แนวทางการส่งเสริมจริยธรรมภาครัฐ ในยุคการพัฒนาเทคโนโลยีสารสนเทศเพื่อรองรับสถานการณ์ Disruption

เสนอที่ประชุม อ.ก.พ. วิสามัญเกี่ยวกับการส่งเสริมจริยธรรมเพื่อราชการใสสะอาด
ครั้งที่ ๑/๒๕๖๓ เมื่อวันที่ ๒๑ มกราคม ๒๕๖๓
และ ครั้งที่ ๔/๒๕๖๓ วันที่ ๒๖ พฤษภาคม ๒๕๖๓

โดย ศูนย์ส่งเสริมจริยธรรม
สำนักงาน ก.พ.

แนวทางการส่งเสริมจริยธรรมภาครัฐในยุคการพัฒนาเทคโนโลยีสารสนเทศ เพื่อรองรับสถานการณ์ Disruption

.....

๑. ที่มา

ตามที่ ก.พ. ในการประชุมครั้งที่ ๑๐/ ๒๕๖๒ เมื่อวันที่ ๙ ธันวาคม ๒๕๖๒ ได้พิจารณาวาระหารือ เรื่อง ระบบบุคลากรภาครัฐรูปแบบใหม่ และให้ฝ่ายเลขานุการนำเสนอประเด็นหารือที่เกี่ยวกับการเตรียมวางแผนบริหารกำลังคนภาครัฐในยุคการพัฒนาเทคโนโลยีเพื่อรองรับสถานการณ์ Disruption ในการประชุมครั้งต่อไป

ศูนย์ส่งเสริมจริยธรรม สำนักงาน ก.พ. ได้รับฟังความเห็นจาก อ.ก.พ. วิสามัญเกี่ยวกับการส่งเสริมจริยธรรมเพื่อราชการใสสะอาด ในประเด็นหารือที่เกี่ยวกับการเตรียมวางแผนบริหารกำลังคนภาครัฐในยุคการพัฒนาเทคโนโลยีเพื่อรองรับสถานการณ์ Disruption ในการประชุมครั้งที่ ๑๒/๒๕๖๒ เมื่อวันที่ ๒๔ ธันวาคม ๒๕๖๒ และ อ.ก.พ.ฯ ให้ความคิดเห็นว่า สถานการณ์ Disruption เป็นโอกาสดีในการเปลี่ยนแปลงระบบราชการให้มีความโปร่งใส ราชการจึงควรเตรียมความพร้อมเพื่อรองรับการเปลี่ยนแปลงในบริบทต่าง ๆ ที่มีภารกิจหลากหลายตามลักษณะงาน ตลอดจนกำหนดคุณลักษณะของข้าราชการและเจ้าหน้าที่ของรัฐ เพื่อส่งเสริมจริยธรรมการใช้เทคโนโลยีสารสนเทศในยุคดิจิทัลด้วย

นอกจากนั้น เพื่อเป็นการเตรียมพร้อมการรองรับความก้าวหน้าของเทคโนโลยีสารสนเทศและการปรับเปลี่ยนภาครัฐสู่รัฐบาลอิเล็กทรอนิกส์ e-Goverment คณะรัฐมนตรีได้มีมติเมื่อวันที่ ๒๖ กันยายน ๒๕๖๐ กำหนดแนวทางการพัฒนาทักษะด้านดิจิทัลของข้าราชการและบุคลากรภาครัฐ ประกอบด้วย ๗ กลุ่มทักษะ คือ

(๑) ความสามารถด้านความเข้าใจ (Digital Literacy)

(๒) ความสามารถด้านการควบคุมกำกับและปฏิบัติตามกฎหมาย นโยบาย และมาตรการจัดการด้านดิจิทัล (Digital Governance, Standard, and Compliance)

(๓) ความสามารถด้านเทคโนโลยีดิจิทัลเพื่อยกระดับศักยภาพองค์กร (Digital Technology)

(๔) ความสามารถด้านการออกแบบกระบวนการและการให้บริการด้วยระบบดิจิทัล (Digital Process and Service Design)

(๕) ความสามารถด้านการบริหารกลยุทธ์และการจัดการโครงการ (Strategic and Project management)

(๖) ความสามารถด้านผู้นำดิจิทัล (Digital Leadership) และ

(๗) ความสามารถด้านการขับเคลื่อนการเปลี่ยนแปลงด้านดิจิทัล (Digital Transformation)

สำนักงาน ก.พ. จึงได้ศึกษาข้อมูลที่เกี่ยวข้อง และเสนอแนวทางการส่งเสริมจริยธรรมในภาครัฐในยุคการพัฒนาเทคโนโลยีสารสนเทศ เพื่อรองรับสถานการณ์ Disruption ต่อที่ประชุม อ.ก.พ. วิสามัญเกี่ยวกับการส่งเสริมจริยธรรมเพื่อราชการใสสะอาด ครั้งที่ ๑/๒๕๖๓ เมื่อวันที่ ๒๑ มกราคม ๒๕๖๓ และครั้งที่ ๔/๒๕๖๓ วันที่ ๒๖ พฤษภาคม ๒๕๖๓ โดยมีรายละเอียดดังนี้

๒. สถานการณ์ปัจจุบัน

๒.๑ สภาวการณ์การเปลี่ยนแปลงของโลกปัจจุบันที่เรียกว่า Disruption อันเป็นผลมาจากความก้าวหน้าทางเทคโนโลยีดิจิทัล ส่งผลให้บริบทในการปฏิสัมพันธ์หรือเชื่อมต่อระหว่างกันแตกต่างจากในอดีตอย่างสิ้นเชิง อาทิ Artificial Intelligence (AI), Internet of Things (IOTs) ทำให้อุปกรณ์/ระบบคอมพิวเตอร์ทำงานแทนคนได้อย่างมีประสิทธิภาพ/ ประสิทธิผลสูงกว่าอย่างก้าวกระโดด FinTech ทำให้ระบบการเงินโลกเปลี่ยนไปอยู่บนมือถือ เทคโนโลยี Blockchain จะทำให้การบริการต่าง ๆ รวมถึงระบบการตรวจสอบทุกอย่างเป็นไปได้ง่าย ความก้าวหน้าทางเทคโนโลยีทำให้การรับข่าวสารข้อมูลเกิดขึ้นอย่างรวดเร็ว ระบบการบริหารจัดการของหน่วยงานต่าง ๆ ก็จะสามารถตอบสนองความต้องการของลูกค้าได้เร็วขึ้น แม่นยำขึ้น มีคุณภาพมากขึ้น ส่งผลให้เกิดความคาดหวังจากประชาชน/ภาคเอกชนต่อการบริหารจัดการและการบริการที่ได้รับจากหน่วยงานภาครัฐมากขึ้น และภาคราชการมีความจำเป็นต้องเร่งปรับตัวให้สอดคล้องกับความก้าวหน้าทางเทคโนโลยี/การเปลี่ยนแปลงดังกล่าว ซึ่งการเปลี่ยนแปลงแบบ Disruption ได้ส่งผลกระทบต่อการบริหารจัดการภาครัฐ

๒.๒ รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช ๒๕๖๐ มาตรา ๒๕๘ ข. บัญญัติให้ดำเนินการปฏิรูปประเทศด้านการบริหารราชการแผ่นดินให้เกิดผล ดังนี้

๒.๒.๑ การนำเทคโนโลยีที่เหมาะสมมาประยุกต์ใช้ในการบริหารราชการแผ่นดินและการจัดทำบริการสาธารณะ เพื่อประโยชน์ในการบริหารราชการแผ่นดิน และเพื่ออำนวยความสะดวกให้แก่ประชาชน

๒.๒.๒ บูรณาการฐานข้อมูลของหน่วยงานของรัฐทุกหน่วยงานเข้าด้วยกัน เพื่อให้เป็นระบบข้อมูลเพื่อการบริหารราชการแผ่นดินและการบริการประชาชน

๒.๒.๓ การปรับปรุงและพัฒนาโครงสร้างและระบบการบริหารงานของรัฐและแผนกำลังคนภาครัฐให้ทันต่อการเปลี่ยนแปลงและความท้าทายใหม่ ๆ โดยต้องดำเนินการให้เหมาะสมกับภารกิจของหน่วยงานของรัฐแต่ละหน่วยงานที่แตกต่างกัน

๒.๒.๔ การปรับปรุงและพัฒนาการบริหารงานบุคคลภาครัฐเพื่อจูงใจให้ผู้มีความรู้ความสามารถอย่างแท้จริงเข้ามาทำงานในหน่วยงานของรัฐ และสามารถเจริญก้าวหน้าได้ตามความสามารถและผลสัมฤทธิ์ของงานของแต่ละบุคคล มีความซื่อสัตย์สุจริต กล้าตัดสินใจและกระทำในสิ่งที่ถูกต้องโดยคิดถึงประโยชน์ส่วนรวมมากกว่าประโยชน์ส่วนตัว มีความคิดสร้างสรรค์ และคิดค้นนวัตกรรมใหม่ เพื่อให้การปฏิบัติราชการและการบริหารราชการแผ่นดินเป็นไปอย่างมีประสิทธิภาพ และมีมาตรการคุ้มครองป้องกันบุคลากรภาครัฐจากการใช้อำนาจโดยไม่เป็นธรรมของผู้บังคับบัญชา

๒.๒.๕ การปรับปรุงระบบการจัดซื้อจัดจ้างภาครัฐให้มีความคล่องตัว เปิดเผยตรวจสอบได้ และมีกลไกในการป้องกันการทุจริตทุกขั้นตอน

ภายใต้บริบทการเปลี่ยนแปลงดังกล่าว การแข่งขันในโลกยุคใหม่จะมุ่งเน้นการสร้างนวัตกรรมหรือ Value เพื่อตอบสนองต่อความต้องการของลูกค้าหรือประชาชนอย่าง รวดเร็ว โดยการสร้างนวัตกรรมหรือคุณค่าดังกล่าวอาจนำเทคโนโลยีมาใช้หรืออาจสร้างโดยไม่ใช้ นวัตกรรมก็ได้ ประเด็นสำคัญ คือ การปรับเปลี่ยนกรอบความคิด (Mindset) และวัฒนธรรมทำให้ข้าราชการต้องมุ่งเรียนรู้และพัฒนาสมรรถนะของตนให้ทันกับการเปลี่ยนแปลง มีความมุ่งมั่นที่จะเรียนรู้ มีความคิดสร้างสรรค์ และนำความรู้มาปรับใช้ให้เกิดประโยชน์ต่อประชาชน สามารถปรับใช้

เทคโนโลยีในงานเพื่อการบริการประชาชนที่รวดเร็ว ตอบสนองความต้องการและแก้ไขปัญหาความเดือดร้อนของประชาชนได้อย่างทันท่วงที มีการวิเคราะห์ข้อมูล/การเชื่อมโยงข้อมูลให้กลายเป็น Big Data เพื่อให้การบริหารจัดการภาครัฐเกิดการบูรณาการข้อมูลเพื่อประสิทธิภาพและประสิทธิผลสูงสุด รวมถึงมีการกำหนดประเด็นหรือแก้ไขข้อกฎหมายที่เกี่ยวข้องเพื่อให้บริบทการทำงานของภาครัฐสามารถตอบสนองต่อความต้องการของประชาชนในโลกยุคดิจิทัลได้ อาทิ การบริการขนส่งสาธารณะ เช่น Grab, Uber เป็นต้น

๒.๓ ปัจจัยที่ส่งผลกระทบต่อการทบทวนแนวทางการขับเคลื่อนภารกิจด้านการส่งเสริมคุณธรรม จริยธรรมในภาครัฐ

๒.๓.๑ สถานการณ์ที่มาจากแนวโน้มสำคัญในอนาคต (Mega Trends) อาทิ การเปลี่ยนแปลงโครงสร้างประชากร (Demographic Shifts) การเปลี่ยนขั้วอำนาจเศรษฐกิจโลก (Shift in Global Economic Power) การเติบโตของสังคมเมือง (Accelerating Urbanisation) การลดลงของทรัพยากรและการเปลี่ยนแปลงสภาวะอากาศ (Resource Scarcity and Climate Change) ความก้าวหน้าในการพัฒนาเทคโนโลยี (Technological Breakthroughs)

๒.๓.๒ การรวมกลุ่มทางเศรษฐกิจในภูมิภาคต่าง ๆ ของโลกจะมีมากขึ้น ศูนย์กลางอำนาจทางเศรษฐกิจจะย้ายมาอยู่ที่เอเชีย และการเป็นประชาคมอาเซียนในปี ๒๕๕๘ ได้ส่งผลกระทบต่อการพัฒนาเศรษฐกิจ สังคม และสิ่งแวดล้อมของไทย ซึ่งต้องมีการเตรียมความพร้อมในหลายด้าน โดยเฉพาะการพัฒนาทรัพยากรมนุษย์และการพัฒนากลไกต่าง ๆ

๒.๓.๓ ความต้องการของสังคมในเรื่องธรรมาภิบาลของระบบราชการที่มีการเรียกร้องอย่างต่อเนื่องทั้งจากธุรกิจ ภาคเอกชน และภาคประชาชน เกี่ยวกับการมีส่วนร่วมในกระบวนการตรวจสอบการทำงานของภาครัฐ และความต้องการของสังคมที่ต้องการเข้ามามีบทบาทและส่วนร่วมในการพัฒนาประเทศมากยิ่งขึ้น รวมถึงการเรียกร้องให้รัฐบาลเร่งแก้ไขปัญหาในด้านต่าง ๆ ทั้งทางด้านเศรษฐกิจ การเมืองและสังคม โดยเฉพาะประเด็นที่ต่างประเทศให้ความสำคัญและมีผลกระทบต่อความน่าเชื่อถือของประเทศ อาทิ ปัญหาด้านการคอร์รัปชันในภาคราชการ ปัญหาเกี่ยวกับมาตรฐาน คุณภาพของสินค้าและบริการ รวมถึงการบริหารงานภาครัฐที่ต้องเปิดกว้างและโปร่งใส มีระบบดิจิทัลสมัยใหม่เพื่อให้บริการสาธารณะตามความต้องการ

ของประชาชนผ่านช่องทางต่าง ๆ ได้ตลอดเวลา ซึ่งเป็นปัญหาที่ภาครัฐต้องเร่งปรับปรุงหรือพัฒนาให้เป็นไปตามข้อบังคับตามมาตรฐานสากล

นอกจากนี้ ยังมีประเด็นเกี่ยวกับความต้องการให้ระบบราชการดำรงอยู่อย่างมีเกียรติภูมิ และศักดิ์ศรี ปราศจากการแทรกแซงทางการเมืองอย่างไม่ชอบธรรม โดยเฉพาะอย่างยิ่งการแทรกแซงในกระบวนการแต่งตั้งโยกย้ายข้าราชการระดับสูง โดยมองว่าการกระทำดังกล่าวขัดต่อหลักคุณธรรม ส่งผลเสียแก่ประเทศชาติ อีกทั้งเป็นการทำลายขวัญ กำลังใจและศักดิ์ศรีของข้าราชการ

๒.๔ แผนการปฏิรูปประเทศ ฉบับปี พ.ศ. ๒๕๖๑ – ๒๕๖๕ เน้นการขับเคลื่อนด้วยเทคโนโลยีและระบบดิจิทัล เพื่อให้ภาครัฐเปิดกว้างและเชื่อมโยงกัน มีประเด็นสำคัญที่ส่งผลต่อการส่งเสริมจริยธรรมภาครัฐ ดังนี้

๒.๔.๑ แผนการปฏิรูปประเทศด้านการบริหารราชการแผ่นดิน

เรื่องและประเด็นปฏิรูปที่ ๔ : กำลังคนภาครัฐมีขนาดที่เหมาะสมและมีสมรรถนะสูงพร้อมขับเคลื่อนยุทธศาสตร์ชาติ กลยุทธ์ที่ ๓ : พัฒนาทักษะและสมรรถนะใหม่เพื่อสร้างความพร้อมเชิงกลยุทธ์ให้กับกำลังคนภาครัฐ (New Mindsets and Skillsets) แผนงานที่ ๔ สร้างวัฒนธรรม ค่านิยม และอุดมการณ์สำหรับการเป็นเจ้าหน้าที่ภาครัฐยุคใหม่อย่างต่อเนื่อง โดยให้ข้าราชการและเจ้าหน้าที่ของรัฐมีค่านิยมและอุดมการณ์ที่กล้ายืนหยัดในสิ่งที่ถูกต้อง แยกผลประโยชน์ส่วนตนออกจากประโยชน์สาธารณะ ดำรงตนตามปรัชญาของเศรษฐกิจพอเพียง เจ้าหน้าที่ของรัฐมีกระบวนทัศน์ใหม่ (New Paradigm) มีกลไกและมาตรการคุ้มครองเจ้าหน้าที่จากการใช้อำนาจที่ไม่เป็นธรรมโดยผู้บังคับบัญชา

เรื่องและประเด็นปฏิรูปที่ ๕ : ระบบบริหารงานบุคคลที่สามารถดึงดูด สร้างและรักษาคนดีคนเก่งไว้ในภาครัฐ กลยุทธ์ที่ ๕ : ส่งเสริมคุณธรรมและจริยธรรมในการบริหารทรัพยากรบุคคล แผนงานที่ ๒ ให้ทุกองค์กรกลางบริหารงานบุคคลหรือหน่วยงานของรัฐนำประมวลจริยธรรมสำหรับเจ้าหน้าที่ของรัฐไปใช้ในการบริหารงานบุคคล และแผนงานที่ ๓ ส่งเสริมการใช้พฤติกรรมคุณธรรม และจริยธรรมเป็นองค์ประกอบสำคัญในการบริหารงานบุคคล โดยให้องค์กรกลางบริหารงานบุคคลกำหนดหลักเกณฑ์การใช้พฤติกรรมคุณธรรมและจริยธรรม

ในการเลื่อนตำแหน่ง การลดตำแหน่ง การย้ายตำแหน่ง เป็นต้น โดยกำหนดตัวชี้วัด เป็นร้อยละของส่วนราชการ/หน่วยงานของรัฐมีแผนการขับเคลื่อนงานด้านจริยธรรมและนำไปบังคับใช้ในการบริหารบุคคลอย่างเป็นรูปธรรม

๒.๔.๒ แผนการปฏิรูปประเทศด้านการป้องกันและปราบปรามการทุจริตและประพฤติมิชอบ ประเด็นการปฏิรูปที่ ๒ ด้านการป้องปราม

กลยุทธ์ที่ ๑ ให้ส่วนราชการมีการบริหารงานบุคคลที่เป็นไปตามระบบคุณธรรม (Merit System) ได้เจ้าหน้าที่ของรัฐ ที่เป็น “คนดี คนเก่ง คนกล้า ยืนหยัดในสิ่งที่ถูกต้อง” และให้จัดทำตัวชี้วัดและวิธีการประเมิน “สัตบุรุษ” เพื่อใช้เป็นส่วนหนึ่งในการประเมินสมรรถนะของข้าราชการ โดยเฉพาะบุคคลที่เข้าสู่ตำแหน่งผู้บริหาร และให้มีระบบเพื่อใช้ในการสรรหาและคัดเลือกบุคคลเข้าดำรงตำแหน่ง รวมถึงกำหนดเส้นทางการรับราชการ (Career Path) การสืบทอดงาน (Succession Planning) ในการเข้าสู่ตำแหน่งผู้บริหารระดับสูงที่ชัดเจน เปิดเผยและตรวจสอบได้จากประชาชน

กลยุทธ์ที่ ๒ ให้หัวหน้าส่วนราชการ หัวหน้าหน่วยงานของรัฐ หรือผู้บังคับบัญชา มีมาตรการเสริมสร้างวัฒนธรรมองค์กรในการป้องกันและปราบปราม การทุจริตและประพฤติมิชอบและเป็นตัวอย่างในการบริหารงานด้วยความซื่อตรงและรับผิดชอบ กรณีปล่อยปละละเลยไม่ดำเนินการให้ถือเป็นความผิดวินัยหรือความผิดทางอาญา โดยให้มีระบบการปลุกจิตสำนึกให้เจ้าหน้าที่ของรัฐมีคุณธรรมความซื่อตรง (Integrity) โดยเน้นความซื่อตรงต่อหน้าที่ (ซื่อสัตย์สุจริต วิริยะอุตสาหะ ทำงานให้สำเร็จตามเป้าหมายอย่างดีที่สุด) และซื่อตรงต่อประชาชน

กลยุทธ์ที่ ๕ ให้เจ้าพนักงานของรัฐบริการประชาชนตามหน้าที่ที่ได้รับโดยไม่คำนึงถึงอามิสสินจ้าง โดยให้หน่วยงานของรัฐทุกหน่วยต้องปลูกจิตสำนึกจิตบริการให้กับเจ้าพนักงานของรัฐ

กลยุทธ์ที่ ๖ ให้มีการแสดงฐานะทางการเงินของเจ้าพนักงานของรัฐที่เปิดเผย ตรวจสอบได้

ประเด็นการปฏิรูปที่ ๒ ด้านการปราบปราม กลยุทธ์ที่ ๑ ออกแบบกระบวนการบริหารคดีใหม่ ให้มีขั้นตอนเท่าที่จำเป็นเพื่อให้เกิดความรวดเร็ว และจัดให้มีประมวลความประพฤติ (Code of conducts) ของเจ้าหน้าที่ของรัฐประเภทต่าง ๆ ที่กำหนดการกระทำผิดที่เชื่อมโยงระหว่างความผิดทางจริยธรรม ความผิดวินัย และความผิดกฎหมายอย่างชัดเจน ในรูปแบบของให้กระทำและไม่ให้กระทำ ซึ่งสะท้อนพฤติกรรมที่ดี ถูกต้อง และเป็นธรรมตามความร้ายแรงแห่งการกระทำ

๒.๕ ความก้าวหน้าของเทคโนโลยีสารสนเทศ ทำให้เรื่องจริยธรรมและความเป็นส่วนตัวบนโลกดิจิทัล หรือ Digital Ethics and Privacy เป็นประเด็นที่ทั่วโลกกล่าวถึงและได้รับความสนใจมากขึ้นเรื่อย ๆ โดยภาครัฐและภาคเอกชนในหลายประเทศได้ยกระดับจริยธรรมและความเป็นส่วนตัวของการใช้เทคโนโลยีและปัญญาประดิษฐ์ และมีการกำหนดนโยบายหรือมาตรการเพื่อกระตุ้นให้คนในสังคมสนใจและให้ความสำคัญกับการที่ภาคเอกชนและภาครัฐได้นำข้อมูลของตนไปใช้ รวมถึงการดำเนินนโยบายเพื่อป้องกันปัญหาจากการใช้เทคโนโลยีสารสนเทศที่อาจเกิดขึ้น ไม่ใช่รอให้เกิดปัญหาแล้วจึงแก้ไขในภายหลัง

๒.๖ Digital Ethics หรือจริยธรรมบนโลกดิจิทัล เป็นกฎเกณฑ์หรือข้อตกลงที่ประชาชนหรือผู้ใช้งานคอมพิวเตอร์และเทคโนโลยีนำมาใช้เพื่อเป็นแนวทางในการปฏิบัติร่วมกัน หรืออาจกล่าวได้ว่า เป็นมาตรการในการป้องกันไม่ให้มีการทำผิดจริยธรรม เช่น การใช้เทคโนโลยีสื่อสารเพื่อทำร้ายคนอื่นให้เกิดความเสียหาย หรือก่อความวุ่นวายให้เกิดขึ้นในสังคม หรือการขโมยและเข้าถึงข้อมูลของบุคคลอื่นโดยไม่ได้รับอนุญาต รวมถึงการละเมิดลิขสิทธิ์ทรัพย์สินทางปัญญา เป็นต้น และเมื่อพิจารณาถึงจริยธรรมเกี่ยวกับการใช้เทคโนโลยีคอมพิวเตอร์และสารสนเทศจะกล่าวถึงใน ๔ ประเด็น หรือที่เรียกโดยย่อว่า PAPA ประกอบด้วย

๒.๖.๑ ความเป็นส่วนตัว หรือ Information Privacy (P) เป็นสิทธิของเจ้าของข้อมูลที่มีอยู่ เพื่อใช้ในการควบคุมข้อมูลของตนเองในการเปิดเผยข้อมูลให้ผู้อื่นได้เห็นหรือเข้าถึงได้ หรือไม่ให้เห็นหรือเข้าถึงไม่ได้ สิทธิที่ว่านี้ครอบคลุมทั้งข้อมูลส่วนบุคคล กลุ่มบุคคล และองค์กร

๒.๖.๒ ความถูกต้อง หรือ Information Accuracy (A) แสดงถึงความรับผิดชอบของเจ้าของข้อมูลหรือผู้ทำการจัดเก็บข้อมูล เพื่อรับรองว่าข้อมูลที่จัดเก็บมีความน่าเชื่อถือ ทั้งนี้ขึ้นอยู่กับความถูกต้องของข้อมูลและการบันทึกข้อมูลนั้นด้วย

๒.๖.๓ สิทธิความเป็นเจ้าของ หรือ Intellectual Property (P) เป็นสิทธิหรือการเป็นเจ้าของในสิ่งที่เป็นผลผลิตทรัพย์สินทางปัญญา ซึ่งกฎหมายรับรองว่ามีอยู่เหนือสิ่งที่เกิดจากความคิดสร้างสรรค์ทางปัญญา แบ่งออกเป็น ๒ ประเภท คือ ประเภทแรก ทรัพย์สินทางอุตสาหกรรม ได้แก่ สิทธิบัตร เครื่องหมายการค้า การออกแบบอุตสาหกรรม ความลับทางการค้า และสิ่งบ่งชี้ทางภูมิศาสตร์ และประเภทที่สอง คือ ลิขสิทธิ์ หมายถึง งานหรือความคิดสร้างสรรค์ในสาขาวรรณกรรม ศิลปกรรม ดนตรี งานภาพยนตร์ งานด้านอื่นในทางวิทยาศาสตร์ รวมถึงโปรแกรมคอมพิวเตอร์และฐานข้อมูล

๒.๖.๔ การเข้าถึงข้อมูล หรือ Data Accessibility (A) เป็นการกำหนดสิทธิและความรับผิดชอบในการเข้าใช้งานข้อมูล เพื่อป้องกันการเข้าไปดำเนินการต่าง ๆ กับข้อมูลของผู้ที่ไม่มีส่วนเกี่ยวข้องหรือไม่ได้รับอนุญาตจากเจ้าของข้อมูล และเป็นการรักษาความลับของข้อมูลไม่ให้รั่วไหล และโดยที่ปัจจุบันการใช้งานคอมพิวเตอร์และเทคโนโลยีสื่อสารมีความซับซ้อนมากขึ้น ส่งผลให้กรอบจริยธรรมที่เป็นข้อตกลงร่วมของสังคมอาจไม่เพียงพอหรือไม่อาจบังคับใช้ได้อย่างทั่วถึง ดังนั้น จึงเป็นประเด็นที่ภาครัฐต้องให้ความสำคัญและตระหนักถึงผลกระทบจากกลไกการพัฒนาทางเทคโนโลยีที่มีทิศทางจะละเมิดกรอบจริยธรรมมากขึ้น โดยถือเป็นความจำเป็นเร่งด่วนของสังคมในยุคดิจิทัลอย่างหลีกเลี่ยงไม่ได้

๒.๗ การเปลี่ยนแปลงอย่างฉับพลัน (Disruption) ในโลกยุคปัจจุบัน

สถานการณ์การเปลี่ยนแปลงอย่างฉับพลันในครั้งนี้ แบ่งออกได้เป็น ๒ สถานการณ์ คือ การเปลี่ยนแปลงที่เกิดจากเทคโนโลยีดิจิทัล (Digital Disruption) และการเปลี่ยนแปลงที่เกิดจากปัญหาโรคระบาด (Pandemic Disruption) ดังนี้

๒.๗.๑ สถานการณ์ของเทคโนโลยีดิจิทัล (Digital Disruption) McKinsey Global Institute ได้ประมวลเทคโนโลยีใหม่ ๆ ที่ก่อให้เกิดการเปลี่ยนแปลงอย่างก้าวกระโดดไว้ เช่น Mobile Internet ที่เชื่อมโยงทั่วโลก ใช้ประโยชน์ทั้งการเรียนการสอน

การตรวจโรคระยะไกล การทำธุรกรรมทางการเงิน หรือเทคโนโลยี Automatic of Knowledge Work ที่สามารถวินิจฉัยข้อมูล อาการ ร่างคำฟ้อง และแนะนำเรื่องกฎหมาย และเทคโนโลยี Internet of Thing (IoT) ที่พัฒนาโดยฝัง Sensor ในตัวสินค้าหรือเม็ดยาเพื่อการสั่งการระยะไกล และการตรวจวัด เป็นต้น

อย่างไรก็ดี disruptive.asia[๑] ซึ่งเป็นสื่อชื่อดังของฮ่องกงได้วิเคราะห์ว่า ความเจริญเติบโตทางเทคโนโลยีดิจิทัลอย่างรวดเร็วได้ส่งผลกระทบอย่างทั่วถึงไปทุกภาคส่วน โดยเฉพาะทำให้องค์กรต้องพัฒนาเครื่องมือที่มีประสิทธิภาพในการทำงานรูปแบบใหม่ ๆ ต้องคำนึงถึงจริยธรรมทางธุรกิจเพิ่มขึ้น ทั้งด้านการรักษาความเป็นส่วนตัวและความปลอดภัยในการสื่อสาร รวมถึงผู้นำขององค์กรที่ต้องมีบทบาทสำคัญในการสื่อสารข้อมูลที่เกี่ยวกับจริยธรรมให้แก่บุคลากรในองค์กร ลงมือทำให้เห็นเป็นตัวอย่าง และติดตามประเมินผลอย่างสม่ำเสมอ

สำหรับประเด็นหรือกลยุทธ์เพื่อนำไปสู่องค์กรที่มีมาตรฐานของพฤติกรรมทางจริยธรรมในยุคดิจิทัล ต้องคำนึงถึง

(๑) ประเด็นจริยธรรมที่มาจากการเปลี่ยนแปลงของเทคโนโลยีที่มีศักยภาพสูงไม่ว่าจะเป็น AI, cloud storage, big data, IoT, wearable devices, blockchain ตัวอย่างผลกระทบทางจริยธรรม เช่น การใช้เทคโนโลยีดิจิทัล ติดตามพฤติกรรมของบุคคลในเรื่องหนึ่งแต่กลับเป็นการรุกล้ำสิทธิเสรีภาพ หรือส่งผลกระทบต่อความรู้สึกของบุคคล เป็นต้น

(๒) ประเด็นจริยธรรมที่สะท้อนจากสังคมดิจิทัล เช่น สังคมต้องการความยุติธรรมในการนำเสนอข้อมูลใน social media ซึ่งหมายถึงต้องมีการพูดความจริงเพิ่มมากขึ้น ข้อสังเกตเกี่ยวกับการจ้างงาน AI แทนการจ้างคน การติดตามพฤติกรรมของบุคคลที่อาจเป็นการรุกล้ำสิทธิเสรีภาพ ความต้องการข้อมูลทางเลือกที่ชัดเจนในการตัดสินใจ เป็นต้น ซึ่งองค์กรต้องให้ความสำคัญกับประเด็นทางสังคมเหล่านี้ เพื่อนำมาประกอบการดำเนินการ

---

[๑] Rohit Talwar, “Businesses must adopt a code of ethics for disruptive echnologies”, เผยแพร่เมื่อ ๒ สิงหาคม๒๕๖๐, สืบค้นจาก https://disruptive.asia/code-ethics-disruptive-technologies/

(๓) การลงมือปฏิบัติและความสม่ำเสมอ องค์กรต้องมีนโยบายที่ชัดเจนเกี่ยวกับการตระหนักถึงแนวคิดทางจริยธรรม เพราะจะนำมาใช้เป็นหลักสำคัญของนโยบายเชิงกลยุทธ์ต่อไป และต้องนำมาใช้ปฏิบัติจริงอย่างสม่ำเสมอ โดยผู้นำองค์กรต้องสื่อสารผ่านการดำเนินชีวิตประจำวัน ด้วยช่องทางต่าง ๆ โดยยกตัวอย่างของทางเลือกที่ควรทำและไม่ควรทำ พร้อมกับอธิบายและหาวิธีแก้ไขปัญหาด้วยแนวคิดจริยธรรม

นอกจากนั้น ในสังคมแห่งโลกดิจิทัล มีความจำเป็นที่จะต้องส่งเสริมการเป็นพลเมืองดิจิทัล (Digital Citizenship)[๒] ให้เกิดผลตามเป้าหมาย ๓ ประการ คือ (๑) การเป็นผู้นำและช่วยเหลือผู้อื่นในการสร้างประสบการณ์ดิจิทัลในเชิงบวก (To lead and assist others inbuilding positive digital experiences) (๒) การตระหนักว่าการกระทำของเราอาจจะส่งผลกระทบต่อบุคคลอื่น (To recognize that our actions have consequences to others) (๓) การมีส่วนร่วมเพื่อประโยชน์ร่วมกัน (To participate in a manner for the common good)

๒.๑.๒ สถานการณ์การระบาดของโรคติดเชื้อไวรัสโคโรนา (COVID-19)

(๑) สถานการณ์การแพร่ระบาดของโรคติดเชื้อไวรัสโคโรนา (COVID-19)

ไปทั่วโลก ส่งผลกระทบต่อรูปแบบการทำงานที่ต้องปรับเปลี่ยนให้สอดคล้องกับนโยบายและแนวทางของสาธารณสุขเพื่อช่วยลดความเสี่ยงของการแพร่กระจายของโรคติดต่อให้มีอัตราที่น้อยลงให้ได้มากที่สุด ซึ่งองค์การอนามัยโลก (World Health Organization: WHO)[๓] มีแนวทางให้สถานที่ทำงานสร้างความพร้อมในสถานการณ์โรคติดเชื้อไวรัสโคโรนา (COVID-19) ๔ แนวทาง ประกอบด้วย (๑) การป้องกันการแพร่กระจายโรคติดเชื้อไวรัสโคโรนา (COVID-19) (๒) การลดความเสี่ยงของการแพร่ระบาด (๓) สิ่งที่ต้องตระหนักเมื่อต้องมีการเดินทาง (๔) การเตรียมความพร้อมเมื่อมีสถานการณ์โรคติดเชื้อดังกล่าวเกิดขึ้นในสถานที่ทำงาน ซึ่งส่งผลให้

๒ Digital citizenship.net/nine-elements.html๓ ประเทศต่าง ๆ ที่ได้รับผลกระทบต่างกำหนดมาตรการควบคุมเพื่อระงับการแพร่กระจายของเชื้อโรคดังกล่าวการเปลี่ยนแปลงวิถีชีวิตและรูปแบบการทำงานอันเนื่องมาจากสถานการณ์โรคติดเชื้อไวรัสโคโรนา (COVID-19)

[๒] Digital citizenship.net/nine-elements.html

[๓] World Health Organization, “Getting your Workplace ready for COVID-19”, เผยแพร่เมื่อวันที่ ๓ มีนาคม ๒๕๖๓, สืบค้นจาก http://www.who.int

เป็นปรากฏการณ์ที่เกิดขึ้นอย่างรวดเร็ว และส่งผลกระทบอย่างรุนแรงต่อทรัพยากรมนุษย์ทั่วทั้งโลกซึ่งต้องรับมือและร่วมมือกันในการแก้ไขวิกฤตการณ์ดังกล่าวให้เข้าสู่ภาวะปกติอย่างเร่งด่วนที่สุด ผู้เชี่ยวชาญด้านสุขภาพโลก (Alunna Shaikh) [๔] กล่าวไว้บนเวที Ted Talk (Technology Entertainment and Design) ที่ TEDxSMU เมื่อวันที่ ๑๑ มีนาคม ๒๕๖๓ ว่าการระบาดใหญ่ครั้งนี้ไม่ใช่ครั้งสุดท้ายที่เผชิญ จากนี้ไปจะมีโรคระบาดเกิดมากขึ้นเรื่อยๆ และจะมีการแพร่กระจายอีกมาก และจะเกิดขึ้นอย่างแน่นอนจากวิธีการที่มนุษย์มีปฏิสัมพันธ์กับโลก

(๒) ผลกระทบจากวิกฤตเชื้อไวรัสโคโรนา (COVID-19) ต่อสังคมไทย

(๒.๑) เมื่อพบว่าการติดต่อกันทางกายภาพกลายเป็นสาเหตุหลักของการแพร่กระจายของเชื้อโรค ดังนั้น การเดินทางติดต่อกันข้ามจังหวัด ข้ามประเทศ การประชุมสัมมนา การชุมนุม การเลี้ยงสังสรรค์ รูปแบบการใช้ชีวิตนอกบ้าน การรับประทานอาหาร การจับจ่ายซื้อของ รวมถึงประเพณีต่าง ๆ ที่ต้องมีการรวมกลุ่มกัน ฯลฯ อาจจำเป็นต้องมีมาตรการที่บ่งบอกได้ถึงความปลอดภัยของสุขอนามัย หรืออาจมีการเปลี่ยนแปลงกิจกรรมบางประเภทไปอย่างสิ้นเชิงโดยมีการนำเทคโนโลยีมาแทนที่

(๒.๒) มีการนำเทคโนโลยีดิจิทัลและนวัตกรรมใหม่ ๆ เพื่อสนับสนุนกิจกรรมต่าง ๆ ในสังคมและองค์กรมากขึ้น เช่น การซื้อขาย Online การทำงานที่บ้าน (WFH) การใช้เทคโนโลยีสมัยใหม่ เช่น Zoom , Google Meets , Microsoft Team เพื่อลดความเสี่ยงในการประชุมร่วมกัน การพัฒนาการเรียนและฝึกอบรมผ่าน E-Learning ให้เกิดผลอย่างมีคุณภาพ การพัฒนา AI เพื่อให้บริการแทนการใช้คน การวินิจฉัยและรักษาโรคผ่าน Video Conference การพัฒนาเทคโนโลยีหรือนวัตกรรมเพื่อทดแทนการนำเข้าจากต่างประเทศ เช่น ชุดตรวจโควิด เป็นต้น ทำให้โลกกลายเป็นสังคมแห่ง Digitalization & Innovation ดังนั้น องค์กรที่ปรับตัวไม่ทันกับยุค Digital Transfomation ก็อาจล่มสลายไปได้ในที่สุด

(๒.๓) จากสถานการณ์วิกฤตทำให้บางคนเกิดความตระหนก หวาดระแวง มีความต้องการเอาตัวรอด เกิดความโลภ ความเห็นแก่ตัว หรือสร้างกระแสสังคมเชิงลบ เช่น

---

[๔] “Design & Creativity COVID-19 พลิกมุมคิด....วิกฤตหรือโอกาส ” เผยแพร่เมื่อวันที่ ๑๔ เมษายน ๒๕๖๓ สืบค้นจาก https://web.tcdc.or.th/th/Articles/Detail/Covid-19-cover-story

การรังเกียจบุคคลที่เป็นกลุ่มเสี่ยงหรือผู้ป่วยด้วยโรคนี้ การรุมประณามบุคคลที่ไม่ปฏิบัติตามข้อตกลงทางสังคม การคิดหวังผลประโยชน์จากสถานการณ์ด้วยการกักตุนสินค้า การปิดบังความจริงจากการไปสัมผัสเชื้อ การสร้างข่าวลวง หรือบางประเทศถึงขั้นการออกกฎหมายห้ามส่งออกอุปกรณ์ทางการแพทย์ที่จำเป็นเพื่อเก็บไว้ใช้เฉพาะประเทศของตน

(๒.๔) เกิดสังคมเชิงสร้างสรรค์ในการสร้างความตระหนักรู้ การช่วยเหลือเอื้ออาทรซึ่งกันและกัน เช่น การแชร์แก้ข่าวปลอมและให้ความรู้แก่ประชาชน การกำหนดสโลแกน “อยู่บ้าน หยุดเชื้อ เพื่อชาติ” การให้กำลังใจเจ้าหน้าที่ทางการแพทย์ผ่านสื่อออนไลน์ การเสียสละช่วยกันทำหน้ากากอนามัย การบริจาคสนับสนุนเครื่องมือทางการแพทย์ การเสนอให้ประกันชีวิตแก่เจ้าหน้าที่ทางการแพทย์ การพร้อมใจร่วมมือกับรัฐบาลในการอยู่บ้าน เป็นต้น

(๒.๕) สื่อโซเชียลเป็นสิ่งสำคัญที่ใช้เป็นช่องทางการแสดงความคิดเห็นของบุคคลสู่สาธารณะ ซึ่งพบการถกเถียงกันทั้งในกลุ่มที่เห็นด้วย และไม่เห็นด้วยต่อเหตุการณ์ต่าง ๆ โดยไม่ได้คำนึงถึงข้อเท็จจริง หรือจิตสำนึกเพื่อประโยชน์ต่อส่วนรวม หลายครั้งที่มีการใช้ถ้อยคำเชิงเสียดสี เย้ยหยัน หรือการแสดงออกทางอารมณ์ที่เป็นตัวอย่างที่ไม่เหมาะสม

(๒.๖) การปรับเปลี่ยนรูปแบบการทำงานและวิถีชีวิตของคนในสังคมจะส่งผลต่อการรักษาสิ่งแวดล้อมได้ระยะยาว เช่น การประหยัดพลังงาน การรักษาสมดุลทางธรรมชาติ การลดปัญหาฝุ่นควัน เป็นต้น

(๒.๗) การทำให้สังคมเกิดตระหนักถึงความไม่แน่นอน ความไม่ประมาท การคำนึงถึงการป้องกันความเสี่ยง การดำรงชีวิตด้วยหลักประหยัดและอดออม รวมถึงการพึ่งพาตนเองเพื่อนำไปสู่ความพอดีตามหลักปรัชญาของเศรษฐกิจพอเพียง ดังนั้นเมื่อทุกอย่างเข้าสู่ภาวะปกติแล้วก็จะเป็นความท้าทาย ที่ยิ่งใหญ่ของทุกประเทศที่ภาครัฐ ภาคเอกชน และภาคประชาชนจะต้องร่วมกันวางแผนเพื่อบริหารจัดการทรัพยากรต่าง ๆ ให้เกิดประโยชน์กับประชาชนอย่างมีประสิทธิภาพ พร้อมกับเตรียมการณ์รองรับต่อสถานการณ์การเปลี่ยนแปลงด้านอื่น ๆ ที่อาจเกิดขึ้นต่อไปในอนาคต

จากสถานการณ์ Disruption ปัจจุบัน หน่วยงานและองค์กรทั้งภาครัฐและภาคเอกชนทั่วโลก ให้ความสนใจและมีการปรับตัว เพื่อสร้างแนวทางการรับมือกับภัยคุกคาม

ทางเทคโนโลยีที่อาจจะเกิดขึ้น ทั้งแนวทางการปราบปรามโดยใช้กฎหมายบังคับ และแนวทางการป้องกัน โดยให้ความสำคัญกับการปลูกฝัง “จริยธรรม” หน้าที่พลเมือง โดยมีข้อมูลความเคลื่อนไหว/การปรับตัวของหน่วยงานและประเทศต่าง ๆ รายละเอียดดังนี้

๓. ข้อมูลความเคลื่อนไหว/การปรับตัวของหน่วยงานและประเทศต่าง ๆ

จากการศึกษาข้อมูลความเคลื่อนไหว/การปรับตัวของหน่วยงานและประเทศต่าง ๆ พบว่า มีนโยบายเพื่อความปลอดภัยทางไซเบอร์ เพื่อรับมือกับสถานการณ์ Digital Disruption ดังนี้

๑. นโยบายความร่วมมือระหว่างประเทศ ได้แก่

๑.๑ กรอบความร่วมมือระหว่างประเทศ Global Cybersecurity Agenda (GCA)[๕] ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) กำหนดกรอบความร่วมมือระหว่างประเทศเพื่อความปลอดภัยของผู้ใช้งาน เช่น เด็กและเยาวชนทั่วโลก (Child Online Protection) โดยกำหนดกฎหมายเพื่อการใช้งานออนไลน์อย่างปลอดภัยในเด็กและเยาวชน ซึ่งอาจจะเกิดเหตุการณ์หรือกิจกรรมที่มีความรุนแรง การกลั่นแกล้ง การล่วงละเมิดทางร่างกายและจิตใจ (Bully and Harrassment) หรือการใช้งานออนไลน์อย่างปลอดภัยและให้คำแนะนำแก่เด็กและเยาวชน ของพ่อแม่และครูผู้ให้การศึกษา คำแนะนำการใช้งานออนไลน์สำหรับภาคอุตสาหกรรม และหน่วยงานผู้กำหนดนโยบายควรเน้นการป้องกันภัยคุกคาม และการเข้าถึงแหล่งข้อมูลที่ปลอดภัยให้เด็กและเยาวชน เป็นต้น

๑.๒ ข้อเสนอแนะด้านความมั่นคงปลอดภัยทางดิจิทัล (OECD Recommendation on Digital Security of Critial Activities)[๖] ขององค์กรเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD)

[๕] https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

[๖] OECD. **Recommendation on Digital Security of Critical Activities.** www.oecd.org/going-digital/topics/digital-security-and-privacy/recommendation-on-digital-security-of-critical-activities.htm

๑.๓ กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปหรือ General Data Protection Regulation (GDPR)[๗]

๑.๔ เครือข่ายการรักษาความปลอดภัยไซเบอร์ในภูมิภาคเอเชียแปซิฟิก โดยมีญี่ปุ่นเป็นแกนนำและพี่เลี้ยงให้ความช่วยเหลือในการตั้งกลุ่ม CSIRT/CERT

๒. นโยบายหรือแผนป้องกันในระดับประเทศ เช่น แผนคุ้มครองโครงสร้างพื้นฐานแห่งชาติ (National Protection Infrastructure Plan) ของสหรัฐอเมริกา โครงการ Great Firewall Project (GFP) และโครงการ Golden Shield Project: GSP ของสาธารณรัฐประชาชนจีน[๘] เพื่อควบคุมการเข้าถึงบริการต่าง ๆ บนโลกออนไลน์ ศูนย์ปฏิบัติการด้านการรักษาความปลอดภัยข้อมูลคอมพิวเตอร์แห่งชาติของเกาหลีใต้ (KoreaInformation Security Agency: KISA) ในภูมิภาคเอเชียแปซิฟิกมีการจัดตั้ง APCERT (Asia Pacific Computer Emergency Response Team) โดย JPCERT/CC ของญี่ปุ่นเป็นแกนนำเพื่อสร้างเครือข่ายการรักษาความปลอดภัยไซเบอร์ในภูมิภาค ประเทศสิงคโปร์มีศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งสิงคโปร์ (SingCERT) เป็นผู้เฝ้าระวังและดูแลความปลอดภัยไซเบอร์ และสหพันธรัฐมาเลเซียได้จัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งมาเลเซีย (Malaysia Computer Emergency Response Team: MyCERT) เป็นต้น

---

[๗] อ่านกฎหมายฉบับเต็มที่ https://gdpr-info.eu/ และอ่านข้อมูลเพิ่มเติมได้ที่ **กฎหมาย GDPR ฉบับรวบรัด.** https://www.etda.or.th/content/gdpr-in-a-nutshell และสำนักเจรจาการค้าบริการและการลงทุน กรมเจรจาการค้าระหว่างประเทศ. **กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป General Data Protection Regulation (GDPR).** https://www.moc.go.th/images/633/GDPR-3-5.pdf

[๘] ที่มา : ๑. ข่าวผู้จัดการออนไลน์ เรื่อง เทคโนโลยีจดจำใบหน้าไหลบ่าท่วมจีน https://mgronline.com/china/detail/9620000117043

๒.บทความ เรื่อง จากสงครามการค้า สู่สงครามเทคโนโลยี : สำรวจแนวรบฝั่งตะวันออก โดย ผศ.ดร.ปิติ ศรีแสงนาม ศูนย์เศรษฐกิจระหว่างประเทศ คณะเศรษฐศาสตร์ จุฬาฯ https://www.chula.ac.th/cuinside/19545/ และ ๓. บทความ เรื่อง การพัฒนาเศรษฐกิจดิจิทัลของจีน จากกรมเอเชียตะวันออก กระทรวงการต่างประเทศ http://www.eastasiawatch.in.th/th/articles/politics-and-economy/771/

๓. การเตรียมความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ของประเทศไทย ที่สำคัญ คือ กฎหมายที่เกี่ยวข้องกับการรักษาความปลอดภัยทางเทคโนโลยี ๓ เรื่อง[๙] ได้แก่ (๑)พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ (๒) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และ (๓) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

สำหรับยุทธศาสตร์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ โดยคณะกรรมการ**การรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ**[๑๐] ได้กำหนดแผนงานระยะเร่งด่วน ๖ เดือน / ๑ ปี และ ๒ ปี ที่หน่วยงานจะร่วมกันทำต่อไปใน ๘ ด้าน ที่สอดคล้องกับแผนยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๖๐ – ๒๕๖๔ คือ

(๑) การปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (Critical Information Infrastructure Protection: CIIP)

(๒) การสร้างศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์ (Emergency Readiness)

(๓) การบูรณาการการจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศ (Cybersecurity Governance)

(๔) การประสานความร่วมมือระหว่างภาครัฐและเอกชนเพื่อความมั่นคงปลอดภัยไซเบอร์ (Public-Private Partnership)

(๕) การสร้างความตระหนักและรอบรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Capacity Building)

(๖) การพัฒนากฎหมาย ระเบียบและมาตรฐานเพื่อความมั่นคงปลอดภัยไซเบอร์ (Law, Regulation and Standard)

---

[๙] ฉบับเต็มสืบค้นได้ที่ www.ratchakitcha.soc.go.th

[๑๐] **ข่าวประชาสัมพันธ์ EDTA สพธอ. เรื่อง** นายกฯ ประธานการประชุม คกก.เตรียมการไซเบอร์แห่งชาติครั้งแรก DE รับลูก พร้อมตั้งเป้าดันไทยติดอันดับ 1 ใน 20 ของโลกที่มีความพร้อม อ่านฉบับเต็มได้ที่ https://www.etda.or.th/content/thailand-national-cyber-security-preparedness-committee-meeting-1-2561.html

(๗) การประสานความร่วมมือระหว่างประเทศเพื่อความมั่นคงปลอดภัยไซเบอร์ (International Cooperation)

(๘) การวิจัยและพัฒนาเพื่อความมั่นคงปลอดภัยไซเบอร์ (Research & Development)

คณะกรรมการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ ได้เห็นชอบการจัดกลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (Critical Information Infrastructure: CII) ๖ กลุ่มแรก ได้แก่ กลุ่มความมั่นคงและบริการภาครัฐ กลุ่มการเงิน กลุ่มเทคโนโลยีสารสนเทศและโทรคมนาคม กลุ่มการขนส่งและโลจิสติกส์ กลุ่มพลังงานและสาธารณูปโภค และกลุ่มสาธารณสุข พร้อมยกระดับแผนการทำงานร่วมกัน เช่น ซ้อมรับมือภัยคุกคามทางไซเบอร์ รวมถึงจัดทำแผนปฏิบัติการรับมือไซเบอร์ (National Incident Handling Flow)

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) หรือ ETDA (เอ็ตด้า) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นเจ้าภาพหลักในการดำเนินงานจัดตั้งศูนย์ความร่วมมืออาเซียน-ญี่ปุ่น เพื่อพัฒนาบุคลากรความมั่นคงปลอดภัยไซเบอร์ หรือ ASEAN-Japan Cybersecurity Capacity Building Centre ตามมติที่ประชุม TELMIN-Japan หรือการประชุมรัฐมนตรีอาเซียนด้านโทรคมนาคมและเทคโนโลยีสารสนเทศร่วมกับประเทศญี่ปุ่น ที่ประเทศกัมพูชา และได้รับการสนับสนุนจากประเทศญี่ปุ่นทั้งด้านงบประมาณและองค์ความรู้สำหรับฝึกอบรมให้แก่ประเทศสมาชิกอาเซียนเพื่อความมั่นคงปลอดภัยไซเบอร์ ยกระดับขีดความสามารถของบุคลากร และปรับปรุงอันดับ ITU GCI ให้สูงขึ้นต่อไป

สำนักงานส่งเสริมเศรษฐกิจดิจิทัล กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ร่วมกับบริษัท กูเกิล (ประเทศไทย) จำกัด จัดทำโครงการพัฒนาทักษะและการเป็นพลเมืองดิจิทัล (Digital Citizenship) เพื่อเผยแพร่ความรู้ที่เกี่ยวข้องกับชุดทักษะและความรู้ การรักษาความปลอดภัย สิทธิและความรับผิดชอบ รวมไปถึงโอกาสและความท้าทายแห่งยุคสมัย อันเป็นเครื่องมือสำคัญในการก้าวเข้าสู่พลเมืองดิจิทัลที่สมบูรณ์

โดยมีรายละเอียดเพิ่มเติม ดังนี้

๑. ข้อมูลความเคลื่อนไหว/ การปรับตัว/ การศึกษา ขององค์กรระหว่างประเทศ รัฐบาลและหน่วยงานต่าง ๆ ในต่างประเทศ เพื่อรับมือกับสถานการณ์ Disruption

ศูนย์ส่งเสริมจริยธรรมได้ศึกษาข้อมูลความเคลื่อนไหว/การปรับตัว การศึกษาของหน่วยงานและประเทศต่าง ๆ ได้แก่ สหภาพโทรคมนาคมระหว่างประเทศ (ITU) องค์กรเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD) สหภาพยุโรป สหรัฐอเมริกา เยอรมัน สหราชอาณาจักร จีน เกาหลีใต้ ญี่ปุ่น สิงคโปร์ มาเลเซีย ในประเด็นต่าง ๆ เพื่อรับมือกับสถานการณ์ Disruption โดยสรุปดังนี้

หน่วยงาน/ประเทศ	ความเคลื่อนไหว/การปรับตัวในด้านต่าง ๆ		
	กรอบความร่วมมือ/ นโยบาย/กฎหมาย	หน่วยงาน/ประเทศ	กรอบความร่วมมือ/นโยบาย/กฎหมาย
๑. สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union: ITU) สำนักงานใหญ่อยู่ที่เมืองเจนีวา ประเทศสวิตเซอร์แลนด์	กรอบความร่วมมือระหว่างประเทศ Global Cybersecurity Agenda (GCA)	International Multilateral Partnership against Cyber Threats (IMPACT) สำนักงานใหญ่อยู่ที่เมืองไซเบอร์จาวา ประเทศมาเลเซีย	- IMPACT เป็นศูนย์บริหารจัดการกับภัยไซเบอร์ มีเทคโนโลยี กลไก หรือแพลตฟอร์มที่กำกับดูแล เตือนภัยไซเบอร์ได้อย่างทันทีทันใด (real time) - เป็นศูนย์กลางฝึกอบรม สัมมนาพัฒนาทักษะ ฝึกซ้อมรับมือภัยคุกคาม ให้ทุนฝึกอบรมแก่องค์กรในประเทศกำลังพัฒนา ให้คำปรึกษา เป็นที่รวมผู้เชี่ยวชาญด้านไซเบอร์ของทุกประเทศ - เป็นศูนย์กลางประกันความปลอดภัย ให้คำแนะนำด้านความปลอดภัยและการตอบโต้ภัยไซเบอร์ และวิจัยในประเด็นที่เกี่ยวข้อง - เป็นศูนย์กลางนโยบายและความร่วมมือระหว่างประเทศ
๒. องค์กรเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD)	ข้อเสนอแนะด้านความมั่นคงปลอดภัยทางดิจิทัล (OECD Recommendation	-	กำหนดข้อเสนอแนะให้รัฐบาลและเจ้าหน้าที่พึงปฏิบัติ ๔ ประการ คือ ๑) กำหนดกรอบนโยบายรองรับความปลอดภัยดิจิทัลในยุทธศาสตร์ชาติ (OverarchingPolicy Framework)

หน่วยงาน/ประเทศ	ความเคลื่อนไหว/การปรับตัวในด้านต่าง ๆ		
	กรอบความร่วมมือ/นโยบาย/กฎหมาย	หน่วยงาน/ประเทศ	กรอบความร่วมมือ/นโยบาย/กฎหมาย
	on Digital Security of Critial Activities)		๒) กำหนดมาตรการปฏิบัติการสำหรับเจ้าหน้าที่ของรัฐ (Measures for Operators) ๓) สร้างความร่วมมือระหว่างภาครัฐและเอกชนทั้งในและต่างประเทศ ในความปลอดภัยดิจิทัล (Trust-Based Partnerships) ๔) พัฒนาความร่วมมือในระดับนานาชาติ (International Co-operation)
๓. สหภาพยุโรป	กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป หรือ General Data Protection Regulation (GDPR)	-	เผยแพร่เนื้อหากฎหมาย ซึ่งมีขอบเขตการบังคับใช้กับ ๓ กลุ่ม คือ ๑) ผู้ควบคุมข้อมูลส่วนบุคคล (Controller) ๒) ผู้ประมวลผลข้อมูลส่วนบุคคล (Processor) รวมถึงการบันทึกและจัดเก็บข้อมูลด้วย และ ๓) เจ้าของข้อมูลการประมวลผลข้อมูลส่วนบุคคล (Data Subject) ซึ่งเป็นผู้พิจารณาให้ความยินยอมหรือไม่ยินยอม (Consent) โดยผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลอาจมีสถานประกอบการอยู่ภายในสหภาพยุโรป หรือไม่อยู่ภายในสหภาพยุโรป แต่การประมวลผลนั้นเกี่ยวข้องกับการเสนอสินค้าหรือบริการให้แก่บุคคลผู้พำนักในสหภาพยุโรปหรือหากมีการประมวลผลข้อมูลส่วน

หน่วยงาน/ประเทศ	ความเคลื่อนไหว/การปรับตัวในด้านต่าง ๆ		
	กรอบความร่วมมือ/นโยบาย/กฎหมาย	หน่วยงาน/ประเทศ	กรอบความร่วมมือ/นโยบาย/กฎหมาย
			บุคคลนอกอาณาเขตของสหภาพยุโรป และประเทศนั้นมีผลผูกพันทางกฎหมายกับประเทศสหภาพยุโรปเช่น สนธิสัญญา จะตกอยู่ภายใต้ขอบเขตการบังคับใช้ของ GDPR ด้วยเช่นเดียวกัน
๔. หน่วยงานเอกชน/วิชาการ ๔.๑ Microsoft	กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป หรือ General Data Protection Regulation (GDPR)	ทีมงานกลางของ Microsoft	- กำหนดขอบเขตที่แน่นอนในการป้องกันข้อมูลส่วนบุคคล - จัดฝึกอบรมให้ทีมงาน สัมมนา เพิ่มขีดความสามารถให้ผู้เชี่ยวชาญเฉพาะด้าน จัดทำเอกสารแนะนำการใช้งาน - ปรับปรุงข้อกำหนดของกฎความเป็นส่วนตัว - ลงทุนกับเทคโนโลยีใหม่
๔.๒ Facebook		ทีมงานด้านความเป็นส่วนบุคคล	- ทำงานร่วมกับผู้เชี่ยวชาญเพื่อออกแบบความเป็นส่วนบุคคล ศึกษาวิจัย สร้างนโยบาย พัฒนาการปกป้องข้อมูลส่วนบุคคล - ปรับปรุงข้อกำหนดความเป็นส่วนตัวและชี้แจงให้ผู้ใช้งานทราบถึงข้อกำหนดและสิทธิของผู้ใช้งาน
๔.๓ Amazon Web Service (AWS)		ทีมงานฝ่ายปกป้องข้อมูล	ปฏิบัติตามข้อกำหนดอื่นนอกเหนือจาก GDPR เพื่อรับรองว่าสินค้าและบริการมีความสอดคล้องกับ GDPR ได้แก่ - EU-US Privacy Shield

หน่วยงาน/ประเทศ	ความเคลื่อนไหว/การปรับตัวในด้านต่าง ๆ		
	กรอบความร่วมมือ/นโยบาย/กฎหมาย	หน่วยงาน/ประเทศ	กรอบความร่วมมือ/นโยบาย/กฎหมาย
			- หลักจรรยาบรรณของ CISPE (Cloud Infrastructure Services Provider in EU) - มาตรฐานความปลอดภัย ISO 27017-8 นอกจากนั้น ยังกำหนดแนวทางแจ้งหน่วยงานที่กำกับ แจ้งเตือนการรั่วไหลของข้อมูล กำหนดข้อตกลงการประมวลผลข้อมูลต่าง ๆ ฯลฯ
๔.๔ Google		ทีมงานรักษาความปลอดภัยของข้อมูล	- ปรับปรุงนโยบายและหลักเกณฑ์เพื่อการปกป้องข้อมูล ให้สอดคล้องกับ GDPR ให้เป็นปัจจุบันและทันสมัยตลอดเวลา - ทำ Client Checklist โดยกำหนดเนื้อหาสำคัญ - แต่งตั้งทีมรักษาความปลอดภัย และให้มีการตรวจสอบโดยผู้ตรวจสอบภายนอก - เตรียมเทคโนโลยีป้องกัน และโปรแกรมจัดการตอบสนองภัยคุกคาม - สร้างความโปร่งใสในการใช้ข้อมูลของ User - ปฏิบัติตามมาตรฐานความปลอดภัยระดับสากลอื่น ๆ
๔.๕ Uber	นโยบายการไม่เลือกปฏิบัติ และ		- นโยบายไม่เลือกปฏิบัติ หากพนักงานคนขับรถคนใดละเมิด จะหมดสิทธิ์ในการเข้าใช้ Platform ของ Uber

หน่วยงาน/ประเทศ	ความเคลื่อนไหว/การปรับตัวในด้านต่าง ๆ		
	กรอบความร่วมมือ/นโยบาย/กฎหมาย	หน่วยงาน/ประเทศ	กรอบความร่วมมือ/นโยบาย/กฎหมาย
	นโยบายการขัดกันของผลประโยชน์		- พนักงานของ Uber ต้องลงนามรับทราบและปฏิบัติตามนโยบายการขัดกันของผลประโยชน์ (Conflict of Interest) เช่น นโยบายการจ้างงาน การใช้โอกาสทางธุรกิจขององค์กรเพื่อประโยชน์ส่วนตัว การรับของขวัญ การเปิดช่องทางรับเรื่องร้องเรียน และความคิดเห็นต่าง ๆ ผ่านแอป หรือ help.uber.com หรืออีเมลไปที่ศูนย์รับเรื่องร้องเรียนลูกค้า
๔.๖ Netflix	จรรยาบรรณสำหรับผู้บริหารและเจ้าหน้าที่		จรรยาบรรณที่เน้นการกระทำด้วยความซื่อสัตย์ จริยธรรม ผลประโยชน์ทับซ้อน การเปิดเผยข้อมูลในรายงานและเอกสารต่าง ๆ ต่อหน่วยงานที่เกี่ยวข้อง การปฏิบัติตามกฎหมาย เป็นต้น
๔.๗ Debrett's และ Facebook	ศิลปะแห่งการส่งข้อความดิจิทัล : แนวทางของการสื่อสารในยุคดิจิทัล (The Art of Digital Messaging: A Guide to Communication in the Digital Age)		คู่มือว่าด้วยกฎ กติกา มารยาทว่าด้วยการแชตสนทนาในยุคดิจิทัล ๑๐ ข้อ ๑) สื่ออารมณ์และความหมายให้ดี ๒) กระชับเข้าไว้ แต่อย่าสั้นจนเกินไป ๓) อย่าส่งหลายข้อความติดๆกัน ๔) แคร์สักนิดก่อนคิดแชร์ ๕) ต้องรู้ว่ากำลังแชตอยู่กับใคร ๖) อย่าปล่อยให้รอเก้อ ๗) ตอบกลับให้ฉับไว ๘) เลิกนิสัยชอบเท ๙) ฝึกลาให้ถูกธรรมเนียม

หน่วยงาน/ประเทศ	ความเคลื่อนไหว/การปรับตัวในด้านต่าง ๆ		
	กรอบความร่วมมือ/นโยบาย/กฎหมาย	หน่วยงาน/ประเทศ	กรอบความร่วมมือ/นโยบาย/กฎหมาย
๔.๘ Mike Ribble	หลักการพื้นฐาน ๙ ประการ ของการใช้เทคโนโลยีอย่างเหมาะสมและมีความรับผิดชอบที่พลเมืองดิจิทัลควรตระหนัก (Nine Elements of Digital Citizenship)		หลักของพลเมืองดิจิทัล ๙ ประการ คือ ๑) โอกาสในการเข้าถึงดิจิทัลอย่างเท่าเทียม ๒) การพาณิชย์ดิจิทัล ๓) การสื่อสารดิจิทัล ๔) เท่าทันดิจิทัล ๕) มารยาททางดิจิทัล ๖) กฎหมายเกี่ยวกับดิจิทัล ๗) สิทธิและความรับผิดชอบทางดิจิทัล ๘) สุขภาพและความเป็นอยู่ที่ดีทางดิจิทัล ๙) ความปลอดภัยทางดิจิทัล
๕. สหรัฐอเมริกา	แผนคุ้มครองโครงสร้างพื้นฐานแห่งชาติ (National Protection Infrastructure Plan)	กระทรวงความมั่นคงแห่งมาตุภูมิ (Department of Homeland Security : DHS) กระทรวงกลาโหม US-CERT สถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา	- รักษาความปลอดภัยไซเบอร์โครงสร้างพื้นฐาน มีกลุ่มเฝ้าระวังและตอบโต้ภัยคุกคามทางคอมพิวเตอร์ (CR) - มีคณะทำงานเพื่อดูแลระบบคอมพิวเตอร์ของสหรัฐ เพื่อตอบโต้การโจมตีทางไซเบอร์ และออกประกาศแจ้งเตือนภัยอย่างต่อเนื่อง ดำเนินงานตลอด ๒๔ ชั่วโมง ๗ วันต่อสัปดาห์ ให้ข้อมูลประชาชนผ่านเว็บไซต์บูรณาการความร่วมมือกับทุกฝ่าย สนับสนุนการสืบหาภัยทางไซเบอร์ด้วยเทคโนโลยีทันสมัย
๖. สหพันธ์สาธารณรัฐเยอรมัน		ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบ	เป็นศูนย์รวมการติดต่อเพื่อกำหนดมาตรการในการป้องกัน ตอบโต้กับเหตุการณ์ทางไซเบอร์ โดยให้บริการตลอด ๒๔ ชั่วโมง ๗ วันต่อสัปดาห์

หน่วยงาน/ประเทศ	ความเคลื่อนไหว/การปรับตัวในด้านต่าง ๆ		
	กรอบความร่วมมือ/นโยบาย/กฎหมาย	หน่วยงาน/ประเทศ	กรอบความร่วมมือ/นโยบาย/กฎหมาย
		คอมพิวเตอร์แห่งเยอรมัน (CERT-Bund)	วิเคราะห์เหตุการณ์ที่มีรายงาน ทำข้อเสนอแนะ และให้การสนับสนุนดำเนินการแจ้งเตือน และส่งสัญญาณเตือนผู้บริหารรัฐกรณีที่เกิดความเสียหายร้ายแรง และเสนอข่าวสารแจ้งเตือนทางออนไลน์
๗. สหราชอาณาจักร		ศูนย์ป้องกันโครงสร้างพื้นฐานแห่งชาติ (Centre for the Protection of National Infrastructure : CPNI)	- เป็นหน่วย Computer Emergency Response Term (CSIRT/CERT) ระดับชาติ - ดูแลโครงสร้างพื้นฐานให้ปลอดภัยจากภัยไซเบอร์
๘.สาธารณรัฐประชาชนจีน	- โครงการ Great Firewall Project - โครงการ Golden Shield Project - นโยบาย Made in China ๒๐๒๕ - กฎหมาย ระบบการจดจำใบหน้า (Facial Recognition)	รัฐบาลและกระทรวงสารสนเทศและเทคโนโลยีแห่งจีน	- สร้างกองทัพไซเบอร์ราว ๒ ล้านคน (ในปี ๒๐๐๓) เพื่อสกัดกั้นข้อมูลข่าวสารที่ไม่พึงประสงค์ - พัฒนาระบบออนไลน์ต่าง ๆ ของจีน เช่น Tencent, Alibaba และ Baidu แทน Facebook, Amazon และ Google ชมคลิปวีดิโอออนไลน์ ผ่าน Youku และ Tudou.com แทน Youtube เป็นต้น - เน้นให้มีการบริโภคภายในประเทศ โดยทำสินค้าให้มีคุณภาพสูง ล้างภาพลักษณ์สินค้าปลอม เพื่อขับเคลื่อนทางเศรษฐกิจ - สร้างระบบสแกนใบหน้า เพื่อลดปัญหามิจฉาชีพ ขโมย และเพิ่มกล้องวงจรปิดในที่สาธารณะ

หน่วยงาน/ประเทศ	ความเคลื่อนไหว/การปรับตัวในด้านต่าง ๆ		
	กรอบความร่วมมือ/นโยบาย/กฎหมาย	หน่วยงาน/ประเทศ	กรอบความร่วมมือ/นโยบาย/กฎหมาย
๙. สาธารณรัฐเกาหลี	แผนงานขับเคลื่อนสู่การปฏิวัติอุตสาหกรรมครั้งที่ ๔ - ปรับปรุงแก้ไขกฎหมายต่าง ๆ เพื่อรองรับเทคโนโลยี เช่น กฎหมายจราจรโดยรองรับสถานะผู้ขับขี่ยานยนต์อัตโนมัติ เพิ่มการควบคุม Drone กฎหมายเกี่ยวกับการเดินเรือเพื่อให้เรืออัตโนมัติสามารถปฏิบัติการได้ ฯลฯ	รัฐบาลเกาหลี และศูนย์ป้องกันการก่อการร้ายทางโลกไซเบอร์ ศูนย์ปฏิบัติการด้านการรักษาความปลอดภัยข้อมูลคอมพิวเตอร์แห่งชาติ (KISA) กระทรวงสารสนเทศและการสื่อสาร	- วิจัย พัฒนา และวางแผนความปลอดภัยข้อมูลสารสนเทศ เครือข่ายอินเตอร์เนตของประเทศ - ประสานงานกับหน่วยงานในต่างประเทศ - ออกใบรับรองอิเล็กทรอนิกส์ของเว็บไซต์ของประเทศ - ให้บริการตรวจสอบระดับความปลอดภัยของหน่วยงานต่าง ๆ - ฝึกอบรม สร้างความตระหนักในความปลอดภัยไซเบอร์ - ทำหนังสือการรักษาความปลอดภัยสัมมนาความปลอดภัยทางไซเบอร์
๑๐. ญี่ปุ่น		JPCERT/CC	เครือข่ายการรักษาความปลอดภัยไซเบอร์ในภูมิภาคเอเชียแปซิฟิก โดยมีญี่ปุ่นเป็นแกนนำและพี่เลี้ยงให้ความช่วยเหลือในการตั้งกลุ่ม CSIRT/CERT
๑๑. สิงคโปร์		SingCERT (ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งสิงคโปร์)	- ประกาศ แจ้งเตือนภัยไซเบอร์ ให้คำปรึกษา เป็นผู้ดูแลด้านความปลอดภัยไซเบอร์ - สร้างความตระหนักด้านความปลอดภัยไซเบอร์ผ่านการสัมมนาประชุม

หน่วยงาน/ประเทศ	ความเคลื่อนไหว/การปรับตัวในด้านต่าง ๆ		
	กรอบความร่วมมือ/นโยบาย/กฎหมาย	หน่วยงาน/ประเทศ	กรอบความร่วมมือ/นโยบาย/กฎหมาย
			ฝึกซ้อมรับมือภัยไซเบอร์ให้ประเทศต่าง ๆ ในอาเซียน
๑๒. สหพันธรัฐมาเลเซีย		ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งมาเลเซีย MyCERT ภายใต้กระทรวงวิทยาศาสตร์เทคโนโลยีและนวัตกรรม (Minister of Science, Technology and Innovation: MOSTI) ของมาเลเซีย	- ให้ความช่วยเหลือในการรับมือภัยไซเบอร์ การระบุตัวตนของผู้กระทำผิดชนิดของมัลแวร์ - พัฒนาเครื่องมือสำหรับจัดการกับมัลแวร์

๑) สหภาพโทรคมนาคมระหว่างประเทศ (ITU)[๑๑]

สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union: ITU) เป็นองค์กรพิเศษของสหประชาชาติซึ่งเป็นองค์กรที่เก่าแก่มากดูแลข้อมูลข่าวสารและเทคโนโลยีการสื่อสาร (Information and Communication Technology: ICT) สำนักงานใหญ่อยู่ที่เมืองเจนีวา ประเทศสวิตเซอร์แลนด์ และมีสำนักงานระดับภูมิภาคอีก ๑๒ แห่ง ทั่วโลก ITU ประกอบด้วยสมาชิกจากประเทศต่างๆ จำนวน ๑๙๓ ประเทศ เท่ากับจำนวนประเทศ ที่เป็นสมาชิกของสหประชาชาติ นอกจากนี้ ITU ยังเปิดรับสมาชิกแบบองค์กรภาคเอกชน สมาคม และหน่วยงานการศึกษาอีกด้วย ประเทศไทยได้เข้าเป็นสมาชิกของ ITU เมื่อวันที่ ๒๐ เมษายน

[๑๑] **สรุปการศึกษาเรื่อง “ความเป็นไปได้ในการพัฒนาระบบเตือนภัยการโจมตี และแนวทางการบริหารจัดการของประเทศไทย”** ของสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ โดยสถาบันเทคโนโลยีพระจอมเกล้าคุณทหารลาดกระบัง สืบค้นจาก http://lib.nbtc.go.th/

ค.ศ. ๑๘๘๓ ปัจจุบันขอบเขตงานของ ITU ขยายจากโทรเลขและโทรศัพท์ มาเป็นการสื่อสารผ่านดาวเทียม โทรศัพท์มือถือ อินเทอร์เน็ต การสื่อสารในช่วงภัยพิบัติ และการใช้งาน ICT ทั่วไป ITU ได้ ก่อตั้ง Global Cybersecurity Agenda (GCA) ซึ่งเป็นกรอบความร่วมมือระหว่างประเทศ มีจุดมุ่งหมายเพื่อการขยายความมั่นคงปลอดภัยในสังคมข้อมูลข่าวสารทางไซเบอร์ GCA เป็นกรอบเพื่อกระตุ้นความร่วมมือระหว่างประเทศสมาชิก ลดกิจกรรมที่ซ้ำซ้อนกัน และยังได้เปิดหน่วยงาน International Multilateral Partnership against Cyber Threats (IMPACT) ขึ้นในปี ๒๐๐๘ เพื่อเป็นจุดรับและกระจายด้านความปลอดภัยไซเบอร์ของโลก (Global Cybersecurity Hub) มีสำนักงานใหญ่ตั้งอยู่ที่เมืองไซเบอร์จาวา ประเทศมาเลเซีย ปัจจุบันมีสมาชิกจำนวน ๑๕๒ ประเทศ IMPACT เป็นหน่วยงานที่ช่วยต่อต้านภัยไซเบอร์พัฒนาวิธีการ และจัดการกับภัยไซเบอร์ในระดับโลกให้แก่องค์กรภาครัฐ และเอกชนของประเทศสมาชิก ภายใต้กรอบของ GCA หน่วยงาน IMPACT ยังได้เปิดเวทีความร่วมมือนานาชาติระหว่างภาครัฐ ผู้นำทางอุตสาหกรรม สถาบันการศึกษา และหน่วยงานบังคับใช้กฎหมาย เพื่ออำนวยการเสริมสร้างยุทธศาสตร์ด้านความปลอดภัยไซเบอร์และการป้องกันระบบข้อมูลของโครงสร้างพื้นฐานของแต่ละประเทศสมาชิก เพิ่มการประสานงานและความร่วมมือที่เกี่ยวกับความปลอดภัยไซเบอร์ โดยหน่วยงาน IMPACT มีวัตถุประสงค์การดำเนินงาน ดังนี้

(๑) เพื่อรักษาระดับและเพิ่มความแข็งแกร่งด้านความร่วมมือกับประเทศสมาชิก เพื่อเสริมสร้างขีดความสามารถในการจัดการกับภัยไซเบอร์

(๒) เพื่อเพิ่มขีดความสามารถในการสื่อสาร และการจัดการกับเหตุการณ์ของประเทศสมาชิก

(๓) เพื่อช่วยเหลือประเทศสมาชิกในการพัฒนา และจัดวางขั้นตอนดำเนินงาน เพื่อตอบโต้กับเหตุการณ์ไซเบอร์ต่างๆ การจัดทำแผนสำหรับการรับมือกับภัยคุกคามในอนาคต รวมถึงการปรับปรุงกระบวนการในการดำเนินงานให้มีประสิทธิภาพมากยิ่งขึ้น

(๔) เพื่อเป็นศูนย์รวมในการประสานงานด้านความปลอดภัยไซเบอร์ที่น่าเชื่อถือ สามารถที่จะระบุปัญหา ป้องกัน ตอบโต้และให้คำแนะนำเกี่ยวกับการจัดการกับภัยไซเบอร์แก่สมาชิกได้อย่างมีประสิทธิภาพ

๒) องค์กรเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD)[๑๒]

องค์กรเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD) เผยแพร่ข้อเสนอแนะด้านความมั่นคงปลอดภัยทางดิจิทัลของภารกิจภาครัฐที่มีความสำคัญ (OECD Recommendation on Digital Security of Critial Activities) ในวันที่ ๑๑ ธันวาคม ๒๕๖๒ โดยระบุว่าในปัจจุบัน ภารกิจด้านสังคมและเศรษฐกิจของรัฐโดยมากต้องพึ่งพาเทคโนโลยีดิจิทัล ซึ่งในกรณีที่ภารกิจซึ่งมีความสำคัญเหล่านี้เกิดความขัดข้อง จะก่อให้เกิดผลกระทบอย่างร้ายแรงต่อสุขภาพ และความมั่นคงปลอดภัยของประชาชนได้ ในทางกลับกัน การปฏิบัติหน้าที่อย่างมีประสิทธิภาพของภารกิจดังกล่าว จะส่งผลให้ต่อความเจริญรุ่งเรืองทางเศรษฐกิจและสังคมอย่างกว้างขวาง สิ่งคุกคามต่อความมั่นคงปลอดภัยทางดิจิทัลนับวันยิ่งมีมากขึ้นเรื่อยๆ ทั้งในแง่ของความถี่และความซับซ้อน สถานการณ์นี้ส่งผลให้รัฐบาลประเทศต่าง ๆ ต้องปรับใช้นโยบาย/กลไกที่จะส่งเสริมความมั่นคงปลอดภัยดิจิทัลในภารกิจของรัฐที่สำคัญ แต่นโยบายดังกล่าวจะต้องไม่ขัดขวางผลประโยชน์ที่ชาติจะได้รับจากการเปลี่ยนแปลงทางดิจิทัลของภารกิจของรัฐที่สำคัญนั้น ๆ ด้วยระบบตรวจสอบป้องกันรูปแบบใด ๆ ที่อาจมีลักษณะกีดขวาง ไม่เหมาะสม หรือไม่สอดคล้องกับการใช้ประโยชน์จากเทคโนโลยีดิจิทัลนั้นๆ

OECD จึงกำหนดข้อเสนอแนะเชิงนโยบายสำหรับเจ้าหน้าที่ของรัฐผู้ปฏิบัติหน้าที่ในภารกิจของรัฐที่สำคัญ โดยมุ่งเน้นไปยังสิ่งที่สำคัญสำหรับเศรษฐกิจและสังคม โดยไม่สร้างภาระที่ไม่จำเป็นต่อภาคส่วนอื่น ๆ โดยระบุให้รัฐบาลพึงปฏิบัติโดยสรุปดังนี้

๑) ปรับใช้กรอบนโยบายที่ครอบคลุม (Overarching Policy Framework)

รัฐบาลควรปลูกฝังกรอบนโยบายที่ครอบคลุม ซึ่งได้ระบุวัตถุประสงค์ที่ชัดเจนในการเสริมสร้างความปลอดภัยดิจิทัล ไว้ในยุทธศาสตร์ด้านความปลอดภัยดิจิทัลระดับชาติ รวมทั้งการประเมินความเสี่ยง และกลไกการบริหารภายในประเทศ ทั้งนี้ การประสานงานภายในประเทศมีความสำคัญอย่างยิ่ง เพื่อให้นโยบายความปลอดภัยดิจิทัลมีความสอดคล้องกับกฎระเบียบที่มีอยู่ในส่วนราชการสำคัญ (เช่น พลังงาน ธนาคาร หรือสาธารณสุข) รัฐบาลควรพัฒนาศักยภาพเพื่อรองรับการจัดการความเสี่ยงด้านความปลอดภัยดิจิทัล และการฟื้นตัวของส่วนราชการสำคัญ

[๑๒] OECD. **Recommendation on Digital Security of Critical Activities.** www.oecd.org/going-digital/topics/digital-security-and-privacy/recommendation-on-digital-security-of-critical-activities.htm

ซึ่งรวมถึงการสร้างหรือพัฒนาความสามารถในการตอบสนองต่อปัญหาในปัจจุบัน ผ่านทางคณะทำงานเพื่อดูแลระบบคอมพิวเตอร์ (CERTs / CSIRTs) หรือ Security Operation Center (SOCs) นอกจากนี้ ยังรวมถึงการเสริมสร้างความปลอดภัยของบริการดิจิทัลภาครัฐที่สำคัญการส่งเสริมมาตรฐานสากลในระดับนานาชาติ (เช่น สหภาพยุโรป) และการสนับสนุนผู้ประกอบการตามความเหมาะสม

๒) ใช้มาตรการสำหรับเจ้าหน้าที่ของรัฐ (Measures for Operators)

เจ้าหน้าที่ของรัฐผู้ได้รับมอบหมายให้บริหารจัดการความเสี่ยงทางความปลอดภัยดิจิทัลของภารกิจภาครัฐที่สำคัญซึ่งตนได้รับมอบหมาย จะต้องปกป้องให้ภารกิจภาครัฐนั้นๆ สามารถดำเนินการได้อย่างต่อเนื่อง ยั่งยืน และปลอดภัย โดยจะต้องลดความเสี่ยงดังกล่าว ให้อยู่ในระดับที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงระดับชาติ โดยการส่งเสริมหรือกำหนดให้เจ้าหน้าที่ของรัฐมีมาตรการในการกำกับดูแล ป้องกัน ตรวจสอบ และฟื้นฟู อย่างมีประสิทธิภาพทุกขั้นตอน

รัฐบาลควรสร้างและส่งเสริมความเชื่อมั่นในความร่วมมือรูปแบบภาคีอย่างยั่งยืนบนพื้นฐานของความเชื่อมั่น (Trust-Based Partnerships)เพื่อให้การจัดการความเสี่ยงทางดิจิทัลของภารกิจภาครัฐที่มีความสำคัญ ได้รับการประโยชน์จากการพึ่งพาข้ามภาคส่วนราชการและประเทศอย่างเหมาะสม โดยภาครัฐจะต้องพัฒนาภาคีสำหรับการกำหนดและบังคับใช้นโยบายเสริมสร้างความร่วมมือในการปฏิบัติการระหว่างเจ้าหน้าที่ของรัฐในภาคส่วนและระดับต่าง ๆ สร้างเงื่อนไขที่ก่อให้เกิดความไว้วางใจกันระหว่างภาคี รวมทั้งระมัดระวังการใช้และแลกเปลี่ยนข้อมูลระหว่างภาคี ซึ่งอาจมีผลกระทบต่อความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคล

๓) ส่งเสริมและพัฒนาความร่วมมือในระดับนานาชาติ (International Co-operation)

รัฐบาลควรส่งเสริมความร่วมมือในระดับนานาชาติ โดยแลกเปลี่ยนข้อมูลประสบการณ์ และข้อมูลรวมทางสถิติร่วมกัน รวมทั้งช่วยเหลือสนับสนุนการสร้างเสริมสมรรถภาพทางด้านความปลอดภัยดิจิทัลของประเทศอื่น ๆ

๓) สหภาพยุโรป

ปรากฏมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป หรือ General Data Protection Regulation (GDPR)[๑๓] โดยสรุปสาระสำคัญได้ดังนี้

General Data Protection Regulation หรือเรียกด้วยอักษรย่อว่า GDPR เป็นกฎหมายของสหภาพยุโรปว่าด้วยมาตรการคุ้มครองความเป็นส่วนตัวของข้อมูลส่วนบุคคล ซึ่งมีผลบังคับใช้วันที่ ๒๕ พฤษภาคม ๒๕๖๑ โดยเข้ามาแทนที่กฎหมายเดิม คือ Data Protection Directive ที่บังคับใช้มาตั้งแต่ปี ๒๕๓๘ สำหรับใช้เป็นหลักการเบื้องต้นให้สมาชิกใช้เป็นแนวทางในการร่างกฎหมายภายใน และกำหนดบทลงโทษของตนเอง และขยายความเรื่องการคุ้มครองข้อมูลและข้อมูลส่วนบุคคลของสหภาพยุโรป ให้มีความชัดเจนและรัดกุมมากขึ้น เพิ่มความโปร่งใส และเป็นมาตรฐานเดียวกันทั่วยุโรป และสิ่งสำคัญคือ การคุ้มครองข้อมูลของพลเมืองสหภาพยุโรปที่ไม่ว่าข้อมูลจะเก็บอยู่ที่ใดในโลก ก็ต้องปฏิบัติตาม GDPR

GDPR อาจส่งผลกระทบต่อหลายฝ่าย โดยเฉพาะอย่างยิ่ง หน่วยงานต่าง ๆ ไม่ว่าภาครัฐ ภาคเอกชน หรือ ภาคธุรกิจที่มีการดำเนินการเกี่ยวกับการเก็บข้อมูลส่วนบุคคล หรือ การให้บริการออนไลน์แก่บุคคลที่อยู่ในสหภาพยุโรป ดังนั้น การเตรียมความพร้อมและทำความเข้าใจกฎหมาย GDPR จึงมีความจำเป็นเพื่อส่งเสริมการคุ้มครองข้อมูลส่วนบุคคลของภาคธุรกิจให้เทียบเท่ากับมาตรฐานสากล และป้องกันผลกระทบจากกฎหมายที่อาจเกิดขึ้นอีกด้วย โดยสามารถสรุปหลักการสำคัญของกฎหมาย GDPR ได้ดังนี้

(๑) ข้อมูลส่วนบุคคล (Personal Data)

ข้อมูลส่วนบุคคลตามนิยามของ GDPR คือ ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม รวมถึงข้อมูลที่นำมารวมกันแล้วสามารถใช้ระบุอัตลักษณ์ของบุคคลได้

ประเภทตัวอย่างข้อมูล	รายการ
ข้อมูลส่วนบุคคล	ชื่อ-นามสกุล
	ที่อยู่บ้าน

[๑๓] ***กฎหมาย GDPR ฉบับรวบรัด.*** https://www.etda.or.th/content/gdpr-in-a-nutshell

สำนักเจรจาการค้าบริการและการลงทุน กรมเจรจาการค้าระหว่างประเทศ. ***กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป General Data Protection Regulation (GDPR).*** https://www.moc.go.th/images/633/GDPR-3-5.pdf

	อีเมล เช่น name.surname@company.com
	หมายเลขบัตรประจำตัว
	ข้อมูลที่ตั้ง (Location Data) เช่น ข้อมูลที่ตั้งจากโทรศัพท์เคลื่อนที่
	IP Address
	Cookie ID
	หมายเลข ID เพื่อใช้ในการโฆษณาในโทรศัพท์เคลื่อนที่
	เวชระเบียนและข้อมูลสุขภาพอื่น ๆ ซึ่งสามารถใช้ระบุอัตลักษณ์ของผู้ป่วยได้
	พฤติกรรมการบริโภคสินค้า-บริการ
ข้อมูลที่ไม่นับว่าเป็นข้อมูลส่วนบุคคล	หมายเลขจดทะเบียนบริษัท
	อีเมล เช่น info@company.com
	ข้อมูลนิรนาม

(๒) บทบาทของผู้เกี่ยวข้องกับการประมวลผลข้อมูล

GDPR ได้ให้คำจำกัดความและหน้าที่ของบทบาทของผู้เกี่ยวข้องกับการประมวลผลข้อมูลหลักไว้ ๓ บทบาท ดังนี้

(๒.๑) ผู้ควบคุมข้อมูลส่วนบุคคล (Controller) คือ กำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูล ซึ่งโดยส่วนมากจะเป็นผู้ขอความยินยอมจากเจ้าของข้อมูล เช่น ผู้ให้บริการเว็บไซต์ต่าง ๆ

(๒.๒) ผู้ประมวลผลข้อมูลส่วนบุคคล (Processor) คือ ผู้ประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์และวิธีการของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งในทางปฏิบัติอาจเป็นบุคคลเดียวกับผู้ควบคุมข้อมูลส่วนบุคคลก็ได้ อนึ่ง “การประมวลผลข้อมูล” (Processing) ตามกฎหมาย GDPR นั้น ไม่ใช่เพียงแค่การวิเคราะห์ หรือ จัดการข้อมูลแบบทั่วไปเท่านั้น แต่ให้รวมถึงการบันทึกและจัดเก็บข้อมูลด้วย

(๒.๓) เจ้าของข้อมูลส่วนบุคคล (Data Subject)

(๓) ขอบเขตการบังคับใช้โดยสังเขป

หลักเกณฑ์ที่จะต้องพิจารณาต่อไปคือ การประมวลผลข้อมูลส่วนบุคคลกระทำ “ที่ใด” และข้อมูลส่วนบุคคลเป็น “ของใคร” ซึ่งกฎหมาย GDPR ได้กำหนดให้ “การประมวลผลข้อมูล” ในลักษณะต่อไปนี้ต้องตกอยู่ภายใต้ขอบเขตการบังคับใช้ของกฎหมาย GDPR ดังนี้

(๓.๑) “ผู้ควบคุมข้อมูลส่วนบุคคล” หรือ “ผู้ประมวลผลข้อมูลส่วนบุคคล” มีสถานประกอบการอยู่ภายในสหภาพยุโรป

(๓.๒) “ผู้ควบคุมข้อมูลส่วนบุคคล” หรือ “ผู้ประมวลผลข้อมูลส่วนบุคคล” ไม่มีสถานประกอบการอยู่ภายในสหภาพยุโรป แต่การประมวลผลนั้นเกี่ยวข้องกับการเสนอสินค้าหรือบริการให้แก่บุคคลผู้พำนักในสหภาพยุโรป

(๓.๓) “ผู้ควบคุมข้อมูลส่วนบุคคล” หรือ “ผู้ประมวลผลข้อมูลส่วนบุคคล” ไม่มีสถานประกอบการอยู่ภายในสหภาพยุโรป แต่การประมวลผลนั้นเกี่ยวข้องกับการเฝ้าสังเกตพฤติกรรมที่เกิดขึ้นในสหภาพยุโรป ทั้งนี้ หากมีการประมวลผลข้อมูลส่วนบุคคลนอกอาณาเขตของสหภาพยุโรป และประเทศนั้นมีผลผูกพันทางกฎหมายกับประเทศสหภาพยุโรป เช่น สนธิสัญญา จะตกอยู่ภายใต้ขอบเขตการบังคับใช้ของ GDPR เช่นเดียวกัน

(๔) หลักการขอ “ความยินยอม” (Consent)

เมื่อการประมวลผลข้อมูลส่วนบุคคลตกอยู่ภายใต้ขอบเขตการบังคับใช้กฎหมาย GDPR ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องปฏิบัติตามหลักพื้นฐานในการประมวลผลข้อมูลส่วนบุคคล เช่น ต้องประมวลผลข้อมูล “โดยชอบด้วยกฎหมาย” เป็นธรรม และโปร่งใสต่อเจ้าของข้อมูล ซึ่งการประมวลผลข้อมูลจะชอบด้วยกฎหมายหรือไม่นั้นต้องพิจารณาจาก “ความยินยอม” (Consent) ซึ่งเป็นหัวใจสำคัญของการคุ้มครองข้อมูลส่วนบุคคล

ตามกฎหมาย GDPR นั้น การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลจะต้องเป็นไปตามหลักเกณฑ์ทั้ง ๔ ข้อ ต่อไปนี้

(๔.๑) เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมอย่างเสรี (Freely given) หมายถึง เจ้าของข้อมูลมีทางเลือกในการตัดสินใจว่าจะให้หรือไม่ให้ข้อมูลส่วนใดบ้าง และการไม่ให้ความยินยอมในส่วนนั้นต้องไม่ทำให้เกิดผลเสียแก่เจ้าของข้อมูลส่วนบุคคล

(๔.๒) มีวัตถุประสงค์ที่เฉพาะเจาะจงในการขอความยินยอม (Specific) หมายถึง การประมวลผลข้อมูลต้องเป็นไปเพื่อวัตถุประสงค์ที่แจ้งเจ้าของข้อมูลส่วนบุคคลเท่านั้น

(๔.๓) แจ้งการประมวลผลข้อมูลให้เจ้าของข้อมูลส่วนบุคคลทราบ (Informed) หมายถึง เจ้าของข้อมูลส่วนบุคคลต้องทราบแล้วว่าจะมีการประมวลผลนั้น ๆ ก่อนให้ความยินยอม

(๔.๔) เจ้าของข้อมูลต้องแสดงความยินยอม**อย่างไม่กำกวม (Unambiguous)** หรือเป็นการแสดงออกโดยชัดเจน ต้องปราศจากความลังเลสงสัยในการตีความว่าเป็นการกระทำของเจ้าของข้อมูลหรือไม่ เช่น การกดอัปโหลดภาพบัตรประจำตัวประชาชน การลงลายมือชื่ออิเล็กทรอนิกส์

(๔.๕) การป้องกันข้อมูลส่วนบุคคลตั้งแต่การออกแบบ (Privacy by Design)

กฎหมาย GDPR กล่าวถึงหลักการ Privacy by Design คือ ฝ่ายผู้ควบคุมข้อมูลต้องคำนึงถึงสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลตั้งแต่ขั้นออกแบบ คงไว้ตลอดกระบวนการที่ตามมา ซึ่งสามารถประยุกต์ใช้ได้ทั้งในบริบทของการพัฒนาระบบ ผลิตภัณฑ์ บริการ แผนธุรกิจ ฯลฯ โดยเรื่อง Privacy by Design นี้มีอยู่ในกระบวนการทางวิศวกรรมบางสาขาและปฏิบัติกันมานานพอสมควรแล้ว แต่ไม่เคยมีการบัญญัติไว้เป็นกฎหมายแน่ชัดมาก่อนจนกระทั่งกฎหมาย GDPR มีผลบังคับใช้

กฎหมาย GDPR ไม่ได้กล่าวถึงหน้าที่ผู้ประมวลผลข้อมูลในหลักการ Privacy by Design อย่างแน่ชัด แต่ระบุว่าผู้ควบคุมข้อมูลต้องเลือกผู้ประมวลผลข้อมูลที่ปฏิบัติตามมาตรการทางเทคนิคและทางการจัดการองค์กรที่เหมาะสมและเพียงพอต่อการคุ้มครองความเป็นส่วนตัวของเจ้าของข้อมูล

นักพัฒนาจำนวนมากมักอ้างอิงถึงหลักการพื้นฐาน ๗ ประการ ดังนี้

(๑) กันไว้ดีกว่าแก้ (Proactive not reactive; preventative not remedial) ผู้ออกแบบต้องป้องกันมากกว่าแก้ไข คือ คาดคะเนถึงเหตุการณ์ที่ไม่พึงประสงค์และสุ่มเสี่ยงต่อความเป็นส่วนตัวของผู้ใช้ แล้วดำเนินมาตรการการป้องกันไว้ก่อนที่จะเกิดขึ้นจริง เริ่มต้นจากการตระหนักถึงคุณประโยชน์ของการปฏิบัติตามนโยบายความเป็นส่วนตัวที่เข้มข้น ยึดมั่นในการใช้มาตรการสูงสุดในการคุ้มครองความเป็นส่วนตัว

(๒) ตั้งเป็นค่าตั้งต้น (Privacy as the Default Setting) การคุ้มครองข้อมูลส่วนบุคคลจะต้องเป็นไปโดยอัตโนมัติและยังคงอยู่แม้ผู้ใช้ไม่ได้กระทำการใดเพิ่มเติม หากระบุการใช้ข้อมูลส่วนบุคคลไว้ไม่ชัดเจน จะต้องใช้มาตรการคุ้มครองขั้นสูงสุดเป็นมาตรฐานตั้งต้น

(๓) ฝังอยู่ในแม่แบบ (Privacy Embedded into Design) มาตรการความเป็นส่วนตัวจะต้องรวมอยู่ในแม่แบบและสถาปัตยกรรมอย่างกลมกลืน มิใช่เพียงอุปกรณ์เสริมในภายหลังเพื่อสอดคล้องกับกฎหมาย

(๔) ยังคงเต็มประสิทธิภาพ (Full Functionality — Positive-Sum, not Zero Sum) นอกจากความเป็นส่วนตัวที่ออกแบบจะเป็นไปตามข้อกำหนดทางกฎหมายแล้ว จะต้องไม่ลดทอนประสิทธิภาพการทำงานของระบบ ผู้ใช้ไม่ต้องเลือกสิทธิประโยชน์ประการใดประการหนึ่ง อาทิ ระหว่างความเป็นส่วนตัวกับความปลอดภัย ในขณะที่สามารถได้รับสิทธิประโยชน์ทั้งสองได้

(๕) จากต้นจรดปลาย (End-to-End Security — Lifecycle Protection) ความเป็นส่วนตัวต้องฝังตัวอยู่ในระบบ เริ่มใช้งานตั้งแต่ก่อนเก็บข้อมูล และมีผลต่อเนื่องตลอดอายุการเก็บรักษาข้อมูล เพื่อสร้างความมั่นใจว่าข้อมูลทั้งหมดได้รับการคุ้มครองและถูกทำลายทิ้งเมื่อสิ้นสุดการใช้งาน

(๖) ประจักษ์และโปร่งใส (Visibility and Transparency — Keep it Open) ผู้มีส่วนได้ส่วนเสียทุกคนจะต้องได้รับแจ้งถึงมาตรการทางธุรกิจและเทคโนโลยีที่ใช้เพื่อให้บรรลุวัตถุประสงค์ที่แจ้งไว้ และอนุญาตให้ขอตรวจสอบได้ กรรมวิธีทั้งหมดต้องโปร่งใสทั้งต่อผู้ใช้และผู้ให้บริการ

(๗) ผู้ใช้คือศูนย์กลาง (Respect for User Privacy — Keep it User-Centric) ผู้ออกแบบและผู้ให้บริการต้องให้ความสำคัญต่อความเป็นส่วนตัวของผู้ใช้เป็นสำคัญ โดยมีมาตรการ เช่น แจ้งเตือนตามความเหมาะสม และจัดสรรตัวเลือกความเป็นส่วนตัว (Privacy Option) ที่ใช้งานง่าย

๔) ตัวอย่างการดำเนินการของบริษัทสากลที่รับมือกับ GDPR[๑๔] และการศึกษาจากหน่วยงานอื่น ๆ

[๑๔] ที่มา : ETDA.OR.TH กฎหมายคุ้มครองข้อมูลส่วนบุคคล กับบริบทการคุ้มครองข้อมูลส่วนบุคคลในกฎหมายฉบับอื่นๆ

๔.๑) วิธีการรับมือ GDPR ของ Microsoft ประกอบด้วย ๔ วิธี ได้แก่

(๑) ระบุขอบเขตที่แน่ชัดของ GDPR เช่น ออก Self-Service privacy Portal สำหรับลูกค้าเพื่อขอสำเนาและลบข้อมูลส่วนบุคคลที่ใช้สำหรับบริการ Cloud สร้าง Data Inventory ข้อมูลส่วนบุคคล ใช้โครงสร้างพื้นฐานเพื่อสร้าง Data schema ให้เป็นมาตรฐาน ทำให้เป็นอัตโนมัติและบังคับใช้นโยบายความเป็นส่วนตัว ทบทวนและกำหนดมาตรฐานนโยบายการเก็บรักษาข้อมูลในธุรกิจระบบและพันธมิตร / ซัพพลายเออร์ อัปเดตเอกสารต่าง ๆ ที่เกี่ยวข้อง เช่น เอกสารทางเทคนิค สัญญาการให้บริการต่าง ๆ ให้สอดคล้องตาม GDPR และตรวจสอบข้อกำหนดความเป็นส่วนตัวของข้อมูลและการสร้างข้อกำหนดในการปฏิบัติตามกระบวนการจัดซื้อ

(๒) จัดฝึกอบรมให้กับทีมงาน สัมมนา workshop ออนไลน์ เพื่ออบรมพนักงานเจ้าหน้าที่ภายในบริษัท คู่ค้า และ ผู้ขาย จัด Train the trainer programs เพื่อเพิ่มขีดความสามารถให้กับผู้เชี่ยวชาญเฉพาะด้าน และจัดทำเอกสารรายละเอียดแนะนำการใช้งานผลิตภัณฑ์และบริการ เพื่อการปฏิบัติตาม GDPR

(๓) ปรับปรุงข้อกำหนดของกฎความเป็นส่วนตัว โดยตั้งทีมกลางที่ประกอบด้วย ผู้บริหาร เจ้าของโปรแกรมและผู้จัดการ Privacy และฝ่ายวิศวกรรม เพื่อทำ Framework ที่ครอบคลุมนโยบาย กระบวนการทางเทคนิค โครงสร้างพื้นฐานและประสบการณ์ของลูกค้า

(๔) ลงทุนกับเทคโนโลยีใหม่ สร้างระบบอัตโนมัติ เพื่อเป็นมาตรฐานให้กับข้อมูล นำไปสู่การกำกับดูแลง่ายขึ้น

ตัวอย่างการทำงาน ใช้โปรแกรม Power BI เพื่อควบคุม GDPR Workstrem Dashboard เพื่อให้การทำงานของทีมเชื่อมโยงกัน

๔.๒) วิธีการรับมือ GDPR ของ Facebook ประกอบด้วย ๒ วิธี ได้แก่

(๑) ทำงานร่วมกับผู้เชี่ยวชาญเพื่อออกแบบความเป็นส่วนบุคคลผลิตภัณฑ์ของบริษัท (Privacy by Design) โดยมีทีมงานด้านความเป็นส่วนบุคคล ที่ประกอบด้วย

ผู้เชี่ยวชาญด้านต่าง ๆ ทำงานประจำ เช่น หน่วยงานกำกับ ผู้ออกนโยบาย ผู้เชี่ยวชาญด้านความเป็นส่วนตัว และนักวิชาการจากทั่วโลก เพื่อให้ผู้เชี่ยวชาญทุกกลุ่มทราบถึงขั้นตอนการดำเนินการของบริษัท รวมถึงรับข้อเสนอแนะและนำมาพัฒนาเรื่องการปกป้องข้อมูลส่วนบุคคลตลอดจนพัฒนาการควบคุมและออกแบบความเป็นส่วนตัวตลอดเวลา โดยลงทุนศึกษาวิจัยและทำงานร่วมกับผู้เชี่ยวชาญ ตั้งผู้ออกแบบ ผู้พัฒนา ผู้เชี่ยวชาญด้านความเป็นส่วนตัว และนโยบายความเป็นส่วนตัว พัฒนาออกแบบความเป็นส่วนตัวกับผลิตภัณฑ์ของบริษัท ตั้งแต่ขั้นตอนแรกตามคำแนะนำของผู้เชี่ยวชาญด้านต่าง ๆ เช่น การปกป้องข้อมูล กฎหมายด้านความเป็นส่วนตัว การรักษาความปลอดภัย Interface Design วิศวกรรม การจัดการผลิตภัณฑ์ และนโยบายสาธารณะ โดยทีมความเป็นส่วนตัวของบริษัทได้มีการทำงานในหลากหลายมิติในทุกขั้นตอนของการพัฒนาผลิตภัณฑ์

(๒) ปรับปรุงข้อกำหนดของความเป็นส่วนตัว กำหนดหลักการของความเป็นส่วนตัว เพื่อชี้แจงให้ผู้ใช้งานได้ทราบถึงข้อกำหนดความเป็นส่วนตัวและการนำข้อมูลของผู้ใช้งานไปใช้งาน เพื่อให้ทราบว่า Facebook เข้าถึงความเป็นส่วนตัวของผู้ใช้งานอย่างไร ให้สิทธิในการควบคุมความเป็นส่วนตัวแก่ผู้ใช้งาน ออกแบบความเป็นส่วนตัวในผลิตภัณฑ์ของบริษัทตั้งแต่ขั้นตอนแรก ให้ผู้ใช้งานสามารถลบข้อมูลของตัวเองได้ มีการปรับปรุงข้อกำหนดตลอดเวลาเพื่อให้ทันสมัย สอดคล้องกับ GDPR และแสดงให้เห็นว่า มีการทำนโยบายความเป็นส่วนตัวที่เชื่อถือได้

๔.๓) วิธีการรับมือ GDPR ของ AWS (Amazon Web Service) ซึ่งปฏิบัติตามข้อกำหนดอื่น ได้แก่ EU-US Privacy Shield หลักจรรยาบรรณของ CISPE (Cloud Infrastructure Services Provider in EU) เพื่อรับรองว่า สินค้าบริการของ AWS สอดคล้องกับ GDPR และข้อปฏิบัติอื่น ๆ เช่น ISO 27017 ปลอดภัยของคลาวด์ ISO 27018 ความเป็นส่วนตัวในระบบคลาวด์ โดยขั้นตอนที่ AWS มีการ Comply ตาม GDPR มีดังนี้

ก. การระบุขอบเขต ความรับผิดชอบของผู้ให้บริการ (บริการโครงสร้างพื้นฐานระบบคลาวด์)

ข. ตรวจสอบมาตรฐานทางเทคนิค และปรับแก้ให้ทันสมัยอย่างสม่ำเสมอ

ค. การเสนอบริการให้ลูกค้า เพื่อให้สอดคล้องกับ GDPR เช่น ควบคุมการเข้าถึงของผู้ดูแลระบบ ผู้ใช้ Application ที่เข้าถึง ติดตามและบันทึกการเปลี่ยนแปลง เข้ารหัสข้อมูลบน AWS จัดให้มี Framework การปฏิบัติตามข้อกำหนดและมาตรฐานด้านความปลอดภัย เช่น ISO 27001/9001 27017/27018 C5 AWS TuV TRUST IT ระบุสิทธิของเจ้าของข้อมูล แจ้งเตือนการรั่วไหลของข้อมูล กำหนดแนวทางแจ้งหน่วยงานที่กำกับ ผู้ที่ได้รับผลกระทบ แต่งตั้งเจ้าหน้าที่ฝ่ายปกป้องข้อมูล ประเมินผลกระทบของการปกป้องข้อมูล กำหนดข้อตกลงการประมวลผลข้อมูล โดยเฉพาะการโอนข้อมูลส่วนบุคคลไปภายนอกเขตเศรษฐกิจยุโรป

๔.๔) วิธีการรับมือ GDPR ของ Google ประกอบด้วย ๖ วิธี ได้แก่

(๑) อัพเดต terms และ contractual protection ให้สอดคล้องกับกฎเกณฑ์และข้อบังคับให้เป็นปัจจุบันเพื่อให้การให้บริการ สินค้า และบริการต่าง ๆ มีความทันสมัย ผู้พิมพ์และผู้โฆษณา ต้องปฏิบัติตามหลักเกณฑ์ที่ Google กำหนด เช่นการให้ความยินยอมตาม EU User Consent Policy ของ Google และการขอความยินยอมจากผู้ใช้ EEA สำหรับการโฆษณาและการใช้ cookies บนเว็บไซต์และ Application

(๒) ทำ Client Checklist โดยกำหนดเนื้อหาที่ต้องคำนึงถึงเกี่ยวกับประเด็นสำคัญ เช่น หน่วยงานของท่านมีการรับรองความโปร่งใสของผู้ใช้งานอินเตอร์เนต (User Transparency) และการควบคุมการใช้ข้อมูลอย่างไร ท่านได้อธิบายประเภทของข้อมูลที่เก็บหรือไม่ และเก็บไปเพื่ออะไร องค์กรของท่านใช้วิธีการให้ความยินยอมที่ถูกต้อง (Right Consents) หรือไม่ (ตาม GDPR, Google EU User Consent Policy) การบันทึกการตั้งค่าของผู้ใช้ (User perference) และการให้ความยินยอม ทำเป็นระบบถูกต้องหรือไม่ และมีวิธีการแสดงให้หน่วยงานกำกับตามกฎหมาย และหุ้นส่วนของท่านเห็นได้อย่างไร ว่าท่านเป็นหน่วยงานที่น่าเชื่อถือและได้ปฏิบัติตาม GDPR

(๓) เสริมสร้างการทำ Safeguards ให้แข็งแรงมากขึ้น โดยจัดให้มีการรักษาความปลอดภัย ป้องกันความปลอดภัยของข้อมูลครอบคลุมองค์กร แต่งตั้งทีมรักษาความปลอดภัยโดยเฉพาะทีมรักษาความเป็นส่วนตัว และจัดให้มีการตรวจสอบอย่างสม่ำเสมอเป็นประจำปี โดยผู้ตรวจสอบภายนอก

(๔) มีการเตรียมความพร้อมในการรับมือกับภัยฉุกเฉิน โดยเตรียมเทคโนโลยีป้องกัน และมีโปรแกรมการจัดการตอบสนองต่อภัยคุกคามต่าง ๆ

(๕) สร้างความโปร่งใสในการใช้ข้อมูลของผู้ใช้งาน (User Transparency) โดยสร้างความโปร่งใสในการใช้ข้อมูลในสินค้าโฆษณา โดยขออนุญาตเมื่อมีการใช้ข้อมูลเพื่อการโฆษณาและแสดงความโปร่งใสแบบ real-time ผ่าน “Why This Ad” และจะแจ้งผู้ใช้งานผ่าน Google Account ว่ามีการบันทึกข้อมูลของผู้ใช้อะไรบ้าง (ผู้ใช้จะสามารถควบคุมการใช้ข้อมูลสำหรับการโฆษณาได้)

(๖) รับรองตาม Privacy Shield ระดับสากลอื่น ๆ อีก เช่น การรับรองภายใต้ EU-US และ Swiss- US Privacy shield และมาตรฐานอื่น ๆ เช่น ISO 27001 (การจัดการความปลอดภัยของข้อมูลข่าวสาร) ISO 27017 (ความปลอดภัยบนคลาวด์) ISO 27018 (ความเป็นส่วนบุคคลบนคลาวด์) SSAE16 / ISAE 3402, FedRAMP และ PCI DSS เป็นต้น

๔.๕) ศิลปะแห่งการส่งข้อความดิจิทัล : แนวทางของการสื่อสารในยุคดิจิทัล (The Art of Digital Messaging : A Guide to Communication in the Digital Age)[๑๕] เป็นคู่มือว่าด้วยกฎ กติกา มารยาทว่าด้วยการแชตสนทนาในยุคดิจิทัล มีจำนวนทั้งสิ้น ๑๐ ข้อ จัดทำในเดือนกันยายน ๒๕๖๒ โดย เดอเบรตต์ (Debrett’s) บริษัทผู้เชี่ยวชาญด้านมารยาทจากประเทศอังกฤษ ร่วมกับ เฟซบุ๊ก (Facebook) ผู้ให้บริการเครือข่ายสังคมออนไลน์ระดับโลก มีรายละเอียด ดังนี้

(๑) สื่ออารมณ์และความหมายให้ดี โทนเสียงในข้อความสามารถส่งผลต่อความหมายได้มากกว่าที่คิด ใช้ภาษาที่เป็นมิตรและเป็นกลางที่สุด หลีกเลี่ยงถ้อยคำเหน็บแนมหรือเสียดสี สัญลักษณ์ต่างๆ หรืออีโมจิน่ารักๆ ช่วยทำให้โทนของข้อความเป็นเชิงบวกได้ นอกจากนั้นยังควรเช็กข้อความก่อนเสมอ ว่าสะกดคำผิดหรือไม่ รวมถึงการใช้เครื่องมือในการแก้ไขข้อความอัตโนมัติที่อาจทำให้ความหมายบิดเบือนไป

---

๑๕ https://messengernews.fb.com/wp-content/uploads/2019/09/The-Art-of-Digital-Messaging_A-Guide-to-Communication-in-the-Digital-Age.pdf และ https://www.thairath.co.th/news/tech/howto/1700501

ผลศึกษาพบว่า ถ้าเป็นคนอเมริกัน หากเจอข้อความที่อาจสื่อถึงการเสียดสี พวกเขาจะถามตรงๆ เพราะไม่ต้องการเข้าใจผิด ขณะที่คนอังกฤษร้อยละ ๓๑ เลือกที่จะไม่สนใจและเพิกเฉยต่อข้อความประเภทนี้

(๒) กระชับเข้าไว้ แต่อย่าสั้นจนเกินไป ข้อความที่ยาวเป็นย่อหน้าอาจทำให้คนเบื่อนหน้าหนี แต่การตอบสั้นๆ 1 คำหรือส่งอีโมจิรูปเดียว อาจสื่อได้ว่าไม่สนใจ โดยเฉลี่ยแล้วความยาวของข้อความที่ส่งบน Messenger อยู่ที่ ๕ คำ

(๓) *อย่าส่งหลายข้อความติดๆกัน* เพราะอาจทำให้ผู้รับรู้สึกรำคาญและเสียสมาธิ โดยเฉพาะในการแชตกลุ่ม การส่งข้อความเยอะๆในครั้งเดียว อาจทำให้คนอื่นสับสนและตามบทสนทนาไม่ทัน โดยร้อยละ ๓๗ ของผู้ตอบแบบสอบถามทั่วโลก เห็นว่า การส่งข้อความรัว ๆ ติดๆ กันนั้น เสียมารยาท

(๔) *แคร์สักนิดก่อนคิดแชร์* ขออนุญาตเจ้าของข้อความเสมอก่อนจะส่งต่อข้อความ รูปภาพหรือเอกสารใดๆให้กับคนอื่นๆ เลี่ยงการเปิดเผยข้อมูลส่วนตัวของคนอื่น เช่น ถามเพื่อนอย่างเปิดเผยถึงวีรกรรมเมื่อไปเดตล่าสุด ซึ่งอาจทำให้เพื่อน รู้สึกว่าโดนแฉและอับอายได้ โดยเกือบครึ่งหนึ่งของผู้ร่วมตอบแบบสอบถามทั่วโลก มองว่าการส่งต่อข้อความของเพื่อนไปให้คนอื่นนั้นเป็นการเสียมารยาท

(๕) *ต้องรู้ว่ากำลังแชตอยู่กับใคร* สิ่งแรกที่ต้องทำเมื่อได้รับคำเชิญเข้าแชตกลุ่ม คือเช็กดูว่ามีใครอยู่ในกลุ่มบ้าง เพื่อจะได้ทราบว่ากลุ่มนี้สนใจบทสนทนาในเรื่องใด หลีกเลี่ยงการเล่นมุกเฉพาะกลุ่ม หรือพูดถึงเรื่องที่คนอื่นไม่เข้าใจ และควรส่งข้อความที่มีความเกี่ยวข้องกับคนส่วนใหญ่อยู่เสมอ หากต้องการพูดคุยกับใครคนใดคนหนึ่ง ควรแชตแยกออกไป โดยร้อยละ ๔๒ ของผู้ร่วมตอบแบบสอบถามทั่วโลก ชอบกลุ่มแชตที่มีสมาชิกน้อยกว่า ๖ คน

(๖) อย่าปล่อยให้รอเก้อ หากเพื่อนที่อยู่ในกลุ่มแชตส่งข้อความมาแต่ไม่มีใครตอบ ควรรีบตอบกลับ โดยอาจตอบแบบง่ายๆ เช่น กด “ถูกใจ” หรือบอกว่าคุณไม่รู้คำตอบก็ได้ การทำเช่นนี้จะช่วยกระตุ้นผู้อื่นให้ตอบกลับเช่นกัน แต่หากเป็นคนที่ถูกปล่อยให้รอเก้อเอง ต้องอย่าไปถือสา รอให้ผ่านไป ๒๔ ชั่วโมงแล้วค่อยติดตามการสนทนาโดยทักด้วยภาษาโทนสบายๆ ว่า

“แค่อยากรู้ว่าเป็นยังไงบ้างนะ...” ทั้งนี้ ผู้ร่วมตอบแบบสอบถามทั่วโลกรู้สึกไม่พอใจเป็นที่สุดเมื่อไม่มีใครตอบคำถามหรือตอบรับความคิดเห็น

(๗) *ตอบกลับให้ฉับไว* การตอบกลับข้อความในทันทีเป็นวิธีที่สุภาพ แต่ก็ไม่ใช่สิ่งที่สำคัญที่สุด หากคุณกำลังยุ่ง ทางที่ดีคืออย่าเพิ่งเปิดอ่าน หรืออีกทางเลือกคือสามารถเปิดการแจ้งเตือนแบบพุช (push) ที่ช่วยให้อ่านข้อความได้ก่อน โดยที่อีกฝ่าย ไม่รู้ว่าอ่านแล้ว และตอบกลับในเวลาที่สะดวก

(๘) เลิกนิสัยชอบเท หากต้องการหยุดความสัมพันธ์ ให้ทำอย่างเปิดเผยและนุ่มนวล อธิบายให้กระชับและสุภาพ หากกำลังคบหาหรือรู้จักอีกฝ่ายมาสักพัก ควรโทรศัพท์ไปหรือบอกต่อหน้าเมื่อพบกัน ต่อกรณีนี้ ร้อยละ ๔๗ ของผู้ร่วมตอบแบบสอบถามทั่วโลกเคยถูกเทระหว่างการสนทนา และร้อยละ ๓๙ ยอมรับว่าเคยเทคนอื่นมาแล้ว

(๙) *ฝึกลาให้ถูกธรรมเนียม* ก่อนจะออกจากกลุ่มใด ต้องวางแผนให้ดี อธิบายเหตุผลสั้นๆให้ใกล้เคียงกับความจริงที่สุดเท่าที่จะทำได้ เช่น ต้องเร่งทำงานให้ทันกำหนดส่ง เลยต้องพักมือถือ จากนั้น ก็ออกจากกลุ่มไปเลย ไม่จำเป็นต้องรอคำตอบ แต่หากคิดว่าการออกจากแชตเป็นเรื่องรุนแรงเกินไป แนะนำให้ “ปิดการแจ้งเตือน” การสนทนาแทน

(๑๐) *ทิ้งท้ายอย่างมีสไตล์* อย่าประเมินค่าของการกล่าวอำลาต่ำไปเด็ดขาด การหายไปจากบทสนทนาเฉยๆอาจสร้างความสับสนให้กับอีกฝ่าย หากจะเปลี่ยนไปทำกิจกรรมอื่น ที่ดีที่สุดคือแจ้งให้อีกฝ่ายทราบ แค่บอกว่า “เดี๋ยวมานะ” ก็ยังดี อย่างไรก็ตาม เกือบครึ่งของผู้ร่วมตอบแบบสอบถามจากทั่วโลกที่มีอายุระหว่าง ๔๕-๖๔ ปี ทิ้งท้ายการสนทนาผ่านข้อความเสมอ ขณะที่มีเพียงหนึ่งในสาม ของผู้คนอายุ ๑๘-๒๔ ปี เท่านั้น ที่รู้สึกว่าต้องกล่าวทิ้งท้าย

๔.๖) หลักการพื้นฐาน ๙ ประการ ของการใช้เทคโนโลยีอย่างเหมาะสมและมีความรับผิดชอบที่พลเมืองดิจิทัลควรตระหนัก (Nine Elements of Digital Citizenship)[๑๖] นำเสนอโดย Mike Ribble นักวิชาการด้านการศึกษาและเทคโนโลยี เขากล่าวว่า

[๑๖] สถาบันสื่อเด็กและเยาวชน. **เท่าทันสื่อ อำนาจในมือพลเมืองดิจิทัล** https://prachatai.com/classifieds/2018/08/78114

ความเป็นพลเมืองดิจิทัลเป็นเรื่องของบรรทัดฐานการใช้เทคโนโลยีอย่างมีความรับผิดชอบและเหมาะสม เขาเห็นว่าคำศัพท์ต่างๆ ไม่ว่าจะเป็น Digital Citizenship Digital Wellness หรือ Digital Ethics ล้วนเป็นเรื่องเดียวกัน นั่นคือ การปฏิบัติตนอย่างไรเมื่ออยู่ในโลกออนไลน์ และเราควรจะสอนคนรุ่นถัดไปในเรื่องนี้อย่างไร ข้อเสนอมีดังนี้

(๑) โอกาสในการเข้าถึงดิจิทัลอย่างเท่าเทียม (Digital access) เขาเสนอว่า ผู้ใช้เทคโนโลยีต้องตระหนักว่า ไม่ใช่ทุกคนที่มีโอกาสเข้าถึงเทคโนโลยี ดังนั้น การทำงานเพื่อสร้างโอกาสให้ทุกคนได้รับสิทธิทางดิจิทัลและสนับสนุนการ เข้าถึงจึงเป็นจุดเริ่มต้นของความเป็นพลเมืองดิจิทัล การเติบโตของทั้งสังคม ที่เหมาะสมจึงไม่ควรมีใครที่ถูกกีดกันการเข้าถึง ดังนั้นการเป็นพลเมือง ดิจิทัลที่ productive เราต้องสร้างหลักประกันว่า ต้องไม่มีใครถูกปฏิเสธหรือ ถูกกีดกันในการเข้าถึงดิจิทัล

(๒) การพาณิชย์ดิจิทัล (Digital Commerce) เราต้องเข้าใจว่าเศรษฐกิจ ระบบตลาดปัจจุบันได้กระทำผ่านอิเล็กทรอนิกส์ ซึ่งทั้งผู้ซื้อและผู้ขายต้อง ตระหนักว่าการซื้อสินค้าและบริการในชีวิตประจำวันเกิดขึ้นในอินเทอร์เน็ต ซึ่งหลายเรื่องอาจจะขัดแย้งกับกฎหมายหรือศีลธรรมในบางประเทศ เช่น การดาวน์โหลดสิ่งผิดกฎหมายในบางประเทศ จำพวกภาพโป๊ การพนัน เป็นต้น ดังนั้นผู้ใช้อินเทอร์เน็ตควรเรียนรู้ในการเป็นผู้บริโภคที่มีประสิทธิภาพในเศรษฐกิจดิจิทัลใหม่นี้ด้วย

(๓) การสื่อสารดิจิทัล (Digital Communication) การติดต่อสื่อสารนับเป็น การเปลี่ยนแปลงในการปฏิวัติดิจิทัลมากที่สุด หากย้อนกลับไปศตวรรษที่ ๑๙ รูปแบบการสื่อสารจำกัดกว่านี้มาก ขณะที่ศตวรรษที่ 21 ทางเลือกการสื่อสาร มีความหลากหลาย ไม่ว่าจะเป็นอีเมล มือถือ การส่งข้อความ แต่ละคน สามารถสื่อสารพูดคุยกับทุกคน ทุกที่ ทุกเวลา แต่สิ่งหนึ่งที่เขาเห็นว่า น่าเสียดายคือ ผู้ใช้เทคโนโลยีจำนวนมากไม่ได้ถูกสอนว่า การตัดสินใจที่ เหมาะสมเป็นอย่างไรเมื่อเราต้องเจอกับทางเลือกในการสื่อสารดิจิทัลที่ หลากหลายเช่นนี้

(๔) เท่าทันดิจิทัล (Digital Literacy) เป็นการจัดให้มีกระบวนการหรือขั้นตอนการสอนและการเรียนรู้เกี่ยวกับเทคโนโลยีและการใช้ เขาเห็นว่า ขั้นตอนการสอนในระดับโรงเรียนควรพิจารณาว่า เทคโนโลยีอะไรที่ควรสอนแก่นักเรียนและเทคโนโลยีแต่ละอย่างนั้นควรนำไปใช้อย่างไร ขณะที่แรงงาน บางสาขาวิชาชีพต้องการทักษะในเรื่องการค้นคว้า

และการประมวลผลข้อมูล ที่รวดเร็วฉับพลัน ขั้นตอนการเรียนรู้สำหรับพวกเขาก็ต้องมีความละเอียดอ่อน เฉพาะกลุ่ม ดังนั้นผู้เรียนควรได้รับการเรียนรู้ที่มีความเฉพาะเรื่อง เฉพาะที่ และเฉพาะเวลา อย่างในวงการธุรกิจ วงการแพทย์ หรือวงการทหาร ตัวเทคโนโลยีและการใช้ก็แตกต่างกันไป ความเป็นพลเมืองดิจิทัลจึงเป็น เรื่องของการให้การศึกษาวิธีการใหม่ ๆ กับประชาชน ซึ่งต้องการทักษะ การเท่าทันข้อมูลข่าวสารในระดับที่สูงเพียงพอต่อความเปลี่ยนแปลง

(๕) มารยาททางดิจิทัล (Digital Etiquette) เป็นมาตรฐานของแนวปฏิบัติ กว่าเราจะรับรู้ว่าพฤติกรรมหนึ่งๆ ไม่เหมาะสมในโลกดิจิทัลก็ต่อเมื่อการ กระทำนั้น ๆ เกิดขึ้นและเราได้เห็นแล้ว แต่ก่อนที่แต่ละคนจะใช้เทคโนโลยี เราไม่ได้เรียนรู้มาก่อนล่วงหน้าว่า มารยาทใดพึงหรือไม่พึงกระทำและ หลายๆ คนพบว่า ไม่ค่อยสบายใจที่จะไปต่อว่าคนอื่นเกี่ยวกับพฤติกรรมที่ ไม่เหมาะสม วิธีการที่นิยมทำกันคือ การออกกฎหรือระเบียบเพื่อควบคุมพฤติกรรมหรือไม่ก็ใช้เทคโนโลยีในการหยุดการใช้ที่ไม่เหมาะสม แต่ Mike Ribble คิดว่าการสร้างกฎหรือนโยบายไม่เพียงพอ สิ่งที่ต้องทำคือการสอน ให้ทุกคนเป็นพลเมืองดิจิทัลที่มีความรับผิดชอบในสังคมใหม่นี้

(๖) กฎหมายเกี่ยวกับดิจิทัล (Digital Law) เป็นเรื่องกฎหมายที่สัมพันธ์ กับจริยธรรมในเรื่องเทคโนโลยีของสังคมหนึ่งๆ การใช้เทคโนโลยีในรูปแบบ การขโมยหรือก่ออาชญากรรมถือเป็นการใช้ที่ผิดจริยธรรม พลเมืองดิจิทัล ควรรู้กฎกติกาและตระหนักในพฤติกรรมที่ผิดกฎหมายและผิดจริยธรรม เช่น การแฮกข้อมูลของผู้อื่น การดาวน์โหลดสื่อที่ผิดกฎหมาย การลอกเลียนแบบ โดยไม่อ้าง การปล่อยไวรัส ส่งสแปม หรือขโมยอัตลักษณ์ของคนอื่นเป็นต้น

(๗) สิทธิและความรับผิดชอบทางดิจิทัล (Digital Rights and Responsibilities) บรรดาสิทธิที่ปรากฏในรัฐธรรมนูญของสหรัฐอเมริกา เป็นชุดแนวคิดที่ขยายมาสู่พลเมืองดิจิทัลด้วยเช่นกัน พลเมืองดิจิทัลมีสิทธิ ในเรื่องความเป็นส่วนตัว เสรีภาพในการพูด เขาเสนอว่า สิทธิพื้นฐานทาง ดิจิทัลต้องได้รับการทำความเข้าใจ แลกเปลี่ยน อภิปราย และแน่นอน

ว่า สิทธิเหล่านี้มาควบคู่กับความรับผิดชอบด้วย ดังนั้นผู้ใช้จึงต้องช่วยนิยาม ว่าการใช้เทคโนโลยีอย่างเหมาะสมควรเป็นอย่างไร

(๘) สุขภาพและความเป็นอยู่ที่ดีทางดิจิทัล (Digital Health and Wellness) หมายถึง ความเป็นอยู่ทั้งทางจิตใจและร่างกายในโลกที่ใช้เทคโนโลยีดิจิทัล ด้วย ตั้งแต่ความปลอดภัยของสายตา อาการเครียดที่เกิดจากการมีพฤติกรรม ซ้ำ ๆ การปฏิบัติที่เกี่ยวข้องกับสรีระ ล้วนเป็นเรื่องที่จะต้องถูกกล่าวถึงใน โลกเทคโนโลยีใหม่นี้รวมทั้งเรื่องทางจิตวิทยา เช่น การติดเน็ต (internet addiction) ซึ่งผู้เรียนควรได้รับการสอนให้รู้ถึงโทษของเทคโนโลยีด้วย ความเป็นพลเมืองดิจิทัลจึงเป็นเรื่องที่รวมถึงวัฒนธรรมซึ่งผู้ใช้เทคโนโลยี ได้รับความรู้ในการปกป้องตนเองโดยอาจจะผ่านการศึกษาหรือการอบรม

(๙) ความปลอดภัยทางดิจิทัล (Digital Security) ในแง่ของการสร้างความปลอดภัยในโลกดิจิทัลและสังคมทั่วไปไม่ได้แตกต่างกัน ตราบใดที่เรา ต้องใส่กุญแจที่ประตู หรือตั้งสัญญาณกันขโมยเพื่อสร้างความปลอดภัย บางระดับให้กับตัวเรา ในโลกดิจิทัลก็เช่นเดียวกัน เราต้องมีระบบป้องกัน ไวรัส มีการแบ็คอัพข้อมูล หรือควบคุมการเข้าถึงอุปกรณ์เครื่องมือของเรา ดังนั้นในฐานะพลเมืองดิจิทัลที่มีความรับผิดชอบ เราต้องเรียนรู้ที่จะปกป้อง ข้อมูลข่าวสารของเราจากภายนอกซึ่งอาจนำอันตรายมาสู่เราได้

๕) สหรัฐอเมริกา[๑๗]

สหรัฐอเมริกา เป็นประเทศที่ให้ความสำคัญกับความปลอดภัยไซเบอร์มีการจัดตั้งกระทรวงความมั่นคงแห่งมาตุภูมิ (Department of Homeland Security: DHS) มีการกำหนดแผนคุ้มครองโครงสร้างพื้นฐานแห่งชาติ มีหน่วยงาน US-CERT ดูแลความปลอดภัยไซเบอร์ในประเทศ มีการจัดตั้ง CERT/CC เพื่อเป็นศูนย์ประสานงาน CSIRT/CERT ของนานาชาติจัดตั้ง CSIRT/CERT ระดับภาคส่วน (sector) เพื่อดูแลกลุ่มอุตสาหกรรมต่างๆ กระทรวงกลาโหมสหรัฐได้เตรียมการด้านสงครามไซเบอร์ ในการรับมือภัยคุกคามได้จัดทำขั้นตอนที่ละเอียด ได้แก่

[๑๗] **สรุปการศึกษาเรื่อง “ความเป็นไปได้ในการพัฒนาระบบเตือนภัยการโจมตี และแนวทางการบริหารจัดการของประเทศไทย”** ของสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ โดยสถาบันเทคโนโลยีพระจอมเกล้าคุณทหารลาดกระบัง สืบค้นจาก http://lib.nbtc.go.th/

(๑) การตรวจหาภัยคุกคาม

(๒) การวิเคราะห์เบื้องต้น และการระบุเหตุการณ์

(๓) การโต้ตอบเบื้องต้น

(๔) การวิเคราะห์ภัยคุกคาม

(๕) การโต้ตอบและการคืนสภาพ และ

(๖) การวิเคราะห์หลังเกิดเหตุการณ์

ITU (International Telecommunication Union) แห่งสหประชาชาติได้จัดอันดับในปี ๒๐๑๔ ให้สหรัฐอเมริกามีความปลอดภัยไซเบอร์เป็นอันดับ ๑ ของโลก เนื่องจากสหรัฐอเมริกามีนโยบายเสริมสร้างศักยภาพในการคุ้มครองโครงสร้างพื้นฐานวิกฤตให้แก่ภาคอุตสาหกรรม มีการจัดตั้งกระทรวงความมั่นคงแห่งมาตุภูมิ (Department of Homeland Security: DHS) ซึ่งมีภารกิจหลักในการป้องกันการโจมตีจากผู้ก่อการร้าย รวมถึงการรับผิดชอบต่อความปลอดภัยในระบบสารสนเทศ และคุ้มครองระบบสารสนเทศของระบบสาธารณูปโภค DHS มีแผนกความปลอดภัยไซเบอร์แห่งชาติ (The National Cyber Security Division: NCSD) ซึ่งมีภารกิจหลัก คือ (๑) ค้นหาวิเคราะห์และป้องกันภัยไซเบอร์ (๒) แจ้งเตือนภัยไซเบอร์และเผยแพร่ ข่าวสาร (๓) ให้ความช่วยเหลือและตอบโต้กับผู้มุ่งร้าย และ (๔) เผยแพร่วิธีการรับมือเพื่อฟื้นสภาพจากเหตุการณ์ที่เกี่ยวข้องกับภัยไซเบอร์ สหรัฐได้กำหนดแผนคุ้มครองโครงสร้างพื้นฐานแห่งชาติ (National Protection Infrastructure Plan) แผนยุทธศาสตร์แห่งชาติเพื่อรักษาความปลอดภัยไซเบอร์รวมถึงมีการรวมกลุ่มเฝ้าระวังและตอบโต้ภัยคุกคามทางคอมพิวเตอร์ (CSIRT/CERT) แผนคุ้มครองโครงสร้างพื้นฐานแห่งชาติ โดยมีวัตถุประสงค์เพื่อการรักษาความปลอดภัยไซเบอร์โครงสร้างพื้นฐานแห่งชาติประกอบด้วยระบบต่างๆ ที่มีความสำคัญและเป็นจุดที่สามารถกระทบต่อความมั่นคงของชาติ เช่น ระบบไฟฟ้า ระบบการควบคุมการบินและจราจร ระบบกำจัดขยะและของเสีย โครงข่ายโทรคมนาคม ไปจนถึงโรงไฟฟ้านิวเคลียร์ ซึ่งปัจจุบันถูกควบคุมโดยระบบคอมพิวเตอร์ทั้งหมด โดยกระทรวงความมั่นคงแห่งมาตุภูมิมีบทบาทที่สำคัญในการเป็นกระทรวงที่ดูแลความมั่นคงทางไซเบอร์ในฝ่ายพลเรือน โดยเฉพาะในภาคธุรกิจเอกชน และให้หน่วยงานรัฐที่เกี่ยวข้องร่วมมือกับภาคเอกชนเพื่อหาแนวทางในการป้องกัน และแก้ไขปัญหาความปลอดภัยของโครงสร้างพื้นฐานที่มีความสำคัญสูงต่อเศรษฐกิจ และความมั่นคงของสหรัฐและมีความเสี่ยงต่อการถูกโจมตี

สถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา (National Institute of Standards and Technology: NIST) ได้กำหนดกรอบการดำเนินงานเพื่อปรับปรุงความมั่นคงปลอดภัย ไซเบอร์เพื่อใช้ในหน่วยงานโครงสร้างพื้นฐานวิกฤต เพื่อให้เป็นแนวทางและมาตรฐาน ซึ่งครอบคลุมทั้งในระดับนโยบาย การจัดการองค์กร และเทคโนโลยีเพื่อบริหารความเสี่ยงด้านไซเบอร์ กรอบนี้ถูกกำหนดขึ้นเพื่อนำมาใช้ในการดำเนินการร่วมกันระหว่างภาครัฐและภาคเอกชน ประกอบด้วยกลุ่มงานย่อย ๕ กลุ่ม ได้แก่ ๑) กลุ่มหน้าที่งาน (functions) ประกอบด้วยกิจกรรมพื้นฐานด้านความปลอดภัยไซเบอร์ ในระดับภาพรวม จำแนกเป็น ๕ กิจกรรมย่อยได้แก่ การระบุ (identify) การป้องกัน (protect) การตรวจจับ (detect) การตอบโต้(respond) และการคืนสภาพ (recover) ๒) กลุ่มงาน (categories) เป็นกลุ่มงานที่จำแนกตามผลลัพธ์ด้านความปลอดภัยไซเบอร์ เช่น การจัดการทรัพย์สิน การควบคุมการเข้าถึง เป็นต้น ๓) กลุ่มงานย่อย (subcategories) เป็นกลุ่มงานที่จำแนกย่อยตามผลลัพธ์เฉพาะด้านในเชิงเทคนิค และ/หรือกิจกรรมที่เกี่ยวข้องในการบริหารจัดการ ๔) กลุ่มข้อมูลอ้างอิง (informative references) เป็นส่วนที่เป็นมาตรฐานแนวทางและแนวปฏิบัติที่ใช้ในกลุ่มหน่วยงานโครงสร้างพื้นฐานวิกฤตในแต่ละกลุ่ม

เพื่อรองรับนโยบายความมั่นคงปลอดภัยไซเบอร์ กระทรวงความมั่นคงแห่งมาตุภูมิของสหรัฐอเมริกา จึงได้มีการก่อตั้งคณะทำงานเพื่อดูแลระบบคอมพิวเตอร์ของสหรัฐ (United State Computer Emergency Response Team: US-CERT) เพื่อตอบโต้การโจมตีทางไซเบอร์ US-CERT หน่วยงานนี้ มีการประสานความร่วมมือกับกองทัพอย่างต่อเนื่อง มีหน้าที่รับผิดชอบในการวิเคราะห์และลดจุดอ่อนเพื่อลดช่องโหว่จากการโจมตีรวมถึงออกประกาศแจ้งเตือนภัยไซเบอร์อย่างต่อเนื่อง US-CERT มีการดำเนินงานตลอด ๒๔ ชั่วโมง ๗ วันต่อสัปดาห์ ให้ข้อมูลกับประชาชนผ่านทางเว็บไซต์บูรณาการ ความร่วมมือให้เกิดขึ้นกับทุกส่วน สนับสนุนการสืบหาภัยไซเบอร์ด้วยเทคโนโลยีที่ทันสมัย รวมถึงช่วยฟื้นสภาพระบบให้กับหน่วยงานของรัฐ

นอกจากนั้น กระทรวงกลาโหมสหรัฐอเมริกามีการจัดตั้งหน่วยงานที่รองรับภัยไซเบอร์ภายในกองทัพ มีการประสานการดำเนินงานกับหน่วยงานภายใต้กระทรวงกลาโหม กระทรวงความมั่นคงแห่งมาตุภูมิ หน่วยงาน US-CERT หน่วยงาน CERT/CC และ CSIRT/CERT อื่น ๆ กระทรวงกลาโหมสหรัฐได้ จัดทำคู่มือการรับมือกับภัยไซเบอร์ “Cyber Incident Handling Program” โดยมีวัตถุประสงค์เพื่อรักษาระดับการป้องกันภัยไซเบอร์ให้มีประสิทธิภาพสูดสุด โดยมุ่งเน้นการเพิ่มขีดความสามารถของกระทรวงกลาโหมสหรัฐในการระบุภัยคุกคาม

และการตอบโต้เหตุการณ์ที่อาจเกิดขึ้นได้อย่างทันเวลา รวมถึงเพื่อให้การดำเนินการมีความเสถียร สามารถปฏิบัติการซ้ำได้ มีคุณภาพ สามารถ วัดได้ และสามารถทำความเข้าใจได้ง่าย เป็นเอกสารที่ระบุความต้องการ และวิธีการสำหรับการสถาปนาการดำเนินงานที่มีมาตรฐาน และการดำรงไว้ซึ่งความสามารถในการรับมือกับภัยไซเบอร์ของกระทรวงกลาโหมสหรัฐอเมริกา

๖) สหพันธ์สาธารณรัฐเยอรมัน

สหพันธ์สาธารณรัฐเยอรมัน มีศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งเยอรมัน (Computer Emergency Response Team for federal agencies: CERT-Bund) มีหน้าที่รับมือภัยไซเบอร์ ได้แก่

(๑) เป็นจุดศูนย์รวมการติดต่อสำหรับการกำหนดมาตรการในการป้องกัน และการตอบโต้กับเหตุการณ์ทางไซเบอร์

(๒) ระบุช่องโหว่ในอุปกรณ์/สินค้า ทั้งฮาร์ดแวร์ และ/หรือ ซอฟต์แวร์

(๓) เสนอมาตรการเพื่อจัดการกับช่องโหว่

(๔) สนับสนุนหน่วยงานสาธารณะในการตอบโต้กับเหตุการณ์ความปลอดภัยไซเบอร์ และ

(๕) แนะนำมาตรการบรรเทาผลกระทบจากภัยไซเบอร์(www.bsi.bund.de)

โดยการให้บริการของ CERT-BUND ประกอบด้วย (๑) ให้บริการตลอด ๒๔ ชั่วโมงต่อวัน ๗ วันต่อสัปดาห์ โดยเป็นการดำเนินงานร่วมกับ IT Situation Centre (๒) วิเคราะห์เหตุการณ์ไซเบอร์ที่มีการรายงานเข้ามา (๓) จัดทำข้อเสนอแนะโดยศึกษาจากการณ์ที่เคยเกิดขึ้น (๔) ให้การสนับสนุนในช่วงที่เกิดเหตุภัยไซเบอร์ (๕) ดำเนินการในเรื่องการแจ้งเตือนและด้านสารสนเทศ และ (๖) ส่งสัญญาณเตือนไปที่ผู้บริหารรัฐในกรณีที่เกิดความเสียหายอย่างร้ายแรง และ (๗) เสนอข่าวสารการแจ้งเตือนครบถ้วนในแบบออนไลน์

๗) สหราชอาณาจักร

การรักษาความมั่นคงปลอดภัยเครือข่ายคอมพิวเตอร์ของสหราชอาณาจักร โดยมีศูนย์ป้องกันโครงสร้างพื้นฐานแห่งชาติ (Centre for the Protection of National Infrastructure: CPNI) ของสหราชอาณาจักรทำหน้าที่เป็นหน่วย Computer Emergency Response Team (CSIRT/CERT) ระดับชาติ มุ่งเน้น ดูแลโครงสร้างพื้นฐานของสหราชอาณาจักรให้ปลอดภัยจากภัยไซเบอร์ สหราชอาณาจักรได้มีการ ระบุโครงสร้างพื้นฐานวิกฤตของชาติอย่างชัดเจน โดยแบ่งออกเป็น ๙ กลุ่ม ได้แก่

(๑) การสื่อสาร

(๒) หน่วยบริการฉุกเฉิน เช่น รถพยาบาล สถานีดับเพลิง หน่วยงานชายฝั่ง และตำรวจ

(๓) พลังงาน

(๔) การบริการด้านการเงิน

(๕) อาหาร

(๖) สำนักงานคณะรัฐมนตรี

(๗) สาธารณสุข

(๘) การขนส่ง และ

(๙) กิจการเกี่ยวกับน้ำ (www.cpni.gov.uk/about/cni/)

๘) สาธารณรัฐประชาชนจีน[๑๘]

อินเตอร์เน็ตเข้ามาในประเทศจีนครั้งแรกในปี ค.ศ. ๑๙๙๔ ขณะนั้นทางการจีนคิดเพียงว่าจะใช้เพื่อประโยชน์ทางเศรษฐกิจ ครั้นเวลาผ่านไปจึงได้ตระหนักว่า อินเตอร์เน็ตมีพลังมากกว่านั้น โดยเฉพาะพลังทางการเมืองที่จะถูกขบวนการประชาธิปไตยในจีนนำมาใช้ประโยชน์ แต่อย่างไรก็ตาม ทางการจีนตระหนักถึงภัยคุกคามต่ออธิปไตยของจีนบนโลกไซเบอร์ที่ไร้พรมแดนมาตั้งแต่ ค.ศ. ๑๙๙๖ เมื่อระบบอินเทอร์เน็ตกลายมาเป็นเครื่องมือสื่อสารใหม่ที่เป็นสากลและเปิดกว้าง ปัจจุบันรัฐบาลจีนสนับสนุนการให้บริการประชาชนในรูปแบบของ

[๑๘] ที่มา : ๑. ข่าวผู้จัดการออนไลน์ เรื่อง เทคโนโลยีจดจำใบหน้าไหลบ่าท่วมจีน https://mgronline.com/china/detail/9620000117043 ๒.บทความ เรื่อง จากสงครามการค้า สู่สงครามเทคโนโลยี : สำรวจแนวรบฝั่งตะวันออก โดย ผศ.ดร.ปิติ ศรีแสงนาม ศูนย์เศรษฐกิจระหว่างประเทศ คณะเศรษฐศาสตร์ จุฬาฯ https://www.chula.ac.th/cuinside/19545/ และ ๓. บทความ เรื่อง การพัฒนาเศรษฐกิจดิจิทัลของจีน จากกรมเอเชียตะวันออก กระทรวงการต่างประเทศ http://www.eastasiawatch.in.th/th/articles/politics-and-economy/771/

E-government ซึ่งจากสถิติเมื่อเดือนมิถุนายน ค.ศ. ๒๐๑๘ ผู้ใช้บริการระบบออนไลน์ของภาครัฐมีจำนวน ๔๗๐ ล้านคน คิดเป็นสัดส่วนร้อยละ ๕๘.๖ ของผู้ใช้งานอินเทอร์เน็ต ทั่วประเทศจีน ซึ่งประชาชนเหล่านี้สามารถเข้าถึงเว็บไซต์ของหน่วยงานรัฐบาลที่มีจำนวน ๑๙,๘๖๘ เว็บไซต์ และบัญชี Weibo จำนวน ๑๓๗,๖๗๗ บัญชี โดยสรุปการพัฒนาเทคโนโลยีเพื่อป้องกันภัยทางไซเบอร์ในประเทศจีนตั้งแต่อดีตถึงปัจจุบัน ได้ดังนี้

(๑) ในปี ค.ศ. ๑๙๙๗ รัฐบาลจีนเริ่มพัฒนาโครงการ **“Golden Shield Project: GSP”** ภายใต้การกำกับดูแลของสำนัก Bureau of Public Information and Network Security Supervision เพื่อรักษาอธิปไตย (ความสามารถในการบริหารจัดการและควบคุมกิจกรรมต่าง ๆ ภายในประเทศของตน) บนโลกไซเบอร์ที่ง่ายต่อการแทรกแซงจากต่างประเทศ

(๒) ปี ค.ศ. ๑๙๙๘ รัฐบาลจีนเริ่ม**โครงการมหากำแพงไฟ (Great Firewall Project : GFP)** เพื่อควบคุมการเข้าถึงบริการต่าง ๆ บนโลกออนไลน์ของประชาชนจีนอย่างต่อเนื่อง เพื่อที่จะสกัดกั้นพลังทางการเมืองของอินเตอร์เน็ต ทำให้ประชาชนจีนที่ใช้ระบบอินเทอร์เน็ตในประเทศจีนไม่สามารถเข้าถึงแหล่งข้อมูลบางแหล่งจากต่างประเทศได้ ไม่สามารถเข้าถึง website และ application ต่าง ๆ ในต่างประเทศได้อย่างอิสระ ซึ่งรวมถึงบริการชื่อดังระดับโลก อาทิ Google, Facebook, Twitter, Wikipedia, Youtube ฯลฯ การปิดกั้นระบบเหล่านี้ภายใต้ The Great Firewall (ชื่อเล่นของ GSP ที่ตั้งล้อกับกำแพงเมืองจีน (The Great Wall)) เป็นผลให้ผู้ผลิตและผู้ให้บริการต่าง ๆ บนโลกออนไลน์ของจีนจำเป็นต้องพัฒนาระบบของตนเองขึ้นมาให้ได้ โดยสรุปในปี ค.ศ. ๒๐๐๐ จีนได้พัฒนาระบบของตนเอง ดังนี้

ระบบของต่างประเทศ	ระบบของประเทศจีน
Facebook, Amazon และ Google	Tencent, Alibaba และ Baidu
eBay	Taobao.com เป็น platform ในการทำธุรกิจแบบ C2C (Customer-to-Customer)
	ซื้อสินค้าและบริการจากภาคธุรกิจ (Business-to-Customer: B2C) ผ่าน Tmall.com

ระบบของต่างประเทศ	ระบบของประเทศจีน
	สั่งซื้อของสดออนไลน์ได้จากซูเปอร์มาร์เก็ตออนไลน์ที่มีหน้าร้านจริง (On-line to Off-line: O2O)
	สั่งร้านต้ม ทอด ปิ้ง ย่างของสดแล้วนำมาส่งถึงบ้านด้วย Hema
Agoda, Expedia, และ Traveloka	จองตั๋วเครื่องบินและที่พักด้วย Feizhu
YouTube	คลิปวิดีโอออนไลน์ ผ่าน Youku และ Tudou.com
-	เล่นเกมผ่าน 9Apps Gaming Platform
-	ฟังเพลง On-line ผ่าน Ali Music ใช้ Social Media ที่ชื่อ Weibo
-	กู้เงินออนไลน์โดยสถาบันการเงิน Ant Financial Service โดยมีเจ้าของชื่อ AliPay
-	เจ้าของร้านโชห่วยซื้อสินค้าจากบริการค้าส่ง LST.1688.com
-	ผู้บริโภคเข้าร้านสะดวกซื้อ Bailian หรือช็อปปิ้งที่ Intime Retail หรือถ้าเป็นวัยรุ่นจะเข้าร้าน Koubei ซื้อของแบรนด์เนมผ่าน Yintai Centerและจัดส่งสินค้าไปที่บ้านด้วยบริการโลจิสติกส์ Cai Niao
Web Browser : Google Chrome	Web Browser : UCBrower ภายใต้ Alibaba Group

(๓) ในปี ค.ศ. ๒๐๐๓ จีนได้พัฒนา**โครงการโล่ทองคำ (Golden Shield Project, GSP)** เป็นส่วนหนึ่งของโครงการมหากำแพงไฟ ใช้งบประมาณราว ๗๐๐ ล้านเหรียญสหรัฐ ฮาร์ดแวร์ของโครงการนี้ได้รับการสนับสนุนจากซิสโก้กับอีกหลายบริษัทในสหรัฐ ทั้งสอง

โครงการนี้ได้ทำให้รัฐบาลจีนควบคุมการใช้อินเตอร์เน็ตได้อย่างมีประสิทธิภาพ นั่นคือ สามารถสกัดกั้นทุกการสื่อสารที่ไม่พึงประสงค์ของรัฐบาลอย่างได้ผล เช่น ถ้าผู้ใช้อินเตอร์เน็ตพิมพ์คำว่า ๖๔ หรือ ๖๐๔ ที่หมายถึง เดือนมิถุนายน (หรือเดือน ๖) วันที่ ๔ ซึ่งเป็นวันที่เกิดเหตุการณ์นองเลือดที่จัตุรัสเทียนอันเหมินในปี ๑๙๘๙ แล้ว คำนี้จะไม่ปรากฏคำอธิบายใด ๆ ด้วยคำนี้จะได้ถูกบล๊อกโดยอัตโนมัติ เพราะเหตุการณ์ดังกล่าวเป็นเรื่องที่รัฐบาลจีนไม่พึงประสงค์ให้กล่าวถึง เป็นต้น

นอกจากนี้ การเข้าถึงข้อมูลข่าวสารที่มาจากโลกภายนอกก็ถือเป็นของต้องห้ามเช่นกัน ดังนั้น ชาวจีนจึงเข้าไม่ถึงทวิตเตอร์ เฟซบุ๊ก ยูทูบ และกูเกิล โดยจีนได้สร้างไป่ตู้ (Baidu) เท็นเซ็นต์ (Tencent) เหญินเหญิน (Renren) โยวคู่ (Youku) ถูโต้ว (Tudou) และซีน่า (Sina) ขึ้นมาใช้แทน ส่วนการสกัดกั้นข้อมูลข่าวสารที่ไม่พึงประสงค์นั้น รัฐบาลได้สร้างกองทัพไซเบอร์ ในปี ๒๐๐๓ รัฐบาลมีกองทัพไซเบอร์ราว ๒ ล้านคน

(๔) หลังปี ค.ศ. ๒๐๐๙ นโยบายของรัฐบาลจีน มีการเตรียมความพร้อมในเรื่องการค้าและการลดการพึ่งพาสหรัฐและตะวันตกมาอย่างต่อเนื่อง ซึ่งจีนได้รับผลกระทบจากวิกฤติเศรษฐกิจ Sub-Prime ในสหรัฐและในยุโรป ทำให้กำลังซื้อตกต่ำ โดย GDP ของจีน ร้อยละ ๘๐ ในขณะนั้นขึ้นกับการส่งออก และตลาดส่งออกที่ใหญ่ที่สุดของจีนก็คือสหรัฐและยุโรป ทำให้จีนเจอภาวะถดถอยในอัตราการขยายตัวทางเศรษฐกิจและการส่งออก จนนำไปสู่การปฏิรูปเศรษฐกิจในปี ๒๐๐๙/๒๐๑๐ ภายใต้นโยบาย New Normal เพื่อเสริมสร้างให้การบริโภคภายในประเทศกลายเป็นพลังหลักในการขับเคลื่อนเศรษฐกิจ

เพื่อสร้างการบริโภคภายในประเทศดังกล่าว จีนเน้นการทำ ๒ เรื่อง คือ ๑) ทำให้คนจีนรวยขึ้น ซึ่งทำมาอย่างต่อเนื่องตั้งแต่ปี ๒๐๐๙ และ ๒) ทำให้คนจีนที่รวยขึ้นนั้นบริโภคภายในประเทศ ซึ่งจะเกิดการบริโภคภายใน ก็ต่อเมื่อ เห็นว่าสินค้าจากจีนเป็นสินค้าคุณภาพสูง ทำให้เกิดนโยบาย Made in China ๒๐๒๕ เพื่อยกระดับ ล้างภาพลักษณ์ของสินค้าจีนที่เคยถูกมองว่าเป็นสินค้าคุณภาพต่ำ เป็นสินค้าปลอม ให้สินค้าจีนกลายเป็นสินค้าคุณภาพสูงให้ได้สำเร็จในปี ๒๐๒๕

(๕) **นโยบาย Made in China ๒๐๒๕** หรือปี ๒๕๖๘ โดยดำเนินการผ่านการสนับสนุนการลงทุนจากต่างประเทศ โดยทางการจีนให้สิทธิพิเศษทางการลงทุนในเงื่อนไขที่ดีที่สุดกับบริษัทต่างชาติที่เข้ามาลงทุนโดยทำตามนโยบายของจีนที่ต้องการการพัฒนาคนและการถ่ายทอดเทคโนโลยีให้กับจีน นวัตกรรมใหม่ๆ หลายๆ อย่างเกิดขึ้นในจีนที่จับตาจับใจ

ผู้บริโภคอย่างยิ่ง อาทิ โทรศัพท์มือถือหัวเว่ย P30Pro ที่ Zoom ได้ ๕๐ เท่า ด้วยอุปกรณ์ของ Sony (ญี่ปุ่น) ผนวกกับเทคโนโลยีของ Laica (เยอรมัน) และในปัจจุบันสินค้าแบรนด์เนม สินค้าคุณภาพสูงจำนวนมากผลิตจากประเทศจีน

(๖) **กระทรวงสารสนเทศและเทคโนโลยีแห่งจีนออกกฎให้ผู้ใช้โทรศัพท์มือถือต้องสแกนใบหน้าเมื่อลงทะเบียนหมายเลขโทรศัพท์ เรียกว่า ระบบการจดจำใบหน้า (Facial Recognition)** โดยมีผลบังคับใช้ในวันที่ ๑ ธันวาคม ๒๕๖๒ เพื่อลดคดีฉ้อฉลในด้านโทรคมนาคม และการหลอกลวงเกี่ยวกับโทรศัพท์ ป้องกันการขายต่อซิมการ์ด และป้องกันมิจฉาชีพลงทะเบียนในเครือข่ายโทรศัพท์มือถือ กรณีที่มีบัตรประชาชนถูกขโมย ตามสถานที่สาธารณะเริ่มทยอยติดตั้งกล้องวงจรปิดเทคโนโลยีจดจำใบหน้าเพื่อการต่าง ๆ เช่น การจับขโมยนักล้วงกระเป๋า การขโมยกระดาษชำระในห้องน้ำ โดยมีการเปิดเผยว่า จำนวนกล้องวงจรปิดที่ใช้ในจีน มีราว ๒๐๐ ล้านตัว และกำลังจะเพิ่มมากขึ้นถึง ๖๒๖ ล้านตัว รวมทั้งมหาวิทยาลัยหลายแห่งในประเทศจีน แจ้งว่า การใช้ระบบจดจำใบหน้ามาเช็คชื่อผู้เข้าเรียนช่วยให้อัตราการเข้าห้องเรียนของนักศึกษาสูงขึ้น

แต่อย่างไรก็ตาม ระบบการจดจำใบหน้าได้รับการต่อต้านจากประชาชน โดยเมื่อเดือนพฤศจิกายน ๒๕๖๒ นาย กัว ปิง รองศาสตราจารย์ด้านกฎหมายประจำ*มหาวิทยาลัยเจ้อเจียง ไฮ-เทค (Zhejiang Sci-tech University)* ได้ยื่นฟ้องร้องสวนสัตว์ซาฟารีเมืองหังโจวในข้อกล่าวหาผิดสัญญาโดยเปลี่ยนระบบยืนยันอัตลักษณ์ของผู้ผ่านประตูเข้าชมสวนสัตว์จากระบบสแกนลายนิ้วมือมาเป็นระบบสแกนใบหน้าหลังจากที่เขาได้ซื้อตั๋วปีเข้าชมสวนสัตว์ไปเมื่อเดือนเมษายน ซึ่งตอนนั้นสวนสัตว์ได้ใช้ระบบผ่านประตู โดยการสแกนลายนิ้วมือ กัวปฏิเสธให้ข้อมูลแก่สวนสัตว์เพื่อนำไปเข้าระบบใหม่ เพราะเชื่อว่าการเปลี่ยนระบบรับเข้าสวนสัตว์นี้เป็นการละเมิดสิทธิผู้บริโภค “วัตถุประสงค์การยื่นฟ้อง ไม่ได้ต้องการค่าชดเชย แต่ต้องการต่อสู้การละเมิดโดยระบบจดจำใบหน้า”

อาจารย์ด้านกฎหมาย เหลา ตงเหยียน ประจำมหาวิทยาลัยชิงหัว ชี้ว่า ข้อมูลใบหน้าไม่เหมือนกับข้อมูลชีวภาพอื่น ๆ อย่างเช่นลายนิ้วมือหรือดีเอ็นเอ ซึ่งต้องได้รับการยินยอมจากเจ้าตัวก่อนที่จะทำการขอจัดเก็บ ส่วนข้อมูลใบหน้านั้นคุณสามารถได้มาโดยที่เจ้าตัวของไม่รู้หรือยินยอม

“เมื่อเราอยู่บนถนน ใบหน้าของเราถูกสแกนหลายร้อยครั้งในแต่ละวันจากทุก ๆ มุม แต่ไม่มีใครบอกคุณเลยว่าข้อมูลใบหน้าของคุณได้ถูกจัดเก็บเข้าระบบไปแล้ว ข้อมูลใบหน้านี้อาจถูกขายให้กับนักการตลาดซึ่งเป็นบุคคลที่สาม และหากข้อมูลนี้รั่วไหลออกไป ความเสียหายที่เกิดขึ้นนั้นจะไม่อาจกู้คืนมาได้เลยเนื่องจากมันไม่อาจเปลี่ยนแปลงอะไรได้แล้ว มันเป็นความเสี่ยงที่ไม่อาจจินตนาการ หากพวกมิจฉาชีพได้ข้อมูลใบหน้าของคุณไป บัญชีการเงินของคุณจะถูกแฮ็คไปได้ง่าย ๆ หรือใบหน้าของคุณอาจถูกตัดต่อนำไปใช้ในวิดีโอลามกอนาจาร”

ยักษ์ใหญ่แอพพลิเคชั่นชำระเงินออนไลน์ อย่าง *WeChat Pay* และ *Alipay* ให้ผู้ใช้ชำระเงินด้วยการสแกนใบหน้า ณ จุดจำหน่ายสินค้าที่มีกล้องติดตั้งไว้ และจากรายการสืบสวนของ *The Beijing News* เผยแพร่ในต้นปีนี้ เผยว่ามี Platform มากมายผุดขึ้นมาเป็นเสมือนกับตลาดที่ให้ประชาชนขายบริการสลับเปลี่ยนใบหน้าของเหล่าเซเลปหรือบุคคลสาธารณะที่มีชื่อเสียงกับภาพของพวกดาวโป๊ในราคาไม่ถึง๑ ดอลลาร์สหรัฐ หรือแค่ราว ๓๐ - ๓๑ บาท

จาง เย่ ซุ่ย โฆษก*สภาผู้แทนประชาชนจีน (National People’s Congress)* หรือรัฐสภาเผยในการพิจารณากฎหมายเมื่อเดือนเมษายน ๒๕๖๒ ว่าสภาผู้แทนได้พิจารณาร่างกฎหมายใหม่ ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล แต่มิได้เผยว่าจะเสร็จสิ้นหรือจะผ่านการรับรองเมื่อไหร่ เนื่องจากจีนยังขาดกฎหมายดูแลคุ้มครองเทคโนโลยีใหม่ ๆ ซึ่งทำให้กลุ่มบริษัทยักษ์ใหญ่เข้าถึงข้อมูลส่วนบุคคลของปัจเจกชนจำนวนมหาศาล ซึ่งกลุ่มผู้สังเกตการณ์ในอุตสาหกรรม กล่าวว่า ข้อเสนอกฎหมายดังกล่าวจะเป็นก้าวสำคัญในการปกป้องข้อมูลส่วนบุคคลพลเมืองโดยเฉพาะข้อมูลทางชีวภาพ (biometric data) อย่างเช่นลายนิ้วมือ และข้อมูลใบหน้า

๙) สาธารณรัฐเกาหลี[๑๙]

เกาหลีใต้ประกาศความพร้อมให้บริการเทคโนโลยี 5G ในโทรศัพท์เคลื่อนที่สู่สาธารณะเป็นประเทศแรกในโลกเมื่อวันที่ ๓ เมษายน ๒๕๖๒ ซึ่งมีความเร็วกว่า 4G ถึง ๒๐ เท่า

---

[๑๙] **ที่มา :** ๑. บทความจากสำนักข่าว Voice of America ประเทศไทย https://www.voathai.com/a/south-korea-launches-5g-networks-early-to-secure-world-first-/4865634.html ๒. ข่าวเกาหลีใต้ผ่านร่างกฎหมายจัดตั้งศูนย์ป้องกันการก่อการร้ายทางโลกไซเบอร์ ๒๕๕๘ สำนักข่าวรัฐสภา และ ๓. บทความ เรื่อง5G กับโอกาสและความท้าทายสู่สังคมเกาหลีใต้ โดย เสกสรร อานันทศิริเกียรติ https://themomentum.co/5g-in-south-korea-and-concern-about-cyber-security/?fbclid=IwAR0uZjRnybJJPXq6CDVwvCdDYDmGSvYQKVk3uV1sLoRPNg2i3Hh79qEh4iE

โดยมีผู้ใช้เฉลี่ย ๑๗,๐๐๐ คนต่อวัน ทั้งนี้ เกาหลีใต้ให้ความสำคัญในการเป็นรัฐบาลที่มุ่งรับใช้ประชาชน โดยใช้เทคโนโลยีมาปรับปรุงบริการภาครัฐเป็นระบบออนไลน์ ทำให้เกาหลีใต้มีผู้ใช้อินเทอร์เน็ตสูงที่สุดในโลก ทั้งนี้เป็นผลจากการพัฒนาเมื่อ ๒๐ ปีที่แล้ว

ในเดือนพฤษภาคม ๒๐๑๗ เมื่อมุน แจ อิน รับตำแหน่งประธานาธิบดีได้ประกาศแผนงานการขับเคลื่อนสู่การปฏิวัติอุตสาหกรรมครั้งที่ ๔ (Fourth Industrial Revolution) และแต่งตั้งคณะกรรมการพิเศษของประธานาธิบดี (Presidential Committee on the Fourth Industrial Revolution: PCFIR) เพื่อให้การขับเคลื่อนการปฏิวัติอุตสาหกรรมครั้งที่ ๔ มีประสิทธิภาพมากขึ้น โดยมีองค์ประกอบของคณะกรรมการฯ ได้แก่ รัฐมนตรี ๕ กระทรวงหลักด้านเศรษฐกิจและอุตสาหกรรม นักวิชาการ และผู้แทนองค์กรธุรกิจชั้นนำด้านเทคโนโลยีสารสนเทศ ซึ่งคณะกรรมการฯ มีบทบาทหลักในการประสานนโยบายระหว่างหน่วยงานที่เกี่ยวข้องในกำกับของคณะกรรมการ การจัดกิจกรรมรณรงค์สร้างความตระหนักรู้สาธารณะ การปฏิรูปกฎหมาย และการสร้างสภาพแวดล้อมที่เอื้อต่อการพัฒนาอุตสาหกรรมใหม่

คณะกรรมการพิเศษได้เสนอแนะแนวทางปรับปรุงแก้ไขกฎหมายสำคัญให้สอดรับกับแผนงานนี้ อาทิ สนับสนุนให้แก้ไขกฎหมายจราจรโดยรับรองสถานะผู้ขับขี่ของยานยนต์อัตโนมัติ แก้ไขเพิ่มเติมบทบัญญัติเกี่ยวกับการควบคุมอากาศยานไร้คนขับ (Drone) ที่อนุญาตให้ออกบินในเวลากลางคืนและออกบินพ้นทัศนวิสัยของผู้ควบคุมได้ ปรับปรุงกฎหมายที่เกี่ยวข้องกับการเดินเรือทั้งหมดเพื่อให้เรือโดยสารอัตโนมัติสามารถปฏิบัติการได้ภายในปี ๒๐๒๒ และทบทวนกฎหมายสาธารณูปโภคไฟฟ้าเพื่อเปิดช่องให้ผู้บริโภคพิจารณาระบบโครงข่ายไฟฟ้าอัจฉริยะ (Smart Grid) ในฐานะทางเลือกหนึ่งของพลังงานไฟฟ้าในครัวเรือนได้

แต่อย่างไรก็ตาม ความทันสมัยทางเทคโนโลยีของเกาหลีใต้ยังเสี่ยงต่อภัยคุกคามสมาชิกรัฐสภาจากพรรคฝ่ายรัฐบาลของเกาหลีใต้ ได้เสนอกฎหมายการจัดตั้งศูนย์ป้องกันการก่อการร้ายทางโลกไซเบอร์ เพื่อป้องกันภัยคุกคามจากอาชญากรคอมพิวเตอร์ เนื่องจากเกาหลีใต้เป็นประเทศหนึ่งที่ได้รับผลกระทบจากภัยคุกคามดังกล่าวอย่างต่อเนื่อง จากสถิติตั้งแต่เดือนกรกฎาคม ๒๕๕๒ ระบบคอมพิวเตอร์ของหน่วยงานสำคัญของรัฐบาลถูกโจมตีแบบ DDoS (Distribute Denial of Service) ทำให้คอมพิวเตอร์ หยุดการทำงานทั้งระบบ เดือนมิถุนายน ๒๕๕๔ ระบบคอมพิวเตอร์ของสหกรณ์การเกษตรและสำนักข่าวหลายแห่งถูกไวรัสทำลายเสียหาย

และเกิดขึ้นอีกหลายครั้งในปีต่อ ๆ มา โดยมีข้อมูลพิสูจน์ชัดเจนว่า การก่ออาชญากรรมดังกล่าวส่วนหนึ่งเป็นการกระทำจากฝ่ายเกาหลีเหนือ ทำให้เว็บไซต์และระบบคอมพิวเตอร์ในเกาหลีใต้ได้รับความเสียหายอย่างหนัก โดยมีเป้าหมายในการโจมตีที่สำคัญ คือ หน่วยงานสำคัญของรัฐบาล ซึ่งตลอดระยะเวลา ๕ ปี ที่ผ่านมาตั้งแต่ปี ๒๕๕๓ ถึงปี ๒๕๕๗ เกิดอาชญากรรมคอมพิวเตอร์ประมาณ ๗๖,๐๐๐ ครั้ง

ประเทศเกาหลีใต้เพิ่มโอกาสเสี่ยงที่จะถูกโจมตีได้โดยง่าย ที่ผ่านมามีเหตุการณ์ถูกโจมตีค่อนข้างมาก (รายงานประจำปี ไทยเซิร์ต ๒๐๑๒, หน้า ๒๔) รัฐบาลเกาหลีใต้จึงจัดทำกรอบความมั่นคงปลอดภัยไซเบอร์ของประเทศ เกาหลีใต้เพื่อรับมือกับภัยคุกคามที่เพิ่มขึ้นและรุนแรงขึ้น ซึ่งประกอบด้วยคณะกรรมการกำหนด กรอบการดำเนินงาน และกฎหมายที่เกี่ยวข้อง โดยมีหน่วยงานต่างๆ เป็นผู้ปฏิบัติ รายละเอียด โครงสร้างกรอบความมั่นคงปลอดภัยไซเบอร์ของประเทศเกาหลีใต้ เกาหลีใต้มีศูนย์ปฏิบัติการด้านการรักษาความปลอดภัยข้อมูลคอมพิวเตอร์แห่งชาติ (KoreaInformation Security Agency: KISA) ก่อตั้งขึ้นในปี ๑๙๙๖ มีวัตถุประสงค์เพื่อควบคุมดูแล ระบบความปลอดภัยของข้อมูลคอมพิวเตอร์ในระดับประเทศ เป็นหน่วยงานที่อยู่ภายใต้การดูแลของกระทรวงสารสนเทศและการสื่อสาร (Ministry of Information and Communication: MIC) ของประเทศเกาหลีใต้ KISA มีหน่วยงานลูก คือ KISC (Korea Internet Security Center) หรือ KrCERT (Korea Computer Emergency Response Team / Coordination Center) ซึ่งมีหน้าที่และการให้บริการต่าง ๆ อาทิ

(๑) วิจัยพัฒนาและวางแผนด้านความปลอดภัยข้อมูล สารสนเทศ การเฝ้าระวังดูแลความปลอดภัยเครือข่ายอินเทอร์เน็ตของประเทศ

(๒) เป็นศูนย์ประสานงานกับหน่วยงานในต่างประเทศ เช่น ประสานงานด้านการวิจัยช่องโหว่ของความปลอดภัยข้อมูลสารสนเทศกับบริษัทชั้นนำ เช่น ไมโครซอฟท์ และซีสโก เป็นต้น

(๓) เป็นผู้ออกใบรับรองอิเล็กทรอนิกส์ของเว็บไซต์ (Root Certification Authority: ROOT CA) ของประเทศ ให้การรับรอง (Accredit) แก่หน่วยงานที่ได้รับการรับรอง (Certification Authority: CA) ในประเทศ และหน่วยงานในต่างประเทศ (Cross Certification CA)

(๔) ให้บริการตรวจสอบระดับความปลอดภัยของหน่วยงานต่าง ๆ (Security Health Check)

(๕) ฝึกอบรมเพื่อสร้างความตระหนักด้านความปลอดภัยไซเบอร์ให้แก่หน่วยงานต่างๆ เพื่อให้สามารถป้องกันตนเองได้ในระดับหนึ่ง ตลอดจนจัดทำหนังสือเกี่ยวกับการรักษาความปลอดภัยข้อมูล และจัดงานสัมมนาด้านความปลอดภัยไซเบอร์อย่างต่อเนื่อง

๑๐) ญี่ปุ่น

ในภูมิภาคเอเชียแปซิฟิกมีการจัดตั้ง APCERT (Asia Pacific Computer Emergency Response Team) โดย JPCERT/CC ของญี่ปุ่นเป็นแกนนำเพื่อสร้างเครือข่ายการรักษาความปลอดภัยไซเบอร์ในภูมิภาค ประกอบด้วย CSIRT/CERT จำนวน ๒๗ หน่วย จาก ๒๐ ประเทศ และมีบริษัทชั้นนำด้านไอทีให้การสนับสนุน ITU ได้จัดอันดับในปี ๒๐๑๔ ให้มาเลเซียและออสเตรเลียมีความปลอดภัยไซเบอร์เป็นอันดับ ๑ ของภูมิภาคนี้ (เป็นอันดับ ๓ ของโลก) ญี่ปุ่นและเกาหลีใต้เป็นอันดับ ๓ สิงคโปร์อันดับ ๔ อินโดนีเซียอันดับ ๕ ส่วนประเทศไทยอยู่อันดับ ๗ ประเทศ ญี่ปุ่นเป็นแกนนำและเป็นพี่เลี้ยงในการให้ความช่วยเหลือในการจัดตั้งกลุ่ม CSIRT/CERT แก่ชาติ ต่างๆ ส่วนเกาหลีใต้มีการจัดตั้งศูนย์ปฏิบัติการด้านการรักษาความปลอดภัยข้อมูลคอมพิวเตอร์ แห่งชาติ (Korea Information Security Agency: KISA) และมี KISC (Korea Internet Security Center) หรือ KrCERT ทำหน้าที่ดูแลด้านการเฝ้าระวังดูแลความปลอดภัยไซเบอร์ เป็นผู้ออกใบรับรองอิเล็กทรอนิกส์ของเว็บไซต์ (ROOT CA) ของประเทศ เป็นหน่วยงานแห่งแรกของเอเชียที่เข้าเป็นสมาชิก FIRST

๑๑) สิงคโปร์

สิงคโปร์ได้รับความยอมรับเป็นอย่างมากในอาเซียน โดย SingCERT จัดการฝึกซ้อมรับมือภัยไซเบอร์ให้กับอาเซียนอย่างต่อเนื่อง สิงคโปร์มีบุคลากรที่พร้อม และได้รับการรับรองจาก CISSP และ GIAC เป็นจำนวนมาก ประเทศสิงคโปร์มีศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่ง สิงคโปร์(SingCERT) เป็นผู้เฝ้าระวังและดูแลความปลอดภัยไซเบอร์ เริ่มก่อตั้งเมื่อเดือนตุลาคม ปี ๑๙๙๗ โดยหน่วยงาน Infocomm Development Authority of Singapore (IDA) ซึ่งได้รับความร่วมมือจาก Centre for Internet Research, National University of Singapore (NUS) หน่วยงาน SingCert มีเป้าหมายการดำเนินงานดังนี้

(๑) ประกาศแจ้งเตือนภัยไซเบอร์ ให้คำปรึกษา และเป็นผู้ดูแลด้านความปลอดภัยไซเบอร์

(๒) สร้างความตระหนักด้านความปลอดภัยไซเบอร์ผ่านการสัมมนา การประชุมเชิงปฏิบัติการและการฝึกด้านความปลอดภัยไซเบอร์และ

(๓) ประสานงานกับหน่วยงาน CSIRT/CERT อื่น ๆ หรือผู้ประกอบการอื่น ๆ เพื่อตอบโต้ภัยไซเบอร์หน่วยงาน

SingCERT ได้เข้าเป็นสมาชิก FIRST ตั้งแต่ปี ๑๙๙๘ เพื่อปรับปรุงความปลอดภัยทางคอมพิวเตอร์ในระดับโลก SingCERT ยังเป็นแกนนำในการสนับสนุนและการประสานงานระหว่าง CSIRT/CERT ของประเทศในกลุ่มอาเซียน มีบทบาทสำคัญในการจัดการฝึกซ้อมรับมือภัยไซเบอร์ (ASEAN CERT Incident Drill: ACID) ให้แก่หน่วยงาน CSIRT/CERT ของประเทศในอาเซียน การฝึกนี้ช่วยเสริมความแข็งแกร่งในการดำเนินงานให้แก่หน่วยงาน CSIRT/CERT รวมถึงเป็นการทดสอบขั้นตอนและความพร้อมในการรับมือของประเทศสมาชิกอาเซียน

๑๒) สหพันธรัฐมาเลเซีย

รัฐบาลของมาเลเซียให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยไซเบอร์โดยกำหนดแนวทางการรักษาความปลอดภัยที่ค่อนข้างครอบคลุม มีการตรวจสอบความมั่นคงของชาติมุ่งเน้นการรักษาความปลอดภัยไซเบอร์และดูแลช่องโหว่ที่อาจจะกระทบต่อความมั่นคงของประเทศและความปลอดภัยของประชาชน รัฐบาลให้การสนับสนุนด้านเทคนิคและพัฒนาบุคลากรทางด้านความปลอดภัยไซเบอร์ รวมถึงดำเนินการวิกฤตการณ์ต่าง ๆ เช่น การบริการฉุกเฉินทางด้านการรักษาความปลอดภัยไซเบอร์ โดยมีคณะกรรมการความปลอดภัยไซเบอร์แห่งชาติ (Malaysian National Security Council) เป็นคณะกรรมการบริหารสูงสุด มีการปรับปรุงนโยบายความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Policy: NCSP) ซึ่งประกาศใช้เมื่อปี ๒๐๐๗ เพื่อให้ทันต่อเหตุการณ์ภัยคุกคามทางคอมพิวเตอร์และเครือข่าย สำหรับกรอบความมั่นคงปลอดภัยไซเบอร์ของประเทศมาเลเซีย

นอกจากนั้น เมื่อวันที่ ๒๔ มกราคม ๒๐๑๕ รัฐบาลมาเลเซียได้จัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งมาเลเซีย (Malaysia

Computer Emergency Response Team: MyCERT) ในเดือนมีนาคม ปี ๑๙๙๗ หน่วยงาน MyCERT เป็นหน่วยงานที่อยู่ภายใต้ศูนย์ความปลอดภัยและการตอบโต้ฉุกเฉินด้านการสื่อสารและสารสนเทศแห่งชาติ (National ICT Security & Emergency Response Centre: NISER) ซึ่งต่อมาในปี ๒๐๐๗ ได้ถูกเปลี่ยนชื่อเป็นศูนย์ความปลอดภัยไซเบอร์แห่งมาเลเซีย (CyberSecurity Malaysia) เป็นหน่วยงานที่ไม่หวังผลกำไร อยู่ภายใต้กระทรวงวิทยาศาสตร์ เทคโนโลยีและนวัตกรรม (Minister of Science, Technology and Innovation: MOSTI) ของมาเลเซีย

พันธกิจหลักของ MyCERT ได้แก่ การจัดการด้านการรักษาความปลอดภัยทาง คอมพิวเตอร์และผู้ใช้อินเทอร์เน็ต มีวิสัยทัศน์ที่จะลดโอกาสการเป็นเป้าการถูกโจมตีทางไซเบอร์ และลดความเสี่ยงของผลกระทบที่จะตามมา หน่วยงาน MyCERT มีเป้าหมายที่จะสร้างความปลอดภัยไซเบอร์ให้แก่ผู้ใช้เครือข่ายอินเทอร์เน็ตของมาเลเซีย ลดโอกาสในการถูกโจมตี รวมถึงลดความเสี่ยงของผลเสียหายที่ตามมา หน่วยงาน MyCERT ให้ความช่วยเหลือในการรับมือกับเหตุการณ์ เช่น การบุกรุกทางไซเบอร์ การระบุตัวตนของผู้กระทำความผิด ระบุชนิดของมัลแวร์ซึ่งสร้างความเสียหายทางไซเบอร์ และระบุเหตุการณ์อื่นๆ ที่เกี่ยวข้องกับความปลอดภัยทาง คอมพิวเตอร์ หน่วยงาน MyCERT ดำเนินการวิจัยและพัฒนาแนวทางการตอบโต้ภัยคุกคามทางไซเบอร์ภายใต้ศูนย์วิจัย Cybersecurity Malaysia Malware Research Centre

ที่ผ่านมา MyCERT มีการพัฒนาเครื่องมือสำหรับจัดการกับมัลแวร์บางชนิด และมีการประสานงานร่วมกับผู้บังคับใช้กฎหมาย เช่น สำนักงานตำรวจแห่งชาติมาเลเซีย (Royal Malaysian Police: RMP) คณะกรรมการด้านความมั่นคง (Securities Commission) ธนาคารต่างๆ เช่น Bank Negara Malaysia และสถาบันการเงินอื่น ๆ หน่วยงาน MyCERT มีการดำเนินงานอย่างใกล้ชิดกับ CERT/CC ของสหรัฐ รวมถึงมีการประสานการดำเนินงานร่วมกับหน่วยงาน และองค์กรในต่างประเทศ เช่น Asia Pacific Computer emergency Response Team (APCERT), Organization of the Islamic Conference-Computer-Emergency Response Team (OIC-CERT), The Honeynet Project, Forum for Incident Response and Security Teams (FIRST), The Anti-Phishing Working Group (APWG), หน่วยงานที่ดูแลด้านความปลอดภัยทางคอมพิวเตอร์ทั่วโลก (CSIRT/CERT) รวมถึงผู้ให้บริการอินเทอร์เน็ต (Internet

Service Provider: ISP) หน่วยงาน MyCERT ได้กำหนดระดับความสำคัญของภัยคุกคามแต่ละชนิด และระยะเวลาในการแก้ปัญหาเพื่อให้ผู้รับบริการทราบ อย่างไรก็ตาม ระยะเวลาที่ใช้จริงอาจจะมากกว่าหรือน้อยกว่าที่ระบุไว้ ทั้งนี้ขึ้นกับขนาดและความซับซ้อนของแต่ละเหตุการณ์ที่เกิดขึ้น

๒. ข้อมูลความเคลื่อนไหว/การปรับตัวของรัฐบาลและหน่วยงานต่าง ๆ ในประเทศไทย เพื่อรับมือกับสถานการณ์ Disruption

ประเทศไทยมีกฎหมายที่เกี่ยวข้องกับการรักษาความปลอดภัยทางเทคโนโลยี ๓ ฉบับ ได้แก่ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ โดยสรุปสาระสำคัญได้ดังนี้

๑) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐[๒๐] กำหนดความผิดเกี่ยวกับคอมพิวเตอร์ โดยครอบคลุมการกระทำผิดของบุคคลเกี่ยวกับคอมพิวเตอร์ เช่น

มาตรา ๕ ผู้เข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท

มาตรา ๖ ผู้ที่ล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ และนำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่จะน่าเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๗ ผู้เข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

[๒๐] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ฉบับเต็มสืบค้นได้ที่ www.ratchakitcha.soc.go.th

มาตรา ๘ ผู้กระทำการโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้เป็นประโยชน์ได้ ต้องระวางโทษจำคุกไม่เกินสามปีหรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๙ ผู้ทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปีหรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๐ ผู้กระทำการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ ต้องระวางโทษจำคุกไม่เกินห้าปีหรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๑ ผู้ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

เป็นต้น

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐[๒๑] กำหนดการกระทำความผิดต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศหรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ และความผิดอื่น ๆ ที่เกี่ยวข้อง เช่น

มาตรา ๕ เป็นการยกเลิกความในมาตรา ๑๒ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๑๒ ถ้าการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ หรือมาตรา ๑๑ เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของ

[๒๑] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ ฉบับเต็มสืบค้นได้ที่ www.ratchakitcha.soc.go.th

ประเทศหรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงเจ็ดปี และปรับตั้งแต่สองหมื่นบาทถึงหนึ่งแสนสี่หมื่นบาท

ถ้าการกระทำความผิดตามวรรคหนึ่งเป็นเหตุให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ตามวรรคหนึ่ง ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงสิบปี และปรับตั้งแต่สองหมื่นบาทถึงสองแสนบาท

ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐ เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ตามวรรคหนึ่ง ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

ถ้าการกระทำความผิดตามวรรคหนึ่งหรือวรรคสามโดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่ห้าปีถึงยี่สิบปี และปรับตั้งแต่หนึ่งแสนบาทถึงสี่แสนบาท”

นอกจากนั้น ในมาตราอื่น ๆ ได้กำหนดการกระทำความผิดเกี่ยวกับทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอม เท็จ น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน หรือมีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้ หรือมีภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการอิเล็กทรอนิกส์หรือวิธีการอื่นใด โดยประการที่น่าจะทำให้ผู้นั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย เป็นต้น

๒) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒[๒๒] กำหนดการคุ้มครองข้อมูลส่วนบุคคล การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยมีคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ประธานกรรมการมาจากการสรรหาและแต่งตั้งจากผู้มีความรู้ ความเชี่ยวชาญและประสบการณ์ต่าง ๆ โดยมีปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นรองประธานกรรมการ กรรมการโดยตำแหน่ง จำนวนห้าคน ได้แก่ ปลัดสำนักนายกรัฐมนตรี เลขาธิการ

[๒๒] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ฉบับเต็มสืบค้นได้ที่ www.ratchakitcha.soc.go.th

คณะกรรมการกฤษฎีกา เลขาธิการคณะกรรมการคุ้มครองผู้บริโภค อธิบดีกรมคุ้มครองสิทธิและเสรีภาพและอัยการสูงสุด และกรรมการผู้ทรงคุณวุฒิ จำนวนเก้าคน ซึ่งมาจากการสรรหาและแต่งตั้งผู้มีความรู้ ความเชี่ยวชาญและประสบการณ์ด้านต่าง ๆ และมีการคุ้มครองข้อมูลส่วนบุคคล เช่น

มาตรา ๑๙ ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น เว้นแต่บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้

...

มาตรา ๒๒ การเก็บรวบรวมข้อมูลส่วนบุคคล ให้เก็บรวบรวมได้เท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

...

มาตรา ๒๗ ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้น ไม่ต้องขอความยินยอมตามมาตรา ๒๔ หรือมาตรา ๒๖

...

มาตรา ๓๐ เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอม

...

เป็นต้น

๓) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒[๒๓] กำหนดมาตรการหรือการดำเนินการเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคง

[๒๓] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ฉบับเต็มสืบค้นได้ที่ www.ratchakitcha.soc.go.th

ทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ โดยให้มีคณะกรรมการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ หรือ กมช. มีชื่อภาษาอังกฤษว่า National Cyber Security Committee หรือ NCSC โดยมีนายกรัฐมนตรี เป็นประธานกรรมการ และมีคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ หรือ กกม. ดำเนินการตามหน้าที่และอำนาจของคณะกรรมการ กมช. โดยมีรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานกรรมการ และมีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ รับผิดชอบงานธุรการ งานวิชาการ งานประชุม และงานเลขานุการของคณะกรรมการ และ กกม. โดยมีหน้าที่และอำนาจต่าง ๆ อาทิ

(๑) เฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตาม วิเคราะห์ และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

(๒) ปฏิบัติการ ประสานงาน สนับสนุน และให้ความช่วยเหลือหน่วยงานที่เกี่ยวข้องในการปฏิบัติตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์หรือตามคำสั่งของคณะกรรมการ

นอกจากนั้น สถานการณ์ความปลอดภัยทางไซเบอร์ของประเทศไทย จากดัชนีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของไทย เมื่อเปรียบเทียบกับต่างประเทศนั้น ในปี ๒๕๖๐ สหภาพโทรคมนาคมระหว่างประเทศ (ITU) ได้ทำการสำรวจระดับความเอาจริงเอาจัง (Commitment) ด้านความมั่นคงปลอดภัยไซเบอร์ของแต่ละประเทศ โดยพิจารณาจากมาตรการ ๕ ด้าน ได้แก่ ด้านกฎหมาย (Legal) ด้านเทคนิค (Technical) ด้านหน่วยงาน/นโยบาย (Organizational) ด้านการพัฒนาศักยภาพ (Capacity building) และด้านความร่วมมือ (Cooperation) พบว่า Global Cybersecurity Index (GCI) ของประเทศไทยอยู่ในอันดับที่ ๒๒ จาก ๑๙๔ ประเทศ ขณะเดียวกัน เมื่อเปรียบเทียบกับประเทศสมาชิกในกลุ่มอาเซียนแล้ว ประเทศไทยอยู่อันดับที่ ๓ รองจากสิงคโปร์ และมาเลเซีย ซึ่งกระทรวงและหน่วยงานที่เกี่ยวข้องจะช่วยกันขับเคลื่อนให้ไทยติดใน ๒๐ อันดับแรกของประเทศที่มีความพร้อม

สำหรับยุทธศาสตร์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ โดยคณะกรรมการ**การรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ**[๒๔] ได้กำหนดแผนงานระยะเร่งด่วน ๖ เดือน / ๑ ปี และ ๒ ปี ที่หน่วยงานจะร่วมกันทำต่อไปใน ๘ ด้าน ที่สอดคล้องกับแผนยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๖๐ – ๒๕๖๔ คือ

(๙) การปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (Critical Information Infrastructure Protection: CIIP)

(๑๐) การสร้างศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์ (Emergency Readiness)

(๑๑) การบูรณาการการจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศ (Cybersecurity Governance)

(๑๒) การประสานความร่วมมือระหว่างภาครัฐและเอกชนเพื่อความมั่นคงปลอดภัยไซเบอร์ (Public-Private Partnership)

(๑๓) การสร้างความตระหนักและรอบรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Capacity Building)

(๑๔) การพัฒนากฎหมาย ระเบียบและมาตรฐานเพื่อความมั่นคงปลอดภัยไซเบอร์ (Law, Regulation and Standard)

(๑๕) การประสานความร่วมมือระหว่างประเทศเพื่อความมั่นคงปลอดภัยไซเบอร์ (International Cooperation)

(๑๖) การวิจัยและพัฒนาเพื่อความมั่นคงปลอดภัยไซเบอร์ (Research & Development)

คณะกรรมการ**การรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ** ได้เห็นชอบการจัดกลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (Critical Information Infrastructure: CII) ๖ กลุ่มแรก ได้แก่ กลุ่มความมั่นคงและบริการภาครัฐ กลุ่มการเงิน กลุ่ม

---

[๒๔] **ข่าวประชาสัมพันธ์ EDTA สพธอ. เรื่อง** นายกฯ ประธานการประชุม คกก.เตรียมการไซเบอร์แห่งชาติครั้งแรก DE รับลูก พร้อมตั้งเป้าดันไทยติดอันดับ 1 ใน 20 ของโลกที่มีความพร้อม อ่านฉบับเต็มได้ที่ https://www.etda.or.th/content/thailand-national-cyber-security-preparedness-committee-meeting-1-2561.html

เทคโนโลยีสารสนเทศและโทรคมนาคม กลุ่มการขนส่งและโลจิสติกส์ กลุ่มพลังงานและสาธารณูปโภค และกลุ่มสาธารณสุข พร้อมยกระดับแผนการทำงานร่วมกัน เช่น ซ้อมรับมือภัยคุกคามทางไซเบอร์ รวมถึงจัดทำแผนปฏิบัติการรับมือไซเบอร์ (National Incident Handling Flow)

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) หรือ **ETDA กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม** เป็นเจ้าภาพหลักในการดำเนินงานจัดตั้ง**ศูนย์ความร่วมมืออาเซียน-ญี่ปุ่น เพื่อพัฒนาบุคลากรความมั่นคงปลอดภัยไซเบอร์** หรือ **ASEAN-Japan Cybersecurity Capacity Building Centre** ตามมติที่ประชุม TELMIN-Japan หรือการประชุมรัฐมนตรีอาเซียนด้านโทรคมนาคมและเทคโนโลยีสารสนเทศร่วมกับประเทศญี่ปุ่นที่ประเทศกัมพูชา และได้รับการสนับสนุนจากประเทศญี่ปุ่นทั้งด้านงบประมาณและองค์ความรู้สำหรับฝึกอบรมให้แก่ประเทศสมาชิกอาเซียนเพื่อความมั่นคงปลอดภัยไซเบอร์ ยกระดับขีดความสามารถของบุคลากร และปรับปรุงอันดับ ITU GCI ให้สูงขึ้นต่อไป

นอกจากนี้ จากการศึกษาพบว่า ประเทศไทย ยังมีความจำเป็นในการดำเนินโครงการเร่งรัดการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์กว่า ๑,๐๐๐ คน ที่ผ่านการรับรองจากหน่วยงาน CII ภาครัฐ-เอกชน และสถาบันการศึกษา

๔) โครงการพัฒนาทักษะและการเป็นพลเมืองดิจิทัล (Digital Citizenship)

จัดทำโดย สำนักงานส่งเสริมเศรษฐกิจดิจิทัล กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ร่วมกับบริษัท กูเกิล (ประเทศไทย) จำกัด เพื่อเผยแพร่ความรู้ที่เกี่ยวข้องกับชุดทักษะและความรู้การรักษาความปลอดภัย สิทธิและความรับผิดชอบ รวมไปถึงโอกาสและความท้าทายแห่งยุคสมัย อันเป็นเครื่องมือสำคัญในการก้าวเข้าสู่พลเมืองดิจิทัลที่สมบูรณ์

พลเมืองดิจิทัล (Digital Citizenship)[๒๕] คือ พลเมืองผู้ใช้งานสื่อดิจิทัลและสื่อสังคมออนไลน์ที่เข้าใจบรรทัดฐานของการปฏิบัติตัวให้เหมาะสมและมีความรับผิดชอบในการใช้เทคโนโลยี โดยเฉพาะอย่างยิ่ง การสื่อสารในยุคดิจิทัลเป็นการสื่อสารที่ไร้พรมแดน สมาชิกของโลกออนไลน์คือ ทุกคนที่ใช้เครือข่ายอินเทอร์เน็ตบนโลกใบนี้ ผู้ใช้สื่อสังคมออนไลน์มีความหลากหลายทางเชื้อชาติ อายุ ภาษา และวัฒนธรรม พลเมืองดิจิทัลจึงต้องเป็นพลเมืองที่มีความรับผิดชอบ

[๒๕] สรานนท์ อินทนนท์. ความฉลาดทางดิจิทัล. http://cclickthailand.com/contents/general/dq3.pdf

มีจริยธรรม เห็นอกเห็นใจและเคารพผู้อื่น มีส่วนร่วมและมุ่งเน้นความเป็นธรรมในสังคม การเป็นพลเมืองในยุคดิจิทัลนั้น มีความฉลาดทางดิจิทัล (DQ: Digital Intelligence Quotient) หรือทักษะที่สำคัญ ๘ ประการ วรพจน์ วงศ์กิจรุ่งเรือง (๒๕๖๑)[๒๖] นิยามความเป็นพลเมืองดิจิทัลออกเป็น ๓ มิติ คือ

(๑) มิติด้านความรู้เกี่ยวกับสื่อและสารสนเทศ พลเมืองดิจิทัลต้องมีความรู้ความสามารถในการเข้าถึง ใช้ สร้างสรรค์ ประเมิน สังเคราะห์ และสื่อสารข้อมูลข่าวสารผ่านเครื่องมือดิจิทัล ดังนั้นพลเมืองยุคใหม่จึงต้องมีความรู้ด้านเทคนิคในการเข้าถึงและใช้เครื่องมือดิจิทัล เช่น คอมพิวเตอร์ สมาร์ตโฟน แท็บเล็ต ได้อย่างเชี่ยวชาญ รวมถึงทักษะในการรู้คิดขั้นสูง เช่น ทักษะการคิดอย่างมีวิจารณญาณ ซึ่งจำเป็นต่อการเลือก จัดประเภท วิเคราะห์ ตีความและเข้าใจข้อมูลข่าวสาร

(๒) มิติด้านจริยธรรม พลเมืองดิจิทัลจะใช้อินเทอร์เน็ตได้อย่างปลอดภัย มีความรับผิดชอบ และมีจริยธรรมได้อย่างไร พลเมืองที่ดีจะต้องรู้จักคุณค่าและจริยธรรมจากการใช้เทคโนโลยี ต้องตระหนักถึงผลพวงทางสังคม การเมือง เศรษฐกิจ และวัฒนธรรมที่เกิดจากการใช้อินเทอร์เน็ต รวมถึงรู้จักสิทธิและความรับผิดชอบออนไลน์ อาทิ เสรีภาพในการพูด การเคารพทรัพย์สินทางปัญญาของผู้อื่น และการปกป้องตนเองและชุมชนจากความเสี่ยงออนไลน์ เช่น การกลั่นแกล้งออนไลน์ ภาพลามกอนาจารเด็ก สแปม เป็นต้น

(๓) มิติด้านการมีส่วนร่วมทางการเมืองและสังคม พลเมืองดิจิทัลต้องรู้จักใช้ศักยภาพของอินเทอร์เน็ตในการมีส่วนร่วมทางการเมือง เศรษฐกิจ และสังคม อินเทอร์เน็ตเป็นได้ทั้งเครื่องมือเพิ่มการมีส่วนร่วมทางการเมืองในระบบ เช่น รัฐบาลใช้อินเทอร์เน็ตในการรับฟังความเห็นของประชาชนก่อนออกกฎหมาย การลงคะแนนเสียงอิเล็กทรอนิกส์ (e-Voting) หรือการยื่นคำร้องออนไลน์ (online petition) นอกจากนั้น อินเทอร์เน็ตยังใช้ส่งเสริมการเมืองภาคพลเมืองผ่านวิธีการใหม่ๆ ซึ่งท้าทายให้เกิดการเปลี่ยนแปลงการเมืองในระดับโครงสร้าง

โดยสรุป การจะเป็นพลเมืองดิจิทัลที่ดีจะต้องมีชุดทักษะและความรู้ทั้งในเชิงเทคโนโลยีและการคิดขั้นสูง หรือที่เรียกว่า “ความรู้ดิจิทัล” (digital literacy) เพื่อใช้ประโยชน์จากข้อมูลข่าวสารในโลกไซเบอร์ รู้จักป้องกันตนเองจากความเสี่ยงต่าง ๆ ในโลกออนไลน์ เข้าใจถึงสิทธิ

---

[๒๖] วรพจน์ วงศ์กิจรุ่งเรือง. ***คู่มือพลเมืองดิจิทัล.*** เผยแพร่ครั้งแรก : มิถุนายน ๒๕๖๑ https://thaidigizen.com/wp-content/uploads/2018/06/DigitalCitizenship-Book-ok.pdf

ความรับผิดชอบ และจริยธรรมที่สำคัญในยุคดิจิทัล และใช้ประโยชน์จากอินเทอร์เน็ตในการมีส่วนร่วมทางการเมือง เศรษฐกิจ และสังคม-วัฒนธรรม ทั้งเพื่อตนเอง ชุมชน ประเทศ และโลก

ความฉลาดทางดิจิทัล (DQ: Digital Intelligence Quotient) คือ กลุ่มความสามารถทางสังคม อารมณ์ และการรับรู้ ที่จะทำให้คนคนหนึ่งสามารถเผชิญกับความท้าทายของชีวิตดิจิทัล และสามารถปรับตัวให้เข้ากับชีวิตดิจิทัลได้ ความฉลาดทางดิจิทัลครอบคลุมทั้งความรู้ ทักษะ ทัศนคติและค่านิยม ที่จำเป็นต่อการใช้ชีวิตในฐานะสมาชิกของโลกออนไลน์ กล่าวอีกนัยหนึ่ง คือ ทักษะการใช้สื่อและการเข้าสังคมในโลกออนไลน์

ความฉลาดทางดิจิทัล เป็นผลจากศึกษาและพัฒนาของ DQ institute หน่วยงานที่เกิดจากความ ร่วมมือกันของภาครัฐและเอกชนทั่วโลกประสานงานร่วมกับ เวิลด์อีโคโนมิกฟอรั่ม (World Economic Forum) ที่มุ่งมั่นให้เด็กๆ ทุกประเทศได้รับการศึกษาด้านทักษะพลเมืองดิจิทัลที่มีคุณภาพและใช้ชีวิต บนโลกออนไลน์อย่างปลอดภัยด้วยความก้าวหน้าของเทคโนโลยีสมัยใหม่ อย่างไรก็ตาม ระดับทักษะ ความฉลาดทางดิจิทัลของเด็กไทยตามรายงาน DQ report 2018 ยังอยู่ในระดับต่ำอยู่ ทั้งนี้เนื่องจาก สำนักงานส่งเสริมเศรษฐกิจดิจิทัล (ดีป้า) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน (สพฐ.) กระทรวงศึกษาธิการ และ DQ Institue ร่วมกันทำโครงการ EveryChild โดยศึกษาเด็กไทยอายุ ๘ - ๑๒ ปี ทั่วประเทศ ๑,๓๐๐ คน ผ่านแบบสำรวจออนไลน์ DQ Screen Time Test ชุดเดียวกันกับเด็กประเทศอื่น ๆ รวมกลุ่มตัวอย่างทั่วโลกทั้งสิ้น ๓๗,๙๖๗ คน ผลการศึกษาพบว่า เด็กไทยมีความเสี่ยงจากภัยออนไลน์ถึง ๖๐% ในขณะที่ค่าเฉลี่ยของการศึกษา ครั้งนี้อยู่ที่ ๕๖% (จาก ๒๙ ประเทศทั่วโลก) ภัยออนไลน์ที่พบจากการศึกษาชุดนี้ประกอบไปด้วย การกลั่นแกล้งบนโลกออนไลน์, ถูกล่อลวงออกไปพบคนแปลกหน้าจากสื่อสังคมออนไลน์, ปัญหา การเล่นเกม เด็กติดเกม, ปัญหาการเข้าถึงสื่อลามกอนาจาร, ดาวน์โหลดภาพหรือวิดีโอที่ยั่วยุอารมณ์เพศ และพูดคุยเรื่องเพศกับคนแปลกหน้าในโลกออนไลน์ ดังนั้น ทักษะความฉลาดทางดิจิทัล จึงควรถูกนำมาใช้ในการพัฒนาคุณภาพและความสามารถของเยาวชนไทย

ความฉลาดทางดิจิทัล (DQ: Digital Intelligence Quotient) หรือทักษะที่สำคัญ ๘ ประการ ของการเป็นพลเมืองดิจิทัล มีรายละเอียดดังนี้

๑. ทักษะในการรักษาอัตลักษณ์ที่ดีของตนเอง (Digital Citizen Identity) สามารถสร้างและบริหารจัดการอัตลักษณ์ที่ดีของตนเองไว้ได้อย่างดีทั้งในโลกออนไลน์และโลกความจริง อัตลักษณ์ที่ดีคือ การที่ผู้ใช้สื่อดิจิทัลสร้างภาพลักษณ์ในโลกออนไลน์ของตนเองในแง่บวกทั้งความคิด ความรู้สึก และการกระทำ โดยมีวิจารณญานในการรับส่งข่าวสารและแสดงความคิดเห็น มีความเห็นอกเห็นใจผู้ร่วมใช้งานในสังคมออนไลน์ และรู้จักรับผิดชอบต่อการกระทำไม่กระทำการที่ผิดกฎหมาย และจริยธรรมในโลกออนไลน์ เช่น การละเมิดลิขสิทธิ์ การกลั่นแกล้งหรือการใช้วาจาที่สร้างความเกลียดชังผู้อื่นทางสื่อออนไลน์

๒. ทักษะในการคิดวิเคราะห์มีวิจารณญาณที่ดี (Critical Thinking) สามารถในการวิเคราะห์แยกแยะระหว่างข้อมูลที่ถูกต้องและข้อมูลที่ผิด ข้อมูลที่มีเนื้อหาเป็นประโยชน์และข้อมูลที่เข้าข่ายอันตราย ข้อมูลติดต่อทางออนไลน์ที่น่าตั้งข้อสงสัยและน่าเชื่อถือได้ เมื่อใช้อินเทอร์เน็ต จะรู้ว่าเนื้อหาอะไร เป็นสาระ มีประโยชน์ รู้เท่าทันสื่อและสารสนเทศ สามารถ

วิเคราะห์และประเมินข้อมูลจากแหล่งข้อมูลที่หลากหลายได้ เข้าใจรูปแบบการหลอกลวงต่าง ๆ ในโลกไซเบอร์ เช่น ข่าวปลอม เว็บปลอม ภาพตัดต่อ เป็นต้น

การคิดวิเคราะห์มีวิจารณญาณที่ดีมีองค์ประกอบดังนี้

(๑) ความรู้ สามารถอธิบายและจดจำข้อมูลได้

(๒) ความเข้าใจ สามารถจัดระเบียบ และเลือกข้อเท็จจริงและความคิดออกมาใช้ได้

(๓) การประยุกต์ สามารถนำข้อเท็จจริงและกฎข้อบังคับ มาสร้างความคิดใหม่ ๆ ได้

(๔) การวิเคราะห์ สามารถแยกความคิดและเรื่องต่าง ๆ ออกมาเป็นข้อย่อย ๆ ได้

(๕) การสังเคราะห์ สามารถนำความคิดย่อย ๆ มารวมเป็นแนวคิดใหญ่ ๆ ได้

(๖)การประเมิน สามารถพัฒนาความคิดเห็น และจัดลำดับความสำคัญได้

(๓)ทักษะในการรักษาความปลอดภัยของตนเองในโลกออนไลน์ (Cybersecurity Management) สามารถป้องกันข้อมูลด้วยการสร้างระบบความปลอดภัยที่เข้มแข็ง และป้องกันการโจรกรรมข้อมูลหรือการโจมตีออนไลน์ได้ มีทักษะในการรักษาความปลอดภัยของตนเองในโลกออนไลน์ การรักษาความปลอดภัยของตนเองในโลกไซเบอร์คือการปกป้องอุปกรณ์ดิจิทัลข้อมูลที่จัดเก็บและข้อมูลส่วนตัวไม่ให้เสียหาย สูญหาย หรือถูกโจรกรรมจากผู้ไม่หวังดีในโลกไซเบอร์ การรักษาความปลอดภัยทางดิจิทัลมีความสำคัญดังนี้

(๑)เพื่อรักษาความเป็นส่วนตัวและความลับ หากไม่ได้รักษาความปลอดภัยให้กับอุปกรณ์ดิจิทัล ข้อมูลส่วนตัวและข้อมูลที่เป็นความลับอาจจะรั่วไหลหรือถูกโจรกรรมได้

(๒)เพื่อป้องกันการขโมยอัตลักษณ์ การขโมยอัตลักษณ์เริ่มมีจำนวนที่มากขึ้นในยุคข้อมูลข่าวสาร เนื่องจากมีการทำธุรกรรมทางออนไลน์มากยิ่งขึ้น ผู้คนเริ่มทำการชำระค่าสินค้าผ่านสื่ออินเทอร์เน็ต และทำธุรกรรมกับธนาคารทางออนไลน์ หากไม่มีการรักษาความปลอดภัยที่เพียงพอ มิจฉาชีพอาจจะล้วงข้อมูลเกี่ยวกับบัตรเครดิตและข้อมูลส่วนตัวของผู้ใช้งานไปสวมรอยทำธุรกรรมได้ เช่น ไปซื้อสินค้า กู้ยืมเงิน หรือสวมรอยรับผลประโยชน์และสวัสดิการ

(๓)เพื่อป้องกันการโจรกรรมข้อมูล เนื่องจากข้อมูลต่างๆ มักเก็บรักษาในรูปของดิจิทัล ไม่ว่าจะเป็นเอกสารภาพถ่าย หรือคลิปวีดิโอ ข้อมูลเหล่านี้อาจจะถูกโจรกรรมเพื่อนำไปขายต่อ แบล็คเมล์ หรือเรียกค่าไถ่

(๔)เพื่อป้องกันความเสียหายของข้อมูลและอุปกรณ์ ภัยคุกคามทางไซเบอร์อาจส่งผลเสียต่อข้อมูลและอุปกรณ์ดิจิทัลได้ ผู้ไม่หวังดีบางรายอาจมุ่งหวังให้เกิดอันตรายต่อข้อมูลและอุปกรณ์ที่เก็บรักษามากกว่าที่จะโจรกรรมข้อมูลนั้น ภัยคุกคามอย่างไวรัสคอมพิวเตอร์ โทรจัน และมัลแวร์ สร้างความเสียหายร้ายแรงให้กับคอมพิวเตอร์หรือระบบปฏิบัติการได้

๔. ทักษะในการรักษาข้อมูลส่วนตัว (Privacy Management) มีดุลพินิจในการบริหารจัดการข้อมูลส่วนตัว รู้จักปกป้องข้อมูลความส่วนตัวในโลกออนไลน์โดยเฉพาะการแชร์ข้อมูลออนไลน์เพื่อป้องกันความเป็นส่วนตัวทั้งของตนเองและผู้อื่น รู้เท่าทันภัยคุกคามทางอินเทอร์เน็ต เช่น มัลแวร์ ไวรัสคอมพิวเตอร์ และกลลวงทางไซเบอร์

(๑) ไม่ควรตั้งรหัสผ่านของบัญชีใช้งานที่ง่ายเกินไป

(๒) ตั้งรหัสผ่านหน้าจอสมาร์ทโฟนอยู่เสมอ

(๓) แชร์ข้อมูลส่วนตัวในสื่อโซเชียลมีเดียอย่างระมัดระวัง

(๔) ใส่ใจกับการตั้งค่าความเป็นส่วนตัว ระมัดระวังในการเปิดเผยชื่อและที่ตั้งของเรา และปฏิเสธแอปที่พยายามจะเข้าถึงข้อมูลส่วนตัวของเรา

(๕) อย่าใช้ไวไฟสาธารณะเมื่อต้องกรอกข้อมูลส่วนตัว เช่น ออนไลน์ชอปปิ้ง หรือธุรกรรมธนาคาร หรือการลงทะเบียนในสื่อสังคมออนไลน์

(๖)รู้เท่าทันภัยคุกคามทางอินเทอร์เน็ต

๕. ทักษะในการจัดสรรเวลาหน้าจอ (Screen Time Management) สามารถในการบริหารเวลาที่ใช้อุปกรณ์ยุคดิจิทัล รวมไปถึงการควบคุมเพื่อให้เกิดสมดุลระหว่างโลกออนไลน์ และโลกภายนอก ตระหนักถึงอันตรายจากการใช้เวลาหน้าจอนานเกินไป การทำงานหลายอย่างในเวลาเดียวกัน และผลเสียของการเสพติดสื่อดิจิทัล

๖. ทักษะในการบริหารจัดการข้อมูลที่ผู้ใช้งานทิ้งไว้บนโลกออนไลน์ (Digital Footprints) สามารถเข้าใจธรรมชาติของการใช้ชีวิตในโลกดิจิทัลว่าจะหลงเหลือร่อยรอยข้อมูลทิ้งไว้เสมอ รวมไปถึงเข้าใจผลลัพธ์ที่อาจเกิดขึ้น เพื่อการดูแลสิ่งเหล่านี้อย่างมีความรับผิดชอบ

รอยเท้าดิจิทัล (Digital Footprints) คือ คำที่ใช้เรียกร่องรอยการกระทำต่าง ๆ ที่ผู้ใช้งานทิ้งรอยเอาไว้ในโลกออนไลน์ โซเชียลมีเดีย เว็บไซต์หรือโปรแกรมสนทนา เช่นเดียวกับรอยเท้าของคนเดินทาง ข้อมูลดิจิทัล เช่น การลงทะเบียน อีเมล การโพสต์ข้อความหรือรูปภาพ เมื่อถูกส่งเข้าโลกไซเบอร์แล้วจะทิ้งร่อยรอยข้อมูลส่วนตัวของผู้ใช้งานไว้ให้ผู้อื่นติดตามได้เสมอ แม้ผู้ใช้งานจะลบไปแล้ว ดังนั้น หากเป็นการกระทำที่ผิดกฎหมายหรือศีลธรรม ก็อาจมีผลกระทบต่อชื่อเสียงและภาพลักษณ์ของผู้กระทำ

๗. ทักษะในการรับมือกับการกลั่นแกล้งบนโลกไซเบอร์ (Cyberbullying Management) การกลั่นแกล้งบนโลกไซเบอร์คือ การใช้อินเทอร์เน็ตเป็นเครื่องมือหรือช่องทางเพื่อก่อให้เกิดการคุกคาม ล่อลวงและการกลั่นแกล้งบนโลกอินเทอร์เน็ตและสื่อสังคมออนไลน์ โดยกลุ่มเป้าหมายมักจะเป็นกลุ่มเด็กจนถึงเด็กวัยรุ่น การกลั่นแกล้งบนโลกไซเบอร์คล้ายกันกับการกลั่นแกล้งในรูปแบบอื่น หากแต่การกลั่นแกล้งประเภทนี้จะกระทำผ่านสื่อออนไลน์หรือสื่อดิจิทัล เช่น การส่งข้อความทางโทรศัพท์ ผู้กลั่นแกล้งอาจจะเป็นเพื่อนร่วมชั้น คนรู้จักในสื่อสังคมออนไลน์ หรืออาจจะเป็นคนแปลกหน้าก็ได้ แต่ส่วนใหญ่ผู้ที่กระทำจะรู้จักผู้ที่ถูกกลั่นแกล้ง รูปแบบของการกลั่นแกล้งมักจะเป็น

(๑) การว่าร้าย ใส่ความขู่ทำร้าย หรือใช้ถ้อยคำหยาบคาย

(๒) การคุกคามทางเพศผ่านสื่อออนไลน์

(๓) การแอบอ้างตัวตนของผู้อื่น

(๔) การแบล็กเมล์

(๕) การหลอกลวง

(๖) การสร้างกลุ่มในโซเชียลเพื่อโจมตีโดยเฉพาะ

๘. ทักษะในการใช้เทคโนโลยีอย่างมีจริยธรรม (Digital Empathy) มีความเห็นอกเห็นใจ และสร้างความสัมพันธ์ที่ดีกับผู้อื่นบนโลกออนไลน์ แม้จะเป็นการสื่อสารที่ไม่ได้เห็นหน้ากัน มีปฏิสัมพันธ์อันดีต่อคนรอบข้าง ไม่ว่าพ่อแม่ ครู เพื่อนทั้งในโลกออนไลน์และในชีวิตจริง ไม่ด่วนตัดสินผู้อื่นจากข้อมูลออนไลน์แต่เพียงอย่างเดียว และจะเป็นกระบอกเสียงให้ผู้ที่ต้องการความช่วยเหลือ

๕) การขับเคลื่อนโครงการเพื่อการพัฒนาความรู้เท่าทันสื่อและดิจิทัล สำหรับเด็กและเยาวชนในต่างประเทศ และแนวทางสำหรับประเทศไทย จากกรณีศึกษาในต่างประเทศจำนวน ๖ กรณีศึกษา จาก ๖ ประเทศ คือ สหรัฐอเมริกา แคนาดา สหภาพยุโรป อินเดีย ออสเตรเลีย และญี่ปุ่น โดย วรัชญ์ ครุจิต ซึ่งเผยแพร่ผลการวิจัยในเดือนมีนาคม ๒๕๖๑ พบ ๕ ประเด็นที่สามารถประยุกต์ใช้กับแนวทางการขับเคลื่อนเพื่อพัฒนาความรู้เท่าทันสื่อและดิจิทัลสำหรับเด็กและเยาวชนในประเทศไทย คือ

(๑) การได้รับการสนับสนุนและการมีส่วนรวมจากภาคส่วนต่าง ๆ ที่เกี่ยวข้อง

(๒) การออกแบบเนื้อหาที่มีประเด็นชัดเจน และสอดคล้องกับปัญหาสำคัญของประเทศ

(๓) การสร้างองค์ความรู้และการวิจัยทางความรู้เท่าทันสื่อ หรือมีองค์กรที่มีความรู้สนับสนุน

(๔) การถ่ายทอดความรู้ เพื่อให้กลุ่มเป้าหมายลงมือทำกิจกรรมการผลิตสื่อโดยมีผู้เชี่ยวชาญเป็นพี่เลี้ยง

(๕) ความต่อเนื่องความทันสมัย และความหลากหลาย ของการสร้างสื่อและทำกิจกรรม

ผู้วิจัยได้พัฒนาโมเดล 3E4I ในการขับเคลื่อนโครงการเพื่อพัฒนาความรู้เท่าทันสื่อและดิจิทัลเพื่อเด็กและเยาวชนที่มีประสิทธิภาพ โดยจะต้องมีองค์ประกอบด้านการดำเนินการ ๓ ข้อ ที่เรียกว่า 3E คือ Education การถ่ายทอดองค์ความรู้ที่ถูกต้องและเหมาะสมกับวัย Experience: การลงมือปฏิบัติเปลี่ยนองค์ความรู้นั้นเป็นชิ้นงาน และ Expert การมีผู้เชี่ยวชาญเป็นพี่เลี้ยงคอยแนะนำ ส่วนองค์ประกอบด้านการส่งเสริมความเข้มแข็งของการขับเคลื่อน ๔ องค์ประกอบ ที่เรียกว่า 4I คือ Interconnectedness ความสามารถเชื่อมโยงโครงการการขับเคลื่อนไปกับภาคส่วนอื่น ๆ ที่ให้การสนับสนุน Information การสร้างข้อมูลความรู้ หรือมีหน่วยงานสนับสนุนความรู้ที่จำเป็นและมีประโยชน์ต่อการขับเคลื่อน Integration การบูรณาการประเด็นการขับเคลื่อนความรู้เท่าทันสื่อให้สอดคล้องกับปัญหาที่สำคัญของประเทศ และ In Trend การใช้สื่อดิจิทัลและกิจกรรมที่ทันสมัย หลากหลาย และต่อเนื่อง

๔. ข้อเสนอแนวทางการส่งเสริมจริยธรรมภาครัฐ ในยุคการพัฒนาเทคโนโลยีเพื่อรองรับสถานการณ์ Disruption

เนื่องจากข้าราชการและเจ้าหน้าที่ของรัฐเป็นบุคคลที่สามารถเข้าถึงแหล่งข้อมูลสำคัญ มีหน้าที่และอำนาจในการบริหารจัดการทรัพยากรของประเทศ ซึ่งการปฏิบัติราชการอาจกระทบต่อความเป็นส่วนตัวของประชาชน องค์กร หรือหน่วยงานที่เป็นเจ้าของข้อมูล สำนักงาน ก.พ. จึงควรมีการดำเนินการส่งเสริมจริยธรรมภาครัฐในยุคการพัฒนาเทคโนโลยีเพื่อรองรับสถานการณ์ Disruption ในเรื่องจริยธรรมและความเป็นส่วนตัวบนโลกดิจิทัล หรือ Digital Ethics and Privacy ดังนี้

๔.๑ กำหนดให้จริยธรรมและความเป็นส่วนตัวบนโลกดิจิทัล (Digital Ethics and Privacy) เป็นนโยบายหรือมาตรการที่หน่วยงานของรัฐต้องให้ความสำคัญ โดยให้องค์กรกลางบริหารงานบุคคลและองค์กรที่มีหน้าที่จัดทำประมวลจริยธรรมนำไปกำหนดในประมวลจริยธรรมของเจ้าหน้าที่ของรัฐที่อยู่ในความรับผิดชอบ เพื่อให้เกิดความตระหนักในสิทธิและหน้าที่ของพลเมืองในฐานะเจ้าของข้อมูล และการให้ความยินยอม (Consent) เผยแพร่ข้อมูลส่วนบุคคล ตลอดจนสิทธิและหน้าที่ของข้าราชการในการรักษาและป้องกันข้อมูลส่วนบุคคลของประชาชนในส่วนราชการต่าง ๆ ตามกฎหมาย

๔.๒ ควรมีการศึกษาเพื่อกำหนดคุณลักษณะของข้าราชการและเจ้าหน้าที่ของรัฐภายใต้สถานการณ์ Disruption ส่งเสริมให้ข้าราชการและเจ้าหน้าที่ของรัฐมีทักษะในการใช้เทคโนโลยีอย่างมีจริยธรรม ตลอดจนสามารถรับมือกับความปลอดภัยในโลกออนไลน์ ผู้บริหารมีบทบาทสำคัญในการเป็นแบบอย่าง กำกับ ติดตาม และสนับสนุนให้ส่วนราชการและหน่วยงานของรัฐจัดทำพฤติกรรมที่พึงประสงค์เพื่อเป็นแนวทางในการปฏิบัติที่ควรกระทำหรือไม่ควรกระทำ (Do and Don’t) ให้แก่ข้าราชการและเจ้าหน้าที่ของรัฐ รวมถึงส่งเสริมให้มีการศึกษาเพื่อออกแบบการส่งเสริมจริยธรรมเพื่อรองรับสถานการณ์ Disruption ตามความเหมาะสมกับบริบทที่แตกต่างกันในแต่ละส่วนราชการ

๔.๓ ส่งเสริมให้ข้าราชการตระหนักถึงความสำคัญกฎหมาย และปฏิบัติตามกฎหมายที่เกี่ยวข้อง โดยเฉพาะพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับ

คอมพิวเตอร์ พ.ศ. ๒๕๕๐ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๔.๔ ส่งเสริมและกระตุ้นให้ส่วนราชการและหน่วยงานของรัฐพัฒนาทักษะด้านดิจิทัลของข้าราชการและบุคลากรภาครัฐในด้านต่าง ๆ โดยเฉพาะความสามารถด้านความเข้าใจและใช้เทคโนโลยีดิจิทัล (Digital Literacy) ส่งเสริมให้ข้าราชการและเจ้าหน้าที่ของรัฐรักษาจริยธรรมและความเป็นส่วนตัวบนโลกดิจิทัล รวมถึงกระตุ้นเตือนให้สังคมเกิดความระมัดระวังในการใช้เทคโนโลยีให้ถูกต้อง ตลอดจนมีช่องทางในการแจ้งเตือนการรั่วไหลของข้อมูล และรับเรื่องร้องเรียนจากผู้ที่ได้รับผลกระทบ

๔.๕ ส่งเสริมให้หน่วยงานของรัฐคำนึงถึงการจัดทำสื่อรณรงค์เพื่อการส่งเสริมจริยธรรม และการเผยแพร่ข้อมูลเกี่ยวกับการดำเนินการทางจริยธรรมกับเจ้าหน้าที่ของรัฐ โดยใช้เทคโนโลยีสารสนเทศและช่องทางการรับรู้ที่เหมาะสมกับกลุ่มเป้าหมาย ตลอดจนความเป็นส่วนตัวบนโลกดิจิทัล (Digital Ethics and Privacy) เพื่อป้องกันไม่ให้เกิดการละเมิดสิทธิส่วนบุคคล ซึ่งอาจก่อให้เกิดความเสียหายและส่งผลกระทบต่อความเชื่อมั่นของประชาชน

มติที่ประชุม

จากการเสนอที่ประชุมประชุม อ.ก.พ. วิสามัญเกี่ยวกับการส่งเสริมจริยธรรมเพื่อราชการใสสะอาด จำนวน ๒ ครั้ง มีมติที่ประชุมดังนี้

การประชุม อ.ก.พ. วิสามัญเกี่ยวกับการส่งเสริมจริยธรรมเพื่อราชการใสสะอาด ครั้งที่ ๑/๒๕๖๓ เมื่อวันที่ ๒๑ มกราคม ๒๕๖๓ ได้พิจารณาแนวทางการส่งเสริมจริยธรรมภาครัฐในยุคการพัฒนาเทคโนโลยีเพื่อรองรับสถานการณ์ Disruption ตามที่ฝ่ายเลขานุการเสนอแล้ว มีมติเห็นชอบและมีความเห็นเพิ่มเติมว่า ข้าราชการและเจ้าหน้าที่ของรัฐในยุคการพัฒนาเทคโนโลยี ต้องปรับตัวเพื่อรับมือกับสถานการณ์ Disruption โดยควรกำหนดกรอบความคิด (Mindset) หรือค่านิยม (Values) สร้างวัฒนธรรมองค์กรใหม่ที่ข้าราชการควรจะยึดถือปฏิบัติ สอดแทรกไปในมาตรฐานทางจริยธรรมเจ้าหน้าที่ของรัฐ ดังต่อไปนี้

๑. มีใจเปิดกว้าง พร้อมทำงานแบบมีส่วนร่วม พร้อมรับการตรวจสอบและมีความโปร่งใส (Openness /transparency)

๒. ปฏิบัติต่อข้อมูลอย่างถูกต้องเหมาะสม มีข้อมูลรอบด้าน รู้จักปกป้องข้อมูลส่วนบุคคล ระมัดระวังการใช้ข้อมูลของส่วนราชการ (Inside Information) เพื่อป้องกันการขัดกันของผลประโยชน์ (Conflict of Interest)

๓. มีความพร้อมรับมือกับการเปลี่ยนแปลง (Dynamics) พัฒนาตนเองอยู่เสมอ

๔. มีวิจารณญาณที่ถูกต้อง รู้ว่าสิ่งใดถูก - ผิด (What is right or wrong) โดยเฉพาะในยุคที่มีกระแสข่าวปลอมต่าง ๆ (Fake news)

๕. มีความรู้เกี่ยวกับเทคโนโลยีดิจิทัล และสามารถสร้างนวัตกรรมดิจิทัลที่เกี่ยวข้องกับภารกิจของหน่วยงาน (Digital Innovation)

ทั้งนี้ ควรกำหนดให้จริยธรรมและความเป็นส่วนตัวบนโลกดิจิทัลอยู่ในประมวลจริยธรรม และกระบวนการบริหารงานบุคคล โดยเฉพาะการประเมินการเลื่อนเงินเดือนและการให้ความดีความชอบด้วย

การประชุม อ.ก.พ. วิสามัญเกี่ยวกับการส่งเสริมจริยธรรมเพื่อราชการใสสะอาด ครั้งที่ ๔/๒๕๖๓ วันที่ ๒๖ พฤษภาคม ๒๕๖๓ ได้พิจารณาแนวทางการปรับกระบวนการคิดเชิงจริยธรรมให้กับข้าราชการพลเรือน เพื่อเตรียมความพร้อมในการรองรับสถานการณ์ Disruption แล้ว มีมติเห็นชอบและมีความเห็นเพิ่มเติมว่า ศูนย์ส่งเสริมจริยธรรม ในฐานะหน่วยงานกลางด้านการส่งเสริมจริยธรรมเจ้าหน้าที่ของรัฐ จะต้องมุ่งเน้นการทำงานในลักษณะของการศึกษาวิจัยหรือการศึกษาค้นคว้าในเรื่องใหม่ ๆ (Research-based) รวมถึงมีการศึกษาแนวทางการปฏิบัติที่ดีหรือแบบอย่างการดำเนินงานที่ประสบความสำเร็จทั้งในและต่างประเทศ (Best Practice) เพื่อพัฒนาองค์ความรู้ เครื่องมือ และนวัตกรรมในการรณรงค์ส่งเสริมจริยธรรมให้สอดคล้องกับการบริหารราชการและการบริหารงานบุคคลภาครัฐยุคใหม่ รวมทั้งการดำเนินชีวิตตามรูปแบบความปกติใหม่ (New Normal) ในโลกยุคปัจจุบันที่เกิดความเปลี่ยนแปลงอย่างฉับพลัน ทั้งจากเทคโนโลยีดิจิทัลและปัญหาโรคระบาด

โดยที่ประชุมมีข้อเสนอแนะดังต่อไปนี้

๑) การรณรงค์ ส่งเสริมจริยธรรมภาครัฐในโลกยุคปัจจุบัน ควรต้องดำเนินการควบคู่ไปกับการให้ความรู้เกี่ยวกับสถานการณ์ Disruption ปัญหาในระบบราชการ ที่ส่งผลกระทบต่อการดำเนินชีวิตและการปฏิบัติหน้าที่ราชการ เช่น ยุคดิจิทัล ข้าราชการและเจ้าหน้าที่ของรัฐต้องใช้ข้อมูลให้เหมาะสมโดยเฉพาะข้อมูลภายใน ข้อมูลชั้นความลับ (inside information) ต้องพร้อมรับการเปลี่ยนแปลง ปัญหาระบบอุปถัมภ์หรือระบบเครือญาติที่มีผลต่อความซื่อสัตย์สุจริต ความรับผิดชอบ ผลประโยชน์ส่วนตัว ซึ่งต้องมีการศึกษาข้อมูลเพื่อปรับปรุงเนื้อหาสาระ รูปแบบ แนวทางหรือวิธีดำเนินการให้มีความเหมาะสม มีประสิทธิภาพ และมีความเป็นสากลยิ่งขึ้น

๒) ควรพิจารณาจัดลำดับความสำคัญของมาตรฐานทางจริยธรรม ๗ ประการ ตามมาตรา ๕ ของพระราชบัญญัติมาตรฐานทางจริยธรรม พ.ศ. ๒๕๖๒ เพื่อส่งเสริมจริยธรรมให้กับเจ้าหน้าที่ของรัฐตามสถานการณ์ปัจจุบันที่สังคมประสบปัญหาบ่อยครั้ง อาทิ ควรส่งเสริมพฤติกรรมในเรื่อง กล้าตัดสินใจและกระทำในสิ่งที่ถูกต้องชอบธรรม ซึ่งเป็นประเด็นปัญหาจริยธรรมที่สำคัญซึ่งเจ้าหน้าที่ของรัฐยังขาดอยู่ และส่งผลให้เกิดการทุจริตคอรัปชันในระบบราชการ หรือการคิดถึงประโยชน์ส่วนตัวมากกว่าประโยชน์ส่วนรวมที่ทำให้การแก้ไขปัญหาต่าง ๆ เป็นไปได้ยาก นอกจากนี้ในประเด็นเกี่ยวกับการพัฒนาด้านการใช้เทคโนโลยีสารสนเทศให้กับเจ้าหน้าที่ของรัฐในแต่ละช่วงอายุซึ่งมีระดับความรู้ความเข้าใจที่แตกต่างกัน จึงควรส่งเสริมให้มีการเรียนรู้เพื่อพัฒนาและส่งเสริมจริยธรรมในการใช้เทคโนโลยีไปพร้อมกัน

๓) ควรมีการจัดทำองค์ความรู้ด้านจริยธรรม เครื่องมือ หรือวิธีการพัฒนากระบวนการคิดเชิงจริยธรรมทั้งในรูปแบบที่เป็นทางการและไม่เป็นทางการ เพื่อใช้ในการส่งเสริมคุณธรรม จริยธรรมให้กับเจ้าหน้าที่ของรัฐ โดยอาจจัดทำในรูปแบบของชุดคู่มือส่งให้องค์กรคุ้มครองจริยธรรมในทุกส่วนราชการนำไปเผยแพร่ สร้างความรู้ความเข้าใจ และนำไปใช้ในการดำเนินงานได้อย่างเป็นรูปธรรม นอกจากนี้ ควรให้ความสำคัญเรื่องการนำข้อมูลเกี่ยวกับพฤติกรรมเชิงจริยธรรมเข้ามาใช้ในการบริหารงานบุคคลให้มากยิ่งขึ้น โดยพิจารณากำหนดรูปแบบ วิธีการ และกระบวนการประเมินและวัดผลพฤติกรรมเชิงจริยธรรมของบุคคล ตั้งแต่การสรรหาและเลือกสรร ไปจนถึงการแต่งตั้ง โยกย้าย เลื่อนตำแหน่ง นอกเหนือจากข้อมูลรูปแบบเดิมที่ได้จากการสังเกต การบันทึกพฤติกรรมที่ผ่านมาในประวัติการศึกษา หรือการทำงาน

๔) การรณรงค์ส่งเสริมจริยธรรมภาครัฐ ควรพิจารณาถึงประเด็นสำคัญคือ การส่งเสริมให้ผู้บังคับบัญชามีกรอบความคิดเชิงจริยธรรมที่ถูกต้อง คำนึงถึงสายตาและความรู้สึกนึกคิดของประชาชน อย่างไรก็ตาม การดำเนินงานในด้านต่าง ๆ โดยเฉพาะการเผยแพร่ข้อมูลกรณีศึกษาด้านจริยธรรม ต้องคำนึงถึงหลักกฎหมายด้วยว่าให้อำนาจในการดำเนินการได้หรือไม่ และต้องระมัดระวังไม่ให้เกิดการละเมิดหรือกระทบสิทธิส่วนบุคคล และควรสร้างความเข้าใจเกี่ยวกับสถานการณ์ Disruption ว่าอาจจะเป็นเหตุให้เกิดการเปลี่ยนแปลงในการบริหารราชการในหลายมิติ แต่หลักการสำคัญของมาตรฐานทางจริยธรรม ๗ ประการ เช่น ความถูกต้อง ความชอบธรรม การเป็นแบบอย่างที่ดี ยังคงเป็นค่านิยมหลัก (Core Values) ที่ไม่เปลี่ยนแปลง ซึ่งศูนย์ส่งเสริมจริยธรรมจะต้องนำหลักการนี้มาปรับใช้เพื่อกำหนดแนวทาง วิธีการส่งเสริมจริยธรรม หรือแนวทางการประพฤติปฏิบัติ ซึ่งแตกต่างกันไปตามลักษณะของส่วนราชการ และสอดคล้องกับสถานการณ์ Disruption ในแต่ละช่วงเวลา

๕) การขับเคลื่อนงานด้านจริยธรรมควรกำหนดแนวทางดำเนินการให้ครอบคลุมทั้งในเรื่องการส่งเสริม (Promotion) และการลงโทษ (Punishment) โดยร่วมมือกับส่วนราชการและองค์กรภาคีเครือข่ายที่เกี่ยวข้อง กำหนดวิธีการให้งานด้านการส่งเสริมจริยธรรม และงานด้านการป้องกันและปราบปรามการทุจริต มีการดำเนินการร่วมกันอย่างมีกลยุทธ์ และควรศึกษาแนวทางการส่งเสริมบทบาทและการมีส่วนร่วมในการติดตามตรวจสอบพฤติกรรมเจ้าหน้าที่ของรัฐของประชาชนในรูปแบบของผู้แจ้งเบาะแส (Whistle Blower) และผู้เฝ้าระวัง (Watchdog) ในสถานการณ์ Disruption เพื่อเปิดโอกาสให้ประชาชนส่งข้อมูลที่เกี่ยวข้องเพื่อประโยชน์ของทางราชการ โดยใช้เทคโนโลยีดิจิทัลเป็นฐาน และเพื่อให้ประชาชนเกิดความมั่นใจในแนวทางดังกล่าว

๖) ควรศึกษาและคิดริเริ่มแนวทางหรือโครงการใหม่ ๆ เพื่อสร้างนวัตกรรมด้านการส่งเสริมจริยธรรมภาครัฐ (Innovation in Public Ethics) ในสถานการณ์ Disruption โดยอาจกำหนดกลไก บัญญัติข้อกฎหมาย หรือบทลงโทษเพิ่มเติม เพื่อให้การส่งเสริมจริยธรรมภาครัฐได้รับผลดียิ่งขึ้น เช่น การจัดตั้งกองทุนจริยธรรม เพื่อสนับสนุนค่าตอบแทนพิเศษแก่ผู้ได้รับการคัดเลือกเป็นข้าราชการพลเรือนดีเด่น เป็นต้น

****