รายงานการประเมินผลสัมฤทธิ์ของ
พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

ส่วนที่ ๑
ข้อมูลเบื้องต้น

---

๑. หน่วยงานผู้รับผิดชอบการประเมินผลสัมฤทธิ์ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

๒. หน่วยงานผู้บังคับใช้กฎหมาย สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

๓. ผู้รักษาการตามกฎหมาย รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

๔. เหตุแห่งการประเมินผลสัมฤทธิ์ (ตอบได้มากกว่า ๑ ข้อ)

☑ ครบรอบระยะเวลาที่กำหนด

☐ ได้รับหนังสือร้องเรียนหรือข้อเสนอแนะจากผู้เกี่ยวข้องในเรื่อง (ระบุเรื่องที่ได้รับการร้องเรียนหรือมีข้อเสนอแนะ).....

☐ ได้รับข้อเสนอแนะจากคณะกรรมการพัฒนากฎหมายในเรื่อง (ระบุเรื่องที่ได้รับการเสนอแนะให้ประเมิน).....

☐ อื่น ๆ คือ.....

.....

๕. วันที่มีเหตุแห่งการประเมินผลสัมฤทธิ์ ๑ มกราคม ๒๕๖๘ **โดยประเมินผลที่เกิดจากการบังคับใช้กฎหมายตั้งแต่วันที่** ๑๘ กรกฎาคม ๒๕๕๐ **ถึงวันที่** ๓๑ ธันวาคม ๒๕๖๗

๖. รายชื่อกฎที่เป็นส่วนหนึ่งของการประเมินผลสัมฤทธิ์ในรายงานฉบับนี้

๑. ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง ลักษณะและวิธีการส่ง และลักษณะและปริมาณของข้อมูล ความถี่และวิธีการส่งซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับ พ.ศ. ๒๕๖๐

๒. ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์ ระยะเวลา และวิธีการปฏิบัติสำหรับการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ของพนักงานเจ้าหน้าที่หรือผู้ให้บริการ พ.ศ. ๒๕๖๐

๓. ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๖๔

๔. ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง ขั้นตอนการแจ้งเตือน การระงับการทำให้แพร่หลายของข้อมูลคอมพิวเตอร์ และการนำข้อมูลคอมพิวเตอร์ออกจากระบบคอมพิวเตอร์ พ.ศ. ๒๕๖๕

๗. รายชื่อกฎที่ดำเนินการประเมินผลสัมฤทธิ์เป็นการเฉพาะ (ประเมินผลสัมฤทธิ์เป็นรายฉบับตามแบบรายงานการประเมินผลสัมฤทธิ์ของกฎ) ไม่มี

ส่วนที่ ๒
การวิเคราะห์ความจำเป็นและผลกระทบของกฎหมาย

๘. กฎหมายนี้มีวัตถุประสงค์เพื่อแก้ปัญหาใด

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ มีเหตุผลในการประกาศใช้ คือ เนื่องจากในปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ หากมีผู้กระทำด้วยประการใด ๆ ให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะอันลามกอนาจาร ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน สมควรกำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำดังกล่าว

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ จึงเป็นกฎหมายที่มีวัตถุประสงค์เพื่อกำหนดฐานความผิดและบทลงโทษสำหรับการก่ออาชญากรรมทางคอมพิวเตอร์หรือการใช้คอมพิวเตอร์ในทางมิชอบขึ้นให้สอดคล้องและทันต่อสภาวการณ์ของความก้าวหน้าทางเทคโนโลยีสารสนเทศ ที่มีผลกระทบกับวิถีชีวิตและพฤติกรรมของบุคคลในสังคมอย่างมาก โดยเฉพาะการใช้คอมพิวเตอร์เป็นเครื่องมือสื่อสาร การบันทึกข้อมูล ตลอดจนการประมวลผลข้อมูลต่าง ๆ เพื่อการใช้ประโยชน์ โดยมีลักษณะของการกระทำความผิดที่อาจแบ่งได้เป็นสองลักษณะ ได้แก่ อาชญากรรมที่กระทำต่อระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ และการใช้คอมพิวเตอร์เป็นเครื่องมือประกอบอาชญากรรม เนื่องจากปัจจุบันได้เกิดอาชญากรรมอันเนื่องมาจากการใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด ซึ่งอาจก่อให้เกิดความเสียหายทางเศรษฐกิจและสังคม หรือส่งผลกระทบต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชนอย่างร้ายแรง และมีผลกระทบต่อส่วนรวม รัฐจึงจำเป็นต้องกำหนดมาตรการทางกฎหมายเพื่อให้การแก้ไขปัญหาดังกล่าวเป็นไปอย่างเหมาะสมและมีประสิทธิภาพ

๙. มาตรการสำคัญที่ทำให้บรรลุวัตถุประสงค์ของกฎหมายนี้ คือ

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ได้กำหนดกลไกอันเป็นมาตรการสำคัญเพื่อให้บรรลุวัตถุประสงค์ของกฎหมาย ดังนี้

๙.๑ กำหนดฐานความผิด และองค์ประกอบความผิด ซึ่งมีโทษจำคุก หรือปรับ หรือทั้งจำทั้งปรับ หรือปรับเป็นพินัย ตามอัตราที่กำหนดไว้ในแต่ละมาตรา โดยแบ่งออกเป็นสองลักษณะความผิด ได้แก่

ลักษณะที่ ๑ ความผิดที่กระทำต่อระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์

(๑) การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ (มาตรา ๕)

(๒) การเปิดเผยมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะโดยมิชอบ (มาตรา ๖)

(๓) การเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ (มาตรา ๗)

(๔) การดักรับข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ (มาตรา ๘)

(๕) การทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติมข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ (มาตรา ๙)

(๖) การกระทำเพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นไม่สามารถทำงานตามปกติได้ (มาตรา ๑๐)

(๗) การส่งข้อมูลคอมพิวเตอร์รบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข (มาตรา ๑๑) (เป็นความผิดทางพินัยซึ่งต้องชำระค่าปรับเป็นพินัย)

(๘) การจำหน่ายชุดคำสั่งที่จัดทำขึ้นเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิด (มาตรา ๑๓)

ลักษณะที่ ๒ การใช้ระบบคอมพิวเตอร์กระทำความผิดอื่น

(๙) การนำข้อมูลคอมพิวเตอร์ที่นิดเนื้อนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วนหรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ หรือเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา หรือมีลักษณะอันลามก เข้าสู่ระบบคอมพิวเตอร์ รวมทั้งการเผยแพร่หรือส่งต่อซึ่งข้อมูลดังกล่าว (มาตรา ๑๔)

(๑๐) ผู้ให้บริการที่ให้ความร่วมมือ ยินยอม หรือรู้เห็นเป็นใจให้มีการกระทำความผิดตามมาตรา ๑๔ (มาตรา ๑๕)

(๑๑) การสร้าง ตัดต่อ เติม หรือดัดแปลงข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่นหรือผู้ตาย (มาตรา ๑๖)

(๑๒) ล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการที่พนักงานเจ้าหน้าที่ได้มาตามมาตรา ๑๘ และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใด (มาตรา ๒๔)

(๑๓) ผู้ให้บริการที่ไม่เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (มาตรา ๒๖) (เป็นความผิดทางพินัยซึ่งต้องชำระค่าปรับเป็นพินัย)

(๑๔) ผู้ที่ไม่ปฏิบัติตามคำสั่งของศาลหรือพนักงานเจ้าหน้าที่ (มาตรา ๒๗) (เป็นความผิดทางพินัยซึ่งต้องชำระค่าปรับเป็นพินัย)

๙.๒ การดำเนินคดี

(๑) กำหนดอำนาจศาลในการสั่งให้ทำลายข้อมูลคอมพิวเตอร์ที่ผิดกฎหมาย สั่งให้โฆษณาหรือเผยแพร่คำพิพากษา หรือสั่งให้ดำเนินการอื่นตามที่ศาลเห็นสมควรเพื่อบรรเทาความเสียหายที่เกิดขึ้นจากการกระทำความผิดนั้น (มาตรา ๑๖/๑)

(๒) กำหนดการกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักรที่ต้องรับโทษในราชอาณาจักร (มาตรา ๑๗)

(๓) กำหนดลักษณะความผิดที่สามารถเปรียบเทียบได้ โดยคณะกรรมการเปรียบเทียบ (มาตรา ๑๗/๑)

(๔) กำหนดการใช้อำนาจในการสืบสวนและสอบสวนของพนักงานเจ้าหน้าที่ ซึ่งไม่ต้องขออนุญาตศาล (มาตรา ๑๘)

(๕) กำหนดการใช้อำนาจในการสืบสวนและสอบสวนของพนักงานเจ้าหน้าที่ ซึ่งต้องขออนุญาตศาล และการตรวจสอบการใช้อำนาจของพนักงานเจ้าหน้าที่โดยศาล (มาตรา ๑๙)

(๖) กำหนดอำนาจศาลในการมีคำสั่งระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่ผิดกฎหมาย หรือที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน โดยความเห็นชอบของคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์ (มาตรา ๒๐)

(๗) กำหนดอำนาจศาลในการห้ามจำหน่ายหรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ (มาตรา ๒๑)

(๘) กำหนดให้ข้อมูล ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้ ให้อ้างและรับฟังเป็นพยานหลักฐานได้ (มาตรา ๒๕)

๙.๓ บทกำหนดโทษ

(๑) กำหนดบทลงโทษที่หนักขึ้นสำหรับการกระทำที่ก่อให้เกิดความเสียหายแก่ประชาชนหรือการรักษาความมั่นคงของประเทศ (มาตรา ๑๒)

(๒) กำหนดบทลงโทษที่หนักขึ้นสำหรับการกระทำที่เป็นเหตุให้เกิดอันตรายแก่บุคคลอื่นหรือทรัพย์สินของผู้อื่น (มาตรา ๑๒/๑)

(๓) กำหนดบทลงโทษสำหรับผู้ฝ่าฝืนไม่ปฏิบัติตามคำสั่งศาลที่สั่งให้ทำลายข้อมูลคอมพิวเตอร์ที่ผิดกฎหมาย (มาตรา ๑๖/๒)

(๔) กำหนดความรับผิดของพนักงานเจ้าหน้าที่ที่เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการให้แก่บุคคลใดที่มิใช่เพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัตินี้ (มาตรา ๒๒) และการกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลดังกล่าว (มาตรา ๒๓)

๑๐. กฎหมายนี้มีบทบัญญัติกำหนดให้ประชาชนต้องกระทำการหรืองดเว้นกระทำการอย่างใดอย่างหนึ่งหรือไม่ อย่างไร

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ได้กำหนดให้ประชาชนต้องกระทำการหรืองดเว้นกระทำการ ดังนี้

(๑) กำหนดให้ผู้ให้บริการมีหน้าที่กำหนดขั้นตอนการแจ้งเตือน การระงับการทำให้แพร่หลายของข้อมูลคอมพิวเตอร์ และการนำข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์ สำหรับการให้บริการของตน เพื่อเป็นการพิสูจน์ว่าตนมิได้ให้ความร่วมมือ ยินยอม หรือรู้เห็นเป็นใจให้มีการกระทำความผิดตามมาตรา ๑๔ (มาตรา ๑๕)

(๒) กำหนดให้ผู้ให้บริการมีหน้าที่เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ สำหรับการให้บริการของตน (มาตรา ๒๖)

(๓) กำหนดให้ประชาชนต้องปฏิบัติตามคำสั่งของศาลหรือพนักงานเจ้าหน้าที่ที่สั่งตามมาตรา ๑๘ มาตรา ๒๐ หรือมาตรา ๒๑ (มาตรา ๒๗)

๑๑. กฎหมายนี้ยังมีความจำเป็นและสอดคล้องกับสภาพการณ์ พัฒนาการของเทคโนโลยี และวิถีชีวิตของประชาชนหรือไม่ เพียงใด

ปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ อีกทั้ง การบริหารราชการแผ่นดินและการจัดทำบริการสาธารณะในปัจจุบันได้มีการนำเทคโนโลยีมาประยุกต์ใช้เพื่อประโยชน์ในการบริหารราชการแผ่นดิน การอำนวยความสะดวกให้แก่ประชาชน และการเสริมสร้างความสามารถในการแข่งขันของประเทศ หากมีผู้กระทำด้วยประการใด ๆ ให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะอันลามกอนาจาร ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน ดังนั้น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ซึ่งเป็นกฎหมายที่กำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำดังกล่าว จึงมีความสอดคล้องกับสภาพการณ์ พัฒนาการของเทคโนโลยี และวิถีชีวิตของประชาชน ที่ระบบคอมพิวเตอร์เป็นส่วนสำคัญของการดำรงชีวิตของประชาชน

๑๒. ประโยชน์ที่ประชาชนได้รับจากการมีกฎหมายนี้ คือ

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ทำให้ประเทศไทยมีกฎหมายที่กำหนดให้การกระทำความผิดเกี่ยวกับคอมพิวเตอร์เป็นความผิดและมีบทลงโทษสำหรับการกระทำดังกล่าว มีมาตรการทางกฎหมายในการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ที่ผิดกฎหมายออกจากระบบคอมพิวเตอร์ กำหนดกลไกในการสืบสวนสอบสวนเพื่อดำเนินคดีความผิดเกี่ยวกับคอมพิวเตอร์เป็นการเฉพาะ ซึ่งเป็นความผิดที่ต้องอาศัยบุคคลที่มีความรู้ ความชำนาญเกี่ยวกับคอมพิวเตอร์ในการรวบรวมพยานหลักฐานโดยวิธีการทางคอมพิวเตอร์เพื่อให้ได้มาซึ่งข้อมูลคอมพิวเตอร์สำหรับพิสูจน์การกระทำความผิดและหาตัวผู้กระทำผิดให้เป็นไปอย่างมีประสิทธิภาพ อันเป็นการคุ้มครองประชาชนและสังคมให้มีความปลอดภัยจากการใช้งานคอมพิวเตอร์ ซึ่งปัจจุบันเป็นส่วนสำคัญในการดำรงชีวิตของประชาชน รวมทั้งเป็นการรักษาความสงบสุขและศีลธรรมอันดีของประชาชนและสังคม

๑๓. กฎหมายนี้ก่อให้เกิดผลดังต่อไปนี้หรือไม่ อย่างไร (ให้พิจารณาตอบเฉพาะประเด็นสำคัญที่ตรงกับวัตถุประสงค์ของกฎหมาย โดยไม่ต้องตอบทุกประเด็นก็ได้)

- เป็นอุปสรรคต่อการดำรงชีวิตหรือการประกอบอาชีพของประชาชน

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เป็นกฎหมายที่กำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ อันเป็นการคุ้มครองประชาชนและสังคมให้มีความปลอดภัยจากการใช้งานคอมพิวเตอร์ จึงไม่เป็นอุปสรรคต่อการดำรงชีวิตหรือการประกอบอาชีพของประชาชน

- ลดความเหลื่อมล้ำและสร้างความเป็นธรรมในสังคม

ไม่มี

- เป็นอุปสรรคต่อการแข่งขันหรือการเพิ่มความสามารถในการแข่งขันของประเทศ

ไม่มี

- เป็นการพัฒนากฎหมายให้สอดคล้องกับหลักสากลและพันธกรณีระหว่างประเทศ

ปัจจุบันประเทศไทยได้เข้าร่วมลงนามอนุสัญญาสหประชาชาติว่าด้วยการต่อต้านอาชญากรรมไซเบอร์ (United Nations Convention against Cybercrime) ซึ่งมีวัตถุประสงค์เพื่อส่งเสริมและสร้างมาตรการในการป้องกันและต่อต้านอาชญากรรมไซเบอร์ให้มีประสิทธิภาพและประสิทธิผลมากขึ้น พร้อมทั้งอำนวยความสะดวกและเสริมสร้างความร่วมมือระหว่างประเทศในการป้องกันและต่อต้านอาชญากรรมไซเบอร์ โดยสาระสำคัญของอนุสัญญาฯ ครอบคลุมมาตรการป้องกันอาชญากรรมไซเบอร์ โดยเฉพาะการล่วงละเมิดทางเพศต่อเด็ก การเผยแพร่ภาพส่วนบุคคลทางออนไลน์โดยไม่ได้รับความยินยอม การกำหนดมาตรการเกี่ยวกับการเก็บรักษาข้อมูลทางอิเล็กทรอนิกส์ การอายัด ยึด และริบทรัพย์ จากอาชญากรรม เพื่อประโยชน์ในการดำเนินคดีและบังคับใช้กฎหมาย การติดตามและนำทรัพย์สินที่ได้จากการกระทำความผิดกลับคืนรวมถึงการแลกเปลี่ยนพยานหลักฐานอิเล็กทรอนิกส์ข้ามพรมแดน การสนับสนุนด้านเทคนิคและการเสริมสร้างขีดความสามารถในการป้องกันและต่อต้านอาชญากรรมไซเบอร์ โดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เป็นหนึ่งในกฎหมายสำคัญที่มีกลไกช่วยให้ประเทศไทยสามารถปฏิบัติตามพันธกรณีของอนุสัญญาดังกล่าวได้อย่างมีประสิทธิภาพ อันเป็นการส่งเสริมบทบาทและเป็นการแสดงเจตนารมณ์ของประเทศไทยในการต่อต้านอาชญากรรมไซเบอร์ซึ่งเป็นปัญหาและความท้าทายของโลกในปัจจุบัน

- มีผลกระทบต่อเศรษฐกิจ สังคม สิ่งแวดล้อมหรือสุขภาวะ หรือผลกระทบอื่นที่สำคัญ

ไม่มี

๑๔. มีสถิติการดำเนินคดีและการลงโทษตามกฎหมาย หรือสถิติการปฏิบัติตามและการบังคับการให้เป็นไปตามกฎหมายอย่างไร

(๑) สถิติการดำเนินการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ออกจากระบบคอมพิวเตอร์ตามมาตรา ๒๐ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ของพนักงานเจ้าหน้าที่ที่ได้รับการแต่งตั้งตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ โดยศาลที่มีเขตอำนาจได้มีคำสั่งระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ออกจากระบบคอมพิวเตอร์ตามคำร้องของพนักงานเจ้าหน้าที่ จำนวน ๑,๙๕๗ คำสั่งศาล เป็นจำนวน ๑๔๘,๐๗๘ โดเมนเนม/URL (ข้อมูล ณ วันที่ ๓๑ ธันวาคม ๒๕๖๗)

(๒) สถิติคดีที่เข้าสู่การพิจารณาพิพากษาของศาลชั้นต้นทั่วราชอาณาจักร ประเภทคดีอาชญากรรมทางเทคโนโลยี (คดีอาญาที่ฟ้องขอให้ลงโทษบุคคลที่กระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์) จำนวน ๑,๖๙๙ คดี โดยพิพากษาแล้วเสร็จ จำนวน ๑,๒๙๘ คดี (ข้อมูล ณ วันที่ ๓๑ ธันวาคม ๒๕๖๗)

๑๕. มีปัญหาและอุปสรรคในการบังคับใช้กฎหมายนี้หรือไม่ อย่างไร

(๑) ผู้ให้บริการยังมีความไม่เข้าใจหรือเข้าใจคลาดเคลื่อนว่า การให้บริการของตนเข้าข่ายเป็นผู้ให้บริการตามกฎหมายนี้หรือไม่ รวมถึงหน้าที่ของผู้ให้บริการในการเก็บรักษาข้อมูลจราจร

ทางคอมพิวเตอร์ และการกำหนดขั้นตอนการแจ้งเตือน การระงับการทำให้แพร่หลายของข้อมูลคอมพิวเตอร์ และการนำข้อมูลคอมพิวเตอร์ออกจากระบบคอมพิวเตอร์

(๒) ประชาชนยังมีความไม่เข้าใจหรือเข้าใจคลาดเคลื่อนเกี่ยวกับลักษณะของการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในบางลักษณะว่า การกระทำของตนเข้าข่ายเป็นความผิดตามกฎหมายหรือไม่ เช่น การดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ การส่งข้อมูลข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว เป็นต้น

(๓) หน่วยงานของรัฐหรือเจ้าหน้าที่ของรัฐยังมีความไม่เข้าใจหรือเข้าใจคลาดเคลื่อนว่า กฎหมายนี้สามารถกำหนดอำนาจในการกำกับดูแลการประกอบกิจการให้กับหน่วยงานของรัฐหรือเจ้าหน้าที่ของรัฐ หรือหน้าที่ในการประกอบกิจการให้กับผู้ให้บริการต้องปฏิบัติในการประกอบกิจการเหมือนดังเช่นกฎหมายที่เกี่ยวกับการกำกับดูแลการประกอบกิจการ เนื่องจากกฎหมายนี้เป็นกฎหมายที่ว่าด้วยการกระทำความผิด และกำหนดโทษสำหรับการกระทำความผิดนั้น ไม่ใช่กฎหมายที่เกี่ยวกับการกำกับดูแลการประกอบกิจการโดยตรง

(๔) หน่วยงานของรัฐหรือเจ้าหน้าที่ของรัฐ องค์กรภาคเอกชน หรือประชาชนยังมีความไม่เข้าใจหรือเข้าใจคลาดเคลื่อนว่า กฎหมายนี้เป็นกฎหมายที่จำกัดเสรีภาพในการแสดงความคิดเห็นหรือการติดต่อสื่อสาร เนื่องจากการแสดงความคิดเห็นหรือการติดต่อสื่อสารที่ไม่เข้าลักษณะที่มีกฎหมายบัญญัติไว้เป็นความผิดย่อมสามารถกระทำได้ และไม่อาจเป็นความผิดตามกฎหมายนี้

(๕) การกระทำความผิดเกี่ยวกับคอมพิวเตอร์เป็นการกระทำความผิดโดยอาศัยเทคโนโลยีเป็นเครื่องมือ ซึ่งไม่มีข้อจำกัดในเรื่องของท้องที่ที่ได้กระทำความผิด ทำให้สามารถกระทำความผิดได้จากทุกพื้นที่ทั่วโลก ในทางปฏิบัติจึงไม่สามารถดำเนินคดีกับผู้ให้บริการหรือผู้กระทำความผิดที่อยู่นอกราชอาณาจักรได้ จึงต้องอาศัยกลไกของกฎหมายอื่นในการกำกับดูแลการประกอบกิจการเพื่อควบคุมการให้และการใช้บริการ และความร่วมมือระหว่างประเทศที่เกี่ยวข้อง ในการดำเนินคดีกับผู้ให้บริการหรือผู้กระทำความผิดที่อยู่นอกราชอาณาจักร

ส่วนที่ ๓
การตรวจสอบเนื้อหาของกฎหมาย

๑๖. กฎหมายนี้มีความสัมพันธ์หรือใกล้เคียงกับกฎหมายอื่นหรือไม่ อย่างไร

(๑) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ มาตรา ๓ ได้บัญญัตินิยามคำว่า “ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

(๒) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ มาตรา ๑๔ (๓) ได้บัญญัติให้การนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับ

ความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา เป็นความผิด และต้องระวางโทษจำคุกไม่เกินห้าปีหรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(๓) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ มาตรา ๒๐ (๓) ได้กำหนดมาตรการในการยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ที่เป็นความผิดอาญาตามกฎหมายเกี่ยวกับทรัพย์สินทางปัญญาหรือกฎหมายอื่นซึ่งข้อมูลคอมพิวเตอร์นั้นมีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

(๔) พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖ มาตรา ๓ ได้บัญญัตินิยามคำว่า “อาชญากรรมทางเทคโนโลยี” หมายความว่า การกระทำหรือพยายามกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เพื่อฉ้อโกง กรรโชก หรือรีดเอาทรัพย์บุคคลหนึ่งบุคคลใด หรือโดยประการที่น่าจะทำให้บุคคลอื่นเสียหาย หรือกระทำความผิดฐานฉ้อโกง กรรโชก หรือรีดเอาทรัพย์ โดยใช้ระบบคอมพิวเตอร์เป็นเครื่องมือ และมาตรา ๗/๑ วรรคหนึ่ง ได้บัญญัติว่า “เมื่อความปรากฏต่อพนักงานเจ้าหน้าที่ซึ่งได้รับการแต่งตั้งตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ว่ามีผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลโดยไม่ได้รับอนุญาตตามกฎหมายว่าด้วยการประกอบธุรกิจสินทรัพย์ดิจิทัล ให้พนักงานเจ้าหน้าที่ดังกล่าวมีคำสั่งระงับการทำให้แพร่หลายของข้อมูลคอมพิวเตอร์หรือนำข้อมูลคอมพิวเตอร์ที่ผิดกฎหมายออกจากระบบคอมพิวเตอร์โดยพลัน

๑๗. มีการฟ้องคดีต่อศาลรัฐธรรมนูญหรือศาลปกครอง หรือการร้องเรียนต่อผู้ตรวจการแผ่นดิน หรือคณะกรรมการสิทธิมนุษยชนแห่งชาติเกี่ยวกับกฎหมายนี้กี่เรื่องและในประเด็นใด

คำวินิจฉัยของศาลรัฐธรรมนูญ คำวินิจฉัยที่ ๒๐/๒๕๖๖ เรื่อง พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ มาตรา ๑๔ ขัดหรือแย้งต่อรัฐธรรมนูญ มาตรา ๒๖ และมาตรา ๓๔ หรือไม่ [ระหว่างศาลอาญา ผู้ร้อง - ผู้ถูกร้อง] สรุปความได้ว่า มาตรา ๑๔ วรรคหนึ่ง เป็นบทบัญญัติที่กำหนดให้การกระทำในลักษณะต่าง ๆ ตามที่กฎหมายบัญญัติเป็นความผิดมีโทษทางอาญา โดยมาตรา ๑๔ วรรคหนึ่ง (๑) มีวัตถุประสงค์หรือคุณธรรมทางกฎหมายเพื่อมุ่งคุ้มครองประโยชน์สาธารณะเป็นสำคัญ แตกต่างจากความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา ซึ่งมีวัตถุประสงค์หรือคุณธรรมทางกฎหมายเพื่อมุ่งคุ้มครองชื่อเสียงและศักดิ์ศรีของบุคคลผู้ถูกใส่ความ ส่วนบทบัญญัติมาตรา ๑๔ วรรคหนึ่ง (๒) มีวัตถุประสงค์หรือคุณธรรมทางกฎหมายเพื่อป้องกันและปราบปรามการนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ เมื่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ มาตรา ๑๔ วรรคหนึ่ง (๑) และ (๒) เป็นบทบัญญัติที่ตราขึ้นอันมีวัตถุประสงค์เพื่อรักษาความมั่นคงของรัฐและเพื่อรักษาความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน ซึ่งการตรากฎหมายจำกัดเสรีภาพในลักษณะเช่นนี้ย่อมกระทำได้ตามที่บัญญัติไว้ในรัฐธรรมนูญมาตรา ๓๔ วรรคหนึ่ง เมื่อชั่งน้ำหนักระหว่างสิทธิและเสรีภาพของประชาชนที่ถูกจำกัดตามกฎหมายกับประโยชน์ส่วนรวมที่ได้รับตามวัตถุประสงค์ของกฎหมาย เป็นไปตามหลักความได้สัดส่วน อีกทั้งกฎหมายกำหนดองค์ประกอบความผิดและบทกำหนดโทษตามแต่ลักษณะความผิดไว้อย่างชัดเจนแน่นอนพอควรตามความร้ายแรงแห่งการกระทำ โดยให้ศาลใช้ดุลพินิจพิจารณาลงโทษตามข้อเท็จจริงของแต่ละคดี บทบัญญัติดังกล่าวไม่ขัดต่อหลักนิติธรรม ไม่เพิ่มภาระหรือจำกัดสิทธิหรือเสรีภาพของบุคคลเกินสมควรแก่เหตุ ไม่กระทบ

ต่อศักดิ์ศรีความเป็นมนุษย์ มีผลใช้บังคับเป็นการทั่วไป ไม่มุ่งหมายให้ใช้บังคับแก่กรณีใดกรณีหนึ่งหรือแก่บุคคลใดบุคคลหนึ่งเป็นการเจาะจง และไม่ขัดต่อเสรีภาพในการแสดงความคิดเห็นของบุคคล ไม่ขัดหรือแย้งต่อรัฐธรรมนูญ มาตรา ๒๖ และมาตรา ๓๔ วรรคหนึ่ง

สำหรับมาตรา ๑๔ วรรคหนึ่ง (๓) เป็นบทบัญญัติที่ตราขึ้นโดยมีวัตถุประสงค์เพื่อป้องกันและปราบปรามการนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา มีคุณธรรมทางกฎหมายมุ่งคุ้มครองความผาสุกของประชาชนในสังคมหรือประเทศชาติเพื่อให้เกิดความมั่นคง ความสงบสุข สันติภาพ และสุขภาวะร่วมกันของคนในสังคม เนื่องจากการกระทำความผิดดังกล่าวเป็นภัยร้ายแรงที่มีผลกระทบต่อความมั่นคงของรัฐ การปกครองในระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข ความสงบเรียบร้อยและความปลอดภัยของประชาชน องค์ประกอบความผิดตามอนุมาตรานี้ เพื่อให้การคุ้มครองเป็นพิเศษหากมีการกระทำความผิดดังกล่าวผ่านระบบคอมพิวเตอร์ ซึ่งเป็นการกระทำความผิดอาญาในรูปแบบเฉพาะที่ก่อให้เกิดความเสียหายเป็นวงกว้างอย่างรวดเร็วซึ่งยากแก่การแก้ไขเยียวยาในภายหลัง และอาจส่งผลกระทบต่อความมั่นคงของประเทศ มีระดับความร้ายแรงและส่งผลกระทบต่อส่วนรวมมากกว่าความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญาที่ได้กำหนดบทยกเว้นความผิดไว้ในประมวลกฎหมายอาญา มาตรา ๓๒๙ และเป็นความผิดที่กระทบต่อเสรีภาพและชื่อเสียงของบุคคลเท่านั้น ประกอบกับมาตรา ๑๔ วรรคหนึ่ง (๓) มิใช่ความผิดเด็ดขาด ผู้ถูกกล่าวหาว่ากระทำความผิดย่อมมีสิทธิที่จะต่อสู้คดีพิสูจน์ความจริงได้ตามกระบวนการของกฎหมาย โดยบุคคลนั้นยังถือว่าเป็นผู้บริสุทธิ์อยู่จนกว่าศาลมีคำพิพากษาอันถึงที่สุดว่าได้กระทำการอันเป็นความผิด และเมื่อชั่งน้ำหนักระหว่างสิทธิและเสรีภาพของประชาชนที่ถูกจำกัดตามกฎหมายกับประโยชน์ส่วนรวมที่ได้รับตามวัตถุประสงค์ของกฎหมาย เป็นไปตามหลักความได้สัดส่วนบทบัญญัติดังกล่าวไม่ขัดต่อหลักนิติธรรม ไม่เพิ่มภาระหรือจำกัดสิทธิหรือเสรีภาพของบุคคลเกินสมควรแก่เหตุไม่กระทบต่อศักดิ์ศรีความเป็นมนุษย์ มีผลใช้บังคับเป็นการทั่วไป ไม่มุ่งหมายให้ใช้บังคับแก่กรณีใดกรณีหนึ่งหรือแก่บุคคลใดบุคคลหนึ่งเป็นการเจาะจง และไม่ขัดต่อเสรีภาพในการแสดงความคิดเห็นของบุคคลไม่ขัดหรือแย้งต่อรัฐธรรมนูญ มาตรา ๒๖ และมาตรา ๓๔ วรรคหนึ่ง

จึงวินิจฉัยว่า พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ มาตรา ๑๔ วรรคหนึ่ง (๑) (๒) และ (๓) ไม่ขัดหรือแย้งต่อรัฐธรรมนูญมาตรา ๒๖ และมาตรา ๓๔ วรรคหนึ่ง

๑๘. การใช้ระบบอนุญาต ระบบคณะกรรมการ ดุลพินิจของเจ้าหน้าที่ และโทษอาญาในกฎหมายนี้ (ถ้ามี) ยังมีความเหมาะสมอยู่หรือไม่ อย่างไร

โทษอาญายังมีความเหมาะสม เนื่องจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ มีวัตถุประสงค์เพื่อรักษาความมั่นคงของรัฐและเพื่อรักษาความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน และมุ่งคุ้มครองสังคมเป็นสำคัญ จึงจำเป็นต้องมีโทษอาญาสำหรับในส่วนของความผิดที่มีโทษปรับสถานเดียว (มาตรา ๑๑ มาตรา ๒๖ และมาตรา ๒๗) ได้มีการเปลี่ยนเป็นความผิดทางพินัยตามพระราชบัญญัติว่าด้วยการปรับเป็นพินัย พ.ศ. ๒๕๖๕ ซึ่งต้องชำระค่าปรับเป็นพินัยแล้ว

ส่วนที่ ๔
ผลการประเมินผลสัมฤทธิ์ของกฎหมาย

๑๙. การรับฟังความคิดเห็น

☑ ได้รับฟังความคิดเห็นโดยถูกต้องตามข้อ ๕ และข้อ ๖ ของแนวทางการประเมินผลสัมฤทธิ์ของกฎหมายแล้ว

☑ ได้รับฟังความคิดเห็นโดยวิธีอื่นนอกจากผ่านระบบกลาง

ในการประเมินผลสัมฤทธิ์ของกฎหมายฉบับนี้ ได้ใช้วิธีการรับฟังความคิดเห็นของบุคคลที่เกี่ยวข้องกับการบังคับใช้กฎหมายและผู้ที่ได้รับผลกระทบทั้งภาคราชการและภาคเอกชน โดยการรับฟังความคิดเห็นผ่านระบบกลางทางกฎหมาย (https://www.law.go.th) มีผู้เข้ามาให้ความคิดเห็น จำนวน ๑๓๐ คน และมีหนังสือสอบถามความคิดเห็นไปยังผู้เกี่ยวข้อง จำนวน ๔๓ หน่วยงาน แบ่งเป็นหน่วยงานภาครัฐ จำนวน ๒๕ หน่วยงาน หน่วยงานภาคเอกชน จำนวน ๑๘ หน่วยงาน โดยมีหน่วยงานให้ความเห็นเป็นหนังสือ จำนวน ๕ หน่วยงาน

ผู้เกี่ยวข้องมีความเห็นเกี่ยวกับกฎหมายนี้หรือผลกระทบของกฎหมายนี้อย่างไร

ผู้เกี่ยวข้องที่ร่วมแสดงความเห็นในประเด็นต่อไปนี้

ประเด็นที่ ๑ ฐานความผิด องค์ประกอบความผิด และอัตราโทษ ตามลักษณะที่ ๑ ความผิดที่กระทำต่อระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ (มาตรา ๕ - ๑๑ และมาตรา ๑๓) มีความเหมาะสม หรือสมควรได้รับการแก้ไขเพิ่มเติมหรือปรับปรุง หรือสมควรยกเลิกหรือไม่อย่างไร

ผลการรับฟังความคิดเห็น

(๑) มีความเหมาะสม จำนวน ๑๐๙ คน (ร้อยละ ๘๓.๘๔)

(๒) สมควรได้รับการแก้ไขเพิ่มเติมหรือปรับปรุง จำนวน ๒๐ คน (ร้อยละ ๑๕.๓๘)

(๓) สมควรยกเลิก จำนวน ๑ คน (ร้อยละ ๐.๗๖)

(๔) อื่น ๆ ไม่มี

นอกจากนี้ผู้เกี่ยวข้องมีความเห็นเพิ่มเติมที่น่าสนใจดังนี้

- ความผิดในส่วนนี้ สมควรได้รับการแก้ไขเพิ่มเติมหรือปรับปรุง ดังนี้ ๑. เพิ่มฐานความผิดที่เกี่ยวกับ Ransomware ไว้เป็นการเฉพาะ เนื่องจากมีลักษณะของการกระทำที่รุนแรงยิ่งกว่าความผิดตามมาตรา ๙ และมาตรา ๑๐ ที่มีอยู่แล้วแต่เดิม ๒. เพิ่มบทยกเว้นความรับผิดที่ชัดเจนสำหรับกรณี Ethical Hacking เพื่อส่งเสริมอุตสาหกรรมด้าน Cybersecurity ของประเทศ

- ๑. บทวิเคราะห์สถานะปัจจุบันและหลักการพื้นฐาน (Current State & Fundamental Principles) แม้ว่ามาตรา ๕ ถึง ๑๑ และมาตรา ๑๓ จะเป็นหัวใจสำคัญที่สอดคล้องกับอนุสัญญาบูดาเปสต์ (Budapest Convention on Cybercrime) ซึ่งเป็นมาตรฐานสากล โดยคุ้มครองหลักการ CIA Triad (Confidentiality, Integrity, Availability) ได้แก่ การเข้าถึงโดยมิชอบ (Access - มาตรา ๕, ๗) คุ้มครองความลับ (Confidentiality) การดักรับข้อมูล (Interception - มาตรา ๘) คุ้มครองความเป็น

ส่วนตัว การแก้ไขเปลี่ยนแปลงข้อมูล (Data Interference - มาตรา ๙) คุ้มครองความถูกต้องครบถ้วน (Integrity) การรบกวนระบบ (System Interference - มาตรา ๑๐) คุ้มครองความพร้อมใช้งาน (Availability) สแปม (Spam - มาตรา ๑๑) คุ้มครองความสงบเรียบร้อย การจำหน่ายชุดคำสั่ง (Misuse of Devices - มาตรา ๑๓) ตัดตอนวงจรอาชญากรรม อย่างไรก็ตาม "ความเหมาะสม" ในทางกฎหมายเทคโนโลยีมีอายุขัยที่สั้นมาก (Short Shelf-Life) สิ่งที่เหมาะสมเมื่อ ๕-๑๐ ปีก่อน ไม่สามารถรับมือกับภัยคุกคามระดับ State-Sponsored Attack หรือ AI-Driven Cybercrime ในปัจจุบันได้ การยืนยันว่ากฎหมาย "เหมาะสม" โดยไม่ปรับปรุง จะทำให้ประสิทธิภาพในการบังคับใช้กฎหมายลดลง และขัดต่อเจตนารมณ์ของรัฐธรรมนูญ มาตรา ๗๗ ที่รัฐพึงจัดให้มีกฎหมายเพียงเท่าที่จำเป็นและทันสมัย ๒. เหตุผลเชิงลึกในการเสนอให้ "แก้ไขเพิ่มเติมหรือปรับปรุง" (In-Depth Rationale for Amendment) เพื่อให้กฎหมายไทยมีประสิทธิภาพสูงสุด (Maximum Efficiency) และมีความทันสมัยระดับโลก (World-Class Modernization) จำเป็นต้องมีการปรับปรุงในประเด็นละเอียดอ่อนดังนี้ A. นิยามศัพท์และการตีความในบริบทเทคโนโลยีอุบัติใหม่ (Definition in Emerging Tech Era) Cloud Computing & Virtualization มาตรา ๕ และ ๗ มักมองภาพคอมพิวเตอร์เป็นกายภาพ (Physical) แต่ในยุค Cloud Native และ Serverless Computing ขอบเขตของ "ระบบ" และ "ข้อมูล" มีความเลื่อนไหล (Fluidity) การเข้าถึง API หรือ Microservices โดยไม่ได้รับอนุญาต จำเป็นต้องมีนิยามที่ชัดเจนกว่านี้เพื่อไม่ให้เกิดช่องว่างทางกฎหมาย IoT & OT (Operational Technology) การโจมตีระบบคอมพิวเตอร์ในปัจจุบันลามไปถึงระบบควบคุมอุตสาหกรรม (SCADA) และอุปกรณ์ Internet of Things ซึ่งมาตรา ๑๐ (การรบกวนระบบ) ต้องขยายความให้ครอบคลุมถึงผลกระทบทางกายภาพ (Kinetic Impact) ที่เกิดจากไซเบอร์อย่างชัดเจน เพื่อให้สอดคล้องกับมาตรา ๑๒ ที่เกี่ยวกับความมั่นคง B. การปรับปรุงมาตรา ๑๓ และข้อยกเว้นเพื่อการวิจัย (Safe Harbor for Security Researchers) มาตรา ๑๓ เอาผิดผู้จำหน่ายหรือเผยแพร่ "ชุดคำสั่ง" (Tools/Malware) ที่ใช้กระทำความผิด แต่ในโลกความเป็นจริง เครื่องมือที่แฮกเกอร์ใช้ (เช่น Metasploit, Cobalt Strike) เป็นเครื่องมือเดียวกับที่ผู้เชี่ยวชาญด้านความปลอดภัย (White Hat Hackers) ใช้ในการทดสอบระบบ (Penetration Testing) เพื่อให้เกิดความคล่องตัวสูงสุด (Maximum Agility) และสร้างบุคลากรไซเบอร์ที่มีคุณภาพ ต้องมีการแก้ไขเพิ่มเติมข้อยกเว้น (Exemption Clause) หรือ "Safe Harbor" ให้กับนักวิจัยความปลอดภัยทางไซเบอร์ที่กระทำไปโดยสุจริตเพื่อการศึกษาหรือแจ้งเตือนช่องโหว่ (Vulnerability Disclosure Policy) มิเช่นนั้นกฎหมายจะกลายเป็นอุปสรรคต่อการพัฒนาภูมิคุ้มกันทางดิจิทัลของชาติ ซึ่งอาจขัดต่อยุทธศาสตร์ชาติ C. การยกระดับมาตรา ๙ และ ๑๐ เพื่อรับมือ Ransomware และ Cyber-Warfare Ransomware Specifics ปัจจุบัน Ransomware ไม่ใช่แค่การ "แก้ไขเปลี่ยนแปลง" หรือ "รบกวน" แบบเดิม แต่เป็นการ "เข้ารหัสลับข้อมูล" (Encryption) เพื่อเรียกค่าไถ่ การปรับปรุงกฎหมายควรกำหนดฐานความผิดเฉพาะที่มีเหตุฉกรรจ์สำหรับการโจมตีแบบ Ransomware โดยเฉพาะอย่างยิ่งเมื่อกระทำต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) อัตราโทษที่ยืดหยุ่นและรุนแรงตามผลกระทบ อัตราโทษควรปรับจากระบบ "โทษคงที่" เป็น "โทษแบบขั้นบันไดตามมูลค่าความเสียหายและผลกระทบทางสังคม" (Impact-Based Sentencing) เพื่อให้เกิดความเท่าเทียมและเป็นธรรมตามหลักสากล D. มาตรา ๑๑ (Spam) กับยุค AI Marketing นิยามของ "การก่อให้เกิดความเดือดร้อนรำคาญ" ต้องปรับปรุงให้เท่าทันเทคโนโลยี Marketing Automation และ AI Bots การส่งข้อมูลโดยไม่มีทางเลือกให้ปฏิเสธ (Opt-out) ควรมีมาตรการลงโทษทางปกครอง (Administrative

Fine) ที่รวดเร็วและเด็ดขาด แทนที่จะพึ่งพากระบวนการทางอาญาที่ล่าช้าเพียงอย่างเดียว เพื่อให้เกิดประสิทธิผลสูงสุด (Maximum Effectiveness) E. การประสานสอดคล้องกับกฎหมายอื่น (Harmonization) ต้องมีการปรับปรุงให้สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ฯ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) อย่างไร้รอยต่อ เพื่อไม่ให้เกิดการตีความที่ซ้ำซ้อน (Double Jeopardy) หรือความขัดแย้งในอำนาจหน้าที่ของพนักงานเจ้าหน้าที่

- ควรเพิ่มอัตราโทษสำหรับความผิดตามมาตราดังกล่าวให้มีความเหมาะสมมากขึ้น เนื่องจากปัจจุบันยังมีผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์อยู่ไม่น้อย ยกตัวอย่างเช่น คอลเซนเตอร์ สแกมเมอร์ ที่หลอกลวงประชาชนด้วยรูปแบบต่าง ๆ โดยไม่คำนึงถึงอัตราโทษที่จะได้รับและอาจมองว่ามีอัตราโทษที่น้อย จึงทำให้ผู้กระทะทำความผิดไม่มีความเกรงกลัวต่อบทลงโทษสำหรับการกระทำความผิดดังกล่าว

- มีความเหมาะสม เนื่องจากเป็นการกำหนดฐานความผิดที่มุ่งเน้นไปที่การกระทำต่อระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์โดยตรง ซึ่งถือว่ามีความจำเป็นและเหมาะสมในการปราบปรามอาชญากรรมทางเทคโนโลยี และมีการไล่ระดับโทษตามความร้ายแรงและความเสียหายที่เกิดขึ้น (ผู้ให้ความคิดเห็น : สำนักงานศาลยุติธรรม (เป็นหนังสือ))

ประเด็นที่ ๒ ฐานความผิด องค์ประกอบความผิด และอัตราโทษ ตามลักษณะที่ ๒ การใช้ระบบคอมพิวเตอร์กระทำความผิดอื่น (มาตรา ๑๔ - ๑๖ มาตรา ๒๔ และมาตรา ๒๖ - ๒๗) มีความเหมาะสม หรือสมควรได้รับการแก้ไขเพิ่มเติมหรือปรับปรุง หรือสมควรยกเลิกหรือไม่อย่างไร

ผลการรับฟังความคิดเห็น

(๑) มีความเหมาะสม จำนวน ๑๐๓ คน (ร้อยละ ๗๙.๒๓)

(๒) สมควรได้รับการแก้ไขเพิ่มเติมหรือปรับปรุง จำนวน ๒๗ คน (ร้อยละ ๒๐.๗๖)

(๓) สมควรยกเลิก ไม่มี

(๔) อื่น ๆ ไม่มี

นอกจากนี้ผู้เกี่ยวข้องมีความเห็นเพิ่มเติมที่น่าสนใจดังนี้

- ความผิดในส่วนนี้ สมควรได้รับการแก้ไขเพิ่มเติมหรือปรับปรุง ดังนี้ ๑. เพิ่มการจำกัดความของข้อมูลคอมพิวเตอร์ที่บิดเบือน / ปลอม / อันเป็นเท็จ ตามที่บัญญัติไว้ในมาตรา ๑๔ ให้มีความชัดเจนมากยิ่งขึ้น ๒. เพิ่มเหตุฉกรรจ์ของความผิดตามที่บัญญัติไว้ในมาตรา ๑๔ และมาตรา ๑๖ ในกรณีที่เป็นสื่อลามกอนาจารเด็ก และกรณี Cyberbullying ในลักษณะที่นอกเหนือจากความผิดที่จะบัญญัติไว้ในประมวลกฎหมายอาญา

- บทวิเคราะห์และแนวทางการปรับปรุงระดับยุทธศาสตร์ (Strategic Analysis & Enhancement) การแก้ไขปรับปรุงนี้ มิใช่การยกเลิกโดยสิ้นเชิง แต่เป็นการ "ยกระดับ" (Upgrade) กฎหมายให้มีความทันสมัย (Modernization) ทัดเทียมกับกฎหมายดิจิทัลของกลุ่มประเทศมหาอำนาจ (เช่น EU Digital Services Act, US Computer Fraud and Abuse Act หรือ Budapest Convention) เพื่อให้เกิดประสิทธิภาพสูงสุดในการบังคับใช้ และคุ้มครองสิทธิเสรีภาพตามรัฐธรรมนูญอย่างแท้จริง ๑. การปฏิรูปมาตรา ๑๔ แยกแยะ "เจตนาทุจริต" ออกจาก "การแสดงความคิดเห็น" (De-coupling Fraud from Speech) สถานะปัจจุบัน มาตรา ๑๔ (๑) และ (๒) มักถูก

ตีความอย่างกว้างขวางเพื่อใช้ดำเนินคดีหมิ่นประมาทออนไลน์ (Defamation) หรือการวิพากษ์วิจารณ์ ซึ่งอาจซ้ำซ้อนกับประมวลกฎหมายอาญาและขัดต่อเจตนารมณ์ดั้งเดิมที่มุ่งเน้นการหลอกลวงทางเทคนิค (เช่น Phishing, Scamming) แนวทางแก้ไขระดับสูง นิยามองค์ประกอบความผิดใหม่ต้องจำกัดวงของคำว่า "ข้อมูลอันเป็นเท็จ" หรือ "นิดเนือน" ให้มุ่งเน้นที่ "อาชญากรรมทางเศรษฐกิจและการฉ้อโกงทางเทคนิค" (Technical Fraud & Cyber Scams) อย่างชัดเจน เช่น การปลอมแปลงหน้าเว็บไซต์ธนาคาร การสร้างข้อมูลเท็จเพื่อล้วงข้อมูลส่วนบุคคล หากเป็นการกระทำที่เข้าข่ายหมิ่นประมาท หรือความผิดต่อชื่อเสียง ให้ไปใช้กฎหมายอาญาปกติหรือกฎหมายแพ่งเพื่อป้องกันการใช้ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ เป็นเครื่องมือในการปิดกั้นเสรีภาพในการแสดงออก (SLAPP Lawsuit) ซึ่งสอดคล้องกับมาตรา ๓๔ ของรัฐธรรมนูญ (เสรีภาพในการแสดงความคิดเห็น) Fake News และ Disinformation สำหรับมาตรา ๑๔ (๒) และ (๓) ที่เกี่ยวกับความมั่นคง ให้เพิ่มกลไกการพิสูจน์เจตนาพิเศษที่ต้องแสดงให้เห็นถึง "เจตนามุ่งร้ายเพื่อทำลายระบบความมั่นคงของรัฐอย่างเป็นระบบ" (Systematic Malicious Intent) ไม่ใช่เพียงการแชร์ข่าวลือโดยรู้เท่าไม่ถึงการณ์ เพื่อให้สอดคล้องกับมาตรฐานสากล ๒. การปฏิรูปมาตรา ๑๕ และ ๒๖ ความรับผิดของผู้ให้บริการและการเก็บรักษาข้อมูล (Intermediary Liability & Data Retention) สถานะปัจจุบัน ภาระของผู้ให้บริการ (ISP/Platform) ในการตรวจสอบเนื้อหาและการเก็บ Log ๙๐ วัน อาจไม่เพียงพอต่อเทคโนโลยีปัจจุบัน หรืออาจสร้างภาระเกินควรแก่ผู้ประกอบการรายย่อย Safe Harbor & Notice-and-Action ปรับปรุงมาตรา ๑๕ ให้สอดคล้องกับหลักการสากล (เช่น DMCA หรือ EU DSA) โดยสร้างกระบวนการ "แจ้งเตือนและนำออก" (Notice and Takedown) ที่มีมาตรฐานเวลาชัดเจน รวดเร็ว และมีกระบวนการโต้แย้งสิทธิ์ (Counter-notice) เพื่อความเป็นธรรม Data Retention (มาตรา ๒๖) ปรับปรุงระยะเวลาและประเภทข้อมูลที่ต้องเก็บ ให้รองรับ "Advanced Persistent Threats (APTs)" ซึ่งอาจต้องใช้เวลาสืบสวนนานกว่า ๙๐ วัน ในกรณีความมั่นคงร้ายแรง แต่ต้องแลกมาด้วยมาตรการคุ้มครองข้อมูลส่วนบุคคล (Data Privacy) ของ Log ที่เก็บรักษาไว้อย่างเข้มงวดตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) เพื่อไม่ให้กระทบสิทธิประชาชนเกินสมควร AI & Algorithm Accountability เพิ่มบทบัญญัติที่เอื้อต่อการตรวจสอบอัลกอริทึมของผู้ให้บริการแพลตฟอร์มขนาดใหญ่ กรณีที่มีการจงใจปล่อยให้เนื้อหาผิดกฎหมายแพร่ระบาดเพื่อผลกำไร ๓. การปฏิรูปมาตรา ๑๖ รองรับภัยคุกคามจาก AI และ Deepfakes (Synthetic Media Regulation) สถานะปัจจุบัน กฎหมายปัจจุบันพูดถึงการตัดต่อภาพแต่เทคโนโลยีไปไกลถึงการสร้างภาพและเสียงสังเคราะห์ (Deepfakes) ที่แนบเนียน ควรขยายคำนิยามแก้ไขให้ครอบคลุม "สื่อสังเคราะห์ด้วยปัญญาประดิษฐ์" (AI-Generated Content / Deepfakes) ทั้งภาพ เสียง และวิดีโอ เพิ่มอัตราโทษ กำหนดโทษหนักขึ้นกรณีใช้ Deepfake เพื่อการฉ้อโกง, การข่มขู่ทางเพศ (Non-consensual pornography), หรือการแทรกแซงกระบวนการยุติธรรมและการเลือกตั้ง เนื่องจากมีผลกระทบวงกว้างและรุนแรงกว่าการตัดต่อภาพแบบเดิม มาตรการทางปกครอง ให้อำนาจศาลสั่งลบหรือระงับการเข้าถึงเนื้อหา Deepfake ได้ทันที (Immediate Injunction) เพื่อระงับความเสียหาย โดยไม่ต้องรอผลคดีอาญา ๔. การปฏิรูปมาตรา ๒๔ และ ๒๗: การรักษาความลับและสภาพบังคับ (Secrecy & Enforcement) สถานะปัจจุบัน บทลงโทษสำหรับการฝ่าฝืนคำสั่งเจ้าพนักงานหรือศาล อาจไม่เพียงพอที่จะป้องปรามบริษัทข้ามชาติขนาดยักษ์ (Big Tech) มาตรการคว่ำบาตรทางปกครอง (Administrative Sanctions) ในมาตรา ๒๗ ควรเพิ่มโทษปรับทางปกครองที่คำนวณจาก "ร้อยละของรายได้ทั่วโลก" (Percentage of Global

Turnover) สำหรับนิติบุคคลที่ไม่ปฏิบัติตามคำสั่งศาลในการส่งมอบพยานหลักฐาน (เลียนแบบ GDPR) เพื่อให้กฎหมายมี "เขี้ยวเล็บ" ที่ศักดิ์สิทธิ์และทัดเทียมมหาอำนาจ ความโปร่งใสในการใช้อำนาจ (มาตรา ๒๔) การรักษาความลับของข้อมูลที่ได้มา ต้องมีกลไกตรวจสอบ (Audit) ว่าเจ้าหน้าที่รัฐไม่ได้นำข้อมูลไปใช้ในทางมิชอบ หรือเพื่อผลประโยชน์ทางการเมือง โดยให้มีหน่วยงานอิสระเข้าตรวจสอบได้ ๕. ความสอดคล้องกับรัฐธรรมนูญและหลักนิติธรรม (Constitutional Compliance) หลักความได้สัดส่วน (Proportionality) การแก้ไขทั้งหมดต้องผ่านการทดสอบว่า "จำกัดสิทธิเพียงเท่าที่จำเป็น" ตามมาตรา ๒๖ ของรัฐธรรมนูญ การลงโทษต้องไม่รุนแรงเกินกว่าเหตุ กระบวนการที่เป็นธรรม (Due Process) การใช้อำนาจตามกฎหมายคอมพิวเตอร์ต้องมีกระบวนการตรวจสอบถ่วงดุลโดยศาล (Judicial Review) อย่างเคร่งครัด ไม่ให้ฝ่ายบริหารใช้อำนาจเบ็ดเสร็จ

- มาตรา ๒๖ วรรคหนึ่ง และวรรคสอง เห็นควรขยายระยะเวลาการเก็บรักษา ๙๐ วัน เป็น ๑ ปี

- มีความเหมาะสม เนื่องจากความผิดในลักษณะที่ ๒ นี้ มิได้คุ้มครองเพียงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์โดยตรง แต่ครอบคลุมถึงการใช้ระบบคอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด อันส่งผลกระทบต่อบุคคล สาธารณะ หรือความสงบเรียบร้อยของประชาชน รวมถึงการคุ้มครองข้อมูลจราจรทางคอมพิวเตอร์และอำนาจเข้าถึงข้อมูลของเจ้าหน้าที่ ซึ่งถือเป็นมาตรการที่จำเป็นต่อการสืบสวนสอบสวนความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี และเป็นหลักการสำคัญที่ยังคงมีความจำเป็นในสภาพสังคมดิจิทัลปัจจุบัน (ผู้ให้ความคิดเห็น : สำนักงานศาลยุติธรรม (เป็นหนังสือ))

ประเด็นที่ ๓ อำนาจหน้าที่ในการดำเนินคดีของพนักงานเจ้าหน้าที่และศาล (มาตรา ๑๖/๑ มาตรา ๑๗ มาตรา ๑๗/๑ มาตรา ๑๘ - ๒๑ และมาตรา ๒๕) มีความเหมาะสม หรือสมควรได้รับการแก้ไขเพิ่มเติมหรือปรับปรุง หรือสมควรยกเลิกหรือไม่ อย่างไร

ผลการรับฟังความคิดเห็น

(๑) มีความเหมาะสม จำนวน ๑๐๒ คน (ร้อยละ ๗๘.๔๖)

(๒) สมควรได้รับการแก้ไขเพิ่มเติมหรือปรับปรุง จำนวน ๒๘ คน (ร้อยละ ๒๑.๕๓)

(๓) สมควรยกเลิก ไม่มี

(๔) อื่น ๆ ไม่มี

นอกจากนี้ผู้เกี่ยวข้องมีความเห็นเพิ่มเติมที่น่าสนใจดังนี้

- บทวิเคราะห์และข้อเสนอแนะเชิงลึกระดับสูงสุด (Comprehensive Strategic Legal Analysis) แม้ว่าบทบัญญัติในปัจจุบันจะวางรากฐานกระบวนการยุติธรรมทางอาญาในโลกไซเบอร์ไว้แล้ว แต่ด้วยบริบทของเทคโนโลยีที่มีพลวัตสูง (High Dynamics) และความซับซ้อนของภัยคุกคามทางไซเบอร์ที่ไร้พรมแดน (Borderless Cyber Threats) การจะยกระดับประเทศไทยให้มีมาตรฐานเทียบเท่ารัฐมหาอำนาจทางเทคโนโลยี และให้สอดคล้องกับรัฐธรรมนูญ มาตรา ๒๖ (การตรากฎหมายต้องไม่เพิ่มภาระเกินสมควร) และ มาตรา ๒๙ (สิทธิในกระบวนการยุติธรรม) จำเป็นต้องมีการ "Re-engineering" หรือปรับปรุงโครงสร้างอำนาจหน้าที่เชิงรุกและเชิงรับ ดังรายละเอียดต่อไปนี้ ๑. การยกระดับมาตรา ๑๘ - ๑๙: จาก "การยึดอายัดทางกายภาพ" สู่ "พยานหลักฐานดิจิทัลบนคลาวด์" (Digital & Cloud Forensics Transformation) สภาพปัจจุบัน อำนาจตามมาตรา ๑๘ ในการเข้าถึง ทำสำเนา หรือยึดระบบคอมพิวเตอร์ ยังยึดติดกับกรอบคิดเรื่อง "วัตถุพยานทางกายภาพ" (Physical Evidence) ซึ่งเจ้าหน้าที่ต้องขออำนาจศาลตามมาตรา ๑๙ เพื่อยึดอุปกรณ์

ความจำเป็นในการปรับปรุง อาชญากรรมปัจจุบันเกิดขึ้นบนระบบ Cloud Computing และ Decentralized Systems (เช่น Blockchain) การยึดอุปกรณ์ทางกายภาพ (Hardware) มักไม่พบข้อมูล หรือข้อมูลถูกเข้ารหัส (Encryption) ข้อเสนอแนะระดับสากล Remote Forensic Acquisition แก้ไขให้พนักงานเจ้าหน้าที่มีอำนาจ (ภายใต้คำสั่งศาลที่ตรวจสอบอย่างเข้มงวด) ในการเข้าถึงข้อมูลระยะไกล (Remote Access) หรือการทำสำเนาข้อมูลแบบ Live Forensics โดยไม่ต้องยึดตัวเครื่อง เพื่อลดผลกระทบต่อภาคธุรกิจตามรัฐธรรมนูญ มาตรา ๔๐ (เสรีภาพในการประกอบอาชีพ) และมาตรา ๓๗ (สิทธิในทรัพย์สิน) Data Preservation Orders เพิ่มมาตรการ "คำสั่งอายัดข้อมูลชั่วคราวแบบเร่งด่วน" (Quick Freeze) ไปยังผู้ให้บริการ (Service Providers) ทันทีที่เกิดเหตุก่อนที่จะขอหมายศาลเพื่อดึงข้อมูล เพื่อป้องกันการลบทำลายหลักฐาน ซึ่งสอดคล้องกับ Budapest Convention ๒. การปฏิรูปมาตรา ๒๐: ดุลยภาพระหว่าง "ความมั่นคงไซเบอร์" กับ "เสรีภาพในการแสดงออก" (Balancing Cybersecurity & Freedom of Expression) สภาพปัจจุบัน การระงับการทำให้แพร่หลาย (Block/Delete) ตามมาตรา ๒๐ ครอบคลุมทั้งเนื้อหาที่ผิดกฎหมายและเนื้อหาที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดี ซึ่งเป็นถ้อยคำกว้าง (Vague term) ความจำเป็นในการปรับปรุง เพื่อให้สอดคล้องกับรัฐธรรมนูญ มาตรา ๓๔ (เสรีภาพในการแสดงความคิดเห็น) และมาตรา ๓๕ (เสรีภาพสื่อมวลชน) อย่างแท้จริง และป้องกันข้อครหาเรื่องการใช้อำนาจเกินขอบเขต ข้อเสนอแนะระดับสากล Precision Targeting แก้ไขให้การระงับข้อมูลต้องระบุ URL หรือ Content ID อย่างจำเพาะเจาะจง (Specific) ห้ามการปิดกั้นแบบเหมาเข่ง (Blanket Ban) ทั้งโดเมนหรือทั้งแพลตฟอร์ม เว้นแต่พิสูจน์ได้ว่าทั้งระบบถูกสร้างมาเพื่ออาชญากรรม Judicial Review Enhancement ศาลควรมีหน่วยงานเทคนิคอิสระ (Independent Technical Advisor) ช่วยพิจารณาคำร้องขอปิดกั้นเว็บไซต์ เพื่อตรวจสอบว่าข้อมูลนั้นกระทบความมั่นคงจริงหรือไม่ ไม่ใช่พิจารณาเพียงตามเอกสารของเจ้าหน้าที่ฝ่ายบริหารเพียงฝ่ายเดียว ๓. การขยายขอบเขตมาตรา ๑๗ เขตอำนาจศาลเหนือดินแดนดิจิทัล (Extraterritorial Jurisdiction & Cross-Border Efficiency) สภาพปัจจุบัน มาตรา ๑๗ กำหนดให้ลงโทษผู้กระทำผิดนอกราชอาณาจักรได้ แต่กระบวนการนำตัวมาลงโทษหรือขอพยานหลักฐานยังต้องพึ่งพา พระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา ซึ่งล่าช้ามาก ความจำเป็นในการปรับปรุง อาชญากรคอมพิวเตอร์มักใช้ Server ในต่างประเทศ หรือเป็นคนต่างชาติโจมตีระบบไทย ข้อเสนอแนะระดับสากล Direct Cooperation Mechanism แก้ไขเพิ่มเติมให้มีช่องทางพิเศษในการขอพยานหลักฐานดิจิทัลจากผู้ให้บริการแพลตฟอร์มระดับโลก (เช่น Facebook, Google, Line) ได้โดยตรง (คล้าย US CLOUD Act) โดยผ่านการตรวจสอบของศาลไทย เพื่อความรวดเร็วและเป็นที่ยอมรับในระดับสากล Long-Arm Statute ขยายขอบเขตอำนาจศาลให้ชัดเจนครอบคลุมถึง "ผลการกระทำ" ที่เกิดขึ้นในไทย แม้ตัวการจะอยู่ต่างประเทศ เพื่อรองรับธุรกรรม Digital Asset และ DeFi ๔. การปรับปรุงมาตรา ๑๖/๑ และ ๒๕ มาตรฐานการพิสูจน์และการคุ้มครองข้อมูลส่วนบุคคล (Standard of Proof & Privacy Protection) สภาพปัจจุบัน มาตรา ๑๖/๑ ให้อำนาจศาลสั่งทำลายข้อมูล และมาตรา ๒๕ ห้ามรับฟังพยานหลักฐานที่ได้มาโดยมิชอบ ความจำเป็นในการปรับปรุง ในยุค AI และ Deepfake การพิสูจน์ความแท้จริงของพยานหลักฐาน (Authentication) ยากขึ้น และการเก็บ Log ตามมาตรา ๒๖ อาจละเมิดรัฐธรรมนูญ มาตรา ๓๒ (สิทธิในความเป็นอยู่ส่วนตัว) หากไม่มีการควบคุม ข้อเสนอแนะระดับสากล Chain of Custody via Blockchain กำหนดมาตรฐานทางกฎหมายให้การเก็บรวบรวมพยานหลักฐานดิจิทัลต้องมีการ Hash และบันทึกลง Blockchain หรือระบบที่แก้ไขไม่ได้ เพื่อยืนยัน

ความถูกต้องแท้จริงในชั้นศาล Privacy by Design แก้ไขกระบวนการได้มาซึ่งข้อมูลจราจรคอมพิวเตอร์ ต้องคำนึงถึงหลักความจำเป็นและได้สัดส่วน (Necessity and Proportionality) ตามหลัก GDPR และ PDPA ของไทย เพื่อไม่ให้กระทบสิทธิประชาชนเกินความจำเป็น ๕. การสร้าง "ศาลชำนัญพิเศษทางไซเบอร์" (Specialized Cyber Court) ข้อเสนอเพิ่มเติม แม้กฎหมายจะให้อำนาจศาลยุติธรรมตามปกติ (มาตรา ๑๘๘ รัฐธรรมนูญ) แต่เพื่อประสิทธิภาพสูงสุด ควรมีการกำหนดแผนกคดีไซเบอร์ที่มีผู้พิพากษาที่มีความรู้เชิงเทคนิคระดับสูง หรืออนุญาตให้ใช้ระบบ AI-Assisted Legal Analytics ช่วยวิเคราะห์พยานหลักฐานจำนวนมหาศาล (Big Data) ในคดีคอมพิวเตอร์เพื่อความรวดเร็วและแม่นยำ

- มีความเหมาะสมในหลักการ เนื่องจากอำนาจหน้าที่ในการดำเนินคดีของพนักงานเจ้าหน้าที่และศาลดังกล่าวยังคงมีความจำเป็นในทางปฏิบัติ เพื่อให้รัฐสามารถรับมือกับอาชญากรรมทางเทคโนโลยีซึ่งเป็นความผิดที่มีลักษณะพิเศษได้อย่างมีประสิทธิภาพ การกำหนดให้การใช้อำนาจของพนักงานเจ้าหน้าที่ส่วนใหญ่ได้รับคำสั่งอนุญาตจากศาลก่อนก็เพื่อป้องกันการใช้อำนาจโดยมิชอบ ซึ่งเป็นไปตามหลักการถ่วงดุลอำนาจและเพื่อคุ้มครองสิทธิของประชาชน นอกจากนั้น การขยายอำนาจศาลไทยตามมาตรา ๑๗ จะช่วยให้การบังคับใช้กฎหมายมีความครอบคลุมถึงความผิดที่กระทำนอกราชอาณาจักรแต่มีผลกระทบในราชอาณาจักรด้วย ซึ่งสอดคล้องกับลักษณะของอาชญากรรมทางเทคโนโลยีที่เป็นเครือข่ายข้ามพรมแดน (ผู้ให้ความคิดเห็น : สำนักงานศาลยุติธรรม (เป็นหนังสือ))

ประเด็นที่ ๔ บทกำหนดโทษ (มาตรา ๑๒ มาตรา ๑๒/๑ มาตรา ๑๖/๒ และมาตรา ๒๒ - ๒๓) มีความเหมาะสม หรือสมควรได้รับการแก้ไขเพิ่มเติมหรือปรับปรุง หรือสมควรยกเลิกหรือไม่อย่างไร

ผลการรับฟังความคิดเห็น

(๑) มีความเหมาะสม จำนวน ๑๐๘ คน (ร้อยละ ๘๓.๐๗)

(๒) สมควรได้รับการแก้ไขเพิ่มเติมหรือปรับปรุง จำนวน ๒๒ คน (ร้อยละ ๑๖.๙๒)

(๓) สมควรยกเลิก ไม่มี

(๔) อื่น ๆ ไม่มี

นอกจากนี้ผู้เกี่ยวข้องมีความเห็นเพิ่มเติมที่น่าสนใจดังนี้

- บทกำหนดโทษในส่วนนี้ ควรเพิ่มเหตุฉกรรจ์ของความผิดตามที่บัญญัติไว้ในมาตรา ๑๒ และมาตรา ๑๒/๑ ให้ครอบคลุมถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับภารกิจหรือบริการภาครัฐ และข้อมูลคอมพิวเตอร์ที่มีลักษณะเป็นข้อมูลส่วนบุคคล / ข้อมูลส่วนบุคคลที่มีความอ่อนไหว ซึ่งยังไม่ถึงขนาดว่าเป็นข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ โดยผู้กระทำจะต้องรับโทษหนักขึ้นกว่ากรณีทั่วไป แต่ยังเบากว่ากรณีเหตุฉกรรจ์ที่บัญญัติไว้แต่เดิม

- ๑. การยกระดับมาตรา ๑๒ และ ๑๒/๑ (ความมั่นคงและโครงสร้างพื้นฐานสำคัญ) สถานะปัจจุบัน บทบัญญัตินี้เน้นการลงโทษผู้ที่กระทำต่อข้อมูลหรือระบบที่เกี่ยวกับความมั่นคง, ความปลอดภัยสาธารณะ, หรือบริการสาธารณะ (Critical Information Infrastructure - CII) โดยมีโทษจำคุกสูงถึง ๑๐-๒๐ ปี หรือจำคุกตลอดชีวิตในกรณีทำให้ผู้อื่นถึงแก่ความตาย เหตุผลในการ

ปรับปรุง (Rationale for Optimization) นิยามความมั่นคงที่ทันสมัย (Redefining Security) ในบริบทของรัฐมหาอำนาจ นิยามของ "ความมั่นคง" ต้องแยกแยะระหว่าง "Cyber Terrorism" (การก่อการร้ายไซเบอร์) กับ "Hacktivism" หรือ "White Hat Hacking" (การแฮ็กเพื่อทดสอบระบบโดยเจตนาดีแต่ขาดกระบวนการ) ให้ชัดเจนยิ่งขึ้น เพื่อให้การบังคับใช้กฎหมายมีความ "แม่นยำ" (Precision) ไม่เหวี่ยงแห มาตรการลงโทษเชิงสมานฉันท์และเศรษฐกิจ (Restorative and Economic Sanctions) โทษจำคุกเพียงอย่างเดียวอาจไม่ใช่ "ประสิทธิผลสูงสุด" สำหรับอาชญากรไซเบอร์ที่มีทักษะสูง ควรพิจารณาเพิ่มบทลงโทษทางเศรษฐกิจที่รุนแรงกว่าเดิม (เช่น ค่าปรับที่ผันแปรตามความเสียหายทางเศรษฐกิจจริง หรือ % ของรายได้ในกรณีองค์กร) และมาตรการคุมประพฤติทางดิจิทัล (Digital Probation) เพื่อนำทักษะของบุคคลเหล่านี้กลับมาใช้ประโยชน์แก่รัฐภายใต้การควบคุม (State-Sanctioned Reformation) การสอดคล้องกับกฎหมายความมั่นคงปลอดภัยไซเบอร์ ต้องมีการเชื่อมโยงบทลงโทษให้สอดรับกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างไร้รอยต่อ เพื่อไม่ให้เกิดความซ้ำซ้อน (Double Jeopardy) หรือช่องว่างทางกฎหมาย (Legal Loophole) ๒. การสังคายนากระบวนทัศน์ในมาตรา ๑๖/๒ (การครอบครองข้อมูลที่ศาลสั่งทำลาย) สถานะปัจจุบัน เอาผิดผู้ที่รู้ว่าข้อมูลคอมพิวเตอร์ในความครอบครองของตนเป็นข้อมูลที่ศาลสั่งให้ทำลายตามมาตรา ๑๖/๑ แต่ไม่ยอมทำลาย เหตุผลในการปรับปรุง (Rationale for Optimization) ความเป็นจริงทางเทคนิค (Technical Reality of "Deletion") ในยุค Cloud Computing และ Distributed Ledger Technology (DLT) การ "ทำลาย" ข้อมูลให้สิ้นซากเป็นเรื่องทางเทคนิคที่ซับซ้อนมาก บางครั้งข้อมูลอาจถูกสำรองอัตโนมัติ (Auto-backup) ใน Server ต่างประเทศที่ผู้ใช้ควบคุมไม่ได้ เจตนาพิเศษ (Specific Intent) ควรปรับปรุงบทลงโทษโดยเน้นที่ "เจตนาในการนำกลับมาใช้ใหม่" หรือ "เจตนาในการเผยแพร่ต่อ" มากกว่าเพียงแค่ "การครอบครองทางเทคนิค" เพื่อให้เกิดความเป็นธรรมและคุ้มครองสิทธิของประชาชนตามรัฐธรรมนูญ มาตรา ๒๙ (บุคคลไม่ต้องรับโทษอาญา เว้นแต่ได้กระทำการอันกฎหมายบัญญัติเป็นความผิด) กลไกทางปกครอง (Administrative Mechanism) ควรเพิ่มมาตรการทางปกครองหรือคำสั่งทางเทคนิคให้ผู้ให้บริการ (Service Providers) เข้ามามีส่วนร่วมในการทำลายข้อมูล แทนที่จะผลักภาระและโทษอาญาไปที่ผู้ใช้บริการเพียงฝ่ายเดียว ซึ่งจะสอดคล้องกับหลักสากลในการจัดการ Content Moderation ๓. การปฏิรูปมาตรา ๒๒ - ๒๓ (ความรับผิดของพนักงานเจ้าหน้าที่) สถานะปัจจุบัน ลงโทษพนักงานเจ้าหน้าที่ที่เปิดเผยหรือประมาทเลินเล่อทำให้ข้อมูลที่ได้มาจากการปฏิบัติหน้าที่รั่วไหล เหตุผลในการปรับปรุง (Rationale for Optimization) ความสมดุลแห่งอำนาจ (Checks and Balances) ในยุคที่ข้อมูลส่วนบุคคลมีค่าดั่งน้ำมัน (Data is the new oil) โทษจำคุก ๓ ปี (ม.๒๒) หรือ ๑ ปี (ม.๒๓) อาจถือว่า "เบาเกินไป" (Too Lenient) เมื่อเทียบกับความเสียหายที่อาจเกิดขึ้นกับประชาชนจากการรั่วไหลของข้อมูลโดยเจ้าหน้าที่รัฐ การบูรณาการกับ PDPA ต้องปรับปรุงบทลงโทษให้มีความสอดคล้องและรุนแรงเทียบเท่าหรือสูงกว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) เพื่อยกระดับมาตรฐานความรับผิดชอบของรัฐ (State Accountability) ให้ทัดเทียมอารยประเทศ ความรับผิดทางวินัยและแพ่ง (Disciplinary and Civil Liability) ควรระบุให้ชัดเจนถึงกระบวนการชดเชยค่าเสียหายแก่ประชาชนผู้ได้รับผลกระทบโดยทันที (Fast-track Compensation) โดยไม่ต้องรอผลคดีอาญา เพื่อให้เกิด "คุณภาพสูงสุด" ในการเยียวยาผู้เสียหายตามรัฐธรรมนูญ

- มีความเหมาะสม และสอดคล้องกับวัตถุประสงค์ของกฎหมายในการป้องปรามและลงโทษผู้กระทำความผิดทางไซเบอร์ที่มีผลกระทบรุนแรง การเพิ่มโทษสำหรับความผิดร้ายแรงตามมาตรา ๑๒

และ ๑๒/๑ โดยกำหนดอัตราโทษที่สูงขึ้นตามระดับความเสียหายที่เกิดขึ้น โดยเฉพาะกรณีที่เกี่ยวข้องกับความมั่นคงของประเทศหรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะสำคัญของประเทศ ซึ่งสร้างความเสียหายที่ร้ายแรงกว่าอาชญากรรมคอมพิวเตอร์ทั่วไป (ผู้ให้ความคิดเห็น : สำนักงานศาลยุติธรรม (เป็นหนังสือ))

ประเด็นที่ ๕ ความคิดเห็นหรือข้อเสนอแนะอื่น ๆ (ถ้ามี)

- ๑. การปรับปรุงนิยามและขอบเขตกฎหมาย (Substantive Law Enhancement) เพื่อให้กฎหมายมีความทันสมัย (Modernization) และรองรับเทคโนโลยีอนาคต (Future-Proofing) เช่น AI, Quantum Computing, Blockchain และ Metaverse ๑.๑ การแยกแยะ "อาชญากรรมทางไซเบอร์โดยเนื้อแท้" (Pure Cybercrime) ออกจาก "อาชญากรรมทางเนื้อหา" (Content-related Crime) ข้อเสนอ ควรจำกัดความผิดตามพระราชบัญญัติคอมพิวเตอร์ฯ ให้เน้นหนักที่การกระทำต่อระบบและข้อมูล (System Interference & Data Interference) เช่น การแฮก (Hacking), การดักรับข้อมูล (Interception), และการปล่อยมัลแวร์ (Malware) ตามมาตรา ๕-๑๐ และ ๑๒-๑๓ ให้มีความเข้มข้นสูงสุดเทียบเท่ามาตรฐานอนุสัญญาบูดาเปสต์ (Budapest Convention) เพื่อป้องกันการใช้กฎหมายนี้ดำเนินคดีกับการแสดงความคิดเห็น (Freedom of Expression) ซึ่งควรบังคับใช้ด้วยกฎหมายหมิ่นประมาทปกติหรือกฎหมายแพ่ง เพื่อให้สอดคล้องกับรัฐธรรมนูญ มาตรา ๓๔ (เสรีภาพในการแสดงความคิดเห็น) และมาตรา ๒๖ (การจำกัดสิทธิเสรีภาพต้องไม่กระทบกระเทือนสาระสำคัญแห่งสิทธิ) การปรับปรุงมาตรา ๑๔ ต้องระบุให้ชัดเจนว่า "ข้อมูลคอมพิวเตอร์อันเป็นเท็จ" หรือ "นิดเนือน" นั้น ต้องเป็นการกระทำที่มีเจตนาทุจริตในทางเทคนิค (Technical Fraud) เช่น Phishing, Spoofing หรือการปลอมแปลงตัวตนทางดิจิทัลเพื่อฉ้อโกงทรัพย์สิน ไม่ใช่การตีความรวมถึงการแสดงความเห็นต่างทางการเมืองหรือการวิพากษ์วิจารณ์โดยสุจริต ๑.๒ การนิยาม "ผู้ให้บริการ" (Service Provider) ในยุค Cloud & Edge Computing ข้อเสนอ ปรับนิยามในมาตรา ๓ ให้ครอบคลุมถึงผู้ให้บริการ Cloud, IoT Platform และ Decentralized Services แต่จำกัดความรับผิด (Limitation of Liability) ตามหลักการ Safe Harbor แบบสากล คือ ผู้ให้บริการไม่ต้องรับผิดในเนื้อหาที่ผู้ใช้นำเข้า เว้นแต่จะได้รับแจ้งและเพิกเฉย (Notice and Takedown) สอดคล้องกับหลักการประกอบธุรกิจเสรีและการแข่งขันที่เป็นธรรมตามรัฐธรรมนูญ มาตรา ๔๐ และมาตรา ๗๗ ที่รัฐไม่ควรสร้างภาระแก่เอกชนเกินความจำเป็น ๒. กระบวนการยุติธรรมทางอาญาและพยานหลักฐานดิจิทัล (Criminal Procedure & Digital Evidence) เพื่อให้การบังคับใช้กฎหมายมีความคล่องตัว (Agility) และมีประสิทธิภาพสูงสุด (Highest Efficiency) ๒.๑ การให้อำนาจเจ้าพนักงานและการตรวจสอบถ่วงดุล (Checks and Balances) ข้อเสนอ การใช้อำนาจตามมาตรา ๑๘, ๑๙ (การเข้าถึงข้อมูล, ยึดอายัด) ต้องผ่านการพิจารณาจากศาลที่มีความเชี่ยวชาญเฉพาะด้าน (Specialized Judges) หรือ "แผนกคดีดิจิทัล" เพื่อให้การออกหมายศาลเป็นไปอย่างรวดเร็วแต่รอบคอบ นำระบบ e-Warrant (หมายศาลอิเล็กทรอนิกส์) มาใช้เต็มรูปแบบ เชื่อมโยงระหว่างพนักงานเจ้าหน้าที่และศาล เพื่อลดระยะเวลาจาก "วัน" เหลือเพียง "นาที" ในกรณีเร่งด่วน โดยยังคงไว้ซึ่งการตรวจสอบตามรัฐธรรมนูญ มาตรา ๒๘ (การค้นหรือจับต้องมีหมายศาล) ๒.๒ การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ (Data Retention - มาตรา ๒๖) ข้อเสนอ ปรับปรุงจาก "การเก็บข้อมูลแบบเหวี่ยงแห" (Blanket Retention) เป็น "การเก็บข้อมูลตามความเสี่ยง" (Risk-based Retention) หรือ "Quick Freeze" (สั่งให้เก็บเฉพาะรายเมื่อมีเหตุสงสัย) เพื่อลดต้นทุนของผู้ประกอบการและลดความเสี่ยงในการรั่วไหลของข้อมูลส่วนบุคคล สอดคล้องกับรัฐธรรมนูญ

มาตรา ๓๒ (สิทธิในความเป็นอยู่ส่วนตัว) และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) ๓. การระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ (Website Blocking/Takedown) เพื่อให้เกิดประสิทธิผลสูงสุดในการจัดการภัยคุกคาม ควบคู่กับความโปร่งใส (Transparency) ๓.๑ กระบวนการตามมาตรา ๒๐ ข้อเสนอ คณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์ ต้องมีความหลากหลายและเป็นอิสระทางวิชาการอย่างแท้จริง การสั่งระงับต้องมี "Due Process" คือ เปิดโอกาสให้เจ้าของข้อมูลโต้แย้งได้ (เว้นแต่กรณีฉุกเฉินร้ายแรง) และคำสั่งศาลต้องระบุ URL หรือเนื้อหาที่ชัดเจน ไม่ใช่การปิดกั้นทั้งโดเมน (Platform Blocking) ซึ่งเกินกว่าเหตุ สอดคล้องกับหลักความได้สัดส่วน (Proportionality) ตามรัฐธรรมนูญ มาตรา ๒๖ ๔. การบูรณาการข้ามพรมแดน (International Cooperation & Jurisdiction) ยกระดับสู่ความเป็นมหาอำนาจทางดิจิทัล (Digital Powerhouse) ๔.๑ สภาพบังคับนอกราชอาณาจักร (Extraterritorial Jurisdiction) ข้อเสนอ พัฒนากลไกความร่วมมือระหว่างประเทศทางอาญา (MLAT) ในรูปแบบดิจิทัล (Digital MLAT) เพื่อให้สามารถขอพยานหลักฐานจากผู้ให้บริการแพลตฟอร์มระดับโลก (เช่น Facebook, Google) ได้อย่างรวดเร็ว โดยรัฐบาลไทยควรเข้าร่วมเป็นภาคีในอนุสัญญาบูดาเปสต์ (Budapest Convention) อย่างเป็นทางการ เพื่อให้ได้รับการยอมรับและแลกเปลี่ยนข้อมูลข่าวกรองภัยไซเบอร์กับนานาชาติได้อย่างเท่าเทียม สอดคล้องกับรัฐธรรมนูญ มาตรา ๕๒ (รัฐต้องพิทักษ์รักษาผลประโยชน์ของชาติ) และมาตรา ๖๖ (ความร่วมมือกับองค์การระหว่างประเทศ) ๕. มาตรการเชิงรุกและการสร้างภูมิคุ้มกัน (Proactive Measures & Immunity) ๕.๑ การคุ้มครองนักวิจัยความปลอดภัย (White Hat Hacker Protection) ข้อเสนอ แก้ไขเพิ่มเติมให้มีบทยกเว้นโทษทางอาญาสำหรับนักวิจัยหรือผู้เชี่ยวชาญที่เจาะระบบเพื่อตรวจสอบช่องโหว่ (Vulnerability Assessment) และรายงานให้เจ้าของระบบทราบโดยสุจริต (Good Faith) เพื่อส่งเสริมระบบนิเวศความมั่นคงปลอดภัยไซเบอร์ของชาติ เหตุผล กฎหมายปัจจุบันอาจตีความว่าการกระทำดังกล่าวผิดมาตรา ๕ หรือ ๗ ซึ่งขัดขวางการพัฒนานวัตกรรม ๕.๒ กองทุนพัฒนาและเยียวยา ข้อเสนอ ใช้กลไกจากมาตรา ๓๑ (ค่าใช้จ่าย) จัดตั้ง "กองทุนความมั่นคงปลอดภัยไซเบอร์" เพื่อเยียวยาประชาชนที่ตกเป็นเหยื่ออาชญากรรมคอมพิวเตอร์ (เช่น เหยื่อ Call Center, Phishing) และสนับสนุนการวิจัยพัฒนานวัตกรรมป้องกันปราบปราม สอดคล้องกับรัฐธรรมนูญ มาตรา ๗๘ (ส่งเสริมการพัฒนาวิทยาศาสตร์เทคโนโลยี)

- ๑) การบูรณาการเรื่องการยืนยันตัวตน (KYC): ขอเสนอให้มีการเชื่อมโยงมาตรฐาน "การพิสูจน์และยืนยันตัวตนทางดิจิทัล" ตามประกาศกระทรวงฯ ฉบับปี ๒๕๖๔ (ข้อ ๘) ให้สอดคล้องกับ "การตรวจสอบอัตลักษณ์บุคคล" ในการจดทะเบียนซิมการ์ดของ กสทช. เพื่อปิดช่องว่างไม่ให้คนร้ายใช้ข้อมูลปลอมในการเปิดใช้บริการทั้งฝั่งคอมพิวเตอร์และโทรคมนาคม ๒) ปัญหา SMS Spam/Scam: ควรมีการระบุให้ชัดเจนในกฎหมายลูกหรือประกาศกระทรวงฯ ว่าการส่ง SMS Spam หรือข้อความรบกวนจำนวนมากโดยไม่มีระบบให้ผู้รับปฏิเสธได้ง่าย (Opt-out) ตามมาตรา ๑๑ นั้น ผู้ให้บริการ (Telco) มีอำนาจระงับได้ทันทีหากตรวจพบ Pattern ที่ผิดปกติ โดยไม่ต้องกลัวว่าจะผิดสัญญาการให้บริการ ๓) การนิยาม "ผู้ให้บริการ": ควรระบุให้ชัดเจนว่าผู้ให้บริการ VoIP หรือ OTT (Over-the-Top) ที่ให้บริการโทรเสียงผ่านอินเทอร์เน็ต ต้องอยู่ภายใต้บังคับของมาตรา ๒๖ (เก็บ Log) อย่างเคร่งครัด เนื่องจากปัจจุบันอาชญากรรมส่วนใหญ่ย้ายฐานจากการโทรผ่านซิมปกติไปเป็นการโทรผ่านแอปพลิเคชันหรือ VoIP จากต่างประเทศ ทำให้ยากต่อการติดตามตัว

- ควรมีการกำหนดบทนิยามศัพท์เป็นการเพิ่มเติมเพื่อให้ลดปัญหาในการตีความ เช่น คอมพิวเตอร์ การเข้าถึง การนำเข้า การบิดเบือนข้อมูล ข้อมูลปลอม เป็นต้น/อาจปรับแก้ไข

ความหมายของนิยามคำว่าระบบคอมพิวเตอร์ให้ชัดเจนขึ้นว่าหมายความถึงอุปกรณ์อิเล็กทรอนิกส์หรือสมาร์ทโฟนด้วย

- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ยังมีความจำเป็น เนื่องจากพระราชบัญญัติฉบับดังกล่าวมีวัตถุประสงค์เพื่อกำหนดมาตรการทางกฎหมายที่เหมาะสมและมีประสิทธิภาพ ในการรับมือกับอาชญากรรมที่เกิดขึ้นจากการใช้เทคโนโลยีคอมพิวเตอร์และสารสนเทศ การมีกฎหมายที่ทันสมัยและครอบคลุมทำให้อาชญากรรมทางเทคโนโลยีได้รับการจัดการอย่างมีประสิทธิภาพ ไม่ว่าจะเป็นอาชญากรรมที่กระทำต่อระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ หรือการใช้คอมพิวเตอร์เป็นเครื่องมือประกอบอาชญากรรม เป็นการสร้างความเชื่อมั่นให้แก่ประชาชนในการใช้เทคโนโลยีสารสนเทศในชีวิตประจำวัน และช่วยให้ประเทศมีความพร้อมในการรับมือกับความก้าวหน้าทางเทคโนโลยีได้อย่างมีประสิทธิภาพ (ผู้ให้ความคิดเห็น : กรมทรัพย์สินทางปัญญา (เป็นหนังสือ))

- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ยังคงมีความเหมาะสมกับสภาพการณ์ปัจจุบัน (ผู้ให้ความคิดเห็น : สำนักงานอัยการสูงสุด (เป็นหนังสือ))

- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ มีความเหมาะสมตามประเด็นการรับฟังความคิดเห็น (ผู้ให้ความคิดเห็น : สำนักงานคณะกรรมการคุ้มครองผู้บริโภค (เป็นหนังสือ))

- ๑. ควรเพิ่มฐานความผิดสำหรับการกระทำที่เป็นการกลั่นแกล้งทางไซเบอร์ (Cyberbullying) และควรให้ศาลมีอำนาจสั่งระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ที่เป็นการกลั่นแกล้งทางไซเบอร์ได้ เพื่อเป็นการระงับมิให้ความเสียหายแพร่ออกไปในวงกว้าง ๒. ควรให้ศาลมีอำนาจสั่งระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ที่แม้จะไม่ถึงขั้นเป็นข้อมูลเท็จหรือปลอม และไม่ถึงขนาดน่าจะเกิดความเสียหายต่อความมั่นคงทางเศรษฐกิจของประเทศ แต่มีผลให้เกิดการกระทำอันไม่เป็นธรรมในตลาด (Market Manipulation) ไม่ว่าจะเป็นตลาดหลักทรัพย์ (Securities Market) หรือศูนย์ซื้อขายคริปโทเคอร์เรนซี (Crypto Exchange) โดยเฉพาะอย่างยิ่งข้อมูลคอมพิวเตอร์โดยผู้ที่เป็นอินฟลูเอนเซอร์ด้านการเงินและการลงทุน (Finfluencer) ๓. ควรเพิ่มฐานความผิดสำหรับผู้ใช้ปัญญาประดิษฐ์ในการสร้างข้อมูลคอมพิวเตอร์ หรือผู้ที่เกี่ยวข้องกับ Agentic AI ให้มีความรับผิดหากข้อมูลคอมพิวเตอร์ที่เกิดจากปัญญาประดิษฐ์ (AI – Generated Content) ปลอมหรือเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ๔. เนื่องจากความผิดตามพระราชบัญญัตินี้มีความจำเป็นต้องใช้พยานหลักฐานอิเล็กทรอนิกส์ในการพิสูจน์ความผิด ประกอบกับราชอาณาจักรไทยร่วมลงนามอนุสัญญาสหประชาชาติต่อต้านอาชญากรรมไซเบอร์ (UN Convention against Cybercrime) จึงควรกำหนดขั้นตอนการยึดหรืออายัดระบบคอมพิวเตอร์ของพนักงานเจ้าหน้าที่อันเป็นแนวทางปฏิบัติที่ดี (Best Practice) โดยเฉพาะอย่างยิ่งเรื่องห่วงโซ่พยานหลักฐาน (Chain of Custody) เพื่อประโยชน์ในด้านนิติวิทยาดิจิทัล (Digital Forensics) การสืบพยานในชั้นศาล และการปฏิบัติตามอนุสัญญาระหว่างประเทศในการแบ่งปันข้อมูลและพยานหลักฐานอิเล็กทรอนิกส์ ๕. ผู้มีอำนาจยื่นคำร้องตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ มาตรา ๒๐ วรรคหนึ่ง กำหนดให้เจ้าพนักงานที่ได้รับความเห็นชอบของรัฐมนตรีเท่านั้นที่มีอำนาจยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจ ขอให้มีการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์นั้นออกจากระบบ

คอมพิวเตอร์ได้ จึงมีลักษณะเป็นคดีที่รัฐเท่านั้นเป็นผู้เสียหาย เป็นผลให้เกิดปัญหาในทางปฏิบัติ คือ ราษฎรที่ได้รับความเสียหายจากการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่มีความจำเป็นต้องได้รับการบรรเทาความเสียหายอย่างรวดเร็ว เช่น กรณีราษฎรที่ถูกนำภาพถ่ายของตนไปตัดต่อเป็นภาพลามกอนาจาร แต่ไม่อาจยื่นคำร้องต่อศาลตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ มาตรา ๒๐ ได้โดยตรง จึงควรกำหนดให้ฐานความผิดบางฐาน เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ มาตรา ๑๖ เป็นความผิดที่ราษฎรได้รับความเสียหายเป็นพิเศษ เพื่อให้สามารถยื่นคำร้องโดยตรงต่อศาลตามมาตรา ๒๐ (๑) ได้

๖. กระบวนการบังคับให้เป็นไปตามคำสั่งศาลที่ให้ระงับการทำให้แพร่หลายหรือลบข้อมูล ศาลจะระบุให้ผู้ร้องต้องรายงานผลการปฏิบัติตามคำสั่งภายใน ๗ วัน นับแต่วันอ่านคำสั่ง ซึ่งในทางปฏิบัติยังไม่ปรากฏการรายงานผลการระงับหรือปิดกั้นข้อมูลทางเว็บไซต์จากทางผู้ร้องแต่อย่างใด จึงควรกำหนดระยะเวลาให้ผู้ร้องบังคับคดีตามคำสั่งศาลและกำหนดให้รายงานผลการบังคับตามคำสั่งให้ศาลทราบในกฎหมายอย่างชัดเจน (ผู้ให้ความคิดเห็น : สำนักงานศาลยุติธรรม (เป็นหนังสือ))

- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม มีขึ้นเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นจากพฤติกรรมที่ไม่ชอบด้วยกฎหมายและอาชญากรรมบนระบบคอมพิวเตอร์ที่กฎหมายทั่วไปอาจคุ้มครองไปไม่ถึง เช่น การเข้าถึงโดยมิชอบซึ่งระบบหรือข้อมูลคอมพิวเตอร์ การดักข้อมูล การทำลายข้อมูล หรือการโจมตีระบบคอมพิวเตอร์ พระราชบัญญัติฯ จึงกำหนดนิยามพื้นฐานขึ้น ได้แก่ ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ และข้อมูลจราจรคอมพิวเตอร์ เพื่อเป็นพื้นฐานหลักในการบังคับใช้กฎหมาย รวมถึงกำหนดความผิดที่เกี่ยวข้องกับความมั่นคงของระบบคอมพิวเตอร์ ความสมบูรณ์ของข้อมูล การรบกวนระบบคอมพิวเตอร์ การเผยแพร่ข้อมูลอันเป็นเท็จ หรือสื่อลามกอนาจาร ตลอดจนการกำหนดโทษสูงขึ้นในกรณีที่ความเสียหายกระทบไปถึงความมั่นคงของรัฐ อีกทั้งยังกำหนดให้ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์มีหน้าที่เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์และดำเนินการลบหรือระงับข้อมูลผิดกฎหมาย อันเป็นการสร้างกลไกความร่วมมือระหว่างหน่วยงานของรัฐและเอกชนในการควบคุมดูแลความปลอดภัยทางไซเบอร์ ซึ่งการมีพระราชบัญญัติฯ ส่งผลให้มาตรการคุ้มครองและป้องกันความเสียหายที่เกิดขึ้นจากความผิดเกี่ยวกับคอมพิวเตอร์ของประเทศไทยมีมาตรฐานเป็นสากล อันเป็นการสร้างความเชื่อมั่นต่อเศรษฐกิจดิจิทัล และเป็นการเสริมสร้างความมั่นใจให้แก่ผู้ประกอบการและผู้ใช้บริการว่าจะได้รับความคุ้มครองจากความเสียหายที่เกิดขึ้นจากความผิดเกี่ยวกับคอมพิวเตอร์ ดังนั้น จึงเห็นควรให้มีการบังคับใช้พระราชบัญญัติฯ ต่อไป (ผู้ให้ความคิดเห็น : กรมการจัดหางาน (เป็นหนังสือ))

๒๐. ได้นำรายงานการวิเคราะห์ผลกระทบที่อาจเกิดขึ้นจากกฎหมายของกฎหมายฉบับนี้ (ถ้ามี) มาประกอบการพิจารณาด้วยแล้วหรือไม่

ไม่มี

๒๑. หน่วยงานได้

๒๑.๑ ออกกฎหรือดำเนินการอย่างหนึ่งอย่างใดตามที่กฎหมายบัญญัติไว้ เพื่อที่ประชาชนจะสามารถปฏิบัติตามกฎหมายหรือได้รับสิทธิประโยชน์จากกฎหมายหรือไม่ อย่างไร

ได้มีการออกกฎ ดังนี้

(๑) ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง ลักษณะและวิธีการส่ง และลักษณะและปริมาณของข้อมูล ความถี่และวิธีการส่งซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับ พ.ศ. ๒๕๖๐ อันเป็นการกำหนดลักษณะและวิธีการส่ง และลักษณะและปริมาณของข้อมูล ความถี่และวิธีการส่งซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับ เพื่อมีขอบเขตที่ชัดเจนว่า การส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ลักษณะใด จะไม่ถือเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่น (Spam mail) ตามมาตรา ๑๑ วรรคสาม แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

(๒) ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์ ระยะเวลา และวิธีการปฏิบัติสำหรับการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ของพนักงานเจ้าหน้าที่หรือผู้ให้บริการ พ.ศ. ๒๕๖๐ อันเป็นการกำหนดหลักเกณฑ์ ระยะเวลา และวิธีการปฏิบัติสำหรับการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ของพนักงานเจ้าหน้าที่หรือผู้ให้บริการตามที่ศาลได้มีคำสั่งให้ระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ที่เป็นความผิดแล้ว ให้เป็นไปในแนวทางเดียวกัน ตามมาตรา ๒๐ วรรคสี่ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

(๓) ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๖๔ อันเป็นการกำหนดหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการโดยแบ่งตามลักษณะการให้บริการ ให้มีความเหมาะสมกับสภาวะเศรษฐกิจ สังคม และเทคโนโลยีในปัจจุบัน ตามมาตรา ๒๖ วรรคสาม แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

(๔) ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง ขั้นตอนการแจ้งเตือน การระงับการทำให้แพร่หลายของข้อมูลคอมพิวเตอร์ และการนำข้อมูลคอมพิวเตอร์ออกจากระบบคอมพิวเตอร์ พ.ศ. ๒๕๖๕ อันเป็นการกำหนดขั้นตอนการแจ้งเตือน การระงับการทาให้แพร่หลายของข้อมูลคอมพิวเตอร์ และการนำข้อมูลคอมพิวเตอร์ออกจากระบบคอมพิวเตอร์ของผู้ให้บริการให้ทันสมัยเพื่อแก้ไขปัญหาการทาให้แพร่หลายของข้อมูลคอมพิวเตอร์ที่ผิดกฎหมายผ่านระบบคอมพิวเตอร์หรือเครือข่ายอินเทอร์เน็ต ตามมาตรา ๑๕ วรรคสอง แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๒๑.๒ ดำเนินการอื่นเพื่อปฏิบัติตามและบังคับการให้เป็นไปตามกฎหมายหรือไม่ อย่างไร

สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ในฐานะที่เป็นหน่วยงานเฝ้าระวังและติดตามสถานการณ์เพื่อความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของประเทศ ได้ตระหนักถึงปัญหาที่เกิดขึ้นจากข่าวปลอมที่ปัจจุบันยังคงทวีความรุนแรง และมีเนื้อหาที่หลากหลายมากขึ้น ส่งผลกระทบต่อสังคมเป็นวงกว้าง ทั้งยังสร้างความแตกแยก ความเข้าใจผิด ตลอดจนการทำลายภาพลักษณ์ของประเทศ จึงได้จัดตั้งศูนย์ต่อต้านข่าวปลอม ประเทศไทย (Anti-Fake News Center Thailand) https://www.antifakenewscenter.com/ เพื่อจัดการกับปัญหาข่าวปลอมที่แพร่กระจายอยู่บนโลกออนไลน์ ด้วยการทำหน้าที่เป็นสื่อกลางในการตรวจสอบข้อมูลข่าวสาร และกระตุ้นให้เกิดการรับรู้ข้อมูลข่าวสารอย่างมีวิจารณญาณ ให้ประชาชนรู้เท่าทัน สามารถปกป้องตนเองจากข่าวปลอมได้ โดยมีภารกิจในการติดตาม ตรวจสอบข้อมูลที่เผยแพร่บนสื่อสังคมออนไลน์ ที่ส่งผลกระทบต่อชีวิตและทรัพย์สินของประชาชน ทั้งโดยตรงและต่อสังคมในวงกว้าง ซึ่งจะวิเคราะห์ตามหลักการที่ตั้งไว้โดยแยกตามหมวดหมู่ หากพบว่ามีแนวโน้มเป็นข่าวปลอม

จะทำการประสานไปยังหน่วยงานที่เกี่ยวข้องเพื่อตรวจสอบข้อมูล และเมื่อได้ข้อเท็จจริง จะทำการเผยแพร่ออกไปตามช่องทางต่าง ๆ ของศูนย์ฯ ให้ประชาชนได้รับทราบต่อไป และเป็นศูนย์ในการรับแจ้งเบาะแสข่าวปลอม และติดตามสถานะข่าวที่แจ้ง อันเป็นการดำเนินการเพื่อสนับสนุนการป้องกันและปราบปรามการนำเข้าข้อมูลอันเป็นเท็จสู่ระบบคอมพิวเตอร์ ตามมาตรา ๑๔ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๒๒. ผลสัมฤทธิ์ของกฎหมาย

๒๒.๑ กฎหมายนี้มีการบังคับใช้หรือไม่ อย่างไร

มีการบังคับใช้จนถึงปัจจุบัน โดยมีสถิติการดำเนินการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ออกจากระบบคอมพิวเตอร์ตามมาตรา ๒๐ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ของพนักงานเจ้าหน้าที่ที่ได้รับการแต่งตั้งตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ โดยศาลที่มีเขตอำนาจได้มีคำสั่งระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ออกจากระบบคอมพิวเตอร์ตามคำร้องของพนักงานเจ้าหน้าที่ จำนวน ๑,๙๕๗ คำสั่งศาล เป็นจำนวน ๑๔๘,๐๗๘ โดเมนเนม/URL (ข้อมูล ณ วันที่ ๓๑ ธันวาคม ๒๕๖๗) และศาลยุติธรรมได้มีการจัดตั้งแผนกคดีอาชญากรรมทางเทคโนโลยีในศาลอาญา ซึ่งมีอำนาจหน้าที่พิจารณาพิพากษาคดีอาชญากรรมทางเทคโนโลยี (คดีอาญาที่ฟ้องขอให้ลงโทษบุคคลที่กระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์) และพิจารณาและมีคำสั่งเกี่ยวกับคำร้องของพนักงานเจ้าหน้าที่ตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ โดยสถิติคดีที่เข้าสู่การพิจารณาพิพากษาของศาลชั้นต้นทั่วราชอาณาจักร ประเภทคดีอาชญากรรมทางเทคโนโลยี จำนวน ๑,๖๙๙ คดี โดยพิพากษาแล้วเสร็จจำนวน ๑,๒๙๘ คดี (ข้อมูล ณ วันที่ ๓๑ ธันวาคม ๒๕๖๗)

๒๒.๒ หากมีการบังคับใช้ เกิดผลสำเร็จตามเป้าหมายที่กำหนดไว้หรือไม่ อย่างไร

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เป็นกฎหมายที่ป้องกันมิให้มีการกระทำความผิดต่อระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ หรือการใช้ระบบคอมพิวเตอร์กระทำความผิดอื่น โดยการกระทำดังกล่าวพระราชบัญญัตินี้ได้บัญญัติให้เป็นความผิดและกำหนดโทษไว้ เพื่อเป็นการคุ้มครองสิทธิและเสรีภาพของประชาชนในการใช้ระบบคอมพิวเตอร์โดยมุ่งคุ้มครองสังคมเป็นสำคัญ การบังคับใช้พระราชบัญญัตินี้จึงเกิดผลสำเร็จตามเป้าหมายของดังกล่าว

๒๒.๓ ประชาชนมีภาระหรือรัฐมีต้นทุนที่เกิดขึ้นจากการปฏิบัติตามและบังคับการให้เป็นไปตามกฎหมายอย่างไร

ผู้ให้บริการและรัฐ (ในกรณีที่เป็นผู้ให้บริการเอง) มีภาระหรือต้นทุนในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ และการกำหนดขั้นตอนการแจ้งเตือน การระงับการทำให้แพร่หลายของข้อมูลคอมพิวเตอร์ และการนำข้อมูลคอมพิวเตอร์ออกจากระบบคอมพิวเตอร์สำหรับการให้บริการของตน เช่น ค่าใช้จ่ายในการจัดซื้อหรือเช่าใช้พื้นที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ ซึ่งแตกต่างกันไปตามลักษณะหรือปริมาณของข้อมูล และความสามารถในการใช้งานที่ต้องการ ค่าใช้จ่ายในการจัดให้มีช่องทางการรับคำร้องแจ้งเตือน ไม่ว่าจะเป็นการจัดให้มีบุคลากรเป็นผู้ดูแลระบบ (Admin) หรือการทำโปรแกรมคอมพิวเตอร์ที่ใช้จำลองการสนทนาโต้ตอบกับมนุษย์ผ่านข้อความหรือเสียงแบบ

อัตโนมัติ (แชทบอท (Chatbot)) เพื่อให้บริการผู้ใช้บริการได้ตลอด ๒๔ ชั่วโมง เป็นต้น อย่างไรก็ตาม ภาระและต้นทุนดังกล่าวเป็นค่าใช้จ่ายในการดำเนินธุรกิจโดยปกติของผู้ให้บริการอยู่แล้ว

๒๒.๔ เกิดผลที่ไม่ได้คาดคิดหรือไม่พึงประสงค์หรือไม่

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เป็นกฎหมายที่มีวัตถุประสงค์เพื่อมุ่งคุ้มครองประโยชน์สาธารณะเป็นสำคัญ แต่ในช่วงระยะแรกของการบังคับใช้กฎหมาย ได้มีการฟ้องร้องเพื่อดำเนินคดีในความผิดฐานนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จตามมาตรา ๑๔ (๑) อันเป็นข้อมูลคอมพิวเตอร์ที่มีลักษณะหมิ่นประมาทตามประมวลกฎหมายอาญา ซึ่งเป็นความผิดต่อส่วนตัวเป็นจำนวนมาก โดยที่มาตรา ๑๔ มีบทลงโทษที่หนักกว่าความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา ทำให้ผู้กระทำความผิดฐานหมิ่นประมาทโดยการนำเข้าสู่ระบบคอมพิวเตอร์ได้รับโทษหนักขึ้น อันเป็นการใช้กฎหมายที่ผิดวัตถุประสงค์ของกฎหมายดังกล่าว อย่างไรก็ดี มาตราดังกล่าวได้มีการแก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ โดยได้บัญญัติให้ชัดเจนว่า “อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา” อันเป็นการแก้ไขปัญหาดังกล่าวแล้ว

๒๓. กฎหมายนี้คุ้มค่าหรือได้สัดส่วนเมื่อเทียบประโยชน์ที่ได้รับกับภาระของประชาชนและทรัพยากรที่ใช้ในการบังคับการให้เป็นไปตามกฎหมายหรือไม่ อย่างไร

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ มุ่งคุ้มครองประโยชน์สาธารณะ ทำให้เกิดความสงบเรียบร้อยในสังคม โดยเฉพาะในการใช้งานระบบคอมพิวเตอร์ซึ่งปัจจุบันเป็นส่วนสำคัญในการดำรงชีวิตของประชาชน เมื่อเทียบกับภาระของผู้ให้บริการในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ และการกำหนดขั้นตอนการแจ้งเตือน การระงับการทำให้แพร่หลายของข้อมูลคอมพิวเตอร์ และการนำข้อมูลคอมพิวเตอร์ออกจากระบบคอมพิวเตอร์สำหรับการให้บริการของตน ซึ่งเป็นค่าใช้จ่ายในการดำเนินธุรกิจโดยปกติของผู้ให้บริการอยู่แล้ว กับทรัพยากรที่ใช้ในการบังคับใช้กฎหมายของรัฐแล้ว ถือว่าคุ้มค่าและได้สัดส่วน

๒๔. สมควรยกเลิก แก้ไข ปรับปรุงกฎหมายหรือกฎหรือไม่ อย่างไร

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ มีความเหมาะสมกับสภาพการณ์ปัจจุบัน จึงสมควรบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ต่อไป โดยสมควรทำการศึกษาและค้นคว้าข้อมูลที่เกี่ยวข้องเพื่อประกอบการพิจารณาแก้ไข หรือปรับปรุงกฎหมายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ หรือกฎที่ออกตามพระราชบัญญัติดังกล่าว เพื่อให้สอดคล้องกับสภาพการณ์ในปัจจุบัน โดยเฉพาะการเปลี่ยนแปลงทางเทคโนโลยีที่ส่งผลต่อรูปแบบการให้บริการของผู้ให้บริการ และพฤติกรรมการใช้งานและการกระทำความผิดของประชาชน และกระบวนการดำเนินคดีที่ต้องอาศัยความรวดเร็วทันต่อสถานการณ์และการเปลี่ยนแปลงทางเทคโนโลยีให้มีความเป็นอัตโนมัติ (automate) มากยิ่งขึ้น โดยอาศัยระบบหรือช่องทางอิเล็กทรอนิกส์ในกระบวนการดำเนินคดี

๒๕. สมควรดำเนินการอื่นเพื่อปรับปรุงประสิทธิภาพในการปฏิบัติตามและบังคับการให้เป็นไปตามกฎหมาย หรือมีข้อเสนออื่นหรือไม่ อย่างไร

ไม่มี

ข้าพเจ้าขอรับรองว่าข้อมูลที่ปรากฏในรายงานนี้เป็นข้อมูลที่ได้จากการตรวจสอบและวิเคราะห์อย่างถี่ถ้วนแล้ว

ลงชื่อ .....

(นายพชร อนันตศิลป์)

ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

๓๐ ธันวาคม ๒๕๖๘

หน่วยงานผู้รับผิดชอบ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

เจ้าหน้าที่ผู้รับผิดชอบ นายศรัลก์ โคตะสินธ์

โทร. ๐๒-๑๔๑-๖๗๖๗ / ๐๒-๑๔๑-๖๗๖๖

อีเมล saran.co@mdes.go.th