www.etda.or.th

เอกสารประกอบการสัมมนารับฟังความคิดเห็น เรื่อง

“การปรับปรุง พ.ร.บ.คอมพิวเตอร์ฯ : ความสมดุลระหว่างเสรีภาพ กับความมั่นคงปลอดภัย”

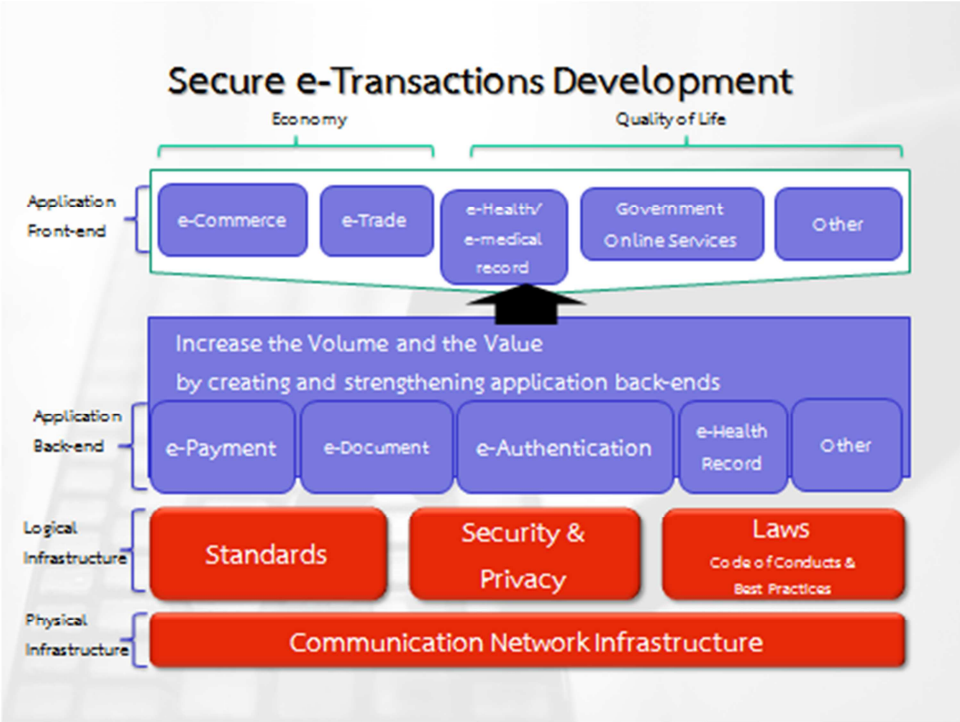
วันที่ 3 เมษายน 2556 เวลา 08.30 – 12.30 น.

ณ ห้องแกรนด์ บอลรูม โรงแรมเชอราตัน แกรนด์ สุขุมวิท กรุงเทพฯ

แนวทางการปรับปรุงกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

1. สพธอ. กับการนำเสนอแนวทางการปรับปรุงกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (Electronic Transactions Development Agency) หรอ สพธอ. (ETDA) เป็นองค์การมหาชน ซึ่งเป็นองค์กรของรัฐที่จัดตั้งขึ้นเพื่อการพัฒนา ส่งเสริมและสนับสนุนการทำธุรกรรมทางอิเล็กทรอนิกส์ เพื่อให้เป็นเครื่องมือในการสร้างมูลค่าเพิ่มทางเศรษฐกิจ ยกระดับคุณภาพชีวิตและขีดความสามารถในการแข่งขันกับประเทศอื่น ๆ รวมทั้งสนับสนุนการดำเนินงานตามนโยบายของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งเป็นคณะกรรมการระดับชาติตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ที่เป็นหลักในการพัฒนาและส่งเสริมการทำธุรกรรมทางอิเล็กทรอนิกส์ ทั้งเชิงรุกและเชิงตั้งรับ ตลอดจนจัดการกับปัญหาและอุปสรรคที่เกิดขึ้นและส่งผลกระทบต่อการทำธุรกรรมทางอิเล็กทรอนิกส์ โดยมิได้ครอบคลุมแต่เพียงการทำอีคอมเมิร์ซ (e-Commerce) แต่ยังครอบคลุมการทำธุรกิจบริการต่าง ๆ ที่เกี่ยวข้อง การให้บริการภาครัฐอันเป็นงานรัฐบาลอิเล็กทรอนิกส์ รวมทั้งการกำหนดมาตรฐานและมาตรการเพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์มีความน่าเชื่อถือและมั่นคงปลอดภัย ดังนั้น ด้วยความรับผิดชอบที่กว้างในเกือบทุกมิติของการทำธุรกรรมทางอิเล็กทรอนิกส์ดังกล่าว จึงจำเป็นต้องมีการจัดตั้งหน่วยงานที่มีรูปแบบการบริหารจัดการที่คล่องตัว และสามารถ ประสานการทำงานกับสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ที่เป็นส่วนราชการอันเป็นโครงสร้างภายใต้สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารอย่างใกล้ชิด



สำหรับแนวทางในการส่งเสริมและผลักดันการทำธุรกรรมทางอิเล็กทรอนิกส์ของประเทศนั้น นอกเหนือจากปัจจัยความพร้อมของการวางโครงสร้างพื้นฐานสารสนเทศที่จะรองรับการทำธุรกรรมทางอิเล็กทรอนิกส์ในรูปแบบ Physical Infrastructure เช่น อินเทอร์เน็ตเครือข่ายความเร็วสูงแล้ว การผลักดันกลไกที่เป็นโครงสร้างพื้นฐานสารสนเทศในรูปแบบ Logical Infrastructure ถือได้ว่าเป็นปัจจัยอีกส่วนหนึ่งที่มีความสาคัญซึ่งจะทำให้ผู้ใช้งานมีความเชื่อมั่นและมีความมั่นใจในการทำธุรกรรมทางอิเล็กทรอนิกส์มากยิ่งขึ้น โดยกลไกดังกล่าวประกอบด้วยการวางมาตรฐานเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อการทำธุรกรรมทางอิเล็กทรอนิกส์ (Standards) การดูแลรกษาความมนคงปลอดภยของระบบสารสนเทศ (Security) และการคุ้มครองความเป็นส่วนตัว (Privacy) ตลอดจนการรองรับผลทางกฎหมาย (Law) และการกำหนดแนวปฏิบัติที่ดีสำหรับเป็นคู่มือแก่ผู้ใช้งานในการทำธุรกรรมทางอิเล็กทรอนิกส์ (Code of Conducts & Best Practices) โดยแนวทางการดำเนินการในส่วนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (Security) นั้น นอกเหนือจากการกำหนดมาตรการหรือวิธีการทั้งในเชิงนโยบายและเชิงเทคนิคในการดูแลระบบสารสนเทศตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ฉบับต่าง ๆ เช่น ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง ประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. 2555 และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555 แล้ว การมีมาตรการทางกฎหมายเพื่อป้องกันและปราบปรามมิให้มีการกระทำใดที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ถือได้ว่าเป็นอีกมาตรการหนึ่งที่มีความจำเป็น เนื่องจากจะมีส่วนช่วยให้จำนวนหรือปริมาณการกระทำความผิดลดน้อยลง ซึ่งปัจจุบันมาตรการทางกฎหมายในส่วนนี้ได้มี

การกำหนดไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่มีหลักการสำคัญในการกำหนดฐานความผิดและบทลงโทษของการกระทำที่มีผลกระทบต่อหลัก C.I.A และการกระทำที่อาศัยคอมพิวเตอร์ในการสร้างความเสียหายต่อบุคคลอื่นหรือส่วนรวม รวมทั้งกลไกในการติดตามและปราบปรามการกระทำความผิดดังกล่าว

โดยภายหลังจากที่มีการประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาเป็นระยะเวลากว่า 5 ปี การบังคับใช้กฎหมายดังกล่าวปรากฏประเด็นปัญหาการใช้บังคับในทางปฏิบัติ ไม่ว่าโดยผลของพัฒนาการทางเทคโนโลยีสารสนเทศที่มีการเปลี่ยนแปลงไปอย่างรวดเร็ว กล่าวคือฐานความผิดที่กำหนดในกฎหมายปัจจุบันไม่ครอบคลุมถึงรูปแบบการกระทำความผิดที่เปลี่ยนแปลงไป เช่น ปัจจุบันไม่สามารถเอาผิดกับผู้กระทำที่ส่งจดหมายอิเล็กทรอนิกส์เป็นจำนวนมากให้แก่ผู้อื่นได้ (Spam mail) เนื่องจากกฎหมายกำหนดให้มีความผิดต่อเมื่อมีการปกปิดหรือปลอมแปลงแหล่งที่มาซึ่งเป็นช่องโหว่ที่กฎหมายไม่สามารถนำตัวผู้กระทำผิดมาลงโทษได้ หรือโดยผลจากการบังคับใช้กฎหมายหรือการตีความกฎหมายที่อาจยังไม่สอดคล้องตรงตามเจตนารมณ์ เช่น การนำฐานความผิดฐานการนำเข้าข้อมูลคอมพิวเตอร์ปลอมและการเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จไปปรับใช้กับการกระทำความผิดฐานหมิ่นประมาท ซึ่งทำให้มีการแจ้งความเพื่อดำเนินคดีจากความผิดฐานดังกล่าวเป็นจำนวนมาก ประกอบกับปริมาณการกระทำความผิดทางคอมพิวเตอร์มีแนวโน้มจะเพิ่มจำนวนสูงขึ้น ก่อให้เกิดผลกระทบกับทั้งผู้ให้บริการ ผู้ใช้คอมพิวเตอร์และอินเทอร์เน็ตโดยทั่วไป ซึ่งปรากฏว่ามีการเรียกร้องจากหลายภาคส่วนให้มีการทบทวนหลักการของกฎหมายที่ใช้บังคับ รวมถึงเพิ่มเติมส่วนที่กฎหมายปัจจุบันยังไม่ครอบคลุมหรือรองรับ

ดังนั้น รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารจึงมีดำริเห็นสมควรให้ สพธอ. ศึกษาวิเคราะห์สภาพปัญหาและพิจารณาแนวทางการปรับปรุงพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เพื่อลดอุปสรรคและสภาพปัญหาในการบังคับใช้กฎหมายที่เกิดขึ้น สพธอ. ในฐานะหน่วยงานทางวิชาการซึ่งมีภารกิจส่วนหนึ่งคือการศึกษาวิจัยเพื่อการจัดทำข้อเสนอแนะในการพัฒนาและปรับปรุงกฎหมาย กฎระเบียบ และแนวปฏิบัติที่เกี่ยวข้องและจำเป็นต่อการสนับสนุนการทำธุรกรรมทางอิเล็กทรอนิกส์ของประเทศไทย จึงรับมอบนโยบายดังกล่าวและจัดให้มีโครงการปรับปรุงพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ขึ้นเพื่อดำเนินการศึกษาสภาพปัญหาทั้งในทางข้อเท็จจริงและข้อกฎหมาย รวมถึงการบังคับใช้กฎหมายในทางปฏิบัติ โดยการศึกษาเปรียบเทียบกับแนวทางของกฎหมายระหว่างประเทศและกฎหมายภายในของต่างประเทศ เพื่อจัดทำข้อเสนอแนะและแนวทางการแก้ไขเสนอต่อรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร และสำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารในฐานะหน่วยงานที่รับผิดชอบดูแลการบังคับใช้กฎหมายฉบับนี้โดยตรงสำหรับเป็นข้อมูลสนับสนุนในการจัดทำและผลักดันการปรับแก้กฎหมายดังกล่าวต่อไป ทั้งนี้ โดยมุ่งหวังให้กฎหมายที่พัฒนาขึ้นมีความเป็นสากลและสามารถใช้บังคับในทางปฏิบัติได้อย่างมีประสิทธิภาพ และในขณะเดียวกันได้คำนึงถึงสิทธิและเสรีภาพของประชาชนในการติดต่อสื่อสารอันเป็นสิทธิขั้นพื้นฐานตามรัฐธรรมนูญ

2. แนวทางการดำเนินงานโครงการปรับปรุงพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

เนื่องจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นกฎหมายที่มีผลกระทบกับทั้งผู้ให้บริการ ผู้ใช้คอมพิวเตอร์และอินเทอร์เน็ตโดยทั่วไปในวงกว้าง โดยในบางมาตราได้ถูกนำไปเชื่อมโยงต่อแนวความคิดที่เป็นความขัดแย้งทางสังคมในปัจจุบัน ซึ่งเป็นประเด็นที่มีความอ่อนไหวอย่างมาก ในขณะที่กลไกการดำเนินการบังคับใช้กฎหมายที่มีอยู่ยังไม่มีความคล่องตัวหรือชัดเจนเพียงพอ ทำให้การตอบสนองต่อปัญหาที่เกิดขึ้นมีความล่าช้า ดังนั้น ในการศึกษาแนวทางในการปรับปรุงกฎหมายฉบับนี้ สพธอ. จึงได้พยายามวางแนวทางการดำเนินงานเพื่อให้ครอบคลุมประเด็นปัญหาต่าง ๆ อย่างรอบด้าน กล่าวคือ นอกเหนือจากการศึกษาหลักเกณฑ์กฎหมายภายในประเทศและต่างประเทศทเกยวข้อง และสภาพปัญหาที่เกิดขึ้นจริงแล้ว สพธอ. ยังได้จัดให้มคณะทางานปรบปรงพระราชบญญตว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่ประกอบด้วยผู้เชี่ยวชาญและตัวแทนจากหน่วยงานที่เกี่ยวข้อง เพื่อร่วมพิจารณาให้ข้อเสนอแนะและระดมความเห็นอันเป็นประโยชน์ต่อการปรับปรุงกฎหมายดังกล่าวอย่างใกล้ชิด รวมทั้งได้จัดให้มีการรับฟังความคิดเห็นจากภาคส่วนต่างๆ ที่มีส่วนได้เสียกับกฎหมายฉบับนี้ เช่น การประสานความร่วมมือกับสมาคมผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์ (Thai e-Commerce Association) สมาคมผู้ดูแลเว็บไทย (Thai Webmaster Association) และสมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (Thailand Information Security Association) ในการจัดสัมมนาในหัวข้อ “5 ปี ของพ.ร.บ.คอมพิวเตอร์ฯ ผลดี ผลกระทบ และอนาคต : Balance of Freedom and National Security” ในระหว่างวันที่ 7 – 14 กนยายน 2555 หรือ การจัดเสวนาในหัวข้อ “ผู้ให้บริการกับบทบาทหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์” ในวันที่ 7 มีนาคม 2556 ที่ผ่านมา เป็นต้น รวมถึงการขอความเห็นจากหน่วยงานของรัฐที่มีความเกี่ยวข้องและมีภารกิจเชื่อมโยงกับกฎหมายฉบับดังกล่าวทั้งในฐานะพนักงานเจ้าหน้าที่ตามกฎหมาย และผู้บังคับกฎหมายในหลายหน่วยงานด้วยกัน เช่น สำนักป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี หรือสำนักงานอัยการสูงสุด เป็นต้น ทั้งนี้ เพื่อที่จะรวบรวม และนำเสนอต่อกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเพื่อเป็นข้อมูลสนับสนุนในการจัดทำและผลักดันการปรับแก้กฎหมายดังกล่าวต่อไป

3. การวิเคราะห์สภาพปัญหาและแนวทางนำเสนอ

จากการดำเนินการศึกษาสภาพปัญหา การประชุมคณะทำงาน และการสัมมนารับฟังความคิดเห็นจากทุกภาคส่วนตลอดช่วงเวลาที่ผ่านมาดังที่ได้กล่าวมาข้างต้น สพธอ. จึงเห็นควรเสนอให้มีการปรับปรุงกฎหมายให้สอดคล้องกับสภาวะแวดล้อมและบริบทของสังคมไทยเพื่อให้สามารถบังคับใช้กฎหมายได้อย่างถูกต้องตามเจตนารมณ์และมีประสิทธิภาพ ซึ่งขอนำเสนอในประเด็นสำคัญ ดังนี้

3.1 การปรับปรุงฐานความผิด

1) การเข้าถึงระบบคอมพิวเตอร์ / ข้อมูลคอมพิวเตอร์ โดยมิชอบ

โดยลักษณะการใช้งานอุปกรณ์อิเล็กทรอนิกส์ของประชาชนในปัจจุบัน ผู้ใช้งานบางรายไม่มีการกำหนดมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ไว้โดยเฉพาะ ส่วนหนึ่งเนื่องมาจากการขาดความรู้ความเข้าใจในการกำหนดมาตรการป้องกันพื้นฐาน แต่ผู้ใช้งานก็ยังคงต้องการที่จะรักษาระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ของตนไว้ไม่ต้องการให้ผู้อื่นเข้าถึงโดยไม่มีสิทธิหรือโดยไม่ได้รับอนุญาต ซึ่งกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฉบับที่ใช้อยู่ในปัจจุบันกำหนดองค์ประกอบความผิดไว้โดยเฉพาะว่าจะเป็นความผิดต่อเมื่อเป็นกรณีที่กระทำต่อระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ซึ่ง “มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ” เท่านั้น จึงเสนอแนวทางการปรับปรุงกฎหมาย โดยกำหนดโทษออกเป็นสองส่วนด้วยกัน โดยกำหนดเป็นความผิดทั้งในกรณีที่ไม่มมาตรการป้องกันและมีมาตรการป้องกัน โดยอัตราโทษของการเข้าถึงระบบหรือข้อมูลที่มีมาตรการป้องกันการเข้าถึงจะสูงกว่า

ทั้งนี้ การเพิ่มเติมบทบัญญัติให้รองรับกรณีการเข้าถึงโดยมิชอบแม้จะไม่มีมาตรการป้องกันการเข้าถึงให้เป็นความผิดน่าจะช่วยป้องปรามความเสียหายของผู้เป็นเจ้าของระบบหรือข้อมูลคอมพิวเตอร์ได้ในระดับหนึ่ง นอกจากนี้หากเป็นเรื่องเล็กน้อย เช่น คนรู้จักกันเข้าไปดูโทรศัพท์มือถือของคนอื่นโดยที่ไม่ได้มีการตั้งรหัสผ่านไว้ ซึ่งเป็นเรื่องวิสาสะก็เป็นการขาดเจตนาตามกฎหมายอาญา และหากเกรงว่าจะเกิดการกลั่นแกล้งกัน หรือไม่ต้องการเอาเรื่องก็กำหนดระดับความผิดให้เบาลงโดยกำหนดให้เป็นความผิดอันยอมความได้ จึงนำเสนอแนวทางการปรับปรุงกฎหมายดังนี้

“มาตรา ... ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ของผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งเดือน หรือปรับไม่เกินห้าพันบาท หรือทั้งจำทั้งปรับ

ถ้าการกระทำความผิดตามวรรคหนึ่ง ได้กระทำต่อระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ... ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่น ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

ถ้าการกระทำความผิดตามวรรคหนึ่ง ได้กระทำต่อข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ... ความผิดตามมาตรา ... วรรคหนึ่ง (เข้าถึงระบบโดยมิชอบ) และมาตรา ... วรรคหนึ่ง (เข้าถึงข้อมูลโดยมิชอบ) ... เป็นความผิดอันยอมความได้”

2) การทำซ้ำ / ทำสำเนา ข้อมูลคอมพิวเตอร์

โดยเหตุที่การกระทำในลักษณะการคัดลอกหรือทำสำเนาข้อมูลนั้นไม่มีบทกฎหมายใดรองรับหรือบัญญัติว่าเป็นความผิด ประกอบกับตามแนวคำพิพากษาศาลฎีกาที่วินิจฉัยว่ากรณีที่เป็นการทำสำเนาข้อมูลคอมพิวเตอร์ไม่สามารถลงโทษผู้กระทำในความผิดฐานลักทรัพย์ตามประมวลกฎหมายอาญาได้ เพราะข้อมูลเดิมยังคงมีอยู่ จึงไม่อาจลงโทษบุคคลผู้มีเจตนาไม่สุจริตที่แอบคัดลอกหรือทำสำเนาข้อมูลของบุคคลอื่นซึ่ง

ก่อหรืออาจก่อให้เกิดความเสียหายอย่างหนึ่งอย่างใดขึ้นได้ จึงได้เสนอแนวทางการปรับปรุงกฎหมายเพื่อให้มีความครอบคลุม

"มาตรา ... ผู้ใดทำซ้ำหรือทำโดยวิธีอื่นใดอันคล้ายคลึงกันต่อข้อมูลคอมพิวเตอร์ของผู้อื่นเพื่อให้ได้ไปซึ่งสำเนาข้อมูลคอมพิวเตอร์ของผู้อื่น โดยประการที่น่าจะก่อให้เกิดความเสียหายแก่ผู้อื่นหรือประชาชน ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ"

การพิจารณาว่าจะเป็นความผิดหรือไม่ เป็นเรื่องที่ต้องพิจารณา "เจตนา" ของผู้กระทำเป็นหลักว่ามีเจตนาอย่างไร เพราะกรณีที่จะเป็นความผิดทางอาญาต้องเป็นการกระทำโดยเจตนา ดังนั้น หากเป็นกรณีการทำโดยระบบปกติของเครื่อง เช่น การ catch ข้อมูลมาเก็บไว้ในตัวเครื่องสำหรับการเรียกใช้งานในสภาวะปกติ เช่นนี้ย่อมไม่อยู่ในความหมายของคำว่า "ทำซ้ำ" แต่อย่างใด

อนึ่ง ข้อความที่นำเสนอนี้ยังคงมีประเด็นโต้แย้งในเรื่องความซ้ำซ้อนกับบทบัญญัติของกฎหมายลิขสิทธิ์อยู่เช่นกัน ซึ่งโดยเจตนาของคณะผู้จัดทำเจตนาที่จะมุ่งหมายให้มาตรานี้หมายถึงการคัดลอกหรือทำสำเนาข้อมูลคอมพิวเตอร์ในส่วนที่ไม่ได้รับความคุ้มครองตามกฎหมายทรัพย์สินทางปัญญา ทงน มข้อสังเกตในแง่ของการบังคับใช้กฎหมายกรณีที่มีกฎหมายหลายฉบับกำหนดบทบัญญัติหรือฐานความผิดในทำนองทับซ้อนกันว่าในหลักการของกฎหมายอาญาเมื่อการกระทำกรรมเดียวเป็นความผิดต่อกฎหมายหลายบท กฎหมายได้กำหนดให้ลงโทษผู้กระทำความผิดตามบทกฎหมายที่มีอัตราโทษหนักกว่า ดังนั้น จึงอาจพิจารณาการกำหนดอัตราโทษให้สอดรับกันกับกฎหมายลิขสิทธิ์เพื่อมิให้เกิดความลักลั่นในการบังคับใช้กฎหมาย

3) spam mail

การส่งข้อมูลหรือจดหมายอิเล็กทรอนิกส์อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของผู้อื่นนั้นมีได้ทั้งกรณีปกปิดและไม่ปกปิดแหล่งที่มาซึ่งอาจเป็นการรบกวนหรือก่อให้เกิดความเสียหายได้ทั้งสิ้น ซึ่งตามมาตรา 11 ปัจจุบันมีการกำหนดองค์ประกอบความผิดประการหนึ่งคือ "โดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูล" แต่ในปัจจุบันการส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์มักจะกระทำโดยมิได้ปกปิดหรือปลอมแปลงแหล่งทมาของการส่งข้อมูล การกระทำดังกล่าวจึงไม่ครบองค์ประกอบความผิดตามที่กฎหมายกำหนดทำให้ผู้กระทำไม่ต้องรับผิดแม้ว่าการส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์นั้นจะเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของผู้อื่น

ทั้งนี้ หากพิจารณากฎหมายของต่างประเทศ เช่น สหรัฐอเมริกา และออสเตรเลีย การกำหนดความรับผิดเรื่องสแปมเมล์จะยึดโยงกับการคุ้มครองความเป็นส่วนตัวและข้อมลส่วนบุคคลในเชิงพาณิชย์เป็นหลัก โดยมีหลักการสำคัญคือการกำหนดขอบเขตที่เข้มงวดในการเข้าถึงความเป็นส่วนตัวและข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต ซึ่งผู้ให้บริการหรือผู้ที่ส่งข้อมูลหรือข้อความใดไปยังผู้รับข้อมูลจะต้องเปิดโอกาสให้ผู้รับข้อมูลมีสิทธิที่จะปฏิเสธไม่รับข้อมูลหรือข้อความนั้นๆ ได้ อีกทั้งยังมีการกำหนดหลักเกณฑ์และความรับผิดในเรื่องนี้อย่างชัดเจนโดยกำหนดเป็นกฎหมายเฉพาะเรื่อง เช่น ประเทศสหรัฐอเมริกา มีกฎหมาย Commercial Electronic Mail Message หรือประเทศออสเตรเลีย มีกฎหมาย Commercial Electronic Message ตราไว้โดยเฉพาะ นอกจากนี้หน่วยงานที่ทำหน้าที่กำกับดูแลเรื่องนี้จะเป็นหน่วยงานที่ทำหน้าที่กำกับดูแลเรื่องกิจการโทรคมนาคม หรือหน่วยงานทางด้านการพาณิชย์ ดังนั้น จึงเห็นได้ว่าโดยเนื้อหาการกระทำอันเข้าลักษณะเป็นสแปมเมล์ตามแนวทางของต่างประเทศนั้น มีลักษณะเป็นการส่งข้อมูลหรือข้อความในเชิงการค้าพาณิชย์ โดยที่บุคคลนั้นไม่พึงประสงค์จะได้รับและเป็นเหตุให้เกิดความรำคาญอันเป็นการละเมิดความเป็นส่วนตัวของบุคคล ซึ่งกฎหมายมุ่งที่จะคุ้มครองความเป็นส่วนตัวมากกว่าที่จะกำหนดให้เป็นความรับผิดในทางอาญาโดยตรง

อย่างไรก็ดี แม้มาตรานี้ยังไม่เคยมีการนำมาใช้จริงในทางปฏิบัติ แต่ในปัจจุบันผู้รับข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ในลักษณะดังกล่าวมีเป็นจำนวนมาก ประกอบกับการผลักดันเรื่องดังกล่าวโดยการตราเป็นกฎหมายเฉพาะอาจใช้ระยะเวลานาน ซึ่งหากมีการยกเลิกฐานความผิดนี้ในขณะที่ยังไม่มีการตรากฎหมายเฉพาะเพื่อรองรับจะทำให้ในระหว่างนั้นไม่มีกฎหมายใดที่สามารถบังคับหรือป้องปรามการกระทำในลักษณะดังกล่าวได้ ดังนั้น การคงฐานความผิดนี้ไว้ในกฎหมายน่าจะช่วยป้องปรามได้ในระดับหนึ่ง แต่เพื่อให้ฐานความผิดดังกล่าวมีความเหมาะสมและตรงตามเจตนารมณ์ รวมทั้งเพื่อมิให้เกิดผลกระทบจนกลายเป็นอุปสรรคในการพัฒนาเศรษฐกิจและการค้าของประเทศ จึงเสนอให้มีการปรับปรุงองค์ประกอบฐานความผิดต่อเมื่อมีการส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์เป็นจำนวนตามหลักเกณฑ์ที่รัฐมนตรีประกาศกำหนด โดยเปิดให้เป็นดุลพินิจในการกำหนดจำนวนที่เหมาะสมซึ่งการออกประกาศกำหนดสามารถปรับเปลี่ยนได้ตามความเหมาะสมกับสภาพเศรษฐกิจและสังคม ดังนี้

“มาตรา ... ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์รบกวนการใช้ระบบคอมพิวเตอร์ของผู้อื่นโดยปกติสุข <u>โดยไม่เปิดโอกาสให้ผู้รับข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์สามารถบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้</u> ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

เงื่อนไขและรายละเอียดเกี่ยวกับการส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ตามวรรคหนึ่ง ให้เป็นไปตามที่กำหนดในกฎกระทรวง”

4) การนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอม

ในบทบัญญัติมาตรา 14 (1) แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เจตนารมณ์ที่แท้จริงของกฎหมายมาตรานี้คือ ไม่ต้องการให้ผู้ได้รับข้อมูลนั้นประมวลผลหรือส่งผลต่อการตัดสินใจที่ผิดพลาด ยกตัวอย่างเช่น ผู้เสียหายถูกปลอม Caller ID เพื่อให้ผู้ให้บริการยอมให้เข้ามาในระบบ ทำให้ผู้ให้บริการประมวลผลผิด เป็นต้น และในขณะเดียวกันกฎหมายก็ต้องการคุ้มครองมิให้บุคคลตกเป็นเหยื่อจากการล่อลวงทางคอมพิวเตอร์ เช่น การทำ Phishing เป็นต้น แต่การตีความในทางปฏิบัติในปัจจุบันมาตรา 14 (1) ถูกนำไปปรับใช้ปะปนกับความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา โดยตีความให้เป็นความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญาด้วย อันบิดเบือนไปจากเจตนารมณ์ของกฎหมาย จึงมีความพยายามที่จะปรับแก้ถ้อยคำในกฎหมายเพื่อให้ตรงตามเจตนารมณ์ของเรื่องที่ต้องการเอาผิดในกรณีของ Phishing มิใช่ในกรณีการหมิ่นประมาททางคอมพิวเตอร์

ดังนั้น เพื่อมิให้มีการกำหนดฐานความผิดที่ซ้ำซ้อนกับกฎหมายอื่น รวมทั้งได้มีการเสนอให้ปรับปรุงกฎหมายเพื่อเปิดช่องให้เจ้าหน้าที่ตามกฎหมายอื่นสามารถร้องขอพนักงานเจ้าหน้าที่ตามกฎหมายนี้รวบรวมหลักฐานและดำเนินการภายใต้กฎหมายนี้ได้ เช่น การฉ้อโกงตามประมวลกฎหมายอาญาซึ่งใช้วิธีการฉ้อโกงผ่านทางสื่ออิเล็กทรอนิกส์เช่นการแสดงข้อความเท็จผ่านทางหน้าเว็บไซต์ เช่นนี้เจ้าพนักงานตำรวจสามารถร้องขอให้พนักงานเจ้าหน้าที่ตามกฎหมายนี้ดำเนินการสืบหาและรวบรวมพยานหลักฐานให้ได้ เป็นต้น โดยจะได้กล่าวต่อไป ดังนั้น แนวทางที่นำเสนอจึงเป็นการจำกัดเฉพาะการกระทำในลักษณะ Identity theft ซึ่งกฎหมายที่มีอยู่ในปัจจุบันยังไม่ครอบคลุมถึง ดังนี้

“มาตรา <u>... ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือปกปิดข้อความจริงซึ่งควรบอกให้แจ้งทั้งหมดหรือบางส่วน ทำให้ผู้หนึ่งผู้ใดหลงเชื่อว่าเป็นข้อมูลที่แท้จริงและทำให้ได้ไปซึ่งข้อมูลส่วนบุคคลโดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น</u> ต้องระวางโทษจำคุกไม่เกินหนึ่งปี ปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ”

5) ความผิดเกี่ยวกับภาพลามกอนาจารของผู้เยาว์ (Child Phonography)

สำหรับฐานความผิดเกี่ยวกับภาพลามกอนาจารของผู้เยาว์นั้น เดิมทีในขณะยกร่างครั้งแรกได้มีการกำหนดไว้เป็นความผิดตามกฎหมาย ซึ่งจะสอดคล้องกับหลักการในกฎหมายแม่แบบว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของประชาคมยุโรป (EU Cybercrime Convention) ที่มีการกำหนดความผิดในเรื่องดังกล่าว เนื่องจากที่ผ่านมาพบว่ามีการจัดทำและเผยแพร่ภาพลามกอนาจารของผู้เยาว์ผ่านอินเทอร์เน็ตจำนวนมาก แต่ปรากฏว่าฐานความผิดนี้ถูกแก้ไขในการพิจารณาชั้นคณะกรรมาธิการของสภาผู้แทนราษฎร โดยปรับแก้ถ้อยคำเป็นการนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามกให้ถือเป็นความผิดตามกฎหมาย ตามที่ปรากฏในมาตรา 14 (4) ซึ่งเป็นการกล่าวถึงสิ่งลามกในภาพรวม และมีความซ้ำซ้อนกับฐานความผิดในประมวลกฎหมายอาญา

ทั้งนี้ ความแตกต่างของความผิดเกี่ยวกับสิ่งลามกที่กำหนดในกฎหมายปัจจุบันกับความผิดกรณีภาพลามกอนาจารของผู้เยาว์ตามแนวทางสากลนั้น หากพิจารณาจากแนวคิดในประเทศตะวันตกภาพลามกอนาจารทั่วไปโดยหลักถือเป็นเรื่องที่ไม่ผิดกฎหมายแต่มีการจำกัดอายุของผู้เข้าถึงข้อมูลเหล่านี้ แต่หากเป็นภาพลามกอนาจารของผู้เยาว์ หรือ Child Pornography นั้นถือเป็นสิ่งผิดกฎหมาย แม้เพียงแต่มีไว้ในครอบครองก็ถือเป็นความผิดแล้ว เนื่องจากในต่างประเทศต้องการมุ่งเน้นการปกป้องดูแลเยาวชน แต่สำหรับประเทศไทยได้มีการกำหนดความผิดเกี่ยวกับสิ่งลามกไว้ โดยหากมีไว้เพื่อประโยชน์ทางการค้า การจำหน่าย จ่ายแจกถือเป็นความผิดทั้งสิ้นโดยไม่คำนึงว่าเป็นภาพลามกอนาจารของผู้ใหญ่หรือผู้เยาว์ ซึ่งมิได้กำหนดให้การครอบครองภาพลามกอนาจารเป็นความผิด จากความแตกต่างข้างต้นจึงก่อให้เกิดปัญหาในทางปฏิบัติโดยเฉพาะอย่างยิ่งเรื่องการส่งผู้ร้ายข้ามแดนที่การรับตัวผู้กระทำความผิดจากอีกประเทศหนึ่ง ประเทศไทยกับประเทศดังกล่าวต้องมีฐานความผิดตามกฎหมายที่รองรับเหมือนกัน ซึ่งเป็นหลักกฎหมายอาญาเกี่ยวกับ Double Criminality ทำให้เกิดเป็นช่องว่างทางกฎหมายที่ประเทศไทยไม่สามารถรับตัวนักโทษที่กระทำความผิดฐานครอบครองภาพลามกอนาจารของผู้เยาว์เพื่อมารับโทษต่อที่ประเทศไทยได้ ซึ่งกรณีดังกล่าวสร้างความกังวลแก่ผู้บังคับใช้กฎหมายโดยเฉพาะยิ่งสำนักงานอัยการสูงสุดที่เป็นผู้รับผิดชอบในกรณีนี้อย่างมาก จึงได้นำเสนอให้มีการพิจารณาถึงความเป็นไปได้ในการเพิ่มฐานความผิดเกี่ยวกับภาพลามกอนาจารไว้ในกฎหมายฉบับนี้

ในประเด็นนี้จึงมีการนำเสนอเป็น 2 แนวทางด้วยกัน

<u>แนวทางที่ 1</u> การปรับแก้บทบัญญัติในประมวลกฎหมายอาญาให้รองรับหลักการเรื่องการครอบครองภาพลามกของผู้เยาว์ โดยหากมคอมพวเตอร์เข้าไปเกี่ยวข้อง เช่น การเผยแพร่ผ่านสื่ออินเทอร์เน็ต ก็อาจกำหนดระวางโทษให้สูงขึ้นกว่าปกติ แนวทางดังกล่าวน่าจะมีความเหมาะสมกว่าการกำหนดฐานความผิดไว้ในกฎหมายฉบับนี้

<u>แนวทางที่ 2</u> การแก้ไขเพิ่มเติมในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งปรากฏอยู่ในมาตรา 14 (3) โดยปรับปรุงถ้อยคำให้สอดคล้องกับกฎหมายสากล ซึ่งแนวทางในเบื้องต้นนำเสนอดังนี้

“มาตรา ... ผู้ใดครอบครองข้อมูลคอมพิวเตอร์ซึ่งมีลักษณะอันลามกที่เกี่ยวข้องกับเด็กหรือเยาวชน ต้องระวางโทษจำคุกไม่เกินหกปี หรือปรับไม่เกินสองแสนบาท หรือทั้งจำทั้งปรับ

ความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำของพนักงานเจ้าหน้าที่ เพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัตินี้หรือตามกฎหมายอื่น”

6) ชุดคำสั่งไม่พึงประสงค์

แม้มาตรา 21 แห่งพ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ นั้นยังไม่เคยมีการนำมาใช้ในทางปฏิบัติ แต่การกำหนดความหมายคำว่า "ชุดคำสั่งไม่พึงประสงค์" ตามความในวรรคสองทำให้เกิดปัญหาการตีความว่าอย่างไรจึงจะถือว่าเป็นชุดคำสั่งไม่พึงประสงค์ เนื่องจากชุดคำสั่งบางอย่างแม้จะมีลักษณะเป็นการปิดกั้นคำสั่งการทำงานของข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่น แต่ก็มีความจำเป็นต้องใช้ชุดคำสั่งนั้น เช่น โปรแกรม anti-virus ที่จะไปทำการแก้ไขเปลี่ยนแปลง หรือยับยั้งการทำงานของชุดคำสั่งที่เป็นไวรัส เช่นนี้ถ้าตีความตรงตามคำนิยามก็จะทำให้ชุดคำสั่งดังกล่าวเข้าข่ายเป็นชุดคำสั่งไม่พึงประสงค์เช่นเดียวกัน เป็นต้น และแม้จะมีการกำหนดให้สามารถประกาศยกเว้นได้ แต่ก็ไม่เคยมีการประกาศกำหนดชุดคำสั่งไม่พึงประสงค์หรือข้อยกเว้นแต่อย่างใด และเห็นว่าเรื่องนี้น่าจะเป็นเรื่องความมั่นคงปลอดภัยมากกว่าอาชญากรรมคอมพิวเตอร์ ซึ่งโดยเจตนารมณ์ของกฎหมายเจตนาจะให้หมายถึง malicious code ซึ่งมีความมุ่งหมายที่จะยับยั้งชุดคำสั่งจำพวกมัลแวร์ (Malware) มิได้มีเจตนาจะให้ครอบคลุมถึงโปรแกรมสำหรับการใช้งานจำพวก anti-virus แต่โดยเหตุที่ต้องการจะให้มีความชัดเจนจึงได้กำหนดความหมายไว้โดยมุ่งเน้นที่ผลคือ "ไม่พึงประสงค์" แต่เหตุที่ถ้อยคำดังกล่าวสามารถตีความได้หลายนัยจึงทำให้เกิดปัญหาในการตีความ นอกจากนี้ การจะประกาศกำหนดข้อยกเว้นก็ทำได้ยากในทางปฏิบัติเนื่องจากชุดคำสั่งมีเป็นจำนวนมหาศาล การประกาศอาจไม่ทันต่อความเปลี่ยนแปลงทางเทคโนโลยี จึงได้นำเสนอแนวทางในการปรับปรุงคำนิยามโดยพิจารณาปรับแก้ถ้อยคำให้เหมาะสม โดยเทียบเคียงจากแหล่งที่มาต่างๆ[1] จึงได้เสนอปรับแก้ถ้อยคำในวรรคสองเป็นดังนี้

"ชุดคำสั่งไม่พึงประสงค์ตามวรรคหนึ่งหมายถึงชุดคำสั่งที่สร้างขึ้นโดยมีเจตนามุ่งร้าย อันมีผลทำให้ข้อมูล คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ หรือโดยประการอื่นตามที่กำหนดในกฎกระทรวง"

---

[1] ***SPECTRIA InfoSec Services, "Malicious Code 101 Definitions and Background"***

Malicious code is software that performs unauthorized functions causing the normal operation of an information system to be abnormal. According to SPECTRIA InfoSec Services, malicious code is defined as "software which interferes with the normal operation of a computer system" or "software, which executes without the express consent of the user."

http://www.webopedia.com

Malicious code is the term used to describe any code in any part of a softwaresystem or script that is intended to cause undesired effects, security breaches or damage to a system. Malicious code describes a broad category of system security terms that includes attack scripts, viruses, worms, Trojan horses,backdoors, and malicious active content.

http://computer.yourdictionary.com

Malicious Code - technical definition

Programs such as viruses and worms designed to exploit weaknesses in computer software replicate and/or attach themselves to other software programs on a computer or a network. Because they are designed to cause harm to a computerÂ's or a networkÂ's operation, viruses and worms are known as malicious code. In short, malicious code not only propagates itself but also typically causes damage to a computer system Â— such as denying access to legitimate users, altering or deleting data, or deleting complete file systems and disks.

2. ภาระหน้าที่ และการกำหนดความรับผิดของผู้ให้บริการ

2.1 ความรับผิดของผู้ให้บริการ

เนื่องจากการให้บริการที่เกี่ยวข้องกับอินเทอร์เน็ตมีหลากหลายลักษณะ ซึ่งการให้บริการบางอย่างมีลักษณะเป็นเพียงตัวกลางหรือสื่อกลางในการเข้าถึงข้อมูลเท่านั้น แต่จากนิยามคำว่า “ผู้ให้บริการ” ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีความหมายอย่างกว้าง ซึ่งเมื่อนำมาพิจารณาเชื่อมโยงกับประเด็นด้านความรับผิดของผู้ให้บริการที่กำหนดไว้ในมาตรา 15 ซึ่งถ้อยคำยังไม่ชัดเจนและต้องอาศัยการตีความ จึงสร้างความกังวลให้กับผู้ประกอบการที่เป็นผู้ให้บริการประเภทต่างๆ ที่เข้าใจว่าอาจจะต้องมีความรับผิดตามกฎหมายด้วย ทำให้ฝั่งผู้ให้บริการเองก็ได้มีการเสนอให้ทบทวนถึงการกำหนดคำนิยามและจำแนกประเภทและลำดับชั้นของผู้ให้บริการเพื่อให้การบังคับใช้กฎหมายสอดคล้องในทางปฏิบัติ ในที่นี้รวมถึงให้ภาครัฐกาหนดขนตอนในการดาเนนการต่างๆ ที่ชัดเจนเพื่อให้โอกาสผู้ให้บริการดำเนินการแก้ไขก่อนที่จะให้ผู้ให้บริการต้องรับผิดตามกฎหมาย เช่น กำหนดระยะเวลาที่ชัดเจนให้ผู้ให้บริการดำเนินการแก้ไขเนื้อหาที่ผิดกฎหมายในเว็บไซต์ที่ให้บริการ เป็นต้น

ทั้งนี้ ความมุ่งหมายแต่เดิมของผู้ยกร่างกฎหมายฉบับนี้คือ การที่จะถือว่าผู้ให้บริการสนับสนุนหรือยินยอมก็ต่อเมื่อมีการร้องขอต่อศาลเพื่อให้มีคำสั่งปิดกั้นเว็บไซต์ แล้วผู้ให้บริการต้องตรวจสอบข้อเท็จจริงที่เกิดขึ้นและแก้ไขปัญหาดังกล่าว หากผู้ให้บรการเพกเฉยย่อมถือเท่ากับว่าเป็นการสนับสนุนหรือยินยอมให้มีการกระทำความผิด แต่อย่างไรก็ตาม คำว่า “จงใจ” เป็นแนวคิดในทางแพ่งตามกฎหมายละเมิดและไม่ควรนำมาใช้ในกฎหมายอาญาที่พิจารณาเรื่องเจตนาเป็นหลัก และอาจทำให้เกิดปัญหาในการตีความได้ ซึ่งในทางปฏิบัติเมื่อเกิดข้อพิพาทขึ้นศาลจะเป็นผู้พิจารณาหรือตีความเองว่าการกระทำของผู้ให้บริการถือได้ว่าเป็นการสนับสนุนหรือยนยอมหรอไม่ จงเสนอให้มการปรบแก้ถ้อยคาจากคาว่า “จงใจสนบสนนหรอยนยอม” เป็นคาว่า “รู้หรอควรได้รู้”

คำว่า “รู้หรือควรได้รู้” นั้น หมายความถึงเจ้าหน้าที่ของผู้ให้บริการที่มีหน้าที่ในการควบคุมดูแลระบบคอมพิวเตอร์รู้หรือควรจะได้รู้ว่ามีข้อมลคอมพิวเตอร์ที่มีลักษณะอันเป็นความผิดอยู่ในระบบคอมพิวเตอร์ของตน โดยไม่จำต้องกำหนดชัดเจนว่าจะถือว่ารู้ต่อเมื่อได้รับแจ้งจากพนักงานเจ้าหน้าที่ตามกฎหมายว่ามีข้อมูลคอมพิวเตอร์ที่มีลักษณะอันเป็นความผิดอยู่ในระบบคอมพิวเตอร์ของผู้ให้บริการ เนื่องจากผู้ให้บริการควรจะต้องมีมาตรการในการกำกับดูแลการให้บริการของตน หากกำหนดให้ถือว่า “รู้” ต่อเมื่อได้รับแจ้งจากพนักงานเจ้าหน้าที่อาจกลายเป็นช่องว่างทำให้ผู้ให้บริการหลีกเลี่ยงหรือละเลยมาตรการในการกำกับดูแลตนเอง และละเลยมาตรการตรวจสอบข้อมูลที่ไม่เหมาะสม กล่าวคือ แม้จะรู้ว่ามีข้อมูลลักษณะดังกล่าวแต่เมื่อไม่ได้รับแจ้งจากพนักงานเจ้าหน้าที่ผู้ให้บริการอาจปล่อยปละละเลยและไม่จัดการแก้ไขก็เป็นได้

สำหรับการกำหนดระยะเวลาในการจัดการเนื้อหาที่ไม่เหมาะสมนั้น ในมุมของผู้บังคับใช้กฎหมายยังมีข้อกังวลอยู่ว่า การกำหนดระยะเวลาแน่นอนก็อาจเกิดเป็นช่องว่างที่ผู้ให้บริการจะไม่จัดการกับเนื้อหาที่ไม่เหมาะสมในทันทีที่ตนเองสามารถทำได้ เนื่องจากยังไม่ครบกำหนดระยะเวลาที่พนักงานเจ้าหน้าที่กำหนด ทำให้เนื้อหาดังกล่าวยังสามารถเผยแพร่ต่อไปได้ และมีการส่งต่อกันออกไปไม่มีสิ้นสุด ดังนั้น การกำหนดรายละเอียดที่เฉพาะเจาะจงมากเกินไปก็อาจทำให้กลายเป็นอุปสรรคต่อการดำเนินงานของพนักงานเจ้าหน้าที่ได้ ขณะเดียวกันในมุมของผู้ให้บริการการกำหนดระยะเวลาตายตัวอาจก่อให้เกิดภาระอย่างมากแก่ผู้ให้บริการบางราย เนื่องจากข้อมูลที่ปรากฏในระบบคอมพิวเตอร์ของผู้ให้บริการแต่ละรายไม่เท่ากัน เช่น เว็บ A มีกระทู้เข้าวันละ 10,000 กระทู้ ในขณะที่เว็บ B มีกระทู้เข้าเพียงวันละ 10 กระทู้ ความสามารถในการตรวจสอบข้อความย่อมแตกต่างกัน เป็นต้น ดังนั้น แนวทางที่จะนำเสนอจึงเห็นว่าเรื่องกำหนดระยะเวลาใน

การดำเนินการกับเนื้อหาที่ไม่เหมาะสมนั้นควรจะให้พนักงานเจ้าหน้าที่กับผู้ให้บริการได้หารือร่วมกันและกำหนดเป็นเกณฑ์มาตรฐานระหว่างกันเอง เพื่อให้มีการใช้ดุลพินิจที่เหมาะสมเป็นกรณีไป ทั้งนี้ขึ้นอยู่กับประเภท ขนาด แนวปฏิบัติของผู้ให้บริการที่จะทำการตกลงร่วมกันเสมือนเป็น Best practice

อย่างไรก็ดี มีแนวคิดเสนอให้มีการนำมาตรการ Notice and Takedown และ Safe Harbor มาพิจารณาประกอบการกำหนดหน้าที่และความรับผิดของผู้ให้บริการ ซึ่งทั้งสองมาตรการเป็นหลักการในการจัดการปัญหาการละเมิดลิขสิทธิ์ของสหรัฐอเมริกาซึ่งกำหนดให้ผู้ให้บริการทำหน้าที่เสมือนหนึ่งเป็นเจ้าพนักงานในการตรวจสอบและกลั่นกรองเนื้อหา จึงอาจนำมาตรการดังกล่าวมาปรับใช้กับการกำหนดหน้าที่ความรับผิดของผู้ให้บริการตามมาตรานี้เพื่อสร้างความชัดเจนเกี่ยวกับระยะเวลาและขั้นตอนการดำเนินการ แต่ก็มีข้อสังเกตว่า ทั้ง Safe Harbor และ Notice & Take down ไม่อาจใช้ได้กับเนื้อหาทุกประเภท สิ่งที่ Notice & Take down จะมีประสิทธิภาพคือเป็นกรณีที่คนในสังคมส่วนใหญ่รู้หรือมีหลักปฏิบัติที่ชัดเจน เช่น YouTube, Facebook ที่ Notice & Take down จะถกใช้มากที่สุดในทางลิขสิทธิ์ นอกจากนี้ การนำมาตรการ Notice & Take down มาใช้ เท่ากับให้ผู้ให้บริการทำหน้าที่เสมือนเป็นศาล คือต้องพิจารณาว่าเนื้อหานั้นเป็นความผิดหรือไม่ เพื่อจะได้ตัดสินใจว่าเอาลงหรือไม่เอาลง

ดังนั้น ในการนำเสนอแนวทางการปรับปรุงจึงได้นำเสนอถ้อยคำเป็น 2 ลักษณะ ดังนี้

<u>แนวทางที่ 1</u>

“มาตรา ... ผู้ให้บริการผู้ใดรู้หรือควรได้รู้ว่ามีข้อมูลคอมพิวเตอร์อันเป็นความผิดตามมาตรา ... (ข้อมูลอันเป็นความผิดเกี่ยวกับความมั่นคง) หรือมาตรา ... (ข้อมูลที่อาจก่อให้เกิดความเสียหายต่อความมั่นคง) ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน และมิได้ดำเนินการแก้ไขหรือระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ดังกล่าวโดยเร็ว ต้องระวางโทษดังที่บัญญัติไว้ในมาตรานั้น ๆ”

<u>แนวทางที่ 2</u>

“มาตรา ... เมื่อผู้ให้บริการรู้ หรือควรได้รู้ หรือได้รับแจ้งจากพนักงานเจ้าหน้าที่ ถึงการกระทำอันเป็นความผิดตามมาตรา ... (ข้อมูลอันเป็นความผิดเกี่ยวกับความมั่นคง) หรือมาตรา ... (ข้อมูลที่อาจก่อให้เกิดความเสียหายต่อความมั่นคง) ซึ่งปรากฏอยู่ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ให้รีบดำเนินการแก้ไขหรือระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ดังกล่าวภายในเวลาอันเหมาะสมนับแต่วันที่รู้หรือได้รับแจ้งหรือภายในระยะเวลาที่พนักงานเจ้าหน้าที่กำหนด หากผู้ให้บริการมิได้ดำเนินการแก้ไขหรือระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ดังกล่าว ต้องระวางโทษ ...

ผู้ให้บริการตามวรรคหนึ่งหมายความถึงบุคคลผู้ดูแลหรือได้รับมอบหมายให้เป็นผู้ดูแลเนื้อหาที่ปรากฏอยู่ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน

หลักเกณฑ์และวิธีการดำเนินการของพนักงานเจ้าหน้าที่ตามวรรคหนึ่ง ให้เป็นไปตามที่รัฐมนตรีประกาศกำหนด”

2.2 ระยะเวลาและรูปแบบการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ที่เหมาะสมและมีคุณภาพ

สำหรับการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ซึ่งตามกฎหมายกำหนดให้ผู้ให้บริการต้องมีการจัดเก็บไม่น้อยกว่า 90 วัน รวมถึงมีการออกหลักเกณฑ์ในทางปฏิบัติเกี่ยวกับการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ตามประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารนั้น มีข้อสังเกตว่าหลักเกณฑ์ที่กำหนดในกฎหมายเหล่านี้ยังไม่สามารถนำไปสู่การบังคับใช้กฎหมายได้อย่างมีประสิทธิภาพ และยังเป็นการสร้างภาระเพิ่มเติมแก่ผู้ให้บริการ จึงมีการเสนอให้ทบทวนหลักเกณฑ์เกี่ยวกับประเภทของผู้ให้บริการ

ที่ต้องจัดเก็บข้อมูลจราจร มาตรฐานข้อมูลจราจรที่ต้องจัดเก็บ และระยะเวลาในการจัดเก็บที่เหมาะสมและสอดคล้องในทางปฏิบัติ นอกจากนี้ ในประเด็นเกี่ยวกับการกำหนดระยะเวลาการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ตามประเภทธุรกิจบริการ และการกำหนด ขั้นตอน และมาตรฐานการจัดเก็บที่มีความชัดเจนนั้น เนื่องจากเทคโนโลยีและรูปแบบการให้บริการมีการพัฒนาอย่างรวดเร็ว การจะกำหนดรายละเอียดไว้ในพระราชบัญญัติฉบับนี้จึงอาจทำให้ยากต่อการแก้ไขให้ทันกับเทคโนโลยี

ดังนั้น จึงนำเสนอแนวทางในการปรับแก้กฎหมายโดยคงหลักการในการกำหนดระยะเวลาการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ 90 วันไว้ โดยกำหนดให้เป็นระยะเวลาขั้นต่ำในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ และเปิดช่องให้พนักงานเจ้าหน้าที่มีคำสั่งให้จัดเก็บข้อมูลดังกล่าวเกินกว่า 90 วันได้ และเสนอให้มีการปรับเปลี่ยนถ้อยคำที่ว่า “ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้” เป็นคำว่า “ในกรณีจำเป็นพนักงานเจ้าหน้าที่ที่ได้รับมอบหมายจะสั่งให้” เพื่อให้มีความชัดเจนว่าพนักงานเจ้าหน้าที่นั้นต้องเป็นผู้ที่ได้รับมอบหมายเพื่อป้องกันการใช้อำนาจเกินขอบเขต โดยอาจมีการแต่งตั้งหรือการประกาศโดยมอบหมายให้ชัดแจ้ง นอกจากนี้ ตามความในวรรคสามของกฎหมายปัจจุบันที่ว่า “ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใด...” นั้น มีขอบเขตจำกัดเฉพาะการกำหนดประเภทผู้ให้บริการ ข้อมูลที่ต้องจัดเก็บและการเริ่มจัดเก็บเท่านั้น จึงเสนอปรับเปลี่ยนถ้อยคำเพื่อให้สามารถกำหนดรายละเอียดที่จำเป็นเพิ่มเติมได้ เช่น รายละเอียดในการจัดเก็บ ระยะเวลาในการจัดเก็บ เป็นต้น โดยออกเป็นประกาศกระทรวงอันจะทำให้เกิดความยืดหยุ่นและเหมาะสมกับแต่ละกรณีไป ดังนี้

“มาตรา ... ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่ที่ได้รับมอบหมายจะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินกว่าเก้าสิบวันก็ได้ แต่มิให้เกินกว่า 2 ปี หากกรณีจำเป็นต้องเก็บรักษาเกินกว่าระยะเวลาดังกล่าวให้เป็นไปตามที่รัฐมนตรีประกาศกำหนดเป็นรายกรณีไป

ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง

รายละเอียดและเงื่อนไขการปฏิบัติตามวรรคหนึ่ง ให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท”

3. การระงับการเข้าถึงข้อมูลคอมพิวเตอร์

ในการดำเนินการเพื่อระงับการแพร่หลายของข้อมูลคอมพิวเตอร์หรือการปิดกั้นเว็บไซต์นั้น ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้กำหนดกระบวนการตรวจสอบการใช้อำนาจในการปิดเว็บไซต์ของพนักงานเจ้าหน้าที่ไว้ตามมาตรา 20 โดยกำหนดให้พนักงานเจ้าหน้าที่มีอำนาจร้องขอต่อศาลที่มีเขตอำนาจโดยความเห็นชอบจากรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารขอให้ศาลมีคำสั่งระงับการเผยแพร่ซึ่งข้อมูลคอมพิวเตอร์ หรือสั่งปิดเว็บไซต์ได้ ซึ่งการกำหนดขั้นตอนดังกล่าวในความเห็นของพนักงานเจ้าหน้าที่เห็นว่าก่อให้เกิดข้อจำกัดในการดำเนินการเนื่องจากกระบวนการที่ต้องขอความเห็นชอบต่อรัฐมนตรีและนำพยานหลักฐานเสนอต่อศาลเพื่อให้ศาลมีคำสั่งระงับการเผยแพร่นั้นเป็นกระบวนการที่ทำให้เกิดความล่าช้า ในขณะที่ฝ่ายองค์กรพัฒนาเอกชน (NGOs) มีความเห็นว่ากระบวนการดังกล่าวมิใช่การตรวจสอบการใช้อำนาจของพนักงานเจ้าหน้าที่อย่างแท้จริง แต่เป็น

การกระทำเพื่อสร้างความชอบธรรมให้แก่พนักงานเจ้าหน้าที่ในการใช้อำนาจเพื่อละเมิดต่อสิทธิเสรีภาพขั้นพื้นฐานของประชาชน เช่น freedom of speech เป็นต้น

ในการศึกษาและจัดทำข้อเสนอแนะจึงมีการตั้งข้อสังเกตและข้อเสนอแนะว่า ในกรณีการให้อำนาจพนักงานเจ้าหน้าที่ในการปิดกั้นเว็บไซต์ควรที่จะมีการกลั่นกรองก่อนดำเนินการปิดกั้นและต้องเป็นการดำเนินการโดยพนักงานเจ้าหน้าที่ที่ได้รับมอบหมาย ซึ่งในเบื้องต้นน่าจะลดประเด็นปัญหาทางปฏิบัติอันก่อให้เกิดความกังวลกับผู้ให้บริการได้ แต่ต้องพิจารณาให้สอดคล้องกับรูปแบบในการบูรณาการการทำงานด้วย และโดยเหตุที่ในปัจจุบันมีการร้องขอระงับการแพร่หลายโดยการปิดกั้นเว็บไซต์ แต่กฎหมายไม่ได้เปิดช่องให้มีการเพิกถอนการระงับดังกล่าวจึงได้มีการเสนอหลักการเพิ่มเติมเรื่องการยกเลิกการระงับการเข้าถึงข้อมูลคอมพิวเตอร์เพื่อลดภาระแก่ผู้ให้บริการที่จะต้องดูแลรักษาพื้นที่ในฐานข้อมูลดังกล่าวและมิให้เป็นการละเมิดหรือก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลจนเกินสมควรหากปรากฏในภายหลังว่าข้อความหรือข้อมูลดังกล่าวมิได้เป็นการละเมิดต่อกฎหมายแต่อย่างใด

ประการถัดมา การระงับการเผยแพร่ของข้อมูลในกฎหมายนี้มิได้เปิดช่องให้สามารถดำเนินการในกรณีที่เป็นความผิดตามกฎหมายอื่นได้ จึงนำเสนอแนวทางการปรับแก้กฎหมายให้เปิดช่องในการบงคบใช้หรือดำเนินการกับการกระทำความผิดตามกฎหมายอื่นๆ ที่มีการใช้คอมพิวเตอร์เป็นเครื่องมือได้ด้วย เพื่อให้เกิดการเชื่อมโยงของการบังคับใช้กฎหมายทั้งระบบในการจัดการปัญหาการอาศัยคอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิดอย่างอื่น โดยหากพนักงานเจ้าหน้าที่ตามกฎหมายอื่นๆ เช่น ตำรวจ พนักงานฝ่ายปกครอง เจ้าหน้าที่จากกรมทรัพย์สินทางปัญญา เจ้าหน้าที่จากสำนักงานคณะกรรมการอาหารและยา เป็นต้น พบเห็นการกระทำความผิด เช่น มีการโพสท์ข้อมูลคอมพิวเตอร์หรือจำหน่ายสินค้าที่ผิดกฎหมายที่ตนเองดูแลอยู่ เป็นต้น ก็สามารถร้องขอให้พนักงานเจ้าหน้าที่ตามกฎหมายนี้ใช้ความเชี่ยวชาญในการดำเนินการสืบสวนสอบสวน หรือระงับการเผยแพร่เว็บไซต์ดังกล่าวได้ ทั้งนี้ เมื่อได้มีการปรับแก้โดยขยายขอบเขตอำนาจหน้าที่ในการสืบสวนและสอบสวน เพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด และการระงับการเผยแพร่ข้อมูลได้ในกรณีที่เป็นความผิดตามกฎหมายอื่นแล้ว กฎหมายฉบับนี้จึงครอบคลุมการกระทำความผิดทั้งที่เป็นการกระทำความผิดต่อคอมพิวเตอร์โดยตรง การกระทำความผิดโดยใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด และการกระทำความผิดอื่นที่อาศัยคอมพิวเตอร์เป็นสื่อกลาง โดยไม่จำต้องกำหนดฐานความผิดในทุกกรณีไว้ในกฎหมายฉบับนี้แต่อย่างใด

อย่างไรก็ตาม ในการกำหนดเพิ่มกระบวนการกลั่นกรองและผู้ตรวจสอบก่อนที่จะมีการยื่นคำร้องขอระงับการเข้าถึงเว็บไซต์เป็นรายละเอียดในทางปฏิบัติ จึงควรที่จะกำหนดรายละเอียดแยกต่างหาก และเพื่อให้ง่ายต่อการปรับปรุงให้เหมาะสมกับสภาพแวดล้อมที่เปลี่ยนแปลงไป

ดังนั้น จึงขอนำเสนอแนวทางการปรับปรุงกฎหมายในเบื้องต้นดังนี้

“มาตรา ... ในกรณีที่การกระทำความผิดตามพระราชบัญญัตินี้เป็นการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่อาจเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา <u>ความผิดเกี่ยวกับองค์กรอาชญากรรมข้ามชาติ</u> หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน หรือ<u>การทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์อันเป็นความผิดตามกฎหมายอื่นซึ่งเจ้าหน้าที่ตามกฎหมายนั้นร้องขอ</u> <u>พนักงานเจ้าหน้าที่ที่ได้รับมอบหมาย</u>อาจยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นได้

ในกรณีที่ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ตามวรรคหนึ่ง ให้พนักงานเจ้าหน้าที่ดำเนินการเอง หรือสั่งให้ผู้ให้บริการดำเนินการระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นจนกว่าพฤติการณ์จะเปลี่ยนแปลงไป

หลักเกณฑ์ วิธีการยื่นคำขอ และวิธีพิจารณาคำร้องขอ ตามวรรคหนึ่ง ให้เป็นไปตามระเบียบที่รัฐมนตรีประกาศกำหนด"

4. อำนาจของพนักงานเจ้าหน้าที่

เนื่องจากมาตรา 18 ในพระราชบัญญัติฉบับนี้ให้อำนาจพนักงานเจ้าหน้าที่ในการดำเนินการได้เฉพาะกรณีที่เป็นความผิดตามพระราชบัญญัตินี้เท่านั้น ทำให้ในกรณีที่เป็นความผดตามกฎหมายฉบบอนซงมการใช้คอมพิวเตอร์ในการกระทำความผิด หรือเกี่ยวข้องกับคอมพิวเตอร์ เจ้าหน้าที่ตำรวจหรือเจ้าพนักงานตามกฎหมายอื่นไม่สามารถใช้อำนาจตามกฎหมายฉบับนี้ได้และในขณะเดียวกันพนักงานเจ้าหน้าที่ตามกฎหมายฉบับนี้ก็ไม่สามารถใช้อำนาจตามกฎหมายฉบับนี้ในการสืบค้นและรวบรวมพยานหลักฐานเพื่อนำไปใช้ในคดีอื่นได้ จึงมีการพิจารณาทบทวนเพื่อให้สามารถนำหลักเกณฑ์และวิธีการที่กำหนดในกฎหมายนี้ไปใช้บังคับกับการรวบรวมพยานหลักฐานเพื่อดำเนินคดีตามกฎหมายอื่นได้ด้วย ทั้งนี้ เพื่อให้ขั้นตอนและวิธีการในการดำเนินการเก็บรวบรวมพยานหลักฐานทางคอมพิวเตอร์ซึ่งมีลักษณะเฉพาะเป็นไปโดยถูกต้อง

การกำหนดอำนาจให้พนักงานเจ้าหน้าที่สามารถใช้อำนาจตามกฎหมายที่กำหนดในกรณีที่เป็นการกระทำความผิดตามกฎหมายอื่นได้ด้วยนั้นน่าจะช่วยแก้ปัญหาการหลีกเลี่ยงไปใช้กฎหมายวิธีพิจารณาความอาญาได้ โดยเฉพาะอย่างยิ่งการใช้อำนาจตามมาตรา 18 (4) – (8) เนื่องจากกฎหมายฉบับที่ใช้บังคับอยู่ในปัจจุบันไม่ได้ให้อำนาจไว้ ทำให้ในการปฏิบัติหน้าที่ของเจ้าพนักงานตำรวจต้องเลี่ยงไปใช้กฎหมายวิธีพิจารณาความอาญาแทน ซึ่งกลายเป็นว่าไม่ตกอยู่ภายใต้เงื่อนไขตามที่กำหนดในกฎหมายฉบับนี้อันก่อให้เกิดผลกระทบเป็นอย่างมาก โดยเฉพาะอย่างยิ่งต่อตัวผู้ให้บริการ เช่น การไปยึดเครื่องคอมพิวเตอร์ เป็นต้น ซึ่งกระบวนการตามกฎหมายโดยเฉพาะอย่างยิ่งตามมาตรา 18 (4) – (8) นั้นเป็นการสร้างความมั่นใจให้กับสังคมว่าการเก็บรวบรวมหรือหาพยานหลักฐานนั้น ต้องใช้ผู้มีความรู้ความสามารถ และต้องรู้กลไกทางเครื่องมือและทางธุรกิจ เพื่อไม่ให้กระทบต่อผู้ประกอบการทั้งยังมีกระบวนการตรวจสอบโดยศาล นอกจากนี้แม้จะกำหนดให้ต้องขอหมายศาลแล้วกฎหมายไม่ได้กล่าวถึงเรื่องการเข้าค้น ดังนั้นในการปฏิบัติงานของพนักงานเจ้าหน้าที่หากต้องเข้าตรวจค้นและยึดก็จะต้องขอต่อศาลเพื่อออกหมายค้นและต้องขอหมายตามมาตรา 18 อีกด้วย นั่นก็ยิ่งเป็นการสร้างความน่าเชื่อถือในกระบวนการอันเป็นหลักประกันได้ว่ากระบวนการจัดเก็บพยานหลักฐานทำโดยมืออาชีพ อยู่บนหลักการ Chain of Custody คือหลักการห่วงโซ่ในการคุ้มครองพยานหลักฐาน ซึ่งเป็นหลักประกันในการนำสืบพยานหลักฐานในชั้นศาลที่สร้างความน่าเชื่อถือว่ากระบวนการทั้งหมดมีความน่าเชื่อถือ มีความครบถ้วนและกระบวนการชอบด้วยกฎหมาย นอกจากนี้ พยานหลักฐานทางอิเล็กทรอนิกส์ไม่ได้มีความสำคัญเฉพาะคดีความผิดเกี่ยวกับคอมพิวเตอร์ ดังนั้น หากเอาหลักที่มีอยู่ของกฎหมายฉบับนี้มาใช้ให้เป็นประโยชน์กับกฎหมายอื่นก็จะเป็นประโยชน์ต่อสังคมอย่างมาก เช่น คดีหมิ่นประมาทโดยการโพสในเว็บพันธุ์ทิพย์ จะเห็นได้ว่าไม่มีพยานหลักฐานอย่างอื่นเลย หากเจ้าพนักงานตำรวจไปเก็บพยานหลักฐานโดยวิธีทั่วไปเช่นสั่งพิมพ์ออกมาจากหน้าเว็บ ก็จะกลายเป็นช่องว่างในการยกขึ้นเป็นข้อต่อสู้ในการจัดเก็บ รวบรวมพยานหลักฐานและการยกข้อต่อสู้ถึงความน่าเชื่อถือของพยานหลักฐาน แล้วจะหาหลักฐานได้อย่างไรและหลักฐานที่ได้มานั้นจะมีความน่าเชื่อถือเพียงใดหากไม่ให้ใช้กระบวนการตามกฎหมายฉบับนี้ ดังนั้น จึงได้นำเสนอแนวทางดังต่อไปนี้

"มาตรา ... <u>เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามมาตรา ... (ข้อมูลอันเป็นความผิดเกี่ยวกับความมั่นคง) หรือมาตรา ... (ข้อมูลที่อาจก่อให้เกิดความเสียหายต่อความมั่นคง) หรือการกระทำความผิดที่มีระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์เข้ามาเกี่ยวข้องด้วย ไม่ว่าจะเป็นความผิดตามกฎหมายใด ให้พนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ตามประมวลกฎหมายวิธีพิจารณาความอาญา หรือพนักงานเจ้าหน้าที่ตามกฎหมายอื่นดำเนินการตามพระราชบัญญัตินี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด โดยมีอำนาจอย่างหนึ่งอย่างใด ตามมาตรา ... (1) (2) และ (3) (อำนาจของพนักงานเจ้าหน้าที่ตามพ.ร.บ.คอมฯ) ได้ หรือในกรณีที่ไม่อาจดำเนินการดังกล่าวอาจร้องขอให้พนักงานเจ้าหน้าที่ดำเนินการได้</u>

<u>เพื่อประโยชน์ในการดำเนินการตามวรรคหนึ่ง ในกรณีที่จำเป็นต้องดำเนินการตามมาตรา ... (4) (5) (6) (7) หรือ (8) (อำนาจของพนักงานเจ้าหน้าที่ตามพ.ร.บ.คอมฯ) ให้ร้องขอพนักงานเจ้าหน้าที่เพื่อดำเนินการต่อไป</u>"

เรื่องนี้เป็นหลักการที่นำเสนอขึ้นใหม่โดยให้พนักงานเจ้าหน้าที่สามารถใช้อำนาจตามกฎหมายที่กำหนดในการสืบสวนและสอบสวนเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิดสามารถนำไปใช้ในกรณีที่เป็นการกระทำความผิดตามกฎหมายอื่นได้ และในขณะเดียวกันก็ให้อำนาจพนักงานฝ่ายปกครองหรือตำรวจในการสืบสวนและสอบสวนกรณีมีการกระทำความผิดที่มีระบบคอมพิวเตอร์ ข้อมูล คอมพิวเตอร์ หรืออุปกรณ์คอมพิวเตอร์เข้ามาเกี่ยวข้องสามารถดำเนินการตามกฎหมายฉบับนี้ได้เช่นเดียวกันนั้น ซึ่งในหลักการที่นำเสนอนี้ให้อำนาจแก่พนักงานฝ่ายปกครองหรือตำรวจตามประมวลกฎหมายวิธีพิจารณาความอาญา หรือพนักงานเจ้าหน้าที่ตามกฎหมายอื่น ดำเนินการตามพระราชบัญญัตินี้ โดยมีอำนาจตาม มาตรา 18 (1) – (3) นั้น อย่างไรก็ตาม ในทางปฏิบัติพนักงานฝ่ายปกครองหรือตำรวจตามประมวลกฎหมายวิธีพิจารณาความอาญา หรือพนักงานเจ้าหน้าที่ตามกฎหมายอื่นอาจขาดความรู้ความชำนาญ หรือความเข้าใจในทางเทคนิคที่จำเป็นต่อการปฏิบัติงานและอาจจำเป็นต้องขอความร่วมมือจากพนักงานเจ้าหน้าที่ตามกฎหมายนี้ จึงเสนอเปิดช่องไว้เพื่อให้ดำเนินการได้ด้วย

สำหรับการดำเนินการตามมาตรา 18 (4) – (8) นั้น ได้กำหนดให้พนักงานฝ่ายปกครองหรือตำรวจ หรือพนักงานเจ้าหน้าที่ตามกฎหมายอื่นต้องร้องขอให้พนักงานเจ้าหน้าที่ตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ดำเนินการ เนื่องจากกรณีดังกล่าวเป็นเรื่องที่กระทบต่อสิทธิของบุคคลอื่นและต้องอาศัยความรู้ความชำนาญทางเทคโนโลยี จึงต้องการจำกัดอำนาจของเจ้าพนักงานตามกฎหมายอื่นในการใช้อำนาจตามกฎหมายนี้ โดยกำหนดให้กระทำได้ต่อเมื่อร้องขอให้พนักงานเจ้าหน้าที่ตามกฎหมายนี้เป็นผู้ดำเนินการ

5. การกระทำความผิดนอกราชอาณาจักร

5.1 หลักดินแดน

ในการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ไม่ว่าจะเป็นการกระทำความผิดต่อคอมพิวเตอร์โดยแท้ หรือใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด ย่อมเป็นการกระทำที่ปราศจากข้อจำกัดทางด้านดินแดน หากปรากฏว่าการกระทำความผิดเกิดขึ้นนอกราชอาณาจักร ย่อมไม่สามารถนำตัวบุคคลผู้กระทำความผิดมาลงโทษได้ จึงได้นำเสนอให้เพิ่มเติม "หลักดินแดน" โดย<u>เทียบเคียงมาตรา 5 แห่ง ประมวลกฎหมายอาญา เพื่อให้ตรงตามเจตนารมณ์ของเรื่องในการขยายหลักดินแดนในกรณีที่มีการกระทำความผิดเกิดขึ้นนอกราชอาณาจักร</u> ดังนี้

"มาตรา ... ความผิดตามพระราชบัญญัตินี้ที่การกระทำแม้แต่ส่วนหนึ่งส่วนใดได้กระทำในราชอาณาจักรก็ดี ผลแห่งการกระทำเกิดในราชอาณาจักรโดยผู้กระทำประสงค์ให้ผลนั้นเกิดในราชอาณาจักร หรือโดยลักษณะแห่งการกระทำผลที่เกิดขึ้นควรเกิดในราชอาณาจักร หรือโดยลักษณะแห่งการกระทำผลที่เกิดขึ้นควรเกิดในราชอาณาจักรหรือย่อมจะเล็งเห็นได้ว่าผลนั้นจะเกิดในราชอาณาจักรก็ดี ให้ถือว่าความผิดนั้นได้กระทำในราชอาณาจักร และต้องรับโทษภายในราชอาณาจักร"

5.2 หลักบุคคล

ในกรณีที่เป็นการกระทำความผิดนอกราชอาณาจักรซึ่งกฎหมายฉบับนี้ได้นำหลักการตามมาตรา 8 แห่งประมวลกฎหมายอาญามาใช้บังคับนั้น เนื่องจากการกระทำความผิดเกี่ยวกับคอมพิวเตอร์เป็นการกระทำที่อาจก่อให้เกิดความเสียหายในวงกว้างภายในเวลาอันรวดเร็ว การกระทำความผิดบางกรณีโดยเฉพาะอย่างยิ่งกรณีที่เป็นการกระทำความผิดอันกระทบกระเทือนต่อความมั่นคงของประเทศซึ่งหากต้องมีการร้องขอตามกระบวนการทั่วไปอาจไม่ทันกับการแก้ไขสถานการณ์หรือความเสียหายที่เกิดขึ้น ดังนั้นจึงเสนอแนวทางให้เพิ่มเพิ่มเติมข้อยกเว้นในกรณีการกระทำความผิดที่อาจกระทบกระเทือนต่อความมั่นคงของประเทศเพื่อให้พนักงานเจ้าหน้าที่สามารถดำเนินการได้แม้จะไม่มีการร้องขอจากผู้เสียหาย ดังนี้

"มาตรา ... ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักรและ

(1) ผู้กระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้นหรือผู้เสียหายได้ร้องขอให้ลงโทษ หรือ

(2) ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็นผู้เสียหายและผู้เสียหายได้ร้องขอให้ลงโทษ

ต้องรับโทษภายในราชอาณาจักร เว้นแต่กรณีที่เป็นการกระทำความผิดตามมาตรา ... (บทหนัก) มาตรา ... (ข้อมูลอันเป็นความผิดเกี่ยวกับความมั่นคง) หรือมาตรา ... (ข้อมูลที่อาจก่อให้เกิดความเสียหายต่อความมั่นคง) ไม่จำต้องร้องขอให้ลงโทษ

ให้นำความในมาตรา 10 แห่งประมวลกฎหมายอาญามาใช้บังคับโดยอนุโลม"