บทที่ 4

กฎหมายเกี่ยวกับการรักษาความปลอดภัยของข้อมูลในต่างประเทศ

4.1 การบัญญัติกฎหมายเพื่อรักษาความปลอดภัยของข้อมูลของประเทศสหรัฐอเมริกา

สหรัฐอเมริกาได้มีการบัญญัติกฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์ขึ้นมาฉบับแรก เมื่อปี ค.ศ. 1984 ได้แก่ The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 อันเป็นกฎหมายที่ออกมาเพื่อจะใช้แก้ปัญหาอาชญากรรมคอมพิวเตอร์โดยเฉพาะ สาเหตุสำคัญประการหนึ่งที่ต้องบัญญัติกฎหมายฉบับนี้ คือการสูญเสียทางการเงินปีละหลายร้อยล้านเหรียญสหรัฐอเมริกา การบัญญัติกฎหมายฉบับนี้สภาครองเกรสต้องใช้เวลาในการพิจารณาปัญหาต่างๆ เช่น การที่มีกฎหมายอาญาที่ใช้บังคับอยู่มากกว่า 40 ฉบับ สามารถนำมาใช้บังคับและครอบคลุมความผิดอาญาเกี่ยวกับคอมพิวเตอร์ได้มากน้อยเพียงใด และในที่สุดสภาครองเกรสก็ตัดสินใจที่จะบัญญัติกฎหมายขึ้นมาใหม่ แทนการปรับปรุงกฎหมายที่ใช้บังคับอยู่ แต่ในขณะที่สภาครองเกรสกำลังพิจารณาปัญหาต่างๆ อยู่ หลายมลรัฐในสหรัฐอเมริกาได้บัญญัติกฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์เป็นที่เรียบร้อยแล้ว

ภายหลังที่กฎหมายดังกล่าวได้ใช้บังคับแล้ว สหรัฐอเมริกาก็ยังต้องเผชิญกับปัญหาจำนวนมาก เช่น ความเหมาะสมในการให้คำนิยามของคำว่า "อาชญากรรมคอมพิวเตอร์" (Computer Crime) การกระจัดกระจายของคำนิยามซึ่งน่าจะจัดอยู่ในมาตราเดียวกัน การจำกัดวงเพื่อป้องกันเฉพาะงานของรัฐไม่ขยายไปสู่ภาคเอกชน การขาดความชัดเจนในมูลค่าการฟ้องร้อง ความเหลื่อมล้ำของเขตอำนาจศาล และปัญหาเกี่ยวกับวิธีพิจารณาความ เช่น การหาพยานหลักฐานมาพิสูจน์ความผิดมีจำนวนน้อยมาก ทำให้ไม่สามารถนำผู้กระทำความผิดมาลงโทษได้ ด้วยเหตุผลต่างๆ เหล่านี้ นักกฎหมายและผู้ที่เกี่ยวข้องจึงได้เรียกร้องให้มีการปรับปรุงกฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์ ในที่สุดก็มีการแก้ไขกฎหมายดังกล่าว วัตถุประสงค์ของการแก้ไขก็เพื่อที่จะเพิ่มประสิทธิภาพในการจัดการ และขจัดปัญหาต่างๆ ที่เกิดขึ้น แต่การแก้ไขก็ไม่ได้ครอบคลุมถึงการกระทำความผิดที่เกี่ยวกับการฉ้อฉลและการใช้คอมพิวเตอร์ในการกระทำความผิด

ต่อมาปี ค.ศ. 1986 ได้มีการออกกฎหมายฉบับใหม่คือ The Computer Fraud and Abuse Act of 1986 โดยกฎหมายฉบับนี้ได้เปลี่ยนแปลงสาระสำคัญไปจากกฎหมายฉบับเดิม 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 (พรชัย เหลียวพัฒนพงศ์, 2537 : 82)

กล่าวโดยสรุปการบัญญัติกฎหมายฉบับนี้ ได้ตั้งความหวังไว้ว่าจะเพิ่มประสิทธิภาพของกฎหมาย โดยการเพิ่มการกระทำที่ต้องห้าม และการใช้กฎหมายที่เหลื่อมล้ำ โดยเน้นสาระสำคัญว่าการกระทำที่ถือว่าเป็นการกระทำความผิดจะต้องกระทำโดยเจตนา และใช้ภาษาที่ชัดเจนเพื่อขจัดการตีความ

สำหรับเนื้อหาสาระของกฎหมายฉบับนี้ จำเป็นอย่างยิ่งที่จะต้องมีการกำหนดฐานความผิดในรูปแบบใหม่ เพื่อที่จะรองรับการกระทำความผิดที่เกิดขึ้น เนื่องจากเทคโนโลยีสารสนเทศเปลี่ยนแปลงไปอย่างรวดเร็ว จึงเกิดการกระทำความผิดในรูปแบบใหม่ๆ ที่ก่อให้เกิดความเสียหายอย่างมากมาย ซึ่งจำเป็นต้องคำนึงถึงการรักษาความปลอดภัยของข้อมูลในคอมพิวเตอร์ด้วย โดย The Computer Fraud and Abuse Act of 1986 ได้แบ่งฐานความผิดออกเป็น 3 ฐาน คือ ความผิดฐานเข้าถึงโดยปราศจากอำนาจ (Unauthorized Access) ความผิดฐานแก้ไขเปลี่ยนแปลง (Alteration) และความผิดฐานทำให้เสียหายหรือทำลาย (Damage or Destruction) โดยใช้บังคับเรื่อยมา ล่าสุดมีการแก้ไขบางอนุมาตรา เมื่อปี ค.ศ. 1994 ดังจะกล่าวถึงในหัวข้อต่อไป

4.2 ความรับผิดเกี่ยวกับการกระทำความผิดเกี่ยวกับข้อมูลในคอมพิวเตอร์ของประเทศสหรัฐอเมริกา

The Computer Fraud and Abuse Act of 1986 ของสหรัฐอเมริกาได้กำหนดการกระทำที่เป็นความผิดเกี่ยวกับข้อมูลในคอมพิวเตอร์ ซึ่งมีรูปแบบแตกต่างไปจากกฎหมายเดิมที่มีอยู่ เพื่อรองรับการกระทำความผิดที่เกิดขึ้นกับข้อมูล แบ่งออกเป็น 3 ฐานความผิดคือ

1. ความผิดฐานเข้าถึงโดยปราศจากอำนาจ (Unauthorized Access)
2. ความผิดฐานแก้ไขเปลี่ยนแปลง (Alteration)
3. ความผิดฐานทำให้เสียหายหรือทำลาย (Damage or Destruction)

4.2.1 **ความผิดฐานเข้าถึงโดยปราศจากอำนาจ (Unauthorized Access)**

ความผิดฐานเข้าถึงโดยปราศจากอำนาจเป็นความผิดชนิดหนึ่ง ซึ่งกฎหมายบัญญัติเป็นพิเศษไว้ใน The Computer Fraud and Abuse Act of 1986 มาตรา 1030 (a) อันเป็นเรื่องการฉ้อโกงหรือการกระทำการใดๆ ที่มีความสัมพันธ์กับคอมพิวเตอร์ โดยมีสาระสำคัญคือการกระทำโดยรู้อยู่แล้วหรือโดยเจตนาเพื่อที่จะเข้าถึงโดยปราศจากอำนาจหรือกระทำเกินอำนาจที่มีอยู่ ซึ่งครอบคลุมความผิด 6 ประเภท คือ

1. โดยรู้อยู่แล้วและได้เข้าสู่ระบบคอมพิวเตอร์โดยปราศจากอำนาจ อันได้ไปซึ่งสารสนเทศด้วยเจตนาหรือเหตุผลที่เชื่อว่าสารสนเทศนั้น อาจใช้เพื่อการอันเป็นภัยต่อความมั่นคงของประเทศหรือเพื่อผลประโยชน์ของชาวต่างชาติ ผู้กระทำผิดตามอนุมาตรานี้ จะถูกลงโทษปรับหรือจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ (และถ้ากระทำผิดซ้ำจะมีโทษจำคุกไม่เกิน 20 ปี)

2. โดยเจตนาจะเข้าสู่ระบบคอมพิวเตอร์โดยปราศจากอำนาจ เพื่อให้ได้ไปซึ่งข้อมูลทางการเงินหรือเข้าสู่ข้อมูลของสถาบันการเงิน จะถูกลงโทษปรับหรือจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ (และถ้ากระทำผิดซ้ำจะมีโทษจำคุกไม่เกิน 10 ปี)

3. โดยเจตนาที่เข้าสู่ระบบคอมพิวเตอร์ของรัฐบาลโดยปราศจากอำนาจ ด้วยการปลอมแปลงหรือแสร้งทำเป็นว่าเป็นเจ้าหน้าที่ของรัฐเพื่อกระทำการเปิดระบบประมวลผล จะถูกลงโทษปรับหรือจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ (และถ้ากระทำผิดซ้ำจะมีโทษจำคุกไม่เกิน 10 ปี)

4. โดยรู้อยู่แล้วเข้าสู่ระบบคอมพิวเตอร์ของรัฐบาลโดยปราศจากอำนาจ เพื่อผลประโยชน์ใดๆ ด้วยเจตนาที่จะฉ้อโกงหรือได้ไปซึ่งสิ่งที่มีค่าใดๆ จะถูกลงโทษปรับหรือจำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับ (และถ้ากระทำผิดซ้ำจะมีโทษจำคุกไม่เกิน 10 ปี)

5. โดยเจตนาที่จะเข้าสู่ระบบคอมพิวเตอร์ของรัฐบาลโดยปราศจากอำนาจ เพื่อผลประโยชน์ใดๆ หลังจากนั้นได้ทำการแก้ไขเปลี่ยนแปลง หรือทำลายสารสนเทศที่ได้เข้าถึงนั้น จะถูกลงโทษปรับหรือจำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับ (และถ้ากระทำผิดซ้ำจะมีโทษจำคุกไม่เกิน 10 ปี)

6. โดยรู้อยู่แล้วหรือโดยเจตนาที่จะฉ้อโกง ทำการใช้รหัสผ่านโดยปราศจากอำนาจ เพื่อเข้าถึงข้อมูลในคอมพิวเตอร์ของรัฐบาลเพื่อการค้าระหว่างรัฐหรือการค้าระหว่างประเทศ จะถูกลงโทษปรับหรือจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ (และถ้ากระทำผิดซ้ำจะมีโทษจำคุกไม่เกิน 10 ปี) (The U.S. Department of Justice, 1989 : 96-97)

จากบทบัญญัติข้างต้น เมื่อมีการเข้าถึงโดยปราศจากอำนาจเกิดขึ้น ผู้กระทำจะต้องมีความผิดตามอนุมาตรานั้นๆ อันเป็นบทบัญญัติที่ใช้สำหรับการแก้ไขปัญหาข้อขัดข้องของกฎหมาย นอกจากนั้นการเข้าถึงโดยปราศจากอำนาจ กฎหมายของประเทศสหรัฐอเมริกายังถือว่า

เป็นการลักขโมยบริการ (Theft of Service) เพราะเป็นการเข้าไปใช้บริการโดยปราศจากอำนาจ แม้ว่าการกระทำบางกรณีไม่ได้ก่อความเสียหายต่อระบบการทำงานของคอมพิวเตอร์ก็ตาม แต่กฎหมายก็ถือว่าเป็นความผิด โดยนักกฎหมายให้ความเห็นว่า "ถือว่าเป็นความเสี่ยงต่อการก่อให้เกิดผลเสียหายต่อสารสนเทศได้และผู้กระทำย่อมรู้ตัวดีว่า ความเสียหายในอนาคตอันใกล้จะปรากฏขึ้น" (สุเนติ คงเทพ, 2541 : 16) การเข้าถึงโดยปราศจากอำนาจอาจทำให้เจ้าของที่แท้จริงไม่สามารถเข้าสู่ระบบได้ การบัญญัติกฎหมายในความผิดฐานนี้ ก็มีวัตถุประสงค์เพื่อที่จะคุ้มครองผู้เช่า หรือผู้ใช้สายสื่อสารที่ต่อเชื่อมกับระบบคอมพิวเตอร์ ซึ่งครอบคลุมถึงการส่งข้อมูลผ่านสายสื่อสาร นอกจากการเข้าถึงโดยปราศจากอำนาจแล้ว ยังมีกรณีที่พนักงานหรือลูกจ้างของบริษัทใช้คอมพิวเตอร์เพื่อทำงานส่วนตัวโดยไม่ได้รับความยินยอมจากนายจ้าง กรณีนี้นิยมเรียกว่า "การทำงานกลางคืน" (Moonlight) การกระทำดังกล่าวข้างต้นไม่ว่าจะเป็นการกระทำของบุคคลที่ปราศจากอำนาจ หรือการกระทำของพนักงานหรือลูกจ้างที่ใช้คอมพิวเตอร์เพื่อทำงานส่วนตัว ถ้ามีการคัดลอกหรือทำสำเนาโปรแกรมหรือข้อมูล ก็จะถือเป็นความผิดฐานลักทรัพย์อีกฐานหนึ่งด้วย ดังจะเห็นได้จากคดีสหรัฐอเมริกา กับ จิราด (United Stated vs. Girard) ที่วินิจฉัยว่าการลักข้อมูลหรือสารสนเทศ (Information) จากคอมพิวเตอร์ ถือว่าเป็นการลักสิ่งที่มีค่าใดๆ (Thing of Value) อันเป็นความผิดฐานลักทรัพย์ การกระทำที่มิชอบเหล่านี้ นอกเหนือจากความผิดฐานลักทรัพย์แล้ว ยังมีความผิดฐานปลอมแปลงเอกสาร และความผิดฐานทำให้เสียทรัพย์ตามกฎหมายอาญา อันมีความแตกต่างกันในเรื่ององค์ประกอบของความผิดบางประการ ทำให้ไม่สามารถนำบทบัญญัติบางมาตราของกฎหมายในฐานความผิดเหล่านั้นมาใช้บังคับได้ อันจะได้กล่าวถึงต่อไป

นอกจากกรณีที่การเข้าถึงคอมพิวเตอร์ได้ก่อให้เกิดการกระทำที่มิชอบขึ้น อันเทียบเคียงได้กับฐานความผิดที่กล่าวมาแล้ว การเข้าถึงคอมพิวเตอร์ยังอาจก่อให้เกิดการกระทำที่มิชอบในลักษณะที่เป็นการเกี่ยวข้องกับความผิดตามกฎหมายอื่นๆ ที่มีอยู่แล้วอีกทางหนึ่งด้วย ดังนี้

กฎหมายการสื่อสารทางอิเล็กทรอนิกส์ส่วนบุคคล (The Electronic Communication Privacy Act of 1986) เป็นกฎหมายที่รับประกันการสื่อสารส่วนบุคคลผ่านทางโทรศัพท์ในระบบต่างๆ คลื่นวิทยุ การสื่อสารผ่านดาวเทียม และการสื่อสารผ่านทางเครือข่ายคอมพิวเตอร์ ไปรษณีย์อิเล็กทรอนิกส์ กฎหมายฉบับนี้ได้ปรับปรุงแก้ไขกฎหมายฉบับปี ค.ศ. 1968 กฎหมายฉบับนี้มีสาระสำคัญ คือ การกำหนดคำนิยามและข้อยกเว้น การสกัดการสื่อสารของภาคเอกชน การสกัดการสื่อสารของภาครัฐ การเก็บรักษาและการใช้ข้อมูลจากการสื่อสาร การรับจดทะเบียน ดังนั้น จะเห็นได้ว่าการเข้าถึงโดยปราศจากอำนาจที่เกี่ยวข้องกับการสื่อสารบางกรณีอาจมีความผิดตามกฎหมายฉบับนี้ (The U.S. Department of Justice, 1989 : 97-99)

กฎหมายการฉ้อโกงทางบัตรเครดิต (The Credit Card Fraud Act of 1984) กฎหมายฉบับนี้ในครั้งแรกออกมา เพื่อตั้งใจจะควบคุมการฉ้อโกงทางบัตรเครดิตและการปลอมบัตรเครดิต แต่เนื่องจากคำนิยามของคำว่า "บัตรเครดิต" ค่อนข้างจะมีความหมายกว้าง ทำให้ครอบคลุมถึงการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เช่น ความผิดที่เป็นการเข้าถึงสื่อทางคอมพิวเตอร์ หมายรวมถึงบัตรต่างๆ แผ่นพลาสติก รหัส หมายเลขบัญชี หรือสิ่งอื่นๆ ของบัญชี และการเข้าถึงไม่ใช่เพียงแต่หมายถึงการเข้าถึงข้อมูลด้านบัญชีเท่านั้น แต่ยังรวมการเข้าถึงสื่อทางคอมพิวเตอร์ด้วย อันถือได้ว่าเป็นการกระทำที่เอาไปซึ่งผลประโยชน์ เงินทอง สินค้า บริการ หรือสิ่งที่มีค่าใดๆ ในส่วนที่มีการอธิบายถึงความผิดเกี่ยวกับคอมพิวเตอร์นั้น เป็นการกระทำความผิดฐานกระทำการฉ้อโกงโดยการทำ ใช้ จำหน่าย หรือการปลอมสื่อทางคอมพิวเตอร์ รวมทั้งการเข้าถึงโดยปราศจากอำนาจ โดยได้กำหนดอัตราโทษไว้คือปรับตั้งแต่ 10,000 - 100,000 เหรียญสหรัฐอเมริกา หรือจำคุกตั้งแต่ 10 - 20 ปี หรือทั้งจำทั้งปรับ กฎหมายฉบับนี้อาจจะใช้กับผู้ที่หลอกลวงโดยใช้กลอุบาย ลักลอบเข้าไปในระบบคอมพิวเตอร์เพื่อที่จะค้นหา ทดสอบ หรือการแก้ไขเปลี่ยนแปลงข้อมูลต่างๆ เช่น หมายเลขโทรศัพท์ รหัสผ่าน ดังนั้น จากที่ได้กล่าวมาเห็นได้ว่าการเข้าถึงโดยปราศจากอำนาจที่เกี่ยวข้องกับบัตรเครดิตที่กฎหมายฉบับนี้ครอบคลุมถึง จะต้องถือว่าเป็นความผิดตามกฎหมายฉบับนี้ด้วย (The U.S. Department of Justice, 1989 : 99-100)

กฎหมายลิขสิทธิ์ (The Copyright Act of 1976) ในส่วนที่ถือว่าเป็นการละเมิดกฎหมายลิขสิทธิ์ที่มีโทษทางอาญา การเข้าถึงโดยปราศจากอำนาจที่ก่อให้เกิดการลักขโมยโปรแกรมหรือข้อมูลในคอมพิวเตอร์นั้น ยังอาจถูกฟ้องร้องได้ตามกฎหมายลิขสิทธิ์ของรัฐบาลกลางแห่งสหรัฐอเมริกา สำนักงานทะเบียนลิขสิทธิ์ได้ยอมรับการจดทะเบียนโปรแกรมคอมพิวเตอร์ว่าเป็น "หนังสือ" (Books) ชนิดหนึ่งมาตั้งแต่ปี ค.ศ. 1964 ตามรายงานของคณะกรรมการรัฐสภาเกี่ยวกับกฎหมายลิขสิทธิ์ ค.ศ. 1976 หน้า 54 ระบุว่า "งานวรรณกรรม" (Literary Works) รวมถึงฐานข้อมูลทางคอมพิวเตอร์และโปรแกรมคอมพิวเตอร์ ในขอบเขตที่ว่าให้รวมถึงงานประพันธ์ที่เป็นการแสดงออกถึงความคิดดั้งเดิมของนักเขียนโปรแกรมเข้าไว้ อันได้แยกออกจากตัวความคิดเอง ดังนั้น ผู้สร้างโปรแกรมคอมพิวเตอร์จึงสามารถป้องกันเอกสารและลายเส้นของรหัสคอมพิวเตอร์ได้จากการคัดลอกหรือทำสำเนาแต่การคุ้มครองทางลิขสิทธิ์นี้ก็ไม่ได้ขยายไปถึง "ขั้นตอนวิธี" (Algorithms) ของนักเขียนโปรแกรมด้วย

นอกจากบทบัญญัติสำหรับการดำเนินคดีทางแพ่ง และการเรียกร้องความเสียหายเนื่องจากการละเมิดทางลิขสิทธิ์แล้ว กฎหมายลิขสิทธิ์ (The Copyright Act of 1976) ยังได้กำหนดการลงโทษทางอาญาแก่การทำละเมิด และแก่การเคลื่อนย้ายโดยหลอกลวงเกี่ยวกับเอกสารที่มีลิขสิทธิ์ไว้ด้วย ความรับผิดทางอาญาของการละเมิด อาจพิสูจน์ได้โดยการแสดงถึงมูลฐานของการละเมิดในทางแพ่ง ความเป็นเจ้าของของคู่ความ และการคัดลอกหรือทำสำเนา รวมทั้งการแสดงถึงความตั้งใจและประโยชน์ทางการเงินที่ได้รับ ประมวลกฎหมายของสหรัฐอเมริกา บรรพที่ 17 มาตรา 506 (2) มาตรา 506 (a) กำหนดอัตราโทษสูงสุดไว้ ให้จำคุก 1 ปี และปรับ 10,000 เหรียญสหรัฐอเมริกา มาตรา 506 (b) ยังได้กำหนดอำนาจในการริบทรัพย์และการทำลายสำเนาเอกสารที่มีการละเมิดนั้นไว้อีกด้วย

มาตรา 506 (d) กำหนดให้การเคลื่อนย้ายหรือแก้ไขเอกสารอันมีลิขสิทธิ์ใดๆ ด้วยเจตนาที่จะหลอกลวงเป็นการกระทำผิดทางอาญา การกระทำเช่นนี้แม้จะไม่เป็นความผิดในทางแพ่งก็ถือว่าเป็นความผิดทางอาญา และบุคคลใดที่ได้ถูกตัดสินลงโทษในการกระทำดังกล่าวจะต้องถูกปรับเป็นเงินจำนวน 2,500 เหรียญสหรัฐอเมริกา

ความหมายในกฎหมายของมลรัฐทั้งหลาย ที่กล่าวถึงการกระทำที่เป็นความผิดทางอาญาหรือที่ถูกต้องตามกฎหมายอันรวมถึงการละเมิดทางลิขสิทธิ์นั้น ถือเป็นโมฆะภายใต้กฎหมายของรัฐบาลกลาง ตามหลักของการให้ใช้กฎหมายของรัฐบาลกลางบังคับก่อน (The Doctrine of Federal Preemption) (The U.S. Department of Justice, 1989 : 100)

กฎหมายการฉ้อโกงทางสายโทรเลข (The Wire Fraud Act) แต่เดิมประมวลกฎหมายสหรัฐอเมริกา บรรพที่ 18 มาตรา 1343 มีลักษณะเช่นเดียวกับ มาตรา 1341 คือ มีการยกเว้นการกระทำความผิดทางสายสื่อสารสาธารณะ แต่เมื่อมีกรณีที่ผู้ใช้คอมพิวเตอร์จากเครือข่ายทางไกลกระทำการฉ้อโกงทางคอมพิวเตอร์เกิดขึ้นเป็นจำนวนมาก ซึ่งมีทั้งการกระทำผิดลำพังเพียงคนเดียว และการร่วมกันกระทำความผิดหลายคน ทำให้เห็นได้ว่าตราบเท่าที่ยังมีการส่งข้อมูลผ่านทางสายสื่อสารสาธารณะ รัฐจะต้องเอาใจใส่ในเรื่องนี้ให้มากขึ้น มีรายงานเกี่ยวกับกรณีมาตรา 1343 มากมาย ทำให้รัฐจะต้องมีหน้าที่สร้างความเชื่อมั่นให้เกิดกับผู้ที่ทำการส่งข้อมูลผ่านสายสื่อสารสาธารณะว่าจะได้รับความปลอดภัย เพราะไม่ว่าจะเป็นการฉ้อโกงทางไปรษณีย์ (Mail Fraud) หรือ การฉ้อโกงทางสายสื่อสาร ผู้กระทำการฉ้อโกงจะได้รับผลประโยชน์ไปมากมาย และยังถือว่าเป็นการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ชนิดหนึ่งด้วย
(The U.S. Department of Justice, 1989 : 100-101)

กฎหมายเกี่ยวกับระเบียบสถาบันทางการเงินและการควบคุมอัตราดอกเบี้ย (The Financial Institutions Regulatory and Interest Rate Control Act of 1978 : FIRA) ซึ่งมีกฎหมายเกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์ (The Electronic Fund Transfer Act) อันเป็นส่วนหนึ่งของกฎหมายเกี่ยวกับระเบียบสถาบันทางการเงินและการควบคุมอัตราดอกเบี้ย โดยมีวัตถุประสงค์คือการกำหนดคำนิยามและสิทธิส่วนบุคคลของผู้บริโภค ผู้ซึ่งได้รับผลกระทบจากการโอนเงินทางอิเล็กทรอนิกส์ กฎหมายฉบับนี้ได้กำหนดให้รัฐบาลกลางออกระเบียบการโอนเงินทางอิเล็กทรอนิกส์ขึ้น โดยประกอบด้วยการก่อตั้งหลักฐานแห่งสิทธิ ความรับผิด และภาระหน้าที่ต่างๆ ของคู่สัญญา รวมถึงตัวสถาบันการเงิน ผู้บริโภค ผู้ใช้บริการ และผู้ที่เกี่ยวข้องกับการโอนเงินทางอิเล็กทรอนิกส์ทั้งหมด

มาตรา 916 ของกฎหมายฉบับนี้ เป็นมาตราที่เกี่ยวกับความรับผิดทางอาญา ซึ่งมีความเกี่ยวข้องโดยตรง หรืออย่างน้อยที่สุดก็มีสัมพันธ์กับการกระทำความผิดทางอาญาเกี่ยวกับคอมพิวเตอร์ อันอยู่ในการดูแลของรัฐบาลกลาง โดยมีการกำหนดให้มีโทษปรับไม่เกิน 5,000 เหรียญสหรัฐอเมริกา หรือจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ แก่บุคคลที่โดยรู้อยู่แล้วหรือจงใจให้ข้อมูลอันเป็นความเท็จ โดยไม่ให้ข้อมูลตามที่กฎหมายกำหนด หรือตามระเบียบต่างๆ ที่มีการประกาศโดยกฎหมายฉบับนี้ หรือจะกล่าวอีกนัยหนึ่งก็คือว่าเป็นการละเว้นกฎหมายหรือระเบียบ

มาตรา 2 ของบทบัญญัติเกี่ยวกับความรับผิดทางอาญา ได้กำหนดอัตราโทษปรับไม่เกิน 10,000 เหรียญสหรัฐอเมริกา หรือจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ แก่การกระทำ 6 ประการ เมื่อเกี่ยวข้องกับการค้าระหว่างรัฐหรือระหว่างประเทศ เมื่อเกี่ยวข้องกับเงิน สินค้า บริการ หรือสิ่งมีค่าใดๆ ที่มีมูลค่าตั้งแต่ 1,000 เหรียญสหรัฐอเมริกาขึ้นไป หรือเมื่อนำมารวมกันภายในระยะเวลา 1 ปี และเมื่อมีการปลอม การทำของเท็จ การแก้ไข การทำให้สูญหาย การลักขโมย หรือการได้มาโดยการหลอกลวง ที่เกี่ยวกับเครื่องมือในการชำระหนี้ (Debit Instrument) คำว่า "เครื่องมือในการชำระหนี้" (Debit Instrument) หมายถึงบัตร รหัส หรือสื่อใดๆ ที่บุคคลนำไปใช้ในการโอนเงินทางอิเล็กทรอนิกส์ได้ การกระทำทั้ง 6 ประการที่กล่าวข้างต้น ได้แก่

1. รู้อยู่แล้วแต่กระทำการใช้ หรือพยายามที่จะร่วมกันใช้เครื่องมือในการชำระหนี้เพื่อที่จะได้ไปซึ่งสิ่งที่มีค่าใดๆ ตามรายละเอียดที่กล่าวข้างต้น

2. เจตนาที่ผิดกฎหมายหรือเจตนาหลอกลวง กระทำการเคลื่อนย้ายหรือพยายามที่จะร่วมกันเคลื่อนย้ายเครื่องมือในการชำระหนี้ โดยรู้อยู่แล้วว่าเป็นของปลอม ของถูกลักขโมย ฯลฯ

3. เจตนาที่ผิดกฎหมายหรือเจตนาหลอกลวง ใช้การค้าระหว่างมลรัฐหรือการค้าระหว่างประเทศเป็นเครื่องมือในการจำหน่ายหรือเคลื่อนย้ายเครื่องมือในการชำระหนี้ โดยรู้อยู่แล้วว่าเป็นของปลอม ของถูกลักขโมย ฯลฯ

4. รู้อยู่แล้วแต่กระทำการรับไว้ ปกปิด ซ่อนเร้น ใช้ หรือเคลื่อนย้ายสิ่งที่มีค่าใดๆ อันอยู่ในการค้าระหว่างมลรัฐหรือการค้าระหว่างประเทศ ซึ่งเป็นสิ่งที่ได้มาโดยเครื่องมือในการชำระหนี้ที่เป็นของปลอม ของถูกลักขโมย ฯลฯ

5. รู้อยู่แล้วแต่กระทำการรับไว้ ปกปิด ซ่อนเร้น ใช้ จำหน่าย หรือเคลื่อนย้าย ใบแสดงยอดหนึ่งใบหรือมากกว่านั้น โดยอาศัยการค้าระหว่างมลรัฐหรือการค้าระหว่างประเทศ อันมีมูลค่ารวมกันตั้งแต่ 500 เหรียญสหรัฐอเมริกาขึ้นไป ภายในเวลา 1 ปี และเป็นของที่ได้มาหรือซื้อมาโดยการใช้เครื่องมือในการชำระหนี้ที่เป็นของปลอม ของถูกลักขโมย ฯลฯ

6. รายการที่มีผลกระทบต่อการค้าระหว่างมลรัฐหรือการค้าระหว่างประเทศ ให้ได้สิ่งที่มีค่าใดๆ ไป โดยผ่านการใช้และรู้อยู่แล้วว่าเป็นเครื่องมือในการชำระหนี้ที่เป็นของปลอม ของถูกลักขโมย ฯลฯ (The U.S. Department of Justice, 1989 : 101)

กฎหมายคุ้มครองส่วนบุคคล (The Privacy Act of 1974) ได้ประมวลไว้ในประมวลกฎหมายสหรัฐอเมริกา บรรพที่ 5 มาตรา 552a อันมีโทษทางอาญาสำหรับการกระทำผิด โดยบัญญัติอยู่ในอนุมาตรา (I) (1) - (3) การลงโทษทางอาญาจะเกิดขึ้นนั้น เนื่องมาจากฝ่าฝืนบทบัญญัติของกฎหมายดังกล่าว เช่น การตั้งใจเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจที่จะกระทำได้ โดยกระทำจากฐานข้อมูลในคอมพิวเตอร์

พื้นฐานของกฎหมายดังกล่าวเป็นการคุ้มครองความเป็นส่วนตัวของบุคคล ดังนั้นในประมวลกฎหมายสหรัฐอเมริกา บรรพที่ 5 มาตรา 551 (1) และ มาตรา 552 (e) จึงได้กำหนดคำนิยามของคำว่า "ตัวแทน" (Agency) ไว้ และห้ามมิให้ตัวแทนกระทำการเปิดเผยบันทึกเอกสารใดๆ ที่ได้เก็บอยู่ในระบบบันทึกทางเอกสารแก่บุคคลอื่น หรือแก่ตัวแทนอื่น แต่มีข้อยกเว้นต่างๆ หลายประการ เช่น เว้นแต่ผู้เป็นเจ้าของบันทึกเอกสารนั้นได้ร้องขอ โดยการทำเป็นหนังสือมายังตัวแทน หรือได้ให้ความยินยอมโดยได้ทำเป็นหนังสือให้กับตัวแทนไว้ก่อนแล้ว

ถ้าพนักงานหรือลูกจ้างของตัวแทนรู้อยู่แล้วว่าการเปิดเผยข้อความพิเศษนั้น ได้มีการห้ามไว้โดยกฎหมายดังกล่าวหรือโดยระเบียบที่ออกโดยกฎหมายดังกล่าว แต่พนักงานหรือลูกจ้างผู้นั้นตั้งใจเปิดเผยข้อความนั้นต่อบุคคลอื่น หรือต่อตัวแทนอื่นที่ไม่มีสิทธิที่จะได้รับทราบข้อความนั้น พนักงานหรือลูกจ้างผู้นั้นจะต้องมีความผิดอาญาในระดับเบา (Misdemeanor) และต้องถูกปรับไม่เกิน 5,000 เหรียญสหรัฐอเมริกา

อัตราโทษดังกล่าวข้างต้นยังนำมาใช้กับ พนักงานหรือลูกจ้างที่กระทำการโดยจงใจเพื่อให้การดูแลรักษาระบบเอกสาร ไม่เป็นไปตามบทบัญญัติในอนุมาตรา (e) (4) ซึ่งรวมถึงการเก็บรักษาข้อมูลในฐานข้อมูลคอมพิวเตอร์ด้วย อนุมาตรา (e) (4) ต้องการให้แต่ละตัวแทนดูแลรักษาระบบเอกสาร และประกาศถึงความอยู่มีของเอกสารนั้นรวมถึงลักษณะของระบบเอกสารนั้นๆ ลงในทะเบียน (Federal Register) ไม่น้อยกว่าหนึ่งครั้งต่อปี ประกาศดังกล่าวต้องมีการระบุถึงชื่อระบบ สถานที่ตั้ง และประเภทของบุคคลที่เป็นเจ้าของ รวมถึงแหล่งที่มาของเอกสารนั้นๆ การใช้งานตามปกติ วิธีการเก็บรักษา การเรียกคืน การควบคุมการเข้าถึง นโยบายและแนวทางปฏิบัติในการใช้เอกสาร พนักงานของตัวแทนที่เป็นผู้รับผิดชอบ ระเบียบการในการใช้ การแจ้งให้เจ้าของได้รับทราบตามความต้องการ เอกสารเหล่านั้นได้บรรจุเรื่องของเจ้าของและระเบียบการสำหรับเจ้าของในการใช้ประโยชน์จากการเข้าถึง รวมทั้งการโต้แย้งข้อความจะบรรจุอยู่ในเอกสารนี้ด้วย

ประการสุดท้ายอัตราโทษดังกล่าว ยังอาจนำมาใช้กับบุคคลใดบุคคลหนึ่ง ผู้ที่โดยรู้อยู่แล้วหรือโดยจงใจเรียกร้องหรือได้ไปซึ่งเอกสารของผู้อื่นโดยการฉ้อโกงหรือหลอกลวง (The U.S. Department of Justice, 1989 : 101)

ประมวลกฎหมายอาญาสหรัฐอเมริกา ซึ่งมีอย่างน้อย 40 มาตรา ในประมวลกฎหมายสหรัฐอเมริกา บรรพที่ 18 ที่พบว่ามีการใช้คอมพิวเตอร์กระทำความผิดทั้งโดยทางตรงและทางอ้อม สำหรับความผิดที่จะนำมาวิเคราะห์แบ่งออกเป็น 7 กลุ่ม คือ ความผิดฐานลักขโมย ความผิดเบ็ดเตล็ดเกี่ยวกับการลักทรัพย์ ความผิดฐานใช้ช่องทางการสื่อสาร ความผิดเกี่ยวกับความมั่นคงของประเทศ ความผิดฐานบุกรุก ความผิดฐานหลอกลวง และความผิดฐานทำให้เสียทรัพย์ แต่ที่เกี่ยวข้องกับความผิดฐานเข้าถึงโดยปราศจากอำนาจ มีด้วยกัน 6 กลุ่ม ส่วนกลุ่มที่ 7 คือความผิดฐานทำให้เสียทรัพย์ จะนำไปวิเคราะห์ในส่วนที่ว่าด้วยความผิดฐานทำให้เกิดความเสียหายหรือทำลาย

1. ความผิดฐานลักขโมย (Theft and Related Offenses) ประมวลกฎหมายสหรัฐอเมริกา บรรพที่ 18 มาตรา 641 มีหลักการพื้นฐานเพื่อที่จะปกป้องทรัพย์จากการถูกลักขโมย แต่สถานะของกฎหมายครอบคลุมไปทั้งการลักทรัพย์และการรับของโจร แม้ว่าบทบัญญัติส่วนมากจะมีข้อความตรงไปตรงมา แต่ก็มีหลายกรณีเกี่ยวพันโดยตรงกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ อันเนื่องมาจากการแปลความในลักษณะที่กว้าง โดยแยกพิจารณาได้ดังนี้

1.1 บุคคลผู้ที่โดยรู้อยู่แล้วเข้าถือกรรมสิทธิ์ (Convert) ในสาธารณะสมบัติถือว่าบุคคลนั้นกระทำความผิดตามมาตรา 641 โดยไม่อาจยกข้อต่อสู้ว่าตนจะคืนทรัพย์นั้นหรือชดใช้ค่าเสียหายให้ในภายหลัง

ความผิดฐานเข้าถือกรรมสิทธิ์แบ่งออกเป็น

(ก) การเข้าถือครองและใช้สิทธิความเป็นเจ้าของแต่เพียงผู้เดียว เหนือทรัพย์สินของบุคคลอื่นโดยปราศจากอำนาจ หรือ

(ข) กระทำการโดยปราศจากอำนาจใดๆ อันเป็นการตัดสิทธิความเป็นเจ้าของในทรัพย์สินของบุคคลอื่นอย่างถาวรหรือไม่จำกัดระยะเวลา หรือให้ความช่วยเหลือยุยงส่งเสริมบุคคลอีกคนหนึ่งเก็บทรัพย์สินไว้แยกจากเจ้าของที่แท้จริง หรือ

(ค) การเข้าถือเอาทรัพย์สินของบุคคลอื่นโดยมิชอบ

จากตัวอย่างในคดีมอริสเสท กับ สหรัฐอเมริกา (Morissette vs. United States) ได้วินิจฉัยว่า "ความผิดฐานเข้าถือกรรมสิทธิ์...อาจสำเร็จได้โดยไม่ต้องมีเจตนาที่จะเก็บรักษาไว้..." เว้นแต่การกระทำนั้นจะไม่ตอบสนองต่อความจำเป็นในการที่จะต้องมีเจตนาร้าย (Mens Rea) ในขณะที่ศาลไม่เคยมีการพิจารณาว่า บุคคลอาจจะยักยอก ลักขโมย หรือฉกฉวยโปรแกรมคอมพิวเตอร์ โดยการคัดลอกหรือทำสำเนาหรือโดยวิธีอื่น แต่ก็ดูเหมือนเป็นเรื่องที่เป็นไปได้ค่อนข้างสูงว่า การกระทำผิดโดยไม่มีสิทธิพิเศษ อาจถือได้ว่าเป็นการเข้าถือกรรมสิทธิ์อย่างหนึ่ง

อย่างไรก็ตาม การเข้าถือกรรมสิทธิ์อาจสำเร็จได้โดยไม่ต้องมีเจตนาที่จะเก็บรักษาทรัพย์สินไว้และโดยที่ปราศจากการแย่งครองที่ผิดกฎหมาย โดยผู้เข้าถือกรรมสิทธิ์นั้นเป็นเรื่องชอบด้วยกฎหมายทั้งสิ้น การเข้าถือกรรมสิทธิ์อาจรวมถึงการใช้ทรัพย์สินไปในทางที่ผิดหรือทางที่มิชอบ และอาจรวมไปถึงการใช้โดยปราศจากอำนาจ ไม่ใช่เรื่องยากที่จะคาดคิดถึงลักษณะการใช้ทรัพย์สินของรัฐในทางที่ผิดและโดยปราศจากอำนาจ โดยเจตนาหรือรู้อยู่แล้ว ซึ่งอาจจะเป็นกรณีของการเข้าถือกรรมสิทธิ์โดยรู้อยู่แล้ว แต่ไม่รวมถึงกรณีการยักยอก ลักขโมย หรือฉกฉวย การเข้าถือกรรมสิทธิ์โดยรู้อยู่แล้วนั้น ช่วยขยายขอบเขตของการคุ้มครองทรัพย์สินของรัฐได้อย่างดี จากคดีสหรัฐอเมริกา กับ ไทเจอรินา (United States vs. Tijerina) ได้วินิจฉัยว่า "การแย่งไปซึ่งสิทธิในการควบคุมรถบรรทุกชั่วระยะเวลาหนึ่งนั้นเป็นความผิดฐานเข้าถือกรรมสิทธิ์ ตามมาตรา 641"

1.2 ความคิดเห็นต่อคำว่า "เข้าถือกรรมสิทธิ์" นั้น มีอยู่อย่างกว้างขวาง ดังเช่นคำว่า Res หมายถึง วัตถุสิ่งของ ยิ่งไปกว่านั้นตัวบทบัญญัติก็มีความหมายกว้างพอที่จะรวมไปถึงการลักขโมยแรงงานหรือบริการ เนื่องจากการตีความตามนัยที่กว้าง เช่น คำว่า "สิ่งที่มีค่าใดๆ"

1.3 ความหมายของถ้อยคำที่ว่า "ของสหรัฐอเมริกาหรือ กระทรวง ทบวง กรม หรือตัวแทนใดๆ" เป็นประโยคที่กว้างกว่าความเป็นเจ้าของธรรมดา คำว่า "ตัวแทน" ของสหรัฐอเมริกาในท่ามกลางคำอื่นนั้น มีความหมายว่า "นิติบุคคลใดๆ ซึ่งสหรัฐอเมริกามีผลประโยชน์ในความเป็นเจ้าของ..." ประมวลกฎหมายสหรัฐอเมริกา บรรพที่ 18 มาตรา 6 ในถ้อยคำที่ว่า "ผลประโยชน์ในความเป็นเจ้าของ" เป็นถ้อยคำที่กว้างโดยรวมถึงความเป็นเจ้าของในทรัพย์สินใดๆ

จากคดีสหรัฐอเมริกา กับ แอนเดอร์สัน (United Stated vs. Anderson) ได้วินิจฉัยว่า สหรัฐอเมริกามีอำนาจในการควบคุมการใช้สาธารณะสมบัติ แม้ว่าจะอยู่ในมือของเอกชนก็ตาม จากคดีเบอร์นาร์ด กับ สหรัฐอเมริกา (Bernhardt vs. United States) ได้วินิจฉัยว่า ทรัพย์สินที่อยู่ในการควบคุมดูแลของกองทัพย่อมได้รับความคุ้มครองตามมาตรา 641 จากคดีสหรัฐอเมริกา กับ เอชเชอร์วาเรีย (United States vs. Echevarria) ได้วินิจฉัยว่า เงินงบประมาณของสหรัฐอเมริกาที่จ่ายให้กับมหาวิทยาลัยย่อมได้รับความคุ้มครองตามมาตรา 641

แม้ว่าจะยังไม่เคยมีคดีที่วินิจฉัยเกี่ยวข้องกับเรื่องนี้โดยตรง แต่ก็ดูเหมือนจะเป็นที่แน่ชัดว่า ผลประโยชน์ที่ร่วมกันไม่ว่าจะแบ่งแยกได้หรือไม่ได้ หรือผลประโยชน์ตามความยุติธรรม เช่น "สิทธิในการใช้" (Right to Use) อาจจะมีการเข้าถือกรรมสิทธิ์ได้ ดังนั้น ในกรณีที่รัฐซื้อสิทธิในการใช้โปรแกรมคอมพิวเตอร์ และโปรแกรมนั้นถูกยักยอกไป ก็อาจจะฟ้องร้องได้ตามมาตรา 641 อนึ่งได้มีคดีหนึ่งกล่าวว่าทรัพย์ที่อยู่ในการควบคุมดูแลของรัฐหรือที่รัฐเป็นเจ้าของอาจเป็นวัตถุแห่งการลักทรัพย์ได้ แม้ว่ารัฐจะไม่มีกรรมสิทธิ์ในทรัพย์สินนั้นตามกฎหมายก็ตาม จากคดีสหรัฐอเมริกา กับ การ์ดเนอร์ (United States vs. Gardner) ได้วินิจฉัยว่าทรัพย์สินที่รอการยึดอันได้มาจากการหนีภาษีศุลกากร เป็นวัตถุแห่งการลักทรัพย์ได้

1.4 เป็นเรื่องที่ชัดเจนว่า ถ้ามีการพัฒนาโปรแกรมเพื่อประโยชน์ของรัฐ การลักหรือการเข้าถือกรรมสิทธิ์ในตัวโปรแกรมนั้น ถือเป็นความผิดตามมาตรา 641 ยิ่งไปกว่านั้น จากคดีสหรัฐอเมริกา กับ แอนเดอร์สัน (United States vs. Anderson) แสดงให้เห็นว่าวัตถุดิบต่างๆ อาจรวมอยู่ในความหมายดังกล่าวด้วย

ในการตีความอย่างกว้าง การยักยอกโปรแกรมคอมพิวเตอร์ใดๆ ที่เป็นวัตถุแห่งการกระทำผิดที่อยู่ในการควบคุมดูแลของรัฐ หรือที่รัฐเป็นเจ้าของ เป็นความผิดตามมาตรา 641

มีคำพิพากษาเกี่ยวกับเรื่องนี้อย่างน้อยสองเรื่องคือ คดีสหรัฐอเมริกา กับ ดิจิลิโอ (United States vs. Digilio) ได้ตัดสินลงโทษผู้ร่วมกระทำความผิดโดยทำการหลอกลวงและเข้าถือกรรมสิทธิ์ในเอกสารต่างๆ เพื่อประโยชน์ของจำเลย โดยเฉพาะอย่างยิ่งสำเนาภาพถ่ายแฟ้มข้อมูลของหน่วยงานสืบสวนสอบสวนของรัฐบาลกลางสหรัฐอเมริกา (Federal Bureau of Investigation : FBI) คดีนี้จำเลยทั้งสองให้การต่อสู้ว่าจะนำมาตรา 641 มาใช้บังคับไม่ได้ เพราะรัฐไม่ได้ถูกแย่งสิทธิในการใช้ข้อมูลที่เก็บอยู่ในแฟ้มข้อมูลเหล่านั้น และสำเนาเอกสารของรัฐไม่เป็นเอกสารในตัวเอง อีกทั้งมาตรา 641 ก็ไม่ได้ห้ามการส่งข้อมูลดังกล่าวโดยปราศจากอำนาจ

รัฐได้วางหลักเกณฑ์พื้นฐาน ข้อต่อสู้เกี่ยวกับความสามารถในการบังคับใช้ของมาตรา 641 ไว้ในคดีสหรัฐอเมริกา กับ บอทโทน (United Stated vs. Bottone) วินิจฉัยว่า การถ่ายภาพไมโครฟิล์มเป็นการนำเอาวิธีทางวิทยาศาสตร์มาใช้ผ่านเครื่องมือของผู้ลักทรัพย์ โดยมีการนำสำเนาภาพถ่ายนั้นเคลื่อนที่ไป อันเป็นการต้องห้ามในความผิดฐานลักทรัพย์ ซึ่งศาลได้วินิจฉัยคล้อยตามความเห็นของรัฐซึ่งเป็นโจทก์ และศาลยังได้หมายเหตุไว้ว่าในคดีดิจิลิโอไม่ปรากฏว่ามีความจำเกี่ยวกับข้อมูล และสิ่งที่ถูกคัดลอกหรือทำสำเนาไปโดยใช้เครื่องมือของผู้กระทำการลักทรัพย์ ผู้กระทำได้ใช้ เวลา เครื่องมือ เครื่องใช้ของรัฐในการคัดลอกหรือทำสำเนาดังกล่าว ประการสุดท้ายศาลยังได้อ้างถึงสำเนาเอกสารคู่ฉบับ อันเป็นความมุ่งหมายของกฎหมายและสำเนาเอกสารคู่ฉบับของรัฐนั้นเองที่ถูกลักไป

จากคดีสหรัฐอเมริกา กับ แลมเบอร์ (United Stated vs. Lambert) เป็นคดีเกี่ยวกับมาตรา 641 จำเลยถูกกล่าวหาว่าได้กระทำการจำหน่ายข้อมูลที่ได้จากคอมพิวเตอร์ของสำนักงานยาเสพติดแห่งกรุงวอชิงตัน ดี ซี ข้อมูลดังกล่าวรวมถึงหลักฐานของข้อมูล และสถานภาพของการสอบสวนของรัฐเกี่ยวกับการขนย้ายยาเสพติด เพียงแต่ข้อมูลเท่านั้น ไม่ใช่ตัวเอกสารที่บรรจุข้อมูลนั้นได้ถูกโอนไป จำเลยได้ต่อสู้ว่า มาตรา 641 สามารถใช้บังคับกับวัตถุที่มีรูปร่างเท่านั้น เช่น กระดาษที่บรรจุข้อมูลไม่ใช่ตัวข้อมูล อย่างไรก็ตามศาลได้วินิจฉัยว่าข้อความที่แปลความครอบคลุมถึงคือ คำว่า "สิ่งที่มีค่าใดๆ" (Thing of Value) ในบทบัญญัติดังกล่าว โดยเห็นได้จากการแสดงถึงเจตนาที่จะให้ครอบคลุมได้อย่างกว้างขวาง

ศาลเห็นว่าไม่มีเหตุผลใดที่จะจำกัดการตีความในมาตรา 641 ให้เป็นไปตามหลักดั้งเดิมของกฎหมายคอมมอนลอว์ โดยวินิจฉัยว่าควรใช้มาตรา 641 ให้ครอบคลุมความผิดฐานลักทรัพย์ในรูปแบบสถานการณ์ใหม่ๆ อันเกิดขึ้นจากเงื่อนไขการเปลี่ยนแปลงของสังคมและไม่อยู่ภายใต้กฎหมายคอมมอนลอว์ ศาลเห็นด้วยกับรัฐว่าทรัพย์สินที่เกี่ยวข้องมีความอ่อนไหวสูง และข้อมูลจะถูกดูแลรักษาไว้ในสื่อทางคอมพิวเตอร์ และจะยังคงมูลค่าอยู่ถ้าข้อมูลยังคงอยู่ในความครอบครองของรัฐแต่เพียงผู้เดียว ดังนั้น ศาลจึงได้วินิจฉัยว่า คำว่า "สิ่งที่มีค่าใดๆ" (Thing of Value) และการอ้างอิงที่แน่ชัดของเอกสารในมาตรา 641 ครอบคลุมถึงสิ่งที่บรรจุอยู่ในเอกสารดังกล่าวด้วย

ประมวลกฎหมายสหรัฐอเมริกา บรรพที่ 18 มาตรา 659 เป็นบทบัญญัติเกี่ยวกับการลักสังหาริมทรัพย์ที่กำลังเคลื่อนที่ ซึ่งอาจเป็นส่วนหนึ่งของการค้าระหว่างมลรัฐ เช่น โปรแกรมคอมพิวเตอร์อาจจะถูกส่งไปยังอีกมลรัฐหนึ่ง เมื่อเป็นเช่นนี้ มาตรา 659 ก็จะคุ้มครองไม่

ให้ถูกลักโดยไม่คำนึงถึงสิทธิความเป็นเจ้าของแตกต่างกับมาตรา 641 มาตรา 659 ไม่ได้ห้ามคัดลอกหรือทำสำเนาโดยปราศจากอำนาจ แม้ว่ามีการใช้คำว่า "แปลง" (Conversion) อันมีความหมายตรงกันในส่วนของเจตนาของผู้กระทำเท่านั้น ไม่ใช่ในส่วนของการกระทำ ซึ่งจะต้องเป็นการยักยอก ลักขโมย ฯลฯ และสิ่งที่น่าสนใจมากในมาตรา 659 คือ การนำส่วนของการลักทรัพย์มาใช้กับกิจการค้าระหว่างมลรัฐ

ข้อพิจารณาที่ดีมากที่จะทำให้เห็นถึงส่วนประกอบต่างๆ และการตีความที่กว้างของการค้าระหว่างมลรัฐในมาตรา 659 เห็นได้จากคดีสหรัฐอเมริกา กับ แอสโทลาส (United States vs. Astolas) ที่ศาลปฏิเสธคำอุทธรณ์ของจำเลยที่ว่า รถบรรทุกที่จำเลยได้ปล้นยังไม่ใช่อยู่หรือได้พ้นไปจากข่ายของการค้าระหว่างมลรัฐแล้ว ท่านผู้พิพากษาเมดินา (Medina) ได้ให้เหตุผลว่าตามที่ศาลล่างได้พิจารณาว่าลักษณะที่อยู่ในข่ายของที่ขนส่งระหว่างมลรัฐ เริ่มต้นเมื่อของนั้นได้เคลื่อนออกจากกิจการค้าระหว่างมลรัฐ และเข้ามาอยู่ในความครอบครองของบุคคลที่ดำเนินการขนส่งระหว่างมลรัฐ และยังเป็นอยู่นี้ต่อไปจนกว่าของนั้นไปถึงจุดหมายปลายทางและได้ส่งมอบต่อไป ไม่ว่าจะเป็นการส่งมอบไปจริง หรือการรอไว้เพื่อการส่งมอบ

ข้อกำหนดของการมีอยู่ของการค้าระหว่างมลรัฐ เกี่ยวกับเวลาของการลักทรัพย์ จากคดีสหรัฐอเมริกา กับ ไทเออร์ (United States vs. Tyers) ได้วินิจฉัยว่า การที่ผู้กระทำการลักโปรแกรมคอมพิวเตอร์และส่งต่อให้ผู้ร่วมกระทำความผิดในภายหลัง ไม่ทำให้ผู้ร่วมกระทำความผิดพ้นจากความรับผิดไปได้ แม้ว่าจะไม่มีการค้าระหว่างมลรัฐอยู่ในเวลานั้นแล้วก็ตาม อีกกรณีหนึ่งเจ้าของโปรแกรมคอมพิวเตอร์จะต้องเป็นผู้ขนส่งด้วยหรือไม่ ไม่ใช่เรื่องสำคัญ ดังจะเห็นได้ชัดว่ามาตรา 659 ครอบคลุมถึงการขนส่งโดยผู้เป็นเจ้าของทรัพย์ด้วย จากคดี ไวเนอร์ กับ สหรัฐอเมริกา (Winer vs. United States) เป็นที่แน่ชัดว่าในบางครั้งการค้าระหว่างมลรัฐก็สิ้นสภาพลง แต่ปัจจุบันก็มีการยอมรับตามขั้นตอนต่างๆ โปรแกรมคอมพิวเตอร์ที่อยู่ระหว่างการขนส่งหรือยังไม่มีการส่งมอบ มาตรา 659 อาจนำไปใช้บังคับได้ โดยมีคดีต่างๆ ที่เกิดขึ้น ดังนี้ คดีโอเคลลี กับ สหรัฐอเมริกา (O'kelly vs. United States) เป็นการลักทรัพย์จากรถตู้ที่มีการส่งมอบแล้วบางส่วน คดีสหรัฐอเมริกา กับ เชอร์แมน (United States vs. Sherman) เป็นการปิดฉลากและส่งมอบม้วนผ้าเต็นท์สำหรับใช้ในการเลี้ยงเปิดให้แก่ท่าเรือ คดีสหรัฐอเมริกา กับ แมดดอกซ์ (United States vs. Maddox) เป็นการหยุดพักระหว่างทางในการเดินทางระหว่างมลรัฐ ซึ่งรวมอยู่ภายใต้บังคับของมาตรา 659 ด้วย

ประมวลกฎหมายสหรัฐอเมริกา บรรพที่ 18 มาตรา 2314 เป็นบทบัญญัติเกี่ยวกับการขนส่งทรัพย์สินที่ลักมาข้ามมลรัฐ ต่างกับมาตรา 659 มาตรา 2314 เป็นกรณีที่เกี่ยวกับ

ทรัพย์สินที่ลักมาต้องขนข้ามมลรัฐ และดูเหมือนจะเป็นการไม่เพียงพอถ้าเพียงแต่ได้นำเข้าไปในข่ายกิจการค้าระหว่างมลรัฐ แม้จะยังไม่มีกรณีเกี่ยวกับเรื่องนี้โดยตรง แต่ก็มีกรณีที่ทรัพย์สินที่ลักมานั้นได้ส่งไปในยานพาหนะที่ใช้ระหว่างมลรัฐ แต่ยังไม่ได้ข้ามเส้นพรมแดน ซึ่งเห็นได้จากคดีสหรัฐอเมริกา กับ โรเซลลี (United States vs. Roselli) นอกจากนี้ยังมีคดีอื่นๆ เกี่ยวกับเรื่องนี้ คือคดีสหรัฐอเมริกา กับ เชริเดน (United States vs. Sheridan) เป็นกรณีของเช็คปลอมถูกส่งข้ามเส้นพรมแดนระหว่างมลรัฐ คดีสหรัฐอเมริกา กับ แฮสเซล (United States vs. Hassel) เป็นกรณีของทรัพย์สินที่ได้มาจากการเล่นเกมส์โดยการหลอกลวงถูกส่งข้ามพรมแดนระหว่างมลรัฐ คดีสหรัฐอเมริกา กับ จาคอบส์ (United States vs. Jacobs) เป็นกรณีของตั๋วเงินที่ถูกลักมาถูกส่งข้ามพรมแดนระหว่างมลรัฐ

ประเด็นสำคัญที่ได้นำมาพิจารณาตามมาตรา 2314 ก็คือสำเนาโปรแกรมคอมพิวเตอร์ที่ถูกลัก การเข้าถือกรรมสิทธิ์ หรือการเอาไปโดยการหลอกลวง และได้ถูกส่งข้ามพรมแดนระหว่างมลรัฐ จะถือว่าเป็นความผิดตามมาตรา 2314 หรือไม่ มีเพียงคดีเดียวที่ได้เกิดขึ้น คือคดีสหรัฐอเมริกา กับ เลสเตอร์ (United States vs. Lester) ในคดีนี้มีการร่วมกันคัดลอกหรือทำสำเนาแผนที่ทางภูมิศาสตร์ที่มีมูลค่าสูงมาก และได้ทำการส่งสำเนาแผนที่นั้นข้ามพรมแดนระหว่างมลรัฐ ซึ่งจำเลยถูกจับและศาลตัดสินว่า จำเลยได้ร่วมกันขนส่งแผนที่ที่ลักมา ซึ่งใช้ในการค้าระหว่างมลรัฐ จำเลยต่อสู้ว่า สำเนาเอกสารไม่ใช่ทรัพย์สินที่ลักมา ศาลได้วินิจฉัยว่าทรัพย์สินที่จำเลยทำการลักมาเป็นความคิดที่มีมูลค่า ไม่ใช่เป็นการลักสำเนาเอกสารที่เป็นกระดาษ

แม้ว่าศาลในคดีเลสเตอร์ จะไม่ได้กล่าวให้เห็นอย่างชัดเจนในความหมายของคำว่า "ทรัพย์สินที่ลักขโมยมา" แต่จากคดีสหรัฐอเมริกา กับ แฮนด์เลอร์ (United States vs. Handler) ได้มีการวิเคราะห์คำนี้อย่างละเอียด ต่อมาก็มีการวิเคราะห์ไว้ในคดีต่างๆ รวมถึงความหมายของคำอื่น เช่น การลักขโมย (Stealing) และประวัติทางกฎหมายของกฎหมายเกี่ยวกับทรัพย์ที่ถูกลักขโมยแห่งชาติ (The National Stolen Property Act) ซึ่งปัจจุบันนี้ได้บัญญัติไว้ในมาตรา 2314 จากการวิเคราะห์ที่กล่าวถึงในคดีแฮนด์เลอร์ข้างต้น ศาลได้สรุปว่า

1. ทรัพย์สินที่ลักขโมยมา ไม่จำเป็นต้องได้มาในลักษณะของการลักทรัพย์ กล่าวคือไม่จำเป็นที่ต้องเป็นทรัพย์สินที่มีรูปร่าง ฯลฯ และ

2. บทบัญญัติดังกล่าวสามารถนำไปใช้บังคับกับ การเอาไปใดๆ เมื่อบุคคลได้ไปซึ่งสังหาริมทรัพย์หรือเอกสารสิทธิโดยทุจริตที่เป็นของบุคคลอื่น โดยมีเจตนาเพื่อที่จะได้ไปซึ่งเจ้าของกรรมสิทธิ์ และประโยชน์ในความเป็นเจ้าของทรัพย์นั้น ดังนั้น สำเนาโปรแกรมคอมพิวเตอร์ย่อมทำให้เกิดการได้ไปซึ่งสิทธิของเจ้าของในประโยชน์ที่เป็นเจ้าของทรัพย์นั้น สำเนาจึงถือเป็นสาระสำคัญของทรัพย์ที่ลักขโมยมาได้ อันเป็นการละเมิดต่อบทบัญญัติในมาตรา 2314

อย่างไรก็ตาม จากคดีสหรัฐอเมริกา กับ ซีดลิทซ์ (United States vs. Seidlitz) ศาลได้ตัดสินยกฟ้องในประเด็นที่อ้างถึงมาตรา 2314 โดยกล่าวว่าสิ่งที่ได้ถูกส่งข้ามพรมแดนระหว่างมลรัฐเป็นเพียงสัญญาณทางอิเล็กทรอนิกส์และสรุปว่าไม่เป็นทรัพย์สิน แต่ในที่สุดซีดลิทซ์ก็ถูกตัดสินว่ากระทำผิดในส่วนของการหลอกลวงทางสายการสื่อสาร

คดีรีวิริคเกอร์ (Re vericker) มีความพยายามที่จะตัดสินลงโทษจำเลยที่ไม่ยอมให้การต่อหน้าคณะลูกขุน หลังจากที่ได้หลุดพ้นจากความผิดทางการค้า สาระสำคัญของปัญหานี้อยู่ที่ว่าจำเลยเพียงได้รับอนุญาตให้พ้นความผิดทางการค้าตามมาตรา 2314 และ 2315 เท่านั้น อันถือได้ว่าการหลุดพ้นจากความรับผิดนี้ ไม่สามารถนำมาใช้บังคับกับความผิดอาญาที่เกิดจากการซักถามของโจทก์ มาตรา 2314 และ มาตรา 2315 เป็นเรื่องที่ว่าด้วยการลักทรัพย์และรับของโจรที่เป็นตัวสินค้า เครื่องมือเครื่องใช้ หลักทรัพย์และเงินตรา ไม่รวมถึงเอกสารของหน่วยงานสืบสวนสอบสวนของรัฐบาลกลางสหรัฐอเมริกา (Federal Bureau of Investigation : FBI) อันมีความสำคัญต่อโจทก์ แม้ว่าศาลจะยอมรับในบางคดีว่าลำพังเพียงกระดาษเอกสารอาจเท่ากับเป็นเครื่องมือเครื่องใช้ได้ เช่น คดีสหรัฐอเมริกา กับ บอทโทน (United States vs. Bottone) มีการกล่าวว่ากระดาษอยู่ในความหมายของเครื่องมือเครื่องใช้ อันถือว่าเป็นทรัพย์สินที่เป็นของทั่วๆ ไปที่เป็นวัตถุในการค้า ดังนั้น แผนที่ทางภูมิศาสตร์หรือความลับของกรรมวิธีในการผลิตสินค้าจึงถือเป็นของทั่วๆ ไป ที่มีไว้เพื่อขายและ/หรือเพื่อการอนุญาตให้ใช้ แต่อย่างไรก็ตามกระดาษที่กล่าวถึงดังกล่าว เป็นสิ่งที่แสดงถึงความผูกพันของแต่ละบุคคลกับการกระทำความผิดทางอาญาที่หน่วยงานสืบสวนสอบสวนของรัฐบาลกลางสหรัฐอเมริกา จะใช้นำตัวผู้กระทำผิดมาลงโทษเป็นสิ่งของทั่วๆ ไป ที่ไม่สามารถซื้อขายกันในท้องตลาดได้ ด้วยเหตุนี้รัฐจึงไม่แสดงให้เห็นถึงความสัมพันธ์ระหว่างการลักทรัพย์ที่เป็นเอกสารของหน่วยงานดังกล่าว กับบทบัญญัติมาตรา 2314 และ มาตรา 2315

คดีสหรัฐอเมริกา กับ กรีนวอลด์ (United States vs. Greenwald) ศาลได้ตั้งประเด็นว่าสูตรเคมีที่เป็นความลับอยู่ในความหมายของมาตรา 2314 ที่ว่าเป็นสินค้า เครื่องมือเครื่องใช้หรือไม่ ซึ่งในคดีนี้มีเอกสารจำนวนหนึ่งที่ระบุถึงสูตรต่างๆ ได้รับการเก็บรักษาไว้โดยเป็นความลับ เพื่อผลประโยชน์ในการแข่งขันทางการค้า แต่มีเอกสารอยู่ชุดหนึ่งที่จำเลยซึ่งเป็นวิศวกรในแผนกขายได้นำไปใช้เพื่อประโยชน์ของตนเอง จากคำเบิกความของคดีนี้แสดงให้เห็นว่ามีการจัดตั้งตลาดเพื่อซื้อขายสูตรทางเคมีต่างๆ ซึ่งผู้ประกอบการได้ทำการซื้อขายกันหรือการอนุญาตให้ใช้ และถือว่าสูตรดังกล่าวเป็นเช่นเดียวกับทรัพย์สินทำนองเดียวกับเครื่องจักรหรือ

อุปกรณ์ ศาลได้อ้างถึงคดีสหรัฐอเมริกา กับ บอทโทน (United States vs. Bottone) และคดีริวิริคเกอร์ (Re vericker) ซึ่งวินิจฉัยว่าการจัดตั้งตลาดสูตรเคมีที่มีขึ้น แม้ว่าจะเป็นตลาดที่ค่อนข้างจำกัดก็ถือว่าเป็นตลาดได้ การเอาเอกสารต้นฉบับที่มีสูตรเคมีไปถือว่าเป็นการกระทำที่ผิดกฎหมายตามมาตรา 2314 เพราะว่าสูตรดังกล่าวเป็นสินค้า เครื่องมือเครื่องใช้

คดีสหรัฐอเมริกา กับ เดรบิน (United States vs. Drebin) คดีนี้จำเลยได้ต่อสู้ว่าการฉายภาพยนตร์เป็นสิ่งที่ไม่รูปร่าง และไม่สามารถนำมาพิจารณาเป็นสินค้า เครื่องมือเครื่องใช้ได้ ภายใต้ประมวลกฎหมายสหรัฐอเมริกา บรรพที่ 18 มาตรา 2314 จำเลยยกข้อต่อสู้โดยยื่นคำร้องว่า ลิขสิทธิ์เป็นทรัพย์สินที่ไม่มีรูปร่างอันแยกได้ต่างหากและแตกต่างจากสิทธิในทรัพย์สินที่มีรูปร่าง สำเนาเอกสารเป็นสิ่งที่ถูกทำขึ้นและไม่สามารถที่จะได้ลิขสิทธิ์โดยการลักทรัพย์ การเข้าถือกรรมสิทธิ์ หรือการหลอกลวง เพราะเจ้าของลิขสิทธิ์ไม่มีสิทธิผลประโยชน์อย่างเจ้าของ เพราะเป็นสิ่งที่คัดลอกหรือทำสำเนา ศาลได้ปฏิเสธข้อต่อสู้จำเลย โดยกล่าวว่าเป็นข้อต่อสู้ที่ไม่มีเหตุผลและขัดกับกฎหมาย และวินิจฉัยว่าสำเนาเอกสารเป็นสินค้า เครื่องมือเครื่องใช้ ในความหมายของมาตรา 2314 และศาลยังได้วินิจฉัยอีกว่าการคัดลอกหรือทำสำเนางานอันมีลิขสิทธิ์โดยมิชอบด้วยกฎหมาย เป็นความผิดที่ไม่น้อยกว่าการที่ต้นฉบับเอกสารนั้นถูกลักไป

คดีสหรัฐอเมริกา กับ โจนส์ (United States vs. Jones) คดีนี้จำเลยได้ถูกกล่าวหากระทำการเคลื่อนย้ายเอกสารสิทธิที่ได้มาจากการลักขโมย การเข้าถือกรรมสิทธิ์ หรือโดยการหลอกลวงในการค้าระหว่างมลรัฐ ตามประมวลกฎหมายสหรัฐอเมริกา บรรพที่ 18 มาตรา 2314 หลักทรัพย์ดังกล่าวเป็นของปลอม และถือไม่ได้ว่าเป็นหลักทรัพย์ และยังอ้างต่อไปอีกว่ามาตรา 2314 ไม่อาจนำมาใช้บังคับหลักฐานแห่งหนี้ของรัฐต่างประเทศหรือธนาคารหรือองค์กรของรัฐต่างประเทศที่เป็นของปลอมหรือมีการแก้ไขเปลี่ยนแปลง

ประมวลกฎหมายสหรัฐอเมริกา บรรพที่ 18 มาตรา 661 เป็นบทบัญญัติเกี่ยวกับการลักทรัพย์ภายในอาณาเขตหรือน่านน้ำพิเศษที่อยู่ในอำนาจของศาล เมื่อโปรแกรมคอมพิวเตอร์ถูกลักไปภายในอาณาเขตของรัฐบาลกลาง ตามคำนิยามที่บัญญัติไว้ในประมวลกฎหมายสหรัฐอเมริกา บรรพที่ 18 มาตรา 7 ถ้าเกิดการกระทำความผิดตามมาตรา 661 ก็จะมีปัญหาลักษณะเดียวกับมาตรา 641 และมาตรา 2314 ว่าการคัดลอกหรือทำสำเนาโดยปราศจากอำนาจเป็นความผิดตามกฎหมายดังกล่าวหรือไม่ แม้ก่อนหน้านี้จะมีการวิเคราะห์และสรุปว่าสำเนาเอกสารไม่อยู่ในข่ายของมาตรา 661 แต่การพิจารณาก็ต้องคำนึงถึงนัยอย่างกว้างไว้ด้วย

จากคดีสหรัฐอเมริกา กับ เฮนรี่ (United States vs. Henry) จำเลยถูกลงโทษฐานลักเรือภายในน่านน้ำที่อยู่ในเขตอำนาจของศาล ในชั้นอุทธรณ์มีการโต้เถียงกันว่ากฎหมายดังกล่าวเป็นเพียงกฎหมายลักทรัพย์ของคอมมอนลอว์ อันเนื่องมาจากรัฐล้มเหลวในการพิสูจน์ข้อเสนอที่ว่าจำเลยมีเจตนาที่เอาไปซึ่งความเป็นเจ้าของอย่างถาวร ศาลสูงจึงยกคำพิพากษาของศาลล่าง แต่ในคดีนี้ศาลได้ยกข้อต่อสู้ของจำเลยโดยวินิจฉัยว่า กฎหมายลายลักษณ์อักษรดังกล่าวมีความหมายที่กว้างกว่ากฎหมายลักทรัพย์ของคอมมอนลอว์ โดยศาลอุทธรณ์ภาค 2 ได้กล่าวถึงคำว่า "ลักขโมย" ในคดีแฮนด์เลอร์ไว้ว่า เมื่อมีบุคคลคนหนึ่งกระทำโดยจงใจเพื่อได้ไปหรือเก็บไว้ซึ่งความเป็นเจ้าของของบุคคลอื่นโดยปราศจากความยินยอม ด้วยเจตนาที่จะได้ไปซึ่งประโยชน์ในความเป็นเจ้าของทรัพย์ การกระทำดังกล่าวเป็นความผิดตามมาตรา 661
(The U.S. Department of Justice, 1989 : 102-105)

2. ความผิดเบ็ดเตล็ดเกี่ยวกับการลักทรัพย์ (Miscellaneous Theft and Theft-Related Offenses)

2.1 แม้ว่าจะยังไม่มีกฎหมายของรัฐบาลกลางที่บัญญัติว่า การลักทรัพย์โดยการฉ้อโกงเป็นความผิด นอกจากประมวลกฎหมายสหรัฐอเมริกา บรรพที่ 18 มาตรา 1025 ที่เป็นบทบัญญัติเกี่ยวกับการฉ้อโกงภายในอาณาเขตหรือเขตน่านน้ำพิเศษที่อยู่ในเขตอำนาจศาล และมาตรา 287 ที่เป็นบทบัญญัติเกี่ยวกับการฟ้องเท็จ ศาลจึงได้แปลความของมาตรา 641 ให้ครอบคลุมถึงการฉ้อโกง ดังจะเห็นได้จากคดีเบอร์เนทท์ กับ สหรัฐอเมริกา (Burnett vs. United States) และคดีมอร์แกน กับ สหรัฐอเมริกา (Morgan vs. United States) เป็นกรณีของการฉ้อโกงภาษีซึ่งเป็นเงินของรัฐ แต่ไม่ปรากฏว่ามีศาลใดลงโทษบุคคลที่ได้ไปซึ่งผลประโยชน์ของคอมพิวเตอร์โดยการหลอกลวง สำหรับการลักโปรแกรมคอมพิวเตอร์โดยอาศัยบทบัญญัติมาตรา 641

2.2 มีกฎหมายลักทรัพย์หลายมาตรา บัญญัติเกี่ยวกับการรับของโจรไว้ด้วย เช่น มาตรา 641 มาตรา 659 และมาตรา 2314 ส่วนบทบัญญัติมาตรา 662 ห้ามการรับของโจรในอาณาเขตและเขตน่านน้ำพิเศษที่อยู่ในเขตอำนาจศาล มาตรา 2315 ห้ามรับทรัพย์สินที่ลักมาจากการค้าระหว่างมลรัฐ ดังนั้น บุคคลที่ก่อให้เกิดการลักโปรแกรมคอมพิวเตอร์ไม่เพียงแต่เป็นผู้กระทำความผิดในฐานะตัวการตามประมวลกฎหมายสหรัฐอเมริกา บรรพที่ 18 มาตรา 2 หรือในฐานะผู้สนับสนุน ตามมาตรา 371 เท่านั้น แต่ยังอาจมีความผิดตามมาตราต่างๆ ที่กล่าวมาข้างต้นด้วย

2.3 กฎหมายของรัฐบาลกลางจำนวนมาก บัญญัติขึ้นเพื่อจะใช้บังคับกับการลักทรัพย์ที่เป็นกรณีพิเศษต่างๆ และยังสามารถนำมาใช้กับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์บางกรณีได้ เช่น การที่บุคคลกระทำการลักโปรแกรมคอมพิวเตอร์ที่ใช้สำหรับการจ่าย

เงินของรัฐ ถือว่าได้กระทำความผิดตามมาตรา 285 อันเป็นบทบัญญัติเกี่ยวกับการลักโดยการเอาไป ส่วนการลักโปรแกรมคอมพิวเตอร์จากธนาคารหรือสถาบันการเงินที่รัฐบาลเป็นประกัน จะตกอยู่ภายใต้บังคับของประมวลกฎหมายสหรัฐอเมริกา บรรพที่ 18 มาตรา 655-657 แม้จะมีข้อสงสัยว่าทรัพย์สินที่ไม่ใช่เงินจะตกอยู่ภายใต้บังคับของมาตรา 656 หรือไม่ เพราะว่าทรัพย์ที่ได้รับการคุ้มครองได้แก่ เงิน เงินทุน หรือสิทธิเรียกร้อง แต่ก็มีการปิดช่องว่างของกฎหมายด้วยการบัญญัติมาตรา 2113 (b) เป็นบทบัญญัติที่ใช้บังคับเกี่ยวกับการลักทรัพย์กับทรัพย์สินใดๆ หรือสิ่งที่มีค่าใดๆ อันลักจากธนาคาร สถาบันการเงิน (The U.S. Department of Justice, 1989 : 105)

3. ความผิดฐานใช้ช่องทางการสื่อสาร ตามประมวลกฎหมายสหรัฐอเมริกา บรรพที่ 18 มาตรา 1341 เป็นบทบัญญัติเกี่ยวกับการฉ้อโกงทางไปรษณีย์ มาตรานี้มีสาระสำคัญอยู่ 2 ประการ คือประการแรกบุคคลจะต้องใช้การไปรษณีย์เพื่อจุดประสงค์การให้บริการหรือพยายามให้บริการ และอีกประการคือการฉ้อโกงหรือการหลอกลวงเพื่อจะได้ไปซึ่งเงินหรือทรัพย์สินเป็นความผิด โดยศาลได้วางหลักว่าการกระทำใดจะถือเป็นการฉ้อโกงซึ่งกฎหมายไม่ได้กำหนดคำนิยามไว้ โดยมีการอ้างถึงคดีไวส์ กับ สหรัฐอเมริกา (Weiss vs. United States) ที่มีการวางขอบเขตของการฉ้อโกงตามมาตรา 1341 คดีบลาชลี่ กับ สหรัฐอเมริกา (Blachey vs. United States) กล่าวถึงการฉ้อโกงโดยการขายแผนงาน คดีสหรัฐอเมริกา กับ รัฐ (United States vs. States) กล่าวถึงการฉ้อโกงหีบคะแนนเสียงในการเลือกตั้งถือเป็นการฉ้อโกงทางไปรษณีย์ ด้วยเหตุนี้จึงมีการปรับเปลี่ยนแนวความคิดของศาล ให้รวมถึงการหลอกลวงเพื่อทำการคัดลอกหรือทำสำเนาโปรแกรมคอมพิวเตอร์ เป็นความผิดฐานฉ้อโกงด้วย เพราะการฉ้อโกงทางไปรษณีย์ในอนาคตมีแนวโน้มที่จะรุนแรงมากขึ้น ถ้าผู้กระทำการลักทรัพย์ทางไปรษณีย์มีการใช้คอมพิวเตอร์เป็นเครื่องมือสื่อกลาง รวมถึงการให้บริการด้านอื่นๆ จากคดีสหรัฐอเมริกา กับ โอเวน (United States vs. Owen) เป็นคดีเกี่ยวกับการฉ้อโกงทางไปรษณีย์โดยฉ้อโกงใบรับสินค้า ซึ่งผู้กระทำได้ใช้โปรแกรมคอมพิวเตอร์ในการกระทำการ อันน่าจะตกอยู่ภายใต้บังคับของมาตรา 1341 โดยโจทก์กล่าวว่า มาตรา 1341 สามารถบังคับใช้กับการใช้คอมพิวเตอร์กระทำความผิดด้วย และว่าเป็นการใช้ประโยชน์จากมาตรา 1341 ได้อย่างแท้จริง (The U.S. Department of Justice, 1989 : 105-106)

4. ความผิดเกี่ยวกับความมั่นคงของประเทศ มีการบัญญัติไว้ในประมวลกฎหมายสหรัฐอเมริกา บรรพที่ 18 หลายมาตรา เช่น มาตรา 793 เป็นบทบัญญัติที่เกี่ยวกับการชุมนุม การสื่อสาร หรือการคุ้มครองข้อมูล มาตรา 794 เป็นบทบัญญัติเกี่ยวกับการชุมนุม และการ

ส่งข้อมูลเพื่อช่วยเหลือรัฐบาลต่างประเทศ มาตรา 795 เป็นบทบัญญัติเกี่ยวกับการคุ้มครองรูปถ่ายหรือภาพเขียน มาตรา 797-799 และ มาตรา 952 โดยมาตรา 797 มีสาระสำคัญเพื่อรักษาประโยชน์ของประเทศ สำหรับการขายรูปถ่ายหรือภาพเขียน อันมีลักษณะเช่นเดียวกับมาตรา 795 ส่วนมาตรา 798 มีสาระสำคัญคือสิ่งที่กฎหมายประสงค์ในการให้ความคุ้มครองนั้นรวมถึงรหัส หนังสือ และระบบเอกสารลับด้วย ซึ่งอาจเกิดมีการกระทำความผิดโดยการใช้เครื่องมือสื่อสารในลักษณะเครือข่ายด้วย มาตรา 799 มีสาระสำคัญคือเพื่อป้องกันการฝ่าฝืนระบบความปลอดภัยขององค์กรการบินและอวกาศ (National Aeronautic and Space Administration : NASA) และสุดท้ายมาตรา 952 อันมีสาระสำคัญเพื่อคุ้มครองความลับทางการฑูต (The U.S. Department of Justice, 1989 : 106)

5. ความผิดฐานบุกรุก ไม่มีกฎหมายของรัฐบาลกลางที่ครอบคลุมความผิดอาญาฐานบุกรุกอย่างสมบูรณ์ มีเพียงกฎหมายที่บัญญัติว่าความผิดฐานบุกรุกเป็นความผิดอาญาในประมวลกฎหมายสหรัฐอเมริกา บรรพที่ 18 มาตรา 2152 ที่บัญญัติถึงการบุกรุกสถานที่ต่างๆ รวมทั้งในอาณาเขตน่านน้ำด้วย และมาตรา 2278 (a) บรรพที่ 42 ที่ห้ามการบุกรุกสำนักงานพลังงานปรมาณู (The Atomic Energy Commission) ทั้งสองมาตราไม่ได้บัญญัติไว้ใช้กับการบุกรุกที่มีวัตถุประสงค์เพื่อการยักยอกโปรแกรมคอมพิวเตอร์เป็นการเฉพาะ มิฉะนั้นคงจะไม่ระบุถึงสถานที่ที่ถูกบุกรุกหรือในอาณาเขตน่านน้ำ ส่วนการบุกรุกเพื่อที่จะลักทรัพย์มีกฎหมายที่ใช้บังคับมากกว่าแต่ก็ไม่มากนัก ประมวลกฎหมายสหรัฐอเมริกา บรรพที่ 18 มีการกำหนดโทษสำหรับการบุกรุกธนาคาร โดยบัญญัติไว้ในมาตรา 2113 (a) การบุกรุกที่ทำการไปรษณีย์บัญญัติไว้ในมาตรา 2115 และการบุกรุกการค้าระหว่างมลรัฐ บัญญัติไว้ในมาตรา 2117 (The U.S. Department of Justice, 1989 : 106-107)

6. ความผิดฐานหลอกลวง ประมวลกฎหมายสหรัฐอเมริกา บรรพที่ 18 มาตรา 912 เป็นบทบัญญัติที่เกี่ยวกับการได้ไปซึ่งสิ่งที่มีค่าใดๆ โดยการปลอมตัวเป็นเจ้าพนักงานหรือลูกจ้างของรัฐ การกระทำความผิดตามมาตรานี้เกิดขึ้นบ่อยครั้ง โดยผู้กระทำจะกระทำโดยการใช้เครื่องมือช่วยในการปลอมตัว แต่มาตรานี้จะจำกัดเกี่ยวกับตัวผู้กระทำว่าจะต้องปลอมตัวเองเป็นเจ้าพนักงานหรือลูกจ้างของรัฐ เพื่อที่จะเข้าถึงโปรแกรมคอมพิวเตอร์ แม้ว่าจะไม่ต้องการสิ่งที่มีค่าใดๆ ก็ตาม จากคดีสหรัฐอเมริกา กับ ลีโปวิทซ์ (United States vs. Lepowitch) เป็นคดีเกี่ยวกับการหลอกลวงเพื่อที่จะได้ไปซึ่งข้อมูลของบุคคลอื่น และการคัดลอกหรือทำสำเนาโปรแกรมน่าจะตกอยู่ภายใต้บทบัญญัตินี้ การตีความมาตรานี้จะต้องตีความในนัยที่กว้างพอ เพื่อที่จะหมายรวม

ถึงสิ่งที่มีค่าใดๆ ในรูปแบบใหม่ๆ เพราะว่าการบัญญัติกฎหมายมาตรานี้ ไม่สามารถที่จะทำการคาดการณ์ล่วงหน้าให้ครอบคลุมถึงสื่อต่างๆ และทุกๆ กลอุบายที่ผู้กระทำจะใช้ในการฉ้อโกงเพื่อรักษาผลประโยชน์ให้ปลอดภัย อนึ่งยังมีความผิดฐานหลอกลวงอื่นๆ อีก โดยบัญญัติไว้ในประมวลกฎหมายสหรัฐอเมริกา บรรพที่ 18 มาตรา 1001 มาตรา 1005 และ มาตรา 1006 ซึ่งเป็นบทบัญญัติเกี่ยวกับการเข้าถึงข้อมูลโดยมิชอบด้วยกฎหมายของธนาคารและสถาบันการเงิน (The U.S. Department of Justice, 1989 : 107)

4.2.2 **ความผิดฐานแก้ไขเปลี่ยนแปลงข้อมูล** (Alteration)

ความผิดฐานนี้ประเทศสหรัฐอเมริกา ได้บัญญัติเป็นความผิดอาญาฐานหนึ่งโดยบัญญัติไว้ใน The Computer Fraud and Abuse Act 1986 ซึ่งครอบคลุมถึงการแก้ไขเปลี่ยนแปลงเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ เครือข่ายคอมพิวเตอร์ ตลอดจนโปรแกรมคอมพิวเตอร์และข้อมูลในคอมพิวเตอร์ สาเหตุที่สหรัฐอเมริกาบัญญัติกฎหมายในเรื่องนี้เป็นความผิดอาญาที่เกี่ยวกับคอมพิวเตอร์อีกฐานหนึ่ง แยกออกจากความผิดฐานเข้าถึงโดยปราศจากอำนาจน่าจะมาจากเหตุผลที่ว่า การแก้ไขเปลี่ยนแปลงทางคอมพิวเตอร์มีส่วนเกี่ยวข้องในแง่ของการกระทำอันเป็นปัญหาที่เกี่ยวกับความผิดฐานปลอมเอกสารด้วย โดยสิ่งที่เกิดขึ้นเป็นเรื่องของการนำบทบัญญัติความผิดฐานปลอมเอกสารมาบังคับใช้ ประสบกับปัญหาการตีความ โดยเฉพาะในเรื่องขององค์ประกอบ ทำให้ฝ่ายนิติบัญญัติของมลรัฐต่างๆ รวมทั้งรัฐบาลกลาง บัญญัติความผิดฐานนี้แยกออกมาให้ครอบคลุมได้ครบถ้วนยิ่งขึ้น

การกระทำดังกล่าวที่จะต้องนำมาพิจารณา ในแง่ของการปลอมเอกสารได้นั้นจะต้องเป็นกรณีของการแก้ไขเปลี่ยนแปลงโปรแกรมคอมพิวเตอร์ หรือข้อมูลที่เก็บอยู่ในคอมพิวเตอร์เท่านั้น เพราะโปรแกรมหรือข้อมูลอาจจะตีความออกมาในแง่ของคำว่า "เอกสาร" ได้ ส่วนการแก้ไขเปลี่ยนแปลงตัวเครื่องคอมพิวเตอร์นั้น ไม่มีส่วนเกี่ยวข้องกับความผิดฐานปลอมเอกสารแต่อย่างใด เพราะไม่อาจจะตีความในแง่ของคำว่า "เอกสาร" ได้ แต่สาเหตุที่กฎหมายของสหรัฐอเมริกาในเรื่องนี้ ได้บัญญัติไว้เป็นความผิดพิเศษออกไปจากการแก้ไขเปลี่ยนแปลงแก่วัตถุธรรมดาทั่วๆ ไป ซึ่งไม่เป็นความผิดอาญาก็เพราะเป็นการแก้ไขเปลี่ยนแปลงวัตถุที่เป็นโลหะอุปกรณ์อันเป็นทรัพย์สินในทางเทคโนโลยีชนิดหนึ่ง และการกระทำดังกล่าวอาจก่อให้เกิดความเสียหายได้ค่อนข้างสูง เมื่อเปรียบเทียบกับการแก้ไขเปลี่ยนแปลงในทรัพย์สินที่เป็นประดิษฐกรรมธรรมดาอื่นๆ

ตามปัญหาที่กล่าวข้างต้น ในเรื่องการตีความของคำว่า "เอกสาร" ว่าจะครอบคลุมถึงสิ่งต่างๆ ในการกระทำความผิดฐานปลอมเอกสารทางคอมพิวเตอร์หรือไม่ เช่น ซอฟต์แวร์ โปรแกรมคอมพิวเตอร์ หรือข้อมูลต่างๆ นั้น เมื่อมีการบัญญัติให้การกระทำดังกล่าวเป็นความผิดฐาน "แก้ไขเปลี่ยนแปลง" เสีย โดยไม่จำต้องมีองค์ประกอบดังเช่น ความผิดฐานปลอมเอกสารที่ได้ใช้อยู่เดิม การแก้ไขเปลี่ยนแปลงเอกสารทางคอมพิวเตอร์นั้น จะได้ไปซึ่งประโยชน์อันเป็นทรัพย์สิน สิทธิ หรือสิ่งของไม่ว่าจะเป็นสิ่งที่มีรูปร่างหรือไม่มีรูปร่างก็ตาม การกระทำการแก้ไขเปลี่ยนแปลงส่วนมากแล้ว จะต้องใช้รหัสผ่านเพื่อที่จะเข้าไปในระบบคอมพิวเตอร์ของบุคคลอื่น การใช้รหัสผ่านเป็นการใช้รหัสเท็จ จุดประสงค์เพื่อที่จะหลอกลวงหรือก่อให้เกิดความเสียหายขึ้น อันอาจถือได้ว่าเป็นการปลอมเอกสารได้ ซึ่งหลายๆ มลรัฐของสหรัฐอเมริกา เช่น มลรัฐคาลิฟอร์เนีย มลรัฐนิวยอร์ค มลรัฐเดอลาแวร์ มลรัฐเท็กซัส และมลรัฐเพ็นซิลวาเนีย ได้ขยายขอบเขตของกฎหมาย เพื่อให้การกระทำการแก้ไขเปลี่ยนแปลง การวางแผนการ การทำให้สมบูรณ์ หรือการรับรองใดๆ แก่รอยตรา ลายเซ็นชื่อ ข้อเขียน หรือสัญลักษณ์แห่งสิทธิ สิทธิพิเศษ หรือบัตรประจำตัวใดๆ ซึ่งอาจเป็นการหลอกลวง หรือการทำให้เกิดความเสียหายแก่บุคคลอื่น เป็นความผิดฐานปลอมเอกสาร แม้ว่ามลรัฐอื่นๆ ยังคงรักษารูปแบบของกฎหมายในเรื่องลายเซ็นชื่อและเอกสารอย่างเคร่งครัด จะไม่สามารถนำกฎหมายในเรื่องความผิดฐานปลอมเอกสารดังกล่าวมาใช้บังคับได้

กฎหมายอาญาของมลรัฐคาลิฟอร์เนีย มาตรา 470 บัญญัติว่า "ผู้ใด...ปลอมหรือแปลงรอยตรา หรือข้อเขียนด้วยมือของบุคคลอีกคนหนึ่ง..." ผู้นั้นมีความผิดฐานปลอมเอกสาร สิ่งที่จะนำมาวิเคราะห์สำหรับความผิดฐานแก้ไขเปลี่ยนแปลงนี้คือ รหัสที่ใช้ในระบบคอมพิวเตอร์ถือว่าเป็นรอยตราหรือลายเซ็นชื่อได้หรือไม่ เมื่อพิจารณาดูก็นับว่าเป็นเรื่องที่เป็นไปได้ที่จะเทียบรหัสที่ใช้ในระบบคอมพิวเตอร์ว่าเป็นลายเซ็นบนเช็ค หรือเป็นรอยตรารับรองของเจ้าพนักงานอย่างหนึ่ง และยิ่งไปกว่านั้น ยังมีคดีอยู่คดีหนึ่งคือคดีประชาชน กับ เบอร์เกตต์ (People vs. Burkett) ศาลสูงได้พิพากษายืนตามศาลล่างว่า "รอยตราหรือข้อเขียนด้วยลายมือ" เป็นถ้อยคำที่กว้างพอที่จะครอบคลุมถึงสำเนารูปถ่ายของรอยตราหรือลายเซ็นชื่อ อันถอดแบบออกมาเหมือนของจริง ที่ได้ทำขึ้นมาใหม่ด้วย ซึ่งข้อเท็จจริงในคดีนี้คือจำเลยได้กระทำความผิดโดยการใช้สำเนารูปถ่ายของธนบัตรในการแลกเปลี่ยนเงินตรา

สำหรับกฎหมายอาญาของมลรัฐนิวยอร์ค ในความผิดฐานปลอมเอกสารนี้ ได้บัญญัติไว้ในมาตรา 170.00 โดยบัญญัติว่า "การกระทำดังที่บัญญัติไว้นั้นเป็นความผิดฐานปลอมเอกสาร" และบัญญัติครอบคลุมไปถึงการกระทำโดยทุจริตใดๆ ต่อข้อเขียนส่วนบุคคล ซึ่งอาจทำให้บุคคลอื่นเสียหายด้วย และอีกหลายมลรัฐ เช่น มลรัฐเดอลาแวร์ มลรัฐเท็กซัส และมลรัฐเพ็นซิลวาเนีย ต่างก็มีกฎหมายในความผิดฐานที่คล้ายคลึงกัน จะแตกต่างกันก็ในเรื่องของอัตราโทษ ดังนั้นจะเห็นได้ว่าหลายมลรัฐได้ถือว่าการใส่รหัสที่ใช้ในระบบคอมพิวเตอร์ หรือสัญลักษณ์แห่งสิทธิ หรือสิทธิพิเศษ หรือเอกสารบัตรประจำตัวที่พิมพ์ออกจากเครื่องจักรกลใดๆ ที่เป็นของเท็จ และได้นำไปใช้เพื่อการหลอกลวงหรือทำให้เสียหายอาจถือว่าเป็นการปลอมเอกสารได้ด้วย

อย่างไรก็ตาม มีสิ่งที่น่าสนใจอยู่กรณีหนึ่ง ซึ่งเป็นเรื่องของเช็คที่มีลายเซ็นชื่อที่พิมพ์ออกจากเครื่องคอมพิวเตอร์ โดยข้อเท็จจริงมีอยู่ว่าลูกจ้างคนหนึ่งได้เข้าไปกระทำการโดยปราศจากอำนาจใช้ข้อมูลที่ได้เก็บรักษาไว้ในเครื่องคอมพิวเตอร์ โดยการใส่รหัสของผู้สั่งจ่ายที่ไม่ถูกต้อง แล้วจึงใส่ข้อมูลโดยเฉพาะสำหรับการพิมพ์เช็คออกมาในนามผู้สั่งจ่ายปลอม เพื่อให้เครื่องพิมพ์เช็คและกระดาษบัญชีจ่ายเงิน ในที่สุดก็ได้เช็คปลอม ประเด็นที่อยู่ในการพิจารณาของศาลก็คือว่าเช็คนั้นก่อให้เกิดความผิดฐานปลอมเอกสารหรือไม่ ด้วยเหตุนี้ทำให้ไม่สามารถนำประมวลกฎหมายสหรัฐอเมริกา บรรพที่ 18 มาตรา 2314 มาใช้บังคับได้ โดยศาลได้หมายเหตุไว้ว่า เมื่อความเท็จในเอกสารนั้นอยู่ในสิ่งที่บรรจุอยู่ภายในนั้นยิ่งไปกว่าอาการของการทำเอกสารนั้นขึ้น ก็ไม่ใช่เป็นการปลอมเอกสาร กรณีนี้เช็คดังกล่าวไม่ได้หลอกลวงในการเขียน แต่เป็นการพิมพ์เช็คโดยปราศจากอำนาจมากกว่า โดยศาลได้วินิจฉัยว่า ข้อเท็จจริงที่เพียงแต่ได้มีการใช้เครื่องคอมพิวเตอร์นั้นไม่ตรงกับปัญหา ทั้งนี้เพราะเครื่องคอมพิวเตอร์เป็นเพียงเครื่องมือที่ไม่มีชีวิต และเพียงทำตามคำสั่งชนิดหนึ่งที่ลูกจ้างดังกล่าวได้นำมาใช้งานเท่านั้น ในทำนองเดียวกับเครื่องจักรกลอื่นๆ ที่ใช้ในการเขียนเช็ค หรือปากกาลูกลื่นธรรมดา และด้วยเหตุนี้จึงไม่ใช่เป็นการปลอมเอกสาร

ในเรื่องของเจตนาของความผิดฐานแก้ไขเปลี่ยนแปลง ตามกฎหมายของสหรัฐอเมริกา มีข้อที่น่าพิจารณาคือความผิดฐานเข้าถึงโดยปราศจากอำนาจ กฎหมายของสหรัฐอเมริกาส่วนใหญ่บัญญัติให้ครอบคลุมทั้งความผิดที่มีเจตนาพิเศษ และความผิดที่มีเพียงเจตนาธรรมดา แต่ความผิดฐานแก้ไขเปลี่ยนแปลงต้องการเพียงเจตนาธรรมดาเท่านั้น และสิ่งสำคัญต้องเป็นการกระทำโดยปราศจากอำนาจด้วย เพราะถ้าผู้กระทำมีอำนาจที่จะกระทำได้แล้ว ก็ย่อมไม่มีความผิดตามหลักกฎหมายทั่วไป

4.2.3 ความผิดฐานทำให้เกิดความเสียหายหรือทำลาย (Damage or Destruction)

การทำให้เกิดความเสียหายหรือทำลายทางคอมพิวเตอร์ หมายถึงการทำให้เกิดความเสียหายหรือทำลายโปรแกรมคอมพิวเตอร์หรือข้อมูลในคอมพิวเตอร์ โดยลักษณะของโปรแกรมคอมพิวเตอร์หรือข้อมูลที่ถูกจัดเก็บรักษาไว้ภายใน จะอยู่ในลักษณะที่ไม่สามารถมองเห็นและจับต้องได้ ทั้งนี้ยังมีสิ่งที่เป็นกรรมของการกระทำความผิดในลักษณะนี้อีกประเภทหนึ่ง คือ เครื่องคอมพิวเตอร์ รวมถึงอุปกรณ์ต่างๆ ของเครื่องคอมพิวเตอร์ที่เรียกกันว่าฮาร์ดแวร์ (Hardware) ซึ่งกฎหมายของสหรัฐอเมริกาถือเป็นความผิดอาญาเกี่ยวกับคอมพิวเตอร์ โดยให้เหตุผลว่าเป็นการกระทำที่ก่อให้เกิดความเสียหายที่ค่อนข้างสูง และสิ่งที่เสียหายนั้นเป็นผลิตผลทางเทคโนโลยีชนิดหนึ่ง จึงมีการบัญญัติให้การกระทำดังกล่าวเป็นความผิดต่างหากแยกออกจากความผิดฐานทำให้เสียทรัพย์ โดยมีการบัญญัติไว้ใน The Computer Fraud and Abuse Act 1986

แต่เดิม The Computer Fraud and Abuse Act 1986 มาตรา 1030 (a) (5) บัญญัติว่า "โดยเจตนาที่จะเข้าสู่ระบบคอมพิวเตอร์ของรัฐบาลโดยปราศจากอำนาจ เพื่อผลประโยชน์ใดๆ หลังจากนั้นได้ทำการเปลี่ยนแปลง ทำลายสารสนเทศที่ได้เข้าถึงนั้น จะถูกลงโทษปรับหรือจำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับ และถ้ากระทำผิดซ้ำจะมีโทษจำคุกไม่เกิน 10 ปี"

ต่อมา ค.ศ. 1994 ได้มีการแก้ไขมาตรานี้ใหม่เพื่อลงโทษผู้กระทำความผิด โดยแบ่งออกเป็น 2 ส่วน ดังนี้ "มาตรา 1030 (a) (5)

(A) โดยรู้อยู่แล้วที่จะก่อให้เกิดความเสียหายต่อโปรแกรม สารสนเทศ รหัสหรือคำสั่งในคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ ถ้า

(1) บุคคลที่ทำการสื่อสารตั้งใจที่จะทำให้เกิด

1.1 ความเสียหายหรือเป็นสาเหตุของความเสียหายต่อคอมพิวเตอร์ ระบบคอมพิวเตอร์ เครือข่ายคอมพิวเตอร์ สารสนเทศ ข้อมูลหรือโปรแกรม หรือ

1.2 การใช้การไม่ได้หรือสาเหตุของการใช้การไม่ได้ของคอมพิวเตอร์ บริการคอมพิวเตอร์ ระบบคอมพิวเตอร์ เครือข่ายคอมพิวเตอร์ สารสนเทศ ข้อมูลหรือโปรแกรม และ

(2) ความเสียหายนั้นเกิดกับส่วนประกอบของโปรแกรม สารสนเทศ รหัสหรือคำสั่ง

2.1 กระทำโดยบุคคลที่ปราศจากอำนาจ

2.2 เป็นสาเหตุของความสูญหายหรือเสียหายของบุคคลคนหนึ่ง หรือหลายคนรวมกันได้ 1,000 เหรียญสหรัฐอเมริกาหรือมากกว่านั้น หรือกระทำมากกว่า 1 ปี หรือทำการแก้ไขหรือทำความเสียหาย

(B) กระทำการโดยไม่ไตร่ตรอง ไม่คำนึง หรือไม่สมควร และน่าจะเกิดความเสี่ยงต่อการสื่อสาร ถ้า

(1) บุคคลที่ทำการสื่อสารตั้งใจที่จะทำให้เกิด

1.1 ความเสียหายหรือเป็นสาเหตุของความเสียหายต่อคอมพิวเตอร์ ระบบคอมพิวเตอร์ เครือข่ายคอมพิวเตอร์ สารสนเทศ ข้อมูลหรือโปรแกรม หรือ

1.2 การใช้การไม่ได้หรือสาเหตุของการใช้การไม่ได้ของคอมพิวเตอร์ บริการคอมพิวเตอร์ ระบบคอมพิวเตอร์ เครือข่ายคอมพิวเตอร์ สารสนเทศ ข้อมูลหรือโปรแกรม และ

(2) ความเสียหายนั้นเกิดกับส่วนประกอบของโปรแกรม สารสนเทศ รหัสหรือคำสั่ง

2.1 กระทำโดยบุคคลที่ปราศจากอำนาจ

2.2 เป็นสาเหตุของความสูญหายหรือเสียหายของบุคคลคนหนึ่ง หรือหลายคนรวมกันได้ 1,000 เหรียญสหรัฐอเมริกาหรือมากกว่านั้น หรือกระทำมากกว่า 1 ปี หรือทำการแก้ไขหรือทำความเสียหาย"

อนึ่ง นอกจากนี้ยังมีการแก้ไขมาตรา 1030 (e) (4) ในส่วนของคำนิยามคำว่า "สถาบันการเงิน" และเพิ่มเติมมาตรา 1030 (g) ด้วย (ตามรายละเอียดในภาคผนวก)

จากบทบัญญัติก่อนที่จะมีการแก้ไขดังกล่าว ถ้าพิจารณาในส่วนขององค์ประกอบจะเห็นได้ว่าการที่จะถือว่าบุคคลใดกระทำความผิดตามอนุมาตรานี้ ผู้กระทำต้องกระทำโดยเจตนา (Intentionally) คือผู้กระทำจะต้องประสงค์โดยตรงต่อการทำให้เกิดความเสียหายหรือทำลายโปรแกรมคอมพิวเตอร์หรือข้อมูลในคอมพิวเตอร์ ซึ่งแตกต่างจากกฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์ ฉบับแรก คือ The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 ที่ได้กำหนดระดับเจตนาร้าย (Mens Rea) ในการก่อให้เกิดความเสียหายหรือทำลายโปรแกรมคอมพิวเตอร์หรือข้อมูลในคอมพิวเตอร์นั้น ไว้ในระดับเพียงแค่ "โดยรู้" (Knowingly) เท่านั้น ต่อมาเมื่อได้มีการบัญญัติกฎหมายฉบับใหม่คือ The Computer Fraud and Abuse Act of 1986 นักคอมพิวเตอร์จำนวนมากพยายามที่จะผลักดันให้มีการเปลี่ยนแปลงเจตนาร้ายดังกล่าว และสภาครองเกรสก็เห็นด้วย โดยให้เหตุผลว่าทุกฝ่ายต่างเห็นว่า

การใช้ระดับเจตนา "โดยรู้" จะก่อให้เกิดความผิดได้ง่ายมาก เพราะการกระทำโดยรู้ผู้กระทำเพียงแต่ตระหนักว่า "ผลที่จะเกิดขึ้นอย่างแน่นอนนั้นเป็นผลมาจากการกระทำของตน ซึ่งอะไรก็ตามที่ผู้นั้นต้องการอาจจะก่อให้เกิดผลเช่นนั้น" แต่ระดับการกระทำ "โดยเจตนา" จะมีความหมายมากกว่าคือ "บุคคลผู้ซึ่งกระทำให้เกิดผล โดยที่ตนเองประสงค์ในการกระทำ หรือเป็นสาเหตุของการกระทำ ดังนั้น การกระทำหรือสาเหตุที่เกิดขึ้น จะต้องเป็นวัตถุที่ประสงค์ต่อ อันมีอยู่ในจิตใจของผู้กระทำ" อีกเหตุผลหนึ่งที่สภาครองเกรสได้ให้ไว้ก็คือว่า การวิตกกังวลต่อมาตรฐานของคำว่า "โดยรู้" ซึ่งไม่น่าจะเหมาะสมกับคดีที่เกี่ยวกับเทคโนโลยีสารสนเทศ เพราะโดยธรรมชาติเทคโนโลยีสารสนเทศมีการพัฒนาไปอย่างรวดเร็ว ปราศจากความแน่นอน ในที่สุดสภาครองเกรสก็ตัดสินใจที่จะยกระดับเจตนาร้าย (Mens Rea) ให้สูงขึ้น โดยบัญญัติไว้ในกฎหมายดังกล่าว แต่เมื่อมีการแก้ไขอนุมาตรานี้ ได้กลับมาใช้คำว่า "โดยรู้" อีกครั้งหนึ่ง โดยการแก้ไขคราวนี้ได้ระบุรายละเอียดให้ชัดเจนยิ่งขึ้น ดังรายละเอียดที่ได้กล่าวไว้ข้างต้น

อย่างไรก็ตาม ได้มีคดีที่เกี่ยวข้องกับบทบัญญัติดังกล่าวเกิดขึ้น (คดีนี้เกิดขึ้นก่อนที่จะมีการแก้ไขอนุมาตราดังกล่าว) คือ คดีของนายโรเบิร์ต ที มอริส (Rober T. Morris) เป็นคดีที่ก่อให้เกิดไวรัสคอมพิวเตอร์ กล่าวโดยสรุปคือว่า นายโรเบิร์ต ที มอริส ได้สร้างไวรัสคอมพิวเตอร์ อันเป็นที่รู้กันในชื่อ "หนอนคอมพิวเตอร์" (Worm) ซึ่งหนอนคอมพิวเตอร์จะทำการคัดลอกหรือทำสำเนาตัวเองลงในหน่วยความจำจนหน่วยความจำเต็ม ในที่สุดคอมพิวเตอร์ก็หยุดทำงาน แต่ไวรัสคอมพิวเตอร์ชนิดนี้ไม่ได้ทำลายโปรแกรมคอมพิวเตอร์หรือข้อมูลในคอมพิวเตอร์ การกระทำดังกล่าวของนายโรเบิร์ต ที มอริส ถือเป็นความผิดอาญา ตามมาตรา 1030 (a) (5) และถูกไต่สวนโดยคณะลูกขุน หลังจากนั้นศาลชั้นต้นตัดสินลงโทษว่านายโรเบิร์ต ที มอริส มีความผิดตามบทบัญญัติดังกล่าว นายโรเบิร์ต ที มอริส ได้อุทธรณ์ว่า มาตรา 1030 (a) (5) นั้น ไม่เพียงแต่ต้องมีเจตนาที่จะเข้าถึงคอมพิวเตอร์ที่รัฐใช้ประโยชน์เท่านั้น แต่จะต้องมีเจตนาที่จะเปลี่ยนแปลงทำให้เกิดความเสียหายหรือทำลายโปรแกรมคอมพิวเตอร์หรือข้อมูลในคอมพิวเตอร์ หรือขัดขวางผู้มีอำนาจใช้เครื่องด้วย จากคำอุทธรณ์ผู้พิพากษาได้กล่าวว่าคำว่า "เจตนา" ใช้เพียงเพื่อขยาย "การเข้าถึง" เท่านั้น ไม่ได้ใช้รวมไปถึงคำว่า "ทำให้เกิดความเสียหาย" และกล่าวทบทวนถึงการบัญญัติกฎหมาย โดยพิจารณาจากเครื่องวรรคตอน ซึ่งแสดงให้เห็นอย่างชัดเจนคำว่า "โดยเจตนา" (Intentionally) เป็นกริยาวิเศษเพียงเจตนาที่ต้องการจะขยายคำว่า "การเข้าถึง" (Access) เท่านั้น โดยศาลอุทธรณ์สรุปว่า การก่อให้เกิดความเสียหายไม่จำเป็นต้องมีเจตนา แต่เพียงต้องมีผลมาจากการเข้าถึงโดยปราศจากอำนาจเท่านั้น ในที่สุดนายโรเบิร์ต ที มอริส ก็ถูกพิพากษาให้ถูกคุมความประพฤติ (Probation) เป็นเวลา 3 ปี และให้ทำงานบริการสาธารณะ (Community

Service) เป็นเวลา 400 ชั่วโมง และปรับเป็นจำนวนเงิน 10,050 เหรียญสหรัฐอเมริกา แต่ถึงแม้ว่าศาลจะตัดสินลงโทษนายโรเบิร์ต ที มอริส แล้วก็ตาม ก็มีนักกฎหมายจำนวนมากต่างวิพากษ์วิจารณ์คำพิพากษาว่าไม่น่าจะเป็นสิ่งที่ถูกต้อง โดยให้เหตุผลว่าถ้าพิจารณาถึงประวัติการบัญญัติกฎหมายแล้ว จะเห็นว่ามีการขยายบทบัญญัติให้มีอนุมาตรามากขึ้น โดย มาตรา 1030 (a) (5) มีหลักว่าการทำให้เกิดความเสียหายนั้นจะต้องกระทำโดยเจตนา ดังนั้น เมื่อผู้กระทำไม่มีเจตนาที่จะก่อให้เกิดความเสียหายแล้ว การกระทำของบุคคลนั้นก็ไม่น่าจะเป็นความผิด

อนึ่ง ยังมีข้อถกเถียงที่ว่า The Computer Fraud and Abuse Act of 1986 เป็นกฎหมายที่เจตนารมย์ให้ครอบคลุมถึงกรณีไวรัสคอมพิวเตอร์หรือไม่ ซึ่งในความเป็นจริงแล้ว กฎหมายฉบับนี้มิได้มีเจตนารมย์ที่จะปรับใช้กับกรณีของไวรัสคอมพิวเตอร์แต่อย่างใด ทั้งนี้เพราะมีเจตนาที่จะลงโทษบุคคลที่รุกล้ำระบบคอมพิวเตอร์ของรัฐเท่านั้น และเหตุผลอีกประการหนึ่งก็คือว่า ไม่ว่าจะเป็นการบัญญัติกฎหมาย The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 หรือ The Computer Fraud and Abuse Act of 1986 ก็มิได้มีการกล่าวถึงกรณีไวรัสคอมพิวเตอร์ไว้ ซึ่งอาจจะเป็นเพราะช่วงเวลาที่บัญญัติกฎหมายอยู่นั้น ปัญหาของไวรัสคอมพิวเตอร์ยังไม่มีหรือมีก็ไม่รุนแรง จนกระทั่ง ค.ศ.1988 ปัญหาไวรัสคอมพิวเตอร์มีความรุนแรงมากขึ้น แต่กฎหมายที่จะบังคับใช้โดยตรงก็ยังไม่มี ศาลจึงต้องทำหน้าที่ตีความกฎหมายที่ใช้บังคับอยู่ ให้ครอบคุลมถึงการก่อให้เกิดไวรัสคอมพิวเตอร์ที่ยังความเสียหายแก่เจ้าของข้อมูล เพราะบางกรณีเป็นที่เห็นชัดจากสังคมว่าสิ่งนั้นเป็นความผิด การลงโทษผู้กระทำความผิดจึงต้องเกิดขึ้นอย่างรวดเร็ว เพราะจะได้เป็นตัวอย่าง แม้ว่ากฎหมายที่บังคับใช้นั้น โดยพื้นฐานแล้วจะไม่ครอบคลุมการกระทำนั้นๆ ก็ตาม แต่การตีความให้ครอบคลุมถึงนั้นบางครั้งอาจจะก่อให้เกิดปัญหาน้อยกว่าการที่จะตัดสินว่า การกระทำอย่างนั้นไม่มีกฎหมายครอบคลุมถึงและไม่ถือว่าเป็นความผิด (พรชัย เหลียวพัฒนพงศ์, 2537 : 93-101)

การแพร่หลายของไวรัสคอมพิวเตอร์ นับวันจะมีจำนวนมากและทวีความรุนแรงมากขึ้นทำให้มีความตื่นตัวต่อปัญหานี้อีกทั้งการบังคับใช้กฎหมายที่มีอยู่ก็เกิดช่องว่าง สหรัฐอเมริกาจึงตัดสินใจที่จะเสนอร่างกฎหมายที่จะมาใช้บังคับกับกรณีไวรัสคอมพิวเตอร์โดยตรง เข้าสู่การพิจารณาของสภาครองเกรส ร่างกฎหมายดังกล่าว คือ The Computer Viruses Eradication Act of 1989 โดยกำหนดความผิดอันเป็นสาระสำคัญอยู่ 2 ประการ คือ ความผิดฐานใส่ไวรัสคอมพิวเตอร์เข้าสู่คอมพิวเตอร์ และความผิดฐานมอบโปรแกรมไวรัสคอมพิวเตอร์ นอกเหนือจากความผิดทางอาญาแล้ว กฎหมายฉบับนี้ยังมีบทบัญญัติเกี่ยวกับการชดใช้ค่าเสียหายทางแพ่งให้

กับผู้ได้รับความเสียหายอีกด้วย (พรชัย เหลียวพัฒนพงศ์, 2537 : 111) และในขณะที่รัฐบาลกลางกำลังบัญญัติกฎหมายกำจัดไวรัสคอมพิวเตอร์อยู่นั้น หลายมลรัฐในสหรัฐอเมริกาก็ได้บัญญัติกฎหมายดังกล่าวเป็นที่เรียบร้อยแล้ว

พิจารณาในส่วนของฐานความผิด โดยนอกจากความผิดที่ผู้ก่อให้เกิดความเสียหายหรือทำลายจะต้องรับผิดตาม The Computer Fraud and Abuse Act of 1986 หรือ The Computer Viruses Eradication Act of 1989 ที่กล่าวมาข้างต้นแล้ว บางกรณีผู้ที่ก่อให้เกิดความเสียหายหรือทำลาย อาจจะต้องรับผิดตามกฎหมายอื่นๆ ที่มีการใช้บังคับอยู่แล้วอีกทางหนึ่งด้วย เช่น ความผิดฐานทำให้เสียทรัพย์

ประมวลกฎหมายสหรัฐอเมริกา บรรพที่ 18 มาตรา 81 เป็นบทบัญญัติเกี่ยวกับการวางเพลิงในอาณาเขตและเขตน่านน้ำที่อยู่ในเขตอำนาจศาล แม้ว่าความผิดตามมาตรานี้จะนำมาใช้บังคับกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้ในบางกรณี ก็เพราะเป็นกลยุทธทางกฎหมายเท่านั้น โจทก์จะต้องใช้ความระมัดระวังในขอบเขตของมาตรานี้ ซึ่งมีปัญหาสำคัญอยู่ว่าฮาร์ดแวร์หรือซอฟต์แวร์จะรวมอยู่ในความหมายของวลีที่ว่า "เครื่องจักรหรือวัตถุที่สร้างขึ้น" (Machinery or Building Material or Supplies) หรือไม่ ซึ่งมีบางคดีที่เกิดขึ้นแสดงให้เห็นว่า วลีดังกล่าวอาจแปลความตามนัยอย่างแคบก็ได้ จากคดีสหรัฐอเมริกา กับ ธนาคาร (United States vs. Banks) จำเลยถูกกล่าวหาว่ากระทำความผิดและถูกลงโทษตามมาตรา 81 คือทำการวางเพลิงรถยนต์ ศาลอุทธรณ์โดยท่านผู้พิพากษานิโคลส์ (Nichols) วินิจฉัยว่า "รถยนต์ไม่ใช่เครื่องจักร" ตามความหมายของมาตรา 81 โดยอ้างถึงหลักความเป็นขนิดเดียวกันและตั้งข้อสังเกตไว้ว่าการตีความของคำว่าเครื่องจักรตามนัยอย่างกว้าง จะเป็นการอันตรายสำหรับการบังคับใช้กฎหมาย เพราะจะเป็นการเคลือบคลุม ดังนั้น โจทก์น่าจะได้รับคำแนะนำในการวางรูปแบบของคำฟ้อง ในการกล่าวหาว่าการวางเพลิงฮาร์ดแวร์หรือซอฟต์แวร์ ให้เป็นความผิดฐานพยายามวางเพลิงต่อวัตถุที่สร้างขึ้น

ประมวลกฎหมายสหรัฐอเมริกา บรรพที่ 18 มาตรา 1361 เป็นบทบัญญัติเกี่ยวกับการทำให้ทรัพย์สินของรัฐเสียหาย มีหลายคดีที่แปลความของมาตรา 1361 ให้มีความหมายตามนัยที่กว้าง ซึ่งศาลต่างๆ ยอมรับฟ้องความผิดฐานนี้เป็นจำนวนมาก แต่เดิมมาตรา 1361 เป็นกฎหมายที่ตายแล้ว จนกระทั่งมีการก่อกวนการเกณฑ์ทหารในปี ค.ศ. 1960 มาตรานี้ก็ได้ถูกนำขึ้นมาใช้อีกครั้งหนึ่ง โดยถือเป็น "บททั่วไป" ที่จะครอบคลุมการกระทำความผิดต่างๆ มิฉะนั้นอาจไม่

สามารถฟ้องร้องได้ เช่น ในคดีสหรัฐอเมริกา กับ อีเบอร์ฮาร์ท (United States vs. Eberhardt) เป็นคดีเกี่ยวกับ การราดโลหิตลงในเอกสารการคัดเลือกบุคคลเข้ารับราชการทหารของบาทหลวงฟิลิป และพวกอีก 2 คน โดยถูกตัดสินลงโทษฐานกระทำความผิดตามมาตรา 1361 ซึ่งศาลอุทธรณ์พิพากษายืนตามศาลล่าง โดยให้จำเลยใช้ราคาของการทำเอกสารขึ้นใหม่อันถือว่าเป็นการกำหนดค่าเสียหาย และจำเลยก็ไม่ได้โต้แย้งต่อสู้ว่าการกระทำของตนไม่ก่อให้เกิดความเสียหายตามบทบัญญัติมาตรานี้ จากคดีนี้ส่งผลให้การตีความในประเด็นแห่งคดีไม่ชัดเจน โดยนัยอย่างแคบที่สุดหมายความว่าการลบทางกายภาพเพียงชั่วคราว ซึ่งภายหลังทำขึ้นใหม่ได้เป็นการทำให้เสียหาย ในขณะที่เอกสารของการคัดเลือกบุคคลเข้ารับราชการทหาร เป็นสิ่งที่กระทบต่อความมั่นคงของประเทศ และยังมีการตีความมาตรา 1361 ที่ว่าความเสียหายไม่จำเป็นต้องเกิดขึ้นกับส่วนใหญ่ของทรัพย์สินหรือเป็นจำนวนมาก เช่น จากคดีทิลแมน กับ สหรัฐอเมริกา (Tillman vs. United States) เป็นคดีเกี่ยวกับประตูกระจกของสถานีจ่ายไฟฟ้าอันเกิดจากสาเหตุเครื่องชักนำกระแสไฟฟ้า คดีเอ็ดเวิร์ด กับ สหรัฐอเมริกา (Edward vs. United States) เป็นคดีเกี่ยวกับกันชนรถบุบ ถ้านำคดีข้างต้นที่เกี่ยวกับมาตรา 1361 มาพิจารณาจะเห็นการตีความนัยกว้างที่สุดจากคดีอีเบอร์ฮาร์ท อาจจะกล่าวได้ว่าการรบกวนการใช้งานทางด้านซอฟต์แวร์ของรัฐ เป็น "การทำให้เสียหาย" (Injury) และค่าเสียหายเป็นได้ทั้งราคาที่ทำขึ้นใหม่ หรือราคาของการซ่อมแซมในกรณีของการที่ไม่ได้ทำขึ้นใหม่

ประมวลกฎหมายสหรัฐอเมริกา บรรพที่ 18 มาตรา 1363 เป็นบทบัญญัติเกี่ยวกับการทำให้เกิดความเสียหายโดยเจตนาร้ายภายในอาณาเขตและเขตน่านน้ำพิเศษ ที่อยู่ในเขตอำนาจศาล มาตรานี้ต่างกับมาตรา 81 โดยเป็นการใช้แทนการทำให้เสียทรัพย์โดยเจตนาร้ายโดยการวางเพลิง

ประมวลกฎหมายสหรัฐอเมริกา บรรพที่ 18 มาตรา 2071 เป็นบทบัญญัติเกี่ยวกับการปิดบังซ่อนเร้น เคลื่อนย้าย ฉีก หรือตัดทอนให้เกิดความเสียหายแก่เอกสารมหาชน เป็นอีกมาตราหนึ่งที่มีการนำกลับมาใช้ใหม่ในยุคการต่อต้านสงครามเวียตนาม มาตรา 2071 น่าจะสามารถนำมาบังคับใช้กับการยักยอกเอกสารคอมพิวเตอร์ของรัฐ โดยเฉพาะกรณีที่ไม่สามารถนำกฎหมายลักทรัพย์ทั่วไปมาใช้บังคับได้ เช่น การคัดลอกหรือทำสำเนาผ่านสถานีสื่อสารทางไกลโดยไม่มีการเคลื่อนที่ คดีที่เกี่ยวกับมาตรา 2071 โดยมากจะเป็นเรื่องเอกสารการคัดเลือกบุคคลเข้ารับราชการทหาร ดังนั้น น่าจะมีการขยายขอบเขตกฎหมายที่เกิดจากคำพิพากษาในคดีก่อนๆ ที่ถือกันว่าเป็นบรรทัดฐาน โดยการขยายขอบเขตนั้นให้รวมถึงบันทึกทางคอมพิวเตอร์ว่าเป็น "เอกสารหรือ

สิ่งที่มีค่าใดๆ" ดังที่กฎหมายบัญญัติไว้ อันเป็นสิ่งที่น่าจะชอบด้วยเหตุผล โดยวัตถุประสงค์ของมาตรา 2071 คือ เพื่อที่จะป้องกันหรือขัดขวางการกระทำใดๆ ที่ทำให้รัฐไม่ได้รับประโยชน์จากเอกสารต่างๆ โดยถือว่าเป็นการปิดบังซ่อนเร้น ทำลาย หรือเคลื่อนย้าย ดังจะเห็นได้จากคดีสหรัฐอเมริกา กับ รอสเนอร์ (United States vs. Rosner) สิ่งที่ได้รับการคุ้มครองจากมาตรา 2071 ไม่เพียงแต่เป็นเอกสารที่เป็นลายลักษณ์อักษรเท่านั้น แต่รวมถึงเอกสารมหาชนทุกประเภทด้วย คดีสหรัฐอเมริกา กับ เดอโกรท (United States vs. DeGroat) เป็นคดีเกี่ยวกับการเน้นที่จะผลักดันกฎหมายต่อเอกสารที่ไม่ใช่กระดาษธรรมดา และด้วยเหตุผลจากการวินิจฉัยในคดีสหรัฐอเมริกา กับ รอสเนอร์ การลบเอกสารทางคอมพิวเตอร์เป็นสิ่งที่แน่ชัดว่าทำให้รัฐไม่ได้รับประโยชน์จากเอกสารนั้น เช่นเดียวกับการราดโลหิตลงเอกสารในคดีสหรัฐอเมริกา กับ อีเบอร์ฮาร์ท การเผาเอกสารในคดีสหรัฐอเมริกา กับ เซส หรือการตัดทอนข้อความเอกสารในคดีสหรัฐอเมริกา กับ ดอนเนอร์

การทำลายทรัพย์สินที่กระทบต่อความมั่นคงของประเทศ มีบัญญัติอยู่ในประมวลกฎหมายสหรัฐอเมริกา บรรพที่ 18 มาตรา 2153 เป็นบทบัญญัติเกี่ยวกับการทำให้เกิดความเสียหายโดยจงใจต่อวัตถุที่ใช้ในสงคราม หรือเพื่อป้องกันประเทศในระหว่างสงครามหรือในภาวะฉุกเฉินของประเทศ ความหมายของวัตถุตามนัยที่กว้างที่สุดจะเห็นได้จากคำนิยามในมาตรา 2151 โดยบัญญัติว่า "วัตถุ ส่วนของวัตถุ หรือส่วนผสมของวัตถุทั้งหลายที่เจตนาจะใช้ มีไว้เพื่อใช้ หรือ เหมาะสมสำหรับ...การทำสงคราม หรือกิจกรรมในการป้องกันประเทศ" แม้จะเป็นที่น่าหนักใจว่าสิ่งที่อยู่ในอุตสาหกรรมคอมพิวเตอร์อาจจะไม่อยู่ภายใต้ความหมายของคำนิยามดังกล่าว แต่ก็เป็นที่แน่ชัดว่า ตราบใดที่ความรู้ว่าผิดในใจของผู้กระทำ มีอยู่ในขณะกระทำนั้นแล้ว ฮาร์ดแวร์และซอฟต์แวร์ของการป้องกันประเทศย่อมเป็นสิ่งที่ได้รับการคุ้มครอง แม้ว่ามาตรานี้จะใช้บังคับเฉพาะช่วงระหว่างสงครามหรือภาวะฉุกเฉินของประเทศหรือการประกาศภาวะฉุกเฉิน ซึ่งประธานาธิบดีทรูแมน (Truman) ได้ประกาศเมื่อปี ค.ศ. 1950 นั้น ปัจจุบันก็ยังมีการใช้บังคับอยู่

มีกฎหมายอีกมาตราหนึ่งที่มีความใกล้เคียงกับมาตรา 2153 โดยมีสาระสำคัญที่แตกต่างกันเพียงประการเดียวคือ ความสามารถในการบังคับใช้ที่ไม่คำนึงถึงภาวะสงครามหรือภาวะฉุกเฉินของประเทศ โดยบัญญัติไว้ในประมวลกฎหมายสหรัฐอเมริกา บรรพที่ 18 มาตรา 2155 เป็นบทบัญญัติเกี่ยวกับการทำลายทรัพย์สินที่มีผลกระทบต่อความมั่นคงของประเทศ (The U.S. Department of Justice, 1989 : 107-108)

4.3 การบัญญัติกฎหมายเพื่อรักษาความปลอดภัยของข้อมูลของประเทศอังกฤษ

ก่อนที่ประเทศอังกฤษจะมีกฎหมายอาญาว่าด้วย การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือการรักษาความปลอดภัยของข้อมูลในคอมพิวเตอร์นั้น การเข้าถึงข้อมูลโดยปราศจากอำนาจไม่ถือว่าเป็นความผิดทางอาญา โดยการเปรียบเทียบกับความผิดฐานบุกรุก (Trespass) และความผิดเกี่ยวกับทรัพย์สิน (Theft) แต่การกระทำนั้นผู้กระทำจะต้องรับผิดในทางแพ่ง (เฉลิมพล ช่อโพธิ์ทอง, 2535 : 73) ภายหลังประเทศอังกฤษได้บัญญัติกฎหมายอาญาว่าด้วยการกระทำความผิดที่เกี่ยวข้องกับคอมพิวเตอร์ขึ้นเป็นฉบับแรก คือ The Computer Misuse Act 1990 ซึ่งบัญญัติว่าการเข้าถึงระบบประมวลผลโดยปราศจากอำนาจเป็นความผิดอาญา โดยไม่จำกัดบุคคลที่กระทำการเข้าถึง ไม่ว่าจะเป็นพนักงานหรือลูกจ้างที่ไม่มีอำนาจ หรือบุคคลภายนอกใดๆ ก็ตาม การบัญญัติกฎหมายดังกล่าวถือได้ว่าเป็นการรองรับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของประเทศอังกฤษ รวมถึงแนวทางการรักษาความปลอดภัยของข้อมูล โดยได้ทำการศึกษาจากกฎหมายของสหรัฐอเมริกาทั้งระดับรัฐบาลกลางและระดับมลรัฐต่างๆ อย่างไรก็ตาม การบัญญัติกฎหมายให้การเข้าถึงโดยปราศจากอำนาจเป็นความผิดอาญานั้น หลักกฎหมายของประเทศอังกฤษถือว่าเป็นสิ่งที่ประหลาดหรือผิดปกติ เพราะแม้แต่การบุกรุกเข้าไปในบ้านของบุคคลอื่นอันเป็นการกระทำทางกายภาพยังไม่เป็นความผิดทางอาญา แต่การบุกรุกโดยการเข้าถึงระบบประมวลผลอันเป็นอุปกรณ์อิเล็กทรอนิกส์ ซึ่งไม่สามารถเห็นได้ด้วยทางกายภาพกลับเป็นความผิดทางอาญา ในเรื่องนี้คณะกรรมการกฎหมายอาญาของอังกฤษถึงกับกล่าวว่า "เป็นสิ่งที่ทำให้ประเทศหวนกลับไปสู่ความล้มเหลวของระบบกฎหมายอังกฤษอีกครั้ง" (This Take Us Back to The Repeated Failure of English Law) ทำให้เป็นสิ่งที่ต้องระแวดระวังจนเกินไป โดยนักกฎหมายอังกฤษเสนอความเห็นว่า กฎหมายอาญาควรจะมีเหตุผลอย่างเพียงพอที่จะขยายขอบเขตของความผิดมากกว่าเป็นการตอบโต้ (สุเนติ คงเทพ, 2541 : 10)

4.4 ความรับผิดเกี่ยวกับการกระทำความผิดเกี่ยวกับข้อมูลในคอมพิวเตอร์ของประเทศอังกฤษ

ตามบทบัญญัติใน The Computer Misuse Act 1990 ได้บัญญัติความรับผิดเกี่ยวกับข้อมูลโดยอาศัยคอมพิวเตอร์ขึ้นมาใหม่ 3 ประการด้วยกัน คือ

1. ความผิดฐานเข้าถึงโดยปราศจากอำนาจ (Unauthorised Access)
2. ความผิดฐานเข้าถึงโดยปราศจากอำนาจโดยมีเจตนาที่จะกระทำ หรือเพื่อความสะดวกในการกระทำความผิดอื่นๆ (Unauthorised Access with Intent to Commit or Facilitate Commission of Further Offences)
3. ความผิดฐานเปลี่ยนแปลงโดยปราศจากอำนาจ (Unauthorised Modification)

4.4.1 ความผิดฐานเข้าถึงโดยปราศจากอำนาจ (Unauthorised Access)

ความผิดฐานเข้าถึงโดยปราศจากอำนาจได้บัญญัติไว้ใน The Computer Misuse Act 1990 มาตรา 1 โดยบัญญัติว่า

(1) บุคคลจะมีความผิด เมื่อ

(a) บุคคลได้กระทำการให้คอมพิวเตอร์แสดงผล หรือแสดงการทำงานใดๆ ด้วยเจตนาที่จะผ่านสิ่งป้องกันที่มีไว้เพื่อกันการเข้าถึงระบบ และได้ทำการผ่านสิ่งป้องกันเช่นว่านั้นเข้าถึงโปรแกรมคอมพิวเตอร์ใดๆ หรือสารสนเทศที่เก็บไว้ในคอมพิวเตอร์ใดๆ

(b) การผ่านสิ่งป้องกันเข้าไปยังระบบนั้น เป็นการกระทำโดยปราศจากอำนาจ และ

(c) บุคคลนั้นได้รู้ขณะที่กระทำอยู่แล้วว่า การกระทำอันเป็นเหตุให้คอมพิวเตอร์แสดงผลหรือแสดงการทำงานนั้นปราศจากอำนาจ

(2) เจตนาของบุคคลที่ได้กระทำความผิดภายใต้มาตรานี้ ไม่จำเป็นต้องเป็นการกระทำที่เป็น

(a) โปรแกรมพิเศษเฉพาะเจาะจงใดๆ หรือข้อมูล

(b) โปรแกรมหรือข้อมูลของสิ่งเฉพาะเจาะจงใดๆ หรือ

(c) โปรแกรมหรือข้อมูลที่ถูกเก็บไว้ในคอมพิวเตอร์อย่างเฉพาะเจาะจงใดๆ

(3) **บุคคลที่มีความผิดภายใต้บทบัญญัตินี้ จะต้องถูกพิจารณาคดีแบบรวดรัดและต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกินระดับ 5 ตามตารางมาตรฐาน หรือทั้งจำทั้งปรับ**

ตามบทบัญญัติดังกล่าวจะเห็นได้ว่า เป็นบทบัญญัติพื้นฐานที่ใช้กับการเข้าถึงโดยปราศจากอำนาจที่ไม่สลับซับซ้อน เน้นการกระทำที่จะเป็นความผิดต้องเป็นการทำให้คอมพิวเตอร์แสดงผลหรือแสดงการทำงานใดๆ แต่ไม่รวมถึงการกระทำทางกายภาพที่กระทำต่อเครื่องคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์ เช่น การดูข้อมูลที่ปรากฏบนจอภาพโดยไม่มีการกระทำใดๆ กับคอมพิวเตอร์ อย่างไรก็ตามความผิดตามบทบัญญัตินี้ รวมถึงการสั่งให้คอมพิวเตอร์แสดงการทำงานโดยระยะทางไกล (Remote) ด้วยและไม่คำนึงถึงผลของการกระทำ เช่น ไม่คำนึงว่าผู้กระทำนั้นจะประสบความสำเร็จในการเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลหรือไม่ หรือผู้กระทำจะประสบความสำเร็จในการที่จะผ่านมาตรการป้องกันความปลอดภัยหรือไม่ นอกจากนั้นยังรวมถึงการกระทำที่เป็นการพยายามกระทำความผิดด้วย ดังจะเห็นได้จากการที่คณะกรรมการยกร่างกฎหมายได้เติมคำว่า "ผู้เข้าถึงโดยปราศจากอำนาจต้องกระทำการเพื่อพังประตูที่ปิดกั้นทางเข้าสู่ระบบคอมพิวเตอร์นั้น" (Knocking on The Door of The Computer) ไม่ว่าจะประสบผลสำเร็จหรือไม่ (สุเนติ คงเทพ, 2541 : 11)

พิจารณาองค์ประกอบของความผิดฐานเข้าถึงโดยปราศจากอำนาจ โดยพิจารณาตามความรับผิดทางอาญาของกฎหมายคอมมอนลอว์ ซึ่งแยกพิจารณาเป็น 2 ส่วน คือ ส่วนแรกส่วนของการกระทำ (Actus Reus) และส่วนที่สองส่วนที่อยู่ในภายจิตใจหรือเจตนาร้าย (Mens Rea) (แสวง บุญเฉลิมวิภาส, 2524)

ส่วนของการกระทำ (Actus Reus) คือผู้กระทำความผิดจะต้องกระทำการอันเป็นเหตุให้คอมพิวเตอร์แสดงผลหรือแสดงการทำงานใดๆ แต่ก็ไม่ได้หมายความถึงกรณีที่เพียงแต่สัมผัสทางกายภาพกับเครื่องคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์โดยไม่มีการกระทำใดๆ ต่อคอมพิวเตอร์ ทั้งนี้ไม่รวมถึงการดูข้อมูลที่ปรากฏทางจอภาพ การดักจับข้อมูล หรือการดักฟังข้อมูล ส่วนผลของการกระทำความผิดเป็นไปตามที่กล่าวไว้แล้วข้างต้น คือผู้กระทำนั้นจะต้องรับผิดไม่ว่าผู้กระทำจะประสบผลสำเร็จในการเข้าสู่ระบบประมวลผลหรือไม่ก็ตาม

ส่วนสิ่งที่อยู่ภายในจิตใจหรือเจตนาร้าย (Mens Rea) สามารถแยกพิจารณาออกเป็น 2 ประการ

1. **เจตนาที่จะผ่านสิ่งป้องกันที่มีไว้เพื่อกันการเข้าถึงระบบ เพื่อการเข้าถึงโปรแกรมคอมพิวเตอร์ใดๆ หรือสารสนเทศที่เก็บไว้ในคอมพิวเตอร์ใดๆ คำว่า "ใดๆ" (Any) ในอนุมาตรา (1) (a) เป็นข้อความที่ขยายความของคำว่า "เจตนา" อันแสดงให้เห็นชัดเจนยิ่งขึ้นว่าเจตนานั้น ไม่จำต้องมีความสัมพันธ์กับคอมพิวเตอร์ที่ผู้กระทำผิดใช้กระทำการดังกล่าวในเวลานั้น และข้อความในอนุมาตรา (2) ได้อธิบายถึงเจตนาของบุคคลที่ได้กระทำความผิด ไม่จำเป็นต้องเป็นเจตนาโดยตรงที่เป็นการมุ่งต่อโปรแกรมเฉพาะเจาะจงใดๆ หรือข้อมูลใดๆ หรือโปรแกรมหรือข้อมูลชนิดใดชนิดหนึ่งโดยเฉพาะ สรุปก็คือว่าเจตนากระทำต่อโปรแกรมหรือข้อมูลใดๆ ก็เป็นความผิด ทั้งนี้ยังรวมความถึงผู้กระทำการโดยปราศจากอำนาจที่เข้าสู่ระบบโดยไม่มีความคิดที่ชัดเจนในตอนแรก แต่เกิดความคิดขึ้นในภายหลัง ดังนั้น จะเห็นได้ว่าการประมาทหรือการไม่ตั้งใจเข้าสู่ระบบคอมพิวเตอร์ก็อาจจะเป็นความผิดได้**

2. **เจตนาภายใน คือผู้กระทำความผิดจะต้องรู้ในขณะที่กระทำให้คอมพิวเตอร์แสดงผลหรือแสดงการทำงานใดๆ ว่าปราศจากอำนาจแต่ได้เข้าถึงโปรแกรมหรือข้อมูลด้วยความจงใจ กล่าวโดยสรุปคือว่า ในการฟ้องร้องผู้กระทำความผิด "ฐานเข้าถึงโดยปราศจากอำนาจ" โจทก์จะต้องพิสูจน์ให้ศาลเห็นถึงสาระสำคัญ 2 ประการ คือ ประการที่หนึ่งจำเลยมีเจตนาเข้าสู่ระบบและประการที่สอง จำเลยได้รู้ในขณะที่เขากระทำให้คอมพิวเตอร์แสดงผลหรือแสดงการทำงานใดๆ ว่าเขาได้เข้าไปสู่ระบบด้วยความจงใจโดยปราศจากอำนาจ ซึ่งการพิสูจน์ทั้งสองประการที่เป็นเรื่องของจิตใจของผู้กระทำนั้นถือเป็นหลักในการที่จะลงโทษผู้นั้น อย่างไรก็ตามบทบัญญัตินี้ก็ยังมีประเด็นปัญหาที่ถกเถียงกันว่า ถ้าผู้เข้าสู่ระบบเป็นพนักงานหรือลูกจ้างขององค์กรนั้นๆ ควรจะต้องรับโทษเช่นเดียวกับบุคคลภายนอกที่เข้าถึงโดยปราศจากอำนาจหรือไม่ เพราะขั้นตอนของการพิจารณานั้นจะต้องพิจารณาถึงการมีอำนาจเข้าสู่ระบบก่อนการพิจารณาในประเด็นอื่นๆ และอีกปัญหาหนึ่งคือใครจะเป็นผู้มีอำนาจในการอนุญาต เพราะถ้ามีการกำหนดกฎเกณฑ์อย่างเคร่งครัดก็จะก่อให้เกิดความไม่สะดวกในการปฏิบัติงาน**

ประการสุดท้ายที่กล่าวถึงสำหรับความผิดฐานเข้าถึงโดยปราศจากอำนาจนั้น คือ ศาลใดที่มีอำนาจในการพิจารณาคดี เนื่องจากบทบัญญัติตามมาตรานี้ เป็นการกระทำความผิดที่ไม่สลับซับซ้อน ศาลที่มีอำนาจในการพิจารณาคดีก็คือศาลแขวง (Magistrate Court) ดังนั้น ทำให้มีกฎหมายที่เกี่ยวข้องอีกฉบับหนึ่งคือ The Magistrates' s Court Act 1980 โดยมาตรา 44 (1) อันเป็นบทบัญญัติ ที่ช่วยเสริมให้สามารถลงโทษบุคคลที่ช่วยเหลือผู้ที่ทำการเข้าถึงโดยปราศจาก

อำนาจ โดยการให้ความรู้ทางด้านข้อมูล การให้รหัสผ่าน หรือให้วิธีการเข้าสู่ระบบเพื่อผ่านไปยังโปรแกรมคอมพิวเตอร์หรือข้อมูลในคอมพิวเตอร์

4.4.2 **ความผิดฐานเข้าถึงโดยปราศจากอำนาจโดยมีเจตนาที่จะกระทำหรือเพื่อความสะดวกในการกระทำความผิดอื่น ๆ** (Unauthorised Access with Intent to Commit or Facilitate Commission of Further Offences)

ความผิดฐานนี้ เป็นความผิดที่สลับซับซ้อนกว่าความผิดฐานเข้าถึงโดยปราศจากอำนาจ จึงได้แยกบัญญัติเป็นอีกมาตราหนึ่ง โดยบัญญัติไว้ใน The Computer Misuse Act 1990 มาตรา 2 ว่า

(1) บุคคลจะมีความผิดภายใต้บทบัญญัตินี้ ถ้าหากว่าเขาได้กระทำความผิดตามมาตรา 1 ข้างต้น (ความผิดฐานเข้าถึงโดยปราศจากอำนาจ) โดยมีเจตนา

(a) กระทำความผิดในสิ่งที่มาตรานี้ใช้บังคับ หรือ

(b) ให้ความสะดวกในการกระทำความผิด (ไม่ว่าจะเป็นการกระทำความผิดของตนเองหรือของบุคคลอื่น) และความผิดที่เขาเจตนากระทำหรือให้ความสะดวกดังจะกล่าวต่อไปในมาตรานี้ ให้ถือว่าเป็นผู้กระทำความผิดเช่นเดียวกับผู้กระทำความผิดที่ตนช่วยเหลือ

(2) มาตรานี้ใช้กับความผิด

(a) ใช้กับความผิดที่ถูกกำหนดไว้ในกฎหมาย หรือ

(b) ใช้กับบุคคลที่มีอายุ 21 ปี หรือกว่านั้น

(3) เพื่อวัตถุประสงค์ของมาตรานี้ ไม่ว่าการกระทำความผิดของผู้กระทำที่อยู่ระยะไกล (Remote) จะได้กระทำลงในโอกาสที่ปราศจากอำนาจเข้าสู่ระบบหรือไม่ หรือโดยการอาศัยโอกาสอื่นใดก็ตาม

(4) บุคคลอาจจะมีความผิดตามมาตรานี้ แม้จะปรากฏข้อเท็จจริงว่าการกระทำความผิดของผู้กระทำที่อยู่ระยะไกลจะไม่ได้กระทำลงก็ตาม

(5) บุคคลผู้กระทำความผิดตามมาตรานี้ จะต้อง

(a) ถูกพิจารณาแบบรวดรัด และจะต้องถูกลงโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกินขั้นสูงตามที่กฎหมายกำหนด หรือทั้งจำทั้งปรับ และ

(b) หากเป็นความผิดร้ายแรงจะถูกลงโทษจำคุกไม่เกิน 5 ปี หรือปรับ หรือทั้งจำทั้งปรับ

ตามบทบัญญัติมาตรา 2 นี้จะเห็นได้ว่าเป็นความผิดที่ร้ายแรงกว่ามาตราก่อน โดยจะต้องผ่านการเข้าถึงโดยปราศจากอำนาจด้วยเจตนาที่จะกระทำความผิดอื่นๆ หรือให้ความสะดวกแก่ผู้กระทำความผิดในการก่อให้เกิดการกระทำความผิดร้ายแรงเกิดขึ้น อันแตกต่างจากความผิดตามมาตรา 1 โดยมาตรา 1 เป็นกรณีที่ใช้กับการที่ไม่อาจพิสูจน์เจตนาในอนาคตได้ ซึ่งจะมีโทษเบากว่า แต่หากพิสูจน์เจตนาในอนาคตได้ (โดยไม่จำเป็นต้องพิสูจน์ว่าเจตนาในอนาคตนั้นได้มีการกระทำความผิดจริงหรือไม่) จะใช้มาตรา 2 อันมีบทลงโทษกับผู้กระทำความผิดที่คิดจะกระทำความผิดในอนาคต ซึ่งสามารถเทียบเคียงกับหลักกฎหมายการพยายามกระทำความผิดใน The Criminal Attempt Act 1981 มาตรา 1 (2) อนึ่ง สำหรับความผิดประเภทที่ไม่จำเป็นต้องพิสูจน์ถึงเจตนาของผู้กระทำความผิดว่าได้เกิดขึ้นหรือไม่ ตามที่กล่าวไว้ข้างต้น เป็นความผิดที่เรียกกันว่า "ความผิดที่ไกลออกไป" (Further offence)

การฟ้องร้องเพื่อจะลงโทษผู้กระทำความผิดตามมาตรานี้ โจทก์จะต้องพิสูจน์ว่าจำเลยได้เข้าถึงสาระสำคัญอันได้แก่ โปรแกรมคอมพิวเตอร์หรือข้อมูลในคอมพิวเตอร์ ด้วยเจตนาที่จะกระทำความผิดอื่น โดยไม่คำนึงถึงเวลาของการกระทำความผิดอื่นว่าจะกระทำในเวลาใด ไม่ว่าจะเป็นในขณะที่เกือบจะเป็นเวลาเดียวกับการเข้าถึงโดยปราศจากอำนาจ หรือในโอกาสต่อมา ความผิดที่เกิดขึ้นในลักษณะนี้มากที่สุดคือ ความผิดฐานฉ้อโกง ความผิดฐานลักทรัพย์ และความผิดฐานยักยอกทรัพย์ แต่ถ้าหากการดำเนินคดีไม่สามารถที่จะลงโทษผู้กระทำความผิดตามมาตรานี้ แต่เข้าองค์ประกอบความผิดตามมาตรา 1 (ความผิดฐานเข้าถึงโดยปราศจากอำนาจ) ก็สามารถจะลงโทษตามมาตรา 1 ได้ โดยถือว่าเป็นความผิดที่ต่อเนื่องหรือลดหลั่นเป็นลำดับชั้น

ศาลที่มีอำนาจในการพิจารณาคดีสำหรับการกระทำความผิดตามมาตรานี้ คือ ศาลสูงคดีอาญา (Crown Court) หรือศาลแขวง (Magistrate Court) ขึ้นอยู่กับความร้ายแรงของความผิด สำหรับโทษที่จะลงนั้นได้บัญญัติไว้ในอนุมาตรา (5) (a) และ (b) ดังได้กล่าวไว้แล้ว ข้อสังเกตประการสุดท้ายสำหรับความผิดมาตรานี้ ซึ่งกฎหมายอังกฤษได้ให้ความระแวดระวังอย่างที่สุดคือ ความผิดตามอนุมาตรา (4) ได้บัญญัติถึงการได้ข้อเท็จจริงมาโดยตั้งใจที่จะทำการเข้าถึงโดยปราศจากอำนาจ แต่ยังไม่กระทำการเข้าถึงก็ถือเป็นความผิดตามอนุมาตรานี้แล้ว

4.4.3 **ความผิดฐานเปลี่ยนแปลงโดยปราศจากอำนาจ (Unauthorised Modification)**

ความผิดฐานนี้เป็นความผิดที่เกี่ยวกับการแก้ไขเปลี่ยนแปลง และการทำลายข้อมูล โดยได้มีการบัญญัติไว้ใน The Computer Misuse Act 1990 มาตรา 3 ว่า

(1) บุคคลจะมีความผิด ถ้า

(a) ผู้นั้นได้กระทำการใดๆ ซึ่งก่อให้เกิดการแก้ไขเปลี่ยนแปลงในเนื้อหาสาระของคอมพิวเตอร์ใดๆ และ

(b) ผู้ที่กระทำการเช่นว่านั้น จะต้องมีเจตนาหรือจะต้องรู้ถึงการกระทำของตนในขณะที่กระทำการนั้น

(2) เพื่อวัตถุประสงค์ของอนุมาตรา (1) (b) ข้างต้น เจตนานั้นจะต้องเป็นเจตนาที่ต้องการแก้ไขเปลี่ยนแปลงเนื้อหาสาระของคอมพิวเตอร์ใดๆ โดยการกระทำ เช่น

(a) ทำให้เกิดความเสียหายต่อการทำงานของคอมพิวเตอร์

(b) ทำการกีดกันหรือขัดขวางการเข้าถึงโปรแกรมคอมพิวเตอร์ หรือข้อมูลในคอมพิวเตอร์ หรือ

(c) ทำให้เกิดความเสียหายต่อการทำงานของโปรแกรมคอมพิวเตอร์ หรือทำลายความเชื่อถือของข้อมูล

(3) เจตนาของการกระทำดังกล่าว ไม่จำต้องเป็นเจตนาที่กระทำโดยตรงต่อ

(a) คอมพิวเตอร์พิเศษเฉพาะเจาะจงใดๆ

(b) โปรแกรมหรือข้อมูลพิเศษเฉพาะเจาะจงใดๆ หรือโปรแกรมหรือข้อมูลชนิดใดชนิดหนึ่งโดยเฉพาะ หรือ

(c) การแก้ไขเปลี่ยนแปลงพิเศษเฉพาะเจาะจงใดๆ หรือการแก้ไขเปลี่ยนแปลงชนิดใดชนิดหนึ่งโดยเฉพาะ

(4) เพื่อวัตถุประสงค์ของอนุมาตรา (1) (b) ข้างต้น ผู้กระทำต้องรู้ว่าการแก้ไขเปลี่ยนแปลงดังกล่าว เขาเจตนาที่กระทำโดยปราศจากอำนาจ

(5) มาตรานี้ไม่ถือวัตถุประสงค์เป็นสิ่งสำคัญ โดยไม่คำนึงว่าการแก้ไขเปลี่ยนแปลงโดยปราศจากอำนาจ หรือผลที่เจตนาที่จะให้เกิดขึ้นตามอนุมาตรา (2) ข้างต้น จะเป็นการเจตนาให้เกิดขึ้นเป็นการถาวรหรือเกิดขึ้นเพียงชั่วคราว

(6) การแก้ไขเปลี่ยนแปลงในเนื้อหาสาระของคอมพิวเตอร์ตามกฎหมายฉบับนี้ จะไม่ถือว่าเป็นการก่อให้เกิดความเสียหายแก่คอมพิวเตอร์ใดๆ ตามกฎหมายอาญาเกี่ยวกับการก่อให้เกิดความเสียหาย (The Criminal Damage Act 1971) เว้นแต่การกระทำนั้นมีผลทางกายภาพเท่านั้น

(7) บุคคลผู้กระทำความผิดตามมาตรานี้ จะต้อง

(a) ถูกพิจารณาแบบรวดรัด และจะต้องถูกลงโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกินขั้นสูงตามที่กฎหมายกำหนด หรือทั้งจำทั้งปรับ และ

(b) หากเป็นความผิดร้ายแรงจะถูกลงโทษจำคุกไม่เกิน 5 ปี หรือปรับ หรือทั้งจำทั้งปรับ

จากบทบัญญัติดังกล่าว พิจารณาองค์ประกอบความผิดในส่วนของการกระทำ จะเห็นได้ว่ามีการกำหนดขอบเขตของการกระทำความผิดไว้ค่อนข้างจำกัด โดยเน้นว่าจะต้องเป็นการแก้ไขเปลี่ยนแปลง (Modification) ในเนื้อหาสาระ (Contents) ของคอมพิวเตอร์เท่านั้นที่จะถือเป็นความผิดตามมาตรานี้ ดังจะเห็นได้จากบทบัญญัติของอนุมาตรา (1) (a) และแม้ว่าการกระทำดังกล่าวจะมีส่วนที่เกี่ยวข้องสัมพันธ์กับการกระทำความผิดเกี่ยวกับความเสียหายทางอาญา แต่ก็ไม่ถือเป็นความผิดตามกฎหมายอาญาเกี่ยวกับการก่อให้เกิดความเสียหาย เว้นแต่การกระทำการแก้ไขเปลี่ยนแปลงนั้นจะเป็นการทำให้เสียหายทางกายภาพ อย่างไรก็ตามมีการตั้งข้อสังเกตว่าความผิดตามบทบัญญัติมาตรานี้ได้วางขอบเขตและรูปแบบของการกระทำภายใต้คำว่า "การแก้ไขเปลี่ยนแปลง" ไว้อย่างกว้างขวาง โดยถือตามส่วนการแปลความหมายของคำ (Interpretation) ในมาตรา 17 ของกฎหมายฉบับนี้

มาตรา 17 (7) ได้ให้คำนิยามของคำว่า "การแก้ไขเปลี่ยนแปลง" ไว้ว่า

การแก้ไขเปลี่ยนแปลงเนื้อหาสาระของคอมพิวเตอร์ใดๆ ถ้าการแก้ไขเปลี่ยนแปลงที่เกิดขึ้นนั้นมีผลต่อการทำงานใดๆ ของคอมพิวเตอร์อันกระทบต่อคอมพิวเตอร์นั้น หรือคอมพิวเตอร์อื่นๆ

(a) โปรแกรมคอมพิวเตอร์หรือข้อมูลใดๆ ที่เก็บอยู่ในคอมพิวเตอร์ ถูกแก้ไขเปลี่ยนแปลง หรือถูกลบ หรือ

(b) โปรแกรมคอมพิวเตอร์หรือข้อมูลใดๆ ถูกเพิ่มเข้าไป

และการกระทำใดๆ ซึ่งมีส่วนที่เป็นสาเหตุให้เกิดการแก้ไขเปลี่ยนแปลง จะถูกพิจารณาว่าเป็นสาเหตุที่ก่อให้เกิดการแก้ไขเปลี่ยนแปลงนั้น

พิจารณาในส่วนของเจตนา การที่จะถือว่าผู้กระทำมีความผิดนั้นผู้นั้นต้องมีเจตนาและจะต้องรู้ในขณะที่กระทำการแก้ไขเปลี่ยนแปลงว่า ตนเจตนาที่แก้ไขเปลี่ยนแปลงเนื้อหาสาระในคอมพิวเตอร์ ส่วนผลของการกระทำนั้นจะต้องก่อให้เกิดความเสียหายต่อคอมพิวเตอร์ หรือโปรแกรมคอมพิวเตอร์ หรือทำลายความเชื่อถือของข้อมูล หรือกระทำการกีดกันหรือขัดขวางมิให้ผู้มีอำนาจเข้าถึงโปรแกรมหรือข้อมูล

การที่ The Computer Misuse Act 1990 เน้นถึงการแก้ไขเปลี่ยนแปลงต้องเป็นการกระทำในส่วนที่เป็นเนื้อหาสาระ ก็เพราะไม่ต้องการให้มีการพิสูจน์ความเสียหายที่เกิดขึ้นต่อวัตถุที่ไม่สามารถมองเห็นได้ด้วยทางกายภาพที่อาจเกิดขึ้นได้จากการกระทำการบางอย่าง เช่น การลบข้อมูล การปลอมข้อมูล ดังนั้น จึงมีการบัญญัติกฎหมายฉบับนี้ขึ้นใหม่ โดยไม่เลือกที่จะไปแก้ไขเพิ่มเติมหรือขยายความคำนิยามของคำว่า "ทรัพย์สิน" ในกฎหมายอาญาเกี่ยวกับการก่อให้เกิดความเสียหาย เพื่อให้ครอบคลุมถึงการกระทำที่ก่อให้เกิดความเสียหายต่อวัตถุที่ไม่สามารถมองเห็นได้ด้วยทางกายภาพ ซึ่งคณะกรรมาธิการร่างกฎหมายฉบับดังกล่าวได้กล่าวว่าเป็นการไม่เหมาะสมอย่างที่สุดที่จะไปแก้ไขกฎหมายอื่นที่เกี่ยวข้องแทนการบัญญัติขึ้นมาใหม่

ประการสุดท้ายที่จะพิจารณาคือปัญหาเกี่ยวกับไวรัสคอมพิวเตอร์ โดยมีประเด็นหลักว่า The Computer Misuse Act 1990 สามารถนำไปใช้กับการกระทำความผิดเกี่ยวกับไวรัสคอมพิวเตอร์ได้หรือไม่ ซึ่งยังเป็นข้อถกเถียงสำหรับนักกฎหมายอังกฤษ โดยฝ่ายหนึ่งเห็นว่ากฎหมายดังกล่าว มิได้บัญญัติไว้ให้ชัดเจนที่จะให้มีผลครอบคลุมถึงการกระทำความผิดเกี่ยวกับไวรัสคอมพิวเตอร์ ไม่ว่าจะเป็นตัวบทบัญญัติหรือเจตนารมย์ของกฎหมาย แต่นักกฎหมายอีกฝ่ายหนึ่งเห็นว่า บทบัญญัติมาตรา 3 ของกฎหมายฉบับนี้สามารถขยายไปถึงความผิดเกี่ยวกับไวรัสคอมพิวเตอร์ได้ เพราะการใส่ไวรัสคอมพิวเตอร์เข้าไปสู่คอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์ ถ้าก่อให้เกิดความเสียหายต่อการใช้งาน อันมีลักษณะคล้ายกับการกีดกันหรือขัดขวางการใช้งานของผู้ที่มีอำนาจ ส่วนความเห็นของคณะกรรมาธิการร่างกฎหมายเห็นว่ากฎหมายฉบับนี้ สามารถปรับใช้กับการกระทำที่เป็นการใส่โปรแกรมอันตรายเข้าไปในคอมพิวเตอร์ซึ่งผู้กระทำอาจถูกฟ้อง ในความผิดฐานการแก้ไขเปลี่ยนแปลงต่อเนื้อหาสาระในคอมพิวเตอร์โดยปราศจากอำนาจอันเนื่องมาจากการกระทำของตน แต่อย่างไรก็ตามยังไม่ปรากฏชัดจากคำพิพากษาของศาลว่า กฎหมายฉบับนี้สามารถปรับใช้กับการกระทำความผิดเกี่ยวกับไวรัสคอมพิวเตอร์ได้หรือไม่ ทำให้นักกฎหมายอังกฤษจะต้องติดตามเพื่อจะใช้เป็นบรรทัดฐานต่อไป