

12 ข้อเสนอ แก่ไขร่างพ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับ คอมพิวเตอร์ (ฉบับที่..) พ.ศ. (ร่าง 26 เม.ย. 2559) (28 มิ.ย. 2559)

โดย เครือข่ายพลเมืองเน็ต ปรับปรุงจากการนำเสนอในงานเสวนาวิชาการ “เสรีภาพออนไลน์ภายใต้กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์” 27 มิถุนายน 2559 จัดโดย สมาคมนักข่าวนักหนังสือพิมพ์แห่งประเทศไทย และสมาคมนักกฎหมายสิทธิมนุษยชน สนับสนุนโดย สมาคมเครือข่ายผู้สื่อข่าวในเอเชียตะวันออกเฉียงใต้ (SEAPA)

<https://thainetizen.org/docs/computer-crime-act-amendments-recommendations-20160628/>

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 ทั้งที่เจตนาจริงของกฎหมายมุ่งที่จะเอาผิดเรื่องฟิชซิง (phishing) หรือการทำเว็บไซต์หรือข้อมูลปลอมเพื่อนำไปหลอกเอาทรัพย์สินหรือข้อมูลส่วนบุคคลจากเหยื่อ
- “เจตนาจริงของกฎหมาย มาตรา 14 แห่งพระราชบัญญัตินี้มีได้มุ่งเจตนาลงโทษผู้กระทำความผิดฐานหมิ่นประมาทด้วยการโฆษณา” – 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....” จะทำให้ชัดเจนกว่าว่าหมายถึงความผิดเฉพาะเรื่องฟิชซิง (ดูเอกสาร [1] และ [2]) ทั้งนี้ควรเปลี่ยนคำว่า “ข้อมูลคอมพิวเตอร์อันเป็นเท็จ” เป็น “ข้อมูลคอมพิวเตอร์ปลอม” ด้วย เพื่อให้ตรงกับความหมายของ “forgery” (ดู [25])
- เสนอให้บทวนภาษาในร่างมาตรา 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: หากยืนยันจะให้อาจใช้เอาผิดกับเนื้อหาลักษณะหมิ่นประมาทได้อยู่ จำเป็นต้อง 1) พิจารณาความเหมาะสมของโทษให้สอดคล้องกับประมวลกฎหมายอาญา 2) ให้มีบทกเว้นความผิดในแบบที่มาตรา 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 หรืออาจถูกนำไปใช้ในทางที่มีขอบ (ดู [2])
- หากต้องการคุ้มครองระบบคอมพิวเตอร์ที่มีความสำคัญต่อชีวิตและความมั่นคง เช่น ระบบโครงสร้างพื้นฐานของประเทศ ระบบป้องกันประเทศ สามารถระบุให้ชัดได้ โดยอาจใช้แนวทางของสหรัฐอเมริกา และสหภาพยุโรป เกี่ยวกับโครงสร้างพื้นฐานที่สำคัญอย่างยิ่งยวด (critical infrastructure)
- เสนอให้กำหนดความผิดให้ชัดเจนว่าเป็นการทำต่อระบบคอมพิวเตอร์ ในประการที่น่าจะก่อให้เกิดความเสียหายต่อความมั่นคงของชาติและความปลอดภัยสาธารณะ โดยอาจกำหนดให้หมายถึงการโพสต์ข้อมูลคอมพิวเตอร์เท็จที่กระทบต่อ “โครงสร้างพื้นฐานที่สำคัญอย่างยิ่งยวด” เช่นแก้ไขร่างมาตรา 14 (2) เป็น

มาตรา 14 (2) นำเข้าสู่ระบบคอมพิวเตอร์ในกิจการตามประกาศของรัฐมนตรีว่าด้วยกิจการที่เป็นโครงสร้างพื้นฐานที่สำคัญอย่างยิ่งยวดของประเทศ ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จโดยประการที่น่าจะเกิดความเสียหายต่อโครงสร้างพื้นฐานที่สำคัญอย่างยิ่งยวดของประเทศ

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

“โครงสร้างพื้นฐานที่สำคัญอย่างยิ่งยวดของประเทศ” หมายความว่า ระบบและทรัพย์สิน ทั้งทางกายภาพและทางคอมพิวเตอร์ ที่สำคัญอย่างยิ่งต่อประเทศ จนการทำลายหรือทำให้ไร้ ความ

สามารถของระบบหรือทรัพย์สินดังกล่าว อาจทำให้เกิดผลกระทบที่สร้างความอ่อนแอ ต่อความมั่นคงของประเทศ ความมั่นคงทางเศรษฐกิจของประเทศ สุขภาพหรือความปลอดภัยของสาธารณชน

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

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

- 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

4. มาตรา 15: แยกแยะประเภทผู้ให้บริการหรือสื่อตัวกลาง และกำหนด ภาระความรับผิดชอบให้เหมาะสมกับประเภท

- การกำหนดให้ผู้ให้บริการ ซึ่งเป็นสื่อตัวกลาง (intermediary) จะต้องมี ความรับผิดชอบด้วยนั้น 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]) และสำหรับเทคโนโลยีอินเทอร์เน็ต นั้นมีอีกประเภทคือ “ที่พักชั่วคราว” (caching) ซึ่งเป็นการเก็บข้อมูลที่ใช้อย่างน้อย โดยอัตโนมัติเพื่อส่งต่อไปให้ผู้ให้บริการได้รวดเร็วขึ้น
- สื่อตัวกลางประเภท “ท่อ” และ “ที่พักชั่วคราว” นั้นนำส่งข้อมูลอย่างเดียวยังไม่เห็นหรือยุ่งเกี่ยวกับข้อมูลเลย จึงไม่ควรมีภาระความรับผิดชอบเกี่ยวกับข้อมูล
- ส่วนสื่อตัวกลางประเภท “ที่เก็บ” ในกรณีที่ทราบถึงการมีอยู่ของข้อมูล อาจต้องมีภาระความรับผิดชอบบ้างตามความเหมาะสม (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 ประเภทใหญ่ (“ท่อ” “ที่พักชั่วคราว” และ “ที่เก็บ”) ไว้ในพ.ร.บ.หลัก (อาจกำหนดไว้ในส่วนนิยามหรือในส่วนของมาตรา 15 เอง) พร้อมทั้งกำหนดภาระ

ความรับผิดชอบให้เหมาะสมตามประเภทของสื่อตัวกลางไว้ในตัวพ.ร.บ.หลักเช่นกัน

- และเสนอให้พิจารณา “หลักการมะนิลาว่าด้วยความรับผิดชอบของสื่อตัวกลาง” ซึ่งเป็นหลักการระหว่างประเทศ ในการกำหนดหน้าที่ ภาระความรับผิดชอบ 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 หรือกรณีใดที่ผู้ให้บริการไม่ได้ยินยอมแต่ทำหน้าที่โดยประมาทเลินเล่อตรวจสอบไม่พบเนื้อหาผิดกฎหมาย หรือเนื่องจากความผิดพลาดส่วนบุคคลโดยไม่ได้ตั้งใจ (ดูความเห็นใน [2])

- ตามหลักกฎหมายอาญาทั่วไป ผู้สนับสนุนการกระทำความผิดจะรับโทษสองในสามของผู้กระทำความผิด

- เมื่อเทียบกับโทษในร่างพ.ร.บ.ฉบับเดียวกันนี้ 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) อย่างที่สหรัฐฯใช้นั้น เป็นหลักการสำหรับเนื้อหาลิขสิทธิ์ ออกแบบมาในสมัยที่ผู้ให้บริการกับผู้เผยแพร่ข้อมูล เป็นคนเดียวกัน การแจ้งเตือน (notice) จึงเป็นการแจ้งไปที่ผู้ให้บริการ (ซึ่งคือผู้เผยแพร่ด้วย)
- แต่ปัจจุบันที่เป็นยุคของเนื้อหาที่ผู้ใช้เป็นผู้สร้าง (user-generated content) ผู้ลงมือเผยแพร่เนื้อหาจริงๆ คือผู้ใช้บริการ ไม่ใช่ผู้ให้บริการ เช่น ผู้โพสต์กระทู้ในพันทิป.คอม ไม่ใช่ผู้ให้บริการคือตัวพันทิป.คอม แต่เป็นผู้ใช้บริการ
- นอกจากนี้ ที่ผ่านมา การบังคับใช้กฎหมายลิขสิทธิ์ (Digital Millenium Copyright Act) ในสหรัฐฯอเมริกา ตามหลักการ “แจ้งเตือนและนำออก” นั้นมีปัญหาและถูกใช้ในทางที่ผิดเป็นจำนวนมาก ผู้ให้บริการมักไม่ตรวจสอบคำแจ้งเตือนให้นำเนื้อหาออกว่าสมเหตุสมผลหรือไม่ (ส่วนหนึ่งเนื่องจากคำร้องมีเป็นจำนวนมาก) จนนำไปสู่การนำเนื้อหาของผู้ใช้บริการออกอย่างผิดพลาดบ่อยครั้ง และยังคงถูกใช้เป็นเครื่องมือเพื่อยับยั้งการแสดงที่ถูกลงกฎหมาย (ดู [6]) เช่น
 - กรณีของบริษัทไทม์วอร์เนอร์เคเบิลส่งคำแจ้งเตือนให้ลบบัญชีสื่อสังคมของเว็บไซต์ที่วิจารณ์การทำงานของแผนกดูแลลูกค้าของบริษัท จนทำให้บัญชียูทูปและทวิตเตอร์หลายบัญชีของเว็บไซต์ดังกล่าวถูกลบ (ดู [7])
 - ภูเกิลระบุในบันทึกว่ามากกว่าครึ่ง (57%) ของการแจ้งเตือนตาม DMCA ที่ภูเกิลได้รับนั้น (ข้อมูลปี 2009) มาจากบริษัทคู่แข่งแจ้งเตือนให้นำเนื้อหาของอีกบริษัทออก ในขณะที่มากกว่า 1 ใน 3 (37%) ของการแจ้งเตือนนั้นไม่เกี่ยวกับการละเมิดลิขสิทธิ์ (ดู [20])
- หลักการ “แจ้งเตือนและแจ้งเตือน” (Notice and Notice) ดังเช่นที่กฎหมายลิขสิทธิ์ของแคนาดาใช้ จึงได้ปรับปรุงกฎหมายให้สอดคล้องกับการส่งเสริมเศรษฐกิจดิจิทัล โดยเน้นกระบวนการให้สามารถส่งการแจ้งเตือนนั้นไปถึงผู้เผยแพร่ที่เป็นตัวการที่แท้จริง และให้ผู้เผยแพร่ตัวจริงมาอยู่ร่วมในกระบวนการนำเนื้อหาออกด้วย (ดู [8] และ [9])

- เสนอให้ใช้หลักการในลักษณะเดียวกับหลักการ “แจ้งเตือนและแจ้งเตือน” เพื่อให้ผู้ให้บริการส่ง การแจ้งเตือนต่อไปยังผู้ใช้บริการและเป็นเหตุให้ยกเว้นความผิดได้ โดยเขียนหลักการนี้ลง ในพ.ร.บ.ฉบับหลักอย่างชัดเจน ส่วนรายละเอียดขั้นตอนวิธีปฏิบัติ สามารถกำหนดในประกาศ รัฐมนตรีได้

7. มาตรา 15: ภาระในการพิสูจน์ความบริสุทธิ์ ชัดหลักกฎหมายอาญา และอาจขัดรัฐธรรมนูญ

- ร่างมาตรา 15 วรรคสาม ระบุว่า
ถ้าผู้ให้บริการพิสูจน์ได้ว่าตนได้ปฏิบัติตามประกาศของรัฐมนตรีที่ออกตามวรรคสอง ผู้นั้นไม่ ต้องรับโทษ
 อาจทำให้ภาระการพิสูจน์ มาตกอยู่ที่ผู้ถูกกล่าวหา ซึ่งตรงข้ามกับหลักกฎหมายอาญาทั่วไปที่กำหนดให้ ภาระแห่งการพิสูจน์นั้นอยู่ที่ผู้กล่าวหา
- ศาลรัฐธรรมนูญได้มีคำวินิจฉัยที่ 3/2559 ลงวันที่ 1 มิถุนายน 2559 ว่า พระราชบัญญัติว่าด้วยความ ผิดเกี่ยวกับการเสนอราคาต่อหน่วยงานของรัฐ พ.ศ. 2559 มาตรา 9 ซึ่งบัญญัติว่า “ในกรณีที่การก ระทำความผิดตามพระราชบัญญัตินี้เป็นไปเพื่อประโยชน์ของนิติบุคคลใด ให้ถือว่าหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหารหรือผู้มีอำนาจในการดำเนินงานในกิจการของ นิติบุคคลนั้น หรือผู้ซึ่งรับ ผิดชอบในการดำเนินงานของนิติบุคคลในเรื่องนั้น เป็นตัวการร่วมในการกระทำ ความผิดด้วย เว้นแต่ จะพิสูจน์ได้ว่าตนมิได้มีส่วนรู้เห็นในการกระทำความผิดนั้น” เป็นบทบัญญัติที่ขัด หรือแย้งต่อ รัฐธรรมนูญแห่งราชอาณาจักรไทย (ฉบับชั่วคราว) พุทธศักราช 2559 มาตรา 4 (ดู [10])
- เสนอให้พิจารณาเรื่องภาระแห่งการพิสูจน์ความผิดให้รอบคอบตามหลักกฎหมายอาญาและหลัก การในรัฐธรรมนูญ

8. มาตรา 15 และ 20: ต้องจำกัดขอบเขตอำนาจและผลกระทบของ ประกาศที่รัฐมนตรีจะออกเพิ่มเติมได้ตามพ.ร.บ.

- มาตรา 15 วรรคสอง และมาตรา 20 วรรคห้า ของร่างที่แก้ไขใหม่ กำหนดให้รัฐมนตรีสามารถออก ประกาศกำหนดหลักเกณฑ์ ระยะเวลา และแนวทางการปฏิบัติสำหรับการระงับการทำให้แพร่หลาย หรือลบข้อมูลคอมพิวเตอร์ของผู้ให้บริการได้ (มาตรา 20 กล่าวถึงการระงับ มาตรา 15 กล่าวถึงความ

ผิดของผู้ให้บริการและเหตุยกเว้นโทษ)

- เสนอให้พิจารณากำหนดขอบเขตของประกาศที่รัฐมนตรีจะออกเพิ่มเติมได้ ดังนี้
 1. ร่างกฎหมายควรวางกรอบหลักการและเกณฑ์ขั้นต่ำ ว่าประกาศที่รัฐมนตรีจะออกได้นั้นจะต้องอยู่ภายใต้หลักการที่กำหนด เช่น ระบุว่าให้ใช้หลักการ “แจ้งเตือนและแจ้งเตือน” สำหรับการแจ้งเตือนข้อมูลที่อาจผิดกฎหมาย หน่วยงานที่มีอำนาจยื่นคำร้องคือใคร สื่อตัวกลางประเภทใด และชนิดใดบ้างที่จำเป็นต้องปฏิบัติตามคำร้อง ข้อมูลที่ต้องระบุในคำร้องอย่างน้อยขั้นต่ำจะต้องมีอะไรบ้าง (เช่น คำแจ้งเตือนให้ระงับหรือลบข้อมูล ต้องระบุข้อมูลกฎหมายที่ข้อมูลนั้นละเมิดด้วย – ดูข้อ 2 และ 3 ของ “หลักการมะนิลาว่าด้วยความรับผิดชอบสื่อตัวกลาง” [5]) และสิทธิของผู้เผยแพร่ข้อมูลในการอุทธรณ์ ส่วนขั้นตอนปฏิบัติโดยละเอียดนั้น รัฐมนตรีสามารถออกเป็นประกาศเพิ่มเติมได้ -- ซึ่งจะช่วยให้กฎหมายยังยืดหยุ่นสามารถเปลี่ยนแปลงตามสถานการณ์ได้ในขณะเดียวกันหลักการใหญ่ก็ยังคงเสถียรอยู่ ผู้บังคับใช้และถูกบังคับใช้กฎหมายสามารถทำงานได้สะดวก
 2. สำหรับเรื่องที่แน่ชัดว่าจะไม่กระทบสิทธิเสรีภาพของประชาชนเป็นการทั่วไป เป็นเพียงแต่การลงรายละเอียดในการปฏิบัติงาน รัฐมนตรีสามารถออกประกาศได้ด้วยตัวเอง
 3. สำหรับเรื่องที่เป็นไปได้ว่าอาจกระทบสิทธิเสรีภาพของประชาชนทั่วไป หรือมีแนวโน้มจะขยายขอบเขตอำนาจของกฎหมายหรือความเป็นไปได้ในการบังคับใช้เกินไปกว่ากฎหมายหลักที่สภาเป็นผู้ออก ต้องให้ออกเป็นกฎหมายระดับพ.ร.บ. เพื่อให้สภาได้พิจารณา รัฐมนตรีไม่สามารถออกประกาศได้ด้วยตัวเอง เช่น มาตราของกฎหมายหลักพูดถึงการระงับการเข้าถึงข้อมูล จะออกประกาศหรือกฎหมายลำดับรองที่อาจทำให้เกิดการละเมิดสิทธิในความเป็นอยู่ส่วนบุคคลโดยทั่วไป 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 เพื่อไม่ให้ใช้ประกาศรัฐมนตรีตามวรรคสอง แทนการใช้คำสั่งศาลตามมาตรา 20 (ดู [26])

9. ตัดมาตรา 20 (4) ที่อนุญาตให้ปิดกั้นข้อมูลได้แม้ไม่ผิดกฎหมายใด

- มาตรา 20 (4) ของร่างที่แก้ไขใหม่ เรื่องการปิดกั้นเว็บไซต์ จะส่งผลให้เว็บไซต์ถูก “บล็อก” ได้ แม้ว่าข้อมูลบนเว็บไซต์ดังกล่าวจะไม่ผิดกฎหมายใดๆ เลยก็ตาม หากคณะกรรมการกถนองข้อมูล

คอมพิวเตอร์เห็นว่าเนื้อหาเหล่านั้น “ขัดต่อความสงบเรียบร้อยและศีลธรรมอันดี” ทั้งนี้คณะกรรมการ
กฤษฎีกาฯ ทั้ง 5 คนมาจากการแต่งตั้งของรัฐมนตรีว่าการกระทรวงดิจิทัลฯ และร่างกฎหมายไม่ได้
กำหนดคุณสมบัติที่ชัดเจนของกรรมการ

- หากพิจารณาว่าการระงับหรือลบข้อมูลหรือการปิดกั้นเว็บไซต์คือ การลงโทษ (เนื่องจากเป็นการจำกัด
สิทธิของผู้ถูกปิดกั้น และอาจกระทบต่อการดำเนินธุรกิจ การใช้ชีวิตโดยปกติของผู้เกี่ยวข้อง) มาตรา
20 (4) นี้ น่าจะขัดกับหลักกฎหมายอาญาที่ว่า ไม่มีกฎหมาย ไม่มีความผิด ไม่มีโทษ นอกจากนี้มาตรา
20 (4) จะส่งผลกระทบต่อการทำงานของสื่อมวลชน การสื่อสารของประชาชน และการทำงานโดย
ทั่วไปของอินเทอร์เน็ต เนื่องจากไม่มีความชัดเจนตามกฎหมายว่าข้อมูลแบบใดกันแน่ที่อาจเข้าข่าย
- เสนอให้ตัดมาตรา 20 (4) นี้ออกจากร่างทั้งหมด (ดู [15])

10. มาตรา 16/1 และ 16/2: คำสั่งให้ลบข้อมูล เจตนา และภาระของทั้ง ผู้ใช้และผู้ให้บริการที่จะสะสมเพิ่มขึ้นจนไม่ได้สัดส่วน

- ตัวบทของร่างฉบับวันที่ 26 เม.ย. 2559 ในมาตรา 16/2 ระบุว่า
*ผู้ใดรู้ว่าข้อมูลอิเล็กทรอนิกส์ในความครอบครองของตนเป็นข้อมูลที่ศาลสั่งให้ยึดและทำลายตาม
มาตรา 16/1 ผู้นั้นต้องทำลายข้อมูลดังกล่าว หากฝ่าฝืนต้องระวางโทษกึ่งหนึ่งของโทษที่บัญญัติไว้
ในมาตรา 16*
ปัญหาคือ จะทราบได้อย่างไรว่าผู้ใด “รู้” จะมีวิธีใดในการพิสูจน์ และใครจะต้องเป็นผู้พิสูจน์
- การรู้ว่ามีข้อมูลอยู่ในระบบของตน – ร่างมาตรา 15 และ 20 และร่างมาตรา 16/1 และ 16/2 นั้นมี
กลไกในการให้ผู้ใช้/ผู้ให้บริการได้รู้ถึงการมีอยู่ของข้อมูลในระบบของตนแตกต่างกัน กล่าวคือ
 - ร่างมาตรา 15 และมาตรา 20 มีกลไกตาม “ประกาศขั้นตอนการแจ้งเตือน” และ “แนวทางการ
ปฏิบัติสำหรับการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์” ที่จะออกโดยรัฐมนตรี ที่
จะแจ้งไปยังผู้ให้บริการโดยตรง เพื่อให้ผู้ให้บริการได้รู้ถึงการมีอยู่ของข้อมูล โดยในคำแจ้งเตือน
หรือคำสั่งศาล ที่ผ่านมาจะต้องระบุถึงที่อยู่หรือตำแหน่งของข้อมูลในระบบ (เช่น URL) ด้วย ซึ่งจะ
ทำให้ผู้บริการทราบถึงตำแหน่งที่แน่นอนของข้อมูลดังกล่าว และระงับการเข้าถึงได้
 - ร่างมาตรา 16/1 และ 16/2 มี 2 ช่องทางที่รู้ได้ว่าระบบของตนมีข้อมูลที่ศาลสั่งให้ยึดและทำลาย
หรือไม่ คือ

1. รับทราบจากคำพิพากษา ในคดีของตนเองหรือตามที่จำเลยโฆษณาตามที่กำหนดไว้ใน

มาตรา 16/1 (2)

2. กรณีที่ไม่ได้รับทราบจากโฆษณาหรือระยะเวลาการโฆษณาได้ผ่านไปแล้ว (อาจเป็นคดีที่เกิดขึ้นในอดีต) บุคคลยังสามารถค้นหาคำพิพากษาย้อนหลังได้จากศาล
 - จะเห็นว่าทั้ง 2 ช่องทาง ไม่ใช่การแจ้งไปที่ผู้ที่มีข้อมูลโดยตรง และในคำพิพากษาจะระบุเฉพาะว่าเป็นข้อมูลอะไร แต่ไม่ได้ระบุว่าข้อมูลดังกล่าวอยู่ในที่ใดของระบบของผู้ใช้/ผู้ให้บริการ (เนื่องจากไม่สามารถระบุได้ เพราะที่อยู่ของข้อมูลจะแตกต่างกันไป)
 - นอกจากนี้ผู้ให้บริการรายใหม่หรือผู้ใช้อินเทอร์เน็ตรายใหม่ จะรู้ได้อย่างไรว่ามีข้อมูลอะไรบ้างที่มีอยู่ในครอบครองแล้วจะเป็นความผิด นอกจากการต้องไปค้นคำพิพากษาย้อนหลังทั้งหมด
- **ภาระของที่จะยิ่งสะสมมากขึ้นเมื่อเวลาผ่านไป** -- ข้อมูลอิเล็กทรอนิกส์ที่ศาลสั่งให้ยึดหรือทำลายตาม มาตรา 16/1 จะมีมากขึ้นทุกปี รายการข้อมูลที่จะต้องลบออกจากระบบจะมีมากขึ้นเรื่อยๆ โดยที่ผู้ใช้ และโดยเฉพาะผู้ให้บริการอาจไม่สามารถทราบได้ว่าข้อมูลดังกล่าวอยู่ ณ ตำแหน่งใดของระบบ เนื่องจากในคำพิพากษาไม่สามารถระบุได้
- นอกจากนี้ในที่ประชุมคณะกรรมการวิสามัญพิจารณาร่างฯ 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
ซึ่งก็จะยิ่งขยายจำนวนข้อมูลที่ทั้งผู้ใช้และผู้ให้บริการจะต้องรู้ว่ามิใช่ในระบบของตน
- เสนอให้ตัดมาตรา 16 (2) ออกจากร่างพ.ร.บ. และหากต้องการให้ลบข้อมูลดังกล่าว ให้ใช้กลไกที่มีอยู่แล้วตามมาตรา 20 เพื่อแจ้งไปยังผู้ครอบครองแทน ซึ่งการแจ้งดังกล่าวจะระบุตำแหน่งที่ตั้งของข้อมูล ทำให้ผู้ครอบครองลบข้อมูลได้ทันที
- เสนอให้ระมัดระวังในการพิจารณาความผิดตามมาตรา 14 (ความเกี่ยวกับคอมพิวเตอร์) และ มาตรา 16 (ความผิดเกี่ยวกับเนื้อหา) เนื่องจากเป็นลักษณะความผิดที่แตกต่างกัน ควรจะใช้มาตรการเฉพาะที่เหมาะสมสำหรับแต่ละประเภทความผิด

11. มาตรา 15, 16, 17, 18, 20 และ 26: กระบวนการอุทธรณ์ การทบทวนการใช้อำนาจ ความโปร่งใสของการใช้อำนาจ และการเยียวยากรณีได้รับผลกระทบ

- คำขอต้องระบุเหตุผลชัดเจน -- เสนอให้การใช้อำนาจตามพ.ร.บ.และประกาศของพ.ร.บ.นี้ เช่น การค้นคอมพิวเตอร์ ขอข้อมูลคอมพิวเตอร์ ระวังการเข้าถึง สั่งให้ลบข้อมูล หรือสั่งให้มีการเก็บข้อมูลการจราจรเพิ่มเติม ต้องมีการทำคำร้องอย่างละเอียดแสดงเหตุผลถึงความจำเป็นว่าไม่สามารถใช้มาตรการอื่นได้แล้ว และให้ศาลอนุมัติ โดยคำอนุมัติดังกล่าวจะต้องมีอายุ และสามารถนำมาใช้ได้ตามความจำเป็น โดยดูแนวทางของกฎหมายที่มีอยู่แล้ว เช่น มาตรา 25 ของพ.ร.บ.การสอบสวนคดีพิเศษ พ.ศ. 2547 ที่เกี่ยวกับการขออนุมัติจากผู้บังคับบัญชา การขออำนาจศาล และการต่ออายุคำร้อง เพื่อประกอบการพิจารณา
- คำขอฝ่ายเดียวต้องมีอายุจำกัด และต้องมีการพิสูจน์ความผิด -- เสนอให้กำหนดในกฎหมายว่า คำสั่งระวังการเข้าถึงข้อมูล ซึ่งเป็นคำขอฝ่ายเดียว เช่นตามมาตรา 20 ต้องมีอายุจำกัด โดยเมื่อหมดอายุคำสั่งดังกล่าวแล้ว และ 1) ไม่มีการพิสูจน์ว่าข้อมูลคอมพิวเตอร์ดังกล่าวมีความผิด หรือ 2) พิสูจน์แล้วว่าข้อมูลคอมพิวเตอร์ดังกล่าวไม่มีความผิด จะต้องเปิดให้เข้าถึงข้อมูลได้ต่อไปตามปกติ
- การอุทธรณ์ -- เสนอให้มีกระบวนการอุทธรณ์จากการใช้อำนาจ ตามมาตราเช่น 15, 18 และ 20 และให้มีการเยียวยาผลกระทบกรณีเกิดความเสียหาย
- การทบทวนการใช้กฎหมาย -- เสนอให้หน่วยงานรับผิดชอบตามกฎหมายนี้เผยแพร่ข้อมูลที่เกี่ยวข้องกับการใช้อำนาจตามกฎหมายนี้ (เช่นตามมาตรา 15, 16/1, 17/1, 18, 20 และ 26) อย่างน้อยดังรายการดังต่อไปนี้ ทั้งนี้เพื่อความโปร่งใสตรวจสอบได้ของการใช้อำนาจ (ดู [5] และ ข้อ 9 และ 10 ของ [11])
 1. จำนวนคำร้องที่ขอไปยังศาล แยกความผิดรายมาตรา และหน่วยงานที่ยื่นคำร้อง
 2. จำนวนคำร้องที่ศาลมีคำสั่งอนุมัติ แยกความผิดรายมาตรา และหน่วยงานที่ยื่นคำร้อง
 3. จำนวนหน้าเว็บที่ได้ยื่นคำร้องเพื่อให้ศาลมีคำสั่งระงับ/ลบ แยกความผิดรายมาตรา และหน่วยงานที่ยื่นคำร้อง
 4. จำนวนหน้าเว็บที่ศาลมีคำสั่งระงับ/ลบ แยกความผิดรายมาตรา และหน่วยงานที่ยื่นคำร้อง

12. กำหนดอายุของกฎหมาย (Sunset Provision) เพื่อให้มีการทบทวนกฎหมายตามเทคโนโลยีที่เปลี่ยนแปลงไป

- เนื่องจากเทคโนโลยีอินเทอร์เน็ตและสภาพสังคมดิจิทัลมีการเปลี่ยนแปลงอย่างรวดเร็ว จึงควรกำหนดให้กฎหมายนี้หรือบางมาตราของกฎหมายนี้ มีอายุจำกัด เพื่อบังคับให้มีการทบทวนกฎหมายตามเทคโนโลยีและสังคมที่เปลี่ยนแปลงไป ไม่ล้าสมัย หรือบังคับใช้มาตรการที่อาจไม่จำเป็นอีกต่อไปแล้ว ทั้งนี้ให้สอดคล้องกับพ.ร.ฎ.การทบทวนความเหมาะสมของกฎหมาย พ.ศ. 2558 (ดู [16])
- ขอเสนอให้เพิ่มบทบัญญัติที่กำหนดให้พ.ร.บ.นี้และประกาศต่างๆ ที่ออกโดยอาศัยอำนาจตามพ.ร.บ.นี้ มีอายุจำกัด และจำเป็นต้องได้รับการทบทวนต่ออายุเมื่อถึงกำหนดเวลา หรือที่เรียกว่า “ข้อบัญญัติอัสดง” (Sunset Provision) เช่น กำหนดให้กฎหมายมีอายุ 5 ปี และหากไม่มีการทบทวนเพื่อต่ออายุ ก็ให้กฎหมายเป็นอันยกเลิกไป
- การทบทวนประสิทธิภาพของการบังคับใช้กฎหมายนั้น สามารถใช้ข้อมูลที่เก็บตามข้อเสนอข้อที่ 11 ในการพิจารณาประกอบ

เอกสารอ้างอิง

1. ร่างฯ ที่สำนักงานคณะกรรมการกฤษฎีกา ตรวจสอบพิจารณาแล้ว (เรื่องเสร็จที่ 919/2558) https://ictlawcenter.etcha.or.th/de_laws/download_file/2_Krisdika_Draft-de_laws_computer-related-crime-act.pdf
2. ร่างแก้ไขพ.ร.บ.คอมพิวเตอร์ฯ “ตั้งคณะกรรมการปิดเว็บแม่ไม่ผิดกฎหมาย” – 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. หลักการมะนิลาว่าด้วยความรับผิดชอบของสื่อตัวกลาง <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. หลักการระหว่างประเทศว่าด้วยการใช้สิทธิมนุษยชนกับการสอดแนมการสื่อสาร ฉบับแปลภาษาไทย <https://thainetizen.org/docs/13-principles/> (แปลจากฉบับวันที่ 10 ก.ค. 2556) ต้นฉบับภาษาอังกฤษ (ฉบับล่าสุด พ.ค. 2557) <https://necessaryandproportionate.org>
12. ผลกระทบของการสอดแนมการสื่อสารโดยรัฐต่อการใช้สิทธิมนุษยชนเพื่อเข้าถึงความเป็นส่วนตัวและเสรีภาพด้านความเห็นและการแสดงออก - รายงานของผู้รายงานพิเศษว่าด้วยการส่งเสริมและคุ้มครองสิทธิและเสรีภาพด้านความเห็นและการแสดงออก แฟรงค์ ลาร์ว (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. สิทธิความเป็นส่วนตัวในยุคริดิเจทัล – 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. ภาระรับผิดชอบทางกฎหมายของตัวกลาง: 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 – สิ่งหนึ่งที่ทำให้

สังเกตได้ว่า 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” คีนซีพ ก.ไอซีทีเสนอในพ.ร.บ.คอมพิวเตอร์ 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.etcha.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 พัทธ์กษัตริย์โยธิน <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/>