



พระราชบัญญัติ
ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒)
พ.ศ. ๒๕๖๐

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒)
พ.ศ. ๒๕๖๐: ที่มาและสาระสำคัญ



พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

- เมื่อวันที่ ๑๖ ธ.ค. ๒๕๕๙ ที่ประชุมสภานิติบัญญัติแห่งชาติ มีมติ เห็นด้วย ๑๖๘ ไม่เห็นด้วย ๐ งดออกเสียง ๕ ให้ผ่านร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ...) พ.ศ. ... โดยรอประกาศใช้เป็นกฎหมายต่อไปใน ๑๒๐ วัน
- พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ.๒๕๖๐ หรือ พ.ร.บ.คอมพิวเตอร์ฉบับใหม่ ได้รับการประกาศในราชกิจจานุเบกษาเมื่อวันที่ ๒๕ มกราคมที่ผ่านมา ซึ่งกฎหมายจะมีผลบังคับใช้อย่างเป็นทางการในอีก ๑๒๐ วัน
- ในระหว่างนี้กระทรวงดีอี จะทำหน้าที่ยกร่างกฎกระทรวงมาใช้งานร่วมกับ พ.ร.บ.คอมพิวเตอร์ เนื่องจากข้อกำหนดหลายประเด็นมีการระบุในเรื่องของเนื้อหาที่กว้างเกินไป การที่มีกฎกระทรวงและกฎหมายลูกเข้ามาใช้ประกอบ จะทำให้การตีความไปจนถึงการบังคับใช้ของกฎหมายมีความละเอียดมากยิ่งขึ้น



ประเด็นต่อต้านและข้อเท็จจริงเกี่ยวกับ **พ.ร.บ.คอมพ์**



ประเด็นต่อต้าน

ให้อำนาจรัฐจัดตั้งซิงเกิล เกตเวย์ และซิงเกิล คอมมานด์ เพื่อสอดแนมข้อมูลประชาชนและทำให้การใช้งานอินเทอร์เน็ตช้าลง

1.

ข้อเท็จจริง

พ.ร.บ.คอมพ์ไม่มีมาตราใดที่กำหนดให้ประเทศไทย มีซิงเกิล เกตเวย์ ดังนั้นร่างพ.ร.บ.คอมพ์จึง ไม่ได้ให้รัฐเข้าไปสอดแนมหรือล้วงข้อมูล การติดต่อสื่อสารของประชาชน ขณะที่การกระทำดังกล่าวมีความผิดตามมาตรา 8 พ.ร.บ.คอมพ์ พ.ศ. 2550



ประเด็นต่อต้าน

มาตรา 14 (1)(2) ปิดกั้นเสรีภาพการแสดงความคิดเห็น/ปิดปากการตรวจสอบโดยประชาชน/ปิดปากคนเห็นต่างเพราะถ้อยคำหรือเงื่อนไขที่ใช้ไม่มีความชัดเจนในตัวเอง ทำให้สามารถตีความขยายได้

2.

ข้อเท็จจริง

มาตรา 14 ที่แก้ไข ไม่ได้ต้องการปิดกั้นเสรีภาพการแสดงความคิดเห็น ปิดปากการตรวจสอบของประชาชน

ประเด็นต่อต้าน

ร่างประกาศกฤษฎีกาใต้ร่างพ.ร.บ. ให้อำนาจรัฐจัดตั้งศูนย์กลางบล็อกเว็บ ที่เชื่อมต่อตรงระบบของผู้ให้บริการ

3.

ข้อเท็จจริง

ร่างประกาศกฤษฎีกาใต้มาตรา 20 ไม่ได้ให้อำนาจรัฐหรือเจ้าหน้าที่เชื่อมต่อระบบผู้ให้บริการเพื่อปิดเว็บไซต์ โดยไม่ได้รับอนุญาตจากศาล ส่วนการจัดตั้งศูนย์กลางตามร่างประกาศกฤษฎีกาก็เพื่อให้มีช่องทางในการประสานงานกับผู้ให้บริการและติดตามการดำเนินการตามทนายศาสตร์

ประเด็นต่อต้าน

ต่อไปถ้าเน็ตล่ม คือ ล่มทั้งประเทศไทย

4.

ข้อเท็จจริง

ประเทศไทยเปิดเสรีในการให้บริการสื่อสารโทรคมนาคมและมีผู้ให้บริการเกตเวย์และอินเทอร์เน็ตหลายรายจึงมีโอกาสน้อยมากที่ผู้ให้บริการทุกรายจะไม่สามารถให้บริการพร้อมกันได้



ประเด็นต่อต้าน

การเข้าถึงเว็บต่างประเทศ จะทำได้ยากขึ้น

5.

ข้อเท็จจริง

ความเร็วและความสามารถในการเข้าเว็บไซต์ต่างประเศยังเหมือนเดิม เนื่องจากพ.ร.บ.คอมพ์ไม่ได้ลดจำนวนช่องทางการใช้อินเทอร์เน็ตต่างประเทศ



พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

โครงสร้างของเนื้อหากฎหมายมีลักษณะคล้ายคลึงฉบับเดิม โดยมีสาระสำคัญที่ต่างไปบ้าง

พ.ร.บ. ฉบับเดิม ใช้บังคับเป็นเวลากว่า ๑๐ ปี โดยที่ผ่านมาพบว่ากฎหมายมีปัญหาในการตีความ จนกระทบกับการบังคับใช้ เช่น การนำฐานความผิดที่ใช้กับเรื่องข้อโกงปลอมแปลงทางออนไลน์ ไปใช้กับการหมิ่นประมาท ทำให้กระทบต่อสิทธิเสรีภาพในการแสดงความคิดเห็น จนทำให้เกิดการโจมตีจากประชาคม โลกและเกิดกระแสสังคมเรียกร้องหลักประกันสิทธิเสรีภาพในการแสดงความคิดเห็นขึ้น กอปรกับเพื่อ เป็นการปรับปรุงกฎหมายให้เท่าทันกับเทคโนโลยีและภัยคุกคามที่เปลี่ยนแปลงไป

วัตถุประสงค์/เหตุผลการแก้ไข

(๑) ให้รัฐมนตรีว่าการกระทรวงดิจิทัลฯ รักษาการตามพระราชบัญญัติ

(๒) บทบัญญัติบางประการที่ไม่เหมาะสมต่อการป้องกันและปราบปรามการกระทำ ความผิดเกี่ยวกับคอมพิวเตอร์ในปัจจุบัน ซึ่งมีรูปแบบการกระทำความผิดที่มีความ ซับซ้อนมากขึ้น เช่นเพิ่มเติมฐานความผิดและกำหนดโทษผู้ส่งข้อมูลคอมพิวเตอร์ หรือจดหมายอิเล็กทรอนิกส์ แก่บุคคลอื่น

(๓) มาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งการเฝ้าระวังและ ติดตามสถานการณ์ด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศของ ประเทศ สมควรปรับปรุงบทบัญญัติในส่วนที่เกี่ยวข้องกับผู้รักษากฎหมาย

(๔) กำหนดโทษของความผิดดังกล่าว การปรับปรุงกระบวนการและหลักเกณฑ์ใน การระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์

หมวด ๑ ความผิดเกี่ยวกับคอมพิวเตอร์

➔ แก้ไขเพิ่มเติม

- ม.๑๑ ความผิดฐานส่งสแปมโดยปกปิดแหล่งที่มา
- ม.๑๒ เพิ่มโทษการเจาะระบบ การทำลายระบบที่เกี่ยวข้องกับความมั่นคง
- ม.๑๔ มุ่งเอาผิดการกระทำต่อทรัพย์สินชัดเจนขึ้น ไม่ให้ตีความเอาความผิดกับการหมิ่นประมาท
เอาความผิดการนำเข้าข้อมูลเท็จที่น่าจะทำให้เกิดความเสียหายต่อความมั่นคงฯ ประเทศ สาธารณะและเศรษฐกิจ/ก่อความตื่นตระหนก
- ม.๑๕ ผู้ให้บริการที่ไม่ลบเนื้อหาผิดกฎหมาย
- ม.๑๖ การเผยแพร่ภาพตัดต่อ ภาพคนตาย ก็อาจผิดได้
- ม.๑๖ ๑๖/๑ ให้ยึดและทำลายภาพตัดต่อได้

หมวด ๒ พนักงานเจ้าหน้าที่

➔ แก้ไขเพิ่มเติม อำนาจหน้าที่ (มาตรา ๑๘)

- (๑) มีหนังสือ/เรียกเพื่อให้ถ้อยคำ/เอกสาร
- (๒) เรียกข้อมูลจราจร
- (๓) สั่งให้ส่งมอบข้อมูลที่อยู่ในครอบครอง
- (๔) ทำสำเนาข้อมูล (๕) สั่งให้ส่งมอบข้อมูล/อุปกรณ์
- (๖) ตรวจสอบ/เข้าถึง (๗) ถอดรหัสลับ (๘) ยึด/อายัดระบบ

➔ แก้ไขเพิ่มเติมการ block เว็บไซต์ ตามมาตรา ๒๐

เพิ่มเติมความผิด ให้ครอบคลุมกรณีต่างๆมากขึ้น เช่นความผิดเกี่ยวกับทรัพย์สินทางปัญญา ความที่ขัดต่อความสงบเรียบร้อย/ศีลธรรม
แต่งตั้งคณะกรรมการกึ่งนกรองพิจารณาการปิดกั้น

➔ หน้าที่ของผู้ให้บริการ มาตรา ๒๖

เก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน แต่ไม่เกิน ๒ ปี
เป็นกรณีพิเศษเฉพาะราย/เฉพาะคราว

พ.ร.บ.(ฉบับที่ ๒) พ.ศ. ๒๕๖๐ ให้มีการร่างประกาศ/ระเบียบ เพื่อให้เห็นแนวทางการใช้บังคับ

<p>มาตรา ๑๑</p> <p>กำหนดให้ชัดเจนวาอะไรคือ สแปม หรือจดหมายอิเล็กทรอนิกส์ ที่ทำให้เดือดร้อนรำคาญ</p>	<p>ประกาศ เรื่อง หลักเกณฑ์เกี่ยวกับลักษณะและวิธีการส่ง ลักษณะ และ ปริมาณของข้อมูลคอมพิวเตอร์ ซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อน รำคาญแก่ผู้รับ และลักษณะอันเป็นการปฏิเสธการตอบรับได้โดยง่าย พ.ศ. ..</p>
<p>มาตรา ๑๕</p> <p>เมื่อผู้ให้บริการจำเป็นต้องระงับการเผยแพร่เว็บไซต์ และยกเว้นโทษให้กับผู้ให้บริการ</p>	<p>ประกาศ เรื่อง ขั้นตอนการแจ้งเตือนการระงับการทำให้แพร่หลายของข้อมูล คอมพิวเตอร์ และการนำข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์ พ.ศ.</p>
<p>มาตรา ๑๗/๑</p> <p>วางกลไกเปรียบเทียบความผิดสำหรับโทษสถานเบา</p>	<p>ประกาศ เรื่อง แต่งตั้งคณะกรรมการเปรียบเทียบ ตาม พ.ร.บ.วาดวย การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.</p>
<p>มาตรา ๒๐</p> <p>การระงับการเผยแพร่ ต้องตรวจสอบ การใช้อำนาจโดยศาล</p> <p>เฉพาะเนื้อหาที่ขัดต่อการสงบเรียบร้อย</p> <p>(ที่กระทบต่อสังคมในวงกว้าง) ต้องมีคณะกรรมการกลั่นกรอง (อย่างน้อยต้องมีเอกชนจากสายสื่อ, สิทธิมนุษยชน ไอที) อีกชั้นหนึ่ง ก่อนให้ศาลตรวจสอบ ถ่วงดุลการทำหน้าที่</p>	<p>ประกาศ เรื่อง หลักเกณฑ์ ระยะเวลา และวิธีการปฏิบัติสำหรับการระงับการ ทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ของพนักงานเจ้าหน้าที่หรือ ผู้ให้บริการ พ.ศ.</p> <p>ประกาศ เรื่อง แต่งตั้งคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์ ตาม พ.ร.บ.วาดวยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ...</p>
<p>มาตรา ๒๑</p> <p>กำหนดชุดคำสั่งไม่พึงประสงค์ ที่ไซประโยชน์ใด เซน ไซตัวสอบของโหวงยอมไม่ผิดกฎหมาย</p>	<p>ประกาศ เรื่อง กำหนดรายชื่อ ลักษณะ หรือรายละเอียดของชุดคำสั่ง ไม่พึงประสงค์ ซึ่งอาจนำมาใช้เพื่อป้องกันหรือแก้ไขชุดคำสั่งไม่พึงประสงค์ ก็ได้ (อาจมีการจัดทำในภายหลัง)</p>

มาตรา ๑๑ กำหนดให้ชัดเจนว่คืออะไรคือ สแปมหรือจดหมายอิเล็กทรอนิกส์ ที่ทำให้เดือดร้อนรำคาญ และเพิ่มโทษพวก spam หรือข้อมูลอิเล็กทรอนิกส์ ที่ทำให้เดือดร้อนรำคาญ โดยเฉพาะในเชิงพาณิชย์พวกโฆษณาอะไรต่างๆ

พรบ. พ.ศ. ๒๕๕๐ มาตรา ๑๑

ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่น โดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข

ระวางโทษปรับไม่เกินหนึ่งแสนบาท

พรบ.(ฉบับที่ ๒) พ.ศ. ๒๕๖๐ มาตรา ๑๑

ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่น

- ลักษณะเป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับข้อมูลคอมพิวเตอร์
- หรือจดหมายอิเล็กทรอนิกส์ โดยไม่เปิดโอกาสให้ผู้รับสามารถบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย

ระวางโทษปรับไม่เกินสองแสนบาท

รมว. ดีอี

ออกประกาศกำหนดลักษณะและวิธีการส่ง รวมทั้งลักษณะและปริมาณของข้อมูลคอมพิวเตอร์/จดหมายอิเล็กทรอนิกส์ ซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับ และลักษณะอันเป็นการบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย

	<p>พรบ.คอมพิวเตอร์ฯ พ.ศ.๒๕๕๐</p>	<p>พรบ.คอมพิวเตอร์ฯ (ฉบับที่ ๒) พ.ศ.๒๕๖๐</p>
<p>มาตรา ๑๒ ความผิดต่อข้อมูล/ ระบบความมั่นคง</p>	<p>ก่อให้เกิดความเสียหายต่อข้อมูล/ ระบบ เกี่ยวกับความมั่นคง ลงโทษ จำคุก ๓-๑๕ ปี และปรับ ๑ หมื่น-๓ แสนบาท เป็นเหตุให้ผู้อื่นถึงแก่ความตาย ลงโทษจำคุก ๑๐-๒๐ ปี</p>	<p>กรณีกระทำต่อข้อมูลคอมพิวเตอร์หรือ ระบบ คอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคง ปลอดภัยของประเทศ <i>ความปลอดภัยสาธารณะ</i> ความมั่นคงในทางเศรษฐกิจของประเทศ หรือ โครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ เพิ่มโทษการเจาะระบบ การทำลายระบบที่เกี่ยวกับความมั่นคงของประเทศ</p>

มาตรา ๑๒ ยกเลิก และให้กำหนดขึ้นใหม่ เน้นเกี่ยวกับการปกป้องโครงสร้างพื้นฐานสำคัญของประเทศ

พรบ. พ.ศ. ๒๕๕๐ มาตรา ๑๒

ถ้าการกระทำความผิดตามมาตรา ๙ หรือ ๑๐

(๑) ก่อให้เกิดความเสียหายแก่ประชาชน (โทษ ๑๐ ปี ๒ แสนบาท)

(๒) เกิดความเสียหายต่อข้อมูล/ระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจ/การบริการสาธารณะ (โทษตั้งแต่ ๓ ปีถึง ๑๕ ปี ปรับตั้งแต่ ๖ หมื่นถึง ๓ แสนบาท)

ถ้าการกระทำความผิดตาม(๒) เป็นเหตุให้ผู้อื่นถึงแก่ความตาย (โทษจำคุกตั้งแต่ ๑๐ ปีถึง ๒๐ ปี)

ระวางโทษที่สูงสุดถึง ๒๐ ปี

พรบ. (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ มาตรา ๑๒

ถ้าการกระทำความผิดตามมาตรา ๕ , ๖ , ๗ , ๘ หรือ ๑๑ เป็นการกระทำต่อข้อมูล/ระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศฯ

ถ้าการกระทำความผิดตามวรรคหนึ่งเป็นเหตุให้เกิดความเสียหายต่อข้อมูล/ระบบคอมพิวเตอร์ดังกล่าว (ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงสิบปี และปรับตั้งแต่สองหมื่นบาทถึงสองแสนบาท)

ถ้าการกระทำความผิดตามมาตรา ๙ หรือ ๑๐ เป็นการกระทำต่อข้อมูล/ระบบคอมพิวเตอร์ตามวรรคหนึ่ง (ต้องระวางโทษจำคุกตั้งแต่ ๓ ถึง ๕ ปีปรับ ๖ หมื่นถึง ๓ แสนบาท)

ถ้าการกระทำความผิดตามวรรคหนึ่งถึงสามถ้าการกระทำความผิดตามมาตรา ๙ หรือ ๑๐ โดยมีได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึงแก่ความตาย(ต้องระวางโทษจำคุกตั้งแต่ห้าปีถึงยี่สิบปี และปรับตั้งแต่หนึ่งแสนบาทถึงสี่แสนบาท”)

เพิ่มเติม ๑๒/๑ ถ้าการกระทำความผิดตามมาตรา ๙ หรือ ๑๐ เป็นเหตุให้เกิดอันตราย/ทรัพย์สินผู้อื่น และ

การกระทำนั้นโดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึงแก่ความตาย (ระวางโทษ ๕ ถึง ๒๐ ปี/ปรับ ๑ ถึง ๔ แสนบาท)

แก้ไขในมาตรา ๑๒ และ ๑๒/๑ สรุปลอัตราโทษที่ปรับปรุงใหม่

มาตรา	ฐานความผิด	อัตราโทษ
ม. ๑๒	<p>* เมื่อการแฮกข้อมูลหรือระบบ, ดักจับ, Spam, เปิดเผยแพร่มาตรการป้องกัน ทำต่อ โครงสร้างสำคัญ เช่น ไฟฟ้า ประปา หากเกิดความเสียหายตามมาดวย</p> <p>*เมื่อแก้ไขเปลี่ยนแปลงข้อมูล, ขัดขวางหรือชะลอการทำงานระบบ ทำต่อ โครงสร้างสำคัญ เช่น ไฟฟ้า ประปา</p> <p>ไม่เจตนา แต่ทำให้คนตาย</p>	<p>โทษ ๑-๗ ป ปรับ ๑๐,๐๐๐ - ๑๔๐,๐๐๐</p> <p>โทษ ๑-๑๐ ป ปรับ ๒๐,๐๐๐ - ๒๐๐,๐๐๐</p> <p>โทษ ๓-๑๕ ป ปรับ ๖๐,๐๐๐ - ๓๐๐,๐๐๐</p> <p>โทษ ๕-๒๐ ปี ปรับ ๑๐๐,๐๐๐ - ๔๐๐,๐๐๐</p>
ม. ๑๒/๑	<p>*แก้ไขเปลี่ยนแปลง, ทำให้ระบบทำงานไม่ปกติ ทำให้ บาดเจ็บ ทรัพย์สินเสียหาย</p> <p>ไม่เจตนา แต่ทำให้คนตาย</p>	<p>ไม่เกิน ๑๐ ป ปรับไม่เกิน ๒๐๐,๐๐๐</p> <p>โทษ ๕-๒๐ ป ปรับ ๑๐๐,๐๐๐ - ๔๐๐,๐๐๐</p>

มาตรา ๑๓ การเผยแพร่ชุดคำสั่ง มีการเพิ่มเติม

พรบ. ปี ๒๕๕๐ มาตรา ๑๓

พรบ. (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ มาตรา ๑๓

ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้น โดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือ ในการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ มาตรา ๙ มาตรา ๑๐ หรือ มาตรา ๑๑

ระวางโทษจำคุกไม่เกิน ๑ ปี หรือปรับไม่เกิน ๒ หมื่นบาท หรือทั้งจำทั้งปรับ

ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะ

- เพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๑๒ (๑)/(๓) (ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ)

- เพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ มาตรา ๙ มาตรา ๑๐ หรือมาตรา ๑๑ หากผู้นำไปใช้ได้กระทำความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม หรือต้องรับผิดตามมาตรา ๑๒ วรรคสองหรือวรรคสี่หรือมาตรา ๑๒/๑ ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งดังกล่าวจะต้องรับผิดทางอาญาตามความผิดที่มีกำหนดโทษสูงขึ้นไปด้วยก็เฉพาะเมื่อตนได้รู้หรืออาจเล็งเห็นได้ว่าจะเกิดผลเช่นที่เกิดขึ้นนั้น

- เพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๑๒ (๑)/(๓) หากผู้นำไปใช้ได้กระทำความผิดตามมาตรา ๑๒ (๑)/(๓) หรือต้องรับผิดตามมาตรา ๑๒ (๒)/(๔) หรือมาตรา ๑๒/๑ ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งดังกล่าวต้องรับผิดทางอาญาตามความผิดที่มีกำหนดโทษสูงขึ้นไปด้วย

ในกรณีที่ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งผู้ใดต้องรับผิดตามวรรคหนึ่งหรือวรรคสอง และตามวรรคสามหรือวรรคสี่ด้วย ให้ผู้นั้นต้องรับโทษที่มีอัตราโทษสูงที่สุดแต่กระหนเดียว”

มาตรา ๑๓ เอาผิดกับคนที่นำชุดคำสั่งไปจำหน่าย คือหากนำไปใช้แล้วเกิดความเสียหายกับความมั่นคงปลอดภัยในเรื่องความมั่นคง ใครที่นำชุดคำสั่งนี้ไปจำหน่าย ทั้งที่รู้อยู่แล้วว่าชุดคำสั่งเหล่านี้ เมื่อนำไปใช้แล้ว มันจะมีผลอย่างนั้น ให้รับโทษ โดยเฉพาะหากนำชุดคำสั่งนี้ไปจำหน่ายแล้วมีการนำไปใช้ จนทำให้มีคนบาดเจ็บ คนเสียชีวิต โทษก็จะมีผลสูงมากขึ้น

มาตรา	ฐานความผิด	อัตราโทษ
๑๓	<p>วรรค ๑ จำหน่ายชุดคำสั่ง/เผยแพร่ไปใช้เป็นเครื่องมือกระทำผิด ต่อข้อมูลหรือระบบ ทำต่อโครงสร้างสำคัญ เช่น ไฟฟ้า ประปา</p> <p>วรรค ๒ จำหน่ายชุดคำสั่ง/เผยแพร่ไปใช้เป็นเครื่องมือกระทำผิด แสกขอมูลหรือระบบ, ดักจับ, Spam,เปิดเผยมาตรการป้องกัน</p> <p>วรรค ๓ เมื่อนำไปใช้เป็นเครื่องมือทำความผิด</p> <p>วรรค ๔ ในกรณีที่ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งผู้ใดต้องรับผิดตามวรรค ๑ หรือวรรค ๒ และตามวรรค ๓ หรือวรรค ๔ ด้วย</p>	<p>โทษ ๒ ป ปรับไม่เกิน ๔๐,๐๐๐</p> <p>รับผิดทางอาญาตามความผิดที่มีกำหนดโทษสูงขึ้นด้วย</p> <p>ตามมาตรา ๑๒ (๑)/(๓) หากผู้นำไปใช้ได้กระทำความผิดตามมาตรา ๑๒ (๑)/(๓) หรือต้องรับผิดตามมาตรา ๑๒ (๒)/(๔) หรือมาตรา ๑๒/๑</p> <p>ให้ผู้นั้นต้องรับโทษที่มีอัตราโทษสูงที่สุดแต่กระหนเดียว</p>

	พรบ.คอมพิวเตอร์ฯ พ.ศ.๒๕๕๐	พรบ.คอมพิวเตอร์ฯ (ฉบับที่ ๒) พ.ศ.๒๕๖๐
<p>การนำเข้าข้อมูล เท็จ ตามมาตรา ๑๔(๑)</p>	<p>เปิดช่องให้ตีความเอาผิดกับ การหมิ่นประมาทออนไลน์</p>	<p>ม.๑๔(๑) โดยทุจริตหรือโดยหลอกลวงนำเข้าสู่ระบบ คอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่ว่า ทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดย ประการที่น่าจะเกิดความเสียหายแก่ประชาชน</p> <p>มุ่งเอาผิดการกระทำต่อทรัพย์สินชัดเจนขึ้น</p> <p>และยังเปิดช่องให้ตีความเอาผิด</p> <p>กับการบิดเบือนได้</p> <p>อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตาม ประมวลกฎหมายอาญา</p>

มาตรา ๑๔

พรบ. ปี ๒๕๕๐ มาตรา ๑๔

กระทำความผิดที่ระบุไว้ ดังต่อไปนี้ (มี ๕ องค์ประกอบ)

มาตรา ๑๔ (๑) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

มาตรา ๑๔ (๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

มาตรา ๑๔ (๓), (๔) และ (๕) ยังเหมือนเดิม

จำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

พรบ. (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ มาตรา ๑๔

มาตรา ๑๔(๑) โดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์ที่**บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วน** หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน **อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา**

มาตรา ๑๔(๒) ต้องเป็นกรณีที่น่าจะเกิดความเสียหาย คือมีการนำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์นั้นเป็นเท็จ คือนำข้อมูลอันเป็นเท็จเข้าไปในระบบ โดยประการที่น่าจะก่อให้เกิดความเสียหาย**ต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ๑ ความมั่นคงทางเศรษฐกิจ ความปลอดภัยของประเทศในเรื่องโครงสร้างพื้นฐาน หรือประโยชน์สาธารณะ**

ถ้าการกระทำความผิดตามวรรคหนึ่ง (๑) มิได้กระทำต่อประชาชน แต่เป็นการกระทำต่อบุคคลใดบุคคลหนึ่ง ผู้กระทำ ผู้เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ดังกล่าวต้อง**ระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ และให้เป็นความผิดอันยอมความได้”**

มาตรา ๑๔ การนำข้อมูลเข้าระบบแล้วทำให้เกิดความเสียหาย กฎหมายที่ใช้อยู่ปัจจุบัน พบว่ามีการนำมาตรา ๑๔ (๑) ไปใช้
แจ้งความฐานหมิ่นประมาท คือนำเข้าข้อมูลอันเป็นเท็จที่ทำให้เกิดความเสียหายต่อผู้อื่น

พรบ. ปี ๒๕๕๐ มาตรา ๑๔

พรบ. (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ มาตรา ๑๔

กระทำความผิดที่ระบุไว้ ดังต่อไปนี้ (มี ๕ องค์ประกอบ)

(๑) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่ง

ข้อมูล คอมพิวเตอร์ปลอมไม่ว่าทั้งหมด
หรือบางส่วน หรือข้อมูลคอมพิวเตอร์อัน
เป็นเท็จ โดยประการที่น่าจะเกิดความเสียหาย
แก่ผู้อื่นหรือประชาชน

ประเด็นที่แก้ไข มาตรา ๑๔(๑)

แก้ไขโดยเพิ่มคำว่า “โดยทุจริตหรือโดยหลอกลวง” เข้าไปจาก เดิมมาตรา
๑๔ ของปี ๒๕๕๐ และ...ซึ่งข้อมูลคอมพิวเตอร์ที่**บิดเบือนหรือปลอม .. และ**
อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา

บิดเบือน เช่น บิดเบือนราคาหุ้นในตลาดหลักทรัพย์ฯ ที่ทำให้กลไกของ
ตลาดหลักทรัพย์ผิดไป

(๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่ง

ข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่
น่าจะเกิดความเสียหาย**ต่อความมั่นคงของ**
ประเทศ หรือก่อให้เกิดความตื่นตระหนก
แก่ประชาชน

ประเด็นที่แก้ไข มาตรา ๑๔(๒)

“นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่
น่าจะเกิดความเสียหาย**ต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความ**
ปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้าง
พื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิดความตื่น
ตระหนกแก่ประชาชน”

มาตรา ๑๕ ให้ยกเลิกความเดิมในมาตรานี้ และให้ใช้ความต่อไปนี้แทน (กำหนดมาตรการในการคุ้มครองผู้ให้บริการ)

พรบ. ปี ๒๕๕๐ มาตรา ๑๕

ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา ๑๔

จำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

พรบ. (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ มาตรา ๑๕

ผู้ให้บริการผู้ใดให้ความร่วมมือ ยินยอม หรือรู้เห็นเป็นใจให้มีการกระทำความผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน **ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา ๑๔**

ให้รัฐมนตรีออกประกาศกำหนดขั้นตอนการแจ้งเตือน การระงับการทำให้แพร่หลายของข้อมูลคอมพิวเตอร์ และการนำข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์

ถ้าผู้ให้บริการพิสูจน์ได้ว่าตนได้ปฏิบัติตามประกาศของรัฐมนตรีที่ออกตามวรรคสอง ผู้นั้นไม่ต้องรับโทษ”

สรุป ออกกฎกระทรวงว่า ไม่ผิด ถ้าเราไม่รู้ เราเป็นเพียงท่อผ่านข้อมูล ไม่ผิดตามกฎหมาย จะผิดก็ต่อเมื่อ ๒ กรณี คือ ๑.เมื่อเราเป็นคนเลือกเอาข้อมูลเข้าไปใส่เอง

๒.เมื่อมีแบบฟอร์มของกระทรวงดิจิทัลฯ ที่ระบุชื่อนามสกุล เหตุพิพาทของผู้ร้องเรียนและใบแจ้งความกับเจ้าหน้าที่ตำรวจ ถ้าใครแจ้งเท็จก็โดนข้อหาไป แล้วส่งมาให้ผู้ให้บริการ เจ้าของเฟซบุ๊ก หรือผู้ให้บริการแต่ละราย ซึ่งจะเป็นคนกำหนดเองว่า จะเอาข้อมูลอันเป็นเท็จออกได้ภายในกี่วัน ซึ่งจะมีอยู่ในประกาศของกระทรวงฯอีกที่ ผู้ให้บริการแต่ละประเภทจะสามารถลบได้ภายในกี่วัน

ประเด็นที่แก้ไข

แต่เดิมมาตรา ๑๕ ของพ.ศ.๒๕๕๐ เขียนไว้ว่า “ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา ๑๔”

พ.ร.บ. ฉบับใหม่ .. “ผู้ให้บริการผู้ใดให้ความร่วมมือ ยินยอม หรือรู้เห็นเป็นใจให้มีการกระทำความผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา ๑๔

ให้รัฐมนตรีออกประกาศกำหนดขั้นตอนการแจ้งเตือน การระงับการทำให้แพร่หลายของข้อมูลคอมพิวเตอร์ และการนำข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์

ถ้าผู้ให้บริการพิสูจน์ได้ว่าตนได้ปฏิบัติตามประกาศของรัฐมนตรีที่ออกตามวรรคสอง **ผู้นั้นไม่ต้องรับโทษ**”

ประเด็นที่แก้ไข

นำเข้าเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้นฯ ถ้าการกระทำตามนี้เป็น การกระทำต่อภาพของผู้ตาย และการกระทำนั้นน่าจะทำให้บิดา มารดา คู่สมรส หรือบุตรของผู้ตายเสีย ชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง หรือได้รับความอับอาย ต้องได้รับโทษ

การนำเข้าสู่ระบบคอมพิวเตอร์โดยสุจริต อันเป็นการติชมด้วยความเป็นธรรม ซึ่งบุคคลหรือสิ่งใดอันเป็นวิสัยของประชาชนย่อมกระทำ ผู้กระทำไม่มีความผิด

ความผิดตามวรรคหนึ่งและวรรคสองเป็นความผิดอันยอมความได้

เพิ่ม มาตรา ๑๖/๑ ในคดีความผิดตามมาตรา ๑๔ หรือมาตรา ๑๖ ซึ่งมีคำพิพากษาว่าจำเลยมีความผิดศาลอาจสั่ง (๑) ให้ทำลายข้อมูล (๒) ให้โฆษณาหรือเผยแพร่คำพิพากษาทั้งหมดหรือแต่บางส่วนในสื่ออิเล็กทรอนิกส์ ฯ (๓) ให้ดำเนินการอื่นตามที่ศาลเห็นสมควรเพื่อบรรเทาความเสียหายที่เกิดขึ้นจากการกระทำความผิดนั้น

๑๖/๒ ข้อมูลคอมพิวเตอร์ในความครอบครองของตนเป็นข้อมูลที่ศาลสั่งให้ทำลายตามมาตรา ๑๖/๑ ผู้นั้นต้องทำลายข้อมูลดังกล่าว หากฝ่าฝืนต้องระวางโทษ

มาตรา ๑๖ ให้ยกเลิกความเดิมในมาตรานี้ และให้ใช้ความต่อไปนี้แทน

พรบ. ปี ๒๕๕๐ มาตรา ๑๖

ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ ที่ปรากฏ เป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้โดยประการที่น่าจะทำให้ผู้อื่นนั้น เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

จำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

ถ้าการกระทำตามวรรคหนึ่ง โดยสุจริต ผู้กระทำไม่มีความผิด ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้

ถ้าผู้เสียหายในวรรคหนึ่งตายก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรสหรือบุตรของผู้เสียหายร้องทุกข์ได้

พรบ. (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ มาตรา ๑๖

ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้นต้องระวางโทษจำคุกไม่เกินสามปี และปรับไม่เกินสองแสนบาท

ถ้าการกระทำตามวรรคหนึ่งเป็นการกระทำต่อภาพของผู้ตาย และการกระทำนั้นน่าจะทำให้บิดา มารดา คู่สมรส หรือบุตรของผู้ตายเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง หรือได้รับความอับอาย ผู้กระทำต้องระวางโทษดังที่บัญญัติไว้ในวรรคหนึ่ง

ถ้าการกระทำตามวรรคหนึ่งหรือวรรคสอง เป็นการนำเข้าสู่ระบบคอมพิวเตอร์โดยสุจริต อันเป็นการติชมด้วยความเป็นธรรม ซึ่งบุคคลหรือสิ่งใดอันเป็นวิสัยของประชาชนย่อมกระทำ ผู้กระทำไม่มีความผิด

ความผิดตามวรรคหนึ่งและวรรคสองเป็นความผิดอันยอมความได้

ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งหรือวรรคสองตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย”

มาตรา ๑๖/๑ และ ๑๖/๒ ให้ยกเลิกความเดิมในมาตรานี้ และให้ใช้ความต่อไปนี้แทน

พรบ. ปี ๒๕๕๐ มาตรา ๑๖

พรบ. (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ มาตรา ๑๖/๑ และ ๑๖/๒

“**มาตรา ๑๖/๑** ในคดีความผิดตามมาตรา ๑๔ หรือมาตรา ๑๖ ซึ่งมีคำพิพากษาว่า จำเลยมีความผิดศาลอาจสั่ง

(๑) ให้ทำลายข้อมูลตามมาตราดังกล่าว

(๒) ให้โฆษณาหรือเผยแพร่คำพิพากษาทั้งหมดหรือแต่บางส่วนในสื่อ อิเล็กทรอนิกส์ วิทยุกระจายเสียง วิทยุโทรทัศน์ หนังสือพิมพ์ หรือสื่ออื่นใด ตามที่ศาล เห็นสมควรโดยให้จำเลยเป็นผู้ชำระค่าโฆษณาหรือเผยแพร่

(๓) ให้ดำเนินการอื่นตามที่ศาลเห็นสมควรเพื่อบรรเทาความเสียหายที่เกิดขึ้นจากการกระทำความผิดนั้น

มาตรา ๑๖/๒ ผู้ใดรู้ว่าข้อมูลคอมพิวเตอร์ในความครอบครองของตน เป็นข้อมูลที่ศาลสั่งให้ทำลายตามมาตรา ๑๖/๑ ผู้นั้นต้องทำลายข้อมูล ดังกล่าว หากฝ่าฝืนต้องระวางโทษกึ่งหนึ่งของโทษที่บัญญัติไว้ในมาตรา ๑๔ หรือมาตรา ๑๖ แล้วแต่กรณี”

มาตรา ๑๘ แก้ไขเพิ่ม การร้องขอให้ดำเนินการกรณีความผิดอาญาต่อกฎหมายอื่นซึ่งได้ใช้ระบบคอมพิวเตอร์ข้อมูลคอมพิวเตอร์

พรบ. ปี ๒๕๕๐ มาตรา ๑๘

พรบ.(ฉบับที่ ๒) พ.ศ. ๒๕๖๐ มาตรา ๑๘

มาตรา ๑๘ อำนาจทั่วไปของพนักงานเจ้าหน้าที่ที่ได้รับการแต่งตั้ง แบ่งเป็น

- อำนาจที่ดำเนินการได้โดย ไม่ต้องใช้อำนาจศาล
 - (๑) มีหนังสือสอบถาม เพื่อให้ส่งคำชี้แจง ให้ข้อมูล
 - (๒) เรียกข้อมูลจากรายการคอมพิวเตอร์
 - (๓) สั่งให้ส่งมอบข้อมูลตาม ม.๒๖
- อำนาจที่ ต้องขออนุญาตศาล
 - ทำสำเนาข้อมูล
 - เข้าถึงระบบคอมพิวเตอร์/ข้อมูลคอมพิวเตอร์
 - ถอดรหัสลับ
 - ยึดอายัดระบบคอมพิวเตอร์

ให้พนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา อาจร้องขอให้พนักงาน เจ้าหน้าที่ตามพระราชบัญญัตินี้ฯ ดำเนินการตาม พระราชบัญญัติในบรรดาความผิดอาญาต่อกฎหมายอื่นซึ่งได้ใช้ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์หรือ อุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ เป็นองค์ประกอบหรือเป็นส่วนหนึ่งในการกระทำความผิดและ **ให้ผู้ได้รับการร้องขอ จากพนักงานเจ้าหน้าที่ดำเนินการตามคำร้องขอโดยไม่ชักช้า**

ให้ผู้ได้รับการร้องขอจากพนักงานเจ้าหน้าที่ตามวรรคหนึ่ง (๑) (๒) (๓) (๔) (๕) (๖) (๗ หรือ (๘) ดำเนินการตามคำร้องขอโดยไม่ชักช้า **แต่ต้องไม่เกินเจ็ดวัน**นับแต่วันที่ได้รับคำร้องขอ หรือภายในระยะเวลาที่พนักงานเจ้าหน้าที่กำหนด ซึ่งต้องไม่น้อยกว่าเจ็ดวันและไม่เกินสิบห้าวัน เว้นแต่ในกรณีที่มีเหตุสมควร ต้องได้รับอนุญาตจากพนักงานเจ้าหน้าที่

มาตรา ๒๐ การปิดกั้นเว็บไซต์ และที่เป็นความผิดกฎหมายอื่น / ลักษณะขัดต่อศีลธรรมอันดี ของประชาชน

พรบ. ปี ๒๕๕๐ มาตรา ๒๐

มาตรา ๒๐ ในกรณีที่การกระทำความผิดเป็นการทำให้
แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่

1. อาจกระทบกระเทือนต่อความมั่นคง
แห่งราชอาณาจักรตามที่กำหนดไว้ในภาคสอง ลักษณะ
๑ หรือลักษณะ ๑/๑ แห่งประมวลกฎหมายอาญา

2. ที่มีลักษณะขัดต่อ ความสงบเรียบร้อย
หรือศีลธรรมอันดีของประชาชน

พนักงานเจ้าหน้าที่โดยได้รับความ
เห็นชอบจากรัฐมนตรีอาจยื่นคำร้องพร้อมแสดง
พยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับ
การทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นได้

ในกรณีที่ศาลมีคำสั่งให้ระงับการทำให้
แพร่หลายซึ่งข้อมูล คอมพิวเตอร์ตามวรรคหนึ่ง ให้
พนักงานเจ้าหน้าที่ทำการระงับการทำให้แพร่หลาย
นั่นเอง หรือสั่งให้ผู้ให้บริการระงับการทำให้แพร่หลาย
ซึ่งข้อมูลคอมพิวเตอร์นั้นก็ได้

พรบ. (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ มาตรา ๒๐

ในกรณีที่มีการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ ดังต่อไปนี้
พนักงานเจ้าหน้าที่โดยได้รับความเห็นชอบจากรัฐมนตรีอาจยื่นคำร้อง
พร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจ ขอให้ มีคำสั่งระงับการ
ทำให้แพร่หลาย/ลบข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์ได้

(๑) ข้อมูลคอมพิวเตอร์ที่เป็นความผิดตามพระราชบัญญัตินี้

(๒) ข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่ง
ราชอาณาจักรตามที่กำหนดไว้ในภาค ๒ ลักษณะ ๑ หรือลักษณะ ๑/๑
แห่งประมวลกฎหมายอาญา

(๓) ข้อมูลคอมพิวเตอร์ที่เป็นความผิดอาญาตามกฎหมายเกี่ยวกับ
ทรัพย์สินทางปัญญา หรือกฎหมายอื่นซึ่งข้อมูลคอมพิวเตอร์นั้นมีลักษณะ
ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชนและเจ้าหน้าที่
ตามกฎหมายนั้น หรือพนักงานสอบสวนตามประมวลกฎหมายวิธี
พิจารณาความอาญาได้ร้องขอ

มาตรา ๒๐ การปิดกั้นเว็บไซต์ และให้มีประกาศหลักเกณฑ์ สำหรับการระงับ/ลบข้อมูล

พรบ. (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ มาตรา ๒๐

ขั้นตอนการปิดกั้น

ในกรณีที่มีคำสั่งให้ระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ ให้พนักงานเจ้าหน้าที่ทำการระงับการทำให้แพร่หลายหรือลบข้อมูลนั้นเอง หรือสั่งให้ผู้ให้บริการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์นั้นก็ได้ ทั้งนี้ ให้รัฐมนตรีประกาศกำหนดหลักเกณฑ์ ระยะเวลา และวิธีปฏิบัติสำหรับการระงับการทำให้เผยแพร่หรือลบข้อมูลของพนักงานเจ้าหน้าที่หรือผู้ให้บริการให้เป็นไปในแนวทางเดียวกันโดยคำนึงถึงพัฒนาการทางเทคโนโลยีสารสนเทศที่เปลี่ยนแปลงไป เว้นแต่ศาลจะมีคำสั่งเป็นอย่างอื่น

ในกรณีที่มีเหตุจำเป็นเร่งด่วน พนักงานเจ้าหน้าที่จะยื่นคำร้องตามวรรคหนึ่งไปก่อนที่จะได้รับความเห็นชอบจากรัฐมนตรีก็ได้ แต่ทั้งนี้ต้องรายงานให้รัฐมนตรีทราบโดยเร็ว

เพิ่มเติม มาตรา ๒๐/๑ ข้อมูลซึ่งขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน โดยให้รัฐมนตรีโดยความเห็นชอบของคณะกรรมการกฤษฎีกาออกข้อมูลคอมพิวเตอร์ให้เจ้าหน้าที่นำไปยื่นเรื่องต่อศาล เพื่อขอให้ศาลมีคำสั่งระงับหรือลบ

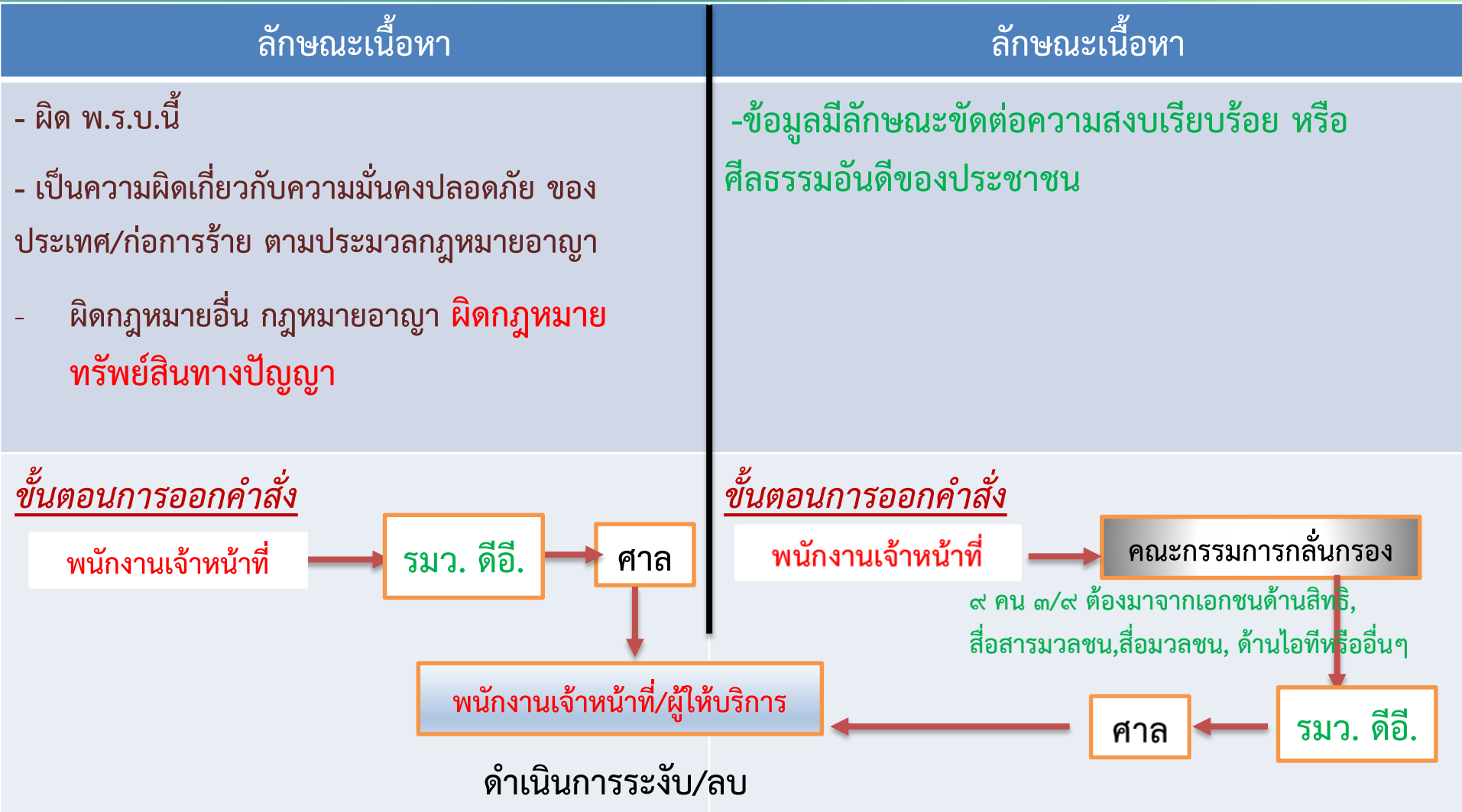
พรบ. (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ มาตรา ๒๐/๑

ในกรณีที่ทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน และรัฐมนตรีโดยความเห็นชอบของคณะกรรมการกฤษฎีกา เห็นสมควรให้พนักงานเจ้าหน้าที่ยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจ ขอให้มมีคำสั่งระงับการทำให้แพร่หลายหรือลบซึ่งข้อมูลนั้นออกจากระบบคอมพิวเตอร์

ให้รัฐมนตรีแต่งตั้งคณะกรรมการกฤษฎีกาออกข้อมูลคอมพิวเตอร์ตามวรรคสองขึ้นคณะหนึ่งหรือหลายคณะ แต่ละคณะให้มีกรรมการจำนวนเก้าคน ซึ่งสามในเก้าคนต้องมาจากผู้แทนภาคเอกชนด้านสิทธิมนุษยชน ด้านสื่อสารมวลชน ด้านเทคโนโลยีสารสนเทศ หรือด้านอื่นที่เกี่ยวข้อง และให้กรรมการได้รับค่าตอบแทนตามหลักเกณฑ์ที่รัฐมนตรีกำหนด โดยได้รับความเห็นชอบจากกระทรวงการคลัง

ในกรณีที่มีเหตุจำเป็นเร่งด่วน พนักงานเจ้าหน้าที่โดยความเห็นชอบของคณะกรรมการกฤษฎีกาจะยื่นคำร้องตามวรรคหนึ่งไปก่อนที่รัฐมนตรีมอบหมาย ก็ได้ แต่ทั้งนี้ต้องรายงานให้รัฐมนตรีทราบโดยเร็ว”

เพิ่มมาตรการดูแลเนื้อหา(Content)ที่ผิดกฎหมายอื่น/กระทบความสงบฯ คีลธรรมฯ
ลดผลกระทบต่อสังคม แต่การปิดเว็บต้องผ่านกลไกของศาล (ตามมาตรา ๒๐)



ประเด็นที่แก้ไข ในกรณีที่ขอให้มีคำสั่งระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์นั้น ออกจากระบบคอมพิวเตอร์ได้

เพิ่มเติม “ข้อมูลคอมพิวเตอร์ที่เป็นความผิดอาญาตามกฎหมายเกี่ยวกับ**ทรัพย์สินทางปัญญา หรือกฎหมายอื่นซึ่งข้อมูลคอมพิวเตอร์นั้นมีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน..**”

ในกรณีที่มีการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่มีลักษณะขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน รัฐมนตรีโดยความเห็นชอบของคณะกรรมการกฤษฎีกา ก่อน แสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้แพร่หลายหรือลบซึ่ง ข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์

ในกรณีที่ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ พนักงาน เจ้าหน้าที่จะทำการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์นั้นเอง หรือจะสั่ง ให้ผู้ให้บริการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์นั้นก็ได้ ทั้งนี้ ให้ รัฐมนตรีประกาศกำหนด หลักเกณฑ์ ระยะเวลา และวิธีการปฏิบัติ

มาตรา ๒๖ การเก็บรักษาข้อมูลจราจร

พรบ. ปี ๒๕๕๐ มาตรา ๒๖

มาตรา ๒๖ ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้**ไม่น้อยกว่าเก้าสิบวัน**นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์**ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปี**เป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้นับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การให้บริการสิ้นสุดลง

ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใด ให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท

พรบ. (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ มาตรา ๒๖

มาตรา ๒๖ ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้**ไม่น้อยกว่าเก้าสิบวัน** นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์**ไว้เกินเก้าสิบวัน แต่ไม่เกินสองปี**เป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

นอกจากนี้ ยังมีการแก้ไขในมาตรา อื่น ๆ ที่เกี่ยวข้องกับพนักงานเจ้าหน้าที่ตามพระราชบัญญัติฯ ให้มีความรัดกุม คล่องตัวในการปฏิบัติงาน และกำหนดบทลงโทษพนักงานเจ้าหน้าที่ที่ชัดเจนขึ้นด้วย

เช่น มีการแก้ไขความในมาตรา ๒๒ มาตรา ๒๓ มาตรา ๒๔ และมาตรา ๒๕ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐

และมาตรา ๒๘ “ผู้ที่ได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ คำนึงถึงภาระหน้าที่ ความรู้ความเชี่ยวชาญ ความขาดแคลนในการหาผู้มาปฏิบัติหน้าที่ หรือมีการสูญเสียผู้ปฏิบัติงานออกระบบราชการเป็นจำนวนมาก คุณภาพของงาน และการดำรงตนอยู่ในความยุติธรรม โดยเปรียบเทียบค่าตอบแทนของผู้ปฏิบัติงานอื่นในกระบวนการยุติธรรมด้วย”

การใช้อำนาจของพนักงานเจ้าหน้าที่ตามร่าง พ.ร.บ. คอมฯ ยังต้องทำตามกลไกตรวจสอบการใช้ อำนาจรัฐตามที่กฎหมายปัจจุบันกำหนดไว้ ซึ่งส่วนใหญ่ต้องขออนุญาตจากศาลก่อนจึงจะ ดำเนินการ ได้ เช่น ทำสำเนา, ถอดรหัส, การตรวจสอบการเข้าถึงข้อมูล, ยึดอายัด ตามมาตรา ๑๘ มาตรา ๑๙ แห่ง พระราชบัญญัติ

มาตรา ๒๐ บรรดาระเบียบหรือประกาศที่ออกตามพระราชบัญญัติว่าด้วยการกระทำ ความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ที่ใช้บังคับอยู่ในวันก่อนวันที่พระราชบัญญัตินี้ใช้บังคับ ให้ยังคงใช้บังคับต่อไปเท่าที่ไม่ขัดหรือแย้งกับบทบัญญัติแห่งพระราชบัญญัตินี้ว่าด้วยการกระทำ ความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัตินี้ จนกว่าจะมีระเบียบหรือประกาศที่ต้องออกตามพระราชบัญญัติว่าด้วยการกระทำ ความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัตินี้ ใช้บังคับ

การดำเนินการออกระเบียบหรือประกาศตามวรรคหนึ่ง ให้ดำเนินการให้แล้วเสร็จ **ภายในหกสิบวัน** นับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ หากไม่สามารถดำเนินการได้ให้ รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรายงานเหตุผลที่ไม่อาจ ดำเนินการได้ต่อคณะรัฐมนตรีเพื่อทราบ

สรุปประเด็นในการเพิ่มเติมแก้ไข พ.ร.บ.คอมพิวเตอร์ฯ

	พ.ร.บ.คอมพิวเตอร์ฯ พ.ศ.๒๕๕๐	พ.ร.บ.คอมพิวเตอร์ฯ (ฉบับที่ ๒) พ.ศ.๒๕๖๐
ความผิดฐาน ส่งสแปมโดยปกปิด แหล่งที่มา	ส่งสแปม โดยปกปิด/ปลอมแปลง โทษปรับเป็น ๑๐๐,๐๐๐ บาท	ส่งสแปม ถ้าไม่เปิดช่องให้บอกเลิก เพิ่มโทษปรับสองเท่า มีประกาศกำหนดลักษณะ วิธีส่ง ซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนเปิดช่องให้บอกเลิกได้
ความผิด ต่อระบบความมั่นคง	ไม่มีโทษเฉพาะ	เพิ่มโทษการเจาะระบบการทำลายระบบ ที่เกี่ยวกับความมั่นคงของประเทศ
การนำเข้าข้อมูลเท็จ ตามมาตรา ๑๔(๑)	ตีความเอาผิดกับ การหมิ่นประมาทออนไลน์	มุ่งเอาผิดการกระทำโดยทุจริต/หลอกลวง นำเข้าระบบคอมพิวเตอร์ซึ่งข้อมูลที่บิดเบือน/ปลอม อันมิใช่การทำความผิดฐานหมิ่นประมาทตาม กม.อาญา
การนำเข้าข้อมูลเท็จ ที่กระทบต่อความมั่นคง	เอาผิดกับการนำเข้า ข้อมูลเท็จที่น่าจะ.... ๑)เสียหายต่อความมั่นคงของประเทศ ๒)ก่อให้เกิดความตื่นตระหนกแก่ ประชาชน	เอาผิดกับการนำเข้า ข้อมูลเท็จที่น่าจะ.... ๑)เสียหายต่อความมั่นคงของประเทศ ๒)เสียหายต่อความปลอดภัยสาธารณะ ๓)เสียหายต่อความมั่นคงทางเศรษฐกิจ ๔)ก่อให้เกิดความตื่นตระหนกแก่ประชาชน
ผู้ให้บริการที่ไม่ลบ เนื้อหาผิดกฎหมาย	รับผิดชอบเมื่อ จงใจสนับสนุนหรือยินยอม	รับผิดชอบเมื่อให้ความร่วมมือ ยินยอม หรือรู้เห็นเป็นใจ ถ้าได้รับแจ้งเตือนแล้วลบออกไม่ต้องรับโทษ

สรุปประเด็นในการเพิ่มเติมแก้ไข พ.ร.บ.คอมพิวเตอร์ฯ

	พ.ร.บ.คอมพิวเตอร์ฯ พ.ศ.๒๕๕๐	พ.ร.บ.คอมพิวเตอร์ฯ (ฉบับที่ ๒) พ.ศ.๒๕๖๐
การเผยแพร่ ภาพตัดต่อ	ผิดเฉพาะ ภาพคนที่มีชีวิต	ภาพคนตาย ก็อาจผิดได้ โทษจำคุก ๓ ปี และปรับ ๒๐๐,๐๐๐ บาท
ให้ทำลายภาพตัดต่อ	ไม่มี	ให้ยึดและทำลายภาพตัดต่อได้ เพื่อบรรเทาความเสียหาย
เนื้อหาที่จะถูกBlock	<ul style="list-style-type: none"> ๑) เป็นความผิดต่อความมั่นคงของประเทศ ๒) เป็นความผิดเกี่ยวกับการก่อการร้าย ๓) ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดี 	<ul style="list-style-type: none"> ๑) เป็นความผิดตาม พรบ.คอมพิวเตอร์ฯ ทุกประเภท ๒) เป็นความผิดต่อความมั่นคงของประเทศ ๓) เป็นความผิดเกี่ยวกับการก่อการร้าย ๔) เป็นความผิดอาญาตามกฎหมาย. เกี่ยวกับทรัพย์สินทางปัญญา ๕) เป็นความผิดต่อกฎหมายอื่น ที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดี
คณะกรรมการ ตามกฎหมาย	ไม่มี	มีคณะกรรมการ ๑) คณะกรรมการเปรียบเทียบปรับ สำหรับ ความผิดที่มีแต่โทษปรับหรือโทษจำคุกไม่เกิน ๒ ปี ๒) คณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์ ที่ไม่ผิดกฎหมายแต่ให้บล็อกได้
ผู้ให้บริการ มีหน้าที่เก็บข้อมูล การใช้งาน	เก็บไว้ไม่น้อยกว่า ๙๐ วัน กรณีจำเป็น สั่งให้เก็บเพิ่มได้ไม่เกิน ๑ ปี	เก็บไว้ไม่น้อยกว่า ๙๐ วัน กรณีจำเป็น สั่งให้เก็บเพิ่มได้ไม่เกิน ๒ ปีเป็นกรณีพิเศษ
เงินพิเศษ สำหรับพนักงานเจ้าหน้าที่	ไม่มี	มีเงินเพิ่ม สำหรับผู้ดำรงตำแหน่งที่มีเหตุพิเศษ

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ

ผลกระทบจากการบังคับใช้ พ.ร.บ.

ภาระ
ผู้ให้บริการ

ผลกระทบที่อาจต้องแบกรับ
มาตรา ๒๖ และ ๒๗

สิทธิของ
ประชาชน

Private Interests & ข้อจำกัด / รั้งมัดระวัง
ในการใช้สิทธิมาตรา ๑๒, ๑๔, ๑๖ และ ๒๐

โครงสร้างพื้นฐานสำคัญ
ของประเทศ

ประโยชน์มหาชน / สาธารณะ
Public Interests

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ

ผลจากการบังคับใช้ พ.ร.บ.

สรุปยังคงมีการกระทำความผิดที่ไม่ลดลง สาเหตุ มีการใช้หลากหลาย การติดต่อทำได้รวดเร็ว มีการแข่งขันของผู้ประกอบการสูง

- ยังคงมีการระงับการเผยแพร่เนื้อหาหรือการปิดกั้นเว็บไซต์โดยอาศัยมาตรา ๒๐ ของพ.ร.บ.

- คดีที่มีเนื้อหาความผิดเกี่ยวเนื่องกับการหมิ่นประมาทต่อบุคคลมีสัดส่วนมากที่สุด ในคดีที่ถูกฟ้องตาม พ.ร.บ.ฯ

รองลงมาได้แก่ คดีที่เป็นอาชญากรรมคอมพิวเตอร์โดยแท้ (เช่น การเจาะข้อมูล การส่งสแปม) อันดับที่ ๓ คดีที่มีเนื้อหาความผิดเกี่ยวเนื่องกับการหมิ่นประมาทกษัตริย์ พระราชินี และรัชทายาท

อันดับที่ ๔ มีสองประเภท คือ คดีที่เกี่ยวข้องกับการฉ้อโกง เช่น โปสต์ข้อความหลอกลวงขายของ และคดีที่เกี่ยวข้องกับเนื้อหาลามก ที่เหลือส่วนน้อยเป็นคดีที่เกี่ยวข้องกับการขายโปรแกรม คดีที่เกี่ยวข้องกับความมั่นคง และคดีอื่นๆ

ความตระหนักถึงความมั่นคงปลอดภัยด้านสารสนเทศ

การใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

หน่วยงานมีระบบงานสารสนเทศ และเครือข่ายที่สามารถเชื่อมต่ออินเทอร์เน็ต ทั้งภายในหน่วยงานเอง(Intranet) และการเชื่อมต่อไปยังภายนอกองค์กร(Internet)

๑.ผู้เกี่ยวข้องในการให้บริการ

๒.ผู้ใช้บริการ

๓.การใช้งาน ระบบงาน/การสื่อสารเชื่อมต่อ

๔.ภัยคุกคามที่อาจเกิดขึ้น แนวทางป้องกันหรือการสร้างความปลอดภัยที่พึงระวังไว้ /การปฏิบัติตามข้อปฏิบัติ หรือกฎหมายที่เกี่ยวข้อง

๕. การบริหารจัดการเพื่อแก้ไขปัญหา การควบคุม เช่นการเข้าถึง การใช้งาน เช่นเครื่องคอมพิวเตอร์ส่วนบุคคล การควบคุมการส่งข้อมูลข่าวสาร/จดหมาย อิเล็กทรอนิกส์

การใช้เทคโนโลยีสารสนเทศ หมายถึง กระบวนการต่างๆ และระบบงานที่ช่วยให้ได้สารสนเทศหรือข่าวสารที่ต้องการ โดยจะรวมถึง

๑. เครื่องมือและอุปกรณ์ต่างๆ หมายถึง เครื่องคอมพิวเตอร์ เครื่องใช้สำนักงาน อุปกรณ์คมนาคมต่างๆ รวมทั้งซอฟต์แวร์ทั้งระบบสำเร็จรูปและพัฒนาขึ้นโดยเฉพาะด้าน

๒. กระบวนการในการนำอุปกรณ์เครื่องมือต่างๆ ข้างต้นมาใช้งาน รวบรวมข้อมูล จัดเก็บประมวลผล และแสดงผลลัพธ์เป็นสารสนเทศในรูปแบบต่างๆ ที่สามารถนำไปใช้ประโยชน์ได้ต่อไป

ในปัจจุบันการใช้งานเทคโนโลยีสารสนเทศเป็นสิ่งจำเป็นสำหรับทุกองค์กร การเชื่อมโยงสารสนเทศผ่านทางคอมพิวเตอร์ ทำให้สิ่งที่มีค่ามากที่สุดของระบบ คือ ข้อมูลและสารสนเทศ อาจถูกจารกรรม ถูกปรับเปลี่ยน ถูกเข้าถึงโดยเจ้าของไม่รู้ตัว ถูกปิดกั้นขัดขวางให้ไม่สามารถเข้าถึงข้อมูลได้ หรือถูกทำลายเสียหายไป ซึ่งสามารถเกิดขึ้นได้ไม่ยากบนโลกของเครือข่าย โดยเฉพาะเมื่ออยู่บนอินเทอร์เน็ต

ปัจจุบันมีกฎหมายที่เกี่ยวข้องด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสาร

๑. กฎหมายเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (Computer Crime Law) เพื่อกำหนดมาตรการทางอาญาในการลงโทษผู้กระทำความผิดต่อระบบการทำงานของคอมพิวเตอร์ ระบบข้อมูล และระบบเครือข่าย ทั้งนี้เพื่อเป็นหลักประกันสิทธิเสรีภาพ และการคุ้มครองการอยู่ร่วมกันของสังคม



๒. กฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ (Electronic Transactions Law) เพื่อรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ให้เสมอด้วยกระดาษ อันเป็นการรองรับนิติสัมพันธ์ต่าง ๆ ซึ่งแต่เดิมอาจจะจัดทำขึ้นในรูปแบบของหนังสือ ให้เท่าเทียมกับนิติสัมพันธ์รูปแบบใหม่ที่จัดทำขึ้นให้อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์

ปัจจุบันมีกฎหมายที่เกี่ยวข้องด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสาร(ต่อ)

๓. กฎหมายอื่น ๆที่เกี่ยวข้อง เช่น

๓.๑ กฎหมายลิขสิทธิ์(มีผลบังคับใช้ ๔ สิงหาคม ๒๕๕๘ นี้ มีความเข้มข้นด้านเทคโนโลยีมากขึ้นกว่าเดิม)

๓.๒ กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Law)

๓.๓ กฎหมายคุ้มครองผู้บริโภค

๓.๓ อื่น ๆ ที่กำลังมีการพิจารณากันอยู่ เช่น กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

บรรดากฎหมายใด ๆ ที่ได้ประกาศใช้ในประเทศไทย ถือเป็นสิ่งสำคัญที่ผู้ใช้งานคอมพิวเตอร์จะต้องตระหนักและปฏิบัติตามอย่างเคร่งครัด และไม่กระทำความผิดนั้น ดังนั้น หากผู้ใช้งานคอมพิวเตอร์กระทำความผิดตามกฎหมายดังกล่าว องค์การถือว่าความผิดนั้นเป็นความผิดส่วนบุคคล

ต้องรับทราบ ทำความเข้าใจ และปฏิบัติตามรายการของนโยบาย กฎระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและ การสื่อสารที่กำหนดขึ้นอย่างเคร่งครัด

ตัวอย่าง เช่น การปฏิบัติตามข้อบังคับด้านกฎหมาย ประกอบด้วย กฎหมายที่เกี่ยวข้อง กฎหมาย ระเบียบข้อบังคับที่เกี่ยวข้อง → พรบ.ว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐, พรบ.ธุรกรรมอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔, นโยบายการรักษาความมั่นคงปลอดภัย, นโยบายในการคุ้มครองข้อมูลส่วนบุคคล, พรบ.ลิขสิทธิ์

แนวทาง/มาตรการที่จะต้องกำหนดให้ปฏิบัติตามข้อกำหนด

ประเภท	แนวปฏิบัติ
ผู้ให้บริการโดยทั่วไป	ผู้ใช้งานอินเทอร์เน็ตต้องทำความเข้าใจและปฏิบัติให้อยู่ในกรอบของกฎหมาย หากฝ่าฝืนอาจถูกดำเนินคดี
องค์กร/หน่วยงาน	ควรให้ความสำคัญ ในประเด็น ดังนี้ ๑. การเข้าถึงหรือควบคุมการใช้งานเครื่องคอมพิวเตอร์และระบบสารสนเทศ - จัดทำนโยบายการควบคุมการเข้าถึงสารสนเทศเป็นลายลักษณ์อักษร ๒. จัดให้มีการสำรองข้อมูลสารสนเทศที่สำคัญอย่างสม่ำเสมอ เพื่อให้อยู่ในสภาพพร้อมการใช้งาน - กำหนดหน้าที่และความรับผิดชอบของบุคลากรที่เกี่ยวข้องกับการดำเนินการจัดทำแผน มีการเตรียมพร้อม ๓. การปฏิบัติตามข้อบังคับของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฯ - กำหนดมาตรการป้องกันระบบคอมพิวเตอร์สำหรับจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ - จัดให้มีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ตามอุปกรณ์ที่เกี่ยวข้องกับการใช้งาน

ในกรณีเกิดการกระทำความผิดขึ้นในองค์กร : ควรมีผังกระบวนการแสดงขั้นตอนการปฏิบัติเมื่อเกิดเหตุการณ์ พร้อมทั้งระบุผู้รับผิดชอบในการปฏิบัติในแต่ละขั้นตอนเป็นเฉพาะกรณีไป เช่นการคุกคามจากผู้ไม่ประสงค์ดีเข้าเปลี่ยนแปลงหน้าเว็บไซต์ขององค์กร โดยกรณีเช่นนี้ การวิเคราะห์และการประเมินเหตุการณ์ การปฏิบัติงานเพื่อแก้ไขปัญหา ก็จะสามารถดำเนินการได้ทันต่อสถานการณ์ ในเมื่อมีความพร้อมและกระบวนการที่ชัดเจน

สร้างความตระหนักถึงความปลอดภัย

๑. อย่า...เข้าระบบที่คนอื่นตั้ง password ไว้

๒. อย่า...เอามาตรการป้องกันการแก้ไข password ที่คนอื่นตั้งไว้ไปเผยแพร่

๓. อย่า...เข้าไปดูหรือเข้าไปเอาข้อมูลของผู้อื่นที่มีมาตรการรักษาความปลอดภัย

๔. อย่า...ใช้ sniffer ดัก e-mail คนอื่น

๕. อย่า...ลองวิชาด้วยการรบกวนระบบคอมพิวเตอร์หรือข้อมูลผู้อื่น

๖. อย่า...สร้างเมลเท็จเพื่อให้ผู้อื่นแตกตื่นตกใจ

๗. อย่า...รื้อนวิชาด้วยการรบกวนระบบโครงสร้างสำคัญของประเทศ

๘. อย่า...เผยแพร่เน็ตที่เป็นภาพลามกหรือเป็นภัยต่อความมั่นคงของประเทศ

๙. อย่า...ตัดต่อภาพเพื่อให้ผู้อื่นอับอาย / เสียชื่อเสียง/ถูกเกลียดชัง

๑๐. อย่า...เผยแพร่โปรแกรมสำหรับใช้กระทำความผิด

การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ เช่นการเจาะระบบทั้งแบบ Hacking Cracking การบุกรุกทางคอมพิวเตอร์ เพื่อทำลายระบบคอมพิวเตอร์ หรือการเปลี่ยนแปลงแก้ไข หรือเข้าถึงข้อมูลที่ได้มีการเก็บรักษาเป็นความลับ เช่น รหัสผ่าน หรือความลับทางการค้าที่อาจจะเป็นที่มาของการใช้คอมพิวเตอร์เพื่อฉ้อโกง/หลอกลวง

ความปลอดภัยและความเป็นส่วนตัว ในการใช้คอมพิวเตอร์และอินเทอร์เน็ต

ความปลอดภัย

- การดูแลจัดการ ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูล ให้พ้นจากอันตรายต่าง ๆ เช่น อาชญากรรมคอมพิวเตอร์ ภัยธรรมชาติ ภัยคุกคามอื่นๆ

ความเป็นส่วนตัว

- การปกป้องข้อมูลส่วนตัวที่ไม่ต้องการเปิดเผยของผู้ใช้

การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้ใช้งานทั่วไป

ความปลอดภัยและความเป็นส่วนตัวบนอินเทอร์เน็ต

๑. เพื่อสร้างความปลอดภัยในการใช้อินเทอร์เน็ต

- ๑). อย่าให้รหัสลับแก่ผู้อื่น
- ๒). ต้องคิดให้ดีทุกครั้ง ที่ให้ข้อมูลส่วนตัวกับบุคคลอื่นในอินเทอร์เน็ต
- ๓). ตรวจสอบว่าได้พิมพ์ชื่อเว็บไซต์ถูกต้องเสียก่อน แล้วจึงกด Enter เพื่อจะได้เข้าเว็บไซต์ที่ต้องการได้ถูกต้อง
- ๔). ถ้าพบเห็นข้อความ หรือสิ่งใด ที่ไม่เหมาะสม หรือ คิดว่าไม่ดีต่อการใช้งานอินเทอร์เน็ต ควรออกจากเว็บไซต์นั้น
- ๕). อย่าส่งรูปภาพของตนเอง หรือรูปภาพของผู้อื่น ให้คนอื่นทางอีเมล
- ๖). ถ้าได้รับอีเมลที่มีข้อความไม่เหมาะสม หรือทำให้ไม่สบายใจ ไม่ควรโต้ตอบ
- ๗). บนอินเทอร์เน็ต ทุกอย่างที่คุณเห็นไม่ใช่เรื่องจริงเสมอไป
- ๘). อย่าบอกวันเดือนปีเกิด หรือ อายุจริงของคุณกับคนอื่น
- ๙). อย่าบอกชื่อจริง และนามสกุลจริงกับบุคคลอื่น
- ๑๐). อย่าบอกที่อยู่ ของคุณกับบุคคลอื่น
- ๑๑). อย่าบอกเบอร์โทรศัพท์ของคุณกับบุคคลอื่น ในอินเทอร์เน็ต

การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้ใช้งานทั่วไป

ความปลอดภัยและความเป็นส่วนตัวบนอินเทอร์เน็ต

๒. การป้องกัน : การใช้งานอินเทอร์เน็ตอย่างปลอดภัย

- อ่านข้อตกลง นโยบายให้ดีก่อนตอบตกลงใด ๆ
- ระมัดระวังการใช้บริการเครื่องคอมพิวเตอร์สาธารณะ
 - ๑) แอบดูการใช้งาน
 - ๒) หลีกเลี่ยงการใส่ข้อมูลสำคัญมาก ๆ
 - ๓) ไม่ให้ระบบช่วยจำ username และ password
- หมั่นลบ temporary internet files, cookies และ history
- Logoff หรือ logout ทุกครั้งหลังใช้งาน
- ไม่ใช้ Password ที่คาดเดาได้ง่าย เช่น คำที่มีใน Dictionary
- ใช้การผสมอักขระที่ซับซ้อน
- เปลี่ยน Password อย่างสม่ำเสมอ เมื่อถึงเวลาที่เหมาะสม เช่น ทุกๆ ๙๐ วัน
- ตั้ง Password ซึ่งผสมอักขระภาษาอังกฤษตัวเล็ก อักขระภาษาอังกฤษตัวใหญ่ ตัวเล็ก และตัวอักขระพิเศษ

๓. การป้องกันภัยคุกคาม ที่เกี่ยวกับการทำธุรกรรม

การป้องกันการใช้เครือข่ายสาธารณะ/Free WiFi

๑. ใช้เครือข่าย WiFi ที่เชื่อถือได้เท่านั้น
๒. ดูชื่อจุดเชื่อมต่อ
๓. หลบชื่อจุดเชื่อมต่อที่ไม่ได้ใช้จากรายการ
๔. เลือกการเชื่อมต่อ ที่ต้องเข้ารหัส (WPA๒.WPAและ WEP)
๕. อย่าแชร์ไฟล์และโฟลเดอร์
๖. เปิดไฟร์วอลล์ส่วนบุคคล

วิธีป้องกันภัยออนไลน์ เช่น ภัยจากมัลแวร์

วิธีที่มัลแวร์เข้าสู่คอมพิวเตอร์ของคุณ

๑. การดาวน์โหลดซอฟต์แวร์จากอินเทอร์เน็ตที่มีมัลแวร์แฝงอยู่
๒. การดาวน์โหลดซอฟต์แวร์ที่ถูกกฎหมายที่แอบมีมัลแวร์ผูกติดมา
๓. การเข้าชมเว็บไซต์ที่ติดเชื่อมัลแวร์
 - การคลิกข้อความแสดงข้อผิดพลาด/หน้าต่างป๊อปอัพ
 - การเปิดไฟล์แนบอีเมลที่มีมัลแวร์

หลักการการป้องกันมัลแวร์

๑. อัปเดตคอมพิวเตอร์และซอฟต์แวร์ของคุณอยู่เสมอ
๒. คิดให้ดีก่อนจะคลิกลิงค์หรือดาวน์โหลดอะไรก็ตาม
๓. คิดก่อนเปิดไฟล์แนบอีเมลหรือรูปภาพ
๔. อย่าเชื่อหน้าต่างป๊อปอัพที่ขอให้ดาวน์โหลดซอฟต์แวร์
๕. ให้ระมัดระวังเรื่องการแบ่งปันไฟล์
๖. การป้องกันโดยใช้ซอฟต์แวร์ป้องกันไวรัส

สิ่งที่ไม่ควรทำบนเครือข่ายสังคมออนไลน์

๑. ไม่โพสต์กิจกรรมที่ผิดกฎหมาย
๒. ไม่ควรโพสต์ข้อความ ที่ชี้ชวนให้มิจฉาชีพรู้ความเคลื่อนไหวส่วนตัว
๓. โพสต์ข้อมูลที่เป็นเรื่องส่วนบุคคล
๔. ให้ระมัดระวังการเช็คอิน (Check-in) ผ่านสื่อสังคมออนไลน์
๕. ไม่ระบุชื่อบุตรหลาน ระบุภาพหรือติด tag ในรูปภาพมากเกินไป
๖. ไม่ส่งหลักฐานส่วนตัวของตนเองและคนในครอบครัวให้ผู้อื่น
๗. พึงระมัดระวังอย่างยิ่งที่จะไว้ใจหรือเชื่อใจคน ที่รู้จักผ่านอินเทอร์เน็ต

เล่น Social Network ให้ปลอดภัย อย่างไร

เล่น **Social Network**
ให้ปลอดภัย “รู้” ไว้เสี่ยงอันตราย



etda.thailand



ThaiCERT



thaicert.or.th



คิดให้รอบ

สักนิดก่อนโพสต์
เพราะมันเปิดเผยและทุกคนเข้าถึงได้ง่าย
การโพสต์ข้อมูลที่สุ่มเสี่ยงอาจเป็นภัยต่อตัวเอง



ระมัดระวัง

ในการคลิกลิงก์
ที่มากับการแชร์ เพราะอาจนำไปสู่ไวรัส
หรือช่องทางขโมยข้อมูลของเราแอกเกอร์



พิมพ์ URL โดยตรง

เสี่ยงคลิกลิงก์ เพราะอาจเป็น URL ปลอมหลอกเอาบัญชีใช้งานของเรา
เช่น facebook.com อาจมี URL หลอกเป็น faebook.com



รอบคอบ

ก่อนตอบรับเป็นเพื่อน
คัดกรองคนที่ขอเป็นเพื่อนโดยเข้าไปดูโปรไฟล์ก่อนทุกครั้ง
เพราะอาจมีผู้ไม่หวังดีแฝงมาด้วย



ตั้งค่า

ความเป็นส่วนตัว
หลีกเลี่ยงตั้งค่าแบบสาธารณะ
และอนุญาตให้เพื่อนเท่านั้นที่เห็นกิจกรรมของเราได้



ไม่แสดงข้อมูล

ส่วนตัวที่เป็นความลับ
เช่น บัตรประชาชน บัตรเครดิต
ไม่ว่าจะอยู่ในรูปแบบข้อความหรือรูปภาพก็ตาม



Do Not Track

เปิดใช้งาน
ป้องกันการติดตามและเก็บข้อมูลจากผู้ให้บริการโซเชียลเน็ตเวิร์ก
รวมถึงผู้ไม่หวังดีที่เข้ามาขโมยข้อมูล



ใช้วิจารณญาณ

ในการรับข่าวสาร
อย่าปักใจเชื่อทันที อาจมีการสร้างกระแส สวมรอย สมอ้างจากผู้ไม่หวังดี



ควบคุมการใช้งาน

ของบุตรหลาน
มองหาเครื่องมือมาเป็นตัวช่วย เช่น Windows Live Family Safety



ตระหนักว่าเป็น สังคมเสรี

แม้ทุกคนมีสิทธิ์ในการแสดงความคิดเห็น
แต่การกระทำที่ไม่เหมาะสมก็เป็นเหตุให้ถูกฟ้องร้อง
และศาลก็อาจรับฟังคำร้องด้วย



การรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับองค์กร/ผู้ดูแลระบบ

“ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายความว่า

การดำรงไว้ซึ่งความลับ(Confidentiality) ความถูกต้อง (Integrity) และสภาพพร้อมใช้งาน (Availability)ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธ ความรับผิดชอบ (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

“การรักษาความมั่นคงปลอดภัยของข้อมูล (Data security)” หมายถึง การป้องกันข้อมูลในบริบทของ การรักษาความลับ บุรณภาพ และความพร้อมใช้งานของข้อมูล ซึ่งสามารถใช้แทน การรักษาความมั่นคงปลอดภัยของสารสนเทศได้

“การปกป้องข้อมูล (Data protection)” หมายถึงการป้องกันข้อมูลส่วนบุคคลต่อการประสงคร้ายของบุคคลที่สาม

“เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายถึง การเกิดเหตุการณ์ หรือสภาพของบริการที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

การควบคุมโดยการออกระเบียบหรือแนวทางปฏิบัติ

๑. มีการประกาศใช้ แผนนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยขององค์กร
การนำแผนนโยบายไปปฏิบัติ ออกมาเช่น การรักษาความมั่นคงปลอดภัย
มีแนวทางการป้องกันทางด้านไซเบอร์ สร้างขั้นตอนปฏิบัติ

๒. การจัดองค์กร และการรักษาความปลอดภัยสำหรับระบบสารสนเทศ

๒.๑.การจัดองค์การการวางโครงสร้างขององค์กรที่สามารถเ้าอำนาจ
ให้แผนงานที่จัดทำขึ้นไปสู่สัมฤทธิ์ผล โดยกำหนดอำนาจหน้าที่และความรับผิดชอบ
ของกลุ่มบุคคลในองค์กร เพื่อให้งานเป็นไปอย่างรวดเร็วและมีประสิทธิภาพ

๒.๒. การพัฒนาระบบงานควบคุมดูแลและปฏิบัติงานที่เกี่ยวกับเรื่อง
ความมั่นคงปลอดภัย และการใช้งาน/เครื่องมืออุปกรณ์

พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์
ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานต้องจัดทำแผนนโยบายและแนวปฏิบัติใน
การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ตัวอย่างการสร้างความปลอดภัยของข้อมูล

- ๑.แผนการป้องกันข้อมูล
- ๒.การโจรกรรมข้อมูล
- ๓.การเข้าถึงข้อมูลเฉพาะผู้มีสิทธิ
- ๔.การป้องกันความเสียหาย
- ๕.การสำรองข้อมูล

การป้องกัน

๑. การระบุตัวผู้ใช้และการเข้าถึงข้อมูล

- การใช้รหัสผ่าน
- การระบุผู้ใช้โดยใช้ลักษณะทางพันธุกรรม :
ลายนิ้วมือ ลายมือ ใบหน้า ม่านตา
- การใช้ลายเซ็น เสียงพูด
- การบัตรผ่าน
- การปฏิบัติตน

การป้องกัน

- การทำลายข้อมูลทิ้ง
- การควบคุมภายใน (log file)
- การตรวจเช็คจากผู้ตรวจสอบ
- การฝึกซ้อมพร้อมรับกับเหตุการณ์
- โปรแกรมป้องกัน

ผู้ที่ได้รับผลกระทบจากการบังคับใช้กฎหมาย : กรณีเป็นผู้เสียหาย

ขั้นตอนการแจ้งความร้องทุกข์ในคดี ตาม พรบ. คอมพิวเตอร์

๑. เมื่อพบการกระทำความผิดหรือถูกละเมิดในสื่ออินเทอร์เน็ต

ควรดำเนินการเบื้องต้น ดังนี้

- ๑.๑ ทำการบันทึกข้อมูลหลักฐานที่ปรากฏไว้ทั้งหมด เช่น หน้าเว็บเพจ ,ข้อความหรือภาพถ่ายที่ก่อให้เกิดความเสียหาย
- ๑.๒ พิมพ์ข้อมูลหน้าเว็บไซต์ที่เกิดเหตุหรือเกี่ยวข้อออกมาเป็นเอกสาร เพื่อป้องกันไม่ให้พยานหลักฐานสูญหาย หรือถูกทำลาย และลงลายมือชื่อรับรองเอกสารนั้น
- ๑.๓ การส่งพิมพ์เอกสารหน้าเว็บเพจ ,ข้อความหรือภาพถ่ายต่างๆ ในเว็บไซต์ที่พบการกระทำความผิด ให้ปรากฏที่ตั้งของเว็บไซต์ หรือ URL ของเว็บไซต์นั้นด้วย และหรือปรากฏวันเวลาบนเว็บไซต์หรือขณะบันทึกข้อมูลหลักฐานนั้นด้วย

ขั้นตอนการแจ้งความร้องทุกข์ในคดี ตาม พรบ. คอมพิวเตอร์

๒. หากประสงค์แจ้งความร้องทุกข์ ให้ผู้ที่ได้รับความเสียหายสามารถแจ้งต่อพนักงานสอบสวนสถานีตำรวจท้องที่เกิดเหตุ หรือที่พบการกระทำความผิด หลักฐานที่ควรนำไปมอบให้พนักงานสอบสวน ได้แก่หลักฐานตามข้อ ๑.๑ - ๑.๓
๓. หากผู้เสียหาย หรือพนักงานสอบสวนที่รับแจ้งความ ต้องการตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์ ก็สามารถประสานเพื่อส่งข้อมูล หลักฐานต่างๆ ตามข้อ ๑. มายัง บก.ปอท. หรือหน่วยงานที่เกี่ยวข้องอื่นๆ เช่น กระทรวง ไอซีที เพื่อตรวจสอบข้อมูลให้ต่อไป
๔. กรณีจำเป็นเร่งด่วนเพื่อป้องกันความเสียหาย เช่น ต้องทำการปิดกั้นเว็บไซต์ หรือระงับการทำธุรกรรมทางอิเล็กทรอนิกส์ ให้พนักงานสอบสวนที่รับแจ้งความ หรือผู้เสียหายประสานงานมายัง บก.ปอท. หรือ กระทรวงไอซีที หรือธนาคาร หรือผู้ให้บริการอินเทอร์เน็ตเพื่อดำเนินการเบื้องต้นในการบรรเทาความเสียหาย ต่อไป

ผังแสดงขั้นตอนการปฏิบัติในการสืบสวนความผิด กรณีตามมาตรา ๑๔

สืบค้นข้อมูลเว็บไซต์

ตรวจสอบข้อมูลบนเว็บไซต์เพื่อสืบหาข้อมูล
ดังนี้

- หมายเลขโทรศัพท์ของผู้โพสต์
- อีเมลของผู้โพสต์
- ข้อมูลอื่น ที่เป็นประโยชน์ต่อการสืบสวน

-นำหมายเลขโทรศัพท์ไปตรวจสอบเพื่อ
หาว่าเป็นผู้ให้บริการรายใด(เช่นใช้
ค้นหาโดย www.checkber.com หรือใช้
www.webdoober.com

-สืบค้นหมายเลข IP Address เช่นหาได้
จาก e-mail header

-นำข้อมูลที่ได้ไปค้นเพิ่มเติม โดยใช้
search engine เช่น google

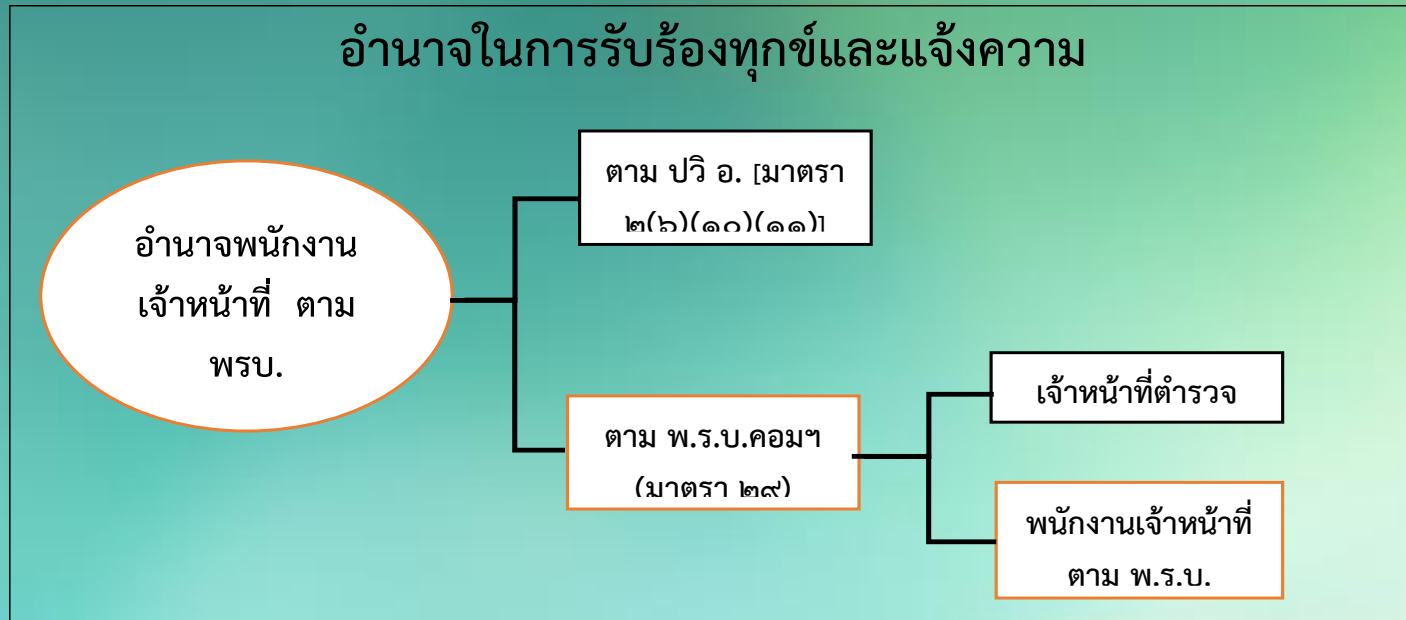
-และหากได้หมายเลข IP Address ให้ทำ
การตรวจสอบข้อมูล IP เช่นใช้
domaintools.com

-ทำการบันทึกพยานหลักฐานที่ค้นมาได้
ทุกครั้ง เช่น บันทึกด้วยวิธีการ Save หน้า
เว็บ บันทึกด้วยการ print screen หรือใช้
โปรแกรมดูเว็บ เช่น web spider, Teleport
pro

-การประสานเพื่อให้ได้มาซึ่งข้อมูล เช่น
ISP, ผู้ให้บริการโทรศัพท์, ผู้ดูแลเว็บไซต์และ
-พนักงานเจ้าหน้าที่ ตาม พรบ. ติดต่อเพื่อ
ขอข้อมูลจากผู้ให้บริการอินเทอร์เน็ต

-ดำเนินการสืบค้นข้อมูลด้านอื่น ๆ
ประกอบ ถ้าจำเป็นก็ต้องดำเนินการเข้าค้น
สถานที่ต้องสงสัย ใช้หลักปฏิบัติทางนิติ
คอมพิวเตอร์

อำนาจในการรับร้องทุกข์และแจ้งความ



ประเด็น : การรับฟังพยานหลักฐานทางอิเล็กทรอนิกส์ของกระบวนการยุติธรรม

การพิจารณาว่าพยานหลักฐาน ที่ต้องพิจารณาเพื่อใช้ในการยืนยันความแท้จริงของเอกสาร ประกอบด้วย

๑. เนื้อหาของเอกสารไม่ได้ถูกเปลี่ยนแปลง
๒. ข้อมูลในเอกสารเป็นไปตามเจตนาที่แท้จริงของผู้สร้างเอกสารนั้น ไม่ว่าจะสร้างจะเป็นมนุษย์หรือคอมพิวเตอร์ก็ตาม
๓. ข้อมูลพิเศษในเอกสาร อันได้แก่ วันเดือนปี ที่ถูกสร้างจะต้องถูกต้อง

การสอบถามข้อมูล : กรณีต้องการทราบรายละเอียดเพิ่มเติม/กรณีเป็นผู้เสียหาย

๑. หากต้องการศึกษาข้อมูลและรายละเอียดเพิ่มเติมสามารถติดต่อได้ที่ไหน และมีหน่วยงานใดบ้างที่คุณแลรับผิดชอบ

สามารถศึกษาข้อมูลเพิ่มเติมเกี่ยวกับพ.ร.บ.นี้ได้จากเว็บไซต์ของหลากหลายหน่วยงานที่มีส่วนเกี่ยวข้องและรับผิดชอบ อาทิ

๑.๑ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม <http://www.mict.go.th/>
สอบถามข้อมูล /แจ้งข้อมูลเว็บไซต์ที่ไม่เหมาะสม

๑.๒ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี(ปอท.) <http://www.tcsd.in.th/> แจ้งความดำเนินคดี

๑.๓ ความรู้ด้านภัยร้ายจากอินเทอร์เน็ต www.catcyfence.com

ขอบคุณครับ