

กฎหมายดิจิทัลในประเทศไทย Digital Laws in Thailand

นิกร โภคอุดม¹ และสุคนธ์ทิพย์ ทินาภรณ์²

Nikorn Pokudom¹ and Sukontip Tinaporn²

¹สำนักวิชาการ มหาวิทยาลัยอีสเทิร์นเอเซีย

¹Office of Academic Affairs, Eastern Asia University

²คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยอีสเทิร์นเอเซีย

²School of Information Technology, Eastern Asia University

Received: March 31, 2021

Revised: May 14, 2021

Accepted: May 17, 2021

บทคัดย่อ

บทความนี้มีวัตถุประสงค์ในการให้ความรู้เกี่ยวกับภาพรวมของกฎหมายดิจิทัลในประเทศไทยที่ได้มีการปรับปรุงและกำหนดขึ้นเพื่อนำมาใช้ในปัจจุบัน เนื่องจากประเทศไทยได้เล็งเห็นถึงความสำคัญของเทคโนโลยีที่จะเข้ามามีบทบาทมากขึ้นทั้งด้านความบันเทิง การศึกษา การทำงาน ระบบการเงินและเศรษฐกิจ จึงได้จัดทำแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมขึ้นมาเพื่อเพิ่มขีดความสามารถด้านการแข่งขันทางเศรษฐกิจโดยใช้นวัตกรรมและเทคโนโลยีดิจิทัล และยกคุณภาพชีวิตของประชาชนให้มีทักษะในการดำเนินชีวิตและประกอบอาชีพและรับรู้ข้อมูลข่าวสารได้อย่างเท่าเทียมกัน และปรับวิธีการทำงานและการให้บริการของภาครัฐด้วยเทคโนโลยีดิจิทัล แต่การพัฒนาเฉพาะเทคโนโลยีด้านดิจิทัลเพียงอย่างเดียวไม่สามารถสร้างความเชื่อมั่นให้กับประชาชนและภาคธุรกิจได้ ประเทศไทยจึงได้มีการปรับปรุงและกำหนดกฎระเบียบและกติกาด้านดิจิทัลและกฎหมายที่เกี่ยวข้องกับเศรษฐกิจให้มีความทันสมัยและมีประสิทธิภาพ โดยเฉพาะอย่างยิ่งเพื่ออำนวยความสะดวกด้านการค้าและการใช้ประโยชน์ในภาคเศรษฐกิจและสังคม เพื่อสร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัลและการทำธุรกรรมออนไลน์ ด้วยการสร้างความมั่นคง ปลอดภัยของระบบสารสนเทศ และการสื่อสาร การคุ้มครองข้อมูลส่วนบุคคลและการคุ้มครองผู้บริโภค

คำสำคัญ: กฎหมายดิจิทัล กฎหมายคอมพิวเตอร์ กฎหมายธุรกรรมทางอิเล็กทรอนิกส์

Abstract

This article aims to provide knowledge about overall of digital law in Thailand which is adjusted and set to apply now. Thailand is aware of the importance of technology which will play a vital role in entertainment, education, work, financial and economic system; therefore, Thailand has set digital developing plan for economy and society to increase capability of economic competition by using innovation and digital technology. Moreover, it will help to leverage quality life of people to have skills about living and career and people will be able to receive information equally. Also, it helps to adjust working and services of government and private sector. However, developing only digital technology is not enough; it is unable to build creditability for people and business. Therefore, Thailand has improved and set regulation and rule about digital and law that related to economy to be up-to-date and efficient and to facilitate about trading and usefulness of economy and business to build creditability of using digital technology and online transaction by creating stability and safety of information technology and communication, data privacy protection and consumer protection.

Keywords: digital law, computer law, electronic transaction law



บทนำ

ปัจจุบันโลกได้พัฒนาเทคโนโลยีด้านดิจิทัลและเศรษฐกิจที่มีความก้าวหน้าไปมาก ผู้คนในยุคปัจจุบันมีการใช้งานเทคโนโลยีดิจิทัลกันอย่างแพร่หลายไม่ใช่เพียงแค่เครื่องมือที่มาช่วยเหลือในการทำงานเท่านั้นแต่ยังรวมถึงการใช้งานในกิจกรรมของชีวิตประจำวัน เช่น การสื่อสารระหว่างบุคคลผ่านช่องทางออนไลน์ ด้านการติดต่อซื้อขายสินค้าหรือการทำธุรกรรมผ่านระบบเศรษฐกิจที่มีเทคโนโลยีดิจิทัลเข้ามาเกี่ยวข้อง การให้บริการของภาครัฐที่ปรับเปลี่ยนรูปแบบการให้บริการจากแบบเดิมที่ต้องมายื่นเรื่องหรือติดต่อที่ทำการของภาครัฐให้สามารถดำเนินกิจกรรมบางอย่างผ่านช่องทางช่องทางออนไลน์ได้ เช่น การยื่นภาษีออนไลน์ การตรวจสอบค่าน้ำและค่าไฟฟ้าผ่านแอปพลิเคชันบนสมาร์ตโฟน เป็นต้น

จากความก้าวหน้าของเทคโนโลยีดิจิทัลดังกล่าว รัฐบาลไทยโดยกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ได้เห็นความสำคัญจึงได้มีการจัดทำแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมขึ้นมาเมื่อ ปี พ.ศ. 2559

(Ministry of Digital Economy and Society, 2016) เพื่อนำเทคโนโลยีดิจิทัลมาใช้เป็นเครื่องมือในการขับเคลื่อนและพัฒนาประเทศให้มีความก้าวหน้าทั้งทางด้านเศรษฐกิจและสังคม ได้แก่ การลงทุนและพัฒนาอุตสาหกรรมในประเทศและอุตสาหกรรมใหม่ เช่น อุตสาหกรรมดิจิทัล แก้ไขปัญหาความเหลื่อมล้ำของสังคมโดยทำให้ประชาชนมีรายได้ที่มากขึ้น ได้รับสวัสดิการที่ทั่วถึงทั้งด้านการศึกษาและการรักษาพยาบาล การพัฒนาความสามารถในการแข่งขันของธุรกิจในกลุ่ม SMEs ทั้งภาคการเกษตร การผลิตและการบริการ การใช้เทคโนโลยีสำหรับการบริหารจัดการเมื่อประเทศไทยเข้าสู่สังคมสูงวัยและการดูแลผู้สูงอายุการนำการบริหารจัดการข้อมูลภาครัฐด้วยการเปิดเผยข้อมูลให้ประชาชนสามารถเข้าตรวจสอบการทำงานเพื่อแก้ไขปัญหาคอร์รัปชัน โดยในแผนดังกล่าวยังให้ความสำคัญด้านการพัฒนาศักยภาพของคนในประเทศทั้งบุคลากรด้านเทคโนโลยีและบุคลากรที่อยู่ในส่วนของภาคอุตสาหกรรมอื่น ๆ เช่น ในภาคเกษตร และบริการ และการพัฒนาให้ประชาชนทั่วไปมีความสามารถด้านเทคโนโลยีมากขึ้น และมีความเท่าทันต่อการเปลี่ยนแปลงของเทคโนโลยีใหม่ ๆ รวม

ทั้งความฉลาดในการรับรู้ข้อมูลข่าวสารจากสื่อต่าง ๆ โดยเฉพาะสื่อออนไลน์ที่ประชาชนสามารถเข้าถึงได้ง่ายมากที่สุด

แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมฉบับนี้ ประกอบด้วย 6 ยุทธศาสตร์ ซึ่งนำมาใช้เป็นกรอบในการผลักดันให้เทคโนโลยีดิจิทัลเป็นกลไกสำคัญในการพัฒนาเศรษฐกิจและสังคมของประเทศไทย ประกอบด้วย

- 1) ยุทธศาสตร์ที่ 1 พัฒนาโครงสร้างพื้นฐานดิจิทัล ประสิทธิภาพสูงให้ครอบคลุมทั่วประเทศ
- 2) ยุทธศาสตร์ที่ 2 ขับเคลื่อนเศรษฐกิจด้วยเทคโนโลยีดิจิทัล
- 3) ยุทธศาสตร์ที่ 3 สร้างสังคมคุณภาพที่ทั่วถึงเท่าเทียมด้วยเทคโนโลยีดิจิทัล
- 4) ยุทธศาสตร์ที่ 4 ปรับเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัล
- 5) ยุทธศาสตร์ที่ 5 พัฒนากำลังคนให้พร้อมเข้าสู่ยุคเศรษฐกิจและสังคมดิจิทัล
- 6) ยุทธศาสตร์ที่ 6 สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล

ซึ่งในยุทธศาสตร์ที่ 1–5 เป็นยุทธศาสตร์ที่เน้นการพัฒนาเทคโนโลยี ระบบการบริการและการเตรียมความพร้อมของประชาชน แต่หากไม่มีกฎหมายหรือระเบียบเพื่อสร้างความมั่นใจให้กับประชาชนและส่วนภาคธุรกิจก็จะทำให้ประเทศไทยไม่สามารถปรับเปลี่ยนประเทศให้เป็นตามเป้าหมายของแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมได้ ดังนั้นในยุทธศาสตร์ที่ 6 จึงเป็นยุทธศาสตร์ที่สำคัญที่จะมีการปรับปรุงกฎหมายด้านดิจิทัลที่ประเทศไทยมีอยู่ให้มีความทันสมัยและสอดคล้องกับเทคโนโลยีด้านดิจิทัลและกิจกรรมด้านเศรษฐกิจในปัจจุบัน เช่น พระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และสร้างกฎหมายใหม่ที่ประเทศไทยไม่เคยมีอยู่เพื่อให้รองรับกับเทคโนโลยีดิจิทัลรูปแบบใหม่ที่กำลังจะเข้ามามีบทบาทในอนาคต เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพื่อสร้างความสะดวกและความเชื่อมั่นใน

การใช้เทคโนโลยีกับผู้ประกอบการธุรกิจ ผู้บริโภคและรวมถึงประชาชนทั่วไปที่ใช้งานเทคโนโลยีดิจิทัลในชีวิตประจำวัน

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์เป็นพระราชบัญญัติที่ตราขึ้นเนื่องจากการทำธุรกรรมในปัจจุบันมีการเพิ่มวิธีการติดต่อสื่อสารและการทำหลักฐานต่าง ๆ ผ่านเทคโนโลยีทางอิเล็กทรอนิกส์มากขึ้น เช่น คอมพิวเตอร์ สมาร์ทโฟน และแท็บเล็ต ทำให้มีประชาชนและองค์กรต่าง ๆ ได้รับความสะดวก รวดเร็วและมีประสิทธิภาพจากบริการด้านธุรกรรมมากขึ้น แต่กฎหมายที่มีก่อน ปี พ.ศ. 2544 นั้นยังไม่ครอบคลุมต่อลักษณะวิธีการทำธุรกรรมทางอิเล็กทรอนิกส์ เช่น การรับรองสถานะข้อมูลทางอิเล็กทรอนิกส์ให้มีผลทางกฎหมายนอกเหนือจากการทำเอกสารเป็นหนังสือ การรับรองวิธีการส่งและรับข้อมูลอิเล็กทรอนิกส์ การลงลายมือชื่อแบบอิเล็กทรอนิกส์แทนการลงลายมือชื่อในเอกสารหนังสือ ตัวอย่างเช่น การใช้บัตรเอทีเอ็มเบิกถอนเงินสดและรับใบสลิปจากตู้เอทีเอ็ม การส่งข้อความยืนยันเงินผ่าน Facebook เป็นต้น ประเทศไทยจึงได้มีการตรา “พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544” (The Electronic Transaction Act B.E. 2544 (2001), 2001) ขึ้นมาโดยมีผลบังคับใช้กับ “ธุรกรรมทางอิเล็กทรอนิกส์” ซึ่งหมายถึงธุรกรรมที่กระทำขึ้นโดยใช้วิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือบางส่วน โดยธุรกรรม หมายถึงกิจกรรมในทางแพ่งและพาณิชย์ และรวมถึงการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ (หมวดที่ 4 มาตรา 35) ภายในพระราชบัญญัติประกอบด้วยหมวดที่ 1 ธุรกรรมอิเล็กทรอนิกส์ มาตรา 7–25 ได้รับความผูกพันทางกฎหมายของเอกสารอิเล็กทรอนิกส์ ความรับรองเอกสารที่มีการลงลายมือชื่ออิเล็กทรอนิกส์ การเก็บข้อมูลการจราจรทางคอมพิวเตอร์ที่เกี่ยวข้องกับการรับและส่งเอกสารที่สามารถระบุผู้รับและผู้ส่งได้ การสรุปลักษณะและการมีผลทางกฎหมายของเอกสารเอกสารอิเล็กทรอนิกส์ในส่วนของผู้รับและผู้ส่ง หมวดที่ 2 ลายมือชื่ออิเล็กทรอนิกส์ มาตรา 26–31 เป็นการกำหนดลักษณะความน่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์ที่จะนำมาใช้ในเอกสารอิเล็กทรอนิกส์ หมวดที่ 3 ธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ มาตรา 32–34 กำหนดให้บุคคลที่จะประกอบธุรกิจที่มีบริการเกี่ยวกับ

ธุรกรรมทางอิเล็กทรอนิกส์ต้องแจ้งให้ทราบ ขอขึ้นทะเบียน หรือได้รับอนุญาตก่อนมิเช่นนั้นจะมีโทษ และการถูกเพิกถอน ใบอนุญาต หมวดที่ 4 ธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ มาตรา 35 กำหนดให้ คำขอ การอนุญาต การจดทะเบียน คำสั่งทางปกครอง การชำระเงิน การประกาศ หรือการ ดำเนินการใด ๆ ตามกฎหมายกับหน่วยงานของรัฐหรือโดย หน่วยงานของรัฐ ถ้าได้กระทำในรูปของข้อมูลอิเล็กทรอนิกส์ ตามหลักเกณฑ์และวิธีการที่กำหนดโดยพระราชกฤษฎีกา ก็ให้ถือว่ามีผลโดยชอบด้วยกฎหมายเช่นเดียวกับการดำเนิน การตามหลักเกณฑ์และวิธีการที่กฎหมายในเรื่องนั้นกำหนด ปัจจุบันภาครัฐได้ปรับปรุงพระราชบัญญัติว่าด้วยธุรกรรม ทางอิเล็กทรอนิกส์ เพิ่มเติมอีก 3 ฉบับ ดังนี้

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ฉบับที่ 2 (The Electronic Transaction Act (No. 2) B.E. 2551 (2008), 2008) ซึ่งได้เพิ่มเติมข้อกำหนด ให้ครอบคลุมกับธุรกรรมทางอิเล็กทรอนิกส์กำหนดให้ เอกสารอิเล็กทรอนิกส์ที่มีหลักฐานการชำระเงินให้ถือว่า เป็นเอกสารที่ต้องมีการปิดอากรแสตมป์และขีดฆ่าตาม กฎหมายแล้ว เพิ่มรายละเอียดความน่าเชื่อถือเกี่ยวกับลายมือ ชื่ออิเล็กทรอนิกส์ สิ่งพิมพ์ที่ออกมาจากข้อมูลอิเล็กทรอนิกส์ และมีข้อความถูกต้องครบถ้วนกับข้อมูลอิเล็กทรอนิกส์ สามารถนำมาใช้แทนต้นฉบับได้ เช่น หนังสือรับรองดอกเบี้ย กู้ยืมจากธนาคาร ในคดีแพ่ง คดีอาญาหรือคดีอื่นใด ข้อมูลอิเล็กทรอนิกส์สามารถนำมาใช้เป็นหลักฐานการ พิจารณาได้ และให้มาตราที่ 10 11 และ 12 มาบังคับ ใช้กับเอกสารที่ถูกนำมาจัดทำหรือแปลงให้อยู่ในรูปแบบ ข้อมูลอิเล็กทรอนิกส์

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ฉบับที่ 3 (The Electronic Transaction Act (No. 3) B.E. 2562 (2019), 2019) ได้เพิ่มบทนิยามคำว่า “ระบบ แลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์อัตโนมัติ” ให้ชัดเจน ยิ่งขึ้น และแก้ไขบทนิยามคำว่า “หน่วยงานของรัฐ” โดย ระบุลักษณะหน่วยงานที่เป็นหน่วยงานรัฐให้ชัดเจน ตัวอย่าง การแก้ไขเพิ่มเติม เช่น แก้ไขเพิ่มเติมวิธีการในการลงลายมือ ชื่ออิเล็กทรอนิกส์แม้กรณีไม่ได้ลงลายมือชื่อแต่ถ้าระบุตัว เจ้าของลายมือชื่อได้ให้ถือว่าเอกสารนั้นลงลายมือชื่อแล้ว เพื่อให้สอดคล้องมาตรฐานสากล เช่น การส่งอีเมล พิมพ์ ได้ตอบกันใน facebook หรือ line การลงลายมือชื่อ

หมายถึงการที่สามารถระบุได้ว่าใครเป็นผู้ส่งข้อความนั้น โดยมาตราที่ 13/1 จะกำหนดให้สัญญาที่ติดต่อผ่านการ สื่อสารทางอิเล็กทรอนิกส์จะมีผลเมื่อสัญญานั้นระบุได้โดย แจ้งชัดถึงเจตนาของบุคคลที่ทำการเสนอและจะมีผลเมื่อมี คนสนองรับต่อสัญญานั้น และมาตราที่ 13/2 จะการห้าม มิให้ปฏิเสธความสมบูรณ์หรือการบังคับใช้ของสัญญาที่ทำ ผ่านระบบแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์อัตโนมัติ โดย จะอ้างว่าระบบอิเล็กทรอนิกส์ของผู้ทำสัญญาเป็นผู้เสนอ ไม่ใช่บุคคลจริง ๆ ไม่ได้ โดยในมาตราที่ 17/1 เปิดโอกาส ให้ถอนการแสดงเจตนาในการลงข้อมูลผิดพลาดที่ส่งผ่าน ระบบแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์อัตโนมัติ หาก กรอกข้อมูลผิดพลาดแต่ต้องแจ้งโดยเร็วและบุคคลดังกล่าว ไม่ได้ประโยชน์จากสัญญาดังกล่าว

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ฉบับที่ 4 (The Electronic Transaction Act (No. 4) B.E. 2562 (2019), 2019) ได้มีการปรับปรุงที่สำคัญ เช่น แก้ไขรัฐมนตรีผู้รักษาการตามกฎหมายเป็น รัฐมนตรีว่าการ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมแทนนายกรัฐมนตรี และเนื่องจากการทำธุรกรรมผ่านระบบอิเล็กทรอนิกส์ จำเป็นต้องมีการพิสูจน์ตัวตนทั้งของผู้ให้บริการและผู้ใช้ บริการ เพื่อให้เกิดความชัดเจนเรื่องการพิสูจน์ตัวตน พระราชบัญญัติจึงเพิ่มบทนิยาม คำว่า “การพิสูจน์และ ยืนยันตัวตน” และ “ระบบการพิสูจน์และยืนยันตัวตนทาง ดิจิทัล” เข้ามา

คำว่า “การพิสูจน์และยืนยันตัวตน” หมายความว่า กระบวนการพิสูจน์และยืนยันความถูกต้องของตัวบุคคล

คำว่า “ระบบการพิสูจน์และยืนยันตัวตนทาง ดิจิทัล” หมายความว่า เครือข่ายทางอิเล็กทรอนิกส์ที่เชื่อมโยง ข้อมูลระหว่างบุคคลใด ๆ หรือหน่วยงานของรัฐเพื่อ ประโยชน์ในการพิสูจน์และยืนยันตัวตนและการทำธุรกรรม อื่น ๆ ที่เกี่ยวเนื่องกับการพิสูจน์และยืนยันตัวตน” และได้ เพิ่มมาตรา 34/3 การพิสูจน์และยืนยันตัวตนของบุคคลอาจ กระทำผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลได้ เพื่อรองรับการทำธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งในมาตรา ที่ 34/4 ได้กำหนดให้ต้องมีการตราพระราชกฤษฎีกากำหนด ให้ผู้ประกอบการที่ต้องการประกอบธุรกิจบริการเกี่ยวกับ ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล ต้องขออนุญาต ก่อน และให้มีการจัดตั้งคณะกรรมการขึ้นมาเพื่อประกาศ

กำหนดหลักเกณฑ์ความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนทางดิจิทัล และกำหนดหลักเกณฑ์ที่ผู้ประกอบการธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลจะต้องปฏิบัติ

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ถูกประกาศใช้ครั้งแรกเมื่อ พ.ศ. 2550 (The Computer Crimes Act B.E. 2550 (2007), 2007) เหตุผลในการประกาศใช้เนื่องจากในปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญของการประกอบกิจการ ธุรกิจและการดำรงชีวิตของประชาชนมากขึ้น โดยปรากฏว่ามีผู้ที่มีความรู้ อาศัยช่องทางต่าง ๆ ด้านคอมพิวเตอร์มากระทำความผิด เช่น การบุกรุกเข้ามายังระบบคอมพิวเตอร์ ขโมยข้อมูล การปล่อยซอฟต์แวร์ที่เป็นอันตรายต่อคอมพิวเตอร์ การส่งข้อมูลรบกวนหรือสแปม (Spam) การทำให้ระบบคอมพิวเตอร์ไม่สามารถทำงานได้ หรือให้ใช้เป็นช่องทางในการเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จและลามกทำให้เกิดความวุ่นวาย เป็นต้น แต่กฎหมายประเทศไทยมีอยู่ยังไม่ได้บัญญัติลักษณะของการกระทำความผิดดังกล่าวไว้ ทำให้ประเทศไทยจึงได้ตราพระราชบัญญัติขึ้นมาเพื่อป้องกันและปราบปรามไม่ให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ หากการกระทำความผิดด้านคอมพิวเตอร์ก่อให้เกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคง ในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชนก็จะต้องได้รับโทษที่สูงขึ้น แต่เนื่องจากการพัฒนาด้านคอมพิวเตอร์ที่มากขึ้นทำให้เกิดการกระทำความผิดในรูปแบบใหม่ ๆ หรือมีความรุนแรงขึ้น ทำให้ประเทศไทยได้มีการปรับปรุงให้กฎหมายมีความเหมาะสมทันต่อเทคโนโลยีและภัยคุกคามด้านคอมพิวเตอร์ที่มีการเปลี่ยนแปลง เป็นพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฉบับที่ 2 พ.ศ. 2560 (The Computer Crimes Act (No. 2) B.E. 2560 (2017), 2017) เช่น เพิ่มเติมความหมายของข้อมูลอิเล็กทรอนิกส์ที่ก่อให้เกิดความเดือดร้อนรำคาญ (Spam)

หากเป็นจดหมายอิเล็กทรอนิกส์ที่ไม่เปิดโอกาสให้ยกเลิกการรับข้อมูลให้ถือว่าจดหมายอิเล็กทรอนิกส์นั้นเป็น Spam ปรับปรุงการนำข้อมูลอันเป็นเท็จเข้าสู่ระบบคอมพิวเตอร์ โดยแยกการหมิ่นประมาทในระบบคอมพิวเตอร์ต้องอันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา และเพิ่มโทษของการกระทำความผิดต่อประเทศให้สูงขึ้น

โดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ทั้ง 2 ฉบับ นอกเหนือจากการระบุฐานความผิดแล้วยังได้กำหนดมาตรการของการใช้อำนาจของพนักงานเจ้าหน้าที่ในการบังคับใช้กฎหมายไว้เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีการกระทำความผิดโดยไม่ใช้อำนาจเกินขอบเขตที่กฎหมายระบุไว้

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ปัจจุบันประชาชนมีใช้เทคโนโลยีดิจิทัลมากขึ้น ทั้งใช้ผ่านเครื่องคอมพิวเตอร์และสมาร์ทโฟน กิจกรรมที่เข้าใช้งานอินเทอร์เน็ตของประชาชนมีทั้งการค้นหาข้อมูล ความบันเทิง การใช้งานเครือข่ายสังคมออนไลน์ เช่น Facebook Tiktok และ Twitter และการทำธุรกรรมออนไลน์ ประเทศไทยได้ออกกฎหมาย พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์มาเพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์บนเทคโนโลยีดิจิทัลมีผลตามกฎหมาย และออกกฎหมายพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์เพื่อดูแลและกำหนดบทลงโทษที่เกิดขึ้นจากการใช้งานเทคโนโลยีดิจิทัล

แต่อีกปัญหาที่ประชาชนพบในการใช้งานเทคโนโลยีดิจิทัลปัจจุบันคือผู้ประกอบการธุรกิจต่าง ๆ มีการละเมิดเอาข้อมูลส่วนตัวของผู้ใช้งานไปใช้โดยไม่ได้รับการยินยอมจากเจ้าของข้อมูลก่อน ซึ่งเป็นทั้งข้อมูลที่ใช้ทำงานรอกลงไปในระบบตอนสมัครเข้าใช้งานระบบของผู้ให้บริการ เช่น ข้อมูลชื่อผู้ใช้ อายุ ที่อยู่ ข้อมูลด้านการเงินและอีเมล เป็นต้น และข้อมูลที่ใช้ซึ่งกันไม่ได้เป็นผู้ให้โดยตรง เช่น ข้อมูลการจราจรทางคอมพิวเตอร์ (หมายเลขไอพีและวันเวลาที่ใช้งาน) ประวัติการค้นหาข้อมูลในเว็บไซต์ พฤติกรรมการใช้งานเว็บและประวัติการเข้าสู่โฆษณา เป็นต้น ข้อมูล

เหล่านี้ผู้ประกอบการภาคเอกชนจะนำข้อมูลของผู้ใช้งานไปทำการวิเคราะห์ วางแผนทางธุรกิจและการโฆษณา ซึ่งผลที่ได้จะมีความแม่นยำมากเนื่องจากมีข้อมูลและพฤติกรรมการใช้งานของผู้บริโภคเป็นจำนวนมาก และอีกปัญหา คือ การประมาทเลินเล่อของผู้ประกอบการที่ได้มีการเก็บข้อมูลของผู้ใช้งานไว้แต่ไม่ได้มีมาตรการในการดูแลรักษาความปลอดภัยของข้อมูลหรือนโยบายการดูแลข้อมูลที่ไม่รัดกุมเพียงพอทำให้ข้อมูลส่วนบุคคลของผู้ใช้งานรั่วไหลออกไปยังบุคคลภายนอก

ประเทศไทยจึงได้จัดทำ“พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562” (The Personal Data Protection Act B.E. 2562 (2019), 2019) ขึ้นมาเพื่อกำหนดให้หน่วยงานหรือผู้ประกอบการที่มีการจัดเก็บข้อมูลผู้ใช้งานจะต้องมีมาตรการในการรักษาความปลอดภัยและความเป็นส่วนตัวของข้อมูลผู้ใช้งานไว้โดยพระราชบัญญัตินี้ได้นำแนวทางการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปที่ชื่อว่า “GDPR” (EU General Data Protection Regulation–GDPR) (Bunaramrueang, Elamchamroonlarp, Oinpat & Thipsamritkul, 2018, pp. 14-15) มาใช้สำหรับร่างกฎหมายเนื่องจากจะต้องให้สอดคล้องกันเพื่อเป็นประโยชน์ต่อภาคเอกชนที่ต้องทำธุรกิจในกลุ่มประเทศที่อยู่ในสหภาพยุโรปด้วย ในมาตรา 5 ของพระราชบัญญัตินี้ให้ใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักรไม่ว่าการเก็บรวบรวม ใช้ หรือเปิดเผยนั้นได้กระทำในหรือนอกราชอาณาจักรก็ตาม โดยในหมวดที่ 2 การคุ้มครองข้อมูลส่วนบุคคล แบ่งออกเป็น 3 ส่วน คือ (Pokudom, 2020)

ส่วนที่ 1 บททั่วไป เป็นมาตรากล่าวถึงการจัดเก็บข้อมูลต้องได้รับความยินยอมจากเจ้าของข้อมูล และต้องแจ้งวัตถุประสงค์การจัดเก็บให้ทราบ

ส่วนที่ 2 การเก็บรวบรวมข้อมูลส่วนบุคคล เป็นมาตรากล่าวถึงการจัดเก็บข้อมูลเท่าที่จำเป็นตามกฎหมายกำหนด ต้องแจ้งให้เจ้าของข้อมูลทราบและได้รับความยินยอม ให้เก็บข้อมูลได้จากเจ้าของข้อมูลเท่านั้นมาเก็บจากแหล่งอื่น ห้ามเก็บข้อมูลอื่น ๆ ซึ่งส่งผลกระทบต่อเจ้าของข้อมูลหากไม่ได้รับความยินยอม

ส่วนที่ 3 การใช้หรือเปิดเผยข้อมูลส่วนบุคคล เป็นมาตราที่ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ

เจ้าของข้อมูลส่วนบุคคลมีสิทธิ ดังนี้

- 1) มีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล
- 2) มีสิทธิขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอม
- 3) มีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล
- 4) มีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้
- 5) มีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการใช้ข้อมูลส่วนบุคคลได้

พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

จากปัจจุบันภัยคุกคามทางไซเบอร์มีจำนวนที่เพิ่มสูงขึ้นและทวีความรุนแรงขึ้นตามลำดับ ซึ่งส่งผลกระทบและสร้างความเสียหายทั้งต่อระดับประชาชนและภาคธุรกิจเป็นอันมาก หากภัยดังกล่าวกระทบต่อโครงสร้างพื้นฐานของประเทศก็จะยิ่งทำให้เกิดผลกระทบที่เป็นวงกว้างและได้รับความเสียหายทั้งทางเศรษฐกิจและความสงบเรียบร้อยของประเทศชาติ ประเทศไทยได้ให้ความสำคัญในการดำเนินงานเพื่อรับมือกับปัญหาภัยคุกคามดังกล่าวจึงจำเป็นต้องกำหนดหลักเกณฑ์เพื่อกำหนดแนวทางและมาตรการต่าง ๆ ที่เกี่ยวข้องอย่างเป็นรูปธรรมเป็น “พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562” (The Cyber Security Act B.E. 2562 (2019), 2019) ซึ่งถูกตราขึ้นมาโดยมีวัตถุประสงค์เพื่อเป็นกลไกเฝ้าระวัง ป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทาง

ไซเบอร์ที่กระทบกับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้งที่เป็นหน่วยงานของรัฐหรือหน่วยงานเอกชนที่มีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ได้แก่ด้านความมั่นคง ด้านการเงิน ด้านการขนส่งและโลจิสติกส์ ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ด้านพลังงานและสาธารณูปโภค ด้านบริการภาครัฐที่สำคัญ ด้านสาธารณสุขและด้านอื่นตามที่คณะกรรมการประกาศกำหนดเพิ่มเติมในอนาคต คำนิยามที่สำคัญในพระราชบัญญัติฉบับนี้ มีดังนี้

“การรักษาความมั่นคงปลอดภัยไซเบอร์” หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อย ภายในประเทศ

“ภัยคุกคามทางไซเบอร์” หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมีขอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้าย ต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภัยอันตรายที่ใกล้จะถึง ที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

“ไซเบอร์” หมายความว่า รวมถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของ ดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

“หน่วยงานของรัฐ” หมายความว่า ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่นรัฐวิสาหกิจ องค์การฝ่ายนิติบัญญัติ องค์การฝ่ายตุลาการ องค์การอิสระ องค์การมหาชน และหน่วยงานอื่นของรัฐ

“ประมวลแนวทางปฏิบัติ” หมายความว่า ระเบียบหรือหลักเกณฑ์ที่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์กำหนด

“เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์” หมายความว่า เหตุการณ์ที่เกิดจากการกระทำ

หรือการดำเนินการใด ๆ ที่มีขอบซึ่งกระทำการผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

“มาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์” หมายความว่า การแก้ไข ปัญหาความมั่นคงปลอดภัยไซเบอร์โดยใช้บุคลากร กระบวนการ และเทคโนโลยี โดยผ่านคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ หรือบริการที่เกี่ยวกับคอมพิวเตอร์ใด ๆ เพื่อสร้างความมั่นใจ และเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

พระราชบัญญัติฉบับนี้กำหนดให้มีการแต่งตั้งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อรับผิดชอบงานด้านความมั่นคงและจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยในหมวดที่ 3 การรักษาความมั่นคงปลอดภัยไซเบอร์ มาตราที่ 41 ได้ระบุว่า การรักษาความมั่นคงต้องสอดคล้องกับนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมตามกฎหมายว่าด้วย การพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม และนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ

มาตราที่ 49 ได้ประกาศลักษณะของหน่วยงานที่มีภารกิจหรือให้บริการในด้านต่อไปนี้ เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ได้แก่ ด้านความมั่นคงของรัฐ ด้านบริการภาครัฐที่สำคัญ ด้านการเงินการธนาคาร ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ด้านการขนส่งและโลจิสติกส์ ด้านพลังงานและสาธารณูปโภค ด้านสาธารณสุข และด้านอื่นตามที่คณะกรรมการประกาศกำหนดเพิ่มเติม ต้องปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์

สำหรับการรับมือภัยคุกคามทางไซเบอร์ ในมาตราที่ 60 ได้แบ่งระดับของภัยคุกคามทางไซเบอร์ไว้ 3 ระดับ ดังนี้

1) ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง หมายถึง ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงอย่างมี

นัยสำคัญถึงระดับที่ทำให้ระบบคอมพิวเตอร์ของหน่วยงาน โครงสร้างพื้นฐานสำคัญของประเทศ หรือการให้บริการ ของรัฐด้วยประสิทธิภาพลง

2) ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หมายถึง ภัยคุกคามที่มีลักษณะการเพิ่มขึ้นอย่างมีนัยสำคัญของการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูล คอมพิวเตอร์ โดยมุ่งหมาย เพื่อโจมตีโครงสร้างพื้นฐาน สำคัญของประเทศและการโจมตีดังกล่าวมีผลทำให้ ระบบคอมพิวเตอร์หรือ โครงสร้างพื้นฐานทางสารสนเทศ ที่เกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐาน สำคัญของประเทศ ความมั่นคงของรัฐ ความสัมพันธ์ระหว่าง ประเทศ การป้องกันประเทศ เศรษฐกิจ การสาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของ ประชาชนเสียหาย จนไม่สามารถทำงานหรือ ให้บริการได้

3) ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ หมายถึง ภัยคุกคามทางไซเบอร์ในระดับวิกฤติที่มีลักษณะ ดังต่อไปนี้

(ก) เป็นภัยคุกคามทางไซเบอร์ที่เกิดจากการโจมตี ระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ในระดับ ที่สูงขึ้นกว่าภัยคุกคามทางไซเบอร์ในระดับร้ายแรง โดยส่ง ผลกระทบรุนแรงต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ของประเทศในลักษณะที่เป็นวงกว้าง จนทำให้การทำงานของ หน่วยงานรัฐหรือการให้บริการของโครงสร้างพื้นฐาน สำคัญของประเทศที่ให้กับประชาชนล้มเหลวทั้งระบบ จนรัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบ คอมพิวเตอร์ของรัฐได้ หรือการใช้มาตรการเยียวยาตาม ปกติในการแก้ไขปัญหาภัยคุกคามไม่สามารถแก้ไขปัญหา ได้และมีความเสี่ยงที่จะลุกลามไปยัง โครงสร้างพื้นฐาน สำคัญอื่น ๆ ของประเทศ ซึ่งอาจมีผลทำให้บุคคลจำนวนมาก เสียชีวิตหรือระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูล คอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับ ประเทศ

(ข) เป็นภัยคุกคามทางไซเบอร์อันกระทบหรืออาจ กระทบต่อความสงบเรียบร้อยของประชาชนหรือเป็นภัยต่อ ความมั่นคงของรัฐหรืออาจทำให้ประเทศหรือส่วนใดส่วน หนึ่งของประเทศตกอยู่ ในภาวะคับขันหรือมีการกระทำให้ ความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมาย อาญา การรบหรือ การสงคราม ซึ่งจำเป็นต้องมีมาตรการ

เร่งด่วนเพื่อรักษาไว้ซึ่งการปกครองระบอบประชาธิปไตย อันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญแห่ง ราชอาณาจักรไทย เอกราชและบูรณภาพแห่งอาณาเขต ผล ประโยชน์ของชาติ การปฏิบัติตามกฎหมาย ความปลอดภัย ของประชาชน การดำรงชีวิตโดยปกติสุข ของประชาชน การ คุ่มครองสิทธิเสรีภาพ ความสงบเรียบร้อยหรือประโยชน์ ส่วนรวม หรือการป้องกันหรือแก้ไขเยียวยาความเสียหาย จากภัยพิบัติสาธารณะอันมีมาอย่างฉุกเฉินและร้ายแรง

กรณีเมื่อเกิดหรือคาดว่าจะเกิดภัยคุกคามทาง ไซเบอร์ในระดับร้ายแรง มาตราที่ 61–69 ได้กำหนดแนวทาง การปฏิบัติเพื่อการรับมือกับภัยคุกคามทางไซเบอร์ไว้ เช่น การให้อำนาจแก่คณะกรรมการการรักษาความมั่นคง ปลอดภัยไซเบอร์แห่งชาติสามารถออกคำสั่งเพื่อจัดการ กับภัยคุกคามได้ เจ้าหน้าที่ที่สามารถทำหนังสือขอความ ร่วมมือจากบุคคลที่เกี่ยวข้องมาให้ข้อมูลเรื่องภัยคุกคาม ทางไซเบอร์ กรณีเกิดความเสี่ยงในระดับร้ายแรงสามารถ ทำหนังสือถึงหน่วยงานรัฐให้กระทำการหรือระงับการ ดำเนินการเพื่อรับมือได้และสามารถออกคำสั่งให้เจ้าของ เครื่องหรือระบบคอมพิวเตอร์เฝ้าระวัง ตรวจสอบ ดำเนิน การแก้ไขและเข้าถึงระบบคอมพิวเตอร์เพื่อแก้ไขปัญหาได้ สามารถให้เจ้าหน้าที่ปฏิบัติการเท่าที่จำเป็นเพื่อเข้าตรวจ สอบสถานที่ เข้าถึงข้อมูลคอมพิวเตอร์ ทดสอบระบบหรือ อายัดคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรืออุปกรณ์ใด ๆ ได้ หากเป็นการคุกคามไซเบอร์ในระดับวิกฤติให้เป็นหน้าที่ และอำนาจของสภาความมั่นคงแห่งชาติ

พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐ ผ่านระบบดิจิทัล พ.ศ. 2562

ในการขับเคลื่อนประเทศไทยให้เป็นไปตามแผน พัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. 2559 นั้นนอกเหนือการจากพัฒนาทางด้านเทคโนโลยี ทรัพยากรบุคคล และด้านกฎหมายแล้ว ส่วนของภาครัฐเองจึงจำเป็นต้องมี การพัฒนาและปรับการให้บริการให้ทันต่อสภาพเศรษฐกิจ และสังคมในยุคดิจิทัลด้วย รัฐบาลไทยจึงได้ตราพระราชบัญญัติ การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 (The Public Administration and Services with Digital Systems Act B.E. 2562 (2019), 2019)

ขึ้นมาโดยให้นิยามคำว่า “รัฐบาลดิจิทัล” หมายความว่า การนำเทคโนโลยีดิจิทัลมาใช้เป็นเครื่องมือในการบริหารงาน ภาครัฐและการบริการสาธารณะ โดยปรับปรุงการบริหารจัดการและบูรณาการข้อมูลภาครัฐและการทำงานให้มีความสอดคล้องและเชื่อมโยงเข้าด้วยกันอย่างมั่นคงปลอดภัยและมีธรรมาภิบาล เพื่อเพิ่มประสิทธิภาพและอำนวยความสะดวกในการให้บริการประชาชน ในการเปิดเผยข้อมูลภาครัฐต่อสาธารณชนและสร้างการมีส่วนร่วมของทุกภาคส่วน ซึ่งหน่วยงานของรัฐที่ต้องมีการปรับปรุงให้การบริการเป็นไปตามพระราชบัญญัติฉบับนี้ประกอบด้วย ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ องค์การมหาชน รัฐสภา ศาล องค์การอิสระตามรัฐธรรมนูญ องค์การอัยการ สถาบันอุดมศึกษาของรัฐ และหน่วยงานอิสระของรัฐ

ภายใต้พระราชบัญญัตินี้กำหนดกลไกที่เป็นส่วนของการขับเคลื่อนให้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 ให้สำเร็จโดยประกอบด้วย

1) หน่วยงานของรัฐต้องมีการปรับปรุงการบริหารงานภาครัฐให้มีประสิทธิภาพ โดยจะต้องนำระบบดิจิทัลที่เหมาะสมมาใช้ในการบริหารและการให้บริการของหน่วยงาน ปรับปรุงระบบดิจิทัลให้หน่วยงานของรัฐให้มีความสอดคล้อง เชื่อมโยงกันและสามารถแลกเปลี่ยนข้อมูลระหว่างกันได้โดยที่ระบบจะต้องมีความมั่นคงปลอดภัยและน่าเชื่อถือ เพื่อให้การให้บริการประชาชนที่มีประสิทธิภาพ

2) สร้างและพัฒนาระบบความมั่นคงปลอดภัยในการใช้ระบบดิจิทัลและมาตรการปกป้อง คัดกรองข้อมูลที่อาจกระทบถึงความมั่นคงหรือความเป็นส่วนตัวของประชาชนที่มีความพร้อมใช้และน่าเชื่อถือ ปัจจุบันได้มีการออกพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งพระราชบัญญัติทั้งสองนี้ได้กำหนดให้ผู้ให้บริการหรือผู้ประกอบการธุรกิจต่าง ๆ ต้องมีการจัดหาระบบที่ต้องมีความปลอดภัยและต้องมีมาตรการในการดูแลคุ้มครองข้อมูลส่วนบุคคลของประชาชน

3) เปิดเผยข้อมูลหรือข่าวสารสาธารณะที่หน่วยงานของรัฐจัดทำและครอบครองในรูปแบบและช่องทาง

ดิจิทัล เพื่อให้ประชาชนเข้าถึงได้โดยสะดวก มีส่วนร่วมและตรวจสอบการดำเนินงานของรัฐ เช่น การจัดทำเว็บไซต์ศูนย์กลางข้อมูลเปิดภาครัฐ (open government data) ชื่อ “data.go.th” ดำเนินการโดยสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ข้อมูลที่เปิดเผยสามารถนำไปพัฒนาบริการและนวัตกรรมที่จะเป็นประโยชน์ต่อประเทศไทยได้

4) จัดทำแผนพัฒนารัฐบาลดิจิทัลของประเทศไทย เพื่อกำหนดกรอบและทิศทางการบริหารงานภาครัฐ และการจัดทำบริการสาธารณะในรูปแบบของเทคโนโลยีดิจิทัล เพื่อการพัฒนาประเทศ มีการปฏิบัติงาน ที่สอดคล้องกันระหว่างหน่วยงานของรัฐ และมีกรอบการพัฒนาและแผนการดำเนินงานของประเทศ โดยสอดคล้องกับวัตถุประสงค์ตาม ยุทธศาสตร์ชาติและแผนระดับชาติที่เกี่ยวข้อง ซึ่งแผนระยะแรก คือ แผนพัฒนารัฐบาลดิจิทัลของประเทศไทย ระยะ 3 ปี (พ.ศ.2559-2561) และแผนระยะที่ 2 คือ แผนพัฒนารัฐบาลดิจิทัลของประเทศไทย พ.ศ. 2563-2565 ซึ่งอยู่ระหว่างการร่าง

5) กำหนดให้มีคณะกรรมการพัฒนารัฐบาลดิจิทัลทำหน้าที่รับผิดชอบให้แผนพัฒนารัฐบาลดิจิทัลของประเทศไทย สำเร็จ และโดยมีสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ทำหน้าที่อำนวยความสะดวกและสนับสนุนการปฏิบัติงานตามที่คณะกรรมการพัฒนารัฐบาลดิจิทัลมอบหมาย

สรุป

แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม ของประเทศไทยเป็นแผนที่มุ่งการพัฒนาไปสู่ความเจริญทั้งทางด้านเศรษฐกิจและสังคมโดยใช้ความก้าวหน้าทางเทคโนโลยีดิจิทัลมาเป็นส่วนสำคัญในการพัฒนา แต่หากประชาชนและภาคธุรกิจไม่มีความเชื่อมั่นในด้านความมั่นคง ความเป็นส่วนตัวและการได้รับความคุ้มครองตามกฎหมายในการใช้งานระบบต่าง ๆ ผ่านเทคโนโลยีดิจิทัล การพัฒนาประเทศจะเป็นอย่างล่าช้า ดังนั้นกฎหมายที่ตราออกมาเป็นพระราชบัญญัติต่าง ๆ จึงเป็นส่วนสำคัญให้ประชาชนและภาคธุรกิจมีความมั่นใจในการทำกิจกรรมและการใช้บริการที่เกี่ยวข้องกับเทคโนโลยีดิจิทัล หากมี

บริการด้านดิจิทัลใหม่ ๆ ที่ได้รับความสนใจและมีการใช้งาน
กันมากขึ้น หน่วยงานภาครัฐที่เกี่ยวข้องก็จะมีการกำหนด
มาตรการหรือกฎหมายใหม่ให้เหมาะสมเพื่อสร้างความมั่นใจ

และดูแลคุ้มครองประชาชนผู้ใช้งานอันจะเป็นประโยชน์ต่อ
การพัฒนาของประเทศ



References

- Bunaramrueang, P., Elamchamroonlarp, P., Oinpat, C., & Thipsamritkul, T. (2018). *Thailand data protection guidelines 1.0*. Bangkok: Chulalongkorn University. (in Thai)
- Ministry of Digital Economy and Society. (2016). *Thailand digital economy and society development plan*. Bangkok: Ministry of Digital Economy and Society. (in Thai)
- Pokudom, N. (2020). Data privacy in the digital age. *EAU Heritage Journal Science and Technology*, 14(2), 59-69. (in Thai)
- The Computer Crimes Act B. E. 2550 (2007). (2007, 10, June). *Royal Thai Government Gazette*. Volume 124, Part 27, pp. 4-13. (in Thai)
- The Computer Crimes Act (No. 2) B. E. 2560 (2017). (2017, 24, January). *Royal Thai Government Gazette*. Volume 134, Part 10, pp. 24-35. (in Thai)
- The Cyber Security Act B. E. 2562 (2019). (2019, 27, May). *Royal Thai Government Gazette*. Volume 136, Part 69, pp. 20-51. (in Thai)
- The Electronic Transaction Act B. E. 254 (2001). (2001, 4, December). *Royal Thai Government Gazette*. Volume 118, Part 112, pp. 81-97. (in Thai)
- The Electronic Transaction Act (No. 2) B. E. 2551 (2008). (2008, 13, February). *Royal Thai Government Gazette*. Volume 125, Part 33, pp. 81-86. (in Thai)
- The Electronic Transaction Act (No. 3) B.E. 2562 (2019). (2019, 14, April). *Royal Thai Government Gazette*. Volume. 136 Part 49, pp. 12-26. (in Thai)
- The Electronic Transaction Act (No. 4) B. E. 2562 (2019). (2019, 22, May). *Royal Thai Government Gazette*. Volume. 136 Part 67, pp. 203-207. (in Thai)
- The Personal Data Protection Act B. E. 2562(2019). (2019, 27, May). *Royal Thai Government Gazette*. Volume. 136 Part 69, pp. 52-95. (in Thai)
- The Public Administration and Services with Digital Systems Act B. E. 2562 (2019). (2019, 22, May). *Royal Thai Government Gazette*. Volume. 136 Part 67, pp. 57-66. (in Thai)

