มูลนิธิเพื่ออินเทอร์เน็ตและวัฒนธรรมพลเมือง Foundation for Internet and Civic Culture
15 ซอยประดิพัทธ์ 17 ชั้น 5 อาคารรัจนาการ 15 Soi Pradipat 17. Rajanakarn Building 5th Floor
แขวงสามเสนใน เขตพญาไท กทม. 10400 Phaya Thai, Bangkok 10500 Thailand
https://thainetizen.org contact@thainetizen.org

12 ข้อเสนอ แก้ไขร่างพ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่..) พ.ศ. .... (ร่าง 26 เม.ย. 2559) (7 ก.ค. 2559)

ข้อเสนอที่เครือข่ายพลเมืองเน็ตยื่นต่อสภานิติบัญญัติแห่งชาติเมื่อวันที่ 7 กรกฎาคม 2559 โดยปรับปรุงจากจากข้อสังเกตและข้อเสนอในจดหมายเข้าชื่อให้แก้ไขกฎหมายบนเว็บไซต์ Change.org และการนำเสนอในงานเสวนาวิชาการ "เสรีภาพออนไลน์ภายใต้กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์" 27 มิถุนายน 2559 (จัดโดย สมาคมนักข่าวนักหนังสือพิมพ์แห่งประเทศไทย สมาคมนักกฎหมายสิทธิมนุษยชน สนับสนุนโดย สมาคมเครือข่ายผู้สื่อข่าวในเอเชียตะวันออกเฉียงใต้)

เอกสารข้อเสนอ https://thainetizen.org/docs/ จดหมายเข้าสื่อสนับสนุน https://change.org/singlegatewayreturn

1. มาตรา 14 (1) ควรแก้ไขให้ชัดเจนว่าเป็นการเอาผิดกับ phishing และตัดโอกาสในการใช้ฟ้องหมิ่นประมาทออกไป

- มาตรา 14 (1) ของร่างวันที่ 26 เม.ย. 2559 ระบุว่า *"ผู้ใด... โดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน"*
- คำว่า "โดยหลอกลวง" อาจถูกตีความให้นำมาใช้กับความผิดฐานหมิ่นประมาทได้ ทั้งที่เจตนารมณ์แท้จริงของกฎหมายมุ่งที่จะเอาผิดเรื่องฟิชชิ่ง (phishing) หรือการทำเว็บไซต์หรือข้อมูลปลอมเพื่อนำไปหลอกเอาทรัพย์สินหรือข้อมูลส่วนบุคคลจากเหยื่อ
- "เจตนารมณ์ของกฎหมาย มาตรา 14 แห่งพระราชบัญญัตินี้มิได้มุ่งเจตนาลงโทษผู้กระทำความผิดฐานหมิ่นประมาทด้วยการโฆษณา" – คำพิพากษาคดีกองทัพเรือ vs สำนักข่าวภูเก็ตหวาน (คดีหมายเลขดำที่ 2161/2557 คดีหมายเลขแดงที่ 6565/2558) (ดูเอกสาร [19])
- **เสนอให้ใช้ภาษาในลักษณะร่างมาตรา 14 (1) ของร่างพ.ร.บ.คอมพิวเตอร์ฯ ฉบับที่คณะกรรมการกฤษฎีกาตรวจพิจารณาแล้ว (เรื่องเสร็จที่ 919/2558) ซึ่งเขียนว่า "ผู้ใดโดยทุจริตนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ ทำให้ได้ไปซึ่งทรัพย์สินหรือข้อมูลส่วนบุคคลของผู้อื่น หรือทำให้ผู้อื่นทำ ถอน หรือทำลายเอกสารสิทธิต้องระวางโทษ...." จะทำให้ชัดเจนกว่าว่าหมายถึงความผิดเฉพาะเรื่องฟิชชิ่ง (ดูเอกสาร [1] และ [2]) ทั้งนี้ควรเปลี่ยนคำว่า "ข้อมูลคอมพิวเตอร์อันเป็นเท็จ" เป็น "ข้อมูลคอมพิวเตอร์ปลอม" ด้วย เพื่อให้ตรงกับความหมายของ "forgery" (ดู [25])**
- **เสนอให้ทบทวนภาษาในร่างมาตรา 14 ทั้งหมด ให้ใช้เจาะจงกับความผิดในลักษณะ Computer-**

related Crime ในลักษณะเดียวมาตรา 264 ของประมวลกฎหมายอาญา (ปลอมแปลงเอกสาร) และ Title 2 – Computer-related offences, Article 7 – Computer-related forgery และ Article 8 – Computer-related fraud ของ Convention on Cybercrime ของ Council of Europe (ดู [21])

- หมายเหตุ: หากยืนยันจะให้สามารถใช้เอาผิดกับเนื้อหาลักษณะหมิ่นประมาทได้อยู่ จำเป็นต้อง 1) พิจารณาความเหมาะสมของโทษให้สอดคล้องกับประมวลกฎหมายอาญา 2) ให้มีบทยกเว้นความผิดในแบบที่มาตรา 16 ของพ.ร.บ.คอมพิวเตอร์และประมวลกฎหมายอาญามีอยู่ด้วย

2. มาตรา 14 (2): กำหนดความผิดต่อ “ความปลอดภัยสาธารณะ” และ “ความมั่นคงทางเศรษฐกิจ” ให้ชัดเจน

- มาตรา 14 (2) ของร่างที่แก้ไขใหม่ กำหนดความผิดฐานโพสต์ข้อมูลเท็จที่กระทบต่อ “ความปลอดภัยสาธารณะ” หรือ “ความมั่นคงทางเศรษฐกิจ” ซึ่งคำทั้งสองไม่ปรากฏใช้ในกฎหมายอาญาอื่น การใช้คำที่ไม่ชัดเจนเช่นนี้ อาจส่งผลให้การบังคับใช้กฎหมายมีปัญหา สร้างความลำบากให้กับผู้บังคับใช้กฎหมาย หรืออาจถูกนำไปใช้ในทางที่มิชอบ (ดู [2])
- หากต้องการคุ้มครองระบบคอมพิวเตอร์ที่มีความสำคัญต่อชีวิตและความมั่นคง เช่น ระบบโครงสร้างพื้นฐานของประเทศ ระบบป้องกันประเทศ สามารถระบุให้ชัดได้ โดยอาจใช้แนวทางของสหรัฐอเมริกาและสหภาพยุโรป เกี่ยวกับโครงสร้งพื้นฐานที่สำคัญอย่างยิ่งยวด (critical intrastructure)
- **เสนอให้กำหนดความผิดให้ชัดเจนว่าเป็นการทำต่อระบบคอมพิวเตอร์ ในประการที่น่าจะทำให้เกิดความเสียหายต่อความมั่นคงของชาติและความปลอดภัยสาธารณะ โดยอาจกำหนดให้หมายถึงการโพสต์ข้อมูลคอมพิวเตอร์เท็จที่กระทบต่อ “โครงสร้างพื้นฐานที่สำคัญอย่างยิ่งยวด” เช่นแก้ไขร่างมาตรา 14 (2) เป็น**

  มาตรา 14 (2) นำเข้าสู่ระบบคอมพิวเตอร์ในกิจการตามประกาศของรัฐมนตรีว่าด้วยกิจการที่เป็นโครงสร้างพื้นฐานที่สำคัญอย่างยิ่งยวดของประเทศ ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จโดยประการที่น่าจะเกิดความเสียหายต่อโครงสร้างพื้นฐานที่สำคัญอย่างยิ่งยวดของประเทศ

  และให้กำหนดนิยาม “โครงสร้างพื้นฐานที่สำคัญอย่างยิ่งยวดของประเทศ” ไว้ในส่วนนิยม (มาตรา 3) หรือที่ในมาตรา 14 เอง ว่า

  “โครงสร้างพื้นฐานที่สำคัญอย่างยิ่งยวดของประเทศ” หมายความว่า ระบบและทรัพย์สิน ทั้งทาง

กายภาพและทางคอมพิวเตอร์ ที่สำคัญอย่างยิ่งต่อประเทศ จนการทำลายหรือทำให้ไร้ ความสามารถของระบบหรือทรัพย์สินดังกล่าว อาจทำให้เกิดผลกระทบที่สร้างความอ่อนแอ ต่อความมั่นคงของประเทศ ความมั่นคงทางเศรษฐกิจของประเทศ สุขภาพหรือความ ปลอดภัยของสาธารณะ

- สำหรับ "ประกาศรัฐมนตรีว่าด้วยกิจการที่เป็นโครงสร้างพื้นฐานที่สำคัญอย่างยิ่งยวดของประเทศ" อาจประกอบด้วยโครงข่ายการสื่อสาร, ระบบคมนาคม, พลังงาน, บริการทางการเงิน, อาคารของรัฐบาล, การสาธารณสุข, นิวเคลียร์, ระบบจัดการน้ำ (ดู [17])

3. ตัดมาตรา 14 (3) และ 14 (4): ซ้ำซ้อนกับมาตราอื่นหรือกฎหมายอื่น

- มาตรา 14 (3) และ (4) ระบุว่า

  ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ [...]

  (3) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

  (4) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

- ความผิดตามมาตรา 14 (3) นั้น ครอบคลุมอยู่แล้วโดยมาตรา 14 (2) (ตามที่เสนอแก้ไขในข้อ 2)
- ความผิดตามมาตรา 14 (4) นั้น ครอบคลุมอยู่แล้วโดยมาตรา 16 ในพ.ร.บ.ฉบับเดียวกันนี้ และโดยประมวลกฎหมายอาญามาตรา 287 ("สิ่งอื่นใดอันลามก" แก้ไขเพิ่มเติมโดยพรบ.แก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่ 5) พ.ศ. 2525) และมาตรา 287/1 และมาตรา 287/2 ("สื่อลามกอนาจารเด็ก" แก้ไขเพิ่มเติมโดยพ.ร.บ.แก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่ 24) พ.ศ. 2558) โดยมีโทษสูงสุดในกรณีมีสื่อลามกอนาจารเด็กไว้เพื่อการค้าคือจำคุก 10 ปี ซึ่งสูงกว่าในพ.ร.บ.คอมพิวเตอร์ (ดู [24])
- **เสนอให้ตัดมาตรา 14 (3) และมาตรา 14 (4) ออกจากพ.ร.บ.ทั้งหมด เนื่องจากซ้ำซ้อนกับกฎหมายอื่น**

4. มาตรา 15: แยกแยะประเภทผู้ให้บริการหรือสื่อตัวกลาง และกำหนดภาระความรับผิดให้เหมาะสมกับประเภท

- การกำหนดให้ผู้ให้บริการ ซึ่งเป็นสื่อตัวกลาง (intermediary) จะต้องมีความรับผิดด้วยนั้น ควรคำนึงถึงลักษณะที่แตกต่างกันของสื่อตัวกลางแต่ละชนิด
- ในกฎหมายปัจจุบันแม้ในมาตรา 3 จะมีนิยามของ “ผู้ให้บริการ” อยู่ 2 ประเภทใน (1) และ (2) คือ

  “ผู้ให้บริการ” หมายความว่า

  (1) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่นโดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

  (2) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

  แต่ในกฎหมายมาตราที่เหลือทั้งหมด ก็ปฏิบัติกับผู้ให้บริการ 2 ประเภทดังกล่าวเหมือนกัน ไม่มีการแยกแยะ
- โดยทั่วไปสื่อตัวกลาง เมื่อแบ่งอย่างหยาบที่สุด มีอยู่ 2 ประเภท คือ สื่อตัวกลางประเภท “ท่อ” (mere conduit) กับ สื่อตัวกลางประเภท “ที่เก็บ” (host) (ดู [3]) และสำหรับเทคโนโลยีอินเทอร์เน็ตนั้นมีอีกประเภทคือ “ที่พักชั่วคราว” (caching) ซึ่งเป็นการเก็บข้อมูลที่ใช้บ่อยๆ โดยอัตโนมัติเพื่อส่งต่อให้กับผู้ใช้บริการได้รวดเร็วขึ้น
- สื่อตัวกลางประเภท “ท่อ” และ “ที่พักชั่วคราว” นั้นนำส่งข้อมูลอย่างเดียวโดยไม่เห็นหรือยุ่งเกี่ยวกับข้อมูลเลย จึงไม่ควรต้องมีภาระความรับผิดเกี่ยวกับข้อมูล
- ส่วนสื่อตัวกลางประเภท “ที่เก็บ” ในกรณีที่ทราบถึงการมีอยู่ของข้อมูล อาจต้องมีภาระความรับผิดบ้างตามความเหมาะสม (ดูข้อเสนอข้อ 4 ประกอบ)
- ตัวอย่างเช่น Directive 2000/31/EC of the European on Electronic commerce ซึ่งได้กำหนดประเภทสื่อตัวกลางออกเป็น 3 ประเภทคือ “ท่อ” (mere conduit – มาตรา 12), “ที่พักชั่วคราว” (caching – มาตรา 13), และ “ที่เก็บรักษาข้อมูล” (hosting – มาตรา 14) และได้ระบุข้อยกเว้นความผิดเอาไว้สำหรับสื่อตัวกลางแต่ละประเภท (ดู [4] และ [18])
- **เสนอให้กำหนดประเภทสื่อตัวกลาง 3 ประเภทใหญ่นี้ (“ท่อ” “ที่พักชั่วคราว” และ “ที่เก็บ”) ไว้ในพ.ร.บ.หลัก (อาจกำหนดไว้ในส่วนนิยามหรือในส่วนของมาตรา 15 เอง) พร้อมทั้งกำหนดภาระ**

ความรับผิดให้เหมาะสมตามประเภทของสื่อตัวกลางไว้ในตัวพ.ร.บ.หลักเช่นกัน

- **และเสนอให้พิจารณา "หลักการมะนิลาว่าด้วยความรับผิดของสื่อตัวกลาง" ซึ่งเป็นหลักการระหว่างประเทศ ในการกำหนดหน้าที่ ภาระความรับผิด ความผิด และโทษที่เกี่ยวกับผู้ให้บริการหรือสื่อตัวกลาง (ดู [5])**

5. มาตรา 15: ความ "ยินยอม" และโทษที่เหมาะสมของผู้ให้บริการ

- ร่างปัจจุบันโทษของผู้ให้บริการตามมาตรา 15 นั้น สูงเท่ากับผู้เผยแพร่เนื้อหา โดยระบุว่า

  มาตรา 15 ผู้ให้บริการผู้ใดให้ความร่วมมือ ยินยอม หรือรู้เห็นเป็นใจ ให้มีการกระทำความผิดตามมาตรา 14 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิด ตามมาตรา 14 [...]

- การ "ให้ความร่วมมือ" หรือ "รู้เห็นเป็นใจ" อาจต้องชัดเจนว่าผู้ให้บริการมีเจตนากระทำความผิดร่วมกับผู้ที่โพสต์เนื้อหาผิดกฎหมายเองด้วย แต่คำว่า "ยินยอม" ยังเป็นเรื่องยากที่จะพิสูจน์ว่า กรณีใดผู้ให้บริการพบเห็นข้อความแล้วแต่มีเจตนาที่จะยินยอมให้อยู่ต่อไป หรือกรณีใดที่ผู้ให้บริการไม่ได้ยินยอม แต่ทำหน้าที่โดยประมาทเลินเล่อตรวจสอบไม่พบเนื้อหาผิดกฎหมาย หรือเนื่องจากความผิดพลาดส่วนบุคคลโดยไม่ได้ตั้งใจ (ดูความเห็นใน [2])
- ตามหลักกฎหมายอาญาทั่วไป ผู้สนับสนุนการกระทำผิดจะรับโทษสองในสามของผู้กระทำความผิด
- เมื่อเทียบกับโทษในร่างพ.ร.บ.ฉบับเดียวกันกัน มาตรา 16/2 กำหนดว่า

  มาตรา 16/2 ผู้ใดรู้ว่าข้อมูลอิเล็กทรอนิกส์ในความครอบครองของตนเป็นข้อมูลที่ศาลสั่งให้ยึดและทำลายตามมาตรา 16/1 ผู้นั้นต้องทำลายข้อมูลดังกล่าว หากฝ่าฝืนต้องระวางโทษกึ่งหนึ่งของโทษที่บัญญัติไว้ในมาตรา 16

- **เสนอให้กำหนดลักษณะความผิดของผู้ให้บริการให้ชัดเจน โดยคำนึงถึงความเป็นไปได้ในการพิสูจน์เจตนา แยกแยะภาระของผู้ให้บริการแต่ละประเภท กำหนดความรับผิดและโทษให้เหมาะสมตามหลักกฎหมายอาญา และให้การกำหนดโทษมีความสม่ำเสมอภายในกฎหมายฉบับเดียวกัน**

6. มาตรา 15: เสนอให้ใช้หลักการ “แจ้งเตือนและแจ้งเตือน” (Notice and Notice) สำหรับขั้นตอนการแจ้งเตือน การระงับ และการนำข้อมูลออกจากระบบ

- ควรระมัดระวังในการให้ผู้ให้บริการต้องทำหน้าที่เหมือนศาลในการพิจารณาว่าเนื้อหาใดอาจผิดกฎหมาย โดยเฉพาะเนื้อหาประเภทที่อาจไม่สามารถพิจารณาได้อย่างตรงไปตรงมานัก
- หลักการ “แจ้งเตือนและนำออก” (Notice and Takedown) อย่างที่สหรัฐใช้นั้น เป็นหลักการสำหรับเนื้อหาลิขสิทธิ์ ออกแบบมาในสมัยที่ผู้ให้บริการกับผู้เผยแพร่ข้อมูล เป็นคนเดียวกัน การแจ้งเตือน (notice) จึงเป็นการแจ้งไปที่ผู้ให้บริการ (ซึ่งคือผู้เผยแพร่ด้วย)
- แต่ปัจจุบันที่เป็นยุคของเนื้อหาที่ผู้ใช้เป็นผู้สร้าง (user-generated content) หรือที่เรียกว่า “เว็บ 2.0” ผู้ลงมือเผยแพร่เนื้อหาจริงๆ คือผู้ใช้บริการ ไม่ใช้ผู้ให้บริการ เช่น ผู้โพสต์กระทู้ในพันทิป.คอม ไม่ใช่ผู้ให้บริการคือตัวพันทิป.คอม แต่เป็นผู้ใช้บริการ
- นอกจากนี้ ที่ผ่านมา การบังคับใช้กฎหมายลิขสิทธิ์ (Digital Millenium Copyright Act) ในสหรัฐอเมริกา ตามหลักการ “แจ้งเตือนและนำออก” นั้นมีปัญหาและถูกใช้ในทางที่ผิดเป็นจำนวนมาก ผู้ให้บริการมักไม่ตรวจสอบคำแจ้งเตือนให้นำเนื้อหาออกว่าสมเหตุผลหรือไม่ (ส่วนหนึ่งเนื่องจากคำร้องมีเป็นจำนวนมาก) จนนำไปสู่การนำเนื้อหาของผู้ใช้บริการออกอย่างผิดพลาดบ่อยครั้ง และยังถูกใช้เป็นเครื่องมือเพื่อยับยั้งการแสดงที่ถูกกฎหมาย (ดู [6]) เช่น
    - กรณีของบริษัทไทม์วอร์เนอร์เคเบิลส่งคำแจ้งเตือนให้ลบบัญชีสื่อสังคมของเว็บไซต์ที่วิจารณ์การทำงานของแผนกดูแลลูกค้าของบริษัท จนทำให้บัญชียูทูบและทวิตเตอร์หลายบัญชีของเว็บไซต์ดังกล่าวถูกลบ (ดู [7])
    - กูเกิลระบุในบันทึกว่ามากกว่าครึ่ง (57%) ของการแจ้งเตือนตาม DMCA ที่กูเกิลได้รับนั้น (ข้อมูลปี 2009) มาจากบริษัทคู่แข่งแจ้งเตือนให้นำเนื้อหาของอีกบริษัทออก ในขณะที่มากกว่า 1 ใน 3 (37%) ของการแจ้งเตือนนั้นไม่เกี่ยวกับการละเมิดลิขสิทธิ์ (ดู [20])
- **หลักการ “แจ้งเตือนและแจ้งเตือน” (Notice and Notice)** ดังเช่นที่กฎหมายลิขสิทธิ์ของแคนาดาใช้ จึงได้ปรับปรุงกฎหมายให้สอดคล้องกับการส่งเสริมเศรษฐกิจยุคดิจิทัล โดยเน้นกระบวนการให้สามารถส่งการแจ้งเตือนนั้นไปถึงผู้เผยแพร่ที่เป็นตัวการที่แท้จริง และให้ผู้เผยแพร่ตัวจริงมาอยู่ร่วมในกระบวนการนำเนื้อหาออกด้วย สอดคล้องกับลักษณะการทำงานของอินเทอร์เน็ตและการเผยแพร่ข้อมูลบนเว็บในปัจจุบัน (ดู [8] และ [9])

- **เสนอให้ใช้หลักการในลักษณะเดียวกับหลักการ “แจ้งเตือนและแจ้งเตือน” เพื่อให้ผู้ให้บริการส่งการแจ้งเตือนต่อไปยังผู้ใช้บริการและเป็นเหตุให้ยกเว้นความผิดได้ โดยเขียนหลักการนี้ลงในพ.ร.บ.ฉบับหลักอย่างชัดเจน ส่วนรายละเอียดขั้นตอนวิธีปฏิบัติ สามารถกำหนดในประกาศรัฐมนตรีได้**

7. มาตรา 15: ภาระในการพิสูจน์ความบริสุทธิ์ ขัดหลักกฎหมายอาญาและอาจขัดรัฐธรรมนูญ

- ร่างมาตรา 15 วรรคสาม ระบุว่า

  > *ถ้าผู้ให้บริการพิสูจน์ได้ว่าตนได้ปฏิบัติตามประกาศของรัฐมนตรีที่ออกตามวรรคสอง ผู้นั้นไม่ต้องรับโทษ*

  อาจทำให้ภาระการพิสูจน์ มาตกอยู่ที่ผู้ถูกกล่าวหา ซึ่งตรงข้ามกับหลักกฎหมายอาญาทั่วไปที่กำหนดให้ภาระแห่งการพิสูจน์นั้นอยู่ที่ผู้กล่าวหา

- ศาลรัฐธรรมนูญได้มีคำวินิจฉัยที่ 3/2559 ลงวันที่ 1 มิถุนายน 2559 ว่า พระราชบัญญัติว่าด้วยความผิดเกี่ยวกับการเสนอราคาต่อหน่วยงานของรัฐ พ.ศ. 2559 มาตรา 9 ซึ่งบัญญัติว่า *“ในกรณีที่การกระทำความผิดตามพระราชบัญญัตินี้เป็นไปเพื่อประโยชน์ของนิติบุคคลใด ให้ถือว่าหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหารหรือผู้มีอำนาจในการดำเนินงานในกิจการของ นิติบุคคลนั้น หรือผู้ซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลในเรื่องนั้น เป็นตัวการร่วมในการกระทำ ความผิดด้วย เว้นแต่จะพิสูจน์ได้ว่าตนมิได้มีส่วนรู้เห็นในการกระทำความผิดนั้น”* เป็นบทบัญญัติที่ขัด หรือแย้งต่อรัฐธรรมนูญแห่งราชอาณาจักรไทย (ฉบับชั่วคราว) พุทธศักราช 2559 มาตรา 4 (ดู [10])

- **เสนอให้พิจารณาเรื่องภาระแห่งการพิสูจน์ความผิดให้รอบคอบตามหลักกฎหมายอาญาและหลักการในรัฐธรรมนูญ**

8. มาตรา 15 และ 20: ต้องจำกัดขอบเขตอำนาจและผลกระทบของประกาศที่รัฐมนตรีจะออกเพิ่มเติมได้ตามพ.ร.บ.

- มาตรา 15 วรรคสอง และมาตรา 20 วรรคห้า ของร่างที่แก้ไขใหม่ กำหนดให้รัฐมนตรีสามารถออกประกาศกำหนดหลักเกณฑ์ ระยะเวลา และแนวทางการปฏิบัติสำหรับการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ของผู้ให้บริการได้ (มาตรา 20 กล่าวถึงการระงับ มาตรา 15 กล่าวถึงความ

ผิดของผู้ให้บริการและเหตุยกเว้นโทษ)

- **เสนอให้พิจารณากำหนดขอบเขตของประกาศที่รัฐมนตรีจะออกเพิ่มเติมได้ ดังนี้**

  1. **ร่างกฎหมายควรวางกรอบหลักการและเกณฑ์ขั้นต่ำ ว่าประกาศที่รัฐมนตรีจะออกได้นั้นจะต้องอยู่ภายใต้หลักการที่กำหนด** เช่น ระบุว่าให้ใช้หลักการ “แจ้งเตือนและแจ้งเตือน” สำหรับการแจ้งเตือนข้อมูลที่อาจผิดกฎหมาย หน่วยงานที่มีอำนาจยื่นคำร้องคือใคร สื่อตัวกลางประเภทใดและชนิดใดบ้างที่จำเป็นต้องปฏิบัติตามคำร้อง ข้อมูลที่ต้องระบุในคำร้องอย่างน้อยขั้นต่ำจะต้องมีอะไรบ้าง (เช่น คำแจ้งเตือนให้ระงับหรือลบข้อมูล ต้องระบุข้อกฎหมายที่ข้อมูลนั้นละเมิดด้วย – ดูข้อ 2 และ 3 ของ “หลักการมะนิลาว่าด้วยความรับผิดการสื่อตัวกลาง” [5]) สิทธิของผู้เผยแพร่ข้อมูลในการอุทธรณ์ และการแจ้งเตือนนั้นจำเป็นจะต้องขออนุญาตจากใครก่อน ส่วนขั้นตอนปฏิบัติโดยละเอียดนั้น รัฐมนตรีสามารถออกเป็นประกาศเพิ่มเติมได้ -- ซึ่งจะทำให้กฎหมายยังยืดหยุ่นสามารถเปลี่ยนแปลงตามสถานการณ์ได้ ในขณะเดียวกันหลักการใหญ่ก็ยังคงเสถียรอยู่ ผู้บังคับใช้และถูกบังคับใช้กฎหมายสามารถทำงานได้สะดวก
  2. **สำหรับเรื่องที่แน่ชัดว่าจะไม่กระทบสิทธิเสรีภาพของประชาชนเป็นการทั่วไป เป็นเพียงแต่การลงรายละเอียดในการปฏิบัติงาน รัฐมนตรีสามารถออกประกาศได้ด้วยตัวเอง**
  3. **สำหรับเรื่องที่เป็นไปได้ว่าอาจกระทบสิทธิเสรีภาพของประชาชนทั่วไป หรือมีแนวโน้มจะขยายขอบเขตอำนาจของกฎหมายหรือความเป็นไปได้ในการบังคับใช้เกินไปกว่ากฎหมายหลักที่สภาเป็นผู้ออก ต้องให้ออกเป็นกฎหมายระดับพ.ร.บ. เพื่อให้สภาได้พิจารณา รัฐมนตรีไม่สามารถออกประกาศได้ด้วยตัวเอง** เช่น มาตราของกฎหมายหลักพูดถึงการระงับการเข้าถึงข้อมูล จะออกประกาศหรือกฎหมายลำดับรองที่อาจทำให้เกิดการละเมิดสิทธิในความเป็นอยู่ส่วนตัวของบุคคลโดยทั่วไป ไม่ได้ (ดู [11] (ข้อ 11) [12] [13] [14] [22] และเหตุผลในการแก้ไขมาตรา 20 ในตารางเปรียบเทียบการแก้ไขแนบท้ายร่างพ.ร.บ.ที่ส่งให้กับสภานิติบัญญัติแห่งชาติเมื่อวันที่ 26 เม.ย. 2559 ที่กล่าวถึงข้อมูลที่ถูกเข้ารหัส SSL และ public-key encryption ดู [23])

- **นอกจากนี้ ยังเสนอให้ พิจารณาเขียนให้มาตรา 15 วรรคสอง มีความรัดกุมมากขึ้น เพื่อให้ในทางปฏิบัติ ไม่เกิดกรณี มีผู้ใช้การแจ้งเตือนตามประกาศรัฐมนตรีในวรรคสอง แทนการใช้คำสั่งศาลตามมาตรา 20 (ดู [26])**

9. ตัดมาตรา 20 (4) ที่อนุญาตให้ปิดกั้นข้อมูลได้แม้ไม่ผิดกฎหมายใด

- มาตรา 20 (4) ของร่างที่แก้ไขใหม่ เรื่องการปิดกั้นเว็บไซต์ จะส่งผลให้เว็บไซต์ถูก “บล็อค” ได้ แม้ว่า

ข้อมูลบนเว็บไซต์ดังกล่าวจะไม่ผิดกฎหมายใดๆ เลยก็ตาม หากคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์เห็นว่าเนื้อหาเหล่านั้น “ขัดต่อความสงบเรียบร้อยและศีลธรรมอันดี” ทั้งนี้คณะกรรมการกลั่นกรองฯ ทั้ง 5 คนมาจากการแต่งตั้งของรัฐมนตรีว่าการกระทรวงดิจิทัลฯ และร่างกฎหมายไม่ได้กำหนดคุณสมบัติที่ชัดเจนของกรรมการ

- หากพิจารณาว่าการระงับหรือลบข้อมูลหรือการปิดกั้นเว็บไซต์คือการลงโทษ (เนื่องจากเป็นการจำกัดสิทธิของผู้ถูกปิดกั้น และอาจกระทบต่อการดำเนินธุรกิจ การใช้ชีวิตโดยปกติของผู้เกี่ยวข้อง) มาตรา 20 (4) นี้น่าจะขัดกับหลักกฎหมายอาญาที่ว่า ไม่มีกฎหมาย ไม่มีความผิด ไม่มีโทษ นอกจากนี้มาตรา 20 (4) จะส่งผลกระทบกับการทำงานของสื่อมวลชน การสื่อสารของประชาชน และการทำงานโดยทั่วไปของอินเทอร์เน็ต เนื่องจากไม่มีความชัดเจนตามกฎหมายว่าข้อมูลแบบใดกันแน่ที่อาจเข้าข่าย
- **เสนอให้ตัดมาตรา 20 (4) นี้ออกจากร่างทั้งหมด (ดู [15])**

10. มาตรา 16/1 และ 16/2: คำสั่งให้ลบข้อมูล เจตนา และภาระของทั้งผู้ใช้และผู้ให้บริการที่จะสะสมเพิ่มขึ้นจนไม่ได้สัดส่วน

- ตัวบทของร่างฉบับวันที่ 26 เม.ย. 2559 ในมาตรา 16/2 ระบุว่า

  > *ผู้ใดรู้ว่าข้อมูลอิเล็กทรอนิกส์ในความครอบครองของตนเป็นข้อมูลที่ศาลสั่งให้ยึดและทำลายตามมาตรา 16/1 ผู้นั้นต้องทำลายข้อมูลดังกล่าว หากฝ่าฝืนต้องระวางโทษกึ่งหนึ่งของโทษที่บัญญัติไว้ในมาตรา 16*

  ปัญหาคือ จะทราบได้อย่างไรว่าผู้ใด “รู้” จะมีวิธีใดในการพิสูจน์ และใครจะต้องเป็นผู้พิสูจน์

- **การรู้ว่ามีข้อมูลอยู่ในระบบของตน** – ร่างมาตรา 15 และ 20 และร่างมาตรา 16/1 และ 16/2 นั้นมีกลไกในการให้ผู้ใช้/ผู้ให้บริการได้รู้ถึงการมีอยู่ของข้อมูลในระบบของตนแตกต่างกัน กล่าวคือ
  - ร่างมาตรา 15 และมาตรา 20 มีกลไกตาม “ประกาศขั้นตอนการแจ้งเตือน” และ “แนวทางการปฏิบัติสำหรับการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์” ที่จะออกโดยรัฐมนตรี ที่จะแจ้งไปยังผู้ให้บริการโดยตรง เพื่อให้ผู้ให้บริการได้รู้ถึงการมีอยู่ของข้อมูล โดยในคำแจ้งเตือนหรือคำสั่งศาล ที่ผ่านมาจะต้องระบุถึงที่อยู่หรือตำแหน่งของข้อมูลในระบบ (เช่น URL) ด้วย ซึ่งจะทำให้ผู้บริการทราบถึงตำแหน่งที่แน่นอนของข้อมูลดังกล่าว และระงับการเข้าถึงได้
  - ร่างมาตรา 16/1 และ 16/2 มี 2 ช่องทางที่รู้ได้ว่าระบบของตนมีข้อมูลที่ศาลสั่งให้ยึดและทำลายหรือไม่ คือ

1. รับทราบจากคำพิพากษา ในคดีของตนเองหรือตามที่จำเลยโฆษณาตามที่กำหนดไว้ในมาตรา 16/1 (2)
2. กรณีที่ไม่ได้รับทราบจากโฆษณาหรือระยะเวลาการโฆษณาได้ผ่านไปแล้ว (อาจเป็นคดีที่เกิดขึ้นในอดีต) บุคคลยังอาจสามารถค้นหาคำพิพากษาย้อนหลังได้จากศาล

- จะเห็นว่าทั้ง 2 ช่องทาง ไม่ใช่การแจ้งไปที่ผู้ที่อาจมีข้อมูลโดยตรง และในคำพิพากษาจะระบุเฉพาะว่าเป็นข้อมูลอะไร แต่ไม่ได้ระบุว่าข้อมูลดังกล่าวอยู่ในที่ใดของระบบของผู้ใช้/ผู้ให้บริการ (เนื่องจากไม่สามารถระบุได้ เพราะที่อยู่ของข้อมูลจะแตกต่างกันไป)
- นอกจากนี้ผู้ให้บริการรายใหม่หรือผู้ใช้อินเทอร์เน็ตรายใหม่ จะรู้ได้อย่างไรว่ามีข้อมูลอะไรบ้างที่มีอยู่ในครอบครองแล้วจะเป็นความผิด นอกจากการต้องไปค้นคำพิพากษาย้อนหลังทั้งหมด

- **ภาระของที่จะยิ่งสะสมมากขึ้นเมื่อเวลาผ่านไป** -- ข้อมูลอิเล็กทรอนิกส์ที่ศาลสั่งให้ยึดหรือทำลายตามมาตรา 16/1 จะมีมากขึ้นทุกปี รายการข้อมูลที่จะต้องลบออกจากระบบจะมีมากขึ้นเรื่อยๆ โดยที่ผู้ใช้และโดยเฉพาะผู้ให้บริการอาจไม่สามารถทราบได้ว่าข้อมูลดังกล่าวอยู่ ณ ตำแหน่งใดของระบบ เนื่องจากในคำพิพากษาไม่สามารถระบุได้
- นอกจากนี้ในที่ประชุมคณะกรรมาธิการวิสามัญพิจารณาร่างฯ เมื่อวันที่ 24 มิ.ย. 2559 มีข้อเสนอให้เพิ่มข้อมูลคอมพิวเตอร์ที่เป็นความผิดตามมาตรา 14 ลงไปในร่างมาตรา 16/1 และ 16/2 ด้วย เป็น

  มาตรา 16/1 ในคดีความผิดตามมาตรา 14 และมาตรา 16 ซึ่งมีคำพิพากษาว่าจำเลยมีความผิด ศาลอาจสั่ง [...]

  มาตรา 16/2 ผู้ใดรู้ว่าข้อมูลคอมพิวเตอร์ในความครอบครองของตนเป็นข้อมูลที่ศาลสั่งให้ยึดและทำลายตามมาตรา 16/1 ผู้นั้นต้องทำลายข้อมูลดังกล่าว หากฝ่าฝืนต้องระวางโทษกึ่งหนึ่งของโทษที่บัญญัติไว้ในมาตรา 14 และมาตรา 16 แล้วแต่กรณี

  ซึ่งก็จะยิ่งขยายจำนวนข้อมูลที่ทั้งผู้ใช้และผู้ให้บริการจะต้องรู้ว่ามีในระบบของตน

- **เสนอให้ตัดมาตรา 16 (2) ออกจากร่างพ.ร.บ. และหากต้องการให้ลบข้อมูลดังกล่าว ให้ใช้กลไกที่มีอยู่แล้วตามมาตรา 20 เพื่อแจ้งไปยังผู้ครอบครองแทน ซึ่งการแจ้งดังกล่าวจะระบุตำแหน่งที่ตั้งของข้อมูล ทำให้ผู้ครอบครองลบข้อมูลได้ทันที**
- **เสนอให้ระมัดระวังในการพิจารณาความผิดตามมาตรา 14 (ความเกี่ยวกับคอมพิวเตอร์) และมาตรา 16 (ความผิดเกี่ยวกับเนื้อหา) เนื่องจากเป็นลักษณะความผิดที่แตกต่างกัน ควรจะใช้มาตรการเฉพาะที่เหมาะสมสำหรับแต่ประเภทความผิด**

11. มาตรา 15, 16, 16/1, 16/2, 17, 17/1, 18, 20, 21 และ 26: กระบวนการอุทธรณ์ ความโปร่งใสของการใช้อำนาจ การเยียวยากรณีได้รับผลกระทบ และการเก็บข้อมูลเพื่อให้สามารถทบทวนและปรับปรุงการใช้อำนาจ

- **คำขอต้องระบุเหตุผลชัดเจน** -- การใช้อำนาจตามพ.ร.บ.และประกาศของพ.ร.บ.นี้ เช่น การค้นคอมพิวเตอร์ ขอข้อมูลคอมพิวเตอร์ ระงับการเข้าถึง สั่งให้ลบข้อมูล หรือสั่งให้มีการเก็บข้อมูลการจราจรเพิ่มเติม ต้องมีการทำคำร้องอย่างละเอียดแสดงเหตุผลถึงความจำเป็นว่าไม่สามารถใช้มาตรการอื่นที่กระทบสิทธิน้อยกว่านี้ได้แล้ว และให้ศาลอนุมัติ โดยคำอนุมัติดังกล่าวจะต้องมีอายุ และสามารถต่ออายุได้ตามความจำเป็น -- โดยดูแนวทางของกฎหมายที่มีอยู่แล้ว เช่น มาตรา 25 ของพ.ร.บ.การสอบสวนคดีพิเศษ พ.ศ. 2547 ที่เกี่ยวกับการขออนุมัติจากผู้บังคับบัญชา การขออำนาจศาล การคำนึงถึงผลกระทบต่อสิทธิเสรีภาพ และการต่ออายุคำร้อง เพื่อประกอบการพิจารณา (ดูการเปรียบเทียบเงื่อนไขเงื่อนไขการขอที่ตารางแนบท้าย)
- **คำขอฝ่ายเดียวต้องมีอายุจำกัด** -- คำขอฝ่ายเดียว เช่น คำสั่งระงับการเข้าถึงข้อมูลตามมาตรา 20 ต้องมีอายุจำกัด โดยเมื่อหมดอายุคำสั่งดังกล่าวแล้ว และ 1) ไม่มีการพิสูจน์ว่าข้อมูลคอมพิวเตอร์ดังกล่าวมีความผิด หรือ 2) พิสูจน์แล้วว่าข้อมูลคอมพิวเตอร์ดังกล่าวไม่มีความผิด จะต้องเปิดให้เข้าถึงข้อมูลได้ต่อไปตามปกติ
- **การอุทธรณ์** -- ให้มีกระบวนการอุทธรณ์ และให้มีการเยียวยาผลกระทบกรณีเกิดความเสียหาย
- **การทบทวนการใช้กฎหมาย** -- ให้หน่วยงานรับผิดชอบตามกฎหมายนี้ต้องเผยแพร่ข้อมูลที่เกี่ยวข้องกับการใช้อำนาจตามกฎหมายนี้ อย่างน้อยดังรายการดังต่อไปนี้ เพื่อความโปร่งใสตรวจสอบได้ของการใช้อำนาจ และสามารถนำข้อมูลมาทบทวนปรับปรุงประสิทธิภาพการบังคับใช้กฎหมายได้ (ดูหลักการมะนิลาว่าด้วยความรับผิดของสื่อตัวกลาง [5] และข้อ 9 (ความโปร่งโส) และข้อ 10 (การตรวจสอบโดยสาธารณะ) ของหลักการระหว่างประเทศว่าด้วยการใช้หลักสิทธิมนุษยชนกับการสอดแนมการสื่อสาร [11])
    1. จำนวนคำร้องที่ขอไปยังศาล แยกความผิดรายมาตรา และหน่วยงานที่ยื่นคำร้อง
    2. จำนวนคำร้องที่ศาลมีคำสั่งอนุมติ แยกความผิดรายมาตรา และหน่วยงานที่ยื่นคำร้อง
    3. จำนวนหน้าเว็บที่ได้ยื่นคำร้องเพื่อให้ศาลมีคำสั่งระงับ/ลบ แยกความผิดรายมาตรา และหน่วยงาน

ที่ยื่นคำร้อง

4. จำนวนหน้าเว็บที่ศาลมีคำสั่งระงับ/ลบ แยกความผิดรายมาตรา และหน่วยงานที่ยื่นคำร้อง

12. กำหนดอายุของกฎหมาย (Sunset Provision) เพื่อให้มีการทบทวนกฎหมายตามเทคโนโลยีที่เปลี่ยนแปลงไป

- เนื่องจากเทคโนโลยีอินเทอร์เน็ตและสภาพสังคมดิจิทัลมีการเปลี่ยนอย่างรวดเร็ว จึงควรกำหนดให้กฎหมายนี้หรือบางมาตราของกฎหมายนี้ มีอายุจำกัด เพื่อบังคับให้มีการทบทวนกฎหมายตามเทคโนโลยีและสังคมที่เปลี่ยนแปลงไป ไม่ล้าสมัย หรือบังคับใช้มาตรการที่อาจไม่จำเป็นอีกต่อไปแล้ว ทั้งนี้ให้สอดคล้องกับพ.ร.ฎ.การทบทวนความเหมาะสมของกฎหมาย พ.ศ. 2558 (ดู [16])
- ตัวอย่างเช่น Sunset Provision ในกฎหมายต่อต้านการก่อการร้าย USA PATRIOT Act ของสหรัฐอเมริกาซึ่งออกมาในปี 2001 และมีเงื่อนไขให้บางมาตราหมดอายุในปี 2005 ซึ่งก็ได้รับการทบทวนและต่ออายุออกไปอีกบางส่วน ต่อมาในปี 2011 มาตราสำคัญ 3 เรื่องหลักเกี่ยวกับการค้นและดักรับข้อมูลในกฎหมายดังกล่าวได้รับการต่ออายุออกไปอีก 4 ปีโดย PATRIOT Sunsets Extension Act อย่างไรก็ตามในปี 2015 สภาไม่ต่ออายุให้กับ Patriot Act และประกาศใช้กฎหมายต่อต้านการก่อการร้ายฉบับใหม่แทนในชื่อ USA Freedom Act ซึ่งเป็นการปรับปรุงจากข้อกฎหมายเดิม ปัญหาในทางปฏิบัติ และกรณีละเมิดสิทธิที่พบในช่วง 15 ปีที่ผ่านมา
- **ขอเสนอให้เพิ่มบทบัญญัติที่กำหนดให้พ.ร.บ.นี้และประกาศต่างๆ ที่ออกโดยอาศัยอำนาจตามพ.ร.บ.นี้ มีอายุจำกัด และจำเป็นต้องได้รับการทบทวนต่ออายุเมื่อถึงกำหนดเวลา หรือที่เรียกว่า “ข้อบัญญัติอัสดง” (Sunset Provision) เช่น กำหนดให้ข้อกฎหมายเกี่ยวข้องกับการใช้อำนาจของเจ้าหน้าที่มีอายุ 5 ปี และหากไม่มีการทบทวนเพื่อต่ออายุ ก็ให้ข้อกฎหมายเป็นอันยกเลิกไป เพื่อบังคับให้มีการทบทวนถึงความจำเป็นและเหมาะสม**
- **การทบทวนประสิทธิภาพของการบังคับใช้กฎหมายนั้น สามารถใช้ข้อมูลที่เก็บตามข้อเสนอข้อที่ 11 ในการพิจารณาประกอบ**

เอกสารอ้างอิง

1. ร่างฯ ที่สำนักงานคณะกรรมการกฤษฎีกา ตรวจพิจารณาแล้ว (เรื่องเสร็จที่ 919/2558) https://ictlawcenter.etda.or.th/de_laws/download_file/2_Krisdika_Draft-

de_laws_computer-related-crime-act.pdf

2. ร่างแก้ไขพ.ร.บ.คอมพิวเตอร์ฯ “ตั้งคณะกรรมการปิดเว็บแม้ไม่ผิดกฎหมาย” – iLaw http://ilaw.or.th/node/4092
3. Frequently asked questions on internet intermediary liability – Association for Progressive Communications https://www.apc.org/en/pubs/frequently-asked-questions-internet-intermediary-l
4. Directive 2000/31/EC on Electronic Commerce http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:HTML
5. หลักการมะนิลาว่าด้วยความรับผิดของสื่อตัวกลาง https://www.manilaprinciples.org/th
6. The Failure of the DMCA Notice and Takedown System – Center for the Protection of Intellectual Property http://cpip.gmu.edu/2013/12/05/the-failure-of-the-dmca-notice-and-takedown-system-2/
7. Takedown Hall of Shame – Electronic Frontier Foundation https://www.eff.org/takedowns
8. รู้จักหลักการ “Notice and Notice” สำหรับการกำกับเนื้อหาออนไลน์ https://thainetizen.org/2016/05/notice-and-notice-content-regulation/
9. Canada’s Approach to Intermediary Liability for Copyright Infringement: the Notice and Notice Procedure – Berkeley Technology Law Journal http://btlj.org/2014/03/canadas-approach-to-intermediary-liability-for-copyright-infringement-the-notice-and-notice-procedure/ และ Notice and Notice Regime – Innovation, Science and Economic Development Canada: “With the coming into force of the Notice and Notice regime – the final step in implementing the Copyright Modernization Act – Canadians now have balanced, modern copyright laws that will help support innovation and drive investment in the economy.” https://www.ic.gc.ca/eic/site/oca-bc.nsf/eng/ca02920.html
10. ประกาศสำนักงานศาลรัฐธรรมนูญ เรื่อง ศาลรัฐธรรมนูญมีคำวินิจฉัยว่าบทบัญญัติแห่งกฎหมายขัดหรือแย้งต่อรัฐธรรมนูญ 2 มิ.ย. 2559 http://www.ratchakitcha.soc.go.th/DATA/PDF/2559/A/050/8.PDF

11. หลักการระหว่างประเทศว่าด้วยการใช้หลักสิทธิมนุษยชนกับการสอดแนมการสื่อสาร ฉบับแปลภาษาไทย https://thainetizen.org/docs/13-principles/ (แปลจากฉบับวันที่ 10 ก.ค. 2556) ต้นฉบับภาษาอังกฤษ (ฉบับล่าสุด พ.ค. 2557) https://necessaryandproportionate.org

12. ผลกระทบของการสอดแนมการสื่อสารโดยรัฐต่อการใช้สิทธิมนุษยชนเพื่อเข้าถึงความเป็นส่วนตัวและเสรีภาพด้านความเห็นและการแสดงออก - รายงานของผู้รายงานพิเศษว่าด้วยการส่งเสริมและคุ้มครองสิทธิและเสรีภาพด้านความเห็นและการแสดงออก แฟรงค์ ลารัว (A/HRC/23/40) (17 เม.ย. 2557) https://thainetizen.org/docs/a-hrc-23-40-surveillance-of-communications/

13. Report of the Special Rapporteur to the Human Rights Council on the use of encryption and anonymity to exercise the rights to freedom of opinion and expression in the digital age (A/HRC/29/32) http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Annual.aspx

14. สิทธิความเป็นส่วนตัวในยุคดิจิทัล – รายงานของสำนักงานข้าหลวงใหญ่ด้านสิทธิมนุษยชนแห่งสหประชาชาติ (A/HRC/27/37) (30 มิ.ย. 2557) https://thainetizen.org/docs/un-right-to-privacy-in-digital-age/

15. แนวโน้มสำคัญและความท้าทายที่จะมีสิทธิของบุคคลทุกคนที่จะค้นหา ได้รับ และรับรู้ข้อมูลและความคิดทุกชนิดผ่านอินเทอร์เน็ต - รายงานของผู้รายงานพิเศษว่าด้วยการส่งเสริมและคุ้มครองสิทธิและเสรีภาพด้านความเห็นและการแสดงออก แฟรงค์ ลารัว (A/HRC/17/27) (16 พ.ค. 2554) https://thainetizen.org/docs/a-hrc-17-27-right-to-internet/

16. พ.ร.ฎ.การทบทวนความเหมาะสมของกฎหมาย พ.ศ. 2558 http://www.ratchakitcha.soc.go.th/DATA/PDF/2558/A/086/91.PDF

17. Presidential Policy Directive -- Critical Infrastructure Security and Resilience (PPD-21) https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

18. ภาระรับผิดทางกฎหมายของตัวกลาง: ปกป้องพื้นที่อินเทอร์เน็ตเพื่อส่งเสริมการแสดงออกและสร้างสรรค์นวัตกรรม - Center for Democracy & Technology https://thainetizen.org/docs/cdt-intermediary-liability/

19. กองทัพเรือ vs สำนักข่าวภูเก็ตหวาน – ศูนย์ข้อมูลกฎหมายและคดีเสรีภาพ http://freedom.ilaw.or.th/case/554

20. Google submission hammers section 92A – PC World
http://www.pcworld.co.nz/article/483729/google_submission_hammers_section_92a/

21. Convention on Cybercrime ของ Council of Europe กำหนดความผิดเอาไว้ในลักษณะคล้ายกับพ.ร.บ.คอมพิวเตอร์ของไทย คือมี 1) ความผิดที่กระทำต่อระบบหรือข้อมูลคอมพิวเตอร์โดยตรง (Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems ตรงกับความผิดตามมาตรา 5 ถึงมาตรา 13 ของพ.ร.บ.คอมพิวเตอร์) 2) ความผิดที่เป็นการใช้ระบบคอมพิวเตอร์ไปเพื่อกระทำความผิดที่เป็นความผิดตามกฎหมายอื่นอยู่แล้ว (Title 2 – Computer-related offences ตรงกับความผิดตามมาตรา 14) และ 3) ความผิดเกี่ยวกับตัวเนื้อหา (Title 3 – Content-related offences ตรงกับความผิดตามมาตรา 16) อย่างไรก็ตามในการบังคับใช้จริงพ.ร.บ.คอมพิวเตอร์มาตรา 14 มักถูกใช้ในความผิดเกี่ยวกับเนื้อหาด้วย – สิ่งหนึ่งที่ทำให้สังเกตได้ว่า ความผิดตามมาตรา 14 (computer-related offence) และมาตรา 16 (content-related offence) นั้นมีลักษณะต่างกันคือมาตรา 14 นั้นไม่มีบทยกเว้นความผิดในกรณี “นำเข้าข้อมูลสู่ระบบคอมพิวเตอร์โดยสุจริต อันเป็นการติชมด้วยความเป็นธรรม” ดังที่มาตรา 16 มี
http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

22. “Single Gateway” คืนชีพ ก.ไอซีทีเสนอในพ.ร.บ.คอมพ์ ให้มีวิธีระงับข้อมูลที่เข้ารหัส SSL – เครือข่ายพลเมืองเน็ต https://thainetizen.org/2016/05/single-gateway-back-ssl-censorship/

23. ร่างพ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ..) พ.ศ. .... ที่เสนอ สนช. วาระหนึ่ง https://ictlawcenter.etda.or.th/de_laws/detail/de-laws-computer-related-crime-act (ดูส่วนที่ 2 หน้า 28-30)

24. 'ครอบครอง' สื่อลามกอนาจารเด็กผิดกฎหมาย 'ค้า-ผลิต-เผยแพร่' จำคุกสูงสุด 10 ปี - iLaw
http://ilaw.or.th/node/3849

25. การฟ้องหมิ่นประมาทกับพ.ร.บ.คอมพิวเตอร์ พ.ศ. 2550 – จอมพล พิทักษ์สันตโยธิน
https://thainetizen.org/2016/06/defamation-computer-crime-act/

26. หวั่น ร่างพ.ร.บ.คอมฉบับใหม่ เปิดช่องให้เลี่ยงมาตรา 20 สั่งปิดเว็บไซต์ -- เครือข่ายพลเมืองเน็ต
https://thainetizen.org/2015/10/digital-economy-laws-update-sawatree/

ดูตารางเปรียบเทียบพ.ร.บ.ปัจจุบันและร่างใหม่ ในภาษาไทยและภาษาอังกฤษ ได้ที่
https://thainetizen.org/docs/cybercrime-amendment-20160426-th-en/

เปรียบเทียบเงื่อนไขการขออำนาจและการทบทวนการใช้อำนาจ ในกฎหมายการเข้าถึงข้อมูลของผู้ต้องสงสัย

	ร่างพ.ร.บ.คอม (เฉพาะ ม.18, 19) (ยังมีมาตราอื่นอีก)	พ.ร.บ.การสอบสวนคดีพิเศษ (ม.25)	ร่างแก้ไขป.วิ.อาญา (ม.131/2)
ผู้ยื่นคำร้อง	พนักงานเจ้าหน้าที่ตามพ.ร.บ.	พนักงานสอบสวนคดีพิเศษซึ่งได้รับอนุมัติจากอธิบดี	พนักงานสอบสวนโดยอนุมัติของผู้บังคับการ ซึ่งเป็นหัวหน้าของพนักงานสอบสวนผู้รับผิดชอบ
ผู้อนุมัติให้ยื่นคำร้อง	(ไม่ต้องมี)	อธิบดีกรมสอบสวนคดีพิเศษ	ผู้บังคับการ ซึ่งเป็นหัวหน้าของพนักงานสอบสวนผู้รับผิดชอบ
ผู้พิจาณาอนุญาตคำร้อง	ศาลที่มีเขตอำนาจ	อธิบดีผู้พิพากษาศาลอาญา	อธิบดีผู้พิพากษาหรือผู้พิพากษาหัวหน้าศาล
สิ่งที่ผู้ยื่นต้องระบุในคำร้อง	• เหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำการอย่างหนึ่งอย่างใดอันเป็นความผิดตามพ.ร.บ.นี้ • เหตุที่ต้องใช้อำนาจ • ลักษณะของการกระทำความผิด • รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิด • (เท่าที่สามารถจะระบุได้)	(ไม่ได้ระบุในคำร้อง แต่ระบุอยู่ในสิ่งที่ศาลจะต้องพิจารณา)	• เหตุผลและความเป็นจำเป็นในการยื่นคำร้อง • รายละเอียดเกี่ยวกับประเภทและลักษณะของข้อมูลที่ต้องการ • วิธีการที่ใช้ในการเข้าถึงและได้มาซึ่งข้อมูลที่จะมีผลกระทบต่อสิทธิส่วนบุคคลน้อยที่สุด • ระยะเวลาที่จำเป็นต้องใช้ในการดำเนินการ
สิ่งที่ต้องพิจารณาเพื่ออนุญาต	• ไม่ได้ระบุชัดเจน แต่มีเขียนเงื่อนไขในมาตรา 19 วรรคสี่ว่า “การทำสำเนาข้อมูลคอมพิวเตอร์ตามมาตรา 18 (4) ให้กระทำได้เฉพาะเมื่อมีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ และต้องไม่เป็น	• ผลกระทบต่อสิทธิส่วนบุคคลหรือสิทธิอื่นใดประกอบกับเหตุผลและความจำเป็นดังต่อไปนี้ • (1) มีเหตุอันควรเชื่อว่ามีการกระทำความผิดหรือจะมีการกระทำความผิดที่เป็นคดีพิเศษ	• คำร้องดังกล่าวมีพยานหลักฐานตามสมควรอันน่าเชื่อว่า จะทำให้ได้มาซึ่งข้อมูลอันเป็นประโยชน์ในการป้องกันและปราบปรามการกระทำความผิดนั้น

	ร่างพ.ร.บ.คอม (เฉพาะ ม.18, 19) (ยังมีมาตราอื่นอีก)	พ.ร.บ.การสอบสวนคดีพิเศษ (ม.25)	ร่างแก้ไขป.วิ.อาญา (ม.131/2)
	อุปสรรคในการดำเนินกิจการของเจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นเกินความจำเป็น”	• (2) มีเหตุอันควรเชื่อว่าจะได้ข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดที่เป็นคดีพิเศษจากการเข้าถึงข้อมูลข่าวสารดังกล่าว • (3) ไม่อาจใช้วิธีการอื่นใดที่เหมาะสมหรือมีประสิทธิภาพมากกว่าได้	• ไม่สามารถรวบรวมพยานหลักฐานได้โดยวิธีการตามปกติเพราะอาจก่อให้เกิดอันตรายอย่างยิ่งต่อเจ้าหน้าที่ของรัฐ • คำนึงถึงผลกระทบของการเข้าถึงและได้มาซึ่งข้อมูลนั้นเท่าที่จำเป็น
ระยะเวลาและเงื่อนไขการอนุญาต	• อนุญาตครั้งเดียว • ไม่มีจำกัดเวลา	• คราวละไม่เกิน 90 วัน • โดยกำหนดเงื่อนไขใดๆ ก็ได้ • ภายหลังที่มีคำสั่งอนุญาต หากปรากฏข้อเท็จจริงว่าเหตุผลความจำเป็นไม่ได้เป็นไปตามที่ระบุหรือพฤติการณ์เปลี่ยนแปลงไป อธิบดีผู้พิพากษาศาลอาญาอาจเปลี่ยนแปลงคำสั่งอนุญาตได้ตามที่เห็นสมควร	• คราวละไม่เกิน 15 วัน • ไม่เกิน 4 คราว • ในกรณีมีเหตุอันสมควร อาจขยายได้อีก แต่รวมแล้วต้องไม่เกิน 90 วัน • ศาลอาจกำหนดเงื่อนไขใดๆ หรือแก้ไขเปลี่ยนแปลงคำสั่ง เพื่อให้มีการเข้าถึงและได้มาซึ่งข้อมูลเท่าที่จำเป็น • รวมทั้งการกำหนดมาตรการเพื่อบรรเทาผลกระทบต่อสิทธิเสรีภาพของบุคคลจากการเข้าถึงและได้มาซึ่งข้อมูลนั้นได้
การรายงานหลังได้อนุญาต	• ให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าในการดำเนินการตามมาตรา 18 (4) (5) (6) (7) และ (8) ส่งสำเนาบันทึกรายละเอียดการดำเนินการและเหตุผลแห่งการดำเนินการให้ศาลที่มีเขตอำนาจภายใน 48 ชั่วโมงนับแต่เวลาลงมือดำเนินการ เพื่อเป็นหลักฐาน	• เมื่อพนักงานสอบสวนคดีพิเศษได้ดำเนินการตามที่ได้รับอนุญาตแล้ว ให้รายงานการดำเนินการให้อธิบดีผู้พิพากษาศาลอาญาทราบ	• รายงานผลการดำเนินการต่อศาลทุก 15 วัน