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 เนื่องจากข้อกฎหมายหลายประเด็นมีการระบุในเรื่องของเนื้อหาที่กว้างเกินไป การที่มีกฎกระทรวงและกฎหมายลูกเข้ามาใช้ประกอบ จะทำให้การตีความไปจนถึงการบังคับใช้ของกฎหมายมีความละเอียดมากยิ่งขึ้น

ประเด็นต่อต้านและข้อเท็จจริง เกี่ยวกับพ.ร.บ.คอมพ์

1.

ประเด็นต่อต้าน

ให้อำนาจรัฐจัดตั้งซิงเกิล เกตเวย์ และซิงเกิล คอมมานด์ เพื่อสอดแนมข้อมูลประชาชนและทำให้การใช้งานอินเตอร์เน็ตช้าลง

ข้อเท็จริง

พ.ร.บ.คอมพ์ไม่มีมาตราใดที่กำหนดให้ประเทศไทยมีซิงเกิล เกตเวย์ ดังนั้นร่างพ.ร.บ.คอมพ์จึงไม่ได้ให้รัฐเข้าไปสอดแนมหรือล้วงข้อมูลการติดต่อสื่อสารของประชาชน ขณะที่การกระทำดังกล่าวมีความผิดตามมาตรา 8 พ.ร.บ.คอมพิวเตอร์ พ.ศ. 2550

2.

ประเด็นต่อต้าน

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

ข้อเท็จริง

มาตรา 14 ที่แก้ไข ไม่ได้ต้องการปิดกั้นเสรีภาพการแสดงความคิดเห็น ปิดปากการตรวจสอบของประชาชน

3.

ประเด็นต่อต้าน

ร่างประกาศฯภายใต้ร่างพ.ร.บ. ให้อำนาจรัฐจัดตั้งศูนย์กลางบล็อกเว็บ ที่เชื่อมต่อตรงระบบของผู้ให้บริการ

ข้อเท็จริง

ร่างประกาศฯที่ออกภายใต้มาตรา 20 ไม่ได้ให้อำนาจรัฐหรือเจ้าหน้าที่เชื่อมต่อระบบผู้ให้บริการเพื่อปิดเว็บไซต์โดยไม่ได้รับอนุญาตจากศาล ส่วนการจัดตั้งศูนย์กลางตามร่างประกาศฯก็เพื่อให้มีช่องทางในการประสานงานกับผู้ให้บริการและติดตามการดำเนินการตามหมายศาล

4.

ประเด็นต่อต้าน

ต่อไปถ้าเน็ตล่ม คือล่มทั้งประเทศใช่ไหม

ข้อเท็จริง

ประเทศไทยเปิดเสรีในการให้บริการสื่อสารโทรคมนาคมและมีผู้ให้บริการเกตเวย์และอินเตอร์เน็ตหลายรายจึงมีโอกาสน้อยมากที่ผู้ให้บริการทุกรายจะไม่สามารถให้บริการพร้อมกันได้

5.

ประเด็นต่อต้าน

การเข้าถึงเว็บต่างประเทศจะทำได้ยากขึ้น

ข้อเท็จริง

ความรวดเร็วและความสามารถในการเข้าเว็บไซต์ต่างประเทศยังเหมือนเดิม เนื่องจากพ.ร.บ.คอมพ์ไม่ได้ลดจำนวนช่องทางการใช้อินเตอร์เน็ตต่างประเทศ

THAN INFOGRAPHIC

ที่มา : กระทรวงดิจิทัลฯ

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

โครงสร้างของเนื้อหากฎหมายมีลักษณะคล้ายคลึงฉบับเดิม โดยมีสาระสำคัญที่ต่างไปบ้าง

พ.ร.บ. ฉบับเดิม ใช้บังคับเป็นเวลากว่า ๑๐ ปี โดยที่ผ่านมาพบว่ากฎหมายมีปัญหาในการตีความ จน กระทบกับการบังคับใช้ เช่น การนำฐานความผิดที่ใช้กับเรื่องฉ้อโกงปลอมแปลงทางออนไลน์ ไปใช้กับการ หมิ่นประมาท ทำให้กระทบต่อสิทธิเสรีภาพในการแสดงความคิดเห็น จนทำให้เกิดการโจมตีจากประชาคม โลกและเกิดกระแสสังคมเรียกร้องหลักประกันสิทธิเสรีภาพในการแสดงความคิดเห็นขึ้น กอปรกับเพื่อ เป็นการปรับปรุงกฎหมายให้เท่าทันกับเทคโนโลยีและภัยคุกคามที่เปลี่ยนแปลงไป

วัตถุประสงค์/เหตุผลการแก้ไข

(๑) ให้รัฐมนตรีว่าการกระทรวงดิจิทัลฯ รักษาการตามพระราชบัญญัติ

(๒) บทบัญญัติบางประการที่ไม่เหมาะสมต่อการป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในปัจจุบัน ซึ่งมีรูปแบบการกระทำความผิดที่มีความซับซ้อนมากขึ้น เช่นเพิ่มเติมฐานความผิดและกำหนดโทษผู้ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ แก่บุคคลอื่น

(๓)มาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งการเฝ้าระวังและติดตามสถานการณ์ด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศของประเทศ สมควรปรับปรุงบทบัญญัติในส่วนที่เกี่ยวกับผู้รักษากฎหมาย

(๔)กำหนดโทษของความผิดดังกล่าว การปรับปรุงกระบวนการและหลักเกณฑ์ในการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์

ภาพรวม แก้ไขเพิ่มเติมพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

หมวด ๑ ความผิดเกี่ยวกับคอมพิวเตอร์

→ แก้ไขเพิ่มเติม

ม.๑๑ ความผิดฐานส่งสแปมโดยปกปิดแหล่งที่มา

ม.๑๒ เพิ่มโทษการเจาะระบบ การทำลายระบบที่เกี่ยวกับความมั่นคง

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

แต่งตั้งคณะกรรมการกลั่นกรองพิจารณาการปิดกั้น

→ หน้าที่ของผู้ให้บริการ มาตรา ๒๖

เก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน แต่ไม่เกิน ๒ ปี เป็นกรณีพิเศษเฉพาะราย/เฉพาะคราว

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

มาตรา ๑๑ กำหนดให้ชัดเจนวาอะไรคือ สแปม หรือจดหมายอิเล็กทรอนิกส ที่ทำให้เดือดรอนรำคาญ	ประกาศ เรื่อง หลักเกณฑ์เกี่ยวกับลักษณะและวิธีการสง ลักษณะ และปริมาณของขอมูลคอมพิวเตอร ซึ่งไมเปนการกอให้เกิดความเดือดรอนรำคาญแกผูรับ และลักษณะอันเปนการปฏิเสธการตอบรับไดโดยงาย พ.ศ. ..
มาตรา ๑๕ เมื่อผูให้บริการจำเปนตองระงับการเผยแพรเว็บไซต และยกเวนโทษให้กับผูให้บริการ	ประกาศ เรื่อง ขั้นตอนการแจงเตือนการระงับการทำให้แพรหลายของขอมูลคอมพิวเตอร และการนำขอมูลคอมพิวเตอรนั้นออกจากระบบคอมพิวเตอร พ.ศ. ....
มาตรา ๑๗/๑ วางกลไกเปรียบเทียบความผิดสำหรับโทษสถานเบา	ประกาศ เรื่อง แตงตั้งคณะกรรมการเปรียบเทียบ ตาม พ.ร.บ.วาดวยการกระทำความผิดเกี่ยวกับคอมพิวเตอร พ.ศ. ....
มาตรา ๒๐ การระงับการเผยแพร ตองตรวจสอบการใชอำนาจโดยศาล เฉพาะเนื้อหาที่ขัดตอการสงบเรียบรอย (ที่กระทบตอสังคมในวงกวาง) ตองมีคณะกรรมการกลั่นกรอง (อยางนองตองมีเอกชนจากสายสื่อ, สิทธิมนุษยชน ไอที) **อีกชั้นหนึ่ง กอนให้ศาลตรวจสอบ ถวงดุลการทำหนาที่**	ประกาศ เรื่อง หลักเกณฑ์ ระยะเวลา และวิธีการปฏิบัติสำหรับการระงับการทำให้แพรหลายหรือลบขอมูลคอมพิวเตอรของพนักงานเจาหนาที่หรือผูให้บริการ พ.ศ. .... ประกาศ เรื่อง แตงตั้งคณะกรรมการกลั่นกรองขอมูลคอมพิวเตอร ตามพ.ร.บ.วาดวยการกระทำความผิดเกี่ยวกับคอมพิวเตอร พ.ศ. ...
มาตรา ๒๑ กำหนดชุดคำสั่งไมพึงประสงค ที่ใชประโยชนได เชน ใชตัวสอบชองโหวงยอมไมผิดกฎหมาย	**ประกาศ เรื่อง กำหนดรายชื่อ ลักษณะ หรือรายละเอียดของชุดคำสั่งไมพึงประสงค ซึ่งอาจนำมาใชเพื่อปองกันหรือแกไขชุดคำสั่งไมพึงประสงคก็ได (อาจมีการจัดทำในภายหลัง)**

มาตรา ๑๑ กำหนดให้ชัดเจนว่าอะไรคือ สแปมหรือจดหมายอิเล็กทรอนิกส ที่ทำให้เดือดร้อนรำคาญ และเพิ่มโทษพวก spam หรือข้อมูลอิเล็กทรอนิกส์ ที่ทำให้เดือดร้อนรำคาญ โดยเฉพาะในเชิงพาณิชย์พวกโฆษณาอะไรต่างๆ

พรบ. พ.ศ. ๒๕๕๐ มาตรา ๑๑	พรบ.(ฉบับที่ ๒) พ.ศ. ๒๕๖๐ มาตรา ๑๑
ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่น โดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ระวางโทษปรับไม่เกิน*หนึ่งแสน*บาท	ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่น -ลักษณะเป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับข้อมูลคอมพิวเตอร์ -หรือจดหมายอิเล็กทรอนิกส์ โดยไม่เปิดโอกาสให้ผู้รับสามารถบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย ระวางโทษปรับไม่เกิน*สองแสน*บาท
ไม่เปิดโอกาศให้คนรับอีเมล กดยกเลิกการรับอีเมล	รมว. ดีอี ออกประกาศกำหนดลักษณะและวิธีการส่ง รวมทั้งลักษณะและปริมาณของข้อมูลคอมฯ/จดหมายอิเล็กทรอนิกส์ ซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับ และลักษณะอันเป็นการบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย

	พรบ.คอมพิวเตอร์ฯ พ.ศ.๒๕๕๐	พรบ.คอมพิวเตอร์ฯ (ฉบับที่ ๒) พ.ศ.๒๕๖๐
มาตรา ๑๒ ความผิดต่อข้อมูล/ระบบความมั่นคง	ก่อให้เกิดความเสียหายต่อข้อมูล/ระบบ เกี่ยวกับความมั่นคง ลงโทษจำคุก ๓-๑๕ ปี และปรับ ๑ หมื่น-๓ แสนบาท เป็นเหตุให้ผู้อื่นถึงแก่ความตาย ลงโทษจำคุก ๑๐-๒๐ ปี	กรณีกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ *ความปลอดภัยสาธารณะ* ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ เพิ่มโทษการเจาะระบบ การทำลายระบบที่เกี่ยวกับความมั่นคงของประเทศ

มาตรา ๑๒ ยกเลิก และให้กำหนดขึ้นใหม่ เน้นเกี่ยวกับการปกป้องโครงสร้างพื้นฐานสำคัญของประเทศ

พรบ. พ.ศ. ๒๕๕๐ มาตรา ๑๒	พรบ. (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ มาตรา ๑๒
ถ้าการกระทำความผิดตามมาตรา ๙ หรือ๑๐ (๑) ก่อให้เกิดความเสียหายแก่ประชาชน (โทษ ๑๐ปี ๒แสนบาท) (๒)เกิดความเสียหายต่อข้อมูล/ระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจ/การบริการสาธารณะ(โทษตั้งแต่ ๓ ปีถึง ๑๕ ปี ปรับตั้งแต่ ๖หมื่นถึง ๓ แสนบาท) ถ้าการกระทำความผิดตาม(๒) เป็นเหตุให้ผู้อื่นถึงแก่ความตาย (โทษจำคุกตั้งแต่ ๑๐ ปีถึง ๒๐ ปี) ระวางโทษที่สูงสุดถึง ๒๐ ปี	ถ้าการกระทำความผิดตามมาตรา ๕ , ๖ , ๗ , ๘ หรือ ๑๑ เป็นการกระทำต่อข้อมูล/ระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศฯ ถ้าการกระทำความผิดตามวรรคหนึ่งเป็นเหตุให้เกิดความเสียหายต่อข้อมูล/ระบบคอมพิวเตอร์ดังกล่าว (ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงสิบปี และปรับตั้งแต่สองหมื่นบาทถึงสองแสนบาท) ถ้าการกระทำความผิดตามมาตรา ๙ หรือ ๑๐ เป็นการกระทำต่อข้อมูล/ระบบคอมพิวเตอร์ตามวรรคหนึ่ง (ต้องระวางโทษจำคุกตั้งแต่ ๓ถึง ๕ ปีปรับ ๖ หมื่นถึง ๓แสนบาท) ถ้าการกระทำความผิดตามวรรคหนึ่งถึงสามถ้าการกระทำความผิดตามมาตรา ๙ หรือ ๑๐ โดยมิได้มีเจตนาฆ่า 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 สรุปอัตราโทษที่ปรับปรุงใหม่

มาตรา	ฐานความผิด	อัตราโทษ
ม. ๑๒	* เมื่อการแฮกขอมูลหรือระบบ, ดักรับ, Spam, เปดเผยมาตรการปองกัน ทำตอโครงสรางสำคัญ เชน ไฟฟา ประปา หากเกิดความเสียหายตามมาดวย	โทษ ๑-๗ ป ปรับ ๑๐,๐๐๐ – ๑๔๐,๐๐๐
	*เมื่อแกไขเปลี่ยนแปลงขอมูล, ขัดขวางหรือชะลอการทำงานระบบ ทำตอโครงสรางสำคัญ เชน ไฟฟา ประปา	โทษ ๑-๑๐ ป ปรับ ๒๐,๐๐๐ – ๒๐๐,๐๐๐ โทษ ๓-๑๕ ป ปรับ ๖๐,๐๐๐ – ๓๐๐,๐๐๐
	ไมเจตนา แตทำใหคนตาย	โทษ ๕-๒๐ ปี ปรับ ๑๐๐,๐๐๐ – ๔๐๐,๐๐๐
ม. ๑๒/๑	*แกไขเปลี่ยนแปลง, ทำใหระบบทำงานไมปกติ ทำใหบาดเจ็บ ทรัพยสินเสียหาย	ไมเกิน ๑๐ ป ปรับไมเกิน ๒๐๐,๐๐๐
	ไมเจตนา แตทำใหคนตาย	โทษ ๕-๒๐ ป ปรับ ๑๐๐,๐๐๐ – ๔๐๐,๐๐๐

มาตรา ๑๓ การเผยแพร่ชุดคำสั่ง มีการเพิ่มเติม

พรบ. ปี ๒๕๕๐ มาตรา ๑๓	พรบ. (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ มาตรา ๑๓
ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือ ในการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ มาตรา ๙ มาตรา ๑๐ หรือ มาตรา ๑๑ ระวางโทษจำคุกไม่เกิน ๑ ปี หรือปรับไม่เกิด 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 วรรคสองหรือวรรคสี่ หรือมาตรา ๑๒/๑ ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งดังกล่าวจะต้องรับผิดทางอาญาตามความผิดที่มีกำหนดโทษสูงขึ้นด้วยก็เฉพาะเมื่อตนได้รู้หรืออาจเล็งเห็นได้ว่าจะเกิดผลเช่นที่เกิดขึ้นนั้น - เพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๑๒ (๑)/(๓) หากผู้นำไปใช้ได้กระทำความผิดตามมาตรา ๑๒ (๑)/(๓) หรือต้องรับผิดตามมาตรา ๑๒ (๒)/(๔) หรือมาตรา ๑๒/๑ ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งดังกล่าวต้องรับผิดทางอาญาตามความผิดที่มีกำหนดโทษสูงขึ้นนั้นด้วย ในกรณีที่ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งผู้ใดต้องรับผิดตามวรรคหนึ่งหรือวรรคสอง และตามวรรคสามหรือวรรคสี่ด้วย ให้ผู้นั้นต้องรับโทษที่มีอัตราโทษสูงที่สุดแต่กระทงเดียว”

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

มาตรา	ฐานความผิด	อัตราโทษ
๑๓	วรรค ๑ จำหน่ายชุดคำสั่ง/เผยแพร่ไปใช้เป็นเครื่องมือกระทำผิด ต่อข้อมูลหรือระบบ ทำตอโครงสรางสำคัญ เชน ไฟฟา ประปา	โทษ ๒ ป ปรับไม่เกิน ๔๐,๐๐๐ บาท
	วรรค ๒ จำหน่ายชุดคำสั่ง/เผยแพร่ไปใช้เป็นเครื่องมือกระทำผิด แฮกขอมูลหรือระบบ, ดักรับ, Spam,เปดเผยมาตรการปองกัน	รับผิดทางอาญาตามความผิดที่มีกำหนดโทษสูงขึ้นด้วย
	วรรค ๓ เมื่อนำไปใช้เป็นเครื่องมือกระทำความผิด	ตามมาตรา ๑๒ (๑)/(๓) หากผู้นำไปใช้ได้กระทำความผิดตามมาตรา ๑๒ (๑)/(๓) หรือต้องรับผิดตามมาตรา ๑๒ (๒)/(๔) หรือมาตรา ๑๒/๑
	วรรค ๔ ในกรณีที่ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งผู้ใดต้องรับผิดตามวรรค ๑ หรือวรรค ๒ และตามวรรค ๓ หรือวรรค ๔ ด้วย	ให้ผู้นั้นต้องรับโทษที่มีอัตราโทษสูงที่สุดแต่กระทงเดียว

มาตรา ๑๔ มีเพิ่มเติม/แก้ไขในมาตรานี้ โดยเน้นประเด็นการหมิ่นประมาทออนไลน์

	พรบ.คอมพิวเตอร์ฯ พ.ศ.๒๕๕๐	พรบ.คอมพิวเตอร์ฯ (ฉบับที่ ๒) พ.ศ.๒๕๖๐
การนำเข้าข้อมูลเท็จ ตามมาตรา ๑๔(๑)	เปิดช่องให้ตีความเอาผิดกับการหมิ่นประมาทบนออนไลน์	ม.๑๔(๑) โดยทุจริตหรือโดยหลอกลวงนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน มุ่งเอาผิดการกระทำต่อทรัพย์สินชัดเจนขึ้น และยังเปิดช่องให้ตีความเอาผิด กับการบิดเบือนได้ อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา

มาตรา ๑๔ รายละเอียดในมาตรานี้

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 ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน **อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา**

มาตรา ๑๔(๒) ต้องเป็นกรณีที่น่าจะเกิดความเสียหาย คือมีการนำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์นั้นเป็นเท็จ คือนำข้อมูลอันเป็นเท็จเข้าไปในระบบ โดยประการที่น่าจะก่อให้เกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ฯ ความมั่นคงทางเศรษฐกิจ ความปลอดภัยของประเทศในเรื่องโครงสร้างพื้นฐานหรือประโยชน์สาธารณะ

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

มาตรา ๑๔ การนำข้อมูลเข้าระบบแล้วทำให้เกิดความเสียหาย กฎหมายที่ใช้อยู่ปัจจุบัน พบว่ามีการนำมาตรา ๑๔ (๑) ไปใช้แจ้งความฐานหมิ่นประมาท คือนำเข้าข้อมูลอันเป็นเท็จที่ทำให้เกิดความเสียหายต่อผู้อื่น

พรบ. ปี ๒๕๕๐ มาตรา ๑๔	พรบ. (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ มาตรา ๑๔
กระทำความผิดที่ระบุไว้ ดังต่อไปนี้ (มี ๕ องค์ประกอบ) (๑) **นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูล คอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ** โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน	**ประเด็นที่แก้ไข มาตรา ๑๔(๑)** แก้ไขโดยเพิ่มคำว่า **“โดยทุจริตหรือโดยหลอกลวง”** เข้าไปจาก เดิมมาตรา ๑๔ ของปี ๒๕๕๐ และ...**ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอม .. และอันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา** บิดเบือน เช่น บิดเบือนราคาหุ้นในตลาดหลักทรัพย์ฯ ที่ทำให้กลไกของตลาดหลักทรัพย์ผิดไป
(๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหาย**ต่อความมั่นคงของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน**	**ประเด็นที่แก้ไข มาตรา ๑๔(๒)** “นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหาย**ต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน”**

มาตรา ๑๕ ให้ยกเลิกความเดิมในมาตรานี้ และให้ใช้ความต่อไปนี้แทน (กำหนดมาตรการในการคุ้มครองผู้ให้บริการ)

พรบ. ปี ๒๕๕๐ มาตรา ๑๕	พรบ. (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ มาตรา ๑๕
ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำผิดตามมาตรา ๑๔	ผู้ให้บริการผู้ใดให้ความร่วมมือ ยินยอม หรือรู้เห็นเป็นใจให้มีการกระทำความผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน **ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา ๑๔**
จำคุกไม่เกิน**ห้าปี** หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ	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 ซึ่งจะมีอยู่ในประกาศของกระทรวงฯอีกที ผู้ให้บริการแต่ละประเภทจะสามารถลบได้ภายในกี่วัน

พรบ. (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ มาตรา ๑๕

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”

มาตรา ๑๖ ให้ยกเลิกความเดิมในมาตรานี้ และให้ใช้ความต่อไปนี้แทน

พรบ. ปี ๒๕๕๐ มาตรา ๑๖	พรบ. (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ มาตรา ๑๖
ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ ที่ปรากฏ เป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้โดยประการ ที่น่าจะทำให้ผู้อื่นนั้น เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย จำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ	ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้นฯ ต้องระวางโทษจำคุกไม่เกินสามปี และปรับไม่เกินสองแสนบาท *ถ้าการกระทำตามวรรคหนึ่งเป็นการกระทำต่อภาพของผู้ตาย และการกระทำนั้นน่าจะทำให้บิดา มารดา คู่สมรส หรือบุตรของผู้ตายเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง หรือได้รับความอับอาย ผู้กระทำต้องระวางโทษดังที่บัญญัติไว้ในวรรคหนึ่ง* ถ้าการกระทำตามวรรคหนึ่งหรือวรรคสอง เป็นการนำเข้าสู่ระบบคอมพิวเตอร์โดยสุจริต อันเป็นการติชมด้วยความเป็นธรรม ซึ่งบุคคลหรือสิ่งใดอันเป็นวิสัยของประชาชนย่อมกระทำ ผู้กระทำไม่มีความผิด
ถ้าการกระทำตามวรรคหนึ่ง โดยสุจริต ผู้กระทำไม่มีความผิด ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้	ความผิดตามวรรคหนึ่งและวรรคสองเป็นความผิดอันยอมความได้
ถ้าผู้เสียหายในวรรคหนึ่งตายก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรสหรือบุตรของผู้เสียหายร้องทุกข์ได้	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 ซึ่งมีคำพิพากษาว่าจำเลยมีความผิดศาลอาจสั่ง (๑) ให้ทำลายข้อมูลตามมาตราดังกล่าว (๒) ให้โฆษณาหรือเผยแพร่คำพิพากษาทั้งหมดหรือแต่บางส่วนในสื่ออิเล็กทรอนิกส์ วิทยุกระจายเสียง วิทยุโทรทัศน์ หนังสือพิมพ์ หรือสื่ออื่นใด ตามที่ศาลเห็นสมควรโดยให้จำเลยเป็นผู้ชำระค่าโฆษณาหรือเผยแพร่ (๓) ให้ดำเนินการอื่นตามที่ศาลเห็นสมควรเพื่อบรรเทาความเสียหายที่เกิดขึ้นจากการกระทำความผิดนั้น
	มาตรา ๑๖/๒ ผู้ใดรู้ว่าข้อมูลคอมพิวเตอร์ในความครอบครองของตนเป็นข้อมูลที่ศาลสั่งให้ทำลายตามมาตรา ๑๖/๑ ผู้นั้นต้องทำลายข้อมูลดังกล่าว หากฝ่าฝืนต้องระวางโทษกึ่งหนึ่งของโทษที่บัญญัติไว้ในมาตรา ๑๔ หรือมาตรา ๑๖ แล้วแต่กรณี”

พรบ. (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ มาตรา ๑๖

ประเด็นที่แก้ไข

นำเข้าเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้นฯ *ถ้าการกระทำตามนี้เป็นการกระทำต่อภาพของผู้ตาย และการกระทำนั้นน่าจะทำให้บิดา มารดา คู่สมรส หรือบุตรของผู้ตายเสียชื่อเสียง 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 ๑๘ แก้ไขเพิ่ม การร้องขอให้ดำเนินการกรณีความผิดอาญาต่อกฎหมายอื่นซึ่งได้ใช้ระบบคอมพิวเตอร์ข้อมูลคอมพิวเตอร์

พรบ. ปี ๒๕๕๐ มาตรา ๑๘	พรบ.(ฉบับที่ ๒) พ.ศ. ๒๕๖๐ มาตรา ๑๘
มาตรา ๑๘ อำนาจทั่วไปของพนักงานเจ้าหน้าที่ที่ได้รับการแต่งตั้ง แบ่งเป็น ๑. อำนาจที่ดำเนินการได้โดยไม่ต้องใช้อำนาจศาล -(๑) มีหนังสือสอบถาม เพื่อให้ส่งคำชี้แจง ให้ข้อมูล - (๒)เรียกข้อมูลจราจรคอมพิวเตอร์ -(๓) สั่งให้ส่งมอบข้อมูลตาม ม.๒๖ ๒. อำนาจที่ต้องขออนุญาตศาล -ทำสำเนาข้อมูล - เข้าถึงระบบคอมพิวเตอร์/ข้อมูลคอมพิวเตอร์ - ถอดรหัสลับ - ยึดอายัดระบบคอมพิวเตอร์	ให้พนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา อาจร้องขอให้พนักงาน เจ้าหน้าที่ตามพระราชบัญญัตินี้ฯ ดำเนินการตาม พระราชบัญญัติในบรรดาความผิดอาญาต่อกฎหมายอื่นซึ่งได้ใช้ระบบคอมพิวเตอร์ข้อมูลคอมพิวเตอร์หรือ อุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์เป็นองค์ประกอบหรือเป็นส่วนหนึ่งในการกระทำความผิดและ**ให้ผู้ได้รับการร้องขอ จากพนักงานเจ้าหน้าที่ดำเนินการตามคำร้องขอโดยไม่ชักช้า** ให้ผู้ได้รับการร้องขอจากพนักงานเจ้าหน้าที่ตามวรรคหนึ่ง (๑) (๒) (๓) (๔) (๕) (๖) (๗ป หรือ(๘) ดำเนินการตามคำร้องขอโดยไม่ชักช้า **แต่ต้องไม่เกินเจ็ดวัน**นับแต่วันที่ได้รับคำร้องขอ หรือภายในระยะเวลาที่พนักงานเจ้าหน้าที่กำหนด ซึ่งต้องไม่น้อยกว่าเจ็ดวันและไม่เกินสิบห้าวัน เว้นแต่ในกรณีที่มีเหตุสมควร ต้องได้รับอนุญาตจากพนักงานเจ้าหน้าที่

มาตรา ๒๐ มาตราในการปิดกั้นเว็บไซต์ และที่เป็นความผิดกฎหมายอื่น /ลักษณะขัดต่อศีลธรรมอันดีของประชาชน

ความผิดอาญาตามกฎหมายเกี่ยวกับทรัพย์สินทางปัญญา หรือกฎหมายอื่นซึ่งข้อมูลคอมพิวเตอร์นั้นมีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

มาตรา ๒๐ การปิดกั้นเว็บไซต์ และที่เป็นความผิดกฎหมายอื่น /ลักษณะขัดต่อศีลธรรมอันดีของประชาชน

พรบ. ปี ๒๕๕๐ มาตรา ๒๐	พรบ. (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ มาตรา ๒๐
มาตรา ๒๐ ในกรณีที่การกระทำความผิดเป็นการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่ 1. อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่กำหนดไว้ในภาคสอง ลักษณะ ๑ หรือลักษณะ ๑/๑ แห่งประมวลกฎหมายอาญา 2. ที่มีลักษณะขัดต่อ ความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน พนักงานเจ้าหน้าที่โดยได้รับความเห็นชอบจากรัฐมนตรีอาจยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นได้ ในกรณีที่ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายซึ่งข้อมูล คอมพิวเตอร์ตามวรรคหนึ่ง ให้พนักงานเจ้าหน้าที่ทำการระงับการทำให้แพร่หลายนั้นเอง หรือสั่งให้ผู้ให้บริการระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นก็ได้	ในกรณีที่มีการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ ดังต่อไปนี้ พนักงานเจ้าหน้าที่โดยได้รับความเห็นชอบจากรัฐมนตรีอาจยื่นคำร้อง พร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจ ขอให้มีคำสั่งระงับการทำให้แพร่หลาย/ลบข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์ได้ (๑) ข้อมูลคอมพิวเตอร์ที่เป็นความผิดตามพระราชบัญญัตินี้ (๒) ข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่กำหนดไว้ในภาค ๒ ลักษณะ ๑ หรือลักษณะ ๑/๑ แห่งประมวลกฎหมายอาญา (๓) ข้อมูลคอมพิวเตอร์ที่เป็นความผิดอาญาตามกฎหมายเกี่ยวกับทรัพย์สินทางปัญญา หรือกฎหมายอื่นซึ่งข้อมูลคอมพิวเตอร์นั้นมีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชนและเจ้าหน้าที่ตามกฎหมายนั้น หรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญาได้ร้องขอ

มาตรา ๒๐ การปิดกั้นเว็บไซต์ และให้มีประกาศหลักเกณฑ์ สำหรับการระงับ/ลบข้อมูล

พรบ. (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ มาตรา ๒๐

ขั้นตอนการปิดกั้น

ในกรณีที่ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ ให้พนักงานเจ้าหน้าที่ทำการระงับการทำให้แพร่หลายหรือลบข้อมูลนั้นเอง หรือสั่งให้ผู้ให้บริการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์นั้นก็ได้ ทั้งนี้ ให้รัฐมนตรีประกาศกำหนดหลักเกณฑ์ ระยะเวลา และวิธีปฏิบัติสำหรับการระงับการทำให้เผยแพร่หรือลบข้อมูลของพนักงานเจ้าหน้าที่หรือผู้ให้บริการให้เป็นไปในแนวทางเดียวกันโดยคำนึงถึงพัฒนาการทางเทคโนโลยีสารสนเทศที่เปลี่ยนแปลงไป เว้นแต่ศาลจะมีคำสั่งเป็นอย่างอื่น

ในกรณีที่มีเหตุจำเป็นเร่งด่วน พนักงานเจ้าหน้าที่จะยื่นคำร้องตามวรรคหนึ่งไปก่อนที่จะได้รับความเห็นชอบจากรัฐมนตรีก็ได้ แต่ทั้งนี้ต้องรายงานให้รัฐมนตรีทราบโดยเร็ว

เพิ่มเติม มาตรา ๒๐/๑ ข้อมูลซึ่งขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน โดยให้รัฐมนตรีโดยความเห็นชอบของคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์ให้เจ้าหน้าที่นำไปยื่นเรื่องต่อศาล เพื่อขอให้ศาลมีคำสั่งระงับหรือลบ

พรบ. (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ มาตรา ๒๐/๑

ในกรณีที่ทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน และรัฐมนตรีโดยความเห็นชอบของคณะกรรมการกลั่นกรอง เห็นสมควรให้พนักงานเจ้าหน้าที่ยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจ ขอให้มีคำสั่งระงับการทำให้แพร่หลายหรือลบซึ่งข้อมูลนั้นออกจากระบบคอมพิวเตอร์

ให้รัฐมนตรีแต่งตั้งคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์ตามวรรคสองขึ้นคณะหนึ่งหรือหลายคณะ แต่ละคณะให้มีกรรมการจำนวนเก้าคน ซึ่งสามในเก้าคนต้องมาจากผู้แทนภาคเอกชนด้านสิทธิมนุษยชน ด้านสื่อสารมวลชน ด้านเทคโนโลยีสารสนเทศ หรือด้านอื่นที่เกี่ยวข้อง และให้กรรมการได้รับค่าตอบแทนตามหลักเกณฑ์ที่รัฐมนตรีกำหนด โดยได้รับความเห็นชอบจากกระทรวงการคลัง

ในกรณีที่มีเหตุจำเป็นเร่งด่วน พนักงานเจ้าหน้าที่**โดยความเห็นชอบของคณะกรรมการกลั่นกรอง**จะยื่นคำร้องตามวรรคหนึ่งไปก่อนที่รัฐมนตรีมอบหมาย ก็ได้ แต่ทั้งนี้ต้องรายงานให้รัฐมนตรีทราบโดยเร็ว”

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

ลักษณะเนื้อหา	ลักษณะเนื้อหา
- ผิด พ.ร.บ.นี้ - เป็นความผิดเกี่ยวกับความมั่นคงปลอดภัย ของประเทศ/ก่อการร้าย ตามประมวลกฎหมายอาญา - ผิดกฎหมายอื่น กฎหมายอาญา **ผิดกฎหมายทรัพย์สินทางปัญญา**	-ข้อมูลมีลักษณะขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน

ขั้นตอนการออกคำสั่ง

พนักงานเจ้าหน้าที่ → รมว. ดีอี. → ศาล → พนักงานเจ้าหน้าที่/ผู้ให้บริการ → ดำเนินการระงับ/ลบ

ขั้นตอนการออกคำสั่ง

พนักงานเจ้าหน้าที่ → คณะกรรมการกลั่นกรอง

๙ คน ๓/๙ ต้องมาจากเอกชนด้านสิทธิ, สื่อสารมวลชน,สื่อมวลชน, ด้านไอทีหรืออื่นๆ

คณะกรรมการกลั่นกรอง → รมว. ดีอี. → ศาล → พนักงานเจ้าหน้าที่/ผู้ให้บริการ → ดำเนินการระงับ/ลบ

พรบ. (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ มาตรา ๒๐

ประเด็นที่แก้ไข ในกรณีที่ขอให้มีคำสั่งระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์ได้

เพิ่มเติม **“ข้อมูลคอมพิวเตอร์ที่เป็นความผิดอาญาตามกฎหมายเกี่ยวกับทรัพย์สินทางปัญญา หรือกฎหมายอื่นซึ่งข้อมูลคอมพิวเตอร์นั้นมีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน..”**

ในกรณีที่มีการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน รัฐมนตรีโดยความเห็นชอบของคณะกรรมการกลั่นกรอง ก่อนแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้แพร่หลายหรือลบซึ่งข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์

ในกรณีที่ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ พนักงานเจ้าหน้าที่จะทำการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์นั้นเอง หรือจะสั่งให้ผู้ให้บริการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์นั้นก็ได้ ทั้งนี้ ให้รัฐมนตรีประกาศกำหนด หลักเกณฑ์ ระยะเวลา และวิธีการปฏิบัติ

มาตรา ๒๖ การเก็บรักษาข้อมูลจราจร

พรบ. ปี ๒๕๕๐ มาตรา ๒๖	พรบ. (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ มาตรา ๒๖
มาตรา ๒๖ ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้ ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใด ให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท	มาตรา ๒๖ ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวัน นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวัน แต่ไม่เกินสองปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

นอกจากนี้ ยังมีการแก้ไขในมมาตรา อื่น ๆที่เกี่ยวข้องกับพนักงานเจ้าหน้าที่ตามพระราชบัญญัติฯ ให้มีความรัดกุม คล่องตัวในการปฏิบัติงาน และกำหนดบทลงโทษพนักงานเจ้าหน้าที่ที่ชัดเจนขึ้นด้วย

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

และมาตรา ๒๘ “ผู้ที่ได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ คำนึงถึงภาระหน้าที่ความรู้ความเชี่ยวชาญ ความขาดแคลนในการหาผู้มาปฏิบัติหน้าที่ หรือมีการสูญเสียผู้ปฏิบัติงานออกจากระบบราชการเป็นจำนวนมาก คุณภาพของงาน และการดำรงตนอยู่ในความยุติธรรม โดยเปรียบเทียบค่าตอบแทนของผู้ปฏิบัติงานอื่นในกระบวนการยุติธรรมด้วย”

การใช้อำนาจของพนักงานเจ้าหน้าที่ตามร่าง พ.ร.บ. คอมฯ ยังต้องทำตามกลไกตรวจสอบการใช้อำนาจรัฐตามที่กฎหมายปัจจุบันกำหนดไว้ ซึ่งส่วนใหญ่ต้องขออนุญาตจากศาลก่อนจึงจะดำเนินการ ได้ เช่น ทำสำเนา, ถอดรหัส, การตรวจสอบการเข้าถึงข้อมูล, ยึดอายัด ตามมาตรา ๑๘ มาตรา ๑๙ แห่ง พระราชบัญญัติ

มาตรา ๒๐ บรรดาระเบียบหรือประกาศที่ออกตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ที่ใช้บังคับอยู่ในวันก่อนวันที่พระราชบัญญัตินี้ใช้บังคับ ให้ยังคงใช้บังคับต่อไปเท่าที่ไม่ขัดหรือแย้งกับบทบัญญัติแห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัตินี้ จนกว่าจะมีระเบียบหรือประกาศที่ต้องออกตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัตินี้ ใช้บังคับ

การดำเนินการออกระเบียบหรือประกาศตามวรรคหนึ่ง ให้ดำเนินการให้แล้วเสร็จ**ภายในหกสิบวัน**นับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ หากไม่สามารถดำเนินการได้ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรายงานเหตุผลที่ไม่อาจดำเนินการได้ต่อคณะรัฐมนตรีเพื่อทราบ

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ

ผลกระทบจากการบังคับใช้ พ.ร.บ.

ผลกระทบที่อาจต้องแบกรับ
มาตรา ๒๖ และ ๒๗

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

ประโยชน์มหาชน / สาธารณะ
Public Interests

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ

ผลจากการบังคับใช้ พ.ร.บ.

สรุปยังคงมีการกระทำผิดที่ไม่ลดลง สาเหตุ มีการใช้หลากหลาย การติดต่อทำได้รวดเร็ว มีการแข่งขันของผู้ประกอบการสูง

- ยังคงมีการระงับการเผยแพร่เนื้อหาหรือการปิดกั้นเว็บไซต์โดยอาศัยมาตรา ๒๐ ของพ.ร.บ.

- คดีที่มีเนื้อหาความผิดเกี่ยวข้องกับการหมิ่นประมาทต่อบุคคลมีสัดส่วนมากที่สุดในคดีที่ถูกฟ้องตาม พ.ร.บ.ฯ

รองลงมาได้แก่ คดีที่เป็นอาชญากรรมคอมพิวเตอร์โดยแท้ (เช่น การเจาะข้อมูล การส่งสแปม)

อันดับที่ ๓ คดีที่มีเนื้อหาความผิดเกี่ยวข้องกับการหมิ่นประมาทกษัตริย์ พระราชินี และรัชทายาท

อันดับที่ ๔ มีสองประเภท คือ คดีที่เกี่ยวข้องกับการฉ้อโกง เช่น โพสท์ข้อความหลอกขายของ และคดีที่เกี่ยวข้องกับเนื้อหาลามก ที่เหลือส่วนน้อยเป็นคดีที่เกี่ยวข้องกับการขายโปรแกรม คดีที่เกี่ยวกับความมั่นคง และคดีอื่นๆ

ความตระหนักถึงความมั่นคงปลอดภัยด้านสารสนเทศ

การใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

หน่วยงานมีระบบงานสารสนเทศ และเครือข่ายทีมสามารถเชื่อมต่ออินเทอร์เน็ตทั้งภายในหน่วยงานเอง(Intranet) และการเชื่อมต่อไปยังภายนอกองค์(Internet)

๑.ผู้เกี่ยวข้องในการให้บริการ

๒.ผู้ใช้บริการ

๓.การใช้งาน ระบบงาน/การสื่อสารเชื่อมต่อ

๔.ภัยคุกคามที่อาจเกิดขึ้น แนวทางป้องกันหรือการสร้างความตระหนักที่พึงระวังไว้ /การปฏิบัติตามข้อปฏิบัติ หรือกฎหมายที่เกี่ยวข้อง

๕. การบริหารจัดการเพื่อแก้ไขปัญหา การควบคุม เช่นการเข้าถึง การใช้งาน เช่นเครื่องคอมพิวเตอร์ส่วนบุคคล การควบคุมการส่งข้อมูลข่าวสาร/จดหมายอิเล็กทรอนิกส์

การใช้เทคโนโลยีสารสนเทศ หมายถึง กระบวนการต่างๆ และระบบงานที่ช่วยให้ได้สารสนเทศหรือข่าวสารที่ต้องการ โดยจะรวมถึง

๑. เครื่องมือและอุปกรณ์ต่างๆ หมายถึง เครื่องคอมพิวเตอร์ เครื่องใช้สำนักงาน อุปกรณ์คมนาคมต่างๆ รวมทั้งซอฟต์แวร์ทั้งระบบสำเร็จรูปและพัฒนาขึ้นโดยเฉพาะด้าน

๒. กระบวนการในการนำอุปกรณ์เครื่องมือต่างๆ ข้างต้นมาใช้งานรวบรวมข้อมูล จัดเก็บประมวลผล และแสดงผลลัพธ์เป็นสารสนเทศในรูปแบบต่างๆ ที่สามารถนำไปใช้ประโยชน์ได้ต่อไป

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

ปัจจุบันมีกฎหมายที่เกี่ยวข้องด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสาร

๑. กฎหมายเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (Computer Crime Law) เพื่อกำหนดมาตรการทางอาญาในการลงโทษผู้กระทำผิดต่อระบบการทำงานของคอมพิวเตอร์ 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

การรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับองค์กร

“ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายความว่า

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

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

“การปกป้องข้อมูล (Data protection)” หมายถึงการป้องกันข้อมูลส่วนบุคคลต่อการประสงค์ร้ายของบุคคลที่สาม

“เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายถึง การเกิดเหตุการณ์ หรือสภาพของบริการที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

การควบคุมโดยการออกระเบียบหรือแนวทางปฏิบัติ

๑. มีการประกาศใช้ แนวนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยขององค์กร การนำแนวนโยบายไปปฏิบัติ ออกมาเช่น การรักษาความมั่นคงปลอดภัย มีแนวทางการป้องกันทางด้านไซเบอร์ สร้างขั้นตอนปฏิบัติ

๒. การจัดองค์กร และการรักษาความปลอดภัยสำหรับระบบสารสนเทศ

๒.๑.การจัดองค์การการวางโครงสร้างขององค์กรที่สามารถเอื้ออำนวยให้แผนงานที่จัดทำขึ้นไปสู่สัมฤทธิ์ผล โดยกำหนดอำนาจหน้าที่และความรับผิดชอบของกลุ่มบุคคลในองค์กร เพื่อให้งานเป็นไปอย่างรวดเร็วและมีประสิทธิภาพ

๒.๒. การพัฒนาระบบงานควบคุมดูแลและปฏิบัติงานที่เกี่ยวกับเรื่องความมั่นคงปลอดภัย และการใช้งาน/เครื่องมืออุปกรณ์

พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

แนวทาง/มาตรการที่จะต้องกำหนดให้เป็นไปตามข้อกฎหมาย

ประเภท	แนวปฏิบัติ
ผู้ใช้บริการโดยทั่วไป	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 การปฏิบัติงานเพื่อแก้ไขปัญหาก็จะสามารถดำเนินการได้ทันต่อสถานการณ์ ในเมื่อมีความพร้อมและกระบวนการที่ชัดเจน

แนวทาง/มาตรการที่จะต้องกำหนดให้เป็นไปตามข้อกฎหมาย

การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย และข้อบังคับต่างๆ ที่เกี่ยวกับความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ

- เพื่อลดความเสี่ยงที่อาจเกิดขึ้นได้จากการปฏิบัติงานระบบสารสนเทศ
- เพื่อให้ระบบสารสนเทศมีความปลอดภัยจากการใช้เทคโนโลยีสารสนเทศที่ไม่เหมาะสม หรือไม่ถูกต้อง
- เพื่อเป็นกรอบการดำเนินงานด้านการรักษาความปลอดภัยสารสนเทศของ องค์กร
- เพื่อให้ผู้ใช้งานตระหนักถึงภัยคุกคาม และความปลอดภัยด้านเทคโนโลยีสารสนเทศ

แนวทาง/มาตรการที่จะต้องกำหนดให้เป็นไปตามข้อกฎหมาย

กำหนดเงื่อนไขนโยบายความปลอดภัยระบบสารสนเทศสำหรับผู้ทำงาน (Acceptable Use Policy: AUP) เพื่อเป็นกรอบที่กำหนดให้ผู้ใช้งานทำงานร่วมกัน โดยมีเป้าหมายเพื่อนำไปพัฒนาเป็นมาตรฐาน กระบวนการ แนวทาง/ขั้นตอนปฏิบัติที่เหมาะสมให้ระบบสารสนเทศเกิดความมั่นคง และปลอดภัยตามพื้นฐานการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ คือ การรักษาความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) ซึ่งผู้ใช้งานทุกระดับต้องให้ความสำคัญ

ควรให้ผู้ใช้งานคอมพิวเตอร์ทั่วไปได้รับทราบ รับเงื่อนไขนโยบายเกี่ยวกับความปลอดภัยระบบสารสนเทศขององค์กร หรือ AUP (Acceptable Use Policy) ด้วยเพื่อให้ผู้ใช้ได้ปฏิบัติตามนโยบาย

ความปลอดภัยของข้อมูลและความเป็นส่วนตัว ในการใช้คอมพิวเตอร์และอินเทอร์เน็ต

ความปลอดภัย

- การดูแลจัดการ ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูล ให้พ้นจากอันตรายต่าง ๆ เช่น อาชญากรรมคอมพิวเตอร์ ภัยธรรมชาติ ภัยคุกคามอื่นๆ

ความเป็นส่วนตัว

- การปกป้องข้อมูลส่วนตัวที่ไม่ต้องการเปิดเผยของผู้ใช้

แนวทาง/มาตรการที่จะต้องกำหนดให้เป็นไปตามข้อกฎหมาย

ตัวอย่างการกำหนดเงื่อนไข

๑.การปฏิบัติตามนโยบาย กฎหมาย/ข้อบังคับ และการปฏิบัติงากฎหมาย และข้อบังคับใดๆ เช่น พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ และประกาศกระทรวงฯเรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ของผู้ให้บริการพ.ศ. 2550 เป็นต้น ถือเป็นสิ่งสำคัญที่ผู้ใช้งานต้องตระหนัก และต้องปฏิบัติตามอย่างเคร่งครัด และไม่กระทำความผิดนั้น ดังนั้น หากผู้ใช้งานกระทำความผิดตามกฎหมาย หรือข้อบังคับที่ประกาศใช้ ถือว่าเป็นความผิด ซึ่งผู้ใช้งานต้องรับผิดชอบต่อความผิดนั้น

๒.ความรับผิดชอบต่อข้อมูลสารสนเทศขององค์กร

-ผู้ใช้งานระบบสารสนเทศ ต้องไม่เปิดเผยข้อมูลสารสนเทศใดๆ ที่เป็นความลับ หรือข้อมูลที่มีความสำคัญต่อองค์กรสู่ภายนอกหรือสาธารณะ ยกเว้นจะได้รับอนุญาตจากผู้มีอำนาจเท่านั้น

-ห้ามผู้ใช้งานระบบสารสนเทศที่ไม่มีสิทธิ เข้าถึงหรือแก้ไข หรือเปลี่ยนแปลงข้อมูลของระบบสารสนเทศโดยไม่ได้รับอนุญาต หรือไม่มีหน้าที่เกี่ยวข้อง

การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย และบทลงโทษ ของการละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศ

เพื่อหลีกเลี่ยงการฝ่าฝืนกฎหมายทั้งทางอาญาและทางแพ่ง พระราชบัญญัติ นโยบาย กฎ ระเบียบข้อบังคับ ที่เกี่ยวข้อง

การถ่ายทอดองค์ความรู้ ความเข้าใจ ข้อกฎหมาย ระเบียบข้อบังคับ รวมถึงการฝึกอบรมผู้เกี่ยวข้องทางด้านความมั่นคงปลอดภัย และการเตรียมความพร้อมอย่างสม่ำเสมอ

ข้าราชการ/พนักงานเจ้าหน้าที่ทุกคนควรรับทราบ ทำความเข้าใจ และปฏิบัติตามรายการของนโยบาย กฎ ระเบียบ ข้อบังคับ กฎหมาย ที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารที่กำหนดขึ้น เช่นนโยบายการรักษาความมั่นคงด้านเทคโนโลยีสารสนเทศและการสื่อสาร พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์ พ.ร.บ. ลิขสิทธิ เป็นต้น

ผู้บริหารระดับสูงขององค์กร ให้ความสำคัญเรื่องความปลอดภัยข้อมูลอย่างเพียงพอ และจริงจังในการผลักดันเรื่องความปลอดภัยข้อมูล

ระบบรักษาความปลอดภัยสำนักงานฯ จะทำให้เจ้าหน้าที่ที่เกี่ยวข้องทราบถึงแนวทางในการปฏิบัติ เพื่อหลีกเลี่ยงความเสี่ยงต่าง ๆ หรือลดความรุนแรงของผลเสียหายต่าง ๆ ที่อาจเกิดขึ้นต่อระบบปฏิบัติราชการของสำนักงานฯ ซึ่งพบว่าปัญหาด้านความปลอดภัยที่อาจเกิดขึ้นได้นั้น ส่วนใหญ่เกิดจาก

๑) บุคลากร (Awareness Training)

๒) กระบวนงาน(process) (นโยบายความปลอดภัยและกระบวนการบริหารจัดการที่ดี)

๓) เทคโนโลยี(Technology)

ปัญหาหรือเหตุการณ์ด้านความมั่นคงปลอดภัย อาจเป็นเหตุการณ์ที่เกิดขึ้นในระบบคอมพิวเตอร์และเครือข่ายขององค์กร ซึ่งส่งผลให้

- เกิดการหยุดชะงักต่อกระบวนการทางธุรกิจสำคัญ (เช่น เนื่องจากระบบงานของกระบวนการทางธุรกิจเกิดการหยุดชะงัก เป็นต้น)
- เป็นการละเมิดนโยบายความมั่นคงปลอดภัยขององค์กร
- เป็นการละเมิดต่อกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดต่างๆ ที่องค์กรต้องปฏิบัติตาม
- เกิดภาพลักษณ์ที่ไม่ดีต่อองค์กร หรือทำให้องค์กรสูญเสียชื่อเสียง

ความสำคัญเรื่องความปลอดภัยข้อมูลหรือ ""Information Security"

การให้ความรู้ ตั้งแต่ ผู้บริหารระดับสูง, ผู้บริหารระดับกลาง, ผู้บริหารระบบ, ผู้ตรวจสอบภายใน รวมถึงผู้ใช้คอมพิวเตอร์ "ทุกคน" ในองค์กร ให้ "ตระหนัก" และ "เข้าใจ" ในข้อกฎหมาย ระเบียบข้อบังคับที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสาร

สร้างความตระหนักด้านความมั่นคงปลอดภัย การกำนดนโยบาย Security Policy หนึ่งในที่สำคัญคือ Acceptable Use Policy (AUP) คือใช้อย่างไรให้เหมาะสม ไม่เอาขององค์กรไปใช้ส่วนตัว พอเอาไปใช้ส่วนตัว ก็มีประเด็นเช่น เปลือง bandwidth องค์กร, ถ้ามีข้อมูลรั่วออกมาแบบนี้แล้วพนักงาน reuse password อาจถูกใช้เป็นหนึ่งในเข้าถึงข้อมูลได้

การควบคุมการใช้งาน แนวนโยบายและแนวทางปฏิบัติที่เกี่ยวกับความปลอดภัยข้อมูลในองค์กร

มีการฝึกอบรม "Security Awareness Training" เพื่อให้ผู้ใช้คอมพิวเตอร์ทุกคนในองค์กรได้ตระหนักถึงบทบัญญัติของ พ.ร.บ. ฯ และทำความเข้าใจ พ.ร.บ. ฯ

ข้อที่ควรระมัดระวัง

สำหรับผู้ให้บริการ ต้องระวัง หมั่นดูแลข้อมูลต่างๆที่คนอื่นโพสทิ้งไว้ในเว็บเราด้วย เช่นพวกเว็บบอร์ด กระทู้ หรือ ความเห็นต่างๆ เพราะมีคนมาโพสต์ข้อความ โพสต์รูปที่ทำให้บุคคลอื่นเสียหาย หรือภาพอนาจาร มีเนื้อหาพาดพิงสถาบัน แล้วถ้าเพิกเฉย ปล่อยให้มี การกระทำนั้น ก็จะมีความผิด พรบ.คอมพิวเตอร์ ในมาตรา ๑๕ ข้อหาสนับสนุนยินยอมให้คนอื่นเผยแพร่ข้อมูลที่กระทบให้ผู้อื่นเดือดร้อน เสียหาย กระทบความมั่นคงของรัฐ และอื่นๆตามที่ พรบ.คอม มาตรา ๑๔

การเก็บข้อมูลจราจรคอมพิวเตอร์ ควรกำหนดให้มีการปฏิบัติตามขั้นตอนปฏิบัติสำหรับการเก็บรวบรวม หลักฐานโดยเคร่งครัด

ในกรณีเกิดการกระทำความผิดขึ้นในองค์กร : ควรมีผังกระบวนการแสดงขั้นตอนการปฏิบัติเมื่อเกิดเหตุการณ์ พร้อมทั้งระบุผู้รับผิดชอบในการปฏิบัติในแต่ละขั้นตอนเป็นเฉพาะกรณีไป เช่นการคุกคามจากผู้ไม่ประสงค์ดีเข้าเปลี่ยนแปลงหน้าเว็บไซต์ขององค์กร โดยกรณีเช่นนี้ การวิเคราะห์และการประเมินเหตุการณ์ การปฏิบัติงานเพื่อแก้ไขปัญหาก็จะสามารถดำเนินการได้ทันต่อสถานการณ์ ในเมื่อมีความพร้อมและกระบวนการที่ชัดเจน

การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยให้ดีขึ้น

1) ตัด Internet Connection ของเครื่องนั้นๆ เสียก่อน เพื่อหยุดการทำลายหรือขโมยข้อมูลไปมากกว่านี้

2) ตรวจดู Log ของ Server ไม่ว่าจะเป็น Log ของ OS หรือ Log ของ Web Server เพื่อค้นหาว่ามีพฤติกรรมผิดปกติใดๆ ที่เกิดขึ้นกับเครือข่าย เมื่อเวลาใด โดย IP ใด

3) จัดการปิด Service ของโปรแกรม Remote ทุกประเภท ที่ติดตั้งไว้ในเครื่องแม่ข่ายหรืออุปกรณ์เครือข่าย

4) Update Patch ต่างๆ ให้เป็นปัจจุบันกับทุก Server และอุปกรณ์

5) ตรวจสอบการทำงานของโปรแกรม Anti Virus และ Update Virus Definitions ให้เป็นปัจจุบันกับทุก Server

6) กรณีข้อมูลสำคัญสูญหาย ให้ทำการ Recovery ข้อมูลที่สำรองไว้กลับคืนสู่ตำแหน่งที่ถูกต้องและทดสอบใช้งาน

7) เมื่อทำขั้นตอนดังกล่าวเรียบร้อยแล้ว ก็ค่อยๆ เปิด Service ไปทีละอย่าง เปิดเท่าที่จำเป็นต่อ Server เท่านั้น

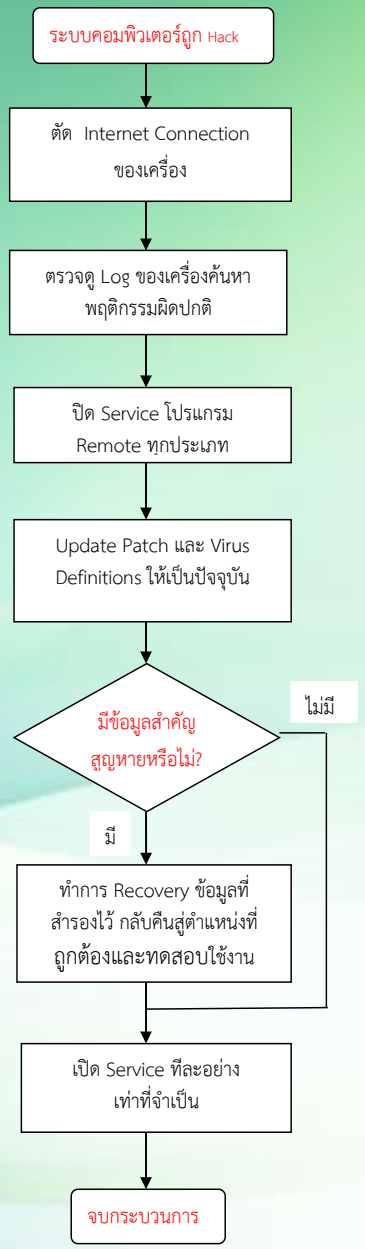
ผู้รับผิดชอบ

1. ระดับนโยบาย

ได้แก่ ผู้ที่รับผิดชอบงานด้านเทคโนโลยีสารสนเทศ(CIO) **และผู้อำนวยการสำนัก**/กอง/กลุ่มงาน

2. ระดับปฏิบัติ

ได้แก่ เจ้าหน้าที่กลุ่มงานคอมพิวเตอร์และเครือข่ายเจ้าหน้าที่ที่ได้รับมอบหมายให้ปฏิบัติงานด้าน IT ของแต่ละหน่วยงาน



: ในกรณีที่จำเป็นต้องมีการดำเนินการทางกฎหมายต่อบุคคลหรือองค์กรหนึ่งไม่ว่าจะเป็นการดำเนินการทางแพ่งหรืออาญาก็ตาม หน่วยงานควรดำเนินการเก็บหลักฐานที่เกี่ยวข้อง จัดเก็บไว้ช่วงระยะเวลาหนึ่ง และนำเป็นพยานหลักฐานเสนอ(อาทิ ต่อศาล) โดยให้สอดคล้องกับหลักการสำหรับการจัดเก็บหลักฐานที่ได้กำหนดไว้

การเก็บรวบรวมพยานหลักฐาน (Collection of evidence)

แนวปฏิบัติ :

(ก) หน่วยงานควรกำหนดขั้นตอนปฏิบัติสาหรับการเก็บรวบรวมหลักฐานเพื่อใช้สนับสนุนกระบวนการทางวินัยหรือกฎหมาย และลงโทษผู้กระทำความผิด

(ข) หน่วยงานควรกำหนดให้มีการปฏิบัติตามขั้นตอนปฏิบัติสำหรับการเก็บรวบรวมหลักฐานโดยเคร่งครัด

(ค) หน่วยงานควรกำหนดให้เฉพาะผู้ที่ผ่านการอบรมและมีทักษะเพียงพอในการเก็บรวบรวมหลักฐานคอมพิวเตอร์เท่านั้น จึงจะสามารถรวบรวมและจัดเก็บหลักฐานได้

(ง) หน่วยงานควรกำหนดให้มีการปฏิบัติตามกฎในการจัดเก็บหลักฐาน เช่น หลักฐานที่สามารถยอมรับได้ (Admissibility) หลักฐานที่จัดเก็บมานั้นต้องมีทั้งคุณภาพและความสมบูรณ์

ตัวอย่างหลักฐานที่อยู่บนสื่อบันทึกข้อมูลคอมพิวเตอร์ ได้แก่ การทำสำเนาข้อมูลจากสื่อบันทึกข้อมูล การทำสำเนาข้อมูลบนฮาร์ดดิสก์หรือหน่วยความจำออกมา การมีพยานที่เชื่อถือได้ในระหว่างที่ทำสำเนาข้อมูล การบันทึกข้อมูลล็อคเพื่อแสดงถึงกิจกรรมต่างๆ ระหว่างที่สำเนาข้อมูลนั้น การจัดเก็บสื่อบันทึกข้อมูลและข้อมูลล็อคไว้ในสถานที่ที่มีความปลอดภัย

การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้ใช้งานทั่วไป

ความปลอดภัยและความเป็นส่วนตัวบนอินเทอร์เน็ต

๑.เพื่อสร้างความปลอดภัยในการใช้อินเตอร์เน็ต

๑). อย่าให้รหัสลับแก่ผู้อื่น

๒). ต้องคิดให้ดีทุกครั้ง ที่ให้ข้อมูลส่วนตัวกับบุคคลอื่นในอินเทอร์เน็ต

๓). ตรวจทานว่าได้พิมพ์ชื่อเว็บไซด์ถูกต้องเสียก่อน แล้วจึงกด Enter เพื่อจะได้เข้าเว็บไซด์ที่ต้องการได้ถูกต้อง

๔). ถ้าพบเห็นข้อความ หรือสิ่งใด ที่ไม่เหมาะสม หรือ คิดว่าไม่ดีต่อการใช้อินเทอร์เน็ต ควรออกจากเว็บไซด์นั้น

๕). อย่าส่งรูปภาพของตนเอง หรือรูปภาพของผู้อื่น ให้คนอื่นทางอีเมล์

๖). ถ้าได้รับอีเมล์ที่มีข้อความไม่เหมาะสม หรือทำให้ไม่สบายใจ ไม่ควรโต้ตอบ

๗). บนอินเทอร์เน็ต ทุกอย่างที่คุณเห็นไม่ใช่เรื่องจริงเสมอไป

๘). อย่าบอกวันเดือนปีเกิด หรือ อายุจริงของคุณกับคนอื่น

๙). อย่าบอกชื่อจริง และนามสกุลจริงกับบุคคลอื่น

๑๐). อย่าบอกที่อยู่ ของคุณกับบุคคลอื่น

๑๑). อย่าบอกเบอร์โทรศัพท์ของคุณกับบุคคลอื่น ในอินเตอร์เน็ต

การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้ใช้งานทั่วไป

ความปลอดภัยและความเป็นส่วนตัวบนอินเทอร์เน็ต

๒. การป้องกัน : การใช้งานอินเทอร์เน็ตอย่างปลอดภัย

- อ่านข้อตกลง นโยบายให้ดีก่อนตอบตกลงใด ๆ
- ระวังการใช้บริการเครื่องคอมพิวเตอร์สาธารณะ

  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 ซึ่งผสมอักษรภาษาอังกฤษตัวเล็ก อักษรภาษาอังกฤษตัวใหญ่ ตัวเล็ก และตัวอักขระพิเศษ

๓. การป้องกันภัยคุกคาม ที่เกี่ยวกับการทำธุรกรรม

การป้องกันการใช้เครือข่ายสาธรณะ/Free WiFi

๑.ใช้เครือข่าย WiFi ที่เชื่อถือได้เท่านั้น

๒.ดูชื่อจุดเชื่อมต่อ

๓.ลบชื่อจุดเชื่อมต่อที่ไม่ได้ใช้จากรายการ

๔. เลือกการเชื่อมต่อ ที่ต้องเข้ารหัส (WPA๒.WPAและ WEP)

๕. อย่าแชร์ไฟล์และโฟลเดอร์

๖. เปิดไฟร์วอลล์ส่วนบุคคล

วิธีป้องกันภัยออนไลน์ เช่น ภัยจากมัลแวร์

วิธีที่มัลแวร์เข้าสู่คอมพิวเตอร์ของคุณ

๑.การดาวน์โหลดซอฟต์แวร์จากอินเทอรีเน็ตที่มีมัลแวร์แฝงอยู่

๒.การดาวน์โหลดซอฟต์แวร์ถูกกฎหมายที่แอบมีมัลแวร์ผูกติดมา

๓.การเข้าชมเว็บไซต์ที่ติดเชื้อมัลแวร์

- การคลิกข้อความแสดงข้อผิดพลาด/หน้าต่างป๊อปอัพ
-การเปิดไฟล์แนบอีเมล์ที่มีมัลแวร์

หลักการการป้องกันมัลแวร์

๑.อัพเดทคอมพิวเตอร์และซอฟต์แวร์ของคุณอยู่เสมอ

๒.คิดให้ดีก่อนจะคลิกลิงค์หรือดาวน์โหลดอะไรก็ตาม

๓.คิดก่อนเปิดไฟต์แนบอีเมล์หรือรูปภาพ

๔.อย่าเชื่อหน้าต่างป๊อปอัพที่ขอให้ดาวน์โหลดซอฟต์แวร์

๕.ให้ระมัดระวังเรื่องการแบ่งปันไฟล์

๖.การป้องกันโดยใช้ซอฟต์แวร์ป้องกันไวรัส

สิ่งที่ไม่ควรทำบนเครือข่ายสังคมออนไลน์

๑.ไม่โพสต์กิจกรรมที่ผิดกฎหมาย

๒. ไม่ควรโพสต์ข้อความ ที่ชี้ชวนให้มิจฉาชีพรับรู้ความเคลื่อนไหวส่วนตัว

๓.โพสต์ข้อมูลที่เป็นเรื่องส่วนบุคคล

๔. ให้ระมัดระวังการเช็คอิน (Check-in) ผ่านสื่อสังคมออนไลน์

๕. ไม่ระบุชื่อบุตรหลาน ระบุภาพหรือติด tag ในรูปภาพมากเกินไป

๖.ไม่ส่งหลักฐานส่วนตัวของตนเองและคนในครอบครัวให้ผู้อื่น

๗. พึงระมัดระวังอย่างยิ่งที่จะไว้ใจหรือเชื่อใจคน ที่รู้จักผ่านอินเทอร์เน็ต

ผู้ที่ได้รับผลกระทบจากการบังคับใช้กฎหมาย : กรณีเป็นผู้เสียหาย

ขั้นตอนการแจ้งความร้องทุกข์ในคดี ตาม พรบ. คอมพิวเตอร์

๑. เมื่อพบการกระทำความผิดหรือถูกละเมิดในสื่ออินเตอร์เน็ต ควรดำเนินการเบื้องต้น ดังนี้

- ๑.๑ ทำการบันทึกข้อมูลหลักฐานที่ปรากฏไว้ทั้งหมด เช่น หน้าเว็บเพจ ,ข้อความหรือภาพถ่ายที่ก่อให้เกิดความเสียหาย
- ๑.๒ พิมพ์ข้อมูลหน้าเว็ปไซต์ที่เกิดเหตุหรือเกี่ยวข้องออกมาเป็นเอกสาร เพื่อป้องกันไม่ให้พยานหลักฐานสูญหาย หรือถูกทำลาย และลงลายมือชื่อรับรองเอกสารนั้น
- ๑.๓ การสั่งพิมพ์เอกสารหน้าเว็บเพจ ,ข้อความหรือภาพถ่ายต่างๆ ในเว็ปไซต์ที่พบการกระทำผิด ให้ปรากฏที่ตั้งของเว็ปไซต์ หรือ URL ของเว็ปไซต์นั้นด้วย และหรือปรากฏวันเวลาบนเว็บไซต์หรือขณะบันทึกข้อมูลหลักฐานนั้นด้วย

ผู้ที่ได้รับผลกระทบจากการบังคับใช้กฎหมาย : กรณีเป็นผู้เสียหาย

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 เพื่อตรวจสอบข้อมูลให้ ต่อไป

๔. กรณีจำเป็นเร่งด่วนเพื่อป้องกันความเสียหาย เช่น ต้องทำการปิดกั้นเว็ปไซต์ หรือระงับการทำธุรกรรมทางอิเลคทรอนิกส์ ให้พนักงานสอบสวนที่รับแจ้งความ หรือผู้เสียหาย ประสานงานมายัง บก.ปอท. หรือ กระทรวงไอซีที หรือธนาคาร หรือผู้ให้บริการอินเทอร์เน็ตเพื่อดำเนินการเบื้องต้นในการบรรเทาความเสียหาย ต่อไป

การสอบถามข้อมูล : กรณีต้องการทราบรายละเอียดเพิ่มเติม/กรณีเป็นผู้เสียหาย

๑. หากต้องการศึกษาข้อมูลและรายละเอียดเพิ่มเติมสามารถติดต่อได้ที่ไหน และมีหน่วยงานใดบ้างที่ดูแลรับผิดชอบ

สามารถศึกษาข้อมูลเพิ่มเติมเกี่ยวกับพ.ร.บ.นี้ได้จากเว็บไซต์ของหลากหลายหน่วยงานที่มีส่วนเกี่ยวข้องและรับผิดชอบ อาทิ

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

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

๑.๓ ความรู้ด้านภัยร้ายจากอินเทอร์เน็ต www.catcyfence.com

ขอบคุณครับ