บทที่ 4

การดำเนินคดีกับผู้กระทำความผิดในต่างประเทศ

การดำเนินคดีกับผู้กระทำความผิดบนอินเทอร์เน็ตเป็นปัญหาทั่วโลกที่ให้สำคัญ เนื่องจากมีข้อจำกัดมากมายในการดำเนินคดีกับผู้กระทำความผิดโดยการปรับใช้กฎหมายวิธีสบัญญัติที่มีอยู่เดิม จึงมีความเป็นที่จะต้องบัญญัติกฎหมายวิธีสบัญญัติใหม่ให้สอดคล้องกับลักษณะของการกระทำผิดบนอินเทอร์เน็ต เช่น การกำหนดอำนาจและวิธีปฏิบัติของพนักงานเจ้าหน้าที่ที่เกี่ยวข้อง รวมถึงการรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์ให้เหมาะสม และกระบวนการดังกล่าวต้องมีข้อจำกัดในการนำมาใช้กับฐานความผิดทั่วไป

ตามเอกสารประกอบการประชุมโลกว่าด้วยสังคมสารสนเทศ(World Summit on the Information Society (WSIS) ได้แบ่งแยกมาตรการที่สำคัญในการดำเนินคดีกับผู้กระทำความผิดบนอินเทอร์เน็ต ไว้ดังนี้[170]

1. อำนาจในการเก็บรักษาข้อมูลคอมพิวเตอร์โดยไม่ชักช้าและการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์โดยไม่ชักช้าและการเปิดเผยข้อมูลจราจรทางคอมพิวเตอร์บางส่วน(Powers of expedited preservation of stored data and expedited preservation and partial disclosure of traffic data)

หลักการในการรวบรวมและการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์จะต้องมีความรวดเร็วแตกต่างจากการดำเนินคดีอาญาปกติ เพื่อการวบรวมข้อมูลคอมพิวเตอร์รวมถึงข้อมูลจราจรทางคอมพิวเตอร์ไว้อย่างถูกต้อง และต้องให้อำนาจเจ้าหน้าที่ในการสั่งให้บุคคลหรือผู้ให้บริการเก็บรักษาข้อมูลดังกล่าวไว้โดยไม่ทำการลบหรือแก้ไขข้อมูลภายในระยะเวลาที่กำหนด ในกรณีที่จำเป็นอาจขอให้บุคคลเช่นว่าเก็บรักษาไว้เป็นความลับในช่วงระยะเวลานั้น และอาจสั่งให้ผู้เก็บรักษาข้อมูลเปิดเผยข้อมูลที่ที่จำเป็นเพื่อระบุตัวผู้เกี่ยวข้องกับข้อมูลนั้น

---

[170] Judge Stien Schjolberg and Amada M. Hubbard , "International telecommunication union", Hamonizing National Legal Approaches on Cybercrime. , WSIS thematic Meeting on Cybersecurity (Geneva,28june-1july2005) , pp. 16-17.

ประเทศในกลุ่มเอเปคที่ได้บัญญัติกฎหมายเกี่ยวกับการเก็บรักษาข้อมูลคอมพิวเตอร์โดยไม่ชักช้า (Expedited preservation of stored data) ได้แก่ฮ่องกง จีน ญี่ปุ่น นิวซีแลนด์ ส่วนประเทศที่ไม่มีบทบัญญัติในลักษณะนี้ ได้แก่ ออสเตรเลีย มาเลเซีย สิงคโปร์ ไต้หวัน[2]

สำหรับประเทศที่มีบทบัญญัติเกี่ยวกับการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์โดยไม่ชักช้าและการเปิดเผยข้อมูลจราจรทางคอมพิวเตอร์บางส่วน (Expedited preservation and partial disclosure of traffic data) ได้แก่ ออสเตรเลีย ฮ่องกง จีน ญี่ปุ่น มาเลเซีย นิวซีแลนด์ ไต้หวัน สหรัฐอเมริกา ส่วนประเทศที่ไม่บัญญัติเรื่องนี้ได้แก่ สิงคโปร์[3]

เจ้าหน้าที่มีอำนาจเรียกข้อมูลต่างๆได้ ทั้งที่เป็นข้อมูลด้านเนื้อหา (Content information) และไม่ใช่เนื้อหาของการสื่อสาร (Non-content information) โดยแต่ละประเทศจะมีกระบวนการบังคับให้ผู้ให้บริการเปิดเผยข้อมูลเช่นว่านี้ที่แตกต่างกันตัวอย่างเช่น[4] ประเทศออสเตรเลีย กฎหมายอนุญาตให้เจ้าหน้าที่ตำรวจสามารถร้องขอ ข้อมูลประเภท Non-content information ไปยังผู้ให้บริการได้โดยตรง ในขณะที่การร้องขอข้อมูลประเภท Content-information จะต้องมีหมายจากศาลเท่านั้น สำหรับประเทศที่ไม่มีกฎหมายให้อำนาจเจ้าหน้าที่เรียกข้อมูลจากผู้ให้บริการโดยตรงนั้นจะใช้หลักเกณฑ์เรื่องอำนาจค้นและยึดตามกฎหมายเดิมที่มีอยู่ ตัวอย่างเช่น ในกรณีประเทศฟิลิปปินส์และญี่ปุ่น กฎหมายอนุญาตให้ผู้ให้บริการเปิดเผยข้อมูลตามคำเรียกร้องจากเจ้าหน้าที่ตำรวจได้ แต่หากผู้ให้บริการปฏิเสธการเปิดเผยข้อมูล เจ้าหน้าที่ตำรวจก็จะต้องไปร้องขอหมายค้นจากศาลเพื่อให้ได้มาซึ่งข้อมูลจากผู้ให้บริการ

2. **การสั่งให้จัดทำ**(Production order)

เพื่อประโยชน์ในการดำเนินคดีมีความจำเป็นที่จะต้องเก็บรักษาข้อมูลบางประเภทไว้ โดยการกำหนดให้ผู้ให้บริการจัดเก็บข้อมูลที่ทำให้สามารถระบุตัวผู้ครอบครองหรือใช้คอมพิวเตอร์และส่งมอบข้อมูลดังกล่าวให้แก่เจ้าหน้าที่ที่เกี่ยวข้อง เช่น ข้อมูลที่บันทึกในกระดาษ ข้อมูล log file

---

[2] Summary of Economy Response to APEC E-Security Task Group Cybercrimes Survey , http://www.apec.org

[3] เรื่องเดียวกัน

[4] สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ,ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, "แนวทางการจัดทำกฎหมายอาชญากรรมทางคอมพิวเตอร์ ," หน้า 78-81.

หรือเนื้อหาของอีเมล์ ซึ่งข้อมูลนี้จะไม่ถูกเปิดเผยจนกว่ามีอำนาจให้เปิดเผยได้โดยชอบ เช่น ได้รับอนุญาตจากศาลให้ทำการเปิดเผยข้อมูลได้ เป็นต้น ซึ่งมาตรการนี้แต่ละประเทศจะมีวิธีการที่แตกต่างกัน เช่น ประเทศสหรัฐอเมริกาและออสเตรเลียมีกฎหมายที่อนุญาตให้หน่วยงานด้านการบังคับใช้กฎหมายสามารถร้องขอไปยังผู้ให้บริการเพื่อเก็บรักษาข้อมูลได้เองโดยไม่ต้องมีการตรวจสอบโดยศาล ส่วนบางประเทศ เช่น ญี่ปุ่นและอินโดนีเซียไม่มีกฎหมายที่กำหนดหลักเกณฑ์ในเรื่องนี้โดยตรง การร้องขอให้เก็บรักษาข้อมูลจึงเป็นไปในลักษณะการขอความร่วมมืออย่างไม่เป็นทางการระหว่างพนักงานเจ้าหน้าที่และผู้ให้บริการ

3. **การค้นและยึดซึ่งข้อมูลคอมพิวเตอร์ที่ถูกเก็บไว้** (Search and seizure of stored computer data)

มาตรการในการค้นและยึดข้อมูลคอมพิวเตอร์ที่ถูกเก็บไว้ควรมีการกำหนดให้ชัดเจนเช่นเดียวกันกับการค้นและยึดทรัพย์ที่มีรูปร่าง(Tangible property) การค้นและยึดจำเป็นต้องมีเหตุสมควรในการขออนุญาตค้นและยึด แต่อาจมีวิธีการที่แตกต่างกัน ข้อมูลคอมพิวเตอร์ที่ถูกเก็บไว้ในระบบคอมพิวเตอร์หรือสื่อเก็บข้อมูลคอมพิวเตอร์ อาจจะถูกเข้าถึงหรือค้นโดยการใช้อุปกรณ์คอมพิวเตอร์หรือผ่านระบบโทรคมนาคมอิเล็กทรอนิกส์ หากข้อมูลที่ต้องการถูกเก็บไว้ในระบบคอมพิวเตอร์อื่น การค้นจะถูกขยายผลไปยังระบบคอมพิวเตอร์นั้นอีกด้วย มาตรการเหล่านี้จะต้องถูกใช้กับการยึดหรือการเก็บรักษาไว้ในลักษณะเดียวกันซึ่งระบบคอมพิวเตอร์หรือบางส่วนของระบบ หรือตัวสื่อการเก็บข้อมูลคอมพิวเตอร์นั้นเอง หน่วยงานบังคับใช้กฎหมายต้องสามารถที่จะจัดทำและรักษาสำเนาของข้อมูลคอมพิวเตอร์ และรักษาความสมบูรณ์ของข้อมูลคอมพิวเตอร์ที่ถูกเก็บไว้ และในขณะเดียวกันก็ต้องทำการป้องกันการเข้าถึงได้หรือเปลี่ยนตำแหน่งการเก็บซึ่งข้อมูลคอมพิวเตอร์ในระบบคอมพิวเตอร์ที่เข้าใช้ บทบัญญัติของกฎหมายควรให้อำนาจเจ้าหน้าที่เท่าที่จำเป็นในการสั่งให้ผู้ที่มีความเชี่ยวชาญเกี่ยวกับการทำงานของระบบคอมพิวเตอร์ทำการป้องกันความเสียหายข้อมูลคอมพิวเตอร์ในระบบนั้นเพื่อให้การยึดและค้นเป็นผลสำเร็จ

4. **การรวบรวมข้อมูลจราจรทางคอมพิวเตอร์แบบ**Real-time**และการดักการสื่อสารของข้อมูล** (Real time collection of traffic data and interception of content data)

มาตรการลักษณะนี้ที่จะให้อำนาจเจ้าพนักงานที่เกี่ยวข้องของตนในการรวบรวมข้อมูลคอมพิวเตอร์หรือข้อมูลจราจรทางคอมพิวเตอร์ไว้เป็นพยานหลักฐานในขณะใช้งานและ

บันทึกสื่อสารของข้อมูลแบบReal-time การรวบรวมข้อมูลจราจรทางคอมพิวเตอร์เป็นพยานหลักฐานในขณะใช้งานทำให้การรวบรวมพยานหลักฐานหรือการบันทึกข้อมูลจำเป็นต้องกระทำเพื่อบันทึกการฝ่าฝืนกฎหมายใดๆซึ่งเกี่ยวกับการสื่อสารครั้งใดโดยเจาะจงในเวลาเดียวกับที่มีการสื่อสารข้อมูลนั้น อย่างไรก็ดีมาตรการนี้อาจกระทบต่อสิทธิอื่นๆตามกฎหมาย จึงจำเป็นที่จะต้องจำกัดเฉพาะการฝ่าฝืนกฎหมายอย่างร้ายแรงเท่านั้น และมาตรการเหล่านี้จะต้องเก็บรักษาไว้เป็นความลับ

4.1 การรวบรวมข้อมูลจราจรทางคอมพิวเตอร์แบบReal-time((Real time collection of traffic data) เป็นการรวบรวมข้อมูลที่มิได้เกี่ยวข้องกับเนื้อหา(Non-Content) แต่เป็นการรวบรวมข้อมูลที่แสดงถึงแหล่งที่มา (Source) และปลายทางของการสื่อสาร เช่น[5] ในประเทศสหรัฐอเมริกานั้น จะทำการรวบรวมข้อมูลได้ต่อเมื่อมีหมายจากศาลเท่านั้น แต่ก็มีเงื่อนไขในการออกหมายน้อยกว่ากรณีการขอหมายเพื่อดัก (Intercept) เนื้อหา (Content) ของการสื่อสาร หรือประเทศออสเตรเลียเจ้าหน้าที่สามารถร้องขออย่างเป็นทางการไปยังผู้ให้บริการเพื่อทำการรวบรวมข้อมูลโดยไม่ต้องมีหมายจากศาล เป็นต้น

4.2 การดักการสื่อสารของเนื้อหาข้อมูล(Interception of content data) เป็นการดักข้อมูลในลักษณะเนื้อหา(Content) โดยหลักเกณฑ์หรือข้อจำกัดในการดักการสื่อสารของแต่ละประเทศมีความแตกต่างกันหลายด้าน เช่น กฎหมายที่แตกต่างกัน การให้ความสำคัญกับปัญหาและลักษณะของปัญหาที่เกิดขึ้นในแต่ละประเทศที่แตกต่างกัน เช่น[6]ประเทศแคนาดา ได้กำหนดหลักเกณฑ์ว่า พนักงานสอบสวนจะทำการดักการสื่อสารได้ต่อเมื่อสามารถแสดงต่อศาลได้ว่า ได้พยายามทุกวิถีทางที่จะรวมรวมพยานหลักฐานด้วยวิธีอื่นแล้วแต่ไม่ประสบความสำเร็จ ประเทศมาเลเซีย อนุญาตให้พนักงานสอบสวนดักการสื่อสารได้เฉพาะในกรณีได้รับอนุญาตจากพนักงานอัยการเท่านั้น ประเทศนิวซีแลนด์ อนุญาตให้ดักการสื่อสารภายใต้หลักเกณฑ์เดิมที่ใช้กับการดักฟังการสนทนาทางโทรศัพท์ โดยมีมาตรการป้องกันการใช้อำนาจในทางมิชอบด้วย

---

[5] สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ,ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, "แนวทางการจัดทำกฎหมายอาชญากรรมทางคอมพิวเตอร์ ," 77-78

[6] เรื่องเดียวกัน หน้า 76-77.

4.1 ประเทศสหรัฐอเมริกา

ประเทศสหรัฐอเมริกามีกฎหมายที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์หลายฉบับ โดยกฎหมายที่กำหนดฐานความผิดต่างๆไว้ เช่น Computer fraud and abuse (18 U.S.C. § 1030 Amended in 1988, 1989, 1990, 1994, 1996, 2001,2002) ซึ่งกำหนดฐานความผิดเกี่ยวกับภยันตรายต่อการรักษาความลับ (Compromising Confidentiality) ,Wiretap Act (18 U.S.C. § 2510) ซึ่งกำหนดฐานความผิดเกี่ยวกับการดักการสื่อสารที่ส่งผ่านสายไฟหรือรูปแบบอิเล็กทรอนิกส์และนอกจากนี้ยังรวมถึงบทบัญญัติอื่นๆ เช่น CAN-SPAM Act (Controlling The Assault of Non-Solicited Pornography and Marketing Act of 2003) (15 U.S.C. § 7704), Identity theft and assumption deterrence act of 1998. (18 U.S.C. § 1028), Wire fraud (18 U.S.C. § 1343), Access device fruad (18 U.S.C. § 1029) เป็นต้น [7]

ในส่วนของกฎหมายที่เกี่ยวข้องกับการดำเนินคดีในชั้นสืบสวนสอบสวนนั้นจะต้องดำเนินการภายใต้กฎหมายสำคัญหลัก2 ส่วน ดังต่อไปนี้1. รัฐธรรมนูญของประเทศสหรัฐอเมริกา แก้ไขครั้งที่ 4 (Fourth Amendment to the U.S. Constitution) และ2.บทบัญญัติในหมวด 18 U.S.C. §§ 2510-22, 18 U.S.C. §§ 2701-12, และ 18 U.S.C. §§ 3121-27 ดังนี้

<u>การค้นและยึดคอมพิวเตอร์โดยมีหมาย (Searching and seizing computer with warrant)</u>

ก. <u>กระบวนการในชั้นขอออกหมาย</u>

หลักการของการค้นและการยึดคอมพิวเตอร์จะกระทำได้ต่อเมื่อมีหมาย (Warrant) โดยการออกหมายจะต้องเป็นไปตามกระบวนการของกฎหมาย กล่าวคือการออกหมายจะต้องมีเหตุอันควรซึ่งยืนยันโดยคำสาบานหรือคำรับรอง (Probable cause, support by Oath or affirmation) และจะต้องระบุเฉพาะเจาะจงถึงสถานที่ที่จะทำการค้น และบุคคลหรือสิ่งของที่จะทำการยึด (ทั้งนี้ ตามU.S const. Amend 4)

---

[7] Christopher p sonderby , "Prosecution and investigation of cybercrime", เอกสารเผยแพร่ในการสัมมนา "อาชญากรรมทางคอมพิวเตอร์ของประเทศสหรัฐอเมริกาและกฎหมายใหม่ของประเทศไทย โรงแรมเรดิสัน กรุงเทพมหานคร 11 มิถุนายน 2550 (เอกสารไม่ตีพิมพ์เผยแพร่)

แต่สำหรับการค้นข้อมูลทางคอมพิวเตอร์ไม่สามารถดำเนินการออกหมายค้นตามกระบวนการข้างต้นได้ เพราะไม่สามารถระบุได้ว่าข้อมูลที่จะทำการค้นถูกเก็บไว้ที่ใดหรือในรูปแบบใด เช่น การเข้าถึงไฟล์อาจต้องมีการเข้ารหัส(Encrypted) การตั้งชื่อลวง (Misleading title) การจัดเก็บในรูปแบบไม่ปกติ(Store in unusual file format) หรือ ผสมกับข้อมูลจำนวนมากที่ไม่เกี่ยวข้อง(Commingled with million of unrelated) เป็นต้น ด้วยข้อจำกัดเหล่านี้การออกหมายค้นข้อมูลทางคอมพิวเตอร์จึงมีความแตกต่างจากการออกหมายค้นตามปกติ โดยจะต้องให้อำนาจแก่เจ้าหน้าที่ที่จะทำการค้นอย่างเพียงพอ และเพื่อให้การค้นประสบความสำเร็จจึงได้กำหนดให้เจ้าหน้าที่หรือพนักงานสอบสวนในการดำเนินการ 4 ประการ ต่อไปนี้[8]

1. จัดตั้งคณะผู้ทำการค้น ซึ่งประกอบด้วยเจ้าหน้าที่ในคดี (Case Agent) พนักงานอัยการและ ผู้ชำนาญทางเทคนิค[9] เจ้าหน้าที่ในคดีจะเป็นศูนย์กลางที่ทำการประสานงานระหว่างพนักงานอัยการ และผู้เชี่ยวชาญทางเทคนิค โดยเริ่มจากเจ้าหน้าที่ในคดีจะทำการศึกษาว่าในคดีนั้นจะต้องแสวงหาพยานหลักฐานใด และ คำรับรอง(Affidavit)มีเหตุสมควร(Probable cause) ที่จะออกหมายค้นหรือไม่ ส่วนผู้เชี่ยวชาญทางเทคนิคจะอธิบายถึงข้อจำกัดของการค้นให้เจ้าหน้าที่ในคดีและพนักงานอัยการเข้าใจ และวางแผนการค้นเพื่อให้ได้มาซึ่งพยานหลักฐาน และพนักงานอัยการจะทำการพิจารณาว่าหมายค้นและกระบวนการในการค้นชอบด้วย U.S const. Amend 4 และ Rule 41of Federal Rules of Criminal Procedure หรือไม่ โดยแต่ละฝ่ายจะประสานงานให้ความร่วมมือกันเพื่อให้การค้นเป็นไปอย่างมีประสิทธิภาพ

2. ศึกษาถึงระบบคอมพิวเตอร์ที่จะทำการค้นก่อนวางแผนการค้นหรือก่อนมีการออกหมาย เมื่อมีการจัดตั้งคณะทำงานข้างต้นแล้ว เจ้าหน้าที่ในคดีจะทำการศึกษาข้อมูลเท่าที่จะสามารถทำได้เกี่ยวกับระบบคอมพิวเตอร์ที่เป็นเป้าหมายในการค้นเพื่อให้ทราบว่าเป็นคอมพิวเตอร์ชนิดใด ใช้ระบบปฏิบัติการ(Operation system)ใด เพราะอาจ

---

[8] Computer Crime and Intellectual Property Section Criminal Division United States Department of Justice, Searching and Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, (Update Appendix version 2006), p. 28.

[9] ผู้เชี่ยวชาญจะมาจากผู้ที่ได้รับการแต่งตั้งตามกฎหมายและได้ผ่านการอบรมในหลักสูตรComputer forensic โดยมีหน่วยงานในลักษณะนี้หลายหน่วยงาน เช่น FBI มีหน่วยงาน Computer Analysis Response Team (Cart), Internal Revenue Service มีหน่วยงาน Seized Computer Evidence Recovery (SCER)และ Secret service มีหน่วยงาน Electric Crime special Agent Program (ECSAP)

เกิดปัญหาในการค้นระบบคอมพิวเตอร์ที่มีความสลับซ้อน เช่น การค้นบริษัทที่ต้องสงสัย อาจจะไม่พบข้อมูลที่เป็นประโยชน์ก็ได้ เพราะบริษัทดังกล่าวอาจส่งข้อมูลไปจัดเก็บไว้ยังเซิฟเวอร์ที่ตั้งอยู่ในพื้นที่ห่างไกล เจ้าหน้าที่ในคดีจึงจำเป็นต้องศึกษาเกี่ยวกับHardware,Software ,Operation system และConfiguration of the network ที่ใช้กระทำความผิดและเพื่อให้การค้นเป็นไปโดยถูกต้อง จำเป็นต้องพิจารณากฎหมายที่เกี่ยวข้องอื่นๆด้วย ได้แก่ Privacy Protection Act (PPA)42 U.S.C. § 2000aa และElectronic communications Privacy Act (ECPA)18 U.S.C. §§ 2701-2712

3.กำหนดแผนการดำเนินการค้น(รวมถึงแผนการสำรองข้อมูล)บนพื้นฐานของข้อมูลที่ได้จากการศึกษาระบบคอมพิวเตอร์เป้าหมาย

เมื่อคณะผู้ทำการค้นทราบถึงระบบคอมพิวเตอร์ที่จะทำการค้นแล้ว ขั้นตอนต่อไปคือ การวางแผนการค้น เช่น การค้นดังกล่าวจะต้องทำการสำรองข้อมูล (Backup)ไว้หรือไม่ มีความจำเป็นที่จะต้องเข้าทำการย้ายอุปกรณ์ทั้งหมดออกจากสถานที่หรือไม่ และหาแผนการดังกล่าวไม่สำเร็จจะมีแผนสำรองอย่างไร เป็นต้น ในการวางแผนการค้นจำเป็นต้องพิจารณากฎหมายที่เกี่ยวข้องใน 4 ประเด็น ต่อไปนี้ 1. แผนการค้นเป็นไปตาม Rule 41 of the Federal Rules of Criminal Procedure และ U.S const. Amend 4 หรือไม่, 2. แผนการค้นได้ล่วงละเมิดกฎหมาย Privacy Protection Act (PPA) หรือ Electronic communications Privacy Act (ECPA) หรือไม่, 3. การค้นต้องมีการพิจารณาขอออกหมายหลายฉบับ (Multiple warrant) หรือไม่, 4. มีความจำเป็นที่จะต้องอนุญาตให้ออกหมายประเภท "No-Knock" หรือ "Sneak-and-peek" หรือไม่

4. การออกหมายและบันทึกคำให้การ

กฎหมายบังคับให้เจ้าหน้าที่จัดทำเอกสาร 2 ฉบับในการขอหมายค้นที่ออกโดยผู้พิพากษา(Magistrate judge)ได้แก่ 1. คำรับรอง(Affidavit) คือเอกสารที่เจ้าหน้าที่ได้สาบานและจะต้องระบุเหตุอันควร(Probable cause) และ 2. คำร้องขอออกหมาย [10]

---

[10] Computer Crime and Intellectual Property Section Criminal Division United States Department of Justice, Searching and Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations , pp. 40-48.

เมื่อผู้พิพากษาพิจารณาบันทึกคำให้การว่ามีเหตุอันควรและคำร้องขอออกหมายได้ระบุถึงสถานที่ที่จะทำการค้นและรายละเอียดของสิ่งของที่จะทำการยึดอย่างพอเพียงแล้วผู้พิพากษาจะลงลายมือชื่อเพื่ออนุญาตออกหมาย ทั้งนี้ ภายใต้ Rule 41 of the Federal Rules of Criminal Procedure และเจ้าหน้าที่จะต้องดำเนินการตามหมายภายในสิบวันนับตั้งแต่วันที่ได้ออกหมาย[11]

ข. <u>กระบวนการในการค้นและยึด</u>

1. วิธีการในการค้นคอมพิวเตอร์

วิธีการในการค้นคอมพิวเตอร์มีหลากหลายวิธี แต่อาจแบ่งได้ 4 ประเภท ดังนี้

(1) ค้นคอมพิวเตอร์และพิมพ์ข้อมูลจากคอมพิวเตอร์ลงบนกระดาษ (Print out a hard copy) ในเวลาเดียวกัน(At that time)

(2) ค้นคอมพิวเตอร์และทำสำเนาอิเล็กทรอนิกส์(Electronic copy) ในเวลาเดียวกัน

(3) สร้างสำเนาอิเล็กทรอนิกส์(Create a duplicate electronic copy) ข้อมูลทั้งหมดที่บรรจุในสถานที่นั้น(On-site) และนำมาสร้างใหม่(Recreate) นอกสถานที่นั้น(Off-site) แล้วนำสำเนาอิเล็กทรอนิกส์ที่ได้มาพิจารณา[12]

(4) ยึดอุปกรณ์และย้ายอุปกรณ์เหล่านั้นออกจากสถานที่นั้น จากนั้นนำมาพิจารณาเนื้อหา(Content) นอกสถานที่นั้น(Off-site)

---

[11] The Federal Rules of Criminal Procedure 41(b).

[12] หรือเป็นที่รู้จักกันในชื่อ วิธีการ "Imaging"

โดยทั่วไปแล้ว การค้นหาเนื้อหา (Content) ที่ระบุไว้ในหมาย (Warrant) อาจใช้ระยะเวลายาวนานเพราะคอมพิวเตอร์ที่ค้นอาจบรรจุข้อมูลจำนวนมาก อาจหาไฟล์ที่ต้องการไม่พบหรือแม้เจ้าหน้าที่จะหาไฟล์ที่ต้องการพบแต่ก็อาจไม่สามารถเข้ารหัส (Encrypted)ได้ การยึดและการค้นข้อมูลคอมพิวเตอร์จึงมีความจำเป็นที่จะต้องกระทำนอกสถานที่นั้น (Off-site) ดังนั้น จึงไม่มีเหตุผลที่เจ้าหน้าที่จะใช้เวลาค้นสิ่งของต่างๆในสถานที่นั้น(On-Site)เป็นเวลายาวนาน[13]

ในบางกรณี การค้นในสถานที่นั้น(On-Site) อาจเสี่ยงต่อการทำลายพยานหลักฐานเพราะเจ้าหน้าที่อาจไม่มีความเข้าใจระบบปฏิบัติการที่ไม่ปกติ(Uncommon operating system)อย่างดีพอ ดังนั้น วิธีการที่ดีที่สุดจึงควรย้ายอุปกรณ์คอมพิวเตอร์ออกจากสถานที่นั้นแล้วให้ผู้เชี่ยวชาญทำการตรวจสอบในภายหลัง การค้นนอกสถานที่นั้น (Off-site) มีความจำเป็นอย่างยิ่งโดยเฉพาะในกรณีที่เจ้าหน้าที่เชื่อว่าได้สร้างหลุมพรางลวง(Booby trapped)ไว้ เช่น ผู้กระทำความผิดอาจใส่โปรแกรมสำหรับทำลายตนเอง(Self-destruct program) ไว้ เมื่อเจ้าหน้าที่ที่ทำการตรวจสอบไม่สามารถใส่รหัสได้ถูกต้องภายในเวลา10 วินาที คอมพิวเตอร์ก็จะทำลายข้อมูลโดยอัตโนมัติ เจ้าหน้าที่จึงจำเป็นที่จะต้องทำการค้นนอกสถานที่นั้น (Off-site และทำการปลดโปรแกรมทุกครั้ง

ส่วนกรณีที่สามารถใช้การค้นในสถานที่นั้น (On-Site) ได้ อาจเป็นกรณีที่ผู้ควบคุมหรือดูแลเครือข่าย(System administer)ให้ความร่วมมือในการค้น การบันทึก หรือสำรองข้อมูลโดยไม่ชักช้า รวมถึงให้ความร่วมมือในพิมพ์ข้อมูลจากคอมพิวเตอร์ลงบนกระดาษ (Print out a hard copy)[14] การที่เจ้าหน้าที่จะเลือกใช้วิธีการใดเจ้าหน้าที่จะพิจารณาตามความเหมาะสมและจะต้องระบุวิธีการดังกล่าวดำเนินการลงในหมาย(Warrant) โดยคำนึงหลักการดำเนินคดีอาญา 2 ประการคือ

---

[13] "United States v. Santarelli, 778 F.2d 609, 615-16 (11th Cir. 1985)"

[14] "United States v. Longo, 70 F. Supp. 2d 225 (W.D.N.Y. 1999)" (ในคดีนี้เจ้าหน้าที่ได้รับการช่วยเหลือจากผู้ควบคุมระบบ(Suspect's secretary)ในการระบุไฟล์ข้อมูลที่เกี่ยวข้อง จำนวน2ไฟล์)

1.1 กรณีที่อุปกรณ์คอมพิวเตอร์นั้นเป็นสิ่งผิดกฎหมาย, พยานหลักฐาน, ใช้เป็นเครื่องมือในการทำความผิด หรือได้มาจากการกระทำความผิด (When Hardware is itself Contraband, Evidence, or an Instrumentality or Fruit of Crime)

ภายใต้ Rule 41(b) of the Federal Rules of Criminal Procedureเจ้าหน้าที่สามารถ "ยึด"คอมพิวเตอร์ได้ เมื่อได้ทำการค้นตาม"หมายค้น"(Search Warrant) หากพบอุปกรณ์คอมพิวเตอร์ที่เป็นสิ่งผิดกฎหมาย (Contraband) ,หลักฐาน (Evidence) ,ใช้เป็นเครื่องมือในการทำความผิด (Instrumentality) หรือได้มาจากการกระทำความผิด (Fruit of crime)[15] ยกตัวอย่างเช่น การใช้คอมพิวเตอร์ส่วนบุคคลในการจัดเก็บหรือส่งภาพผิดกฎหมาย ถือว่าได้ใช้คอมพิวเตอร์นั้นเป็นเครื่องมือในการทำความผิด (Instrumentality)และเมื่อได้ทำการยึดแล้วเจ้าหน้าที่จะนำคอมพิวเตอร์ดังกล่าวเก็บไว้ยังสถานีตำรวจหรือส่งไปยัง Forensic laboratory ต่อไป

1.2 กรณีที่อุปกรณ์คอมพิวเตอร์ นั้นเป็นเพียงสิ่งบรรจุพยานหลักฐานในการกระทำผิดอาญา (When Hardware is merely a Storage Device for Evidence of Crimes)

ในกรณีนี้คำรับรอง (Affidavit) จะต้องอธิบายให้ชัดเจนว่าเหตุใดจึงถือว่ามีเหตุอันควรเชื่อได้ว่าอาจพบพยานหลักฐานในสถานที่ทำการค้น แต่ไม่จำเป็นต้องระบุเฉพาะเจาะจงถึงขนาดว่าหลักฐานนั้นจัดเก็บไว้ในคอมพิวเตอร์ ส่วนวิธีการค้นในกรณีนี้มีข้อแตกต่างจากกรณีที่อุปกรณ์คอมพิวเตอร์นั้นเป็นสิ่งผิดกฎหมาย (Contraband), พยานหลักฐาน (Evidence),ใช้เป็นเครื่องมือในการทำความผิด (Instrumentality) หรือได้มาจากการกระทำความผิด (Fruit of crime) ข้างต้น กล่าวคือ Fed. R. Crim. P. 41 (b) ให้อำนาจเจ้าหน้าที่ที่จัดการตามหมาย (Warrant) มีอำนาจยึด" "พยานหลักฐานอิเล็กทรอนิกส์" (Electronic Evidence) แต่ไม่ได้ให้อำนาจเจ้าหน้าที่โดยตรงในการยึด"อุปกรณ์คอมพิวเตอร์"(Hardware) ที่เป็นสิ่งบรรจุพยานหลักฐาน[16] (Hardware that happens to contain that evidence) เพราะไม่ถือว่าอุปกรณ์คอมพิวเตอร์เหล่านี้เป็นพยานหลักฐานในตัวเอง(Not evidence itself) แต่มิได้หมายความว่าห้ามยึดเสียทีเดียว แต่หมายความว่าเจ้าหน้าที่รัฐอาจยึดได้หากไม่มีทางเลือกอื่นซึ่งอาจกระทำได้เพื่อให้ได้มาซึ่งพยานหลักฐานนั้นโดยต้องพิจารณาเป็นกรณีไป

---

[15] Thomas Alfred Johnson, Forensic Computer Crime Investigation(United States : CRC Press, 2005) p. 293.

[16] "United States v. Tamura, 694 F.2d 591, 595 (9th Cir. 1982)"

2. การพิจารณากฎหมายที่เกี่ยวข้องกับการยึดและค้นตามหมาย

นอกจากจะต้องพิจารณากฎหมาย Fed. R. Crim. P. 41 และความชอบตาม U.S const. Amend 4 ดังที่ได้กล่าวมาแล้วข้างต้น กรณีที่การยึดคอมพิวเตอร์ที่เกี่ยวข้องกับความผิดไม่ใช่คอมพิวเตอร์ส่วนบุคคล (Stand-alone-PC) แต่เป็นเครือข่ายคอมพิวเตอร์ (Network) ที่มีความสลับซับซ้อนย่อมเกิดเสียหายหากมีการยึดเครือข่ายคอมพิวเตอร์ทั้งระบบ แต่เมื่อพิจารณาจากตัวบทกฎหมายแล้วกฎหมายได้เปิดช่องให้เจ้าหน้าที่สามารถยึดเครือข่ายคอมพิวเตอร์ได้ทั้งระบบ แต่การยึดเครือข่ายคอมพิวเตอร์ทั้งระบบดังกล่าวต้องใช้ความระมัดระวังเป็นพิเศษเพราะอาจทำให้รัฐถูกฟ้องได้ ภายใต้กฎหมายPrivacy Protection Act (PPA) (42 U.S.C. § 2000aa) และ Electronic Communications Privacy Act (ECPA) (18 U.S.C. §§ 2701-2712)[17] ดังนี้

2.1 Privacy Protection Act (PPA)

แต่เดิมศาลสหรัฐอเมริกา ไม่อนุญาตออกหมายค้นเพื่อที่จะค้น หรือ ยึด วัตถุที่เป็นเพียงพยานหลักฐาน (mere evidence)ได้ เนื่องจากหมายค้นจะออกได้เฉพาะในการยึดสิ่งผิดกฎหมาย (Contraband) ,ใช้เป็นเครื่องมือในการทำความผิด (Instrumentality) หรือได้มาจากการกระทำความผิด (Fruit of crime)เท่านั้น[18] จนกระทั่ง ศาลได้กลับหลักนี้ และวางหลักขึ้นใหม่ว่า รัฐธรรมนูญฉบับแก้ไขเพิ่มเติมฉบับที่สี่ (Fourth Amendment) ให้อำนาจหน่วยงานของรัฐที่จะขอหมายค้นเพื่อที่จะยึดวัตถุที่เป็นเพียงหลักฐานได้[19] แต่หลักการเช่นว่าได้ก่อให้เกิด ปัญหาระหว่างเจ้าหน้าที่กับสื่อมวลชน เนื่องจากสื่อมวลชนมักจะถือครอง "พยานหลักฐาน (mere evidence)" เจ้าหน้าที่จึงออกหมายและทำการค้นสื่อมวลชนเพื่อให้ได้มาซึ่งวัตถุที่เป็นเพียงพยานหลักฐานได้ แม้ว่าสื่อมวลชนจะมิใช่ผู้กระทำความผิดก็ตาม[20] ในปี 1980

---

[17] "Steve Jackson Games, Inc. v. Secret Service, 816 F. Supp. 432, 440, 443 (W.D. Tex. 1993)"

[18] "Boyd v. United States, 116 U.S. 616 (1886)"

[19] "Warden v. Hayden, 387 U.S. 294, 309 (1967)"

[20] "Zurcher v Stanford Daily, 436 U.S. 547 (1978)"(District Attorney's Office (สำนักงานอัยการประจำเมือง) ใน Santa Clara County ได้ขอออกหมายค้นและทำการค้นหนังสือพิมพ์ Stanford Daily เนื่องจากได้ตีพิมพ์ภาพเกี่ยวกับการชุมนุมประท้วง และเจ้าหน้าที่เชื่อว่าทางสำนักพิมพ์น่าจะมีพยานหลักฐานเพิ่มเติมที่อาจทำให้เจ้าหน้าที่สามารถระบุตัวผู้ประท้วงได้ อย่างไรก็ตามเจ้าหน้าที่ไม่พบหลักฐานใดๆ หนังสือพิมพ์จึงฟ้องเจ้าหน้าที่เป็นคดีนี้ แต่ศาลยกฟ้อง โดยให้เหตุผลว่า First Amendment หรือ Fourth Amendment ไม่ได้ห้ามการค้นสื่อมวลเช่นว่านี้)

จึงได้มีการออกกฎหมาย PPA เพื่อลดการแสวงหาพยานหลักฐานจากผู้เผยแพร่ข่าวสารที่มิได้มีส่วนร่วมในการกระทำความผิด

การละเมิด PPA จะไม่ทำให้หลักฐานนั้นเป็นหลักฐานที่ต้องห้ามนำเสนอต่อศาล (ดู 42 U.S.C. § 2000aa6-6(d)) แต่จะก่อให้เกิดสิทธิเรียกร้องค่าเสียหายทางแพ่งต่อรัฐจากการที่เจ้าหน้าที่ หรือ ลูกจ้างของรัฐได้ปฏิบัติการค้น[21] หากเจ้าหน้าที่ หรือ ลูกจ้างของรัฐละเมิดต่อ PPA และรัฐมิได้สละความคุ้มกันในฐานะที่เป็นรัฐาธิปัตย์ เจ้าหน้าที่ย่อมได้รับความคุ้มกันจากการฟ้องคดี[22] พนักงานหรือลูกจ้างของรัฐอาจจะต้องรับผิดในการกระทำที่อยู่ภายใต้ขอบเขตหรือในทางการที่จ้าง แต่จะต้องอยู่ภายใต้ข้อต่อสู้ที่ได้กระทำไปโดยสุจริต (§ 2000aa-6(a)(2),(b))

กล่าวโดยสรุปคือ ในการค้นและยึดอุปกรณ์คอมพิวเตอร์เจ้าหน้าที่จำเป็นต้องพิจารณากฎหมายPPA เป็นพิเศษเนื่องจากในปัจจุบันนี้ประชาชนแทบทุกคนมีเครื่องคอมพิวเตอร์ และสามารถเข้าอินเทอร์เน็ตได้ จึงอาจจะถือเป็นผู้เผยแพร่ข้อมูลข่าวสารที่ได้รับความคุ้มครองตาม PPA เช่น การที่เจ้าหน้าที่เข้าไปคัดลอกข้อมูลที่เผยแพร่ผ่านทางผ่านทางอินเทอร์เน็ตอาจถือเป็นการละเมิดกฎหมายนี้

2.2 Electronic communications Privacy Act (ECPA)

เมื่อการค้นและยึดข้อมูลในเครือข่ายคอมพิวเตอร์ที่เกี่ยวข้องซึ่งเป็นของบุคคลภายนอกผู้บริสุทธิ์ เจ้าหน้าที่ของรัฐควรที่จะต้องพยายามทุกวิถีทางเพื่อคุ้มครองสิทธิของบุคคลภายนอกเพื่อป้องกันความรับผิดจาก ECPA เพราะเมื่อเจ้าหน้าที่ดำเนินการค้นผู้ให้บริการอินเทอร์เน็ต และยึดข้อมูล (account) ของลูกค้าและใช้บริการ ลูกค้าและผู้ใช้บริการอาจฟ้องเจ้าหน้าที่ในทางแพ่งว่าการค้นนั้นละเมิดต่อกฎหมายความเป็นส่วนตัวในการสื่อสารทางอิเล็กทรอนิกส์ ตาม ECPA

---

[21] "Davis v Gracey, 111 F.3d 1472, 1482 (10th Cir. 1997)" (ศาลยกฟ้องคดี PPA ต่อเจ้าหน้าที่ท้องถิ่นในความรับผิดเฉพาะตัวเนื่องจากการฟ้องคดีจะต้องเป็นการฟ้องคดีต่อ "หน่วยงานของรัฐ" เว้นแต่หน่วยงานของรัฐจะไม่ได้สละความคุ้มกันในฐานะที่เป็นรัฐาธิปัตย์)

[22] "Barnes v. State of Missouri, 960 F.2d 63, 65 (8th Cir. 1992)"

ECPA จะควบคุมเจ้าหน้าที่ในการเข้าถึงเนื้อหาของการสื่อสารทางอิเล็กทรอนิกส์ที่จัดเก็บโดยผู้ให้บริการ (ดู 18 U.S.C. § 2703) นอกจากนั้น ECPA ยังมีบทบัญญัติกำหนดโทษทางอาญาที่ห้ามการเข้าถึงการสื่อสารทางอิเล็กทรอนิกส์ หรือ การติดต่อสื่อสารผ่านสายโทรศัพท์ (Electronic or wire communications) ที่เก็บไว้ในรูปแบบอิเล็กทรอนิกส์ (Electronic storage.) (ดู 18 U.S.C. § 2701-2702) เช่น E-mail, Account,Record เป็นต้น

หลักการที่แสดงให้เห็นว่าการค้นตามหมายค้นที่ชอบด้วยกฎหมายอาจจะละเมิดต่อ ECPA มาจากคดี Steve Jackson Games[23] จึงได้มีการกำหนดแนวทางการดำเนินคดีให้สอดคล้องกับ ECPA คือ การปฏิบัติการค้นจะต้องกระทำโดยอาศัยการให้ความระมัดระวังอย่างสูง เมื่อเจ้าหน้าที่จะต้องปฏิบัติการค้นผู้ให้บริการอินเทอร์เน็ต และบุคคลอื่นที่ถือครองข้อมูลการติดต่อสื่อสารทางอิเล็กทรอนิกส์เหล่านั้น

ในคดีส่วนใหญ่ เจ้าหน้าที่จะหลีกเลี่ยง การค้น หรือ ยึดคอมพิวเตอร์ของผู้ให้บริการทั้งหมด เว้นแต่ ไม่มีทางเลือกอื่น เช่น ในกรณีที่หน่วยงานที่เป็นเจ้าของเครือข่ายอินเทอร์เน็ต มีเหตุอันควรสงสัยเป็นอย่างยิ่งว่ามีความเกี่ยวพันกับการกระทำความผิดอาญาแต่ทั้งนี้เจ้าหน้าที่จะต้องกระทำการโดยใช้ความระมัดระวังเป็นอย่างยิ่ง โดยหลีกเลี่ยงไม่เข้าไปค้นข้อมูลเกี่ยวกับลูกค้าที่ที่ไม่มีส่วนรู้เห็น และจะต้องกระทำการทุกประการเพื่อรับประกันความลับของข้อมูลเหล่านั้นเพื่อรับประกันความเป็นส่วนตัวของลูกค้าหรือผู้ให้บริการ (18 U.S.C.§ 2701) เพราะผลของการละเมิดกฎหมายนี้อาจทำให้เจ้าหน้าที่ถูกฟ้องร้องทางแพ่งได้

ดังที่ได้กล่าวมาแล้วว่าการละเมิดกฎหมายPrivacy Protection Act, 42 U.S.C. § 2000aa และ Electronic Communications Privacy Act, 18 U.S.C. §§ 2701-2712 อาจทำให้รัฐหรือเจ้าหน้าที่รัฐถูกฟ้องร้องได้ ตามคู่มือการค้นและยึดคอมพิวเตอร์และได้มาซึ่งพยานหลักฐานอิเล็กทรอนิกส์ในการสืบสวนคดีอาญาของสหรัฐอเมริกาจึงได้กำหนดให้กรณี

---

[23] "Steve Jackson Games, Inc. v. Secret Service, 816 F. Supp. 432 (W.D. Tex. 1993)" (ศาลเห็นว่า การที่เจ้าหน้าที่อ่านข้อความการสื่อสารของลูกค้าของจำเลยที่เก็บไว้ในคอมพิวเตอร์ของจำเลย โดยที่ข้อความเหล่านั้นไม่เกี่ยวข้องกับการกระทำความผิดอาญา และได้ลบ หรือ ทำลาย การติดต่อสื่อสารไม่ว่าจะกระทำโดยตั้งใจ หรือ โดยบังเอิญก็ถือว่ามีความรับผิดตาม ECPA)

ที่เจ้าหน้าที่สงสัยว่าการดำเนินการของตนอาจขัดต่อกฎหมายดังกล่าว เจ้าหน้าที่ควรจะติดต่อหน่วยงาน Crime and Intellectual Property หรือหน่วยงาน CTC ในท้องที่ของตน[24]

3. การพิจารณาเพื่อขอหมายค้นหลายฉบับในการค้นเครือข่าย (Multiple warrants)

เจ้าหน้าที่ควรที่จะมีหมายค้นหลายฉบับ ในกรณีที่มีเหตุอันควรเชื่อได้ว่าการค้นเข้าไปในเครือข่าย (Network) จะทำให้ได้มาซึ่งข้อมูลเก็บไว้ในหลายท้องที่

Fed. R. Crim P. 41(a) บัญญัติว่าผู้พิพากษาในศาลที่มีเขตอำนาจสามารถออกหมายค้นเพื่อ "ค้นทรัพย์สิน.....ที่อยู่ในท้องที่ของตน" หรือ "ค้นทรัพย์สิน.....ที่อยู่นอกท้องของตนในกรณีที่ทรัพย์สินนั้น....อยู่ในเขตอำนาจศาลขณะที่มีการออกหมาย แต่ทรัพย์สินอาจจะถูกเคลื่อนย้ายออกไปจากท้องที่นั้นก่อนที่จะมีการปฏิบัติการตามหมาย"[25]

ศาลฎีกาสหรัฐอเมริกาได้วินิจฉัยว่า "ทรัพย์สิน" ที่ระบุอยู่ใน Rule 41 รวมไปถึงวัตถุที่ไม่มีรูปร่างเช่น ข้อมูลในคอมพิวเตอร์ด้วย [26] ทำให้เกิดปัญหาการใช้กฎหมายของเจ้าหน้าที่ ด้วยเหตุว่า ข้อมูลในคอมพิวเตอร์ที่อยู่ในเครือข่ายคอมพิวเตอร์อาจจะอยู่ณ ที่ใดบนโลกก็ได้ เช่น ในกรณีที่เจ้าหน้าที่เข้าไปค้นสำนักงานใน Manhattan ตามหมายที่มาจาก Southern District of New York อาจจะสามารถเข้าไปสู่ข้อมูลที่อยู่ในคอมพิวเตอร์ที่เก็บไว้ในสถานที่ที่ไกลออกไป เช่น ในมลรัฐ New Jersey มลรัฐ California หรือ แม้แต่ที่อยู่ในต่างประเทศ ทั้งนี้ ไฟล์ที่ระบุไว้ในหมายอาจจะอยู่ที่ใดบนโลกก็เป็นได้ หรือ ไฟล์นั้นอาจจะมีการแบ่งส่วนอยู่ในสถานที่หลายๆท้องที่ หรือ หลายประเทศ หรือ ในกรณีที่ยากกว่านั้น คือ ในขณะที่เจ้าหน้าที่ได้

---

[24] Computer Crime and Intellectual Property Section Criminal Division United States Department of Justice, Searching and Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations , pp. 35 – 36.

[25] Fed. R. Crim. P. 41(a) states that a magistrate judge located in one judicial district may issue a search warrant for "a search of property . . . within the district," or "a search of property . . . outside the district if the property . . . is within the district when the warrant is sought but might move outside the district before the warrant is executed."

[26] "United States v. New York Tel. Co., 434 U.S. 159, 170 (1977)."

ปฏิบัติการค้น เจ้าหน้าที่ไม่อาจทราบว่าข้อมูลที่เจ้าหน้าที่ได้ยึดมาอยู่ในที่ท้องที่นั้น หรือ อยู่นอกท้องที่นั้น หรือในบางกรณีเจ้าหน้าที่ก็ไม่อาจรู้ได้ว่าสถานที่เก็บข้อมูลอยู่ที่ใดจนกระทั้งการค้นได้กระทำสำเร็จลุล่วงไปแล้ว

หากเจ้าหน้าที่รู้ได้ก่อนที่จะมีการค้นว่าข้อมูลบางส่วน หรือทั้งหมดที่ระบุในหมายอยู่ที่เก็บในท้องที่ที่อื่นที่แตกต่างจากที่เจ้าหน้าที่ได้กระทำการค้น วิธีการที่ดีที่สุดในกรณีเช่นนี้จะขึ้นอยู่กับว่าสถานที่ที่เก็บข้อมูลที่อื่นอยู่ ณ ที่ใด

ในกรณีที่ข้อมูลถูกแยกเก็บในสถานที่ 2 แห่งหรือมากกว่านั้น ซึ่งสถานที่เหล่านั้นอยู่ในอาณาบริเวณ (Territory) ของประเทศสหรัฐอเมริกา เจ้าหน้าที่จะต้องปฏิบัติตามข้อกำหนดของ Rule 41 อย่างเคร่งครัด เช่น ในกรณีที่ข้อมูลถูกเก็บอยู่ในสถานที่ 2 ท้องที่ เจ้าหน้าที่จะต้องได้รับหมายจากศาลในทั้ง 2 ท้องที่นั้น[27]

ในกรณีที่ต้องทำการค้นนอกประเทศสหรัฐอเมริกา ตามคู่มือการค้นและยึดคอมพิวเตอร์และได้มาซึ่งพยานหลักฐานอิเล็กทรอนิกส์ในการสืบสวนคดีอาญาของสหรัฐอเมริกาจึงได้กำหนดให้เจ้าหน้าที่ และอัยการควรที่จะต้องติดต่อ Office of International Affairs เพื่อประสานงานกับเจ้าหน้าที่ของต่างประเทศ

---

[27] "United States v. Ramirez, 112 F.3d 849, 852 (7th Cir. 1997) (Posner, C.J.)"(ศาลนำหลัก permissive construction of the territoriality provisions of Title III มาใช้); United States v. Denman, 100 F.3d 399, 402 (5th Cir. 1996); "United States v. Rodriguez, 968 F.2d 130, 135-36 (2d Cir. 1992)" (แม้มีการยึดหลักฐานที่อยู่ในท้องที่อื่นเกิดขึ้นโดยไม่ขอหมายในท้องที่นั้นก่อน ก็ไม่ทำให้หลักฐานนั้นเป็นหลักฐานที่ต้องห้ามนำเสนอต่อศาลหากเจ้าหน้าที่ดำเนินการโดยสุจริต และถือว่าเป็นการละเมิด U.S const. Amend 4 เพียงเล็กน้อย) ; "United States v. Burke, 517 F.2d 377, 386 (2d Cir. 1975) (Friendly, J.)"; "United States v. Martinez-Zayas, 857 F.2d 122, 136 (3d Cir. 1988)"

4. การพิจารณาเพื่อขอหมายประเภท "No-Knock" หรือ "Sneak-and-peek"

4.1 หมายที่ไม่ต้องแจ้งเตือน(No-knock Warrants)

ในกรณีทั่วไป เจ้าหน้าที่จะต้องแสดงตน และแจ้งให้ผู้ถูกค้นทราบก่อนที่จะปฏิบัติการตามหมายค้น[28] (18 U.S.C. § 3109.) หลักการนี้เรียกว่า Knock and announce อย่างไรก็ตามหลักการนี้มิใช้หลักการที่กำหนดว่าต้องปฏิบัติอย่างเคร่งครัด ทั้งนี้ ในคดี Richards v. Wisconsin 520 U.S. 385 (1997) ศาลฎีกาสหรัฐอเมริกาได้วางหลักว่า เจ้าหน้าที่ไม่จำต้องปฏิบัติตามหลัก Knock and announce หากเจ้าหน้าที่มีเหตุอันควรต้องสงสัยตามพฤติการณ์ว่าการแจ้งเตือนของเจ้าหน้าที่จะก่อให้เกิดอันตราย หรือ การค้นไม่ประสบความสำเร็จ หรือ ไม่มีประสิทธิภาพ เช่น มีการทำลายพยานหลักฐาน เป็นต้น

ในคดีที่เกี่ยวข้องกับคอมพิวเตอร์ เจ้าหน้าที่อาจจะต้องกระทำการค้นโดยไม่มีการแจ้งเตือน (No-knock)หากเจ้าหน้าที่สงสัยว่าการแจ้งเตือนก่อนค้น จะทำให้ผู้ต้องสงสัยมีเวลาพอที่จะทำลายหลักฐานเหล่านั้น โดยเจ้าหน้าที่อาจขอให้ศาลออกหมายประเภทไม่ต้องแจ้งเตือน(No-knock warrant)ก็ได้ อย่างไรก็ดี แม้เจ้าหน้าที่มีหมายไม่ต้องแจ้งเตือน (No-knock) เจ้าหน้าที่ก็สามารถตัดสินใจโดยใช้ดุลพินิจว่าตนจะกระทำการค้นโดยไม่ต้องแจ้งเตือนก็ได้เมื่อมีเหตุอันควรสงสัยว่า "การแจ้งเตือน และการแสดงตนจะก่อให้เกิดอันตราย หรืออาจทำให้การค้นไม่ประสบผลสำเร็จ หรือ การแจ้งเตือน และแสดงตนจะทำให้การค้นไม่มีประสิทธิภาพ เช่น อาจก่อให้เกิดการทำลายหลักฐาน" [29]

4.2 หมายซุ่มสังเกต (Sneak-and-Peak Warrants)

ศาลมีอำนาจที่ออกหมายลักลอบเข้าไป (Surreptitious entry warrants) หรือ หมาย Sneak-and-peak ซึ่งเจ้าหน้าที่ไม่จำเป็นต้องแจ้งให้บุคคลที่เป็นเจ้าของสถานที่ที่ถูกค้นทราบในเวลาที่ปฏิบัติการค้น (18 U.S.C. § 3103a, ซึ่งแก้ไขโดย The USA

---

[28] "Wilson v. Arkansas, 514 U.S. 927, 934 (1995)"

[29] "Richards, 520 U.S. at 395"

PATRIOT Act of 2001 § 213, Pub. L. No. 107-56, 115 Stat. 272 (2001) ศาลมีอำนาจที่จะให้ปฏิบัติการค้นตามหมายโดยให้แจ้งให้ทราบภายหลังได้(Delay Notice) ในกรณีที่มีเหตุอันควรเชื่อว่าหากมีการแจ้งว่าจะมีการปฏิบัติการค้นโดยทันทีจะทำให้การค้นตามหมายนั้นมีผลที่เปลี่ยนแปลงไป (18 U.S.C § 2705) กล่าวคือ ก่อให้เกิดอันตรายแก่ชีวิต หรือ ความปลอดภัยของร่างกายในบุคคล มีการหลีกเลี่ยงการดำเนินคดี การทำลายหลักฐาน การข่มขู่พยาน หรือ อาจจะก่อให้เกิดความเสียหายต่อการสืบสวน หรือ ก่อให้เกิดความล่าช้าโดยไม่เหมาะสมต่อการดำเนินคดี

นอกจากนี้ ตามมาตรา 3103a ได้กำหนดให้เจ้าหน้าที่กระทำการแจ้งให้ทราบภายหลังในช่วงเวลาที่เหมาะสม (Reasonable period) หลังจากที่ได้มีการปฏิบัติการค้นตามหมาย แต่ศาลอาจจะอนุญาตให้มีการแจ้งล่าช้าไปกว่านั้นอีกก็ได้หากมีเหตุผลที่ดีพอ แต่หลักการอนุญาตให้มีการแจ้งล่าช้า(Delay notice)ภายหลังจากการค้น จะไม่นำไปใช้กับการยึดด้วย ดังนั้น หากพนักงานสอบสวนต้องการลักลอบคัดลอกข้อมูลที่อยู่ในคอมพิวเตอร์ที่ต้องสงสัย พนักงานก็ควรจะได้รับอำนาจจากศาลเสียก่อน

<u>การค้นและยึดคอมพิวเตอร์โดยไม่ต้องมีหมาย (Searching and seizing computer without warrant)</u>

โดยหลักแล้วการค้นจะต้องมีหมาย เนื่องจาก Fourth Amendment บัญญัติว่า "สิทธิของบุคคลที่จะได้รับความปลอดภัยในร่างกาย ที่อยู่อาศัย เอกสาร และทรัพย์สินเกี่ยวกับบุคคล จากการค้นหรือยึดโดยไม่มีเหตุผลอันควรจะละเมิดมิได้ และหมายจะออกมิได้เว้นแต่มีเหตุอันควรซึ่งยืนยันโดยคำสาบาน หรือ คำรับรอง และจะต้องกำหนดถึงสถานที่ที่จะทำการค้น และบุคคลหรือสิ่งของ ที่จะมีการยึด" แต่แนวบรรทัดฐานของศาลฎีกาสหรัฐอเมริกา การค้นโดยไม่มีหมายจะไม่ถือเป็นการละเมิด Fourth Amendment หากเป็นไปตามเงื่อนไขประการใด ประการหนึ่งในสอง ประการดังต่อไปนี้

ก. หากการกระทำของหน่วยงานของมิได้ล่วงละเมิดต่อ "ความต้องการที่เหมาะสมในการมีความเป็นส่วนตัวของบุคคล (Person's reasonable expectation of privacy)" ถือเป็นการค้นโดยชอบ ดังนั้น การค้นนี้ไม่จำเป็นต้องมีหมาย [30]

---

[30] "Illinois v. Andreas, 463 U.S. 765, 771 (1983)"

ข. การค้นที่ไม่มีหมายที่ล่วงละเมิดต่อ ความต้องการที่เหมาะสมที่ในการมีความเป็นส่วนตัวของบุคคล จะถือว่า เหมาะสม (Reasonable) และชอบด้วยรัฐธรรมนูญ หากอยู่ในกรณีที่เป็นข้อยกเว้น (Exception) ของการค้นที่ต้องมีหมาย[31]

ก. การกระทำของหน่วยงานของมิได้ล่วงละเมิดต่อ "ความต้องการที่เหมาะสมในการมีความเป็นส่วนตัวของบุคคล (Person's Reasonable Expectation of Privacy) ถือเป็นการค้นโดยชอบ

การค้นจะถือว่าชอบด้วยรัฐธรรมนูญ ถ้ามิได้ล่วงละเมิด ความต้องการที่เหมาะสม (Reasonable expectation) หรือ ความต้องการที่ชอบด้วยกฎหมาย (Legitimate expectation) ในการมีความเป็นส่วนตัวของบุคคล เช่น ศาลฎีกาสหรัฐอเมริกาได้เคยตัดสินว่าบุคคลมีความต้องการที่เหมาะสมในการมีความเป็นส่วนตัวในเคหสถาน[32] ,ในค่าความร้อน (Relative heat) ที่ออกมาจากห้องที่อยู่ในบ้านซึ่งตรวจจับโดยเครื่องThermal imager[33],ในบทสนทนาทางโทรศัพท์[34] ในสิ่งของที่อยู่ในบรรจุภัณฑ์ซึ่งทึบ[35]

อย่างไรก็ตามในทางตรงกันข้าม บุคคลไม่อาจมีความต้องการที่เหมาะสมในการมีความเป็นส่วนตัวในกิจกรรมที่กระทำในสถานที่เปิดต่อสาธารณชน[36] ,ในขยะทิ้งอยู่ข้างนอกบ้าน[37] หรือในบ้านของคนแปลกหน้าซึ่งตนเข้าไปโดยปราศจากความยินยอมของเจ้าของบ้านโดยวัตถุประสงค์เพื่อกระทำการลักทรัพย์[38]

---

[31] "Illinois v. Rodriguez, 497 U.S. 177, 185 (1990)"

[32] "Payton v. New York, 445 U.S. 573, 589-90 (1980)"

[33] " Kyllo v. United States, 533 U.S. 27 (2001)"

[34] "Katz, 389 U.S. at 358"

[35] "United States v. Ross, 456 U.S. 798, 822-23 (1982)"

[36] "Oliver v. United States, 466 U.S. 170, 177 (1984)"

[37] "California v. Greenwood, 486 U.S. 35, 40-41 (1988)"

[38] "Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978)"

หลักการดังกล่าวข้างต้นนำมาใช้กับการค้น" ข้อมูลที่เก็บรักษาไว้ในเครื่องคอมพิวเตอร์"ด้วย โดยถือว่าคอมพิวเตอร์เสมือนหนึ่งเป็นกล่องที่ปิดอยู่ เช่นเดียวกับ กระเป๋าใส่ของ หรือ กล่องบรรจุไฟล์ ทั้งนี้ ตามหลักทั่วไป Fourth Amendment จะห้ามเจ้าหน้าที่ในการเข้าถึงข้อมูล และตรวจดูข้อมูลที่อยู่ในคอมพิวเตอร์โดยไม่มีหมาย เช่นเดียวกับที่ Fourth Amendment ห้ามเจ้าหน้าที่เปิดกล่องที่ปิดอยู่เพื่อตรวจสอบสิ่งที่อยู่ข้างใน[39]

อย่างไรก็ตามแม้ว่าโดยทั่วไปปัจเจกชนย่อมมีความต้องการที่เหมาะสมในการมีความเป็นส่วนตัวตามสมควรในเครื่องคอมพิวเตอร์ที่ตนใช้งาน แต่ในบางกรณีความต้องการนี้อาจจะถูกจำกัดได้ เช่น ปัจเจกชนย่อมไม่อาจมีความต้องการที่เหมาะสมในการมีความเป็นส่วนตัวในข้อมูลที่บุคคลนั้นได้ทำให้สาธารณชนเข้าถึงได้[40] หรือปัจเจกชนย่อมไม่อาจมีความต้องการที่เหมาะสมในการมีความเป็นส่วนตัวในสิ่งที่อยู่คอมพิวเตอร์ที่บุคคลนั้นขโมยมา[41]

นอกจากนี้ปัจเจกชนอาจจะต้องสูญเสียความคุ้มครองตาม Fourth Amendment เมื่อปัจเจกชนคนนั้นสูญเสียการครอบครองข้อมูลนั้นให้กับบุคคลภายนอก เช่น ในกรณีที่ปัจเจกชนนำภาชนะที่ใส่ข้อมูลทางอิเล็กทรอนิกส์ไปให้บุคคลภายนอกโดยนำเครื่องคอมพิวเตอร์ที่เสียไปร้านซ่อม หรือ ส่งแผ่น Floppy disk ทางจดหมายให้กับเพื่อ เว้นแต่ เป็นการส่งมอบการครอบครองไว้เป็นการชั่วคราว[42]

---

[39] "United States v. Blas, 1990 WL 265179, at *21 (E.D. Wis. Dec. 4, 1990)"

[40] "United States v. David, 756 F. Supp. 1385 (D. Nev. 1991)" (เจ้าหน้าที่ได้มองผ่านไหล่ของจำเลยเพื่อที่จะอ่าน password ของจำเลยบนจอขณะที่จำเลยพิมพ์ password ของตนลงบนคอมพิวเตอร์พกพา ในกรณีนี้ศาลเห็นว่าการกระทำของเจ้าหน้าที่มิได้เป็นการล่วงละเมิดต่อ Fourth Amendment ในการได้มาซึ่ง password เพราะไม่อาจถือได้ว่าจำเลยมีความต้องการที่เหมาะสมในการมีความเป็นส่วนตัว เนื่องจากจำเลยนำ password แสดงบนจอภาพ)

[41] "United States v. Lyons, 992 F.2d 1029, 1031-32 (10th Cir. 1993)"

[42] "United States v. Most, 876 F.2d 191, 197-98 (D.C. Cir. 1989) และ United States v. Barth, 26 F. Supp. 2d 929, 936-37 (W.D. Tex. 1998)" (ศาลเห็นว่าจำเลยยังคงมีความต้องการที่เหมาะสมในข้อมูลใน hard drive ที่อยู่ในคอมพิวเตอร์ซึ่งนำไปให้ช่างซ่อมคอมพิวเตอร์ซ่อมเพียงชั่วคราว)

อย่างไรก็ตาม หากเป็นข้อมูลที่ส่งผ่านระบบเครือข่ายอินเทอร์เน็ตย่อมไม่ได้รับความคุ้มครองตาม Fourth Amendment แต่อาจได้รับการคุ้มตามกฎหมายอื่น (ดู หัวข้อการควบคุมทางอิเล็กทรอนิกส์ในเครือข่ายสื่อสารต่อไป) ส่วนข้อมูลที่บันทึกไว้อื่นๆ เช่น รายชื่อลูกค้าที่จัดเก็บและเก็บรักษาโดยผู้ให้บริการทางอินเทอร์เน็ตเพื่อการประกอบธุรกิจ ย่อมไม่ถือว่ามีความต้องการที่เหมาะสมในการที่จะได้รับความเป็นส่วนตัวที่ได้รับการคุ้มครองตาม Fourth Amendment[43]

1. การค้นโดยเอกชน(Private Searches)

Fourth Amendment จะไม่นำไปใช้ในการค้นโดยเอกชนที่มิได้กระทำการในฐานะที่เป็นตัวแทนของหน่วยงานของรัฐหรือเข้าร่วมกับการกระทำการของหน่วยงานของรัฐหรือรู้ว่าเป็นการกระทำโดยหน่วยงานของรัฐใดๆ แม้ว่าการค้น หรือการยึดนั้นจะกระทำโดยไม่มีเหตุผลก็ตาม[44] เช่น ในคดี United States v. Hall, 142 F.3d 988 (7th Cir. 1998) จำเลยนำเครื่องคอมพิวเตอร์ของตนไปให้ผู้เชี่ยวชาญทางคอมพิวเตอร์ของเอกชนซ่อมแซม ในกระบวนการตรวจสอบคอมพิวเตอร์ของจำเลย พนักงานซ่อมคอมพิวเตอร์พบว่าไฟล์ที่อยู่ในคอมพิวเตอร์มีชื่อไฟล์ที่เกี่ยวข้องกับภาพลามกของเด็ก พนักงานซ่อมคอมพิวเตอร์จึงเข้าไปดูไฟล์เหล่านั้นและพบว่ามีภาพลามกของเด็กอยู่จริง จึงติดต่อเจ้าหน้าที่ตำรวจ และได้มีการขอออกหมายในเวลาต่อมา จำเลยจึงถูกจับกุมในข้อหาครอบครองภาพอนาจารของผู้เด็ก ในคดีนี้ศาลวินิจฉัยว่าการค้นของพนักงานซ่อมคอมพิวเตอร์กระทำการด้วยตนเอง และ Fourth Amendment จะไม่นำมาใช้กับการค้นโดยเอกชน

ในคดี United States v. Jacobsen, 466 U.S. 109 (1984) ศาลได้อธิบายขยายหลักการนี้ออกไปอีกโดยวินิจฉัยว่า เจ้าหน้าที่ที่ทราบถึงหลักฐานจากการค้นโดยเอกชนสามารถทำการค้นโดยต่อเนื่องจากเอกชนได้ โดยไม่ถือเป็นการละเมิดความต้องการที่เหมาะสมในการมีความเป็นส่วนตัว แต่สิ่งที่เจ้าหน้าที่ไม่สามารถกระทำการค้นได้ คือ "การค้นที่เกินกว่าการค้นของเอกชน"

---

[43] "United States v. Hambrick, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999), aff'd, 225 F.3d 656 (4th Cir. 2000)" (ศาลเห็นว่ามิได้มีการให้ความคุ้มครองบัญชีเครือข่ายข้อมูลของลูกค้าตาม Fourth Amendment ในข้อมูลที่ได้มาจากผู้ให้บริการอินเทอร์เน็ต)

[44] "United States v. Jacobsen, 466 U.S. 109, 113 (1984)"

อย่างไรก็ตาม หากการค้นของเจ้าหน้าที่เกินกว่าขอบเขตของการค้นของเอกชนที่ไม่มีหมาย หลักฐานที่ได้จากการค้นอาจจะต้องถูกยื่นคำร้องคัดค้านห้ามศาลรับฟังพยานหลักฐานดังกล่าว

ประเด็นที่สำคัญในเรื่องการค้นโดยเอกชน คือ แม้ข้อเท็จจริงปรากฏว่าบุคคลที่กระทำการค้นมิใช้ลูกจ้างของรัฐบาลก็ไม่ได้หมายความว่าการค้นโดยบุคคลนั้นจะถือเป็น "การค้นโดยเอกชน" ตาม Fourth Amendment เสมอไป โดยการค้นที่กระทำโดยเอกชนที่จะถือเป็นการค้นโดยรัฐ ตาม Fourth Amendment เมื่อ "การค้นโดยเอกชนกระทำในฐานะที่เป็นเครื่องมือของรัฐ หรือตัวแทนของรัฐ" ("if the private party act[s] as an instrument or agent of the Government."[45]

2.การใช้เทคโนโลยีเพื่อให้ได้มาซึ่งข้อมูล

(Use of technology to obtain Information)

การที่รัฐใช้นวัตกรรมทางเทคโนโลยีเพื่อให้ได้มาซึ่งข้อมูลที่ต้องการสามารถนำ Fourth Amendment มาปรับใช้ได้[46] ในคดี Kyllo นี้ศาลสูงสุดแห่งประเทศสหรัฐอเมริกาพิจารณาว่า การใช้เครื่อง Thermal imager เพื่อตรวจสอบปริมาณความร้อนที่มาจากห้องหลายห้องในบ้านที่ต้องสงสัยถือเป็นการค้นที่ล่วงละเมิดต่อ Fourth Amendment ศาลได้กล่าวประเด็นที่น่าสนใจไว้ว่าการที่เจ้าหน้าที่ของรัฐได้ใช้เครื่องมือที่สาธารณชนมิได้ใช้กันทั่วไป เพื่อตรวจสอบรายละเอียดเกี่ยวกับเคหสถานแม้จะไม่มีการรุกล้ำทางกายภาพ แต่การตรวจสอบเช่นนี้ก็ถือเป็น "การค้น"เมื่อไม่มีข้อเท็จจริงปรากฏว่ามีเหตุอันสมควรจึงไม่สามารถค้นได้โดยปราศจากหมายค้น

---

[45] "Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 614 (1989)"; "United States v. Lambert, 771 F.2d 83, 89 (6th Cir. 1985)" (ศาลวินิจฉัยว่า การกระทำของเอกชนจะถือเป็นการกระทำของรัฐตาม Fourth Amendment หากเจ้าหน้าที่ตำรวจช่วยเหลือ สนับสนุน หรือ เข้าร่วมการค้น และเอกชนกระทำการค้นโดยตั้งใจที่จะช่วยเหลือตำรวจในการสืบสวน)

[46] "Kyllo v. United States, 533 U.S. 27 (2001)"

การที่รัฐใช้นวัตกรรมทางเทคโนโลยีที่สาธารณชนทั่วไปมิได้ใช้เพื่อให้ได้มาซึ่งข้อมูลที่เก็บอยู่ในคอมพิวเตอร์หรือที่ส่งผ่านคอมพิวเตอร์ อาจจะต้องนำหลักการของคดี Kyllo มาใช้ ดังนั้น การกระทำเช่นนี้จึงจำเป็นที่จะต้องมีหมาย ทั้งนี้ การใช้เทคโนโลยีที่อยู่ภายใต้ขอบเขตของ Kyllo จะขึ้นอยู่กับหลักการอย่างน้อย 2 ประการ คือ (1) การใช้เทคโนโลยีที่จะไม่นำหลัก Kyllo มาใช้จะต้องเป็นเทคโนโลยีที่สาธารณชนใช้โดยทั่วไป (General public use) (2) ศาลฎีกาสหรัฐอเมริกาจำกัดการนำ Kyllo ไปใช้เฉพาะในกรณีที่เป็นเทคโนโลยีที่เปิดเผยข้อมูลนั้นเกี่ยวกับ "เคหะสถาน"

ข.การค้นที่ไม่มีหมายที่ล่วงละเมิดต่อความต้องการที่เหมาะสมที่ในการมีความเป็นส่วนตัวของบุคคล จะถือว่า "เหมาะสม (reasonable)" (และชอบด้วยรัฐธรรมนูญ) หากอยู่ในกรณีที่เป็นข้อยกเว้น (Exception) ของการค้นที่ต้องมีหมาย

โดยปกติแล้วการค้นที่ไม่มีหมาย ถือเป็นการล่วงละเมิดต่อสิทธิในความเป็นส่วนตัว แต่ในบางกรณี ถือเป็นข้อยกเว้นที่เจ้าหน้าที่สามารถกระทำได้โดยไม่จำเป็นต้องมีหมายและถือว่าเป็นการค้นโดยชอบด้วยกฎหมายและชอบด้วยรัฐธรรมนูญ ดังนี้

1. ความยินยอม (Consent)

เจ้าหน้าที่สามารถทำการค้นได้โดยไม่ต้องมีหมายหากได้รับความยินยอมโดยสมัครใจจากผู้มีอำนาจให้ความยินยอมในการค้น[47]ความยินยอมนี้อาจกระทำโดยการยินยอมโดยชัดเจน(Explicit) หรือโดยปริยาย(Implicit)[48] โดยศาลจะพิจารณาจากสภาพแวดล้อมโดยรวมในขณะนั้น รวมถึงปัจจัยอื่นๆ เช่น อายุ การศึกษา สติปัญญา ,สภาพร่างกายหรือจิตใจของผู้ให้ความยินยอม,พิจารณาว่าบุคคลนั้นถูกจับกุมแล้วหรือไม่,บุคคลนั้นปฏิเสธที่จะให้ความยินยอมหรือไม่[49] รัฐมีภาระการพิสูจน์(Burden of proving)ว่าความยินยอมนั้นเป็นไปโดยสมัครใจ[50]

---

[47] "Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973)."

[48] "United States v. Milian-Rodriguez, 759 F.2d 1558, 1563-64 (11th Cir. 1985)"

[49] "Schneckloth, 412 U.S. at 226"

[50] "United States v. Matlock, 415 U.S. 164, 177 (1974); United States v. Price, 599 F.2d 494, 503 (2d Cir. 1979)."

1.1 ขอบเขตความยินยอม (Scope of consent)

ในคดีความผิดเกี่ยวกับคอมพิวเตอร์อาจเกิดปัญหาในการพิจารณาว่าการค้นโดยความยินยอมมีขอบเขตครอบคลุมเพียงใด ซึ่งตามแนวคำพิพากษามีแนวทางดังนี้ "ขอบเขตความยินยอมในการค้นโดยทั่วไปอธิบายได้จากการแสดงออกและถูกจำกัดโดยความยินยอมที่ได้ให้ไว้" ขอบเขตความยินยอมสามารถพิจารณาได้จากความสามารถในการสื่อสารระหว่างเจ้าหน้าที่และผู้ให้ความยินยอมโดยพิจารณาในระดับวิญญูชน (Reasonable person)[51] ในกรณีที่ความยินยอมได้ให้ไว้โดยจำกัด เจ้าหน้าที่ต้องทำการค้นโดยให้ความเคารพกับข้อจำกัดนั้น[52] โดยขอบเขตของการค้นจะขึ้นอยู่กับข้อเท็จจริงเป็นรายกรณีไป เช่น การได้รับความยินยอมให้มองเข้าไปในรถ (Look inside the car)รวมถึง การตรวจสอบเบอร์ที่ค้างอยู่ในเพจเจอร์ที่พบหลังที่นั่งท้ายรถ[53] แต่การให้ความยินยอมให้การให้ดูเพจเจอร์(Look at a pager) หมายถึงให้ดูเพื่อทราบว่าใช้วัสดุใด ยี่ห้อใด ขนาดเท่าใดเท่านั้น ไม่รวมถึงอนุญาตให้ตรวจสอบเบอร์ที่ค้างอยู่ในเพจเจอร์[54] หรือ การให้ความยินยอมเป็นลายลักษณ์อักษรระบุว่า "...ยินยอมให้ค้นทรัพย์สินใดที่อยู่ในการควบคุมของจำเลยและให้การค้นทรัพย์สินหรือหลักฐานตามที่อยู่ของจำเลยสำเร็จลุล่วง..." ("...any property" under the defendant's control and to "a complete search of the premises and property" at the defendant's address...") หมายถึงการค้นในที่อยู่อาศัยของจำเลยเท่านั้น แต่ไม่รวมถึงการยึดคอมพิวเตอร์และทำการค้นนอกสถานที่นั้น(Off-site) เพราะไม่ถือว่าสิ่งของนั้นตั้งอยู่ในที่อยู่อาศัยของจำเลย เป็นต้น

เพื่อป้องกันปัญหาการตีความว่าความยินยอมนั้นมีขอบเขตเพียงใด ในทางปฏิบัติจึงแนะนำให้เจ้าหน้าที่ใช้แบบฟอร์มการให้ความยินยอมเป็นลายลักษณ์อักษรเพื่อจะได้ทราบขอบเขตความยินยอมโดยชัดแจ้งว่า การยินยอมให้ค้นนั้นรวมถึงการยินยอมให้ค้นคอมพิวเตอร์และข้อมูลอิเล็กทรอนิกส์ที่บรรจุในคอมพิวเตอร์นั้นด้วย [55]

---

[51] "Florida v. Jimeno, 500 U.S. 248, 251 (1991)."

[52] "Vaughn v. Baldwin, 950 F.2d 331, 333 (6th Cir. 1991)."

[53] "United States v. Reyes, 922 F. Supp. 818, 834 (S.D.N.Y. 1996)."

[54] "United States v. Blas, 1990 WL 265179, at *20 (E.D. Wis. Dec. 4, 1990)."

[55] Computer Crime and Intellectual Property Section Criminal Division United States Department of Justice, Searching and Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations , pp. 12-13

1.2 ผู้มีอำนาจให้ความยินยอม

โดยหลักแล้ว ผู้มีอำนาจให้ความยินยอมคือเจ้าของ(Owner)หรือผู้ใช้(User)คอมพิวเตอร์นั้น นอกจากนี้บางกรณียังให้อำนาจบุคคลภายนอกในการให้ความยินยอม(Third party consent)อีกด้วย ได้แก่

1. ผู้ร่วมใช้คอมพิวเตอร์(Co-users of computer) ในกรณีที่มีเจ้าของร่วมหรือผู้ร่วมใช้คอมพิวเตอร์หลายคน หากคนใดคนหนึ่งให้ความยินยอม เจ้าหน้าที่ย่อมดำเนินการค้นได้ โดยศาลฎีกาสหรัฐถือว่าเป็นอำนาจทั่วไป(Common authority)ในการให้ความยินยอมในกรณีที่เจ้าของร่วมหรือผู้ใช้ร่วมคนอื่นไม่อยู่[56] และในกรณีที่ทรัพย์สินนั้นอยู่ในการควบคุมของบุคคลภายนอก บุคคลภายนอกย่อมมีอำนาจทั่วไปในการให้เจ้าหน้าที่ตรวจสอบ โดยไม่เป็นการละเมิด U.S const. Amend 4[57] หรือผู้หญิงสามารถให้ความยินยอมต่อเจ้าหน้าที่ในการค้นคอมพิวเตอร์ของเพื่อนชาย(Boyfriend)ที่ตั้งอยู่ในบ้านของพวกเขาได้[58] แต่ไม่รวมถึงกรณีที่ไม่ได้มีการใช้รหัสผ่านไฟล์ร่วมกัน (Has not shared the passwords with others)และไฟล์นั้นใส่รหัสผ่านไว้ (Password-protected files)[59] แต่หากได้มีการมอบรหัสผ่านให้ผู้ใช้ร่วม(Co-user) ผู้ใช้ร่วมก็มีอำนาจทั่วไปในการยินยอมให้มีการค้นไฟล์นั้น[60]

---

[56] "United States v. Matlock, 415 U.S. 164 (1974)."

[57] "United States v. Jacobsen, 466 U.S. 109, 119 (1984)"; "United States v. Block, 590 F.2d 535, 541 (4th Cir. 1978)" (แม่สามารถให้ความยินยอมในการค้นห้องนอนลูกชายอายุ 23 ปีได้ แต่ไม่รวมถึงการค้นหีบที่ใส่กุญแจ(Locked footlockers) ที่อยู่ในห้องนอนนั้น); "United States v. Sumlin, 567 F.2d 684, 687-88 (6th Cir. 1977)"(ผู้หญิงสามารถให้ความยินยอมในการค้นห้องได้ แม้เพื่อนชายที่อาศัยอยู่ด้วยกันปฏิเสธไม่ให้ความยินยอม)

[58] "United States v. Smith, 27 F. Supp. 2d 1111, 1115-16 (C.D. Ill. 1998)"

[59] "Trulock v. Freeh, 275 F.3d 391, 403-04 (4th Cir. 2001)" (เทียบได้กับกรณีหีบที่ใส่กุญแจ(locked footlockers)ในห้องนอน)

[60] "United States v. Murphy, 506 F.2d 529, 530 (9th Cir. 1974)"(เทียบเคียงกับกรณีที่นายจ้างสามารถให้ความยินยอมในการค้นโกดังของลูกจ้างได้ เมื่อข้อเท็จจริงปรากฏว่า นายจ้างครอบครองกุญแจของลูกจ้าง โดยลูกจ้างเป็นผู้ส่งมอบแก่นายจ้างด้วยตนเอง)

2. <u>คู่สมรสและผู้ร่วมอาศัย(Spouses and Domestic partner)</u> เมื่อผู้มีอำนาจให้ความยินยอมไม่อยู่ในที่นั้น คู่สมรสสามารถให้ความยินยอมได้[61] เช่น ในคดีหนึ่งที่ภรรยายินยอมให้ทำการค้นคอมพิวเตอร์ของสามีในบ้าน แม้ว่าภรรยาจะแทบไม่ได้ใช้คอมพิวเตอร์ของสามีเลยก็ตาม ศาลก็ถือว่าเป็นการให้ความยินยอมโดยชอบ โดยศาลให้เหตุผลว่าเธอไม่ได้ถูกสามีปฏิเสธไม่ให้เข้าไปในห้องที่เก็บคอมพิวเตอร์และสามีก็ไม่ได้ใส่รหัสผ่านไฟล์ไว้(Password-protected files)[62]

3. <u>ผู้ปกครอง (Parents)</u> ผู้ปกครองสามารถให้ความยินยอมในการค้นห้องของบุตรได้ หากบุตรอายุต่ำกว่า18 ปี แต่ในกรณีบุตรอายุเกินกว่า 18 ปีการให้ความยินยอมโดยผู้ปกครองจำเป็นต้องพิจารณาข้อเท็จจริงเป็นรายกรณีไป โดยพิจารณาว่าหากบุตรมีอายุพอสมควรแล้ว,จ่ายค่าเช่าห้องและ/หรือ ปฏิเสธที่จะให้ผู้ปกครองเข้าไปหรือเป็นพื้นที่ส่วนตัว ผู้ปกครองย่อมไม่มีอำนาจให้ความยินยอม[63] เช่น กรณีที่บุตรชายอายุ 24 ปี เปลี่ยนกุญแจห้องโดยไม่บอกกล่าวกับมารดา และจ่ายค่าเช่าห้องนั้น มารดาย่อมไม่มีอำนาจให้ความยินยอม[64]

4. <u>ผู้จัดการระบบ (System Administrators)</u> ในกรณีการค้นเครือข่าย(Network) มีความจำเป็นที่จะต้องประสานงานกับผู้จัดการระบบหรือผู้คุมระบบ (System AdministratorหรือSystem operator) เพื่อขอความยินยอมในการค้นข้อมูลของผู้กระทำความผิดตามรายชื่อลูกค้า(Account)ที่เจ้าหน้าที่ได้สืบทราบ

---

[61] "United States v. Duran, 957 F.2d 499, 504-05 (7th Cir. 1992)" (ภรรยาสามารถให้ความยินยอมในการค้นยุ้งข้าวที่เธอมิได้ใช้ได้ เพราะสามีมิได้ปฏิเสธไม่ให้เธอเข้าไป); "United States v. Long, 524 F.2d 660, 661 (9th Cir. 1975)"(ภรรยาที่มิได้อยู่กับสามี สามารถให้ความยินยอมในการค้นบ้านที่เป็นกรรมสิทธิ์รวมได้แม้ว่าสามีเธอจะเปลี่ยนกุญแจบ้านแล้วก็ตาม)

[62] "United States v. Smith, 27 F. Supp. 2d 1111 (C.D. Ill. 1998)."

[63] "United States v. Whitfield, 939 F.2d 1071, 1075 (D.C. Cir. 1991)."

[64] "United States v. Durham, 1998 WL 684241, at *4 (D. Kan. Sept. 11, 1998)" ; "United States v. Rith, 164 F.3d 1323, 1331 (10th Cir. 1999)"(ผู้ปกครองยินยอมให้ค้นห้องบุตรอายุ18ปีได้ เพราะเขามิได้จ่ายค่าเช่า)และ United States v. Block, 590 F.2d 535, 541 (4th Cir. 1978)(แม่ให้ความยินยอมในการค้นห้องลูกชายอายุ23 ปีได้ เพราะเขามิได้จ่ายค่าเช่า)

การขอความยินยอมในกรณีนี้เป็นอำนาจที่เจ้าหน้าที่มีตามกฎหมาย(Statutory) ไม่ใช่ความชอบตามรัฐธรรมนูญ (Constitutional) โดยพิจารณาจาก Electronic communications Privacy Act (ECPA) โดยถือว่าผู้จัดการระบบเป็น "ผู้ให้บริการการสื่อสารอิเล็กทรอนิกส์"(Provider(s) of electronic communication service)(18 U.S.C. §§ 2701-2712) มีหน้าที่ในการให้ความร่วมมือกับเจ้าหน้าที่ในการค้นหมายเลขบัญชีที่ระบุตัวบุคคล(Individual's account)(18 U.S.C. § 2702-2703)

2. สถานการณ์ฉุกเฉิน (Exigent Circumstances)

ในกรณี "สถานการณ์ฉุกเฉิน" (Exigent Circumstances) ถือเป็นกรณีที่สามารถค้นได้โดยไม่ต้องมีหมาย[65] ในการพิจารณาว่ากรณีใดเป็นสถานการณ์ฉุกเฉิน เจ้าหน้าที่จะพิจารณาจาก 1.) ระดับของสภาพความเร่งด่วน 2.) ระยะเวลาที่จำเป็นในการขอหมาย 3.) หลักฐานอาจถูกเคลื่อนย้ายหรือทำลายหรือไม่ 4.) อันตรายที่อาจเกิดขึ้นได้ในสถานที่นั้น 5.) ข้อมูลระบุว่าผู้ครอบครองสิ่งผิดกฎหมายทราบว่าตำรวจกำลังดำเนินการติดตามอยู่ 6.) สิ่งผิดกฎหมายนั้นมีความพร้อมที่จะถูกทำลาย [66]

สถานการณ์ฉุกเฉิน(Exigent Circumstances) อาจเกิดขึ้นได้เสมอในคดีเกี่ยวกับคอมพิวเตอร์ เพราะข้อมูลอิเล็กทรอนิกส์สามารถถูกทำลายได้โดยง่ายและใช้เวลาอันรวดเร็ว ไม่ว่าจะโดยความชื้น, อุณหภูมิ, การถูกทำลายทางกายภาพหรือสนามแม่เหล็ก ยกตัวอย่างเช่นในคดีหนึ่งเจ้าหน้าที่พบเห็นจำเลยกำลังลบข้อมูลบันทึกช่วยจำ(Memo book)ที่บรรจุอยู่ในคอมพิวเตอร์ของจำเลย เจ้าหน้าที่จึงทำการยึดคอมพิวเตอร์นั้นในทันที ศาลในคดีนั้นวินิจฉัยว่า เจ้าหน้าที่สามารถยึดได้โดยไม่ต้องมีหมายเพราะถือได้ว่าการกระทำของจำเลยเป็นกรณีสถานการณ์ฉุกเฉิน [67] และในอีกคดีหนึ่งศาลวินิจฉัยว่า เจ้าหน้าที่มีอำนาจตรวจสอบข้อมูลในเพจเจอร์ได้ตามสมควรโดยไม่ต้องมีหมาย เมื่อมีเหตุอันควรเชื่อได้ว่าผู้ต้องสงสัยอาจทำลายพยานหลักฐานนั้น เพราะข้อความที่เก็บไว้ในเพจเจอร์สามารถลบได้อย่างรวดเร็ว ,แบตเตอร์รี่อาจหมดและทำให้ข้อมูลสูญหายไปได้[68]หรือการดาวน์โหลดและทำสำเนาข้อมูลโดยไม่

---

[65] "United States v. McConney, 728 F.2d 1195, 1199 (9th Cir. 1984)."

[66] "United States v. Reed, 935 F.2d 641, 642 (4th Cir. 1991)."

[67] "United States v. David, 756 F. Supp. 1385 (D. Nev. 1991)."

[68] "United States v. Romero-Garcia, 991 F. Supp. 1223, 1225 (D. Or. 1997)."

มีหมาย ในกรณีที่มีเหตุควรเชื่อว่าคอมพิวเตอร์ของรัสเซียกำลังจะทำลายข้อมูลที่เป็นพยานหลักฐาน[69] อย่างไรก็ดี การพิจารณาสถานการณ์ฉุกเฉินจำเป็นต้องพิจารณาข้อเท็จจริงที่เกิดขึ้นเป็นกรณีไป และสถานการณ์ฉุกเฉินมีอยู่เท่าที่จำเป็นต่อการป้องกันการทำลายพยานหลักฐานเท่านั้น เจ้าหน้าที่ไม่อาจอ้างเหตุดังกล่าวในการไม่ขอหมายค้นเมื่อสถานการณ์ฉุกเฉินดังกล่าวผ่านพ้นไปได้[70] และในการ "ยึด"อุปกรณ์คอมพิวเตอร์(Hardware)เพื่อป้องกันการทำลายหลักฐาน ไม่เป็นเหตุให้สามารถ"ค้น"ข้อมูลโดยไม่ต้องมีหมายได้

3.สิ่งที่พบเห็นได้โดยง่าย (Plain View)

หลักฐานที่เกิดขึ้นจากการกระทำความผิดอาญาอาจจะถูกยึดได้โดยไม่ต้องมีหมายตามข้อยกเว้นเรื่องสิ่งที่พบเห็นได้โดยง่าย (Plain View) ซึ่งเป็นข้อยกเว้นของการค้นที่ต้องมีหมาย ภายใต้ข้อยกเว้นนี้เจ้าหน้าที่จะต้องอยู่ในฐานะที่ชอบด้วยกฎหมายในการเข้าไปตรวจสอบ และเข้าถึงพยานหลักฐาน และจะต้องปรากฏว่าหลักฐานนั้นมีลักษณะที่เกี่ยวข้องกับการกระทำความผิดอาญา[71] เจ้าหน้าที่ได้กระทำการค้น Hard drive โดยชอบด้วยกฎหมาย โดยในขณะที่ค้นได้พบกับหลักฐานการกระทำความผิดอาญาในคดีที่ไม่ได้เกี่ยวข้องกับคดีแรก ในกรณีนี้เจ้าหน้าที่สามารถยึดหลักฐานนั้นได้ตามหลักสิ่งที่พบเห็นได้โดยง่าย (Plain View)

ในการนำหลักการนี้มาใช้กับคดีที่เกี่ยวข้องกับคอมพิวเตอร์ย่อมจะหมายความว่ารัฐไม่อาจใช้ข้อยกเว้นเรื่องสิ่งที่พบเห็นโดยชัดแจ้ง (Plain View) มาใช้กับการเข้าเปิดไฟล์คอมพิวเตอร์ให้ถือเป็นการกระทำที่ชอบด้วยกฎหมายได้ หากเจ้าหน้าที่ไม่มีอำนาจในการเข้าตรวจ ในกรณีที่การเข้าไปตรวจเนื้อหาของไฟล์ได้จะต้องมีการเปิดออกเสียก่อนจะย่อมไม่ว่าเป็นไปตามข้อยกเว้นเรื่องสิ่งที่พบเห็นโดยง่าย (Plain View)[72] หลักการนี้เป็นไปตามบรรทัดฐานที่มีการนำข้อยกเว้นเรื่อง Plain View ไปใช้กับกล่องบรรจุเอกสารที่ปิดอยู่

---

[69] "United States v. Gorshkov, 2001 WL 1024026, at *4 (W.D. Wash. May 23, 2001)."

[70] "United States v. Doe, 61 F.3d 107, 110-11 (1st Cir. 1995)."

[71] "Horton v California, 496 U.S. 128 (1990)"

[72] "United States v. Maxwell, 45 M.J. 406, 422 (C.A.A.F. 1996)"; "United States v. Villarreal, 963 F.2d 770, 776 (5th Cir. 1992)" (ศาลพิเคราะห์ว่า ป้ายที่ติดอยู่กับภาชนะที่มีลักษณะทึบน้ำหนัก 55 แกลอนมิได้แสดงให้เห็นถึงสิ่งที่อยู่ข้างในภาชนะได้โดยง่าย) (ป้ายที่อยู่บนภาชนะไม่ถือเป็นเหตุให้มีการค้นภายในภาชนะนั้นได้ หากรัฐต้องการที่จะทราบถึงสิ่งที่อยู่ภายในมากกว่าข้อความที่ปรากฏอยู่บนป้าย โดยวิธีการเปิดภาชนะนั้น รัฐจะต้องกระทำการค้นโดยมีหมาย)

ในคดี United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999) ศาลได้แสดงให้เห็นถึงข้อจำกัดของหลักการนี้ โดยในคดี Carey เจ้าหน้าที่ตำรวจได้ค้นใน Hard drive โดยมีหมายเพื่อหาหลักฐานในคดีการค้ายาเสพติด และได้เปิดไฟล์ในรูปแบบ JPG แต่กลับพบภาพอนาจารของผู้เยาว์ เมื่อเป็นเช่นนี้เจ้าหน้าตำรวจได้ใช้เวลา 5 ชั่วโมงในการเข้าไปถึงไฟล์ และดาวน์โหลดไฟล์รูปแบบ JPG หลายร้อยไฟล์ในการค้นนั้น แต่ไม่ได้ค้นหลักฐานจากการค้ายาเสพติดตามหมายเดิมแต่เจ้าหน้าที่ทำไปเพื่อค้นรูปอนาจารของผู้เยาว์เพิ่มเติม ในคดีนี้จำเลยจึงได้ร้องขอให้ศาลไม่รับฟังไฟล์ที่เป็นรูปอนาจารของผู้เยาว์เป็นพยาน โดยให้เหตุผลว่าการยึดของเจ้าหน้าที่ตำรวจเป็นการกระทำที่เกินขอบเขตของการค้น แต่หน่วยงานราชการเห็นว่าการยึดไฟล์ JPF ของเจ้าหน้าที่นั้นเป็นการกระทำที่ชอบด้วยกฎหมาย เพราะเหตุว่า เจ้าหน้าที่สามารถยึดไฟล์ที่เป็นผิดกฎหมายได้ตามข้อยกเว้นเรื่องสิ่งที่พบเห็นได้โดยชัดแจ้ง (Plain View) ในคดีนี้ศาลได้ปฏิเสธข้อกล่าวอ้างของหน่วยงานราชการในส่วนที่เกี่ยวข้องกับไฟล์ทุกไฟล์ยกเว้นแต่ไฟล์ JPG ไฟล์แรกที่เจ้าหน้าที่ได้ค้นเจอ

อย่างไรก็ตาม ในคดี United States v. Runyan, 275 F.3d 449, 464-65 (5th Cir. 2001), และคดี United States v. Slanina, 283 F.3d 670, 680 (5th Cir. 2002) ศาลเห็นว่า สิ่งที่พบได้โดยง่าย (Plain View) ในไฟล์หนึ่งบนคอมพิวเตอร์ หรือ ภาชนะที่มีไว้เก็บของสามารถเป็นหลักการพื้นฐานในการค้นเพิ่มเติมได้ ทั้งนี้ ในคดีที่ 2 คดีที่กล่าวมานี้ ศาลเห็นว่า การค้นโดยไม่มีหมายในส่วนหนึ่งของคอมพิวเตอร์ หรืออุปกรณ์เก็บของที่กระทำไปชอบด้วยกฎหมาย ย่อมทำให้จำเลยไม่อาจที่จะมีความต้องการที่เหมาะสมในการมีความเป็นส่วนตัว (reasonable expectation of privacy) ในส่วนที่อื่นของคอมพิวเตอร์หรือส่วนอื่นของภาชนะนั้นได้อีกต่อไป[73] ดังนั้น การที่เจ้าหน้าที่ค้นโดยเจ้าหน้าที่ผู้บังคับใช้กฎหมายเพิ่มเติมคอมพิวเตอร์หรือภาชนะเก็บของเพิ่มเติมจากก็ไม่ถือเป็นการละเมิด Fourth Amendment เมื่อไฟล์นั้นอยู่ส่วนเห็นได้โดยง่าย (plain view)

4. การค้นอันเนื่องมาจากการจับกุมโดยชอบด้วยกฎหมาย (Search Incident to Lawful Arrest)

เมื่อดำเนินการจับกุมโดยชอบด้วยกฎหมาย เจ้าหน้าที่อาจดำเนินการค้นตัวผู้ถูกจับกุมโดยละเอียด(Full search) รวมถึงพื้นที่โดยรอบ

---

[73] "Slanina, 283 F.3d at 680; Runyan, 275 F.3d at 464-65."

(Surrounding area) โดยไม่ต้องมีหมายได้ เช่น ในคดีหนึ่งเจ้าหน้าที่ได้จับกุมผู้กระทำผิดกฎจราจร ภายหลังการจับกุมเจ้าหน้าที่พบห่อบุหรี่ที่บรรจุเฮโรอีนในกระเป๋าเสื้อของผู้ถูกจับกุม ศาลฎีกาสหรัฐวินิจฉัยว่าการค้นเป็นไปโดยชอบ แม้ว่าเจ้าหน้าที่จะไม่มีเหตุผลเชื่อมโยงในการเปิดห่อบุหรี่นั้นก็ตาม[74] หลักการนี้แสดงให้เห็นว่าศาลให้ความสำคัญกับการรวบรวมพยานหลักฐานและการป้องกันเจ้าหน้าที่จากภยันตรายจากการจับกุม จึงอนุญาตให้ทำการค้นภายหลังการจับกุมโดยชอบด้วยกฎหมายได้

ในปัจจุบัน ผู้คนจำนวนมากใช้คอมพิวเตอร์หรืออุปกรณ์เก็บข้อมูลอิเล็กทรอนิกส์อื่นที่สามารถพกพาได้สะดวก ดังนั้น หากเจ้าหน้าที่จับกุมโดยชอบก็อาจค้นพบเพจเจอร์ โทรศัพท์มือถือ คอมพิวเตอร์พกพา หรืออุปกรณ์เล็กทรอนิกส์อื่น(เช่น Palm pilots) เจ้าหน้าที่จึงอาจใช้อำนาจค้นได้อุปกรณ์ทั้งหลายดังกล่าวได้โดยไม่ต้องมีหมาย[75] เทียบเคียงได้กับกรณีที่เจ้าหน้าที่สามารถค้นกระเป๋าสตางค์ที่พบในตัวผู้ถูกจับได้[76]หรือกรณีที่เจ้าหน้าที่สามารถทำสำเนาภาพถ่ายสมุดจดที่อยู่(Address book)ที่พบในระหว่างจับกุม[77] ดังนั้น หลักการเดียวกันนี้จึงอาจนำมาปรับใช้กับการค้นคอมพิวเตอร์หรืออุปกรณ์เก็บข้อมูลอิเล็กทรอนิกส์อื่นได้[78]

---

[74] เทียบเคียง United States v. Robinson, 414 U.S. 218, 235 (1973) และ Chimel v. California, 395 U.S. 752, 762-63 (1969).

[75] United States v. Reyes, 922 F. Supp. 818, 833 (S.D.N.Y. 1996) (ภายหลังการจับกุม 12 นาที เจ้าหน้าที่พบเพจเจอร์ในถุงที่เก็บไว้ในเก้าอี้รถเข็น(wheelchair) จึงมีอำนาจตรวจสอบหมายเลขที่ค้างอยู่ในเครื่องได้ โดยไม่ต้องมีหมาย) และ United States v. Chan, 830 F. Supp. 531, 535 (N.D. Cal. 1993); United States v. Lynch, 908 F. Supp. 284, 287 (D.V.I. 1995); Yu v. United States, 1997 WL 423070, at *2 (S.D.N.Y. Jul. 29, 1997); United States v. Thomas, 114 F.3d 403, 404 n.2 (3d Cir. 1997) (dicta), United States v. Ortiz, 84 F.3d 977, 984 (7th Cir. 1996) (แต่กรณีเหล่านี้ ศาลปรับใช้หลัก สถานการณ์ฉุกเฉิน (Exigent Circumstances))

[76] United States v. Castro, 596 F.2d 674, 676 (5th Cir. 1979); United States v. Molinaro, 877 F.2d 1341, 1347 (7th Cir. 1989) (citing cases).

[77] United States v. Rodriguez, 995 F.2d 776, 778 (7th Cir. 1993) และ United States v. Johnson, 846 F.2d 279, 283-84 (5th Cir. 1988); United States v. Lam Muk Chiu, 522 F.2d 330, 332 (2d Cir. 1975).(เจ้าหน้าที่สามารถค้นกระเป๋าเอกสารได้)

[78] United v. Tank, 200 F.3d 627, 632 (9th Cir. 2000) (ในขณะจับกุม เจ้าหน้าที่ค้นรถยนต์ของผู้ต้องสงสัยพบ Zipdisk และสามารถทำการยึด(Seize) Zipdisk ได้โดยชอบ, แต่ในคดีนี้ไม่มีประเด็นโต้แย้งว่าการค้น(Searchi)และทำสำเนาข้อมูล(Image)ภาพลามกอนาจารเด็กที่พบในZipdisk เป็นไปโดยชอบหรือไม่)

อย่างไรก็ดีหลักการนี้จำเป็นต้องใช้อย่างจำกัด โดยจะใช้ได้เมื่อมีเหตุผลสมควร[79] การค้นสิ่งของที่พบในตัวผู้ถูกจับกุมถือว่ามีเหตุผลสมควร แต่การค้นในลักษณะรุกรานเกินสมควรอาจเป็นการละเมิด U.S const. Amend 4[80] ดังนั้น เจ้าหน้าที่จึงควรใช้หลักการค้นในกรณีนี้อย่างระมัดระวัง และควรให้ความสำคัญกับพยานหลักฐานในฐานความผิดหลัก(หรือความผิดตามหมาย กรณีที่มีหมาย) ก่อนการพิจารณาเนื้อหาของพยานหลักฐานอิเล็กทรอนิกส์ที่พบในการจับกุม[81]

5. การค้นเพื่อแสดงรายละเอียดวัตถุที่ได้ยึดมา (Inventory searches)

เจ้าหน้าที่มักจะกระทำการแสดงรายละเอียดวัตถุที่ตนได้ทำการยึดมา ทั้งนี้ การค้นเพื่อแสดงรายละเอียดนี้จะถือเป็นการกระทำที่เหมาะสม การค้นเพื่อแสดงรายละเอียดย่อมทำให้การค้นนั้นอยู่ภายใต้ข้อยกเว้นของการค้นที่ต้องมีหมาย เมื่อการกระทำนั้นเป็นไปตามเงื่อนไข 2 ประการนี้

เงื่อนไขประการแรก การค้นจะต้องกระทำโดยชอบด้วยกฎหมาย และกระทำไปโดยไม่มีวัตถุประสงค์เพื่อการสอบสวน (เช่น ป้องกันการสูญหาย ขโมย หรือถูกทำลายซึ่งทรัพย์สินที่เจ้าหน้าที่ได้เก็บรักษาไว้ หรือเพื่อป้องกันอันตรายที่อาจเกิดขึ้นกับตำรวจ) (Illinois v. Lafayette, 462 U.S. 640, 644 (1983); South Dakota v. Opperman, 428 U.S. 364, 369-70 (1976).

เงื่อนไขประการที่สอง การค้นจะต้องกระทำการตามกระบวนการมาตรฐาน (Standardize procedure) (Colorado v. Bertine, 479 U.S. 367, 374 n.6 (1987); Florida v. Wells, 495 U.S. 1, 4-5 (1990)

---

[79] "Swain v. Spinney, 117 F.3d 1, 6 (1st Cir. 1997)"

[80] "Mary Beth G. v. City of Chicago, 723 F.2d 1263, 1269-71 (7th Cir. 1983)"

[81] Computer Crime and Intellectual Property Section Criminal Division United States Department of Justice, Searching and Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, p. 19.

การค้นเพื่อแสดงรายละเอียดที่เป็นข้อยกเว้นของการค้นที่ต้องมีหมายนี้ไม่อาจนำมาใช้กับการค้นเครื่องไฟล์ในคอมพิวเตอร์ในเครื่องคอมพิวเตอร์ที่ถูกยึดมาได้[82] ในกรณีเช่นว่านี้แม้กระบวนการค้นตามมาตรฐานได้ให้อำนาจการค้นเช่นว่านั้น แต่ในประเด็นเรื่องวัตถุประสงค์ของการค้นโดยชอบด้วยกฎหมายไม่อาจแปลความว่าการค้นเพื่อแสดงรายละเอียดในวัตถุที่จับต้องได้ไปใช้กับวัตถุที่ไม่อาจจับต้องได้ได้ เพราะเหตุว่าข้อมูลไม่จำเป็นต้องทำการตรวจสอบเพื่อรับความคุ้มครองใดๆ และมิอาจมีความเสี่ยงที่จะเกิดความเสียหายทางกายภาพ ทั้งนี้ ในบางกรณีที่เจ้าของได้ฟ้องคดีว่าได้มีการเปลี่ยนแปลงไฟล์ในคอมพิวเตอร์ หรือ ลบไฟล์ในคอมพิวเตอร์ ในขณะที่ตำรวจเก็บรักษาไฟล์ แต่การตรวจสอบเนื้อหาของไฟล์ก็มิได้ช่วยป้องกันความเสียหายเช่นว่านั้นเท่าใดนัก ดังนั้น เจ้าหน้าที่จะต้องมีหมายค้นเพื่อตรวจสอบไฟล์ในคอมพิวเตอร์ที่อยู่ในการรักษาของเจ้าหน้าที่นั้น

6.การค้นบริเวณพรมแดน (Border Searches)

รัฐมีหน้าที่ในการสอดส่องดูแลสิ่งผิดกฎหมายหรือทรัพย์สินอื่นมิให้ถูกนำเข้า(Enter)หรือออก(Exit)[83]จากรัฐนั้นโดยผิดกฎหมาย ศาลฎีกาสหรัฐจึงได้แสดงให้เห็นว่ากรณีนี้เป็นกรณีพิเศษที่อาจทำการค้นได้โดยไม่จำเป็นต้องมีหมาย ในกรณีที่การค้นนั้นกระทำในเขตแนวพรมแดนของสหรัฐ โดยศาลระบุว่าการค้นดังกล่าวเป็นการค้นโดยปกติ(Routine searches)ในบริเวณพรมแดน หรือ เป็นการปฏิบัติหน้าที่ตามความเหมาะสมโดยไม่จำเป็นต้องมีหมาย, ไม่ต้องมีเหตุอันควร(Probable cause), อีกทั้งไม่ต้องมีเหตุอันควรสงสัย (Reasonable suspicion) ในการค้นหาสิ่งผิดกฎหมายหรือพยานหลักฐาน[84]

---

[82] "United States v. O'Razvi, 1998 WL 405048, at *6-7 (S.D.N.Y. July 17, 1998)" (ศาลตั้งข้อสังเกตว่า ข้อกำหนดของการค้นเพื่อแสดงรายละเอียดไม่อาจนำมาใช้กับการค้นดิสต์ในคอมพิวเตอร์ได้); "United States v. Flores, 122 F. Supp. 2d 491, 493-95 (S.D.N.Y. 2000)" (ศาลเห็นว่าการค้นโทรศัพท์เคลื่อนที่ถือเป็น การค้นเพื่อสืบสวนโดยตรง (Purely investigatory) ดังนั้น การค้นจึงไม่อาจถือได้ว่าเป็นการค้นเพื่อแสดงรายละเอียดได้)

[83] "United States v. Oriakhi, 57 F.3d 1290, 1297 (4th Cir. 1995)"(หลักการนี้ใช้ทั้งกรณีเข้าและออกจากสหรัฐ)

[84] "United States v. Montoya De Hernandez, 473 U.S. 531, 538 (1985)"

ดังนั้น เจ้าหน้าที่จึงมีอำนาจค้นคอมพิวเตอร์และZip disk ที่ผู้ต้องสงสัยพกพาติดตัวและจะนำขึ้นเครื่องบินออกนอกประเทศได้โดยไม่ต้องมีหมาย[85] แต่หลักการค้นบริเวณพรมแดนได้โดยไม่จำเป็นต้องมีหมายนี้ ไม่รวมไปถึงการดักข้อมูล (Interception of data) ที่มีการส่งเข้าหรือออกจากสหรัฐ[86] (หรืออาจถือว่าข้อมูลนั้นไม่อยู่ในบริเวณพรมแดนในขณะทำการค้น)[87]

7. ความร่วมมือระหว่างประเทศ (International Issues)

ในกรณีที่เจ้าหน้าที่ทราบว่ามีส่วนใด ส่วนหนึ่งของข้อมูล หรือ ข้อมูลทั้งหมดอยู่ในอยู่นอกประเทศสหรัฐอเมริกา ถือเป็นประเด็นที่ค่อนข้างมีความซับซ้อน โดยหน่วยงานของรัฐในประเทศสหรัฐอเมริกาอาจจะต้องใช้วิธีหลายรูปแบบตั้งแต่การแจ้งอย่างไม่เป็นการ จนถึงการแจ้งอย่างเป็นทางการเพื่อขอความร่วมมือจากประเทศที่เกี่ยวข้อง ทั้งนี้ ขึ้นอยู่กับหลักเกณฑ์ที่กำหนดไว้ในแต่ละประเทศ การขอความร่วมมือในการขอข้อมูลจากต่างประเทศนั้น เจ้าหน้าที่สามารถดำเนินการได้โดยไม่ต้องมีหมาย

---

[85] "United States v. Roberts, 86 F. Supp. 2d 678 (S.D. Tex. 2000" (ภาพลามกอนาจารเด็กจำนวนมากที่อยู่ในคอมพิวเตอร์และZip disk ถือเป็นสิ่งผิดกฎหมาย)

[86] แต่ต้องดำเนินการตาม 18 U.S.C. §§ 2510-2522 หรือ Pen/Trap statute, 18 U.S.C. §§ 3121-3127

[87] เทียบเคียง Almeida-Sanchez v. United States, 413 U.S. 266, 273-74 (1973) (การค้นเกิดห่างจากจุดพรมแดน 25 ไมล์ ไม่เข้าข้อยกเว้นการค้นบริเวณพรมแดน เพราะผ่านจุดพรมแดนมาแล้ว แม้เป็นที่รู้กันโดยทั่วไปว่าถนนเส้นนั้นเป็นเส้นทางลักลอบเข้าเมืองโดยผิดกฎหมายก็ตาม)

การควบคุมทางอิเล็กทรอนิกส์ในเครือข่ายสื่อสาร (ELECTRONIC SURVEILLANCE IN COMMUNICATIONS NETWORKS)

ในคดีที่เกี่ยวกับคอมพิวเตอร์ การควบคุมทางอิเล็กทรอนิกส์เป็นมาตรการสำคัญหนึ่งที่จะช่วยเหลือเจ้าหน้าที่ในการสืบสวนสอบสวนความผิดที่เกิดขึ้น เช่น การเฝ้าระวังผู้กระทำความผิดในฐานแฮกเกอร์, การโคลน(Clone) อีเมล์ที่มีภาพลามกอนาจารเด็กหรือการตรวจสอบกิจกรรมต่าง ๆ บนอินเทอร์เน็ต เป็นต้น

ในการใช้มาตรการต่างๆเหล่านี้จำเป็นที่จะต้องพิจารณากฎหมาย(Federal statues)ต่างๆที่เกี่ยวข้อง ซึ่งได้แก่ 1)Pen/Trap statute (18 U.S.C. §§ 3121-3127) และ 2) Wiretap statute(18 U.S.C. §§ 2510-2522) หรือ Title III[88] บทบัญญัติทั้งสองมีมาตรการควบคุมที่แตกต่างกัน โดย Pen/Trap statute มุ่งรวบรวมข้อมูลที่ระบุที่อยู่หรือตัวผู้ใช้ ในลักษณะที่มิใช่เนื้อหา (Non-content) หากเทียบกับการสื่อสารทางโทรศัพท์ ก็อาจเทียบได้กับหมายเลขโทรศัพท์(Phone number) ส่วน Wiretap statute เป็นการรวบรวมข้อมูลในลักษณะเนื้อหา(Content) หรืออาจเทียบได้กับเนื้อหาบทสนทนา(Conversation)ที่พูดคุยผ่านทางโทรศัพท์

1.The Pen/Trap Statute (18 U.S.C. §§ 3121-3127)

บทนิยาม

ดังที่ได้กล่าวมาแล้วว่าบทบัญญัตินี้ให้อำนาจเจ้าหน้าที่ในการรวบรวมข้อมูลที่มิใช่เนื้อหา (Non-content) ซึ่งเดิมทีเดียวถูกกำหนดไว้เพื่อใช้เฉพาะกับการสื่อสารทางโทรศัพท์ แต่ศาลก็ปรับใช้กับการสื่อสารบนเครือข่ายอินเทอร์เน็ตเป็นจำนวนมากมายหลายคดี[89] จนกระทั่งปี ค.ศ. 2001 ได้ประกาศใช้กฎหมาย USA PATRIOT Act เพื่อให้กฎหมายดังกล่าวรองรับกับเทคโนโลยีได้กว้างขึ้น[90]

---

[88] หลักการตามกฎหมายฉบับนี้เดิมทีเดียวอยู่ใน Title III ของกฎหมาย Omnibus Crime Control and Safe Streets Act of 1968 (จึงมีชื่อที่รู้จักกันโดยทั่วไปว่า "Title III")

[89] Computer Crime and Intellectual Property Section Criminal Division United States Department of Justice, Searching and Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, pp. 67.

[90] PATRIOT Act § 216, 115 Stat. 272, 288-90 (2001)

บทบัญญัตินี้นิยามความหมายของ "Pen register" ไว้ดังนี้ "Pen register หมายถึง อุปกรณ์หรือกระบวนการในการบันทึก การถอดรหัสการหมุนโทรศัพท์, เส้นทาง, ที่อยู่ หรือสัญญาณข้อมูล ที่ส่งผ่านเครื่องมือ หรือเครื่องอำนวยความสะดวก ไม่ว่าจะการสื่อสารหรือการดำเนินการนั้นจะผ่านทางสายไฟหรือสื่อสารทางอิเล็กทรอนิกส์ อย่างไรก็ตาม ข้อมูลนั้นไม่รวมถึงเนื้อหาของการสื่อสารนั้น..." นอกจากนี้ยังรวมถึงใบแจ้งหนี้ (Billing) หรือบัญชีบันทึกค่าใช้จ่าย (cost accounting)ด้วย

และได้นิยามความหมายของ "Trap and trace device" ไว้ดังนี้ " อุปกรณ์หรือกระบวนการ ไม่ว่าจะเป็นการดักจับข้อมูล หรือ สิ่งกระตุ้นอื่น (Impulse) ที่แสดงที่มาของหมายเลขหรือการเชื่อมต่ออื่นเช่นเดียวกับการหมุนโทรศัพท์, เส้นทาง, ที่อยู่ หรือสัญญาณข้อมูล ที่มีเหตุผลว่าสามารถระบุแหล่งที่มาของการสื่อสารผ่านทางสายไฟหรือสื่อสารทางอิเล็กทรอนิกส์ อย่างไรก็ตาม ข้อมูลนั้นไม่รวมถึงเนื้อหาของการสื่อสารนั้น"[91]จากคำนิยามข้างต้นแสดงให้เห็นว่ากระบวนการ"Pen register" และ"Trap and trace device" ครอบคลุมถึงการเทคโนโลยีการสื่อสารรูปแบบใหม่ๆด้วย จึงครอบคลุมทั้งหมายเลขโทรศัพท์, โทรศัพท์มือถือ, หมายเลขผู้ใช้อินเทอร์เน็ต หรือ IP Address นอกจากนี้ยังรวมถึงอุปกรณ์และ Software[92]อีกด้วย

<u>คำสั่ง Pen/trap: การขอคำสั่ง, การออกคำสั่ง, การปฏิบัติการ (service) และการรายงาน</u>

ในกระบวนการขอคำสั่ง Pen/trap ผู้ขอคำสั่งจะต้องแสดงว่าตนเป็นใคร แสดงว่าเจ้าหน้าที่คนใดกระทำการสอบสวน และให้การรับรองว่าตนเชื่อว่าข้อมูลที่จะได้มามีความเกี่ยวข้องกับคดีอาญาที่กำลังกระทำการสอบสวนโดยเจ้าหน้าที่นั้นอยู่ (มาตรา 18 U.S.C. § 3122 (b) (1)-(2)) และศาลที่ออกคำสั่ง Pen/Trap จะต้องมีเขตอำนาจ

---

[91] 18 U.S.C. § 3127(4) the term "trap and trace device" means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication;

[92] โดยพิจารณาจากคำว่า "...device or process..."

เหนือการกระทำผิดที่มีการสอบสวนอยู่ (ดู 18 U.S.C. § 3127(2)(a)) หากคำขอต่อศาลเป็นไปตามเงื่อนไขที่กล่าวมานี้ ศาลย่อมให้มีการติดตั้ง และใช้เครื่อง Pen/trap ที่ใดก็ได้ในประเทศสหรัฐอเมริกา (ดู 18 U.S.C. § 3123 (a)(1) โดยบทบาทของศาลในการเห็นชอบการใช้ trap และเครื่อง trap เป็นอำนาจสั่งการเมื่อเงื่อนไขครบตามที่กฎหมายกำหนดและจะไม่ใช้ดุลยพินิจเข้าไปไต่สวนหาความจริง ("The judicial role in approving use of trap and trace devices is ministerial in nature.")

คำสั่ง pen/trap อาจจะมีผลนอกเขตอำนาจของศาลที่ออกคำสั่งได้ ในประเด็นที่คำขอเป็นระดับมลรัฐ เมื่อมีคำสั่ง คำสั่งนั้นจะนำไปใช้กับบุคคลใดๆ หรือ กลุ่มบุคคลใดที่ให้บริการติดต่อสื่อสารทางอิเล็กทรอนิกส์ หรือ ให้บริการติดต่อสื่อสารในประเทศสหรัฐอเมริกาซึ่งสามารถให้ความสะดวกในการปฏิบัติการตามหมาย (18 U.S.C. § 3123 (a) (1)) เช่น อัยการในระดับ Federal มีสิทธิที่จะได้รับคำสั่งเพื่อสะกดรอยการโทรศัพท์ในโทรศัพท์เครื่องใดเครื่องหนึ่ง และคำสั่งนี้จะนำไปใช้กับผู้ให้บริการส่งสัญญาณโทรศัพท์ของท้องถิ่น รวมไปถึงผู้ให้บริการระดับอื่นด้วย (เช่น ผู้ให้บริการส่งสัญญาณโทรศัพท์ทางไกล และผู้ให้บริการส่งสัญญาณคลื่นโทรศัพท์ในระดับภูมิภาคที่ในส่วนอื่นของประเทศ) ซึ่งหลักการนี้ถูกนำไปใช้ในกับอินเทอร์เน็ตด้วย

กฎหมาย Pen/Trap มิได้กำหนดให้ คำขอ Pen/trap หรือ คำสั่ง Pen/Trap จะต้องระบุชื่อผู้ให้บริการทุกรายที่จะต้องปฏิบัติตามคำสั่ง แต่ในคำสั่งนั้นจะต้องระบุถึงผู้ให้บริการที่อยู่จะต้องปฏิบัติตามคำสั่งรายแรกเท่านั้น (ดู 18 U.S.C. § 3123 (b)(1)(A)) พนักงานสอบสวนจะต้องนำคำสั่งศาลไปให้ผู้ให้บริการเพื่อจะได้รับความร่วมมือจากผู้ให้บริการนั้น และในกรณีที่ผู้ให้บริการร้องขอ เจ้าหน้าที่จะต้องแสดง "ใบรับรองเป็นลายลักษณ์อักษร หรือ ใบรับรองที่เป็นอิเล็กทรอนิกส์(written or electronic certification)" ที่ให้คำสั่งนั้นมีผลต่อผู้ให้บริการ (ดู 18 U.S.C. § 3123(a)(1)) แต่ในทางปฏิบัติจะเป็นการยื่นคำขออย่างไม่เป็นทางการ เพราะอัยการที่ได้ยื่นคำขอคำสั่ง Pen/trap มักจะยังไม่ระบุตัวผู้ให้บริการกลุ่มแรกในเครือข่ายของการสื่อสารข้อมูลที่อยู่ในคำสั่งนั้น เพราะ หากกำหนดว่าเจ้าหน้าที่ต้องกลับไปรายงานให้ศาลทราบทุกครั้งที่สามารถระบุผู้ให้บริการรายใหม่ได้ก็ย่อมส่งผลให้การสืบสวนล่าช้าได้

คำสั่ง Pen/Trap ให้อำนาจให้ติดตั้งเครื่อง Pen/Trap ได้อย่างมาก 60 วัน และอาจขยายระยะเวลาเพิ่มขึ้นอีก 60 วันได้ (ดู 18 U.S.C. § 3123 (c)) ในคำสั่งศาลจะกำหนดห้ามผู้ให้บริการเปิดเผยถึงการติดตั้งเครื่อง Pen/Trap "แก่บุคคลใดๆ เว้นแต่จะเป็นไปตามคำสั่งของศาลหรือศาลจะมีคำสั่งเป็นอย่างอื่น" (18 U.S.C. § 3123(d)(2)) และในคำสั่งอาจจะสั่งให้ผู้ให้บริการติดต่อสื่อสารตามสาย หรือ ผู้ให้บริการติดต่ออิเล็กส์ทรอนิกส์ ผู้ให้เช่า ผู้ควบคุมดูแล หรือ บุคคลอื่นใด ในการ "จัดหา....ข้อมูลทั้งหมด ให้ความสะดวก และให้ความช่วยเหลือทางเทคนิคที่จำเป็น" ในการติดตั้งเครื่อง pen/trap (ดู 18 U.S.C § 3124 (a), (b)) สำหรับผู้ให้บริการที่ได้รับคำสั่งให้ช่วยเหลือในการติดตั้งเครื่อง Pen/trap มีสิทธิได้รับค่าตอบแทนตามควร(Reasonable expenses)ในค่าใช้จ่ายที่จำเป็นอันเกิดขึ้นจากการให้ความสะดวกหรือการให้ความช่วยเหลือทางเทคนิคที่จำเป็นแก่เจ้าหน้าที่ (ดูมาตรา 18 U.S.C. § 3124) ทั้งนี้ การกระทำที่กล่าวมานี้ของผู้ให้บริการที่กระทำการไปโดยสุจริตตามคำสั่งศาลจะทำให้ผู้ให้บริการได้รับการคุ้มครองจากการดำเนินคดีแพ่ง หรือ คดีอาญาใดๆ ที่มาจากการดำเนินการตามคำสั่งศาล

กฎหมาย Pen/Trap ได้กำหนดให้มีการรายงานขอบเขตของลักษณะในระดับของคดี (Narrow class of case) ที่เจ้าหน้าที่ติดตั้งเครื่อง pen/trap ในเครื่อง Packet switched network ของผู้ให้บริการการติดต่อสื่อสารทางอินเทอร์เน็ต (ดู 18 U.S.C. § 3123 (a)(3)(A)) โดยหลักการเมื่อหน่วยงานใช้บังคับกฎหมายได้ใช้คำสั่ง Pen/Trap กับผู้ให้บริการ ผู้ให้บริการก็จะต้องรวบรวมข้อมูลที่ระบุไว้ตามคำสั่ง และนำส่งต่อหน่วยงานที่กฎหมายกำหนด ในกรณีที่ผู้ให้บริการไม่สามารถกระทำการตามคำสั่งได้ หรือ ไม่ยอมปฏิบัติการตามคำสั่ง หรือ ในกรณีอื่นใด หน่วยงานของรัฐก็มีสิทธิที่จะติดตั้งเครื่อง Pen/trap เองได้ เช่น เข้าติดตั้งเครื่อง DCS 1000 ของหน่วยงาน FBI เป็นต้น ในกรณีที่กล่าวมานี้หน่วยงานของรัฐจะต้องนำเสนอข้อมูลดังต่อไปนี้ให้กับศาล ภายใน30 วัน

(1) ระบุตัวเจ้าหน้าที่ซึ่งทำการติดตั้ง และใช้เครื่องมือ

(2) วัน และเวลาที่เครื่องมือนั้นได้มีการติดตั้ง ใช้ และการนำออก

(3) เครื่องมือที่ใช้ทั้งหมด (Configuration of the device) ในสถานที่ติดตั้ง และการปรับเปลี่ยนเครื่องมือนั้น

(4) ข้อมูลที่ได้จัดเก็บได้จากเครื่องมือนั้น (ดู 18 U.S.C. § 3123 (a)(3))

เมื่อหน่วยงานของรัฐได้ทำการติดตั้งเครื่อง Pen/trap แล้ว หน่วยงานของรัฐจะต้องใช้ "เทคโนโลยีที่มีอยู่ตามควรกับเครื่องมือนั้น (Technology reasonably available to it)" เพื่อป้องกันจากการบันทึก หรือ การถอดรหัส ในข้อมูลที่อยู่ในการติดต่อสื่อสารตามสาย หรือ ที่อยู่ในการติดต่อสื่อสารทางอิเล็กทรอนิกส์ (ดู 18 U.S.C. § 3121(c))

ขั้นตอนที่สำคัญที่สุด คือการกำหนดให้ศาลตรวจสอบทบทวนคำสั่ง Pen/Trap ว่ามีการใช้อำนาจอันเป็นการฝ่าฝืนกฎหมายหรือไม่ (18 U.S.C. § 3123(d) ซึ่งกำหนดโทษทางอาญาจากการกระทำที่ขัดต่อกฎหมาย Pen/Trap) โดยศาลให้เหตุผลว่า "จุดประสงค์ที่สำคัญที่สุดในการกำหนดให้คำขอจะต้องยื่นเพื่อให้ศาลออกคำสั่ง คือการสร้างความรับผิดให้แก่บุคคลในการที่จะต้องรับรองความถูกต้องของคำขอนั้น

ในบทบัญญัติ Pen/Trap ได้ให้อำนาจโดยทั่วไปแก่ผู้ให้บริการ ในการใช้เครื่อง Pen/Trap ในเครือข่ายของตนโดยไม่จำเป็นต้องขอคำสั่งของศาล โดย 18 U.S.C. § 3121(b) บัญญัติว่า ผู้ให้บริการมีสิทธิใช้เครื่อง Pen/trap Device โดยไม่ต้องมีคำสั่งศาล ในกรณีต่อไปนี้

(1) กรณีที่เกี่ยวข้องกับ การปฏิบัติการ การดูแลรักษา และการทดลองสำหรับการให้บริการสื่อสารตามสาย หรือ การให้บริการสื่อสารทางอิเล็กทรอนิกส์ หรือ เพื่อคุ้มครองสิทธิ หรือ ทรัพย์สิน ของผู้ให้บริการเอง หรือ เพื่อคุ้มครองผู้ใช้บริการจากการให้บริการที่ไม่เหมาะสม หรือ การใช้บริการที่ไม่ชอบด้วยกฎหมาย หรือ

(2) เพื่อบันทึกข้อเท็จจริงซึ่งการเริ่มต้น สื่อสารตามสาย หรือ การสื่อสารทางอิเล็กทรอนิกส์ หรือ การสื่อสารเหล่านั้นได้กระทำเสร็จสิ้นแล้ว เพื่อ

คุ้มครองผู้ให้บริการเอง หรือคุ้มครองผู้ให้บริการรายอื่นในการนำการให้บริการจากการสื่อสารตามที่สมบูรณ์แล้ว หรือให้ความคุ้มครองผู้ใช้บริการของผู้ให้บริการนั้น จากการฉ้อฉล หรือจากการใช้บริการที่ไม่ชอบด้วยกฎหมาย หรือ การใช้บริการโดยมิชอบ

(3) ในกรณีที่ผู้รับบริการให้ความยินยอม (18 U.S.C. § 3121 (b))

2. Wiretap Statue หรือ Title III (18 U.S.C. §§ 2510-2522)

บทบัญญัตินี้ใช้สำหรับควบคุมและการสอดแนมเนื้อหาของการติดต่อสื่อสารทางอิเล็กทรอนิกส์ในลักษณะReal-time กฎหมายนี้ได้ตราขึ้นเมื่อปี 1968 และได้แก้ไขในปี 1986 เพื่อให้เจ้าหน้าที่ต้องการที่จะดักฟังโทรศัพท์ที่ต้องสงสัย หรือ ตรวจสอบการใช้แป้นพิมพ์ของHacker ("Keystroke" a hacker) ได้ โดยเจ้าหน้าที่จะต้องพิจารณาหลักเกณฑ์ของ Title III เสียก่อน

หลักการพื้นฐานของกฎหมายนี้คือห้ามบุคคลภายนอก (เช่น หน่วยงานของรัฐ) ที่ไม่ได้เป็นคู่กรณีในการสื่อสารที่เข้าร่วมการสื่อสาร เข้าแทรกในการสื่อสารของเอกชนโดยใช้ "เครื่องมือทางอิเล็กทรอนิกส์ เครื่องมือของช่าง หรือเครื่องมืออื่นใด" เว้นแต่จะเป็นกรณีที่นำข้อยกเว้นประการใดประการหนึ่งมาใช้ได้ (18 U.S.C. § 2511(1) d) กล่าวคือ ห้ามมิให้ลักลอบดักสัญญาณ(Eavesdropping)(ซึ่งจะอยู่ภายใต้ข้อยกเว้นบางประการ และข้อกำหนดระหว่างมลรัฐ)ไม่ว่าการดักสัญญาณนั้นจะอยู่ในพื้นที่ใดๆ หรือโดยบุคคลใดๆก็ตามในประเทศสหรัฐอเมริกา ทั้งนี้ เป็นการประกันความคุ้มครองตามบทบัญญัติ Wiretap Statue ไม่ว่าพนักงานสอบสวนจะดำเนินการดักฟังในบ้าน หรือ ในที่ทำงาน หรือ ในสำนักงานของหน่วยงานราชการ หรือ ในคุก หรือ บนอินเทอร์เน็ต ก็ตาม ทำให้ในการใช้อำนาจดักฟังสัญญาณ เจ้าหน้าที่และอัยการจะดำเนินการได้ต่อเมื่อพิจารณาเงื่อนไขดังต่อไปนี้

(1) การตรวจสอบการสื่อสารเป็นกรณีของการสื่อสารนั้นได้รับความคุ้มครองอย่างหนึ่งตามความหมายของ 18 U.S.C § 2510 หรือไม่

(2) การสอบแนมที่มีขึ้นจะก่อให้เกิดการแทรกเข้าไประหว่างการสื่อสารหรือไม่

(3) เมื่อพิจารณาเงื่อนสองข้อแรกแล้ว ต่อมาต้องพิจารณาว่าข้อยกเว้นตามกฎหมายที่จะอนุญาตให้เข้าไปแทรกแซงการสื่อสารหรือไม่ ซึ่งในการกระทำความผิดที่เกี่ยวข้องกับคอมพิวเตอร์ ส่วนใหญ่จะพิจารณาจากข้อยกเว้น 7 ประการดังนี้

ก) Interception pursuant to a § 2518 court order;

ข) The 'consent' exception, § 2511(2)(c)-(d);

ค) The 'provider' exception, § 2511(2)(a)(i);

ง) The 'computer trespasser' exception, § 2511(2)(i);

จ) The 'extension telephone' exception, § 2510(5)(a);

ฉ) The 'inadvertently obtained criminal evidence' exception, § 2511(3)(b)(iv); and

ช) The 'accessible to the public' exception, § 2511(2)(g)(i).

ผลของการฝ่าฝืน Pen/Trap Statute และ Wiretap Statue

กรณีที่เจ้าหน้าที่หรือยการฝ่าฝืนบทบัญญัติเหล่านี้อาจทำให้ต้องรับผิดในทางแพ่ง(18 U.S.C. § 2520) ทางอาญา (ตามU.S.C. § 3121(d) กรณีฝ่าฝืนPentrap หรือตามU.S.C. § 2511(4) กรณีฝ่าฝืน Wiretap)หรือทำให้พยานหลักฐานที่ได้ไม่สามารถรับฟังเป็นพยานหลักฐานในคดีได้ (ตามU.S.C. § 2518(10)(a) กรณีฝ่าฝืน Wiretap)

นอกจากที่ได้กล่าวมาแล้วทั้งหมดข้างต้น เพื่อเป็นการส่งเสริมความร่วมมือระหว่างประเทศสหรัฐอเมริกาจึงได้เข้าร่วมและให้สัตยาบันในอนุสัญญาของคณะมนตรียุโรปว่าด้วยการกระทำผิดบนอินเทอร์เน็ต (The Council of Europe Convention on Cybercrime) ในเดือนสิงหาคม ปี ค.ศ.2006 และมีผลบังคับในวันที่1 มกราคม ปี ค.ศ. 2007[93] ส่งผลให้ประเทศสหรัฐอเมริกานำเสนอร่างกฎหมายCyber-Crime Act of 2007ต่อสภาคอนเกสเพื่อบังคับใช้เป็นกฎหมายต่อไป

4.1.1 หน่วยงานและเจ้าหน้าที่ที่เกี่ยวข้องกับการดำเนินคดีในสหรัฐอเมริกา

ในสหรัฐอเมริกา การแจ้งการกระทำผิดต่อเจ้าหน้าที่ที่เกี่ยวข้องจะต้องคำนึงถึงเขตอำนาจในการสืบสวนสอบสวนว่าอยู่ในความรับผิดชอบของหน่วยงานใด โดยแบ่งตามเขตอำนาจระดับท้องถิ่น ระดับรัฐ ระดับรัฐบาลกลาง หรือระดับระหว่างรัฐและจะต้องพิจารณาถึงประเภทของความผิดนั้นๆด้วย ซึ่งหน่วยงานที่เกี่ยวข้องได้แก่ Federal Bureau of Investigation (FBI), the United States Secret Service, the United States Immigration and Customs Enforcement (ICE) , the United States Postal Inspection Service, and the Bureau of Alcohol, Tobacco and Firearms (ATF) การแจ้งการกระทำความผิดอาจทำได้โดยการแจ้งผ่านทางโทรศัพท์[256] เพื่อติดต่อไปยังหน่วยงานที่เหมาะสม ดังนี้

---

[93] http:// www.cybercrime.gov

[256]หน่วยงานที่ทำหน้าที่ติดต่อไปยังหน่วยงานที่เกี่ยวข้องมีชื่อเรียกว่า Duty Complaint Agent.

ตารางที่ 4.1 แสดงหน่วยงานรับผิดชอบในสหรัฐอเมริกา[257]

ประเภทของการกระทำผิด	หน่วยงานที่มีอำนาจสืบสวนสอบสวน
การบุกรุกทางคอมพิวเตอร์ (Computer intrusion) (เช่น การเจาะระบบ)	• หน่วยงานFBIในท้องที่ • U.S. Secret Service • Internet Fraud Complaint Center
การลักลอบตักรหัสผ่าน (Password trafficking)	• หน่วยงานFBIในท้องที่ • U.S. Secret Service • Internet Fraud Complaint Center
การละเมิดลิขสิทธิ์ (Copyright (software, movie, sound recording) piracy)	• หน่วยงานFBIในท้องที่ • กรณี การลักลอบนำเข้าประเทศ, U.S. Immigration and Customs Enforcement • Internet Fraud Complaint Center
การขโมยความลับทางการค้า (Theft of trade secrets)	• หน่วยงานFBIในท้องที่
การปลอมแปลงเครื่องหมายการค้า (Trademark counterfeiting)	• หน่วยงานFBIในท้องที่ • กรณี การลักลอบนำเข้าประเทศ, U.S. Immigration and Customs Enforcement • Internet Fraud Complaint Center
การปลอมแปลงเงินตรา (Counterfeiting of currency)	• U.S. Secret Service

[257] http://www.usdoj.gov/criminal/cybercrime/reporting.htm.

การเผยแพร่ภาพลามกอนาจารเด็ก *(Child Pornography or Exploitation)*	• หน่วยงานFBIในท้องที่ • กรณี การลักลอบนำเข้าประเทศ, U.S. Immigration and Customs Enforcement • Internet Fraud Complaint Center
การกระทำผิดต่อเด็กและการฉ้อโกง *(Child Exploitation and Internet Fraud matters that have a mail nexus)*	• U.S. Postal Inspection Service • Internet Fraud Complaint Center
การฉ้อโกงทางอินเทอร์เน็ตและการส่งแสปม *Internet fraud and SPAM*	• หน่วยงานFBIในท้องที่ • U.S. Secret Service (Financial Crimes Division) • Federal Trade Commission (online complaint) • กรณีการฉ้อโกงเกี่ยวกับการรักษาความปลอดภัยและการแสวงหาประโยชน์จากแสปม, Securities and Exchange Commission (online complaint) • The Internet Fraud Complaint Center
(การรบกวนผ่านอินเทอร์เน็ต) *Internet harassment*	• หน่วยงานFBIในท้องที่
(การขู่วางระเบิดผ่านอินเทอร์เน็ต) *Internet bomb threats*	• หน่วยงานFBIในท้องที่ • หน่วยงานATFในท้องที่
การลักลอบเกี่ยวกับวัตถุระเบิดหรือปืนทางอินเทอร์เน็ต *Trafficking in explosive or incendiary devices or firearms over the Internet*	• หน่วยงานFBIในท้องที่ • หน่วยงานATFในท้องที่

เมื่อมีหน่วยงานที่เกี่ยวข้องมากมายจึงมีการจัดตั้ง The Internet Crime Complaint Center (IC3) ซึ่งเป็นความร่วมมือระหว่าง Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C). IC3 ซึ่งมีหน้าที่ในการให้ความสะดวกแก่ผู้เสียหายที่จะรายงานการกระทำความผิดไปยังหน่วยงานที่เกี่ยวข้องได้อย่างถูกต้องเหมาะสม[258] นอกจากนี้ในการสืบสวนสอบสวนยังมีการส่งเจ้าหน้าที่ที่มีความเชี่ยวชาญไปประจำการยังประเทศต่างๆอีกด้วย เช่น FBIของสหรัฐอเมริกาจะมีฑูตทางกฎหมายประจำอยู่ 41 ประเทศ[259] เพื่อให้ความช่วยเหลือพนักงานสอบสวนในการรวบรวมและเก็บรักษาพยานหลักฐาน

4.2 ประเทศสิงคโปร์

การดำเนินคดีกับผู้กระทำความผิดทางคอมพิวเตอร์สำหรับประเทศสิงคโปร์ถูกบัญญัติไว้ใน Computer Misuse Act (กฎหมายฉบับนี้ร่างขึ้นโดยใช้ British Computer Misuse Act 1990 เป็นต้นแบบ)[94]โดยได้กำหนดไว้ทั้งฐานความผิดและวิธีพิจารณาไว้ในกฎหมายฉบับเดียวกัน โดยสามารถแบ่งออกได้ เป็น 3 ส่วนได้แก่ Part I – Preliminary , Part II – Offences , Part III –Miscellaneous and General

ฐานความผิดต่างๆตามกฎหมายนี้ที่กำหนดไว้ใน Part II – Offences ได้แก่ การเข้าถึงอุปกรณ์คอมพิวเตอร์โดยปราศจากอำนาจ (Unauthorised access to computer material) การเข้าถึงโดยเจตนากระทำความผิดหรือสะดวกในการกระทำความผิด(Access with intent to commit or facilitate commission of offence) การแก้ไขโดยปราศจากสิทธิซึ่งอุปกรณ์คอมพิวเตอร์(Unauthorised Modification of computer material) การใช้โดยปราศจากสิทธิหรือการดักบริการคอมพิวเตอร์(Unauthorised use or interception of computer service) การสร้างอุปสรรคการใช้คอมพิวเตอร์โดยปราศจากสิทธิ(Unauthorised obstruction of use of computer)

---

[258]นอกจากนี้ยังมีหน่วยงานอื่นๆอีก เช่น Department of Homeland Security's National Infrastructure Coordinating Center, U.S. Computer Emergency Readiness Team (U.S. CERT) เป็นต้น

[259]ไพจิตร สวัสดิสาร, การใช้คอมพิวเตอร์ทางกฎหมายและกฎหมายที่เกี่ยวกับคอมพิวเตอร์, หน้า 118.

[94] "Katherine S Williams and Indira Mahalingam Carr, The Singapore Computer Misuse Act - Better Protection for the Victims?" http://www.jlis.law.utas.edu.au/v5i2misuse.html (นอกจากนี้ยังมีประเทศอื่นที่ใช้ British Computer Misuse Act 1990 เป็นต้นแบบ เช่น มาเลเซีย และบรูไน)

การเปิดเผยรหัสการเข้าถึงโดยปราศจากสิทธิ (Unauthorised disclosure of access code)[95] นอกจากนี้ยังมีบทเพิ่มโทษและการเอาผิดกับผู้สนับสนุนหรือผู้พยายามหรือตระเตรียมการกระทำความผิดด้วย[96]

ในส่วนของการดำเนินคดีอาญาได้การกำหนดให้อำนาจเจ้าพนักงานในกรณีเกี่ยวกับความผิดเกี่ยวกับคอมพิวเตอร์ไว้โดยเฉพาะทั้งที่บัญญัติไว้ในส่วนของประมวลกฎหมายวิธีพิจารณาความอาญา(Criminal Procedure code)และในกฎหมาย Computer Misuse Act ดังที่จะได้กล่าวต่อไปนี้

1.อำนาจเข้าถึงคอมพิวเตอร์(Power to access computer)

มาตรา 125A ตามประมวลกฎหมายวิธีพิจารณาความอาญาของสิงคโปร์มีเนื้อหาสำคัญเกี่ยวกับอำนาจเข้าถึงคอมพิวเตอร์ของเจ้าพนักงาน(Power to access computer)[97] ดังนี้

" 125 A (1) เจ้าพนักงานตำรวจหรือบุคคลซึ่งมีอำนาจ(Authorised person) ในการสืบสวน Seizable offence[98] สามารถกระทำการต่อไปนี้ได้ทุกเวลา(May at any time)

(a) เข้าถึง ,เฝ้าระวังและตรวจสอบการปฏิบัติงานของคอมพิวเตอร์ใดๆได้ หากมีเหตุผลอันควรสงสัย(Reasonable cause to suspect) หรือถูกใช้เกี่ยวข้องกับ Seizable offence หรือ

---

[95] ต่อมาได้มีการแก้ไข Computer Misuse Act โดยให้ผู้บัญชาการตำรวจแห่งชาติ หรือบุคคลใดที่ได้รับมอบหมายกำหนดฐานความผิดได้ (มาตรา 12 A)

[96] Computer Misuse Act , Article 9 และ 10

[97] เดิมหลักการนี้ถูกบัญญัติไว้ใน Computer Misuse Act มาตรา 15 Power of police officer to access computer and data แต่ต่อมาได้ถูกยกเลิก(Deleted by Act 42/2005, wef 01/01/2006.)และได้นำหลักการดังกล่าวมาบัญญัติไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา125A และ 125B แทน

[98] "seizable offence" means an offence for which and "seizable case" means a case in which a police officer may ordinarily arrest without warrant according to the third column of Schedule A.

(b) ใช้หรือมีเหตุเชื่อว่าได้ใช้คอมพิวเตอร์ในการสืบค้นข้อมูลใดๆ ที่อยู่หรือใช้งานได้โดยคอมพิวเตอร์

(2) เจ้าพนักงานตำรวจหรือบุคคลซึ่งมีอำนาจอาจจะร้องขอความร่วมมือใดๆที่ต้องการเพื่อเข้าถึง จาก

(a) บุคคลใดที่มีเหตุอันควรสงสัยว่าได้ใช้คอมพิวเตอร์เกี่ยวข้องกับ Seizable offenceหรือได้ใช้โดยวิธีการใดเช่นว่านั้น หรือ

(b) บุคคลใดที่ได้รับการแจ้งข้อกล่าวหา หรือได้เกี่ยวข้องกับการปฏิบัติงานในทางอื่น เช่นเดียวกับคอมพิวเตอร์

(3) บุคคลใดซึ่งได้ขัดขวางการดำเนินการโดยชอบด้วยกฎหมายภายใต้บทบัญญัติตามอนุมาตรา

1) หรือผู้ซึ่งมิได้กระทำความการร้องขอภายใต้บทบัญญัติตามอนุมาตรา(2) ถือเป็นความผิดตามอาญาและมีโทษปรับไม่เกิน 5,000 ดอลล่าห์สิงคโปร์หรือจำคุกไม่เกิน6เดือนหรือทั้งจำทั้งปรับ

4) การกระทำความผิดตามอนุมาตรา(3) ถือเป็น Seizable offence

5) บุคคลใดที่ได้กระทำโดยสุจริตตามอนุมาตรา(1) หรือได้ให้ความร่วมมือตามคำขอตามอนุมาตรา(2) ไม่มีความผิดทางอาญา และไม่ต้องรับผิดใดๆในทางแพ่งตามกฎหมาย

6) ตามมาตรานี้หรือมาตรา 125 B

"บุคคลซึ่งมีอำนาจ (Authorized person)" หมายถึง บุคคลที่มีอำนาจตามที่ผู้บัญชาการตำรวจได้แต่งตั้งตามกฎหมายเพื่อให้เป็นไปตามวัตถุประสงค์ของมาตรานี้มาตรา125B หรือทั้งสองมาตรา

"คอมพิวเตอร์ (Computer)" หมายถึง มีความหมายเดียวกับที่บัญญัติไว้ในกฎหมาย Computer Misuse Act"[99]

2.อำนาจถอดรหัสของข้อมูล(Power to access decryption information)

ตามประมวลกฎหมายวิธีพิจารณาความอาญาของสิงคโปร์มาตรา 125B มีเนื้อหาสัมพันธ์กับมาตรา125A ที่ได้กล่าวมาแล้วข้างต้นโดยได้ให้อำนาจเจ้าหน้าที่ถอดรหัสของข้อมูล(Power to access decryption information) ดังนี้

" มาตรา 125B (1) เพื่อวัตถุประสงค์ในการสืบสวน Seizable offence พนักงานอัยการ(Public prosecutor) อาจออกคำสั่งให้เจ้าพนักงานตำรวจหรือบุคคลซึ่งมีอำนาจในการดำเนินการ ,เพิ่มเติมจากอำนาจภายใต้มาตรา 125A,ทั้งหมดหรือตามอำนาจใดภายใต้มาตรานี้

(2) เจ้าพนักงานตำรวจหรือบุคคลซึ่งมีอำนาจตามที่ได้กล่าวไว้ในอนุมาตรา(1) มีสิทธิที่จะ

(a) เข้าถึงข้อมูลใด,รหัสหรือใช้เทคโนโลยีในการแปลข้อมูลหรือถอดรหัสข้อมูล (Encrypted data)เพื่อให้เข้าใจได้และรูปแบบที่เข้าใจได้หรือข้อความเพื่อวัตถุประสงค์ในการสืบสวน Seizable offence

(b) ร้องขอให้-

---

[99] Computer Misuse Act section 2 "computer" means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include —

(a) an automated typewriter or typesetter;

(b) a portable hand held calculator;

(c) a similar device which is non-programmable or which does not contain any data storage facility; or

(d) such other device as the Minister may, by notification in the *Gazette*, prescribe;

(i) บุคคลใดที่มีเหตุผลอันควรสงสัยว่าได้ใช้คอมพิวเตอร์เกี่ยวข้องกับSeizable offenceหรือได้ใช้ในทางเดียวกันนั้น หรือ

(ii) บุคคลใดที่ได้รับการแจ้งข้อกล่าวหา หรือได้เกี่ยวข้องกับการปฏิบัติงานในทางอื่น เช่นเดียวกับคอมพิวเตอร์ดำเนินการทางเทคนิคอย่างสมเหตุสมผลและการช่วยเหลืออื่นตามที่เขาต้องการเพื่อวัตถุประสงค์ในการดำเนินการตามข้อ(a) และ

(c) ร้องขอให้บุคคลใดที่มีเหตุอันควรสงสัยว่าได้ครอบครองรหัสเพื่อให้เขาอนุญาตให้ถอดรหัสเท่าที่จำเป็นในการถอดรหัสตามวัตถุประสงค์ในการสืบสวน Seizable offence

(3) บุคคลใดซึ่งได้ขัดขวางการดำเนินการโดยชอบด้วยกฎหมายภายใต้บทบัญญัติตามอนุมาตรา

(2)(a) หรือผู้ซึ่งมิได้กระทำความการร้องขอภายใต้บทบัญญัติตามอนุมาตรา(2)(b)หรือ(c)ถือเป็นความผิดตามอาญาและมีโทษปรับไม่เกิน 10,000 ดอลล่าสิงคโปร์หรือจำคุกไม่เกิน3 ปีหรือทั้งจำทั้งปรับ

(4) ในกรณีที่บุคคลใดได้ต้องโทษภายใต้บทบัญญัติตามอนุมาตรา (3)และมีพยานหลักฐานที่ได้จากการถอดรหัสแสดงให้เห็นว่าได้วางแผน ตระเตรียม หรือได้ถูกใช้ให้กระทำความผิดอุกฉกรรจ์ที่กำหนดไว้ (Specified serious offence) จะต้องได้รับการลงโทษต่อไปนี้แทนการกำหนดโทษภายใต้บทบัญญัติตามอนุมาตรา (3)

(a) จะต้องได้รับโทษเช่นเดียวกันกับโทษในความผิดอุกฉกรรจ์ที่กำหนดไว้(Specified serious offence)นั้นเว้นแต่โทษนั้นมีโทษที่กำหนดไว้เกินกว่า โทษปรับ 50,000 ดอลล่าห์สิงคโปร์หรือจำคุกไม่เกิน 10 ปีหรือทั้งจำทั้งปรับ หรือ

(b) จะต้องได้รับการลงโทษปรับ50,000 ดอลล่าห์สิงคโปร์หรือจำคุกไม่เกิน 10 ปีหรือทั้งจำทั้งปรับ ในกรณีที่ความผิดอุกฉกรรจ์ที่กำหนดไว้(Specified serious offence)นั้นมีโทษถึงขั้นจำคุกตลอดชีวิตหรือประหารชีวิต

(5) เพื่อวัตถุประสงค์ของอนุมาตรา (4) และกรณีตามอนุมาตรา (6) "ความผิดอุกฉกรรจ์ที่กำหนดไว้ (Specified serious offence)" หมายถึง ความผิดภายใต้กฎหมายที่ระบุไว้ดังต่อไปนี้

(a) กฎหมายลายลักษณ์อักษรใดที่มีความผิดที่กำหนดไว้เกี่ยวกับการฆ่าหรือทำร้ายร่างกาย

(b) กฎหมายลายลักษณ์อักษรใดที่เกี่ยวกับการกระทำหรือขู่เข็ญว่าจะกระทำการอันเป็นภัยคุกคามต่อความมั่นคงของชาติ

(c) กฎหมายลายลักษณ์อักษรใดที่เกี่ยวกับอาวุธรังสีหรืออาวุธชีวภาพ

(d) Arms and Explosives Act (Cap. 13);

(e) Chemical Weapons (Prohibition) Act (Cap. 37B);

(f) Corrosive and Explosive Substances and Offensive Weapons Act (Cap. 65);

(g) Hijacking of Aircraft and Protection of Aircraft and International Airports Act (Cap. 124);

(h) Kidnapping Act (Cap. 151);

(i) Maritime Offences Act (Cap. 170B);

(j) Official Secrets Act (Cap. 213);

(k) Protected Areas and Protected Places Act (Cap. 256);

(l) Statutory Bodies and Government Companies (Protection of Secrecy) Act (Cap. 319);

(m) Strategic Goods (Control) Act (Cap. 300);

(n) Terrorism (Suppression of Financing) Act (Cap. 325);

(o) United Nations (Anti-Terrorism Measures) Regulations (Cap. 339, Rg 1); and

(p) รวมถึงกฎหมายลายลักษณ์อักษรอื่นที่รัฐมนตรีกำหนด

(6) ไม่มีความผิดใดที่จะถือเป็นความผิดอุกฉกรรจ์ที่กำหนดไว้ (Specified serious offence) เว้นแต่โทษสูงสุดที่กำหนดไว้สำหรับความผิดนั้น จะเป็นไปตามที่ระบุไว้ดังนี้

(a) มีโทษจำคุก 5 ปี หรือมากกว่านั้น

(b) มีโทษจำคุกตลอดชีวิต หรือ

(c) ประหารชีวิต

(7) ในการดำเนินคดีกับบุคคลใดสำหรับความผิดภายใต้มาตรานี้ ถ้าหากพิสูจน์ได้ว่าบุคคลนั้นครอบครองรหัสข้อมูล(Decryption information) ในเวลาใดก่อนที่จะมีการร้องขอ(Request)เพื่อการเข้าถึงข้อมูล เพื่อประโยชน์ในการดำเนินคดีให้สันนิษฐานว่าบุคคลเช่นว่านั้นยังคงครอบครองครอบรหัสข้อมูลต่อมาภายหลังอย่างต่อเนื่อง เว้นแต่ จะพิสูจน์ได้ว่ารหัสข้อมูลนั้น

(a) เขามิได้ครอบครองในช่วงเวลาที่ได้มีการได้ร้องขอ (Request) และ

(b) เขามิได้ครอบครองอย่างต่อเนื่องภายหลังได้มีการร้องขอ (Request)

(8) บุคคลใดที่กระทำการโดยสุจริต หรือ ยินยอมกระทำการตามการร้องขอภายใต้อนุมาตรา (2) ไม่มีความผิดทางอาญา และไม่ต้องรับผิดใดๆในทางแพ่งตามกฎหมาย

(9) ตามมาตรานี้ ได้นิยามความหมายของคำว่า “data” “Encrytion information” “ Encypted data ” และ “Plain text version” ไว้ด้วย[100]”

---

[100] data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer;

"decryption information" means information, code or technology or part thereof that enables or facilitates the retransformation or unscrambling of encrypted data from its unreadable and incomprehensible format to its plain text version;

"encrypted data" means data which has been transformed or scrambled from its plain text version to an unreadable or incomprehensible format, regardless of the technique utilized for such transformation or scrambling and irrespective of the medium in which such data occurs or can be found for the purposes of protecting the content of such data;

"plain text version" means original data before it has been transformed or scrambled to an unreadable or incomprehensible format

3.บทคุ้มครองการสืบสวนโดยตำรวจและเจ้าหน้าที่ตามกฎหมาย (Saving for investigations by police and law enforcement officers)

หลักการนี้บัญญัติขึ้นนอกเหนือจากประมวลกฎหมายวิธีพิจารณาความอาญา โดยกำหนดบทคุ้มครองตำรวจและเจ้าหน้าที่ที่กระทำการโดยชอบด้วยกฎหมายไว้ในกฎหมาย Computer Misuse Act ดังนี้

" มาตรา14 ไม่มีสิ่งใดในกฎหมายนี้จะห้ามหน้าที่ตำรวจ บุคคลผู้ได้รับอนุญาตตามความหมายของมาตรา 125A ตามประมวลกฎหมายวิธีพิจารณาความอาญา (Cap. 68) หรือเจ้าหน้าที่รักษากฎหมายที่ได้รับอนุญาตตามความเหมาะสม จากการกระทำการสืบสวนตามอำนาจที่ชอบตามที่กฎหมายบัญญัติไว้ "[101]

4.การป้องกันหรือการตอบโต้ ภัยคุกคามต่อความมั่นคงของชาติ และกรณีอื่น (Preventing or countering threats to national security, etc)

หลักการนี้ถูกเพิ่มเติมในการแก้ไข Computer Misuse Act[102] โดยยกเลิกมาตรา 15 และเพิ่มเติมมาตรา 15 A แทนโดยหลักการตามมาตรา 15 ได้ถูกนำไปบัญญัติไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 125A และมาตรา125 B

โดยเหตุผลที่จำเป็นต้องเพิ่มเติมหลักการนี้ในกฎหมาย Computer Misuse Act เนื่องจากเล็งเห็นถึงความสำคัญของสาธารณูปโภคพื้นฐานที่จำเป็น เช่น น้ำประปา ไฟฟ้า ก๊าซ เทคโนโลยีการสื่อสารและการคมนาคมที่จำเป็นจะต้องพึ่งพาเครือข่ายคอมพิวเตอร์มากขึ้น จึงมีโอกาสที่จะถูกโจมตีจากผู้ก่อการร้ายหรือผู้กระทำความผิดทางอาญา นำมาซึ่งความเสียหายต่อระบบเศรษฐกิจและความมั่นคงของชาติ จึงจำเป็นที่จะต้องให้อำนาจกับหน่วยงานรักษาความปลอดภัยที่จะป้องกันก่อน(Preemptive) ที่จะมีการโจมตีทางไซเบอร์ โดยมาตรา 15A ที่บัญญัติขึ้นมาใหม่นี้ได้ให้อำนาจรัฐมนตรีที่จะมอบหมายให้บุคคลหรือองค์กรใดในการใช้มาตรการที่จำเป็นในการป้องกันหรือตอบโต้การกระทำที่เป็นภัยต่อสาธารณูปโภคพื้นฐาน การป้องกันประเทศ หรือ ความสัมพันธ์ระหว่างประเทศกับสิงคโปร์ มาตรการตามมาตรา15A นี้สามารถใช้จัดการกับ

---

[101] Computer Misuse Act -Saving for investigations by police and law enforcement officers

[102] Computer Misuse (Amendment)Act มีผลบังคับใช้เมื่อ 01/01/2006

สถานการณ์ฉุกเฉินที่ถูกโจมตีทางไซเบอร์ หรือ การจับสัญญาณว่าจะมีการโจมตีสถานที่สำคัญ เช่น โรงงานผลิตไฟฟ้าหรือโรงงานผลิตน้ำประปาโดยมาตรการนี้จะถูกนำมาใช้อย่างจำกัดสำหรับวัตถุประสงค์ในการป้องกันหรือตอบโต้การกระทำที่เป็นภัยต่อความมั่นคงของชาติหรือสาธารณูปโภคพื้นฐานที่จำเป็นเท่านั้น แต่จะไม่นำมาใช้กับการกระทำผิดอาญาทั่วไป[103] ซึ่งมาตรา 15 A มีเนื้อหาดังนี้

" มาตรา 15A ในกรณีที่รัฐมนตรีพิสูจน์ตามสมควรแล้วว่า เป็นการจำเป็นเพื่อวัตถุประสงค์ที่จะป้องกันหรือตอบโต้ ภัยคุกคามต่อความมั่นคงของชาติ บริการที่จำเป็น(Essential services) การป้องกันประเทศ หรือความสัมพันธ์ระหว่างประเทศของสิงคโปร์ รัฐมนตรีที่มีอำนาจอาจมอบอำนาจให้บุคคลหรือองค์กรใด ที่ถูกระบุในคำอนุญาตนั้น ให้ดำเนินมาตรการเท่าที่จำเป็นต่อการป้องกันหรือตอบโต้ ภัยคุกคามต่อคอมพิวเตอร์เครื่องหนึ่ง หรือบริการคอมพิวเตอร์นั้น หรือกลุ่มคอมพิวเตอร์หรือบริการคอมพิวเตอร์หลายบริการ(a computer or computer service or any class of computers or computer services)

(2) มาตรการที่กล่าวถึงในอนุมาตรา (1) โดยไม่จำกัดอยู่เท่านี้ อาจรวมถึงการดำเนินการโดยบุคคลหรือองค์กรที่ได้รับมอบหมายให้ใช้อำนาจที่กล่าวถึงในมาตรา 125A และ 125B[104] ของประมวลกฎหมายวิธีพิจารณาความอาญา (Cap. 68)

(3) ในกรณีที่ความผิดถูกเปิดเผยในโดยการกระทำหรือเนื่องมาจากการใช้อำนาจตามมาตรานี้

(a) ไม่มีข้อมูลใดเกี่ยวกับความผิดนั้นจะถูกรับฟังเป็นพยานหลักฐานในการพิจารณาความแพ่งหรืออาญา

(b) ไม่มีพยานบุคคลใดจะต้องให้การในการพิจารณาความแพ่งหรืออาญา ในเรื่อง

(i) การจะเปิดเผยชื่อ ที่อยู่ หรือข้อมูลจำเพาะอย่างอื่นของตัวผู้ให้ข้อมูลเกี่ยวกับความผิดนั้น หรือ ,

---

[103] Ministry of Home Affairs, "Computer Misuse (Amendment) Act," http://www.mha.gov.sg/basic_content.aspx?pageid=52

[104] ได้กล่าวถึงมาตรา 125A และ 125B มาแล้วข้างต้น ในหัวข้ออำนาจเข้าถึงคอมพิวเตอร์(Power to access computer) และอำนาจถอดรหัสของข้อมูล(Power to access decryption information)

(ii) การตอบคำถามใดหากคำตอบนั้นจะนำไปสู่ หรือมีแนวโน้มที่จะนำไปสู่การเปิดเผยชื่อ ที่อยู่ หรือข้อมูลจำเพาะอย่างอื่นของตัวผู้ให้ข้อมูล

(4) หากหนังสือ เอกสาร ข้อมูล หรือการแสดงออกจากคอมพิวเตอร์ชิ้นใดซึ่งได้รับฟังไว้เป็นพยานหลักฐานหรือจำเป็นต้องถูกสอบสวนในการพิจารณาความแพ่งหรืออาญา มีการลงบันทึกซึ่งระบุหรือแจ้งชื่อผู้ให้ข้อมูล หรือที่อาจนำไปสู่การเปิดเผยตัวผู้ให้ข้อมูล ศาลจะต้องทำให้การลงบันทึกเหล่านั้นถูกปกปิดจากการดูหรือการถูกถอดความได้เท่าที่จะจำเป็นต่อการปกป้องตัวผู้ให้ข้อมูลจากการถูกเปิดเผย

(5)ในอนุมาตรา (1) " บริการที่จำเป็น(Essential services) " หมายความว่า

(a) บริการต่างๆที่เกี่ยวข้องโดยตรงกับโครงสร้างพื้นฐานด้านการสื่อสาร การเงินและการธนาคาร บริการสาธารณะ การขนส่งสาธารณะ หรือโครงสร้างพื้นฐานสำคัญของสาธารณะ และ

(b) บริการฉุกเฉินอย่างเช่น ตำรวจ ป้องกันภัยพลเรือน หรือบริการทางการแพทย์ "

5.การจับกุมโดยตำรวจโดยไม่ต้องมีหมาย(Arrest by police without warrant)

ตามประมวลกฎหมายวิธีพิจารณาความอาญาของประเทศสิงคโปร์ได้แบ่งประเภทของการจับกุมความผิดออกเป็น 2 ประเภท คือ1. "Seizable offence"[105] คือ การจับกุมที่เจ้าพนักงานตำรวจสามารถจับได้โดยไม่ต้องมีหมายเมื่อมีเหตุอันควรเชื่อได้ว่าบุคคลใดได้กระทำความผิดตามที่กฎหมายระบุไว้ และในกรณีนี้กฎหมายอนุญาตให้เจ้าพนักงานตำรวจสามารถทำการค้นในสถานที่รโหฐานได้โดยไม่ต้องมีหมายค้น[106] และ 2."Non-seizable offence"[107] คือ การจับกุมที่ต้องมีหมาย เมื่อพิจารณาจากประมวลกฎหมายวิธีพิจารณาความอาญาของประเทศสิงคโปร์แล้วจะเห็นได้ว่าการจับกุมโดยไม่ต้องมีหมายจำกัดเฉพาะความผิดที่กฎหมายระบุไว้ตาม

---

[105] "Seizable offence" means an offence for which and "seizable case" means a case in which a police officer may ordinarily arrest without warrant according to the third column of Schedule A

[106] Siva Murugaiyan/Parveen Kaur Nagpal ,Azman Soh and Murugaiyan, "Introduction to Singapore Law and Legal System ," www.sma.org.sg/whatsnew/ethics/Y1_S2_siva_article.doc

[107] "Non-seizable offence" means an offence for which and "non-seizable case" means a case in which a police officer may not ordinarily arrest without warrant according to the third column of Schedule A

ตารางท้ายประมวลเท่านั้น(The third column of Schedule A) ดังนั้น เพื่อประโยชน์ในการดำเนินคดีจึงได้มีการกำหนดให้ฐานความผิดตามกฎหมายComputer Misuse Act เป็นความผิดที่สามารถจับกุมได้โดยไม่ต้องมีหมาย ตามมาตรา 16 ดังนี้

" มาตรา16 เจ้าพนักงานตำรวจอาจจับกุมบุคคลใดที่มีเหตุอันควรสงสัยว่าได้กระทำความผิดตามกฎหมายนี้ได้โดยไม่มีต้องมีหมาย "

ข้อสังเกตประการหนึ่งของกฎหมายฉบับนี้ คือกฎหมายฉบับนี้มีต้นแบบมาจากกฎหมาย Computer Misuse Act ของประเทศอังกฤษ แต่กฎหมายฉบับนี้ได้พัฒนาขึ้นในช่วงปี 1990 ซึ่งเป็นช่วงยังไม่มีการใช้อินเทอร์เน็ตอย่างแพร่หลาย บทบัญญัติต่างๆ จึงไม่เพียงพอต่อการลงโทษการกระทำความผิดทางคอมพิวเตอร์ที่มีการพัฒนาอย่างต่อเนื่อง[108]

4.3 ประเทศอินเดีย

ในประเทศอินเดีย การกำหนดฐานความผิดและการดำเนินคดีกับผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้บัญญัติไว้ใน The Information technology Act , 2000 โดยวัตถุประสงค์เพื่อควบคุมการติดต่อสื่อสารและการรวบรวมข้อมูลในทางการค้าอิเล็กทรอนิกส์ (Electronic commerce) ที่มีความแตกต่างจากการค้าในรูปแบบเดิมที่เก็บรวมรวมข้อมูลทางการค้าไว้ในรูปแบบเอกสาร กฎหมายฉบับนี้จึงได้บัญญัติถึงพยานหลักฐานอิเล็กทรอนิกส์ประเภทต่างๆไว้ เช่น Digital Signature และมีการบัญญัติแก้ไขกฎหมายอื่นๆ[109]ที่เกี่ยวข้องกับพยานหลักฐานอิเล็กทรอนิกส์ไว้อีกด้วย

---

[108] สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ,ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, "แนวทางการจัดทำกฎหมายอาชญากรรมทางคอมพิวเตอร์ ," หน้า 69.

[109] ได้แก่ THE FIRST SCHEDULE - Amendments to the indian penal code ,THE SECOND SCHEDULE - Amendments to the Indian Evidence Act, 1872 , THE THIRD SCHEDULE - Amendments to the bankers' books evidence act ' 891 ,THE FOURTH SCHEDULE - Amendment to the reserve bank of india act, 1934 นอกจากนี้ยังมีประกาศในเรื่องระเบียบปฏิบัติของทางรัฐบาลกลาง อีก2 ฉบับ ได้แก่ The information Technology (Certification Authorities) Rules และ Cyber Regulations Appellate Tribunal (Procedure) Rules

[110] Rodney Ryder, "India: India's cyber crimes" http:// www.legalweek.com

[111] The Information technology Act , 2000 ส่วนแรก

การกำหนดฐานความผิดตามกฎหมายฉบับนี้ไม่ได้อ้างอิงฐานความผิดที่กำหนดไว้ในแบบสากล[110] กล่าวคือมิได้จัดหมวดหมวดหมู่โดยใช้The Council of Europe Convention on Cybercrimeเป็นต้นแบบ (แต่ได้ใช้ UNCITRAL's (United Nations Commission on International Trade Laws) เป็นต้นแบบ[111]) โดยได้กำหนดฐานความผิดไว้ เช่น การเจาะระบบคอมพิวเตอร์ (Hacking with computer system) การเข้ายุ่งเกี่ยวกับเอกสารทางคอมพิวเตอร์(Tampering with computer source document) การเผยแพร่ข้อมูลอันลามกในรูปแบบอิเล็กทรอนิกส์ (Publishing of information which is obscene in the electronic form) ละเมิดความลับและความเป็นส่วนตัว (Breach of confidentiality and privacy) การจัดพิมพ์ใบรับรองลายมือชื่อดิจิตอลอันเป็นเท็จโดยจงใจเป็นการเฉพาะและเพื่อวัตถุประสงค์ในทางฉ้อฉล(Publishing digital signature certificate false in certain particulars and for fraudulent purpose) เป็นต้น

กฎหมายฉบับนี้ได้มีการจัดตั้ง Cyber Appellate Tribunal[112] เพื่อพิจารณาคดีตามกฎหมายฉบับนี้แทนการฟ้องต่อศาลตามปกติ และได้มีการจัดตั้งองค์กรCertification Authority[113] เพื่อควบคุมและออกใบรับรองลายมือชื่อดิจิตอล ส่วนการดำเนินคดีอาญาในชั้นสืบสวนได้มีการกำหนดหลักการให้พนักงานตำรวจยศไม่ต่ำกว่าชั้นรองผู้กำกับการ (Deputy superintendent) จึงจะมีอำนาจสืบสวนตามกฎหมายฉบับนี้[114]

<u>อำนาจของพนักงานตำรวจหรือพนักงานอื่นในการเข้าไป,ค้น หรือใช้วิธีการอื่น</u> <u>(Power of police officer and other officers to enter, search, etc.)</u>

หลักการนี้ถูกกำหนดไว้ใน CHAPTER XIII - Miscellaneous[115] ในมาตรา 80 โดยให้อำนาจเจ้าพนักงานตำรวจที่มีอำนาจหรือเจ้าหน้าที่อื่นที่ได้รับการแต่งตั้งในการเข้าไปใน

---

[112] The Information technology Act, Articles 48-64.

[113] Ibid., Articles 17-34

[114] Article 78 " Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Deputy Superintendent of Police shall investigate any offence under this Act. "

[115] รัฐบัญญัติฉบับนี้แบ่งออกเป็น 13 Chapter ได้แก่ CHAPTER I - Preliminary , CHAPTER II - Digital Signature , CHAPTER III - Electronic Governance ,CHAPTER IV - Attribution, Acknowledgemet and Despatch of Electronic Records , CHAPTER V - Secure Electronic Records and Secure Digital Signature , CHAPTER VI - Regulation of Certifying Authorities , CHAPTER VII - Digital Signature

สถานที่สาธารณะและค้นและจับบุคคลได้โดยไม่ต้องมีหมายเมื่อมีเหตุอันควรสงสัยหรือได้กระทำความผิดหรือกำลังกระทำความผิดหรือได้เกี่ยวข้องกับการกระทำความผิดภายใต้กฎหมายฉบับนี้ โดยบทบัญญัติดังกล่าวมีเนื้อหาดังนี้

" มาตรา 80 อำนาจของพนักงานตำรวจหรือพนักงานอื่นในการเข้าไป,ค้น หรือใช้วิธีการอื่น(Power of police officer and other officers to enter, search, etc.)

(1) ไม่ว่าประมวลกฎหมายวิธีพิจารณาความอาญา 1973 จะกำหนดไว้อย่างไรก็ตาม, เจ้าพนักงานตำรวจ ที่มียศไม่ต่ำกว่าชั้นรองผู้กำกับการ (Deputy superintendent) หรือพนักงานอื่นของรัฐบาลกลางหรือรัฐบาลรัฐที่ได้รับมอบหมายจากรัฐบาลกลาง ให้มีอำนาจเข้าไปในสถานที่สาธารณะ(Public place) และค้นและจับได้โดยไม่ต้องมีหมาย (Without warrant) เมื่อได้พบบุคคลใดที่มีเหตุอันควรสงสัย (Reasonably suspect) หรือได้กระทำความผิดหรือกำลังกระทำความผิดหรือได้เกี่ยวข้องกับการกระทำความผิดใดๆภายใต้กฎหมายฉบับนี้

คำอธิบาย (Explanation) –เพื่อวัตถุประสงค์ของอนุมาตรานี้- การให้ความหมายของคำว่า " สถานที่สาธารณะ(Public place) " ให้หมายรวมถึงยานพาหนะสาธารณะ,โรงแรมใด, ร้านค้าใด หรือ สถานที่อื่นเช่นเดียวกันนั้น, หรือสามารถเข้าสู่สาธารณะได้

(2) ในกรณีที่บุคคลใดถูกจับภายใต้อนุมาตรา (1).โดยเจ้าหน้าที่อื่นนอกเหนือจากเจ้าพนักงานตำรวจ ,โดยไม่ชักช้าโดยไม่จำเป็น เจ้าหน้าที่เช่นว่านั้นจะต้องนำหรือส่งตัวผู้ถูกจับก่อนที่ศาลจะมีอำนาจในคดีหรือก่อนพนักงานผู้รับผิดชอบยังสถานีตำรวจ

(3) บทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญา 1973 จะต้องอยู่ภายใต้บทบัญญัติของมาตรานี้ , การใช้,รวมถึงการเข้าไป ค้น จับจะต้องอยู่ภายใต้มาตรานี้ "

ในส่วนของหน้าที่และความรับผิดของผู้ให้บริการอินเทอร์เน็ต กฎหมายฉบับนี้ไม่ได้กำหนดให้ผู้ให้บริการอินเทอร์เน็ต (Network service provider) มีหน้าที่จัดเก็บข้อมูลคอมพิวเตอร์ในส่วนของเนื้อ (Content) หรือข้อมูลจราจร (Traffic data) ของผู้ใช้บริการเพื่อ

Certificates , CHAPTER VIII - Duties of Subscribers , CHAPTER IX - Penalties and Adjudications , CHAPTER X - The Cyber Regulations Appellate Tribunal , CHAPTER XI - Offences , CHAPTER XII - Network Service Providers not to be liable in Certain Cases , CHAPTER XIII - Miscellaneous

ประโยชน์ในการสอบสวนคดีอาญา มีเพียงบทบัญญัติยังเอาผิดกับผู้ให้บริการอินเทอร์เน็ตรู้เห็นหรือละเลยไม่ป้องกันหรือต่อต้านการกระทำความผิดเท่านั้น[116]

ข้อสังเกตเกี่ยวกับกฎหมายฉบับนี้ คือ กฎหมายฉบับนี้ไม่ได้มุ่งเอาผิดทางอาญากับผู้กระทำความผิดทางคอมพิวเตอร์อย่างเคร่งครัดหรือมีบทบัญญัติที่เป็นประโยชน์ในการดำเนินคดีทางอาญาเท่าที่ควร อาจเป็นเพราะกฎหมายฉบับนี้มีต้นแบบมาจากมติสมัชชาใหญ่ของสหประชาชาติ(General Assembly Resolution) ที่ A/51/628 ที่มีวัตถุประสงค์ในการควบคุมและส่งเสริมการค้าอิเล็กทรอนิกส์ ((Electronic commerce) เป็นหลัก

4.4 สหภาพยุโรป

อนุสัญญาของคณะมนตรียุโรปว่าด้วยการกระทำผิดบนอินเทอร์เน็ต (The Council of Europe Convention on Cybercrime of 2001) สามารถแบ่งออกได้เป็น 4 ส่วนหลักๆ คือ Chapter I – Use of terms , Chapter II – Measures to be taken at the national level, Chapter III – International co-operation, Chapter IV – Final provisions โดยในส่วนของการดำเนินคดีได้บัญญัติไว้ในส่วน Chapter II – Measures to be taken at the national level ซึ่งแบ่งออกได้เป็น 2 ส่วน คือ ส่วนที่เกี่ยวกับการกำหนดฐานความผิด(Section 1 – Substantive criminal law)[117] และ ส่วนที่เกี่ยวกับกฎหมายวิธีสบัญญัติ(Section 2 – Procedural

---

[116] "The Information technology Act มาตรา 79For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made there under for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention.

Explanation.—For the purposes of this section,—

(a) "network service provider" means an intermediary;

(b) "third party information" means any information dealt with by a network service provider in his capacity as an intermediary;..."

[117] ได้กล่าวมาแล้วในบทที่ 2.4.1

[118] The Council of Europe Convention on Cybercrime , Article 14 – Scope of procedural provisions

law) โดยกำหนดให้รัฐสมาชิกจะต้องบัญญัติกฎหมายวิธีพิจารณาและวิธีการเพื่อประโยชน์ในการสอบสวนสำหรับความผิดเกี่ยวกับคอมพิวเตอร์โดยมีขอบเขตครอบคลุมกรณีดังต่อไปนี้[118]

1. ฐานความผิดต่างๆที่กำหนดไว้ในอนุสัญญาของคณะมนตรียุโรปว่าด้วยการกระทำผิดบนอินเทอร์เน็ต (The Council of Europe Convention on Cybercrime of 2001)

2. ความผิดอาญาอื่นๆที่ถูกกระทำโดยผ่านทางระบบคอมพิวเตอร์

3. การเก็บรวบรวมพยานหลักฐานในรูปแบบอิเล็กทรอนิกส์สำหรับความผิดอาญา

แต่ทั้งนี้ แต่ละรัฐอาจจำกัดสิทธิในการออกกฎหมายมิให้ครอบคลุมถึง การใช้คอมพิวเตอร์ที่มีกลุ่มของผู้ใช้ในวงจำกัดและไม่ได้ใช้เครือข่ายการสื่อสารสาธารณะและไม่ได้ถูกเชื่อมต่อกับระบบคอมพิวเตอร์อื่น ไม่ว่าจะเป็นของเอกชนหรือสาธารณะ

นอกจากนี้อนุสัญญาฉบับนี้ได้กำหนดเงื่อนไขและความคุ้มครองสิทธิของประชาชนไว้ โดยกำหนดให้กฎหมายภายในของแต่ละรัฐที่จะบัญญัติขึ้นจะต้องคุ้มครองสิทธิมนุษยชนและเสรีภาพไว้อย่างเพียงพอ รวมถึงสิทธิที่เกิดขึ้นเนื่องมาจากพันธกรณีที่ต้องปฏิบัติตามอนุสัญญาของคณะมนตรียุโรปว่าด้วยการปกป้องสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐาน ปี 1950 กติกาสหประชาชาติว่าด้วยสิทธิพลเรือนและสิทธิทางการเมือง ปี 1966 และตราสารระหว่างประเทศอื่นๆเกี่ยวกับสิทธิมนุษยชนที่สามารถปรับใช้ได้ และต้องสอดคล้องกับหลักความได้สัดส่วน[119] การกำหนดเงื่อนไขและความคุ้มครองสิทธิของประชาชนนี้ครอบคลุมถึงกระบวนการพิจารณาคดี การใช้อำนาจตุลาการ และการใช้อำนาจของหน่วยงานอิสระที่จะสามารถกระทำได้ตามที่กฎหมายให้อำนาจและตามระยะเวลาที่กฎหมายกำหนด โดยสอดคล้องกับผลประโยชน์สาธารณะที่สุดเท่าที่เป็นไปได้ โดยเฉพาะการอำนวยความยุติธรรมอย่างสมเหตุสมผล[120]

---

[119] "...the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality."

[120] Article 15 – Conditions and safeguards

ในส่วนของหลักการในการสอบสวนและรวมรวมพยานหลักฐานอนุสัญญาฉบับนี้ ได้กำหนดหลักการไว้ ดังนี้

1. การเก็บรักษาข้อมูลคอมพิวเตอร์โดยไม่ชักช้า (Expedited preservation of stored data)

การรวบรวมข้อมูลคอมพิวเตอร์ จะต้องดำเนินการโดยรวดเร็วเพื่อรักษาความถูกต้องของข้อมูลไว้อย่างสมบูรณ์เท่าที่จะทำได้ จึงกำหนดให้เจ้าหน้าที่รัฐสามารถเรียกข้อมูลคอมพิวเตอร์จากผู้ให้บริการได้อย่างรวดเร็ว โดยอนุสัญญาฉบับนี้ได้กำหนดหลักการนี้ไว้ ดังนี้

" มาตรา16 การเก็บรักษาข้อมูลคอมพิวเตอร์โดยไม่ชักช้า (Expedited preservation of stored data)

1. รัฐภาคีแต่ละรัฐจะต้องออกกฎหมายและมาตรการอื่นเท่าที่จะจำเป็นในการทำให้เจ้าหน้าที่ผู้มีอำนาจสามารถที่จะออกคำสั่งหรือในวิธีการอื่นในทำนองเดียวกันเพื่อทำให้ได้มาซึ่งข้อมูลคอมพิวเตอร์ที่เก็บรักษาไว้โดยไม่ชักช้า รวมถึงข้อมูลจราจรทางคอมพิวเตอร์ ซึ่งถูกเก็บไว้ในระบบคอมพิวเตอร์ โดยเฉพาะกรณีมีเหตุอันควรเชื่อได้ว่าข้อมูลคอมพิวเตอร์ดังกล่าวมีความเสี่ยงต่อการสูญหายหรือถูกแก้ไขเปลี่ยนแปลง

2. เพื่อการบังคับตามข้อ1อาจใช้วิธีการออกคำสั่งไปยังบุคคลที่ครอบครองหรือควบคุมคอมพิวเตอร์ให้เก็บรักษาข้อมูลคอมพิวเตอร์นั้นไว้ภายในระยะเวลายาวนานเท่าที่จำเป็น โดยมีระยะเวลายาวนานสูงสุดไม่เกิน 90 วัน(แต่อาจกำหนดให้สามารถขอขยายระยะเวลาได้) เพื่อให้เจ้าหน้าที่ที่เกี่ยวข้องสามารถตรวจสอบข้อมูลดังกล่าวได้

3. การดำเนินคดีทางกฎหมายและมาตรการอื่นๆเท่าที่จะจำเป็นดังกล่าวที่จะผูกพันผู้เก็บรักษาข้อมูลหรือบุคคลอื่นที่จะต้องเก็บรักษาข้อมูลคอมพิวเตอร์ตามกระบวนการเหล่านี้ ไว้เป็นความลับในช่วงระยะเวลาที่กฎหมายกำหนด..."

2. การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์โดยไม่ชักช้าและการเปิดเผยข้อมูลจราจรทางคอมพิวเตอร์บางส่วน (Expedited preservation and partial disclosure of traffic data)

การรวบรวมข้อมูลจราจรทางคอมพิวเตอร์(Traffic data) จะต้องทำโดยรวดเร็วเช่นกัน เพื่อให้เจ้าหน้าที่สามารถทราบถึงเส้นทางการสื่อสาร และข้อมูลเบื้องต้นที่ทำให้สามารถระบุตัวผู้ใช้บริการ เช่น ข้อมูลประเภทหมายเลขID, IP Address เป็นต้น ดังที่ได้บัญญัติไว้ ดังนี้

" มาตรา 17 การเก็บรักษาข้อมูลคอมพิวเตอร์โดยไม่ชักช้า (Expedited preservation of stored data)

1.ภายใต้หลักเกณฑ์ข้อ 16 รัฐภาคีแต่ละรัฐจะต้องออกกฎหมายและมาตรการอื่นเท่าที่จะจำเป็นเพื่อที่จะ

a .ประกันว่าการรักษาข้อมูลจราจรทางคอมพิวเตอร์โดยไม่ชักช้าโดยไม่คำนึงถึงว่าผู้ให้บริการรายหนึ่งหรือหลายราย จะเกี่ยวข้องในการรับส่งการสื่อสารนั้นหรือไม่ และ

b .ประกันการเปิดเผยโดยไม่ชักช้าต่อเจ้าหน้าที่ผู้มีอำนาจของรัฐภาคีหรือบุคคลที่ได้รับมอบหมายจากเจ้าหน้าที่นั้น ซึ่งข้อมูลการจราจรที่เพียงพอต่อการทำให้สามารถระบุตัวผู้ใช้บริการและเส้นทางผ่านซึ่งการสื่อการที่รับส่งข้อมูลนั้น..."

3. การสั่งให้จัดทำ(Production order)

ในการดำเนินคดีให้เกิดประสิทธิภาพจะต้องบันทึกและเก็บรักษาข้อมูลบางประเภทไว้ รัฐจึงควรกำหนดให้ผู้ให้บริการจัดเก็บข้อมูลที่ทำให้สามารถระบุตัวผู้ครอบครองหรือใช้คอมพิวเตอร์ นอกเหนือจากข้อมูลคอมพิวเตอร์และข้อมูลจราจรทางคอมพิวเตอร์ และส่งมอบข้อมูลดังกล่าวให้แก่เจ้าหน้าที่ เช่น ข้อมูลที่บันทึกในกระดาษ ข้อมูล Log file เป็นต้น ดังนี้

" มาตรา 18 การสั่งให้จัดทำ(Production order)

1. รัฐภาคีแต่ละรัฐจะต้องออกกฎหมายและมาตรการอื่นเท่าที่อาจจะจำเป็นในการที่จะให้อำนาจเจ้าหน้าที่ผู้มีอำนาจในการออกคำสั่ง

a. ให้บุคคลในดินแดนของตนรัฐนั้นส่งมอบข้อมูลคอมพิวเตอร์โดยเจาะจงที่อยู่ในความครอบครองหรือควบคุมของบุคคลนั้น ซึ่งถูกเก็บไว้ในระบบคอมพิวเตอร์ หรือสื่อเก็บข้อมูลคอมพิวเตอร์ และ

b. ให้ผู้ให้บริการของรัฐนั้นส่งมอบข้อมูลของผู้ใช้บริการ ซึ่งอยู่ในความครอบครองหรือควบคุมของตน

2. อำนาจและการดำเนินคดีที่กล่าวมานี้ต้องอยู่ภายใต้หลักเกณฑ์ข้อ 14 และ 15

3. เพื่อวัตถุประสงค์ของข้อนี้ คำว่า "ข้อมูลของผู้ใช้บริการ" หมายความว่า ข้อมูลใดที่ถูกเก็บไว้ในรูปแบบของข้อมูลคอมพิวเตอร์หรือรูปแบบอื่นใดที่ครอบครองโดยผู้จัดทำบริการเกี่ยวกับผู้ใช้บริการของผู้จัดทำบริการรายนั้นนอกเหนือไปจากข้อมูลจราจรทางคอมพิวเตอร์หรือข้อมูลเนื้อหาและจัดทำสิ่งต่างๆ เหล่านี้ ได้แก่

a.ชนิดของการสื่อสารที่ถูกใช้ การจัดทำบริการทางเทคนิคที่ถูกใช้ในการนั้น และระยะเวลาในการบริการ

b. ข้อมูลระบุตัวผู้ใช้บริการ ที่อยู่ทางไปรษณีย์หรือทางภูมิศาสตร์ หมายเลขโทรศัพท์และหมายเลขเข้าใช้บริการ ข้อมูลการชำระเงินและใบเสร็จรับเงิน ทั้งนี้ตามข้อตกลงหรือการให้บริการ

c. ข้อมูลอื่นใดในที่ตั้งของอุปกรณ์การสื่อสาร ทั้งนี้ตามข้อตกลงหรือการให้บริการ"

4.การค้นและยึดซึ่งข้อมูลคอมพิวเตอร์ที่ถูกเก็บไว้ (Search and seizure of stored computer data)

การค้นและยึดข้อมูลคอมพิวเตอร์ที่ถูกเก็บไว้ควรกำหนดให้มีความแตกต่างจากการวิธีการค้นและยึดตามปกติ เช่น หากข้อมูลที่ต้องการถูกเก็บไว้ในระบบคอมพิวเตอร์อื่น การค้นจะถูกขยายผลไปยังระบบคอมพิวเตอร์นั้นได้ด้วย และต้องให้อำนาจเจ้าหน้าที่ในการจัดทำและรักษาสำเนาของข้อมูลคอมพิวเตอร์ และรักษาความสมบูรณ์ของข้อมูลคอมพิวเตอร์ที่ถูกเก็บไว้ ดังนี้

" มาตรา 19 การค้นและยึดซึ่งข้อมูลคอมพิวเตอร์ที่ถูกเก็บไว้ (Search and seizure of stored computer data)

1. รัฐภาคีแต่ละรัฐจะต้องออกกฎหมายและมาตรการอื่นที่จำเป็นเพื่อที่จะให้อำนาจเจ้าพนักงานที่เกี่ยวข้องในการค้น หรือวิธีการคล้ายคลึงกันในการเข้าถึง:

a. ระบบคอมพิวเตอร์หรือส่วนหนึ่งส่วนใดของระบบและข้อมูลคอมพิวเตอร์ที่ถูกเก็บไว้ในนั้น และ

b. สื่อเก็บข้อมูลคอมพิวเตอร์ ในที่ซึ่งข้อมูลคอมพิวเตอร์อาจถูกเก็บไว้ในดินแดนของรัฐนั้น

2. รัฐภาคีแต่ละรัฐจะต้องออกกฎหมายและมาตรการอื่นเท่าที่อาจจะจำเป็นเพื่อที่จะประกันว่า ในการที่เจ้าหน้าที่ของตนค้น หรือการเข้าถึงระบบคอมพิวเตอร์หรือบางส่วนของระบบนั้น เป็นไปตามวรรค 1 a และมีเหตุอันควรเชื่อว่าข้อมูลที่ถูกค้นหาถูกเก็บอยู่ในระบบคอมพิวเตอร์หรือส่วนของระบบแห่งอื่นในดินแดนของรัฐนั้น และเมื่อได้ข้อมูลโดยการค้นโดยชอบด้วยกฎหมายในครั้งแรกแล้ว เจ้าหน้าที่สามารถขยายผลการค้น เพื่อค้นและเข้าถึงระบบอื่นๆได้

3. รัฐภาคีแต่ละรัฐจะต้องออกกฎหมายและมาตรการอื่นเท่าที่อาจจะจำเป็นเพื่อที่จะให้อำนาจเจ้าหน้าที่ที่เกี่ยวข้องในการยึดและเช่นเดียวกันนั้นอายัดข้อมูลคอมพิวเตอร์ที่ถูกเข้าถึงตามวรรค 1 และ 2 มาตรการเหล่านี้จะต้องให้อำนาจที่จะ

a. ยึดหรือได้มาด้วยวิธีการคล้ายคลึงกันซึ่งระบบคอมพิวเตอร์หรือบางส่วนของระบบหรือสื่อการเก็บข้อมูลคอมพิวเตอร์

b. ทำและเก็บรักษาสำเนาของข้อมูลคอมพิวเตอร์เหล่านั้น

c. รักษาความสมบูรณ์ของข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องซึ่งถูกเก็บไว้

d. ย้ายที่ หรือลบข้อมูลเพื่อทำให้ข้อมูลคอมพิวเตอร์เหล่านั้นไม่สามารถถูกเข้าถึงได้

4. รัฐภาคีแต่ละรัฐจะต้องออกกฎหมายและมาตรการอื่นเท่าที่จำเป็นเพื่อที่จะให้อำนาจเจ้าพนักงานที่เกี่ยวข้องของตนในการสั่งบุคคลผู้ใดผู้มีความรู้เกี่ยวกับการทำงานของระบบคอมพิวเตอร์หรือมาตรการที่ใช้เพื่อป้องกันข้อมูลคอมพิวเตอร์ภายในระบบนั้น ตามความเหมาะสมให้จัดทำข้อมูลที่จำเป็น เพื่อให้สามารถดำเนินมาตรการที่ถูกกล่าวถึงในวรรค 1 และ 2 ได้ ..."

5. การรวบรวมข้อมูลจราจรทางคอมพิวเตอร์แบบReal-time((Real time collection of traffic data)

การรวบรวมข้อมูลจราจรทางคอมพิวเตอร์แบบReal-time เป็นการรวบรวมข้อมูลที่มิได้เกี่ยวข้องกับเนื้อหา(Non-Content) แต่เป็นการรวบรวมข้อมูลที่แสดงถึงต้นทางและปลายทางของการสื่อสาร ดังนี้

" มาตรา20 การรวบรวมข้อมูลจราจรทางคอมพิวเตอร์แบบReal-time((Real time collection of traffic data)

รัฐภาคีแต่ละฝ่ายจะต้องออกกฎหมายและมาตรการอื่นเท่าที่อาจจะจำเป็นเพื่อที่จะให้อำนาจเจ้าพนักงานที่เกี่ยวข้องของตนในการที่จะ

a. เก็บรวบรวมหรือทำบันทึกผ่านการใช้เครื่องมือทางเทคนิคในดินแดนของรัฐภาคีนั้น และ

b. บังคับผู้ให้บริการ ตามความสามารถทางเทคนิคของผู้จัดทำบริการรายนั้น ให้:

i. เก็บรวบรวมหรือทำบันทึกผ่านการใช้เครื่องมือทางเทคนิคในดินแดนของรัฐภาคีนั้น หรือให้ความร่วมมือและช่วยเหลือเจ้าหน้าที่ที่เกี่ยวข้องในการเก็บรวบรวมหรือทำบันทึกเกี่ยวกับข้อมูลข้อมูลจราจรทางคอมพิวเตอร์(Traffic data) ในแบบ Real-time จากการสื่อสารใดโดยเจาะจง ในดินแดนของรัฐนั้น ที่ถูกรับส่งโดยเครื่องมือของระบบคอมพิวเตอร์

ii. ในกรณีที่รัฐภาคี ไม่สามารถใช้มาตรการที่ถูกกล่าวถึงในวรรค 1 ก เนื่องจากระบบกฎหมายภายในของรัฐนั้น รัฐนั้นอาจใช้มาตรการทางนิติบัญญัติหรือทางอื่นเท่าที่จะจำเป็นในการที่จะประกันว่ามีการเก็บรวบรวมหรือการทำบันทึกข้อมูลจราจรทางคอมพิวเตอร์(Traffic data)ใดโดยเจาะจงแบบreal-timeในดินแดนของรัฐนั้นผ่านการใช้เครื่องมือทางเทคนิคในดินแดนของรัฐนั้นแทน

3. รัฐภาคีแต่ละรัฐจะต้องออกกฎหมายหรือมาตรการอื่นเท่าที่จำเป็นในการบังคับให้ผู้ให้บริการรักษาความลับเรื่องข้อเท็จจริงในการใช้อำนาจใดที่บัญญัติไว้ในข้อนี้และข้อมูลที่เกี่ยวข้องของการใช้อำนาจ..."

6. การดักการสื่อสารของเนื้อหาข้อมูล(Interception of content data)

การดักการสื่อสารของเนื้อหาข้อมูลมีความแตกต่างจากการรวบรวมข้อมูลจราจรทางคอมพิวเตอร์ เพราะการดำเนินการโดยวิธีการนี้เป็นการดักเนื้อหาของข้อมูล(Content) ,มิใช่เพียงข้อมูลที่แสดงต้นทางและปลายทางการสื่อสารเท่านั้น

" มาตรา 21 การดักการสื่อสารของเนื้อหาข้อมูล(Interception of content data)

1. รัฐภาคีแต่ละรัฐจะต้องออกกฎหมายหรือมาตรการอื่นเท่าที่จำเป็น ตามระดับของความร้ายแรงของความผิดตามกฎหมายภายใน ที่จะให้อำนาจเจ้าหน้าที่ที่เกี่ยวข้องของตนในการที่จะ

a. เก็บรวบรวมและทำบันทึกผ่านการใช้เครื่องมือทางเทคนิคในดินแดนของรัฐนั้น และ

b. บังคับผู้ให้บริการ ตามความสามารถทางเทคนิคของผู้จัดทำบริการรายนั้น ให้:

i. เก็บรวบรวมหรือทำบันทึกผ่านการใช้เครื่องมือทางเทคนิคในดินแดนของรัฐนั้น หรือ

ii. ให้ความร่วมมือและช่วยเหลือเจ้าหน้าที่ที่เกี่ยวข้องในการเก็บรวบรวมหรือทำบันทึกเกี่ยวกับข้อมูลเนื้อหา (Content data) ในแบบ Real-time จากการสื่อสารใดโดยเจาะจง ในดินแดนของรัฐนั้น ที่ถูกรับส่งโดยเครื่องมือของระบบคอมพิวเตอร์

2. ในกรณีที่รัฐภาคี ไม่สามารถใช้มาตรการที่ถูกกล่าวถึงในวรรค 1 a เนื่องจากระบบกฎหมายภายในของรัฐนั้น รัฐนั้นอาจใช้มาตรการทางนิติบัญญัติหรือทางอื่นเท่าที่จะจำเป็นในการที่จะประกันว่ามีการเก็บรวบรวมหรือการทำบันทึกข้อมูลเนื้อหา(Content data) ในการสื่อสารใดโดยเจาะจงแบบreal-timeในดินแดนของรัฐนั้นผ่านการใช้เครื่องมือทางเทคนิคในดินแดนของรัฐนั้นแทน

3. รัฐภาคีแต่ละรัฐจะต้องออกกฎหมายหรือมาตรการอื่นเท่าที่จำเป็นในการบังคับให้ผู้ให้บริการรักษาความลับเรื่องข้อเท็จจริงในการใช้อำนาจใดที่บัญญัติไว้ในข้อนี้และข้อมูลที่เกี่ยวข้องของการใช้อำนาจ... "

7. การส่งเสริมความร่วมมือระหว่างประเทศ

ความผิดที่กระทำบนอินเทอร์เน็ตอาจเกิดปัญหาในการดำเนินคดีกับผู้กระทำความผิดที่อยู่นอกประเทศ ดังนั้น จึงควรส่งเสริมความประสานงานลักษณะถ้อยทีถ้อยอาศัยกันระหว่างประเทศสมาชิกในการดำเนินคดี โดยอนุสัญญาฉบับนี้กำหนดให้ประเทศสมาชิกจัดต้องศูนย์ความร่วมมือและประสานงานที่ปฏิบัติงานตลอด 24 ชั่วโมงต่อวันและทำงานสัปดาห์ละ 7 วัน หรือที่เรียกว่า "24/7 Network" เพื่อให้ความร่วมมือกันและกันในเรื่องการแนะนำทางด้านเทคนิค ซึ่งกันและกัน จัดเตรียมข้อมูลที่เป็นพยานหลักฐานในคดีให้กับประเทศสมาชิกอื่นที่ขอความช่วยเหลือ ให้ความช่วยเหลือด้านกฎหมายและการระบุสถานที่ (Locating) ที่ผู้กระทำผิดใช้กระทำความผิดให้ความร่วมมือในการติดต่อสื่อสารและประสานงานอย่างไม่ชักช้า จัดฝึกฝนบุคลากรให้มีความรู้ความสามารถและจัดหาเครื่องมือที่ความทันสมัย