แนวทางการแก้ไขปัญหาและการป้องกันการละเมิดข้อมูลส่วนบุคคลเพื่อการปฏิรูปประเทศไทยสู่ดิจิทัลไทยแลนด์

โดย

นายปรนนท์ ฐิตะวรรโณ
กรรมการบริหารสภาอุตสาหกรรมแห่งประเทศไทย
กระทรวงอุตสาหกรรม

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ 65
ประจำปีการศึกษา พุทธศักราช 2565 - 2566

หนังสือรับรอง

วิทยาลัยป้องกันราชอาณาจักร สถาบันวิชาการป้องกันประเทศ ได้อนุมัติให้เอกสารวิจัยส่วนบุคคล เรื่อง “แนวทางการแก้ไขปัญหาและการป้องกันการละเมิดข้อมูลส่วนบุคคลเพื่อการปฏิรูปประเทศไทยสู่ดิจิทัลไทยแลนด์” ลักษณะวิชา ยุทธศาสตร์ ของ นายปรนนท์ ฐิตะวรรโณ เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรการป้องกันราชอาณาจักร รุ่นที่ 65 ประจำปีการศึกษา พุทธศักราช 2565 - 2566

พลโท

(ชาติชาย ชัยเกษม)
ผู้อำนวยการวิทยาลัยป้องกันราชอาณาจักร
สถาบันวิชาการป้องกันประเทศ

บทคัดย่อ

เรื่อง แนวทางการแก้ไขปัญหาและการป้องกันการละเมิดข้อมูลส่วนบุคคลในการพัฒนาประเทศสู่ดิจิทัลไทยแลนด์

ลักษณะวิชา ยุทธศาสตร์

ผู้วิจัย นายปรนนท์ ฐิตะวรรโณ **หลักสูตร** วปอ. **รุ่นที่** 65

งานวิจัยเชิงคุณภาพนี้มีวัตถุประสงค์ดังนี้ 1. เพื่อศึกษาสถานการณ์และแนวโน้มการละเมิดข้อมูลส่วนบุคคลผ่านระบบดิจิทัลและผลกระทบต่อการพัฒนาประเทศ 2. เพื่อศึกษาปัญหาและอุปสรรคในการดำเนินการแก้ไขปัญหาและผลกระทบการละเมิดข้อมูลส่วนบุคคลผ่านเทคโนโลยีดิจิทัล 3. เพื่อศึกษาแนวทางการแก้ไขปัญหาและการป้องกันการละเมิดข้อมูลส่วนบุคคลในการพัฒนาประเทศสู่ดิจิทัลไทยแลนด์

จากผลการวิจัยผู้วิจัยเสนอแนะว่าจากการที่ประเทศไทยได้มีการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ PDPA เพื่อเป็นกฎหมายกลางในการคุ้มครองข้อมูลส่วนบุคคลของประชาชนทั่วไป แต่ด้วยกฎหมายฉบับนี้เป็นกฎหมายใหม่ ทุกหน่วยงานทั้งภาครัฐและภาคเอกชนจึงต้องมีการเตรียมพร้อมรับกฎหมายฉบับนี้ และจัดทำแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลให้ได้มาตรฐานสากลและเพื่อให้สอดคล้องกับหลักการของกฎหมายฉบับนี้ ทั้งนี้ภาครัฐต้องมีการทบทวนและประเมินผลการใช้กฎหมาย PDPA เพื่อให้กฎหมายฉบับนี้มีความชัดเจนมากขึ้นในบางมาตราที่มีปัญหา รวมถึงภาครัฐต้องมีการประชาสัมพันธ์และให้ความรู้เกี่ยวกับกฎหมาย PDPA ในการคุ้มครองข้อมูลส่วนบุคคลให้แก่ประชาชนรับรู้อย่างต่อเนื่อง

Abstract

Title Guidelines for solving problems and preventing personal data breach in development country to digital Thailand

Field Strategy

Name Mr. Paranont Thitawanno **Course** NDC **Class** 65

This qualitative research had the objectives as follows; 1. To study the situation and trends of personal data breaches through digital systems and their impact on national development. 2. To study problems and obstacles in solving problems and the impact of personal data breaches through digital technology. 3. To study solutions and prevention of personal data breaches in developing the country towards digital Thailand. The method used in this research was the content analysis from the in-depth interview and academic papers. From the research results, the researcher suggested that Thailand has enacted the Personal Data Protection Act B.E. 2562 or PDPA to be a central law for protection of personal information of the general public. This law is a new law all agencies, both government and private sectors, must prepare to accept this law and develop personal data protection practices to meet international standards and to comply with the principles of this law. However, the government sector needs to review and evaluate the implementation of the PDPA law in order to make this law clearer on some problematic sections. The government sector must publicize and provide knowledge about the PDPA law in protecting personal data to the public continuously.

คำนำ

การวิจัยเรื่องแนวทางการแก้ไขปัญหาและการป้องกันการละเมิดข้อมูลส่วนบุคคลในการพัฒนาประเทศสู่ดิจิทัลไทยแลนด์ มีวัตถุประสงค์ดังนี้ 1. เพื่อศึกษาสถานการณ์และแนวโน้มการละเมิดข้อมูลส่วนบุคคลผ่านระบบดิจิทัลและผลกระทบต่อการพัฒนาประเทศ 2. เพื่อศึกษาปัญหาและอุปสรรคในการดำเนินการแก้ไขปัญหาและผลกระทบการละเมิดข้อมูลส่วนบุคคลผ่านเทคโนโลยีดิจิทัล และ 3. เพื่อศึกษาแนวทางการแก้ไขปัญหาและการป้องกันการละเมิดข้อมูลส่วนบุคคลในการพัฒนาประเทศสู่ดิจิทัลไทยแลนด์

ผลของการวิจัยนี้จะทำให้ทราบถึงสถานการณ์และแนวโน้มการละเมิดข้อมูลส่วนบุคคลผ่านระบบดิจิทัลและผลกระทบต่อการพัฒนาประเทศ ปัญหาและอุปสรรคในการดำเนินการแก้ไขปัญหาและผลกระทบการละเมิดข้อมูลส่วนบุคคลผ่านเทคโนโลยีดิจิทัล เพื่อนำไปวิเคราะห์และสังเคราะห์แนวทางการแก้ไขปัญหาและการป้องกันการละเมิดข้อมูลส่วนบุคคลในการพัฒนาประเทศสู่ดิจิทัลไทยแลนด์เสนอต่อหน่วยงานที่เกี่ยวข้องในการนำไปประยุกต์ใช้เพื่อเป็นประโยชน์ต่อไป

งานวิจัยฉบับนี้สำเร็จลงได้ด้วยความอนุเคราะห์จากผู้ให้ข้อมูลหลักหลายท่าน จึงขอขอบพระคุณมา ณ โอกาสนี้ และขอขอบพระคุณคณาจารย์วิทยาลัยป้องกันราชอาณาจักรทุกท่านที่ได้กรุณาให้คำแนะนำที่สำคัญด้วยดีตลอดมา ผู้วิจัยหวังเป็นอย่างยิ่งว่างานวิจัยฉบับนี้จะก่อให้เกิดประโยชน์ต่อผู้มีส่วนเกี่ยวข้องในการเสริมสร้างวัฒนธรรมทางการเมืองในระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขให้เยาวชนไทยไม่มากก็น้อย

(นายปรนนท์ ฐิตะวรรโณ)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร วปอ. รุ่นที่ 65
ผู้วิจัย

สารบัญ

สารบัญ (ต่อ)

หน้า

สารบัญแผนภาพ

หน้า

แผนภาพที่

บทที่ 1
บทนำ

ความเป็นมาและความสำคัญของปัญหา

ตามที่ประเทศไทยได้มีการปฏิรูปสู่สังคมดิจิทัลหรือดิจิทัลไทยแลนด์ตามนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมที่เป็นแผนหลักในการพัฒนาเศรษฐกิจและสังคมดิจิทัลของประเทศไทยระยะ 20 ปี (พ.ศ.2561-2580) รัฐบาลให้ความสำคัญในการนำเทคโนโลยีดิจิทัลมาช่วยในการขับเคลื่อนเศรษฐกิจและสังคม ทั้งการพัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูงให้ครอบคลุมทั่วประเทศ การขับเคลื่อนเศรษฐกิจด้วยเทคโนโลยีดิจิทัล การปรับเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัล ส่งผลให้เกิดการนำเทคโนโลยีไปใช้ในการดำเนินกิจการของทุกภาคส่วน เพิ่มประสิทธิภาพในการดำเนินงาน เพิ่มความสามารถในการแข่งขันทางการค้า การอำนวยความสะดวกและยกคุณภาพชีวิตให้ประชาชนและมีการผลักดันให้เกิดการเปลี่ยนแปลงรูปแบบการทำธุรกรรมจากระบบกระดาษเป็นระบบดิจิทัล จากรายงานการศึกษา Thailand Digital Outlook 2564 ของสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.) (2564) ที่ได้กล่าวถึงการประเมินการพัฒนาดิจิทัลชองประเทศไทย 8 มิติ ได้แก่ มิติการเข้าถึง (Access) มิติการใช้งาน (Use) มิตินวัตกรรม (Inovation) มิติงาน (Jobs) มิติความน่าเชื่อถือ (Trust) มิติสังคม (Society) มิติการเปิดการค้าเสรี (Market Openness) และมิติการเติบโตและสภาพความเป็นอยู่ (Growth & Wellbeing)

รายงานดังกล่าวสามารถชี้ให้เห็นว่า ประเทศไทยมีการพัฒนาด้านดิจิทัลที่มีแนวโน้มเพิ่มขึ้นทุกมิติในทุกภาคส่วนทั้งระดับบุคคล หน่วยงานเอกชนและหน่วยงานของรัฐ โดยการเข้าถึงมีสัดส่วนของผู้ใช้บริการอินเทอร์เน็ตบรอดแบนด์ประจำที่และแบบเคลื่อนที่มีแนวโน้มเพิ่มขึ้น สัดส่วนจำนวนผู้ใช้งานเทคโนโลยีดิจิทัลหรือมิติการใช้งานมีจำนวนเพิ่มมากขึ้นในทุกภาคส่วน ในด้านการพัฒนาดิจิทัลของประเทศไทยในมิตินวัตกรรมพบว่าเมื่อปี พ.ศ.2562 มีมูลค่าการลงทุนด้านเทคโนโลยีสารสนเทศและดิจิทัลของประเทศไทย มีมูลค่า 316.5 พันล้านบาท หรือคิดเป็นร้อยละ 2.02 ต่อผลิตภัณฑ์มวลรวมรายได้ประชาชาติ อีกทั้งยังพบว่ามีการเพิ่มค่าใช้จ่ายในด้านการวิจัยและพัฒนามากขึ้น ในมิติอาชีพพบว่ามีเจ้าหน้าที่และผู้ทำงานในอุตสาหกรรมที่เกี่ยวข้องกับเทคโนโลยีดิจิทัลในหลากหลายกลุ่มและหลากหลายระดับทักษะความสามารถในปี พ.ศ. 2563 มีจำนวนกำลังแรงงานที่มีงานทำทั้งหมด 37,680,000 คน และมีจำนวนกำลังแรงงานที่มีการใช้เทคโนโลยีดิจิทัลในระดับปานกลางค่อนข้างสูงจนถึงระดับสูงอยู่ที่ 10,235,500 คน คิดเป็นสัดส่วนร้อยละ 27.2 ของจำนวนแรงงานที่มีงานทำทั้งหมด ในด้านมิติสังคมพบว่ามีผู้ใช้เทคโนโลยีดิจิทัลในแต่ละช่วงวัย ทั้งเพศหญิงและเพศชาย ในส่วนภาครัฐก็มีการนำเทคโนโลยีมาใช้เพื่อบริการประชาชนและเพิ่มประสิทธิภาพของหน่วยงานมากขึ้น ในมิติความน่าเชื่อถือในด้านความปลอดภัยทางสารสนเทศ การรักษาข้อมูลส่วนบุคคล และปัญหาภัยคุกคามทางไซเบอร์ ซึ่งมีปริมาณเพิ่มมากขึ้นทุกวันและกำลังเป็นปัญหาและ

อุปสรรคต่อการพัฒนาเศรษฐกิจและสังคมดิจิทัลเป็นอย่างมาก ทำให้เกิดความไม่เชื่อมั่นในการใช้งานเทคโนโลยีในการทำธุรกรรมต่าง ๆ ในปัจจุบัน เนื่องจากในปัจจุบันนี้หน่วยงานภาครัฐมีการเก็บข้อมูลส่วนบุคคลของประชาชนไว้ เช่น ชื่อ นามสกุล ที่อยู่ตามทะเบียนราษฎร์ เลขบัตรประชาชน เบอร์โทรศัพท์ รวมทั้งการเก็บข้อมูลสุขภาพของประชาชน (Data Set) ในรูปแบบดิจิทัล เพื่อให้เกิดความสะดวกในการนำไปใช้และการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานที่เกี่ยวข้องได้ ตัวอย่างเช่น กระทรวงสาธารณสุขและสถานพยาบาลต่าง ๆ มีการเก็บข้อมูลด้านสุขภาพของประชาชนและสถิติที่เกี่ยวข้องไว้ที่ส่วนกลาง Health Data Center (HDC) ซึ่งถ้ามีการรั่วไหลของข้อมูลก็จะเป็นปัญหาได้ เพราะเป็นข้อมูลที่มีความอ่อนไหว นอกจากนั้นยังมีประเด็นที่สำคัญตามมาคือด้านการรักษาความมั่งคงปลอดภัย และการจัดการข้อมูลส่วนบุคคล ในมิติการเปิดการค้าเสรีมีการบริการและจัดจำหน่ายสินค้าผ่านช่องทางออนไลน์มากขึ้นสร้างโอกาสให้กับผู้ประกอบการ อำนวยความสะดวกทั้งผู้ซื้อและผู้ขาย อีกทั้งยังเพิ่มช่องทางในการดำเนินธุรกิจทั้งในประเทศและต่างประเทศ มิติการเติบโตและสภาพความเป็นอยู่พบว่าอัตราการเติบโตเฉลี่ยต่อปีของมูลค่าเพิ่มในภาคธุรกิจดิจิทัลนั้น จากรายงานการศึกษาช่วงปี พ.ศ.2559-2562 มีอัตราการเพิ่มขึ้นของผลิตภัณฑ์มวลรวมประชาชาติที่แท้จริงแบบลูกโซ่เฉพาะธุรกิจดิจิทัล อยู่ที่ 279,000 ล้านบาท แต่อย่างไรก็ตามจากรายงานยังพบผู้ที่ประสบปัญหาถูกละเมิดข้อมูลส่วนบุคคลอยู่ที่ร้อยละ 6.3 ซึ่งเป็นอุปสรรคในการพัฒนาเทคโนโลยีดิจิทัลของประเทศเป็นอย่างมาก ส่งผลให้ผู้ใช้งานในทุกภาคส่วนเกิดความไม่เชื่อมั่น ความท้าทายในการส่งเสริมให้มีการใช้เทคโนโลยีดิจิทัลในการดำเนินธุรกรรมต่าง ๆ ปรับเปลี่ยนข้อมูลจากรูปแบบเอกสารกระดาษเป็นข้อมูลดิจิทัล การส่งเสริมให้เกิดการให้บริการและซื้อขายผ่านออนไลน์ การจัดเก็บข้อมูลในรูปแบบดิจิทัลเพื่อให้เกิดการแลกเปลี่ยนและนำไปใช้ระหว่างหน่วยงานที่เกี่ยวข้อง ในด้านภัยคุกคามทางไซเบอร์นั้นจะพบว่ามีการละเมิดหรือการดำเนินการเพื่อวัตถุประสงค์เพื่อทำลายระบบหรือโจรกรรมข้อมูล หรือการหวังผลทางการเงิน หรือเพื่อวัตถุประสงค์อื่นที่ไม่สอดคล้องกับการพัฒนาเทคโนโลยีสารสนเทศและดิจิทัล โดยอาจจะเกิดจากการดำเนินการของผู้ไม่หวังดี (Hacker) หรืออาจจะเกิดจากการปฏิบัติที่ไม่ถูกต้อง รู้เท่าไม่ถึงการณ์ การประมาท ส่งผลให้เกิดความเสียหายทั้งต่อองค์กรและส่วนบุคคล หรือในหลายกรณีส่งผลต่อข้อมูลประชาชนจำนวนมาก ส่งผลให้ผู้ใช้งานเกิดความไม่เชื่อมั่นต่อเทคโนโลยีดิจิทัลเป็นอุปสรรคต่อการพัฒนาประเทศเป็นอย่างยิ่ง ที่ผ่านมาเกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคลขึ้นจำนวนมากทั้งในประเทศและต่างประเทศ หากศึกษาแนวโน้มการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในต่างประเทศ เช่น ในรายงานประจำปีของหน่วยงานกำกับดูแลของฝรั่งเศส พบว่า ในปี พ.ศ. 2564 ที่ผ่านมา มีการแจ้งเหตุละเมิด (Data Breach Notification) มายังหน่วยงานด้านกำกับดูแลถึง 5,000 เรื่อง โดยสาเหตุจำนวนมากมาจากการถูกโจมตีจากมัลแวร์ประเภทเรียกค่าไถ่ หรือ Ransomware Attack นอกจากเหตุละเมิดที่เกิดจากการถูกเจาะระบบแล้ว ยังมีเหตุละเมิดอื่น ๆ เช่น ความผิดพลาดจากการลบข้อมูลโดยไม่ตั้งใจแต่ไม่มีการสำรองข้อมูลเก็บไว้ทำให้ข้อมูลของผู้ใช้งานและลูกค้าไม่พร้อมใช้งาน และการเก็บข้อมูลส่วนบุคคลไว้ที่อุปกรณ์จัดเก็บข้อมูล แต่ไม่ได้ทำการเข้ารหัสข้อมูลไว้

ดังนั้นมาตรการลงโทษทางปกครองโดยหน่วยงานกำกับดูแลครึ่งหนึ่งเป็นผลมาจากการไม่ปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยและธุรกิจประกันภัยก็เป็นหนึ่งในกลุ่มธุรกิจที่ได้รับผลกระทบค่อนข้างมาก หรือกรณีศึกษาจากประเทศไอร์แลนด์ ซึ่งมีบริษัทด้านเทคโนโลยีดิจิทัล

ขนาดใหญ่ตั้งสำนักงานใหญ่อยู่จำนวนมาก พบว่า ปี พ.ศ. 2564 ที่มีการแจ้งเหตุละเมิด Data Breach มายังหน่วยงานกำกับดูแลในปริมาณมากเช่นกัน โดยกว่า 70 % เป็นเรื่องการเปิดเผยข้อมูลไม่ถูกต้อง เนื่องจากกระบวนการควบคุมการใช้ข้อมูลภายในองค์กรไม่รัดกุมหรือไม่เป็นไปตามแนวปฏิบัติที่กำหนดไว้ รวมทั้งเกิดความผิดพลาดจากพนักงานหรือผู้เกี่ยวข้องในองค์กร เป็นส่วนใหญ่จากกรณีศึกษาทั้งสองประเทศนอกจากการเน้นเรื่องการสร้างความรู้ความเข้าใจให้กับผู้ประกอบการในด้านข้อควรปฏิบัติ ระเบียบข้อบังคับ และข้อกฎหมายที่เกี่ยวข้องกับการเก็บรวบรวมและการใช้ ข้อมูลส่วนบุคคลอย่างถูกต้องแล้ว อีกประเด็นสำคัญที่ต้องเร่งให้ความรู้กับผู้ประกอบการคือ การรักษาความ มั่นคงปลอดภัยของข้อมูลส่วนบุคคลหรือ Security Safeguards ทั้งในแง่ของการกำหนดมาตรการเชิงองค์กร (Organizational Measure) ให้มีการจัดโครงสร้างองค์กร กำหนดบทบาทหน้าที่รับผิดชอบในด้าน Security และ Privacy ให้ชัดเจน และต้องมีมาตรการเชิงเทคนิค (Technical Measure) เพื่อป้องกันการเข้าถึง การใช้การเปลี่ยนแปลงและแก้ไข การลบข้อมูลหรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบด้วย ในส่วนของไทย ตั้งแต่ 1 มิถุนายน พ.ศ. 2565 ที่ผ่านมามีองค์กรแจ้งเหตุละเมิด โดยทำเป็นหนังสือและส่งมาที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ทั้งหน่วยงานของรัฐและหน่วยงานเอกชน โดยมีการละเมิดที่ได้รับแจ้งมีทั้งกรณี Cyber และ Non-cyber โดยสาเหตุส่วนใหญ่สอดคล้องกับกรณีศึกษาของฝรั่งเศสและไอร์แลนด์คือระบบคอมพิวเตอร์ขององค์กรถูกเจาะระบบ กระบวนการควบคุมขั้นตอนการเปิดเผยข้อมูลส่วนบุคคลขององค์กรไม่รัดกุม พนักงานดำเนินการผิดพลาด ส่งข้อมูลให้ผู้รับผิดคน

ในปัจจุบันด้วยความเจริญของเทคโนโลยีทำให้การติดต่อสื่อสารสามารถเดินทางติดต่อสื่อสารถึงกันได้ทั่วทุกมุมของโลกอย่างไร้ขีดจำกัด ข้อมูลข่าวสารจึงมีความจำเป็นสำหรับมนุษย์ในการดำรงชีวิตผ่านรูปแบบและกระบวนการที่หลากหลายทั้งจากกระบวนการคิด การเรียนรู้ การประมวลผล และมีความสำคัญต่อการวางแผนการทำงาน การดำเนินกิจกรรมต่าง ๆ ทั้งของภาครัฐและภาคเอกชน ทำให้เกิดปัญหาติดตามมาคือการแย่งชิงกันครอบครองข้อมูล เพื่อให้มีข้อมูลมาใช้ประโยชน์ในกิจการของตนเองให้มากที่สุดเพื่อการมีโอกาสและมีอิทธิพลอำนาจเหนือกว่าผู้อื่น ซึ่งข้อมูลเหล่านี้จะมีข้อมูลข่าวสารส่วนหนึ่งที่เป็นข้อมูลส่วนบุคคลรวมอยู่ด้วย จึงทำให้เกิดปัญหาตามมาคือมีการนำข้อมูลส่วนบุคคลไปใช้โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล ทำให้เกิดปัญหาการละเมิดความเป็นส่วนตัวในข้อมูลส่วนบุคคลเป็นวงกว้างอยู่ในขณะนี้และเนื่องจากการพัฒนาด้านเทคโนโลยีสารสนเทศเติบโตอย่างรวดเร็ว ทำให้สามารถจัดเก็บรวบรวม ข้อมูลข่าวสารต่าง ๆ ได้เป็นจำนวนมากและสามารถเรียกดู ตรวจสอบ วิเคราะห์ ประมวลผล เผยแพร่รับ–ส่ง แลกเปลี่ยนข้อมูลได้อย่างสะดวกและรวดเร็ว ให้เกิดผลกระทบต่อความเป็นส่วนตัวคือ การนำข้อมูลส่วนบุคคลไปใช้ประมวลผลหรือเปิดเผยทำให้ผู้เป็นเจ้าของข้อมูลอาจได้รับความเสียหาย เช่นเรื่องของความปลอดภัยในชีวิต สิทธิและเสรีภาพของบุคคลของเจ้าของข้อมูล สำหรับประเทศไทยได้มีการบัญญัติให้การรับรองและคุ้มครองสิทธิส่วน บุคคลและข้อมูลส่วนบุคคล ไว้ในรัฐธรรมนูญแห่งราชอาณาจักรไทยมาตั้งแต่อดีตที่ผ่านมาจนถึงปัจจุบัน โดย รับรองไว้อย่างชัดเจน เป็นครั้งแรกในรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2534 มาตรา 44 ซึ่ง บัญญัติว่า “สิทธิของบุคคลในครอบครัวเกียรติยศหรือชื่อเสียงและความเป็นอยู่ส่วนตัวย่อมได้รับความ คุ้มครอง” รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540 บัญญัติไว้มาตรา 34 รัฐธรรมนูญแห่ง ราชอาณาจักรไทย

พุทธศักราช 2550 บัญญัติไว้ในมาตรา 35 และปัจจุบันภายใต้ รัฐธรรมนูญแห่ง ราชอาณาจักรไทย พุทธศักราช 2560 ก็บัญญัติไว้ในมาตรา 32 ให้การรับรองและคุ้มครองสิทธิส่วนบุคคลและ ข้อมูลส่วนบุคคลเช่นเดียวกัน ซึ่งปัจจุบันประเทศไทยมีกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล โดยเฉพาะคือพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act :PDPA)ทั้งนี้ได้เริ่มบังคับใช้ตั้งแต่ในวันที่ 1 มิถุนายน 2565

จากแผนการพัฒนาประเทศเพื่อเกิดการนำเทคโนโลยีดิจิทัลมาใช้ในทุกมิติ สอดคล้องกับการพัฒนาประเทศตามแผนหลักในการพัฒนาเศรษฐกิจและสังคมดิจิทัลของประเทศไทย ระยะ 20 ปี (พ.ศ.2561–2580) จำเป็นอย่างยิ่งที่จะต้องสร้างความเชื่อมั่นกับทุกภาคส่วน จนประเทศไทยมีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งได้มีผลบังคับใช้เมื่อวันที่ 1 มิถุนายน 2565 โดยมีวัตถุประสงค์ส่งเสริมและสนับสนุนให้เกิดการพัฒนาด้านการคุ้มครองข้อมูลส่วนบุคคลของประเทศ มีการพัฒนาหลักเกณฑ์ มาตรฐาน และวิธีการกำกับดูแลเกี่ยวกับการใช้ข้อมูลส่วนบุคคลให้เป็นไปอย่างถูกต้อง โดยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีลักษณะเป็นกฎหมายกลาง ที่ครอบคลุมการดำเนินการของบุคคลหรือนิติบุคคลที่เป็นหน่วยงานภาครัฐและภาคเอกชนที่ทำการเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคลต้องปฏิบัติตามหลักเกณฑ์ วิธีการและเงื่อนไขตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดส่งผลทำให้ทุกภาคส่วนทั้งประชาชนทั่วไป บริษัทเอกชนและหน่วยงานภาครัฐต่าง ๆ ต้องมีความเข้าใจต่อกฎหมายอย่างถูกต้อง เข้าใจวิธีการดูแลเรื่องความปลอดภัยข้อมูลส่วนบุคคลและการปฏิบัติตามหลักเกณฑ์ข้อกำหนดที่ถูกต้อง แต่อย่างไรก็ตามในการดำเนินการด้านการจัดการข้อมูลส่วนบุคคลยังต้องอาศัยแนวทางอีกหลายด้านเพื่อแก้ไขปัญหาและการป้องกันการละเมิดข้อมูลส่วนบุคคลเพื่อการปฏิรูปประเทศสู่ดิจิทัลไทยแลนด์ ด้วยเหตุผลที่กล่าวมาผู้วิจัยจึงมีความสนใจในการศึกษาสถานการณ์และแนวโน้มการละเมิดข้อมูลส่วนบุคคลผ่านระบบดิจิทัลและผลกระทบต่อการพัฒนาประเทศ ปัญหาและอุปสรรคในการดำเนินการแก้ไขปัญหาและผลกระทบการละเมิดข้อมูลส่วนบุคคลผ่านเทคโนโลยีดิจิทัล รวมทั้งเพื่อนำเสนอแนวทางการแก้ไขปัญหาและการป้องกันการละเมิดข้อมูลส่วนบุคคลในการพัฒนาประเทศสู่ดิจิทัลไทยแลนด์เพื่อเป็นประโยชน์ต่อหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและภาคเอกชนต่อไปในการนำไปประยุกต์ใช้

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาสถานการณ์และแนวโน้มการละเมิดข้อมูลส่วนบุคคลผ่านระบบดิจิทัลและผลกระทบต่อการพัฒนาประเทศ

2. เพื่อศึกษาปัญหาและอุปสรรคในการดำเนินการแก้ไขปัญหาและผลกระทบการละเมิดข้อมูลส่วนบุคคลผ่านเทคโนโลยีดิจิทัล

3. เพื่อศึกษาแนวทางการแก้ไขปัญหาและการป้องกันการละเมิดข้อมูลส่วนบุคคลในการพัฒนาประเทศสู่ดิจิทัลไทยแลนด์

ขอบเขตของการวิจัย

1. ขอบเขตด้านเนื้อหา

การวิจัยนี้เน้นการศึกษาหาแนวทางการแก้ไขปัญหาและการป้องกันเหตุละเมิดข้อมูลส่วนบุคคลทั้งเชิงรับและเชิงรุกที่เหมาะสมในภาพรวมของประเทศไม่ได้เจาะจงเฉพาะหน่วยงานใดหน่วยงานหนึ่ง โดยประกอบด้วย

1.1 การศึกษาสถานการณ์การคุ้มครองข้อมูลและการละเมิดข้อมูลส่วนบุคคลของทั้งภาครัฐและภาคเอกชน

1.2 การวิเคราะห์ปัญหา อุปสรรค ผลกระทบการละเมิดข้อมูลบุคคลที่มีผลต่อการพัฒนาดิจิทัลในประเทศไทย

2. ขอบเขตด้านประชากร

เป้าหมายการศึกษาวิจัยในครั้งนี้คือทุกภาคส่วน โดยภาคประชาชนจะเป็นทั้งเจ้าของข้อมูลและผู้จัดเก็บข้อมูล ในส่วนของภาคเอกชนเป็นเรื่องการจัดเก็บและการนำข้อมูลไปใช้งานตามวัตถุประสงค์ของเจ้าของข้อมูล ในส่วนของภาครัฐและภาคเอกชน เป็นเรื่องการเป็นผู้ทำหน้าที่คุ้มครองข้อมูลส่วนบุคคล การจัดเก็บ การนำข้อมูลไปใช้งานและกฎระเบียบที่เกี่ยวข้อง รวมไปถึงระบบที่ใช้ในการดำเนินการจัดการข้อมูลส่วนบุคคลในปัจจุบันและอนาคต

3. ขอบเขตด้านเวลา

การศึกษาวิจัยเริ่มตั้งแต่วันที่ 1 ตุลาคม 2565 จนถึงวันที่ 31 พฤษภาคม 2566

วิธีดำเนินการวิจัย

1. รูปแบบการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) โดยมีการรวบรวมข้อมูลนำมาวิเคราะห์เนื้อหา (Content Analysis)

2. การรวบรวมข้อมูล

2.1 ข้อมูลปฐมภูมิ การเก็บข้อมูลภาคสนามโดยการทำเก็บข้อมูล รวบรวมข้อมูลจากการประชุม สัมภาษณ์ผู้ที่เกี่ยวข้องทั้งระดับนโยบาย ผู้ใช้งาน ผู้จัดเก็บข้อมูล และผู้ใช้ข้อมูล จากหน่วยงานภาครัฐ ภาคเอกชน และภาคประชาชน

2.2 ข้อมูลทุติยภูมิ ทำการศึกษาเอกสารและงานวิจัยที่เกี่ยวข้อง

3. การวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลจะดำเนินการจากข้อมูลการศึกษาเอกสารที่เกี่ยวข้องและข้อมูลที่ได้จากภาคสนามนำมาวิเคราะห์เนื้อหา (Content Analysis) ตามวัตถุประสงค์ที่กำหนดไว้และดำเนินการตามกรอบแนวคิดของการวิจัยในครั้งนี้เพื่อสร้างแนวทางการแก้ไขปัญหาและการป้องกันการละเมิดข้อมูลส่วนบุคคลเพื่อการปฏิรูปประเทศไทยสู่ดิจิทัลไทยแลนด์

4. การนำเสนอข้อมูล

การศึกษาวิจัยครั้งนี้จะมีการนำเสนอและสรุปผลการศึกษาวิจัยในรูปแบบรายงานและนำเสนอในลักษณะงานวิจัยเชิงพรรณนาในแนวทางการแก้ไขปัญหาและการป้องกันการละเมิดข้อมูลส่วนบุคคล

ประโยชน์ที่ได้รับจากการวิจัย

1. ทำให้ทราบสถานการณ์ และแนวโน้มการละเมิดข้อมูลส่วนบุคคลผ่านระบบดิจิทัลและผลกระทบต่อการพัฒนาประเทศ
2. ทำให้ทราบปัญหาและอุปสรรคในการดำเนินการแก้ไขปัญหาและผลกระทบการละเมิดข้อมูลส่วนบุคคลผ่านเทคโนโลยีดิจิทัล
3. ได้เสนอแนวทางการแก้ไขปัญหาและการป้องกันการละเมิดข้อมูลส่วนบุคคลในการพัฒนาประเทศสู่ดิจิทัลไทยแลนด์

คำจำกัดความ

ข้อมูลส่วนบุคคล (Personal Data)

หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ เช่น ชื่อ เลขที่บัญชีธนาคาร ที่อยู่ บัตรประชาชน บัตรเครดิต และเบอร์โทรศัพท์ เป็นต้น

การละเมิดข้อมูลส่วนบุคคล (personal data breach)

หมายถึง การเก็บ การประมวลผล การเปิดเผยข้อมูลส่วนบุคคลไม่เป็นไปตามวัตถุประสงค์และไม่เป็นไปตามกฎหมายกำหนด รวมถึงการถูกโจมตีทางไซเบอร์

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act: PDPA)

หมายถึง บทบัญญัติที่ให้ความคุ้มครองข้อมูลส่วนบุคคลของ “บุคคลธรรมดา” ให้สิทธิ์ในการแก้ไข, เข้าถึง หรือแจ้งลบข้อมูลที่ให้ไว้กับองค์กรเป็นต้น และกำหนดบทบาทหน้าที่และบทลงโทษหากองค์กรไม่ปฏิบัติตาม

ดิจิทัลไทยแลนด์ (Digital Thailand)

หมายถึง การที่ประเทศไทยที่สามารถสร้างสรรค์และใช้ประโยชน์จากเทคโนโลยีดิจิทัลอย่างเต็มศักยภาพในการพัฒนาโครงสร้างพื้นฐาน นวัตกรรม ข้อมูล ทุนมนุษย์ และทรัพยากรอื่นใดเพื่อขับเคลื่อนการพัฒนาเศรษฐกิจและสังคมของประเทศ ไปสู่ความมั่นคง มั่งคั่ง และยั่งยืน

บทที่ 2
แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

ในบทนี้ผู้วิจัยศึกษาเรื่อง แนวทางการแก้ปัญหาและการป้องกันการละเมิดข้อมูลส่วนบุคคลเพื่อการปฏิรูปประเทศไทยสู่ดิจิทัลไทยแลนด์ โดยศึกษาเอกสาร ตำรา และงานวิจัยที่เกี่ยวข้อง ดังนี้

1. นโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม
2. ยุทธศาสตร์และแผนปฏิบัติการด้านข้อมูลส่วนบุคคล
3. กฎหมายที่เกี่ยวข้องการคุ้มครองข้อมูลส่วนบุคคล
4. งานวิจัยที่เกี่ยวข้อง
5. กรอบแนวคิดของการวิจัย
6. สรุป

นโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (2559) หรือกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม นำเสนอว่าพระราชบัญญัติการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. 2560 ได้กำหนดว่า “เพื่อให้การพัฒนาดิจิทัลเกิดประโยชน์ต่อเศรษฐกิจและสังคมของประเทศเป็นส่วนรวม ทั้งนี้ได้ให้คณะรัฐมนตรีจัดให้มีนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมขึ้นตามข้อเสนอของคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ การประกาศใช้และการแก้ไขปรับปรุงนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม ให้ทำเป็นประกาศพระบรมราชโองการและประกาศในราชกิจจานุเบกษา”

นโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมจะเป็นแผนแม่บทหลักในการพัฒนาเศรษฐกิจและสังคมดิจิทัลของประเทศ ระยะ 20 ปี (พ.ศ. 2561 – 2580) ที่กำหนดทิศทางการขับเคลื่อนการพัฒนาประเทศที่ยั่งยืนโดยใช้เทคโนโลยีดิจิทัล ซึ่งมีความสอดคล้องกับยุทธศาสตร์ชาติ 20 ปี(พ.ศ. 2561-2580) และแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 13 พ.ศ. 2566-2570

1. แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม 20 ปี

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (2559) หรือกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้ให้ความหมายของดิจิทัลไทยแลนด์ (Digital Thailand) ว่าหมายถึงประเทศไทยที่สามารถสร้างสรรค์ และใช้ประโยชน์จากเทคโนโลยีดิจิทัลอย่างเต็มศักยภาพในการพัฒนาโครงสร้างพื้นฐาน นวัตกรรม ข้อมูล ทุนมนุษย์ และทรัพยากรอื่นใดเพื่อขับเคลื่อนการพัฒนาเศรษฐกิจและ

สังคมของประเทศไปสู่ความมั่นคง มั่งคั่ง และยั่งยืน โดยแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม 20 ปี จะมีเป้าหมายในภาพรวม 4 ประการ ดังต่อไปนี้

1.1 เพิ่มขีดความสามารถในการแข่งขันทางเศรษฐกิจของประเทศด้วยการใช้นวัตกรรมละเทคโนโลยีดิจิทัลเป็นเครื่องมือหลักในการสร้างสรรค์นวัตกรรมการผลิตและการบริการ

1.2 สร้างโอกาสทางสังคมอย่างเท่าเทียมด้วยข้อมูลข่าวสารและบริการต่าง ๆ ผ่านสื่อดิจิทัล เพื่อยกระดับคุณภาพชีวิตของประชาชน

1.3 เตรียมความพร้อมให้บุคลากรทุกกลุ่มมีความรู้และทักษะที่เหมาะสมต่อการดำเนินชีวิตละการประกอบอาชีพในยุคดิจิทัล

1.4 ปฏิรูปกระบวนทัศน์การทำงานและการให้บริการของภาครัฐ ด้วยเทคโนโลยีดิจิทัลและการใช้ประโยชน์จากข้อมูล เพื่อให้การปฏิบัติงานเกิดความโปร่งใส มีประสิทธิภาพ และประสิทธิผล

2. ภูมิทัศน์ดิจิทัลของประเทศไทย (Thailand Digital Landscape)

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (2559) หรือกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมในปัจจุบัน นำเสนอว่าการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมของประเทศไทยมุ่งเน้นการพัฒนาระยะยาวอย่างยั่งยืนสอดคล้องกับการจัดทายุทธศาสตร์ชาติ 20 ปี แต่เนื่องจากเทคโนโลยีดิจิทัลมีการเปลี่ยนแปลงอย่างรวดเร็วดังนั้น นโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมฉบับนี้ จึงกำหนดภูมิทัศน์ดิจิทัลเพื่อกำหนดทิศทางการพัฒนาและเป้าหมายใน 4 ระยะ ดังนี้

ระยะที่ 1 (1 ปี 6 เดือน) Digital Foundation ประเทศไทยลงทุนและสร้างฐานรากในการพัฒนาเศรษฐกิจ และสังคมดิจิทัล

ระยะที่ 2 (5 ปี) Digital Thailand: Inclusion ทุกภาคส่วนของประเทศไทยมีส่วนร่วมในการพัฒนาเศรษฐกิจ และสังคมดิจิทัลตามแนวประชารัฐ

ระยะที่ 3 (10 ปี) Digital Thailand II : Full Transformation ประเทศไทยก้าวสู่ดิจิทัลไทยแลนด์ที่ขับเคลื่อนละใช้ประโยชน์จากนวัตกรรมดิจิทัลได้อย่างเต็มศักยภาพ

ระยะที่ 4 (10 – 20 ปี) Global Digital Leadership ประเทศไทยอยู่ในกลุ่มประเทศที่พัฒนาแล้วสามารถใช้เทคโนโลยีดิจิทัลสร้างมูลค่าทางเศรษฐกิจและคุณค่าทางสังคมอย่างยั่งยืน

3. ยุทธศาสตร์การพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (2559) หรือกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม นำเสนอว่ายุทธศาสตร์การพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมเพื่อขับเคลื่อนการพัฒนาดิจิทัลของประเทศไทยตามวิสัยทัศน์และแนวทางการพัฒนาตามภูมิทัศน์ดิจิทัลของประเทศไทยได้กำหนดเป็น 4 ระยะ ดังนั้นกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร จึงได้กำหนดยุทธศาสตร์การพัฒนาไว้ 6 ยุทธศาสตร์ ที่ส่งเสริมซึ่งกันและกันมีการกำหนดเป้าหมายเพื่อให้สามารถติดตามและประเมินความก้าวหน้าได้อย่างชัดเจนและมีแผนงานเพื่อดำเนินการตามยุทธศาสตร์ ดังนี้

3.1 พัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูงให้ครอบคลุมทั่วประเทศ: เข้าถึงพร้อมใช้จ่ายได้

3.2 ขับเคลื่อนเศรษฐกิจด้วยเทคโนโลยีดิจิทัล: ขับเคลื่อน New S-Curve เพิ่มศักยภาพสร้างธุรกิจ เพิ่มมูลค่า

3.3 สร้างสังคมคุณภาพด้วยเทคโนโลยีดิจิทัล: สร้างการมีส่วนร่วม การใช้ประโยชน์อย่างทั่วถึงและเท่าเทียม

3.4 ปรับเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัล: โปร่งใส อำนวยความสะดวก รวดเร็ว เชื่อมโยงเป็นหนึ่งเดียว

3.5 พัฒนากำลังคนให้พร้อมเข้าสู่ยุคเศรษฐกิจและสังคมดิจิทัล: สร้างคน สร้างงาน สร้างความเข็มแข็งจากภายใน

3.6 สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล: กฎระเบียบทันสมัย เชื่อมั่นในการลงทุน มีความมั่นคงปลอดภัย

ยุทธศาสตร์ทั้ง 6 ยุทธศาสตร์มีรายละเอียดที่สำคัญดังนี้

ยุทธศาสตร์ที่ 1 พัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูงให้ครอบคลุมทั่วประเทศ

โครงสร้างพื้นฐานดิจิทัลที่มีประสิทธิภาพที่ทุกคนเข้าถึงและใช้ประโยชน์ เพื่อรองรับการเป็นดิจิทัลไทยแลนด์ เป็นการยกระดับเศรษฐกิจและสังคมของประเทศด้วยเทคโนโลยีดิจิทัล

โครงสร้างพื้นฐานดิจิทัลที่สำคัญ ประกอบด้วยโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศโทรคมนาคม และการแพร่ภาพกระจายเสียงที่มีความทันสมัย มีคุณภาพ ขนาดเพียงพอครอบคลุมทุกพื้นที่และสามารถให้บริการได้อย่างต่อเนื่อง เพื่อรองรับการติดต่อสื่อสาร การเชื่อมต่อการแลกเปลี่ยนข้อมูลสารสนเทศการค้าและพาณิชย์ การบริการภาครัฐและเอกชน ตลอดจนการใช้งานรูปแบบต่าง ๆ อันเป็นประโยชน์ต่อการสร้างความมั่งคั่งทางเศรษฐกิจ และความมั่นคงทางสังคมของประเทศ รวมทั้งเพื่อรองรับการเป็นศูนย์กลางด้านดิจิทัลในอนาคต

สำหรับยุทธศาสตร์ที่ 1 นี้จะสร้างให้เกิดโครงสร้างพื้นฐานดิจิทัลที่ทันสมัย ประชาชนทุกคนสามารถเข้าถึงและใช้ประโยชน์ได้ ซึ่งการเข้าถึงบริการจะสามารถทำได้ทุกที่ ทุกเวลา อย่างมีคุณภาพด้วยอินเทอร์เน็ตความเร็วสูงที่รองรับความต้องการ และราคาค่าบริการที่ต้องจ่ายจะต้องไม่เป็นอุปสรรคในการเข้าถึงบริการดิจิทัลอีกต่อไป ในอนาคตโครงสร้างพื้นฐานอินเทอร์เน็ตความเร็วสูงจะกลายเป็นสาธารณูปโภคขั้นพื้นฐานเช่นเดียวกับ ถนน ไฟฟ้า ประปา ที่สามารถรองรับการเชื่อมต่อกับทุกสรรพสิ่ง

ยุทธศาสตร์ที่ 2 ขับเคลื่อนเศรษฐกิจด้วยเทคโนโลยีดิจิทัล

การขับเคลื่อนเศรษฐกิจด้วยเทคโนโลยีดิจิทัล หมายถึง การพัฒนาเศรษฐกิจของประเทศโดยอาศัยเทคโนโลยีดิจิทัลเพื่อให้ภาคธุรกิจสามารถลดต้นทุนการผลิตสินค้าและบริการพร้อมกับเพิ่มประสิทธิภาพในการดำเนินธุรกิจ ตลอดจนวางรากฐานการแข่งขันเชิงธุรกิจรูปแบบใหม่ในระยะยาว ภายใต้การส่งเสริมเศรษฐกิจดิจิทัล จำเป็นต้องเร่งสร้างระบบนิเวศสำหรับธุรกิจดิจิทัล โดยมุ่งเน้นการยกระดับและพัฒนาขีดความสามารถในการแข่งขันของภาคธุรกิจที่จะส่งผลต่อการขยายฐานเศรษฐกิจและอัตราการจ้างงานของประเทศไทยอย่างยั่งยืนในอุนาคต

สำหรับยุทธศาสตร์นี้เป็นการเร่งส่งเสริมเศรษฐกิจด้วยเทคโนโลยีดิจิทัล (Digital Economy Acceleration) โดยมุ่งเน้นการสร้างระบบนิเวศสำหรับธุรกิจดิจิทัล (Digital Business

Ecosystem)ควบคู่กับการพัฒนาระบบโครงสร้างพื้นฐานดิจิทัล และการใช้ประโยชน์จากเทคโนโลยีดิจิทัลในเชิงธุรกิจ และกระตุ้นให้ภาคเอกชนเกิดความตระหนักถึงความสำคัญ และความจำเป็นที่จะต้องเรียนรู้และปรับปรุงแนวทางการทำธุรกิจด้วยการใช้เทคโนโลยีดิจิทัลอย่างมีศักยภาพ โดยเฉพาะอย่างยิ่งธุรกิจขนาดกลางและเล็ก SMES รวมถึงธุรกิจใหม่ (Startup) ในด้านเศรษฐกิจชุมชน เทคโนโลยีดิจิทัลจะช่วยเชื่อมโยงท้องถิ่นกับตลาดโลกสร้างมูลค่าเพิ่มให้กับสินค้าชุมชน

ยุทธศาสตร์ที่ 3 สร้างสังคมคุณภาพด้วยเทคโนโลยีดิจิทัล

การสร้างสังคมคุณภาพด้วยเทคโนโลยีดิจิทัล หมายถึง การพัฒนาประเทศไทยที่ประชาชนทุกกลุ่ม โดยเฉพาะอย่างยิ่งกลุ่มเกษตรกร ผู้ที่อยู่ในชุมชนห่างไกล ผู้สูงอายุ ผู้ด้อยโอกาส และคนพิการ สามารถเข้าถึงและใช้ประโยชน์จากบริการต่าง ๆ ของภาครัฐผ่านเทคโนโลยีดิจิทัล มีการรวบรวมและแปลงข้อมูลองค์ความรู้ของประเทศทั้งระดับประเทศและระดับท้องถิ่นให้อยู่ในรูปแบบดิจิทัลที่ประชาชนสามารถเข้าถึงและนำไปใช้ประโยชน์ได้โดยง่ายและสะดวก โดยประชาชนมีความรู้เท่าทันข้อมูลข่าวสาร และมีทักษะในการใช้ประโยชน์จากเทคโนโลยีดิจิทัลอย่างมีความรับผิดชอบต่อสังคม

สำหรับยุทธศาสตร์ที่ 3 นี้ เป็นการสร้างสังคมดิจิทัลที่มีคุณภาพ (Digital Society) มุ่งหวังที่จะลดความเหลื่อมล้ำทางโอกาสของประชาชนที่เกิดจากการเข้าไม่ถึงโครงสร้างพื้นฐาน การขาดความรู้ความเข้าใจในเรื่องเทคโนโลยีดิจิทัล หรือการไม่สามารถเข้าถึงข้อมูลข่าวสารผ่านเทคโนโลยีดิจิทัลที่ยังมีราคาแพงเกินไป และให้ความสำคัญกับการพัฒนาพลเมืองที่ฉลาด รู้เท่าทันข้อมูล และมีความรับผิดชอบ เพื่อให้เกิดการใช้เทคโนโลยีดิจิทัลอย่างสร้างสรรค์ โดยสุดท้ายเมื่อโครงสร้างพื้นฐานดิจิทัลพร้อม และพลเมืองดิจิทัลพร้อมแล้ว เทคโนโลยีดิจิทัลจะเป็นเครื่องมือในการยกระดับคุณภาพชีวิตของคนทุกกลุ่มผ่านบริการดิจิทัลต่าง ๆ

ยุทธศาสตร์ที่ 4 ปรับเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัล

ปรับเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัล หมายถึง การนำเทคโนโลยีดิจิทัลมาใช้ในการปรับปรุงประสิทธิภาพการบริหารจัดการของหน่วยงานรัฐทั้งส่วนกลางและส่วนภูมิภาคอย่างมีแบบแผนและเป็นระบบจนพัฒนาสู่การเป็นรัฐบาลดิจิทัลโดยสมบูรณ์ โดยลักษณะของบริการภาครัฐหรือบริการสาธารณะจะอยู่ในรูปแบบดิจิทัลที่ขับเคลื่อนโดยความต้องการของประชาชนหรือผู้ใช้บริการ ซึ่งประชาชนทุกคนสามารถเข้าถึงบริการได้โดยไม่มีข้อจำกัดทางกายภาพ พื้นที่ และภาษา และในระยะต่อไป รัฐบาลสามารถหลอมรวมการทำงานของภาครัฐเสมือนเป็นองค์กรเดียว ภาครัฐจะแปรเปลี่ยนไปเป็นผู้อำนวยความสะดวกในการสร้างบริการสาธารณะโดยเอกชนและประชาชนเรียกว่า บริการระหว่างกัน (Peer to Peer) ตามหลักการออกแบบที่เป็นสากล (Universal Design) ประชาชนมีส่วนร่วมในการกำหนดแนวทางการพัฒนาเศรษฐกิจและสังคมการปกครอง/การบริหารบ้านเมืองและเสนอความคิดเห็นต่อการดำเนินงานของภาครัฐได้อย่างสมบูรณ์

ยุทธศาสตร์ที่ 4 นี้ เป็นการมุ่งเน้นการใช้เทคโนโลยีดิจิทัลในกระบวนการทำงานและการให้บริการภาครัฐ เพื่อให้เกิดการปฏิรูปกระบวนการทำงานและขั้นตอนการให้บริการให้มีประสิทธิภาพ ถูกต้อง รวดเร็ว อำนวยความสะดวกให้ผู้ใช้บริการ สร้างบริการของภาครัฐที่มีธรรมาภิบาล และสามารถให้บริการประชาชนแบบเบ็ดเสร็จ ณ จุดเดียวผ่านระบบเชื่อมโยงข้อมูลอัตโนมัติ การเปิดเผยข้อมูลของภาครัฐที่ไม่กระทบต่อสิทธิส่วนบุคคลและความมั่นคงของชาติ ผ่านการจัดเก็บ

รวบรวม และแลกเปลี่ยนอย่างมีมาตรฐาน ให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยไซเบอร์และข้อมูล รวมไปถึงการสร้างแพลตฟอร์มการให้บริการภาครัฐ เพื่อให้ภาคเอกชนหรือนักพัฒนาสามารถนำข้อมูลและบริการของภาครัฐไปพัฒนาต่อยอดให้เกิดนวัตกรรมบริการ และสร้างรายได้ให้กับระบบเศรษฐกิจต่อไป

ยุทธศาสตร์ที่ 5 พัฒนากำลังคนให้พร้อมเข้าสู่ยุคเศรษฐกิจและสังคมดิจิทัล

การพัฒนากำลังคนดิจิทัล หมายถึง การสร้างและพัฒนาบุคลากรผู้ทำงานให้มีความสามารถในการสร้างสรรค์และใช้เทคโนโลยีดิจิทัลอย่างชาญฉลาดในการประกอบอาชีพ รวมถึงการพัฒนาทักษะด้านเทคโนโลยีดิจิทัลในบุคลากรภาครัฐ ภาคเอกชน ทั้งที่ประกอบอาชีพในสาขาเทคโนโลยีดิจิทัลโดยตรง และทุกสาขาอาชีพ ให้มีความรู้ความสามารถและความเชี่ยวชาญตามระดับมาตรฐานสากล เพื่อสร้างให้เกิดการจ้างงานที่มีคุณค่าสูงรองรับการพัฒนาประเทศในยุคเศรษฐกิจและสังคมที่ใช้เทคโนโลยีดิจิทัลเป็นปัจจัยหลักในการขับเคลื่อน

ยุทธศาสตร์ที่ 5 นี้ มุ่งเน้นการพัฒนากำลังคนดิจิทัล (Digital Workforce) ขึ้นมารองรับการทำงานในระบบเศรษฐกิจดิจิทัล โดยเน้นทั้งกลุ่มคนทำงานที่จะเป็นกำลังสำคัญในการสร้างผลิตภาพการผลิต (Productivity) ในระบบเศษฐกิจ และกลุ่มคนที่เป็นผู้เชี่ยวชาญด้านดิจิทัล อย่างไรก็ตามการเตรียมความพร้อมให้ประชาชนทั่วไปก็เป็นอีกเรื่องที่สำคัญอย่างทัดเทียมกัน

ยุทธศาสตร์ที่ 6 สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล

การสร้างความเชื่อมันในการใช้เทคโนโลยีดิจิทัล หมายถึง มาตรฐาน กฎหมาย กฎระเบียบ และกติกาที่มีประสิทธิภาพทันสมัยและสอดคล้องกับหลักเกณฑ์สากลที่เป็นพลังในการขับเคลื่อนเศรษฐกิจ และสังคมดิจิทัลของประเทศ ตลอดจนการสร้างความมั่นคงปลอดภัย การสร้างความเชื่อมั่น และการคุ้มครองสิทธิให้แก่ผู้ใช้งานเทคโนโลยีดิจิทัลในทุกภาคส่วน เพื่อก่อให้เกิดการอำนวยความสะดวก ลดอุปสรรค เพิ่มประสิทธิภาพในการประกอบกิจกรรมที่เกี่ยวข้องต่าง ๆ พร้อมกับสร้างแนวทางขับเคลื่อนอย่างบูรณาการ เพื่อรองรับการเติบโตของเทคโนโลยีดิจิทัลในอนาคต

ยุทธศาสตร์ที่ 6 นี้ มุ่งเน้นการสร้างความมั่นคงปลอดภัย และความเชื่อมั่นในการทำธุรกรรมด้วยเทคโนโลยีดิจิทัลให้กับผู้ประกอบการ ผู้ทำงาน และผู้ใช้บริการ ซึ่งถือได้ว่าเป็นปัจจัยพื้นฐานที่ช่วยขับเคลื่อนประเทศสู่ยุคเศรษฐกิจดิจิทัล และเป็นบทบาทหน้าที่หลักของภาครัฐในการอำนวยความสะดวกให้กับทุกภาคส่วน โดยภารกิจสำคัญยิ่งยวดของยุทธศาสตร์นี้ จะครอบคลุมเรื่องมาตรฐาน (Standard) การคุ้มครองความเป็นส่วนตัวและข้อมูลส่วนบุคคล (Privacy) การรักษาความมั่นคงปลอดภัย (Cybersecurity)

สรุปได้ว่า การจัดทำนโยบายและแผนระดับชาติ ประเด็น การพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมที่เป็นแผนหลักในการพัฒนาเศรษฐกิจและสังคมดิจิทัลของประเทศไทย ระยะ 20 ปี เป็นกรอบในการจัดทำพลวัตของเทคโนโลยีดิจิทัลที่เปลี่ยนแปลงอย่างรวดเร็วและไม่หยุดยั้งส่งผลกระทบอย่างมากต่อวิถีชีวิต รูปแบบ กิจกรรมของปัจเจกชนและองค์กร รวมถึงระบบเศรษฐกิจ และสังคม ความสามารถในการใช้ประโยชน์จากเทคโนโลยีดิจิทัลจึงเป็นปัจจัยสำคัญของการพัฒนาประเทศดังที่หลากหลายประเทศได้ตระหนักและมีการลงทุน พัฒนา และส่งเสริมการใช้เทคโนโลยีดิจิทัลเพื่อนำไปสู่เศรษฐกิจและสังคมดิจิทัลที่หมายถึงระบบเศรษฐกิจและสังคมที่เทคโนโลยีดิจิทัลเป็นกลไกสำคัญในการดำเนินกิจกรรมทางเศรษฐกิจและสังคม การใช้ชีวิตประจำวันของประชาชน การเปลี่ยน

กระบวนทัศน์ทางความคิดรูปแบบการมีปฏิสัมพันธ์ของคนในสังคม การปฏิรูปกระบวนการทงธุรกิจ ซึ่งรวมถึงการผลิต การค้าการบริการ และการบริหารราชการแผ่นดินอันนำมาสู่การพัฒนาทางเศรษฐกิจการพัฒนาคุณภาพชีวิตของคนในสังคม โดยแนวทางการพัฒนาเศรษฐกิจและสังคมดิจิทัลของประเทศไทยนั้นจะตั้งอยู่บนคุณลักษณะสำคัญที่เกิดจากความสามารถและพลวัตของเทคโนโลยีดิจิทัล อันได้แก่ 1) การใช้เทคโนโลยีเป็นเครื่องมือในการเชื่อมต่อกิจกรรมทางเศรษฐกิจและสังของแระชาคมในประเทศและประชาคมโลก 2) การเข้าสู่ระบบเศรษฐกิจและสังคมที่ขับเคลื่อนด้วยนวัตกรรม 3) การสร้างและใช้ประโยชน์จากข้อมูลจำนวนมหาศาล 4) การใช้เทคโนโลยีดิจิทัลที่แพร่กระจายแทรกซึมไปทุกภาคส่วน

ยุทธศาสตร์และแผนปฏิบัติการด้านข้อมูลส่วนบุคคล

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (2559) หรือกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม นำเสนอว่าการสร้างความเชื่อมันในการใช้เทคโนโลยีดิจิทัล หมายถึง มาตรฐาน กฎหมาย กฎระเบียบ และกติกาที่มีประสิทธิภาพทันสมัยและสอดคล้องกับหลักเกณฑ์สากลที่เป็นพลังในการขับเคลื่อนเศรษฐกิจและสังคมดิจิทัลของประเทศ ตลอดจนการสร้างความมั่นคงปลอดภัย การสร้างความเชื่อมั่นและการคุ้มครองสิทธิให้แก่ผู้ใช้งานเทคโนโลยี ดิจิทัลในทุกภาคส่วน เพื่อก่อให้เกิดการอำนวยความสะดวก ลดอุปสรรค เพิ่มประสิทธิภาพในการประกอบกิจกรรมที่เกี่ยวข้องต่าง ๆ พร้อมกับสร้างแนวทางขับเคลื่อนอย่างบูรณาการ เพื่อรองรับการเติบโตของเทคโนโลยีดิจิทัลในอนาคต กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมจึงได้กำหนดแผนปฏิบัติการยุทธศาสตร์ที่ 6 สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล โดยมีเป้าหมายที่สำคัญดังนี้

1. ประชาชนและภาคธุรกิจมีความเชื่อมั่นในการทำธุรกรรมออนไลน์อย่างเต็มรูปแบบ โดยมีผู้ใช้อินเทอร์เน็ตที่ทำธุรกรรมเพิ่มสูงขึ้นต่อเนื่องและมูลค่า e Commerce เพิ่มขึ้นไม่น้อยกว่าร้อยละ 4 ต่อปี

2. มีชุดกฎหมาย กฎระเบียบที่ทันสมัย เพื่อรองรับการพัฒนาเศรษฐกิจและสังคมดิจิทัล โดยผลักดัน Data Protection Law และปรับแก้ไข Computer Crime Law ให้บังคับใช้ได้

3. มีมาตรฐานข้อมูลที่เป็นสากล เพื่อรองรับการเชื่อมโยงและใช้ประโยชน์ในการทำธุรกรรม

3.1 ภาคธุรกิจดำเนินธุรกิจภายในและระหว่างประเทศได้สะดวก รวดเร็ว และต้นทุนทำธุรกรรมผ่านสื่อดิจิทัลลดลง

3.2 กระบวนการขอใบอนุญาต มีระยะเวลาที่สั้นลงตามเกณฑ์ของกลุ่มผู้นำในดัชนี Ease of Doing Business

3.3 มีมาตรฐานข้อมูล และมาตรฐานเอกสารอิเล็กทรอนิกส์ เพื่อให้สามารถเปลี่ยนและเชื่อมโยงข้อมูลภายในหน่วยงานภาครัฐ และระหว่างหน่วยงานภาครัฐและเอกชน

โดยได้จัดทำแผนปฏิบัติการด้านข้อมูลส่วนบุคคลดังนี้

1. จัดให้มีระบบนิเวศที่เหมาะสมต่อการดำเนินธุรกิจและการปรับปรุงคุณภาพชีวิตของประชาชนโดยสร้างความมั่นคงปลอดภัยในการใช้งานเทคโนโลยีดิจิทัลด้วยการกำหนดมาตรฐาน กฎระเบียบและกติกา ให้มีความทันสมัยและมีประสิทธิภาพ เพื่ออำนวยความสะดวกด้านการค้า และ

การใช้ประโยชน์ในภาคเศรษฐกิจและสังคม ซึ่งภาครัฐจะเป็นผู้เริ่มต้นในการลดอุปสรรคในการดำเนินการต่าง ๆ

1.1 จัดให้มีสิ่งอำนวยความสะดวกในการดำเนินธุรกิจดิจิทัลที่เหมาะสม ที่ทำให้ผู้ใช้งานมีความมั่นใจ ซึ่งประกอบด้วย ระบบเชื่อมโยงมาตรฐานสินค้าที่เป็นสากล การจัดเก็บฐานข้อมูลกลางสินค้า (Trusted Source Data Pool) ระบบการชำระเงินอิเล็กทรอนิกส์ (e-Payment) การสาธารณสุขอิเล็กทรอนิกส์ (e-Health) การค้าสินค้าอิเล็กทรอนิกส์ (e-Trade) ที่เชื่อมโยงกันได้ การดำเนินการมาตรฐานข้อความที่เกี่ยวกับการค้า เช่น e-Invoice ของภาคธุรกิจที่สามารถใช้เป็นหลักฐานทางกฎหมายได้การกำหนดกฎระเบียบที่เกี่ยวข้องกับการประยุกต์และนำ Internet of Things (IOT) มาใช้ในภาคอุตสาหกรรม และการผลิต(Industrial Internet) เป็นต้น เพื่อสนับสนุนการทำธุรกิจที่เชื่อมโยงกันทั้งในประเทศและต่างประเทศให้มีมาตรฐานใช้งานร่วมกันที่ได้รับการยอมรับจากผู้เกี่ยวข้อง

1.2 ปรับแก้กฎหมายให้ภาครัฐและภาคเอกชนยอมรับการใช้เอกสารอิเล็กทรอนิกส์โดยไม่ต้องยื่นแบบฟอร์มกระดาษในการทำธุรกรรมต่าง ๆ ตลอดตนสามารถใช้เป็นหลักฐานทางกฎหมายได้

1.3 ลดขั้นตอน ลดจำนวนใบอนุญาต ลดจำนวนเอกสาร และลดระยะเวลาในการดำเนินงานทางธุรกรรมทั้งภาครัฐและเอกชน

1.4 สร้างกลไกและแรงจูงใจในการกำกับดูแลตนเองในกลุ่มผู้ประกอบการ และการมีกระบวนการติดตามและประเมินระดับความสามารถในการดำเนินธุรกิจอย่างต่อเนื่อง

1.5 กำหนดมาตรฐานการแลกเปลี่ยนข้อมูลทางเทคนิคเพื่อการปฏิบัติงานร่วมกัน (Interoperability Standard) ในการเชื่อมโยง วิเคราะห์ สังเคราะห์ และใช้ประโยชน์จากข้อมูล เช่น การกำหนดรายการข้อมูลและโครงสร้างข้อมูลเพื่อการแลกเปลี่ยน กฎกติกาการตั้งชื่อรายการข้อมูล กฎกติกาการออกแบบโครงสร้างเอกสาร มาตรฐานกลางเชื่อมโยงข้อมูลการค้า การชำระเงินภาษี เป็นต้น

2. ปรับปรุงกฎหมายที่เกี่ยวข้องกับเศรษฐกิจและสังคมดิจิทัลให้มีความทันสมัยสอดคล้องต่อพลวัตของเทคโนโลยีดิจิทัลและบริบทของสังคม

2.1 มีกฎหมายที่เกี่ยวข้องที่ทันต่อความก้าวหน้าของเทคโนโลยีดิจิทัลและสอดคล้องกับมาตรฐานสากล ซึ่งสามารถสนับสนุนการใช้งานและใช้ประโยชน์ได้อย่างเป็นรูปธรรม เช่น กฎหมายที่เกี่ยวกับความมั่นคงปลอดภัยของระบบสารสนเทศและข้อมูลส่วนบุคคล กฎหมายเกี่ยวกับทรัพย์สินทางปัญญาเพื่อส่งเสริม และสร้างแรงจูงใจในการทำนวัตกรรม เป็นต้น

2.2 เร่งปรับปรุงกลไกการคุ้มครองทรัพย์สินทางปัญญาที่รองรับความก้าวหน้าทางเทคโนโลยีดิจิทัล และสอดคล้องกับหลักเกณฑ์ แนวปฏิบัติสากล และสร้างแรงจูงใจให้เกิดการใช้ประโยชน์จากทรัพย์สินทางปัญญาที่สร้างสรรค์โดยคนไทย รวมถึงการใช้โปรแกรมคอมพิวเตอร์ที่ถูกกฎหมาย

2.3 ให้ประชาชน และหน่วยงานที่เกี่ยวข้อง สามารถมีส่วนร่วมในกระบวนการยกร่าง พัฒนาตรวจสอบ และทบทวนกฎหมายต่าง ๆ ที่เกี่ยวข้องกับเทคโนโลยีดิจิทัล ซึ่งเป็นการเริ่มต้น

ของการติดต่อสื่อสารระหว่างประชาชนกับรัฐบาลในเรื่องการตัดสินใจเกี่ยวกับนโยบายสาธารณะที่มีผลกระทบต่อประชาชน (e-Participation)

2.4 ให้หน่วยงานที่เกี่ยวข้องดำเนินการนำนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมแปลงสู่การปฏิบัติอย่างเป็นรูปธรรม โดยมีการวัดผล ตรวจสอบ ติดตามและประเมินความเหมาะสมเป็นระยะอย่างต่อเนื่อง รวมถึงจัดสรรทรัพยากรสนับสนุนเพื่อให้เกิดผลสัมฤทธิ์

3. สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัลและการทำธุรกรรมออนไลน์

3.1 สร้างความมั่นคงปลอดภัยของระบบสารสนเทศและการสื่อสาร เพื่อสร้างความเชื่อมั่นให้กับภาคธุรกิจและประชาชนในการสื่อสาร และการทำธุรกรรมออนไลน์ เช่น จัดให้มีระบบการชำระเงินที่ตรงตามความต้องการมีประสิทธิภาพและความมั่นคงปลอดภัย เป็นต้น

3.2 กำหนดมาตรการและแนวปฏิบัติสำหรับผู้ให้บริการทั้งภาครัฐและภาคเอกชนในการคุ้มครองสิทธิส่วนบุคคลและการคุ้มครองข้อมูลส่วนบุคคลของผู้รับบริการ เช่น แนวปฏิบัติในการใช้งาน Mobile Commerce หรือ Smart Phone แนวปฏิบัติในการใช้งาน Social Media เป็นต้น เพื่อรองรับการเติบโตของการใช้งานเทคโนโลยีดิจิทัลในอนาคต

3.3 การกำหนดมาตรการการเฝ้าระวังและรับมือภัยคุกคามไซเบอร์ที่เหมาะสมและสอดคล้องตามมาตรฐานสากล โดยเฉพาะการปกป้องโครงสร้างพื้นฐานที่มีความจำเป็นอย่างยิ่งยวด (Critical Infrastructure) เช่น โครงสร้างพื้นฐานทางไฟฟ้า โครงสร้างพื้นฐานทางการเงิน เพื่อให้มีความมั่นคงปลอดภัยเพียงพอต่อการค้าและการลงทุน การสร้างเครือข่ายแลกเปลี่ยนข้อมูลภัยคุกคามไซเบอร์ พร้อมกำหนดหน่วยงานรับแจ้งเหตุ และสร้างกลไกการบังคับใช้กฎหมายที่มีประสิทธิภาพในการป้องกันปราบปรามการกระทำความผิดที่มีผลต่อระบบความมั่นคงปลอดภัยดิจิทัล ทั้งนี้ การส่งเสริมให้เกิดความตระหนักและรู้เท่าทันภัยคุกคามทางไซเบอร์เป็นสิ่งสำคัญที่ต้องดำเนินการอย่างต่อเนื่อง

3.4 สร้างระบบและกลไกการคุ้มครองผู้บริโภคที่ใช้ธุรกรรมออนไลน์ เช่น ส่งเสริมและผลักดันให้หน่วยงานหลักที่เกี่ยวข้องมีความพร้อมและความเข้มแข็ง สามารถทำงานร่วมกับหน่วยงานที่เกี่ยวข้องได้อย่างมีประสิทธิภาพ รวมถึงกระบวนการในการระงับข้อพิพาทออนไลน์และการเน้นให้ภาคธุรกิจสามารถดูแลและกำกับกันเองได้อย่างมีธรรมาภิบาล โปร่งใส ตรวจสอบได้ เป็นไปตามมาตรฐานที่ได้รับการรับรองโดยภาครัฐ(Self-Regulation) ทั้งนี้ ในบางสถานการณ์ภาครัฐอาจร่วมกำกับดูแล (Co-Regulation)ตามความเหมาะสม เพื่อให้ระบบการควบคุมกำกับดูแลมีประสิทธิภาพ

สรุปได้ว่า แผนปฏิบัติการข้อมูลส่วนบุคคลตามยุทธศาสตร์ที่ 6 สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล มีเป้าหมายคือมุ่งเน้นการสร้างความมั่นคงปลอดภัย และความเชื่อมั่นในการทำธุรกรรมด้วยเทคโนโลยีดิจิทัลให้กับผู้ประกอบการ ผู้ทำงาน และผู้ใช้บริการ ซึ่งถือได้ว่าเป็นปัจจัยพื้นฐานที่ช่วยขับเคลื่อนประเทศสู่ยุคเศรษฐกิจดิจิทัล และเป็นบทบาทหน้าที่หลักของภาครัฐในการอำนวยความสะดวกให้กับทุกภาคส่วน โดยภารกิจสำคัญยิ่งยวดของยุทธศาสตร์นี้ จะครอบคลุมเรื่องมาตรฐาน (Standard) การคุ้มครองความเป็นส่วนตัวและข้อมูลส่วนบุคคล (Privacy) การรักษาความมั่นคงปลอดภัย (Cybersecurity)

กฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

ผู้วิจัยได้รวบรวมกฎหมายที่เกี่ยวข้องกับการคุ้มครองส่วนบุคคลทั้งทางตรงและทางอ้อม ดังนี้

1. พระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม (ฉบับที่ 17) พ.ศ.2559 (เพื่อจัดตั้งกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม)

การประกาศใช้พระราชบัญญัติฉบับนี้คือโดยที่เทคโนโลยีสารสนเทศและการสื่อสารด้านดิจิทัลได้เข้ามามีบทบาทสำคัญในการพัฒนาและขับเคลื่อนเศรษฐกิจ สังคม ฐานความรู้ และขีดความสามารถในการแข่งขันของประเทศ โดยหน่วยงานภาครัฐและภาคธุรกิจต่างมีความต้องการนำระบบเทคโนโลยีสารสนเทศ และการสื่อสารด้านดิจิทัลมาใช้ในการพัฒนาศักยภาพและประสิทธิภาพของการให้บริการ แต่กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารมีขอบเขตอำนาจหน้าที่จำกัดเฉพาะเรื่องเทคโนโลยีสารสนเทศและระบบสื่อสารซึ่งไม่ครอบคลุมถึงเรื่องการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมเพื่อรองรับการดำเนินกิจกรรมทางเศรษฐกิจ และสังคมในปัจจุบันที่มีการขับเคลื่อนโดยเทคโนโลยีดิจิทัลเป็นหลัก ซึ่งจำเป็นต้องมีหน่วยงานภาครัฐทำหน้าที่บูรณาการกลไกต่าง ๆ ทั้งภาครัฐและภาคเอกชนให้มีการดำเนินการไปในทิศทางเดียวกันอันจะเป็นประโยชน์ต่อภาพรวมของการพัฒนาเศรษฐกิจและสังคมของประเทศโดยเน้นให้เทคโนโลยีดิจิทัลเข้าไปมีบทบาทในทุกภาคส่วน ดังนั้น เพื่อให้มีกระทรวงที่มีอำนาจหน้าที่ครอบคลุมถึงเรื่องดิจิทัลเพื่อเศรษฐกิจและสังคม จึงต้องดำเนินการปรับโครงสร้างกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารให้มีขอบเขตอำนาจหน้าที่มากขึ้นและเปลี่ยนชื่อเป็นกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม จึงจำเป็นต้องตราพระราชบัญญัตินี้

2. พระราชบัญญัติการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ.2560

การประกาศใช้พระราชบัญญัติฉบับนี้ด้วยเหตุผลคือโดยที่เทคโนโลยีสารสนเทศและการสื่อสารในด้านดิจิทัลได้เข้ามามีบทบาทสำคัญในการพัฒนาและขับเคลื่อนเศรษฐกิจและสังคม รวมทั้งส่งผลต่อฐานความรู้และขีดความสามารถในการแข่งขันของประเทศ ซึ่งหน่วยงานภาครัฐและภาคธุรกิจต่างมีความต้องการนำระบบเทคโนโลยีด้านดิจิทัลดังกล่าวมาใช้ในการพัฒนาศักยภาพและประสิทธิภาพของการให้บริการ เพื่อประโยชน์ที่ประชาชนจะได้รับหรือการพัฒนาในการแข่งขันทางธุรกิจของภาคเอกชน แต่ประเทศไทยยังขาดการพัฒนาเทคโนโลยีสารสนเทศและการสื่อสารในด้านดิจิทัลอย่างเป็นระบบที่จะสามารถตอบสนองความต้องการดังกล่าวได้อย่างมีประสิทธิภาพ อันจะนำไปสู่การพัฒนาทางด้านเศรษฐกิจและสังคมของประเทศ ดังนั้น เพื่อให้การพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมของประเทศครอบคลุมการดำเนินงานในด้านต่าง ๆ ที่มีส่วนสำคัญต่อการพัฒนาเศรษฐกิจและสังคมของประเทศและการวางโครงสร้างพื้นฐานสารสนเทศอย่างเป็นระบบเพื่อลดความซ้ำซ้อนในการดำเนินงานและส่งเสริมกิจกรรมในด้านเศรษฐกิจและสังคมของประเทศทั้งของภาครัฐและภาคเอกชนจึงจำเป็นต้องตราพระราชบัญญัตินี้

3. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

การประกาศใช้พระราชบัญญัติฉบับนี้ด้วยเหตุผลคือเนื่องจากปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือ

ความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคลประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวกและรวดเร็ว ก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวม สมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้น เพื่อกำหนดหลักเกณฑ์กลไกหรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป จึงจำเป็นต้องตราพระราชบัญญัตินี้

4. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 คือมาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกันและรับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหารและความสงบเรียบร้อยภายในประเทศ ดังนั้นเพื่อให้สามารถป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงทีจึงมีการกำหนดกฎหมายนี้ขึ้นมา ซึ่งการตราพระราชบัญญัตินี้สอดคล้องกับเงื่อนไขที่บัญญัติไว้ในมาตรา 26 ของรัฐธรรมนูญแห่งราชอาณาจักรไทยที่บัญญัติไว้ว่า “การตรากฎหมายที่มีผลเป็นการจำกัดสิทธิหรือเสรีภาพของบุคคลต้องเป็นไปตามเงื่อนไขที่บัญญัติไว้ในรัฐธรรมนูญ ในกรณีที่รัฐธรรมนูญมิได้บัญญัติเงื่อนไขไว้ว่า กฎหมายดังกล่าวต้องไม่ขัดต่อหลักนิติธรรม ไม่เพิ่มภาระหรือจำกัดสิทธิหรือเสรีภาพของบุคคลเกินสมควรแก่เหตุและจะกระทบต่อศักดิ์ศรีความเป็นมนุษย์ของบุคคล มิได้ รวมทั้งต้องระบุเหตุผลความจำเป็นในการจำกัดสิทธิและเสรีภาพไว้ด้วย กฎหมายตามวรรคหนึ่ง ต้องมีผลใช้บังคับเป็นการทั่วไปไม่มุ่งหมายให้ใช้บังคับแก่กรณีใดกรณีหนึ่งหรือแก่บุคคลใดบุคคลหนึ่งเป็นการเจาะจง”

การประกาศใช้พระราชบัญญัติฉบับนี้ด้วยเหตุผลคือในปัจจุบันการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคมหรือการให้บริการโดยปกติของดาวเทียมมีความเสี่ยงจากภัยคุกคามทางไซเบอร์ซึ่งอาจกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อย ภายในประเทศ ดังนั้นเพื่อให้สามารถป้องกันหรือรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงทีทั้งหน่วยงานของรัฐและหน่วยงานเอกชนจะต้องมีการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ไม่ให้เกิดผลกระทบต่อความมั่นคงในด้านต่าง ๆ ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์อันเป็นภัยต่อความ มั่นคงอย่างร้ายแรงก็ตาม

5. พระราชบัญญัติสภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย พ.ศ. 2562

การประกาศใช้พระราชบัญญัติฉบับนี้ด้วยเหตุผลคือเนื่องด้วยการพัฒนานวัตกรรมดิจิทัลมีความสำคัญต่อการพัฒนาศักยภาพ ขีดความสามารถการแข่งขันของประเทศและนวัตกรรมดิจิทัลมีการเปลี่ยนแปลงอย่างรวดเร็วและมีผลกระทบโดยตรงต่อประชาชนและสังคม สมควรที่ประเทศไทยจะมีการจัดตั้งสภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย อันเป็นการรวมตัวของภาคเอกชนในธุรกิจหรืออุตสาหกรรมดิจิทัลซึ่งมีความพร้อมทั้งด้านกำลังคน ความรู้ความสามารถประสบการณ์โดยตรง รวมทั้งมีความใกล้ชิดและความเข้าใจพฤติกรรมของผู้บริโภค เพื่อให้เป็นองค์กรสำคัญในการทำงานร่วมกับรัฐบาล และภาคเอกชนอื่น ในการสนับสนุนการผลิตและพัฒนานวัตกรรมดิจิทัล อันจะนำไปสู่การเพิ่มขีดความสามารถในการแข่งขัน การพัฒนาบุคลากรด้านดิจิทัล และการ

นำนวัตกรรมดิจิทัลไปประยุกต์ใช้ในประเทศไทยเพื่อให้เกิดการพัฒนาประเทศอย่างยั่งยืน จึงจำเป็นต้องตราพระราชบัญญัตินี้

6. พระราชบัญญัติสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2562

การประกาศใช้พระราชบัญญัติฉบับนี้ด้วยเหตุผลคือโดยที่ปัจจุบันสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ซึ่งมีสถานะเป็นองค์การมหาชน ตามกฎหมายว่าด้วยองค์การมหาชนมีหน้าที่เฉพาะการส่งเสริมและสนับสนุนการทำธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานต่าง ๆ เท่านั้น แต่ด้วยความก้าวหน้าทางเทคโนโลยีและการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมจะต้องมีการพัฒนา ส่งเสริมและสนับสนุนการทำธุรกรรมทางอิเล็กทรอนิกส์ของประเทศให้เป็นไปตามนโยบายและยุทธศาสตร์ของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ในฐานะคณะกรรมการระดับชาติและต้องมีการควบคุมดูแลการประกอบธุรกิจเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์อย่างเป็นระบบและมีมาตรฐานสากล สามารถแข่งขันกับนานาประเทศ รวมทั้งต้องมีการบูรณาการการทำงานระหว่างหน่วยงานของรัฐที่เกี่ยวข้องกับการส่งเสริมภาคเอกชนในการดำเนินการด้านธุรกรรมทางอิเล็กทรอนิกส์ของประเทศ ตลอดจนการดำเนินการในด้านพาณิชย์อิเล็กทรอนิกส์และด้านอื่นที่เกี่ยวข้อง สมควรที่จะมีหน่วยงานที่มีการบริหารงานที่คล่องตัวและมีประสิทธิภาพเพื่อรับผิดชอบในการดำเนินการดังกล่าว ในกรณีจึงได้ปรับปรุงสถานะและอำนาจหน้าที่ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์กรมหาชน) เพื่อให้สามารถรองรับการปฏิบัติงานตามภารกิจได้อย่างเหมาะสมและสอดคล้องกับนโยบายและยุทธศาสตร์ด้านการพัฒนาส่งเสริมและสนับสนุนการทำธุรกรรมทางอิเล็กทรอนิกส์ของประเทศ จึงจำเป็นต้องตราพระราชบัญญัตินี้

7. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 4) พ.ศ. 2562

การประกาศใช้พระราชบัญญัติฉบับนี้ด้วยเหตุผลคือ โดยที่การยืนยันตัวตนของบุคคลเป็นขั้นตอนสำคัญในการทำธุรกรรมในระบบเศรษฐกิจ แต่ที่ผ่านมาผู้ที่ประสงค์จะขอรับบริการจากผู้ประกอบการหรือหน่วยงานใด ๆ จะต้องทำการพิสูจน์และยืนยันตัวตนโดยการแสดงตนต่อผู้ให้บริการพร้อมกับต้องส่งเอกสารหลักฐาน ซึ่งเป็นภาระต่อผู้ใช้บริการและผู้ให้บริการ สมควรกำหนดให้บุคคลสามารถพิสูจน์และยืนยันตัวตนผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลได้ โดยมีกลไกการควบคุมดูแลผู้ประกอบธุรกิจบริการที่เกี่ยวข้องเพื่อให้ระบบดังกล่าวมีความน่าเชื่อถือและปลอดภัย จึงจำเป็นต้องตราพระราชบัญญัตินี้

8. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

การประกาศใช้พระราชบัญญัติฉบับนี้ด้วยเหตุผลคือปัจจุบันเทคโนโลยีได้มีความก้าวหน้าและเป็นส่วนหนึ่งในวิถีชีวิตและการประกอบธุรกิจของประชาชน ซึ่งในการบริหารงานและการให้บริการภาครัฐที่ผ่านมายังมิได้นำเทคโนโลยีมาใช้ในการพัฒนาให้เกิดประสิทธิภาพและอำนวยความสะดวกแก่ประชาชนได้อย่างเต็มที่และโดยที่รัฐธรรมนูญแห่งราชอาณาจักรไทยบัญญัติให้มีการปฏิรูปประเทศด้านการบริหารราชการแผ่นดิน โดยให้มีการนำเทคโนโลยีที่เหมาะสม

มาประยุกต์ใช้ในการบริหารราชการแผ่นดินและการจัดทำบริการสาธารณะ และให้มีการบูรณาการฐานข้อมูลของหน่วยงานของรัฐทุกหน่วยงานเข้าด้วยกันเพื่อให้เป็นระบบข้อมูล เพื่อประโยชน์ในการบริหารราชการแผ่นดินและเพื่ออำนวยความสะดวกให้แก่ประชาชน สมควรให้มีกฎหมายในการขับเคลื่อนให้เกิดการปฏิรูปการบริหารราชการแผ่นดินและการบริการประชาชนตามบทบัญญัติแห่งรัฐธรรมนูญ และเพื่อยกระดับการบริหารงานและการให้บริการภาครัฐให้อยู่ในระบบดิจิทัล อันจะนำไปสู่การเป็นรัฐบาลดิจิทัลที่มีระบบการทำงานและข้อมูลเชื่อมโยงกันระหว่างหน่วยงานของรัฐอย่างมั่นคงปลอดภัยมีประสิทธิภาพ รวดเร็ว เปิดเผยและโปร่งใส รวมทั้งประชาชนได้รับความสะดวกในการรับบริการและสามารถตรวจสอบการดำเนินงานของหน่วยงานของรัฐได้ จึงจำเป็นต้องตราพระราชบัญญัตินี้

สรุปได้ว่า กฎหมายที่ได้กล่าวไว้ข้างต้น แม้ว่าจะมีเนื้อหาที่แตกต่างกัน แต่ก็มีวัตถุประสงค์ร่วมกันในการสนับสนุน และส่งเสริมการใช้เทคโนโลยีดิจิทัลในธุรกรรมประจำวัน บางครั้งจึงอาจทำให้เกิดการกำหนดหน้าที่ที่ทับซ้อนกันอยู่บ้าง แม้ว่ากฎหมายที่เกี่ยวกับการส่งเสริมและพัฒนาเศรษฐกิจและสังคมดิจิทัลจะดูมีความคืบหน้าไปในทิศทางที่ดี แต่ผลลัพธ์ในเชิงรูปธรรมยังคงต้องใช้เวลาอีกสักพักหนึ่งภายหลังจากที่กฎหมายเหล่านี้มีผลใช้บังคับแล้ว และอาจจะต้องมีการแก้ไข ปรับปรุงกฎหมายเหล่านี้ต่อไปในอนาคต เพราะการพัฒนาการในด้านนี้ยังเป็นเรื่องใหม่สำหรับประเทศไทย เหล่าผู้ประกอบการในประเทศไทยจึงควรติดตามกฎหมายด้านนี้อย่างใกล้ชิด เพื่อจะได้รับมือกับความเปลี่ยนแปลงต่อไปได้อย่างทันท่วงที

งานวิจัยที่เกี่ยวข้อง

นพดล นิ่มหนู (2564) การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อศึกษาเปรียบเทียบหลักการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย โดยเฉพาะอย่างยิ่งตามกฎหมายสองฉบับคือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลพ.ศ.2562 กับพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ว่ามีมาตรฐานในการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลเป็นไปตามมาตรฐานสากลหรือไม่ โดยใช้การดำเนินการวิจัยเชิงคุณภาพ(Qualitative Research) ในรูปแบบการวิจัยเอกสาร (Documentary Research) ผลการศึกษาพบว่า หลักการคุ้มครองข้อมูลส่วนบุคคลของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ที่มีฐานะเป็นกฎหมายกลาง กำหนดหลักการคุ้มครองข้อมูลส่วนบุคคลในลักษณะทั่วไปครอบคลุมทุกมิตินั้นได้รับอิทธิพลจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) ทำให้มีมาตรฐานในการคุ้มครองสิทธิทัดเทียมกับนานาอารยะประเทศ แต่สำหรับในส่วนของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 มีหลักการคุ้มครองข้อมูลส่วนบุคคลเป็นการเฉพาะ มุ่งเน้นคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความควบคุมดูแลของหน่วยงานภาครัฐ ยังมีประเด็นปัญหาเกี่ยวกับหลักการคุ้มครองข้อมูลอยู่หลายประการ ไม่ว่าจะเป็นเรื่องของการเก็บรักษาข้อมูล การกำหนดให้มีเจ้าหน้าที่ควบคุมข้อมูล การประมวลผลและการใช้ข้อมูลส่วนบุคคล ซึ่งมาตรฐานยังแตกต่างจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ผู้วิจัยจึงเสนอให้มีการทำการทบทวนหลักการและแก้ไขบทบัญญัติเพื่อให้กฎหมายทั้งสองฉบับมีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลเป็นไปในทิศทางเดียวกันโดยไม่เกิดภาวะสองมาตรฐาน

นิกร โภคอุดม (2563) บทความวิชาการนี้มีวัตถุประสงค์ในการให้ความรู้เกี่ยวกับความเป็นส่วนตัวของข้อมูล ซึ่งความเป็นส่วนตัวของข้อมูล นั้นเกี่ยวข้องกับความสัมพันธ์ระหว่างการรวบรวมและการเผยแพร่ ข้อมูล เทคโนโลยี ความคาดหวังของประชาชนเกี่ยวกับความเป็นส่วนตัว และความรู้เกี่ยวกับกฎหมายความเป็นส่วนตัว โดยเกี่ยวข้องกับกฎระเบียบการจัดเก็บและการใช้ข้อมูลส่วนบุคคล ข้อมูลด้านสุขภาพส่วนบุคคลและข้อมูลทางการเงินของบุคคล ซึ่งรัฐบาล องค์กรเอกชน หรือบุคคลอื่นสามารถรวบรวมได้ และยังหมายถึงข้อมูลใช้ในภาคธุรกิจเช่นความลับทางการค้า เพื่อเป็นการป้องกันปัญหาเรื่องความเป็นส่วนตัวของข้อมูลรั่วไหลสหภาพยุโรปจึงได้ออกกฎหมายการคุ้มครองข้อมูลส่วนบุคคล เรียกว่า "GDPR" (EU General Data Protection Regulation-G DPR) เพื่อกำหนดให้องค์กรต่าง ๆ ต้องมีมาตรกรรักษาความปลอดภัยของข้อมูลที่จัดเก็บไว้ ซึ่งประเทศไทยได้นำกฎหมายนี้มาเป็นแนวทางสำหรับออกเป็นกฎหมายเพื่อการคุ้มครองข้อมูลส่วนบุคคลของประชาชนในประเทศเรียกว่า "พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 " และอธิบายแนวทางการปฏิบัติให้กับองค์กร และเจ้าของข้อมูลซึ่งสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

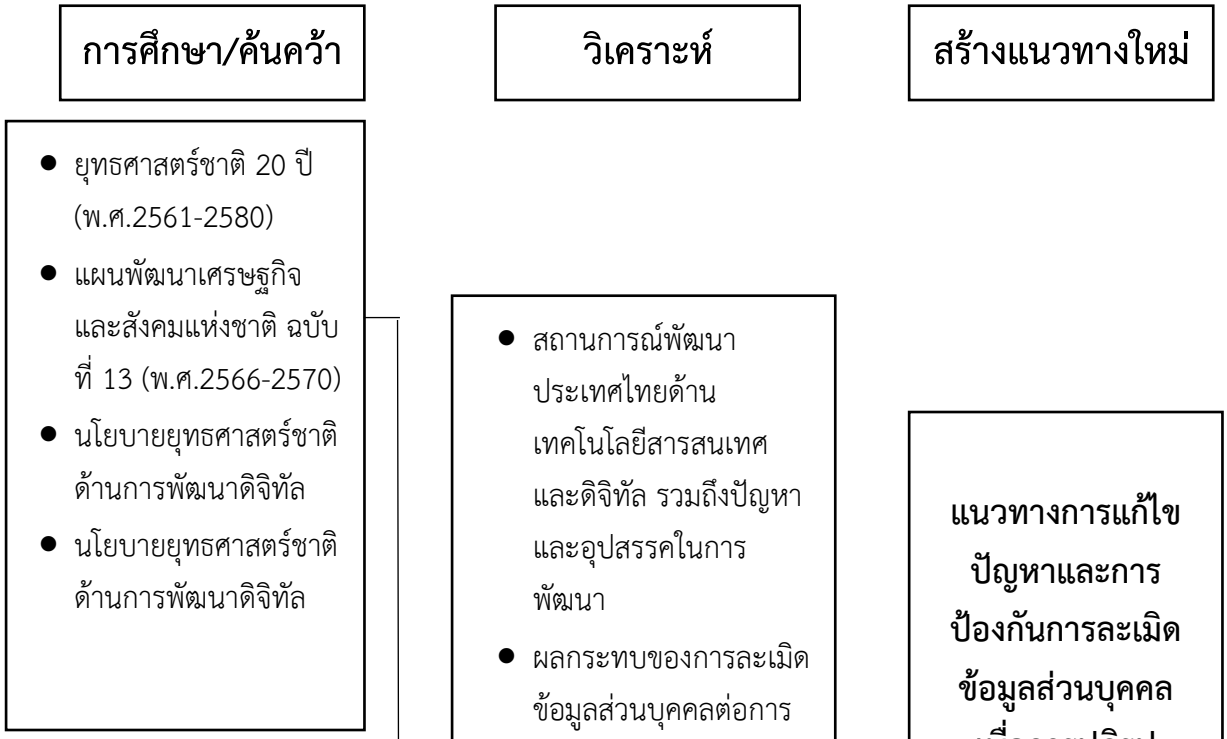
จันทร์ทิพย์ แสงแปง (2559) การวิจัยนี้มุ่งเน้นศึกษาปัญหาการจัดเก็บข้อมูลส่วนบุคคลในหน่วยงานเอกชน ตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ศึกษาแนวทางการคุ้มครองข้อมูลส่วนบุคคลใน ประเทศต่าง ๆ ที่มีการคุ้มครองข้อมูลส่วนบุคคลจากหน่วยงานเอกชนที่ชัดเจน เช่น ประเทศแคนาดา ประเทศสวีเดน และประเทศญี่ปุ่น เป็นต้น และศึกษาแนวทางการคุ้มครองข้อมูลส่วนบุคคลใน มาตรฐานสากล รวมถึงวิเคราะห์ปัญหาและแนวทางในการจัดเก็บข้อมูลส่วนบุคคลในหน่วยงาน เอกชน เนื่องจากในปัจจุบันมีเทคโนโลยีที่ช่วยให้หน่วยงานเอกชนสามารถเก็บรวบรวมข้อมูล ประมวลข้อมูล และส่งผ่านข้อมูลส่วนบุคคลได้อย่างสะดวกและรวดเร็ว ซึ่งเป็นประโยชน์อย่างมากต่อ การวิเคราะห์ วิจัย ทำสถิติ และอีกหลากหลายกิจกรรม แต่ในทางกลับกัน ก็ทำให้เกิดการละเมิด ข้อมูลส่วนบุคคลได้โดยง่าย เกิดการรั่วไหลของข้อมูลส่วนบุคคลเข้าสู่มือของมิจฉาชีพ หรือธุรกิจที่แอบแฝงผลประโยชน์ต่าง ๆ เช่นเดียวกัน

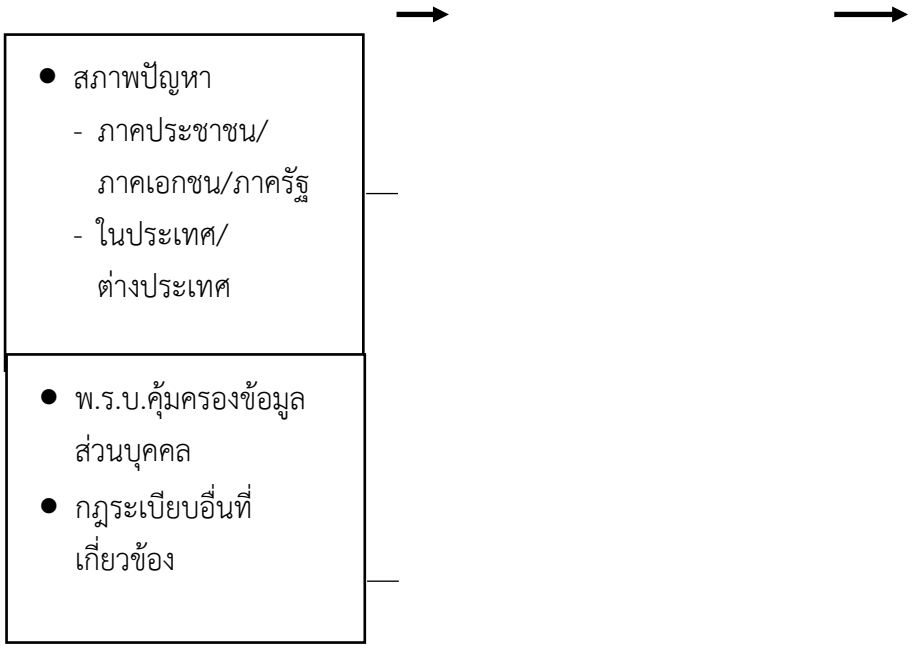
จากการศึกษาร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... และแนวทางการคุ้ม ครองข้อมูลส่วนบุคคลในต่างประเทศพบว่า ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ยัง ขาดความชัดเจนในเรื่องการขอความยินยอมในการจัดเก็บข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคลโดยตรง และการแจ้งวัตถุประสงค์ในการจัดเก็บข้อมูล กล่าวคือ ปัญหาการจัดเก็บข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมของเจ้าของข้อมูล ซึ่งทำให้หน่วยงานเอกชนสามารถจัดเก็บข้อมูลส่วนบุคคล โดยที่ไม่ได้รับความยินยอมของเจ้าของข้อมูลก่อน เพียงแค่แจ้งให้เจ้าของข้อมูลทราบเท่านั้น ส่งผลให้เกิดการรั่วไหลของข้อมูลส่วนบุคคลที่เป็นอยู่ในปัจจุบัน ทำให้กระจายข้อมูลเป็นยังแหล่งอื่นได้โดยง่าย และปัญหาการจัดเก็บข้อมูลส่วนบุคคลโดยไม่แจ้งวัตถุประสงค์ในการจัดเก็บข้อมูลนั้น ทำให้หน่วยงานเอกชนสามารถเก็บข้อมูลส่วนบุคคลได้ โดยที่ไม่แจ้งวัตถุประสงค์ในการจัดเก็บข้อมูลหรือไม่ กำหนดวัตถุประสงค์ในการจัดเก็บข้อมูลให้ชัดเจน หรือนำข้อมูลไปใช้เกินกว่ากรอบของวัตถุประสงค์ที่เคยกำหนดไว้ เป็นต้น ซึ่งล้วนแล้วแต่เป็นการละเมิดสิทธิส่วนบุคคล ทั้งสิ้น โดยอาศัยความคลุมเครือของกฎหมายทำให้ประชาชนทั่วไปได้รับผลกระทบในการถูกละเมิดสิทธิส่วนบุคคล

ด้วยเหตุดังกล่าว ผู้วิจัยเห็นว่าร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... จึงควรแก้ไขเพิ่มเติมในมาตรา 22 เพื่อกำหนดหลักการขอความยินยอมในการจัดเก็บข้อมูลส่วนบุคคลจากแหล่งอื่น ซึ่งไม่ใช่เจ้าของข้อมูลโดยตรงและกำหนดหลักการแจ้งวัตถุประสงค์ในการจัดเก็บข้อมูลให้ชัดเจนเพื่อให้สอดคล้องกับมาตรฐานสากล

ภาระวี ปุณเสรีพิพัฒน์ (2557) การละเมิดข้อมูลส่วนบุคคลโดยใช้เทคโนโลยีอย่างคุกกี้ (cookie) ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น เป็นปัญหาสำคัญที่ทั่วโลกตระหนักถึงและให้ความสนใจ กฎหมายจึงมีบทบาทสำคัญ และมีความจำเป็นในการคุ้มครองความปลอดภัยของข้อมูลส่วนบุคคลในการดำเนินธุรกรรมอิเล็กทรอนิกส์ให้มีประสิทธิภาพและครอบคลุมมากยิ่งขึ้น บทความวิจัยนี้มีวัตถุประสงค์เพื่อที่จะหาคำตอบว่า มาตรการทางกฎหมายของประเทศไทยตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลนั้นเพียงพอต่อการคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมอิเล็กทรอนิกส์หรือไม่ผลการวิจัยพบว่าร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลนั้นเป็นการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป ไม่ได้แยกบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมอิเล็กทรอนิกส์ไว้ต่างหาก อย่างในมาตรการทางกฎหมายของต่างประเทศ จึงส่งผลถึงประสิทธิภาพในการคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมอิเล็กทรอนิกส์ที่ยังไม่ชัดเจนและครอบคลุมเพียงพอ ข้อเสนอแนะของการวิจัยจึงเห็นว่าร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลดังกล่าวควรมีการแยกประเภท เพื่อคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมอิเล็กทรอนิกส์เป็นการเฉพาะ

กรอบแนวคิดของการวิจัย





สรุป

บทนี้ได้นำเสนอทฤษฎีที่เกี่ยวข้องกับแนวคิดเกี่ยวกับแนวทางการแก้ไขปัญหาและการป้องกันการละเมิดข้อมูลส่วนบุคคลเพื่อการปฏิรูปประเทศไทยสู่ดิจิทัลไทยแลนด์ ซึ่งในการศึกษาครั้งนี้ผู้วิจัยได้นำเรื่อง นโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมที่เป็นแผนหลักในการพัฒนาเศรษฐกิจและสังคมดิจิทัลของประเทศไทย ระยะ 20 ปี ยุทธศาสตร์แผนปฏิบัติการด้านข้อมูลส่วนบุคคล กฎหมายที่เกี่ยวข้องและงานวิจัยที่เกี่ยวข้องเพื่อนำมาเป็นกรอบในการศึกษาวิเคราะห์วิธีพิจารณาแนวทางการแก้ไขปัญหาและการป้องกันเพื่อปฏิรูปประเทศไทยสู่ดิจิทัลไทยแลนด์ โดยมีประเด็นสำคัญเกี่ยวกับการละเมิดข้อมูลส่วนบุคคล เพื่อมากำหนดกรอบในการสร้างประเด็นคำถามตามวัตถุประสงค์ของงานวิจัย และนำไปสู่แนวทางการแก้ไขปัญหาและการป้องกันการละเมิดข้อมูลส่วนบุคคลเพื่อการปฏิรูปประเทศไทยสู่ดิจิทัลไทยแลนด์

บทที่ 3
สถานการณ์ การดำเนินการ และปัญหา อุปสรรคด้านการแก้ไขปัญหาการละเมิดข้อมูลส่วนบุคคล

ในบทที่ 3 นี้ผู้วิจัยนำเสนอผลการวิจัยตามวัตถุประสงค์ ข้อที่ 1 และ 2 ดังนี้

1. เพื่อศึกษาสถานการณ์และแนวโน้มการละเมิดข้อมูลส่วนบุคคลผ่านระบบดิจิทัลและผลกระทบต่อการพัฒนาประเทศ

2. เพื่อศึกษาปัญหาและอุปสรรคในการดำเนินการแก้ไขปัญหาและผลกระทบการละเมิดข้อมูลส่วนบุคคลผ่านเทคโนโลยีดิจิทัล

โดยจะนำเสนอผลการวิจัยตามหัวข้อดังนี้

1. สถานการณ์ทั่วไปและแนวโน้มการละเมิดข้อมูลส่วนบุคคลผ่านระบบดิจิทัลในปัจจุบัน

2. พัฒนาการในการแก้ไขปัญหาและผลกระทบการละเมิดข้อมูลส่วนบุคคล

3. ปัญหาและอุปสรรคในการดำเนินการแก้ไขปัญหาและผลกระทบการละเมิดข้อมูลส่วนบุคคลผ่านเทคโนโลยีดิจิทัล

4. สรุป

สถานการณ์ทั่วไปและแนวโน้มการละเมิดข้อมูลส่วนบุคคลผ่านระบบดิจิทัลในปัจจุบัน

ผู้วิจัยได้รวบรวมข้อมูลจากการศึกษาเอกสารต่างๆและรายงานการวิจัยที่เกี่ยวข้องผลการวิจัยมีดังนี้

1. สถานการณ์ทั่วไปของการละเมิดข้อมูลส่วนบุคคลผ่านระบบดิจิทัลในปัจจุบัน

ประเทศไทยได้มีการปฏิรูปสู่สังคมดิจิทัลหรือดิจิทัลไทยแลนด์ตามนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมที่เป็นแผนหลักในการพัฒนาเศรษฐกิจและสังคมดิจิทัลของประเทศไทย ระยะ 20 ปี (พ.ศ.2561-2580) รัฐบาลให้ความสำคัญในการนำเทคโนโลยีดิจิทัลมาช่วยในการขับเคลื่อนเศรษฐกิจและสังคม ทั้งการพัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูงให้ครอบคลุมทั่วประเทศ การขับเคลื่อนเศรษฐกิจด้วยเทคโนโลยีดิจิทัล การปรับเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัลส่งผลให้เกิดการนำเทคโนโลยีไปใช้ในการดำเนินกิจการของทุกภาคส่วน เพิ่มประสิทธิภาพในการดำเนินงาน เพิ่มความสามารถในการแข่งขันทางการค้า การอำนวยความสะดวกและยกคุณภาพชีวิตให้ประชาชน มีการผลักดันให้เกิดการเปลี่ยนแปลงรูปแบบการทำธุรกรรมจากระบบกระดาษเป็นระบบดิจิทัล ผลกระทบที่ตามมาจากความเจริญของ

เทคโนโลยีทำให้การติดต่อสื่อสารสามารถเดินทางติดต่อสื่อสารถึงกันได้ทั่วทุกมุมของโลกอย่างไร้ขีดจำกัดคือการแย่งชิงกันครอบครองข้อมูลเพื่อให้มีข้อมูลมาใช้ประโยชน์ในกิจการของตนเองให้มากที่สุด เพื่อการมีโอกาสและมีอิทธิพลอำนาจเหนือกว่าผู้อื่น ซึ่งข้อมูลเหล่านี้จะมีข้อมูลข่าวสารส่วนหนึ่งที่เป็นข้อมูลส่วนบุคคลรวมอยู่ด้วย จึงทำให้เกิดปัญหาตามมาคือมีการนำข้อมูลส่วนบุคคลไปใช้โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลทำให้เกิดปัญหาการละเมิดความเป็นส่วนตัวในข้อมูลส่วนบุคคลเป็นวงกว้างอยู่ในขณะนี้และเนื่องจากการพัฒนาด้านเทคโนโลยีสารสนเทศเติบโตอย่างรวดเร็ว ทำให้สามารถจัดเก็บรวบรวมข้อมูลข่าวสารต่าง ๆ ได้เป็นจำนวนมากและสามารถเรียกดู ตรวจสอบ วิเคราะห์ ประมวลผล เผยแพร่ รับ – ส่งแลกเปลี่ยนข้อมูลได้อย่างสะดวกและรวดเร็วให้เกิดผลกระทบต่อความเป็นส่วนตัวคือการนำข้อมูลส่วนบุคคลไปใช้ประมวลผลหรือเปิดเผยทำให้ผู้เป็นเจ้าของข้อมูลอาจได้รับความเสียหาย เช่นเรื่องของความปลอดภัยในชีวิต และทรัพย์สิน สิทธิและเสรีภาพของบุคคลของเจ้าของข้อมูล ผลกระทบต่อการทำธุรกรรมของบุคคล

ดังนั้น เพื่อเป็นการแก้ไขปัญหาการละเมิดข้อมูลส่วนบุคคล ประเทศไทยจึงมีกฎหมายเกี่ยวกับการคุ้มครองข้อมูลข่าวสารส่วนบุคคลโดยเฉพาะคือพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act B.E. 2562 (2019)) หรือกฎหมาย PDPA ทั้งนี้ได้เริ่มบังคับใช้ตั้งแต่ในวันที่ 1 มิถุนายน 2565 พระราชบัญญัติฯ ฉบับนี้มีลักษณะเป็นกฎหมายกลางที่ครอบคลุมการดำเนินการของบุคคลหรือนิติบุคคลที่เป็นหน่วยงานภาครัฐและภาคเอกชนที่ทำการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลต้องปฏิบัติตามหลักเกณฑ์ วิธีการ และเงื่อนไขตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดส่งผลทำให้ทุกภาคส่วนทั้งประชาชนทั่วไป บริษัทเอกชนและหน่วยงานภาครัฐต่างๆ ต้องมีความเข้าใจต่อกฎหมายอย่างถูกต้อง เข้าใจวิธีการดูแลเรื่องความปลอดภัยข้อมูลส่วนบุคคลและการปฏิบัติตามหลักเกณฑ์ข้อกำหนดที่ถูกต้องตามกฎหมายฉบับนี้ต่อไป

จากการศึกษาวิจัยโดยการวิเคราะห์เอกสารงานวิจัยและเอกสารที่เกี่ยวข้องกับการละเมิดข้อมูลส่วนบุคคลหลังการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ผลการวิจัยมีดังนี้

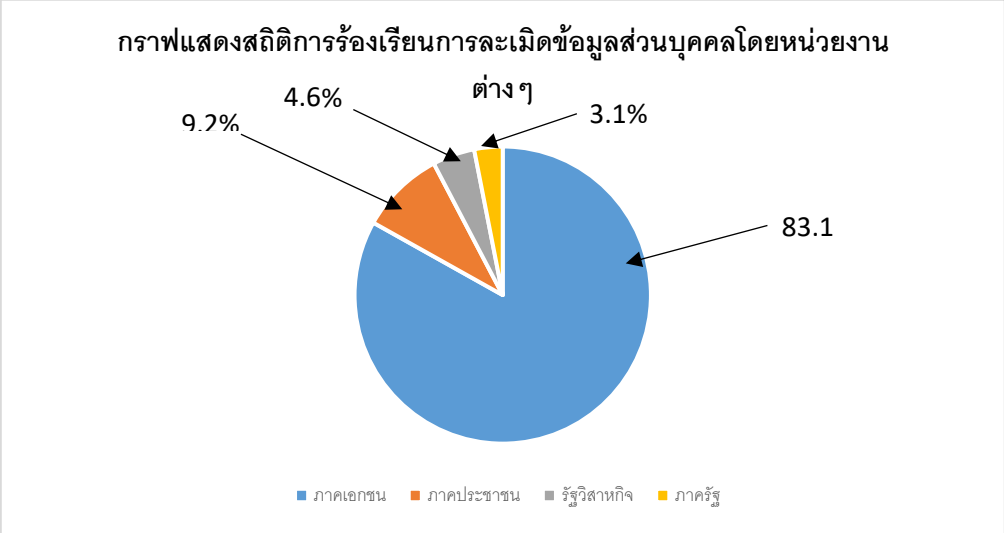
ในปัจจุบันประเทศไทยมีหน่วยงานที่ทำหน้าที่กำกับดูแลคุ้มครองข้อมูลส่วนบุคคลคือสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ซึ่งเป็นองค์กรอิสระตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หมวด 1 มาตรา 8 ที่ได้กำหนดไว้ว่าให้มีคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล อันประกอบด้วย ประธานกรรมการ รองประธานกรรมการ กรรมการผู้ทรงคุณวุฒิ เลขาธิการเป็นกรรมการและเลขานุการ

หลังพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล หรือกฎหมาย PDPA (Personal Data Protection Act B.E. 2562) ประกาศใช้อย่างเป็นทางการเมื่อวันที่ 1 มิถุนายน 2565 ที่ผ่านมาทางสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ได้นำเสนอสถิติการรับเรื่องร้องเรียนและสอบถามทางโทรศัพท์เรื่อง PDPA โดยมีการจัดระยะเวลาทั้งหมด 1 ปี ในระหว่างวันที่ 1 ตุลาคม

2564 – 15 พฤศจิกายน 2565 โดยทาง สคส. รายงานว่าใน 1 ปีที่ผ่านมามีผู้ร้องเรียนสูงถึง 2,246 ครั้ง โดยหัวข้อร้องเรียนที่ทาง สคส.รับเรื่องจัดอันดับได้ดังนี้ (สถิติในวันที่ 1 ตุลาคม 2564 – 15 พฤศจิกายน 2565)

1. ร้องเรียนเรื่องการบังคับให้ความยินยอมเพื่อเปิดใช้บริการ
2. การถูกเก็บข้อมูลส่วนบุคคลมาจากแหล่งอื่นโดยมิชอบ
3. ไม่เปิดให้ใช้สิทธิขอรับสำเนาข้อมูลหรือลบข้อมูลตามกฎหมาย
4. เรื่องการใช้และเปิดเผยข้อมูลระหว่างบุคคลธรรมดา

แผนภาพที่ 3 - 1 แสดงสถิติข้อมูลการละเมิดข้อมูลส่วนบุคคล



ที่มา : สำนักงานคุ้มครองข้อมูลส่วนบุคคล, 2565.

จากสถิติที่ทางสำนักงานคุ้มครองข้อมูลส่วนบุคคลในช่วงวันที่ 1 ตุลาคม 2564 – 15 พฤศจิกายน 2565 ดังแผนภาพที่ 3 - 1 จะเห็นได้ว่า หน่วยงานเอกชนได้มีการถูกร้องเรียนในเรื่องการฝ่าฝืนกฎหมาย PDPA อยู่ในกลุ่มที่สูงที่สุด ถึง 83.1% ลำดับถัดมาคือประชาชนอยู่ที่ 9.2% หน่วยงานรัฐวิสาหกิจ 4.6% และหน่วยงานรัฐเพียง 3.1% โดยเหตุผลส่วนใหญ่ที่มีการละเมิดการคุ้มครองข้อมูลส่วนบุคคลนั้น มีสาเหตุมาจากการที่บุคลากรขององค์ขาดความรู้และความเข้าใจในด้านกฎหมาย PDPA รวมไปถึงกระบวนการทำงานขององค์กรมีการไหลเวียนข้อมูลส่วนบุคคลเป็นส่วนใหญ่ แต่ไม่มีการดำเนินงานให้ถูกต้องและครบกระบวนการ ทั้งนี้สาเหตุการละเมิดที่ได้รับแจ้งสาเหตุส่วนใหญ่ที่สำนักงานคุ้มครองข้อมูลส่วนบุคคล (2565) รวบรวมได้ มีดังต่อไปนี้

1. ระบบคอมพิวเตอร์ขององค์กรถูกเจาะระบบ
2. กระบวนการควบคุมขั้นตอนการเปิดเผยข้อมูลส่วนบุคคลขององค์กรไม่รัดกุม
3. พนักงานดำเนินการผิดพลาด ส่งข้อมูลให้ผู้รับผิดคน

ทั้งนี้แนวโน้มสถิติของการละเมิดข้อมูลส่วนบุคคลจะมีทิศทางมากขึ้น เนื่องจากประชาชนโดยทั่วไปไม่มีความรู้ความเข้าใจต่อกฎหมายฉบับนี้มากพอ และการรั่วไหลของข้อมูลจากหน่วยงานต่างๆยังคงสร้างตวามกังวลให้กับเจ้าของข้อมูล

สรุปได้ว่า ประเทศไทยมีกฎหมายเกี่ยวกับการคุ้มครองข้อมูลข่าวสารส่วนบุคคล โดยเฉพาะคือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ทั้งนี้ได้เริ่มบังคับใช้ตั้งแต่ในวันที่ 1 มิถุนายน 2565 พระราชบัญญัติฯ ฉบับนี้ มีลักษณะเป็นกฎหมายกลางที่ครอบคลุมการดำเนินการของบุคคลหรือนิติบุคคลที่เป็นหน่วยงานภาครัฐและภาคเอกชนที่ทำการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลต้องปฏิบัติตามหลักเกณฑ์ วิธีการ และเงื่อนไขตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนด แต่จากการดำเนินการที่ผ่านมาหลังการประกาศใช้พระราชบัญญัติดังกล่าวสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นองค์กรอิสระตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้รับเรื่องการถูกร้องเรียนในเรื่องการฝ่าฝืนกฎหมาย เรื่องการบังคับให้ความยินยอมเพื่อเปิดใช้บริการ การถูกเก็บข้อมูลส่วนบุคคลมาจากแหล่งอื่นโดยมิชอบ ไม่เปิดให้ใช้สิทธิขอรับสำเนาข้อมูลหรือลบข้อมูลตามกฎหมาย และเรื่องการใช้และเปิดเผยข้อมูลระหว่างบุคคลธรรมดา เป็นต้น

2. ผลกระทบของการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

จากการวิเคราะห์ข้อมูลจากเอกสารและรายงานการวิจัย ผู้วิจัยได้วิเคราะห์ผลกระทบของการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ดังนี้

2.1 ผลกระทบในแง่ภาระต้นทุนทางธุรกิจของผู้ประกอบการ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(1) ซึ่งกำหนดหน้าที่ให้ผู้ควบคุมข้อมูลส่วนบุคคลจัดให้มีมาตรการการรักษาความปลอดภัยที่เหมาะสม นอกจากนี้มาตรา 40 ยังกำหนดหน้าที่ลักษณะเดียวกันให้กับผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งรวมถึงผู้ให้บริการต่าง ๆ ที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้บริการ เช่น การรับฝากข้อมูล การจ้างวิเคราะห์ข้อมูล เป็นต้น หลักการดังกล่าวส่งผลให้ผู้ประกอบธุรกิจต้องลงทุนในหลายมิติ เช่น ระบบเครือข่ายซอฟต์แวร์เกี่ยวกับการรักษาความปลอดภัยของข้อมูลการจ้างที่ปรึกษาทางเทคนิคและบุคลากรเกี่ยวกับความปลอดภัยทางคอมพิวเตอร์และเมื่อมี การละเมิดข้อมูลส่วนบุคคลเกิดขึ้น ต้องมีการแจ้งต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและการแจ้งต่อเจ้าของข้อมูล หลักการนี้ส่งผลให้เกิดภาระต้นทุนการทำให้สอดคล้องกับกฎหมาย เช่น ก่อนการแจ้งต้องมีการประเมินสถานการณ์ ตรวจสอบข้อเท็จจริงและหลักฐานทางอิเล็กทรอนิกส์ (Forensic) ซึ่งต้องอาศัยงบประมาณและการจ้างผู้เชี่ยวชาญ รวมทั้งต้นทุนในการปฏิบัติการส่งข้อมูลการแจ้งต่าง ๆ ดังนั้นผู้ประกอบการขนาดใหญ่ย่อมได้เปรียบกว่าผู้ประกอบการขนาดกลางและขนาดย่อม (SMEs) ในด้านของงบประมาณการลงทุนระบบการคุ้มครองข้อมูลส่วนบุคคลทั้งในด้านทรัพยากรบุคล เทคโนโลยีที่นำมาใช้

2.2 ผลกระทบต่อการแข่งขันทางการค้าที่ไม่เป็นธรรม

จากปัญหาการละเมิดข้อมูลส่วนบุคคลส่งผลให้ประเทศไทยต้องมีการคุ้มครองข้อมูลส่วนบุคคลทำให้เป็นข้อได้เปรียบของธุรกิจขนาดใหญ่ซึ่งมีงบประมาณเพื่อการนี้เช่นการอัพเกรดระบบป้องกันการจ้างผู้เชี่ยวชาญด้านความปลอดภัย การร่างสัญญาและนโยบาย แต่จะสร้างความ

เสียเปรียบแก่ผู้ประกอบการขนาดกลางและย่อม (SMEs) ที่มีต้นทุนต่ำกว่า การสร้างความเชื่อมั่นด้วยการมีระบบการคุ้มครองข้อมูลส่วนบุคคลที่ได้มาตรฐาน อาจเกิดสถานการณ์เช่นเดียวกับต่างประเทศคือหลังจากกฎหมายสหภาพยุโรปที่เป็นกฎหมายการคุ้มครองข้อมูลส่วนบุคคล (GDPR) ใช้บังคับในปี ค.ศ. 2018 (Bjorn, 2018) ธุรกิจขนาดกลางและย่อมในสหรัฐอเมริกา ที่ได้รับผลกระทบจากกฎหมาย GDPR ได้แก่ ธุรกิจการโฆษณาออนไลน์ (Ad tech) ธุรกิจเกี่ยวกับการวิเคราะห์ข้อมูลในสื่อสังคมออนไลน์ (social media analytics) (Russel, 2018) ธุรกิจเกี่ยวกับการติดตามข้อมูลเพื่อการโฆษณา (Ad tracking) หลายแห่งปิดตัวเพราะได้รับผลกระทบ ธุรกิจเกี่ยวกับเกมส์ออนไลน์ ความบันเทิงออนไลน์ ต้องมีการยุติการให้บริการเมื่อพิจารณาชั่งน้ำหนักกับต้นทุนที่จะต้องปฏิบัติให้สอดคล้องกับกฎหมายสหภาพยุโรป ดังนั้นประเทศไทยก็อาจมีแนวโน้มที่จะเกิดสถานการณ์เดียวกับในประเทศยุโรปก็เป็นได้ในการที่จะเกิดปัญหาความเหลื่อมล้ำไม่เป็นธรรมทางการค้า

2.3 ผลกระทบในแง่การค้าและการลงทุนระหว่างประเทศ

การละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นในประเทศอยู่บ่อยครั้งซึ่งถ้าประเทศไทยไม่สามารถที่จะป้องกันและแก้ไขปัญหาดังกล่าวด้วยการมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลเช่นเดียวกับต่างประเทศได้ย่อมส่งผลต่อความเชื่อมั่นต่อประเทศคู่ค้าได้ ทำให้เกิดผลกระทบที่ตามมาคือเรื่องของการค้าและการลงทุน ทั้งนี้เพราะต้องมีการส่งข้อมูลข้ามแดนกัน แต่ขณะเดียวกันข้อกฎหมายดังกล่าวสามารถส่งผลต่อธุรกิจต่างๆในการมีภาระต้นทุนที่สูงขึ้นจากการที่ต้องมีระบบการคุ้มครองข้อมูลส่วนบุคคลที่เป็นไปตามกฎหมายของประเทศนั้นๆ

2.4 ผลกระทบในการสร้างโอกาสให้เกิดการโจรกรรมข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 30 - 34 ซึ่งให้สิทธิเจ้าของข้อมูลหลายประการในด้านของผู้ประกอบการที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ปฏิบัติตามกฎหมาย โดยจัดให้มีระบบและการตอบสนองต่อการใช้สิทธิของเจ้าของข้อมูลในการยื่นคำร้องต่าง ๆ ดังนั้นผลกระทบทางลบดังกล่าวสามารถเกิดขึ้นกับผู้มีส่วนได้เสียต่าง ๆ ในประเทศไทยได้ เช่น วิธีการวิศวกรรมทางสังคม (Social engineering) การแสวงหาข้อมูลจากแหล่งต่าง ๆ เช่น สื่อสังคมออนไลน์ สามารถนำไปประกอบในการปลอมตัว (Impersonate) เป็นเจ้าของข้อมูลและยื่นคำร้องต่อผู้ควบคุมข้อมูลขอใช้สิทธิเข้าถึงข้อมูล (Right of access) ส่งผลให้ผู้ปลอมตัวได้มาซึ่งข้อมูลส่วนบุคคลอื่นของเจ้าของข้อมูลรวมถึงข้อมูลละเอียดอ่อน เช่น ข้อมูลธุรกรรม บัญชีการเงิน (Martino et al, 2019) เป็นต้น เจ้าของข้อมูลที่อาจตกเป็นเหยื่อของการโจรกรรมข้อมูลเอกลักษณ์ โดยอาชญากรปลอมตัวเป็นเจ้าของข้อมูลและแอบอ้างสิทธิยื่นคำร้องขอข้อมูลอื่น ๆ ของเจ้าของข้อมูล ทำให้สูญเสียด้านต่างๆทั้งข้อมูลส่วนบุคคล การเงิน เกิดความสูญเสียทางเศรษฐกิจ เป็นต้น

2.5 ผลกระทบต่อสิทธิเสรีภาพของบุคคล

จากการทบทวนวรรณกรรมจะเห็นได้ว่าสิทธิในความเป็นอยู่ส่วนตัวเป็นกรอบแนวคิดพื้นฐานของกฎหมายคุ้มครองข้อมูลส่วนบุคคล อย่างไรก็ตามองค์ประกอบและเงื่อนไขของ

กฎหมายคุ้มครองข้อมูลส่วนบุคคล อาจส่งผลกระทบทางลบต่อสิทธินี้ เช่น การสร้างโอกาสให้กับอาชญากรรมที่ส่งผลต่อความเป็นส่วนตัวของเจ้าของข้อมูลดังกล่าวที่มาแล้ว รวมทั้งการที่ผู้ประกอบการใช้วิธีการปฏิบัติเพื่อให้สอดคล้องกับกฎหมายด้วยเทคนิคต่าง ๆ อันส่งผลให้เจ้าของข้อมูลมีความเสี่ยงต่อการถูกล่วงละเมิดข้อมูลส่วนบุคคลมากขึ้น นอกจากนั้นยังกระทบต่อสิทธิในการแสดงความคิดเห็น เช่น กรณีสิทธิของเจ้าของข้อมูลในการขอให้ลบหรือ ทำลายข้อมูลระบุตัวของตน (Right to erase or right to be forgotten) เปิดทางให้มีการใช้เพื่อ วัตถุประสงค์อื่น (Abuse) เช่น เพื่อปิดกั้นการวิพากษ์วิจารณ์แสดงความคิดเห็น นอกจากนี้บุคคลสาธารณะ หรือภาครัฐอาจอาศัยกลไกดังกล่าวเพื่อปิดกั้นเนื้อหาผิดกฎหมาย (Illegal content) ของประเทศหนึ่ง ซึ่งไม่ผิดกฎหมายประเทศอื่น เช่น การร้องขอต่อผู้ประกอบการสื่อออนไลน์เพื่อให้ปิดกั้นข้อมูลที่ผิดกฎหมายประเทศหนึ่งจากการเข้าถึงได้ในประเทศอื่น ๆ (The International Association of Privacy Professionals (IAPP), 2018)

สรุปได้ว่า การประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 นอกจากมีผลดีต่อการที่ข้อมูลส่วนบุคคลจะได้รับการคุ้มครองไม่ให้มีการนำไปใช้ให้เกิดความเสียหายต่อตัวบุคคลหรือองค์กรแล้ว ยังอาจส่งผลกระทบทางลบเกิดขึ้นได้เช่นกัน ได้แก่ภาระต้นทุนทางธุรกิจของผู้ประกอบการที่เพิ่มขึ้น การแข่งขันทางการค้าที่ไม่เป็นธรรม ผลกระทบในแง่การค้าและการลงทุนระหว่างประเทศ การสร้างโอกาส ให้เกิดการโจรกรรมข้อมูลส่วนบุคคล ผลกระทบต่อสิทธิเสรีภาพของบุคคล เป็นต้น

พัฒนาการในการแก้ไขปัญหาและผลกระทบการละเมิดข้อมูลส่วนบุคคล

ผู้วิจัยได้ทำการศึกษาวิวัฒนาการการแก้ไขปัญหาและผลกระทบการละเมิดข้อมูลส่วนบุคคลตั้งแต่อดีตจนถึงปัจจุบันจากเอกสารต่าง ๆ ผลการศึกษามีดังนี้

1. พัฒนาการในการแก้ไขปัญหาและผลกระทบการละเมิดข้อมูลส่วนบุคคล

ตั้งแต่ในอดีตประเทศไทยมีการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล เริ่มมีการกำหนดไว้ในรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2535 (แก้ไขเพิ่มเติม พ.ศ. 2538) โดยได้บัญญัติคุ้มครอง “สิทธิในความเป็นส่วนตัว” ไว้ในมาตรา 47 และต่อมามีการนำมาบัญญัติไว้ในรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 มาตรา 34 เพื่อเป็นการกำหนดยืนยันหลักการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวว่า “สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียงหรือความเป็นอยู่ส่วนตัวย่อมได้รับความคุ้มครอง การกล่าวหรือไขข่าว แพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชนอันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัวจะกระทำมิได้ เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณชน” บทบัญญัติมาตรานี้นำไปสู่ความพยายามตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลขึ้นทั้งในส่วนที่อยู่ในความครอบครองของทางภาคราชการและภาคเอกชน ซึ่งในส่วนทางภาคราชการได้มีการตราพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 โดยช่วงระยะเวลาในระหว่างที่ประเทศไทยยังไม่มีกฎหมายกลางนั้น ประเทศไทยก็ได้มีการตรากฎหมายเฉพาะอื่น ๆ ออกมาหลายฉบับ เพื่อ

คุ้มครองสิทธิในความเป็นอยู่ส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในบางเรื่อง (ในรูปแบบ กฎหมายเฉพาะ) เช่น พระราชบัญญัติการประกอบธุรกิจข้อมูลบัตรเครดิต พ.ศ. 2545 คุ้มครองสิทธิของเจ้าของข้อมูลเครดิต พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 คุ้มครองสิทธิของเจ้าของข้อมูลประวัติสุขภาพ หรือพระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544 คุ้มครองสิทธิของเจ้าของข้อมูลในการติดต่อสื่อสารระหว่างกันของบุคคล ฯลฯ เป็นต้น จนกระทั่งถึงวันที่ 28 พฤษภาคม พ.ศ. 2562 ก็ได้มีการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ออกมาใช้บังคับในที่สุด ซึ่งจะเห็นได้ว่าพัฒนาการทางกฎหมายที่จะกำหนดหลักการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลมีพัฒนาการที่ล่าช้ามาก เพราะพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลที่ได้มีการริเริ่มที่จะตราขึ้นเป็นกฎหมายนับตั้งแต่ปี พ.ศ. 2540 กว่าจะตราขึ้นเป็นกฎหมายได้รวมระยะเวลากว่า 20 ปี

จากการรวบรวมข้อมูลพบว่า การตรากฎหมายขึ้นมาเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศไทยไม่ได้มีการตราไว้ในกฎหมายฉบับเดียว แม้ว่าจะมีพระราชบัญญัติข้อมูลข่าวสารของทางราชการพ.ศ. 2540 เป็นกฎหมายหลักแต่ก็มีขอบเขตของการคุ้มครองที่จำกัดไม่ได้ครอบคลุมไปถึงข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของภาคเอกชน ซึ่งมีปริมาณข้อมูลที่จัดเก็บเป็นจำนวนมากไม่น้อยไปกว่าข้อมูลที่อยู่กับภาครัฐ ไม่ว่าจะเป็นข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของ บรรดาธนาคารเอกชน โรงพยาบาลเอกชน โรงแรมห้างสรรพสินค้าหรือบรรษัทห้างร้านที่จำหน่ายสินค้า ผลิตภัณฑ์หรือให้บริการที่มีการจัดเก็บข้อมูลของลูกค้าไว้ เมื่อพิจารณาประกอบกับความก้าวหน้าทางด้านเทคโนโลยีอันได้อธิบายมาแล้วก็จะทำให้เห็นถึงความเสี่ยงที่จะมีการล่วงละเมิดสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลได้โดยง่าย โดยที่ระบบกฎหมายของไทยยังไม่สามารถให้ความคุ้มครองได้อย่างมีประสิทธิภาพ แต่อย่างไรก็ดีอย่างน้อยเราก็เห็นได้ถึงความพยายามของภาครัฐในอันที่จะใช้กฎหมายมหาชนเป็นเครื่องมือในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ซึ่งก็คือพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ที่รับหลักการมาจากบทบัญญัติของรัฐธรรมนูญ พ.ศ. 2540 มาตรา 34 และมาตรา 58 ซึ่งได้กำหนดหลักการคุ้มครองข้อมูลข่าวสารของบุคคลในฐานะที่เป็นส่วนหนึ่งของสิทธิส่วนบุคคลนั้นเอง

นพดล นิ่มหนู (2563) ได้นำเสนอผลการวิจัยเรื่องพัฒนาการของการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลในประเทศไทยซึ่งรายงานผลว่า ปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคลประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวมการใช้และการเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว สามารถทำได้โดยง่ายสะดวกและรวดเร็ว รวมทั้งก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวมที่ใช้เทคโนโลยีดิจิทัลอย่างแพร่หลาย แม้ว่าจะได้มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลในบางเรื่องแต่ก็ยังไม่มีหลักเกณฑ์กลไกหรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป สมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้นจากหลักการและเหตุผลข้างต้นจะเห็นได้ว่า เหตุผลสำคัญที่ประเทศไทยต้องตรากฎหมายคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวข้อมูลส่วนบุคคลฉบับนี้ ก็คือ

1. ก่อนหน้านี้ประเทศไทยยังไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลซึ่งทำให้ไม่มีหลักประกันในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ซึ่งเป็นสิทธิมนุษยชน

ขั้นพื้นฐาน ในขณะที่นานาอารยประเทศ ไม่ว่าจะเป็นประเทศในแถบยุโรป อเมริกาใต้ ได้มีการตรากฎหมายเพื่อมาคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลและวางระบบ การเยียวยาความเสียหายอันเกิดจากละเมิดเป็นที่เรียบร้อยแล้ว

2. จัดสร้างกลไกในการปกป้องสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล โดยพยายามรักษาดุลยภาพของการคุ้มครองสิทธิของบุคคลในความเป็นส่วนตัว (right of privacy) เสรีภาพในการไหลเวียนของข้อมูลข่าวสาร (free flow of Information) และความมั่นคงของประเทศ (national security) เพื่อเป็นโครงสร้างพื้นฐานสารสนเทศที่มั่นคงในช่วงระยะเวลาแห่งข้อมูลข่าวสาร ภายใต้หลักการปกครองระบอบประชาธิปไตยและหลักนิติรัฐ

3. เพื่อสนับสนุนการทำธุรกรรมทางอิเล็กทรอนิกส์ เนื่องในปัจจุบันการพัฒนาการทางเทคโนโลยีสารสนเทศมีความก้าวหน้าอย่างรวดเร็ว ทำให้มีการนำเอาเทคโนโลยีมาประยุกต์ใช้ให้เกิดประโยชน์กับเศรษฐกิจและสังคมมากมาย โดยเฉพาะการประมวลผลข้อมูลส่วนบุคคล อันสามารถทำได้อย่างสะดวกและรวดเร็ว จึงมีความจำเป็นออกกฎหมายมาคุ้มครองข้อมูลส่วนบุคคล ซึ่งมีการใช้อย่างแพร่หลายในยุคสังคมสารสนเทศ

จนกระทั่งวันที่ 28 พฤษภาคม พ.ศ. 2562 ก็ได้มีการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ออกมาใช้บังคับในที่สุด พระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ที่เรียกว่า PDPA ย่อมาจาก Personal Data Protection Act (B.E., 2562) เป็นกฎหมายว่าด้วยการให้สิทธิ์กับเจ้าของข้อมูลส่วนบุคคล สร้างมาตรฐานการรักษาข้อมูลส่วนบุคคลให้ปลอดภัย และนำไปใช้ให้ถูกวัตถุประสงค์ตามคำยินยอมที่เจ้าของข้อมูลส่วนบุคคลอนุญาต โดยกฎหมาย PDPA ได้ประกาศไว้ในราชกิจจานุเบกษาเมื่อวันที่ 27 พฤษภาคม 2562 และได้ถูกเลื่อนให้มีผลบังคับใช้ในวันที่ 1 มิถุนายน 2565 องค์กรต่าง ๆ จึงได้รับผลกระทบพอสมควรกับการประกาศใช้พระราชบัญญัติฉบับนี้ ทั้งนี้ต้องมีการเพิ่มมาตรฐานนโยบายการรักษาข้อมูลส่วนบุคคลให้ปลอดภัยและนำไปใช้ให้ถูกวัตถุประสงค์ตามคำยินยอมที่เจ้าของข้อมูลส่วนบุคคลได้ให้ไว้ และที่สำคัญต้องสอดคล้องต่อกฎหมายด้วย ทำให้กระบวนการทำการคุ้มครองข้อมูลส่วนบุคคลจะต้องมีการดำเนินการอย่างเป็นระบบ โดยเฉพาะองค์กรขนาดใหญ่ที่มีการเก็บรวบรวมข้อมูลส่วนบุคคลและมีการนำข้อมูลส่วนบุคคลไปใช้เป็นจำนวนมาก ผู้ควบคุมข้อมูลส่วนบุคคลจึงต้องมีการกำหนดนโยบายความปลอดภัยของข้อมูลส่วนบุคคลภายในองค์กรและให้ความรู้แก่บุคคลากรในองค์กร รู้ขอบเขตการเก็บรวบรวม การใช้ การเผยแพร่ข้อมูลส่วนบุคคล มีระบบการจัดเก็บข้อมูลส่วนบุคคลที่ปลอดภัย มีการจำกัดการเข้าถึงข้อมูลส่วนบุคคล มีการบันทึกกิจกรรมการใช้ข้อมูลส่วนบุคคล สิ่งเหล่านี้ล้วนจำเป็นอย่างยิ่งที่ผู้ควบคุมข้อมูลจะต้องปฏิบัติตามเพื่อให้สอดคล้องกับกฎหมายต่อไป

2. การจัดระบบการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานในปัจจุบัน

ผู้วิจัยได้ศึกษาการดำเนินการในการป้องกันการละเมิดข้อมูลส่วนบุคคลขององค์กรต่าง ๆ ทั้งภาครัฐ และภาคเอกชนพบว่าจากการดำเนินการที่ผ่านมามีระบบการคุ้มครองข้อมูลส่วนบุคคลที่คล้ายคลึงกัน ผู้วิจัยจึงได้ยกตัวอย่างการศึกษาระบบการป้องกันคุ้มครองข้อมูลของของสถาบันพระปกเกล้ามาเป็นกรณีศึกษาดังนี้

สถาบันพระปกเกล้า (2563) ได้นำเสนอกรอบการทำงานเป็นขั้นตอนของผู้ควบคุมข้อมูล (Data Controller) ตามมาตรา 37 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลพ.ศ. 2562

เรื่องหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งมีทั้งหมด 5 ข้อ ดังนี้ มาตรา 37 (1) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึงใช้ เปลี่ยนแปลง แก้ไขหรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป เพื่อให้มีประสิทธิภาพในการรักษา ความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ให้เป็นไปตามมาตรฐานขั้นต่ำตามประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563 ซึ่งมีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลครอบคลุม 3 ประเด็น ได้แก่

2.1 การธำรงไว้ซึ่งความลับ (confidentiality)

2.2 ความถูกต้องครบถ้วน (integrity)

2.3 สภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล

ทั้งนี้เพื่อป้องกันการสูญหาย เข้าถึงใช้ เปลี่ยนแปลง แก้ไขหรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ โดยดำเนินการ ดังนี้ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) คือบุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ “ตัดสินใจ” เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมกำหนด

1. แจ้งมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลและสร้างเสริมความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล ให้แก่บุคลากร พนักงาน ลูกจ้าง หรือบุคคลที่เกี่ยวข้องทราบ เพื่อให้ปฏิบัติตามมาตรการที่กำหนดอย่างเคร่งครัด

2. จัดให้มีมาตรการเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (access control) โดยอย่างน้อยต้องประกอบด้วย

2.1 การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผล

2.2 การกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล

2.3 การบริหารจัดการการเข้าถึงของผู้ใช้งานเพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตแล้ว

2.4 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งานเพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต

2.5 การจัดให้มีวิธีการตรวจสอบย้อนหลังการเข้าถึงข้อมูลส่วนบุคคลได้

รายละเอียดของมาตรการต่างๆที่เกี่ยวข้องกับระบบการคุ้มครองข้อมูลส่วนบุคคลมีดังนี้

1. มาตรการป้องกันด้านการบริหารจัดการ (administrative safeguard)

1.1 มีการออกระเบียบ วิธีปฏิบัติ สำหรับควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการ จัดเก็บและประมวลผลข้อมูลส่วนบุคคล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย มีการกำหนดบันทึกการเข้าออกพื้นที่ให้เจ้าหน้าที่รักษาความปลอดภัยตรวจสอบผู้มีสิทธิ

ผ่านเข้าออก โดยความเข้มข้นของมาตรการเป็นไปตามระดับความเสี่ยงหรือความเสียหายที่อาจเกิดขึ้นหากข้อมูลส่วนบุคคลรั่วไหล ถูกแก้ไข ถูกคัดลอก หรือ ถูกทำลายโดยมิชอบ

1.2 มีการกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของ ผู้ใช้งาน (user responsibilities) แบ่งเป็นรูปแบบต่าง ๆ เช่น สิทธิในการเข้าดู แก้ไขเพิ่มเติม เปิดเผยและเผยแพร่ การตรวจสอบคุณภาพข้อมูลตลอดจนการลบทำลาย

2. มาตรการป้องกันด้านเทคนิค (technical safeguard)

2.1. การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคลให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคล

2.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาต ตามระดับสิทธิการใช้งาน ได้แก่ การนำเข้าเปลี่ยนแปลง แก้ไข เปิดเผย ตลอดจนการลบทำลาย

2.3 จัดให้มีระบบสำรองและกู้คืนข้อมูล เพื่อให้ระบบ และ/หรือ บริการต่าง ๆ ยังสามารถดำเนินการได้อย่างต่อเนื่อง

3. มาตรการป้องกันทางกายภาพ (physical safeguard)

ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (access control)

3.1 มีการควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วน บุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย เช่น มีบันทึกการเข้าออกพื้นที่ มีเจ้าหน้าที่รักษาความปลอดภัยของพื้นที่ มีระบบกล้องวงจรปิดติดตั้ง มีการล็อคประตูทุกครั้ง มีระบบบัตรผ่านเฉพาะผู้มีสิทธิเข้าออก ทั้งนี้ความเข้มข้นของมาตรการให้เป็นไปตามระดับความเสี่ยง หรือความเสียหายที่อาจเกิดขึ้นหากข้อมูลส่วนบุคคลรั่วไหล ถูกแก้ไข ถูกคัดลอก หรือถูกทำลายโดยมิชอบ

3.2 กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล การลักลอบนำอุปกรณ์เข้าออก

3. มาตรการบทลงโทษทางกฎหมาย

การประกาศใช้พระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ซึ่งเป็นกฎหมายว่าด้วยการให้สิทธิ์กับเจ้าของข้อมูลส่วนบุคคล สร้างมาตรฐานการรักษาข้อมูลส่วนบุคคลให้ปลอดภัยและนำไปใช้ให้ถูกวัตถุประสงค์ตามคำยินยอมที่เจ้าของข้อมูลส่วนบุคคลอนุญาต โดยกฎหมายได้ประกาศไว้ในราชกิจจานุเบกษา เมื่อวันที่ 27 พฤษภาคม 2562 และได้ถูกเลื่อนให้มีผลบังคับใช้ในวันที่ 1 มิถุนายน 2565 พระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ที่บังคับใช้ในประเทศไทยนี้จะมีบทบาทในการคุ้มครองและให้สิทธิที่เราควรมีต่อข้อมูลส่วนบุคคลของเราเองได้ รวมไปถึงการสร้างมาตรฐานของบุคคลหรือนิติบุคคล ในการเก็บข้อมูลส่วนบุคคล, รวบรวมข้อมูลส่วนบุคคล, ใช้ข้อมูลส่วนบุคคล หรือเพื่อการเปิดเผยข้อมูลส่วนบุคคลก็ตาม ซึ่งล้วนแล้วเกี่ยวข้องกับพระราชบัญญัติฉบับนี้ที่จะต้องปฏิบัติตาม หากผู้ใดหรือองค์กรใดไม่ปฏิบัติตามย่อม

มีบทลงโทษตามกฎหมายตามมา ซึ่งบทลงโทษของพระราชบัญญัติฉบับนี้สำหรับผู้ที่ไม่ปฏิบัติตามนั้น มีทั้งโทษทางแพ่ง โทษทางอาญา และโทษทางปกครองด้วย

ถ้าไม่ปฏิบัติตามบทลงโทษของผู้ที่ไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (PDPA) มีถึง 3 ประเภท ได้แก่

3.1 โทษทางแพ่ง

โทษทางแพ่งกำหนดให้ชดใช้ค่าสินไหมทดแทนที่เกิดขึ้นจริงให้กับเจ้าของข้อมูลส่วนบุคคลที่ได้รับความเสียหายจากการละเมิด และอาจจะต้องจ่ายบวกเพิ่มอีกเป็นค่าค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มเติมสูงสุดได้อีก 2 เท่าของค่าเสียหายจริง ตัวอย่าง หากศาลตัดสินว่าให้ผู้ควบคุมข้อมูลส่วนบุคคล ต้องชดใช้ค่าสินไหมทดแทนแก่เจ้าของข้อมูลส่วนบุคคล เป็นจำนวน 1 แสนบาท ศาลอาจมีคำสั่งกำหนดค่าสินไหมเพื่อการลงโทษเพิ่มอีก 2 เท่าของค่าเสียหายจริง เท่ากับว่าจะต้องจ่ายเป็นค่าปรับทั้งหมด เป็นจำนวนเงิน 3 แสนบาท

3.2 โทษทางอาญา

โทษทางอาญาจะมีทั้งโทษจำคุกและโทษปรับ โดยมี โทษจำคุกสูงสุดไม่เกิน 1 ปี หรือปรับไม่เกิน 1 ล้านบาท หรือทั้งจำทั้งปรับ โดยโทษสูงสุดดังกล่าวจะเกิดจากการไม่ปฏิบัติตาม PDPA ในส่วนการใช้ข้อมูล หรือเปิดเผยข้อมูล หรือส่งโอนข้อมูลไปยังต่างประเทศ ประเภทข้อมูลที่มีความละเอียดอ่อน(Sensitive Personal Data) ส่วนกรณีหากผู้กระทำความผิดคือ บริษัท (นิติบุคคล) ก็อาจจะสงสัยว่าใครจะเป็นผู้ถูกจำคุก เพราะบริษัทติดคุกไม่ได้ ในส่วนตรงนี้ก็อาจจะตกมาที่ผู้บริหาร กรรมการ หรือบุคคลซึ่งรับผิดชอบในการดำเนินงานของบริษัทนั้น ๆ ที่จะต้องได้รับการลงโทษจำคุกแทน

3.3 โทษทางปกครอง

โทษปรับมีตั้งแต่ 1 ล้านบาทจนถึงสูงสุดไม่เกิน 5 ล้านบาท ซึ่งโทษปรับสูงสุด 5 ล้านบาท จะเป็นกรณีของการไม่ปฏิบัติตาม PDPA ในส่วนการใช้ข้อมูล หรือเปิดเผยข้อมูล หรือส่งโอนข้อมูลไปยังต่างประเทศของประเภทข้อมูลที่มีความละเอียดอ่อน (Sensitive Personal Data) ซึ่งโทษทางปกครองนี้จะแยกต่างหากกับการชดใช้ค่าเสียหายที่เกิดจากโทษทางแพ่งและโทษทางอาญาด้วย

ปัญหาและอุปสรรคในการดำเนินการแก้ไขปัญหาและผลกระทบการละเมิดข้อมูลส่วนบุคคลผ่านเทคโนโลยีดิจิทัล

จากการศึกษาข้อมูลจากเอกสารและวิเคราะห์บทสัมภาษณ์เชิงลึกของผู้ที่มีส่วนเกี่ยวข้อง ผลการวิจัยในประเด็นปัญหาและอุปสรรคในการดำเนินการแก้ไขปัญหาและผลกระทบการละเมิดข้อมูลส่วน บุคคลผ่านเทคโนโลยีดิจิทัล มีดังนี้

1. ปัญหาความไม่ชัดเจนของกฎหมาย

จากการศึกษาเอกสารพบว่ามีความไม่ชัดเจนบางมาตราในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ดังนี้

1.1 ประเด็นการขอความยินยอมในการจัดเก็บข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคลโดยตรง

จากการศึกษาพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และแนวทางการคุ้มครองข้อมูลส่วนบุคคลในต่างประเทศพบว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังขาดความชัดเจนในเรื่องการขอความยินยอมในการจัดเก็บข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคลโดยตรงและการแจ้งวัตถุประสงค์ในการจัดเก็บข้อมูลกล่าวคือปัญหาการจัดเก็บข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมของเจ้าของข้อมูล ซึ่งทำให้หน่วยงานเอกชนสามารถจัดเก็บข้อมูลส่วนบุคคลโดยที่ไม่ได้รับความยินยอมของเจ้าของข้อมูลก่อนเพียงแค่แจ้งให้เจ้าของข้อมูลทราบเท่านั้น ส่งผลให้เกิดการรั่วไหลของข้อมูลส่วนบุคคลที่เป็นอยู่ในปัจจุบัน ทำให้กระจายข้อมูลเป็นยังแหล่งอื่นได้โดยง่ายและปัญหาการจัดเก็บข้อมูลส่วนบุคคลโดยไม่แจ้งวัตถุประสงค์ในการจัดเก็บข้อมูลนั้นทำให้หน่วยงานเอกชนสามารถเก็บข้อมูลส่วน บุคคลได้ โดยที่ไม่แจ้งวัตถุประสงค์ในการจัดเก็บข้อมูลหรือไม่กำหนดวัตถุประสงค์ในการจัดเก็บข้อมูลให้ ชัดเจนหรือนำข้อมูลไปใช้เกินกว่ากรอบของวัตถุประสงค์ที่เคยกำหนดไว้เป็นต้น ซึ่งล้วนแล้วแต่เป็นการละเมิดสิทธิส่วนบุคคลทั้งสิ้น โดยอาศัยความคลุมเครือของกฎหมายทำให้ประชาชนทั่วไปได้รับผลกระทบในการถูกละเมิดสิทธิส่วนบุคคล

อภิปรายว่า จากปัญหาความไม่ชัดเจนของกฎหมายในส่วนการขอความยินยอมในการจัดเก็บข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคลโดยตรงและการแจ้งวัตถุประสงค์ในการจัดเก็บข้อมูลนั้นได้สอดคล้องกับงานวิจัยของจันทร์ทิพย์ แสงแปง (2559) ที่ได้ทำการศึกษาปัญหาการคุ้มครองข้อมูลส่วนบุคคล ศึกษากรณีการจัดเก็บข้อมูลส่วนบุคคลในหน่วยงานเอกชนแล้วพบว่าร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ยังขาดความชัดเจนในเรื่องการขอความยินยอมในการจัดเก็บข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคลโดยตรง ดังนั้นจึงควรแก้ไขเพิ่มเติมในมาตรา 22 เพื่อกำหนดหลักการขอความยินยอมในการจัดเก็บข้อมูลส่วนบุคคลจากแหล่งอื่นซึ่งไม่ใช่เจ้าของข้อมูลโดยตรงและกำหนดหลักการแจ้งวัตถุประสงค์ในการจัดเก็บข้อมูลให้ชัดเจนเพื่อให้สอดคล้องกับมาตรฐานสากล

1.2 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นกฎหมายใหม่ที่มีการประกาศใช้ทำให้เมื่อนำมาใช้อาจมีการตีความไม่ได้ชัดเจนในบางมาตรา เช่น ตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 39 วรรคสาม บัญญัติว่าเว้นแต่มีการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือมิใช่กิจการที่เก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว หรือมีการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26 นั้น บทบัญญัติ ดังกล่าวมีความไม่ชัดเจนในเรื่องของ “ความเสี่ยงต่อสิทธิ เสรีภาพของเจ้าของมูลส่วนบุคคลและการเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว” เนื่องจากไม่มีหลักเกณฑ์กำหนดว่าการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลอย่างไรที่ถือว่าทำให้เกิดความเสี่ยงต่อสิทธิเสรีภาพหรือถือเป็นการเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราวทำให้เกิดปัญหาการตีความทางกฎหมายที่ไม่สอดคล้องกันก่อให้เกิดปัญหาแก่ผู้ที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลดังกล่าว

อภิปรายว่าความเห็นนี้สอดคล้องกับงานวิจัยของณฐพร วิริยะลัพภะและธเนศ สุจารีกุล (2563) ที่ได้ศึกษาปัญหาทางกฎหมายเกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

พ.ศ.2562 : ศึกษากรณีหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา39 ซึ่งผลการวิจัยพบว่าหน้าที่ของผู้ประกอบกิจการในการบันทึกข้อมูลส่วนบุคคลของลูกค้าและลูกจ้างเป็นภาระอย่างมากนับแต่กระบวนการบันทึกที่ใช้เทคนิคมีความซับซ้อน และมีความเสี่ยงที่ต้องรับผิดตามกฎหมาย ดังนั้นกิจการขนาดใหญ่และขนาดเล็กจำเป็นต้องจ้างผู้เชี่ยวชาญทั้งด้านกฎหมายและเทคนิค เพื่อให้คำปรึกษาในกระบวนการบันทึก แม้ว่ากฎหมายจะมีบทบัญญัติผ่อนปรนให้กิจการขนาดเล็กก็ตาม แต่บทบัญญัติส่วนนี้ยังคงมีปัญหาในวลีที่ไม่มีความชัดเจน เช่นกิจการขนาดเล็กอาจได้รับการยกเว้นจากหน้าที่ผู้ประกอบการกิจการมีหน้าที่บันทึกเพียงข้อมูลซึ่ง “มีความเสี่ยง” ที่จะกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลอย่างไรก็ตามปัญหาอาจเกิดจากวลีที่ว่า “อาจได้รับยกเว้น” และ “มีความเสี่ยง” มีความหมายอย่างไร ซึ่งความไม่ชัดเจนของวลีทั้งสองดังกล่าวก่อให้เกิดความไม่แน่นอนและความกังวลกับบุคคลทุกฝ่ายที่เกี่ยวข้อง ด้วยเหตุดังกล่าวจึงมีความเห็นว่าบทบัญญัติบางส่วนโดยเฉพาะอย่างยิ่งวลีทั้งสองข้างต้นควรได้รับการแก้ไขให้มีความชัดเจนเพื่อให้การตีความกฎหมายเป็นไปในทางเดียวกัน

2. ปัญหาการยกเว้นทางกฎหมายให้กับการใช้ข้อมูลส่วนบุคคลในหน่วยงานของรัฐ

เขมภัทร ทฤษฎีคุณ (2565) กล่าวว่าหลังจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ใช้บังคับคณะรัฐมนตรีได้มีมติและเห็นชอบหลักการของพระราชกฤษฎีกายกเว้นการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ให้กับการใช้ข้อมูลส่วนบุคคลในหน่วยงานของรัฐ เพื่อวัตถุประสงค์ในการป้องกันประเทศ การรักษาความมั่นคงของประเทศ ความปลอดภัยสาธารณะ การจัดเก็บภาษีของหน่วยงานรัฐ การดำเนินการเพื่อประโยชน์สาธารณะ การดำเนินการตามพันธกรณีระหว่างประเทศ การดำเนินการของหน่วยงาน ศาล อัยการ และผู้บังคับใช้กฎหมาย ซึ่งขอบเขตของการยกเว้นดังกล่าวค่อนข้างกว้าง และอาจกระทบต่อสิทธิและเสรีภาพของประชาชน รวมทั้งเศรษฐกิจของประเทศ ในด้านสิทธิและเสรีภาพของประชาชนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ช่วยลดการแทรกแซงสิทธิความเป็นส่วนตัวและคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล โดยการกำหนดมาตรฐานและวิธีการในการใช้ข้อมูลส่วนบุคคล การยกเว้นการบังคับใช้พระราชบัญญัตินั้นมีความน่ากังวลในประเด็นนี้ 2 เรื่อง

2.1 ขอบเขตของการยกเว้น ซึ่งตามร่างพระราชกฤษฎีกานี้มีการยกเว้นการนำกฎหมายมาใช้ในเรื่องสำคัญๆ ได้แก่ การคุ้มครองข้อมูลส่วนบุคคล สิทธิของเจ้าของข้อมูลส่วนบุคคล การร้องเรียน ความรับผิดทางแพ่งและบทกำหนดโทษ โดยเปิดโอกาสให้หน่วยงานของรัฐลอยนวลพ้นผิดจากการละเมิดสิทธิของเจ้าของข้อมูลส่วนบุคคลในรูปแบบต่างๆ

2.2 วัตถุประสงค์ของการยกเว้น อาทิ การรักษาความมั่นคงของประเทศ ความปลอดภัยสาธารณะ และการดำเนินการเพื่อประโยชน์สาธารณะนั้นมีความไม่เฉพาะเจาะจง และไม่อาจคาดหมายได้ว่าจะมีความหมายเช่นไรขึ้นกับดุลยพินิจและการตีความของหน่วยงานรัฐ ซึ่งข้อยกเว้นดังกล่าวนั้นขยายออกไปจากข้อยกเว้นเดิมที่กฎหมายกำหนดไว้

อภิปรายว่า การยกเว้นการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ให้กับการใช้ข้อมูลส่วนบุคคลในหน่วยงานของรัฐยิ่งอาจจะทำให้มีปัญหาให้หน่วยงานของรัฐใช้หรือเข้าถึงข้อมูลส่วนบุคคลโดยปราศจากความรับผิดชอบและกลายเป็นการซ้ำเติมปัญหาการพ้นผิดเมื่อเกิดการละเมิดข้อมูลส่วนบุคคลของภาครัฐและบั่นทอนความเชื่อมั่นของประชาชนถ้ามีการรั่วไหลของข้อมูลจากภาครัฐ

3. ปัญหาข้อกฎหมายในการเคลื่อนย้ายข้อมูลส่วนบุคคลข้ามพรมแดน

เขมภัทร ทฤษฎีคุณ (2565) กล่าวว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ทำหน้าที่สำคัญในฐานะเป็นส่วนหนึ่งของกฎหมายเศรษฐกิจดิจิทัลที่กำหนดหลักเกณฑ์และวิธีการเคลื่อนย้ายข้อมูลส่วนบุคคลข้ามพรมแดน ซึ่งเป็นหัวใจสำคัญของเศรษฐกิจสมัยใหม่ที่มีความจำเป็นต้องมีการเคลื่อนย้ายข้อมูลส่วนบุคคลข้ามพรมแดน ดังจะเห็นได้จากกรอบความตกลงทางเศรษฐกิจต่าง ๆ เช่น RCEP หรือ CPTPP ที่กำหนดให้ประเทศภาคีต้องรับรองหลักการดังกล่าว หลักการสำคัญของการเคลื่อนย้ายข้อมูลส่วนบุคคลข้ามพรมแดนนั้นให้ความสำคัญกับการส่งข้อมูลส่วนบุคคลของประเทศผู้รับข้อมูลส่วนบุคคลนั้นจะต้องมีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอไม่น้อยกว่าประเทศผู้ส่งข้อมูลส่วนบุคคล ทั้งนี้ GDPR หรือ General Data Protection Regulation ของสหภาพยุโรปกำหนดว่ามาตรฐานที่เพียงพอนี้ รวมถึงการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายจะต้องไม่ถูกแทรกแซงโดยรัฐหรือหน่วยงานด้านความมั่นคงของรัฐซึ่งเป็นหลักการพื้นฐานของรัฐที่เป็นนิติรัฐที่มุ่งคุ้มครองสิทธิและเสรีภาพของประชาชน

อภิปรายว่า ดังนั้นผลของพระราชกฤษฎีการยกเว้นการบังคับใช้กฎหมาย PDPA ให้กับการใช้ข้อมูลส่วนบุคคลในหน่วยงานของรัฐเปิดช่องให้สามารถตีความรวมถึงไม่ได้รับรองสิทธิของเจ้าของข้อมูลส่วนบุคคลเอาไว้ก็อาจจะทำให้ประเทศไทยไม่ได้รับการยอมรับว่าเป็นประเทศที่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เท่าเทียมกันกับสหภาพยุโรป นอกจากนี้อิทธิพลของ GDPR ได้สร้างมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลใหม่ทั่วโลก หากประเทศไทยไม่มีมาตรฐานเทียบเท่า GDPR ก็จะมีผลให้ประเทศไทยไม่มีมาตรฐานเทียบเท่ากับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศอื่น ซึ่งทำให้การเคลื่อนย้ายข้อมูลส่วนบุคคลเข้ามาในประเทศไทยทำได้ยากและทำให้เอกชนของประเทศไทยอาจจะพลาดโอกาสในการเติบโตในยุคเศรษฐกิจดิจิทัล

4. ปัญหาการร้องเรียนการละเมิดข้อมูลส่วนบุคคล

เนื่องจากในปัจจุบันพบว่ามีการร้องเรียนจากประชาชนจำนวนมากว่าองค์กรต่าง ๆ มิได้ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลทั้งการร้องเรียนองค์กรภาครัฐ ภาคเอกชน รัฐวิสาหกิจ และภาค ประชาชนเอง โดยทำการร้องเรียนไปยังคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือหน่วยงานที่มีอำนาจ กำกับดูแลที่ได้รับการแต่งตั้งโดยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือตามกฎหมาย

อภิปรายว่า ปัญหาการร้องเรียนการละเมิดข้อมูลส่วนบุคคลนี้มีแนวโน้มจะเพิ่มขึ้น ทั้งนี้ก่อนการร้องเรียนดังกล่าวหน่วยงานต่างๆที่ถูกร้องเรียนไม่มีโอกาสได้รับทราบข้อเท็จจริงและได้มีโอกาสชี้แจงในประเด็นต่าง ๆ รวมถึงจัดการแก้ไขก่อนในโอกาสแรก จากช่วง 1 ปีหลังมีการ

ประกาศใช้คือตั้งแต่เดือนตุลาคม 2564 – 15 พฤศจิกายน 2565 พบว่ามีการร้องเรียนโดยการสอบถามทางโทรศัพท์จำนวนทั้งหมด 2,246 ครั้ง โดยมีประเด็นการร้องเรียนคือบังคับให้ความยินยอมเพื่อเปิดใช้บริการ เก็บข้อมูลมาจากแหล่งอื่นโดยมิชอบไม่เปิดให้ใช้สิทธิขอรับสำเนาข้อมูลหรือลบข้อมูลตามกฎหมาย เรื่องการใช้และเปิดเผยข้อมูลระหว่างบุคคลธรรมดา (สำนักงานคุ้มครองข้อมูลส่วนบุคคล, 2565) ทั้งนี้ สคส. รายงานเพิ่มเติมว่านอกจากการร้องเรียนทางโทรศัพท์แล้ว ตั้งแต่ 1 มิถุนายน 2565 มีองค์กรแจ้งเหตุละเมิดโดยทำเป็นหนังสือและส่งมาที่ สคส. แล้ว โดยมีประเด็นดังนี้

1. หน่วยงานที่แจ้งเหตุมีทั้งหน่วยงานของรัฐและหน่วยงานเอกชน
2. เหตุการณ์ละเมิดที่ได้รับแจ้งมีทั้งกรณี cyber และ non-cyber

สาเหตุส่วนใหญ่ ได้แก่

1. ระบบคอมพิวเตอร์ขององค์กรถูกเจาะระบบ
2. กระบวนการควบคุมขั้นตอนการเปิดเผยข้อมูลส่วนบุคคล ขององค์กรไม่รัดกุม
3. พนักงานดำเนินการผิดพลาด ส่งข้อมูลให้ผู้รับผิดคน

ซึ่งในปัญหาที่มีการร้องเรียน สคส. นั้นจะต้องมีการสอบข้อเท็จจริงดังกล่าว ดังนั้นมีความจำเป็นที่จะต้องสร้างความเข้าใจในกฎหมายฉบับนี้ให้กับหน่วยงานต่าง ๆ รวมทั้งประชนที่เป็นเจ้าของข้อมูลนั้น ๆ ด้วย

4. การขาดแคลนทรัพยากรที่จำเป็นต่อการปฏิบัติหน้าที่ตามกฎหมาย

จากการสัมภาษณ์เจ้าหน้าที่คุ้มครองข้อมูล ให้ข้อมูลว่าในปัจจุบันมีการขาดแคลนทรัพยากรที่จำเป็นต่อการปฏิบัติหน้าที่ตามกฎหมายโดยเฉพาะเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือ DPO (Data Protection Officer) และมีความไม่ชัดเจนในการกำหนดโครงสร้างการทำงานของ DPO ทั้งนี้การกำหนดคุณสมบัติของ DPO ที่เป็นมาตรฐานส่งผลให้เกิดปัญหาหลายประการกล่าวคือ DPO ขาดความเป็นอิสระในการปฏิบัติหน้าที่และเกิดความขัดแย้งทางผลประโยชน์ ไม่มีการกำหนดกระบวนการปรึกษาหารือระหว่างฝ่ายงานกับ DPO ที่ครอบคลุมทั้งกระบวนการใช้ข้อมูลส่วนบุคคล ขาดพนักงานที่มีความรู้ความเข้าใจและขาดเครื่องมือและเทคโนโลยีที่ใช้ในการรักษาความปลอดภัยของข้อมูล นอกจากนี้ยังพบว่าไม่มีการกำหนดระยะเวลาการทบทวนตำแหน่ง DPO สถานะทางกฎหมายของตำแหน่งผู้ช่วย DPO ตลอดจนวิธีการตรวจสอบการประมวลผลข้อมูลส่วนบุคคล

อภิปรายว่า ผลการวิจัยสอดคล้องกับของ อริยะ ตังสวานิช (2563) นิสิตหลักสูตรนิติศาสตร์ ปริญญามหาบัณฑิต สาขาวิชากฎหมายเอกชนและธุรกิจคณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ได้ศึกษาปัญหาการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในสถาบันการเงินภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พบว่า DPO จำเป็นต้องได้รับการสนับสนุนทรัพยากรในด้านต่าง ๆ เพื่อให้สามารถทำความเข้าใจและตรวจสอบกระบวนการประมวลผลขององค์กรเป็นไปตามกฎหมายได้อย่างครบถ้วน อีกทั้งการได้รับทรัพยากรที่เพียงพอยังส่งผลโดยตรงต่อความเป็นอิสระในการปฏิบัติหน้าที่ของ DPO จากการสัมภาษณ์พบว่า ในทางปฏิบัติ DPO และคณะทำงานภายในสถาบันการเงินต่าง ๆ ประสบปัญหาด้านทรัพยากรที่จำเป็นต่อการปฏิบัติหน้าที่ตามกฎหมาย

5. ประชาชนขาดความรู้และความเข้าใจในกฎหมาย

จากการสัมภาษณ์ประชาชนที่เป็นเจ้าของข้อมูลทั่วไปพบว่าเนื่องจากพระราชบัญญัติคุ้มครอง ข้อมูลส่วนบุคคล พ.ศ.2562 เป็นกฎหมายใหม่และมีรายละเอียดที่เกี่ยวข้องกับตัวบุคคลค่อนข้างมาก ทำให้ประชาชนขาดความรู้และความเข้าใจในตัวกฎหมายอย่างถ่องแท้ ดังนั้นในชีวิตประจำวันจึงเกิดความสับสนว่าเรื่องใดทำได้เรื่องใดทำไม่ได้ ตัวอย่างเช่น การโพสต์รูปตนเองแต่ติดบุคคลอื่นด้วย ถ้านำคลิปหรือรูปถ่ายที่ติดคนอื่นไปโพสต์ในโซเชียลมีเดียโดยบุคคลอื่นไม่ยินยอมจะผิดกฎหมาย เจ้าของข้อมูลส่วนบุคคลต้องให้ความยินยอมทุกครั้งก่อนนำข้อมูลไปใช้ เป็นต้น ทำให้เกิดประเด็นร้องเรียนมากมายหลังพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ประกาศใช้

อภิปรายว่า ประเด็นในส่วนที่เกี่ยวข้องกับชีวิตประจำวันของคนทั่วไป สำนักงานคณะกรรมการ คุ้มครองข้อมูลส่วนบุคคล กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมต้องมีการประชาสัมพันธ์ให้ประชาชนทั่วไป เข้าใจเพราะเป็นกฎหมายใหม่ ทำให้ประชาชนขาดความรู้และความเข้าใจต่อกฎหมายนี้ทำให้มีการร้องเรียนไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลในเรื่องต่าง ๆ

6. มาตรฐานรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลขององค์กรที่ไม่มีประสิทธิภาพเพียงพอ

มาตรฐานรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลขององค์กรที่ไม่มีประสิทธิภาพสามารถทำให้เกิดการหลุดรั่วของข้อมูลส่วนบุคคล สิ่งสำคัญที่ผู้ประกอบการในฐานะผู้ควบคุมข้อมูลส่วนบุคคลจะต้องให้ความสำคัญคือการกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่มีมาตรฐาน สามารถตรวจสอบและป้องกันการหลุดรั่วของข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพและเมื่อเกิดเหตุการณ์หลุดรั่วของข้อมูลส่วนบุคคลแล้วจะต้องมีมาตรการในการตรวจสอบ เพื่อให้พบเหตุดังกล่าวอย่างทันท่วงที เพื่อที่จะได้จำกัดความเสียหายที่อาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคล

อภิปรายว่า หลังพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ใช้มีการร้องเรียนไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลรายงานว่าหน่วยงานเอกชนได้มีการถูกร้องเรียนในเรื่องการฝ่าฝืนกฎหมาย PDPA อยู่ในกลุ่มที่สูงที่สุดถึง 83.1% ลำดับถัดมาคือประชาชนอยู่ที่ 9.2% หน่วยงานรัฐวิสาหกิจ 4.6% และหน่วยงานรัฐเพียง 3.1% โดยเหตุผลส่วนใหญ่ที่มีการละเมิดการคุ้มครองข้อมูลส่วนบุคคลนั้น มีสาเหตุมาจากการที่บุคลากรขององค์ขาดความรู้และความเข้าใจในด้านกฎหมาย PDPA รวมไปถึงกระบวนการทำงานขององค์กรมีการไหลเวียนข้อมูลส่วนบุคคลเป็นส่วนใหญ่แต่ไม่มีการดำเนินงานให้ถูกต้องและครบกระบวนการทำให้เกิดการรั่วไหลของข้อมูลส่วนบุคคล

7. ปัญหากฎหมายคุ้มครองข้อมูลส่วนบุคคลได้การเพิ่มภาระค่าใช้จ่ายให้ผู้ประกอบการธุรกิจ

จากการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ดังนั้นเพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพที่ผู้ประกอบการต้องมีการปฏิบัติตามกฎหมายซึ่งกระบวนการของบันทึกเริ่มตั้งแต่การจัดระบบข้อมูลโดยการรวบรวม วิเคราะห์จัดทำเป็นบันทึก

รายการข้อมูล ส่วนบุคคลให้เห็นลักษณะของกิจกรรมทั้งหมดที่กระทำต่อข้อมูลส่วนบุคคล จึงจำเป็นที่ต้องใช้ผู้เชี่ยวชาญด้านวิศวกรและทางด้านกฎหมาย สร้างภาระค่าใช้จ่ายจำนวนมากให้แก่ผู้ควบคุมข้อมูล ซึ่งส่วนใหญ่เป็นผู้ประกอบกิจการและกฎหมายไทยกำหนดโทษปรับทางปกครองไว้สูงถึง 1 ล้านบาท แม้กฎหมายยกเว้นหน้าที่จัดทำบันทึกให้กิจการขนาดเล็กก็ตามแต่เมื่อพิจารณาเงื่อนไขตามมาตรา 39 วรรคสามแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 แต่ก็ยังมีปัญหาการตีความในข้อบัญญัติที่อาจต้องมีการทบทวนกฎหมายและตีความกฎหมายกันใหม่ให้ชัดเจน

อภิปรายว่า ทำความความเข้าใจในข้อกฎหมายรวมถึงสิทธิและหน้าที่ในฐานะต่างๆ ไม่ว่าจะเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในส่วนขององค์กร ต้องมีการทำงานร่วมกันจากทุกฝ่าย รวมถึงมีการสื่อสารให้ลูกค้าได้รับทราบถึงผลกระทบที่อาจจะเกิดขึ้นด้วย ซึ่งแนวทางปฏิบัติตามกฎหมายจะมีประสิทธิภาพหรือไม่นั้น ความเข้าใจอย่างเดียวอาจไม่เพียงพอ ดังนั้นการมีที่ปรึกษาเข้าไปช่วยประเมินผลกระทบ วางกลยุทธ์ในการเตรียมความพร้อมและนำเทคโนโลยีเข้าไปช่วยในการบริหารจัดการข้อมูลอย่างมีประสิทธิภาพ จะช่วยให้องค์กรสามารถรับมือกับข้อกฎหมายฉบับนี้ได้อย่างสัมฤทธิ์ผลมากยิ่งขึ้น ซึ่งจำเป็นที่องค์กรต่างๆต้องมีการจัดสรรงบประมาณดำเนินการในส่วนการจัดทำระบบคุ้มครองข้อมูลส่วนบุคคล

สรุป

ปัจจุบันประเทศไทยใช้พระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ที่เรียกว่า PDPA ย่อมาจาก Personal Data Protection Act (B.E., 2562) เป็นกฎหมายว่าด้วยการให้สิทธิ์กับเจ้าของข้อมูลส่วนบุคคล สร้างมาตรฐานการรักษาข้อมูลส่วนบุคคลให้ปลอดภัย และนำไปใช้ให้ถูกวัตถุประสงค์ตามคำยินยอมที่เจ้าของข้อมูลส่วนบุคคลอนุญาต โดยกฎหมาย PDPA ได้ประกาศไว้ในราชกิจจานุเบกษาเมื่อวันที่ 27 พฤษภาคม 2562 และได้ถูกเลื่อนให้มีผลบังคับใช้ในวันที่ 1 มิถุนายน 2565 องค์กรต่าง ๆ จึงได้รับผลกระทบพอสมควรกับการประกาศใช้ PDPA ทั้งนี้ต้องมีการเพิ่มมาตรฐานนโยบายการรักษาข้อมูลส่วนบุคคลให้ปลอดภัยและนำไปใช้ให้ถูกวัตถุประสงค์ตามคำยินยอมที่เจ้าของข้อมูลส่วนบุคคลได้ให้ไว้ และที่สำคัญต้องสอดคล้องต่อ PDPA ด้วย ทำให้กระบวนการทำ PDPA จะต้องมีการดำเนินการอย่างเป็นระบบ โดยเฉพาะองค์กรขนาดใหญ่ที่มีการเก็บรวบรวมข้อมูลส่วนบุคคลและมีการนำข้อมูลส่วนบุคคลไปใช้เป็นจำนวนมาก ผู้ควบคุมข้อมูลส่วนบุคคลจึงต้องมีการกำหนดนโยบายความปลอดภัยของข้อมูลส่วนบุคคลภายในองค์กรและให้ความรู้แก่บุคคลากรในองค์กร รู้ขอบเขตการเก็บรวบรวม การใช้และการเผยแพร่ข้อมูลส่วนบุคคล มีระบบการจัดเก็บข้อมูลส่วนบุคคลที่ปลอดภัย มีการจำกัดการเข้าถึงข้อมูลส่วนบุคคล มีการบันทึกกิจกรรมการใช้ข้อมูลส่วนบุคคล สิ่งเหล่านี้ล้วนจำเป็นอย่างยิ่งที่ผู้ควบคุมข้อมูลจะต้องปฏิบัติตาม เพื่อให้สอดคล้องกับ PDPA ต่อไป

แต่จากการดำเนินการที่ผ่านมาหลังการประกาศใช้พระราชบัญญัติดังกล่าวสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นองค์กรอิสระตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้รับเรื่องการถูกร้องเรียนในเรื่องการฝ่าฝืนกฎหมาย เรื่องการบังคับให้ความยินยอมเพื่อเปิดใช้บริการ การถูกเก็บข้อมูลส่วนบุคคลมาจากแหล่งอื่นโดยมิชอบ ไม่เปิดให้ใช้สิทธิ

ขอรับสำเนาข้อมูลหรือลบข้อมูลตามกฎหมาย และเรื่องการใช้และเปิดเผยข้อมูลระหว่างบุคคลธรรมดา เป็นต้น ทั้งนี้การประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลพ.ศ.2562 นอกจากมีผลดีต่อการที่ข้อมูลส่วนบุคคลจะได้รับการคุ้มครองไม่ให้มีการนำไปใช้ให้เกิดความเสียหายต่อตัวบุคคลหรือองค์กรแล้ว ยังอาจส่งผลกระทบทางลบเกิดขึ้นได้เช่นกัน ได้แก่ภาระต้นทุนทางธุรกิจของผู้ประกอบการที่เพิ่มขึ้น การแข่งขันทางการค้าที่ไม่เป็นธรรม ผลกระทบในแง่การค้าและการลงทุนระหว่างประเทศ การสร้างโอกาสให้เกิดการโจรกรรมข้อมูลส่วนบุคคล ผลกระทบต่อสิทธิเสรีภาพของบุคคล เป็นต้น นอกจากนั้นจากการศึกษายังพบประเด็นปัญหาและอุปสรรค ได้แก่ ความไม่ชัดเจนของกฎหมายฉบับนี้ในบางมาตรา การยกเว้นทางกฎหมายให้กับการใช้ข้อมูลส่วนบุคคลในหน่วยงานของรัฐ มาตรฐานรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลขององค์กรที่ไม่มีประสิทธิภาพเพียงพอ การขาดแคลนทรัพยากรที่จำเป็นต่อการปฏิบัติหน้าที่ตามกฎหมาย กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้การเพิ่มภาระค่าใช้จ่ายให้ผู้ประกอบการธุรกิจ ประชาชนขาดความรู้และความเข้าใจในกฎหมาย ปัญหาการร้องเรียนการละเมิดข้อมูลส่วนบุคคล ดังนั้นจึงมีความจำเป็นในฝ่ายต่าง ๆ ที่เกี่ยวข้องกับการร่างกฎหมายต้องมีการทบทวนและแก้ไขกฎหมายให้มีความชัดเจนและครอบคลุมตามเจตนารมณ์ของกฎหมายฉบับนี้ต่อไป

บทที่ 4
แนวทางการแก้ไขปัญหาและการป้องกัน การละเมิดข้อมูลส่วนบุคคล

ในบทนี้ผู้วิจัยจะนำเสนอแนวทางการแก้ไขปัญหาและการป้องกันการละเมิดข้อมูลส่วนบุคคล โดยมีวัตถุประสงค์ในการศึกษาวิจัยข้อที่ 3 คือเพื่อศึกษาแนวทางการแก้ไขปัญหาและการป้องกันการละเมิดข้อมูลส่วนบุคคลในการพัฒนาประเทศสู่ดิจิทัลไทยแลนด์

แนวทางการแก้ไขปัญหาและการป้องกันการละเมิดข้อมูลส่วนบุคคล

ประเทศไทยได้ตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ PDPA ย่อมาจาก Personal Data Protection Act B.E. 2562 (2019) ซึ่งเป็นกฎหมายว่าด้วยการให้สิทธิ์กับเจ้าของข้อมูลส่วนบุคคล สร้างมาตรฐานการรักษาข้อมูลส่วนบุคคลให้ปลอดภัยและนำไปใช้ให้ถูกวัตถุประสงค์ตามคำยินยอมที่เจ้าของข้อมูลส่วนบุคคลอนุญาต โดยกฎหมาย PDPA ได้ประกาศไว้ในราชกิจจานุเบกษาเมื่อวันที่ 27 พฤษภาคม 2562 และได้ถูกเลื่อนให้มีผลบังคับใช้ในวันที่ 1 มิถุนายน 2565 เป็นต้นมา กฎหมาย PDPA ฉบับนี้มีบทบาทในการคุ้มครองและให้สิทธิที่ประชาชนที่ควรมีต่อข้อมูลส่วนบุคคลของตนเองได้ รวมไปถึงการสร้างมาตรฐานของบุคคลหรือนิติบุคคลในการเก็บข้อมูลส่วนบุคคล รวบรวมข้อมูลส่วนบุคคล ใช้ข้อมูลส่วนบุคคล หรือเพื่อการเปิดเผยข้อมูลส่วนบุคคลก็ตาม ซึ่งล้วนแล้วเกี่ยวข้องกับกฎหมายฉบับนี้ที่จะต้องปฏิบัติตาม หากผู้ใดหรือองค์กรใดไม่ปฏิบัติตามย่อมมีบทลงโทษตามกฎหมายตามมา ซึ่งบทลงโทษของกฎหมาย PDPA สำหรับผู้ที่ไม่ปฏิบัติตามนั้น มีทั้งโทษทางแพ่ง โทษทางอาญา และโทษทางปกครองด้วย ผู้วิจัยได้ศึกษาข้อมูลจากเอกสารและการให้สัมภาษณ์ผู้ที่เกี่ยวข้องทั้งเจ้าหน้าที่ภาครัฐ ภาคเอกชนและประชาชนทั่วไปถึงบทบาทการดำเนินการในการแก้ไขปัญหาและการป้องกันการละเมิดข้อมูลส่วนบุคคล ผลการศึกษาวิจัยที่ได้จากการศึกษาเอกสารต่าง ๆ และวิเคราะห์บทสัมภาษณ์เชิงลึกมีรายละเอียดดังนี้

1. การดำเนินการของภาครัฐ

1.1 สร้างความเข้าใจและความชัดเจนในบทบาทหน้าที่ของภาครัฐในฐานะผู้ควบคุมข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (Personal Data Protection Act; PDPA)

อภิปรายได้ว่า การสร้างความเข้าใจและความชัดเจนในบทบาทหน้าที่ของภาครัฐในฐานะผู้ควบคุมข้อมูลส่วนบุคคลตามกฎหมาย PDPA เป็นสิ่งสำคัญเพราะความไม่เข้าใจหรือไม่ชัดเจนในบทบาทของภาครัฐในฐานะผู้ควบคุมข้อมูลส่วนบุคคลตาม PDPA ทำให้เกิดปัญหาตามมาได้จากการที่มีสถิติในการที่ประชาชนถูกการละเมิดข้อมูลส่วนบุคคลจากหน่วยงานภาครัฐมีหลายกรณีมาก ทั้งนี้เพราะเจ้าหน้าที่ภาครัฐบางส่วนอาจเห็นว่าการคุ้มครองข้อมูลส่วนบุคคลเป็นหน้าที่ของสำนัก/กอง/กลุ่ม/แผนกหนึ่งในหน่วยงานของภาครัฐเป็นผู้รับผิดชอบ เช่น สำนักเทคโนโลยี

เป็นต้น จึงไม่ได้ให้ความสำคัญต่อเรื่องนี้เท่าที่ควร แต่ตามหลักการคือหน่วยงานภาครัฐจะต้องสร้างความเข้าใจให้กับเจ้าหน้าที่ทุกคนและยึดหลักปฏิบัติเดียวกันทั้งองค์กร นอกจากนั้นความเข้าใจที่ไม่ชัดเจนอาจทำให้เกิดปัญหาในทางปฏิบัติ อย่างเช่นหลังจาก PDPA มีการใช้บังคับ ทางคณะรัฐมนตรีได้มีมติและเห็นชอบหลักการของพระราชกฤษฎีกายกเว้นการบังคับใช้กฎหมาย PDPA ให้กับการใช้ข้อมูลส่วนบุคคลในหน่วยงานของรัฐ เพื่อวัตถุประสงค์ในการป้องกันประเทศ การรักษาความมั่นคงของประเทศ ความปลอดภัยสาธารณะ การจัดเก็บภาษีของหน่วยงานรัฐ การดำเนินการเพื่อประโยชน์สาธารณะ การดำเนินการตามพันธกรณีระหว่างประเทศ การดำเนินการของหน่วยงาน ศาล อัยการ และผู้บังคับใช้กฎหมาย ซึ่งขอบเขตของการยกเว้นดังกล่าวค่อนข้างกว้างและอาจกระทบต่อสิทธิและเสรีภาพของประชาชน รวมทั้งเศรษฐกิจของประเทศ เรื่องนี้สอดคล้องกับความคิดเห็นของเขมภัทร ทฤษฎีคุณ (2565) ในบทความเรื่องยกเว้น กฎหมาย ‘PDPA’ กับผลที่ตามมา โดยได้กล่าวว่า การยกเว้นการบังคับใช้ PDPA นั้นมีความน่ากังวลในประเด็นนี้ 2 เรื่อง เรื่องแรกคือขอบเขตของการยกเว้น ซึ่งตามร่างพระราชกฤษฎีกานี้มีการยกเว้นการนำกฎหมายมาใช้ในเรื่องสำคัญ ๆ ได้แก่

1. การคุ้มครองข้อมูลส่วนบุคคล สิทธิของเจ้าของข้อมูลส่วนบุคคล การร้องเรียน ความรับผิดทางแพ่ง และบทกำหนดโทษ โดยเปิดโอกาสให้หน่วยงานของรัฐลอยนวลพ้นผิดจากการละเมิดสิทธิของเจ้าของข้อมูลส่วนบุคคลในรูปแบบต่าง ๆ

2. วัตถุประสงค์ของการยกเว้น อาทิ การรักษาความมั่นคงของประเทศ ความปลอดภัยสาธารณะ และการดำเนินการเพื่อประโยชน์สาธารณะนั้นมีความไม่เฉพาะเจาะจง และไม่อาจคาดหมายได้ว่าจะมีความหมายเช่นไรขึ้นกับดุลยพินิจและการตีความของหน่วยงานรัฐ ซึ่งข้อยกเว้นดังกล่าวนั้นขยายออกไปจากข้อยกเว้นเดิมที่กฎหมายกำหนดไว้

ดังนั้น การยกเว้นการบังคับใช้กฎหมาย PDPA ยิ่งอาจจะทำให้มีปัญหาให้หน่วยงานของรัฐใช้หรือเข้าถึงข้อมูลส่วนบุคคลโดยปราศจากความรับผิดชอบและกลายเป็นการซ้ำเติมปัญหาวัฒนธรรมการลอยนวลพ้นผิดเมื่อเกิดการละเมิดข้อมูลส่วนบุคคล ดังนั้นภาครัฐจำเป็นต้องสร้างความตระหนักและความรู้ ความเข้าใจในการคุ้มครองข้อมูลส่วนบุคคลของประชาชนและจะต้องมีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอไม่น้อยกว่าประเทศผู้ส่งข้อมูลส่วนบุคคล GDPR หรือ General Data Protection Regulation ของสหภาพยุโรป กำหนดว่ามาตรฐานที่เพียงพอนี้รวมถึงการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายจะต้องไม่ถูกแทรกแซงโดยรัฐหรือหน่วยงานด้านความมั่นคงของรัฐ ซึ่งเป็นหลักการพื้นฐานของรัฐที่เป็นนิติรัฐที่มุ่งคุ้มครองสิทธิและเสรีภาพของประชาชน

1.2 หน่วยงานของภาครัฐต้องมีนโยบายและแนวปฏิบัติภายในหน่วยงานทุกหน่วยเพื่อรองรับการปฏิบัติตาม PDPA

อภิปรายได้ว่า เนื่องจากกฎหมาย PDPA เป็นกฎหมายใหม่ดังนั้นทุกหน่วยงานของภาครัฐต้องมีการเตรียมพร้อมรับนโยบายและจัดทำแนวปฏิบัติหรือแม้แต่การปรับเปลี่ยนกฎเกณฑ์ทางกฎหมายภายใต้อำนาจของหน่วยงานของรัฐ เพื่อให้สอดคล้องกับหลักการของกฎหมายคุ้มครองข้อมูลส่วนบุคคล PDPA ทั้งนี้ ต้องมีการเตรียมพร้อมเจ้าหน้าที่ภาครัฐให้มีความเข้าใจต่อการพิจารณาฐานทางกฎหมายในการปฏิบัติงานด้วย เมื่อขาดนโยบายและแนวปฏิบัติ จากการดำเนินงานการใช้กฎหมาย PDPA ที่ผ่านมาพบว่า เจ้าหน้าที่หน่วยงานของรัฐส่วนใหญ่ยังไม่มั่นใจว่าในภารกิจ

หรือกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของตนจะต้องใช้ฐานการประมวลผลข้อมูลส่วนบุคคลใด โดยเฉพาะอย่างยิ่งในมาตราที่กฎหมายห้ามไม่ให้เก็บรวบรวมข้อมูลส่วนบุคคล หากไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ซึ่งจะเป็นปัญหาสำหรับหน่วยงานของรัฐที่มีภารกิจต้องเก็บจากบุคคลเป็นจำนวนมาก เช่น ฐานข้อมูลทะเบียนราษฎร หรือฐานข้อมูลบัตรประจำตัวประชาชน เป็นต้น ทั้งนี้เจ้าหน้าที่รัฐอาจไม่มั่นใจว่าจะสามารถขอความยินยอมได้อย่างไร ซึ่งในความเป็นจริงแล้ว PDPA ได้ให้อำนาจหน่วยงานของรัฐในฐานการประมวลผลเพื่อการใช้ประโยชน์ในการจัดทำบริการสาธารณะเอาไว้ โดยไม่ต้องขอความยินยอม ดังนั้น การที่หน่วยงานภาครัฐทุกหน่วยงานมีนโยบายและแนวปฏิบัติภายในองค์กร เพื่อรองรับการปฏิบัติตามกฎหมายเป็นสิ่งสำคัญในการใช้กฎหมาย PDPA ได้อย่างมีประสิทธิภาพ

1.3 การประเมินผล การทบทวนและปรับปรุงกฎหมาย PDPA ในการคุ้มครองข้อมูลส่วนบุคคล

อภิปรายว่า เนื่องจาก PDPA เป็นกฎหมายใหม่และยังไม่มีคำพิพากษาของศาลที่ใช้เป็นบรรทัดฐาน จึงมีความจำเป็นอย่างยิ่งที่จะต้องติดตามประกาศของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้เข้าใจถึงการใช้และการตีความกฎหมายต่อไป อีกทั้งเพื่อสร้างความเข้าใจให้กับผู้ใช้กฎหมายและประชาชน และจากการศึกษาเอกสารงานวิจัยต่าง ๆ พบประเด็นที่ภาครัฐจะต้องมีการประเมิน การทบทวน การตีความและปรับปรุงกฎหมายให้ชัดเจนขึ้น ดังข้อคิดเห็นและเสนอแนะของนักวิชาการบางคนดังนี้

ปัทมา มัญชุนากร (2565) มีข้อเสนอแนะเกี่ยวกับการกำหนดหลักเกณฑ์และแนวปฏิบัติของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ดังนี้

1. เสนอให้คณะกรรมการกำหนดแนวทางปฏิบัติโดยอาศัยอำนาจตามมาตรา 16(6) เรื่องการใช้และการ ตีความนิยามคำว่า “ผู้ควบคุมข้อมูลส่วนบุคคล” โดยสามารถแบ่งองค์ประกอบหลักเป็น 4 ประการ เพื่ออธิบายความ ดังนี้ (1) “บุคคลธรรมดาหรือนิติบุคคล” (2) “ซึ่งมีอำนาจหน้าที่” (3) “ตัดสินใจ” และ (4) “การเก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคล” เนื้อหาสาระควรระบุชัดเจนว่า บุคคลใดบ้างที่กฎหมายไม่ถือว่าเป็นผู้ควบคุมข้อมูลส่วนบุคคล เช่น ลูกจ้างหรือพนักงานที่ดำเนินการตามขอบเขตการจ้าง, การตัดสินใจเกี่ยวกับวัตถุประสงค์และวิธีการที่เป็นสาระสำคัญที่กฎหมายถือว่ามีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคล, ความหมายของการเก็บรวบรวมใช้หรือเปิดเผย หมายความรวมถึงการดำเนินการใดหรือกระบวนการดำเนินการใดที่กระทำต่อข้อมูลส่วนบุคคลหรือกลุ่มของข้อมูล ส่วนบุคคล ไม่ว่าด้วยวิธีการอัตโนมัติหรือไม่ เช่น การรวบรวม การบันทึก การจัดองค์กร การจัดโครงสร้าง การ จัดเก็บ การปรับหรือการเปลี่ยนแปลง การค้นคืน การให้คำปรึกษา การใช้ การเปิดเผยโดยการส่ง การเผยแพร่หรือ การเปิดเผย การจัดเรียงหรือการรวมเข้ากัน การจำกัด การลบหรือการทำลาย พร้อมตัวอย่างประกอบโดยเฉพาะใน กรณีที่มีการประมวลผลข้อมูลส่วนบุคคลบนเครือข่ายสังคมออนไลน์และแพลตฟอร์มดิจิทัล เพื่อให้ผู้ใช้กฎหมายทราบ อย่างชัดเจนว่าตนมีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือไม่

2. เสนอให้เพิ่มเติมบทบัญญัติเกี่ยวกับความสัมพันธ์ระหว่างผู้ความคุมข้อมูลส่วนบุคคลร่วมในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยมีเนื้อหาสาระดังนี้ ในกรณี

ผู้ควบคุมข้อมูลส่วนบุคคลตั้งแต่สองคนขึ้นไปเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่มาจากแหล่งเดียวกัน ให้ถือว่าผู้ควบคุมข้อมูลส่วนบุคคลนั้นเป็นผู้ควบคุมข้อมูลส่วนบุคคลร่วม

เขมภัทร ทฤษฎีคุณ (2565) กล่าวถึงการยกเว้นการบังคับใช้ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 สิ่งที่เกิดขึ้นนำมาสู่การวิพากษ์วิจารณ์เกี่ยวกับความโปร่งใส และความรับผิดชอบของภาครัฐ ดังนั้นการยกเว้นการบังคับใช้ของกฎหมาย PDPA อาจจะทำให้มีปัญหาให้หน่วยงานของรัฐใช้หรือเข้าถึงข้อมูลส่วนบุคคลโดยปราศจากความรับผิดชอบ และกลายเป็นการซ้ำเติมปัญหาวัฒนธรรมการลอยนวลพ้นผิดเมื่อเกิดการละเมิดข้อมูลส่วนบุคคล ในทางเศรษฐกิจของประเทศ กฎหมาย PDPA ทำหน้าที่สำคัญในฐานะเป็นส่วนหนึ่งของกฎหมายเศรษฐกิจดิจิทัลที่กำหนดหลักเกณฑ์และวิธีการเคลื่อนย้ายข้อมูลส่วนบุคคล ข้ามพรมแดน ซึ่งเป็นหัวใจสำคัญของเศรษฐกิจสมัยใหม่ที่มีความจำเป็นต้องมีการเคลื่อนย้ายข้อมูลส่วนบุคคลข้ามพรมแดน ดังจะเห็นได้จากกรอบความตกลงทางเศรษฐกิจต่าง ๆ เช่น RCEP หรือ CPTPP ที่กำหนดให้ประเทศภาคีต้องรับรองหลักการดังกล่าว หลักการสำคัญของการเคลื่อนย้ายข้อมูลส่วนบุคคลข้ามพรมแดนนั้นให้ความสำคัญกับการส่งข้อมูลส่วนบุคคลของประเทศผู้รับข้อมูลส่วนบุคคลนั้น จะต้องมีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอไม่น้อยกว่าประเทศผู้ส่งข้อมูลส่วนบุคคล GDPR หรือ General Data Protection Regulation ของสหภาพยุโรปที่กำหนดว่ามาตรฐานที่เพียงพอนี้รวมถึงการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายจะต้องไม่ถูกแทรกแซงโดยรัฐ หรือหน่วยงานด้านความมั่นคงของรัฐ ซึ่งเป็นหลักการพื้นฐานของรัฐที่เป็นนิติรัฐที่มุ่งคุ้มครองสิทธิและเสรีภาพของประชาชน ดังนั้นผลของพระราชกฤษฎีกาฉบับนี้เปิดช่องให้สามารถตีความรวมถึงไม่ได้รับรองสิทธิของเจ้าของข้อมูลส่วนบุคคลเอาไว้ก็อาจจะทำให้ประเทศไทยไม่ได้รับการยอมรับว่าเป็นประเทศที่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เท่าเทียมกันกับสหภาพยุโรป

ผู้วิจัยได้ยกตัวอย่างบางกรณีที่นักวิชาการทางกฎหมายได้แสดงความคิดเห็นเอาไว้จากการตีความกฎหมาย PDPA หลังการประกาศใช้ ทั้งนี้สิ่งที่ภาครัฐควรดำเนินการคือการประเมินผล การทบทวนและปรับปรุงกฎหมาย PDPA ในการคุ้มครองข้อมูลส่วนบุคคล โดยการจัดเวทีการประชุม สัมมนา ที่มีตัวแทนจากหลายภาคส่วนทั้งภาครัฐ ภาคเอกชน/ผู้ประกอบการ/ผู้ให้บริการ และประชาชนจากหลากหลายอาชีพเพื่อร่วมกันประเมินผลการใช้กฎหมาย PDPA ต่อไป

3. ภาครัฐต้องมีการประชาสัมพันธ์และให้ความรู้เกี่ยวกับกฎหมาย PDPA ในการคุ้มครองข้อมูลส่วนบุคคลให้แก่ประชาชนรับรู้

อภิปรายว่า ภาครัฐต้องมีการประชาสัมพันธ์และให้ความรู้เกี่ยวกับกฎหมาย PDPA ในการคุ้มครองข้อมูลส่วนบุคคลให้แก่ประชาชนรับรู้ เพราะหน่วยงานของรัฐมีภารกิจต้องเก็บจากบุคคลเป็นจำนวนมาก เช่น ฐานข้อมูลทะเบียนราษฎร หรือฐานข้อมูลบัตรประจำตัวประชาชน เป็นต้น เจ้าหน้าที่รัฐอาจไม่มั่นใจว่าจะสามารถขอความยินยอมได้อย่างไร ซึ่งในความเป็นจริงแล้ว PDPA ได้ให้อำนาจหน่วยงานของรัฐในฐานการประมวลผลเพื่อการใช้ประโยชน์ในการจัดทำบริการสาธารณะเอาไว้ โดยไม่ต้องขอความยินยอม นอกจากนี้ในกรณีอื่น ๆ หน่วยงานของรัฐก็อาจจะอาศัยฐานในการประมวลผลอื่น ๆ เพื่อเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ ได้แก่ ฐานสัญญา ฐานสถิติ เอกสารประวัติศาสตร์ และจดหมายเหตุ ฐานป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล ฐานประโยชน์โดยชอบด้วยกฎหมาย และฐานการปฏิบัติตามกฎหมาย

ซึ่งกฎหมาย PDPA รับรองเอาไว้ แต่ในทั้งนี้ในกรณีที่ภาครัฐจะต้องเก็บรวบรวมและใช้ข้อมูลส่วนบุคคล ภาครัฐควรจะต้องมีการแจ้งให้ประชาชนทราบ เพื่อให้ประชาชนสามารถใช้สิทธิของตนเองได้ตามกฎหมายเพราะหน่วยงานของรัฐส่วนใหญ่ยังขาดการเตรียมกระบวนการเพื่อแจ้งเจ้าของข้อมูลส่วนบุคคลให้ทราบเกี่ยวกับการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคล การจัดเตรียมช่องทางการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล โดยควรจะต้องแจ้งให้ประชาชนรับรู้เพื่อประโยชน์ของประชาชนในการควบคุมสิทธิในข้อมูลส่วนบุคคลของตนเอง

4. ส่งเสริมและสนับสนุน การวิจัย เพื่อพัฒนาเทคโนโลยีที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

อภิปรายได้ว่า ภาครัฐต้องมีระบบเทคโนโลยีสารสนเทศที่ปลอดภัย หน่วยงานของรัฐบางแห่งยังไม่ มีระบบเทคโนโลยีสารสนเทศที่ทันสมัยเพียงพอกับการรับมือกับการละเมิด/รั่วไหลของข้อมูลส่วนบุคคล ซึ่งอาจเกิดการรั่วไหลหรือถูกโจมตีต่อระบบคอมพิวเตอร์ได้ หรือในกรณีที่เก็บรักษาเอกสารอิเล็กทรอนิกส์ไว้ในเครื่องคอมพิวเตอร์ สำนักงานโดยไม่มีการตั้งรหัสการเข้าถึงข้อมูล (access control) อาจทำให้บุคคลที่ไม่มีส่วนเกี่ยวข้องเข้าถึง ข้อมูลได้โดยไม่จำเป็น สอดคล้องกับความคิดเห็นของเขมภัทร ทฤษฎีคุณ (2565) ที่กล่าวไว้ในบทความเรื่องสำรวจความพร้อมภาครัฐ ปฏิบัติตาม “PDPA” ว่าความเปลี่ยนแปลงที่เกิดขึ้นในหลายหน่วยงานภาครัฐมีเพียงบนกระดาษ ไม่ได้เปลี่ยนแปลงระดับนโยบาย กระบวนการทำงาน ไปจนถึงเทคโนโลยีเพื่อการรักษาความปลอดภัยข้อมูลส่วนบุคคล ซึ่งอาจทำให้ข้อมูลส่วนบุคคลของประชาชนถูกละเมิด/รั่วไหลได้ ตามที่เคยเกิดขึ้นแล้ว หลังกฎหมาย PDPA ประกาศใช้ในช่วงปี 2565 ก็ยังมีการละเมิด/รั่วไหลของข้อมูลส่วนบุคคลในส่วนของภาครัฐ

5. การจัดทำหลักสูตรในระดับอุดมศึกษา/การวิจัยพัฒนาด้านการคุ้มครองข้อมูลส่วนบุคคล

อภิปรายว่า ภาครัฐควรมีนโยบายมอบให้กระทรวงอุดมศึกษาฯ ร่วมมือกับหน่วยงานที่เกี่ยวข้องของภาครัฐ เช่น สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ในการจัดทำหลักสูตรพื้นฐานด้านการคุ้มครองข้อมูลส่วนบุคคลสำหรับการเรียนการสอนในระดับอุดมศึกษาเพื่อผลิตกำลังคนที่มีความรู้ความสามารถในการทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลทั้งด้านกฎหมาย ด้านความเชี่ยวชาญทางเทคโนโลยีสารสนเทศ รวมทั้งการส่งเสริมสนับสนุนการวิจัยพัฒนาด้านการคุ้มครองข้อมูลส่วนบุคคลให้ได้ตามมาตรฐานสากล

2. การดำเนินงานของภาคเอกชน/ผู้ประกอบการ

2.1 การสร้างความตระหนักรู้ของบุคลากรและบุคคลที่เกี่ยวข้องในการปฏิบัติตามกฎหมาย PDPA

อภิปรายได้ว่า เพื่อให้การดำเนินงานของภาคเอกชน/ผู้ประกอบการในการปฏิบัติตาม PDPA เป็นไปอย่างมีประสิทธิภาพและยั่งยืน บุคลากรและบุคคลที่เกี่ยวข้องทุกฝ่ายขององค์กรควรตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องในการดำเนินงานอยู่เสมอ ทั้งนี้เนื่องจาก PDPA มีบทบัญญัติหลาย ๆ ส่วนที่ซับซ้อนและเข้าใจได้ยาก เพื่อให้การอบรมมีประสิทธิผลองค์กรจึงควรออกแบบเนื้อหาการอบรมให้เหมาะสมกับผู้เข้าอบรมในแต่ละกรณี ภัทรพร กายบริบูรณ์ (2565) ได้เสนอแนวทางการอบรมไว้ดังนี้

2.1.1 การจัดอบรมให้ผู้บริหารองค์กร: เป้าประสงค์สำคัญควรเป็นการชี้ให้ผู้บริหารเห็นภาพรวมและตระหนักถึงความสำคัญ ตลอดจนความเสี่ยงกรณีการไม่ปฏิบัติตาม PDPA เพื่อให้ผู้บริหารช่วยสนับสนุนและผลักดันให้องค์กรเกิดความตื่นตัวในการปฏิบัติตาม PDPA อยู่เสมอ

2.1.2 การจัดอบรมให้คณะทำงาน PDPA : การอบรมคณะทำงานซึ่งรับผิดชอบโดยตรงในการช่วยให้องค์กรปฏิบัติตาม PDPA ควรเป็นการอบรมแบบลงรายละเอียดข้อกำหนดที่เกี่ยวข้องกับการดำเนินงานจริงขององค์กร รวมทั้งแนวทางในการจัดการข้อมูลส่วนบุคคลภาคปฏิบัติแบบรอบด้านตั้งแต่กระบวนการเก็บรวบรวม ใช้ เปิดเผย จนถึงการลบหรือทำลายข้อมูลส่วนบุคคลทั้งในแง่มุมกฎหมายและแง่มุมอื่น ๆ เช่น ความเสี่ยง เพื่อให้การบริหารจัดการข้อมูลเป็นไปอย่างมีประสิทธิภาพ

2.1.3 การจัดอบรมให้บุคลากรหรือผู้ปฏิบัติงานในองค์กร : การอบรมควรย่อยเฉพาะส่วนที่เกี่ยวข้องกับการปฏิบัติงานของบุคลากรแต่ละฝ่ายเพื่อให้สามารถเข้าใจได้ง่าย และตรงกับขอบข่ายงานจริงที่เกี่ยวข้องกับการประมวลผลข้อมูลขององค์กร

2.2 การกำหนดแนวทางขององค์กรเพื่อควบคุมดูแลการปฏิบัติตาม PDPA

อภิปรายได้ว่า เมื่อ PDPA มีผลใช้บังคับแล้วข้อกำหนดต่าง ๆ ของ PDPA จะคงอยู่ต่อไปจนกว่าจะมีการแก้ไขเพิ่มเติม ดังนั้นสิ่งหนึ่งที่องค์กรต้องสำรวจความพร้อมคือมาตรการควบคุมดูแลการปฏิบัติตาม PDPA ขององค์กรจากเอกสารแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Bunaramrueang Elamchamroonlarp Oinpat & Thipsamritkul 2019) ได้เสนอแนวทางปฏิบัติไว้สำหรับผู้ประกอบการว่า ผู้ประกอบการจำเป็นต้องแสดงให้เห็นว่ามีขั้นตอนการกำหนดข้อมูลให้เป็นข้อมูลส่วนบุคคลในองค์กร โดยอย่างน้อยต้องประกอบด้วยมาตรการ ดังนี้

2.2.1 การกำหนดนโยบายและนิยามความหมายของข้อมูลส่วนบุคคล (data policy)

2.2.2 การกำหนดขั้นตอนการตรวจสอบข้อมูลส่วนบุคคล (data discovery)

2.2.3 การระบุความเชื่อมโยงและเส้นทางการส่งข้อมูลส่วนบุคคลที่จะเกิดขึ้นในองค์กรรวมถึงระบุ แหล่งที่จะได้มาซึ่งข้อมูลส่วนบุคคลทั้งหลาย (data proliferation)

2.2.4 การกำหนดความเสี่ยงของข้อมูลส่วนบุคคลชุดต่าง ๆ (data risk level)

2.2.5 มีมาตรการคุ้มครองข้อมูลส่วนบุคคล (data protection)

2.3 การสร้างมาตรฐานความมั่นคงปลอดภัยทางด้านเทคโนโลยี เพื่อคุ้มครองข้อมูลส่วนบุคคลให้ได้ตามมาตรฐานสากล

อภิปรายได้ว่า หน่วยงานและบริษัทต่าง ๆ ต้องมีการปรับตัวและพัฒนาให้องค์กรตนเองมีมาตรฐานความมั่นคงปลอดภัยทางด้านเทคโนโลยีให้ได้ตามมาตรฐานสากล เพื่อทำให้สามารถรักษาความเป็นส่วนตัวของข้อมูลที่จัดเก็บไว้ เพื่อให้เกิดความปลอดภัยและได้รับความเชื่อถือต่อการดำเนินกิจการขององค์กรจากทั้งในประเทศและในระดับสากล เช่นสหภาพยุโรป ซึ่งมีหลักการที่สำคัญเดียวกันคือข้อมูลส่วนบุคคลจะได้รับการปกป้องจากการละเมิดขององค์กรและภาคเอกชนต่าง ๆ เนื่องจากประชาชนมีสิทธิคุ้มครองข้อมูลส่วนบุคคลของตนในโลกดิจิทัลซึ่งถือว่าเป็นสิทธิพื้นฐาน ทั้งนี้หลังจากการประกาศใช้กฎหมาย PDPA ภาคเอกชนก็มีการเตรียมความพร้อมทางด้านเทคโนโลยีเพื่อคุ้มครองข้อมูลส่วนบุคคลให้ได้ตามมาตรฐานสากล

2.4 การกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่มีมาตรฐานสากล

อภิปรายได้ว่าผู้ประกอบการ/ผู้ให้บริการต้องมีการกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่มีมาตรฐานสากลสามารถตรวจสอบและป้องกันการหลุดรั่วของข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพและเมื่อเกิดเหตุการณ์หลุดรั่วของข้อมูลส่วนบุคคลแล้วจะต้องมีมาตรการในการตรวจสอบ เพื่อให้พบเหตุดังกล่าวอย่างทันท่วงที เพื่อที่จะได้จำกัดความเสียหายที่อาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคล และเมื่อเกิดเหตุการณ์ดังกล่าวขึ้นแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการตรวจสอบเหตุการณ์ที่เกิดขึ้นโดยละเอียด เพื่อที่จะได้ระบุสาเหตุแห่งการละเมิดข้อมูลส่วนบุคคลและหามาตรการในการแก้ไขเยียวยาเหตุการณ์ที่เกิดขึ้นได้โดยเร็ว โดยจะต้องแจ้งเหตุการณ์ดังกล่าวให้กับบุคคลที่เกี่ยวข้องอย่างตรงไปตรงมาและทันทีด้วย

3. การดำเนินการของบุคคลทั่วไปและเจ้าของข้อมูลส่วนบุคคล

ผลการศึกษาวิจัยจากการศึกษาเอกสารและบทสัมภาษณ์ผู้ที่เกี่ยวข้อง พบว่าการดำเนินการสำหรับบุคคลทั่วไปและเจ้าของข้อมูลส่วนบุคคลที่สำคัญ มีดังนี้

3.1 ต้องศึกษาสิทธิของตนเองตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

อภิปรายได้ว่า บุคคลทั่วไปและเจ้าของข้อมูลส่วนบุคคลต้องมีการศึกษาสิทธิของเจ้าของข้อมูลส่วนบุคคลเพื่อให้ทราบถึงสิทธิที่ตนเองมีและสิทธิที่จะการดำเนินการกับหน่วยงานภาครัฐ/ผู้ประกอบการบริษัทต่าง ๆ ที่เก็บข้อมูลไว้ โดยสิทธิที่มี มีดังนี้ สิทธิในการได้รับการแจ้งให้ทราบรายละเอียด (Privacy Notice) สิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล สิทธิขอให้โอนข้อมูลส่วนบุคคล สิทธิคัดค้านการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคล สิทธิขอให้ลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ สิทธิขอให้ระงับการใช้ข้อมูลส่วนบุคคล สิทธิขอให้แก้ไขข้อมูลส่วนบุคคล สิทธิในการร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญในกรณีที่มีการฝ่าฝืนและไม่ปฏิบัติตามกฎหมายหรือประกาศที่ออกตามกฎหมาย PDPA นอกจากนี้หากมีการละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงที่จะกระทบสิทธิเสรีภาพของเจ้าของข้อมูล ต้องทราบว่าผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ที่จะต้องแจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบและมีแนวทางการเยียวยาโดยไม่ชักช้า

3.2 ควรศึกษานโยบายการจัดเก็บข้อมูลหรือการขอสิทธิเข้าใช้ข้อมูลของตนเอง

อภิปรายได้ว่า เจ้าของข้อมูลส่วนบุคคลควรศึกษานโยบายการจัดเก็บข้อมูลหรือการขอสิทธิเข้าใช้ข้อมูลของตนเองจากหน่วยงานภาครัฐ ผู้ประกอบการ/ผู้ให้บริการที่ผู้ใช้ได้เข้าไปใช้โดยละเอียด โดยเฉพาะในเครือข่ายสื่อสังคมออนไลน์ เช่น เพจเฟสบุ๊ค อินสตราแกรม เว็บไซต์ และแอปพลิเคชันต่าง ๆ เพื่อเป็นการปกป้องข้อมูลไม่ถูกนำไปใช้โดยไม่ได้รับความยินยอมและถูกนำไปใช้งานโดยที่ไม่มีความจำเป็นต่อตัวผู้ใช้

3.3 การป้องกันการรั่วไหลของข้อมูลส่วนบุคคลของตนเอง

อภิปรายได้ว่า การป้องกันการรั่วไหลของข้อมูลส่วนบุคคลของตนเองเป็นการกระทำเบื้องต้นในการคุ้มครองข้อมูลของตนเอง เช่น การตั้งรหัสผ่านที่คาดเดาได้ยาก มีความหลากหลายและไม่ซ้ำกับแอคเคาน์อื่น ๆ เปลี่ยนรหัสผ่านเป็นประจำและหลีกเลี่ยงการใช้ Wi-Fi สาธารณะเพื่อป้องกันการดักจับข้อมูลส่วนบุคคล จดบันทึกประวัติการใช้งานทางการเงินเสมอ ไม่ว่า

จะเป็นในช่องทางออนไลน์หรือออฟไลน์ก็ตาม เพื่อป้องกันไม่ให้โดนแฮกบัญชีธนาคารหรือบัตรเครดิต ตรวจสอบประวัติการใช้งานอินเทอร์เน็ตเสมอ เพื่อรักษาตัวเองให้ปลอดภัยจากการติดตามทางออนไลน์ เลือกใช้ระบบรักษาความปลอดภัยในทุกอุปกรณ์ที่มีการเชื่อมต่อออนไลน์ เป็นต้น ซึ่งสาเหตุโดยส่วนใหญ่ที่มีการหลุดรั่วข้อมูลส่วนบุคคลจากเจ้าของข้อมูลเอง เกิดจากการให้ข้อมูลโดยรู้เท่าไม่ถึงการณ์ การให้ข้อมูลโดยไม่รู้ที่มาที่ไปของผู้จัดทำและการทิ้งหรือนำเอกสารมาใช้ซ้ำ เป็นต้น

แนวทางการป้องกันและแก้ไขการหลุดรั่วของข้อมูลส่วนบุคคลในทางการปฏิบัติให้สอดคล้องกับกฎหมาย PDPA

กฎหมายคุ้มครองข้อมูลส่วนบุคคล PDPA ให้ความสำคัญกับเจ้าของข้อมูลส่วนบุคคลที่จะได้รับการรับรองคุ้มครองถึงสิทธิเกี่ยวกับข้อมูลส่วนบุคคลโดยกฎหมายได้กำหนดหน้าที่ของ “ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)” เอาไว้ว่าจะต้องมีการกำหนดมาตรการในการรักษาความปลอดภัยให้สอดคล้องกับกฎหมาย PDPA และกฎหมายอื่น ๆ ที่เกี่ยวข้อง ทั้งนี้ในส่วนของกฎหมาย PDPA ได้มีการกล่าวถึงบทบาทหน้าที่ของ “ผู้ควบคุมข้อมูลส่วนบุคคล” ซึ่งเป็นทั้งหน่วยงานภาครัฐ ผู้ประกอบการหรือผู้ให้บริการที่ต้องมีบทบาทเกี่ยวกับเรื่องของการป้องกันและรับมือการหลุดรั่วของข้อมูลส่วนบุคคล โดยแบ่งเป็น 2 เรื่อง คือ หน้าที่ในการ “ป้องกัน” และ หน้าที่ในการ “แก้ไข” (Sanpob Pornwattanakij, 2564)

1. หน้าที่ในการป้องกัน

ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม และมีหน้าที่ในการป้องกันมิให้เกิดการหลุดรั่วของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมเพื่อป้องกันการสูญหาย เข้าถึงใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบและต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป เพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยหลักการดังกล่าว ภาครัฐได้มีการประกาศใช้บังคับ “ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ.2563” ที่กำหนดมาตรฐานขั้นต่ำในการวางระบบความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ที่ต้องให้ความสำคัญใน 3 ด้านหลัก ๆ คือ

1.1 ด้านการธำรงไว้ซึ่งความลับ (Confidentiality) ซึ่งเป็นมาตรการในการเตรียมความพร้อมเกี่ยวกับความสามารถของระบบในการควบคุมการเข้าถึงข้อมูลเพื่อรักษาข้อมูลให้เป็นความลับ และป้องกันมิให้บุคคลอื่นที่ไม่เกี่ยวข้องเข้าถึงข้อมูลดังกล่าว

1.2 ด้านความถูกต้องครบถ้วน (Integrity) ซึ่งเป็นมาตรฐานเกี่ยวกับการสร้างความน่าเชื่อถือของระบบในการทำงานที่ถูกต้องครบถ้วน และเป็นปัจจุบันตลอดเวลา

1.3 ด้านความพร้อมใช้งาน (Availability) ซึ่งเป็นมาตรการเกี่ยวกับความพร้อมของการใช้งาน เพื่อให้การให้บริการยังคงดำเนินการได้อย่างต่อเนื่อง แม้เกิดปัญหาเกี่ยวกับการหลุดรั่วของข้อมูลส่วนบุคคล

ซึ่งหลักการดังกล่าวในต่างประเทศจะรู้จักในนามของ “CIA Triad” ที่เป็นหลักการพื้นฐานของการวางระบบความมั่นคงปลอดภัยสารสนเทศ (Sanpob Pornwattanakij, 2564)

2. หน้าที่ในการแก้ไข

กฎหมาย PDPA ได้กำหนดหน้าที่อีกประการหนึ่งของผู้ควบคุมข้อมูลส่วนบุคคลในการแก้ไข โดยในการแก้ไขปัญหาที่เกิดขึ้น ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแบ่งบุคคลที่เกี่ยวข้องโดยหากเกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการ (Sanpob Pornwattanakij, 2564) ดังนี้

2.1 กรณีที่ไม่มีความเสี่ยงต่อสิทธิของเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องทำการบันทึกเหตุการณ์ดังกล่าวเอาไว้เพื่อใช้เป็นหลักฐานในการอ้างอิง

2.2 กรณีเกิดการละเมิดข้อมูลส่วนบุคคลและมีความเสี่ยงต่อสิทธิของเจ้าของข้อมูลส่วนบุคคล ให้ผู้ควบคุมข้อมูลส่วนบุคคล แจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง นับแต่ทราบเหตุการละเมิดข้อมูลส่วนบุคคลเท่าที่จะสามารถกระทำได้

2.3 กรณีการละเมิดข้อมูลส่วนบุคคลมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล นอกจากจะต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแล้ว ยังมีหน้าที่ต้องแจ้งเหตุการณ์ละเมิดดังกล่าวให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย

Sanpob Pornwattanakij (2564) กล่าวว่าในประเทศไทยก็ได้มีนำหลักการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่เป็นที่นิยมใช้กันในต่างประเทศ คือ “NIST Cybersecurity Framework” โดยหลักการดังกล่าวได้มีการนำเสนอหลักการและแนวทางปฏิบัติเกี่ยวกับการบริหารจัดการความเสี่ยง เพื่อยกระดับความมั่นคงปลอดภัยขององค์กร เพื่อป้องกันภัย ตรวจสอบภัย และตอบสนองต่อภัยที่เกิดขึ้นอย่างเป็นแบบแผนขั้นตอน โดยหลักการสำคัญของ “NIST Cybersecurity Framework” แบ่งออกเป็น 5 ฟังก์ชันหลัก คือ

1. Identify – การระบุถึงความเสี่ยงที่เกิดขึ้น เพื่อให้เราสามารถตรวจสอบเหตุการการละเมิดข้อมูลส่วนบุคคลได้อย่างเท่าทัน เพื่อความสะดวกในการกำหนดกลยุทธ์และบริหารจัดการความเสี่ยงที่เกิดขึ้น

2. Protect – การกำหนดมาตรฐานในการควบคุมเพื่อปกป้องระบบขององค์กร

3. Detect – การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อตรวจจับสถานการณ์ที่ผิดปกติ

4. Respond – การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อรับมือกับสถานการณ์ผิดปกติที่เกิดขึ้น

5. Recovery – การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อให้ธุรกิจสามารถดำเนินได้อย่างต่อเนื่อง และฟื้นฟูระบบให้กลับคืนมาเหมือนเดิม

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้นำหลักการ NIST Cybersecurity Framework ดังกล่าวเข้ามาประยุกต์ใช้และกำหนดอยู่ใน “พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562” ด้วยโดยการกำหนดกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จะต้องมีวิธีการและมาตรการ ดังต่อไปนี้

1. การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล

2. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น

3. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

4. มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์

5. มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

ดังนั้น ผลการศึกษาวิจัยครั้งนี้ได้พบว่าประเทศไทยมีนโยบายในการคุ้มครองข้อมูลส่วนบุคคล และมีการป้องกันแก้ไขการละเมิดข้อมูลส่วนบุคคล โดยการกำหนดเป็นกฎหมายคือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่บังคับใช้โดยตรงและยังมีกฎหมายที่เกี่ยวข้อง คือพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ.2563 นอกจากนั้นยังมีพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 เพื่อการป้องกันและแก้ไขโดยการกำหนดมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งการเฝ้าระวังและติดตามสถานการณ์ด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศของประเทศ

สรุป

แผนการพัฒนาประเทศเพื่อเกิดการนำเทคโนโลยีดิจิทัลมาใช้ในทุกมิติมีความสอดคล้องกับการพัฒนาประเทศตามแผนหลักในการพัฒนาเศรษฐกิจและสังคมดิจิทัลของประเทศไทย ระยะ 20 ปี (พ.ศ.2561 –2580) จำเป็นอย่างยิ่งที่จะต้องสร้างความเชื่อมั่นกับทุกภาคส่วนในการนำเทคโนโลยีดิจิทัลมาใช้ในทุกมิติ ภาครัฐได้มีการจัดทำพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งได้มีผลบังคับใช้เมื่อวันที่ 1 มิถุนายน 2565 โดยมีวัตถุประสงค์ส่งเสริมและสนับสนุนให้เกิดการพัฒนาด้านการคุ้มครองข้อมูลส่วนบุคคลของประเทศ มีการพัฒนาหลักเกณฑ์ มาตรฐาน และวิธีการกำกับดูแลเกี่ยวกับการใช้ข้อมูลส่วนบุคคลให้เป็นไปอย่างถูกต้อง โดยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีลักษณะเป็นกฎหมายกลาง ที่ครอบคลุมการดำเนินการของบุคคลหรือนิติบุคคลที่เป็นหน่วยงานภาครัฐและภาคเอกชนที่ทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ต้องปฏิบัติตามหลักเกณฑ์ วิธีการ และเงื่อนไขตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนด ส่งผลทำให้ทุกภาคส่วนทั้ง ประชาชนทั่วไป บริษัทเอกชนและหน่วยงานภาครัฐต่าง ๆ ต้องมีความเข้าใจต่อกฎหมายอย่างถูกต้อง เข้าใจวิธีการดูแลเรื่องความปลอดภัยข้อมูลส่วนบุคคล และการปฏิบัติตามหลักเกณฑ์ข้อกำหนดที่ถูกต้อง แต่อย่างไรก็ตามในการดำเนินการด้านการจัดการข้อมูลส่วนบุคคลยังต้องอาศัยแนวทางอีกหลายด้านเพื่อแก้ไขปัญหาและการป้องกันการละเมิดข้อมูลส่วนบุคคลเพื่อการปฏิรูปประเทศสู่ดิจิทัลไทยแลนด์

ดังนั้นภาครัฐ ภาคเอกชน/ผู้ประกอบการหรือผู้ให้บริการและผู้ใช้งานในฐานะบุคคลหรือนิติบุคคลมีความจำเป็นอย่างยิ่งที่จะต้องเข้าใจถึงนิยาม หน้าที่และความรับผิดของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งเป็นบุคคลที่มีหน้าที่โดยตรงในการเก็บรักษาข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลให้มีความปลอดภัยและใช้ให้ตรงตามวัตถุประสงค์ซึ่งจะต้องเริ่มตั้งแต่การวางแผน การเก็บ

รวบรวมไปจนถึงขั้นตอนการทำลายข้อมูลส่วนบุคคลให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล PDPA ซึ่งผลจากการศึกษาแนวทางการป้องกันการละเมิดข้อมูลส่วนบุคคลที่สำคัญที่สุดคือการที่ภาครัฐ/ภาคเอกชน ต้องมีการประชาสัมพันธ์และให้ความรู้เกี่ยวกับกฎหมาย PDPA ในการคุ้มครองข้อมูลส่วนบุคคลให้แก่ประชาชนรับรู้ เพราะหน่วยงานมีภารกิจต้องเก็บจากบุคคลเป็นจำนวนมาก จึงควรจะต้องมีการแจ้งให้ประชาชนทราบเพื่อให้ประชาชนสามารถใช้สิทธิของตนเองได้ตามกฎหมาย รวมทั้งการดำเนินการที่ทั้งหน่วยงานทั้งภาครัฐและภาคเอกชนต้องเตรียมพร้อมกับการใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับนี้คือการจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยอย่างเหมาะสมและได้มาตรฐานสากลเพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจโดยมิชอบ เช่น การกำหนดนโยบายการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล มีการขอความยินยอมจากเจ้าของข้อมูลก่อนการเก็บ รวบรวม ใช้ หรือเปิดเผย มีการประเมินความเสี่ยงของข้อมูลส่วนบุคคล ดังนั้นการบริหารจัดการข้อมูลส่วนบุคคลจึงเป็นเรื่องที่เกี่ยวข้องกับทุกภาคส่วนในองค์กรและจำเป็นต้องดำเนินการอย่างต่อเนื่อง การบริหารจัดการข้อมูลส่วนบุคคลให้มีประสิทธิภาพและประสิทธิผลที่ดีนั้นขึ้นอยู่กับการกำกับดูแลของกรรมการและผู้บริหารและการมีส่วนร่วมของบุคคลในองค์กร การออกแบบกระบวนการที่มีการสอดแทรกมาตรการการคุ้มครองข้อมูลส่วนบุคคล การนำเทคโนโลยีเข้ามาช่วยในการติดตามตรวจสอบการปฏิบัติงาน การฝ่าฝืนนโยบาย และมาตรการที่กำหนดไว้ รวมถึงการวิเคราะห์ ตรวจสอบ ค้นหาและตอบสนองต่อภัยคุกคามจากภายนอก รวมทั้งการที่เจ้าของข้อมูลต้องมีการป้องกันตนเองโดยการป้องกันการรั่วไหลของข้อมูลส่วนบุคคลของตนเอง เช่น การตั้งรหัสผ่านที่คาดเดาได้ยาก มีความหลากหลายและไม่ซ้ำกับแอคเคาน์อื่น ๆ เปลี่ยนรหัสผ่านเป็นประจำและหลีกเลี่ยงการใช้ Wi-Fi สาธารณะเพื่อป้องกันการดักจับข้อมูลส่วนบุคคล เลือกใช้ระบบรักษาความปลอดภัยในทุกอุปกรณ์ที่มีการเชื่อมต่อออนไลน์ เป็นต้น ซึ่งสาเหตุโดยส่วนใหญ่ที่มีการหลุดรั่วข้อมูลส่วนบุคคลจากเจ้าของข้อมูลเอง เกิดจากการให้ข้อมูลโดยรู้เท่าไม่ถึงการณ์ การให้ข้อมูลโดยไม่รู้ที่มาที่ไปของผู้จัดทำและการทิ้งหรือนำเอกสารมาใช้ซ้ำ เป็นต้น

บทที่ 5
สรุปและข้อเสนอแนะ

ในบทที่ 5 นี้ผู้วิจัยทำการสรุปและอภิปรายผลของการศึกษาตามวัตถุประสงค์การวิจัยทั้ง 3 ข้อ รวมทั้งให้ข้อเสนอแนะ โดยมีรายละเอียดสรุปได้ดังนี้

สรุป

1. สถานการณ์ทั่วไปของการละเมิดข้อมูลส่วนบุคคลผ่านระบบดิจิทัลในปัจจุบัน

สรุปผลการศึกษาสถานการณ์ทั่วไปและแนวโน้มการละเมิดข้อมูลส่วนบุคคลผ่านระบบดิจิทัลในปัจจุบันได้ดังนี้

1.1 ประเทศไทยมีกฎหมายเกี่ยวกับการคุ้มครองข้อมูลข่าวสารส่วนบุคคลโดยเฉพาะคือพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 หรือกฎหมาย PDPA ทั้งนี้ได้เริ่มบังคับใช้ตั้งแต่ในวันที่ 1 มิถุนายน 2565 พระราชบัญญัติฯ ฉบับนี้มีลักษณะเป็นกฎหมายกลางที่ครอบคลุมการดำเนินการของบุคคลหรือนิติบุคคลที่เป็นหน่วยงานภาครัฐและภาคเอกชนที่ทำการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลต้องปฏิบัติตามหลักเกณฑ์ วิธีการ และเงื่อนไขตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กำหนด แต่จากการดำเนินการที่ผ่านมาหลังการประกาศใช้พระราชบัญญัติดังกล่าวสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นองค์กรอิสระตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ได้รับเรื่องการถูกร้องเรียนในเรื่องการฝ่าฝืนกฎหมาย เรื่องการบังคับให้ความยินยอมเพื่อเปิดใช้บริการ การถูกเก็บข้อมูลส่วนบุคคลมาจากแหล่งอื่นโดยมิชอบ ไม่เปิดให้ใช้สิทธิขอรับสำเนาข้อมูลหรือลบข้อมูลตามกฎหมาย และเรื่องการใช้และเปิดเผยข้อมูลระหว่างบุคคลธรรมดา เป็นต้น

1.2 สถิติที่ทางสำนักงานคุ้มครองข้อมูลส่วนบุคคลในช่วงวันที่ 1 ตุลาคม 2564 – 15 พฤศจิกายน 2565 พบว่า หน่วยงานเอกชนได้มีการถูกร้องเรียนในเรื่องการฝ่าฝืนกฎหมาย PDPA อยู่ในกลุ่มที่สูงที่สุด ถึง 83.1 % ลำดับถัดมาคือประชาชนอยู่ที่ 9.2 % หน่วยงานรัฐวิสาหกิจ 4.6% และหน่วยงานรัฐเพียง 3.1% โดยเหตุผลส่วนใหญ่ที่มีการละเมิดการคุ้มครองข้อมูลส่วนบุคคลนั้นมีสาเหตุมาจากการที่บุคลากรขององค์ขาดความรู้และความเข้าใจในด้านกฎหมาย PDPA รวมไปถึงกระบวนการทำงานขององค์กรมีการไหลเวียนข้อมูลส่วนบุคคลเป็นส่วนใหญ่ แต่ไม่มีการดำเนินงานให้ถูกต้องและครบกระบวนการ ทั้งนี้สาเหตุการละเมิดที่ได้รับแจ้งสาเหตุส่วนใหญ่ที่สำนักงานคุ้มครองข้อมูลส่วนบุคคล รวบรวมได้มีดังต่อไปนี้

1.2.1 ระบบคอมพิวเตอร์ขององค์กรถูกเจาะระบบ

1.2.2 กระบวนการควบคุมขั้นตอนการเปิดเผยข้อมูลส่วนบุคคลขององค์กรยังไม่รัดกุมเพียงพอ

1.2.3 พนักงานดำเนินการผิดพลาดส่งข้อมูลให้ผู้รับผิดคน

ทั้งนี้แนวโน้มสถิติของการละเมิดข้อมูลส่วนบุคคลจะมีทิศทางมากขึ้น เนื่องจากประชาชนโดยทั่วไปไม่มีความรู้ความเข้าใจต่อกฎหมายฉบับนี้มากพอและปัญหาจากการรั่วไหลของข้อมูลจากหน่วยงานต่าง ๆยังคงสร้างความกังวลให้กับเจ้าของข้อมูล

2. ผลกระทบของการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

สรุปผลจากการวิเคราะห์ข้อมูลผลกระทบของการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ดังนี้

2.1 ผลกระทบในแง่ภาระต้นทุนทางธุรกิจของผู้ประกอบการ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กำหนดหน้าที่ให้ผู้ควบคุมข้อมูลส่วนบุคคลจัดให้มีมาตรการการรักษาความปลอดภัยที่เหมาะสม หลักการดังกล่าวส่งผลให้ผู้ประกอบธุรกิจต้องลงทุนในหลายมิติ เช่น ระบบเครือข่ายซอฟต์แวร์เกี่ยวกับการรักษาความปลอดภัยของข้อมูล การจ้างที่ปรึกษาทางเทคนิคและบุคลากรเกี่ยวกับความปลอดภัยทางคอมพิวเตอร์ หลักการนี้ส่งผลให้เกิดภาระต้นทุนเพราะต้องอาศัยงบประมาณและการจ้างผู้เชี่ยวชาญรวมทั้งต้นทุนในการปฏิบัติการส่งข้อมูลการแจ้งต่าง ๆ ดังนั้นผู้ประกอบการขนาดใหญ่ย่อมได้เปรียบกว่าผู้ประกอบการขนาดกลางและขนาดย่อม (SMEs) ในด้านของงบประมาณการลงทุนระบบการคุ้มครองข้อมูลส่วนบุคคลทั้งในด้านทรัพยากรบุคลและเทคโนโลยีที่นำมาใช้

2.2 ผลกระทบต่อการแข่งขันทางการค้าที่ไม่เป็นธรรม

จากปัญหาการละเมิดข้อมูลส่วนบุคคลส่งผลให้ประเทศไทยต้องมีการคุ้มครองข้อมูลส่วนบุคคลทำให้เป็นข้อได้เปรียบของธุรกิจขนาดใหญ่ซึ่งมีงบประมาณเพื่อการนี้ เช่น การอัพเกรดระบบป้องกัน การจ้างผู้เชี่ยวชาญด้านความปลอดภัย การร่างสัญญาและนโยบาย แต่จะสร้างความเสียเปรียบแก่ผู้ประกอบการขนาดกลางและย่อม (SMEs) ที่มีต้นทุนต่ำกว่า การสร้างความเชื่อมั่นด้วยการมีระบบการคุ้มครองข้อมูลส่วนบุคคลที่ได้มาตรฐานของผู้ประกอบการขนาดใหญ่อาจทำให้เกิดปัญหาความเหลื่อมล้ำไม่เป็นธรรมทางการค้า

2.3 ผลกระทบในแง่การค้าและการลงทุนระหว่างประเทศ

การละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นในประเทศอยู่บ่อยครั้งย่อมส่งผลต่อความเชื่อมั่นต่อประเทศคู่ค้าได้ ทำให้เกิดผลกระทบที่ตามมาคือเรื่องของการค้าและการลงทุน ทั้งนี้เพราะต้องมีการส่งข้อมูลข้ามแดนกัน แต่ขณะเดียวกันข้อกฎหมายดังกล่าวสามารถส่งผลต่อธุรกิจต่าง ๆ ในการมีภาระต้นทุนที่สูงขึ้นจากการที่ต้องมีระบบการคุ้มครองข้อมูลส่วนบุคคลให้ได้มาตรฐานและเป็นไปตามกฎหมายของประเทศนั้น ๆ

2.4 ผลกระทบในการสร้างโอกาสให้เกิดการโจรกรรมข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 30 - 34 ซึ่งให้สิทธิเจ้าของข้อมูลหลายประการในด้านของผู้ประกอบการที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ปฏิบัติตามกฎหมาย โดยจัดให้มีระบบและการตอบสนองต่อการใช้สิทธิของเจ้าของข้อมูลในการยื่นคำร้อง

ต่าง ๆ ดังนั้นผลกระทบทางลบดังกล่าวสามารถเกิดขึ้นกับผู้มีส่วนได้เสียต่าง ๆ ในประเทศไทยได้ เช่น วิธีการวิศวกรรมทางสังคม การแสวงหาข้อมูลจากแหล่งต่าง ๆ เช่น สื่อสังคมออนไลน์ สามารถนำไปประกอบในการปลอมตัวเป็นเจ้าของข้อมูลและยื่นคำร้องต่อผู้ควบคุมข้อมูลขอใช้สิทธิเข้าถึงข้อมูล ส่งผลให้ผู้ปลอมตัวได้มาซึ่งข้อมูลส่วนบุคคลอื่นของเจ้าของข้อมูลรวมถึงข้อมูลละเอียดอ่อน เช่น ข้อมูลธุรกรรม ทั้งนี้เจ้าของข้อมูลที่อาจตกเป็นเหยื่อของการโจรกรรมข้อมูลเอกลักษณ์ โดยอาชญากรปลอมตัวเป็นเจ้าของข้อมูลและแอบอ้างสิทธิยื่นคำร้องขอข้อมูลอื่น ๆ ของเจ้าของข้อมูล ทำให้สูญเสียด้านต่าง ๆทั้งข้อมูลส่วนบุคคล การเงิน เกิดความสูญเสียทางเศรษฐกิจ เป็นต้น

2.5 ผลกระทบต่อสิทธิเสรีภาพของบุคคล

องค์ประกอบและเงื่อนไขของกฎหมาย PDPA ที่เป็นการคุ้มครองข้อมูลส่วนบุคคลอาจส่งผลกระทบทางลบต่อสิทธินี้ เช่นการสร้างโอกาสให้กับอาชญากรรมที่ส่งผลต่อความเป็นส่วนตัวของเจ้าของข้อมูล การที่ผู้ประกอบการใช้วิธีการปฏิบัติเพื่อให้สอดคล้องกับกฎหมายด้วยเทคนิคต่าง ๆ อันส่งผลให้เจ้าของข้อมูลมีความเสี่ยงต่อการถูกล่วงละเมิดข้อมูลส่วนบุคคลมากขึ้น นอกจากนั้นยังกระทบต่อสิทธิในการแสดงความคิดเห็น เช่น กรณีสิทธิของเจ้าของข้อมูลในการขอให้ลบหรือทำลายข้อมูลระบุตัวของตนเปิดทางให้มีการใช้เพื่อวัตถุประสงค์อื่น นอกจากนี้บุคคลสาธารณะหรือภาครัฐอาจอาศัยกลไกดังกล่าวเพื่อปิดกั้นเนื้อหาผิดกฎหมาย ของประเทศหนึ่งซึ่งไม่ผิดกฎหมายประเทศอื่น เช่น การร้องขอต่อผู้ประกอบการสื่อออนไลน์เพื่อให้ปิดกั้นข้อมูลที่ผิดกฎหมายประเทศหนึ่งจากการเข้าถึงได้ในประเทศอื่น ๆ

3. สรุปพัฒนาการการแก้ไขปัญหาและผลกระทบการละเมิดข้อมูลส่วนบุคคล

สรุปผลการศึกษาวิวัฒนาการการแก้ไขปัญหาและผลกระทบการละเมิดข้อมูลส่วนบุคคลตั้งแต่อดีตจนถึงปัจจุบันจากเอกสารต่าง ๆ ดังนี้

3.1 พัฒนาการการแก้ไขปัญหาและผลกระทบการละเมิดข้อมูลส่วนบุคคล

3.1.1 ตั้งแต่ในอดีตประเทศไทยมีการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล โดยเริ่มมีการกำหนดไว้ในรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2535 (แก้ไขเพิ่มเติม พ.ศ.2538) นำไปสู่ความพยายามตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลขึ้นทั้งในส่วนที่อยู่ในความครอบครองของทางภาคราชการและภาคเอกชน ซึ่งในส่วนทางภาคราชการได้มีการตราพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 จนกระทั่งถึงวันที่ 28 พฤษภาคม พ.ศ.2562 ก็ได้มีการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 หรือกฎหมาย PDPA ออกมาใช้บังคับในที่สุด ซึ่งจะเห็นได้ว่าพัฒนาการทางกฎหมายที่จะกำหนดหลักการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลมีพัฒนาการที่ล่าช้ามาก เพราะพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลที่ได้มีการริเริ่มที่จะตราขึ้นเป็นกฎหมายนับตั้งแต่ปี พ.ศ.2540 กว่าจะตราขึ้นเป็นกฎหมายได้รวมระยะเวลากว่า 20 ปี

3.1.2 การตรากฎหมายขึ้นมาเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลของประเทศไทยไม่ได้มีการตราไว้ในกฎหมายฉบับเดียว แม้ว่าจะมีพระราชบัญญัติข้อมูลข่าวสารของทางราชการพ.ศ.2540 เป็นกฎหมายหลักแต่ก็มีขอบเขตของการคุ้มครองที่จำกัดไม่ได้ครอบคลุมไปถึงข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของภาคเอกชนซึ่งมีปริมาณข้อมูล

ที่จัดเก็บเป็นจำนวนมากไม่น้อยไปกว่าข้อมูลที่อยู่กับภาครัฐ ไม่ว่าจะเป็นข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของ บรรดาธนาคารเอกชน โรงพยาบาลเอกชน โรงแรมห้างสรรพสินค้าหรือบรรษัทห้างร้านที่จำหน่ายสินค้า ผลิตภัณฑ์หรือให้บริการที่มีการจัดเก็บข้อมูลของลูกค้าไว้

3.1.3 จากการศึกษาเหตุผลสำคัญที่ประเทศไทยต้องตรากฎหมาย PDPA เพื่อคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ ก็คือ

3.1.3.1 ก่อนหน้านี้ประเทศไทยยังไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคล ซึ่งทำให้ไม่มีหลักประกันในการคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล ซึ่งเป็นสิทธิมนุษยชนขั้นพื้นฐาน ในขณะที่นานาอารยประเทศ ไม่ว่าจะเป็นประเทศในแถบยุโรป อเมริกาใต้ ได้มีการตรากฎหมายเพื่อมาคุ้มครองสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลและวางระบบการเยียวยาความเสียหายอันเกิดจากละเมิดเป็นที่เรียบร้อยแล้ว

3.1.3.2 จัดสร้างกลไกในการปกป้องสิทธิในความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคล โดยพยายามรักษาดุลยภาพของการคุ้มครองสิทธิของบุคคลในความเป็นส่วนตัว (right of privacy) เสรีภาพในการไหลเวียนของข้อมูลข่าวสาร (free flow of Information) และความมั่นคงของประเทศ (national security) เพื่อเป็นโครงสร้างพื้นฐานสารสนเทศที่มั่นคงในช่วงระยะเวลาแห่งข้อมูลข่าวสาร ภายใต้หลักการปกครองระบอบประชาธิปไตยและหลักนิติรัฐ

3.1.3.3 เพื่อสนับสนุนการทำธุรกรรมทางอิเล็กทรอนิกส์ เนื่องในปัจจุบันการพัฒนาการทางเทคโนโลยีสารสนเทศมีความก้าวหน้าอย่างรวดเร็ว ทำให้มีการนำเอาเทคโนโลยีมาประยุกต์ใช้ให้เกิดประโยชน์กับเศรษฐกิจและสังคมมากมาย โดยเฉพาะการประมวลผลข้อมูลส่วนบุคคลอันสามารถทำได้อย่างสะดวกและรวดเร็ว จึงมีความจำเป็นออกกฎหมายมาคุ้มครองข้อมูลส่วนบุคคลซึ่งมีการใช้อย่างแพร่หลายในยุคสังคมสารสนเทศ

3.1.3.4 การตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 หรือที่เรียกว่ากฎหมาย PDPA ซึ่งย่อมาจาก Personal Data Protection Act (B.E., 2562) เป็นกฎหมายว่าด้วยการให้สิทธิ์กับเจ้าของข้อมูลส่วนบุคคล สร้างมาตรฐานการรักษาข้อมูลส่วนบุคคลให้ปลอดภัยและนำไปใช้ให้ถูกวัตถุประสงค์ตามคำยินยอมที่เจ้าของข้อมูลส่วนบุคคลอนุญาต โดยกฎหมาย PDPA ได้ประกาศให้มีผลบังคับใช้ในวันที่ 1 มิถุนายน 2565 องค์กรต่าง ๆ จึงได้รับผลกระทบพอสมควรกับการประกาศใช้พระราชบัญญัติฉบับนี้ ทั้งนี้ต้องมีการเพิ่มมาตรฐานนโยบายการรักษาข้อมูลส่วนบุคคลให้ปลอดภัยและนำไปใช้ให้ถูกวัตถุประสงค์ตามคำยินยอมที่เจ้าของข้อมูลส่วนบุคคลได้ให้ไว้และที่สำคัญต้องสอดคล้องต่อกฎหมายด้วย องค์กรต่าง ๆ ทั้งนี้การเพิ่มมาตรฐานนโยบายการรักษาข้อมูลส่วนบุคคลให้ปลอดภัยและนำไปใช้ให้ถูกวัตถุประสงค์ตามคำยินยอมที่เจ้าของข้อมูลส่วนบุคคลได้ให้ไว้โดยต้องมีความสอดคล้องต่อกฎหมายด้วย ทำให้กระบวนการทำการคุ้มครองข้อมูลส่วนบุคคลจะต้องมีการดำเนินการอย่างเป็นระบบ โดยเฉพาะองค์กรขนาดใหญ่ที่มีการเก็บรวบรวมข้อมูลส่วนบุคคลและมีการนำข้อมูลส่วนบุคคลไปใช้เป็นจำนวนมาก ผู้ควบคุมข้อมูลส่วนบุคคลจึงต้องมีการกำหนดนโยบายความปลอดภัยของข้อมูลส่วนบุคคลภายในองค์กรและให้ความรู้แก่บุคคลากรในองค์กรรู้ขอบเขตการเก็บรวบรวม การใช้ การเผยแพร่ข้อมูลส่วนบุคคล และมีระบบการจัดเก็บข้อมูลส่วนบุคคลที่ปลอดภัย มีการจำกัดการเข้าถึงข้อมูลส่วนบุคคล มีการบันทึกกิจกรรมการ

ใช้ข้อมูลส่วนบุคคล สิ่งเหล่านี้ล้วนจำเป็นอย่างยิ่งที่ผู้ควบคุมข้อมูลจะต้องปฏิบัติตามเพื่อให้สอดคล้องกับกฎหมายต่อไป

3.2 การจัดระบบการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานในปัจจุบัน

ผู้วิจัยมีการศึกษาระบบการป้องกันคุ้มครองข้อมูลของของสถาบันพระปกเกล้า มาเป็นกรณีศึกษาผลการวิจัยมีดังนี้

3.2.1 การจัดระบบการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานในปัจจุบันต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมเพื่อป้องกันการสูญหาย เข้าถึงใช้เปลี่ยนแปลงและแก้ไขหรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบและต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ให้เป็นไปตามมาตรฐานขั้นต่ำตามประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563 ซึ่งมีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลครอบคลุม 3 ประเด็น ได้แก่

3.2.1.1 การธำรงไว้ซึ่งความลับ

3.2.1.2 ความถูกต้องครบถ้วน

3.2.1.3 สภาพพร้อมใช้งานของข้อมูลส่วนบุคคล

3.2.2 จัดให้มีผู้ควบคุมข้อมูลส่วนบุคคลคือบุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมกำหนด

3.2.3 กำหนดมาตรการต่าง ๆที่สำคัญและเกี่ยวข้องกับระบบการคุ้มครองข้อมูลส่วนบุคคล ดังนี้

3.2.3.1 มาตรการป้องกันด้านการบริหารจัดการ

1. การออกระเบียบ วิธีปฏิบัติ สำหรับควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการ จัดเก็บและประมวลผลข้อมูลส่วนบุคคล

2. การกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของ ผู้ใช้งาน แบ่งเป็นรูปแบบต่าง ๆ เช่น สิทธิในการเข้าดู แก้ไข เพิ่มเติม เปิดเผยและเผยแพร่ การตรวจสอบคุณภาพข้อมูลตลอดจนการลบทำลาย

3.2.3.2 มาตรการป้องกันด้านเทคนิค ในระบบการรักษาความปลอดภัยของข้อมูล

1. การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึงเปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคลให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคล

2. การบริหารจัดการการเข้าถึงของผู้ใช้งานควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาต ตามระดับสิทธิการใช้งาน ได้แก่ การนำเข้าเปลี่ยนแปลงแก้ไข เปิดเผย ตลอดจนการลบทำลาย

3. จัดให้มีระบบสำรองและกู้คืนข้อมูล เพื่อให้ระบบ และ/หรือ บริการต่าง ๆ ยังสามารถ ดำเนินการได้อย่างต่อเนื่อง

3.2.3.3 มาตรการป้องกันทางกายภาพ ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล

1. มีการควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วน บุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

2. กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล การลักลอบนำอุปกรณ์เข้าออก

3.3 มาตรการบทลงโทษทางกฎหมาย

การประกาศใช้พระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ซึ่งเป็นกฎหมายว่าหากผู้ใดหรือองค์กรใดไม่ปฏิบัติตามย่อมมีบทลงโทษตามกฎหมายตามมา ซึ่งบทลงโทษของพระราชบัญญัติฉบับนี้สำหรับผู้ที่ไม่ปฏิบัติตามนั้น มีทั้งโทษทางแพ่ง โทษทางอาญา และโทษทางปกครองด้วย

ถ้าไม่ปฏิบัติตามบทลงโทษของผู้ที่ไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (PDPA) มีถึง 3 ประเภท ได้แก่

3.3.1 โทษทางแพ่ง

โทษทางแพ่งกำหนดให้ชดใช้ค่าสินไหมทดแทนที่เกิดขึ้นจริงให้กับเจ้าของข้อมูลส่วนบุคคลที่ได้รับความเสียหายจากการละเมิด และอาจจะต้องจ่ายบวกเพิ่มอีกเป็นค่าสินไหมทดแทนเพื่อการลงโทษ

3.3.2 โทษทางอาญา

โทษทางอาญาจะมีทั้งโทษจำคุกและโทษปรับ โดยมี โทษจำคุกสูงสุดไม่เกิน 1 ปี หรือ ปรับไม่เกิน 1 ล้านบาท หรือทั้งจำทั้งปรับ โดยโทษสูงสุดดังกล่าวจะเกิดจากการไม่ปฏิบัติตาม PDPA ในส่วนการใช้ข้อมูล หรือเปิดเผยข้อมูล หรือส่งโอนข้อมูลไปยังต่างประเทศ

3.3.3 โทษทางปกครอง

โทษปรับมีตั้งแต่ 1 ล้านบาทจนถึงสูงสุดไม่เกิน 5 ล้านบาท ซึ่งโทษปรับสูงสุด 5 ล้านบาท จะเป็นกรณีของการไม่ปฏิบัติตาม PDPA ในส่วนการใช้ข้อมูล หรือเปิดเผยข้อมูล หรือส่งโอนข้อมูลไปยังต่างประเทศของประเภทข้อมูลที่มีความละเอียดอ่อนซึ่งโทษทางปกครองนี้จะแยกต่างหากกับการชดใช้ค่าเสียหายที่เกิดจากโทษทางแพ่งและโทษทางอาญาด้วย

4. สรุปปัญหาและอุปสรรคในการดำเนินการแก้ไขปัญหาและผลกระทบการละเมิดข้อมูลส่วนบุคคลผ่านเทคโนโลยีดิจิทัล

สรุปผลการวิจัยในประเด็นปัญหาและอุปสรรคในการดำเนินการแก้ไขปัญหาและผลกระทบการละเมิดข้อมูลส่วนบุคคลผ่านเทคโนโลยีดิจิทัล ดังนี้

4.1 ปัญหาความไม่ชัดเจนของกฎหมาย

ผลการศึกษาพบว่า พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 เป็นกฎหมายใหม่อาจมีการตีความไม่ได้ชัดเจนในบางมาตรา ยกตัวอย่างเช่น

4.1.1 ประเด็นการขอความยินยอมในการจัดเก็บข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคลโดยตรง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ยังขาดความชัดเจนในเรื่องการขอความยินยอมในการจัดเก็บข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคลโดยตรงและการแจ้งวัตถุประสงค์ในการจัดเก็บข้อมูลกล่าวคือปัญหาการจัดเก็บข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมของเจ้าของข้อมูล ซึ่งทำให้หน่วยงานเอกชนสามารถจัดเก็บข้อมูลส่วนบุคคลโดยที่ไม่ได้รับความยินยอมของเจ้าของข้อมูลก่อนเพียงแค่แจ้งให้เจ้าของข้อมูลทราบเท่านั้น ส่งผลให้เกิดการรั่วไหลของข้อมูลส่วนบุคคลที่เป็นอยู่ในปัจจุบัน

4.1.2. ตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 39 วรรคสาม บัญญัติว่าเว้นแต่มีการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลหรือมิใช่กิจการที่เก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว หรือมีการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26 นั้น บทบัญญัติดังกล่าวมีความไม่ชัดเจนในเรื่องของ “ความเสี่ยงต่อสิทธิ เสรีภาพของเจ้าของมูลส่วนบุคคลและการเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว” เนื่องจากไม่มีหลักเกณฑ์กำหนดว่าการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลอย่างไรที่ถือว่าทำให้เกิดความเสี่ยงต่อสิทธิเสรีภาพหรือถือเป็นการเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราวทำให้เกิดปัญหาการตีความทางกฎหมายที่ไม่สอดคล้องกันก่อให้เกิดปัญหาแก่ผู้ที่เกี่ยวข้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลดังกล่าว

4.2 ปัญหาการยกเว้นทางกฎหมายให้กับการใช้ข้อมูลส่วนบุคคลในหน่วยงานของรัฐ

การยกเว้นการบังคับใช้กฎหมาย PDPA ให้กับการใช้ข้อมูลส่วนบุคคลในหน่วยงานของรัฐ อาจจะทำให้มีปัญหาให้หน่วยงานของรัฐใช้หรือเข้าถึงข้อมูลส่วนบุคคลโดยปราศจากความรับผิดชอบและกลายเป็นการซ้ำเติมปัญหาการพ้นผิดเมื่อเกิดการละเมิดข้อมูลส่วนบุคคลของภาครัฐและบั่นทอนความเชื่อมั่นของประชาชนถ้ามีการรั่วไหลของข้อมูลจากภาครัฐ นักวิชาการมีความน่ากังวลในประเด็นนี้ 2 เรื่อง

4.2.1 ขอบเขตของการยกเว้น ซึ่งตามร่างพระราชกฤษฎีกานี้มีการยกเว้นการนำกฎหมายมาใช้ในเรื่องสำคัญ ๆ ได้แก่ การคุ้มครองข้อมูลส่วนบุคคล สิทธิของเจ้าของข้อมูลส่วนบุคคล การร้องเรียน ความรับผิดทางแพ่งและบทกำหนดโทษ โดยเปิดโอกาสให้หน่วยงานของรัฐพ้นผิดจากการละเมิดสิทธิของเจ้าของข้อมูลส่วนบุคคลในรูปแบบต่าง ๆ

4.2.2 วัตถุประสงค์ของการยกเว้น อาทิ การรักษาความมั่นคงของประเทศ ความปลอดภัยสาธารณะ และการดำเนินการเพื่อประโยชน์สาธารณะนั้นมีความไม่เฉพาะเจาะจง และไม่อาจคาดหมายได้ว่าจะมีความหมายเช่นไรขึ้นกับดุลยพินิจและการตีความของหน่วยงานรัฐ ซึ่งข้อยกเว้นดังกล่าวนั้นขยายออกไปจากข้อยกเว้นเดิมที่กฎหมายกำหนดไว้

4.3 ปัญหาข้อกฎหมายในการเคลื่อนย้ายข้อมูลส่วนบุคคลข้ามพรมแดน

ผลของพระราชกฤษฎีการยกเว้นการบังคับใช้กฎหมายให้กับการใช้ข้อมูลส่วนบุคคลในหน่วยงานของรัฐเปิดช่องให้สามารถตีความรวมถึงไม่ได้รับรองสิทธิของเจ้าของข้อมูลส่วนบุคคลเอาไว้ ก็อาจจะทำให้ประเทศไทยไม่ได้รับการยอมรับว่าเป็นประเทศที่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เท่าเทียมกันกับสหภาพยุโรป นอกจากนี้อิทธิพลของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ได้สร้างมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลใหม่ทั่วโลก หากประเทศไทยไม่มีมาตรฐานเทียบเท่าก็จะมีผลให้ประเทศไทยไม่มีมาตรฐานเทียบเท่ากับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศอื่น ซึ่งทำให้การเคลื่อนย้ายข้อมูลส่วนบุคคลเข้ามาในประเทศไทยทำได้ยากและทำให้เอกชนของประเทศไทยอาจจะพลาดโอกาสในการเติบโตในยุคเศรษฐกิจดิจิทัล

4.4 ปัญหาการร้องเรียนการละเมิดข้อมูลส่วนบุคคล

ปัญหาการร้องเรียนการละเมิดข้อมูลส่วนบุคคลนี้มีแนวโน้มจะเพิ่มขึ้นจากการไม่เข้าใจในตัวกฎหมายที่บังคับใช้ ซึ่งในปัญหาที่มีการร้องเรียนนั้นสำนักงานคุ้มครองข้อมูลส่วนบุคคล (สคส.) นั้นจะต้องมีการสอบข้อเท็จจริงดังกล่าว ดังนั้นมีความจำเป็นที่จะต้องสร้างความเข้าใจในกฎหมายฉบับนี้ให้กับหน่วยงานต่าง ๆ รวมทั้งประชนที่เป็นเจ้าของข้อมูลนั้น ๆ ด้วย

4.5 การขาดแคลนทรัพยากรที่จำเป็นต่อการปฏิบัติหน้าที่ตามกฎหมาย

ปัญหาการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 พบว่าจำเป็นต้องได้รับการสนับสนุนทรัพยากรในด้านต่าง ๆ เพื่อให้สามารถทำความเข้าใจและตรวจสอบกระบวนการประมวลผลขององค์กรเป็นไปตามกฎหมายได้อย่างครบถ้วน อีกทั้งการได้รับทรัพยากรที่เพียงพอยังส่งผลโดยตรงต่อความเป็นอิสระในการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลภายใต้กฎหมาย

4.6 ประชาชนขาดความรู้และความเข้าใจในกฎหมาย

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 เป็นกฎหมายใหม่และมีรายละเอียดที่เกี่ยวข้องกับตัวบุคคลค่อนข้างมาก ทำให้ประชาชนขาดความรู้และความเข้าใจในตัวกฎหมายอย่างถ่องแท้ ดังนั้นในชีวิตประจำวันจึงเกิดความสับสนว่าเรื่องใดทำได้เรื่องใดทำไม่ได้ ตัวอย่างเช่นการโพสต์รูปตนเองแต่ติดบุคคลอื่นด้วย ถ้านำคลิปหรือรูปถ่ายที่ติดคนอื่นไปโพสต์ในสื่อสังคมออนไลน์โดยบุคคลอื่นไม่ยินยอมจะผิดกฎหมาย เจ้าของข้อมูลส่วนบุคคลต้องให้ความยินยอมทุกครั้งก่อนนำข้อมูลไปใช้ เป็นต้น ทำให้เกิดประเด็นร้องเรียนมากมายหลังพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ประกาศใช้

4.7 มาตรฐานรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลขององค์กรที่ไม่มีประสิทธิภาพเพียงพอ

มาตรฐานรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลขององค์กรที่ไม่มีประสิทธิภาพสามารถทำให้เกิดการหลุดรั่วของข้อมูลส่วนบุคคล หลังกฎหมาย PDPA มีการประกาศใช้มีการร้องเรียนไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลรายงานว่าหน่วยงานเอกชนได้มีการถูกร้องเรียนในเรื่องการฝ่าฝืนกฎหมาย PDPA อยู่ในกลุ่มที่สูงที่สุด ถึง 83.1% ลำดับ

ถัดมาคือประชาชนอยู่ที่ 9.2% หน่วยงานรัฐวิสาหกิจ 4.6% และหน่วยงานรัฐเพียง 3.1% โดยเหตุผลส่วนใหญ่ที่มีการละเมิดการคุ้มครองข้อมูลส่วนบุคคล นั้นมีสาเหตุมาจากการที่บุคลากรขององค์ขาดความรู้และความเข้าใจในด้านกฎหมาย PDPA รวมไปถึงกระบวนการทำงานขององค์กรมีการไหลเวียนข้อมูลส่วนบุคคลเป็นส่วนใหญ่แต่ไม่มีการดำเนินงานให้ถูกต้องและครบกระบวนการทำให้เกิดการรั่วไหลของข้อมูลส่วนบุคคล

4.8 ปัญหากฎหมายคุ้มครองข้อมูลส่วนบุคคลได้การเพิ่มภาระค่าใช้จ่ายให้ผู้ประกอบการธุรกิจ

การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพเมื่อผู้ประกอบการสามารถปฏิบัติตามกฎหมาย PDPA ซึ่งกระบวนการของบันทึกเริ่มตั้งแต่การจัดระบบข้อมูลโดยการรวบรวม วิเคราะห์จัดทำเป็นบันทึก รายการข้อมูลส่วนบุคคลให้เห็นลักษณะของกิจกรรมทั้งหมดที่กระทำต่อข้อมูลส่วนบุคคล จึงจำเป็นที่ต้องใช้ผู้เชี่ยวชาญด้านวิศวกรและทางด้านกฎหมายเป็นการสร้างภาระค่าใช้จ่ายจำนวนมากให้แก่ผู้ควบคุมข้อมูล ซึ่งส่วนใหญ่เป็นผู้ประกอบกิจการ

5. สรุปแนวทางการแก้ไขปัญหาและการป้องกันการละเมิดข้อมูลส่วนบุคคล

สรุปผลการศึกษาวิจัยที่ได้จากการศึกษาเอกสารต่าง ๆ และวิเคราะห์บทสัมภาษณ์เชิงลึกดังนี้

5.1 การดำเนินการของภาครัฐ

5.1.1 สร้างความเข้าใจและความชัดเจนในบทบาทหน้าที่ของภาครัฐในฐานะผู้ควบคุมข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ภาครัฐจำเป็นต้องสร้างความตระหนักและความรู้ ความเข้าใจในการคุ้มครองข้อมูลส่วนบุคคลของประชาชนและจะต้องมีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอไม่น้อยกว่าประเทศผู้ส่งข้อมูลส่วนบุคคล GDPR หรือ General Data Protection Regulation ของสหภาพยุโรป การกำหนดว่ามาตรฐานที่เพียงพอนี้รวมถึงการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายจะต้องไม่ถูกแทรกแซงโดยรัฐหรือหน่วยงานด้านความมั่นคงของรัฐ ซึ่งเป็นหลักการพื้นฐานของรัฐที่เป็นนิติรัฐที่มุ่งคุ้มครองสิทธิและเสรีภาพของประชาชน

5.1.2 หน่วยงานของภาครัฐต้องมีนโยบายและแนวปฏิบัติภายในหน่วยงานทุกหน่วย เพื่อรองรับการปฏิบัติตาม PDPA ทุกหน่วยงานของภาครัฐต้องมีการเตรียมพร้อมรับนโยบายและจัดทำแนวปฏิบัติหรือแม้แต่การปรับเปลี่ยนกฎเกณฑ์ทางกฎหมายภายใต้อำนาจของหน่วยงานของรัฐเพื่อให้สอดคล้องกับหลักการของกฎหมายคุ้มครองข้อมูลส่วนบุคคล PDPA ทั้งนี้ต้องมีการเตรียมพร้อมเจ้าหน้าที่ภาครัฐให้มีความเข้าใจต่อการพิจารณาฐานทางกฎหมายในการปฏิบัติงานด้วย

5.1.3 การประเมินผล การทบทวนและปรับปรุงกฎหมาย PDPA ในการคุ้มครองข้อมูลส่วนบุคคล

เนื่องจาก PDPA เป็นกฎหมายใหม่และยังไม่มีคำพิพากษาของศาลที่ใช้เป็นบรรทัดฐาน จึงมีความจำเป็นอย่างยิ่งที่จะต้องติดตามประกาศของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้เข้าใจถึงการใช้และการตีความกฎหมายต่อไป อีกทั้งเพื่อสร้างความเข้าใจให้กับผู้ใช้กฎหมายและประชาชน และจากการศึกษาเอกสารงานวิจัยต่าง ๆ พบประเด็นที่ภาครัฐจะต้องมีการประเมิน การทบทวน การตีความและปรับปรุงกฎหมายให้ชัดเจนขึ้น ดังข้อคิดเห็นและเสนอแนะของนักวิชาการบางคนคือหลังการประกาศใช้ ทั้งนี้สิ่งที่ภาครัฐควรดำเนินการคือการประเมินผล การทบทวนและปรับปรุงกฎหมาย PDPA ในการคุ้มครองข้อมูลส่วนบุคคล โดยการจัดเวทีการประชุมสัมมนาที่มีตัวแทนจากหลายภาคส่วนทั้งภาครัฐ ภาคเอกชน/ผู้ประกอบการ/ผู้ให้บริการ และประชาชนจากหลากหลายอาชีพเพื่อร่วมกันประเมินผลการใช้กฎหมาย PDPA ต่อไป

5.1.4 ภาครัฐต้องมีการประชาสัมพันธ์และให้ความรู้เกี่ยวกับกฎหมาย PDPA ในการคุ้มครองข้อมูลส่วนบุคคลให้แก่ประชาชนรับรู้ ภาครัฐต้องมีการประชาสัมพันธ์และให้ความรู้เกี่ยวกับกฎหมาย PDPA ในการคุ้มครองข้อมูลส่วนบุคคลให้แก่ประชาชนรับรู้เพราะหน่วยงานของรัฐมีภารกิจต้องเก็บจากบุคคลเป็นจำนวนมาก เช่น ฐานข้อมูลทะเบียนราษฎรหรือฐานข้อมูลบัตรประจำตัวประชาชน เป็นต้น เพื่อให้ประชาชนสามารถใช้สิทธิของตนเองได้ตามกฎหมาย เพราะหน่วยงานของรัฐส่วนใหญ่ยังขาดการเตรียมกระบวนการเพื่อแจ้งเจ้าของข้อมูลส่วนบุคคลให้ทราบเกี่ยวกับการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคล การจัดเตรียมช่องทางการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล โดยควรจะต้องแจ้งให้ประชาชนรับรู้เพื่อประโยชน์ของประชาชนในการควบคุมสิทธิในข้อมูลส่วนบุคคลของตนเอง

5.1.5 ส่งเสริมและสนับสนุน การวิจัย เพื่อพัฒนาเทคโนโลยีที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล ภาครัฐต้องมีระบบเทคโนโลยีสารสนเทศที่ปลอดภัยและทันสมัยเพียงพอกับการรับมือกับการละเมิด/รั่วไหลของข้อมูลส่วนบุคคล ซึ่งอาจเกิดการรั่วไหลหรือถูกโจมตีต่อระบบคอมพิวเตอร์ได้ หรือในกรณีที่เก็บรักษาเอกสารอิเล็กทรอนิกส์ไว้ในเครื่องคอมพิวเตอร์

5.1.6 การจัดทำหลักสูตรในระดับอุดมศึกษา/การวิจัยพัฒนาด้านการคุ้มครองข้อมูลส่วนบุคคล ภาครัฐควรมีนโยบายมอบให้กระทรวงอุดมศึกษาฯ ร่วมมือกับหน่วยงานที่เกี่ยวข้องของภาครัฐ เช่นสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ในการจัดทำหลักสูตรพื้นฐานด้านการคุ้มครองข้อมูลส่วนบุคคลสำหรับการเรียนการสอนในระดับอุดมศึกษา เพื่อผลิตกำลังคนที่มีความรู้ความสามารถในการทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลทั้งด้านกฎหมาย ด้านความเชี่ยวชาญทางเทคโนโลยีสารสนเทศ รวมทั้งการส่งเสริมสนับสนุนการวิจัยพัฒนาด้านการคุ้มครองข้อมูลส่วนบุคคลให้ได้ตามมาตรฐานสากล

5.2 การดำเนินงานของภาคเอกชน/ผู้ประกอบการ

5.2.1 การสร้างความตระหนักรู้ของบุคลากรและบุคคลที่เกี่ยวข้องในการปฏิบัติตามกฎหมาย PDPA บุคลากรและบุคคลที่เกี่ยวข้องทุกฝ่ายขององค์กรควรตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องในการดำเนินงานอยู่เสมอ โดยการการอบรมที่มีประสิทธิภาพและเกิดประสิทธิผลองค์กรจึงควรออกแบบเนื้อหาการอบรมให้เหมาะสมกับผู้เข้าอบรมในแต่ละกรณี ดังนี้

5.2.1.1 การจัดอบรมให้ผู้บริหารองค์กร : เป้าประสงค์สำคัญควรเป็นการชี้ให้ผู้บริหารเห็นภาพรวมและตระหนักถึงความสำคัญตลอดจนความเสี่ยงกรณีการไม่ปฏิบัติตาม PDPA เพื่อให้ผู้บริหารช่วยสนับสนุนและผลักดันให้องค์กรเกิดความตื่นตัวในการปฏิบัติตาม PDPA อยู่เสมอ

5.2.1.2 การจัดอบรมให้คณะทำงานของกฎหมาย PDPA : การอบรมคณะทำงานซึ่งรับผิดชอบโดยตรงในการช่วยให้องค์กรปฏิบัติตามกฎหมาย PDPA ควรเป็นการอบรมแบบลงรายละเอียดข้อกำหนดที่เกี่ยวข้องกับการดำเนินงานจริงขององค์กร รวมทั้งแนวทางในการจัดการข้อมูลส่วนบุคคลภาคปฏิบัติแบบรอบด้านตั้งแต่กระบวนการเก็บรวบรวม ใช้ เปิดเผย จนถึงการลบหรือทำลายข้อมูลส่วนบุคคล ทั้งในแง่มุมกฎหมายและแง่มุมอื่น ๆ เช่น ความเสี่ยงเพื่อให้การบริหารจัดการข้อมูลเป็นไปอย่างมีประสิทธิภาพ

5.2.1.3 การจัดอบรมให้บุคลากรหรือผู้ปฏิบัติงานในองค์กร : การอบรมควรย่อยเฉพาะส่วนที่เกี่ยวข้องกับการปฏิบัติงานของบุคลากรแต่ละฝ่ายเพื่อให้สามารถเข้าใจได้ง่ายและตรงกับขอบข่ายงานจริงที่เกี่ยวข้องกับการประมวลผลข้อมูลขององค์กร

5.2.2 การกำหนดแนวทางขององค์กรเพื่อควบคุมดูแลการปฏิบัติตามกฎหมาย PDPA องค์กรต้องสำรวจความพร้อมคือมาตรการควบคุมดูแลการปฏิบัติตามกฎหมาย PDPA ขององค์กร ผู้ประกอบการจำเป็นต้องแสดงให้เห็นว่ามีขั้นตอนการ กำหนดข้อมูลให้เป็นข้อมูลส่วนบุคคลในองค์กรโดยอย่างน้อยต้องประกอบด้วยมาตรการ ดังนี้

5.2.2.1 การกำหนดนโยบายและนิยามความหมายของข้อมูลส่วนบุคคล (data policy)

5.2.2.2 การกำหนดขั้นตอนการตรวจสอบข้อมูลส่วนบุคคล (data discovery)

5.2.2.3 การระบุความเชื่อมโยงและเส้นทางการส่งข้อมูลส่วนบุคคลที่จะเกิดขึ้นในองค์กรรวมถึงระบุ แหล่งที่จะได้มาซึ่งข้อมูลส่วนบุคคลทั้งหลาย (data proliferation)

5.2.2.4 การกำหนดความเสี่ยงของข้อมูลส่วนบุคคลชุดต่าง ๆ (data risk level) (5) มีมาตรการคุ้มครองข้อมูลส่วนบุคคล (data protection)

5.2.3 การสร้างมาตรฐานความมั่นคงปลอดภัยทางด้านเทคโนโลยีเพื่อคุ้มครองข้อมูลส่วนบุคคลให้ได้ตามมาตรฐานสากล หน่วยงานและบริษัทต่าง ๆ ต้องมีการปรับตัวและพัฒนาให้องค์กรตนเองมีมาตรฐานความมั่นคงปลอดภัยทางด้านเทคโนโลยีให้ได้ตามมาตรฐานสากลเพื่อทำให้สามารถรักษาความเป็นส่วนตัวของข้อมูลที่จัดเก็บไว้เพื่อให้เกิดความปลอดภัยและได้รับความเชื่อถือต่อการดำเนินกิจการขององค์กรจากทั้งในประเทศและในระดับสากล

5.2.2.4 การกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่มีมาตรฐานสากล ผู้ประกอบการ/ผู้ให้บริการต้องมีการกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่มีมาตรฐานสากล สามารถตรวจสอบและป้องกันการหลุดรั่วของข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพและเมื่อเกิดเหตุการณ์หลุดรั่วของข้อมูลส่วนบุคคลแล้วจะต้องมีมาตรการในการตรวจสอบเพื่อให้พบเหตุดังกล่าวอย่างทันท่วงที เพื่อที่จะได้จำกัดความเสียหายที่อาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคล และเมื่อเกิดเหตุการณ์ดังกล่าวขึ้นแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลจะต้อง

ดำเนินการตรวจสอบเหตุการณ์ที่เกิดขึ้นโดยละเอียดเพื่อที่จะได้ระบุสาเหตุแห่งการละเมิดข้อมูลส่วนบุคคลและหามาตรการในการแก้ไขเยียวยาเหตุการณ์ที่เกิดขึ้นได้โดยเร็ว โดยจะต้องแจ้งเหตุการณ์ดังกล่าวให้กับบุคคลที่เกี่ยวข้องอย่างตรงไปตรงมาด้วย

5.3 การดำเนินการของบุคคลทั่วไปและเจ้าของข้อมูลส่วนบุคคล

ผลการศึกษาพบว่าการดำเนินการสำหรับบุคคลทั่วไปและเจ้าของข้อมูลส่วนบุคคลที่สำคัญ มีดังนี้

5.3.1 ต้องศึกษาสิทธิของตนเองตามที่กฎหมาย PDPA กำหนดเพื่อให้ทราบถึงสิทธิที่ตนเองมีและสิทธิที่จะการดำเนินการกับหน่วยงานภาครัฐ/ผู้ประกอบการบริษัทต่าง ๆ ที่เก็บข้อมูลไว้โดยสิทธิที่พึงมี ได้แก่ สิทธิในการได้รับการแจ้งให้ทราบรายละเอียด สิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล สิทธิขอให้โอนข้อมูลส่วนบุคคล สิทธิคัดค้านการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคล สิทธิขอให้ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ สิทธิขอให้ระงับการใช้ข้อมูลส่วนบุคคล สิทธิขอให้แก้ไขข้อมูลส่วนบุคคล สิทธิในการร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญในกรณีที่มีการฝ่าฝืนและไม่ปฏิบัติตามกฎหมายหรือประกาศที่ออกตามกฎหมาย PDPA ควรศึกษานโยบายการจัดเก็บข้อมูลหรือการขอสิทธิเข้าใช้ข้อมูลของตนเอง

5.3.2 การป้องกันการรั่วไหลของข้อมูลส่วนบุคคลของตนเอง การป้องกันการรั่วไหลของข้อมูลส่วนบุคคลของตนเองเป็นการกระทำเบื้องต้นในการคุ้มครองข้อมูลของตนเอง ตั้งรหัสผ่านที่คาดเดาได้ยาก มีความหลากหลาย ไม่ซ้ำกับแอคเคาน์อื่น ๆ และเปลี่ยนรหัสผ่านเป็นประจำ หลีกเลี่ยงการใช้ Wi-Fi สาธารณะเพื่อป้องกันการดักจับข้อมูลส่วนบุคคล จดบันทึกประวัติการใช้งานทางการเงินเสมอ ไม่ว่าจะเป็นในช่องทางออนไลน์หรือออฟไลน์ก็ตาม เพื่อป้องกันไม่ให้โดนแฮกบัญชีธนาคารหรือบัตรเครดิต ตรวจสอบประวัติการใช้งานอินเทอร์เน็ตเสมอ เพื่อรักษาตัวเองให้ปลอดภัยจากการติดตามทางออนไลน์ เลือกใช้ระบบรักษาความปลอดภัยในทุกอุปกรณ์ที่มีการเชื่อมต่อออนไลน์ เป็นต้น

5.4 แนวทางการป้องกันและแก้ไขการหลุดรั่วของข้อมูลส่วนบุคคลในทางการปฏิบัติให้สอดคล้องกับกฎหมาย PDPA

ผลการวิจัยพบว่า ผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งเป็นทั้งหน่วยงานภาครัฐ ผู้ประกอบการหรือผู้ให้บริการที่ต้องมีบทบาทเกี่ยวกับเรื่องของการป้องกันและรับมือการหลุดรั่วของข้อมูลส่วนบุคคล โดยแบ่งเป็น 2 เรื่อง คือ หน้าที่ในการ “ป้องกัน” และ หน้าที่ในการ “แก้ไข”

5.4.1 หน้าที่ในการป้องกัน

ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมและมีหน้าที่ในการป้องกันมิให้เกิดการหลุดรั่วของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมเพื่อป้องกันการสูญหาย เข้าถึงใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบและต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป เพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยหลักการดังกล่าวต้องให้ความสำคัญใน 3 ด้านหลัก ๆ คือ

5.4.1.1 ด้านการธำรงไว้ซึ่งความลับ (Confidentiality) ซึ่งเป็นมาตรการในการเตรียมความพร้อมเกี่ยวกับความสามารถของระบบในการควบคุมการเข้าถึงข้อมูล เพื่อรักษาข้อมูลให้เป็นความลับ และป้องกันมิให้บุคคลอื่นที่ไม่เกี่ยวข้องเข้าถึงข้อมูลดังกล่าว

5.4.1.2 ด้านความถูกต้องครบถ้วน (Integrity) ซึ่งเป็นมาตรฐานเกี่ยวกับการสร้างความน่าเชื่อถือของระบบในการทำงานที่ถูกต้องครบถ้วน และเป็นปัจจุบันตลอดเวลา

5.4.1.3 ด้านความพร้อมใช้งาน (Availability) ซึ่งเป็นมาตรการเกี่ยวกับความพร้อมของการใช้งาน เพื่อให้การให้บริการยังคงดำเนินการได้อย่างต่อเนื่อง แม้เกิดปัญหาเกี่ยวกับการหลุดรั่วของข้อมูลส่วนบุคคล

5.4.2 หน้าที่ในการแก้ไข

ผลการวิจัยพบว่ากฎหมายได้กำหนดหน้าที่อีกประการหนึ่งของผู้ควบคุมข้อมูลส่วนบุคคลในการแก้ไข โดยในการแก้ไขปัญหาที่เกิดขึ้น ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแบ่งบุคคลที่เกี่ยวข้องโดยหากเกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการดังนี้

5.4.2.1 กรณีที่ไม่มีความเสี่ยงต่อสิทธิของเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องทำการบันทึกเหตุการณ์ดังกล่าวเอาไว้ เพื่อใช้เป็นหลักฐานในการอ้างอิง

5.4.2.2 กรณีเกิดการละเมิดข้อมูลส่วนบุคคลและมีความเสี่ยงต่อสิทธิของเจ้าของข้อมูลส่วนบุคคลให้ผู้ควบคุมข้อมูลส่วนบุคคล แจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ภายใน 72 ชั่วโมง นับแต่ทราบเหตุการละเมิดข้อมูลส่วนบุคคลเท่าที่จะสามารถกระทำได้

5.4.2.3 กรณีการละเมิดข้อมูลส่วนบุคคลมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล นอกจากจะต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแล้ว ยังมีหน้าที่ต้องแจ้งเหตุการณ์ละเมิดดังกล่าวให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยทันทีด้วย

ข้อเสนอแนะ

ในส่วนนี้ผู้วิจัยจะให้ข้อเสนอแนะ 2 ประเด็น คือ ข้อเสนอแนะที่เป็นผลมาจากการศึกษาวิจัยและข้อเสนอแนะสำหรับการศึกษาวิจัยต่อไป

1. ข้อเสนอเชิงนโยบาย

1.1 ภาครัฐควรกำหนดนโยบายให้มีการทบทวนและประเมินผลการใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 หลังจากที่กฎหมายบังคับใช้ไปแล้ว เพื่อให้กฎหมายฉบับนี้มีความชัดเจนมากขึ้นในบางมาตราที่มีปัญหา

1.2 ต้องมีนโยบายให้มาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอไม่น้อยกว่าประเทศผู้ส่งข้อมูลส่วนบุคคล GDPR หรือ General Data Protection Regulation ของสหภาพยุโรป

1.3 ภาครัฐควรกำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายว่าจะต้องไม่ถูกแทรกแซงโดยหน่วยงานภาครัฐหรือหน่วยงานด้านความมั่นคงของรัฐ ซึ่งเป็นหลักการพื้นฐานของรัฐที่เป็นนิติรัฐที่มุ่งคุ้มครองสิทธิและเสรีภาพของประชาชน

1.4 กำหนดนโยบายการทำงานแบบบูรณาการของหน่วยงานที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

1.5 ภาครัฐต้องมีบทบาทสำคัญในการกระตุ้นและส่งเสริมให้ทุกภาคส่วนยอมรับและตระหนักในเรื่องการคุ้มครองข้อมูลส่วนบุคคล

1.6 ภาครัฐควรมีนโยบายมอบให้กระทรวงอุดมศึกษาฯ ร่วมมือกับหน่วยงานที่เกี่ยวข้องของภาครัฐ เช่น สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ในการจัดทำหลักสูตรพื้นฐานด้านการคุ้มครองข้อมูลส่วนบุคคลสำหรับการเรียนการสอนในระดับอุดมศึกษา เพื่อผลิตกำลังคนที่มีความรู้ความสามารถในการทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลทั้งด้านกฎหมายด้านความเชี่ยวชาญทางเทคโนโลยีสารสนเทศ

2. ข้อเสนอเชิงปฏิบัติการ

2.1 ข้อเสนอแนะสำหรับภาครัฐ มีดังนี้

2.1.1 ภาครัฐต้องมีการประชาสัมพันธ์และให้ความรู้เกี่ยวกับกฎหมาย PDPA ในการคุ้มครองข้อมูลส่วนบุคคลให้แก่ประชาชนรับรู้อย่างต่อเนื่อง

2.1.2 กรณีที่ภาครัฐจะต้องเก็บรวบรวมและใช้ข้อมูลส่วนบุคคล ภาครัฐควรจะต้องมีการแจ้งให้ประชาชนทราบเพื่อให้ประชาชนสามารถใช้สิทธิของตนเองได้ตามกฎหมายเพื่อประโยชน์ของประชาชนในการควบคุมสิทธิในข้อมูลส่วนบุคคลของตนเอง

2.1.3 ส่งเสริมสนับสนุนการวิจัยพัฒนาด้านการคุ้มครองข้อมูลส่วนบุคคลให้ได้ตามมาตรฐานสากล

2.2 ข้อเสนอแนะสำหรับภาคเอกชน/ผู้ประกอบการ

2.2.1 การสร้างความร่วมมือเป็นภาคีเครือข่ายกับทุกภาคส่วน ทั้งภาครัฐ ภาคธุรกิจ และภาคประชาสังคมเพื่อร่วมกันแก้ไขปัญหาการละเมิดข้อมูลส่วนบุคคล

2.2.2 ผู้ประกอบการ/ผู้ให้บริการต้องมีการกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่มีมาตรฐานสากล สามารถตรวจสอบและป้องกันการหลุดรั่วของข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพและเมื่อเกิดเหตุการณ์หลุดรั่วของข้อมูลส่วนบุคคลแล้วจะต้องมีมาตรการในการตรวจสอบเพื่อให้พบเหตุดังกล่าวอย่างทันท่วงทีเพื่อที่จะได้จำกัดความเสียหายที่อาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคล

2.3 ข้อเสนอแนะสำหรับเจ้าของข้อมูล

2.3.1 ศึกษาสิทธิของตนเองตามที่กฎหมาย PDPA กำหนดเพื่อให้ทราบถึงสิทธิที่ตนเองมีและสิทธิที่จะการดำเนินการกับหน่วยงานภาครัฐ/ผู้ประกอบการบริษัทต่าง ๆ ที่เก็บข้อมูลไว้

2.3.2 การป้องกันการรั่วไหลของข้อมูลส่วนบุคคลของตนเองเป็นการกระทำเบื้องต้นในการคุ้มครองข้อมูลของตนเอง ตั้งรหัสผ่านที่คาดเดาได้ยาก มีความหลากหลายและไม่ซ้ำกับแอคเคาน์อื่น ๆ เปลี่ยนรหัสผ่านเป็นประจำและหลีกเลี่ยงการใช้ Wi-Fi สาธารณะเพื่อป้องกันการดักจับข้อมูลส่วนบุคคล

3. ข้อเสนอแนะในการศึกษาวิจัยครั้งต่อไป

3.1 ศึกษาวิจัยถึงปัจจัยที่ส่งผลต่อการละเมิดข้อมูลส่วนบุคคลเพื่อได้ทราบถึงสาเหตุของปัญหาที่สำคัญและนำไปสู่การประยุกต์ใช้ในการหาทางป้องกันและแก้ไขปัญหา

3.2 ศึกษาเปรียบเทียบแนวทางการคุ้มครองข้อมูลส่วนบุคคลของประเทศต่าง ๆ กับการดำเนินงานของประเทศไทย เพื่อนำผลการวิจัยมาประยุกต์ใช้ให้เกิดประโยชน์ต่อไป

บรรณานุกรม

ภาษาไทย

หนังสือ

คณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ, สำนักงาน. ยุทธศาสตร์ชาติ พ.ศ. 2561-2580. พิมพ์ครั้งที่ 2. กรุงเทพฯ : สานักงานคณะกรรมการยุทธศาสตร์ชาติ, สำนักงานคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ, 2562.

คณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ, สำนักงาน. การศึกษา Thailand Digital Outlook. กรุงเทพฯ : บริษัท ไฮสปีด เลเซอร์ปริ้นต์จำกัด (สำนักงานใหญ่), 2564.

เทคโนโลยีสารสนเทศและการสื่อสาร, กระทรวง. แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม 20 ปี. กรุงเทพฯ : กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, 2559.

วีรชัย ตันติวีระวิทยา. In Search of Excellence. กรุงเทพฯ : ซีเอ็ดยูเคชั่น, 2530.

วารสาร

นพดล นิ่มหนู. “พัฒนาการของการคุ้มครองสิทธิในความเป็นส่วนตัว เกี่ยวกับข้อมูลส่วนบุคคลในประเทศไทย”. Journal of Politics and Governance. 12(2), May – August 2022. หน้า 161-177.

นิกร โภคอุดม. “ความเป็นส่วนตัวของข้อมูลในยุคดิจิทัล”. วารสารวิชาการมหาวิทยาลัยอีสเทิร์นเอเชีย. 14(2). พฤษภาคม - สิงหาคม 2563. หน้า 59-69.

ภาระวี ปุณเสรีพิพัฒน์. “มาตรการทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมอิเล็กทรอนิกส์ : ศึกษากรณีการใช้คุกกี้บนอินเทอร์เน็ต”. วารสารนิติศาสตร์ มหาวิทยาลัยนเรศวร. 7(1), พฤษภาคม 2557. หน้า 166-193.

วิทยานิพนธ์ รายงานการวิจัย

จันทร์ทิพย์ แสงแปง. “ปัญหาการคุ้มครองข้อมูลส่วนบุคคล ศึกษากรณีการจัดเก็บข้อมูลส่วนบุคคลในหน่วยงานเอกชน”. วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, สถาบันบัณฑิตพัฒนบริหารศาสตร์, 2559.

ณฐพร วิริยะลัพภะ และธเนศ สุจารีกุล. “ปัญหาทางกฎหมาย : พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ศึกษากรณีหน้าที่ของผู้คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 39”. การประชุมนำเสนอรายงานการวิจัยระดับบัณฑิตศึกษา, 2563.

ปัทมา มัญชุนากร. “ปัญหากฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในเครือข่ายสังคมออนไลน์ : ศึกษากรณีผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล ตาม

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562". วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, สถาบันบัณฑิตพัฒนบริหารศาสตร์, 2564.

อริยะ ตังสวานิช. "ปัญหาการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในสถาบันการเงินภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562". วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, จุฬาลงกรณ์มหาวิทยาลัย, 2563.

เอกสารไม่ตีพิมพ์

พระปกเกล้า, สถาบัน. "แนวปฏิบัติสำหรับการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล". เอกสารแผนงาน, 2563.

กฎหมาย

"ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ.2563". ราชกิจนุเบกษา. เล่มที่ 137 ตอนพิเศษ 164 ง. 17 กรกฎาคม 2563. หน้า 12.

"พระราชบัญญัติการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ.2560". ราชกิจนุเบกษา. เล่มที่ 134 ตอนพิเศษ 10 ก. 24 มกราคม 2560. หน้า 1 - 10.

"พระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม (ฉบับที่ 17) พ.ศ.2559". ราชกิจนุเบกษา. เล่มที่ 133 ตอนที่ 80 ก. 15 กันยายน 2559. หน้า 1 - 6.

"พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562". ราชกิจนุเบกษา. เล่มที่ 136 ตอนที่ 67 ก. 22 พฤษภาคม 2562. หน้า 57 - 66.

"พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562". ราชกิจนุเบกษา. เล่มที่ 136 ตอนที่ 69 ก. 22 พฤษภาคม 2562. หน้า 20 - 22.

"พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562". ราชกิจนุเบกษา. เล่มที่ 136 ตอนที่ 69 ก. 27 พฤษภาคม 2562. หน้า 52 - 55.

"พระราชบัญญัติสภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย พ.ศ. 2562". ราชกิจนุเบกษา. เล่มที่ 136 ตอนที่ 56 ก. 30 เมษายน 2562. หน้า 69 - 70.

"พระราชบัญญัติสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2562". ราชกิจนุเบกษา. เล่มที่ 136 ตอนที่ 49 ก. 14 เมษายน 2562. หน้า 45/14.

"พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 4) พ.ศ. 2562". ราชกิจนุเบกษา. เล่มที่ 136 ตอนที่ 67 ก. 22 พฤษภาคม 2562. หน้า 203 - 207.

ฐานข้อมูลอิเล็กทรอนิกส์

เขมภัทร ทฤษฎีคุณ. "สำรวจความพร้อมภาครัฐ ปฏิบัติตาม PDPA". (ออนไลน์) เข้าถึงจาก : https://www.bangkokbiznews.com/columnist/1012966, 2565.

คุ้มครองข้อมูลส่วนบุคคล, สำนักงาน. “สถิติข้อมูลการละเมิดข้อมูลส่วนบุคคล”. (ออนไลน์) เข้าถึงจาก : https://www.mdes.go.th/mission/82, 2565.

ภัทรพร กายบริบูรณ์. “3 หลักสำคัญ ธุรกิจเตรียมพร้อม PDPA”. (ออนไลน์) เข้าถึงจาก : https://thestandard.co/3-importance-of-pdpa-business-preparation/, 2565.

Sanpob Pornwattanakij. “การหลุดรั่วของข้อมูลส่วนบุคคลในประเทศไทย และแนวทางเบื้องต้นในการปฏิบัติให้สอดคล้องกับกฎหมาย PDPA”. (ออนไลน์) เข้าถึงจาก : https://www.everydaymarketing.co/knowledge/leakage-of-personal-information/, 2564.

ภาษาต่างประเทศ

Books

Bunaramrueang, P., Elamchamroonlarp, P., Oinpat, C., & Thipsamritkul, T. Thailand data protection guidelines 2.0. Bangkok : Chulalongkorn University, 2019.

Journals

Martino, M. D., Robyns, P., Weyts, W., Quax, P., Lamotte, W., & Andries, K. Personal Information Leakage by Abusing the GDPR “Right of Access”. Proceedings of the Fifteenth Symposium on Usable Privacy and Security. August 12–13, 2019 - Santa Clara, CA, USA. 371-386.

Electronic Data Base

Björn, G. “Study: Google Is the Biggest Beneficiary of the GDPR”. (online) available : https://cliqz.com/en/magazine/study-google-is-the-biggest-ene ficiary-ofthe-gdp, 2018.

Russel, J. “RIP Klout”. (online) available from: https://techcrunch.com/2018/05/10/rip-klout/, 2018.

The International Association of Privacy Professionals (IAPP). “Global 500 compa nies to spend $7.8B on GDPR compliance”. (online) available from: https://iapp.org/ news/a/survey, 2018.

The Internet Corporation for Assigned Names and Numbers (ICANN). “Temporary Specification for gTLD Registration Data”. (online) available from: https://www.icann.org/resources/pages/gtld-registration-data-specs-en, 2018.

ภาคผนวก

แบบสัมภาษณ์เชิงลึก
หัวข้อ “แนวทางการแก้ไขปัญหาและการป้องกันการละเมิดข้อมูลส่วนบุคคล
เพื่อการปฏิรูปประเทศไทยสู่ดิจิทัลไทยแลนด์”

ชื่อ.....อาชีพ.....
ตำแหน่ง.....

คำถามในการสัมภาษณ์

1. ท่านมีความเข้าใจในกฎหมาย PDPA หรือไม่ อย่างไร

.....

2. ในความคิดเห็นของท่านคิดว่า กฎหมาย PDPA มีประโยชน์ต่อท่านหรืออาชีพของท่านหรือไม่ อย่างไร

.....

3. การที่ภาครัฐได้มีการออกกฎหมาย PDPA ฉบับนี้มาท่านคิดว่าภาครัฐได้สร้างความรู้ ความเข้าใจให้ประชาชนและผู้ประกอบการ หรือไม่ อย่างไร

.....

4. กฎหมาย PDPA ได้สร้างผลกระทบต่อการทำงานของท่านหรือองค์กรของท่านบ้างหรือไม่ อย่างไร

.....

5. ท่านคิดว่าปัญหาและอุปสรรคสำคัญต่อการใช้กฎหมายนี้ในการคุ้มครองข้อมูลส่วนบุคคล ในมุมมองของอาชีพท่านมีอะไรบ้าง

.....

6. สำหรับตัวท่านเคยได้รับการละเมิดข้อมูลส่วนบุคคลบ้างหรือไม่ และท่านมีวิธีจัดการเรื่องนี้อย่างไร

.....

7. ข้อแนะนำสำหรับการใช้กฎหมาย PDPA ฉบับนี้ในการคุ้มครองข้อมูลส่วนบุคคล มีอะไรบ้างในมุมมองของท่าน

.....

ประวัติย่อผู้วิจัย

ชื่อ-นามสกุล นายปรนนท์ ฐิตะวรรโณ
วัน เดือน ปีเกิด 1 พฤษภาคม 2515
ประวัติการศึกษา

- ปริญญาโท Telecommunication Management National University
- ปริญญาตรี วิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมอุตสาหการ มหาวิทยาลัยเกษตรศาสตร์
- ระดับสามัญศึกษา
  - ระดับมัธยมศึกษา โรงเรียนเตรียมอุดมศึกษา
  - ประถมศึกษา โรงเรียนกรุงเทพคริสเตียนวิทยาลัย

ตำแหน่งปัจจุบัน

- กรรมการบริหารสภาอุตสาหกรรมแห่งประเทศไทย
- กรรมการผู้จัดการบริษัทอินฟอร์เมชั่นเอนเตอร์ไพรส์ จำกัด

สรุปย่อ

ลักษณะวิชา ยุทธศาสตร์
เรื่อง แนวทางการแก้ไขปัญหาและการป้องกันการละเมิดข้อมูลส่วนบุคคลเพื่อการปฏิรูปประเทศไทยสู่ดิจิทัลไทยแลนด์
ผู้วิจัย นายปรนนท์ ฐิตะวรรโณ **หลักสูตร** วปอ. **รุ่นที่** 65
ตำแหน่ง กรรมการบริหารสภาอุตสาหกรรมแห่งประเทศไทย

ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันด้วยความเจริญของเทคโนโลยีทำให้การติดต่อสื่อสารสามารถเดินทางติดต่อสื่อสารถึงกันได้ทั่วทุกมุมของโลกอย่างไร้ขีดจำกัด ทำให้เกิดปัญหาติดตามมาคือการแย่งชิงกันครอบครองข้อมูล เพื่อให้มีข้อมูลมาใช้ประโยชน์ในกิจการของตนเองให้มากที่สุดเพื่อการมีโอกาสและมีอิทธิพลอำนาจเหนือกว่าผู้อื่น ซึ่งข้อมูลเหล่านี้จะมีข้อมูลข่าวสารส่วนหนึ่งที่เป็นข้อมูลส่วนบุคคลรวมอยู่ด้วย จึงทำให้เกิดปัญหาตามมาคือมีการนำข้อมูลส่วนบุคคลไปใช้โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล ทำให้เกิดปัญหาการละเมิดความเป็นส่วนตัวในข้อมูลส่วนบุคคลเป็นวงกว้างอยู่ในขณะนี้และเนื่องจากการพัฒนาด้านเทคโนโลยีสารสนเทศเติบโตอย่างรวดเร็ว ทำให้สามารถจัดเก็บรวบรวม ข้อมูลข่าวสารต่าง ๆ ได้เป็นจำนวนมากและสามารถเรียกดู ตรวจสอบ วิเคราะห์ ประมวลผล เผยแพร่รับ–ส่ง แลกเปลี่ยนข้อมูลได้อย่างสะดวกและรวดเร็ว ส่งผลกระทบต่อความเป็นส่วนตัวคือการนำข้อมูลส่วนบุคคลไปใช้ประมวลผลหรือเปิดเผยทำให้ผู้เป็นเจ้าของข้อมูลอาจได้รับความเสียหาย เช่นเรื่องของความปลอดภัยในชีวิต สิทธิและเสรีภาพของบุคคลของเจ้าของข้อมูล สำหรับประเทศไทยได้มีการบัญญัติให้การรับรองและคุ้มครองสิทธิส่วนบุคคลและข้อมูลส่วนบุคคลไว้ในรัฐธรรมนูญแห่งราชอาณาจักรไทยมาตั้งแต่อดีตที่ผ่านมาจนถึงปัจจุบัน โดยรับรองไว้อย่างชัดเจนจนถึงปัจจุบันภายใต้รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 บัญญัติไว้ในมาตรา 32 ให้การรับรองและคุ้มครองสิทธิส่วนบุคคลและข้อมูลส่วนบุคคลเช่นเดียวกัน จนในปัจจุบันประเทศไทยมีกฎหมายเกี่ยวกับการคุ้มครองข้อมูลข่าวสารส่วนบุคคล โดยเฉพาะคือพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act: PDPA) ทั้งนี้ได้เริ่มบังคับใช้ตั้งแต่ในวันที่ 1 มิถุนายน 2565 พระราชบัญญัติฯ ฉบับนี้มีลักษณะเป็นกฎหมายกลางที่ครอบคลุมการดำเนินการของบุคคลหรือนิติบุคคลที่เป็นหน่วยงานภาครัฐและภาคเอกชนที่ทำการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลต้อง ปฏิบัติตามหลักเกณฑ์ วิธีการ และเงื่อนไขตามที่กำหนด ส่งผลทำให้ทุกภาคส่วนทั้งประชาชนทั่วไป บริษัทเอกชนและหน่วยงานภาครัฐต่างๆ ต้องมีความเข้าใจต่อกฎหมายอย่างถูกต้อง เข้าใจวิธีการดูแลเรื่องความปลอดภัยข้อมูลส่วนบุคคลและการปฏิบัติตามหลักเกณฑ์ข้อกำหนดที่ถูกต้อง แต่อย่างไรก็ตามในการดำเนินการด้านการจัดการข้อมูลส่วนบุคคลยังต้องอาศัยแนวทางอีกหลายด้านเพื่อแก้ไขปัญหาและการป้องกันการละเมิดข้อมูลส่วนบุคคล ด้วยเหตุผลที่กล่าวมาผู้วิจัยจึงมีความสนใจแนวทางการแก้ไขปัญหาและการป้องกันการละเมิดข้อมูลส่วนบุคคลในการ

พัฒนาประเทศสู่ดิจิทัลไทยแลนด์เพื่อเป็นประโยชน์ต่อหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและภาคเอกชนต่อไปในการนำไปประยุกต์ใช้

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาสถานการณ์และแนวโน้มการละเมิดข้อมูลส่วนบุคคลผ่านระบบดิจิทัลและผลกระทบต่อการพัฒนาประเทศ
2. เพื่อศึกษาปัญหาและอุปสรรคในการดำเนินการแก้ไขปัญหาและผลกระทบการละเมิดข้อมูลส่วนบุคคลผ่านเทคโนโลยีดิจิทัล
3. เพื่อศึกษาแนวทางการแก้ไขปัญหาและการป้องกันการละเมิดข้อมูลส่วนบุคคลในการพัฒนาประเทศสู่ดิจิทัลไทยแลนด์

ขอบเขตของการวิจัย

1.ขอบเขตด้านเนื้อหา

การวิจัยนี้เน้นการศึกษาหาแนวทางการแก้ไขปัญหาและการป้องกันเหตุละเมิดข้อมูลส่วนบุคคลทั้งเชิงรับและเชิงรุกที่เหมาะสมในภาพรวมของประเทศไม่ได้เจาะจงเฉพาะหน่วยงานใดหน่วยงานหนึ่ง

2. ขอบเขตด้านประชากร

ประชากรในงานวิจัยนี้คือทุกภาคส่วน โดยภาคประชาชนจะเป็นทั้งเจ้าของข้อมูลและผู้จัดเก็บข้อมูล ในส่วนของภาคเอกชนเป็นเรื่องการจัดเก็บและการนำข้อมูลไปใช้งานตามวัตถุประสงค์ของเจ้าของข้อมูล และในส่วนของภาครัฐและภาคเอกชน เป็นเรื่องการเป็นผู้ทำหน้าที่คุ้มครองข้อมูลส่วนบุคคล การจัดเก็บ การนำข้อมูลไปใช้งานและกฎระเบียบที่เกี่ยวข้อง รวมไปถึงระบบและงบประมาณที่ใช้ในการดำเนินการจัดการข้อมูลส่วนบุคคลในปัจจุบันและอนาคต

3. ขอบเขตด้านเวลา

การศึกษาวิจัยเริ่มตั้งแต่วันที่ 1 ตุลาคม 2565 จนถึงวันที่ 31 พฤษภาคม 2566

วิธีดำเนินการวิจัย

ในการวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) โดยการนำเนื้อหามาทำการวิเคราะห์ (Content Analysis)

1. การเก็บรวบรวมข้อมูล

1.1 ข้อมูลปฐมภูมิ เก็บรวบรวมจากโดยการทำเก็บข้อมูลภาคสนาม รวบรวมข้อมูลจากการสัมภาษณ์ผู้ที่เกี่ยวข้องทั้งระดับนโยบาย ผู้จัดเก็บข้อมูลและผู้ใช้ข้อมูล

1.2 ข้อมูลทุติยภูมิ เก็บรวบรวมจากทำการศึกษา รวบรวม ค้นคว้า ข้อมูลจากการดำเนินการจากเอกสารและงานวิจัยที่เกี่ยวข้อง รวมถึงทำการศึกษากฎหมาย ยุทธศาสตร์ แผนปฏิบัติการด้านข้อมูลส่วนบุคคล

2. การวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลจะดำเนินการจากข้อมูลการศึกษาเอกสารที่เกี่ยวข้อง รวมถึงข้อมูลที่ได้จากภาคสนาม และดำเนินการตามกรอบแนวคิดของการวิจัยในครั้งนี้เพื่อให้เกิดแนวทางการแก้ไขปัญหาและการป้องกันการละเมิดข้อมูลส่วนบุคคลเพื่อการปฏิรูปประเทศไทยสู่ดิจิทัลไทยแลนด์

3. การนำเสนอข้อมูล

การนำเสนอและสรุปผลการศึกษาวิจัยเชิงพรรณนาในรูปแบบรายงานเพื่อนำเสนอแนวทางการแก้ไขปัญหาและการป้องกันการละเมิดข้อมูลส่วนบุคคล

ผลการวิจัย

ผลการวิจัยเพื่อตอบวัตถุประสงค์ข้อที่ 1 เพื่อศึกษาสถานการณ์และแนวโน้มการละเมิดข้อมูลส่วนบุคคลผ่านระบบดิจิทัลและผลกระทบต่อการพัฒนาประเทศ

1. ประเทศไทยมีกฎหมายเกี่ยวกับการคุ้มครองข้อมูลข่าวสารส่วนบุคคล โดยเฉพาะคือ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือกฎหมาย PDPA ซึ่งมีลักษณะเป็นกฎหมายกลางที่ครอบคลุมการดำเนินการของบุคคลหรือนิติบุคคลที่เป็นหน่วยงานภาครัฐและภาคเอกชนที่ทำการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลส่วนบุคคลต้องปฏิบัติตามหลักเกณฑ์ วิธีการและเงื่อนไขตามที่กำหนด

2. หลังการประกาศใช้พระราชบัญญัติดังกล่าว สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นองค์กรอิสระตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้รับเรื่องการถูกร้องเรียนในเรื่องการฝ่าฝืนกฎหมาย เรื่องการบังคับให้ความยินยอมเพื่อเปิดใช้บริการ การถูกเก็บข้อมูลส่วนบุคคลมาจากแหล่งอื่นโดยมิชอบ ไม่เปิดให้ใช้สิทธิขอรับสำเนาข้อมูลหรือลบข้อมูลตามกฎหมาย และเรื่องการใช้และเปิดเผยข้อมูลระหว่างบุคคลธรรมดา เป็นต้น สาเหตุสำคัญคือ ระบบคอมพิวเตอร์ขององค์กรถูกเจาะระบบ กระบวนการควบคุมขั้นตอนการเปิดเผยข้อมูลส่วนบุคคลขององค์กรยังไม่รัดกุม และพนักงานดำเนินการผิดพลาดส่งข้อมูลให้ผู้รับผิดคน เป็นต้น

3. ผลกระทบของการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

3.1 ผลกระทบในแง่ภาระต้นทุนทางธุรกิจของผู้ประกอบการในด้านการลงทุนระบบการคุ้มครองข้อมูลส่วนบุคคลทั้งในด้านทรัพยากรบุคลคล เทคโนโลยีที่นำมาใช้

3.2 ผลกระทบต่อการแข่งขันทางการค้าที่ไม่เป็นธรรม ธุรกิจขนาดใหญ่ ซึ่งมีงบประมาณเพื่อการนี้เช่นการอัพเกรดระบบป้องกันการจ้างผู้เชี่ยวชาญด้านความปลอดภัย การร่างสัญญาและนโยบาย แต่จะสร้างความเสียเปรียบแก่ผู้ประกอบการขนาดกลางและย่อม (SMEs) ที่มีต้นทุนต่ำกว่าทำให้เกิดปัญหาความเหลื่อมล้ำไม่เป็นธรรมทางการค้า

3.3 ผลกระทบในแง่การค้าและการลงทุนระหว่างประเทศ การละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นในประเทศอยู่บ่อยครั้งย่อมส่งผลต่อความเชื่อมั่นต่อประเทศคู่ค้าได้ ทั้งนี้เพราะต้องมีการส่งข้อมูลข้ามแดนกัน

3.4 ผลกระทบในการสร้างโอกาสให้เกิดการโจรกรรมข้อมูลส่วนบุคคล การโจรกรรมข้อมูลด้วยวิธีการวิศวกรรมทางสังคม การแสวงหาข้อมูลจากแหล่งต่าง ๆ เช่น สื่อสังคมออนไลน์ สามารถนำไปประกอบในการปลอมตัว เป็นเจ้าของข้อมูลและยื่นคำร้องต่อผู้ควบคุมข้อมูลขอใช้สิทธิเข้าถึงข้อมูลทำให้สูญเสียด้านต่างๆทั้งข้อมูลส่วนบุคคล การเงิน เกิดความสูญเสียทางเศรษฐกิจ

3.5 ผลกระทบต่อสิทธิเสรีภาพของบุคคล การที่ผู้ประกอบการใช้วิธีการปฏิบัติเพื่อให้สอดคล้องกับกฎหมายด้วยเทคนิคต่าง ๆ อันส่งผลให้เจ้าของข้อมูลมีความเสี่ยงต่อการถูกล่วงละเมิดข้อมูลส่วนบุคคลมากขึ้น นอกจากนั้นยังกระทบต่อสิทธิในการแสดงความคิดเห็น เช่น กรณีสิทธิของเจ้าของข้อมูลในการขอให้ลบหรือทำลายข้อมูลระบุตัวของตนเปิดทางให้มีการใช้เพื่อวัตถุประสงค์อื่น

ผลการวิจัยเพื่อตอบวัตถุประสงค์ข้อที่ 2 เพื่อศึกษาปัญหาและอุปสรรคในการดำเนินการแก้ไขปัญหาและผลกระทบการละเมิดข้อมูลส่วนบุคคลผ่านเทคโนโลยีดิจิทัล

1. ปัญหาความไม่ชัดเจนของกฎหมายเพราะกฎหมายใหม่อาจมีการตีความไม่ได้ชัดเจนในบางมาตรา

2. ปัญหาการยกเว้นทางกฎหมายให้กับการใช้ข้อมูลส่วนบุคคลในหน่วยงานของรัฐอาจจะทำให้มีปัญหาให้หน่วยงานของรัฐใช้หรือเข้าถึงข้อมูลส่วนบุคคลโดยปราศจากความรับผิดชอบและกลายเป็นการซ้ำเติมปัญหาการพ้นผิดเมื่อเกิดการละเมิดข้อมูลส่วนบุคคลของภาครัฐและบั่นทอนความเชื่อมั่นของประชาชนถ้ามีการรั่วไหลของข้อมูลจากภาครัฐ

3. ปัญหาข้อกฎหมายในการเคลื่อนย้ายข้อมูลส่วนบุคคลข้ามพรมแดน อิทธิพลของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ได้สร้างมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลใหม่ทั่วโลก หากประเทศไทยไม่มีมาตรฐานเทียบเท่า ซึ่งทำให้การเคลื่อนย้ายข้อมูลส่วนบุคคลเข้ามาในประเทศไทยทำได้ยากและทำให้เอกชนของประเทศไทยอาจจะพลาดโอกาสในการเติบโตในยุคเศรษฐกิจดิจิทัล

4. ปัญหาการร้องเรียนการละเมิดข้อมูลส่วนบุคคล ทั้งนี้พบว่าปัญหาการร้องเรียนการละเมิดข้อมูลส่วนบุคคลนี้มีแนวโน้มจะเพิ่มขึ้นเนื่องจากประชาชนทั่วไปการไม่เข้าใจในตัวกฎหมายที่บังคับใช้

5. การขาดแคลนทรัพยากรที่จำเป็นต่อการปฏิบัติหน้าที่ขององค์กรทั้งภาครัฐและภาคเอกชนตามกฎหมาย เช่นการขาดแคลนบุคลากร งบประมาณรวมถึงเทคโนโลยีที่ต้องใช้ในระบบ

6. ประชาชนขาดความรู้และความเข้าใจในกฎหมาย พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 เพราะเป็นกฎหมายใหม่และมีรายละเอียดที่เกี่ยวข้องกับตัวบุคคลค่อนข้างมาก การที่ขาดความรู้และความเข้าใจในตัวกฎหมายอย่างถ่องแท้จึงสร้างความกังวลและสับสนให้กับประชาชน

7. มาตรฐานรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลขององค์กรยังไม่มีประสิทธิภาพเพียงพอทำให้สามารถทำให้เกิดการหลุดรั่วของข้อมูลส่วนบุคคลได้ เจ้าหน้าที่ขาดความชำนาญในการดูแลระบบ

8. ปัญหากฎหมายคุ้มครองข้อมูลส่วนบุคคลได้เป็นการเพิ่มภาระค่าใช้จ่ายให้ทั้งภาครัฐและผู้ประกอบการภาคเอกชนที่ต้องมีข้อมูลจำนวนมากในการครอบครอง

ผลการวิจัยเพื่อตอบวัตถุประสงค์ข้อที่ 3 เพื่อศึกษาแนวทางการแก้ไขปัญหาและการป้องกันการละเมิดข้อมูลส่วนบุคคลในการพัฒนาประเทศสู่ดิจิทัลไทยแลนด์

การดำเนินการของภาครัฐ

1.สร้างความเข้าใจและความชัดเจนในบทบาทหน้าที่ของภาครัฐในฐานะผู้ควบคุมข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2. หน่วยงานของภาครัฐต้องมีนโยบายและแนวปฏิบัติภายในหน่วยงานทุกหน่วยเพื่อรองรับการปฏิบัติตามกฎหมาย PDPA

3. การประเมินผล การทบทวนและปรับปรุงกฎหมาย PDPA ในการคุ้มครองข้อมูลส่วนบุคคล จึงมีความจำเป็นอย่างยิ่งที่จะต้องติดตามประกาศของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้เข้าใจถึงการใช้และการตีความกฎหมายต่อไป อีกทั้งเพื่อสร้างความเข้าใจให้กับผู้ใช้กฎหมายและประชาชน

4. ภาครัฐต้องมีการประชาสัมพันธ์และให้ความรู้เกี่ยวกับกฎหมาย PDPA ในการคุ้มครองข้อมูลส่วนบุคคลให้แก่ประชาชนรับรู้

5. ส่งเสริมและสนับสนุน การวิจัย เพื่อพัฒนาเทคโนโลยีที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

6. การจัดทำหลักสูตรในระดับอุดมศึกษา/การวิจัยพัฒนาด้านการคุ้มครองข้อมูลส่วน

การดำเนินงานของภาคเอกชน/ผู้ประกอบการ

1. การสร้างความตระหนักรู้ของบุคลากรและบุคคลที่เกี่ยวข้องในการปฏิบัติตามกฎหมาย PDPA ด้วยการจัดอบรมให้ผู้บริหารองค์กร การจัดอบรมให้คณะทำงานตามกรอบกฎหมาย PDPA

2. การกำหนดแนวทางขององค์กรเพื่อควบคุมดูแลการปฏิบัติตามกฎหมาย PDPA โดยอย่างน้อยต้องประกอบด้วยมาตรการ ดังนี้ กำหนดนโยบายและนิยามความหมายของข้อมูลส่วนบุคคล การกำหนดขั้นตอนการตรวจสอบข้อมูลส่วนบุคคล การระบุความเชื่อมโยงและเส้นทางการส่งข้อมูลส่วนบุคคลที่จะเกิดขึ้นในองค์กรรวมถึงระบุแหล่งที่จะได้มาซึ่งข้อมูลส่วนบุคคลทั้งหลาย การกำหนดความเสี่ยงของข้อมูลส่วนบุคคลชุดต่างๆ มีมาตรการคุ้มครองข้อมูลส่วนบุคคล

3. การสร้างมาตรฐานความมั่นคงปลอดภัยทางด้านเทคโนโลยีเพื่อคุ้มครองข้อมูลส่วนบุคคลให้ได้ตามมาตรฐานสากล

4. มีการกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่มีมาตรฐานสากลสามารถตรวจสอบและป้องกันการหลุดรั่วของข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพและเมื่อเกิดเหตุการณ์หลุดรั่วของข้อมูลส่วนบุคคลแล้วจะต้องมีมาตรการในการตรวจสอบ

การดำเนินการของบุคคลทั่วไปและเจ้าของข้อมูลส่วนบุคคล

1. ต้องศึกษาสิทธิของตนเองตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อให้ทราบถึงสิทธิที่ตนเองมีและสิทธิที่จะการดำเนินการกับหน่วยงานภาครัฐ/ผู้ประกอบการบริษัทต่าง ๆ ที่เก็บข้อมูลไว้

2. การป้องกันการรั่วไหลของข้อมูลส่วนบุคคลของตนเองเป็นการกระทำเบื้องต้นในการคุ้มครองข้อมูลของตนเอง ตั้งรหัสผ่านที่คาดเดาได้ยาก และเปลี่ยนรหัสผ่านเป็นประจำ เลือกใช้ระบบรักษาความปลอดภัยในทุกอุปกรณ์ที่มีการเชื่อมต่อออนไลน์ เป็นต้น

ข้อเสนอแนะ

1. ข้อเสนอแนะเชิงนโยบาย

1.1 ภาครัฐควรกำหนดนโยบายให้มีการทบทวนและประเมินผลการใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 หรือกฎหมาย PDPA เพื่อให้กฎหมายฉบับนี้มีความชัดเจนมากขึ้นในบางมาตราที่มีปัญหา

1.2 ต้องมีนโยบายให้มาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอไม่น้อยกว่าประเทศผู้ส่งข้อมูลส่วนบุคคล GDPR หรือ General Data Protection Regulation ของสหภาพยุโรป

1.3 ภาครัฐควรกำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายว่าจะต้องไม่ถูกแทรกแซงโดยหน่วยงานภาครัฐหรือหน่วยงานด้านความมั่นคงของรัฐ ซึ่งเป็นหลักการพื้นฐานของรัฐที่เป็นนิติรัฐที่มุ่งคุ้มครองสิทธิและเสรีภาพของประชาชน

1.4 กำหนดนโยบายการทำงานแบบบูรณาการของหน่วยงานที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

1.5 ภาครัฐต้องมีบทบาทสำคัญในการกระตุ้นและส่งเสริมให้ทุกภาคส่วนยอมรับและตระหนักในเรื่องการคุ้มครองข้อมูลส่วนบุคคล

1.6 ภาครัฐควรมีนโยบายมอบให้กระทรวงอุดมศึกษาฯ ร่วมมือกับหน่วยงานที่เกี่ยวข้องของภาครัฐ เช่น สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ในการจัดทำหลักสูตรพื้นฐานด้านการคุ้มครองข้อมูลส่วนบุคคลสำหรับการเรียนการสอนในระดับอุดมศึกษาเพื่อผลิตกำลังคนที่มีความรู้ความสามารถในการทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลทั้งด้านกฎหมาย ด้านความเชี่ยวชาญทางเทคโนโลยีสารสนเทศ

2. ข้อเสนอแนะระดับปฏิบัติ

1.1 ภาครัฐต้องมีการประชาสัมพันธ์และให้ความรู้เกี่ยวกับกฎหมาย PDPA ในการคุ้มครองข้อมูลส่วนบุคคลให้แก่ประชาชนรับรู้อย่างต่อเนื่อง

1.2 กรณีที่ภาครัฐจะต้องเก็บรวบรวมและใช้ข้อมูลส่วนบุคคล ภาครัฐควรจะต้องมีการแจ้งให้ประชาชนทราบ เพื่อให้ประชาชนสามารถใช้สิทธิของตนเองได้ตามกฎหมายเพื่อประโยชน์ของประชาชนในการควบคุมสิทธิในข้อมูลส่วนบุคคลของตนเอง

1.3 ส่งเสริมสนับสนุนการวิจัยพัฒนาด้านการคุ้มครองข้อมูลส่วนบุคคลให้ได้ตามมาตรฐานสากล

1.4 การสร้างความร่วมมือเป็นภาคีเครือข่ายกับทุกภาคส่วน ทั้งภาครัฐ ภาคธุรกิจ และภาคประชาสังคมเพื่อร่วมกันแก้ไขปัญหาการละเมิดข้อมูลส่วนบุคคล

1.5 ผู้ประกอบการ/ผู้ให้บริการต้องมีการกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่มีมาตรฐานสากล สามารถตรวจสอบและป้องกันการหลุดรั่วของข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพและเมื่อเกิดเหตุการณ์หลุดรั่วของข้อมูลส่วนบุคคลแล้วจะต้องมีมาตรการในการตรวจสอบเพื่อให้พบเหตุดังกล่าวอย่างทันท่วงทีเพื่อที่จะได้จำกัดความเสียหายที่อาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคล

1.6 เจ้าของข้อมูลศึกษาสิทธิของตนเองตามกฎหมาย PDPA เพื่อให้ทราบถึงสิทธิที่ตนเองมีและสิทธิที่จะการดำเนินการกับหน่วยงานภาครัฐ/ผู้ประกอบการบริษัทต่าง ๆ ที่เก็บข้อมูลไว้

1.8 การป้องกันการรั่วไหลของข้อมูลส่วนบุคคลของตนเองเป็นการกระทำเบื้องต้นในการคุ้มครองข้อมูลของตนเอง ตั้งรหัสผ่านที่คาดเดาได้ยาก มีความหลากหลาย ไม่ซ้ำกับแอคเคาน์อื่น ๆ และเปลี่ยนรหัสผ่านเป็นประจำ หลีกเลี่ยงการใช้ Wi-Fi สาธารณะเพื่อป้องกันการดักจับข้อมูลส่วนบุคคล

3. ข้อเสนอแนะในการทำวิจัยครั้งต่อไป

3.1 ศึกษาวิจัยถึงปัจจัยที่ส่งผลต่อการละเมิดข้อมูลส่วนบุคคล เพื่อได้ทราบถึงสาเหตุของปัญหาที่สำคัญและนำไปสู่การประยุกต์ใช้ในการหาทางป้องกันและแก้ไขปัญหา

3.2 ศึกษาเปรียบเทียบแนวทางการคุ้มครองข้อมูลส่วนบุคคลของประเทศต่าง ๆ กับการดำเนินงานของประเทศไทย เพื่อนำผลการวิจัยมาประยุกต์ใช้ให้เกิดประโยชน์ต่อไป