บทที่ 3
การเข้าถึงข้อมูลส่วนบุคคลจากข้อมูลอิเล็กทรอนิกส์ในกฎหมายต่างประเทศ

ในบทที่แล้วได้กล่าวถึงความหมาย ลักษณะ และสภาพปัญหาของการแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลจากข้อมูลอิเล็กทรอนิกส์ในอาชญากรรมทางคอมพิวเตอร์รูปแบบต่างๆดังที่ได้กล่าวมาแล้ว ซึ่งปัญหาอาชญากรรมคอมพิวเตอร์นี้ก็มิใช่ว่าจะเกิดแต่เฉพาะในประเทศไทยเท่านั้น แต่ยังส่งผลกระทบต่อกฎหมายอาญาของประเทศอื่นๆ ด้วย ดังนั้นในบทนี้จะกล่าวถึงแนวความคิดในการบัญญัติกฎหมายเพื่อรักษาความปลอดภัยของข้อมูล สภาพปัญหาเกี่ยวกับการปราบปรามอาชญากรรมคอมพิวเตอร์ และมาตรการทางกฎหมายและปัญหาเกี่ยวกับการแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลจากข้อมูลอิเล็กทรอนิกส์ในอาชญากรรมคอมพิวเตอร์ของประเทศต่างๆ ได้แก่ ประเทศสหรัฐอเมริกา อังกฤษ และญี่ปุ่น โดยการศึกษาถึงแนวความคิด เหตุผล ขั้นตอน วิธีการ และระยะเวลาในการค้น และการรับฟังเป็นพยานหลักฐานในศาลของประเทศต่างๆ เพื่อเป็นแนวทางในการแก้ปัญหาที่เกิดขึ้นในกฎหมายไทยต่อไป

3.1 ประเทศสหรัฐอเมริกา

ประเทศสหรัฐอเมริกาเป็นประเทศหนึ่งที่มีความเจริญก้าวหน้าทางเทคโนโลยีในหลายๆด้าน และมีกฎหมายที่จะใช้ดำเนินคดีกับอาชญากรรมคอมพิวเตอร์มากกว่า 40 ฉบับ เช่น National Stolen Property Act , Copyright Act ฯลฯ จึงต้องพิจารณาว่ากฎหมายที่มีอยู่ทั้ง 40 ฉบับนั้น สามารถนำมาใช้บังคับและครอบคลุมความผิดอาญาเกี่ยวกับคอมพิวเตอร์ได้มากน้อยเพียงใด สำหรับความผิดเกี่ยวกับคอมพิวเตอร์สหรัฐเองก็มีการบัญญัติกฎหมายตั้งแต่ปี ค.ศ. 1984 คือ The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (CFAA) ซึ่งแบ่งความผิดเกี่ยวกับคอมพิวเตอร์เป็น 3 ลักษณะ ได้แก่

ก. Subsection 1030 (a) (1) ความผิดที่ก่อความเสียหายแก่ความมั่นคงของรัฐโดยตรง

ข. Subsection 1030 (a) (2) ความผิดที่ก่อให้เกิดความเสียหายต่อระบบความเชื่อถือส่วนบุคคลที่มีในสถาบันการเงิน หรือหน่วยงานที่ทำหน้าที่ดูแลประวัติ และผู้บริโภค

ค. Su bsection 1030 (a) (3) ความผิดที่กระทำต่อข้อมูลข่าวสารของเครื่องคอมพิวเตอร์อันก่อให้เกิดความเสียหายต่อรัฐบาลสหรัฐ[1]

และมีการแก้ไขเพิ่มเติมในปี 1988 และ 1990 ตามลำดับเพื่อให้ครอบคลุมความผิดที่เกิดขึ้น สภาคองเกรสได้มีมติให้ออกกฎหมาย The National Information Infrastructure Protection Act of 1996 (NIIPA) [2] และเพิ่มเติมการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ใน U.S. Code title 18 มาตรา 1030 (18 U.S.C.A. section 1030)[3] สำหรับกฎหมายของมลรัฐต่างๆ เริ่มมีใน ค.ศ. 1987 โดยเริ่มมีที่มลรัฐอริโซน่า และมลรัฐฟลอริดา และหลังจากถูกกลุ่มผู้ก่อการร้ายโจมตีตึกเพนทากอนและอาคารเวิลด์เทรดเซ็นเตอร์ เมื่อวันที่ 11 กันยายน ค.ศ. 2001 จึงให้ความสำคัญกับการรักษาความปลอดภัยและความเป็นส่วนตัวกันมากขึ้น และได้จัดสรรเงินเพื่อแก้ปัญหาอาชญากรรม โดยเฉพาะในส่วนที่เกี่ยวกับความปลอดภัยในเครือข่ายคอมพิวเตอร์ (Cyber-security) และการวิจัยเกี่ยวกับการก่อการร้ายในเครือข่ายคอมพิวเตอร์ (Cyber-terrorism) [4]

3.1.1 มาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกา ประเทศสหรัฐอเมริกาเป็นประเทศแรกที่ประกาศใช้กฎหมายจำกัดการใช้อินเตอร์เน็ตเพื่อความบันเทิงทางเพศ คือกฎหมายควบคุมสื่อลามกและข้อความที่ไม่สมควรทางเพศบนอินเตอร์เน็ต (Communications Decency Act 1996 : CDA.) ซึ่งมีเนื้อหากำกับสิ่งที่ให้บริการทางอินเตอร์เน็ตโดยเฉพาะ โดยกำหนดให้บุคคลที่ส่งภาพหรือข้อความลามกอนาจารหรือไม่เหมาะสมขัดต่อศีลธรรมอันดี แก่ผู้เยาว์อายุต่ำกว่า 18 ปี มีความผิดต้องรับโทษปรับหรือจำคุกไม่เกิน 2 ปี [5] และถ้าผู้ใดอนุญาตให้ผู้เยาว์อายุต่ำกว่า 18 ปี ใช้อินเตอร์เน็ตหรือสถานที่เพื่อการดังกล่าวย่อมมีความผิดด้วย[6] จะเห็นได้ว่ากฎหมายฉบับนี้จำกัดสิทธิเสรีภาพและความเป็นส่วนตัวของบุคคล เมื่อกฎหมายฉบับนี้ใช้บังคับในวันที่ 8 กุมภาพันธ์ 1996 สมาคมสิทธิทางแพ่งของสหรัฐอเมริกัน (ACLU) และ

---

[1] นิติ ผดุงชัย. (2532,มิถุนายน). “กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับ Computer.” **วารสารอัยการ**. หน้า 86-88.

[2] Michael Hatcher , Jay Mc Danell , and Stacy Ostfeld. (1999). “Computer Crimes.” **American Criminal Law Review**. 36 : p.402.

[3] Ibid.p.401.

[4] “The Governance Challenge : Creating a smart and Secure Cyberspace,” Madanmohan Rao report from the ‘New Directions in Internet Policy’ conference in Atlanta, <http://www.indiainfoline.com/nevi/inwi/mm66.html.>,2002.

[5] CDA, Section 223.

[6] CDA, Section 223 (a) (2).

สมาคมห้องสมุด (ALA) ได้ยื่นฟ้องต่อศาลขอประกาศว่ากฎหมายฉบับนี้ขัดต่อรัฐธรรมนูญว่าด้วยการคุ้มครองเสรีภาพในการแสดงออก และสิทธิความเป็นส่วนตัว ตามบทแก้ไขเพิ่มเติมฉบับที่ 1 (First Amendment) และรัฐบาลสหรัฐอเมริกาก็ได้โต้แย้งว่ากฎหมายฉบับนี้บังคับใช้แต่เฉพาะบุคคลที่ไม่สุจริตและรู้ว่าผู้เยาว์ใช้บริการในสถานที่ของตน และยกเว้นบุคคลที่ไม่รู้ว่าข้อความที่ผ่านคอมพิวเตอร์ของตนนั้นเป็นข้อความหรือภาพลามก การจำกัดเสรีภาพจะกระทำต่อเด็กและเยาวชนเท่านั้น ไม่รวมถึงบุคคลทั่วไป แต่ในที่สุดศาลก็ตัดสินให้ระงับใช้กฎหมายฉบับนี้เพราะอาจจะขัดต่อรัฐธรรมนูญ [7]

3.1.2 การกำหนดความผิดเพื่อคุ้มครองสิทธิส่วนบุคคลที่เป็นข้อมูลอิเล็กทรอนิกส์ ในปี ค.ศ. 1986 สภาคองเกรสของสหรัฐอเมริกาได้ออก The Computer Fraud and Abuse Act of 1986 ซึ่งกฎหมายฉบับนี้มีบทบัญญัติที่เปลี่ยนแปลงไปจากกฎหมายที่มีอยู่เดิม ได้แก่

3.1.2.1 ความผิดฐานเข้าถึงโดยปราศจากอำนาจ (Unauthorized Access)

3.1.2.2 ความผิดฐานแก้ไขเปลี่ยนแปลง (Alteration)

3.1.2.3 ความผิดฐานทำให้เสียหายหรือทำลาย (Damage or Destruction)

3.1.2.1 ความผิดฐานเข้าถึงโดยปราศจากอำนาจ (Unauthorized Access) ความผิดฐานเข้าถึงโดยปราศจากอำนาจเป็นความผิดฐานหนึ่ง ที่เป็นการฉ้อโกงหรือกระทำการใดๆ ต่อเครื่องคอมพิวเตอร์โดยเจตนา เป็นการกระทำโดยปราศจากอำนาจ หรือกระทำเกินกว่าอำนาจที่มีอยู่ ได้แก่

(1) เข้าสู่ระบบคอมพิวเตอร์โดยรู้ว่าไม่มีอำนาจ และได้ไปซึ่งข้อมูลนั้น โดยมีเหตุเชื่อได้ว่าข้อมูลนั้นอาจถูกใช้ไปเพื่อการอันเป็นภัยต่อความมั่นคงของประเทศ หรือเพื่อประโยชน์ของชาติอื่น ผู้กระทำผิดจะมีโทษปรับหรือจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ และในกรณีที่เป็นการกระทำผิดซ้ำจะมีโทษจำคุกไม่เกิน 20 ปี

(2) เข้าสู่ระบบคอมพิวเตอร์โดยรู้ว่าไม่มีอำนาจ และได้ไปซึ่งข้อมูลทางการเงินหรือข้อมูลของสถาบันการเงิน ผู้กระทำผิดจะมีโทษปรับหรือจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ และในกรณีที่เป็นการกระทำผิดซ้ำจะมีโทษจำคุกไม่เกิน 10 ปี

(3) เข้าสู่ระบบคอมพิวเตอร์ของรัฐบาลโดยรู้ว่าไม่มีอำนาจ และปลอมแปลงหรือแสร้งว่าเป็นเจ้าหน้าที่ของรัฐเพื่อเปิดระบบประมวลผล ผู้กระทำผิดจะมีโทษปรับหรือจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ และในกรณีที่เป็นการกระทำผิดซ้ำจะมีโทษจำคุกไม่เกิน 10 ปี

---

[7] เลอสรร ธนสุกาญจน์และคณะ. (2541). **กฎหมายสำหรับบริการอินเตอร์เน็ตในประเทศไทย กรอบ ข้อเสนอแนะ และการควบคุมดูแล การให้บริการ**. หน้า 154.

(4) เข้าสู่ระบบคอมพิวเตอร์ของรัฐบาลโดยรู้ว่าไม่มีอำนาจ เพื่อผลประโยชน์ใดๆ ด้วยเจตนาฉ้อโกงหรือได้ไปซึ่งสิ่งมีค่าใดๆ ผู้กระทำผิดจะมีโทษปรับหรือจำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับ และในกรณีที่เป็นการกระทำผิดซ้ำจะมีโทษจำคุกไม่เกิน 10 ปี

(5) เข้าสู่ระบบคอมพิวเตอร์ของรัฐบาลโดยรู้ว่าไม่มีอำนาจ และได้แก้ไขเปลี่ยนแปลงหรือทำลายข้อมูลที่ได้เข้าถึงนั้นเพื่อผลประโยชน์ใดๆ ผู้กระทำผิดจะมีโทษปรับหรือจำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับ และในกรณีที่เป็นการกระทำผิดซ้ำจะมีโทษจำคุกไม่เกิน 10 ปี

(6) รู้และใช้รหัสผ่านโดยปราศจากอำนาจเพื่อเข้าถึงข้อมูลในคอมพิวเตอร์ของรัฐบาลเพื่อการค้าระหว่างรัฐหรือการค้าระหว่างประเทศ ผู้กระทำผิดจะมีโทษปรับหรือจำคุกไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ และในกรณีที่เป็นการกระทำผิดซ้ำจะมีโทษจำคุกไม่เกิน 10 ปี

นอกจากความผิดข้างต้นแล้ว การเข้าถึงข้อมูลในคอมพิวเตอร์โดยปราศจากอำนาจสหรัฐอเมริกาถือเป็นการกระทำที่มิชอบเกี่ยวข้องกับกฎหมายอื่นๆอีก ดังนี้

(1) ประมวลกฎหมายอาญาสหรัฐอเมริกา เนื่องจากการเข้าถึงข้อมูลในคอมพิวเตอร์ถือเป็นการลักขโมยบริการ (Theft of Service) เพราะเป็นการใช้บริการโดยไม่มีอำนาจ แม้ในบางครั้งจะไม่ก่อให้เกิดความเสียหายก็ตาม แต่กฎหมายก็ถือว่ามีความผิด โดยถือว่าเป็นความเสี่ยงต่อการก่อให้เกิดความเสียหายต่อสารสนเทศได้และผู้กระทำย่อมรู้ตัวดี และความเสียหายจะเกิดขึ้นในอนาคต[8] เพราะว่าในการเข้าถึงโดยปราศจากอำนาจ อาจทำให้เจ้าของที่แท้จริงไม่สามารถเข้าสู่ระบบได้ จึงมีการบัญญัติกฎหมายนี้ขึ้นเพื่อคุ้มครองผู้เช่าหรือผู้มีอำนาจใช้สายสื่อสารที่ต่อเชื่อมกับระบบคอมพิวเตอร์ และกรณีของพนักงานของบริษัทที่ใช้คอมพิวเตอร์ทำงานส่วนตัวหรือคัดลอกทำสำเนาข้อมูลโดยไม่ได้รับความยินยอมจากนายจ้าง ที่เรียกว่า “การทำงานกลางคืน” (Moonlight) ก็เป็นการกระทำที่ปราศจากอำนาจ ถือเป็นการลักสิ่งที่มีค่าใดๆ (Thing of Value) อันเป็นความผิดฐานลักทรัพย์ และการกระทำดังกล่าวยังเข้าลักษณะความผิดฐานปลอมแปลงเอกสารและความผิดฐานทำให้เสียทรัพย์ตามประมวลกฎหมายอาญาด้วย ซึ่งจะเห็นได้ว่ามีกฎหมายมากกว่า40 มาตราในบรรพที่ 8 ประมวลกฎหมายอาญาสหรัฐอเมริกาที่บัญญัติถึงการใช้เครื่องคอมพิวเตอร์ในการกระทำความผิดไม่ว่าโดยตรงหรือโดยอ้อม

(2) กฎหมายการสื่อสารทางอิเล็กทรอนิกส์ส่วนบุคคล (The Electronic Communication Privacy Act of 1986) กฎหมายฉบับนี้เป็นกฎหมายที่รับประกันการสื่อสารระหว่างบุคคลที่ผ่านทางโทรศัพท์ในระบบต่างๆ คลื่นวิทยุ การสื่อสารผ่านดาวเทียม และการสื่อสารผ่านทางเครือข่าย

---

[8] สุเนติ คงเทพ . (2541). **เอกสารประกอบการสัมมนาแนวทางในการแก้ปัญหากฎหมายอาชญากรรมยุคไอที เรื่องการไม่มีอำนาจเข้าสู่ระบบประมวลผล**. หน้า 16.

คอมพิวเตอร์ ไปรษณีย์อิเล็กทรอนิกส์ สาระสำคัญของกฎหมายฉบับนี้ คือ คำนิยามและข้อยกเว้น การจำกัดการสื่อสารของภาคเอกชน การเก็บรักษาและการใช้ข้อมูลจากการสื่อสาร การรับจดทะเบียน ฯลฯ

(3) กฎหมายการฉ้อโกงบัตรเครดิต (The Credit Card Fraud Act of 1984) เป็นกฎหมายที่ออกมาเพื่อควบคุมการฉ้อโกงบัตรเครดิตและการปลอมบัตรเครดิต แต่คำนิยามของคำว่า "บัตรเครดิต" ในกฎหมายฉบับนี้ได้ครอบคลุมไปถึงการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ด้วย เช่น การกระทำความผิดที่เข้าถึงสื่อทางคอมพิวเตอร์ หมายความรวมถึงบัตรต่างๆ แผ่นพลาสติก รหัส หมายเลขบัญชี หรือสิ่งอื่นๆของบัญชี และการเข้าถึงให้หมายความถึงการเข้าถึงทางด้านบัญชีและการเข้าถึงสื่อทางคอมพิวเตอร์ อันถือเป็นการกระทำที่ได้ไปซึ่งผลประโยชน์ในด้านต่างๆ ส่วนที่กล่าวถึงการกระทำความผิดเกี่ยวกับเครื่องคอมพิวเตอร์นั้น เป็นการกระทำความผิดฐานฉ้อโกงการทำ ใช้ จำหน่าย ปลอมสื่อทางคอมพิวเตอร์ หรือการเข้าถึงโดยปราศจากอำนาจ ลักษณะของการกระทำความผิดตามกฎหมายฉบับนี้ที่เกิดขึ้นในปัจจุบัน ได้แก่ การลักลอบเข้าสู่ระบบคอมพิวเตอร์เพื่อค้นหา ทดสอบ หรือการแก้ไขเปลี่ยนแปลงข้อมูลต่างๆ เช่น หมายเลขโทรศัพท์ หมายเลขบัญชีธนาคาร หรือรหัสผ่าน

(4) กฎหมายลิขสิทธิ์ (The Copyright Act of 1976) กรณีที่มีการเข้าถึงข้อมูลในเครื่องคอมพิวเตอร์โดยปราศจากอำนาจในลักษณะที่เป็นการลักขโมยโปรแกรมหรือข้อมูลในคอมพิวเตอร์นั้น ถือเป็นการละเมิดลิขสิทธิ์ที่มีโทษทางอาญา ตามรายงานของคณะกรรมาธิการรัฐสภาเกี่ยวกับกฎหมายลิขสิทธิ์ ค.ศ. 1976 หน้า 54 ระบุว่า "งานวรรณกรรม" (Literary Works) ให้รวมถึงฐานข้อมูลทางคอมพิวเตอร์และโปรแกรมคอมพิวเตอร์ รวมถึงงานประพันธ์ที่เป็นการแสดงออกถึงความคิดดั้งเดิมของนักเขียนโปรแกรม จึงเป็นสิทธิของผู้เขียนโปรแกรมที่จะปกป้องเอกสารและลายเส้นของรหัสคอมพิวเตอร์จากการคัดลอกหรือทำสำเนา แต่การคุ้มครองดังกล่าวก็มิได้ครอบคลุมถึง "ขั้นตอนวิธี" (Algorithms) ของผู้เขียนโปรแกรมด้วย การกระทำความผิดตามกฎหมายฉบับนี้มีโทษทั้งทางแพ่งและในทางอาญา

(5) กฎหมายการฉ้อโกงทางสายโทรศัพท์ (The Wire Fraud Act) เดิมประมวลกฎหมายสหรัฐอเมริกา มีการยกเว้นการกระทำความผิดทางสายสื่อสารสาธารณะ แต่เมื่อมีการใช้คอมพิวเตอร์จากเครือข่ายทางไกลกระทำการฉ้อโกงทางคอมพิวเตอร์ขึ้นเป็นจำนวนมาก ทั้งเป็นการกระทำความผิดของบุคคลเพียงคนเดียวและหลายคนร่วมมือกัน และผู้ที่กระทำความผิดก็ได้ผลประโยชน์ไปเป็นจำนวนมาก รัฐจึงมีมาตรการออกมาเพื่อปกป้องคุ้มครองการส่งข้อมูลผ่านทางสายสื่อสารสาธารณะดังกล่าว

(6) กฎหมายเกี่ยวกับระเบียบสถาบันทางการเงินและการควบคุมอัตราดอกเบี้ย (The Financial Institutions Regulatory and Interest rate Control Act of 1978 : FIRA) ในส่วนที่เป็นเรื่องการโอนเงินทางอิเล็กทรอนิกส์ (The Electronic Fund Transfer Act) ซึ่งมีการกำหนดคำนิยามและสิทธิส่วนบุคคลของผู้บริโภคที่ได้รับผลกระทบจากการโอนเงินทางอิเล็กทรอนิกส์ โดยกฎหมายฉบับนี้ได้กำหนดให้รัฐบาลกลางออกระเบียบการโอนเงินทางอิเล็กทรอนิกส์ขึ้น

(7) กฎหมายคุ้มครองส่วนบุคคล (The Privacy Act of 1974) กรณีที่เป็นการเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจที่จะกระทำได้ โดยกระทำผ่านฐานข้อมูลในเครื่องคอมพิวเตอร์ เป็นการให้ความคุ้มครองความเป็นส่วนตัวของบุคคล ดังนั้นการเข้าถึงข้อมูลในเครื่องคอมพิวเตอร์โดยปราศจากอำนาจจึงอาจมีความผิดตามกฎหมายฉบับนี้ด้วย

3.1.2.2 ความผิดฐานแก้ไขเปลี่ยนแปลง (Alteration) ความผิดฐานแก้ไขเปลี่ยนแปลงข้อมูลตาม The Computer Fraud and Abuse Act 1986 ครอบคลุมถึงการแก้ไขเปลี่ยนแปลงเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ เครือข่ายคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ และข้อมูลที่ถูกจัดเก็บอยู่ในคอมพิวเตอร์ เหตุที่นำความผิดดังกล่าวมาบัญญัติเอาไว้ต่างหาก เนื่องมาจากการกระทำความผิดดังกล่าวมีลักษณะคล้ายกับความผิดฐานปลอมแปลงเอกสาร แต่เมื่อมีการกระทำความผิดเกิดขึ้นกลับไม่สามารถนำบทบัญญัติของกฎหมายในความผิดฐานปลอมแปลงเอกสารมาใช้บังคับได้ เพราะประสบปัญหาการตีความ โดยเฉพาะเรื่องขององค์ประกอบของความผิด ฝ่ายนิติบัญญัติของรัฐบาลกลางและมลรัฐต่างๆ จึงจำเป็นที่จะต้องบัญญัติกฎหมายขึ้นมาใช้บังคับกับความผิดดังกล่าวโดยเฉพาะ

การกระทำที่เป็นการแก้ไขเปลี่ยนแปลงโปรแกรมคอมพิวเตอร์หรือการแก้ไขเปลี่ยนแปลงข้อมูลที่เก็บอยู่ในเครื่องคอมพิวเตอร์ ในส่วนที่เกี่ยวกับความผิดฐานปลอมเอกสารนั้นตีความจากคำว่า “เอกสาร” ที่หมายความรวมถึงโปรแกรมคอมพิวเตอร์และข้อมูลที่เก็บอยู่ในเครื่องคอมพิวเตอร์

3.1.2.3 ความผิดฐานทำให้เสียหายหรือทำลาย (Damage or Destruction) ความผิดฐานทำให้เสียหายหรือทำลายทางคอมพิวเตอร์ตาม The Computer Fraud and Abuse Act 1986 นั้น เป็นการกระทำที่ทำให้เกิดความเสียหายหรือทำลายโปรแกรมคอมพิวเตอร์หรือข้อมูลที่ถูกจัดเก็บอยู่ในเครื่องคอมพิวเตอร์และการกระทำให้เกิดความเสียหายโดยตรงต่อเครื่องคอมพิวเตอร์รวมทั้งอุปกรณ์ต่างๆของเครื่องคอมพิวเตอร์ที่เรียกว่าฮาร์ดแวร์ (Hardware) ด้วย โดยบัญญัติแยกต่างหากจากความผิดฐานทำให้เสียทรัพย์ตามประมวลกฎหมายอาญา เนื่องจากเห็นว่าเป็นการกระทำความผิดที่ก่อให้เกิดความเสียหายที่ร้ายแรง และก่อให้เกิดความเสียหายต่อเทคโนโลยี

3.1.3 สาเหตุ วิธีการ และระยะเวลาในการเข้าถึงข้อมูลอิเล็กทรอนิกส์ การค้นข้อมูลอิเล็กทรอนิกส์เป็นการค้นที่แตกต่างจากการค้นที่มีอยู่แต่เดิม ซึ่งเมื่อพนักงานสอบสวนเห็นสมควรจะค้นจะต้องมีหมายค้น โดยจะต้องบรรยายสถานที่ที่จะทำการค้นในหมายนั้นด้วย แต่สำหรับการค้นพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์จะต้องทำการค้นหาจากฮาร์ดแวร์หรือฮาร์ดดิสก์

ในการปฏิบัติหน้าที่ของพนักงานสอบสวนของสหรัฐอเมริกาจะต้องเป็นการค้นหาพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์โดยไม่ขัดต่อหลักการไม่รับฟังพยานหลักฐาน ซึ่งได้มาโดยการค้นที่มิชอบ (Exclusionary Rule) ตามรัฐธรรมนูญสหรัฐอเมริกาแก้ไขเพิ่มเติมฉบับที่ 4 (The Fourth Amendment) บัญญัติว่า “สิทธิของบุคคลที่จะมีความปลอดภัยมั่นคงในร่างกาย เคหสถาน เอกสารและวัตถุสิ่งของ ต่อการค้น การยึด และการจับที่ไม่มีเหตุอันสมควร จะถูกล่วงละเมิดมิได้ และห้ามมิให้มีการออกหมาย เว้นแต่จะโดยมีเหตุอันควร ซึ่งได้มาโดยการสาบาน หรือปฏิญาณตน และหมายนั้นจะต้องระบุเฉพาะเจาะจงถึงสถานที่ที่จะถูกค้น ตัวบุคคลที่จะถูกจับ และสิ่งของที่ถูกยึด”

นอกจากนี้กฎว่าด้วยวิธีพิจารณาความอาญาของสหรัฐได้รับรองหลักของรัฐธรรมนูญแก้ไขเพิ่มเติมฉบับที่นี้ไว้ในมาตรา 41 (a) ซึ่งบัญญัติว่า “เจ้าพนักงานผู้มีอำนาจหรือพนักงานอัยการต้องขอหมายค้น…

(1) หมายค้นต้องออกโดยศาล Magistrate ของมลรัฐ หรือศาลของสหรัฐ สำหรับการค้นสิ่งของหรือค้นหาบุคคลในเขตอำนาจศาล

(2) หมายค้นออกโดยศาล Magistrate สำหรับกรณีการค้นสิ่งของหรือค้นหาบุคคลในเขตอำนาจศาลหรือค้นสิ่งของที่ถูกโยกย้ายหรือบุคคลหลบหนีออกนอกเขตก่อนจะถูกดำเนินการตามกฎหมาย”

จากกฎหมายดังกล่าวจะเห็นได้ว่าเจ้าหน้าที่ของรัฐจะทำการค้นได้ก็ต่อเมื่อมีหมายค้น และหมายค้นดังกล่าวจะต้องออกโดยผู้พิพากษา แม้ในกรณีของการค้นข้อมูลอิเล็กทรอนิกส์ ซึ่งเป็นพยานหลักฐานที่มีลักษณะพิเศษ ที่อาจถูกแก้ไขเปลี่ยนแปลงได้ง่าย เจ้าพนักงานของรัฐก็จะต้องทำการค้นโดยมีหมาย เพราะต้องการจะให้กระบวนการในการออกหมายเป็นมาตรการในการตรวจสอบการใช้ดุลพินิจของเจ้าหน้าที่ (Warrant Process) เพื่อให้เจ้าหน้าที่ปฏิบัติหน้าที่โดยไม่ขัดกับรัฐธรรมนูญแก้ไขเพิ่มเติมฉบับที่ 4

ในกรณีที่เจ้าหน้าที่ไม่จำเป็นที่จะต้องเข้าไปค้นในเคหสถานหรือสำนักงานของผู้อื่น แต่สามารถทำการค้นโดยการใช้เครื่องคอมพิวเตอร์หรือเครื่องมืออื่นใดเชื่อมต่อเข้ากับระบบ LAN หรือ WAN ของเคหสถาน หรือสำนักงาน ตลอดจนเครือข่ายอินเตอร์เน็ต โดยไม่มีการบุกรุกเข้าไปทางกายภาพ หากพิจารณาถึงสิทธิที่ได้รับการรับรองคุ้มครองตามรัฐธรรมนูญแก้ไขเพิ่มเติมฉบับที่

4 ซึ่งรวมไปถึงสิทธิส่วนบุคคลด้วย การค้นข้อมูลอิเล็กทรอนิกส์ในลักษณะนี้ ก็ถือเป็นการบุกรุกเช่นกัน

3.1.4 การรับฟังเป็นพยานหลักฐานในศาล ภายหลังที่กฎหมายอาชญากรรมคอมพิวเตอร์ในสหรัฐอเมริกาใช้บังคับแล้วยังมีปัญหาที่ตามมาอีกหลายประการ เช่น ปัญหาในการให้คำนิยามคำว่า “อาชญากรรมคอมพิวเตอร์” (Computer crime) การจำกัดการให้ความคุ้มครองที่จำกัดเฉพาะงานของรัฐไม่รวมภาคเอกชน การขาดความชัดเจนในเรื่องของเขตอำนาจศาล และปัญหาเกี่ยวกับวิธีพิจารณาความ เช่น การแสวงหาพยานหลักฐาน และการรับฟังเป็นพยานหลักฐานในศาล ทำให้ไม่สามารถนำผู้กระทำผิดมาลงโทษได้

ศาลของสหรัฐอเมริกาจะไม่รับฟังพยานหลักฐานที่เกิดจากการค้นโดยมิชอบ ดังนั้นในการค้นพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ก็จะต้องเป็นการค้นที่ไม่ขัดต่อหลักการห้ามรับฟังพยานหลักฐานซึ่งได้มาโดยมิชอบ (Exclusionary Rule) ดังนั้นหากเจ้าหน้าที่แสวงหาพยานหลักฐานจากข้อมูลอิเล็กทรอนิกส์โดยวิธีการที่มิชอบด้วยกฎหมาย เป็นการล่วงล้ำสิทธิส่วนบุคคล พยานหลักฐานดังกล่าวก็จะถูกตัดออกจากกระบวนการพิจารณาของศาลทันที โดยศาลจะไม่รับฟัง ทำให้ไม่สามารถนำตัวผู้กระทำผิดมาลงโทษได้

3.2 ประเทศอังกฤษ

ก่อนที่จะมีกฎหมายอาญาว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือการรักษาความปลอดภัยของข้อมูลในคอมพิวเตอร์นั้น การเข้าถึงข้อมูลที่ถูกจัดเก็บอยู่ในเครื่องคอมพิวเตอร์ในประเทศอังกฤษโดยปราศจากอำนาจไม่ถือเป็นความผิดอาญา โดยพิจารณาเปรียบเทียบจากความผิดฐานบุกรุก (Trespass) ความผิดเกี่ยวกับทรัพย์ (Theft) ที่ผู้กระทำผิดรับผิดแต่เพียงในทางแพ่ง [9] ต่อมาจึงได้บัญญัติ The Computer Misuse Act 1990 เป็นกฎหมายอาญาว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ขึ้นเป็นฉบับแรก ทั้งได้วางมาตรการในการรักษาความปลอดภัยของข้อมูลเอาไว้ด้วย

3.2.1 มาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลของประเทศอังกฤษ วัฒนธรรมของประเทศอังกฤษนั้นให้ความเคารพต่อสิทธิส่วนบุคคล โดยมีคดีตัวอย่างเกี่ยวกับนายจ้างและลูกจ้างที่ศาลตัดสินว่านายจ้างไม่อาจเปิดเผยข้อมูลส่วนบุคคลของลูกจ้าง ไม่ว่าข้อมูลนั้นจะเก็บไว้

---

[9] เฉลิมพล ช่อโพธิ์ทอง. (2535). **ความผิดฐานลักทรัพย์และฉ้อโกง : ศึกษาเปรียบเทียบกฎหมายอังกฤษ เยอรมัน และไทย**. หน้า 73.

ในระบบธรรมดาหรือเก็บไว้ในคอมพิวเตอร์ก็ตาม[10] ต่อมารัฐบาลอังกฤษได้พิจารณาถึงข้อมูลส่วนบุคคลที่ถูกจัดเก็บอยู่ในเครื่องคอมพิวเตอร์ว่าควรจะมีกฎหมายคุ้มครอง เพราะจำเป็นต้องดำเนินการให้กฎหมายภายในของอังกฤษสอดคล้องกับอนุสัญญาแห่งสภายุโรปว่าด้วยการให้ความคุ้มครองข้อมูล (The Council of Europe's Data Protection) รัฐสภาของประเทศอังกฤษได้ออกพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (The Data Protection Act 1984 แก้ไขเพิ่มเติม ค.ศ. 1998) เพราะในการแสวงหาพยานหลักฐานของเจ้าพนักงานของรัฐ โดยล่วงล้ำเข้าไปรับรู้ถึงข้อมูลที่เกี่ยวกับการดำเนินชีวิตของผู้ต้องสงสัยหรือสารสนเทศที่อยู่ในความครอบครองของผู้ใช้ และการแสดงความคิดเห็นส่วนตัว เท่ากับเป็นการล่วงล้ำข้อมูลส่วนบุคคลที่กฎหมายอังกฤษประสงค์จะให้ปกปิด ดังเช่นคดีระหว่างนายจ้างและลูกจ้างข้างต้น การรวบรวมพยานหลักฐานด้วยวิธีการดังกล่าวอาจถูกหาว่าเป็นพยานหลักฐานที่ได้มาโดยมิชอบได้

3.2.2 การกำหนดความผิดเพื่อคุ้มครองสิทธิส่วนบุคคลที่เป็นข้อมูลอิเล็กทรอนิกส์ กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของอังกฤษ คือ The Data Protection Act 1998 และมีมาตรการควบคุม และตรวจสอบการทำงานของเจ้าหน้าที่โดยองค์กรภายนอกไว้อย่างรัดกุม และไม่ทำให้ประสิทธิภาพในการปราบปรามอาชญากรรมของเจ้าหน้าที่ลดลง โดยการให้ดุลพินิจในการปฏิบัติหน้าที่ของเจ้าหน้าที่ ภายใต้กฎเกณฑ์ที่กฎหมายบัญญัติไว้ใน The Police and Criminal Evidence Act 1984

กฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์ของอังกฤษ คือ The Computer Misuse Act 1990 ที่กำหนดความผิดไว้ 3 รูปแบบ ได้แก่

3.2.2.1 ความผิดเนื่องจากปราศจากอำนาจในการเข้าสู่ระบบ (Basic Hacking Offence หรือ Unauthorized Access)

3.2.2.2 ความผิดเกี่ยวกับการให้ความสะดวกแก่ผู้กระทำความผิดในการก่อให้เกิดความผิดร้ายแรง (Ulterial Hacking Offence หรือ Unauthorized Access with Intent to Commit or Facilitate Commission of Further Offences) และ

3.2.2.3 ความผิดเกี่ยวกับการทำลายแก้ไขเปลี่ยนแปลงข้อมูลโดยปราศจากอำนาจ (Modification of Computer Material หรือ Unauthorized Modification)

---

[10] Edward Wilding. (1997). **Computer Evidence : A Forensic Investigations Handbook**. London : Sweet & Maxwell Ltd. p.93.

3.2.2.1 ความผิดเนื่องจากปราศจากอำนาจในการเข้าสู่ระบบ (Basic Hacking Offence หรือ Unauthorized Access) ความผิดเนื่องจากปราศจากอำนาจในการเข้าสู่ระบบ บัญญัติอยู่ใน The Computer Misuse Act 1990 มาตรา 1 บัญญัติว่า

(1) บุคคลจะมีความผิดเมื่อ

(a) บุคคลได้กระทำการให้คอมพิวเตอร์แสดงผล หรือแสดงการทำงานใดๆ ด้วยเจตนาที่จะผ่านสิ่งป้องกันที่มีไว้เพื่อกันการเข้าถึงระบบ และได้ทำการผ่านสิ่งป้องกันเช่นว่านั้นเข้าถึงโปรแกรมคอมพิวเตอร์ใดๆ หรือสารสนเทศที่เก็บไว้ในคอมพิวเตอร์ใดๆ

(b) การผ่านสิ่งป้องกันเข้าไปยังระบบนั้น เป็นการกระทำโดยปราศจากอำนาจ

(c) บุคคลนั้นได้รู้ขณะที่กระทำอยู่แล้วว่า การกระทำอันเป็นเหตุให้คอมพิวเตอร์แสดงผลหรือแสดงการกระทำนั้นปราศจากอำนาจ

(2) เจตนาของบุคคลที่ได้กระทำความผิดภายใต้มาตรานี้ ไม่จำเป็นต้องเป็นการกระทำที่เป็น

(a) โปรแกรมพิเศษเฉพาะเจาะจงใดๆ หรือข้อมูล

(b) โปรแกรมหรือข้อมูลของสิ่งเฉพาะเจาะจงใดๆ หรือ

(c) โปรแกรมหรือข้อมูลที่ถูกเก็บไว้ในคอมพิวเตอร์อย่างเฉพาะเจาะจงใดๆ

(3) บุคคลที่มีความผิดภายใต้บทบัญญัตินี้ จะต้องถูกพิจารณาคดีแบบรวดรัดและต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกินระดับ 5 ตามตารางมาตรฐานหรือทั้งจำทั้งปรับ

จากบทบัญญัติข้างต้นเป็นบทบัญญัติที่ไม่มีความซับซ้อน แสดงถึงการเข้าถึงข้อมูลโดยปราศจากอำนาจ แต่จะเป็นการกระทำที่มีความผิดตามมาตรานี้จะต้องเป็นการทำให้เครื่องคอมพิวเตอร์แสดงผลหรือแสดงการทำงานใดๆ รวมทั้งการสั่งให้เครื่องคอมพิวเตอร์แสดงการทำงานโดยระยะทางไกล (Remote) โดยไม่คำนึงถึงผลของการกระทำ ซึ่งรวมถึงการพยายามกระทำความผิดด้วย แต่ไม่รวมถึงการทำงานทางกายภาพที่กระทำต่อเครื่องหรืออุปกรณ์คอมพิวเตอร์

หากพิจารณาความรับผิดทางอาญาในระบบคอมมอนลอว์ สำหรับความผิดฐานเข้าถึงโดยปราศจากอำนาจ สามารถแยกพิจารณาได้เป็น 2 ส่วน ได้แก่

ก. ส่วนของการกระทำ (Actus Reus) คือการที่ผู้ใดกระทำการอย่างหนึ่งอย่างใดเป็นเหตุให้คอมพิวเตอร์แสดงผลหรือแสดงการทำงานใดๆ และผู้กระทำต้องรับผิดแม้จะไม่สำเร็จ ทั้งนี้ไม่รวมถึงการกระทำที่เพียงแต่สัมผัสทางกายกับอุปกรณ์หรือเครื่องคอมพิวเตอร์โดยไม่มีการกระทำใดๆต่อเครื่องคอมพิวเตอร์ และการดูข้อมูลที่ปรากฏบนจอภาพ การดักข้อมูล หรือการดักฟังข้อมูล

ข. ภายในจิตใจหรือเจตนาร้าย (Mens Rea) แยกพิจารณาได้ดังนี้

(1) เจตนาที่จะผ่านสิ่งป้องกันที่มีเพื่อเข้าสู่ระบบ เพื่อเข้าสู่ข้อมูลที่เก็บอยู่ในเครื่องคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ใดๆก็เป็นความผิดแล้ว ไม่จำเป็นจะต้องเป็นเจตนาโดยตรงต่อโปรแกรมหรือข้อมูลใดๆ ตามที่บัญญัติใน (2) แสดงให้เห็นว่าเจตนาของผู้กระทำไม่จำเป็นจะต้องเป็นเจตนาโดยตรงต่อโปรแกรมพิเศษเฉพาะเจาะจงใดๆ หรือข้อมูล โปรแกรมหรือข้อมูลของสิ่งเฉพาะเจาะจงใดๆ หรือโปรแกรมหรือข้อมูลที่ถูกเก็บไว้ในคอมพิวเตอร์อย่างเฉพาะเจาะจงใดๆ ดังนั้น การกระทำโดยประมาทก็อาจมีความผิดตามมาตรานี้ได้

(2) เจตนาภายใน คือผู้กระทำต้องรู้ในขณะที่กระทำว่าตนไม่มีอำนาจที่จะกระทำได้เป็นการทำให้เครื่องคอมพิวเตอร์แสดงผลหรือแสดงการทำงานใดๆโดยปราศจากอำนาจ

ดังนั้นในการฟ้องร้องผู้กระทำความผิด โจทก์จะต้องพิสูจน์ให้ศาลเห็นว่าจำเลยมีเจตนาเข้าสู่ระบบและจำเลยรู้ว่าการกระทำของตนเป็นการทำให้คอมพิวเตอร์แสดงผลหรือแสดงการทำงานใดๆ และเป็นการกระทำโดยปราศจากอำนาจ การพิสูจน์องค์ประกอบภายในทั้ง 2 ประการข้างต้นนี้ถือเป็นหลักในการพิสูจน์ความผิดของผู้กระทำความผิดตามหลักพื้นฐานของคอมมอนลอว์

3.2.2.2 ความผิดเกี่ยวกับการให้ความสะดวกแก่ผู้กระทำความผิดในการก่อให้เกิดความผิดร้ายแรง (Ulterial Hacking Offence หรือ Unauthorized Access with Intent to Commit or Facilitate Commission of Further Offences) ความผิดเกี่ยวกับการให้ความสะดวกแก่ผู้กระทำความผิดในการก่อให้เกิดความผิดร้ายแรง บัญญัติอยู่ใน The Computer Misuse Act 1990 มาตรา 2 บัญญัติว่า

(1) บุคคลจะมีความผิดภายใต้บทบัญญัตินี้ ถ้าหากว่าเขาได้กระทำความผิดตามมาตรา 1 ข้างต้นโดยมีเจตนา

(a) กระทำความผิดในสิ่งที่มาตรานี้ใช้บังคับ หรือ

(b) ให้ความสะดวกในการกระทำความผิดไม่ว่าจะเป็นการกระทำความผิดของตนเองหรือของผู้อื่น และความผิดที่เขาเจตนากระทำหรือให้ความสะดวกดังจะกล่าวต่อไปในมาตรานี้ให้ถือว่าเป็นผู้กระทำความผิดเช่นเดียวกับผู้ที่กระทำความผิดที่ตนช่วยเหลือ

(2) มาตรานี้ใช้กับความผิด

(a) ความผิดที่บัญญัติไว้ในกฎหมายหรือ

(b) ใช้กับบุคคลที่มีอายุตั้งแต่ 21 ปีขึ้นไป

(3) ภายใต้บทบัญญัติของมาตรานี้ ไม่ว่าการกระทำความผิดของผู้กระทำที่อยู่ระยะไกล (Remote) จะได้กระทำไปในโอกาสที่ปราศจากอำนาจเข้าสู่ระบบหรือไม่ หรือโดยอาศัยโอกาสอื่นใดก็ตาม

(4) บุคคลอาจจะมีความผิดตามมาตรานี้ แม้จะปรากฏข้อเท็จจริงว่าการกระทำความผิดของผู้กระทำที่อยู่ระยะไกลจะไม่ได้กระทำลงก็ตาม

(5) บุคคลผู้กระทำความผิดตามมาตรานี้จะต้อง

(a) ถูกพิจารณาอย่างรวดเร็วและต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกินระดับ 5 ตามตารางมาตรฐานหรือทั้งจำทั้งปรับ

(b) หากเป็นความผิดร้ายแรงต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกินระดับ 5 ตามตารางมาตรฐานหรือทั้งจำทั้งปรับ

จากบทบัญญัติดังกล่าวข้างต้นจะเห็นได้ว่าความผิดฐานนี้เป็นความผิดที่มีความซับซ้อนกว่าและร้ายแรงกว่าความผิดฐานเข้าถึงโดยปราศจากอำนาจ จึงไม่นำมาบัญญัติเอาไว้ต่างหาก เพราะการกระทำความผิดในมาตรานี้จะต้องเป็นการกระทำโดยเจตนาที่จะกระทำความผิดและปราศจากอำนาจที่จะกระทำ หรือเป็นการกระทำเพื่อให้ความสะดวกแก่ผู้กระทำความผิดเพื่อที่จะกระทำความผิดที่ร้ายแรง ข้อแตกต่างระหว่างมาตรา 1 กับมาตรา 2 นี้จึงอยู่ที่การพิสูจน์เจตนาในอนาคต นั่นคือการกระทำความผิดตามมาตรา 1 เป็นการกระทำที่ไม่อาจพิสูจน์เจตนาในอนาคตได้ ซึ่งจะมีโทษเบากว่า โดยถือว่าเป็นความผิดที่เรียกว่า “ความผิดที่ไกลออกไป” (Further Offence) หมายถึงความผิดที่ไม่จำเป็นต้องพิสูจน์ถึงเจตนาของผู้กระทำความผิดว่าได้เกิดขึ้นหรือไม่ แต่ถ้าเป็นกรณีที่สามารถพิสูจน์เจตนาในอนาคตได้ก็จะเป็นการกระทำความผิดตามมาตรา 2 ที่จะมีบทลงโทษผู้กระทำความผิดที่คิดจะกระทำความผิดในอนาคต และถ้าหากไม่สามารถลงโทษผู้กระผิดตามมาตรา 2 นี้ได้ก็สามารถลงโทษได้ตามมาตรา 1 ความผิดที่เกิดขึ้นในลักษณะนี้ ได้แก่ ความผิดฐานฉ้อโกง ความผิดฐานลักทรัพย์ และความผิดฐานยักยอกทรัพย์

การพิจารณาความรับผิดทางอาญาในทางคอมมอนลอว์ สำหรับความผิดฐานนี้สามารถแยกพิจารณาได้ ดังนี้

ก. การกระทำ (Actus Reus) โจทก์ต้องพิสูจน์ให้ได้ว่าจำเลยได้เข้าถึงสาระสำคัญ ได้แก่ โปรแกรมคอมพิวเตอร์หรือข้อมูลในคอมพิวเตอร์ และ

ข. ภายในจิตใจหรือเจตนาร้าย (Mens Rea) ผู้กระทำมีเจตนาที่จะกระทำความผิดอื่นโดยไม่คำนึงถึงเวลาของการกระทำความผิดอื่นว่าจะกระทำในเวลาใด ไม่ว่าจะเป็นขณะที่เกือบจะเป็นเวลาเดียวกับที่เข้าถึงโดยปราศจากอำนาจ หรือในโอกาสต่อมา นั่นคือหากผู้กระทำความผิดเพียงแต่ได้ข้อเท็จจริงมาโดยตั้งใจที่จะกระทำการเข้าถึงโดยปราศจากอำนาจ แต่ยังไม่ลงมือกระทำก็ถือว่ามีความผิดตาม (4) แล้ว

3.2.2.3 ความผิดเกี่ยวกับการทำลายแก้ไขเปลี่ยนแปลงข้อมูลโดยปราศจากอำนาจ (Modification of Computer Material หรือ Unauthorized Modification) ความผิดเกี่ยวกับการ

ทำลายแก้ไขเปลี่ยนแปลงข้อมูลโดยปราศจากอำนาจ บัญญัติอยู่ใน The Computer Misuse Act 1990 มาตรา 3 บัญญัติว่า

(1) บุคคลจะมีความผิดถ้า

(a) ผู้นั้นได้กระทำการใดๆ ซึ่งก่อให้เกิดการแก้ไขเปลี่ยนแปลงในเนื้อหาสาระของคอมพิวเตอร์ใดๆ และ

(b) ผู้ที่กระทำการเช่นว่านั้น จะต้องมีเจตนาหรือจะต้องรู้ถึงการกระทำของตนในขณะที่กระทำการนั้น

(2) ภายใต้บทบัญญัติของอนุมาตรา (1) (b) เจตนานั้นจะต้องเป็นเจตนาที่ต้องการแก้ไขเปลี่ยนแปลงเนื้อหาสาระของคอมพิวเตอร์ใดๆ โดยการกระทำ เช่น

(a) ทำให้เกิดความเสียหายต่อการทำงานของเครื่องคอมพิวเตอร์

(b) ขัดขวางหรือทำการกีดกันการเข้าถึงโปรแกรมคอมพิวเตอร์ หรือข้อมูลในคอมพิวเตอร์หรือ

(c) ทำให้เกิดความเสียหายต่อการทำงานของโปรแกรมคอมพิวเตอร์ หรือทำลายความเชื่อถือของข้อมูล

(3) เจตนาของการกระทำดังกล่าว ไม่จำต้องเป็นเจตนาโดยตรงต่อ

(a) คอมพิวเตอร์เฉพาะเจาะจงใดๆ

(b) โปรแกรมหรือข้อมูลพิเศษเฉพาะเจาะจงใดๆ หรือโปรแกรมหรือข้อมูลชนิดใดชนิดหนึ่งโดยเฉพาะ หรือ

(c) การแก้ไขเปลี่ยนแปลงพิเศษเฉพาะเจาะจงใดๆ หรือการแก้ไขเปลี่ยนแปลงชนิดใดชนิดหนึ่งโดยเฉพาะ

(4) ภายใต้บทบัญญัติของอนุมาตรา (1) (b) ผู้กระทำต้องรู้ว่าการแก้ไขเปลี่ยนแปลงดังกล่าว กระทำไปโดยปราศจากอำนาจ และผู้กระทำมีเจตนาเช่นนั้น

(5) มาตรานี้ไม่ถือวัตถุประสงค์เป็นสิ่งสำคัญ โดยไม่คำนึงถึงการแก้ไขเปลี่ยนแปลงโดยปราศจากอำนาจ หรือผลจากเจตนาที่จะก่อขึ้นตาม (2) ไม่ว่าจะเป็นเจตนาที่จะก่อให้เกิดขึ้นเป็นการถาวรหรือชั่วคราว

(6) การแก้ไขเปลี่ยนแปลงในเนื้อหาสาระของคอมพิวเตอร์ตามกฎหมายฉบับนี้ จะไม่ถือว่าเป็นการก่อให้เกิดความเสียหายแก่คอมพิวเตอร์ใดๆ ตามกฎหมายอาญาเกี่ยวกับการก่อให้เกิดความเสียหายเว้นแต่การกระทำนั้นมีผลทางกายภาพเท่านั้น

(7) บุคคลที่กระทำความผิดตามมาตรานี้จะต้อง

(a) ถูกพิจารณาอย่างรวดเร็วและต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกินระดับ 5 ตามตารางมาตรฐานหรือทั้งจำทั้งปรับ

(b) หากเป็นความผิดร้ายแรงต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกินระดับ 5 ตามตารางมาตรฐานหรือทั้งจำทั้งปรับ

การพิจารณาความรับผิดทางอาญาในทางคอมมอนลอว์ สำหรับความผิดฐานนี้สามารถแยกพิจารณาได้ ดังนี้

ก. การกระทำ (Actus Reus) มีการกำหนดขอบเขตของการกระทำความผิดไว้ค่อนข้างจำกัด โดยเน้นแต่เฉพาะที่เป็นการแก้ไขเปลี่ยนแปลง (Modification) ในเนื้อหาสาระ (Content) ของคอมพิวเตอร์เท่านั้น และแม้ว่าการกระทำดังกล่าวจะมีความสัมพันธ์กับการก่อให้เกิดความเสียหายทางอาญา แต่ก็ไม่ถือว่าเป็นความผิดตามกฎหมายอาญา เว้นแต่จะเป็นการกระทำความผิดที่ก่อให้เกิดความเสียหายทางกายภาพ

ข. ภายในจิตใจหรือเจตนาร้าย (Mens Rea) ผู้กระทำจะต้องมีเจตนาและรู้อยู่ในขณะที่กระทำการแก้ไขเปลี่ยนแปลง ส่วนผลของการกระทำนั้นจะก่อให้เกิดความเสียหายกับทำให้เกิดความเสียหายต่อการทำงานของเครื่องคอมพิวเตอร์ ขัดขวางหรือทำการกีดกันการเข้าถึงโปรแกรมคอมพิวเตอร์ หรือข้อมูลในคอมพิวเตอร์ ทำให้เกิดความเสียหายต่อการทำงานของโปรแกรมคอมพิวเตอร์ หรือทำลายความเชื่อถือของข้อมูลเครื่องคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ หรือข้อมูลในเครื่องคอมพิวเตอร์อย่างไรไม่จำต้องนำมาพิจารณา

3.2.3 สาเหตุ วิธีการ และระยะเวลาในการเข้าถึงข้อมูลอิเล็กทรอนิกส์ กฎหมายที่เป็นหลักเกณฑ์ในการค้นหาพยานหลักฐานของอังกฤษ คือ The Police and Criminal Evidence Act 1984 (PACE) มาตรา 1 บัญญัติว่า “การค้นเคหสถานต้องมีเหตุอันควรสงสัยตามสมควร โดยถือมาตรฐานของบุคคลในฐานะและพฤติการณ์เดียวกับผู้ค้นเป็นเกณฑ์” และการค้นจะต้องมีการออกหมายค้นจากศาล (Justice of the peace) โดยศาลจะออกหมายค้นก็ต่อเมื่อเป็นเหตุอันควรเชื่อว่าเป็นความผิดอาญาร้ายแรง (Serious arrestable offence) ดังนั้น จึงต้องพิจารณาว่าอาชญากรรมคอมพิวเตอร์จะถือเป็นความผิดอาญาร้ายแรงที่ศาลสมควรจะออกหมายค้นหรือไม่

การค้นและยึดพยานหลักฐานต่างๆ ตามกฎหมายวิธีพิจารณาความอาญาของประเทศอังกฤษต้องคำนึงถึงแนวความคิดในเรื่องการคุ้มครองสิทธิมนุษยชนในทางอาญา ซึ่งได้บัญญัติรับรองไว้ในกฎบัตรแมคนาคาร์ตา (Magna Carta, 1215) กฎหมายของประเทศอังกฤษได้วางมาตรการควบคุม และตรวจสอบการทำงานของเจ้าพนักงานตำรวจโดยองค์กรภายนอกเอาไว้ ขณะเดียวกันก็ไม่ทำให้ประสิทธิภาพในการดำเนินงานของเจ้าหน้าที่ลดลง โดยให้เจ้าหน้าที่ของรัฐ

ได้แก่ ตำรวจ อัยการ และผู้พิพากษา สามารถใช้ดุลพินิจในการบังคับใช้กฎหมายได้มากขึ้น และในขณะเดียวกันก็มีข้อบังคับที่ตราขึ้นเพื่อควบคุมการปฏิบัติงานเอาไว้โดยละเอียด[11]

การค้นตาม The Police and Criminal Evidence Act 1984 (PACE) สามารถแยกพิจารณาได้ ดังนี้

3.2.3.1 การค้นเครื่องคอมพิวเตอร์พีซีในที่รโหฐาน

3.2.3.2 การค้นข้อมูลอิเล็กทรอนิกส์ในระบบ LAN ระบบ WAN และระบบอินเตอร์เน็ต

3.2.3.3 การยึดและรักษาพยานหลักฐานอิเล็กทรอนิกส์

3.2.3.1 การค้นเครื่องคอมพิวเตอร์พีซีในที่รโหฐาน ตาม PACEวางหลักไว้ในมาตรา 1 ว่าการค้นในเคหสถานต้องมีเหตุอันควรสงสัยตามสมควร โดยถือเอามาตรฐานของบุคคลในฐานะและพฤติการณ์เดียวกับผู้ค้นเป็นเกณฑ์ และจะต้องขอหมายค้นจากศาล[12] ดังนั้นในการค้นข้อมูลอิเล็กทรอนิกส์ ไม่ว่าจะอยู่ที่ใดทั้งที่อยู่ในเคหสถาน หรือที่รโหฐานอื่น เจ้าพนักงานตำรวจจะต้องมีเหตุอันควรสงสัยตามสมควรว่าจะมีพยานหลักฐานอยู่ที่นั้น และจะต้องมีศาลเป็นผู้ทำหน้าที่ตรวจสอบการดำเนินงานอีกชั้นหนึ่ง ในการออกหมายค้นนั้นศาลจะออกให้ก็ต่อเมื่อมีเหตุอันควรเชื่อว่ามีความผิดอาญาร้ายแรง (Serious Arrestable Offence) เกิดขึ้นและพยานหลักฐานที่จะพิสูจน์ความผิดได้ถูกเก็บอยู่ในนั้น จึงต้องพิจารณาว่าอาชญากรรมคอมพิวเตอร์ที่เกิดขึ้นเป็นความผิดอาญาร้ายแรงที่ศาลจะออกหมายค้นหรือไม่ ถ้าอาชญากรรมคอมพิวเตอร์ที่เกิดขึ้นเป็นความผิดอาญาร้ายแรง ศาลก็จะออกหมายค้นให้ และในการเข้าตรวจค้นตามหลักใน PACE มาตรา 16 จะต้องกระทำภายในหนึ่งเดือนนับแต่วันออกหมายค้น โดยจะต้องแจ้งเหตุแห่งการค้น และต้องค้นในเวลาที่เหมาะสม กรณีที่เจ้าของบ้านอยู่ด้วยในเวลาที่ค้น ตำรวจต้องแสดงหมายและมอบสำเนาหมายค้นให้ไว้ แต่ถ้าเจ้าของบ้านไม่อยู่ต้องปิดหมายค้นไว้ในที่ที่เหมาะสม แต่พยานหลักฐานนั้นต้องไม่เป็นพยานหลักฐานที่เป็นความลับตาม PACE มาตรา 15 ,16

กรณีการค้นโดยไม่มีหมายวางหลักไว้ใน PACE มาตรา 17 กำหนดให้ผู้ค้นจะต้องเป็นเจ้าพนักงานตำรวจที่อยู่ในเครื่องแบบ และต้องเป็นการค้นเพื่อช่วยชีวิตบุคคลในเคหสถานนั้น และเพื่อป้องกันการทำลายทรัพย์อย่างร้ายแรง

3.2.3.2 การค้นข้อมูลอิเล็กทรอนิกส์ในระบบ LAN ระบบ WAN และระบบอินเตอร์เน็ต

---

[11]ณรงค์ ใจหาญและคณะ. (2540). **รายงานศึกษาวิจัยฉบับสมบูรณ์ เรื่อง สิทธิผู้ต้องหา จำเลย และผู้ต้องโทษในคดีอาญา (รายงานการศึกษาวิจัยเสนอต่อคณะกรรมการกฤษฎีกา)**. หน้า 23.

[12] ณรงค์ ใจหาญและคณะ. เล่มเดิม. หน้า 51.

ตำรวจอังกฤษจะใช้วิธีนำเครื่องคอมพิวเตอร์หรือเครื่องมืออื่นเชื่อมเข้าไปในระบบเฉพาะของสำนักงาน และระบบเครือข่ายอินเตอร์เน็ต เพื่อเข้าไปตรวจค้นข้อมูลในนั้น จะขอหมายจาก Justice of the Peace ไม่ได้ แต่จะต้องขอจาก Circuit Judge และศาลจะออกหมายให้ต่อเมื่อไต่สวนได้ความว่า "มีเหตุอันควรเชื่อว่าพยานหลักฐานที่เกี่ยวกับการสอบสวนในคดีความผิดเป็น ความผิดอาญาร้ายแรง (Serious Arrestable Offence) ซึ่งเกิดขึ้นในบ้านนี้ และถ้าไม่ค้นบ้านนี้ก็จะไม่ได้มาซึ่งพยานหลักฐานดังกล่าว และในการค้นนั้นจะได้มาซึ่งพยานหลักฐานอันเป็นประโยชน์ต่อสาธารณชน"[13]

3.2.3.3 การยึดและรักษาพยานหลักฐานอิเล็กทรอนิกส์ ในการยึดและรักษาพยานหลักฐานอิเล็กทรอนิกส์มีบัญญัติอยู่ใน PACE มาตรา 18,19 ดังนี้

มาตรา 18 บัญญัติว่า "เมื่อค้นแล้วตำรวจต้องทำบันทึกการค้นและบันทึกรายการสิ่งของที่ค้นและยึด รายการเหล่านั้นผู้ค้นต้องมอบให้แก่เจ้าของบ้านเมื่อผู้นั้นร้องขอ" และ

มาตรา 19 บัญญัติว่า "กรณีที่ตำรวจยึดวัตถุที่มีเหตุเชื่อได้ว่าเป็นพยานหลักฐานที่เกี่ยวข้องกับการสอบสวน หรือความผิดอื่น หรือมีความผิดอื่นรวมอยู่ด้วย หรือมีความจำเป็นต้องยึดเพื่อป้องกันการเคลื่อนย้าย ซ่อนเร้น หรือทำลายหลักฐาน"

จากบทบัญญัติข้างต้นจะเห็นได้ว่าเครื่องคอมพิวเตอร์ที่ยึดได้นั้นเป็นวัตถุที่ใช้เป็นพยานหลักฐานในการสอบสวนที่เจ้าหน้าที่ตำรวจยึดได้ รวมทั้งข้อมูลที่อยู่ภายในเครื่องด้วย เว้นแต่กรณีที่เป็นข้อมูลที่เป็นความลับ ที่จะต้องพิจารณาตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลประกอบ

3.2.4 การรับฟังเป็นพยานหลักฐานในศาล การรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ของศาลอังกฤษ โดยหลักจะรับฟังแต่พยานหลักฐานโดยตรง พยานบอกเล่า (Hearsay) ถือว่ามีน้ำหนักน้อยหรือไม่รับฟังเลย แต่ The Police and Criminal Evidence Act 1984 เป็นกฎหมายพยานหลักฐานในคดีอาญา ที่มีบทบัญญัติเกี่ยวกับการรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์อยู่ เป็นข้อยกเว้นของพยานบอกเล่า (Hearsay) โดยให้รับฟังพยานเอกสารที่เป็นผลจากการประมวลผลหรือคำนวณของเครื่องคอมพิวเตอร์ได้ การค้นและยึดพยานหลักฐานกระทำโดยเจ้าพนักงานตำรวจ กรณีที่ประสบปัญหาการกระทำความผิดทางอินเตอร์เน็ตที่การกระทำอาจเกิดขึ้นในต่างประเทศ อำนาจในการสอบสวนจะสามารถกระทำได้เพียงใด เช่น การกระทำความผิดเกิดขึ้นในประเทศเยอรมนี และผู้กระทำความผิดอยู่ที่ประเทศนั้น แต่เครือข่ายที่ใช้ข้อมูลหรือข้อมูลที่ใช้ผ่านประเทศอังกฤษจะต้องคำนึงถึงข้อตกลงระหว่างประเทศ โดยเฉพาะข้อตกลงระหว่าง

---

[13] ณรงค์ ใจหาญและคณะ. เล่มเดิม. หน้า 52.

ประชาคมยุโรปด้วย แม้ว่าจะต้องคำนึงถึงเรื่องดังกล่าวการดำเนินคดีตามกฎหมายอังกฤษจะถือหลักว่า ถ้าเข้าหลักเกณฑ์ 2 ประการดังต่อไปนี้ประเทศอังกฤษก็อาจจะไม่นำมาดำเนินคดี คือ

ก. ถ้าผู้กระทำความผิดหรือผู้ร่วมกระทำความผิดไม่ใช่พลเมืองของประเทศอังกฤษ หรือ

ข. ความผิดที่เกิดขึ้นไม่ได้บัญญัติไว้ใน The Computer Misuse Act 1990

ศาลที่มีอำนาจในการพิจารณาคดี สามารถแบ่งได้ตามฐานความผิด ดังนี้

(1) ความผิดเนื่องจากปราศจากอำนาจในการเข้าสู่ระบบ (Basic Hacking Offence หรือ Unauthorized Access) เป็นการกระทำความผิดที่ไม่ซับซ้อน ศาลที่มีอำนาจในการพิจารณาคดีคือศาลแขวง(Magistrate Court) จึงมีกฎหมายที่เกี่ยวข้องอีกฉบับคือ The Magistrate's Court Act 1980 เป็นเรื่องเกี่ยวกับการกำหนดฐานความผิดแก่ผู้ที่ให้ความช่วยเหลือในการกระทำความผิดในมาตรา 44 (1) ซึ่งบัญญัติว่า "สามารถลงโทษบุคคลที่ให้ความช่วยเหลือผู้ที่กระทำการเข้าถึงโดยปราศจากอำนาจ โดยการให้ความรู้ทางด้านข้อมูล การให้รหัสผ่าน หรือให้วิธีการเข้าสู่ระบบเพื่อผ่านไปยังโปรแกรมคอมพิวเตอร์หรือข้อมูลในคอมพิวเตอร์"

(2) ความผิดเกี่ยวกับการให้ความสะดวกแก่ผู้กระทำความผิดในการก่อให้เกิดความผิดร้ายแรง และความผิดเกี่ยวกับการทำลายแก้ไขเปลี่ยนแปลงข้อมูลโดยปราศจากอำนาจขึ้นอยู่กับความร้ายแรงของการกระทำความผิด หากมีความร้ายแรงมากก็จะอยู่ในอำนาจพิจารณาของศาลสูงคดีอาญา (Crown Court) แต่ถ้าไม่ร้ายแรงมากก็จะอยู่ในอำนาจพิจารณาของศาลแขวง (Magistrate Court)

โดยลักษณะของข้อมูลอิเล็กทรอนิกส์ที่ไม่สามารถพิสูจน์ได้ในทางกายภาพ จึงไม่สามารถนำมาพิสูจน์ในกระบวนพิจารณาคดีอาญาได้ ดังนั้นรายงานที่ประมวลผลจากคอมพิวเตอร์ (Printout) จะเป็นพยานบอกเล่า (Hearsay) เนื่องจากเกิดจากการกระทำของมนุษย์ ต้องห้ามรับฟังตามกฎหมาย Criminal Justice Act 1988 มาตรา 24 แต่จากความสามารถในการทำงานของคอมพิวเตอร์เองที่สามารถใช้เป็นเครื่องกล หรือเครื่องมือในการคำนวณ จึงไม่น่าจะเป็นพยานหลักฐานในรูปพยานบอกเล่าเสมอไป ถ้าอ้างเป็นพยานหลักฐานโดยยืนยันการใช้ที่เป็นธุรกิจปกติ และข้อมูลที่ได้ก็เกิดจากการประมวลผลโดยคอมพิวเตอร์อันเป็นปกติเช่นกัน[14]

3.3 ประเทศญี่ปุ่น

---

[14] Richard May. (1999). **Criminal Evidence. London**. p. 11-36.

รัฐธรรมนูญของประเทศญี่ปุ่นไม่ได้วางหลักคุ้มครองความเป็นอยู่ส่วนตัวไว้โดยชัดแจ้งแต่เป็นหลักที่อาจสังเคราะห์ขึ้นจากหลักเสรีภาพทั่วไปที่บัญญัติไว้ในมาตรา 13[15] ประกอบกับหลักเสรีภาพในการติดต่อสื่อสารกันโดยอิสระในมาตรา 21[16] และหลักเสรีภาพในเคหสถาน ในเอกสาร และทรัพย์สินส่วนตัว ในมาตรา 35[17] ดังนั้นการเข้าไปในเคหสถาน การค้นและการยึดทรัพย์สินจะกระทำมิได้ ยกเว้นมีหมายที่ออกโดยข้าราชการฝ่ายตุลาการ โดยในหมายนั้นจะต้องระบุเหตุผลที่สมควรและกำหนดสถานที่ตรวจค้นและทรัพย์ที่ต้องการยึดไว้โดยชัดแจ้ง

3.3.1 มาตรการเพื่อการรักษาความปลอดภัยของข้อมูลส่วนบุคคลของประเทศญี่ปุ่น การค้นตามกฎหมายวิธีพิจารณาความอาญาของญี่ปุ่นนั้น ให้อำนาจพนักงานอัยการ หรือเจ้าพนักงานตำรวจดำเนินการค้นได้ ภายใต้รัฐธรรมนูญ มาตรา 35 วรรคหนึ่ง ดังนั้นทำการค้นได้ตามกฎหมายญี่ปุ่นต้องมีหมายค้น การค้นข้อมูลอิเล็กทรอนิกส์ก็เช่นกัน ยกเว้นกรณีที่เป็นการกระทำความผิดซึ่งหน้าตามมาตรา 33 ที่ไม่ต้องมีหมายค้น เนื่องจากเป็นการกระทำความผิดหรือถูกจับเนื่องจากการกระทำความผิดซึ่งหน้า รัฐธรรมนูญได้วางหลักเกณฑ์ให้เจ้าพนักงานสามารถค้น และยึดได้ก็ต่อเมื่อมีหมายค้นหรือหมายยึด หรือเป็นกรณีที่เป็นการค้นหรือการยึดที่สืบเนื่องจากการจับกุมตัวผู้กระทำความผิด

สำหรับการค้นเพื่อทำการยึดจดหมายหรือโทรสาร เนื่องจากรัฐธรรมนูญได้ให้ความคุ้มครองสิทธิเสรีภาพในการสื่อสารของบุคคลไว้ใน มาตรา 35 วรรคหนึ่ง ดังนั้นการยึดจดหมายหรือโทรสารที่บุคคลใช้ติดต่อสื่อสารกันย่อมเป็นการกระทำที่ขัดต่อสิทธิเสรีภาพในการสื่อสารที่รัฐธรรมนูญได้บัญญัติรับรองไว้ แต่ถ้าเป็นกรณีที่เจ้าพนักงานกระทำไปเพื่อการแสวงหาพยานหลักฐานในการพิสูจน์ความผิด หรือเพื่อป้องกันอาชญากรรมก็สามารถดำเนินการค้นและยึดได้ [18]

---

[15] มาตรา 13 บัญญัติว่า “ประชาชนทุกคนย่อมได้รับการเคารพในฐานะปัจเจกบุคคล สิทธิของประชาชนในชีวิต เสรีภาพ และการแสวงหาความผาสุกภายในขอบเขตที่ไม่ขัดต่อประโยชน์สุขอันร่วมกันของสาธารณะ ต้องได้รับความเคารพสูงสุดในการออกกฎหมายหรือในการอื่นใดที่เกี่ยวกับการปกครองประเทศ”

[16] มาตรา 21 บัญญัติว่า “เสรีภาพในการชุมนุม การรวมกลุ่ม รวมทั้งการพูด การพิมพ์ และสิ่งใดทั้งปวงที่เป็นการแสดงออกเป็นสิ่งที่ได้รับการคุ้มครอง

[17] มาตรา 35 บัญญัติว่า “บุคคลใดก็ตาม หากไม่มีหมายซึ่งออกโดยเหตุผลอันชอบธรรมและระบุชัดถึงสถานที่ที่จะตรวจค้นและสิ่งของที่จะอายัด สิทธิที่จะไม่ให้เข้าไปในเคหสถาน ไม่ให้ถูกตรวจค้นและอายัดเอกสารและสิ่งของในครอบครอง ย่อมจะไม่ถูกละเมิด เว้นแต่กรณีตามมาตรา 33

การตรวจค้นและอายัดจะดำเนินการโดยหมายแต่ละประเภท ซึ่งออกโดยเจ้าพนักงานกระบวนการยุติธรรมที่มีอำนาจ”

[18] Shigemitsu Dando. (1965). **Japanese Criminal Procedure**. p. 270

กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในการประมวลผลด้วยเครื่องคอมพิวเตอร์ของหน่วยงานฝ่ายปกครอง ค.ศ. 1988 รัฐสภาญี่ปุ่นบัญญัติขึ้นโดยอาศัยแนวทางของ Organization for Economic Co-operation and Development (OECD) ที่เสนอให้กำหนดหน้าที่ของหน่วยงานในการรักษาความปลอดภัย วางหลักเกณฑ์ในการเข้าถึงข้อมูล และการแก้ไขข้อมูลให้ถูกต้อง โดยกฎหมายฉบับนี้ได้กำหนดให้หน่วยงานของรัฐจำกัดบทบาทในการรวบรวมข้อมูลข่าวสารส่วนบุคคลและโฆษณาให้สาธารณชนทราบการจัดระบบข้อมูลข่าวสารส่วนบุคคลของหน่วยงาน และห้ามมิให้หน่วยงานของรัฐใช้ข้อมูลของรัฐโดยผิดวัตถุประสงค์ คือห้ามมิให้นำข้อมูลข่าวสารส่วนบุคคลซึ่งจัดเก็บโดยมีวัตถุประสงค์อย่างหนึ่งไปใช้ในวัตถุประสงค์อย่างอื่น

3.3.2 การกำหนดความผิดเพื่อคุ้มครองสิทธิส่วนบุคคลที่เป็นข้อมูลอิเล็กทรอนิกส์ การดักฟังการติดต่อสื่อสารถือเป็นการละเมิดเสรีภาพในการติดต่อสื่อสารซึ่งได้รับความคุ้มครองตามรัฐธรรมนูญ มาตรา 21 วรรคสองตอนท้าย บัญญัติว่า “ความลับในการสื่อสารจะละเมิดมิได้” ดังนั้นโดยหลักแล้วการดักฟังย่อมกระทำมิได้ อย่างไรก็ดีรัฐสภาญี่ปุ่นได้ตรากฎหมายว่าด้วยการดักฟังการสื่อสารทางโทรคมนาคม (Communications Interception Law) ขึ้นใช้บังคับในเดือนสิงหาคม ค.ศ. 1999 ซึ่งให้อำนาจเจ้าพนักงานอัยการหรือตำรวจชั้นผู้ใหญ่ในการดักฟังทางโทรศัพท์หรือการดักจับสัญญาณโทรสารและติดตามเฝ้าดูกฎหมายอิเล็กทรอนิกส์ในการสอบสวนคดียาเสพติด การฆาตกรรม หรือคดีอาญาที่มีการใช้อาวุธ หรือการลักลอบหนีภาษีของชาวต่างชาติ โดยจะต้องได้รับอนุญาตจากศาล และให้มีระยะเวลาดักฟังยาวนานที่สุดไม่เกิน 10 วัน โดยจะขอขยายได้ไม่เกิน 30 วัน

นอกจากนี้ในการดักฟังจะต้องมีบุคคลอื่นที่เป็นบุคคลภายนอก เช่น เจ้าหน้าที่ของบริษัทโทรเลขโทรศัพท์แห่งชาติของญี่ปุ่นร่วมฟังด้วยและภายหลังจากการดักฟังสิ้นสุดลงเจ้าพนักงานตำรวจหรือพนักงานอัยการซึ่งทำหน้าที่ดักฟังจะต้องแจ้งให้ผู้ถูกดักฟังทราบถึงการดักฟังนั้นภายใน 30 วัน

สำหรับสิ่งที่กฎหมายญี่ปุ่นบัญญัติไม่ให้ดำเนินการค้นหรือยึด[19] ได้แก่

ก. เอกสารที่เป็นความลับทางราชการ ซึ่งเจ้าพนักงานจะทำการค้นหรือยึดได้ก็ต่อเมื่อมีคำร้องไปยังหัวหน้าหน่วยงานที่มีเอกสารดังกล่าว และต้องได้รับความยินยอมให้ทำการตรวจค้นหรือยึดเอกสารดังกล่าวจากหัวหน้าหน่วยงานนั้นๆด้วย หากหัวหน้าหน่วยงานดังกล่าวไม่ยินยอมให้ค้นหรือยึดเอกสารนั้น เนื่องจากความมั่นคงของประเทศก็สามารถทำได้

---

[19] Ibid. p.300.

ข. เอกสารหรือสิ่งของที่เป็นความลับของลูกค้าในทางการแพทย์ หรือลูกความ เจ้าพนักงานไม่สามารถเข้าไปค้นหรือยึดได้ เว้นแต่จะได้รับความยินยอมจากบุคคลผู้ครอบครอง หากผู้ครอบครองไม่ยินยอมให้เจ้าพนักงานทำการค้นหรือยึดก็ต้องแจ้งเหตุผลที่ไม่ยินยอมให้เจ้าพนักงานทราบด้วย

3.3.3 สาเหตุ วิธีการ และระยะเวลาในการเข้าถึงข้อมูลอิเล็กทรอนิกส์ รัฐธรรมนูญของประเทศญี่ปุ่นบัญญัติไว้ว่าการค้นจะกระทำได้ก็ต่อเมื่อมีหมายที่ออกโดยศาล และจะต้องเป็นการค้นเพื่อการสืบสวนการกระทำความผิดอาญา เป็นการแสวงหาพยานหลักฐานเพื่อพิสูจน์การกระทำความผิดอาญา ซึ่งการแสวงหาพยานหลักฐานดังกล่าวจะกระทำได้ทั้งก่อน และระหว่างการพิจารณา

3.3.3.1 เหตุแห่งค้น ตามกฎหมายประเทศญี่ปุ่น แบ่งออกเป็น 2 ประเภท ได้แก่

ก. กรณีปกติ ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 218 กฎหมายบัญญัติให้อำนาจเจ้าพนักงานของรัฐ ได้แก่ พนักงานอัยการ อัยการผู้ช่วย หรือตำรวจสามารถดำเนินการค้นและยึดได้ แต่ถ้าเป็นการค้นหรือยึดในที่รโหฐานก็ต้องดำเนินการตามหมายค้นหรือยึดที่ออกโดยศาล โดยกำหนดว่าการค้นหรือยึดสิ่งของต่างๆนั้นต้องเป็นไปเพื่อการสืบสวนการกระทำความผิดอาญา การสอบสวนเป็นกระบวนการที่กฎหมายอนุญาตให้เจ้าพนักงานดังกล่าวข้างต้นมีอำนาจในการแสวงหาพยานหลักฐานเพื่อพิสูจน์การกระทำความผิด โดยการแสวงหาพยานหลักฐานนั้นจะต้องกระทำก่อนหรือในระหว่างการพิจารณาคดี[20] เหตุที่เจ้าพนักงานจะขอหมายค้นหรือหมายยึดภายในที่รโหฐานได้ ต้องเป็นกรณีที่มีการแสวงหาพยานหลักฐานที่พิสูจน์การกระทำความผิดกรณีที่พยานหลักฐานดังกล่าวเป็นวัตถุสิ่งของ หากเป็นการค้นหาตัวบุคคลนั้นรัฐธรรมนูญ มาตรา 33 ได้กำหนดว่าเป็นการค้นเพื่อจับกุมผู้กระทำความผิดตามหมายจับ หรือค้นเพื่อหาตัวบุคคลที่ได้กระทำความผิดซึ่งหน้า เจ้าพนักงานสามารถดำเนินการค้นภายในที่รโหฐานได้โดยไม่จำเป็นต้องขอหมายศาล

ข. กรณีพิเศษ เป็นการค้นที่รโหฐานกรณีที่ไม่ต้องมีหมายค้น หรือหมายยึด แต่ก็ต้องเป็นกรณีที่สืบเนื่องมาจากการจับกุม ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 199 บัญญัติหลักเกณฑ์ที่สามารถทำได้ 3 กรณี ได้แก่

(1) การค้นและยึดที่สืบเนื่องจากการจับกุมภายใต้หมายจับที่ออกโดยศาล ตามมาตรา 199 ประกอบมาตรา 220 โดยมาตรา 220 อนุญาตให้เจ้าพนักงานสามารถทำการค้นและยึดสิ่งของกรณีที่เจ้าพนักงานทำการจับกุมผู้ต้องหาที่ศาลออกหมายจับได้ โดยกฎหมายกำหนดให้เจ้าพนักงาน

---

[20] Ibid. p.303.

เหล่านั้นแจ้งต่อศาลว่ามีการกระทำความผิดเกิดขึ้น และเชื่อว่าบุคคลที่จะต้องถูกจับมีความผิดอาญาดังกล่าว

หากเจ้าพนักงานเห็นว่าสิ่งใดสามารถใช้ในการพิสูจน์ความผิดได้ ก็สามารถนำเหตุผลดังกล่าวไปขออนุญาตต่อศาล เพื่อขอหมายค้นเข้าไปค้นหาสิ่งของดังกล่าวมาประกอบการพิจารณาได้ แต่ถ้าเป็นความผิดที่มีอัตราโทษน้อย เช่น โทษปรับไม่เกิน 100 เยน เป็นต้น ไม่จำต้องขอหมายจับจากศาล

3.3.3.2 วิธีการค้น ตามกฎหมายประเทศญี่ปุ่น แบ่งออกเป็น 2 ประเภท ได้แก่

ก.การค้นที่สืบเนื่องจากการจับกุมตามหมายจับ ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 201 เมื่อเจ้าพนักงานได้รับหมายจับจากศาลแล้วสามารถไปดำเนินการตามหมายจับดังกล่าวได้เลย หากบุคคลดังกล่าวอยู่ภายในเคหสถาน หรือสถานที่ใดก็ตาม เจ้าพนักงานสามารถเข้าไปได้โดยไม่ต้องมีหมายค้นจากศาล แต่เมื่อพบบุคคลดังกล่าวแล้วก็ต้องแสดงหมายจับให้ดู

ข. การค้นที่สืบเนื่องจากการจับกุมที่ผู้กระทำความผิดได้กระทำความผิดซึ่งหน้า ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 213 บัญญัติให้อำนาจเจ้าพนักงานได้แก่ เจ้าพนักงานอัยการ อัยการผู้ช่วย หรือตำรวจ สามารถทำการจับกุมผู้ที่กระทำความผิดซึ่งหน้าตนได้โดยไม่ต้องมีหมายจับ ถ้าการจับกุมดังกล่าวเกิดขึ้นในที่รโหฐาน เจ้าพนักงานสามารถค้นและยึดสิ่งของภายในสถานที่ดังกล่าวได้โดยไม่ต้องมีหมาย แต่จะต้องเป็นกรณีที่สามารถออกหมายค้นหรือยึดได้ด้วย และเมื่อพบสิ่งที่ต้องการยึดแล้วจะต้องรีบคืนสิ่งของดังกล่าวให้เจ้าของที่แท้จริงโดยด่วน

สำหรับการกระทำความผิดซึ่งหน้านั้น ตามกฎหมายญี่ปุ่น ได้แก่การกระทำความผิดที่บุคคลได้ลงมือกระทำความผิดในขณะนั้น หรือเพิ่งลงมือกระทำความผิด มีลักษณะการกระทำความผิด 4 ประเภท [21] ได้แก่

(1) เมื่อพบเห็นการกระทำความผิดและติดตามจับกุมแบบกระชั้นชิด

(2) เมื่อพบผู้กระทำความผิดครอบครองทรัพย์สิน อาวุธ หรือสิ่งของที่เกี่ยวข้องกับการกระทำความผิด

(3) เมื่อพบว่าร่างกาย หรือเสื้อผ้าของบุคคลดังกล่าวมีร่องรอยการต่อสู้ บาดแผล หรือมีสิ่งที่บ่งบอกว่าได้กระทำความผิดมา

(4) เมื่อเจ้าพนักงานเรียกให้หยุดแต่กลับวิ่งหนี

---

[21] Ibid. p.310.

หากพบเห็นลักษณะของการกระทำประเภทใดประเภทหนึ่งข้างต้นแล้ว ผู้กระทำความผิดได้ถูกจับกุมในเคหสถาน หรือที่รโหฐาน เจ้าพนักงานที่มีอำนาจสามารถทำการตรวจค้นและยึดสิ่งของภายในสถานที่ดังกล่าวได้โดยไม่ต้องมีหมายค้น หรือยึด

ค. การค้นในกรณีฉุกเฉิน เป็นการค้นหรือการยึดในที่รโหฐานที่สืบเนื่องมาจากการจับกุมผู้ต้องหาในกรณีฉุกเฉินตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 210 กรณีที่มีเหตุเพียงพอที่จะเชื่อว่ามีการกระทำความผิดที่มีอัตราโทษจำคุกมากกว่า 3 ปีขึ้นไป โดยเจ้าพนักงานอัยการ อัยการผู้ช่วย หรือตำรวจ แต่ไม่สามารถขอหมายศาลได้ในขณะนั้น เป็นเหตุให้จับกุมโดยไม่มีหมาย เมื่อทำการจับกุมผู้ต้องหาได้แล้วต้องรีบดำเนินการขอหมายศาลทันที เมื่อเจ้าพนักงานทำการจับกุมผู้ต้องหาได้แล้ว เจ้าพนักงานก็สามารถทำการตรวจค้นหรือยึดได้โดยไม่ต้องมีหมายค้น แต่ถ้าศาลไม่ออกหมายจับให้ เจ้าพนักงานผู้ดำเนินการจับกุมก็ต้องปล่อยตัวบุคคลดังกล่าวทันที พร้อมทั้งคืนสิ่งที่ค้นหรือยึดมาด้วย หากศาลออกหมาย[22]

ง.การค้นโดยประชาชนทั่วไป กรณีที่เป็นการกระทำความผิดซึ่งหน้า ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 213 ให้อำนาจประชาชนทั่วไปสามารถจับกุมผู้ที่กระทำความผิดดังกล่าวได้ด้วย แต่กฎหมายไม่อนุญาตให้บุคคลดังกล่าวตรวจค้น หรือยึดสิ่งของ

3.3.3.3 ระยะเวลาในการค้น การที่กฎหมายให้อำนาจเจ้าพนักงานทำการค้นได้ถือเป็นการกระทำที่ละเมิดต่อสิทธิของบุคคลผู้เป็นเจ้าของ เพราะสิ่งที่กฎหมายประสงค์จะคุ้มครอง คือ สิทธิในการครอบครองและการพักอาศัยของบุคคลในเคหสถาน แต่ด้วยเหตุจำเป็นจึงอนุญาตให้ทำได้ อย่างไรก็ตามกฎหมายก็ได้กำหนดระยะเวลาในการค้นเอาไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 116 เนื่องจากเป็นการกระทำที่รบกวนสิทธิของผู้เป็นเจ้าของสถานที่กฎหมายจึงบัญญัติให้ทำการค้นและยึดได้แต่ในเวลากลางวันเท่านั้น ซึ่งเป็นเวลาตั้งแต่พระอาทิตย์ขึ้นจนถึงพระอาทิตย์ตก เพราะในเวลากลางคืนเป็นเวลาพักผ่อนของผู้ครอบครอง

กรณีที่เจ้าพนักงานทำการตรวจค้นในเวลากลางวันแล้วไม่เสร็จในช่วงเวลานั้น ก็สามารถทำการตรวจค้นต่อเนื่องไปในเวลากลางคืนได้ และกฎหมายก็ให้อำนาจทำการค้นในเวลากลางคืนได้ ตามมาตรา 117 กรณีที่ศาลเห็นว่าจำเป็นที่จะต้องทำการค้นในเวลากลางคืน โดยระบุลงไปในหมายไว้ด้วย สถานที่ที่ศาลอนุญาตให้ทำการตรวจค้นในเวลากลางคืนได้ เช่น สถานบันเทิงเริงรมย์ บ่อนการพนัน โรงแรม หรือร้านอาหาร ฯลฯ

---

[22] Ibid. p.316.

3.3.4 การรับฟังเป็นพยานหลักฐานในศาล ศาลสูงสุดของประเทศญี่ปุ่นได้วางมาตรการในการรับฟังพยานหลักฐานสำหรับการค้นเอาไว้เช่นเดียวกับประเทศอื่นๆ คือ ห้ามมิให้รับฟังพยานหลักฐานที่ได้มาจากการค้น โดยไม่มีหมายค้น โดยมาตรการดังกล่าวเป็นเพียงวิธีการในการป้องกันมิให้เจ้าหน้าที่ใช้อำนาจในทางมิชอบเท่านั้น มิใช่ไม่รับฟังพยานหลักฐานดังกล่าวเลย เพราะในทางปฏิบัติของศาลญี่ปุ่นการรับฟังพยานหลักฐานจะพิจารณาถึงความรุนแรงของการกระทำความผิด ประกอบกับความมุ่งหมายของการสอบสวน

จากการศึกษากฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกานั้นไม่ได้มีกฎหมายที่เป็นกลางซึ่งจะวางหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลอย่างเพียงพอ กฎหมายที่มีผลใช้บังคับอยู่ในปัจจุบันเป็นแต่เพียงกฎหมายที่ให้ความคุ้มครองเฉพาะเรื่อง เช่น การเงิน คอมพิวเตอร์ ฯลฯ ทั้งยังขาดหน่ายงานอิสระที่เป็นองค์กรกลางคอยทำหน้าที่ควบคุม ตรวจตรา และบังคับการให้เป็นไปตามกฎหมาย สำหรับหน่วยงานที่มีอยู่ในปัจจุบันก็ขาดความเป็นอิสระและไม่มีอำนาจเด็ดขาด เนื่องจากเป็นหน่วยงานของฝ่ายบริหาร

สำหรับประเทศอังกฤษซึ่งให้ความเคารพต่อสิทธิส่วนบุคคล และความจำเป็นที่จะต้องดำเนินการให้กฎหมายภายในของตนสอดคล้องกับอนุสัญญาแห่งสภายุโรปว่าด้วยการให้ความคุ้มครองข้อมูล (The Council of Europe’s Data Protection) รัฐสภาของประเทศอังกฤษจึงต้องออกกฎหมายเพื่อแสวงหาพยานหลักฐานของเจ้าพนักงานของรัฐ สามารถล่วงล้ำเข้าไปรับรู้ถึงข้อมูลที่เกี่ยวกับการดำเนินชีวิตของผู้ต้องสงสัยหรือสารสนเทศที่อยู่ในความครอบครองของผู้ใช้ และการแสดงความคิดเห็นส่วนตัว เท่ากับเป็นการล่วงล้ำข้อมูลส่วนบุคคลที่กฎหมายอังกฤษประสงค์จะให้ปกปิด ดังเช่นคดีระหว่างนายจ้างและลูกจ้างข้างต้น การรวบรวมพยานหลักฐานด้วยวิธีการดังกล่าวอาจถูกหาว่าเป็นพยานหลักฐานที่ได้มาโดยมิชอบได้ ทั้งกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของอังกฤษ ที่มีมาตรการควบคุม และตรวจสอบการทำงานของเจ้าหน้าที่โดยองค์กรภายนอกไว้อย่างรัดกุม และไม่ทำให้ประสิทธิภาพในการปราบปรามอาชญากรรมของเจ้าหน้าที่ลดลง โดยการให้ดุลพินิจในการปฏิบัติหน้าที่ของเจ้าหน้าที่ ภายใต้กฎเกณฑ์ที่กฎหมายบัญญัติไว้ จึงดูมีความน่าเชื่อถือที่สุด

ประเทศญี่ปุ่นเองก็มีความพยายามที่จะตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลไว้เป็นกฎหมายทั่วไป แต่ก็ไม่ได้วางมาตรการที่ให้ความคุ้มครองที่เคร่งครัดเกินไป เพราะในขณะเดียวกันก็ให้ตรากฎหมายให้อำนาจเจ้าพนักงานของรัฐเข้าสู่ข้อมูลบางประเภทได้ แต่การแสวงหาพยานหลักฐานจากข้อมูลส่วนบุคคลในประเทศญี่ปุ่นเมื่อเทียบกับอีกสองประเทศข้างต้น ก็ยังเป็นเรื่องใหม่ที่ยังต้องรอให้มีการวางมาตรการ บัญญัติกฎหมายลำดับรอง เพื่อบังคับใช้ตามกฎหมายที่มีอยู่ให้มีประสิทธิภาพมากขึ้น เนื่องจากกฎหมายที่มีนั้นยังไม่สามารถนำมาใช้บังคับได้อย่างเต็มที่

อย่างไรก็ดีประสบการณ์ของทั้งสามประเทศต่างก็มีประโยชน์ต่อการนำมาศึกษาเปรียบเทียบกับกฎหมายของไทยที่มีอยู่