิตหรือสุขภาพของบุคคล

(8) ต่อศาล และเจ้าหน้าที่ของรัฐหรือหน่วยงานของรัฐหรือบุคคลที่มีอำนาจตามกฎหมายที่จะขอข้อเท็จจริงดังกล่าว

(9) กรณีอื่นตามที่กำหนดในพระราชกฤษฎีกา

การเปิดเผยข้อมูลข่าวสารส่วนบุคคลตามวรรคหนึ่ง (3) (4) (5) (6) (7) (8) และ (9) ให้มีการจัดทำบัญชีแสดงการเปิดเผยกำกับไว้กับข้อมูลข่าวสารนั้น ตามหลักเกณฑ์และวิธีการที่กำหนดในกฎกระทรวง

มาตรา 25 ภายใต้บังคับ มาตรา 14 และมาตรา 15 บุคคลย่อมมีสิทธิที่จะได้รู้ถึงข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับตน และเมื่อบุคคลนั้นมีคำขอเป็นหนังสือ หน่วยงานของรัฐที่ควบคุมดูแลข้อมูลข่าวสารนั้นจะต้องให้บุคคลนั้นหรือผู้กระทำการแทนบุคคลนั้นได้ตรวจดูหรือได้รับสำเนาข้อมูลข่าวสารส่วนบุคคลส่วนที่เกี่ยวกับบุคคลนั้น และให้นำ มาตรา 9 วรรคสอง และวรรคสาม มาใช้บังคับโดยอนุโลม

สรุปได้ว่าพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มีสาระสำคัญอยู่ 2 ประการ คือ การรับรองสิทธิของประชาชนในการเข้าถึงข้อมูล และการคุ้มครองข้อมูลส่วนบุคคลของประชาชน ซึ่งหลักการสำคัญในการคุ้มครองข้อมูลส่วนบุคคลคือ หากหน่วยงานของรัฐจะเปิดเผย

ข้อมูลส่วนบุคคลที่หน่วยงานของตนเก็บรักษาอยู่ ไม่ว่าจะเป็นการเปิดเผยต่อหน่วยงานราชการอื่น ๆ หรือต่อบุคคลอื่น ๆ จะต้องได้รับความยินยอมจากเจ้าของข้อมูล เว้นแต่กรณีที่กฎหมายยกเว้นให้ อย่างไรก็ตาม ยังคงปรากฏให้เห็นอยู่ทั่วไปว่า ข้อมูลส่วนบุคคลของประชาชนที่หน่วยงานของรัฐมีหน้าที่ต้องควบคุมดูแลและคุ้มครองอย่างดีนั้น ถูกเปิดเผยและนำไปใช้ประโยชน์กันอยู่บ่อยครั้ง โดยไม่ได้รับคำยินยอมจากเจ้าของข้อมูลแต่อย่างใด

นอกจากนี้ ข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานของรัฐบางแห่งยังไม่ได้รับการคุ้มครองหรือการเก็บรักษาไว้ดีเท่าที่ควร เพราะปรากฏว่ามีการนำเสนอข่าวทางสื่อต่าง ๆ ว่ามีการนำข้อมูลส่วนบุคคลบางส่วนออกไปใช้ในทางที่ไม่เหมาะสมอยู่บ่อยครั้ง เช่น กรณีผู้สมัครรับเลือกตั้งไปสืบค้นวันเดือนปีเกิดของผู้ที่อยู่ในเขตรับเลือกตั้งเพื่อส่งจดหมายไปอวยพรวันเกิด ซึ่งคณะกรรมการข้อมูลข่าวสารของราชการเห็นว่า พระราชบัญญัติข้อมูลข้อมูลข่าวสาร พ.ศ. 2540 มีจุดมุ่งหมายที่จะคุ้มครองข้อมูลส่วนบุคคลมิให้ถูกเปิดเผย หรือถูกนำไปใช้อย่างไม่เหมาะสม หรือเป็นผลเสียหายต่อเจ้าของข้อมูล และการเปิดเผยข้อมูลส่วนบุคคลจะต้องได้รับความยินยอมจากเจ้าของข้อมูล เว้นแต่เป็นการเปิดเผยตามข้อยกเว้นตามที่กฎหมายกำหนดไว้ ดังนั้น เพื่อให้การปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานของรัฐเป็นไปอย่างถูกต้อง คณะกรรมการข้อมูลข่าวสารของราชการได้มีหนังสือแจ้งกำชับหน่วยงานของรัฐเมื่อวันที่ 8 มิถุนายน พ.ศ. 2549 กำชับหน่วยงานต่าง ๆ ของรัฐให้ปฏิบัติตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 โดยเคร่งครัดต่อไป ตามมติของคณะรัฐมนตรี วันที่ 28 ธันวาคม พ.ศ. 2547[6]

3.1.1.2 ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...[7]

ปัจจุบันปัญหาการล่วงละเมิดข้อมูลส่วนบุคคลมีอยู่เป็นจำนวนมาก โดยเฉพาะการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์เปิดเผยหรือเผยแพร่จนทำให้เกิดความเสียหาย ปัจจุบันประเทศไทยมีการคุ้มครองข้อมูลส่วนบุคคลโดยบทบัญญัติของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 แต่เนื่องจากใช้บังคับเฉพาะในหน่วยงานของรัฐเท่านั้น ไม่ครอบคลุมข้อมูลส่วนบุคคลที่อยู่ในภาคเอกชน ซึ่งมีปริมาณข้อมูลที่จัดเก็บไม่น้อยกว่าข้อมูลในภาครัฐ เช่น ข้อมูลในธนาคารพาณิชย์ ข้อมูลในโรงพยาบาลเอกชน ข้อมูลพนักงานลูกจ้างในบริษัท ห้างร้านเอกชนต่าง ๆ ข้อมูลลูกค้า ข้อมูลสมาชิกกิจกรรมทางธุรกิจ ข้อมูลของผู้สมัครเป็นสมาชิกบัตรและบริการต่าง ๆ ดังนั้น เพื่อให้การ

---

[6] สำนักนายกรัฐมนตรี, **รายงานเกี่ยวกับการปฏิบัติตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540** [Online], 17 มกราคม 2558. แหล่งที่มา http://www.oic.go.th/FILEROOM-PDF/CABOICFORM05/ DRAWER05/GENERAL/DATA0000/00000419.tif.pdf.

[7] สำนักงานคณะกรรมการกฤษฎีกา, **ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...** [Online], 2552. แหล่งที่มา http://web.krisdika.go.th/data/news/news10837.pdf.

คุ้มครองสิทธิในข้อมูลส่วนบุคคลเป็นไปอย่างมีประสิทธิภาพ และลดช่องว่างของกฎหมายที่มีอยู่ จึงควรมีบทบัญญัติของกฎหมายที่มีลักษณะเป็นกฎหมายกลาง เพื่อขยายขอบเขตการคุ้มครองสิทธิและเสรีภาพให้ครอบคลุมข้อมูลส่วนบุคคลทั้งหมด สำนักนายกรัฐมนตรีโดยสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการได้ศึกษาเตรียมการดำเนินงานเพื่อการคุ้มครองข้อมูลส่วนบุคคลของประชาชน และยกร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... ขึ้นมา

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... นี้ มีวัตถุประสงค์ที่บัญญัติขึ้นเพื่อเป็นกฎหมายกลางในการให้ความคุ้มครองสิทธิข้อมูลส่วนบุคคล ซึ่งจะกำหนดหลักเกณฑ์ กระบวนการและมาตรการต่าง ๆ ที่เป็นมาตรฐานทั่วไป การให้การดูแลและคุ้มครองสิทธิส่วนบุคคลซึ่งมีกฎหมายบัญญัติไว้เป็นการเฉพาะแล้ว การให้การดูแลและคุ้มครองสิทธิส่วนบุคคลในเรื่องนั้นก็จะเป็นไปตามหลักเกณฑ์ กระบวนการ และมาตรการที่กฎหมายเฉพาะนั้นกำหนด แต่หากเป็นกรณีที่กฎหมายอื่นใดที่บัญญัติเกี่ยวกับข้อมูลส่วนบุคคลไม่ได้กำหนด หรือกำหนดไว้บางเรื่อง กรณีดังกล่าวร่างพระราชบัญญัติฉบับนี้กำหนดให้นำหลักเกณฑ์ กระบวนการ และมาตรการตามที่กำหนดไว้ในร่างพระราชบัญญัติฉบับนี้ไปใช้บังคับในส่วนที่กฎหมายอื่นมิได้กำหนด อย่างไรก็ดีด้วยวัตถุประสงค์ของร่างพระราชบัญญัติฉบับนี้ประสงค์ที่จะให้ความคุ้มครองสิทธิข้อมูลส่วนบุคคลในความครอบครองของเอกชน และหน่วยงานของรัฐที่มีวัตถุประสงค์ในการดำเนินงานเชิงธุรกิจหรือการพาณิชย์เป็นหลัก ดังนั้นบทบัญญัติต่าง ๆ ตามพระราชบัญญัตินี้จึงกำหนดมิให้นำไปใช้บังคับกับการประมวลผลข้อมูลส่วนบุคคลของหน่วยงานของรัฐ ซึ่งอยู่ภายใต้บังคับตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และเพื่อให้บรรลุวัตถุประสงค์แห่งพระราชบัญญัตินี้ที่จะให้เป็นกฎหมายกลางใช้บังคับกับหน่วยงานทั้งหลายที่เกี่ยวข้อง รวมถึงการบริหารกฎหมายให้เป็นไปอย่างมีประสิทธิภาพ จึงได้กำหนดให้นายกรัฐมนตรีเป็นผู้รักษาการตามพระราชบัญญัติฉบับนี้

นอกจากหลักการดังกล่าวแล้ว ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... ได้กำหนดสาระสำคัญในการให้ความคุ้มครองสิทธิในข้อมูลส่วนบุคคลดังต่อไปนี้

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... มาตรา 7 กำหนดให้มี “คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล” ทำหน้าที่ดูแลคุ้มครองข้อมูลข่าวสารส่วนบุคคลตามกฎหมาย และวางนโยบายและมาตรการในการให้ความคุ้มครองสิทธิในข้อมูลส่วนบุคคล ประกอบด้วยนายกรัฐมนตรีหรือรัฐมนตรีซึ่งนายกรัฐมนตรีมอบหมายเป็นประธานกรรมการ และกรรมการจากส่วนราชการ ภาคเอกชน รวมถึงผู้ทรงคุณวุฒิเพื่อให้การใช้อำนาจเป็นไปอย่างมีประสิทธิภาพ ได้แก่

กรรมการโดยตำแหน่งจากส่วนราชการ ประกอบด้วยปลัดสำนักนายกรัฐมนตรี ปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เลขาธิการคณะกรรมการกฤษฎีกา อธิบดีกรมคุ้มครองสิทธิและเสรีภาพ และผู้ว่าการธนาคารแห่งประเทศไทย

กรรมการ ซึ่งเป็นผู้แทนคณะกรรมการคุ้มครองผู้บริโภคหนึ่งคน ผู้แทนจากหอการค้าไทยหนึ่งคน และผู้แทนสมาคมธนาคารแห่งประเทศไทยหนึ่งคน

กรรมการผู้ทรงคุณวุฒิซึ่งนายกรัฐมนตรีแต่งตั้งจากผู้ที่มีความรู้ความเชี่ยวชาญด้านกฎหมาย และด้านเทคโนโลยี ด้านละสองคน ซึ่งต้องแต่งตั้งจากภาคเอกชนไม่น้อยกว่ากึ่งหนึ่ง

คณะกรรมการชุดนี้ นอกจากมีอำนาจหน้าที่ดังกล่าวข้างต้นแล้ว ยังมีอำนาจหน้าที่ในการควบคุมดูแล และส่งเสริมการให้ความคุ้มครองสิทธิในข้อมูลส่วนบุคคล[8]

เพื่อประโยชน์ในการดำเนินการของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และเพื่อให้เป็นไปตามวัตถุประสงค์แห่งร่างพระราชบัญญัตินี้ ตลอดจนเพื่อให้เกิดประสิทธิภาพในการดำเนินการตามอำนาจหน้าที่ของคณะกรรมการ ร่างพระราชบัญญัติฉบับนี้กำหนดให้มี “สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล” อยู่ในสังกัดของสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ ซึ่งจะมีฐานะเป็นกรม มีเลขาธิการสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการเป็นผู้บังคับบัญชาและรับผิดชอบในการปฏิบัติราชการของสำนักงาน ทำหน้าที่หน่วยงานธุรการของคณะกรรมการขึ้น เพื่อรับผิดชอบในการปฏิบัติงานด้านธุรการและด้านวิชาการให้แก่คณะกรรมการ โดยมีอำนาจหน้าที่ตามที่บัญญัติไว้ในร่างพระราชบัญญัติ มาตรา 15

ความหมายของข้อมูลส่วนบุคคลตามร่างพระราชบัญญัติฉบับนี้ มีความหมายกว้างกว่าข้อมูลส่วนบุคคลตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 เนื่องจากเป็นข้อมูลส่วนบุคคลที่อยู่ในความครอบครอง หรือดำเนินการของภาคเอกชน และหน่วยงานของรัฐที่ดำเนินงานเชิงธุรกิจหรือการพาณิชย์ ดังนั้นการให้ความคุ้มครองสิทธิในข้อมูลส่วนบุคคลจึงได้แก่ การเก็บรวบรวม การบันทึก การจัดหมวดหมู่ การใช้ประโยชน์ การเก็บรักษา การแก้ไข การโอน และการเปิดเผย ฯลฯ ซึ่งตามร่างพระราชบัญญัตินี้เรียกว่า “การควบคุมข้อมูลส่วนบุคคล”

การควบคุมข้อมูลส่วนบุคคลตามร่างพระราชบัญญัตินี้ ได้กำหนดหลักการในการคุ้มครองสิทธิในข้อมูลส่วนบุคคลไว้ได้แก่ หลักความยินยอมและปกปิด เป็นหลักการทั่วไป ส่วนการเปิดเผย เป็นข้อยกเว้น นอกจากนี้ในการประมวลผลต้องเป็นไปตามวัตถุประสงค์ของกิจการของผู้ควบคุมข้อมูลส่วนบุคคลด้วย[9]

สำหรับหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลนั้น นอกจากผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการควบคุมข้อมูลส่วนบุคคลตามหลักเกณฑ์ วิธีการและเงื่อนไขตามที่บัญญัติไว้ในร่างพระราชบัญญัตินี้ และจะต้องจัดให้มีนายทะเบียนขึ้นเพื่อทำหน้าที่ในการควบคุมดูแลรับผิดชอบในการประมวลผลข้อมูลส่วนบุคคล

---

[8] มาตรา 11 ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...

[9] มาตรา 20 ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...

ตามร่างพระราชบัญญัตินี้ ได้แบ่งการประมวลผลข้อมูลส่วนบุคคลออกเป็นส่วนต่าง ๆ ดังนี้

1) การเก็บรวบรวมข้อมูลส่วนบุคคล

กำหนดให้เก็บรวบรวมข้อมูลส่วนบุคคลได้เพียงเท่าที่เกี่ยวข้องและจำเป็นแก่การดำเนินกิจการตามวัตถุประสงค์ของผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น โดยห้ามเก็บรวบรวมข้อมูลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ข้อมูลทางพันธุกรรม ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนา ฯลฯ เว้นแต่ได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูล และเพื่อให้สอดคล้องกับหลักการในการให้ความคุ้มครองสิทธิในข้อมูลส่วนบุคคลของเจ้าของข้อมูล ร่างพระราชบัญญัติฉบับนี้ได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งต่อเจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดก่อนหรือในขณะเก็บรวบรวมข้อมูล[10]

เมื่อได้ดำเนินการเก็บรวบรวมข้อมูลส่วนบุคคลแล้ว ร่างพระราชบัญญัติฉบับนี้ได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งเจ้าของข้อมูลส่วนบุคคลถึง ชื่อ สถานที่ทำการ สถานภาพของผู้ควบคุม แจ้งถึงวัตถุประสงค์ และระยะเวลาของการเก็บรวบรวมข้อมูล รวมถึงสิทธิของเจ้าของข้อมูลส่วนบุคคลด้วย[11]

2) การใช้และการเปิดเผยข้อมูล

กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องใช้ข้อมูลส่วนบุคคลที่อยู่ในความครอบครองดูแลตามวัตถุประสงค์ของการเก็บรวบรวมข้อมูลเท่านั้น การใช้นอกเหนือวัตถุประสงค์จะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อน อย่างไรก็ดีในกรณีที่มีเหตุจำเป็นที่มีผลกระทบต่อชีวิต ร่างกาย อนามัยของเจ้าของข้อมูลส่วนบุคคล ร่างพระราชบัญญัติฉบับนี้กำหนดเป็นข้อยกเว้นให้สามารถเปิดเผยข้อมูลส่วนบุคคลได้ในกรณีต่าง ๆ[12] โดยการเปิดเผยจะต้องทำเท่าที่จำเป็น และเมื่อได้เปิดเผยแล้วให้แจ้งเจ้าของข้อมูลทราบ รวมทั้งผู้ซึ่งได้รับข้อมูลต้องใช้ข้อมูลตามวัตถุประสงค์เท่านั้น และผู้ควบคุมข้อมูลต้องบันทึกการเปิดเผยข้อมูลนั้นเพื่อการตรวจสอบด้วย

3) การเก็บรักษาข้อมูลส่วนบุคคล

กำหนดให้เก็บรักษาข้อมูลของเจ้าของข้อมูลส่วนบุคคลได้เท่าระยะเวลาที่กำหนดหรือเท่าที่จำเป็นตามวัตถุประสงค์ของการเก็บรวบรวมข้อมูล และเมื่อพ้นระยะเวลา หรือหมดความจำเป็น หรือเจ้าของข้อมูลเพิกถอนความยินยอม ผู้ควบคุมข้อมูลส่วนบุคคลต้องลบทำลายข้อมูลนั้นโดยเร็ว เว้นแต่ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีความจำเป็นต้องเก็บรักษาข้อมูลนั้นไว้เพื่อเป็น

---

[10] มาตรา 23 ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...

[11] มาตรา 24 ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...

[12] มาตรา 25 ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...

สถิติการศึกษาวิจัย ผู้ควบคุมข้อมูลส่วนบุคคลอาจไม่ลบทำลายข้อมูลนั้นก็ได้ แต่ต้องได้รับความยินยอมจากเจ้าของข้อมูล[13]

4) การแก้ไขข้อมูล

กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่แก้ไขข้อมูลส่วนบุคคลให้ทันสมัยถูกต้องครบถ้วนตามที่เจ้าของข้อมูลร้องขอเป็นหนังสือ ในการแก้ไขเปลี่ยนแปลงนั้น ผู้ควบคุมข้อมูลส่วนบุคคลจะขอให้เจ้าของข้อมูลส่วนบุคคลจัดส่งเอกสาร หรือหลักฐานเพื่อใช้ในการเปลี่ยนแปลงก็ได้[14]

5) การโอนข้อมูลส่วนบุคคล

กำหนดห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลโอนข้อมูลส่วนบุคคลที่อยู่ในความดูแลไปให้บุคคลอื่น เว้นแต่จะได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูล อย่างไรก็ดีในกรณีมีความจำเป็นเร่งด่วน ซึ่งหากรอรับความยินยอมก่อนอาจเกิดความเสียหายแก่ส่วนรวม หรือชีวิตร่างกาย หรืออนามัยของบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลอาจส่งหรือโอนข้อมูลนั้นได้[15]

นอกจากนี้ตามร่างพระราชบัญญัติยังมีบทบัญญัติในการห้ามส่งหรือโอนข้อมูลส่วนบุคคลไปนอกราชอาณาจักร โดยเฉพาะในประเทศที่ยังไม่มีบทบัญญัติของกฎหมายในการคุ้มครองข้อมูลส่วนบุคคล หรือมีแต่บทบัญญัติของกฎหมายนั้นมีมาตรฐานต่ำกว่าบทบัญญัติตามร่างพระราชบัญญัตินี้ เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล[16]

โดยที่ร่างพระราชบัญญัตินี้มีวัตถุประสงค์ที่จะให้การคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลเป็นหลัก ดังนั้นจึงกำหนดให้เจ้าของข้อมูลส่วนบุคคล รวมถึงผู้ที่เกี่ยวข้องอื่น ๆ ไม่ว่าจะเป็น ผู้ปกครอง ผู้อนุบาล หรือผู้พิทักษ์ รวมตลอดถึงทายาท มีสิทธิในข้อมูลส่วนบุคคลดังนี้[17]

1) เข้าตรวจดู แก้ไข หรือขอสำเนารับรองถูกต้อง

2) ขอแก้ไขหรือเปลี่ยนแปลงข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตนให้ถูกต้องสมบูรณ์

3) ขอให้ระงับการใช้การเปิดเผยในกรณีที่ข้อมูลไม่ถูกต้องเป็นจริง

4) ขอให้ลบทำลายข้อมูลส่วนบุคคลที่พ้นกำหนดระยะเวลาการเก็บรวบรวมข้อมูลหรือไม่เกี่ยวข้อง หรือเกินความจำเป็นตามวัตถุประสงค์ของการเก็บรวบรวมข้อมูลนั้น

นอกจากนี้ร่างพระราชบัญญัติฉบับนี้ยังกำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิเรียกร้องให้ผู้ที่ได้รับข้อมูลเปิดเผยแหล่งที่มาของข้อมูลนั้นได้ หากผู้ได้รับข้อมูลมาโดยมิได้รับความ

---

[13] มาตรา 31 ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...

[14] มาตรา 33 ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...

[15] มาตรา 29 ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...

[16] มาตรา 30 ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...

[17] มาตรา 31-33 ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...

ยินยอมจากเจ้าของข้อมูลไม่ยอมเปิดเผย เจ้าของข้อมูลมีสิทธิเรียกร้องค่าสินไหมทดแทนได้ นอกจากนี้ยังให้สิทธิเจ้าของข้อมูลร้องเรียนต่อคณะกรรมการได้อีกทางหนึ่ง[18]

ทั้งนี้ร่างพระราชบัญญัติฉบับนี้กำหนดให้สิทธิเจ้าของข้อมูลส่วนบุคคลที่จะร้องเรียนต่อคณะกรรมการ ในกรณีที่เจ้าของข้อมูลส่วนบุคคลได้ร้องขอให้นายทะเบียนแก้ไขการดำเนินการให้เป็นไปตามพระราชบัญญัตินี้ แล้วนายทะเบียนมิได้แก้ไขให้ถูกต้องภายใน 30 วัน และเมื่อเจ้าของข้อมูลส่วนบุคคลได้ร้องเรียนต่อคณะกรรมการแล้ว คณะกรรมการมีหน้าที่จะต้องพิจารณาเรื่องดังกล่าวโดยเร็ว หากคณะกรรมการเห็นว่าการไม่ดำเนินการตามพระราชบัญญัตินี้ของผู้ประมวลข้อมูลส่วนบุคคล และก่อให้เกิดความเสียหายอย่างร้ายแรงต่อเจ้าของข้อมูลส่วนบุคคล คณะกรรมการอาจสั่งให้หยุดกิจการ หรือพักใช้ หรือเพิกถอนใบอนุญาตก็ได้ตามความร้ายแรงที่เกิดขึ้น[19]

เพื่อให้การบังคับใช้กฎหมายอย่างมีประสิทธิภาพ ร่างพระราชบัญญัติฉบับนี้ได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลแต่งตั้งผู้ควบคุมข้อมูลส่วนบุคคลเชิงธุรกิจหรือการพาณิชย์ขึ้นเพื่อรับผิดชอบในการดูแลข้อมูลส่วนบุคคลที่อยู่ในความครอบครอง รวมถึงการกำหนดให้รายงานการประมวลผลข้อมูลส่วนบุคคลต่อคณะกรรมการด้วย[20]

โดยที่การควบคุมข้อมูลส่วนบุคคลมีเป็นจำนวนมาก และการควบคุมสมควรที่จะได้มีการแบ่งแยกประเภทให้ชัดเจน เพื่อประโยชน์ในการติดตามการดำเนินการเพื่อให้เป็นไปตามร่างพระราชบัญญัตินี้ จึงกำหนดมาตรการส่งเสริมขึ้นเพื่อให้ผู้ประมวลข้อมูลส่วนบุคคลขอรับการสนับสนุนจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลในการขอคำปรึกษาในการดำเนินการประมวลผล การอบรมพัฒนา และกำหนดให้สำนักงานคณะกรรมคุ้มครองข้อมูลส่วนบุคคลนำเสนอต่อคณะกรรมการเพื่อพิจารณาในการออกใบรับรองมาตรฐานให้แก่ผู้ประมวลผลข้อมูลส่วนบุคคลด้วย ทั้งนี้เพื่อให้การควบคุมข้อมูลส่วนบุคคลเป็นไปอย่างมีประสิทธิภาพ

ร่างพระราชบัญญัติฉบับนี้มีข้อกำหนดที่ชัดเจนในความรับผิดทางแพ่ง บทกำหนดโทษ และบทเฉพาะกาล ให้ผู้ประมวลข้อมูลส่วนบุคคล ผู้ครอบครองดูแลข้อมูลส่วนบุคคลต้องรับผิดชดใช้ค่าสินไหมทดแทนให้แก่เจ้าของข้อมูลส่วนบุคคล ในกรณีที่บุคคลดังกล่าวกระทำการใด ๆ ที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคล หรือบุคคลที่เกี่ยวข้องด้วย[21]

เนื่องจากข้อมูลส่วนบุคคลถือเป็นสิทธิของเจ้าของข้อมูล ดังนั้นการละเมิดสิทธิในข้อมูลส่วนบุคคลจึงเป็นเรื่องต้องห้าม ผู้ใดละเมิดสิทธิของเจ้าของข้อมูลผู้นั้นสมควรได้รับโทษทาง

---

[18] มาตรา 41 ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...

[19] มาตรา 41-44 ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...

[20] มาตรา 34-40 ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...

[21] มาตรา 53-55 ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...

อาญา ดังนั้นจึงมีการกำหนดให้ผู้ใดก็ตามและนายทะเบียนที่กระทำโดยการเผยแพร่ข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย ผู้นั้นต้องได้รับโทษทางอาญา[22]

ทั้งนี้เพื่อให้การดำเนินการคุ้มครองข้อมูลส่วนบุคคลเกิดขึ้นโดยเร็ว จึงมีการกำหนดให้มีการแต่งตั้งคณะกรรมการขึ้นเพื่อปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ภายใน 90 วัน นับแต่วันที่พระราชบัญญัตินี้มีผลบังคับใช้ นอกจากนี้โดยที่ร่างพระราชบัญญัติฉบับนี้กำหนดให้มีสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลขึ้นในสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ ประกอบกับขณะนี้พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 อยู่ระหว่างการพิจารณาแก้ไขยกสถานะของสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ ซึ่งมีสถานะเป็นกองในสำนักงานปลัดสำนักนายกรัฐมนตรี ให้มีสถานะเป็นกรมในสังกัดสำนักนายกรัฐมนตรี ดังนั้นจึงจำเป็นต้องกำหนดบทเฉพาะกาลให้ผู้อำนวยการสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการปฏิบัติหน้าที่เลขาธิการสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการและตามพระราชบัญญัตินี้ด้วย[23]

เมื่อพิจารณาถึงบทบัญญัติตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... นี้ นับว่าเป็นร่างกฎหมายที่สำคัญที่จะส่งผลต่อการพัฒนาการคุ้มครองข้อมูลข่าวสารส่วนบุคคลในภาคเอกชนของประเทศไทยในอนาคตเป็นอย่างมาก เพราะเป็นการแก้ไขข้อจำกัดที่มีอยู่ในการคุ้มครองตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ที่ใช้บังคับเฉพาะข้อมูลส่วนบุคคลในภาครัฐเท่านั้น ให้ครอบคลุมถึงข้อมูลที่จัดเก็บโดยเอกชน รวมทั้งสามารถนำไปประยุกต์ใช้กับกรณี Big Data ได้ด้วย ทั้งนี้พระราชบัญญัติฉบับนี้จะช่วยสร้างมาตรฐานกลางในการคุ้มครองข้อมูลส่วนบุคคลในภาคเอกชนให้เกิดขึ้นในฐานเป็นกฎหมายทั่วไป แตกต่างจากกฎหมายฉบับอื่นที่เป็นการคุ้มครองข้อมูลในลักษณะเฉพาะเรื่องตามแต่ละประเภทข้อมูล

คณะรัฐมนตรีในการประชุม เมื่อวันที่ 1 สิงหาคม พ.ศ. 2549 ได้อนุมัติหลักการร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... และให้ส่งสำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณา ซึ่งหลังจากสำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้ว รัฐบาลโดยนายอภิสิทธิ์ เวชชาชีวะ ได้ส่งร่างกฎหมายดังกล่าวไปยังรัฐสภาเมื่อเดือนตุลาคม พ.ศ. 2552 แต่ยังไม่ได้รับการบรรจุเป็นวาระเพื่อพิจารณาของรัฐสภา

รัฐบาลในสมัยนางสาวยิ่งลักษณ์ ชินวัตร ได้เสนอร่างดังกล่าวไปยังรัฐสภาอีกครั้งเมื่อเดือนกุมภาพันธ์ พ.ศ. 2556 แต่เกิดการรัฐประหารเมื่อวันที่ 22 พฤษภาคม พ.ศ. 2557 เสียก่อน และล่าสุด เมื่อวันที่ 22 กรกฎาคม พ.ศ. 2557 ในการประชุมคณะรักษาความสงบแห่งชาติ (คสช.)

---

[22] มาตรา 56-59 ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...

[23] มาตรา 60-61 ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...

ครั้งที่ 7/ 2557 คณะรักษาความสงบแห่งชาติได้ให้ความเห็นชอบให้นำร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... เสนอต่อสภานิติบัญญัติแห่งชาติตามที่ฝ่ายกฎหมายและกระบวนการยุติธรรม (ฝกย.) เสนอว่าร่างพระราชบัญญัติดังกล่าวเป็นกฎหมายที่ควรเร่งรัดให้มีผลบังคับใช้[24]

3.1.1.3 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มีวัตถุประสงค์เพื่อรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ให้เสมอกับหนังสือ หรือหลักฐานเป็นหนังสือ รับรองวิธีการส่งและรับข้อมูลอิเล็กทรอนิกส์ รวมทั้งการรับฟังพยานหลักฐาน และการชั่งน้ำหนักพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ดังนั้น เพื่อส่งเสริมการติดต่อสื่อสารโดยวิธีการทางอิเล็กทรอนิกส์ให้มีความน่าเชื่อถือ และก่อให้เกิดความเชื่อมั่น ซึ่งเอื้อต่อการทำธุรกรรมทางอิเล็กทรอนิกส์ อีกทั้ง ได้มีการตั้งคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งมีอำนาจในการเสนอแนะต่อคณะรัฐมนตรีเพื่อวางนโยบายการส่งเสริมและพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ตลอดจนแก้ไขปัญหาปละอุปสรรคที่เกี่ยวข้อง ติดตามดูแลการประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ เสนอแนะให้คำปรึกษาต่อคณะรัฐมนตรีเพื่อการตราพระราชกฤษฎีกาตามกฎหมายนี้ และออกระเบียบหรือประกาศเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์เพื่อให้เป็นไปตามกฎหมายนี้ หรือตามพระราชกฤษฎีกาที่ออกตามกฎหมายนี้

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553 เพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานของรัฐมีความมั่นคงปลอดภัย ความน่าเชื่อถือ และมีการคุ้มครองข้อมูลส่วนบุคคลที่เป็นไปตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เห็นสมควรกำหนดแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐให้มีมาตรฐานเดียวกัน อาศัยอำนาจตามความในมาตรา 6 แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 บัญญัติว่า “ในกรณีที่หน่วยงานของรัฐมีการรวบรวม จัดเก็บ ใช้ หรือเผยแพร่ข้อมูล หรือ ข้อเท็จจริงที่ทำให้สามารถระบุตัวบุคคล ไม่ว่าโดยตรงหรือโดยอ้อม ให้หน่วยงานของรัฐจัดทำแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล” ดังนั้น คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงออก “ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553” เพื่อให้หน่วยงานของรัฐให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคล ด้วยการจัดทำแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

---

[24] **ข้อเสนอแนะนำร่างนโยบายด้านข้อมูลส่วนบุคคล** [Online], กรกฎาคม 2557. แหล่งที่มา http://www.siamintelligence.com/data-privacy-guideline/.

ของหน่วยงานของรัฐ สำหรับการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐด้วย โดยในประกาศฯ ต้องมีสาระสำคัญอย่างน้อย ประกอบด้วย 2 ส่วน ได้แก่

ส่วนที่ 1: นโยบายการคุ้มครองข้อมูลส่วนบุคคล

การจัดทำนโยบายในการคุ้มครองข้อมูลส่วนบุคคล มีวัตถุประสงค์เพื่อเป็นการแจ้งให้กับผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐกับหน่วยงานได้ทราบว่า หน่วยงานมีแนวทางในการบริหารจัดการข้อมูลส่วนบุคคลของผู้ใช้บริการซึ่งเป็นเจ้าของข้อมูลอย่างไร เพื่อให้ผู้ใช้บริการทราบและสามารถตัดสินใจได้ว่าสมควรให้ข้อมูลส่วนบุคคลของตนหรือไม่ เพื่อให้สอดคล้องเป็นไปตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553 ในส่วนของนโยบายการคุ้มครองข้อมูลส่วนบุคคลจะต้องมีหัวข้อหลักที่เป็นสาระสำคัญอย่างน้อย 8 ข้อ ดังนี้

1) การเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด กล่าวคือ ในการเก็บรวบรวมข้อมูลนั้นต้องชอบด้วยกฎหมาย และต้องใช้วิธีการที่เป็นธรรมและเหมาะสมโดยในการเก็บรวบรวมข้อมูลนั้นต้องให้เจ้าของข้อมูลรู้เห็น รับรู้ หรือได้รับความยินยอมจากเจ้าของข้อมูล

2) คุณภาพของข้อมูลส่วนบุคคล ข้อมูลดังกล่าวจะต้องถูกต้อง สมบูรณ์ หรือทำให้เป็นปัจจุบันหรือทันสมัยอยู่เสมอ และต้องเกี่ยวข้องกับวัตถุประสงค์ที่กำหนดไว้ด้วย

3) การระบุวัตถุประสงค์ในการเก็บรวบรวมว่าเก็บรวบรวมข้อมูลไปเพื่ออะไร พร้อมทั้งกำหนดระยะเวลาที่เก็บรวบรวมหรือรักษาข้อมูลนั้น ตลอดจนกรณีที่จำเป็นต้องมีการเปลี่ยนแปลงวัตถุประสงค์ในการเก็บรวบรวมข้อมูลเช่นว่านั้นไว้ให้ชัดเจน

4) ข้อจำกัดในการนำข้อมูลส่วนบุคคลไปใช้ จะต้องไม่มีการเปิดเผย หรือปรากฏในลักษณะอื่นที่ไม่ได้แจ้งไว้ในวัตถุประสงค์

5) การรักษาความมั่นคงปลอดภัยของข้อมูล จะต้องมีการกำหนดมาตรการที่เหมาะสม เพื่อป้องกันข้อมูลนั้นสูญหาย เข้าถึง ทำลาย ใช้ ดัดแปลงแก้ไข หรือเปิดเผยโดยมิชอบ

6) การเปิดเผยเกี่ยวกับการดำเนินการแนวปฏิบัติ ควรมีการประกาศนโยบายที่เกี่ยวกับข้อมูลส่วนบุคคลให้ทราบถึงโดยทั่วกันหากมีการปรับปรุงแก้ไข หรือพัฒนาแนวนโยบายหรือแนวปฏิบัติที่เกี่ยวกับข้อมูลส่วนบุคคล ก็ควรเปิดเผยหรือประกาศไว้ให้ชัดเจน

7) การมีส่วนร่วมของเจ้าของข้อมูลให้บุคคลซึ่งเป็นเจ้าของข้อมูลได้รับแจ้งหรือยืนยันจากหน่วยงานของรัฐที่เก็บรวบรวมหรือจัดเก็บข้อมูลภายในระยะเวลาที่เหมาะสม

8) ความรับผิดชอบของบุคคลซึ่งทำหน้าที่ควบคุมข้อมูล ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

ส่วนที่ 2: แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

การจัดทำแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล มีวัตถุประสงค์เพื่อเป็นการประกาศให้กับบุคลากรในหน่วยงานปฏิบัติตามนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการทั้งนี้ แนวปฏิบัติต้องแสดงถึงขั้นตอนและวิธีการดำเนินการเพื่อให้บุคลากรซึ่งเป็นผู้ปฏิบัติสามารถปฏิบัติได้อย่างถูกต้อง เพื่อให้สอดคล้องเป็นไปตามประกาศคณะกรรมการฯ จะต้องมีหัวข้อหลักที่เป็นสาระสำคัญในแนวปฏิบัติ อย่างน้อย 9 ข้อ ดังนี้

1) ข้อมูลเบื้องต้น
2) การเก็บรวบรวม จัดประเภท และการใช้ข้อมูลส่วนบุคคล
3) การแสดงระบุความเชื่อมโยงให้ข้อมูลส่วนบุคคลกับหน่วยงานหรือองค์กรอื่น
4) การรวมข้อมูลจากที่มาหลาย ๆ แห่ง
5) การให้บุคคลอื่นใช้หรือการเปิดเผยข้อมูลส่วนบุคคล
6) การรวบรวม จัดเก็บ ใช้ และการเปิดเผยข้อมูลเกี่ยวกับผู้ใช้บริการ
7) การเข้าถึง การแก้ไขให้ถูกต้อง และการปรับปรุงให้เป็นปัจจุบัน
8) การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล
9) การติดต่อกับเว็บไซต์

3.1.1.4 พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีวัตถุประสงค์เพื่อป้องกันและปราบปรามการกระทำความผิดกับบุคคลที่ใช้คอมพิวเตอร์กระทำความผิด ไม่ว่าจะเป็นการทำให้ระบบคอมพิวเตอร์ไม่ทำงานตามคำสั่งที่กำหนดไว้ หรือระบบได้ทำตามคำสั่งผิดพลาดไป อีกทั้งการใช้วิธีการอันใด ๆ ที่เป็นการเข้าระบบคอมพิวเตอร์ แก้ไข หรือทำลายข้อมูลในระบบคอมพิวเตอร์ของบุคคลอื่น รวมถึงเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือเป็นข้อมูลที่มีลักษณะลามกอนาจาร อันส่งผลให้เกิดความเสียหายต่อสังคม เศรษฐกิจ ความมั่นคงของรัฐและความสงบสุขหรือศีลธรรมอันดีของประชาชน ทั้งนี้ไม่ว่าตัวผู้กระทำความผิดจะอยู่นอกราชอาณาจักร ไม่ว่าจะเป็นคนไทยหรือเป็นคนต่างชาติ ถ้าผู้เสียหายมีการร้องขอให้ลงโทษ ผู้กระทำความผิดต้องรับโทษภายในราชอาณาจักรไทยตามพระราชบัญญัตินี้

ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ซึ่งในทางวิทยาศาสตร์ ได้แก่ ฮาร์ดแวร์และซอฟต์แวร์ที่พัฒนาขึ้นเพื่อประมวลผลข้อมูล Digital อันประกอบด้วยเครื่องคอมพิวเตอร์ และอุปกรณ์รอบข้าง (Peripheral) ต่าง ๆ ในการรับเข้าหรือป้อนข้อมูล (Input) นำเข้าหรือแสดงผลข้อมูล (Output) และบันทึกหรือเก็บข้อมูล (Store and Record) ระบบคอมพิวเตอร์จึงอาจเป็นอุปกรณ์เพียงเครื่องเดียว หรือหลายเครื่องอันมีลักษณะเป็นชุดเชื่อมต่อกัน โดยอาจเชื่อมต่อ

ผ่านระบบเครือข่ายก็ได้ และมีลักษณะการทำงานโดยอัตโนมัติตามโปรแกรมหรือซอฟต์แวร์ที่กำหนดไว้

ความหมายในภาษาทั่วไป หมายถึง อุปกรณ์ที่ได้มีการพัฒนาให้มีการทำงานประมวลผลข้อมูลโดยอัตโนมัติแล้ว ดังนั้นเครื่องคอมพิวเตอร์ เช่น Laptop/ Notebook ยังไม่ถือว่าเป็น “ระบบคอมพิวเตอร์” จนกว่าจะได้มีการทำงานผ่านระบบเครือข่ายหรือโดยซอฟต์แวร์

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

ความหมาย “ข้อมูลคอมพิวเตอร์” หมายถึงข้อมูลทุกอย่างที่อยู่ในระบบคอมพิวเตอร์ รวมทั้งชุดคำสั่งด้วยหากอยู่ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ นอกจากนั้นยังให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

ความจริงแล้ว “ข้อมูลอิเล็กทรอนิกส์” ย่อมอยู่ในความหมายของข้อมูลคอมพิวเตอร์อยู่แล้ว แต่เพื่อให้ครอบคลุมถึงข้อมูลประเภทอื่น ๆ ที่อาจสร้างด้วยวิธีการทางอิเล็กทรอนิกส์อื่น ๆ ในอนาคตที่ไม่ใช่เทคโนโลยีคอมพิวเตอร์ก็ได้ อย่างไรก็ตาม “ข้อมูลอิเล็กทรอนิกส์” ตามที่บัญญัติไว้ในพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ได้ให้ความหมายคำว่า “ข้อมูลอิเล็กทรอนิกส์” ไว้ว่า “ข้อความที่ได้สร้าง ส่ง เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือ โทรสาร” ดังนั้น ความหมายจึงกว้างรวมออกไปถึงโทรเลข โทรพิมพ์ โทรสาร อย่างไรก็ตามองค์ประกอบความผิดตามพระราชบัญญัตินี้ส่วนใหญ่จะเชื่อมโยงองค์ประกอบความผิด “ข้อมูลคอมพิวเตอร์” กับ “ระบบคอมพิวเตอร์” เข้าด้วยกัน ดังนั้น กรณีของโทรเลข โทรพิมพ์ หรือโทรสารหากเป็นความผิดที่ต้องเชื่อมโยงกับระบบคอมพิวเตอร์ เช่น การดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์โดยมิชอบนั้น[25] จะต้องเป็นกรณีที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ เป็นต้น ดังนั้นการดักรับโทรเลข โทรพิมพ์ หรือโทรสารที่ไม่ได้ส่งในระบบคอมพิวเตอร์ย่อมไม่เป็นความผิดตามมาตราดังกล่าว เป็นต้น

“ข้อมูลจราจรทางคอมพิวเตอร์” หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

[25] มาตรา 8 พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550.

“ข้อมูลจราจรทางคอมพิวเตอร์” หมายถึงข้อมูลที่แสดงรายการให้เห็นถึงการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์ซึ่งจะแสดงถึงแหล่งกำเนิด เช่น IP address ของเครื่อง ชื่อที่อยู่ของผู้ใช้ บริการที่มีการลงทะเบียน ข้อมูลของผู้ให้บริการ (Service Provider) ลักษณะของการให้บริการว่าผ่านระบบใดหรือเครือข่ายใด วันเวลาของการส่งข้อมูล และข้อมูลทุกประเภทที่เกิดจากการสื่อสาร (Communication) ผ่าน “ระบบคอมพิวเตอร์”

การสื่อสารผ่านระบบคอมพิวเตอร์นั้นจะต้องมีระบบเครือข่ายคอมพิวเตอร์และมีผู้ให้บริการซึ่งผู้ให้บริการจะมีข้อมูลจราจรทางคอมพิวเตอร์อยู่ในระบบคอมพิวเตอร์ของตน และตามพระราชบัญญัตินี้กำหนดว่า ผู้ให้บริการมีหน้าที่เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ที่ผู้ใช้บริการได้ใช้บริการในระบบคอมพิวเตอร์ของตนดังกล่าว[26]

3.1.1.5 พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545

พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 มีวัตถุประสงค์ในการกำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขในการทำธุรกรรมข้อมูลเครดิต เพื่อตอบสนองความจำเป็นในด้านข้อมูลทางการเงิน และประวัติการชำระหนี้ของลูกหนี้ในการพิจารณาสินเชื่อของสถาบันการเงินต่าง ๆ เพื่อลดความเสี่ยง และความเสียหายที่อาจจะเกิดขึ้น รวมทั้งช่วยป้องกันไม่ให้เกิดหนี้ที่ไม่ก่อให้เกิดรายได้ของสถาบันการเงิน ซึ่งจะส่งผลถึงความมั่นคงของระบบสถาบันการเงินโดนรวม บริษัทข้อมูลเครดิตจะจัดเก็บข้อมูลได้เฉพาะข้อมูลเครดิตเท่านั้น ซึ่ง มาตรา 3 ได้ให้คำนิยามไว้ ดังนี้

“ข้อมูลเครดิต” หมายความว่า ข้อเท็จจริงเกี่ยวกับลูกค้าที่ขอสินเชื่อ ดังต่อไปนี้

1) ข้อเท็จจริงที่บ่งชี้ถึงตัวลูกค้า และคุณสมบัติของลูกค้าที่ขอสินเชื่อ

(ก) กรณีบุคคลธรรมดา หมายถึง ชื่อ ที่อยู่ วันเดือนปีเกิด สถานภาพ การสมรส อาชีพ เลขที่บัตรประจำตัวประชาชน หรือบัตรประจำตัวเจ้าหน้าที่ของรัฐ หรือหนังสือเดินทาง และเลขประจำตัวผู้เสียภาษีอากร (ถ้ามี)

(ข) กรณีนิติบุคคล หมายถึง ชื่อ สถานที่ตั้ง เลขที่ทะเบียนการจัดตั้งนิติบุคคล หรือเลขประจำตัวผู้เสียภาษีอากร

2) ประวัติการขอและการได้รับอนุมัติสินเชื่อ และการชำระสินเชื่อของลูกค้าที่ขอสินเชื่อรวมทั้งประวัติการชำระราคาสินค้าหรือบริการโดยบัตรเครดิต

จะเห็นได้ว่า ข้อมูลเครดิตจำกัดเฉพาะข้อมูลทางสินเชื่อ และการชำระสินเชื่อของลูกค้าของสถาบันการเงิน ซึ่งหากพิจารณานิยามของคำว่า สินเชื่อ กล่าวคือ

---

[26] มาตรา 25 พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550.

“สินเชื่อ” หมายความว่า การให้กู้ยืมเงินหรือวงเงินในการให้กู้ยืม หรือให้ยืมหลักทรัพย์ ให้เช่าซื้อ ให้เช่าซื้อแบบลิสซิ่ง ค้ำประกัน รับอาวัล รับรองตั๋วเงิน ซื้อ ซื้อลดหรือรับช่วงซื้อลดตั๋วเงิน เป็นเจ้าหนี้เนื่องจากได้จ่ายหรือสั่งให้จ่ายเงินเพื่อประโยชน์ของผู้เคยค้า หรือเป็นเจ้าหนี้เนื่องจากได้จ่ายเงินตามภาระผูกพันตาม Letter of Credit หรือภาระผูกพันอื่น รวมทั้งการรับประกันภัย การรับประกันชีวิต การรับเป็นลูกค้าเพื่อซื้อขายหลักทรัพย์ และธุรกรรมอื่นใดตามที่คณะกรรมการประกาศกำหนด

จะเห็นได้ว่านิยามของคำว่าสินเชื่อตามพระราชบัญญัตินี้มิได้จำกัดเฉพาะการกู้ยืมเงินเท่านั้น แต่ยังรวมถึงธุรกรรมอื่น ๆ ด้วย ดังนั้น ข้อมูลใด ๆ ที่เกี่ยวกับประวัติการใช้สินเชื่อ หรือการชำระสินเชื่อของธุรกรรมต่าง ๆ เหล่านี้ จึงจัดอยู่ในความหมายของข้อมูลเครดิตด้วย พระราชบัญญัติฉบับนี้มุ่งที่จะจำกัดของเขตการประกอบธุรกิจข้อมูลเครดิตให้จำกัดอยู่เฉพาะการจัดเก็บรวบรวมข้อมูลเครดิตที่เกี่ยวกับบุคคลที่เป็นลูกค้าผู้ขอสินเชื่อเท่านั้น ซึ่งบุคคลตามกฎหมายนี้รวมไปถึงบุคคลธรรมดาและนิติบุคคลด้วย และจะต้องเป็นประวัติการของและการได้รับอนุมัติสินเชื่อและการชำระสินเชื่อด้วย

ข้อมูลเครดิตจึงมีขอบเขตเนื้อหาประกอบไปด้วย 2 ส่วน คือ [27]

ก) ส่วนที่เป็นข้อเท็จจริงเกี่ยวกับลูกค้า และ

ข) ส่วนที่เป็นประวัติเกี่ยวกับการชำระหนี้ โดยในส่วนนี้ยังสามารถแบ่งเป็น

ส่วนที่หนึ่ง คือ ประวัติเกี่ยวกับการชำระหนี้ หรือชำระสินเชื่อของลูกค้าที่ขอสินเชื่อว่ามีประวัติการชำระหนี้อย่างไร และ

ส่วนที่สอง คือ ประวัติการชำระโดยบัตรเครดิต ซึ่งเป็นการชำระตามใบเรียกเก็บในแต่ละเดือนแต่ละค่างวดว่ามีการชำระอย่างไร โดยไม่ได้ไปถึงรายละเอียดของสินค้าว่าซื้อสินค้าอะไร ดังนั้น ในส่วนของบัตรเครดิตจึงหมายถึงการชำระสินเชื่อบัตรเครดิต ไม่ใช่การใช้บัตรเครดิต

ส่วนข้อมูลบุคคลอื่น ๆ นอกเหนือจากนี้ ไม่ถือเป็นข้อมูลเครดิต บริษัทข้อมูลเครดิตจึงไม่สามารถจัดเก็บได้ ดังนั้น ข้อมูลส่วนบุคคลที่จะได้รับความคุ้มครองตามกฎหมายฉบับนี้ต้องเป็นข้อมูลส่วนบุคคลที่เกี่ยวกับลูกค้าที่ขอสินเชื่อเท่านั้น หากเป็นข้อมูลส่วนบุคคลประเภทอื่น ๆ ย่อมไม่ได้รับความคุ้มครองตามกฎหมายฉบับนี้

พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 มีหลักการคุ้มครองข้อมูลเครดิต ดังนี้

---

[27] ชาลวรี ชูทรัพย์, **ปัญหาการปรับใช้พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545: กรณีศึกษาเรื่องการให้ความยินยอมของเจ้าของข้อมูล**, (วิทยานิพนธ์มหาบัณฑิต นิติศาสตรมหาบัณฑิต บัณฑิตวิทยาลัย มหาวิทยาลัยธรรมศาสตร์, 2552), 25.

1) หลักข้อจำกัดในการเก็บรวบรวมข้อมูล[28] ห้ามบริษัทข้อมูลเครดิตจัดเก็บข้อมูลที่ไม่เกี่ยวข้องกับการรับบริการ หรือการขอสินเชื่อ หรือที่มีผลกระทบต่อความรู้สึกหรืออาจก่อให้เกิดความเสียหายหรือมีผลกระทบต่อสิทธิเสรีภาพของผู้เป็นเจ้าของข้อมูลอย่างชัดเจน เช่น ลักษณะพิการทางร่างกาย ลักษณะทางพันธุกรรม ข้อมูลของบุคคลที่อยู่ในกระบวนการสอบสวนหรือพิจารณาคดีอาญา เป็นต้น

2) หลักคุณภาพของข้อมูล[29] บริษัทข้อมูลเครดิตต้องทำการประมวลผลข้อมูลจากสมาชิกหรือจากแหล่งข้อมูลที่เชื่อถือได้ และในการประมวลผลข้อมูล บริษัทข้อมูลเครดิตต้องจัดให้มีระบบและข้อกำหนดที่กฎหมายกำหนด เช่น ต้องจัดให้มีระบบการจำแนกข้อมูล ระบบการแก้ไขข้อมูล ระบบการตรวจสอบและแก้ไขข้อมูลของเจ้าของข้อมูล เป็นต้น นอกจากนี้ ในกรณีที่บริษัทข้อมูลเครดิตหรือสมาชิกเห็นว่าข้อมูลไม่ถูกต้องไม่ว่าด้วยเหตุใด ให้บริษัทข้อมูลเครดิตหรือสมาชิกนั้นแก้ไขข้อมูลให้ถูกต้องโดยเร็ว รวมทั้งต้องแจ้งข้อมูลที่แก้ไขให้แก่แหล่งข้อมูลสมาชิกหรือผู้ใช้บริการที่เกี่ยวข้องเพื่อนำไปแก้ไขข้อมูลให้ถูกต้องต่อไปด้วย[30]

3) หลักการรักษาความมั่นคงปลอดภัย[31] บริษัทข้อมูลเครดิตต้องจัดให้มีระบบการรักษาความลับ และความมั่นคงปลอดภัยของข้อมูลเพื่อป้องกันมิให้มีการนำข้อมูลไปใช้ผิดวัตถุประสงค์ และมิให้ผู้ไม่มีสิทธิได้รับรู้ข้อมูล รวมทั้งระบบป้องกันมิให้ข้อมูลถูกแก้ไข ทำให้เสียหายหรือถูกทำลายโดยไม่ชอบหรือโดยไม่ได้รับอนุญาต

4) หลักความยินยอม[32] บริษัทข้อมูลเครดิตเปิดเผยหรือให้ข้อมูลแก่สมาชิกหรือผู้ใช้บริการที่ประสงค์จะใช้ข้อมูลเพื่อประโยชน์ในการวิเคราะห์การให้สินเชื่อ และการออกบัตรโดยการเปิดเผยหรือให้ข้อมูลดังกล่าว จะต้องได้รับคำยินยอมเป็นหนังสือจากเจ้าของข้อมูลก่อน เว้นแต่จะเข้าข้อยกเว้นตามที่กฎหมายกำหนด เช่น เมื่อมีคำสั่งศาลหรือตามหมายศาลหรือเป็นข้อมูลเกี่ยวกับการฟ้องร้องคดีต่าง ๆ ที่เปิดเผยต่อสาธารณะ หรือเมื่อมีหนังสือจากพนักงานสอบสวนเพื่อประโยชน์ในการสอบสวนความผิดอาญาเกี่ยวกับธุรกิจการเงินซึ่งตนเป็นผู้รับผิดชอบการสอบสวนคดีดังกล่าว เป็นต้น กรณีที่ได้มีการเปิดเผยหรือให้ข้อมูลตามข้อยกเว้นแล้ว ให้บริษัทข้อมูลเครดิตแจ้งเป็นหนังสือแก่เจ้าของข้อมูลทราบภายในสามสิบวันนับแต่วันเปิดเผยหรือให้ข้อมูล

---

[28] มาตรา 10 พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545.

[29] มาตรา 16 พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545.

[30] มาตรา 26 วรรคสอง พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545.

[31] มาตรา 16 (3) พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545.

[32] มาตรา 20 พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545.

5) หลักข้อจำกัดในการนำไปใช้ ห้ามมิให้บริษัทข้อมูลเครดิตดำเนินการประมวลผลข้อมูลที่มีอายุของข้อมูลเกินกว่าที่คณะกรรมการประกาศกำหนด[33] และต้องจัดให้มีระบบการทำลายข้อมูลที่มีอายุเกินกว่าที่คณะกรรมการกำหนด[34] สำหรับผู้ใช้ข้อมูลนั้นอาจใช้ข้อมูลที่บริษัทข้อมูลเครดิตเปิดเผยได้เฉพาะเพื่อการวิเคราะห์เครดิตเท่านั้น[35]

6) หลักการมีสิทธิเข้าถึงข้อมูลของตน [36] เพื่อประโยชน์ในการคุ้มครองให้ความเป็นธรรมแก่เจ้าของข้อมูลให้เจ้าของข้อมูลมีสิทธิตามที่กฎหมายกำหนด เช่น เจ้าของข้อมูลมีสิทธิที่จะรับรู้ว่าบริษัทข้อมูลเครดิตเก็บรักษาข้อมูลใดของตน มีสิทธิที่จะตรวจสอบข้อมูลของตน มีสิทธิที่จะขอแก้ไขข้อมูลที่ไม่ถูกต้อง เป็นต้น

7) หลักการบังคับการตามกฎหมาย[37] หากบริษัทข้อมูลเครดิตหรือผู้ใช้ข้อมูลละเมิดหลักการคุ้มครองเครดิตข้างต้น ผู้นั้นจะต้องชดใช้ค่าเสียหายให้แก่เจ้าของข้อมูล และต้องรับโทษทางอาญาด้วย

3.2 กฎหมายต่างประเทศที่เกี่ยวข้องกับ Big Data

การคุ้มครองข้อมูลใน Big Data ตามกฎหมายคุ้มครองข้อมูลในต่างประเทศส่วนใหญ่ จะครอบคลุมประเด็นเกี่ยวกับอำนาจควบคุมเหนือข้อมูลในการรวบรวม และการนำข้อมูลไปใช้ประโยชน์มากกว่าที่จะมองว่าข้อมูลอยู่ที่ใด หรืออยู่ในการครอบครองของใคร เพราะโดยลักษณะและความสามารถอันแทบไร้ข้อจำกัดของระบบคอมพิวเตอร์ ที่สามารถครอบครองและควบคุมการเคลื่อนไหวของข้อมูลจากที่หนึ่งไปยังอีกที่หนึ่งได้อย่างง่ายดายและรวดเร็ว ซึ่งในกฎหมายการคุ้มครองของนานาประเทศอาจมีมาตรฐานการคุ้มครองข้อมูลที่ไม่เท่าเทียมกัน แต่ถึงแม้ว่าจะไม่สามารถกำหนดรูปแบบของขอบเขตการคุ้มครองให้ได้มาตรฐานเดียวกันในทุกประเทศ ในภาพรวมของบทบัญญัติกฎหมายทั้งหลายนี้ตั้งอยู่บนพื้นฐานเดียวกัน ซึ่งหลักการคุ้มครองข้อมูลที่สามารถนำไปประยุกต์กับข้อมูลใน Big Data มีดังนี้

1) ในการจัดเก็บข้อมูล ต้องมีการบอกกล่าว หรือการแจ้ง ซึ่งในบางครั้งอาจหมายถึง การจดทะเบียน หรือการทำเป็นเอกสาร หรือ การได้ใบอนุญาต ซึ่งหมายถึงการได้รับอำนาจในการดำเนินการจัดเก็บข้อมูล ซึ่งผู้ดำเนินการ (Data Controller) ต้องยื่นเอกสารต่อเจ้าพนักงานเกี่ยวกับ

---

[33] มาตรา 13 พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545.

[34] มาตรา 16 (7) พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545.

[35] มาตรา 22 พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545.

[36] มาตรา 25 พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545.

[37] มาตรา 41 และหมวด 8 พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545.

การดำเนินการเกี่ยวกับข้อมูลที่ถูกต้อง ซึ่งหมายถึงการกำหนดขอบเขตและวัตถุประสงค์และการประมวลผลที่แน่นอนชัดเจน

2) การคุ้มครองข้อมูลที่เป็นข้อมูลส่วนตัวโดยเฉพาะ (Sensitive Data) เป็นประเด็นที่แต่ละประเทศต้องให้ความคุ้มครองอย่างเคร่งครัด แม้ว่าในคำจำกัดความของข้อมูลส่วนตัวโดยเฉพาะจะไม่สามารถกำหนดได้อย่างชัดเจนก็ตาม เช่นในเรื่องเกี่ยวกับการเมือง ลัทธิทางศาสนา แนวทางในการดำเนินชีวิต การเป็นสมาชิกสหพันธ์ ข้อมูลเกี่ยวกับสุขภาพ พฤติกรรม ทางเพศ และประวัติอาชญากรรม เป็นต้น ซึ่งการเก็บหรือการประมวลผลอาจมีได้โดยการให้ความยินยอมของเจ้าของข้อมูลอย่างชัดเจน หรืออาจกำหนดว่าไม่สามารถที่จะส่งข้อมูลเหล่านี้ออกนอกประเทศได้ หรืออาจให้ความคุ้มครองที่มากกว่านี้ คือ ห้ามมิให้มีการดำเนินการใด ๆ เกี่ยวกับข้อมูลเหล่านี้เลย เว้นแต่กฎหมายให้อำนาจ ซึ่งข้อมูลเหล่านี้อาจไม่ได้อยู่ในความคุ้มครองของ Data Controller แต่อาจอยู่ในความครอบครองของนายจ้าง ซึ่งได้เก็บข้อมูลข่าวสารของลูกจ้างไว้เช่น ประวัติการรักษาสุขภาพ หรือข้อมูลเกี่ยวกับความสัมพันธ์ในการทำสัญญา

3) การส่งข้อมูลระหว่างประเทศ (International Data Transfers or Transborderdata Flows) เป็นเรื่องที่นานาประเทศให้ความสำคัญ โดยส่วนมากจะไม่ยินยอมให้มีการเข้าถึงข้อมูลหรือส่งข้อมูลออกไปยังประเทศที่ไม่มีการคุ้มครองข้อมูลในระดับมาตรฐานที่น่าพอใจ เช่น ในกรณีการอนุญาตให้มีเสรีในการส่งข้อมูลภายในประเทศสมาชิกของสหภาพยุโรป และในขณะเดียวกันได้มีการห้ามการส่งข้อมูลของประเทศสมาชิกสหภาพยุโรป ไปยังประเทศที่ไม่ได้เป็นสมาชิก และประเทศซึ่งไม่มีมาตรการที่เพียงพอในการคุ้มครองข้อมูล

4) ส่วนมากของบทบัญญัติคุ้มครองข้อมูลจะเริ่มต้นด้วยขอบเขตในการคุ้มครอง เช่น การเก็บข้อมูล ขอบเขตการประมวลผลข้อมูล ที่อาจมีได้ในระยะเวลาที่กำหนด ความชอบธรรม ซึ่งอยู่บนพื้นฐานของการให้ความยินยอม ในการเก็บ ประมวลผล และเปิดเผยข้อมูลของเจ้าของข้อมูล (Data Subject) ภาระหน้าที่ในการให้การรับรองว่าข้อมูลดังกล่าว จะได้รับการแก้ไขปรับปรุงให้ทันสมัยอยู่เสมอ ซึ่งต้องทำให้เพียงพอแก่การยอมรับโดยการกำหนดเป็นนโยบาย และกระบวนการ รวมทั้งการมีมาตรการรักษาความมั่นคงปลอดภัยอย่างเพียงพอ ที่จะป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตโดยเฉพาะอย่างยิ่งข้อมูลที่มีการส่งด้วยวิธีการทางอิเล็กทรอนิกส์

5) สิทธิของเจ้าของข้อมูล ซึ่งได้แก่ สิทธิในการอนุญาตให้ใช้ข้อมูล สิทธิในการเข้าถึงข้อมูลของตนเอง สิทธิในการได้รับการแจ้งการใช้ข้อมูล สิทธิในการแก้ไขข้อมูลเมื่อพบว่าข้อมูลของตนมีความผิดพลาด และสิทธิในการได้รับการเยียวยาเมื่อได้รับความเสียหาย

6) การห้ามการกระทำบางอย่างในกิจกรรมบางอย่างบางประเภท เพื่อทำให้การคุ้มครองข้อมูลสำเร็จด้วยดี

โดยในการศึกษากฎหมายต่างประเทศเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่สามารถนำมาประยุกต์ใช้กับกรณีข้อมูลใน Big Data ได้ ผู้ศึกษาจะศึกษากฎหมายของประเทศสหรัฐอเมริกา และประเทศอังกฤษตามข้อกำหนดของสหภาพยุโรป ดังนี้

3.2.1 กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในประเทศสหรัฐอเมริกา

ประเทศสหรัฐอเมริกาถือเป็นดินแดนแห่งเสรีภาพและยึดถือแนวความคิดเรื่องสิทธิตามธรรมชาติว่ามนุษย์ทั้งหลายเกิดมาเท่าเทียมกัน มนุษย์มีสิทธิบางประการที่ติดตัวมนุษย์มาตั้งแต่เกิดจนกระทั่งถึงแก่ความตาย สิทธิดังกล่าว ได้แก่ สิทธิในชีวิต เสรีภาพในร่างกายสิทธิในทรัพย์สิน และความเสมอภาคซึ่งเป็นสิทธิที่ไม่สามารถโอนให้แก่กันได้ และผู้ใดจะล่วงละเมิดมิได้ โดยหลักประกันสำคัญที่สุดในการคุ้มครองสิทธิของบุคคลของประเทศสหรัฐอเมริกา ได้แก่ รัฐธรรมนูญ โดยเฉพาะฉบับแก้ไขเพิ่มเติม (Amendments) มาตรา 1-10 หรือ ที่เรียกว่า Bill of Right แต่การศึกษาบทบัญญัติของรัฐธรรมนูญแต่เพียงอย่างเดียวนั้น อาจไม่สามารถทราบถึงขอบเขตสิทธิที่ได้รับการคุ้มครองและแนวปฏิบัติที่แท้จริงได้ จึงจะต้องศึกษาแนวทางคำพิพากษาของศาลสูงสุดของสหรัฐอเมริกา (U.S. Supreme Court) ซึ่งเป็นองค์กรที่มีอำนาจตีความรัฐธรรมนูญด้วย

ประเทศสหรัฐอเมริกาใช้กฎหมายระบบคอนมอนลอว์ (Common Law) ซึ่งในอดีตที่ผ่านมาแนวความคิดเรื่องการคุ้มครองสิทธิในความเป็นอยู่มักจะอยู่ในรูปของกฎหมายคอมมอนลอว์ในเรื่องละเมิดอันเป็นการคุ้มครองความเป็นอยู่ส่วนตัวโดยคำพิพากษาของศาลในคดีละเมิดที่เรียกว่า Case Law การคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวได้รับการพัฒนาอีกครั้ง เมื่อมีการเผยแพร่บทความเรื่อง “The Right to Privacy” งานเขียนของนักนิติศาสตร์นามว่า Louis Brandies & Samuel Warren ที่ได้เสนอในบทความว่านอกเหนือจากสิทธิในความเป็นอยู่ส่วนตัวที่ได้รับความคุ้มครองแล้วตามที่มีในคอมมอนลอว์ บุคคลควรได้รับความคุ้มครองในความเป็นอยู่ส่วนตัวที่เกี่ยวกับการเผยแพร่หรือการตีพิมพ์ข้อเท็จจริงที่เกี่ยวกับตนด้วย และความตื่นตัวในเรื่องความเป็นอยู่ส่วนตัวในภาคเอกชนในประเทศสหรัฐอเมริกาได้ทวีความรุ่นแรงมากยิ่งขึ้นเมื่อมีความเจริญเติบโตของการใช้เทคโนโลยีต่าง ๆ โดยเฉพาะคอมพิวเตอร์ ตั้งแต่ทศวรรษที่ 1960 เป็นต้นมา โดยกฎหมายเกี่ยวกับการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวของประเทศสหรัฐอเมริกามีลักษณะเป็นระบบกฎหมายเฉพาะเรื่อง (Sectoral Law) ไม่มีกฎหมายแม่บทหรือกฎหมายกลางวางหลักเกณฑ์เป็นการทั่วไป สภาคองเกรสจะตรากฎหมายก็ต่อเมื่อเกิดปัญหาการป้องกันความลับหรือความเป็นอยู่ส่วนตัวของประชาชนถูกละเมิดขึ้น ดังนั้น การออกกฎหมายคุ้มครองส่วนบุคคลของประเทศสหรัฐอเมริกาจึงมีลักษณะเป็นการแก้ปัญหา

ที่เกิดขึ้นมากกว่าที่จะวางหลักเกณฑ์ทั่วไปเพื่อป้องกันปัญหา เป็นการตอบสนองหรือแก้ไขเป็นเรื่อง ๆ ไป กฎหมายคุ้มครองส่วนบุคคลของสหรัฐอเมริกาจึงมีลักษณะเฉพาะเรื่อง ไม่สมบูรณ์[38]

เนื่องจากประเทศสหรัฐอเมริกาปกครองประเทศในรูปแบบสหรัฐ นอกเหนือจากกฎหมายกลางของประเทศแล้ว มลรัฐต่าง ๆ ก็จะมีกฎหมายเฉพาะที่ตราออกมาใช้ภายในเขตรัฐนั้น ๆ ด้วย ดังนั้น การคุ้มครองความเป็นอยู่ส่วนตัวในประเทศสหรัฐอเมริกาจึงประกอบไปด้วยกฎหมายหลาย ๆ ส่วน ทั้งที่เป็นลายลักษณ์อักษร และไม่เป็นลายลักษณ์อักษร ดังนี้

1) รัฐธรรมนูญแห่งสหรัฐอเมริกา

ผู้พิพากษาศาลสูงสุดแห่งสหรัฐอเมริกานามว่า Black ได้เคยเขียนเอาไว้ในคำพิพากษาคดี *Griswold v. Connecticut* [39] ว่า “ข้อความว่าด้วยความเป็นอยู่ส่วนตัวนั้นเป็นสิ่งที่มีความหมายกว้าง เป็นนามธรรม และมีความหมายไม่ชัดเจน” รัฐธรรมนูญแห่งสหรัฐอเมริกาเองก็ไม่ได้ระบุถึงคำว่า “ความเป็นอยู่ส่วนตัว” เอาไว้ในรัฐธรรมอย่างชัดแจ้ง แต่ศาลสูงสุดก็ได้ตัดสินคดีโดยวินิจฉัยคุ้มครองถึงสิทธิในความเป็นอยู่ของประชาชนด้วย อย่างไรก็ตาม สิทธิในความเป็นอยู่ส่วนตัวก็ถือเป็นสิทธิที่มีความเกี่ยวข้องกับอิสรภาพและเสรีภาพของประชาชนที่ได้รับความคุ้มครองตามรัฐธรรมนูญแห่งสหรัฐอเมริกาอย่างไม่สามารถแบ่งแยกออกจากกันได้ และในประเทศสหรัฐอเมริกาก็ได้มีการกล่าวถึงความเป็นส่วนตัวมาเป็นเวลานานแล้วในฐานะที่เป็นสิทธิในการที่บุคคลจะเป็นอิสระจากการตรวจค้น การยึด หรือถูกรบกวนแทรกแซงโดยไม่มีเหตุอันควร รวมถึงสิทธิที่จะได้รับความคุ้มครองในข้อมูลส่วนบุคคล นอกจากนี้ยังมีการอธิบายความหมายของคำว่าสิทธิในความเป็นอยู่ส่วนตัวว่าหมายความรวมถึงสิทธิที่จะไม่เปิดเผยตัวตนและสิทธิที่จะอยู่โดยลำพัง ซึ่งการใช้ Big Data ส่งผลให้ผู้ใช้ข้อมูลสามารถทราบถึงข้อมูลส่วนบุคคล จนถึงสามารถบ่งชี้ตัวบุคคล ย่อมถือว่าเป็นบริบทที่เกี่ยวข้องกันสิทธิในความเป็นอยู่ส่วนตัวเช่นเดียวกัน

---

[38] ประสิทธิ์ ปิวาวัฒนพาณิช, “กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกาและประเทศออสเตรเลีย”, **วารสารนิติศาสตร์** 34, 537(ธันวาคม 2547).

[39] เป็นคดีที่เจ้าพนักงานได้ตรวจค้นห้องนอนของสามีภรรยาคู่หนึ่งเพื่อหาเครื่องมือหรือยาที่ใช้ในการคุมกำเนิด ศาลพิจารณาว่าเป็นการละเมิดสิทธิในความเป็นอยู่ส่วนตัว อันเป็นการคุ้มครองสิทธิโดยอาศัยหลัก Due Process หรือวิธีการที่ถูกต้องตามกฎหมาย ซึ่งเป็นกระบวนการคุ้มครองสิทธิของจำเลย โดยมีหลักการปฏิบัติต่อผู้กระทำความผิดต้องคำนึงถึงสิทธิเสรีภาพของบุคคลในฐานะที่เขาเป็นส่วนหนึ่งของสังคมด้วย ผู้ต้องหาไม่สามารถถูกบังคับให้ตอบคำถามเพื่อเป็นพยานหลักฐานที่เป็นปฏิปักษ์ต่อตนเองและไม่สามารถถูกค้นหรือยึดสิ่งของเพื่อนำไปเป็นหลักฐานโดยไม่มีเหตุอันสมควร.

2) กฎหมายสหพันธรัฐ (Federal Law)

ในระดับสหพันธรัฐ (Federal Law) ไม่มีกฎหมายกลาง หรือกฎหมายแม่บทที่วางหลักเกณฑ์คุ้มครองสิทธิในความเป็นอยู่ส่วนตัวไว้แต่อย่างใด แต่การคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวจะปรากฏเป็นกฎหมายเฉพาะเรื่องในกฎหมายหลายฉบับกระจัดกระจายกันไป อาทิ การคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวในมุมมองของภาครัฐ รัฐบาลของประเทศสหรัฐอเมริกาได้ตรากฎหมายเพื่อสร้างหลักเกณฑ์ที่ช่วยป้องกันมิให้หน่วยงานของรัฐบาลลุกล้ำความเป็นส่วนตัวของประชาชน กฎหมายฉบับดังกล่าว คือ The Privacy Act of 1974 ซึ่งกฎหมายฉบับนี้เป็นการจำกัดสิทธิของตัวแทนของรัฐบาลในการเก็บข้อมูลส่วนบุคคลของประชาชนโดยกำหนดให้ข้อมูลที่หน่วยงานของรัฐบาลจัดเก็บจะต้องมีลักษณะตาม § 552 a (e) เช่น เป็นการจัดเก็บเฉพาะข้อมูลที่เกี่ยวข้องและจำเป็นเพื่อให้เป้าหมายของหน่วยงานลุล่วงตามกฎหมายหรือตามคำสั่งฝ่ายบริหารของประธานาธิบดี เป็นการเก็บข้อมูลจากบุคคลเพื่อขยายขอบเขตความสามารถในการปฏิบัติงานใด ซึ่งข้อมูลนั้นอาจส่งผลทำให้เกิดการตัดสินใจที่เป็นปรปักษ์กับสิทธิส่วนบุคคลของบุคคลนั้น หรือเป็นการเก็บข้อมูลจากบุคคลเพื่อประโยชน์และอภิสิทธิ์ภายใต้โครองการของรัฐบาลกลาง หรือก่อนการเผยแพร่ข้อมูลเกี่ยวกับบุคคลนั้น ๆ ต้องมีความพยายามตามสมควรในการให้หลักประกันอันเหมาะสมว่าข้อมูลนั้นมีความถูกต้อง สมบูรณ์ เกิดขึ้นในเวลาที่เหมาะสมและเป็นข้อมูลมีความเกี่ยวข้องกับหน่วยงาน เป็นต้น นอกจาก The Privacy Act of 1974 แล้ว กฎหมายที่เกี่ยวข้องกับการคุ้มครองความเป็นส่วนตัวยังมีอีกหลายฉบับ อาทิ

- Electronic Freedom of Information Act (EFOIA) (กฎหมายความอิสระของข้อมูล)
- Fair Credit Reporting Act (1970) (กฎหมายรายงานเครดิตอย่างยุติธรรม)
- Family Educational Rights and Privacy Act (1974) (กฎหมายสิทธิการศึกษาของครอบครัวและความเป็นส่วนตัว)
- Tax Reform Act (1976) (กฎหมายการปฏิรูปภาษี)
- Right to Financial Privacy Act (1978) (กฎหมายสิทธิความเป็นส่วนตัวทางด้านการเงิน)
- Privacy Protection Act (1978) (กฎหมายคุ้มครองความเป็นส่วนตัว)
- Electronic Fund Transfer Act (1980) (กฎหมายการโอนเงินทางอิเล็กทรอนิกส์)
- Electronic Communications Privacy Act (1986) (กฎหมายความเป็นส่วนตัวในการสื่อสารทางอิเล็กทรอนิกส์)
- Video Privacy Protection Act (1988) (กฎหมายคุ้มครองความเป็นส่วนตัวทางวีดิทัศน์)

- Bank Secrecy Act of 1970 (กฎหมายเกี่ยวกับความลับในกิจการของธนาคาร)
- Occupational Health and Safety Act of 1970 (กฎหมายความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงาน
- Employee Polygraph Protection Act of 1988 (กฎหมายเกี่ยวกับการจับเท็จของพนักงาน)

กฎหมายดังกล่าว แบ่งการคุ้มครองตามลักษณะของข้อมูลหรือกิจกรรมที่ควรได้รับการคุ้มครอง เช่น ความเป็นส่วนตัวของผู้บริโภค (Consumer Privacy) ข้อมูลการขับขี่ (Driving Records) ความเป็นส่วนตัวทางการเงิน (Financial Privacy) ข้อมูลทางราชการ (Government Records) ข้อมูลทางการแพทย์ (Medical Records) ข้อมูลภายในโรงเรียน (School Records) การเช่าวีดีโอ (Video Rentals) การดักฟังโทรศัพท์ การควบคุม การเข้ารหัส (Wiretapping, Surveillance and Encryption) หรือทดสอบในที่ทำงาน (Workplace Testing) เป็นต้น

อย่างไรก็ตาม กฎหมายที่เกี่ยวข้องกับการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวในระดับสหพันธรัฐดังกล่าวมานั้น ยังไม่ยืดหยุ่นเพียงพอที่จะนำมาปรับใช้กับการใช้ Big Data ในทางมิชอบได้ โดยกฎหมายต่าง ๆ ที่กล่าวมาต่างก็มีข้อจำกัดบางประการที่ทำให้ไม่สามารถนำมาบังคับใช้กับการละเมิดสิทธิในความเป็นอยู่ส่วนตัวอันรวมถึงการละเมิดข้อมูลส่วนบุคคลจากการใช้ Big Data ได้ อาทิ The Privacy Act of 1974 นั้นใช้กับการคุ้มครองข้อมูลส่วนบุคคลที่จัดเก็บโดยเจ้าหน้าที่ของรัฐเท่านั้น มิได้ให้ความคุ้มครองถึงข้อมูลส่วนบุคคลที่จัดเก็บโดยเอกชน หรือ Electronic Communications Privacy Act (1986) ที่มุ่งคุ้มครองความเป็นส่วนตัวในข้อมูลที่มีเนื้อหาเกี่ยวกับการติดต่อสื่อสารกันทางอิเล็กทรอนิกส์ก็คุ้มครองเฉพาะข้อมูลที่เกี่ยวข้องกับการสื่อสารเท่านั้น ไม่ใช่บังคับกับข้อมูลที่เกี่ยวกับธุรกรรมซื้อขาย ซึ่งข้อมูลใน Big Data นั้น มีข้อมูลที่เป็นพฤติกรรมของผู้บริโภคอันทำให้บริษัทผู้ทำการบันทึกสามารถเก็บรวบรวมข้อมูลผู้บริโภคได้มากมายมหาศาล แต่ข้อมูลที่เก็บไว้ดังกล่าวกลับไม่อยู่ภายใต้บังคับของ Electronic Communications Privacy Act (1986)

3) กฎหมายในระดับมลรัฐ (State Law)

แม้ในขณะนี้ประเทศสหรัฐอเมริกาจะยังไม่มีกฎหมายใดที่ออกมาเพื่อควบคุมการใช้ Big Data โดยเฉพาะ แต่รัฐต่าง ๆ ในสหรัฐอเมริกาได้มีความพยายามในการออกกฎหมายเพื่อคุ้มครองความเป็นส่วนตัว เช่น มลรัฐ California ได้พยายามผลักดันร่างกฎหมาย The Identity Information Protection Act of 2005 ซึ่งมีวัตถุประสงค์เพื่อควบคุมการเก็บข้อมูลที่มีการระบุถึงตัวตน และข้อมูลการรักษาพยาบาลทั้งทางด้านอายุรเวชหรือจิตเวช ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่สามารถเผยแพร่หรือถูกอ่านได้จากระยะไกลโดยใช้คลื่นความถี่วิทยุเป็นสื่อกลางในการอ่าน โดยกำหนดให้ข้อมูลเหล่านั้นต้องมีการเก็บรักษาตามเงื่อนไขที่ได้กำหนดไว้ในกฎหมาย อาจกล่าวได้ว่าร่าง

กฎหมายฉบับนี้มีวัตถุประสงค์เพื่อจัดการกับประเด็นปัญหาการใช้ Big Data กับข้อมูลที่ใช้เพื่อการระบุตัวตนโดยเฉพาะ (ร่างกฎหมายดังกล่าวนี้ได้ตกไป แต่มีการเสนอร่างกฎหมายที่มีสาระสำคัญในทำนองเดียวกันนี้เข้ามาใหม่ในปี ค.ศ. 2008) และในปี ค.ศ. 2005 นี้ มลรัฐ California ยังได้เสนอร่างกฎหมายที่เกี่ยวข้องกับการเก็บสะสมข้อมูลอีกฉบับหนึ่งซึ่งมีเนื้อหาเกี่ยวข้องกับการทำธุรกรรมการเงิน กล่าวคือ มีเนื้อหาเกี่ยวข้องกับการใช้เครื่องกดเงินอัตโนมัติ (Automated Teller Machines หรือ ATM) โดยมีสาระสำคัญว่ากรณีที่มีการนำเทคโนโลยีใด ๆ มาใช้เพื่อช่วยเหลือบุคคลที่มีความบกพร่องในทางสายตาให้สามารถเข้าถึงระบบของเครื่อง ATM จะต้องมีการกำหนดมาตรการเพื่อรักษาสิทธิในความเป็นอยู่สาวนตัวสำหรับผู้ที่มีความบกพร่องทางสายตานั้นในระดับเดียวกันกับบุคคลโดยทั่วไป

4) คำพิพากษาของศาลในคดีละเมิด (Common Law: Tort Law)

นักนิติศาสตร์นามว่า William Prosser ได้แยกแยะสิทธิในความเป็นอยู่ส่วนตัวออกเป็น 4 รูปแบบตามแบบอย่างที่แตกต่างกันของคดี และผลประโยชน์ที่แตกต่างกัน ซึ่งมุ่งจะคุ้มครองต่อรูปแบบที่แตกต่างกันของการละเมิด คือ[40]

(1) การรบกวนแทรกแซงความสันโดษหรือกิจกรรมส่วนตัว (Intrusion) ได้แก่ การรบกวนขอบเขตส่วนตัวโดยไม่ได้รับอนุญาตหรือเข้าไปยุ่งในกิจกรรมส่วนตัวของเขา เช่น ลอบฟังการสนทนาส่วนตัวด้วยการดักฟังโทรศัพท์ หรือลอบสังเกตในที่อยู่อาศัย เป็นต้น

(2) การเปิดเผยเรื่องราวส่วนตัว (Public Disclosure of Private Facts) ได้แก่ การพิมพ์เผยแพร่ข้อเท็จจริงเกี่ยวกับชีวิตส่วนตัวของบุคคลโดยไม่มีอำนาจ แม้จะเป็นความจริงแต่ก็ทำให้อับอายขายหน้า ซึ่งคดีเหล่านี้มักจะยุ่งยากที่จะชั่งน้ำหนักผลประโยชน์ส่วนตัวที่จะเก็บความลับในชีวิตส่วนตัวของเขากับผลประโยชน์ของสาธารณะที่ได้รับการแนะนำ

(3) การไขข่าวแพร่หลายซึ่งข้อความอันฝ่าฝืนความจริง (False Light in the Public Eye) ได้แก่ การทำให้โจทก์ต้องเป็นที่เสื่อมเสียในสายตาของประชาชน โดยการใช้ชื่อโจทก์หรือภาพแสดงเรื่องราวที่เขาไม่ได้เกี่ยวข้อง

(4) การใช้ชื่อหรือภาพของบุคคลเพื่อผลประโยชน์โดยไม่ได้รับความยินยอม (Appropriation) ได้แก่ การใช้ชื่อหรือภาพของโจทก์โดยที่เขามิได้ยินยอมเพื่อเขียนหรือถ่ายทำภาพยนตร์หรือโฆษณา หรือใช้เป็นชื่อบริษัทหรือสินค้าเพื่อประโยชน์ของตน

การละเมิดสิทธิในความเป็นอยู่ส่วนตัวอันเป็นส่วนหนึ่งของกฎหมายคอมมอนลอว์เรื่องละเมิดตามทฤษฎีของ Prosser ดังกล่าวนั้น เป็นที่ยอมรับกันเป็นการทั่วไปโดยศาลของ

---

[40] เรื่องเดียวกัน, 5-6.

สหรัฐอเมริกา ซึ่งต่อมาแนวความคิดดังกล่าวได้รับการคุ้มครองไว้ใน The Restatement Second of Torts ดังที่ได้บัญญัติไว้ใน The Restatement Second of Torts Sections 652A-652I โดยใน § 652A[41] แบ่งการละเมิดสิทธิในความเป็นอยู่ส่วนตัวไว้เป็นประเภทต่าง ๆ 4 ประเภท ดังนี้

(1) การละเมิดความต้องการอยู่คนเดียวโดยปราศจากการรบกวน

(2) การใช้ชื่อหรือสิ่งที่คล้ายคลึงกันของผู้อื่นโดยมิชอบ

(3) การเปิดเผยข้อมูลส่วนตัวต่อสาธารณะ

(4) การไขข่าวแพร่หลายซึ่งข้อความอันฝ่าฝืนความจริง

5) แนวปฏิบัติ (Guideline) ต่าง ๆ

เนื่องจากประเทศสหรัฐอเมริกาไม่มีองค์กรอิสระที่มีอำนาจหน้าที่ในการควบคุมดูแลสิทธิส่วนบุคคลโดยตรง การคุ้มครองสิทธิความเป็นอยู่ส่วนตัวในภาคเอกชนจึงอาศัยกลไกในการดำเนินการให้บรรลุตามวัตถุประสงค์ของกฎหมายที่เรียกว่า “ระบบการการคุ้มครองตนเอง” (Self-Regulation) กล่าวคือ กฎหมายเปิดโอกาสให้เอกชนหรือผู้ประกอบการซึ่งเป็นผู้ดำเนินกิจการสามารถออกกฎเกณฑ์ แนวปฏิบัติ หรือประมวลจริยธรรมเพื่อใช้ควบคุมกันเองภายในองค์กร โดยมีบุคคลหรือคณะบุคคลที่ได้รับเลือกตั้งหรือแต่งตั้งจากคนในองค์กรเป็นผู้ดำเนินการให้บรรลุวัตถุประสงค์ การใช้มาตรการให้ภาคธุรกิจไม่ให้เอาเปรียบผู้บริโภคของตน โดยมองว่าหน้าที่ในการคุ้มครองผู้บริโภคไม่ใช่ภารกิจที่รัฐมีบทบาทเพียงลำพัง ภาคธุรกิจซึ่งอยู่ในฐานะที่ได้เปรียบย่อมมีหน้าที่ในการปกป้องสิทธิของผู้บริโภคด้วยกันเอง หากภาคธุรกิจควบคุมกันอย่างแข็งขันแล้วผลที่ตามมาก็คือ ทำให้ผู้บริโภคมีความมั่นใจต่อการทำธุรกรรมกับผู้ประกอบการนั้น ๆ

การควบคุมดูแลกันเองโดยภาคเอกชนนี้จะมีเจ้าหน้าที่หรือหน่วยงานของรัฐมาคอยตรวจสอบควบคุม หรือกำกับดูแลอีกชั้นหนึ่ง โดยหน่วยงานของรัฐที่มีอำนาจหน้าที่ตามกฎหมายเกี่ยวกับการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวก็คือ คณะกรรมการการค้าแห่งสหพันธรัฐ (The Federal Trade Commission หรือ FCT) ที่อาศัยอำนาจตาม มาตรา 5 แห่ง Federal Trade Commission Act ใน

---

[41] § 652A. General Principle

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

(2) The right of privacy is invaded by

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

(b) Appropriation of the other’s name or likeness, as stated in§ 652C; or

(c) Unreasonable publicity given to the other’s private life, as stated in § 652D; or

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

การสั่งให้ภาคเอกชนหยุดหรือระงับการกระทำที่ไม่เป็นธรรมหรือมีเจตนาที่หลอกลวงในกิจการต่าง ๆ เช่น มีอำนาจตรวจสอบเกี่ยวกับการแข่งขันทางการค้าที่ไม่เป็นธรรม รวมไปถึงในกรณีที่ภาคเอกชนไม่ปฏิบัติตาม Self-Regulation ไม่ว่าทั้งหมด หรือเพียงส่วนหนึ่งส่วนใดของหลักการดังกล่าว FCT มีอำนาจที่จะควบคุมดูแลให้ภาคเอกชนต้องปฏิบัติตาม Self-Regulation นั้น ๆ ของตนอย่างเคร่งครัด กล่าวคือ มีหน้าที่บังคับหารให้เป็นไปตาม Self-Regulation ที่ภาคเอกชนได้ออกกฎเกณฑ์ แนวปฏิบัติ หรือประมวลจริยธรรมเพื่อใช้ควบคุมกันเองภายในองค์กร โดยมีองค์กรเอกชนที่นำกรอบแนวนโยบายนี้ไปเป็นหลักการแล้ว มีตัวอย่างดังนี้

Electronic Product Code Global (EPC Global) เป็นหน่วยงานที่มีบทบาทสำคัญในการผลักดันการนำ Electronic Product Code[42] หรือเลขรหัสสินค้าอิเล็กทรอนิกส์ มาใช้ทั่วโลก มองว่าควรมีการตระหนักถึงประเด็นปัญหาเกี่ยวกับสิทธิในความเป็นอยู่ส่วนตัวที่อาจเกิดจากการใช้งานระบบ EPC สามารถบรรลุประโยชน์สูงสุดให้แก่ลูกค้า ดังนั้น EPC Global หน่วยงานผู้รับผิดชอบจึงได้มีการออกแนวปฏิบัติการใช้งานเลขรหัสสินค้าอิเล็กทรอนิกส์ในสินค้าอุปโภคบริโภค “Guidelines on EPC for Consumer Products” โดยมีเจตนารมณ์เพื่อให้การใช้งานสอดคล้องกับกฎหมายหรือกฎเกณฑ์ที่เกี่ยวข้องกับการคุ้มครองสิทธิของผู้บริโภค โดยมีเนื้อหาหลักแบ่งออกได้เป็น 4 ส่วน ได้แก่

1) การแจ้งต่อลูกค้า (Consumer Notice) มีหลักว่าต้องมีการแจ้งอย่างชัดเจนถึงการใช้ EPC บนสินค้าหรือหีบห่อ โดยการแจ้งถึงการใช้ EPC นั้น จะทำโดยการติด Logo ของ EPC บนสินค้าหรือหีบห่อ

2) การใช้สิทธิแก่ลูกค้า (Consumer Choice) ลูกค้าจะต้องได้รับการแจ้งสิทธิในการทิ้งหรือเอาป้าย EPC ออกจากสินค้า โดยป้าย EPC นั้นควรติดอยู่กับส่วนที่สามารถเอาออกได้ และผู้สนับสนุนการใช้เทคโนโลยีควรหาวิธีที่มีประสิทธิภาพ และเชื่อถือได้ เพื่อสร้างทางเลือกให้แก่ลูกค้าในราคาที่สมเหตุสมผล

3) การให้ความรู้แก่ลูกค้า (Consumer Education) ลูกค้าต้องมีโอกาสที่จะได้รับความรู้ที่ถูกต้องเกี่ยวกับเทคโนโลยี EPC รวมถึงข้อมูลเกี่ยวกับความก้าวหน้าทางเทคโนโลยี บริษัทที่นำ EPC ไปใช้ในระกับผู้บริโภคจะต้องพยายามทำให้ลูกค้าเกิดความคุ้นเคยกับ Logo ของ EPC โดย EPC Global จะทำหน้าที่เป็นเวทีระหว่างบริษัทที่ใช้ EPC กับลูกค้า เพื่อเรียนรู้เกี่ยวกับเทคโนโลยี EPC หรือเพื่อพูดถึงปัญหาในการใช้งาน

[42] Ibid, 48.

4) การเก็บ การใช้ข้อมูล และการรักษาความมั่นคงปลอดภัย (Record, Use, Retention and Security) โดยมีหลักว่าป้าย EPC นั้นต้องไม่ได้มีการเก็บรวบรวมหรือบรรจุข้อมูลที่สามารถระบุตัวบุคคลได้ ทั้งนี้ เช่นเดียวกับการเก็บข้อมูลโดยใช้บาร์โค้ด โดยข้อมูลที่ถูกจัดเก็บ ใช้ หรือรักษาไว้โดยบริษัทสมาชิกของ EPC Global ซึ่งการเก็บ ใช้ หรือรักษาจะเป็นตามกฎหมาย

3.2.2 กฎหมายเกี่ยวกับการคุ้มครองข้อมูลในประเทศอังกฤษตามข้อกำหนดของสหภาพยุโรป (Directive 95/46/EC)

กฎหมายเกี่ยวกับการคุ้มครองข้อมูลในประเทศอังกฤษ มีความเป็นมาเริ่มต้นในปี ค.ศ. 1970 เมื่อมีภัยคุกคามต่อความเป็นส่วนตัวของข้อมูลข่าวสารส่วนบุคคลที่เกิดจากการเกิดขึ้นของคอมพิวเตอร์ มีการใช้ข้อมูลในทางที่ผิดที่เกิดขึ้นได้อย่างรวดเร็ว ซึ่งนั่นรวมถึงการใช้ข้อมูลใน Big Data ด้วย กฎหมายที่บังคับใช้ในขณะนั้นไม่สามารถรับมือกับปริมาณของข้อมูลข่าวสารส่วนบุคคลที่องค์กรต่าง ๆ ครอบครองได้ ในปี ค.ศ. 1972 The Younger Committee on Privacy จึงเสนอแนวทางในการใช้คอมพิวเตอร์ที่มีข้อมูลส่วนบุคคล โดยกำหนดว่าควรมีการครอบครองข้อมูลเฉพาะเพื่อวัตถุประสงค์ใดวัตถุประสงค์หนึ่งโดยเฉพาะ และไม่ควรนำข้อมูลมาใช้เพื่อวัตถุประสงค์อื่น ๆ โดยไม่ได้รับอนุญาต การนำข้อมูลไปใช้ต้องมีการบอกกล่าวกับเจ้าของข้อมูลว่าสามารถเข้าถึงข้อมูล หรือครอบครองข้อมูลของบุคคลนั้น ๆ อยู่

พระราชบัญญัติคุ้มครองข้อมูลข่าวสารปี ค.ศ. 1984 กำหนดให้มีการจัดตั้งสำนักทะเบียนคุ้มครองข้อมูลข่าวสาร และกำหนดให้ผู้ประมวลผลดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลต้องลงทะเบียนการปฏิบัติการดังกล่าว และปฏิบัติตามข้อกำหนดหลัก 8 ประการของการคุ้มครองข้อมูลข่าวสารตามกฎหมาย ปี ค.ศ. 1998 (Data Protection Act 1998) ซึ่งสามารถนำมาประยุกต์ใช้กับกรณีข้อมูลใน Big Data มีสาระสำคัญดังนี้

1) ข้อมูลส่วนบุคคลจะถูกประมวลผลอย่างยุติธรรมและถูกกฎหมาย และการประมวลผลดังกล่าวต้องสอดคล้องกฎที่เฉพาะเจาะจงอย่างน้อยหนึ่งกฎ

2) ข้อมูลส่วนบุคคลจะได้รับเมื่อวัตถุประสงค์โดยเฉพาะ และถูกกฎหมายหนึ่งวัตถุประสงค์ หรือมากกว่าหนึ่งวัตถุประสงค์ และจะไม่ถูกประมวลผลในวิถีทางที่ขัดกับวัตถุประสงค์นั้น หรือวัตถุประสงค์อื่น ๆ

3) ข้อมูลส่วนบุคคลจะต้องเพียงพอ มีความสอดคล้อง และมีปริมาณที่สัมพันธ์กับวัตถุประสงค์ใด ๆ หรือหลาย ๆ วัตถุประสงค์ในการประมวลผล

4) ข้อมูลส่วนบุคคลจะต้องถูกต้อง และต้องไม่ล้าสมัย

5) ข้อมูลส่วนบุคคลที่ถูกประมวลผลเพื่อวัตถุประสงค์ใดวัตถุประสงค์หนึ่ง หรือวัตถุประสงค์หลาย ๆ อย่าง จะต้องไม่ถูกเก็บรักษาไว้นานกว่าที่จำเป็นต่อวัตถุประสงค์ใดวัตถุประสงค์หนึ่ง หรือวัตถุประสงค์หลาย ๆ อย่าง

6) ข้อมูลส่วนบุคคลจะต้องถูกประมวลผลอย่างสอดคล้องกับสิทธิของเจ้าของข้อมูลตามพระราชบัญญัติ

7) มาตรการทางเทคนิคที่เหมาะสมจะถูกนำไปใช้คัดค้านการประมวลผลข้อมูลส่วนบุคคลที่ไม่ได้รับอนุญาตและผิดกฎหมาย และป้องกันการสูญเสียหรือการทำลายและความเสียหายที่มีต่อข้อมูลส่วนบุคคล

8) ข้อมูลส่วนบุคคลจะไม่ถูกส่งต่อไปยังประเทศ หรือเขตที่อยู่ภายนอกเศรษฐกิจยุโรป ยกเว้นว่าประเทศนั้นหรือเขตเศรษฐกิจนั้นได้รับประกันระดับการคุ้มครองที่เพียงพอในสิทธิและเสรีภาพของเจ้าของข้อมูลที่มีต่อการประมวลผลข้อมูลข่าวสารส่วนบุคคล

ซึ่งหลักการทั้ง 8 ประการดังกล่าวผ่านการเห็นชอบโดยสหราชอาณาจักร เพื่อให้สอดคล้องกับข้อกำหนดของสหภาพยุโรป Directive 95/46/EC (European Directive 95/46/EC) โดยได้ขยายนิยามของการประมวลผลข้อมูล การเพิ่มประเภทข้อมูล ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) การขยายสิทธิในการเข้าถึงของเจ้าของข้อมูล และการห้ามโอนข้อมูลส่วนบุคคลไปยังนอกประเทศสหภาพยุโรป

เนื่องจากประเทศอังกฤษเป็นประเทศหนึ่งในสหภาพยุโรป และกฎหมายคุ้มครองข้อมูลข่าวสารของประเทศอังกฤษในปัจจุบันได้บัญญัติให้สอดคล้องกับหลักการการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ซึ่งออกในปี ค.ศ. 1995 จึงเห็นสมควรศึกษาแนวทางการคุ้มครองตามข้อกำหนดของสหภาพยุโรป (Directive 95/46/EC)

European Union Directive on Data Protection-Directive 95/46/EC เป็นระเบียบของสหภาพยุโรปที่มีวัตถุประสงค์เพื่อคุ้มครองข้อมูลส่วนบุคคล และความเป็นส่วนตัวของบุคคลในประเทศสมาชิกของสหภาพยุโรป โดยเฉพาะในเรื่องการประมวลผลข้อมูลส่วนบุคคลโดยวิธีการอัตโนมัติ หรือโดยวิธีการอื่นใด ซึ่งข้อมูลส่วนบุคคลนั้นเป็นส่วนหนึ่งของระบบการจัดเก็บข้อมูลโดยคำนึงถึงหลักพื้นฐานของสิทธิขั้นพื้นฐานและเสรีภาพส่วนบุคคลเป็นสำคัญ ทั้งนี้ แนวปฏิบัตินี้ได้กำหนดให้ประเทศสมาชิกของสหภาพยุโรปบัญญัติกฎหมายให้เป็นไปตามแนวทางที่กำหนดนี้

หลักการและสาระสำคัญของกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่สามารถนำมาประยุกต์ใช้กับกรณีข้อมูลใน Big Data ซึ่งยกร่างขึ้นตามแนวทางของสหภาพยุโรป คือ

1) ขอบเขตของกฎหมาย

ร่างพระราชบัญญัติฯกำหนดให้ใช้บังคับแก่การประมวลผลข้อมูลส่วนบุคคลแม้เพียงส่วนหนึ่งส่วนใดหรือทั้งหมดโดยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีอัตโนมัติ หรือโดยวิธีการอื่นใดที่มิใช่วิธีการทางอิเล็กทรอนิกส์ หรือวิธีการโดยอัตโนมัติซึ่งกระทำขึ้นในราชอาณาจักร รวมทั้งที่มีการจัดเก็บไว้นอกราชอาณาจักร แต่ไม่ใช้บังคับกับการประมวลผลข้อมูลส่วนบุคคลโดยบุคคลธรรมดา เพียงเพื่อ

วัตถุประสงค์ในการใช้ส่วนบุคคล เว้นแต่จะมีวัตถุประสงค์ในการเปิดเผยข้อมูลนั้นโดยทั่วไป หรือโดยเฉพาะเจาะจง

2) คำนิยาม

ร่างพระราชบัญญัติฯ ได้บัญญัติคำนิยามที่สำคัญดังนี้

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้น หรือเลขหมาย รหัสหรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่าย และให้หมายความรวมถึง ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมด้วย

“การประมวลผลข้อมูล” หมายความว่า การดำเนินการใด ๆ กับข้อมูลส่วนบุคคล โดยวิธีการทางอิเล็กทรอนิกส์ วิธีการอัตโนมัติ หรือวิธีการอื่นใดในการเก็บ รวบรวม บันทึก จัดหมวดหมู่ เก็บรักษา ให้รายละเอียด แก้ไขเปลี่ยนแปลง คัดเลือก เรียกข้อมูลจากระบบ เปรียบเทียบ ใช้ประโยชน์ เชื่อมโยง ระงับการใช้ชั่วคราว เปิดเผยข้อมูลโดยเฉพาะเจาะจงหรือโดยทั่วไป ลบ หรือทำลายข้อมูล

“ผู้ควบคุมข้อมูล” หมายความว่า บุคคลธรรมดา คณะบุคคล นิติบุคคล หรือหน่วยงานของรัฐ ซึ่งดำเนินการประมวลผล หรือควบคุมและกำกับการประมวล ผลข้อมูลส่วนบุคคลของผู้ประมวลผลข้อมูล โดยกำหนดวัตถุประสงค์หรือวิธีการในการประมวลผลข้อมูลนั้น

“ผู้ประมวลผลข้อมูล” หมายความว่า บุคคลธรรมดา คณะบุคคล หรือหน่วยงานของรัฐ ซึ่งดำเนินการประมวลผลข้อมูลเอง หรือดำเนินการในนามหรือแทนผู้ควบคุมข้อมูล หรือผู้ทำหน้าที่กำกับการประมวลผลข้อมูล

“คณะกรรมการ” หมายความว่า คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

3) หลักการประมวลผลข้อมูลส่วนบุคคล

ร่างพระราชบัญญัตินี้กำหนดหลักการของการประมวลผลข้อมูลไว้ว่า การประมวลผลข้อมูลส่วนบุคคล โดยวิธีการทางอิเล็กทรอนิกส์ วิธีการอัตโนมัติ หรือวิธีการอื่นใดในการเก็บ รวบรวม บันทึก จัดหมวดหมู่ เก็บรักษา ให้รายละเอียด แก้ไขเปลี่ยนแปลง คัดเลือก เรียกข้อมูลจากระบบเปรียบเทียบ ใช้ประโยชน์ เชื่อมโยง ระงับการใช้ชั่วคราว เปิดเผยข้อมูลโดยเฉพาะเจาะจงหรือโดยทั่วไป ลบ หรือทำลายข้อมูล จะกระทำมิได้ เว้นแต่ได้รับความเห็นชอบจากเจ้าของข้อมูล และภายในวัตถุประสงค์ของการประมวลผลข้อมูลโดยชัดแจ้ง โดยมีการรักษาความมั่นคงปลอดภัยของข้อมูล และต้องตรวจสอบข้อมูลนั้นให้ถูกต้องเสมอ

4) ผู้ควบคุมข้อมูล

เป็นบทบัญญัติกำหนดเกี่ยวกับหน้าที่ให้บุคคลที่ประสงค์จะทำหน้าที่เป็นผู้ควบคุมข้อมูลต้องแจ้ง (Notification) ให้คณะกรรมการทราบ นอกจากนี้บัญญัติเกี่ยวกับข้อยกเว้นให้ผู้ควบคุมข้อมูลไม่

ต้องแสดงรายการบางรายการสำหรับการประมวลผลบางประเภท เช่น การประมวลผลโดยหน่วยงานของรัฐเพื่อประโยชน์สาธารณะ การประมวลผลโดยผู้ประกอบวิชาชีพเกี่ยวกับหนังสือพิมพ์ หรือการเขียนข่าว เป็นต้น และบัญญัติเกี่ยวกับข้อยกเว้นในกรณีที่ไม่จำเป็นต้องแจ้งต่อคณะกรรมการ หากเป็นการประมวลข้อมูลตามที่กำหนดในกฎหมายอื่นเป็นการเฉพาะ การประมวลผลข้อมูลจากเอกสารมหาชน หรือจากเอกสารที่สามารถหาได้โดยทั่วไป หรือการประมวลผลเกี่ยวกับบัญชี เงินเดือน ผลกำไร รายงานประจำปี เพื่อใช้ภายในหน่วยงาน เป็นต้น อีกทั้งยังกำหนดให้มีการจัดให้มีรูปแบบการเข้าถึงข้อมูลสำหรับผู้ด้อยโอกาส หรือคนพิการด้วย

5) การประมวลผลข้อมูล

เป็นบทบัญญัติเกี่ยวกับการประมวลผลโดยชอบด้วยกฎหมายและรูปแบบคุณภาพของข้อมูล และบทบัญญัติเกี่ยวกับความยินยอมของเจ้าของข้อมูล และข้อยกเว้นที่สามารถประมวลผลข้อมูลได้แม้จะไม่ได้รับความยินยอมจากเจ้าของข้อมูล เช่น การประมวลผลเพื่อประโยชน์ต่อการศึกษาวิจัยทางวิทยาศาสตร์ หรือเป็นข้อมูลทางสถิติ การประมวลผลสาขาวิชาชีพเกี่ยวกับหนังสือพิมพ์ หรือการเขียนข่าว การประมวลผลเพื่อประโยชน์ในการคุ้มครองหรือประกันชีวิต หรือสุขภาพ ในกรณีที่เจ้าของข้อมูลไม่สามารถให้ความยินยอมได้ เป็นต้น

6) การคุ้มครองเจ้าของข้อมูล

เป็นบทบัญญัติเกี่ยวกับสิทธิของเจ้าของข้อมูล เช่น ตรวจสอบข้อมูลของตนที่มีการจัดเก็บไว้ สิทธิโต้แย้งคัดค้านว่า ข้อมูลของตนไม่ถูกต้อง เป็นต้น

7) ความมั่นคงปลอดภัยของข้อมูลที่มีการประมวลผล

เป็นบทบัญญัติเกี่ยวกับความมั่นคงปลอดภัยของข้อมูล คือ การกำหนดให้ประมวลผลโดยใช้มาตรฐานทางเทคโนโลยีและมาตรฐานความมั่นคงปลอดภัยขั้นต่ำของข้อมูล ซึ่งกำหนดให้เป็นไปตามที่คณะกรรมการประกาศกำหนด และบทบัญญัติเกี่ยวกับการหยุดประมวลผล

8) การเปิดเผยข้อมูลโดยทั่วไปและเปิดเผยข้อมูลโดยเฉพาะเจาะจง

เป็นบทบัญญัติกำหนดเกี่ยวกับหลักเกณฑ์ของการเปิดเผยข้อมูลว่า จะทำการประมวลผลโดยการเปิดเผยข้อมูล ทั้งโดยทั่วไปและโดยเฉพาะเจาะจง โดยปราศจากความยินยอมของเจ้าของข้อมูลโดยชัดแจ้งไม่ได้ เว้นแต่เป็นการใช้ข้อมูลตามปกติภายในวัตถุประสงค์ของการประมวลผลข้อมูลนั้น หรือเป็นการบัญญัติกฎหมาย หรือประกาศ ระเบียบหรือกฎเกณฑ์ที่ออกตามในบทบัญญัติแห่งกฎหมาย รวมถึงการเปิดเผยในขอบเขตของวิชาชีพหนังสือพิมพ์หรือการเขียนข่าว เป็นต้น

9) ข้อมูลห้ามประมวลผล

เป็นบทบัญญัติกำหนดเกี่ยวกับลักษณะของข้อมูลส่วนบุคคลชนิดพิเศษ ซึ่งต้องห้ามมิให้มีการประมวลผล เช่น ข้อมูลเกี่ยวกับ เชื้อชาติ เผ่าพันธุ์ ความเชื่อทางศาสนา ปรัชญาหรือลัทธิความเชื่อถือ ความคิดเห็นทางการเมือง สุขภาพ เป็นต้น รวมทั้งหลักเกณฑ์ของการเปิดเผยข้อมูลดังกล่าวด้วย

10) การส่งหรือโอนข้อมูลไปประเทศอื่น

เป็นบทบัญญัติกำหนดเกี่ยวกับหลักเกณฑ์ของการส่งหรือโอนข้อมูลไปนอกราชอาณาจักร และข้อยกเว้นของการห้ามโอนข้อมูลดังกล่าว

11) คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เป็นบทบัญญัติกำหนดเกี่ยวกับเรื่อง คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล อาทิ องค์ประกอบของคณะกรรมการ อำนาจหน้าที่ของคณะกรรมการ รูปแบบการดำเนินงานของคณะกรรมการ สำนักงาน อำนาจหน้าที่ของสำนักงาน และเลขาธิการ นอกจากนี้ยังได้วางหลักเกณฑ์เกี่ยวกับการร้องเรียน การอุทธรณ์ ความรับผิดทางแพ่ง และการกำหนดโทษทางอาญา กรณีที่มีการฝ่าฝืนบทบัญญัติของกฎหมาย

ทางด้านการรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security) ของสหภาพยุโรป ในปี ค.ศ. 2012 คณะกรรมาธิการยุโรปได้พิจารณาว่า มีความจำเป็นหรือไม่ที่จะต้องเพิ่มเติมกฎระเบียบและความครอบคลุมเกี่ยวกับการแจ้งเตือนเมื่อข้อมูลส่วนบุคคลใน Big Data รั่วไหล

ผู้ประกอบกิจการโทรคมนาคมและผู้ให้บริการอินเทอร์เน็ตเก็บข้อมูลจำนวนมากเกี่ยวกับลูกค้า ซึ่งรวมถึง ชื่อ ที่อยู่ และรายละเอียดบัญชีธนาคาร กฎหมายแม่บทเรื่องความเป็นส่วนตัวและการสื่อสารอิเล็กทรอนิกส์ของสหภาพยุโรป (E-Privacy Directive) ฉบับปัจจุบัน ระบุว่าผู้ให้บริการจำเป็นจะต้องเก็บรักษาข้อมูลเหล่านี้ไว้อย่างปลอดภัย และต้องแจ้งเจ้าของข้อมูลทุกคนให้ทราบหากข้อมูลดังกล่าวสูญหายหรือถูกขโมย รวมถึงจะต้องรายงานกรณีการรั่วไหลดังกล่าวไปยังองค์กรดูแลระดับประเทศที่เกี่ยวข้องด้วย ซึ่งกรณีนี้สามารถนำมาประยุกต์ใช้กับข้อมูลใน Big Data ได้

อย่างไรก็ตาม นีลี โครส์ กรรมาธิการวาระดิจิทัลของคณะกรรมาธิการยุโรป ได้ประกาศเมื่อวันที่ 14 กรกฎาคม พ.ศ. 2554 ว่าเธอจะเปิดให้สาธารณะเข้าร่วมปรึกษาหารือให้ความคิดเห็นว่าสมควรจะมีกฎระเบียบอะไรเพิ่มเติมอีกหรือไม่ “หน้าที่ที่จะแจ้งให้ทราบถึงการรั่วไหลของข้อมูล เป็นส่วนประกอบสำคัญในกฎระเบียบใหม่ของสหภาพยุโรปว่าด้วยกิจการโทรคมนาคม แต่มันต้องสม่ำเสมอกันทั่วทั้งสหภาพยุโรป เพื่อที่ธุรกิจต่าง ๆ จะได้ไม่ต้องวุ่นวายกับระเบียบที่แตกต่างกันในแต่ละประเทศ และเพื่อเพิ่มความมั่นใจให้กับผู้บริโภคและมีวิธีที่ปฏิบัติได้จริงให้กับธุรกิจ”

กรรมาธิการยุติธรรมได้เสนอว่า ข้อบังคับเรื่องการแจ้งเตือนว่าข้อมูลรั่วไหลดังกล่าว ควรจะขยายไปให้ครอบคลุมกิจกรรมอย่าง ธนาคารออนไลน์ เกมออนไลน์ การซื้อสินค้า และสื่อสังคม รวมถึง Big Data ด้วย เพราะเจ้าของข้อมูลควรจะได้รับทราบว่ามีคนกำลังเข้าถึงข้อมูลของพวกเขา

โดยผิดกฎหมาย และผู้ให้บริการเครือข่ายสังคมที่มีผู้ใช้มากกว่า 200 ล้านคนในสหภาพยุโรป จะต้องทำตามกฎหมายของสหภาพยุโรป แม้ว่ามันจะดำเนินกิจการในสหรัฐอเมริกา[43]

เมื่อเดือนมกราคม ค.ศ. 2012[44] คณะกรรมาธิการยุโรป (European Commission) ได้เสนอร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับใหม่ โดยมีประเด็นสำคัญคือ ให้สิทธิบุคคลในการร้องขอให้องค์กรต่าง ๆ โดยเฉพาะอย่างยิ่ง บริษัทอินเทอร์เน็ต ลบข้อมูลเกี่ยวกับตัวเองออก หรือเรียกกันว่าเป็น “Right to be Forgotten” ตามร่างกฎหมายนี้ องค์กรจะต้องทำตามคำร้องขอลบข้อมูล หากว่าไม่มีเหตุผลอันสมควร (Legitimate Ground) ที่จะต้องเก็บข้อมูลนั้นไว้

ตามที่คณะกรรมาธิการยุโรปจะทำการปรับปรุงกฎหมายคุ้มครองข้อมูลส่วนบุคคล (Data Protection Directive) ซึ่งใช้บังคับมาตั้งแต่ปี พ.ศ. 2538 (ค.ศ. 1995) โดยจะทำการหารือผู้มีส่วนได้เสียทั้งหมดแล้วนำความเห็นมาประกอบการยกร่างแก้ไขปรับปรุงกฎหมายเพื่อเสนอต่อคณะมนตรียุโรปและรัฐสภายุโรปต่อไปนั้น เมื่อวันที่ 25 มกราคม พ.ศ. 2555 คณะกรรมาธิการยุโรปด้านการยุติธรรมได้เสนอการปรับปรุงแก้ไขกฎหมายคุ้มครองข้อมูลต่อคณะมนตรีและรัฐสภายุโรปโดยให้เหตุผลความจำเป็นและข้อเสนอในการปรับปรุงกฎหมายในสาระสำคัญดังนี้ [45]

เหตุผลความจำเป็น

1) การปรับปรุง Data Protection Directive ของประเทศสมาชิก (โดยการออกเป็นกฎหมาย หรือพระราชบัญญัติภายในประเทศ) ตั้งแต่ พ.ศ. 2538 เป็นต้นมา มีความแตกต่างกันทั้งในรายละเอียดและแนวทางปฏิบัติ ทำให้การคุ้มครองข้อมูลส่วนบุคคลในแต่ละประเทศสมาชิกมีระดับที่ไม่เท่าเทียมกัน และทำให้เกิดภาระค่าใช้จ่ายสูงสำหรับภาคธุรกิจในการปฏิบัติตามกฎระเบียบของแต่ละประเทศสมาชิกและกลายเป็นอุปสรรคทางการค้าสำหรับ SMEs ทั้งนี้หากบริษัทไม่สามารถปฏิบัติตามกฎระเบียบได้อย่างถูกต้อง ก็จะทำให้บริษัทขาดความเชื่อถือจากลูกค้าและส่งผลกระทบต่อการดำเนินธุรกิจทั้งในระยะสั้นและระยะยาว

---

[43] Reding, V., **Securing personal data and fighting breaches** [Online], 23 October 2009. Available from https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/PressNews/Events/09-10-23_Speech_Reding_EN.pdf.

[44] Reding, V., & Newman, M., **EU data protection law proposals include large fines** [Online], 25 January 2012. Available from http://www.bbc.com/news/ technology-16722229.

[45] European Commission, **Propasal for a Regulation of the European Parliament and of the Council: on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)** [Online], 25 January 2012. Available from http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

2) เทคโนโลยีด้านคอมพิวเตอร์และอินเทอร์เน็ตได้พัฒนาไปไกล โดยเฉพาะการเชื่อมโยงและจัดเก็บข้อมูลผ่าน Social Networking Sites และระบบ Cloud Computing ทำให้ระบบการคุ้มครองข้อมูลส่วนบุคคลตาม Data Protection Directive ล้าสมัยและไม่สามารถตอบสนองความต้องการของผู้ใช้งานในปัจจุบัน

3) บทบัญญัติภายใต้กฎหมายเดิมยังขาดความชัดเจน และไม่ให้ความคุ้มครองแก่เจ้าของข้อมูลอย่างเพียงพอ ทำให้ผู้ใช้งานอินเตอร์เน็ตขาดความมั่นใจในการให้บริการแบบออนไลน์ต่าง ๆ ซึ่งส่งผลกระทบต่อการเติบโตของเศรษฐกิจในยุคดิจิทัลและการมุ่งสู่การเป็น Single Market ของสหภาพยุโรป

ข้อเสนอปรับปรุงกฎหมาย

1) ด้านรูปแบบ

ปรับกฎระเบียบให้เป็นรูปแบบเดียวกันทั้งสหภาพยุโรป โดยการเปลี่ยนกฎหมายจากรูปแบบ Directive ซึ่งเป็นเพียงแนวทางให้แต่ละประเทศสมาชิกนำไปออกกฎหมายภายในประเทศ เป็น Regulations ซึ่งมีผลใช้บังคับโดยตรงเสมือนหนึ่งเป็นกฎหมายภายในของแต่ละประเทศสมาชิก ทำให้ทุกประเทศสมาชิกมีรูปแบบกระบวนการทางปกครองสำหรับการควบคุมและตรวจสอบที่เหมือนกัน ซึ่งจะช่วยลดภาระค่าใช้จ่ายของบริษัทต่าง ๆ ในการปฏิบัติตามกฎหมาย โดยคาดว่าจะประหยัดค่าใช้จ่ายได้ถึง 2.3 พันล้านยูโรต่อปี และลดขั้นตอนทางราชการลง ซึ่งจะช่วยประหยัดค่าใช้จ่ายได้ถึง 130 ล้านยูโรต่อปี

2) ด้านเนื้อหา

เพิ่มสิทธิในการลบข้อมูลทั้งหมด (Right to be Forgotten) ให้แก่ เจ้าของข้อมูล เปลี่ยนหลักการจัดเก็บและประมวลผลข้อมูลเป็นให้กระทำได้ต่อเมื่อได้รับการยินยอมอย่างชัดแจ้งจากเจ้าของข้อมูลเท่านั้น เพิ่มหน้าที่และความรับผิดชอบให้แก่ผู้จัดเก็บและประมวลผลข้อมูล เช่น บังคับให้ผู้จัดเก็บข้อมูลต้องแจ้งการละเมิดหรือการถูกขโมยข้อมูลให้เจ้าของข้อมูลทราบภายใน 24 ชั่วโมง เป็นต้น ให้สิทธิแก่เจ้าของข้อมูลในการนำคดีทุกประเภทไปดำเนินการยังหน่วยงานคุ้มครองข้อมูลในประเทศที่ตนอาศัยอยู่แม้ว่าการประมวลผลจะเกิดขึ้นนอกประเทศตนก็ตาม เพิ่มความชัดเจนว่ากฎระเบียบใหม่นี้จะใช้บังคับแก่บริษัทในประเทศที่สามที่ให้บริการจัดเก็บหรือประมวลผลข้อมูลของเจ้าของข้อมูลที่อยู่ในสหภาพฯ และจะลดข้อยุ่งยากของกฎระเบียบเกี่ยวกับการส่งข้อมูลไปยังประเทศที่สาม

3) ด้านกลไกการประสานงานแบบใหม่และการบังคับใช้กฎหมายที่เข้มงวดขึ้น

กำหนดให้ใช้ระบบ “One-Stop-Shop” โดยให้แต่ละประเทศสมาชิกมี Data Protection Authority (DPA) เพียงหนึ่งหน่วยงานเพื่อเป็นศูนย์กลางติดต่อประสานงานกับประชาชนและภาคธุรกิจ และให้บริษัทที่มีลูกจ้างมากกว่า 250 คนหรือที่ทำธุรกิจเกี่ยวข้องกับการจัดเก็บประมวลผล

ข้อมูลส่วนบุคคลจะต้องมี Data Protection Officer ทำหน้าที่ดูแลเรื่องนี้โดยเฉพาะ ส่วนขั้นตอนการให้ความเห็นชอบแก่ Binding Corporate Rules (ซึ่งบริษัทมักใช้เป็นระเบียบภายในบริษัทสำหรับการส่งข้อมูลให้แก่บริษัทในเครือหรือคู่ค้าที่ตั้งอยู่ในประเทศที่สาม) ก็จะดำเนินการโดย DPA ในประเทศที่บริษัทนั้นมีสำนักงานใหญ่ตั้งอยู่เพียงครั้งเดียว และการให้ความเห็นชอบนั้นจะมีผลครอบคลุมทั้งสหภาพฯ นอกจากนี้ ได้กำหนดเพิ่มค่าปรับแก่บริษัทที่ไม่ ปฏิบัติตามกฎระเบียบให้สูงถึง 1 ล้านยูโร หรือร้อยละ 2 ของรายได้ (ต่อปี) จากการดำเนินงานทั่วโลก

และเมื่อวันที่ 7 กุมภาพันธ์ พ.ศ. 2554[46] องค์กร Think Tank ใน Belgium ชื่อ Friends of Europe ได้จัดสัมมนาเรื่อง Europe's Data Protection Future: Prospects and Implications for Business เพื่อแลกเปลี่ยนความเห็นเกี่ยวกับข้อเสนอของคณะกรรมาธิการฯ ว่าด้วยการปรับปรุงกฎหมายคุ้มครองข้อมูลส่วนบุคคล (Data Protection Directive) โดยสหภาพยุโรปกำลังปรับ EU Directive เป็นกฎหมายในรูปแบบ Regulation เรียกว่า EU General Data Protection Regulation[47] ซึ่งกฎระเบียบใหม่นี้ให้อำนาจแก่สหภาพยุโรปมากเกินไป อีกทั้งยังเป็นการนำระบบใหม่เข้ามาใช้ในขณะที่การปฏิบัติตามกฎหมายเดิมยังดำเนินการไม่ครบทุกประเทศสมาชิก จึงเกรงว่าอาจจะก่อให้เกิดความสับสนแก่ภาคธุรกิจและประชาชนมากกว่าผลดี นอกจากนี้ กฎระเบียบใหม่ยังไม่สอดคล้องกับเทคโนโลยีอินเทอร์เน็ต และระบบ Cloud Computing ในปัจจุบัน ปัญหาความไม่สอดคล้องเหล่านี้จะแสดงผลอย่างชัดเจนเมื่อมีการออก Delegated Act ในภายภาคหน้า เพราะจะเกี่ยวกับการปฏิบัติ ควบคุม และตรวจสอบของหน่วยงาน DPA ในรายละเอียด ในการนี้ ได้ตั้งข้อสังเกตว่ากฎระเบียบใหม่นี้จะใช้บังคับกับบริษัทขนาดใหญ่ซึ่งเป็นเจ้าของระบบ Cloud Computing ที่ตั้งอยู่นอกสหภาพยุโรปได้อย่างไร[48]

การปรับกฎระเบียบใหม่ให้อยู่ในรูป Regulations น่าจะส่งผลดีในแง่ความชัดเจนและแน่นอนในทางกฎหมาย อันจะช่วยลดภาระค่าใช้จ่ายของภาคธุรกิจซึ่งเป็นสิ่งจำเป็นในภาวะวิกฤตเศรษฐกิจปัจจุบัน แต่ความท้าทายที่สำคัญคือ จะทำอย่างไรให้ประชาชนตระหนักและทราบถึงสิทธิในการคุ้มครองข้อมูลของตนเอง และทำอย่างไรให้ภาคธุรกิจมีแนวปฏิบัติที่เป็นไปในทิศทางเดียวกัน

---

[46] **Europe's Data Protection Future: Prospects and Implications for Business** [Online], 7 February 2012. Available from http://www.cloudlegal.ccls.qmul.ac.uk/News/2012/96607.html.

[47] European Commission, **Regulation of the European Parliament and of Council** [Online], 25 January 2012. Available from http://ec.europa.eu/justice/data-protection/document/review2012 / com_2012_11_en.pdf.

[48] Millard, C., **Europe's Data Protection Future: Prospects and Implications for Business** [Online], 7 February 2011. Available from http://www2.thaieurope.net-europes-data-protection-future-prospects-and-implications-for-business/.

ซึ่งในประการหลังนี้ อาจส่งเสริมให้ ภาคธุรกิจแลกเปลี่ยนแนวปฏิบัติที่ดีที่สุดระหว่างกัน ทั้งนี้ ในภาพรวมรัฐสภาฯ เห็นประโยชน์ของข้อเสนอของคณะกรรมาธิการฯ และเรียกร้องให้ทุกฝ่ายให้ความร่วมมือเพื่อให้การดำเนินการบรรลุผลสัมฤทธิ์ตามเป้าหมาย[49]

การมีกฎระเบียบ เดียวกันทั่วทั้งสหภาพฯ ย่อมเป็นประโยชน์แก่ SMEs อย่างเห็นได้ชัด เพราะจะช่วยให้ SMEs เหล่านี้สามารถนำเวลาและเงินทุนที่ต้องใช้ในการปฏิบัติตามกฎระเบียบของประเทศต่าง ๆ ไปใช้ในการวิจัยและพัฒนาแทนได้ ส่งผลให้มีขีดความสามารถเพิ่มขึ้น อย่างไรก็ตาม ยังไม่แน่ใจว่าการปฏิบัติตามกฎระเบียบใหม่จะมีความยุ่งยากสลับซับซ้อนหรือมีค่าใช้จ่ายสูงเหมือนเดิมหรือไม่ในทางปฏิบัติ เพราะสหภาพฯ มักมองว่าเทคโนโลยีใหม่ ๆ เป็นภัยคุกคามต่อสิทธิขั้นพื้นฐานของประชาชน จึงทำให้ออกกฎระเบียบในเชิงควบคุมและตรวจสอบ ในขณะที่สหรัฐฯ มองว่าเทคโนโลยีใหม่ ๆ เป็นโอกาสในทางธุรกิจของภาคเอกชน ทำให้สหรัฐฯ มีกฎระเบียบที่เอื้ออำนวยต่อการพัฒนาธุรกิจมากกว่า[50]

การเสนอแก้ไขปรับปรุงกฎหมายครั้งนี้เป็นการดำเนินการตามที่สนธิสัญญาลิสบอนกำหนดและให้อำนาจไว้ โดยยึดหลักการคุ้มครองสิทธิขั้นพื้นฐานของประชาชนสหภาพฯ เป็นฐานในการดำเนินงาน และที่ผ่านมาได้มีการหารือกับผู้มีส่วนได้เสียแล้วอย่างรอบคอบ ตลอดจนได้หารือกับประเทศที่มีบทบาทสำคัญในด้านการพัฒนากฎหมายและเทคโนโลยีที่เกี่ยวข้องด้วย เช่น สหรัฐอเมริกา เป็นต้น จึงมีความมั่นใจว่ากฎระเบียบใหม่นี้จะช่วยให้สิทธิของประชาชนได้รับการคุ้มครองที่ดีขึ้น[51]

3.3 ข้อตกลงระหว่างประเทศที่เกี่ยวข้องกับ Big Data

เนื่องจากข้อมูลเป็นพื้นฐานในการพัฒนาเศรษฐกิจ การได้มาซึ่งข้อมูลโดยเสรีเป็นปัจจัยสำคัญสำหรับเศรษฐกิจ ซึ่งในปัจจุบันนี้การติดต่อสัมพันธ์ทางเศรษฐกิจไม่ได้จำกัดอยู่เฉพาะในประเทศของตนและกลายเป็นความสัมพันธ์ระหว่างประเทศ ทุกประเทศในโลกไม่สามารถจะหลีกเลี่ยงการทำ

---

[49] Papadopoulou, A., **Europe's Data Protection Future: Prospects and Implications for Business** [Online], 7 February 2011. Available from http://www2.thaieurope.net-europes-data-protection-future-prospects-and-implications-for-business/.

[50] Polad, G., **Europe's Data Protection Future: Prospects and Implications for Business** [Online], 7 February 2011. Available from http://www2.thaieurope.net-europes-data-protection-future-prospects-and-implications-for-business/.

[51] Selmayr, M., **Europe's Data Protection Future: Prospects and Implications for Business** [Online], 7 February 2011. Available from http://www2.thaieurope.net-europes-data-protection-future-prospects-and-implications-for-business/.

การค้ากับต่างประเทศ หรือประเทศในภูมิภาคเดียวกัน การมีกฎหมายที่สอดคล้องกันเพื่อไม่ให้เป็นอุปสรรคในการดำเนินการทางการค้าระหว่างประเทศเป็นเรื่องที่มีความจำเป็นมาก เช่น การไหลเวียนของข้อมูลโดยการส่งสัญญาณดาวเทียม และเครือข่ายการสื่อสารแบบไร้สาย ซึ่งอยู่นอกเหนือข้อจำกัดทางเขตแดนของประเทศ แต่รัฐสามารถระงับการติดต่อสื่อสารที่มีการใช้ข้อมูลข่าวสารเกี่ยวกับบุคคลไปใช้ในทางที่ผิดได้

กรอบในการคุ้มครองข้อมูลส่วนบุคคลที่นิยมของสากลประเทศและประเทศไทยสามารถใช้นำมาอ้างอิงเป็นแนวทางในการคุ้มครองข้อมูลใน Big Data ที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ ซึ่งข้อมูลส่วนบุคคลใน Big Data นั้น ต้องได้รับการคุ้มครองที่เหมาะสมในทุกขั้นตอนตั้งแต่การเก็บรวบรวม การเก็บรักษา และการเปิดเผย คือ

1) กรอบในการคุ้มครองข้อมูลขององค์การร่วมมือและพัฒนาทางเศรษฐกิจ (OECD: The Organization for Economic Cooperation and Development)

2) ข้อกำหนดว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลแห่งสหภาพยุโรป (The European Union Data Protection Directive)

3) กรอบการคุ้มครองข้อมูลส่วนบุคคลในการประชุมความร่วมมือทางเศรษฐกิจในภูมิภาคเอเชีย-แปซิฟิก (APEC)

3.3.1 กรอบในการคุ้มครองข้อมูลส่วนบุคคลขององค์การร่วมมือและพัฒนาทางเศรษฐกิจ (OECD: The Organization for Economic Cooperation and Development)[52]

OECD เป็นเวทีแลกเปลี่ยนข้อคิดเห็นระหว่างประเทศสมาชิกเกี่ยวกับการจัดการปัญหาต่าง ๆ ในยุคโลกาภิวัฒน์บนพื้นฐานของการศึกษาวิจัยอย่างรอบคอบและเป็นกลาง เพื่อนำไปสู่ข้อสรุปร่วมระดับนโยบายในลักษณะ Guidelines for Best Practices และการปรับเปลี่ยนนโยบายภายในประเทศสมาชิกให้สอดคล้องกับ Guidelines เหล่านั้นในที่สุด

กระบวนการหารือและแลกเปลี่ยนความคิดเห็นในหมู่ประเทศสมาชิก ใช้หลัก Peer Review/ Peer Pressure ซึ่งเน้นการโน้มน้าวด้วยเหตุผลทางวิชาการ ประกอบกับการแลกเปลี่ยนความคิดเห็นและการเรียนรู้จากประสบการณ์ของประเทศอื่น ๆ ทั้งที่เป็นสมาชิกและมิใช่สมาชิก โดยไม่มีบทลงโทษประเทศสมาชิกที่ไม่ปฏิบัติตาม Guidelines แต่จะเน้นย้ำว่าการปฏิบัติตาม Guidelines จะเป็นประโยชน์ต่อการพัฒนาของสมาชิกเอง OECD มีบทบาทที่สร้างสรรค์ในการ Influence ความคิดเชิงนโยบายของกลุ่มประเทศสมาชิก และโดยที่ OECD เล็งเห็นแนวโน้มพลวัตรและความเสี่ยงต่อความไม่มั่นคงทางเศรษฐกิจและสังคม (Vulnerabilities to Systemic Risks) ที่

---

[52] สำนักงานคณะกรรมการทางอิเล็กทรอนิกส์, **การคุ้มครองข้อมูลส่วนบุคคล (Data Privacy)** [Online], 2557. แหล่งที่มา http://www.etcommission.go.th/files/article/article-dp.pdf.

เกิดจากปรากฏการณ์โลกาภิวัฒน์ จึงจัดกิจกรรมการประชุมและกำหนดหัวข้อการศึกษาวิจัยที่มีความสำคัญ ตรงประเด็น (Relevant) และทันสมัย[53]

แนวทางดังกล่าวได้เกิดขึ้นในปี ค.ศ.1980 (พ.ศ. 2523) ซึ่งมีการวางหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลขึ้นอย่างเป็นรูปธรรม และเป็นหลักเกณฑ์ที่ประเทศส่วนใหญ่ให้การยอมรับ คือ Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder flows of Personal Data โดย OECD (Organization for Economic Cooperation and Development) ภายใต้ Guidelines ฉบับนี้ได้กลายเป็นที่ยอมรับกันโดยทั่วไปว่าเป็นหลักเกณฑ์พื้นฐานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่สำคัญ ประเทศส่วนใหญ่ในโลกต่างรับและนำไปบัญญัติเป็นกฎหมายภายในของตน แนวทางที่สามารถนำมาประยุกต์ใช้กับการคุ้มครองข้อมูลใน Big Data นั้น กล่าวคือ

แนวทางเรื่อง Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data มีหลักการพื้นฐาน 8 ประการ ดังนี้

1) หลักข้อจำกัดในการเก็บรวบรวมข้อมูล (Collection Limitation Principle) ในการเก็บรวบรวมข้อมูลนั้น ต้องชอบด้วยกฎหมายและต้องใช้วิธีการที่เป็นธรรมและเหมาะสมโดยในการเก็บรวบรวมข้อมูลนั้นต้องให้เจ้าของข้อมูลรู้เห็น รับรู้ หรือได้รับความยินยอมจากเจ้าของข้อมูล

2) หลักคุณภาพของข้อมูล (Data Quality Principle) ข้อมูลที่เก็บรวบรวมนั้น ต้องเกี่ยวข้องกับวัตถุประสงค์ที่กำหนดขึ้นว่า “จะนำไปใช้ทำอะไร” และเป็นไปตามอำนาจหน้าที่และวัตถุประสงค์ในการดำเนินงานของหน่วยงานตามที่กฎหมายกำหนด นอกจากนั้นข้อมูลดังกล่าวจะต้องถูกต้อง สมบูรณ์ หรือทำให้เป็นปัจจุบันหรือทันสมัยอยู่เสมอ

3) หลักการกำหนดวัตถุประสงค์ในการจัดเก็บ (Purpose Specification Principle) ต้องกำหนดวัตถุประสงค์ว่า ข้อมูลที่มีการเก็บรวบรวมนั้น เก็บรวมรวมไปเพื่ออะไร พร้อมทั้งกำหนดระยะเวลาที่เก็บรวบรวมหรือรักษาข้อมูลนั้น ตลอดจนกรณีที่จำเป็นต้องมีการเปลี่ยนแปลงวัตถุประสงค์ในการเก็บรวบรวมข้อมูลเช่นว่านั้น ไว้ให้ชัดเจน

4) หลักข้อจำกัดในการนำไปใช้ข้อมูลส่วนบุคคล (Use Limitation Principle) นั้น จะต้องไม่มีการเปิดเผยทำให้มี หรือปรากฏในลักษณะอื่นใด ซึ่งไม่ได้กำหนดไว้โดยชัดแจ้งในวัตถุประสงค์ของการเก็บรวบรวมข้อมูล เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูล หรือโดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย

---

[53] กรมเศรษฐกิจระหว่างประเทศ, **ความรู้เกี่ยวกับ OECD** [Online], 2556. แหล่งที่มา http://www.mfa.go.th/.

5) หลักการรักษาความมั่นคงปลอดภัยข้อมูล (Security Safeguards) จะต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม เพื่อป้องกันความเสี่ยงภัยใด ๆ ที่อาจจะทำให้ข้อมูลนั้นสูญหาย เข้าถึง ทำลาย ใช้ ดัดแปลงแก้ไข หรือ เปิดเผยโดยมิชอบ

6) หลักการเปิดเผยข้อมูล (Openness Principle) ควรมีการประกาศนโยบายให้ทราบโดยทั่วกัน หากมีการปรับปรุงแก้ไข หรือพัฒนาแนวนโยบายหรือแนวปฏิบัติที่เกี่ยวกับข้อมูลส่วนบุคคล ก็ควรเปิดเผยหรือประกาศไว้ให้ชัดเจน รวมทั้งให้ข้อมูลใด ๆ ที่สามารถระบุเกี่ยวกับหน่วยงานของรัฐผู้ให้บริการที่อยู่ผู้ควบคุมข้อมูลส่วนบุคคลด้วย

7) หลักการมีส่วนร่วมของบุคคล (Individual Participation Principle) ให้บุคคลซึ่งเป็นเจ้าของข้อมูลได้รับแจ้งหรือยืนยันจากหน่วยงานของรัฐที่เก็บรวบรวมหรือจัดเก็บข้อมูลทราบว่า “หน่วยงานของรัฐนั้น ๆ ได้รวบรวมข้อมูลหรือจัดเก็บข้อมูลส่วนบุคคลดังกล่าวหรือไม่ ภายในระยะเวลาที่เหมาะสม”

8) หลักความรับผิดชอบ (Accountability Principle) ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

แนวทางดังกล่าวนี้สามารถป้องกันปัญหาการละเมิดสิทธิความเป็นอยู่ส่วนตัว และความมั่นคงปลอดภัยของข้อมูลใน Big Data ได้ ซึ่งเป็นแนวทางที่จะคุ้มครอง Big Data ให้มีประสิทธิภาพมากยิ่งขึ้น และลดความเสียหายที่จะเกิดขึ้นต่อประเทศไทยได้อีกด้วย

3.3.2 การคุ้มครองสิทธิในชีวิตส่วนตัวตามกรอบอนุสัญญาแห่งยุโรปว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐาน[54]

สิทธิในชีวิตส่วนตัว (Droit à la vie privée) เป็นสิทธิมนุษยชนประการหนึ่ง (Un droitde l’homme) ที่ได้รับการรับรองและคุ้มครองไว้อย่างชัดแจ้งในปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Déclaration Universelle des Droits de l’Homme) ลงวันที่ 10 ธันวาคม 1948 โดยกำหนดไว้ในข้อ 12 ความว่า “บุคคลใดจะถูกแทรกแซงตามอำเภอใจในชีวิตส่วนตัว ครอบครัว ที่อยู่อาศัย หรือการสื่อสารหรือจะถูกลบหลู่เกียรติยศและชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองของกฎหมายต่อการแทรกแซงสิทธิหรือการลบหลู่ดังกล่าวนั้น”[55] นอกจากนี้ สิทธิในชีวิตส่วนตัวยังได้รับ

---

[54] สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ, **ปัญหาและมาตรการทางกฎหมายในการรับรอง และคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว (Right to privacy)** [Online], 2012. แหล่งที่มา www.nhrc.or.th/2012/wb/img_contentpage.../511_file_name_4667.pdf.

[55] Article 12 Déclaration Universelle des Droits de l’Homme du 10 décembre 1948, J.O. 19 février 1949 « Nul ne sera l’objet d’immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d’atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.

การรับรองและคุ้มครองไว้ในอนุสัญญาแห่งยุโรปว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐาน (Convention Européenne de Sauvegarde des Droits de l'Homme et des Libertés Fondamentales)[56] อีกด้วย ซึ่งรวมถึงสิทธิความเป็นส่วนตัวในกรณี Big Data ด้วย โดยกำหนดไว้ในข้อ 8 ความว่า "1) บุคคลทุกคนมีสิทธิได้รับการเคารพในชีวิตส่วนตัวและครอบครัว ที่อยู่อาศัยและการสื่อสาร 2) การแทรกแซงการใช้สิทธิในชีวิตส่วนตัวของบุคคลโดยองค์กรของรัฐจะกระทำได้ก็เฉพาะแต่เมื่อมีกฎหมายบัญญัติให้กระทาได้ และการแทรกแซงดังกล่าว เป็นมาตรการที่จำเป็นในสังคมประชาธิปไตยต่อความปลอดภัยแห่งชาติ ความมั่นคงของรัฐ ประโยชน์ทางเศรษฐกิจของประเทศ การรักษาความสงบเรียบร้อยและการป้องกันการกระทำความผิดทางอาญา การคุ้มครองสุขภาพหรือจิตใจ หรือการคุ้มครองสิทธิและเสรีภาพของบุคคลอื่น"[57] (1) Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. 2) Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.)

3.3.2.1 สิทธิในชีวิตส่วนตัวอันเกี่ยวกับข้อมูลส่วนบุคคล (Droit au respect de la vie privée)

สิทธิในชีวิตส่วนตัว ได้แก่ สิทธิที่บุคคลทุกคนจะได้รับการเคารพจากองค์กรของรัฐและบุคคลทั้งหลายในอันที่จะไม่เข้าไปสืบสวน เก็บบันทึก หรือเปิดเผยเกี่ยวกับชีวิตส่วนตัวซึ่งเป็นความลับในชีวิตส่วนตัวของตน อันเป็นการแทรกแซงหรือละเมิดสิทธิในชีวิตส่วนตัว โดยนัยเช่นนี้การคุ้มครองสิทธิในชีวิตส่วนตัวของบุคคลจึงเป็นการคุ้มครองในแง่ความลับเกี่ยวกับชีวิตส่วนตัว เช่น ข้อมูลเกี่ยวกับประวัติวัยเยาว์ของบุคคลคนหนึ่ง ข้อมูลเกี่ยวกับประวัติการกระทำความผิดทางอาญาและภาพถ่าย ตลอดจนลายพิมพ์นิ้วมือ (des empreintes digitales) ของบุคคลคนหนึ่ง ชีวิตส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล (les données à caractère personnel) ชีวิตส่วนตัวอันเกี่ยวกับรสนิยมทางเพศหรือความเป็นตัวตนในเรื่องเพศ (une identité sexuelle) สิทธิในชีวิตส่วนตัวของบุคคลยังได้รับการคุ้มครองในแง่ของเสรีภาพเกี่ยวกับชีวิตส่วนตัวอีกด้วย ศาลแห่งยุโรปด้านสิทธิมนุษยชนได้

[56] Signée le, 4 novembre 1950 et entrée en vigueur le, 3 septembre 1953.

[57] Article 8 Convention Européenne de la Sauvegarde des Droits de l'Homme et des Libertés fondamentales.

เคยอธิบายไว้ในคดีหนึ่งว่า “...สิทธิที่จะได้รับการเคารพในชีวิตส่วนตัวยังรวมถึงสิทธิที่จะก่อความสัมพันธ์กับมนุษย์คนอื่น โดยเฉพาะในเรื่องที่เกี่ยวกับความรู้สึกเสน่หา เพื่อพัฒนาและตอบสนองความเป็นตัวตนของบุคคลนั้นด้วย”[58] สิทธิในชีวิตส่วนตัวที่จะได้รับการคุ้มครองในแง่นี้ ได้แก่ เสรีภาพในการมีความสัมพันธ์กับบุคคลอื่น ซึ่งครอบคลุมไปถึงเสรีภาพในการมีความสัมพันธ์ทางเพศ (les relations sexuelles) กับบุคคลอื่นทั้งเสรีภาพในความสัมพันธ์ทางเพศระหว่างชายและหญิง (la liberté des relations sexuelles entre les deux sexes) และเสรีภาพในความสัมพันธ์ทางเพศระหว่างชายรักร่วมเพศ (la liberté des relations sexuelles entre homme) ซึ่งสิทธิในชีวิตส่วนตัวดังกล่าว รวมถึงสิทธิความเป็นส่วนตัวในกรณี Big Data ด้วย

3.3.2.2 ข้อกำหนดว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลแห่งสหภาพยุโรป (The European Union Data Protection Directive)

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[59]

ข้อตกลงนี้เป็นการให้ความคุ้มครองความเป็นส่วนตัวในข้อมูลส่วนบุคคล ซึ่งสามารถนำไปประยุกต์ใช้กับการคุ้มครองข้อมูลใน Big Data ได้ รวมทั้งการโอนถ่ายข้อมูลส่วนบุคคล ข้อตกลงนี้ถูกจัดทำขึ้นเพื่อสร้างหลักประกันในเรื่องความเป็นส่วนตัวของข้อมูลส่วนบุคคลใน Big Data ภายใต้วัตถุประสงค์เพื่อให้การถ่ายโอนข้อมูลส่วนบุคคลภายในรัฐสมาชิกของสหภาพยุโรปสามารถทำได้โดยอิสระ และสร้างความเป็นมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลของรัฐสมาชิกให้มีมาตรฐานเดียวกัน

โดยที่ขอบเขตของข้อตกลงนี้จะใช้บังคับกับการประมวลผลข้อมูลส่วนบุคคลทั้งการประมวลผลโดยอัตโนมัติและการประมวลผลโดยวิธีการ Manual สำหรับการประมวลผลโดยวิธีการ Manual นั้น ข้อมูลที่ถูกประมวลผลโดยวิธีนี้จะต้องเป็นส่วนหนึ่งหรือมีเจตนาที่จะให้เป็นส่วนหนึ่งของระบบการจัดเก็บข้อมูล (Filing System เช่น ระบบการจัดเก็บข้อมูลทางการเงินของธนาคาร เป็นต้น) อย่างไรก็ตาม กฎหมายไม่ได้บังคับกับการประมวลผลข้อมูลโดยบุคคลธรรมดา ทั้งนี้ สาระสำคัญของข้อตกลงนี้มีดังต่อไปนี้

---

[58] Req. n° 6825/74, X. c/l’Islande, Décision de la Commission du 18 mai 1976, Ann., 1976, p. 343. Le droit au respect de la vie privée « comprend...dans une certaine mesure, le droit d’établir et de développer des liens avec d’autres êtres humains, notamment dans le domaine affectif, pour développer et épanouir sa propre personnalité ».

[59] ธนัท สุวรรณปริญญา, **ปัญหาทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์** (การศึกษาค้นคว้าอิสระ นิติศาสตรมหาบัณฑิต บัณฑิตวิทยาลัย มหาวิทยากรุงเทพ, 2550), 37.

1) ข้อมูลที่กฎหมายคุ้มครอง

ข้อมูลที่ได้รับความคุ้มครองตามข้อตกลงนี้ ก็คือ ข้อมูลส่วนบุคคล ซึ่งตามข้อตกลงนี้ คำว่า “ข้อมูลส่วนบุคคล” หรือ “Personal Data” หมายถึง ข้อมูลข่าวสารใด ๆ ที่สามารถระบุตัวหรืออาจระบุตัวบุคคลนั้นได้ ซึ่งบุคคลที่อาจระบุตัวได้ไม่ว่าโดยตรงหรือโดยอ้อมนี้ อาจทำได้โดยการอ้างอิงจากหมายเลขเฉพาะตัวของบุคคล หรือจากปัจจัยอื่น ๆ ที่มีลักษณะเฉพาะทางร่างกาย จิตใจ ฐานะทางเศรษฐกิจเอกลักษณ์ทางวัฒนธรรม และสภาพสังคมของบุคคลนั้น เป็นต้น

2) กระบวนการหรือการดำเนินการที่กฎหมายควบคุม

กระบวนการหรือการดำเนินการที่กฎหมายควบคุมตามข้อตกลงนี้ คือ การประมวลผลข้อมูล (Processing) ซึ่งหมายความว่า การดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล ไม่ว่าโดยวิธีการอัตโนมัติ หรือวิธีการอื่นใด เช่น การเก็บรวบรวม การบันทึกการจัดเรียบเรียง การเก็บรักษา การแก้ไขเปลี่ยนแปลง การส่งผ่าน การใช้ การเปิดเผย การเผยแพร่ หรือโดยวิธีการ
อื่น ๆ ที่ทำให้เข้าถึงข้อมูลได้

3) บุคคลที่ถูกกฎหมายควบคุม

เมื่อพิจารณาจากบทนิยามของข้อตกลงดังกล่าวจะเห็นได้ว่า บุคคลที่ถูกควบคุม คือ ผู้ควบคุมข้อมูล (Controller) และผู้ประมวลผลข้อมูล (Processor) โดยที่ผู้ควบคุมข้อมูล หมายความว่า บุคคลธรรมดาหรือนิติบุคคล เจ้าหน้าที่รัฐหน่วยงานหรือองค์กรอื่นใด ที่ทำหน้าที่ควบคุมข้อมูลส่วนบุคคลโดยลำพังหรือร่วมกับผู้อื่นในการกำหนดวัตถุประสงค์ และวิธีการในการประมวลผลข้อมูลส่วนบุคคลในกรณีที่วัตถุประสงค์ และวิธีการของการประมวลผลถูกกำหนดโดยกฎหมายหรือข้อบังคับของรัฐสมาชิกหรือโดยสหภาพยุโรป ส่วนผู้ประมวลผลข้อมูลคือบุคคลธรรมดาหรือนิติบุคคล เจ้าหน้าที่รัฐหน่วยงานหรือองค์กรอื่นใดซึ่งประมวลผลข้อมูลส่วนบุคคลแทนผู้ควบคุมข้อมูล

4) หน้าที่ของบุคคลที่ถูกควบคุม

ข้อตกลงนี้กำหนดให้ผู้ควบคุมข้อมูลมีหน้าที่ต้องแจ้งก่อนที่จะทำการประมวลผลข้อมูลส่วนบุคคลด้วยวิธีการอัตโนมัติ โดยในการแจ้งนั้นต้องประกอบด้วยรายการข้อมูลดังนี้

(1) ชื่อที่อยู่ของผู้ควบคุมข้อมูลและผู้แทน (ถ้ามี)

(2) วัตถุประสงค์ของการประมวลผล

(3) ประเภทของข้อมูลที่เก็บ

(4) ผู้รับข้อมูล

(5) วัตถุประสงค์ของการส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ

(6) ข้อมูลเบื้องต้นเกี่ยวกับมาตรการที่ใช้เพื่อรักษาความมั่นคงปลอดภัยในการประมวลผลข้อมูล

ทั้งนี้ก่อนการประมวลผลข้อมูล ข้อตกลงนี้กำหนดว่าการประมวลผลข้อมูลส่วนบุคคลต้องกระทำโดยชอบด้วยกฎหมาย ซึ่งการประมวลผลเช่นใดถึงจะเรียกว่าชอบด้วยกฎหมายนั้น ข้อตกลงนี้ได้กำหนดไว้ 7 กรณีดังนี้

(1) ได้รับความยินยอมจากเจ้าของข้อมูล

(2) เป็นกรณีจำเป็นเพื่อปฏิบัติตามสัญญาหรือเป็นการดำเนินการก่อนเข้าทำสัญญา

(3) ตามที่กฎหมายกำหนด

(4) เพื่อรักษาชีวิตของเจ้าของข้อมูล

(5) เพื่อปฏิบัติภารกิจที่ผลประโยชน์ของสาธารณะ

(6) เป็นการจำเป็นต่อการปฏิบัติหน้าที่ของของเจ้าพนักงาน

(7) เพื่อประโยชน์ที่ชอบด้วยกฎหมายของผู้ควบคุมข้อมูลหรือบุคคลที่สาม และการประมวลผลดังกล่าวไม่เป็นการประทบกระเทือนต่อประโยชน์ของการคุ้มครองสิทธิขั้นพื้นฐานของเจ้าของข้อมูลโดยเฉพาะสิทธิในความเป็นส่วนตัว

5) หลักการทั่วไปเกี่ยวกับการประมวลผลข้อมูล

ข้อตกลงนี้กำหนดว่าประเทศสมาชิกต้องปฏิบัติการต่อไปนี้ในการดำเนินการต่อข้อมูลส่วนบุคคล Big Data อันได้แก่

(1) ข้อมูลส่วนบุคคลต้องถูกประมวลผลอย่างเป็นธรรมและชอบด้วยกฎหมาย

(2) ข้อมูลส่วนบุคคลต้องถูกจัดเก็บโดยมีวัตถุประสงค์ที่ชัดเจน แน่นอน และชอบด้วยกฎหมาย (Specified, Explicit, and Legitimate Purpose) นอกจากนี้จะต้องไม่มีการประมวลผลข้อมูลที่ขัดแย้งกับวัตถุประสงค์นั้น เว้นแต่การประมวลผลข้อมูลที่มีวัตถุประสงค์ทางด้านประวัติศาสตร์ สถิติ หรือวิทยาศาสตร์

(3) ข้อมูลส่วนบุคคลต้องมีความเพียงพอ (Adequate) ไม่มากเกินจำเป็น (Not Excessive) และสอดคล้องกับวัตถุประสงค์ในการจัดเก็บ หรือประมวลผลข้อมูลนั้น

(4) ข้อมูลส่วนบุคคลต้องมีความถูกต้องครบถ้วน และกรณีจำเป็นต้องเป็นปัจจุบันด้วย

(5) ไม่ควรเก็บไว้ในรูปแบบที่สามารถระบุตัวบุคคลผู้เป็นเจ้าของข้อมูลไว้นานเกินไป อีกทั้งต้องใช้มาตรการที่เหมาะสมในการรักษาความมั่นคงปลอดภัยของข้อมูล

นอกจากนี้ตามข้อตกลงได้กำหนดให้ข้อมูลที่มีความอ่อนไหว (Sensitive Data) ซึ่งกฎหมายกำหนดให้เป็นหน้าที่ของผู้ควบคุมการประมวลผลข้อมูลส่วนบุคคลที่ต้องใช้มาตรการทางเทคนิคและการจัดการที่เหมาะสมเพื่อคุ้มครองข้อครองข้อมูลส่วนบุคคลจาก

(1) การทำลายข้อมูลโดยอุบัติเหตุหรือโดยมิชอบด้วยกฎหมาย

(2) การสูญเสียข้อมูลโดยอุบัติเหตุ

(3) การแก้ไขเปลี่ยนแปลงโดยอุบัติเหตุ

(4) การเปิดเผยหรือการเข้าถึงโดยปราศจากอำนาจ และ

(5) ป้องกันการประมวลผลที่มิชอบด้วยกฎหมายทุกรูปแบบ

การพิจารณาถึงความเหมาะสมที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคลนั้นต้องพิจารณาถึงความเสี่ยงที่เกิดขึ้นจากการประมวลผล และลักษณะของข้อมูลที่ทำการประมวลผล

โดยสรุปข้อกำหนดของ EU ได้กำหนดให้รัฐสมาชิกอนุญาตให้มีการประมวลผลข้อมูลส่วนบุคคลภายใต้หลักทั่วไป ดังนี้

(1) ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล

(2) การประมวลผลจะทำให้เท่าที่จำเป็นในการทำนิติกรรมสัญญาใด ๆ ของผู้เป็นเจ้าของข้อมูลเท่านั้น

(3) การประมวลผลจะต้องอยู่ภายใต้กรอบของกฎหมาย

(4) การประมวลผลจะต้องกระทำเพื่อปกป้องผลประโยชน์สำคัญของผู้เป็นเจ้าของข้อมูล

(5) การประมวลผลจำเป็นที่จะต้องกระทำเพื่อผลประโยชน์ของสาธารณะหรือในการดำเนินงานของหน่วยงานของรัฐที่ได้รับมอบหมายให้เป็นผู้ควบคุมข้อมูล หรือเปิดเผยข้อมูลต่อบุคคลที่สาม

(6) การประมวลผลที่จำเป็นและอยู่ภายใต้กรอบของกฎหมายจะต้องไม่กระทบต่อผลประโยชน์ หรือสิทธิขั้นพื้นฐานของผู้เป็นเจ้าของข้อมูล

นอกจากนี้ ข้อตกลงนี้ยังได้ให้ความสำคัญเกี่ยวกับความลับ ความเป็นส่วนตัว และความมั่นคงปลอดภัยของข้อมูล รวมถึงข้อยกเว้นในการเปิดเผยข้อมูลกรณีที่ไม่ได้นำข้อมูลไปใช้ประโยชน์สาธารณะ แต่นำไปใช้เพื่อประโยชน์ส่วนตัว และกำหนดเกี่ยวกับเรื่องความเสียหายที่เกิดขึ้นต่อข้อมูล เมื่อมีการประมวลผลโดยไม่ชอบด้วยกฎหมาย และการเปิดเผยข้อมูลจะต้องไม่ละเมิดต่อความมั่นคงของรัฐ

(6) การส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ

ข้อตกลงนี้ห้ามมิให้มีการส่งหรือโอนข้อมูลส่วนบุคคล เพื่อประมวลผลหรือเจตนาที่จะประมวลผลไปยังต่างประเทศที่มิได้เป็นสมาชิกสหภาพยุโรป เว้นแต่ประเทศที่รับข้อมูลจะมีระดับการคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอ อย่างไรก็ตาม ข้อตกลงนี้ก็ได้กำหนดข้อยกเว้นไว้ เช่น ในกรณีที่ได้รับความยินยอมจากเจ้าของข้อมูลโดยชัดแจ้ง หรือการส่งหรือโอนข้อมูลส่วนบุคคลจำเป็นเพื่อปฏิบัติตามสัญญาที่เจ้าของข้อมูลและผู้ควบคุมข้อมูลมีอยู่ระหว่างกัน หรือเพื่อปฏิบัติการให้เป็นไปตามข้อตกลงก่อนเข้าทำสัญญาตามคำร้องขอของเจ้าของข้อมูล

ในกรณีที่ผู้ประกอบการภายในสหภาพยุโรปต้องการโอนข้อมูลส่วนบุคคลที่ได้รับมาจากผู้บริโภคไปยังผู้ประกอบการ E-commerce ในประเทศสหรัฐอเมริกาได้นั้น การโอนถ่ายข้อมูลจะต้องอยู่ภายใต้ข้อตกลงที่เรียกว่า Safe Harbor ซึ่งเป็นการทำความตกลงระหว่างสหภาพยุโรปและประเทศสหรัฐอเมริกา ซึ่งผู้ประกอบการภายในประเทศสหรัฐอเมริกาที่จะได้รับอนุญาตให้สามารถรับโอนข้อมูลจากผู้ประกอบการภายในสหภาพยุโรปได้นั้น ผู้ประกอบการภายในประเทศสหรัฐอเมริกาจะต้องปฏิบัติตามเงื่อนไขที่กำหนดตาม Safe Harbor Principles และมีรายชื่ออยู่ใน Safe Harbor List ที่จะปรากฏทางทะเบียนของกระทรวงพาณิชย์ของสหรัฐเมริกาก่อน

(7) สิทธิของเจ้าของข้อมูล ข้อตกลงนี้ได้ให้สิทธิของเจ้าของข้อมูลดังนี้

(1) สิทธิที่จะได้รับข้อมูลตามที่กฎหมายกำหนดเมื่อถูกเก็บรวบรวมข้อมูล

(2) สิทธิเข้าถึงข้อมูลส่วนบุคคลของตน

(3) สิทธิที่จะแก้ไขข้อมูลส่วนบุคคลของตนให้ถูกต้อง

(8) องค์การที่ทำหน้าที่ควบคุมและบังคับการให้เป็นไปตามกฎหมาย

ข้อตกลงนี้วางแนวทางให้ประเทศสมาชิกสหภาพยุโรป กำหนดให้มีองค์กรที่ทำหน้าที่ควบคุมดูแลให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่มีความเป็นอิสระไว้ในกฎหมายคุ้มครองของแต่ละประเทศ ซึ่งประเทศสมาชิกส่วนใหญ่ก็จะกำหนดไว้ในรูปของ Commissioner ซึ่งตามข้อตกลงนี้กำหนดให้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสมาชิกอย่างน้อยต้องกำหนดอำนาจหน้าที่ดังต่อไปนี้ให้กับบุคคลหรือองค์กรที่ทำหน้าที่ควบคุมดูแลให้เป็นไปตามกฎหมาย คือ

(1) อำนาจในการสืบสวน เช่น อำนาจในการเข้าถึงและเก็บรวบรวมข้อมูลที่จำเป็นต่อการปฏิบัติหน้าที่ของผู้ควบคุมดูแล

(2) อำนาจในการแทรกแซง เช่น อำนาจในการออกคำสั่งขัดขวาง ลบ หรือทำลายข้อมูล หรือการห้ามการประมวลผลข้อมูลชั่วคราว

(3) รับคำร้องทุกข์เกี่ยวกับการดำเนินการที่เป็นการฝ่าฝืนกฎหมายคุ้มครองข้อมูลส่วนบุคคลและวินิจฉัยคำร้องทุกข์ดังกล่าว

(4) จัดทำรายงานการปฏิบัติงานและเผยแพร่รายงานดังกล่าวต่อสาธารณะ ข้อตกลงนี้ใช้กับกระบวนการทางอิเล็กทรอนิกส์ทุกขั้นตอนนับตั้งแต่ การเก็บ รวบรวม การเก็บรักษา การเปิดเผยข้อมูลส่วนบุคคล โดยที่ข้อตกลงนี้ให้สิทธิแก่บุคคลเหนือข้อมูลส่วนบุคคลของตน และข้อตกลงนี้ได้กำหนดหน้าที่ให้ผู้ควบคุมดูแลข้อมูลมีหน้าที่ต้องรักษาข้อมูลส่วนบุคคล ตามมาตรฐานที่กำหนดในข้อตกลงนี้ โดยรัฐสมาชิกของสหภาพยุโรป สามารถกำหนดได้ว่า ข้อมูลประเภทใดบ้างที่จะต้องดำเนินการภายใต้ตามข้อตกลงนี้ ซึ่งสามารถนำไปประยุกต์ใช้กับข้อมูลใน Big Data ได้ โดยผู้ควบคุมดูแลข้อมูลต้องดำเนินการดังต่อไปนี้

– ผู้ประกอบการหรือผู้ควบคุมดูแลข้อมูลส่วนบุคคลจะต้องรวบรวมและจัดเก็บข้อมูลส่วนบุคคลอย่างเป็นธรรมและถูกต้องตามกฎหมายเท่านั้น

– การเก็บรวบรวมและการดำเนินการจะต้องมีวัตถุประสงค์โดยเฉพาะเจาะจง ชัดแจ้ง และถูกต้องตามกฎหมาย มีความเหมาะสมและอยู่ภายใต้วัตถุประสงค์ที่เกี่ยวข้อง

– ข้อมูลส่วนบุคคลจะต้องมีความถูกต้องทันสมัย โดยต้องอนุญาตให้เจ้าของข้อมูลแก้ไขข้อมูลส่วนบุคคลของตนให้ถูกต้องได้

– ผู้ประกอบการหรือผู้ควบคุมดูแลข้อมูลส่วนบุคคลโดยจะนำข้อมูลส่วนบุคคลมาใช้ได้ต่อเมื่อได้รับความยินยอมอย่างชัดแจ้งจากผู้บริโภคสำหรับวัตถุประสงค์นั้น ๆ แล้ว การนำข้อมูลมาใช้ต้องมีเอกสารให้ความยินยอมที่ชัดแจ้ง เช่น ในสัญญา หรือในข้อตกลงต่าง ๆ

– ผู้ประกอบการหรือผู้ควบคุมดูแลข้อมูลส่วนบุคคลจะต้องมีการบอกกล่าวว่าข้อมูลจะถูกเก็บรักษาและถูกนำไปใช้อย่างไร

– ผู้ประกอบการหรือผู้ควบคุมดูแลข้อมูลส่วนบุคคล จะต้องอนุญาตให้ผู้เป็นเจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะดูข้อมูลและแก้ไขหากมีความผิดพลาดได้

– ก่อนที่ข้อมูลจะถูกให้แก่บุคคลที่สาม ผู้ประกอบการหรือผู้ควบคุมดูแลข้อมูลส่วนบุคคลจะต้องได้รับความยินยอมจากเจ้าของข้อมูลนั้น และเจ้าของข้อมูลมีสิทธิที่จะไม่ให้ข้อมูลส่วนบุคคลนั้นก็ได้

– ในกรณีที่ข้อมูลส่วนบุคคลเป็นข้อมูลที่มีความอ่อนไหว การเก็บรวบรวมข้อมูล จะต้องเกี่ยวข้องกับวัตถุประสงค์ที่ระบุ และจะต้องมีกฎระเบียบเป็นพิเศษสำหรับข้อมูลที่อ่อนไหว เช่น ข้อมูลทางการแพทย์ การเงิน ศาสนา การเมือง

ข้อกำหนดและหลักการของการคุ้มครองสิทธิความเป็นส่วนตัว และข้อมูลส่วนบุคคลตามกรอบอนุสัญญาแห่งยุโรปตามที่ได้กล่าวข้างต้นนี้ สามารถนำมาประยุกต์ใช้กับข้อมูลใน Big Data ได้ โดยมีหลักการคุ้มครองในเรื่องความเป็นส่วนตัว และการรักษาความมั่นคงปลอดภัยของข้อมูลใน Big Data

3.3.3 กรอบการคุ้มครองข้อมูลส่วนบุคคลในการประชุมความร่วมมือทางเศรษฐกิจในภูมิภาคเอเชีย-แปซิฟิก (APEC) [60]

ความร่วมมือทางเศรษฐกิจเอเชีย-แปซิฟิก (APEC) (Asia-Pacific Economic Cooperation: APEC) ก่อตั้งขึ้นเมื่อปี พ.ศ. 2532 โดยมีจุดประสงค์มุ่งเน้นความเจริญเติบโตและการพัฒนาที่ยั่งยืนของภูมิภาค และผลักดันให้การเจรจาการค้าหลายฝ่าย รอบอุรุกวัยประสบผลสำเร็จ ขณะเดียวกัน APEC ก็ต้องการถ่วงดุลอำนาจทางเศรษฐกิจของกลุ่มเศรษฐกิจต่าง ๆ โดยเฉพาะกลุ่มสหภาพยุโรปอีกด้วย ปัจจุบัน APEC มีสมาชิกทั้งสิ้น 21 เขตเศรษฐกิจ (19 ประเทศ 2 เขตเศรษฐกิจ) ประกอบด้วยประเทศมหาอำนาจทางการเมืองและเศรษฐกิจที่สำคัญ คือ สหรัฐอเมริกา รัสเซียสาธารณรัฐประชาชนจีน และญี่ปุ่น รวมทั้งสมาชิกอาเซียน และประเทศในอเมริกาเหนือและใต้

APEC เป็นกลุ่มความร่วมมือทางเศรษฐกิจระหว่างเขตเศรษฐกิจในภูมิภาคเอเชีย-แปซิฟิก เป็นเวทีสำหรับการแลกเปลี่ยนข้อคิดเห็นเกี่ยวกับประเด็นทางเศรษฐกิจที่ประเทศสมาชิกสนใจการดำเนินงานยึดหลักฉันทามติ ความเท่าเทียมกัน และผลประโยชน์ร่วมกันของประเทศสมาชิก[61] ซึ่งได้กำหนดหลักเกณฑ์เกี่ยวกับข้อมูลส่วนบุคคล (APEC Information Privacy Principles) ซึ่งสามารถนำมาประยุกต์ใช้กับข้อมูลส่วนบุคคลใน Big Data ได้

APEC ได้จัดการประชุมเชิงปฏิบัติการฯ จัดขึ้นระหว่างวันที่ 12 – 13 สิงหาคม พ.ศ. 2551 เพื่อหารือและแลกเปลี่ยนประสบการณ์ด้านการคุ้มครองข้อมูลส่วนบุคคลระหว่างประเทศ เสริมสร้างความเข้าใจแก่สมาชิกในการนำ APEC Privacy Framework ไปปรับใช้ให้เหมาะสมกับแต่ละสมาชิกที่มีความแตกต่างกันด้านกฎระเบียบและวิธีการดำเนินงาน รวมทั้ง เพื่อส่งเสริมการขับเคลื่อนโครงการนำร่อง Data Privacy Pathfinder ในปี 2551 และการทดสอบโครงการฯ ในปี 2552

สมาชิกที่เข้าร่วมประชุมประกอบด้วยผู้แทนจากภาครัฐและเอกชน โดยประเด็นหลักในการหารือคือ การพัฒนาแผนการดำเนินโครงการย่อย 9 โครงการภายใต้โครงการนำร่อง Data Privacy Pathfinder และผลการดำเนินงานของสมาชิกที่เข้าร่วมโครงการนำร่องฯ ซึ่งสมาชิกได้ร่วมสรุปผลแนวทางการดำเนินงานของโครงการและแบบสอบถาม ซึ่งที่ประชุมฯ เห็นชอบให้เสนอเอกสารดังกล่าวเป็นผลผลิตหนึ่งภายใต้ตัวชี้วัดการดำเนินงานของคณะทำงานกลุ่มย่อยด้านการคุ้มครองข้อมูลส่วนบุคคล

---

[60] นคร เสรีรักษ์, **กรอบการคุ้มครองข้อมูลส่วนบุคคลของเอเปค** [Online], กันยายน 2550. แหล่งที่มา http://www.fpps.or.th/news.php?detail=n1240887531.news.

[61] กรมเจรจาการค้าระหว่างประเทศ, **บทบาทและภารกิจ** [Online], 9 กุมภาพันธ์ 2553. แหล่งที่มา http://www.dtn.go.th/dtn/aboutus/dtn_th.pdf.

โครงการย่อย 9 โครงการประกอบด้วย

1) CBPR Self-Assessment Guidance for Organizations

พัฒนามาตรฐานแนวทางการประเมินตนเอง (Self-Assessment) เพื่อช่วยให้ภาคธุรกิจนำแนวทางดังกล่าว ไปพัฒนาเป็นแนวทางในการคุ้มครองข้อมูลส่วนบุคคลข้ามพรมแดน (Cross-Border Privacy Rules (CBPRs)) ของตนเองได้

สร้างความตระหนักและการรับรู้ในหลักการคุ้มครองข้อมูลส่วนบุคคลภายใต้กรอบ APEC (APEC Privacy Principles) และการคุ้มครองบุคคลข้ามพรมแดน (CBPRs)

2) Guidelines for Trustmarks Participating in a CBPR System

องค์กรที่ออก Trustmark จะต้องพัฒนาแนวทางที่จะต้องปฏิบัติเพื่อให้เป็นที่ยอมรับในเรื่องของ CBPRs ภายใต้กรอบ APEC

3) Compliance Review of an Organization's CBPRs

พัฒนาแนวทางสำหรับองค์กรที่ออก Trustmark เพื่อใช้ในการประเมินภาคธุรกิจที่ต้องการนำหลักการคุ้มครองข้อมูลส่วนบุคคลภายใต้กรอบ APEC ไปใช้

4) Directory of Compliant Organizations

พัฒนาฐานข้อมูลรายชื่อของภาคธุรกิจที่มี CBPRs และได้รับการรับรองว่าได้ปฏิบัติตามหลักการคุ้มครองข้อมูลส่วนบุคคลภายใต้กรอบ APEC

5) Data Protection Authority and Privacy Contact Officer Directory

พัฒนาฐานข้อมูลที่เกี่ยวข้องกับอำนาจ หน้าที่ต่าง ๆ ที่เกี่ยวข้องในการคุ้มครองข้อมูล รายชื่อเจ้าหน้าที่ที่ดูแลในเรื่องการคุ้มครองข้อมูลส่วนบุคคลในเขตเศรษฐกิจภายใต้กรอบ APEC

6) Template Enforcement Cooperation Arrangements

พัฒนารูปแบบเอกสาร เช่น บันทึกความเข้าใจ (MOU) หรือ หนังสือผูกพัน (Letter of Commitment) ซึ่งแสดงถึงข้อตกลงร่วมกันระหว่างหน่วยงานที่มีอำนาจในการแลกเปลี่ยนข้อมูล ส่งเสริมความร่วมมือระหว่างพรมแดนในการสอบสวน และบังคับใช้

7) Template Cross-border Complaint Handling Form

พัฒนาแบบฟอร์มรับเรื่องร้องเรียน ในรูปแบบเดียวกับแบบฟอร์มขอความช่วยเหลือของ OECD (OECD Request for Assistant Form) เพื่อสะดวก เป็นที่ยอมรับต่อการจัดการข้อร้องเรียนข้ามพรมแดน และพัฒนาความร่วมมือระหว่างหน่วยงานที่มีอำนาจในการแลกเปลี่ยน สอบสวน บังคับใช้ และให้ความช่วยเหลือในทางที่จำเป็นและเหมาะสม

8) Guidelines and Procedures for Responsive Regulation in a CBPR System

พัฒนาแนวทางและขั้นตอน (เช่น แผนผัง) ที่ช่วยในการพิจารณาว่า ขั้นตอนในการจัดการข้อร้องเรียนข้ามพรมแดนควรจะเป็นเช่นไร และควรจะดำเนินการอย่างไรเพื่อไปยังขั้นตอนถัดไป

9) CBPR International Implementation Pilot Project

พัฒนาและทดสอบโครงการนำร่องระหว่างเขตเศรษฐกิจที่สนใจเข้าร่วมทดสอบระบบ CBPR

การดำเนินโครงการนำร่องฯ มิได้บังคับให้สมาชิกจะต้องปฏิบัติทุกโครงการย่อย แต่สมาชิกสามารถเลือกดำเนินโครงการใด ก่อนหรือหลังได้ตามความสมัครใจ โดยพิจารณาจากความพร้อมและการดำเนินงานภายในเขตเศรษฐกิจเป็นหลัก ทั้งนี้ เป้าหมายหลักของการดำเนินโครงการนำร่องเพื่อให้สมาชิกได้ตื่นตัวและเริ่มดำเนินการอย่างจริงจัง ซึ่งความสำเร็จของโครงการนำร่อง มุ่งที่จำนวนสมาชิกที่เข้าร่วมฯ และการดำเนินงานที่เห็นผลเป็นรูปธรรมของสมาชิก

APEC ได้กำหนดหลักเกณฑ์เกี่ยวกับข้อมูลส่วนบุคคล (APEC Information Privacy Principles) ที่สามารถนำมาประยุกต์ใช้กับกรณีข้อมูลใน Big Data ซึ่งมีสาระสำคัญดังนี้

1) เพื่อเป็นการรักษาผลประโยชน์ของบุคคลในเรื่องสิทธิความเป็นส่วนตัว จึงต้องมีการกำหนดมาตรการการคุ้มครองข้อมูลส่วนบุคคลใน Big Data เพื่อป้องกันการใช้ข้อมูลโดยมิชอบ และป้องกันความเสียหายที่จะเกิดจากการใช้โดยมิชอบ ไม่ว่าจะเป็นการเก็บ การใช้ และการส่งต่อ

2) ต้องแจ้งเจ้าของข้อมูลอย่างชัดเจนว่าจะมีการเก็บข้อมูลส่วนบุคคล วัตถุประสงค์การเก็บ ประเภทบุคคลหรือองค์กรที่ข้อมูลส่วนบุคคลอาจได้รับการเปิดเผย ต้องแจ้งสิทธิของเจ้าของข้อมูล และมาตรการที่จะใช้ในการจำกัดการใช้ การเปิดเผย การเข้าถึง และการแก้ไข ทั้งนี้ต้องแจ้งก่อนหรือในขณะที่เก็บ หรือเร็วที่สุดหลังการจัดเก็บ

3) ต้องมีการจัดเก็บอย่างจำกัดเท่าที่เป็นไปตามวัตถุประสงค์ของการเก็บ การเก็บต้องทำโดยวิธีที่ถูกกฎหมาย และวิธีที่เป็นธรรมและเหมาะสม โดยได้แจ้งต่อและได้ขอคำยินยอมจากเจ้าของข้อมูลแล้ว

4) ข้อมูลที่เก็บไว้จะเอาไปใช้ได้เฉพาะตามวัตถุประสงค์ของการเก็บเท่านั้น เว้นแต่ได้รับคำยินยอมจากเจ้าของข้อมูลหรือเป็นไปตามข้อยกเว้นตามที่กฎหมายกำหนด

5) เจ้าของข้อมูลมีสิทธิเลือกว่าจะยินยอมให้มีการเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลของตน

6) ข้อมูลที่จัดเก็บต้องมีความถูกต้อง สมบูรณ์ เป็นปัจจุบัน ตามความจำเป็นและตามวัตถุประสงค์การเก็บ

7) มาตรการคุ้มครองข้อมูลอย่างเหมาะสมเพื่อป้องกันอันตรายที่อาจเกิด ไม่ว่าจะเป็นการสูญหาย เสียหาย การเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การทำลายโดยไม่ได้รับอนุญาต การใช้ปรับเปลี่ยน แก้ไข เปิดเผยโดยมิชอบ

8) เจ้าของข้อมูลมีสิทธิรับรู้ว่ามีการเก็บข้อมูลส่วนบุคคลของตนหรือไม่ และมีสิทธิเข้าถึงข้อมูลของตนเอง และมีสิทธิขอให้ตรวจสอบความถูกต้องและขอให้ปรับปรุง แก้ไข เพิ่มเติม หรือทำลายข้อมูลของตน

9) ผู้เก็บข้อมูลจะต้องรับผิดชอบการจัดมาตรการต่าง ๆ ให้เป็นไปตามหลักเกณฑ์ดังกล่าว การส่งข้อมูลส่วนบุคคลไปยังบุคคลหรือองค์การอื่น ๆ ไม่ว่าภายในประเทศหรือส่งไปยังต่างประเทศจะต้องได้รับคำยินยอมจากเจ้าของข้อมูล และจะต้องมีมาตรการที่เหมาะสมที่ประกันได้ว่าบุคคลหรือองค์กรที่ได้รับข้อมูลไปแล้วจะเก็บรักษาข้อมูลให้เป็นไปตามหลักเกณฑ์นี้

ข้อกำหนดและหลักการตามกรอบการคุ้มครองข้อมูลส่วนบุคคลในการประชุมความร่วมมือทางเศรษฐกิจในภูมิภาคเอเชีย-แปซิฟิก (APEC) ที่ได้กล่าวข้างต้นนี้ สามารถนำมาประยุกต์ใช้กับข้อมูลใน Big Data ได้ โดยมีหลักการคุ้มครองในเรื่องความเป็นส่วนตัว และการรักษาความมั่นคงปลอดภัยของข้อมูลใน Big Data

ตารางที่ 3.1: สรุปเปรียบเทียบเรื่องการคุ้มครองข้อมูลส่วนบุคคลของ OECD, EU และ APEC

กรอบ	หลักข้อจำกัดในการเก็บรวบรวมข้อมูล	หลักคุณภาพของข้อมูล	หลักการกำหนดวัตถุประสงค์ในการจัดเก็บ	หลักข้อจำกัดในการนำไปใช้	หลักการรักษาความมั่นคงปลอดภัยข้อมูล	หลักการเปิดเผยข้อมูล	หลักการมีส่วนร่วม	หลักความรับผิดชอบ
OECD	*ข้อมูลนั้นต้องชอบด้วยกฎหมาย *ต้องใช้วิธีการที่เป็นธรรมและเหมาะสม *ต้องให้เจ้าของข้อมูลรู้เห็น รับรู้ หรือได้รับความยินยอมจากเจ้าของข้อมูล	*ต้องเกี่ยวข้องกับวัตถุประสงค์ *ข้อมูลดังกล่าวจะต้องถูกต้องสมบูรณ์ ทันสมัย *เป็นไปตามอำนาจหน้าที่และวัตถุประสงค์ตามที่กฎหมายกำหนด	*เก็บรวมรวมไปเพื่ออะไร *กำหนดระยะเวลาที่เก็บรวบรวม/รักษาข้อมูล *กำหนดระยะเวลาที่จำเป็นต้องมีการเปลี่ยนแปลงวัตถุประสงค์	*จะต้องไม่มีการเปิดเผย ทำให้มีหรือปรากฏ ซึ่งไม่ได้กำหนดไว้โดยชัดแจ้งในวัตถุประสงค์ *เว้นแต่ได้รับค. ยินยอมจากเจ้าของข้อมูลหรือโดยอำนาจกฎหมาย	*ต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันความเสี่ยงภัยใดๆ ที่อาจทำให้ข้อมูลสูญหาย เข้าถึง ทำลาย ใช้ ดัดแปลงแก้ไข	ควรมีการประกาศนโยบายให้ทราบโดยทั่วกัน หากมีการปรับปรุงแก้ไขหรือพัฒนาแนวนโยบาย/แนวปฏิบัติก็ควรเปิดเผยหรือประกาศไว้ให้ชัดเจน	ให้เจ้าของข้อมูลได้รับแจ้งหรือยินยันจากหน่วยงานของรัฐที่จัดเก็บข้อมูล ทราบว่า "หน่วยงานของรัฐนั้นๆ ได้รวบรวม/จัดเก็บ ข้อมูลส่วนบุคคลดังกล่าวภายใน	ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล
EU	ข้อมูลส่วนบุคคลต้องถูกประมวลผลอย่างเป็นธรรมและชอบด้วยกฎหมาย	ต้องถูกจัดเก็บโดยมีวัตถุประสงค์ที่ชัดเจน แน่นอน ต้องเป็นปัจจุบัน			ให้ความสำคัญเกี่ยวกับความลับและความมั่นคงเมื่อมีการประมวลผลโดยไม่ชอบ จะต้องไม่ละเมิดต่อความมั่นคงของรัฐ		*สิทธิเข้าถึงข้อมูลส่วนบุคคลของตน *สิทธิที่จะแก้ไขข้อมูลส่วนบุคคลของตนให้ถูกต้อง	องค์การที่ทำหน้าที่ควบคุมและบังคับการให้เป็นไปตามกฎหมาย
APEC	การเก็บต้องทำโดยวิธีที่ถูกกฎหมาย และวิธีที่เป็นธรรมและเหมาะสม โดยได้แจ้งต่อและได้ขอคำยินยอมจากเจ้าของข้อมูลแล้ว	ข้อมูลที่จัดเก็บต้องมีความถูกต้อง สมบูรณ์ เป็นปัจจุบัน ตามความจำเป็นและตามวัตถุประสงค์การเก็บ	วัตถุประสงค์การเก็บ ประเภทบุคคลหรือองค์กรที่ข้อมูลส่วนบุคคลอาจได้รับการเปิดเผย	เอาไปใช้ได้เฉพาะตามวัตถุประสงค์ของการเก็บเท่านั้น เว้นแต่ได้รับคำยินยอมจากเจ้าของข้อมูลหรือเป็นไปตามข้อยกเว้นตามที่กฎหมายกำหนด	มาตรการคุ้มครองข้อมูลเพื่อป้องกันอันตรายไม่ว่าจะเป็นการสูญหาย-เสียหาย-การเข้าถึง/ทำลาย โดยไม่ได้รับอนุญาต การใช้-ปรับเปลี่ยนแก้ไข-เปิดเผยโดยมิชอบ		*เจ้าของข้อมูลมีสิทธิเลือกว่าจะยินยอมให้มีการเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลของตน *มีสิทธิเข้าถึง ตรวจสอบความถูก ต้อง ปรับปรุงแก้ ไข เพิ่มเติมทำ ลาย	ผู้เก็บข้อมูลจะต้องรับผิดชอบการจัดมาตรการตามหลักเกณฑ์การส่งข้อมูลไปยังองค์การอื่นๆ ไม่ว่าภายใน หรือต่างประเทศจะต้องได้รับคำยินยอมจากเจ้าของข้อมูล

บทที่ 4

วิเคราะห์เปรียบเทียบกฎหมายไทยและต่างประเทศ

ในบทนี้ผู้ศึกษาจะแบ่งการวิเคราะห์ออกเป็น 2 หัวข้อใหญ่ คือ วิเคราะห์การคุ้มครองข้อมูลใน Big Data ตามกฎหมายไทย ซึ่งประกอบไปด้วยกฎหมาย 5 ฉบับ ได้แก่ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 และ วิเคราะห์การคุ้มครองข้อมูลใน Big Data ตามกฎหมายต่างประเทศ ได้แก่ ประเทศสหรัฐอเมริกา และประเทศอังกฤษตามข้อกำหนดของสหภาพยุโรป ซึ่งประเด็นที่จะศึกษาคือ ความเป็นส่วนตัว และความมั่นคงปลอดภัยของข้อมูลใน Big Data โดยทำการศึกษา วิเคราะห์เปรียบเทียบว่ามีกฎหมาย กฎ กติกา แนวปฏิบัติ และองค์กรที่ทำการควบคุมหรือกำกับดูแลที่เกี่ยวข้องกับกรณี Big Data อยู่หรือไม่ อย่างไร โดยจะเน้นไปที่การวิเคราะห์บทบัญญัติแห่งกฎหมายไทยที่มีผลใช้บังคับอยู่ในขณะนี้ หรือที่กำลังจะมีผลบังคับใช้ ว่าสามารถนำมาประยุกต์ใช้กับการละเมิดสิทธิในความเป็นอยู่ส่วนตัว และความมั่นคงปลอดภัยของข้อมูลใน Big Data ได้หรือไม่

4.1 วิเคราะห์การคุ้มครอง Big Data ตามกฎหมายไทย

สำหรับประเทศไทยนั้น ในปัจจุบันมีกฎหมายอยู่หลายฉบับที่ให้หลักประกันต่อสิทธิในความเป็นอยู่ส่วนตัวอันหมายความรวมถึงข้อมูลส่วนบุคคล เช่น รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550 ประมวลกฎหมายแพ่งและพาณิชย์ ประมวลกฎหมายอาญา พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 นอกจากนี้ยังมีร่างกฎหมายอีกฉบับหนึ่งที่วางหลักการเพื่อคุ้มครองข้อมูลส่วนบุคคลสำหรับภาคเอกชนเป็นการทั่วไป โดยผู้ศึกษาจะวิเคราะห์ถึงการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว (Privacy) และการรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security) ในกรณีการคุ้มครองข้อมูลใน Big Data

4.1.1 วิเคราะห์การคุ้มครอง Big Data ตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

กรณีความเป็นส่วนตัว (Privacy) พบว่าพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มาตรา 23 มาตรา 24 และมาตรา 25 ได้บัญญัติไว้ถึงการคุ้มครองข้อมูลใน Big Data ด้านการเก็บรวบรวมข้อมูล ไม่ว่าจะเป็นเรื่องการเก็บรักษาความลับข้อมูล การยินยอมของผู้ให้ข้อมูล

การรับรู้ของผู้ให้ข้อมูลต่อการมีอยู่ของฐานข้อมูล หรือการรับรู้ของผู้ให้ข้อมูลต่อการใช้ฐานข้อมูล ปัญหาของระบบการจัดเก็บฐานข้อมูล ด้านความมั่นคงปลอดภัยของระบบการจัดเก็บฐานข้อมูล การเข้าไปในฐานข้อมูลโดยไม่ได้รับอนุญาต ปัญหาการใช้ฐานข้อมูลที่ไม่ถูกต้องหรือมีความผิดพลาด ความยินยอมของผู้ให้ข้อมูลต่อการใช้ข้อมูลดังกล่าว รวมถึงการรับรู้ของผู้ให้ข้อมูลต่อการใช้ข้อมูล แต่ก็ยังมีปัญหาการคุ้มครองข้อมูลใน Big Data อีกหลายด้านที่พระราชบัญญัติฉบับนี้ยังไม่ได้กล่าวไว้ เช่น ปัญหาในการส่งผ่านข้อมูล การเชื่อมโยงฐานข้อมูลที่ต่างกัน การรวมศูนย์และการวิเคราะห์ฐานข้อมูล และการส่งข้อมูลข้ามพรมแดน เป็นต้น ซึ่งหลักการที่สามารถนำมาประยุกต์ใช้กับกรณีข้อมูลใน Big Data ได้มีดังต่อไปนี้[1]

1) หลักการกำหนดวัตถุประสงค์ในการจัดเก็บ หน่วยงานของรัฐที่จัดเก็บข้อมูลต้องแจ้งให้เจ้าของข้อมูลทราบถึงวัตถุประสงค์ที่จะใช้ข้อมูลนั้น โดยต้องแจ้งให้ทราบอย่างน้อยในขณะที่จัดเก็บข้อมูลใน Big Data

2) หลักความยินยอม หน่วยงานของรัฐจะเปิดเผยข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความควบคุมดูแลของตนต่อหน่วยงานของรัฐแห่งอื่นหรือผู้อื่น โดยปราศจากความยินยอมเป็นหนังสือของเจ้าของข้อมูลที่ให้ไว้ล่วงหน้าหรือในขณะนั้นไม่ได้ เว้นแต่จะเข้าข้อยกเว้นตามที่กฎหมายกำหนด เช่น เป็นการเปิดเผยต่อเจ้าหน้าที่ของรัฐในหน่วยงานของตนเพื่อการนำไปใช้ตามอำนาจหน้าที่ของหน่วยงานของรัฐแห่งนั้น เป็นการใช้ข้อมูลตามปกติภายในวัตถุประสงค์ของการจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลนั้น เป็นการเปิดเผยต่อหน่วยงานของรัฐที่ทำงานด้วยการวางแผน หรือการสถิติหรือสำมะโนต่าง ๆ ซึ่งมีหน้าที่ต้องรักษาข้อมูลข่าวสารส่วนบุคคลใน Big Data ไว้ไม่ให้เปิดเผยต่อไปยังผู้อื่น เป็นการเปิดเผยต่อเจ้าหน้าที่ของรัฐ เพื่อการป้องกันการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย การสืบสวน การสอบสวน หรือการฟ้องคดี ไม่ว่าเป็นคดีประเภทใดก็ตาม เป็นต้น

3) หลักข้อจำกัดในการเก็บรวบรวมข้อมูลใน Big Data ข้อมูลส่วนบุคคลที่จัดเก็บจะต้องเกี่ยวข้อง และจำเป็นเพื่อการดำเนินงานของหน่วยงานของรัฐให้สำเร็จตามวัตถุประสงค์ของการจัดเก็บข้อมูลเท่านั้น

4) หลักข้อจำกัดในการนำไปใช้ หน่วยงานของรัฐจะต้องนำข้อมูลข่าวสารส่วนบุคคลไปใช้หรือเปิดเผยเฉพาะตามวัตถุประสงค์ที่กำหนดไว้ เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูล รวมทั้งข้อมูลส่วนบุคคลที่ได้นำไปใช้แล้วก็ต้องเก็บรักษาไว้ในเวลาเท่าที่จำเป็น หน่วยงานของรัฐต้องยกเลิกการจัดเก็บข้อมูลใน Big Data นั้นเมื่อหมดความจำเป็นแล้ว

---

[1] ชาญชัย แสวงศักดิ์, **สาระน่ารู้ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540**, (กรุงเทพฯ: วิญญูชน, 2540), 46-47.

5) หลักคุณภาพของข้อมูลใน Big Data หน่วยงานของรัฐต้องพยายามเก็บข้อมูลส่วนบุคคลโดยตรงจากเจ้าของข้อมูล โดยเฉพาะอย่างยิ่งในกรณีที่จะกระทบถึงประโยชน์ได้เสียโดยตรงของบุคคลนั้น นอกจากนี้ข้อมูลส่วนบุคคลที่จัดเก็บไว้โดยหน่วยงานของรัฐต้องถูกต้องและแก้ไขให้เป็นปัจจุบันอยู่ตลอดเวลา โดยเจ้าของข้อมูลมีสิทธิที่จะมีคำขอเป็นหนังสือให้แก้ไขหรือลบข้อมูลที่ไม่ถูกต้อง

6) หลักการมีระบบบริหารจัดการข้อมูลที่โปร่งใส หน่วยงานของรัฐต้องมีระบบบริหารจัดการข้อมูลส่วนบุคคลใน Big Data ที่โปร่งใสและสามารถตรวจสอบได้ โดยการจัดให้มีการพิมพ์เกี่ยวกับนโยบายและหลักเกณฑ์แนวปฏิบัติของระบบข้อมูลส่วนบุคคลของหน่วยงานของตนในเรื่องที่กฎหมายกำหนดในราชกิจจานุเบกษา เช่น ประเภทของบุคคลที่มีการเก็บข้อมูลไว้ ประเภทของระบบข้อมูลข่าวสารส่วนบุคคล ลักษณะการใช้ข้อมูลตามปกติ วิธีการขอตรวจดูข้อมูลข่าวสารของเจ้าของข้อมูล วิธีการขอให้แก้ไขเปลี่ยนแปลงข้อมูล และแหล่งที่มาของข้อมูล เป็นต้น

7) หลักการมีสิทธิเข้าถึงข้อมูลของตน เจ้าของข้อมูลมีสิทธิเข้าถึงข้อมูลใน Big Dataของตนเมื่อมีคำขอเป็นหนังสือ รวมทั้งยังมีสิทธิขอให้หน่วยงานของรัฐแก้ไข เปลี่ยนแปลง หรือลบข้อมูลส่วนบุคคลที่ไม่ถูกต้องตรงตามความเป็นจริงได้

8) หลักการมีสิทธิร้องเรียน ในกรณีที่หน่วยงานของรัฐไม่แก้ไขเปลี่ยนแปลงหรือลบข้อมูลส่วนบุคคลใน Big Data ให้ตรงตามที่มีคำขอของเจ้าของข้อมูล ให้เจ้าของมีสิทธิอุทธรณ์ต่อคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารภายใน 30 วัน นับแต่วันที่ได้รับแจ้งคำสั่งไม่ยินยอมแก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสารส่วนบุคคลใน Big Data

9) หลักการมีองค์กรกำกับดูแลการเปิดเผยข้อมูลใน Big Data กฎหมายได้กำหนดให้มีคณะกรรมการข้อมูลข่าวสารของทางราชการเป็นองค์กรที่กำกับดูแลการเปิดเผยข้อมูลตามกฎหมายฉบับนี้

กรณีความมั่นคงปลอดภัยของข้อมูล (Data Security) พระราชบัญญัติดังกล่าวได้กำหนดหลักการรักษาความมั่นคงปลอดภัยไว้ในมาตรา 23 วรรคแรก (5) ว่าหน่วยงานของรัฐต้องจัดให้มีวิธีการรักษาความมั่นคงปลอดภัยของข้อมูลใน Big Data ที่จัดเก็บ เพื่อป้องกันมิให้ข้อมูลถูกนำไปใช้โดยไม่เหมาะสมหรือเป็นผลร้ายต่อเจ้าของข้อมูล

กฎหมายข้อมูลข่าวสารของราชการของราชการนี้ ตอนร่างไม่ได้เน้นไปที่ข้อมูลข่าวสาร แต่เน้นไปที่ “ความครอบครอง” กล่าวคือ ข้อมูลข่าวสารใดอยู่ในความครอบครองของราชการ ข้อมูลข่าวสารนั้นเป็นข้อมูลข่าวสารของราชการ ซึ่งเป็นการมองในมิติของพื้นที่ มิใช่การมองในมิติของเนื้อหา ด้วยเหตุนี้จึงจำเป็นต้องมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลเพื่อที่จะกำหนดความคุ้มครองในส่วนของเอกชนจึงจะทำให้เกิดความสมบูรณ์ว่าข้อมูลส่วนบุคคลถูกบังคับในส่วนของราชการและในส่วนเอกชนเหมือนกัน ดังนั้น กฎหมายคุ้มครองข้อมูลส่วนบุคคลที่กำลังจะออกมานี้ก็จะไปกำกับ

ข้อมูลในภาคเอกชน แต่ไม่ว่าจะเป็นข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของภาครัฐหรือภาคเอกชน สาระจะต้องได้รับความคุ้มครองเหมือนกัน โดยมีหลักว่าข้อมูลส่วนบุคคลต้องได้รับความคุ้มครอง เว้นแต่จะมีข้อยกเว้นตามกฎหมาย

หากพิจารณาจากการคุ้มครองตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 พบว่า พระราชบัญญัตินี้มีวัตถุประสงค์เพื่อให้ประชาชนมีโอกาสรับรู้ข้อมูลข่าวสารเกี่ยวกับการดำเนินการต่าง ๆ ของรัฐ อันเป็นการเปิดเผยข้อมูลข่าวสารของราชการให้ประชาชนมีโอกาสได้รับรู้ โดยมีการกำหนดข้อยกเว้นในการเปิดเผยข้อมูลข่าวสารของราชการในบางกรณีเท่านั้น ส่วนประเด็นที่เกี่ยวข้องกับข้อมูลส่วนบุคคลตามกฎหมายฉบับนี้เป็นการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของรัฐ โดยการกำหนดหน้าที่ให้เจ้าหน้าที่ของรัฐต้องปฏิบัติตาม จึงสามารถนำมาประยุกต์ใช้กับกรณีความคุ้มครองความเป็นอยู่ส่วนตัว และความมั่นคงปลอดภัยของข้อมูลใน Big Data โดยภาครัฐได้ แต่ไม่สามารถนำมาปรับใช้กับความคุ้มครองความเป็นอยู่ส่วนตัวและความมั่นคงปลอดภัยของข้อมูลใน Big Data โดยภาคเอกชน

4.1.2 วิเคราะห์การคุ้มครอง Big Data ตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...

กรณีความเป็นส่วนตัว (Privacy) พบว่าร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... ได้บัญญัติไว้ครอบคลุมถึงปัญหาการคุ้มครองข้อมูลใน Big Data ด้านการเก็บรวบรวมข้อมูล ไม่ว่าจะเป็นเรื่องการเก็บรักษาความลับข้อมูล การยินยอมของผู้ให้ข้อมูล การรับรู้ของผู้ให้ข้อมูลต่อการมีอยู่ของฐานข้อมูล หรือการรับรู้ของผู้ให้ข้อมูลต่อการใช้ฐานข้อมูล ปัญหาของระบบการจัดเก็บฐานข้อมูล ด้านความมั่นคงปลอดภัยของระบบการจัดเก็บฐานข้อมูล การเข้าไปในฐานข้อมูลโดยไม่ได้รับอนุญาต ปัญหาการใช้ฐานข้อมูลที่ไม่ถูกต้องหรือมีความผิดพลาด ความยินยอมของผู้ให้ข้อมูลต่อการใช้ข้อมูลดังกล่าว การรับรู้ของผู้ให้ข้อมูลต่อการใช้ข้อมูล รวมถึงปัญหาในการส่งผ่านข้อมูล การเชื่อมโยงฐานข้อมูลที่ต่างกัน การรวมศูนย์และการวิเคราะห์ฐานข้อมูล และการส่งข้อมูลข้ามพรมแดน ซึ่งหลักการที่สามารถนำมาประยุกต์ใช้กับกรณี Big Data สรุปได้ตามดังต่อไปนี้

1) การกำหนดวัตถุประสงค์ในการจัดเก็บข้อมูลใน Big Data

กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลใน Big Data เพื่อวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือขณะที่รวบรวม ใช้ หรือเปิดเผย

2) ความยินยอม

กำหนดให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลใน Big Data จะต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่กรณีตามที่ได้กำหนดไว้ในกฎหมาย เช่น เป็นการปฏิบัติตามกฎหมาย เป็นไปเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคลและการขอความยินยอมไม่สามารถ

ดำเนินการได้ หรือเป็นไปเพื่อประโยชน์แก่การสอบสวนของพนักงานสอบสวนตามประมวนกฎหมายวิธีพิจารณาความอาญาหรือการพิจารณาพิพากษาคดีของศาล เป็นต้น

3) การเก็บรวบรวมข้อมูลส่วนบุคคลใน Big Data

กำหนดให้เก็บรวบรวมข้อมูลส่วนบุคคลได้เพียงเท่าที่เกี่ยวข้องและจำเป็นแก่การดำเนินกิจการตามวัตถุประสงค์ของผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น โดยห้ามเก็บรวบรวมข้อมูลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ข้อมูลทางพันธุกรรม ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนา ฯลฯ เว้นแต่ได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูล และเพื่อให้สอดคล้องกับหลักการในการให้ความคุ้มครองสิทธิในข้อมูลส่วนบุคคลของเจ้าของข้อมูล ร่างพระราชบัญญัติฉบับนี้ได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งต่อเจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดก่อนหรือในขณะเก็บรวบรวมข้อมูลใน Big Data

เมื่อได้ดำเนินการเก็บรวบรวมข้อมูลส่วนบุคคลแล้ว ร่างพระราชบัญญัติฉบับนี้ได้กำหนดให้นายทะเบียนจัดทำรายการจัดเก็บข้อมูล เพื่อให้เจ้าของข้อมูลสามารถตรวจสอบ อย่างไรก็ดีโดยที่กฎหมายเกี่ยวกับการพิมพ์จัดได้ว่าเป็นกฎหมายเฉพาะกฎหมายหนึ่ง ดังนั้นร่างพระราชบัญญัติฉบับนี้จึงกำหนดเป็นข้อยกเว้นมิให้ใช้บังคับ

4) การใช้และการเปิดเผยข้อมูลใน Big Data

กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องใช้ข้อมูลส่วนบุคคลที่อยู่ในความครอบครองดูแลตามวัตถุประสงค์ของการเก็บรวบรวมข้อมูลเท่านั้น การใช้นอกเหนือวัตถุประสงค์จะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อน อย่างไรก็ดีในกรณีที่มีเหตุจำเป็นที่มีผลกระทบต่อชีวิต ร่างกาย อนามัยของเจ้าของข้อมูลส่วนบุคคล ร่างพระราชบัญญัติฉบับนี้กำหนดเป็นข้อยกเว้นให้สามารถเปิดเผยข้อมูลส่วนบุคคลได้ในกรณีต่าง ๆ โดยการเปิดเผยจะต้องทำเท่าที่จำเป็น และเมื่อได้เปิดเผยแล้วให้แจ้งเจ้าของข้อมูลทราบ รวมทั้งผู้ซึ่งได้รับข้อมูลต้องใช้ข้อมูลตามวัตถุประสงค์เท่านั้น และผู้ควบคุมข้อมูลต้องบันทึกการเปิดเผยข้อมูลใน Big Data นั้นเพื่อการตรวจสอบด้วย

5) การเก็บรักษาข้อมูลส่วนบุคคลใน Big Data

กำหนดให้เก็บรักษาข้อมูลของเจ้าของข้อมูลส่วนบุคคลได้เท่าระยะเวลาที่กำหนด หรือเท่าที่จำเป็นตามวัตถุประสงค์ของการเก็บรวบรวมข้อมูล และเมื่อพ้นระยะเวลา หรือหมดความจำเป็น หรือเจ้าของข้อมูลเพิกถอนความยินยอม ผู้ควบคุมข้อมูลส่วนบุคคลต้องลบทำลายข้อมูลนั้นโดยเร็ว เว้นแต่ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีความจำเป็นต้องเก็บรักษาข้อมูลนั้นไว้เพื่อเป็นสถิติการศึกษาวิจัย ผู้ควบคุมข้อมูลส่วนบุคคลอาจไม่ลบทำลายข้อมูลนั้นก็ได้ แต่ต้องได้รับความยินยอมจากเจ้าของข้อมูล

6) การแก้ไขข้อมูลใน Big Data

กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่แก้ไขข้อมูลส่วนบุคคลให้ทันสมัยถูกต้องครบถ้วนตามที่เจ้าของข้อมูลร้องขอเป็นหนังสือ ในการแก้ไขเปลี่ยนแปลงนั้น ผู้ควบคุมข้อมูลส่วนบุคคลจะขอให้เจ้าของข้อมูลส่วนบุคคลจัดส่งเอกสาร หรือหลักฐานเพื่อใช้ในการเปลี่ยนแปลงก็ได้

7) การโอนข้อมูลส่วนบุคคลใน Big Data

กำหนดห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลโอนข้อมูลส่วนบุคคลที่อยู่ในความดูแลไปให้บุคคลอื่น เว้นแต่จะได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูล อย่างไรก็ดีในกรณีมีความจำเป็นเร่งด่วนซึ่งหากรอรับความยินยอมก่อนอาจเกิดความเสียหายแก่ส่วนรวม หรือชีวิตร่างกาย หรืออนามัยของบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลอาจส่งหรือโอนข้อมูลนั้นได้

นอกจากนี้ตามร่างพระราชบัญญัติยังมีบทบัญญัติในการห้ามส่งหรือโอนข้อมูลส่วนบุคคลไปนอกราชอาณาจักร โดยเฉพาะในประเทศที่ยังไม่มีบทบัญญัติของกฎหมายในการคุ้มครองข้อมูลส่วนบุคคล หรือมีแต่บทบัญญัติของกฎหมายนั้นมีมาตรฐานต่ำกว่าบทบัญญัติตามร่างพระราชบัญญัตินี้ เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

กรณีความมั่นคงปลอดภัยของข้อมูล (Data Security) พบว่าร่างพระราชบัญญัตินี้ได้กำหนดหลักความมั่นคงปลอดภัยของข้อมูลใน Big Data ไว้ใน มาตรา 17 ซึ่งกำหนดให้ผู้ควบคุมข้อมูลมีหน้าที่ดูแลรักษาความมั่นคงปลอดภัยมิให้ข้อมูลส่วนบุคคลสูญหาย ถูกแก้ไข หรือเปลี่ยนแปลง และมีหน้าที่ดูแลข้อมูลส่วนบุคคลที่ใช้หรือเปิดเผยให้มีความถูกต้อง ครบถ้วน และเป็นปัจจุบัน

ดังนั้นพิจารณาการคุ้มครองตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม ประวัติการทำงาน หรือประวัติกิจกรรม บรรดาที่มีชื่อของคุคลนั้นหรือมีเลขหมาย รหัส หรือสิ่งอื่นที่ทำให้รู้ตัวบุคคลนั้นได้เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคน หรือรูปถ่าย และให้หมายความรวมถึงข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของผู้ถึงที่ถึงแก่กรรมแล้วด้วย

รองศาสตราจารย์กิตติศักดิ์ ปรกติ ได้อธิบายความหมายของข้อมูลส่วนบุคคลไว้ว่า “ข้อมูลส่วนบุคคล หมายถึง ข้อมูลข่าวสารที่เป็นเรื่องส่วนตัวเท่านั้น แต่ถ้าเป็นเรื่องข้อมูลข่าวสารเกี่ยวกับบุคคลก็ไม่ถือว่าเป็นเรื่องส่วนตัว” ซึ่งส่วนนี้จะแตกต่างจากกฎหมายของประเทศอื่น ๆ ที่คุ้มครองข้อมูลส่วนบุคคล ที่ไม่ว่าจะเป็นข้อมูลอะไร หากระบุหรือบ่งบอกให้รู้ตัวบุคคลได้ก็เป็นสิ่งที่กฎหมายให้ความคุ้มครองทั้งสิ้น ดังนั้น เมื่อการคุ้มครองข้อมูลของไทยกำหนดว่าต้องเป็นเรื่องส่วนตัวหรือเฉพาะตัวที่บ่งบอกตัวบุคคลได้เท่านั้น ทำให้ขอบเขตของความคุ้มครองแคบลงทันที เช่น รสนิยมทางเพศ ประวัติการศึกษา แต่ไม่รวมถึงเรื่องที่เกี่ยวกับบุคคล เช่น ตำแหน่งหน้าที่การงาน เป็นต้น โดยได้อธิบายถึงความแตกต่างที่ชัดเจน ระหว่าง ข้อมูลข่าวสารที่เป็นเรื่องส่วนตัว กับ ข้อมูลข่าวสาร

เกี่ยวกับบุคคล ว่าถ้าเป็นเรื่องเกี่ยวกับบุคคลนั้นโดยทั่ว ๆ ไปแล้ว ถือว่าเป็นข้อมูลข่าวสารเกี่ยวกับบุคคล แต่ถ้าเป็นเรื่องเฉพาะตัวของบุคคลนั้นเท่านั้น ไม่เกี่ยวกับคนอื่น ๆ ถือเป็นข้อมูลข่าวสารที่เป็นเรื่องส่วนตัว

ยกตัวอย่างเช่น หมายเลขโทรศัพท์ ถ้าเป็นหมายเลขโทรศัพท์บนโต๊ะทำงาน ถือว่าไม่ใช่เรื่องส่วนตัวเพราะบุคคลทั่วไปสามารถทราบถึงเบอร์ดังกล่าวและสามารถโทรหาได้เสมอในเวลาทำงาน แต่ถ้าเป็นหมายเลขโทรศัพท์ส่วนตัว เช่น หมายเลขโทรศัพท์ในห้องนอน ถือเป็นเรื่องส่วนตัวเพราะเป็นเรื่องเฉพาะตัวที่จะนำมาเปิดเผยไม่ได้ ตัวอย่างอื่น ๆ เช่น ข้อมูลสถานที่ทำงาน สถานการศึกษา ตำแหน่งหน้าที่ ชื่อหัวหน้า ถือว่าไม่ใช่เรื่องส่วนตัว แต่ข้อมูลที่อยู่บ้านพักอาศัย ชื่อ หรือหมายเลขโทรศัพท์ของบุตรหรือคู่สมรส ตำหนิรอยแผลเป็น รสนิยมทางเพศ ทะเบียนประวัติอาชญากรรม ข้อมูลทะเบียนราษฎร์ ถือเป็นเรื่องส่วนตัว เป็นต้น

นอกจากนี้ พันตำรวจศิริพงษ์ ติมูลา รองผู้บังคับการกองบังคับการกรอบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี ได้แสดงความเห็นว่า “ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคล” ซึ่งแตกต่างจากคำว่า ข้อมูลบุคคล ดังนั้น จึงต้องทำความเข้าใจว่าข้อมูลใดบ้างที่เป็นสิ่งเฉพาะตัวของบุคคล อันได้แก่[2]

1) ข้อมูลที่ติดตัวมาตั้งแต่เกิด เช่น DNA คู่แฝด ลายนิ้วมือ เป็นต้น

2) ข้อมูลที่เกิดจากพฤติกรรม นิสัย หรือกิจกรรมที่ทำ ซึ่งตำรวจเรียกว่า แผนประทุษกรรมที่สามารถนำมาใช้วิเคราะห์เค้าโครงร่างอาชญากรรมได้

3) ข้อมูลที่เกิดจากสิ่งสมมุติ หรือบริบทที่เกี่ยวข้อง เช่น ข้อมูลรายการการใช้โทรศัพท์ การเช่าหนังสือ การใช้บัตรเครดิต เป็นต้น

4) ข้อมูลที่เป็นปฐมภูมิ เช่น หมายเลขบัญชีธนาคารหรือบัตรเครดิต รหัสประจำเครื่องโทรศัพท์ เป็นต้น

เนื่องจากการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายไทยนั้นแคบกว่ากฎหมายทั่วไป เพราะควบคุมไว้เฉพาะเรื่องส่วนตัวเท่านั้น แต่ความจริงแล้วเรื่องที่เกี่ยวข้องกับข้อมูลส่วนบุคคลก็สามารถนำไปใช้ได้โดยวิธีการทำ Data Matching ซึ่งผู้ประกอบการในทางพาณิชย์ อาชญากร หรือผู้ที่เกี่ยวข้องอาจจะเก็บรวบรวมข้อมูลนั้นเพื่อแสวงหาประโยชน์อย่างอื่นที่มิใช่ประโยชน์ในทางทรัพย์สินได้ เช่น การก่ออาชญากรรม ดังนั้น ถ้ากระบวนการตรวจสอบและควบคุมไม่ละเอียดและกว้างขวางเพียงพอก็จะทำให้เกิดช่องว่างในการแสวงหาประโยชน์อันมิควรได้โดยชอบอย่างกว้างขวางมากขึ้น

---

[2] เพลินตา ต้นรังสรรค์, **สรุปการสัมมนาทางวิชาการโครงการเสวนาให้ความเห็นต่อร่างกฎหมายเรื่องร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...** [Online], 2553. แหล่งที่มา http://www.senate.go.th/lawdatacenter/includes/FCKeditor/upload/Image/b/s36%20jun_7_5.pdf.

สำหรับการตีความคำว่า “ข้อมูลส่วนบุคคล” ใน Big Data ที่จะได้รับความคุ้มครองตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... นั้น สามารถตีความถึงกรณีที่ได้รับความคุ้มครองอยู่ 2 ประเภท คือ

1) กรณีที่ Big Data เป็นข้อมูลส่วนบุคคลโดยตรง

2) กรณีที่ Big Data ไม่ใช่ข้อมูลส่วนบุคคล เนื่องจากเป็นเพียงข้อมูลรายละเอียดต่าง ๆ แต่ข้อมูลดังกล่าวนั้นสามารถเชื่อมโยงไปยังข้อมูลอื่น ๆ ได้โดยอาศัยกระบวนการวิเคราะห์ Big Data จนประมวลผลออกมาแล้วสามารถกำหนดหรือระบุตัวบุคคลได้

ส่วนเรื่องประเด็นเรื่องหน่วยงานที่ควบคุม กำกับ ดูแลการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวกรณี Big Data นั้น หากพิจารณาตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... มาตรา 11 ได้กำหนดให้คณะกรรมการมีอำนาจหนาที่ ดังต่อไปนี้

1) กำหนดนโยบาย มาตรการ หรือแนวทางการดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเพื่อใหเปนไปตามพระราชบัญญัตินี้

2) เสนอความเห็นตอรัฐมนตรีเพื่อออกกฎกระทรวงตามพระราชบัญญัตินี้

3) เสนอแนะตอคณะรัฐมนตรีใหมีการตราหรือปรับปรุงแกไขกฎหมายที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

4) ให้คำแนะนำและคำปรึกษาเกี่ยวกับการดำเนินการใด ๆ ในการคุ้มครองข้อมูลส่วนบุคคลรวมทั้งส่งเสริมการพัฒนาเทคโนโลยีที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

5) กำหนดหลักเกณฑ์ในการไดรับเครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลรวมทั้งมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล

6) ออกระเบียบหรือประกาศเพื่อปฏิบัติการให้เป็นไปตามพระราชบัญญัตินี้

7) จัดทำรายงานเกี่ยวกับการปฏิบัติการตามพระราชบัญญัตินี้เสนอตอคณะรัฐมนตรีหรือรัฐสภาเป็นครั้งคราวตามความเหมาะสมอยางนอยปละหนึ่งครั้ง และใหประกาศรายงานดังกลาวในราชกิจจานุเบกษาดวย

8) แต่งตั้งคณะอนุกรรมการเพื่อดำเนินการใด ๆ ตามพระราชบัญญัตินี้

9) ปฏิบัติการอื่นใดตามที่พระราชบัญญัตินี้หรือกฎหมายอื่นกำหนดให้เป็นอำนาจหนาที่ของคณะกรรมการหรือตามที่รัฐมนตรีหรือคณะรัฐมนตรีมอบหมาย

4.1.3 วิเคราะห์การคุ้มครอง Big Data ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

กรณีความเป็นส่วนตัว (Privacy) และความมั่นคงปลอดภัยของข้อมูล (Data Security) พบว่าพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มีวัตถุประสงค์เพื่อรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ที่ใช้ในการทำธุรกรรมหรือสัญญา ให้มีผลเช่นเดียวกับการทำ

สัญญาตามหลักเกณฑ์ที่กฎหมายปัจจุบันกำหนดไว้ ได้แก่ การทำเป็นหนังสือ หลักฐานเป็นหนังสือ การลงลายมือชื่อ กล่าวคือถ้ามีการทำสัญญาระหว่างบุคคลที่ใช้ข้อมูลอิเล็กทรอนิกส์หรือลายมือชื่ออิเล็กทรอนิกส์ตามความหมายของกฎหมายแล้ว กฎหมายนี้ถือว่าการทำสัญญานั้นได้ทำตามหลักเกณฑ์ข้างต้นของกฎหมายแพ่งและพาณิชย์แล้ว เป็นผลทำให้สัญญานั้นมีผลสมบูรณ์หรือใช้บังคับได้ตามกฎหมาย

ในการวิเคราะห์ข้อมูลใน Big Data นั้น โดยทั่วไปใช้ระบบคอมพิวเตอร์ซึ่งถือว่าเป็นระบบอิเล็กทรอนิกส์ เพื่อประมวลผล และวิเคราะห์ข้อมูลต่าง ๆ ดังนั้นจึงมีความจำเป็นต้องนำพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาพิจารณาประกอบด้วยว่าสามารถปรับใช้กับบริบทของการคุ้มครองข้อมูลส่วนบุคคลใน Big Data ซึ่งผู้ศึกษาได้พิจารณาแล้วเห็นว่าการวิเคราะห์ข้อมูลใน Big Data ที่อาจเป็นความผิดตามพระราชบัญญัติฉบับนี้ คือการละเมิดต่อข้อมูลส่วนบุคคลซึ่งได้ให้ความหมายของข้อมูลอิเล็กทรอนิกส์ไว้ว่า “ข้อมูลอิเล็กทรอนิกส์ หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร” ซึ่งจากการศึกษาพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ผู้ศึกษาเห็นว่าพระราชบัญญัตินี้ได้กำหนดการรองรับสถานะทางกฎหมายของข้อมูลทางอิเล็กทรอนิกส์ให้เสมอกับการทำเป็นหนังสือ หรือหลักฐานเป็นหนังสือ การรับรองวิธีการส่งและรับข้อมูลอิเล็กทรอนิกส์ การใช้ลายมือชื่ออิเล็กทรอนิกส์ ตลอดจนการรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ เพื่อเป็นการส่งเสริมการทำธุรกรรมทางอิเล็กทรอนิกส์ให้น่าเชื่อถือ และมีผลในทางกฎหมายเช่นเดียวกับการทำธุรกรรมโดยวิธีการทั่วไปที่เคยปฏิบัติอยู่เดิมควรกำหนดให้มีคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ทำหน้าที่วางนโยบายกำหนดหลักเกณฑ์เพื่อส่งเสริมการทำธุรกรรมทางอิเล็กทรอนิกส์ ติดตามดูแลการประกอบธุรกิจเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ รวมทั้งมีหน้าที่ในการส่งเสริมการพัฒนาการทางเทคโนโลยีเพื่อติดตามความก้าวหน้าของเทคโนโลยี ซึ่งมีการเปลี่ยนแปลงและพัฒนาศักยภาพตลอดเวลาให้มีมาตรฐานน่าเชื่อถือ ตลอดจนเสนอแนะแนวทางแก้ไขปัญหาและอุปสรรคที่เกี่ยวข้องอันจะเป็นการส่งเสริมการใช้ธุรกรรมทางอิเล็กทรอนิกส์ทั้งภายในประเทศและระหว่างประเทศด้วยการมีกฎหมายรองรับในลักษณะที่เป็นเอกรูป และสอดคล้องกับมาตรฐานที่นานาประเทศยอมรับ อีกทั้งยังมีการกำหนดไว้ในพระราชกฤษฎีการกำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 ซึ่งเป็นกฎหมายลำดับรองของกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ซึ่งบังคับใช้เฉพาะกับหน่วยงานของรัฐเท่านั้น ได้บัญญัติไว้ว่า “มาตรา 6 ในกรณีที่มีการรวบรวม จัดเก็บ ใช้ หรือเผยแพร่ข้อมูล หรือข้อเท็จจริงที่ทำให้สามารถระบุตัวบุคคล ไมวาโดยตรงหรือโดยออม ให้หน่วยงานของรัฐจัดทำแนวนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลบุคคลด้วย” ฉะนั้นผู้ศึกษาจึงเห็นว่า พระราชบัญญัตินี้ได้กำหนดไว้เพียงการคุ้มครอง

ข้อมูลส่วนบุคคลทางอิเล็กทรอนิกส์ที่อยู่ในการครอบครองของรัฐเท่านั้น ยังไม่มีกฎหมายที่บัญญัติไว้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล และความมั่นคงปลอดภัยของข้อมูลทางอิเล็กทรอนิกส์ในกรณี Big Data ที่อยู่ในการครอบครองของเอกชน

4.1.4 วิเคราะห์การคุ้มครอง Big Data ตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

กรณีความเป็นส่วนตัว (Privacy) และความมั่นคงปลอดภัยของข้อมูล (Data Security) พบว่าพระราชบัญญัติฉบับนี้เป็นกฎหมายอาญาที่ระบุความผิดที่เกี่ยวข้องกับการใช้คอมพิวเตอร์โดยผิดกฎหมาย และการวิเคราะห์ข้อมูลใน Big Data มีกระบวนการรวบรวมประมวลผล และเชื่อมโยงข้อมูลที่อาจทำให้เกิดการละเมิดข้อมูลส่วนบุคคลขึ้นได้นั้น จำเป็นต้องใช้ระบบคอมพิวเตอร์เพื่อประมวลผลและเก็บรวบรวมข้อมูลในกระบวนการวิเคราะห์ ดังนั้น จึงมีความจำเป็นต้องนำพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาพิจารณาประกอบด้วยว่าสามารถปรับใช้กับบริบทของการคุ้มครองข้อมูลส่วนบุคคลจากการวิเคราะห์ข้อมูลใน Big Data ได้เพียงใด ซึ่งผู้ศึกษาได้พิจารณาแล้วเห็นว่าการวิเคราะห์ข้อมูลใน Big Data ที่อาจเป็นความผิดตามพระราชบัญญัติฉบับนี้ คือการละเมิดต่อข้อมูลส่วนบุคคลที่เก็บอยู่ในคอมพิวเตอร์ ซึ่งถือเป็นการกระทำต่อ “ข้อมูลคอมพิวเตอร์” ที่เป็นข้อมูลส่วนบุคคลซึ่งมีความผิดที่เกี่ยวข้อง คือ ความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ (มาตรา 7) ความผิดฐานดักรับข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ (มาตรา 8) และความผิดฐานทำให้เสียหาย แก้ไข เปลี่ยนแปลง เพิ่มเติมข้อมูลคอมพิวเตอร์โดยมิชอบ (มาตรา 9) ซึ่งอธิบายได้ดังนี้

1) ความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ

มาตรา 7 “ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่ มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาทหรือทั้งจำทั้งปรับ”

การเข้าถึง ในกฎหมายนานาประเทศมีรูปแบบของการเข้าถึงมากมาย เช่น การกระทำที่เป็นการทำให้คอมพิวเตอร์ทำงานอย่างใดอย่างหนึ่ง การกระทำที่เป็นการบุกรุกเข้าไปในคอมพิวเตอร์ การกระทำที่เป็นการได้มาหรือการกระทำที่เป็นการควบคุมข้อมูลหรือระบบคอมพิวเตอร์ การเข้าถึงอาจอธิบายได้ว่า คือ การตอบสนองกับคอมพิวเตอร์โดยวิการใด ๆ ก็ตาม ไม่ว่าจะเป็นทางกายภาพหรือระยะไกลเพื่อก่อให้เกิดการทำงานของคอมพิวเตอร์ โดยรวมถึงการดักรับข้อมูลคอมพิวเตอร์ที่เป็นการเข้าถึงในเชิงรับด้วย และรวมถึงการใช้คอมพิวเตอร์เพื่อประโยชน์ของตนเองด้วย[3]

[3] ชาตรี ส่งสัมพันธ์, **อาชญากรรมคอมพิวเตอร์: ศึกษาวิเคราะห์การเข้าถึงโดยมิชอบ** (วิทยานิพนธ์มหาบัณฑิต นิติศาสตรมหาบัณฑิต บัณฑิตวิทยาลัย มหาวิทยาลัยธรรมศาสตร์, 2552), 114.

โดยมิชอบ ซึ่งเป็นอีกองค์ประกอบความผิดหนึ่ง ตามพระราชบัญญัตินี้มีความหมายว่า

(ก) เข้าถึงโดยปราศจากความยินยอม

(ข) เข้าถึงโดยเกินจากขอบอำนาจหน้าที่ที่ตนได้รับ

(ค) เข้าถึงโดยไม่มีกฎหมายให้อำนาจไว้

วัตถุประสงค์ของมาตรา 7 นี้ คือ กฎหมายต้องการคุ้มครองความลับของข้อมูล ความสมบูรณ์ของข้อมูลคอมพิวเตอร์ และความเป็นส่วนตัวของเจ้าของระบบคอมพิวเตอร์หรือเจ้าของข้อมูลคอมพิวเตอร์มิให้บุคคลอื่นสามารถเข้าถึง ตรวจสอบ หรือดู และใช้ประโยชน์จากข้อมูลคอมพิวเตอร์ดังกล่าวโดยไม่ได้รับอนุญาตจากเจ้าของระบบคอมพิวเตอร์ หรือเจ้าของข้อมูลคอมพิวเตอร์หรือไม่มีสิทธิตามกฎหมาย

2) ความผิดฐานดักรับข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ

มาตรา 8 “ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการ ทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ ระหว่างการส่งในระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อ ประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ ต้องระวางโทษจำคุกไม่เกินสามปีหรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ”

การดักรับข้อมูลคอมพิวเตอร์ในมาตรานี้ หมายถึง การดักรับโดยวิธีการทางเทคนิค เพื่อลอบดักฟัง ตรวจสอบ หรือติดตามเนื้อหาสาระของข่าวสารที่สื่อสารถึงกันระหว่างบุคคล หรือเป็นการกระทำเพื่อให้ได้มาซึ่งเนื้อหาข้อมูลโดยตรงหรือโดยการเข้าถึงและใช้ระบบคอมพิวเตอร์ หรือการทำให้ได้มาซึ่งเนื้อหาของข้อมูลโดยทางอ้อมด้วยการแอบบันทึกข้อมูลสื่อสารถึงกันด้วยอุปกรณ์อิเล็กทรอนิกส์ โดยไม่คำนึงว่าอุปกรณ์อิเล็กทรอนิกส์ที่ใช้บันทึกข้อมูลดังกล่าวจะต้องเชื่อมต่อเข้ากับสายสัญญาณสำหรับส่งผ่านข้อมูลหรือไม่ เพราะบางกรณีอาจใช้อุปกรณ์เช่นว่านั้นเพื่อบันทึกการสื่อสารข้อมูลที่ได้ส่งผ่านด้วยวิธีการแบบไร้สายก็ได้ เช่น การติดต่อผ่านทางโทรศัพท์เคลื่อนที่ เป็นต้น โดยวัตถุประสงค์ของมาตรา 8 นี้ คือ เพื่อคุ้มครองสิทธิความเป็นส่วนตัวในการติดต่อสื่อสาร ทำนองเดียวกับการให้ความคุ้มครองสิทธิความเป็นส่วนตัวในการติดต่อสื่อสารรูปแบบที่ห้ามดักฟังหรือแอบบันทึกการสนทนาทางโทรศัพท์

3) ความผิดฐานทำให้เสียหาย แก้ไข เปลี่ยนแปลง เพิ่มเติมข้อมูลคอมพิวเตอร์โดยมิชอบ

มาตรา 9 “ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วนซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่น โดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาทหรือทั้งจำทั้งปรับ”

มาตรานี้มีเจตนารมณ์มุ่งจะรักษาความมั่นคงปลอดภัย และคุ้มครองความถูกต้องของข้อมูลความถูกต้องแท้จริง และเสถียรภาพหรือความพร้อมในการใช้งานหรือการใช้ข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ที่บันทึกเก็บไว้บนสื่อคอมพิวเตอร์ได้อย่างเป็นปกติ จึงเป็นการกำหนดขึ้น

เพื่อให้ข้อมูลคอมพิวเตอร์และโปรแกรมคอมพิวเตอร์ได้รับความคุ้มครองเช่นเดียวกับสิ่งของที่สามารถจับต้องได้

พิจารณาการคุ้มครองตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ผู้ศึกษาได้พิจารณาแล้วเห็นว่าการวิเคราะห์ข้อมูลใน Big Data ที่อาจเป็นความผิดตามพระราชบัญญัติฉบับนี้ คือ การละเมิดต่อข้อมูลส่วนบุคคลที่เก็บอยู่ในคอมพิวเตอร์ ซึ่งถือเป็นการกระทำต่อ “ข้อมูลคอมพิวเตอร์” ที่เป็นข้อมูลส่วนบุคคลซึ่งมีความผิดที่เกี่ยวข้อง คือ ความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ (มาตรา 7) ความผิดฐานดักรับข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ (มาตรา 8) และความผิดฐานทำให้เสียหาย แก้ไข เปลี่ยนแปลง เพิ่มเติมข้อมูลคอมพิวเตอร์โดยมิชอบ (มาตรา 9) แต่กฎหมายฉบับนี้ไม่ได้ตราขึ้นเพื่อคุ้มครองข้อมูลส่วนบุคคลโดยตรง แค่มีวัตถุประสงค์เพื่อควบคุมและลงโทษผู้กระทำความผิดที่ใช้อุปกรณ์คอมพิวเตอร์หรือระบบคอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิดเท่านั้น

4.1.5 วิเคราะห์การคุ้มครอง Big Data ตามพระราชบัญญัติประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545

กรณีความเป็นส่วนตัว (Privacy) พบว่ากฎหมายฉบับนี้มีหลักการคุ้มครองข้อมูลเครดิต เช่น หลักข้อจำกัดในการเก็บรวบรวมข้อมูล หลักคุณภาพของข้อมูล หลักความยินยอม หลักข้อจำกัดในการนำไปใช้ หลักการมีสิทธิเข้าถึงข้อมูลของตน รวมถึงหลักการบังคับการตามกฎหมาย แต่ยังไม่ครอบคลุมถึงปัญหาเกี่ยวกับการใช้ข้อมูลใน Big Data อย่างไรก็ตามกฎหมายฉบับนี้ก็มีวัตถุประสงค์เพื่อคุ้มครอง “ข้อมูลเครดิต” ที่จำกัดเฉพาะข้อมูลทางสินเชื่อของผู้ที่เป็นลูกค้าของ “สถาบันการเงิน” มุ่งที่จะจำกัดของเขตการประกอบธุรกิจข้อมูลเครดิตให้จำกัดอยู่เฉพาะการจัดเก็บรวบรวมข้อมูลเครดิตที่เกี่ยวกับบุคคลที่เป็นลูกค้าผู้ขอสินเชื่อเท่านั้น หากเป็นข้อมูลส่วนบุคคลประเภทอื่น ๆ ย่อมไม่ได้รับความคุ้มครองตามกฎหมายฉบับนี้

กรณีความมั่นคงปลอดภัยของข้อมูล (Data Security) พบว่ากฎหมายนี้ได้กำหนดหลักการรักษาความมั่นคงปลอดภัยไว้ว่า บริษัทข้อมูลเครดิตต้องจัดให้มีระบบการรักษาความลับและความมั่นคงปลอดภัยของข้อมูลเพื่อป้องกันมิให้มีการนำข้อมูลไปใช้ผิดวัตถุประสงค์ และมิให้ผู้ไม่มีสิทธิได้รับรู้ข้อมูล รวมทั้งระบบป้องกันมิให้ข้อมูลถูกแก้ไข ทำให้เสียหายหรือถูกทำลายโดยไม่ชอบหรือโดยไม่ได้รับอนุญาต แต่ทั้งนี้กฎหมายฉบับนี้ก็มุ่งคุ้มครองเฉพาะ “ข้อมูลเครดิต” ที่จำกัดเฉพาะข้อมูลทางสินเชื่อเท่านั้น

อย่างไรก็ตาม กฎหมายฉบับนี้นับเป็นกฎหมายฉบับแรกที่ออกมาเพื่อคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของภาคเอกชนเฉพาะเรื่องข้อมูลส่วนบุคคลทางการเงิน ไม่ใช่กฎหมายทั่วไปที่ใช้บังคับได้กับข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของเอกชนในทุกเรื่องทุกกรณี ดังนั้น

การคุ้มครองตามพระราชบัญญัติประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 จึงไม่ได้กล่าวถึงการคุ้มครองข้อมูลใน Big Data ไว้ เนื่องจากเป็นกฎหมายที่บัญญัติไว้ตั้งแต่ปี พ.ศ. 2545

4.2 วิเคราะห์การคุ้มครอง Big Data ตามกฎหมายต่างประเทศ

กฎหมายต่างประเทศที่ศึกษา คือ กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในประเทศสหรัฐอเมริกา และกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในประเทศอังกฤษตามข้อกำหนดของสหภาพยุโรป ซึ่งวิเคราะห์ได้ดังนี้

4.2.1 วิเคราะห์การคุ้มครอง Big Data ตามกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในประเทศสหรัฐอเมริกา

กฎหมายที่เกี่ยวข้องกับการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว และความมั่นคงปลอดภัยของข้อมูลใน Big Data มีลักษณะเป็นกฎหมายเฉพาะเรื่อง (Sectoral Law) ไม่มีกฎหมายกลางที่วางหลักเกณฑ์เป็นการทั่วไป การคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวมักจะกระทำในรูปแบบของการออกกฎหมายเพื่อแก้ปัญหาที่เกิดขึ้นแล้วมากกว่าที่จะวางหลักเกณฑ์ทั่วไปเพื่อป้องกันปัญหาโดยการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวปรากฏออกมาในกฎหมายต่าง ๆ คือ

รัฐธรรมนูญแห่งสหรัฐอเมริกา ได้ให้ความคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว ในฐานะเป็นสิทธิที่มีความเกี่ยวข้องกับอิสรภาพและเสรีภาพของประชาชน กล่าวคือ เป็นสิทธิในการที่บุคคลจะเป็นอิสระจากการตรวจค้น การยึด หรือการถูกรบกวนแทรกแซงโดยไม่มีเหตุอันควร รวมถึงสิทธิที่จะได้รับความคุ้มครองในข้อมูลส่วนบุคคล สิทธิที่จะไม่เปิดเผยตัวตนและสิทธิที่จะอยู่โดยลำพัง

อย่างไรก็ตาม รัฐธรรมนูญแห่งสหรัฐอเมริกาก็ไม่ได้มีบทบัญญัติที่รับรองคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวไว้โดยชัดแจ้ง แต่การคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวก็มีพัฒนาการภายใต้การปรับปรุงแก้ไขรัฐธรรมนูญในแต่ละครั้ง ซึ่งเมื่อพิจารณาถึงบริบทของการละเมิดสิทธิในความเป็นอยู่ส่วนตัว และความมั่นคงปลอดภัยของข้อมูลใน Big Data การละเมิดต่อความเป็นส่วนตัวในตำแหน่งที่อยู่ถือเป็นการละเมิดต่อสิทธิที่จะอยู่โดยลำพังโดยปราศจากการรบกวนแทรกแซงโดยไม่มีเหตุอันควร อันเป็นสิ่งที่รัฐธรรมนูญนี่ได้ให้ความคุ้มครอง รวมไปถึงความเป็นส่วนตัวในข้อมูลส่วนบุคคลที่อยู่ภายใต้กรอบการคุ้มครองตามรัฐธรรมนูญเช่นเดียวกัน เพียงแต่ในปัจจุบันยังไม่มีคำพิพากษาเกี่ยวกับกรณีนี้ที่จะเป็นการวางแนวทางในการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว และความมั่นคงปลอดภัยของข้อมูลใน Big Data

กฎหมายสหพันธรัฐ (Federal Law) ให้ความคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวในกฎหมายเฉพาะเรื่องในกฎหมายหลายฉบับกระจัดกระจายกันไป โดยไม่มีกฎหมายกลางหรือกฎหมายแม่บทที่วางหลักเกณฑ์การคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวไว้แต่อย่างใด ส่วนกฎหมายที่มีผลบังคับใช้ครอบคลุมสิทธิในความเป็นอยู่ส่วนตัวมากที่สุดคือ The Privacy Act of 1974 แต่กฎหมาย

ฉบับนี้ก็ไม่ได้มีผลบังคับใช้กับภาคเอกชน โดยจะใช้บังคับกับหน่วยงานของรัฐหรือหน่วยงานที่อยู่ภายใต้การควบคุมกำกับดูแลของรัฐเท่านั้น และถึงแม้จะสามารถนำ Privacy Act ฉบับนี้มาใช้กับภาคเอกชนด้วย ภาคเอกชนก็จะไม่ได้รับความคุ้มครองเรื่องการบันทึกหรือรวบรวมข้อมูลส่วนบุคคล รวมถึงข้อมูลใน Big Data ด้วย เพราะกฎหมายนี้ไม่ได้ห้ามมิให้ทำการบันทึกหรือรวบรวมข้อมูลส่วนบุคคล แต่ห้ามมิให้นำข้อมูลส่วนบุคคลที่บันทึกหรือรวบรวมไว้ไปใช้ในทางที่มิชอบเท่านั้น โดยกฎหมายฉบับนี้จะนำมาปรับใช้กับข้อมูลส่วนบุคคลที่บันทึกหรือรวบรวมไว้แล้วในความครอบครองของหน่วยงานของรัฐหรือหน่วยงานที่อยู่ภายใต้การควบคุมกำกับดูแลของรัฐ ส่วนกฎหมายอื่น ๆ ที่ให้ความคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวก็จะเป็นกฎหมายเฉพาะเรื่อง อาทิ Electronic Communications Privacy act (1986), Video Privacy Protection Act (1988), Employee Polygraph Protection Act (1988) หรือ Occupational Health and Safety Act (1970) อันเป็นกฎหมายที่แบ่งการคุ้มครองตามลักษณะของข้อมูลหรือกิจกรรมที่ควรได้รับการคุ้มครองตามกฎหมายนั้น ๆ ซึ่งต่างก็มีข้อจำกัดบางประการที่ทำให้ไม่สามารถนำมาปรับใช้กับการละเมิดสิทธิในความเป็นอยู่ส่วนตัว และความมั่นคงปลอดภัยของข้อมูลใน Big Data ได้[4]

จากการที่มีข้อจำกัดทางด้านกฎหมายอันเกี่ยวกับการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวนี้ ได้มีบทความในทางวิชาการที่เสนอทางออกเพื่อคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว เสนอให้แก้บทบัญญัติแห่ง The Privacy Act of 1974 โดยให้เพิ่มหลักการดังต่อไปนี้เข้าไปด้วย[5]

หน่วยงานหรือองค์กรต่าง ๆ มีหน้าที่ดังต่อไปนี้

1) กระทำการใด ๆ เพื่อจำกัดการบันทึกหรือรวบรวมข้อมูลส่วนบุคคล และมีหน้าที่ต้องรักษาความลับของข้อมูลที่ทำการบันทึกหรือรวบรวมนั้น

2) ในกรณีที่ไม่อาจรักษาความลับของข้อมูลส่วนบุคคลได้ ไม่ว่าจะมีเหตุอันเนื่องมาจากปัญหาในทางเทคนิคหรือปัญหาในการบริหารจัดการ การนำข้อมูลส่วนบุคคลเช่นว่านั้นไปใช้ในกรณีดังต่อไปนี้ จะต้องได้รับความยินยอมโดยชัดแจ้งจากผู้เป็นเจ้าของข้อมูล

(a) การเปิดเผยข้อมูลที่สามารถบ่งชี้ถึงตัวบุคคลต่อผู้บริโภคใด ๆ เพื่อวัตถุประสงค์อย่างใดอย่างหนึ่ง

---

[4] Eden, J. M., **When Big Brother Privatizes: Commercial Surveillance, the Privacy Act of 1974, and the Future of RFID** [Online], 2005. Available from http://scholarship.law.duke.edu/cgi/ viewcontent.cgi?article=1140&context=dltr.

[5] Ibid, 19-20.

(b) การบันทึกหรือรวบรวมข้อมูลผู้บริโภคใด ๆ โดยเทคโนโลยีที่มีขึ้นเพื่อวัตถุประสงค์ในการติดตามเฝ้าดู หรือเพื่อวัตถุประสงค์ในทางการค้า อันมีพฤติการณ์ที่อาจเป็นการละเมิดต่อสิทธิที่จะอยู่โดยลำพังและไม่เปิดเผยตัวของผู้บริโภคนั้น

3) ห้ามมิให้บริษัทเอกชนกระทำการใด ๆ อันเป็นการเลือกปฏิบัติต่อผู้บริโภคที่มิได้ให้ความยินยอมให้ กระทำการบันทึกหรือรวบรวมข้อมูลส่วนบุคคลของตน

นอกจากข้อเสนอให้แก้ไขเพิ่มเติม The Privacy Act of 1974 ดังกล่าวแล้ว ยังมีบทความทางวิชาการที่เสนอให้แก้ไขเพิ่มเติม United State Code: Chapter 94 - Privacy โดยเสนอให้เพิ่มเติมหลักการลงไปใน Title 15 - Commerce and Trade โดยให้มีหลักการว่าด้วย “การบันทึกรวบรวมข้อมูลส่วนบุคคลและข้อมูลการระบุตัวตนโดยคลื่นความถี่วิทยุ (Aggregation of Nonpublic Personal Information and Radio Frequency Identification Information)” อันมีวัตถุประสงค์เพื่อห้ามมิให้หน่วยงานหรือองค์การทางธุรกิจกระทำการดังต่อไปนี้[6]

(1) รวบรวมและเชื่อมโยงข้อมูลส่วนบุคคล

(2) เปิดเผยข้อมูลส่วนบุคคลที่ได้จากการประมวลผลข้อมูล ไปยังบุคคลภายนอก

(3) ทำการประมวลผลข้อมูลเพื่อเชื่อมโยงระบุตัวตนของบุคคล

ในประเทศสหรัฐอเมริกา คณะกรรมการการค้าแห่งสหพันธรัฐ (The Federal Trade Commission หรือ FTC) ซึ่งเป็นหน่วยงานของรัฐที่มีอำนาจหน้าที่ตามกฎหมายเกี่ยวข้องกับการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว ได้ออกมาวางกรอบนโยบายที่เรียกว่า Fair Information Practice[7] เพื่อให้ภาคเอกชนนำไปเป็นแนวทางในการออกกฎเกณฑ์ แนวปฏิบัติ หรือประมวลจริยธรรมเพื่อใช้ควบคุมกันเองในองค์กร อันถือเป็นการใช้มาตรการให้ภาคธุรกิจควบคุมกันเอง (Self-Regulatory) ซึ่งภาคเอกชนในประเทศสหรัฐอเมริกาก็ได้ตอบสนองต่อกรอบนโยบายนี้กันอย่างตื่นตัว ดังเช่น Electronic Privacy Information Center (EPIC) ได้ออกความเห็นเกี่ยวกับ Big Data ไว้ในบทความ Big Data and the Future of Privacy อีกด้วย[8]

---

[6] Stein, S. G., **WHERE WILL CONSUMERS FIND PRIVACYPROTECTION FROM RFIDS?: A CASE FOR FEDERAL LEGISLATION** [Online], 2007. Available from http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1169&context=dltr.

[7] Fair Information Practice Principles (FIPPs), **NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE** [Online], Available from http://www.nist.gov/nstic/NSTIC-FIPPs.pdf.

[8] EPIC, **Request for Information: Big Data and the Future of Privacy, COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER to THE OFFICE OF SCIENCE AND TECHNOLOGY POLICY**, 4 April 2014. Available from https://epic.org/privacy/big-data/EPIC-OSTP-Big-Data.pdf.

อย่างไรก็ตาม หน่วยงานที่ทำหน้าที่ควบคุม กำกับ ดูแลการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวนั้น จะเป็นการควบคุม กำกับ ดูแลการควบคุมดูแลกันเองโดยภาคเอกชนอีกชั้นหนึ่ง โดยหน่วยงานของรัฐที่มีอำนาจหน้าที่ดังกล่าวนี่ คือ คณะกรรมการการค้าแห่งสหพันธรัฐ (The Federal Trade Commission หรือ FTC) ที่อาศัยอำนาจตามมาตรา 5 แห่ง Federal Trade Commission Act ในการสั่งให้ภาคเอกชนหยุดหรือระงับการกระทำที่ไม่เป็นธรรมหรือมีเจตนาหลอกลวงในกิจการต่าง ๆ รวมไปถึงกรณีที่ภาคเอกชนไม่ปฏิบัติตาม Self-Regulation ไม่ว่าจะทั้งหมดหรือเพียงบางส่วนหนึ่งส่วนใดของหลักการดังกล่าว FTC มีอำนาจที่จะควบคุมดูแลให้ภาคเอกชนต้องปฏิบัติตาม Self-Regulation นั้น ๆ ของตนอย่างเคร่งครัด กล่าวคือ มีหน้าที่บังคับการให้เป็นไปตาม Self-Regulation ที่ภาคเอกชนได้ออกเป็นกฎเกณฑ์ แนวปฏิบัติ หรือประมวลจริยธรรมเพื่อใช้ควบคุมกันเองภายในองค์กร โดย FTC ได้ออกประกาศในเดือนมีนาคม ค.ศ. 2005 เพื่อกำหนดกรอบของนโยบายเกี่ยวกับการคุ้มครองข้อมูลที่เรียกว่า Fair Information Practice มาเป็นแนวทางให้องค์กรเอกชนนำไปเป็นหลักในการออกกฎเกณฑ์ แนวปฏิบัติ หรือประมวลจริยธรรมต่าง ๆ เพื่อคุ้มครองสิทธิความเป็นอยู่ส่วนตัวกรณี Big Data มีหลักการที่สำคัญอยู่ 5 ประการ คือ

1) ต้องมีการประกาศและแจ้งให้ผู้บริโภคทราบถึงการบันทึกหรือรวบรวมข้อมูลส่วนบุคคลในกรณีที่มีการกระทำดังกล่าว

2) ต้องมีการเสนอทางเลือกให้แก่ผู้บริโภคว่าจะยินยอมให้นำข้อมูลส่วนบุคคลของไปใช้ได้หรือไม่ เพียงใด

3) ต้องให้ผู้บริโภคสามารถเข้าถึงข้อมูลส่วนบุคคลของตนและสามารถตรวจสอบความถูกต้องสมบูรณ์ของข้อมูลนั้น

4) ต้องเก็บรักษาข้อมูลให้มีความปลอดภัยและครบถ้วนสมบูรณ์

5) มีมาตรการในเชิงบังคับสำหรับการไม่ปฏิบัติตามหลักการที่กล่าวมานี้

จะเห็นได้ว่า ถึงแม้ว่า The Privacy Act of 1974 (Privacy Act) จะไม่สามารถนำมาปรับใช้กับการคุ้มครอง Big Data ได้ เพราะตามกฎหมายสามารถให้ทำการบันทึกหรือรวบรวมข้อมูลส่วนบุคคลได้ แต่ห้ามมิให้นำข้อมูลส่วนบุคคลที่บันทึกหรือรวบรวมไว้ไปใช้ในทางที่มิชอบเท่านั้น แต่อย่างไรก็ดีคณะกรรมการการค้าแห่งสหพันธรัฐ (The Federal Trade Commission หรือ FTC) ก็ยังแก้ไขได้โดยกำหนดกรอบของนโยบายเกี่ยวกับการคุ้มครองข้อมูลที่เรียกว่า Fair Information Practice มาเป็นแนวทางให้องค์กรเอกชนนำไปเป็นหลักในการออกกฎเกณฑ์ แนวปฏิบัติ หรือประมวลจริยธรรมต่าง ๆ เพื่อคุ้มครองสิทธิความเป็นอยู่ส่วนตัว และสามารถนำมาปรับใช้ในกรณี Big Data ได้

นอกจากนี้ในส่วนของการคุ้มครองผู้บริโภค ยังพบปัญหาการขาดบทบัญญัติแห่งกฎหมายเพื่อคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวของผู้บริโภคที่มาสามารถใช้ได้ครอบคลุมกับการละเมิดสิทธิใน

ความเป็นอยู่ส่วนตัวจากการใช้เทคโนโลยีใหม่ ๆ ได้ทุกกรณี ทำให้เกิดช่องว่างทางกฎหมายซึ่งจำเป็นต้องหามาตรการต่าง ๆ มาอุดช่องว่างทางกฎหมายนี้ ซึ่งการออกกฎหมายเพื่อบังคับใช้กับเทคโนโลยีใดเทคโนโลยีหนึ่งเป็นการเฉพาะ (Technology-Specific Legislation) ก็เป็นอีกทางเลือกหนึ่งเพื่อคุ้มครองการละเมิดความเป็นส่วนตัวจากการใช้ Big Data แต่การออกกฎหมายเพื่อบังคับใช้กับ Big Data เป็นการเฉพาะนี้ แม้จะทำให้มีบทบัญญัติที่จะนำมาบังคับใช้กับกรณีได้ตรงประเด็นมากยิ่งขึ้น แต่การออกกฎหมายในลักษณะนี้ก็มีข้อเสียคือเป็นบทบัญญัติที่ใช้ได้จำกัดเฉพาะในวงแคบเท่านั้น โดยมีผู้ให้ความเห็นว่าการบัญญัติกฎหมายเพื่อบังคับกับเทคโนโลยีใดเทคโนโลยีหนึ่งเป็นการเฉพาะ ซึ่งจะมีเหตุอันควรเพื่อออกกฎหมายลักษณะดังกล่าวก็ต่อเมื่อ

1) ผู้บริโภคไม่ทราบและขาดความเข้าใจเกี่ยวกับกระบวนการทำงานของเทคโนโลยี และผลกระทบที่อาจเกิดขึ้นกับตนจากการประยุกต์ใช้เทคโนโลยีนั้น ๆ

2) กฎหมายทั่วไปที่มีผลใช้บังคับอยู่ในขณะนั้นขาดบทบัญญัติที่เพียงพอในการห้ามมิให้มีการรวบรวมข้อมูลส่วนบุคคล และ

3) กฎหมายทั่วไปที่มีผลใช้บังคับอยู่ในขณะนั้นขาดบทลงโทษ หรือมาตรการในเชิงบังคับ ในกรณีที่มีการนำข้อมูลไปใช้ในทางมิชอบ

เมื่อมีเหตุใดเหตุหนึ่งตามที่กล่าวมานี้เกิดขึ้นจึงจะสมควรให้มีการพิจารณาทางเลือกในการออกกฎหมายเพื่อบังคับใช้กับเทคโนโลยีใดเทคโนโลยีหนึ่งเป็นการเฉพาะ เช่น กรณีกฎหมายเกี่ยวกับใช้ Big Data ดังนั้น การออกกฎหมายเพื่อบังคับใช้กับเทคโนโลยีใดเทคโนโลยีหนึ่งเป็นการเฉพาะก็ยิ่งจะก่อประโยชน์ต่อการนำไปบังคับใช้อย่างยิ่ง[9]

4.2.2 วิเคราะห์การคุ้มครอง Big Data ตามกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในประเทศอังกฤษตามข้อกำหนดของสหภาพยุโรป Directive 95/46/EC

EU Directive 95/46/EC ได้กำหนดหลักเกณฑ์บังคับสำหรับการดำเนินการใด ๆ กับข้อมูลส่วนบุคคลที่เรียกว่า การประมวลผล (Processing) ซึ่งหมายถึงการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล ไม่ว่าโดยวิธีการอัตโนมัติหรือวิธีการอื่นใด เช่น การเก็บรวบรวม การบันทึก การจัดเรียบเรียง การเก็บรักษา การแก้ไขเปลี่ยนแปลง การใช้ การเปิดเผยโดยการส่งผ่าน การเผยแพร่ การทำให้เข้าถึงข้อมูลได้ การขัดขวาง การลบ หรือการทำลายข้อมูล โดยการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลทุกขั้นตอนต้องตกอยู่ภายใต้หลักเกณฑ์การคุ้มครองเดียวกัน ซึ่งหลักเกณฑ์ ตาม Recital 2 ของ EU Directive 95/46/EC ว่าระบบการประมวลผลข้อมูลนั้นถูกสร้างขึ้นเพื่อให้เกิดประโยชน์แก่มนุษย์

---

[9] Laura, H., **Defusing the Threat of RFID: Protecting Consumer Privacy Through Technology-Specific Legislation at the State Level** [Online], 2006. Available from http://www.law.harvard.edu/students/orgs/crcl/vol41_1/hildner.pdf.

ดังนั้น เมื่อมีการใช้จึงต้องมีการคำนึงถึงและเคารพต่อสิทธิขั้นพื้นฐานและสิทธิเสรีภาพของมนุษย์ไม่ว่าจะมีสัญชาติใดหรือมีถิ่นพำนักอยู่ที่ใด โดยสิทธิหลักที่ต้องคำนึงถึงคือสิทธิในความเป็นอยู่ส่วนตัว และความมั่นคงปลอดภัยของข้อมูลใน Big Data

1) หลักคุณภาพของข้อมูล (Data Quality) ผู้ครอบครอง ควบคุม หรือบันทึกข้อมูลจะต้องดำเนินการโดยคำนึงถึงหลักการดังต่อไปนี้

1.1) หลักข้อจำกัดในการนำไปใช้ (Use Limitation principle) มีหลักการว่าข้อมูลส่วนบุคคลจะต้องไม่นำไปเปิดเผยหรือใช้ในวัตถุประสงค์อื่น ๆ นอกเหนือจากที่ได้กำหนดไว้ในวัตถุประสงค์ที่จัดเก็บ (Directive 95/46/EC Article 6(1)(b))

1.2) หลักคุณภาพของข้อมูล (The Data Quality principle) หลักการนี้กำหนดว่าข้อมูลส่วนบุคคลที่จัดเก็บจะต้องเป็นไปตามวัตถุประสงค์ที่จะนำไปใช้ และจะต้องไม่จัดเก็บข้อมูลใด ๆ ที่ไม่เกี่ยวข้อง อีกทั้งข้อมูลที่จัดเก็บต้องมีความถูกต้อง

1.3) หลักการเก็บรักษาข้อมูล (The Conservation principle) หลักการนี้กำหนดว่าข้อมูลส่วนบุคคลจะต้องไม่เก็บไว้นานเกินความจำเป็นเกินกว่าวัตถุประสงค์ของการนำข้อมูลไปใช้

2) หลักการประมวลผลข้อมูล (Data Processing) (Directive 95/46/EC Article 7) การจะประมวลผลข้อมูลส่วนบุคคลนั้นจะกระทำได้ถูกต้องตามกฎหมายก็ต่อเมื่อมีเหตุผลตามกฎหมายมารองรับการประมวลผลของข้อมูลนั้นจะต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล

2.1) การประมวลผลของข้อมูลนั้นเป็นความจำเป็นเพื่อการชำระหนี้ตามความผูกพันที่เป็นผลของสัญญาที่มีเจ้าของข้อมูลเป็นคู่สัญญาอยู่ด้วย

2.2) การประมวลผลของข้อมูลเป็นส่วนสำคัญในการปฏิบัติตามภาระหน้าที่ของผู้ควบคุมและบันทึกข้อมูล

2.3) การประมวลผลของข้อมูลนั้นเป็นไปเพื่อปกป้องประโยชน์ของเจ้าของข้อมูล

2.4) การประมวลผลของข้อมูลนั้นมีความจำเป็นในการดำเนินงานเพื่อผลประโยชน์ของสาธารณชน

2.5) การประมวลผลของข้อมูลนั้นมีความจำเป็นเพื่อส่งเสริมผลประโยชน์ตามกฎหมายของผู้ที่เกี่ยวข้อง

3) หลักการให้ข้อมูล (Information requirements) (Directive 95/46/EC Article10) กำหนดไว้ว่า ผู้ครอบครอง ควบคุม หรือบันทึกข้อมูลจะต้องให้ข้อมูลเหล่านี้แก่เจ้าของข้อมูล

- ต้องมีการเปิดเผยตัวตนของผู้ครอบครอง ควบคุม หรือบันทึกข้อมูล
- วัตถุประสงค์ของการประมวลผลข้อมูล
- ข้อมูลเกี่ยวกับบุคคลที่เป็นผู้รับข้อมูล

4) หลักการเข้าถึงข้อมูลของเจ้าของข้อมูล (Data Subject's Right of Access) (Directive 95/46/EC Article 12) ให้สิทธิแก่เจ้าของข้อมูลในการตรวจสอบความถูกต้องของข้อมูล เพื่อให้แน่ใจว่าข้อมูลที่จัดเก็บมีความถูกต้อง

5) หลักการรักษาความมั่นคงปลอดภัยของข้อมูล (Security Related Obligation) (Directive 95/46/EC Article 17) กำหนดหน้าที่แก่ผู้ครอบครอง ควบคุม หรือบันทึกข้อมูล โดยจะต้องมีการหามาตรการไม่ว่าจะเป็นทางด้านเทคนิคหรือนโยบายขององค์กรเพื่อคุ้มครองข้อมูลส่วนบุคคล หรือการเข้าถึงโดยไม่ได้รับอนุญาต เป็นต้น

6) หลักการโอนข้อมูลข้ามประเทศ (Cross-Border Transfers) ข้อมูลส่วนบุคคลอาจถ่ายโอนไปยังประเทศที่สามนอกสหภาพยุโรปได้เฉพาะเมื่อประเทศปลายทางนั้นมีระดับการคุ้มครองที่เพียงพอ (Adequate Level of Protection) เท่านั้น ประเทศที่มีระดับการคุ้มครองที่ไม่เพียงพอจะถูกรายงานไปยังประเทศในกลุ่มสหภาพยุโรปทุกประเทศ (Black-list)

ในสหภาพยุโรป ตามหลักที่กำหนดไว้ใน Directive 95/46/EC อันเป็นแนวปฏิบัติเพื่อคุ้มครองข้อมูลส่วนบุคคลนั้น ได้กำหนดให้รัฐสมาชิกของ EU กำหนดให้มีการจัดตั้งหน่วยงานของรัฐเพื่อทำหน้าที่ควบคุม กำกับดูแลการปฏิบัติการให้เป็นไปตาม Directive 95/46/EC รวมถึงประเทศอังกฤษด้วย โดยหน่วยงานของรัฐที่จัดตั้งขึ้นนี้มีหน้าที่รวมไปถึงการควบคุมตรวจสอบป้องกันไม่ให้มีการละเมิดต่อสิทธิในความเป็นอยู่ส่วนตัวและข้อมูลส่วนบุคคล หรือหากจำเป็นหน่วยงานของรัฐที่จัดตั้งขึ้นนี้ต้องจัดแนวปฏิบัติที่มารายละเอียดเกี่ยวข้องกับ Big Data หรืออาจต้องจัดทำประมวลจริยธรรม เพื่อใช้กับการเก็บรวบรวม ใช้ เปิดเผย Big Data เป็นการเฉพาะสำหรับแต่ละประเทศ[10]

จากการศึกษา EU นั้น มุ่งไปพิจารณาถึงแนวปฏิบัติที่มีอยู่แล้วอันอาจนำมาปรับใช้ได้ก็คือแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ซึ่ง EU ได้มีข้อกำหนดว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลแห่งสหภาพยุโรป (The European Union Data Protection Directive) ใช้เป็นการเฉพาะเพื่อวางแนวทางในการพิจารณากรณีของ Big Data ที่มีความเกี่ยวข้องกับการบันทึก รวบรวม ประมวลผล ส่งหรือรับข้อมูลนั้น จะอยู่ภายใต้ความคุ้มครองของ EU Directive 95/46/EC อันเป็นแนวปฏิบัติเพื่อคุ้มครองข้อมูลส่วนบุคคลหรือไม่ หลักการเดียวกันนี้ EU จะต้องพิจารณาก่อนว่า การใช้ Big Data มีความเกี่ยวข้องกับปัจเจกบุคคลหรือไม่ และข้อมูลดังกล่าวนั้นสามารถเชื่อมโยงแล้วสามารถระบุหรืออาจระบุถึงตัวบุคคลได้หรือไม่ ซึ่งโดยทั่วไป Big Data ถือเป็นข้อมูลส่วนบุคคลโดยตรงอยู่แล้ว เช่น การมีชื่อ นามสกุล ที่อยู่ หรือวันเดือนปีเกิด ข้อมูลทางสุขภาพ เป็นต้น ซึ่งตามหลักที่ได้

---

[10] Commission of the European Community, **Protection of personal data** [Online], 2011. Available from http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm.

กำหนดไว้ใน Directive 95/46/EC อันเป็นแนวปฏิบัติเพื่อคุ้มครองข้อมูลส่วนบุคคลนั้น ได้กำหนดให้รัฐสมาชิกของ EU กำหนดให้มีการจัดตั้งหน่วยงานของรัฐเพื่อทำหน้าที่ควบคุม กำกับดูแลการปฏิบัติการให้เป็นไปตาม Directive 95/46/EC โดยหน่วยงานของรัฐที่จัดตั้งขึ้นนี้มีหน้าที่รวมไปถึงการควบคุมตรวจสอบ หรือป้องกันไม่ให้มีการละเมิดต่อสิทธิในความเป็นอยู่ส่วนตัวและข้อมูลส่วนบุคคลใน Big Data หรือหากมีความจำเป็น หน่วยงานของรัฐที่จัดตั้งขึ้นนี้ต้องจัดทำแนวปฏิบัติที่มีรายละเอียดเกี่ยวข้องกับการใช้ Big Data เป็นการเฉพาะสำหรับแต่ละประเทศ

อย่างไรก็ตาม กฎเกณฑ์ หรือแนวปฏิบัติต่าง ๆ ที่ออกโดย EU นี้ จะส่งผลต่อการยกร่างกฎหมายของประเทศต่าง ๆ เป็นอย่างมาก เนื่องจากเป็นหน่วยงานที่ได้รับการยอมรับกันอย่างกว้างขวาง ดังเช่นในกรณีแนวปฏิบัติเพื่อคุ้มครองข้อมูลส่วนบุคคลที่หลาย ๆ ประเทศทั่วโลกได้นำไปเป็นหลักในการบัญญัติกฎหมายภายในของตน รวมถึงประเทศไทยที่ได้มีการยึดเอาแนวปฏิบัติของ EU มายกร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... ด้วย

สืบเนื่องจากที่คณะกรรมาธิการยุโรปจะทำการปรับปรุงกฎหมายคุ้มครองข้อมูลส่วนบุคคล (Data Protection Directive) โดยการเปลี่ยนกฎหมายจากรูปแบบ Directive ซึ่งเป็นเพียงแนวทางให้แต่ละประเทศสมาชิกนำไปออกกฎหมายภายในประเทศ เป็น Regulations เรียกว่า EU General Data Protection Regulation[11] ซึ่งมีผลใช้บังคับโดยตรงเสมือนหนึ่งเป็นกฎหมายภายในของแต่ละประเทศสมาชิก และเพิ่มสิทธิในการลบข้อมูลทั้งหมด (Right to be Forgotten) ให้แก่เจ้าของข้อมูล เพิ่มหน้าที่และความรับผิดชอบให้แก่ผู้จัดเก็บและประมวลผลข้อมูล และลดข้อยุ่งยากของกฎระเบียบเกี่ยวกับการส่งข้อมูลไปยังประเทศที่สาม ซึ่งเมื่อกฎหมายนี้ได้รับการรับรองแล้ว และทำให้สามารถประยุกต์ใช้กับกรณีการใช้ข้อมูลใน Big Data มากยิ่งขึ้น และมีการคาดการณ์ว่า หากกฎระเบียบใหม่ดังกล่าวมีผลบังคับใช้ สหภาพยุโรปจะผลักดันให้ประเทศคู่ค้าต่าง ๆ พัฒนากฎหมายของตนเพื่อให้มีการคุ้มครองข้อมูลส่วนบุคคลในระดับเดียวกัน โดยดำเนินการผลักดันผ่านเวทีความร่วมมือต่าง ๆ เช่น FTA หรือ PCA ด้วย

---

[11] European Commission, **Regulation of the European Parliament and of Council** [Online], 25 January 2012. Available from http://ec.europa.eu/justice/data-protection/document/review2012 / com_2012_11_en.pdf.

ตารางที่ 4.1: สรุปปัญหาการคุ้มครอง Big Data ของกฎหมายไทย และกฎหมายต่างประเทศ

ปัญหาการคุ้มครอง Big Data	กฎหมายไทย					กฎหมายต่างประเทศ	
	พ.ร.บ. ข้อมูลข่าวสารของราชการ พ.ศ. 2540	ร่าง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...	พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544	พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	พ.ร.บ. การประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545	สหรัฐอเมริกา	อังกฤษตามสหภาพยุโรป Directive 95/46/EC
1.การเก็บรวบรวมข้อมูล							
- การเก็บรักษาความลับข้อมูล	√	√	—	√	√	√	√
- การยินยอมของผู้ให้ข้อมูล	√	√	—	√	√	√	√
- การรับรู้ของผู้ให้ข้อมูลต่อการมีอยู่ของฐานข้อมูล	√	√	—	—	√	√	√
- การรับรู้ของผู้ให้ข้อมูลต่อการใช้ข้อมูล	√	√	—	—	√	√	√
2. ปัญหาของระบบการจัดเก็บฐานข้อมูล							
- ความปลอดภัยของระบบการจัดเก็บฐานข้อมูล	√	√	—	√	√	√	√
- การเข้าไปในฐานข้อมูลโดยไม่ได้รับอนุญาต	√	√	—	√	√	√	√

(ตารางมีต่อ)

ตารางที่ 4.1 (ต่อ): สรุปปัญหาการคุ้มครอง Big Data ของกฎหมายไทย และกฎหมายต่างประเทศ

ปัญหาการคุ้มครอง Big Data	กฎหมายไทย					กฎหมายต่างประเทศ	
	พ.ร.บ. ข้อมูลข่าวสารของราชการ พ.ศ. 2540	ร่าง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...	พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544	พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	พ.ร.บ. การประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545	สหรัฐอเมริกา	อังกฤษตามสหภาพยุโรป Directive 95/46/EC
3. ปัญหาการใช้ฐานข้อมูล							
- ข้อมูลทีไม่ถูกต้องหรือมีความผิดพลาด	√	√	—	√	√	√	√
- ความเกี่ยวข้องของข้อมูล	—	√	—	—	—	—	√
- ความยินยอมของผู้ให้ข้อมูลต่อการใช้ข้อมูลดังกล่าว	√	√	—	√	√	√	√
- การรับรู้ของผู้ให้ข้อมูลต่อการใช้ข้อมูล	√	√	—	—	√	√	√
4. ปัญหาในการส่งผ่านข้อมูล							
- การเชื่อมโยงฐานข้อมูลทีต่างกัน	—	√	—	—	—	—	√
- การรวมศูนย์และการวิเคราะห์ฐานข้อมูล	—	√	—	—	—	—	√
- การส่งข้อมูลข้ามพรมแดน	—	√	—	—	—	—	√

บทที่ 5
บทสรุปและข้อเสนอแนะ

5.1 บทสรุป

จากการพัฒนาเทคโนโลยีที่มีความเจริญก้าวหน้าขึ้นเรื่อย ๆ อย่างไร้ขีดจำกัดประกอบกับปัจจุบันที่มีการเปิดเสรีในทางการค้าทั่วโลก ทำให้มีการนำเทคโนโลยีมาประยุกต์ใช้เพื่อพัฒนาสังคม เศรษฐกิจ และชีวิตประจำวันมากขึ้น การจัดเก็บรวบรวมและวิเคราะห์ข้อมูลอย่างแม่นยำและรวดเร็ว ทั้งภาพ เสียง ตัวอักษร ตัวเลข และอื่น ๆ มีความหลากหลายและมากมายจนระบบฐานข้อมูลเดิมไม่สามารถจัดการได้ รวบรวมไว้เป็นข้อมูลมหาศาล เรียกว่า Big Data แม้ว่าการใช้งาน Big Data จะเต็มไปด้วยประโยชน์มากมายแต่ก็อาจเปรียบดังเหรียญที่มีสองด้าน เนื่องจากคุณสมบัติเฉพาะตัวบางประการที่สามารถสร้างผลกระทบในเชิงลบต่อบุคคลได้ และสิ่งหนึ่งที่ต้องระลึกถึงอยู่เสมอคือ ความมั่นคงปลอดภัยของข้อมูลที่ต้องมีการป้องกันไม่ให้เกิดความเสียหายหรือรั่วไหล ตลอดจนตระหนักถึงการใช้งานข้อมูลทั้งของตนเองและขององค์กรอย่างเหมาะสม

สิทธิในความเป็นอยู่ส่วนตัว (Right of Privacy) เป็นคำที่มีความหมายกว้างครอบคลุมได้หลายเรื่อง โดยมุ่งหมายถึง การจำกัดการเข้าถึงบุคคลโดยบุคคลอื่น อันมีลักษณะเป็นการจำกัดมิให้ผู้อื่นทราบข้อมูลที่เกี่ยวข้องกับตนเอง การกีดกันหวงห้ามมิให้ผู้อื่นทราบว่าตนเป็นใคร ชื่ออะไร หรือการกีดกันหวงห้ามมิให้ผู้อื่นมาอยู่ใกล้ชิดในทางกายภาพอันเป็นความต้องการที่อยู่คนเดียวโดยปราศจากการรบกวนแทรกแซงจากบุคคลอื่น ซึ่งบุคคลย่อมมีความเป็นส่วนตัวในการติดต่อสื่อสาร (Communication Privacy) ความเป็นส่วนตัวในดินแดน หรืออาณาเขต (Territorial Privacy) ความเป็นส่วนตัวในตำแหน่งที่อยู่ (Location Privacy) ความเป็นส่วนตัวในชีวิตร่างกาย (Bodily Privacy) หรือ ความเป็นส่วนตัวในข้อมูลข่าวสาร (Information Privacy) ฯลฯ อันหมายความรวมถึงความเป็นส่วนตัวในข้อมูลส่วนบุคคล (Personal Information) ด้วย

ในปัจจุบัน แม้ว่าจะมีการรับรองหรือให้ความคุ้มครองสิทธิในความเป็นส่วนตัวโดยบัญญัติเป็นกฎหมายไว้ในหลายฉบับ เช่น รัฐธรรมนูญ มาตรา 35 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ที่กำหนดหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคล การครอบครองของหน่วยงานรัฐ พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 ที่กำหนดการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในการครอบครองของสถาบันการเงิน หรือพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ที่มีประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553 เป็นต้น แต่ในภาพรวมแล้วกฎหมายที่มีอยู่ยังไม่ครอบคลุมหน่วยงานทั้งหมดที่มีการจัดเก็บข้อมูลส่วนบุคคล รวมถึงกลไกการคุ้มครองข้อมูลส่วนบุคคลในกฎหมายหลายฉบับก็ยังไม่ชัดเจนและไม่เป็นไปตามมาตรฐานสากลสำหรับภาครัฐนั้น

เมื่อพิจารณาถึงการดำเนินการของหน่วยงานของรัฐตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง การคุ้มครองข้อมูลส่วนบุคคลก็พบว่ามีหน่วยงานที่ส่งแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลให้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ตรวจพิจารณาไม่มากนัก ทั้งที่เมื่อประเมินจากปริมาณการครอบครองข้อมูลส่วนบุคคลของภาครัฐจะพบว่าหน่วยงานส่วนใหญ่มีการจัดเก็บข้อมูลของประชาชนไว้ค่อนข้างมาก ซึ่งหากมีภัยคุกคามหรือข้อผิดพลาดเกิดขึ้นแล้วก็อาจส่งผลต่อประเทศในภาพรวมได้ ปัญหาเหล่านี้จึงเป็นปัญหาที่ทุกภาคส่วนต้องหันมาให้ความสำคัญและร่วมมือกันอย่างจริงจัง โดยภาครัฐต้องมีมาตรการที่ให้ความคุ้มครองสิทธิในความเป็นส่วนตัวกรณี Big Data แก่ประชาชนอย่างทั่วถึง ส่วนภาคเอกชนก็อาจมีการนำนโยบายกำกับดูแลตัวเอง (Self-Regulation) ตามหลักของกฎหมายต่างประเทศ ด้วยการส่งเสริมให้ผู้ใช้เว็บไซต์เครือข่ายสังคมตระหนักถึงความสำคัญของสิทธิในความเป็นส่วนตัว หรือการใช้มาตรการทางเทคนิคต่าง ๆ เช่น การปรับตั้งค่าความเป็นส่วนตัว (Setting Privacy) ในเว็บไซต์เครือข่ายสังคม เพื่อลดปัญหาการละเมิดสิทธิในความเป็นส่วนตัวกรณี Big Data และสุดท้ายคือภาคประชาชนเองที่ต้องตระหนักรู้และให้ความสำคัญกับสิทธิในความเป็นส่วนตัวของบุคคลอันเป็นสิทธิขั้นพื้นฐานของตนเอง หากได้รับความร่วมมือจากทุกภาคส่วนแล้ว ก็จะช่วยให้มาตรการต่าง ๆ ในการนำมาใช้ป้องกันปัญหาการละเมิดสิทธิในความเป็นส่วนตัว และการคุ้มครอง Big Data มีประสิทธิภาพมากยิ่งขึ้น และลดความเสียหายที่จะเกิดขึ้นต่อประชาชนและประเทศไทยได้

แต่ทั้งนี้ เนื่องจากร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... ฉบับปัจจุบันได้กำหนดคำนิยามศัพท์ของคำว่า “ข้อมูลส่วนบุคคล” ไว้ไม่ชัดเจน ซึ่งอาจทำให้เกิดปัญหาว่า ข้อมูลส่วนบุคคลตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... นี้ มีความหมายและขอบเขตกว้างขวางเพียงใด สามารถประยุกต์ใช้กับกรณีข้อมูล Big Data หรือไม่ เนื่องจากไม่มีการบัญญัติไว้เป็นการเฉพาะ เพียงแต่บัญญัติไว้รวมเป็นคำว่า “ข้อมูลส่วนบุคคล” เพราะฉะนั้น มาตรการคุ้มครองข้อมูลส่วนบุคคลแต่ละประเภทจึงต้องมีมาตรการคุ้มครองที่แตกต่างกัน ซึ่งควรจะกำหนดไว้เป็นการเฉพาะ ทั้งนี้ กฎหมายไทยอาจยังกำหนดมาตรการคุ้มครองไว้ไม่เข้มงวดและยังไม่มีความเป็นระบบมากนักหากเทียบกับกฎหมายของต่างประเทศ ซึ่งจากสภาพปัญหาดังกล่าวยังส่งผลต่อผู้ที่ต้องปฏิบัติตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... ด้วย ไม่ว่าจะเป็นเจ้าของข้อมูล ผู้ใช้ข้อมูล และผู้ควบคุมข้อมูล เนื่องจากร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... มีความไม่ชัดเจนตามประเด็นที่กล่าวข้างต้นก็จะส่งผลต่อผู้ที่ต้องปฏิบัติตามกฎหมายดังกล่าวซึ่งอาจไม่เข้าใจถึงเจตนารมณ์ที่แท้จริงของกฎหมายว่าต้องการคุ้มครองข้อมูลส่วนบุคคลในเรื่องใด และต้องการคุ้มครองข้อมูลส่วนบุคคลเรื่องใดเป็นพิเศษ

ฉะนั้น จึงเห็นว่าร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...ของประเทศไทย ควรที่กำหนดถึงการคุ้มครองข้อมูลส่วนบุคคลโดยกำหนดให้สามารถประยุกต์ใช้ได้กับกรณี Big Data ไว้ด้วย

โดยการบัญญัติกฎหมายและให้คำจำกัดความโดยยึดหลักความเป็นกลางทางเทคโนโลยี (Technological Neutrality) เพื่อรองรับการเปลี่ยนแปลงของเทคโนโลยีที่สามารถเกิดขึ้นได้ตลอดเวลา รวมถึงกำหนดบทลงโทษของการละเมิดข้อมูลส่วนบุคคล และการรักษาความมั่นคงปลอดภัยของข้อมูลไว้ให้สามารถประยุกต์ใช้ได้กับด้วย ควรมีมาตรการการรักษาความมั่นคงปลอดภัยของข้อมูลที่เข้มงวดมากยิ่งขึ้น และมีความเป็นระบบดังเช่นกรณีกฎหมายของต่างประเทศ แต่อย่างไรก็ดี สำหรับประเทศไทยก็ควรที่จะมีการสำรวจความคิดเห็นของประชาชนคนไทยด้วย เนื่องจากการให้ความสำคัญของข้อมูลส่วนบุคคล และความมั่นคงปลอดภัยของข้อมูลของประชากรในแต่ละประเทศย่อมมีความคิดเห็น ประเพณี และวัฒนธรรมที่แตกต่างกันไป ดังนั้น การที่เราจะนำเอาหลักกฎหมายของต่างประเทศมาปรับใช้จึงควรที่จะศึกษาถึงทัศนคติของประชาชนในประเทศไทย และพิจารณาถึงความสมดุลระหว่างสิทธิของเจ้าของข้อมูลที่ควรจะได้รับความคุ้มครองกับผู้ที่ต้องการใช้ข้อมูลส่วนบุคคลด้วย กล่าวคือ การคุ้มครองที่เข้มงวดมากเกินไป หรือหย่อนจนเกินไป อาจทำให้เกิดความไม่สมดุลระหว่างสิทธิของเจ้าของข้อมูลที่ควรจะได้รับความคุ้มครองกับผู้ที่ต้องการใช้ข้อมูลส่วนบุคคล

สำหรับกรณีของประเทศไทย หลังจากได้ทำการศึกษากฎหมายต่าง ๆ ทั้งที่มีผลใช้บังคับอยู่ในปัจจุบันและที่กำลังอยู่ในระหว่างการพิจารณาของรัฐสภา พบว่ากฎหมายที่ให้ความคุ้มครองความเป็นส่วนตัวในข้อมูลส่วนบุคคล (Personal Information) และการรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security) ก็มีการให้ความคุ้มครองในลักษณะเป็นกฎหมายเฉพาะเรื่อง แต่ยังขาดกฎหมายคุ้มครองข้อมูลส่วนบุคคลเพื่อบังคับใช้กับภาคเอกชนเป็นการทั่วไป ดังนั้น ผู้ศึกษาจึงมีความเห็นว่า ควรสนับสนุนให้เร่งมีการออกกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคล และการรักษาความมั่นคงปลอดภัยของข้อมูลที่อยู่ในความครอบครองของเอกชนเป็นการทั่วไป โดยผู้ศึกษาเห็นว่าการออกกฎหมายนั้นจะต้องไม่มีลักษณะเฉพาะเจาะจงเกินไป แต่ควรยึดหลักความเป็นกลางทางเทคโนโลยี (Technological Neutrality) เพื่อรองรับการเปลี่ยนแปลงของเทคโนโลยีที่สามารถเกิดขึ้นได้ตลอดเวลา เนื่องจากในอนาคตนอกจาก Big Data แล้ว เทคโนโลยีใหม่ ๆ จะยังคงได้รับการพัฒนาอย่างต่อเนื่อง ดังนั้น สิ่งที่เหมาะสมคือการออกกฎหมายที่สามารถนำมาปรับใช้กับการคุ้มครองข้อมูลส่วนบุคคล และความมั่นคงปลอดภัยของข้อมูลได้กับทุก ๆ กรณีโดยไม่จำกัด

5.2 ข้อเสนอแนะ

เมื่อพิจารณาจากร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย กรณีความเป็นส่วนตัว และความมั่นคงปลอดภัยของข้อมูล พบว่ามีทั้งประเด็นที่ถือว่าสามารถประยุกต์ใช้กับการคุ้มครอง Big Data ได้ แต่ก็มีประเด็นบางประการที่อาจจะเป็นสิ่งที่น่านำมา

พิจารณาเพื่อที่จะปรับเปลี่ยนและแก้ไขร่างพระราชบัญญัติดังกล่าวเพื่อให้สามารถประยุกต์ใช้ได้กับการคุ้มครอง Big Data ต่อไปคือ

1) ประเด็นเรื่องขอบเขตการใช้บังคับ จะพบว่าร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลถือว่ามีขอบเขตที่มีลักษณะทั่วไป คือมีขอบเขตที่ครอบคลุมในการใช้บังคับทั้งเรื่องการประมวลผลสัญชาติของเจ้าของข้อมูล ฯลฯ ทำให้การใช้บังคับไม่ใช้เฉพาะแต่เรื่องใดเรื่องหนึ่งมีลักษณะเป็นกฎหมายทั่วไปอย่างประเทศอังกฤษตามแนวทางของสหภาพยุโรป แต่ขอบเขตการใช้บังคับของประเทศสหรัฐอเมริกานั้นเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่มีลักษณะเฉพาะทำให้สหภาพยุโรปไม่ยอมรับในตัวกฎหมายดังกล่าวของสหรัฐอเมริกา จึงได้ทำข้อตกลงระหว่างประเทศที่เรียกว่า The Safe Harbor Agreement ขึ้นใช้บังคับ เนื่องจากมาตรฐานของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหรัฐอเมริกามีข้อบกพร่องบางประการทำให้การคุ้มครองไม่เพียงพอต่อความต้องการของสหภาพยุโรปจนเกิดแรงกดดันให้ทำข้อตกลงระหว่างประเทศดังกล่าว จากที่กล่าวมาถือว่าเป็นบทเรียนที่สำคัญที่ประเทศไทยจำเป็นต้องนำมาพิจารณาในการประกอบการร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล เพื่อที่จะให้นานาประเทศยอมรับในตัวร่างพระราชบัญญัติดังกล่าว เพราะถ้าหากกฎหมายที่กำลังจะใช้บังคับไม่เป็นที่ยอมรับ ก็อาจจะมีความจำเป็นที่จะต้องทำข้อตกลงระหว่างประเทศเพิ่มขึ้น และส่งผลกระทบต่อการทำธุรกิจระหว่างประเทศ ทำให้ต่างชาติไม่มั่นใจที่จะเข้ามาลงทุนเมื่อการคุ้มครองข้อมูลส่วนบุคคลไม่มีประสิทธิภาพที่จะคุ้มครองข้อมูลส่วนบุคคลได้

2) ประเด็นเรื่องการแก้ไขเพิ่มเติมกฎหมาย โดยการเสนอให้มีการแก้ไขเพิ่มเติมกฎหมายที่ให้ความคุ้มครองสิทธิความเป็นอยู่ส่วนตัวที่มีผลบังคับใช้เป็นการทั่วไปอยู่แล้ว อาทิ การเพิ่มเติมข้อความหรืออนุมาตราในบทบัญญัติที่เกี่ยวข้องให้สามารถปรับใช้กับกรณี Big Data หรือเทคโนโลยีอื่นในทำนองเดียวกันเป็นการเฉพาะได้ด้วย ยกตัวอย่างเช่น การใช้หลักให้ภาคเอกชนควบคุมกันเอง (Self-regulations) ในประเทศสหรัฐอเมริกา โดยการให้ภาคเอกชนนำหลัก Fair Information Practice[1] ไปเป็นแนวทางในการออกกฎเกณฑ์ แนวปฏิบัติ หรือประมวลจริยธรรมเพื่อใช้ควบคุมกันเองในองค์กร

3) ประเด็นเรื่องการตีความกฎหมาย โดยการพยายามตีความกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่มีอยู่ให้สามารถนำมาประยุกต์ใช้กับความเป็นส่วนตัว และความมั่นคงปลอดภัยของข้อมูลใน Big Data เช่น หลักข้อจำกัดในการรวบรวมข้อมูล หลักคุณภาพของข้อมูล การกำหนดวัตถุประสงค์ในการจัดเก็บ เป็นต้น รวมทั้งอาศัยอำนาจแห่งกฎหมายว่าด้วยการคุ้มครอง

[1] Fair Information Practice Principles (FIPPs), **NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE** [Online], Available from http://www.nist.gov/nstic/NSTIC-FIPPs.pdf.

ข้อมูลส่วนบุคคล ออกแนวปฏิบัติเพื่อแนะนำวิธีการใช้การตีความกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ความเป็นส่วนตัว และความมั่นคงปลอดภัยของข้อมูลใน Big Data ด้วย

4) ประเด็นการเปิดเผยข้อมูล ถือว่าร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลควรจะกำหนดหลักการคุ้มครองข้อมูลส่วนบุคคลไว้เป็นการทั่วไป โดยข้อมูลส่วนบุคคลจะต้องได้รับการปกป้องไว้ มิให้ใครสามารถที่จะเข้าถึง หรือนำเอาข้อมูลส่วนบุคคลไปใช้จนก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลได้ ตามหลักการรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security) และร่างพระราชบัญญัติดังกล่าวนี้ควรจะกำหนดข้อยกเว้นไว้ที่สามารถเปิดเผยข้อมูลส่วนบุคคลได้ หากมิได้ปฏิบัติตามข้อยกเว้นแล้วเปิดเผยข้อมูลส่วนบุคคลก็ถือว่าเป็นการละเมิดสิทธิของเจ้าของข้อมูล

5) ประเด็นในการฟ้องร้องคดี เมื่อมองในแง่องค์กรที่ทำหน้าที่ควบคุมและบังคับให้เป็นไปตามกฎหมาย ประเทศไทยไม่นิยมการฟ้องร้องอย่างประเทศสหรัฐอเมริกา ซึ่งร่างพระราชบัญญัติดังกล่าวควรจะกำหนดให้เจ้าของข้อมูลผู้เสียหายยื่นคำร้องต่อคณะกรรมการ และสามารถที่จะยื่นฟ้องต่อศาลเองได้ โดยไม่จำเป็นต้องผ่านองค์กรที่ทำหน้าที่ควบคุม เพราะหากเกิดการปฏิบัติล่าช้าหรือมีการทุจริตขึ้นแล้ว จะทำให้ผู้ที่เสียหายไม่ได้รับความเป็นธรรมในการดำเนินการเรียกร้องสิทธิที่ถูกละเมิดข้อมูลส่วนบุคคล

6) ประเด็นเรื่องการโอนข้อมูลส่วนบุคคลระหว่างประเทศ ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลควรจะกำหนดหลักห้ามการโอนข้อมูลไปยังประเทศอื่น เว้นแต่ประเทศที่จะโอนไปนั้นจะมีกฎหมายที่คุ้มครองข้อมูลส่วนบุคคลที่ไม่น้อยกว่าร่างพระราชบัญญัตินี้ แต่ก็จำกัดแต่เฉพาะกฎหมายเท่านั้น ซึ่งมีสิ่งที่น่าพิจารณาว่าหากเป็นมาตรการอื่นที่มิใช่กฎหมายแล้วก็อาจจะทำให้การคุ้มครองข้อมูลนั้นอยู่ในระดับที่ไม่เพียงพอ ซึ่งตามกฎหมายคุ้มครองข้อมูลของสหภาพยุโรปนั้นเน้นว่าจะต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคลที่เพียงพอถึงจะโอนข้อมูลระหว่างประเทศได้ ซึ่งสามารถตีความได้ว่ามีทั้งมาตรการที่เป็นกฎหมายและมาตรการอื่นที่สามารถคุ้มครองข้อมูลส่วนบุคคลได้ ฉะนั้นหากประเทศไทยสามารถบัญญัติกฎหมายมีเนื้อหาและกลไกการบังคับใช้ที่มีประสิทธิภาพซึ่งสอดคล้องกับกฎหมายของสหภาพยุโรปแล้ว ก็สามารถหลีกเลี่ยงการเกิดปัญหาอันเนื่องมาจากการรับโอนข้อมูลส่วนบุคคล ซึ่งจะเป็นปัจจัยที่สำคัญที่จะส่งผลกระทบต่อการประกอบการค้าระหว่างประเทศ

7) ประเด็นเรื่ององค์กรที่ทำหน้าที่ควบคุม จะเห็นว่าร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลกำหนดหลักเกณฑ์เกี่ยวกับคณะกรรมการให้คัดเลือกมาจากหลายสาขา เนื่องจากข้อมูลส่วนบุคคลส่วนใหญ่ถูกนำมาใช้กับแวดวงสุขภาพ สาธารณสุข ระบบการขนส่ง การคมนาคม การศึกษา กฎหมาย จึงคัดเลือกคณะกรรมการเหล่านี้ จากทั้งทางด้านการแพทย์ วิศวกรรมศาสตร์ คอมพิวเตอร์ เศรษฐศาสตร์ นิติศาสตร์ เป็นต้น การที่คณะกรรมการมีความชำนาญในหลาย ๆ สาขาทำให้การทำงานเกิดประสิทธิภาพมาก อีกทั้งการดำเนินงานของคณะกรรมการก็มีความเป็นอิสระ ไม่ขึ้นต่อ

บุคคลใดบุคคลหนึ่ง ทำให้การดำเนินงานมีอำนาจที่เด็ดขาด จนสามารถปฏิบัติงานเป็นประโยชน์ต่อประเทศชาติและเจ้าของข้อมูลส่วนบุคคลที่ถูกประมวลผล ทำให้เป็นที่ยอมรับจากเจ้าของข้อมูลที่เป็นประชาชนในประเทศไทยและนักลงทุนหรือผู้ประกอบกิจการจากต่างประเทศที่ได้รับความคุ้มครองข้อมูลจากร่างพระราชบัญญัติดังกล่าว

8) ประเด็นเรื่องบทบาทของภาคเอกชน ควรจะสนับสนุนให้ภาคเอกชนมีบทบาทอย่างต่อเนื่องในการพัฒนาเทคโนโลยี เพื่อเป็นการคุ้มครองประชาชน และจัดตั้งองค์กรภาคเอกชนที่ทำหน้าที่รับรองคุณภาพของจัดทำกลไกการกำกับดูแลตนเอง และพัฒนาเทคโนโลยีเพื่อเพิ่มความมั่นคงปลอดภัยให้กับข้อมูลส่วนบุคคล รวมถึงการมีส่วนร่วมของตัวแทนของผู้ประกอบการ และตัวแทนของประชาชนในการพัฒนามาตรการในการคุ้มครองข้อมูลส่วนบุคคลให้มีประสิทธิภาพ รวมถึงกฎเกณฑ์วิธีการระงับข้อพิพาท และขั้นตอนการเรียกร้องสิทธิของผู้บริโภค

9) ประเด็นเรื่องการร่วมกันของภาคเอกชนและภาครัฐ ควรจะสนับสนุนให้ภาคเอกชนร่วมกับภาครัฐ โดยการเผยแพร่ประชาสัมพันธ์เนื้อหา วัตถุประสงค์ของแนวทางการคุ้มครองข้อมูลส่วนบุคคลให้แพร่หลาย พร้อมทั้งอำนวยความสะดวกแก่ประชาชนให้สามารถตรวจดูข้อมูล ความรู้คำปรึกษา และการให้คำแนะนำในการยื่นข้อร้องเรียนเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล รวมถึงออกกฎหมายให้ภาคเอกชนปฏิบัติตามกฎเกณฑ์ที่ภาครัฐกำหนดขึ้น และร่วมมือกับภาครัฐในการพัฒนากฎหมายให้มีความทันสมัย ให้มีสอดคล้องกับยุคสมัยเพื่อรองรับเทคโนโลยีที่เจริญก้าวหน้า และให้ข้อมูล เบาะแส แก่ภาครัฐ เกี่ยวกับรูปแบบและวิธีการละเมิดความเป็นส่วนตัวในข้อมูลส่วนบุคคล การทุจริตต่าง ๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

ดังนั้น การคุ้มครองข้อมูลใน Big Data มีความสำคัญต่อการทำธุรกรรมทางอิเล็กทรอนิกส์อันสืบเนื่องจากการพัฒนาเทคโนโลยีที่ก้าวหน้าและรวดเร็ว ทำให้ประเทศไทยจำเป็นที่จะต้องมีกฎหมายที่สามารถคุ้มครองข้อมูลใน Big Data ที่มีมาตรฐานและมีประสิทธิภาพในการบังคับใช้ เพื่อทำให้ประชาชนในประเทศไทยยอมรับในกฎหมายคุ้มครองของข้อมูล และสำหรับปัจจุบันการค้าระหว่างประเทศมีความสำคัญมาก จึงจำเป็นต้องบัญญัติกฎหมายให้เป็นที่ยอมรับของนักลงทุนต่างชาติเพื่อสร้างความน่าเชื่อถือในการคุ้มครองข้อมูลส่วนบุคคล ความเป็นส่วนตัว รวมถึงความมั่นคงปลอดภัยของข้อมูลใน Big Data และบัญญัติกฎหมายเป็นที่ยอมรับจากนานาประเทศเพื่อไม่เป็นอุปสรรคต่อการค้าระหว่างประเทศ สิ่งที่เหมาะสมกับประเทศไทย คือ การออกกฎหมายที่สามารถนำมาปรับใช้กับการคุ้มครองข้อมูลส่วนบุคคล ความเป็นส่วนตัว และความมั่นคงปลอดภัยของข้อมูลได้กับทุก ๆ กรณีโดยไม่จำกัด รวมถึงกรณี Big Data ด้วย เพื่อเป็นการรองรับการเปลี่ยนแปลงของของเทคโนโลยีที่สามารถเกิดขึ้นใหม่ได้ตลอดเวลา

บรรณานุกรม

คัชชิดา มีท่อธาร และณัฐวรรธน์ สุขวงศ์ตระกูล. (2555). *บทบาทของกฎหมายเทคโนโลยีสารสนเทศ*. ม.ป.ท.: สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน).

คณาธิป ทองรวีวงศ์. (2552). *มาตรการทางกฎหมายในการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว: ศึกษาเปรียบเทียบการเฝ้าติดตามคุกคาม (Stalking) กับการถ่ายภาพโดยมิได้รับรู้และยินยอม*. ม.ป.ท.: สำนักงานกิจการยุติธรรมและสภานิติศึกษา.

จันทจิรา เอี่ยมมยุรา. (2547). การคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย. *วารสารนิติศาสตร์*, *34*, 627-652.

จันทจิรา เอี่ยมมยุรา. (2547). แนวคิดและหลักการยกร่างกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย. *วารสารนิติศาสตร์*, *34*, 653-683.

ชูชาติ หฤไชยะศักดิ์. (2557). *What is Big Data?*. สืบค้นจาก http://www.datamininginnovation.com/wp-content/uploads/2014/02/What_is_big_data.pdf.

ชาญชัย แสวงศักดิ์. (2540). *สาระน่ารู้พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540*. กรุงเทพฯ: วิญญูชน.

ชาตรี ส่งสัมพันธ์. (2552). *อาชญากรรมคอมพิวเตอร์: ศึกษาวิเคราะห์การเข้าถึงโดยมิชอบ*. วิทยานิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์.

ณรงค์ฤทธิ์ มโนมัยพิบูลย์. (2556). *“Big Data” is (now) all around Big Data*. สืบค้นจาก http://www.g-able.com/portal/page/portal/g-able/thai/it_talks/Y2013/it_talks_V34_02 /G-Magz_V34_2.pdf.

นคร เสรีรักษ์. (2550). *กรอบการคุ้มครองข้อมูลส่วนบุคคลของเอเปค*. สืบค้นจาก http://www.fpps.or.th/news.php?detail=n1240887531.news.

บุญสิทธิ์ บุญโพธิ์. (2553). สื่อมวลชนกับการละเมิดสิทธิส่วนบุคคล. *วารสารนักบริหาร*, 86-88.

ปัญหาและมาตรการทางกฎหมายในการรับรอง และคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว (Right to Privacy). (ม.ป.ป.). ม.ป.ท.: สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ.

ปฏิวัติ อุ่นเรือน. (ม.ป.ป.). *ปัญหาการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลระหว่างประเทศ Privacy Policy & Trustmark กลไกลการคุ้มครองข้อมูลส่วนบุคคลกับการสร้างความน่าเชื่อถือในการทำ e-Business*. สืบค้นจาก http://www.nectec.or.th/pub/books/privacy-policy.pdf.

ปทีป เมธาคุณวุฒิ และอภิรัตน์ เพชรศิริ. (2539). *แนวทางในการออกกฎหมายคุ้มครองข้อมูลสารสนเทศส่วนบุคคลในประเทศไทย*. ม.ป.ท.: สำนักงานคณะกรรมการวิจัยแห่งชาติ.

ปิยะพร วงศ์เบี้ยสัจจ์. (2551). *การเปิดเผยข้อมูลส่วนบุคคลโดยธนาคารพาณิชย์กับมาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคล*. วิทยานิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยธุรกิจบัณฑิต.

ปรีดี เกษมทรัพย์. (2531). *นิติปรัชญา* (พิมพ์ครั้งที่ 2). กรุงเทพฯ: มิตรนราการพิมพ์.

ประสิทธิ์ ปิวาวัฒนพานิช. (2547). กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกาและประเทศออสเตรเลีย, *วารสารนิติศาสตร์*, *34*, 535-556.

เพชรรัตน์ จงปัญญาประพันธ์. (2546). ความสำคัญของกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล. *วารสารนิติศาสตร์*, *33*, 821-830.

พสุ เดชะรินทร์. (2556). *Big Data หรืออภิมหาข้อมูล*. สืบค้นจาก http://library.acc.chula.ac.th/PageController.php?page=FindInformation/ArticleACC/2556/Pasu/BangkokBiznews/B2901131.

สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์. (2547). *แนวทางการจัดทำกฎหมายคุ้มครองข้อมูลส่วนบุคคล* (พิมพ์ครั้งที่ 2). กรุงเทพฯ: ศูนย์เทคโนโลยีอีเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ.

สุรางคณา วายุภาพ. (2557 ก). *นโยบายด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานภาครัฐ*. สืบค้นจาก http://ega.or.th/Files/20140515101917.pdf.

สุรางคณา วายุภาพ. (2557 ข). *ETDA ร่วมเวที "ไซเบอร์: ภัยคุกคามต่อความมั่นคงของชาติ" เผยแนวโน้มและทิศทาง Cyber Security ของไทย และบทบาท National CERT*. สืบค้นจาก https://www.etda.or.th/etda_website/content/etda-cybersecurity-national-cert.html.

สหภาพโทรคมนาคมระหว่างประเทศ (ITU). (2557). *ผลสำรวจรายงานประจำปีดัชนีชี้วัดสังคมสารสนเทศปี 2557*. สืบค้นจาก http://www.innnews.co.th/shownews/show?newscode =581921.

ศศิภา เรืองฤทธิ์ชาญกุล. (2553). *มาตรการทางกฎหมายในการควบคุมการเผยแพร่ข่าวผู้เสียหายในความผิดเกี่ยวกับเพศ*. วิทยานิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์.

อุดม รัฐอมฤต, นพนิธิ สุริยะ และบรรเจิด สิงคะเนติ. (2544). *การอ้างศักดิ์ศรีความเป็นมนุษย์หรือใช้สิทธิเสรีภาพของบุคคลตามมาตรา 28 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540*. กรุงเทพฯ: นานาสิ่งพิมพ์.

IT News. (2555). *ระบบใหม่และ Oracle Big Data Connectors ช่วยให้ได้รับประโยชน์จากข้อมูลขนาดใหญ่ ภายในองค์กร*. สืบค้นจาก http:// www.blognone.com/node/29312.

อำนาจ เนตยสุภา. (2551). การคุกคามทางอินเตอร์เน็ต. *วารสารวิชาการรพีเซนต์จอห์น*.

MK. (2555). *ยุทธศาสตร์ Big Data และ Enterprise Storage ของ Dell*. สืบค้นจาก http://www.blognone.com/ node/33147.

OSTC. (2555). *MEXT & NSF ร่วมวิจัยด้าน Big Data และภัยธรรมชาติ*. สืบค้นจาก http://www.ostc.thaiembdc.org/test2012/stnews_ July12_1.

Bansal, S., & Rana, A. (2014). *International Journal of Advanced Research in Computer Science and Software Engineering: Transitioning from Relational Databases to Big Data*. Retrieved from http://www.ijarcsse.com/docs/papers/Volume_4/1_January2014/V4I1-0320.pdf.

Cull, B. (2013). 3 ways big data is transforming government. *FCW: The Business of Federal Technology*. Retrieved from http://fcw.com/articles/2013/09/25/big-data-transform-government.aspx.

Dell Global Technology Adoption Index. (2014). *Revealing decision points around technology adoption, use and benefits in organizations*. Retrieved from https://kapost-files-prod.s3.amazonaws.com/uploads/direct/1415199563-23-1043/Executive_Summary_Global_ Technology_Adoption_Index.PDF.

Dumbill, E. (2012). *What is big data?: An introduction to the big data landscape*. Retrieved from http://radar.oreilly.com/2012/01/what-is-big-data.html.

EPIC. (2014). *Request for Information: Big Data and the Future of Privacy*. Retrieved from https://epic.org/privacy/big-data/EPIC-OSTP-Big-Data.pdf.

Fair Information Practice Principles (FIPPs). (n.d.). *NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE*. Retrieved from http://www.nist.gov/nstic/NSTIC-FIPPs.pdf.

Fayyad, U., Piatetsky-Shapiro, G., & Smyth, P. (1996). *From Data Mining to Knowledge Discovery in Databases*. Retrieved from http://www.csd.uwo.ca/faculty/ling/cs435 /fayyad.pdf.

Federal Big Data Commission. (n.d.). Demystifying BIG DATA, *TechAmerican Foundation*, 11. Retrieved from https://www304.ibm.com/industries/publicsector/fileserve?contentid=239170.

ICO Information Commissioner's Office. (2014). *Big Data and data protection*. Retrieved from http://ico.org.uk/news/latest_news/2014/~/media/documents/library/Data_Protection/Practical_application/big-data-and-data-protection.pdf.

Informatica. (2012). *Big Data for the Telecommunications Industry: Minimize Data Cost, Maximize Data Value*. Retrieved from http://www.informatica.com/Images/02190_big-data-telecommunications_eb_en-US.pdf.

Laney, D. (2013). *3D Data Management: Controlling Data Volume, Velocity, and Variety*. Retrieved from http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf.

Melodia, M., & Smith, R. (2012). Defending BIG DATA, *LTN LAW TECHNOLOGY NEWS*. Retrieved from http://www.reedsmith.com/files/News/f6b538a3-7681-40a2-b2bd-ab653940bab5/Presentation/NewsAttachment/f55071a4-b28a-49df-a396-ac3f4403205c/LTN%20October%202012%20-%20Data%20Privacy.pdf.

Moed, H. (2012). *Research Trends: Special Issue on Big Data*. Retrieved from http://www.researchtrends.com/wp-content/uploads /2012/09/Research_Trends_Issue30.pdf.

ประวัติผู้เขียน

ชื่อ นามสกุล	นางสาว ปิยะภัสร์ โรจน์รัตนวาณิชย์
อีเมล	phonglapas@gmail.com
ประวัติการศึกษา	นิติศาสตรบัณฑิต มหาวิทยาลัยแม่ฟ้าหลวง

มหาวิทยาลัยกรุงเทพ

ข้อตกลงว่าด้วยการอนุญาตให้ใช้สิทธิในวิทยานิพนธ์/สารนิพนธ์

วันที่ 6 เดือน กุมภาพันธ์ พ.ศ. 2558

ข้าพเจ้า (~~นาย/นาง~~/นางสาว) ปิยะภัสร์ โรจน์รัตนวาณิชย์ อยู่บ้านเลขที่ 43
ซอย ปุณณวิถี 12 ถนน สุขุมวิท 101 ตำบล/แขวง ปากน้ำ
อำเภอ/เขต พระโขนง จังหวัด กรุงเทพมหานคร รหัสไปรษณีย์ 10260
เป็นนักศึกษาของมหาวิทยาลัยกรุงเทพ รหัสประจำตัว 7550400035
ระดับปริญญา ☐ ตรี ☑ โท ☐ เอก
หลักสูตร นิติศาสตรมหาบัณฑิต สาขาวิชา - คณะ นิติศาสตร์
ซึ่งต่อไปนี้เรียกว่า **"ผู้อนุญาตให้ใช้สิทธิ"** ฝ่ายหนึ่ง และ

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

ผู้อนุญาตให้ใช้สิทธิ และ ผู้ได้รับอนุญาตให้ใช้สิทธิ ตกลงทำสัญญากันโดยมีข้อความดังต่อไปนี้

ข้อ 1. ผู้อนุญาตให้ใช้สิทธิขอรับรองว่าเป็นผู้สร้างสรรค์และเป็นผู้มีสิทธิแต่เพียงผู้เดียวในงานสารนิพนธ์/วิทยานิพนธ์หัวข้อ แนวทางการคุ้มครองข้อมูลใหญ่ Big Data : ศึกษาประเด็นความเป็นส่วนตัว และ ความมั่นคงปลอดภัยของข้อมูล

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

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

ข้อ 3. หากกรณีมีข้อขัดแย้งในปัญหาลิขสิทธิ์ในสารนิพนธ์/วิทยานิพนธ์ระหว่างผู้อนุญาตให้ใช้สิทธิกับบุคคลภายนอกก็ดี หรือระหว่างผู้ได้รับอนุญาตให้ใช้สิทธิกับบุคคลภายนอกก็ดี หรือมีเหตุขัดข้องอื่นๆ เกี่ยวกับลิขสิทธิ์ อันเป็นเหตุให้ผู้รับอนุญาตให้ใช้สิทธิไม่สามารถนำงานนั้นออกทำซ้ำ เผยแพร่ หรือโฆษณาได้ ผู้อนุญาตให้ใช้สิทธิยินยอมรับผิดและชดใช้ค่าเสียหายแก่ผู้ได้รับอนุญาตให้ใช้สิทธิในความเสียหายต่าง ๆ ที่เกิดขึ้นแก่ผู้ได้รับอนุญาตให้ใช้สิทธิทั้งสิ้น

สัญญานี้ทำขึ้นสองฉบับ มีข้อความเป็นอย่างเดียวกัน คู่สัญญาได้อ่านและเข้าใจข้อความในสัญญานี้โดยละเอียดแล้ว จึงได้ลงลายมือชื่อให้ไว้เป็นสำคัญต่อหน้าพยาน และเก็บรักษาไว้ฝ่ายละฉบับ

ลงชื่อ  ผู้อนุญาตให้ใช้สิทธิ

(ปิยะภัชร์ โรจน์รัตนวาณิชย์)

ลงชื่อ  ผู้ได้รับอนุญาตให้ใช้สิทธิ

(ดร.ชนันนา รอดสุทธิ)

ผู้อำนวยการสำนักหอสมุดและศูนย์การเรียนรู้

ลงชื่อ  พยาน

(ผู้ช่วยศาสตราจารย์ ดร.ศิวพร หวังพิพัฒน์วงศ์)

คณบดีบัณฑิตวิทยาลัย

ลงชื่อ  พยาน

(ผู้ช่วยศาสตราจารย์ ดร.อรรยา สิงห์สงบ)

ผู้อำนวยการหลักสูตร/ ผู้รับผิดชอบหลักสูตร