3.3 บทวิเคราะห์ : ข้อพิจารณาเกี่ยวกับการใช้มาตรการทางอาญา กรณีผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในต่างประเทศ

การนำมาตรการทางอาญามาใช้กับพฤติกรรมอาชญากรรมในรูปแบบใหม่ซึ่งเพิ่งก่อตัวขึ้นท่ามกลางความเปลี่ยนแปลงในยุคของเทคโนโลยีสารสนเทศ บางกรณีอาจประสบปัญหาอันเนื่องมาจากธรรมชาติของพฤติกรรมการกระทำความผิดในลักษณะเช่นนี้มีความแตกต่างไปจากการกระทำความผิดทั่ว ๆ ไป เมื่อบ่อเกิดหรือบริบทของอาชญากรรมคอมพิวเตอร์มีความผิดแผกแตกต่างไปจากอาชญากรรมแบบดั้งเดิม แนวความคิดและทฤษฎีว่าด้วยการลงโทษผู้กระทำผิดกรณีอาชญากรรมแบบดั้งเดิมในบางประการ จึงมิอาจนำมาอธิบายและปรับใช้กับกรณีการกระทำความผิดของอาชญากรคอมพิวเตอร์ได้อย่างสมบูรณ์ ฉะนั้นเพื่อให้มาตรการบังคับทางอาญาที่จะนำมาใช้กับกรณีผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบมีความเหมาะสมและมีประสิทธิภาพในการควบคุมอาชญากรรมคอมพิวเตอร์ได้ จึงจำเป็นต้องศึกษาทำความเข้าใจถึงข้อพิจารณาบางประการเกี่ยวกับวัตถุประสงค์ในการลงโทษ รวมถึงข้อพิจารณาเกี่ยวกับประสิทธิภาพในการลงโทษผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในต่างประเทศ ทั้งนี้เพื่อเป็นแนวทางในการนำมาปรับใช้กับกระบวนการยุติธรรมทางอาญาของประเทศไทยได้ต่อไป

3.3.1 ข้อพิจารณาในแง่วัตถุประสงค์ในการลงโทษ

(ก) การลงโทษให้ได้สัดส่วนกับความผิด (Proportionality of Punishment)

เป็นหลักการลงโทษตามความยุติธรรม (Just Deserts) กล่าวคือ ความรุนแรงของการลงโทษจะต้องได้สัดส่วนกับความร้ายแรงของการกระทำความผิด ยกตัวอย่างเช่น การกระทำความผิดฝ่าฝืนกฎจราจรมีความร้ายแรงน้อยกว่าการกระทำผิดโดยเจตนาฆ่าผู้อื่น ฉะนั้นผู้กระทำผิดกฎจราจรย่อมได้รับการลงโทษที่มีความรุนแรงน้อยกว่าผู้ที่กระทำผิดโดยเจตนาฆ่าผู้อื่น แต่สำหรับในกรณีอาชญากรรมทางคอมพิวเตอร์บางกรณีอาจประเมินถึงความร้ายแรงของพฤติกรรมการกระทำความผิดได้ยาก เนื่องจากพฤติกรรมเหล่านี้โดยธรรมชาติไม่มีลักษณะของ

ความรุนแรงในทางกายภาพ และอาจไม่มีความสัมพันธ์เกี่ยวข้องกับบุคคลอื่นโดยตรง เช่น การสร้างหรือทำให้แพร่หลายซึ่งไวรัสคอมพิวเตอร์ เป็นต้น[59]

(ข) การประณามการกระทำความผิด (Expressive or Denunciatory Justification)

เป็นการแสดงปฏิกิริยาต่อต้านของคนในสังคมที่มีต่อการกระทำความผิดนั้น สำหรับในคดีอาชญากรรมทางคอมพิวเตอร์นั้นเป็นเรื่องที่อยู่ในความสนใจของสื่อสารมวลชนมาโดยตลอด ผู้กระทำความผิดมักจะกลับกลายเป็นผู้ที่มีชื่อเสียงในเวลาต่อมา รวมทั้งถูกยกย่องในทำนองว่าเป็นพวกอัจฉริยะ เหล่านี้อาจจะนำไปสู่การกระตุ้นให้เยาวชนหรือวัยรุ่นสนใจและมีพฤติกรรมเลียนแบบเพื่อความต้องการมีชื่อเสียงเช่นเดียวกับอาชญากรคอมพิวเตอร์คนนั้น[60]

(ค) การตัดโอกาสกระทำความผิด (Incapacitation)

เป็นการแยกผู้กระทำความผิดออกจากสังคม โดยทั่วไปหมายถึงกรณีจำคุก ทั้งนี้เพื่อป้องกันไม่ให้มีการกระทำความผิดซ้ำ แต่ในกรณีของคดีอาชญากรรมทางคอมพิวเตอร์บางกรณีผู้กระทำผิดสามารถกระทำความผิดซ้ำได้แม้ว่าจะถูกจองจำอยู่ในคุก เนื่องจากในคุกบางแห่งอาจมีบริการคอมพิวเตอร์และอินเทอร์เน็ตแก่ผู้ต้องขัง ปัญหาอีกประการหนึ่ง คือ แม้ว่าผู้กระทำผิดจะไม่กระทำความผิดซ้ำในขณะถูกจองจำอยู่ในเรือนจำ แต่เมื่อเขาถูกปล่อยตัวออกมาแล้ว พวกเขามักจะกระทำความผิดซ้ำในทันทีที่มีโอกาส

ยกตัวอย่างเช่นในคดีของนาย Kevin Mitnick ซึ่งกระทำความผิดซ้ำโดยการเจาะระบบคอมพิวเตอร์หลายแห่งในระหว่างการพักการลงโทษ เขาถูกจับอันเนื่องมาจากการเจาะระบบในช่วงทศวรรษที่ 1980 เป็นจำนวนถึง 4 ครั้ง[61]

---

[59] Russell G. Smith, “CYBER CRIME SENTENCING : The Effectiveness of Criminal Justice Responses,” <http://www.aic.gov.au/conferences/2004/smith.pdf>, 29-30 November 2004.

[60] *Ibid.*

[61] United States v. Mitnick, 145 F. 3d 1342 (9th Cir. 1998), see also Tsutomu Shimomura and John Markoff, วิสามัญฯ แฮกเกอร์ (Take Down), แปลโดย Super U:-), (กรุงเทพมหานคร: สำนักพิมพ์มติชน, 2543), น.292-390.

(ง) การข่มขู่ยับยั้ง (Deterrence)

เป็นการลงโทษเพื่อให้บุคคลตระหนักถึงความเป็นไปได้ที่ตนอาจจะถูกลงโทษอันเนื่องมาจากการกระทำความผิด เมื่อบุคคลทราบดีว่าโอกาสที่ตนจะถูกจับหรือถูกลงโทษมีสูง จะมีการยับยั้งพฤติกรรมในการกระทำความผิดนั้น ๆ แต่สำหรับในคดีอาชญากรรมทางคอมพิวเตอร์จากการสำรวจพบว่า ผู้กระทำความผิดส่วนมากไม่ทราบว่าการกระทำของพวกเขาผิดกฎหมาย และนอกจากนี้ยังพบว่าการตัดสินใจของ ผู้กระทำความผิดต่อไปหรือจะหยุดการกระทำนั้นเสีย แทบจะไม่สัมพันธ์กับความเป็นไปได้ในการถูกลงโทษ กล่าวคือ การถูกลงโทษไม่ได้มีผลในการข่มขู่หรือยับยั้งการกระทำความผิดของอาชญากรคอมพิวเตอร์[62]

ปัญหาในเรื่องการข่มขู่ยับยั้งอีกประการหนึ่ง คือ สภาพความเป็นจริงในสังคมของแฮกเกอร์ที่เชื่อว่า การกระทำของพวกเขาไม่ควรเป็นสิ่งที่ผิดกฎหมาย จากการให้สัมภาษณ์ของแฮกเกอร์และอาชญากรคอมพิวเตอร์ซึ่งถูกลงโทษ พบว่า พวกเขาอ้างว่าการกระทำของพวกเขาไม่ได้มีเจตนามุ่งร้าย แต่มีเพียงแรงจูงใจอันเกิดจากความอยากรู้อยากเห็นเท่านั้น ส่วนคนที่กระทำความผิดโดยละเมิดสิทธิ์ในโปรแกรมคอมพิวเตอร์ (software piracy) อ้างว่าพวกเขาเชื่อว่าเป็นสิทธิอันชอบธรรมของพวกเขาที่จะใช้สิ่งใดก็ตามที่มีอยู่ในเครือข่ายอินเทอร์เน็ตได้อย่างเสรี เหล่านี้แสดงให้เห็นว่าอาชญากรคอมพิวเตอร์ส่วนใหญ่มักจะไม่ยอมรับว่าการกระทำของพวกเขาเป็นความผิด ฉะนั้นจึงไม่มีเหตุผลใดที่จะทำให้พวกเขาต้องยับยั้งพฤติกรรมดังกล่าว แม้ว่าตนจะเคยถูกลงโทษมาแล้ว หรืออาจจะถูกดำเนินคดีในอนาคตก็ตาม แต่อย่างไรก็ตามการพิพากษาลงโทษอาชญากรคอมพิวเตอร์โดยศาล ยังคงเป็นแนวทางข่มขู่ยับยั้งตามวัตถุประสงค์ของการลงโทษ แม้ว่าฝ่ายนิติบัญญัติจะเสนอให้มีการกำหนดโทษขั้นสูงสุดเพิ่มขึ้น ทั้งนี้เพื่อที่จะลดพฤติกรรมอาชญากรรมคอมพิวเตอร์ลง แต่ผลการวิจัยพบว่าแม้จะมีการเพิ่มโทษให้สูงขึ้นก็ไม่ได้ทำให้การกระทำความผิดของแฮกเกอร์นั้นลดลง[63]

(จ) การชดใช้ (Restitution)

มีวัตถุประสงค์เพื่อชดเชยค่าเสียหายให้แก่เหยื่ออันเนื่องมาจากการกระทำความผิดของผู้กระทำผิด ปัญหาในการชดใช้ค่าเสียหายให้แก่เหยื่อ คือ ผู้กระทำความผิดในบางกรณีโดยเฉพาะอย่างยิ่งในกรณีผู้กระทำผิดซึ่งเป็นเยาวชน ไม่อยู่ในสถานะที่จะสามารถชดใช้ค่าเสียหายให้

---

[62] Russell G. Smith, *supra note* 53.

[63] Russell G. Smith, Peter Grabosky and Gregor Urbas, *supra note* 2, p.113.

แก่เหยื่อได้ ปัญหาอีกประการหนึ่ง คือ ศาลอาญา รวมทั้งหน่วยงานด้านกระบวนการยุติธรรมทางอาญาที่เกี่ยวข้องยังไม่มีความเชี่ยวชาญในการคำนวณความเสียหายทางการเงินที่เกิดขึ้นจากคดีอาชญากรรมคอมพิวเตอร์[64] ซึ่งต่างจากศาลแพ่งที่มีความเชี่ยวชาญทางด้านนี้มากกว่า ตัวอย่างคดีที่ศาลตัดสินให้ผู้กระทำผิดชดใช้ค่าเสียหายเป็นจำนวนมากให้แก่เหยื่อ เช่น คดีของ Osowski & Tang[65] ถูกศาลตัดสินจำคุก 34 เดือน และชดใช้ค่าเสียหายให้แก่เหยื่อเป็นจำนวนถึง 7.9 ล้านเหรียญสหรัฐ

3.3.2 ข้อพิจารณาในแง่ประสิทธิภาพในการลงโทษ

(ก) การริบทรัพย์สิน เช่น เครื่องคอมพิวเตอร์และโมเด็มของผู้กระทำความผิดไม่อาจหยุดพฤติกรรมการกระทำความผิดโดยใช้คอมพิวเตอร์ได้อย่างแท้จริง เนื่องจากปัจจุบันนี้มีบริการคอมพิวเตอร์และอินเทอร์เน็ตอย่างแพร่หลาย ทั้งในห้องสมุดและร้านอินเทอร์เน็ตคาเฟ่ ดังนั้นผู้กระทำผิดอาจหาช่องทางอื่นในการกระทำความผิดลักษณะนี้ได้โดยง่าย การริบทรัพย์สินดังกล่าวจึงไม่สามารถตัดโอกาสในการกระทำความผิดของจำเลยได้

(ข) การริบอุปกรณ์คอมพิวเตอร์ของผู้กระทำผิด อาจจะส่งผลกระทบต่อบุคคลอื่นมากกว่าตัวผู้กระทำผิดได้ ตัวอย่างเช่น หากอุปกรณ์คอมพิวเตอร์นั้นเป็นเครื่องคอมพิวเตอร์ประจำบ้าน ซึ่งสมาชิกในบ้านคนอื่นๆ ใช้สำหรับทำงานต่างๆ ด้วย การริบอุปกรณ์คอมพิวเตอร์ดังกล่าวย่อมเป็นการขัดต่อหลักการลงโทษให้ได้สัดส่วนกับความผิด เพราะเท่ากับเป็นการลิดรอนสิทธิของบุคคลอื่นที่ไม่ใช่ผู้กระทำผิด ซึ่งถือได้ว่าเป็นการลงโทษที่รุนแรงมากเกินกว่าความร้ายแรงของความผิด

---

[64] Russell G. Smith, *supra note* 53; see also Jenifer S. Granick, “Faking It: Calculating Loss in Computer Crime Sentencing,” <http://infosecon.net/workshop/pdf/FakingIt.granick.pdf>.

[65] Former Cisco Systems, Inc. Accountants Sentenced for Unauthorized Access to Computer Systems to Illegally Issue Almost $8 Million in Cisco Stock to Themselves, < http://www.usdoj.gov/criminal/cybercrime/Osowski_TangSent.htm >, 26 November 2001.

(ค) คำสั่งจำกัดการใช้งานคอมพิวเตอร์และอินเทอร์เน็ตจำเป็นต้องมีเจ้าหน้าที่ที่มีศักยภาพในการควบคุมสอดส่องพฤติกรรมของจำเลย ตัวอย่างเช่น พนักงานคุมประพฤติอาจจะต้องผ่านการฝึกฝนอบรมในด้านนิติวิทยาศาสตร์ทางคอมพิวเตอร์ (computer forensic) เพื่อที่จะสามารถสืบเสาะและสอดส่องพฤติกรรมในการใช้งานคอมพิวเตอร์ของผู้กระทำผิดได้ แต่ในสภาพความเป็นจริงงานในลักษณะเช่นนี้อาจจะไม่เหมาะสมกับงานคุมประพฤติ ประกอบกับผู้กระทำผิดเป็นบุคคลที่มีความรู้ความเชี่ยวชาญในด้านคอมพิวเตอร์เป็นพิเศษจึงสามารถที่จะหลบหลีกหรือปกปิดการกระทำอันฝ่าฝืนคำสั่งของศาลได้โดยง่าย

(ง) กรณีการนำเอาโปรแกรมคอมพิวเตอร์มาใช้ในการควบคุมสอดส่องพฤติกรรมของผู้ถูกคุมความประพฤติยังคงมีจุดอ่อนในกรณีที่ผู้ถูกคุมความประพฤติเป็นผู้ที่มีความรู้ทางเทคนิคในด้านคอมพิวเตอร์ ผู้ถูกคุมความประพฤติดังกล่าวจึงสามารถหลบเลี่ยงหรือฝ่าฝืนการทำงานของโปรแกรมคอมพิวเตอร์ดังกล่าวได้ ยกตัวอย่างเช่น การใช้วิทยาการการเข้ารหัสข้อมูล (encryption) หรือใช้วิทยาการอำพรางข้อมูล (steganography) ในการหลบเลี่ยงการตรวจสอบจากโปรแกรมทางด้านนิติวิทยาศาสตร์ (forensic software) หรืออาจใช้วิธีการเปลี่ยนไปใช้ระบบปฏิบัติการอื่นในการหลบเลี่ยงการตรวจสอบจากโปรแกรมควบคุมสอดส่อง (monitoring software) หรืออาจใช้เทคนิคอื่นใดในการฝ่าฝืนเข้าถึงเว็บไซต์ต้องห้ามไว้โดยโปรแกรมกลั่นกรองเว็บไซต์ ฉะนั้นเพื่อให้การควบคุมสอดส่องพฤติกรรมของผู้ถูกคุมความประพฤติมีประสิทธิภาพศาลควรจะพิจารณาถึงความรู้ความสามารถ ทักษะและประสบการณ์ในการควบคุมสอดส่องโดยใช้โปรแกรมคอมพิวเตอร์ดังกล่าวของพนักงานคุมประพฤติควบคู่ไปกับระดับความรู้ทักษะในด้านคอมพิวเตอร์ของผู้ถูกคุมความประพฤติ[66] นอกจากนี้การนำเทคโนโลยีโปรแกรมคอมพิวเตอร์มาใช้ในการควบคุมสอดส่องพฤติกรรมของผู้ถูกคุมความประพฤติ ไม่ว่าจะเป็นโปรแกรมด้านนิติวิทยาศาสตร์ หรือโปรแกรมด้านควบคุมสอดส่อง ยังคงมีปัญหาในทางปฏิบัติเนื่องจากเทคโนโลยีดังกล่าวอาจถูกใช้ในลักษณะก้าวล่วงสิทธิส่วนบุคคลของผู้ถูกคุมความประพฤติจนเกินขอบเขตของการคุมความประพฤติได้[67]

---

[66] Lanny L. Newvill, “Cyber Crime and the Courts – Investigating and Supervising the Information Age Offender,” Federal Probation 65, 2(September 2001): p.13, available at <http://www.uscourts.gov/fedprob/2001septfp.pdf>

[67] United States v. Lifshitz, 369 F.3d 173, 193 (2d Cir. 2004); see also Shauna Curphey, *supra note* 28.

(จ) ในกรณีที่ผู้กระทำความผิดเป็นผู้ประกอบอาชีพในด้านคอมพิวเตอร์หรือเทคโนโลยีสารสนเทศ การริบอุปกรณ์คอมพิวเตอร์และคำสั่งศาลที่จำกัดการใช้งานหรือเข้าถึงคอมพิวเตอร์และอินเทอร์เน็ตนั้นอาจจะก่อให้เกิดปัญหาในแง่การแก้ไขฟื้นฟูผู้กระทำผิด เพราะการสั่งห้ามดังกล่าวอาจจะส่งผลให้ผู้กระทำความผิดต้องตกงาน ไม่มีรายได้ในระหว่างการคุมประพฤติหรือการพักการลงโทษ และอาจไม่มีเงินเพียงพอในการจ่ายค่าเสียหายให้แก่เหยื่อในกรณีที่ศาลมีคำพิพากษาให้ชดใช้ค่าเสียหาย นอกจากนี้อาจจะส่งผลกระทบโดยอ้อมต่อผู้กระทำความผิดในด้านการใช้บริการทางสังคมบางกรณีที่มีความจำเป็นต้องอาศัยการใช้งานคอมพิวเตอร์หรืออินเทอร์เน็ตร่วมด้วย เช่น การทำธุรกรรมทางอิเล็กทรอนิกส์ หรือเสียภาษีผ่านทางอินเทอร์เน็ต เป็นต้น

โดยสรุป มาตรการทางอาญากรณีการกระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในต่างประเทศ บางมาตรการไม่มีความจำเป็นที่จะนำมาใช้กับผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ เช่น มาตรการริบทรัพย์สินประเภทเครื่องคอมพิวเตอร์และโมเด็มของผู้กระทำผิด เนื่องจากมาตรการดังกล่าวมีวัตถุประสงค์ในการลงโทษเพื่อตัดโอกาสในการกระทำผิดซ้ำ แต่สำหรับกรณีการกระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบนั้น ผู้กระทำผิดยังคงสามารถอาศัยเครื่องมือดังกล่าวจากแหล่งที่มาอื่นในการกระทำผิดซ้ำได้โดยง่าย ฉะนั้นมาตรการริบทรัพย์สินจึงไม่จำเป็นที่จะนำมาใช้กับกรณีนี้ ส่วนมาตรการอื่น ๆ แม้ว่าจะมีความจำเป็นที่จะนำมาใช้กับกรณีการกระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ แต่อย่างไรก็ตาม การนำมาใช้กับกรณีเช่นนี้ จะต้องพิจารณาถึงแนวทางปฏิบัติและความเหมาะสมในแต่ละกรณีควบคู่กันไปด้วย ยกตัวอย่างเช่น การนำมาตรการทางเทคโนโลยีมาใช้ในการควบคุมสอดส่องพฤติกรรมของผู้กระทำผิดในระหว่างคุมประพฤติหรือพักการลงโทษ ศาลจะต้องพิจารณาถึงความรู้ความสามารถ ทักษะและประสบการณ์ในการควบคุมสอดส่องโดยใช้เทคโนโลยีดังกล่าวของพนักงานคุมประพฤติควบคู่ไปกับระดับความรู้ ทักษะในด้านคอมพิวเตอร์ของผู้ถูกคุมความประพฤติ ทั้งนี้เพื่อให้การนำเอามาตรการดังกล่าวมาใช้กับผู้กระทำผิดเกิดประสิทธิภาพสูงสุด