พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 : กฎหมายคุ้มครองสิทธิเสรีภาพหรือรัฐประหารแบบเบ็ดเสร็จ ?

ไพบูลย์ อมรภิญโญเกียรติ*

เมื่อวันที่ 18 กรกฎาคม 2550 ภายหลังจากที่ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีผลบังคับใช้นั้น กฎหมายฉบับนี้ได้รับการวิพากษ์วิจารณ์จากสื่อมวลชนอยู่มากมายหลายประเด็น แม้ว่าวัตถุประสงค์ในการออกกฎหมายฉบับนี้ จะมุ่งเน้นการปราบปรามอาชญากรรมที่เกิดจากการใช้เครื่องคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เพิ่มขึ้นอย่างมากมายในปัจจุบันก็ตาม ประเด็นที่ได้รับการวิพากษ์วิจารณ์อย่างหนักได้แก่ กฎหมายฉบับนี้ให้ผู้ให้บริการต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) จากผู้ใช้บริการทั่วไป เป็นการละเมิดสิทธิเสรีภาพหรือสิทธิส่วนบุคคลที่ระบุไว้ตามกฎหมายรัฐธรรมนูญ หรือไม่ เพราะต้องเปิดเผยผู้ใช้บริการว่าเป็นบุคคลใด การห้ามส่งต่อ (forward) ข้อมูลที่ลามกอนาจาร การให้อำนาจแก่รัฐบาลในการปิดหรือบล็อกเว็บไซท์ พูดง่ายๆ ว่า กฎหมายฉบับนี้คือ รัฐประหารแบบเบ็ดเสร็จสำหรับสิทธิเสรีภาพของผู้ใช้บริการในโลกไซเบอร์สเปส หรือในโลกอินเตอร์เน็ตหรือเปล่า ดังนั้น ในบทความนี้ผู้เขียนจะอธิบายถึงที่มาและวัตถุประสงค์ของการร่างกฎหมาย เนื้อหาของกฎหมาย และแนะนำแนวทางในการใช้กฎหมายฉบับนี้อย่างมีประสิทธิภาพครับ

ที่มาและรายละเอียดของกฎหมาย กฎหมายฉบับนี้ มีต้นร่างมาตั้งแต่สมัยรัฐบาลคุณชวน หลีกภัย ในปี พ.ศ. 2540 จนมาถึงรัฐบาลชุดปัจจุบันได้มีการตั้งกรรมาธิการวิสามัญเพื่อพิจารณากฎหมายฉบับดังกล่าวเมื่อวันที่ 15 พฤศจิกายน 2549 และคณะกรรมการวิสามัญได้แก้ไขเพิ่มเติมรายละเอียดของกฎหมายเกือบทั้งหมดก่อนออกมาบังคับใช้ในวันที่ 18 กรกฎาคม 2550 โดยสามารถแบ่งสาระสำคัญของกฎหมายออกเป็น 6 ส่วน ดังนี้

1. ฐานความผิดที่เกี่ยวข้องกับคอมพิวเตอร์ (มาตรา 5-16)
2. การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ (มาตรา 26)
3. อำนาจของพนักงานเจ้าหน้าที่ตามกฎหมายใหม่ (มาตรา 18-21)
4. เขตอำนาจของศาลในการพิจารณาคดี (มาตรา 17)
5. อำนาจของ รมต. ไอซีที (มาตรา 20)
6. บทกำหนดโทษสำหรับพนักงานเจ้าหน้าที่ (มาตรา 22-24)

---

* กรรมการบริษัท ที่ปรึกษากฎหมาย ไพบูลย์ จำกัด, นิติศาสตร์บัณฑิต (เกียรตินิยมอันดับ 2) มหาวิทยาลัยธรรมศาสตร์, นิติศาสตร์มหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์, นิติศาสตร์มหาบัณฑิต มหาวิทยาลัยลอนดอน (เกียรตินิยม)

1. ฐานความผิดที่เกี่ยวข้องกับคอมพิวเตอร์ (มาตรา 5-16)

ใน ส่วนฐานความผิดที่เกี่ยวกับการใช้คอมพิวเตอร์ในกฎหมายฉบับนี้นั้นทุกมาตรา เป็นความผิดอาญาที่ยอมความไม่ได้ ยกเว้นมาตรา 16 (การตัดต่อภาพโดยสื่ออิเล็กทรอนิกส์) โดยแบ่งแยกประเภทของความผิดออกเป็น 8 ประเภทหลักๆ คือ

ก. การเข้าถึงระบบคอมพิวเตอร์[1] และข้อมูลคอมพิวเตอร์[2] โดยมิชอบ (มาตรา 5 และมาตรา 7)

องค์ประกอบของความผิดต้องประกอบด้วย

1) การเข้าถึง (Access) ระบบคอมพิวเตอร์ ไม่ว่าจะเป็นเครื่องคอมพิวเตอร์แบบ Stand Alone คอมพิวเตอร์โน้ตบุ๊ค เครื่องคอมพิวเตอร์เซิฟเวอร์ หรือมือถือ และอุปกรณ์ใด ๆ ที่สามารถประมวลผลข้อมูลคอมพิวเตอร์ได้ และ

2) การที่จะเป็นความผิดตามมาตรา 5 และมาตรา 7 นั้น จะต้องเป็นการเข้าถึงโดยมิชอบ[3] ซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะหรือ *"มาตรการรักษาความปลอดภัย"* (เช่น ระบบ User Name, Password, ระบบ SSL, SET, ฯลฯ) นั่นเอง และ

3) ระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์นั้น มิได้มีไว้สำหรับผู้ที่กระทำความผิด ตัวอย่างเช่น นาย ก. แฮคเกอร์ ใช้โปรแกรมคอมพิวเตอร์เจาะระบบป้องกันรักษาความปลอดภัยแบบ Firewall ของกระทรวงไอซีที เพื่อแก้ไขข้อมูลในเว็บไซท์ของไอซีที โดยที่กระทรวงไอซีทีไม่ได้อนุญาต ถือเป็นความผิดตามมาตรา 5 และมาตรา 7

ข้อที่น่าสังเกตคือ มาตรา 5 และมาตรา 7 มุ่งเน้นและให้ความคุ้มครองกับ *"ข้อมูลส่วนบุคคลและข้อมูลส่วนตัว"* ของ บุคคลที่อยู่ในเครื่องคอมพิวเตอร์ หรือระบบคอมพิวเตอร์แต่ละเครื่องเป็นสำคัญ ดังนั้น หากนายจ้าง เจ้าของ องค์กรภาครัฐหรือเอกชน หรือผู้ที่ควบคุมระบบคอมพิวเตอร์ (Computer Manager) ผู้ จัดการระบบคอมพิวเตอร์เข้าถึงข้อมูลคอมพิวเตอร์ของลูกจ้าง หรือผู้อื่น โดยเกินจากขอบเขตอำนาจหน้าที่ที่ตนเองได้รับมอบหมายก็ถือเป็นความผิดตาม กฎหมายฉบับนี้ด้วย เช่น นาย ข. เป็นผู้ควบคุมคอมพิวเตอร์ของบริษัท A เข้าดูข้อมูลส่วนตัวของนางสาว B โดย ไม่ได้รับอนุญาตก็ถือว่าผิดตามกฎหมายฉบับนี้ ซึ่งมาตรการดังกล่าวจะทำให้ลูกจ้างและผู้ใช้คอมพิวเตอร์ทั้งหลายมีความมั่น ใจในเรื่องสิทธิเสรีภาพส่วนบุคคลมากขึ้น

ข. การล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ (มาตรา 6) มาตรานี้จะเอาผิดในกรณีที่ผู้ที่เก็บรักษาหรือล่วงรู้ถึงระบบป้องกันรักษาความปลอดภัย (อาทิเช่น ชื่อผู้ใช้บริการ (User Name) และรหัสผ่าน (Password)) และ นำเอาข้อมูลระบบรักษาความปลอดภัยดังกล่าวไปเปิดเผยโดยก่อให้เกิดความเสียหาย ก็มีโทษตามกฎหมายฉบับนี้ ตัวอย่างเช่น นาย ก. เป็นผู้จัดการระบบคอมพิวเตอร์ และทราบรหัสผ่านและชื่อผู้ใช้บริการของพนักงานและกรรมการของบริษัททั้งหมด และนำไปเปิดเผยแก่บุคคลภายนอก ก็ถือว่าเป็นความผิดตามมาตรา 6 ตามกฎหมายฉบับนี้ นอกจากนี้ กรณีที่แฮคเกอร์เจาะระบบคอมพิวเตอร์และนำรหัสผ่านหรือหมายเลขบัตรเครดิตที่ ได้จากการเจาะรหัสไปเผยแพร่ในเว็บไซท์ต่างๆ ก็ถือเป็นความผิดตามกฎหมายฉบับนี้เช่นเดียวกัน

ค. การดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์โดยมิชอบ (มาตรา 8) มาตรานี้เข้ามาอุดช่องโหว่ทางกฎหมายของมาตรา 74 พ.ร.บ.การประกอบกิจการโทรคมนาคม[4] ซึ่งแต่เดิมระบุความผิดไว้เพียงการดักรับฟังทางโทรศัพท์หรือสื่อโทรคมนาคมโดยมิชอบตามกฎหมายเท่านั้น มาตรา 8 ของกฎหมายฉบับนี้ให้ขยายความรวมถึงการกระทำทุกวิธีที่ใช้วิธีการทาง อิเล็กทรอนิกส์เพื่อดักรับข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่ง และข้อมูลนั้นมิได้มีไว้ใช้เพื่อประโยชน์สาธารณะ ตัวอย่างของความผิดตามมาตรานี้ได้แก่ ความผิดเกี่ยวกับการใช้เครื่องสแกนเนอร์ขโมยรหัสผ่านและข้อมูลของบัตรเอที เอ็มและบัตรเครดิตของบุคคลอื่น รวมถึงการดักรับการส่ง sms mms อีเมล์ หรือข้อมูลภาพเสียงใดๆ ที่ส่งผ่านระบบคอมพิวเตอร์ของบุคคลอื่น (Sniffing หรือ Interception) ในกรณีที่อาชญากรนั้นใช้เครื่องคอมพิวเตอร์บันทึกรหัสผ่านหรือข้อมูลบัตรเครดิตของผู้อื่น นอกจากเป็นความผิดตามมาตรา 8 ของกฎหมายฉบับนี้แล้ว ยังอาจถือว่าเป็นความผิดตามประมวลกฎหมายอาญา มาตรา 269/1 – 269/7 – ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์อีกด้วย

---

[1] **"ระบบคอมพิวเตอร์"** หมายถึง อุปกรณ์ หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดย อัตโนมัติ

[2] **"ข้อมูลคอมพิวเตอร์"** หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจ ประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทาง อิเล็กทรอนิกส์ด้วย

[3] **"โดยมิชอบ"** หมายถึง 1) การเข้าถึงโดยไม่ได้รับความยินยอมจากเจ้าของระบบคอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ 2) การเข้าถึงที่เกินจากขอบเขตอำนาจหน้าที่ที่ตนเองได้รับมอบหมาย 3) การเข้าถึงระบบคอมพิวเตอร์ผู้อื่นโดยไม่มีเหตุโดยชอบตามกฎหมาย

[4] **มาตรา 74 พ.ร.บ.การประกอบกิจการโทรคมนาคม** ความว่า ผู้ใดกระทำด้วยประการใดๆ เพื่อดักรับไว้ ใช้ประโยชน์ หรือเปิดเผยข้อความ ข่าวสาร หรือข้อมูลอื่นใดที่มีการสื่อสารทางโทรคมนาคมโดยไม่ชอบด้วยกฎหมาย ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่แสนบาท หรือทั้งจำทั้งปรับ

ง. การทำลายแก้ไขเปลี่ยนแปลงข้อมูลทางคอมพิวเตอร์โดยมิชอบ (มาตรา 9 – มาตรา 10) ในกรณีที่อาชญากรทางคอมพิวเตอร์ทำการแก้ไขเปลี่ยนข้อมูลทางคอมพิวเตอร์ หรือปล่อยไวรัสคอมพิวเตอร์ โปรแกรม Malware อาทิเช่น Trojan Horse, Worm, Mail Bomb เข้าสู่ระบบคอมพิวเตอร์ผู้อื่น ถือว่าเป็นความผิดตามมาตรา 9 แต่หากการกระทำดังกล่าวทำให้ระบบคอมพิวเตอร์ถูกชะลอขัดขวางจนไม่สามารถทำงานเป็นปกติได้ อาทิเช่น การทำ DOS (Denial – of – Service) ถือว่าเป็นความผิดตามมาตรา 10

นอก จากนี้ หากการกระทำดังกล่าวข้างต้นทำให้ประชาชนเสียหาย หรือเป็นการทำลายบริการทางสาธารณะ หรือทำให้บุคคลอื่นเสียชีวิต หรือทำลายความมั่นคงของประเทศ ก็จะมีบทเพิ่มโทษในมาตรา 12

จ. ความผิดเกี่ยวกับการส่งอีเมล์ขยะ (มาตรา 11) การส่งอีเมล์ขยะ ไม่ว่าจะส่งในรูปแบบอีเมล์ sms mms หรือรูปแบบอื่นใด หากส่งโดยปกปิดหรือปลอมแปลงแหล่งที่มาดังกล่าว[1] และการส่งดังกล่าวรบกวนระบบการใช้โปรแกรมคอมพิวเตอร์ของผู้อื่นโดยปกติสุข มีโทษปรับอีเมล์ หรือ sms ข้อความละ 100,000 บาท

ฉ. การเผยแพร่ชุดคำสั่งที่ใช้กระทำความผิด (มาตรา 13) กฎหมายฉบับนี้ลงโทษผู้ที่สนับสนุนให้มีการกระทำความผิดตามมาตรา 5 ถึงมาตรา 11 โดยการจัดหาเผยแพร่โปรแกรมชุดคำสั่งที่ใช้กระทำความผิด เพื่อป้องปรามเว็บไซท์ต่างๆ ที่ให้บริการดาว์นโหลดซอฟท์แวร์เพื่อใช้กระทำความผิดเกี่ยวกับคอมพิวเตอร์

ช. การเผยแพร่ข้อมูลคอมพิวเตอร์ที่ผิดกฎหมาย (มาตรา 14 – 15) กฎหมายในส่วนนี้จะเอาผิดในกรณีที่บุคคลโดยทั่วไป นำเข้าสู่ เผยแพร่ ส่งต่อ เว็บไซท์หรือระบบคอมพิวเตอร์ที่มีข้อมูลคอมพิวเตอร์ ที่ปลอม เป็นเท็จ ข้อมูลคอมพิวเตอร์ที่เป็นความผิดเกี่ยวกับความมั่นคงของราชอาณาจักร หรือความผิดเกี่ยวกับการก่อการร้าย ตามประมวลกฎหมายอาญา และข้อมูลคอมพิวเตอร์ที่มีลักษณะลามกอนาจาร โดยระบุโทษปรับไว้สูงถึง 5 ปี และปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ ดังนั้น การส่งต่อ sms หรือ e-mail ที่มีข้อมูลดังกล่าวอยู่ก็ผิดกฎหมายฉบับนี้

ผู้ให้บริการ[2]ที่เป็นบริษัทต่างๆ ที่ให้บริการระบบคอมพิวเตอร์แก่บุคคลอื่นก็มีหน้าที่ต้องตรวจสอบการใช้คอมพิวเตอร์ของลูกจ้างหรือลูกค้าของตน (Monitoring Duty) มิฉะนั้นอาจมีความผิดเช่นเดียวกับผู้ใช้ข้อมูลคอมพิวเตอร์ได้

ซ. ความผิดเกี่ยวกับการตัดต่อภาพผู้อื่นด้วยวิธีการทางอิเล็กทรอนิกส์ (มาตรา 16) มาตรานี้เป็นเพียงมาตราเดียวที่เป็นความผิดอาญาที่ยอมความได้ โดยระบุโทษกับบุคคลที่ตัดต่อ ดัดแปลง สร้างขึ้น ซึ่งภาพผู้อื่นและทำให้บุคคลอื่นนั้นเสื่อมเสียชื่อเสียง ถูกดูหมิ่น เกลียดชัง หรืออับอาย ซึ่งจะปรับใช้กับกรณีภาพตัดต่อของดาราหรือผู้มีชื่อเสียงต่างๆ ที่มักจะตัดต่อเพื่อความสนุกสนานหรือใช้ทำให้บุคคลดังกล่าวได้รับความอับอาย

2. การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (มาตรา 26) มาตรานี้ใช้แก้ปัญหาการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ (e-evidence accumulation) ที่ อาชญากรใช้ในการกระทำความผิด ซึ่งตามปกติการดำเนินคดีกับอาชญากรทางคอมพิวเตอร์นั้น เจ้าหน้าที่ตำรวจต้องรวบรวมข้อมูลพยานหลักฐานเพื่อพิสูจน์ว่าผู้กระทำความ ผิดนั้นกระทำความผิดจริงโดยต้องรวบรวมพยานหลักฐาน ได้แก่ ข้อมูลการเข้าสู่ระบบอินเตอร์เน็ตผ่านระบบโทรศัพท์ (ไม่ว่า แบบ Modem หรือ Leased Line) ข้อมูลที่ส่งผ่านระบบคอมพิวเตอร์ของผู้ให้บริการ (ISP) หรือ Log File ซึ่งข้อมูลดังกล่าวจะแสดงถึงเส้นทางและรายละเอียดการใช้ข้อมูลคอมพิวเตอร์ของผู้ใช้บริการอินเตอร์เน็ตแต่ละราย ซึ่งก็คือ ***"ข้อมูลจราจรทางคอมพิวเตอร์"*** ของกฎหมายฉบับนี้นั่นเอง เหตุที่ต้องมีมาตรา 26 เพราะว่า ก่อนหน้ากฎหมายฉบับนี้ใช้บังคับ ผู้ให้บริการอินเตอร์เน็ต (ISP) หรือผู้ให้บริการโทรศัพท์บางรายไม่ให้ความร่วมมือในการส่งมอบข้อมูลจราจรทาง คอมพิวเตอร์โดยอ้างว่าไม่ได้จัดเก็บไว้ ทำให้กฎหมายฉบับนี้ต้องระบุให้ผู้ให้บริการต้องจัดเก็บข้อมูลจราจร คอมพิวเตอร์อย่างน้อย 90 วัน มิฉะนั้นอาจมีโทษปรับไม่เกิน 500,000 บาท

ในทางปฏิบัติกระทรวงไอซีทีได้ออกประกาศหลักเกณฑ์เกี่ยวกับการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 เมื่อวันที่ 23 สิงหาคม 2550 โดยผ่อนผันระยะเวลาการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ให้แก่บุคคล 3 กลุ่ม กล่าวคือ ผู้ประกอบกิจการโทรคมนาคม และกิจการกระจายภาพและเสียง อาทิเช่น ผู้ให้บริการมือถือ AIS DTAC Truemove มีระยะเวลา 30 วัน (นับแต่วันที่ 23 สิงหาคม 2550) ขณะที่ผู้ให้บริการเข้าถึงระบบเครือข่ายคอมพิวเตอร์โดยทั่วไป บริษัท ห้างร้าน องค์กร มีระยะเวลาผ่อนผัน 180 วัน ส่วนผู้ให้บริการอินเตอร์เน็ตคาเฟ่และเกมส์ออนไลน์ให้ระยะเวลาผ่อนผันถึง 1 ปี

---

[1] **"ปลอมแปลงแหล่งที่มาของการส่ง"** หมายถึง การปลอมแปลง e-mail address, IP Address ที่แท้จริง

[2] **"ผู้ให้บริการ"** หมาย ถึง (1) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเตอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น (2) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

3. อำนาจของพนักงานเจ้าหน้าที่ตามกฎหมายใหม่ (มาตรา 18 – 21 และมาตรา 27) กฎหมายฉบับนี้ ได้แต่งตั้ง ***"พนักงานเจ้าหน้าที่ (Cyber Cop)"*** ซึ่งเป็นบุคคลที่มีความรู้ความเชี่ยวชาญเกี่ยวกับกฎหมายการสืบสวนสอบสวนและนิติเวชวิทยา (Computer Forensic) โดยให้อำนาจในการเรียกผู้ให้บริการให้ส่งคำชี้แจงหรือส่งมอบข้อมูล คอมพิวเตอร์และข้อมูลจราจรคอมพิวเตอร์เมื่อพนักงานเจ้าหน้าที่พบว่ามีการ กระทำความผิดเกิดขึ้นได้ โดยไม่ต้องขออำนาจจากศาล เว้นแต่การทำสำเนาการทำข้อมูลคอมพิวเตอร์ ข้อมูลจราจรคอมพิวเตอร์ การถอดรหัส การยึดอายัดระบบคอมพิวเตอร์ จะต้องได้รับอำนาจจากศาลเท่านั้น

4. เขตอำนาจศาลในการพิจารณาคดี (มาตรา 17) กฎหมาย ฉบับนี้ยังให้อำนาจพิเศษกับศาลในการรับพิจารณาคดีในกรณีที่ผู้กระทำความผิด เป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยร้องขอ และต้องรับโทษในราชอาณาจักรได้ (Arm's Length Doctrine) อาทิเช่น กรณีเว็บไซท์ youtube.com ที่เผยแพร่ข้อความหรือวีดีโอคลิปที่หมิ่นพระบรมเดชานุภาพ หากรัฐบาลไทย หรือคนไทยร้องขอ ศาลไทยก็มีอำนาจรับพิจารณาคดีกับบุคคลดังกล่าวได้

5. อำนาจของรัฐมนตรีไอซีทีในการปิดหรือบล็อกเว็บไซท์ (มาตรา 20) การปิดหรือบล็อกเว็บไซท์ที่เป็นที่กังวลของสื่อทั้งหลายว่าจะละเมิดสิทธิ ส่วนบุคคลหรือไม่นั้น กฎหมายฉบับนี้ให้อำนาจพนักงานเจ้าหน้าที่ว่าอาจปิดหรือบล็อกเว็บไซท์ได้ แต่ต้องผ่านกระบวนการกลั่นกรองถึง 3 ขั้นตอนคือ

ขั้นตอนที่ 1 มีการกระทำความผิดที่กระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรเฉพาะที่ระบุไว้ในภาค 2 ลักษณะ 1 หรือลักษณะ 1/1 ของประมวลกฎหมายอาญา[1] หรือขัดต่อความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน[2] ซึ่งเมื่อพนักงานเจ้าหน้าที่รวบรวมข้อมูลได้แล้ว จะต้องส่งมอบข้อมูลดังกล่าวให้รัฐมนตรีกระทรวงไอซีทีพิจารณา

ขั้นตอนที่ 2 รัฐมนตรีกระทรวงไอซีทีพิจารณาแล้วมีเหตุอันสมควรก็จะยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อสั่งให้ปิดหรือบล็อกเว็บไซท์

---

[1] ได้แก่ ความผิดเกี่ยวกับพระมหากษัตริย์

[2] ได้แก่ ความผิดเกี่ยวกับการพนันขันต่อ ภาพลามกอนาจาร ยาเสพติด ฯลฯ

ขั้นตอนที่ 3 ศาลจะพิจารณาคำร้องของรัฐมนตรีไอซีทีและพยานหลักฐานทั้งหมด และมีคำสั่งอนุญาตหรือไม่อนุญาตให้มีการปิดหรือบล็อกเว็บไซท์ การปิดหรือบล็อกเว็บไซท์ในกรณีที่เกี่ยวข้องกับความมั่นคงหรือการก่อการร้าย (State Security) นั้น เป็นที่ยอมรับกันโดยสากลแม้แต่กฎหมาย the Patriot Act ของอเมริกาก็ให้อำนาจดังกล่าวไว้เช่นกัน อย่างไรก็ตาม กฎหมายฉบับนี้ไม่ได้ให้อำนาจรัฐบาลในการปิดหรือบล็อกเว็บไซท์ทางการเมือง

6. บทกำหนดโทษสำหรับพนักงานเจ้าหน้าที่ (มาตรา 22 – 24) กฎหมาย ฉบับนี้กำหนดโทษทางอาญา ทั้งโทษจำคุกและโทษปรับกับพนักงานเจ้าหน้าที่ที่เปิดเผยหรือส่งมอบข้อมูล คอมพิวเตอร์ หรือข้อมูลจราจรคอมพิวเตอร์ของผู้อื่นโดยไม่ได้รับอนุญาตทั้งโดยประมาทและ โดยเจตนา และยังเอาผิดกับผู้ที่ล่วงรู้ข้อมูลคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่นำมา เปิดเผยโดยมิชอบด้วย

บทสรุป ดัง นั้น หากดูสภาพโดยรวมของกฎหมายฉบับนี้ ถือว่าเป็นกฎหมายที่คุ้มครองสิทธิประชาชนมากกว่าลิดรอนสิทธิ โดยมุ่งเน้นการปราบปรามอาชญากรรมทางคอมพิวเตอร์ที่นับวันจะทวีความรุนแรงมาก ขึ้น โดยมีบทบัญญัติคุ้มครองสิทธิ และระบุโทษจำคุกและโทษปรับในทางกฎหมายกับพนักงานเจ้าหน้าที่และเจ้าหน้าที่ ของรัฐที่เปิดเผยข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาต อย่างไรก็ตาม การใช้กฎหมายให้มีประสิทธิภาพโดยที่ไม่ละเมิดสิทธิส่วนบุคคลหรือใช้อำนาจโดย มิชอบนั้น คงต้องเป็นหน้าที่ของหน่วยงานรัฐที่ต้องเน้นย้ำมาตรการด้านจริยธรรม และประสิทธิภาพของบุคลากรมากกว่าตัวบทกฎหมาย ประกอบกับการใช้มาตรการทางเทคนิค (Lex Electronica และให้องค์กรต่างๆ ในอินเตอร์เน็ตดูแลควบคุมตัวเอง (Self-Regulation) การแก้ปัญหาอาชญากรรมคอมพิวเตอร์จึงจะมีประสิทธิภาพ