

พิเคราะห์ พ.ร.บ.คอมพิวเตอร์

ควบคุมจริยธรรมได้จริงหรือ?

โดย ผศ.สุพล พรหมมาพันธุ์

คณะวารสารศาสตร์ มหาวิทยาลัยศรีปทุม

ลงตีพิมพ์ในหนังสือพิมพ์ไทยโพสต์ รายวัน ฉบับที่ 4572 วันพฤหัสบดีที่ 7 พฤษภาคม พ.ศ. 2552 หน้า 4

คอมพิวเตอร์ นับเป็นเครื่องมืออิเล็กทรอนิกส์ที่จำเป็นในชีวิตประจำวัน เนื่องจากทุกสำนักงาน ทุกบริษัทองค์กร ล้วนแล้วแต่ต้องใช้คอมพิวเตอร์ด้วยกันทั้งนั้น จากสถิติจำนวนผู้ใช้คอมพิวเตอร์และอินเทอร์เน็ตได้ทวีเพิ่มมากขึ้นทุกขณะทั้งในประเทศและต่างประเทศ สำหรับในประเทศไทยจากการสำรวจปี พ.ศ. 2550 ประมาณ 10 ล้านคน และในปี พ.ศ. 2552 นี้ประมาณ 14 ล้านคน แต่ทั่วโลกจากสถิติปี พ.ศ. 2548 ประมาณ 1,000 ล้านคน และในปี พ.ศ. 2552 นี้ประมาณ 1,007,730,000 ล้านคน เมื่อมีจำนวนผู้ใช้งานมาก สถิติผู้ทำผิดกฎหมายหรือผิดจริยธรรมศีลธรรมย่อมมีมากขึ้นตามลำดับ ไม่นานมานี้ มีประกาศพระราชบัญญัติออกมาใหม่ล่าสุด คือพระราชบัญญัติ ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ประกาศออกมาเมื่อวันที่ 10 มิถุนายน พ.ศ. 2550 พระราชบัญญัตินี้จะมีผลบังคับใช้เมื่อพ้นกำหนดสามสิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป เท่ากับว่า ปัจจุบันมีผลการบังคับใช้อย่างสมบูรณ์ คราวนี้ขอพิเคราะห์ พ.ร.บ.คอมพิวเตอร์เพียงบางมาตราว่า สามารถควบคุมประพฤติและจริยธรรมของคนในสังคมได้จริงหรือ ? :

มาตรา 8 ผู้ใดกระทำความผิดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักจับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ ต้องระวางโทษจำคุกไม่เกินสามปีหรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ.

ในมาตรานี้ เป็นการให้ความคุ้มครองกับสิทธิความเป็นส่วนตัว (Right of Privacy) ซึ่งหมายถึง สิทธิที่จะอยู่ตามลำพัง โดยปลอดจากการแทรกสอดในความเป็นอยู่ส่วนตัว ทำให้ได้รับความเดือดร้อนรำคาญใจหรือการนำภาพ และข้อมูลไปใช้ในการแสวงหาผลประโยชน์ในทางมิชอบ ความเป็นส่วนตัวบนอินเทอร์เน็ต หรือ World Wide Web มีหลายประเภทได้แก่ การส่งจดหมายอิเล็กทรอนิกส์ การสืบค้นข้อมูล การดาวน์โหลด การสนทนา กลุ่มข่าว ที่มีการเปิดอ่านข้อมูล หรือส่งข้อความกันอย่างกว้างขวาง ซึ่งบางอย่างเป็นเรื่องส่วนตัว เช่น เรื่อง ข้อมูลการรักษาโรค ข้อมูลการทำธุรกิจการค้าหรือข้อมูลที่เป็นความลับของบริษัท การดักจับข้อมูลถือว่าเป็นการละเมิดสิทธิของบุคคลอื่นและเป็นอาชญากรรมคอมพิวเตอร์ เช่น จดหมายลับอิเล็กทรอนิกส์ที่ถูกติดตามอ่านโดยบริษัท สารสนเทศส่วนบุคคลที่มีการจัดเก็บโดยอัตโนมัติ เมื่อเราคลิกเข้าไปสู่เว็บไซต์ เราก็ทิ้งร่องรอยไว้ในรูปของไฟล์ Cookie ซึ่งก็อาจเทียบได้กับลายนิ้วมือที่เราทิ้งร่องรอยไว้ตามที่ต่างๆ ความหมายของ Cookie คือไฟล์ที่เก็บข้อมูลการติดต่อระหว่างบราวเซอร์กับเว็บเซิร์ฟเวอร์ ซึ่งจะถูกเก็บเอาไว้บนเครื่องของผู้ใช้ ซึ่งมันจะทำหน้าที่จดจำชื่อผู้ใช้และรหัสผ่านและจะทำการอ่านไฟล์ cookie ทุกครั้งที่ผู้ใช้เข้าไปที่หน้า login ดังนั้นใครก็สามารถเปิดอ่านไฟล์ cookie เหล่านี้ได้ (www.lawyerthai.com) ส่วนแนวทางอื่น ๆ ที่บริษัทจะได้ข้อมูลจากผู้ใช้หรือลูกค้าคือการซื้ออีเมลล์หรือข้อมูล ซึ่งก็จะมีบริษัทจำพวกหนึ่งที่เขาจะขาย list ลูกค้ารวมทั้งข้อมูลต่าง ๆ ของลูกค้าให้กับบริษัทอื่น ๆ โดยลูกค้าไม่รู้เลยว่าเขานำข้อมูลส่วนตัวไปทำอะไรบ้าง กรณีนี้คล้ายคลึงกับการดักฟังทางโทรศัพท์ซึ่งถือว่ามีคามผิดตามกฎหมายด้วยเช่นกัน



มาตรา 9 ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

ในมาตรานี้ ปัญหาส่วนใหญ่ที่เกิดขึ้นเกี่ยวกับด้านการเงิน ลองมาดูข้อมูลจากบริษัท เทอร์นด ไมโคร อิงค์ ซึ่งระบุลักษณะและขอบเขตของภัยคุกคามใหม่ ระบุว่า “เงิน” เงินที่ได้จากการขายข้อมูลลับที่ขโมยมา เป็นสิ่งที่ดึงดูดใจของบรรดาเหล่ามิจฉาชีพ และคนกลุ่มนี้กำลังใช้เว็บไซต์เป็นสื่อในการกระทำที่เลวร้ายผสมกับเทคนิคที่มีอยู่ในปัจจุบัน ไม่ว่าจะเป็นการกระจายไวรัส การโจมตีอย่างมีเป้าหมาย อาทิ การขโมยข้อมูลส่วนตัว การดึงเอาข้อมูลลับในองค์กรไปใช้งาน การทำงานที่เสี่ยงขององค์กรให้ได้รับความเสียหาย และการดึงเอาความลับจากผู้ใช้อินเทอร์เน็ตมาทีละน้อย เรื่องลักษณะนี้กำลังเกิดขึ้นในองค์กรขนาดใหญ่ รวมไปถึงธุรกิจขนาดเล็ก แม้แต่ผู้บริโภคทั่วไปที่ใช้งานอินเทอร์เน็ต ก็มีสิทธิ์โดนขโมยข้อมูลลับด้วยเช่นกัน “ภัยคุกคามบนเว็บ” กำลังมีแนวโน้มเติบโตและเพิ่มจำนวนมากขึ้น โดยเป้าหมายของมิจฉาชีพเหล่านี้มีหลายอย่าง ได้แก่ ในต่างประเทศจะต้องการหมายเลขประกันสังคม หมายเลขบัตรเครดิตจากสถาบันการเงิน และข้อมูลเฉพาะตัวจากบริษัทด้านเทคโนโลยี นอกจากนี้จะขโมยข้อมูลลับกันไปแบบง่าย ๆ แล้ววิธีการดังกล่าวยังเป็นการล่อลวงละเมิดสิทธิส่วนบุคคลของผู้บริโภค ทำลายระบบธนาคารออนไลน์ การทำธุรกรรม และอี-คอมเมิร์ซผ่านทีละเล็กทีละน้อย อีกทั้งดูเหมือนว่าการพึ่งพาระบบป้องกันเดิมๆ ที่มีอยู่ดูเหมือนว่าจะไม่สามารถป้องกันภัยเหล่านี้ได้เพียงพอ เพราะไม่มีเทคโนโลยี หรือวิธีการใดๆ แบบใดที่จะแก้สถานการณ์ให้ดีขึ้นมาได้ จำเป็นต้องใช้เทคนิคขั้นสูง และมีหลายชั้นเข้ามารวมด้วยกันเพื่อให้ระบบเหล่านี้สมบูรณ์จริงๆ (www.adsthailand.com)

มาตรา 10 ผู้ใดกระทำด้วยประการใดมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ชัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ.

ในมาตรานี้ เคยมีปัญหเกิดขึ้นในระบบเครือข่ายคอมพิวเตอร์ทั่วโลก ซึ่งเมื่อไม่นานมานี้ มีแฮกเกอร์ (Hacker) ทำการอัปโหลดข้อมูลจำนวนมหาศาลลงไปในระบบเครือข่ายคอมพิวเตอร์หรืออินเทอร์เน็ต ทำให้หลายคนเปิดเข้าไปใช้งานในเว็บไซตไม่ได้ โดยเฉพาะเว็บไซตอย่าง www.amazon.com ซึ่งทำธุรกิจพาณิชย์อิเล็กทรอนิกส์ (e-Commerce) ทำให้ลูกค้าของ amazon.com ไม่สามารถเปิดเข้าไปในเว็บไซต เพื่อซื้อสินค้าได้ ทำให้ต้องเสียหายได้ต่อวันไปจำนวนมหาศาล

มาตรา 11 ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่น โดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

ในมาตราชั้นนี้ ได้แก่ผู้ไม่ประสงค์ดีส่งข้อความไร้สาระหรือเมลล์ขยะ (Spamming) มาเป็นจำนวนมากศาลแล้ว ยังมีกรณีหนึ่งคือ การหลอกลวงด้วยจดหมายอิเล็กทรอนิกส์ (Phishing Attack) หรือการโจมตีผ่านทางอีเมล โดยจะเน้นการโจมตีไปที่กลุ่มผู้ใช้บริการออนไลน์และผู้ใช้บริการ e-Commerce เช่น eBay, Amazon หรือ PayPal เป็นต้น และ แสกเกอร์ยังนิยมโจมตีกลุ่มผู้ใช้บริการอินเทอร์เน็ตแบบคั้งอีกด้วย วิธีการของเหล่ามิจฉาชีพก็คือ การส่งอิเล็กทรอนิกส์เมลล์หลอกมายังผู้ใช้บริการออนไลน์ต่างๆ เช่น ผู้ใช้บริการอินเทอร์เน็ตแบบคั้งว่าอิเล็กทรอนิกส์เมลล์นั้นถูกส่งมาจากธนาคารที่ผู้ใช้บริการติดต่อใช้บริการอยู่ โดยมีการปลอมแปลงชื่อผู้ส่งและที่อยู่ของผู้ส่งว่ามาจากธนาคารดังกล่าว และมีเนื้อความในอิเล็กทรอนิกส์เมลล์หลอกให้เหยื่อหลงเข้าไป "Log-on" หรือ "Sign-on" เข้าไปในหน้าเว็บหลอกที่มี URL ปากกอยู่ในรูปแบบของ Link ที่อยู่ในเนื้อความของอิเล็กทรอนิกส์เมลล์ ซึ่ง Link ดังกล่าวก็จะเชื่อมโยงไปยังเว็บไซต์หลอกที่แสกเกอร์ได้ทำไว้เพื่อดักชื่อผู้ใช้และรหัสผ่านของเหยื่อ เมื่อเหยื่อหลงเข้าไป "Log-on" ก็เท่ากับว่าไปบอกชื่อผู้ใช้และรหัสผ่านซึ่งเป็นความลับ ให้กับแสกเกอร์โดยรู้เท่าไม่ถึงการณ์ (www.csa44.com) สำหรับทางแก้ไขที่ได้ประสิทธิภาพก็คือการนำระบบ "Two-Factor Authentication" หรือ ระบบการพิสูจน์ตัวตนโดยการใช้อุปกรณ์ Token หรือ Smart Card ร่วมกับรหัสผ่าน หรือ ใช้ระบบรหัสผ่านแบบ "One Time Password" (OTP) ซึ่งจะมีความปลอดภัยมากกว่าระบบที่ใช้อยู่เพียงแค่ "ชื่อผู้ใช้" และ "รหัสผ่าน" แบบเดิมๆ ที่ไม่สามารถป้องกันวิธีการโจมตีแบบ "Phishing" ได้

ลักษณะปัญหาการกระทำความผิดทางคอมพิวเตอร์ต่างๆ ดังกล่าวนี ปัจจุบันได้ทวีเพิ่มจำนวนมากขึ้นตามลำดับ สอดคล้องกับผู้จัดการทั่วไปของบริษัท เอ.อาร์.ไอที คือนายวรเทพ มงคลวาทย์ ที่กล่าวว่า จากการเก็บสถิติการรับแจ้งเหตุละเมิดความปลอดภัยของคอมพิวเตอร์ผ่านศูนย์ประสานงานการรักษาความปลอดภัยทางคอมพิวเตอร์ (Thai CERT) พบว่าในปี 2551 รูปแบบการละเมิดที่ใช้มากที่สุด คือรูปแบบฟิชชิ่ง หรือการหลอกลวงผู้ใช้ให้เปิดเผยข้อมูลส่วนตัวที่สำคัญแก่เว็บไซต์ที่ปลอมแปลง มีจำนวนสูงถึง 68% รองลงมาคือรูปแบบเมลล์แวร์หรือซอฟต์แวร์ที่ออกแบบเพื่อแทรกซึมเข้าไปทำลายระบบคอมพิวเตอร์ มีอยู่ 16% และสแปมเมลล์หรือเมลล์ขยะ มีอยู่ 1% จากข้อมูล IDC ที่คาดการณ์ว่าปี พ.ศ. 2552 ภาพรวมของตลาดไอทีจะเติบโตลดลง โดยมูลค่ารวมตลาดไอทีในประเทศไทยจะอยู่ที่ 6.5 พันล้านเหรียญสหรัฐฯ ปรับตัวลดลงประมาณ 217 ล้านเหรียญสหรัฐฯ และอัตราการเติบโตจะลดลงจาก 12.9% เป็น 6.7% อย่างไรก็ตาม วิฤตเศรษฐกิจขณะนี้ไม่ส่งผลกระทบต่อโอกาสทางธุรกิจด้าน IT Security ที่มีแนวโน้มเติบโตเพิ่มสูงขึ้น เพราะการโจรกรรมข้อมูล และการใช้อินเทอร์เน็ตมีความเสี่ยงเพิ่มขึ้น จากการสำรวจทั่วโลกพบว่าประเทศไทยติดอันดับ 1 ใน 4 ที่ถูกโจรกรรมมากที่สุด โดยสาเหตุที่มีการโจรกรรมมากขึ้น เพราะกฎหมายที่มีอยู่ไม่เข้มงวด และไม่ชัดเจน แม้จะประกาศใช้พระราชบัญญัติความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 หรือ พ.ร.บ.คอมฯ แล้วก็ตาม ดังนั้น จากแนวโน้มความเสี่ยงด้านโจรกรรมที่มากขึ้น ทำให้ความต้องการบุคคลากรที่เกี่ยวข้องทางด้าน IT Security มีมากขึ้นประมาณ 60% จากคนที่มีความรู้ทางไอที 100% เมื่อพิจารณาหัดดูจะพบว่า พ.ร.บ.คอมพิวเตอร์สามารถควบคุมความประพฤติหรือจริยธรรมของคนได้จริงหรือไม่? คงตอบได้ว่าควบคุมได้บ้าง แต่ว่า ยังไม่ได้รับผลอย่างเต็มที่ ในขณะที่เดียวกันภาคเอกชนได้ออกมาติงว่า พ.ร.บ. คอมพิวเตอร์มีโทษรุนแรงเกินไป เป็นอุปสรรคต่อการทำธุรกิจ หลังประกาศใช้มาแล้ว 1 ปี มีคดีทั้งหมดประมาณ 10 คดี อย่างไรก็ตามการประกาศใช้ พ.ร.บ. คอมพิวเตอร์ออกมา สรุปว่า "มี ดีกว่าไม่มี" เพราะอย่างน้อยก็ช่วยปราบคนที่คิดจะกระทำความผิด ให้ยำเกรงต่อกฎหมายบ้านเมือง ดังนั้น จึงควรส่งเสริมประชาชนให้ได้รับทราบข้อมูลอย่างทั่วถึง และมีความเข้มงวดเรื่องการบังคับใช้กฎหมายให้มากขึ้นด้วย.

