ปัญหาทางกฎหมายของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่เกี่ยวข้องกับสถาบันการเงิน[1]

กฤษณะ นาวารัตน์[2]

จากการศึกษาปัญหาทางกฎหมายของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่เกี่ยวข้องกับสถาบันการเงิน โดยมีวัตถุประสงค์เพื่อศึกษา ประวัติความเป็นมา ความหมาย แนวคิดและทฤษฎีเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล โดยวิเคราะห์ให้ทราบถึงปัญหาทางกฎหมายของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่เกี่ยวข้องกับสถาบันการเงิน เนื่องจากสังคมสมัยใหม่เป็นสังคมแห่งการติดต่อสื่อสาร ข้อมูลส่วนบุคคลจึงมีความสำคัญต่อการดำเนินกิจกรรมต่างๆ ไม่ว่าจะเป็นในภาครัฐ ภาคเอกชน หรือในสถาบันการเงิน ต่างก็มีความจำเป็นที่จะต้องมีข้อมูลส่วนบุคคลไว้ในครอบครอง ซึ่งข้อมูลส่วนบุคคลจำนวนมากที่มีการครอบครองหรือมีการแลกเปลี่ยนหรือแย่งชิงแข่งขันกันครอบครองนี้ ทำให้เกิดปัญหามีการนำข้อมูลส่วนบุคคลของเจ้าของข้อมูลไปใช้โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล ซึ่งทำให้เจ้าของข้อมูลอาจได้รับความเสียหาย หรือการนำข้อมูลข่าวสารไปใช้ประโยชน์ในทางพาณิชย์โดยปราศจากการได้รับอนุญาตหรือยินยอมจากผู้เป็นเจ้าของข้อมูล ทำให้เกิดความเสียหายหรือความเดือดร้อนรำคาญกับเจ้าของข้อมูล ซึ่งปัญหาที่เกิดขึ้นในปัจจุบันคือในกรณีที่ข้อมูลส่วนบุคคลของผู้ใช้บริการบางประเภท เกิดการรั่วไหลสู่บุคคลภายนอก ไม่ว่าจะเกิดจากระบบความปลอดภัยที่ไม่ได้มาตรฐานของธนาคารหรือสถาบันการเงินเองเป็นผู้นำมาเปิดเผย ปัญหาเหล่านี้ย่อมก่อให้เกิดความเสียหายต่อผู้เป็นเจ้าของข้อมูลส่วนบุคคลนั้น อีกทั้งยังสร้างความเดือดร้อนรำคาญ และอาจทำให้เจ้าของข้อมูลเสื่อมเสียชื่อเสียง หรือนำไปสู่อาชญากรรมได้ ทั้งนี้ เกี่ยวกับปัญหาทางกฎหมายของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่เกี่ยวข้องกับสถาบันการเงิน ทำให้เกิดปัญหาหลายกรณี ดังนี้

ปัญหาการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศตามมาตรา 28 (Cross-border data transfer) เนื่องจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดว่าประเทศปลายทางที่ได้รับข้อมูลส่วนบุคคลจะต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ

---

[1] บทความนี้เรียบเรียงจากการศึกษาอิสระ เรื่อง ปัญหาการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่เกี่ยวข้องกับสถาบันการเงินโดยมีอาจารย์ที่ปรึกษา คือ ผู้ช่วยศาสตราจารย์ ดร.ดนพร จิตต์จุงเกียรติ และคณะกรรมการสอบ คือ ผู้ช่วยศาสตราจารย์ ดร.มณทิชา ภักดีคง และรองศาสตราจารย์ ดร.พันธ์เทพ วิทิตอนันต์

[2] ชื่อนักศึกษาปริญญาโท หลักสูตรนิติศาสตรมหาบัณฑิต (ส่วนกลาง) คณะนิติศาสตร์ มหาวิทยาลัยรามคำแหง

ตามหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด แต่เนื่องจากในปัจจุบันยังไม่มีประกาศของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่กำหนดหลักเกณฑ์ในการพิจารณามาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอของประเทศปลายทางที่รับข้อมูลส่วนบุคคล จึงมีปัญหาว่าสถาบันการเงินที่มีความจำเป็นต้องส่งหรือโอนข้อมูลส่วนบุคคลของลูกค้าไปยังต่างประเทศ ไม่อาจทราบได้ว่าประเทศปลายทางนั้น ถือว่ามีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอหรือไม่ เพื่อให้เป็นไปตามหลักการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ในส่วนของหลักข้อจำกัดในการส่งหรือโอนข้อมูลส่วนบุคคลให้แก่บุคคลอื่นข้ามพรมแดนในการส่งข้อมูลไปต่างประเทศ และตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศอื่นๆ

ปัญหาประการที่สอง ปัญหาการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลตามมาตรา 40 (2) (Personal Data Breach Notification) เนื่องจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 40 (2) ได้ระบุหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสม และแจ้งผู้ควบคุมข้อมูลส่วนบุคคลทราบเมื่อมีเหตุการละเมิดเกิดขึ้น แต่บทบัญญัติดังกล่าวไม่ได้กำหนดระยะเวลาให้ผู้ประมวลผลข้อมูลส่วนบุคคลแจ้งแก่ผู้ควบคุมข้อมูลส่วนบุคคล และรายละเอียดหรือหัวข้อหรือกรอบประเด็นในการแจ้งข้อมูลเหตุละเมิด หากไม่มีการกำหนดระยะเวลาพร้อมทั้งรายละเอียดหรือหัวข้อหรือกรอบประเด็นในการแจ้งข้อมูลเหตุละเมิด ให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบ อาจมีผลทำให้ผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถทราบเหตุละเมิดได้โดยเร็ว และไม่อาจทราบรายละเอียดการละเมิดที่เพียงพอ เพราะไม่มีการกำหนดรายละเอียดหรือหัวข้อหรือกรอบประเด็นในการแจ้งข้อมูลเหตุละเมิดที่เพียงพอให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบ ดังนั้น หากไม่มีการกำหนดระยะเวลาพร้อมทั้งรายละเอียดหรือหัวข้อหรือกรอบประเด็นในการแจ้งข้อมูลเหตุละเมิด ให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบ ย่อมมีผลทำให้เจ้าของข้อมูลส่วนบุคคลไม่ได้รับการคุ้มครองความเป็นส่วนตัวตามกฎหมายอย่างครบถ้วน

ปัญหาประการที่สาม ปัญหาเกี่ยวกับหน้าที่ในการประเมินความเสี่ยงผลกระทบต่อข้อมูลส่วนบุคคลตามมาตรา 42 (Data Protection Impact Assessment หรือ DPIA) เนื่องจากการประมวลผลข้อมูลส่วนบุคคลของสถาบันการเงินอาจก่อให้เกิดความเสี่ยงที่กระทบต่อสิทธิและเสรีภาพของบุคคล สถาบันการเงินจึงควรมีการประเมินผลกระทบและควบคุมความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment : DPIA) ในกรณีที่การประมวลผลข้อมูลมีความเสี่ยงที่จะเกิดผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลด้วย แต่ปรากฏว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 42 ได้กำหนดหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในประการต่างๆไว้ แต่บทบัญญัติดังกล่าวไม่ได้

กำหนดหน้าที่ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องดำเนินการประเมินความเสี่ยงผลกระทบต่อข้อมูลส่วนบุคคล (Data Protection Impact Assessment หรือ DPIA) ซึ่งตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation) (GDPR) ได้กำหนดหน้าที่ให้ผู้ควบคุมข้อมูลต้องดำเนินการประเมินความเสี่ยงผลกระทบ (ซึ่งรวมถึงการเก็บรวบรวม ใช้เปิดเผยข้อมูลวนบุคคล) หากเข้าเงื่อนไขว่าข้อมูลส่วนบุคคลใช้เทคโนโลยีใหม่และเมื่อพิจารณาถึงลักษณะ ขอบเขตวัตถุประสงค์ของการประมวลผลข้อมูลแล้วอาจส่งผลให้เกิดความเสี่ยงสูงต่อสิทธิและเสริภาพของบุคคลมาตรา 39 ของ GDPR ดังนั้น เพื่อป้องกันความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล และมีมาตรการในการรักษาความมั่นคงและปลอดภัยที่เหมาะสมกับความเสี่ยง และเพื่อเป็นการปฏิบัติให้สอดคล้องกับ GDPR อีกทั้งยังเป็นการสร้างความเชื่อมั่นและความไว้วางใจให้กับเจ้าของข้อมูลส่วนบุคคลและส่วนรวมมากขึ้น ช่วยลดความเสี่ยงในการประมวลผลข้อมูลส่วนบุคคลที่ไม่เหมาะสม ลดความเสี่ยงที่จะเกิดผลกระทบต่อชื่อเสียงขององค์กร ซึ่งจะเป็นผลดีแก่องค์กรเอง และเพื่อเป็นการคุ้มครองเจ้าของข้อมูลตามสิทธิที่พึงควรได้รับและเป็นไปตามหลักการสากล พระราชบัญญัติคุ้มครองข้อมูลฯ จึงควรเพิ่มเติมหน้าที่ดังกล่าวของเจ้าหน้าที่คุ้มครองข้อมูลให้มีหน้าที่ในการประเมินความเสี่ยงผลกระทบต่อข้อมูลส่วนบุคคลด้วย

ปัญหาประการสุดท้าย ปัญหาเกี่ยวกับสิทธิของเจ้าของข้อมูลที่จะไม่อยู่ภายใต้การตัดสินใจโดยอัตโนมัติ (Right not to be subject to automated individual decision-making, including profiling) เนื่องจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ไม่ได้มีการบัญญัติสิทธิของเจ้าของข้อมูลในการคัดค้านหรือปฏิเสธการใช้เทคโนโลยีตัดสินใจโดยอัตโนมัติ หรือสิทธิที่จะไม่อยู่ภายใต้การตัดสินใจโดยอัตโนมัติ ซึ่งมีผลเสียและกระทบต่อสิทธิของเจ้าของข้อมูลส่วนบุคคลซึ่งเป็นคู่สัญญา อันอาจมีผลทำให้เกิดการประมวลผลและตัดสินใจส่งผลกระทบในแง่ต่าง ๆ ต่อเจ้าของข้อมูลโดยทั้งหมดเกิดจากระบบหรือโปรแกรมที่ทำงานโดยอัตโนมัติไม่ผ่านการตัดสินใจหรือแทรกแซงจากมนุษย์ เช่น การนำข้อมูลส่วนบุคคลที่ได้มาจากหลายแหล่งเชื่อมโยงกันและสร้างเป็นประวัติ (Profiling) ของบุคคลหนึ่งซึ่งครอบคลุมข้อมูลหลายมิติ การใช้ปัญญาประดิษฐ์ (Artificial Intelligence หรือ AI) หรือการใช้โปรแกรมอัตโนมัติมาทำการแทนเจ้าหน้าที่ซึ่งเป็นมนุษย์ในการตัดสินใจที่เกี่ยวเนื่องกับนิติกรรมสัญญาต่าง ในชีวิตประจำวันของบุคคล เช่น การวิเคราะห์ข้อมูลและตัดสินใจอนุมัติการเข้าทำสัญญาการค้าหรือใช้บริการเรื่องต่างๆ การอนุมัติการกู้เงิน การอนุมัติในการสมัครทำสัญญาหรือใช้บริการต่าง ๆ หรือการทำสัญญาแบบสมาร์ท (Smart contract) ลักษณะเช่นนี้อาจส่งผลกระทบในแง่สิทธิเสรีภาพหากบุคคลไม่สามารถโต้แย้งหรือขอให้มีมนุษย์เข้ามา

แทรกแซงระบบอัตโนมัติดังกล่าว ซึ่งตาม GDPR ได้กำหนดสิทธิโดยเฉพาะสำหรับเจ้าของข้อมูลส่วนบุคคลที่กฎหมายไทยไม่ได้นำมากำหนดไว้ คือ สิทธิที่จะไม่อยู่ภายใต้การตัดสินใจโดยอัตโนมัติ (Right not to be subject to automated individual decision-making, including profiling) ตามมาตรา 22 โดยมีหลักว่า เจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะไม่อยู่ภายใต้การตัดสินใจซึ่งเกิดขึ้นเฉพาะเพียงบนพื้นฐานการประมวลผลข้อมูลส่วนบุคคลโดยอัตโนมัติ ดังนั้น เมื่อพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ในส่วนหมวด 3 ว่าด้วยสิทธิของเจ้าของข้อมูลส่วนบุคคล ไม่ได้กำหนดรับรองสิทธิในทำนองเดียวกับมาตรา 22 ของ GDPR จึงเห็นควรที่พระราชบัญญัติคุ้มครองฯ จะได้บัญญัติสิทธิดังกล่าวไว้ด้วย เพื่อเป็นการคุ้มครองสิทธิของเจ้าของข้อมูลให้เป็นไปตามหลักสากล

จากการศึกษาปัญหาของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่เกี่ยวข้องกับสถาบันการเงิน ผู้ศึกษาจึงขอเสนอแนะแนวทางที่นำไปสู่การปรับปรุงแก้ไขกฎหมายดังกล่าว ดังนี้

1. ปัญหาการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศตามมาตรา 28 (Cross-border data transfer) ผู้ศึกษาขอเสนอกรอบแนวทางในการพิจารณามาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอสำหรับการประกาศของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่กำหนดหลักเกณฑ์ดังกล่าว ดังนี้

(1) ประเทศปลายทางต้องมีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ซึ่งอาจเป็นกฎหมายเป็นการทั่วไปหรือเป็นรายภาคส่วน โดยสะท้อนหลักนิติธรรม หลักการคุ้มครองสิทธิมนุษยชนและสิทธิขั้นพื้นฐาน ตลอดจนการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์กรระหว่างประเทศและการใช้บังคับได้ของสิทธิของเจ้าของข้อมูล

(2) ประเทศปลายทางต้องมีองค์กรหรือหน่วยงานกำกับดูแลที่เป็นอิสระที่มีความรับผิดชอบในการบังคับใช้ให้เป็นไปตามกฎเกณฑ์ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของประเทศนั้น รวมถึงมีอำนาจในการช่วยเหลือหรือให้คำปรึกษาแก่เจ้าของข้อมูลตลอดจนทำหน้าที่ร่วมมือกับ หน่วยงานกำกับดูแลของประเทศอื่น ๆ

(3) ประเทศปลายทางต้องมีพันธะกรณีระหว่างประเทศในการเข้าผูกพันทางกฎหมายหรือการเข้าร่วมในระบบพหุพาคีหรือภูมิภาคในเรื่องการคุ้มครองข้อมูลส่วนบุคคล

และเห็นควรแก้ไขเพิ่มเติมพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 28 ในวรรคท้าย ดังนี้

มาตรา 28 ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ทั้งนี้ ต้องเป็นไปตามหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลตามที่คณะกรรมการประกาศกำหนดตามมาตรา 16 (5) เว้นแต่

……

ในกรณีที่มีปัญหาเกี่ยวกับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคล ให้เสนอต่อคณะกรรมการเป็นผู้วินิจฉัย ทั้งนี้ คำวินิจฉัยของคณะกรรมการอาจขอให้ทบทวนได้เมื่อมีหลักฐานใหม่ทำให้เชื่อได้ว่าประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลมีการพัฒนาจนมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ในกรณีที่ผู้ควบคุมข้อมมูลส่วนบบุคคลมีความจำเป็นต้องโอนข้อมูลส่วนบุคคลไปยังประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลซึ่งยังไม่มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอหรือประกาศของคณะกรรมการรับรอง ผู้ควบคุมข้อมูลส่วนบุคคลย่อมมีหน้าที่ต้องรับผิดชอบข้อมูลส่วนบุคคลที่มีอยู่ในความครอบครองและการควบคุมดูแล รวมไปถึงข้อมูลที่ถูกถ่ายโอนไปให้บุคคลที่สามเพื่อการประมวลผลด้วย โดยมีคณะกรรมการทำหน้าที่ตรวจสอบวิธีการที่องค์กรใช้ในการจัดการกับข้อมูลส่วนบุคคลได้

2. ปัญหาการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลตามมาตรา 40(2) (Personal Data Breach Notification) เดิมมาตรา 40 (2) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติว่า “ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(2) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น ”

ผู้ศึกษาขอเสนอแนะให้แก้ไขเพิ่มเติมมาตรา 40 (2) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ดังนี้

“ จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ ซึ่งอย่างน้อยต้องมีรายละเอียดหรือหัวข้อหรือกรอบ

ประเด็นในการแจ้งดังกล่าวและระบุสาระสำคัญเท่าที่จะสามารถกระทำได้ เช่น ข้อมูลโดยสังเขปเท่าที่จะสามารถระบุได้เกี่ยวกับลักษณะและประเภทของการละเมิดข้อมูลส่วนบุคคล, ข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้นจากเหตุการละเมิดข้อมูลส่วนบุคคล ”

3. ปัญหาเกี่ยวกับหน้าที่ในการประเมินความเสี่ยงผลกระทบต่อข้อมูลส่วนบุคคลตามมาตรา 42 (Data Protection Impact Assessment หรือ DPIA)

เดิมมาตรา 42 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 บัญญัติว่า “เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(1) ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้

(2) ตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามพระราชบัญญัตินี้

(3) ประสานงานและให้ความร่วมมือกับสำนักงานในกรณีที่มีปัญหาเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในการปฏิบัติตามพระราชบัญญัตินี้

(4) รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้

ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลต้องสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล……

ผู้ศึกษาขอเสนอแนะให้แก้ไขเพิ่มเติมมาตรา 40 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ดังนี้ แก้ไขเป็น มาตรา 42 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีหน้าที่ ดังนี้

(5) ให้คำปรึกษาในด้านที่เกี่ยวข้องกับการประเมินสถานการณ์ ผลกระทบการคุ้มครองข้อมูลและการตรวจตราการ ปฏิบัติหน้าที่ตามมาตรา 29/1 เมื่อถูกร้องขอผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลต้องสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล……

และเห็นควรบัญญัติเพิ่มเติมมาตรา เกี่ยวกับการให้คำปรึกษาในด้านที่เกี่ยวข้องกับการประเมินสถานการณ์ ผลกระทบการคุ้มครองข้อมูลและการตรวจตราการปฏิบัติหน้าที่ตามมาตรา 42 เมื่อถูกร้องขอ โดยบัญญัติมาตรา 29/1 เพิ่มเติม ดังนี้

มาตรา 29/1 การประเมินสถานการณ์ผลกระทบการคุ้มครองข้อมูล

1. เมื่อชนิดของการประมวลผลข้อมูลที่ถูกระบุนั้นใช้เทคโนโลยีใหม่ และเมื่อพิจารณาโดยละเอียดร่วมกับลักษณะ ขอบเขต บริบท และวัตถุประสงค์ของการประมวลผลแล้วมีแนวโน้มที่จะส่งผลให้เกิดความเสี่ยงในระดับสูงต่อสิทธิเสรีภาพของบุคคลธรรมดา ผู้ควบคุมจะต้องดำเนินการประเมินสถานการณ์ผลกระทบต่อการคุ้มครองข้อมูลส่วนบุคคลของการประมวลผลที่คาดไว้ก่อนดำเนินการประมวลผล

2. ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องขอคำแนะนำจากเจ้าหน้าที่คุ้มครองข้อมูลที่ ถูกกำหนดไว้เมื่อดำเนินการประเมินสถานการณ์ผลกระทบการคุ้มครองข้อมูล

3. ผู้ควบคุมจะต้องขอความเห็นจากผู้ถูกประมวลผลข้อมูล หรือผู้แทนถึงการประมวลผลที่ต้องการให้เกิดขึ้นเมื่อเหมาะสม โดยต้องไม่ส่งผลเสียต่อการคุ้มครองประโยชน์ทางการค้าหรือสาธารณะหรือ ความปลอดภัยในปฏิบัติการประมวลผล

4. ปัญหาเกี่ยวกับสิทธิของเจ้าของข้อมูลที่จะไม่อยู่ภายใต้การตัดสินใจโดยอัตโนมัติ (Right not to be subject to automated individual decision-making, including profiling)

โดยผู้ศึกษาเห็นควรที่จะได้บัญญัติสิทธิดังกล่าวเพิ่มเติมไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หมวดที่ 3 โดยบัญญัติมาตราใหม่ ดังนี้ มาตรา 34/1 การสร้างการวินิจฉัยบุคคลอัตโนมัติ ผู้ถูกประมวลผลข้อมูลจะต้องมีสิทธิที่จะไม่อยู่ใต้อำนาจของการวินิจฉัยอันมาจากกระบวนการประมวลผลอัตโนมัติเท่านั้น อันรวมถึงการทำโปรไฟล์ที่ก่อให้เกิดผลทางกฎหมายซึ่งเกี่ยวข้องกับผู้ถูกประมวลผลข้อมูลหรือมีผลกระทบอย่างมีนัยสำคัญเช่นเดียวกันกับผู้ถูกประมวลผลข้อมูล

เอกสารอ้างอิง

หนังสือ

คนาธิป ทองรวีวงศ์ **คำอธิบายหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล**
พิมพ์ครั้งที่ 3 แก้ไขเพิ่มเติม , (กรุงเทพ สำนักพิมพ์ นิติธรรม พ.ศ. 2565)

นคร เสรีรักษ์ ณรงค์ใจหาญ ประสิทธิ์ ปิวาวัฒนพานิช ศุภเกียรติ ศุภศักดิ์ศึกษากร
นิชานันท์ นันทศิริศรณ์ **แปลและเรียบเรียง GDPR ฉบับภาษาไทย** พิมพ์ครั้งแรก ,
(สำนักพิมพ์บริษัท พี.เพรส จำกัด)

นคร เสรีรักษ์, ความเป็นส่วนตัว : **ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการ**
คุ้มครองข้อมูลส่วนบุคคลในประเทศไทย, (กรุงเทพมหานคร : สำนักพิมพ์
พีเพรส, 2557)

ปรีดี เกษมทรัพย์, **นิติปรัชญา**, พิมพ์ครั้งที่ 5 (กรุงเทพมหานคร : โครงการประกอบตารา
และเอกสารคำสอน คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2543)
,อ้างถึงใน นคร เสรีรักษ์, ความเป็นส่วนตัว : ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการ
คุ้มครองข้อมูล ส่วนบุคคลในประเทศไทย (กรุงเทพมหานคร : สำนักพิมพ์พีเพรส, 2557)

สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์, **แนวทางการจัดทำ**
กฎหมายคุ้มครองข้อมูลส่วนบุคคล, พิมพ์ครั้งที่ 2 (กรุงเทพมหานคร : ศูนย์เทคโนโลยี
อิเล็กทรอนิกส์ และคอมพิวเตอร์แห่งชาติ, 2547)

วิทยานิพนธ์

กิตติพงศ์ กมลธรรมวงศ์, **“การคุ้มครองข้อมูลข่าวสารส่วนบุคคลในระบบกฎหมายไทย**
: ปัญหาและแนวทางแก้ไข,” (วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัย ธรรมศาสตร์,
2549)

ชื่นอารี มาลีศรีประเสริฐ, **“การคุ้มครองสิทธิส่วนตัวกับสื่อสารสนเทศ,”** (วิทยานิพนธ์
มหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2539), อ้างถึงในนคร เสรีรักษ์, ความ เป็น
ส่วนตัว : ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศ
ไทย, (กรุงเทพมหานคร : สำนักพิมพ์พีเพรส , 2557)

ศิริกุล ภู่พันธ์, “**ข้อความคิดว่าด้วยข้อมูลข่าวสารส่วนบุคคล**,” (วิทยานิพนธ์
มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2548),

วรพจน์ วิศรุตพิชญ์, **“สิทธิเสรีภาพตามรัฐธรรมนูญ (ศึกษารูปแบบการจำกัดสิทธิและ**

เสรีภาพที่รัฐธรรมนูญให้ไว้อย่างเหมาะสม)", วารสารกฎหมายจุฬา, เล่มที่ 3, ปีที่ 17, น.7. อ้างถึงในศิริกุล ภู่พันธ์, "ข้อความคิดว่าด้วยข้อมูลข่าวสารส่วนบุคคล," (วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2548)

วรรณรัชชา ทรัพย์รดาพัดชา, **ปัญหาการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลระหว่างประเทศกับ สหภาพยุโรป : ศึกษาผลกระทบของคดีคำพิพากษาศาลยุติธรรม แห่งสหภาพยุโรปในคดี C-362/14 ต่อโครงการเซฟฮาร์เบอร์ (Safe Harbour)** (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต สาขากฎหมายมหาชน คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ ปีการศึกษา 2558)

บทความในวารสาร

วิริยะ รามสมภพ **ความสัมพันธ์เชิงวิเคราะห์ของร่างพระราชบัญญัติคุ้มครองข้อมูลข่าวสารส่วนบุคคล พ.ศ. ..... กับ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540**, เอกสารวิชาการของ สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ , น.5 – 7

นนทวัชร์ นวตระกูลพิสุทธิ์, **"สิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล กับมาตรการคุ้มครองตาม ร่างพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...,"** วารสารนิติศาสตร์, ปีที่ 43 ฉบับที่ 4, น.740 (ธันวาคม 2557).

เอกสารอื่น ๆ

ภาพรวมหลักเกณฑ์กำกับดุแลเงินกองทุนธนาคารพาณิชย์ chapter 2 ความรู้พื้นฐานเกี่ยวกับหลักเกณฑ์ของ Basel Capital Accord สืบค้นเมื่อวันที่ 20 เมษายน 2566 จาก https://www.bot.or.th/Thai/FinancialInstitutions/Highlights/Basel3_VDO/printA1.pdf

ปฏิวัติ อุ่นเรือน, "**ปัญหาการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลระหว่างประเทศ**," (สารนิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2547), น. 7.

สมศักดิ์ นวตระกูลพิสุทธิ์, **"กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดา,"** รายงานการวิจัยโครงการจัดทำความเห็นทางวิชาการเพื่อจัดทำรายงานเกี่ยวกับหลักเกณฑ์และแนวทางการพิจารณาและดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และจัดทำคู่มือ ปฏิบัติงานเกี่ยวกับข้อมูลส่วนบุคคลภาครัฐตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 (กรุงเทพมหานคร : สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์, 2547) น.97.

เอกณัท สุชาติพนัธุ์ ,**การคุ้มครองข้อมูลส่วนบคุคล กรณีศึกษาการโอนข้อมูลข้ามพรมแดนธรุกิจธนาคาร** (การศึกษาค้นคว้าอิสระเป็นส่วนหนึ่งของการศึกษาตามหลักสตูรนิติศาสตรมหาบัณฑิต มหาวิทยาลัยหอการค้าไทย ปีการศึกษา 2561)

กฎหมาย

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

เอกสารภาษาอังกฤษ

Article 12 UDHR. “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.” **คำแปลปฏิญญาสากลว่าด้วยสิทธิมนุษยชน** สืบค้นจาก www.mfa.go.th/humanrights/images/stories/book.pdf. เมื่อวันที่ 22 เมษายน 2566

Office of the Privacy Commissioner of Canada, **“Guidelines for Processing Personal Data Across Borders,”** สืบค้นเมื่อวันที่ 10 พฤษภาคม 2566, จาก https://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.asp