
# พระราชบัญญัติ

## ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒)

พ.ศ. ๒๕๖๐

---

**Presented by Asst.Prof.Nitiporn Vonnasopon**

# พ.ร.บ. คอมพิวเตอร์ มีกี่ฉบับ

**ประเทศไทย** มี พ.ร.บ. คอมพิวเตอร์ มาแล้ว **2** ฉบับ คือ **ฉบับแรก ปี 2550** และ **ฉบับสอง ปี 2560** โดย **พ.ร.บ. คอมพิวเตอร์ฉบับล่าสุด คือ ฉบับปี 2560**

**ความแตกต่างสำคัญ**ระหว่างฉบับปี 2560 กับ 2550 คือ แก้ไขมิให้ **"ความผิดหมิ่นประมาท"** เป็นความผิดตาม พ.ร.บ คอมพิวเตอร์ อีกต่อไป

เพราะในอดีต **ความผิดหมิ่นประมาท** ถือว่าเข้าข่ายผิด พ.ร.บ. คอมพิวเตอร์ ซึ่งกฎหมายระบุว่า ไม่สามารถยอมความได้ ดังนั้นแม้ต่อมา คู่ความจะเจรจายอมความสำเร็จ หรืออยากถอนฟ้อง ศาลก็ไม่สามารถใช้ดุลพินิจที่จะไม่ลงโทษคู่ความได้ ส่งผลให้มีคดีฟ้องร้องขึ้นศาลจำนวนมากและเกิดปัญหาทางปฏิบัติ

เพื่อแก้ปัญหาดังกล่าว จึงมีการนำ **"ความผิดหมิ่นประมาท"** ออกจาก พรบ คอมพิวเตอร์ แต่ไปบังคับใช้ด้วยประมวลกฎหมายอาญาแทน ทำให้การบังคับใช้กฎหมายมีประสิทธิภาพมากขึ้น

# กฎหมายดิจิทัล ในประเทศไทย

- สร้างความเชื่อมั่น
- โครงสร้างพื้นฐาน และการขับเคลื่อน

ETDA สพธอ www.etda.or.th | กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม

## 2001

**พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544**
รองรับสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ และลายมือชื่ออิเล็กทรอนิกส์

## 2007

**พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550**
กำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

## 2008

**พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551**
รองรับในเรื่องตราประทับอิเล็กทรอนิกส์ และเอกสารซึ่งเป็นสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์มาใช้แทนต้นฉบับได้

## 2010

**พ.ร.บ. องค์กรจัดสรรคลื่นความถี่และกำกับการประกอบกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคม พ.ศ. 2553**
จัดตั้งองค์กรทำหน้าที่จัดสรรคลื่นความถี่และกำกับการประกอบกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคม

## 2016

**พ.ร.บ.ปรับปรุงกระทรวง ทบวง กรม (ฉบับที่ 17) พ.ศ. 2559**
ปรับโครงสร้างกระทรวงไอซีทีเป็นกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และจัดตั้งสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.)

## 2017

**พ.ร.บ.การพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. 2560**
ให้มีคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ, จัดตั้งกองทุนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม, และจัดตั้งสำนักงานส่งเสริมเศรษฐกิจดิจิทัล (depa) ให้เกิดการพัฒนาอุตสาหกรรมและนวัตกรรมดิจิทัล

**พ.ร.บ. องค์กรจัดสรรคลื่นความถี่ฯ (ฉบับที่ 2) พ.ศ. 2560**
ปรับปรุงโครงสร้างองค์กรและอำนาจหน้าที่รองรับแนวทางการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม

**พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560**
กำหนดฐานความผิดขึ้นใหม่และแก้ไขเพิ่มเติมฐานความผิดเดิม รวมทั้งปรับปรุงกระบวนการและหลักเกณฑ์ในการระงับหรือลบข้อมูล

## 2019

**พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562**
ดูแลบริการที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ป้องกัน รับมือ และลดความเสี่ยงจากภัยไซเบอร์ได้

**พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562**
กำหนดมาตรฐานในการดูแลข้อมูลส่วนบุคคล รักษาสิทธิของเจ้าของข้อมูล และเปิดโอกาสให้พัฒนานวัตกรรมการใช้ข้อมูลในการขับเคลื่อนเศรษฐกิจได้อย่างถูกต้อง

**พ.ร.บ.สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2562**
ยกระดับการทำงานของ ETDA ในการส่งเสริม สนับสนุน และพัฒนาธุรกรรมออนไลน์และอีคอมเมิร์ซ

**พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 3) พ.ศ. 2562**
นำหลักการUN e-Communication มาปรับปรุงให้การทำสัญญาในรูปแบบอิเล็กทรอนิกส์ครบถ้วนยิ่งขึ้น

**พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 4) พ.ศ. 2562**
รองรับสถานะทางกฎหมายในการใช้งานระบบพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital ID)

**พ.ร.บ.สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย พ.ศ. 2562**
จัดตั้งสภาความร่วมมือระหว่างภาครัฐและเอกชน ส่งเสริมการใช้เทคโนโลยีดิจิทัลพัฒนาประเทศ

**พ.ร.บ. องค์กรจัดสรรคลื่นความถี่ฯ (ฉบับที่ 3) พ.ศ. 2562**
กำหนดสิทธิในการเข้าใช้วงโคจรดาวเทียม รวมทั้งกำหนดเรื่องเลขหมายโทรศัพท์ฉุกเฉินแห่งชาติ

**พ.ร.บ.การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562**
กำหนดแผนพัฒนารัฐบาลดิจิทัล และการจัดทำบริการสาธารณะในรูปแบบดิจิทัลเพื่อการพัฒนาประเทศ

# กฎหมายดิจิทัลในประเทศไทย

- สร้างความเชื่อมั่น
- โครงสร้างพื้นฐานและการขับเคลื่อน

ETDA สพธอ www.etda.or.th | กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม

## 2001

**พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544**
รองรับสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ และลายมือชื่ออิเล็กทรอนิกส์

## 2007

**พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550**
กำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

## 2008

**พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551**
รองรับในเรื่องตราประทับอิเล็กทรอนิกส์และเอกสารซึ่งเป็นสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์มาใช้แทนต้นฉบับได้

## 2010

**พ.ร.บ. องค์กรจัดสรรคลื่นความถี่และกำกับการประกอบกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคม พ.ศ. 2553**
จัดตั้งองค์กรทำหน้าที่จัดสรรคลื่นความถี่และกำกับการประกอบกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคม

## 2016

**พ.ร.บ.ปรับปรุงกระทรวง ทบวง กรม (ฉบับที่ 17) พ.ศ. 2559**
ปรับโครงสร้างกระทรวงไอซีทีเป็นกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และจัดตั้งสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.)

## 2017

**พ.ร.บ.การพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. 2560**
ให้มีคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ, จัดตั้งกองทุนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม, และจัดตั้งสำนักงานส่งเสริมเศรษฐกิจดิจิทัล (depa) ให้เกิดการพัฒนาอุตสาหกรรมและนวัตกรรมดิจิทัล

**พ.ร.บ. องค์กรจัดสรรคลื่นความถี่ฯ (ฉบับที่ 2) พ.ศ. 2560**
ปรับปรุงโครงสร้างองค์กรและอำนาจหน้าที่รองรับแนวทางการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม

**พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560**
กำหนดฐานความผิดขึ้นใหม่และแก้ไขเพิ่มเติมฐานความผิดเดิม รวมทั้งปรับปรุงกระบวนการและหลักเกณฑ์ในการระงับหรือลบข้อมูล

## 2019

**พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562**
ดูแลบริการที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ป้องกัน รับมือ และลดความเสี่ยงจากภัยไซเบอร์ได้

**พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562**
กำหนดมาตรฐานในการดูแลข้อมูลส่วนบุคคล รักษาสิทธิของเจ้าของข้อมูล และเปิดโอกาสให้พัฒนานวัตกรรมการใช้ข้อมูลในการขับเคลื่อนเศรษฐกิจได้อย่างถูกต้อง

**พ.ร.บ.สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2562**
ยกระดับการทำงานของ ETDA ในการส่งเสริม สนับสนุน และพัฒนาธุรกรรมออนไลน์และอีคอมเมิร์ซ

**พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 3) พ.ศ. 2562**
นำหลักการUN e-Communication มาปรับปรุงให้การทำสัญญาในรูปแบบอิเล็กทรอนิกส์ครบถ้วนยิ่งขึ้น

**พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 4) พ.ศ. 2562**
รองรับสถานะทางกฎหมายในการใช้งานระบบพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital ID)

**พ.ร.บ.สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย พ.ศ. 2562**
จัดตั้งสภาความร่วมมือระหว่างภาครัฐและเอกชน ส่งเสริมการใช้เทคโนโลยีดิจิทัลพัฒนาประเทศ

**พ.ร.บ. องค์กรจัดสรรคลื่นความถี่ฯ (ฉบับที่ 3) พ.ศ. 2562**
กำหนดสิทธิในการเข้าใช้วงโคจรดาวเทียม รวมทั้งกำหนดเรื่องเลขหมายโทรศัพท์ฉุกเฉินแห่งชาติ

**พ.ร.บ.การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562**
กำหนดแผนพัฒนารัฐบาลดิจิทัล และการจัดทำบริการสาธารณะในรูปแบบดิจิทัลเพื่อการพัฒนาประเทศ

## วันที่ ๒๓ มกราคม พ.ศ. ๒๕๖๐

สมเด็จพระเจ้าอยู่หัวมหาวชิราลงกรณ บดินทรเทพยวรางกูร มีพระราชโองการโปรดเกล้าฯ ให้ประกาศว่า โดยที่เป็นการสมควรแก้ไขเพิ่มเติมกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ จึงทรงพระกรุณาโปรดเกล้าฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของ สภานิติบัญญัติแห่งชาติ ดังต่อไปนี้

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐”

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งร้อยยี่สิบวันนับแต่วันประกาศในราชกิจจานุเบกษา เป็นต้นไป

มาตรา ๓ ให้ยกเลิกความในมาตรา ๔ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๔ ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรักษาการตามพระราชบัญญัตินี้ และให้มีอำนาจแต่งตั้งพนักงานเจ้าหน้าที่กับออกกฎกระทรวงและประกาศเพื่อปฏิบัติการตามพระราชบัญญัตินี้กฎกระทรวงและประกาศนั้น เมื่อได้ประกาศในราชกิจจานุเบกษาแล้วให้ใช้บังคับได้” เป็นต้น...

# ความเป็นมา...ของ

## พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

- **เมื่อวันที่ 16 ธ.ค. 2559 ที่ประชุมสภานิติบัญญัติแห่งชาติ มีมติ เห็นด้วย 168 ไม่ เห็นด้วย 0 งดออกเสียง 5 ให้ผ่านร่างพระราชบัญญัติว่าด้วยการกระทำความผิด เกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ...) พ.ศ. ... โดยรอประกาศใช้เป็นกฎหมายต่อไปใน 120 วัน**
- **พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ.2560 หรือ พ.ร.บ. คอมพิวเตอร์ฉบับใหม่ ได้รับการประกาศในราชกิจจานุเบกษาเมื่อวันที่ 23 มกราคม 2560 ซึ่งกฎหมายจะมีผลบังคับใช้อย่างเป็นทางการในอีก 120 วัน**
- **ในระหว่างนี้กระทรวงดีอี จะทำหน้าที่ยกร่างกฎกระทรวงมาใช้งานร่วมกับ พ.ร.บ. คอมพิวเตอร์ เนื่องจากข้อกฎหมายหลายประเด็นมีการระบุในเรื่องของเนื้อหาที่กว้าง เกินไป การที่มีกฎกระทรวงและกฎหมายลูกเข้ามาใช้ประกอบ จะทำให้การตีความไป จนถึงการบังคับใช้ของกฎหมายมีความละเอียดมากยิ่งขึ้น**

## โครงสร้างของเนื้อหากฎหมายมีลักษณะคล้ายคลึงฉบับเดิม โดยมีสาระสสำคัญที่ต่างไปบ้าง

พ.ร.บ. ฉบับเดิม ใช้บังคับเป็นเวลากว่า ๑๐ ปี โดยที่ผ่านมาพบว่า กฎหมายมีปัญหาในการตีความ จนกระทบกับการบังคับใช้ เช่น การนำฐานความผิดที่ใช้กับเรื่องฉ้อโกงปลอมแปลงทางออนไลน์ ไปใช้กับ การหมิ่นประมาท ทำให้กระทบต่อสิทธิเสรีภาพในการแสดงความ คิดเห็น จนทำให้เกิดการโจมตีจากประชาคมโลกและเกิดกระแสสังคมเรียกร้องหลักประกันสิทธิเสรีภาพในการแสดงความคิดเห็นขึ้น กอปร กับเพื่อเป็นการปรับปรุงกฎหมายให้เท่าทันกับเทคโนโลยีและภัยคุกคามที่เปลี่ยนแปลงไป

# วัตถุประสงค์/เหตุผลการแก้ไข

1. ให้รัฐมนตรีว่าการกระทรวงดิจิทัลฯ รักษาการตามพระราชบัญญัติ
2. บทบัญญัติบางประการที่ไม่เหมาะสมต่อการป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในปัจจุบัน ซึ่งมีรูปแบบการกระทำความผิดที่มีความซับซ้อนมากขึ้น เช่น เพิ่มเติมฐานความผิดและกำหนดโทษผู้ส่งข้อมูลคอมพิวเตอร์ หรือจดหมายอิเล็กทรอนิกส์ แก่บุคคลอื่น
3. มาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งการเฝ้าระวังและติดตามสถานการณ์ด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศของประเทศ สมควรปรับปรุงบทบัญญัติในส่วนที่เกี่ยวกับผู้รักษากฎหมาย
4. กำหนดโทษของความผิดดังกล่าว การปรับปรุงกระบวนการและหลักเกณฑ์ใน การระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์

RUTS RAJAMANGALA UNIVERSITY OF TECHNOLOGY SRIVIJAYA

LA

# 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

# หลักการใหม่ ใน ร่างแก้ไข พ.ร.บ.คอมพิวเตอร์ฯ

| | พ.ร.บ.คอมพิวเตอร์ฯ พ.ศ. 2550 | ร่างแก้ไข พ.ร.บ.คอมพิวเตอร์ฯ ฉบับปี 2559 |
|---|---|---|
| ความผิดฐานส่งสแปมโดยปกปิดแหล่งที่มา | ส่งสแปม ถ้าไม่เปิดช่องให้บอกเลิก เพิ่มโทษปรับเป็น 200,000 บาท | เพิ่มโทษปรับสองเท่า หากไม่เปิดช่องให้บอกเลิกได้ |
| ความผิดต่อระบบความมั่นคง | ไม่มีโทษเฉพาะ | เพิ่มโทษการเจาะระบบ การทำลายระบบ ที่เกี่ยวกับความมั่นคงของประเทศ |
| การนำเข้าข้อมูลเท็จตามมาตรา 14(1) | เปิดช่องให้ตีความเอาผิดกับการหมิ่นประมาทออนไลน์ | มุ่งเอาผิดการกระทำต่อทรัพย์สินชัดเจนขึ้น แต่ยังเปิดช่องให้ตีความเอาผิดกับการหมิ่นประมาทได้อยู่ |
| การนำเข้าข้อมูลเท็จที่กระทบต่อความมั่นคง | เอาผิดกับการนำเข้าข้อมูลเท็จที่น่าจะ...<br>1) เสียหายต่อความมั่นคงของประเทศ<br>2) ก่อให้เกิดความตื่นตระหนกแก่ประชาชน | เอาผิดกับการนำเข้าข้อมูลเท็จที่น่าจะ...<br>1) เสียหายต่อความมั่นคงของประเทศ<br>2) เสียหายต่อความปลอดภัยสาธารณะ<br>3) เสียหายต่อความมั่นคงทางเศรษฐกิจ<br>4) ก่อให้เกิดความตื่นตระหนกแก่ประชาชน |
| ผู้ให้บริการที่ไม่ลบเนื้อหาผิดกฎหมาย | รับผิดต่อเมื่อ "จงใจสนับสนุนหรือยินยอม" | รับผิดต่อเมื่อให้ความร่วมมือ ยินยอม หรือรู้เห็นเป็นใจ ถ้าได้รับแจ้งเตือนแล้วลบออกไม่ต้องรับโทษ |

| | พ.ร.บ.คอมพิวเตอร์ฯ พ.ศ. 2550 | ร่างแก้ไข พ.ร.บ.คอมพิวเตอร์ฯ ฉบับปี 255 |
|---|---|---|
| การเผยแพร่ภาพตัดต่อ | ผิดเฉพาะภาพคนที่ยังมีชีวิต | ภาพคนตาย ก็อาจผิดได้ |
| ให้ทำลายภาพตัดต่อ | ไม่ได้เขียนไว้ | ให้ยึดและทำลายภาพตัดต่อได้ |
| เนื้อหาที่จะถูก Block | 1) เป็นความผิดต่อความมั่นคงของประเทศ<br>2) เป็นความผิดเกี่ยวกับการก่อการร้าย<br>3) ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดี | 1) เป็นความผิดตาม พ.ร.บ.คอมพิวเตอร์ฯ ทุกประเภท<br>2) เป็นความผิดต่อความมั่นคงของประเทศ<br>3) เป็นความผิดเกี่ยวกับการก่อการร้าย<br>4) เป็นความผิดต่อกฎหมายอื่น ที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดี และเจ้าหน้าที่ตามกฎหมายนั้นร้องขอ<br>5) ไม่เป็นความผิดต่อกฎหมาย แต่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดี และคณะกรรมการกลั่นกรองมีมติเอกฉันท์ |
| คณะกรรมการตามกฎหมายนี้ | ไม่มี | มีคณะกรรมการสองชุด<br>1) คณะกรรมการเปรียบเทียบปรับ สำหรับความผิดที่มีแต่โทษปรับหรือโทษจำคุกไม่เกินสองปี<br>2) คณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์ที่ไม่ผิดกฎหมายแต่ให้บล็อคได้ |
| ผู้ให้บริการมีหน้าที่เก็บข้อมูลการใช้งาน | เก็บไว้ไม่น้อยกว่า 90 วัน กรณีจำเป็นสั่งให้เก็บเพิ่มได้ไม่เกิน 1 ปี | เก็บไว้ไม่น้อยกว่า 90 วัน กรณีจำเป็นสั่งให้เก็บเพิ่มได้ไม่เกิน 2 ปี |
| เงินพิเศษสำหรับเจ้าพนักงาน | ไม่มี | มีเงินเพิ่มสำหรับผู้ดำรงตำแหน่งที่มีเหตุพิเศษ |

LA

W


รู้จัก W.S.U. ฉบับที่ 2
คอมพิวเตอร์ฯ 2560
1 พ.ร.บ.คอม
ไม่ได้กำหนดเรื่อง
SINGLE GATEWAY
2 ไม่ทำให้
เน็ตช้า
3 ยังท่องเว็บไทยและ
เว็บต่างประเทศ
ได้ตามปกติ
4 ได้มีการตัด
หมิ่นประมาท
ออกไปโดยชัดเจน
5 สร้างความ
สมดุล
6 เจ้าหน้าที่
ไม่มีอำนาจ
เข้าถึงตามใจชอบ

# ภาพรวม แก้ไขเพิ่มเติม
# พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

## หมวด 1 ความผิดเกี่ยวกับคอมพิวเตอร์

**แก้ไขเพิ่มเติม**

ม.11 ความผิดฐานส่งสแปมโดยปกปิดแหล่งที่มา

ม.12 เพิ่มโทษการเจาะระบบ การทาลายระบบที่เกี่ยวกับความมั่นคง

ม.14 มุ่งเอาผิดการกระทาต่อทรัพย์สินชัดเจนขึ้น ไม่ให้ตีความเอาความผิดกับการหมิ่นประมาท เอาความผิดการนาเข้าข้อมูลเท็จที่น่าจะทำให้เกิดความเสียหายต่อความมั่นคงฯ ประเทศ สาธารณะและเศรษฐกิจ/ก่อความตื่นตระหนก

ม.15 ผู้ให้บริการที่ไม่ลบเนื้อหาผิดกฎหมาย

ม.16 การเผยแพร่ภาพตัดต่อ ภาพคนตาย ก็อาจ ผิดได้

ม.16 16/1 ให้ยึดและทาลายภาพตัดต่อได้

**หน้าที่ของผู้ให้บริการ มาตรา 26**
เก็บข้อมูลจราจรไม่น้อยกว่า 90 วัน
แต่ไม่เกิน 2 ปี เป็นกรณีพิเศษเฉพาะราย/เฉพาะคราว

## หมวด 2 พนักงานเจ้าหน้าที่

แก้ไขเพิ่มเติม อำนาจหน้าที่ (มาตรา 18)
(1) มีหนังสือ/เรียกเพื่อให้ถ้อยคา/เอกสาร
(2) เรียกข้อมูลจราจร
(3) สั่งให้ส่งมอบข้อมูลที่อยู่ในครอบครอง
(4) ทำสำเนาข้อมูล
(5) สั่งให้ส่งมอบข้อมูล/อุปกรณ์
(6) ตรวจสอบ/เข้าถึง
(7) ถอดรหัสลับ
(8) ยึด/อายัดระบบ

**แก้ไขเพิ่มเติมการ block เว็บไซต์**
**ตามมาตรา 20** เพิ่มเติมความผิด ให้ครอบคลุมกรณีต่าง ๆ มากขึ้น เช่น ความผิดเกี่ยวกับทรัพย์สินทางปัญญา ความผิดที่ขัดต่อความสงบเรียบร้อย/ ศีลธรรม
แต่งตั้งคณะกรรมการกลั่นกรองพิจารณาการปิดกั้น

# พ.ร.บ.(ฉบับที่ 2) พ.ศ. 2560

## ให้มีการร่างประกาศ/ระเบียบ เพื่อให้เห็นแนวทางการใช้บังคับ

| | |
|---|---|
| มาตรา 11<br>กำหนดให้ชัดเจนว่าอะไรคือ สแปม<br>หรือจดหมายอิเล็กทรอนิกส์ ที่ทำให้เดือดร้อนรำคาญ | ประกาศ เรื่อง หลักเกณฑ์เกี่ยวกับลักษณะและวิธีการลงลักษณะและปริมาณของข้อมูลคอมพิวเตอร์ ซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อน รำคาญแก่ผู้รับ และลักษณะอันเป็นการปฏิเสธการตอบรับได้โดยง่าย พ.ศ. .. |
| มาตรา 15<br>เมื่อผู้ให้บริการจำเป็นต้องระงับการเผยแพร่เว็บไซต์ และยกเว้นโทษให้กับผู้ให้บริการ | ประกาศ เรื่อง ขั้นตอนการแจ้งเตือนการระงับการทำให้แพร่หลายของข้อมูล คอมพิวเตอร์ และการนำข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์ พ.ศ. .... |
| มาตรา 17/1<br>วางกลไกเปรียบเทียบความผิดสาหรับโทษสถานเบา | ประกาศ เรื่อง แต่งตั้งคณะกรรมการเปรียบเทียบ ตาม พ.ร.บ. ว่าด้วย การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... |
| มาตรา 20<br>การระงับการเผยแพร่ ต้องตรวจสอบ การใช้อำนาจโดยศาล<br>เฉพาะเนื้อหาที่ขัดต่อการสงบเรียบร้อย<br>(ที่กระทบต่อสังคมในวงกว้าง) ต้องมีคณะกรรมการกลั่นกรอง (อย่างน้อยต้องมีเอกชนจากสายสื่อ, สิทธิมนุษยชน ไอที) อีกชั้นหนึ่ง ก่อนให้ศาลตรวจสอบ ถวงดุลการทำหน้าที่ | ประกาศ เรื่อง หลักเกณฑ์ ระยะเวลา และวิธีการปฏิบัติสำหรับการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ของพนักงานเจ้าหน้าที่หรือ ผู้ให้บริการ พ.ศ. ....<br>ประกาศ เรื่อง แต่งตั้งคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์ ตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ... |
| มาตรา 21<br>กำหนดชุดคาสั่งไม่พึ่งประสงค์ ที่ใช้ประโยชน์ได้ เช่น ใช้ตรวจสอบช่องโหวงยอมไม่ผิดกฎหมาย | ประกาศ เรื่อง กำหนดรายชื่อ ลักษณะ หรือรายละเอียดของชุดคำสั่ง ไม่พึ่งประสงค์ ซึ่งอาจนำมาใช้เพื่อป้องกันหรือแก้ไขชุดคำสั่งไม่พึ่งประสงค์ ก็ได้ (อาจมีการจัดทำในภายหลัง) |

# มาตรา 11

**กำหนดให้ชัดเจนว่าอะไรคือ สแปมหรือจดหมายอิเล็กทรอนิกส์ ที่ทำให้เดือด ร้อนรำคาญ และเพิ่มโทษพวก spam หรือข้อมูลอิเล็กทรอนิกส์ ที่ทำให้เดือดร้อนรำคาญ โดยเฉพาะในเชิงพาณิชย์พวกโฆษณาอะไรต่าง ๆ**

| พรบ. พ.ศ. 2550 มาตรา 11 | พรบ.(ฉบับที่ 2) พ.ศ. 2560 มาตรา 11 |
|---|---|
| ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ แก่บุคคลอื่น โดยปกปิดหรือปลอมแปลงแหล่งที่มา ของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข<br><br>ระวางโทษปรับไม่เกินหนึ่งแสนบาท | ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่น<br>• ลักษณะเป็นการก่อให้เกิดความเดือดร้อนรำคาญ แก่ผู้รับ ข้อมูลคอมพิวเตอร์<br>• หรือจดหมายอิเล็กทรอนิกส์ โดยไม่เปิดโอกาสให้ผู้รับสามารถ บอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย<br><br>ระวางโทษปรับไม่เกินสองแสนบาท |
| ไม่เปิดโอกาศให้คนรับอีเมล<br>กดยกเลิกการ<br>รับอีเมล | **รมว. ดีอี**<br>ออกประกาศกาหนดลักษณะและวิธีการส่ง รวมทั้งลักษณะและปริมาณของข้อมูลคอมฯ/ จดหมายอิเล็กทรอนิกส์ ซึ่งไม่เป็นการก่อให้เกิด ความเดือดร้อนราคาญแก่ผู้รับ และลักษณะอัน เป็นการบอกเลิกหรือแจ้งความประสงค์เพื่อ ปฏิเสธการตอบรับได้โดยง่าย |

# มาตรา12
## ความผิดต่อข้อมูล/ ระบบความมั่นคง

| พรบ.คอมพิวเตอร์ฯ พ.ศ.2550 | พรบ.คอมพิวเตอร์ฯ (ฉบับที่ 2) พ.ศ.2560 |
|---|---|
| ก่อให้เกิดความเสียหายต่อข้อมูล/ ระบบเกี่ยวกับความมั่นคง ลงโทษจาคุก 3-15 ปี และปรับหนึ่งหมื่น - 3 แสนบาท | กรณีกระทำต่อข้อมูลคอมพิวเตอร์หรือ ระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้าง พื้นฐานอันเป็นประโยชน์สาธารณะ |
| เป็นเหตุให้ผู้อื่นถึงแก่ความ ตาย ลงโทษจาคุก 10-20 ปี | เพิ่มโทษการเจาะระบบ การทำลายระบบที่เกี่ยวกับความมั่นคงของประเทศ |

# มาตรา 12

**ยกเลิก และให้กาหนดขึ้นใหม่ เน้นเกี่ยวกับการปกป้องโครงสร้างพื้นฐานสาคัญของประเทศ**

| พรบ. พ.ศ. 2550 มาตรา 12 | พรบ. (ฉบับที่ 2) พ.ศ. 2560 มาตรา 12 |
|---|---|
| ถ้าการกระทำความผิดตามมาตรา 9 หรือ10<br>(1) ก่อให้เกิดความเสียหายแก่ประชาชน (โทษ 10ปี 2แสนบาท)<br>(2) เกิดความเสียหายต่อข้อมูล/ระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความ ปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจ/การบริการ สาธารณะ (โทษตั้งแต่ 3 ปีถึง 15 ปี ปรับตั้งแต่ 6หมื่นถึง 3 แสนบาท)<br><br>ถ้าการกระทำความผิดตาม(2) เป็นเหตุให้ผู้อื่นถึงแก่ความตาย (โทษจาคุกตั้งแต่ 10 ปีถึง 20 ปี)<br><br>ระวางโทษที่สูงสุดถึง 20 ปี | ➢ ถ้าการกระทำความผิดตามมาตรา 5 , 6 , 7 , 8 หรือ 11 เป็นการกระทำต่อข้อมูล/ระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคง ปลอดภัยของประเทศฯ<br>➢ ถ้าการกระทำความผิดตามวรรคหนึ่งเป็นเหตุให้เกิดความเสียหายต่อ ข้อมูล/ระบบคอมพิวเตอร์ดังกล่าว (ต้องระวางโทษจาคุกตั้งแต่หนึ่งปีถึง 10 ปี และปรับตั้งแต่สองหมื่นบาทถึงสองแสนบาท)<br>➢ ถ้าการกระทำความผิดตามมาตรา 9 หรือ 10 เป็นการกระทาต่อข้อมูล/ระบบคอมพิวเตอร์ตามวรรคหนึ่ง (ต้องระวางโทษจาคุกตั้งแต่ 3ถึง 5 ปีปรับ 6 หมื่นถึง 3แสนบาท)<br>➢ ถ้าการกระทำความผิดตามวรรคหนึ่งถึงสามถ้าการกระทาความผิดตามมาตรา 9 หรือ 10 โดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึงแก่ความตาย(ต้องระวางโทษจาคุกตั้งแต่ห้าปีถึงยี่สิบปี และปรับตั้งแต่หนึ่งแสนบาทถึงสี่แสนบาท”)<br>➢ เพิ่มเติม 12/1 ถ้าการกระทาความผิดตามมาตรา 9 หรือ 10 เป็นเหตุ ให้เกิดอันตราย/ทรัพย์สินผู้อื่น และ การกระทำนั้นโดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึง แก่ความตาย (ระวางโทษ 5 ถึง 20 ปี/ปรับ 1 ถึง 4 แสนบาท) |

# แก้ไขในมาตรา 12 และ 12/1
## สรุปอัตราโทษที่ปรับปรุงใหม่

| มาตรา | ฐานความผิด | อัตราโทษ |
|---|---|---|
| ม. 12 | ❖ เมื่อการแฮกข้อมูลหรือระบบ, ดักรับ, Spam, เปิดเผยมาตรการป้องกัน ทำต่อโครงสร้างสำคัญ เช่น ไฟฟ้า ประปา<br>หากเกิดความเสียหายตามมาด้วย<br>❖ เมื่อแก้ไขเปลี่ยนแปลงข้อมูล, ขัดขวางหรือชะลอการทำงานระบบ ทำต่อ โครงสร้างสำคัญ เช่น ไฟฟ้า ประปา<br>ไม่เจตนา แต่ทำให้คนตาย | โทษ 1-7 ปี ปรับ 10,000 – 140,000<br>โทษ 1-10 ปี ปรับ 20,000 – 200,000<br>โทษ 3-15 ปี ปรับ 60,000 – 300,000<br>โทษ 5-20 ปี ปรับ 100,000 – 400,000 |
| ม. 12/1 | ❖ แก้ไขเปลี่ยนแปลง, ทำให้ระบบทำงานไม่ปกติ ทำให้บาดเจ็บ ทรัพย์สินเสียหาย<br>ไม่เจตนา แต่ทำให้คนตาย | ไม่เกิน 10 ปี ปรับไม่เกิน 200,000 โทษ<br>5-20 ปี ปรับ 100,000 – 400,000 |

# มาตรา 13
## การเผยแพร่ชุดคำสั่ง มีการเพิ่มเติม

| พรบ. ปี 2550 มาตรา 13 | พรบ. (ฉบับที่ 2) พ.ศ. 2560 มาตรา 13 |
|---|---|
| ผู้ใดจำหน่ายหรือเผยแพร่ชุดคาสั่งที่ จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือ ในการกระทำความผิดตาม มาตรา 5 มาตรา 6 มาตรา 7 มาตรา 8 มาตรา 9 มาตรา 10 หรือมาตรา 11<br><br>**ระวางโทษจาคุกไม่เกิน 1 ปี หรือปรับไม่เกิด 2 หมื่นบาท หรือทั้งจาทั้งปรับ** | ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะ<br>❑ เพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา 12 (1)/(3) (ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาทหรือทั้งจำทั้งปรับ)<br>❑ เพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา 5 มาตรา 6 มาตรา 7 มาตรา 8 มาตรา 9 มาตรา 10 หรือมาตรา 11 หากผู้นำไปใช้ได้กระทำความผิดตาม มาตรา 12 วรรคหนึ่งหรือวรรคสาม หรือต้องรับผิดตามมาตรา 12 วรรคสองหรือวรรคสี่ หรือมาตรา 12/1 ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งดังกล่าวจะต้องรับผิดทางอาญาตาม ความผิดที่มีกำหนดโทษสูงขึ้นด้วยก็เฉพาะเมื่อตนได้รู้หรืออาจเล็งเห็นได้ว่าจะเกิดผลเช่นที่ เกิดขึ้นนั้น<br>❑ เพื่อนำไปใช้เป็นเครื่องมือในการกระทาความผิดตามมาตรา 12 (1)/(3) หากผู้นำไปใช้ได้กระทำความผิดตามมาตรา 12 (1)/(3) หรือต้องรับผิดตาม มาตรา 12 (2)/(4) หรือมาตรา 12/1 ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งดังกล่าว ต้องรับผิดทางอาญาตามความผิดที่มีกำหนดโทษสูงขึ้นนั้นด้วย<br><br>ในกรณีที่ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งผู้ใดต้องรับผิดตามวรรคสามหรือวรรคสี่ด้วย ให้ผู้นั้นต้องรับโทษที่มีอัตราโทษสูงที่สุดแต่กระทงเดียว |

# มาตรา 13

เอาผิดกับคนที่นำชุดคำสั่งไปจำหน่าย คือหากนำไปใช้แล้วเกิดความเสียหายกับความมั่นคงปลอดภัยในเรื่องความมั่นคง ใครที่นำชุดคำสั่งนี้ไปจำหน่าย ทั้งที่รู้อยู่แล้วว่าชุดคำสั่งเหล่านี้เมื่อนำไปใช้แล้ว มันจะมีผลอย่างนั้น ให้รับโทษ โดยเฉพาะหากนำชุดคำสั่งนี้ไปจำหน่ายแล้วมีการนำไปใช้ จนทำให้มีคนบาดเจ็บ คนเสียชีวิต โทษก็จะมีผลสูงมากขึ้น

| ฐานความผิด | อัตราโทษ |
|---|---|
| <u>วรรค 1</u> จำหน่ายชุดคำสั่ง/เผยแพร่ไปใช้เป็น เครื่องมือกระทำผิด ต่อข้อมูลหรือระบบ ทำต่อโครงสร้างสำคัญ เช่น ไฟฟ้า ประปา | โทษ 2 ปี ปรับไม่เกิน 40,000 บาท |
| <u>วรรค 2</u> จำหน่ายชุดคำสั่ง/เผยแพร่ไปใช้เป็นเครื่องมือกระทำผิด แฮกข้อมูลหรือระบบ, ดักรับ, Spam,เปิดเผยมาตรการป้องกัน | รับผิดทางอาญาตามความผิดที่มีกาหนดโทษสูงขึ้นด้วย |
| <u>วรรค 3</u> เมื่อนำไปใช้เป็นเครื่องมือกระทำความผิด | ตามมาตรา 12 (1)/(3) หากผู้นำไปใช้ได้กระทำความผิดตามมาตรา 12 (1)/(3) หรือต้องรับผิด ตามมาตรา 12 (2)/(4) หรือมาตรา 12/1 |
| <u>วรรค 4</u> ในกรณีที่ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่ง ผู้ใดต้องรับผิดตามวรรค 1 หรือวรรค 2 และตามวรรค 3 หรือวรรค 4 ด้วย | ให้ผู้นั้นต้องรับโทษที่มีอัตราโทษสูงที่สุดแต่กระทงเดียว |

# มาตรา 14

**มีเพิ่มเติม/แก้ไขในมาตรานี้ โดยเน้นประเด็นการหมิ่นประมาทออนไลน์**

| | พรบ.คอมพิวเตอร์ฯ พ.ศ.2550 | พรบ.คอมพิวเตอร์ฯ (ฉบับที่ 2) พ.ศ.2560 |
|---|---|---|
| การนำเข้าข้อมูลเท็จ ตามมาตรา 14(1) | เปิดช่องให้ตีความเอาผิด กับการหมิ่นประมาทบนออนไลน์ | ม.14(1) โดยทุจริตหรือโดยหลอกลวงนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน มุ่งเอาผิดการกระทำต่อทรัพย์สินชัดเจนขึ้น และยังเปิดช่องให้ตีความเอาผิด กับการบิดเบือนได้<br><br>อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา |

# มาตรา 14
## รายละเอียดในมาตรานี้

| พรบ. ปี 2550 มาตรา 14 | พรบ. (ฉบับที่ 2) พ.ศ. 2560 มาตรา 14 |
|---|---|
| กระทำความผิดที่ระบุไว้ ดังต่อไปนี้ (มี 5 องค์ประกอบ)<br>มาตรา 14 (1) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน<br><br>มาตรา 14 (2) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน | มาตรา 14(1) โดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่ว่าทั้งหมด หรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา<br><br>มาตรา 14(2) ต้องเป็นกรณีที่น่าจะเกิดความเสียหาย คือมีการนำเข้าสู่ระบบ คอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์นั้นเป็นเท็จ คือนำข้อมูลอันเป็นเท็จเข้าไปในระบบ โดยประการที่น่าจะก่อให้เกิดความเสียหายต่อการรักษาความ มั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ฯ ความมั่นคง ทางเศรษฐกิจความปลอดภัยของประเทศในเรื่องโครงสร้างพื้นฐาน หรือประโยชน์สาธารณะ |
| มาตรา 14 (3), (4)และ(5) ยังเหมือนเดิม<br><br>จำคุกไม่เกิน 5 ปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ | ถ้าการกระทำความผิดตามวรรคหนึ่ง (1) มิได้กระทำต่อประชาชน แต่เป็นการกระทำต่อบุคคลใดบุคคลหนึ่ง ผู้กระทำผู้เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ดังกล่าวต้องระวางโทษจำคุก ไม่เกิน 3 ปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ และให้เป็นความผิดอันยอมความได้” |

# มาตรา 14

การนำข้อมูลเข้าระบบแล้วทำให้เกิดความเสียหาย กฎหมายที่ใช้อยู่ปัจจุบัน พบว่ามีการนำมาตรา 14 (1) ไป ใช้แจ้งความฐานหมิ่นประมาท คือนำเข้าข้อมูลอันเป็นเท็จที่ทำให้เกิดความเสียหายต่อผู้อื่น

| พรบ. ปี 2550 มาตรา 14 | พรบ. (ฉบับที่ 2) พ.ศ. 2560 มาตรา 14 |
|---|---|
| กระทำความผิดที่ระบุไว้ ดังต่อไปนี้ (มี 5 องค์ประกอบ)<br>(1) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่ง ข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมด หรือบางส่วน หรือข้อมูลคอมพิวเตอร์อัน เป็นเท็จ โดยประการที่น่าจะเกิดความเสียหาย แก่ผู้อื่นหรือประชาชน | ประเด็นที่แก้ไข มาตรา 14(1)<br>แก้ไขโดยเพิ่มคำว่า “โดยทุจริตหรือโดยหลอกลวง” เข้าไปจาก เดิมมาตรา 14 ของปี 2550 และ...ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอม .. และอันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา บิดเบือน เช่น บิดเบือนราคาหุ้นในตลาดหลักทรัพย์ฯ ที่ทำให้กลไกของตลาดหลักทรัพย์ผิดไป |
| (2) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่ง ข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศ หรือก่อให้เกิดความตื่นตระหนก แก่ประชาชน | ประเด็นที่แก้ไข มาตรา 14(2)<br>“นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่ น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน” |

# มาตรา 15

**ให้ยกเลิกความเดิมในมาตรานี้ และให้ใช้ความต่อไปนี้แทน**
**(กำหนดมาตรการในการคุ้มครองผู้ให้บริการ)**

| พรบ. ปี 2550 มาตรา 15 | พรบ. (ฉบับที่ 2) พ.ศ. 2560 มาตรา 15 |
|---|---|
| ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอม ให้มีการกระทำความผิดตามมาตรา 14 ใน ระบบคอมพิวเตอร์ ที่อยู่ในความควบคุมของ ตน ต้องระวางโทษเช่นเดียวกับผู้กระทำผิด ตามมาตรา 14 | ผู้ให้บริการผู้ใดให้ความร่วมมือ ยินยอม หรือรู้เห็นเป็นใจให้มีการกระทำความผิดตามมาตรา 14 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา 14<br>ให้รัฐมนตรีออกประกาศกำหนดขั้นตอนการแจ้งเตือน การระงับการทำให้แพร่หลายของข้อมูลคอมพิวเตอร์ และการนำข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์ |
| จำคุกไม่เกิน 5 ปี<br>หรือปรับไม่เกินหนึ่งแสนบาท<br>หรือทั้งจำทั้งปรับ | ถ้าผู้ให้บริการพิสูจน์ได้ว่าตนได้ปฏิบัติตามประกาศของรัฐมนตรีที่ออกตาม วรรคสอง “ผู้นั้นไม่ต้องรับโทษ”<br>สรุป ออกกฎกระทรวงว่า ไม่ผิด ถ้าเราไม่รู้ เราเป็นเพียงท่อผ่านข้อมูล ไม่ผิดตาม กฎหมาย จะผิดก็ต่อเมื่อ 2 กรณี คือ<br>1. เมื่อเราเป็นคนเลือกเอาข้อมูลเข้าไปใส่เอง<br>2. เมื่อมีแบบฟอร์มของกระทรวงดิจิทัลฯ ที่ระบุชื่อนามสกุล เหตุพิพาทของผู้ ร้องเรียนและใบแจ้งความกับเจ้าหน้าที่ตำรวจ ถ้าใครแจ้งเท็จก็โดนข้อหาไป แล้วส่งมา ให้ผู้ให้บริการ เจ้าของเฟซบุ๊ก หรือผู้ให้บริการแต่ละราย ซึ่งจะเป็นคนกำหนดเองว่า จะ เอาข้อมูลอันเป็นเท็จออกได้ภายในกี่วัน |

# พรบ. (ฉบับที่ 2) พ.ศ. 2560 มาตรา 15

| |
|---|
| **ประเด็นที่แก้ไข** แต่เดิมมาตรา 15 ของ พ.ศ.2550 เขียนไว้ว่า “ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มี การกระทำความผิดตามมาตรา 14 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา 14” |
| **พ.ร.บ. ฉบับใหม่ ..** “ผู้ให้บริการผู้ใดให้ความร่วมมือ ยินยอม หรือรู้เห็นเป็นใจให้มีการกระทำความผิดตามมาตรา 14 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษ เช่นเดียวกับผู้กระทำความผิดตามมาตรา 14 |
| ให้รัฐมนตรีออกประกาศกำหนดขั้นตอนการแจ้งเตือน การระงับการทำให้แพร่หลายของข้อมูลคอมพิวเตอร์ และการนำข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์ ถ้าผู้ให้บริการพิสูจน์ได้ว่าตนได้ปฏิบัติตามประกาศของรัฐมนตรีที่ออกตามวรรคสอง ผู้นั้นไม่ต้องรับโทษ” |

# มาตรา 16
## ให้ยกเลิกความเดิมในมาตรานี้ และให้ใช้ความต่อไปนี้แทน

| พรบ. ปี 2550 มาตรา 16 | พรบ. (ฉบับที่ 2) พ.ศ. 2560 มาตรา 16 |
|---|---|
| ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไป อาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ ที่ปรากฏ เป็น ภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้โดยประการที่น่าจะทำให้ผู้อื่นนั้น เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย<br><br>จำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ | ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูล คอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้นฯ ต้องระวางโทษจำคุกไม่เกินสามปี และปรับไม่เกินสองแสนบาท<br>ถ้าการกระทำตามวรรคหนึ่งเป็นการกระทำต่อภาพของผู้ตายและการกระทำนั้นน่าจะทำให้บิดา มารดา คู่สมรส หรือบุตรของผู้ตายเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง หรือได้รับความอับอาย ผู้กระทำต้องระวางโทษ ดังที่บัญญัติไว้ในวรรคหนึ่ง<br>ถ้าการกระทำตามวรรคหนึ่งหรือวรรคสอง เป็นการนำเข้าสู่ระบบ คอมพิวเตอร์โดยสุจริต อันเป็นการติชมด้วยความเป็นธรรม ซึ่งบุคคลหรือสิ่งใดอันเป็นวิสัยของประชาชนย่อมกระทำ ผู้กระทำไม่มีความผิด |
| ถ้าการกระทำตามวรรคหนึ่ง โดยสุจริต ผู้กระทำไม่ มีความผิด ความผิดตามวรรคหนึ่งและวรรคสองเป็นความผิดอันยอมความได้<br><br>ถ้าผู้เสียหายในวรรคหนึ่งตายก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรสหรือบุตรของผู้เสียหายร้องทุกข์ได้ | ความผิดตามวรรคหนึ่งเป็นความผิดอัน ยอมความได้<br><br>ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งหรือวรรคสองตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย” |

# มาตรา 16/1 และ 16/2
## ให้ยกเลิกความเดิมในมาตรานี้ และให้ใช้ ความต่อไปนี้แทน

| พรบ. ปี 2550 มาตรา 16 | พรบ. (ฉบับที่ 2) พ.ศ. 2560 มาตรา 16/1 และ 16/2 |
|---|---|
| | “มาตรา 16/1 ในคดีความผิดตามมาตรา 14 หรือมาตรา 16 ซึ่งมีคำพิพากษาว่า จำเลยมีความผิดศาลอาจสั่ง<br>1) ให้ทำลายข้อมูลตามมาตราดังกล่าว<br>2) ให้โฆษณาหรือเผยแพร่คำพิพากษาทั้งหมดหรือแต่บางส่วนในสื่อ อิเล็กทรอนิกส์ วิทยุกระจายเสียง วิทยุโทรทัศน์ หนังสือพิมพ์ หรือสื่ออื่นใด ตามที่ศาลเห็นสมควรโดยให้จำเลยเป็นผู้ชำระค่าโฆษณาหรือเผยแพร่<br>3) ให้ดำเนินการอื่นตามที่ศาลเห็นสมควรเพื่อบรรเทาความเสียหายที่ เกิดขึ้นจากการกระทำความผิดนั้น |
| | มาตรา 16/2 ผู้ใดรู้ว่าข้อมูลคอมพิวเตอร์ในความครอบครองของตน เป็นข้อมูลที่ศาลสั่งให้ทำลายตามมาตรา 16/1 ผู้นั้นต้องทำลายข้อมูล ดังกล่าว หากฝ่าฝืนต้องระวางโทษกึ่งหนึ่งของโทษที่บัญญัติไว้ในมาตรา 14 หรือมาตรา 16 แล้วแต่กรณี |

| พรบ. (ฉบับที่ 2) พ.ศ. 2560 มาตรา 16 |
| --- |
| **ประเด็นที่แก้ไข**<br>นำเข้าเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้นฯ ถ้าการกระทำตามนี้เป็นการกระทำต่อภาพของผู้ตาย และการกระทำนั้นน่าจะทำให้บิดา มารดา คู่สมรส หรือบุตรของผู้ตายเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง หรือได้รับความอับอาย ต้องได้รับโทษ การนำเข้าสู่ระบบคอมพิวเตอร์โดยสุจริต อันเป็นการติชมด้วยความเป็นธรรม ซึ่งบุคคลหรือสิ่ง ใดอันเป็นวิสัยของประชาชนย่อมกระทำ ผู้กระทำไม่มีความผิด ความผิดตามวรรคหนึ่งและวรรคสองเป็นความผิดอันยอมความได้ |
| **เพิ่ม** มาตรา 16/1 ในคดีความผิดตามมาตรา 14 หรือมาตรา 16 ซึ่งมีคำพิพากษาว่าจำเลยมีความผิดศาลอาจสั่ง (1) ให้ทำลายข้อมูล (2) ให้โฆษณาหรือเผยแพร่คำพิพากษาทั้งหมดหรือแต่บางส่วนในสื่ออิเล็กทรอนิกส์ ฯ (3) ให้ดำเนินการอื่นตามที่ศาลเห็นสมควรเพื่อบรรเทาความเสียหายที่เกิดขึ้นจากการกระทำความผิดนั้น<br>16/2 ข้อมูลคอมพิวเตอร์ในความครอบครองของตนเป็นข้อมูลที่ศาลสั่งให้ทำลายตามมาตรา 16/1 ผู้นั้นต้องทำลายข้อมูลดังกล่าว หากฝ่าฝืนต้องระวางโทษ |

# มาตรา 18

**แก้ไขเพิ่ม การร้องขอให้ดำเนินการกรณีความผิดอาญาต่อกฎหมายอื่น ซึ่งได้ใช้ ระบบคอมพิวเตอร์ข้อมูลคอมพิวเตอร์**

| พรบ. ปี 2550 มาตรา 18 | พรบ.(ฉบับที่ 2) พ.ศ. 2560 มาตรา 18 |
|---|---|
| มาตรา 18 อำนาจทั่วไปของพนักงาน เจ้าหน้าที่ที่ได้รับการแต่งตั้ง แบ่งเป็น<br>1. อำนาจที่ดำเนินการได้โดยไม่ต้องใช้อำนาจศาล<br>1) มีหนังสือสอบถาม เพื่อให้ส่งคำชี้แจง ให้ข้อมูล<br>2) เรียกข้อมูลจราจรคอมพิวเตอร์<br>3) สั่งให้ส่งมอบข้อมูลตาม ม.26<br>2. อำนาจที่ต้องขออนุญาตศาล<br>- ทำสำเนาข้อมูล<br>- เข้าถึงระบบคอมพิวเตอร์/ข้อมูลคอมพิวเตอร์<br>- ถอดรหัสลับ<br>- ยึดอายัดระบบคอมพิวเตอร์ | ให้พนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา อาจร้องขอให้พนักงาน เจ้าหน้าที่ตามพระราชบัญญัตินี้ฯ ดำเนินการตาม พระราชบัญญัติในบรรดา ความผิดอาญาต่อกฎหมายอื่นซึ่งได้ใช้ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์หรือ อุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ เป็นองค์ประกอบหรือเป็นส่วนหนึ่งในการกระทำความผิดและให้ผู้ได้รับการร้องขอ จากพนักงานเจ้าหน้าที่ดำเนินการตามคำร้องขอโดยไม่ชักช้า<br>ให้ผู้ได้รับการร้องขอจากพนักงานเจ้าหน้าที่ตามวรรคหนึ่ง (1) (2) (3) (4) (5) (6) (7) หรือ(8) ดำเนินการตามคำร้องขอโดยไม่ชักช้า แต่ต้องไม่ เกินเจ็ดวันนับแต่วันที่ได้รับคำร้องขอ หรือภายในระยะเวลาที่พนักงานเจ้าหน้าที่กำหนด ซึ่งต้องไม่น้อยกว่าเจ็ดวันและไม่เกินสิบห้าวัน เว้นแต่ในกรณีที่มีเหตุสมควร ต้องได้รับอนุญาตจากพนักงานเจ้าหน้าที่ |

# มาตรา 20

## มาตราในการปิดกั้นเว็บไซต์ และที่เป็นความผิดกฎหมายอื่น/ลักษณะขัดต่อศีลธรรมอันดีของประชาชน

ความผิดอาญาตามกฎหมายเกี่ยวกับทรัพย์สินทางปัญญา หรือกฎหมายอื่นซึ่งข้อมูลคอมพิวเตอร์นั้นมีลักษณะขัดต่อ ความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

# มาตรา 20

## การปิดกั้นเว็บไซต์ และที่เป็นความผิดกฎหมายอื่น / ลักษณะขัดต่อศีลธรรมอันดี ของประชาชน

| พรบ. ปี 2550 มาตรา 20 | พรบ. (ฉบับที่ 2) พ.ศ. 2560 มาตรา 20 |
|---|---|
| มาตรา 20 ในกรณีที่การกระทาความผิดเป็นการทาให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่<br>1. อาจกระทบกระเทือนต่อความมั่นคง แห่งราชอาณาจักรตามที่กาหนดไว้ในภาคสองลักษณะ 1 หรือลักษณะ 1/1 แห่งประมวลกฎหมายอาญา<br>2. ที่มีลักษณะขัดต่อ ความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน<br>พนักงานเจ้าหน้าที่โดยได้รับความ เห็นชอบจากรัฐมนตรีอาจยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับ การทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นได้<br>ในกรณีที่ศาลมีคำสั่งให้ระงับการทำให้ แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ตามวรรคหนึ่ง ให้พนักงานเจ้าหน้าที่ทำการระงับการทำให้แพร่หลาย นั้นเอง หรือสั่งให้ผู้ให้บริการระงับการทำให้แพร่หลาย ซึ่งข้อมูลคอมพิวเตอร์นั้นก็ได้ | ในกรณีที่มีการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ดังต่อไปนี้ พนักงานเจ้าหน้าที่โดยได้รับความเห็นชอบจากรัฐมนตรีอาจยื่นคำร้อง พร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจ ขอให้มีคำสั่งระงับการ ทำให้แพร่หลาย/ลบข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์ได้<br>1) ข้อมูลคอมพิวเตอร์ที่เป็นความผิดตามพระราชบัญญัตินี้<br>2) ข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่กำหนดไว้ในภาค 2 ลักษณะ 1 หรือลักษณะ 1/1 แห่งประมวลกฎหมายอาญา<br>3) ข้อมูลคอมพิวเตอร์ที่เป็นความผิดอาญาตามกฎหมายเกี่ยวกับ ทรัพย์สินทางปัญญา หรือกฎหมายอื่นซึ่งข้อมูลคอมพิวเตอร์นั้นมีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชนและเจ้าหน้าที่ ตามกฎหมายนั้น หรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญาได้ร้องขอ |

# มาตรา 20

## การปิดกั้นเว็บไซต์ และให้มีประกาศหลักเกณฑ์ สาหรับการระงับ/ลบข้อมูล

| พรบ. (ฉบับที่ 2) พ.ศ. 2560 มาตรา 20 |
| --- |
| **ขั้นตอนการปิดกั้น**<br>ในกรณีที่ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ ให้พนักงานเจ้าหน้าที่ทำการระงับการทำให้แพร่หลายหรือลบข้อมูลนั้นเอง หรือสั่งให้ผู้ให้บริการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์นั้นก็ได้ ทั้งนี้ ให้รัฐมนตรีประกาศกำหนดหลักเกณฑ์ ระยะเวลา และวิธีปฏิบัติสำหรับการระงับการทำให้เผยแพร่หรือลบข้อมูลของพนักงานเจ้าหน้าที่หรือผู้ให้บริการ ให้เป็นไปในแนวทางเดียวกันโดยคำนึงถึงพัฒนาการทางเทคโนโลยีสารสนเทศที่เปลี่ยนแปลงไป เว้น แต่ศาลจะมีคำสั่งเป็นอย่างอื่น<br>ในกรณีที่มีเหตุจำเป็นเร่งด่วน พนักงานเจ้าหน้าที่จะยื่นคำร้องตามวรรคหนึ่งไปก่อนที่จะได้รับความเห็นชอบจากรัฐมนตรีก็ได้ แต่ทั้งนี้ต้องรายงานให้รัฐมนตรีทราบโดยเร็ว |

# เพิ่มเติม มาตรา 20/1

**ข้อมูลซึ่งขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของ ประชาชน โดยให้รัฐมนตรีโดยความเห็นชอบของคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์ ให้เจ้าหน้าที่นาไปยื่นเรื่องต่อศาล เพื่อขอให้ศาลมีคาสั่งระงับหรือลบ**

| พรบ. (ฉบับที่ 2) พ.ศ. 2560 มาตรา 20/1 |
| --- |
| ในกรณีที่ทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่มีลักษณะขัดต่อ**ความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน** และรัฐมนตรีโดยความเห็นชอบของคณะกรรมการกลั่นกรอง เห็นสมควร ให้พนักงานเจ้าหน้าที่ยื่น คำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจ ขอให้มีคำสั่งระงับการ ทำให้แพร่หลายหรือลบซึ่งข้อมูลนั้นออกจากระบบคอมพิวเตอร์ ให้รัฐมนตรีแต่งตั้งคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์ตามวรรคสองขึ้นคณะหนึ่งหรือหลายคณะ แต่ละคณะให้มีกรรมการจำนวนเก้าคน ซึ่งสามในเก้าคนต้องมาจากผู้แทนภาคเอกชนด้านสิทธิมนุษยชน ด้านสื่อสารมวลชน ด้านเทคโนโลยีสารสนเทศ หรือด้านอื่นที่เกี่ยวข้อง และให้กรรมการได้รับ ค่าตอบแทนตามหลักเกณฑ์ที่รัฐมนตรีกำหนด โดยได้รับความเห็นชอบจากกระทรวงการคลัง<br>ในกรณีที่มีเหตุจำเป็นเร่งด่วน พนักงานเจ้าหน้าที่โดยความเห็นชอบของคณะกรรมการ กลั่นกรองจะยื่นคำร้องตามวรรคหนึ่งไปก่อนที่รัฐมนตรีมอบหมายก็ได้ แต่ทั้งนี้ต้องรายงานให้รัฐมนตรี ทราบโดยเร็ว” |

## เพิ่มมาตรการดูแลเนื้อหา(Content) ที่ผิดกฎหมายอื่น/กระทบความสงบฯ ศีลธรรมฯ ลดผลกระทบต่อสังคม แต่การปิดเว็บต้องผ่านกลไกของศาล (ตามมาตรา 20)

| ลักษณะเนื้อหา | ลักษณะเนื้อหา |
|---|---|
| ▪ ผิด พ.ร.บ.นี้<br>▪ เป็นความผิดเกี่ยวกับความมั่นคงปลอดภัย ของประเทศ/ก่อการร้าย ตามประมวลกฎหมายอาญา<br>▪ ผิดกฎหมายอื่น กฎหมายอาญา ผิดกฎหมายทรัพย์สินทางปัญญา | ▪ ข้อมูลมีลักษณะขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน |
| **ขั้นตอนการออกคำสั่ง**<br>พนักงานเจ้าหน้าที่ → รมว.ดีอี. → ศาล → พนักงานเจ้าหน้าที่/ผู้ให้บริการ<br>ดำเนินการระงับ/ลบ | **ขั้นตอนการออกคำสั่ง**<br>พนักงานเจ้าหน้าที่ → คณะกรรมการกลั่นกรอง<br>9 คน 3/9 ต้องมาจากเอกชนด้านสิทธิ, สื่อสารมวลชน,สื่อมวลชน,ด้านไอทีหรืออื่น ๆ<br>รมว.ดีอี. → ศาล → พนักงานเจ้าหน้าที่/ผู้ให้บริการ |

| พรบ. (ฉบับที่ 2) พ.ศ. 2560 มาตรา 20 |
| --- |
| **ประเด็นที่แก้ไข** ในกรณีที่ขอให้มีคำสั่งระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์ได้<br>**เพิ่มเติม** “ข้อมูลคอมพิวเตอร์ที่เป็นความผิดอาญาตามกฎหมายเกี่ยวกับทรัพย์สินทางปัญญา หรือ กฎหมายอื่นซึ่งข้อมูลคอมพิวเตอร์นั้นมีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน..” |
| ในกรณีที่มีการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่มีลักษณะขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน รัฐมนตรีโดยความเห็นชอบของคณะกรรมการกลั่นกรอง ก่อนแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้แพร่หลายหรือลบซึ่งข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์ |
| ในกรณีที่ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ พนักงาน เจ้าหน้าที่จะทำการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์นั้นเอง หรือจะสั่งให้ผู้ให้บริการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์นั้นก็ได้ ทั้งนี้ ให้รัฐมนตรีประกาศกำหนดหลักเกณฑ์ ระยะเวลา และวิธีการปฏิบัติ |

# มาตรา 26 การเก็บรักษาข้อมูลจราจร

| พรบ. ปี 2550 มาตรา 26 | พรบ. (ฉบับที่ 2) พ.ศ. 2560 มาตรา 26 |
|---|---|
| มาตรา 26 ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทาง คอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้า สู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะ สั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะราย และเฉพาะคราวก็ได้<br>ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของ ผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการ นับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อย กว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง ความในวรรคหนึ่งจะใช้กับผู้ให้บริการ ประเภทใด อย่างไร และเมื่อใด ให้เป็นไปตามที่รัฐมนตรี ประกาศในราชกิจจานุเบกษา ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท | มาตรา 26 ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทาง คอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวัน นับแต่วันที่ข้อมูลนั้น เข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็น พนักงาน เจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทาง คอมพิวเตอร์ไว้เกินเก้าสิบวัน แต่ไม่เกินสองปีเป็นกรณีพิเศษ เฉพาะรายและเฉพาะคราวก็ได้ |

**นอกจากนี้** ยังมีการแก้ไขในมาตรา อื่น ๆ ที่เกี่ยวข้องกับพนักงานเจ้าหน้าที่ตามพระราชบัญญัติฯ ให้มีความรัดกุม คล่องตัวในการปฏิบัติงาน และกำหนดบทลงโทษพนักงานเจ้าหน้าที่ที่ชัดเจนขึ้นด้วย เช่น มีการแก้ไขความในมาตรา 22 มาตรา 23 มาตรา 24 และมาตรา 25 แห่ง พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

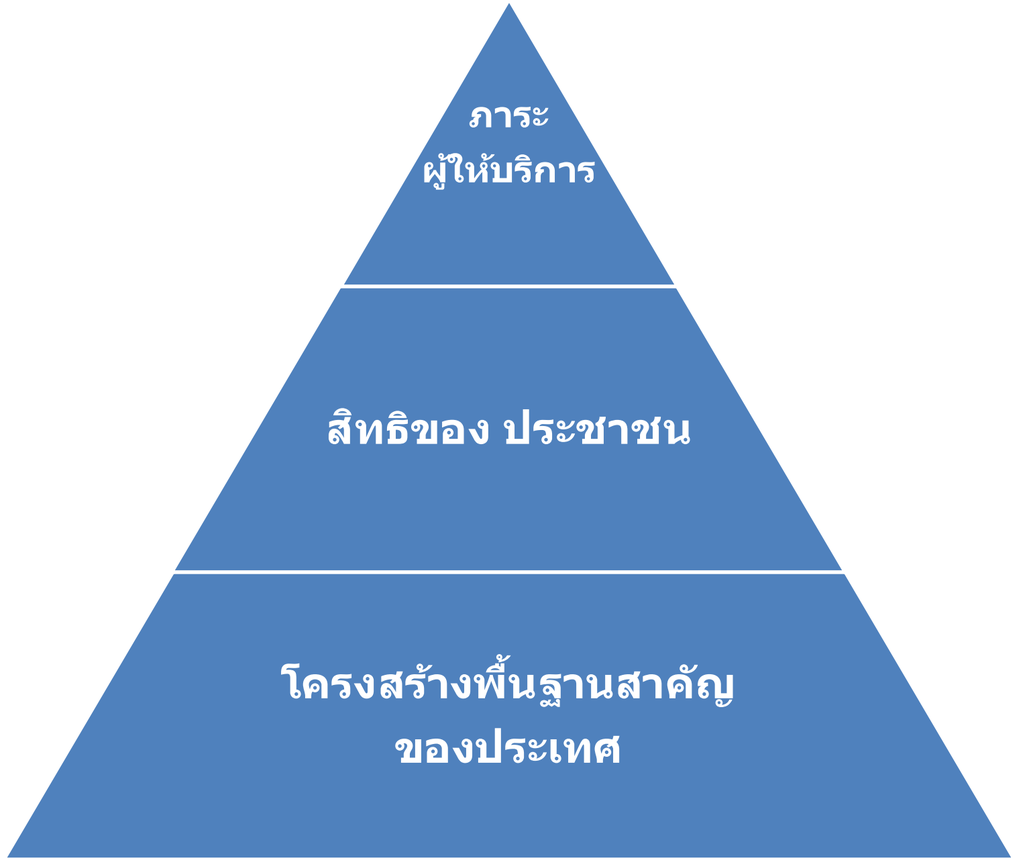
และมาตรา 28 “ผู้ที่ได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ คำนึงถึงภาระหน้าที่ ความรู้ความเชี่ยวชาญ ความขาดแคลนในการหาผู้มาปฏิบัติหน้าที่ หรือมีการสูญเสียผู้ปฏิบัติงานออกจาก ระบบราชการเป็นจานวนมาก คุณภาพของงาน และการดารงตนอยู่ในความยุติธรรม โดยเปรียบเทียบ ค่าตอบแทนของผู้ปฏิบัติงานอื่นในกระบวนการยุติธรรมด้วย”

การใช้อำนาจของพนักงานเจ้าหน้าที่ตามร่าง พ.ร.บ. คอมฯ ยังต้องทำตามกลไกตรวจสอบการใช้อำนาจรัฐตามที่กฎหมายปัจจุบันกำหนดไว้ ซึ่งส่วนใหญ่ต้องขออนุญาตจากศาลก่อนจึงจะดำเนินการได้ เช่น ทำสำเนา, ถอดรหัส, การตรวจสอบการเข้าถึงข้อมูล, ยึดอายัด ตามมาตรา 18 มาตรา 19 แห่ง พระราชบัญญัติ

**มาตรา 20** บรรดาระเบียบหรือประกาศที่ออกตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่ใช้บังคับอยู่ในวันก่อนวันที่พระราชบัญญัตินี้ใช้บังคับ **ให้ยังคงใช้บังคับต่อไปเท่าที่ไม่ขัดหรือแย้งกับบทบัญญัติแห่งพระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550** ซึ่งแก้ไขเพิ่มเติมโดย พระราชบัญญัตินี้ จนกว่าจะมีระเบียบหรือประกาศที่ต้องออกตามพระราชบัญญัติว่าด้วย การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งแก้ไขเพิ่มเติมโดย พระราชบัญญัตินี้ ใช้บังคับ

การดำเนินการออกระเบียบหรือประกาศตามวรรคหนึ่ง ให้ดำเนินการให้แล้วเสร็จ ภายในหกสิบวันนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ หากไม่สามารถดำเนินการได้ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม รายงานเหตุผลที่ไม่อาจดำเนินการได้ต่อคณะรัฐมนตรีเพื่อทราบ

# ผลกระทบจากการบังคับใช้ พ.ร.บ.




**ผลกระทบที่อาจต้องแบกรับ**
**มาตรา 26 และ 27**

**Private Interests & ข้อจากัด / ระมัดระวัง**
**ในการใช้สิทธิมาตรา 12, 14, 16 และ 20**

**ประโยชน์มหาชน / สาธารณะ**
**Public Interests**

# พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ

## ผลจากการบังคับใช้ พ.ร.บ.

สรุปยังคงมีการกระทำผิดที่ไม่ลดลง

สาเหตุ มีการใช้หลากหลาย การติดต่อทำได้รวดเร็ว มีการแข่งขันของผู้ประกอบการสูง

- ❑ ยังคงมีการระงับการเผยแพร่เนื้อหาหรือการปิดกั้นเว็บไซต์โดยอาศัยมาตรา 20 ของ พ.ร.บ.
- ❑ คดีที่มีเนื้อหาความผิดเกี่ยวข้องกับการหมิ่นประมาทต่อบุคคลมีสัดส่วนมาก ที่สุดในคดีที่ถูกฟ้องตาม พ.ร.บ.ฯ

รองลงมาได้แก่ คดีที่เป็นอาชญากรรมคอมพิวเตอร์โดยแท้ (เช่น การเจาะข้อมูล การส่งสแปม)

อันดับที่ 3 คดีที่มีเนื้อหาความผิดเกี่ยวข้องกับการหมิ่นประมาทกษัตริย์ พระราชินี และรัช ทายาท

อันดับที่ 4 มีสองประเภท คือ คดีที่เกี่ยวข้องกับการฉ้อโกง เช่น โพสท์ข้อความหลอกขายของ และคดีที่เกี่ยวข้องกับเนื้อหาลามก ที่เหลือส่วนน้อยเป็นคดีที่เกี่ยวข้องกับการขายโปรแกรม คดีที่เกี่ยวกับความมั่นคง และคดีอื่น ๆ

# ความตระหนักถึงความมั่นคงปลอดภัยด้านสารสนเทศ

## การใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

หน่วยงานมีระบบงานสารสนเทศ และเครือข่ายทีมสามารถเชื่อมต่ออินเทอร์เน็ต ทั้งภายในหน่วยงานเอง(Intranet ) และการเชื่อมต่อไปยังภายนอกองค์(Internet)

1. ผู้เกี่ยวข้องในการให้บริการ
2. ผู้ใช้บริการ
3. การใช้งาน ระบบงาน/การสื่อสารเชื่อมต่อ
4. ภัยคุกคามที่อาจเกิดขึ้น แนวทางป้องกันหรือการสร้างความตระหนักที่พึงระวังไว้ /การปฏิบัติตามข้อปฏิบัติ หรือกฎหมายที่เกี่ยวข้อง
5. การบริหารจัดการเพื่อแก้ไขปัญหา การควบคุม เช่นการเข้าถึง การใช้งาน เช่น เครื่องคอมพิวเตอร์ส่วนบุคคล การควบคุมการส่งข้อมูลข่าวสาร/จดหมายอิเล็กทรอนิกส์

การใช้เทคโนโลยีสารสนเทศ หมายถึง กระบวนการต่าง ๆ และระบบงานที่ช่วยให้ได้ สารสนเทศหรือข่าวสารที่ต้องการ โดยจะรวมถึง

1. เครื่องมือและอุปกรณ์ต่าง ๆ หมายถึง เครื่องคอมพิวเตอร์ เครื่องใช้สานักงาน อุปกรณ์คมนาคมต่าง ๆ รวมทั้งซอฟต์แวร์ทั้งระบบ สำเร็จรูปและพัฒนาขึ้นโดยเฉพาะด้าน
2. กระบวนการในการนำอุปกรณ์เครื่องมือต่าง ๆ ข้างต้นมาใช้งานรวบรวมข้อมูล จัดเก็บประมวลผล และแสดงผลลัพธ์เป็นสารสนเทศในรูปแบบต่าง ๆ ที่สามารถนำไปใช้ประโยชน์ได้ต่อไป

ในปัจจุบันการใช้งานเทคโนโลยีสารสนเทศ เป็นสิ่งจำเป็นสำหรับทุกองค์กร การเชื่อมโยงสารสนเทศผ่านทางคอมพิวเตอร์ ทำให้สิ่งที่มีค่ามากที่สุดของระบบ คือ ข้อมูลและสารสนเทศ อาจถูกจารกรรม ถูกปรับเปลี่ยน ถูกเข้าถึงโดยเจ้าของไม่รู้ตัว ถูกปิดกั้นขัดขวางให้ไม่สามารถเข้าถึงข้อมูลได้ หรือถูกทำลายเสียหายไป ซึ่งสามารถเกิดขึ้นได้ไม่ยาก บนโลกของเครือข่าย โดยเฉพาะเมื่อยู่บนอินเทอร์เน็ต

## ปัจจุบันมีกฎหมายที่เกี่ยวข้องด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสาร

1. กฎหมายเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (Computer Crime Law) เพื่อกำหนดมาตรการทางอาญา ในการลงโทษผู้กระทำผิดต่อระบบการทำงานของคอมพิวเตอร์ ระบบข้อมูล และระบบเครือข่าย ทั้งนี้เพื่อเป็นหลักประกันสิทธิเสรีภาพและการคุ้มครองการอยู่ร่วมกันของสังคม
2. กฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ (Electronic Transactions Law) เพื่อรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ให้เสมอด้วยกระดาษ อันเป็นการรองรับนิติสัมพันธ์ต่าง ๆ ซึ่งแต่เดิมอาจจะจัดทำขึ้นในรูปแบบของหนังสือ ให้เท่าเทียมกับนิติสัมพันธ์รูปแบบใหม่ที่จัดทำขึ้นให้อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์

## ปัจจุบันมีกฎหมายที่เกี่ยวข้องด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสาร (ต่อ)

3. กฎหมายอื่น ๆ ที่เกี่ยวข้อง เช่น

   3.1 กฎหมายลิขสิทธิ์ (มีผลบังคับใช้ 4 สิงหาคม 2558 นี้ มีความเข้มข้นด้านเทคโนโลยีมากขึ้นกว่าเดิม )

   3.2 กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Law)

   3.3 กฎหมายคุ้มครองผู้บริโภค

   3.4 อื่น ๆ ที่กำลังมีการพิจารณากันอยู่ เช่น กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

# การรักษาความมั่นคงปลอดภัยด้านสารสนเทศสาหรับองค์กร

**“ความมั่นคงปลอดภัยด้านสารสนเทศ”** หมายความว่า การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้อง (Integrity) และ สภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

**“การรักษาความมั่นคงปลอดภัยของข้อมูล (Data security)”** หมายถึง การป้องกันข้อมูลในบริบทของการรักษาความลับ บูรณภาพ และความพร้อมใช้งานของข้อมูล ซึ่งสามารถ ใช้แทนการรักษาความมั่นคงปลอดภัยของสารสนเทศได้

**“การปกป้องข้อมูล (Data protection)”** หมายถึงการป้องกันข้อมูลส่วนบุคคลต่อการประสงค์ร้ายของบุคคลที่สาม

**“เหตุการณ์ด้านความมั่นคงปลอดภัย”** หมายถึง การเกิดเหตุการณ์หรือสภาพของบริการที่แสดงให้เห็นความเป็นไปได้ ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

# การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

## การควบคุมโดยการออกระเบียบหรือแนวทางปฏิบัติ

1. มีการประกาศใช้ แนวนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยขององค์กร การนำแนวนโยบายไปปฏิบัติออกมา เช่น การรักษาความมั่นคงปลอดภัย มีแนวทางการป้องกันทางด้านไซเบอร์ สร้างขั้นตอนปฏิบัติ
2. การจัดองค์กรและการรักษาความปลอดภัยสาหรับระบบสารสนเทศ

   2.1. การจัดองค์กรการวางโครงสร้างขององค์กรที่สามารถเอื้ออำนวย ให้แผนงานที่จัดทำขึ้นไปสู่สัมฤทธิ์ผล โดยกำหนดอำนาจหน้าที่และความรับผิดชอบ ของกลุ่มบุคคลในองค์กร เพื่อให้งานเป็นไปอย่างรวดเร็วและมีประสิทธิภาพ

   2.2. การพัฒนาระบบงานควบคุมดูแลและปฏิบัติงานที่เกี่ยวกับเรื่องความมั่นคงปลอดภัย และการใช้งาน/เครื่องมืออุปกรณ์

พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ. 2549 กำหนดให้หน่วยงานต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

# แนวทาง/มาตรการที่จะต้องกาหนดให้เป็นไปตามข้อกฎหมาย

| ประเภท | แนวปฏิบัติ |
|---|---|
| ผู้ใช้บริการโดยทั่วไป | ผู้ใช้งานอินเทอร์เน็ตต้องทำความเข้าใจและปฏิบัติให้อยู่ในกรอบของกฎหมาย<br>หากฝ่าฝืนอาจถูกดำเนินคดี |
| องค์กร/หน่วยงาน | ควรให้ความสำคัญในประเด็น ดังนี้<br>1. การเข้าถึงหรือควบคุมการใช้งานเครื่องคอมพิวเตอร์และระบบสารสนเทศ<br>▪ จัดทำนโยบายการควบคุมการเข้าถึงสารสนเทศเป็นลายลักษณ์อักษร<br>2. จัดให้มีการสำรองข้อมูลสารสนเทศที่สำคัญอย่างสม่ำเสมอเพื่อให้อยู่ในสภาพพร้อมการใช้งาน<br>▪ กำหนดหน้าที่และความรับผิดชอบของบุคลากรที่เกี่ยวข้องกับการดำเนินการจัดทำแผน มีการเตรียมพร้อม<br>3. การปฏิบัติตามข้อบังคับของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฯ<br>▪ กำหนดมาตรการป้องกันระบบคอมพิวเตอร์สาหรับจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์<br>▪ จัดให้มีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ตามอุปกรณ์ที่เกี่ยวข้องกับการใช้งาน |

**ในกรณีเกิดการกระทำความผิดขึ้นในองค์กร : ควรมีผังกระบวนการแสดงขั้นตอนการปฏิบัติเมื่อเกิดเหตุการณ์ พร้อมทั้งระบุผู้รับผิดชอบในการปฏิบัติในแต่ละขั้นตอนเป็นเฉพาะกรณีไป เช่น การคุกคามจากผู้ไม่ประสงค์ดีเข้าเปลี่ยนแปลงหน้าเว็บไซต์ขององค์กร โดยกรณีเช่นนี้ การวิเคราะห์และการประเมินเหตุการณ์ การปฏิบัติงานเพื่อแก้ไขปัญหา ก็จะสามารถดำเนินการได้ทันต่อสถานการณ์ ในเมื่อมีความพร้อมและกระบวนการที่ชัดเจน**

# แนวทาง/มาตรการที่จะต้องกาหนดให้เป็นไปตามข้อกฎหมาย

การปฏิบัติตามข้อกาหนดทางด้านกฎหมายและข้อบังคับต่าง ๆ
ที่เกี่ยวกับความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ

- เพื่อลดความเสี่ยงที่อาจเกิดขึ้นได้จากการปฏิบัติงานระบบสารสนเทศ
- เพื่อให้ระบบสารสนเทศมีความปลอดภัยจากการใช้เทคโนโลยี สารสนเทศที่ไม่เหมาะสม หรือไม่ถูกต้อง
- เพื่อเป็นกรอบการดาเนินงานด้านการรักษาความปลอดภัยสารสนเทศ ของ องค์กร
- เพื่อให้ผู้ใช้งานตระหนักถึงภัยคุกคาม และความปลอดภัยด้าน เทคโนโลยีสารสนเทศ

# แนวทาง/มาตรการที่จะต้องกาหนดให้เป็นไปตามข้อกฎหมาย

กำหนดเงื่อนไขนโยบายความปลอดภัยระบบสารสนเทศสำหรับผู้ทำงาน (Acceptable Use Policy: AUP) เพื่อเป็นกรอบที่กำหนดให้ผู้ใช้งานทำงาน ร่วมกันโดยมีเป้าหมายเพื่อนำไปพัฒนาเป็นมาตรฐาน กระบวนการ แนวทาง/ ขั้นตอนปฏิบัติที่เหมาะสมให้ระบบสารสนเทศเกิดความมั่นคง และปลอดภัยตาม พื้นฐานการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ คือ

- การรักษาความลับ (Confidentiality)
- ความถูกต้องสมบูรณ์ (Integrity)
- ความพร้อมใช้งาน (Availability)

ซึ่งผู้ใช้งานทุกระดับต้องให้ความสำคัญ ควรให้ผู้ใช้งานคอมพิวเตอร์ทั่วไปได้รับทราบรับเงื่อนไขนโยบายเกี่ยวกับความปลอดภัยระบบสารสนเทศขององค์กรหรือ AUP (Acceptable Use Policy) ด้วยเพื่อให้ผู้ใช้ได้ปฏิบัติตามนโยบาย

# ความปลอดภัยของข้อมูลและความเป็นส่วนตัว ในการใช้คอมพิวเตอร์และอินเทอร์เน็ต

**ความปลอดภัย**

- การดูแลจัดการฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูล ให้พ้นจากอันตรายต่าง ๆ เช่น อาชญากรรมคอมพิวเตอร์ ภัยธรรมชาติ ภัยคุกคามอื่น ๆ

**ความเป็นส่วนตัว**

- การปกป้องข้อมูลส่วนตัวที่ไม่ต้องการเปิดเผยของผู้ใช้

# แนวทาง/มาตรการที่จะต้องกาหนดให้เป็นไปตามข้อกฎหมาย

## ตัวอย่างการกำหนดเงื่อนไข

1. การปฏิบัติตามนโยบาย กฎหมาย/ข้อบังคับ และการปฏิบัติงานกฎหมาย และข้อบังคับใด ๆ เช่น พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ และประกาศกระทรวง ฯ เรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ของผู้ ให้บริการพ.ศ. 2550 เป็นต้น ถือเป็นสิ่งสำคัญที่ผู้ใช้งานต้องตระหนัก และต้องปฏิบัติตามอย่างเคร่งครัด และไม่กระทำความผิดนั้น ดังนั้น หากผู้ใช้งานกระทำความผิด ตามกฎหมายหรือข้อบังคับที่ประกาศใช้ถือว่าเป็นความผิด ซึ่งผู้ใช้งานต้องรับผิดชอบต่อความผิดนั้น
2. ความรับผิดชอบต่อข้อมูลสารสนเทศขององค์กร
   - ผู้ใช้งานระบบสารสนเทศ ต้องไม่เปิดเผยข้อมูลสารสนเทศใด ๆ ที่เป็นความลับ หรือ ข้อมูลที่มีความสำคัญต่อองค์กรสู่ภายนอกหรือสาธารณะ ยกเว้นจะได้รับอนุญาตจากผู้มีอำนาจเท่านั้น
   - ห้ามผู้ใช้งานระบบสารสนเทศที่ไม่มีสิทธิเข้าถึงหรือแก้ไข หรือเปลี่ยนแปลงข้อมูลของ ระบบสารสนเทศโดยไม่ได้รับอนุญาตหรือไม่มีหน้าที่เกี่ยวข้อง

## การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย และบทลงโทษของการละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศ

**เพื่อหลีกเลี่ยงการฝ่าฝืนกฎหมายทั้งทางอาญาและทางแพ่ง**
**พระราชบัญญัติ นโยบาย กฎ ระเบียบข้อบังคับ ที่เกี่ยวข้อง**

การถ่ายทอดองค์ความรู้ ความเข้าใจ ข้อกฎหมาย ระเบียบข้อบังคับ รวมถึงการฝึกอบรมผู้เกี่ยวข้องทางด้านความมั่นคงปลอดภัย และการเตรียมความพร้อม อย่างสม่ำเสมอ

ข้าราชการ/พนักงาน เจ้าหน้าที่ ทุกคนควรรับทราบ ทำความเข้าใจ และปฏิบัติตามรายการของนโยบาย กฎ ระเบียบ ข้อบังคับ กฎหมาย ที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารที่กำหนดขึ้น เช่น นโยบายการรักษาความมั่นคงด้านเทคโนโลยีสารสนเทศ และการสื่อสาร พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์ พ.ร.บ. ลิขสิทธิ์ เป็นต้น

**ผู้บริหารระดับสูงขององค์กร ให้ความสำคัญเรื่องความปลอดภัยข้อมูล อย่างเพียงพอ และจริงจังในการผลักดันเรื่องความปลอดภัยข้อมูล**

**ระบบรักษาความปลอดภัยสำนักงานฯ จะทำให้เจ้าหน้าที่ที่เกี่ยวข้อง ทราบถึงแนวทางในการปฏิบัติ เพื่อหลีกเลี่ยงความเสี่ยงต่าง ๆ หรือ ลดความรุนแรงของผลเสียหายต่าง ๆ ที่อาจเกิดขึ้นต่อระบบปฏิบัติราชการ ของสำนักงานฯ ซึ่งพบว่าปัญหาด้านความปลอดภัยที่อาจเกิดขึ้นได้นั้น ส่วนใหญ่เกิดจาก**

1) **บุคลากร (Awareness Training)**
2) **กระบวนงาน(process) (นโยบายความ ปลอดภัยและกระบวนการ บริหารจัดการที่ดี)**
3) **เทคโนโลยี(Technology)**

**ปัญหาหรือเหตุการณ์**ด้านความมั่นคง ปลอดภัย อาจเป็น เหตุการณ์ที่เกิดขึ้นในระบบคอมพิวเตอร์และเครือข่ายขององค์กร ซึ่งส่งผลให้

- เกิดการหยุดชะงักต่อกระบวนการทางธุรกิจสำคัญ (เช่น เนื่องจากระบบงานของกระบวนการทางธุรกิจเกิดการหยุดชะงัก เป็นต้น)
- เป็นการละเมิดนโยบายความมั่นคงปลอดภัยขององค์กร
- เป็นการละเมิดต่อกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดต่าง ๆ ที่องค์กรต้องปฏิบัติตาม
- เกิดภาพลักษณ์ที่ไม่ดีต่อองค์กร หรือท าให้องค์กรสูญเสียชื่อเสียง

## ความสำคัญเรื่องความปลอดภัยข้อมูลหรือ "Information Security"

การให้ความรู้ ตั้งแต่ ผู้บริหารระดับสูง, ผู้บริหารระดับกลาง, ผู้บริหารระบบ, ผู้ตรวจสอบภายใน รวมถึงผู้ใช้คอมพิวเตอร์ "ทุกคน" ในองค์กร ให้ "ตระหนัก" และ "เข้าใจ" ในข้อกฎหมายระเบียบข้อบังคับที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศ และการสื่อสาร

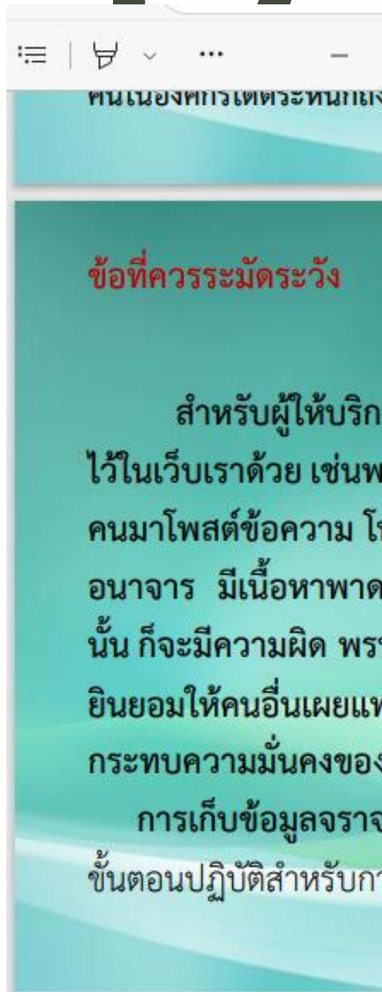
สร้างความตระหนักด้านความมั่นคงปลอดภัย การกำหนดนโยบาย Security Policy หนึ่งในที่สำคัญคือ Acceptable Use Policy (AUP) คือใช้อย่างไรให้เหมาะสม ไม่เอาขององค์กรไป ใช้ส่วนตัว พอเอาไปใช้ส่วนตัว ก็มีประเด็น เช่น เปลือง bandwidth องค์กร, ถ้ามีข้อมูลรั่ว ออกมาแบบนี้แล้วพนักงาน reuse password อาจถูกใช้เป็นหนึ่งในเข้าถึงข้อมูลได้

การควบคุมการใช้งาน แนวนโยบายและแนวทางปฏิบัติที่เกี่ยวกับความปลอดภัย ข้อมูลในองค์กร

มีการฝึกอบรม "Security Awareness Training" เพื่อให้ผู้ใช้คอมพิวเตอร์ทุก คนในองค์กรได้ตระหนักถึงบทบัญญัติของ พ.ร.บ. ฯ และท าความเข้าใจ พ.ร.บ. ฯ

# ข้อที่ควรระมัดระวัง

สำหรับผู้ให้บริการต้องระวัง หมั่นดูแลข้อมูลต่าง ๆ ที่คนอื่นโพสทิ้งไว้ในเว็บเราด้วย เช่น พวกเว็บบอร์ด กระทู้ หรือ ความเห็นต่าง ๆ เพราะมีคนมาโพสต์ข้อความโพสต์รูปที่ทำให้บุคคลอื่นเสียหายหรือภาพอนาจาร มีเนื้อหาพาดพิงสถาบัน แล้วถ้าเพิกเฉย ปล่อยให้มีการกระทำ นั้น ก็จะมีความผิด พรบ.คอมพิวเตอร์ มาตรา 15 ข้อหาสนับสนุน ยินยอมให้คนอื่นเผยแพร่ข้อมูลที่กระทบให้ผู้อื่นเดือดร้อน เสียหาย กระทบความมั่นคงของรัฐ และอื่น ๆ ตามที่ พรบ.คอมพิวเตอร์ มาตรา 14 การเก็บข้อมูลจราจรคอมพิวเตอร์ควรกำหนดให้มีการปฏิบัติตามขั้นตอนปฏิบัติสำหรับการเก็บรวบรวม หลักฐานโดยเคร่งครัด



**ในกรณีเกิดการกระทำความผิดขึ้นในองค์กร : ควรมีผังกระบวนการแสดงขั้นตอนการปฏิบัติเมื่อเกิดเหตุการณ์ พร้อมทั้งระบุผู้รับผิดชอบในการปฏิบัติในแต่ละขั้นตอนเป็นเฉพาะกรณีไป เช่น การคุกคามจากผู้ไม่ประสงค์ดีเข้าเปลี่ยนแปลงหน้าเว็บไซต์ขององค์กร โดยกรณีเช่นนี้ การวิเคราะห์และการประเมินเหตุการณ์ การปฏิบัติงานเพื่อแก้ไขปัญหาก็จะสามารถดำเนินการได้ทันต่อสถานการณ์ ในเมื่อมีความพร้อมและกระบวนการที่ชัดเจน**

: ในกรณีที่จำเป็นต้องมีการดำเนินการทางกฎหมายต่อบุคคลหรือองค์กรหนึ่ง ไม่ว่าจะเป็นการดำเนินการทางแพ่งหรืออาญาก็ตาม หน่วยงานควรดำเนินการเก็บหลักฐานที่เกี่ยวข้อง จัดเก็บไว้ช่วงระยะเวลาหนึ่ง และนำเป็นพยานหลักฐานเสนอ (อาทิ ต่อศาล) โดยให้สอดคล้องกับหลักการสำหรับการจัดเก็บหลักฐานที่ได้กำหนดไว้

## การเก็บรวบรวมพยานหลักฐาน (Collection of evidence)

**แนวปฏิบัติ :**

ก) หน่วยงานควรกำหนดขั้นตอนปฏิบัติสำหรับการเก็บรวบรวมหลักฐานเพื่อใช้สนับสนุนกระบวนการทางวินัยหรือกฎหมาย และลงโทษผู้กระทำความผิด

ข) หน่วยงานควรกำหนดให้มีการปฏิบัติตามขั้นตอนปฏิบัติสำหรับการเก็บรวบรวม หลักฐานโดยเคร่งครัด

ค) หน่วยงานควรกำหนดให้เฉพาะผู้ที่ผ่านการอบรมและมีทักษะเพียงพอในการเก็บรวบรวมหลักฐานคอมพิวเตอร์เท่านั้น จึงจะสามารถรวบรวมและจัดเก็บหลักฐานได้

ง) หน่วยงานควรกำหนดให้มีการปฏิบัติตามกฎในการจัดเก็บหลักฐาน เช่น หลักฐานที่สามารถยอมรับได้ (Admissibility) หลักฐานที่จัดเก็บมานั้นต้องมีทั้งคุณภาพและความสมบูรณ์

ตัวอย่างหลักฐานที่อยู่บนสื่อบันทึกข้อมูลคอมพิวเตอร์ ได้แก่ การทำสำเนา ข้อมูลจากสื่อบันทึกข้อมูล การทำสำเนาข้อมูลบนฮาร์ดดิสก์หรือหน่วยความจำออกมา การมีพยานที่เชื่อถือได้ ในระหว่างที่ทำสำเนาข้อมูล การบันทึกข้อมูลล็อค เพื่อแสดงถึงกิจกรรมต่าง ๆ ระหว่างที่สำเนาข้อมูลนั้น การจัดเก็บสื่อบันทึกข้อมูลและข้อมูลล็อคไว้ในสถานที่ที่มีความปลอดภัย

# การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้ใช้งานทั่วไป

## ความปลอดภัยและความเป็นส่วนตัวบนอินเทอร์เน็ต

1. เพื่อสร้างความปลอดภัยในการใช้อินเตอร์เน็ต
   1) อย่าให้รหัสลับแก่ผู้อื่น
   2) ต้องคิดให้ดีทุกครั้ง ที่ให้ข้อมูลส่วนตัวกับบุคคลอื่นในอินเทอร์เน็ต
   3) ตรวจทานว่าได้พิมพ์ชื่อเว็บไซต์ถูกต้องเสียก่อน แล้วจึงกด Enter เพื่อจะได้เข้าเว็บไซต์ที่ต้องการได้ถูกต้อง
   4) ถ้าพบเห็นข้อความ หรือสิ่งใด ที่ไม่เหมาะสม หรือคิดว่าไม่ดีต่อการใช้ อินเทอร์เน็ต ควรออกจากเว็บไซต์นั้น
   5) อย่าส่งรูปภาพของตนเอง หรือรูปภาพของผู้อื่น ให้คนอื่นทางอีเมล์
   6) ถ้าได้รับอีเมล์ที่มีข้อความไม่เหมาะสม หรือทำให้ไม่สบายใจ ไม่ควรโต้ตอบ
   7) บนอินเทอร์เน็ต ทุกอย่างที่คุณเห็นไม่ใช่เรื่องจริงเสมอไป
   8) อย่าบอกวันเดือนปีเกิด หรืออายุจริงของคุณกับคนอื่น
   9) อย่าบอกชื่อจริง และนามสกุลจริงกับบุคคลอื่น
   10) อย่าบอกที่อยู่ ของคุณกับบุคคลอื่น
   11) อย่าบอกเบอร์โทรศัพท์ของคุณกับบุคคลอื่น ในอินเตอร์เน็ต

## ความปลอดภัยและความเป็นส่วนตัวบนอินเทอร์เน็ต

2. การป้องกัน : การใช้งานอินเทอร์เน็ตอย่างปลอดภัย
   - อ่านข้อตกลง นโยบาย ให้ดีก่อนตอบตกลงใด ๆ
   - ระวังการใช้บริการเครื่องคอมพิวเตอร์สาธารณะ
     1) แอบดูการใช้งาน
     2) หลีกเลี่ยงการใส่ข้อมูลสำคัญมาก ๆ
     3) ไม่ให้ระบบช่วยจำ username และ password
   - หมั่นลบ temporary internet files, cookies และ history
   - Logoff หรือ logout ทุกครั้งหลังใช้งาน
   - ไม่ใช้ Password ที่คาดเดาได้ง่าย เช่น ค าที่มีใน Dictionary
   - ใช้การผสมอักขระที่ซับซ้อน
   - เปลี่ยน Password อย่างสม่ำเสมอ เมื่อถึงเวลาที่เหมาะสม เช่น ทุก ๆ 90 วัน
   - ตั้ง Password ซึ่งผสมอักษรภาษาอังกฤษตัวเล็ก อักษรภาษาอังกฤษตัวใหญ่ ตัวเล็ก และตัว อักขระพิเศษ

## ความปลอดภัยและความเป็นส่วนตัวบนอินเทอร์เน็ต

### 3. การป้องกันภัยคุกคาม ที่เกี่ยวข้องกับการทำธุรกรรม

- ❑ การป้องกันการใช้เครือข่ายสาธรณะ/Free WiFi
  - 1) ใช้เครือข่าย WiFi ที่เชื่อถือได้เท่านั้น
  - 2) ดูชื่อจุดเชื่อมต่อ
  - 3) ลบชื่อจุดเชื่อมต่อที่ไม่ได้ใช้จากรายการ
  - 4) เลือกการเชื่อมต่อ ที่ต้องเข้ารหัส (WPA2.WPAและ WEP)
  - 5) อย่าแชร์ไฟล์และโฟลเดอร์
  - 6) เปิดไฟล์วอลล์ส่วนบุคคล

# การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้ใช้งานทั่วไป

## ความปลอดภัยและความเป็นส่วนตัวบนอินเทอร์เน็ต

### วิธีป้องกันภัยออนไลน์ เช่น ภัยจากมัลแวร์

**วิธีที่มัลแวร์เข้าสู่คอมพิวเตอร์ของคุณ**

1. การดาวน์โหลดซอฟต์แวร์จากอินเทอร์เน็ตที่มีมัลแวร์แฝงอยู่
2. การดาวน์โหลดซอฟต์แวร์ถูกกฎหมายที่แอบมีมัลแวร์ผูกติดมา
3. การเข้าชมเว็บไซต์ที่ติดเชื้อมัลแวร์
   - การคลิกข้อความแสดงข้อผิดพลาด/หน้าต่างป๊อปอัพ
   - การเปิดไฟล์แนบอีเมล์ที่มีมัลแวร์

**หลักการการป้องกันมัลแวร์**

1. อัพเดทคอมพิวเตอร์และซอฟต์แวร์ของคุณอยู่เสมอ
2. คิดให้ดีก่อนจะคลิกลิงค์หรือดาวน์โหลดอะไรก็ตาม
3. คิดก่อนเปิดไฟต์แนบอีเมล์หรือรูปภาพ
4. อย่าเชื่อหน้าต่างป๊อปอัพที่ขอให้ดาวน์โหลดซอฟต์แวร์
5. ให้ระมัดระวังเรื่องการแบ่งปันไฟล์
6. การป้องกันโดยใช้ซอฟต์แวร์ป้องกันไวรัส

# สิ่งที่ไม่ควรทำบนเครือข่ายสังคมออนไลน์

1. ไม่โพสต์กิจกรรมที่ผิดกฎหมาย
2. ไม่ควรโพสต์ข้อความ ที่ชี้ชวนให้มิจฉาชีพรับรู้ความเคลื่อนไหวส่วนตัว
3. โพสต์ข้อมูลที่เป็นเรื่องส่วนบุคคล
4. ให้ระมัดระวังการเช็คอิน (Check-in) ผ่านสื่อสังคมออนไลน์
5. ไม่ระบุชื่อบุตรหลาน ระบุภาพหรือติด tag ในรูปภาพมากเกินไป
6. ไม่ส่งหลักฐานส่วนตัวของตนเองและคนในครอบครัวให้ผู้อื่น
7. พึงระมัดระวังอย่างยิ่งที่จะไว้ใจหรือเชื่อใจคน ที่รู้จักผ่านอินเทอร์เน็ต

## ผู้ที่ได้รับผลกระทบจากกการบังคับใช้กฎหมาย
## : กรณีเป็นเสียหาย

**ขั้นตอนการแจ้งความร้องทุกข์ในคดี ตาม พรบ. คอมพิวเตอร์**

1. เมื่อพบการกระทำความผิดหรือถูกละเมิดในสื่ออินเตอร์เน็ต ควรดำเนินการเบื้องต้น ดังนี้

   1.1 ทำการบันทึกข้อมูลหลักฐานที่ปรากฏไว้ทั้งหมด เช่น หน้าเว็บเพจ ,ข้อความ หรือภาพถ่ายที่ก่อให้เกิดความเสียหาย

   1.2 พิมพ์ข้อมูลหน้าเว็ปไซต์ที่เกิดเหตุหรือเกี่ยวข้องออกมาเป็นเอกสาร เพื่อป้องกันไม่ให้พยานหลักฐานสูญหาย หรือถูกทำลาย และลงลายมือชื่อรับรองเอกสารนั้น

   1.3 การสั่งพิมพ์เอกสารหน้าเว็บเพจ ,ข้อความหรือภาพถ่ายต่าง ๆ ในเว็ปไซต์ ที่พบการกระทำผิด ให้ปรากฏที่ตั้งของเว็ปไซต์ หรือ URL ของเว็ปไซต์นั้นด้วย และหรือปรากฏวันเวลาบนเว็บไซต์หรือขณะบันทึกข้อมูลหลักฐานนั้นด้วย

# ผู้ที่ได้รับผลกระทบจากกการบังคับใช้กฎหมาย

## : กรณีเป็นเสียหาย

**ขั้นตอนการแจ้งความร้องทุกข์ในคดี ตาม พรบ. คอมพิวเตอร์**

2. หากประสงค์แจ้งความร้องทุกข์ ให้ผู้ที่ได้รับความเสียหายสามารถแจ้งต่อพนักงานสอบสวนสถานีตำรวจท้องที่เกิดเหตุ หรือที่พบการกระทำความผิด หลักฐานที่ควรนำไปมอบให้พนักงานสอบสวน ได้แก่หลักฐานตามข้อ 1.1 - 1.3
3. หากผู้เสียหาย หรือพนักงานสอบสวนที่รับแจ้งความ ต้องการตรวจสอบข้อมูล จราจรทางคอมพิวเตอร์ ก็สามารถประสานเพื่อส่งข้อมูล หลักฐานต่าง ๆ ตามข้อ 1. มายัง บก.ปอท. หรือหน่วยงานที่เกี่ยวข้องอื่น ๆ เช่น กระทรวง ไอซีที เพื่อตรวจสอบ ข้อมูลให้ ต่อไป
4. กรณีจำเป็นเร่งด่วนเพื่อป้องกันความเสียหาย เช่น ต้องทำการปิดกั้นเว็ปไซต์ หรือ ระงับการทำธุรกรรมทางอิเลคทรอนิกส์ ให้พนักงานสอบสวนที่รับแจ้งความ หรือ ผู้เสียหายประสานงานมายัง บก.ปอท. หรือ กระทรวงไอซีที หรือธนาคาร หรือผู้ ให้บริการอินเทอร์เน็ตเพื่อดำเนินการเบื้องต้นในการบรรเทาความเสียหาย ต่อไป

*กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) สังกัดกองบัญชาการตำรวจสอบสวนกลาง(บช.ก.)

# การสอบถามข้อมูล

## : กรณีต้องการทราบรายละเอียดเพิ่มเติม/กรณีเป็นผู้เสียหาย

หากต้องการศึกษาข้อมูลและรายละเอียดเพิ่มเติมสามารถติดต่อได้ที่ไหน และมีหน่วยงานใดบ้างที่ดูแลรับผิดชอบ

สามารถศึกษาข้อมูลเพิ่มเติมเกี่ยวกับ พ.ร.บ.นี้ได้จากเว็บไซต์ของหลากหลาย หน่วยงานที่มีส่วนเกี่ยวข้องและรับผิดชอบ อาทิ

1. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม https://www.mdes.go.th
   - สอบถามข้อมูล /แจ้งข้อมูลเว็บไซต์ที่ไม่เหมาะสม
2. กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) https://www.cib.go.th/departments/technologyCrime
   - แจ้งความดำเนินคดี

...เป็นต้น

RUTS RAJAMANGALA UNIVERSITY OF TECHNOLOGY SRIVIJAYA

สรุป

# การกระทำที่ถือเป็นความผิดตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่ปรับปรุงแก้ไข พ.ศ.2560

## มาตรา ๕ - ๘ เข้าถึงระบบ/ข้อมูล ของผู้อื่นโดยมิชอบ

- เข้าถึงระบบคอมพิวเตอร์
- จำคุกไม่เกิน ๖ เดือน / ปรับไม่เกิน ๑ หมื่นบาท / ทั้งจำทั้งปรับ
- เข้าถึงข้อมูลคอมพิวเตอร์
- จำคุกไม่เกิน ๒ ปี / ปรับไม่เกิน ๔ หมื่นบาท / ทั้งจำทั้งปรับ
- ล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์และนำไปเปิดเผย
- จำคุกไม่เกิน ๑ ปี / ปรับไม่เกิน ๒ หมื่นบาท / ทั้งจำทั้งปรับ
- ดักรับข้อมูลคอมพิวเตอร์
- จำคุกไม่เกิน ๒ ปี / ปรับไม่เกิน ๔ หมื่นบาท / ทั้งจำทั้งปรับ

## มาตรา ๙ - ๑๐ แก้ไข/ ดัดแปลง/ ทำให้ข้อมูลเสียหาย

- ทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติม ข้อมูลของผู้อื่นโดยมิชอบ
- ทำให้ระบบคอมพิวเตอร์ของผู้อื่นไม่สามารถทำงานได้ตามปกติ
- จำคุกไม่เกิน ๕ ปี / ปรับไม่เกิน ๑ แสนบาท / ทั้งจำทั้งปรับ
- กรณีเป็นการกระทำต่อระบบหรือข้อมูลคอมพิวเตอร์ตามมาตรา ๑๒ จำคุก ๓ - ๑๕ ปี และ ปรับ ๖ หมื่น - ๓ แสนบาท
  - ถ้าเป็นเหตุให้เกิดอันตรายแก่บุคคลอื่น จำคุกไม่เกิน ๑๐ ปี และปรับ ๒ แสนบาท
  - ถ้าเป็นเหตุให้บุคคลอื่นถึงแก่ความตาย จำคุก ๕ - ๒๐ ปี และปรับ ๑ แสน - ๒ แสนบาท

## มาตรา ๑๑ ส่งข้อมูลหรืออีเมล์ก่อกวนผู้อื่น


- ส่งโดยปกปิดหรือปลอมแปลงแหล่งที่มา
- ปรับไม่เกิน ๑ แสนบาท
- ส่งโดยไม่เปิดโอกาสให้ปฏิเสธการตอบรับได้โดยง่าย
- จำคุกไม่เกิน ๒ ปี / ปรับไม่เกิน ๔ หมื่นบาท / ทั้งจำทั้งปรับ

## มาตรา ๑๒ เข้าถึงระบบ/ข้อมูลด้านความมั่นคงโดยมิชอบ

- เข้าถึงระบบหรือข้อมูลคอมพิวเตอร์
- ล่วงรู้มาตรการการป้องกันการเข้าถึงระบบคอมพิวเตอร์และนำไปเปิดเผย
- กรณีไม่เกิดความเสียหาย จำคุก ๑ - ๗ ปี และปรับ ๒ หมื่น - ๑.๔ แสนบาท
- กรณีเกิดความเสียหาย จำคุก ๑ - ๑๐ ปี และปรับ ๒ หมื่น - ๒ แสนบาท
- กรณีเป็นเหตุให้ผู้อื่นถึงแก่ความตาย จำคุก ๕ - ๒๐ ปี และปรับ ๑ แสน - ๔ แสนบาท

สรุป

# การกระทำที่ถือเป็นความผิดตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่ปรับปรุงแก้ไข พ.ศ.2560

## มาตรา ๑๓ จำหน่ายหรือเผยแพร่ชุดคำสั่งเพื่อนำไปใช้กระทำความผิด

- กรณีทำเพื่อเป็นเครื่องมือในการกระทำความผิดทางคอมพิวเตอร์ ตามมาตรา ๕ - ๑๑
  - จำคุกไม่เกิน ๑ ปี / ปรับไม่เกิน ๒ หมื่นบาท / ทั้งจำทั้งปรับ หากมีผู้นำไปใช้กระทำความผิด ผู้จำหน่าย/เผยแพร่ต้องรับผิดด้วย (เมื่อมีส่วนรู้เห็น)
  - หากมีผู้นำไปใช้กระทำความผิด หรือต้องรับผิดตามมาตรา ๑๒ ผู้จำหน่ายหรือเผยแพร่จะต้องรับผิดทางอาญาด้วย (เมื่อมีส่วนรู้เห็น)
- กรณีทำเพื่อเป็นเครื่องมือในการกระทำความผิดทางคอมพิวเตอร์ ตามมาตรา ๑๒
  - จำคุกไม่เกิน ๒ ปี / ปรับไม่เกิน ๔ หมื่นบาท / ทั้งจำทั้งปรับ หากมีผู้นำไปใช้กระทำความผิด ผู้จำหน่าย/เผยแพร่ต้องรับผิดด้วย (ทุกกรณี)

## มาตรา ๑๔ นำข้อมูลที่ผิด พ.ร.บ. เข้าสู่ระบบคอมพิวเตอร์

- ข้อมูลปลอม / ทุจริต / หลอกลวง
- ข้อมูลเท็จ
- ข้อมูลความผิดเกี่ยวกับความมั่นคงปลอดภัย ฯลฯ (มาตรา ๑๒)
- ข้อมูลความผิดเกี่ยวกับความมั่นคง / ก่อการร้าย
- ข้อมูลลามก ประชาชนเข้าถึงได้
- เผยแพร่ / ส่งต่อ ข้อมูล โดยรู้อยู่แล้วว่าผิด

กรณีการกระทำนั้น ส่งผลถึงประชาชน
จำคุกไม่เกิน ๕ ปี / ปรับไม่เกิน ๑ แสนบาท / ทั้งจำทั้งปรับ

กรณีการกระทำนั้น ส่งผลต่อบุคคลใดบุคคลหนึ่ง
จำคุกไม่เกิน ๓ ปี / ปรับไม่เกิน ๖ แสนบาท / ทั้งจำทั้งปรับ (ยอมความได้)

## มาตรา ๑๕ ให้ความร่วมมือ ยินยอม รู้เห็นเป็นใจ

- ผู้ให้บริการที่ให้ความร่วมมือ ยินยอม รู้เห็นเป็นใจให้มีการกระทำผิดตามมาตรา ๑๔ ต่อระบบคอมพิวเตอร์ของตน
- ต้องระวางโทษเช่นเดียวกับผู้กระทำผิด
  - หากผู้ให้บริการพิสูจน์ได้ว่าตนได้ปฏิบัติตามขั้นตอนการแจ้งเตือนแล้ว ไม่ต้องรับโทษ

** ผู้ให้บริการมีหน้าที่เก็บข้อมูลการใช้งานไว้ไม่น้อยกว่า ๙๐ วัน กรณีจำเป็น ศาลอาจสั่งให้เก็บเพิ่มได้ไม่เกิน ๒ ปี **

## มาตรา ๑๖ ตัดต่อ เติม ดัดแปลงภาพ

- ตัดต่อ เติม ดัดแปลงภาพ ผู้อื่น / ผู้ตาย นำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปเข้าถึงได้
  - ทำให้เสียชื่อเสียง ถูกดูหมิ่น - ทำให้ถูกเกลียดชัง ได้รับความอับอาย
- จำคุกไม่เกิน ๓ ปี และ ปรับไม่เกิน ๒ แสนบาท
  - ศาลอาจสั่งให้ทำลายข้อมูล / เผยแพร่คำพิพากษา / ดำเนินการอื่นเพื่อบรรเทาความเสียหายที่เกิดจากการกระทำ
  - ผู้ที่ครอบครองข้อมูลคอมพิวเตอร์ที่ศาลสั่งให้ทำลาย แต่ไม่ทำลายตามคำสั่ง ต้องรับโทษกึ่งหนึ่ง

(รวมถึงการกระทำความผิดตามมาตรา ๑๔ ด้วย)


สาระสำคัญ
พระราชบัญญัติคอมพิวเตอร์
(ฉบับที่ 2) พ.ศ.2560
1. การคุ้มครองประชาชน
- คุ้มครองความเป็นส่วนตัว
ให้ปฏิเสธไม่รับ spam ง่ายขึ้น
- คุ้มครองภาพบุคคลทั่วไป
2. บทลงโทษ
ฉ้อโกง ปลอม
ข้อมูลเป็นเท็จ
ตัดต่อ เผยแพร่
ภาพผู้เสียชีวิต
3. การเยียวยาความเสียหาย
ศาลอาจสั่งให้
- ชดเชยค่าเสียหาย
- ทำลายข้อมูล
- เผยแพร่คำพิพากษา
4.ลดคดีขึ้นสู่ศาล
ตำรวจมีอำนาจปรับ
สำหรับคดีที่มีอัตราโทษ
จำคุกไม่เกิน 1 เดือน
หรือปรับไม่เกิน 10,000 บ.
5. ศาลเป็นผู้มีอำนาจ
สั่งปิดเว็บไซต์
ที่มีเนื้อหา
ผิดกฎหมาย
6.การละเว้นโทษ
ยกเว้นความผิด
กรณีติชมอย่างเป็นธรรม

RUTS RAJAMANGALA UNIVERSITY OF TECHNOLOGY SRIVIJAYA

# ข้อต้องรู้ !

# พ.ร.บ.

## คอมพิวเตอร์ฯ

### ส่ง Email ขายของ

ถือเป็นสแปม ปรับ **200,000** บาท

### การฝากร้านใน

Facebook IG ถือเป็นสแปม ปรับ **200,000** บาท

### การโพสต์ด่าว่าผู้อื่น

มีกฎหมายอาญาอยู่แล้ว ไม่มีข้อมูลจริง หรือถูกตัดต่อ ผู้ถูกกล่าวหา เอาผิดผู้โพสต์ได้ โทษจำคุกไม่เกิน **3** ปี ปรับไม่เกิน **200,000** บาท

### การให้ข้อมูลเกี่ยวกับผู้เสียชีวิต

ต้องไม่ทำให้เกิดความเสื่อมเสียชื่อเสียง หรือถูกดูหมิ่น เกลียดชัง ญาติสามารถฟ้องร้องได้ตามกฎหมาย

### แอดมินเพจ

ที่เปิดให้มีการแสดงความเห็น เมื่อพบข้อความที่ผิด พ.ร.บ.ฯ เมื่อลบออกจากพื้นที่ที่ตนดูแล จะถือเป็นผู้พ้นผิด

### การโพสต์เกี่ยวกับเด็ก

เยาวชน ต้องปิดบังใบหน้า ยกเว้น เมื่อเป็นการเชิดชู ชื่นชม อย่างให้เกียรติ

### ไม่ทำการละเมิดลิขสิทธิ์ผู้ใด

ไม่ว่าข้อความ เพลง รูปภาพ หรือวิดีโอ

### ไม่โพสต์สิ่งลามกอนาจาร

ที่ทำให้เกิดการเผยแพร่สู่ประชาชนได้

### กด Like

ได้ไม่ผิด พ.ร.บ.ฯยกเว้นการกดไลค์ข้อมูลที่มีฐานความผิด และมีผลกระทบต่อสังคม เศรษฐกิจและความมั่นคงโดยเมื่อไต่สวนแล้วมีเจตนาในเนื้อหานั้น


### กด Share

ถือเป็นการเผยแพร่ หากข้อมูลที่แชร์ไม่มีผลกระทบต่อสังคม เศรษฐกิจ ความมั่นคง หรือละเมิดสิทธิส่วนบุคคล ไม่เป็นความผิด

### ส่ง SMS โฆษณา

โดยไม่รับความยินยอม ให้ผู้รับสามารถปฏิเสธข้อมูลนั้นได้ ไม่เช่นนั้นถือเป็นสแปม ปรับ **200,000** บาท

### ส่งรูปภาพแชร์ของผู้อื่น

เช่น สวัสดี อวยพร ไม่ผิด ถ้าไม่เอาภาพไปใช้ในเชิงพาณิชย์หารายได้

# กฎหมายที่ให้อำนาจรัฐ "ดักรับ" ข้อมูล


| กฎหมายที่เกี่ยวข้อง | พ.ร.บ. คอมพิวเตอร์ฯ | พ.ร.บ. ดีเอสไอฯ | พ.ร.บ. มั่นคงไซเบอร์ฯ | พ.ร.บ. ข่าวกรอง |
|---|---|---|---|---|
| อำนาจขอข้อมูลจากผู้ให้บริการ | ✓ | ✗ | ✓ | ✓ |
| เข้าถึงข้อมูลการสื่อสารด้วยตัวเอง | ✗ | ✗ | ✗ | ✓ |
| เข้าถึงข้อมูลการสื่อสารเมื่อได้รับอนุญาตจากศาล | ✓ | ✓ | ได้เฉพาะกรณีภัยคุกคามระดับร้ายแรงขึ้นไป | ไม่ต้องผ่านศาล |
| ถอดรหัสลับด้วยตัวเอง | ✗ | ✗ | ✗ | ✓ |
| ถอดรหัสลับเมื่อได้รับอนุญาตจากศาล | ✓ | ✓ | ได้เฉพาะกรณีภัยคุกคามระดับร้ายแรงขึ้นไป | ไม่ต้องผ่านศาล |
| ดักรับข้อมูลแบบReal-time | ✗ | ✗ | ได้เฉพาะกรณีภัยคุกคามระดับร้ายแรงขึ้นไป | ✓ |

# ชาวเน็ตสายวีน ระวัง !

## โดนคดีแพ่งและอาญา หากโพสต์แชร์ข้อมูล ทำทัวร์ลง

1. โพสต์ใส่ความบุคคลอื่นต่อบุคคลที่สาม ทำให้ผู้อื่นเสียชื่อเสียงถูกดูหมิ่นเกลียดชัง
2. โพสต์หมิ่นประมาทบุคคลอื่นโดยการโฆษณา (การโพสต์เป็นสาธารณะหรือบุคคลทั่วไปที่เข้าถึงได้)
3. ข่มขู่ ขู่เข็ญ ผู้อื่นผ่านสื่อสังคมออนไลน์ ทำให้ผู้อื่นเกิดความกลัว ตกใจ

4. ส่งต่อ แชร์ รีโพสต์ที่เข้าข่ายเป็นความผิด เสี่ยงต่อการถูกฟ้องร้องดำเนินคดี เช่นเดียวกับผู้โพสต์ ในฐานะผู้สนับสนุน
5. โพสต์ภาพของผู้อื่นที่เกิดจากการสร้างขึ้น ตัดต่อ หรือดัดแปลงด้วยวิธีการอื่นใด ทำให้ผู้อื่นเสียชื่อเสียงถูกดูหมิ่นเกลียดชัง

ผู้ใดได้รับความเสียหายจากการล้อเลียน กลั่นแกล้ง หรือหมิ่นประมาททางสื่อสังคมออนไลน์ สามารถแจ้งความร้องทุกข์ต่อพนักงานสอบสวนได้ที่สถานีตำรวจในท้องที่เกิดเหตุได้ตลอด 24 ชั่วโมง

ที่มา : ตำรวจสอบสวนกลาง (CIB)

**ANTI-FAKE NEWS CENTER ศูนย์ต่อต้านข่าวปลอม ประเทศไทย**

# การ "ปิดกั้นเนื้อหา" ตาม พ.ร.บ.คอมพิวเตอร์ฯ ปี 2560

| เนื้อหาที่ถูกปิดกั้นได้ | วิธีการปิดกั้นเนื้อหา |
|---|---|
| ข้อมูลที่เป็นความผิดตาม พ.ร.บ.คอมฯ | เจ้าพนักงานตาม พ.ร.บ.คอมฯ + ความเห็นชอบของรัฐมนตรี DE ขอหมายศาลเพื่อปิดกั้นหรือลบเนื้อหา |
| ข้อมูลที่กระทบต่อความมั่นคงฯ เช่น ม.112, ม.116 หรือก่อการร้าย | |
| ข้อมูลที่ละเมิดทรัพย์สินทางปัญญา หรือความผิดตามกฎหมายอื่น ที่มีลักษณะขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน | เจ้าหน้าที่ตามกฎหมายนั้น หรือ พนักงานสอบสวน ร้องขอเจ้าพนักงานตาม พ.ร.บ.คอมฯ + ความเห็นชอบของรัฐมนตรี DE ขอหมายศาลเพื่อปิดกั้นหรือลบเนื้อหา |
| ข้อมูลที่มีลักษณะขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน (แต่ไม่ผิดกฎหมายใด) | คณะกรรมการกลั่นกรองฯ เห็นชอบ และมอบหมายให้เจ้าพนักงานขออำนาจศาลดำเนินการปิดกั้นหรือลบเนื้อหา |

RUTS RAJAMANGALA UNIVERSITY OF TECHNOLOGY SRIVIJAYA

| การกระทำความผิด | โทษตามกฎหมาย |
| --- | --- |
| 1. แอบเข้าคอมฯ คนอื่น | จำคุก 6 เดือน (ม.5) |
| 2. แอบเข้าคอมฯ คนอื่นได้แล้วไปบอกต่อ | จำคุกไม่เกิน 1 ปี (ม.6) |
| 3. เข้าล้วงข้อมูลในคอมฯ คนอื่น | จำคุกไม่เกิน 2 ปี (ม.7) |
| 4. ดักจับข้อมูลบนเครือข่าย | จำคุกไม่เกิน 3 ปี (ม.8) |
| 5. แอบแก้ไขข้อมูลบนเครื่องคนอื่น | จำคุกไม่เกิน 5 ปี (ม.9) |
| 6. ก่อกวนทำให้ระบบคนอื่นล่ม | จำคุกไม่เกิน 5 ปี (ม.10) |
| 7. ทำผิดในข้อ5,6 แล้วเกิดความเสียหายกับหลายคน | จำคุก 10 ปีขึ้นไป (ม.12) |
| 8. ขายหรือเผยแพร่โปรแกรมเพื่อช่วยทำความผิด ในข้อ 1-7 | จำคุกไม่เกิน 1 ปี (ม.13) |
| 9. ลงภาพโป๊ บิดเบือน ท้าทายอำนาจรัฐ ทั้งคนโพสต์และเจ้าของเว็บ | จำคุกไม่เกิน 5 ปี (ม.15) |
| 10. เผยแพร่รูปตัดต่อชาวบ้าน | จำคุกไม่เกิน 3 ปี (ม.16) |

LA

W

# THA

Presented by **Asst.Prof.Nitiporn Vonnasopon**

# กิจกรรมรายบุคคล 5 คะแนน

ให้นักศึกษาสืบค้นข้อมูลมานำเสนอเกี่ยวกับอุปกรณ์รักษาความปลอดภัยทางคอมพิวเตอร์ หรือระบบเครือข่าย คนละ 1 อย่าง โดยบอกรายละเอียดดังนี้

(นำเสนอรูปภาพ และอธิบายการรักษาความปลอดภัย รูปแบบการรักษาความปลอดภัยมีการทำงานขั้นตอนอย่างไร). >>> **ส่งวันที่ 3 มกราคม 68**

ให้นักศึกษาสรุปข้อมูล พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐” ในรูปแบบ MIND MAP >>> **ส่งวันที่ 9 มกราคม 68**