

กฎหมาย

และจริยธรรมที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ



บทนำ

ด้วยความก้าวหน้าทางเทคโนโลยีสารสนเทศ ทำให้มีการนำระบบ
เครือข่าย อินเทอร์เน็ต และการสื่อสารเข้ามามีบทบาทในชีวิตประจำวัน การ
ประกอบธุรกิจ การทำธุรกรรมทางอิเล็กทรอนิกส์ กันมากขึ้น ขณะเดียวกัน ก็มี
ผู้ใช้เทคโนโลยีสารสนเทศในทางที่ไม่ถูกต้อง ดังนั้น การพัฒนาความรู้ทางด้าน
วิทยาการ ด้านคอมพิวเตอร์ และการสื่อสารอย่างเดียวยังไม่เพียงพอ ผู้ใช้จะต้อง
ศึกษาและให้ความสำคัญต่อกฎหมายและประเด็นจริยธรรมที่เกี่ยวข้องกับ
เทคโนโลยีสารสนเทศด้วย เพื่อให้ปฏิบัติได้ถูกต้องตามกฎหมาย และระมัดระวัง
การละเมิดประเด็นจริยธรรมที่อาจจะเกิดขึ้น ทั้งโดยตั้งใจและไม่ตั้งใจ อันจะ
ก่อให้เกิดความเสียหายแก่ตนเองและหน่วยงาน





กฎหมายและจริยธรรม

ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ



1. การละเมิดลิขสิทธิ์โปรแกรมคอมพิวเตอร์
2. อาชญากรรมคอมพิวเตอร์
3. การใช้คอมพิวเตอร์ในทางที่ผิด
4. ไวรัสคอมพิวเตอร์
5. กฎหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ
6. จริยธรรมในระบบสารสนเทศ



1. การละเมิดลิขสิทธิ์โปรแกรมคอมพิวเตอร์



(Software)

“โปรแกรมคอมพิวเตอร์”

ตามพระราชบัญญัติลิขสิทธิ์

พ.ศ.2537 มาตรา 4 หมายถึง คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่นำไปใช้กับเครื่องคอมพิวเตอร์ เพื่อให้เครื่องคอมพิวเตอร์ทำงานหรือเพื่อให้ได้รับผลอย่างใดอย่างหนึ่ง หากมีบุคคลใดไปทำซ้ำ ดัดแปลง หรือกระทำการอย่างหนึ่งอย่างใดโดยไม่ได้อนุญาตจากเจ้าของ ถือว่าเป็นการละเมิดลิขสิทธิ์ ตามรายละเอียดของกฎหมายที่ให้ความหมายของลิขสิทธิ์ (Copyright)



f1.4 f 2.8 f 3.5 f 4 f 5.6 f 8 f16

1 2 4 8 15 30 60 125 250 500 1000 2000 4000

1. การละเมิดลิขสิทธิ์โปรแกรมคอมพิวเตอร์ (ต่อ)

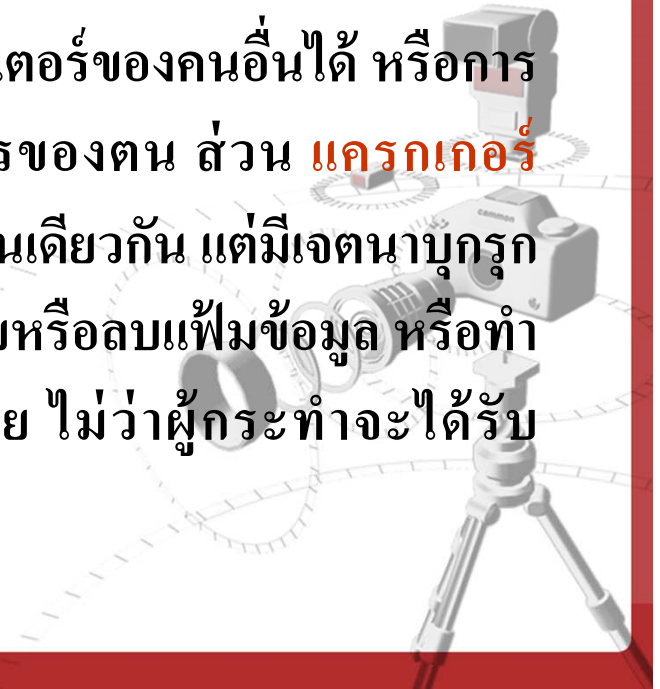
โปรแกรมคอมพิวเตอร์ถือเป็นทรัพย์สินทางปัญญาประเภทหนึ่งที่เกิดจากการใช้สติปัญญาของมนุษย์ในการสร้างสรรค์งานให้เกิดขึ้นมา มีคุณค่าทางเศรษฐกิจและศีลธรรม ได้รับความคุ้มครองทางกฎหมายโดยอัตโนมัตินับแต่สร้างสรรค์ผลงาน ลิขสิทธิ์เป็นสิทธิของเจ้าของแต่เพียงผู้เดียว โปรแกรมคอมพิวเตอร์เป็นงานที่มีลิขสิทธิ์ ประการสำคัญที่ผู้ซื้อโปรแกรมคอมพิวเตอร์ควรทำความเข้าใจแม้จะเป็นการซื้อโปรแกรมคอมพิวเตอร์ด้วยวิธีที่ถูกต้องตามกฎหมาย โปรแกรมคอมพิวเตอร์ก็ยังเป็นงานที่มีลิขสิทธิ์ จึงหมายถึงข้อตกลงการอนุญาตให้ใช้ (User License Agreement) แต่ผู้เดียว หรือให้ใช้ภายในองค์กร หรือเพื่อใช้ในการศึกษาเท่านั้น มิให้ดัดแปลง ทำซ้ำเพื่อประโยชน์ทางการค้า





2. อาชญากรรมคอมพิวเตอร์ (Computer crime)

อาชญากรรมคอมพิวเตอร์ (Computer crime) หมายถึงการกระทำใด ๆ ก็ตามเกี่ยวกับการใช้คอมพิวเตอร์ ที่ทำให้ผู้ใช้ (User) ได้รับความเสียหาย ลักษณะของอาชญากรรมคอมพิวเตอร์ ที่พบบ่อยคือ แฮกเกอร์ (Hacker) หรือผู้บุกรุก ซึ่งหมายถึงบุคคลที่มีความรู้เรื่องระบบคอมพิวเตอร์เป็นอย่างดี สามารถเข้าถึงข้อมูลโดยการเจาะผ่านระบบรักษาความปลอดภัยของคอมพิวเตอร์ได้ เพื่อเข้าไปทดสอบความสามารถของตนเอง ที่สามารถเข้าไปถอดหรือเจาะรหัสระบบรักษาความปลอดภัยเครื่องคอมพิวเตอร์ของคนอื่นได้ หรือการเข้าไปทดสอบระบบรักษาความปลอดภัยในองค์กรของตน ส่วน แครกเกอร์ (Cracker) ก็คือผู้เชี่ยวชาญด้านคอมพิวเตอร์เช่นเดียวกัน แต่มีเจตนาบุกรุกระบบคอมพิวเตอร์ของผู้อื่นโดยผิดกฎหมาย เพื่อทำลายหรือลบแฟ้มข้อมูล หรือทำให้ระบบปฏิบัติการของเครื่องคอมพิวเตอร์เสียหาย ไม่ว่าผู้กระทำจะได้รับผลประโยชน์หรือกลั่นแกล้งเพื่อความสนุกก็ตาม



2. วิชากรรมคอมพิวเตอร์ (ต่อ)

ปัจจุบันทั่วโลกจัดอาชญากรรมคอมพิวเตอร์เป็น 9 ประเภท คือ

1. การขโมยข้อมูลทางอินเทอร์เน็ต ซึ่งรวมถึงการขโมยประโยชน์ในการลักลอบใช้บริการ
2. การนำระบบการสื่อสารมาปิดกั้นความผิดของตนเอง
3. การละเมิดลิขสิทธิ์ เลียนแบบ ปลอมแปลงโปรแกรมคอมพิวเตอร์ (Software)
4. ใช้คอมพิวเตอร์แพร่ภาพ หรือข้อมูลที่ไม่เหมาะสม
5. ใช้คอมพิวเตอร์ฟอกเงิน
6. ใช้คอมพิวเตอร์ก่อวินาศกรรม ทำลายระบบ
7. หลอกลวงให้ทำการค้า หรือลงทุนปลอม
8. ลักลอบเอาเลขบัตรเครดิตของคนอื่นมาใช้ หรือวางกับดักเพื่อให้ผู้อื่นเสียประโยชน์
9. ใช้คอมพิวเตอร์โอนเงินในบัญชีของผู้อื่นมาเป็นของตน



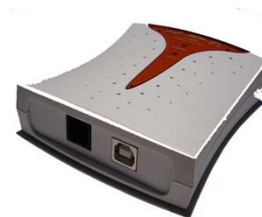
3. **การใช้อินเทอร์เน็ตในทางที่ผิด**



(Computer abuse)

หมายถึงการกระทำโดยการใช้คอมพิวเตอร์ไปในทางที่อาจจะไม่ผิดกฎหมายแต่ผิดจริยธรรม หรืออาจผิดทั้งกฎหมายและจริยธรรม เช่น ลักษณะของจดหมายอิเล็กทรอนิกส์ (E-mail) ที่สร้างความเสียหาย หรือสร้างความเดือดร้อนรำคาญแก่ผู้ใช้อินเทอร์เน็ต แบ่งเป็นประเภทใหญ่ๆ ได้ 2 ประเภทคือ

Chain mail



Spam mail (Send Prodigious Amount of Mail)



4. ไวรัสคอมพิวเตอร์ (Computer virus)

ไวรัสคอมพิวเตอร์ (Computer virus) เป็นโปรแกรมคอมพิวเตอร์ขนาดเล็กชนิดหนึ่ง ส่วนใหญ่ถูกสร้างจากผู้ที่มีความรู้ด้านการเขียนโปรแกรม ไวรัสคอมพิวเตอร์ส่วนใหญ่จะทำงานด้วยตัวเอง โดยไม่ต้องรับคำสั่งหรือคำขออนุญาตจากผู้ใช้แต่อย่างใด โดยไวรัสคอมพิวเตอร์จะทำงานโดยลอบเข้าไปในระบบคอมพิวเตอร์โดยที่ผู้ใช้ไม่รู้ตัว และแพร่กระจายฝังตัวเองติดกับ file ต่าง ๆ ในเครื่องคอมพิวเตอร์และฝังตัวอยู่ในหน่วยความจำ ทำความเสียหายให้กับระบบคอมพิวเตอร์ได้

ในปัจจุบันได้**บัญญัติคำศัพท์ของไวรัสคอมพิวเตอร์**ขึ้นมาใหม่ เรียกว่า **มัลแวร์ (Malicious software: Malware)** ซึ่งหมายถึงชุดคำสั่งทางคอมพิวเตอร์ โปรแกรมหรือ Software ใด ๆ ที่ถูกจัดทำขึ้นมาเพื่อสร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่าย



4. ไวรัสคอมพิวเตอร์ (ต่อ)

หากจะแบ่งไวรัสคอมพิวเตอร์เป็นประเภทต่าง ๆ ตามลักษณะการติดต่อและการทำงานบนคอมพิวเตอร์แล้ว แบ่งเป็น

1. ไวรัสที่ฝังตัวอยู่ที่ **Boot sector**
2. ไวรัสที่ติดไฟล์ข้อมูลหรือโปรแกรม
3. ไวรัสมาโคร (**Macro virus**)
4. หนอนอินเทอร์เน็ต (**Internet worm**)
5. ม้าโทรจัน (**Trojan horse**)
6. ระเบิดเวลา (**Logic bomb**)





5. กฎหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

เทคโนโลยีสารสนเทศเป็นสังคมใหม่ การอยู่ร่วมกันในสังคม ต้องมี กฎเกณฑ์ เพื่อให้อยู่ร่วมกันอย่างสงบสุข หลายประเทศ เช่น สิงคโปร์ อินเดีย เกาหลีใต้ สหรัฐอเมริกา มีการออกกฎหมายเทคโนโลยีสารสนเทศของตนแล้ว สำหรับประเทศไทย ตามมติของคณะรัฐมนตรีเมื่อ **วันที่ 15 ธันวาคม 2541** เห็นชอบให้มีการพัฒนาเกี่ยวกับกฎหมายสารสนเทศใช้ในประเทศ **6 ฉบับ** โดยกระทรวงวิทยาศาสตร์และเทคโนโลยี ร่วมกับศูนย์อิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (**NECTEC**) ดำเนินการ ประกอบด้วย



5. กฎหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ(ต่อ)

1. กฎหมายธุรกรรมอิเล็กทรอนิกส์ (Electronic Transactions Law) เน้นเรื่องการใช้ข้อมูลอิเล็กทรอนิกส์ซึ่งจะไม่ถูกปฏิเสธความรับผิดชอบทางกฎหมาย
2. กฎหมายลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signatures Law) เน้นเรื่องการใช้ลายมือชื่อดิจิตอล
3. กฎหมายอาชญากรรมทางคอมพิวเตอร์ (Computer Crime Law) เป็นกฎหมายที่เข้ามากำกับ ดูแลความสงบสุขของการใช้เทคโนโลยีสารสนเทศ
4. กฎหมายคุ้มครองข้อมูลส่วนบุคคล (Data Protection Law)
5. กฎหมายว่าด้วยการโอนเงินทางอิเล็กทรอนิกส์ (Electronic Fund Transfer Law)
6. กฎหมายการพัฒนาโครงสร้างพื้นฐานสารสนเทศ (National Information Infrastructure Law)
7. กฎหมายลิขสิทธิ์ พระราชบัญญัติลิขสิทธิ์พ.ศ. ๒๕๓๗



ปัจจุบันมีการประกาศเป็นกฎหมายแล้ว 2 ฉบับคือ พระราชบัญญัติว่าด้วยการทำธุรกรรมทางอิเล็กทรอนิกส์ และพระราชบัญญัติลายมือชื่อทางอิเล็กทรอนิกส์

พระราชบัญญัติ ธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

1 2 4 8 15 30 60 125 250 500 1000 2000 4000

f1.4 f 2.8 f 3.5 f 4 f 5.6 f 8 f16

5. กฎหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ(ต่อ)

พระราชบัญญัติ 1 ฉบับได้ประกาศใช้อย่างเป็นทางการไป คือ



พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ประกาศใช้เมื่อวันที่ 18 มิถุนายน 2550

เล่ม ๑๒๔ ตอนที่ ๒๗ ก	หน้า ๔ ราชกิจจานุเบกษา	๑๘ มิถุนายน ๒๕๕๐
		
พระราชบัญญัติ		
ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์		
พ.ศ. ๒๕๕๐		

1 2 4 8 15 30 60 125 250 500 1000 2000 4000

5. กฎหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ(ต่อ)

พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550



หมวดที่ 1 ความผิดเกี่ยวกับคอมพิวเตอร์

มาตราที่ 5 ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษ จำคุกไม่เกิน 6 เดือนหรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตราที่ 9 ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วนซึ่งข้อมูลคอมพิวเตอร์ ของผู้โดยมิชอบ ต้องระวางโทษ จำคุกไม่เกิน 5 ปีหรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

f1.4 f 2.8 f 3.5 f 4 f 5.6 f 8 f16

1 2 4 8 15 30 60 125 250 500 1000 2000 4000

จริยธรรมในระบบสารสนเทศ



จริยธรรม (Ethics) หมายถึง หลักความประพฤติที่ดีงาม เพื่อประโยชน์สุขแก่ตนเองและสังคม โดยการพิจารณาไตร่ตรองว่าอะไรควรทำ อะไรไม่ควรทำ

ความสัมพันธ์ระหว่างเทคโนโลยีสารสนเทศและจริยธรรม ประกอบด้วย

1. ความเป็นส่วนตัว (Privacy)
2. ความถูกต้อง (Accuracy)
3. ความเป็นเจ้าของ (Property)
4. การเข้าถึงข้อมูล (Access)



หลักการปกป้องคุ้มครองข้อมูล

กฎหมายอาญาได้ให้ความสำคัญกับการปกป้องคุ้มครองข้อมูลตามมาตรา 323 เกี่ยวกับการเปิดเผยความลับของผู้รับบริการ มีสาระดังนี้ “ผู้ใดล่วงรู้หรือได้มาซึ่งความลับของผู้อื่น โดยเหตุที่เป็นเจ้าพนักงานผู้มีหน้าที่ โดยเหตุที่ประกอบอาชีพเป็นแพทย์ เภสัชกร นางผดุงครรภ์ ผู้พยาบาล นักบวช หมอความ ทนายความ หรือผู้สอบบัญชี หรือโดยเหตุที่เป็นผู้ช่วยในการประกอบอาชีพนั้น แล้วเปิดเผยความลับนั้น ในประการที่น่าจะเกิดความเสียหายแก่ผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งพันบาท หรือทั้งจำทั้งปรับ”

ดังนั้น สิ่งที่ผู้รับผิดชอบข้อมูลในสถานบริการสุขภาพ ต้องพิจารณา คือ การรักษาความลับการคุ้มครองข้อมูลส่วนบุคคล (Confidentiality) ความเป็นส่วนตัว (Privacy) ของเจ้าของข้อมูล และการรักษาความปลอดภัย (Security) โดยออกแบบระบบเพื่อป้องกันระบบคอมพิวเตอร์ และข้อมูลจากความเสียหายทั้งโดยเจตนาหรือไม่ได้เจตนา



วิธีการปกป้องคุ้มครองข้อมูล

1. **การปกป้องทางกายภาพ (Physical Security)** หมายถึง การจัดเก็บรักษาข้อมูล
ด้านสถานที่ สภาพแวดล้อม
2. **การควบคุมการเข้าถึงข้อมูล (Data Access Security)** หมายถึงการออกแบบ
ระบบที่มีการปกป้องรักษาข้อมูล
3. **การกำหนดมาตรการใช้ข้อมูล (Data Access Measure)** หมายถึง การกำหนด
หรือควบคุมผู้ใช้ข้อมูล (User)
4. **การเปลี่ยนแปลงรหัสข้อมูล (Data Encryption)** หมายถึง การแปลงข้อมูลให้ไม่
สามารถอ่านได้ ถ้าข้อมูลถูกเรียกใช้จากผู้ที่ไม่ได้รับอนุญาต
5. **สำรองข้อมูล (Backup)** เพื่อป้องกันปัญหา ความผิดพลาดต่าง ๆ ควรสำรอง
ข้อมูลอยู่เสมอ โดยคัดลอกแฟ้มข้อมูลต่าง ๆ จากฮาร์ดดิสก์ลงในแผ่นดิสเก็ต





วิธีการปกป้องคุ้มครองข้อมูล (ต่อ)

สมาคมผู้รับทุนใจกล้า ประเทศไทย (2545) เผยแพร่จรรยาบรรณผู้ใช้อินเทอร์เน็ต มี 10 ประการ ดังนี้

- 1) ต้องไม่ใช้คอมพิวเตอร์ทำร้ายหรือละเมิดผู้อื่น
- 2) ต้องไม่รบกวนการทำงานของผู้อื่น
- 3) ต้องไม่สอดแนม แก้ไขหรือเปิดเผยข้อมูลของผู้อื่น
- 4) ต้องไม่ใช้คอมพิวเตอร์เพื่อการโจรกรรมข้อมูล
- 5) ต้องไม่ใช้คอมพิวเตอร์เพื่อสร้างหลักฐานอันเป็นเท็จ

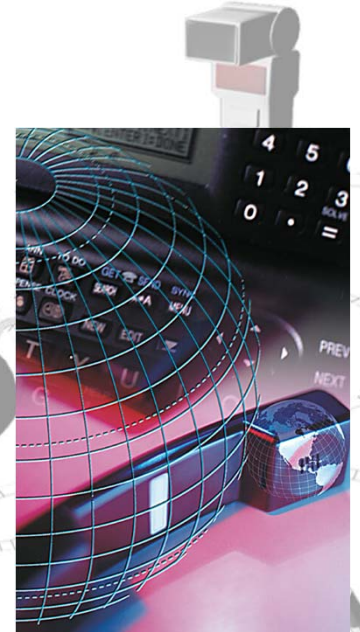




วิธีการปกป้องคุ้มครองข้อมูล (ต่อ)

สมาคมผู้รับทุนใจกล้า ประเทศไทย (2545) เผยแพร่จรรยาบรรณผู้ใช้
อินเทอร์เน็ต มี 10 ประการ ดังนี้

- 6) ต้องไม่คัดลอกโปรแกรมของผู้อื่นที่มีลิขสิทธิ์
- 7) ต้องไม่ละเมิดการใช้ทรัพยากรคอมพิวเตอร์โดยที่ตนเองไม่มีสิทธิ์
- 8) ต้องไม่นำเอาผลงานของคนอื่นมาเป็นของตน
- 9) ต้องคำนึงถึงสิ่งที่จะเกิดขึ้นกับสังคมอันเนื่องมาจากการกระทำของผู้ผิดจรรยาบรรณ
- 10) ต้องใช้คอมพิวเตอร์โดยเคารพกฎ ระเบียบ กติกา มารยาท



ลวสดี