

บทที่ 4

วิเคราะห์ปัญหากฎหมายที่เกี่ยวข้องกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

จากการที่ผู้วิจัยได้ดำเนินการค้นคว้าวิจัยถึงแนวทางของกฎหมายที่เกี่ยวข้องกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลในบทที่ 1 บทที่ 2 และ บทที่ 3 พร้อมทั้ง ศึกษากฎหมายที่เกี่ยวข้องกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลของประเทศไทยและต่างประเทศ ได้แก่ สหภาพยุโรป สาธารณรัฐสิงคโปร์ ประเทศญี่ปุ่น และประเทศแคนาดา พบว่าประเทศไทยนั้น ยังคงประสบปัญหากฎหมายในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไม่ว่าจะเป็นปัญหากฎหมายคุ้มครองข้อมูลส่วนบุคคลยังขาดความชัดเจน ปัญหาการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สำนักงาน สกส.) รวมถึงปัญหาบทลงโทษทางอาญา ซึ่งพบว่าในต่างประเทศมีการตรากฎหมายคุ้มครองข้อมูลส่วนบุคคล ไม่ว่าจะเป็นแนวทางปฏิบัติ หลักเกณฑ์ หรือ บทลงโทษต่างๆ โดยมีการอ้างอิงหลักการพื้นฐานมาจากสหภาพยุโรป เช่นเดียวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย หรือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แต่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้น ในส่วนของการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลยังไม่เหมาะสมต่อการบังคับใช้กับบริบทของประเทศไทย ผู้วิจัยจึงวิเคราะห์สภาพประเด็นปัญหากฎหมายในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ดังต่อไปนี้

4.1 ปัญหาพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(4)

ปัจจุบันประเทศไทยได้ให้ความสำคัญกับการคุ้มครองสิทธิความเป็นส่วนตัวในด้านข้อมูลส่วนบุคคลมากยิ่งขึ้น เพื่อให้ประชาชนตกอยู่ในสถานะที่ไม่ปลอดภัยต่อการดำรงชีพซึ่งการคุ้มครองข้อมูลส่วนบุคคลนั้น ถือเป็นส่วนหนึ่งของการคุ้มครองสิทธิความเป็นส่วนตัว (Right of Privacy) เนื่องจากความเป็นอยู่ส่วนตัวนั้น ย่อมหมายความรวมถึง ความเป็นส่วนตัวเกี่ยวกับข้อมูล (Information Privacy) ความเป็นส่วนตัวในชีวิตร่างกาย (Bodily Privacy) ความเป็นส่วนตัวในการติดต่อสื่อสาร (Communication Privacy) และความเป็นส่วนตัวในเคหสถาน (Territorial Privacy) ซึ่งการคุ้มครองข้อมูลส่วนบุคคลนั้นถือได้ว่าเป็นความเป็นส่วนตัวเกี่ยวกับข้อมูล โดยสิทธิความเป็นส่วนตัวมีการรับรองไว้อย่างชัดเจนในปฏิญญาสากลว่าด้วยสิทธิมนุษยชนข้อ 12 ที่กล่าวว่าบุคคลใดจะถูกแทรกแซงโดยพลการในความเป็นส่วนตัว ในครอบครัว ในเคหสถาน หรือในการ

สื่อสาร หรือจะถูกกลบเกลื่อนเกียรติยศและชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองตามกฎหมายต่อการแทรกแซงสิทธิ หรือการลบล้างดังกล่าวนี้

เช่นเดียวกับแนวคิดของโทมัส ฮอบส์ (Thomas Hobbs) ที่กล่าวในหนังสือ Leviathan ไว้ว่า “ในสภาวะที่ยัง ไม่มีสังคมมนุษย์มีชีวิตอยู่ในธรรมชาติด้วยความหวาดกลัว เห็นแก่ตัวและชอบใช้ความรุนแรงเป็นสภาวะของอนาธิปไตย ด้วยความจำเป็นเพื่อหลีกเลี่ยงจากสภาวะอันเลวร้ายมนุษย์จึงรวมตัวกันขึ้นเป็นสังคม และทำความตกลงมอบสิทธิตามธรรมชาติของตนบางส่วนให้กับรัฐควบคุมดูแล เพื่อไม่ให้เกิดสภาวะที่เป็นอนาธิปไตยได้อีก เช่นเดียวกับแนวคิดของจอห์น ล็อก (John Locke) ที่กล่าวไว้ในหนังสือ The Second Treaties of Government ว่า “มนุษย์ในสภาวะธรรมชาตินั้นเป็นสภาวะแห่งสันติสุขต่างช่วยเหลือเกื้อกูลกัน มีความเสมอภาคและเป็นอิสระมีสิทธิที่สำคัญ 3 ประการ คือ สิทธิในชีวิต อิสรภาพ และทรัพย์สิน ภายใต้การควบคุมของกฎแห่งธรรมชาติ การล่วงละเมิดสิทธิที่มนุษย์มีอยู่ตามธรรมชาติจะถูกลงโทษโดยการแก้แค้นทดแทนจากผู้เสียหายหรือญาติมิตรของผู้เสียหาย

รวมถึงแนวคิดของซามูเอล ดี วอร์เรนที่ 2 (Samuel D. Warren) และหลุยส์ แบริน (Louis D. Brandeis) นักกฎหมายชาวอเมริกันและรองผู้พิพากษาในศาลฎีกาของสหรัฐอเมริกาที่กล่าวว่า ความก้าวหน้าดังกล่าวนี้ทำให้มีความจำเป็นต้องให้ความคุ้มครองแก่บุคคล เพราะพัฒนาการของเทคโนโลยีดังกล่าวทำให้เกิดการคุกคามสิทธิประโยชน์ของบุคคลอย่างน่ากลัว จึงมีแนวความคิดว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection) เป็นแนวความคิดที่มีพัฒนาการมาจากการคุ้มครองสิทธิในความเป็นส่วนตัว (Privacy Right) มีพัฒนาการมาเป็นระยะเวลายาวนานแล้วโดยในสมัยโรมันแนวความคิดเกี่ยวกับเรื่องความเป็นส่วนตัวยอมรับว่าบุคคลแต่ละคนมีเขตแดนของตนเอง ในเขตแดนเสมือนเป็นที่พักที่บุคคลไม่เกี่ยวข้องกับกิจกรรมทางสังคมในช่วงเวลาส่วนตัว เป็นดินแดนเฉพาะตัวของแต่ละบุคคลเท่านั้น และเป็นที่ปราศจากการเข้ามาเกี่ยวข้องจากคนอื่น แนวความคิดในการคุ้มครองความเป็นส่วนตัวที่มีความชัดเจนและได้รับการยอมรับมากที่สุดเมื่อมีการเผยแพร่บทความเรื่อง “The Right to Privacy” หรือ “สิทธิในความเป็นส่วนตัว”

เนื่องจากปัจจุบันประชาชนมีการนำเทคโนโลยีมาประยุกต์ใช้กับชีวิตประจำวันมากกว่าเมื่อก่อน ไม่ว่าจะเป็นการเก็บ รวบรวม และการเปิดเผยข้อมูลส่วนบุคคลที่สามารถกระทำได้ง่ายผ่านช่องทางอิเล็กทรอนิกส์ จึงอาจส่งผลให้มีการละเมิดข้อมูลส่วนบุคคลขึ้น และอาจสร้างความเสียหาย เดือดร้อนให้กับเจ้าของข้อมูลส่วนบุคคลได้ และเมื่อมีเหตุละเมิดข้อมูลส่วนบุคคลขึ้นจะต้องมีการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลในลำดับต่อมา ซึ่งแม้ว่าประเทศไทยนั้นจะมีการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ขึ้น และมีผลบังคับใช้อย่างเต็มรูปแบบเมื่อวันที่ 1 มิถุนายน 2565 แล้วก็ตาม แต่กฎหมายดังกล่าวยังไม่ได้ครอบคลุมถึงกรณีการแจ้งเหตุละเมิด

ข้อมูลส่วนบุคคลที่ชัดเจนมากพอ จึงทำให้เกิดปัญหาในการบังคับใช้กฎหมายขึ้น และทำให้การบังคับใช้กฎหมายไม่สามารถบรรลุผลในการให้ความคุ้มครองสิทธิในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลได้อย่างครบถ้วนหลายประการ และก่อให้เกิดปัญหาหรือช่องว่างทางกฎหมาย

จากการศึกษาพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เรื่อง การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล มาตรา 37 (4) “แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่มีการละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด” จากบทบัญญัติดังกล่าวพบว่า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังขาดความชัดเจน เนื่องจากการกำหนดไว้อย่างชัดเจนว่ากรณีใดบ้างที่ต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) และเจ้าของข้อมูลส่วนบุคคล รวมถึงไม่มีการกำหนดข้อยกเว้นว่าหากเป็นการเข้าถึง เก็บ ใช้เปิดเผย คัดลอก หรือแก้ไขข้อมูลส่วนบุคคล โดยไม่ได้รับอนุญาตภายในองค์กร ไม่ให้ถือว่าเป็นการรั่วไหลที่ต้องแจ้งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จึงทำให้องค์กรไม่มีระยะเวลาเพียงพอต่อการประเมินสถานการณ์เหตุละเมิดข้อมูลส่วนบุคคลก่อนที่จะรายงานให้ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ ทำให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลไม่ได้รับข้อมูลที่ถูกต้อง และเพียงพอ สำหรับเหตุละเมิดข้อมูลส่วนบุคคลดังกล่าว

อย่างไรก็ตาม หากพิจารณาตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศเกี่ยวกับการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล พบว่าในต่างประเทศมีการกำหนดหลักเกณฑ์ในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไว้อย่างชัดเจน ซึ่งมีความยืดหยุ่น และเหมาะสมต่อการบังคับใช้กฎหมายในปัจจุบัน โดยกฎหมายของสหภาพยุโรป หรือ General data Protection Regulation (GDPR) ได้กำหนดหลักการของการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไว้อย่างชัดเจนว่ากรณีใดบ้างที่ต้องมีการแจ้งกรณีที่มีการละเมิดข้อมูลส่วนบุคคล ในกรณีที่มีการละเมิดข้อมูลส่วนบุคคล ผู้ตรวจสอบจะต้องดำเนินการโดยไม่ล่าช้าและจะต้องดำเนินการภายใน 72 ชั่วโมงนับแต่ทราบเหตุ ซึ่งหลักเกณฑ์ดังกล่าว ถือเป็นต้นแบบในการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของประเทศไทย แต่เนื่องจากบริบทของประเทศไทย และสหภาพยุโรปมีความแตกต่างกันอยู่มาก อาทิ ด้านการสื่อสาร ด้านเทคโนโลยี ด้านดิจิทัล เป็นต้น อาจจะทำให้การดำเนินการเพื่อแจ้งเหตุละเมิดข้อมูลส่วนบุคคลภายในระยะเวลา 72 ชั่วโมงนับแต่ทราบเหตุ นั้น ส่งผลให้การ

ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นไปยาก โดยกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ หรือ Personal Data Protection Act: PDPA ไม่ได้กำหนดว่าต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง ซึ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ ได้กำหนดหลักการของการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไว้ว่า กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ บังคับใช้กับองค์กร บุคคล บริษัท สมาคม หรือหน่วยงานที่ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลไม่ว่าจะเป็นองค์กรที่ตั้งขึ้นตามสาธารณรัฐสิงคโปร์ หรือมีถิ่นที่อยู่ในสาธารณรัฐสิงคโปร์ หรือไม่ ซึ่งหากมีบุคคลถูกละเมิดสิทธิในข้อมูลส่วนบุคคล กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ ได้ให้สิทธิเจ้าของข้อมูลสามารถแจ้งต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้ โดยกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐสิงคโปร์ กำหนดให้องค์กรผู้ใช้อ้างอิงให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Commission) ทราบเมื่อมีการละเมิดข้อมูลที่อาจก่อให้เกิดความกังวลหรือสร้างความเสียหาย เช่นเดียวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่น (Act on the Protection of Personal Information: APPI) ก็มีกำหนดหลักเกณฑ์ว่าต้องแจ้งเหตุละเมิดภายใน 72 ชั่วโมง เช่นเดียวกับสาธารณรัฐสิงคโปร์ โดยกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่น ได้กำหนดหลักการของการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไว้ว่า การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล จะต้องแจ้งต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และเจ้าของข้อมูลส่วนบุคคลเกี่ยวกับเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ที่มีความเสี่ยงที่จะก่อให้เกิดอันตรายต่อสิทธิและประโยชน์ของเจ้าของข้อมูลเท่านั้น ไม่ว่าจะเป็นการละเมิดข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่อ่อนไหวหรือไม่ รวมถึงการละเมิดข้อมูลซึ่งมีความเสี่ยงต่อความเสียหายทางทรัพย์สิน การละเมิดข้อมูลซึ่งน่าจะนำไปใช้ในทางที่ไม่เหมาะสม เช่น ภัยคุกคามทางไซเบอร์ เป็นต้น ทั้งนี้ ต้องแจ้งโดยไม่ชักช้าตามวิธีการที่คณะรัฐมนตรีกำหนด และคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่นมีอำนาจแก้ไขซึ่งรวมถึงการระงับละเมิดหรือดำเนินการอื่นที่จำเป็นเพื่อแก้ไขการละเมิดตลอดจนการให้คำแนะนำและคำปรึกษาอีกด้วย อีกทั้ง ในส่วนกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดา หรือ กฎหมายคุ้มครองข้อมูลส่วนบุคคลและเอกสารอิเล็กทรอนิกส์ (Personal Information Protection and Electronic Documents Act :PIPEDA) ก็ไม่ได้กำหนดหลักเกณฑ์ว่าต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง ซึ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดา ได้กำหนดหลักการของการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไว้ว่า เพียงแต่จะต้องรายงานเหตุละเมิดต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเท่านั้น

จะเห็นได้ว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศ อาทิ สาธารณรัฐสิงคโปร์ ประเทศญี่ปุ่น และประเทศแคนาดา ไม่ได้กำหนดหลักเกณฑ์ว่าต้องแจ้งเหตุละเมิดข้อมูล

ส่วนบุคคลภายใน 72 ชั่วโมง ซึ่งต่างจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย และของสหภาพยุโรป เพียงแต่ในต่างประเทศมีการกำหนดหลักเกณฑ์ในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไว้ว่า หากมีเหตุละเมิดข้อมูลส่วนบุคคลขึ้น จะต้องดำเนินการแจ้งเหตุละเมิดนั้นต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของประเทศนั้น ๆ เท่านั้น ซึ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศมีการกำหนดไว้อย่างชัดเจนว่ากรณีใดบ้างที่ต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และไม่ได้กำหนดระยะเวลาในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลที่บีบรัดมากเกินไป จึงมีความยืดหยุ่น และเหมาะสมต่อการบังคับใช้กฎหมายในปัจจุบัน มากกว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย

4.2 ปัญหากฎหมายในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

จากการศึกษาหลักเกณฑ์ในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่างประเทศ พบว่าสหภาพยุโรปได้นำ Directive 95/46/EC ขึ้นมาบังคับใช้ในกลุ่มประเทศสมาชิกของสหภาพยุโรป โดยเป็นบทบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและเสรีภาพในการเคลื่อนไหวของข้อมูล ต่อมาในปี พ.ศ. 2559 ซึ่งรัฐสภาแห่งยุโรปได้ประกาศใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับใหม่ คือ EU General Data Protection Regulation (GDPR) ซึ่งมีผลบังคับใช้แล้วเมื่อปี พ.ศ. 2561 โดยเป็นกฎหมายที่มีสาระสำคัญเกี่ยวกับการคุ้มครองสิทธิของประชาชนในกลุ่มประเทศสมาชิกสหภาพยุโรปเกี่ยวกับข้อมูลส่วนบุคคลและความเป็นส่วนตัวโดยมีหลักเกณฑ์เกี่ยวกับการใช้อำนาจนอกอาณาเขต คือ ให้ความคุ้มครองต่อข้อมูลส่วนบุคคลของประชาชนในกลุ่มประเทศสหภาพยุโรปไม่ว่าข้อมูลนั้นจะถูกรวบรวมหรือประมวลผลในพื้นที่ใดในโลก และมีการกำหนดบทลงโทษแก่ผู้ที่ก่อให้เกิดความเสียหายหรือทำให้ข้อมูลส่วนบุคคลรั่วไหล โดยต้องโทษปรับ 20 ล้านยูโร หรือปรับไม่เกินร้อยละ 4 ของรายได้ทั่วโลกของกิจการนั้น ขึ้นอยู่กับว่าจำนวนใดมากกว่า ซึ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปนี้ ถือเป็นแม่แบบในการตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลของหลายประเทศทั่วโลก

ตามที่ผู้วิจัยได้ศึกษาหลักเกณฑ์ในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สำนักงาน สกส.) ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เรื่อง การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล มาตรา 37 (4) “แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการ

ละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นที่ไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศ กำหนด” จากบทบัญญัติมาตรานี้ที่กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งเหตุการ ละเมิดข้อมูลส่วนบุคคลแก่สำนักงาน โดยไม่ชักช้าภายในเจ็ด 72 ชั่วโมงนับแต่ทราบเหตุ ละเมิดเท่าที่จะสามารถกระทำได้ ผู้วิจัยเห็นควรให้เริ่มนับระยะเวลาเมื่อผู้ควบคุมข้อมูลส่วนบุคคลได้ประเมินสถานการณ์เบื้องต้นแล้วว่าเป็นกรณีที่ต้องแจ้งสำนักงานคณะกรรมการคุ้มครอง ข้อมูลส่วนบุคคล (สคส.) และ/หรือ เจ้าของข้อมูลส่วนบุคคลหรือไม่ หากกรณีการรั่วไหลนั้นไม่ ร้ายแรง หรือไม่น่าจะเกิดผลกระทบกับเจ้าของข้อมูลส่วนบุคคล ไม่ควรต้องแจ้งสำนักงาน คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เนื่องจากไม่เกิดประโยชน์ทั้งกับเจ้าของข้อมูลส่วนบุคคล และผู้ประกอบการ นอกจากนี้ เมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคล ผู้ประกอบการต้องให้ ความสำคัญกับการรวบรวมข้อเท็จจริง จัดการแก้ไขปัญหาเบื้องต้น และระงับเหตุเป็นอันดับแรก การกำหนดให้ผู้ประกอบการต้องแจ้งเหตุละเมิดดังกล่าวให้สำนักงานคณะกรรมการคุ้มครอง ข้อมูลส่วนบุคคล (สคส.) ภายใน 72 ชั่วโมง จะทำให้เป็นอุปสรรคต่อการดำเนินการข้างต้น

อีกทั้ง เมื่อพิจารณาร่วมกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศ เกี่ยวกับการ แจ้งเหตุละเมิดข้อมูลส่วนบุคคลที่ได้ศึกษาค้นคว้าข้อมูลไว้ในบทที่ 3 นั้น พบว่าในต่างประเทศ มีการกำหนดหลักเกณฑ์ในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลที่ชัดเจน และไม่ได้กำหนด ระยะเวลาในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลที่บีบรัดมากเกินไป อาทิ กฎหมายคุ้มครองข้อมูล ส่วนบุคคลของสาธารณรัฐสิงคโปร์นั้น ไม่ได้กำหนดว่าต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ภายใน 72 ชั่วโมง ซึ่งบังคับใช้กับองค์กร บุคคล บริษัท สมาคม หรือหน่วยงานที่ดำเนินการ เกี่ยวกับข้อมูลส่วนบุคคลไม่ว่าจะเป็นองค์กรที่ตั้งขึ้นตามกฎหมายสิงคโปร์ หรือมีถิ่นที่อยู่ใน สิงคโปร์หรือไม่ ซึ่งหากมีบุคคลถูกละเมิดสิทธิในข้อมูลส่วนบุคคล และกฎหมายคุ้มครอง ข้อมูลส่วนบุคคลของประเทศสิงคโปร์ได้ให้สิทธิเจ้าของข้อมูลสามารถแจ้งต่อคณะกรรมการ คุ้มครองข้อมูลส่วนบุคคลได้ เช่นเดียวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศ ญี่ปุ่น ไม่ได้กำหนดว่าต้องแจ้งเหตุละเมิดภายใน 72 ชั่วโมง เพียงแต่กำหนดหลักเกณฑ์ไว้ว่าจะต้อง แจ้งต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และเจ้าของข้อมูลส่วนบุคคลเกี่ยวกับเหตุการ ละเมิดข้อมูลส่วนบุคคล ที่มีความเสี่ยงที่จะก่อให้เกิดอันตรายต่อสิทธิและประโยชน์ของเจ้าของ ข้อมูลเท่านั้น ไม่ว่าจะเป็นการละเมิดข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่อ่อนไหวหรือไม่ รวมถึงกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศแคนาดา ก็มีได้กำหนดว่าต้องแจ้งเหตุละเมิด ข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง ซึ่งได้กำหนดหลักการของการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ไว้ว่า จะต้องรายงานเหตุละเมิดต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเพียงเท่านั้น เป็นต้น

ในประเด็นนี้ พบว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศ ได้กำหนดหลักเกณฑ์ในการแจ้งเหตุละเมิดไว้ต่างหากจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(4) ของประเทศไทยอย่างชัดเจน ซึ่งหากมีเหตุละเมิดข้อมูลส่วนบุคคลขึ้น กฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศ อันได้แก่ สาธารณรัฐสิงคโปร์ ประเทศญี่ปุ่น และประเทศแคนาดา ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการแจ้งเหตุละเมิดนั้นต่อ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของประเศนั้น ๆ แต่การกำหนดหลักเกณฑ์ดังกล่าวมิได้ ระบุระยะเวลาในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลเหมือนดังเช่นพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(4) ของประเทศไทยจึงทำให้การดำเนินการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลตามกฎหมายของต่างประเทศข้างต้น สามารถกระทำการได้อย่างสะดวก รวดเร็ว และเหมาะสมกับการปฏิบัติตามกฎหมายมากกว่าบริบทของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(4)

ดังนั้น ผู้วิจัยจึงเห็นควรให้มีการแก้ไขพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(4) ในส่วนของการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล ไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สำนักงาน สกส.) เนื่องจากหากเป็นกรณีที่มีการรั่วไหลของข้อมูลนั้นไม่ร้ายแรง หรือไม่น่าจะเกิดผลกระทบกับเจ้าของข้อมูลส่วนบุคคล ไม่ควรต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และควรให้เริ่มนับระยะเวลาที่ต้องแจ้งเหตุการละเมิดเมื่อผู้ควบคุมข้อมูลส่วนบุคคลได้ประเมินสถานการณ์เบื้องต้นเรียบร้อยแล้วเท่านั้น เพื่อให้การบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(4) เป็นไปตามหลักการให้การออกประกาศใช้พระราชบัญญัติฉบับนี้ คือ ป้องกันการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าวทำได้โดยง่าย สะดวก และรวดเร็ว ก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวม เพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป และเพื่อให้มีความเหมาะสมกับสภาพการบังคับใช้ภายในประเทศไทย และเพื่อให้เกิดประสิทธิภาพของกฎหมายอย่างแท้จริง

4.3 ปัญหาบทลงโทษทางอาญา

จากการศึกษาวิจัยพบว่าบทลงโทษทางอาญาสำหรับผู้กระทำความผิดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(4) ในส่วนที่ 1 โทษอาญา (มาตรา 77 - มาตรา 79) การกำหนดโทษตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 79 กำหนดไว้ว่าหากผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืน โดยประเด็นที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ และในมาตรา 80 ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ถ้าผู้นั้นนำไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับนั้น

หากพิจารณาโทษทางอาญาในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคล ฝ่าฝืน หรือไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เช่น เกิดเหตุละเมิดอันเกี่ยวข้องกับข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลละเอียดอ่อน โดยที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ซึ่งการกำหนดโทษอาญาตามพระราชบัญญัตินี้ไม่เหมาะสมกับบริบทของประเทศไทย เนื่องจากลักษณะของพระราชบัญญัตินี้มีขึ้นเพื่อคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล ซึ่งการไม่ปฏิบัติตามพระราชบัญญัติฯ ดังกล่าวมีลักษณะเป็นการกระทำผิดในทางแพ่งมากกว่าการก่ออาชญากรรมที่ต้องมีโทษทางอาญา ซึ่งการกำหนดโทษทางอาญาไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยเฉพาะโทษจำคุกนั้น มีความรุนแรงเกินความจำเป็น เนื่องจากการที่ลงโทษทางอาญานั้น เป็นการลงโทษที่มีผลกระทบต่อสิทธิและเสรีภาพในชีวิต ร่างกาย และทรัพย์สินของบุคคล จึงถือเป็นที่ยอมรับโดยทั่วกันว่า โทษทางอาญาควรบังคับใช้กับการกระทำที่มีผลกระทบต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชนอย่างร้ายแรงเท่านั้น และตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีการกำหนดบทลงโทษไว้สำหรับผู้ฝ่าฝืนกฎหมาย ซึ่งมีความรับผิดชอบโทษทางอาญา เป็นกรณีการบังคับโทษสำหรับความผิดที่เกิดขึ้นจากการฝ่าฝืน หรือไม่ปฏิบัติตามหลักเกณฑ์ที่กฎหมายกำหนด บทลงโทษทางปกครองจึงเป็นมาตรการลงโทษรูปแบบหนึ่งที่มีวัตถุประสงค์เพื่อลงโทษผู้กระทำความผิด เนื่องจากฝ่าฝืน หรือไม่ปฏิบัติตามกฎหมายที่มีลักษณะคล้ายคลึงกับโทษทางอาญาด้วย การกระทำความผิดที่มีลักษณะเป็นการละเมิดหน้าที่ตามกฎหมายที่บุคคลต้องกระทำ หรือละเว้นการกระทำเพื่อประโยชน์แห่งการจัดทำบริการสาธารณะ ซึ่งลักษณะความผิดดังกล่าว ไม่มีลักษณะเป็นความชั่วร้ายหรือกระทบต่อความสงบเรียบร้อย หรือศีลธรรมอันดี

ผู้วิจัยพบว่าโทษทางอาญาในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคล ผ่าฝืน หรือไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เช่น เกิดเหตุละเมิดอันเกี่ยวเนื่องกับข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลละเอียดอ่อนโดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ซึ่งการกำหนดโทษอาญาตามพระราชบัญญัตินี้ไม่เหมาะสมกับบริบทของประเทศไทย เนื่องจากลักษณะของพระราชบัญญัตินี้ มีขึ้นเพื่อคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล ซึ่งการไม่ปฏิบัติตามพระราชบัญญัติฯ ดังกล่าวมีลักษณะเป็นการกระทำผิดในทางแพ่งมากกว่าการก่ออาชญากรรมที่ต้องมีโทษทางอาญา ซึ่งการกำหนดโทษทางอาญาไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยเฉพาะโทษจำคุกนั้น มีความรุนแรงเกินความจำเป็น เนื่องจากการที่ลงโทษทางอาญานั้น เป็นการลงโทษที่มีผลกระทบต่อสิทธิและเสรีภาพในชีวิต ร่างกาย และทรัพย์สินของบุคคล จึงถือเป็นที่ยอมรับโดยทั่วกันว่า โทษทางอาญาควรบังคับใช้กับการกระทำที่มีผลกระทบต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชนอย่างร้ายแรงเท่านั้น และจากการศึกษากฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่น (Act on the Protection of Personal Information: APPI) พบว่ามีการกำหนดโทษกรณี que ผู้ควบคุมข้อมูลส่วนบุคคลฝ่าฝืนคำสั่งของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล กฎหมายกำหนดโทษบุคคลผู้กระทำความผิด จากเดิมโทษจำคุกสูงสุดไม่เกิน 6 เดือน หรือโทษปรับสูงสุดไม่เกินสามล้านเยน และกำหนดโทษสำหรับนิติบุคคลจากเดิมโทษปรับสูงสุดไม่เกินสามล้านเยน เป็นโทษปรับสูงสุดไม่เกินหนึ่งร้อยล้านเยน (ประมาณยี่สิบเจ็ดล้านบาทไทย) หรือในกรณีที่มีการส่งข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย ก็มีการเปลี่ยนโทษปรับในส่วนของนิติบุคคลจากเดิมโทษปรับสูงสุดไม่เกินห้าล้านเยน เป็นโทษปรับสูงสุดไม่เกินหนึ่งร้อยล้านเยน จะเห็นได้ว่าแนวทางการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่น แม้จะมีการกำหนดโทษทางอาญาในกรณีมีการดำเนินการกับข้อมูลที่ไม่ถูกต้องตามกฎหมาย และสร้างกฎเกณฑ์ที่เข้มงวดมากขึ้นเพื่อให้องค์กรต่าง ๆ ซึ่งมีการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของผู้ที่อาศัยอยู่ในญี่ปุ่นต้องปฏิบัติตาม แต่ประเทศญี่ปุ่นมีการกำหนดโดยเน้นเฉพาะโทษปรับมากกว่าโทษทางอาญา ซึ่งต่างจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยอย่างสิ้นเชิง

ทั้งนี้ ลักษณะของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นี้ มีขึ้นเพื่อคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล ซึ่งการไม่ปฏิบัติตามพระราชบัญญัติฯ ดังกล่าวไม่ใช่การก่ออาชญากรรมที่ต้องมีโทษทางอาญา การกำหนดโทษทางอาญาไว้ในพระราชบัญญัติฯ นี้ โดยเฉพาะโทษจำคุกนั้น จึงมีความรุนแรงเกินความจำเป็น อีกทั้ง อาจถูกใช้เป็นช่องทางหรือเครื่องมือของผู้แสวงหาผลประโยชน์ได้ จึงควรยกเลิกโทษอาญา และกำหนดเป็นโทษปรับเป็นพินัยแทนบทลงโทษทางอาญา เนื่องจากปัจจุบันประเทศไทยได้มีการ

ตราพระราชบัญญัติว่าด้วยการปรับเป็นพินัย พ.ศ. 2565 ขึ้นบังคับใช้ซึ่งมีการกำหนดในเรื่องของค่าสินไหมทดแทนค่าปรับ มากกว่าที่จะให้เป็นโทษจำคุก ด้วยเหตุกรณีนี้เป็นเพียงการฝ่าฝืนไม่ใช่อาชกรรมร้ายแรง จะเกิดความเหมาะสมกว่าในการบังคับใช้กฎหมายมากกว่า ซึ่งปัจจุบันนานาชาติได้เริ่มปรับเปลี่ยนบทลงโทษจากความผิดอาญาเป็นมาตรการอื่นที่มีโทษอาญามากขึ้น รวมทั้งการใช้มาตรการอื่นแทนการลงโทษทางอาญา เช่น การคุมประพฤติกรณีจึงสมควรที่ประเทศไทย จะพัฒนากฎหมายไทยให้สอดคล้องกับนานาชาติ และเกิดประโยชน์แก่ประชาชนยิ่งขึ้น โดยปรับเปลี่ยน โทษอาญาบางประการที่มุ่งต่อการปรับเป็นเงินตามบัญชีท้ายพระราชบัญญัติเปลี่ยนเป็นมาตรการปรับเป็นพินัย ที่สร้างขึ้นใหม่ไม่ให้มีสภาพเป็นโทษอาญา โดยกำหนดหลักเกณฑ์ให้ใช้ดุลพินิจกำหนดค่าปรับที่ต้องชำระให้เหมาะสมกับสภาพความร้ายแรงแห่งการกระทำและฐานะทางเศรษฐกิจของผู้กระทำความผิดให้สอดคล้องกัน และในกรณีที่ผู้กระทำความผิดไม่มีเงินชำระค่าปรับ อาจขอทำงานบริการสังคมหรือทำงานสาธารณประโยชน์แทนการชำระค่าปรับได้ โดยไม่มีการกักขังแทนค่าปรับดังเช่นที่เป็นอยู่ในคดีอาญา การเปลี่ยนสภาพบังคับไม่ให้เป็นโทษอาญาโดยกำหนดวิธีการดำเนินการขึ้นใหม่เป็นการเฉพาะนี้ ย่อมจะช่วยทำให้ประชาชนที่ถูกกล่าวหาว่ากระทำความผิดไม่ต้องเข้าสู่กระบวนการทางอาญา และไม่มีประวัติอาชญากรรมติดตัวอีกต่อไป การเปลี่ยนแปลงเช่นนี้จะเป็นกลไกทางกฎหมายเพื่อสร้างความเป็นธรรมและขจัดความเหลื่อมล้ำทางสังคม และส่งเสริมการบังคับใช้กฎหมายให้มีประสิทธิภาพยิ่งขึ้น ดังนั้น จึงควรยกเลิกโทษอาญา และให้กำหนดเป็นโทษปรับเป็นพินัยตามพระราชบัญญัติว่าด้วยการปรับเป็นพินัย พ.ศ. 2565 แทนบทลงโทษทางอาญา ย่อมมีความเหมาะสมมากกว่า ซึ่งประกอบด้วยเหตุผลดังต่อไปนี้

1) ควรกำหนดมาตรการในการลงโทษตามการจำแนกประเภทของข้อมูลอย่างเหมาะสม โดยเฉพาะอย่างยิ่งข้อมูลที่มีความละเอียดอ่อนให้รับการคุ้มครองข้อมูลส่วนบุคคลพิเศษ เฉพาะเพื่อมุ่งเน้นมาตรการด้านการรักษาความมั่นคงปลอดภัยและมีประสิทธิภาพยิ่งขึ้น รวมทั้งความระมัดระวังในการประมวลผล การเก็บ รวบรวมเปิดเผย ใช้ ลบ หรือ ทำลายซึ่งเป็นข้อมูลส่วนบุคคลที่สามารถบ่งชี้เอกลักษณ์เฉพาะของบุคคลได้นั้น ซึ่งมีความแตกต่างจากข้อมูลทั่วไป เพื่อให้มีความสอดคล้องกับเศรษฐกิจหรือวิถีปฏิบัติตามกรอบมาตรฐานของสากลยอมรับเท่าที่จะเป็นไปได้ โดยหากเป็นข้อมูลส่วนบุคคลที่มีผลกระทบต่อเศรษฐกิจและสังคมส่วนรวมควรเป็นโทษเด็ดขาด กล่าวคือ นำโทษทางอาญามาปรับใช้โดยให้มีเฉพาะ โทษปรับ

2) แม้บทลงโทษทางอาญา จำคุกไม่เกิน 1 ปีและปรับ แต่อย่างไรก็ดี ประเทศไทยยังไม่มีกำหนดฐานความผิดในกรณีที่มีการล่วงละเมิดข้อมูลส่วนบุคคลอันมีพฤติการณ์

ประกอบการกระทำในลักษณะการชักชวนการลงทุนหรือการพัฒนาสังคมและเศรษฐกิจ เพื่อให้การลงโทษมีประสิทธิภาพ

3) แม้มีบทลงโทษในการละเมิดต่อผู้อื่นซึ่งเป็นบทลงโทษทางแพ่ง แต่ไม่สอดคล้องกับหลัก GDPR ตาม Article 83 ของ Regulation (EU) 2018/1725 ซึ่งควรมีบทลงโทษที่หนักสำหรับผู้ควบคุมและผู้ประมวลผลข้อมูลส่วนบุคคลให้สูงกว่าความรับผิดของบุคคลธรรมดาโดยนำโทษปรับมาใช้ มิใช่เพียงเฉพาะในกรณีที่มีความเสียหายเกิดขึ้นเท่านั้นแต่จำนวนความรับผิดตามโทษปรับควรมีจำนวนที่เพิ่มขึ้นตามการกระทำนั้นว่าเป็นการกระทำในระดับโทษรุนแรง หรือระดับโทษรุนแรงมาก โดยพิจารณาถึงความจงใจหรือประมาทสำหรับผู้ควบคุมและผู้ประมวลผลข้อมูลส่วนบุคคล

4) เมื่อเปรียบเทียบกับกฎหมาย GDPR พบว่า มาตรการลงโทษทางอาญาตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เฉพาะโทษจำคุกอาจจะเป็นการผลักดันให้ผู้ประกอบการธุรกิจต้องตกอยู่ภายใต้ความเสี่ยงที่จะรับโทษอาญาซึ่งไม่สอดคล้องกับยุคดิจิทัลที่ผู้ประกอบการธุรกิจมีอยู่ทั่วโลก จึงควรเน้นให้มีการกำหนดบทลงโทษทางปกครองแก่การกระทำ ความผิดตามพระราชบัญญัตินี้เพิ่มขึ้นแทนโทษทางอาญา

5) การเก็บ การใช้หรือการเปิดเผยลับหรือทำลายข้อมูลส่วนบุคคลต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อน โดยมีการแจ้งวัตถุประสงค์ในการเก็บ ใช้ เผยอย่างชัดเจน และต้องทำเท่าที่จำเป็นที่ให้ความยินยอมไว้ โดยมีการกำหนดหน้าที่ของผู้ควบคุมและผู้ประมวลผล ข้อมูลส่วนบุคคลในการจัดมาตรการรักษาความปลอดภัยและบันทึกข้อมูลส่วนบุคคล โดยการกำหนดมาตรฐานในการโอนย้ายข้อมูลไปต่างประเทศ รวมถึงการเพิ่มสิทธิของเจ้าของข้อมูลส่วนบุคคลในการโต้แย้งระงับการใช้ข้อมูลหากฝ่าฝืนจะต้องมีโทษทางอาญาซึ่งกำหนดเฉพาะโทษปรับเท่านั้น