

การวิเคราะห์ผลกระทบที่อาจเกิดขึ้นจาก ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.

การวิเคราะห์ผลกระทบที่อาจเกิดขึ้นจากร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ที่ได้จัดทำขึ้น เป็นการพิจารณาผลกระทบของบทบัญญัติตามร่างพระราชบัญญัตินี้ ที่อาจส่งผลทั้งในเชิงบวกและเชิงลบ โดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้รวบรวมประเด็นและนำผลสรุปการรับฟังความคิดเห็นและข้อเสนอแนะจากผู้ที่เกี่ยวข้องทั้งภาครัฐ ภาคเอกชน ตลอดจนประชาชนทั่วไป มาเป็นข้อมูลประกอบการพิจารณาวิเคราะห์ผลกระทบที่อาจเกิดขึ้น เพื่อใช้เป็นข้อมูลประกอบการพิจารณา ร่างพระราชบัญญัติต่อไป

๑. ผู้ซึ่งอาจได้รับผลกระทบจากการบังคับใช้กฎหมาย

จากผลการวิเคราะห์พบว่า ผู้ซึ่งได้รับผลกระทบจากการบังคับใช้กฎหมาย ดังนี้

๑.๑ หน่วยงานภาครัฐ

๑.๒ ภาคเอกชน

๑.๓ ประชาชนทั่วไป

โดยผู้ที่จะได้รับผลกระทบจากร่างกฎหมายโดยตรง ได้แก่ หน่วยงานของรัฐ และหน่วยงานที่ให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure) ทั้งที่เป็นหน่วยงานภาครัฐและภาคเอกชน ในการดำเนินมาตรการที่จำเป็นเพื่อประโยชน์ในการรักษาความมั่นคงปลอดภัยไซเบอร์

๒. ผลกระทบที่อาจได้รับจากร่างกฎหมาย

โดยการวิเคราะห์ผลกระทบแยกออกเป็น ๒ ส่วน คือ ผลกระทบเชิงบวกและผลกระทบเชิงลบ ดังนี้

ส่วนที่ ๑ ผลกระทบเชิงบวก

(๑) ผลกระทบด้านเศรษฐกิจและสังคม

(๑.๑) การยกระดับความสามารถในการแข่งขันของประเทศ

จากผลการสำรวจระดับความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์โดยสหภาพโทรคมนาคมระหว่างประเทศ (ITU) ที่สำรวจระดับความเอาใจจริงเอาใจ (Commitment) ด้านความมั่นคงปลอดภัยไซเบอร์ของแต่ละประเทศ โดยพิจารณาจากมาตรการ ๕ ด้าน ได้แก่ ด้านกฎหมาย (Legal) ด้านเทคนิค (Technical) ด้านหน่วยงาน/นโยบาย (Organizational) ด้านการพัฒนาศักยภาพ (Capacity building) และด้านความร่วมมือ (Cooperation) ในปี พ.ศ. ๒๕๖๐ พบว่า Global Cybersecurity Index (GCI) ของประเทศไทยอยู่ในอันดับที่ ๒๒ จาก ๑๙๔ ประเทศ นอกจากนี้ เมื่อเปรียบเทียบกับประเทศสมาชิกในกลุ่มอาเซียนแล้ว ประเทศไทยอยู่อันดับที่ ๓ รองจากสิงคโปร์และมาเลเซีย ซึ่งผลการสำรวจดังกล่าวเป็นส่วนหนึ่ง que แสดงให้เห็นถึงแนวโน้มความน่าเชื่อถือของประเทศในการประกอบธุรกิจ รวมถึงกลไกลดความเสี่ยงในการทำธุรกรรมทางอิเล็กทรอนิกส์ การยกอันดับ GCI ของประเทศจึงเป็นหนึ่งในนโยบายของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมที่ตั้งเป้าหมายในการยกอันดับของประเทศให้อยู่ใน ๒๐ อันดับแรก เพื่อเพิ่มระดับความน่าเชื่อถือของประเทศไทยอันจะส่งผลต่อการพิจารณาเรื่องการค้าการลงทุนด้วย ดังนี้

ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. จึงเป็นโครงสร้างพื้นฐานทางกฎหมายสำคัญฉบับหนึ่งที่มีส่วนช่วยในการยกระดับความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยตาม Global Cybersecurity Index (GCI) รวมทั้งมีส่วนช่วยในการยกระดับการดูแลความมั่นคงปลอดภัยไซเบอร์ของประเทศในทุกมิติ โดยเฉพาะบริการที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructures) ของประเทศให้สามารถให้บริการแก่ ประชาชน ผู้ประกอบธุรกิจ และหน่วยงานของรัฐได้อย่างต่อเนื่อง

นอกจากนี้ ร่างกฎหมายดังกล่าวยังเป็นการส่งเสริมกระบวนการบริหารจัดการความเสี่ยงและกำหนดแผนรองรับทั้งด้านความพร้อมใช้งาน การฟื้นตัว การกู้คืนระบบ และความต่อเนื่องในการให้บริการของกลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ซึ่งเป็นผลดีต่อการรักษาประสิทธิภาพและความสามารถในการให้บริการสำคัญเมื่อเกิดเหตุขัดข้องจากภัยคุกคามในระบบนิเวศทางดิจิทัล เพื่อให้มีสภาพพร้อมใช้งานที่สามารถดำเนินการได้อย่างต่อเนื่องแม้เมื่อเกิดสถานการณ์ด้านภัยคุกคามไซเบอร์ อันจะช่วยสร้างความเชื่อมั่นให้แก่นักลงทุนในการตัดสินใจเข้ามาประกอบธุรกิจในประเทศไทย ซึ่งส่งผลสำคัญต่อการส่งเสริมให้ขีดความสามารถด้านการแข่งขันของประเทศดีขึ้น

(๑.๒) การเสริมสร้างประสิทธิภาพหรือนวัตกรรมในการปฏิบัติราชการ

ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์จำเป็นต้องมีการสร้างกลไกสำหรับประสานความร่วมมือระหว่างภาครัฐและเอกชนที่สะท้อนการมีความรับผิดชอบต่อสังคมในการรักษาความมั่นคงปลอดภัยไซเบอร์ของทุกภาคส่วน โดยจำเป็นต้องอาศัยรูปแบบการมีส่วนร่วมในกระบวนการตัดสินใจ (Multi-stakeholders) การแลกเปลี่ยนข้อมูลภัยคุกคามไซเบอร์ การรับมือสถานการณ์ฉุกเฉินอย่างรอบด้าน ซึ่งการสร้างกลไกดังกล่าวจะส่งเสริมการทำงานและประสิทธิภาพของหน่วยงานของรัฐทำให้มีระบบการให้บริการแก่ประชาชนที่มีความมั่นคงปลอดภัย และสามารถช่วยลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่จะเกิดขึ้นกับหน่วยงานของรัฐ

นอกจากนี้ หน่วยงานของรัฐสามารถลดค่าใช้จ่ายที่เป็นต้นทุนในการดำเนินการเพื่อรับมือภัยคุกคามทางไซเบอร์ได้ เนื่องจากเป็นการวางโครงสร้างในภาพรวม ทำให้ไม่เกิดการลงทุนที่ซ้ำซ้อน การมีหน่วยงานกลางทำหน้าที่ประสานงานทำให้การดำเนินงานมีประสิทธิภาพมากยิ่งขึ้น

(๑.๓) การยกระดับคุณภาพชีวิตของประชาชน

การพัฒนาให้เกิดกลไกในการประสานความร่วมมือและหน้าที่ที่จำเป็นสำหรับหน่วยงานของรัฐและโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่พร้อมปกป้อง รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ อันจะทำให้สามารถให้บริการได้อย่างต่อเนื่องและมีประสิทธิภาพ รวมทั้งมีหน่วยงานและกลไกในการให้ความช่วยเหลือ สนับสนุน ในการจัดการกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น ส่งผลให้ประเทศไทยมีระบบนิเวศ หรือ Ecosystem ที่ช่วยสร้างความเชื่อมั่นในดำเนินกิจกรรมต่างๆ ผ่านช่องทางออนไลน์ เนื่องจากมีกลไกสำหรับการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์อย่างเอาใจจริงเอาใจใส่ กลไกดังกล่าวจึงทำให้ประชาชนได้รับบริการจากระบบที่เป็นบริการอันเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure) อย่างต่อเนื่อง นำไปสู่การยกระดับคุณภาพชีวิตของประชาชนที่สามารถได้รับบริการที่ดี มีคุณภาพ มีคุณภาพชีวิตที่ดีขึ้นจากระบบบริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ดี

นอกจากนี้ การกำหนดมาตรการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นการสร้างความเข้มแข็งทั้งระบบ และยกระดับการดูแลความมั่นคงปลอดภัยไซเบอร์ในทุกมิติ เนื่องจากการดำเนินกิจกรรมต่าง ๆ อาศัยเทคโนโลยีเป็นเครื่องมือในการพัฒนาบริการและเพิ่มมูลค่าทางเศรษฐกิจ การให้บริการอันเป็นโครงสร้างพื้นฐานทางสารสนเทศที่สำคัญซึ่งต้องให้บริการได้อย่างต่อเนื่อง จึงก่อให้เกิดประโยชน์แก่ภาคเอกชนที่สามารถประกอบกิจกรรมหรือดำเนินธุรกิจได้อย่างสะดวกและราบรื่น ซึ่งหากไม่มีมาตรการดูแลที่ดีเพียงพอ อาจกลายเป็นข้อจำกัดและอุปสรรคในการดำเนินธุรกิจของภาคเอกชน เนื่องจากขาดความน่าเชื่อถือ และภาคเอกชนอาจเสียโอกาสในการประกอบธุรกิจ ทั้งยังกระทบต่อระบบเศรษฐกิจในภาพรวมได้

อีกทั้งเมื่อประเทศไทยมีกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ จะทำให้หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure) มีมาตรการในการดูแลความมั่นคงปลอดภัยไซเบอร์ของทรัพย์สินสารสนเทศของตนตามมาตรฐานขั้นต่ำที่กฎหมายกำหนด ซึ่งจะมีส่วนช่วยให้การให้บริการของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งเมื่อเกิดเหตุภัยคุกคามทางไซเบอร์ขึ้น หน่วยงานต่างๆ จะมีแนวปฏิบัติในการทำงานร่วมกัน ซึ่งจะทำให้การจัดการ เยียวยา แก้ปัญหา กู้คืน และฟื้นฟู สามารถดำเนินการได้อย่างทันท่วงที

(๒) ผลกระทบต่อประเทศในระยะยาว

การที่ร่างพระราชบัญญัติดังกล่าวกำหนดโครงสร้างการทำงานเพื่อการบูรณาการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ซึ่งครอบคลุมการทำงานทั้งภาครัฐและภาคเอกชนนั้น ส่งผลให้ประเทศไทยมีความพร้อม สามารถปกป้อง ป้องกัน และรับมือกับสถานการณ์ด้านภัยคุกคามไซเบอร์ทั้งในสถานการณ์ปกติ สถานการณ์อันเป็นภัยต่อความมั่นคง และสถานการณ์อันเป็นภัยต่อความมั่นคงอย่างร้ายแรง ทั้งนี้ การบูรณาการการจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศ (Cybersecurity Governance) การเตรียมแผนปฏิบัติการและมาตรการตอบสนองด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เป็นกลไกควบคุมการใช้ อำนาจเป็นการเฉพาะตามระดับความรุนแรงของสถานการณ์ รวมทั้งมีการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง ยังก่อให้เกิดประโยชน์ในการสร้างศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์ (Emergency Readiness) เพื่อรับมือและป้องกันภัยคุกคามไซเบอร์ได้อย่างทันท่วงที ถือเป็นกลไกสำคัญที่ทำให้สามารถแก้ไขสถานการณ์ที่เกิดขึ้นได้อย่างมีประสิทธิภาพและเป็นเอกภาพ สร้างความเชื่อมั่นในการดำเนินกิจกรรมต่างๆ ภายใต้สถานการณ์ภัยคุกคามไซเบอร์ และบริหารจัดการความเสี่ยงของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ อันส่งผลต่อการดำเนินชีวิตประจำวันของประชาชน เสถียรภาพทางเศรษฐกิจ และความมั่นคงของชาติ

การขับเคลื่อนเรื่องความมั่นคงปลอดภัยไซเบอร์ยังจำเป็นต้องอาศัยการศึกษา วิจัยและพัฒนาอย่างต่อเนื่อง เนื่องจากการวิจัยและพัฒนาเทคโนโลยีและองค์ความรู้ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นเป้าหมายสำคัญของนโยบายและแผนการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่ต้องกำหนดให้มีขึ้นเพื่อหาแนวโน้มความเสี่ยงของภัยคุกคามไซเบอร์ และพัฒนาต่อยอดเทคโนโลยีในการป้องกัน รับมือ และตอบโต้ภัยคุกคาม จะส่งผลให้ประเทศสามารถพึ่งพาตัวเองทางเทคโนโลยีได้อย่างยั่งยืน ไม่ยึดติดกับเทคโนโลยีต่างประเทศซึ่งอาจมีช่องโหว่ด้านความมั่นคงปลอดภัยทั้งแบบที่ตั้งใจและไม่ตั้งใจ

นอกจากนี้ การดำเนินงานตามร่างพระราชบัญญัตินี้จะช่วยลดงบประมาณแผ่นดินในระยะยาว และทำให้เกิดความคุ้มค่า เนื่องจากการดำเนินการแบบองค์รวมในการเสริมสร้างความเข้มแข็งในการดูแลความมั่นคงปลอดภัยไซเบอร์ของประเทศอย่างเป็นระบบ ทั้งมาตรการเชิงรุกที่ต้องมีการสร้างความแข็งแกร่งทั้งด้านนโยบาย องค์กร คน และองค์ความรู้ และมาตรการเชิงรับที่ต้องรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันทั่วทั้ง ซึ่งการดำเนินการดังกล่าวยังช่วยสร้างความเชื่อมั่นด้านการค้าและการลงทุนอันส่งผลดีต่อระบบเศรษฐกิจโดยรวม ส่วนการจำกัดสิทธิเสรีภาพของประชาชนนั้น ร่างพระราชบัญญัติฉบับนี้จำกัดเฉพาะการดำเนินการเพื่อปกป้อง และรับมือภัยคุกคามทางไซเบอร์ในระดับร้ายแรง เพื่อประโยชน์ในการรวบรวมข้อมูลและวิเคราะห์เพื่อหาแนวทางการรับมือได้อย่างมีประสิทธิภาพ

ส่วนที่ ๒ ผลกระทบเชิงลบ

- ไม่มี -

๓. ประโยชน์ที่ประชาชนและสังคมจะได้รับ

ประชาชนจะได้รับบริการจากระบบที่เป็นบริการอันเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure) ได้อย่างต่อเนื่อง มีความมั่นคงปลอดภัย รวมทั้งมีหน่วยงานและกลไกในการให้ความช่วยเหลือ สนับสนุน ในการจัดการกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น โดยการตราพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. มีเจตนารมณ์เพื่อเป็นการป้องกัน รับมือ และลดความเสี่ยงภัยจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ รวมทั้งเป็นการสร้างความเข้มแข็งให้ระบบการให้บริการผ่านออนไลน์ของหน่วยงานรัฐ และเอกชน ให้ดียิ่งขึ้น โดยมีหน่วยงานรับผิดชอบในการดำเนินการประสานการปฏิบัติงานร่วมกันทั้งภาครัฐ และเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์อันเป็นภัยต่อความมั่นคงอย่างร้ายแรง ตลอดจนกำหนดให้มีแผนปฏิบัติการและมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อการให้บริการเป็นไปอย่างมีประสิทธิภาพและต่อเนื่อง
