ปัญหากฎหมายเกี่ยวกับการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562[1]

ฐาปนี ชูจันทร์[2]

การศึกษาเกี่ยวกับปัญหากฎหมายเกี่ยวกับการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีวัตถุประสงค์เพื่อศึกษาถึงความเป็นมา แนวคิดและทฤษฎีเกี่ยวกับการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายเกี่ยวกับการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อให้ผู้ศึกษาได้รับความรู้ความเข้าใจในเรื่องของการคุ้มครองข้อมูลส่วนบุคคล เนื่องจากในปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมาก ไม่เพียงแต่จะก่อความเสียหายให้แก่องค์กรและบุคคลแล้ว ยังก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวมอีกด้วย กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้ตระหนักถึงปัญหาที่เกิดขึ้นจึงได้เสนอ เพื่อบรรเทาผลกระทบที่อาจเกิดขึ้นกับหน่วยงานภาครัฐ เอกชน และประชาชน โดยให้ตรากฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้น เพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคล โดยให้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ขึ้นใช้บังคับ เพื่อพัฒนาเมืองไปสู่ความเป็นอัจฉริยะ กฎหมายจะเน้นไปที่การสร้างมาตรฐานให้กับองค์กรต่าง ๆ ที่มีการเก็บรวบรวมข้อมูลส่วนบุคคล รวมถึงการนำไปใช้ เพื่อควบคุมการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลและต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลในเวลาทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล การนำข้อมูลส่วนบุคคลไปใช้เป็นประการอื่นนอกจากที่ได้แจ้งไว้จะไม่สามารถกระทำได้ หากเว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หากผู้ควบคุมข้อมูลส่วนบุคคลเปลี่ยนแปลงวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล นอกจากนี้เจ้าของข้อมูลส่วนบุคคลมีสิทธิเพิกถอนความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้เว้นแต่มีกฎหมายหรือสัญญาซึ่งให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคลห้ามไว้ แม้ว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีการบังคับใช้มาแล้วเป็นระยะเวลาถึง 2 ปี นับจากวันที่ประกาศใช้ โดยวัตถุประสงค์ “การคุ้มครอง” ข้อมูลส่วนบุคคล ทั้งนี้ผู้ศึกษาเห็นว่า ในใจความสำคัญของกฎหมายฉบับนี้ กลับมุ่งเน้นไปที่องค์กร หน่วยงาน หรือนิติบุคคลให้มี “มาตรฐาน” ในการจัดการข้อมูลส่วนบุคคลอย่างเหมาะสมและเพียงพอ เมื่อมีความ

---

[1]บทความนี้เรียบเรียงจากการศึกษาอิสระ เรื่อง ปัญหากฎหมายเกี่ยวกับการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยมีอาจารย์ที่ปรึกษา คือ ผู้ช่วยศาสตราจารย์ ดร.ดนพร จิตต์จรุงเกียรติ และคณะกรรมการสอบ คือ ผู้ช่วยศาสตราจารย์ ดร.มณฑิชา ภักดีคง และรองศาสตราจารย์ ดร.พันธ์เทพ วิทิตอนันต์

[2]นักศึกษาปริญญาโท หลักสูตรนิติศาสตรมหาบัณฑิต สาขาวิทยบริการเฉลิมพระเกียรติ จังหวัดตรัง คณะนิติศาสตร์ มหาวิทยาลัยรามคำแหง

จำเป็นต้องขอใช้ข้อมูลส่วนบุคคล แต่ปัจจุบันกลับพบว่าข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานของรัฐบางแห่ง ยังไม่ได้รับการคุ้มครองหรือการเก็บรักษาไว้ดีเท่าที่ควร เนื่องจากบ่อยครั้งมักจะมีการนำเสนอข่าวทางสื่อต่าง ๆ ว่ามีการนำข้อมูลส่วนบุคคลบางส่วนออกไปใช้ในทางที่ไม่เหมาะสม ผู้ศึกษาได้เล็งเห็นถึงปัญหาและความสำคัญที่จะเกิดขึ้นต่อไปอนาคต เมื่อศึกษาแล้วพบว่ากฎหมายในบางเรื่องยังไม่มีความสอดคล้องกันจึงมีปัญหาข้อกฎหมาย ที่น่าศึกษาอยู่หลายประการ ด้วยกัน

จากการศึกษาทำให้ทราบว่าการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังมีกฎหมายในบางเรื่องที่ไม่มีความสอดคล้องกัน และไม่มีความชัดเจน ซึ่งสรุปได้ดังนี้

การศึกษาในประเด็นปัญหาเกี่ยวกับปัญหาเกี่ยวกับการตีความประโยชน์สาธารณะ ตามมาตรา 28(6)

สำหรับประโยชน์สาธารณะ โดยทั่วไปทุกคนมักจะเข้าใจตรงกันว่าหมายถึง ประโยชน์อันเกิดแก่ประชาชนทั้งในระดับชาติและระดับท้องถิ่น ซึ่งรัฐเป็นผู้ดำเนินการเพื่อตอบสนองความต้องการของคนส่วนใหญ่ในสังคมมิใช่เพื่อตอบสนองความต้องการของผู้ดำเนินการเองหรือบุคคลกลุ่มใดกลุ่มหนึ่งเท่านั้น ดังนั้น จากหลักกฎหมายมาตรา 28 (6) โดยกำหนดหลักการเกี่ยวกับกฎเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลไปยังต่างประเทศและอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน หากมีนโยบายการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับการตรวจสอบและรับรองจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล สามารถโอนข้อมูลไปยังต่างประเทศได้ เว้นแต่ เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะ ซึ่งในกรณีที่มีปัญหาเกี่ยวกับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอของประเทศปลายทาง หรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคล ให้เสนอต่อคณะกรรมการเป็นผู้วินิจฉัย หากคณะกรรมการเห็นว่าเป็นข้อมูลที่เข้าข้อยกเว้น ตามาตรา 28 (6) ข้อมูลดังกล่าวนี้ไม่ได้รับการคุ้มครอง เมื่อพิจารณาจากมาตรา 28 (6) ดังกล่าวข้างต้นนี้ เห็นว่าคำว่า เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ หมายความว่า การอ้างถึงเหตุบางอย่างของผู้ปกครองในการให้กระทำหรือละเว้นให้กระทำอย่างหนึ่งอย่างใดแก่ผู้ที่จะกระทำ ซึ่งเป็นการใช้ดุลพินิจของผู้มีอำนาจหน้าที่ใช้ในทางปฏิบัติอันเป็นสำคัญในการอ้างถึงเหตุแห่งการนั้น ๆ เพื่อให้เข้าข้อยกเว้น ซึ่งในการตีความของคำดังกล่าวนี้ไม่ได้มีการระบุอย่างแน่ชัดว่า มีข้อจำกัดหรือหลักเกณฑ์การพิจารณาเช่นไร มีเพียงการให้อำนาจคณะกรรมการในการใช้ดุลพินิจ ดังนั้น หากกฎหมายตีความรวม ๆ เช่นนี้ ซึ่งเป็นเหตุให้ผู้ใช้อำนาจสามารถตีความได้กว้างมากโดยไม่มีการกำหนดกรอบหรือลักษณะในการตีความที่มันชัดเจน ทั้ง ๆ ที่หลักการตีความกฎหมาย เป็นหลักการค้นหาหรืออธิบายความหมายของถ้อยคำที่ปรากฏในตัวบทกฎหมาย โดยอาศัยการใช้เหตุผลตามหลักตรรกวิทยาและสามัญสำนึกให้มีความหมายที่ชัดเจน เมื่อพบว่าบทบัญญัติของกฎหมายเคลือบคลุม มีข้อความกำกวม คลุมเครือ ไม่ชัดเจน หรือว่ามีการแปลความหมายไปได้หลายทาง เพื่อนำกฎหมายนั้นไปใช้บังคับแก่กรณีที่มีปัญหาได้อย่างถูกต้องและเป็นธรรม เนื่องจากการตีความกฎหมายเปรียบเสมือนเป็นกุญแจดอกสำคัญที่ผู้ที่เกี่ยวข้องกับการตีความกฎหมายจะได้นำไปใช้แก้ไขปัญหา

ในทางกฎหมายต่าง ๆ ได้ เพราะการตีความที่แตกต่างกันโดยไม่มีขอบเขตนั้นจะส่งผลกระทบต่อเจ้าของข้อมูลได้

ประเด็นปัญหาที่สอง คือ ปัญหาเกี่ยวกับคุณสมบัติของคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ตามมาตรา 48

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (ส.ค.ส.) เป็นหน่วยงานที่มีหน้าที่กำหนดมาตรฐานในการเก็บรวบรวมข้อมูล การใช้ และการเปิดเผยข้อมูลส่วนบุคคล โดยมีคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ซึ่งมาจากการสรรหาและแต่งตั้งอันประกอบด้วยกรรมการที่เป็นข้าราชการโดยตำแหน่ง 2 คน คือปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เลขาธิการคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ กรรมการคนอื่น ๆ มาจากการสรรหาและแต่งตั้งจากผู้มีความรู้ ความเชี่ยวชาญและประสบการณ์ในด้านการคุ้มครองข้อมูลส่วนบุคคลทั้งหมด ตามมาตรา 48 ซึ่งการที่กฎหมายกำหนดไว้เช่นนี้ ทำให้การถ่วงดุลในการใช้อำนาจในการตัดสินใจในประเด็นต่าง ๆ ย่อมเกิดขึ้นได้ยาก เพราะไม่สามารถคานการใช้อำนาจของอีกฝ่ายได้ หากมีการทุจริตกันเกิดขึ้น เพราะการใช้อำนาจของบุคคล 2 คนนี้ อาจเป็นไปอย่างไม่เต็มที่ในการพิจารณาและการปฏิบัติงาน เนื่องจากกฎหมายให้อำนาจ และหน้าที่แก่ ส.ค.ส. ไว้ในแต่ละประการนั้นล้วนมีผลอย่างมากในการดำเนินงานของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เนื่องจากกฎหมายกำหนดนโยบายการบริหารงาน และให้ความเห็นชอบแผนการดำเนินงานของสำนักงาน ออกข้อบังคับว่าด้วยการจัดองค์กร การเงิน การบริหารงานบุคคล การบริหารงานทั่วไป การตรวจสอบภายใน และตลอดจนแต่งตั้งคณะกรรมการสรรหาเลขาธิการ และวินิจฉัยอุทธรณ์คำสั่งทางปกครองของเลขาธิการในส่วนที่เกี่ยวกับการบริหารงานของสำนักงานด้วย ตามมาตราที่บัญญัติไว้ใน 54 ดังนั้น การกำหนดจำนวนของข้าราชการที่จะมาปฏิบัติงานกับกรรมการผู้ที่ได้มาจากการเลือกที่เท่า ๆ กัน ตามหลักการถ่วงดุลกัน เพื่อให้สามารถทำงานร่วมกันได้อย่างราบรื่น มีประสิทธิภาพมิให้ฝ่ายใดฝ่ายหนึ่งใช้อำนาจจนเกินขอบเขต โดยแต่ละฝ่ายสามารถถือสิทธิ และปกป้องสิทธิของตนเอง โดยการยับยั้ง และสนับสนุนในกิจกรรมสำคัญๆ ของอีกฝ่ายหนึ่งได้ แต่เป็นการแบ่งแยกหน้าที่โดยใช้อำนาจร่วมกันจึงกล่าวได้ว่าหลักการถ่วงดุลอำนาจนี้ มีผลช่วยให้การปฏิบัติหน้าที่ตามอำนาจที่ได้รับมอบหมายจากเพื่อเป็นไปได้โดยสะดวก และป้องกันการเป็นเผด็จการในการใช้อำนาจของฝ่ายใดฝ่ายหนึ่ง

ประเด็นปัญหาที่สาม คือ ปัญหาเกี่ยวกับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล ในการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

ปัจจุบันประเทศไทยมีการติดต่อรับส่งข้อมูลกับทางประเทศสมาชิกสหภาพยุโรปเป็นจำนวนมาก โดยมีคณะกรรมการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลคอยควบคุมมาตรฐานของข้อมูลที่ส่งออกไปยังต่างประเทศ ดังนั้นจึงมีความจำเป็นยิ่งที่จะต้องยกระดับการคุ้มครองข้อมูลส่วนบุคคลให้เท่าเทียมกับประเทศที่มีการใช้ GDPR กับทั้งนา ๆ ประเทศ เนื่องจากข้อมูลส่วนบุคคลสามารถระบุถึงลักษณะของบุคคล

กับทั้งการระบุข้อมูลลักษณะที่อยู่ ข้อมูลที่มีรายละเอียดเชิงลึกไปจนสามารถระบุถึงพฤติกรรมของบุคคลนั้น ๆ ได้ ดังนั้นการกำหนดมาตรการในการคุ้มครองข้อมูลส่วนบุคคลจึงเป็นเรื่องที่มีความสำคัญ ทางรัฐจึงมีการออกกฎหมายเพื่อคุ้มครองสิทธิการเป็นส่วนตัวเอาไว้ในลักษณะเป็นการยินยอมของเจ้าของข้อมูลนั้น ๆ โดยเฉพาะขึ้น ทั้งนี้ในการคุ้มครองการส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศของประเทศไทยนั้น ยังคงมีการให้ผู้ที่ทำการควบคุมข้อมูลส่วนบุคคลเป็นผู้มีหน้าที่ ในการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ เพื่อป้องกันการสูญหาย การเข้าถึง การใช้เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ตามมาตรา 37 แม้ว่าจะมีการให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลในการลบหรือทำลาย หรือทำให้ข้อมูลนั้นไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ทั้งนี้ก็อาจทำให้ข้อมูลนั้นเกิดการรั่วไหล สูญหาย หรือเข้าถึง ใช้ เปลี่ยนแปลงแก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลได้อยู่ดี ซึ่งในต่างประเทศอย่างในสหภาพยุโรป หรือ EU ได้วางมาตรการคุ้มครองความเป็นส่วนตัวของข้อมูลส่วนบุคคล ในรูปแบบที่เรียกว่า GDPR ซึ่งเป็นกลไกการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป กับทั้งมีการกำหนดบทลงโทษแก่หน่วยงานที่ไม่ปฏิบัติตามข้อกำหนดอันเป็นเหตุให้เกิดความเสียหายหรือการรั่วไหลของข้อมูล อีกทั้ง ขอบเขตการคุ้มครองอย่างกินพื้นที่มาถึงการรับส่งข้อมูลที่อยู่ภายนอกประเทศสมาชิกด้วย เพื่อเป็นมาตรการอย่างหนึ่งที่เกิดจากความเป็นส่วนตัวและข้อมูลส่วนบุคคลนั้นมิให้ต้องถูกล่วงละเมิดมาใช้บังคับต่อสมาชิกและที่ส่งมายังประเทศสมาชิกจะต้องถือปฏิบัติด้วย ดังนั้น ผู้ควบคุมต้องใช้ดุลพินิจในการพิจารณาเปรียบเทียบสิทธิของเจ้าของข้อมูลกับประโยชน์สาธารณะในการมีอยู่ของข้อมูลนั้น สิทธิที่จะได้รับการคุ้มครองในข้อมูลเกี่ยวกับตัวเอง เพื่อป้องกันไม่ให้เกิดการละเมิดสิทธิส่วนบุคคลเกิดขึ้น จากการรั่วไหลของข้อมูลไปยังหน่วยงานหรือองค์กรอื่น ๆ

ประเด็นปัญหาที่สี่ คือ ปัญหาเกี่ยวกับการกำหนดโทษทางอาญา ตามมาตรา 80

โทษทางอาญา เป็นมาตรการที่กฎหมายกำหนดไว้สำหรับลงโทษแก่ผู้กระทำความผิดอาญา ตามพระราชบัญญัติฉบับนี้กำหนดว่าผู้ควบคุมข้อมูล ถือเป็นผู้ล่วงรู้ข้อมูลโดยมีหน้าที่สำคัญที่กฎหมายกำหนดไว้ เช่น จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล เพื่อป้องกันมิให้ผู้อื่นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ กับทั้งแจ้งเหตุละเมิดข้อมูลส่วนบุคคลให้สำนักงานคุ้มครองข้อมูลส่วนบุคคลทราบภายใน 72 ชั่วโมง นับแต่ทราบเหตุ และผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ดำเนินการตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคล ทั้งนี้เมื่อพิจารณาตามมาตรา 80 กำหนดให้ ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ถ้า ผู้นั้นนำไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ ในการกำหนดโทษเป็นการอาศัยอำนาจดุลพินิจในการเรียกโทษ ทั้งนี้ จากประเด็นที่ว่าโทษทางอาญาตามมาตรา 80 นั้นเป็นบทกำหนดโทษที่มีลักษณะทั่วไปและมีอัตราโทษที่น้อยเกินไป เพราะกฎหมายกำหนดไว้เพียงว่าห้ามนำไปเปิดเผย โดยที่กฎหมายไม่ได้กำหนดถึงความสำคัญของข้อมูลที่ถูกนำไปเปิดเผย หากว่าข้อมูลนั้นเป็นข้อมูลส่วนบุคคลที่มีความสำคัญยิ่งและเมื่อถูก

เปิดเผยไปกลับส่งผลกระทบต่อร่างกาย เสรีภาพ อนามัยและสิทธิ์ต่าง ๆ รวมถึงการเปลี่ยนการดำเนินชีวิตประจำวันของเจ้าของข้อมูลที่เป็นเหตุร้ายแรงอันสำคัญ ดังนั้น หากกฎหมายมีมาตรการจัดการหรือลงโทษกับบุคคลที่เปิดเผยข้อมูลไว้นั้น ส่งผลให้การละเมิดสิทธิส่วนบุคคลลดลง เพื่อให้เจ้าของข้อมูลได้รับการคุ้มครองจากรัฐและเพิ่มเป็นความมั่นใจว่าไม่มีบุคคลใดจะมาละเมิดข้อมูลของตนได้ ทั้งนี้ เพื่อให้เป็นไปตามเจตนารมณ์และสอดคล้องกับวัตถุประสงค์ของกฎหมาย ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

จากการศึกษาค้นคว้าปัญหากฎหมายเกี่ยวกับการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ผู้ศึกษาพบว่ามีข้อเสนอแนะ คือ

1. เพิ่มคำนิยาม ในมาตรา 6 เป็น

“ประโยชน์สาธารณะ หมายความว่า ประโยชน์ต่อสาธารณะหรือประโยชน์อันเกิดแก่การจัดทำบริการสาธารณะ หรือประโยชน์อื่นใดที่เกิดจากการดำเนินการหรือการกระทำที่มีลักษณะเป็นการส่งเสริมหรือสนับสนุนแก่ประชาชนเป็นส่วนรวม หรือประชาชนส่วนรวมจะได้รับประโยชน์จากการดำเนินการหรือการกระทำนั้น ที่มิใช่เพื่อประโยชน์ของเอกชนรายหนึ่งรายใด อันกิจกรรมเหล่านี้เรียกว่า ประโยชน์สาธารณะ”

2. แก้ไขเพิ่มเติมมาตรา 48 วรรคหนึ่ง เป็น

“ให้มีคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ประกอบด้วย ประธานกรรมการซึ่งสรรหาและแต่งตั้งจากผู้มีความรู้ ความเชี่ยวชาญ และประสบการณ์ในด้านการคุ้มครองข้อมูลส่วนบุคคล ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และเลขาธิการคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ เป็นกรรมการ และเลขาธิการสภาพัฒนาเศรษฐกิจแห่งชาติและเลขาธิการคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ ปลัดกระทรวงการต่างประเทศ และกรรมการผู้ทรงคุณวุฒิจำนวนสี่คนซึ่งสรรหาและแต่งตั้งจากผู้มีความรู้ ความเชี่ยวชาญ และประสบการณ์ในด้านการคุ้มครองข้อมูลส่วนบุคคลอย่างน้อยสองคน”

3. แก้ไขเพิ่มเติมมาตรา 29 วรรคสองและวรรคสาม เป็น

วรรคสอง นโยบายในการคุ้มครองข้อมูลส่วนบุคคล ลักษณะของเครือกิจการหรือเครือธุรกิจเดียวกัน เพื่อการประกอบกิจการหรือธุรกิจร่วมกัน และหลักเกณฑ์และวิธีการตรวจสอบและรับรองตามวรรคหนึ่ง จะต้องสร้างขึ้นโดยเจตนาและโดยปริยายคุ้มครองข้อมูล ในการจัดเก็บข้อมูลส่วนบุคคลโดยใช้นามแฝง หรือนิรนามโดยสิ้นเชิง และใช้การตั้งค่าภาวะเฉพาะส่วนตัวสูงสุดเท่าที่เป็นไปได้โดยปริยาย เพื่อให้ข้อมูลไม่มีการเปิดเผยต่อสาธารณะหากปราศจากความยินยอมอย่างชัดแจ้ง และไม่สามารถใช้เพื่อระบุบุคคลได้โดยปราศจากสารสนเทศเพิ่มเติมที่เก็บแยกกัน ห้ามประมวลผลข้อมูลส่วนบุคคล ยกเว้นกระทำภายใต้กฎหมายที่ระบุตามกฎระเบียบการคุ้มครองข้อมูลทั่วไป GDPR หรือหากผู้ควบคุมหรือผู้ประมวลผลข้อมูลได้รับความยินยอมแบบเลือกภายหลังอย่างชัดแจ้งจากเจ้าของข้อมูล เจ้าของข้อมูลมีสิทธิ

เพิกถอนการอนุญาตนี้เมื่อใดก็ได้ และผู้ประมวลผลข้อมูลส่วนบุคคลต้องเปิดเผยการเก็บข้อมูลใด ๆ อย่างชัดเจน ประกาศเหตุผลและความมุ่งหมายอันชอบด้วยกฎหมายสำหรับการประมวลผลข้อมูล ว่าจะเก็บข้อมูลนานเท่าใด และมีการแบ่งข้อมูลนั้นกับบุคคลภายนอก หรือไม่ ผู้ใช้มีสิทธิขอสำเนาพกพาได้ของข้อมูลที่ผู้ประมวลผลข้อมูลเก็บรวบรวมในรูปแบบร่วม และมีสิทธิลบข้อมูลของตนภายใต้พฤติการณ์บางอย่าง กำหนดให้ทางการสาธารณะและธุรกิจซึ่งมีกิจกรรมกับการประมวลผลข้อมูลส่วนบุคคลเป็นประจำหรือเป็นระบบเป็นหลักว่าจ้างเจ้าพนักงานคุ้มครองข้อมูลซึ่งรับผิดชอบต่อการจัดการให้เป็นไปตาม GDPR ธุรกิจต้องรายงานการละเมิดข้อมูลใด ๆ ภายใน 72 ชั่วโมงหากมีผลเสียต่อภาวะเฉพาะบุคคลของผู้ใช้

วรรคสาม ในกรณีมาตรา 28 หรือยังไม่มีนโยบายในการคุ้มครองข้อมูลส่วนบุคคลตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอาจส่ง หรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศได้โดยได้รับยกเว้นไม่ต้องปฏิบัติตามมาตรา 28 เมื่อผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้จัดให้มีมาตรการคุ้มครองสามารถบังคับตามสิทธิของเจ้าของข้อมูลส่วนบุคคลได้ รวมทั้งมีมาตรการเยียวยาทางกฎหมายที่มีประสิทธิภาพ ตามหลักเกณฑ์และวิธีการเป็นไปตามมาตรฐานขั้นต่ำ ตาม GDPR โดยการเคลื่อนย้ายข้อมูลส่วนบุคคลโดยเสรีภายในสหภาพจะไม่ถูกจำกัดหรือห้ามด้วยเหตุผลที่เกี่ยวข้องกับการคุ้มครองบุคคลธรรมดาเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล โดยใช้กับการประมวลผลข้อมูลส่วนบุคคลทั้งหมดหรือบางส่วนด้วยวิธีการอัตโนมัติและการประมวลผลอื่น ๆ ที่ไม่ใช่วิธีอัตโนมัติของข้อมูลส่วนบุคคลซึ่งเป็นส่วนหนึ่งของระบบการจัดเก็บหรือมีวัตถุประสงค์เพื่อเป็นส่วนหนึ่งของระบบการจัดเก็บ

ในส่วนของผู้ควบคุมนั้น ต้องใช้มาตรการที่เหมาะสมเพื่อให้ข้อมูลใด ๆ ที่อ้างถึง ที่เกี่ยวข้องกับการประมวลผลกับเจ้าของข้อมูลในรูปแบบที่กระชับ โปร่งใส เข้าใจได้ และเข้าถึงได้ง่าย โดยใช้ข้อความที่ชัดเจนและชัดเจน ภาษา โดยเฉพาะอย่างยิ่งสำหรับข้อมูลใด ๆ ที่ส่งถึงเด็กโดยเฉพาะ ข้อมูลจะต้องจัดให้มีขึ้นเป็นลายลักษณ์อักษรหรือโดยวิธีการอื่น รวมถึงตามความเหมาะสมโดยวิธีการทางอิเล็กทรอนิกส์ เมื่อได้รับการร้องขอจากเจ้าของข้อมูล ข้อมูลอาจถูกจัดให้โดยวาจา โดยมีเงื่อนไขว่าตัวตนของเจ้าของข้อมูลนั้นได้รับการพิสูจน์ด้วยวิธีการอื่น และต้องอำนวยความสะดวกในการใช้สิทธิ์ของเจ้าของข้อมูล โดยผู้ควบคุมต้องไม่ปฏิเสธที่จะดำเนินการตามคำขอของเจ้าของข้อมูลเพื่อใช้สิทธิ์ของตน เว้นแต่ผู้ควบคุมจะแสดงให้เห็นว่าไม่อยู่ในฐานะที่จะระบุเจ้าของข้อมูลได้ และหากกระทำผิดนั้นต้องลงโทษ

3. ยกเลิก มาตรา 37 (1) และควรเพิ่ม “มาตรฐานขั้นต่ำ ตามกฎระเบียบของ (EU) ในรูปแบบ General Data Protection Regulation (GDPR)” มาตรา 1 (9) ในเรื่องมาตรฐานการคุ้มครองที่แตกต่างกันตามคำสั่งที่ 95/46/EC โดยมีลักษณะคือ

หลักการคุ้มครองข้อมูลเป็นไปตามมาตรฐานของ EU Directive ข้อกำหนดใน GDPR ดังนี้

1. ขอบเขตการบังคับใช้เชิงพื้นที่ GDPR บังคับใช้ในทุกหน่วยงานที่มีการประมวลผลข้อมูลส่วนบุคคลพลเมืองที่อาศัยอยู่ใน EU ไม่ว่าบริษัทจะตั้งอยู่ที่ไหน นั่นคือ GDPR บังคับใช้กับผู้ควบคุมข้อมูลและผู้

ประมวลผลข้อมูลใน EU ไม่ว่าการประมวลผลจะทำใน EU หรือไม่ก็ตาม โดยจะบังคับใช้กับทุกกิจกรรมที่เป็นการจำหน่ายสินค้าและบริการแก่พลเมือง EU และทุกกิจกรรมที่มีลักษณะการติดตามพฤติกรรมของพลเมืองที่เกิดขึ้นใน EU หากเป็นธุรกิจของประเทศอื่นที่ไม่ใช่สมาชิก EU (Non-EU Business) ก็ต้องดำเนินการแต่งตั้งผู้แทนใน EU ด้วย

2. บทลงโทษ ในกรณีที่เกิดความเสียหายหรือการรั่วไหลของข้อมูล (Data Breach) หน่วยงานที่ไม่ปฏิบัติตามข้อกำหนดจะถูกปรับเป็นจำนวนเงินถึง 20 ล้านยูโร หรือ 2-4% ของรายได้ต่อปีขึ้นอยู่กับว่าวงเงินใดสูงกว่า ซึ่งเป็นโทษปรับสูงสุดในกรณีร้ายแรง เช่น การไม่ขอความยินยอมที่เหมาะสมเพียงพอในการประมวลผลข้อมูล หรือการปฏิบัติขัดหลักการ Privacy by Design บางกรณีมีโทษปรับ 2% เช่นกรณีการไม่มีการบันทึกข้อมูลอย่างเป็นระบบ การไม่แจ้ง Supervising Authority และเจ้าของข้อมูลเมื่อเกิดเหตุรั่วไหล หรือการไม่จัดทำ Privacy Impact Assessment

3. การให้ความยินยอม หลักความยินยอมได้รับการยืนยันเข้มแข็งมากขึ้น โดยระบุว่าการขอความยินยอมต้องดำเนินการในรูปแบบที่เข้าใจได้และสามารถเข้าถึงได้สะดวก (Intelligible and easily access) ต้องแจ้งวัตถุประสงค์ของการประมวลผลข้อมูลในการขอคำยินยอม โดยการขอความยินยอมต้องมีความชัดเจน ใช้ภาษาที่ง่ายต่อการเข้าใจ นอกจากนี้การยกเลิกการให้ความยินยอมต้องก็ต้องดำเนินการได้ด้วยความสะดวก

ภายใต้ GDPR มีการกำหนดสิทธิของเจ้าของข้อมูลที่ชัดเจนมากขึ้น ดังนี้

1. สิทธิที่จะได้รับแจ้งเมื่อเกิดความเสียหาย (Breach Notification) ภายใต้ GDPR ถือว่าการแจ้งเป็นหน้าที่ที่ต้องปฏิบัติ เมื่อเกิดความเสียหายหรือการรั่วไหลของข้อมูล ซึ่งเกิดผลกระทบมีความเสี่ยงต่อสิทธิเสรีภาพของเจ้าของข้อมูล ทั้งนี้การแจ้งต้องดำเนินการภายใน 72 ชั่วโมง โดยผู้ประมวลผลต้องแจ้งต่อลูกค้าและผู้ควบคุมข้อมูลโดยไม่ชักช้าหลังจากเกิดความเสียหาย

2. สิทธิที่จะรู้และเข้าถึงข้อมูล (Right to Access) เจ้าของข้อมูลมีสิทธิที่จะได้รับการแจ้งจากผู้ควบคุมข้อมูลว่า มีการประมวลผลข้อมูลหรือไม่ การประมวลผลดำเนินการที่ไหน มีวัตถุประสงค์อะไร และเมื่อร้องขอ ผู้ควบคุมข้อมูลจะต้องจัดหาสำเนาข้อมูลดังกล่าวให้เจ้าของข้อมูลในรูปแบบอิเล็กทรอนิกส์โดยไม่คิดค่าใช้จ่าย ข้อกำหนดนี้เป็นการเปลี่ยนแปลงที่สำคัญในเรื่องความโปร่งใสของข้อมูลและเป็นการยืนยันความเข้มแข็งของเจ้าของข้อมูล

3. สิทธิที่จะขอให้ลบข้อมูล (Right to be Forgotten/Right to erase) เจ้าของข้อมูลมีสิทธิ (1) ในการแจ้งให้ลบข้อมูล ระงับการเผยแพร่ หยุดการประมวลผลโดยบุคคลที่สาม (2) มีสิทธิในการแจ้งให้ลบข้อมูลที่ไม่มีส่วนเกี่ยวข้องตามวัตถุประสงค์ในการจัดเก็บครั้งแรก และ (3) มีสิทธิในการลบข้อมูลที่เจ้าของข้อมูลได้ยกเลิกความยินยอม ทั้งนี้ ผู้ควบคุมต้องใช้ดุลพินิจในการพิจารณาเปรียบเทียบสิทธิของเจ้าของข้อมูลกับประโยชน์สาธารณะในการมีอยู่ของข้อมูลนั้น

4. สิทธิที่จะได้รับข้อมูลเกี่ยวกับตัวเอง (Data Portability) สิทธิที่จะได้รับข้อมูลเกี่ยวกับตัวเอง ในรูปแบบที่สามารถใช้งานได้ตามปกติรวมทั้งรูปแบบที่อ่านได้ด้วยเครื่องมือ/อุปกรณ์ (machine-readable format)

5. สิทธิที่จะได้รับความคุ้มครองตั้งแต่ต้น (Privacy by Design/Privacy by Default) กำหนดให้มีการวางระบบความคุ้มครอง(Protection) ตั้งแต่ในโอกาสแรกของการออกแบบระบบ มากกว่าการมาเพิ่มการดำเนินการในภายหลัง โดยกำหนดว่าต้องมีการใช้มาตรการทางเทคนิคและการบริหารที่เหมาะสม โดยยึดหลักประสิทธิภาพ เพื่อให้เป็นไปตามข้อกำหนดและเป็นการคุ้มครองสิทธิเจ้าของข้อมูล ผู้ควบคุมข้อมูลจะเก็บและและประมวลผลข้อมูลได้เพียงเท่าที่จำเป็นเพื่อให้ภารกิจสำเร็จ (data minimization) และต้องมีการจำกัดการเข้าถึงข้อมูลโดยผู้ที่ไม่มีความเกี่ยวข้องใด ๆกับการประมวลผล

6. สิทธิที่จะได้รับการคุ้มครองโดยเจ้าหน้าที่คุ้มครองข้อมูล (Data Protection Officers: DPO) ใช้ระบบการเก็บบันทึกข้อมูลภายในองค์กร (Internal Record Keeping) แทนระบบการรายงานต่อ Data Protection Authorities (DPA) และกำหนดให้มีการแต่งตั้งเจ้าหน้าที่รับผิดชอบ (DPO) สำหรับผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลขนาดใหญ่ และมีภารกิจหลักในการติดตามและประมวลผลข้อมูลเป็นประจำและเป็นระบบ (Regularly and Systematic monitoring Data Subjects) แต่การแต่งตั้ง DPO ต้องคำนึงถึงคุณสมบัติด้านวิชาชีพและความเชี่ยวชาญด้านกฎหมายและภาคปฏิบัติ โดยอาจแต่งตั้งเจ้าหน้าที่ภายในองค์กรหรือผู้ให้บริการภายนอก ต้องแจ้งข้อมูลการติดต่อกับทาง DPA และต้องมีทรัพยากรเหมาะสมกับการปฏิบัติภารกิจและพัฒนาความรู้ความเชี่ยวชาญของ DPO ทั้งนี้ DPO มีระบบรายงานต่อผู้บริหารระดับสูงและต้องไม่ทำหน้าที่อื่นที่อาจเป็นกรณีผลประโยชน์ทับซ้อน

4. เห็นควรให้เพิ่มเติม วรรคสอง ในมาตรา 80 เป็น

“วรรคสอง ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ถ้าผู้นั้นนำไปเปิดเผยแก่ผู้อื่นตามวรรคหนึ่ง อันเป็นเหตุให้เจ้าของข้อมูลเกิดความเสียหายอย่างร้ายแรงจากการกระทำนั้น ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ และให้ปรับห้าแสนบาท”

เอกสารอ้างอิง

กาญจนารัตน์ ลีวิโรจน์. “สิทธิและเสรีภาพของประชาชน:ความคุ้มครองที่อาจถูกจากัดโดยกฎหมายและกฎ.” **เอกสารวิชาการส่วนบุคคล (Individual Study)**. รายงานการฝึกอบรมหลักสูตรหลักนิติธรรมเพื่อประชาธิปไตยรุ่นที่ 1. วิทยาลัยรัฐธรรมนูญ สำนักงานศาลรัฐธรรมนูญ.

กรุงเทพธุรกิจ. **'ข้อมูลส่วนบุคคล' สำคัญแค่ไหน ตามกฎหมาย GDPR ยุโรป** [Online]. Available URL: https://www.bangkokbiznews.com/news/detail/882376, 2564 (พฤษภาคม, 24).

ณัฐดนัย วงศ์ประถม. **GDPR กฎหมายข้อมูลส่วนบุคคล (DATA PRIVACY)** [Online]. Available URL: https://nutdnuy.medium.com/ข้อมูลส่วนบุคคล-data-privacy-7ef3310bcb5d, 2564 (พฤษภาคม, 24).

ฤทัย หงส์สิริ และ มานิตย์ จุมปา. **คำอธิบายกฎหมายข้อมูลข่าวสารของราชการ**. กรุงเทพมหานคร: นิติธรรม, 2542.