ปัญหาทางกฎหมายเกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 : ศึกษาเฉพาะกรณีการเก็บรักษาข้อมูลของภาคเอกชน[1]

นัตติยา คงอิว[2]

จากการศึกษาปัญหาทางกฎหมายเกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 : ศึกษาเฉพาะกรณีการเก็บรักษาข้อมูลของภาคเอกชน โดยพิจารณาตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยมีวัตถุประสงค์เพื่อศึกษาความหมาย ประวัติความเป็นมา แนวคิดและทฤษฎีที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลกรณีการเก็บรักษาข้อมูลของภาคเอกชน เพื่อแสวงหาแนวทางในการปรับปรุงบทบัญญัติกฎหมายที่เกี่ยวข้องกับกรณีดังกล่าวให้มีความเหมาะสมยิ่งขึ้น เมื่อกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลมีผลใช้บังคับ ถือเป็นเรื่องใหม่สำหรับประเทศไทย และเป็นเรื่องที่อยู่ในความสนใจของภาคราชการ ภาคเอกชน และประชาชนทั่วไปเป็นอย่างมาก ตั้งแต่เริ่มมีการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เนื่องจากกฎหมายฉบับนี้ทำให้ทุกภาคส่วนจะต้องปรับตัวเพื่อปรับเปลี่ยนนโยบาย แนวทางการดำเนินงานให้สอดคล้องกับกฎหมาย เพื่อคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความดูแลของหน่วยงานให้มีประสิทธิภาพ การคุ้มครองเจ้าของข้อมูลส่วนบุคคลมีระบบมาตรการการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่ทันสมัยเพื่อป้องกันการนำข้อมูลส่วนบุคคลไปใช้ในทางที่จะก่อให้เกิดผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลและส่งผลกระทบต่อเศรษฐกิจในภาพรวม ซึ่งปัจจุบันความก้าวหน้าทางเทคโนโลยีทำให้การเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคลทำได้โดยง่าย สะดวก และรวดเร็ว จึงทำให้มีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเสียหายและความเดือดร้อนให้แก่เจ้าของข้อมูลส่วนบุคคล รวมทั้งก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวม จึงเป็นเหตุผลอันสมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลขึ้น ซึ่งข้อมูลส่วนบุคคลมีความสำคัญต่อการวางแผนการทำงานและ การดำเนินกิจกรรมต่าง ๆ ของทั้งทางภาครัฐและภาคเอกชน ดังนั้น การคุ้มครองสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลจึงต้องให้ความสำคัญทั้งสองทาง นั่นคือ การให้ความสำคัญในการคุ้มครองสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของรัฐ และการให้ความสำคัญในการคุ้มครองสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของภาคเอกชน ทั้งนี้ เพราะทั้งภาครัฐและภาคเอกชนต่างก็มีความต้องการที่จะนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ตามวัตถุประสงค์ที่แตกต่างกันไป สำหรับภาคเอกชน

---

[1] บทความนี้เรียบเรียงจากการค้นคว้าอิสระ เรื่อง ปัญหาทางกฎหมายเกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562: ศึกษาเฉพาะกรณีการเก็บรักษาข้อมูลของภาคเอกชน โดยมีอาจารย์ที่ปรึกษา คือ รองศาสตราจารย์ ดร.ณฐ สันตาสว่าง และคณะกรรมการสอบ คือ รองศาสตราจารย์จุฑามาศ นิศารัตน์ และรองศาสตราจารย์อรวรรณ พจนานุรัตน์

[2] นักศึกษาปริญญาโท หลักสูตรนิติศาสตรมหาบัณฑิต (ส่วนกลาง) คณะนิติศาสตร์ มหาวิทยาลัยรามคำแหง

ก็มักจะนำมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เพื่อประโยชน์ทางด้านธุรกิจของตน เช่น สถาบันการเงิน จะต้องรักษาความลับของลูกค้าของตน การที่พนักงานหรือเจ้าหน้าที่เปิดเผยความลับลูกค้าโดยที่ลูกค้าไม่ได้ให้ความยินยอม นอกจากจะเป็นการทำผิดจรรยาบรรณแล้ว ยังจะมีความผิดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งปัจจุบันผู้ศึกษาเห็นว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อันเป็นกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย ยังมีบทบัญญัติที่อาจยังไม่สอดคล้องกับกฎเกณฑ์ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลระหว่างประเทศ ซึ่งถือว่าเป็นอุปสรรคในการคุ้มครองข้อมูลส่วนบุคคล รวมถึงข้อจำกัดเกี่ยวกับการใช้ การตีความ การนำกฎหมายไปบังคับใช้ในทางปฏิบัติ แม้กฎหมายฉบับนี้จะมีวัตถุประสงค์ในการคุ้มครองข้อมูลส่วนบุคคลให้เหมาะสม แต่ก็ยังคงมีปัญหาหลายประการที่ภาคเอกชนและเจ้าของข้อมูลต้องเผชิญในการปฏิบัติตามข้อกำหนดของกฎหมาย ผู้ศึกษาจึงมีความเห็นว่า เพื่อให้การคุ้มครองสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลที่อยู่ในความคุ้มครองของภาคเอกชนมีประสิทธิภาพยิ่งขึ้น มีความชัดเจนและเกิดผลสัมฤทธิ์

อย่างไรก็ตาม เมื่อได้ทำการศึกษาปัญหากฎหมายกรณีการเก็บรักษาข้อมูลของภาคเอกชนตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พบว่ายังมีปัญหาอยู่หลายประการ สามารถสรุปได้ดังนี้

ประการแรก ปัญหาเกี่ยวกับสิทธิในการขอแก้ไขข้อมูลของเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อาศัยอำนาจตามความในมาตรา 35 ที่กำหนดไว้ว่า “ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้อง เป็นปัจจุบัน สมบูรณ์และไม่ก่อให้เกิดความเข้าใจผิด”

เห็นได้ว่ามาตรา 35 กำหนดให้ผู้ควบคุมข้อมูลต้องรับผิดชอบ “โดยลำพัง” ในการดำเนินการให้ข้อมูลถูกต้อง โดยไม่คำนึงถึงว่าผู้ควบคุมข้อมูลจะทราบหรือไม่ว่าข้อมูลนั้นมีการเปลี่ยนแปลงในทางปฏิบัติข้อมูลของเจ้าของข้อมูลอาจเปลี่ยนแปลงโดยที่ผู้ควบคุมข้อมูลไม่สามารถทราบได้ เช่น การย้ายที่อยู่ เปลี่ยนชื่อ หรือเปลี่ยนเบอร์โทรศัพท์ การแก้ไขกฎหมายเพื่อกำหนดว่าเจ้าของข้อมูลต้องเป็น “ผู้ร้องขอ” หรือ “ผู้แจ้ง” ให้มีการแก้ไขข้อมูล จะทำให้เกิดระบบที่ เป็นธรรม และ ปฏิบัติได้จริงมากขึ้น หากเจ้าของข้อมูลมีสิทธิในการร้องขอแก้ไขข้อมูล จะทำให้เกิด กลไกร่วมระหว่างเจ้าของข้อมูลและผู้ควบคุมข้อมูล ในการรักษาความถูกต้องของข้อมูล กลไกนี้จะส่งเสริมให้เกิดความร่วมมือและความรับผิดชอบร่วมกัน ลดโอกาสการเกิดข้อผิดพลาดหรือการรั่วไหลของข้อมูล ซึ่งการที่เจ้าของข้อมูลเป็นผู้แจ้งข้อมูลที่ไม่ถูกต้องหรือไม่เป็นปัจจุบันจะช่วยให้ผู้ควบคุมข้อมูลสามารถอัปเดตข้อมูลได้อย่างรวดเร็ว ลดปัญหาความล่าช้า หรือขั้นตอนการตรวจสอบข้อมูลที่ซับซ้อน ซึ่งในบางกรณีอาจขัดกับหลักการของ PDPA ที่กำหนดให้ดำเนินการภายในเวลาที่เหมาะสม ถือได้ว่าเป็นการเพิ่มประสิทธิภาพการบริหารจัดการข้อมูลได้รวดเร็วยิ่งขึ้น และปรับปรุงให้สอดคล้องกับเจตนารมณ์ของ PDPA เอง เจตนารมณ์ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล คือการคุ้มครองสิทธิของเจ้าของข้อมูลและการใช้ข้อมูลอย่างเป็นธรรม หากไม่มีการบัญญัติให้เจ้าของข้อมูลมีสิทธิขอแก้ไขโดยชัดเจน อาจทำให้เกิด

ความสับสนหรือขาดกลไกที่เอื้อต่อการปกป้องสิทธิของเจ้าของข้อมูลเอง ซึ่งหากตีความตามตัวอักษรจะเห็นได้ว่า บทบัญญัติดังกล่าวมีลักษณะเป็นการกำหนดหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งถือเป็นการสร้างภาระให้แก่ผู้ควบคุมข้อมูลมากเกินความจำเป็น เนื่องจากผู้ควบคุมข้อมูลส่วนบุคคลทำหน้าที่ควบคุมฐานข้อมูลที่มีขนาดใหญ่และมีรายละเอียดค่อนข้างมาก ซึ่งหากภายหลังข้อมูลส่วนบุคคลมีการเปลี่ยนแปลงและไม่ใช่ข้อมูลที่เป็นปัจจุบันอีกต่อไป เจ้าของข้อมูลก็ควรที่จะเป็นผู้ร้องขอหรือผู้แจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการแก้ไขข้อมูล โดยไม่จำต้องให้ผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้ดำเนินการแก้ไขข้อมูลเอง เพื่อเป็นการลดภาระงานของผู้ควบคุมข้อมูล ประกอบกับเมื่อพิจารณากฎหมาย General Data Protection Regulation (GDPR) ของสหภาพยุโรปที่วางหลักเกณฑ์ไว้ในมาตรา 16 โดยบัญญัติให้เป็นสิทธิของเจ้าของข้อมูลส่วนบุคคลที่สามารถขอให้ผู้ควบคุมข้อมูลส่วนบุคคลแก้ไขข้อมูลส่วนบุคคลของตนให้ถูกต้องสมบูรณ์และเป็นปัจจุบันเพื่อเป็นการลดภาระของผู้ควบคุมข้อมูลด้วยเช่นกัน ทั้งนี้ การบัญญัติให้เจ้าของข้อมูลส่วนบุคคลสามารถร้องขอให้ผู้คสบคุมข้อมูลส่วนบุคคลแก้ไขข้อมูลส่วนบุคคลของตนให้ถูกต้อง เป็นปัจจุบัน และสมบูรณ์ตามข้อกำหนดในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และเป็นไปตามหลักเกณฑ์ของ General Data Protection Regulation (GDPR) มีข้อดีหลายประการ ทั้งในมุมของผู้ควบคุมข้อมูลและเจ้าของข้อมูล ไม่ว่าจะเป็นการทำให้ข้อมูลถูกต้องจะช่วยเพิ่มความน่าเชื่อถือในการใช้ข้อมูลต่างๆ ในการตัดสินใจ ไม่ว่าจะเป็นในกระบวนการทางธุรกิจการให้บริการ หรือการดำเนินการด้านกฎหมาย เมื่อข้อมูลที่ใช้ในการตัดสินใจเป็นข้อมูลที่ถูกต้อง ก็จะช่วยลดความเสี่ยงที่อาจเกิดจากการตัดสินใจที่ผิดพลาดจากข้อมูลที่ไม่ถูกต้อง ซึ่งข้อมูลที่ถูกต้องและเป็นปัจจุบันจะช่วยลดความเข้าใจผิดของทั้งสองฝ่าย (เจ้าของข้อมูลและผู้ควบคุมข้อมูล) เช่น การนำข้อมูลไปใช้ทางการแพทย์เพื่อตรวจสอบประวัติการรักษาของโรงพยาบาล หรือข้อมูลทางธุรกรรมการเงิน ที่สามารถตรวจสอบสถานะทางการเงินของผู้รับบริการ เป็นต้น รวมถึงการที่ข้อมูลส่วนบุคคลมีความถูกต้องและครบถ้วน จะช่วยลดความเสี่ยงในการละเมิดข้อมูลที่อาจเกิดจากความไม่สมบูรณ์หรือความคลาดเคลื่อนของข้อมูล ซึ่งอาจนำไปสู่การเปิดเผยข้อมูลที่ไม่ถูกต้องหรือการใช้ข้อมูลในทางที่ผิด การมีข้อมูลที่เป็นปัจจุบันจะช่วยให้ผู้ควบคุมข้อมูลสามารถพัฒนาบริการที่ตอบสนองความต้องการของลูกค้าได้ดีขึ้น เช่น การส่งข้อเสนอหรือการแนะนำบริการที่เหมาะสมกับผู้ใช้ในช่วงเวลาปัจจุบัน ซึ่งหากนำกฎหมายระหว่างประเทศอย่าง General Data Protection Regulation (GDPR) ของสหภาพยุโรปมาปรับปรุงพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 35 จะช่วยให้บริษัทหรือองค์กรภาคเอกชนสามารถปฏิบัติตามข้อกำหนดของกฎหมาย ข้อมูลมีความถูกต้อง สมบูรณ์ และเป็นปัจจุบัน รวมถึงช่วยลดความเสี่ยงทางกฎหมายและการถูกปรับ หรือการสูญเสียความเชื่อมั่นจากลูกค้าของสถาบันการเงินหรือผู้ใช้บริการของโรงพยาบาลได้อีกด้วย

ประการที่สอง ปัญหาเกี่ยวกับกระบวนการเก็บรักษาข้อมูลที่ไม่รัดกุมของเจ้าของข้อมูลส่วนบุคคล ซึ่งปัญหาดังกล่าวทำให้ข้อมูลส่วนบุคคลรั่วไหลได้โดยง่าย จะเห็นว่า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ PDPA (Personal Data Protection Act) มาตรา 22 บัญญัติว่า “การเก็บรวบรวมข้อมูลส่วนบุคคล ให้เก็บรวบรวมได้เท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล”

เห็นว่า มาตรา 22 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังไม่เพียงพอต่อการป้องกันข้อมูลรั่วไหลในทางปฏิบัติ แม้มาตรา 22 จะระบุให้เก็บข้อมูล "เท่าที่จำเป็น" ตามวัตถุประสงค์อันชอบด้วยกฎหมาย แต่ไม่ได้ระบุชัดเจนเกี่ยวกับมาตรการรักษาความปลอดภัยของข้อมูล ในทางปฏิบัติข้อมูลอาจถูกเก็บมากเกินไป หรือมีการเก็บข้อมูลที่ไม่ได้ถูกใช้ แต่ไม่ได้ลบทิ้งหรือควบคุมอย่างเหมาะสม ซึ่งกลายเป็น “จุดเสี่ยง” ต่อการรั่วไหลหรือถูกละเมิด แม้พระราชบัญญัติฉบับดังกล่าวได้มีข้อกำหนดและมาตรการที่ชัดเจนในการเก็บรักษาและคุ้มครองข้อมูลส่วนบุคคลของประชาชน แต่ในทางปฏิบัติยังพบปัญหาเกี่ยวกับกระบวนการเก็บรักษาข้อมูลที่ไม่รัดกุมจากเจ้าของข้อมูล ซึ่งอาจส่งผลให้ข้อมูลส่วนบุคคลรั่วไหลหรือถูกนำไปใช้โดยไม่ได้รับอนุญาตได้โดยง่าย ไม่ว่าจะเป็นการจัดการข้อมูลที่ไม่ปลอดภัย เจ้าของข้อมูลบางรายอาจเก็บข้อมูลส่วนบุคคลในรูปแบบที่ไม่ปลอดภัย เช่น การเข้าระบบที่ไม่มีการเข้ารหัสข้อมูล การเก็บข้อมูลในที่สาธารณะ หรือการไม่ปฏิบัติตามมาตรการรักษาความปลอดภัยที่มีประสิทธิภาพ โดยข้อมูลอาจถูกเข้าถึงหรือถูกนำไปใช้โดยผู้ที่ไม่ได้รับอนุญาต หากไม่มีระบบการเข้ารหัสที่ดีหรือการควบคุมการเข้าถึงข้อมูลอย่างเหมาะสม การเก็บข้อมูลโดยไม่จำเป็น ในบางกรณีเจ้าของข้อมูลอาจเก็บข้อมูลส่วนบุคคลมากเกินความจำเป็นสำหรับการให้บริการ โดยไม่มีการกำหนดระยะเวลาในการเก็บข้อมูล ซึ่งเป็นการเพิ่มความเสี่ยงให้ข้อมูลรั่วไหลหรือถูกนำไปใช้ในทางที่ไม่เหมาะสม ซึ่งการเก็บข้อมูลในระยะยาวอาจทำให้ข้อมูลถูกโจมตีได้ง่ายขึ้น หากไม่มีมาตรการป้องกันที่เข้มงวด หากมีการฝ่าฝืนสิทธิของเจ้าของข้อมูล เจ้าของข้อมูลอาจไม่ได้รับข้อมูลเกี่ยวกับการเก็บรักษาข้อมูลของตัวเอง หรือไม่ได้รับการแจ้งเตือนถึงวิธีการจัดการกับข้อมูลนั้น ๆ รวมถึงการขออนุญาตให้ใช้ข้อมูล หากเจ้าของข้อมูลไม่สามารถเข้าถึงหรือแก้ไขข้อมูลของตนเองได้ อาจทำให้เกิดปัญหาการจัดการข้อมูลที่ไม่เหมาะสมและข้อมูลอาจรั่วไหลออกไป รวมถึงมีการใช้มาตรการรักษาความปลอดภัยที่ไม่เพียงพอ แม้จะมีการใช้มาตรการรักษาความปลอดภัย แต่บางครั้งยังไม่เพียงพอที่จะป้องกันการรั่วไหลของข้อมูล เช่น การไม่อัปเดตซอฟต์แวร์รักษาความปลอดภัย หรือการให้สิทธิ์เข้าถึงข้อมูลที่กว้างเกินไป จึงควรมีมาตรการที่มุ่งเน้นให้เจ้าของข้อมูลและองค์กรที่เก็บข้อมูลต้องใช้มาตรการรักษาความปลอดภัยที่เหมาะสม เช่น การเข้ารหัสข้อมูล การจัดเก็บข้อมูลในที่ปลอดภัย การควบคุมการเข้าถึงข้อมูล และการจำกัดการใช้ข้อมูลเฉพาะที่จำเป็น เพื่อป้องกันไม่ให้ข้อมูลส่วนบุคคลถูกนำไปใช้ในทางที่ไม่เหมาะสมหรือเกิดการรั่วไหลออกไป สำหรับประเทศไทยเคยมีกรณีที่เกิดจากการเก็บหรือควบคุมข้อมูลของลูกค้าไม่รัดกุม ซึ่งส่งผลให้ข้อมูลรั่วไหลออกไปได้ง่าย โดยเฉพาะในภาคธุรกิจการเงินและธนาคาร ตัวอย่างที่เด่นชัด ได้แก่ เมื่อปี 2567 เกิดกรณีพนักงานธนาคารขายข้อมูลลูกค้าให้กับแก๊งคอลเซ็นเตอร์ ซึ่งตำรวจไซเบอร์ได้เข้าจับกุมหัวหน้าฝ่ายสินเชื่อ

ของธนาคารชื่อดังรายหนึ่ง ซึ่งเป็นพนักงานภายในองค์กรได้มีการนำข้อมูลลูกค้ากลุ่มเครดิตดีส่งขายให้กับนายหน้าสินเชื่อ นายหน้าประกัน หรือแก๊งคอลเซ็นเตอร์ โดยจะทยอยปล่อยข้อมูลชุดละประมาณ 3,000 –5,000 รายชื่อต่อชุด ในราคาเพียง 1 บาทต่อลูกค้า ทำให้ผู้กระทำได้รายได้หลายหมื่นบาทต่อเดือน ถือเป็นกรณีที่แสดงให้เห็นช่องโหว่จากภายในองค์กรอย่างร้ายแรง หากพิจารณากฎหมาย General Data Protection Regulation (GDPR) ของสหภาพยุโรป มีผลบังคับใช้เมื่อปี 2018 เป็นกฎหมายที่เข้มงวดที่สุดในโลกเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล มีการกำหนดมาตรการในการเก็บรักษาข้อมูลอย่างปลอดภัย รวมถึงข้อกำหนดในการให้ความยินยอมจากเจ้าของข้อมูลก่อนที่จะนำข้อมูลไปใช้ โดยกำหนดว่าองค์กรต้องใช้มาตรการป้องกันที่เหมาะสมเพื่อคุ้มครองข้อมูลจากการถูกเข้าถึงโดยไม่ได้รับอนุญาต เช่น การเข้ารหัสข้อมูล หรือการใช้ระบบที่มีการตรวจสอบสิทธิ์หลายขั้นตอน

ประการที่สาม ปัญหาเกี่ยวกับการโจรกรรมข้อมูลส่วนบุคคลโดยอาชญากรไซเบอร์ ถือเป็นกรณีการเข้าถึงข้อมูลที่เป็นความลับหรือข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต ซึ่งจะเห็นว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) มาตรา 24 บัญญัติว่า “ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(1) เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติ ซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ตามที่คณะกรรมการประกาศกำหนด

(2) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกายหรือสุขภาพของบุคคล

(3) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

(4) เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

(5) เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

(6) เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล”

เห็นว่า การเก็บรักษาข้อมูลต้องได้รับการยินยอมจากเจ้าของข้อมูลและต้องมีวัตถุประสงค์ที่ชัดเจนในการใช้ข้อมูลนั้น ๆ ซึ่งบทบัญญัติดังกล่าวยังไม่ครอบคลุมถึงการป้องกันการโจรกรรมข้อมูล ซึ่งการโจรกรรมข้อมูลถือเป็นการกระทำที่ผิดกฎหมาย เนื่องจากพระราชบัญญัตินี้มีจุดมุ่งหมายในการคุ้มครองสิทธิของบุคคลในการควบคุมข้อมูลส่วนบุคคลของตนเอง และการใช้ข้อมูลดังกล่าวโดยไม่ได้รับอนุญาตจะถือเป็นการละเมิดสิทธิของบุคคลนั้น ๆ โดยเฉพาะในกรณีที่มีการโจรกรรมข้อมูลที่เป็นข้อมูลส่วนบุคคล ซึ่งสามารถก่อให้เกิดความเสียหายทางการเงิน อาทิ ข้อมูลบัตรเครดิต ข้อมูลในสถาบันการเงิน

อาจถูกใช้ในการโอนเงินหรือทำธุรกรรมอย่างอื่นโดยที่ไม่ได้รับอนุญาต เสียชื่อเสียงหรือความเป็นส่วนตัว อาทิ ที่อยู่ ข้อมูลทางสุขภาพ สถานภาพ ซึ่งปัญหาการโจรกรรมข้อมูลนั้น สามารถเกิดขึ้นได้ในหลายรูปแบบ ไม่ว่าจะเป็นการแฮกข้อมูล (Hacking) โดยการเจาะระบบรักษาความปลอดภัยของเว็บไซต์หรือแอปพลิเคชัน เพื่อขโมยข้อมูลที่สำคัญ การฟิชชิง (Phishing) โดยหลอกลวงเจ้าของข้อมูลให้เปิดเผยข้อมูลสำคัญ การมัลแวร์ (Malware) โดยใช้ซอฟแวร์ที่เป็นอันตรายเพื่อขโมยข้อมูลจากเครื่องคอมพิวเตอร์หรืออุปกรณ์มือถือ ถือได้ว่าการโจรกรรมข้อมูลนั้นเป็นปัญหาที่ส่งผลกระทบต่อทั้งบุคคลและองค์กรอย่างกว้างขวาง แม้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะมีการกำหนดมาตรการต่าง ๆ เพื่อปกป้องข้อมูลส่วนบุคคลจากการโจรกรรม แต่การบังคับใช้กฎหมายในทางปฏิบัตินั้นยังคงเผชิญกับความท้าทาย เช่น การตรวจสอบและติดตามการโจรกรรมข้อมูลทางไซเบอร์ไม่ใช่เรื่องง่าย เนื่องจากอาชญากรไซเบอร์สามารถใช้เทคโนโลยีในการปกปิดตัวตนและตำแหน่งที่ตั้งของตนได้ เนื่องจากการโจรกรรมข้อมูลส่วนบุคคลสามารถเกิดขึ้นได้จากอาชญากรที่อยู่ต่างประเทศ จึงเป็นความท้าทายในการดำเนินการตามกฎหมายในกรณีที่ผู้กระทำผิดไม่ได้อยู่ในประเทศไทย เช่น กรณีแก๊งคอลเซ็นเตอร์ที่มีฐานที่ตั้งอยู่ที่ประเทศเพื่อนบ้าน ทำให้เกิดผลกระทบทั้งในด้านกฎหมายและการเสียความเชื่อมั่นจากประชาชนที่มารับบริการจากองค์กรภาคเอกชน

ดังนั้นแล้วเพื่อให้การเก็บรักษาข้อมูลของภาคเอกชนตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นไปอย่างมีประสิทธิภาพ ผู้ศึกษาจึงมีข้อเสนอแนะให้มีการแก้ไขเพิ่มเติมในประเด็นปัญหาดังต่อไปนี้

1. ปัญหาเกี่ยวกับสิทธิในการขอแก้ไขข้อมูลของเจ้าของข้อมูลส่วนบุคคล ผู้ศึกษาเห็นว่า ควรแก้ไขเพิ่มเติมพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 35 จากเดิมกำหนดให้ผู้ควบคุมข้อมูลต้องดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้อง เป็นปัจจุบัน สมบูรณ์และไม่ก่อให้เกิดความเข้าใจผิดภายในระยะเวลาที่กำหนด เพื่อให้ข้อมูลที่ใช้มีความถูกต้องและเป็นปัจจุบัน อย่างไรก็ดี บทบัญญัติดังกล่าวทำให้เกิดความท้าทายในแง่ของกระบวนการดำเนินการที่อาจมีข้อจำกัดหรือความล่าช้าได้ เนื่องจากในการปฏิบัติจริงอาจเกิดปัญหาหลายประการ ไม่ว่าจะเป็นในเรื่องของการยืนยันความถูกต้องของข้อมูล ซึ่งอาจทำให้การแก้ไขข้อมูลไม่สามารถทำได้ทันที ประกอบกับบทบัญญัติดังกล่าวอาจมีข้อจำกัดหรือความล่าช้าในการดำเนินการ หากระบบการจัดการข้อมูลของผู้ควบคุมข้อมูลไม่พร้อมหรือไม่ทันสมัย อาจทำให้กระบวนการขอแก้ไขข้อมูลไม่รวดเร็วหรือไม่ทันตามระยะเวลาที่กำหนด รวมถึงเรื่องข้อจำกัดทางเทคโนโลยี ซึ่งการจัดการข้อมูลส่วนบุคคลในบางองค์กรของภาคเอกชนอาจมีข้อจำกัดทางเทคโนโลยีที่ทำให้ไม่สามารถดำเนินการแก้ไขข้อมูลได้ในทันที ซึ่งอาจทำให้เกิดความไม่สะดวกแก่เจ้าของข้อมูล ซึ่งหากตีความตามตัวอักษร จะเห็นได้ว่า บทบัญญัติดังกล่าวมีลักษณะเป็นการกำหนดหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการ โดยไม่ได้ระบุให้เจ้าของข้อมูลเป็นผู้ร้องขอให้มีการตรวจสอบข้อมูลหรือแจ้งข้อมูล ซึ่งถือเป็นการสร้างภาระให้แก่ผู้ควบคุมข้อมูลมากเกินความจำเป็น เนื่องจากผู้ควบคุมข้อมูลส่วนบุคคลทำหน้าที่ควบคุมฐานข้อมูลที่มีขนาดใหญ่และมีรายละเอียดค่อนข้างมาก ซึ่งหากภายหลังข้อมูล

ส่วนบุคคลมีการเปลี่ยนแปลงและไม่ใช่ข้อมูลที่เป็นปัจจุบันอีกต่อไป เจ้าของข้อมูลก็ควรที่จะเป็นผู้ร้องขอหรือแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการแก้ไขข้อมูล โดยไม่จำต้องให้ผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้ดำเนินการแก้ไขข้อมูลเอง เพื่อเป็นการลดภาระงานของผู้ควบคุมข้อมูลดังกล่าวข้างต้น ตัวอย่างเช่น เวลาไปโรงพยาบาล ต้องมีการถามประวัติคนไข้ ประวัติการรักษา อาชีพ สิ่งแวดล้อมที่อยู่ โรคที่เป็น สิ่งเหล่านี้คนไข้หรือผู้ป่วยซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลต้องแจ้งแก่เจ้าหน้าที่ซึ่งเป็นผู้ควบคุมข้อมูล ถ้าข้อมูลมีการเปลี่ยนแปลงก็ต้องแจ้งเจ้าหน้าที่โรงพยาบาลให้แก้ไขข้อมูลตามที่คนไข้ร้องขอหรือแจ้งให้แก้ไข เจ้าหน้าที่ก็มีหน้าที่ตรวจสอบและแก้ไขให้ตรงกับที่แจ้ง เป็นต้น ด้วยเหตุดังกล่าวจึงควรมีการแก้ไขเพิ่มเติมพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 35 ดังนี้

เดิม มาตรา 35 กำหนดว่า “ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้องเป็นปัจจุบัน สมบูรณ์และไม่ก่อให้เกิดความเข้าใจผิด”

ขอเสนอแนะให้แก้ไขเพิ่มเติมเป็น มาตรา 35 กำหนดว่า “**เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้**ผู้ควบคุมข้อมูลส่วนบุคคล**ดำเนินการแก้ไขข้อมูลของตน**ให้ถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด **โดยผู้ควบคุมข้อมูลต้องดำเนินการภายในระยะเวลาที่สมควร**”

2. ปัญหาเกี่ยวกับกระบวนการเก็บรักษาข้อมูลที่ไม่รัดกุมของเจ้าของข้อมูลส่วนบุคคล ผู้ศึกษาเห็นว่าควรมีการแก้ไขเพิ่มเติมบทบัญญัติในเรื่องของการเก็บรวบรวมข้อมูลส่วนบุคคล ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 22 ที่เพียงกำหนดให้การเก็บรวบรวมข้อมูลส่วนบุคลต้องกระทำเท่าที่จำเป็นตามวัตถุประสงค์ที่ชอบด้วยกฎหมาย เพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล และไม่ให้มีการเก็บข้อมูลเกินความจำเป็นโดยไม่มีเหตุผลอันสมควร เนื่องจากการเก็บข้อมูลมากเกินไปเปิดช่องให้มีความเสี่ยงด้านความปลอดภัยและนำไปสู่การใช้ข้อมูลในทางที่ไม่เหมาะสม แต่ในทางปฏิบัติพบว่าปัญหาเกี่ยวกับกระบวนการเก็บรักษาข้อมูลที่ไม่รัดกุมจากเจ้าของข้อมูล ซึ่งอาจส่งผลให้ข้อมูลส่วนบุคคลรั่วไหลหรือถูกนำไปใช้โดยไม่ได้รับอนุญาตได้โดยง่ายนั้น เกิดจากการจัดการข้อมูลที่ไม่ปลอดภัย เจ้าของข้อมูลบางรายอาจเก็บข้อมูลส่วนบุคคลในรูปแบบที่ไม่ปลอดภัย เช่น การเข้าระบบที่ไม่มีการเข้ารหัสข้อมูล การเก็บข้อมูลในที่สาธารณะ หรือการไม่ปฏิบัติตามมาตรการรักษาความปลอดภัยที่มีประสิทธิภาพ โดยข้อมูลอาจถูกเข้าถึงหรือถูกนำไปใช้โดยผู้ที่ไม่ได้รับอนุญาต หากไม่มีระบบการเข้ารหัสที่ดี หรือการควบคุมการเข้าถึงข้อมูลอย่างเหมาะสม การเก็บข้อมูลโดยไม่จำเป็น ในบางกรณีเจ้าของข้อมูลอาจเก็บข้อมูลส่วนบุคคลมากเกินความจำเป็นสำหรับการให้บริการ โดยไม่มีการกำหนดระยะเวลาในการเก็บข้อมูล ซึ่งเป็นการเพิ่มความเสี่ยงให้ข้อมูลรั่วไหลหรือถูกนำไปใช้ในทางที่ไม่เหมาะสม ซึ่งการเก็บข้อมูลในระยะยาวอาจทำให้ข้อมูลถูกโจมตีได้ง่ายขึ้น หากไม่มีมาตรการป้องกันที่เข้มงวด หากมีการฝ่าฝืนสิทธิของเจ้าของข้อมูล เจ้าของข้อมูลอาจไม่ได้รับข้อมูลเกี่ยวกับการเก็บรักษาข้อมูลของตัวเอง หรือไม่ได้รับการแจ้งเตือนถึงวิธีการจัดการกับข้อมูลนั้น ๆ รวมถึงการขออนุญาตให้ใช้ข้อมูล หากเจ้าของข้อมูลไม่สามารถเข้าถึงหรือแก้ไขข้อมูลของตนเองได้ อาจทำให้เกิดปัญหาการจัดการข้อมูลที่ไม่เหมาะสมและข้อมูลอาจรั่วไหลออกไป รวมถึงมีการใช้มาตรการรักษาความปลอดภัยที่ไม่เพียงพอ

แม้จะมีการใช้มาตรการรักษาความปลอดภัย แต่บางครั้งยังไม่เพียงพอที่จะป้องกันการรั่วไหลของข้อมูล เช่น การไม่อัปเดตซอฟต์แวร์รักษาความปลอดภัย หรือการให้สิทธิ์เข้าถึงข้อมูลที่กว้างเกินไป จึงควรมีมาตรการที่มุ่งเน้นให้เจ้าของข้อมูลและองค์กรที่เก็บข้อมูลต้องใช้มาตรการรักษาความปลอดภัยที่เหมาะสม เช่น การเข้ารหัสข้อมูล การจัดเก็บข้อมูลในที่ปลอดภัย การควบคุมการเข้าถึงข้อมูล และการจำกัดการใช้ข้อมูลเฉพาะที่จำเป็นเพื่อป้องกันไม่ให้ข้อมูลส่วนบุคคลถูกนำไปใช้ในทางที่ไม่เหมาะสมหรือเกิดการรั่วไหลออกไป อย่างไรก็ตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังขาดกลไกการแก้ปัญหาเกี่ยวกับกระบวนการเก็บรักษาข้อมูลที่ไม่รัดกุมของเจ้าของข้อมูลส่วนบุคคล ดังนั้น จึงควรมีการแก้ไขเพิ่มเติมในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ในส่วนที่ 2 การเก็บรวบรวมข้อมูลส่วนบุคคล มาตรา 22

เดิม มาตรา 22 กำหนดว่า “การเก็บรวบรวมข้อมูลส่วนบุคลให้เก็บรวบรวมได้เท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล”

ขอเสนอแนะให้แก้ไขเพิ่มเติมเป็น มาตรา 22 กำหนดว่า “การเก็บรวบรวมข้อมูลส่วนบุคคลให้เก็บรวบรวมได้เท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล **โดยมีข้อกำหนดดังต่อไปนี้**

(1) ผู้ควบคุมข้อมูลส่วนบุคคลต้องประเมินและกำหนดประเภทของข้อมูลที่เก็บรวบรวมเฉพาะที่จำเป็นต่อการบรรลุวัตถุประสงค์ที่ชัดเจนและกำหนดไว้ล่วงหน้าเท่านั้น และต้องไม่เก็บข้อมูลที่เกินกว่าความจำเป็นในการดำเนินการตามวัตถุประสงค์นั้น ๆ

(2) ผู้ควบคุมข้อมูลต้องใช้มาตรการที่เหมาะสมในการรักษาความปลอดภัยของข้อมูลส่วนบุคคล เช่น การเข้ารหัสข้อมูล การใช้การยืนยันตัวตนหลายปัจจัย หรือมาตรการการควบคุมการเข้าถึงข้อมูลที่มีการจำกัดสิทธิ์ให้เข้าถึงข้อมูลเฉพาะบุคคลที่มีความจำเป็นต่อการทำงาน

(3) ข้อมูลส่วนบุคคลที่เก็บรวบรวมจะต้องถูกเก็บรักษาเฉพาะในระยะเวลาที่จำเป็นต่อการบรรลุวัตถุประสงค์ที่ได้แจ้งไว้กับเจ้าของข้อมูล เมื่อข้อมูลไม่จำเป็นอีกต่อไปต้องมีการทำลายข้อมูล หรือถอดถอนข้อมูลออกจากระบบในระยะเวลาที่เหมาะสมและไม่ล่าช้า

(4) ผู้ควบคุมข้อมูลต้องมีการประเมินความจำเป็นในการเก็บข้อมูลอย่างสม่ำเสมออย่างน้อยทุกปี เพื่อให้มั่นใจว่าการเก็บข้อมูลยังคงเป็นไปตามหลักการของความจำเป็นและเหมาะสม หากพบว่าข้อมูลที่เก็บไม่มีความจำเป็นแล้ว จะต้องมีการทำลายหรือถอนข้อมูลนั้นออกจากระบบ

(5) การเข้าถึงข้อมูลส่วนบุคคลจะต้องถูกจำกัดเฉพาะบุคคลที่มีความจำเป็นต้องใช้ข้อมูลนั้นเพื่อดำเนินการตามวัตถุประสงค์ของการเก็บข้อมูล โดยการเข้าถึงข้อมูลจะต้องมีการตรวจสอบสิทธิการเข้าถึงอย่างรัดกุม โดยมีการใช้การยืนยันตัวตนที่เหมาะสม

(6) หากมีการเก็บรวบรวมข้อมูลส่วนบุคคลที่เกินความจำเป็น หรือไม่สอดคล้องกับวัตถุประสงค์ที่แจ้งไว้ เจ้าของข้อมูลต้องได้รับการแจ้งให้ทราบภายในระยะเวลาที่เหมาะสมไม่เกินสามสิบวัน เพื่อให้เจ้าของข้อมูลสามารถยืนยันหรือขอให้ข้อมูลถูกลบออกได้

(7) ผู้ควบคุมข้อมูลต้องนำเทคโนโลยีที่ทันสมัยและมีความปลอดภัยมาใช้ในการจัดการข้อมูลส่วนบุคคลอย่างเหมาะสม และต้องมีการปรับปรุงเทคโนโลยีตามพัฒนาการของภัยคุกคามไซเบอร์ที่เกิดขึ้นใหม่ ๆ เพื่อให้มั่นใจในความปลอดภัยของข้อมูลที่เก็บรวบรวม"

3. ปัญหาเกี่ยวกับการโจรกรรมข้อมูลส่วนบุคคลโดยอาชญากรไซเบอร์ โดยการเข้าถึงข้อมูลที่เป็นความลับหรือข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต ผู้ศึกษาเห็นว่า ควรมีการเพิ่มบทบัญญัติในเรื่องของการเก็บรวบรวมข้อมูลส่วนบุคคล เพิ่มเติมจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24 ที่เพียงกำหนดให้การเก็บรักษาข้อมูลต้องได้รับการยินยอมจากเจ้าของข้อมูลและต้องมีวัตถุประสงค์ที่ชัดเจนในการใช้ข้อมูลนั้น ๆ เนื่องจากปัญหาการโจรกรรมข้อมูลส่วนบุคคลโดยอาชญากรไซเบอร์ที่เกิดจากการเข้าถึงข้อมูลที่เป็นความลับหรือข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตเป็นปัญหาที่มีผลกระทบอย่างมากทั้งในด้านความเสียหายต่อเจ้าของข้อมูลและต่อภาคเอกชนที่รับผิดชอบในการเก็บข้อมูลนั้น ๆ การโจรกรรมข้อมูลถือเป็นการกระทำที่ผิดกฎหมาย เนื่องจากพระราชบัญญัตินี้มีจุดมุ่งหมายในการคุ้มครองสิทธิของบุคคลในการควบคุมข้อมูลส่วนบุคคลของตนเอง และการใช้ข้อมูลดังกล่าวโดยไม่ได้รับอนุญาตจะถือเป็นการละเมิดสิทธิของบุคคลนั้น ๆ โดยเฉพาะในกรณีที่มีการโจรกรรมข้อมูลที่เป็นข้อมูลส่วนบุคคล ซึ่งสามารถก่อให้เกิดความเสียหายทางการเงิน อาทิ ข้อมูลบัตรเครดิต ข้อมูลในสถาบันการเงินอาจถูกใช้ในการโอนเงินหรือทำธุรกรรมอย่างอื่นโดยที่ไม่ได้รับอนุญาต เสียชื่อเสียงหรือความเป็นส่วนตัว อาทิ ที่อยู่ ข้อมูลทางสุขภาพ สถานภาพ ซึ่งปัญหาการโจรกรรมข้อมูลนั้นสามารถเกิดขึ้นได้ในหลายรูปแบบ ไม่ว่าจะเป็นการแฮกข้อมูล (Hacking) โดยการเจาะระบบรักษาความปลอดภัยของเว็บไซต์หรือแอปพลิเคชันเพื่อขโมยข้อมูลที่สำคัญ การฟิชชิง (Phishing) โดยหลอกลวงเจ้าของข้อมูลให้เปิดเผยข้อมูลสำคัญ การมัลแวร์ (Malware) โดยใช้ซอฟแวร์ที่เป็นอันตรายเพื่อขโมยข้อมูลจากเครื่องคอมพิวเตอร์หรืออุปกรณ์มือถือ ถือได้ว่าการโจรกรรมข้อมูลนั้น เป็นปัญหาที่ส่งผลกระทบต่อทั้งบุคคลและองค์กรอย่างกว้างขวาง อย่างไรก็ตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังขาดกลไกการแก้ปัญหาเกี่ยวกับการโจรกรรมข้อมูลส่วนบุคคลโดยอาชญากรไซเบอร์ โดยการเข้าถึงข้อมูลที่เป็นความลับหรือข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต ดังนั้น จึงควรมีการเพิ่มบทบัญญัติในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ในส่วนที่ 2 การเก็บรวบรวมข้อมูลส่วนบุคคล นอกเหนือจากมาตรา 24 โดยอาจมีบทบัญญัติเพิ่มเติมในส่วนของมาตรการในการดำเนินการเพื่อป้องกันมิให้เกิดการโจรกรรมข้อมูลส่วนบุคคล

มาตรา 24 กำหนดว่า "ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่

(1) เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ตามที่คณะกรรมการประกาศกำหนด

(2) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกายหรือสุขภาพของบุคคล

(3) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

(4) เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

(5) เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

(6) เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล”

ขอเสนอแนะให้มีบทบัญญัติเพิ่มเติมในส่วนของมาตรการในการดำเนินการเพื่อป้องกันมิให้เกิดการโจรกรรมข้อมูลส่วนบุคคล เป็น มาตรา ... กำหนดว่า **“การเก็บรวบรวมข้อมูลส่วนบุคคลต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลและต้องมีวัตถุประสงค์ที่ชัดเจนในการใช้ข้อมูลนั้น ๆ โดยต้องมีการดำเนินการดังนี้**

(1) ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการเพื่อรักษาความปลอดภัยของข้อมูลที่เก็บรวบรวมและจัดเก็บ โดยการใช้มาตรการที่เหมาะสม เช่น การ เข้ารหัสข้อมูล การ จำกัดการเข้าถึงข้อมูล และการใช้เทคโนโลยีที่ทันสมัย ในการป้องกันข้อมูลไม่ให้ถูกเข้าถึงโดยไม่ได้รับอนุญาต

(2) ผู้ควบคุมข้อมูลต้องกำหนด สิทธิ์การเข้าถึงข้อมูล อย่างเข้มงวด โดยเฉพาะข้อมูลที่มีความละเอียดอ่อน และควรมีการตรวจสอบสิทธิ์การเข้าถึงข้อมูลอย่างสม่ำเสมอ รวมถึงการบันทึกการเข้าถึงข้อมูล

(3) ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำการ อัปเดตระบบซอฟต์แวร์ และ เทคโนโลยีรักษาความปลอดภัยอย่างต่อเนื่อง เพื่อป้องกันช่องโหว่ที่อาจทำให้ข้อมูลถูกโจรกรรมจากอาชญากรไซเบอร์

(4) ผู้ควบคุมข้อมูลต้องดำเนินการ ประเมินความเสี่ยง ที่อาจเกิดขึ้นจากการเก็บรวบรวมข้อมูลส่วนบุคคลและต้องดำเนินการตามแผนการป้องกันและบรรเทาผลกระทบจากความเสี่ยงเหล่านั้น

(5) ในกรณีที่เกิดการรั่วไหลของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลต้อง แจ้งเตือนเจ้าของข้อมูลและ หน่วยงานที่เกี่ยวข้อง โดยทันที พร้อมทั้งต้องดำเนินการแก้ไขสถานการณ์และบรรเทาผลกระทบที่เกิดขึ้น”

จากการศึกษา จะเห็นว่าภาคเอกชนที่มีการเก็บข้อมูลส่วนบุคคลจะต้องรับผิดชอบในการปกป้องข้อมูลเหล่านั้นอย่างเหมาะสมตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลกำหนด หากภาคเอกชนไม่สามารถเก็บข้อมูลได้อย่างปลอดภัย หรือมีการจัดเก็บที่ไม่เพียงพอ อาจทำให้ข้อมูลส่วนบุคคลรั่วไหลหรือถูกโจรกรรม ซึ่งจะเกิดปัญหาตามมา เช่น การละเมิดสิทธิส่วนบุคคลของเจ้าของข้อมูลและการเสี่ยงต่อการสูญเสียทางการเงินจากการใช้ข้อมูลในทางที่ผิด ดังนั้น จากประเด็นปัญหาดังกล่าวข้างต้นจึงสรุปได้ว่าปัญหาหลักที่พบคือการขาดมาตรการป้องกันที่เพียงพอ โดยเฉพาะในกรณีที่องค์กรไม่ได้ใช้เทคโนโลยีที่ทันสมัยหรือไม่มีการรักษาความปลอดภัยข้อมูลขั้นสูง มิได้กำหนดชั้นความลับ ซึ่งทำให้ข้อมูลในองค์กรมีช่องโหว่ที่อาชญากรไซเบอร์สามารถโจมตีได้ง่าย อย่างไรก็ตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งถือว่าเป็นกฎหมายที่มีการคุ้มครองสิทธิและความเป็นส่วนตัวของบุคคลในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล รวมถึงการจัดการข้อมูลส่วนบุคคลอย่างเหมาะสม เพื่อให้เกิดความสมดุลระหว่างการคุ้มครองข้อมูลส่วนบุคคลและการใช้ข้อมูลในกิจกรรมทางธุรกิจหรือการพัฒนาเทคโนโลยีในสังคม ยังคงมีข้อบกพร่องที่ควรพิจารณาอยู่หลายประการซึ่งควรมีการปรับปรุงแก้ไขเพื่อให้การบังคับใช้กฎหมายนั้นมีประสิทธิภาพยิ่งขึ้น

เอกสารอ้างอิง

คู่มือการปฏิบัติงานตามกฎหมายข้อมูลข่าวสารของราชการ พุทธศักราช 2540 ของเจ้าหน้าที่ของรัฐ, สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ, บริษัท ศรีเมืองการพิมพ์ จำกัด: มิถุนายน 2548, 1.

ชุลีพร น่วมทนง, “หลักสิทธิมนุษยชน เรื่อง สิทธิมนุษยชนกับการคุ้มครองข้อมูลส่วนบุคคล,” (เอกสารของการอบรมหลักสูตรหลักนิติธรรมเพื่อประชาธิปไตยรุ่นที่ 2 วิทยาลัยรัฐธรรมนูญ สถาบันรัฐธรรมนูญศึกษา สำนักงานศาลรัฐธรรมนูญ: 2557), 5.

ธาริณี มณีรอด, “ปัญหาทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล,” (วิทยานิพนธ์, หลักสูตรนิติศาสตรมหาบัณฑิต สาขาวิชานิติศาสตร์ คณะนิติศาสตร์ปรีดี พนมยงค์ มหาวิทยาลัยธุรกิจบัณฑิต, 2559), 57-64.

นิติกร จิรฐิติกาลกิจ, “ข้อสังเกตบางประการเกี่ยวกับการรับรองและคุ้มครองสิทธิและเสรีภาพของประชาชนในรัฐธรรมนูญไทยและบริบทสากล,” จดหมายข่าวสำนักงานศาลรัฐธรรมนูญ, ฉ.2 (เมษายน-มิถุนายน 2562): 9 - 16.

บรรเจิด สิงคะเนติ, **หลักพื้นฐานของสิทธิและเสรีภาพและศักดิ์ศรีความเป็นมนุษย์ตามรัฐธรรมนูญ** (กรุงเทพฯ: วิญญูชน, 2547), หน้า 260.

บวรศักดิ์ อุวรรณโณ, **คำอธิบายกฎหมายมหาชนเล่ม 2 การแบ่งแยกกฎหมายมหาชน -เอกชน และพัฒนาการกฎหมายมหาชนในประเทศไทย** (กรุงเทพ: นิติธรรม, 2538), หน้า 49-50.

บุญศรี มีวงศ์อุโฆษ, **คำอธิบายวิชากฎหมายรัฐธรรมนูญเปรียบเทียบ : รัฐธรรมนูญเยอรมันโครงการตำราและเอกสารประกอบการสอนคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์** (กรุงเทพฯ: โรงแก้วการพิมพ์, 2535), หน้า 157-158.

ภูริชญา วัฒนรุ่ง, **หลักกฎหมายมหาชน** (กรุงเทพฯ: สำนักพิมพ์มหาวิทยาลัยรามคำแหง, 2542), หน้า 366.

วีรพงษ์ บึงไกร, การเปิดเผยข้อมูลส่วนบุคคลตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พุทธศักราช 2540, (2543), 14.

วรดนู วิจาระนันท์, “หลักความได้สัดส่วนในระบบกฎหมายไทย,” (วิทยานิพนธ์, นิติศาสตรมหาบัณฑิต จุฬาลงกรณ์มหาวิทยาลัย, 2548), 1.

สุธรรม อยู่ในธรรม และคณะ, โครงการศึกษากฎหมายคุ้มครองข้อมูลส่วนบุคคลและผลกระทบของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลต่อประเทศไทย, คณะนิติศาสตร์ มหาวิทยาลัยหอการค้าไทย, 2559.

สมเกียรติ สุทธินวล, “ปัญหาการคุ้มครองข้อมูลสุขภาพอิเล็กทรอนิกส์ของผู้เข้ารับการรักษาในโรงพยาบาล,” สำนักงานบัณฑิตศึกษา คณะนิติศาสตร์ มหาวิทยาลัยรามคำแหง, 2560

สมยศ เชื้อไทย, **คำอธิบายหลักรัฐธรรมนูญทั่วไป**, (กรุงเทพฯ: เรือนแก้วการพิมพ์, 2535), หน้า 127.

หยุด แสงอุทัย, **หลักรัฐธรรมนูญทั่วไป**, (กรุงเทพฯ: วิญญูชน, 2538), หน้า 123-124.