

บทที่ 11 กฎหมายและจริยธรรมทางเทคโนโลยีสารสนเทศ

วัตถุประสงค์

1. มีความรู้ในเรื่องกฎหมายเทคโนโลยีสารสนเทศ
2. มีความรู้เกี่ยวกับพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
3. มีความรู้เกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550
4. มีความรู้เกี่ยวกับอาชญากรรมคอมพิวเตอร์ และศึกษากฎนี้ตัวอย่างเกี่ยวกับการกระทำ

ความผิดและกฎหมาย

5. คำแนะนำเพื่อป้องกันการกระทำความผิด
6. มีความรู้เกี่ยวกับจริยธรรมกับเทคโนโลยีสารสนเทศ

บทนำ

สังคมสารสนเทศเป็นสังคมใหม่ เพื่อให้การอยู่ร่วมกันของคนในสังคมเป็นไปโดยสันติและสงบสุข เอื้อประโยชน์ซึ่งกันและกัน จึงต้องมีกฎเกณฑ์ที่กำหนดควบคุมเพื่อให้สังคมดังกล่าวให้มีความสงบเรียบร้อย

ในปัจจุบันเครือข่ายอินเทอร์เน็ตได้เข้ามามีบทบาท ในชีวิตประจำวัน มีการใช้คอมพิวเตอร์ และระบบสื่อสารกันมาก ขณะเดียวกันก็มีผู้ใช้เทคโนโลยีสารสนเทศในทางที่ไม่ถูก ไม่ควร ดังนั้นจึงจำเป็นต้องมีกฎหมายเทคโนโลยีสารสนเทศมาใช้บังคับควบคุมการใช้เทคโนโลยีสารสนเทศ และเมื่อมีกฎหมายออกมาบังคับใช้แล้ว ผู้ใช้เทคโนโลยีสารสนเทศจะปฏิเสธว่าไม่รู้กฎหมายไม่ได้

กฎหมายเทคโนโลยีสารสนเทศ

กฎหมายเทคโนโลยีสารสนเทศ (Information Law) หรือมักเรียกกันว่า กฎหมายไอที (IT Law) เสนอโดยกระทรวงวิทยาศาสตร์ เทคโนโลยี และ สิ่งแวดล้อม และเห็นชอบให้คณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ (National Information Technology Committee) หรือที่เรียกโดยย่อว่า คณะกรรมการไอทีแห่งชาติ หรือ กทสช. (NITC) ทำหน้าที่เป็นศูนย์กลางและประสานงานระหว่างหน่วยงานต่าง ๆ ดำเนินการจัดทำกฎหมายเทคโนโลยีสารสนเทศและกฎหมายอื่น ๆ ที่เกี่ยวข้อง ทั้งนี้คณะกรรมการไอทีแห่งชาติหรือ กทสช. (NITC) ได้แต่งตั้งคณะอนุกรรมการเฉพาะกิจ เพื่อยกร่างกฎหมายไอทีทั้ง 6 ฉบับ โดยมอบหมายให้ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (National Electronics and Computer Technology Center) หรือที่มักเรียกโดยย่อว่า "เนคเทค" (NECTEC) สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (National Science

and Technology Development Agency) หรือที่เรียกโดยย่อว่า "สวทช." กระทรวงวิทยาศาสตร์ เทคโนโลยี และสิ่งแวดล้อม ในฐานะสำนักงานเลขานุการคณะกรรมการไอทีแห่งชาติ ทำหน้าที่เป็นเลขานุการในการยกร่างกฎหมายไอทีทั้ง 6 ฉบับ เนคเทคจึงได้เริ่มต้นโครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศขึ้น เพื่อปฏิบัติตามนโยบายที่ได้รับมอบหมายจากรัฐบาลและคณะกรรมการไอทีแห่งชาติ ในการยกร่างกฎหมายไอทีทั้ง 6 ฉบับ ให้แล้วเสร็จ คือ

1. กฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ (Electronic Transactions Law)

เพื่อรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ให้เสมอข้อมูลที่ทำในกระดาษ อันเป็นการรองรับนิติสัมพันธ์ต่าง ๆ ซึ่งแต่เดิมอาจจะจัดทำขึ้นในรูปแบบของหนังสือให้เท่าเทียมกับนิติสัมพันธ์รูปแบบใหม่ที่จัดทำขึ้นให้อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ รวมตลอดทั้งการลงลายมือชื่อในข้อมูลอิเล็กทรอนิกส์ และการรับฟังพยานหลักฐานที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์

2. กฎหมายเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signatures Law)

เพื่อรับรองการใช้ลายมือชื่ออิเล็กทรอนิกส์ด้วยกระบวนการใด ๆ ทางเทคโนโลยีให้เสมอด้วยการลงลายมือชื่อธรรมดา อันส่งผลต่อความเชื่อมั่นมากขึ้นในการทำธุรกรรมทางอิเล็กทรอนิกส์ และกำหนดให้มีการกำกับดูแลการให้บริการ เกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ตลอดจนการให้บริการอื่น ที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์

3. กฎหมายเกี่ยวกับการพัฒนาโครงสร้างพื้นฐานสารสนเทศให้ทั่วถึง และเท่าเทียมกัน (National Information Infrastructure Law)

เพื่อก่อให้เกิดการส่งเสริม สนับสนุน และพัฒนาโครงสร้างพื้นฐานสารสนเทศ อันได้แก่โครงข่ายโทรคมนาคม เทคโนโลยีสารสนเทศ สารสนเทศทรัพยากรมนุษย์ และโครงสร้างพื้นฐานสารสนเทศสำคัญอื่น ๆ อันเป็นปัจจัยพื้นฐาน สำคัญในการพัฒนาสังคม และชุมชนโดยอาศัยกลไกของรัฐ ซึ่งรองรับเจตนารมณ์สำคัญประการหนึ่งของแนวนโยบายพื้นฐานแห่งรัฐตาม รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550 มาตรา 78 (3) ในการกระจายสารสนเทศให้ทั่วถึง และเท่าเทียมกัน และนับเป็นกลไกสำคัญในการช่วยลดความเหลื่อมล้ำของสังคมอย่างค้ำเป็นค้ำไป เพื่อสนับสนุนให้ท้องถิ่นมีศักยภาพในการปกครองตนเองพัฒนาเศรษฐกิจภายในชุมชน และนำไปสู่สังคมแห่งปัญญา และการเรียนรู้

4. กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Law)

เพื่อก่อให้เกิดการรับรองสิทธิ และให้ความคุ้มครองข้อมูลส่วนบุคคลซึ่งอาจถูกประมวลผลเปิดเผยหรือเผยแพร่ถึงบุคคลจำนวนมากได้ในระยะเวลาอันรวดเร็วโดยอาศัยพัฒนาการทางเทคโนโลยี จนอาจก่อให้เกิดการนำข้อมูลนั้นไปใช้ในทางมิชอบอันเป็นการละเมิดต่อเจ้าของข้อมูล ทั้งนี้โดยคำนึงถึงการรักษาคุณภาพระหว่างสิทธิขั้นพื้นฐานในความเป็นส่วนตัว เสรีภาพในการติดต่อสื่อสาร และความมั่นคงของรัฐ

5. กฎหมายเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (Computer Crime Law)

เพื่อกำหนดมาตรการทางอาญา ในการลงโทษผู้กระทำความผิดต่อระบบการทำงานของคอมพิวเตอร์ระบบ ข้อมูล และระบบเครือข่าย ทั้งนี้เพื่อเป็นหลักประกันสิทธิเสรีภาพ และการคุ้มครองการอยู่ร่วมกันของสังคม

6. กฎหมายเกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์ (Electronic Funds Transfer Law)

เพื่อกำหนดกลไกสำคัญทางกฎหมายในการรองรับระบบการโอนเงินทางอิเล็กทรอนิกส์ ทั้งที่เป็นการโอนเงินระหว่างสถาบันการเงิน และ ระบบการชำระเงินรูปแบบใหม่ในรูปแบบของเงินอิเล็กทรอนิกส์ก่อให้เกิดความเชื่อมั่น ต่อระบบการทำธุรกรรมทางการเงิน และการทำธุรกรรมทางอิเล็กทรอนิกส์มากยิ่งขึ้น

ต่อมาคณะกรรมการกฤษฎีกาได้นำร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์และร่างพระราชบัญญัติลายมือชื่ออิเล็กทรอนิกส์รวมเป็นฉบับเดียว โดยได้ผ่านร่างพระราชบัญญัติดังกล่าวให้รัฐสภาพิจารณาและตราเป็นพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ดังนั้นกฎหมายเทคโนโลยีสารสนเทศของไทยในปัจจุบันจึงมีทั้งสิ้น 5 ฉบับ ได้แก่

1. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
2. ร่างพระราชบัญญัติว่าด้วยการพัฒนาโครงสร้างพื้นฐานสารสนเทศ พ.ศ...
3. ร่างพระราชบัญญัติว่าด้วย ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ...
4. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
5. ร่างพระราชบัญญัติว่าด้วยการโอนเงินทางอิเล็กทรอนิกส์ พ.ศ...

จะเห็นได้ว่ากฎหมายดังที่กล่าวมาข้างต้นทั้ง 5 ฉบับ มี 3 ฉบับที่เป็นร่างของกฎหมายซึ่งยังคงอยู่ในขั้นตอนการพิจารณาออกบังคับใช้ จึงควรพิจารณาแต่เฉพาะกฎหมายที่มีผลบังคับใช้อยู่ในปัจจุบัน คือ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มีผลบังคับใช้เมื่อวันที่ 3 เมษายน 2545 นับเป็นกฎหมายเทคโนโลยีสารสนเทศฉบับแรกที่ใช้บังคับกับการทำธุรกรรมทางอิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์ เนื่องจากการทำธุรกรรมทางอิเล็กทรอนิกส์บางประเภท เช่น การทำสัญญา กฎหมายกำหนดว่าต้องมีการลงลายมือชื่อคู่สัญญาจึงจะมีผลสมบูรณ์และใช้บังคับได้ตามกฎหมาย กฎหมายทั้งสองส่วนจึงมีความสัมพันธ์กันอย่างใกล้ชิด

ความเป็นมาของพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

รับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ที่ใช้ในการทำธุรกรรมหรือสัญญา

- รับรองตราประทับอิเล็กทรอนิกส์ซึ่งเป็นสิ่งที่สามารถระบุถึงตัวผู้ทำธุรกรรมทางอิเล็กทรอนิกส์ได้เช่นเดียวกับลายมือชื่ออิเล็กทรอนิกส์
- สามารถนำเอกสารซึ่งเป็นสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์มาใช้แทน ต้นฉบับหรือให้เป็นพยานหลักฐานในศาลได้
- ส่งเสริมความเชื่อมั่นในการทำธุรกรรมทาง อิเล็กทรอนิกส์และเสริมสร้างศักยภาพการแข่งขันในเวทีการค้าระหว่างประเทศ

เจตนารมณ์ในการร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

โดยที่การทำธุรกรรมในปัจจุบันมี แนวโน้มที่จะปรับเปลี่ยนวิธีการในการติดต่อสื่อสารที่อาศัยการพัฒนาการเทคโนโลยีทาง อิเล็กทรอนิกส์ซึ่งมีความสะดวก รวดเร็วและมีประสิทธิภาพ แต่เนื่องจากการทำธุรกรรมทาง อิเล็กทรอนิกส์ดังกล่าวมีความแตกต่างจากวิธีการทำธุรกรรมซึ่งมีกฎหมายรองรับอยู่ในปัจจุบันเป็น อย่างมาก อันส่งผลให้ต้องมีการรองรับสถานะทางกฎหมายของข้อมูลทางอิเล็กทรอนิกส์ให้เสมือนกับ การทำเป็นหนังสือ หรือ หลักฐานเป็นหนังสือ การรับรองวิธีการส่งและรับข้อมูลอิเล็กทรอนิกส์การใช้ ลายมือชื่ออิเล็กทรอนิกส์ตลอดจนการ รับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์เพื่อเป็นการ ส่งเสริมการทำธุรกรรมทางอิเล็กทรอนิกส์ให้น่าเชื่อถือ และมีผลในทางกฎหมายเช่นเดียวกับการทำ ธุรกรรมโดยวิธีการทั่วไปที่เคยปฏิบัติอยู่เดิม อันจะเป็นการส่งเสริม ความเชื่อมั่นในการทำธุรกรรมทาง อิเล็กทรอนิกส์และเสริมสร้างศักยภาพการแข่งขันในเวทีการค้าระหว่างประเทศ

สาระสำคัญ

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มีทั้งหมด 46 มาตรา ซึ่งในบทเรียนนี้จะกล่าวถึง หมวดที่ 1 ธุรกรรมทางอิเล็กทรอนิกส์ หมวดที่ 2 ลายมือชื่ออิเล็กทรอนิกส์ และหมวดที่ 6 บทกำหนดโทษ ในบางมาตราเท่านั้น

บทนิยามศัพท์

มาตรา 4 ในพระราชบัญญัตินี้

“ธุรกรรมทางอิเล็กทรอนิกส์” หมายความว่า ธุรกรรมที่กระทำขึ้นโดยใช้วิธีการทาง อิเล็กทรอนิกส์ ทั้งหมดหรือแต่บางส่วน

“ข้อมูลอิเล็กทรอนิกส์” หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือ ประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร

“ลายมือชื่ออิเล็กทรอนิกส์” หมายความว่า อักษร อักขระ ตัวเลข เสียงหรือสัญลักษณ์อื่นใดที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์ซึ่งนำมาใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดง ความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็น เจ้าของลายมือชื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้น และเพื่อแสดงว่าคุณคน ดังกล่าวยอมรับข้อความในข้อมูลอิเล็กทรอนิกส์นั้น

“เจ้าของลายมือชื่อ” หมายความว่า ผู้ซึ่งถือข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์ และสร้างลายมือชื่ออิเล็กทรอนิกส์นั้นในนามตนเองหรือแทนบุคคลอื่น

หมวด 1 อธิบายกฎหมายทางอิเล็กทรอนิกส์

การรองรับสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์

มาตรา 7 “ห้ามมิให้ปฏิเสธความมีผลผูกพันและการบังคับใช้ทางกฎหมายของข้อความใด เพียงเพราะเหตุที่ข้อความนั้นอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์”

มาตรานี้เป็นมาตราสำคัญที่สุดของพระราชบัญญัตินี้โดยเป็นการกำหนดหลักการพื้นฐานมิให้เลือกปฏิบัติระหว่างสิ่งที่ทำขึ้นเป็นหนังสือกับข้อมูลอิเล็กทรอนิกส์ แต่มาตรานี้เป็นเพียงมาตราที่ห้ามมิให้ปฏิเสธผลทางกฎหมายของข้อมูลอิเล็กทรอนิกส์เท่านั้น มิได้เป็นการรับรองว่าข้อมูลนั้นถูกต้องสมบูรณ์

การทำเป็นหนังสือ

มาตรา 8 “ภายใต้บังคับบทบัญญัติแห่งมาตรา ๘ ในกรณีที่ถูกกฎหมายกำหนดให้การใดต้องทำ เป็นหนังสือ มีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดง ถ้าได้มีการจัดทำข้อความขึ้นเป็นข้อมูล อิเล็กทรอนิกส์ที่สามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง ให้ถือว่าข้อความ นั้นได้ทำเป็นหนังสือ มีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดงแล้ว”

มาตรานี้บัญญัติขึ้นเพื่อขยายหลักการทั่วไปตามมาตรา 7 ซึ่งให้ถือว่าข้อความอิเล็กทรอนิกส์ที่ทำขึ้นนั้นเป็นข้อความที่ได้ทำเป็นหนังสือ มีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดงตามที่กฎหมายกำหนดแล้ว

ลายมือชื่อ

มาตรา 9 “ในกรณีที่บุคคลพึงลงลายมือชื่อในหนังสือ ให้ถือว่าข้อมูลอิเล็กทรอนิกส์นั้น มีการลงลายมือชื่อแล้ว ถ้า

(1) ใช้วิธีการที่สามารถระบุตัวเจ้าของลายมือชื่อ และสามารถแสดงได้ว่าเจ้าของลายมือชื่อ รับรองข้อความในข้อมูลอิเล็กทรอนิกส์นั้นว่าเป็นของตน และ

(2) วิธีการดังกล่าวเป็นวิธีการที่เชื่อถือได้โดยเหมาะสมกับวัตถุประสงค์ของการสร้างหรือส่ง ข้อมูลอิเล็กทรอนิกส์โดยคำนึงถึงพฤติการณ์แวดล้อมหรือข้อตกลงของคู่กรณี

วิธีการที่เชื่อถือได้ตาม (2) ให้คำนึงถึง

ก. ความมั่นคงและรัดกุมของการใช้วิธีการหรืออุปกรณ์ในการระบุตัวบุคคล สภาพพร้อมใช้ งานของทางเลือกในการระบุตัวบุคคล กฎเกณฑ์เกี่ยวกับลายมือชื่อที่กำหนดไว้ในกฎหมายระดับ ความมั่นคงปลอดภัยของการใช้ลายมือชื่ออิเล็กทรอนิกส์การปฏิบัติตามกระบวนการในการระบุตัว บุคคลผู้เป็นสื่อกลาง ระดับของการยอมรับหรือไม่ยอมรับ วิธีการที่ใช้ในการระบุตัวบุคคลในการทำ ธุรกิจ วิธีการระบุตัวบุคคล ณ ช่วงเวลาที่มีการทำธุรกรรมและติดต่อสื่อสาร

ข. ลักษณะ ประเภท หรือขนาดของธุรกรรมที่ทำ จำนวนครั้งหรือความสม่ำเสมอในการทำ ธุรกิจ ประเพณีทางการค้าหรือทางปฏิบัติความสำคัญ มูลค่าของธุรกรรมที่ทำ หรือ

ค. ความรัดกุมของระบบการติดต่อสื่อสาร ให้นำความในวรรคหนึ่งมาใช้บังคับกับการประทับตราของนิติบุคคลด้วยวิธีการทาง อิเล็กทรอนิกส์ด้วยโดยอนุโลม”

มาตรานี้บัญญัติขึ้นเพื่อรับรองสถานะทางกฎหมายของลายมือชื่อในข้อมูลอิเล็กทรอนิกส์เพื่อระบุหรือยืนยันตัวบุคคล เป็นอีกมาตราหนึ่งที่ขยายเงื่อนไขเพิ่มเติมมาตรา 7 มาตรา 9 เป็นบทบัญญัติที่กำหนดขึ้นบนพื้นฐานหลักความเท่าเทียมกัน ระหว่าง “ลายเซ็นหรือลายมือชื่อที่อยู่บนกระดาษ” กับ ลายมือชื่อที่อยู่ในรูปข้อมูลอิเล็กทรอนิกส์ ซึ่งลายมือชื่อขึ้นอยู่กับคู่กรณีว่าจะประสงค์ใช้แบบใด

การรับฟังพยานหลักฐานและชั่งน้ำหนักพยานหลักฐาน

มาตรา 11 “ห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในกระบวนการพิจารณาตามกฎหมายทั้งในคดีแพ่ง คดีอาญา หรือคดีอื่นใด เพียงเพราะเหตุว่าเป็นข้อมูลอิเล็กทรอนิกส์

ในการชั่งน้ำหนักพยานหลักฐานว่าข้อมูลอิเล็กทรอนิกส์จะเชื่อถือได้หรือไม่เพียงใดนั้นให้พิจารณาถึงความน่าเชื่อถือของลักษณะหรือวิธีการที่ใช้สร้าง เก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์ ลักษณะหรือวิธีการเก็บรักษา ความครบถ้วน และไม่มีการเปลี่ยนแปลงของข้อความลักษณะ หรือวิธีการที่ใช้ในการระบุหรือแสดงตัวผู้ส่งข้อมูล รวมทั้งพฤติการณ์ที่เกี่ยวข้องทั้งปวงให้นำความในวรรคหนึ่งมาใช้บังคับกับสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์ด้วย”

มาตรานี้ได้กำหนดห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานใน กระบวนการพิจารณาคดีเพียงเพราะข้อมูลดังกล่าวเป็นข้อมูลอิเล็กทรอนิกส์

สัญญาและเจตนาในรูปของข้อมูลอิเล็กทรอนิกส์

มาตรา 13 “คำเสนอหรือคำสนองในการทำสัญญาอาจทำเป็นข้อมูลอิเล็กทรอนิกส์ก็ได้ และห้ามมิให้ปฏิเสธการมีผลทางกฎหมายของสัญญาเพียงเพราะเหตุที่สัญญานั้นได้ทำคำเสนอหรือคำสนองเป็นข้อมูลอิเล็กทรอนิกส์”

มาตรา 14 “ในระหว่างผู้ส่งข้อมูลและผู้รับข้อมูล การแสดงเจตนาหรือคำบอกกล่าวอาจทำเป็นข้อมูลอิเล็กทรอนิกส์ก็ได้”

การแสดงเจตนาและการทำสัญญาจะไม่ถูกปฏิเสธโดยผลของกฎหมายแม้กระทำให้ขึ้นในรูปของข้อมูลอิเล็กทรอนิกส์ โดยบทบัญญัติดังกล่าวจะคำนึงถึงหลักความศักดิ์สิทธิ์แห่งการแสดงเจตนา อย่างไรก็ตามมาตรา 13 ยังใช้ได้กับคำเสนอ หรือคำสนองอย่างใดอย่างหนึ่งทางอิเล็กทรอนิกส์ด้วย

หมวดที่ 2 ลายมือชื่ออิเล็กทรอนิกส์

ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้

มาตรา 26 “ลายมือชื่ออิเล็กทรอนิกส์ที่มีลักษณะดังต่อไปนี้ให้ถือว่าเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้

(1) ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์นั้นได้เชื่อมโยงไปยังเจ้าของลายมือชื่อ โดยไม่เชื่อมโยงไปยังบุคคลอื่นภายใต้สภาพที่นำมาใช้

(2) ในขณะที่สร้างลายมือชื่ออิเล็กทรอนิกส์นั้น ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น

(3) การเปลี่ยนแปลงใดๆ ที่เกิดแก่ลายมือชื่ออิเล็กทรอนิกส์ นับแต่เวลาที่ได้สร้างขึ้นสามารถจะตรวจพบได้ และ

(4) ในกรณีที่กฎหมายกำหนดให้การลงลายมือชื่ออิเล็กทรอนิกส์เป็นไปเพื่อรับรองความครบถ้วนและไม่มี การเปลี่ยนแปลงของข้อความ การเปลี่ยนแปลงใดแก่ข้อความนั้นสามารถตรวจพบได้นับแต่เวลาที่ลงลายมือชื่ออิเล็กทรอนิกส์

บทบัญญัติในวรรคหนึ่ง ไม่เป็นการจำกัดว่าไม่มีวิธีการอื่นใดที่แสดงได้ว่าเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ หรือการแสดงพยานหลักฐานใดเกี่ยวกับความไม่น่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์”

หมวดที่ 6 บทกำหนดโทษ

มาตรา 44 “ผู้ใดประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์โดยไม่แจ้งหรือขึ้นทะเบียนต่อพนักงานเจ้าหน้าที่ตามที่กำหนดในพระราชกฤษฎีกาตามมาตรา 33 วรรคหนึ่ง หรือโดยฝ่าฝืน คำสั่งห้ามการประกอบธุรกิจของคณะกรรมการตามมาตรา 33 วรรคหก ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ”

มาตรา 45 “ผู้ใดประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์โดยไม่ได้รับใบอนุญาตตามมาตรา 34 ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสองแสนบาท หรือทั้งจำทั้งปรับ”

มาตรา 46 “บรรดาความผิดตามพระราชบัญญัตินี้ที่กระทำโดยนิติบุคคล ผู้จัดการหรือผู้แทนนิติบุคคล หรือผู้ซึ่งมีส่วนร่วมในการดำเนินงานของนิติบุคคล ต้องรับผิดในความผิดนั้นด้วยเว้นแต่พิสูจน์ได้ว่าตนมิได้รู้เห็น หรือมีส่วนร่วมในการกระทำความผิดนั้น”

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ผ่านการเห็นชอบจากสภานิติบัญญัติ การลงพระปรมาภิไธย และการประกาศลงในราชกิจจานุเบกษาแล้ว เมื่อ 18 มิถุนายน พ.ศ. 2550 และจะมีผลใช้บังคับตั้งแต่ 19 กรกฎาคม พ.ศ. 2550 เป็นต้นไป ดังนั้นผู้ใช้คอมพิวเตอร์ อินเทอร์เน็ตโดยทั่วไป ผู้ให้บริการ ซึ่งรวมไปถึงหน่วยงานต่างๆ ที่เปิดบริการอินเทอร์เน็ตให้แก่ผู้อื่นหรือ กลุ่มพนักงานนักศึกษาในองค์กร ควรทราบถึงรายละเอียดของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยประเทศไทยได้มีการนำค้ใช้เป็นที่เรียบร้อยแล้ว

ความเป็นมาของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

สภาพปัญหาเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ในปัจจุบัน

- ความสำคัญของคอมพิวเตอร์ในชีวิตประจำวัน
- ผลของการกระทำผิดกระทบหรือความเสียหายในวงกว้างและรวดเร็ว
- ยังไม่มีกฎหมายกำหนดความผิดมาก่อน
 - การที่กฎหมายอาญามุ่งคุ้มครอง วัตถุที่มีรูปร่างเท่านั้น แต่ในยุคไอที ข้อมูลข่าวสารเป็นวัตถุที่ไม่มีรูปร่าง ตัวอย่างของการก่ออาชญากรรมทางคอมพิวเตอร์ ได้แก่ การโจรกรรมเงินในบัญชีลูกค้าของธนาคาร การโจรกรรมความลับของบริษัทต่างๆ ที่เก็บไว้ในคอมพิวเตอร์ การปล่อยไวรัสเข้าไปในคอมพิวเตอร์
 - พยานหลักฐานที่เกี่ยวข้องกับคอมพิวเตอร์นั้นสามารถเปลี่ยนแปลงได้ตลอดเวลาและถูกกระทำได้ง่ายแต่ยากต่อการสืบหา
 - ปัญหาเรื่องขอบเขตพื้นที่ซึ่งเป็นเรื่องที่มีความสำคัญ เพราะผู้กระทำความผิดอาจกระทำจากที่อื่นๆ ที่ไม่ใช่ประเทศไทย ซึ่งอยู่นอกเขตอำนาจของศาลไทย

เจตนารมณ์ในการร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พ.ศ. 2550

เนื่องจากปัญหาภัยคุกคามที่เกิดจาก ไวรัสคอมพิวเตอร์ แสกเกอร์ การเผยแพร่ รูปภาพ ข้อความ ที่มีลักษณะลามก อนาจาร หรือข้อมูลอันเป็นเท็จที่ก่อให้เกิดความเสียหายต่อบุคคล ต่อความมั่นคงทางการเมือง สังคม และเศรษฐกิจของประเทศ จึงเป็นเหตุให้เกิดการร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ขึ้นโดยมีเจตนารมณ์ดังนี้

1. เพื่อเป็นการใช้กรอบแห่งกฎหมายในการกำหนดฐานความผิดและบทลงโทษในการเรียกค่าเสียหายแก่ผู้กระทำความผิดเพื่อคุ้มครองสิทธิให้แก่ประชาชน
2. เพื่อกำหนดบทบัญญัติเกี่ยวกับอำนาจหน้าที่ของเจ้าพนักงาน เจ้าหน้าที่ทั้งด้านนโยบาย มาตรฐาน แนวปฏิบัติ และกำหนดหน้าที่ของผู้ให้บริการไม่ว่าจะแก่ตนเองหรือบุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยผ่านระบบคอมพิวเตอร์ก็ตาม โดยให้มีแนวทางการปฏิบัติการดำเนินงานให้เกิดความชัดเจนถูกต้องในแนวทางเดียวกัน

สาระสำคัญ

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีทั้งหมด 30 มาตรา ซึ่งในบทเรียนนี้จะกล่าวถึงหมวดที่ 1 ความผิดเกี่ยวกับคอมพิวเตอร์ เท่านั้น

บทนิยามศัพท์

มาตรา 3 ในพระราชบัญญัตินี้

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้ อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดา ที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้ หมายความว่ารวมถึง ข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

“ข้อมูลจราจรทางคอมพิวเตอร์” หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบ คอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิดต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

“ผู้ให้บริการ” หมายความว่า

(๑) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดย ประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือ ในนามหรือเพื่อประโยชน์ของบุคคลอื่น

(๒) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

หมวดที่ 1 ความผิดเกี่ยวกับคอมพิวเตอร์ ฐานความผิดและบทลงโทษสำหรับการกระทำโดยมิชอบ

การเข้าถึงระบบคอมพิวเตอร์

มาตรา 5 “ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่ มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและ มาตรการนั้นมีได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ”

“การเข้าถึง” หมายถึงการเข้าถึงทั้งในระดับกายภาพ เช่น กรณีที่มีการกำหนดรหัสผ่านเพื่อป้องกันมิให้บุคคลอื่นใช้เครื่องคอมพิวเตอร์และผู้กระทำความผิดดำเนินการด้วยวิธีใดวิธีหนึ่งเพื่อให้ได้รหัสผ่านนั้นมาและ สามารถใช้เครื่องคอมพิวเตอร์นั้นได้โดยนั่งอยู่หน้าเครื่องคอมพิวเตอร์นั่นเอง และ หมายความรวมถึงการเข้าถึงระบบคอมพิวเตอร์หรือเข้าถึงข้อมูลคอมพิวเตอร์แม้ตัวบุคคลที่เข้าถึงจะอยู่ห่างโดยระยะทางกับเครื่องคอมพิวเตอร์แต่สามารถเจาะเข้าไปในระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่ตนต้องการได้

การล่วงรู้มาตรการป้องกันการเข้าถึง

มาตรา 6 “ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึง ระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านำ มาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแต่ ผู้อื่น ต้องระวางโทษจำคุกไม่เกิน หนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ”

องค์ประกอบความผิดมาตรานี้ ประกอบด้วย

(1) ล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้น เป็นการเฉพาะ หมายความว่า ระบบคอมพิวเตอร์นั้นมีมาตรการป้องกันการเข้าถึง เช่นมีการลงทะเบียน username และ password หรือมีวิธีการอื่นใดที่จัดทำขึ้นเป็นการเฉพาะ และไม่สำคัญว่าผู้กระทำล่วงรู้ถึงมาตรการ ป้องกันมาโดยชอบ หรือไม่ชอบ

- (2) เปิดเผยโดยมิชอบ หมายความว่าเพียงแต่นำมาตรการนั้นเปิดเผยแก่ผู้หนึ่งผู้ใดหรือหลายคนก็เข้าองค์ประกอบความผิดแล้วเมื่อเปิดเผยแล้วผู้ใดจะทราบหรือนำไปใช้หรือไม่สำคัญ
- (3) ในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น เป็นองค์ประกอบความผิดอีกประการหนึ่งที่ต้องพิจารณาด้วยว่าการเปิดเผยนั้น อยู่ในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือไม่หากเป็นเรื่องที่ไม่น่าจะทำให้ผู้ใดเสียหายก็ไม่มี ความผิด
- (4) เจตนาตามประมวลกฎหมายอาญา มาตรา 59 กล่าวคือ ผู้กระทำได้กระทำโดยรู้สำนึกในการที่กระทำ และในขณะที่เดียวกันผู้กระทำประสงค์ต่อผลหรือย่อมเล็งเห็นผลของการกระทำนั้น ซึ่งถ้าผู้กระทำไม่มีเจตนาที่ย่อมไม่มีความผิด

การเข้าถึงข้อมูลคอมพิวเตอร์

มาตรา 7 “ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาทหรือทั้งจำทั้งปรับ”

องค์ประกอบความผิดตามมาตรา 7 ตรงกับองค์ประกอบความผิดตามมาตรา 5 เพียงแต่เปลี่ยนจาก “ระบบคอมพิวเตอร์” เป็น “ข้อมูลคอมพิวเตอร์”

การดักจับข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ

มาตรา 8 “ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการ ทางอิเล็กทรอนิกส์เพื่อดักจับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ ระหว่างการส่งในระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ ต้องระวางโทษจำคุกไม่เกินสามปีหรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ”

ตามคำอธิบายของเนคเทคประกอบการเสนอร่างกฎหมายมีดังนี้ การดักจับข้อมูลในมาตรานี้ หมายถึง การดักจับโดยวิธีการทางเทคนิค (technical means) เพื่อลักลอบดักฟัง (listen) ตรวจสอบ (monitoring) หรือติดตาม เนื้อหาสาระของข่าวสาร (surveillance) ที่สื่อสารถึงกันระหว่างบุคคล หรือเป็นการกระทำเพื่อให้ได้มาซึ่งเนื้อหาของข้อมูลโดยตรงหรือโดยการเข้าถึงและใช้ระบบคอมพิวเตอร์หรือการทำให้ได้มาซึ่งเนื้อหาของข้อมูลโดยทางอ้อมด้วยการแอบบันทึกข้อมูลสื่อสารถึงกันด้วยอุปกรณ์อิเล็กทรอนิกส์โดยไม่คำนึงว่าอุปกรณ์อิเล็กทรอนิกส์ที่ใช้บันทึกข้อมูลดังกล่าวจะต้องเชื่อมต่อเข้ากับสายสัญญาณสำหรับส่งผ่านข้อมูลหรือไม่ เพราะบางกรณีอาจใช้อุปกรณ์เช่นนั้นเพื่อบันทึกการสื่อสารข้อมูลที่ได้ส่งผ่านด้วย วิธีการแบบไร้สายก็ได้ เช่นการติดต่อผ่านทางโทรศัพท์เคลื่อนที่การติดต่อโดยใช้เทคโนโลยีไร้สายประเภท wireless LAN เป็นต้น อีกทั้งข้อมูลนั้นมิได้มีไว้เพื่อ

ประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ ทั้งนี้การกระทำผิดดังกล่าวจะต้องประกอบด้วยเจตนา ตามประมวลกฎหมายอาญา มาตรา 59

การทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลงข้อมูลคอมพิวเตอร์โดยมิชอบ

มาตรา 9 “ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วนซึ่ง ข้อมูลคอมพิวเตอร์ของผู้อื่น โดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาทหรือทั้งจำทั้งปรับ”

ความผิดตามมาตรา 9 นี้หมายถึงการกระทำอันเป็นการรบกวนข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ตัวอย่างของการกระทำที่ผิดตามมาตรา 9 นี้ ได้แก่ การป้อนโปรแกรมที่มีไวรัสทำลายข้อมูลหรือโปรแกรมคอมพิวเตอร์ หรือการป้อน Trojan Horse เข้าไปในระบบ เพื่อขโมยรหัสผ่านของผู้ใช้คอมพิวเตอร์หรือเพื่อเข้าไป ลบ เปลี่ยนแปลงแก้ไขข้อมูล หรือกระทำการใดๆ อันเป็นการรบกวนข้อมูล เป็นต้น อย่างไรก็ตามการกระทำ ความผิดตามมาตรา 9 นี้มีองค์ประกอบความผิดที่สำคัญคือ “โดยมิชอบ” ดังนั้นหากเป็นการกระทำของบุคคลผู้มีสิทธิ โดยชอบ ก็จะไม่เป็นความผิด เช่น การเปลี่ยนแปลงข้อมูลจราจรทางคอมพิวเตอร์ (traffic data) เพื่อประโยชน์ในการสื่อสารแบบไม่ระบุชื่อ ตัวอย่างเช่น การสื่อสารผ่านระบบ anonymous remailer system หรือการ เปลี่ยนแปลงข้อมูลเพื่อการรักษาความลับและความปลอดภัยของการสื่อสาร อาทิการเข้ารหัสข้อมูล (encryption) เป็นต้น

การรบกวน ขัดขวางการทำงานของระบบคอมพิวเตอร์

มาตรา 10 “ผู้ใดกระทำด้วยประการใดโดยมิชอบเพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกรับ ชะลอ ขัดขวาง หรือรบกวน จนไม่สามารถทำงานตามปกติได้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ”

ความผิดตามมาตรา 10 นี้มีวัตถุประสงค์และองค์ประกอบความผิดคล้ายคลึง กับมาตรา 9 เพียงแต่เปลี่ยนวัตถุประสงค์แห่งการถูกกระทำจาก “ข้อมูลคอมพิวเตอร์” เป็น “ระบบคอมพิวเตอร์” โดยมีเจตนาพิเศษคือ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกรับ ชะลอ ขัดขวาง หรือรบกวน จนไม่สามารถทำงานตามปกติได้ “จนไม่สามารถทำงานตามปกติได้” ย่อมหมายความว่า ระบบ คอมพิวเตอร์นั้นไม่สามารถทำงานได้โดยสมบูรณ์ดังนั้น ถึงแม้ว่าระบบคอมพิวเตอร์จะทำงานได้แต่เป็นการทำงานที่ไม่สมบูรณ์หรือผิดปกติไป (malfunctioning) ก็ย่อมอยู่ใน ความหมายของถ้อยคำอันเป็นองค์ประกอบความผิดนี้แล้ว

การสแปมเมล (Spam mail)

มาตรา 11 “ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมาย อิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูล ดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษไม่เกินหนึ่งแสนบาท”

ความผิดตามมาตรา 11 เป็นการเอาผิดแก่การกระทำที่ไม่ถึงกับทำให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามปกติได้ แต่เป็นการทำให้เกิดการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่น เช่น ส่ง e-mail มากจนล้นระบบคอมพิวเตอร์จนทำให้เกิดความยุ่งยากในการใช้ระบบคอมพิวเตอร์ องค์ประกอบความผิดตามมาตรา 11 สำคัญมากเพราะไม่ใช่เรื่อง “โดยมิชอบ” เหมือนกับ ความผิดตามมาตราอื่นๆในพระราชบัญญัตินี้ แต่เป็นเรื่องปกปิดหรือปลอมแปลง แหล่งที่มาของการส่งข้อมูล ได้แก่ การปกปิดหรือปลอมแปลง IP address และหมายถึงการกระทำที่ทำให้ไม่สามารถตรวจสอบถึงแหล่งที่มาของการส่งข้อมูล และส่งผลให้ไม่อาจตรวจสอบได้ทางระบบข้อมูลจราจรทางคอมพิวเตอร์ เป็นต้น

การกระทำความผิดต่อ ประชาชนโดยทั่วไป / ความมั่นคง

มาตรา 12 “ถ้าการกระทำ ความผิดตามมาตรา 9 หรือ มาตรา 10

(1) ก่อให้เกิดความเสียหายแก่ประชาชนไม่ว่าความเสียหายนั้นจะเกิดขึ้นในทันที หรือในภายหลังและไม่ว่าจะเกิดขึ้นพร้อมกันหรือไม่ต้องระวางโทษจำคุกไม่เกิน สิบปี และปรับไม่เกินสองแสนบาท

(2) เป็นการกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบ คอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศความปลอดภัย สาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ที่มีไว้เพื่อประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

ถ้าการกระทำความผิดตาม (2) เป็นเหตุให้ผู้อื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่สิบปีถึงยี่สิบปี”

เป็นบทลงโทษที่ หนักขึ้นสำหรับการกระทำความผิดตามมาตรา 9 หรือมาตรา 10 (ไม่รวมความผิดฐาน spamming ตามมาตรา 11) ซึ่งเป็นการกระทำ โดยมิชอบกับข้อมูลคอมพิวเตอร์ของผู้อื่น ดังนั้นจะเป็นความผิดตามมาตรา 11 ได้จะต้อง เป็นความผิดใน 2 มาตราดังกล่าวก่อน

การจำหน่าย / เผยแพร่ชุดคำสั่งเพื่อใช้กระทำความผิด

มาตรา 13 “ผู้ใดจำหน่ายหรือ เผยแพร่ชุดคำสั่ง ที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิด ตามมาตรา 5 มาตรา 6 มาตรา 7 มาตรา 8 มาตรา 9 มาตรา 10 หรือมาตรา 11 ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ”

ชุดคำสั่งตามมาตรานี้อาจเป็นแบบวัตถุ เช่น แผ่นซีดีก็ได้หรืออาจเป็นไฟล์ดิจิทัลก็ได้ ส่วนการใช้เป็นเครื่องมือในการกระทำความผิดนั้นเป็นความผิดตามมาตราหนึ่งมาตราใดก็ได้

นำเข้า / ปลอม / เท็จ / ภัยมั่นคง / ลามก / ส่งต่อข้อมูลคอมพิวเตอร์

มาตรา 14 “ผู้ใด กระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำ ทั้งปรับ

(1) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

(2) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความ ตื่นตระหนกแก่ประชาชน

(3) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(4) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามก และข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(5) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (1) (2) (3) หรือ (4)”

ข้อมูลคอมพิวเตอร์ปลอมตาม (1) หมายถึงข้อมูลคอมพิวเตอร์ที่มีการเปลี่ยนแปลง แก้ไขไม่ว่าการเปลี่ยนแปลงแก้ไขนั้นจะทั้งหมดหรือแต่เพียงบางส่วน

ส่วนข้อมูลคอมพิวเตอร์เป็นเท็จตาม (2) นั้น น่าจะหมายถึงข้อมูลคอมพิวเตอร์ที่ไม่ใช่ของจริง เช่น ข้อมูลคอมพิวเตอร์ที่ระบุว่าเป็นเครื่องมือป้องกันไวรัสของบริษัทหนึ่ง แต่แท้จริงแล้วไม่ใช่ เป็นต้น

การจะเป็นความผิดตาม (4) นอกจากข้อมูลคอมพิวเตอร์นั้นมีลักษณะอันลามกแล้ว ยังต้องเป็นข้อมูลคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้อีกด้วย ดังนั้นหากเป็นการนำข้อมูลคอมพิวเตอร์ของตนโดยเฉพาะที่ไม่ได้ประสงค์จะให้ผู้ใดเข้าถึง แต่บังเอิญนำเครื่องคอมพิวเตอร์ไปซ่อมแล้วช่างซ่อมตรวจพบเข้า จึงนำไปเข้าสู่ระบบคอมพิวเตอร์และเผยแพร่ดังที่เป็นข่าวคราว เช่นนี้เฉพาะช่างซ่อมเท่านั้นที่มีความผิดตามมาตรา 14 (4)

ความรับผิดชอบของผู้ให้บริการ

มาตรา 15 “ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือ ยินยอมให้มีการกระทำความผิดตามมาตรา 14 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา 14”

มาตรานี้ใช้ถ้อยคำว่า “จงใจ” ซึ่งเป็นคำที่เพิ่มขึ้นมาจาก “เจตนา” โดยมี เจตนารมณ์ที่จะเน้นให้เห็นว่า “จงใจ” นั้นหมายถึงต้องรู้ว่ามีมีการกระทำความผิดตาม มาตรา 14 เช่นมีการเตือนหรือแจ้งให้ทราบแล้วว่า ข้อมูลคอมพิวเตอร์นั้นเป็นความผิดต่อกฎหมายตามบทบัญญัติมาตรา 14 เมื่อผู้ให้บริการยังปล่อยให้มีการเผยแพร่ ข้อมูลคอมพิวเตอร์อันเป็นความผิดในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ก็จะได้ถือว่าเป็นการจงใจ สนับสนุนหรือยินยอมให้มีการกระทำความผิด

การเผยแพร่ภาพ ตัดต่อ / ตัดแปลง

มาตรา 16 “ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏ เป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทาง อิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือ ได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ”

ความผิดตามมาตรา 16 นี้เป็นลักษณะของการดูหมิ่นหรือหมิ่นประมาทด้วย การตกแต่งภาพของบุคคล ด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ความผิดตามมาตรา 16 นี้ต้องเป็นข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพ ของผู้อื่น หมายถึงการแสดงข้อมูลคอมพิวเตอร์นั้นออกเป็นภาพของบุคคล และภาพนั้น อาจเกิดจากการสร้างขึ้น ใหม่ หรือเป็นภาพที่มีอยู่แต่ได้มีการตัดต่อ เติมหรือดัดแปลง ซึ่งเป็นการทำด้วยวิธีการทางอิเล็กทรอนิกส์หรือ วิธีการอื่นใด ทั้งนี้การกระทำความผิดดังกล่าวจะต้องมีเจตนาตามมาตรา 59 แห่งประมวลกฎหมายอาญาด้วย

กรณีความผิดเกิดขึ้นนอกราชอาณาจักร

มาตรา 17 “ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักรและ

(1) ผู้กระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้นหรือผู้เสียหายได้ร้อง ขอให้ลงโทษ หรือ

(2) ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็นผู้เสียหายและผู้เสียหายได้ร้อง ขอให้ลงโทษ จะต้องรับโทษภายในราชอาณาจักร”

ตัวอย่างลักษณะความผิดที่พบได้บ่อยในปัจจุบันสำหรับการใช้งานอินเทอร์เน็ต

1. การส่งเมลล์ก่อนทวงหรือโฆษณาขายสินค้าหรือขายบริการ ประเภทป้อปอัพ หรือพวกส่งอีเมลล์ขยะที่เขาไม่ต้องการมีโทษปรับอย่างเดียวไม่เกิน 100,000 บาท โทษฐานก่อความรำคาญ
2. การส่งเมลล์ ใส่ร้ายป้ายสีคนอื่น ข่าวลือที่ก่อให้เกิดความวุ่นวาย การส่งภาพลามกอนาจารทั้งหลาย รวมถึงการได้รับแล้วส่งต่อด้วย มีโทษเสมอกันคือ จำคุกไม่เกิน 5 ปี ปรับไม่เกิน 100,000 บาท ดังนั้นจึงไม่ควรส่งต่อเมลล์ที่ไม่เหมาะสม
3. การตัดต่อภาพของคนอื่น แล้วนำเข้าเผยแพร่ทางอินเทอร์เน็ต ทำให้เจ้าของภาพเสียหาย อับอาย ต้องโทษจำคุกไม่เกิน 3 ปี ปรับไม่เกิน 600,000 บาท แต่กฎหมายยกเว้นสำหรับผู้ที่ทำด้วยความสุจริต จะไม่เป็นความผิด
4. การ ใช้ user name/password ของผู้อื่น Log in เข้าสู่ระบบ มีความผิดตามมาตรา 5 ปรับไม่เกิน 10,000 บาท จำคุกไม่เกิน 6 เดือน ดังนั้น ไม่ควรใช้ user/password ของผู้อื่นและไม่ควรให้ผู้อื่นล่วงรู้ password ของตนเอง
5. การโพสต์ข้อความตามกระทู้ต่างๆที่มีเนื้อหาไม่เหมาะสม เป็นเท็จ กระทบความมั่นคง หรือลามกอนาจาร มีความผิดตามมาตรา 14 ปรับไม่เกิน 100,000 บาท จำคุกไม่เกิน 5 ปี ดังนั้นจึงควรใช้วิจารณญาณในการแสดงความคิดเห็น และคำนึงถึงผลที่จะตามมา

สรุปบทลงโทษสำหรับผู้กระทำความผิดกฎหมายภายใต้ พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ตารางที่ 11-1 ความผิดเกี่ยวกับคอมพิวเตอร์

ฐานความผิด	โทษจำคุก	โทษปรับ
การเข้าถึงระบบคอมพิวเตอร์โดยไม่ชอบ	ไม่เกิน 6 เดือน	ไม่เกิน 10,000 บาท
การเปิดเผยมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะโดยไม่ชอบ	ไม่เกิน 1 ปี	ไม่เกิน 20,000 บาท
การเข้าถึงข้อมูลคอมพิวเตอร์โดยไม่ชอบ	ไม่เกิน 2 ปี	ไม่เกิน 40,000 บาท
การดักจับข้อมูลคอมพิวเตอร์ของผู้อื่นโดยไม่ชอบ	ไม่เกิน 3 ปี	ไม่เกิน 60,000 บาท
การทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติม ข้อมูลคอมพิวเตอร์โดยไม่ชอบ	ไม่เกิน 5 ปี	ไม่เกิน 100,000 บาท
การกระทำเพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นไม่สามารถทำงานได้ตามปกติ	ไม่เกิน 5 ปี	ไม่เกิน 100,000 บาท
การส่งข้อมูลคอมพิวเตอร์รบกวนการใช้ระบบคอมพิวเตอร์ของคนอื่นโดยปกติสุข (Spam Mail)	ไม่มี	ไม่เกิน 100,000 บาท
การจำหน่ายชุดคำสั่งที่จัดทำขึ้นเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิด	ไม่เกิน 1 ปี	ไม่เกิน 20,000 บาท
การกระทำต่อความมั่นคง - ก่อความเสียหายแก่ข้อมูลคอมพิวเตอร์ - กระทบต่อความมั่นคงปลอดภัยของประเทศ/เศรษฐกิจ - เป็นเหตุให้ผู้อื่นถึงแก่ชีวิต	ไม่เกิน 10 ปี 3 ปีถึง 15 ปี 10 ปีถึง 20 ปี	และไม่เกิน 200,000 บาท และ 60,000-300,000 บาท ไม่มี
การใช้ระบบคอมพิวเตอร์ทำความผิดอื่น (การเผยแพร่เนื้อหาอันไม่เหมาะสม)	ไม่เกิน 5 ปี	ไม่เกิน 100,000 บาท
ผู้ให้บริการจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิด	ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิด	ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิด
การตกแต่งข้อมูลคอมพิวเตอร์ที่เป็นภาพของบุคคล	ไม่เกิน 3 ปี	ไม่เกิน 60,000 บาท

กระทรวงเทคโนโลยีและการสื่อสารได้จัดทำ พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 (ฉบับการ์ตูน)¹ เพื่อให้เข้าใจในเรื่องของฐานความผิดและบทลงโทษได้ง่ายขึ้น

¹ http://www.mict.go.th/download/law/law_com_cartoon_p1-10.pdf

อาชญากรรมคอมพิวเตอร์

ความหมายของอาชญากรรมทางคอมพิวเตอร์

1. การกระทำใด ๆ ก็ตาม ที่เกี่ยวกับการใช้คอมพิวเตอร์ อันทำให้เหยื่อได้รับความเสียหาย และทำให้ผู้กระทำได้รับผลตอบแทน

2. การกระทำผิดกฎหมายใด ๆ ซึ่งจะต้องใช้ความรู้เกี่ยวข้องกับคอมพิวเตอร์ มาประกอบการกระทำความผิด และต้องใช้ผู้มีความรู้ทางคอมพิวเตอร์ ในการสืบสวน ติดตาม รวบรวมหลักฐาน เพื่อการดำเนินคดี จับกุม

อาชญากรรมคอมพิวเตอร์จะก่ออาชญากรรมหลายรูปแบบ ซึ่งปัจจุบันทั่วโลกจัดออกเป็น 9 ประเภท (ตามข้อมูลคณะกรรมการเฉพาะกิจร่างกฎหมายอาชญากรรมคอมพิวเตอร์)

- 1) การขโมยข้อมูลทางอินเทอร์เน็ต ซึ่งรวมถึงการขโมยประโยชน์ในการลักลอบใช้บริการ
- 2) อาชญากรรมนำเอาระบบการสื่อสารมาปิดกั้นความผิดของตนเอง
- 3) การละเมิดสิทธิปลอมแปลงรูปแบบ เลียนแบบระบบซอฟต์แวร์โดยมิชอบ
- 4) ใช้คอมพิวเตอร์แพร่ภาพ เสียง ลามก อนาจาร และข้อมูลที่ไม่เหมาะสม
- 5) ใช้คอมพิวเตอร์ฟอกเงิน
- 6) อันธพาลทางคอมพิวเตอร์ที่เข้าไปก่อความ ทำลายระบบสาธารณสุขบุคคล เช่น ระบบจ่ายน้ำ จ่ายไป ระบบการจราจร
- 7) หลอกลวงให้ร่วมค้าขายหรือลงทุนปลอม
- 8) แทรกแซงข้อมูลแล้วนำข้อมูลนั้นมาเป็น)ประโยชน์ต่อตนโดยมิชอบ เช่น ลักลอบคั้นหารหัสบัตรเครดิตของผู้อื่นมาใช้ ดักข้อมูลทางการค้าเพื่อเอาผลประโยชน์นั้นเป็นของตน
- 9) ใช้คอมพิวเตอร์แอบโอนเงินบัญชีผู้อื่นเข้าบัญชีตัวเอง

นอกจากนั้นในส่วนของอินเทอร์เน็ต ยังมีรูปแบบการกระทำผิดอีกมาก เช่นการแอบขโมยโดเมนเนม , แอบใช้ รับ-ส่ง อีเมล, แอบใช้บัญชีอินเทอร์เน็ต (เวลาการใช้งาน), การส่ง อีเมลจำนวนมากศาล ฯลฯ รวมทั้งการกระทำผิดแบบดั้งเดิมที่ใช้เทคโนโลยีอินเทอร์เน็ต เป็นเครื่องมือ เช่น ภาพลามกอนาจาร การค้าประเวณี การพนัน ใสร้ายป้ายสี หมิ่นประมาท ฯลฯ

กรณีศึกษาอาชญากรรมและกฎหมายเทคโนโลยีสารสนเทศ²

กรณีที่ 1: นายจ้างหรือผู้บังคับบัญชา เปิด e-mail ลูกจ้างหรือผู้ใต้บังคับบัญชาอ่านได้หรือไม่?

ในการใช้งาน e-mail ภายในองค์กรนั้น จะมีคำถามว่า ถ้าองค์กรนั้น ๆ มีการกำหนด User name และ Password ให้กับคนในองค์กร แล้วถ้านายจ้างหรือผู้บังคับบัญชารู้ User name และ Password ของคนในองค์กร

²

<http://www.lawyerthai.com/articles/it/006.php>

แล้ว นายจ้างหรือผู้บังคับบัญชามีสามารถเปิดอ่าน e-mail ของลูกจ้างได้หรือไม่ ถ้าในประเทศสหรัฐอเมริกา มีกฎหมายกำหนดไว้อย่างชัดเจนว่า นายจ้างหรือผู้บังคับบัญชาขององค์กรนั้น ๆ สามารถเปิดดูและตรวจสอบ e-mail ของลูกจ้างได้รวมทั้งสามารถดูแฟ้มข้อมูลต่าง ๆ ในฮาร์ดดิสก์คอมพิวเตอร์ของบริษัทได้ หากเป็น e-mail ที่เป็นขององค์กร เพราะเป็น e-mail สำหรับการปฏิบัติงาน แต่หากเป็น e-mail อื่นที่ไม่ใช่ขององค์กร นายจ้างหรือผู้บังคับบัญชาไม่ได้รับอนุญาตให้เปิดอ่าน หากนายจ้างหรือผู้บังคับบัญชาละเมิดสิทธิ์ ลูกจ้างสามารถฟ้องร้อง นายจ้างหรือผู้บังคับบัญชาให้ชดใช้ค่าเสียหายทางแพ่งได้

กรณีที่ 2: การ Copy รูปภาพ/ข้อความบนเว็บไซต์ของผู้อื่นมาใช้ เป็นการละเมิดลิขสิทธิ์ทุกกรณีหรือเปล่า?

หากต้องทำการ copy รูปภาพหรือข้อความบนเว็บไซต์ของผู้อื่นมาใช้งาน จำเป็นต้องขออนุญาตเจ้าของเสียก่อน เพราะหากนำมาใช้โดยไม่ได้รับอนุญาตจะถือว่าละเมิดลิขสิทธิ์ผิดกฎหมาย หากนำไปใช้เพื่อการค้าอาจถูกฟ้องเป็นคดีแพ่งหรือคดีอาญาได้ อย่างไรก็ตามก็มีข้อยกเว้นสำหรับกรณีเพื่อการศึกษา โดยต้องมีการอ้างอิงและขออนุญาตเจ้าของลิขสิทธิ์

กรณีที่ 3: การหมิ่นประมาททางอินเทอร์เน็ต สามารถฟ้องร้องเอาผิดได้หรือไม่?

หากมีการหมิ่นประมาทบุคคลผ่านทางอินเทอร์เน็ต สามารถฟ้องร้องได้ทั้งคดีอาญา และคดีแพ่ง ซึ่งตามกฎหมาย การหมิ่นประมาททางแพ่งหมายถึง “ การกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความอันฝ่าฝืนความจริง และการกล่าวหรือไขข่าวนั้นทำให้เกิดความเสียหายแก่ชื่อเสียงเกียรติคุณ ทางทำมาหาได้หรือทางเจริญของบุคคลอื่น ซึ่งแม้ว่าผู้ที่หมิ่นประมาทจะไม่รู้ว่าข้อความที่ตนกล่าวหรือไขข่าวนั้นไม่จริง แต่หากว่าควรจะได้ก็จะต้องรับผิดชอบความเสียหายที่เกิดขึ้น” ส่วนใหญ่คดีหมิ่นประมาทจะฟ้องร้องกันเป็นคดีแพ่งและเรียกค่าเสียหายกันมากๆ เพื่อให้จำเลยเข็ดหลาบ คดีแพ่งเรื่องหมิ่นประมาท ในประเทศไทยยังมีประเด็นที่น่าสนใจคือ เรื่องศาลที่จะฟ้องคดี คือ โจทก์สามารถฟ้องคดีได้ที่ศาลที่จำเลยมีภูมิลำเนาอยู่ในเขต หรือศาลที่เป็นที่เกิดของเหตุในการฟ้องคดี ทางปฏิบัติที่เกิดขึ้นการหมิ่นประมาทโดยการโฆษณาหนังสือพิมพ์นั้นเนื่องจาก หนังสือพิมพ์มีการส่งไปขายทั่วประเทศ ฝ่ายผู้เสียหาย ซึ่งมักเป็นนักการเมือง อาจถือว่าความผิดเกิดขึ้นทั่วประเทศ จึงทำการตระเวนไปฟ้องตามศาลต่าง ๆ ทั่วประเทศ ส่งผลให้จำเลยต้องตามไปแก้คดี

กรณีที่ 4: การทำ Hyperlink อย่างไรไม่ให้ละเมิดลิขสิทธิ์?

การอ้างอิงเว็บไซต์ของผู้อื่น มาใส่ไว้ในเว็บของเรา มีโอกาสละเมิดลิขสิทธิ์ หากมีการมองว่าเป็นการทำซ้ำงานอันมีลิขสิทธิ์ แต่ถ้าการเชื่อมโยงนั้นเป็นการเชื่อมโยงต่อไปยังหน้าแรกของเว็บผู้อื่นก็สามารถได้แต่ควรขออนุญาตเจ้าของลิขสิทธิ์ให้เรียบร้อย หากเป็นการเชื่อมโยงลิงก์ไปถึงเนื้อหาส่วนอื่นของเว็บผู้อื่นจะถือเป็นการละเมิดลิขสิทธิ์ได้ ในกรณีที่ไม่ต้องการให้ใครนำเว็บของเราไปเชื่อมโยงอาจจะระบุไว้ที่เว็บเลยว่า ไม่อนุญาตจะทำให้ผู้ที่เข้ามาเชื่อมโยง หากยังมีการละเมิดสิทธิ์ก็จะมีผลโดยไม่ต้องตีความ

กรณีที่ 5: โหลดโปรแกรมหรือเพลงทางอินเทอร์เน็ตผิดกฎหมายหรือเปล่า?

การ Download โปรแกรมทางอินเทอร์เน็ตมาใช้งานแบบถูกต้องตามกฎหมายโดยไม่ละเมิดลิขสิทธิ์ ก็ต่อเมื่อโปรแกรมที่ผู้ใช้ Download มาใช้นั้น ถูกระบุว่า เป็นประเภท Freeware, Shareware สำหรับการโหลดเพลงทางอินเทอร์เน็ตสามารถทำได้โดยไม่เป็นการละเมิดลิขสิทธิ์หากได้รับอนุญาต แต่โดยทั่วไปแล้วค่ายเพลงมักจะไม่นิยมนุญาต ยกเว้นจะทำการค้า ส่วนการ Upload เพลงขึ้นบนอินเทอร์เน็ตให้คนทั่วไปโหลดได้ฟรี ๆ เป็นการละเมิดลิขสิทธิ์ถือเป็นคดีอาญา

กรณีที่ 6: ซื้อมาโปรแกรมลิขสิทธิ์มา copy แจกเพื่อนได้หรือเปล่า?

การทำสำเนาหรือการ copy โปรแกรมคอมพิวเตอร์นั้น ตามกฎหมายลิขสิทธิ์เขาเรียกว่า "ทำซ้ำ" ซึ่งถือเป็นการละเมิดลิขสิทธิ์ แม้กฎหมายเขาจะมีข้อยกเว้นให้การทำสำเนาโดยเจ้าของโปรแกรมมีลิขสิทธิ์ทำได้โดยไม่ผิดกฎหมาย แต่กฎหมายเขาจำกัดจำนวนสำเนาว่า **ให้มีจำนวนตามสมควรเพื่อวัตถุประสงค์ในการบำรุงรักษาหรือป้องกันการสูญหาย** คือทำสำเนาได้เฉพาะ backup ถ้าจะมา copy แจกเพื่อน ๆ ทั้ง office ก็ถือว่ามีความผิดในเรื่องการละเมิดลิขสิทธิ์

คำแนะนำเพื่อป้องกันการกระทำผิด

- ไฟล์วอลล์ส่วนตัว (Personal Firewall)

ไฟล์วอลล์ส่วนตัวคือซอฟต์แวร์ที่ติดตั้งในเครื่องคอมพิวเตอร์ส่วนตัวซึ่งทำหน้าที่ป้องกันผู้บุกรุกหรือผู้ไม่ประสงค์ดีเข้ามาในเครื่องคอมพิวเตอร์ส่วนตัวของเราหรือช่วยป้องกันโปรแกรมที่ไม่ประสงค์ดี เช่น ไวรัส โทรจัน สปายแวร์ ถูกติดตั้งลงในเครื่องคอมพิวเตอร์ส่วนตัวโดยที่เราไม่ทราบหรือไม่รู้ตัว ดังนั้นเราควรติดตั้งไฟล์วอลล์ส่วนตัวโดยสามารถดาวน์โหลดได้จากเว็บ

- การสวมรอยบุคคล (Identity Theft)

ในปัจจุบัน การขโมยและการฉ้อฉลนั้น สามารถกระทำได้กับเอกสารอิเล็กทรอนิกส์ที่อยู่ในเครื่องคอมพิวเตอร์ ทั้งนี้เนื่องจากปัจจุบันเอกสารสำคัญที่ใช้ระบุตัวตนมากมายได้ถูกจัดเก็บไว้ในเครื่องคอมพิวเตอร์และอาจเข้าถึงได้ โดยผู้บุกรุกโดยผ่านเครือข่ายอินเทอร์เน็ต การขโมยเอกสารสำคัญนั้นอาจนำไปสู่การสวมรอยเป็นตัวบุคคลผู้เป็นเจ้าของเอกสารนั้น และอาจใช้ในการดำเนินเรื่องต่าง ๆ แทนเจ้าของโดยมิได้รับอนุญาตซึ่งเป็นการกระทำที่ผิดกฎหมาย เช่นการขโมยบัญชีผู้ใช้และรหัสผ่านเพื่อทำการล็อกอินเข้าไปซื้อสินค้า ผลที่เกิดขึ้นต่อผู้ที่ถูก

สวมรอย ได้แก่ เสียประวัติทางการเงิน เสียชื่อเสียง และอื่นๆ คำแนะนำก็คือ ให้ระมัดระวังไม่เปิดเผยข้อมูลส่วนตัวเกินความจำเป็น ระมัดระวังให้ข้อมูลเกี่ยวกับบัตรเครดิต เปลี่ยนรหัสผ่านบ่อย ๆ

- **ข้อความฉับพลัน ห้องสนทนา และการแชร์ไฟล์บนอินเทอร์เน็ต (Instant Messaging, Chat Rooms, File Sharing)**

ห้องสนทนาและการใช้ข้อความฉับพลันได้มีการใช้งานกันอย่างแพร่หลาย ถึงแม้ว่าการสนทนาในทั้งสองรูปแบบจะมีประโยชน์อย่างมากในการแลกเปลี่ยนความคิดเห็นหรือข้อมูลต่างๆ แต่ถ้าไม่ได้เตรียมการป้องกันไว้ให้ดีแล้ว ผลลบก็อาจจะเกิดขึ้นได้ เช่น การติดไวรัสหรือโทรจัน การเปิดเผยข้อมูลส่วนตัว

การแชร์ไฟล์เป็นรูปแบบหนึ่งของการแลกเปลี่ยนข้อมูลบนอินเทอร์เน็ต ก็อาจเปิดโอกาสทำให้ผู้บุกรุกเข้ามาเอาไฟล์ในเครื่องของผู้ใช้งานไปได้ คำแนะนำ ให้หลีกเลี่ยงการส่งข้อความฉับพลัน การสนทนาในห้องสนทนา และการแชร์ไฟล์บนอินเทอร์เน็ต เพราะอาจก่อให้เกิดการละเมิดความเป็นส่วนตัวได้

- **อีเมลหลอกลวง (Instant Scams)**

ปัจจุบันได้มีอีเมลหลอกลวงให้ผู้รับอีเมลหลงเชื่อซึ่งหลาย ๆ ครั้งทำให้เกิดความเสียหายต่อผู้รับอีเมล เช่น การเสียเงิน เสียเวลา ปัจจุบันองค์กร Federal Trade Commission (FTC) ของสหรัฐอเมริกาได้ระบุอีเมลไว้ 12 ประเภท ที่ผู้ใช้ต้องให้ความระมัดระวัง

1. การสร้างโอกาสทางธุรกิจ อีเมลนี้จะเสนอรายได้ก้อนใหญ่โดยไม่ต้องทำอะไรมา
2. อีเมลการขายสินค้าที่มีกลุ่มผู้ใช้งานเป็นจำนวนมาก (Bulk E-mail) อีเมลนี้จะเสนอรายชื่อกลุ่มผู้ใช้งานอีเมลซึ่งมีจำนวนมากและชักชวนว่าสามารถโฆษณาหรือขายสินค้าไปยังกลุ่มผู้ใช้งานอีเมลนี้ได้
3. อีเมลลึกลับชักชวนให้ผู้รับส่งเงินจำนวนเล็กน้อยไปยังผู้ส่งและส่งอีเมลนี้ไปยังผู้อื่นต่อไป
4. การทำงานที่บ้านโดยลงแรงเล็กน้อย อีเมลนี้จะเสนอรายได้อย่างสม่าเสมอ แต่ต้องจ่ายค่าธรรมเนียมแรกเข้าและทำตามที่อีเมลขอให้ทำ แต่ผู้รับไม่มีทางได้รับค่าตอบแทนใดๆ ทั้งสิ้นกลับคืน
5. การรักษาสุขภาพและการควบคุมน้ำหนัก อีเมลนี้จะเสนอยาประเภทต่างๆ ถ้าหลงเชื่อคำโฆษณาซื้อผลิตภัณฑ์มาใช้ส่วนใหญ่แล้วจะเป็นการเสียเงินไปโดยเปล่าประโยชน์
6. รายได้ก้อนโตโดยไม่ต้องเสียแรงมากนัก อีเมลนี้จะเสนอวิธีร่ำรวยได้อย่างรวดเร็ว
7. สินค้าฟรี อีเมลนี้จะเสนอให้สินค้าฟรีโดยชำระเงินเพียงเล็กน้อย เช่น เพื่อเข้าเป็นสมาชิก
8. โอกาสการลงทุนที่มีผลตอบแทนสูง อีเมลนี้จะเสนอผลตอบแทนที่สูงกับการลงทุนที่ไม่มีความเสี่ยงเงินที่ลงทุนไปก็จะสูญไปโดยเปล่าประโยชน์
9. ชุดอุปกรณ์เชื่อมต่อเคเบิลทีวี อีเมลนี้จะขายชุดอุปกรณ์สำหรับเชื่อมต่อเข้ากับเคเบิลได้โดยไม่ต้องเสียค่าสมาชิก ถึงแม้ว่าจะทำได้จริงแต่เป็นสิ่งที่ผิดกฎหมาย

10. การให้เงินกู้หรือสินเชื่อโดยมีเงื่อนไขง่าย ๆ ซึ่งสถาบันการเงินที่ถูกต้องตามกฎหมายจะไม่ใช้วิธีการส่งอีเมลแบบนี้
11. การเคลียร์สินเชื่อ อีเมลนี้จะเสนอช่วยเคลียร์ข้อมูลสินเชื่อที่ติดลบในบัญชีธนาคาร การทำตามข้อเสนอถือเป็นการกระทำที่ผิดกฎหมาย
12. การเสนอให้รางวัลไปเที่ยวฟรี อีเมลจะเสนอว่าท่านเป็นผู้ที่ได้รับรางวัลไปเที่ยวฟรี ภายหลังจากจะพบว่าข้อเสนออื่นไม่เป็นอย่างที่คิด หรือไม่ก็ต้องชำระเงินเพิ่มเติม

คำแนะนำ คือ ให้ระมัดระวังโฆษณาชวนเชื่อในลักษณะดังกล่าว และ หมั่นติดตามประเภทของอีเมลหลอกลวงในแหล่งข้อมูลเพิ่มเติม³

- **สแปม (Spam)**

สแปม คืออีเมลที่เป็นขยะ ผู้รับสแปมอาจจะต้องใช้เวลาในการจัดการกับสแปมจำนวนมากในแต่ละวัน และ สแปมยังกีดขวางการทำงานของเมลเซิร์ฟเวอร์ทั่วโลก ซึ่งทำให้ทุกคนประสบกับปัญหาการเชื่อมต่อที่ช้าลงและเสียค่าใช้จ่ายในการเชื่อมต่อที่สูงขึ้น ถึงแม้ว่าจะไม่สามารถจัดการกับสแปมได้อย่างเด็ดขาด แต่ก็สามารถลดระดับความรุนแรงลงได้ ดังนี้

- ไม่ส่งอีเมลเพื่อตอบกลับสแปมที่ส่งมา การตอบกลับสแปมนั้นเท่ากับเป็นการยืนยันอีเมลแอดเดรสของผู้รับว่ามีอยู่จริงและจะทำให้ผู้รับตกเป็นเป้าหมายที่ชัดเจนยิ่งขึ้น
- ใช้อีเมลแอดเดรสประจำเพื่อติดต่อกับผู้ที่ติดต่ออยู่ด้วยเป็นประจำ เช่น ผู้ร่วมงาน ครอบครัว สำหรับการส่งอีเมลเพื่อจุดประสงค์อื่น ๆ ให้ใช้อีเมลแอดเดรสต่างหาก
- ใช้ตัวกรองสแปม ให้เลือกชนิดที่เหมาะสมกับโปรแกรมอีเมลที่ใช้งานอยู่ให้มากที่สุด

- **สปายแวร์ (Spyware)**

สปายแวร์คือซอฟต์แวร์ใดๆ ที่ใช้ช่องทางการเชื่อมต่อกับอินเทอร์เน็ตในเครื่องคอมพิวเตอร์ของผู้อื่นใช้เพื่อแอบส่งข้อมูลส่วนตัวของผู้ใช้นั้นไปให้กับบุคคลหรือองค์กรหนึ่งโดยที่ผู้ใช้เองก็ไม่ทราบ โดยสปายแวร์ สามารถเข้าสู่เครื่องคอมพิวเตอร์ที่ใช้งานได้โดยผ่านทางไวรัสคอมพิวเตอร์ เว็บที่เข้าไปดู หรือ อีเมลที่เปิดอ่าน คำแนะนำ คือ สามารถดาวน์โหลดโปรแกรมตรวจสอบสปายแวร์มาใช้งานเช่นโปรแกรม “Ad-aware” (www.lavasoft.de)

³ <http://www.ftc.gov> และ <http://www.crimes-of-persuasion.com>

- **การหมิ่นประมาทหรือการทำให้ผู้อื่นเสียชื่อเสียง (Online Defamation)**

ข้อความทุกรูปแบบที่ใช้งานบนอินเทอร์เน็ต ต้องระวังไม่ให้เป็นข้อความอันเป็นเท็จหรือก่อให้เกิดความเสียหายต่อบุคคลหรือองค์กรที่ถูกพาดพิงกล่าวถึง หรือ อ้างอิง

- **ประเด็นทางกฎหมาย (Legal Issues)**

กิจกรรมบนอินเทอร์เน็ตทั่วไปที่ถือว่าการกระทำที่ผิดกฎหมาย ได้แก่

- การเล่นเกมพนัน
- การซื้ออาวุธปืน
- การซื้อขายยาเสพติด
- การนำเสนอสื่อลามกทุกประเภท
- การบุกรุกคอมพิวเตอร์หรือเครือข่าย
- การพัฒนาและการแพร่ไวรัสคอมพิวเตอร์
- การทำให้เครือข่ายหรือเครื่องคอมพิวเตอร์ของผู้อื่นไม่สามารถใช้งานหรือให้บริการได้
- การสวมรอยบุคคลเพื่อทำการฉ้อฉล

คำแนะนำ คือ ไม่ควรเข้าไปยุ่งเกี่ยวกับกิจกรรมที่ผิดกฎหมาย และ ปฏิบัติตามกฎหมายของประเทศในเรื่องต่างๆ ไปและที่เกี่ยวข้องกับการใช้งานอินเทอร์เน็ต รวมทั้งกฎหมายในระดับนานาชาติด้วย

ปฏิบัติตัวอย่างไรให้ปลอดภัยจากการกระทำคามผิด

1. ไม่ติดต่อและเผยแพร่ภาพติดต่อของผู้อื่น ที่ทำให้เขาเสียหายหรือเสียชื่อเสียง
2. ก่อนดาวน์โหลดโปรแกรมหรือข้อมูลจากเว็บไซต์ ควรอ่านเงื่อนไขให้ละเอียดเสียก่อน
3. ไม่ส่งต่อ (forward) อีเมล หรือคลิปวิดีโอภาพลามกอนาจารหรือข้อความที่ไม่เหมาะสม
4. ไม่เผยแพร่ spam mail หรือไวรัส
5. ไม่เปิดเผยมาตรการระบบคอมพิวเตอร์ให้ผู้อื่นล่วงรู้
6. ไม่ขโมยข้อมูลระบบคอมพิวเตอร์ของผู้อื่น
7. ระวังการ chat กับคนแปลกหน้า อย่าหลงเชื่อเขาง่าย ๆ
8. อย่าลืมลงโปรแกรมป้องกันไวรัสและสปายแวร์
9. ไม่แฮกระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ของผู้อื่น
10. ไม่ควรบันทึกรหัสผ่าน (Password) ไว้ในคอมพิวเตอร์ และควรเปลี่ยนรหัสผ่าน (password) ทุก ๆ 3 เดือน
11. ไม่แอบดักจับข้อมูลคอมพิวเตอร์ของผู้อื่น

12. ไม่นำเข้าข้อมูลหรือภาพลามกอนาจารเข้าไปในระบบคอมพิวเตอร์
13. อย่าแอบเข้าใช้งานระบบคอมพิวเตอร์ของผู้อื่นโดยที่เจ้าของไม่อนุญาต
14. ให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการสืบสวนสอบสวนตัวผู้กระทำความผิด

จริยธรรมกับเทคโนโลยีสารสนเทศ

เทคโนโลยีสารสนเทศมีผลกระทบต่อสังคมเป็นอย่างมาก โดยเฉพาะประเด็นจริยธรรมที่เกี่ยวข้องกับระบบสารสนเทศที่จำเป็นต้องพิจารณารวมทั้งเรื่องความปลอดภัยของระบบสารสนเทศการใช้เทคโนโลยีสารสนเทศหากไม่มีกรอบจริยธรรมกำกับไว้แล้ว สังคมย่อมจะเกิดปัญหาต่าง ๆ ตามมาไม่สิ้นสุด รวมทั้งปัญหาอาชญากรรมคอมพิวเตอร์ด้วย ดังนั้นหน่วยงานที่ใช้ระบบสารสนเทศจึงจำเป็นต้องสร้างระบบความปลอดภัยเพื่อป้องกันปัญหาดังกล่าว

กรอบความคิดเรื่องจริยธรรม

หลักปรัชญาเกี่ยวกับจริยธรรม มีดังนี้ (Laudon & Laudon, 1999) R.O. Mason และคณะ ได้จำแนกประเด็นเกี่ยวกับจริยธรรมที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศเป็น 4 ประเภทคือ ความเป็นส่วนตัว (Privacy) ความถูกต้องแม่นยำ (Accuracy) ความเป็นเจ้าของ (Property) และความสามารถในการเข้าถึงได้ (Accessibility) (O'Brien, 1999: 675; Turban, et al., 2001: 512)

1) ประเด็นความเป็นส่วนตัว (Information Privacy) คือ การเก็บรวบรวม การเก็บรักษา และการเผยแพร่ ข้อมูลสารสนเทศเกี่ยวกับปัจเจกบุคคล หรือองค์กร ซึ่งเจ้าของข้อมูลหรือสารสนเทศนั้นๆ มีสิทธิที่จะไม่เผยแพร่ข้อมูลต่อสาธารณะ

2) ประเด็นความถูกต้อง (Information Accuracy) ข้อมูลหรือสารสนเทศที่ดีต้องสามารถตรวจสอบถึงแหล่งที่มาได้ รวมถึงมีการตรวจสอบความถูกต้องก่อนที่จะทำการเผยแพร่ข้อมูลนั้นๆ

3) ประเด็นของความเป็นเจ้าของ (Intellectual Property) คือ กรรมสิทธิ์และมูลค่าของข้อมูลสารสนเทศ (ทรัพย์สินทางปัญญา)

4) ประเด็นของการเข้าถึงข้อมูล (Data Accessibility) คือ เนื่องจากการเข้าถึงข้อมูลทำได้ง่าย ทำให้เกิดการกำหนดสิทธิในการเข้าถึงข้อมูลสารสนเทศเพื่อความปลอดภัยของข้อมูล และสามารถตรวจสอบได้ว่าใครเป็นผู้บันทึก แก้ไขข้อมูลนั้นๆ

การคุ้มครองความเป็นส่วนตัว (Privacy)

- ความเป็นส่วนตัวของบุคคลต้องได้คู่กับความต้องการของสังคม
- สิทธิของสาธารณชนอยู่เหนือสิทธิความเป็นส่วนตัวของปัจเจกชน

การคุ้มครองทางทรัพย์สินทางปัญญา

ทรัพย์สินทางปัญญาเป็นทรัพย์สินที่จับต้องไม่ได้ที่สร้างสรรค์ขึ้นโดยปัจเจกชน หรือนิติบุคคล ซึ่งอยู่ภายใต้ความคุ้มครองของกฎหมายลิขสิทธิ์ กฎหมายความลับทางการค้า และกฎหมายสิทธิบัตร

ลิขสิทธิ์ (copyright) ตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 หมายถึง สิทธิแต่ผู้เดียวที่จะกระทำการใด ๆ เกี่ยวกับงานที่ผู้สร้างสรรค์ได้ทำขึ้น ซึ่งเป็นสิทธิในการป้องกันการคัดลอกหรือทำซ้ำในงานเขียน งานศิลปะ หรืองานด้านศิลปะอื่น ตามพระราชบัญญัติดังกล่าวลิขสิทธิ์ทั่วไปมีอายุห้าสิบบปีนับแต่งานได้สร้างสรรค์ขึ้น หรือนับแต่ได้มีการโฆษณาเป็นครั้งแรกในขณะที่ประเทศสหรัฐอเมริกาจะมีอายุเพียง 28 ปี

สิทธิบัตร (Patent) ตามพระราชบัญญัติสิทธิบัตร พ.ศ. 2522 หมายถึง หนังสือสำคัญที่ออกให้เพื่อคุ้มครองการประดิษฐ์ หรือการออกแบบผลิตภัณฑ์ ตามที่กฎหมายบัญญัติไว้ โดยสิทธิบัตรการประดิษฐ์มีอายุยี่สิบบปีนับแต่วันขอรับสิทธิบัตร ในขณะที่ประเทศสหรัฐอเมริกาจะคุ้มครองเพียง 17 ปี

ประโยชน์ของการมีจริยธรรม

1. ประโยชน์ต่อตนเอง ภาคภูมิใจ เป็นที่รักใคร่ เป็นคนดี
2. ประโยชน์ต่อสังคม สบสุข ประองตอง สามัคคี
3. ประโยชน์ต่อประเทศชาติ ความเจริญรุ่งเรือง สามัคคี ความพัฒนา
4. ประโยชน์ต่อองค์กรธุรกิจ ยกระดับมาตรฐานขององค์กร
5. ประโยชน์ต่อการดำรงรักษาไว้ซึ่งจริยธรรม เผยแพร่ รักษาจริยธรรมไปสู่รุ่นต่อไป

จริยธรรมของนักคอมพิวเตอร์

1. มีความรับผิดชอบต่อการขายสินค้าและบริการ
2. ทำงานด้วยความศรัทธา และจริงใจ
3. รักษาผลประโยชน์ของผู้บริโภค
4. นำเสนอคุณภาพสินค้าตามความจริง
5. ไม่เผยแพร่สิ่งที่ก่อให้เกิดผลเสียต่อสังคม
6. ทำตามกฎหมาย ข้อบังคับ ระเบียบของสังคม
7. ทำประโยชน์ต่อสังคม

บรรณานุกรม

- <http://www.lawyerthai.com/articles/it/006.php>
- http://www.nectec.or.th/index.php?option=com_content&view=article&id=79:-2550&catid=40:technology-news&Itemid=165
- http://th.wikisource.org/wiki/พระราชบัญญัติ_ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์_พ.ศ._๒๕๕๐
- กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร http://www.mict.go.th/more_news.php?cid=47
คู่มือการปฏิบัติและแนวทางการป้องกันเพื่อหลีกเลี่ยงการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
- กฎหมายเบื้องต้น http://computer.pcru.ac.th/worachai/teach/GESC103/103_ch7.doc
- กฎหมายเทคโนโลยีสารสนเทศ <https://sites.google.com/site/jantiwaporn813/kdhmay-thekhnoloyi-sarsnthes-it-law>
- กฎหมายพาณิชย์อิเล็กทรอนิกส์ <http://phung0895.blogspot.com/2012/01/2544.html>
- คำอธิบายพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์
- คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 โดย นายพรเพชร วิชิตชลชัย ประธานศาลอุธรณ์ภาค4