ความเป็นส่วนตัวของข้อมูลในยุคดิจิทัล
Data Privacy in the Digital Age

นิกร โภคอุดม[1]
Nikorn Pokudom[1]
[1]คณะวิศวกรรมศาสตร์ มหาวิทยาลัยอีสเทิร์นเอเชีย
[1]School of Engineering, Eastern Asia University
Received: March 30, 2020
Revised: July 1, 2020
Accepted: July 8, 2020

บทคัดย่อ

บทความวิชาการนี้มีวัตถุประสงค์ในการให้ความรู้เกี่ยวกับความเป็นส่วนตัวของข้อมูล ซึ่งความเป็นส่วนตัวของข้อมูล นั้นเกี่ยวข้องกับความสัมพันธ์ระหว่างการรวบรวมและการเผยแพร่ ข้อมูล เทคโนโลยี ความคาดหวังของประชาชนเกี่ยวกับความเป็นส่วนตัวและความรู้เกี่ยวกับกฎหมายความเป็นส่วนตัว โดยเกี่ยวข้องกับกฎระเบียบการจัดเก็บและการใช้ ข้อมูลส่วนบุคคล ข้อมูลด้านสุขภาพส่วนบุคคลและข้อมูลทางการเงินของบุคคล ซึ่งรัฐบาล องค์กรเอกชน หรือบุคคลอื่นสามารถรวบรวมได้ และยังหมายถึงข้อมูลใช้ในภาคธุรกิจเช่นความลับทางการค้า เพื่อเป็นการป้องกันปัญหาเรื่องความเป็นส่วนตัวของข้อมูลรั่วไหลสหภาพยุโรปจึงได้ออกกฎหมายการคุ้มครองข้อมูลส่วนบุคคล เรียกว่า “GDPR” (EU General Data Protection Regulation--GDPR) เพื่อกำหนดให้องค์กรต่าง ๆ ต้องมีมาตรการรักษาความปลอดภัยของข้อมูลที่จัดเก็บไว้ ซึ่งประเทศไทยได้นำกฎหมายนี้มาเป็นแนวทางสำหรับออกเป็นกฎหมายเพื่อการคุ้มครองข้อมูลส่วนบุคคลของประชาชนในประเทศเรียกว่า “พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562” และอธิบายแนวทางการปฏิบัติให้กับองค์กรและเจ้าของข้อมูลซึ่งสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

คำสำคัญ: ข้อมูลส่วนบุคคล, ความเป็นส่วนตัวของข้อมูล, การคุ้มครองข้อมูล

Abstract

This academic article aimed to provide knowledge of data privacy. Data privacy relates to the relationship between the collection and dissemination of information, technology, privacy expectations of people and knowledge of privacy laws in relation to the rules of storage and the use of personal information, personal health and personal financial information This data can be collected by governments, private organizations, or others. Moreover, it is also meant for data used in business sectors, such as trade secrets. In order to prevent the privacy concerns of data breaches, the European Union issued a law on personal data protection called “GDPR” (EU General Data Protection Regulation--GDPR). The rule requires organizations to have security measures on stored data. Thailand has adopted this law as a guideline for making laws to protect the personal data of people in the country, called “Personal data Protection Act b.e.2562”. In this Act, details of various regulations were given to organizations and data owners to be able to comply with the Personal Data Protection Act.

Keywords: personal data, data privacy, data protection.

บทนำ

การเติบโตและพัฒนาการด้านเทคโนโลยีอินเทอร์เน็ตปัจจุบันมีความก้าวหน้าเป็นอย่างมาก ผู้คนสามารถเข้าถึงเทคโนโลยีดังกล่าวได้อย่างกว้างขวางผ่านทางเครื่องคอมพิวเตอร์ อุปกรณ์สมาร์ทโฟนและอุปกรณ์ IoT ประชาชนชาวไทยปัจจุบันมีการดำเนินชีวิตที่ใช้ประโยชน์จากเทคโนโลยีอินเทอร์เน็ตอย่างมากมายทั้งด้านการศึกษา การทำงาน การเงินและธนาคารและการใช้งานสื่อสังคมออนไลน์ เป็นต้น ผู้บริโภคนอกจากจะเป็นผู้ที่ใช้งานเทคโนโลยีแล้วในขณะเดียวกันนั้นก็ยังเป็นผู้ที่สร้างข้อมูลส่วนตัวบันทึกลงไประบบด้วยทั้งทางตรง เช่น ข้อมูลชื่อผู้ใช้ ความชอบ ข้อมูลบัตรเครดิตและอีเมล เป็นต้น และข้อมูลตามอ้อมที่ผู้ใช้ไม่ได้เป็นผู้ใส่ข้อมูลเข้าไปโดยตรง เช่น หมายเลขไอพีที่ใช้งาน ตำแหน่ง GPS และประวัติการเข้าดูโฆษณา เป็นต้น ข้อมูลเหล่านี้มีความสำคัญอย่างมากต่อการวางแผนดำเนินกิจกรรมทั้งของภาครัฐและภาคเอกชน โดยเฉพาะส่วนของภาคเอกชนนั้นมีความต้องการได้ข้อมูลของผู้บริโภคให้ได้มากที่สุดเพื่อประโยชน์ต่อการวางแผน การวิเคราะห์และตัดสินใจในการดำเนินการทางธุรกิจ ในยุคก่อนที่ระบบคอมพิวเตอร์จะถูกนำมาใช้ในกิจกรรมทางธุรกิจอย่างมากนั้น บริษัทต่าง ๆ จะได้ข้อมูลของผู้บริโภคผ่านทางการทำแบบสำรวจหรือการทำแบบสอบถามเพื่อจัดเก็บข้อมูลของผู้บริโภคเพื่อนำมาทำการวิจัยตลาด แต่การสำรวจแบบนี้ก็พบปัญหาเกี่ยวกับจำนวนข้อมูลอาจเก็บได้ไม่มากและได้ข้อมูลที่ไม่ถูกต้องเนื่องจากบางครั้งผู้ตอบแบบสอบถามก็ให้ข้อมูลที่ไม่เป็นความจริง ปัจจุบันเมื่อระบบคอมพิวเตอร์เข้ามามีบทบาทมากขึ้นการจัดเก็บข้อมูลของผู้บริโภคทำได้อย่างสะดวกและรวดเร็วมาก สามารถเก็บข้อมูลได้ตลอดเวลาและคอมพิวเตอร์สามารถประมวลผลข้อมูลที่เกี่ยวข้องกับผู้บริโภคได้อย่างมีประสิทธิภาพ

ข้อมูลจึงมีความสำคัญอย่างมากต่อการดำเนินธุรกิจในปัจจุบัน การได้มาซึ่งข้อมูลของผู้บริโภคจึงมีความสุ่มเสี่ยงต่อการละเมิดความเป็นส่วนตัวของผู้บริโภค เช่น การนำข้อมูลของผู้บริโภคที่ให้ไว้กับบริษัทไปใช้ประโยชน์ทั้งการใช้ข้อมูลส่วนบุคคลไปใช้ประมวลผล การเปิดเผยข้อมูลให้กับบริษัทอื่นโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลทำให้เกิดความเสียหายต่อเจ้าของข้อมูลและยังถือว่าเป็นละเมิดต่อสิทธิเสรีภาพของบุคคลอีกด้วย

ปัญหาด้านความเป็นส่วนตัวที่ผู้ใช้งานเทคโนโลยีมักพบมีอยู่ 2 แบบ ได้แก่ แบบแรกคือการบุกรุกเพื่อขโมยข้อมูลซึ่งอาจเกิดจากเหล่าแฮกเกอร์หรือมัลแวร์

คอมพิวเตอร์ที่พยายามขโมยหรือหลอกลวงข้อมูลของผู้ใช้เอาไปใช้ประโยชน์ ซึ่งผู้ใช้งานจะต้องมีความรู้ในการใช้เทคโนโลยีเพื่อป้องกันตนเองจากการใช้งานเทคโนโลยีให้มีความปลอดภัย ปัจจุบันประเทศไทยได้มีการออกพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 (Royal Thai Government Gazette, 2007) และฉบับที่ 2 พ.ศ.2560 (Royal Thai Government Gazette, 2017) เพื่อกำหนดบทลงโทษต่อความผิดดังกล่าว และแบบที่สอง คือ การละเมิดเอาข้อมูลส่วนตัวของผู้ใช้งานจากบริษัทเอกชนต่าง ๆ ที่ผู้ใช้ได้บันทึกหรือใช้งานกับบริษัทเหล่านั้น ไปใช้ประโยชน์ทั้งเพื่อการเมือง การวิเคราะห์พฤติกรรมผู้บริโภค และขายข้อมูลของผู้ใช้ให้กับบุคคลหรือบริษัทอื่นโดยที่ผู้ใช้งานไม่ได้ยินยอม ซึ่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ไม่ได้ครอบคลุมการนำเอาข้อมูลส่วนบุคคลไปใช้โดยไม่ได้รับความยินยอมเนื่องจากเป็นข้อมูลที่ผู้ใช้บันทึกและเก็บไว้บนเครื่องคอมพิวเตอร์เซิร์ฟเวอร์ของผู้ใช้บริการ

ในยุคที่ข้อมูลส่วนบุคคลของผู้บริโภคถูกจัดเก็บไว้ในคลาวด์ (Cloud) ของผู้ให้บริการนั้น โอกาสที่ข้อมูลจะรั่วไหลออกมามีอยู่ตลอดเวลาทั้งที่เกิดจากตัวผู้บริโภคเอง เช่น ขาดความรู้ในการรักษาความปลอดภัยให้กับอุปกรณ์หรือระบบไอทีที่ใช้อยู่ และความประมาทในการใช้งาน เป็นต้น และที่เกิดจากความบกพร่องของระบบขององค์กร หรือผู้ให้บริการด้านไอทีที่ขาดความเอาใจใส่ หรือมีนโยบายการคุ้มครองข้อมูลผู้บริโภคที่ไม่รัดกุมเพียงพอ

การคุ้มครองข้อมูลส่วนบุคคลนั้นสหภาพยุโรปได้ออกกฎหมายฉบับใหม่ที่ เรียกกันว่า “GDPR” (EU General Data Protection Regulation--GDPR) เพื่อนำมาคุ้มครองข้อมูลส่วนบุคคลไม่ให้ถูกละเมิด โดยข้อมูลส่วนบุคคลของสหภาพยุโรปอยู่ภายใต้ความคุ้มครองไม่ว่าจะอยู่ในที่ใดในโลก มีผลบังคับใช้เมื่อเดือนพฤษภาคม 2561 (Bunaramrueang, Elamchamroonlarp, Oinpat & Thipsamritkul, 2018, pp. 14-15) จึงทำให้ประเทศไทยได้พิจารณาแนวทางของกฎหมายในการคุ้มครองข้อมูลให้มากขึ้น จึงเป็นที่มาของ “พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562” (Royal Thai Government Gazette, 2019) ซึ่งประกาศใช้เมื่อวันที่ 24 พฤษภาคม พ.ศ. 2562 และจะมีผลบังคับใช้เดือนพฤษภาคม พ.ศ. 2563 โดยได้ให้องค์กรต่าง ๆ ต้องปฏิบัติตามมาตรฐานในการคุ้มครองข้อมูลของผู้บริโภคที่ได้จัดเก็บไว้ และระบุความผิดหากองค์กรเหล่านี้ไม่ปฏิบัติตามมาตรฐาน ซึ่งองค์กรต่าง ๆ ต้องมีการจัดทำระบบ นโยบาย และการดำเนินงานต่าง ๆ ตามที่กฎหมายกำหนด เช่น การกำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคล การให้สิทธิแก่เจ้าของข้อมูลเพื่อตรวจสอบแก้ไข หรือลบข้อมูลที่ร้องขอได้ การจัดทำระบบการรักษาความปลอดภัยและการโอนย้ายข้อมูล การตรวจประเมินมาตรฐานการรักษาข้อมูล เป็นต้น

นิยามศัพท์สำคัญเกี่ยวกับข้อมูล

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 (Royal Thai Government Gazette, 1997) ได้กำหนดนิยามศัพท์เกี่ยวข้อมูลที่สำคัญ คือ

“ข้อมูลข่าวสาร” หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริง ข้อมูล หรือสิ่งใด ๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพ หรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

“ข้อมูลข่าวสารของราชการ” หมายความว่า ข้อมูลข่าวสารที่อยู่ในความครอบครอง หรือควบคุมดูแลของหน่วยงานของรัฐ ไม่ว่าจะเป็นข้อมูลข่าวสารเกี่ยวกับการดำเนินงานของรัฐหรือข้อมูลข่าวสารเกี่ยวกับเอกชน

“ข้อมูลข่าวสารส่วนบุคคล” หมายความว่า ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้น หรือมีเลขหมายรหัสหรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่าย และให้หมายความรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดนิยามศัพท์เกี่ยวข้อมูลที่สำคัญ คือ

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจ เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่ง หรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

กรณีศึกษาผู้ใช้งานถูกละเมิดข้อมูลส่วนตัว

ที่ผ่านมามักมีข่าวรายงานเกี่ยวกับข้อมูลของผู้บริโภครั่วไหลออกจากบริษัทที่ผู้บริโภคได้ใช้บริการอยู่เป็นระยะ ซึ่งบางครั้งอาจเกิดจากบริษัทเหล่านั้นถูกโจมตีจากแฮกเกอร์แล้วถูกขโมยไปหรือบางกรณีอาจเกิดจากตัวซอฟต์แวร์ที่ทางบริษัทใช้แล้วมีข้อผิดพลาดมีการส่งข้อมูลให้กับผู้ให้บริการภายนอกหรือบุคคลที่สาม (third party) โดยที่ผู้บริโภคไม่ได้ยินยอม เมื่อเดือนมีนาคม 2561[1] สำนักข่าวต่างประเทศได้รายงานว่ามีบริษัทวิเคราะห์ข้อมูลชื่อ Cambridge Analytica ซึ่งตั้งอยู่ที่ประเทศอังกฤษได้มีการเข้าถึงข้อมูลส่วนตัวของผู้ใช้งาน Facebook โดยที่ผู้ใช้งานไม่ได้รับอนุญาตเป็นจำนวนมากถึง 50 ล้านบัญชี เพื่อนำข้อมูลส่วนตัวเหล่านั้นมาใช้วิเคราะห์ข้อมูลเพื่อช่วยหาเสียงทางการเมื่อให้กับ โดนัลด์ ทรัมป์ เมื่อปี พ.ศ. 2559 (ค.ศ. 2016) ส่งผลทำให้ โดนัลด์ ทรัมป์ เอาชนะการเลือกตั้งเหนือ ฮิลลารี่ คลินตัน ขึ้นเป็นประธานาธิบดีของประเทศสหรัฐอเมริกาได้ทั้ง ๆ ที่ ผลสำรวจคะแนนนิยมโดนัลด์ ทรัมป์ เป็นรอง ฮิลลารี่ คลินตัน อยู่มาก เหตุการณ์นี้ไม่ได้เกิดจากบริษัท Facebook นำเอาข้อมูลของลูกค้าไปให้บริษัท Cambridge Analytica เพื่อเอื้อประโยชน์ทางการค้าแก่กัน และไม่ได้เกิดจาก Facebook ถูกแฮ็กเอาข้อมูลไป แต่เกิดจาก บริษัท Cambridge Analytica ได้พัฒนาโปรแกรมชื่อว่า “thisisyourdigitallife” ซึ่งเป็นโปรแกรมที่ใช้ข้อมูลทางจิตวิทยามาทดสอบบุคลิกภาพ ซึ่งมีผู้ใช้งานจำนวน 270,000 คน โปรแกรมนี้ได้ใช้ Application Programming Interface--API ของ Facebook ที่พัฒนาขึ้นมาเพื่อให้โปรแกรมที่นำเอา API นี้ไปใช้สามารถเชื่อมต่อกับ Facebook ได้ โปรแกรมได้นำความสามารถของ API นี้มาใช้งานโดยให้ผู้ใช้สามารถลงชื่อเข้าใช้งานโดยล็อกอินด้วยบัญชี Facebook ของตนเองได้ ซึ่งโปรแกรม Thisisyourdigitallif นี้จะได้สิทธิเข้าถึงข้อมูลส่วนตัวต่าง ๆ ในบัญชี Facebook ของผู้ใช้ เช่น ข้อมูลกิจกรรมส่วนตัว ข้อมูลเพื่อน ๆ ที่มีอยู่ในรายการเพื่อนในบัญชี Facebook โดยโปรแกรม Thisisyourdigitallif ได้แจ้งขอสิทธิเข้าถึงข้อมูลส่วนตัวของผู้ใช้ไว้ในขั้นตอนการติดตั้ง ซึ่งมีรายละเอียดเป็นจำนวนมากทำให้ผู้ใช้ไม่ได้ระมัดระวังตอนอนุญาตให้สิทธิแก่โปรแกรมก่อนการติดตั้งเพื่อใช้งาน จากเหตุการณ์ดังกล่าวทำให้บริษัท Cambridge Analytica สามารถเข้าถึงข้อมูลส่วนตัวต่าง ๆ ของคนใช้งานมากถึง 50 ล้านบัญชี เมื่อได้ข้อมูลผู้ใช้งาน Facebook มาแล้วบริษัท Cambridge Analytica ก็นำข้อมูลเหล่านั้นมาวิเคราะห์เพื่อสร้างแคมเปญรณรงค์การเลือกตั้งเพื่อให้ตรงใจกับผู้ใช้ Facebook ในสหรัฐอเมริกามากที่สุด โดยสามารถโฆษณาแบบเจาะจงกลุ่มได้ สามารถสร้างโฆษณาที่ตรงใจทำให้ส่งผลต่อการตัดสินใจเลือกผู้สมัครประธานาธิบดีของผู้ลงคะแนนเลือกตั้งได้

ซึ่งเหตุการณ์ครั้งนี้มีประเด็นที่สำคัญคือการละเมิดการเข้าถึง และเข้าใช้งานข้อมูลส่วนตัวของผู้ใช้งานโดยที่ไม่ได้รับอนุญาตทั้งผู้ใช้งานโปรแกรม“Thisisyourdigitallife” และเพื่อนในบัญชี Facebook ของผู้ใช้งานทั้งที่ไม่ได้ติดตั้งโปรแกรมดังกล่าว แม้ว่า Facebook เองจะไม่ได้เป็นผู้ละเมิดเองแต่ก็ถือว่าบริษัทบกพร่องต่อการรักษาความปลอดภัยของข้อมูลและความเป็นส่วนตัวของผู้ใช้งาน คณะกรรมาธิการการค้าของรัฐบาลกลางสหรัฐอเมริกา (The Federal Trade Commission--FTC) ได้สั่งปรับบริษัท Facebook จากกรณีดังกล่าวในความผิดที่ Facebook

[1] จาก “Facebook โดนปรับ 150,000 ล้านบาท จากกรณี Cambridge Analytica” สืบค้นจาก ww.brandbuffet.in.th /2019/07/facebook-finned-5-billion-usd-for-cambridge-analytica-scandal

ละเมิดข้อตกลงกับคณะกรรมการซึ่งสัญญาว่า “จะไม่มอบข้อมูลผู้ใช้ให้แก่บุคคลที่สาม (third party) โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล” เป็นจำนวนเงินถึง 5 พันล้านเหรียญสหรัฐ (ประมาณ 150,000 ล้านบาท) และต้องปรับองค์กรเพื่อให้มีการปรับปรุงความปลอดภัยและข้อมูลส่วนตัวของผู้ใช้งาน คณะกรรมาธิการการค้าของรัฐบาลกลางสหรัฐอเมริกา ขอให้บริษัท Facebook ได้ปรับปรุงเรื่องความเป็นส่วนตัวใหม่จำนวน 6 เรื่อง ได้แก่

1) เพิ่มการตรวจสอบการทำงานแอปของบุคคลที่สาม (Third-party apps)

2) ห้ามนำหมายเลขโทรศัพท์ของผู้ใช้ที่ให้ไว้เพื่อความปลอดภัยมาใช้เพื่อการโฆษณา

3) แจ้งเตือนผู้ใช้อย่างชัดเจนและต้องได้รับความยินยอมก่อนใช้การจดจำใบหน้า

4) พัฒนาและการบำรุงรักษาโปรแกรมรักษาความปลอดภัยข้อมูลให้ทันสมัยอยู่ตลอดเวลา

5) รหัสผ่านของผู้ใช้ต้องมีการเข้ารหัสและตรวจสอบเป็นประจำเพื่อดูว่ามีการเก็บรหัสผ่านในรูปแบบข้อความธรรมดาและรหัสผ่านมีช่องโหว่หรือไม่

6) ห้ามให้บริการอื่น ๆ ขอรหัสผ่านอีเมลเมื่อผู้ใช้ Facebook สมัครใช้งานในบริการนั้น

จากข่าวนี้แสดงให้เห็นว่าความเสี่ยงของการถูกละเมิดข้อมูลส่วนตัวไม่จำเป็นต้องถูกขโมยจากอุปกรณ์สื่อสารที่ผู้บริโภคใช้อยู่เท่านั้น แต่ยังอาจเกิดจากการรั่วไหลจากความผิดพลาดของบริษัทหรือองค์กรที่ผู้บริโภคใช้บริการมีนโยบายการดูแลข้อมูล ความเป็นส่วนตัวที่ไม่เหมาะสมและการรักษาความปลอดภัยของฐานข้อมูลที่เก็บไว้ไม่มีประสิทธิภาพเพียงพอ

การให้ความสำคัญต่อข้อมูลส่วนบุคคลของคนไทย

ท่ามกลางการเปลี่ยนผ่านเข้าสู่ยุคดิจิทัล มีคนไทยจำนวนมากที่ได้มีการเข้าใช้งานอินเทอร์เน็ตและใช้เวลาทำกิจกรรมอยู่กับโลกออนไลน์มากขึ้น สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้ดำเนินการสำรวจพฤติกรรมการใช้งานของผู้ใช้อินเทอร์เน็ตเพื่อสำรวจพฤติกรรมที่สุ่มเสี่ยงต่อการถูกละเมิดข้อมูลส่วนบุคคลในทุกกลุ่มอายุ (Electronic Transactions Development Agency, 2019) ได้สำรวจพฤติกรรมผู้ใช้อินเทอร์เน็ตในประเทศไทย ปี พ.ศ. 2561 พบว่าชาวไทยให้ความสำคัญต่อข้อมูลส่วนบุคคลค่อนข้างน้อยและขาดความระมัดระวังในการให้ข้อมูลส่วนบุคคลของตนเองในอินเทอร์เน็ต ซึ่งการเข้าใช้งานเว็บไซต์ และแอปพลิเคชันบนมือถือสมาร์ทโฟนมักจะใช้ผู้ใช้สมัครเข้าใช้เข้าใช้งานก่อนซึ่งข้อมูลที่ต้องกรอก ได้แก่ ชื่อ นามสกุล วันเดือนปีเกิด หมายเลขโทรศัพท์ และ อีเมล เป็นต้น หรืออาจเข้าในผ่านระบบโซเชียลมีเดียที่นิยมเช่น Facebook และบัญชี Google จากรายงานผลการสำรวจพฤติกรรมผู้ใช้อินเทอร์เน็ตในประเทศไทย ปี 2560 พบว่า ผู้ใช้งานกลุ่ม Baby Boomer เป็นกลุ่มที่มีความเสี่ยงในการเปิดเผยข้อมูลส่วนตัวโดยกำหนดการแสดงผลข้อมูลส่วนตัวเป็นสาธารณะในสื่อสังคมออนไลน์อย่างเช่น Facebook มากกว่ากลุ่มผู้ใช้อื่น ๆ โดยไม่ระมัดระวังการเปิดเผยข้อมูลส่วนตัว เช่น วันเกิด หมายเลขโทรศัพท์ อีเมล รูปภาพ และข้อมูลอื่น ๆ ผู้ใช้งานกลุ่ม Gen Y นิยมทำกิจกรรมผ่านสื่อสังคมออนไลน์และตั้งค่าเป็นสาธารณะ แชร์ตำแหน่งการใช้งานแบบ Real time และมักใช้ทำธุรกรรมทางการเงินบนระบบออนไลน์ ผู้ใช้งานกลุ่ม Gen Z มักระบุข้อมูลส่วนตัวลงในสื่อสังคมออนไลน์แบบสาธารณะ และมีพฤติกรรมเสี่ยงในการใช้งานมากกว่ากลุ่มอื่น ๆ เนื่องจากขาดความระมัดระวังเรื่องความปลอดภัยในการใช้งาน เช่น เปิดอีเมลหรือคลิกลิงค์ที่ไม่รู้จัก เป็นต้น สาเหตุที่ผู้ใช้งานมักตั้งข้อมูลส่วนตัวและการแชร์ข้อมูลอื่น ๆ เป็นแบบสาธารณะเนื่องจากมีความมั่นใจว่าและไม่มีความกังวลเรื่องความเป็นส่วนตัวของตนมีอยู่ถึงร้อยละ 46.10

ตาราง 1

กลุ่มผู้ใช้งานอินเทอร์เน็ต

เจนเนอเรชั่น	ช่วง พ.ศ. เกิด
Baby Boomer	2489-2507
Gen X	2508-2523
Gen Y	2524-2543
Gen Z	2544 เป็นต้นไป

Note. Adapted from "Thailand Internet User Profile 2018"(p. 42), by Electronic Transactions Development Agency (Public Organization), 2019, Bangkok: Ministry of Digital Economy and Society

นอกเหนือจากการกรอกข้อมูลส่วนตัวลงในเว็บไซต์หรือแอปพลิเคชันแล้ว แต่ละเว็บไซต์หรือแอปพลิเคชันจะมีรายละเอียดนโยบายการใช้งาน ซึ่งเป็นข้อกำหนดและเงื่อนไขการใช้บริการของผู้ให้บริการซึ่งจะประกอบด้วยการใช้บริการ นโยบายข้อมูลส่วนบุคคล ทรัพย์สินทางปัญญา และการจำกัดความรับผิดชอบ เป็นต้น และการสำรวจเกี่ยวกับการอ่านนโยบายการใช้งานเว็บไซต์และแอปพลิเคชัน พบว่าผู้ใช้งานส่วนมากยังคงละเลยการอ่านนโยบาย โดยมีรายละเอียด ดังนี้

ตาราง 2

พฤติกรรมการอ่านนโยบาย

การอ่านนโยบาย	ร้อยละ
เคยอ่าน	63.00
ไม่เคย	32.20
ไม่ทราบ	4.50

Note. Adapted from "Thailand Internet User Profile 2018"(p. 92), by Electronic Transactions Development Agency (Public Organization), 2019, Bangkok: Ministry of Digital Economy and Society

ตาราง 3

พฤติกรรมของผู้เคยอ่านนโยบาย (ร้อยละ 63.00)

การอ่านอย่างละเอียด	ร้อยละ
เคยอ่านอย่างละเอียด	12.30
เคยอ่านอย่างละเอียดเฉพาะหัวข้อที่สำคัญ	36.00
เคยอ่านบางส่วน	51.70

Note. Adapted from "Thailand Internet User Profile 2018"(p. 92), by Electronic Transactions Development Agency (Public Organization), 2019, Bangkok: Ministry of Digital Economy and Society

ผลการสำรวจพฤติกรรมจะเห็นได้ว่า ผู้ใช้งานอินเทอร์เน็ตมีเพียงร้อยละ 63.30 เท่านั้นที่เคยอ่านนโยบายการใช้ข้อมูล และกลุ่มที่เคยอ่านนั้นมีเพียงร้อยละ 12.30 ที่อ่านอย่างละเอียด ร้อยละ 36.0 จะอ่านเฉพาะหัวข้อที่สำคัญ และมีอยู่ร้อยละ 51.7 ที่อ่านเป็นบางส่วน เหตุผลที่ผู้ใช้อินเทอร์เน็ตที่ไม่เคยอ่านนโยบาย หรืออ่านบางส่วนเนื่องจากเนื้อหายาวและเป็นภาษาทางกฎหมายซึ่งทำความเข้าใจยาก และมีความมั่นใจว่ากฎหมายน่าจะคุ้มครองผู้ใช้งานอยู่แล้ว

ซึ่งจากผลการสำรวจพฤติกรรมผู้ใช้อินเทอร์เน็ตในประเทศไทย ปี พ.ศ. 2561 สรุปได้ว่าผู้ใช้งานอินเทอร์เน็ตในประเทศไทยมีพฤติกรรมการใช้งานที่สุ่มเสียงต่อการถูกละเมิดความเป็นส่วนตัวมากเนื่องจากมีความไว้ใจต่อผู้ให้บริการมากเกินไปและเชื่อมั่นว่าระบบที่ใช้งานอยู่จะมีความปลอดภัยสูง

นโยบายการจัดเก็บข้อมูลของผู้ใช้งาน

ปัจจุบันมีกฎหมายที่กำหนดให้ผู้ให้บริการทั้งเว็บไซต์ หรือแอปพลิเคชันต้องชี้แจงให้ผู้ใช้งานทราบว่าผู้ให้บริการจะจัดเก็บข้อมูลใดบ้าง เพื่อเป็นข้อมูลในการตัดสินใจของผู้ใช้ว่าจะยินยอมให้ผู้ให้บริการจัดเก็บ หรือไม่ก่อนตกลงใช้ ตัวอย่างเช่น บริษัท Facebook ก็มีการจัดเก็บข้อมูลและมีการแจ้งข้อมูลที่จัดเก็บให้ผู้ใช้งานทราบด้วย เช่นกัน (Facebook, 2018) ซึ่งตัวอย่างข้อมูลที่จัดเก็บมีดังนี้

1. สิ่งที่ผู้ใช้และผู้อื่นดำเนินการและให้ไว้

1.1 ข้อมูลและเนื้อหาที่ผู้ใช้งานให้ คือเนื้อหาการสื่อสาร และข้อมูลอื่น ๆ เมื่อผู้ใช้บันทึกเมื่อใช้ Facebook เช่น ที่การสมัครใช้งานบัญชีผู้ใช้ สร้างหรือแชร์เนื้อหา และส่งข้อความหรือติดต่อสื่อสารกับคนอื่น ๆ ข้อมูลที่อยู่ในเนื้อหาหรือเกี่ยวกับเนื้อหาที่ผู้ใช้บริการให้ (เช่น เมตาดาต้า) ตัวอย่าง เช่น ตำแหน่งที่ตั้งของรูปภาพหรือวันที่สร้างไฟล์ ข้อมูลโปรไฟล์ใน Facebook ได้แก่ มุมมองทางศาสนาทรรศนะทางการเมือง บุคคลที่คุณ “สนใจ” หรือสุขภาพของคุณ ข้อมูลนี้และข้อมูลอื่น ๆ (เช่น เชื้อชาติ หรือชาติกำเนิด ความเชื่อทางปรัชญา หรือการเป็นสมาชิกสหภาพการค้า)

1.2 รายละเอียดเครือข่ายและการเชื่อมต่อเกี่ยวกับผู้คน เพจ บัญชีผู้ใช้ แฮชแท็ก และกลุ่มที่ผู้ใช้เชื่อมต่อด้วย สมุดรายชื่อ ประวัติการโทร หรือบันทึกประวัติ SMS

1.3 การใช้งาน ข้อมูลเกี่ยวกับการใช้ facebook เช่น ประเภทเนื้อหาที่ดูหรือโต้ตอบด้วย ฟีเจอร์ที่ใช้ ผู้คนหรือบัญชีผู้ใช้ที่คุณโต้ตอบด้วย รวมทั้งเวลา ความถี่ และระยะเวลาที่ทำกิจกรรม

1.4 ข้อมูลเกี่ยวกับการทำธุรกรรมใน facebook ข้อมูลการชำระเงิน เช่น หมายเลขบัตรเครดิต หรือบัตรเดบิต และข้อมูลอื่น ๆ ของบัตร ข้อมูลเกี่ยวกับบัญชีผู้ใช้ และข้อมูลการยืนยันตัวตน และรายละเอียดเกี่ยวกับการเรียกเก็บเงิน การส่งสินค้า และการติดต่อ

1.5 สิ่งที่ผู้อื่นทำ และข้อมูลที่บุคคลเหล่านั้นให้เกี่ยวกับคุณ facebook มีการรับ และวิเคราะห์เนื้อหาการสื่อสาร และข้อมูลที่ผู้อื่นให้เมื่อบุคคลเหล่านั้นใช้ ซึ่งอาจรวมถึงข้อมูลเกี่ยวกับผู้ใช้ เช่น เมื่อผู้อื่นแชร์หรือแสดงความคิดเห็นบนรูปภาพของคุณ ส่งข้อความหา หรืออัพโหลดซิงค์ หรือนำเข้าข้อมูลติดต่อของผู้ใช้

2. ข้อมูลของอุปกรณ์

2.1 ข้อมูลของอุปกรณ์ เช่น ระบบปฏิบัติการ เวอร์ชันของฮาร์ดแวร์และซอฟต์แวร์ ระดับแบตเตอรี่ ความแรงของสัญญาณ พื้นที่จัดเก็บที่มี ประเภทเบราว์เซอร์ ชื่อและประเภทไฟล์และแอพ และปลั๊กอิน

2.2 การทำงานของอุปกรณ์ ข้อมูลเกี่ยวกับการทำงานและพฤติกรรมต่าง ๆ ในอุปกรณ์ เช่น วินโดว์ทำงานอยู่เบื้องหน้า หรือเบื้องหลัง หรือการเคลื่อนไหวของเมาส์

2.3 ตัวระบุต่าง ๆ ตัวระบุที่ไม่ซ้ำกัน, ID ของอุปกรณ์ และตัวระบุอื่น ๆ เช่น จากเกม แอพ หรือบัญชีที่ใช้ และ ID ของอุปกรณ์ในครอบครัว

2.4 สัญญาณของอุปกรณ์ สัญญาณบลูทูธและข้อมูลเกี่ยวกับจุดเชื่อมต่อสัญญาณ Wi-Fi, บีคอน และเสาสัญญาณโทรศัพท์ที่อยู่ใกล้เคียง

2.5 ข้อมูลจากการตั้งค่าอุปกรณ์ ข้อมูลที่ผู้ใช้อนุญาตให้เราได้รับผ่านทางการตั้งค่าอุปกรณ์ที่คุณเปิดไว้ เช่น การเข้าถึงตำแหน่งที่ตั้ง GPS กล้อง หรือรูปภาพ

2.6 เครือข่ายและการเชื่อมต่อ ข้อมูล เช่น ชื่อของผู้ให้บริการมือถือของผู้ใช้หรือ ISP ภาษา โซนเวลา หมายเลขโทรศัพท์มือถือ ที่อยู่ IP ความเร็วในการเชื่อมต่อ

2.7 ข้อมูลคุกกี้ ข้อมูลจากคุกกี้ที่เก็บอยู่บนอุปกรณ์ ซึ่งรวมถึง ID คุกกี้และการตั้งค่าต่าง ๆ

3. ข้อมูลจากพาร์ทเนอร์

ผู้ลงโฆษณา ผู้พัฒนาแอพ และผู้เผยแพร่สามารถส่งข้อมูลมาหา facebook ได้ รวมถึงข้อมูลเกี่ยวกับอุปกรณ์ของผู้ที่ใช้บริการของพาร์ทเนอร์ เช่น เว็บไซต์ที่เข้าชม สิ่งที่ซื้อ โฆษณาที่เห็น และวิธีที่ใช้บริการของพาร์ทเนอร์ เป็นต้น และ facebook ยังจะได้รับข้อมูลเกี่ยวกับการดำเนินการและการซื้อทั้งออนไลน์และออฟไลน์ของผู้ใช้จากผู้ให้บริการข้อมูลบุคคลที่สามซึ่งมีสิทธิ์มอบข้อมูลให้ facebook

จากนโยบายการจัดเก็บข้อมูลผู้ใช้งานผลิตภัณฑ์ของบริษัท facebook จะพบว่าข้อมูลที่จัดเก็บมีหลากหลายตั้งแต่ข้อมูลส่วนตัว เนื้อหา การติดต่อกับผู้ใช้อื่น รายละเอียดของอุปกรณ์และการสื่อสารที่ผู้ใช้ใช้งาน และ facebook ยังจะทราบข้อมูลการใช้งานของผู้ใช้ผ่านบริษัทที่เป็นพาร์ทเนอร์กัน ซึ่งข้อมูลเหล่านี้ถือว่าเป็นข้อมูลที่มีค่ามากสำหรับบริษัทที่จะนำไปวิเคราะห์และประมวลเพื่อประโยชน์ต่อธุรกิจของ facebook

กฎหมาย General Data Protection Regulation

เมื่อวันที่ 25 พฤษภาคม พ.ศ.2561 สหภาพยุโรป (EU--European Union) ได้ออกกฎหมายชื่อว่า

“General Data Protection Regulation” เรียกโดยย่อว่า “GDPR” โดยหลักการที่สำคัญของ GDPR มีดังนี้ (Ministry of Commerce, 2018)

1. การบังคับใช้กฎหมายนอกอาณาเขต (extraterritorial applicability) คือ ผู้รับข้อมูลไม่ว่าจะอยู่ที่ใดก็ต้องทำตาม GDPR

2. บทลงโทษที่แรงขึ้น คือ มีค่าปรับสูงถึง 20 ล้านยูโร หรือร้อยละ 4 ของผลประกอบการของบริษัท

3. การขอความยินยอม (consent) จากเจ้าของข้อมูล ต้องใช้ภาษาที่ชัดเจนกระชับไม่ใช่ภาษากฎหมายและเข้าใจง่าย เช่นเดียวกับการถอนความยินยอมก็ต้องทำได้ง่ายเช่นกัน

4. การแจ้งเตือนเมื่อเกิดเมื่อเกิดเหตุข้อมูลรั่วไหล (breach notification) ต้องดำเนินการภายใน 72 ชั่วโมง

5. สิทธิในการเข้าถึง (right to access) คือ ต้องแจ้งให้เจ้าของข้อมูลทราบว่าข้อมูลถูกใช้ไปเพื่อวัตถุประสงค์ใด และต้องจัดทำสำเนาข้อมูลให้กับเจ้าของข้อมูลในรูปแบบอิเล็กทรอนิกส์โดยห้ามเก็บค่าใช้จ่ายเพิ่ม

6. สิทธิที่จะถูกลืม (right to be forgotten) คือ เจ้าของข้อมูลสามารถขอให้ลบข้อมูลของตัวเองออกได้ และข้อมูลที่ไม่มีความเกี่ยวข้อกับการประมวลผลต้องลบออกด้วย

7. สิทธิในการโอนย้ายข้อมูลของตนจากผู้ประกอบการหนึ่งไปยังผู้ประกอบการอื่นได้ (data portability)

GDPR มีกำหนดบังคับใช้ในประเทศกลุ่มสมาชิกของสหภาพยุโรป ซึ่งนอกจากการมีผลบังคับใช้ภายในประเทศสมาชิกสหภาพยุโรปแล้ว สำหรับผู้ประกอบการที่ไม่ได้เป็นสมาชิกสหภาพยุโรปแต่หากต้องติดต่อรับ-ส่งข้อมูลกับบุคคลของประเทศสมาชิกสหภาพยุโรป ก็ต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมตามเกณฑ์ของ GDPR กำหนดเพื่อทำให้ไม่เกิดปัญหาในการดำเนินธุรกิจในสหภาพยุโรป GDPR มีข้อกำหนดให้ทุกองค์กรที่มีการรวบรวม (collect), ประมวลผล (process), จัดการ (manage) หรือจัดเก็บ (store) ข้อมูลส่วนบุคคลผู้บริโภคที่เป็นพลเมืองที่อยู่ในสหภาพยุโรป (ครอบคลุมทุกบริษัทไม่ใช่เฉพาะบริษัทด้านไอทีหรือที่ให้บริการออนไลน์เท่านั้น) ต้องเพิ่มความคุ้มครองข้อมูลส่วนบุคคลของผู้บริโภค โดยจะต้องปฏิบัติตามมาตรการต่าง ๆ ที่ GDPR กำหนดขึ้น เช่น การนำข้อมูลส่วนบุคคลของผู้บริโภค ข้อมูลและเนื้อหา เครือข่ายและการเชื่อมต่อ ข้อมูลติดต่อของข้อมูลจากอุปกรณ์ (เช่น สมุดรายชื่อ ประวัติการโทร หรือบันทึกประวัติ SMS) ข้อมูลของอุปกรณ์ ระบบปฏิบัติการ การทำงานและพฤติกรรมต่าง ๆ ในอุปกรณ์ เช่น วินโดว์ทำงานอยู่เบื้องหน้าหรือเบื้องหลัง หรือการเคลื่อนไหวของเมาส์ ตำแหน่งที่ตั้ง GPS กล้อง หรือรูปภาพ ชื่อของผู้ให้บริการมือถือ หรือ ISP มาประมวลผลเพื่อวิเคราะห์เพื่อประโยชน์ของบริษัท การทำตามคำร้องขอของผู้บริโภคหากต้องการให้บริษัทลบร่องรอยทางดิจิทัล (Digital footprint) ออกจากฐานข้อมูลของบริษัท เป็นต้น หากบริษัทใดได้ทำการละเมิดกฎหมายดังกล่าวจะส่งผลให้ถูกปรับด้วยมูลค่ามหาศาลสูงสุด 20 ล้านยูโร หรือร้อยละ 4 ของรายได้ของบริษัท

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย

สำหรับกฎหมายที่เกี่ยวกับการให้ความคุ้มครองสิทธิในข้อมูลส่วนบุคคลของประเทศไทยนั้นได้มีการออกพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ไว้ แต่พระราชบัญญัติฉบับนี้ให้การคุ้มครองข้อมูลส่วนบุคคลซึ่งทางราชการเป็นผู้จัดเก็บไว้เท่านั้นไม่ครอบคลุมข้อมูลของบุคคลที่หน่วยงานเอกชนเป็นจัดเก็บไว้ ทำให้ประชาชนได้รับความเดือดร้อนจากการละเมิดความเป็นส่วนตัวจากบริษัทเอกชนเหล่านั้น เช่น การซื้อขายข้อมูลลูกค้าเพื่อใช้ประโยชน์ด้านการตลาดและโฆษณา หรือข้อมูลรั่วไหลออกจากบริษัทไปโดยที่ผู้ใช้ไม่ได้ยินยอม เป็นต้น ดังนั้นประเทศไทยจึงได้ออกกฎหมายอีกฉบับหนึ่ง คือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ขึ้น ซึ่งออกมาตรการเพื่อสำหรับการคุ้มครองข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

เนื่องจากสหภาพยุโรป (European Union--EU) ได้ออกกฎหมายคุ้มครองข้อมูลส่วนบุคคล (General Data Protection Regulation--GDPR) เมื่อ 25 พฤษภาคม พ.ศ. 2561 มีผลบังคับเรื่องการคุ้มครองข้อมูลส่วนบุคคลให้กับ

ประชาชนที่อยู่ในประเทศสมาชิกสหภาพยุโรป แม้จะเป็นกฎหมายของสหภาพยุโรปแต่ในรายละเอียดยังครอบคลุมไปถึงองค์กรที่อยู่นอกสหภาพยุโรปที่มีการดำเนินกิจกรรมและธุรกิจที่มีการจัดเก็บ รับ และส่งข้อมูลส่วนบุคคลของประชาชนในประเทศที่เป็นสมาชิกสหภาพยุโรปด้วย ซึ่งองค์กรเหล่านั้นต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลตามข้อกำหนดของ GDPR ด้วย ประเทศไทยจึงได้มีการออกพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 โดยจะมีผลบังคับใช้เดือนพฤษภาคม พ.ศ. 2563 ซึ่งแสดงให้เห็นว่าประเทศไทยให้ความสำคัญต่อการปกป้องข้อมูลส่วนตัว และได้กำหนดมาตรการให้องค์กรหรือบริษัทในประเทศไทยมีการคุ้มครองข้อมูลส่วนบุคคลให้มีความปลอดภัยส่งผลให้บริษัทมีความน่าเชื่อถือสำหรับการทำธุรกิจระหว่างประเทศ ในมาตรา 5 พระราชบัญญัตินี้ให้ใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่าการเก็บรวบรวม ใช้ หรือเปิดเผยนั้น ได้กระทำใน หรือนอกราชอาณาจักรก็ตาม การผลบังคับพระราชบัญญัตินี้จึงใช้มีความสอดคล้องกับกฎหมาย GDPR ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล หมวดที่ 2 การคุ้มครองข้อมูลส่วนบุคคล มีการกำหนดมาตราที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลแบ่งออกเป็น 3 ส่วน คือ

ส่วนที่ 1 บททั่วไป เป็นมาตรากล่าวถึง การจัดเก็บข้อมูลต้องได้รับความยินยอมจากเจ้าของข้อมูล และต้องแจ้งวัตถุประสงค์การจัดเก็บให้ทราบ

ส่วนที่ 2 การเก็บรวบรวมข้อมูลส่วนบุคคล เป็นมาตรากล่าวถึงการจัดเก็บข้อมูลเท่าที่จำเป็นตามกฎหมายกำหนด ต้องแจ้งให้เจ้าของข้อมูลทราบและได้รับความยินยอมให้เก็บข้อมูลได้จากเจ้าของข้อมูลเท่านั้นมาเก็บจากแหล่งอื่น ห้ามเก็บข้อมูลอื่น ๆ ซึ่งส่งผลกระทบต่อเจ้าของข้อมูล เช่น เชื้อชาติ ความเชื่อ ศาสนา และ ข้อมูลชีวภาพ (ลายนิ้วมือ การสแกนใบหน้า) หากไม่ได้รับความยินยอม

ส่วนที่ 3 การใช้หรือเปิดเผยข้อมูลส่วนบุคคล เป็นมาตราที่ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล หมวดที่ 3 สิทธิของเจ้าของข้อมูลส่วนบุคคล เป็นหมวดที่กำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึง และขอรับสำเนาข้อมูลส่วนบุคคล ที่เกี่ยวกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอม เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอรับข้อมูลส่วนบุคคลที่เกี่ยวกับตนจากผู้ควบคุม ข้อมูลส่วนบุคคลได้ เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ส่วนบุคคลที่เกี่ยวกับตนเมื่อใดก็ได้ เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการใช้ ข้อมูลส่วนบุคคลได้

การเตรียมความพร้อมเมื่อกฎหมายคุ้มครองข้อมูลส่วนบุคคลบังคับใช้

ผู้ประกอบการ องค์กร หรือหน่วยงานใดที่ต้องมีการเก็บข้อมูลส่วนบุคคลของผู้ใช้ไว้จำเป็นต้องศึกษารายละเอียดที่ต้องปฏิบัติตามมาตรการของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล เช่น ต้องรู้คำนิยามของข้อมูลแต่ละประเภท ขอบเขตของการเข้าถึงและการเปิดเผยข้อมูลส่วนบุคคลของผู้ใช้ มีระบบควบคุมการเข้าถึง และมีระบบยืนยันตัวตนของผู้ขอเข้าถึงข้อมูลส่วนบุคคล และต้องมีการปรับปรุงหรือกำหนดนโยบายสำหรับบุคคลภายในองค์กรที่ต้องเกี่ยวข้องกับการใช้งานข้อมูลส่วนบุคคลที่ตามพระราชาบัญญัติฉบับนี้ จากเอกสารแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Bunaramrueang, Elamchamroonlarp, Oinpat & Thipsamritkul, 2019, p. 32) ได้เสนอแนวทางปฏิบัติไว้สำหรับผู้ประกอบการว่าผู้ประกอบการจำเป็นต้องแสดงให้เห็นว่ามีขั้นตอนการกำหนดข้อมูลให้เป็นข้อมูลส่วนบุคคลในองค์กร โดยอย่างน้อยต้องประกอบด้วยมาตรการ ดังนี้

(1) การกำหนดนโยบายและนิยามความหมายของข้อมูลส่วนบุคคล (data policy)

(2) การกำหนดขั้นตอนการตรวจสอบข้อมูลส่วนบุคคล (data discovery)

(3) การระบุความเชื่อมโยงและเส้นทางการส่งข้อมูลส่วนบุคคลที่จะเกิดขึ้นในองค์กร รวมถึงระบุแหล่งที่จะได้มาซึ่งข้อมูลส่วนบุคคลทั้งหลาย (data proliferation)

(4) การกำหนดความเสี่ยงของข้อมูลส่วนบุคคลชุดต่าง ๆ (data risk level)

(5) มีมาตรการคุ้มครองข้อมูลส่วนบุคคล (data protection)

สำหรับบุคคลทั่วไปและเจ้าของข้อมูลส่วนบุคคลต้องศึกษาสิทธิของตนเองตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลในหมวดที่ 3 สิทธิของเจ้าของข้อมูลส่วนบุคคล เพื่อให้ทราบถึงสิทธิที่ตนเองมีและสิทธิที่จะการดำเนินการกับบริษัทต่าง ๆ ที่เก็บข้อมูลไว้ และควรศึกษานโยบายการจัดเก็บข้อมูล หรือการขอสิทธิเข้าใช้ข้อมูลของตนเองจากผู้ให้บริการที่ผู้ใช้ได้เข้าไปใช้โดยละเอียด เช่น จากสื่อออนไลน์ เว็บไซต์ และแอปพลิเคชัน เพื่อเป็นการปกป้องข้อมูลไม่ถูกนำไปใช้โดยไม่ได้รับความยินยอมและถูกนำไปใช้งานโดยที่ไม่มีความจำเป็นต่อตัวผู้ใช้

สรุป

ปัจจุบัน “ข้อมูล” ถือว่าสิ่งสำคัญต่อการวางแผนงานและการดำเนินธุรกิจของหน่วยงานและบริษัทต่าง ๆ ทำให้บริษัทเหล่าต้องเสาะแสวงหาข้อมูลของผู้ใช้งานให้ได้มากที่สุด เช่น ประวัติส่วนตัว ความชอบ และทัศนคติในการดำเนินชีวิต จากเหตุผลดังกล่าวจึงเป็นสาเหตุทำให้มีการหาช่องทางเพื่อที่จะได้มาซึ่งข้อมูลดังกล่าว เช่น นำมาจากผู้ประกอบการที่มีข้อมูลลูกค้าหรือผู้ใช้งานไว้ ซึ่งสุ่มเสี่ยงที่จะเป็นการละเมิดข้อมูลโดยไม่รับความยินยอมจากลูกค้า ประชาชนในกลุ่มสหภาพยุโรปถือว่าเรื่องดังกล่าวเป็นปัญหาที่ร้ายแรงมาก จึงได้ออกกฎหมายคุ้มครองข้อมูลส่วนบุคคล (General Data Protection Regulation--GDPR ขึ้นมา และประเทศไทยได้นำมาใช้เป็นแนวทางในการออกพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ด้วย เพื่อออกมาตรการให้บริษัท องค์กร หรือหน่วยงานหาวิธีดูแลข้อมูลลูกค้าให้มีความปลอดภัย หลังจากนี้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติ จะมีการสรรหาประธานกรรมการและกรรมการที่เป็นมีความรู้ ความเชี่ยวชาญและประสบการณ์ ในหลากหลายด้าน ได้แก่ ด้านการคุ้มครองข้อมูลส่วนบุคคล ด้านการคุ้มครองผู้บริโภค ด้านเทคโนโลยีสารสนเทศ และการสื่อสาร ด้านสังคมศาสตร์ ด้านกฎหมาย ด้านสุขภาพ ด้านการเงิน หรือด้านอื่น ที่เกี่ยวข้องและเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคล เพื่อมาจัดทำแผนแม่บทการดำเนินงาน ให้ความรู้และส่งเสริมและสนับสนุนหน่วยงานของรัฐและภาคเอกชน ดำเนินกิจกรรมตามแผนแม่บท กำหนดมาตรการหรือแนวทางการดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ออกประกาศ หรือระเบียบการดำเนินการ กำหนดหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ กำหนดข้อปฏิบัติให้กับผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลปฏิบัติ ให้ความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้แก่ประชาชน และส่งเสริมและสนับสนุนการวิจัย เพื่อพัฒนาเทคโนโลยีที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

ดังนั้นหน่วยงานและบริษัทต่าง ๆ จึงควรปรับตัวและพัฒนาให้องค์กรตนเองมีมาตรฐานความมั่นคงปลอดภัยทางด้านเทคโนโลยีเพื่อทำให้สามารถรักษาความเป็นส่วนตัวของข้อมูลที่จัดเก็บไว้เพื่อให้ได้รับความเชื่อถือต่อการดำเนินกิจการขององค์กรจากทั้งในประเทศและในระดับสหภาพยุโรป สำหรับบุคคลทั่วไปที่มีการใช้อินเทอร์เน็ตหรือกิจกรรมบนออนไลน์ควรที่จะศึกษาพระราชบัญญัติฉบับนี้เพื่อประโยชน์ต่อการตรวจสอบและการสิทธิจัดการข้อมูลส่วนบุคคลของตนเอง และผู้ใช้งานต้องมีความตะหนักต่อการปกป้องข้อมูลส่วนตัวของตนเองด้วยเพื่อไม่ใช้ถูกขโมยหรือล่อลวงขโมยเอาข้อมูลส่วนตัวของตนไปใช้งานได้ทั้งจากเว็บไซต์

หรือแอปพลิเคชันที่ใช้งานอยู่ จึงต้องมั่นศึกษาการใช้งานเทคโนโลยีที่มีความปลอดภัยมากขึ้น หากผู้ใช้ทั่วไป บริษัท องค์กรหรือหน่วยงานถูกผู้ใดกระทำความผิดทางคอมพิวเตอร์ให้ได้รับความเสียหายที่ไม่ใช้ข้อมูลส่วนบุคคล ก็จะใช้พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์เป็นบทบัญญัติในการดูแลและลงโทษแทน

References

Facebook. (2018). *Facebook data policy*. Retrieved from https://www.facebook.com/policy.php

Bunaramrueang, P., Elamchamroonlarp, P., Oinpat, C., & Thipsamritkul, T. (2018). *Thailand data protection guidelines 1.0.* Bangkok: Chulalongkorn University. (in Thai)

Bunaramrueang, P., Elamchamroonlarp, P., Oinpat, C., & Thipsamritkul, T. (2019). *Thailand data protection guidelines 2.0*. Bangkok: Chulalongkorn University. (in Thai)

Electronic Transactions Development Agency (Public Organization) Ministry of Digital Economy and Society. (2019). *Thailand internet user profile 2018*. Retrieved from https://www.etda.or.th/publishing-detail/thailand-internet-user-profile-2018.html

Ministry of Commerce. (2018). *General data protection regulation*. Retrieved from https://www.moc.go.th/index.php/คู่มือประชาชน2561/item/สรุปสาระสำคัญของ-gdpr-general-data-protection-regulation.html

Royal Thai Government Gazette. (1997). *The Official Information Act B.E. 2540 (1997).* Bangkok: Publisher of the Cabinet and the Government Gazette. (in Thai)

Royal Thai Government Gazette. (2007). *The Computer Crimes Act B.E. 2550 (2007).* Bangkok: Publisher of the Cabinet and the Government Gazette. (in Thai)

Royal Thai Government Gazette. (2017). *The Computer Crimes Act (No. 2) B.E. 2560 (2017).* Bangkok: Publisher of the Cabinet and the Government Gazette. (in Thai)

Royal Thai Government Gazette. (2019). *The Personal Data Protection Act B.E. 2562 (2019).* Bangkok: Publisher of the Cabinet and the Government Gazette. (in Thai)