บทที่ 3

ความรับผิดเกี่ยวกับไวรัสคอมพิวเตอร์ของต่างประเทศ

3.1 ลักษณะการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

การกระทำความผิดเกี่ยวกับคอมพิวเตอร์มีหลายประเภทแตกต่างกันออกไป โดยขึ้นอยู่กับการกำหนดรูปแบบต่าง ๆ ของผู้เขียนโปรแกรมขึ้น เพื่อตอบสนองความต้องการโดยเฉพาะของเขา ซึ่งจะมีผลกระทบถึงการเริ่มการเตรียมการในเบื้องต้น ในอันที่จะกำหนดเกี่ยวกับการอธิบายถึงผลกระทบที่เกิดขึ้นจากการกระทำความผิดเกี่ยวกับคอมพิวเตอร์หลาย ๆ อย่าง อันจะทำไปสู่การวิเคราะห์ถึงการกระทำเกี่ยวกับไวรัสคอมพิวเตอร์จะเป็นการกระทำในรูปแบบใด และการนำกฎหมายมาบังคับใช้

ก่อนที่จะวิเคราะห์ถึงปัญหาทางกฎหมาย สมควรอย่างยิ่งที่จะต้องกล่าวถึงปัญหาที่สำคัญ ซึ่งเป็นลักษณะทั่วไปของการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ว่าการกระทำความผิดเกี่ยวกับคอมพิวเตอร์สามารถที่จะกระทำได้ในรูปแบบใดบ้าง ดังนี้

3.1.1 การเข้าถึงโดยปราศจากอำนาจ (Unauthorized access)

สิ่งที่จะต้องพิจารณาถึงประโยชน์ที่จะได้รับจากการเข้าถึง "ข้อมูล"หรือ"โปรแกรม" โดยปราศจากอำนาจที่เก็บอยู่ในคอมพิวเตอร์ โดยได้กำหนดปัญหาที่เกิดขึ้นนี้ในชื่อของ "การเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจ" (Unauthorized access to a computer) ชื่อที่ถูกกำหนดนี้ เป็นการสะท้อนให้เห็นถึงสภาพที่แท้จริงว่า โดยเนื้อแท้มิได้กังวลเกี่ยวกับการเข้าถึงโดยปราศจากอำนาจ ต่ออุปกรณ์ต่างๆ ที่ประกอบขึ้นเป็นเครื่องคอมพิวเตอร์ หรือที่เรียกว่า ฮาร์ดแวร์ (Hardware) แต่มีความกังวลถึงสิ่งที่จะได้รับจากกการเข้าถึงสาระสำคัญ (Meterial) ที่เก็บ

ไว้ในคอมพิวเตอร์ คือโปรแกรมหรือข้อมูล

ปัญหานี้มิได้เป็นปัญหาเกี่ยวกับกฎหมายพิเศษ ที่จะยกขึ้นในอันที่จะเกี่ยวพันถึงการได้ประโยชน์จากการเข้าถึงโดยปราศจากอำนาจในฮาร์ดแวร์ ความรับผิดอาญาใด ๆ ในคดี ขึ้นอยู่กับเหตุผลของการเข้าถึง การขโมยหรือทำให้เสียหาย เกี่ยวกับส่วนประกอบของคอมพิวเตอร์ที่สามารถจับต้องได้ สามารถที่จะถูกฟ้องร้องได้ในความผิดฐานลักทรัพย์หรือเสียหายทางอาญา และการเข้าไปในอาคารหรือส่วนของอาคาร เช่น ห้องคอมพิวเตอร์ จะเป็นองค์ประกอบของความผิดฐานลักทรัพย์และบุกรุก หากพิสูจน์ได้ว่าผู้ที่ได้บุกรุกนั้นมีเจตนาที่จะขโมยหรือกระทำให้เกิดความเสียหายหรือไม่ โดยนำมาปรับใช้กับกฎหมายที่มีอยู่แล้วซึ่งไม่มีความจำเป็นที่จะต้องกำหนดเป็นความผิดพิเศษที่จะครอบคลุมถึงการกระทำความผิดเช่นนี้อีก[1]

อย่างไรก็ตามกฎหมายอาญาที่ใช้บังคับอยู่มิได้ขยายขอบเขตไปถึง "การเข้าถึงโดยปราศจากอำนาจ" ต่อโปรแกรมหรือข้อมูลที่จัดเก็บอยู่ภายในคอมพิวเตอร์ บุคคลอาจจะเข้าถึงโดยปราศจากอำนาจถึงสาระสำคัญ (ข้อมูลหรือโปรแกรม) โดยวิธีใด ๆ ก็ตามซึ่งมีหลายรูปแบบ แต่ไม่ว่าผู้นั้นเป็นลูกจ้างของบริษัท ซึ่งปกติการเข้าถึงจะมีการจำกัดอำนาจการเข้าถึงไว้ เพื่อวัตถุประสงค์ของการเข้าถึงคอมพิวเตอร์โดยเฉพาะ หรือจำกัดเวลาไว้โดยเฉพาะ แต่ได้กระทำโดยนอกเหนือจากอำนาจโดยใช้โอกาสเช่นนั้นโดยปราศจากการอนุญาต หรือผู้นั้นอาจจะเป็นบุคคลภายนอกก็ตาม

ซึ่งตามที่กล่าวมานี้ คอมพิวเตอร์ชนิดตั้งโต๊ะ (Desk-top computers) ที่ได้เชื่อมกับคอมพิวเตอร์กลาง จัดได้ว่ามีโอกาสมากที่จะมิได้ปฏิบัติไปตามหน้าที่ โดยการเข้าถึงโดยปราศจากอำนาจ โดยการกระทำผิดประเภทนี้ จะกระทำโดยลูกจ้างมากกว่ากรณีอื่น ๆ

การเข้าถึงโดยปราศจากอำนาจอาจจะเป็นเพียงเพื่ออยากรู้อยากเห็น หรือเพื่อที่จะค้นหาข้อมูลที่เก็บอยู่ในคอมพิวเตอร์เกี่ยวกับลูกจ้างหรือลูกจ้างคนอื่น ๆ หรือความคาดหวังอื่น ๆ

---

1. Martin Wasik, Crime and the Computer(Great Britain:Biddle, 1990), p.42.

เกี่ยวกับการปฏิบัติงานของบริษัท ซึ่งก็มิได้เป็นเจตนาที่ชั่วร้ายจนเกินไป แต่ที่สำคัญเมื่อข้อมูลที่เก็บไว้นั้นเป็นความลับ และเราจะพิจารณาอย่างไรถึงจะเหมาะสมที่จะใช้กฎหมายอาญาที่จะป้องกันข้อมูลซึ่งเป็นความลับนั้น โดยเฉพาะปัญหาหนึ่งซึ่งได้รับความสนใจมากคือการที่นักคอมพิวเตอร์ผู้ซึ่งกระตือรือร้น ที่จะท้าทายความสามารถของตนเกี่ยวกับคอมพิวเตอร์ ในการที่จะเข้าถึงคอมพิวเตอร์ ที่มีมาตรการรักษาความปลอดภัยในทุก ๆ แห่ง

ผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์เป็นจำนวนมาก ใช้เพียงอุปกรณ์คอมพิวเตอร์แบบง่าย ๆ โดยทั่วไปจะเป็นไมโครคอมพิวเตอร์ผูกเข้าคู่กับเครื่องโมเด็ม (Modem) ซึ่งทำให้ผู้กระทำผิดสามารถที่จะเข้าถึงคอมพิวเตอร์เป้าหมาย โดยผ่านทางสายเชื่อมติดต่อสื่อสาร เช่น ระบบโทรศัพท์สาธารณ[2]

คอมพิวเตอร์ส่วนใหญ่จะถูกป้องกัน โดยอุปกรณ์ที่จำกัดการเข้าถึงซึ่งผู้มีอำนาจใช้จะต้องพิสูจน์ลักษณะเฉพาะ เช่น รหัสผ่าน จะมากหรือน้อยก็แล้วแต่ เพื่อเป็นกุญแจในรูปของรหัสผ่าน แต่อย่างไรก็ตาม ระบบความปลอดภัยของคอมพิวเตอร์บ่อยครั้งที่ไม่แน่นหนาพอเท่าที่ควรจะเป็น และในบางกรณีเกือบจะใช้ไม่ได้เลย (non existent) ไม่มีความปลอดภัยในสถานที่ทั้งหมดหรือแม้แต่สถานที่ซึ่งต้องการให้พิสูจน์รหัสผ่านก็ตาม

การกระทำโดยเข้าถึงอาจจะเป็นการกระทำโดยลูกจ้าง ซึ่งมันเป็นเรื่องที่ง่ายมากและง่ายที่จะทำนาย มีหลายครั้งที่ผู้กระทำผิดจะสามารถที่จะได้รับประโยชน์จากการเข้าถึง เพราะรู้รหัสผ่านทั้งหมด ซึ่งทำให้เขาเข้าไปสู่ระบบคอมพิวเตอร์ได้ หรืออาจจะเป็นไปได้ว่า ผู้กระทำผิดค้นพบรหัสผ่าน โดยการสืบหาหรือโดยบังเอิญ เช่น การใช้โปรแกรมซึ่งเป็นการสุ่มตัวเลขหรือตัวอักษร จนกระทั่งถูกต้อง อันเป็นวิธีการหนึ่งซึ่งสามารถถูกพบ อีกประการหนึ่งเป็นการละเลยรูปแบบความปลอดภัยขั้นพื้นฐาน ซึ่งการป้องกันความพยายามที่จะบันทึกรหัสผ่านซ้ำ มันเป็นความจริงว่าเทคนิคการกระทำความผิดมีความเป็นอัจฉริยะมากกว่า และเป็นที่เห็นได้ชัดจากคดีเป็นจำนวนมากเกี่ยวกับการเข้าถึงโดยปราศจากอำนาจ เกิดขึ้นเนื่องจากวิธีการป้องกันความปลอดภัยไม่ดีพอ ซึ่งมันจะสัมพันธ์กับคอมพิวเตอร์ที่ราคาถูกและง่ายในการติดตั้งเพื่อป้องกัน อย่างไรก็ตามนัก

---

2. Ibid., p.43

คอมพิวเตอร์ที่มีทักษะสูงและมีประสบการณ์จะพิจารณาการเข้าถึง ในฐานะที่เป็นการท้าทายส่วนบุคคลที่เป็นอุปกรณ์รักษาความปลอดภัยที่อยู่ในสถานที่นั้น และมันยากมากที่จะแน่ใจว่าระบบคอมพิวเตอร์ทั้งหมดมีความปลอดภัย

มีการกระทำผิดรูปแบบบางอย่าง ซึ่งมิได้มีเจตนาชั่วร้ายจนเกินไป กรณีนี้มีผู้ที่สนับสนุนและรู้ดีที่สุดคนหนึ่ง คือ นายฮิวโก คอร์นวอล์ (Hugo Conwall) ที่ว่ามันมิได้เป็นการมากเกินไปกว่า "เป็นการศึกษาและกีฬาที่สร้างสรรค์... ในรูปแบบของกระบวนการของ "การเข้าไปข้างใน" (getting in) สิ่งเหล่านี้เป็นความพอใจมากกว่า ในอันที่จะค้นหาไฟล์คอมพิวเตอร์ที่มีระบบการป้องกัน"[3]

ปัญหาที่สำคัญประการหนึ่งสำหรับกฎหมายอาญา ไม่ว่าจะเป็นการกระทำความผิดเกี่ยวกับคอมพิวเตอร์หรือไม่ มีการบรรยายในฐาน "การบุกรุกทางคอมพิวเตอร์" (computer trespass) ควรที่จะผิดกฎหมาย แม้ว่าจะมีการพูดว่า การกระทำดังกล่าวผู้กระทำไม่มีเจตนาชั่วร้าย แต่อย่างไรก็ตามการกระทำเช่นนั้น อาจจะได้รับประโยชน์จากการเข้าถึงความลับหรือกระทบถึงข้อมูลที่อ่อนไหว (sensitive) และแม้จะไม่ได้เคลื่อนไหวข้อมูลดังกล่าว ที่จะทำให้ได้รับประโยชน์หรือสาเหตุของความเสียหาย ในสิ่งที่ตนอาจจะได้ประโยชน์จากการเข้าถึง แต่อาจจะก่อให้เกิดความเสียหาย ซึ่งเกิดขึ้นโดยความประมาทต่อโปรแกรมหรือข้อมูลในคอมพิวเตอร์หรือกระตุ้นระบบความปลอดภัยซึ่งอยู่ข้างใน อันเป็นสาเหตุให้ทั้งระบบถูกปิดลง ซึ่งเป็นผลให้เกิดความไม่สะดวก สูญเสีย หรืออันตรายได้

เป็นสิ่งที่ยากในการที่จะแบ่งแยกความแตกต่างระหว่างนักคอมพิวเตอร์ ซึ่งเข้าถึงโดยไม่มีเจตนาชั่วร้าย ในกรณีนี้นายคอร์นวอล์ ได้กล่าวว่าคอมพิวเตอร์นั้น สำหรับตนแล้วเป็นเพียงกีฬาชนิดหนึ่ง โดยเฉพาะคอมพิวเตอร์ที่มีการพัฒนาสิ่งใหม่ ๆ ขึ้นมา ย่อมเป็นจุดมุ่งหมายที่น่าสน

---

3. Hugo Cornwall, the New Hacker's Handbook (London : Century Hutchinson,1985), p.8

ใจที่จะเข้าถึง โดยที่ตนเองไม่เคยมีเจตนาที่จะก่อให้เกิดความเสียหาย ต่อคอมพิวเตอร์แต่อย่างใด[4]

มีตัวอย่างจำนวนมาก ที่ชี้ให้เห็นถึงการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และมีพยานเล็ก ๆ น้อย ๆ อีกเป็นจำนวนมาก โดยการกระทำความผิดนี้เข้ามามีชื่อเสียงในตอนต้นทศวรรษที่ 1980 ได้เริ่มมีรายงานชี้ให้เห็น เช่น ในคดีหนึ่งซึ่งเกิดขึ้นในปี 1974 เด็กนักเรียนชายเวสท์มินสเตอร์(Westminster) ซึ่งมีอายุเพียง 15 ปี ได้ทำลายระบบรักษาความปลอดภัยของศูนย์บริการระบบแบ่งเวลาคอมพิวเตอร์ (Computer time-sharing) และได้รับประโยชน์จากไฟล์ที่ถูกใช้

มีคดีหนึ่งซึ่งมีชื่อเสียง คือ "แก๊งค์ 414"(414 gang) กลุ่มซึ่งมีงานอดิเรกเกี่ยวกับคอมพิวเตอร์ ซึ่งได้เข้าถึงคอมพิวเตอร์ในธนาคารที่ลอสแองเจอลิส (Los Angeles), บริษัทบูนในมอนทรีโอ (Montreal) โรงพยาบาลในนิวยอร์ค (New York) นอกจากนี้ ในปี 1985 เด็กนักเรียนชาย 7 คน ซึ่งมีความสนใจในคอมพิวเตอร์ ที่นิวเจอซี่ (New Jersey) ได้เข้าถึงระบบติดต่อสื่อสารทางทหารที่เพนตากอน (Pentagon) และในปี 1986 นักเรียนเทคโนโลยีคอมพิวเตอร์หนุ่ม 3 คน ในผรั่งเศส ยอมรับว่าเขาได้เข้าไปถึง 15 ครั้ง ในระบบคอมพิวเตอร์ที่ใหญ่ที่สุดในผรั่งเศส ระหว่างวันหยุดอีสเตอร์ (Easter holiday) รวมถึงคอมพิวเตอร์ Cray One ซึ่งเก็บข้อมูลเกี่ยวกับการวิจัยทางอวกาศแห่งชาติ และที่อื่น ๆของรัฐ และได้บันทึกข้อมูลด้านเทคโนโลยีและด้านกองทัพซึ่งลับสุดยอด เขาได้อธิบายว่า เขาต้องการที่จะรู้จริง ๆ ว่า "ไกลเท่าไหร่ที่เขาสามารถจะทำได้"[5]

วัตถุประสงค์ของการเข้าถึงโดยปราศจากอำนาจบางอย่างนั้น วัตถุประสงค์นี้ค่อนข้างที่จะเคลือบคลุมในจิตใจของผู้กระทำผิดหรือที่จะชี้ได้เฉพาะเจาะจง ผู้กระทำผิดอาจจะค้นหาความบกพร่อง (weakness) ในระบบความปลอดภัยของบริษัทและโอกาสที่จะทำการฉ้อฉล

---

4. Ibid.,p.7

5. Ibid.,p.45

เจตนาที่จะเอาผลประโยชน์ตลอดเวลาที่มี เป็นการยากที่จะชี้เจตนาของบุคคลให้เห็นได้ชัดเจน การฟ้องบ่อยครั้งที่จะสามารถใช้องค์ประกอบในฐานความผิดของการขโมย ฉ้อโกง และการหลอกลวง หรือการการพยายามกระทำความผิด ซึ่งกฎหมายไม่คำนึงถึงผลของการกระทำ แต่การกระทำต้องมากกว่าเพียงขั้นเตรียมการจึงจะเป็นความผิด

3.1.2. การฉ้อฉลเกี่ยวกับคอมพิวเตอร์ (Computer fraud)

การฉ้อฉลเกี่ยวกับคอมพิวเตอร์เกิดขึ้นมากที่สุด ในจำนวนการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งจากการสำรวจของสถาบันเทคโนโลยีคอนฟิวส์ (the Conlfield Institute of technology) ในออสเตรเลีย[6] พบว่ามีการฉ้อฉลทางคอมพิวเตอร์มีจำนวนมากถึง 60 ครั้ง จากจำนวน 123 ครั้ง ของการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ทั้งหมด และในการสำรวจของสถาบันอื่น ๆ โดยทั่วไปก็ได้ผลเช่นเดียวกัน

เหตุผลที่สำคัญของการฉ้อฉลทางคอมพิวเตอร์ เนื่องจากวัตถุประสงค์ที่ฉ้อฉลนั้นอยู่ที่ทรัพย์สินหรืออื่น ๆ ซึ่งผู้ที่ฉ้อฉลอาจจะทำการเปลี่ยนแปลงข้อมูลเกี่ยวกับเงินเดือน การแจ้งหนี้ค่าใช้จ่าย การจ่ายค่าครองชีพและบัญชีธนาคาร ที่เห็นได้ชัดจากแนวโน้มของการเพิ่มขึ้นของสังคมที่ไม่ใช้เงินสด รูปแบบของการฉ้อฉลจะเป็นที่แพร่ขยายมากขึ้นแทนที่การฉ้อฉลทางกระดาษ โดยเฉพาะการเสี่ยงของการที่เงินจำนวนมหาศาล ซึ่งจะถูกโอนโดยทางคอมพิวเตอร์นี้เป็นการโอนกันทางไฟฟ้า

การฉ้อฉลเกี่ยวกับคอมพิวเตอร์ อาจถูกกระทำผิดได้ในหลายรูปแบบ ทั้งโดยผู้มีอำนาจใช้และไม่มีอำนาจใช้คอมพิวเตอร์ ก็สามารถที่จะทำการฉ้อฉลได้ โดยการฉ้อฉลอาจแบ่งได้เป็นขั้นตอน ดังนี้

<u>ขั้นตอนที่ 1</u> ขั้นตอนขณะใส่ข้อมูลเข้าไปในคอมพิวเตอร์ อาจจะโดยการปลอม เพิ่ม หรือเปลี่ยนแปลงข้อมูลเดิมเข้าไปโดยตรงหรือในระหว่างการใส่ข้อมูลเข้าไปในเครื่องคอมพิวเตอร์ การเปลี่ยนแปลงอาจถูกกำหนด ให้เป็นสาเหตุให้มีการจ่ายเงินตามบัญชีธนาคาร ซึ่งผู้ฉ้อฉล

6.Martin Wasik, Ibid.,p.48

เป็นเจ้าของหรือจ่ายให้แก่ผู้ร่วมกระทำความผิด หรืออาจจะลบหรือปิดบังพยานหลักฐาน จากการกระทำความผิดอื่นรวมถึงการเพิ่มข้อมูลด้านความเชื่อถือ ให้มากขึ้นหรือลบข้อมูลที่ไม่น่าเชื่อถือออกไปจากคอมพิวเตอร์ ข้อมูลด้านการติดต่อซื้อขายสินค้า ด้านความเชื่อถืออาจจะสูงขึ้นหรือถูกลดลงได้ ในฐานะที่ซึ่งข้อมูลการซื้อขายถูกปิดบัง บัญชีเงินเดือนก็เป็นอีกสิ่งหนึ่งที่ง่ายต่อการฉ้อฉล การฉ้อฉลนี้เป็นรูปแบบที่มีการกระทำความผิดโดยเสมียน พนักงานพิมพ์ข้อมูล เจ้าหน้าที่ผู้รับผิดชอบเกี่ยวกับการรวบรวม ตรวจ ติดต่อ และใส่ข้อมูลลงในคอมพิวเตอร์

ขั้นตอนที่ 2 ขั้นตอนการทำงานของคอมพิวเตอร์ ขั้นตอนนี้อาจจะเป็นผลโดยตรงจากการกระทำของผู้ฉ้อฉล โดยการเปลี่ยนรหัสคอมพิวเตอร์หรือโปรแกรมการทำงานในคอมพิวเตอร์ โปรแกรมอาจจะถูกใส่เข้าไปโดยผู้ฉ้อฉล ซึ่งได้ทำงานโดยตรงต่อส่วนที่เกี่ยวข้องกับการเงิน เพื่อไปสู่บัญชีที่กำหนด หรือโปรแกรมอาจจะถูกลบออก การกระทำในขั้นตอนนี้ยังรวมไปถึงการกระทำที่เรียกว่า "ไวรัสคอมพิวเตอร์ " (Computer Virus) ด้วย

ขั้นตอนที่ 3 ขั้นตอนการนำข้อมูลออก ซึ่งในขณะที่มีการนำข้อมูลออกอาจจะมีการปิดบังหรือเปลี่ยน หรืออาจใช้ในการบังหน้าการฉ้อฉลอื่น ๆ

ซึ่งการแบ่งลักษณะของการฉ้อฉลออกเป็น 3 ขั้นตอนนี้ อาจจะมีการฉ้อฉลในทางอื่น ๆ อีกก็ได้ และบ่อยครั้งที่พบว่า มีการกระทำความผิดมากกว่า 1 ขั้นตอน ในการฉ้อฉลแต่ละครั้ง

ในการสำรวจเกี่ยวกับการกระทำความผิดและการฉ้อฉลเกี่ยวกับคอมพิวเตอร์ ในปี 1987 ว่า จำนวนการกระทำความผิด 118 ครั้ง ซึ่งได้มีการรายงานโดย the Audit Commission[7] ของประเทศอังกฤษว่ามีจำนวน 61 ครั้ง ถูกจัดอยู่ในประเภทของการฉ้อฉล ซึ่งเป็นการฉ้อฉลในขั้นตอนการนำข้อมูลเข้า(Input) จำนวน 57 ครั้ง ฉ้อฉลโดยโปรแกรมจำนวน 3

7.Audit Commission, Survey of Computer Fraud and Abuse (London: Hmso,1987)

ครั้ง และฉ้อฉลขณะนำข้อมูลออก (out put) อีก 1 ครั้ง

จะเห็นได้ว่าการฉ้อฉลขณะนำข้อมูลเข้ามีมากที่สุด โดยตัวเลขนี้ได้รับมาจาก the Audit Commission ซึ่งในการสำรวจในตอนต้น ๆ ในปี 1981 และ 1984 ผลก็ได้รับเช่นนี้เหมือนกัน และไม่ว่าจะมีการวิจัยที่ไหนก็ตาม การฉ้อฉลโดยการนำเข้าในบางครั้งย่อมเป็นการแสดงให้เห็นถึงบริเวณที่มีความเสี่ยงสูง เพราะมันเป็นขั้นตอนกระบวนการทำงานหมุนเวียนของคอมพิวเตอร์ (Computer processing cycle) คณะกรรมาธิการ (the Audit Commission) ได้แจ้งในรายงานในปี 1984 และ 1987 ว่า การฉ้อฉลขณะนำเข้าเป็นการทำโดยใช้ความสามารถที่ไม่จำเป็นต้องอาศัยความเชี่ยวชาญโดยเฉพาะ แต่สามารถใช้ประโยชน์จากการที่การควบคุมความปลอดภัยไม่มั่นคงพอ โดยเฉพาะอย่างยิ่งไม่มีการแบ่งแยกเจ้าหน้าที่ออกจากกันอย่างชัดเจน ซึ่งพื้นฐานของการรักษาความปลอดภัยจะต้องมี การฝึกฝนและผู้ดูแลเจ้าพนักงานมีไม่เพียงพอ และการที่ไม่มีการควบคุมขณะขั้นตอนการนำข้อมูลเข้า[8]

ในคดีหนึ่งเกี่ยวกับการฉ้อฉลขณะนำข้อมูลเข้า ซึ่งเป็นรายงานของคณะกรรมาธิการปรับบรุงกฎหมายของอังกฤษ ซึ่งได้เปิดเผยถึงเจ้าหน้าที่จ่ายเงินของบริษัทแห่งหนึ่ง ได้สร้างบัญชีการจ่ายเงินซึ่งที่ตนเองไม่มีอำนาจ โดยที่ตนได้ใส่ข้อมูลรายการแจ้งจำนวนราคาสินค้าเท็จเข้าไปในเครื่องคอมพิวเตอร์ ที่เขารับผิดชอบ อันเป็นการก่อให้เกิดจำนวนเงินของเจ้าหนี้ปลอมขึ้น เช็คได้ออกโดยคอมพิวเตอร์ และได้ถูกส่งไปตามที่อยู่ซึ่งถูกใช้ไปทางไปรษณีย์ ในช่วงเวลากว่า 5 เดือน เป็นเงินกว่า 14,000 ปอนด์ ที่เขาได้รับ[9]

หรือในคดีซึ่งได้มีการกระทำผิดเป็นระยะเวลากว่า 18 เดือน ในการฉ้อฉลบนพื้นฐานของการแจ้งรายการหนี้สินค้าเท็จขึ้น และนำเข้าสู่ระบบบัญชีแยกประเภทการซื้อขายโดยคอมพิวเตอร์ซึ่งมีมูลค่ากว่า 80,000 ปอนด์ โดยการกระทำเป็นการกระทำของผู้จัดการฝ่ายขาย ผู้มีอำนาจที่จะเปิดดูบัญชีที่ได้บรรจุเข้าไปใหม่ในไฟล์ของการซื้อ ดูรายการคำสั่งเดิม มีอำนาจในการรับสินค้า และยอมรับการแจ้งราคาสินค้าเพื่อที่จะชำระเงินอันเป็นเท็จนั้น เช็คได้

8.Martin Wasik, Ibid., p.49

9.Ibid., p.49

ถูกออกโดยอัตโนมัติจากคอมพิวเตอร์และใช้เครื่องจักรกลลงนามในเช็ค ถูกส่งไปยังที่อยู่ที่ถูกกำหนดโดยผู้จัดการฝ่ายขายนั้น[10]

ในการฉ้อฉลในการขั้นตอนการทำงานของคอมพิวเตอร์ คือการฉ้อฉลเกี่ยวกับโปรแกรม วิธีการฉ้อฉลโดยวิธีนี้เป็นวิธีที่น่าสนใจ แต่มีหลักฐานที่จะแสดงให้เห็นเพียงเล็กน้อยเท่านั้น แม้ว่าจะเกิดขึ้นบ่อยครั้งมาก ตั้งแต่ผู้กระทำความผิดได้เข้ามาเกี่ยวข้องเกี่ยวพันกับซอฟต์แวร์ ซึ่งจะต้องมีความสามารถอย่างมากเกี่ยวกับคอมพิวเตอร์ มีรูปแบบการกระทำและได้มีการตั้งชื่อแตกต่างกันออกไปคือ

1. วิธีฉ้อฉลแบบม้าโทรจัน (Thojan Horse) ซึ่งผู้กระทำผิดได้เพิ่มหรือขยายโครงสร้างในซอฟแวร์ก่อนที่จะให้โปรแกรมนั้นทำงาน เมื่อโปรแกมนั้นถูกทำงาน ผลของการขยายหรือส่วนของคำสั่งที่เขียนเพิ่มขึ้นให้กับโปรแกรม ให้อยู่ในช่องที่เกี่ยวกับการเงินให้เข้าไปสู่บัญชีของผู้ฉ้อฉล โปรแกรมอาจจะเขียนขึ้นมาเพื่อจุดประสงค์ใดจุดประสงค์หนึ่งโดยเฉพาะ และหลังจากที่มีการปฏิบัติการตามที่กำหนดแล้วก็อาจจะกำหนดให้ลบตัวมันเองทิ้งทันที ซึ่งทำให้ไม่สามารถค้นพบหลักฐานของการกระทำความผิดได้

2. วิธีประตูกล (Trap Doors) โดยในการพัฒนาระบบการทำงานของเครื่องคอมพิวเตอร์และโปรแกรมคอมพิวเตอร์สำเร็จรูปขนาดใหญ่นั้น ในทางปฏิบัตินักเขียนโปรแกรมคอมพิวเตอร์มักจะมีการเว้นตำแหน่งช่องว่างไว้ในชุดคำสั่งในการเขียนทุกครั้ง เพื่อใช้ในการเพิ่มคำสั่งและใช้ในการปรับปรุงแก้ไขโปรแกรมในภายหลัง หรือเพิ่มความสามารถในการผลิตข้อมูลกลางคันอันเป็นการขจัดข้อบกพร่องเล็ก ๆ น้อย ๆ ให้หมดไป ตำแหน่งช่องว่างเหล่านี้อาจกลายเป็นประตูกลให้มีการกระทำความผิดขึ้นได้เมื่อถูกปล่อยทิ้งไว้โดยไม่ลบทิ้ง หลังจากเขียนโปรแกรมเสร็จแล้วจะปิดโปรแกรม ซึ่งถ้าผู้เขียนโปรแกรมไม่สุจริต ก็อาจจะปิดโปรแกรมขึ้นภายหลังและเพิ่มคำสั่งเข้าไปได้ และบางครั้งแม้แต่ผู้ใช้โปรแกรมเองซึ่งไม่ใช่เป็นคนเขียนโปรแกรมก็อาจค้นพบประตูกลอันนี้ได้โดยบังเอิญ แม้ว่าระบบการทำงานของเครื่องคอมพิวเตอร์จะได้ออกแบบขึ้นโดยมีระบบก็สามารถที่จะใส่รหัสชนิดที่ระบบการป้องกันดังกล่าวไม่อาจคุ้มครองได้ โดยวิธีใส่เข้าไปใน

---

10. Ibid., p.49

ช่องว่างที่ทำขึ้นนั้น ทั้งในขณะที่มีการบำรุงรักษาและในขณะปรับปรุงแก้ไขระบบการทำงานของเครื่องคอมพิวเตอร์ รหัสคำสั่งที่แอบใส่เพิ่มเติมเข้าไปในช่องว่างหรือประตูกลนี้ สามารถทำให้เครื่องคอมพิวเตอร์ทำงานให้ตามที่ต้องการได้โดยไม่มีขีดจำกัด[11]

3. การฉ้อฉลโดยวิธีแบบซาลามิ (Salami) เป็นรูปแบบการฉ้อฉลที่ซึ่งเกี่ยวข้องกับการสอดโปรแกรม ส่วนปะ(patch) ซึ่งจะย้ายผลของจำนวนเงินเล็กน้อยจากหลาย ๆ บัญชี เพื่อว่าผู้ใช้จะไม่สังเกตเห็นสิ่งที่ผิดปกติใด ๆ

รูปแบบการฉ้อฉลวิธีนี้เป็นการจัดโปรแกรมให้สั่งให้เครื่องคอมพิวเตอร์ ทำการปัดเศษสตางค์จากบัญชีผู้อื่นจำนวนมากมาเข้าบัญชีปลอม เพื่อจะได้ถอนเอาออกมาเป็นของตน หรืออาจเป็นการปัดเศษเล็กน้อยของทรัพย์สินชนิดอื่นแทนที่จะเป็นเงินก็ได้ ตัวอย่างของวิธีการเหล่านี้ เช่น การฉ้อฉลด้วยการปัดเศษลง (Round down fraud) ซึ่งในการคำนวนดอกเบี้ยให้แก่ลูกค้าของธนาคารนั้น แทนที่จำนวนเงินที่เครื่องคอมพิวเตอร์บันทึกไว้ซึ่งมีเศษทศนิยมเกินกว่า 0.05 หรือ 5 สตางค์ จะถูกปัดเศษขึ้น (Round up) และเศษทศนิยมที่ต่ำกว่า 0.05 หรือ 5 สตางค์จะถูกปัดเศษลง (round down) โปรแกรมคอมพิวเตอร์จะสั่งให้ปัดเศษลงเสมอ ไม่ว่าจะเกินหรือต่ำกว่า 5 สตางค์ และเศษสตางค์ที่ถูกปัดออกนั้นก็จะถูกสั่งให้โอนไปเข้าบัญชีปลอมของผู้สร้างโปรแกรม ซึ่งจะถูกถอนเงินออกไปในภายหลัง

มีตัวอย่างคดีหนึ่งผู้ฉ้อฉลได้เปิดบัญชีในชื่อของ Zwana และโปรแกรมคอมพิวเตอร์ได้ถูกกำหนดให้โอนจำนวนเศษเล็ก ๆ น้อย ของบัญชีลูกค้าทั้งหมด ตั้งแต่บัญชีแรกจนถึงบัญชีสุดท้าย การฉ้อฉลถูกสืบพบโดยการตรวจสอบการหักจำนวนของบัญชีลูกค้า ตั้งแต่บัญชีแรกจนถึงบัญชีสุดท้ายตามลำดับอักษร[12]

11.US. Department of Justice, Computer Crime:Criminal Justice Resource Manual, p.19

12.Martin Wasik, Ibid., p.50

หัวข้อการฉ้อฉลคอมพิวเตอร์ต่างๆ ที่เกิดขึ้น ได้มีการรายงานเกี่ยวกับคดีของประเทศอังกฤษในปี ค.ศ. 1987 นักบัญชีและวิเคราะห์ระบบได้จัดทำแผนงานบริษัท ซึ่งได้มีการพัฒนาโปรแกรมสำเร็จรูป (Software package) โดยมีเป้าหมายอยู่ที่ร้าน วี ดี โอ (VDO) โดยซอฟต์แวร์ดังกล่าว จะให้ระบบแก่ร้านค้าในการบันทึกสถิติ การติดตามการเช่าวีดีโอ และรายได้ที่ให้เช่า ภายในโปรแกรมจะถูกซ่อนไว้โดยโปรแกรมส่วนปะหรือส่วนเขียนเพิ่มเติมขึ้น (Patch) ซึ่งเมื่อทำงานโดยการใส่รหัสผ่านเข้าไป จะมีการบกพร่องส่วนรายได้ของเจ้าของร้านในแต่ละวัน ทั้งนี้เพื่อจุดประสงค์ในการหลีกเลี่ยงภาษีมูลค่าเพิ่มให้ต้องชำระให้ลดน้อยลง ซอฟต์แวร์ชนิดนี้ได้ถูกขายไปกว่า 120 ชิ้น แต่มีเพียง 20 ชิ้นเท่านั้นที่ถูกกำหนดให้มีการฉ้อฉล เป็นผลให้มีการจ่ายภาษีน้อยกว่าจำนวนที่แท้จริงถึง 100,000 ปอนด์

ส่วนวัตถุประสงค์ของการฉ้อฉลในขั้นตอนการออกหรือการแสดงผล อาจจะต้องการที่จะบิดเบือนข้อมูลบางประการ เพื่อที่จะกระทำความผิดหรือบกพร่องการกระทำความผิด หรืออาจจะเป็นการขโมยข้อมูลที่เกี่ยวกับคอมพิวเตอร์ โดยทั่วไปการกระทำความผิดในขั้นตอนนี้ขึ้นอยู่กับการนำข้อมูลเข้า การฉ้อฉลโดยการนำข้อมูลออกตลอด โดยไม่เกี่ยวกับการนำข้อมูลเข้าเลยนั้นมีน้อย ในหลาย ๆ คดีการกระทำของจำเลยจะกระทำโดยการนำข้อมูลเข้าก่อน อันเป็นการนำไปสู่สาเหตุของการที่คอมพิวเตอร์ปฏิบัติการตามที่ใส่ข้อมูล และแสดงผลออกมาตามความประสงค์ของผู้ทำการฉ้อฉล

3.1.3 การคัดลอกข้อมูลหรือโปรแกรมโดยปราศจากอำนาจ (Unauthorized Remove of Data or Program)

ข้อมูลหรือโปรแกรมซึ่งอยู่ในรูปแบบที่ไม่สามารถจับต้องได้ สามารถที่จะถูกนำมาและใช้โดยบุคคลใดก็ตามผู้ซึ่ง ได้รับประโยชน์จากการเข้าถึงหน่วยความจำโดยมิได้ทำให้สิ่งใดลดน้อยลงไป ไม่ว่าจะโดยวิธีการถ่ายภาพหรือวิธีการบันทึก ซึ่งในแต่ละวิธีการผู้กระทำมิได้ประสงค์ที่จะแทรกแซงตัวเนื้อหาแต่อย่างใด ไม่ว่าจะด้วยสื่อกลางภายในหรือต่อข้อมูลที่ถูกเก็บสะสมอยู่นี้

เป็นวัตถุประสงค์หลักของผู้กระทำในการจารกรรมข้อมูลซึ่งเป็นความลับของอุตสาหกรรมการเงินหรือประวัติของบุคคลากร ซึ่งผู้กระทำผิดในรูปนี้ปรารถนาที่จะให้บริษัทหรือผู้ที่ตกเป็นเหยื่อที่ละเลยไม่ให้ความใจต่อความปลอดภัยของข้อมูล ได้รับความเสียหายนานเท่าที่จะเป็นไปได้

การเก็บสะสมข้อมูลที่เพิ่มขึ้นเรื่อย ๆ ซึ่งมีมูลค่าทางเศรษฐกิจจำนวนมหาศาลที่ถูกเก็บอยู่ในคอมพิวเตอร์ การจารกรรมข้อมูลหรือโปรแกรมเกี่ยวกับคอมพิวเตอร์ อาจจะสร้างผลกำไรเป็นจำนวนมากแก่ผู้ที่ทำการจารกรรม ในการที่จะนำไปใช้พัฒนาวิจัยหรือข้อมูลสินค้า ดังนั้นจึงมีความจำเป็นที่จะต้องรักษาข้อมูลเหล่านั้น โดยการวางมาตรการความปลอดภัยให้เหมาะสม ทั้งความปลอดภัยทางกายภาพและควบคุมการเข้าถึงคอมพิวเตอร์ เช่นการใช้รหัสผ่านและรหัสประจำตัวผู้ใช้

ในปี คศ.1982 คณะกรรมาธิการความมั่นคงของอังกฤษได้เสนอรายงานต่อรัฐบาล โดยได้แจ้งถึงความเสี่ยงภัยและเสนอแนะว่า

"ปริมาณข้อมูลจำนวนมากนั้น สามารถที่จะถูกเก็บในแผ่นดิสก์หรือเทปแม่เหล็กเพียงชิ้นเดียวและสามารถเข้าถึงได้อย่างรวดเร็ว ซึ่งข้อมูลก็สามารถที่จะถูกเรียกคืนมาใช้ได้ นั้นย่อมหมายความว่าหากมีความอ่อนแอใด ๆ ในการเข้าถึงข้อมูลที่ถูกจัดเก็บในคอมพิวเตอร์หรือเครื่องประมวลผล (Word processor) ย่อมอาจจะก่อให้เกิดความหายนะอย่างใหญ่หลวงในประเทศ แน่นอนว่าในส่วนหนึ่งย่อมมีผลกระทบต่อการทำงานด้านข่าวกรองด้วย"[13]

การเข้าถึงข้อมูลโดยปราศจากอำนาจได้ มีหลายวิธีซึ่งอาจจะโดยการอ่านจากจอภาพที่เชื่อมกับคอมพิวเตอร์ซึ่งเป็นตัวเก็บข้อมูล ไม่ว่าจะโดยการที่บุคคลนั้นได้เข้าถึงในตัวคอมพิวเตอร์นั้นเองหรือโดยการแอบซ่อนอุปกรณ์การดักฟัง หรือจะเป็นกล้องถ่ายภาพที่สามารถทำงานระยะไกลได้

เหตุผลโดยทั่วไปของการจารกรรมเป็นเรื่องเกี่ยวกับข้อมูลอุตสาหกรรม รวมถึงการ

13.Home Office, Statement on Recommention of the Security Commission,(London:HMSO , 1982),P.12.

ฉ้อฉล(Corruption) หรือรีดไถ่ (blackmail) ของลูกจ้าง การแทรกซึมของลูกจ้างของบริษัทคู่แข่งเข้าไปในบริษัทอื่น ในช่วงระยะเวลาสั้น ๆ (the hello-Goodbye method) และสอบถามทั้งอย่างเป็นทางการหรือไม่เป็นทางการ หรือสร้างความสนิทสนมกับคนงานคนสำคัญในบริษัทคู่แข่ง เพื่อที่จะดึงดูดข้อมูลเกี่ยวกับการวิจัยและการพัฒนา ซึ่งอาจจะเป็นการชั่วคราวเกี่ยวกับการคัดลอกแผ่นดิสก์หรือเทปที่เก็บข้อมูล เพื่อที่จะนำไปคัดลอกและนำมาคืนหลังจากข้อมูลนั้นได้ถูกคัดลอกเรียบร้อยแล้ว

ข้อมูลที่บรรจุในคอมพิวเตอร์บางอย่างหรือในบางโปรแกรมคอมพิวเตอร์ อาจจะมีมูลค่าเป็นจำนวนมหาศาล เป็นสินค้าที่มีราคาแพง ต้องใช้เวลาจำนวนมากในการที่จะวิจัยและต้องใช้ความพยายามสูงในการที่จะกำหนดขึ้นมา

ตามรายงานของคณะกรรมาธิการแก้ไขกฎหมายของอังกฤษ(the Audit commission) ในปี 1987 พบว่าในคดีหนึ่งนักคอมพิวเตอร์ ซึ่งตามสัญญาเขามีอำนาจที่จะเข้าถึงระบบคอมพิวเตอร์เวลาได้ใช้อภิสิทธิ์เอาเทปคอมพิวเตอร์ ออกไปจากที่ทำงานและทำการคัดลอกเทปคอมพิวเตอร์ที่บรรจุข้อมูลต่าง ๆ ของบริษัทไว้ ซึ่งการคัดลอกนี้ได้ปรากฏเรื่องขึ้นมาเมื่อเขาได้เสนอที่จะขายสิ่งที่คัดลอกนี้ต่อนายจ้างใหม่ของเขา

ในอีกคดีหนึ่ง นักปฏิบัติการคอมพิวเตอร์ซึ่งได้ลาออกจากงานและได้นำเทปแม่เหล็กซึ่งตนได้คัดลอกโปรแกรมที่ใช้ประโยชน์จำนวนมากออกมาด้วย ซึ่งตนคิดว่าตนอาจจะได้รับความไว้วางใจจากนายจ้างคนใหม่ของเขา

ซึ่งปัญหาการลักลอบคัดลอกโปรแกรมคอมพิวเตอร์ ทางธุรกิจเป็นสิ่งที่ต้องให้ความสำคัญมากเป็นพิเศษ ในตลาดซอฟต์แวร์ของยุโรปตะวันตกถูกประเมินว่า มีการสั่งซื้อประมาณ 1 หมื่นล้านปอนด์ต่อปี[14] และมีการประมาณว่าบางทีมีการสูญเสีย รายได้ถึง 1 พันล้านปอนด์ เนื่องจากการลักลอบคัดลอกหมุนเวียนกันในองค์การธุรกิจ เนื่องจากการคัดลอกเป็นสิ่งที่สามารถกระทำได้ง่าย ผู้ใช้ส่วนมากจะมีเครื่องคัดลอกที่ติดอยู่ในอุปกรณ์ฮาร์ดแวร์ของเครื่องคอมพิวเตอร์อยู่แล้ว การคัดลอกซอฟต์แวร์ในครั้งแรกจะถูกซื้อมา และหลังจากนั้นตัวสำเนานั้นก็จะถูกแบ่งเป็น 10 หรือ

14.Martin Wasik, Ibid., p.53

บางทีอาจเป็นจำนวนร้อย ที่จะถูกบรรจุลงในเครื่องคอมพิวเตอร์บุคคล (PC) ภายในบริษัทนั้น กฎหมายสิบสิทธิ์จึงเป็นที่ชัดเจนว่าเป็นสิ่งที่มีความสำคัญมากต่อกรณีนี้

มีคดีหนึ่งซึ่งมีการกล่าวหากันอย่างรุนแรงมาก เกิดขึ้นในปี คศ. 1989 โดยกลุ่มของประเทศเยอรมันตะวันตก ซึ่งนักคอมพิวเตอร์ของเขาและขณะเดียวกันก็เป็นนักจารกรรมด้วย ได้เข้าถึงข้อมูลเป็นความลับระดับสูง เกี่ยวกับการวิจัยนิวเคลียร์และการป้องกันประเทศในยุโรป สหรัฐ และญี่ปุ่น ในการใช้เครือข่ายคอมพิวเตอร์ทางการทหาร (Milnet) ซึ่งเป็นข่ายงานคอมพิวเเตอร์ที่เชื่อมกันเกี่ยวกับการป้องกันประเทศ การทดลองและที่ตั้งของกองทัพ ข้อมูลเหล่านี้เป็นที่แน่ชัดว่าต่อมามีการขายให้กับ หน่วย เค จี บี (KGB) ในช่วงเวลากว่า 4 ปี โดยได้รับเงินและยาเสพติดเป็นค่าตอบแทน และมีการรายงานว่าเคจีบี เตรียมที่จะจ่ายเงินจำนวนมากสำหรับข้อมูลเกี่ยวกับรหัสผ่านและระบบรักษาความปลอดภัย ข้อมูลเกี่ยวกับโครงสร้างชิลิคอนชิพ ซอฟต์แวร์ และรายชื่อข้อมูลเกี่ยวกับทหารและโครงการวิทยาศาสตร์ การกระทำผิดที่ปรากฏออกมาโดยบังเอิญ เมื่อนายคลิฟฟอร์ด สโทล นักวิทยาศาสตร์ของมหาวิทยาลัย ฮาร์ดวาร์ด และทำงานด้านความปลอดภัยเกี่ยวกับคอมพิวเตอร์ ในซานฟรานซิสโก สหรัฐอเมริกา ด้วยได้สังเกตุถึงความไม่ตรงกันของบัญชีการใช้เวลาของคอมพิวเตอร์ (time-sharing bill) และได้พิจารณาถึงเวลาและพลังงานเพื่อที่จะติดตามผู้กระทำความผิด จำเลยถูกฟ้องด้วยข้อหาที่รุนแรงมาก รวมถึงการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งประเทศเยอรมันตะวันตกใช้เป็นกฎหมายตั้งแต่ปี 1985 หนึ่งในผู้ร่วมกระทำผิดได้ฆ่าตัวตายก่อนที่จะได้เริ่มมีการสอบสวน ซึ่งการเริ่มสอบสวนได้เริ่มขึ้นเมื่อต้นปี คศ.1990

3.1.4. การใช้เวลาหรือบริการทางคอมพิวเตอร์โดยปราศจากอำนาจ(Unauthorized Use of Computer or Facilities)

บ่อยครั้งที่ต้องเผชิญรูปแบบการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ในการเข้าถึงคอมพิวเตอร์เพื่อที่จะใช้ประโยชน์จากเวลาคอมพิวเตอร์หรือความสะดวก ซึ่งผู้ที่เข้าถึงนั้นไม่มีสิทธิ์ การกระทำ

ความผิดเช่นนี้บ่อยครั้งที่รู้จักในฐานของ "ขโมยบริการ" (theft of services) หรือ "ขโมยเวลา"(time-theft) การกระทำผิดอาจจะทำโดยผู้ซึ่งมีอำนาจใช้คอมพิวเตอร์ แต่ไปใช้ในเวลาอื่นหรือจุดประสงค์อย่างอื่น หรือโดยบุคคลภายนอก

มีหลายคดีซึ่งได้รับการเปิดเผยถึงการกระทำผิดเนื่องจากความอยากรู้อยากเห็น และบ่อยครั้งที่เป็นนักศึกษาในมหาวิทยาลัย ทั้งนี้เพื่อประสงค์ที่จะเรียนรู้เกี่ยวกับวิธีการใช้คอมพิวเตอร์ เดี๋ยวนี้มีแนวโน้มเป็นจำนวนมากว่าลูกจ้างของบริษัทต่าง ๆ จะเข้ามาเกี่ยวข้องกับการใช้คอมพิวเตอร์ของนายจ้างของเขา เพื่อวัตถุประสงค์อื่น ๆ มากกว่างานที่เขารับผิดชอบ

ระบบการทำงานร่วมกันโดยผู้ใช้หลาย ๆ คนในเวลาเดียวกัน (Multi-user) เป็นเป้าหมายสำหรับการใช้โดยบราศจากอำนาจ ไม่ว่าผู้ใช้จะมีอำนาจใช้แต่ได้ใช้เกินสิทธิของเขา หรือผู้ใช้โดยบราศจากอำนาจปลอมตัวเป็นผู้มีอำนาจใช้ การกระทำผิดรูปแบบนี้ค่อนข้างจะมีความสำคัญน้อย ในฐานะที่ซึ่งลูกจ้างใช้คอมพิวเตอร์ของนายจ้างเล่นเกมส์คอมพิวเตอร์ หรือออกแบบโปรแกรมเพื่อตัวเขาเองแต่ใช้เวลาของบริษัท

ในคดีหนึ่งซึ่งได้รับความสนใจมาก คือ การที่นักโปรแกรมคอมพิวเตอร์ 2 คน ซึ่งเป็นลูกจ้างของบริษัท Speray - Univac รัฐฟิลาเดลเฟีย ได้ใช้คอมพิวเตอร์ของบริษัทในการทำงานธุรกิจเกี่ยวกับดนตรี ซึ่งเป็นงานส่วนตัวของเขาเอง โดยใช้เวลากว่า 3 ปีในการพัฒนาซอฟต์แวร์ดังกล่าว ให้มีลักษณะที่มีรูปแบบแตกต่างกันออกไป รวมถึงพิมพ์ซอฟต์แวร์นั้นออกมา โดยการกระทำดังกล่าวมีการประเมินว่า พวกเขาได้กระทำผิดคิดเป็นมูลค่า 144,000 เหรียญ โดยคำนวนจากการใช้เวลาคอมพิวเตอร์[15]

ในการสำรวจของคณะกรรมาธิการแก้ไขกฎหมายของอังกฤษในปี คศ.1984 มีจำนวน 17 คดี จาก 77 คดี ได้ถูกเปิดเผยว่าเกี่ยวข้องกับการกระทำผิดชนิดนี้ แต่ที่สำคัญมิได้ก่อให้เกิดความสูญเสียในจำนวนมาก แต่คณะกรรมธิการมีความรู้สึกว่ามันจะเป็นการที่สมควรเป็นอย่างยิ่งที่จะแนะนำว่า "ในอนาคตความเสี่ยงของการฉ้อฉลและการใช้ในทางที่ผิด เน้นการใช้ในทางที่ไม่ถูกต้องของคอมพิวเตอร์ ว่าการกระทำผิดมีแนวโน้มจากปัจจุบันว่าจะเป็นปัญหาที่สำคัญมากที่สุด

15.Martin Wasik, Ibid., p.55

สำหรับปัญหาที่จะต้องจัดการ" โดยคล้าย ๆ กันนี้ได้มีผู้เขียนเรื่อง "การสำรวจอาชญกรรมคอมพิวเตอร์" (The Computer Crime Survey) ของสำนักเนติบัณฑิตของอเมริกา (American Bar Association) ได้กล่าวถึงคดีที่เกี่ยวกับการขโมยใช้เครื่องคอมพิวเตอร์ ในฐานะที่เริ่มที่จะต้องเผชิญหน้าบ่อยครั้งขึ้น และได้ทำนายไว้ว่า ปัญหาดังกล่าวมีแนวโน้มที่จะขยายออกไปอย่างมากในอนาคต

3.1.5. การทำให้เกิดความเสียหายหรือทำลาย

การก่อให้เกิดความเสียหายหรือทำลายเกี่ยวกับคอมพิวเตอร์ ได้มีรายงานจำนวนมากแสดงให้เห็นถึงการติดตั้งเครื่องคอมพิวเตอร์นั้น จะเป็นเป้าหมายที่น่าสนใจและดึงดูด ในอันที่ผู้ไม่ประสงค์ดีต้องการที่จะแก้แค้น โดยการสร้างความเสียหายให้กับคอมพิวเตอร์ ซึ่งทั้งหมดนี้นักคอมพิวเตอร์ต่างเข้าใจดีถึงความเสียหายที่จะเกิดขึ้นกับฮาร์ดแวร์ โดยเฉพาะหากการกระทำนั้นจะเกิดขึ้นต่อโปรแกรมหรือข้อมูลที่ถูกเก็บอยู่ภายในเครื่องคอมพิวเตอร์

สถานที่แท้จริงและบางทีรูปแบบของการติดตั้งเป็นสิ่งสำคัญ ทั้งนี้เพราะนั้นหมายถึงสิ่งนั้นมีโอกาสที่จะเป็นจุดมุ่งหมายของการกระทำผิด และรวมถึงการก่อการร้ายในรูปแบบอื่น ๆ เจตนาที่จะทำให้เกิดความเสียหาย อาจจะถูกกระทำโดยลูกจ้างในฐานะที่เป็นรูปแบบหนึ่งของการแก้แค้น ซึ่งนิตยสาร Extremist Europian[16] ได้แนะนำถึงวิธีการหลาย ๆ อย่าง ที่สามารถก่อให้เกิดความเสียหายแก่คอมพิวเตอร์ได้ ทั้งนี้เพื่อประสงค์ที่จะให้ใช้ในการติดตามเกี่ยวกับความขัดแย้งเกี่ยวกับแรงงานภายในบริษัท โดยวิธีการดังกล่าว เช่น การราดน้ำเกลือหรือน้ำยาที่ใช้ทำความสะอาด ซึ่งมีคุณสมบัติที่กัดอย่างด่างผสมอยู่เข้าไปในส่วนประกอบของคอมพิวเตอร์ พ่นควันบุหรี่หรือสเปรย์ฉีดผมเข้าไปภายใน วางภาชนะซึ่งบรรจุกรดไฮโดรคลอลิคไว้หน้าช่องเครื่องปรับอากาศ รบกวนสายส่งกำลังไฟฟ้า และแม้แต่เอาหนูมาไว้ในห้องซึ่งสามารถที่จะกัดแทะสายไฟฟ้าได้

สถาบัน Stanford Research ได้ทำการศึกษาในปี คศ.1975 พบว่ามีไม่น้อยกว่า 66

16.Martin Wasik, Ibid., p.57

คดี ที่เกิดขึ้นจากการรายงานของนักข่าวอเมริกันและที่อื่น ๆ อีก ถึงการก่อให้เกิดความเสียหายที่เกิดขึ้นทางกายภาพต่อคอมพิวเตอร์ ทั้งนี้รวมถึง 4 คดี ที่เกิดขึ้นโดยเจ้าหน้าที่ผู้ปฏิบัติงานเกี่ยวกับเครื่องคอมพิวเตอร์นั้นเองได้ใช้ปืนยิงเครื่องคอมพิวเตอร์ เนื่องจากไม่พอใจนายจ้างของเขา

นักศึกษาซึ่งสร้างความวุ่นวายในสหรัฐอเมริกาในช่วงเกิดสงครามเวียดนาม เป็นผลให้มีได้ก่อให้เกิดความเสียหายแก่ศูนย์คอมพิวเตอร์หลายแห่ง และต่อมาในช่วงเวลาสิ้นสุดทศวรรษที่ 1970 สู่ ทศวรรษที่ 1980 ได้มีผู้ก่อการร้ายมีชื่อว่า the Red Brigade ได้เข้ามาสร้างความเสียหายต่อคอมพิวเตอร์ในประเทศอิตาลี และในประเทศฝรั่งเศสซึ่งจนกระทั่งบัดนี้ก็ยังไม่ทราบถึงกลุ่มผู้ก่อการร้ายว่าเป็นกลุ่มใด และในปี 1983 ได้มีการวางระเบิดโจมตีศูนย์คอมพิวเตอร์ของประเทศเยอรมันตะวันตก การกระทำนี้กระทำโดยกลุ่มผู้ประท้วงต่อต้านการเข้าร่วมของบริษัทคอมพิวเตอร์ในการผลิตอาวุธนิวเคลียร์ ในปี 1988 ที่ชานฟรานซิสโก ผู้หญิงคนหนึ่งซึ่งถูกแถลงข่าวต่อนักข่าวว่าเป็นบุคคลหนึ่งในกลุ่มซึ่งเรียกตนเองว่า "กลุ่มสันติภาพ" ซึ่งต่อมาผู้หญิงคนนี้ก็ถูกพิพากษาจำคุก 5 ปี และให้ชดใช้เงิน 500,000 ดอลล่าร์ ภายหลังจากก่อให้เกิดความเสียหายแก่ระบบคอมพิวเตอร์ที่ซึ่งเธอเชื่อว่า เป็นสถานที่จะปล่อยอาวุธนิวเคลียร์

จากเหตุการณ์ข้างต้นได้ชี้ให้เห็นถึงสถานการณ์ที่เกิดขึ้นที่ได้ก่อให้เกิดความเสียหาย หรือการทำลายคอมพิวเตอร์ทางกายภาพ ซึ่งในขณะที่บางประเทศได้มีการปรับปรุงกฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์ ซึ่งเป็นกฎหมายที่ใช้ในการปราบปรามการกระทำความผิดขึ้นมา โดยเฉพาะในอันที่เกี่ยวกับการติดตั้งเครื่องคอมพิวเตอร์หรือตัวฮาร์ดแวร์ ซึ่งสิ่งเหล่านี้ดูเหมือนว่ามันมิใช่สิ่งที่จำเป็น เพราะโดยทั่ว ๆ ไป ก็สามารถที่ประยุกต์ใช้ได้กับกฎหมายที่มีอยู่แล้ว แต่อย่างไรก็ตามการพัฒนาเหล่านี้บางทีอาจจะมีผลสะท้อนอย่างรุนแรงเกี่ยวกับความเห็นว่า ความสำคัญของคอมพิวเตอร์อันเป็นสิ่งที่ยั่วยวนในการประกอบอาชญากรรม และกฎหมายอาญาที่เกี่ยวกับคอมพิวเตอร์โดยเฉพาะ เป็นสิ่งที่จำเป็นอย่างยิ่งที่จะกำหนดผลที่ออกมาให้แตกต่างกันเป็นพิเศษ

การก่อให้เกิดความเสียหายหรือการทำลายทางคอมพิวเตอร์ อีกรูปแบบหนึ่ง คือ การกระทำต่อสิ่งที่เรียกว่า "ข้อมูล"หรือ"โปรแกรม" คอมพิวเตอร์ ซึ่งความเสียหายที่กระทำต่อสิ่ง

เหล่านี้ไม่สามารถที่จะรู้เห็นได้ทางกายภาพ และโดยเฉพาะสิ่งที่เกิดขึ้นเหล่านี้เป็นการกระทำของโปรแกรมไวรัสคอมพิวเตอร์ (Computer Virus) ซึ่งเป็นวัตถุประสงค์ของการทำวิจัยฉบับนี้

มันเป็นสิ่งที่ยากมากในคดีที่ชี้รูปแบบของความเสียหาย ที่ได้สร้างความเสียหายขึ้นกับโปรแกรมคอมพิวเตอร์หรือข้อมูล มีคดีเป็นจำนวนมากที่เกิดขึ้น เช่น โปรแกรมได้ถูกลบทิ้งโดยเจตนา หรือใช้แม่เหล็กในอันที่จะลบข้อมูลออกจากเทปคอมพิวเตอร์ ในบางครั้งก็เพื่อเหตุผลทางการเมือง บางครั้งก็อาจจะมาจากการโกรธแค้นของลูกจ้าง ในกรณีอื่นอาจมีการโยกย้ายหรือทำลายข้อมูลที่ถูกเก็บไว้โดยอุปกรณ์ปลายทางระยะไกล บางครั้งก็เกิดจากผู้มีความคิดแปลก ๆ หรือเหตุผลทางธุรกิจ ความมีจุดบกพร่องของอุตสาหกรรมที่จะถูกรบกวนได้ง่ายทางคอมพิวเตอร์ในการที่จะคุกคามจากการฉ้อฉลเกี่ยวกับโปรแกรมหรือข้อมูลเป็นไปได้มาก

วิธีธรรมดาซึ่งเป็นสาเหตุของความเสียหายคือโดยการใส่โปรแกรมซึ่งเมื่อใส่เข้าไปแล้วจะทำให้เครื่องคอมพิวเตอร์หยุดทำงาน(Crash program) หรือพวกโลจิกบอมบ์ (Logic Bomb) ซึ่งสามารถที่จะลบข้อมูลได้จำนวนมากในเวลาอันสั้น หรือโปรแกรมที่ใส่เข้าไปครั้งหนึ่งและอาจจะปฏิบัติการในเวลาต่อมาหลังจากที่ผู้กระทำผิดได้ออกจากงานไปแล้ว

ความหลากหลายของการกระทำผิดได้มีการพัฒนาขึ้น โปรแกรม"มะเร็งหรือไวรัสคอมพิวเตอร์" ได้ถูกสร้างขึ้นและใส่เข้าไปในเครือข่ายคอมพิวเตอร์โดยมีเจตนาที่จะก่อให้เกิดความเสียหายหรือทำลายข้อมูลหรือโปรแกรมคอมพิวเตอร์ โดยขณะนั้นได้มีความคิดว่ามันเป็นไปได้ที่ไวรัสคอมพิวเตอร์เกิดขึ้นมาจากคำสั่งต่าง ๆ ในโปรแกรมที่ผู้เขียนโปรแกรมเขียนขึ้น หลักฐานกรณีนี้เป็นไปได้น้อยมาก แต่มันเป็นที่ชัดเจนว่าจริง ๆ แล้วไวรัสคอมพิวเตอร์ถูกสร้างขึ้นมาโดยเจตนาที่ชั่วร้าย

โปรแกรมไวรัสคอมพิวเตอร์เป็นที่รู้จักในอเมริกาตั้งแต่ต้นทศวรรษที่ 1980 แต่ปัจจุบันได้แพร่ไปทั่วโลก เพราะเมื่อใส่เข้าไปในคอมพิวเตอร์จะมีการสร้างตัวมันเองขึ้นมาใหม่ อันจะทำให้เกิดความเสียหายแก่โปรแกรมหรือไฟล์ข้อมูลอื่น ๆ การติดเชื้ออาจจะโดยการใช้แผ่นดิสก์ซึ่งติดเชื้อไวรัสคอมพิวเตอร์เรียบร้อยแล้ว หรือโดยการเชื่อมกันทางการสื่อสารทางคอมพิวเตอร์ ถ้าการรักษาความปลอดภัยถูกปล่อยปละละเลยทำให้ไวรัสคอมพิวเตอร์ผ่านเข้าไปในเครื่องคอมพิวเตอร์ซึ่ง

อาจจะมีการโอนมาจากเครื่องคอมพิวเตอร์อื่นโดยวิธีตามสาย ซึ่งผลกระทบที่คล้าย ๆ กันนี้คือ หนอนคอมพิวเตอร์ (worm) ซึ่งเมื่อถูกใส่เข้าไปจะมีการถอดแบบด้วยตัวมันเองอย่างรวดเร็ว บรรจุจนเต็มหน่วยความจำด้วยแฟ้มข้อมูลที่ไม่ต้องการ เพื่อว่าเครื่องคอมพิวเตอร์จะหยุดการทำงานเนื่องจากหน่วยความจำหมดพื้นที่ความจำ และแน่นอนว่าที่ซึ่งคอมพิวเตอร์มีการเชื่อมโยงกันโดยทางสายโทรศัพท์ มันอาจจะเข้ามาจากที่ใด ๆ ในโลกก็ได้

ในระหว่างปี 1988 ไวรัสคอมพิวเตอร์ที่รู้จักในชื่อของ Amigo ถูกพบโดยการพิจารณาจากความเสียหายต่อการจัดเก็บผลงานวิจัยต่าง ๆ มหาวิทยาลัยฮิบรูจในเจรูซาเล็มสหรัฐอเมริกา ไวรัสคอมพิวเตอร์ชื่อ "Lehigh" ซึ่งเกิดขึ้นมาจากมหาวิทยาลัยเพนซิลวาเนีย ได้ทำลายแฟ้มข้อมูลไปเป็นจำนวนมาก โดยการขยายตัวมันเองโดยทางแฟ้มที่มีชื่อเฉพาะในคอมพิวเตอร์บุคคล (PC) ไวรัสถูกกำหนดให้ซ่อนอยู่ในแฟ้ม ซึ่งจะถูกเรียกมาใช้บ่อย โดยไวรัสจะติดต่อไปทุกครั้งที่เรียกมันมาใช้ เมื่อแผ่นดิสก์ถูกนำมาใส่ในคอมพิวเตอร์เครื่องอื่น ๆ เชื้อจะถูกติดแพร่ขยายออกไปด้วยและในปี 1988 หนอนคอมพิวเตอร์ (worm) ก็เป็นที่รู้จักกันโดยทั่วไป โดยการที่นักศึกษาบริญญาโทมหาวิทยาลัยเคอร์เนล เป็นผลให้ติดไปสู่เครื่องคอมพิวเตอร์ Arpanet (Advanced Research Project Agency) ซึ่งเป็นระบบที่มีการทำงานโดยกระทรวงกลาโหมที่เพนตากอน (Pentagon) โดยไวรัสคอมพิวเตอร์ชนิดนี้ ถูกส่งจากคอมพิวเตอร์เครื่องหนึ่งไปสู่คอมพิวเตอร์เครื่องอื่น ๆ โปรแกรมอันตรายนี้ถูกค้นพบโดยนักวิทยาศาสตร์ ซึ่งทำงานวิจัยอาวุธนิวเคลียร์ในห้องทดลอง ในคาลิฟลอเนีย ผู้ซึ่งได้สังเกตุความผิดปกติอย่างมากในการใช้ระบบคอมพิวเตอร์ ซึ่งจากการกระทำครั้งนี้เป็นผลให้คอมพิวเตอร์กว่า 6,000 เครื่องได้รับความเสียหายหยุดการทำงานและจะเป็นสิ่งที่เลวร้ายยิ่งจากการที่หนังสือพิมพ์ New York Time รายงานว่าคอมพิวเตอร์จำนวนกว่า 60,000 เครื่อง ที่เชื่อมโยงกับข่ายงานของกระทรวงกลาโหม มีความเสี่ยงที่จะติดโปรแกรมดังกล่าว

การป้องกันที่มีประสิทธิภาพมากที่สุดต่อกรณีไวรัสคอมพิวเตอร์คือ การรักษาความปลอดภัยโดยการป้องกันการเข้าถึงโดยปราศจากอำนาจ โดยเฉพาะการใช้ซอฟต์แวร์ที่ไม่รู้หรือที่มีความน่าสงสัยครั้งหนึ่ง ไวรัสหรือหนอนคอมพิวเตอร์ที่ถูกนำมาใส่ไว้ในคอมพิวเตอร์ซึ่งยากมากที่จะกำจัดมัน แต่ปัจจุบันมีแนวโน้มของการที่ผู้เชี่ยวชาญได้คิดค้นโปรแกรมที่เขียนขึ้นมาโดยเฉพาะในการที่จะตรวจสอบและกำจัดไวรัสคอมพิวเตอร์มากขึ้น และยังมีโปรแกรมสำเร็จรูปที่มีชื่อโดยทั่วไปว่า เป็น "วัคซีน" ซึ่งสามารถที่จะช่วยดูแลคอมพิวเตอร์โดยการตรวจและกำจัดโปรแกรมไวรัสที่อยู่ในระบบ แต่วิธีการเหล่านี้มิได้มีประสิทธิภาพอย่างเด็ดขาดทั้งหมด ทั้งนี้เพราะไวรัสคอมพิวเตอร์เป็นโปรแกรมชนิดหนึ่งซึ่งผู้สร้างสามารถที่จะพัฒนาให้มีความซับซ้อน หลบหลีกการตรวจสอบของโปรแกรมที่เขียนขึ้นมาตรวจสอบโดยเฉพาะได้ และในปัจจุบันก็ไม่พบว่าจะมีโปรแกรมใดที่สามารถที่จะตรวจสอบและกำจัดไวรัสคอมพิวเตอร์ทุกชนิดได้

3.2 <u>ไวรัสคอมพิวเตอร์กับการทำให้เกิดความเสียหายหรือทำลายทรัพย์สินทางอาญา</u>

ความผิดฐานทำให้เกิดความเสียหายหรือทำลายทรัพย์สิน ย่อมบัญญัติอยู่ในกฎหมายของทุกประเทศ แต่ขอบเขตของความผิดฐานนี้จะกว้างหรือแคบเพียงใดขึ้นอยู่กับคำนิยามของกฎหมายประเทศนั้น

ในการวิจัยส่วนนี้จะแสดงให้เห็นถึงปัญหาของกฎหมายอาญาที่จะนำมาปรับใช้กับปัญหาของไวรัสคอมพิวเตอร์ของต่างประเทศ ก่อนที่ประเทศเหล่านี้จะมีกฎหมายอาญาเกี่ยวกับคอมพิวเตอร์ออกบังคับใช้ ในความผิดฐานทำให้เกิดความเสียหายหรือทำลายทรัพย์สินในปัญหาเหล่านี้ โดยจะแบ่งออกเป็น 2 ส่วน คือ ความหมายของ "ความเสียหายหรือทำลายทางอาญา" กับความหมายของคำว่า "ทรัพย์สิน"

ซึ่งโดยแท้จริงแล้วทั้ง 2 ส่วนจะต้องไปด้วยกัน แต่เนื่องจากคำทั้ง 2 นี้ มีความหมายที่สำคัญในอันที่จะกำหนดได้ว่า การกระทำใดเป็นความผิดฐานทำให้เกิดความเสียหายหรือทำลายต่อทรัพย์สินหรือไม่

3.2.1 ความเสียหายหรือทำลายจากการกระทำของไวรัสคอมพิวเตอร์กับความเสียหายหรือทำลายทางอาญา

โปรแกรมไวรัสคอมพิวเตอร์ทุกชนิดล้วนแต่ก่อให้เกิดความเสียหาย ซึ่งรูปแบบของการก่อให้เกิดความเสียหายที่เกิดขึ้น ขึ้นอยู่กับผู้เขียนโปรแกรมว่าประสงค์จะให้เกิดความเสียหายในรูปแบบใด เช่น ทำให้ไม่สามารถบันทึกข้อมูลลงไปได้ ทำการฟอร์แมตแผ่นดิสเก็ต หรือทำให้การทำงานของคอมพิวเตอร์ช้าลง เป็นต้น ความเสียหายหรือการทำลายโปรแกรมหรือข้อมูลนี้ เรียกได้ว่าเป็น "ความเสียหายทางคอมพิวเตอร์"

แต่ความเสียหายหรือการทำลายตามความหมายของกฎหมายอาญานั้น มีความหมายที่แตกต่างไปจากความเสียหายทางคอมพิวเตอร์ เพราะต้องขึ้นอยู่กับคำนิยามและเจตนารมย์ของกฎหมายว่าจะกำหนดให้มีขอบเขตเพียงใด

ปัญหาของการกระทำให้เกิดความเสียหายหรือทำลาย เกี่ยวกับคอมพิวเตอร์สามารถแบ่งปัญหาที่จะนำมาวิเคราะห์ได้ โดยแบ่งออกเป็น 2 ประเภทด้วยกัน คือ

1. การทำให้เสียหายหรือทำลายเกี่ยวกับตัวคอมพิวเตอร์เอง หรืออาจเรียกว่าเป็นการกระทำต่อทรัพย์สินที่สามารถจับต้องได้ เช่น แผ่นดิสก์ เทป

2. การทำให้เกิดความเสียหาย ทำลาย หรือรบกวนต่อโปรแกรม หรือข้อมูลที่ถูกเก็บอยู่ในแผ่นดิสก์หรือเทป หรืออาจเรียกว่าเป็นการกระทำต่อทรัพย์สินซึ่งไม่อาจจับต้องได้

ในกรณีที่ก่อให้เกิดความเสียหายหรือทำลายในประการแรก ไม่มีปัญหาทางกฎหมายอาญาที่จะนำมาปรับใช้ แต่ในขณะที่ประการที่สองมีปัญหาที่สำคัญที่จะต้องพิจารณา เนื่องจากปัญหาเกี่ยวกับการนำกฎหมายมาปรับใช้ หรืออีกแง่หนึ่งเกี่ยวกับแนวความคิดของคำจำกัดความของคำว่า "ทรัพย์สิน" ต่อสิ่งซึ่งไม่สามารถจับต้องได้

3.2.1.1 ทรัพย์สินที่จับต้องได้ (Tangible Property)

ในตัวคอมพิวเตอร์มีหลายสิ่งหลายอย่างที่น่าสนใจ อันเป็นเป้าหมายของการกระทำผิดทางอาญา มีคดีซึ่งมีการบันทึกไว้ไม่ว่าจะเกี่ยวกับการตั้งองค์กรขึ้นมา ในกลุ่มของชาวยุโรปที่มุ่งจะทำลายศูนย์คอมพิวเตอร์ต่าง ๆ เช่น กลุ่ม Red Brigade ในประเทศอิตาลี และ CLODO ในประเทศฝรั่งเศส และการทำลายคอมพิวเตอร์โดยกลุ่มผู้ประท้วงต่อต้านสงครามเวียดนามในอเมริกา หรือบางทีอาจจะถูกสร้างความเสียหายโดยลูกจ้างที่โกรธแค้นนายจ้าง ซึ่งการทำให้เกิดความเสียหายหรือทำลาย มีวิธีการมากมายหลายรูปแบบ โดยมีความซับซ้อนมากน้อยต่างกัน

ปัญหาที่สำคัญที่มีการยกขึ้นพิจารณาเกี่ยวกับการเกิดความเสียหายทางกายภาพของคอมพิวเตอร์ และการดูแลรักษาของลูกจ้าง แต่อย่างไรก็ตามปัญหาดังกล่าวมิได้เป็นปัญหาสำคัญ เมื่อพิจารณาตามกฎหมายอาญาที่มีอยู่

ในประเทศอังกฤษมีการบัญญัติความผิดไว้ต่างหากโดยเฉพาะ ในการที่จะจัดการกับการทำให้เกิดการระเบิด และกฎหมายต่อต้านการก่อการร้าย และโดยทั่ว ๆ ไปแล้วมักจะตกอยู่ภายใต้บทบัญญัติของ the Criminal Damage Act 1971 ตามมาตรา (1) ซึ่งบัญญัติว่า

"ผู้ใดปราศจากอำนาจ ก่อให้เกิดความเสียหายหรือทำลายทรัพย์สินใด ๆ อันเป็นของผู้อื่น โดยมีเจตนาที่จะก่อให้เกิดความเสียหายหรือทำลายในทรัพย์สินนั้น หรือโดยไม่ไตร่ตรอง ไม่ว่าจะเป็นทรัพย์สินใด ถูกทำให้เกิดความเสียหายหรือทำลาย การกระทำเช่นนั้นเป็นความผิด"

และมาตรา 4 การกระทำความผิดตามมาตรานี้มีโทษจำคุกไม่เกิน 10 ปี ดังนั้นหากปรับใช้ตามกฎหมายนี้ จะเห็นได้ว่าเป็นการทำให้เกิดความเสียหายทางกายภาพโดยเจตนาต่อคอมพิวเตอร์ ซึ่งไม่น่าจะเป็นปัญหาที่จะนำกฎหมายนี้มาปรับใช้กับกรณีเช่นนี้

ซึ่งหากจะมีการออกกฎหมายใหม่ เพื่อที่จะมารองรับการกระทำในรูปแบบนี้ มันจะกลายเป็นสิ่งที่เกินความจำเป็น ในอันที่จะสร้างบทบัญญัติถึงความเสียหายทางอาญาขึ้นมาใหม่ ในความเสียหายทางกายภาพ เกี่ยวกับคอมพิวเตอร์ขึ้นมาโดยเฉพาะ

แต่อย่างไรก็ตามในบางมลรัฐของสหรัฐอเมริกา ก็ได้ออกกฎหมายมา เช่น ใน

มลรัฐแคลิฟอร์เนีย ตาม the California Penal Code มาตรา 502 บัญญัติว่า

"... ผู้ใดโดยเจตนา... ทำให้เกิดความเสียหายหรือทำลาย ระบบคอมพิวเตอร์ใดๆ ข่ายงานคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์หรือข้อมูล การกระทำเช่นนี้เป็นความผิด"

และนอกจากนี้ยังมีอีกหลายรัฐในอเมริกา ได้บัญญัติกฎหมายอาญาเกี่ยวกับคอมพิวเตอร์ เช่นเดียวกับแคลิฟอร์เนีย

3.2.1.2 ทรัพย์สินที่จับต้องไม่ได้ (Intangible Asset)

ไวรัสคอมพิวเตอร์เป็นโปรแกรมชนิดหนึ่ง ซึ่งก่อให้เกิดความเสียหายหรือทำลายโปรแกรมหรือข้อมูลอื่น ๆ ซึ่งโดยสภาพของตัวของไวรัสคอมพิวเตอร์เองแล้ว เป็นสิ่งซึ่งไม่สามารถมองเห็นได้ และรวมไปถึงความเสียหายที่เกิดขึ้นในการที่กระทำต่อโปรแกรมหรือข้อมูลอื่น ๆ ที่เก็บไว้ในคอมพิวเตอร์ ก็เป็นสิ่งที่ไม่สามารถมองเห็นได้ด้วยสายตาปกติ จึงเป็นการกระทำต่อทรัพย์สินไม่มีรูปร่างและซึ่งไม่อาจจับต้องได้ อันนำไปสู่ปัญหาทางกฎหมายว่า "ความเสียหายทางคอมพิวเตอร์" เช่นนี้ จะถือว่าเป็นความเสียหายทางอาญา" หรือไม่ เนื่องจากความเสียหายหรือการทำลายต่อสิ่งซึ่งเป็นสาระสำคัญในคอมพิวเตอร์เป็นสิ่งซึ่งไม่สามารถเห็นได้โดยทางกายภาพ

Smith และ Hogan ได้ให้ความหมายของ "การทำให้เกิดความเสียหายหรือทำลาย" ทางอาญาว่า หมายถึงการทำให้เกิดความเสียหายหรือทำให้เสวลงทางกายภาพ ซึ่งสามารถที่จะรับรู้ได้โดยความรู้สึก[17]

แต่อย่างไรก็ตามมันไม่แน่ชัดว่าจะต้องเกิดความเสียหายทางกายภาพเป็นจำนวนมากเท่าใดที่จะถือว่ามีความเสียหายเกิดขึ้น ในอดีตศาลเคยมีการตัดสินว่า ต้นหญ้าสามารถที่จะถูก

---

17. Matin Wasik, Crime and the Computer(Great Britain:Biddles Ltd ;,1991), p.139

ทำให้เกิดความเสียหายได้โดยการเหยียบย่ำ แต่ในปัจจุบันมิได้คิดไปไกลถึงขนาดนั้น เพียงแค่งอตะปูเหล็กยังถือไม่ได้ว่าเป็นความเสียหายทางอาญา[18]

มีคดีหนึ่งที่เกิดขึ้นในประเทศอังกฤษ คือคดี Cox V. Riley ซึ่งเป็นการกระทำของลูกจ้างที่ได้มีการเปลี่ยนแปลงโปรแกรมคอมพิวเตอร์จนเป็นเหตุให้เครื่องจักรมีการทำงานผิดพลาด ซึ่งคดีนี้แม้จะมิได้เป็นการก่อให้เกิดความเสียหายหรือทำลายโดยตรงจากโปรแกรมไวรัสคอมพิวเตอร์ แต่ก็สามารถที่จะสะท้อนให้เห็นถึงแนวความคิดต่าง ๆ ในความหมายของ "การทำให้เกิดความเสียหายหรือทำลายทางอาญา"

จำเลยเป็นลูกจ้างทำงานเกี่ยวกับการควบคุมคอมพิวเตอร์เพื่อการตัดสิ่งของ ซึ่งจำเป็นต้องอาศัยความแน่นอนในการทำงานต่อการตัดบัตรต่าง ๆ ที่ถูกสอดเข้าไป โปรแกรมที่บรรจุใช้งานอยู่มีความสามารถในการทำงาน โดยตัดได้อย่างเที่ยงตรงตามรูปแบบที่กำหนดไว้แตกต่างกัน จำเลยได้แก้ไขโปรแกรมโดยเจตนาที่จะให้มีการเว้นการตัดบัตร 1 ครั้งทุก ๆ 16 ครั้งที่โปรแกรมทำงาน เช่นนี้ทำให้การตัดไม่เป็นไปตามรูปแบบที่กำหนดไว้ปกติ และการทำงานก็ค่อนข้างจะมีการปฏิบัติการช้าลง

ซึ่งในที่สุดศาลก็พิพากษาว่า การกระทำเช่นนั้นเป็นความผิดเกี่ยวกับความเสียหายทางอาญาภายใต้ the Criminal Damage 1971 และตามรายงานของคณะกรรมาธิการกฎหมายในความผิดเกี่ยวกับคอมพิวเตอร์ของอังกฤษ กล่าวว่า

"การแทรกแซงใด ๆ ต่อการทำงานของคอมพิวเตอร์หรือซอฟต์แวร์ ซึ่งเป็นสาเหตุของการสูญเสียหรือไม่คล่องตัวในการทำงาน ต่อผู้มีอำนาจใช้ตามกฎหมาย ปัจจุบันสามารถที่จะถูกฟ้องในฐานทำให้เกิดความเสียหายทางอาญาได้... กฎหมายเกี่ยวกับความเสียหายทางอาญาปัจจุบัน ดูเหมือนจะมีการขยายไปถึงบุคคลผู้ซึ่งสร้างความเสียหายให้กับระบบคอมพิวเตอร์โดยปราศจากความจำเป็นที่จะต้องการให้มีการปฏิรูปกฎหมายขึ้นมาใหม่อีก"

จากรายงานฉบับนี้จะทำให้เห็นได้ว่า โปรแกรมหรือข้อมูลที่เก็บอยู่ในคอมพิวเตอร์

---

18. Ibid.

และต่อมาถูกทำให้เสียหายหรือทำลายโดยไวรัสคอมพิวเตอร์นั้น เมื่อพิจารณาจากคำพิพากษาในคดีของ Cox V. Riley ดูเหมือนจะเป็นการชี้ให้เห็นว่าไม่มีความจำเป็นที่จะต้องมีการแบ่งแยกกฎหมายออกไปสำหรับรูปแบบที่แตกต่างกัน เกี่ยวกับการกระทำความผิดที่ก่อให้เกิดความเสียหายต่อสาระสำคัญที่เก็บไว้ในคอมพิวเตอร์

อย่างไรก็ตาม ความเห็นดังกล่าวข้างต้นของคณะกรรมาธิการกฎหมาย ได้มีการทบทวนแก้ไขความเห็นดังกล่าวในเวลาต่อมา

และโดยที่คดีดังกล่าวที่เกิดขึ้นในประเทศอังกฤษ เป็นคดีซึ่งเป็นเพียงคดีเล็กน้อยเท่านั้น ดังนั้นมันจึงไม่สมควรที่จะมาชี้นำเราในการที่จะวิเคราะห์กฎหมายเกี่ยวกับกรณี ของการกระทำให้เกิดความเสียหายหรือทำลายซึ่งข้อมูลหรือโปรแกรมโดยไวรัสคอมพิวเตอร์

ผลต่อมาของคดีนี้ ทำให้นักกฎหมายจำนวนมากต่างให้ความสนใจและนำมาวิเคราะห์ว่าอะไรเป็นความเสียหายในคดี Cox V. Riley อันเป็นผลให้จำเลยถูกลงโทษ

ตามทฤษฎีแล้วมีเหตุผลที่เป็นไปได้ 3 อย่างด้วยกัน ที่จะบรรยายถึงความเสียหายที่เกิดขึ้นนี้

<u>เหตุผลที่ 1</u> ความเสียหายที่เกิดขึ้นเป็นความเสียหายที่เกิดขึ้นกับตัวโปรแกรมของตัวมันเอง จากการถูกแก้ไข

เหตุผลนี้ เป็นการให้เหตุผลโดยที่ปรึกษากฎหมายของฝ่ายจำเลยที่ได้ยื่นต่อศาลว่ามันเป็นลักษณะที่แท้จริงของความเสียหาย (the real nature of damage) แต่เหตุผลนี้ได้ถูกปฏิเสธ การเสนอเหตุผลดังกล่าวเพื่อเหตุผลที่ต้องการให้จำเลยได้รับการปล่อยตัว ทั้งนี้เพราะโปรแกรมเป็นทรัพย์สินที่จับต้องไม่ได้อย่างแน่นอน และทรัพย์สินดังกล่าวนี้ไม่อยู่ภายใต้มาตรา 1 ของ the Criminal Damage Act 1971

<u>เหตุผลที่ 2</u> ความเสียหายที่เกิดขึ้นเป็นการสร้างความเสียหายต่อตัวเครื่องจักรกล่าวคือ ทำให้เสื่อยของเครื่องจักรทำงานผิดปกติไปจากการทำงานตามปกติ

แนวความคิดนี้ได้มีเจ้าหน้าที่หลายคน พยายามที่จะชี้ให้เห็นว่าการกระทำดังกล่าวเป็นการมุ่งประสงค์ร้ายโดยตรงต่อตัวเครื่อง เพราะการกระทำอันเกี่ยวข้องกับการทำลาย การเคลื่อนย้าย หรือตัดการติดต่อของส่วนประกอบส่วนใดของเครื่อง เป็นการกระทำการที่ก่อให้เกิดความเสียหายอาญาที่ได้กระทำต่อตัวเครื่อง

เหตุผลที่ 3 ความเสียหายที่เกิดขึ้นเป็นการทำให้เกิดความเสียหายต่อตัวบัตร

ในความเห็นนี้ผู้พิพากษา สตีเฟน เบราว์ (Stephen Brown L J.) เห็นด้วยกับความคิดนี้เพราะ เป็นการเห็นได้ชัดว่าความเสียหายนั้น เกิดขึ้นต่อตัวบัตรพลาสติกที่ถูกพิมพ์ออกมา อย่างไรก็ตามความเห็นนี้ก็ได้มีความเห็นต่อมาอีกว่า วิธีใดที่เป็นการทำความเสียหายต่อตัวบัตร ถ้าบัตรดังกล่าวเป็นวัตถุที่มุ่งหมายกระทำต่อในฐานะที่เป็นภาชนะที่รองรับ โดยภาชนะที่รองรับนั้นเป็นสิ่งที่ว่างเปล่าอันจะเป็นตัวรับโปรแกรม กรณีนี้ก็เห็นได้ว่าตัวภาชนะที่รองรับไม่ได้รับความเสียหาย และจะถูกวิเคราะห์ต่อมาอีกว่า ทรัพย์สินที่จับต้องไม่ได้ ไม่สามารถที่จะถูกทำให้เสียหายได้ภายใต้พระราชบัญญัตินี้

ภายใต้ความไม่ชัดเจนถึงความเสียหายที่เกิดขึ้น ต่อทรัพย์สินซึ่งไม่อาจจับต้องได้ที่ได้กระทำต่อโปรแกรมหรือข้อมูลซึ่งเก็บไว้ในคอมพิวเตอร์ อันจะนำไปสู่การวิเคราะห์ถึงความเสียหายเช่นนั้น เป็นความเสียหายทางอาญา สำหรับผู้วิจัยเห็นด้วยกับความเห็นที่ 1 ที่ว่าความเสียหายที่เกิดขึ้น เป็นความเสียหายที่เกิดขึ้นกับตัวโปรแกรมที่ถูกแก้ไข เนื่องจากเป็นวัตถุที่ถูกกระทำโดยตรงแม้จะมีผลต่อมาให้เครื่องจักรทำงานผิดพลาดหรือบัตรที่ถูกตัดได้รับความเสียหาย แต่นั่นก็เป็นผลสืบเนื่องมาจากการแก้ไขโปรแกรม และเมื่อความเสียหายที่เกิดขึ้นเป็นการกระทำต่อตัวโปรแกรมอันเป็นทรัพย์สินที่ไม่มีตัวตน ไม่สามารถมองเห็นได้ และความเสียหายที่เกิดขึ้นไม่สามารถรับรู้ได้โดยความรู้สึก การแก้ไขโปรแกรมนี้ย่อมไม่ตกอยู่ภายใต้ the Criminal Damage 1971

และนอกจากนี้เป็นที่ยอมรับว่าขอบเขตของ the criminal Damage Act ไม่ขยายไกลเกินไป อันเนื่องจากถูกจำกัดต่อเฉพาะคดีเกี่ยวกับ การแทรกแซงทางกายภาพด้วยทรัพย์สินที่จับต้องได้เท่านั้น โดยทรัพย์สินที่จะถูกทำให้เกิดความเสียหายนั้น จะต้องถูกนำมาลบ เปลี่ยน

ในทรัพย์สินนั้นและต้องใช้เวลา ความพยายาม และค่าใช้จ่ายในการซ่อมแซม [19]

และเนื่องจากความไม่ชัดเจนของกฎหมายถึงความเสียหาย หรือการทำลายทางอาญา จะมีความหมายไปถึงรูปแบบของความเสียหายหรือทำลายซึ่งไม่สามารถมองเห็นได้ด้วยหรือไม่ ซึ่งต่อมาคณะกรรมาธิการร่างกฎหมาย the Comperter Misuse ได้กล่าวว่า พระราชบัญญัติ the Criminal Damage Act 1971 ที่แท้จริงแล้วไม่เป็นการเหมาะสม ที่จะแก้ไขเกี่ยวกับการกระทำต่อสิ่งซึ่งไม่มีรูปร่าง รวมไปถึงผลของการกระทำก็ไม่สามารถมองเห็นได้ เช่น โปรแกรมหรือข้อมูล การที่จะกำหนดออกมาเป็นกฎหมายใหม่จะเป็นวิธีการที่ดีที่สุด[20]

ซึ่งที่กล่าวมาทั้งหมดนี้ล้วนมีสภาพเช่นเดียวกับการกระทำในรูปแบบของโปรแกรมไวรัสคอมพิวเตอร์ ซึ่งก่อให้เกิดความเสียหายหรือการทำลายต่อโปรแกรมหรือข้อมูลที่เก็บอยู่ภายในซึ่งโดยสภาพแล้วมนุษย์ไม่สามารถมองเห็นด้วยตาเปล่าได้ และนักกฎหมายบางท่านก็ได้กล่าวว่าความเสียหายหรือการทำลายทางอาญานั้น จะต้องเป็นความเสียหายที่มองเห็นได้โดยทางกายภาพและสามารถรับรู้ได้โดยความรู้สึก

3.2.2 ปัญหาความหมายคำว่า "ทรัพย์สิน" (Property)

ในกฎหมายอาญา คำจำกัดความของคำแต่ละคำเป็นสิ่งที่มีความหมายเป็นอย่างยิ่ง เพราะนอกจากจะได้รู้ถึงขอบเขตของกฎหมายอาญาแล้ว ยังสามารถที่จะรู้ถึงที่มาและเจตนารมย์ของกฎหมาย ทั้งนี้ในการตีความกฎหมายอาญาจะต้องตีความโดยเคร่งครัด ซึ่งหมายถึงบทบัญญัติแห่งกฎหมายอาญาซึ่งกำหนดความผิดหรือบัญญัติโทษไว้จะต้องใช้บังคับตามตัวอักษรจะลงโทษบุคคลเพราะ

---

19. Matin Wasik, Ibid., p.141

20. Matin Wasik, Ibid., p.143

ได้กระทำการอันคล้ายคลึงกันกับที่ได้มีกฎหมายบัญญัติไว้นั้นมิได้ [21] นอกจากนี้จะนำบทกฎหมายใกล้เคียงมาใช้ได้เป็นผลร้ายหรือจะนำจารีตประเพณีมาใช้ให้เป็นผลร้ายก็มิได้ [22]

การสร้างความเสียหายของไวรัสคอมพิวเตอร์ ซึ่งอาจจะเป็นการทำลายข้อมูลหรือโปรแกรมทั้งหมดที่ถูกเก็บไว้ในคอมพิวเตอร์ อาจจะเป็นการสร้างความเสียหายเป็นจำนวนเงินที่มากต่อผู้ที่เป็นเจ้าของ ซึ่งตามกฎหมายลักษณะแพ่งผู้เสียหายอาจฟ้องร้องให้ผู้กระทำผิดชดใช้ค่าเสียหายที่เกิดขึ้นได้ตามกฎหมายลักษณะละเมิด แต่ตามกฎหมายอาญาผู้เสียหายจะฟ้องร้องให้ผู้กระทำผิดรับโทษทางอาญาในความผิดฐานทำให้เกิดความเสียหายหรือทำลายทรัพย์สินได้หรือไม่ ย่อมจำเป็นต้องพิจารณาถึงคำนิยามของกฎหมายของคำว่า "ทรัพย์สิน" ว่าจะมีความหมายครอบคลุมถึงข้อมูลหรือโปรแกรมที่บรรจุอยู่ในคอมพิวเตอร์หรือไม่

ในประเทศอังกฤษ ตามพระราชบัญญัติ the Criminal Damage Ace 1971 มาตรา 10(1) ได้ให้คำนิยามของคำว่า "ทรัพย์สิน" (Property) หมายถึง "ทรัพย์สินซึ่งตามลักษณะแล้วสามารถที่จะจับต้องได้ ไม่ว่าจะเป็นอสังหาริมทรัพย์หรือสังหาริมทรัพย์และให้รวมถึงเงินด้วย"

จากคำนิยามดังกล่าว ย่อมมีผลกระทบถึง โปรแกรมและข้อมูล ที่ถูกบันทึกอยู่ในคอมพิวเตอร์ ไม่ถือว่าเป็นทรัพย์สินตามความหมาของ the Criminal Damage Act 1971 ดังนั้นความเสียหายที่เกิดขึ้นโดยผลของโปรแกรมไวรัสคอมพิวเตอร์ ที่สร้างความเสียหายแก่โปรแกรมหรือข้อมูลจึง ไม่สามารถถูกลงโทษได้ตามกฎหมายฉบับนี้

ส่วนในสหรัฐอเมริกา ก็มีปัญหาทางกฎหมายในลักษณะเดียวกันที่กฎหมายอาญาที่มีอยู่ไม่สามารถลงโทษผู้กระทำความผิดต่อ บุคคลผู้ซึ่งทำให้โปรแกรม หรือข้อมูลทางคอมพิวเตอร์ได้รับความเสียหาย ซึ่งต่อมาในบางมลรัฐได้แก้ไขคำนิยามของคำว่า "ทรัพย์สิน" ให้กว้างขวางมากยิ่งขึ้น

---

21. เกียรติขจร วัจนะสวัสดิ์, คำอธิบายกฎหมายอาญา ภาค 1 (สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์, 2531), หน้า 21.

22. เรื่องเดิม

เช่น ให้รวมถึง

"สิ่งกระตุ้นทางอิเลคโทรนิค ข้อมูลหรือข่าวสารที่ผลิตขึ้นหรือทำขึ้นโดยกระบวนการทางอิเลคโทรนิค อุปกรณ์อิเลคโทรนิค ซอฟต์แวร์คอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ ไม่ว่าจะเป็นรูปแบบใดที่คนหรือเครื่องจักรกลสามารถอ่านออกหรือไม่ บริการทางคอมพิวเตอร์ วัตถุที่มีราคาที่เกี่ยวกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข่ายงานคอมพิวเตอร์ ไม่ว่าจะจับต้องได้หรือไม่ก็ตาม และสาเนาใด ๆ ของสิ่งนั้น"

แต่อย่างไรก็ตามในทางตรงกันข้าม ตามกฎหมายของประเทศอังกฤษ ซึ่งได้กำหนดว่า"คำที่ส่งผ่านโดยสิ่งกระตุ้นทางอิเลคโทรนิค ไม่ถือว่าอยู่ในสถานะภาพของทรัพย์สิน ข้อมูลต่าง ๆ ก็เช่นเดียวกันไม่ว่าจะอยู่ในคอมพิวเตอร์หรือไม่ก็ตาม"

ดังนั้น จึงเห็นได้ว่าคำจำกัดความของคำว่า "ทรัพย์สิน" มีความสำคัญต่อการที่จะกำหนดว่า การกระทำใดจะมีความผิดฐานทำให้เสียหายหรือทำลายทรัพย์ ในอันที่จะกำหนดว่าวัตถุนั้นเป็นทรัพย์สินหรือไม่ หากวัตถุชิ้นนั้นหรือสิ่ง ๆ นั้น มิได้อยู่ในคำจำกัดความของคำว่า"ทรัพย์สิน" แล้วก็ไม่อาจที่จะถือว่า จำเลยมีความผิดฐานทำให้เสียหายหรือทำลายทรัพย์สินนั้นได้

เช่นเดียวกับการกระทำของไวรัสคอมพิวเตอร์เมื่อโปรแกรมหรือข้อมูลตามกฎหมายไม่ถือว่าเป็นทรัพย์สิน แม้บางทีโปรแกรมหรือข้อมูลอาจมีมูลค่ามหาศาล หรืออาจจะเป็นความลับถูกทำลายโดยไวรัสคอมพิวเตอร์ กฎหมายอาญาก็ไม่สามารถที่จะลงโทษบุคคลนั้นได้

3.3 ความรับผิดเกี่ยวกับการกระทำความผิดต่อคอมพิวเตอร์ของต่างประเทศและปัญหาทางกฎหมายเกี่ยวกับไวรัสคอมพิวเตอร์

ในการวิจัยส่วนนี้จะแสดงให้เห็นถึง ความเป็นมาเกี่ยวกับกฎหมายคอมพิวเตอร์ของสหรัฐอเมริกา และเนื้อหาของกฎหมายที่ใช้บังคับในปัจจุบัน เพื่อที่จะให้ทราบถึงเจตนารมย์และการบังคับใช้ของกฎหมายที่ใช้อยู่ และแนวทางบังคับใช้กฎหมายของอังกฤษ ทั้งนี้เพื่อประโยชน์ที่จะนำไปวิเคราะห์ต่อกรณีการกระทำความผิดเกี่ยวกับไวรัสคอมพิวเตอร์

3.3.1 ความรับผิดเกี่ยวกับคอมพิวเตอร์ของสหรัฐอเมริกา

ก่อน ปี ค.ศ.1984 สหรัฐอเมริกามิได้มีกฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์ จนกระทั่งในปี ค.ศ.1984 จึงได้ออกมาเป็นกฎหมาย ในช่วงเวลาก่อนปี ค.ศ.1984 ความผิดอาญาเกี่ยวกับคอมพิวเตอร์ได้ถูกฟ้องร้องภายใต้กฎหมายอาญามากกว่า 40 ฉบับ จนกระทั่งในปี ค.ศ.1984 สภาคองเกสได้พิจารณาเป็นครั้งสุดท้ายและได้ผ่านกฎหมายดังกล่าวเป็นฉบับแรกที่จะนำมาใช้แก้ไขปัญหาเกี่ยวกับอาชญากรรมคอมพิวเตอร์โดยเฉพาะคือ the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984

ในขณะที่สภาคองเกสได้พิจารณาถึงปัญหาดังกล่าวในอันที่จะออกกฎหมายแรกนั้น ได้มีหลายมลรัฐออกกฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์เรียบร้อยแล้ว และนอกจากนี้ยังมีกฎหมายของสหรัฐอเมริกาอีกหลายฉบับ ที่สามารถนำมาใช้บังคับฟ้องร้องได้กับความผิดเกี่ยวกับคอมพิวเตอร์ ปัญหาเหล่านี้ล้วนเป็นสิ่งที่สภาคองเกสจะต้องไตร่ตรองอย่างรอบคอบถึงการที่จะออกกฎหมายของสหรัฐอเมริกา

มีสิ่งหนึ่งที่เกิดขึ้นมาพร้อมกับการออกกฎหมายอาญาเกี่ยวกับคอมพิวเตอร์คือ การเผยแพร่รายงานของ the American Bar Association ชี้ให้เห็นว่าอาชญากรรมคอมพิวเตอร์เป็นสาเหตุของการสูญเสียทางการเงินในช่วงระหว่าง 145 ล้านเหรียญถึง 750 ล้านเหรียญในแต่ละปี นอกจากนี้เพื่อให้ครอบคลุมถึงเครื่องมือที่ขยายขึ้นของ "การกระทำความผิดเกี่ยวกับคอมพิวเตอร์" ทำให้สภาคองเกสมีความต้องการที่จะออกกฎหมายขึ้นมาโดยเฉพาะ

และเมื่อครั้งการปรับปรุงกฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์ในครั้งสุดท้าย สภาคองเกสได้ตั้งข้อสังเกตุถึงการเพิ่มขึ้นของการใช้คอมพิวเตอร์ในสังคมอเมริกาและ

ความสามารถที่จะเป็นไปได้ ของการกระทำความผิดอาญาในกรณีที่ใช้ในทางที่ผิดเกี่ยวกับเทคโนโลยี ซึ่งเป็นสิ่งที่จำเป็นอย่างมากในการนำมาใช้กับการดำเนินชีวิตของเรา

หลังปี ค.ศ.1984 ซึ่งเป็นเวลาภายหลังจากที่ได้ออกกฎหมายดังกล่าวแล้ว สภาคองเกสได้ลังเลที่จะแก้ไขกฎหมายอันเนื่องจากต้องเผชิญกับปัญหาเป็นจำนวนมาก ทั้งนี้เพราะพยานหลักฐานในการพิสูจน์ความผิดมีน้อยและยิ่งไปกว่านั้น ความเห็นที่ยังตกลงกันไม่ได้ถึงความเหมาะสมในการให้คำนิยามของคำว่า "ความผิดเกี่ยวกับคอมพิวเตอร์" (Computer Crime) และยังมีเหตุผลเพิ่มขึ้นมาอีก ซึ่งสภาคองเกสยิ่งจะต้องระมัดระวังถึงรูปแบบในการที่จะออกกฎหมายอันจะต้องคำนึงถึงความเหลื่อมล้ำของอำนาจศาล (federal jurisdictional overreaching) และการที่มีกฎหมายมากเกินไป

ในขณะที่นักวิจารณ์ต่าง ๆ ได้เรียกร้องให้มีการปรับปรุงกฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์ ปัญหาเหล่านี้ก็ได้มีการแพร่หลายออกไป ท่ามกลางข้อบกพร่องที่สามารถเห็นได้จาก the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 ที่รวมถึงการขาดมาตราที่เป็นตัวกำหนดคำนิยาม ที่ควรเอามาไว้รวมกัน ความล้มเหลวที่จะขยายการป้องกันไปสู่เครื่องคอมพิวเตอร์ที่ใช้ในภาคเอกชน การขาดการกำหนดมูลค่าต่าง ๆ อันจะฟ้องได้

ด้วยเหตุผลต่าง ๆ ตามที่กล่าวมานี้ ทันทีที่กฎหมายปี 1984 ถูกนำมาบังคับใช้ การออกกฎหมายเพื่อปรับปรุงใหม่ก็ถูกเรียกร้องขึ้น

ในปี ค.ศ.1986 ได้มีการนำกฎหมาย ปี ค.ศ.1984 มาแก้ไขใหม่ ซึ่งในการแก้ไขครั้งนี้ได้รวมถึงมาตราซึ่งเป็นปัญหาในคดีของนายมอริส (Morris) เกี่ยวกับการปล่อยไวรัสคอมพิวเตอร์เข้าไปในคอมพิวเตอร์ด้วย โดยเฉพาะในเรื่องของ"เจตนา" ซึ่งในการแก้ไขใหม่นี้มีวัตถุประสงค์ เพื่อที่จะเพิ่มประสิทธิภาพในการจัดการกับปัญหาให้มากขึ้น ต่อการกระทำเกี่ยวกับการฉ้อฉลและการใช้ในทางที่ผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งการแก้ไขที่เป็นเป้าหมายคือการแก้ไขในปัญหาที่กฎหมายปี 1984 ไม่สามารถครอบคลุมถึง

และในปี ค.ศ.1986 จึงได้ออกกฎหมายฉบับใหม่ขึ้นมาชื่อ the Computer Fraud and Abuse Act 1986 ซึ่งกฎหมายฉบับนี้ได้เปลี่ยนสาระสำคัญของกฎหมายปี 1984 ที่สำคัญ

คือ

1. การเปลี่ยนเจตนาร้าย (Mens rea) ตามมาตรา 1030 (a) (2) และ (a) (3) จาก "โดยรู้" (knowingly) เป็น "โดยเจตนา" (intentionally)

2. ขยายข้อความในอนุมาตรา 1030 (a) (3) ออกเป็น 2 อนุมาตรา เพื่อให้ข้อความชัดเจนยิ่งขึ้น

3. ขยายมาตราที่จะกำหนดคำนิยามในกฎหมาย

การแก้ไขกฎหมายปี 1986 ยังคงจำกัดอำนาจศาลอยู่เฉพาะ คดีที่อยู่ในอำนาจของรัฐบาลกลาง[23] คือคดีที่ผลกระทบต่อประโยชน์ของประเทศ ซึ่งทั้งหมดนี้ถูกตั้งไว้เป็นความหวังในการที่จะแก้ไข เพื่อที่จะเพิ่มประสิทธิภาพของกฎหมายโดยการเพิ่มการกระทำที่ต้องห้าม การใช้ภาษาที่ชัดเจนและแก้ไขกฎหมายที่เหลื่อมล้ำกัน

ตาม the Computer Fraud and Abuse Act 1986 ของสหรัฐอเมริกาได้กำหนดความผิดขึ้นใหม่ซึ่งมีรูปแบบแตกต่างไปจากความผิดที่กฎหมายเดิมมีอยู่ เพื่อรองรับการกระทำความผิดที่เกิดขึ้นโดยอาศัยเทคโนโลยีสมัยใหม่ ออกเป็น 3 ฐานความผิด คือ

1. ความผิดฐานเข้าถึงโดยปราศจากอำนาจ (Unauthorized Access)

2. ความผิดฐานแก้ไขเปลี่ยนแปลง (Alteration)

3. ความผิดฐานทำให้เสียหายหรือทำลาย (Damage or Destruction)

โดยการออกกฎหมายของสหรัฐอเมริกานี้ ได้ออกมาเพื่อแก้ไขปัญหาความรุนแรงของการกระทำอันเป็นความผิดเหล่านี้ในขณะนั้นโดยเฉพาะ เพราะกฎหมายเท่าที่มีอยู่ไม่สามารถนำมาปรับใช้ได้ ซึ่งขณะนั้นปัญหาเกี่ยวกับไวรัสคอมพิวเตอร์ (Computer Virus) มิได้เป็นปัญหาที่รุนแรง และสภาคองเกสก็มิได้คาดคิดว่าปัญหาเกี่ยวกับไวรัสคอมพิวเตอร์นี้จะเป็นปัญหาที่รุนแรงในปัจจุบัน นอกจากนี้ยังมีปัญหาในข้อกฎหมายด้วยว่ากฎหมายที่ออกมาใหม่นี้จะครอบคลุมถึงการกระทำ

---

23. Susan m. Mello, " Administering the Antidote to Computer Viruses: AComment on United States V. Morris," Rutgers Computer and Technology Law Journal 19 (1993): p.264.

เกี่ยวกับไวรัสคอมพิวเตอร์หรือไม่ จนในที่สุดได้มีสมาชิกสภาคองเกสได้เสนอร่างกฎหมาย the Computer Virus Eradication Act ขึ้น

และเพื่อการวิจัยฉบับนี้จะได้สมบูรณ์ยิ่งขึ้น ผู้เขียนจึงขอกล่าวถึงหลักการสำคัญของความผิดทั้ง 3 ประการของ the Computer Fraud and Abuse Act 1986 เพื่อใช้ในการวิเคราะห์ความผิดเกี่ยวกับไวรัสคอมพิวเตอร์ต่อไป

3.3.1.1. ความผิดฐานเข้าถึงโดยปราศจากอำนาจ (Unauthorized Access)

ตาม the Computer Fraud and Abuse Act 1986 มาตรา 1030 (a) (1) ได้บัญญัติว่า "โดยรู้ถึง การเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจ..."

ตามบทบัญญัติดังกล่าวได้กำหนดความผิดขึ้นมาใหม่ โดยได้กำหนดลักษณะของการกระทำผิดขึ้นมาคือ "การเข้าถึงโดยปราศจากอำนาจ" และนอกจากนี้ยังรวมถึงการกระทำการเกินกว่าอำนาจแห่งการเข้าถึง (exceeds authorized access)ด้วย

คำนิยามของคำว่า"เข้าถึง"ที่กฎหมายของสหรัฐอเมริกาส่วนใหญ่นิยมใช้กันอยู่[24]ได้แก่ "เข้าถึง"(access) หมายถึง เข้าไปสู่ สั่ง สื่อสารกับ ใส่ข้อมูลเข้าไปเก็บไว้ ล้วงข้อมูลมาจากหรืออีกนัยหนึ่ง เอาประโยชน์ใดๆของเครื่องคอมพิวเตอร์ระบบคอมพิวเตอร์ หรือข่ายงานคอมพิวเตอร์มาใช้ โดยที่ตนเองไม่มีอำนาจที่จะกระทำเช่นนั้น

ตามคำนิยามนี้ใช้คำว่า"อีกนัยหนึ่ง...." ดังนั้นการเข้าไปสู่ สั่ง สื่อสารกับ ใส่ข้อมูลเข้าไปเก็บไว้ ล้วงข้อมูลมาจากเครื่องคอมพิวเตอร์ หรือข่ายงานคอมพิวเตอร์ จึงมีความหมายในลักษณะของการกระทำที่เป็นไปเพื่อการเอาประโยชน์ของเครื่องคอมพิวเตอร์ ฯลฯ มาใช้ด้วยและดังนั้นความหมายของการกระทำต่างๆ ในคำนิยามจึงอาจอธิบายได้ดังนี้

เข้าไปสู่ (Approach) หมายถึง การกระทำที่เป็นการเข้าหาหรือเข้าไปสู่สิ่งที่ตนต้องการภายในเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือข่ายงานคอมพิวเตอร์

---

24. ภานุ รังสีสหัส, เรื่องเดิม, หน้า 53

สั่ง (Instruct) หมายถึงการกระทำที่เป็นการสั่งให้เครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือข่ายงานคอมพิวเตอร์ ทำงานให้ตามความต้องการของตน

สื่อสารกับ (Communicate with) หมายถึงการกระทำที่เป็นการติดต่อกับเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือข่ายงานคอมพิวเตอร์ ด้วยวิธีการทางการสื่อสาร เช่น ผ่านสายโทรศัพท์ เป็นต้น เพื่อให้ได้ข้อมูลหรือประโยชน์อย่างอื่นตามความต้องการของตน

ใส่ข้อมูลเข้าไปเก็บไว้(Store data in) หมายถึงการกระทำที่เป็นการนำข้อมูลใส่เข้าไปในเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข่ายงานคอมพิวเตอร์ เพื่อตนจะได้ประโยชน์จากการทำงานของเครื่องคอมพิวเตอร์ ฯลฯ ในภายหลัง

ล้วงข้อมูลมาจาก (Retrieve data from) หมายถึงการกระทำที่เป็นการเอาข้อมูลออกมาจากเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข่ายงานคอมพิวเตอร์ เพื่อประโยชน์ของตน

เอาประโยชน์ใดๆ มาใช้(Make use of any resources of) หมายถึง การกระทำใด ๆ ต่อเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข่ายงานคอมพิวเตอร์ ที่เป็นไปเพื่อประโยชน์ของตน

ส่วนคำนิยามของคำว่า "การกระทำเกินกว่าอำนาจแห่งการเข้าถึง" (Exceeds Authorized Access) หมายถึงการเข้าถึงคอมพิวเตอร์โดยมีอำนาจ แต่ได้ใช้การเข้าถึงนั้นเพื่อที่จะได้รับ หรือเปลี่ยนแปลงข้อมูลที่เก็บไว้ในคอมพิวเตอร์นั้น ซึ่งผู้ที่เข้าถึงไม่มีสิทธิที่จะได้รับหรือเปลี่ยนแปลงข้อมูลนั้น[25]

ซึ่งการเข้าถึงทางคอมพิวเตอร์ หรือกระทำเกินกว่าอำนาจแห่งการเข้าถึง อาจก่อให้เกิดการกระทำที่มิชอบขึ้นได้ในรูปแบบต่างๆ กัน การกระทำที่มิชอบเหล่านี้มีลักษณะคล้ายคลึงกับความผิดฐานลักทรัพย์ ความผิดฐานบลอมแปลงเอกสาร และความผิดฐานทำให้เสียทรัพย์ตามกฎหมายอาญา แต่มีความแตกต่างกันของในเรื่องขององค์ประกอบของความผิดบางประการ ซึ่งทำให้ไม่สามารถนำบทบัญญัติแห่งกฎหมายในเรื่องของความผิดฐานลักทรัพย์ ความผิดฐานปลอมเอกสาร และความผิด

---

25. 18 U.S.C.S. 1030(e)(6)

ฐานทำให้เสียทรัพย์มาบังคับใช้กับการกระทำที่ก่อให้เกิดความเสียหายนี้ขึ้นได้

เฉพาะในส่วนของการกระทำทำนองลักทรัพย์นั้น กฎหมายที่มีอยู่แล้วในเรื่องของการลักทรัพย์ได้ประสบกับปัญหาข้อขัดข้อง ในการนำมาบังคับใช้กับความผิดที่เกิดขึ้นกับเทคโนโลยี่สมัยใหม่นี้ โดยเหตุที่ความผิดฐานลักทรัพย์นั้นส่วนใหญ่จะเป็นเรื่องที่เกี่ยวกับทรัพย์ที่จับต้องได้ และทรัพย์ที่จับต้องไม่ได้ในบางกรณี เพราะฉะนั้น "การเอาไป" จึงถือว่าเป็นสาระสำคัญของความผิดฐานนี้ องค์ประกอบเกี่ยวกับการ "เอาไป" นี้ได้ก่อให้เกิดปัญหาขึ้นในเมื่อมันได้เข้าไปเกี่ยวข้องกับคอมพิวเตอร์ เพราะการเอาไปในกรณีนี้อาจมิได้มีการจับต้องหรือการพาไปตามความเป็นจริงเลยก็ได้[26] ดังนั้น กฎหมายของสหรัฐอเมริกาในปัจจุบันจึงได้บัญญัติกฎหมายอาญาในความผิดเกี่ยวกับคอมพิวเตอร์ในส่วนของความผิดดังกล่าวเป็น "ความผิดฐานเข้าถึง"(Access) ขึ้น ต่างหากจากความผิดฐานลักทรัพย์ เพื่อที่จะสามารถนำมาใช้บังคับกับการกระทำที่ก่อให้เกิดความเสียหายอันมีลักษณะของการลักขโมยนี้ขึ้นโดยเฉพาะ

นอกจากกรณีที่การเข้าถึงทางคอมพิวเตอร์ได้ก่อให้เกิดการกระทำที่มิชอบขึ้น อันเทียบเคียงได้กับความผิดฐานลักทรัพย์ ความผิดฐานปลอมแปลงเอกสาร และความผิดฐานทำให้เสียทรัพย์ ซึ่งเป็นลักษณะที่กฎหมายอาญาที่เกี่ยวกับคอมพิวเตอร์ของสหรัฐอเมริกา ได้บัญญัติความผิดขึ้นใหม่สามประการดังกล่าวแล้ว การเข้าถึงทางคอมพิวเตอร์อาจก่อให้เกิดการกระทำที่มิชอบในลักษณะที่เป็นความผิดตามกฎหมายอื่นๆ ที่มีอยู่แล้วอีกทางหนึ่งด้วย เช่นการฝ่าฝืนต่อกฎหมาย Privacy Act การละเมิดต่อกฎหมายสิทธิ์ที่มีโทษทางอาญาอยู่ด้วย และกฎหมายที่เกี่ยวกับการระเบียบสถาบันการเงินและการควบคุมอัตราดอกเบี้ย

ในส่วนของการฝ่าฝืนกฎหมาย Privacy Act นั้น กฎหมาย Privacy Act ค.ศ.1974 ได้นำมาประมวลไว้ในประมวลกฎหมาย สหรัฐอเมริกา บรรพที่ 5 มาตรา 552 เอ. ซึ่งมีบทลงโทษทางอาญาอยู่ในอนุมาตรา (ไอ) (1)-(3) การลงโทษทางอาญาเหล่านี้อาจเกิดขึ้นได้เมื่อมีการ

---

26. วีระพงษ์ บุญโญภาส,"อาชญากรรมจากคอมพิวเตอร์," เอกสารภาษีอากร:วารสารธรรมนิติ 7 (กรกฎาคม 2531) : 103

ฝ่าฝืนต่อบทบัญญัติของกฎหมายดังกล่าว โดยการเปิดเผยข่าวสารของบุคคลโดยตั้งใจ และโดยปราศจากอำนาจซึ่งได้กระทำจากฐานข้อมูลทางคอมพิวเตอร์

พื้นฐานของบทบัญญัติในกฎหมายดังกล่าวเป็นเรื่องของ การที่จะคุ้มครองความเป็นส่วนบุคคล ฉะนั้น ในประมวลกฎหมายสหรัฐอเมริกา บรรพที่ 5 มาตรา 551(1) และ 552 (อี) จึงได้บัญญัติคำนิยามของคำว่า Agency ไว้และห้ามมิให้ Agency ทำการเปิดเผยบันทึกเอกสารใดๆ ที่ได้บรรจุอยู่ในระบบบันทึกทางเอกสารต่าง ๆ แก่บุคคลอื่นหรือแก่ Agency อีกแห่งหนึ่ง โดยมีข้อยกเว้นต่าง ๆ หลายประการ เว้นแต่บุคคลที่เป็นเจ้าของบันทึกนั้นจะได้ร้องขอเป็นหนังสือ หรือได้ให้คำยินยอมเป็นหนังสือก่อนหน้านั้น

ถ้าพนักงานหรือลูกจ้างของ Agency แห่งหนึ่งรู้อยู่แล้วว่า การเปิดเผยข้อความที่พิเศษเฉพาะนั้น ได้มีการห้ามโดยกฎหมายดังกล่าวหรือโดยระเบียบที่ได้ออกตามกฎหมายดังกล่าวอันใดอันหนึ่ง และพนักงานหรือลูกจ้างผู้นั้นทำการเปิดเผยข้อความดังกล่าวโดยตั้งใจแก่บุคคลอื่น หรือ Agency อีกแห่งหนึ่งซึ่งไม่มีสิทธิที่จะรับรู้ข้อความนั้น ต้องถือว่าพนักงานหรือลูกจ้างผู้นั้นได้กระทำความผิดในระดับ Misdemeanor และต้องถูกปรับไม่เกิน 5,000 เหรียญสหรัฐ

ในส่วนของการละเมิดต่อกฎหมายลิขสิทธิที่มีโทษทางอาญา การเข้าถึงทางคอมพิวเตอร์ที่ก่อให้เกิดการลักขโมยโปรแกรมทางคอมพิวเตอร์นั้น ยังอาจถูกฟ้องร้องได้ตามกฎหมายลิขสิทธิ์ของรัฐบาลกลางแห่งสหรัฐอเมริกา สำนักงานทะเบียนลิขสิทธิได้ยอมรับการจดทะเบียนโปรแกรมคอมพิวเตอร์ว่าเป็น "หนังสือ" (Books) ชนิดหนึ่งมาตั้งแต่ปี ค.ศ.1964 รายงานคณะกรรมการรัฐสภาเกี่ยวกับกฎหมายลิขสิทธิ์ ค.ศ.1976 หน้า 54 ระบุว่า คำว่า "งานวรรณกรรม" (Literary Work) รวมถึงฐานข้อมูลทางคอมพิวเตอร์และโปรแกรมคอมพิวเตอร์ ในขอบเขตที่ว่าให้รวมถึงงานประพันธ์ ที่เป็นการแสดงออกถึงความคิดดั้งเดิมของนักเขียนโปรแกรมเข้าไว้ อันได้แยกออกจากตัวความคิดเอง ดังนั้น ผู้สร้างโปรแกรมคอมพิวเตอร์จึงสามารถป้องกันเอกสารและลายเส้นของรหัสคอมพิวเตอร์ได้จากการแอบคัดลอก แต่การคุ้มครองทางลิขสิทธิ์นี้ก็ไม่ได้ขยายไปถึง "ชุดของกฎเกณฑ์" (Algorithms) ของนักเขียนโปรแกรมด้วย

นอกจากลักษณะที่การเข้าถึงได้ก่อให้เกิดการกระทำอันเป็นความผิดต่างๆ กัน ดังที่กล่าว

มานี้ ลำพังของตัวการกระทำที่เป็นเพียงการเข้าถึงยังอาจเป็นการกระทำความผิดทางอาญาได้โดยไม่ต้องคำนึงถึงว่าจำเลยจะได้ทำการอื่นใดอีกหรือไม่ ภายหลังจากที่ได้รับประโยชน์จากการเข้าถึงเครื่องคอมพิวเตอร์ ถ้าจำเลย

1. ได้รับประโยชน์จากการทุจริต เช่นโดยการใช้ "รหัสผ่าน" ของบุคคลอื่น หรือโดยการใช้ "รหัสผ่าน" เท็จ เพื่อที่จะได้รับประโยชน์จากการเข้าถึงนั้น

2. ได้รับประโยชน์จากการเข้าถึงในความมุ่งหมายของการกระทำ ความผิดในทางอาญา เช่นการยักยอก โดยไม่ต้องคำนึงถึงความสำเร็จจากผลของการกระทำนั้น

3. ได้รับประโยชน์จากการเข้าถึงโดยวิถีทางที่มิชอบ เช่นการดักฟังทางสาย

กฎหมายของหลายๆ มลรัฐในสหรัฐอเมริกาได้กำหนดเป็นการพิเศษของการเข้าถึงโดยไม่มีอำนาจนั้นไม่จำเป็นต้องคำนึงถึงการกระทำอื่นใดเพิ่มขึ้นอีก

การเข้าถึง (Access) เป็นลักษณะของการกระทำอย่างหนึ่งซึ่งจำเป็นต้องมีขึ้นทุกครั้งที่ต้องการจะได้ประโยชน์จากการทำงานของเครื่องคอมพิวเตอร์ จากจุดที่ว่า "จำเป็นจะต้องกระทำขึ้นทุกครั้ง" อันเป็นลักษณะพิเศษเฉพาะของการได้ไปซึ่งประโยชน์จากการทำงานของเครื่องคอมพิวเตอร์นี้เอง ทำให้มีปัญหาข้อขัดข้องของลักษณะการกระทำในการ"เอาไป" ในความผิดฐานลักทรัพย์ซึ่งต้องมีการ "แย่งการครอบครอง" และ "พาเคลื่อนที่ไป" ที่ไม่ได้เกิดขึ้นในการได้ไปซึ่งทรัพย์สินในทางคอมพิวเตอร์ อาจแก้ไขได้ด้วยการบัญญัติความผิดของการได้ไปซึ่งทรัพย์สินในทางคอมพิวเตอร์ (ทรัพย์สินที่ไม่มีรูปร่าง) ในส่วนของการกระทำที่เป็นไปตามหลักการของเทคโนโลยีทางคอมพิวเตอร์ ซึ่งอาศัยการ"เข้าถึง" มาเป็นการกระทำเพื่อให้ได้ไปซึ่งทรัพย์สินนั้น ให้เป็นองค์ประกอบของความผิดใน หลักการเช่นนี้ยังอาจนำมาใช้ได้ในอนาคต เมื่อมีเทคโนโลยีใหม่ๆ เกิดขึ้น

3.3.1.2. ความผิดฐานแก้ไขเปลี่ยนแปลง (Alteration)

ตาม The Computer Fraud and Abuse Act 1986 ได้กำหนดความผิดฐานแก้ไขเปลี่ยนแปลง(Alterative) ซึ่งได้กระทำต่อข้อมูลใดๆ ที่เก็บอยู่ในคอมพิวเตอร์ใดๆ อันรัฐได้ใช้ประโยชน์จากคอมพิวเตอร์นั้น หรือขัดขวางการใช้คอมพิวเตอร์หรือข้อมูลของผู้มีอำนาจใช้

การแก้ไขเปลี่ยนแปลงเกี่ยวกับคอมพิวเตอร์นี้ หมายถึงการแก้ไขเปลี่ยนแปลงโปรแกรมหรือข้อมูลใดๆ ที่ได้บรรจุอยู่ในเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข่ายงานคอมพิวเตอร์ ซึ่งในลักษณะของการแก้ไขเปลี่ยนแปลงนั้น บางลักษณะก็จะต้องอาศัยการเข้าถึงทางคอมพิวเตอร์ด้วย ดังที่ได้กล่าวมาแล้ว แต่บางลักษณะก็อาจจะเป็นการแก้ไขเปลี่ยนแปลงที่ไม่ต้องอาศัยการเข้าถึงใดๆ อันเป็นการแก้ไขเปลี่ยนแปลงแก่วัตถุที่เป็นโลหะอุปกรณ์โดยตรง และเนื่องจากโลหะอุปกรณ์เช่นว่านี้เป็นทรัพย์สินในทางเทคโนโลยีชนิดหนึ่ง การกระทำนั้นจึงอาจก่อให้เกิดความเสียหายค่อนข้างสูง เมื่อเทียบกับการแก้ไขเปลี่ยนแปลงในทรัพย์สินที่เป็นประดิษฐกรรมธรรมดาอย่างอื่นๆ ประกอบกับวัตถุที่ผู้กระทำความผิดที่เจตนาที่จะกระทำต่อนั้น เป็นสิ่งที่ไม่สามารถที่จะมองเห็นได้ด้วยตาเปล่า ดังนั้นด้วยเหตุนี้เอง กฎหมายอาญาในความผิดเกี่ยวกับคอมพิวเตอร์ของสหรัฐอเมริกาจึงได้บัญญัติความผิดชนิดนี้ขึ้นมา

ในส่วนของการแก้ไขเปลี่ยนแปลงที่ต้องอาศัยการเข้าถึงนั้น สาเหตุที่กฎหมาย ในเรื่องความผิดทางอาญาเกี่ยวกับคอมพิวเตอร์ได้บัญญัติความผิดฐาน"แก้ไขเปลี่ยนแปลง" แยกออกต่างหากจากความผิดฐานเข้าถึง น่าจะมาจากเหตุผลที่ว่า การแก้ไขเปลี่ยนแปลงทางคอมพิวเตอร์ อาจเป็นไปได้ทั้งในรูปแบบที่ต้องอาศัยการเข้าถึงและในรูปแบบที่ไม่ต้องอาศัยการเข้าถึงก็ได้[27] ประการหนึ่ง และการแก้ไขเปลี่ยนแปลงทางคอมพิวเตอร์มีส่วนเกี่ยวข้อง ในแง่ของการกระทำซึ่งเป็นปัญหาเกี่ยวกับความผิดฐานปลอมเอกสารอยู่ด้วยอีกประการหนึ่ง โดยเฉพาะในส่วนที่เกี่ยวข้องกับความผิดฐานปลอมเอกสารนี้ ปัญหาที่เกิดขึ้นเกี่ยวพันไปถึงความขัดข้องของการนำบทบัญญัติอันว่าด้วย ความผิดฐานปลอมเอกสารมาบังคับใช้ซึ่งเป็นเรื่องของการขาดองค์ประกอบของความผิด ฝ่ายนิติบัญญัติของมลรัฐต่างๆ และของรัฐบาลกลางแห่งสหรัฐอเมริกาจึงได้บัญญัติความผิดฐานนี้ แยกออกมาให้ครอบคลุมได้ครบถ้วนอย่างกว้างขวางยิ่งขึ้น

ปัญหาของการแก้ไขเปลี่ยนแปลงทางคอมพิวเตอร์ ในส่วนที่จะนำมาพิจารณาในแง่ของการปลอมเอกสารได้นั้นเป็นไปได้ก็แต่ในกรณีของการแก้ไขเปลี่ยนแปลงโปรแกรมคอมพิวเตอร์ หรือข้อมูลต่างๆ ส่วนการแก้ไขเปลี่ยนแปลงเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข่ายงานคอมพิว

---

27. ภานุ รังสีสหัส, เรื่องเดิม, หน้า 96

เตอร์นั้น ย่อมไม่มีปัญหาในเรื่องของการปลอมเอกสารแต่อย่างใด เพราะไม่มีส่วนเกี่ยวข้องกับคำว่า "เอกสาร" อยู่เลย ส่วนสาเหตุที่กฎหมายของสหรัฐอเมริกา ในเรื่องความผิดทางอาญาเกี่ยวกับคอมพิวเตอร์ ได้บัญญัติไว้ให้เป็นความผิดพิเศษออกไปจากการแก้ไขเปลี่ยนแปลงแก่วัตถุธรรมดาทั่วๆ ไป ซึ่งไม่เป็นความผิดทางอาญาเลยก็เป็นดังที่ได้กล่าวมาแล้วว่า เป็นการกระทำความเสียหายให้แก่ผลิตผลในทางเทคโนโลยีอันควรได้รับการคุ้มครองอย่างหนึ่งนั่นเอง

ความผิดฐานแก้ไขเปลี่ยนแปลงทางคอมพิวเตอร์ส่วนใหญ่จะมีส่วนสัมพันธ์กับการได้ประโยชน์ไปในทางทรัพย์สิน เช่นเดียวกันกับความผิดฐานเข้าถึงทางคอมพิวเตอร์ รูปแบบของการทุจริตด้วยวิธีนี้แม้ว่าจะมีอยู่มากมาย แต่วิธีการจัดทำ และกระบวนการต่าง ๆ เพื่อการทุจริตพอจะจำแนกได้เพียง 3 ลักษณะ คือ

1. การแก้ไขเปลี่ยนแปลงหรือปรุงแต่งข้อมูลนำเข้าเพื่อการบันทึก

2. การแก้ไขคำสั่งหรือโปรแกรมโดยไม่มีอำนาจ

3. การแก้ไขหรือสับเปลี่ยนข้อมูลในแฟ้มข้อมูล[28]

การแก้ไขเปลี่ยนแปลงหรือปรุงแต่งข้อมูลนำเข้าเพื่อการบันทึกนั้น เป็นวิธีที่ผู้ทุจริตจัดทำมากที่สุดวิธีหนึ่ง วิธีการจัดทำการปรุงแต่งข้อมูลนี้อาจจะทำได้หลายประการเช่น

ก. การเพิ่มรายการที่จะบันทึก

ข. การงดเว้นการบันทึกรายการที่ควรจะบันทึก

ค. การดัดแปลงรายการที่จะบันทึก

ง. การทำการปรับปรุงรายการที่จะบันทึก

จ. การทำการปรับปรุงรายการโดยเจตนาทำผิด

ฉ. การใช้วิธีการแก้ไขข้อผิดพลาดนอกเหนือจากวิธีที่ได้กำหนดไว้

การแก้ไขเปลี่ยนแปลงโปรแกรม หรือคำสั่งโดยไม่มีอำนาจนั้น โดยที่ข้อมูลนำเข้าก็ถูกต้องและแฟ้มข้อมูลหลักหากถูกต้อง จุดหนึ่งที่จะคดโกงได้ก็คือตัวโปรแกรม ซึ่งอาจจะทำได้ในทั้งระดับ

---

28. เกียรติศักดิ์ จีรเธียรนาถ, "คอมพิวเตอร์กับการทุจริต," ในแนวทางการป้องกันทุจริต: มะเร็งร้ายของการดำเนินธุรกิจ (กรุงเทพมหานคร: สำนักพิมพ์กรุงสยาม-จตุพร, 2528) หน้า 117

โปรแกรมควบคุมการปฏิบัติงานภายในของเครื่อง (System Program) โปรแกรมใช้งานร่วม (Utilities) และโปรแกรมใช้งานเฉพาะกิจ (Specific Application Program) ในกรณีของ System Program อาจจะมีการกำหนดรหัสให้ผู้ทราบรหัสเท่านั้น ที่สามารถจะไปแก้ไขแฟ้มข้อมูลนี้ได้ ในกรณีนี้ก็อาจจะแก้ไข System Program ให้เพิ่มรหัสพิเศษ ทำให้ผู้ทราบรหัสพิเศษสามารถเข้าไปแก้ไขแฟ้มข้อมูลต่างๆ ได้ในระดับ Utilities ก็อาจจะมีการแก้ไขโปรแกรม Utilities ให้ทำสิ่งที่ผู้แก้ไขต้องการ เช่นในการคัดลอกแฟ้มข้อมูลให้ฝ่ายตรวจสอบ ก็ให้เว้นการคัดลอกข้อมูลที่ไม่ต้องการให้ฝ่ายที่ตรวจสอบข้อมูลทราบเป็นต้น ส่วนในด้านโปรแกรมใช้งานเฉพาะกิจก็อาจจะแก้ไขให้ปัดเศษสตางค์ไปเข้าบัญชีพิเศษเป็นต้น

การแก้ไขโปรแกรมหรือคำสั่งโดยไม่มีอำนาจนั้น เป็นวิธีการทุจริตที่ต้องใช้ความรู้ความชำนาญในการเขียนคำสั่ง ดังนั้นในการค้นหาให้พบการกระทำเช่นนี้จึงเป็นสิ่งที่ยากอย่างยิ่ง การแก้ไขคำสั่งในบางกรณีไม่สามารถจะทำการตรวจสอบพบได้ และด้วยเหตุที่เป็นการกระทำที่ยากต่อการตรวจพบนี้เอง ทำให้เกิดแรงจูงใจอย่างสูงแก่ผู้กระทำผิดในการที่จะตัดสินใจกระทำการทุจริต เพราะด้วยการกระทำเพียงอึดใจเดียว อาจได้รับผลตอบแทนจากการกระทำเป็นอย่างสูง นอกจากนั้นยังยากแก่การถูกจับกุมดำเนินคดี ก็เพราะว่าผู้ที่มีความเข้าใจคำสั่งที่จะใช้กับคอมพิวเตอร์จะมีหลายๆ คนในหน่วยงานหนึ่งๆ ผลที่เกิดจากการแก้ไข ก็มักจะไม่สามารถตรวจพบข้อผิดพลาดนั้นก็เป็นการยากที่จะทำการทดสอบย้อนกลับไปว่าเป็นการกระทำของผู้ใด

การแก้ไขหรือสับเปลี่ยนข้อมูลในแฟ้มข้อมูลนั้น โดยที่ในงานการประมวลผลข้อมูลส่วนมาก เมื่อคอมพิวเตอร์ได้รับข้อมูลนำเข้า เช่นหมายเลขบัญชีแล้ว คอมพิวเตอร์ก็จะต้องไปหาข้อมูลเพิ่มเติมจากแฟ้มข้อมูลหลัก ซึ่งเป็นแหล่งเก็บข้อมูล ฉะนั้น แม้ข้อมูลนำเข้าถูกต้อง ก็ยังอาจจะมีการคดโกงเกิดขึ้นได้ ถ้ามีการปลอมแปลงข้อมูลในแฟ้มข้อมูลหลัก เช่นถ้าลูกค้ามีสิทธิ์เบิกเงินเกินบัญชีอยู่จำนวนน้อย แต่มีการปลอมแปลงแฟ้มข้อมูลให้ระบุว่ามีวงเงินเกินบัญชีเป็นจำนวนมาก ลูกค้าคนนั้นก็อาจจะเบิกเงินเกินบัญชีได้มากกว่าที่ธนาคารอนุญาตไว้ เป็นต้น

การแก้ไขหรือสับเปลี่ยนข้อมูลในแฟ้มข้อมูล ซึ่งเป็นแหล่งเก็บข้อมูลที่อยู่ภายในเครื่องคอมพิวเตอร์นั้น การทุจริตในลักษณะนี้จะแตกต่างจากการปรุงแต่งข้อมูลนำเข้าเพื่อการบันทึกหรือ การแก้ไขโปรแกรมหรือคำสั่งโดยไม่มีอำนาจ การดำเนินการโดยวิธีนี้ เป็นการเข้าถึงโดยตรงที่ แฟ้มข้อ

มูลซึ่งอาจจะเป็นการแอบแก้ไขแฟ้มข้อมูลนั้น โดยใช้คำสั่งที่เขียนขึ้นเพื่อการนี้โดยเฉพาะ หรือใช้คำสั่งโดยทั่วไป การแก้ไขนี้อาจจะแก้ไขทั้งรายการที่เป็นตัวเงินหรือไม่เกี่ยวกับตัวเงินก็ได้ เป็นที่น่าสังเกตุว่า ถ้าการแก้ไขเป็นเรื่องที่ไม่เกี่ยวกับตัวเงินโดยตรง จะทำให้การค้นพบความผิดปกตินี้เป็นไปด้วยความยากลำบากมาก อีกวิธีหนึ่งที่จะทำการเปลี่ยนแปลงรายการของแฟ้มข้อมูลอาจจะเป็นการกระทำโดยการสับเปลี่ยนข้อมูลบางส่วนในแฟ้มข้อมูล ผู้ทุจริตอาจจะฉวยโอกาสทำ ขณะที่ทำการแก้ไขเพิ่มเติมข้อมูลให้เป็นปัจจุบัน(Up-date) โดยนำเทปหรือสิ่งใดก็ตามที่ใช้เก็บข้อมูลมาทำการประมวลแล้วทำการแก้ไขในระหว่างที่คอมพิวเตอร์กำลังทำการประมวลผลอยู่ การเปลี่ยนนี้อาจทำโดยคำสั่งพิเศษที่จัดเตรียมไว้

3.3.1.3. ความผิดฐานทำให้เกิดความเสียหายหรือทำลาย (Damage or Destruction)

การก่อปัญหาของไวรัสคอมพิวเตอร์(Computer Virus) ที่สำคัญที่สุดคือการก่อให้เกิดความเสียหาย หรือทำลายโปรแกรม หรือข้อมูลที่ถูกจัดเก็บอยู่ในคอมพิวเตอร์ รูปแบบการกระทำในลักษณะของไวรัสคอมพิวเตอร์ มีความแตกต่างจากการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในรูปแบบอื่นซึ่งผู้กระทำความผิดได้กระทำโดยการแสดงออกทางกายภาพ แต่ความเสียหายหรือการถูกทำลายข้อมูลหรือโปรแกรม โดยไวรัสคอมพิวเตอร์เป็นการกระทำที่ก่อผลดังกล่าวโดยใช้โปรแกรมซึ่งเป็นโปรแกรมอันตราย(Rogue Program,destructive computer program) ดังนั้นในขณะที่โปรแกรมไวรัสคอมพิวเตอร์ปฏิบัติการดังกล่าว จึงไม่สามารถที่จะมองเห็นได้โดยทางกายภาพ รวมถึงการสร้างความเสียหายนี้ ก็มิได้เจาะจงที่จะกระทำต่อข้อมูลหรือโปรแกรมใด ๆ โดยเฉพาะ ด้วยเหตุนี้จึงเกิดปัญหาที่ขึ้นว่า the Computer Fraud and Abuse Act of 1986 จะมีเจตนารมย์ที่จะให้ครอบคลุมถึงกรณีความผิดในการกระทำเกี่ยวกับไวรัสคอมพิวเตอร์ด้วยหรือไม่[29]

ตาม the Computer Fuand and Abuse Act 1986 มาตรา 1030(a)(5) ได้

---

29. Peter J. Denning, Computer Under Attack intruders,worms and viruses (USA.:Van Nostrand Reinhold Ltd.,1990) , p.72

บัญญัติว่า "การเข้าถึงโดยเจตนา ...ซึ่งการกระทำดังกล่าว ก่อให้เกิดความเสียหายหรือทำลายโปรแกรมหรือข้อมูล ที่เก็บอยู่ในคอมพิวเตอร์ของรัฐบาล" เป็นความผิด

การทำให้เกิดความเสียหายหรือทำลายทางคอมพิวเตอร์ในที่นี้ หมายถึงการทำให้เกิดความเสียหายหรือทำลายโปรแกรม หรือข้อมูล ที่มีการจัดเก็บอยู่ในคอมพิวเตอร์ ซึ่งโดยลักษณะของโปรแกรมหรือข้อมูลที่จัดเก็บอยู่ภายในนั้น จะอยู่ในลักษณะที่ไม่สามารถมองเห็น หรือจับต้องได้ ทั้งนี้ไม่รวมถึงอุปกรณ์ต่าง ๆ ของเครื่องคอมพิวเตอร์ที่เรียกว่าฮาร์ดแวร์

สิ่งสำคัญอีกประการหนึ่งของบทบัญญัติดังกล่าวคือ จะต้องกระทำ "โดยเจตนา" (Intentionally) ที่จะก่อให้เกิดความเสียหายหรือทำลายโปรแกรมหรือข้อมูลที่จัดเก็บอยู่ภายในคอมพิวเตอร์ การกระทำนี้ต้องประสงค์โดยตรงในการทำลาย หรือทำให้เกิดความเสียหายโปรแกรมหรือข้อมูลนั้น

อันที่จริงกฎหมายเกี่ยวกับคอมพิวเตอร์ของสหรัฐอเมริกาฉบับแรกคือ the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 ซึ่งได้กำหนดระดับของเจตนาร้าย (Mens rea) ที่กระทำให้เกิดความเสียหาย หรือทำลายข้อมูลหรือโปรแกรมคอมพิวเตอร์ไว้เพียง "โดยรู้" (Knowingly)

ต่อมาเจตนาร้ายดังกล่าวได้เปลี่ยนจากการกระทำ "โดยรู้" เป็น การกระทำ "โดยเจตนา" ซึ่งแก้ไขโดย the Computer Fraud and Abuse Act 1986 ทั้งนี้เพราะเกิดจากการผลักดันของนักคอมพิวเตอร์จำนวนมากให้เปลี่ยนแปลง และสภาคองเกสก็เห็นด้วยกับแนวความคิดของการเปลี่ยนแปลงดังกล่าว เนื่องจากทุกฝ่ายต่างเห็นว่าเป็นการง่ายมากที่กระทำเพียงอาศัยเจตนา "โดยรู้" ซึ่งก็จะเป็นความผิด

การกระทำที่จะหมายถึงการกระทำ "โดยรู้" (Knowingly) เมื่อผู้นั้นเพียงตระหนักว่า "ผลนั้นจะเกิดขึ้นอย่างแน่นอนอันนั้นเป็นผลมาจากการกระทำของตน ซึ่งอะไรก็ตามที่ผู้นั้นต้องการอาจจะก่อให้เกิดผลเช่นนั้น แต่สำหรับการกระทำ"โดยเจตนา" มีความหมายมากกว่าการกระทำเช่นนั้น ซึ่งหมายถึง บุคคลผู้ซึ่งกระทำให้เกิดผล โดยที่ตนเองประสงค์ในการกระทำ หรือเป็นสาเหตุของการกระทำ ดังนั้นการกระทำหรือสาเหตุที่เกิดขึ้น จะต้องเป็นวัตถุที่ประสงค์ต่อ อันมีอยู่ในจิตใจของผู้

กระทำ"30

นอกจากนี้สภาคองเกสของสหรัฐอเมริกา ยังได้วิตกถึงมาตรฐานของ"การรู้" ว่าอาจจะไม่เหมาะสมต่อคดีที่เกี่ยวข้องกับเทคโนโลยีคอมพิวเตอร์ เนื่องจากโดยธรรมชาติของเทคโนโลยีคอมพิวเตอร์เป็นสิ่งที่ไม่แน่นอน มีการพัฒนาไปอย่างรวดเร็ว ดังนั้นสภาคองเกสจึงได้พยายามที่จะต้องการยกระดับของเจตนาร้าย(Mens Rea) ให้สูงขึ้น ต่อกรณีความผิดเกี่ยวกับคอมพิวเตอร์30

และผู้ซึ่งกระทำความผิดฐานนี้ ต้องระวางโทษจำคุกไม่เกิด 5 ปี หรือปรับไม่เกิน 250,000 ดอลล่าร์

3.3.1.4. ปัญหาด้านกฎหมายเกี่ยวกับไวรัสคอมพิวเตอร์ของสหรัฐอเมริกา

นับตั้งแต่มีการพิจารณาออกกฎหมายฉบับแรกในความผิดอาญาเกี่ยวกับคอมพิวเตอร์คือ the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 จนกระทั่งมีการแก้ไขเพิ่มเติมโดย the Computer Fraud and Abuse Act of 1986 เหตุการณ์การกระทำเกี่ยวกับโปรแกรมไวรัสคอมพิวเตอร์ ยังมิได้นำไปพิจารณาเพื่อออกกฎหมายหรือปรับปรุงกฎหมายที่มีอยู่ให้ครอบคลุมถึงการกระทำความผิดเกี่ยวกับไวรัสคอมพิวเตอร์ เพราะก่อนหน้านี้โปรแกรมไวรัสคอมพิวเตอร์ยังปรากฏออกมาไม่มากนัก

จนกระทั่งในปี คศ. 1988 ก็ได้มีคดีความผิดที่เกี่ยวกับไวรัสคอมพิวเตอร์เกิดขึ้นเป็นครั้งแรก ที่ได้นำขึ้นสู่ศาลของสหรัฐอเมริกา โดยนาย โรเบิร์ต ที มอริส (Mr. Robert T. Morris) และทั้งระหว่างการพิจารณาคดีของศาล และภายหลังจากที่มีคำพิพากษา ได้มีการวิพากษ์วิจารณ์ของนักกฎหมายของอเมริกาเป็นจำนวนมาก จึงได้มีการเสนอร่างกฎหมาย the Computer Viruses Eradication Act เข้าสู่การพิจารณาของสภาคองเกส และเพื่อความเข้าใจถึงปัญหาทางกฎหมายของสหรัฐอเมริกาต่อกรณี การกระทำความผิดเกี่ยวกับไวรัสคอมพิวเตอร์ในคดีนี้ จึงขอกล่าวความเป็นมาของคดี และการวิเคราะห์กฎหมายของอเมริกา อันเป็นเหตุผลหนึ่งที่ทำให้มี

---

30. Daniel J. Kluth ,Ibid, p.303

สมาชิกสภาคองเกส เสนอที่จะออกกฎหมายมาเพื่อป้องกันการกระทำความผิด เกี่ยวกับไวรัสคอมพิวเตอร์ ดังนี้

นายโรเบิร์ต ที มอริส นักศึกษาได้เริ่มเข้าศึกษาในสาขาวิชาคอมพิวเตอร์ มหาวิทยาลัยเคอเนล ในฤดูใบไม้ร่วง ของปี คศ. 1988 ซึ่งหลาย ๆ คน ได้กล่าวว่าเขาเป็นนักโปรแกรมที่ชาญฉลาดคนหนึ่ง นายมอริส ได้มีการคิดอย่างลับ ๆ ในการที่จะสร้างโปรแกรมไวรัสคอมพิวเตอร์ และเขาก็ได้สร้างโปรแกรมดังกล่าว ซึ่งเป็นที่รู้จักกันเป็นอย่างดีในฐานะ "หนอนคอมพิวเตอร์" (Worm) หรือ มีผู้เรียกชื่ออย่างอื่น ว่า "ไวรัสระหว่างข่ายงาน" (internet virus) โดยได้ใส่โปรแกรมนี้เข้าไปในระบบการทำงานของ ยู-นิกซ์ (Unix) เมื่อวันที่ 2 พฤศจิกายน คศ. 1988

ภายหลังจากที่นายมอริส ได้ใส่ไวรัสคอมพิวเตอร์ประเภทนี้เข้าไปในคอมพิวเตอร์ ซึ่งมีการเชื่องโยงระหว่างกันทั่วประเทศแล้ว หนอนคอมพิวเตอร์ (Worm) ได้เข้าไปในเครือข่ายงานคอมพิวเตอร์แห่งชาติ ซึ่งเชื่อมต่อกับรัฐบาล บริษัทต่าง ๆ และคอมพิวเตอร์ของมหาวิทยาลัยซึ่งโปรแกรมที่ถูกเขียนขึ้นนี้ ถูกจดบันทึกอยู่ในระบบบัญชีของสถาบันเทคโนโลยีแมสซาชูเซ็ทช (the Massachusetts Institute of Technology) และเป็นสถานที่ซึ่งมีการปล่อยโปรแกรมชนิดนี้

นายโรเบิร์ต ที มอริส ได้กล่าวว่า เขาตั้งใจที่จะให้ไวรัสคอมพิวเตอร์ชนิดนี้แพร่ขยายข้ามข่ายงานไปอย่างช้า ๆ แต่มันกลับไม่เป็นดังที่เขาตั้งใจไว้ และเพื่อที่จะให้แน่ใจว่าโปรแกรมของเขาจะแพร่ขยายนั้นยังคงอยู่ เขาก็ได้กำหนดให้โปรแกรมหนอนคอมพิวเตอร์ (Worm) นี้ทำการคัดลอกตัวมันเองทุก ๆ ครั้งที่ 7 ที่มันเข้าเข้าไปในคอมพิวเตอร์เครื่องหนึ่ง และโดยการที่มีการคัดลอกตัวเองไปเรื่อย ๆ นี้เอง กลับบรากฏว่าเป็นสิ่งซึ่งเป็นอันตรายอย่างยิ่ง แม้แต่นายมอริสเองก็ยังประมาณอัตราการคัดลอกตัวเองของไวรัสคอมพิวเตอร์ชนิดนี้ต่ำไปมาก และได้มีผู้กล่าวว่าการคัดลอกตัวเองของหนอนคอมพิวเตอร์ (Worm) นี้อยู่ในความเร็วที่เกือบเท่ากับความเร็วของแสง[31] และทำให้หน่วยความจำในคอมพิวเตอร์เต็มอย่างรวดเร็ว (clogged) ดังนั้นจึงเป็นสาเหตุที่ทำให้คอมพิวเตอร์จำนวนมากหยุดการทำงาน (crash)

---

31. Susan M. Mell, Ibid, p.19

ดังเหตุที่เกิดขึ้นดังกล่าวจึงทำให้วงการคอมพิวเตอร์ ต้องเสียเวลาอันมีค่าในการที่จะต้องติดตาม เพื่อศึกษาและวิเคราะห์ไวรัสคอมพิวเตอร์ชนิดนี้ที่ได้ค้นพบ และวิธีที่จะกำจัดออกไปจากเครื่องคอมพิวเตอร์ ซึ่งโปรแกรมชนิดนี้ได้เข้าไปเป็นจำนวนมาก

โปรแกรมหนอนคอมพิวเตอร์ (Worm) ของนายมอริส อาจจะถูกมองในแง่ที่ดีกว่าโปรแกรมไวรัสคอมพิวเตอร์อื่น ๆ เนื่องจากมันไม่ได้เป็นสาเหตุของการทำลายที่ถาวรต่อฮาร์ดแวร์ใด ๆ หรือทำให้เสื่อมเสียหรือทำลายไฟล์ ข้อมูลใด ๆ แต่อย่างไรก็ตามแม้มันจะถูกมองในแง่ของสิ่งที่ดี แต่หนอนคอมพิวเตอร์ (Worm) ก็ยังคงเป็นสาเหตุของการทำให้เกิดความเสียหายที่สำคัญของการสูญเสียเวลาในการวิจัยอันมีค่า รวมถึงการต่อสู้และจำกัดโปรแกรมนี้ ซึ่งมีการประเมินกันว่ามีตัวเลขสูงถึง 186 ล้านเหรียญ[32]

และผลจากเหตุการณ์ที่เกิดขึ้น ได้มีการพิจารณาโต้แย้งกันเกี่ยวกับว่าจะมีกฎหมายใดหรือไม่ ที่จะนำมาปรับใช้ต่อการกระทำของนายมอริส เพราะผลที่เกิดขึ้นจากการกระทำของเขามีความรุนแรง แต่ก็ไม่สามารถที่จะตกลงกันได้ แม้แต่เจ้าหน้าที่ของสหรัฐไม่ว่าจะเป็นเจ้าหน้าที่สืบสวนกลาง (FBI) และเจ้าหน้าที่ด้านยุติธรรม (Department of Justice) ซึ่งต้องการที่จะชี้ให้เห็นว่าการกระทำดังกล่าวเป็นความผิดอาญาขั้นรุนแรง (felony) ในขณะที่สำนักงานอัยการของสหรัฐชี้ว่าเป็นความผิดอาญาขั้นเล็กน้อย (Misdemeanor)

การไต่สวนของคณะลูกขุนได้มีขึ้นที่ศาลในซีราคิวส์ (Syracuse) นิวยอร์ค ของเดือนมกราคม ปี 1990 ในที่สุดนาย มอริส ก็ได้ถูกพิพากษาถึงการกระทำที่ได้ใส่ไวรัสคอมพิวเตอร์เข้าไปในข่ายงานคอมพิวเตอร์ว่า การกระทำดังกล่าวเป็นความผิดตาม มาตรา 1030(a)(5)(A) ซึ่งบัญญัติว่า

"ผู้ใดก็ตาม เข้าถึงโดยเจตนาต่อคอมพิวเตอร์ที่รัฐใช้ประโยชน์ โดยปราศจากอำนาจ และโดยการกระทำเช่นนั้นได้เปลี่ยนแปลง ทำให้เกิดความเสียหาย หรือทำลายข้อมูลใด ๆ ที่เก็บ

---

32. Aaron Harber," Give No Quarter to Creator of Computer Virus," PC Week (Dec. 19910), p.51

อยู่ภายใน หรือขัดขวาง ผู้มีอำนาจใช้เครื่องคอมพิวเตอร์หรือข้อมูลใด ๆ และ โดยการกระทำเช่นนี้ (A) เป็นสาเหตุที่ก่อให้เกิดความเสียหายต่อคอมพิวเตอร์เครื่องหนึ่งหรือหลายเครื่อง มีมูลค่ารวมกัน 1,000 ดอลล่าร์ หรือ มากกว่า ในช่วงระยะเวลา 1 ปี "

ภายหลังจากที่ศาลชั้นต้นพิพากษาลงโทษนายมอริส โดยถือว่าการกระทำดังกล่าวเป็นความผิดตามมาตราดังกล่าวข้างต้นแล้ว นาย มอริส ได้อุทธรณ์ โต้แย้งภายใต้ปัญหาข้อกฎหมายของบทบัญญัติดังกล่าวโดยชี้ว่า การกระทำที่จะเป็นการกระทำความผิดตาม มาตรา 1030 (a)(5)(A) ได้นั้นไม่เพียงแต่ต้องมีเจตนาที่จะเข้าถึงคอมพิวเตอร์ที่รัฐใช้ประโยชน์เท่านั้น แต่จะต้องมีเจตนาที่จะเปลี่ยนแปลงทำให้เกิดความเสียหาย หรือทำลายข้อมูล หรือขัดขวางผู้มีอำนาจใช้เครื่องคอมพิวเตอร์หรือข้อมูลนั้นด้วย

ซึ่งจากคำอุทธรณ์ ของนายมอริส ในเบื้องต้นนั้น ผู้พิพากษา มันสัน (Munson) ได้กล่าวว่า "เจตนา" นั้นมิได้นำมาปรับใช้กับคำว่า "ทำให้เกิดความเสียหาย" แต่คำว่า "เจตนา" นี้เพียงแต่ต้องการขยาย "การเข้าถึง" เท่านั้น

ในการตีความกฎหมายดังกล่าว ในศาลชั้นต้นได้กำหนดว่า ไม่มีความจำเป็นที่จะต้องพิจารณาถึงที่มาของการออกกฎหมายเพราะกฎหมาย"ชัดเจนและไม่เคลือบคลุม" แต่อย่างไรก็ตามในชั้นอุทธรณ์ ไม่เห็นด้วยกับการระบุเช่นนั้น และกล่าวว่า ข้อความใน the Computer Fraud and Abuse Act "ไม่ชัดเจนเป็นอย่างมาก และเพื่อที่จะให้หมดข้อสงสัยจึงต้องทบทวนถึงประวัติของการออกกฎหมาย" และจากพิจารณาถึงเครื่องหมายวรรคตอนที่ใช้ในข้อความกฎหมาย ได้แสดงให้เห็นได้อย่างชัดเจนซึ่งหมายความว่ากริยาวิเศษ "โดยเจตนา" (intentionally) เป็นเพียงเจตนาที่ต้องการขยาย "การเข้าถึง" (access) และนอกจากนี้ ในการทบทวนประวัติของการออกกฎหมายได้ทำให้ศาลอุทธรณ์ สรุปว่า เจตนาที่เป็นสาเหตุที่ก่อให้เกิดความเสียหายไม่จำเป็นต้องนำมาใช้ ในการพิจารณาภายใต้ กฎหมาย ปี 1986

ในการทบทวนประวัติความเป็นมาของการออกกฎหมายปี คศ. 1986 เพื่อต้องการทราบถึงเจตนารมย์ของกฎหมาย ของคำว่า "โดยเจตนา" จะครอบคลุมไปถึงการก่อให้เกิดความเสียหายนั้นผู้กระทำต้องกระทำโดยมีเจตนาด้วยหรือไม่ อันเป็นที่ถกเถียงในหมู่นักกฎหมายของสหรัฐ

อเมริกาในขณะนี้นั้น ได้ย้อนไปถึงการแก้ไขกฎหมายปี คศ.1984 โดยได้แก้ไขในมาตรา 1030 (a)(3) เดิม ซึ่งต่อมาได้ถูกแทนที่โดยมาตรา 1030 (a)(5) ของกฎหมาย ปี คศ. 1986 ที่ใช้อยู่ในปัจจุบัน

ในปี คศ.1986 สภาคองเกส ได้มีการแก้ไขเรื่องเจตนาร้าย (Mens rea) ที่ผู้กระทำมี โดยเปลี่ยนจาก "โดยรู้" (Knowingly) เป็น "โดยเจตนา" (intentionally) เพื่อที่จะฟ้องบุคคลบางคนผู้ซึ่งเข้าถึงไฟล์หรือข้อมูลในคอมพิวเตอร์ของผู้อื่น มันเป็นที่แน่นอนว่าสภาคองเกสต้องการที่จะทำให้แน่ใจว่ากฎหมายได้ปรับใช้ต่อเฉพาะบุคคลที่มี เจตนาชัดแจ้งที่จะเข้าถึงคอมพิวเตอร์ของผู้อื่น ซึ่งไม่มีอำนาจใช้[33] ขณะที่เป็นความจริงว่าสภาคองเกสได้หยิบประเด็นการต้องการที่จะให้เป็น "โดยเจตนา"เพราะเป็นที่กังวลว่า มันจะเป็นการง่ายเกินไป ที่จะเป็นการเข้าถึงโดยปราศจากอำนาจ "โดยรู้"

โดยตาม กฎหมาย ปี 1984 เดิมต้องการเจตนาร้าย โดยใช้คำว่า "โดยรู้" (Knowingly) โดยบัญญัติไว้ทั้งก่อนหน้าวลี "การเข้าถึง" และ วลี "การทำให้เกิดความเสียหาย" [...โดยรู้ถึงการเข้าถึงโดยปราศจากอำนาจ ... และโดยรู้ว่าการกระทำเช่นนั้นเป็นการแก้ไขเปลี่ยนแปลงทำให้เกิดความเสียหาย ทำลาย ...] แต่เมื่อได้มีการแก้ไขกฎหมายในปี คศ. 1986 แล้วได้เปลี่ยนจากคำว่า "โดยรู้" เป็น "โดยเจตนา" และให้คงไว้หน้าวลี "การเข้าถึง" เพียงแห่งเดียวเท่านั้น

การบัญญัติเพิ่มเติมดังกล่าวจึงเป็นการสนับสนุนข้อสรุปของศาลที่ว่า เจตนาที่ต้องการนั้นเพียงปรับใช้กับการเข้าถึงเท่านั้น ถ้าในปี 1986 สภาคองเกสต้องการที่จะให้มีเจตนา (intent) ปรับใช้ทั้ง "การเข้าถึงและทำให้เกิดความเสียหาย" ในมาตรา 1030 (a)(5) แล้ว ศาลได้กล่าวว่าสภาคองเกสจะต้องใส่เจตนาร้ายเช่นนั้นก่อนทั้ง 2 วลี แต่สภาคองเกสก็ไม่ได้วางเจตนา (โดยเจตนา)ดังกล่าวไว้หน้า วลี "ทำให้เกิดความเสียหาย" (damage)

ทั้งหมดนี้จึงเป็นสิ่งที่ทำให้ศาลอุทธรณ์มีความเห็นว่า การก่อให้เกิดความเสียหายไม่จำเป็นต้องมีเจตนา แต่เพียงต้องมีผลมาจากการเข้าถึงโดยปราศจากอำนาจ เท่านั้น

---

33. Susan M. Mello,Ibid, p.269

นอกจากนี้นาย มอริส ยังได้โต้แย้งอีกว่าขณะที่โปรแกรมไวรัสคอมพิวเตอร์เข้าไปในข่ายงานคอมพิวเตอร์ เขามีอำนาจที่จะเข้าถึง (access) ดังนั้นเขาจึงไม่ตกอยู่ภายใต้การเข้าถึงโดยปราศจากอำนาจตามกฎหมาย และจากรายงานของวุฒิสมาชิก ถึงการร่วมเข้าแก้ไขกฎหมาย ปี คศ. 1984 ได้ระบุว่า มาตรา 1030 (a)(5) มีวัตถุประสงค์ไปที่บุคคลภายนอก แต่ศาลได้กล่าวว่าสภาคองเกสมิได้มีเจตนาไปถึง "บุคคลภายนอก"[34] เสียทั้งหมด ซึ่งจะเป็นการรับประกันในความรับผิดจากการเข้าถึงโดยมีอำนาจ

ตาม the Computer Fraud and Abuse Act กำหนดว่าบุคคลซึ่งกระทำความผิดตาม มาตรา 1030 (a)(5) อาจถูกปรับ และหรือถูกจำคุกไม่เกิน 5 ปี ในคดีนี้นายมอริส ถูกพิพากษาให้ถูกคุมความประพฤติ (Probation) เป็นเวลา 3 ปี และให้ทำงานบริการสาธารณะ (Community service) เป็นเวลา 400 ชั่วโมง และ ปรับเป็นเงิน 10,050 เหรียญ

อย่างไรก็ตามแม้จะมีคำพิพากษาในคดีนายมอริส ว่าการกระทำดังกล่าวเป็นการกระทำความผิดตามมาตรา 1030 (a)(5) แล้วก็ตาม ก็ได้มีนักกฎหมายเป็นจำนวนมากต่างวิพากวิจารณ์คำพิพากษาดังกล่าวว่าเป็นสิ่งที่ไม่ถูกต้อง[35] เพราะความจริงแล้วมาตรา 1030 (a)(5) ของกฎหมาย ปี คศ. 1984 ได้ถูกแทนที่โดยกฎหมายปัจจุบัน (กฎหมาย ปี 1986)โดยได้แบ่งแยกออกเป็นมาตรา 1030 (a)(3) และ (a)(5)

เดิมมาตรา 1030 (a)(3) ได้พูดถึงการเข้าถึงโดยปราศจากอำนาจ เช่น การบุกรุกและใช้ แก้ไขเปลี่ยนแปลง ทำลายข้อมูลจากคอมพิวเตอร์ของรัฐบาล ซึ่งมีความสับสนอยู่บางประการในถ้อยคำของกฎหมายปี 1984 ในมาตรา 1030 (a)(3) ที่สามารถใช้ต่อ "การกระทำที่เพียงแต่บุกรุก" ก็ถือเป็นความผิด หรือว่าจำเป็นที่ต้องการสิ่งที่แสดงเพิ่มขึ้นอีกว่าข้อมูลที่ถูกพบนั้น "ถูกใช้ แก้ไขเปลี่ยนแปลงทำลายหรือซ้อนเร้น"

เพื่อที่จะให้ความเคลือบคลุมนี้เกิดความชัดเจนขึ้น กฎหมาย ปี คศ. 1986 จึงได้แบ่งมาตรา 1030 (a)(3) ออก เพื่อว่า บทบัญญัติที่เกี่ยวกับการบุกรุกที่เข้มงวดเด็ดขาด ให้รวมอยู่ใน

---

34. Ibid, p.270

35. Ibid, p.273

มาตรา 1030 (a)(3) ใหม่ และกรณีที่มีผลที่เกิดขึ้นมาภายหลังการบุกรุกก็จะถูกห้าม โดยมาตรา 1030 (a)(5) แต่หากไม่มีผลที่เกิดขึ้นต่อมาภายหลังการเข้าถึงแล้ว ตามมาตรา 1030 (a)(5) ก็ไม่สามารถถูกฟ้องได้

ดังนั้น จึงเห็นได้ว่า ในมาตรา 1030(a)(3) เดิมนั้น มีวัตถุประสงค์อยู่ 2 ประการคือ

1. เพื่อที่จะลงโทษการบุกรุกที่เข้มงวด (to punish strict trespass) หรือ

2. เพื่อที่จะลงโทษผู้ซึ่งโดยรู้อยู่ว่าเป็นสาเหตุของการก่อให้เกิดความเสียหาย อันมีผลมาจากการเข้าถึง

เมื่อได้พิจารณาถึงที่มาของการออกกฎหมายแล้ว จะเห็นได้ว่าตามเหตุผลดังกล่าว เป็นการสนับสนุนว่าการทำให้เกิดความเสียหายนั้นจะต้องกระทำโดยเจตนา จึงจะถูกลงโทษโดยมาตรา 1030 (a)(5) และ วุฒิสภาก็ได้กล่าวไว้โดยเฉพาะว่า "ตามมาตรา 1030 (a)(5) ใหม่ ถูกกำหนดโดยตัวร่างกฎหมายซึ่ง ได้กำหนดเพื่อที่จะลงโทษผู้ซึ่งกระทำ "โดยเจตนา" เปลี่ยนแปลงทำให้เกิดความเสียหายหรือทำลาย ข้อมูลเกี่ยวกับคอมพิวเตอร์อันเป็นของบุคคลอื่น"[36] ดังนั้น เมื่อนายมอริสไม่มีเจตนาที่จะก่อให้เกิดความเสียหายดังที่เกิดขึ้น การกระทำของนายมอริสยอมไม่เป็นความผิดตามที่ศาลพิพากษา

นอกจากนี้ ยังมีปัญหาทางกฎหมายที่คั่งค้างอยู่ว่า ภายใต้กฎหมาย the Computer Fraud and Abuse Act of 1986 มีเจตนารมย์ที่จะครอบคลุมถึงกรณีของไวรัสคอมพิวเตอร์หรือไม่ ซึ่งในที่จริงแล้วกฎหมายฉบับนี้ มิได้มีเจตนารมย์ที่จะบริบาลกับ การกระทำความผิด เกี่ยวกับไวรัสคอมพิวเตอร์ ทั้งนี้เพราะกฎหมายมีเจตนาที่จะลงโทษ บุคคลผู้รุกล้ำเข้าไปในระบบคอมพิวเตอร์ของรัฐเท่านั้น[37]

อีกทั้งเจตนารมย์ของกฎหมายในขณะที่มีการร่างกฎหมายเกี่ยวกับคอมพิวเตอร์ฉบับแรก คือ the Conterfeit Access Device and Computer Fraud and Abuse Act of 1984 ก็มิได้กล่าวถึงหรือวิตกถึงการกระทำในรูปแบบของโปรแกรมไวรัสคอมพิวเตอร์ เพราะในขณะนั้นสภาพ

---

36. Ibid, p.273

37. Peter J. Denning,Ibid, p.480

ปัญหาของไวรัสคอมพิวเตอร์ยังไม่รุนแรง แม้กระทั่งมีการแก้ไขกฎหมายฉบับนี้โดย the computer fraud and abuse Act of 1986 ก็มิได้แก้ไขในปัญหานี้ จนกระทั่งในปี คศ. 1988 ปัญหาเกี่ยวกับไวรัสคอมพิวเตอร์จึงมีความรุนแรงขึ้น แต่กฎหมายที่จะใช้ในการลงโทษผู้กระทำผิดเช่นนี้โดยตรงยังไม่มี จึงอาจเป็นเหตุผลหนึ่งที่ศาลสหรัฐจำต้องตีความกฎหมายที่มีอยู่ให้ครอบคลุมถึงการกระทำเช่นนี้

เหตุผลอีกประการหนึ่งที่จะนำมาพิจารณาได้ว่า ทำไมกฎหมายอาญาของสหรัฐอเมริกาถึงล้มเหลวไม่อาจที่จะครอบคลุมถึงการกระทำเกี่ยวกับไวรัสคอมพิวเตอร์ได้ เพราะกฎหมายที่ใช้อยู่ปัจจุบัน กำหนดเป็นความผิดต่อการรุกล้ำเข้าไปในทรัพย์สิน ในรูปแบบที่เป็นพยานหลักฐานที่สามารถมองเห็นได้โดยทางกายภาพ[38] เช่น บ้าน หรือการที่ผู้เข้าถึงคอมพิวเตอร์นั่งอยู่หน้าจอคอมพิวเตอร์ ซึ่งผู้ออกกฎหมายต้องการที่จะคุ้มครอง และเมื่อกฎหมายดังกล่าวได้ผ่านออกมาเป็นกฎหมาย กฎหมายเหล่านี้ก็ได้มุ่งที่จะป้องกันการกระทำที่เห็นได้ทางกายภาพ ในการทำลายหรือกระทำอันตรายสิ่งอื่น ๆ โดยที่กฎหมายไม่ได้กำหนดรูปแบบความเสียหายที่อาจเกิดขึ้นได้จากการบุกรุกเข้าไปของสิ่งซึ่งไม่อาจจับต้องได้ เช่น ไวรัสคอมพิวเตอร์

แม้นาย มอริส จะสามารถที่จะอธิบายถึงประวัติความเป็นมาของ the Computer Fraud and Abuse Act of 1986 และเหตุผลที่ใช้สนับสนุนเขาเพียงใดก็ตาม แต่ในบางครั้งเมื่อบุคคลได้กระทำบางสิ่งบางอย่าง ที่เห็นได้ชัดจากสังคมว่าสิ่งนั้นเป็นความผิด การที่จะต้องรีบพิพากษาและลงโทษผู้กระทำผิด เพื่อที่จะสร้างตัวอย่างว่า บุคคลอาจจะถูกลงโทษได้ แม้ว่ากฎหมายซึ่งใช้พิพากษานั้น โดยพื้นฐานแล้วไม่ครอบคลุมถึงการกระทำเกี่ยวกับไวรัสคอมพิวเตอร์[39] ทั้งนี้เพราะนายมอริส เป็นบุคคลแรกที่ถูกฟ้องภายใต้กฎหมายฉบับนี้ ในการที่ได้ใส่โปรแกรมไวรัสเข้าสู่ระบบคอมพิวเตอร์ อีกทั้งไม่มีบรรทัดฐานที่จะตีความกฎหมายฉบับนี้ และประเภทของพฤติกรรมเช่นนี้ ซึ่งบางทีคำตัดสินของศาลที่พิพากษาไปเช่นนี้อาจจะมีปัญหาน้อยกว่า ถ้าหากศาลจะตัดสินว่า

38.Ibid, p.482

39. Peter J. Denning,Ibid, p.480

กฎหมายไม่ครอบคลุมถึงการกระทำเช่นนี้[40]

ปัญหาความไม่ชัดเจนของกฎหมายของสหรัฐอเมริกาเหล่านี้ จึงเป็นที่มาของการเรียกร้องให้สภาคองเกสออกกฎหมาย เพื่อปราบปรามการกระทำความผิดเกี่ยวกับไวรัสคอมพิวเตอร์ขึ้นมาโดยเฉพาะ และการเรียกร้องเหล่านี้ก็สัมฤทธิ์ผล เพราะขณะนี้ได้มีวุฒิสมาชิกของสภาคองเกสได้เสนอร่างกฎหมาย เพื่อบังคับใช้กับปัญหาไวรัสคอมพิวเตอร์ โดยหวังว่ากฎหมายดังกล่าวจะเป็นมาตรการหนึ่งที่จะช่วยปราบปรามการกระทำผิด และสร้างความมั่นใจให้กับวงการคอมพิวเตอร์ได้ในระดับหนึ่ง

3.3.2 ความรับผิดเกี่ยวกับคอมพิวเตอร์ของอังกฤษ

The Computer Misuse Act 1990 เป็นกฎหมายอาญาเกี่ยวกับการกระทำความผิดที่เกี่ยวข้องกับคอมพิวเตอร์ ฉบับแรกของประเทศอังกฤษ

พระราชบัญญัติ The computer Misuse Act นี้ได้รับการเห็นชอบผ่านรัฐสภาในระหว่างฤดูใบไม้ผลิของปี 1990 โดยกษัตริย์ของอังกฤษได้ลงนาม เมื่อวันที่ 20 มิถุนายน และได้เริ่มมีผลบังคับใช้ในวันที่ 29 สิงหาคม ปี 1990 the Computer Misuse Act 1990 การกระทำความผิดเกี่ยวกับคอมพิวเตอร์

the Computer Misuse Act 1990 ที่ใช้อยู่ในปัจจุบันกับปัญหากรณีไวรัสคอมพิวเตอร์ยังเป็นที่ถกเถียงกันอยู่ในหมู่นักกฎหมายของอังกฤษ ว่าจะครอบคลุมถึงการกระทำความผิดในกรณีนี้หรือไม่

ในการวิจัยส่วนนี้ จึงขอแสดงให้เห็นถึงกฎหมายเกี่ยวกับคอมพิวเตอร์ของประเทศอังกฤษและเนื้อหาที่สำคัญของกฎหมายฉบับนี้ เพื่อเป็นพื้นฐานความรู้ในอันที่จะนำมาวิเคราะห์การกระทำความผิด เกี่ยวกับไวรัสคอมพิวเตอร์ต่อไป

---

40. Martin Wasik,Ibid, p.7

ตาม the Computer Misuse Act 1990 ได้บัญญัติความผิดขึ้นมาใหม่ 3 ประการด้วยกัน การปรับปรุงกฎหมายอาญาดังกล่าวอาจเรียกได้ว่า เป็นการพัฒนากฎหมายอาญาครั้งใหญ่ที่สุด เพื่อที่จะรองรับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของอังกฤษ การปรับปรุงกฎหมายฉบับนี้รูปแบบส่วนใหญ่ได้มาจากการศึกษากฎหมายของสหรัฐอเมริกา ทั้งของรัฐบาลกลางและ ของมลรัฐต่าง ๆ[41] ซึ่งความผิดที่กำหนดขึ้นใหม่ คือ

1. ความผิดฐานเข้าถึงโดยปราศจากอำนาจ (Unauthorized access)
2. ความผิดฐานเข้าถึงโดยปราศจากอำนาจโดยมีเจตนาที่จะกระทำหรือเพื่อความสะดวกในการกระทำความผิดอื่น ๆ (Unauthorised access with intent to commit or facilitate commission of further offences)
3. ความผิดฐานเปลี่ยนแปลงโดยปราศจากอำนาจ (Unauthorised modification)

โดยความผิดแต่ละฐานความผิดมีรายละเอียดดังนี้

3.3.2.1. ความผิดฐานเข้าถึงโดยปราศจากอำนาจ

กฎหมายเกี่ยวกับความผิดทางอาญาของประเทศอังกฤษ ได้กำหนดความผิดฐานเข้าถึงโดยปราศจากอำนาจ ในการปรับปรุงรูปแบบที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์โดยเลือกการเริ่มต้นของการเข้าถึงเป็นความผิด มากกว่าที่จะกำหนดขอบเขตของความผิดเกี่ยวกับทรัพย์สิน ซึ่งบุคคลได้รับจากการเข้าถึงโดยปราศจากอำนาจ อาจมีอยู่ในจิตใจในขณะที่เข้าถึง

the Computer Misuse Act 1990 มาตรา 1 บัญญัติว่า

" (1) บุคคลจะมีความผิด เมื่อ

(เอ)เขากระทำให้คอมพิวเตอร์ปฏิบัติงานใดๆ ด้วยเจตนาที่เข้าถึงโปรแกรมหรือ

---

41. Martin Wasik, Ibid, p.69

ข้อมูลใด ๆ ซึ่งเก็บอยู่ในคอมพิวเตอร์

(บี) การเข้าถึงดังกล่าวเขาไม่ได้รับอนุญาต และ

(ซี) เขารู้ในขณะที่เขากระทำให้คอมพิวเตอร์ปฏิบัติงานนั้น..."

ตามบทบัญญัติดังกล่าวนี้ การกระทำของจำเลยที่จะเป็นความผิดได้นั้นจะต้อง "กระทำให้คอมพิวเตอร์ปฏิบัติอย่างใดอย่างหนึ่ง"(Cause a computer to perform any function) ในความหมายนี้ ไม่รวมถึงการสัมผัสทางกายภาพกับเครื่องคอมพิวเตอร์ และการตรวจดูข้อมูลโดยปราศจากการกระทำใด ๆ กับเครื่องคอมพิวเตอร์ เช่น การถ่ายความลับจากกระดาษที่ถูกพิมพ์ออกมาจากเครื่องคอมพิวเตอร์ หรือการอ่านข้อมูลที่ปรากฏอยู่บนจอภาพ ซึ่งกรณีเหล่านี้ กฎหมายไม่ครอบคลุมถึง

นอกจากนี้ ความผิดฐาน"เข้าถึงโดยปราศจากอำนาจ" ดังกล่าวไม่คำนึงถึงว่าจำเลยจะต้องประสบความสำเร็จจากการเข้าถึง อันได้เข้าสู่โปรแกรม หรือข้อมูลหรือไม่ หรือประสบความสำเร็จในการที่จะผ่านมาตรการรักษาความปลอดภัยของคอมพิวเตอร์หรือไม่

ในส่วนของผู้กระทำความผิด ซึ่งมีการสั่งการทางคอมพิวเตอร์โดยระยะทางไกล (remote) โดยในการสั่งการนั้น"เป็นเหตุให้คอมพิวเตอร์ได้ทำงานอย่างใดอย่างหนึ่ง" การกระทำเช่นนี้จะเป็นความผิดเมื่อมีการเข้าถึงโดยระยะทางไกล และเครื่องคอมพิวเตอร์สนองรับคำสั่งนั้น เช่น อุปกรณ์ที่ใช้ในการรักษาความปลอดภัยของคอมพิวเตอร์ทำงาน หรือการใส่รหัสเพื่อเข้าสู่ระบบของบรรดาลูกจ้างต่าง ๆ ที่จะก่อให้เกิดการปฏิบัติงานใด ๆ ของคอมพิวเตอร์ จะถือว่าการกระทำเช่นนั้นเป็นความผิดฐานเข้าถึง ทันทีที่เขาเปิดสวิตท์คอมพิวเตอร์ ถ้าหากพิสูจน์ได้ว่าเขากระทำโดยเจตนาในการเข้าถึงโดยปราศจากอำนาจ นอกจากนี้พระราชบัญญัติดังกล่าวยังรวมถึงการกระทำที่อาจจะตกอยู่ภายใต้ขอบเขตของการพยายามกระทำความผิดตามกฎหมายได้

การกระทำความผิดฐานเข้าถึงโดยปราศจากอำนาจ ประกอบด้วย สาระสำคัญ 2 ประการด้วยกันคือ

1. เจตนาที่จะเข้าถึงโปรแกรมหรือข้อมูลใด ๆ ที่เก็บไว้ในคอมพิวเตอร์ใด ๆ คำว่า "ใด ๆ " (Any) ทำให้เห็นได้ชัดว่า เจตนาไม่จำต้องสัมพันธ์กับคอมพิวเตอร์ซึ่ง

ผู้กระทำผิดได้กระทำการดังกล่าวในเวลานั้น โดยเจตนาที่บุคคลจะกระทำความผิดตามมาตรานี้ ไม่จำเป็นต้องกระทำต่อโปรแกรมหรือข้อมูลใดโดยเฉพาะ หรือโปรแกรมหรือข้อมูลชนิดใดชนิดหนึ่งโดยเฉพาะ[42]

และการกระทำดังกล่าวนี้รวมถึงผู้กระทำความผิด ผู้ซึ่งเข้าถึงคอมพิวเตอร์โดยปราศจากความผิดที่ชัดเจนแน่นอนว่า เขาจะพบโปรแกรมหรือข้อมูลในคอมพิวเตอร์นั้นหรือไม่

2. ผู้กระทำผิดความผิดจะต้องรู้ในขณะที่กระทำให้คอมพิวเตอร์ปฏิบัติงานใด ๆ ว่าเขาไม่มีอำนาจที่จะเข้าถึงโปรแกรมหรือข้อมูล

ดังนั้นในการที่จะฟ้องร้องผู้กระทำความผิดฐาน"เข้าถึงโดยปราศจากอำนาจ" โจทก์ จะต้องพิสูจน์ให้ศาลเห็นถึงสาระสำคัญทั้ง 2 ประการนี้ โดยอัตราโทษของความผิดนี้ the Computer Misuse Act 1990 มาตรา 1 (3) ได้กำหนดว่า "บุคคลซึ่งกระทำความผิดตามมาตรานี้ จะต้องระวางโทษจำคุก ไม่เกิน 6 เดือน หรือ ปรับไม่เกินระดับ 5 ของตารางมาตรฐานหรือทั้งจำทั้งปรับ"

3.3.2.2. ความผิดฐานเข้าถึงโดยปราศจากอำนาจ โดยมีเจตนาที่จะกระทำหรือเพื่อความสะดวกในการกระทำความผิดอื่นๆ

ความผิดฐานนี้เป็นความผิดฐานหนึ่งที่บัญญัติขึ้นใหม่ ตาม the Computer Misuse Act 1990 มาตรา 2 ซึ่งกำหนดว่า

"บุคคลมีความผิดตามมาตรานี้ ถ้าเขาได้กระทำความผิดตาม มาตราข้างต้น(ความผิดฐานเข้าถึงโดยปราศจากอำนาจ) โดยมีเจตนา

(เอ) กระทำความผิดซึ่งมาตรานี้ใช้บังคับได้ หรือ

(บี) ให้ความสะดวกต่อการกระทำความผิดของตนเอง หรือคนอื่นๆ

และความผิดที่เขาเจตนากระทำหรือให้ความสะดวก ที่ได้อ้างถึงตามมาตรานี้เป็นความผิดอื่นๆ..."

---

42. Ibid, p.212

ความผิดฐานเข้าถึงโดยปราศจากอำนาจ โดยมีเจตนาที่จะกระทำหรือเพื่อความสะดวกในการ ในการกระทำความผิดอื่นๆ ตามมาตรา 2 นี้ การกระทำความผิดจะต้องมีการเข้าถึงโดยปราศจากอำนาจตาม มาตรา 1 ก่อน ด้วยเจตนาที่จะกระทำหรือเพื่อความสะดวกในการกระทำความผิดอื่นๆ ที่มีความรุนแรงมากกว่า โดยไม่จำเป็นต้องพิสูจน์ว่า เจตนาที่จะกระทำความผิดอื่นๆ ต่อไปนั้น ได้มีการกระทำความผิดนั้นจริงหรือไม่ และความผิดที่มีเจตนามุ่งหมายสุดท้าย ซึ่งความผิดอันเป็นที่น่ากังวลเป็นอย่างยิ่งและมีมากที่สุดคือ การฉ้อโกง ลักทรัพย์และยักยอก

ตามความผิดฐานเข้าถึงโดยปราศจากอำนาจตามมาตรา 1 และความผิดฐานเข้าถึงโดยปราศจากอำนาจ โดยเจตนาที่จะกระทำความผิดอื่นๆ ตามมาตรา 2 เป็นความผิดที่ต่อเนื่องและลดหลั่นเป็นลำดับชั้นกัน ซึ่งมาตรา 2 เป็นการกระทำความผิดของจำเลย ผู้ซึ่งเข้าไปสู่สาระสำคัญ (ข้อมูลหรือโปรแกรม) ที่เก็บอยู่ในคอมพิวเตอร์ด้วยเจตนาที่จะกระทำความผิดที่รุนแรง ในการฟ้องผู้กระทำความผิดตามมาตรานี้ หากปรากฏต่อมาภายหลัง การพิสูจน์ได้ความว่า ไม่สามารถลงโทษ ผู้กระทำความผิดตามมาตรานี้ แต่หากเข้าองค์ประกอบของมาตรา 1 (ความผิดฐานเข้าถึงโดยปราศจากอำนาจ) ความผิดที่ฟ้องนี้อาจถูกลงโทษตามมาตรา 1 ได้

ความผิดตามมาตรา 2 จะเป็นความผิดสำเร็จไม่ว่า ความผิดที่มุ่งหมายที่จะกระทำต่อนี้อาจจะต้องเผชิญกับการกระทำของจำเลย ซึ่งได้กระทำความผิดที่มีเจตนากระทำต่อไปนั้น จะกระทำในขณะที่เกือบจะเป็นเวลาเดียวกับการเข้าถึงโดยปราศจากอำนาจ เช่น จำเลยได้เข้าถึงสาระสำคัญที่เก็บอยู่ในคอมพิวเตอร์ เพื่อที่จะเปลี่ยนแปลงข้อมูลบัญชีธนาคารซึ่งตนเองเป็นเจ้าของในขณะนั้น หรือในโอกาสต่อมา เช่น จำเลยได้รับข้อมูลซึ่งเป็นความลับเกี่ยวกับบุคคลที่ถูกบันทึกอยู่ในคอมพิวเตอร์โดยมีเจตนาที่จะรีดทรัพย์เขาในอนาคต

ผู้กระทำความผิดฐานเข้าถึงโดยปราศจากอำนาจ โดยมีเจตนาที่จะกระทำ หรือ เพื่อความสะดวกในการกระทำผิดอื่น ๆ ตามมาตรา 2 (5) กำหนดโทษจำคุกไม่เกิน 5 ปี หรือ ปรับไม่เกินขั้นสูงตามที่กฎหมายกำหนด หรือ ทั้งจำทั้งปรับ

3.3.2.3. ความผิดฐานเปลี่ยนแปลงโดยปราศจากอำนาจ (Unauthorized modification)

ตามบทบัญญัติของ the Computer Misuse Act 1990 มาตรา 3 บัญญัติไว้ว่า "บุคคลมีความผิดเมื่อ

(เอ)เขากระทำการใด ๆ ซึ่งก่อให้เกิดการเปลี่ยนแปลงในเนื้อหาของคอมพิวเตอร์ใดๆ โดยปราศจากอำนาจ ..."

ความผิดตามบทบัญญัตินี้ได้วางขอบเขตที่กว้างขวางถึงรูปแบบที่แตกต่างของการกระทำที่ถูกรวมอยู่ภายใต้ของการ "เปลี่ยนแปลง" ซึ่งจะครอบคลุมถึง คดีที่เกี่ยวข้องกับการกระทำโดยเจตนาทั้งหมดที่ได้กระทำในสิ่งที่เรียกว่า "การเปลี่ยนแปลง"

ตามมาตรา 17(7) ได้ให้คำนิยามของคำว่า "การเปลี่ยนแปลง"(Modification)ว่า

"การเปลี่ยนแปลงเนื้อหา(contents) ของคอมพิวเตอร์ใดเกิดขึ้น ถ้าการเกิดขึ้นนั้นมีผลต่อการปฏิบัติงานใด ๆ ของคอมพิวเตอร์ ซึ่งมีผลต่อคอมพิวเตอร์นั้น หรือคอมพิวเตอร์อื่น ๆ

(เอ) โปรแกรมหรือข้อมูลใด ๆ ที่เก็บอยู่ในคอมพิวเตอร์มีผลให้ถูกแก้ไขหรือถูกลบ หรือ

(บี) โปรแกรมหรือข้อมูลใด ๆ ถูกเพิ่มเข้าไป

และการกระทำใด ๆ ซึ่งมีส่วนที่เป็นสาเหตุให้เกิดการเปลี่ยนแปลง จะถูกพิจารณาว่าเป็นสาเหตุที่ก่อให้เกิดการเปลี่ยนแปลง"

บุคคลซึ่งจะกระทำอันเป็นความผิดฐานนี้จะต้องกระทำโดยเจตนาที่จะก่อให้เกิดการเปลี่ยนแปลงในเนื้อหาของคอมพิวเตอร์ และในการกระทำเช่นนี้

1. ทำให้เกิดความเสียหายแก่การปฏิบัติงานของคอมพิวเตอร์

2. เพื่อกีดกันหรือขัดขวาง การเข้าถึงโปรแกรมหรือข้อมูลที่เก็บอยู่ในคอมพิวเตอร์ หรือ

3. ทำให้เกิดความเสียหาย แก่การปฏิบัติการของโปรแกรมหรือความเชื่อถือใด ๆ ของข้อมูลและการกระทำโดยเจตนา ดังกล่าวก็ไม่จำต้องมีเจตนาที่จะกระทำโดยตรงต่อ

(1) คอมพิวเตอร์ใด ๆ โดยเฉพาะ

(2)โปรแกรมหรือข้อมูลหนึ่งข้อมูลใด หรือโปรแกรมหรือข้อมูลชนิดใดชนิดหนึ่งโดยเฉพาะ หรือ

(3) แก้ไขเปลี่ยนแปลงอย่างหนึ่งอย่างใดโดยเฉพาะ หรือแก้ไขเปลี่ยนแปลงชนิดใดชนิดหนึ่งโดยเฉพาะ

โดยการกระทำนี้ผู้กระทำต้องรู้ว่า การเปลี่ยนแปลงดังกล่าวตนไม่มีอำนาจที่จะกระทำเช่นนั้นได้ และโดยไม่ต้องคำนึงว่าการเปลี่ยนแปลงโดยปราศจากอำนาจ หรือผลที่ เจตนา ที่จะให้เกิดขึ้น จะเกิดขึ้นเพียงชั่วคราว หรือ ถาวร

ความผิดฐานนี้ยังมีความเกี่ยวข้องสัมพันธ์ระหว่างการกระทำความผิดฐานนี้ กับการกระทำความผิดเกี่ยวกับความเสียหายทางอาญา ตาม the Criminal Damage Act 1971 โดย the Computer Misuse Act 1990 ได้กำหนดให้การเปลี่ยนแปลงในเนื้อหาของคอมพิวเตอร์ จะไม่ถือว่าเป็นการที่ก่อให้เกิดความเสียหายแก่คอมพิวเตอร์ใด ๆ ตาม the Criminal Damage Act 1971 เว้นแต่จะมีผลต่อคอมพิวเตอร์ ในทางกายภาพเท่านั้น

บุคคลผู้ซึ่งกระทำความผิดฐานเปลี่ยนแปลงโดยปราศจากอำนาจนี้ ต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกินขั้นสูงที่กฎหมายกำหนดไว้ หรือทั้งจำทั้งปรับ

มีนักกฎหมายของอังกฤษบางท่านกล่าวว่า[43] ความผิดในมาตรานี้สามารถที่จะขยายไปถึงคดีที่จำเลยนำโปรแกรมไวรัสคอมพิวเตอร์ เข้าไปสู่ระบบคอมพิวเตอร์หรือข่ายงานคอมพิวเตอร์ อันก่อให้เกิดความเสียหายแก่การใช้งาน ซึ่งมีผลคล้าย ๆ กับการกีดกัน หรือขัดขวางการเข้าถึงของผู้มีอำนาจตามกฎหมายที่จะใช้

และภายในมาตรานี้ การที่มีเจตนาที่จะนำไวรัสเข้าสู่ระบบคอมพิวเตอร์ เช่น นาย ก. ได้ใส่ไวรัสคอมพิวเตอร์เข้าไป โดยเจตนาที่จะใส่เข้าไปสู่ เพื่อให้แพร่หลายแก่แผ่นดิสก์ และนาย ข. ผู้บริสุทธิ์ได้ใช้แผ่นดิสก์นั้นในคอมพิวเตอร์ของตน ทำให้เกิดความเสียหาย จากการกระทำเช่นนี้ นาย ก.จะต้องรับโทษสำหรับการกระทำของเขา ในเวลาที่เขาได้ใส่ไวรัสคอมพิวเตอร์ลงในแผ่นดิสก์ และได้มอบให้แก่ผู้อื่นทั้งนี้เพราะ มาตรา 17 (7) ได้ระบุว่าการกระทำใด ๆ ซึ่งได้มีส่วนอัน

43.Martin Wasik,Ibid, p.215

เป็นสาเหตุโดยตรงต่อการเปลี่ยนแปลง ที่จะถูกพิจารณาว่าสาเหตุเกิดจากกระทำนี้ และนอกจากนี้ ความรับผิดของนาย ก. จะไม่ถูกกระทบกระเทือนแม้นาย ข. ซึ่งมิได้ใช้แผ่นดิสต์นั้น แต่ ได้ผ่านแผ่นดิสต์นั้นแก่นาย ค หรือบุคคลอื่นผู้บริสุทธิ์ และได้ก่อให้เกิดความเสียหายแก่เครื่องคอมพิวเตอร์ของนาย ค. หรือ บุคคลอื่น ๆ ทั้งนี้เพราะตาม the Computer Misuse Act 1990 ไม่คำนึงว่าเจตนาของนาย ก จะประสงค์โดยตรงต่อคอมพิวเตอร์หรือโปรแกรม หรือข้อมูลใด ๆ โดยเฉพาะ

พระราชบัญญัติดังกล่าวได้พยายามที่จะหลีกเลี่ยงปัญหาการลบ ปลอม หรือฉ้อฉลข้อมูลหรือโปรแกรม ในอันจะถูกเรียกร้องให้พิสูจน์เกี่ยวกับความเสียหาย ที่เกิดขึ้นต่อวัตถุที่จับต้องได้จึงใช้คำว่า"เนื้อหา" (Contents) ที่เก็บอยู่ในหน่วยความจำของคอมพิวเตอร์ หรือวัตถุที่เป็นตัวเก็บความจำของคอมพิวเตอร์ กรณีดังกล่าวถือได้ว่าเป็นการแก้ปัญหา ได้ดีกว่าทางเลือกอื่น ๆ ที่จะแก้ไข the Criminal Damage Act 1971 โดยจะขยายคำนิยามของคำว่า "ทรัพย์สิน" ที่จะให้รวมไปถึงสาระสำคัญ(material) ที่ถูกเก็บไว้ในคอมพิวเตอร์ซึ่งไม่สามารถจับต้องได้ ซึ่งคณะกรรมาธิการร่างกฎหมายฉบับดังกล่าวได้กล่าวว่า the Criminal Damage Act 1971 ไม่เหมาะสมจริง ๆ ที่จะนำมาแก้ไขกับการกระทำต่อสิ่ง ซึ่งไม่มีรูปร่าง เช่น โปรแกรมหรือข้อมูล การที่ต้องแยกกฎหมายดังกล่าวออกมาจึงเป็นวิธีการที่ดีที่สุด[44]

อย่างไรก็ตาม มีนักกฎหมายของอังกฤษบางท่านได้กล่าวว่า the Computer Misuse Act 1990 มิได้บัญญัติไว้ให้ชัดเจนที่จะให้มีผลครอบคลุมถึงการกระทำกรณีไวรัสคอมพิวเตอร์ด้วย ทั้งตัวบทและเจตนารมย์ของกฎหมาย (ซึ่งปัญหากฎหมายของอังกฤษต่อกรณีไวรัสคอมพิวเตอร์ จะได้กล่าวต่อไป)

3.3.2.4 ปัญหาด้านกฎหมายเกี่ยวกับไวรัสคอมพิวเตอร์อังกฤษ

the Computer Misuse Act 1990 เป็นกฎหมายของประเทศอังกฤษฉบับแรกที่เกี่ยวกับคอมพิวเตอร์ โดยได้กำหนดความผิดขึ้นใหม่ 3 ฐานความผิดคือ

---

44. Ibid, p.143

1. ความผิดเกี่ยวกับการเข้าถึงโดยบราศจากอำนาจ โดยเข้าถึงสาระสำคัญที่เก็บอยู่ในคอมพิวเตอร์ (โปรแกรม,ข้อมูล) ความผิดนี้มีโทษจำคุกไม่เกิน 6 เดือน และหรือปรับไม่เกินระดับ 5 ของเกณฑ์มาตรฐาน

2. ความผิดเกี่ยวกับการเข้าถึงโดยบราศจากอำนาจ โดยมีเจตนาที่จะกระทำหรือเพื่อความสะดวกในการกระทำความผิดอื่น โดยมีโทษจำคุกไม่เกิน 5 ปี และหรือ ปรับไม่เกินอัตราที่กฎหมายกำหนดไว้สูงสุด

3. ความผิดเกี่ยวกับการเปลี่ยนแปลงสาระสำคัญในคอมพิวเตอร์โดยบราศจากอำนาจ โดยการกระทำเช่นนี้มีโทษจำคุกไม่เกิน 5 ปี และหรือปรับไม่เกินอัตราที่กฎหมายกำหนดไว้สูงสุด

นอกจากนี้ตามรายงานของคณะกรรมาธิการกฎหมาย ยังกล่าวด้วยว่ากฎหมายฉบับนี้สามารถที่จะปรับใช้ได้กับบุคคลซึ่งมีเจตนาเฉพาะ ในการกระทำที่ได้ใส่ซอฟต์แวร์อันตรายเข้าไปในคอมพิวเตอร์[45] โดยผู้เขียนโปรแกรมต่าง ๆ สามารถที่จะถูกฟ้องได้ด้วยสาเหตุที่ก่อให้เกิดการเปลี่ยนแปลงโดยบราศจากอำนาจ ต่อเนื้อหาของคอมพิวเตอร์ อันเนื่องมาจากติดโปรแกรมไวรัสคอมพิวเตอร์นั้น ทั้งนี้ไม่ว่าบัญหาเกี่ยวกับกฎหมายมีขอบเขต ที่จะลงโทษผู้เขียนโปรแกรมสามารถที่จะกำหนดความรับผิดสำหรับการกระทำเกี่ยวกับไวรัสคอมพิวเตอร์ของเขา หรือไม่ ตามมาตรา 3 ของ the Computer Misuse Act 1990 ซึ่งเป็นปัญหาที่น่าสนใจที่จะต้องติดตามกันต่อไป

กฎหมายฉบับนี้ไม่มีผลย้อนหลังไปถึงการกระทำที่ก่อให้เกิดขึ้น กฎหมายฉบับนี้มีผลใช้บังคับอย่างในกรณีที่มีการใส่โปรแกรมไวรัสเข้าไปภายใน ก่อนที่กฎหมายใช้บังคับก็ไม่สามารถลงโทษบุคคลนั้นได้

เหตุผลประการหนึ่ง ซึ่งทำให้นักกฎหมายของอังกฤษ เชื่อว่า the Computer Misuse Act 1990 สามารถที่จะปรับใช้ได้กับกรณีของไวรัสคอมพิวเตอร์ เพราะตามพระราชบัญญัติที่ใช้คำซึ่งมีความหมายที่กว้างขวางเกี่ยวกับ การเข้าถึงโดยบราศจากอำนาจ และการเปลี่ยนแปลงโดยบราศจากอำนาจ ดังนั้น หากมีคดีเกิดขึ้นก็สามารถที่จะคาดได้ว่า จะอยู่ภายใต้คำนิยามของกฎหมายฉบับนี้ที่

---

45. Springer ,Ibid, p.234

สามารถปรับใช้ได้

จะเห็นได้ว่าพระราชบัญญัติฉบับนี้กำหนดไว้โดยเฉพาะถึงความผิดเกี่ยวกับการเข้าถึงโดยปราศจากอำนาจหรือการก่อให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ แต่อย่างไรก็ตามมีนักกฎหมายส่วนหนึ่งได้ตั้งข้อสงสัยว่า กฎหมายฉบับนี้ ได้รวมถึงการกระทำความผิดที่มีความสัมพันธ์กับการกระทำเกี่ยวกับไวรัสคอมพิวเตอร์หรือไม่ โดยเฉพาะมีปัญหาถึงการบัญญัติกฎหมายที่ไม่ชัดเจนเกี่ยวกับว่า[46]

1. ผู้เขียนโปรแกรมไวรัสคอมพิวเตอร์ที่กำลังแพร่ระบาดอยู่ จะมีความผิดหรือไม่
2. การสร้างและดึงโปรแกรมไวรัสคอมพิวเตอร์เพื่อวัตถุประสงค์ของการวิจัย จะเป็นความผิดหรือไม่
3. หากขณะที่มีการทำวิจัยเกี่ยวกับไวรัสคอมพิวเตอร์ ได้มีไวรัสคอมพิวเตอร์หลุดรอดออกไป ผู้เขียนโปรแกรมจะต้องรับผิดต่อความเสียหายหรือไม่
4. ในการดึงโปรแกรมไวรัสคอมพิเตอร์ ซึ่งมีลักษณะที่ดี (อาจใช้ประโยชน์) จะถือว่าเป็นความผิดหรือไม่
5. ถ้าผู้ใช้ คอมพิวเตอร์ขาดความระมัดระวัง เป็นเหตุให้ติดเชื้อไวรัส ผู้นั้นจะมีความผิดหรือไม่

คำถามเหล่านี้ อาจจะมีผู้ที่ตอบไปได้ต่าง ๆ นานา ภายใต้ขอบเขตของ the Computer Misuse Act 1990 ซึ่งปัญหาเหล่านี้ยังไม่เคยมีตัวอย่างขึ้นสู่ศาลของอังกฤษ ดังนั้น จึงจำเป็นอย่างยิ่งที่จะต้องรอดูผลของคำพิพากษาของศาล ในอันที่จะชี้ขาดว่า กฎหมายที่ใช้อยู่สามารถที่จะครอบคลุมการกระทำเกี่ยวกับไวรัสคอมพิวเตอร์เพียงใด เพื่อใช้เป็นแนวบรรทัดฐานของคดีต่อไป

---

46. Ibid, p.234

3.3.3 ความรับผิดเกี่ยวกับไวรัสคอมพิวเตอร์ของอเมริกา

ในขณะที่หลายมลรัฐของสหรัฐอเมริกา ได้ออกกฎหมายเพื่อป้องกันการกระทำความผิดเกี่ยวกับไวรัสคอมพิวเตอร์เรียบร้อยแล้ว สมาชิกสภาคองเกสก็ได้เสนอกฎหมายเพื่อใช้ในการปราบปรามการกระทำความผิดเกี่ยวกับไวรัสคอมพิวเตอร์เช่นเดียวกัน โดยร่างกฎหมายดังกล่าวใช้ชื่อว่า The Computer Virus Eradication Act of 1989 โดยร่างกฎหมายฉบับนี้ได้เสนอเพื่อเพิ่มเติมกฎหมายปี 1986 ซึ่งเนื้อหายังคงมีอยู่เช่นเดิมมิได้เปลี่ยนแปลง โดยได้กำหนดขึ้นเพื่อใช้อุดช่องว่างของกฎหมาย ซึ่งไม่ได้มีการคาดคิดไว้ก่อนเกี่ยวกับปัญหาไวรัสคอมพิวเตอร์ 47

The Computer Virus Eradication Act หรือกฎหมายกำจัดไวรัสคอมพิวเตอร์นี้ ได้เสนอสาระสำคัญเพิ่มขึ้น 2 ประการ จากกฎหมายปี 1986 คือ

1. ความผิดฐานใส่ไวรัสคอมพิวเตอร์เข้าสู่คอมพิวเตอร์
2. ความผิดฐานมอบโปรแกรมไวรัสคอมพิวเตอร์

และนอกจากนี้ ยังมีบทบัญญัติเกี่ยวกับการชดใช้ค่าเสียหายทางแพ่งให้แก่ผู้ได้รับความเสียหาย

3.3.3.1 การกระทำความผิดฐานใส่ไวรัสคอมพิวเตอร์เข้าสู่คอมพิวเตอร์

สำหรับบทบัญญัติที่เกี่ยวกับการใส่ไวรัสคอมพิวเตอร์ คือการกำหนดถ้อยคำเพื่อที่จะเป็นการห้ามบุคคลมิให้ใส่โปรแกรมไวรัสคอมพิวเตอร์เข้าไปในโปรแกรมสำหรับคอมพิวเตอร์หรือเครื่องคอมพิวเตอร์

47.Lance J. Denning, ROGUE PROGRAMS viruses, worms and trojan horses (USA.: Van Nostrand Reinhold Ltd, 1990), p.75.

มีปัญหาหลายประการซึ่งเกิดขึ้น ในขณะที่ผู้บัญญัติกฎหมายและผู้สนับสนุนในการแก้ไขกฎหมายที่มีอยู่ในขณะนี้ หรือพยายามที่จะออกกฎหมายที่ทันสมัยต่อเทคโนโลยีสมัยใหม่ เพื่อที่จะใช้บังคับกับโปรแกรมไวรัสคอมพิวเตอร์

สิ่งที่สำคัญที่สุดในการริเริ่มการออกกฎหมาย คือการที่จะใช้ถ้อยคำใด ที่จะให้ตรงมากที่สุดสำหรับการกระทำต่าง ๆ ที่จะถูกห้ามมิให้กระทำ โดยเฉพาะอย่างยิ่งที่จะรวมพฤติกรรมที่มิชอบ ซึ่งจะเห็นได้จากการสอดแทรกไวรัสคอมพิวเตอร์ประเภทหนอนคอมพิวเตอร์ (Worm) เข้าไปในข่ายงานคอมพิวเตอร์ โดยเฉพาะอย่างยิ่งผู้ออกกฎหมายจะต้องตัดสินใจว่า จะให้จำกัดความเป็นการทั่วไปหรือเป็นพิเศษ สำหรับการฝ่าฝืนซึ่งจะถูกห้ามมิให้กระทำ โดยถ้อยคำที่ใช้ในการออกกฎหมายได้รับการเสนอขึ้นมา รวมถึงข้อความดังต่อไปนี้ [48]

- "เข้าครอบครอง" (take possesion of)
- "เข้ายุ่งเกี่ยว" (tampers with)
- "ทำให้เสื่อม" หรือ "ทำให้ไร้ความสามารถ" (degrades or disables)
- "รบกวนหรือก่อให้เกิดการรบกวนหรือการเสื่อมลงของการบริการทางคอมพิวเตอร์" (disrupts or causes the disruption or degrates of computer services)
- "ขัดขวางการปฏิบัติงาน (ของ)" [interrupt (s) the operation (of)] หรือ "ก่อให้เกิดการปฏิบัติงานโดยผิดปกติ (ของ)" [cause the malfunction (of)]
- "คัดลอกตัวเอง หรือ แพร่พันธุ์ด้วยตัวเอง" (self-replication or self-propagating) และ "ถูกกำหนดให้เข้าไปปะปนเพื่อให้ใช้การไม่ได้... ทำให้สิ้นเปลืองไปซึ่งทรัพยากรของคอมพิวเตอร์... หรือ... เข้ายึดการปฏิบัติงานปกติของคอมพิวเตอร์" (designed to contaminate...

48.Lance J. Denning, Ibid., p.77

consume computer resources... or.. usurp the normal operation of the computer"

และในที่สุดก็ได้เลือกการกระทำที่จะเป็นการสร้างไวรัสคอมพิวเตอร์ โดยใช้ถ้อยคำว่า "ใส่"(inserts) ซึ่งถือว่าเป็นการบัญญัติที่มีความกว้างพอที่จะครอบคลุมถึง การกระทำเกี่ยวกับโปรแกรมไวรัสคอมพิวเตอร์ที่ก่อให้เกิดความเสียหายได้มากที่สุด[49] ตามร่าง the Computer Virus Eradication Act of 1989 ได้บัญญัติว่า

"โดยเจตนา -

(เอ) ใส่เข้าไปในโปรแกรมสำหรับคอมพิวเตอร์, หรือในเครื่องคอมพิวเตอร์เอง, ซึ่งข้อมูลหรือคำสั่ง, โดยรู้ว่าหรือมีเหตุผลอันเชื่อได้ว่า ข้อมูลหรือคำสั่งดังกล่าว อาจก่อให้เกิดความเสียหาย, ค่าใช้จ่าย หรือเสี่ยงต่อสุขภาพหรือสวัสดิภาพ

(1) ของผู้ใช้คอมพิวเตอร์ดังกล่าว หรือคอมพิวเตอร์ซึ่งใช้โปรแกรมดังกล่าวปฏิบัติงาน หรือต่อผู้ที่เชื่อถือข้อมูลที่ผ่านกระบวนการในคอมพิวเตอร์ดังกล่าว

(2) ของผู้ใช้คอมพิวเตอร์อื่น ๆ หรือบุคคลผู้ซึ่งเชื่อถือข้อมูลที่ผ่านกระบวนการในคอมพิวเตอร์อื่น ๆ

ถ้าการใส่...ข้อมูลหรือคำสั่งนั้นมีผลกระทบหรือถูกทำให้เกิดผล หรือผลอย่างอื่นไปอีกโดยวิถีทางพาณิชย์ระหว่างมลรัฐ หรือการพาณิชย์ระหว่างประเทศ"

ประการแรก ที่น่าจะพิจารณาถึงร่างกฎหมาย the Computer Virus Eradication Act 1989 คือการกระทำที่เกี่ยวกับไวรัสคอมพิวเตอร์ที่จะถือว่ากระทำความผิด คือ การห้ามมิให้นักโปรแกรมหรือนักคอมพิวเตอร์ "ใส่" (inserts) โปรแกรมไวรัสเข้าไปใน

49.The Computer Virus Eradication Act of 1989, Ibid., p.736

โปรแกรมซอฟต์แวร์หรือคอมพิวเตอร์ อันมีวัตถุประสงค์ที่จะสร้างความเสียหายให้แก่คอมพิวเตอร์อื่น ๆ การกระทำที่กำหนดไว้อันเป็นความผิด ยังได้ห้ามไปถึงโปรแกรมซึ่งเป็นแบบพิมพ์ของไวรัส ซึ่งเป็นสาเหตุของการสูญเสียต่อบุคคลผู้ซึ่งเชื่อถือในข้อมูลที่ผ่านกระบวนการ โดยคอมพิวเตอร์ที่ติดไวรัสคอมพิวเตอร์ด้วย [50]

ตามบทบัญญัตินี้ลงโทษผู้กระทำความผิด เพียงถ้าโปรแกรมนี้ถูกใส่เข้าไปเท่านั้น โดยผู้กระทำไม่จำเป็นต้องรู้ถึงความเสียหายที่ได้รับ [51]

ตามร่างกฎหมายกำจัดไวรัสคอมพิวเตอร์ได้กำหนดการ "ใส่" หรือการปล่อยไวรัสคอมพิวเตอร์ ถ้าหากการกระทำเช่นนี้มีผลกระทบต่อธุรกิจระหว่างมลรัฐหรือระหว่างประเทศเป็นความผิด ซึ่งได้ถูกเสนอในฐานะเป็นเครื่องมืออย่างหนึ่งให้ผู้กระทำละเว้นการกระทำผิด ทั้งนี้เนื่องจากการที่จะติดตามไวรัสคอมพิวเตอร์ ไปสู่ผู้เริ่มต้นนั้นเป็นการยาก [52]

โดยลักษณะของไวรัสคอมพิวเตอร์แล้ว เป็นการยากที่จะนำผู้ปล่อยไวรัสคอมพิวเตอร์มาฟ้องร้อง และนับตั้งแต่มีการค้นพบไวรัสคอมพิวเตอร์ที่ถูกปล่อยในคอมพิวเตอร์ หรือข่ายงานคอมพิวเตอร์ต่าง ๆ การติดตามเพื่อหาผู้ใส่โปรแกรมเช่นนั้น ไม่เคยประสบความสำเร็จแม้แต่ครั้งเดียวถึงการที่มันเกิดขึ้นมา โดยปราศจากการช่วยเหลือของผู้ที่เริ่มต้นนั้น ความเร็วของไวรัสคอมพิวเตอร์ซึ่งสามารถแพร่ขยายไปสู่คอมพิวเตอร์อื่น ๆ อย่างรวดเร็ว และออกไปได้ไกลมากจากจุดเริ่มต้น ประกอบกับความซับซ้อนของงานที่ติดตาม [53]

นอกจากนี้ผู้กระทำความผิด ก็มิได้มีการควบคุมเส้นทางการเดินทางของไวรัสคอมพิวเตอร์นับตั้งแต่มีการปล่อยไวรัสคอมพิวเตอร์นั้น เข้าสู่ระบบคอมพิวเตอร์ หรือข่ายงานคอมพิวเตอร์และหากพิจารณาถึง เจตนาของผู้กระทำผิด และผลเสียหายที่จะเกิดขึ้นจากการกระทำการกำหนดให้การกระทำในขั้นตอน "การใส่" ไวรัสคอมพิวเตอร์ เป็นความผิดจึงเป็นการเหมาะ

---

50. The Computer Virus Eradication Act of 1989, Ibid., p.741

51. Lance J. Denning, Ibid., p.256

52. Daniel J. Kluth, Ibid., p.306

53. Ibid.

สมอย่างยิ่ง

ประการที่ 2 "ข้อมูลหรือคำสั่ง" ซึ่งใส่เข้าไปในโปรแกรมสำหรับคอมพิวเตอร์หรือในเครื่องคอมพิวเตอร์โดยตรง โดยรู้ว่าหรือมีเหตุผลอันเชื่อได้ว่า "ข้อมูลหรือคำสั่ง" ดังกล่าวอาจก่อให้เกิดความเสียหายต่อเครื่องคอมพิวเตอร์นั้น หรือคอมพิวเตอร์อื่น ๆ จึงมีปัญหาที่น่าจะวิเคราะห์ว่า "ข้อมูลหรือคำสั่ง" ที่จะก่อให้เกิดความเสียหาย มีความหมายเพียงใด

the Computer Virus Eradication Act เป็นบทบัญญัติที่กำหนดขึ้นเพื่อใช้อุดช่องว่างของกฎหมายซึ่งไม่ได้มีการคิดไว้ก่อนเกี่ยวกับปัญหาไวรัสคอมพิวเตอร์ แต่ในร่างกฎหมายมิได้ใช้คำว่า "ไวรัส" (Virus) และมิได้ให้ความหมายของโปรแกรมไวรัสคอมพิวเตอร์ไว้ แต่อย่างไรก็ตาม กฎหมายฉบับนี้มีจุดประสงค์เพื่อที่จะปราบปรามการกระทำความผิดเกี่ยวกับโปรแกรมไวรัสคอมพิวเตอร์โดยเฉพาะ

การนิยามความหมายของคำในกฎหมายเป็นสิ่งที่สำคัญ เพื่อผู้ใช้กฎหมายสามารถที่จะเข้าใจเจตนารมย์ที่แท้จริงของกฎหมาย และขอบเขตของกฎหมายที่จะใช้บังคับ คำว่า "ไวรัสคอมพิวเตอร์" ถ้อยคำนี้หากพิจารณาแล้วดูเหมือนว่าจะเป็นถ้อยคำที่ใช้กันอยู่ทั่วไป ไม่มีความหมายซับซ้อนประการใด แต่อย่างไรก็ตามความหมายที่เข้าใจกันธรรมดานี้อาจจะไม่เหมือนกับความหมายที่ใช้กันอยู่ในฐานความหมายทางเทคโนโลยีเกี่ยวกับคอมพิวเตอร์ การที่จะตีความถึงขอบเขตของกฎหมายที่ใช้บังคับจะต้องพิจารณาถึงภาษาที่ใช้ ถ้าไม่มีความชัดเจนที่แสดงให้เห็นถึงเจตนารมย์ของผู้ออกกฎหมายที่จะให้มีผลในทางตรงกันข้ามแล้ว คำที่ใช้ในกฎหมายก็ควรที่จะตีความตามความหมายที่เข้าใจกันทั่ว ๆ ไป [54] ตลอดจนคำนิยามที่ให้ความหมายไม่ชัดเจนแก่คำในกฎหมาย อาจทำให้การนำกฎหมายไปใช้ไม่สมกับเจนารมย์ อันเป็นวัตถุประสงค์ของกฎหมายอาญาเกี่ยวกับคอมพิวเตอร์[55]

และหากจะพิจารณาจากกฎหมายระดับมลรัฐของสหรัฐอเมริกา ถึงความหมายของโปรแกรมไวรัสคอมพิวเตอร์ก็จะเป็นประโยชน์อย่างยิ่งสำหรับการวิจัยฉบับนี้ และอาจจะเป็นแนวทาง

54.The Computer Virus Eradication Act of 1989, Ibid., p.737

55.Ibid., p.738

ในการพัฒนากฎหมายของประเทศไทยต่อไป

มลรัฐมินเนสโซต้า (MINNESOTA)

มินเนสโซต้า ได้ออกกฎหมายเกี่ยวกับคอมพิวเตอร์มาตั้งแต่ปี 1982 โดยบัญญัติมีผลให้ห้ามการเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจและการที่บุกรุกเข้าไปสู่ระบบความปลอดภัยของคอมพิวเตอร์เป็นความผิดอาญา โดยไม่ต้องพิจารณาถึงจำนวนของความเสียหายที่เกิดขึ้นมาจากการบุกรุก และความเสียหายที่เกิดขึ้นไม่เพียงแต่จะเกิดขึ้นกับคอมพิวเตอร์ของผู้ใช้หรือเจ้าของเท่านั้น โดยกฎหมายของมินเนโซต้าบัญญัติว่า

"บุคคลมีความผิดเกี่ยวกับการเข้าถึงโดยปราศจากอำนาจ ถ้าผู้นั้นโดยเจตนาและปราศจากอำนาจ พยายามหรือกระทำการบุกรุก (Penetrate) เข้าสู่ระบบความปลอดภัยของคอมพิวเตอร์"

ส่วนโทษที่ผู้กระทำความผิดจะได้รับ ขึ้นอยู่กับระดับของความเสี่ยงที่เกิดขึ้นต่อสุขภาพ หรือความปลอดภัยของประชาชน

บทบัญญัติของกฎหมายเกี่ยวกับคอมพิวเตอร์ของรัฐมินเนสโซต้า ครอบคลุมการกระทำความผิดเกี่ยวกับคอมพิวเตอร์หลายประการ แต่อย่างไรก็ตามกฎหมายฉบับนี้ก็ล้มเหลวในอันที่จะแก้ปัญหาเกี่ยวกับไวรัสคอมพิวเตอร์ ซึ่งถูกปล่อยให้อยู่ในระบบคอมพิวเตอร์ทั่วไป ทั้งนี้เพราะผู้ที่แพร่ไวรัสคอมพิวเตอร์ อาจจะไม่จำเป็นต้องบุกรุกเข้าไปในระบบควบคุมความปลอดภัยของคอมพิวเตอร์ จนกระทั่งไวรัสคอมพิวเตอร์อาจจะถูกใส่เข้าไป [56]

ดังนั้น ในปี ค.ศ.1989 รัฐมินเนสโซต้าได้มีการแก้ไขกฎหมาย โดยเสนอในชื่อของ the Computer Virus Act กฎหมายนี้ได้มีการลงนามเป็นกฎหมาย เมื่อวันที่ 17 พฤษภาคม ปี 1989 และมีผลบังคับใช้ในเดือนสิงหาคม ปี 1989

the Minnesota Computer Virus Act ได้แก้ไขคำนิยาม Minn. Stat. มาตรา 609.87 โดยเพิ่มคำนิยามของ "โปรแกรมคอมพิวเตอร์อันตราย" (destructive Computer program) โดยให้ความหมายว่า

---

56. Daniel J. Kluth, Ibid., p.309

"โปรแกรมคอมพิวเตอร์ ซึ่งได้ก่อให้เกิดอันตรายแก่การปฏิบัติงาน หรือผลิตผลผลิตที่เป็นอันตราย โปรแกรมซึ่งก่อให้เกิดอันตรายแก่การปฏิบัติงาน ถ้ามีผลกระทบให้คอมพิวเตอร์มีการปฏิบัติงานเลวลง ; ทำให้เกิดความเสียหายแก่คอมพิวเตอร์ คอมพิวเตอร์อื่นๆ หรือโปรแกรมคอมพิวเตอร์ ; หรือทำลายหรือเปลี่ยนแปลงโปรแกรมหรือข้อมูลคอมพิวเตอร์ โปรแกรมซึ่งผลิตผลผลิตที่เป็นอันตราย ถ้ามันผลิตข้อมูลโดยปราศจากอำนาจ รวมถึงข้อมูลซึ่งทำให้พื้นที่หน่วยความจำ ของคอมพิวเตอร์ไม่สามารถใช้ประโยชน์ได้;ทำให้เปลี่ยนแปลงข้อมูลหรือโปรแกรมคอมพิวเตอร์โดยปราศจากอำนาจ;หรือผลิตโปรแกรมคอมพิวเตอร์ที่เป็นอันตราย ซึ่งรวมถึงโปรแกรมคอมพิวเตอร์ซึ่งสามารถคัดลอกตัวเองได้"

การบรรยายการปฏิบัติงานอันก่อให้เกิดความเสียหาย ตามคำนิยามนี้ครอบคลุมโปรแกรมไวรัสคอมพิวเตอร์ เช่น ไวรัสในรูปแบบที่มีการปล่อยเข้าสู่ข่ายงานของ ARPAnet และในรูปแบบของม้าโทรจัน ซึ่งบรรจุไวรัสคอมพิวเตอร์อยู่ภายใน ส่วนคำบรรยายของผลผลิตที่เป็นอันตราย ในคำนิยามนี้ครอบคลุมถึงลักษณะพิเศษของไวรัสคอมพิวเตอร์ ที่สามารถคัดลอกตัวเองทุกชนิด 57

มลรัฐอิลินอยส์ ตามกฎหมายของมลรัฐอิลินอยส์ ซึ่งได้ออกกฎหมายเพื่อที่จะแก้ไขกฎหมายอาญาเกี่ยวกับคอมพิวเตอร์ ได้แบ่งการกระทำความผิดเกี่ยวกับไวรัสคอมพิวเตอร์ออกเป็น 2 ระดับ คือ 1. การใส่ไวรัสคอมพิวเตอร์ธรรมดา (computer virus inserting) และ 2.การใส่ไวรัสคอมพิวเตอร์ที่ร้ายแรง (aggravated computer virus insertion)

การใส่ไวรัสคอมพิวเตอร์ธรรมดา ได้ถูกนิยามในฐานะการใส่ไวรัสคอมพิวเตอร์เข้าไปในระบบคอมพิวเตอร์ด้วยการรู้ว่า มันอาจจะก่อให้เกิดความเสียหาย ผู้เขียนโปรแกรมไวรัสดังกล่าวจะต้องรับผิดชอบสำหรับความเสียหายที่เกิดขึ้น ต่อคอมพิวเตอร์ซึ่งไวรัสคอมพิวเตอร์เข้าไปทั้งหมด ส่วนการใส่ไวรัสคอมพิวเตอร์ที่ร้ายแรง ถูกกำหนดเช่นเดียวกับไวรัสคอมพิวเตอร์ธรรมดา

---

57. Ibid., p.310

แต่ได้ก่อให้เกิดความเสียหายแก่รัฐและรัฐบาลท้องถิ่น และระบบคอมพิวเตอร์ซึ่งเป็นสาธารณะหรือเป็นสาเหตุที่ก่อให้เกิดอันตรายเกี่ยวกับร่างกาย 58

มลรัฐแคลิฟอร์เนีย ได้ออกกฎหมายเพื่อที่จะให้ครอบคลุมถึงโปรแกรมอันตรายต่าง ๆ ซึ่งได้กำหนดให้โปรแกรมเหล่านี้อยู่ในความหมายของ "สิ่งที่ทำให้เกิดความเสียหายแก่คอมพิวเตอร์" (computer contaminants) โดยกฎหมายของรัฐแคลิฟอร์เนีย บัญญัติห้ามมิให้ใส่ "สิ่งที่ทำให้เกิดความเสียหายแก่คอมพิวเตอร์" เข้าไปในคอมพิวเตอร์ ข่ายงานคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ และได้ให้ความหมายของ "สิ่งที่ทำให้เกิดความเสียหายแก่คอมพิวเตอร์" ว่าหมายถึง

"การติดตั้งคำสั่งทางคอมพิวเตอร์ ที่ถูกกำหนดเพื่อที่จะเปลี่ยนแปลง ทำให้เสียหาย ทำลาย บันทึกหรือย้ายข้อมูลภายในคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข่ายงานคอมพิวเตอร์ โดยปราศจากเจตนาหรือการอนุญาตของผู้เป็นเจ้าของข้อมูล และรวมถึงกลุ่มของคำสั่งทางคอมพิวเตอร์ ซึ่งมีชื่อทั่วไปในฐานะของไวรัสหรือหนอนคอมพิวเตอร์ (worm) ซึ่งได้แพร่ขยายด้วยตัวเอง และถูกกำหนดเพื่อที่จะก่อให้เกิดความเสียหายต่อโปรแกรมคอมพิวเตอร์อื่น ๆ หรือข้อมูลคอมพิวเตอร์, เปลี่ยนแปลง ทำลาย หรือย้ายข้อมูล หรือในรูปแบบอื่นซึ่งก่อให้เกิดความเสียหายแก่การปฏิบัติงานโดยปกติของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข่ายงานคอมพิวเตอร์" 59

เมื่อพิจารณาถึง the Computer Virus Eradication Act ซึ่งเป็นกฎหมายของรัฐบาลกลาง ซึ่งมิได้ให้คำนิยามความหมายที่ชัดเจนของ "ข้อมูลหรือคำสั่ง" ที่ใส่เข้าไปโดยเชื่อว่าอาจจะก่อให้เกิดความเสียหายต่อคอมพิวเตอร์นั้น จะมีความหมายและขอบเขตเพียงใด และการขาดคำนิยามที่ให้ความหมายชัดเจนแก่คำในกฎหมาย ซึ่งอาจทำให้มีการนำกฎหมายไปใช้ไม่สมกับเจตนารมย์ อันเป็นวัตถุประสงค์ของกฎหมายอาญาเกี่ยวกับคอมพิวเตอร์

---

58. Ibid., p.307

59.Lance J. Denning, Ibid., p.72

ประการที่สาม เกี่ยวกับการกำหนดระดับของเจตนา ในการพิสูจน์ความรับผิดทางอาญา ซึ่งการที่จะพิสูจน์ให้เห็นโดยชัดแจ้งในการสร้างความเสียหายนั้น ยากที่จะพิสูจน์ได้หลาย ๆ กรณี เกี่ยวกับปัญหาของไวรัสคอมพิวเตอร์

เดิมกฎหมายเกี่ยวกับคอมพิวเตอร์ คือ ได้กำหนดระดับของเจตนาในการกระทำความผิดไว้ที่การกระทำ "โดยรู้" (knowingly) และต่อมาถูกแก้ไขโดย the Computer Fraud and Abuse Act 1986 ซึ่งกำหนดระดับของเจตนาในการกระทำความผิดว่า จะต้องกระทำ"โดยเจตนา"(intentionally) ในขณะที่ร่าง the Computer Virus Eradication Act ก็ได้กำหนดระดับของเจตนาว่าจะต้อง "โดยรู้" ถึงผลที่จะเกิดขึ้นจากการกระทำเกี่ยวกับโปรแกรมไวรัสคอมพิวเตอร์

บุคคลซึ่งจะกระทำการ "โดยรู้"(knowingly) หมายถึง หากเขารู้สำนึกว่าผลจะเกิดขึ้นจากการกระทำของเขา ไม่ว่าผลนั้นจะเป็นไปตาม ความเข้าใจของเขาหรือไม่ส่วน "โดยเจตนา" (Intentionally) หมายความว่า ยิ่งกว่าหรือมากกว่านั้น การที่บุคคลจะเกี่ยวข้องในการกระทำหรือเหตุที่ก่อให้เกิดผลโดยเจตนานั้น ซึ่งเหตุที่ก่อให้เกิดผลจะต้อง เป็นไปตามวัตถุประสงค์ของบุคคลที่ได้ตั้งใจไว้ 60

แต่อย่างไรก็ตาม ตามแนวคำพิพากษาคดีจริง ๆ แล้ว สภาวะทางจิตของ "โดยรู้" ไม่สามารถที่จะให้คำจำกัดความที่ชัดเจน และอาจจะต้องการบางสิ่งน้อยกว่าที่กฎหมายบัญญัติไว้ 61

ดังนั้น ตามร่าง the Computer Virus Eradication Act จึงจำเป็นที่จะต้องพิสูจน์ถึงสภาวะทางจิตใจ ซึ่งเป็นสิ่งที่ยากมากสำหรับอัยการที่จะต้องพิสูจน์ว่าผู้กระทำความผิด "โดยรู้" (Knowingly) ใส่โปรแกรมไวรัสคอมพิวเตอร์เข้าไปในคอมพิวเตอร์ หรือโปรแกรม และรู้หรือมีเหตุผลที่เชื่อว่าไวรัสคอมพิวเตอร์นั้น "อาจเป็นสาเหตุที่ก่อให้เกิดการสูญเสีย, เสียหาย

60.Daniel J. Kluth, Ibid., p.303

61.The Computer Virus Eradication Act of 1989, Ibid., p.739

หรือเสี่ยงต่อสุขภาพหรือสวัสดิภาพ..." ปัญหาที่ถูกยกขึ้นคือ การฟ้องร้องเป็นภาระที่จะต้องมีการพิสูจน์จนสิ้นความสงสัย ว่าผู้กระทำผิดรู้ว่าโปรแกรมที่เขาสร้างเป็นไวรัสคอมพิวเตอร์ และสิ่งนั้นเขารู้หรือควรรู้ว่าความเสียหายหรือการสูญเสีย จะเป็นผลมาจากการเขียนโปรแกรมของเขา

และหากในการพิจารณาได้ความว่าผู้เขียนโปรแกรมไวรัสคอมพิวเตอร์ ไม่สามารถที่จะควบคุมไวรัสนั้นได้ก่อนที่มันจะสร้างความเสียหาย และนักโปรแกรมซึ่งไม่มีวิธีที่จะควบคุมมิให้มันขยายต่อไป ดังนั้น การฟ้องอาจจะพบกับอุปสรรคในการที่จะพิสูจน์ว่า นักโปรแกรมที่เขียนไวรัสคอมพิวเตอร์นั้นจำเป็นต้องรู้ว่าโปรแกรมไวรัสคอมพิวเตอร์ จะเป็นสาเหตุที่ก่อให้เกิดอันตราย ซึ่งผู้เขียนโปรแกรมไวรัสคอมพิวเตอร์อาจจะเพียงพิสูจน์ให้เห็นว่าไวรัสคอมพิวเตอร์นั้น ได้มีการทำงานที่แตกต่างไปมากกว่าที่เขาคาดคิดไว้ อันเป็นผลให้เขาอาจจะสามารถรอดพ้นจากการถูกลงโทษได้[62]

ความผิดฐานใส่โปรแกรมไวรัสคอมพิวเตอร์นี้ ได้มีหลายมลรัฐออกเป็นกฎหมายทำนองเดียวกันนี้ ซึ่งมีผลบังคับใช้แล้วและอยู่ระหว่างการแก้ไข เช่น

<u>มลรัฐแมรีแลนด์</u> ได้มีการแก้ไขกฎหมายซึ่ง ผู้ว่าการรัฐได้ลงนามแล้วตั้งแต่วันที่ 25 พฤษภาคม ปี ค.ศ. 1989 เกี่ยวกับการเข้าถึงคอมพิวเตอร์ซึ่งก่อให้เกิดอันตรายต่อคอมพิวเตอร์ โดยกฎหมายดังกล่าวได้เพิ่มการกระทำซึ่งต้องห้าม 2 ประการด้วยกัน คือ " (1) การกระทำอันเป็นสาเหตุให้การทำงานผิดพลาดหรือการแทรกแซงการทำงานของคอมพิวเตอร์ (2) เปลี่ยนแปลงทำให้เสียหาย หรือทำลายข้อมูล หรือโปรแกรมคอมพิวเตอร์" ซึ่งถ้อยคำของตัวอักษรเหล่านี้เป็นเพียงการขยายความให้ครอบคลุมถึงการกระทำผิด ซึ่งรัฐอื่น ๆ ส่วนใหญ่ได้ห้ามการกระทำเหล่านี้เรียบร้อยแล้ว โดยการห้ามกระทำในประการแรกนั้น ได้กำหนดให้มีความหมายกว้างกว่ากฎหมายของรัฐซึ่งใช้อยู่ ซึ่งกว้างพอที่จะเผชิญกับการกระทำเกี่ยวกับโปรแกรมไวรัสคอมพิวเตอร์ [63]

62.Ibid.

63.Lance J. Denning, Ibid., p.70

มลรัฐเวสเวอร์จีเนีย ได้ออกกฎหมายในปี ค.ศ. 1989 ซึ่งเป็นกฎหมายอาญาเกี่ยวกับคอมพิวเตอร์ฉบับแรก โดยกฎหมายฉบับนี้ได้รับการสนับสนุนเป็นอย่างมากในอันที่จะออกมาเป็นกฎหมาย ทั้งนี้เพื่อที่จะใช้คุ้มครองวงการคอมพิวเตอร์ ภายในกฎหมายฉบับนี้ได้กำหนดไว้กว้างพอที่จะให้ครอบคลุมซึ่งการใส่โปรแกรมไวรัสคอมพิวเตอร์เข้าไปได้กำหนดว่า "ซึ่งการทำลายนั้นให้รวมถึงการกระทำของโปรแกรมด้วย" 63

มลรัฐอิลสินอยส์ โดยสถาบันวิจัยกฎหมายของมลรัฐได้ออกรายฉบับหนึ่งใช้ชื่อว่า "ไวรัสคอมพิวเตอร์และกฎหมาย (Computer Viruses and the Law) ได้แนะนำให้มีการแก้ไขกฎหมายของรัฐหลายประการ และรวมถึงกฎหมายซึ่งได้ออกมาเมื่อเร็ว ๆ นี้ ที่ได้กำหนดความผิดขึ้นใหม่เกี่ยวกับการใส่หรือพยายามใส่โปรแกรมโดยขณะนั้น "รู้หรือมีเหตุผลที่จะเชื่อ" ว่ามันอาจจะก่อให้เกิดความเสียหายหรือทำลาย 64

มลรัฐเพนซิลวาเนีย คณะกรรมาธิการกฎหมายเกี่ยวกับงบประมาณและการเงินได้ออกรายงานในหัวข้อ "ไวรัสคอมพิวเตอร์และความเป็นไปได้ที่จะลดระบบคอมพิวเตอร์คอมมอน-เวสท์" (Common wealth Computer Systems) ตามรายงานได้แนะนำถึงพฤติกรรมที่ควรถูกห้ามและควรที่จะกำหนดคำนิยามให้ดีขึ้น ซึ่งต่อมาก็ได้มีการแก้ไขกฎหมายโดยระบุคำนิยามของไวรัสคอมพิวเตอร์ให้มากขึ้นในฐานะ "โปรแกรมหนึ่งหรือการกำหนดโครงสร้างของคอมพิวเตอร์ซึ่งมีความสามารถที่จะคัดลอกตัวมันเองทั้งหมดหรือบางส่วน..." ในอันที่จะห้ามมิให้ใส่ไวรัสคอมพิวเตอร์เข้าไปในหน่วยความจำ ข่ายงาน หรือระบบคอมพิวเตอร์ 65

มลรัฐเมทซาชูเสส ได้ออกกฎหมายซึ่งครอบคลุมถึงการกระทำเกี่ยวกับโปรแกรมไวรัสคอมพิวเตอร์ เมื่อต้นปี ค.ศ. 1989 โดยได้กำหนดความแตกต่างระหว่างความผิดฐานลักทรัพย์

---

63. Ibid.

64. Ibid., p.71

65. Lance J. Denning, Ibid., p.71

ทางคอมพิวเตอร์ (computer larceny) และการหยุดชะงักทางคอมพิวเตอร์ (computer breaking) การลักทรัพย์ทางคอมพิวเตอร์ถูกนิยามในฐานะของ "การปล่อยไวรัสคอมพิวเตอร์โดยรู้ว่าเป็นสาเหตุของการทำงานหรือเปลี่ยนแปลงข้อมูล" การหยุดชะงักทางคอมพิวเตอร์ในฐานะของการปล่อย "ไวรัสคอมพิวเตอร์ซึ่งมิได้ทำลายหรือเปลี่ยนแปลงข้อมูล แต่ได้แทรกแซงความสามารถของผู้ใช้เพื่อจะใช้คอมพิวเตอร์" 66

3.3.3.2 ความผิดฐานมอบโปรแกรมไวรัสคอมพิวเตอร์

ความผิดฐานมอบ (provides) โปรแกรมไวรัสคอมพิวเตอร์ เป็นบทบัญญัติที่เกี่ยวกับการห้ามมิให้มีการแพร่โปรแกรมไวรัสคอมพิวเตอร์ (the Virus Infection Section)

ความผิดฐานมอบโปรแกรมไวรัสคอมพิวเตอร์ เป็นความผิดฐานหนึ่งตามร่างกฎหมาย the Computer Virus Eradication Act ที่กำหนดขึ้นมาเพื่อที่จะฟ้องร้องบุคคลใดก็ตาม ที่ได้มอบโปรแกรมไวรัสให้แก่ผู้อื่น โดยบัญญัติว่า

"โดยเจตนา...

(บี) มอบ (โดยรู้ถึงการมีอยู่ของข้อมูลหรือคำสั่งดังกล่าว) โปรแกรมนั้นหรือคอมพิวเตอร์นั้นให้แก่บุคคลใด ๆ ในลักษณะที่บุคคลดังกล่าวมิได้รู้ถึงการใส่นั้น หรือผลของการใส่ข้อมูลหรือคำสั่งนั้น ;

หากการใส่หรือมอบข้อมูลหรือคำสั่งนั้นมีผลกระทบหรือถูกทำให้เกิดผลหรือผลอย่างอื่นไปอีก โดยวิธีทางพาณิชย์ระหว่างมลรัฐหรือการพาณิชย์ระหว่างประเทศ"

มาตรานี้มีวัตถุประสงค์ที่จะลงโทษบุคคล ผู้ซึ่งมีเจตนาที่จะแพร่ไวรัสคอมพิวเตอร์ไปสู่คอมพิวเตอร์อื่น ๆ โดยการมอบให้แก่บุคคลอื่นโดยมีเจตนาที่จะก่อให้เกิดความเสียหายต่อโปรแกรมหรือข้อมูลของบุคคลอื่น แต่หากการมอบนั้นผู้กระทำมิได้มีเจตนาที่จะนำโปรแกรมคอมพิวเตอร์

---

66. Ibid., p.72

อันตรายไปสู่คอมพิวเตอร์อื่น ผู้นั้นย่อมไม่มีความผิดเพราะไม่มีเจตนาที่จะกระทำให้เกิดความเสียหาย

กฎหมายฉบับนี้ไม่ใช้กับบุคคลผู้ซึ่งปล่อยโปรแกรมคุ้มกันไวรัส ซึ่งโปรแกรมดังกล่าวจะทำลายโปรแกรมไวรัสคอมพิวเตอร์ ซึ่งที่แท้จริงก็มิได้มีเจตนาที่จะทำให้เกิดความเสียหาย เพียงแต่มีเจตนาที่จะแก้ไขให้ตรงต่อสถานะการณ์เท่านั้น รวมถึงการปล่อยไวรัสคอมพิวเตอร์ โดยมีอำนาจที่จะกระทำเช่นนั้น เพื่อที่จะทำให้เกิดความเสียหายซึ่งได้กระทำในการปฏิบัติการ ในช่วงเวลาของการวิจัยทางการศึกษาเกี่ยวกับไวรัสคอมพิวเตอร์ 67

ความผิดฐานมอบโปรแกรมไวรัสคอมพิวเตอร์ให้แก่บุคคลอื่น สามารถที่จะปรับใช้กับโปรแกรมคอมพิวเตอร์อันตรายที่พบไม่ว่าที่ใดก็ตาม หรือที่ซึ่งถูกปล่อย โดยความผิดฐานนี้ระบบความปลอดภัยของคอมพิวเตอร์ไม่จำเป็นต้องมีการถูกละเมิด หรือถูกกระทบก่อนจึงจะเป็นความผิด จะถือเป็นความผิดทันทีที่ได้มอบโปรแกรมหรือคอมพิวเตอร์ ซึ่งตนรู้ว่ามีไวรัสคอมพิวเตอร์อยู่โดยบุคคลที่รับมอบมิได้รู้ถึงการมีอยู่ของไวรัสคอมพิวเตอร์นั้น

จุดประสงค์ที่แท้จริงของกฎหมายฉบับนี้ เกี่ยวกับการแพร่ไวรัสคอมพิวเตอร์ โดยการที่ผู้เป็นเจ้าของโปรแกรมนั้นหรือมีโปรแกรมนั้นไม่ว่าจะได้มาโดยตั้งใจหรือไม่ ให้มีการเคลื่อนย้ายจากคอมพิวเตอร์หรือไปสู่คอมพิวเตอร์อื่นโดยผู้เป็นเจ้าของนั้น

สำหรับความผิดเกี่ยวกับการมอบโปรแกรมไวรัสคอมพิวเตอร์ ที่ออกบังคับใช้ในระดับมลรัฐ เช่น รัฐมินเนสโซต้า (Minnesota) ซึ่ง the Minnesota Computer Virus Act ได้แก้ไขกฎหมายเกี่ยวกับคอมพิวเตอร์ มาตรา 609.88 ซึ่งบัญญัติว่า

การกระทำของบุคคลจะมีความผิดถ้าบุคคลนั้น: "มอบโปรแกรมคอมพิวเตอร์อันตราย, โดยปราศจากอำนาจและด้วยเจตนาที่จะก่อให้เกิดความเสียหาย หรือทำลาย คอมพิวเตอร์ ระบบคอมพิวเตอร์ ข่ายงานคอมพิวเตอร์ ซอฟต์แวร์คอมพิวเตอร์ หรือทรัพย์สินอื่น ๆ ที่ถูกนิยามเป็นพิเศษ..."

67.Daniel J. Kluth, Ibid., p.311

จากการที่ the Computer Virus Eradication Act ได้เสนอความผิดขึ้นใหม่ 2 ฐานความผิด ดังที่กล่าวมาแล้ว คือ

1. ความผิดฐานใส่ไวรัสคอมพิวเตอร์เข้าสู่คอมพิวเตอร์ และ

2. ความผิดฐานมอบโปรแกรมไวรัสคอมพิวเตอร์

และหากจะนำไวรัสคอมพิวเตอร์ซึ่งกำลังแพร่ระบาดอยู่ในขณะนี้ มาทดลองปรับกับกฎหมายดังกล่าว จะทำให้เรามั่นใจได้ว่า กฎหมายซึ่งออกมาในลักษณะนี้ สามารถที่จะป้องกันและปราบปรามการกระทำความผิดได้อย่างมีประสิทธิภาพ ตัวอย่างเช่น

<u>ไวรัสม้าโทรจัน</u> (Trogan horse) the Computer Virus Eradication Act จะเป็นประโยชน์อย่างยิ่งในอันที่จะฟ้องร้อง นักโปรแกรมผู้ซึ่งเขียนโปรแกรมไวรัสม้าโทรจันซึ่งลักษณะของไวรัสม้าโทรจันคือ มีโปรแกรมไวรัสคอมพิวเตอร์ซ่อนอยู่ในโปรแกรมหลัก โดยผู้เขียนโปรแกรมไวรัสคอมพิวเตอร์ได้ "ใส่เข้าไปในโปรแกรม" (inserts into a program) ซึ่งถือว่าเป็นการกระทำที่กฎหมายบัญญัติไว้ว่าการกระทำเช่นนี้เป็นความผิด นอกจากนี้ความผิดเกี่ยวกับการใส่โปรแกรมไวรัสคอมพิวเตอร์ ยังต้องการเพิ่มเติมอีกว่า ผู้สร้างโปรแกรมไวรัสคอมพิวเตอร์ต้อง"รู้หรือมีเหตุผลที่เชื่อได้ว่า" ไวรัสคอมพิวเตอร์นั้น "อาจเป็นสาเหตุที่จะทำให้เกิดความเสียหายค่าใช้จ่าย หรือเสี่ยงต่อสุขภาพหรือสวัสดิภาพ" ของบุคคลใดก็ตาม ผู้ซึ่งใช้หรือเชื่อใจในโปรแกรมหรือคอมพิวเตอร์

และการกระทำจะเป็นการฝ่าฝืนบทบัญญัติที่ห้ามการแพร่ไวรัสคอมพิวเตอร์ ซึ่งกำหนดว่าบุคคลใดก็ตาม ได้ให้โปรแกรมคอมพิวเตอร์หรือคอมพิวเตอร์ที่ติดเชื้อ โดยรู้อยู่ถึงการมีไวรัสคอมพิวเตอร์นั้นให้แก่บุคคลใดก็ตาม แต่จะถือว่าเป็นความผิดตาม the Computer Virus Eradication Act เมื่อผู้รับนั้น มิได้รู้ถึงการมีอยู่ของไวรัสคอมพิวเตอร์ บทบัญญัติที่ห้ามการแพร่ไวรัสคอมพิวเตอร์นี้จะช่วยป้องกันบุคคลอื่น ๆ ที่มิได้รู้ถึงการมีอยู่ของไวรัสคอมพิวเตอร์อีกด้วย แต่จะใช้จัดการกับบุคคลผู้ซึ่งรู้ และได้มอบโปรแกรมที่ติดเชื้อหรือคอมพิวเตอร์ที่ติดเชื้อให้แก่บุคคลใดก็ตาม

<u>ไวรัสหนอนคอมพิวเตอร์</u> (worm) the Computer Virus Eradication Act สามารถที่จะนำไปบรับใช้กับผู้สร้างโปรแกรมหนอนคอมพิวเตอร์ (worm) ได้ ตามบทบัญญัติที่

ห้ามการสร้างไวรัสคอมพิวเตอร์ ได้ห้ามถึงการที่โดยรู้อยู่ ได้ใส่ไวรัสคอมพิวเตอร์ชนิดนี้เข้าไปในคอมพิวเตอร์หรือโปรแกรม ซึ่งเป็นสาเหตุให้เกิดความเสียหายแก่การใช้คอมพิวเตอร์ โปรแกรมหนอนคอมพิวเตอร์โดยปกติทั่ว ๆ ไปจะถูกใส่เข้าไปในข่ายงานคอมพิวเตอร์โดยตรง และจะทำให้มีการติดเชื้อดังกล่าวทั่วทั้งระบบ ซึ่งการที่ใส่ไวรัสหนอนคอมพิวเตอร์ (worm) เข้าไปในข่ายงานคอมพิวเตอร์ ถือได้ว่าเป็นการกระทำการอันเป็นความผิดเกี่ยวกับการใส่ไวรัสคอมพิวเตอร์เข้าไปในคอมพิวเตอร์

ไวรัสโลจิกบอมบ์ (Logic Bomb) the Computer Virus Eradication Act จะเป็นประโยชน์ที่จะดำเนินการกับนักโปรแกรมที่เขียนไวรัสโลกจิกบอมบ์ บทบัญญัติที่สร้างไวรัสคอมพิวเตอร์ ห้ามการใส่โดยรู้ว่าเป็นไวรัสโลจิกบอมบ์ เข้าไปไม่ว่าจะในคอมพิวเตอร์หรือโปรแกรม โลจิกบอมบ์จะถูกใส่เข้าไปโดยตรงต่อคอมพิวเตอร์หรือโปรแกรม และจะปฏิบัติการตามเหตุการณ์หรือเงื่อนไขที่กำหนด ซึ่งการใส่โปรแกรมโลจิกบอมบ์ถือว่าเป็นการฝ่าฝืนบทบัญญัติที่ห้ามการสร้างไวรัสคอมพิวเตอร์ ดังนั้น ผู้เขียนโปรแกรมโลจิกบอมบ์ (Logic Bomb) จึงสามารถที่จะถูกฟ้องได้ตาม the Computer Virus Eradication Act

บุคคลผู้กระทำความผิดฐานใส่โปรแกรมไวรัสคอมพิวเตอร์ และความผิดฐานมอบโปรแกรมชนิดนี้ให้แก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกิน 10 ปี ซึ่งนอกจากโทษจำคุกนี้แล้ว ศาลอาจจะกำหนดให้ผู้กระทำความผิด ต้องชดใช้ค่าเสียหาย แก่ผู้ที่ได้รับความเสียหายอันมีผลมาจากโปรแกรมไวรัสคอมพิวเตอร์นั้นได้

วิเคราะห์กฎหมายกำจัดไวรัสคอมพิวเตอร์ของสหรัฐอเมริกา

แม้ว่าร่างกฎหมาย the Computer Virus Eradication Act จะยังคงเป็นร่างกฎหมายที่ใช้ในการปราบปรามการกระทำความผิดเกี่ยวกับไวรัสคอมพิวเตอร์ ซึ่งยังมิได้มีผลใช้บังคับ แต่มีแนวโน้มเป็นอย่างสูงที่ร่างกฎหมายฉบับนี้ จะได้รับความเห็นชอบจากสภาคองเกส เนื่องจากสมาชิกสภาคองเกสหลายท่าน ได้สนับสนุนในร่างกฎหมายฉบับนี้

ดังนั้น การที่จะนำร่างกฎหมายฉบับนี้มาวิเคราะห์ถึงข้อดีและข้อเสียย่อมจะเป็นประโยชน์แก่ผู้ที่จะศึกษาถึงการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ต่อไป

ร่างกฎหมายกำจัดไวรัสคอมพิวเตอร์ของสหรัฐอเมริกาฉบับนี้ มีทั้งข้อดีและข้อเสีย ข้อดีของกฎหมายฉบับนี้คือการที่บัญญัติการกระทำที่เป็นความผิด มีถ้อยคำที่มีความกว้างพอที่จะให้ครอบคลุมถึงโปรแกรมไวรัสคอมพิวเตอร์ ซึ่งก่อให้เกิดความเสียหายมากที่สุด ถ้อยคำเกี่ยวกับเขตอำนาจศาลกว้างพอที่รัฐบาลกลางสามารถที่จะฟ้องร้องการกระทำความผิดเกี่ยวกับไวรัสคอมพิวเตอร์ โทษที่จะลงแก่ผู้เขียนโปรแกรมไวรัสคอมพิวเตอร์มีความเหมาะสม[68]

แต่ข้อเสียของกฎหมายฉบับนี้คือ บทบัญญัติของกฎหมายนี้ มิได้กำหนดคำนิยามในการที่จะให้ความหมายถ้อยคำซึ่งมีความสำคัญ และเป็นการไม่เหมาะสมในการที่กำหนดระดับของสภาวะทางจิตใจ (mental state standards) อันผู้กระทำจะต้องรับโทษอาญา

ตาม the Computer Virus Eradication Act ซึ่งได้กำหนดถึงการกระทำเกี่ยวกับโปรแกรมไวรัสคอมพิวเตอร์เป็นความผิด โดยใช้ถ้อยคำ "ใส่เข้าไปในโปรแกรม" (Inserts into a program) แต่กฎหมายฉบับนี้ก็มิได้ให้คำนิยามของคำว่า "ใส่"(inserts) และ "โปรแกรม" (program) ไว้ ว่าคำเหล่านี้จะมีความหมายอย่างไร และมีขอบเขตเพียงใด นอกจากนี้ยังมีคำอื่น ๆ อีกเช่น "ข้อมูล" (information) หรือ "คำสั่ง" (commands) ก็มิได้ถูกนิยามไว้ในร่างกฎหมายฉบับนี้

68.The Computer Virus Eradication Act of 1989, Ibid., p.736

การขาดคำนิยามที่ให้ความหมายชัดเจนแก่คำในกฎหมาย อาจทำให้มีการนำกฎหมายไปใช้ไม่สมกับเจตนารมย์อันเป็นวัตถุประสงค์ของกฎหมาย ความผิดพลาดในการที่มิได้บัญญัติคำนิยามของกฎหมาย จึงเป็นการบังคับให้อัยการจำต้องหาเหตุผลต่างๆ เพื่อมาสนับสนุนว่าผู้กระทำความผิดได้กระทำในสิ่งที่กฎหมายบัญญัติไว้ว่าเป็นความผิด และศาลจะเป็นผู้ตัดสินว่าเจตนาของผู้ออกกฎหมายต้องการที่จะให้ความหมายของคำเหล่านี้ว่าอย่างไร ความจำเป็นของอัยการที่ต้องมีภาระในการพิสูจน์ ในอันที่จะต้องมีการอธิบายหรือโต้แย้งเกี่ยวกับคำในกฎหมาย ซึ่งอัยการจะต้องมีภาระหนักขึ้นกว่าปกติ ในการที่จะต้องพิสูจน์ความผิดของจำเลยในแต่ละองค์ประกอบของการกระทำความผิดอาญาที่ฟ้อง ให้ชัดเจนจนปราศจากความสงสัย

ดังนั้น จึงควรที่จะมีการกำหนดคำนิยามของคำที่มีความสำคัญไว้ใน the Computer Virus Eradication Act เพื่อที่จะใช้เป็นแนวทางในการพิจารณาฟ้องร้องผู้กระทำความผิดให้ถูกต้องต่อไป

นอกเหนือจากการแก้ไขโดยการที่บัญญัติคำนิยามในกฎหมายเพิ่มเติมแล้ว การนิยามความหมายของกฎหมายที่มีปัญหา ยังสามารถที่จะกระทำได้โดยหลักของกฎหมายคอมมอนลอร์ (Common Law) โดยการนี้ ปัญหาในการให้คำนิยามความหมายก็จะหมดไป ถ้าหากในกรณีที่มีคดีการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่เกิดขึ้นจำนวนมากพอ คดีที่มีการตัดสินก่อน ๆ จะอยู่ภายใต้ the Computer Fraud and Abuse Act 1986 เมื่อศาลได้พิพากษาอย่างไรแล้ว คำพิพากษาดังกล่าวก็จะเป็นแนวบรรทัดฐานในการตีความของคดีต่อไป และสามารถนำมาใช้ได้กับการตีความของ the Computer Virus Eradication Act [69] แต่อย่างไรก็ตามเป็นที่น่าเสียดาย ที่ได้มีคดีขึ้นสู่ศาลในอันที่ศาลจะพิพากษาตามกฎหมายปี 1986 นั้นมีน้อยมาก ซึ่งทำให้คำนิยามตามหลักกฎหมายคอมมอนลอร์ (Common Law) ในถ้อยคำที่มีความสำคัญในกฎหมายจึงต้องมีการพัฒนาไปอย่างช้า ๆ

ข้อเสียของ the Computer Virus Eradication Act อีกประการหนึ่งคือการที่จะต้องพิสูจน์สภาวะทางจิตใจของผู้กระทำผิดว่า ผู้กระทำผิดได้กระทำโดยรู้ (knowing) ใน

---

69. Ibid., p.738

การใส่ไวรัสคอมพิวเตอร์เข้าไปในคอมพิวเตอร์หรือโปรแกรม และรู้หรือมีเหตุผลที่เชื่อว่าไวรัสคอมพิวเตอร์นั้นอาจเป็นสาเหตุที่ก่อให้เกิดการสูญเสีย เสียหาย หรือเสี่ยงต่อสุขภาพหรือสวัสดิภาพ

ซึ่งภาระในการพิสูจน์ถึงการที่กระทำความผิด "โดยรู้" จะเป็นสิ่งที่ยากมากสำหรับอัยการ ซึ่งในประเด็นนี้ได้มีนักกฎหมายของสหรัฐอเมริกาบางท่าน [70] ได้ให้ความเห็นว่าปัญหาของอัยการที่จะฟ้องร้อง อาจจะได้รับการเยียวยาได้โดยการลดภาระในการพิสูจน์เกี่ยวกับสภาวะจิตใจของนักเขียนโปรแกรมไวรัสคอมพิวเตอร์ที่จะกระทำโดย "ประมาทเลินเล่ออย่างร้ายแรง"(gross negligence) หรือด้วยความ "ประมาท" (recklessness) ในส่วนที่เกี่ยวกับความเสียหายที่น่าจะมีผลมาจากโปรแกรมไวรัสคอมพิวเตอร์

การกำหนดสภาวะจิตใจของผู้กระทำผิดเป็น "ความประมาทเลินเล่ออย่างร้ายแรง" หรือ "ความประมาท" ยังคงเป็นสิ่งที่ต้องการ เพื่อพิสูจน์การฟ้องร้องให้ปราศจากความสงสัย (prove beyond a reasonable doubt)ว่าจำเลยได้สร้างไวรัสคอมพิวเตอร์ ซึ่งก็เป็นเหตุผลที่สามารถที่จะจัดได้ว่าเป็นสาเหตุให้เกิดความเสียหาย ซึ่งเป็นการลดภาวะการพิสูจน์จาก "โดยรู้" เป็น "โดยประมาทเลินเล่ออย่างร้ายแรง" หรือ "โดยประมาท" ซึ่งน่าจะเป็นสิ่งที่จะนำตัวผู้กระทำผิดมาลงโทษได้มากขึ้น

3.3.3.3. การขยายคำนิยาม "ทรัพย์สิน" (Property)

การแก้ปัญหาเกี่ยวกับโปรแกรมไวรัสคอมพิวเตอร์ ซึ่งได้ก่อให้เกิดความเสียหายขึ้นแก่โปรแกรมหรือข้อมูล ซึ่งกฎหมายที่มีอยู่ไม่สามารถที่จะปรับใช้ได้โดยตรง อันเนื่องจากความไม่แน่ชัดถึงโปรแกรมหรือข้อมูลที่ถูกทำให้เกิดความเสียหายนั้น จะเป็นทรัพย์สินตามความหมายของกฎหมายอาญาในอันที่จะได้รับความคุ้มครองหรือไม่

และในการนี้ได้มี 2-3 มลรัฐ ได้เพียงแต่ขยายกฎหมายอาญาที่มีอยู่ เพื่อที่จะให้

---

70. Ibid., p.738

คำนิยามของ "ทรัพย์สิน" (property) รวมถึงข้อมูลที่อยู่บนแผ่นดิสก์คอมพิวเตอร์ หรือภายในข่ายงานคอมพิวเตอร์ หรือในคอมพิวเตอร์ขนาดใหญ่ เช่น

รัฐมอนตาน่า (Montana) ได้นิยามคำว่า "ทรัพย์สิน" หมายถึง "สิ่งที่กระตุ้นทางอิเลคทรอนิค (electronic inpulses) ข้อมูลหรือข่าวสารที่ผลิตขึ้นหรือทำขึ้นโดยกระบวนการทางอิเลคทรอนิค (electronically processed or produced data or information),..., หรือโปรแกรมคอมพิวเตอร์ ไม่ว่าจะเป็นรูปแบบใดที่คนหรือเครื่องจักรกลสามารถอ่านออกได้หรือไม่ บริการทางคอมพิวเตอร์ สิ่งอื่น ๆ ที่จับต้องได้หรือจับต้องไม่ได้ ซึ่งมีมูลค่า (value) อันเกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือข่ายงานคอมพิวเตอร์ และสำเนาใด ๆ ของสิ่งนั้น"[71]

รัฐเมสซาชูเสท ได้ให้คำจำกัดความที่สั้นลงไปอีก โดยให้คำนิยาม "ทรัพย์สิน" ว่ารวมถึง"กระบวนการทางอิเลคทรอนิค (electronically processed) หรือข้อมูลที่ถูกเก็บ (stored data),ไม่ว่าจะจับต้องได้หรือจับต้องไม่ได้, และข้อมูลในขณะที่ส่ง (transit)..."[72]

แม้ว่ากฎหมายจะได้นิยาม "ทรัพย์สิน" ให้รวมถึงข้อมูลซึ่งเป็นสื่อในทางคอมพิวเตอร์ สิ่งเหล่านี้มิได้มีความสำคัญในการที่จะแก้ไขปัญหาอย่างอื่น ๆ ด้วย เช่น มิได้เป็นการแก้ปัญหาเกี่ยวกับความผิดฐานลักทรัพย์หรือบลันทรัพย์ เพราะความผิดประเภทนี้องค์ประกอบของความผิดต้องมีการ "เอาไป" (taking) ด้วยเจตนาที่จะตัดกรรมสิทธิ์ของผู้เป็นเจ้าของทรัพย์สิน แต่ผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์ไม่มีเจตนาที่จะตัดกรรมสิทธิ์หรือก่อให้เกิดอันตราย หรือไวรัสคอมพิวเตอร์ซึ่งมีผลในแง่ดี มิได้มีการตัดกรรมสิทธิ์ของเจ้าของหรือผู้ใช้

แต่อย่างไรก็ตาม ได้มีนักกฎหมายและนักคอมพิวเตอร์บางท่าน ได้กล่าวว่าการที่จะแก้ไขคำนิยามของคำว่า "ทรัพย์สิน" ให้มีความหมายกว้างขึ้น เป็นสิ่งที่เป็นการไม่เหมาะสมต่อรูปแบบของการกระทำความผิดที่ใช้เทคโนโลยีชั้นสูง และมีการเปลี่ยนแปลงความก้าวหน้าอย่างรวดเร็ว การแก้ไขคำนิยามในวันนี้อาจจะเป็นสิ่งที่ล้าสมัยในเวลาเพียงไม่กี่ปี

---

71. Lance J. Denning, Ibid., p.66

72. Ibid.

การก่อให้เกิดความเสียหายโดยโปรแกรมไวรัสคอมพิวเตอร์ ก็อาจจะมิได้กระทำโดยตรงต่อ "ทรัพย์สิน" ตามคำนิยามของกฎหมายที่มลรัฐต่าง ๆ ยกตัวอย่างเช่น ขโมยรหัสผ่าน เปลี่ยนคำนิยามของปุ่ม ทำให้การทำงานของคอมพิวเตอร์ช้าลง หรืออาจจะมีรูปแบบความเสียหายอื่น ๆ เพิ่มขึ้นมาอีก ซึ่งมิได้อยู่ในความหมายของ "ทรัพย์สิน" ตามที่ให้คำนิยาม

นอกจากนี้ ยังเป็นการสร้างความยุ่งยากให้แก่ทางอัยการ ในการที่จะพิสูจน์การกระทำของจำเลย ว่าความเสียหายที่เกิดขึ้นเป็นผลมาจากโปรแกรมไวรัสคอมพิวเตอร์ ซึ่งจำเลยใส่เข้าไปในคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข่ายงานคอมพิวเตอร์ ซึ่งอัยการจะต้องพิสูจน์ทั้งการกระทำของจำเลยที่ปล่อยไวรัสคอมพิวเตอร์ และทั้งความเสียหายที่เกิดขึ้น และยิ่งคอมพิวเตอร์นั้นมีโปรแกรมไวรัสคอมพิวเตอร์มากกว่า 1 โปรแกรม ก็ยิ่งสร้างความยุ่งยากขึ้นไปอีก

และจากเหตุผลดังกล่าวทำให้หลาย ๆ มลรัฐของสหรัฐอเมริกา รวมถึงร่างกฎหมายของรัฐบาลกลาง ได้หลีกเลี่ยงที่จะขยายคำนิยามของ "ทรัพย์สิน" และกำหนดความผิดฐาน "ใส่" โปรแกรมไวรัสคอมพิวเตอร์แทน

3.3.4. ความรับผิดเกี่ยวกับไวรัสคอมพิวเตอร์ของอังกฤษ

ตามบทบัญญัติของ the Computer Misuse Act 1990 อันเกี่ยวกับความผิดที่จะนำมาปรับใช้ต่อกรณีโปรแกรมไวรัสคอมพิวเตอร์ ตามบทบัญญัติในมาตรา 3 ในความผิดฐานเปลี่ยนแปลงโดยบราศจากอำนาจในสาระสำคัญเกี่ยวกับคอมพิวเตอร์ (computer material) ซึ่งตามพระราชบัญญัติฉบับนี้ เมื่อพิจารณาทั้งหมดจะสังเกตุได้ว่า ไม่มีบทบัญญัติที่จะให้คำนิยามของโปรแกรมไวรัสคอมพิวเตอร์ หรือบทมาตราใดที่จะกล่าวถึงการกระทำเกี่ยวกับไวรัสคอมพิวเตอร์ แต่นักกฎหมายของอังกฤษส่วนใหญ่ได้ให้ความเห็นว่าตาม the Computer Misuse Act 1990 นี้สามารถที่จะตีความขยายให้ครอบคลุมถึงการกระทำเกี่ยวกับไวรัสคอมพิวเตอร์นี้ได้เมื่อพิจารณาตามบทบัญญัติตามมาตรา 3 ประกอบกับมาตรา 17(7) ซึ่งเป็นบทบัญญัติที่ให้คำนิยามของคำว่า

"การเปลี่ยนแปลงเกี่ยวกับเนื้อหา" (modification of the contents) ที่กว้างขวางพอที่จะให้รวมถึงการกระทำเกี่ยวกับไวรัสคอมพิวเตอร์ได้

ซึ่งมาตรา 3 ของ the Computer Misuse Act 1990 บัญญัติว่า

"(1) บุคคลกระทำความผิด เมื่อ

(เอ) เขากระทำการใด ๆ ซึ่งก่อให้เกิดการเปลี่ยนแปลงเนื้อหาของคอมพิวเตอร์ใด ๆ โดยปราศจากอำนาจ และ

(บี) ในขณะที่เขากระทำ เขามีเจตนาธรรมดา (requisite intent) และเจตนาพิเศษ (requisite knowledge)

(2) เพื่อประโยชน์ในการปฏิบัติตามมาตรา (1)(บี) ข้างต้น เจตนาธรรมดาคือเจตนาที่ก่อให้เกิดการเปลี่ยนแปลงเนื้อหาของคอมพิวเตอร์ใด ๆ และโดยการกระทำดังนี้

(เอ) ทำให้เกิดความเสียหายแก่การปฏิบัติงานของคอมพิวเตอร์

(บี) เพื่อกีดกันหรือขัดขวางการเข้าถึงโปรแกรมหรือข้อมูลที่เก็บอยู่ในคอมพิวเตอร์ใด ๆ หรือ

(ซี) ทำให้เกิดความเสียหายแก่การปฏิบัติการของโปรแกรมหรือความเชื่อถือใด ๆ ของข้อมูล

(3) เจตนาไม่จำเป็นต้องกระทำโดยตรงต่อ

(เอ) คอมพิวเตอร์ใด ๆ โดยเฉพาะ

(บี) โปรแกรมหรือข้อมูลใดโดยเฉพาะ หรือโปรแกรมหรือข้อมูลชนิดใดชนิดหนึ่งโดยเฉพาะ

(ซี) แก้ไขเปลี่ยนแปลงอย่างใดโดยเฉพาะ หรือแก้ไขเปลี่ยนแปลงชนิดใดชนิดหนึ่งโดยเฉพาะ

(4) เพื่อประโยชน์ของการปฏิบัติตามมาตรา (1)(บี) ข้างต้น เจตนาพิเศษคือการรู้ว่าการแก้ไขเปลี่ยนแปลง เขาเจตนาที่จะกระทำขึ้นนั้นไม่มีอำนาจที่จะกระทำ

(5) มาตรานี้มิได้คำนึงว่า การเปลี่ยนแปลงโดยปราศจากอำนาจหรือผลที่เจตนาที่ให้

เกิดขึ้น หรือชนิดที่ได้กล่าวแล้วในอนุมาตรา (2) ข้างต้นได้กระทำหรือเจตนากระทำเป็นการถาวร หรือชั่วคราว"

ตามบทบัญญัตินี้ได้รวมถึงการกระทำเกี่ยวกับไวรัสคอมพิวเตอร์ เช่น การใส่โปรแกรมหนอนคอมพิวเตอร์ (worm) หรือม้าโทรจัน (Trojan Horse) เข้าไปในคอมพิวเตอร์ด้วย ซึ่งมีผลให้มีการใช้เนื้อที่ความจำของคอมพิวเตอร์ทั้งหมด หรือก่อให้เกิดผลกระทบต่อระบบการทำงานของคอมพิวเตอร์ได้รับความเสียหาย แม้ว่าผลกระทบของหนอนคอมพิวเตอร์ (worm) นี้จะไม่มีผลกระทบต่อสาระสำคัญ (โปรแกรมหรือข้อมูล) ที่บรรจุอยู่ในคอมพิวเตอร์ ซึ่งจะถูกครอบคลุมโดยคำนิยามของคำว่า "การเปลี่ยนแปลง" (modification) ตามมาตรา 17(7) ซึ่งหมายถึง

"การเปลี่ยนแปลงเนื้อหา(contents) ของคอมพิวเตอร์ใดเกิดขึ้น ถ้าการเกิดขึ้นนั้นมีผลต่อการปฏิบัติงานใดๆ ของคอมพิวเตอร์ ซึ่งมีผลต่อคอมพิวเตอร์นั้น หรือคอมพิวเตอร์อื่น ๆ

(เอ) โปรแกรมหรือข้อมูลใดๆ ที่เก็บอยู่ในคอมพิวเตอร์มีผลให้ถูกแก้ไขหรือถูกลบ หรือ

(บี) โปรแกรมหรือข้อมูลใด ๆ ถูกเพิ่มเข้าไป

และการกระทำใด ๆ ซึ่งมีส่วนที่เป็นสาเหตุให้เกิดการเปลี่ยนแปลง จะถูกพิจารณาว่าเป็นสาเหตุที่ก่อให้เกิดการเปลี่ยนแปลง"

และประกอบกับถ้อยคำในมาตรา 3(2)(เอ) ที่ใช้ถ้อยคำว่า "ทำให้เกิดความเสียหายแก่การปฏิบัติงานของคอมพิวเตอร์"

เมื่อพิจารณามาตรา 3 ประกอบมาตรา 17(7) แล้วจะเห็นว่า ขอบเขตของการกระทำที่จะอยู่ภายใต้ความผิดนี้มีขอบเขตที่กว้างขวาง ถึงรูปแบบที่แตกต่างของการกระทำที่ถูกรวมไว้ในขอบเขตของการกระทำความผิดนี้ ซึ่งจะครอบคลุมถึงความผิดที่เกี่ยวข้องกับการกระทำโดยเจตนาทั้งหมด แต่ไม่รวมถึงการกระทำโดยประมาท ในอันที่จะเป็นการเปลี่ยนหรือลบ เกี่ยวกับโปรแกรมหรือข้อมูลใด ๆ ของคอมพิวเตอร์ ก่อให้เกิดอุปสรรคในการเข้าถึงข้อมูล โดยผู้ใช้ที่มีอำนาจตามกฎหมาย หรือทำให้เกิดความเสียหายแก่การทำงานหรือความเชื่อถือของข้อมูลคอมพิวเตอร์ และที่

ซึ่งเขาได้รู้ถึงการเปลี่ยนแปลงโดยจงใจนั้น เป็นการกระทำที่ไม่ต้องพิสูจน์ว่าจำเลยได้มีเป้าหมายต่อคอมพิวเตอร์ โปรแกรม หรือข้อมูล โดยเฉพาะอยู่ในจิตใจหรือไม่

ดังนั้นหากมีการเพิ่มเติมโปรแกรมไวรัสคอมพิวเตอร์เข้าไป ย่อมเป็นการเพิ่มโปรแกรมแก่เนื้อหาของคอมพิวเตอร์ตามมาตรา 17(7)(บี) และด้วยการเพิ่มโปรแกรมนี้ ได้ก่อให้เกิดความเสียหายแก่การปฏิบัติงานของคอมพิวเตอร์ตามมาตรา 3(2)(เอ) ผู้กระทำความผิดจึงมีความผิดฐานเปลี่ยนแปลงโดยปราศจากอำนาจ ในสาระสำคัญเกี่ยวกับคอมพิวเตอร์ ต้องระวางโทษจำคุกไม่เกิน 6 เดือน ปรับไม่เกิน 2,000 ปอนด์ หรือทั้งจำทั้งปรับ

นอกจากนี้ ยังรวมถึงการที่ผู้กระทำผิดได้กระทำโดยเจตนา ที่จะนำโปรแกรมไวรัสคอมพิวเตอร์เข้าไปสู่ระบบคอมพิวเตอร์ โดยการมอบแผ่นดิสก์ที่มีโปรแกรมไวรัสคอมพิวเตอร์อยู่ เป็นเหตุให้ผู้บริสุทธิ์ได้รับความเสียหาย ในกรณีเช่นนี้ถือว่าผู้กระทำได้กระทำอันเป็นความผิดตั้งแต่ได้มอบแผ่นดิสก์ให้แก่ผู้อื่น ซึ่งเป็นไปตามมาตรา 17(7) ที่กำหนดว่า การกระทำใด ๆ ซึ่งเป็นการได้มอบออกไปนั้น เป็นสาเหตุโดยตรงต่อการเปลี่ยนแปลง โปรแกรมหรือข้อมูล ที่มีการจัดเก็บอยู่ในคอมพิวเตอร์

และแม้บุคคลผู้สุจริตซึ่งได้รับมอบแผ่นดิสก์ซึ่งมีโปรแกรมอันตรายอยู่ จะมิได้เป็นผู้ที่ใช้แผ่นดิสก์นั้นเอง แต่ได้นำไปมอบให้กับผู้อื่น และผู้นั้นได้นำไปใช้จนก่อให้เกิดความเสียหายต่อการทำงานของเครื่องคอมพิวเตอร์ ความรับผิดของผู้กระทำผิดในตอนแรกก็มิได้เปลี่ยนไป ทั้งนี้เพราะเจตนาของผู้กระทำผิดไม่ต้องมีเจตนาโดยตรงที่จะกระทำต่อคอมพิวเตอร์ โปรแกรม หรือข้อมูลใด ๆ โดยเฉพาะ ซึ่งเป็นไปตามมาตรา 3(3)

ด้วยเหตุผลทั้งหมดที่กล่าวมานี้ เป็นสิ่งที่นักกฎหมายของอังกฤษส่วนใหญ่เชื่อว่า กฎหมายฉบับนี้สามารถที่จะครอบคลุมถึงการกระทำเกี่ยวกับไวรัสคอมพิวเตอร์ด้วย แต่อย่างไรก็ตาม the Computer Misuse Act 1990 เป็นกฎหมายอาญาเกี่ยวกับคอมพิวเตอร์ฉบับแรกของอังกฤษ ซึ่งขณะร่างกฎหมายฉบับนี้ขึ้นมาปัญหาเกี่ยวกับ ไวรัสคอมพิวเตอร์ยังไม่ปรากฏ และแม้ภายหลังที่กฎหมายฉบับนี้มีผลบังคับใช้แล้วตั้งแต่วันที่ 29 สิงหาคม ค.ศ. 1990 ก็ไม่เคยมีคดีตัวอย่างขึ้นสู่การพิจารณาคดีของศาลอังกฤษ ว่าในการพิจารณาตีความของศาลจะออกมาในรูปแบบใด สิ่งเหล่านี้จึงเป็นสิ่งที่นักกฎหมายอังกฤษจะต้องคอยติดตามต่อไป