ปัญหาทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล : ศึกษากรณีนายหน้าข้อมูล

นิจญาณอมร อินสุข

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรนิติศาสตรมหาบัณฑิต
สาขาวิชานิติศาสตร์ คณะนิติศาสตร์ปรีดี พนมยงค์
มหาวิทยาลัยธุรกิจบัณฑิตย์
ปีการศึกษา 2565

LEGAL ISSUES RELATING TO THE PERSONAL DATA PROTECTION : A CASE STUDY ON THE DATA BROKER

NIDYARNAMORN INSUK

A Thesis Submitted in Partial Fulfilment of the Requirements for the Decree of Master of Master of Master of Laws

Department of Law

Pridi Banomyong Faculty of Law, Dhurakij Pundit University

Academic Year 2022

ใบรับรองวิทยานิพนธ์

คณะนิติศาสตร์ปรีดี พนมยงค์ มหาวิทยาลัยธุรกิจบัณฑิตย์

ปริญญานิติศาสตรมหาบัณฑิต

หัวข้อวิทยานิพนธ์ ปัญหาทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล : ศึกษากรณีนายหน้าข้อมูล

เสนอโดย นิจญาณอมร อินสุข

สาขาวิชา นิติศาสตร์

หมวดวิชา กฎหมายธุรกิจและนวัตกรรม

อาจารย์ที่ปรึกษาวิทยานิพนธ์ รองศาสตราจารย์พินิจ ทิพย์มณี

ได้พิจารณาเห็นชอบโดยคณะกรรมการสอบวิทยานิพนธ์แล้ว

.....ประธานกรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.สมชาย รัตนชื่อสกุล)

.....กรรมการและอาจารย์ที่ปรึกษาวิทยานิพนธ์

(รองศาสตราจารย์พินิจ ทิพย์มณี)

.....กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.สิรีกานต์ อยู่เรือง)

คณะนิติศาสตร์ปรีดี พนมยงค์ รับรองแล้ว

..... คณบดีคณะนิติศาสตร์ปรีดี พนมยงค์

(ผู้ช่วยศาสตราจารย์ ดร.สมชาย รัตนชื่อสกุล)

วันที่ 9 เดือน กรกฎาคม พ.ศ. 2566

หัวข้อวิทยานิพนธ์	ปัญหาทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล : ศึกษากรณีนายหน้าข้อมูล
ชื่อผู้เขียน	นิจญาณอมร อินสุข
อาจารย์ที่ปรึกษา	รองศาสตราจารย์พินิจ ทิพย์มณี
หลักสูตร	นิติศาสตรมหาบัณฑิต
ปีการศึกษา	2565

บทคัดย่อ

การคุ้มครองข้อมูลส่วนบุคคล และการซื้อขายข้อมูลนั้นมีมายาวนาน ในปัจจุบันประเทศไทยมีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพและมีมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิ แต่ในประเทศไทยนั้น การคุ้มครองข้อมูลส่วนบุคคล กรณีนายหน้าข้อมูลยังไม่ปรากฏในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และยังไม่มีกฎหมายฉบับใดได้บัญญัติในเรื่องการคุ้มครองข้อมูลส่วนบุคคล กรณีนายหน้าข้อมูลไว้เป็นการเฉพาะ นอกจากนี้ประเทศที่ใช้ระบบกฎหมายเช่นเดียวกันกับประเทศไทย เช่น ใน Act on the Protection of Personal Information (APPI) ประเทศญี่ปุ่น หรือแม้แต่องค์กรระหว่างประเทศ เช่น European Union (EU) หรือ the Organization for Economic Cooperation and Development (OECD) ก็ไม่ได้บัญญัติเกี่ยวกับการนายหน้าข้อมูลไว้เช่นเดียวกัน

จากการศึกษาพบว่าในต่างประเทศ เช่น ในสหรัฐอเมริกา รัฐแคลิฟอร์เนียได้บัญญัติคำนิยามคำว่า Data Broker ไว้ใน California Consumer Privacy Act (CCPA) ซึ่งเป็นประมวลกฎหมายแพ่งแห่งรัฐแคลิฟอร์เนีย (California Civil Code §1798.99.88) และยังได้กำหนดเงื่อนไขให้อยู่ภายใต้กรอบที่ CCPA กำหนด และรัฐเวอร์มอนต์ก็ได้มีการบัญญัติเกี่ยวกับนายหน้าข้อมูลไว้เช่นเดียวกัน โดยได้บัญญัติคำนิยามเกี่ยวกับนายหน้าข้อมูลส่วนบุคคลไว้ใน Vermont Data Broker Regulation (VDBR) และยังได้กำหนดคำแนะนำ หรือแนวปฏิบัติของนายหน้าข้อมูลไว้ใน Guidance on Vermont's Act 171 of 2018 Data Broker Regulation เป็นต้น ส่งผลให้การซื้อขายข้อมูลสามารถกระทำได้โดยอยู่ภายใต้กรอบที่กฎหมายกำหนด และสามารถตรวจสอบและทราบถึงแหล่งที่มาของข้อมูลที่ถูกซื้อขายกันได้ง่ายขึ้น ถึงแม้ว่าประเทศสิงคโปร์จะใช้ระบบกฎหมายเช่นเดียวกันกับสหรัฐอเมริกา แต่ประเทศสิงคโปร์ก็ไม่ได้มีการบัญญัติเกี่ยวกับนายหน้าข้อมูลไว้เป็นการเฉพาะเช่นเดียวกันกับประเทศไทย

ด้วยเหตุดังกล่าวข้างต้น สำหรับประเทศไทยควรมีการบัญญัติกฎหมายเพิ่มเติมในส่วนของนายหน้าข้อมูล โดยกำหนดแนวปฏิบัติให้แก่นายหน้าข้อมูล เพื่อให้อยู่ภายใต้กรอบที่กฎหมายกำหนด และการกำหนดบทลงโทษที่สามารถใช้บังคับได้อย่างเป็นธรรมแก่เจ้าของข้อมูล

(รศ.พินิจ ทิพย์มณี)

อาจารย์ที่ปรึกษา

Thesis Title	LEGAL ISSUES RELATING TO THE PERSONAL DATA PROTECTION : A CASE STUDY ON THE DATA BROKER
Author	Nidyarnamorn Insuk
Thesis Advisor	Associate Professor Pinit Thipmanee
Program	Master of Laws
Academic Year	2022

ABSTRACT

Issues regarding the protection of personal data and the trade of data have been around for a long time. Currently, Thailand has the Personal Data Protection Act, B.E. 2562 (2019), or PDPA, to ensure the effectiveness of data protection and provide remedies for individuals whose rights have been violated. However, in Thailand, the protection of personal data regarding data brokers is not yet included in the act, and there are no laws specifically regulating the protection of personal data relating to data brokers. In addition to that, countries that have legal systems similar to Thailand, such as Japan who has the Act on the Protection of Personal Information (APPI), or even international organizations, such as the European Union or the Organization for Economic Cooperation and Development (OECD), do not regulate the laws specifically relating to data brokers either.

This study found that in foreign countries such as the United States, the state of California has enacted a definition of data brokers in the California Consumer Privacy Act (CCPA), which is a state-wide law (California Civil Code §1798.99.88), and has established conditions within the framework of CCPA. Vermont also has regulations about data brokers and has defined the definition of a personal data broker in the Vermont Data Broker Regulation (VDBR) and has provided guidelines or regulations of data brokers in the Guidance on Vermont's Act 171 of 2018 Data Broker Regulation. This has enabled the buying and selling of data to be conducted within legal boundaries, making it easier to verify the source of purchased data. Although Singapore uses the same legal system as the United States, Singapore has not enacted any specific regulations about data brokers, similar to Thailand.

Hence, there should be amendments to the laws in Thailand regarding data brokers,

specifying practices for data brokers to operate within legal frameworks and punishments that can be enforced to fairly protect data owners.

(รศ.พิมล ทิพย์มณี)

Advisor

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้อย่างสมบูรณ์ โดยได้รับความอนุเคราะห์อย่างดียิ่งจากหลายท่าน ทำให้วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้ด้วยดี วิทยานิพนธ์ฉบับนี้จะสำเร็จด้วยดีมิได้ หากขาดบุคคลากรทุกท่านเหล่านี้ และขอกราบขอบพระคุณและจารึกพระคุณนี้ไว้อย่างมิลืมเลือน

ผู้เขียนขอกราบขอบพระคุณ ท่านรองศาสตราจารย์พินิจ ทิพย์มณี ที่ให้ความเมตตารับเป็นอาจารย์ที่ปรึกษา โดยได้สละเวลาอันมีค่ายิ่งในการช่วยชี้แนะ ให้ความรู้ คำปรึกษาต่าง ๆ เพื่อความสมบูรณ์ความถูกต้องของเนื้อหา และรูปแบบในการทำวิทยานิพนธ์ฉบับนี้ รวมถึงกรุณารับเป็นกรรมการสอบวิทยานิพนธ์ด้วย

ผู้เขียนขอกราบขอบพระคุณ ผศ.ดร.สมชาย รัตนชื่อสกุล ที่ให้กรุณารับเป็นประธานกรรมการสอบวิทยานิพนธ์ และผศ.ดร.สิรีกานต์ อยู่เรือง ที่กรุณารับเป็นกรรมการสอบวิทยานิพนธ์ และที่ท่านได้สละเวลาอันมีค่ายิ่งที่ทำการตรวจพิจารณา ให้ความรู้ คำแนะนำในการปรับปรุง แก้ไขวิทยานิพนธ์ฉบับนี้ให้มีความสมบูรณ์ยิ่งขึ้น

ผู้เขียนขอกราบขอบพระคุณ อาจารย์ ดร.อังค์วรา ไชยองค์ ที่สละเวลาอันมีค่าให้การชี้แนะ ให้ความรู้ และคำปรึกษาในการทำวิทยานิพนธ์ฉบับนี้

นอกจากนี้ ผู้เขียนขอขอบพระคุณ นายดุลยวัต ธรรมรัตนวิมล ในการให้ความช่วยเหลือ และให้คำแนะนำเกี่ยวกับวิทยานิพนธ์ฉบับนี้ ขอขอบพระคุณ พี่ๆ ในคณะนิติศาสตร์ ปรีดี พนมยงค์ ทุกท่านที่ให้ความช่วยเหลือ ให้คำแนะนำ ในการทำวิทยานิพนธ์ฉบับนี้ เพื่อให้สำเร็จลุล่วงด้วยดี

สุดท้ายนี้ผู้เขียนขอขอบพระคุณ คุณพ่อ คุณแม่ ที่ให้กำลังใจในการทำวิทยานิพนธ์ฉบับนี้ และให้การสนับสนุน ให้มีแรงผลักดันในการทำวิทยานิพนธ์ฉบับนี้ให้สำเร็จลุล่วงด้วยดี

หากวิทยานิพนธ์ฉบับนี้เกิดความรู้อันเป็นประโยชน์ทางการศึกษา ทางวิชาการ หรือทางด้านอื่นๆ ผู้เขียนขอมอบประโยชน์แห่งการนี้ให้แก่ คุณพ่อ คุณแม่ ครูบาอาจารย์ และทุกๆ ท่าน ทั้งที่เอ่ยนามและไม่ได้เอ่ยนาม รวมถึงผู้แต่งหนังสือ ตำรา ผู้เขียนวิทยานิพนธ์ บทความ ทุกท่าน ที่ผู้เขียนนำมาอ้างอิงในวิทยานิพนธ์ฉบับนี้ ตลอดจนที่มีผลให้การทำวิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปด้วยดี แต่หากมีข้อผิดพลาดประการใดในวิทยานิพนธ์ฉบับนี้ ผู้เขียนขอน้อมรับไว้แต่เพียงผู้เดียว

นิจญาณอมร อินสุข

สารบัญ

หน้า

สารบัญ (ต่อ)

บทที่ **หน้า**

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันประเทศไทยมีประชากรกว่า 66 ล้านคน ข้อมูลของประชากรตั้งแต่เกิดจนถึงเสียชีวิตจะถูกจัดเก็บโดยหน่วยงานของรัฐ และมีข้อมูลจำนวนมากที่ถูกจัดเก็บโดยหน่วยงานเอกชนเช่นกัน ข้อมูลต่าง ๆ ล้วนเป็นข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคล ได้แก่ เลขบัตรประจำตัวประชาชน ทะเบียนบ้าน เบอร์โทรศัพท์ ข้อมูลทางการแพทย์ เป็นต้น ในยุคแอนะล็อก กล่าวคือ ยุคที่โทรศัพท์มือถือเป็นรูปแบบสัญญาณวิทยุส่งคลื่นเสียงสามารถโทรออกและรับสายเท่านั้น โดยในยุคแอนะล็อกข้อมูลต่าง ๆ จะถูกจัดเก็บไว้เป็นระบบกระดาษ หรือที่เรียกว่า การจัดเก็บข้อมูลรูปแบบออฟไลน์ (Offline) โดยมีการจัดเก็บไว้อย่างดีทั้งในสถานที่ราชการ หรือองค์กรที่ให้คำมั่นว่าจะจัดเก็บข้อมูลไว้เป็นความลับ แต่เมื่อโลกได้มีการพัฒนาเปลี่ยนแปลงไป โดยมีเครื่องมืออิเล็กทรอนิกส์และอินเทอร์เน็ตเข้ามามีบทบาทในชีวิตของผู้บริโภคในสังคม ข้อมูลส่วนบุคคลต่าง ๆ จะถูกจัดเก็บไว้ในระบบอิเล็กทรอนิกส์หรือระบบอินเทอร์เน็ต หรือที่เรียกว่าการจัดเก็บข้อมูลรูปแบบออนไลน์ (Online) เพื่อให้สามารถจัดการข้อมูลได้สะดวกและง่ายต่อการค้นหาข้อมูล แต่การจัดเก็บข้อมูลรูปแบบออนไลน์ (Online) อาจมีความเสี่ยงต่อการโจรกรรมข้อมูล โดยมีบุคคลที่สามดำเนินการรวบรวมและจัดเก็บข้อมูลต่าง ๆ ของผู้บริโภค โดยที่ผู้บริโภคไม่สามารถทราบได้ เช่น แฮ็กเกอร์ บริษัทผู้ให้บริการ แอปพลิเคชัน บริษัทขายประกัน หรือธนาคารผู้ปล่อยสินเชื่อ เป็นต้น ปัจจุบันถือได้ว่าเทคโนโลยีเข้ามามีบทบาท และมีอิทธิพลต่อการดำเนินชีวิตประจำวันอย่างหลีกเลี่ยงไม่ได้ ส่งผลให้องค์กรต่าง ๆ ทั้งหน่วยงานภาครัฐและภาคเอกชน ทั้งขนาดใหญ่และขนาดเล็กต้องปรับเปลี่ยนแผนการดำเนินธุรกิจ และกลยุทธ์ในการบริหารองค์กรให้ทันต่อโลกที่มีการเปลี่ยนแปลงไปอย่างรวดเร็ว โดยนำเทคโนโลยีเข้ามาช่วยสนับสนุนการปฏิบัติงานด้านต่าง ๆ เพื่อสร้างความได้เปรียบทางการแข่งขันด้านธุรกิจสำหรับภาคเอกชน หรือสนับสนุนด้านการกำหนดนโยบายงานด้านกำกับดูแล สำหรับหน่วยงานภาครัฐ โดยเฉพาะอย่างยิ่งในยุคที่มีการเติบโตของข้อมูลที่มีปริมาณมากมายมหาศาล อีกทั้งข้อมูลมีรูปแบบหลากหลาย ไม่ว่าจะเป็นข้อความ รูปภาพ วิดีโอมัลติมีเดีย และยังเป็นข้อมูลที่เปลี่ยนแปลงตลอดเวลาและรวดเร็ว[1] ซึ่งในยุคปัจจุบันหลายธุรกิจกำลังเข้าสู่โลกของการทำการตลาดการค้าออนไลน์ หรือการทำการตลาดดิจิทัล เนื่องจากในปัจจุบันเป็นยุคที่การพัฒนาเทคโนโลยีดิจิทัลกำลังนำสังคมโลกเข้าสู่การวิวัฒนาการอย่างรวดเร็วแบบก้าวกระโดด มีความซับซ้อน เชื่อมโยงได้หลายมิติ ไร้พรมแดน และคาดการณ์ได้ยาก โดยการใช้เทคโนโลยีสารสนเทศ และการสื่อสาร การโทรคมนาคม เครือข่ายอินเทอร์เน็ตที่เชื่อมโยงไปทุกพื้นที่สามารถส่งผ่านข้อมูลขนาดใหญ่ด้วยความเร็วสูงได้อย่างมีประสิทธิภาพเป็น

[1] สาครรัตน์ นักปราชญ์, คัคนางค์ จามะริก, ‘การเปิดเผยข้อมูลภาครัฐในรูปแบบ (Business Intelligence (BI) ในยุค Big Data)’ (2559) วารสาร กสทช. ประจำปี 2559, <https://so04.tci-thaijo.org/index.php/NBTC_Journal/article/download/119148/ 91209/308584>. สืบค้นเมื่อ 1 สิงหาคม 2565.

การเปลี่ยนผ่านจากยุคแอนะล็อกเข้าสู่ยุคดิจิทัล ทำให้กิจการต่าง ๆ ของทุกภาคส่วนถูกพัฒนาโดยเทคโนโลยีให้มีความทันสมัยในทุก ๆ ด้าน ส่งผลกระทบต่อระบบเศรษฐกิจ การเมือง สังคมจิตวิทยา ความมั่นคง และวิถีชีวิตของประชาชนทุกคนในสังคม การคิดค้นพัฒนาเทคโนโลยีคอมพิวเตอร์ และการสื่อสารเชื่อมโยงกันเป็นระบบเครือข่าย (Network system) ทำให้วิวัฒนาการของสังคมโลกเป็นไปอย่างรวดเร็วมีอัตราเร่งสูง มีการพัฒนาแอปพลิเคชัน มาใช้บนเครื่องคอมพิวเตอร์และโทรศัพท์มือถือ ให้สามารถติดต่อสื่อสารบนโลกออนไลน์โดยใช้ Social Media , Platform , Big Data และปัญญาประดิษฐ์ (Artificial Intelligence (AI)) ที่มีความฉลาดสามารถติดต่อสื่อสาร และสั่งการให้เครื่องมือและอุปกรณ์ต่าง ๆ สามารถทำงานได้เองโดยอัตโนมัติ ทำให้เกิด Digital Disruption หรือการเปลี่ยนแปลงที่เกิดจากเทคโนโลยีดิจิทัล ทำให้มนุษย์มีความสะดวกสบายและมีคุณภาพชีวิตดีขึ้น ในขณะเดียวกันก็ทำให้เกิดปัญหาการว่างงาน การเลื่อมล้ำของรายได้ และอาชญากรรมทางไซเบอร์ตามมา[2] เนื่องจากการเข้าถึงข้อมูลและการประมวลผลข้อมูลของผู้บริโภคสามารถทำได้โดยง่าย สะดวก และรวดเร็ว

ปัจจุบันมักเกิดขึ้นบ่อยครั้งที่พบว่ามีโทรศัพท์จากเลขหมายที่ไม่รู้จัก หรือไม่ปรากฏเลขหมายโทรศัพท์ติดต่อมาถึงเจ้าของข้อมูลซึ่งเป็นผู้บริโภค โดยอ้างว่าเป็นบุคคลที่รู้จักหรือสนิทกับเจ้าของข้อมูล หรือบางครั้งอาจเป็นการเสนอขายประกันชีวิต เสนอสินเชื่อส่วนบุคคล หรือเสนอขายสินค้าในรูปแบบขายตรง ซึ่งเจ้าของข้อมูลมิได้ให้ข้อมูลส่วนตัวไว้แก่บุคคลหรือบริษัทเหล่านั้นแต่อย่างใด เหตุใดบริษัทเหล่านั้นจึงมีหมายเลขโทรศัพท์ส่วนตัว ซึ่งเป็นข้อมูลส่วนบุคคลของเจ้าของข้อมูลได้ ในกรณีของมิจฉาชีพ การกระทำดังกล่าวอาจเป็นผลจากการที่มิจฉาชีพเล็งเห็นว่าเป็นช่องทางที่สะดวกที่สุด เพียงใช้เทคนิคทางจิตวิทยาในการโน้มน้าวก็สามารถได้เงินมาอย่างง่าย หรือในกรณีของบริษัทต่าง ๆ อาจมีความเกี่ยวข้องปัจจัยทางการตลาดของผู้ประกอบการที่ต้องการขยายช่องทางในการเสนอขายสินค้า เพื่อให้ตรงตามเป้าหมายที่กำหนด การโฆษณาสินค้าทางโทรศัพท์อาจก่อให้เกิดความรำคาญใจต่อเจ้าของข้อมูล และการกระทำเช่นนี้ ปัจจุบันได้ครอบคลุมไปถึงกลุ่มมิจฉาชีพ โดยนับวันยิ่งทวีความรุนแรงมากขึ้น ส่งผลให้เจ้าของข้อมูลสูญเงินเป็นจำนวนมาก และข้อมูลส่วนบุคคลต่าง ๆ ที่อยู่บนระบบอินเทอร์เน็ตอาจถูกมิจฉาชีพหรือแฮกเกอร์ที่เป็นนายหน้าข้อมูล นำข้อมูลที่ได้จากฐานข้อมูลในเว็บไซต์ต่าง ๆ ไปเสนอขายให้แก่บริษัทหรือกลุ่มบุคคลที่สนใจหรือต้องการข้อมูล

นายหน้าข้อมูลเป็นธุรกิจที่ดำเนินการ ซื้อ รวบรวม จัดเก็บ และขายข้อมูลให้แก่บริษัทหรือกลุ่มบุคคลที่สนใจหรือต้องการข้อมูลต่าง ๆ ซึ่งการขายข้อมูลของนายหน้าข้อมูลส่งผลกระทบต่อการดำรงชีวิตของผู้บริโภคเป็นอย่างมาก ข้อมูลบางส่วนถูกนำไปใช้เพื่อประกอบธุรกิจ แต่ข้อมูลบางส่วนอาจถูกนำข้อมูลไปใช้ในทางที่มิชอบ เช่น การถูกมิจฉาชีพหลอกให้ทำธุรกรรมทางการเงิน เนื่องด้วยสาเหตุต่าง ๆ ส่งผลให้เจ้าของข้อมูลหรือบุคคลที่มีความเกี่ยวข้องต่อการทำธุรกรรมนั้น ๆ สูญเงินเป็นจำนวนมาก และในปัจจุบันการนำข้อมูลไปใช้ในทางที่มิชอบมีการขยายวงกว้างมากขึ้น ส่งผลกระทบต่อผู้บริโภคเป็นอย่างมาก เจ้าของข้อมูลซึ่ง

[2] ปัณณทัต กาญจนะวสิต, โลกยุค 4.0 World 4.0 (สำนักงานเลขานุการกองทัพบก 2559) 1.

เป็นผู้บริโภคบางรายอาจทราบถึงภัยที่เกิดขึ้น โดยปัจจุบันมีกลุ่มมิจฉาชีพโทรศัพท์ถึงเจ้าของข้อมูล โดยหลอกให้เจ้าของข้อมูลโอนเงินไปยังบัญชีที่กลุ่มมิจฉาชีพกำหนด เพื่อสะดวกต่อการดำเนินการต่าง ๆ เช่น การดำเนินการลงบันทึกประจำวันในสำนักงานตำรวจฯ แทนเจ้าของข้อมูล หรือการโอนค่าศุลกากรเพื่อเสียภาษีนำเข้าสินค้าที่ผิดกฎหมาย โดยให้โอนเงินผ่านบัญชีม้า เป็นต้น และนอกจากนี้กลุ่มมิจฉาชีพได้มีการพัฒนาจากการโทรศพท์เป็นการส่งข้อความ โดยอ้างชื่อว่าเป็นหน่วยงานราชการ หรือหน่วยงานรัฐวิสาหกิจ และให้ดำเนินการกดลิ้งค์และกรอกข้อมูลส่วนบุคคลของเจ้าของข้อมูล ผ่านโทรศัพท์มือของเจ้าของข้อมูล แต่เจ้าของข้อมูลบางรายอาจไม่ทันต่อภัยที่เกิดขึ้นในปัจจุบัน หรือไม่ทราบถึงภัยดังกล่าวที่เกิดขึ้น เช่น การติดต่อมาเพื่อให้ทำธุรกรรมทางการเงิน โดยการหลอกว่าเป็นบุคคลที่รู้จักกันมานาน ซึ่งเป็นการก่อให้เกิดความรำคาญต่อเจ้าของข้อมูล หรือดังที่ปรากฏเป็นข่าวขึ้น ในประเทศไทยเมื่อประมาณเดือนกุมภาพันธ์ พ.ศ. 2565 เป็นข้อมูลของเยาวชนจากฐานข้อมูลเว็บไซต์ mytcas.com ซึ่งเป็นระบบกลางของการสอบเข้ามหาวิทยาลัยของประเทศไทย จำนวนกว่า 23,000 รายการ และข้อมูลเหล่านั้นได้ถูกนำไปขายในเว็บบอร์ดมืดในเว็บไซต์หนึ่ง โดยข้อมูลรั่วไหลที่ถูกเผยแพร่ออกไปนั้น ล้วนเป็นข้อมูลส่วนบุคคลทั้งสิ้น ได้แก่ ชื่อ นามสกุล ที่มีข้อมูลภาษาไทยและภาษาอังกฤษ หมายเลขบัตรประจำตัวประชาชนในระบบ Mytcas รหัสมหาวิทยาลัยที่เลือก รหัสคณะที่เลือก และสถานะในระบบการสอบอื่น ๆ และต่อมาทางสมาคมที่ประชุมอธิการบดีแห่งประเทศไทย (ทปอ.) ได้ชี้แจงว่า “ข้อมูลดังกล่าวเป็นข้อมูลของ TCAS64 จริง คาดว่าน่าจะหลุดออกมาจากขั้นตอนที่เจ้าหน้าที่ของมหาวิทยาลัยนำข้อมูลออกไปเพื่อจัดเรียงคะแนน ซึ่งเป็นเพียงข้อมูลบางส่วนเท่านั้น ไม่ใช่ข้อมูลทั้งหมดที่มีกว่า 826,250 รายการ” โดยการกระทำดังกล่าวถือเป็นการละเมิดสิทธิส่วนบุคคลของเจ้าของข้อมูล

เนื่องจากเทคโนโลยีในปัจจุบันมีความก้าวหน้า และช่องทางการสื่อสารมีความหลากหลาย ทำให้การละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลสามารถกระทำได้โดยง่าย และหลายครั้งนำมาซึ่งความเดือดร้อนรำคาญ หรือสร้างความเสียหายให้แก่เจ้าของข้อมูล ตลอดจนสามารถส่งผลต่อเศรษฐกิจโดยรวมของประเทศ จึงเป็นเหตุในการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วน พ.ศ. 2562 (Personal Data Protection Act, B.E. 2562 (2019) (PDPA)) ซึ่งได้ประกาศในราชกิจจานุเบกษาเมื่อวันที่ 27 พฤษภาคม พ.ศ. 2562 แต่ปรากฏว่าได้เลื่อนการบังคับใช้ด้วยเหตุผลที่ว่า “โดยที่พระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดยกเว้นไม่ให้นำบทบัญญัติบางส่วนแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาใช้บังคับแก่บางหน่วยงานและบางกิจการในช่วงระยะเวลาระหว่างวันที่ 27 พฤษภาคม พ.ศ. 2563 จนถึงวันที่ 31 พฤษภาคม พ.ศ. 2564 อันเนื่องจากการปฏิบัติตามหลักเกณฑ์ วิธีการ และเงื่อนไขตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดนั้นมีรายละเอียดมากและซับซ้อน กับต้องใช้เทคโนโลยีขั้นสูงเพื่อให้การคุ้มครองข้อมูลส่วนบุคคลเป็นไปอย่างมีประสิทธิภาพสมดังเจตนารมณ์ของกฎหมาย ประกอบกับสถานการณ์การแพร่ระบาดของโรคติดเชื้อไวรัสโคโรนา 2019 ยังคงมีอยู่อย่างต่อเนื่องและรุนแรงยิ่งขึ้นจนถึงปัจจุบัน ส่งผลกระทบต่อเศรษฐกิจและสังคมโดยรวมเป็นอย่างมาก ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็น

หน่วยงานและกิจการต่าง ๆ ทั้งภาครัฐและภาคเอกชนจำนวนมากทั่วประเทศยังไม่พร้อมที่จะปฏิบัติตามพระราชบัญญัติดังกล่าว ดังนั้น เพื่อเป็นการบรรเทาผลกระทบที่จะเกิดขึ้น สมควรขยายระยะเวลาการใช้บังคับพระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ออกไปอีกจนถึงวันที่ 31 พฤษภาคม พ.ศ. 2565 จึงจำเป็นต้องตราพระราชกฤษฎีกานี้”[3] และมีผลบังคับใช้เมื่อวันที่ 1 มิถุนายน พ.ศ. 2565 ซึ่งพระราชบัญญัติฉบับนี้เป็นการกำหนด เพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่รวมถึงการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ในต่างประเทศมีบริษัทที่ทำธุรกิจเกี่ยวกับข้อมูลเป็นจำนวนมาก โดยบริษัทเหล่านี้จะทำการเก็บรวบรวมข้อมูลของกลุ่มบุคคลเป้าหมายจากอินเทอร์เน็ตที่เป็นข้อมูลออนไลน์ (Online) รวมไปถึงข้อมูลจากออฟไลน์ (Offline) ให้กับลูกค้าของตัวเองเพื่อเอามาใช้ประโยชน์ ไม่ว่าจะเป็นเชิงพาณิชย์ หรือเชิงกฎหมาย ฯลฯ บริษัทเหล่านั้น อาจซื้อข้อมูลของกลุ่มลูกค้าที่เป็นที่ต้องการของตลาดจากแหล่งอื่นโดยตรง เช่น การซื้อข้อมูลสุขภาพผู้ป่วยจากคลินิก การซื้อข้อมูลการใช้รถจากบริษัทขายรถ ฯลฯ และขายให้กับผู้ที่ต้องการใช้ประโยชน์จากข้อมูลดังกล่าว ถึงแม้ข้อมูลบางอย่างอาจไม่ถูกต้อง แต่สามารถเป็นประโยชน์ให้กับนักลงทุน นักการตลาด หรือบริษัทโฆษณาต่าง ๆ โดยบริษัทที่ทำการซื้อขายข้อมูลของบุคคลอื่น เรียกว่า Data Brokers หรือนายหน้าข้อมูล หากข้อมูลถูกซื้อไปโดยมือปืนรับจ้างหรือผู้ประสงค์ร้ายต่อเจ้าของข้อมูล อาจส่งผลกระทบต่อเจ้าของข้อมูลได้ ในประเทศไทยสามารถเห็นหรือรับรู้ถึงการเข้าถึงข้อมูลที่ได้จากการซื้อขายข้อมูลได้จากการที่เจ้าของข้อมูลไม่ทราบความเป็นมาของบุคคลที่สาม ในการเสนอขาย หรือเสนอการให้บริการอย่างใดเปรียบเสมือนการถูกละเมิดสิทธิความเป็นส่วนตัวของเจ้าของข้อมูล

บางรัฐในสหรัฐอเมริกา เช่น รัฐแคลิฟอร์เนีย และรัฐเวอร์มอนต์ ก่อนหน้านี้ข้อมูลส่วนบุคคลสามารถสร้างกำไรมหาศาล และเอื้อประโยชน์ให้กับกลุ่มคนที่หาประโยชน์จากข้อมูลของบุคคลอื่น แต่ปัจจุบันเมื่อกฎหมายมีความเข้มงวดขึ้น แต่ยังมีข้อยกเว้นในบางธุรกิจ เช่น นายหน้าข้อมูลที่นำข้อมูลของบุคคลอื่นรวบรวมมาใช้ทำเป็นสมุดโทรศัพท์ เพื่อช่วยให้ธุรกิจต่าง ๆ สามารถใช้ประโยชน์จากข้อมูลในสมุดโทรศัพท์ได้และไม่สร้างความเสียหายให้กับเจ้าของข้อมูลและผู้ที่ทำการซื้อข้อมูลเอง แต่เมื่อเทคโนโลยีปัจจุบันมีการพัฒนาอย่างต่อเนื่อง การรวบรวมข้อมูลสามารถทำได้โดยง่าย ข้อมูลส่วนบุคคลบางส่วนที่ถูกจัดเก็บจึงถูกนำไปใช้ในแง่ที่เกี่ยวกับเทคโนโลยีเช่นกัน เช่น ถูกนำไปใช้ในงานโปรแกรมที่สร้างขึ้นเพื่อดูแลการสนทนาของผู้ใช้งาน เพื่อให้จดจำรูปแบบการสนทนาที่ซ้ำ ๆ และเมื่อโปรแกรมที่สร้างขึ้นเพื่อดูแลการสนทนาของผู้ใช้งานสามารถจดจำรูปแบบการสนทนาได้ก็สามารถโต้ตอบกับผู้ใช้งานได้ เช่น งานที่ต้องวิเคราะห์คำถามของผู้ใช้งานและงานลูกค้าสัมพันธ์ ส่วนปัญญาประดิษฐ์ (Artificial Intelligence (AI)) ก็นำเอาข้อมูลส่วนบุคคลไปใช้เพื่อพัฒนาระบบหุ่นยนต์ที่มีอยู่เดิมให้ดูมีความสามารถด้านเชาว์ปัญญาที่ดีขึ้น ดังนั้น ไม่ว่าจะเป็นการประกาศบท

[3] หมายเหตุ แห่งพระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (ฉบับที่ 2) พ.ศ. 2564.

สนทนา หรือแสดงความคิดเห็น ข้อมูลเหล่านี้จะช่วยให้ปัญญาประดิษฐ์และหุ่นยนต์ทำงานได้อย่างมีประสิทธิภาพ และสามารถทำงานได้ใกล้เคียงมนุษย์มากยิ่งขึ้น

ในปัจจุบันการมีฐานข้อมูล และบัญชีรายชื่อลูกค้าที่เพียงพอ เป็นสิ่งสำคัญสำหรับการทำการตลาดทางตรง เพราะธุรกิจจะไม่สามารถสื่อสารหรือเข้าถึงกลุ่มลูกค้าที่คาดหวังได้ หากปราศจากข้อมูลและบัญชีรายชื่อลูกค้า การจัดเก็บข้อมูลส่วนบุคคลโดยทั่วไป มีจุดมุ่งหมายเพื่อให้บริการ หรือเพื่อดำเนินการทางนิติกรรม หรือธุรกรรมกับผู้ที่เป็นเจ้าของข้อมูล โดยปกติเจ้าของข้อมูลจะต้องยินยอมให้ข้อมูลกับบริษัทหรือหน่วยงานที่จัดเก็บข้อมูลโดยตรง ด้วยความเข้าใจว่าข้อมูลที่บริษัทหรือหน่วยงานจัดเก็บไว้เป็นไปเพื่อใช้ในกิจกรรมที่ตนเองเกี่ยวข้องกับบริษัทนั้น ๆ เท่านั้น ปัญหาผู้จัดเก็บอาจนำข้อมูลไปใช้ในทางอื่นที่เจ้าของข้อมูลไม่ยินยอม หรือวิธีการจัดเก็บข้อมูลไม่ดีหรือไม่ได้มาตรฐาน อาจมีผู้ลักลอบนำข้อมูลไปใช้ประโยชน์ในทางที่มิชอบได้

จากการศึกษาพบว่า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีปัญหาดังนี้

1. การซื้อขายข้อมูลโดยนายหน้าข้อมูล
2. ขอบเขตความรับผิดของนายหน้าข้อมูล และ
3. การกำกับดูแลนายหน้าข้อมูลโดยหน่วยงานของรัฐ

1.2 วัตถุประสงค์ของการศึกษา

1.2.1 เพื่อศึกษาถึงประวัติความเป็นมาเกี่ยวกับการจัดเก็บข้อมูล แนวคิดและทฤษฎีที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

1.2.2 เพื่อศึกษาถึงมาตรการที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลจากการซื้อขายข้อมูลโดยนายหน้าข้อมูล ในต่างประเทศ เฉพาะ สหภาพยุโรป (European Union (EU)) ข้อตกลงรัฐสภายุโรปและองค์การเพื่อความร่วมมือทางด้านเศรษฐกิจและการพัฒนา (The Organization for Economic Co-operation and Development (OECD)) ประเทศสหรัฐอเมริกา เฉพาะรัฐแคลิฟอร์เนีย และรัฐเวอร์มอนต์ ประเทศญี่ปุ่น และประเทศสิงคโปร์

1.2.3 เพื่อศึกษาถึงสภาพปัญหาของการคุ้มครองข้อมูลส่วนบุคคลจากการซื้อขายข้อมูลโดยนายหน้าข้อมูล

1.2.4 เพื่อศึกษาหาแนวทางแก้ไขปัญหาเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลจากการซื้อขายข้อมูลโดยนายหน้าข้อมูล

1.3 สมมติฐานของการศึกษา

การคุ้มครองข้อมูลส่วนบุคคลจากการซื้อขายข้อมูลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในปัจจุบันมิได้บัญญัติในส่วนของคำนิยาม เนื่องจากยังไม่มีบทกฎหมายบัญญัติให้ความคุ้มครองไว้เป็นการเฉพาะทั้งในส่วนของการซื้อขายข้อมูล และในส่วนของแนวปฏิบัติของนายหน้าข้อมูล ในการปรับใช้ข้อกฎหมายเกี่ยวกับการซื้อขายข้อมูล ประกอบกับไม่มีหน่วยงานที่เข้ามากำกับดูแล ควบคุม โดยการกำหนดหลักเกณฑ์ หรือแนวปฏิบัติ ที่ช่วยให้การดำเนินงานของนายหน้าข้อมูลที่ทำการซื้อขายข้อมูลเป็นไปอย่างมีประสิทธิภาพ และเกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลอย่างน้อยที่สุด และยังไม่มีกฎหมายบัญญัติกำหนดขอบเขตความรับผิดและบทลงโทษเมื่อมีการซื้อขายข้อมูลในลักษณะที่เป็นการละเมิดเกิดขึ้น โดยการแก้ไขปัญหาที่เกิดขึ้นอาจทำได้เพียงการนำกฎหมายที่มีอยู่ปัจจุบันที่เกี่ยวข้องกับประเด็นปัญหามาปรับใช้บังคับเป็นกรณีไป แต่อย่างไรก็ตามกฎหมายที่นำมาปรับใช้ก็ไม่สามารถแก้ไขปัญหาได้ในทุกกรณี เนื่องจากบทกฎหมายดังกล่าวย่อมมีข้อจำกัด จึงควรที่จะปรับปรุงแก้ไข กำหนดเงื่อนไขเป็นการเฉพาะเพื่อป้องกันปัญหาที่จะเกิดขึ้นในภายหลัง แม้ว่าสิทธิในฐานะของการเป็นเจ้าของข้อมูลจะได้รับการคุ้มครอง แต่การใช้สิทธิก็ต้องเป็นไปตามหลักเกณฑ์ของกฎหมาย และไม่ละเมิดสิทธิหรือเสรีภาพของผู้อื่นที่เป็นเจ้าของข้อมูลส่วนบุคคล หากข้อมูลดังกล่าวถูกนำไปใช้ในสถานการณ์ที่เจ้าของข้อมูลประสงค์ที่จะกระทำการหรือต้องการสิ่งเหล่านั้นถือว่าเป็นผลดีกับเจ้าของข้อมูล เนื่องจากเป็นการเอื้อประโยชน์ให้แก่เจ้าของข้อมูล ส่งผลให้เจ้าของข้อมูลสามารถตัดสินใจได้อย่างรวดเร็ว แต่หากข้อมูลดังกล่าวถูกนำไปใช้ในสถานการณ์ที่เจ้าของข้อมูลไม่ต้องการหรือข้อมูลดังกล่าวถูกใช้นำไปโดยผู้ไม่หวังดี ก็สามารถสร้างความเดือดร้อนและความเสียหายให้กับเจ้าของข้อมูลได้เช่นกัน

1.4 ขอบเขตการศึกษา

ศึกษาถึงประวัติความเป็นมาเกี่ยวกับการจัดเก็บข้อมูล แนวคิดและทฤษฎีที่เกี่ยวข้องกับข้อมูลส่วนบุคคล และแนวคิด ทฤษฎีเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงกฎหมายและหลักเกณฑ์ แนวปฏิบัติของต่างประเทศ และประเทศไทยที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลจากการซื้อขายข้อมูล

1.5 วิธีการดำเนินการศึกษา

ศึกษาค้นคว้าจากการวิจัยเอกสาร รวมรวบจาก หนังสือ ตำรา บทความ เอกสารต่างๆ และสืบค้นข้อมูลจากอินเตอร์เน็ต เพื่อศึกษาถึงปัญหาที่เกิดขึ้นและหาแนวทางการปรับใช้ให้เกิดความเหมาะสมกับสภาพสังคมในปัจจุบันและในอนาคตต่อไป

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1.6.1 ทำให้ทราบถึงประวัติความเป็นมา แนวคิด ทฤษฎี และหลักการพื้นฐานที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

1.6.2 ทำให้ทราบถึง แนวคิด ทฤษฎี และหลักการพื้นฐานที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลจากการซื้อขายข้อมูล โดยนายหน้าข้อมูล

1.6.3 ทำให้ทราบถึงกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลจากการซื้อขายข้อมูล โดยนายหน้าข้อมูล

1.6.4 ทำให้ทราบถึงแนวทางการแก้ไขปัญหาในกรณีการคุ้มครองข้อมูลส่วนบุคคลจากการซื้อขายข้อมูลโดยนายหน้าข้อมูล

บทที่ 2
ประวัติความเป็นมา แนวคิด ทฤษฎี และหลักการพื้นฐานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

ตั้งแต่อดีตจนถึงปัจจุบันปฏิเสธไม่ได้ว่าการมีข้อมูลให้อยู่ในการเก็บรวบรวมอย่างมากที่สุด สามารถทำให้การดำเนินธุรกิจให้ประสบความสำเร็จได้ และส่วนใหญ่ผู้ประกอบกิจการจำเป็นจะต้องปรับตัวให้ทันต่อสภาวการณ์ของโลกที่เปลี่ยนแปลงไป อาจเนื่องด้วยความก้าวหน้าทางเทคโนโลยีสารสนเทศ (Information Technology หรือ IT) ควบคู่ไปด้วย เพื่อให้การเก็บรวบรวมข้อมูล และประมวลผลข้อมูลสามารถทำได้โดยง่าย ในปัจจุบันสามารถประมวลผลข้อมูลจำนวนมหาศาลได้อย่างรวดเร็ว ข้อมูลต่าง ๆ จึงเปรียบเสมือนวัตถุดิบชั้นเยี่ยมที่ผู้ประกอบกิจการนำมาใช้ประมวลผลเพื่อวิเคราะห์ และหาแนวทางในการดำเนินธุรกิจ ข้อมูลที่นำมาใช้ส่วนใหญ่มักเป็นข้อมูลส่วนบุคคลของผู้บริโภคที่ผู้ประกอบกิจการอาจได้รับข้อมูลมาจากผู้บริโภคโดยตรง โดยผู้บริโภคให้ข้อมูลกับธุรกิจนั้น ๆ เพื่อความสะดวกในการซื้อสินค้าหรือบริการ หรือดำเนินการอย่างอื่นที่มีความเกี่ยวข้องกับธุรกิจนั้น ๆ แต่ผู้ประกอบกิจการหรือธุรกิจ ซึ่งอาจเป็นบุคคลหรือกลุ่มบุคคลภายในองค์กรอาจนำข้อมูลของผู้บริโภคไปขาย เพื่อแสวงหาประโยชน์ส่วนตน โดยลูกค้าไม่ได้ยินยอม เป็นการสร้างความเดือดร้อนรำคาญให้แก่ผู้บริโภคที่เป็นเจ้าของข้อมูล ในขณะที่ข้อมูลส่วนบุคคลถือเป็นสิทธิในความเป็นส่วนตัวของเจ้าของข้อมูลที่รัฐสมาชิกแห่งองค์กรสหประชาชาติจำเป็นต้องให้ความคุ้มครองในฐานะสิทธิมนุษยชนประเภทหนึ่งตามประกาศปฏิญาณสากลว่าด้วยสิทธิมนุษยชน[1]

การคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection) ถือเป็นสิทธิมนุษยชนขั้นพื้นฐานประเภทหนึ่งที่หลายประเทศให้ความสำคัญ ถือเป็นส่วนหนึ่งของการคุ้มครองสิทธิความเป็นส่วนตัว (Right of Privacy) ความเป็นส่วนตัวย่อมหมายความรวมถึง ความเป็นส่วนตัวเกี่ยวกับข้อมูล (Information Privacy) ความเป็นส่วนตัวในชีวิตร่างกาย (Bodily Privacy) ความเป็นส่วนตัวในการติดต่อสื่อสาร (Communication Privacy) และความเป็นส่วนตัวในเคหสถาน (Territorial Privacy) โดยการคุ้มครองข้อมูลส่วนบุคคล ถือได้ว่าเป็นความส่วนตัวเกี่ยวกับข้อมูล

คำว่า “สิทธิส่วนบุคคล” หมายถึง สิทธิของบุคคลที่ประกอบไปด้วย สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัวในเรื่องดังกล่าวน่าจะจัดอยู่ในเรื่องของความ เป็นอยู่ส่วนตัวซึ่งหมายความว่า สถานะที่บุคคลจะรอดพ้นจากการสังเกต การรู้เห็น การสืบความลับ การรบกวนต่าง ๆ และความมีสันโดษไม่ติดต่อสัมพันธ์กับสังคม โดยทั้งนี้ขอบเขตที่บุคคลควรได้รับการคุ้มครองและการเคารพในสิทธิส่วนบุคคลก็คือการดำรงชีวิตอย่างเป็นอิสระ มีการพัฒนาบุคลิกลักษณะตามที่ต้องการ สิทธิที่จะแสวงหา

---

[1] ณฐพร วิริยะลัพภะ และ ธเนศ สุจารีกุล, ‘ปัญหาทางกฎหมายเกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 : ศึกษากรณีหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 39’ (การประชุมนำเสนอผลงานวิจัยระดับบัณฑิตศึกษา ครั้งที่ 15 2563) 1.

ความสุขในชีวิตตามวิถีทางที่อาจเป็นไปได้และเป็นความพอใจตราบเท่าที่ไม่ขัดต่อกฎหมาย ไม่ขัดต่อความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน และไม่เป็นการล่วงละเมิดสิทธิเสรีภาพของผู้อื่น

คำว่า ข้อมูลส่วนบุคคล (Personal Data) ได้แก่ ชื่อ - นามสกุล, เลขประจำตัวประชาชน, ที่อยู่, เบอร์โทรศัพท์, วันเกิด, อีเมล, การศึกษา, เพศ, อาชีพ, รูปถ่าย, ข้อมูลทางการเงิน นอกจากนี้ยังรวมถึง ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data) เช่น ข้อมูลทางการแพทย์หรือสุขภาพ, ข้อมูลทางพันธุกรรมและไบโอเมทริกซ์, เชื้อชาติ, ความคิดเห็นทางการเมือง, ความเชื่อทางศาสนาหรือปรัชญา, พฤติกรรมทางเพศ, ประวัติอาชญากรรม, ข้อมูลสหภาพแรงงาน เป็นต้น

ข้อมูลส่วนบุคคลเป็นสิ่งที่สำคัญต่อเจ้าของข้อมูลเป็นอย่างมาก และสามารถสร้างกำไรได้อย่างมหาศาลให้แก่บุคคลหรือกลุ่มบุคคลที่ทำธุรกิจนายหน้าข้อมูลได้เช่นกัน ตั้งแต่อดีตจนถึงปัจจุบันมีธุรกิจที่ทำหน้าที่จัดเก็บรวบรวมข้อมูลต่าง ๆ ของบุคคล กลุ่มบุคคลหรือนิติบุคคล เพื่อนำข้อมูลไปขาย เพื่อแสวงหาประโยชน์ส่วนตน และในบางครั้งอาจมีการซื้อจากแหล่งข้อมูลต่าง ๆ โดยตรง เช่น ซื้อข้อมูลการใช้บัตรเครดิตจากสถาบันการเงินผู้ปล่อยสินเชื่อ หรือการซื้อข้อมูลเบอร์โทรศัพท์จากเครือข่ายโทรศัพท์มือถือ เป็นต้น เพื่อนำมาเก็บรวบรวมไว้ และนำข้อมูลไปขายต่ออีกทอดหนึ่ง เพื่อแสวงหาประโยชน์ส่วนตน โดยที่เจ้าของข้อมูลไม่ทราบถึงการเก็บรวบรวมข้อมูลของนายหน้าข้อมูลและการนำข้อมูลไปขาย โดยธุรกิจในลักษณะนี้ เรียกว่านายหน้าข้อมูล

ดังนั้น เมื่อข้อมูลส่วนบุคคลเป็นสิ่งที่ความสำคัญต่อเจ้าของข้อมูล การจัดเก็บข้อมูลให้ดีย่อมเป็นสิ่งที่มีความสำคัญเช่นกัน เมื่อการจัดการฐานข้อมูล หรือ Database มีความเป็นระบบระเบียบ สามารถทำให้การประมวลข้อมูลต่าง ๆ สามารถทำได้โดยง่าย สะดวก และรวดเร็ว ซึ่งหากเป็นในยุคอะแนล็อกการจัดเก็บข้อมูลต่าง ๆ อาจต้องหาสถานที่ที่เป็นความลับเพื่อจัดเก็บข้อมูลให้มีความปลอดภัย แต่เมื่อเป็นยุคปัจจุบันการจัดเก็บข้อมูลเป็นรูปแบบอิเล็กทรอนิกส์ การจัดเก็บข้อมูลอาจต้องอาศัยความทันสมัยของโปรแกรมที่สามารถต่อต้านการโจรกรรมข้อมูลได้ โดยในบทนี้ผู้เขียนจะกล่าวถึงประวัติศาสตร์ความเป็นมาเกี่ยวกับการจัดเก็บข้อมูล แนวคิดและทฤษฎีที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

2.1 ประวัติความเป็นมาเกี่ยวกับการจัดเก็บข้อมูล

ในช่วงประมาณ 150 ปีก่อนคริสตกาล ชาวกรีกโบราณได้ประดิษฐ์อุปกรณ์ ชื่อว่า “Antikythera” เป็นอุปกรณ์สำหรับใช้ในการจัดเก็บข้อมูลการเคลื่อนที่ของดวงดาวบนท้องฟ้า เพื่อสร้างรูปแบบทางดาราศาสตร์

ในปี ค.ศ. 1880 Herman Hollerith สร้างอุปกรณ์ที่ใช้ในการเจาะกระดาษ เพื่อช่วยนำมาเสริมงานในด้านการจัดเก็บข้อมูลจากการสำรวจสำมะโนประชากรสหรัฐอเมริกา

ต่อมาในปี ค.ศ. 1890 อุปกรณ์ดังกล่าวนี้ได้เป็นส่วนหนึ่งของเครื่องคอมพิวเตอร์เพื่อธุรกิจหรือ IBM ในปัจจุบัน

และต่อมาในปี ค.ศ.1960 รัฐบาลสหรัฐอเมริกาได้ใช้เมนเฟรมคอมพิวเตอร์ในการจัดเก็บข้อมูลประชากรเป็นจำนวนมหาศาล และบริษัทเอกชนใช้เครื่องคอมพิวเตอร์ดังกล่าว ในการจัดเก็บข้อมูลและประมวลผลพฤติกรรมของผู้บริโภค

ในปัจจุบันเมื่อเข้าสู่ยุคอินเทอร์เน็ตข้อมูลต่าง ๆ สามารถจัดเก็บได้โดยง่าย และสะดวกขึ้น เนื่องจากข้อมูลต่าง ๆ ส่วนใหญ่จะถูกจัดเก็บผ่านคอมพิวเตอร์เป็นหลัก นอกจากจะสามารถจัดเก็บโดยใช้คอมพิวเตอร์ได้แล้ว สามารถจัดเก็บข้อมูลผ่านสมาร์ทโฟนได้เช่นกันในตอนที่ใช้งาน แต่ในอนาคตการจัดเก็บข้อมูลไม่ได้เก็บไว้และนำเอาออกมาใช้โดยมนุษย์อย่างเดียว แต่ข้อมูลเหล่านี้จะถูกนำมาใช้และวิเคราะห์ประมวลผลที่มีความเหนือชั้นขึ้น โดยวิเคราะห์ผ่านทางปัญญาประดิษฐ์ (Artificial Intelligence (AI)) และพฤติกรรมของผู้บริโภคจากข้อมูลต่าง ๆ จะถูกตัดสินไม่ทางใดก็ทางหนึ่ง เช่น ปัญญาประดิษฐ์ (Artificial Intelligence (AI)) จะแจ้งให้ทราบว่า ควรจะดูแลสุขภาพอย่างไร และผู้กระทำผิดบุคคลใดควรได้รับการประกันตัวโดยไม่ต้องกังวลว่าจะเกิดการหลบหนี สิ่งเหล่านี้เกิดจากการวิเคราะห์และประมวลผลของปัญญาประดิษฐ์ที่เก็บรวบรวมพฤติกรรมมนุษย์ ถึงแม้ในปัจจุบันจะมีข้อกำหนดในเรื่องของข้อมูลและความเป็นส่วนบุคคลมากขึ้นก็ตาม แต่บริษัทด้านเทคโนโลยี เช่น Amazon, Google, Apple และ Facebook พยายามผลักดัน เพื่อให้มีการใช้ข้อมูลของผู้บริโภคอย่างมีประสิทธิภาพ แต่ยังมีข้อถกเถียงว่า หากบริษัทเหล่านี้หรือบริษัทอื่นที่ต้องการใช้ประโยชน์จากข้อมูลส่วนบุคคลของผู้บริโภค อาจต้องมีการจ่ายเงินเพื่อซื้อข้อมูล

แต่ถึงอย่างนั้นข้อมูลส่วนบุคคลต่าง ๆ ที่ผู้บริโภคได้กรอกในแอปพลิเคชันต่าง ๆ อาจตกอยู่ในมือของบุคคลที่สามได้ง่าย เช่น แฮกเกอร์ บริษัทผู้ให้บริการแอปพลิเคชัน บริษัทขายประกัน หรือบริษัทขายยาต่าง ๆ เป็นต้น ดังนั้น จึงควรที่จะระมัดระวังในการกรอกข้อมูลส่วนตัวตามเว็บไซต์ หรือแอปพลิเคชันต่าง ๆ เพื่อป้องกันการนำข้อมูลไปใช้โดยไม่จำเป็น

จากข้อมูลดังกล่าวจะเห็นได้ว่าวิวัฒนาการการเก็บข้อมูลนับตั้งแต่อดีตจนถึงปัจจุบัน ได้มีช่องทางการจัดเก็บข้อมูลที่มีความหลากหลายดังที่ได้กล่าวไปในข้างต้น และในอนาคตอาจมีการจัดเก็บข้อมูลที่มีช่องทางเพิ่มมากขึ้น และเมื่อการจัดเก็บข้อมูลหรือการประมวลผลข้อมูลสามารถทำได้โดยง่าย อาจส่งผลกระทบในหลายด้าน อาจสะดวกต่อบุคคลที่สาม มิจฉาชีพ แฮกเกอร์ หรือผู้ไม่ประสงค์ดีต่อเจ้าของข้อมูล นำข้อมูลไป และอาจก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล หากการจัดเก็บข้อมูลไม่มีประสิทธิภาพและความปลอดภัยสูง

2.2 ที่มาและความสำคัญของอาชีพนายหน้า

อาชีพนายหน้าเป็นอาชีพหนึ่งที่มีประวัติความเป็นมาที่ยาวนาน เพราะเป็นอาชีพที่ทุกคนสามารถทำได้ เนื่องจากไม่มีกำหนดกฎเกณฑ์อายุ และอาชีพนายหน้าสามารถแบ่งได้หลายแขนง เช่น นายหน้าอสังหาริมทรัพย์ นายหน้าประกันภัย เป็นต้น โดยในบทนี้จะกล่าวถึงที่มาและความสำคัญของอาชีพนายหน้า

หลักกฎหมายนายหน้าเป็นหลักกฎหมายที่มีมาอย่างยาวนาน ครั้งเมื่อแต่สมัยโรมัน โดยเป็นหลักที่ถูกพัฒนามาจากหลักเรื่องตัวแทน[2] แต่เดิมความสัมพันธ์รูปแบบนี้ มีลักษณะเป็นการที่ตัวการแสดงออกกับตัวแทนโดยการมอบอำนาจให้ผู้ที่เป็นตัวแทนดำเนินการแทนแบบเด็ดขาด (Mandatum Contractum) กล่าวคือ อำนาจในการดำเนินการของตัวแทนนั้นมีอย่างเด็ดขาดในอันที่จะกระทำการใด ๆ ตามคำสั่งของตัวการได้ ผลแห่งอำนาจเด็ดขาดนี้เองจะส่งผลถึงความรับผิดชอบของตัวแทนด้วย โดยตัวแทนจำต้องรับผิดแห่งการกระทำนั้น เพียงลำพังเด็ดขาดเช่นกัน ตัวการจึงไม่มีการรับผิดแห่งการนี้ ต่อมาได้มีหลักแนวคิดในการมอบอำนาจให้ตัวแทนดำเนินการแทนแบบไม่เด็ดขาด ซึ่งต้องพิจารณาเกี่ยวกับขอบอำนาจที่ตัวการได้มอบให้ด้วย กล่าวคือ หากตัวแทนได้ กระทำการใด ๆ ภายในขอบอำนาจอันมาจากคำสั่งของตัวการแล้วตัวการจำต้องรับผิดในผลแห่งการกระทำของตัวแทนนี้นั่นเอง ซึ่งครั้งในยุคสมัย Anglo Saxon สหราชอาณาจักร ก็ได้มีการนำเอาแนวคิดเกี่ยวกับเรื่องตัวแทนมาใช้ในสหราชอาณาจักร ทั้งในรูปแบบลักษณะที่เป็นสัญญาซื้อขาย แลกเปลี่ยน ให้ จำนอง จำนำ เป็นต้น[3] ในส่วนของหลักเรื่องนายหน้าของประเทศไทยแต่เดิมนั้น ยังไม่เคยรับเกี่ยวกับเรื่องสัญญาตัวแทน[4] ไม่ยอมรับหลักการที่จะให้มีการกระทำนิติกรรมใด ๆ แทนบุคคลอื่นได้ กล่าวคือ หากแม้มีการแต่งตั้งให้มีตัวแทนกระทำการก็ตามตัวแทนก็จำต้องรับผิดผูกพันในฐานะที่เป็นคู่สัญญาเองโดยตรง กฎหมายเดิมของไทยนั้นมีเพียงหลักตัวแทนเฉพาะเรื่อง แค่การพิจารณาคดีที่ยอมให้บุคคลหนึ่งว่าความแทนอีกบุคคลหนึ่งที่อยู่ภายใต้อำนาจของตนเท่านั้น กรณีเช่น การเป็นผู้แทนของผู้เยาว์หรือผู้ไร้ความสามารถตามกฎหมายจะมีความเกี่ยวพันในวิธีพิจารณาความ ต่อมาครั้งเมื่อได้มีการออกประกาศใช้ประมวลกฎหมายแพ่งและพาณิชย์จึงได้ปรากฏหลักกฎหมายอันเกี่ยวกับสัญญาขึ้นใหม่ โดยส่วนใหญ่มาจากหลักกฎหมายของสหราชอาณาจักรอันเนื่องมาจากความเป็นมาทางประวัติศาสตร์ที่สยามประเทศในขณะนั้นได้ทำการค้าขายกับสหราชอาณาจักร อีกทั้งบรรดานักกฎหมายขณะนั้นก็นิยมไปศึกษากฎหมายจากสหราชอาณาจักรเป็นส่วนมาก ซึ่งหลักสัญญาตัวแทนนี้ก็เป็นหลักกฎหมายใหม่ ในประมวลกฎหมายแพ่งและพาณิชย์ที่ได้ออกประกาศใช้ในครั้งนั้นด้วย เดิมในสมัยนั้น เรียกว่า สัญญาตัวแทน (agency) ซึ่งเป็นหลักกฎหมายที่มีความสำคัญยิ่งอันนำพาความเจริญมาสู่การค้าขายในสมัยใหม่ได้

ในทางปฏิบัติก่อนมีการประกาศใช้ บรรพ 3 แห่งประมวลกฎหมายแพ่งและพาณิชย์ เคยมีการนำหลักแนวคิดของสัญญาตัวแทน และสัญญาทรัสต์ (Trust) มาปรับใช้แก่การพิจารณาข้อเท็จจริงแห่งคดีโดยศาล

---

[2] วิจักขณ์ภัค เกศา, ‘กฎหมายนายหน้าอสังหาริมทรัพย์ในประเทศไทย: ศึกษาเปรียบเทียบกับกฎหมาย นายหน้าอสังหาริมทรัพย์ประเทศสิงคโปร์ และประเทศฟิลิปปินส์’ (สารนิพนธ์ นิติศาสตรมหาบัณฑิต สาขานิติศาสตร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช 2559) 39-40.

[3] มาโนช สุทธิวาทนฤพุฒิ, กฎหมายแพ่งและพาณิชย์ว่าด้วยตัวแทน นายหน้า (ศรีเมืองการ พิมพ์ 2538) 3. อ้างถึงใน จิตรทิวัส โคตรทัศน์, ‘มาตรการทางกฎหมายในการควบคุมการทำสัญญานายหน้าอสังหาริมทรัพย์’ (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยศรีปทุม 2564) 8-9.

[4] ร. แรงกาต์, ประวัติศาสตร์กฎหมายไทย เล่ม 2 (พิมพ์ครั้งที่ 1 ไทยวัฒนาพาณิชย์ 2526) 285-286.

ได้รับรองหลักการของการทำสัญญาตัวแทนไว้ คือ คำพิพากษาศาลฎีกาที่ 306/2465 “ตัวแทนกระทำการไม่สำเร็จโดยความผิดของตนเอง ต้องรับผิดชอบใช้ค่าเสียหายให้แก่ตัวแทนเท่าจำนวนตามที่ตัวแทนควรจะได้ ถ้าตัวแทนกระทำการสำเร็จตามสัญญา...” และต่อมาปรากฏเป็นบทบัญญัติแห่งกฎหมายที่มีความชัดเจนขึ้นเป็นกฎหมายลักษณะนายหน้าตามประมวลกฎหมายแพ่งและพาณิชย์ตลอดจนถึงปัจจุบัน

สำหรับประเทศไทยกฎหมายนายหน้าปรากฏอยู่ในประมวลกฎหมายแพ่งและพาณิชย์ บรรพ 3 ลักษณะนายหน้า ตั้งแต่ มาตรา 845 จนถึงมาตรา 849 เท่านั้น เมื่อพิจารณาจากบทบัญญัติดังกล่าวแล้ว มิได้มีการบัญญัติไว้โดยแจ้งชัดว่า นายหน้า หมายความว่าอะไร เพียงแต่กำหนดลักษณะกิจการที่บุคคลผู้เป็นนายหน้าจะต้องดำเนินการเท่านั้น ตามบทบัญญัติ มาตรา 845 วรรคแรก บัญญัติว่า “บุคคลผู้ใดตกลงจะให้ค่าบำเหน็จแก่นายหน้าเพื่อที่ชี้ช่องให้ได้เข้าทำสัญญาก็ดี จัดการให้ได้ทำสัญญากันก็ดี ท่านว่าบุคคลผู้นั้นจะต้องรับผิดใช้ค่าบำเหน็จก็ต่อเมื่อสัญญานั้นได้ทำกันสำเร็จเนื่องแต่ผลแห่งการที่นายหน้าได้ชี้ช่อง หรือจัดการนั้น ถ้าสัญญาที่ได้ทำกันไว้นั้น มีเงื่อนไขเป็นเงื่อนบังคับก่อนไซร้ ท่านว่าจะเรียกร้องบำเหน็จค่านายหน้ายังหาได้ไม่จนกว่า เงื่อนไขนั้นสำเร็จแล้ว...” และความหมายของ “นายหน้า” ที่ระบุไว้ในพจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ.2554 ได้ให้ความหมายของ “นายหน้า” มีอยู่ 2 ความหมาย[5] ซึ่งเป็นการกำหนดให้หมายความเป็นไปดังที่มาตรา 845 ได้กำหนดไว้ดังนี้

ความหมายที่หนึ่ง (กฎ) น. หมายถึง ชื่อสัญญาซึ่งบุคคลหนึ่งตกลงจะให้ค่าบำเหน็จ แก่อีกบุคคลหนึ่งเพื่อที่ชี้ช่องให้ได้เข้าทำสัญญาหรือจัดการให้ได้ทำสัญญากัน

ส่วนความหมายที่สอง น. หมายถึง บุคคลผู้ชี้ช่องหรือจัดการให้บุคคลสองฝ่ายได้เข้าทำสัญญากันโดยจะได้รับบำเหน็จเป็นการตอบแทน

ดังนั้น คุณสมบัติของบุคคลที่จะถือว่าเป็นนายหน้า จึงมีลักษณะเพียงเป็นบุคคลที่แสวงหาบำเหน็จด้วยการทำหน้าที่ เป็นสื่อชี้ช่องหรือชักพาให้ตัวการผู้ซึ่งว่าจ้างหรือติดต่อกับตนได้เข้าทำสัญญากับบุคคลภายนอก โดยที่นายหน้าไม่ได้ครอบครองทรัพย์และไม่ได้ลงชื่อในสัญญาแทนตัวการ แต่หากว่าได้ลงชื่อแทนด้วยก็ขึ้นชื่อว่าเป็นตัวแทนทำสัญญานั้น[6] และในระดับสากลนายหน้าถือว่า ผู้ที่เป็นนายหน้ามีลักษณะเป็นตัวแทนทางธุรกิจจำพวกหนึ่งที่มีความสำคัญ โดยลักษณะของการเข้าชี้ช่องนี้ หมายถึง การบอกให้ทราบ หรือแนะนำให้รู้หรือหาลู่ทางให้ได้ทำสัญญา ซึ่งอาจมีการบอกกล่าวต่อ ๆ กันไปหลายทอด และส่วนของการจัดให้ได้ทำสัญญา หมายถึง นายหน้าจะมีหน้าที่จัดแจงช่วยเหลือให้ทั้งสองฝ่ายได้ทำสัญญากัน นายหน้าอาจขับรถไปส่งช่วยต่อรองราคา และเตรียมสัญญา ตลอดจนการนัดคู่สัญญาไปดำเนินการจดทะเบียนซื้อขายกัน โดย

---

[5] สำนักงานราชบัณฑิตยสภา, ‘นายหน้า’ <https://dictionary.orst.go.th/> (2563, 1 กุมภาพันธ์).

[6] สถิต เล็งไธวง, *กฎหมายลักษณะตัวแทน และนายหน้า* (พิมพ์ครั้งที่4 ห้างหุ้นส่วนจำกัด พิมพ์อักษร 2550) 406-410.

เกี่ยวกับนายหน้าในต่างประเทศ เช่น กฎหมายฝรั่งเศสได้มีการใช้คำเรียกนายหน้าว่า “courtier” ซึ่งหมายถึงเป็นคนกลางที่มีอิสระ[7] (un intermédiaire indépendant) เป็นต้น

2.3 แนวคิด ทฤษฎี และหลักการพื้นฐานที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

แนวคิด ทฤษฎี และหลักการพื้นฐานที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลเป็นแนวคิด ทฤษฎี และหลักการพื้นฐานที่เกี่ยวข้องกับมนุษย์ทุกคนเป็นอย่างมาก เช่น ศักดิ์ศรีความเป็นมนุษย์ ซึ่งเป็นสิ่งที่มีคุณค่าติดตัวมนุษย์มาตั้งแต่เกิดและเป็นที่ยอมรับกันโดยทั่วไปว่าศักดิ์ศรีความเป็นมนุษย์นั้น ดำรงอยู่ในชีวิตของมนุษย์ทุกคนอย่างเท่าเทียมกัน ซึ่งไม่อาจพรากไปหรือไม่อาจถูกล่วงละเมิดได้ ด้วยเหตุนี้สิทธิเสรีภาพในร่างกาย และสิทธิในความเสมอภาคซึ่งนับเป็นรากฐานอันเป็นสาระสำคัญในความมีอยู่ของศักดิ์ศรีความเป็นมนุษย์[8] จึงได้รับความคุ้มครองดังที่ปรากฏในปฏิญญาสากลว่าด้วยสิทธิมนุษยชน มาตรา 6 และมาตรา 29[9] กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในประเทศต่าง ๆ ตลอดจนในข้อตกลงระหว่างประเทศ แม้ในรายละเอียดของบทบัญญัติกฎหมายจะมีความแตกต่างกัน เนื่องจากสภาพปัญหาและกระบวนการการคุ้มครองทางกฎหมายที่แตกต่างกันของแต่ละประเทศและเงื่อนไขที่แตกต่างกันในแต่ละภูมิภาค แต่ในท้ายที่สุดแล้วหลักการสำคัญก็เพื่อให้ความคุ้มครองความเป็นส่วนตัวของบุคคลในมิติของข้อมูลหรือการคุ้มครองข้อมูลส่วนบุคคลของพลเมือง ซึ่งอยู่บนพื้นฐานของหลักความยินยอม (Consent) เป็นสำคัญ[10] ในการที่เจ้าของข้อมูล

---

[7] François Collart Dutilleul et Phililppe Delebecque, Contracts civils et commerciaux, Dalloz: Collection Précis 2011. อ้างถึงใน นนทวัชร์นวตระกูลพิสุทธิ์, *กฎหมายเอกเทศสัญญาลักษณะตัวแทน – ลักษณะนายหน้า* (พิมพ์ครั้งที่ 4 โรงพิมพ์มหาวิทยาลัยธรรมศาสตร์ 2564) 198.

[8] บรรเจิด สิงคะเนติ, *หลักพื้นฐานเกี่ยวกับสิทธิเสรีภาพและศักดิ์ศรีความเป็นมนุษย์* (พิมพ์ครั้งที่ 3 วิญญูชน 2552) 88.

[9] Universal Declaration of Human Rights 1948

Article 1 Free and equal

All human beings are born free and equal and should be treated the same way.

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

Article 29 Duty to your community

You have duties toward the community within which your personality can fully develop. The law should guarantee human rights. It should allow everyone to respect others and to be respected....

(2) In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.”

[10] นคร เสรีรักษ์, ‘มาตรฐานสากลในการคุ้มครองข้อมูลส่วนบุคคล: ผลกระทบต่อประเทศไทย’ <https://www.fpps.or.th/news.php?detail=n1588215051.news.> สืบค้นเมื่อ 14 กรกฎาคม 2565.

ยินยอมให้ข้อมูลแก่เจ้าของธุรกิจ หรือบุคคลใดก็ตาม ถือว่าเจ้าข้อมูลยินดีและยินยอมที่จะให้เจ้าของธุรกิจหรือบุคคลใดก็ตามเก็บข้อมูลเหล่านั้นเป็นความลับ เจ้าของข้อมูลหรือบุคคลใดนั้น ย่อมต้องถือหลักสุจริตและไม่ก้าวล่วงในสิทธิความเป็นส่วนตัวของเจ้าของมูล โดยการไม่นำข้อมูลเหล่านั้น นำไปเปิดเผย หรือใช้ประโยชน์ในทางที่มิชอบ หรือเจ้าของข้อมูลมิได้ยินยอม

2.3.1 แนวคิด ทฤษฎี และหลักการพื้นฐานว่าด้วยหลักศักดิ์ศรีความเป็นมนุษย์

ตามพจนานุกรมฉบับราชบัณฑิตยสถานได้ให้ความหมายของคำว่า “ศักดิ์” ไว้ว่า อำนาจ ,ความสามารถ เช่น มีศักดิ์สูง ถือศักดิ์ เป็นต้น กำลัง, ฐานะ เช่น มีศักดิ์ และสิทธิแห่งปริญญานี้ทุกประการ เป็นต้น โดยมีคำว่า “ศักดิ์ศรี” เป็นคำลูก ซึ่งคำว่า “ศักดิ์ศรี” นั้น มีความหมายว่า เกียรติศักดิ์ เช่น ประพฤติตนไม่สมศักดิ์ศรี เป็นต้น

ศักดิ์ศรีความเป็นมนุษย์ (Human Dignity) หมายถึง คุณสมบัติ จิตใจ สิทธิเฉพาะตัวที่พึงสงวนของมนุษย์ทุกคน และรักษาไว้มิให้บุคคลอื่นมาล่วงละเมิดได้ การถูกละเมิดศักดิ์ศรีความเป็นมนุษย์จึงเป็นสิ่งที่ต้องได้รับความคุ้มครอง[11]

ความหมายของศักดิ์ศรีความเป็นมนุษย์ “ศักดิ์ศรี” ในความเข้าใจของศาสนาคริสต์ หมายถึงความเมตตาของพระเจ้า ซึ่งเกี่ยวกับข้อเท็จจริงในทางศาสนาคริสต์ว่า มนุษย์นั้นถูกสร้างขึ้นมาตามความประสงค์ของพระผู้เป็นเจ้า ดังนั้น ศักดิ์ศรีของมนุษย์มิอาจถูกทำลายหรือถูกพรากไปได้โดยการกระทำของบุคคลอื่น หากแต่ถูกทำลายได้โดยบาปของตนเอง ศักดิ์ศรีความเป็นมนุษย์ในศาสนาคริสต์จึงเป็นเรื่องระหว่างความสัมพันธ์ระหว่างมนุษย์กับพระผู้เป็นเจ้า[12] คำสอนว่ามนุษย์ทุกคนเสมอกันในสายตาของพระผู้เป็นเจ้า คำสอนในเรื่องศักดิ์ศรีหรือคุณค่าของความเป็นมนุษย์ ในความหมายที่มนุษย์คือสัตว์โลกที่พระผู้เป็นเจ้าสร้างขึ้นตามรูปแบบฉายาของพระองค์ (Image of God) มนุษย์จึงไม่อาจยอมให้อำนาจรัฐอยู่เหนือมนุษย์ชนิดที่ปราศจากเงื่อนไขโดยนัยดังกล่าวมนุษย์จึงมีศักดิ์ศรีอันศักดิ์สิทธิ์ที่ได้รับจากพระเจ้า ความเป็นมนุษย์จึงสูงส่ง มนุษย์เป็นศูนย์กลางของสรรพสิ่ง มนุษย์จึงไม่อาจปฏิบัติต่อมนุษย์เหมือนไม่ใช่มนุษย์หรือไม่มองมนุษย์ด้วยกันเหมือนสัตว์ ตรงกันข้ามมนุษย์จักต้องมีความเคารพต่อกันหรือรู้จักรับใช้กันและกัน[13] ในขณะที่ความหมายของคำว่า “ศักดิ์ศรีความเป็นมนุษย์” ในทางกฎหมายนั้น หมายความว่า มนุษย์ทุกคนเป็นมนุษย์โดยอำนาจแห่งจิตวิญญาณของเขาเอง ซึ่งทำให้เขาแตกต่างจากความเป็นอยู่ในสภาวะธรรมชาติที่ปราศจากความเป็นส่วนบุคคล และการทำให้บรรลุเป้าหมายภายในขอบเขตส่วนบุคคลนั้นย่อมขึ้นอยู่กับการตัดสินใจ ของบุคคลนั้นเองในอัน

---

[11] สุรชัย ศรีสารคาม, ‘บทความเกี่ยวกับหลักสิทธิมนุษยชน’ <https://www.constitutionalcourt.or.th/occ_web/ewt_dl_link.php?nid=1394>. สืบค้นเมื่อ 14 มกราคม 2566.

[12] บรรเจิด สิงคะเนติ (เชิงอรรถ 8)

[13] จรัล โฆษณานันท์, สิทธิมนุษยชนไร้พรมแดน : ปรัชญา กฎหมาย และความเป็นจริงทางสังคม (นิติธรรม 2545) 99.

ที่จะกำหนดตนเองและในการสร้างสภาพแวดล้อมของตนเอง[14] ลักษณะเฉพาะและเป็นคุณค่าที่มีความผูกพันอยู่กับความเป็นมนุษย์ซึ่งบุคคลในฐานะที่เป็นมนุษย์ทุกคนได้รับคุณค่าดังกล่าวโดยไม่จำเป็นต้องคำนึงถึงเพศ เชื้อชาติ ศาสนา วัย หรือคุณสมบัติอื่น ๆ ของบุคคล ในความหมายนี้ “ศักดิ์ศรี” จึงหมายถึงลักษณะบางประการที่สร้างออกมาเป็นคุณค่าเฉพาะตัวของมนุษย์ อันเป็นสารัตถะในการกำหนดความรับผิดชอบของตนเอง และเป็นสารัตถะที่มนุษย์แต่ละคนได้รับเพื่อความเป็นมนุษย์ของบุคคลนั้น[15] รวมทั้งศักดิ์ศรีวามเป็นมนุษย์นั้นเป็นการแสดงออกถึงการสร้างปริมณฑลของความเป็นอิสระของปัจเจกบุคคลให้กว้างที่สุดเท่าที่จะทำได้ และใช้ประโยชน์จากปริมณฑลดังกล่าวเพื่อการดำรงไว้ซึ่งชีวิต และเพื่อปรับปรุงชีวิตมนุษย์ให้ดีขึ้น โดยวิธีการพัฒนาขีดความสามารถของมนุษย์ไปสู่เป้าหมายที่กำหนดไว้[16] นอกจากนี้ยังหมายถึงความมีค่าของมนุษย์แต่ละคนทั้งในแง่ของความมีค่าในตัวของผู้นั้นเองและในสถานภาพของความเป็นมนุษย์ของแต่ละคนด้วย ศักดิ์ศรีความเป็นมนุษย์ย่อมเป็นส่วนหนึ่งที่เป็นสาระสำคัญของมนุษย์แต่ละคน อันไม่อาจจะพรากได้เสีย และการที่ศักดิ์ศรีความเป็นมนุษย์ได้กลายมาเป็นส่วนที่เป็นสาระสำคัญของมนุษย์แต่ละคนอันไม่อาจจะพรากเสียได้นี้ ทำให้ศักดิ์ศรีความเป็นมนุษย์ได้กลายมาเป็นความหมายจำเพาะและเป็นตัวกำหนดความหมายของความเป็นมนุษย์ไปโดยปริยาย ศักดิ์ศรีในตัวมนุษย์มีออยู่ในตัวของมนุษย์ทุกคน โดยไม่คำนึงถึงเพศ วัย สีผิว สัญชาติ หรือศาสนา นอกจากนี้แล้ว จะต้องไม่คำนึงถึงความสามารถทางสติปัญญาในการรับรู้สิ่งต่าง ๆ ของตัวผู้นั้นถึงเรียกได้ว่าเพียงความเป็นมนุษย์ที่มีอยู่ในตัวมนุษย์ทุกคนดังกล่าวนี้จึงถือได้ว่ากลายมาเป็นแก่นสาระสำคัญตามธรรมชาติของความเป็นมนุษย์ไปแล้วอย่างปฏิเสธไม่ได้ และเมื่อเป็นเช่นนี้ ศักดิ์ศรีความเป็นมนุษย์จึงเป็นสิ่งที่ไม่อาจถูกพรากหรือทำให้สูญเสียไปด้วยวิธีการใดๆได้[17]

คุณค่าของบุคคลอันมีลักษณะเฉพาะเนื่องจากผู้นั้นเป็นมนุษย์ คุณค่านี้ไม่ขึ้นอยู่กับเงื่อนไขใด ๆ ไม่ว่าเพศ เผ่าพันธุ์ เชื้อชาติ สีผิว ความเชื่อทางศาสนา สถานภาพทางสังคม ความมั่งคั่งของทรัพย์สิน และไม่ถูกจำกัด ด้วยวัย ความรู้ ความสามารถทางสติปัญญา หรือทางกาย ศักดิ์ศรีความเป็นมนุษย์เป็นสิทธิประการหนึ่งของบุคคล ทำให้บุคคลอื่นมีหน้าที่ต้องเคารพต่อเจ้าของสิทธิโดยการปฏิบัติให้สอดคล้องกับคุณค่ามนุษย์ในตัวบุคคล ในขณะเดียวกันองค์กรทางสังคมการเมืองมีหน้าที่ต้องเคารพคุณค่าของมนุษย์ เพราะองค์กรเหล่านั้นก่อตั้งขึ้นและดำรงอยู่ได้ เพื่อสนองประโยชน์ของมนุษย์ แนวคิดทางปรัชญาการเมืองเห็นว่าคุณค่าความเป็นมนุษย์เป็นสิ่งที่จะช่วยจรรโลงให้มนุษย์พัฒนาคุณค่าในตัวเองได้อย่างเต็มที่ตามความสามารถของแต่ละคน เงื่อนไขที่จะทำให้มนุษย์พัฒนาศักยภาพของตนเอง ได้อย่างเต็มที่ประกอบด้วยสิทธิทางด้านชีวิตและ

---

[14] Duering,Grundgedetz-Kommentar,Art.1,Abs.1,Rdnr.17,อ้างถึงใน บรรเจิด สิงคะเนติ (เชิงอรรถ 8) 87.

[15] Klaus Sten,Das Staatsrechtder Bunderepublik Deutschland,Band II/2 Allgemein Lehrender Grundrechte,S.113.

[16] Albert blackmann, StaatsrechDie Grundrechte, 4 Autl.,1997,s.543.

[17] บุญศรี มีวงศ์อุโฆษ, *กฎหมายรัฐธรรมนูญ*, (โครงการตำราและเอกสารประกอบการสอนคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ 2556) 520.

ร่างกาย อิสรภาพ และความเสมอภาค ศักดิ์ศรีความเป็นมนุษย์เป็นปรัชญาทางมโนธรรมที่เป็นพื้นฐาน ในการจัดทำปฏิญญาสากลว่าด้วยสิทธิมนุษยชน โดยการให้คุณค่ากับมนุษย์ ในฐานะที่เป็นมนุษย์ที่ไม่ได้อิงอยู่กับแนวคิดเรื่องคุณค่าทางศาสนาใดศาสนาหนึ่ง โดยเฉพาะดังปรากฏในอารัมภบทของปฏิญญาว่า “ด้วยเหตุที่การยอมรับศักดิ์ศรีแต่กำเนิดและสิทธิที่เท่าเทียมกัน และไม่อาจเพิกถอนได้ของสมาชิกทั้งปวงแห่งครอบครัวมนุษยชาติ เป็นพื้นฐานแห่งอิสรภาพความยุติธรรมและสันติภาพในพิภพ โดยที่ประชาชนแห่งสหประชาชาติได้ยืนยันอีกครั้งไว้ในกฎบัตรถึงศรัทธาในสิทธิมนุษยชนขั้นพื้นฐานในศักดิ์ศรีและคุณค่าของมนุษย์ และในความเท่าเทียมกันของบรรดาชายและหญิง และได้มุ่งมั่นที่จะส่งเสริมความก้าวหน้าทางสังคมและมาตรฐานแห่งชีวิตที่ดีขึ้นในอิสรภาพให้กว้างขวางยิ่งขึ้น ฉะนั้น บัดนี้ สมัชชาสหประชาชาติ จึงประกาศปฏิญญาสากลว่าด้วยสิทธิมนุษยชนขึ้น” และศักดิ์ศรีความเป็นมนุษย์ได้รับรองในกฎหมายไทยครั้งแรกโดย รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540 (ค.ศ. 1997) มาตรา 4 ซึ่งบัญญัติว่า “ศักดิ์ศรีความเป็นมนุษย์ สิทธิ และเสรีภาพ ของบุคคลย่อมได้รับความคุ้มครอง” ต่อมาได้รับรองในรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550 (ค.ศ. 2007) รับรองไว้อย่างเดียวกันในมาตรา 4 เช่นกัน[18]

2.3.2 แนวคิด ทฤษฎี และหลักการพื้นฐานว่าด้วยหลักความยินยอม

หลักความยินยอม (Volenti non fit injuria) หมายความว่า เมื่อให้ความยินยอมแล้วย่อมไม่ถือว่ามีความเสียหาย หรือความยินยอมของผู้เสียหายทำให้ไม่เป็นละเมิด เนื่องจากการละเมิดเป็นการกระทำที่ผิดกฎหมายและเกิดความเสียหายแก่บุคคลอื่น เมื่อถือว่าไม่มีความเสียหายการกระทำนั้นจึงไม่เป็นละเมิด ผู้เสียหายจึงไม่มีสิทธิเรียกค่าเสียหายอันเกิดจากการกระทำที่ตนให้ความยินยอม อย่างไรก็ตาม การจะนำหลักดังกล่าวมาใช้ยกเว้นให้การกระทำที่ผิดกฎหมายเป็นการกระทำที่ชอบด้วยกฎหมายนั้น จะต้องพิจารณาด้วยว่าจะนำมาใช้ยกเว้นกฎหมายที่มีวัตถุประสงค์เพื่อคุ้มครองสิ่งใด หากกฎหมายมีวัตถุประสงค์เพื่อคุ้มครองเฉพาะตัวผู้เสียหายแล้ว ผู้เสียหายย่อมให้ความยินยอมต่อการกระทำนั้นได้ แต่ถ้าวัตถุประสงค์ที่กฎหมายมุ่งคุ้มครองคือสังคมหรือประชาชนด้วยแล้ว ย่อมไม่สามารถนำความยินยอมของผู้เสียหายเพียงคนเดียวมาทำให้การกระทำที่ไม่ชอบด้วยกฎหมายนั้นชอบด้วยกฎหมายขึ้นมาได้จึงไม่อาจใช้หลักความยินยอมกับการกระทำที่ขัดต่อความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน[19] กล่าวคือ หลักความยินยอม คือ การแสดงเจตนาของผู้เสียหายหรือผู้มีอำนาจกระทำการแทน ผู้เสียหายที่จะยินยอมให้ผู้อื่นมาก่อให้เกิดความเสียหาย โดยการจงใจปล่อยให้เหตุการณ์อย่างใดอย่างหนึ่งเกิดขึ้น โดยไม่ขัดขวางทั้งที่สามารถขัดขวางได้เป็นการแสดงความประสงค์ที่จะให้เกิดเหตุการณ์เช่นนั้นขึ้นลักษณะทางกฎหมายของหลักความยินยอม เช่น ผู้ให้ความยินยอมต้องเป็นผู้มีความสามารถในการให้ความยินยอมวิธีการให้ความยินยอมอาจแสดงออกด้วยการกระทำอย่างหนึ่ง

---

[18] คณะกรรมการสิทธิมนุษยชนแห่งชาติ, *ประมวลศัพท์และความรู้สิทธิมนุษยชน เล่ม 2 คณะกรรมการสิทธิมนุษยชนแห่งชาติ ศัพท์สิทธิมนุษยชน ในกระบวนการยุติธรรม และสิทธิมนุษยชนศึกษา* (พิมพ์ครั้งที่ 1 2556) 112-113.

[19] พิชัยศักดิ์ หรยางกูร, นริศรา แดงไผ่, ‘หน่วยที่ 3 หลักความยินยอม’ <https://www.stou.ac.th/Schools/Slw/upload/Ex%2040701-3.pdf.> สืบค้นเมื่อ 6 สิงหาคม 2565. 3-3.

โดยตนเองหรือให้ผู้อื่นกระทำแทนตน ซึ่งทำให้เข้าใจว่าตนอนุญาตให้ทำยกเว้นแต่ในกรณีพิเศษอย่างยิ่งเท่านั้นที่การนิ่งไม่ขัดขวางอาจถือได้ว่าเป็นความยินยอม เพราะเป็นที่เข้าใจกันโดยปกติทั่วไปว่าการนิ่งเช่นนั้นเป็นการยินยอม และการแสดงออกซึ่งความประสงค์อันถือได้ว่าเป็นความยินยอมอาจแสดงออกโดยชัดแจ้งหรือโดยปริยายก็ได้ และผลของความยินยอมคือถ้ามีความเสียหายใด ๆ เกิดขึ้นจากการกระทำผู้กระทำไม่ต้องรับผิดในความเสียหายที่เกิดขึ้นนั้น อย่างไรก็ตาม ถ้าเป็นความตกลงหรือความยินยอมของผู้เสียหายสำหรับการกระทำที่ต้องห้ามชัดแจ้งโดยกฎหมายหรือขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชนจะนำมาอ้างเป็นเหตุยกเว้นหรือจำกัดความรับผิดเพื่อละเมิดมิได้[20]

ความยินยอมไม่ก่อให้เกิดละเมิด หรือ Volenti non fit injuria (หรือ injuria) มีความหมายว่า to a willing person, injury is not done คือ บุคคลที่สมัครใจ เต็มใจ ให้กระทำการละเมิดหรือการผิดกฎหมายก็จะไม่เกิดขึ้น หลักเกณฑ์ดังกล่าวเป็นหลักกฎหมายในระบบ Common Law ซึ่งมีสาระอยู่ที่ว่าหากใครบางคนเต็มใจที่จะให้เองตกอยู่ในภาวะที่อาจเกิดอันตราย ทราบระดับความรุนแรงของอันตรายและผลที่จะเกิดขึ้น บุคคลนั้นไม่อาจจะฟ้องร้อง เรียกร้อง บุคคลที่มาทำให้เกิดอันตรายในฐานละเมิด หรือการกระทำที่ก่อให้เกิดความรับผิดทางแพ่ง (delict)[21]

อย่างไรก็ตาม การอ้างเรื่องความยินยอมหรือความสมัครใจนี้ ต้องเป็นกรณีที่วิญญูชนสามารถตัดสินใจเกี่ยวกับการกระทำของตนเองได้โดยสมัครใจ เช่น ความยินยอมในการเล่นกีฬา ความยินยอมที่ไม่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน ความยินยอมตามจารีตประเพณีที่ยอมรับกัน ความยินยอมในการรับการรักษาทางการแพทย์ เป็นต้น[22] สำหรับที่มาของหลักนี้มาจากกฎเกณฑ์ทางกฎหมาย (legal maxim) คำว่า Nulla injuria est,quoe in volentem fiat ซึ่งกำหนดขึ้นโดย Ulpian นักกฎหมายโรมัน

ในกรณีของประเทศอังกฤษ กฎหมายในเรื่องละเมิดมีการยกเรื่องของความยินยอมขึ้นต่อสู้ให้พ้นความรับผิดโดยจำเลยต้องพิสูจน์ให้เห็นถึงสาระสำคัญ 2 ประการ กล่าวคือ

1. ผู้เสียหายได้ทราบอย่างชัดเจนเกี่ยวกับความเสี่ยงภัยที่อาจจะเกิดขึ้น ทั้งในแง่ของสภาพแห่งภัยและรายละเอียดของภัยนั้น

2. ผู้เสียหายได้มีการให้ความยินยอมโดยชัดแจ้ง โดยอาจเป็นด้วยวาจาหรือการกระทำว่าจะไม่เรียกร้องค่าเสียหาย โดยความยินยอมนั้นต้องเป็นไปโดยอิสระและด้วยความสมัครใจไม่ใช่ถูกบังคับ ข่มขู่ ชักจูง หลอกลวง ต้องเป็นความยินยอมที่บริสุทธิ์[23]

---

[20] เพิ่งอ้าง. 3-7.

[21] สุพิศ ประณีตพลกรัง, *หลักและทฤษฎีกฎหมายแพ่ง* (พิมพ์ครั้งที่ 4 นิติธรรม 2565) 27.

[22] เพิ่งอ้าง. 28.

[23] บุญศรี มีวงศ์อุโฆษ (เชิงอรรถ17).

ความหมายของหลักความยินยอม[24]

นักวิชาการหลายท่านได้ให้ความหมาย “ความยินยอม” (volenti non fit injuria) ไว้ดังนี้

ศาสตราจารย์จิตติ ติงศภัทิย์ ให้หมายความว่า การจงใจปล่อยให้เหตุการณ์อย่างใดอย่างหนึ่งเกิดขึ้นโดยไม่ขัดขวางทั้งที่สามารถขัดขวางได้ซึ่งจะต้องเป็นการแสดงความประสงค์ที่จะให้เกิดเหตุการณ์เช่นนั้นขึ้น โดยแสดงออกด้วยการกระทำอย่างหนึ่งโดยตนเองหรือโดยให้ผู้อื่นกระทำแทนตน อันเป็นการแสดงความประสงค์ต่อผู้กระทำเหตุการณ์นั้นให้เข้าใจว่าตนอนุญาตให้ทำ ยกเว้นแต่ในกรณีพิเศษอย่างยิ่งเท่านั้นที่การนิ่งไม่ขัดขวางอาจถือได้ว่าเป็นความยินยอม เพราะเป็นที่เข้าใจกันโดยปกติทั่วไปว่าการนิ่งเช่นนั้นเป็นการยินยอม และการแสดงออกซึ่งความประสงค์อันถือได้ว่าเป็นความยินยอมนั้นอาจแสดงออกโดยชัดแจ้งหรือโดยปริยายก็ได้

อาจารย์พจน์ ปุษปาคม ให้หมายความว่า เป็นความยินยอมที่เกิดจากฝ่ายผู้เสียหายยอมให้กระทำไม่ว่าต่อเนื้อตัว ร่างกายทรัพย์สินหรือสิทธิของตนความยินยอมโดยแท้จริงแล้วเป็นข้อแก้ตัวของผู้กระทำไม่ใช่สิทธิของผู้กระทำ

อาจารย์เพ็ง เพ็งนิติ ให้หมายความว่า เป็นเรื่องที่ผู้เสียหายยินยอมให้กระทำการประทุษร้ายโดยสมัครใจหรือยอมเข้าสู่อันตรายไม่ว่าจะเป็นการทำอันตรายต่อร่างกายทรัพย์สินหรือสิทธิอื่นใดการนิ่งเฉยไม่ขัดขืนหรือไม่ขัดขวางคัดค้านต่อการกระทำที่เป็นการประทุษร้ายหรือพฤติการณ์นั้นควรจะขัดขวางห้ามปรามหรือคัดค้าน แต่ไม่ขัดขวาง ไม่ห้ามปรามหรือไม่คัดค้าน ถือเป็นความยินยอมโดยปริยาย

ศาสตราจารย์ศักดิ์ สนองชาติ ให้หมายความว่า เป็นเรื่องที่ผู้เสียหายยอมให้กระทำหรือยอมต่อการกระทำหรือเข้าเสี่ยงรับความเสียหาย ซึ่งถือได้ว่าเป็นการให้ความยินยอมย่อมทำให้การกระทำนั้นไม่เป็นละเมิดตามมาตรา 420 ไม่ว่าผู้เสียหายจะได้รับความเสียหายจากการกระทำอย่างใด และได้รับความเสียหายแก่ชีวิต ร่างกาย อนามัย เสรีภาพ ทรัพย์สิน หรือสิทธิอย่างอื่นอย่างใดมากน้อยเพียงใดก็ตาม

อาจารย์ประจักษ์ พุทธิสมบัติ ให้หมายความว่า การที่ผู้เสียหายยินยอมโดยสมัครใจต่อการกระทำ ประทุษร้าย หรือผู้เสียหายสมัครใจเข้าสู่อันตรายเอง ไม่ว่าจะยินยอมให้กระทำต่อร่างกายทรัพย์สินหรือ สิทธิของตน และเป็นการยินยอมของผู้สามารถให้ความยินยอม ทำให้การกระทำไม่เป็นละเมิด อันที่จริงความยินยอมของผู้เสียหายมิใช่เป็นสิทธิของผู้กระทำ แต่เป็นข้อแก้ตัวของผู้กระทำ ทำให้ผู้กระทำไม่ต้องรับผิดเพื่อละเมิด

เมื่อพิเคราะห์ความเห็นของนักวิชาการหลายท่านที่กล่าวในตอนต้นพอสรุปได้ว่าความยินยอม คือ การแสดงเจตนาของผู้เสียหายหรือผู้มีอำนาจกระทำการแทนผู้เสียหายที่จะเป็นการยินยอมให้ผู้อื่นมาก่อให้เกิดความเสียหายแก่ชีวิต ร่างกาย อนามัย เสรีภาพ ทรัพย์สินหรือสิทธิอื่นใดของผู้เสียหาย

2.3.3 แนวคิด ทฤษฎี และหลักการพื้นฐานว่าด้วยหลักสุจริต

---

[24] เพิ่งอ้าง. 3-8.

หลักสุจริต (Good Faith) เป็นหลักกฎหมายทั่วไปและได้รับการยอมรับว่าเป็นพื้นฐานของกฎหมายแพ่งทั้งระบบจึงเป็นเครื่องมือทางกฎหมายที่สำคัญที่นักกฎหมายโรมันพัฒนาขึ้น โดยมีจุดมุ่งหมายเพื่อให้กฎเกณฑ์ที่มีความตายตัวยืดหยุ่นในการปรับใช้แก่ข้อเท็จจริงในสถานการณ์ทั้งในทางเศรษฐกิจและสังคมที่เปลี่ยนแปลงไป ซึ่งในระบบกฎหมายแพ่งและพาณิชย์ของไทยบัญญัติรับรองเกี่ยวกับการใช้สิทธิโดยสุจริตไว้ตามมาตรา 5 แห่งประมวลกฎหมายแพ่งและพาณิชย์อันเป็นหลักกฎหมายทั่วไปที่กำหนดเกี่ยวกับการใช้สิทธิแห่งตนก็ดีการชำระหนี้ก็ดีบุคคลทุกคนต้องกระทำโดยสุจริตซึ่งกำหนดไว้อย่างกว้าง ๆ ในลักษณะเดียวกับบทกฎหมายยุติธรรม (jus aequum) และเป็นหลักกฎหมายทั่วไป (General Principle) ที่มีฐานะสูงกว่าบทกฎหมายอื่น หรือมาตรา 368 แห่งประมวลกฎหมายแพ่งและพาณิชย์ กำหนดว่า สัญญานั้นท่านให้ตีความไปตามความประสงค์ในทางสุจริต โดยพิเคราะห์ถึงปกติประเพณีด้วย ดังนั้น สิทธิและหน้าที่ของคู่สัญญาจึงต้องตีความตามเจตจำนงของคู่สัญญาเป็นหลักโดยไม่พิจารณาเฉพาะข้อความที่ปรากฏเป็นลายลักษณ์อักษรเท่านั้น และต้องพิจารณาตามหลักความเป็นธรรมที่สังคมยอมรับและการปฏิบัติของกลุ่มอาชีพเดียวกันอันเป็นปกติประเพณีนั่นเอง[25]

คำว่า “สุจริต” เป็นคำที่มีความหมายกว้างและมีลักษณะเป็นนามธรรมจึงเป็นการยากที่จะกำหนดความหมายหรือหลักเกณฑ์เกี่ยวกับความสุจริตที่แน่นอนลงไปให้ชัดเจน อย่างไรก็ตาม เมื่อพิจารณาจากบทบัญญัติของประมวลกฎหมายแพ่งและพาณิชย์แล้ว อาจแบ่งหลักสุจริตออกเป็น 2 กรณีได้แก่ หลักสุจริตเฉพาะเรื่องและหลักสุจริตทั่วไปประกอบกับการพิจารณาลักษณะทางกฎหมายของหลักสุจริตอาจทำให้เข้าใจความหมาย และองค์ประกอบของหลักสุจริตได้ชัดเจนยิ่งขึ้น[26]

หลักสุจริตพัฒนามาจากระบบการควบคุมสังคมโดยการนำหลักศาสนา ความเชื่อ และความศรัทธามาเกี่ยวข้อง เนื่องจากมนุษย์เริ่มเปลี่ยนแปลงมุมมองจากการต้องปฏิบัติหน้าที่ของตน เพื่อความอยู่รอดเป็นการฝ่าฝืนความไว้วางใจกันทำให้ต้องนำหลักศาสนา ความเชื่อ และความศรัทธามาใช้ เพื่อปรามพฤติกรรมเช่นว่านี้ ซึ่งเมื่อมนุษย์ได้อ้อนวอนหรือสาบานต่อสิ่งที่ตนเชื่อถือ ศรัทธาก็ไม่กล้าที่จะผิดคำพูด เพราะกลัวการถูกลงโทษ ต่อมาแนวคิดเกี่ยวกับหลักสุจริตมีบทบาทและพัฒนาขึ้นในระบบกฎหมายโรมันเกี่ยวกับการรักษาคำพูดเมื่อบุคคลใดไม่ปฏิบัติตามคำสัตย์ที่ให้ไว้ย่อมถือว่าทำผิดหลักปฏิบัติต่อกันแม้จะมิได้ถือเป็นกฎหมาย แต่การไม่รักษาคำสัตย์ในสมัยนั้นถือว่าเป็นมลทินในสังคม ดังนั้น ความหมายและขอบเขตของหลักสุจริต จึงเป็นเรื่องของความรู้สึกผิดชอบชั่วดีของคนในสังคมมากกว่าที่จะเป็นผลโดยกฎหมายโดยแท้ต่อมา จึงมีการพัฒนาหลักสุจริตเป็นส่วนหนึ่งของกฎหมายสัญญาโรมันและระบบกฎหมายโรมันนี้เองเป็นต้นแบบของระบบกฎหมายแบบ Civil Law อันเป็นหลักการพื้นฐานของกฎหมายแพ่งทั้งระบบ[27] คำว่า “สุจริต” เป็นคำที่มาตั้งแต่

---

[25] วรนารี สิงโต, ‘หน่วยที่ 1 หลักสุจริต’ <https://www.stou. ac.th/schools /slw/ upload/ex40701-1.pdf.> สืบค้นเมื่อ 1 สิงหาคม 2565. 1-13.

[26] เพิ่งอ้าง. 1-3.

[27] วรนารี สิงโต (เชิงอรรถ 25). 1-7.

กฎหมายโรมัน ในภาษาละตินเรียกว่า bona fides แปลว่า ความซื่อสัตย์หรือสัจจะที่ดีอย่างไรก็ตาม คำว่า “สุจริต” นั้น เป็นคำที่มีความหมายกว้างและยากที่จะกำหนดหลักเกณฑ์ที่แน่นอนลงไปให้ชัดเจน[28] และเมื่อพิจารณาตาม Black’s law Dictionary พบว่ามีการอธิบายคำว่า “สุจริต” (Good Faith) ว่าหมายถึง สภาวะทางจิตใจอันประกอบด้วย

(1) ความซื่อสัตย์ในความเชื่อถือหรือวัตถุประสงค์

(2) ความซื่อตรงต่อหน้าที่หรือหนี้ของตน

(3) ความสอดคล้องกับมาตรฐานทางการค้าหรือธุรกิจใดๆ อันชอบด้วยเหตุผลในการต่อรองกันอย่างเป็นธรรม และ

(4) การไร้ซึ่งเจตนาหลอกลวงหรือแสวงหาผลประโยชน์โดยมิชอบ[29]

หลักสุจริตได้รับการรับรองเป็นลายลักษณ์อักษรครั้งแรกในประมวลกฎหมายแพ่งเยอรมัน ค.ศ.1900 ในมาตรา 157 และมาตรา 242 คำว่า “สุจริต” ในภาษาเยอรมันตรงกับคำว่า Treu und Glauben คำว่า Treu แปลว่า ความซื่อสัตย์ความไว้วางใจ ความน่าเชื่อถือ ส่วนคำว่า Glauben แปลว่า เชื่อในความไว้วางใจ หรือที่ ศ.ดร. ปรีดี เกษมทรัพย์ ได้อธิบายไว้ว่า “หลักสุจริตก็คือหลักความซื่อสัตย์และความไว้วางใจ แต่การที่จะบอกว่าความซื่อสัตย์และความไว้วางใจประกอบด้วยอะไรบ้างนั้นกล่าวได้ว่าทำได้ยากยิ่ง และยอมรับกันว่าหลักสุจริตนั้นเป็นเรื่องของแนวคิด แม้จะมีผู้พยายามอธิบายหลักสุจริตจากหลักย่อย ๆ ที่มาจากหลักสุจริต เช่น หลักการใช้สิทธิโดยไม่สุจริต หลักกฎหมายปิดปาก หรือหลักความรับผิดก่อนสัญญาแต่ก็ยังไม่อาจกล่าวได้ว่าเป็นการอธิบายความหมายของหลักสุจริต” เมื่อพิเคราะห์บทบัญญัติตามประมวลกฎหมายแพ่งและพาณิชย์แล้วจะพบว่าคำว่า “สุจริต” ใช้ในความหมายที่แตกต่างกัน 2 ประการ ได้แก่

1. หลักสุจริตทั่วไป ในภาษาละตินเรียกว่า bona fides แปลว่าความซื่อสัตย์หรือสัจจะที่ดี ปรากฏตามมาตรา 5 และมาตรา 368 แห่งประมวลกฎหมายแพ่งและพาณิชย์ซึ่งคำว่า “สุจริต” ในบทบัญญัติเหล่านี้มีความหมายโดยทั่วไปกว้างๆ โดยไม่หมายเฉพาะเจาะจงถึงความรู้เท่าไม่ถึงการณ์ของคู่กรณีแต่เป็นมาตรฐานทั่วไปที่กฎหมายได้บัญญัติไว้ให้ใช้เป็นเครื่องวัดความประพฤติของมนุษย์ในกรณีต่างๆ ว่า การกระทำเหล่านั้นอยู่ในกรอบที่กฎหมายจะสนับสนุนหรือประณามหรือไม่

2. หลักสุจริตเฉพาะเรื่อง หมายถึง ความรู้หรือไม่รู้ข้อเท็จจริงของคู่กรณีที่เกี่ยวข้อง เช่น มาตรา 412 มาตรา 413 มาตรา 1299 มาตรา 1300 มาตรา 1303 มาตรา 1310 มาตรา 1311 มาตรา 1312 มาตรา 1329 มาตรา 1330 มาตรา 1331 และ มาตรา 1332 แห่งประมวลกฎหมายแพ่งและพาณิชย์ ซึ่งคำว่า “สุจริต”ในที่นี้ใช้ในความหมายที่ว่าคู่กรณีที่เกี่ยวข้องรู้หรือไม่รู้ข้อเท็จจริงอันเป็นองค์ประกอบของกฎหมายหรือไม่ ดังนั้นคำว่า “สุจริต” จึงมีความหมายอย่างแคบซึ่งตามแนวคำพิพากษาศาลฎีกาอธิบายเกี่ยวกับความสุจริตว่าหมายถึงการกระทำโดยไม่รู้หรือไม่ควรรู้ถึงความบกพร่องแห่งสิทธิที่มีมาแต่อดีต (คำพิพากษาศาลฎีกา

---

[28] วรนารี สิงโต (เชิงอรรถ 25). 1-8.

[29] เพิ่งอ้าง. 1-8.

ที่ 550/2490) แต่ถ้าการกระทำโดยรู้ถึงความบกพร่องแห่งสิทธิของตนจะถือว่าสุจริตไม่ได้ (คำพิพากษาศาลฎีกาที่ 1012/2504) และยังได้ให้ความหมายเลยไปถึงว่าถ้าความไม่รู้นั้นเกิดจากความประมาทเลินเล่ออย่างร้ายแรงของผู้กระทำก็ถือว่าไม่สุจริตเช่นเดียวกัน[30]

ลักษณะทางกฎหมายของหลักสุจริต[31]

หลักสุจริตมีลักษณะสำคัญ 5 ประการ คือ

1. เป็นบทกฎหมายยุติธรรม (jus aequum) ซึ่งมิได้กำหนดข้อเท็จจริงอันเป็นองค์ประกอบหรือผลทางกฎหมายไว้อย่างแน่ชัดในการใช้และตีความกฎหมายเหล่านี้จำต้องใช้ดุลพินิจประกอบเพื่อเสริมเนื้อความให้กฎหมายสมบูรณ์ยิ่งขึ้น เพื่อให้เป็นธรรมและเหมาะสมกับพฤติการณ์แห่งคดีและตามกาลสมัยซึ่งตรงข้ามกับบทกฎหมายเคร่งครัด (jus strictum) ที่กำหนดข้อเท็จจริงอันเป็นองค์ประกอบและผลทางกฎหมายเอาไว้ชัดเจนแน่นอนผู้ใช้ หรือตีความกฎหมายไม่สามารถใช้ดุลพินิจเสริมแต่งเนื้อหาของบทบัญญัติเพียงแต่จะต้องตีความหรือใช้กฎหมายตามที่ได้บัญญัติไว้ชัดแจ้งอยู่แล้วซึ่งจะเป็นกรณีที่กฎหมายต้องการความชัดเจน แน่นอนเพื่อความสะดวกในกิจการบางอย่าง

2. เป็นบทกฎหมายที่เป็นบทบังคับ (jus cogens) กล่าวคือ เป็นกฎหมายที่คู่กรณีไม่สามารถตกลงแก้ไขเปลี่ยนแปลงได้ซึ่งตรงกันข้ามกับบทกฎหมายที่ไม่เป็นบทบังคับ (jus dispositivum) โดยกฎหมายที่บัญญัติขึ้นเพื่อป้องกันมิให้บุคคลทำการทุจริตเป็นกฎหมายเอกชนเรื่องหนึ่งที่เกี่ยวกับความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน เช่น กรณีจงใจก่อให้เกิดความเสียหายคู่กรณีไม่สามารถจะตกลงกันไม่เรียกค่าเสียหายได้

3. เป็นกฎหมายที่มีเนื้อความไม่ชัดแจ้ง โดยกฎหมายจะใช้ถ้อยคำอย่างกว้าง ๆ ไม่สามารถให้ความหมายที่แน่ชัดไว้ล่วงหน้าได้ต้องรอให้เกิดข้อพิพาทขึ้นจึงจะสามารถนำไปวินิจฉัยขอบเขตของหลักสุจริตเพื่อเป็นแนวทางให้กฎหมายควบคุมการแสดงเจตนาทำนิติกรรมของเอกชนไม่ให้ขัดกับผลประโยชน์ส่วนรวมและความรู้สึกผิดชอบชั่วดีของสังคมอย่างรุนแรง

4. เป็นหลักกฎหมายทั่วไป (General Principle) หรือเป็นบทที่เป็นหลักการของความประพฤติของมนุษย์ในสังคม แต่มิใช่เป็นกฎหมายทั่วไป (jus generale) ที่จะถูกตัดโดยกฎหมายพิเศษ (jus speciale) โดยในกรณีที่มีกฎหมายพิเศษ (jus speciale) ที่ต้องด้วยกรณีนั้น ๆ เป็นการเฉพาะแล้วย่อมต้องปรับด้วยกฎหมายพิเศษ (jus speciale) นั้นและจะนำกฎหมายทั่วไป (jusgenerale) มาปรับใช้ก็ต่อเมื่อไม่มีกฎหมายพิเศษ (jus speciale) จะปรับใช้แล้วเท่านั้นดังนั้นสุภาษิตกฎหมายที่ว่ากฎหมายพิเศษยกเว้นกฎหมายทั่วไป (Specialia generalibus derogant) จึงไม่อาจนำมาใช้กับหลักสุจริตได้อนึ่งดร.กิตติศักดิ์ปรกติมีความเห็นว่า “หลักสุจริตเป็นหลักกฎหมายทั่วไป (jus generale) ในกรณีที่มีบทกฎหมายพิเศษ (jus speciale) ย่อมมาก่อนกฎหมายทั่วไป ต่อเมื่อไม่มีบทเฉพาะหรือบทพิเศษจะปรับใช้ให้ต้องด้วยกรณีแล้วจึงจะหันมาปรับใช้ หลัก

---

[30] วรนารี สิงโต (เชิงอรรถ 25). 1-8.

[31] วรนารี สิงโต (เชิงอรรถ 25). 1-10.

สุจริต อาจกล่าวได้ว่าหลักสุจริตในมาตรา 5 แห่งประมวลกฎหมายแพ่งและพาณิชย์จะนำมาปรับใช้ได้ในฐานะเป็นที่พึ่งสุดท้าย”

ความเห็นเกี่ยวกับความหมายของหลักกฎหมายทั่วไป (General Principle) อาจแบ่งออกเป็น 2 แนวทาง ได้แก่ ความเห็นที่หนึ่ง ถือว่าสุภาษิตกฎหมายที่เขียนเป็นภาษาละตินเป็นหลักกฎหมายทั่วไป และความเห็นที่สอง ถือว่าหลักกฎหมายที่ผู้ร่างประมวลกฎหมายแพ่งและพาณิชย์นำมาใช้ในการร่างประมวลกฎหมายฉบับนั้นเป็นหลักกฎหมายทั่วไปซึ่งจะทราบได้จากการนำบทบัญญัติหลาย ๆ มาตราที่บัญญัติสำหรับข้อเท็จจริงที่คล้ายคลึงกันมาพิจารณา และเมื่อพิจารณาบทบัญญัติหลายมาตราดังกล่าวแล้วก็จะพบหลักกฎหมายทั่วไปที่ผู้ร่างประมวลกฎหมายนำมาใช้ซึ่งเป็นวิธีพิจารณาค้นคว้าจากเรื่องเฉพาะหลาย ๆ เรื่องมาสู่หลักเกณฑ์ทั่วไป (Induction) ซึ่ง ศ.ดร.หยุด แสงอุทัย เห็นด้วยกับความเห็นที่สองนี้[32]

5. เป็นบทครอบจักรวาล (Generalklausel) คือ แม้จะมีบทบัญญัติเกี่ยวกับเรื่องนั้นไว้อยู่แล้ว หลักสุจริตก็ยังใช้เป็นฐาน โดยเป็นบทที่ทำหน้าที่เป็นมาตรฐานควบคุมความประพฤติของบุคคลในทุกเรื่องจึงได้รับการยกย่องว่าเป็นรากฐานของกฎหมายทั้งระบบนับเป็นการประกาศอุดมคติแห่งความสัมพันธ์ของมนุษย์ในสังคมว่าจะต้องปฏิบัติต่อกันโดยสุจริต[33]

2.3.4 แนวคิด ทฤษฎี และหลักการพื้นฐานว่าด้วยสิทธิความอยู่เป็นส่วนตัว (Right of Privacy)

สิทธิความเป็นอยู่ส่วนตัวเป็นแนวคิดพื้นฐานที่รองรับการคุ้มครองข้อมูลส่วนบุคคลในแต่ละลักษณะซึ่งสัมพันธ์เชื่อมโยงกันจากแก่นความคิดหลักในเรื่องสิทธิความเป็นอยู่ส่วนตัว [34] ซึ่งเป็นหนึ่งในสิทธิเสรีภาพ และเป็นสิทธิขั้นพื้นฐานของมนุษย์ที่ได้รับการรับรองและคุ้มครอง ในสังคมยุคใหม่เกือบทุกประเทศให้ความสำคัญอย่างมาก และได้รับการรับรองคุ้มครองไว้ในปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ. 1948 (Universal Declaration of Human Right 1948) ซึ่งได้บัญญัติไว้ในข้อ 12 ดังนี้[35]

“บุคคลย่อมไม่ถูกแทรกแซงโดยพลการในความเป็นอยู่ส่วนตัว ในครอบครัวเคหสถานหรือในการสื่อสาร หรือไม่อาจถูกลบหลู่ในเกียรติยศและชื่อเสียง ทั้งนี้ บุคคลทุกคนย่อมมีสิทธิที่จะได้รับการปกป้องคุ้มครอง โดยกฎหมายอันเนื่องมาจากการก้าวล่วงในสิทธิเช่นว่านั้น”[36]

โดยบุคคลต้องได้รับการคุ้มครองตามกฎหมาย แนวคิดในการคุ้มครองสิทธิความเป็นส่วนตัวได้เกิดขึ้นมานานและหลากหลาย แนวคิดหนึ่งที่ได้รับการยอมรับและมีการอ้างอิงถึงอย่างแพร่หลาย คือ แนวคิด

---

[32] หยุด แสงอุทัย, *ความรู้เบื้องต้นเกี่ยวกับกฎหมายทั่วไป* (พิมพ์ครั้งที่ 16 สำนักพิมพ์ประกายพรึก 2548) 145.

[33] บุญศรี มีวงศ์อุโฆษ (เชิงอรรถ17) 520.

[34] สกล อดิศรประเสริฐ, ‘มาตรการทางกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคล: ศึกษาเฉพาะกรณีการแยกแยะประเภทข้อมูล’ (วิทยานิพนธ์ นิติศาตรมหาบัณฑิต มหาวิทยาลัยธุรกิจบัณฑิตย์ 2553) 14.

[35] เพิ่งอ้าง. 12.

[36] Universal Declaration og Human Right 1948, article 12 “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attack upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.”

ของ Samuel D. Warren และ Louis D. Brandeis ในปี ค.ศ. 1980 ที่ได้ให้ความหมายคำว่า “Privacy” ในรูปของวลีสั้น ๆ ว่า “สิทธิที่จะอยู่ตามลำพัง” หรือ “Right to be let alone” โดยมีแนวคิดการคุ้มครองสิทธิในความเป็นส่วนตัวซึ่งเป็นที่ยอมรับ คือ แนวความคิดของ แซมมวล ดี. วอร์เรน (Samuel D. Warren) และหลุยส์ ดี. แบรนดีส์ (Louis D. Brandeis) โดยให้คำจำกัดความของความเป็นอยู่ส่วนตัวไว้ในบทความชื่อ The Right to be let alone)[37] ซึ่งการอยู่โดยลำพังเป็นเขตแดนส่วนบุคคลที่ควรได้รับความเคารพและความคุ้มครอง เพื่อให้บุคคลมีสิทธิที่จะแสวงหาความสุขในชีวิตตามความพอใจโดยที่ไม่ถูกล่วงละเมิดจากผู้อื่นหรือจากสาธารณะ

สิทธิความเป็นอยู่ส่วนตัวในระบบกฎหมาย Civil Law นั้น ได้แก่ สิทธิในชีวิตร่างกาย เคหสถาน การเดินทาง การติดต่อสื่อสาร เกียรติยศ ชื่อเสียง และความเป็นอยู่ส่วนตัวของบุคคล ฯลฯ แนวความคิดเรื่องสิทธิในความเป็นอยู่ส่วนตัวได้รับการพัฒนามาจากทฤษฎีทางกฎหมายในศตวรรษที่ 19[38] โดยเริ่มจากการให้ความคุ้มครองสิทธิในความเป็นส่วนตัวบนพื้นฐานความรับผิดทางละเมิดในประมวลกฎหมายแพ่งและพาณิชย์และความคุ้มครองสิทธิในความเป็นส่วนตัวในกฎหมายอาญาว่าด้วยความรับผิดฐานหมิ่นประมาท[39]

ส่วนหลักการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวจากการกระทำอันเป็นละเมิดในระบบ Common Law ประกอบไปด้วยหลักสำคัญ ดังนี้[40]

ความรับผิดฐานบุกรุก (Trespass) ความรับผิดฐานบุกรุกมีลักษณะสำคัญ คือ ต้องเป็นการบุกรุกทางกายภาพ ได้แก่ การบุกรุกเข้าไปในที่ดิน สิ่งปลูกสร้าง และการเข้าไปรบกวนทางกายภาพต่อบุคคล โดยไม่ได้รับอนุญาต เช่น บุคคลภายนอกหรือเพื่อนบ้านบุกเข้ามาในบ้าน การบุกรุกเข้ามาจะเพื่อทำร้าย หรือเพื่อเข้าพบเข้าพบหรือรบกวนความเป็นอยู่ส่วนตัวก็ตามการบุกรุกเข้ามานี้เน้นว่าต้องเป็นการกระทำในทางกายภาพต่อบุคคลหรือต่อทรัพย์สินโดยตรง ดังนั้น หากข้อเท็จจริงเปลี่ยนเป็นว่าบุคคลภายนอกได้ใช้กล้องส่องทางไกลสอดแนมดูบริเวณบ้าน ดูทรัพย์สิน หรือสอดส่องพฤติกรรมของบุคคล หรือใช้เครื่องมืออิเล็กทรอนิกส์อื่น ๆ เพื่อสอดแนมจากภายนอกลักษณะนี้ไม่มีการกระทำในทางกายภาพต่อบุคคล การกระทำดังกล่าวย่อมไม่ก่อให้เกิดความรับผิดฐานนี้ได้ แต่หากมีการลักลอบเข้าไปติดกล้องโทรทัศน์วงจรปิด ไมโครโฟน หรือเครื่องไม้เครื่องมือต่าง ๆ ที่ใช้สอดแนม แม้จะไม่เกิดการทำลายหรืองัดแงะข้าวของหรือทรัพย์สิน กรณีนี้ย่อมเกิดความรับผิดฐานบุกรุกได้เพราะมีการกระทำทางกายภาพแม้เพียงเล็กน้อยก็ตาม

หากข้อเท็จจริงปรากฏว่าการบุกรุกดังกล่าวเกิดขึ้นในห้องพักผู้ป่วยในโรงพยาบาลหรือห้องพักโรงแรม กรณีนี้ประสบปัญหาในการปรับใช้เช่นกัน ความรับผิดฐานนี้จะเกิดขึ้นได้ผู้ที่จะกล่าวอ้างการละเมิด

---

[37] กิตติพงศ์ กมลธรรมวงศ์, ‘การคุ้มครองข้อมูลข่าวสารส่วนบุคคลในระบบกฎหมายไทย : ปัญหาและแนวทางการแก้ไข’ (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ 2549) 19.

[38] Mark Littman and Peter Carter Ruck, (1970), Privacy and the Law. P.21.

[39] Mark Littman and Peter Carter Ruck, (1970), Privacy and the Law. P.24-25.

[40] จิรารัตน์ วรวัฒน์ธำรง, การคุ้มครองข้อมูลส่วนบุคคล, 14-16.

ความเป็นส่วนตัวในฐานความผิดนี้ต้องมีการแสดงออกซึ่งการเป็นเจ้าของหรือเป็นผู้ทรงสิทธิเป็นสำคัญ ดังนั้น บุคคลที่สามารถกล่าวอ้างตามกฎหมายนี้ได้ต้องเป็นเจ้าของโรงแรมหรือเจ้าของโรงพยาบาลเท่านั้น ผู้ป่วยหรือแขกผู้มาพักจึงไม่สามารถฟ้องร้องหรือได้รับการเยียวยาความเสียหายจากการบุกรุกหรือรบกวนดังกล่าวได้

ด้วยเหตุผลว่าความรับผิดบุกรุกนี้ไม่ได้ถูกสร้างมาเพื่อคุ้มครองความเป็นอยู่ส่วนตัวโดยตรง ดังนั้น ความรับผิดในฐานความผิดนี้จึงไม่ค่อยประสบความสำเร็จหากจะกล่าวอ้าง เพื่อคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวในปัจจุบัน เพราะความเจริญทางเทคโนโลยีในปัจจุบันทำให้การสอดแนม การลักลอบบันทึกภาพหรือเสียง หรือการดักฟัง ทำได้ง่ายและมีการพัฒนาการไปมากขนาดที่ว่าเครื่องมือบางอย่างไม่ต้องอาศัยการยึดติดในทางกายภาพก็สามารถใช้งานได้ ดังนั้น เมื่อไม่มีการกระทำก็ไม่ก่อให้เกิดความรับผิดฐานบุกรุกได้

แต่ปัญหาที่เพิ่มขึ้น เนื่องจากเครื่องดักฟังหรือเครื่องมือสอดแนมในปัจจุบันไม่สามารถปรับในฐานความผิดบุกรุกได้เลย และการนำความรับผิดฐานบุกรุกไปปรับใช้กับบุคคลนั้นต้องปรากฏว่ามีการเข้าไปจู่โจมและมีลักษณะที่เป็นการปะทะ เช่น การตรวจค้นสินค้าที่ตัวลูกค้า หากสงสัยว่าลูกค้าได้ขโมยของ ผู้จัดการร้านไม่สามารถทำการค้นได้ สิ่งที่ต้องกระทำคือให้เป็นหน้าที่ของเจ้าหน้าที่ตำรวจในขณะค้นจึงจะไม่มีความผิดฐานบุกรุก[41] ท้ายที่สุดพบว่าหากจะนำความรับผิดฐานบุกรุกไปปรับใช้ในการให้การเยียวยาความเสียหายในการละเมิดซึ่งปัจจุบันนี้ด้วยสถานการณ์ที่ซับซ้อน เนื่องจากข้อจำกัดทางกายภาพที่นับวันการพัฒนาเทคโนโลยีสมัยใหม่ทำให้ความรับผิดฐานบุกรุกทางกายภาพมีน้อยลง ทำให้ความรับผิดฐานบุกรุกไม่เหมาะสมกับการปรับใช้เยียวยาความเสียหายอันเกิดจากการละเมิดในสถานการณ์ใหม่ ๆ ได้อย่างมีประสิทธิภาพ

การก่อให้เกิดความเดือนร้อนรำคาญ (Nuisance) เป็นลักษณะการทำให้เกิดความเดือดร้อนรำคาญ โดยการสอดรู้สอดเห็นหรือรบกวนความเป็นส่วนตัวโดยเพื่อนบ้าน ในกรณีนี้ศาลได้เคยวางบรรทัดฐานไว้ว่า ความรับผิดฐานก่อให้เกิดความเดือดร้อนรำคาญมีได้แม้ว่าผู้ก่อให้เกิดความเดือนร้อนรำคาญอาจต่อสู้ว่าตนได้ใช้ความระมัดระวังถึงที่สุดแล้ว แต่ก็เหลือความสามารถที่จะระงับได้ ก็ยังต้องรับผิดเสมอ กรณีที่เห็นบ่อยครั้ง เช่น การที่บริษัทหรือห้างร้านโทรศัพท์ชักชวนให้ซื้อสินค้าและบริการบ่อยครั้งจนเกินความจำเป็นสร้างความอึดอัดใจหรือรำคาญ หรือแม้กระทั่งการที่เพื่อนบ้านโทรศัพท์มาที่บ้านเพื่อพูดคุยในเวลากลางดึกโดยที่ไม่ได้มีเหตุด่วนเหตุร้ายหรือมีความจำเป็นใด ๆ ซึ่งนอกจากจะเป็นการก่อให้เกิดความเดือดร้อนรำคาญแล้ว ยังเป็นการละเมิดความเป็นส่วนตัวของบุคคลด้วย

หมิ่นประมาท (Defamation) เป็นการแสดงข้อความหรือความหมายใด ๆ ต่อบุคคลหนึ่งบุคคลใดให้เขาได้รับความเสียหายต่อชื่อเสียง เกียรติคุณ หรือถูกประเมินคุณค่าให้ต่ำลงหรือถูกดูหมิ่นเกลียดชังในสายตาของคนทั่วไป

ในการกระทำหมิ่นประมาทเป็นบทบัญญัติที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลโดยตรง เนื่องจากส่วนใหญ่เป็นเรื่องของการเผยแพร่ความเป็นส่วนตัวของบุคคลต่อสาธารณะ เช่น การกล่าวข้อความอันเป็นเท็จ การพูดจาเยาะเย้ย ถากถาง หรือการกระทำที่เป็นสาเหตุทำให้เขาต้องอับอายขายหน้าหรือต้อง

---

[41] Mark Littman and Peter Carter Ruck, (1970), Privacy and the Law. P.8.

หลีกหนีจากผู้คน เช่น การกล่าวร้ายว่าเป็นคนไม่มีความรู้สึกเป็นคนไม่มีศักดิ์ศรี เป็นตัวสำรอง ซึ่งเป็นสาระสำคัญทำให้ชีวิตแต่งงานล้มเหลวเนื่องจากคำกล่าวนั้น ในกรณีนี้ นอกจากจะเป็นการหมิ่นประมาทแล้วยังเป็นการละเมิดข้อมูลข่าวสารอันเป็นความลับ และละเมิดชีวิตความเป็นอยู่ในครอบครัวด้วย[42]

ในบางกรณี เช่น การให้บริการข้อมูลข่าวสารการเงินขององค์กร Credit Reference หรือเครดิตบูโร อาจเป็นการลดฐานะความน่าเชื่อถือทางการเงินของบุคคล หรือเป็นการทำให้บุคคลได้รับความไม่ไว้วางใจในฐานะทางการเงิน แต่ในระบบกฎหมาย Common Law การให้ข้อมูลข่าวสารอันอาจเป็นการทำให้เขาได้รับความเสียหายหรืออับอายจากการถูกประเมินฐานะทางการเงินไม่ถือว่าเป็นหมิ่นประมาท เนื่องจากการกล่าวนั้นเป็นการกล่าวข้อความจริงซึ่งเป็นความรับผิดฐานหมิ่นประมาทไม่ได้มีความหมายรวมถึงการเปิดเผยข้อเท็จจริงส่วนตัว แม้ว่าการเปิดเผยดังกล่าวเป็นการเปิดเผยโดยไม่จำเป็นหรือไม่มีเหตุผลอันควรและเป็นการที่มุ่งประสงค์ร้ายต่อบุคคลอื่นก็ตาม

ความรับผิดต่อความไว้วางใจต่อกัน (Breach of Confidence) โดยหลักเมื่อมีการถ่ายทอดข้อมูลข่าวสารแก่อีกคนหนึ่งที่เป็นผู้รับข้อมูล ผู้รับข้อมูลมีหน้าที่ต้องก่อให้เกิดความไว้วางใจในการรักษาข้อมูล โดยไม่เปิดเผยต่อบุคคลอื่น หากข้อมูลข่าวสารนั้นเป็นข้อมูลที่เป็นความลับและบุคคลภายนอกเกิดรู้ข้อมูลข่าวสารนั้นภายในเวลาที่ผู้รับข้อมูลนั้นได้รับรู้เช่นกันและโดยที่ผู้บอกเล่านั้นไม่ได้อนุญาต ถือว่าผู้รับข้อมูลข่าวสารไม่ทำให้เกิดการไม่ไว้วางใจต่อภระหน้าที่ดังกล่าว ซึ่งภาระหน้าที่นี้จะเกิดขึ้นทันที เมื่อข้อมูลข่าวสารได้ถูกบอกหรือแจ้งให้ทราบและในการกล่าวอ้างนั้น ผู้กล่าวอ้างต้องแสดงให้เห็นว่าผู้รับข้อมูลข่าวสารมีหน้าที่ เนื่องจากมีการรับรู้เรื่องที่เป็นความลับนั้น[43] ภาระหน้าที่นี้อาจเกิดขึ้น โดยเรียกว่าเป็นหน้าที่ตามศีลธรรมเป็นความผูกพันที่บุคคลพึงปฏิบัติต่อกันหรือเป็นหน้าที่ตามสัญญาคือมีการทำเป็นลายลักษณ์อักษร

การกระทำโดยประมาทเป็นเหตุให้ผู้อื่นได้รับความเสียหาย (Negligence) ในกฎหมายลักษณะละเมิด การเยียวยาความเสียหายในความรับผิดฐานประมาทเป็นมาตรการทั่วไปในการเยียวยาความเสียหาย องค์ประกอบความรับผิดฐานประมาทนั้น เป็นการกระทำที่ไม่ได้เกิดจากการจงใจเป็นการขาดความระมัดระวังจริงอยู่ที่การละเมิดความเป็นส่วนตัวส่วนตัวมากเกิดจากความจงใจ แต่ในบางกรณีความเสียหายที่เกิดขึ้นแม้ผู้กระทำความจะไม่ได้ตั้งใจ แต่หากเกิดจากการประมาทเลินเล่อทำให้เกิดการละเมิดความเป็นส่วนตัวผู้กระทำก็มีโอกาสที่จะต้องถูกฟ้องในความรับผิดฐานประมาทเลินเล่อทำให้เขาได้รับความเสียหายได้

การคุ้มครองสิทธิส่วนบุคคลในเรื่องการค้นและการยึดทรัพย์สิน (Searches and Seizures) จากการคุ้มครองสิทธิส่วนตัวที่สำคัญอีกประการหนึ่งถูกตีความให้อยู่ภายใต้ขอบเขตของ The Forth Amendment จากการตีความของศาลเห็นพ้องตรงกันว่าห้ามมิให้มีการตรวจค้นและยึดทรัพย์สินของประชาชน ความคุ้มครองนี้ ได้แก่ ในบ้าน เอกสาร และต่อตัวบุคคลเอง โดยไม่มีเหตุอันควรหรือตามอำเภอใจของเจ้าหน้าที่ของรัฐ สิทธิส่วนบุคคลในการค้นและยึดนี้มีความเกี่ยวข้องกับ Due Process หรือวิธีการที่ถูกต้องตามกฎหมาย

---

[42] Mark Littman and Peter Carter Ruck,Loc.cit.

[43] Raymond Wacks, Personal Information: Privacy and the Law. 1993 P. 51.

เพราะกระบวนการ Due Process คือ กระบวนการคุ้มครองสิทธิของจำเลย มีวัตถุประสงค์ในการคุ้มครองสิทธิของบุคคลที่ตกเป็นจำเลยในคดีอาญา การปฏิบัติต่อผู้กระทำผิดต้องคำนึงถึงสิทธิและเสรีภาพของบุคคลในฐานะที่เขาเป็นส่วนหนึ่งในสังคม[44] ผู้ต้องหาไม่สามารถถูกบังคับให้ตอบคำถามเพื่อเป็นพยานหลักฐานที่เป็นปฏิปักษ์ต่อตนเองและไม่สามารถถูกค้นและยึดสิ่งของเพื่อนำไปเป็นหลักฐานโดยไม่มีเหตุผลอันสมควร การค้นสื่อลามกบ้านของจำเลย โดยไม่ได้รับอนุญาตแม้ว่าจะไม่เป็นการบังคับขู่เข็ญในทางกายภาพ แต่ศาลอาจมองว่าการครอบครองและควบคุมสื่อลามกเป็นความผิดอาญา แต่การตรวจค้นต้องชอบด้วยวิธีการเพื่อคุ้มครองสิทธิของบุคคลด้วย การค้นและยึดโดยไม่ได้รับอนุญาตจึงเป็นการไม่ชอบด้วยรัฐธรรมนูญ ถือว่าเป็นการแทรกแซงเสรีภาพในการพูดและเสรีภาพในการอ่าน

กระบวนการ Due Process มีพื้นฐานความคิดมาจากกระบวนการคุ้มครองสิทธิของจำเลย มีวัตถุประสงค์ในการคุ้มครองสิทธิของบุคคล การปฏิบัติต่อผู้กระทำความผิดต้องคำนึงถึงสิทธิเสรีภาพของบุคคลในฐานะที่เขาเป็นส่วนหนึ่งในสังคม ผู้ต้องหาไม่สามารถถูกบังคับให้ตอบคำถามเพื่อเป็นพยานหลักฐานที่เป็นปฏิปักษ์ต่อตนเอง และไม่สามารถถูกค้นและยึดสิ่งของเพื่อนำไปเป็นหลักฐานโดยไม่มีเหตุอันสมควร ซึ่งหลักการดังกล่าวศาลได้วินิจฉัยไว้ในคดี Gliswold v. Connecticut ในกรณีที่เจ้าพนักงานได้ตรวจค้นในห้องนอนของคู่สามีภรรยา เพื่อตรวจค้นเครื่องมือ หรือยาที่ใช้ในการคุมกำเนิด ศาลวินิจฉัยว่าการกระทำดังกล่าวเป็นการละเมิดสิทธิส่วนบุคคลด้วย[45]

หลักว่าด้วยวิธีการที่เหมาะสมนี้ศาลได้นำมาใช้ในกรณีที่มีการนำพยานหลักฐานมาโดยการใช้เครื่องมือทางอิเล็กทรอนิกส์ด้วย ในการดักฟังการสนทนาทางโทรศัพท์ เช่น ในคดี Katz v. United States การติดเครื่องดักฟังโทรศัพท์ ซึ่งกรณีนี้เครื่องดักฟังไม่ได้ติดอยู่กับเครื่องโทรศัพท์บ้าน หรือภายในบริเวณบ้านอันเป็นที่ส่วนบุคคล การกระทำดังกล่าวนี้นอกจากจะเป็นการไม่ชอบด้วยหลักว่าด้วยวิธีการที่เหมาะสมแล้ว ยังเป็นการละเมิดข้อมูลส่วนบุคคลอีกด้วย แต่ปัญหาคือเครื่องดักฟังดังกล่าวติดอยู่กับโทรศัพท์สาธารณะ กรณีนี้จะคาดหวังความเป็นส่วนตัวได้หรือไม่ ซึ่งผู้พิพากษาได้ให้เหตุผลว่า การคุ้มครองความเป็นอยู่ส่วนตัวของบุคคลเป็นสิทธิที่ติดไปกับตัวของบุคคลไม่ว่าบุคคลนั้นจะอยู่ในที่ส่วนตัวหรืออยู่ในพื้นที่สาธารณะก็ย่อมต้องได้รับความคุ้มครองด้วยเช่นเดียวกัน และภายใต้ The Forth Amendment ฉบับนี้ยังขยายขอบเขตการคุ้มครองไป

---

[44] นริศ ชำนาญชานันท์, ‘ละเมิดอำนาจศาล: โทษที่ขัดต่อกระบวนการ Due Process’(2539, มกราคม) วารสารอัยการ,19, 215. 138-139.

[45] จากคดีนี้ ศาลพิจารณาว่าสิทธิส่วนบุคคลเป็นสิทธิที่มีมาก่อน The Bill of Right มีมาก่อนสถาบันทางการเมือง และมีมาก่อนโรงเรียนสอนกฎหมายเสียอีก ชีวิตแต่งงานเป็นการก้าวต่อไปด้วยกันเพื่อความดีขึ้นหรือเลวลง เป็นการคงอยู่ซึ่งความหวัง และเป็นส่วนตัวอย่างมากอันเป็นเรื่องที่ไม่สามารถล่วงเกินได้ การส่งเสริมความสัมพันธ์ในการดำเนินชีวิต ไม่เป็นเรื่องที่เป็นความกันในโรงในศาล ไม่ใช่การยึดมั่นในนโยบายทางการเมืองการแต่งงานเป็นความจงรักภักดีของบุคคลสองฝ่าย ไม่ใช่การค้าขายหรือเป็นการวางแผนการอยู่ร่วมกันในสังคม. อ้างถึงใน สกล อดิศรประเสริฐ, ‘มาตรการทางกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคล: ศึกษาเฉพาะกรณีการแยกแยะประเภทข้อมูล’ (วิทยานิพนธ์ นิติศาตรมหาบัณฑิตย์ มหาวิทยาลัยธุรกิจบัณฑิตย์ 2553) 17.

ถึงสิทธิในความมั่นคงปลอดภัยของบุคคลในบ้าน เอกสาร ดังนั้นการติดเครื่องดักฟังกับตู้โทรศัพท์สาธารณะจึงเป็นการละเมิดความเป็นส่วนตัวและละเมิดข้อมูลส่วนบุคคลด้วย

2.4 ประเภทและองค์ประกอบของข้อมูลส่วนบุคคล[46]

ความคุ้มครองข้อมูลส่วนบุคคลแบ่งความคุ้มครองข้อมูลออกเป็น 2 ประเภท คือ ข้อมูลทั่วไป (Non- Sensitive Data) และข้อมูลที่มีความอ่อนไหว (Sensitive Data) โดยลักษณะของข้อมูลทั้ง 2 ประเภท มีรายละเอียด ดังต่อไปนี้

2.4.1 ข้อมูลทั่วไป (Non-Sensitive Data)

ข้อมูลเกี่ยวกับผู้เป็นเจ้าของข้อมูลซึ่งสามารถบ่งชี้เฉพาะเจาะจงไปยังเจ้าของข้อมูลได้ เช่น ชื่อ ที่อยู่ อาชีพ อายุ เบอร์โทรศัพท์ การศึกษา สถานภาพในการสมรส ตำแหน่งหน้าที่ ทางการงาน หรือลักษณะทางกายภาพของบุคคล เป็นต้น ข้อมูลประเภทดังกล่าวเป็นข้อมูล ซึ่งมิได้มีความละเอียดอ่อน จนอาจนำมาสู่ปัญหาต่าง ๆ ได้ จึงทำให้ข้อมูลดังกล่าวเป็นข้อมูลที่อาจเก็บรวบรวมเปิดเผยหรือใช้ได้ ทั้งนี้ ภายใต้หลักเกณฑ์ที่กฎหมายกำหนดไว้ ซึ่งข้อมูลเหล่านี้สามารถนำมาประมวลผลรวมกันเป็นข้อเท็จจริงที่สามารถบ่งชี้ถึงลักษณะเฉพาะตัวของบุคคลได้ โดยสภาพของข้อมูลเหล่านี้เป็นข้อมูลข่าวสารของบุคคลที่สามารถเปิดเผยต่อสาธารณะได้เป็นเรื่องปกติธรรมดาทั่วไป

2.4.2 ข้อมูลที่มีความอ่อนไหว (Sensitive Data)

ข้อมูลส่วนบุคคลที่เป็นความลับ ศาสตราจารย์จิตติ ติงศภัทย์ ได้ให้คำนิยามความหมายไว้ว่า “ความลับ” หมายถึง ข้อเท็จจริงหรือวิธีการที่ไม่ประจักษ์แก่คนทั่วไป และเป็นสิ่งที่เจ้าของประสงค์จะปกปิดเพื่อกิจการส่วนตัวของเจ้าของความลับ ฉะนั้นการที่จะถือว่าข้อเท็จจริงใดเป็นความลับจึงแล้วแต่ข้อเท็จจริงว่าเจ้าของต้องการปกปิดหรือไม่ การปกปิดอาจปิดเฉพาะคนอื่น นอกจากคนที่รู้ความลับนั้นในวงจำกัด ถ้าเป็นสิ่งที่รู้กันทั่วไป เช่นของผสมที่ได้แยกธาตุแสดงโดยเปิดเผยแล้วก็ไม่เป็นความลับ[47] ข้อมูลของบุคคลซึ่งถือเป็นเรื่องเฉพาะตัวของบุคคล เป็นข้อมูลซึ่งมีความละเอียดอ่อนสูง กล่าวคือ ข้อมูลดังกล่าวเป็นข้อมูลที่เป็นความลับหรือไม่พึงประสงค์ที่จะให้มีการเปิดเผย ซึ่งหากมีการเปิดเผยอาจก่อให้เกิดผลกระทบที่ไม่พึงประสงค์ตามมา เช่น กระทบต่อความรู้สึกของเจ้าของข้อมูลหรือประชาชนทั่วไป เป็นข้อมูลที่ก่อให้เกิดความ ขัดแย้งได้ ก่อให้เกิดผลกระทบต่อชื่อเสียงหรือเกียรติคุณของเจ้าของข้อมูล หรือเป็นข้อมูลซึ่งหากมีการเปิดเผยอาจก่อให้เกิดการตั้งข้อรังเกียจหรือเลือกปฏิบัติหรือเกิดอันตรายต่อเจ้าของข้อมูล โดยประเภทข้อมูลเจ้าของข้อมูลมีวัตถุประสงค์ที่จะเก็บข้อมูลประเภทนี้ไว้เป็นความลับ หรือไม่ประสงค์ให้มีการเปิดเผยข้อมูล เช่น ข้อมูล

---

[46] อธิพร สิทธิธีรรัตน์, ‘ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลในบริบทอิเล็คทรอนิกส์’ (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ 2558) 31.

[47] ศิริกุล ภู่พันธ์, ‘ข้อความคิดว่าด้วยข้อมูลข่าวสารส่วนบุคคล’ (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ 2548) 83.

เกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อเกี่ยวกับลัทธิ ศาสนา พฤติกรรมทางเพศ ประวัติสุขภาพ ประวัติอาชาญกรรม ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือ สถานะทางการเงิน เป็นต้น

ในทางปฏิบัติตามกฎหมาย การคุ้มครองข้อมูลส่วนบุคคลในปัจจุบันนั้น กำหนดขอบเขตไว้อย่างกว้างขวาง ซึ่งไม่ได้มีขอบเขตเฉพาะข้อมูลประเภทที่มีความอ่อนไหวเท่านั้น แต่ยังรวมถึงข้อมูลทั่ว ๆ ไปด้วย ดันนั้น ข้อมูลใด ๆ ที่จะเป็นข้อมูลส่วนบุคคลจึงต้องประกอบด้วยองค์ประกอบ 2 ประการ ดังนี้[48]

ข้อมูลที่เกี่ยวข้องกับสิ่งเฉพาะตัวของบุคคล คือ ข้อมูลข่าวสารที่เป็นเรื่องเฉพาะตัวของบุคคลและมีผลเฉพาะตัวไม่เกี่ยวกับบุคคลภายนอก ได้แก่ คุณสมบัติติดตัวของบุคคล ซึ่งอาจเป็นคุณสมบัติที่ติดตัวบุคคลไปตลอดชีวิตหรือลักษณะพันธุกรรมของบุคคล เช่น เชื้อชาติ กลุ่มเลือด สีผิว สีตา ลายนิ้วมือ ความพิการของร่างกายที่มีแต่กำหนดติดตัวบุคคลไปจนตาย หรือสิ่งที่เป็นเฉพาะตัวของบุคคลที่สามารถเปลี่ยนแปลงได้ตามกาลเวลา เช่น น้ำหนัก ส่วนสูง อายุ วุฒิการศึกษา ความสามารถ หน้าที่การงาน ฯ หรือ การประเมินคุณค่าในตัวบุคคล เช่น ทัศนคติ การประเมินความประพฤติ และความเห็นเกี่ยวกับการกระทำต่าง ๆ ของบุคคล เนื่องจากข้อมูลข่าวสารเหล่านี้เป็นสิ่งที่สื่อให้เห็นถึงความคิด ความสามารถ และการแสดงออก และแนวความคิด ความเชื่อ พฤติกรรมซึ่งอาจเปลี่ยนแปลงไปตามวัยและวันเวลา เช่น ความสนใจทางการเมือง ความสนใจทางเพศ ความรักหรือความชอบ ความสามารถ เป็นต้น

ข้อมูลที่สามารถพิสูจน์ตัวบุคคลได้ คือ สิ่งที่บอกลักษณะที่ทำให้รู้จักบุคคลจากข้อมูลข่าวสารนั้นได้ หรือเรียกได้ว่าเป็นข้อมูลที่บ่งบอกความเป็นตัวตนของบุคคล หรือเป็นข้อมูลที่แสดงถึงลักษณะเฉพาะตัวที่แตกต่างไปจากบุคคลอื่น ได้แก่ เครื่องหมายบ่งชี้ตัวบุคคล เช่น ชื่อ นามสกุล ฉายา หรือ นามแฝง หรือเลขรหัส กล่าวคือ หมายเลขบัตรประชาชน หมายเลขในใบอนุญาตขับขี่ฯ หรือ ลักษณะทางกายภาพของบุคคลภายนอก เช่น ความสูงต่ำ ความสมบูรณ์ หรือความพิการของบุคคลในทางกายภาพ และข้อมูลที่มีลักษณะเป็นการประเมินคุณค่าของบุคคล ทัศนคติต่อบุคคล การประพฤติปฏิบัติและการกระทำต่าง ๆ ของบุคคล ซึ่งข้อมูลข่าวสารเหล่านี้เป็นสิ่งที่สื่อให้เห็นถึงความคิดของบุคคลสามารถแสดงออกถึงความมีตัวตนของบุคคลได้ทั้งสิ้น เช่น ผลการสอบ การประเมินผลงาน ฯลฯ

อาจกล่าวได้ว่าข้อมูลส่วนบุคคลที่เป็นความลับเป็นข้อมูลที่มีความอ่อนไหว (Sensitive Data) อันเป็นข้อมูลที่ถือว่าเป็นเรื่องเฉพาะตัว (Intimate) ของบุคคลผู้เป็นเจ้าของข้อมูลโดยเฉพาะ ซึ่งเป็นข้อมูลที่ไม่พึงประสงค์ที่จะให้มีการเปิดเผยแก่สาธารณะชน ได้แก่ เรื่องส่วนตัวในการติดต่อสื่อสารทางโทรศัพท์ การดำเนินชีวิตส่วนตัว ทัศนคติ ความเชื่อในทางศาสนา ลัทธิการเมือง ลักษณะพิการทางกาย การมีเพศสัมพันธ์ พฤติกรรมหรือรสนิยมทางเพศ เป็นต้น ข้อมูลที่มีความอ่อนไหว เป็นข้อมูลที่มีลักษณะพิเศษกว่าข้อมูลข่าวสารทั่ว ๆ ไปเพราะข้อมูลประเภทนี้หากมีการเปิดเผยจะกระทบถึงความรู้สึกของประชาชนทั่วไปในทางลบต่อ

[48] เพิ่งอ้าง. 84-85.

ชื่อเสียงเกียรติคุณ และการเปิดเผยอาจก่อให้เกิดอันตรายต่อบุคคลได้ เช่น การเปิดเผยเชื้อชาติซึ่งบาง กรณีหากมีการเปิดเผยทางเชื้อชาตินั้น อาจนำมาซึ่งความไม่ปลอดภัยในชีวิตและทรัพย์สินของบุคคลได้

2.5 รูปแบบของการคุ้มครองข้อมูลส่วนบุคคล[49]

รูปแบบของการให้การคุ้มครองข้อมูลส่วนบุคคลนั้นมีรูปแบบที่แตกต่างกันที่สำคัญในปัจจุบันสามารถแบ่งแยกได้ดังรายละเอียดต่อไปนี้

การคุ้มครองโดยกฎหมายทั่วไป

ในปี ค.ศ. 1970 ได้บัญญัติกฎหมายทั่วไปขึ้นมาฉบับหนึ่งซึ่งเป็นกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลขึ้น (Comprehensive Law) ซึ่งนับเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับแรกของโลก ซึ่งในเวลาต่อมาหลายประเทศก็ได้มีการบัญญัติกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล โดยวางหลักการทั่วไปครอบคลุมถึงการเก็บรวมรวม การใช้ การเปิดเผยข้อมูลส่วนบุคคลทั้งของภาครัฐและภาคเอกชน โดยกำหนดให้มีหน่วยงานกลางคอยกำกับดูแลให้มีการปฏิบัติตามกฎหมายภาคธุรกิจอุตสาหกรรมอาจกำหนดหลักเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคลขึ้น เพื่อใช้บังคับกันเองและมีหน่วยงานกลางคอยดูแลให้มีการปฏิบัติตามหลักเกณฑ์ที่กำหนด ซึ่งการออกกฎหมายลักษณะดังกล่าวนี้ ได้นำแบบอย่างมาจากกฎหมายของประเทศเยอรมัน

การคุ้มครองโดยกฎหมายเฉพาะ

การบัญญัติกฎหมายเฉพาะเพื่อคุ้มครองข้อมูลส่วนบุคคลเฉพาะกรณีเป็นวิธิการที่นิยมใช้ในบางประเทศเช่น ประเทศสหรัฐอเมริกา เป็นการหลีกเลี่ยงการวางหลักการทั่วไปโดยมีกฎหมายแต่ละเรื่องไว้เป็นการเฉพาะ เช่น กฎหมายคุ้มครองข้อมูลส่วนบุคคลของเด็กบนเครือข่ายอินเทอร์เน็ต(Children's Online Privacy Act of 1998 COPPA) กฎหมายคุ้มครองข้อมูลส่วนบุคคลในการหาคู่ทางคอมพิวเตอร์ (Computer Matching and Privacy Protection Act of 1988) ข้อดีของการบัญญัติกฎหมายเฉพาะต้องมีการบัญญัติกฎหมายคือรัฐสามารถวางกฎเกณฑ์เฉพาะเรื่องได้ ส่วนข้อเสียคือการบัญญัติกฎหมายเฉพาะต้องมีการปรับปรุง พัฒนา แก้ไข หรือบัญญัติกฎหมายใหม่เพื่อรองรับให้ทันกับเทคโนโลยีที่มีการเปลี่ยนแปลงตลอดเวลา

การคุ้มครองโดยกลไกการกำกับดูแลตนเอง

การใช้กลไกกำกับดูแลตนเอง (Personal Data Protection) ในการคุ้มครองข้อมูลส่วนบุคคลนั้นเป็นการที่ผู้ประกอบการภาคธุรกิจประเภทเดียวกันหรือกลุ่มเดียวกันร่วมกันจัดทำประมวลจริยธรรม เพื่อเป็นระเบียบปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลและร่วมกันดูแลให้สมาชิกปฏิบัติตามกฎระเบียบปฏิบัตินั้น โดยไม่มีหน่วยงานกลางคอยกำกับดูแล

การคุ้มครองโดยใช้เทคโนโลยี

---

[49] สุขวสา ถมังรักษ์สัตว์, 'การคุ้มครองข้อมูลส่วนบุคคลของเด็กบนสื่ออิเล็กทรอนิกส์' (2562 มกราคม-มิถุนายน) 20 วารสารเกษมบัณฑิต 1. 136-137.

เนื่องจากในปัจจุบันเทคโนโลยีได้พัฒนาไปอย่างรวดเร็วจึงมีการติดต่อสื่อสารผ่านคอมพิวเตอร์ เช่น การส่งจดหมายอิเล็กทรอนิกส์ (E-mail) หรือ MSN Messenger กันอย่างแพร่หลาย จึงมีผู้คิดค้นเทคโนโลยีเพื่อคุ้มครองข้อมูลส่วนบุคคลในระหว่างการติดต่อสื่อสารในช่องทางดังกล่าวและเรียกเทคโนโลยีนี้ว่า “Privacy Enhancing Technologies-PET” ซึ่งเทคโนโลยีดังกล่าวจะทำหน้าที่ป้องกันหรือลดการเก็บรวมรวมข้อมูลที่สามารถระบุตัวบุคคล (identifiable information) ได้ จะเห็นได้ว่าเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลนั้นมีหลายรูปแบบโดยหลักเกณฑ์หรือรูปแบบดังกล่าวมีลักษณะมีหลักเกณฑ์หรือหลักปฏิบัติที่แตกต่างกันออกไป อาจเนื่องมาจากลักษณะของการบังคับใช้กฎหมายในแต่ละประเทศหรือองค์กรนั้นรวมทั้งรูปแบบของข้อมูลที่แตกต่างกันรูปแบบของหลักเกณฑ์ให้ความคุ้มครองจึงมีความแตกต่างกันออกไป แต่ทั้งนี้หลักเกณฑ์ดังกล่าวต่างก็มีวัตถุประสงค์ในการให้ความคุ้มครองข้อมูลส่วนบุคคลทั้งสิ้น

จะเห็นได้ว่า การคุ้มครองข้อมูลส่วนบุคคลนั้นมีหลายรูปแบบโดยแนวทางหรือรูปแบบดังกล่าวมีลักษณะมีหลักเกณฑ์หรือหลักปฏิบัติที่แตกต่างกันออกไป อาจเนื่องมาจากลักษณะของการบังคับใช้กฎหมายในแต่ละประเทศ หรือองค์กรนั้นรวมทั้งรูปแบบของข้อมูลที่แตกต่างกัน รูปแบบของหลักเกณฑ์ให้ความคุ้มครองจึงมีความแตกต่างกันออกไปแต่ทั้งนี้หลักเกณฑ์ดังกล่าวต่างก็มีวัตถุประสงค์ในการให้ความคุ้มครองข้อมูลส่วนบุคคลทั้งสิ้น

2.6 แหล่งที่มาของข้อมูลส่วนบุคคล[50]

ข้อมูลส่วนบุคคลอาจอยู่ในการควบคุมดูแลหรือจัดเก็บโดยบุคคลหรือนิติบุคคล องค์กร หรือหน่วยงานของรัฐ เมื่อบุคคลเจ้าของข้อมูลเข้าไปดำเนินการติดต่อ ซึ่งการจัดเก็บดูแลรักษาข้อมูลสามารถแยกความสัมพันธ์ได้ ดังนี้

ข้อมูลส่วนบุคคลที่จัดเก็บโดยบุคคล นิติบุคคล หรือองค์กรซึ่งมีความสัมพันธ์กับบุคคลนั้นโดยตรง ถือเป็นความยินยอมพร้อมใจของบุคคลผู้เป็นเจ้าของข้อมูลที่จะยอมให้ข้อมูลของตนอยู่ในความครอบครองหรือดูแลรักษาของบุคคล นิติบุคคล หรือองค์กรที่ตนไปติดต่อ เช่น ชื่อ ที่อยู่ หมายเลขโทรศัพท์ หรือข้อมูลอื่น ๆ ที่จำเป็นต้องใช้ในการเปิดบัญชีเงินฝาก การให้บริการบัตรเครดิต ฯ ในทางปฏิบัติผู้เป็นเจ้าของข้อมูลมักเข้าใจว่า ข้อมูลของตนจะไม่ถูกนำไปเผยแพร่หรือนำไปใช้ในวัตถุประสงค์อื่น ๆ

ข้อมูลส่วนบุคคลที่จัดเก็บดูแลโดยรัฐหรือเอกชน ซึ่งไม่มีความสัมพันธ์กับบุคคลนั้นโดยตรง

กรณีข้อมูลส่วนบุคคลที่จัดเก็บดูแลโดยรัฐ อาจจำแนกได้ 3 กลุ่ม ได้แก่

กลุ่มที่ 1 ข้อมูลที่จัดเก็บโดยหน่วยงานพิเศษของรัฐ

กลุ่มที่ 2 ข้อมูลงานทะเบียนราษฎร์ งานสถิติ

---

[50] ชุลีพร น่วมทนง, ‘สิทธิมนุษยชนกับการคุ้มครองข้อมูลส่วนบุคคล’ (เอกสารวิชาการการอบรมหลักสูตรหลักนิติธรรมเพื่อประชาธิปไตย รุ่นที่ 2 วิทยาลัยรัฐธรรมนูญ สถาบันรัฐธรรมนูญศึกษา สำนักงานศาลรัฐธรรมนูญ) 7-8.

กลุ่มที่ 3 ข้อมูลที่บางหน่วยงานดำเนินการสืบเสาะหาข้อมูลเกี่ยวกับบุคคลหนึ่งจากแหล่งต่าง ๆ ไว้อย่างละเอียดเพื่อวัตถุประสงค์เฉพาะกรณี

ส่วนข้อมูลส่วนบุคคลที่จัดเก็บดูแลโดยหน่วยงานเอกชน เช่น การจัดเก็บข่าวสาร และข้อมูลของสำนักงานทนายความ นักสืบเอกชน เจ้าหนี้ ที่ต้องการจะสืบค้นล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่น ซึ่งอาจไม่มีความสัมพันธ์โดยตรงและไม่ได้รับความยินยอมจากเจ้าของข้อมูล

2.7 สิทธิของเจ้าของข้อมูล

ด้วยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ Personal Data Protection Act, B.E. 2562 ที่ประเทศไทยมีผลบังคับใช้เมื่อวันที่ 1 มิถุนายน พ.ศ. 2565 ที่ผ่านมาไม่เพียงแต่ครอบคลุมแก่เจ้าของข้อมูลส่วนบุคคล แต่ยังมีรายละเอียดการบังคับใช้ต่อองค์กร หน่วยงานของรัฐ ฯลฯ หลายองค์กรจึงกระตือรือร้นที่จะจัดทำข้อมูลให้ถูกต้องตามกฎหมาย และสิ่งที่สำคัญที่เจ้าของข้อมูลส่วนบุคคล และผู้ประกอบการควรเตรียมพร้อมและทำความเข้าใจอย่างถูกต้อง คือ สิทธิของเจ้าของข้อมูล

สิทธิของเจ้าของข้อมูล เจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล หรือ Personal Data Protection Act, B.E. 2562 จะต้องให้ความยินยอมแก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประกอบการเพื่อรวบรวม ใช้ หรือเปิดเผยข้อมูล ซึ่งเจ้าของข้อมูลก็มีสิทธิในข้อมูลของตัวเองตามกฎหมาย และสามารถใช้สิทธินั้นได้โดยแบ่งออกได้ ดังนี้

1. สิทธิได้รับการแจ้งให้ทราบ

ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องแจ้งรายละเอียดและวัตถุประสงค์ในการเก็บรวบรวมข้อมูล การใช้ หรือเปิดเผยข้อมูลส่วนบุคคลให้เจ้าของข้อมูลทราบก่อนหรือขณะเก็บรวบรวมข้อมูล โดยเจ้าของข้อมูลมีสิทธิที่จะทราบว่าจะจัดเก็บข้อมูลอะไรบ้าง รวมถึงระยะเวลาการจัดเก็บ สถานที่ และวิธีการติดต่อกับผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งเรามักจะเห็นการแจ้งข้อมูลเหล่านี้ตามข้อกำหนดและตามนโยบายความเป็นส่วนตัวก่อนที่ผู้ใช้งานเว็บไซต์จะสมัครสมาชิก หรือตามแบบฟอร์มก่อนเปิดบัญชีธนาคาร

2. สิทธิในการแก้ไขข้อมูล

เจ้าของข้อมูลมีสิทธิที่จะขอแก้ไขข้อมูลส่วนบุคคลของตนเองให้มีความถูกต้อง เป็นปัจจุบัน และไม่ก่อให้เกิดความเข้าใจผิดได้ โดยการแก้ไขนั้นจะต้องเป็นไปด้วยความสุจริต และไม่ขัดต่อหลักกฎหมาย ซึ่งตามเว็บไซต์ส่วนใหญ่ เราจะสามารถเข้าไปแก้ไขข้อมูลส่วนตัว เช่น ที่อยู่ เบอร์โทรศัพท์ รหัสผ่าน ในหน้าบัญชีสมาชิกเองได้

3. สิทธิในการเพิกถอนความยินยอม

กรณีเจ้าของข้อมูลเคยให้ความยินยอมในการใช้ข้อมูลไป ต่อมาเกิดเปลี่ยนใจ ก็สามารถยกเลิกความยินยอมนั้นเมื่อไหร่ก็ได้ โดยการยกเลิกจะต้องไม่ขัดต่อข้อจำกัดสิทธิในการถอนความยินยอมทางกฎหมายหรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคลที่ได้ให้ความยินยอมไปก่อนหน้านี้ เช่น เราสามารถขอ

ยกเลิกติดตามข่าวสารทางอีเมลของเว็บไซต์ได้ โดยกดที่ปุ่ม unsubscribe ที่แนบมาในอีเมล โดยการยกเลิกนี้ไม่ควรยุ่งยากซับซ้อน หรือต้องเสียค่าใช้จ่าย

4. สิทธิในการขอระงับการใช้ข้อมูล

เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลระงับการใช้ข้อมูลได้ ไม่ว่าจะในกรณีที่เกิดเปลี่ยนใจไม่ต้องการให้ข้อมูลแล้ว หรือเปลี่ยนใจระงับการทำลายข้อมูลเมื่อครบกำหนดที่ต้องทำลาย เพราะมีความจำเป็นต้องนำข้อมูลไปใช้ในทางกฎหมาย หรือการใช้สิทธิเรียกร้อง ก็สามารถทำได้

5. สิทธิในการเข้าถึง ขอสำเนา หรือให้เปิดเผยถึงการได้มาของข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตนเองจากผู้ควบคุมข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลที่ตัวเองอาจไม่แน่ใจว่าได้ให้ความยินยอมไปหรือไม่ โดยสิทธิการเข้าถึงข้อมูลนั้นต้องไม่ขัดต่อกฎหมายหรือคำสั่งศาล และการใช้สิทธินั้นต้องไม่ละเมิดสิทธิหรือเสรีภาพของบุคคลอื่น ซึ่งผู้ใช้งานเว็บไซต์อาจเข้าไปดูข้อมูลตนเองในบัญชีสมาชิกของตนเองได้ หรือร้องขอกับผู้ดูแลระบบได้

6. สิทธิในการขอรับและให้โอนย้ายข้อมูลส่วนบุคคล

ในกรณีที่เจ้าของข้อมูลต้องการให้ผู้ควบคุมข้อมูลส่วนบุคคลรายแรกโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมรายอื่น ก็สามารถขอให้ผู้ควบคุมรายแรกจัดทำข้อมูลที่อ่านได้ง่ายหรือจัดทำข้อมูลในรูปแบบที่เข้าถึงได้ด้วยวิธีการอัตโนมัติ และโอนไปยังผู้ควบคุมอีกรายได้ ซึ่งข้อมูลที่โอนไปนั้น เจ้าของข้อมูลสามารถขอรับข้อมูลนั้นจากผู้ควบคุมข้อมูลรายแรกได้ แต่การใช้วิธีการนี้จะต้องไม่ขัดต่อกฎหมาย สัญญา หรือละเมิดสิทธิเสรีภาพของผู้อื่น เช่น การย้ายพนักงานจากบริษัทหนึ่งไปยังอีกบริษัทหนึ่ง พนักงานสามารถใช้สิทธิให้บริษัทแรกโอนย้ายข้อมูลส่วนบุคคลไปยังบริษัทที่กำลังจะย้ายไปได้ รวมถึงขอรับสำเนาข้อมูลของตนเองได้

7. สิทธิในการขอคัดค้านการเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคลสามารถคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้ โดยร้องขอต่อผู้ควบคุมข้อมูลเมื่อไรก็ได้ โดยร้องขอผ่านแบบฟอร์มที่ผู้ให้บริการจัดไว้ หรือติดต่อกับผู้ดูแลระบบ

8. สิทธิในการขอให้ลบ หรือทำลายข้อมูลส่วนบุคคล

ในกรณีที่ข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ หรือผู้ควบคุมนำข้อมูลไปเผยแพร่ในที่สาธารณะ หรือข้อมูลนั้นสามารถเข้าถึงได้ง่าย เจ้าของข้อมูลมีสิทธิขอให้ผู้ควบคุมลบหรือทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนได้ โดยผู้ควบคุมข้อมูลต้องเป็นผู้รับผิดชอบค่าใช้จ่ายและการดำเนินการนั้น

9. สิทธิในการร้องเรียน

เจ้าของข้อมูลมีสิทธิร้องเรียนต่อพนักงานเจ้าหน้าที่และคณะกรรมการตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ ถ้าผู้ควบคุมข้อมูล ผู้ประมวลผลข้อมูล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้

ควบคุมข้อมูล ผู้ประมวลผลข้อมูล ฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย รวมถึงมีสิทธิในการเรียกค่าสินไหมทดแทนทางศาลด้วย

จะเห็นได้ว่า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ Personal Data Protection Act, B.E. 2562 เป็นกฎหมายว่าด้วยการให้สิทธิกับเจ้าของข้อมูลส่วนบุคคลเป็นอย่างมาก เพื่อให้เกิดความเชื่อมั่นว่าข้อมูลส่วนบุคคลของตนจะได้รับความคุ้มครอง ปลอดภัย และลดความเสี่ยงจากการถูกละเมิดข้อมูลส่วนบุคคลและอาจถูกนำข้อมูลส่วนบุคคลไปใช้ในทางที่มิชอบ

บทที่ 3
หลักกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลระหว่างประเทศ ต่างประเทศ เปรียบเทียบกฎหมายไทย

ในสภาพสังคมปัจจุบัน ความเป็นส่วนตัวที่เกี่ยวข้องกับข้อมูลเป็นสิ่งที่ประเทศส่วนใหญ่ให้ความสำคัญเป็นอย่างมาก ทั้งนี้ เนื่องจากความเจริญก้าวหน้าทางเทคโนโลยีสารสนเทศที่เป็นไปอย่างรวดเร็ว การรับรู้ข้อมูลข่าวสารต่าง ๆ จึงมีความสะดวกสบายมากขึ้น เมื่ออินเทอร์เน็ตได้เข้ามาเป็นสื่อที่มีบทบาทสำคัญในการติดต่อสื่อสารระหว่างกันและเป็นช่องทางหนึ่งที่ได้รับความนิยมอย่างแพร่หลาย ทำให้ในหลายกิจกรรมที่เกิดขึ้นล้วนแต่มีความเกี่ยวข้องกับอินเทอร์เน็ตทั้งสิ้น ส่งผลให้ภาคธุรกิจและการทำธุรกรรมต่าง ๆ บนอินเทอร์เน็ตเกิดขึ้นมากมาย ในแต่ละวันข้อมูลนับล้านถูกส่งผ่านเครือข่ายต่าง ๆ เพื่ออำนวยความสะดวกให้กับการทำธุรกรรมทางอิเล็กทรอนิกส์ แต่ในทางกลับกัน เมื่อข้อมูลต่าง ๆ สามารถเข้าถึงได้ง่าย ในบางครั้งอาจมีบุคคลหรือกลุ่มบุคคลที่นำข้อมูลเหล่านี้ไปใช้ เพื่อแสวงหาประโยชน์ โดยที่เจ้าของข้อมูลไม่ได้ให้ความยินยอม ส่งผลให้เกิดความเสียหายหรือสูญหายของข้อมูล หรืออาจถูกนำข้อมูลไปใช้ในทางที่ผิด ไม่ว่าจะโดยเจตนาหรือไม่เจตนาก็ตาม

การใช้สื่อสังคมออนไลน์ทำให้สามารถเชื่อมต่อกับบุคคลอื่นได้สะดวก และได้เรียนรู้เกี่ยวกับตนเองมากยิ่งขึ้น รวมถึงการพัฒนาชีวิตของผู้คนสังคม โดยมี The Quantified Self หรือกลุ่มซึ่งก่อตั้งขึ้นเพื่อสนับสนุนการใช้เทคโนโลยีติดตามตัวเพื่อให้ผู้คนรู้จักตนเอง เช่น การวัดวงจรการนอนในช่วงเวลาต่าง ๆ การวัดชีพจรของตนเอง ความชอบส่วนตัว เป็นต้น โดยข้อมูลเหล่านี้ก่อให้เกิดผลประโยชน์ที่มีมูลค่ามากสำหรับนายหน้าข้อมูล โดยนายหน้าข้อมูลจะดำเนินการจัดเก็บ และรวบรวมข้อมูลต่าง ๆ ของผู้บริโภคในฐานข้อมูล เพื่อดำเนินการนำข้อมูลเหล่านั้นไปแสวงหาผลประโยชน์ให้แก่ตนเองหรือกลุ่มบุคคล ในปัจจุบันประเทศไทยได้บัญญัติกฎหมายพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 หรือ Personal Data Protection Act, B.E. 2562 ออกมาเพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล โดยในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 หรือ Personal Data Protection Act, B.E. 2562 ได้กำหนดกรอบของผู้ควบคุมข้อมูล และผู้ประมวลผลข้อมูล ซึ่งเป็นบุคคลที่มีความสำคัญไม่น้อยกว่าเจ้าของข้อมูลส่วนบุคคล และนอกจากนี้ในต่างประเทศได้มีการบัญญัติกฎหมายออกมา เพื่อป้องกันการละเมิดข้อมูลส่วนบุคคลเช่นเดียว แต่ในการบัญญัติกฎหมายของแต่ละประเทศนั้น ขึ้นอยู่กับระบบกฎหมายของแต่ละประเทศในการที่จะบัญญัติกฎหมายออกมาเพื่อกำหนด จำกัด หรือป้องกันสิทธิของผู้คนในสังคม โดยในบทนี้จะกล่าวถึงหลักกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลระหว่างประเทศ ต่างประเทศ และกฎหมายไทย เพื่อนำมาเปรียบเทียบกฎหมายที่ออกมาเพื่อคุ้มครองข้อมูลส่วนบุคคลในแต่ละประเทศ

3.1 การคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายระหว่างประเทศ

3.1.1 สหภาพยุโรป (European Union)

สหภาพยุโรป (European Union) ปัจจุบันประกอบด้วยประเทศสมาชิก 27 รัฐสมาชิก ได้แก่ ออสเตรีย เบลเยียม เดนมาร์ก ฟินแลนด์ ฝรั่งเศส เยอรมนี กรีซ ไอร์แลนด์ อิตาลี ลักเซมเบิร์ก เนเธอร์แลนด์ โปรตุเกส สเปน สวีเดน สหราชอาณาจักร ไซปรัส เช็ก เอสโตเนีย ฮังการี ลัตเวีย ลิทัวเนีย มอลตา โปแลนด์ สโลวีเนีย สโลวะเกีย โรมาเนีย และบัลแกเรีย ก่อตั้งขึ้นจากการรวมกลุ่มระดับภูมิภาคของประเทศในทวีปยุโรป ที่รัฐสมาชิกให้ความเห็นชอบในการสละอำนาจอธิปไตยบางส่วนให้เป็นความร่วมมือเหนือชาติ (Supranational Cooperation) มีการจัดตั้งองค์กรที่มีอำนาจเหนือรัฐสมาชิกขึ้น 4 องค์กร ได้แก่ สหภาพยุโรป คณะมนตรียุโรป คณะกรรมาธิการยุโรป และศาลยุติธรรมแห่งสหภาพยุโรป โดยในส่วนที่เกี่ยวข้องกับการบังคับใช้กฎหมายมีศาลยุติธรรมแห่งสหภาพยุโรป (Court of Justice of the European Union: CJEU) ทำหน้าที่ตีความกฎหมายที่ใช้บังคับในสหภาพยุโรปเพื่อให้ประเทศสมาชิกสามารถนำกฎหมายดังกล่าวไปบังคับใช้ในรูปแบบเดียวกัน

โดยในสหภาพยุโรปมีคณะกรรมการ ซึ่งตั้งขึ้นเพื่อดูแลเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเป็นการเฉพาะ โดยกำหนดไว้ใน Article 29 Data Protection Working Party และกฎเกณฑ์สำคัญของ สหภาพยุโรปเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่จะกล่าวถึงต่อไป คือ Directive 2002/58 Directive 95/46/EC และ General Data Protection Regulation ความแตกต่าง ระหว่าง Directive และ Regulation คือ Regulation มีผลใช้บังคับเสมือนเป็นกฎหมายของประเทศสมาชิก โดยประเทศสมาชิกไม่จำต้องออกกฎหมายอนุวัติการตาม Regulation นี้ส่วน Directive เป็นกฎที่เสนอโดยคณะกรรมาธิการยุโรปและได้รับความเห็นชอบจากคณะมนตรีแห่งสหภาพยุโรป Directive นี้จะกำหนดกรอบการดำเนินงาน เพื่อให้ประเทศสมาชิกมีการปฏิบัติที่สอดคล้องกันโดยประเทศต่าง ๆ ต้องดำเนินการออกกฎหมายในเรื่องนั้น ๆ[1]

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

ในข้อกำหนด (ของสหภาพยุโรป) 2016/679 แห่งสภายุโรปและที่ประชุมยุโรป ลงวันที่ 27 เมษายน 2016 ว่าด้วยการคุ้มครองบุคคลธรรมดาในกรณีที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลและว่าด้วยการเคลื่อนย้ายข้อมูลดังกล่าวโดยเสรี และการยกเลิกคำสั่ง 95/46/EC (ข้อกำหนดทั่วไปว่าด้วยการคุ้มครองข้อมูล)[2] หรือ Directive 95/46/EC of the Protection of Personal นั้น ได้ใช้บังคับเมื่อวันที่ 24 ตุลาคม ค.ศ. 1995 บัญญัติขึ้นเพื่อเป็นแนวทางเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของ EU เพื่อกำหนดให้ประเทศสมาชิกให้ความคุ้มครองข้อมูลส่วนบุคคลในระดับที่เท่าเทียมกันในยุโรป Directive 95/46/EC นั้นนำมาบังคับใช้แก่การประมวลผลข้อมูลส่วนบุคคลทั้งหมดหรือบางส่วนโดยวิธีอัตโนมัติ แต่จะไม่นำมาบังคับใช้

[1] European commission, ‘legislation’, <http://ec.europa.eu/legislation/index_ en.html> Accedssed14 March 2016.

[2] นคร เสรีรักษ์, ผู้แปล, GDPR ภาษาไทย, 25-26

แก่การประมวลผลข้อมูลส่วนบุคคลซึ่งมิได้ตกอยู่ภายใต้กฎหมายแห่งประชาคมยุโรป Directive 95/46/EC ได้ให้ความหมายของคำต่าง ๆ ไว้ในมาตรา 2 ซึ่งมีสาระสำคัญ ดังต่อไปนี้

“ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลใด ๆ ที่เกี่ยวข้องกับบุคคลที่ถูกระบุตัวหรือ บุคคลที่อาจถูกระบุตัวได้ โดยบุคคลซึ่งถูกระบุตัวได้ คือ บุคคลที่สามารถถูกระบุตัวได้โดยตรงหรือโดยอ้อม โดยเฉพาะอย่างยิ่งจากการอ้างอิงโดยเลขบัตรประชาชน หรือปัจจัยหนึ่งหรือหลายปัจจัยซึ่งบ่งเฉพาะทางร่างกาย สรีรวิทยา จิตใจ เศรษฐกิจ วัฒนธรรม หรืออัตลักษณ์ทางสังคม

“การประมวลผลข้อมูลส่วนบุคคล” หมายถึง การดำเนินการต่างๆหรือชุดของการดำเนินการซึ่งกระทำต่อข้อมูลส่วนบุคคล ไม่ว่าจะเป็นไปโดยวิธีอัตโนมัติหรือไม่ก็ตาม เช่น การเก็บ รวบรวม การบันทึก การจัดระเบียบ การเก็บรักษา การเปลี่ยนแปลงหรือปรับปรุง การกู้คืน การใช้ การเปิดเผยโดยการส่ง การเผยแพร่หรือการทำให้สามารถเข้าถึงได้โดยประการอื่น การจัดหรือการรวม การปิดกั้น การลบหรือการทำลาย

“ผู้ควบคุม” หมายถึง บุคคลธรรมดาหรือนิติบุคคล หน่วยงานรัฐ ตัวแทนหรือ หรือบุคคลอื่นใดไม่ว่าโดยตนเองหรือโดยร่วมกับบุคคลอื่นกำหนดวัตถุประสงค์และวิธีในการประมวลผลข้อมูลส่วนบุคคล ในกรณีที่วัตถุประสงค์และวิธีในการประมวลผลข้อมูลส่วนบุคคลกำหนด โดยกฎหมายหรือกฎของประเทศหรือประชาคม ผู้ควบคุมข้อมูลส่วนบุคคลหรือหลักเกณฑ์เฉพาะ เพื่อการแต่งตั้งผู้ควบคุมข้อมูลให้กำหนดโดยกฎหมายของประเทศหรือประชาคม

“ความยินยอมของเจ้าของข้อมูลส่วนบุคคล” หมายถึง การแสดงเจตนาโดย อิสระมีลักษณะเฉพาะเจาะจงและบ่งบอกถึงวัตถุประสงค์ที่เจ้าของข้อมูลส่วนบุคคลแสดงถึงความ ยินยอมให้ทำการประมวลผลข้อมูลส่วนบุคคล

การบังคับใช้ Directive 95/46/EC กำหนดให้รัฐสมาชิกต้องนำบทบัญญัติแห่ง Directive นี้มาใช้บังคับแก่การประมวลผลข้อมูลส่วนบุคคลซึ่งผู้ควบคุมข้อมูลตั้งอยู่ในดินแดนของรัฐ สมาชิก ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลตั้งอยู่ในหลายดินแดนของรัฐสมาชิก ผู้ควบคุมข้อมูลต้อง ปฏิบัติตามกฎหมายของแต่ละประเทศด้วย หรือผู้ควบคุมข้อมูลส่วนบุคคลมิได้ตั้งอยู่ในดินแดนของรัฐสมาชิกแต่กฎหมายของรัฐสมาชิกนั้นถูกนำมาใช้บังคับต่อผู้ควบคุมข้อมูลส่วนบุคคล และในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลอยู่นอกดินแดนของสหภาพยุโรป แต่วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลใช้อุปกรณ์ อาจเป็นระบบอัตโนมัติหรือไม่ก็ตาม ซึ่งตั้งอยู่ในดินแดนแห่งรัฐสมาชิก เว้นแต่ อุปกรณ์นั้นใช้เพื่อวัตถุประสงค์ในการส่งข้อมูลข้ามดินแดนเท่านั้น ซึ่งในกรณีดังกล่าวผู้ควบคุมข้อมูลส่วนบุคคลต้องตั้งตัวแทนในดินแดนของรัฐสมาชิก

ประเภทของข้อมูลส่วนบุคคลตาม Directive 95/46/EC สามารถแบ่งออกได้ 2 ประเภท คือ ข้อมูลส่วนบุคคล และข้อมูลพิเศษ ซึ่งการประมวลผลข้อมูลพิเศษนี้ต้องเป็นไปตาม มาตรา 9 กล่าวคือ ห้ามทำการประมวลข้อมูลที่เปิดเผยเชื้อชาติ หรือแหล่งกำเนิดทางชาติพันธุ์ ความเห็นทางการเมือง ความเชื่อทางศาสนา ความเป็นสมาชิกของสหภาพแรงงาน และการประมวล ข้อมูลเกี่ยวกับสุขภาพหรือความประพฤติทางเพศ โดยมีข้อยกเว้น คือ ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่กฎหมายกำหนด

ห้ามมิให้เจ้าของข้อมูลส่วนบุคคลให้ความยินยอม หรือเป็นการจำเป็นในการปฏิบัติหน้าที่หรือสิทธิพิเศษของเจ้าของข้อมูลส่วนบุคคลในด้าน กฎหมายแรงงานตราบเท่าที่ไม่ขัดต่อกฎหมายของประเทศนั้น ๆ หรือเป็นการจำเป็น เพื่อปกป้องผลประโยชน์ที่สำคัญของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่นในกรณีที่เจ้าของข้อมูลไม่สามารถให้ความยินยอมได้ไม่ว่าทางกายภาพหรือทางกฎหมาย หรือการประมวลผลได้ทำขึ้นโดยชอบด้วยกฎหมายและมีหลักประกันที่เหมาะสมจากมูลนิธิ องค์กร หรือบุคคลซึ่งไม่แสวงหากำไร ซึ่งมีวัตถุประสงค์ในทางการเมือง ปรัชญา ศาสนา หรือสหภาพแรงงาน โดยการประมวลผลนั้นต้องเกี่ยวข้องกับสมาชิกของบุคคลหรือองค์นั้นเท่านั้น และข้อมูลต้องไม่ถูกเปิดเผยไปยังบุคคลที่สามโดย ไม่ได้รับความยินยอมจากเจ้าของข้อมูล หรือ การประมวลผลนั้นเป็นข้อมูลที่ถูกทำให้เป็นสาธารณะ โดยเจ้าของข้อมูลส่วนบุคคลหรือจำเป็นในการก่อตั้ง การใช้สิทธิหรือการต่อสู้คดี สำหรับในด้านของข้อมูลส่วนบุคคลการประมวลผลข้อมูลส่วนบุคคลจะสามารถกระทำได้ใน 6 กรณี คือ

1. ได้กระทำต่อเมื่อได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล

2. เป็นการจำเป็นเพื่อปฏิบัติตามสัญญา ซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาในสัญญานั้น หรือเป็นการปฏิบัติตามขั้นตอนก่อนมีการเข้าทำสัญญาโดยคำร้องขอของเจ้าของข้อมูลส่วนบุคคล

3. การประมวลผลเป็นการจำเป็นเพื่อปฏิบัติหน้าที่ตามกฎหมาย

4. การประมวลผลเป็นการจำเป็น เพื่อการปกป้องผลประโยชน์สำคัญของเจ้าของข้อมูลส่วนบุคคล

5. การประมวลผลจำเป็น เพื่อการปฏิบัติหน้าที่อันเป็นประโยชน์สาธารณะหรือเป็นการใช้อำนาจขององค์กรรัฐต่อผู้ควบคุมข้อมูลส่วนบุคคล หรือบุคคลที่สามซึ่งข้อมูลนั้นถูกเปิดเผย หรือ

6. การประมวลผลเป็นการจำเป็น เพื่อวัตถุประสงค์เกี่ยวกับผลประโยชน์ที่ชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือบุคคลที่สาม เว้นแต่ ประโยชน์นี้ทับซ้อนกับประโยชน์เกี่ยวกับสิทธิและเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล ซึ่งต้องได้รับการคุ้มครอง

มาตรา 6 กำหนดเรื่องคุณภาพของข้อมูลถูกกำหนดไว้โดยกำหนดให้ข้อมูลส่วนบุคคลต้องประมวลผลโดยชอบด้วยกฎหมายหรือเป็นธรรม การเก็บรวบรวมข้อมูลส่วนบุคคลต้องมีวัตถุประสงค์ที่ชัดแจ้งชอบด้วยกฎหมาย และต้องไม่ประมวลผลนอกเหนือจากวัตถุประสงค์ที่ระบุไว้ แต่การประมวลเพื่อประวัติศาสตร์ สถิติ หรือวิทยาศาสตร์ ไม่ถือเป็นการขัดกับวัตถุประสงค์หากรัฐสมาชิกมีหลักการคุ้มครองที่เพียงพอ ข้อมูลส่วนบุคคลนั้นต้องเกี่ยวข้องและไม่เกินความจำเป็นต่อวัตถุประสงค์ ซึ่งข้อมูลส่วนบุคคลนั้นถูกเก็บรวบรวมและ/หรือประมวลผลในภายหน้า นอกจากนี้ข้อมูลส่วนบุคคลนั้นต้องถูกต้องเป็นปัจจุบันและมีมาตรการเพื่อทำให้แน่ใจว่าข้อมูลที่ไม่ถูกต้องหรือไม่สมบูรณ์จะถูกทำลายหรือแก้ไขให้ถูกต้องหรือสมบูรณ์ และการเก็บรักษาข้อมูลนั้นต้องเก็บไว้เท่าระยะเวลาที่จำเป็นเพื่อการประมวลผลตามวัตถุประสงค์ที่ข้อมูลนั้นถูกเก็บรวบรวมมา เมื่อมีการเก็บรวบรวมข้อมูลส่วนบุคคลแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งแก่เจ้าของข้อมูลส่วนบุคคลว่าได้ข้อมูลนั้นมาจากบุคคลใด รวมทั้งต้องแจ้งถึงตัวผู้ควบคุมข้อมูลและตัวแทน(ถ้ามี) วัตถุประสงค์ในการประมวลข้อมูล และข้อมูลอื่น ๆ เช่น ผู้รับหรือประเภทของผู้รับข้อมูลส่วนบุคคล สิทธิในการเข้าถึงและ

แก้ไขข้อมูล หากข้อมูลส่วนบุคคลนั้นผู้ควบคุมข้อมูลส่วน บุคคลมิได้เก็บรวบรวมโดยตรงจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งเจ้าของข้อมูลส่วนบุคคลถึงตัวผู้ควบคุมข้อมูลส่วนบุคคลและตัวแทน (ถ้ามี) วัตถุประสงค์ในการประมวลผล ข้อมูล และข้อมูลอื่นๆ เช่น ประเภทของข้อมูล ประเภทหรือบุคคลที่จะได้รับข้อมูลนั้น

สิทธิในการเข้าถึงและสิทธิในการแก้ไขข้อมูลส่วนบุคคลสำหรับสิทธิของเจ้าของข้อมูลส่วนบุคคล Directive 95/46/EC ได้กำหนดไว้สองประการ ได้แก่ สิทธิในการเข้าถึงข้อมูลส่วนบุคคล และสิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล โดยสิทธิในการเข้าถึงข้อมูลส่วนบุคคลกำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิได้รับแจ้งจากผู้ควบคุมข้อมูลภายในเวลาอันควรโดยค่าใช้จ่ายไม่เกินสมควร ยืนยันถึงการมีอยู่ของข้อมูลส่วนบุคคล และการประมวลผลข้อมูลนั้น พร้อมทั้งบอกถึงวัตถุประสงค์ในการประมวลผล ประเภทของข้อมูลและบุคคลหรือประเภทของบุคคลที่ข้อมูลนั้นจะถูกเปิดเผย ซึ่งการแจ้งดังกล่าวต้องอยู่ในรูปแบบที่บุคคลนั้นสามารถเข้าใจได้ นอกจากนี้ Directive 95/46/EC ยังกำหนดสิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคลสามารถแบ่งออกได้สองกรณี คือ สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล และสิทธิในการคัดค้านการประมวลผลโดยระบบอัตโนมัติ สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล ให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลคัดค้านเรื่องความชอบด้วยกฎหมายในกรณีที่เกิดสถานการณ์พิเศษในการประมวลผลข้อมูลส่วนบุคคลของตนเมื่อข้อมูลส่วนบุคคลของตนถูกประมวลผล เพื่อประโยชน์สาธารณะหรือเกี่ยวกับประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลที่สาม และให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลคัดค้านในกรณีที่เห็นว่าการประมวลผลข้อมูลส่วนบุคคลนั้นทำเพื่อการตลาด โดยการคัดค้านนี้ต้องปราศจากค่าใช้จ่ายสำหรับสิทธิในการคัดด้านการประมวลผลโดยระบบอัตโนมัติ ให้สิทธิแก่เจ้าของข้อมูลคัดค้านการประมวลผลโดยระบบอัตโนมัติที่ก่อให้เกิดผลทางกฎหมายหรือ ส่งผลเสียต่อเจ้าของข้อมูลส่วนบุคคล หรือเป็นความเห็นของระบบอัตโนมัติเท่านั้น เช่น การประเมินความน่าเชื่อถือ ความประพฤติ หรือความสามารถในการทำงาน[3]

3.1.1.2 General Data Protection Regulation

General data Protection Regulation (GDPR) เป็นกฎเกณฑ์ของสหภาพยุโรป ซึ่งจะถูกนำมาบังคับใช้แทน Directive 95/46/EC on the Protection of Personal Data ความคิดในการแก้ไขกฎหมายคุ้มครองข้อมูลส่วนบุคคลเริ่มต้นขึ้นเมื่อวันที่ 25 มกราคม ค.ศ. 2012 โดย GDPR มีวัตถุประสงค์เพื่อเพิ่มความคุ้มครองแก่เจ้าของข้อมูลส่วนบุคคล ซึ่งเป็นปัจเจกบุคคลให้เจ้าของข้อมูลส่วนบุคคลสามารถควบคุมข้อมูลของตนได้ นอกจากนี้ GDPR นำมาบังคับใช้แก่การประมวลผลข้อมูลส่วนบุคคลซึ่งเป็นระบบอัตโนมัติด้วย ทั้งยังมีบทบัญญัติเกี่ยวกับการโอนข้อมูลส่วนบุคคลไปนอกสหภาพยุโรป

---

[3] อธิพร สิทธิธีรรัตน์, ‘ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลในบริบทอิเล็คทรอนิกส์’ (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ 2558) 76-79.

ขอบเขตการบังคับใช้ GPDR ได้ถูกกำหนดไว้ในมาตรา 3 โดยให้นำมาใช้บังคับกับการประมวลผลข้อมูลส่วนบุคคลซึ่งกระทำ โดยผู้ควบคุมข้อมูลส่วนบุคคลที่ตั้งอยู่ในสหภาพยุโรป หรือ ใช้กับการประมวลผลข้อมูลส่วนบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลนั้นอยู่ในสหภาพยุโรป หรือแม้ตัวผู้ควบคุมข้อมูลส่วนบุคคลจะมิได้ตั้งอยู่ในดินแดนของรัฐสมาชิกในสหภาพยุโรปแต่มีการประมวลผล ข้อมูลเพื่อเสนอขายสินค้าหรือบริการให้แก่เจ้าของข้อมูลส่วนบุคคลที่อยู่ในดินแดนแห่งรัฐสมาชิกของสหภาพยุโรปไม่ว่าการเสนอขายสินค้าหรือบริการนั้นจะมีค่าใช้จ่ายหรือไม่ก็ตาม หรือเป็นการสังเกต พฤติกรรมของเจ้าของข้อมูลส่วนบุคคล ซึ่งพฤติกรรมนั้นเกิดขึ้นในดินแดนแห่งรัฐสมาชิกของสหภาพยุโรป หรือในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่ตกอยู่ภายใต้บังคับแห่ง GDPR ในกรณีทั้งหมดที่กล่าว มาแต่บทบัญญัติว่าด้วยกฎหมายขัดกันให้นำ GDPR มาใช้ ผู้ควบคุมข้อมูลส่วนบุคคลนั้นต้องปฏิบัติ ตาม GDPR ด้วย[4]

ซึ่ง GDPR ครอบคลุมถึง “ผู้ควบคุมข้อมูลส่วนบุคคล” หรือ “ผู้ประมวลผลข้อมูลส่วนบุคคล” มีสถานประกอบการอยู่ภายในสหภาพยุโรป “ผู้ควบคุมข้อมูลส่วนบุคคล” หรือ “ผู้ประมวลผลข้อมูลส่วนบุคคล” ไม่มีสถานประกอบการอยู่ภายในสหภาพยุโรป แต่การประมวลผลนั้นเกี่ยวข้องกับการเสนอสินค้าหรือบริการให้แก่บุคคลผู้พำนักในสหภาพยุโรป “ผู้ควบคุมข้อมูลส่วนบุคคล” หรือ “ผู้ประมวลผลข้อมูลส่วนบุคคล” ไม่มีสถานประกอบการอยู่ภายในสหภาพยุโรป แต่การประมวลผลนั้นเกี่ยวข้องกับการเฝ้าสังเกตพฤติกรรมที่เกิดขึ้นในสหภาพยุโรป ทั้งนี้ หากมีการประมวลผลข้อมูลส่วนบุคคลนอกอาณาเขตของสหภาพยุโรป และประเทศนั้นมีผลผูกพันทางกฎหมายกับประเทศสหภาพยุโรป เช่น สนธิสัญญา จะตกอยู่ภายใต้ขอบเขตการบังคับใช้ของ GDPR เช่นเดียวกัน

สหภาพยุโรปได้ออกคำสั่งคุ้มครองข้อมูลที่ 95/46/EC เพื่อใช้บังคับกับการจัดการข้อมูลส่วนบุคคลภายในสหภาพยุโรป ซึ่งมีความสำคัญมากต่อนโยบาย และกฎหมายเรื่องสิทธิมนุษยชน คำสั่งนี้ได้ออกมาใช้อย่างสมบูรณ์ในปี ค.ศ.1995 โดยมติของสภาสหภาพยุโรปเอง โดยใน GDPR ได้ให้คำนิยาม สำหรับ “ข้อมูลส่วนบุคคล” “ผู้ควบคุม” และ“ผู้ประมวลผล” ไว้ในมาตรา 4 ดังนี้

“ข้อมูลส่วนบุคคล” หมายถึง “ข้อมูลส่วนบุคคล” หมายถึงข้อมูลสารสนเทศใดๆก็ตามที่ สัมพันธ์กับบุคคลธรรมดาที่ถูกระบุหรือสามารถถูกระบุอัตลักษณ์ได้ (“ผู้ถูกประมวลผลข้อมูล”) บุคคลธรรมดาที่สามารถถูกระบุอัตลักษณ์ได้ คือบุคคลที่สามารถถูกระบุอัตลักษณ์ได้ไม่ว่าจะโดยตรงหรือโดยอ้อม โดยเฉพาะอย่างยิ่งด้วยการอ้างอิงจากสิ่งระบุอัตลักษณ์เป็นการเฉพาะ เช่น ชื่อ หมายเลขประจำตัว ข้อมูลสถานที่ สิ่งระบุอัตลักษณ์ออนไลน์ หรือปัจจัยอย่างหนึ่งหรือมากกว่าที่เจาะจงไปยังอัตลักษณ์ทางกายภาพ กายวิทยา พันธุกรรม จิตใจ เศรษฐกิจ วัฒนธรรม หรือสังคมของบุคคล ธรรมดานั้น[5]

“ผู้ควบคุม” หมายถึง บุคคลธรรมดาหรือนิติบุคคล หน่วยงาน สาธารณะที่มีอำนาจ หรือองค์กรใดที่กำหนดวัตถุประสงค์และวิธีการ ประมวลผลข้อมูลส่วนบุคคล ไม่ว่าจะโดยลำพังหรือร่วมกัน โดยที่

---

[4] เพิ่งอ้าง. 79.

[5] นคร เสรีรักษ์ (เชิงอรรถ 2) 101.

วัตถุประสงค์และวิธีการในการประมวลผลดังกล่าวถูกกำหนดโดยกฎหมายของสหภาพหรือรัฐสมาชิก ผู้ควบคุมหรือเกณฑ์เฉพาะสำหรับ การแต่งตั้งตัวแทนผู้ควบคุมอาจถูกกำหนดไว้โดยกฎหมายของสหภาพ หรือรัฐสมาชิก[6]

“ผู้ประมวลผล” หมายถึง บุคคลธรรมดาหรือนิติบุคคล หน่วยงานสาธารณะที่มีอำนาจ หน่วยงานหรือองค์กรอื่นใดที่ประมวล ผลข้อมูลส่วนบุคคลในนามของผู้ควบคุม[7]

“ผู้รับ” หมายถึง บุคคลธรรมดาหรือนิติบุคคล หน่วยงาน สาธารณะที่มีอำนาจ หน่วยงาน หรือองค์กรอื่นใดที่เข้าถึงการเปิดเผย ข้อมูลส่วนบุคคล ไม่ว่าจะเป็นบุคคลที่สามหรือไม่ก็ตาม อย่างไรก็ดี หน่วยงานสาธารณะที่มีอำนาจอาจได้รับข้อมูลส่วนบุคคลภายใต้กรอบ การทำงานของการไต่สวนบางประการโดยเป็นไปตามกฎหมายของสหภาพหรือรัฐสมาชิกจะไม่ถูกพิจารณาว่าเป็นผู้รับการประมวลผลข้อมูลดังกล่าว โดยหน่วยงานสาธารณะที่มีอำนาจจะต้องเป็นไปตามกฎในการคุ้มครองข้อมูลทั้งหมดที่บังคับใช้กับวัตถุประสงค์ของการประมวลผลนั้นได้[8]

โดยคำจำกัดความนี้เป็นความหมายอย่างกว้างมาก ข้อมูลที่เป็นข้อมูลส่วนบุคคลนั้น ได้แก่ การที่ข้อมูลใด ๆ ที่สามารถเชื่อมต่อข้อมูลไปยังอีกบุคคลหนึ่งได้ หรือแม้จะไม่สามารถเชื่อมต่อไปยังบุคคลนั้นได้ก็ตาม เช่น ที่อยู่ หมายเลขบัตรเครดิต รายการบัญชี บันทึกคดีอาญา เป็นต้น

ข้อมูลส่วนบุคคลไม่ควรจะถูกจัดเก็บใด ๆ เว้นแต่มีเงื่อนไขที่แน่นอน ซึ่งเงื่อนไขเหล่านั้นต้องอยู่ภายใต้หลักการ 3 ประการ คือ

หลักความโปร่งใส (Transparency) เนื้อหาในข้อมูลของแบบฟอร์มในการดำเนินการนั้น ต้องปรากฏสิทธิแก่เจ้าของข้อมูล โดยผู้ควบคุมต้องกำหนดชื่อ ที่อยู่ วัตถุประสงค์ในการดำเนินการข้อมูลของผู้รับและข้อมูลใด ๆ ที่ถูกเรียกร้องให้แสดงถึงความชอบธรรมในการดำเนินการด้วย

การจำกัดวัตถุประสงค์ (Legitimate purpose) ข้อมูลส่วนบุคคลสามารถดำเนินการจัดเก็บเพื่อการเจาะจงอย่างเปิดเผย และการจำกัดวัตถุประสงค์นี้ ไม่อาจดำเนินการเกินไปถึงลักษณะที่ขัดแย้งต่อวัตถุประสงค์เหล่านั้น

ความได้สัดส่วน (Proportionality) ข้อมูลส่วนบุคคลอาจดำเนินการเพียงเท่าที่เหมาะสม และสัมพันธ์กัน และไม่เกินกว่าวัตถุประสงค์ที่เกี่ยวข้องกับการจัดเก็บ หรือเกินกว่าการดำเนินการนั้น ข้อมูลดังกล่าวต้องมีความถูกต้องแม่นยำ และจำเป็นที่จะต้องปรับปรุง เพราะเหตุผลทุกอย่างต้องแน่ใจว่าเป็นข้อมูลที่ไม่ผิดพลาด หรือไม่สมบูรณ์ ด้วยความเคารพต่อวัตถุประสงค์ในการจัดเก็บนั้น หรือเพื่อทำให้ไม่เกินขอบเขตดังกล่าว ด้วยการลบล้าง หรือถูกทำลาย ข้อมูลจะไม่ถูกเก็บรักษาโดยความยินยอมไว้เป็นเวลานานเกินกว่า

---

[6] นคร เสรีรักษ์ (เชิงอรรถ 2) 102-103.

[7] นคร เสรีรักษ์ (เชิงอรรถ 2) 103.

[8] เพิ่งอ้าง.

ความจำเป็นตามวัตถุประสงค์ในการจัดเก็บ โดยประเทศสมาชิกจะต้องมีวิธีการป้องกันที่เหมาะสมในการจัดเก็บข้อมูลส่วนบุคคลในระยะยาวเพื่อการใช้ในเชิงประวัติศาสตร์

เนื้อหาในข้อมูลบางครั้งอาจมีเป้าหมายการจัดเก็บข้อมูลส่วนบุคคลสำหรับวัตถุประสงค์เพื่อการขายตรงได้ (มาตรา 14) (Article The data subject may object at any time to the processing of personal data for the purpose of direct marketing)

GDPR ได้กำหนดความหมายของคำสำคัญต่าง ๆ ไว้ ดังนี้ “ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งสามารถถูกระบุตัวได้หรือ อาจถูกระบุตัวได้ ไม่ว่าโดยทางตรงหรือทางอ้อมจากข้อมูลนั้น โดยเฉพาะอย่างยิ่งจากการอ้างอิงจาก สิ่งพิสูจน์เอกลักษณ์ เช่น ชื่อ เลขบัตรประจำตัวประชาชน ข้อมูลที่อยู่ เอกลักษณ์ทางออนไลน์ หรือ เอกลักษณ์อย่างใดอย่างหรือหลายอย่างเกี่ยวกับร่างกาย สรีรวิทยา พันธุกรรม จิตใจ เศรษฐกิจ วัฒนธรรมหรือสังคมของบุคคลนั้น

“การจำกัดการประมวลผล” หมายถึง การทำเครื่องหมายข้อมูลส่วนบุคคลที่ได้รับมาโดยมีวัตถุประสงค์เพื่อจำกัดการประมวลผลในอนาคต [9]

“การปกปิดอัตลักษณ์ (pseudonymisation)” หมายถึง การประมวลผลข้อมูลส่วนบุคคลในลักษณะที่ข้อมูลส่วนบุคคลไม่สามารถ ระบุเจาะจงไปยังผู้ถูกประมวลผลคนใดคนหนึ่งหากไม่มีการใช้ข้อมูลเพิ่มเติม ด้วยเงื่อนไขว่าข้อมูลเพิ่มเติมดังกล่าวจะถูกเก็บแยกจากกันและ อยู่ภายใต้การควบคุมโดยมาตรการทางเทคนิคและการจัดการองค์กรที่จะรับประกันว่าข้อมูลเพิ่มเติมดังกล่าวถูกเก็บรักษาแยกจากกัน และ อยู่ภายใต้มาตรการทางเทคนิคและการจัดการองค์กรที่จะรับประกันว่า ข้อมูลส่วนบุคคลจะไม่ถูกใช้บ่งชี้ไปถึงบุคคลธรรมดาที่ถูกระบุอัตลักษณ์ หรือสามารถถูกระบุอัตลักษณ์ได้ [10]

“ข้อมูลพันธุกรรม” หมายถึง ข้อมูลส่วนบุคคลที่สัมพันธ์กับคุณลักษณะทางพันธุกรรมที่สืบทอดกันมาหรือเกิดขึ้นภายหลัง ซึ่งให้ข้อมูลลักษณะพิเศษเฉพาะเกี่ยวกับกายวิทยาหรือสุขภาพของบุคคลธรรมดานั้น และโดยเฉพาะอย่างยิ่งเป็นผลจากการวิเคราะห์ตัวอย่างทางชีววิทยาของบุคคลธรรมดาที่ถูกกล่าวถึง

“ข้อมูลไบโอเมตริก (Biometric)” หมายถึง ข้อมูลส่วนบุคคลเกิดจากการประมวลผลโดยใช้เทคนิคเฉพาะเกี่ยวกับกายภาพ หรือความประพฤติของบุคคลนั้น ซึ่งทำให้บ่งชี้ลักษณะเฉพาะของบุคคล เช่น รูปหน้า หรือ ลายนิ้วมือ[11]

“การทำโพรไฟล์” หมายถึงรูปแบบใด ๆ ก็ตามของการประมวลผลข้อมูลส่วนบุคคลที่ประกอบด้วยการใช้ประโยชน์จากข้อมูล ส่วนบุคคลในการประเมินบางแง่มุมส่วนบุคคลที่สัมพันธ์กับบุคคลธรรมดา หนึ่ง ๆ โดยเฉพาะอย่างยิ่งเพื่อวิเคราะห์หรือคาดการณ์ในแง่ที่เกี่ยวข้อง กับประสิทธิภาพในการ

---

[9] นคร เสรีรักษ์ (เชิงอรรถ 2) 102.

[10] เพิ่งอ้าง.

[11] นคร เสรีรักษ์ (เชิงอรรถ 2) 104.

ทำงาน สถานภาพทางเศรษฐกิจ สุขภาพ ความชอบส่วนบุคคล ความสนใจ ความเชื่อถือได้อุปนิสัย สถานที่หรือ การเคลื่อนไหวของบุคคลธรรมดานั้น ๆ[12]

GDPR ได้แบ่งข้อมูลส่วนบุคคลออกเป็น 2 ประเภท ได้แก่ ข้อมูลส่วนบุคคล และ ข้อมูลพิเศษ ซึ่งข้อมูลส่วนบุคคลได้แก่ข้อมูลทั่วไปเกี่ยวกับบุคคลผู้เป็นเจ้าของข้อมูลส่วนบุคคล ซึ่งมีหลักเกณฑ์ในการเก็บรวบรวม ใช้ หรือเปิดเผยแตกต่างไปจากข้อมูลที่มีลักษณะพิเศษซึ่งจะกล่าวต่อไป โดยข้อมูลที่มีลักษณะพิเศษนี้เป็นข้อมูลซึ่งมีความอ่อนไหว GDPR กำหนดให้ห้ามทำการประมวลผลข้อมูลที่เปิดเผยถึง เชื้อชาติ แหล่งกำเนิดชาติพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนา หรือปรัชญา การเป็นสมาชิกสภาพแรงงาน และการประมวลผลข้อมูลเกี่ยวกับพันธุกรรมและข้อมูลไบโอเมตริก (Biometric) หรือข้อมูลเกี่ยวกับสุขภาพหรือพฤติกรรมทางเพศ โดยมีข้อยกเว้น 10 ประการ คือ

1. เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมโดยชัดแจ้ง เว้นแต่การให้ความยินยอมนั้นต้องห้ามโดยกฎหมาย

2. การประมวลผลเป็นการจำเป็นเพื่อวัตถุประสงค์ในการปฏิบัติตามหน้าที่หรือ ใช้สิทธิเฉพาะเจาะจงของผู้ควบคุมข้อมูลส่วนบุคคล หรือของเจ้าของข้อมูลส่วนบุคคลเกี่ยวกับการจ้างงาน ประกันสังคม ทั้งนี้ เฉพาะที่ชอบด้วยกฎหมายของประเทศนั้น ๆ

3. การประมวลผลจำเป็นในการปกป้องประโยชน์ของเจ้าของข้อมูลส่วนบุคคล หรือของบุคคลอื่นในกรณีที่เจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมทางทางกายภาพ หรือตามกฎหมายได้

4. การประมวลผลนั้นเป็นกิจกรรมที่ชอบด้วยกฎหมายและมีมาตรการป้องกัน โดยองค์กร สมาคม หรือบุคคลซึ่งไม่แสวงหากำไร โดยมีวัตถุประสงค์ในทางการเมือง ปรัชญา ศาสนา หรือสหภาพแรงงาน ภายใต้เงื่อนไขว่าต้องเป็นการประมวลผลข้อมูลของสมาชิกหรือบุคคลที่เคยเป็นสมาชิกและไม่เปิดเผยข้อมูลนั้น

5. เป็นข้อมูลส่วนบุคคลที่ถูกเปิดเผยไว้เป็นสาธารณะโดยเจ้าของข้อมูลส่วนบุคคล

6. การประมวลผลนั้นจำเป็นเพื่อการก่อตั้ง การใช้สิทธิหรือการต่อสู้คดี หรือเป็นการปฏิบัติหน้าที่ของศาล

7. การประมวลผลนั้นจำเป็นเพื่อวัตถุประสงค์ในทางประโยชน์สาธารณะโดย ประเทศต้องมีมาตรการป้องกันประโยชน์ของเจ้าของข้อมูลด้วย

8. การประมวลผลนั้นจำเป็นเพื่อวัตถุประสงค์ทางการแพทย์

9. การประมวลนั้นจำเป็นเพื่อประโยชน์สาธารณะเกี่ยวกับสุขภาพของประชาชน เช่น การป้องกันอันตรายร้ายแรงที่ข้ามพรมแดนหรือเพื่อให้มีมาตรฐานความปลอดภัยและคุณภาพทางสาธารณสุขที่สูง

10. การประมวลผลจำเป็นเพื่อประโยชน์สาธารณะ เช่น ประวัติศาสตร์ สถิติ วิทยาศาสตร์ โดยมีมาตรการป้องกันความปลอดภัยของรัฐ

---

[12] นคร เสรีรักษ์ (เชิงอรรถ 2) 102.

และในการประมวลผลข้อมูลเกี่ยวกับความผิดอาญา GDPR ได้กำหนดให้สามารถกระทำได้ โดยองค์กรของรัฐ ซึ่งต้องมีมาตรการป้องกันความปลอดภัยด้วย

ในเรื่องของการประมวลผลข้อมูลส่วนบุคคล GDPR กำหนดให้การเก็บรวบรวมผู้ควบคุมข้อมูลส่วนบุคคลต้องทำโดยระบุวัตถุประสงค์ที่ชัดแจ้งและชอบด้วยกฎหมาย ซึ่งวัตถุประสงค์ดังกล่าวต้องพอเหมาะเกี่ยวข้องและไม่เกินสมควรเมื่อพิจารณาถึงวัตถุประสงค์ในการประมวลผล ข้อมูลส่วนบุคคลและต้องนำข้อมูลส่วนบุคคลไปใช้ตามวัตถุประสงค์นั้น เว้นแต่เป็นการประมวลผลข้อมูลส่วนบุคคล เพื่อวัตถุประสงค์สาธารณะหรือวิทยาศาสตร์ หรือวัตถุประสงค์ทางประวัติศาสตร์ การประมวลผลต้องทำโดยชอบด้วยกฎหมาย เป็นธรรมและโปร่งใส และมีมาตรการรักษาความ ปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม ผู้เก็บรวบรวมข้อมูลส่วนบุคคลต้องทำให้ข้อมูลนั้น ถูกต้อง เป็นปัจจุบัน และทำทุกวิถีทางเพื่อให้ข้อมูลส่วนบุคคลที่ไม่ถูกต้องถูกลบหรือแก้ไขโดยไม่ชักช้า ทั้งนี้ เมื่อพิจารณาถึงวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล การเก็บรักษาข้อมูลส่วนบุคคลที่ยังสามารถแสดงให้เห็นตัวเจ้าของข้อมูลจะต้องทำเพียงเท่าเวลาที่จำเป็น เพื่อวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลนั้นเท่านั้น ภายใต้มาตรา 6 กำหนดให้การประมวลจะถือว่าชอบด้วยกฎหมายในกรณีใด กรณีหนึ่งดังต่อไปนี้

1. เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมโดยชัดแจ้งในการประมวลผล ข้อมูลส่วนบุคคล เพื่อวัตถุประสงค์หนึ่งหรือหลายวัตถุประสงค์

2. การประมวลผลเป็นการจำเป็น เพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนการเข้าทำสัญญา

3. การประมวลผล เพื่อการปฏิบัติตามหน้าที่ตามกฎหมาย

4. การประมวลผลเป็นการจำเป็น เพื่อปกป้องผลประโยชน์สำคัญของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่น

5 . การประมวลเป็นการจำเป็น เพื่อการปฏิบัติภารกิจอันเกี่ยวกับสาธารณประโยชน์หรือเป็นการใช้อำนาจรัฐเหนือผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าว ทับซ้อนกับประโยชน์หรือสิทธิเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคลซึ่งได้รับการคุ้มครอง ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะอย่างยิ่งเมื่อเจ้าของข้อมูลส่วนบุคคลเป็นเด็ก

การประมวลผลในภายภาคหน้าต้องสอดคล้องกับวัตถุประสงค์ที่ทำการเก็บ รวบรวมข้อมูลส่วนบุคคล ซึ่งจะสอดคล้องกับวัตถุประสงค์หรือไม่นั้น ผู้ควบคุมข้อมูลส่วนบุคคลต้องพิจารณาตามกรณีดังต่อไปนี้ เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

1. มีความเชื่อมโยงระหว่างวัตถุประสงค์ที่ข้อมูลนั้นถูกเก็บรวบรวม และ วัตถุประสงค์ที่จะทำการประมวลผลต่อไป

2. บริบทที่ข้อมูลส่วนบุคคลถูกเก็บรวบรวม

3. ลักษณะของข้อมูลส่วนบุคคลที่จะทำการประมวลผลโดยเฉพาะอย่างยิ่งข้อมูลที่มีลักษณะพิเศษ

4. ผลที่อาจเกิดจากการประมวลที่จะทำต่อไปอันจะส่งผลต่อเจ้าของข้อมูลส่วนบุคคล

5. มีมาตรการป้องกันที่เหมาะสม

อย่างไรก็ตามหากข้อมูลส่วนบุคคลที่จะทำการประมวลผลต่อไปขัดกับวัตถุประสงค์ในตอนแรกที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคล โดยผู้ควบคุมข้อมูลส่วนบุคคลคนเดียวกัน การประมวลผลต่อไปนั้นอย่างน้อยต้องมีหลักการตามที่กล่าวมาอย่างน้อยหนึ่งข้อ การประมวลผลเพื่อประโยชน์ของผู้ควบคุมข้อมูลส่วนบุคคล หรือบุคคลที่สามซึ่งขัดกับวัตถุประสงค์ในตอนแรกจะถือว่าชอบด้วยกฎหมายต่อเมื่อประโยชน์นั้นสำคัญกว่าประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

สำหรับการให้ความยินยอม GDPR ได้กำหนดไว้ในมาตรา 7 โดยในกรณีที่มีการประมวลผลข้อมูลส่วนบุคคลและข้อมูลลักษณะพิเศษภายใต้ความยินยอมของเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลต้องสามารถแสดงว่าเจ้าของข้อมูลส่วนบุคคลมีการให้ความยินยอมโดยชัดแจ้ง ในกรณีที่ความยินยอมต้องทำเป็นลายลักษณ์อักษรซึ่งมีเรื่องอื่น ๆ รวมอยู่ด้วย การขอความยินยอมต้องแยกออกมาอย่างเด่นชัดจากเรื่องอื่น ๆ และอยู่ในรูปแบบที่สามารถเข้าใจได้ เข้าถึงได้ง่าย และใช้ภาษาที่ง่ายและชัดเจน นอกจากนี้เจ้าของข้อมูลส่วนบุคคลมีสิทธิเพิกถอนความยินยอมไม่ว่าในเวลาใด ๆ โดยการเพิกถอนนั้นจะไม่กระทบความชอบด้วยกฎหมายในการประมวลผลข้อมูลก่อนมีการเพิกถอนความยินยอม ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งสิทธิในการเพิกถอนความยินยอมแก่เจ้าของข้อมูลด้วย

ในด้านการประมวลผลข้อมูล Pseudonymous หากการประมวลผลข้อมูลนั้นไม่จำเป็นต้องระบุตัวเจ้าของข้อมูลส่วนบุคคลอีกต่อไป ผู้ควบคุมข้อมูลส่วนบุคคลต้องไม่เก็บรักษา หรือหาข้อมูลเพิ่มเติมหรือไม่จำต้องประมวลผลเพิ่มเติมเพียง เพื่อจะปฏิบัติตามกฎเกณฑ์ฉบับนี้ หากผู้ควบคุมข้อมูลส่วนบุคคลได้ทำการหาข้อมูลเพิ่มเติมก่อให้สามารถระบุตัวเจ้าของข้อมูลส่วนบุคคลได้ เจ้าของข้อมูลส่วนบุคคลนั้นมีสิทธิตามที่กำหนดไว้ในกฎเกณฑ์นี้ เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถควบคุมข้อมูลของตนเองได้ โดย GDPR ได้ กำหนดสิทธิของเจ้าของข้อมูลส่วนบุคคลไว้หลายประการ ดังนี้

สิทธิในการขอเข้าถึงข้อมูลส่วนบุคคล

สิทธิดังกล่าวกำหนดไว้ในมาตรา 15 กำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิ ได้รับการยืนยันจากผู้ควบคุมข้อมูลส่วนบุคคลภายในเวลาอันสมควรโดยไม่มีค่าใช้จ่ายแสดงว่าข้อมูล ส่วนบุคคลนั้นได้ถูกประมวลผลหรือไม่ได้ถูกประมวลผลที่ใด และมีสิทธิเข้าถึงข้อมูล ดังต่อไปนี้

1. วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล

2. ผู้รับหรือบุคคลที่ข้อมูลนั้นอาจถูกเปิดเผย โดยเฉพาะอย่างยิ่งผู้รับซึ่งอยู่ในประเทศที่สามหรือเป็นองค์การระหว่างประเทศ

3. หากเป็นไปได้ให้บอกระยะเวลาในการเก็บรักษาข้อมูลนั้น

4. สิทธิในการขอให้แก้ไขหรือลบข้อมูลส่วนบุคคลหรือสิทธิในการคัดค้านการประมวลผล

5. สิทธิในการร้องเรียนต่อเจ้าหน้าที่

6. ในกรณีที่ข้อมูลนั้นมิได้ได้รับมาโดยตรงจากเจ้าของข้อมูลส่วนบุคคล ต้องบอกถึงที่มาของข้อมูลนั้น

7. ในกรณีที่มีการตัดสินใจโดยระบบอัตโนมัติ รวมถึงการทำ Profiling ต้องบอกข้อมูลที่เป็นเหตุผลที่เกี่ยวข้อง รวมถึงผลที่อาจเกิดจากการประมวลผลด้วย

สิทธิในการแก้ไขข้อมูลส่วนบุคคล

ในกรณีที่ข้อมูลส่วนบุคคลนั้นไม่ถูกต้องหรือไม่เป็นปัจจุบัน เจ้าของข้อมูลมีสิทธิร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการแก้ไขข้อมูลให้ถูกต้องโดยไม่ชักช้า โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งการแก้ไขให้แก่บุคคลอื่นซึ่งข้อมูลส่วนบุคคลนั้นถูกเปิดเผย เว้นแต่ไม่สามารถกระทำได้หรือเป็นการใช้ความพยายามเกินสมควร

สิทธิในการขอให้ลบข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ในการลบข้อมูลโดยไม่ชักช้า โดยเฉพาะข้อมูลที่เก็บรวบรวมในขณะที่เจ้าของข้อมูลส่วนบุคคลเป็นเด็ก และเจ้าของข้อมูลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลลบข้อมูลในกรณีดังต่อไปนี้ด้วย

1. ข้อมูลนั้นไม่จำเป็นอีกต่อไป เมื่อพิจารณาถึงวัตถุประสงค์ที่ทำการเก็บรวบรวมหรือ

2. เจ้าของข้อมูลส่วนบุคคลเพิกถอนความยินยอมและไม่มีพื้นฐานกฎหมาย รองรับการประมวลผลอีกต่อไปหรือ

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

4. ข้อมูลถูกประมวลผลโดยไม่ชอบด้วยกฎหมายหรือ

5. ข้อมูลนั้นจำเป็นต้องถูกลบ เพื่อปฏิบัติตามกฎหมายที่ควบคุมผู้ควบคุม ข้อมูลส่วนบุคคล เมื่อเจ้าของข้อมูลส่วนบุคคลขอใช้สิทธิแล้วผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้ง การขอใช้สิทธิลบข้อมูลให้แก่บุคคลอื่น ซึ่งข้อมูลส่วนบุคคลนั้นถูกเปิดเผย เว้นแต่ไม่สามารถกระทำได้ หรือเป็นการใช้ความพยายามเกินสมควร

สิทธิในการยับยั้งการประมวลผลข้อมูลส่วนบุคคล

สิทธิดังกล่าวกำหนดไว้ในมาตรา 17a ให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิได้รับการยังยั้งการประมวลผลข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลใน 3 กรณี กล่าวคือ

1. เจ้าของข้อมูลส่วนบุคคลคัดค้านความถูกต้องของข้อมูลส่วนบุคคล กรณีเช่นนี้ผู้ควบคุมข้อมูลส่วนบุคคลต้องยับยั้งการประมวลผลข้อมูลนั้นภายในกำหนดเวลาสำหรับการตรวจสอบความถูกต้องของข้อมูลนั้น หรือ

2. ผู้ควบคุมข้อมูลส่วนบุคคลไม่จำเป็นต้องมีข้อมูลส่วนบุคคลนั้นเพื่อการประมวลผลแต่เป็นการจำเป็นสำหรับเจ้าของข้อมูลเพื่อการก่อตั้ง ใช้สิทธิ หรือต่อสู้คดี หรือ

3. เป็นกรณีที่เจ้าของข้อมูลส่วนบุคคลคัดค้านวัตถุประสงค์ของการประมวลผลตามมาตรา 19(1) ผู้ควบคุมข้อมูลส่วนบุคคล ต้องยับยั้งการประมวลข้อมูลนั้นจนกระทั่งมีการยืนยันว่าเหตุผลอันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลเหนือกว่าเจ้าของข้อมูลส่วนบุคคล โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งการจำกัดการประมวลผลให้แก่บุคคลอื่น ซึ่งข้อมูลส่วนบุคคลนั้นถูกเปิดเผย เว้นแต่ไม่สามารถกระทำได้ หรือเป็นการใช้ความพยายามเกินสมควร

4. สิทธิในการโอนข้อมูลส่วนบุคคล (Right to data portability) สิทธิดังกล่าวก่อให้เจ้าของข้อมูลส่วนบุคคลสามารถรับข้อมูลเกี่ยวกับตน ซึ่งได้ให้ไว้แก่ผู้ควบคุมข้อมูลส่วนบุคคลในรูปแบบที่เป็นแบบแผน ใช้งานได้ และสามารถอ่านได้โดยเครื่อง (machine-readable) และมีสิทธิที่จะโอนข้อมูลนั้นไปยังผู้ควบคุมข้อมูลอื่น เว้นแต่การประมวลผลนั้นเป็นความยินยอมของเจ้าของข้อมูลส่วนบุคคล หรือเป็นไปตามสัญญา หรือเป็นการประมวลผลโดยวิธีอัตโนมัติ แต่หากการใช้สิทธินี้นำมาซึ่งการละเมิดลิขสิทธิ์ในการประมวลผลข้อมูลส่วนบุคคล เจ้าของข้อมูลส่วนบุคคลไม่สามารถใช้นี้ได้

5. สิทธิในการคัดค้าน สิทธิดังกล่าวกำหนดไว้ในมาตรา 19 ให้เจ้าของบุคคลมีสิทธิคัดค้านเมื่อมีสถานการณ์พิเศษต่อเจ้าของข้อมูลส่วนบุคคลในการประมวลผลข้อมูลส่วนบุคคลที่เป็นการจำเป็น เพื่อการปฏิบัติภารกิจอันเกี่ยวกับสาธารณประโยชน์หรือเป็นการใช้อำนาจรัฐเหนือผู้ควบคุมข้อมูลส่วนบุคคล หรือเป็นการประมวลผลซึ่งจำเป็น โดยมีวัตถุประสงค์เพื่อประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือบุคคลที่สาม โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องไม่ประมวลผลข้อมูลนั้น เว้นแต่แสดงได้ว่ามีกฎหมายบังคับซึ่งเหนือกว่าประโยชน์หรือสิทธิเสรีภาพของเจ้าของของมูล เพื่อการก่อตั้ง ใช้สิทธิ หรือการต่อสู้คดี หากข้อมูลส่วนบุคคลนั้นถูกประมวลผล เพื่อการตลาด เจ้าของข้อมูลมีสิทธิคัดค้านและหากมีการคัดค้าน ดังนั้นแล้วผู้ควบคุมข้อมูลส่วนบุคคลต้องไม่ประมวลผลต่อไป ในกรณีที่ข้อมูลส่วนบุคคลนั้นถูกประมวลผล เพื่อวัตถุประสงค์ทางประวัติศาสตร์ สถิติ หรือวิทยาศาสตร์ เจ้าของ ข้อมูลส่วนบุคคลมีสิทธิคัดค้านได้ เว้นแต่การประมวลผลนั้นจำเป็นเพื่อประโยชน์สาธารณะ

6. สิทธิเกี่ยวกับการตัดสินใจโดยวิธีอัตโนมัติ บทบัญญัติเกี่ยวกับการตัดสินใจโดยวิธีอัตโนมัติถูกกำหนดไว้ในมาตรา 20 เป็นการคุ้มครองเจ้าของข้อมูลมิให้ตกอยู่ภายใต้การตัดสินใจโดยระบบอัตโนมัติเพียงอย่างเดียว ซึ่งรวมถึงการทำ Profiling โดยเฉพาะอย่างยิ่งเมื่อการประมวลผลนั้นอาจทำให้เกิดผลทางกฎหมายอย่าง มีนัยสำคัญแก่บุคคลดังกล่าว อย่างไรก็ตามการตัดสินใจโดยวิธีอัตโนมัตินี้มีข้อยกเว้น 3 กรณีคือ

(1) เป็นการจำเป็นเพื่อการเข้าทำสัญญาหรือการปฏิบัติตามสัญญาระหว่าง เจ้าของข้อมูลส่วนบุคคล และผู้ควบคุมข้อมูลส่วนบุคคล

(2) ได้รับอนุญาตตามกฎหมายของสหภาพยุโรปหรือกฎหมายของรัฐสมาชิก ซึ่งต้องมีมาตรการคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลที่เหมาะสม

(3) เป็นการกระทำภายใต้ความยินยอมโดยแจ้งของเจ้าของข้อมูลส่วนบุคคล[13]

---

[13] อธิพร สิทธิธีรรัตน์ (เชิงอรรถ 4) 79-86.

ให้คำนิยามข้อมูลส่วนบุคคลไว้ว่า คือ ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม รวมถึงข้อมูลที่นำมารวมกันแล้วสามารถใช้ระบุอัตลักษณ์ของบุคคลได้ ซึ่ง GDPR ได้ให้คำจำกัดความและหน้าที่ของบทบาทของผู้เกี่ยวข้องกับการประมวลผลข้อมูลหลักไว้ 3 บทบาท ดังนี้

ผู้ควบคุมข้อมูลส่วนบุคคล (Controller) คือ กำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูล ซึ่งโดยส่วนมากจะเป็นผู้ขอความยินยอมจากเจ้าของข้อมูล เช่น ผู้ให้บริการเว็บไซต์ต่าง ๆ รวมไปถึงบุคคล นิติบุคคล องค์กรหรือหน่วยงานรัฐ

ผู้ประมวลผลข้อมูลส่วนบุคคล (Processor) คือ ผู้ประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์และวิธีการของผู้ควบคุมข้อมูลส่วนบุคคล ในทางปฏิบัติอาจเป็นบุคคลเดียวกับผู้ควบคุมข้อมูลส่วนบุคคลก็ได้ อนึ่ง “การประมวลผลข้อมูล” (Processing) ตามกฎหมาย GDPR นั้น ไม่ใช่เพียงแค่การวิเคราะห์ หรือ จัดการข้อมูลแบบทั่วไปเท่านั้น แต่ให้รวมถึงการบันทึกและจัดเก็บข้อมูลด้วย

เจ้าของข้อมูลส่วนบุคคล (Data Subject) คือ ข้อมูลใด ๆ อันเกี่ยวข้องกับบุคคลธรรมดาที่ระบุตัวตนหรืออาจระบุตัวตนได้

การคุ้มครองข้อมูลตามกฎหมายคุ้มครองข้อมูลในต่างประเทศส่วนใหญ่ จะครอบคลุมประเด็นเกี่ยวกับอำนาจควบคุมเหนือข้อมูลในการรวบรวม และการนำข้อมูลไปใช้ประโยชน์มากกว่าที่จะมองว่าข้อมูลอยู่ที่ใด หรืออยู่ในการครอบครองของใคร เพราะโดยลักษณะและความสามารถอันแทบไร้ข้อจำกัดของระบบคอมพิวเตอร์ ที่สามารถครอบครองและควบคุมการเคลื่อนไหวของข้อมูลจากที่หนึ่งไปยังอีกที่หนึ่งได้อย่างง่ายและรวดเร็ว ซึ่งในกฎหมายการคุ้มครองของนานาประเทศอาจมีมาตรฐานการคุ้มครองข้อมูลที่ไม่เท่าเทียมกัน ถึงแม้ว่าจะไม่สามารถกำหนดรูปแบบของขอบเขตการคุ้มครองให้ได้มาตรฐานเดียวกันในทุกประเทศ ในภาพรวมของบทบัญญัติกฎหมายทั้งหลายนี้ ตั้งอยู่บนพื้นฐานเดียวกัน

3.1.2 องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD)

องค์การเพื่อความร่วมมือและการพัฒนาทางเศรษฐกิจ The Organization for Economic Cooperation and Development (OECD) ก่อตั้งขึ้นเมื่อปี พ.ศ. 2504 ได้จัดทำคู่มือในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลที่เรียกว่า Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data แรกเริ่มประกอบไปด้วยประเทศสมาชิกทั้งหมด 20 ประเทศซึ่งส่วนใหญ่เป็นประเทศที่พัฒนาแล้ว เป็นองค์กรระหว่างประเทศที่ส่งเสริมการประสานงานด้านนโยบายและเสรีภาพทางเศรษฐกิจในหมู่ประเทศที่พัฒนาแล้ว OECD มาจากองค์การเพื่อความร่วมมือทางเศรษฐกิจยุโรป Organisation for European Economic Co-operation (OEEC) ซึ่งก่อตั้งขึ้นในปี พ.ศ. 2491 เพื่อติดตามผลงานของอเมริกาและแคนาดาภายใต้แผนมาร์แชล OECD มีสำนักงานใหญ่อยู่ที่กรุงปารีส ประเทศฝรั่งเศส ก่อตั้งขึ้นในปี พ.ศ. 2504 และรวมสมาชิกจากรัฐประชาธิปไตย เช่น สหรัฐอเมริกา ประเทศในยุโรปตะวันตก ญี่ปุ่น แคนาดา ออสเตรเลีย และนิวซีแลนด์

ภารกิจหลักของ OECD คือ กระตุ้นการเจริญเติบโตทางเศรษฐกิจและการค้าโลก และเป็นเวทีในการเปรียบเทียบนโยบาย แลกเปลี่ยนประสบการณ์ และประสานงานนโยบายทั้งในประเทศและระหว่างประเทศสมาชิก ซึ่งรวมถึงการปราบปรามการค้าผิดกฎหมายด้วยเช่นกัน ปัจจุบัน ประเทศสมาชิกของ OECD มีทั้งหมด 31 ประเทศทั่วโลก ตั้งแต่อเมริกาเหนือและใต้ไปจนถึงยุโรปและเอเชียแปซิฟิก เป็นตัวแทนของทูตที่สภา OECD ซึ่งกำหนดและดูแลงานตามที่กำหนดไว้ในอนุสัญญา OECD

ในระดับกฎหมายระหว่างประเทศนั้น องค์การความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD) ได้กำหนดแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและการส่งผ่านข้อมูลส่วนบุคคลระหว่างประเทศ เพื่อเป็นแนวทางในการบัญญัติกฎหมายภายในของประเทศต่าง ๆ แนวทางของ OECD จัดว่าเป็นหลักการคุ้มครองข้อมูลส่วนบุคคลชุดแรกที่กำหนดขึ้นในกรอบของความตกลงระหว่างประเทศ[14] ในปี ค.ศ. 1980 องค์การเพื่อความร่วมมือทางด้านเศรษฐกิจและการพัฒนา (The organization for economic and development) ได้กำหนด Guideline governing the protection of privacy and transporter data flow of personal data ซึ่งเป็นหลักการขั้นพื้นฐานในการให้ความคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในรูปแบบอิเล็กทรอนิกส์ที่หลายประเทศต่างยอมรับ โดยมีสาระสำคัญคือข้อมูลส่วนบุคคลต้องได้รับความคุ้มครองที่เหมาะสมในทุกขั้นตอน ตั้งแต่การเก็บรวบรวม การใช้ การเก็บรักษา และการเปิดเผย

แนวทางในการคุ้มครองข้อมูลส่วนบุคคลและการส่งข้อมูลข้ามพรหมแดนขององค์การเพื่อความร่วมมือทางเศรษฐกิจและพัฒนา (OECD) ได้ให้คำนิยามคำว่า “ข้อมูลส่วนบุคคล” ไว้ว่าหมายถึงข้อมูลใด ๆ อันระบุตัวหรือสามารถระบุถึงตัวบุคคลได้

บทบัญญัติที่เกี่ยวกับการส่งหรือโอนข้อมูลไปต่างประเทศ มิได้เป็นบทบัญญัติที่ปรากฏอยู่ใน OECD Guideline ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล แต่เป็นบทบัญญัติที่ปรากฏใน EU Directive ซึ่งบัญญัติขึ้นในปี ค.ศ. 1995 ดังนั้น จึงเป็นที่น่าสังเกตว่ากฎหมายของประเทศที่ออกก่อนปี ค.ศ. 1995 โดยที่ไม่ได้มีการแก้ไขเพิ่มเติมภายหลังจึงไม่มีบทบัญญัติในเรื่องนี้ ปรากฏอยู่ในกฎหมาย เช่น กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศนิวซีแลนด์ ในขณะที่กฎหมายที่ออกภายหลังปี ค.ศ. 1995 แม้จะมิใช่ประเทศสมาชิกสหภาพยุโรป แต่ได้บัญญัติหลักการดังกล่าวไว้ด้วย เช่น กฎหมายคุ้มครองความเป็นอยู่ส่วนตัวของเครือรัฐออสเตรเลียหรือกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศฮ่องกง เป็นต้น

จากการศึกษาหลักการสำคัญของการคุ้มครองข้อมูลส่วนบุคคลตามหลักการขององค์กรระหว่างประเทศระหว่างสหภาพยุโรปและข้อตกลงรัฐสภายุโรป และองค์การเพื่อความร่วมมือทางด้านเศรษฐกิจและการพัฒนา (OECD) นั้น สามารถสรุปได้ดังนี้

---

[14] คณาทิป ทองรวีวงศ์, *การปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทย เพื่อเข้าสู่ประชาคมอาเซียน* (วิจัยจากสำนักงานเลขาธิการสภาผู้แทนราษฎร) 42.

หลักการจัดเก็บอย่างจำกัดชอบด้วยกฎหมายและเป็นธรรม กล่าวคือ ผู้ที่มีหน้าที่ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลและต้องกระทำอย่างจำกัดเท่าที่จำเป็น ข้อมูลที่จัดเก็บจะต้องได้มาโดยวิธีการที่ชอบด้วยกฎหมาย เป็นธรรม และเหมาะสม โดยเจ้าของข้อมูลจะต้องรับทราบและให้ความยินยอม

หลักการจัดเก็บอย่างมีคุณภาพ ถูกต้องและได้สัดส่วน กล่าวคือ การเก็บรวบรวมข้อมูลส่วนบุคคลจะต้องกระทำด้วยความถูกต้องแม่นยำ โดยข้อมูลที่จะจัดเก็บต้องเป็นข้อมูลที่ถูกต้องสมบูรณ์ มีการปรับปรุงข้อมูลให้ตรงตามความเป็นจริง และทันสมัยอยู่ตลอดเวลาที่มีการประมวลผลและใช้ข้อมูลนั้น ๆ อีกทั้งต้องจัดเก็บให้สอดคล้อง พอเพียงและได้สัดส่วนกับวัตถุประสงค์ นอกจากนี้จะต้องจัดเก็บเท่าที่เกี่ยวข้อง จำเป็น ไม่เกินจริง และไม่ล่วงล้ำหรือก้าวก่ายกิจการส่วนตัวของบุคคลที่เกี่ยวข้อง

หลักการกำหนดวัตถุประสงค์และระยะเวลาในการจัดเก็บ กล่าวคือ จะต้องมีการกำหนดวัตถุประสงค์ในการจัดเก็บและเงื่อนไขของการใช้ ก่อนที่จะมีการจัดเก็บข้อมูลนั้น ๆ ต้องแจ้งวัตถุประสงค์ให้เจ้าของข้อมูลได้ทราบก่อนทำการรวบรวมข้อมูล การใช้ข้อมูลส่วนบุคคลในภายหลังสามารถกระทำได้เพื่อให้สำเร็จตามวัตถุประสงค์ หรือเพื่อการอื่นที่ไม่ขัดหรือแย้งกับวัตถุประสงค์ ในกรณีเช่นนี้จะต้องระบุวัตถุประสงค์การใช้ที่เปลี่ยนแปลงไปนั้นทุกคราว ส่วนระยะเวลาการจัดเก็บและใช้ข้อมูลส่วนบุคคลสามารถกระทำได้ภายในระยะเวลาพอสมควรและเท่าที่จำเป็น แต่จะต้องไม่เกินกว่าระยะเวลาเพื่อให้บรรลุตามวัตถุประสงค์ที่ระบุไว้

หลักการใช้ข้อมูลอย่างจำกัด กล่าวคือ จะต้องใช้ข้อมูลส่วนบุคคลภายในกรอบวัตถุประสงค์ที่ได้ระบุไว้โดยไม่มีการเปิดเผย เข้าถึง ให้แพร่หลาย หรือใช้เพื่อการอื่น นอกเหนือจากวัตถุประสงค์ที่ระบุและได้แจ้งให้เจ้าของข้อมูลทราบก่อนหน้านั้น เว้นแต่ ได้รับอนุญาตจากบุคคลผู้เป็นเจ้าของข้อมูลอาศัยอำนาจตามกฎหมายเพื่อประโยชน์ในการป้องกันรักษาความมั่นคงของชาติ ความสงบเรียบร้อยของสังคม ประโยชน์สาธารณะ เพื่อรักษากฎหมายหรือเพื่อประโยชน์มหาชนอื่น ๆ

นอกจากนี้บุคคลใดจะนำข้อมูลส่วนบุคคลของบุคคลอื่นไปเปิดเผยโดยเจ้าของข้อมูลไม่ยินยอมไม่ได้ หากเจ้าของข้อมูลไม่อนุญาตให้เปิดเผย ไม่ว่าการเปิดเผยนั้นจะทำให้เจ้าของข้อมูลเสียหายหรือไม่ก็ตามถือเป็นการละเมิดสิทธิในความเป็นอยู่ส่วนตัวทั้งสิ้น แม้เจ้าของข้อมูลจะได้อนุญาตแล้วก็ยังคงมีสิทธิขอให้เลิกการเผยแพร่ข้อมูลส่วนบุคคลได้ทุกเมื่อ

หลักการรักษาความปลอดภัย กล่าวคือ ผู้จัดเก็บครอบครองหรือควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีมาตรการรักษาความปลอดภัยในการจัดเก็บข้อมูลส่วนบุคคลอย่างเพียงพอ เพื่อมิให้ข้อมูลส่วนบุคคลเสี่ยงต่อการเข้าถึง สูญหายหรือเสียหายโดยเหตุสุดวิสัย การทำลายโดยบุคคลอื่น โดยธรรมชาติหรือโดยไวรัสคอมพิวเตอร์ การใช้ การแก้ไขเปลี่ยนแปลงหรือการเปิดเผยโดยปราศจากอำนาจ และในกรณีที่ต้องให้บันทึกข้อมูลส่วนบุคคลแก่บุคคลอื่นต้องดำเนินการป้องกันมิให้บุคคลอื่นนั้นได้ใช้ข้อมูลส่วนบุคคลโดยปราศจากอำนาจ

หลักเปิดเผยโปร่งใส กล่าวคือ จะต้องมีการประกาศนโยบายในการประมวลผลข้อมูลส่วนบุคคลเพื่อให้บุคคลที่เกี่ยวข้องทราบถึงกระบวนการจัดเก็บ รวบรวม นำไปใช้ นอกจากนี้ จะต้องมีการแสดงให้เห็นถึง

ความมีอยู่และประเภทของข้อมูลส่วนบุคคล วัตถุประสงค์ของการใช้ข้อมูลส่วนบุคคล ตลอดจนชื่อ สถานที่จัดตั้ง และรายละเอียดของผู้ที่ทำหน้าที่เก็บรักษาข้อมูล ผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูลให้เจ้าของข้อมูลทราบ

หลักการมีส่วนร่วมของเจ้าของข้อมูล กล่าวคือ การเก็บรวบรวมของข้อมูลส่วนบุคคลต้องสอดคล้องกับสิทธิของเจ้าของข้อมูลส่วนบุคคล และจะต้องมีส่วนร่วมในการจัดเก็บข้อมูลนั้น ๆ โดยเจ้าของข้อมูลจะมีสิทธิ ดังต่อไปนี้

ต้องได้รับการแจ้งหรือคำยืนยันจากผู้เก็บรักษาข้อมูลหรือผู้ควบคุมข้อมูลว่าได้ทำการจัดเก็บประมวลผลใช้ หรือส่ง โอนข้อมูลส่วนบุคคลของตนหรือไม่

หากมีการจัดเก็บข้อมูลส่วนบุคคลของตน จะต้องได้รับติดต่อจากผู้จัดเก็บข้อมูลภายในระยะเวลาที่เหมาะสม โดยปราศจากค่าธรรมเนียม แต่หากมีการเก็บค่าธรรมเนียมจะต้องไม่สูงจนเกินไป และโดยวิธีการที่เหมาะสม นอกจากนี้ การจัดเก็บจะต้องอยู่ในรูปแบบที่สามารถเข้าถึงได้ง่าย

หลักการไม่เลือกปฏิบัติ กล่าวคือ การจัดเก็บหรือรวบรวมข้อมูลส่วนบุคคลจะต้องไม่ทำให้เกิดการเลือกปฏิบัติต่อบุคคลที่แตกต่างกัน เช่น ข้อมูลที่เกี่ยวกับเชื้อชาติ เผ่าพันธุ์ สีผิว พฤติกรรมทางเพศ ความคิดเห็นทางการเมือง หรือความเชื่ออื่นใด ๆ รวมถึงความเป็นสมาชิกสหภาพการค้า เป็นต้น ข้อมูลดังกล่าวเป็นข้อมูลส่วนบุคคลประเภทที่เรียกว่า “Sensitive Data (ข้อมูลส่วนบุคคลที่มีผลกระทบต่อความรู้สึก ข้อมูลส่วนบุคคลที่ต้องให้ความสำคัญเป็นพิเศษ ข้อมูลละเอียดอ่อน)” อาจกล่าวได้ว่า เป็นหลักการที่ห้ามมิให้จัดเก็บข้อมูลส่วนบุคคลประเภทที่กระทบต่อความรู้สึก

หลักข้อจำกัดในการส่งหรือโอนข้อมูลส่วนบุคคล กล่าวคือ หลักการนัดกำหนดห้ามมิให้มีการส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศที่มิได้มีบทบัญญัติในการให้ความคุ้มครองข้อมูลส่วนบุคคลในระดับที่เท่าเทียมกันในสาระสำคัญ เว้นแต่ ได้รับความยินยอมจากเจ้าของข้อมูลหรือจำเป็น เพื่อชำระหนี้ตามความผูกพันที่เป็นผลของสัญญา หรือทำเพื่อประโยชน์ของบุคคลซึ่งไม่สามารถให้ความยินยอมได้

หลักความรับผิดชอบ กล่าวคือ ผู้จัดเก็บข้อมูล ผู้ครอบครองข้อมูลหรือ ผู้ประมวลผลข้อมูลจะต้องมีความรับผิดชอบในการปฏิบัติตามหลักการหรือมาตรการต่างๆข้างต้นให้ครบถ้วนทุกประการอย่างเคร่งครัด หากมีการฝ่าฝืนหรือละเลยมีผลให้เกิดความเสียหายแก่ข้อมูลส่วนบุคคล ผู้จัดเก็บข้อมูล ผู้ครอบครองข้อมูลหรือผู้ประมวลผลข้อมูลจะต้องรับผิดทั้งทางแพ่งและทางอาญา นอกจากนี้ ยังจะต้องรับผิดค่าใช้จ่ายที่เกิดขึ้นเพื่อกระทำการแก้ไขข้อมูลให้ถูกต้อง ลบหรือทำลายข้อมูลส่วนบุคคล รวมทั้งเยียวยาความเสียหายแล้วแต่กรณี

แม้หลักการ OECD จะเป็นหลักการที่ประเทศส่วนใหญ่ยอมรับและนำไปบัญญัติเป็นกฎหมายภายในประเทศของตนก็ตาม แต่การปรับใช้หลักการต่าง ๆ เหล่านี้กับข้อเท็จจริงที่เกิดขึ้นก็ความหมายต่างกันและต้องอาศัยหลักการและเหตุผลพื้นฐานอื่น ๆ มาประกอบการตัดสินใจเสมอ เพราะกฎหมายการคุ้มครองข้อมูลส่วนบุคคลมิใช่เป็นแต่เพียงหลักการกำหนดหลักเกณฑ์กลาง เพื่อให้ทุกคนปฏิบัติเท่านั้น ซึ่งการจะปรับใช้

ยังคงต้องชั่งน้ำหนักประโยชน์ได้เสียระหว่างบุคคลทุกฝ่ายที่เกี่ยวข้องอย่างเหมาะสม ไม่ให้เกิดกรณีที่เข้มงวดเกินไป หรือหละหลวมจนไม่สามารถคุ้มครองสิทธิของประชาชนได้[15]

3.2 การคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายต่างประเทศ

3.2.1 ประเทศสหรัฐอเมริกา

ประเทศสหรัฐอเมริกา เป็นประเทศที่ปกครองแบบสหพันธรัฐ จึงมีลักษณะเหมือนกับมีอำนาจอธิปไตยสองอันซ้อนกันอยู่ กล่าวคือ อำนาจอธิปไตยในแต่ละมลรัฐ และอำนาจอธิปไตยของสหรัฐ ซึ่งเป็นอำนาจที่ได้รับมอบจากทุกมลรัฐที่มารวมกันเป็นสหรัฐ ดังนั้น ในแต่ละรัฐย่อมมีอำนาจที่จะจัดตั้งศาลของตนเองขึ้นมา เพื่อบริหารงานยุติธรรมภายในเขตมลรัฐของตนเอง ในระดับสหรัฐ หรือรัฐบาลกลางก็มีการจัดตั้งศาลของรัฐบาลกลาง ซึ่งมีเขตอำนาจ ตามที่รัฐธรรมนูญของสหรัฐ และตามกฎหมายอื่นที่ตราขึ้น โดยรัฐสภาของสหรัฐ กฎหมายที่สำคัญ ได้แก่ รัฐบัญญัติงานยุติธรรมฉบับแรก (Judiciary Act 1789) ได้มีแนวคิดทางกฎหมายของประเทศสหรัฐอเมริกาในการคุ้มครองสิทธิส่วนบุคคลนั้น มีพัฒนาการมาจากบทความเรื่อง “The Right to Privacy” โดย Warren และ Brandies ซึ่งได้ให้ความหมายของสิทธิในความเป็นอยู่ส่วนตัวว่าหมายถึง “สิทธิที่จะอยู่โดยลำพัง” (The Right to be Let Alone) ปราศจากการรบกวน กล่าวคือ บุคคลย่อมมีสิทธิที่จะไม่ถูกสังเกต รู้เห็น สืบความลับ รวมทั้งมีสิทธิที่จะอยู่โดยปราศจากการแทรกแซงจากสังคม[16] หลังจากบทความดังกล่าว สิทธิในความเป็นอยู่ส่วนตัวในระบบกฎหมายสหรัฐอเมริกาได้รับการพัฒนาต่อเนื่องมา โดย William L. Prosser ได้ขยายความการละเมิดสิทธิในความเป็นส่วนตัวออกไป โดยแบ่งออกเป็น 4 ประเภท[17] ได้แก่ การแทรกแซงความสันโดษของผู้อื่น การแสวงหาประโยชน์จากชื่อหรือลักษณะของผู้อื่น โดยมิได้รับความยินยอม การเปิดเผยเรื่องราวส่วนตัวของผู้อื่นต่อสาธารณะ และการเผยแพร่ซึ่งทำให้ผู้อื่นเสื่อมเสียในสายตาของสาธารณะชน ซึ่งศาลในสหรัฐอเมริกาได้นำหลักดังกล่าวมาใช้ในการพิจารณาคดีในบริบทของกฎหมายลักษณะละเมิด (Privacy Tort)[18]

ในสหรัฐอเมริกามีหน่วยงานด้านความมั่นคงของสหรัฐอเมริกาที่ดำเนินการเก็บรวบรวมข้อมูลส่วนตัวและการดำเนินกิจกรรมทางดิจิทัลต่าง ๆ ของผู้คน นอกจากนี้ยังมีระบบที่สามารถสร้างปัญหาได้เช่นกัน

---

[15] ปิยะพร วงศ์เบี้ยสัจจ์, ‘การเปิดเผยข้อมูลส่วนบุคคลโดยธนาคารพาณิชย์กับมาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคล’ (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ปรีดี พนมยงค์ มหาวิทยาลัยธุรกิจบัณฑิตย์ 2552) 111.

[16] Warren, D, Samual and Brandies, D, Louis. (1890). The Right to Privacy. Harvard Law Review, Vol IV December15,1890, [Online]. Available: http://www.lawrence.edu/fast/boardmaw.

[17] William L. Prosser, Handbook of the law of torts,4 ed. (St.Paul, Minn. West Publishing Co 1971). 804-814.

[18] คณาธิป ทองรวีวงศ์, ‘ปัญหากฎหมายเกี่ยวกับการคุ้มครองสิทธิส่วนบุคคลของบุคคลสาธารณะ:กรณีศึกษาเปรียบเทียบกฎหมายสหรัฐอเมริกาและกฎหมายไทย’ (1 มิถุนายน 2558) 7 วารสารวิชาการ คณะนิติศาสตร์ มหาวิทยาลัยหอการค้าไทย 204.

เช่น บริษัทการตลาด โฆษณา และธุรกิจเหมืองข้อมูล (data mining) บริษัทเอกชนจะดำเนินการจัดเก็บข้อมูลส่วนตัวอย่างเป็นระบบ มีทั้งวิธีการจัดเก็บข้อมูลจากสมาชิกห้างสรรพสินค้าไปจนถึงการโฆษณาที่เจาะจงไปยังกลุ่มเป้าหมายโดยตรง มีการรวบรวมข้อมูลส่วนตัวของผู้คนทั้งออนไลน์และออฟไลน์เข้าไว้ด้วยกัน จากนั้นจะนำข้อมูลมาวิเคราะห์แล้วดำเนินการขายให้กับนักการตลาด บริษัทต่าง ๆ รัฐบาล และอาชญากร เป็นต้น แต่ในการดำเนินการนั้นยังไม่มีการควบคุมการทำงานของบริษัทขายข้อมูลต่าง ๆ ซึ่งอาจกล่าวได้ว่ามีการเก็บข้อมูลส่วนบุคคล 2 แบบ ได้แก่ การรวบรวมข้อมูลโดยบริษัทเอกชนซึ่งเจ้าของข้อมูลไม่เต็มใจ และการรวบรวมเก็บข้อมูลที่เจ้าของข้อมูลสมัครใจ

อุตสาหกรรมการรวบรวมและซื้อขายข้อมูลเป็นที่รู้จักกันดีในชื่อ “นายหน้าข้อมูล” เป็นการทำการตลาดด้วยฐานข้อมูล บริษัท Acxiom เป็นบริษัทที่ใหญ่เป็นอันดับสอง เป็นเจ้าของเซิร์ฟเวอร์คอมพิวเตอร์ 23,000 เครื่องที่ประมวลผลข้อมูลมากกว่า 50 ล้านล้านข้อมูลต่อปี บริษัทยังอ้างว่ามีบันทึกหลายร้อยล้านข้อมูลของคนอเมริกันซึ่งรวมทั้ง 11,000 ข้อมูลคุกกี้ (ข้อมูลชิ้นเล็กๆ ที่ส่งจากเว็บไซต์ และถูกใช้เพื่อสะกดรอยกิจกรรมของผู้ใช้) ประวัติการใช้โทรศัพท์โดยเฉลี่ยแล้วมักมีการเก็บข้อมูลประมาณ 1,500 รายการต่อผู้บริโภคหนึ่งคน ข้อมูลเหล่านี้มีทั้งข้อมูลที่หาได้ทั่วไปในที่สาธารณะ เช่น การประเมินราคาบ้าน การเป็นเจ้าของยานพาหนะต่าง ๆ ข้อมูลพฤติกรรมออนไลน์ที่ติดตามได้จากคุกกี้ ข้อมูลจากการทำแบบสอบถามของลูกค้า และ พฤติกรรมการซื้อสินค้า “ออฟไลน์” ในช่วงที่สก็อตต์ ฮาว์ (Scott Howe) ได้ดำรงตำแหน่งผู้บริหารระดับสูงของบริษัท ได้กล่าวว่า “อีกไม่นานพวกเราจะเข้าถึงข้อมูลดิจิทัลของผู้ใช้อินเทอร์เน็ตเกือบทั้งหมดในสหรัฐอเมริกา”

บริษัท Acxiom มีบริการ “ข้อมูลพฤติกรรมเชิงลึกแบบพิเศษที่ครอบคลุมความสนใจของผู้บริโภคหลายหมื่นคน และจัดลำดับความชื่นชอบของยี่ห้อสินค้า และช่องทางที่เชื่อมโยงกับการใช้สินค้าและช่วงเวลาในการซื้อได้” ในอีกทางหนึ่ง Acxiom ได้สร้างประวัติ และแฟ้มรวบรวมเอกสารดิจิทัลของผู้ใช้หลายล้านคน โดยใช้ข้อมูล 1,500 จุดของข้อมูลที่เกี่ยวข้องกับผู้คน ซึ่งข้อมูลเหล่านี้อาจจะรวมถึง ข้อมูลบุตร ประวัติการซื้อขายหุ้น ประวัติการซื้อสินค้า สัญชาติ อายุ และระดับการศึกษาของคุณ เป็นต้น นอกจากนี้ บริษัท Acxiom ยังขายประวัติของผู้คนให้กับลูกค้าของบริษัท ซึ่งได้แก่บริษัทบัตรเครดิต 12 บริษัทจาก 15 บริษัทชั้นนำ ธนาคาร 7 แห่งจากธนาคารชั้นนำ 10 แห่ง บริษัทโทรคมนาคม 8 แห่งจากบริษัทชั้นนำสิบอันดับแรก และเก้าในสิบของบริษัทประกันภัยอสังหาริมทรัพย์ และอุบัติเหตุชั้นนำ

บริษัท Acxiom อาจเป็นหนึ่งในบริษัทค้าข้อมูลที่ใหญ่ที่สุด และสะท้อนการเปลี่ยนแปลงครั้งสำคัญต่อวิธีการที่ข้อมูลส่วนบุคคลถูกดูแลอยู่บนโลกออนไลน์ Big Data ซึ่งเป็นเทคนิคทางคอมพิวเตอร์เพื่อค้นหาความเข้าใจที่ลึกซึ้งทางสังคมจากการจัดกลุ่มข้อมูลที่มีขนาดใหญ่มากกำลังเปลี่ยนแปลงอุตสาหกรรมอย่างรวดเร็ว ตั้งแต่การบริการสุขภาพไปจนถึงการเลือกตั้ง การใช้ Big Data มีชื่อเสียงในการใช้กับประเด็นทางสังคม ตัวอย่างเช่น การใช้งานของตำรวจ หรือผู้จัดการที่ต้องการเพิ่มประสิทธิผลในการทำงาน แต่ก็นำมา

ซึ่งความท้าทายใหม่ต่อประเด็นความเป็นส่วนตัวในระดับที่ไม่เคยเป็นมาก่อน โดย Big Data มาจาก “ข้อมูลเล็ก ๆ” ที่รวบรวมให้เป็นข้อมูลที่มีขนาดใหญ่ขึ้น และข้อมูลเล็ก ๆ นี้อาจจะเป็นข้อมูลส่วนตัวที่ลึกล้ำได้

นอกจากนี้ บริษัท USA Data (www.usadata.com) เป็นบริษัทที่ดำเนินงานธุรกิจซื้อขายข้อมูลส่วนบุคคลของลูกค้า โดยสามารถสั่งซื้อได้ผ่านทางเว็บไซต์ซึ่งเชื่อมต่ออยู่กับฐานข้อมูลขนาดใหญ่จากบริษัทผู้ให้บริการข้อมูลทางการตลาดและทางธุรกิจชื่อดัง 2 บริษัท ได้แก่ บริษัท Acxiom และบริษัท Dun & Bradstreet (D&B) ตามลำดับ บุคคลใดก็ตามที่มีบัตรเครดิต ก็สามารถซื้อรายชื่อผู้บริโภคได้ หรือลูกค้าจำแนกตามเงื่อนไขต่าง ๆ ได้อย่างง่าย ทางด้านคณะกรรมการการอุดมศึกษา (College Board) ของสหรัฐอเมริกาก็ได้มีการขายข้อมูลนักเรียน High School ที่กำลังจะจบการศึกษาให้กับวิทยาลัยและมหาวิทยาลัยต่าง ๆ มากถึง 1,700 แห่ง ในราคาเพียง 28 เซนต์ (Cent) ต่อ 1 รายชื่อนักเรียน ธุรกิจขายข้อมูลดังกล่าวอยู่ภายใต้การควบคุมของกฎหมายแต่การขายข้อมูลที่เป็นธุรกิจที่ทำให้ได้รายการข้อมูลบัตรเครดิตและหมายเลขโทรศัพท์มือถือของบุคคลอื่นมาอย่างผิดกฎหมายด้วยเช่นกัน โดยเฉพาะการขายให้กับนักสืบเอกชน อย่างไรก็ตามธุรกิจซื้อขายข้อมูลยังเป็นธุรกิจที่เติบโตแบบก้าวกระโดดมาอย่างต่อเนื่อง

สำหรับธุรกิจธนาคารหรือบริษัทที่เป็นนายหน้าข้อมูล (Data Broker)โดยส่วนใหญ่แล้วจะไม่ได้ถูกควบคุมโดยกฎหมาย กล่าวคือไม่ได้มีกฎระเบียบบังคับใช้อย่างครอบคลุม จะมีเพียงข้อบังคับจากส่วนกลางหรือจากรัฐบาลเพียงเล็กน้อยเท่านั้น ที่ได้มีการกำหนดกฎระเบียบในการรวบรวม บำรุงรักษา และขายข้อมูลไว้ ธุรกิจชนิดนี้มีการเติบโตอย่างต่อเนื่อง เนื่องจากมีตลาดขนาดใหญ่ที่ต้องการข้อมูลส่วนบุคคลของผู้บริโภคจำนวนมาก อีกทั้งข้อมูลเหล่านี้ยังมีประโยชน์ต่อบริษัทประกันภัย ธนาคาร นายจ้าง รัฐบาลกลาง รัฐ และเจ้าหน้าที่ของรัฐในแต่ละท้องถิ่นด้วย เช่น กรมสรรพากรและกระทรวงความมั่นคงแห่งมาตุภูมิ ได้ชำระเงินแก่นายหน้าข้อมูลเป็นจำนวน 30 ล้านดอลล่าร์ ในปี ค.ศ. 2005 แลกกับข้อมูลที่ใช้ในการบังคับใช้กฎหมายและการต่อต้านการก่อการร้าย สำหรับกรมสรรพากรได้ลงนามชำระเงินจำนวน 200 ล้านดอลลาร์ต่อ 5 ปี ในการเข้าถึงฐานข้อมูลของบริษัท ChoicePoint ผู้ให้บริการข้อมูลแก่ทางภาครัฐและอุตสาหกรรมต่าง ๆ เพื่อที่จะสามารถระบุทรัพย์สินของผู้เสียภาษีที่พยายามกระทำผิดทางกฎหมายต่อการเสียภาษี หลังจากเหตุการณ์ผู้ก่อการร้ายได้ขับเครื่องบินชนตึกเวิร์ลเทรด เซ็นเตอร์ (ในวันที่ 11 กันยายน ค.ศ. 2001) บริษัท ChoicePoint ได้มีส่วนช่วยรัฐบาลสหรัฐในการคัดเลือกเจ้าหน้าที่ ความมั่นคงปลอดภัยทางด้านอากาศยานใหม่

บริษัท ChoicePoint เป็นหนึ่งในบริษัทนายหน้าข้อมูลที่ใหญ่ที่สุดของสหรัฐอเมริกา มีพนักงานมากกว่า 5,000 คน รอให้บริการตรวจสอบข้อมูลส่วนบุคคลแก่ธุรกิจทุกประเภทและทุกขนาด รวมทั้งให้บริการแก่รัฐบาลกลาง รัฐ และ รัฐบาลท้องถิ่น ในปี ค.ศ. 2004 บริษัท ChoicePoint ได้แสดงให้เห็นถึงปริมาณข้อมูลที่ต้องประมวลผลในแต่ละวินาทีมากถึงพันกว่ารายการ รวมทั้งสิ้นกว่า 7 ล้านรายการที่ต้องตรวจสอบในแต่ละครั้ง ChoicePoint ได้สร้างฐานข้อมูลของข้อมูลส่วนบุคคลที่มีขนาดใหญ่ ด้วยการขยายเครือข่ายของคู่สัญญาว่าจ้างเป็นตัวแทนรวบรวมข้อมูลจากระบบเอกสารสาธารณะ สถาบันการเงิน สมุดหน้า

เหลือง และแบบฟอร์มใบสมัคร สินเชื่อ ทำให้ ChoicePoint มีรายการข้อมูลมากกว่า 10,000 ล้านรายการ ซึ่งส่วนใหญ่เป็นข้อมูลส่วนบุคคลของผู้บริโภควัยทำงาน

ข้อเสียของการมีฐานข้อมูลขนาดใหญ่ที่ดูแลรักษาโดยบริษัท ChoicePoint และ Data Broker อื่น ๆ คือ “ภัยคุกคามต่อสิทธิส่วนบุคคล” ของเจ้าของข้อมูลเหล่านั้น และต่อความปกติสุขทางสังคม เนื่องจากบางครั้งข้อมูลที่บริษัทดูแลอยู่ไม่ถูกต้องและไม่สามารถเชื่อถือได้ ทำให้บุคคลผู้ที่เป็นเจ้าของข้อมูลสูญเสียโอกาสบางอย่างไปหรือเกิดความเดือดร้อนโดยไม่มีความผิด เช่น กรณีที่บริษัท Boston Market ไล่พนักงานออกหลังจากได้รับผลการตรวจสอบภูมิหลังจากบริษัท ChoicePoint ว่าพนักงานคนดังกล่าวมีความผิดทางอาญา ทั้ง ๆ ที่ข้อมูลดังกล่าวเป็นข้อมูลที่ไม่ถูกต้อง หรือกรณีที่พนักงานในสายการผลิตของบริษัท GE ถูกเรียกเก็บเงินชดเชยค่าเสียหายเป็นจำนวนมาก เนื่องจากประวัติการขับขี่ของพนักงานคนดังกล่าวเต็มไปด้วยรายการอุบัติเหตุ ซึ่งเป็นการบันทึกประวัติที่ผิดพลาด โดยเป็นการนำประวัติการขับขี่ของผู้อื่นมาบันทึกแทน เป็นต้น

กระทั่งเมื่อต้นปี ค.ศ. 2005 บริษัท ChoicePoint ได้ถูกวิพากษ์วิจารณ์อย่างหนัก เมื่อทางบริษัทตัดสินใจขายข้อมูลลูกค้าจำนวน 145,000 ราย ให้กับอาชญากรที่มาในคราบของธุรกิจที่ถูกต้องตามกฎหมาย โดยอาชญากรได้นำข้อมูลลูกค้าดังกล่าวไปเปิดบัญชีบัตรเครดิต สร้างความเสียหายแก่เจ้าของข้อมูลที่แท้จริงอย่างมาก จากนั้นเป็นต้นมา บริษัท ChoicePoint จึงได้ทำการลดรายละเอียดข้อมูลสำคัญออกก่อนขายให้แก่หน่วยงานต่าง ๆ เช่น หมายเลขประกันสังคม หมายเลขใบขับขี่ อีกทั้งยังได้มีการจำกัดการเข้าถึงฐานข้อมูลของบริษัทอื่น ๆ ที่เป็นตัวแทน และได้กำหนดกระบวนการตรวจสอบผู้ซื้อข้อมูลอย่างเข้มงวดอีกด้วย

Marc Rotenberg เจ้าหน้าที่ของศูนย์สารสนเทศสิทธิส่วนบุคคลทางอิเล็กทรอนิกส์ในกรุงวอชิงตัน ดี.ซี. เชื่อว่า บริษัท ChoicePoint คือกรณีศึกษาที่ค่อนข้างชัดเจนที่แสดงให้เห็นว่าการดูแลและกำกับตนเองไม่สามารถได้ผลที่สมบูรณ์กับธุรกิจที่เกี่ยวข้องกับข้อมูลสารสนเทศและยังได้แสดงให้เห็นว่าธุรกิจเหล่านี้ยังต้องการกฎหมายเพิ่มเติมมาควบคุม ดังนั้น ในรัฐแคลิฟอร์เนียและอื่น ๆ อีก 99 รัฐรวมถึงนิวยอร์กได้ผ่านร่างกฎหมายบังคับให้บริษัทแจ้งต่อลูกค้าก่อนเมื่อจะนำข้อมูลส่วนบุคคลของลูกค้าไปใช้ การผ่านร่างกฎหมายเป็นผลให้สภาคองเกรสได้ตราพระราชบัญญัติเกี่ยวกับความมั่นคงปลอดภัยของข้อมูลหลายฉบับในปี ค.ศ. 2006

3.2.1.1 รัฐแคลิฟอร์เนีย

รัฐแคลิฟอร์เนีย เป็นมลรัฐหนึ่งในประเทศสหรัฐอเมริกา ในท่ามกลางกฎหมาย California Consumer Privacy Act of 2018 (CCPA) ได้มีผลใช้บังคับวันที่ 1 กรกฎาคม ค.ศ. 2020 ที่เกี่ยวข้องกับกฎหมายความเป็นส่วนตัวของผู้บริโภคแห่งแคลิฟอร์เนีย สภานิติบัญญัติแห่งรัฐแคลิฟอร์เนียยังได้ออกกฎหมาย California Consumer Privacy Act of 2018 (CCPA) ซึ่งเป็นกฎหมายที่ให้สิทธิผู้บริโภคเกี่ยวกับข้อมูลส่วนบุคคล ตามที่กำหนดไว้ซึ่งถูกรวบรวมโดยบริษัท หรือนิติบุคคล ตามที่กำหนดไว้ รวมถึงให้สิทธิในการดำเนินธุรกิจที่เกี่ยวกับการรวบรวมข้อมูลส่วนบุคคล รวมถึงข้อมูลละเอียดอ่อน โดยกำหนดให้นายหน้าข้อมูลต้องลงทะเบียน และปฏิบัติตามกฎหมายที่กำหนด โดยฝ่ายนิติบัญญัติของรัฐแคลิฟอร์เนียกำหนดให้กฎหมายนายหน้าข้อมูลทำการซื้อขายหลักทรัพย์ก่อน ใน California Consumer Privacy Act of 2018 (CCPA) ได้

ชี้แจงไว้ในประมวลกฎหมายแพ่งของรัฐแคลิฟอร์เนีย (California Civil Code §1798.99.88) ว่า "ไม่มีสิ่งใดจะถูกตีความเพื่อแทนที่หรือแทรกแซงการดำเนินการของกฎหมายคุ้มครองความเป็นส่วนตัวของผู้บริโภคแห่งรัฐแคลิฟอร์เนียได้"

ใน CCPA และ ประมวลกฎหมายแพ่งของรัฐแคลิฟอร์เนีย (California Civil Code §1798.99.88) TITLE 1.81.48. (d) ได้บัญญัติให้คำนิยามคำว่า “ข้อมูลผู้บริโภคแบบบูรณาการ” หมายถึง ข้อมูลที่เกี่ยวข้องกับกลุ่มหรือประเภทของผู้บริโภค ซึ่งสามารถระบุตัวตนของผู้บริโภคส่วนบุคคลได้ โดยสามารถลบข้อมูลได้หากไม่สามารถติดต่อกับผู้บริโภคหรือครอบครัวของผู้บริโภคบุคคลนั้น ได้อย่างสมเหตุสมผล โดยรวมถึงการดำเนินการผ่านอุปกรณ์

“สรุปข้อมูลผู้บริโภค” ไม่ได้หมายถึงการบันทึกข้อมูลผู้บริโภคส่วนบุคคลที่ได้รับการระบุอย่างน้อยหนึ่งรายการ

“ข้อมูลไบโอเมตริกซ์” หมายถึง ลักษณะทางสรีระวิทยา ชีววิทยา หรือพฤติกรรมของบุคคล รวมถึงข้อมูลที่เกี่ยวข้องกับ DNA ของบุคคล ซึ่งบุคคลดังกล่าว ถูกใช้โดยลำพัง หรือตั้งใจที่จะใช้ร่วมกับข้อมูลที่ระบุตัวตนอื่นๆ เพื่อสร้างการระบุตัวตนของบุคคล รวมถึงข้อมูลไบโอเมตริกซ์ แต่ไม่จำกัดเฉพาะภาพของม่านตา,จอประสาทตา ,ลายนิ้วมือ ,ใบหน้า ,มือ ,ฝ่ามือ ,รูปแบบเส้นเลือด และการบันทึกเสียง ซึ่งสามารถดึงแม่แบบ เช่น ลายนิ้วมือ ,ใบหน้า ,แม่แบบลายละเอียด หรือลายเส้นเสียง รวมถึงรูปแบบการกดแป้นพิมพ์ หรือจังหวะรูปแบบการเดิน ,ข้อมูลการนอนหลับ ,ข้อมูลสุขภาพ และข้อมูลการออกกำลังกายที่มีข้อมูลระบุ

นายหน้าข้อมูล (Data Broker) ไว้ว่า “ นายหน้าข้อมูล หมายถึง ธุรกิจที่รวบรวมและขายข้อมูลส่วนบุคคลของผู้บริโภคให้แก่บุคคลที่สามโดยที่ธุรกิจไม่มีความสัมพันธ์โดยตรง แต่นายหน้าซื้อขายข้อมูลไม่รวมถึงสิ่งต่อไปนี้

หน่วยงานการรายงานผู้บริโภคในขอบเขตที่อยู่ภายใต้กฎหมายการรายงานเครดิตที่เป็นธรรมของรัฐบาลกลาง (15 U.S.C. Sec. 1681 et seq.)

สถาบันการเงินภายในขอบเขตที่กฎหมาย Gramm-Leach-Bliley ครอบคลุม (กฎหมายมหาชน 106-102) และระเบียบปฏิบัติ

นิติบุคคลภายในขอบเขตที่ครอบคลุมโดยพระราชบัญญัติข้อมูลการประกันภัยและการคุ้มครองความเป็นส่วนตัว (มาตรา 6.6 (เริ่มต้นด้วยมาตรา 1791) ของบทที่ 1 ของประมวลกฎหมายประกันภัย)”

คำจำกัดความของ "นายหน้าข้อมูล" ของรัฐแคลิฟอร์เนียกำหนดไว้ที่มาตรา 1798.99.80 (d) กฎหมายนายหน้าข้อมูลของแคลิฟอร์เนียนั้น หมายถึง ธุรกิจที่รวบรวมและขายข้อมูลส่วนบุคคลของผู้บริโภคแก่บุคคลที่สามซึ่งธุรกิจไม่มีความสัมพันธ์โดยตรง" ตามประมวลกฎหมายแพ่งของรัฐแคลิฟอร์เนีย คำว่า "ความสัมพันธ์โดยตรง" ไม่ได้กำหนดไว้ใน CCPA หรือกฎหมายนายหน้าซื้อขายข้อมูลส่วนบุคคล คำดังกล่าวถูกเพิ่มลงใน CCPA เมื่อปลายปี 2019 สำหรับธุรกิจที่ดำเนินการทางออนไลน์โดยเฉพาะ และมีความสัมพันธ์โดยตรงกับผู้บริโภค และคำจำกัดความนี้ครอบคลุมถึงธุรกิจ ใดๆ ที่เก็บรวบรวมข้อมูลส่วนบุคคลของผู้บริโภค

อย่างรู้เท่าทัน ไม่มีความสัมพันธ์โดยตรงกับผู้บริโภครายนั้น และขายข้อมูลส่วนบุคคลของผู้บริโภคให้กับบุคคลที่สาม

ภายใต้กฎหมายใหม่ของรัฐแคลิฟอร์เนีย ประมวลกฎหมายแพ่งของรัฐแคลิฟอร์เนีย§ 1798.99.80 et seq. ได้กำหนดให้นายหน้าขายข้อมูลจะต้องลงทะเบียนทุกปีหรือก่อนวันที่ 31 มกราคม ของทุกปี กับสำนักงานอัยการสูงสุดแห่งแคลิฟอร์เนียบนเว็บไซต์อินเทอร์เน็ตที่สามารถเข้าถึงได้โดยสาธารณะ (https://oag.ca.gov/data-broker/register.) ซึ่งนายหน้าข้อมูลมีหน้าที่จะต้องชำระค่าธรรมเนียมการลงทะเบียนและให้ข้อมูลตามที่กฎหมายกำหนด รวมถึงชื่อของนายหน้าข้อมูล ที่อยู่เว็บไซต์ อีเมล และข้อมูลเพิ่มเติมหรือคำอธิบายใดๆ ที่นายหน้าข้อมูลเลือกที่จะให้เกี่ยวกับแนวทางปฏิบัติในการรวบรวมข้อมูล ซึ่งค่าธรรมเนียมการลงทะเบียนรายปีเป็นจำนวน 400 เหรียญต่อปี สำหรับนายหน้าข้อมูลที่ลงทะเบียนไว้จะได้รับอีเมลพร้อมใบแจ้งให้ชำระค่าธรรมเนียมและคำแนะนำในการชำระเงิน ถ้าหากไม่เคยลงทะเบียนมาก่อนจะต้องสร้างบัญชีด้วยที่อยู่ อีเมลที่ถูกต้องเสียก่อน เมื่อการลงทะเบียนของนายหน้าขายข้อมูลนั้นได้รับการอนุมัติก็จะได้รับอีเมลพร้อมใบแจ้งให้ชำระค่าธรรมเนียมและข้อมูลการชำระเงิน หากชำระเงินออนไลน์เสร็จสิ้นจะต้องชำระค่าธรรมเนียมบริการเพิ่มเติม 2.99% เพื่อทำธุรกรรมบัตรเครดิตให้เสร็จสมบูรณ์ ทั้งนี้ สำนักงานอัยการสูงสุดไม่ได้รับส่วนใดส่วนหนึ่งของค่าบริการนี้ ซึ่งนายหน้าข้อมูลที่ไม่ได้ลงทะเบียนภายในวันที่ 31 มกราคมที่กำหนดตามกฎหมายควรที่จะลงทะเบียนโดยเร็วที่สุดซึ่งจะต้องรับโทษทางแพ่ง ทางรัฐแคลิฟอร์เนียได้เปิดเว็บไซต์การลงทะเบียนและมีบริษัทมากกว่า 50 แห่งได้ลงทะเบียนแล้ว

ในรัฐแคลิฟอร์เนีย ทุกธุรกิจต้องมีมุมมองของตนเองว่าจะกำหนดขอบเขตในส่วนที่ถือเป็น "ความสัมพันธ์โดยตรง" เพื่อวัตถุประสงค์ในการปฏิบัติตามกฎหมายการจดทะเบียนนายหน้าข้อมูล ของบริษัทที่รวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่ "โดยตรง" จากผู้บริโภค

บริษัทที่ได้รับข้อความว่า "อย่าขายข้อมูลส่วนบุคคลที่เชื่อมโยงกับฉัน" บนเว็บไซต์ตั้งแต่วันที่ 1 มกราคม 2019 ควรประเมินว่าจะต้องลงทะเบียนเป็นนายหน้าซื้อขายข้อมูลส่วนบุคคลด้วยหรือไม่ ตามประมวลกฎหมายแพ่งของรัฐแคลิฟอร์เนีย (c) (1) นายหน้าซื้อขายข้อมูลส่วนบุคคลที่ไม่สามารถลงทะเบียนตามที่กำหนดจะต้องถูกสั่งห้ามและจะต้องรับผิดในค่าปรับทางแพ่ง รวมถึงชำระค่าธรรมเนียมและค่าใช้จ่ายในการดำเนินการของรัฐแคลิฟอร์เนียให้กับอัยการสูงสุด ซึ่งรวมถึงค่าปรับทางแพ่งจำนวน 100 ดอลลาร์ ต่อวัน หากนายหน้าซื้อขายข้อมูลส่วนบุคคลไม่ลงทะเบียน ค่าธรรมเนียมที่ครบกำหนดในระหว่างช่วงเวลาที่ไม่สามารถลงทะเบียน และค่าใช้จ่ายที่เกิดขึ้นให้อัยการสูงสุดมีอำนาจในการสอบสวนและดำเนินคดี ค่าปรับค่าธรรมเนียม และค่าใช้จ่ายใดๆ ที่ได้รับจากการดำเนินการจะถูกฝากไว้ในกองทุน Consumer Privacy Fund

3.2.1.2 รัฐเวอร์มอนต์

รัฐเวอร์มอนต์ เป็นมลรัฐหนึ่งที่มีกฎหมายเกี่ยวกับนายหน้าข้อมูลเช่นเดียวกันกับรัฐแคลิฟอร์เนียร์ โดยเมื่อวันที่ 22 พฤษภาคม ค.ศ. 2018 รัฐเวอร์มอนต์ได้ตรากฎหมาย House Bill 764 ซึ่งเป็นกฎหมายที่

ควบคุมนายหน้าข้อมูลที่ซื้อขายข้อมูลส่วนบุคคลเกี่ยวกับผู้อยู่อาศัยในรัฐเวอร์มอนต์เป็นครั้งแรก[19] รัฐเวอร์มอนต์ มีการบัญญัติเกี่ยวกับนายหน้าข้อมูลไว้ โดยได้บัญญัติเกี่ยวกับนายหน้าข้อมูลไว้ใน Vermont Data Broker Regulation (VDBR) และยังได้กำหนดคำแนะนำ หรือแนวปฏิบัติของนายหน้าข้อมูล ไว้ใน Guidance on Vermont's Act 171 of 2018 Data Broker Regulation[20]

รัฐเวอร์มอนต์ของประเทศสหรัฐอเมริกาก็ได้ให้คำนิยามของ นายหน้าข้อมูล ไว้ใน Vermont Data Broker Regulation (VDBR) 9 V.S.A. § 2430 (4) ไว้ว่า "นายหน้าข้อมูล หมายความว่า ธุรกิจหรือหน่วยหรือหน่วยของธุรกิจแยกต่างหากหรือร่วมกันโดยรู้เท่าทันรวบรวมและขายหรืออนุญาตให้บุคคลที่สามข้อมูลส่วนบุคคลที่เป็นนายหน้าของผู้บริโภคที่ธุรกิจไม่มีความสัมพันธ์โดยตรง"

VDBR ได้กำหนดคำว่า 'นายหน้าข้อมูล' เป็นธุรกิจหรือหน่วยของธุรกิจใด ๆ ที่รวบรวมและขายหรืออนุญาตให้บุคคลที่สาม 'นายหน้าข้อมูล' ของผู้บริโภค (เช่นผู้มีถิ่นที่อยู่ในเวอร์มอนต์) ซึ่งธุรกิจไม่ได้ทำ มีความสัมพันธ์โดยตรง 'ข้อมูลส่วนบุคคลที่นายหน้า' รวมถึงองค์ประกอบข้อมูลใด ๆ ต่อไปนี้เกี่ยวกับผู้บริโภคหากจัดหมวดหมู่หรือจัดระเบียบเพื่อเผยแพร่ไปยังบุคคลที่สาม[21]

1. ชื่อ
2. ที่อยู่
3. วันเดือนปีเกิดหรือสถานที่เกิด
4. นามสกุลเดิมของมารดา
5. ข้อมูลไบโอเมตริกซ์เฉพาะที่สามารถระบุหรือรับรองความถูกต้องของผู้บริโภค (เช่น ลายนิ้วมือ เรตินา หรือภาพไอริส)
6. ชื่อหรือที่อยู่ของสมาชิกในครอบครัวหรือครัวเรือนของผู้บริโภค
7. หมายเลขประกันสังคมหรือหมายเลขประจำตัวอื่นๆ ที่ทางราชการออกให้
8. ข้อมูลอื่นใดที่เพียงอย่างเดียวหรือร่วมกับข้อมูลอื่นๆ ที่ขายหรือได้รับอนุญาตจะช่วยให้บุคคลที่สมเหตุสมผลสามารถระบุตัวผู้บริโภคได้ด้วยความแน่นอนตามสมควร

---

[19] Practical Law Data Privacy Advisor, 'Vermont Enacts First Data Broker Law' <https://content.next.westlaw.com/practical-law/document/Ie07faf6e641e11e89bf199c0ee06c731/Legal-Updates-Vermont-Enacts-First-Data-Broker-Law?viewType=FullText&transitionType=Default&contextData=%28sc.De fault%29> สืบค้นเมื่อ 20 สิงหาคม 2565.

[20] the Vermont Office of the Attorney General. 'Guidance on Vermont's Act 171 of 2018 Data Broker Regulation December 11, 2018' <https://ago.vermont.gov/wp-content/uploads/2018/12/2018-12-11-VT-Data-Broker-Regulation-Guidance.pdf. p.1.> สืบค้นเมื่อ 20 สิงหาคม 2565.

[21] Dataguidance, 'Vermont: Overview of the Data Broker Act' <https://www.dataguidance.com/opinion/vermont-overview-data-broker-act.> สืบค้นเมื่อ 20 สิงหาคม 2565.

ข้อมูลส่วนบุคคลที่นายหน้าไม่รวมถึงข้อมูลที่เปิดเผยต่อสาธารณะที่เกี่ยวข้องกับธุรกิจหรืออาชีพ ตัวอย่างเช่น ตาม Guidance on Vermont's Act 171 ของ 2018 Data Broker Regulation ที่ออกโดย Vermont Office of the Attorney General ('AG') ('the Guidance') ที่อยู่และหมายเลขโทรศัพท์ของสำนักงานแพทย์ไม่ใช่ ข้อมูลส่วนบุคคล แต่ถ้าหมายเลขโทรศัพท์มือถือส่วนตัวของแพทย์นับเป็นข้อมูลส่วนบุคคลที่มี "ความสัมพันธ์โดยตรง" สำหรับธุรกิจที่ขายข้อมูลของผู้บริโภค "ถ้าผู้บริโภคเป็นอดีตหรือปัจจุบันของลูกค้า สมาชิก ผู้ใช้ หรือผู้ใช้ที่ลงทะเบียนของสินค้าหรือบริการของธุรกิจ พนักงาน ผู้รับเหมา หรือตัวแทนของธุรกิจ นักลงทุนในธุรกิจ หรือ ผู้บริจาคให้กับธุรกิจ" ซึ่งแน่นอนว่า คำจำกัดความในกฎเกณฑ์ของรัฐเวอร์มอนต์ใช้ไม่ได้ในแคลิฟอร์เนีย นอกจากนี้ยังปรากฏในบริบททางกฎหมายที่แตกต่างกัน เนื่องจากกฎหมายเวอร์มอนต์มีคำจำกัดความและภาระผูกพันที่สำคัญต่างกัน

แนวทางปฏิบัติของรัฐเวอร์มอนต์เกี่ยวกับนายหน้าข้อมูล มีกำหนดไว้ใน Guidance on Vermont’s Act 171 of 2018 Data Broker Regulation โดยให้นายหน้าข้อมูลจะต้องลงทะเบียนกับเลขาธิการรัฐเวอร์มอนต์ (Vermont Secretary of State) เป็นรายปีระหว่างวันที่ 1 มกราคม ถึง 31 มกราคม ตามปีปฏิทิน โดยชำระค่าธรรมเนียมการลงทะเบียนเป็นเงินจำนวน $100 และจะต้องกำหนดมาตรการขั้นต่ำให้เป็นไปตามที่ Guidance on Vermont’s Act 171 of 2018 Data Broker Regulation กำหนดไว้ อีกทั้งจะต้องระบุถึงชื่อ , ที่อยู่อีเมลของนายหน้าข้อมูล ซึ่งจะต้องเปิดเผยถึงรายละเอียดเกี่ยวกับการเลือกที่จะไม่รับโดยนายหน้าข้อมูลกำหนดให้บริษัทที่ประมวลผลข้อมูลจากผู้ที่ไม่ใช่ลูกค้าโดยตรงลงทะเบียนเป็นนายหน้าข้อมูลกับรัฐ ในส่วนหนึ่งของการลงทะเบียนจะต้องระบุด้วยว่าอนุญาตให้บุคคลที่จะห้ามการรวบรวมและการขายข้อมูลของพวกเขาที่ผ่านๆมา ส่งผลให้การซื้อขายข้อมูลส่วนบุคคลสามารถกระทำได้โดยอยู่ภายใต้กรอบที่กฎหมายกำหนด และสามารถตรวจสอบและทราบถึงแหล่งที่มาของข้อมูลที่ถูกซื้อขายกันได้ง่ายขึ้น และมีการกำหนดโทษไว้ ซึ่งกำหนดอัตราโทษปรับในทางแพ่งจำนวน 50 ดอลลาร์ต่อวัน หรือ ไม่เกิน 10,000 ดอลลาร์ต่อปี สำหรับนายหน้าข้อมูลที่ฝ่าฝืนไม่ได้ลงทะเบียน โดยให้อำนาจแก่อัยการสูงสุดในการนำกฎเกณฑ์ในการดำเนินคดีทางแพ่ง และบังคับใช้กฎหมายสำหรับกรณีการกระทำที่ฝ่าฝืนซึ่งเป็นการกระทำที่ไม่เป็นธรรมและเป็นการหลอกลวง

3.2.2 ประเทศญี่ปุ่น[22]

ประเทศญี่ปุ่น เป็นประเทศที่มีรูปแบบการปกครองเป็นประชาธิปไตยที่มีจักรพรรดิเป็นประมุขของประเทศ และเป็นศูนย์รวมความเป็นหนึ่งเดียวของประชาชน โดยมีรัฐธรรมนูญกำหนดให้รัฐสภา (The Diet) เป็นองค์กรที่อยู่ในลำดับสูงสุดในการใช้อำนาจรัฐ และมีอำนาจในการตรากฎหมาย สำหรับอำนาจบริหาร

[22] อุดม รัฐอมฤต, สมคิด เลิศไพฑูรย์ และกิตติพงศ์ กมลธรรมวงศ์, *พัฒนามาตรการในการดำเนินการพิจารณาความเหมาะสมความเป็นไปได้ เพื่อจัดทำแนวทาง ขั้นตอนและวิธีการในการเข้าร่วมหรือทำความตกลงตามกรอบว่าด้วยการคุ้มครองความเป็นส่วนตัวของ APEC (APEC Privacy Framework)* (สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์ 2557) 39-44.

ประเทศเป็นของคณะรัฐบาล (The Cabinet) ประกอบด้วยนายกรัฐมนตรี และรัฐมนตรีตามจำนวนที่กฎหมายกำหนด ในขณะที่ศาลสูง (Supreme Court) และศาลล่างอื่นๆ (Inferior Court) เป็นองค์กรที่ชิอำนาจตุลาการ ซึ่งหากพิจารณาโดยภาพรวมของโครงสร้างการปกครองของประเทศญี่ปุ่นแล้วจะพบว่ามีลักษณะคล้ายกับโครงสร้างการปกครองของประเทศไทย

กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (Act on the Protection of Personal Information: APPI) เป็นกฎหมายหลักที่เกี่ยวข้องกับข้อมูลส่วนบุคคลในประเทศญี่ปุ่น โดย APPI มีผลบังคับใช้กับผู้ประกอบธุรกิจทั้งหมด (บุคคลและนิติบุคคล) ที่ดำเนินการกับข้อมูลส่วนบุคคล นอกจากนี้ APPI ยังจำแนกความแตกต่างระหว่างข้อมูลส่วนบุคคลกับข้อมูลส่วนตัวอีกด้วย (ซึ่ง APPI กำหนดว่าข้อมูลส่วนบุคคลถือเป็นส่วนหนึ่งของฐานข้อมูลของข้อมูลส่วนบุคคล) ข้อผูกพันของผู้ประกอบธุรกิจจะแตกต่างกันไปโดยขึ้นอยู่กับว่าผู้ประกอบธุรกิจได้รับ ใช้งาน หรือให้ข้อมูลส่วนบุคคลหรือข้อมูลส่วนตัว

กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ของประเทศญี่ปุ่นที่บังคับใช้กับผู้ประกอบธุรกิจทั้งหมดที่มีการเก็บข้อมูลส่วนบุคคล ซึ่ง APPI ของญี่ปุ่นนั้นประกาศใช้โดยทั่วไปในปี พ.ศ. 2546 และประกาศใช้อย่างเต็มรูปแบบทุกภาคส่วนในปี พ.ศ. 2548

อีกทั้งในปี พ.ศ. 2562 ทาง EU ก็ได้ทำการรับรองมาตรฐานการคุ้มครองข้อมูลกับประเทศญี่ปุ่นอีกด้วย ทำให้สามารถถ่ายโอนข้อมูลส่วนตัวระหว่างสองเขตเศรษฐกิจได้อย่างอิสระ บนพื้นฐานของการรับประกันความคุ้มครองข้อมูล ซึ่งการรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลระหว่าง EU กับญี่ปุ่นก็จะช่วยให้มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของญี่ปุ่นมีระดับสูงขึ้น และช่วยเพิ่มขีดความสามารถในการแข่งขันและการทำธุรกิจ ให้สามารถขยายเข้าไปยังฝั่ง EU ได้มากยิ่งกว่าเดิม

สหภาพยุโรป เริ่มกระบวนการให้การรับรองมาตรฐานการคุ้มครองข้อมูลของญี่ปุ่น (Adequacy Decision) เพื่ออำนวยความสะดวกในการรับส่งข้อมูลระหว่างประเทศสมาชิกและญี่ปุ่น หลังจากที่เห็นชอบในเนื้อหาการรับรองมาตรฐานการคุ้มครองมาตรฐานของญี่ปุ่นไปเมื่อเดือนกรกฎาคม 2561 ล่าสุดเมื่อวันที่ 5 กันยายน 2561 สหภาพยุโรปได้เริ่มกระบวนการให้การรับรองมาตรฐานการคุ้มครองข้อมูลของญี่ปุ่น ภายใต้กฎระเบียบ GDPR ที่มีผลบังคับใช้ไปตั้งแต่เดือนพฤษภาคม 2561 ที่ผ่านมา

โดย APPI เป็นกฎหมายที่มีมาตรการป้องกันไม่ให้สามารถระบุตัวตนได้ ข้อมูลส่วนบุคคลทุกประเภทจะต้องได้รับการคุ้มครอง โดยเจ้าของข้อมูลมีสิทธิในการตรวจสอบ การแก้ไขข้อมูล การไม่ยินยอมให้ประมวลผล เป็นต้น และมีการคุ้มครองข้อมูลที่มีความอ่อนไหว (sensitive data) ซึ่งเป็นข้อมูลได้รับการคุ้มครองพิเศษ

APPI ได้ให้ความหมายของข้อมูลส่วนบุคคลไว้ว่า “ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลที่เกี่ยวข้องกับบุคคลที่มีชีวิตอยู่ ได้แก่ ชื่อ วันเกิด หรือสิ่งต่างๆ ที่สามารถระบุ ที่อยู่ การบันทึกด้วยสิ่งต่างๆ เช่น เสียง การเคลื่อนไหว การได้ยิน หรือหระบวนการในการจัดเก็บข้อมูลทางเอกสาร หรือภาพวาด หรือการบนทึกทางแม่เหล็กไฟฟ้า (หมายถึง การบันทึกทางอิเล็กทรอนิกส์ หรือรูปแบบอื่นที่ไม่สามารถรับรู้ผ่านประสาทสัมผัสของ

มนุษย์ โดนสามารถระบุตัวบุคคลเฉพาะได้ เช่นเดียวกับ รหัสประจำตัวบุคคล ซึ่งรวมถึง อักขระ ตัวอักษร ตัวเลข สัญลักษณ์ หรือรหัสอื่นๆ ที่อยู่ภายใต้ข้อใดข้อหนึ่งต่อไปนี้ รหัสคอมพิวเตอร์ และแปลจากข้อมูลทางกายภาพของบุคคล เพื่อระบุตัวบุคคล หรือตัวอักษร ตัวเลข สัญลักษณ์ หรือรหัสอื่น ซึ่งเกี่ยวข้องกับการให้บริการแก่บุคคล หรือการซื้อสินค้าที่ขายให้กับบุคคล หรือระบุไว้ในบัตรหรือบันทึกทางอิเล็กทรอนิกส์ หรือเอกสารอื่นที่สามารถระบุตัวผู้ใช้ ผู้ซื้อ หรือผู้รับการแจกจ่ายได้ โดยกำหนดประกาศ หรือบันทึกรหัสที่แตกต่างกัน สำหรับผู้ใช้ ผู้ซื้อ หรือผู้รับการแจกจ่าย APPI ยังกำหนดข้อมูลส่วนบุคคลเป็นข้อมูลส่วนบุคคลที่สร้างฐานข้อมูลของข้อมูลส่วนบุคคล)

ภาคธุรกิจของญี่ปุ่นต้องเพิ่มความเข้มงวดด้านการคุ้มครองข้อมูลส่วนบุคคลเพิ่มมากขึ้น เพราะร่างข้อมติรับรองมาตรฐานการคุ้มครองข้อมูล (Draft Decision) ที่จัดทำโดยคณะกรรมาธิการยุโรป ระบุข้อปฏิบัติเพิ่มเติม (Supplementary Rules) จากกฎหมายการคุ้มครองข้อมูลส่วนบุคคลของญี่ปุ่นที่มีอยู่แล้ว (Act on the Protection of Personal Information : APPI) โดยข้อปฏิบัติเพิ่มเติมดังกล่าวมีสาระสำคัญดังต่อไปนี้

กระบวนการทำให้ข้อมูลยืนยันตัวบุคคลไม่ปรากฏชื่อของบุคคลนั้น หรือสิ่งที่สามารถระบุตัวตนของบุคคลนั้น (anonymization) โดยจะต้องไม่ให้สามารถระบุตัวตนได้อีก เพื่อปกป้องข้อมูลส่วนบุคคลที่ได้รับการโอนมาจากประเทศสมาชิก ซึ่งภาคธุรกิจของญี่ปุ่นจะต้องลบข้อมูลสำคัญที่จะทำให้สามารถระบุตัวตนได้ (destroy the key permitting to re-identify the data) ทั้งนี้ เพราะกฎหมาย APPI ของญี่ปุ่น ระบุเพียงแค่ให้มีมาตรการป้องกันไม่ให้สามารถระบุตัวตนได้เท่านั้น (merely required to prevent re-identification) แต่อาจใช้วิธีการอื่นๆ เพื่อระบุตัวตนได้

ข้อมูลส่วนบุคคลทุกประเภทจะต้องได้รับการคุ้มครองโดยเจ้าของข้อมูลเท่ากันที่มีสิทธิ เช่น สิทธิในการเข้าถึงเพื่อตรวจสอบ สิทธิในการแก้ไขข้อมูล หรือการไม่ยินยอมให้ประมวลผล เป็นต้น ซึ่งรวมถึงข้อมูลที่มีกำหนดลบทิ้ง (set to be deleted) ภายในระยะเวลาไม่เกิน 1 ปี เนื่องจากกฎหมาย APPI ไม่ได้ให้สิทธิการคุ้มครองข้อมูลประเภทดังกล่าว

การนำข้อมูลไปประมวลผลไม่สามารถใช้เกินขอบเขตที่เจ้าของข้อมูลให้ความยินยอมไว้ โดยจะต้องขอความยินยอมใหม่ทุกครั้ง ซึ่งต่างจากกฎหมาย APPI เดิมที่ไม่มีความชัดเจนเกี่ยวกับการขอความยินยอมจากเจ้าของข้อมูล ในกรณีที่จุดประสงค์ในการประมวลผลข้อมูลแตกต่างไปจากจุดประสงค์เดิมที่เจ้าของข้อมูลให้ความยินยอมไว้ก่อน

การยกระดับการคุ้มครองข้อมูลที่มีความอ่อนไหว (sensitive data) ภายใต้กฎระเบียบ GDPR ให้ได้รับการคุ้มครองแบบพิเศษ (special care-required personal information) ตามกฎหมาย APPI เพราะข้อมูลประเภทข้อมูลละเอียดอ่อนภายใต้กฎระเบียบ GDPR เช่น เชื้อชาติ ศาสนา ประวัติการรักษา และอาชญากรรม เป็นประเภทข้อมูลเดียวกันกับข้อมูลประเภทที่ได้รับการคุ้มครองพิเศษ ภายใต้กฎหมาย APPI

การกำหนดว่าการถ่ายโอนข้อมูล โดยทั่วไปแล้วการถ่ายโอนข้อมูลส่วนบุคคลไปยังบุคคลที่สามเป็นกรณีที่เจ้าของข้อมูลไม่ได้รับความยินยอมล่วงหน้าจากหน่วยงานจะไม่สามารถกระทำได้ เว้นแต่จะมีข้อยกเว้น:

1.การโอนที่ได้รับอนุญาตตามกฎหมาย หากเป็นกรณีที่ได้รับอนุญาตแล้วไม่จำเป็นต้องได้รับความยินยอมล่วงหน้าจากเจ้าของหลักในการถ่ายโอนข้อมูลส่วนบุคคล (รวมถึงข้อมูลที่มีลักษณะละเอียดอ่อน)

2. กรณีที่จำต้องได้รับความยินยอมจากเจ้าของข้อมูล ที่ถือว่าเป็นข้อกำหนดหรือได้รับอนุญาตโดยเฉพาะตามกฎหมายหรือข้อบังคับของญี่ปุ่น จะต้องเป็นกรณีที่มีความจำเป็นสำหรับการปกป้องชีวิต สุขภาพ หรือทรัพย์สินของบุคคล และได้รับความยินยอมจากเจ้าของข้อมูลเป็นการยากเท่าที่จำเป็น

3. มีความจำเป็นสำหรับการพัฒนาด้านสาธารณสุขและสุขอนามัย หรือการส่งเสริมการเลี้ยงดูที่ดีและการได้รับความยินยอมจากผู้ปกครองหรือบิดา มารดานั้นทำได้ยาก เท่าที่จำเป็น

ซึ่งจะเห็นได้ว่าสำหรับกฎหมายในเรื่องการแบ่งปันข้อมูลส่วนบุคคลในประเทศญี่ปุ่นนั้น ถือได้ว่ามีหลักการคือจะต้องได้รับความยินยอมจากเจ้าของข้อมูลโดยตรงเสียก่อน แต่อย่างไรก็ตามหากมีเหตุฉุกเฉินหรือเกี่ยวข้องกับทางด้านสาธารณสุข สามารถที่ใช้ข้อมูลเท่าที่จำเป็นในสถาการณ์นั้นที่เกิดเหตุขึ้น[23]

การโอนข้อมูลส่วนบุคคลของผู้ที่มีถิ่นพำนักใน EU จากญี่ปุ่นไปยังประเทศที่สาม (onward transfer) จะต้องเป็นไปตามระเบียบที่กำหนดไว้ โดยการโอนข้อมูลส่วนบุคคลต่อจากญี่ปุ่นไปยังประเทศที่สามมี 2 กรณี คือ

กรณีที่ 1 ประเทศที่สามนั้นได้รับการรับรองมาตรฐานการคุ้มครองข้อมูลจากญี่ปุ่น และ

กรณีที่ 2 ในกรณีที่ผู้รับโอนอยู่ในประเทศที่มีระดับการให้ความคุ้มครองแตกต่างกัน

ผู้ประกอบการต้องจัดทำกฎข้อบังคับหรือสัญญาที่ให้ความคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร (Binding Corporate Rules) ตามมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของญี่ปุ่นและข้อปฏิบัติเพิ่มเติม (Supplementary Rules) ตามที่ญี่ปุ่นมีความตกลงร่วมกับสหภาพยุโรป

การใช้ข้อมูลส่วนบุคคลเพื่อทำการตลาดทางตรง (Direct Marketing) จะต้องได้รับการยินยอมจากเจ้าของข้อมูล และต้องสามารถให้เจ้าของข้อมูลบอกยกเลิกการใช้ข้อมูลส่วนบุคคลได้ (opt-out) โดยการใช้ข้อมูลส่วนบุคคลที่โอนจากสหภาพยุโรปไปยังญี่ปุ่น หรือจากญี่ปุ่นไปยังประเทศที่สามจะต้องเป็นไปตามจุดประสงค์เดิมที่เจ้าของข้อมูลได้ให้ความยินยอมไว้เท่านั้น หากต้องการใช้ข้อมูลเพื่อทำการตลาดทางตรงเพิ่มเติมจะต้องขอความยินยอมจากเจ้าของข้อมูลก่อน รวมทั้งต้องให้เจ้าของข้อมูลสามารถบอกยกเลิกการใช้ข้อมูลของตนได้ทุกเมื่อ (opt-out)

---

[23] พงษ์มนัส ดีอด,พระครูวินัยธรวรชัด ปยุตฺโต,ปาริฉัตร ไชยเดช,พระมหาชัยชนะ บุญนาดี , *รูปแบบที่เหมาะสมการแบ่งปันข้อมูลส่วนบุคคลเพื่อการบริหารภาครัฐ ภายใต้กรอบพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล* (2022) ,บทความวิชาการ วารสารมหาจุฬานาครทรรน์, 133.

การบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลมีความเข้มงวดมากขึ้น โดยเฉพาะในกรณีละเมิดการประมวลผลข้อมูลที่โอนจากสหภาพยุโรปมายังญี่ปุ่น ซึ่งผู้ประกอบการจะต้องปฏิบัติตามคำแนะนำของหน่วยงานคุ้มครองข้อมูล และไม่สามารถอ้างเหตุผลใดๆ ที่จะไม่ปฏิบัติตามได้ ยกเว้นกรณีภัยธรรมชาติ หรือผู้ประกอบการได้ปรับปรุงแก้ไขด้วยวิธีการอื่นแล้วเท่านั้น

นอกจากนี้ ญี่ปุ่นยังได้จัดทำมาตรการป้องกันเพิ่มเติมสำหรับการใช้ข้อมูลส่วนบุคคลที่โอนมาจาก EU โดยหน่วยงานภาครัฐ ซึ่งรวมถึงการปฏิบัติงานของตำรวจ และหน่วยงานด้านความมั่นคงอื่น ๆ โดยจำกัดการเข้าถึงและการใช้ข้อมูลโดยหน่วยงานภาครัฐ ตามความจำเป็นและสมเหตุสมผล (necessary and proportionate) เท่านั้น โดยเจ้าของข้อมูลในสหภาพยุโรปสามารถฟ้องร้องหน่วยภาครัฐได้หากพบกรณีละเมิด

ดังนั้น จะเห็นได้ว่าประเทศญี่ปุ่นไม่ได้มีกฎหมายที่เกี่ยวข้องหรือมาตรการที่ออกมาเพื่อควบคุมการซื้อขายข้อมูลโดยนายหน้าข้อมูล แต่มีมาตรการในการยกระดับข้อมูลแบบอ่อนไหวภายใต้กฎระเบียบ GDPR ให้ได้รับการคุ้มครองแบบพิเศษ ตามกฎหมาย APPI จึงเป็นการเพิ่มความปลอดภัยให้กับข้อมูลส่วนบุคคลของประชากรญี่ปุ่นเพิ่มมากขึ้น ทำให้เจ้าของข้อมูลได้รับความเสียหายจากการกระทำของนายหน้าข้อมูลอย่างน้อยที่สุด

3.2.3 ประเทศสิงคโปร์

ระบบกฎหมายของสิงคโปร์ได้รับอิทธิพลจากระบบ กฎหมายจารีตประเพณีของอังกฤษอย่างมีนัยสำคัญ อันเป็นผลมาจากประวัติศาสตร์การเป็นอาณานิคมของอังกฤษเป็นระยะเวลากว่า 150 ปี (พ.ศ. 2362-2506) อย่างไรก็ดี เนื่องจากบริบทในอังกฤษและสิงคโปร์มีการเปลี่ยนแปลงไปตามสภาพแวดล้อมทั้งในและต่างประเทศ ทำให้สิงคโปร์มีการยกเลิกกฎหมายบางฉบับที่ได้รับมาจากอังกฤษ และพัฒนากฎหมายที่มีความเหมาะสมกับบริบทของประเทศสิงคโปร์เอง ในส่วนนี้จึงแบ่งการนำเสนอออกเป็น 2 ส่วน คือ ภาพรวมของระบบกฎหมายจารีตประเพณี และภาพรวมของกฎหมายที่สิงคโปร์พัฒนาขึ้นเอง[24]

การคุ้มครองข้อมูลส่วนบุคคลสำหรับประเทศสิงคโปร์นั้น ได้มีการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล หรือ Personal Data Protection Act: PDPA เช่นเดียวกับของประเทศไทย ซึ่งได้ประกาศใช้ตั้งแต่ปี พ.ศ. 2555 และมีการบังคับใช้อย่างเต็มรูปแบบในปี พ.ศ. 2556 โดยมีระยะเวลาเตรียมความพร้อมถึง 18 เดือนด้วยกัน โดยระหว่างนั้นได้มีการจัดอบรม เผยแพร่ความรู้ เพื่อเตรียมความพร้อมให้กับภาคเอกชนและประชาชนอย่างต่อเนื่อง เพื่อสร้างความเข้าใจอันดีเกี่ยวกับข้อดีของ Personal Data Protection Act ที่จะมีผลบังคับใช้ภายในประเทศ โดยมีคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Commission ('PDPC')) ซึ่งเป็นหน่วยงานกำกับดูแลด้านการคุ้มครองข้อมูล

---

[24] สถาบันวิจัยเพื่อการพัฒนาประเทศไทย, *กฎหมายของประเทศสิงคโปร์และข้อกฎหมายที่เกี่ยวข้องกับการค้าและการลงทุนของประเทศสิงคโปร์* (สำนักงานคณะกรรมการกฤษฎีกา 2557) 1-9.

แม้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์ (Personal Data Protection Act 2012) จะได้ ประกาศใช้ตั้งแต่วันที่ 7 ธันวาคม ค.ศ. 2012 แต่การมีผลบังคับใช้กฎหมายทุกบทบัญญัติยังไม่เกิดขึ้นทันที กฎหมายฉบับนี้เพิ่งมีผลบังคับใช้อย่างสมบูรณ์เมื่อวันที่ 2 กรกฎาคม ค.ศ. 2014 ซึ่งจะเห็นได้ว่าระยะเวลา ที่หน่วยงานรัฐของสิงคโปร์ได้ใช้เตรียมพร้อมกินเวลานานถึง 18 เดือน (1 ปี 6 เดือน) ทั้งนี้การใช้เวลานาน เช่นนี้มักจะไม่พบในการประกาศใช้กฎหมายของประเทศไทย เพราะที่ผ่านมาระยะเวลาที่พบส่วนใหญ่จะน้อยกว่า 1 ปี ซึ่งการให้เวลาเตรียมพร้อมนานขนาดนี้สามารถวิเคราะห์ถึงเหตุผลสำคัญของกฎหมายที่เห็นว่า เรื่องนี้เป็นเรื่องใหม่ที่กระทบกับองค์กรธุรกิจจำนวนมาก ไม่ใช่เพียงที่ตั้งอยู่ประเทศสิงคโปร์เท่านั้น แต่รวมถึงบริษัทต่างชาติอื่นๆ ที่อยู่ในต่างประเทศที่อาจมีการส่งต่อข้อมูลจากสิงคโปร์ไปยังประเทศที่สาม ต้องปฏิบัติ ตามมาตรการของกฎหมาย Personal Data Protection Act ด้วย จึงจำเป็นต้องสร้างความเข้าใจที่ถูกต้องให้เกิดขึ้น[25]

ใน PERSONAL DATA PROTECTION ACT 2012 ได้ให้ความหมายของข้อมูลส่วนบุคคลไว้ว่า

“ข้อมูลส่วนบุคคล” หมายถึง ข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นจริงหรือไม่ก็ตามเกี่ยวกับบุคคลที่สามารถระบุตัวตนได้

(ก) จากข้อมูลนั้น หรือ

(ข) จากข้อมูลนั้นและข้อมูลอื่น ๆ ที่องค์กรมีหรือมีแนวโน้มที่จะเข้าถึงได้[26]

โดยมีตัวกลางข้อมูล “ตัวกลางข้อมูล” หมายถึง องค์กรที่ประมวลผลข้อมูลส่วนบุคคลในนามขององค์กร แต่ไม่รวมถึงพนักงานขององค์กรนั้นๆ[27] เป็นผู้ประมวลผลข้อมูลส่วนบุคคล ที่ได้รับข้อมูลส่วนบุคคลมาโดยวิธีการตามที่ Personal Data Protection Act 2012 กำหนดดังนี้ “การได้รับข้อมูลส่วนบุคคล”

(ก) หมายถึง ข้อมูลส่วนบุคคลเกี่ยวกับบุคคลที่องค์กรได้มาจากข้อมูลส่วนตัวอื่นๆ เกี่ยวกับบุคคลหรือบุคคลอื่นๆ ที่อยู่ในความครอบครองหรืออยู่ภายใต้การควบคุมขององค์กร แต่

(ข) ไม่รวมถึงข้อมูลส่วนบุคคลที่ได้รับจากองค์กรโดยใช้วิธีการหรือวิธีการที่กำหนด[28]

---

[25] กิตติพงศ์ กมลธรรมวงศ์, ‘ประสบการณ์ของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศสาธารณรัฐสิงคโปร์ : บทเรียนสำหรับประเทศไทย’ (2563) 2 วารสารสังคมวิจัยและพัฒนา 2, 19.

[26] PERSONAL DATA PROTECTION ACT 2012 2. (1) : “personal data” means data, whether true or not, about an individual who can be identified

(a) from that data; or

(b) from that data and other information to which the organisation has or is likely to have access;

[27] PERSONAL DATA PROTECTION ACT 2012 2. (1) : ‘data intermediary’ means an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation;

[28] PERSONAL DATA PROTECTION ACT 2012 2. (1) : “derived personal data” —

“การประมวลผล” ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล หมายถึง การดำเนินการใดๆหรือชุดการดำเนินการใด ๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล และรวมถึงสิ่งต่อไปนี้:

(ก) การบันทึก;

(ข) โฮลดิ้ง;

(ค) องค์กร การปรับตัวหรือการเปลี่ยนแปลง;

(ง) การค้นคืน;

(จ) การผสมผสาน;

(ฉ) การส่งผ่าน;

(ช) ลบหรือทำลาย;[29]

“การดำเนินคดี” หมายถึง การดำเนินคดีทางแพ่ง ทางอาญา หรือทางปกครอง โดยศาลหรือต่อหน้าศาล ซึ่งศาลหรือหน่วยงานกำกับดูแลที่เกี่ยวข้องกับข้อกล่าวหาของ —

(ก) การละเมิดข้อตกลง;

(ข) การฝ่าฝืนกฎหมายหรือจรรยาบรรณทางวิชาชีพหรือข้อกำหนดอื่น ๆ ที่กำหนดโดยหน่วยงานกำกับดูแล ในการใช้อำนาจภายใต้กฎหมายลาย หรือ

(ค) ความผิดหรือการละเมิดหน้าที่ที่เรียกร้องค่าชดเชยตามกฎหมายใด ๆ[30]

(a) means personal data about an individual that is derived by an organisation in the course of business from other personal data, about the individual or another individual, in the possession or under the control of the organisation; but

(b) does not include personal data derived by the organisation using any prescribed means or method;

[29] PERSONAL DATA PROTECTION ACT 2012 2. (1) : “processing”, in relation to personal data, means the carrying out of any operation or set of operations in relation to the personal data, and includes any of the following:

(a) recording;

(b) holding;

(c) organization, adaptation or alteration;

(d) retrieval;

(e) combination;

(f) transmission;

(g) erasure or destruction;

[30] PERSONAL DATA PROTECTION ACT 2012 2. (1) : “proceedings” means any civil, criminal or administrative proceedings by or before a court, tribunal or regulatory authority that is related to the allegation of —

โดยใน Personal Data Protection Act 2012 ไม่ได้ระบุความหมายของนายหน้าข้อมูล หรือความหมายของสถานะบุคคลไว้โดยตรง โดนส่วนใหญ่แล้วจะเป็นการดำเนินการต่าง ๆ ที่สอดคล้องกับการดำเนินการอันเกี่ยวกับข้อมูลส่วนบุคคล

Personal Data Protection Act 2012 มีการกำหนด โดยจำกัดองค์กรต่าง ๆ ไม่ว่าจะเป็นภาครัฐหรือเอกชนไม่ให้ถ่ายโอนข้อมูลส่วนบุคคลออกนอกประเทศสิงคโปร์หรือเรียกอีกอย่างหนึ่งว่า ข้อผูกพันในการจำกัดการโอน (Transfer Limitation obligation) เว้นแต่จะมีการป้องกันที่กำหนดไว้อย่างน้อยหนึ่งอย่างเพื่อให้แน่ใจว่าผู้รับข้อมูลจะให้มาตรฐานการป้องกันการถ่ายโอน ข้อมูลส่วนบุคคลที่เทียบเท่ากับการคุ้มครองภายใต้ PDPA ข้อบังคับยังระบุขั้นตอนที่องค์กรอาจดำเนินการเพื่อให้แน่ใจว่าผู้รับข้อมูลส่วนบุคคลในต่างประเทศจะต้องถูกผูกมัดที่จะต้องบังคับตามกฎหมายเพื่อให้มีมาตรฐานการป้องกันข้อมูลส่วนบุคคลที่เทียบเท่ากับข้อมูลส่วนบุคคลที่ถ่ายโอนไป

ทั้งนี้ ในพระราชบัญญัติได้มีการกำหนดกลไกและวิธีการการถ่ายโอนข้อมูลส่วนบุคคลที่เกิดขึ้นภายในประเทศจะต้องมีองค์ประกอบที่รวมถึง

1. มีความยินยอมจากเจ้าของของข้อมูลของแต่ละบุคคล โดยมีเงื่อนไขว่าได้ดำเนินการตามขั้นตอนที่กำหนดไว้ในการได้รับความยินยอมดังกล่าว
2. จะต้องมีข้อสัญญาที่มีผลผูกพันทางกฎหมายเพื่อกำหนดภาระหน้าที่ในการปกป้องข้อมูลให้กับเจ้าข้องข้อมูลส่วนบุคคล
3. การถ่ายโอนข้อมูลจะต้องทำตามสัญญาที่ได้ตกลงกันไว้(Singapore Statutes Online, 2022)

ดังนี้ ในการกำหนดวิธีการแบ่งปันข้อมูลส่วนบุคคลของประเทศสิงคโปร์ได้แบ่งวิธีการโอนข้อมูลส่วนบุคคลออกเป็น 2 ลักษณะ คือ 1. มาตรการคุ้มครองข้อมูลส่วนบุคคลภายในประเทศ 2. มาตรการแบ่งปันข้อมูลส่วนบุคคลให้กับต่างประเทศ ซึ่งหลักการสำคัญของทั้ง 2 มาตรการในการแบ่งปันข้อมูลส่วนบุคคลทั้ง 2 วิธี คือจะต้องมีการขอความยินยอมหรืออนุญาตจากเจ้าของข้อมูลส่วนบุคคลก่อนจึงจะสามารถทำการแบ่งปันข้อมูลส่วนบุคคลได้[31]

นอกจากนี้ ประเทศสิงคโปร์ยังมีการจัดตั้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์ หรือ Personal Data Protection Commission ซึ่งถือเป็นอีกหนึ่งข้อดีของการนำ Personal Data Protection Act 2012 เข้ามาบังคับใช้ โดย Personal Data Protection Commission จะเข้ามามีบทบาท

(a) a breach of an agreement;

(b) a contravention of any written law or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written law; or

(c) a wrong or a breach of a duty for which a remedy is claimed under any law;

[31] พงษ์มนัส ดือด,พระครูวินัยธรวรชัด ปยุตฺโต,ปาริฉัตร ไชยเดช,พระมหาชัยชนะ บุญนาดี (เชิงอรรถ 23), 133-134.

ในเรื่องการให้คำปรึกษา รวมถึงให้ความช่วยเหลือตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้ระบุเอาไว้ นอกจากนี้ยังจะเป็นการช่วยสร้างความตระหนักให้เห็นถึงความสำคัญของข้อมูลส่วนบุคคลและการปกป้องข้อมูลเหล่านั้นอย่างเต็มที่ Personal Data Protection Commission เป็นการบังคับใช้เฉพาะภาคเอกชนเท่านั้น ในการขอความยินยอม ในการจัดเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล จะเป็นการขอความยินยอมเฉพาะจุดประสงค์และความยินยอม เฉพาะที่เจ้าของข้อมูลให้การอนุญาต

การให้ความคุ้มครองข้อมูลส่วนบุคคลจะต้องคำนึงถึงความต้องการในการปกป้องความเป็นส่วนตัวของบุคคลและความต้องการขององค์กรในการนำข้อมูลเพื่อวัตถุประสงค์ที่ชอบด้วยกฎหมายและให้ความคุ้มครองข้อมูลทั้งที่มีการจัดเก็บในรูปแบบอิเล็กทรอนิกส์และไม่ใช่อิเล็กทรอนิกส์

ดังนั้น จะเห็นได้ว่าประเทศสิงคโปร์ไม่มีกฎหมายหรือมาตรการเพื่อออกมาควบคุมการซื้อขายข้อมูลโดยนายหน้าข้อมูล ส่งผลให้การซื้อขายข้อมูลโดยนายหน้าข้อมูลยังคงมีอยู่และอาจส่งผล กระทบต่อประชากรสิงคโปร์เกี่ยวกับความเป็นส่วนตัวมากขึ้น

3.3 การคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายไทย

ประเทศไทยเราในปัจจุบันมีกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลหลากหลายฉบับด้วยกัน ซึ่งแต่ละฉบับนั้นก็มีเนื้อหาที่แตกต่างกันไป ตามความประสงค์ หรือตามประเภทแต่ละฉบับซึ่งในเนื้อหาใจความ ซึ่งแต่ละฉบับนั้นมีเนื้อหาที่คล้ายๆ กันคือ การมุ่งคุ้มครองข้อมูลส่วนบุคคล ในแต่ละกรณีต่างๆ และมีพระราชบัญญัติข้อมูลส่วนบุคคล พ.ศ. 2562 ที่พึ่งประกาศบังคับใช้เมื่อวันที่ 1 มิถุนายน พ.ศ. 2565 ที่ผ่านมา กฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยนั้น เป็นกฎหมายที่จะบ่งบอกถึงสถานของบุคคลต่างๆในการกระทำการต่างๆ หรือการใช้สิทธิที่ตนเองมีอยู่ หรือการที่ปกป้องสิทธิของตนเองที่ถูกผู้อื่นกระทำ ส่วนมากก็จะเป็นการคุ้มครองสิทธิของตนเองเพื่อไม่ให้ผู้อื่นมากระทำละเมิด โดยเป็นกฎหมายที่มีบทบัญญัติไว้ในการคุ้มครองข้อมูลส่วนบุคคลเป็นบางกรณีเท่านั้น ซึ่งยังไม่ครอบคลุมข้อมูลส่วนบุคคลทั้งหมด

3.3.1 รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560

ประเทศไทยเรานั้นได้มีการรับรอง “สิทธิรับรู้ข้อมูลราชการ” และ “สิทธิที่จะได้รับความคุ้มครองในข้อมูลส่วนบุคคล” อย่างจริงจัง โดยการเกิดขึ้นของ “พ.ร.บ.ข้อมูลข่าวสารของราชการ พ.ศ. 2540” เมื่อเกือบยี่สิบปีก่อน ทั้งยังได้รับการยืนยันรับรองโดยรัฐธรรมนูญแห่งราชอาณาจักรไทยทั้งฉบับปี พ.ศ. 2540 และปีพ.ศ. 2550 โดยในส่วนของข้อมูลส่วนบุคคลนั้น รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540[32] ได้กำหนด

[32] นคร เสรีรักษ์. ‘ความเป็นส่วนตัวภายใต้รัฐธรรมนูญใหม่ "ต้องจับตา"’. <https://www.ilaw.or.th/node/4255> สืบค้นเมื่อ 10 กันยายน 2565.

ไว้ในมาตรา 34[33] ส่วนรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550 ประเด็นการคุ้มครองข้อมูลส่วนบุคคลปรากฏอยู่ในหมวด 3 ส่วนที่ 3 ซึ่งว่าด้วยสิทธิและเสรีภาพส่วนบุคคล มาตรา 35[34] สำหรับรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 ประเด็นการคุ้มครองข้อมูลส่วนบุคคล รัฐธรรมนูญได้บัญญัติรับรองไว้ใน หมวด 1 บททั่วไป มาตรา 4[35] และปรากฏอยู่ในหมวด 3 ว่าด้วยสิทธิและเสรีภาพของปวงชนชาวไทย โดยได้กล่าวไว้ใน มาตรา 25[36] มาตรา 32[37] ซึ่งมีเนื้อหาเน้นในเรื่องของสิทธิในความเป็นมนุษย์ ซึ่งหากบุคคลใดถูกละเมิด

---

[33] รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 มาตรา 34 “สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัว ย่อมได้รับความคุ้มครอง

การกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชน อันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัว จะกระทำมิได้ เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณชน”

[34] รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550 มาตรา 35 “สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง ตลอดจนความเป็นอยู่ส่วนตัว ย่อมได้รับความคุ้มครอง

การกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชน อันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัว จะกระทำมิได้ เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณะ

บุคคลย่อมมีสิทธิได้รับความคุ้มครองจากการแสวงประโยชน์โดยมิชอบจากข้อมูลส่วนบุคคลที่เกี่ยวกับตน ทั้งนี้ตามที่กฎหมายบัญญัติ”

[35] รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 มาตรา 4 “มาตรา 4 ศักดิ์ศรีความเป็นมนุษย์ สิทธิ เสรีภาพ และความเสมอภาคของบุคคลย่อมได้รับความคุ้มครอง

ปวงชนชาวไทยย่อมได้รับความคุ้มครองตามรัฐธรรมนูญเสมอกัน”

[36] รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 มาตรา 25 “สิทธิและเสรีภาพของปวงชนชาวไทย นอกจากที่บัญญัติคุ้มครองไว้เป็นการเฉพาะในรัฐธรรมนูญแล้ว การใดที่มิได้ห้ามหรือจำกัดไว้ในรัฐธรรมนูญหรือในกฎหมายอื่น บุคคลย่อมมีสิทธิและเสรีภาพที่จะทำการนั้นได้และได้รับความคุ้มครองตามรัฐธรรมนูญ ตราบเท่าที่การใช้สิทธิหรือเสรีภาพเช่นว่านั้นไม่กระทบกระเทือนหรือเป็นอันตรายต่อความมั่นคงของรัฐ ความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน และไม่ละเมิดสิทธิหรือเสรีภาพของบุคคลอื่น

สิทธิหรือเสรีภาพใดที่รัฐธรรมนูญให้เป็นไปตามที่กฎหมายบัญญัติ หรือให้เป็นไปตามหลักเกณฑ์และวิธีการที่กฎหมายบัญญัติ แม้ยังไม่มีการตรากฎหมายนั้นขึ้นใช้บังคับ บุคคลหรือชุมชนย่อมสามารถใช้สิทธิหรือเสรีภาพนั้นได้ตามเจตนารมณ์ของรัฐธรรมนูญ

บุคคลซึ่งถูกละเมิดสิทธิหรือเสรีภาพที่ได้รับความคุ้มครองตามรัฐธรรมนูญ สามารถยกบทบัญญัติแห่งรัฐธรรมนูญเพื่อใช้สิทธิทางศาลหรือยกขึ้นเป็นข้อต่อสู้คดีในศาลได้

บุคคลซึ่งได้รับความเสียหายจากการถูกละเมิดสิทธิหรือเสรีภาพหรือจากการกระทำความผิดอาญาของบุคคลอื่นย่อมมีสิทธิที่จะได้รับการเยียวยาหรือช่วยเหลือจากรัฐตามที่กฎหมายบัญญัติ”

[37] รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 มาตรา 32 “บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว

สิทธิหรือเสรีภาพที่รัฐธรรมนูญรับรองไว้ สามารถยกบทบัญญัติแห่งรัฐธรรมนูญเพื่อใช้สิทธิทางศาลหรือยกขึ้นเป็นข้อต่อสู้คดีในศาลได้ ถ้าหากมีการละเมิด หรือการกระทำการ อันเป็นการกระทบสิทธิของบุคคล รวมถึงการนำข้อมูลส่วนบุคคลไปใช้ไม่ว่าในทางใด ๆ จะกระทำมิได้ เว้นแต่ อาศัยอำนาจแห่งกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ

3.3.2 ประมวลกฎหมายอาญา

การคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายอาญา มีอยู่ใน 2 หมวด คือ ลักษณะ 11 หมวด 2 ความผิดฐานเปิดเผยความลับและหมวด 3 ความผิดฐานหมิ่นประมาท ไว้ดังนี้[38] ความผิดฐานเปิดเผยความลับตาม มาตรา 322 คือการที่ผู้ใดเปิดผนึกหรือเอาจดหมาย โทรเลข หรือเอกสารใดๆ ซึ่งปิดผนึกของผู้อื่นไป เพื่อล่วงรู้ข้อความก็ดี เพื่อนำข้อความในจดหมายโทรเลขหรือเอกสารเช่นว่านั้นออกเปิดเผยก็ดี ถ้าการกระทำนั้นน่าจะเกิดความเสียหายแก่ผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งพันบาท หรือทั้งจำทั้งปรับมาตรา 322 อยู่ในหมวด 2 ลักษณะ 11 ว่าด้วยความผิดฐานเปิดเผยความลับ มีเจตนารมณ์เพื่อคุ้มครองสิทธิส่วนตัวหรือความลับของบุคคลจากการสื่อข้อมูลข่าวสาร การเปิดผนึกหรือเอาไปอย่างใดอย่างหนึ่งหรือทั้งสองอย่าง ซึ่งเอกสาร จดหมายหรือโทรเลขที่ปิดผนึกไว้ของผู้อื่น และการกระทำนั้นน่าจะเกิดความเสียหายแก่ผู้หนึ่งผู้ใดด้วย นอกจากเจตนาธรรมดาแล้ว ความผิดตามมาตรานี้ยังต้องการเจตนาพิเศษหรือมูลเหตุจูงใจ 2 ประการ คือ เพื่อล่วงรู้ข้อความในเอกสารนั้น และเพื่อนำข้อความนั้นออกเปิดเผย ถ้ามีเจตนาดังกล่าวถึงแม้จะยังไม่รู้ข้อความในจดหมายหรือยังไม่ได้นำข้อความไปเปิดเผยก็ถือว่าความผิดสำเร็จแล้วเพราะมาตรานี้ได้บัญญัติเพียงว่า “เพื่อ” เท่านั้น แค่เพียงมีเจตนากระทำก็ถือว่ามีความผิดแล้ว

ความผิดฐานเปิดเผยความลับจากการเป็นเจ้าหน้าที่หรือมีอาชีพ ตามมาตรา 323 โดยผู้ใดล่วงรู้หรือได้มาซึ่งความลับของผู้อื่น โดยเหตุที่เป็นเจ้าพนักงานผู้มีหน้าที่ โดยเหตุที่ประกอบอาชีพเป็นแพทย์ เภสัชกร คนจำหน่ายยา นางผดุงครรภ์ ผู้พยาบาล นักบวช หมอความ ทนายความ หรือผู้สอบบัญชีหรือโดยเหตุที่เป็นผู้ช่วยในการประกอบ อาชีพนั้น แล้วเปิดเผยความลับนั้น ในประการที่น่าจะเกิดความเสียหาย แก่ผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกิน หนึ่งพันบาท หรือทั้งจำทั้งปรับ

ความผิดฐานหมิ่นประมาทมาตรา 326 คือการที่ผู้ใดใส่ความผู้อื่นต่อบุคคลที่สาม โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชังนั้น บุคคลผู้กระทำนั้นต้องได้รับโทษ แต่อย่างไรก็ดีความผิดฐานหมิ่นประมาทนั้น ได้มีการกำหนดข้อยกเว้นเอาไว้ในมาตรา 329 ซึ่งก็คือการแสดงความคิดเห็นหรือข้อความใดโดยสุจริตนั้นไม่ถือว่าเป็นความผิด เช่นการทำเพื่อความชอบธรรม ป้องกันตนหรือป้องกันส่วน

การกระทำอันเป็นการละเมิดหรือกระทบต่อสิทธิของบุคคลตามวรรคหนึ่ง หรือการนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใด ๆ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ”

[38] จันทร์ทิพย์ แสงแปง, ‘ปัญหาการคุ้มครองข้อมูลส่วนบุคคล ศึกษากรณี การจัดเก็บข้อมูลส่วนบุคคลในหน่วยงานเอกชน’ (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต สถาบันบัณฑิตพัฒนศาสตร์ 2559) 73.

ได้เสียเกี่ยวกับตนตามคลองธรรม การทำในฐานะเป็นเจ้าพนักงานปฏิบัติการตามหน้าที่ การติชม ด้วยความเป็นธรรม ซึ่งบุคคลหรือสิ่งใดอันเป็นวิสัยของประชาชนย่อมกระทำ หรือการแจ้งข่าวด้วยความเป็นธรรม เรื่องการดำเนินการอันเปิดเผยในศาลหรือในการประชุม การกระทำเหล่านี้นั้นเป็นข้อยกเว้นว่า ไม่มีความผิดฐานหมิ่นประมาท

ตามประมวลกฎหมายอาญาโดยส่วนใหญ่ จะมีลักษณะเน้นไปในทางป้องกันก่อนที่ความผิดหรือความเสียหายจะเกิดขึ้น มีเจตนารมณ์เพื่อที่จะคุ้มครองสิทธิส่วนบุคคล หรือข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลความลับของบุคคลจากการที่ได้ล่วงรู้ข้อมูลส่วนบุคคล หรือได้ข้อมูลส่วนบุคคลมาเพราะเหตุที่ตนเป็นเจ้าพนักงานผู้มีหน้าที่ในการประกอบอาชีพนั้นๆ เช่น เป็นหมอ เป็นทนาย นักบวช ซึ่งหากมีการเปิดเผยความลับหรือ หรือการล่วงรู้ความลับ หรือการใส่ความต่างๆ โดยประการที่จะเกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคล หรือแม้กระทั่งผู้อื่นตามประมวลกฎหมายอาญาก็ถือว่ามีความผิดแล้ว

3.3.3 ประมวลกฎหมายแพ่งและพาณิชย์

การคุ้มครองข้อมูลส่วนบุคคลตามหลักกฎหมายแพ่งและพาณิชย์นั้นเป็นการมุ่งคุ้มครองในลักษณะที่จะเป็นการเยียวยาแก้ไข ในสิ่งที่บุคคลผู้นั้นได้กระทำลงไปโดยละเมิด โดยให้มีการใช้ค่าสินไหมทดแทนแก่บุคคลผู้ที่ได้รับความเสียหายนั้นๆ โดยมีมาตรา 420 เป็นหลักการทั่วไปในการให้ความคุ้มครองสิทธิส่วนบุคคล คือ

มาตรา 420 นั้นเป็นการที่ผู้ใดจงใจหรือประมาทเลินเล่อ ทำต่อบุคคลอื่นโดยผิดกฎหมายให้เขาเสียหายถึงแก่ชีวิตก็ดี แก่ร่างกายก็ดี อนามัยก็ดี เสรีภาพก็ดี ทรัพย์สินหรือสิทธิอย่างหนึ่งอย่างใดก็ดี ถือว่า ผู้นั้นทำละเมิด จำต้องใช้ค่าสินไหมทดแทนเพื่อการนั้น อย่างไรก็ดี นอกจากการคุ้มครองตามมาตรา 420 แล้วยังมีการคุ้มครองสิทธิส่วนบุคคลตามมาตรา 423 อีกด้วย ซึ่งเป็นการคุ้มครองข้อมูลส่วนบุคคลในเรื่องชื่อเสียงหรือเกียรติคุณ คือตามมาตรา 423 นั้นคือผู้ใดกล่าวหรือไขข่าวแพร่หลาย ซึ่งข้อความอันฝ่าฝืน ต่อความจริงเป็นที่เสียหายแก่ชื่อเสียงหรือเกียรติคุณของบุคคลอื่น หรือเป็นที่เสียหายแก่ทางทำมาหาได้ หรือทางเจริญของเขาโดย ประการอื่น บุคคลจะต้องใช้ค่าสินไหมทดแทนให้แก่เขาเพื่อความเสียหายอย่างใดๆอันเกิดแต่การนั้น ซึ่งถึงแม้ว่าตนไม่ได้รู้ว่าข้อความนั้นไม่จริงนั้น แต่หากควรจะรู้ได้ รวมไปถึงผู้ส่งข่าวสารด้วย

ในส่วนของคำว่า “นายหน้า” นั้นมีปรากฏอยู่ในประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 845[39] ซึ่งการที่บุคคลหนึ่งจะต้องอาศัยนายหน้าเข้าทำการชี้ช่องให้มีการทำสัญญากัน แทนที่จะเข้าทำสัญญากับบุคคลใด ๆ โดยตรงนั้น ก็อาจเป็นเพราะว่าบุคคลดังกล่าวอาจไม่ทราบหรือไม่สามารถจะติดต่อบุคคลอื่นใดให้เข้ามาทำสัญญากับตนได้ เพราะถ้าบุคคลนี้ทราบก็คงไม่ต้องอาศัยนายหน้าเข้ามาชี้ช่องให้ นายหน้าจึงเปรียบเสมือนคนกลางที่ทำให้บุคคลทั้งสองฝ่ายที่ต้องการทำสัญญากันมาพบ มารู้จัก และมาทำสัญญาใน

---

[39] ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 845 “บุคคลผู้ใดตกลงจะให้ค่าบำเหน็จแก่นายหน้าเพื่อที่ชี้ช่องให้ได้เข้าทำสัญญาก็ดี จัดการให้ได้ทำสัญญากันก็ดี ท่านว่าบุคคลผู้นั้นจะต้องรับผิดใช้ค่าบำเหน็จก็ต่อเมื่อสัญญานั้นได้ทำกันสำเร็จเนื่องแต่ผลแห่งการที่นายหน้าได้ชี้ช่องหรือจัดการนั้น ถ้าสัญญาที่ได้ทำกันไว้นั้นมีเงื่อนไขเป็นเงื่อนบังคับก่อนไซร้ ท่านว่าจะเรียกร้องบำเหน็จค่านายหน้ายังหาได้ไม่ จนกว่าเงื่อนไขนั้นสำเร็จแล้ว”

ระหว่างกัน ส่วนทางด้านตัวของนายหน้าเองจะทำการเป็นนายหน้าก็เพื่อเป็นการช่วยเหลือบุคคลผู้ที่ต้องการจะทำสิ่งใดสิ่งหนึ่งให้สามารถทำการตามประสงค์ได้ ไม่ว่านายหน้าจะหวังบำเหน็จนายหน้าเป็นการตอบแทนหรือไม่ เพราะอาจจะเป็นเพื่อนหรือเป็นญาติก็ได้ แต่ส่วนใหญ่แล้วนายหน้ามักทำการด้วยประสงค์ที่จะได้รับค่าบำเหน็จโดยเฉพาะนายหน้าในการซื้อขายอสังหาริมทรัพย์ นายหน้าจัดหางาน หรือนายหน้าเกี่ยวกับการเช่าอสังหาริมทรัพย์

บุคคลที่ตกลงว่าจะเป็นคนกลางในการทำหน้าที่ชี้ช่องทางหรือจัดการให้บุคคลอีกคนหนึ่งซึ่งเรียกว่าตัวการได้เข้าทำสัญญากับบุคคลภายนอก โดยบุคคลที่เป็นตัวการนั้นตกลงจะให้ค่าตอบแทนที่เรียกว่า “บำเหน็จ” แก่คนกลางที่เรียกว่า “นายหน้า” ในการทำหน้าที่ดังกล่าว ดังนั้นการที่ตัวการได้เข้าทำสัญญากับบุคคลภายนอกอันเป็นผลโดยตรงมาจากการที่มีคนกลางซึ่งเป็นนายหน้าได้ทำหน้าที่ในการชี้ช่องทางหรือจัดการให้บุคคลภายนอกนั้นได้เข้าทำสัญญากับตัวการแล้ว เพียงเท่านี้คนกลางที่เรียกว่า “นายหน้า” นั้นก็มีสิทธิได้รับค่าตอบแทนที่เรียกว่า “ค่าบำเหน็จ” หรือที่เราเรียกกันโดยทั่วไปว่า “ค่านายหน้า” จากตัวการตามที่ได้มีการตกลงกันไว้

3.3.4 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ Personal Data Protection Act, B.E. 2562 (2019) ที่มีผลบังคับใช้ทั้งฉบับในวันที่ 1 มิถุนายน พ.ศ. 2565 นั้น กล่าวถึงรายละเอียดการเก็บรวบรวมข้อมูลส่วนบุคคลไว้ เป็นสิ่งที่ใกล้ตัวเรามากกว่าที่คิด เพราะไม่ว่าเราจะอยู่ในฐานะที่เป็น ลูกค้า พนักงาน หรือผู้รับผิดชอบดูแลงานในนิติบุคคล ก็ล้วนต้องเกี่ยวข้องกับข้อมูลส่วนบุคคลตามพระราชบัญญัติฉบับนี้ด้วยกันทุกคน สาระสำคัญของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล คือ การให้ความคุ้มครองข้อมูลเกี่ยวกับบุคคลที่ทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม อาจเป็นได้ทั้งรูปแบบออนไลน์และออฟไลน์ เช่น ชื่อ-สกุล ที่อยู่ เลขบัตรประชาชน เบอร์ติดต่อ อีเมล การศึกษา ประวัติการทำงาน ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม รวมถึงไปถึง ลายนิ้วมือ แผ่นบันทึกลักษณะเสียง เป็นต้น ทั้งนี้ วัตถุประสงค์ของการเก็บรักษาข้อมูลส่วนบุคคลก็เพื่อป้องกันการละเมิดสิทธิความเป็นส่วนตัวของเจ้าของข้อมูล ที่อาจนำมาซึ่งความเดือดร้อนรำคาญหรือสร้างความเสียหายได้

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 “ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ[40] โดยมีผู้ควบคุมข้อมูลเป็นผู้ที่มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และมีผู้ประมวลผลข้อมูลเป็นผู้ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูล แต่ผู้ประมวลผลข้อมูลไม่เป็นผู้ควบคุมข้อมูล

มาตรา 6 ได้ให้ความหมายของผู้ควบคุมข้อมูล และผู้ประมวลผลข้อมูลไว้ ดังนี้

---

[40] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 6 “ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งมือ านาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามค าสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งด าเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

“ มาตรา 19 ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น เว้นแต่บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้”

การขอความยินยอมต้องทำโดยชัดแจ้ง เป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เว้นแต่โดยสภาพไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้

ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไปด้วย และการขอความยินยอมนั้นต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน มีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ รวมทั้งใช้ภาษาที่อ่านง่าย และไม่เป็นการหลอกลวงหรือทาให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ดังกล่าว ทั้งนี้ คณะกรรมการจะให้ผู้ควบคุมข้อมูลส่วนบุคคลขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามแบบและข้อความที่คณะกรรมการประกาศกำหนดก็ได้

ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องคำนึงอย่างถึงที่สุดในความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม ทั้งนี้ ในการเข้าทำสัญญาซึ่งรวมถึงการให้บริการใด ๆ ต้องไม่มีเงื่อนไขในการให้ความยินยอมเพื่อเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่มีความจำเป็นหรือเกี่ยวข้องสำหรับการเข้าทำสัญญาซึ่งรวมถึงการให้บริการนั้น ๆ

เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเสียเมื่อใดก็ได้โดยจะต้องถอนความยินยอมได้ง่ายเช่นเดียวกับการให้ความยินยอม เว้นแต่มีข้อจำกัดสิทธิในการถอนความยินยอมโดยกฎหมายหรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล ทั้งนี้ การถอนความยินยอมย่อมไม่ส่งผลกระทบต่อการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมไปแล้วโดยชอบตามที่กำหนดไว้ในหมวดนี้

ในกรณีที่การถอนความยินยอมส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลในเรื่องใด ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงผลกระทบจากการถอนความยินยอมนั้นการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลที่ไม่เป็นไปตามที่กำหนดไว้ในหมวดนี้ ไม่มีผลผูกพันเจ้าของข้อมูลส่วนบุคคล และไม่ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถทำการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้”

“ มาตรา 21 ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งเจ้าของข้อมูลส่วนบุคคลไว้ก่อนหรือในขณะที่เก็บรวบรวม

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่แตกต่างไปจากวัตถุประสงค์ที่ได้แจ้งไว้ตามวรรคหนึ่งจะกระทำมิได้ เว้นแต่

(1) ได้แจ้งวัตถุประสงค์ใหม่นั้นให้เจ้าของข้อมูลส่วนบุคคลทราบและได้รับความยินยอมก่อนเก็บรวบรวม ใช้ หรือเปิดเผยแล้ว

(2) บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้”

“มาตรา 22 การเก็บรวบรวมข้อมูลส่วนบุคคล ให้เก็บรวบรวมได้เท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล”

“ มาตรา 23 ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียด ดังต่อไปนี้เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว

(1) วัตถุประสงค์ของการเก็บรวบรวมเพื่อการนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยซึ่งรวมถึงวัตถุประสงค์ตามที่มาตรา 24 ให้อำนาจในการเก็บรวบรวมได้โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

(2) แจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือสัญญาหรือมีความจำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา รวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล

(3) ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม

(4) ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย

(5) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อในกรณีที่มีตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ให้แจ้งข้อมูล สถานที่ติดต่อ และวิธีการติดต่อของตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย

(6) สิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 19 วรรคห้า มาตรา 30 วรรคหนึ่ง มาตรา 31 วรรคหนึ่ง มาตรา 32 วรรคหนึ่ง มาตรา 33 วรรคหนึ่ง มาตรา 34 วรรคหนึ่ง มาตรา 36 วรรคหนึ่ง และมาตรา 73 วรรคหนึ่ง ”

“ มาตรา 24 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(1) เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุ เพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสม เพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ตามที่คณะกรรมการประกาศกำหนด

(2) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

(3) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

(4) เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

(5) เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

(6) เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล ”

“ มาตรา 25 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่

(1) ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า แต่ต้องไม่เกินสามสิบวันนับแต่วันที่เก็บรวบรวมและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

(2) เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26

ให้นำบทบัญญัติเกี่ยวกับการแจ้งวัตถุประสงค์ใหม่ตามมาตรา 21 และการแจ้งรายละเอียดตามมาตรา 23 มาใช้บังคับกับการเก็บรวบรวมข้อมูลส่วนบุคคลที่ต้องได้รับความยินยอมตามวรรคหนึ่งโดยอนุโลม เว้นแต่กรณีดังต่อไปนี้

(1) เจ้าของข้อมูลส่วนบุคคลทราบวัตถุประสงค์ใหม่หรือรายละเอียดนั้นอยู่แล้ว

(2) ผู้ควบคุมข้อมูลส่วนบุคคลพิสูจน์ได้ว่าการแจ้งวัตถุประสงค์ใหม่หรือรายละเอียดดังกล่าวไม่สามารถทำได้หรือจะเป็นอุปสรรคต่อการใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ ในกรณีนี้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิ เสรีภาพ และประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

(3) การใช้หรือการเปิดเผยข้อมูลส่วนบุคคลต้องกระทำโดยเร่งด่วนตามที่กฎหมายกำหนดซึ่งได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

(4) เมื่อผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้ซึ่งล่วงรู้หรือได้มาซึ่งข้อมูลส่วนบุคคลจากหน้าที่หรือจากการประกอบอาชีพหรือวิชาชีพและต้องรักษาวัตถุประสงค์ใหม่หรือรายละเอียดบางประการตามมาตรา 23 ไว้เป็นความลับตามที่กฎหมายกำหนด

การแจ้งรายละเอียดตามวรรคสอง ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบภายในสามสิบวันนับแต่วันที่เก็บรวบรวมตามมาตรานี้ เว้นแต่กรณีที่นำข้อมูลส่วนบุคคลไปใช้เพื่อการ

ติดต่อกับเจ้าของข้อมูลส่วนบุคคลต้องแจ้งในการติดต่อครั้งแรก และกรณีที่จะนำข้อมูลส่วนบุคคลไปเปิดเผยต้องแจ้งก่อนที่จะนำข้อมูลส่วนบุคคลไปเปิดเผยเป็นครั้งแรก ”

“มาตรา 26 ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(1) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม

(2) เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิสมาคม หรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงานให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรตามวัตถุประสงค์ดังกล่าวโดยไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกมูลนิธิสมาคม หรือองค์กรที่ไม่แสวงหากำไรนั้น

(3) เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล

(4) เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

(5) เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ

(ก) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ ทั้งนี้ ในกรณีที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์

(ข) ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

(ค) การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองทางสังคมซึ่งการ

เก็บรวบรวมข้อมูลส่วนบุคคลเป็นสิ่งจำเป็นในการปฏิบัติตามสิทธิหรือหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคล โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

(ง) การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น ทั้งนี้ ต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น และได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ตามที่คณะกรรมการประกาศกำหนด

(จ) ประโยชน์สาธารณะที่สำคัญ โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

ข้อมูลชีวภาพตามวรรคหนึ่งให้หมายถึงข้อมูลส่วนบุคคลที่เกิดจากการใช้เทคนิคหรือเทคโนโลยีที่เกี่ยวข้องกับการนำลักษณะเด่นทางกายภาพหรือทางพฤติกรรมของบุคคลมาใช้ทำให้สามารถยืนยันตัวตนของบุคคลนั้นที่ไม่เหมือนกับบุคคลอื่นได้ เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจาลองม่านตา หรือข้อมูลจำลองลายนิ้วมือ ในกรณีที่เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมต้องกระทำภายใต้การควบคุมของหน่วยงานที่มีอำนาจหน้าที่ตามกฎหมาย หรือได้จัดให้มีมาตรการคุ้มครองข้อมูลส่วนบุคคล ตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด”

“มาตรา 27 ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26

บุคคลหรือนิติบุคคลที่ได้รับข้อมูลส่วนบุคคลมาจากการเปิดเผยตามวรรคหนึ่ง จะต้องไม่ใช้หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลส่วนบุคคลในการขอรับข้อมูลส่วนบุคคลนั้น

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกการใช้หรือเปิดเผยนั้นไว้ในรายการตามมาตรา 39”

“ มาตรา 28 ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ทั้งนี้ ต้องเป็นไปตามหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลตามที่คณะกรรมการประกาศกำหนดตามมาตรา 16 (5) เว้นแต่

(1) เป็นการปฏิบัติตามกฎหมาย

(2) ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลแล้ว

(3) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

(4) เป็นการกระทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่นเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

(5) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้

(6) เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญในกรณีที่มีปัญหาเกี่ยวกับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคล ให้เสนอต่อคณะกรรมการเป็นผู้วินิจฉัย ทั้งนี้ คำวินิจฉัยของคณะกรรมการอาจขอให้ทบทวนได้เมื่อมีหลักฐานใหม่ทำให้เชื่อได้ว่าประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลมีการพัฒนาจนมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ”

โดยหลักของพระราชบัญญัติข้อมูลส่วนบุคคล พ.ศ.2562 นั้น การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจะต้องมีการดำเนินการ ดังนี้

1. เจ้าของข้อมูลส่วนบุคคลจะต้องให้ความยินยอม
2. ต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
3. มีแบบหรือข้อความที่อ่านแล้วเข้าใจได้โดยง่ายและต้องไม่เป็นการหลอกลวง
4. เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเมื่อใดก็ได้

ทั้งนี้ ในการขอความยินยอมต้องคำนึงอย่างถึงที่สุดในความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม และต้องไม่มีเงื่อนไขใดๆในการให้ความยินยอมเพื่อเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่มีความจำเป็นหรือเกี่ยวข้องสำหรับการเข้าทำสัญญาซึ่งรวมถึงการให้บริการนั้น ๆ[41]

มาตรา 77 ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลอันเป็นการฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติแห่งพระราชบัญญัตินี้ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้นแก่เจ้าของข้อมูล ส่วนบุคคล ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่ก็ตาม เว้นแต่ ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้นจะพิสูจน์ได้ว่า

(1) ความเสียหายนั้นเกิดจากเหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั้นเอง

---

[41] สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, ‘สรุปสาระสำคัญ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562’ <https://www.dct.or.th/upload/downloads/1612025563SummaryPDPA_DigitalCouncilofThailand.pdf.> สืบค้นเมื่อ 15 กรกฎาคม 2565.

(2) เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามหน้าที่และอำนาจตามกฎหมาย ค่าสินไหมทดแทนตามวรรคหนึ่ง ให้หมายความรวมถึงค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูล ส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหาย ที่เกิดขึ้นแล้วด้วย

3.3.5 พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545

พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 ได้ประกาศใช้เมื่อวันที่ 13 พฤศจิกายน พ.ศ. 2545 ซึ่งแต่ก่อนหน้านั้นยังไม่มีกฎหมายที่กำหนดหลักเกณฑ์ วิธีการและเงื่อนในการทำธุรกรรมข้อมูลเครดิตแต่อย่างใด เป็นการออกกฎหมายนี้มาทั้งนี้เพื่อการคุ้มครองข้อมูลของเจ้าของข้อมูลไว้โดยเฉพาะ โดยมีเนื้อหาที่น่าสนใจที่ว่า กฎหมายฉบับนี้นั้นได้วางหลักเกณฑ์ เพื่อคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในหน่วยงานภาคเอกชนที่เป็นข้อมูลเครดิต ซึ่งครอบคลุมข้อมูลส่วนบุคลของประชาชนหลายประเภท[42]

คำนิยาม นั้นมีอยู่หลายประเภทซึ่งได้บัญญัติไว้ใน มาตรา 3 เช่น “ข้อมูล” หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงของข้อมูลเครดิตไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเอง หรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำในรูปของเอกสาร แฟ้มรายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้ และมีคำว่า “ข้อมูลเครดิต”โดยได้ให้ความหมายไว้ ว่า “ข้อมูลเครดิต” หมายความว่า ข้อเท็จจริงเกี่ยวกับลูกค้าที่ขอสินเชื่อ ดังต่อไปนี้

ข้อเท็จจริงที่บ่งชี้ถึงตัวลูกค้า และคุณสมบัติของลูกค้าที่ขอสินเชื่อ

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

กรณีนิติบุคคล หมายถึง ชื่อ สถานที่ตั้ง เลขที่ทะเบียนการจัดตั้งนิติบุคคล หรือเลขประจำตัวผู้เสียภาษีอากร

ประวัติการขอและการได้รับอนุมัติสินเชื่อ และการชำระสินเชื่อของลูกค้าที่ขอสินเชื่อรวมทั้งประวัติการชำระราคาสินค้าหรือบริการโดยบัตรเครดิต

แต่ในขณะเดียวกันก็มีข้อมูลที่ไม่สามารถจัดเก็บได้นั่น คือ “ข้อมูลห้ามจัดเก็บ” กล่าวคือ เป็นข้อมูลของบุคคลธรรมดาที่ไม่เกี่ยวกับการรับบริการ การขอสินเชื่อ หรือที่มีผลกระทบต่อความรู้สึกหรืออาจก่อให้เกิดความเสียหายหรือมีผลกระทบต่อสิทธิเสรีภาพของผู้เป็นเจ้าของข้อมูลอย่างชัดเจน ดังต่อไปนี้

1. ลักษณะพิการทางร่างกาย

2. ลักษณะทางพันธุกรรม

---

[42] สำนักงานเศรษฐกิจการคลัง, ‘พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พุทธศักราช 2545’ <http://www.fpo.go.th/FPO/index2.php?mod=Category&file=categoryview&categoryID=CAT0000 506.> สืบค้นเมื่อ 8 มกราคม 2565.

3. ข้อมูลของบุคคลที่อยู่ในกระบวนการสอบสวนหรือพิจารณาคดีอาญา

4. ข้อมูลอื่นใดตามที่คณะกรรมการประกาศ

ดังนั้น เมื่อเราทราบถึงความหมายของข้อมูลแล้ว ผู้ซึ่งเป็นเจ้าของข้อมูลนั้นก็จะถือว่ามีความสำคัญในการให้ข้อมูล ซึ่งตามพระราชบัญญัตินี้ “เจ้าของข้อมูล” หมายความว่า บุคคลธรรมดา หรือนิติบุคคลใดๆ ซึ่งเป็นเจ้าของข้อมูล หรือเป็นเจ้าของประวัติลูกค้าผู้ขอใช้บริการจากสมาชิกไม่ว่าจะเป็นการขอสินเชื่อหรือบริการอื่นใด “สถาบันการเงิน” อาจหมายความรวมถึงหน่วยงานเอกชน ซึ่งหมายถึง นิติบุคคลที่ได้รับอนุญาตให้ประกอบธุรกิจหรือดำเนินกิจการในราชอาณาจักร ดังนี้

1. ธนาคารพาณิชย์

2. บริษัทเงินทุน

3. บริษัทหลักทรัพย์

4. บริษัทเครดิตฟองซิเอร์

5. บริษัทประกันภัย

6. บริษัทประกันชีวิต

7. นิติบุคคลที่ให้บริการบัตรเครดิต

8. นิติบุคคลที่มีกฎหมายเฉพาะจัดตั้งขึ้นเพื่อดำเนินการทางการเงิน

9. นิติบุคคลอื่นที่ประกอบกิจการให้สินเชื่อเป็นทางการค้าปกติตามที่คณะกรรมการประกาศกำหนด ซึ่ง “ผู้ใช้บริการ” หมายความว่า สมาชิก หรือนิติบุคคลที่ประกอบกิจการอันชอบด้วยกฎหมายโดยให้สินเชื่อเป็นทางการค้าปกติ และ“แหล่งข้อมูล” หมายความว่า บุคคลธรรมดา คณะบุคคลหรือนิติบุคคลซึ่งเป็นผู้ให้ข้อมูลแก่บริษัทข้อมูลเครดิต

หลักเกณฑ์ในการคุ้มครองข้อมูล

ในพระราชบัญญัตินี้ ได้มีการกำหนดในเรื่องของหลักเกณฑ์ ในการจัดเก็บข้อมูลไว้ ใน มาตรา 10 และ มาตรา 18 โดยมีการกำหนดไว้ดังนี้ว่า ห้ามมิให้บริษัทข้อมูลเครดิต ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลจัดเก็บข้อมูลห้ามจัดเก็บ และในกรณีที่เป็นประโยชน์ในการควบคุมและประมวลผลข้อมูลของบริษัทข้อมูลเครดิตให้สมาชิกส่งข้อมูลของลูกค้าของตนแก่บริษัทข้อมูลเครดิตที่ตนเป็นสมาชิก และแจ้งเป็นหนังสือให้ลูกค้าของตนทราบเกี่ยวกับข้อมูลที่ส่งไปภายในสามสิบวันนับแต่วันที่ส่งข้อมูลแก่บริษัทข้อมูลเครดิตแต่การส่งข้อมูลเพิ่มเติมในส่วนของประวัติการชำระสินเชื่อ และประวัติการชำระราคาสินค้าหรือบริการโดยบัตรเครดิตให้แก่บริษัทข้อมูลเครดิต ให้สมาชิกแจ้งให้ลูกค้าของตนทราบตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่คณะกรรมการกำหนด

การละเมิดข้อมูล

ซึ่งในส่วนใหญ่แล้วเป็นการกระทำที่ไม่ว่าจะเป็นในเรื่องของ การจงใจหรือว่าประมาทเลินเล่อ ที่จะเปิดเผยข้อมูลที่ไม่ถูกต้องแก่ผู้อื่น หรือเปิดเผยข้อมูลที่ถูกต้องแต่มิใช่เป็นไปตามวัตถุประสงค์ที่กำหนดไว้ ก็ถือ

ว่าเป็นการละเมิดทั้งสิ้น ซึ่งจะมีโทษทางแพ่งและทางอาญา โดยเฉพาะในกรณีที่เป็นการคุ้มครองข้อมูลส่วนบุคคลของผู้อื่นที่เป็นข้อมูลเครดิต แต่อย่างไรก็ดีก็จะมีข้อยกเว้นไว้ว่า ไม่ถือเป็นความผิดตามมาตรา 19

การให้ความยินยอมในการเปิดเผยข้อมูล

พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต ได้กำหนดหลักเกณฑ์ให้บริษัทข้อมูลเครดิตเปิดเผยหรือให้ข้อมูลแก่สมาชิกหรือผู้ใช้บริการที่ประสงค์จะใช้ข้อมูลเพื่อประโยชน์ในการวิเคราะห์การให้สินเชื่อ รวมทั้งการรับประกันภัยการรับประกันชีวิต และการออกบัตรเครดิต ทั้งนี้ จะต้องได้รับคำยินยอมเป็นหนังสือจากเจ้าของข้อมูลเพื่อให้เปิดเผยหรือให้ข้อมูลแก่สมาชิกหรือผู้ใช้บริการนั้นก่อนตามมาตรา 20

จะเห็นได้ว่า พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 เป็นกฎหมายที่ออกมาเพื่อคุ้มครองข้อมูลส่วนบุคคลของเรา ในกรณีที่เราไปทำบัตรเครดิตกับสถาบันทางการเงิน ไม่ว่าจะเป็นธนาคารหรือบริษัท ไม่ว่าจะเป็นหน่วยงานของรัฐ หรือหน่วยงานเอกชนก็ตาม ซึ่งได้มีข้อกำหนดในการจัดเก็บข้อมูลส่วนบุคคล และการคุ้มครองข้อมูลส่วนบุคคล ซึ่งหากสถาบันทางการเงินมีการละเมิดข้อมูลหรือเปิดเผยข้อมูลของลูกค้า หรือผู้ใช้บริการ ก็จะมีบทลงโทษในการกระทำความผิดนั้นด้วย

3.3.6 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 นั้นได้มีบทบัญญัติที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลเอาไว้ แต่ก็เป็นการคุ้มครองเฉพาะข้อมูลส่วนบุคคลที่อยู่ในหน่วยงานหรือเกี่ยวข้องกับภาครัฐเท่านั้น โดยให้คำนิยามไว้ว่าว "ข้อมูลข่าวสาร" หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริง ข้อมูลหรือสิ่งใดๆ ไม่ว่าการสื่อความหมายนั้น จะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใดๆ และไม่ว่าจะได้จัดทำไว้ในรูปของเอกสาร แฟ้ม รายงาน หนังสือแผนผัง แผนที่ ภาพวาด ภาพถ่ายฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้ ส่วนคำว่า "ข้อมูลข่าวสารของราชการ" หมายความว่า ข้อมูลข่าวสารที่อยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐ ไม่ว่าจะเป็นข้อมูลข่าวสารเกี่ยวกับการดำเนินงานของรัฐหรือข้อมูลข่าวสารเกี่ยวกับเอกชน และพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 นั้นยังได้ให้คำนิยามของคำว่า ข้อมูลส่วนบุคคล รวมถึงหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคล และการจัดเก็บข้อมูลส่วนบุคคลไว้ด้วย

3.3.5.1 คำนิยามข้อมูลส่วนบุคคล

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ได้ให้คำนิยาม ของคำว่า ข้อมูลส่วนบุคคลไว้ซึ่งหมายถึง ข้อมูลข่าวสารที่เกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่นการศึกษาฐานะทางการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน ในบรรดาที่มีชื่อของผู้นั้น หรือมีเลขหมายรหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึก ลักษณะ เสียงคน หรือรูปถ่าย และให้หมายรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งของผู้ที่ถึงแก่กรรมแล้ว เป็นต้น

3.3.5.2 หลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคล

บุคคลที่จะได้รับการคุ้มครองตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 นั้นจะต้องเป็นบุคคลตามพระราชบัญญัติฉบับนี้ นั่นคือบุคคลธรรมดาที่มีสัญชาติไทยและบุคคลธรรมดาที่ไม่มีสัญชาติไทยแต่มีถิ่นที่อยู่ในประเทศไทย ตามมาตรา 21 ซึ่งในการจัดเก็บข้อมูลส่วนบุคคลนั้นต้องเก็บจากเจ้าของข้อมูลโดยตรง เพื่อความถูกต้องของข้อมูลนั้นๆ เพราะหากนำข้อมูลที่ได้มาไม่ถูกต้องไปใช้หรือเผยแพร่ ก็อาจกระทบถึงประโยชน์ ของบุคคลผู้เป็นเจ้าของข้อมูลนั้นนอกจากนี้ต้องมีการตรวจสอบแก้ไขข้อมูลให้ถูกต้องอยู่เสมอ

3.3.5.3 การจัดเก็บข้อมูลส่วนบุคคลโดยตรง

นอกจากนี้แล้ว ในการที่จะจัดเก็บข้อมูลส่วนบุคคลโดยตรงจากเจ้าของข้อมูลในหน่วยงานของรัฐนั้นจะต้องปฏิบัติตาม มาตรา 23 คือ

1. ต้องแจ้งถึงวัตถุประสงค์ ที่จะนำไปใช้ให้เจ้าของข้อมูลทราบล่วงหน้าหรือพร้อมกับการขอข้อมูล

2. ต้องแจ้งให้เจ้าของข้อมูลทราบถึงลักษณะการใช้ข้อมูลว่าจะนำไปใช้กรณีใดบ้าง

3. ต้องแจ้งให้เจ้าของข้อมูลทราบด้วยว่า การขอข้อมูลเป็นกรณีที่เจ้าของข้อมูลอาจให้ข้อมูล หรือไม่ให้ข้อมูลก็ได้ หรือเป็นกรณีที่กฎหมายบังคับต้องให้ข้อมูล

บทที่ 4
วิเคราะห์ปัญหาในการคุ้มครองข้อมูลส่วนบุคคล กรณีนายหน้าข้อมูล

ปัจจุบันเป็นที่ยอมรับกันทั่วไปว่า ข้อมูลส่วนบุคคลเป็นส่วนหนึ่งของสิทธิในความเป็นอยู่ส่วนตัว (Right of Privacy) การคุ้มครองข้อมูลส่วนบุคคลเป็นพัฒนาการในเรื่องการคุ้มครองชีวิต ร่างกาย และทรัพย์สินของบุคคล ซึ่งได้ขยายขอบเขตการคุ้มครองไปถึงการคุ้มครองความคิด ความรู้สึกที่แสดงออกมาของบุคคล สิทธิดังกล่าวนี้จึงเป็นส่วนหนึ่งของสิทธิส่วนบุคคล ในการที่จะอยู่ลำพังปราศจากการรบกวนหรือขัดขวาง และครอบคลุมถึงสิทธิขั้นพื้นฐานของบุคคลไว้ทั้งหมด เช่น ความเป็นส่วนตัวในร่างกาย สิทธิในการเดินทางติดต่อสื่อสาร สิทธิในการรับรู้ข้อมูลข่าวสาร และยังเกี่ยวโยงถึงรากฐานของสิทธิมนุษยชน เช่น สิทธิและเสรีภาพในตัวของบุคคลอีกด้วย

เมื่อการทำงานกับเทคโนโลยีที่เปลี่ยนไปโดยใช้ข้อมูลจำนวนมหาศาลเป็นเสมือนทรัพยากรพื้นฐานที่สำคัญขององค์กร สิ่งที่เลี่ยงไม่ได้ที่มากับการใช้ข้อมูลก็คือ ความรับผิดชอบที่ต้องเพิ่มมากขึ้นกับข้อมูล เพราะธุรกิจนั้นนำข้อมูลของลูกค้ามาใช้เพื่อกิจกรรมทางธุรกิจ บางครั้งความสมดุลในการนำมาใช้กับเรื่องความเป็นส่วนตัว จึงเป็นสิ่งที่ต้องคำนึงถึง เพราะถือเป็นเรื่องสำคัญทางกฎหมายในเรื่อง สิทธิความเป็นส่วนตัวในเรื่องต่าง ๆ ซึ่งมีองค์ประกอบและเกี่ยวพันกันทั้งในทางสังคม กฎหมาย จริยธรรม สิทธิความเป็นส่วนตัวทางด้านข้อมูลจึงเป็นเรื่องที่ทุกฝ่ายให้ความสนใจเป็นอย่างมาก[1] สังคมไทยในปัจจุบันเป็นสังคมสมัยใหม่ เป็นสังคมแห่งการติดต่อสื่อสาร ข้อมูลข่าวสารต่างๆจึงมีความสำคัญต่อการวางแผน ระบบการทำงานและการบริหารจัดการการดำเนินกิจกรรมต่างๆ ไม่ว่าจะเป็นภาครัฐหรือเอกชน จำเป็นที่จะต้องมีข้อมูลไว้ในครอบครองไว้ให้ได้มากที่สุด ซึ่งในข้อมูลข่าวสารจำนวนมากมายมหาศาลที่มีการครอบครอง หรือมีการแลกเปลี่ยนหรือแย่งชิงแข่งขันกันครอบครองนี้ ส่วนหนึ่งเป็นข้อมูลส่วนบุคคล ซึ่งปัญหาที่เกิดขึ้นในเรื่องการคุ้มครองข้อมูลส่วนบุคคลนี้เกิดขึ้นเนื่องจากการเข้าถึงข้อมูลข่าวสารที่ทำได้สะดวกและรวดเร็วมาก โดยเฉพาะความสามารถในการจัดเก็บด้วยคอมพิวเตอร์ การสืบค้นข้อมูล การเข้าถึงข้อมูล การรับ-ส่งข้อมูล ซึ่งการแลกเปลี่ยนข้อมูลข่าวสารนั้นเกิดขึ้นตลอดเวลาและมีอยู่ทั่วไป การสะสมข้อมูลไว้ในครอบครองเพื่อหาประโยชน์จากข้อมูลนั้นมีมากขึ้นและมีอยู่ในทุกๆวงการธุรกิจ ทั้งนี้ เพื่อเพิ่มโอกาสในการดำเนินธุรกิจ แต่ผลกระทบต่อบุคคลที่เกิดขึ้นคือการนำข้อมูลส่วนบุคคลไปใช้ ประมวลผล หรือเปิดเผย ทำให้บุคคลผู้เป็นเจ้าของข้อมูลอาจได้รับความเสียหาย เช่น อาจมีผลต่อความปลอดภัยต่อชีวิต ร่างกาย สิทธิ และเสรีภาพของบุคคล หรือการนำข้อมูลข่าวสารไปใช้ประโยชน์ในทางพาณิชย์โดยปราศจากการได้รับอนุญาตจากผู้เป็นเจ้าของข้อมูล ทำให้เกิดความเสียหายหรือความเดือดร้อนรำคาญ

---

[1] Admin กรมส่งเสริมอุตสาหกรรม, ‘ข้อมูลส่วนบุคคลคืออะไร สำคัญแค่ไหน’ <https://dip360.dip.go.th/ข้อมูลส่วนบุคคลคืออะไร.> สืบค้นเมื่อ 15 กรกฎาคม 2565.

พระราชบัญญัติข้อมูลส่วนบุคคล พ.ศ. 2562 ที่มีผลใช้บังคับเมื่อวันที่ 1 มิถุนายน พ.ศ. 2565 ที่ผ่านมาได้ระบุถึงเจตนารมณ์ในการตราพระราชบัญญัติไว้ว่า “ เนื่องจากปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจานวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหาย ให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวก และรวดเร็ว ก่อให้เกิด ความเสียหายต่อเศรษฐกิจโดยรวม สมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล เป็นการทั่วไปขึ้น เพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไปจึงจำเป็นต้องตราพระราชบัญญัตินี้ ” จากการศึกษา ผู้เขียนมีความเห็นว่าพระราชบัญญัตินี้ยังมีความบกพร่องในเนื้อหากฎหมายและการบังคับใช้กฎหมาย ซึ่งอาจกระทบในด้านต่าง ๆ โดยผู้เขียนได้แบ่งประเด็นทางกฎหมายที่ได้วิเคราะห์ไว้ ดังนี้

4.1 ปัญหาเกี่ยวกับบทนิยามของนายหน้าข้อมูล

ปัจจุบันเทคโนโลยี Big Data Analytics ส่งผลกระทบอย่างมากต่อการทำการตลาดในโลกของธุรกิจ ทำให้เกิด Data-Driven Marketing หรือ การตลาดที่ขับเคลื่อนด้วยข้อมูลของผู้บริโภคโดยหนึ่งในการทำการตลาดที่พบเห็นได้มากที่สุด คือ การได้รับข้อความโปรโมทสินค้า หรือบริการ แม้กระทั่งการพบเห็นโฆษณาสินค้าบนช่องทางโซเชียลมีเดีย ที่หลาย ๆ คนสงสัยกันว่า การโปรโมทโฆษณาเหล่านี้ รู้ได้อย่างไรว่าเรากำลังสนใจ หรือมองหาอะไร โดยบริษัทที่ขายข้อมูลเหล่านี้เรียกว่า Data Broker หรือนายหน้าข้อมูล โดยนายหน้าข้อมูลจะมีการจัดเก็บข้อมูลของกลุ่มบุคคลเป้าหมายจากโลกอินเทอร์เน็ต รวมไปถึงข้อมูลจากออฟไลน์ เพื่อนำมาใช้ประโยชน์ ไม่ว่าจะในลักษณะเชิงพาณิชย์ หรือการค้นคว้าเพื่อต่อยอด ซึ่งไม่ใช่แค่ในต่างประเทศที่มีการซื้อขายข้อมูลของผู้บริโภคให้เห็น แม้แต่ในประเทศไทยเองก็มีบริษัทที่ทำธุรกิจซื้อขายข้อมูลส่วนบุคคลของคนจำนวนมากให้กับองค์กร หรือบริษัทต่าง ๆ ที่ต้องการใช้ประโยชน์จากข้อมูลดังกล่าวเช่นกัน มีทั้งการได้ข้อมูลมาในแบบที่ถูกกฎหมาย และการได้มาของข้อมูลมาโดยไม่ชอบด้วยกฎหมาย ซึ่งการขายข้อมูลนี้ไม่ใช่มีเพียงแค่ประเทศไทยเท่านั้น แต่มีหลายประเทศที่มีการขายข้อมูลซึ่งอยู่เหนือการควบคุมของรัฐบาล และนับวันยิ่งทวีความรุนแรงมากขึ้น ส่งผลต่อระบบเศรษฐกิจของทุกประเทศ สำหรับในประเทศไทยที่มีข่าวการโจรกรรมข้อมูล เพื่อซื้อขายบนตลาดมืดอยู่หลายครั้ง ดังที่ปรากฏเป็นข่าวของเครือข่ายโทรศัพท์ยี่ห้อหนึ่ง ประกาศแจ้งพบเหตุคอมพิวเตอร์ของพนักงานที่ทำหน้าที่ในช่วง work from home ถูกบุกรุกด้วยมัลแวร์ และคนร้ายได้นำข้อมูลออกไปเผยแพร่ใน Dark Web ประมาณ 100,000 รายการ ซึ่งข้อมูลลูกค้าที่ได้รับผลกระทบมีชื่อ นามสกุล , เลขบัตรประจำตัวประชาชน , วัน เดือน ปีเกิด , และหมายเลขโทรศัพท์ หลุดออกไป ส่งผลให้ผู้ที่เป็นเจ้าของข้อมูลได้รับความเสียหายเป็นอย่างมาก และไม่สามารถตรวจสอบได้ว่าข้อมูลดังกล่าวนั้น หลุดไปอยู่ในการรวบรวม ควบคุม ของใคร นำไปใช้โดยมีวัตถุประสงค์เพื่ออะไร และไม่สามารถยกเลิกการเก็บรวบรวมนั้นได้

หากกล่าวถึงในต่างประเทศนั้น ประเทศสหรัฐอเมริกาเป็นประเทศที่มีประชากรเป็นอันดับที่ 3 ของโลก และเป็นประเทศที่มีการก่ออาชญากรรมสูง โดยในรัฐแคลิฟอร์เนียของประเทศสหรัฐอเมริกาเป็นหนึ่งในรัฐที่มีการก่ออาชญากรรมสูงเป็นอันดับต้น ๆ ของประเทศสหรัฐอเมริกา โดยหลังจากที่สหภาพยุโรปได้กำหนดกฎระเบียบการคุ้มครองข้อมูลส่วนบุบคคล GDPR นั้น รัฐแคลิฟอร์เนียได้มีการประกาศใช้ California Consumer Privacy Act (CCPA) ในเดือนกรกฎาคม ซึ่งส่งผลต่อการเปลี่ยนแปลงในด้านความเป็นส่วนตัวของผู้บริโภค โดยได้มีการระบุนายหน้าข้อมูลไว้ใน California Consumer Privacy Act (CCPA) และได้ให้คำนิยามคำว่า นายหน้าข้อมูล (Data Broker) ไว้ใน California Consumer Privacy Act (CCPA) และประมวลกฎหมายแพ่งของรัฐแคลิฟอร์เนีย (California Civil Code §1798.99.88) TITLE 1.81.48. (d) ไว้ว่า “นายหน้าข้อมูล หมายถึง ธุรกิจที่รวบรวมและขายข้อมูลส่วนบุคคลของผู้บริโภคแก่บุคคลที่สามโดยที่ธุรกิจไม่มีความสัมพันธ์โดยตรง แต่นายหน้าข้อมูลไม่รวมถึงสิ่งต่อไปนี้

(1) หน่วยงานการรายงานผู้บริโภคในขอบเขตที่อยู่ภายใต้กฎหมายการรายงานเครดิตที่เป็นธรรมของรัฐบาลกลาง

(2) สถาบันการเงินภายในขอบเขตที่กฎหมาย Gramm-Leach-Bliley ครอบคลุม (กฎหมายมหาชน 106-102) และระเบียบปฏิบัติ

(3) นิติบุคคลภายในขอบเขตที่ครอบคลุมโดยพระราชบัญญัติข้อมูลการประกันภัยและการคุ้มครองความเป็นส่วนตัว”

ซึ่งเป็นการระบุโดยกำหนดบทนิยามของบุคคล กลุ่มบุคคล ที่ใช้ข้อมูลของผู้บริโภคในการทำธุรกิจรวบรวมและขายข้อมูลของผู้บริโภคให้แก่บุคคลที่สาม

และนอกจากนี้มลรัฐเวอร์มอนรัฐเวอร์มอนต์ก็ได้ให้คำนิยามของ นายหน้าข้อมูล ไว้เช่นเดียวกัน โดยกำหนดบทนิยามไว้ใน Vermont Data Broker Regulation (VDBR) 9 V.S.A. § 2430 (4) ว่า “นายหน้าข้อมูล หมายความว่า ธุรกิจหรือหน่วยหรือหน่วยของธุรกิจแยกต่างหากหรือร่วมกันโดยรู้เท่าทันรวบรวมและขายหรืออนุญาตให้บุคคลที่สามข้อมูลส่วนบุคคลที่เป็นนายหน้าของผู้บริโภคที่ธุรกิจไม่มีความสัมพันธ์โดยตรง” และได้กำหนดแนวปฏิบัติให้แก่นายหน้าข้อมูลไว้ใน Guidance on Vermont’s Act 171 of 2018

ซึ่งหากมีการกำหนดบทนิยามนายหน้าข้อมูลไว้ในกฎหมายดังเช่น รัฐแคลิฟอร์เนียร์ และรัฐเวอร์มอนต์ จะส่งผลให้การกำหนดกฎหมายที่เกี่ยวข้อง หรือแนวปฏิบัติ สามารถกำหนดได้โดยง่าย และเมื่อมีข้อพิพาทเกิดขึ้น อาจสามารถตรวจสอบย้อนกลับของข้อมูลได้ หากได้มีการกำหนดแนวปฏิบัติไว้สำหรับนายหน้าข้อมูล โดยกำหนดให้นายหน้าข้อมูลลงทะเบียนเป็นประจำทุกปี และแสดงข้อมูลที่ทำการจัดเก็บ โดยกำหนดวัตถุประสงค์ในการจัดเก็บด้วย

ส่วนในกรณีของ Personal Data Protection Act 2012 ของประเทศสิงคโปร์ ที่ใช้ระบบกฎหมาย Common Law เหมือนดังเช่นประเทศสหรัฐอเมริกาก็ตาม แต่ในประเทศสิงคโปร์มีกฎหมาย Personal Data Protection Act 2012 เป็นเพียงกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่มีเนื้อหาคล้ายคลึงกับ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของประเทศไทย ซึ่งใน Personal Data Protection Act 2012 ไม่มีการบัญญัติถึงนายหน้าข้อมูลและสถานะบุคคลไว้ แต่มีการระบุถึง “ตัวกลางข้อมูล” หมายถึง องค์กรที่ประมวลผลข้อมูลส่วนบุคคลในนามขององค์กร แต่ไม่รวมถึงพนักงานในองค์กรนั้นๆ เป็นผู้ประมวลผลข้อมูลส่วนบุคคล ที่ได้รับข้อมูลส่วนบุคคลมาโดยวิธีการตามที่ Personal Data Protection Act 2012 กำหนด

จากการศึกษาถึงที่มาของคำว่านายหน้าข้อมูลนั้น นายหน้าข้อมูลอาจเป็นบริษัทที่เก็บรวบรวมและจำหน่าย ให้สิทธิ์ใช้งาน หรือเปิดเผยข้อมูลส่วนตัวของผู้ใช้ทั่วไปรายใดรายหนึ่งให้แก่บริษัทอื่นที่ไม่ได้มีความสัมพันธ์ทางธุรกิจโดยตรงกับผู้ใช้รายนั้น ซึ่ง Data Broker หรือ นายหน้าข้อมูลที่ได้อธิบายไปนั้น เปรียบเสมือนพ่อค้าคนกลางที่มีการจัดซื้อจัดหาข้อมูลของกลุ่มเป้าหมาย อีกทั้งยังเป็นผู้เก็บข้อมูลของกลุ่มเป้าหมายเอง ทั้งทางออนไลน์และออฟไลน์ เพื่อนำมาขายให้กับองค์กรหรือธุรกิจต่าง ๆ นำไปใช้ประโยชน์ทางการตลาด โดยข้อมูลหลัก ๆ ที่เป็นที่สนใจสำหรับเหล่า Data Broker หรือนายหน้าข้อมูล คือ ชื่อ นามสกุล , ที่อยู่อาศัย, หมายเลขโทรศัพท์, อายุ, เพศ, อีเมล, หมายเลขประกันสังคม, ข้อมูลอสังหาริมทรัพย์, รายได้, การศึกษา , อาชีพ เป็นต้น

ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่มีผลบังคับใช้เมื่อวันที่ 1 มิถุนายน พ.ศ. 2565 ที่ผ่านมา ได้นิยามคำที่บ่งถึงตัวบุคคลแต่ละประเภทที่เกี่ยวข้องกับข้อมูลส่วนบุคคลซึ่งบัญญัติไว้อยู่ในมาตรา 6 ไว้ดังนี้

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

ซึ่งในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มิได้ระบุถึงคำนิยามคำว่า “นายหน้าข้อมูล” ซึ่งเป็นบุคคลกลางในการซื้อขายข้อมูล นายหน้าข้อมูลเปรียบเสมือนบุคคลหรือกลุ่มบุคคลที่อาจช่วยให้บุคคลที่ประสงค์ร้ายนำข้อมูลไปใช้ในทางที่มิชอบ เช่น การโทรศัพท์มาก่อกวน หรือโทรศัพท์มา เพื่อหลอกให้ทำธุรกรรมทางการเงิน เป็นต้น ซึ่งอาจส่งผลต่อความเป็นส่วนตัวของผู้คนในสังคมเป็นจำนวนมาก และนับวันยิ่งทวีคูณ เนื่องการไม่มีมาตรการหรือกฎหมายเพื่อออกมาคุ้มครองครองประชาชนจากการ ขายข้อมูลโดยนายหน้าข้อมูล นายหน้าข้อมูลจึงเป็นตัวกลางสำคัญในการเก็บ รวบรวม ใช้ จำหน่าย ข้อมูล หากสังเกตุในมุมของพฤติรรมของผู้ควบคุมข้อมูล “บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจ เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล” อาจปฏิเสธไม่ได้ว่าการจำหน่ายเป็นการใช้หรือเปิดเผยข้อมูล ตามพจนานุกรมราชบัณฑิตยสถานได้คำนิยามของคำว่า “ใช้” ไว้ว่า (๑) ก. บังคับให้ทำ เช่น ใช้งาน (๒) ก. จับจ่าย

เช่น ใช้เงิน(๓) ก. เอามาทำให้เกิดผลหรือประโยชน์ เช่น ใช้เวลา ใช้เรือ ใช้รถ (๔) ก. ชำระ ในคำว่า ใช้หนี้ (๕) ก. ตอบแทน, ให้ทดแทน, เช่น เราไปทำแก้วเขาแตก ต้องซื้อใช้เขา และได้ให้คำนิยามคำว่า “ขาย” ไว้ว่า เอาของแลกเงินตรา, โอนกรรมสิทธิ์แห่งทรัพย์สินให้แก่กันโดยตกลงกันว่าผู้รับโอนจะใช้ราคาแห่งทรัพย์สินนั้น มีหลายลักษณะ คือ ชำระเงินในขณะที่ซื้อขายกัน เรียกว่า ขายเงินสด, ขายโดยยอมเก็บเงินอันเป็นราคาของในวันหลัง เรียกว่า ขายเชื่อ, (เลิก) เอาเงินเขามาโดยยอมตนเข้ารับใช้การงานของเจ้าเงิน เรียกว่า ขายตัวลงเป็นทาส. ดังนั้น จะเห็นได้ว่าการขายเปรียบเสมือนการแลกเปลี่ยนซึ่งกันและกัน โดยนำเงินตราไปแลกสินค้า คำนิยามของนายหน้าข้อมูลจึงกว้างกว่า ผู้ควบคุมข้อมูลตามพระราชบัญญัติข้อมูลส่วนบุคคล พ.ศ. 2562 ถึงแม้ความหมายของนายหน้าข้อมูลอาจมีความคล้ายกับความหมายของผู้ควบคุมข้อมูลก็ตาม แต่นายหน้าข้อมูลมีสิ่งที่ต่างออกไป ซึ่งหากมีการกำหนดความหมายหรือบทนิยามของนายหน้าข้อมูล จะสามารถออกกฎหมายหรือมาตรการเพื่อออกมาควบคุมการทำงานของนายหน้าข้อมูล ที่ดำเนินการเก็บ รวบรวม ใช้ จำหน่าย ข้อมูลได้

จากการที่ผู้เขียนได้ศึกษาและค้นคว้า คำนิยามของคำว่า “ผู้ควบคุมข้อมูล” และ “ผู้ประมวลผลข้อมูล” ไม่ครอบคลุมถึงคำว่า “นายหน้าข้อมูล” และในประเทศไทยไม่ได้มีการบัญญัติหรือให้คำนิยามคำว่านายหน้าข้อมูลไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นการเฉพาะ เมื่อไม่มีการบัญญัติคำว่านายหน้าข้อมูลไว้ ทำให้ไม่สามารถรู้ถึงการจัดเก็บข้อมูลหากข้อมูลส่วนตัวได้รั่วไหลออกไปและเกิดความเสียหายขึ้น และเนื่องจากในพระราชบัญญัติข้อมูลส่วนบุคคล พ.ศ. 2562 ไม่มีบทนิยามของบุคคลที่เรียกว่านายหน้าข้อมูล ซึ่งทำให้เกิดข้อสงสัยว่าความเสียหายที่เกิดแก่เจ้าของข้อมูลที่แท้จริงนั้นจริง ๆ แล้วเกิดจากบุคคลที่ทำการซื้อขายข้อมูลหรือที่เรียกว่านายหน้าข้อมูลที่มิได้ใช้ความระมัดระวังตามสมควรเป็นเหตุทำให้ข้อมูลรั่วไหลออกไปหรือเกิดจากบุคคลที่สามที่เข้าถึงระบบโดยมิชอบกันแน่ แต่หากพิจารณาถึงความหมายของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลนั้น อาจกล่าวได้ว่า ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล สามารถเป็นนายหน้าข้อมูลได้เช่นเดียวกัน หากพิจารณาความหมายของนายหน้าข้อมูลทั้งใน CCPA และ VDBR เอง นายหน้าข้อมูลเป็นทั้งผู้รวบรวมและขายข้อมูลให้แก่บุคคลที่สาม แต่แตกต่างกันในกรณีที่ธุรกิจไม่มีความสัมพันธ์โดยตรง เพราะ ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลอาจมีความสัมพันธ์โดยตรงกับเจ้าของข้อมูลก็ได้ รวมถึงอาจกำหนดหน่วยงานในการเข้ามาดูแลอย่างเป็นกิจจะลักษณะ

ดังนั้น จะเห็นว่า หากมีการกำหนดบทนิยามของนายหน้าขอมูลไว้ โดยกำหนดเป็นพระราชบัญญัติของนายหน้าข้อมูลเป็นการเฉพาะ หรือแก้ไขเพิ่มเติมในราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 6 จะเป็นการบัญญัติกฎหมายให้มีความครอบคลุมมากขึ้น และเป็นการดีต่อผู้ใช้กฎหมาย จึงเห็นสมควรที่จะเพิ่มเติมบทบัญญัติในส่วนของบทนิยามคำว่านายหน้าข้อมูลเพื่อที่จะบังคับใช้กฎหมายได้อย่างมีประสิทธิภาพต่อไป

4.2 ปัญหาเกี่ยวกับการกำหนดความรับผิดและบทลงโทษของผู้กระทำความผิด

ทุกวันนี้โลกของอินเทอร์เน็ตเข้ามามีบทบาทในชีวิตประจำวันมากขึ้น การซื้อสินค้าหรือบริการผ่านเว็บไซต์ จองตั๋วเครื่องบิน จองโรงแรมผ่านแอปพลิเคชัน ทำธุรกรรมการเงินต่าง ๆ ฯลฯ ซึ่งในการใช้งานหรือเข้าถึงบริการต่าง ๆ บนอินเทอร์เน็ตนั้น จำเป็นต้องเปิดเผย ข้อมูลส่วนตัว หรือ ข้อมูลส่วนบุคคลบางอย่าง เช่น ชื่อ-นามสกุล เพศ อายุ ที่อยู่ วันเดือนปีเกิด หมายเลขโทรศัพท์ เลขบัตรประจำตัวประชาชน เลขบัตรเครดิต บัญชีธนาคาร ฯลฯ ในบางครั้งเป็นการยืนยันตัวตนเพื่อความมั่นคงปลอดภัยในการเข้าใช้ระบบ บางครั้งเพื่อการติดต่อรับส่งสินค้าหรือการชำระค่าสินค้า ข้อมูลที่เราให้ไปนั้น อาจไปปรากฏอยู่บนอินเทอร์เน็ตหรือถูกนำไปใช้งานอย่างอื่นที่เราไม่คาดคิด ซึ่งความเสียหายที่อาจเกิดขึ้นอาจถูกนำไปในทางผิดกฎหมาย เช่น เลขที่บัตรประชาชนอาจถูกนำไปใช้ในการเปิดบัญชีเพื่อฉ้อโกงผู้อื่น อาจโดนโจรกรรมทางการเงิน เช่น ใช้บัตรเครดิตในการซื้อสินค้า หรือ ถูกโอนเงินออกไปจากบัญชีธนาคาร หรือที่เป็นสิ่งที่เลวร้ายที่สุดคืออาจถูกปลอมแปลงตัวตน เอาไปแอบอ้างทำเรื่องที่เสียหายหรือผิดกฎหมายทำให้เรากลายเป็นเหยื่อหรือผู้ประสบภัยออนไลน์ได้ ซึ่งปัญหาข้อมูลรั่วไหลของไทยก็เกิดขึ้นหลายครั้ง ทั้งการถูกโจรกรรมข้อมูลโดยไม่ทราบสาเหตุ อาจมีทั้งบริษัทเอกชน รัฐวิสาหกิจ และหน่วยงานภาครัฐ โดยเฉพาะข้อมูลด้านสาธารณสุขครั้งใหญ่ 16 ล้านคน ที่เป็นข่าวดังก็คือ ข่าวการถูกโจรกรรมข้อมูลของ รพ.เพชรบูรณ์ ที่ทำข้อมูลคนไข้หลุด 10,095 ราย ในช่วงเดือนกันยายน นอกจากนี้ ยังมีบริษัทขนส่งสินค้า ทำข้อมูลลูกค้าหลุดกว่า 4 หมื่นราย ซึ่งได้มีการชี้แจงในเวลาต่อมาว่าเป็นข้อมูลเก่า และยังมีการหลุดของแอปพลิเคชันช็อปปิ้ง แอปพลิเคชันแนะนำอาหาร ที่หลุดมากกว่า 4 ล้านราย ข้อมูลเว็บไซต์ต่างประเทศที่ติดตามเรื่องการซื้อขายข้อมูลส่วนบุคคล บัญชีการเงิน บัตรเครดิต คริปโตเคอร์เรนซี หรือแม้แต่การโจรกรรมข้อมูลเพื่อเข้าใช้บริการต่างๆ เช่น Netflix, Facebook เป็นต้น

จากข้อมูลตั้งแต่เดือนตุลาคม ค.ศ. 2020 ถึงเดือนกุมภาพันธ์ ค.ศ. 2021 ระบุว่า ช่วงที่ผ่านมาถือเป็นเวลาที่มีปัญหามากที่สุดในกรณี “ข้อมูลรั่วไหล” โดยเฉพาะจากการโจรกรรมข้อมูล แล้วนำข้อมูลไปขายต่อใน Dark Web โดยมีการเปิดเผยราคาอย่างชัดเจน อาทิ การ Cloned Mastercard และ VISA ในราคา 25 ดอลล่าร์ นอกจากนี้ยังมีสแปมระบบจากข้อมูลของผู้อื่นเพื่อทำไปขายต่อ เช่น Internet Banking ที่ขายเริ่มต้นในราคา 40 ดอลล่าร์ หรือแม้แต่บริการ Netflix ที่ถูกเสนอขายบัญชีละ 4 ดอลล่าร์ ต่อปี[2] ถึงแม้ว่าประเทศไทยจะมีการให้ความคุ้มครองข้อมูลส่วนบุคคลเป็นจำนวนมากทั้งกฎหมายในระดับรัฐธรรมนูญ พระราชบัญญัติและกฎหมายที่มีสถานะที่ต่ำกว่าพระราชบัญญัติเช่น รัฐธรรมนูญแห่งราชอาณาจักรไทย , พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 , พระราชบัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่มีผลใช้บังคับเมื่อวันที่ 1 มิถุนายน พ.ศ. 2565 ที่ผ่านมา คือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เนื่องจากปัจจุบันการละเมิดข้อมูลส่วนบุคคลเป็นการกระทำให้เกิดความเสียหายต่อบุคคลผู้เป็นเจ้าของข้อมูลในวงกว้างและยากต่อการเยียวยาหากว่ามีการจับตัวผู้กระทำการละเมิดมาลงโทษได้ล่าช้า

---

[2] ไทยรัฐออนไลน์, ‘ข้อมูลส่วนบุคคล ขายเกลื่อน ราคาถูก คนไทยโดนดูดเงิน DES ดูดาย?’ <https://www.thairath.co.th/scoop/theissue/2224486.> สืบค้นเมื่อ 6 กรกฎาคม 2565.

แม้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะมีหลักการอยู่บนพื้นฐานของการรักษาความปลอดภัยของข้อมูลส่วนบุคคล แต่ในอีกแง่หนึ่ง หลักการและเงื่อนไขในบางส่วนของกฎหมายอาจสร้างโอกาสให้กับอาชญากรรมไซเบอร์ได้ เช่น ในกรณีที่ข้อมูลส่วนบุคคลรั่วไหลออกไปโดยมิชอบ หรือที่เรียกว่า “การละเมิดข้อมูลส่วนบุคคล” ซึ่งหมายถึง การสูญหาย การเข้าถึง การเปลี่ยนแปลง การแก้ไข หรือ การเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ซึ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลมิได้กำหนดความผิดสำหรับผู้กระทำการโดยมิชอบ หากปรากฏว่านายหน้าข้อมูลมิได้มีการจัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสม อาชญากรอาจอาศัยโอกาสในการก่อให้เกิดความเสียหายและล่วงละเมิดต่อการรักษาความปลอดภัย ซึ่งส่งผลกระทบต่อชื่อเสียง ความน่าเชื่อถือในการทำธุรกิจ ซึ่งที่ผ่านมาภัยคุกคามที่เกิดมักจะมาจากการกระทำของบุคคลภายในองค์กรหรือหน่วยงานที่เป็นการกระทำโดยเจตนา เช่น ลูกจ้างเข้าถึงข้อมูลความลับทางการค้าในระบบที่ตนไม่มีสิทธิเข้าถึงเพื่อนำไปขายให้แก่บริษัทคู่แข่งของนายจ้าง ส่งผลให้เกิดความเสียหายต่อองค์กรโดยตรง ซึ่งในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีบัญญัติถึงความรับผิดทางแพ่ง ซึ่งอยู่ในมาตรา 77 ระบุว่า

“ มาตรา 77 ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลอันเป็นการฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติแห่งพระราชบัญญัตินี้ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้นแก่เจ้าของข้อมูลส่วนบุคคล ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่ก็ตาม เว้นแต่ ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้นจะพิสูจน์ได้ว่า

(1) ความเสียหายนั้นเกิดจากเหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั้นเอง

(2) เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามหน้าที่และอำนาจตามกฎหมายค่าสินไหมทดแทนตามวรรคหนึ่ง ให้หมายความรวมถึงค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย ”

สำหรับความรับผิดทางแพ่งตามพระราชบัญญัติข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 77 นั้น เป็นสิทธิของเจ้าของข้อมูลส่วนบุคคลกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลอันเป็นการฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติแห่งพระราชบัญญัตินี้ โดยให้ใช้ค่าสินไหมทดแทนแก่เจ้าของข้อมูลส่วนบุคคล ซึ่งจะสังเกตได้ว่า บุคคลที่จะต้องรับผิดทางแพ่งตามมาตรานี้มีเฉพาะผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเท่านั้น ไม่รวมถึงบุคคลที่สามที่เป็นผู้ก่อให้เกิดข้อมูลรั่วไหลที่แท้จริงก็เป็นได้

ใน CCPA ของมลรัฐแคลิฟอร์เนียร์ และ VDBR ของมลรัฐเวอร์มอนต์ไม่ได้มีการกำหนดความรับผิดและบทลงโทษของนายหน้าข้อมูลกรณีที่นายหน้าทำให้เกิดความเสียหายต่อเจ้าของข้อมูลได้โดยตรง มีเพียง

การกำหนดให้นายหน้าข้อมูลมีหน้าที่ต้องชำระค่าธรรมเนียมและให้ข้อมูลตามที่กฎหมายกำหนด หากนายหน้าข้อมูลไม่ลงทะเบียนภายในกำหนดจะต้องรับโทษทางแพ่งเท่านั้น

ซึ่งหากเกิดในกรณีมีการละเมิดต่อเจ้าของข้อมูลในประเทศไทย อันสืบเนื่องจากการกระทำของนายหน้าข้อมูลผู้เขียนเห็นว่าอาจต้องพิจารณากฎหมายอื่น เช่น อาจจะต้องฟ้องให้ชดใช้ตามหลักกฎหมายแพ่งและพาณิชย์ ว่าด้วยลักษณะละเมิดตามมาตรา 420 ซึ่งเป็นบททั่วไป และค่าสินไหมทดแทนที่จะต้องใช้ให้แก่เจ้าของข้อมูลส่วนบุคคลนั้นจะต้องเป็นค่าเสียหายที่แท้จริง ซึ่งเจ้าของข้อมูลส่วนบุคคลมีหน้าที่ที่จะต้องพิสูจน์ถึงความเสียหายที่เกิดขึ้นว่าความเสียหายที่เกิดขึ้นนั้นเสียหายเพียงใด เมื่อพิจารณาจากสภาพความเป็นจริงในบางกรณีอาจเป็นการยากที่จะพิสูจน์ความเสียหายอย่างเป็นรูปธรรม เนื่องจากเจ้าของข้อมูลส่วนบุคคลบางคนอาจไม่มีความเชี่ยวชาญทางเทคนิคพอที่จะสามารถพิสูจน์ได้ เช่น กรณีข้อมูลส่วนตัวได้รั่วไหลออกไปจากการที่มีบุคคลที่สามเข้าถึงระบบโดยมิชอบ จึงเห็นสมควรเพื่อให้เจ้าของข้อมูลส่วนบุคคลที่ถูกละเมิดได้รับการเยียวยาความเสียหายควรกำหนดให้มีมาตรการในการเยียวยาความเสียหายให้แก่เจ้าของข้อมูลที่ได้รับความเสียหายหรือถูกละเมิดข้อมูลส่วนบุคคล ทั้งในด้านความเสียหายที่สามารถคำนวณเป็นจำนวนเงินได้และความเสียหายทางจิตใจ

4.3 ปัญหาเกี่ยวกับการปรับใช้ข้อกฎหมายในการซื้อขายข้อมูลส่วนบุคคล

ปัจจุบันการซื้อขายข้อมูลลูกค้าในวงการบัตรเครดิตค่อนข้างแพร่สะพัดมาก และถูกใช้เป็นฐานในการกระจายข้อมูลไปยังธุรกิจต่าง ๆ ที่ต้องอาศัยรายชื่อลูกค้าเป็นจำนวนมาก ๆ เช่น ธุรกิจประกัน ธุรกิจโรงแรม โดยที่ส่วนใหญ่การซื้อขายมีทั้งระดับผู้จัดการขึ้นไปติดต่อซื้อขายกันโดยตรง อาทิ ผู้จัดการฝ่ายบัตรเครดิตและผู้จัดการฝ่ายขายประกัน หรือในกลุ่มพนักงานขายบัตรเครดิตทั่วไปที่สะสมฐานข้อมูลไว้ เพื่อนำไปเสนอขายกับผู้จัดการฝ่ายขายประกัน โดยมีอัตราการซื้อขาย เช่น รายชื่อลูกค้าเดิมที่เป็นบัตรแพลทตินัมและมีรายได้ 25,000 บาทต่อเดือน มูลค่า 5-10 บาทต่อรายชื่อ บัตรทอง บัตรเงินและบัตรปกติ รายได้ 15,000-20,000 บาทต่อเดือน มูลค่า 1-4 บาทต่อรายชื่อเป็นต้น นอกจากนี้ยังมีธุรกิจอื่น ๆ ที่เป็นแหล่งกระจายฐานข้อมูลลูกค้า เช่น ธุรกิจโรงแรมระดับ 5 ดาว ที่มีรายชื่อสมาชิกเป็นจำนวนมาก ทั้งคนไทยและชาวต่างชาติหรือสปอร์ตคลับ ซึ่งส่วนใหญ่ต้องถือบัตรเครดิตในระดับแพลทินัม ฐานข้อมูลลูกค้ากลุ่มนี้มีมูลค่า 8-12 บาทต่อรายชื่อ และยังสามารถต่อรองราคาเพิ่มได้อีก ปริมาณการซื้อขายฐานข้อมูลลูกค้าจะเป็นในลักษณะเหมาเข่งเป็นจำนวนมาก ๆ ขั้นต่ำหลัก 100 รายชื่อต่อครั้ง และขั้นสูงสุดเป็นหลัก 10,000 รายชื่อต่อครั้ง ด้วยเหตุนี้เองการสะสมฐานข้อมูลลูกค้าถือว่ามีแรงจูงใจสูงมาก จากการที่รายชื่อลูกค้ามีมูลค่าสามารถแปลงเป็นเงินง่ายและค่อนข้างสูงโดยขั้นต่ำ สามารถขายข้อมูลได้ถึง 2,000 บาทต่อวัน

การคุ้มครองข้อมูลส่วนบุคคลในปัจจุบันจึงเกิดกระแสตื่นตัวกันมาก นอกจากตัวบุคคลซึ่งเป็นเจ้าของข้อมูลเองแล้ว ผู้ให้บริการที่ต้องอาศัยข้อมูลส่วนตัว เช่น สถาบันการเงิน,ธนาคารต่าง ๆ ก็หันมาให้ความสนใจ และกำหนดโยบายในการคุ้มครองข้อมูลส่วนบุคคลด้วย ดังเห็นได้จากนโยบายการคุ้มครองข้อมูล

และความเป็นส่วนตัวของสถาบันการเงิน,ธนาคารต่าง ๆ ไม่ว่าจะเป็นนโยบายการคุ้มครองข้อมูลและความเป็นส่วนตัวที่เกี่ยวข้องเฉพาะกับข้อมูลที่ทางลูกค้าได้ให้ไว้ ข้อมูลส่วนบุคคลใด ๆ ที่ได้ให้ไว้ผ่านทางเว็บไซต์ของธนาคารจะนำไปใช้เพียงเพื่อวัตถุประสงค์ในการให้บริการ หรือกรณีรายละเอียดข้อมูลที่ได้ให้ไว้ในเว็บไซต์ของธนาคารนั้น ทางธนาคารตกลงจะไม่เปิดเผยรายละเอียดข้อมูลส่วนบุคคลให้แก่บุคคลภายนอกใด ๆ เว้นแต่กรณีจะได้รับอนุญาต

ตามพระราชบัญญัติข้อมูลส่วนบุคคล พ.ศ. 2562 ที่มีผลใช้บังคับเมื่อวันที่ 1 มิถุนายน พ.ศ. 2565 ที่ผ่านมา ได้ระบุถึงเจตนารมณ์ในการตราพระราชบัญญัติไว้ว่า “ เนื่องจากปัจจุบันมีการละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหาย ให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทาให้การเก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวก และรวดเร็ว ก่อให้เกิด ความเสียหายต่อเศรษฐกิจโดยรวม สมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้น เพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป จึงจำเป็นต้องตราพระราชบัญญัตินี้ ” แต่อย่างไรก็ดี ในอดีตคำว่า “ข้อมูลส่วนบุคคล” จนถึงปัจจุบันที่พระราชบัญญัตินี้มีผลใช้บังคับนั้น ยังไม่เคยปรากฏในคำพิพากษาของศาลยุติธรรมโดยตรง[3] และยังไม่มีแนวที่ออกมาเป็นบรรทัดฐานแต่อย่างใด

หลักกฎหมายว่าด้วยการซื้อขายในประเทศไทย มีระบุไว้ในประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 453 ซึ่งบัญญัติไว้ว่า “อันว่าซื้อขายนั้น คือสัญญาซึ่งบุคคลฝ่ายหนึ่ง เรียกว่าผู้ขาย โอนกรรมสิทธิ์แห่งทรัพย์สินให้แก่บุคคลอีกฝ่ายหนึ่ง เรียกว่าผู้ซื้อ และผู้ซื้อตกลงว่าจะใช้ราคาทรัพย์สินนั้นให้แก่ผู้ขาย” ซึ่งตามประมวลกฎหมายแพ่งและพาณิชย์ของไทยบัญญัติไว้ในกรณีการซื้อขายซึ่งมีลักษณะเป็นสัญญาต่างตอบแทนอย่างหนึ่ง ซึ่งผู้ขายได้ตกลงขายทรัพย์สินโดยโอนกรรมสิทธิ์ในทรัพย์สินให้แก่ผู้ซื้อ และผู้ซื้อตกลงจะชดใช้ด้วยเงินตราเป็นราคาทรัพย์สินนั้นให้แก่ผู้ขาย และกรรมสิทธิ์ในทรัพย์สินที่ขายย่อมโอนให้แก่ผู้ซื้อตั้งแต่ขณะเมื่อได้ทำสัญญาซื้อขายกัน ดังนั้นผลตามสัญญาซื้อขายคือกรรมสิทธิ์ในทรัพย์สินจะโอนไปยังผู้ซื้อโดยข้อสัญญา โดยไม่จำต้องมีการส่งมอบทรัพย์สินหรือชำระราคาในขณะนั้นแต่อย่างใด เพียงแต่ผู้ซื้อตกลงว่าจะใช้ราคาทรัพย์สินนั้นให้แก่ผู้ขาย สัญญาซื้อขายนั้นก็เกิดขึ้นแล้ว ทั้งนี้ ผู้ขายจะต้องเป็นผู้ถือกรรมสิทธิ์ในทรัพย์นั้น และสามารถโอนกรรมสิทธิ์ไปยังผู้ซื้อได้ทันทีเมื่อได้ทำสัญญาซื้อขายกันถูกต้องตามกฎหมาย

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 คำว่า “เจ้าของข้อมูลส่วนบุคคล” ที่ระบุไว้ในหลายๆมาตรานั้นมิได้ให้คำนิยามของคำว่าเจ้าของข้อมูลส่วนบุคคลเอาไว้แต่อย่างใด เมื่อเปรียบเทียบกับกฎหมายสหภาพยุโรปซึ่งไม่ได้เรียกว่าเจ้าของ แต่ใช้คำว่า “Data Subject” ซึ่งปรากฏอยู่ในส่วนนิยามของข้อมูลส่วนบุคคลที่ว่า “ข้อมูลใด ๆ อันเกี่ยวข้องกับบุคคลธรรมดาที่ระบุตัวตนหรืออาจระบุตัวตนได้” ส่วน

---

[3] ‘กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย’ <http://www.oic.go.th/FILEROOM/CABOICFORM02/DRAWER 05/GENERAL/DATA0000/00000333.PDF.> สืบค้นเมื่อ 6 กรกฎาคม 2565.

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักรได้ให้คำนิยามของเจ้าของข้อมูลส่วนบุคคล (Data Subject) เอาไว้ว่า “บุคคลธรรมดาที่ยังมีชีวิตอยู่ที่ถูกระบุหรือสามารถถูกระบุตัวได้ด้วยข้อมูลส่วนบุคคลที่เกี่ยวกับบุคคลนั้น”[4] จะเห็นได้ว่า กฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นกฎหมายที่ไม่ได้กำหนดสิทธิในความเป็นเจ้าของในลักษณะเดียวกับกรรมสิทธิ์ แต่เป็นการกำหนดหลักการคุ้มครองบุคคลที่ข้อมูลนั้นสามารถระบุตัวบุคคลได้และให้สิทธิบางประการ ซึ่งแตกต่างกับกรรมสิทธิ์ เช่น สิทธิในการเข้าถึงข้อมูล สิทธิในการขอรับสำเนา สิทธิในการขอให้ลบ สิทธิในการขอให้แก้ไขข้อมูล เนื่องจากโดยสภาพของข้อมูลแล้วมีลักษณะแตกต่างจากทรัพย์สินทั่ว ๆ ไป ดังนั้น แม้กฎหมายใช้คำว่า “เจ้าของ” แต่ก็มีความหมายที่แตกต่างจากเจ้าของกรรมสิทธิ์ในทรัพย์

การจะวินิจฉัยปรับใช้ข้อกฎหมายในการซื้อขายข้อมูลส่วนบุคคลนั้น เนื่องจากในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มิได้บัญญัติเรื่องการซื้อขายข้อมูลส่วนบุคคลเอาไว้ จึงต้องพิจารณาว่าการซื้อขายข้อมูลส่วนบุคคลที่เกิดขึ้นในปัจจุบันจะสามารถนำประมวลกฎหมายแพ่งและพาณิชย์ว่าด้วยเรื่องซื้อขายมาปรับใช้หรือไม่นั้น ผู้เขียนมีความเห็นว่า สัญญาซื้อขายนั้นถือเป็นเอกเทศสัญญาซึ่งมีลักษณะเป็นสัญญาต่างตอบแทนอย่างหนึ่ง โดยผู้ขายตกลงขายทรัพย์สินโดยโอนกรรมสิทธิ์ในทรัพย์สินให้แก่ผู้ซื้อ และผู้ซื้อตกลงจะชดใช้ด้วยเงินตราเป็นราคาทรัพย์สินนั้นให้แก่ผู้ขาย และกรรมสิทธิ์ในทรัพย์สินที่ขายย่อมโอนให้แก่ผู้ซื้อตั้งแต่ขณะเมื่อได้ทำสัญญาซื้อขายกัน ซึ่งหมายความว่า ผลตามสัญญาซื้อขายคือกรรมสิทธิ์ในทรัพย์สินจะโอนไปยังผู้ซื้อโดยข้อสัญญาที่ได้ทำกันขึ้นระหว่างคู่สัญญา โดยไม่จำต้องมีการส่งมอบทรัพย์สินหรือชำระราคาในขณะนั้นแต่อย่างใด เพียงแต่ผู้ซื้อตกลงว่าจะใช้ราคาทรัพย์สินนั้นให้แก่ผู้ขาย สัญญาซื้อขายนั้นก็เกิดขึ้นแล้ว ซึ่งจะต้องมีลักษณะเป็นกรรมสิทธิ์ในตัวทรัพย์นั้นจึงจะทำการซื้อขายตามประมวลกฎหมายแพ่งและพาณิชย์ว่าด้วยเรื่องซื้อขายได้ ซึ่งในส่วนของข้อมูลส่วนบุคคลนั้นจากที่ได้กล่าวไว้แล้วข้างต้นว่า กฎหมายคุ้มครองข้อมูลส่วนบุคคลไม่ได้กำหนดสิทธิในความเป็นเจ้าของในลักษณะเดียวกับกรรมสิทธิ์ แต่เป็นการกำหนดหลักการคุ้มครองบุคคลที่ข้อมูลนั้นระบุตัวและให้สิทธิบางประการ ซึ่งมีลักษณะที่แตกต่างกับกรรมสิทธิ์ของทรัพย์สินทั่วๆไป ถึงแม้ว่าในพระราชบัญญัติจะใช้คำว่า “เจ้าของข้อมูลส่วนบุคคล” แต่ก็มีความหมายที่แตกต่างจากเจ้าของกรรมสิทธิ์ในทรัพย์ จึงอาจกล่าวได้ว่า เจ้าของข้อมูลส่วนบุคคลไม่อาจถือได้ว่าเป็นเจ้าของกรรมสิทธิ์ในข้อมูลนั้นตามหลักประมวลกฎหมายแพ่งและพาณิชย์ว่าด้วยเรื่องการซื้อขาย ดังนั้น ในการซื้อขายข้อมูลส่วนบุคคลจึงไม่สามารถนำประมวลกฎหมายแพ่งและพาณิชย์ว่าด้วยเรื่องซื้อขายมาปรับใช้ในกรณีการซื้อขายข้อมูลส่วนบุคคลได้แต่อย่างใด

เมื่อไม่มีบทกฎหมายใดที่สามารถปรับใช้ในกรณีการซื้อขายข้อมูลส่วนบุคคล สิ่งที่เกิดขึ้นในปัจจุบันซึ่งบ่อยครั้งที่แทบจะพบเห็นเป็นประจำจนเกิดความเดือดร้อนคือ มักจะมีโทรศัพท์ซึ่งเป็นเลขหมายที่ไม่รู้จักหรือในบางครั้งอาจไม่ปรากฏเลขหมายได้โทรเข้ามาในโทรศัพท์ส่วนตัว ในบางครั้งก็เป็นการเสนอขายประกัน

[4] Guide to the General Data Protection Regulation (GDPR), <https://ico.org.uk/for-organisations/guide-to-data-protection.>

ชีวิต เสนอทำบัตรเครดิตหรือสินค้าแบบขายตรง เพราะเหตุใดทำไมบริษัทเหล่านั้นจึงมีหมายเลขโทรศัพท์ส่วนตัวซึ่งเป็นข้อมูลส่วนตัวได้ เพียงแต่ถ้าการโฆษณาดังกล่าว ไม่ว่าจะเป็นการขายสินค้า เชิญชวนให้ทำบัตรเครดิต ฯลฯ นั้นตรงตามวัตถุประสงค์ของเจ้าของเลขหมายที่กำลังต้องการในขณะนั้นพอดีก็ถือเป็นเรื่องที่ดี แต่สภาพปัญหาที่เกิดขึ้นในปัจจุบันมักจะไม่เป็นเช่นนั้น เนื่องจากไม่มีบทบัญญัติกฎหมายเข้ามาควบคุมในกรณีดังกล่าว อีกทั้ง การเข้าถึงข้อมูลส่วนตัวของผู้อื่นโดยไม่มีกฎหมายบัญญัติรองรับไว้ย่อมเป็นการละเมิดต่อสิทธิส่วนบุคคลของบุคคลผู้นั้น ย่อมถือว่าเป็นการกระทำโดยมิชอบด้วยกฎหมาย เพราะนอกจากจะเป็นการผิดมรรยาทตามวิชาชีพของผู้ประกอบการแล้ว ยังถือว่าเป็นการละเมิดสิทธิส่วนบุคคลของลูกค้าด้วย แต่อย่างไรก็ดี เนื่องจากปัจจัยทางการตลาดของผู้ประกอบการที่ต้องการขยายช่องทางในการเสนอขายสินค้าของตนให้มากขึ้น การมีฐานข้อมูลและบัญชีรายชื่อลูกค้าที่เพียงพอและทันเหตุการณ์ เป็นสิ่งสำคัญสำหรับทำการตลาดโดยตรงเพราะกิจการจะไม่สามารถสื่อสารหรือเข้าใจถึงกลุ่มลูกค้าที่คาดหวังได้เลย ฐานข้อมูลของลูกค้าและบัญชีรายชื่อลูกค้ามีประโยชน์ในแง่ต่าง ๆ มากมาย ตั้งแต่ใช้ในการกำหนดส่วนต่างของการตลาด การกำหนดการตลาดทางตรงไม่ว่าจะเป็น กลยุทธ์การสร้างสรรค์งานโฆษณา กลยุทธ์สื่อ ตลอดจนแนวทางในการวิเคราะห์ข้อมูลด้านต่าง ๆ อีกมากมาย ทั้งยังมีผลให้เศรษฐกิจของประเทศไทยเจริญก้าวหน้าอีกด้วยเพียงแต่ในปัจจุบันยังไม่มีบทบัญญัติกฎหมายรองรับไว้โดยเฉพาะ จึงสมควรที่จะกำหนดหลักเกณฑ์ มาตรการกำกับดูแลในการซื้อขายข้อมูลส่วนบุคคลไว้เป็นการเฉพาะเพื่อผลประโยชน์ในทางเศรษฐกิจของประเทศไทยและก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลให้น้อยที่สุด

บทที่ 5
บทสรุปและข้อเสนอแนะ

5.1 บทสรุป

ข้อมูลส่วนบุคคล เป็นสิ่งที่สำคัญสำหรับมนุษย์ทุกคน จึงต้องอยู่ภายใต้หลักศักดิ์ศรีความเป็นมนุษย์ เป็นสิ่งที่ไม่อาจถูกพรากหรือทำให้สูญเสียไปโดยวิธีการใดๆได้ เป็นสิ่งที่มีลักษณะเฉพาะของแต่ละบุคคล การให้ความคุ้มครองความเป็นส่วนตัวของมนุษย์ หรือการคุ้มครองข้อมูลส่วนบุคคลจะต้องอยู่ภายใต้พื้นฐานของหลักความยินยอมผู้ใดจะละเมิดมิได้ โดยหลักความยินยอมไม่ก่อให้เกิดละเมิด เนื่องจากเป็นการที่บุคคลสมัครใจหรือเต็มใจให้กระทำ และการที่บุคคลยินยอมให้ใช้ข้อมูล บุคคลที่นำข้อมูลไปใช้จะต้องนำข้อมูลไปใช้โดยอยู่บนพื้นฐานของหลักสุจริตที่เป็นมาตรฐานของการควบคุมความประพฤติหรือการกระทำของบุคคลในทุกเรื่อง ปัจจุบันประเทศต่างๆต่างให้ความสำคัญของการคุ้มครองสิทธิความเป็นอยู่ส่วนตัวหรือสิทธิส่วนบุคคล มีความพยายามที่จะพัฒนากฎหมายและออกกฎเกณฑ์ใหม่ๆ เพื่อให้ความคุ้มครองและป้องกันความเสียหายของบุคคลในประเทศ โดยมีวัตถุประสงค์เพื่อให้เกิดความสงบสุขของสังคมส่วนรวม ดังจะเห็นได้จากการรับรองหลักการดังกล่าวไว้ในรัฐธรรมนูญ โดยเฉพาะในสังคมปัจจุบันที่มีการใช้เครือข่ายอินเตอร์เน็ตในการติดต่อสื่อสารกันอย่างแพร่หลาย ซึ่งมีการนำเครือข่ายดังกล่าวไปใช้ทั้งในทางที่ชอบอันก่อให้เกิดประโยชน์อย่างมาก แต่ในขณะเดียวกันก็มีการนำไปใช้ในทางที่มิชอบอันก่อให้เกิดการรบกวนสิทธิส่วนบุคคลและเกิดความเสียหายในวงกว้าง ดังนั้น ประเทศต่างๆ โดยเฉพาะประเทศที่พัฒนาแล้วจึงให้ความสำคัญกับการออกกฎหมายเพื่อให้ความคุ้มครองสิทธิส่วนบุคคลซึ่งเป็นสิทธิขั้นพื้นฐาน โดยมีวัตถุประสงค์ให้กฎหมายดังกล่าวเป็นแนวทางให้ทุกฝ่ายปฏิบัติตามไปในทิศทางเดียวกันเพื่อลดปัญหาการลักลอบนำข้อมูลส่วนบุคคลของผู้อื่นไปใช้ในทางที่ผิด

ประเภทของข้อมูลส่วนบุคคลสามารถแบ่งออกได้เป็นสองประเภท ได้แก่ ข้อมูลทั่วไป เป็นข้อมูลที่เกี่ยวกับบุคคลผู้เป็นเจ้าของข้อมูลที่สามารถชี้เฉพาะไปยังเจ้าของข้อมูลส่วนบุคคลได้ และข้อมูลที่มีความอ่อนไหว คือข้อมูลที่ละเอียดอ่อนสูง หากมีการเปิดเผยอาจก่อให้ผลกระทบที่พึงประสงค์ต่อเจ้าของข้อมูลส่วนบุคคลได้ กล่าวคือ กระทบต่อความรู้สึกของเจ้าของข้อมูลหรือประชาชนทั่วไป หรือเป็นข้อมูลที่ก่อให้เกิดความขัดแย้ง เช่นความคิดเห็นทางการเมือง ข้อมูลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความเชื่อเกี่ยวกับลัทธิ ศาสนา ประวัติอาชญากรรม หรือประวัติสุขภาพ เป็นต้น

การซื้อขายข้อมูลส่วนบุคคลมีอยู่ในทุกยุคทุกสมัย เพราะข้อมูลเป็นสิ่งสำคัญ เป็นสิ่งที่มีมูลค่ามหาศาล โดยเฉพาะข้อมูลส่วนบุคคล การซื้อขายข้อมูลโดยผ่านนายหน้าข้อมูลจึงเป็นช่องทางที่ง่ายที่สุดสำหรับธุรกิจหรือบุคคลที่ต้องการขยายตลาดเพื่อใช้ในการขยายช่องทางการจัดจำหน่ายสินค้า ในปัจจุบันการมีฐานข้อมูล และบัญชีรายชื่อลูกค้าที่เพียงพอ เป็นสิ่งสำคัญสำหรับการทำการตลาดทางตรง เพราะธุรกิจจะไม่สามารถสื่อสารหรือเข้าถึงกลุ่มลูกค้าที่คาดหวังได้ หากปราศจากข้อมูลและบัญชีรายชื่อลูกค้า การจัดเก็บข้อมูล

ส่วนบุคคลโดยทั่วไปนั้นมีจุดมุ่งหมายเพื่อให้บริการหรือเพื่อดำเนินการทางนิติกรรม หรือธุรกรรมกับผู้ที่เป็นเจ้าของข้อมูล โดยปกติเจ้าของข้อมูลจะต้องยินยอมให้ข้อมูลกับบริษัทหรือหน่วยงานที่จัดเก็บข้อมูลโดยตรงด้วยความเข้าใจว่าข้อมูลที่บริษัทหรือหน่วยงานจัดเก็บไว้เป็นไปเพื่อใช้ในกิจกรรมที่ตนเองเกี่ยวข้องกับบริษัทนั้น ๆ เท่านั้น แต่ปัญหาที่เกิดขึ้นในปัจจุบันบ่อยๆ ผู้ที่มีหน้าที่จัดเก็บข้อมูลดังกล่าวอาจนำข้อมูลไปใช้ในทางอื่นที่เจ้าของข้อมูลไม่ต้องการ หรือหากวิธีการจัดเก็บไม่ดีก็อาจมีผู้ลักลอบนำข้อมูลไปใช้ประโยชน์ในทางที่มิชอบได้ ตั้งแต่อดีตก่อนที่ประเทศไทยจะมีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อาชีพนายหน้าข้อมูลหรือธุรกิจที่แสวงหาผลประโยชน์จากข้อมูล ส่งผลกระทบต่อผู้คนในสังคมเป็นจำนวนมาก เกิดการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวก และรวดเร็ว ก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวม[1] จึงกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นหลักการทั่วไปเพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ให้ความหมายของ “ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

สหภาพยุโรป ไม่ได้กำหนดคำนิยามของนายหน้าข้อมูลโดยตรง ใน Directive 95/46/EC on the Protection of Personal Data แต่ได้ให้ความหมายของ “ผู้ควบคุม” หมายถึง บุคคลธรรมดาหรือนิติบุคคล หน่วยงานรัฐ ตัวแทนหรือ หรือบุคคลอื่นใดไม่ว่าโดยตนเองหรือโดยร่วมกับบุคคลอื่นกำหนดวัตถุประสงค์และวิธีในการประมวลผลข้อมูลส่วนบุคคล ในกรณีที่วัตถุประสงค์และวิธีในการประมวลผลข้อมูลส่วนบุคคลกำหนดโดยกฎหมายหรือกฎของประเทศหรือประชาคม ผู้ควบคุมข้อมูลส่วนบุคคลหรือหลักเกณฑ์เฉพาะเพื่อ การแต่งตั้งผู้ควบคุมข้อมูลให้กำหนดโดยกฎหมายของประเทศหรือประชาคม

General data Protection Regulation หรือ GDPR ได้ให้ความหมายของ “ผู้ควบคุม” หมายถึง บุคคลธรรมดาหรือนิติบุคคล หน่วยงาน สาธารณะที่มีอำนาจ หรือองค์กรใดที่กำหนดวัตถุประสงค์และวิธีการประมวลผลข้อมูลส่วนบุคคล ไม่ว่าจะโดยลำพังหรือร่วมกัน โดยที่วัตถุประสงค์และวิธีการในการประมวลผลดังกล่าวถูกกำหนดโดย กฎหมายของสหภาพหรือรัฐสมาชิก ผู้ควบคุมหรือเกณฑ์เฉพาะสำหรับ การแต่งตั้งตัวแทนผู้ควบคุมอาจถูกกำหนดไว้โดยกฎหมายของสหภาพ หรือรัฐสมาชิก[2]

ใน GDPR ข้อมูลส่วนบุคคลไม่ควรจะถูกจัดเก็บใด ๆ เว้นแต่มีเงื่อนไขที่แน่นอน ซึ่งเงื่อนไขเหล่านั้นต้องอยู่ภายใต้หลักการ 3 ประการ คือ

---

[1] หมายเหตุ พระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562,95

[2] นคร เสรีรักษ์, ผู้แปล, GDPR ภาษาไทย, 25-26

1. หลักความโปร่งใส (Transparency) เนื้อหาในข้อมูลของแบบฟอร์มในการดำเนินการนั้น ต้องปรากฏสิทธิแก่เจ้าของข้อมูล โดยผู้ควบคุมต้องกำหนดชื่อ ที่อยู่ วัตถุประสงค์ในการดำเนินการข้อมูลของผู้รับและข้อมูลใดๆที่ถูกเรียกร้องให้แสดงถึงความชอบธรรมในการดำเนินการด้วย

2. การจำกัดวัตถุประสงค์ (Legitimate purpose) ข้อมูลส่วนบุคคลสามารถดำเนินการจัดเก็บเพื่อการเจาะจงอย่างเปิดเผย และการจำกัดวัตถุประสงค์นี้ ไม่อาจดำเนินการเกินไปถึงลักษณะที่ขัดแย้งต่อวัตถุประสงค์เหล่านั้น

3. ความได้สัดส่วน (Proportionality) ข้อมูลส่วนบุคคลอาจดำเนินการเพียงเท่าที่เหมาะสม และสัมพันธ์กัน และไม่เกินกว่าวัตถุประสงค์ที่เกี่ยวข้องกับการจัดเก็บ หรือเกินกว่าการดำเนินการนั้น ข้อมูลดังกล่าวต้องมีความถูกต้องแม่นยำ และจำเป็นที่จะต้องปรับปรุง เพราะเหตุผลทุกอย่างต้องแน่ใจว่าเป็นข้อมูลที่ไม่ ผิดพลาด หรือไม่สมบูรณ์ ด้วยความเคารพต่อวัตถุประสงค์ในการจัดเก็บนั้น หรือเพื่อทำให้ไม่เกินขอบเขตดังกล่าว ด้วยการลบล้าง หรือถูกทำลาย ข้อมูลจะไม่ถูกเก็บรักษาโดยความยินยอมไว้เป็นเวลานานเกินกว่าความจำเป็นตามวัตถุประสงค์ในการจัดเก็บ โดยประเทศสมาชิกจะต้องมีวิธีการป้องกันที่เหมาะสมในการจัดเก็บข้อมูลส่วนบุคคลในระยะยาวเพื่อการใช้ในเชิงประวัติศาสตร์

ในกฎหมายที่ใช้กันระหว่างประเทศ ก็ได้ให้ความสำคัญเกี่ยวกับข้อมูลส่วนบุคคล เช่นเดียวกัน โดยมีหลักการสำคัญของการคุ้มครองข้อมูลส่วนบุคคลตามหลักการขององค์กรระหว่างประเทศระหว่างสหภาพยุโรปและข้อตกลงรัฐสภายุโรป และองค์การเพื่อความร่วมมือทางด้านเศรษฐกิจและการพัฒนา (OECD) นั้นสามารถสรุปได้ดังนี้

1. หลักการจัดเก็บอย่างจำกัดชอบด้วยกฎหมายและเป็นธรรม กล่าวคือ ผู้ที่มีหน้าที่ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลและต้องกระทำอย่างจำกัดเท่าที่จำเป็น ข้อมูลที่จัดเก็บจะต้องได้มาโดยวิธีการที่ชอบด้วยกฎหมาย เป็นธรรม และเหมาะสม โดยเจ้าของข้อมูลจะต้องรับทราบและให้ความยินยอม

2. หลักการจัดเก็บอย่างมีคุณภาพ ถูกต้องและได้สัดส่วน กล่าวคือ การเก็บรวบรวมข้อมูลส่วนบุคคลจะต้องกระทำด้วยความถูกต้องแม่นยำ โดยข้อมูลที่จะจัดเก็บต้องเป็นข้อมูลที่ถูกต้องสมบูรณ์ มีการปรับปรุงข้อมูลให้ตรงตามความเป็นจริง และทันสมัยอยู่ตลอดเวลาที่มีการประมวลผลและใช้ข้อมูลนั้นๆ อีกทั้งต้องจัดเก็บให้สอดคล้อง พอเพียงและได้สัดส่วนกับวัตถุประสงค์ นอกจากนี้จะต้องจัดเก็บเท่าที่เกี่ยวข้องจำเป็น ไม่เกินจริง และไม่ล่วงล้ำหรือก้าวก่ายกิจการส่วนตัวของบุคคลที่เกี่ยวข้อง

3. หลักการกำหนดวัตถุประสงค์และระยะเวลาในการจัดเก็บ กล่าวคือ จะต้องมีการกำหนดวัตถุประสงค์ในการจัดเก็บและเงื่อนไขของการใช้ ก่อนที่จะมีการจัดเก็บข้อมูลนั้นๆต้องแจ้งวัตถุประสงค์ให้เจ้าของข้อมูลได้ทราบก่อนทำการรวบรวมข้อมูล การใช้ข้อมูลส่วนบุคคลในภายหลังสามารถกระทำได้เพื่อให้สำเร็จตามวัตถุประสงค์ หรือเพื่อการอื่นที่ไม่ขัดหรือแย้งกับวัตถุประสงค์ ในกรณีเช่นนี้ จะต้องระบุวัตถุประสงค์การใช้ที่เปลี่ยนแปลงไปนั้นทุกคราว ส่วนระยะเวลาการจัดเก็บและใช้ข้อมูลส่วนบุคคลสามารถ

กระทำได้ภายในระยะเวลาพอสมควรและเท่าที่จำเป็น แต่จะต้องไม่เกินกว่าระยะเวลาเพื่อให้บรรลุตามวัตถุประสงค์ที่ระบุไว้

4. หลักการใช้ข้อมูลอย่างจำกัด กล่าวคือ จะต้องใช้ข้อมูลส่วนบุคคลภายในกรอบวัตถุประสงค์ที่ได้ระบุไว้โดยไม่มีการเปิดเผย เข้าถึง ให้แพร่หลาย หรือใช้เพื่อการอื่น นอกเหนือจากวัตถุประสงค์ที่ระบุและได้แจ้งให้เจ้าของข้อมูลทราบก่อนหน้านั้น เว้นแต่

(1) ได้รับอนุญาตจากบุคคลผู้เป็นเจ้าของข้อมูล

(2) อาศัยอำนาจตามกฎหมายเพื่อประโยชน์ในการป้องกันรักษาความมั่นคงของชาติ ความสงบเรียบร้อยของสังคม ประโยชน์สาธารณะ เพื่อรักษากฎหมายหรือเพื่อประโยชน์มหาชนอื่นๆ

นอกจากนี้บุคคลใดจะนำข้อมูลส่วนบุคคลของบุคคลอื่นไปเปิดเผยโดยเจ้าของข้อมูลไม่ยินยอมไม่ได้ หากเจ้าของข้อมูลไม่อนุญาตให้เปิดเผย ไม่ว่าการเปิดเผยนั้นจะทำให้เจ้าของข้อมูลเสียหายหรือไม่ก็ตาม ถือเป็นการละเมิดสิทธิในความเป็นอยู่ส่วนตัวทั้งสิ้น แม้เจ้าของข้อมูลจะได้อนุญาตแล้วก็ยังคงมีสิทธิขอให้เลิกการเผยแพร่ข้อมูลส่วนบุคคลได้ทุกเมื่อ

5. หลักการรักษาความปลอดภัย กล่าวคือ ผู้จัดเก็บครอบครองหรือควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีมาตรการรักษาความปลอดภัยในการจัดเก็บข้อมูลส่วนบุคคลอย่างเพียงพอ เพื่อมิให้ข้อมูลส่วนบุคคลเสี่ยงต่อการเข้าถึง สูญหายหรือเสียหายโดยเหตุสุดวิสัย การทำลายโดยบุคคลอื่น โดยธรรมชาติหรือโดยไวรัสคอมพิวเตอร์ การใช้ การแก้ไขเปลี่ยนแปลงหรือการเปิดเผยโดยปราศจากอำนาจ และในกรณีที่ต้องให้บันทึกข้อมูลส่วนบุคคลแก่บุคคลอื่นต้องดำเนินการป้องกันมิให้บุคคลอื่นนั้นได้ใช้ข้อมูลส่วนบุคคลโดยปราศจากอำนาจ

6. หลักเปิดเผยโปร่งใส กล่าวคือ จะต้องมีการประกาศนโยบายในการประมวลผลข้อมูลส่วนบุคคลเพื่อให้บุคคลที่เกี่ยวข้องทราบถึงกระบวนการจัดเก็บ รวบรวม นำไปใช้ นอกจากนี้ จะต้องมีการแสดงให้เห็นถึงความมีอยู่และประเภทของข้อมูลส่วนบุคคล วัตถุประสงค์ของการใช้ข้อมูลส่วนบุคคล ตลอดจนชื่อ สถานที่จัดตั้ง และรายละเอียดของผู้ที่ทำหน้าที่เก็บรักษาข้อมูล ผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูล ให้เจ้าของข้อมูลทราบ

7. หลักการมีส่วนร่วมของเจ้าของข้อมูล กล่าวคือ การเก็บรวบรวมของข้อมูลส่วนบุคคลต้องสอดคล้องกับสิทธิของเจ้าของข้อมูลส่วนบุคคล และจะต้องมีส่วนร่วมในการจัดเก็บข้อมูลนั้นๆ โดยเจ้าของข้อมูลจะมีสิทธิ ดังต่อไปนี้

(1) ต้องได้รับการแจ้งหรือคำยืนยันจากผู้เก็บรักษาข้อมูลหรือผู้ควบคุมข้อมูลว่าได้ทำการจัดเก็บประมวลผลใช้ หรือส่ง โอนข้อมูลส่วนบุคคลของตนหรือไม่

(2) หากมีการจัดเก็บข้อมูลส่วนบุคคลของตน จะต้องได้รับติดต่อจากผู้จัดเก็บข้อมูลภายในระยะเวลาที่เหมาะสม โดยปราศจากค่าธรรมเนียม แต่หากมีการเก็บค่าธรรมเนียมจะต้องไม่สูงจนเกินไป และโดยวิธีการที่เหมาะสม นอกจากนี้ การจัดเก็บจะต้องอยู่ในรูปแบบที่สามารถเข้าถึงได้ง่าย

8. หลักการไม่เลือกปฏิบัติ กล่าวคือ การจัดเก็บหรือรวบรวมข้อมูลส่วนบุคคลจะต้องไม่ทำให้เกิดการเลือกปฏิบัติต่อบุคคลที่แตกต่างกัน เช่น ข้อมูลที่เกี่ยวกับเชื้อชาติ เผ่าพันธุ์ สีผิว พฤติกรรมทางเพศ ความคิดเห็นทางการเมือง หรือความเชื่ออื่นใดๆ รวมถึงความเป็นสมาชิกสหภาพการค้า เป็นต้น ข้อมูลดังกล่าวเป็นข้อมูลส่วนบุคคลประเภทที่เรียกว่า “Sensitive Data(ข้อมูลส่วนบุคคลที่มีผลกระทบต่อความรู้สึก ข้อมูลส่วนบุคคลที่ต้องให้ความสำคัญเป็นพิเศษ ข้อมูลที่มีความอ่อนไหว)” อาจกล่าวได้ว่า เป็นหลักการที่ห้ามมิให้จัดเก็บข้อมูลส่วนบุคคลประเภทที่กระทบต่อความรู้สึก

9. หลักข้อจำกัดในการส่งหรือโอนข้อมูลส่วนบุคคล กล่าวคือ หลักการนัดกำหนดห้ามมิให้มีการส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศที่มิได้มีบทบัญญัติในการให้ความคุ้มครองข้อมูลส่วนบุคคลในระดับที่เท่าเทียมกันในสาระสำคัญ เว้นแต่ ได้รับความยินยอมจากเจ้าของข้อมูลหรือจำเป็นเพื่อชำระหนี้ตามความผูกพันที่เป็นผลของสัญญา หรือทำเพื่อประโยชน์ของบุคคลซึ่งไม่สามารถให้ความยินยอมได้

10. หลักความรับผิดชอบ กล่าวคือ ผู้จัดเก็บข้อมูล ผู้ครอบครองข้อมูลหรือ ผู้ประมวลผลข้อมูลจะต้องมีความรับผิดชอบในการปฏิบัติตามหลักการหรือมาตรการต่างๆข้างต้นให้ครบถ้วนทุกประการอย่างเคร่งครัด หากมีการฝ่าฝืนหรือละเลยแล้วมีผลให้เกิดความเสียหายแก่ข้อมูลส่วนบุคคล ผู้จัดเก็บข้อมูล ผู้ครอบครองข้อมูล หรือผู้ประมวลผลข้อมูลจะต้องรับผิดทั้งทางแพ่งและทางอาญา นอกจากนี้ ยังจะต้องรับผิดค่าใช้จ่ายที่เกิดขึ้น เพื่อกระทำการแก้ไขข้อมูลให้ถูกต้อง ลบหรือทำลายข้อมูลส่วนบุคคล รวมทั้งเยียวยาความเสียหายแล้วแต่กรณี

แม้หลักการ OECD จะเป็นหลักการที่ประเทศส่วนใหญ่ยอมรับและนำไปบัญญัติเป็นกฎหมายภายในประเทศของตนก็ตาม แต่การปรับใช้หลักการต่างๆเหล่านี้กับข้อเท็จจริงที่เกิดขึ้นก็ความหมายต่างกันและต้องอาศัยหลักการและเหตุผลพื้นฐานอื่นๆมาประกอบการตัดสินใจเสมอ เพราะกฎหมายการคุ้มครองข้อมูลส่วนบุคคลมิใช่เป็นแต่เพียงหลักการกำหนดหลักเกณฑ์กลางเพื่อให้ทุกคนปฏิบัติเท่านั้น ซึ่งการจะปรับใช้ยังคงต้องชั่งน้ำหนักประโยชน์ได้เสียระหว่างบุคคลทุกฝ่ายที่เกี่ยวข้องอย่างเหมาะสม ไม่ให้เกิดกรณีที่เข้มงวดเกินไป หรือหละหลวมจนไม่สามารถคุ้มครองสิทธิของประชาชนได้ แต่ในกฎหมายระหว่างประเทศไม่ได้กำหนดความหมายของคำว่านายหน้าข้อมูลไว้เช่นเดียวกัน มีเพียงประเทศสหรัฐอเมริกา ยกตัวอย่าง รัฐแคลิฟอร์เนีย และรัฐเวอร์มอนต์ ที่ได้มีการกำหนดความหมายของนายหน้าข้อมูลไว้เป็นการเฉพาะ

ส่วนในกรณีของประเทศญี่ปุ่น APPI เป็นกฎหมายที่มีมาตรการป้องกันไม่ให้สามารถระบุตัวตนได้ ข้อมูลส่วนบุคคลทุกประเภทจะต้องได้รับการคุ้มครอง โดยเจ้าของข้อมูลมีสิทธิในการตรวจสอบ การแก้ไขข้อมูล การไม่ยินยอมให้ประมวลผล เป็นต้น และมีการคุ้มครองข้อมูลที่มีความอ่อนไหว (sensitive data) ซึ่งเป็นข้อมูลได้รับการคุ้มครองพิเศษ

ส่วนในกรณีของ Personal Data Protection Act 2012 ของประเทศสิงคโปร์ ที่ใช้ระบบกฎหมาย Common Law เหมือนดังเช่นประเทศสหรัฐอเมริกาก็ตาม แต่ Personal Data Protection Act

2012 เป็นเพียงกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่มีลักษณะคล้ายกับ Personal Data Protection Act, B.E. 2562 (2019) ของประเทศไทย โดยไม่มีการบัญญัติถึงนายหน้าข้อมูลและสถานะบุคคลไว้

ใน CCPA และ ประมวลกฎหมายแพ่งของรัฐแคลิฟอร์เนีย (California Civil Code §1798. 99.88) TITLE 1.81.48. (d) ได้บัญญัติให้คำนิยามคำว่า นายหน้าข้อมูล (Data Broker) ไว้ว่า " นายหน้าข้อมูล หมายถึง ธุรกิจที่รวบรวมและขายข้อมูลส่วนบุคคลของผู้บริโภคให้แก่บุคคลที่สามโดยที่ธุรกิจไม่มีความสัมพันธ์โดยตรง แต่นายหน้าซื้อขายข้อมูลไม่รวมถึงสิ่งต่อไปนี้

(1) หน่วยงานการรายงานผู้บริโภคในขอบเขตที่อยู่ภายใต้กฎหมายการรายงานเครดิตที่เป็นธรรมของรัฐบาลกลาง (15 U.S.C. Sec. 1681 et seq.)

(2) สถาบันการเงินภายในขอบเขตที่กฎหมาย Gramm-Leach-Bliley ครอบคลุม (กฎหมายมหาชน 106-102) และระเบียบปฏิบัติ

(3) นิติบุคคลภายในขอบเขตที่ครอบคลุมโดยพระราชบัญญัติข้อมูลการประกันภัยและการคุ้มครองความเป็นส่วนตัว (มาตรา 6.6 (เริ่มต้นด้วยมาตรา 1791) ของบทที่ 1 ของประมวลกฎหมายประกันภัย)"

และใน Vermont Data Broker Regulation (VDBR) 9 V.S.A. § 2430 (4) ไว้ว่า "นายหน้าข้อมูล หมายความว่า ธุรกิจหรือหน่วยหรือหน่วยของธุรกิจแยกต่างหากหรือร่วมกันโดยรู้เท่าทันรวบรวมและขายหรืออนุญาตให้บุคคลที่สามข้อมูลส่วนบุคคลที่เป็นนายหน้าของผู้บริโภคที่ธุรกิจไม่มีความสัมพันธ์โดยตรง"

ดังนั้นจะเห็นได้ว่า ในประเทศไทยไม่ได้มีการบัญญัติการคุ้มครองข้อมูลส่วนบุคคล กรณีการซื้อขายข้อมูลโดยนายหน้าข้อมูลไว้เป็นการเฉพาะ ซึ่งส่งผลให้การคุ้มครองข้อมูลส่วนบุคคลโดยนายหน้าข้อมูลเป็นไปอย่างมีประสิทธิภาพ ถึงแม้ว่า "ผู้ควบคุมข้อมูล" และ "ผู้ประมวลผลข้อมูล" ความหมายเป็นไปในทางเดียวกันกับนายหน้าข้อมูลของ VDBR หรือ CCPA ก็ตาม แต่การนำมาใช้บังคับในกรณีของการขายข้อมูลก็ยังไม่มีกฎหมายฉบับใดที่ได้นำมาบัญญัติไว้เป็นการเฉพาะ ประกอบกับการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้น ถึงแม้จะอยู่ภายใต้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ที่เป็นองค์กรอิสระในการกำกับดูแลเรื่องข้อมูลส่วนบุคคล หรือแม้แต่การที่ สคส. ระบุให้ทุกหน่วยงานจำเป็นต้องมี Data Protection Officer (DPO) ในกรณีที่ 1. ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นหน่วยงานของรัฐ 2. มีการเก็บรวบรวม ใช้ หรือเปิดเผย จำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ โดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมาก 3. กิจกรรมหลักเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ซึ่งข้อมูลละเอียดอ่อน (Sensitive personal data) ก็ตามก็ไม่มีความครอบคลุมถึงนิติบุคคล หรือกลุ่มบุคคล หรือบุคคลที่ทำการเก็บรวบรวมข้อมูลที่นำไปขายโดยที่เจ้าของข้อมูลไม่ยินยอม เพื่อประโยชน์ส่วนตนของนิติบุคคล หรือกลุ่มบุคคล หรือบุคคลเอง

5.2 ข้อเสนอแนะ

5.2.1 ปัญหาเกี่ยวกับบทนิยามของนายหน้าข้อมูล

ข้อมูลส่วนบุคคลเป็นสิ่งสำคัญที่มิอาจให้บุคคลใดล่วงละเมิดได้ การอนุญาตให้นำข้อมูลไปใช้จึงเป็นสิ่งที่ควรได้รับความยินยอมจากเจ้าของข้อมูล ในอดีตเกิดการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวก และรวดเร็ว ก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวม[3] จึงกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นหลักการทั่วไป เพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป ในขณะที่เทคโนโลยีปัจจุบันมีความก้าวหน้า และช่องทางการสื่อสารมีความหลากหลาย ทำให้การละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลสามารถกระทำได้โดยง่าย และหลายครั้งนำมาซึ่งความเดือดร้อนรำคาญ หรือสร้างความเสียหายให้แก่เจ้าของข้อมูล ตลอดจนสามารถส่งผลต่อเศรษฐกิจโดยรวมของประเทศ จึงมีการบัญญัติพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดมาใช้บังคับเพื่อออกมาควบคุมการนำข้อมูลส่วนบุคคลของผู้อื่นมาใช้โดยมิชอบ แต่เนื่องจากในอดีตยังไม่มีบทบัญญัติในส่วนของการคุ้มครองข้อมูลส่วนบุคคลและการล่วงละเมิดข้อมูลส่วนบุคคบจึงเกิดขึ้น และนับวันยิ่งทวีความรุนแรงมากขึ้น เช่น พนักงานบริษัทนำข้อมูลไปขายเพื่อผลประโยชน์ส่วนตัว หรือการทำธุรกิจเกี่ยวกับการซื้อขายข้อมูล โดยบุคคลเหล่านั้นถูกเรียกว่านายหน้าข้อมูล ซึ่งเป็นอาชีพหนึ่งที่สามารถสร้างกำไรได้มหาศาลจากการรวบรวมข้อมูล และขายข้อมูล โดยในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มิได้บัญญัติความหมายนายหน้าข้อมูลไว้เป็นการเฉพาะ รวมถึงในประเทศไทยยังไม่มีการบัญญัติกฎหมายที่เกี่ยวข้องเพื่อมาบังคับใช้ หรือมีการนำข้อกฎหมายที่เกี่ยวข้องมาปรับใช้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลจากการซื้อขายข้อมูล ประกอบกับไม่มีหน่วยงาน ที่เข้ามากำกับ ดูแล และควบคุมเป็นการเฉพาะ

จากการผู้เขียนได้ศึกษาและค้นคว้า รัฐเวอร์มอนต์ และรัฐแคลิฟอร์เนียร์ ในประเทศสหรัฐอเมริกาที่มีการบัญญัติถึงนายหน้าข้อมูลไว้ รวมถึงกำหนดหน่วยงานที่เข้ามากำกับดูแล เพื่อควบคุมการซื้อขายข้อมูลของนายหน้าข้อมูล โดยการกำหนดให้นายหน้าข้อมูลจะต้องลงทะเบียนทุกปี เพื่อเป็นการตรวจสอบว่าบริษัทใดยังคงดำเนินการรวบรวมข้อมูลและยังประกอบธุรกิจอยู่ การที่รัฐแคลิฟอร์เนียร์ได้มีการบัญญัติไว้ในกฎหมาย เนื่องจากรัฐแคลิฟอร์เนียร์เป็นรัฐที่อยู่ในอันดับต้นๆ ของรัฐที่มีการก่ออาชกรรมสูง ส่วนในรัฐเวอร์มอนต์ถึงแม้จะเป็นเพียงรัฐเล็ก ๆ แต่เป็นรัฐที่มองสิทธิความเป็นส่วนตัวของประชากรในรัฐเป็นสำคัญ และเล็งเห็นว่านายหน้าข้อมูลเป็นอาชีพที่ควรให้การควบคุมเป็นพิเศษ และหากนายหน้าข้อมูลขายข้อมูลให้แก่ผู้ที่นำข้อมูลไปใช้ประโยชน์ในทางที่มิชอบ อาจส่งผลต่อผู้บริโภค และอาจรวมถึงภาพรวมทางเศรษฐกิจของประเทศ ถึงแม้ว่าในองค์กรระหว่างประเทศ เช่น GDPR ,OECD หรือในต่างประเทศ เช่น ประเทศญี่ปุ่น หรือแม้แต่ประเทศไทยเอง เป็นประเทศที่ใช้ระบบประมวลกฎหมาย ในประเทศสหรัฐอเมริกา หรือประเทศสิงคโปร์ เป็นประเทศที่ใช้

[3] หมายเหตุ พระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562,95

ระบบจารีตประเพณี แต่ในการบัญญัติกฎหมายในส่วนของคำนิยามคำว่า นายหน้าข้อมูล ผู้ใช้ ผู้ควบคุมข้อมูล หรือผู้ประมวลผล อาจมีลักษณะที่คล้ายคลึงกัน เพียงแต่มีการใช้คำนิยามที่แตกต่างกัน

โดยในประเทศไทยไม่ได้มีการบัญญัติหรือให้คำนิยามคำว่า นายหน้าข้อมูล ไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นการเฉพาะ แต่มีการบัญญัติคำนิยามของคำว่า “ผู้ควบคุมข้อมูล” และ “ผู้ประมวลผลข้อมูล” ไว้ โดยเป็นการบัญญัติคำนิยามแยกออกจากกัน และไม่ครอบคลุมถึงคำว่า “นายหน้าข้อมูล” เมื่อไม่มีการบัญญัติคำว่านายหน้าข้อมูลไว้ อาจส่งผลทำให้บุคคลหรือกลุ่มบุคคลที่ประกอบธุรกิจนายหน้าข้อมูลไม่เข้าข่ายการกระทำที่อยู่ในความหมายของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล ดังนั้น เมื่อไม่มีการกำหนดบทนิยามการดำเนินการตรวจสอบไม่สามารถรู้ถึงการจัดเก็บข้อมูลหากข้อมูลส่วนตัวได้รั่วไหลออกไปและเกิดความเสียหายขึ้น และเนื่องจากไม่มีบทนิยามของบุคคลที่เรียกว่า นายหน้าข้อมูล ซึ่งอาจทำให้เกิดข้อสงสัยว่าความเสียหายที่เกิดแก่เจ้าของข้อมูลที่แท้จริงนั้นจริง ๆ แล้วเกิดจากบุคคลที่ทำการซื้อขายข้อมูลหรือที่เรียกว่านายหน้าข้อมูลที่มิได้ใช้ความระมัดระวังตามสมควรเป็นเหตุทำให้ข้อมูลรั่วไหลออกไปหรือเกิดจากบุคคลที่สามที่เข้าถึงระบบโดยมิชอบกันแน่ แต่หากพิจารณาถึงความหมายของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลนั้น อาจกล่าวได้ว่า ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล สามารถเป็นนายหน้าข้อมูลได้เช่นเดียวกัน หากพิจารณาความหมายของนายหน้าข้อมูลทั้งใน CCPA และ VDBR นายหน้าข้อมูลเป็นทั้งผู้รวบรวมและขายข้อมูลให้แก่บุคคลที่สาม แต่แตกต่างกันในกรณีที่ธุรกิจไม่มีความสัมพันธ์โดยตรง เพราะ ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลอาจมีความสัมพันธ์โดยตรงกับเจ้าของข้อมูลก็ได้

ดังนั้น จะเห็นว่า การบัญญัติกฎหมายให้มีความครอบคลุมจะเป็นการดีต่อผู้ใช้กฎหมาย จึงเห็นสมควรที่จะเพิ่มเติมบทบัญญัติในส่วนของบทนิยามคำว่านายหน้าข้อมูลไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ไว้ในมาตรา 6 หรือกำหนดเป็นพระราชบัญญัตินายหน้าข้อมูลเป็นการเฉพาะ เพื่อให้มีความครอบคลุมมากขึ้น และสามารถจะบังคับใช้กฎหมายในการณีการซื้อขายข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพต่อไป รวมถึงอาจกำหนดหน่วยงานที่จะเข้ามากำกับ ดูแลนายหน้าข้อมูล โดยกำหนดหลักเกณฑ์หรือแนวปฏิบัติ ที่ช่วยให้การดำเนินงานของนายหน้าข้อมูลที่ทำการซื้อขายข้อมูลเป็นไปอย่างมีประสิทธิภาพและเกิดความเสียหายแก่เจ้าของข้อมูลอย่างน้อยที่สุด

5.2.2 ปัญหาเกี่ยวกับการกำหนดความรับผิดและบทลงโทษของผู้กระทำความผิด

แม้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะมีหลักการอยู่บนพื้นฐานของการรักษาความปลอดภัยของข้อมูลส่วนบุคคล แต่ในอีกแง่หนึ่ง หลักการและเงื่อนไขในบางส่วนของกฎหมายอาจสร้างโอกาสให้กับอาชญากรรมไซเบอร์ได้ เช่น ในกรณีที่ข้อมูลส่วนบุคคลรั่วไหลออกไปโดยมิชอบ หรือที่เรียกว่า “การละเมิดข้อมูลส่วนบุคคล” ซึ่งหมายถึง การสูญหาย การเข้าถึง การเปลี่ยนแปลง การแก้ไข หรือ การเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ซึ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลมิได้กำหนดความผิดสำหรับผู้กระทำการโดยมิชอบ หากปรากฏว่านายหน้าข้อมูลมิได้มีการจัดให้มีมาตรการรักษาความ

ปลอดภัยที่เหมาะสม อาชญากรอาจอาศัยโอกาสในการก่อให้เกิดความเสียหายและล่วงละเมิดต่อการรักษาความปลอดภัย ซึ่งส่งผลกระทบต่อชื่อเสียง ความน่าเชื่อถือในการทำธุรกิจ ซึ่งที่ผ่านมาภัยคุกคามที่เกิดมักจะมาจากการกระทำของบุคคลภายในองค์กรหรือหน่วยงานที่เป็นการกระทำโดยเจตนา เช่น ลูกจ้างเข้าถึงข้อมูลความลับทางการค้าในระบบที่ตนไม่มีสิทธิเข้าถึงเพื่อนำไปขายให้แก่บริษัทคู่แข่งของนายจ้าง ส่งผลให้เกิดความเสียหายต่อองค์กรโดยตรง ซึ่งในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีบัญญัติถึงความรับผิดทางแพ่ง ซึ่งอยู่ในมาตรา 77 ระบุว่า

“ มาตรา 77 ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลอันเป็นการฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติแห่งพระราชบัญญัตินี้ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล ต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้นแก่เจ้าของข้อมูลส่วนบุคคล ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่ก็ตาม เว้นแต่ ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้นจะพิสูจน์ได้ว่า

(1) ความเสียหายนั้นเกิดจากเหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั้นเอง

(2) เป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามหน้าที่และอำนาจตามกฎหมายค่าสินไหมทดแทนตามวรรคหนึ่ง ให้หมายความรวมถึงค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็นในการป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย ”

สำหรับความรับผิดทางแพ่งตามมาตรา 77 นั้น เป็นสิทธิของเจ้าของข้อมูลส่วนบุคคลกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลอันเป็นการฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติแห่งพระราชบัญญัตินี้ โดยให้ใช้ค่าสินไหมทดแทนแก่เจ้าของข้อมูลส่วนบุคคล ซึ่งจะสังเกตได้ว่า บุคคลที่จะต้องรับผิดทางแพ่งตามมาตรานี้มีเฉพาะผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเท่านั้น ไม่รวมถึงบุคคลที่สามที่เป็นผู้ก่อให้เกิดข้อมูลรั่วไหลที่แท้จริงก็เป็นได้ ซึ่งผู้เขียนเห็นว่าอาจต้องพิจารณากฎหมายอื่น เช่น อาจจะต้องฟ้องให้ชดใช้ตามกฎหมายแพ่งลักษณะละเมิดตามมาตรา 420 ซึ่งเป็นบททั่วไป และค่าสินไหมทดแทนที่จะต้องใช้ให้แก่เจ้าของข้อมูลส่วนบุคคลนั้นจะต้องเป็นค่าเสียหายที่แท้จริง ซึ่งเจ้าของข้อมูลส่วนบุคคลมีหน้าที่ที่จะต้องพิสูจน์ถึงความเสียหายที่เกิดขึ้นว่าความเสียหายมีเพียงใด เมื่อพิจารณาจากสภาพความเป็นจริงในบางกรณีอาจเป็นการยากที่จะพิสูจน์ความเสียหายอย่างเป็นรูปธรรม เนื่องจากเจ้าของข้อมูลส่วนบุคคลอาจไม่มีความเชี่ยวชาญทางเทคนิคที่จะสามารถพิสูจน์ได้ เช่น กรณีข้อมูลส่วนตัวได้รั่วไหลออกไปจากการที่มีบุคคลที่สามเข้าถึงระบบโดยมิชอบ

จึงเห็นสมควรเพื่อให้เจ้าของข้อมูลส่วนบุคคลที่ถูกละเมิดได้รับการเยียวยาความเสียหายควรกำหนดให้มีมาตรการในการเยียวยาความเสียหายให้แก่เจ้าของข้อมูลที่ได้รับความเสียหายหรือถูกละเมิดข้อมูลส่วนบุคคล ทั้งในด้านความเสียหายที่สามารถคำนวณเป็นจำนวนเงินได้และความเสียหายทางด้านจิตใจ ในกรณีการกำหนดความรับผิดและบทลงโทษของผู้กระทำความผิดได้มีการกำหนดมาตรการที่สามารถจัดการให้

บทลงโทษมีความเป็นธรรมต่อเจ้าของข้อมูลอย่างมากที่สุด หรือมีการกำหนดโทษที่มีความชัดเจน อาจทำให้ผู้กระทำความผิดเล็งเห็นได้ว่า หากกระทำการดังกล่าวไป อาจจะเกิดผลเสียต่อผู้ที่จะกระทำความผิด และเกิดความเกรงกลัวต่อความรับผิดและบทลงโทษที่ตนจะได้รับก็ได้

5.2.3 ปัญหาเกี่ยวกับการปรับใช้ข้อกฎหมายในการซื้อขายข้อมูลส่วนบุคคล

นายหน้าข้อมูล เป็นอาชีพที่ทำธุรกิจเกี่ยวกับการซื้อขายข้อมูล ซึ่งอาจรวมถึงการเก็บรวบรวมข้อมูลด้วย ในปัจจุบันการซื้อขายข้อมูลยังคงมีอยู่ในปัจจุบันและอาจแพร่หลายมากขึ้น หากสังเกตุจากการที่ประชาชนถูกหลอก ไม่ว่าจะเป็นทางโทรศัพท์ E-Mail หรือ SMS ก็ตาม โดยผู้ที่ต้องการแสวงหาผลประโยชน์โดยมิชอบ กฎหมายในเรื่องการซื้อขายที่มีอยู่ในปัจจุบันตามประมวลกฎหมายแพ่งและพาณิชย์ อาจไม่ครอบคลุมถึงการซื้อขายข้อมูล และในพระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ก็มิได้บัญญัติในส่วนของการซื้อขายข้อมูล โดยนายหน้าข้อมูลไว้

เนื่องจากในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มิได้บัญญัติเรื่องการซื้อขายข้อมูลส่วนบุคคลเอาไว้ จึงต้องพิจารณาว่าการซื้อขายข้อมูลส่วนบุคคลที่เกิดขึ้นในปัจจุบันจะสามารถนำประมวลกฎหมายแพ่งและพาณิชย์ว่าด้วยเรื่องซื้อขายมาปรับใช้หรือไม่นั้น ผู้เขียนมีความเห็นว่า สัญญาซื้อขายนั้นถือเป็นเอกเทศสัญญาซึ่งมีลักษณะเป็นสัญญาต่างตอบแทนอย่างหนึ่ง โดยผู้ขายตกลงขายทรัพย์สินโดยโอนกรรมสิทธิ์ในทรัพย์สินให้แก่ผู้ซื้อ และผู้ซื้อตกลงจะชดใช้ด้วยเงินตราเป็นราคาทรัพย์สินนั้นให้แก่ผู้ขาย และกรรมสิทธิ์ในทรัพย์สินที่ขายย่อมโอนให้แก่ผู้ซื้อตั้งแต่ขณะเมื่อได้ทำสัญญาซื้อขายกัน ซึ่งหมายความว่า ผลตามสัญญาซื้อขายคือกรรมสิทธิ์ในทรัพย์สินจะโอนไปยังผู้ซื้อโดยข้อสัญญาที่ได้ทำกันขึ้นระหว่างคู่สัญญา โดยไม่จำต้องมีการส่งมอบทรัพย์สินหรือชำระราคาในขณะนั้นแต่อย่างใด เพียงแต่ผู้ซื้อตกลงว่าจะใช้ราคาทรัพย์สินนั้นให้แก่ผู้ขาย สัญญาซื้อขายนั้นก็เกิดขึ้นแล้ว ซึ่งจะต้องมีลักษณะเป็นกรรมสิทธิ์ในตัวทรัพย์นั้นจึงจะทำการซื้อขายตามประมวลกฎหมายแพ่งและพาณิชย์ว่าด้วยเรื่องซื้อขายได้ ซึ่งในส่วนของข้อมูลส่วนบุคคลนั้นจากที่ได้กล่าวไว้แล้วข้างต้นว่า กฎหมายคุ้มครองข้อมูลส่วนบุคคลไม่ได้กำหนดสิทธิในความเป็นเจ้าของในลักษณะเดียวกับกรรมสิทธิ์ แต่เป็นการกำหนดหลักการคุ้มครองบุคคลที่ข้อมูลนั้นระบุตัวและให้สิทธิบางประการ ซึ่งมีลักษณะที่แตกต่างกับกรรมสิทธิ์ของทรัพย์สินทั่วๆไป ถึงแม้ว่าในพระราชบัญญัติจะใช้คำว่า “เจ้าของข้อมูลส่วนบุคคล” แต่ก็ความหมายที่แตกต่างจากเจ้าของกรรมสิทธิ์ในทรัพย์ จึงอาจกล่าวได้ว่า เจ้าของข้อมูลส่วนบุคคลไม่ใช่เจ้าของกรรมสิทธิ์ในข้อมูลนั้น ดังนั้น ในการซื้อขายข้อมูลส่วนบุคคลจึงไม่สามารถนำประมวลกฎหมายแพ่งและพาณิชย์ว่าด้วยเรื่องซื้อขายมาปรับใช้ในกรณีการซื้อขายข้อมูลส่วนบุคคลได้แต่อย่างใด

การเข้าถึงข้อมูลส่วนตัวของผู้อื่นโดยไม่มีกฎหมายบัญญัติรองรับไว้ย่อมเป็นการละเมิดต่อสิทธิส่วนบุคคลของบุคคลผู้นั้น ย่อมถือว่าเป็นการกระทำโดยมิชอบด้วยกฎหมาย เพราะนอกจากจะเป็นการผิดมรรยาทตามวิชาชีพของผู้ประกอบการแล้ว ยังถือว่าเป็นการละเมิดสิทธิส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลโดยไม่มีเหตุอันควรด้วย เมื่อไม่มีบทบัญญัติกฎหมายรองรับไว้โดยเฉพาะ จึงสมควรที่จะกำหนดหลักเกณฑ์ มาตรการ

กำกับดูแลในการซื้อขายข้อมูลส่วนบุคคลไว้เป็นการเฉพาะเพื่อผลประโยชน์ในทางเศรษฐกิจของประเทศไทย และก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลให้น้อยที่สุด

การจัดเก็บข้อมูลส่วนบุคคลโดยทั่วไปแล้วมีจุดมุ่งหมายเพื่อให้บริการ หรือเพื่อดำเนินการทางนิติกรรม หรือธุรกรรมกับผู้ที่เป็นเจ้าของข้อมูล ซึ่งปกติแล้วการที่เจ้าของข้อมูลให้ข้อมูลด้วยความเข้าใจว่าข้อมูลที่บริษัทหรือหน่วยงานจัดเก็บไว้นั้นก็เพื่อใช้ในกิจกรรมที่ตนเองเกี่ยวข้อง แต่ปัญหาที่เกิดขึ้นในปัจจุบันบ่อยๆนั้น ผู้ที่มีหน้าที่จัดเก็บข้อมูลดังกล่าวอาจนำข้อมูลไปใช้ในทางอื่นที่เจ้าของข้อมูลไม่ต้องการให้ทำ หรือหากวิธีการจัดเก็บไม่ดีก็อาจมีผู้ลักลอบนำข้อมูลไปใช้ประโยชน์ในทางที่มิชอบได้

ด้วยเหตุดังกล่าวข้างต้นจึงควรที่จะมีบทบัญญัติกฎหมายใช้บังคับในการซื้อขายข้อมูลสำหรับนายหน้าข้อมูล โดยออกเป็นกฎหมาย กำหนดหลักเกณฑ์ ประเภทข้อมูลที่สามารถซื้อขายได้ ระเบียบวิธีในทางปฏิบัติในการซื้อขายข้อมูลส่วนบุคคล เพื่อให้อยู่ภายใต้กรอบที่กฎหมายกำหนด การดูแลจัดเก็บข้อมูล การใช้ การเปิดเผยข้อมูลส่วนบุคคล ซึ่งไม่ก่อให้เกิดความเดือดร้อนแก่เจ้าของข้อมูลที่แท้จริง ควรอยู่ในมาตรฐานความปลอดภัยขั้นสูงและกำหนดหลักเกณฑ์ถึงความปลอดภัยต่อข้อมูลของเจ้าของข้อมูล โดยให้คำนึงถึงสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลในการที่จะดำเนินกิจกรรมใดๆ รวมไปถึงแนวทางปฏิบัติของนายหน้าข้อมูล ซึ่งอาจรวมถึงผู้ควบคุมข้อมูล และผู้ประมวลผลข้อมูล โดยจัดให้มีความสอดคล้องกับกฎหมายของประเทศอื่นๆที่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่มีคุณภาพ เพื่อให้การคุ้มครองข้อมูล การจัดเก็บ การประมวลผล รวมถึงการนำข้อมูลดังกล่าวไปใช้ให้เป็นไปอย่างมีประสิทธิภาพ เพื่อก่อให้เกิดประโยชน์แก่ภาพลักษณ์เศรษฐกิจของประเทศไทยและก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลให้น้อยที่สุด

บรรณานุกรม

บรรณานุกรม

ชื่อผู้แต่ง, ‘กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย’ <http://www.oic.go.th/FILEROOM/CABOICFORM02/DRAWER05/GENERAL/DATA0000 00000333.PDF.> สืบค้นเมื่อ 6 กรกฎาคม 2565.

กิตติพงศ์ กมลธรรมวงศ์, ‘ประสบการณ์ของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศสาธารณรัฐสิงคโปร์ : บทเรียนสำหรับประเทศไทย’ (2563) 2 วารสารสังคมวิจัยและพัฒนา 2.

กิตติพงศ์ กมลธรรมวงศ์, ‘การคุ้มครองข้อมูลข่าวสารส่วนบุคคลในระบบกฎหมายไทย : ปัญหาและแนวทางการแก้ไข’ (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ 2549).

กรมส่งเสริมอุตสาหกรรม. ‘ข้อมูลส่วนบุคคลคืออะไร สำคัญแค่ไหน’ <https://dip360.dip.go.th/ข้อมูลส่วนบุคคลคืออะไร.> สืบค้นเมื่อ 15 กรกฎาคม 2565.

คณาธิป ทองรวีวงศ์, ‘ปัญหากฎหมายเกี่ยวกับการคุ้มครองสิทธิส่วนบุคคลของบุคคลสาธารณะ:กรณีศึกษาเปรียบเทียบกฎหมายสหรัฐอเมริกาและกฎหมายไทย’ (2558) 7 วารสารวิชาการ คณะนิติศาสตร์ มหาวิทยาลัยหอการค้าไทย 1.

คณะกรรมการสิทธิมนุษยชนแห่งชาติ, ประมวลศัพท์และความรู้สิทธิมนุษยชน เล่ม 2 คณะกรรมการสิทธิมนุษยชนแห่งชาติ ศัพท์สิทธิมนุษยชน ในกระบวนการยุติธรรมและสิทธิมนุษยชนศึกษา (พิมพ์ครั้งที่ 1 2556).

จิตรทิวัส โคตรทัศน์, ‘มาตรการทางกฎหมายในการควบคุมการทำสัญญานายหน้าอสังหาริมทรัพย์’ (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิตย์ คณะนิติศาสตร์ มหาวิทยาลัยศรีปทุม 2564).

จรัล โฆษณานันท์, *สิทธิมนุษยชนไร้พรมแดน : ปรัชญา กฎหมาย และความเป็นจริงทางสังคม* (นิติธรรม 2545).

จันทร์ทิพย์ แสงแปง, ‘ปัญหาการคุ้มครองข้อมูลส่วนบุคคล ศึกษากรณี การจัดเก็บข้อมูลส่วนบุคคลในหน่วยงานเอกชน’ (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต สถาบันบัณฑิตพัฒนศาสตร์ 2559).

ชุลีพร น่วมทนง, ‘สิทธิมนุษยชนกับการคุ้มครองข้อมูลส่วนบุคคล’ (เอกสารวิชาการการอบรมหลักสูตรหลักนิติธรรมเพื่อประชาธิปไตย รุ่นที่ 2 วิทยาลัยรัฐธรรมนูญ สถาบันรัฐธรรมนูญศึกษา สำนักงานศาลรัฐธรรมนูญ).

ณฐพร วิริยะลัพภะ และ ธเนศ สุจารีกุล, ‘ปัญหาทางกฎหมายเกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลพ.ศ.2562 : ศึกษากรณีหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 39’ (การประชุมนำเสนอผลงานวิจัยระดับบัณฑิตศึกษา ครั้งที่ 15).

ไทยรัฐออนไลน์. ‘ข้อมูลส่วนบุคคล ขายเกลื่อน ราคาถูก คนไทยโดนดูดเงิน DES ดูดาย?’ <https://www.thairath.co.th/scoop/theissue/2224486.> สืบค้น 6 กรกฎาคม 2565.

นคร เสรีรักษ์. ‘มาตรฐานสากลในการคุ้มครองข้อมูลส่วนบุคคล:ผลกระทบต่อประเทศไทย’
<https://www.fpps.or.th/news.php?detail=n1588215051.news.>
สืบค้นเมื่อ 14 กรกฎาคม 2565.

นคร เสรีรักษ์. ‘ความเป็นส่วนตัวภายใต้รัฐธรรมนูญใหม่ ต้องจับตา’
<https://www.ilaw.or.th/node/4255.> สืบค้นเมื่อ 10 กันยายน 2565.

นริศ ชำนาญชานันท์, ‘ละเมิดอำนาจศาล: โทษที่ขัดต่อกระบวนการ Due Process’
(2539, มกราคม) วารสารอัยการ.

บุญศรี มีวงศ์อุโฆษ, *กฎหมายรัฐธรรมนูญ*, โครงการตำราและเอกสารประกอบการสอนคณะนิติศาสตร์
มหาวิทยาลัยธรรมศาสตร์.

บรรเจิด สิงคะเนติ, หลักพื้นฐานเกี่ยวกับสิทธิเสรีภาพและศักดิ์ศรีความเป็นมนุษย์,
(พิมพ์ครั้งที่ 3 วิญญูชน 2552).

ปัณณทัต กาญจนะวสิต, *โลกยุค 4.0World 4.0*, (สำนักงานเลขานุการกองทัพบก 2559).

ปิยะพร วงศ์เบี้ยสัจจ์, ‘การเปิดเผยข้อมูลส่วนบุคคลโดยธนาคารพาณิชย์กับมาตรการทางกฎหมาย
ในการคุ้มครองข้อมูลส่วนบุคคล’ (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต
คณะนิติศาสตร์ปรีดี พนมยงค์ มหาวิทยาลัยธุรกิจบัณฑิตย์ 2552).

พิชัยศักดิ์ หรยางกูร, อาจารย์นริศรา แดงไผ่, ‘หน่วยที่ 3 หลักความยินยอม’
<https://www.stou.ac .th/Schools/Slw/upload/Ex%2040701-3.pdf.>
สืบค้นเมื่อ 6 สิงหาคม 2565.

มาโนช สุทธิวาทนฤพุฒิ, *กฎหมายแพ่งและพาณิชย์ว่าด้วยตัวแทน นายหน้า*, (ศรีเมืองการพิมพ์ 2538).

ร. แรงกาต์, *ประวัติศาสตร์กฎหมายไทย เล่ม 2* (พิมพ์ครั้งที่1 ไทยวัฒนาพาณิชย์ 2526).

วิจักขณ์ภัค เกศา, ‘กฎหมายนายหน้าอสังหาริมทรัพย์ในประเทศไทย: ศึกษาเปรียบเทียบกับกฎหมาย
นายหน้าอสังหาริมทรัพย์ประเทศสิงคโปร์ และประเทศฟิลิปปินส์’
(สารนิพนธ์ นิติศาสตรมหาบัณฑิต สาขานิติศาสตร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช 2559).

วรนารี สิงโต, ‘หน่วยที่ 1 หลักสุจริต’ <https://www.stou. ac.th/schools /slw/upload/ex40701-1.pdf.>
สืบค้นเมื่อ 1 สิงหาคม 2565.

ศิริกุล ภู่พันธ์, ‘ข้อความคิดว่าด้วยข้อมูลข่าวสารส่วนบุคคล’ (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต
คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ 2548).

สุขวสา ถมังรักษ์สัตว์, ‘การคุ้มครองข้อมูลส่วนบุคคลของเด็กบนสื่ออิเล็กทรอนิกส์’ (2562 มกราคม-มิถุนายน)
20 วารสารเกษมบัณฑิต 1.

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, ‘สรุปสาระสำคัญ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ.

2562'.
<https://www.dct.or.th/upload/downloads/1612025563SummaryPDPA_DigitalCouncilofThailand.pdf.> สืบค้นเมื่อ 15 กรกฎาคม 2565.

สำนักงานเศรษฐกิจการคลัง, 'พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พุทธศักราช 2545'
<http://www.fpo.go.th/FPO/index2.php?mod=Category&file=categoryview&categoryID=CAT0000 506.Admin> สืบค้นเมื่อ 8 มกราคม 2565.

สกล อดิศรประเสริฐ, 'มาตรการทางกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคล: ศึกษาเฉพาะกรณีการแยกแยะประเภทข้อมูล' (วิทยานิพนธ์ นิติศาตรมหาบัณฑิตย์ มหาวิทยาลัยธุรกิจบัณฑิตย์ 2553).

สาครรัตน์ นักปราชญ์, และ คัคนางค์ จามะริก, 'การเปิดเผยข้อมูลภาครัฐในรูปแบบ (Business Intelligence (BI) ในยุค Big Data)' (2559) วารสาร กสทช.
<https://so04.tci-thaijo.org/index.php/NBTC_Journal/ article/download/119148/91209/308584.> สืบค้นเมื่อ 1 สิงหาคม 2565.

สถิต เล็งไธวง, *กฎหมายลักษณะตัวแทน และนายหน้า* (พิมพ์ครั้งที่4 ห้างหุ้นส่วนจำกัด พิมพ์อักษร 2550).

สถาบันวิจัยเพื่อการพัฒนาประเทศไทย, กฎหมายของประเทศสิงคโปร์และข้อกฎหมายที่เกี่ยวข้องกับการค้าและการลงทุนของประเทศสิงคโปร์ (สำนักงานคณะกรรมการกฤษฎีกา 2550).

สุพิศ ประณีตพลกรัง, *หลักและทฤษฎีกฎหมายแพ่ง*, (พิมพ์ครั้งที่ 4 นิติธรรม 2565).

สุรชัย ศรีสารคาม, 'บทความเกี่ยวกับหลักสิทธิมนุษยชน'
<https://www.constitutionalcourt.or.th/occ_web/ewt_dl_link.php?nid=1394.> สืบค้นเมื่อ 14 มกราคม 2566.

หยุด แสงอุทัย, ความรู้เบื้องต้นเกี่ยวกับกฎหมายทั่วไป (พิมพ์ครั้งที่ 16 สำนักพิมพ์ประกายพรึก 2548).

อุดม รัฐอมฤต, สมคิด เลิศไพฑูรย์ และกิตติพงศ์ กมลธรรมวงศ์, *พัฒนามาตรการในการดำเนินการพิจารณาความเหมาะสมความเป็นไปได้ เพื่อจัดทำแนวทาง ขั้นตอนและวิธีการในการเข้าร่วมหรือทำความตกลงตามกรอบว่าด้วยการคุ้มครองความเป็นส่วนตัวของ APEC (APEC Privacy Framework)* (สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์ 2557).

อธิพร สิทธิธีรรัตน์, 'ปัญหากฎหมายการคุ้มครองข้อมูลส่วนบุคคลในบริบทอิเล็คทรอนิกส์'
(วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ 2558).

ภาษาต่างประเทศ

Albert blackmann, StaatsrechDie Grundrechte, 4 Autl.,1997,s.543

Dataguidance. “Vermont: Overview of the Data Broker Act”. https://www.dataguidance.com/opinion/vermont-overview-data-broker-act.

Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

Duering,Grundgedetz-Kommentar,Art.1,Abs.1,Rdnr.17

European commission ,“legislation” <http://ec.europa.eu/legislation/index_en.html> Accedssed 14 March 2016.

François Collart Dutilleul et Phililppe Delebecque. (2011). Contracts civils et commerciaux (9 éd). Dalloz: Collection Précis.

GDPR : Article 4

Mark Littman and Peter Carter Ruck, (1970), Privacy and the Law. P.21.

PERSONAL DATA PROTECTION ACT 2012

Practical Law Data Privacy Advisor. “Vermont Enacts First Data Broker Law” Available: https://content.next.westlaw.com/practicallaw/document/Ie07faf6e641e11e89bf199c0ee06c731/Legal-Updates-Vermont-Enacts-First-Data-Broker-Law?viewType=FullText&transitionType=Default&contextData=%28sc.De fault%29

Raymond Wacks. (1993). Personal Information: Privacy and the Law. P. 51

The Vermont Office of the Attorney General. “Guidance on Vermont’s Act 171 of 2018 Data Broker Regulation December 11, 2018” Availablehttps://ago.vermont.gov/wp-content/uploads/2018/12/2018-12-11-VT-Data-Broker-Regulation-Guidance.pdf.

Universal Declaration og Human Right 1948, article 12

Universal Declaration of Human Rights 1948 Article 29.

Warren, D, Samual and Brandies, D, Louis. (1890). The Right to Privacy. Harvard Law Review, Vol IV December15,1890, Available http://www.lawrence.edu/fast/boardmaw.

William L. Prosser, Handbook of the law of torts,4 ed. (London: St.Paul, Minn. West Publishing Co 1971). p. 804-814.

ภาคผนวก

California Civil Code

CIVIL CODE - CIV

DIVISION 3. OBLIGATIONS [1427 - 3273.55] (Heading of Division 3 amended by Stats. 1988, Ch. 160, Sec. 14.)

PART 4. OBLIGATIONS ARISING FROM PARTICULAR TRANSACTIONS [1738 - 3273.55] (Part 4 enacted 1872.)

TITLE 1.81.48. Data Broker Registration [1798.99.80 - 1798.99.88] (Title 1.81.48 added by Stats. 2019, Ch. 753, Sec. 2.)

1798.99.80.

For purposes of this title:

(a) “Business” has the meaning provided in subdivision (d) of Section 1798.140.

(b) “Collects” and “collection” have the meaning provided in subdivision (f) of Section 1798.140.

(c) “Consumer” has the meaning provided in subdivision (i) of Section 1798.140.

(d) “Data broker” means a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship. “Data broker” does not include any of the following:

(1) A consumer reporting agency to the extent that it is covered by the federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.).

(2) A financial institution to the extent that it is covered by the Gramm-Leach-Bliley Act (Public Law 106-102) and implementing regulations.

(3) An entity to the extent that it is covered by the Insurance Information and Privacy Protection Act (Article 6.6 (commencing with Section 791) of Chapter 1 of Part 2 of Division 1 of the Insurance Code).

(e) “Personal information” has the meaning provided in subdivision (v) of Section 1798.140.

(f) “Sell” has the meaning provided in subdivision (ad) of Section 1798.140.

(g) “Third party” has the meaning provided in subdivision (ai) of Section 1798.140.

(Amended by Stats. 2022, Ch. 420, Sec. 10. (AB 2960) Effective January 1, 2023.)

1798.99.81.

A fund to be known as the "Data Brokers' Registry Fund" is hereby created within the State Treasury. All registration fees received pursuant to paragraph (1) of subdivision (b) of Section 1798.99.82 shall be deposited into the Data Brokers' Registry Fund, to be available for expenditure by the Department of Justice, upon appropriation by the Legislature, to offset costs of establishing and maintaining the informational internet website described in Section 1798.99.84.

(Added by Stats. 2020, Ch. 14, Sec. 3. (AB 82) Effective June 29, 2020.)

1798.99.82.

(a) On or before January 31 following each year in which a business meets the definition of data broker as provided in this title, the business shall register with the Attorney General pursuant to the requirements of this section.

(b) In registering with the Attorney General, as described in subdivision (a), a data broker shall do all of the following:

(1) Pay a registration fee in an amount determined by the Attorney General, not to exceed the reasonable costs of establishing and maintaining the informational internet website described in Section 1798.99.84. Registration fees shall be deposited in the Data Brokers' Registry Fund, created within the State Treasury pursuant to Section 1798.99.81, and used for the purposes outlined in this paragraph.

(2) Provide the following information:

(A) The name of the data broker and its primary physical, email, and internet website addresses.

(B) Any additional information or explanation the data broker chooses to provide concerning its data collection practices.

(c) A data broker that fails to register as required by this section is subject to injunction and is liable for civil penalties, fees, and costs in an action brought in the name of the people of the State of California by the Attorney General as follows:

(1) A civil penalty of one hundred dollars ($100) for each day the data broker fails to register as required by this section.

(2) An amount equal to the fees that were due during the period it failed to register.

(3) Expenses incurred by the Attorney General in the investigation and prosecution of the action as the court deems appropriate.

(d) Any penalties, fees, and expenses recovered in an action prosecuted under subdivision (c) shall be deposited in the Consumer Privacy Fund, created within the General Fund pursuant to subdivision (a) of Section 1798.160, with the intent that they be used to fully offset costs incurred by the state courts and the Attorney General in connection with this title.

(Amended by Stats. 2020, Ch. 14, Sec. 4. (AB 82) Effective June 29, 2020.)

1798.99.84.

The Attorney General shall create a page on its internet website where the information provided by data brokers under this title shall be accessible to the public.

(Added by Stats. 2019, Ch. 753, Sec. 2. (AB 1202) Effective January 1, 2020.)

1798.99.88.

Nothing in this title shall be construed to supersede or interfere with the operation of the California Consumer Privacy Act of 2018 (Title 1.81.5 (commencing with Section 1798.100)).

The Vermont Data Broker Regulation (Act 171 of 2018)

Title 9: Commerce And Trade

Chapter 62: Protection Of Personal Information

Subchapter 1: General Provisions

§ 2430. Definitions

As used in this chapter:

(1)(A) “Brokered personal information” means one or more of the following computerized data elements about a consumer, if categorized or organized for dissemination to third parties:

(i) name;

(ii) address;

(iii) date of birth;

(iv) place of birth;

(v) mother’s maiden name;

(vi) unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data;

(vii) name or address of a member of the consumer's immediate family or household;

(viii) Social Security number or other government-issued identification number; or

(ix) other information that, alone or in combination with the other information sold or licensed, would allow a reasonable person to identify the consumer with reasonable certainty.

(B) "Brokered personal information" does not include publicly available information to the extent that it is related to a consumer's business or profession.

(2) "Business" means a commercial entity, including a sole proprietorship, partnership, corporation, association, limited liability company, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the laws of this State, any other state, the United States, or any other country, or the parent, affiliate, or subsidiary of a financial institution, but does not include the State, a State agency, any political subdivision of the State, or a vendor acting solely on behalf of, and at the direction of, the State.

(3) "Consumer" means an individual residing in this State.

(4)(A) "Data broker" means a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship.

(B) Examples of a direct relationship with a business include if the consumer is a past or present:

(i) customer, client, subscriber, user, or registered user of the business's goods or services;

(ii) employee, contractor, or agent of the business;

(iii) investor in the business; or

(iv) donor to the business.

(C) The following activities conducted by a business, and the collection and sale or licensing of brokered personal information incidental to conducting these activities, do not qualify the business as a data broker:

(i) developing or maintaining third-party e-commerce or application platforms;

(ii) providing 411 directory assistance or directory information services, including name, address, and telephone number, on behalf of or as a function of a telecommunications carrier;

(iii) providing publicly available information related to a consumer's business or profession; or

(iv) providing publicly available information via real-time or near-real-time alert services for health or safety purposes.

(D) The phrase "sells or licenses" does not include:

(i) a one-time or occasional sale of assets of a business as part of a transfer of control of those assets that is not part of the ordinary conduct of the business; or

(ii) a sale or license of data that is merely incidental to the business.

(5)(A) "Data broker security breach" means an unauthorized acquisition or a reasonable belief of an unauthorized acquisition of more than one element of brokered personal information maintained by a data broker when the brokered personal information is not encrypted, redacted, or protected by another method that renders the information unreadable or unusable by an unauthorized person.

(B) "Data broker security breach" does not include good faith but unauthorized acquisition of brokered personal information by an employee or agent of the data broker for a legitimate purpose of the data broker, provided that the brokered personal information is not used for a purpose unrelated to the data broker's business or subject to further unauthorized disclosure.

(C) In determining whether brokered personal information has been acquired or is reasonably believed to have been acquired by a person without valid authorization, a data broker may consider the following factors, among others:

(i) indications that the brokered personal information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing brokered personal information;

(ii) indications that the brokered personal information has been downloaded or copied;

(iii) indications that the brokered personal information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or

(iv) that the brokered personal information has been made public.

(6) "Data collector" means a person who, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with personally identifiable

information, and includes the State, State agencies, political subdivisions of the State, public and private universities, privately and publicly held corporations, limited liability companies, financial institutions, and retail operators.

(7) “Encryption” means use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key.

(8) “License” means a grant of access to, or distribution of, data by one person to another in exchange for consideration. A use of data for the sole benefit of the data provider, where the data provider maintains control over the use of the data, is not a license.

(9) “Login credentials” means a consumer’s user name or e-mail address, in combination with a password or an answer to a security question, that together permit access to an online account.

(10)(A) “Personally identifiable information” means a consumer’s first name or first initial and last name in combination with one or more of the following digital data elements, when the data elements are not encrypted, redacted, or protected by another method that renders them unreadable or unusable by unauthorized persons:

(i) a Social Security number;

(ii) a driver license or nondriver State identification card number, individual taxpayer identification number, passport number, military identification card number, or other identification number that originates from a government identification document that is commonly used to verify identity for a commercial transaction;

(iii) a financial account number or credit or debit card number, if the number could be used without additional identifying information, access codes, or passwords;

(iv) a password, personal identification number, or other access code for a financial account;

(v) unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data;

(vi) genetic information; and

(vii)(I) health records or records of a wellness program or similar program of health promotion or disease prevention;

(II) a health care professional’s medical diagnosis or treatment of the consumer; or

(III) a health insurance policy number.

(B) “Personally identifiable information” does not mean publicly available information that is lawfully made available to the general public from federal, State, or local government records.

(11) “Record” means any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics.

(12) “Redaction” means the rendering of data so that the data are unreadable or are truncated so that no more than the last four digits of the identification number are accessible as part of the data.

(13)(A) “Security breach” means unauthorized acquisition of electronic data, or a reasonable belief of an unauthorized acquisition of electronic data, that compromises the security, confidentiality, or integrity of a consumer’s personally identifiable information or login credentials maintained by a data collector.

(B) “Security breach” does not include good faith but unauthorized acquisition of personally identifiable information or login credentials by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personally identifiable information or login credentials are not used for a purpose unrelated to the data collector’s business or subject to further unauthorized disclosure.

(C) In determining whether personally identifiable information or login credentials have been acquired or is reasonably believed to have been acquired by a person without valid authorization, a data collector may consider the following factors, among others:

(i) indications that the information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing information;

(ii) indications that the information has been downloaded or copied;

(iii) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or

(iv) that the information has been made public. (Added 2005, No. 162 (Adj. Sess.), § 1, eff. Jan. 1, 2007; amended 2011, No. 109 (Adj. Sess.), § 4, eff. May 8, 2012; 2017, No. 171 (Adj. Sess.), § 2, eff. Jan. 1, 2019; 2019, No. 89 (Adj. Sess.), § 2.)

§ 2431. Acquisition of brokered personal information; prohibitions

(a) Prohibited acquisition and use.

(1) A person shall not acquire brokered personal information through fraudulent means.

(2) A person shall not acquire or use brokered personal information for the purpose of:

(A) stalking or harassing another person;

(B) committing a fraud, including identity theft, financial fraud, or e-mail fraud; or

(C) engaging in unlawful discrimination, including employment discrimination and housing discrimination.

(b) Enforcement.

(1) A person who violates a provision of this section commits an unfair and deceptive act in commerce in violation of section 2453 of this title.

(2) The Attorney General has the same authority to adopt rules to implement the provisions of this section and to conduct civil investigations, enter into assurances of discontinuance, bring civil actions, and take other enforcement actions as provided under chapter 63, subchapter 1 of this title. (Added 2017, No. 171 (Adj. Sess.), § 2, eff. Jan. 1, 2019.)

Subchapter 2: Security Breach Notice Act

§ 2435. Notice of security breaches

(a) This section shall be known as the Security Breach Notice Act.

(b) Notice of breach.

(1) Except as otherwise provided in subsection (d) of this section, any data collector that owns or licenses computerized personally identifiable information or login credentials shall notify the consumer that there has been a security breach following discovery or notification to the data collector of the breach. Notice of the security breach shall be made in the most expedient time possible and without unreasonable delay, but not later than 45 days after the discovery or notification, consistent with the legitimate needs of the law enforcement agency, as provided in subdivisions (3) and (4) of this subsection, or with any measures necessary to determine the scope of the security breach and restore the reasonable integrity, security, and confidentiality of the data system.

(2) Any data collector that maintains or possesses computerized data containing personally identifiable information or login credentials that the data collector does not own or license or any data collector that acts or conducts business in Vermont that maintains or possesses records or data containing personally identifiable information or login credentials that the data collector does not own or license shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement as provided in subdivisions (3) and (4) of this subsection.

(3) A data collector or other entity subject to this subchapter shall provide notice of a breach to the Attorney General or to the Department of Financial Regulation, as applicable, as follows:

(A) A data collector or other entity regulated by the Department of Financial Regulation under Title 8 or this title shall provide notice of a breach to the Department. All other data collectors or other entities subject to this subchapter shall provide notice of a breach to the Attorney General.

(B)(i) The data collector shall notify the Attorney General or the Department, as applicable, of the date of the security breach and the date of discovery of the breach and shall provide a preliminary description of the breach within 14 business days, consistent with the legitimate needs of the law enforcement agency as provided in this subdivision (3) and subdivision (4) of this subsection (b), of the data collector's discovery of the security breach or when the data collector provides notice to consumers pursuant to this section, whichever is sooner.

(ii) Notwithstanding subdivision (B)(i) of this subdivision (b)(3), a data collector who, prior to the date of the breach, on a form and in a manner prescribed by the Attorney General, had sworn in writing to the Attorney General that it maintains written policies and procedures to maintain the security of personally identifiable information or login credentials and respond to a breach in a manner consistent with Vermont law shall notify the Attorney General of the date of the security breach and the date of discovery of the breach and shall provide a description of the breach prior to providing notice of the breach to consumers pursuant to subdivision (1) of this subsection (b).

(iii) If the date of the breach is unknown at the time notice is sent to the Attorney General or to the Department, the data collector shall send the Attorney General or the Department the date of the breach as soon as it is known.

(iv) Unless otherwise ordered by a court of this State for good cause shown, a notice provided under this subdivision (3)(B) shall not be disclosed to any person other than the Department, the authorized agent or representative of the Attorney General, a State's Attorney, or another law enforcement officer engaged in legitimate law enforcement activities without the consent of the data collector.

(C)(i) When the data collector provides notice of the breach pursuant to subdivision (1) of this subsection (b), the data collector shall notify the Attorney General or the Department, as applicable, of the number of Vermont consumers affected, if known to the data collector, and shall provide a copy of the notice provided to consumers under subdivision (1) of this subsection (b).

(ii) The data collector may send to the Attorney General or the Department, as applicable, a second copy of the consumer notice, from which is redacted the type of personally identifiable information or login credentials that was subject to the breach, and which the Attorney General or the Department shall use for any public disclosure of the breach.

(D) If a security breach is limited to an unauthorized acquisition of login credentials, a data collector is only required to provide notice of the security breach to the Attorney General or Department of Financial Regulation, as applicable, if the login credentials were acquired directly from the data collector or its agent.

(4)(A) The notice to a consumer required by this subsection shall be delayed upon request of a law enforcement agency. A law enforcement agency may request the delay if it believes that notification may impede a law enforcement investigation, or a national or Homeland Security investigation, or jeopardize public safety or national or Homeland Security interests. In the event law enforcement makes the request for a delay in a manner other than in writing, the data collector shall document such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. A law enforcement agency shall promptly notify the data collector in writing when the law enforcement agency no longer believes that notification may impede a law enforcement investigation, or a national or Homeland Security investigation, or jeopardize public safety or national or Homeland Security interests. The data collector shall provide notice required by this section without unreasonable delay upon receipt of a written communication, which includes facsimile or electronic communication, from the law enforcement agency withdrawing its request for delay.

(B) A Vermont law enforcement agency with a reasonable belief that a security breach has or may have occurred at a specific business shall notify the business in writing of its belief. The agency shall also notify the business that additional information on the security breach may need to be furnished to the Office of the Attorney General or the Department of Financial Regulation and shall include the website and telephone number for the Office and the Department in the notice required by this subdivision (4)(B). Nothing in this subdivision (4)(B) shall alter the responsibilities of a data collector under this section or provide a cause of action against a law enforcement agency that fails, without bad faith, to provide the notice required by this subdivision (4)(B).

(5) The notice to a consumer required in subdivision (1) of this subsection shall be clear and conspicuous. A notice to a consumer of a security breach involving personally identifiable information shall include a description of each of the following, if known to the data collector:

(A) the incident in general terms;

(B) the type of personally identifiable information that was subject to the security breach;

(C) the general acts of the data collector to protect the personally identifiable information from further security breach;

(D) a telephone number, toll-free if available, that the consumer may call for further information and assistance;

(E) advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports; and

(F) the approximate date of the security breach.

(6) A data collector may provide notice of a security breach involving personally identifiable information to a consumer by one or more of the following methods:

(A) Direct notice, which may be by one of the following methods:

(i) written notice mailed to the consumer's residence;

(ii) electronic notice, for those consumers for whom the data collector has a valid e-mail address, if:

(I) the data collector's primary method of communication with the consumer is by electronic means, the electronic notice does not request or contain a hypertext link to a request that the consumer provide personal information, and the electronic notice conspicuously warns consumers not to provide personal information in response to electronic communications regarding security breaches; or

(II) the notice is consistent with the provisions regarding electronic records and signatures for notices in 15 U.S.C. § 7001; or

(iii) telephonic notice, provided that telephonic contact is made directly with each affected consumer and not through a prerecorded message.

(B)(i) Substitute notice, if:

(I) the data collector demonstrates that the lowest cost of providing notice to affected consumers pursuant to subdivision (6)(A) of this subsection among written, e-mail, or telephonic notice would exceed $10,000.00; or

(II) the data collector does not have sufficient contact information.

(ii) A data collector shall provide substitute notice by:

(I) conspicuously posting the notice on the data collector's website if the data collector maintains one; and

(II) notifying major statewide and regional media.

(c) In the event a data collector provides notice to more than 1,000 consumers at one time pursuant to this section, the data collector shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notice. This subsection shall not apply to a person who is licensed or registered under Title 8 by the Department of Financial Regulation.

(d)(1) Notice of a security breach pursuant to subsection (b) of this section is not required if the data collector establishes that misuse of personally identifiable information or login credentials is not reasonably possible and the data collector provides notice of the determination that the misuse of the personally identifiable information or login credentials is not reasonably possible pursuant to the requirements of this subsection. If the data collector establishes that misuse of the personally identifiable information or login credentials is not reasonably possible, the data collector shall provide notice of its determination that misuse of the personally identifiable information or login credentials is not reasonably possible and a detailed explanation for said determination to the Vermont Attorney General or to the Department of Financial Regulation in the event that the data collector is a person or entity licensed or registered with the Department under Title 8 or this title. The data collector may designate its notice and detailed explanation to the Vermont Attorney General or the Department of Financial Regulation as "trade secret" if the notice and detailed explanation meet the definition of trade secret contained in 1 V.S.A. § 317(c)(9).

(2) If a data collector established that misuse of personally identifiable information or login credentials was not reasonably possible under subdivision (1) of this subsection, and subsequently obtains facts indicating that misuse of the personally identifiable information or login credentials has occurred or is occurring, the data collector shall provide notice of the security breach pursuant to subsection (b) of this section.

(3) If a security breach is limited to an unauthorized acquisition of login credentials for an online account other than an e-mail account the data collector shall provide notice of the security breach to the consumer electronically or through one or more of the methods specified in subdivision

(b)(6) of this section and shall advise the consumer to take steps necessary to protect the online account, including to change his or her login credentials for the account and for any other account for which the consumer uses the same login credentials.

(4) If a security breach is limited to an unauthorized acquisition of login credentials for an email account:

(A) the data collector shall not provide notice of the security breach through the email account; and

(B) the data collector shall provide notice of the security breach through one or more of the methods specified in subdivision (b)(6) of this section or by clear and conspicuous notice delivered to the consumer online when the consumer is connected to the online account from an Internet protocol address or online location from which the data collector knows the consumer customarily accesses the account.

(e) A data collector that is subject to the privacy, security, and breach notification rules adopted in 45 C.F.R. Part 164 pursuant to the federal Health Insurance Portability and Accountability Act, P.L. 104-191 (1996) is deemed to be in compliance with this subchapter if:

(1) the data collector experiences a security breach that is limited to personally identifiable information specified in 2430(10)(A)(vii); and

(2) the data collector provides notice to affected consumers pursuant to the requirements of the breach notification rule in 45 C.F.R. Part 164, Subpart D.

(f) Any waiver of the provisions of this subchapter is contrary to public policy and is void and unenforceable.

(g) Except as provided in subdivision (3) of this subsection, a financial institution that is subject to the following guidances, and any revisions, additions, or substitutions relating to an interagency guidance, shall be exempt from this section:

(1) The Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision.

(2) Final Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, issued on April 14, 2005, by the National Credit Union Administration.

(3) A financial institution regulated by the Department of Financial Regulation that is subject to subdivision (1) or (2) of this subsection shall notify the Department as soon as possible after it becomes aware of an incident involving unauthorized access to or use of personally identifiable information.

(h) Enforcement.

(1) With respect to all data collectors and other entities subject to this subchapter, other than a person or entity licensed or registered with the Department of Financial Regulation under Title 8 or this title, the Attorney General and State's Attorney shall have sole and full authority to investigate potential violations of this subchapter and to enforce, prosecute, obtain, and impose remedies for a violation of this subchapter or any rules or regulations made pursuant to this chapter as the Attorney General and State's Attorney have under chapter 63 of this title. The Attorney General may refer the matter to the State's Attorney in an appropriate case. The Superior Courts shall have jurisdiction over any enforcement matter brought by the Attorney General or a State's Attorney under this subsection.

(2) With respect to a data collector that is a person or entity licensed or registered with the Department of Financial Regulation under Title 8 or this title, the Department of Financial Regulation shall have the full authority to investigate potential violations of this subchapter and to prosecute, obtain, and impose remedies for a violation of this subchapter or any rules or regulations adopted pursuant to this subchapter, as the Department has under Title 8 or this title or any other applicable law or regulation.

(i) [Repealed.] (Added 2005, No. 162 (Adj. Sess.), § 1, eff. Jan. 1, 2007; amended 2011, No. 109 (Adj. Sess.), § 4, eff. May 8, 2012; 2013, No. 29, §§ 10, 11, eff. May 13, 2013; 2013, No. 199 (Adj. Sess.), § 67; 2015, No. 55, § 8; 2019, No. 89 (Adj. Sess.), § 3.)

Subchapter 3: Social Security Number Protection Act

§ 2440. Social Security number protection

(a) This section shall be known as the Social Security Number Protection Act.

(b) Except as provided in subsection (c) of this section, a business may not do any of the following:

(1) intentionally communicate or otherwise make available to the general public an individual's Social Security number;

(2) intentionally print or imbed an individual's Social Security number on any card required for the individual to access products or services provided by the person or entity;

(3) require an individual to transmit his or her Social Security number over the Internet unless the connection is secure or the Social Security number is encrypted;

(4) require an individual to use his or her Social Security number to access an Internet website, unless a password or unique personal identification number or other authentication device is also required to access the internet website;

(5) print an individual's Social Security number on any materials that are mailed to the individual, unless State or federal law requires the Social Security number to be on the document to be mailed;

(6) sell, lease, lend, trade, rent, or otherwise intentionally disclose an individual's Social Security number to a third party without written consent to the disclosure from the individual, when the party making the disclosure knows or in the exercise of reasonable diligence would have reason to believe that the third party lacks a legitimate purpose for obtaining the individual's Social Security number.

(c) Subsection (b) of this section shall not apply:

(1) When a Social Security number is included in an application or in documents related to an enrollment process, or to establish, amend, or terminate an account, contract, or policy; or to confirm the accuracy of the Social Security number for the purpose of obtaining a credit report pursuant to 15 U.S.C. § 1681(b)(2). A Social Security number that is permitted to be mailed under this section may not be printed, in whole or in part, on a postcard or other mailer not requiring an envelope, or visible on an envelope without the envelope having been opened.

(2) To the collection, use, or release of a Social Security number reasonably necessary for administrative purposes or internal verification.

(3) To the opening of an account or the provision of or payment for a product or service authorized by an individual.

(4) To the collection, use, or release of a Social Security number to investigate or prevent fraud; conduct background checks; conduct social or scientific research; collect a debt; obtain a credit report from or furnish data to a consumer reporting agency pursuant to the Fair Credit Reporting Act, 15 U.S.C. § 1681, et seq.; undertake a permissible purpose enumerated under Gramm Leach Bliley, 12

C.F.R. § 216.13-15; or locate an individual who is missing, is a lost relative, or is due a benefit, such as a pension, insurance, or unclaimed property benefit.

(5) To a business acting pursuant to a court order, warrant, subpoena, or when otherwise required by law, or in response to a facially valid discovery request pursuant to rules applicable to a court or administrative body that has jurisdiction over the disclosing entity.

(6) To a business providing the Social Security number to a federal, State, or local government entity, including a law enforcement agency, the Department of Public Safety, and a court, or their agents or assigns.

(7) To a Social Security number that has been redacted.

(8)(A) To a business that has used, prior to January 1, 2007, an individual's Social Security number in a manner inconsistent with subsection (b) of this section, which may continue using that individual's Social Security number in that manner on or after January 1, 2007, if all of the following conditions are met:

(i) The use of the Social Security number is continuous. If the use is stopped for any reason, subsection (b) of this section shall apply.

(ii) The individual is provided an annual disclosure that informs the individual that he or she has the right to stop the use of his or her Social Security number in a manner prohibited by subsection (b) of this section.

(iii) A written request by an individual to stop the use of his or her Social Security number in a manner prohibited by subsection (b) of this section is implemented within 30 days of the receipt of the request. There shall not be a fee or charge for implementing the request.

(iv) The person or entity does not deny services to an individual because the individual makes a written request pursuant to this subsection.

(B) Nothing in this subdivision (8) is intended to apply to the collection, use, or dissemination of Social Security numbers collected prior to January 1, 2007 and exempted from the provisions of subsection (b) of this section pursuant to subdivisions (1) through (7) or (9) and (10) of this subsection.

(9) To information obtained from a recorded document in the official records of the town clerk or municipality.

(10) To information obtained from a document filed in the official records of the courts.

(d) Except as provided in subsection (e) of this section, the State and any State agency, political subdivision of the State, or an agent or employee of the State, may not do any of the following:

(1) Collect a Social Security number from an individual unless authorized or required by law, State or federal regulation, or grant agreement to do so or unless the collection of the Social Security number or records containing the Social Security number is related to the performance of that agency's duties and responsibilities as prescribed by law.

(2) Fail, when collecting a Social Security number from an individual in a hard copy format, to segregate that number on a separate page from the rest of the record, or as otherwise appropriate, in order that the Social Security number can be more easily redacted pursuant to a valid public records request.

(3) Fail, when collecting a Social Security number from an individual, to provide, at the time of or prior to the actual collection of the Social Security number by that agency, that individual, upon request, with a statement of the purpose or purposes for which the Social Security number is being collected and used.

(4) Use the Social Security number for any purpose other than the purpose set forth in the statement required under subdivision (3) of this subsection.

(5) Intentionally communicate or otherwise make available to the general public a person's Social Security number.

(6) Intentionally print or imbed an individual's Social Security number on any card required for the individual to access government services.

(7) Require an individual to transmit the individual's Social Security number over the Internet, unless the connection is secure or the Social Security number is encrypted.

(8) Require an individual to use the individual's Social Security number to access an Internet website, unless a password or unique personal identification number or other authentication device is also required to access the Internet website.

(9) Print an individual's Social Security number on any materials that are mailed to the individual, unless a State or federal law, regulation, or grant agreement requires that the Social Security number be on the document to be mailed. A Social Security number that is permitted to be mailed under this subdivision may not be printed, in whole or in part, on a postcard or other mailer not requiring an envelope, or visible on an envelope, without the envelope having been opened.

(e) Subsection (d) of this section does not apply to:

(1) Social Security numbers disclosed to another governmental entity or its agents, employees, contractors, grantees, or grantors of a governmental entity if disclosure is necessary for the receiving entity to perform its duties and responsibilities. The receiving governmental entity and its agents, employees, and contractors shall maintain the confidential and exempt status of such numbers. As used in this subsection, "necessary" means reasonably needed to promote the efficient, accurate, or economical conduct of an entity's duties and responsibilities.

(2) Social Security numbers disclosed pursuant to a court order, warrant, or subpoena, or in response to a facially valid discovery request pursuant to rules applicable to a court or administrative body that has jurisdiction over the disclosing entity.

(3) Social Security numbers disclosed for public health purposes pursuant to and in compliance with requirements of the Department of Health under Title 18.

(4) The collection, use, or release of a Social Security number reasonably necessary for administrative purposes or internal verification. Internal verification includes the sharing of information for internal verification between and among governmental entities and their agents, employees, contractors, grantees, and grantors.

(5) Social Security numbers that have been redacted.

(6)(A) A State agency or State political subdivision that has used, prior to January 1, 2007, an individual's Social Security number in a manner inconsistent with subsection (d) of this section, which may continue using that individual's Social Security number in that manner on or after January 1, 2007, if all of the following conditions are met:

(i) The use of the Social Security number is continuous. If the use is stopped for any reason, subsection (d) of this section shall apply.

(ii) The individual is provided an annual disclosure that informs the individual that he or she has the right to stop the use of his or her Social Security number in a manner prohibited by subsection (d) of this section.

(iii) A written request by an individual to stop the use of his or her Social Security number in a manner prohibited by subsection (d) of this section is implemented within 30 days of the receipt of the request. There shall not be a fee or charge for implementing the request.

(iv) The State agency or State political subdivision does not deny services to an individual because the individual makes a written request pursuant to this subdivision.

(B) Nothing in this subdivision (e)(6) is intended to apply to the collection, use, or dissemination of Social Security numbers collected prior to January 1, 2007 and exempted from the provisions of subsection (d) of this section pursuant to subdivisions (1) through (5) or (7) through (11) of this subsection.

(7) Certified copies of vital records issued by the Department of Health and other authorized officials pursuant to 18 V.S.A. part 6.

(8) A recorded document in the official records of the town clerk or municipality.

(9) A document filed in the official records of the courts.

(10) The collection, use, or dissemination of Social Security numbers by law enforcement agencies and the Department of Public Safety in the execution of their duties and responsibilities.

(11) The collection, use, or release of a Social Security number to investigate or prevent fraud; conduct background checks; conduct social or scientific research; collect a debt; obtain a credit report from or furnish data to a consumer reporting agency pursuant to the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq.; undertake a permissible purpose enumerated under Gramm Leach Bliley, 12 C.F.R. § 216.13-15; or locate an individual who is missing, is a lost relative, or is due a benefit, such as a pension, insurance, or unclaimed property benefit.

(f) Any person has the right to request that a town clerk or clerk of court remove from an image or copy of an official record placed on a town's or court's Internet website available to the general public or an Internet website available to the general public to display public records by the town clerk or clerk of court, the person's Social Security number, employer taxpayer identification number, driver's license number, State identification number, passport number, checking account number, savings account number, credit card or debit card number, or personal identification number (PIN) code or passwords contained in that official record. A town clerk or clerk of court is authorized to redact the personal information identified in a request submitted under this section. The request must be made in writing, legibly signed by the requester, and delivered by mail, facsimile, or electronic transmission, or delivered in person to the town clerk or clerk of court. The request must specify the personal information to be redacted, information that identifies the document that contains the personal information and unique information that identifies the location within the document that contains the Social Security number, employer taxpayer identification number, driver's license number, State identification number, passport number, checking account number, savings account number, credit card number, or debit card number, or personal identification number (PIN) code or

passwords to be redacted. The request for redaction shall be considered a public record with access restricted to the town clerk, the clerk of court, their staff, or upon order of the court. The town clerk or clerk of court shall have no duty to inquire beyond the written request to verify the identity of a person requesting redaction and shall have no duty to remove redaction for any reason upon subsequent request by an individual or by order of the court, if impossible to do so. No fee will be charged for the redaction pursuant to such request. Any person who requests a redaction without proper authority to do so shall be guilty of an infraction, punishable by a fine not to exceed $500.00 for each violation.

(g) Enforcement.

(1) With respect to businesses, the State, State agencies, political subdivisions of the State, and agents or employees of the State, a State agency, or a political subdivision of the State, subject to this subchapter, other than a person or entity licensed or registered with the Department of Financial Regulation under Title 8 or this title, the Attorney General and State's Attorney shall have sole and full authority to investigate potential violations of this subchapter, to enforce, prosecute, obtain, and impose remedies for a violation of this subchapter, or any rules made pursuant to this subchapter, and to adopt rules under this subchapter, as the Attorney General and State's Attorney have under chapter 63 of this title. The Attorney General may refer the matter to the State's Attorney in an appropriate case. The Superior Courts shall have jurisdiction over any enforcement matter brought by the Attorney General or a State's Attorney under this subsection.

(2) With respect to a person or entity licensed or registered with the Department of Financial Regulation under Title 8 or this title, the Department shall have full authority to investigate potential violations of this subchapter, and to prosecute, obtain, and impose remedies for a violation of this subchapter or any rules adopted pursuant to this subchapter as the Department has under Title 8 or this title, or any other applicable law or regulation.

(3) With respect to the information provided by the Vermont Department of Public Safety and law enforcement agencies, and any agent or employee thereof, to the Vermont Attorney General or State's Attorney pursuant to subdivision (1) of this subsection, the information provided or made available by the agency or Department to the Attorney General may be designated by the agency or Department as confidential, and shall not be released under the provisions of 1 V.S.A. § 317. (Added 2005, No. 162 (Adj. Sess.), § 1, eff. July 1, 2007.)

Subchapter 3A: Student Privacy

§ 2443. Definitions

As used in this subchapter:

(1) “Covered information” means personal information or material, or information that is linked to personal information or material, in any media or format that is:

(A)(i) not publicly available; or

(ii) made publicly available pursuant to the federal Family Educational and Rights and Privacy Act; and

(B)(i) created by or provided to an operator by a student or the student’s parent or legal guardian in the course of the student’s, parent’s, or legal guardian’s use of the operator’s site, service, or application for PreK-12 school purposes;

(ii) created by or provided to an operator by an employee or agent of a school or school district for PreK-12 school purposes; or

(iii) gathered by an operator through the operation of its site, service, or application for PreK-12 school purposes and personally identifies a student, including information in the student’s education record or electronic mail, first and last name, home address, telephone number, electronic mail address or other information that allows physical or online contact, discipline records, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, Social Security number, biometric information, disability status, socioeconomic information, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, or geolocation information.

(2) “Operator” means, to the extent that an entity is operating in this capacity, the operator of an Internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for PreK-12 school purposes and was designed and marketed for PreK-12 school purposes.

(3) “PreK-12 school purposes” means purposes that are directed by or that customarily take place at the direction of a school, teacher, or school district; aid in the administration of school activities, including instruction in the classroom or at home, administrative activities, and collaboration between students, school personnel, or parents; or are otherwise for the use and benefit of the school.

(4) “School” means:

(A) a public or private preschool, kindergarten, elementary or secondary educational institution, vocational school, special educational agency or institution; and

(B) a person, agency, or institution that maintains school student records from more than one of the entities described in subdivision (6)(A) of this section.

(5) "Targeted advertising" means presenting advertisements to a student where the advertisement is selected based on information obtained or inferred over time from that student's online behavior, usage of applications, or covered information. The term does not include advertising to a student at an online location based upon that student's current visit to that location or in response to that student's request for information or feedback, without the retention of that student's online activities or requests over time for the purpose in whole or in part of targeting subsequent ads. (Added 2019, No. 89 (Adj. Sess.), § 4.)

§ 2443a. Operator prohibitions

(a) An operator shall not knowingly do any of the following with respect to its site, service, or application:

(1) Engage in targeted advertising on the operator's site, service, or application or target advertising on any other site, service, or application if the targeting of the advertising is based on any information, including covered information and persistent unique identifiers, that the operator has acquired because of the use of that operator's site, service, or application for PreK-12 school purposes.

(2) Use information, including a persistent unique identifier, that is created or gathered by the operator's site, service, or application to amass a profile about a student, except in furtherance of PreK-12 school purposes. "Amass a profile" does not include the collection and retention of account information that remains under the control of the student, the student's parent or legal guardian, or the school.

(3) Sell, barter, or rent a student's information, including covered information. This subdivision (3) does not apply to the purchase, merger, or other type of acquisition of an operator by another entity if the operator or successor entity complies with this subchapter regarding previously acquired student information.

(4) Except as otherwise provided in section 2443c of this title, disclose covered information, unless the disclosure is made for one or more of the following purposes and is proportionate to the identifiable information necessary to accomplish the purpose:

(A) to further the PreK-12 school purposes of the site, service, or application, provided:

(i) the recipient of the covered information does not further disclose the information except to allow or improve operability and functionality of the operator's site, service, or application; and

(ii) the covered information is not used for a purpose inconsistent with this subchapter;

(B) to ensure legal and regulatory compliance or take precautions against liability;

(C) to respond to judicial process;

(D) to protect the safety or integrity of users of the site or others or the security of the site, service, or application;

(E) for a school, educational, or employment purpose requested by the student or the student's parent or legal guardian, provided that the information is not used or further disclosed for any other purpose; or

(F) to a third party if the operator contractually prohibits the third party from using any covered information for any purpose other than providing the contracted service to or on behalf of the operator, prohibits the third party from disclosing any covered information provided by the operator to subsequent third parties, and requires the third party to implement and maintain reasonable security procedures and practices.

(b) This section does not prohibit an operator's use of information for maintaining, developing, supporting, improving, or diagnosing the operator's site, service, or application. (Added 2019, No. 89 (Adj. Sess.), § 4.)

§ 2443b. Operator duties

An operator shall:

(1) implement and maintain reasonable security procedures and practices appropriate to the nature of the covered information and designed to protect that covered information from unauthorized access, destruction, use, modification, or disclosure;

(2) delete, within a reasonable time period and to the extent practicable, a student's covered information if the school or school district requests deletion of covered information under the control of the school or school district, unless a student or his or her parent or legal guardian consents to the maintenance of the covered information; and

(3) publicly disclose and provide the school with material information about its collection, use, and disclosure of covered information, including publishing a term of service agreement, privacy policy, or similar document. (Added 2019, No. 89 (Adj. Sess.), § 4.)

§ 2443c. Permissive use or disclosure

An operator may use or disclose covered information of a student under the following circumstances:

(1) if other provisions of federal or State law require the operator to disclose the information and the operator complies with the requirements of federal and State law in protecting and disclosing that information;

(2) for legitimate research purposes as required by State or federal law and subject to the restrictions under applicable State and federal law or as allowed by State or federal law and under the direction of a school, school district, or the State Board of Education if the covered information is not used for advertising or to amass a profile on the student for purposes other than for PreK-12 school purposes; and

(3) disclosure to a State or local educational agency, including schools and school districts, for PreK-12 school purposes as permitted by State or federal law. (Added 2019, No. 89 (Adj. Sess.), § 4.)

§ 2443d. Operator actions that are not prohibited

This subchapter does not prohibit an operator from doing any of the following:

(1) using covered information to improve educational products if that information is not associated with an identified student within the operator's site, service, or application or other sites, services, or applications owned by the operator;

(2) using covered information that is not associated with an identified student to demonstrate the effectiveness of the operator's products or services, including in their marketing;

(3) sharing covered information that is not associated with an identified student for the development and improvement of educational sites, services, or applications;

(4) using recommendation engines to recommend to a student either of the following:

(A) additional content relating to an educational, other learning, or employment opportunity purpose within an online site, service, or application if the recommendation is not determined in whole or in part by payment or other consideration from a third party; or

(B) additional services relating to an educational, other learning, or employment opportunity purpose within an online site, service, or application if the recommendation is not determined in whole or in part by payment or other consideration from a third party; and

(5) responding to a student's request for information or for feedback without the information or response being determined in whole or in part by payment or other consideration from a third party. (Added 2019, No. 89 (Adj. Sess.), § 4.)

§ 2443e. Applicability

This subchapter does not:

(1) limit the authority of a law enforcement agency to obtain any content or information from an operator as authorized by law or under a court order;

(2) limit the ability of an operator to use student data, including covered information, for adaptive learning or customized student learning purposes;

(3) apply to general audience Internet websites, general audience online services, general audience online applications, or general audience mobile applications, even if login credentials created for an operator's site, service, or application may be used to access those general audience sites, services, or applications;

(4) limit service providers from providing Internet connectivity to schools or students and their families;

(5) prohibit an operator of an Internet website, online service, online application, or mobile application from marketing educational products directly to parents if the marketing did not result from the use of covered information obtained by the operator through the provision of services covered under this subchapter;

(6) impose a duty upon a provider of an electronic store, gateway, marketplace, or other means of purchasing or downloading software or applications to review or enforce compliance with this subchapter on those applications or software;

(7) impose a duty upon a provider of an interactive computer service, as defined in 47 U.S.C. § 230, to review or enforce compliance with this subchapter by third-party content providers;

(8) prohibit students from downloading, exporting, transferring, saving, or maintaining their own student-created data or documents; or

(9) supersede the federal Family Educational Rights and Privacy Act or rules adopted pursuant to that Act. (Added 2019, No. 89 (Adj. Sess.), § 4.)

§ 2443f. Enforcement

A person who violates a provision of this chapter commits an unfair and deceptive act in commerce in violation of section 2453 of this title. (Added 2019, No. 89 (Adj. Sess.), § 4.)

Subchapter 4: Document Safe Destruction Act

§ 2445. Safe destruction of documents containing personal information

(a) As used in this section:

(1) “Business” means sole proprietorship, partnership, corporation, association, limited liability company, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the laws of this State, any other state, the United States, or any other country, or the parent, affiliate, or subsidiary of a financial institution, but in no case shall it include the State, a State agency, or any political subdivision of the State. The term includes an entity that destroys records.

(2) “Customer” means an individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business.

(3) “Personal information” means the following information that identifies, relates to, describes, or is capable of being associated with a particular individual: his or her signature, Social Security number, physical characteristics or description, passport number, driver’s license or State identification card number, insurance policy number, bank account number, credit card number, debit card number, or any other financial information.

(4)(A) “Record” means any material, regardless of the physical form, on which information is recorded or preserved by any means, including in written or spoken words, graphically depicted, printed, or electromagnetically transmitted.

(B) “Record” does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address, or telephone number.

(b) A business shall take all reasonable steps to destroy or arrange for the destruction of a customer’s records within its custody or control containing personal information that is no longer to be retained by the business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or indecipherable through any means for the purpose of:

(1) ensuring the security and confidentiality of customer personal information;

(2) protecting against any anticipated threats or hazards to the security or integrity of customer personal information; and

(3) protecting against unauthorized access to or use of customer personal information that could result in substantial harm or inconvenience to any customer.

(c) An entity that is in the business of disposing of personal financial information that conducts business in Vermont or disposes of personal information of residents of Vermont must take all reasonable measures to dispose of records containing personal information by implementing and monitoring compliance with policies and procedures that protect against unauthorized access to or use of personal information during or after the collection and transportation and disposing of such information.

(d) This section does not apply to any of the following:

(1) any bank, credit union, or financial institution as defined under the federal Gramm Leach Bliley law that is subject to the regulation of the Office of the Comptroller of the Currency, the Federal Reserve, the National Credit Union Administration, the Securities and Exchange Commission, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision of the U.S. Department of the Treasury, or the Department of Financial Regulation and is subject to the privacy and security provisions of the Gramm Leach Bliley Act, 15 U.S.C. § 6801 et seq.;

(2) any health insurer or health care facility that is subject to and in compliance with the standards for privacy of individually identifiable health information and the security standards for the protection of electronic health information of the Health Insurance Portability and Accountability Act of 1996; or

(3) any consumer reporting agency that is subject to and in compliance with the Federal Credit Reporting Act, 15 U.S.C. § 1681 et seq., as amended.

(e) Enforcement.

(1) With respect to all businesses subject to this section, other than a person or entity licensed or registered with the Department of Financial Regulation under Title 8 or this title, the Attorney General and State's Attorney shall have sole and full authority to investigate potential violations of this section, and to prosecute, obtain, and impose remedies for a violation of this section, or any rules adopted pursuant to this section, and to adopt rules under this chapter, as the Attorney General and State's Attorney have under chapter 63 of this title. The Superior Courts shall have jurisdiction over any enforcement matter brought by the Attorney General or a State's Attorney under this subsection.

(2) With respect to a person or entity licensed or registered with the Department of Financial Regulation under Title 8 or this title to do business in this State, the Department of Financial Regulation shall have full authority to investigate potential violations of this chapter, and to prosecute, obtain, and impose remedies for a violation of this chapter, or any rules or regulations made pursuant to this chapter, as the Department has under Title 8 and this title, or any other applicable law or regulation. (Added 2005, No. 162 (Adj. Sess.), § 1, eff. Jan. 1, 2007.)

Subchapter 5: Data Brokers

§ 2446. Annual registration

(a) Annually, on or before January 31 following a year in which a person meets the definition of data broker as provided in section 2430 of this title, a data broker shall:

(1) register with the Secretary of State;

(2) pay a registration fee of $100.00; and

(3) provide the following information:

(A) the name and primary physical, e-mail, and Internet addresses of the data broker;

(B) if the data broker permits a consumer to opt out of the data broker's collection of brokered personal information, opt out of its databases, or opt out of certain sales of data:

(i) the method for requesting an opt-out;

(ii) if the opt-out applies to only certain activities or sales, which ones; and

(iii) whether the data broker permits a consumer to authorize a third party to perform the opt-out on the consumer's behalf;

(C) a statement specifying the data collection, databases, or sales activities from which a consumer may not opt out;

(D) a statement whether the data broker implements a purchaser credentialing process;

(E) the number of data broker security breaches that the data broker has experienced during the prior year, and if known, the total number of consumers affected by the breaches;

(F) where the data broker has actual knowledge that it possesses the brokered personal information of minors, a separate statement detailing the data collection practices, databases, sales activities, and opt-out policies that are applicable to the brokered personal information of minors; and

(G) any additional information or explanation the data broker chooses to provide concerning its data collection practices.

(b) A data broker that fails to register pursuant to subsection (a) of this section is liable to the State for:

(1) a civil penalty of $50.00 for each day, not to exceed a total of $10,000.00 for each year, it fails to register pursuant to this section;

(2) an amount equal to the fees due under this section during the period it failed to register pursuant to this section; and

(3) other penalties imposed by law.

(c) The Attorney General may maintain an action in the Civil Division of the Superior Court to collect the penalties imposed in this section and to seek appropriate injunctive relief. (Added 2017, No. 171 (Adj. Sess.), § 2, eff. Jan. 1, 2019.)

§ 2447. Data broker duty to protect information; standards; technical requirements

(a) Duty to protect personally identifiable information.

(1) A data broker shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to:

(A) the size, scope, and type of business of the data broker obligated to safeguard the personally identifiable information under such comprehensive information security program;

(B) the amount of resources available to the data broker;

(C) the amount of stored data; and

(D) the need for security and confidentiality of personally identifiable information.

(2) A data broker subject to this subsection shall adopt safeguards in the comprehensive security program that are consistent with the safeguards for protection of personally identifiable information and information of a similar character set forth in other State rules or federal regulations applicable to the data broker.

(b) Information security program; minimum features. A comprehensive information security program shall at minimum have the following features:

(1) designation of one or more employees to maintain the program;

(2) identification and assessment of reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of any electronic, paper, or other records containing personally identifiable information, and a process for evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including:

(A) ongoing employee training, including training for temporary and contract employees;

(B) employee compliance with policies and procedures; and

(C) means for detecting and preventing security system failures;

(3) security policies for employees relating to the storage, access, and transportation of records containing personally identifiable information outside business premises;

(4) disciplinary measures for violations of the comprehensive information security program rules;

(5) measures that prevent terminated employees from accessing records containing personally identifiable information;

(6) supervision of service providers, by:

(A) taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect personally identifiable information consistent with applicable law; and

(B) requiring third-party service providers by contract to implement and maintain appropriate security measures for personally identifiable information;

(7) reasonable restrictions upon physical access to records containing personally identifiable information and storage of the records and data in locked facilities, storage areas, or containers;

(8)(A) regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personally identifiable information; and

(B) upgrading information safeguards as necessary to limit risks;

(9) regular review of the scope of the security measures:

(A) at least annually; or

(B) whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personally identifiable information; and

(10)(A) documentation of responsive actions taken in connection with any incident involving a breach of security; and

(B) mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personally identifiable information.

(c) Information security program; computer system security requirements. A comprehensive information security program required by this section shall at minimum, and to the extent technically feasible, have the following elements:

(1) secure user authentication protocols, as follows:

(A) an authentication protocol that has the following features:

(i) control of user IDs and other identifiers;

(ii) a reasonably secure method of assigning and selecting passwords or use of unique identifier technologies, such as biometrics or token devices;

(iii) control of data security passwords to ensure that such passwords are kept in a location and format that do not compromise the security of the data they protect;

(iv) restricting access to only active users and active user accounts; and

(v) blocking access to user identification after multiple unsuccessful attempts to gain access; or

(B) an authentication protocol that provides a higher level of security than the features specified in subdivision (A) of this subdivision (c)(1);

(2) secure access control measures that:

(A) restrict access to records and files containing personally identifiable information to those who need such information to perform their job duties; and

(B) assign to each person with computer access unique identifications plus passwords, which are not vendor-supplied default passwords, that are reasonably designed to maintain the integrity of the security of the access controls or a protocol that provides a higher degree of security;

(3) encryption of all transmitted records and files containing personally identifiable information that will travel across public networks and encryption of all data containing personally identifiable information to be transmitted wirelessly or a protocol that provides a higher degree of security;

(4) reasonable monitoring of systems for unauthorized use of or access to personally identifiable information;

(5) encryption of all personally identifiable information stored on laptops or other portable devices or a protocol that provides a higher degree of security;

(6) for files containing personally identifiable information on a system that is connected to the Internet, reasonably up-to-date firewall protection and operating system security patches that are reasonably designed to maintain the integrity of the personally identifiable information or a protocol that provides a higher degree of security;

(7) reasonably up-to-date versions of system security agent software that must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions and is set to receive the most current security updates on a regular basis or a protocol that provides a higher degree of security; and

(8) education and training of employees on the proper use of the computer security system and the importance of personally identifiable information security.

(d) Enforcement.

(1) A person who violates a provision of this section commits an unfair and deceptive act in commerce in violation of section 2453 of this title.

(2) The Attorney General has the same authority to adopt rules to implement the provisions of this chapter and to conduct civil investigations, enter into assurances of discontinuance, and bring civil actions as provided under chapter 63, subchapter 1 of this title. (Added 2017, No. 171 (Adj. Sess.), § 2, eff. Jan. 1, 2019.)

ประวัติผู้เขียน

ชื่อ – นามสกุล นิจญาณอมร อินสุข

ประวัติการศึกษา

- ปริญญาตรี หลักสูตรนิติศาสตรบัณฑิต มหาวิทยาลัยหอการค้าไทย

ประสบการณ์ทำงาน

- นิติกร กรมบังคับคดี กระทรวงยุติธรรม
- Assistant Section Manager บริษัท บริหารสินทรัพย์ เจ จำกัด