บทที่ 4

มาตรการทางอาญาที่จำเป็นแก่ผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในประเทศไทย

จากการศึกษารูปแบบพฤติกรรมการกระทำความผิดของอาชญากรคอมพิวเตอร์ในปัจจุบันทำให้เห็นว่า อาชญากรรมทางคอมพิวเตอร์มิได้เป็นแต่เพียงการก่อกวน หรือสร้างความเดือนร้อนรำคาญให้แก่ผู้ใช้งานคอมพิวเตอร์เท่านั้น แต่ยังเป็นมิติใหม่ของอาชญากรรมในยุคเทคโนโลยีสารสนเทศที่อาชญากรไฮเทคอาศัยความรู้ความเชี่ยวชาญในการแสวงหาผลประโยชน์ให้แก่ตนเองหรือองค์กรของตน เมื่อผลตอบแทนที่ได้รับคุ้มค่าแก่การเสี่ยงต่อการถูกดำเนินคดี ประกอบกับธรรมชาติของอาชญากรรมรูปแบบใหม่นี้มีความยากในการติดตามสืบสวนหาตัวผู้กระทำความผิดมาลงโทษ จึงส่งผลให้อัตราการเกิดอาชญากรรมในลักษณะนี้เพิ่มขึ้นและขยายวงกว้างยิ่งขึ้นเรื่อย ๆ ตามแนวโน้มการเติบโตของเทคโนโลยีใหม่ ๆ

ประเด็นในเรื่องความเหมาะสมในการลงโทษผู้กระทำความผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบเป็นปัญหาที่ท้าทายประการหนึ่งในการควบคุมอาชญากรรมทางคอมพิวเตอร์ กล่าวคือ จะนำมาตรการลงโทษหรือมาตรการบังคับทางอาญารูปแบบใดมาใช้กับกรณีการกระทำความผิดของอาชญากรคอมพิวเตอร์จึงจะเหมาะสม สอดคล้องกับวัตถุประสงค์ในการลงโทษทั้งในทางข่มขู่ผู้กระทำผิดคนอื่นให้เกิดความรู้สึกเกรงกลัวไม่กล้าที่จะกระทำความผิดในลักษณะเช่นนั้นและยับยั้งผู้กระทำผิดมิให้กลับไปกระทำความผิดเช่นนั้นซ้ำอีกหลังจากพ้นโทษไปแล้ว รวมทั้งจะต้องหามาตรการในการแก้ไขฟื้นฟูผู้กระทำผิดให้กลับตัวกลับใจเป็นพลเมืองดีของสังคมนั้นต่อไป ทั้งนี้เนื่องจากรูปแบบของอาชญากรรมทางคอมพิวเตอร์ซึ่งเกิดจากการกระทำของอาชญากรคอมพิวเตอร์เป็นมิติใหม่ของอาชญากรรมที่เกิดขึ้นในสังคมพร้อม ๆ กับการพัฒนาของเทคโนโลยีสารสนเทศ โดยสภาพหรือโดยธรรมชาติของการประกอบอาชญากรรมในลักษณะนี้แตกต่างไปจากอาชญากรรมพื้นฐานทั่ว ๆ ไปและผู้กระทำผิดยังเป็นบุคคลที่มีความรู้ความเชี่ยวชาญและมีศักยภาพในด้านเทคโนโลยีสูง ด้วยเหตุนี้ข้อพิจารณาในเรื่องมาตรการบังคับทางอาญาสำหรับกรณีการกระทำความผิดของอาชญากรคอมพิวเตอร์จึงต้องมีการพิจารณาอย่างละเอียดถี่ถ้วนและมีมาตรการพิเศษที่จะนำมาใช้กับกรณีนี้โดยเฉพาะ

ในเบื้องต้น ประเด็นเรื่องความเหมาะสมของมาตรการบังคับทางอาญาที่จะนำมาปรับใช้กับกรณีผู้กระทำความผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบนั้น โดยหลักการที่จะพิจารณาว่า

มาตรการในรูปแบบใดมีความเหมาะสมหรือไม่เหมาะสมจะต้องพิจารณาจาก 2 ปัจจัย คือ ความเหมาะสมกับสภาพตัวผู้กระทำผิดและความเหมาะสมกับลักษณะการกระทำความผิด

(ก) <u>ความเหมาะสมกับสภาพตัวผู้กระทำผิด</u>

ปัจจัยเกี่ยวกับตัวผู้กระทำผิด ศาลจะต้องพิเคราะห์ถึงคุณลักษณะเฉพาะของผู้กระทำผิดแต่ละคนว่าจัดอยู่ในกลุ่มใด ประเภทใด ทั้งนี้เนื่องจากคุณลักษณะเฉพาะของผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในแต่ละกลุ่ม แต่ละประเภทจะสะท้อนให้เห็นถึงที่มาและแรงจูงใจในการกระทำความผิดได้ ดังต่อไปนี้

หากเป็นผู้กระทำผิดในกลุ่มมือใหม่ หรือ Script-Kiddies ซึ่งส่วนมากมักจะเป็นเด็กเยาวชนหรือนักศึกษาที่ต้องการเพียงทดสอบความสามารถของตนเองเป็นหลัก ผู้กระทำผิดในลักษณะเช่นนี้จึงไม่ต่างไปจากการกระทำความผิดของเด็กและเยาวชนในรูปแบบอื่น ๆ ซึ่งผู้กระทำผิดก้าวสู่วงจรอาชญากรรมด้วยความอ่อนด้อยในด้านวุฒิภาวะ ขาดความรู้สึกรับผิดชอบต่อสังคม และในบางครั้งกระทำผิดเพียงเพื่อความสนุก ความท้าทายและความอยากรู้อยากเห็นอยากลองในสิ่งต่าง ๆ โดยมิได้คำนึงความเสียหายหรือผลที่ตามมาจากการกระทำนั้น ๆ ของตน การนำเอามาตรการทางอาญามาใช้กับผู้กระทำผิดในประเภทนี้ควรใช้รูปแบบของการแก้ไขฟื้นฟูพฤติกรรมของผู้กระทำผิดเป็นสำคัญ ทั้งนี้เพื่อให้ผู้กระทำผิดในกลุ่มนี้ได้ปรับเปลี่ยนทัศนคติที่มีต่อการกระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ และปรับปรุงพฤติกรรมของตน กลับตัวเป็นคนดีของสังคมได้ต่อไป รูปแบบของมาตรการที่ศาลควรนำมาใช้กับผู้กระทำผิดกลุ่มนี้ คือ การคุมความประพฤติโดยกำหนดเงื่อนไขควบคุมเกี่ยวกับการใช้งานคอมพิวเตอร์เป็นหลัก ทั้งนี้ผู้เขียนเห็นว่าศาลอาจนำเอามาตรการทำงานบริการสังคมมาใช้กับผู้กระทำผิดประเภทนี้ได้ โดยการกำหนดให้ผู้กระทำผิดซึ่งมีความสนใจในด้านคอมพิวเตอร์และมีความสามารถในด้านนี้เป็นทุนเดิม ได้นำเอาความรู้ที่ตนมีมาใช้ในแนวทางที่ถูกต้องเหมาะสม เช่น กำหนดให้ความช่วยเหลือเจ้าหน้าที่หรือหน่วยงานราชการเกี่ยวกับงานด้านคอมพิวเตอร์ หรือบำเพ็ญประโยชน์โดยการให้ความรู้เกี่ยวกับเทคโนโลยีสารสนเทศ อาชญากรรมคอมพิวเตอร์ให้แก่ชุมชน เป็นต้น ลักษณะงานที่นำเอาศักยภาพของผู้กระทำผิดมาใช้ในทิศทางที่ถูกต้องเหมาะสมนี้ นอกจากจะทำให้ผู้กระทำผิดสามารถปรับเปลี่ยน แก้ไขพฤติกรรมที่ไม่ดีและมีความรับผิดชอบต่อสังคมมากขึ้นแล้ว ยังทำให้ผู้กระทำผิดเกิดความรู้สึกภาคภูมิใจในการนำความสามารถของตนมาใช้เพื่อเป็นประโยชน์ต่อสังคมหรือชุมชนได้อีกทางหนึ่ง

ผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบอีกประเภทหนึ่ง เป็นกลุ่มที่กระทำผิดโดยมีเจตนาบริสุทธิ์ กล่าวคือ มีเจตนาเข้าถึงข้อมูลของผู้อื่นเพื่อต้องการที่จะทดสอบระบบความปลอดภัยทางคอมพิวเตอร์ของเหยื่อ ซึ่งหากพบว่าระบบดังกล่าวมีช่องโหว่ หรือข้อบกพร่องประการใด จะแจ้งไปยังผู้ดูแลระบบความปลอดภัยซึ่งรับผิดชอบ เพื่อทำการแก้ไขปรับปรุงระบบนั้น ๆ ต่อไป ทั้งนี้โดยทั่วไปแล้วผู้กระทำผิดในลักษณะเช่นนี้มักจะไม่มีเจตนาในการสร้างความเสียหายให้แก่ระบบหรือข้อมูลคอมพิวเตอร์ของเหยื่อ และไม่มีแรงจูงใจเกี่ยวกับผลประโยชน์ทางการเงินเข้ามาเกี่ยวข้องในการกระทำผิดดังกล่าว ดังนี้เมื่อศาลได้พิเคราะห์จากข้อมูลประวัติภูมิหลังของผู้กระทำผิดในลักษณะเช่นนี้แล้ว หากปรากฏว่าผู้กระทำผิดไม่เคยเข้าไปมีส่วนเกี่ยวข้องกับการกระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในลักษณะที่มีแรงจูงใจอันเกี่ยวกับผลประโยชน์ทางการเงินเข้ามาเกี่ยวข้องร่วมด้วยแล้ว ศาลควรลงโทษผู้กระทำผิดในลักษณะนี้โดยนำมาตรการแก้ไขฟื้นฟูผู้กระทำผิดมาใช้ ยกตัวอย่างเช่น การคุมความประพฤติเกี่ยวกับการใช้งานหรือเข้าถึงคอมพิวเตอร์ หรือกำหนดให้ทำงานบริการสังคมโดยนำเอาความสามารถทางด้านคอมพิวเตอร์ของผู้กระทำผิดมาใช้ในการบำเพ็ญประโยชน์แก่สังคม เป็นต้น

ผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบอีกรูปแบบหนึ่ง เป็นผู้กระทำผิดที่มีแรงจูงใจในการกระทำความผิดมาจากความโกรธแค้นส่วนตัวและต้องการที่จะแก้แค้นเหยื่อ ส่วนมากมักจะเป็นคนในองค์กรที่ไม่พอใจผู้บริหาร เช่น ถูกนายจ้างต่อว่า หรือลดเงินเดือน เป็นต้น หรืออาจจะเป็นอดีตลูกจ้างขององค์กรซึ่งถูกไล่ออกจากงานไปแล้ว (disgruntled former employee) โดยเฉพาะอย่างยิ่งหากอดีตลูกจ้างคนนั้นทำหน้าที่ดูแลเกี่ยวกับระบบคอมพิวเตอร์ขององค์กร เมื่อถูกไล่ออกจากงานอาจจะใช้ความรู้ความสามารถของตน รวมทั้งสถานะของผู้ดูแลระบบ (supervisor) เข้าไปทำลายหรือแก้ไขเปลี่ยนแปลงระบบการทำงานของคอมพิวเตอร์ในองค์กรนั้น ๆ ได้[1] แต่อย่างไรก็ตามผู้กระทำผิดในกลุ่มนี้บางกรณีอาจมีลักษณะของพฤติกรรมการกระทำ

---

[1] โปรดดูตัวอย่างคดี U.S. v. Fisher (D. Utah), < http://www.usdoj.gov/criminal/cybercrime/fisherIndict.htm>, February 15, 2006; U.S. v. Benimeli (N.D. Ohio), < http://www.usdoj.gov/criminal/cybercrime/benimeliSent.htm>, 13 July 2006; U.S. v. Meydbray (N.D. Cal.), < http://www.usdoj.gov/criminal/cybercrime/meydbrayPlea.htm>, 8 June 2005; U.S. v. Cotton(S.D. N.Y.), < http://www.usdoj.gov/criminal/cybercrime/cottonPlea.htm>,9 September 2004; U.S. v. Angle (D. Mass.), < http://www.usdoj.gov/ criminal/cybercrime/angleCharged.htm>, 23 August 2004; U.S. v. Garcia (C.D. Cal.), < http://

ความผิดที่มีความเกี่ยวข้องกับผลประโยชน์ในทางการเงินร่วมอยู่ด้วย[2] ข้อพิจารณาในเบื้องต้นเกี่ยวกับผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในลักษณะนี้ เนื่องจากผู้กระทำผิดอาศัยอำนาจหน้าที่ของตนเป็นประโยชน์ในการกระทำผิดต่อนายจ้าง หรือหน่วยงานที่ตนทำงานหรือเคยทำงาน การกระทำเช่นนี้ย่อมเป็นการฝ่าฝืนต่ออำนาจหน้าที่ หรือเป็นการอาศัยอำนาจหน้าที่ที่เคยมีมาใช้ในการกระทำผิด (ในกรณีอดีตลูกจ้าง) การกระทำผิดในลักษณะเช่นนี้ศาลสมควรนำเอามาตรการด้านข่มขู่ยับยั้ง เช่น โทษจำคุกหรือปรับ มาใช้กับผู้กระทำผิด เพื่อให้ผู้กระทำผิดเกิดความรู้สึกเกรงกลัวและเข็ดหลาบไม่กลับไปกระทำผิดซ้ำอีก นอกจากนี้ควรมีมาตรการควบคุมในการประกอบอาชีพด้านเทคโนโลยีสารสนเทศของผู้กระทำผิดในลักษณะเช่นนี้ภายหลังจากที่ผู้กระทำผิดได้รับโทษแล้ว เช่น การขึ้นทะเบียนผู้กระทำผิดเกี่ยวกับคอมพิวเตอร์ รวมถึงประวัติการกระทำผิดเกี่ยวกับคอมพิวเตอร์ที่มีต่อนายจ้าง ทั้งนี้เพื่อเป็นข้อมูลให้แก่หน่วยงานที่จะรับพิจารณาผู้กระทำผิดเป็นพนักงานใหม่ เป็นต้น

ผู้กระทำผิดประเภทสุดท้าย เป็นผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบที่มีแรงจูงใจหลักในการกระทำผิดมาจากผลประโยชน์ทางการเงิน ผู้กระทำผิดในกลุ่มนี้จัดอยู่ในกลุ่มที่มีพฤติกรรมการกระทำผิดที่มีความโน้มเอียงไปทางอาชญากรมากที่สุด กล่าวคือ ผู้กระทำผิดที่มีแรงจูงใจในการกระทำความผิดอันเนื่องมาจากผลประโยชน์ในทางการเงิน (monetary gains) นี้

---

www.usdoj.gov/criminal/cybercrime/garciaSent.htm>, 23 February 2004; U.S. v.Patterson (W.D. Pa.), <http://www.usdoj.gov/criminal/cybercrime/pattersonSent .htm>, 2 December 2003; U.S. v. Castillo (W.D. Tex.), < http://www.usdoj.gov/criminal/ cybercrime/castilloArrest.htm>, 17 July 2003; U.S. v. Tran(C.D. Cal), < http://www.usdoj. gov/ criminal/cybercrime/tranPlea.htm>, 18 April 2003; U.S. v. Duronio (D. N.J.), < http:// www.usdoj.gov/criminal/cybercrime/duronioIndict.htm>, 17 December 2002, U.S. v. Lloyd (D. NJ), < http://www.usdoj.gov/criminal/cybercrime/lloydSent.htm>, 26 February 2002.

[2] โปรดดูตัวอย่างคดี U.S. v. Dopps (C.D. Cal.), <http://www.usdoj.gov/ criminal/cybercrime/doppsPlea.htm>, 9 September 2002; U.S. v. Turner (N.D. Ohio), <http://www.usdoj.gov/criminal/cybercrime/williams_turnerSent.htm>, 19 February 2002.

อาจจัดอยู่ในกลุ่มของแฮกเกอร์ที่มีเจตนาชั่วร้าย (malevolent hacker)[3] ซึ่งกระทำความผิดทางคอมพิวเตอร์เพื่อหวังผลตอบแทน หรือผลประโยชน์ที่จะได้รับจากการกระทำดังกล่าว ซึ่งอาจจะปรากฏอยู่ในรูปแบบของแฮกเกอร์รับจ้าง (hired hacker) โดยจะรับทำงานให้กับผู้ว่าจ้างตามรูปแบบที่ผู้ว่าจ้างต้องการ ตัวอย่างเช่น เจาะระบบคอมพิวเตอร์ของบริษัทที่เป็นคู่แข่งทางการค้าของผู้ว่าจ้างเพื่อลักลอบเอาข้อมูลที่ผู้ว่าจ้างต้องการ หรือเข้าไป แก้ไขเปลี่ยนแปลง หรือทำลายข้อมูลหรือระบบคอมพิวเตอร์ของฝ่ายตรงข้ามเพื่อทำให้ได้รับความเสียหาย เป็นต้น[4] บางกรณีแฮกเกอร์ที่มีเจตนาร้ายอาจกระทำการด้วยตัวเองโดยไม่มีผู้ว่าจ้าง กล่าวคือ เมื่อเจาะระบบคอมพิวเตอร์ของเหยื่อได้แล้ว จะคัดลอกข้อมูลซึ่งเป็นความลับ หรือเป็นข้อมูลที่สำคัญขององค์กรนั้น ๆ เพื่อนำมาข่มขู่เหยื่อให้นำเงินมาไถ่ถอนมิฉะนั้นจะนำข้อมูลดังกล่าวไปเปิดเผยหรือนำไปให้กับองค์กรธุรกิจซึ่งเป็นคู่แข่งทางการค้า โดยเรียกพฤติกรรมของแฮกเกอร์ในลักษณะเช่นนี้ว่า “ransom-ware”[5] ในปัจจุบันผู้กระทำผิดในกลุ่มนี้อาจมีการพัฒนาไปสู่ความร่วมมือในระดับเครือข่ายองค์กรอาชญากรรมและขบวนการก่อการร้าย โดยจะนำมาซึ่งภัยอันร้ายแรงต่อสังคม ฉะนั้นการนำมาตรการทางอาญามาใช้กับผู้กระทำผิดในกลุ่มนี้ ศาลสมควรใช้รูปแบบของมาตรการเพื่อข่มขู่ยับยั้งพฤติกรรมของผู้กระทำผิด เช่น โทษจำคุกหรือปรับ เพื่อให้ผู้กระทำผิดเกิดความเกรงกลัว เข็ดหลาบและไม่กลับไปกระทำผิดซ้ำอีก

---

[3] John Blyler, “Balance Hacker Crime and Punishment,” <http://www.wsdmag.com/Articles/ArticleID/7063/7063.html>, November/ December 2003.

[4] David Icove, Karl Seger and William VonStorch, Computer Crime : A Crimefighter’s Handbook, (United States of America : O’Reilly & Associates, 1995), pp.63; see also “McAfee Virtual Criminology Report : North American Study into Organized Crime and the Internet,” <http://www.mcafee.com/us/local_content/misc/mcafee_na_virtual_criminology_report.pdf>, July 2005.

[5] “ระวังแรนซอมแวร์เรียกค่าไถ่ไฟล์ 200 เหรียญฯ,” <http://www.arip.co.th/news.php?id=404143>, 25 พฤษภาคม 2548.

(ข) ความเหมาะสมกับลักษณะการกระทำความผิด

การกำหนดโทษให้มีความเหมาะสมนอกเหนือจากการพิจารณาจากสภาพตัวผู้กระทำผิดแล้ว ยังต้องพิจารณาถึงความเหมาะสมกับลักษณะของการกระทำความผิดนั้น ๆ ด้วย กล่าวคือ โดยหลักการทั่วไปการกระทำความผิดที่ส่งผลกระทบอันเป็นภัยต่อสังคมร้ายแรง ผู้กระทำผิดดังกล่าวย่อมจะต้องได้รับโทษที่รุนแรงกว่าผู้ที่กระทำความผิดอันเล็กน้อย ฉะนั้นความเหมาะสมในแง่ของลักษณะการกระทำความผิดจึงพิจารณาจากความรุนแรงแห่งคดีเป็นสำคัญ สำหรับกรณีการกระทำความผิดเกี่ยวกับคอมพิวเตอร์นั้นลักษณะความรุนแรงแห่งคดีอาจจะพิจารณาได้จากหลายๆ ปัจจัย ยกตัวอย่างเช่น เป้าหมายหรือเหยื่อของการกระทำความผิด ความสูญเสียทางการเงิน (Financial Loss) และผลกระทบที่เกิดขึ้นจากการกระทำความผิด (Effects on Victims) เป็นต้น[6]

เป้าหมายหรือเหยื่อของการกระทำความผิดเป็นปัจจัยหนึ่งที่นำมาใช้ในการพิจารณาความรุนแรงของอาชญากรรมได้ ยกตัวอย่างในกรณีของอาชญากรรมทั่ว ๆ ไป เช่น การฆ่าผู้อื่นย่อมมีความรุนแรงน้อยกว่าการฆ่าบุพการีหรือการฆ่าเจ้าพนักงานของรัฐ การลักทรัพย์ทั่ว ๆ ไปย่อมมีความรุนแรงที่น้อยกว่าการลักทรัพย์สินของทางราชการที่ใช้หรือมีไว้เพื่อสาธารณประโยชน์เป็นต้น ในกรณีการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ก็เช่นเดียวกัน เมื่อเป้าหมายหรือเหยื่อของการกระทำความผิดเป็นหน่วยงานของรัฐ ซึ่งอาจจะเป็นระบบคอมพิวเตอร์ของหน่วยงานใดหน่วยงานหนึ่งของรัฐ ระบบฐานข้อมูลของทางราชการ ข้อมูลคอมพิวเตอร์หรือแม้กระทั่งเว็บไซต์ของหน่วยงานรัฐ การกระทำความผิดในลักษณะเช่นนี้ย่อมมีความรุนแรงแห่งคดีมากกว่าการกระทำต่อระบบคอมพิวเตอร์ของเอกชนทั่ว ๆ ไป

ส่วนข้อพิจารณาเรื่องความสูญเสียทางการเงินและผลกระทบที่เกิดจากการกระทำความผิดเป็นอีกปัจจัยหนึ่งในการพิจารณาความรุนแรงแห่งคดี โดยมองจากผลลัพธ์ที่เกิดขึ้นจากการกระทำความผิดเป็นสำคัญ สำหรับการกระทำความผิดของอาชญากรคอมพิวเตอร์ โดยสภาพของอาชญากรรมทางคอมพิวเตอร์ การกระทำความผิดเพียงกรรมเดียว เช่น การทำให้แพร่หลายซึ่งไวรัสคอมพิวเตอร์ อาจจะก่อให้เกิดความสูญเสียในทางการเงินเป็นจำนวนมหาศาล รวมถึงอาจส่งผลกระทบเป็นวงกว้างโดยการแพร่กระจายของไวรัสคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์ในเครือข่ายอินเทอร์เน็ตอีกหลายล้านเครื่องทั่วทุกมุมโลกได้ภายในเวลาเพียงไม่กี่นาทีเท่านั้น

---

[6] Russell G. Smith, Peter Grabosky and Gregor Urbas, CYBER CRIMINALS ON TRIAL, (Australia: Ligare Pty Lid, 2004), pp.124-149.

ยกตัวอย่างเช่นในกรณีผลกระทบที่เกิดจากไวรัสคอมพิวเตอร์ ชื่อ “I Love You” จากการประเมินความเสียหายที่เกิดขึ้นจากทั่วโลกมีมูลค่าประมาณ 6.7-15.3 พันล้านเหรียญสหรัฐ[7]

จากการศึกษาถึงพฤติกรรมการกระทำผิดของผู้กระทำผิดเกี่ยวกับคอมพิวเตอร์ในปัจจุบัน ผู้เขียนเห็นว่า โดยหลักการทั่วไป กลุ่มของผู้กระทำผิดที่มีแรงจูงใจทางการเงินเป็นกลุ่มที่สมควรได้รับการลงโทษอย่างเข้มงวดมากกว่ากลุ่มที่มีแรงจูงใจอื่น เนื่องจากเป็นกลุ่มที่มีพฤติกรรมอาชญากรที่เด่นชัดที่สุด ในบางกรณียังมีการทำงานเป็นกลุ่ม ประสานกันเป็นเครือข่ายอย่างมีระบบ หรือมีความเกี่ยวข้องกับองค์กรอาชญากรรมในรูปแบบอื่น ๆ ด้วย ทั้งยังสามารถสร้างความเสียหายให้เกิดขึ้นในสังคมได้อย่างที่มิอาจคาดคิดได้ แนวทางการลงโทษที่เหมาะสมจึงควรเน้นในเรื่องการข่มขู่ยับยั้งให้ผู้กระทำผิดรู้สึกเข็ดหลาบและเกรงกลัวต่อกฎหมาย รูปแบบที่อาจนำมาใช้ เช่น การจำคุก ปรับและริบทรัพย์สิน เป็นต้น ส่วนผู้กระทำผิดในกลุ่มที่มิได้มีแรงจูงใจทางการเงิน ซึ่งส่วนใหญ่มักจะเป็นเพียงเยาวชนหรือวัยรุ่นที่หลงผิด หรือมีทัศนคติที่ผิดๆ มาตรการที่จะนำมาใช้จึงควรมุ่งเน้นในทางแก้ไขฟื้นฟูผู้กระทำผิดเป็นหลัก เพื่อให้ผู้กระทำผิดรู้สึกสำนึกผิด พร้อมทั้งปรับทัศนคติให้ถูกต้องสอดคล้องกับปทัสถานของสังคมและสามารถกลับตัวกลับใจเป็นพลเมืองที่ดีของสังคมต่อไป รูปแบบของมาตรการที่อาจนำมาใช้ เช่น การคุมประพฤติ การให้ทำงานบริการสังคม เป็นต้น อย่างไรก็ตาม ข้อเสนอดังกล่าวเป็นเพียงแนวทางอย่างกว้างในการนำไปพิจารณาต่อไป

ตารางที่ 4.1

แนวทางพิจารณาในการกำหนดมาตรการทางอาญาสำหรับผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ

สภาพผู้กระทำผิด / ข้อพิจารณา	กลุ่มที่มีแรงจูงใจมาจากผลประโยชน์ทางการเงิน	กลุ่มที่ไม่มีแรงจูงใจมาจากผลประโยชน์ทางการเงิน
วัตถุประสงค์ในการลงโทษที่มุ่งเน้น	การข่มขู่ยับยั้ง	การแก้ไขฟื้นฟู
รูปแบบของมาตรการทางอาญาที่แนะนำ	จำคุก / ปรับ / ริบทรัพย์สิน	การคุมประพฤติ / การทำงานบริการสังคม

[7] *Ibid*, p.134.

ส่วนประเด็นในเรื่องระยะเวลาที่เหมาะสมในการลงโทษจำคุกในคดีการกระทำผิดของอาชญากรคอมพิวเตอร์ ผู้เขียนเห็นว่าประเด็นดังกล่าวขึ้นอยู่กับดุลพินิจของศาลในการกำหนดระดับโทษที่เหมาะสม โดยศาลจะตัดสินลงโทษหนักหรือเบานั้นขึ้นอยู่กับปัจจัยต่าง ๆ หลายปัจจัย อาทิ ปัจจัยของผู้กระทำผิด เช่น กรณีผู้กระทำผิดเป็นเยาวชน หรือปัจจัยจากพฤติการณ์ความร้ายแรงแห่งคดี เช่น ความเสียหายที่เกิดจากการกระทำความผิด การกระทำต่อหน่วยงานของรัฐ การกระทำความผิดซ้ำ เป็นต้น แต่อย่างไรก็ดีแม้ว่าศาลจะตัดสินลงโทษสถานหนักหรือแม้ว่าฝ่ายนิติบัญญัติจะแก้ไขกฎหมายเพิ่มโทษสำหรับการกระทำผิดของแฮกเกอร์ให้สูงขึ้นเพียงใดก็ตาม หาได้เป็นหนทางหรือหลักประกันที่ยั่งยืนในการควบคุมอาชญากรรมประเภทนี้ได้อย่างสิ้นเชิง[8] ดังนั้นแนวทางที่เหมาะสมจึงมิได้จำกัดอยู่ที่การลงโทษหนักหรือเบา แต่จะต้องนำรูปแบบของมาตรการอื่น ๆ มาใช้เป็นมาตรการเสริมควบคู่กันไปกับการลงโทษทางอาญา ทั้งนี้เพื่อให้สามารถบรรลุวัตถุประสงค์ในการลงโทษได้อย่างแท้จริง

นอกเหนือจากมาตรการทางอาญาทั่ว ๆ ไป เช่น มาตรการลงโทษจำคุก ปรับหรือมาตรการควบคุมความประพฤติที่ศาลอาจนำมาใช้กับผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบแล้ว ทั้งนี้เพื่อให้การควบคุมพฤติกรรมการกระทำความผิดของผู้กระทำผิดเหล่านี้มีประสิทธิภาพมากยิ่งขึ้น ผู้เขียนเห็นว่าศาลควรมีมาตรการเสริมเพิ่มเติมจากมาตรการทั่ว ๆ ไป โดยกำหนดรูปแบบของมาตรการเสริมตามความเหมาะสมกับผู้กระทำผิดและพฤติการณ์แห่งคดีในแต่ละคดี ยกตัวอย่างเช่น

(ก) กรณีผู้กระทำผิดเป็นกลุ่มเด็กและเยาวชน

ควรมีการกำหนดให้ผู้ปกครองและครูอาจารย์เข้ามามีส่วนร่วมในการดูแลควบคุมพฤติกรรมด้านการใช้งานคอมพิวเตอร์ของเด็กและเยาวชนที่กระทำผิดเกี่ยวกับคอมพิวเตอร์ด้วย

(ข) กรณีผู้กระทำผิดต่อนายจ้าง

ควรมีการกำหนดให้ผู้กระทำผิดจะต้องเปิดเผยข้อมูลประวัติการกระทำผิดต่อนายจ้างให้นายจ้างคนใหม่รับทราบ หรืออาจมีการขึ้นทะเบียนประวัติเพื่อเป็นข้อมูลให้หน่วยงานที่จะรับพิจารณาผู้กระทำผิดดังกล่าวเป็นพนักงานใหม่รับทราบก่อนเสมอ

---

[8] Russell G. Smith, “CONFERENCE PAPER: CYBER CRIME SENTENCING The Effectiveness of Criminal Justice Responses,” <http://www.aic.gov.au/conferences/2004/smith.pdf>

(ค) กรณีผู้กระทำผิดที่มีแรงจูงใจมาจากผลประโยชน์ทางการเงิน

ควรมีการกำหนดมาตรการตัดประโยชน์ที่ผู้กระทำผิดได้รับมาจากการกระทำความผิดควบคู่กันไปด้วย ยกตัวอย่างเช่น ริบทรัพย์สินหรือประโยชน์อื่นใดที่ได้มาจากการกระทำความผิด ทั้งนี้เพื่อเป็นการลดแรงจูงใจในการกระทำความผิดในรูปแบบที่มีที่มาจากผลประโยชน์ทางการเงิน

(ง) มาตรการลดแรงจูงใจทางสังคม

เนื่องจากผลรายงานการวิจัยทางอาชญาวิทยาเกี่ยวกับผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบแสดงให้เห็นว่า ปัจจัยด้านการปฏิสัมพันธ์กับกลุ่มเพื่อนแฮกเกอร์ทั้งในทางกายภาพ เช่น การประชุมสัมมนาของกลุ่มแฮกเกอร์ การแข่งขันด้านการเจาะระบบคอมพิวเตอร์ เป็นต้น และในทางอิเล็กทรอนิกส์ เช่น การติดต่อสื่อสารผ่านทางอินเทอร์เน็ต โดยการใช้กระดานข่าวอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์หรือการพูดคุยออนไลน์ เป็นต้น เหล่านี้ล้วนมีอิทธิพลต่อแรงจูงใจในการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ฉะนั้นเพื่อเป็นการลดแรงจูงใจในส่วนนี้ ผู้เขียนเห็นว่าศาลควรมีมาตรการเสริมในการควบคุมการปฏิสัมพันธ์กับกลุ่มเพื่อนแฮกเกอร์ทั้งในทางกายภาพและทางอิเล็กทรอนิกส์ควบคู่กันไปด้วย ยกตัวอย่างเช่น ห้ามเข้าร่วมการประชุมสัมมนาของกลุ่มแฮกเกอร์ ห้ามเข้าร่วมกิจกรรมที่เกี่ยวข้องกับการเข้าถึงระบบคอมพิวเตอร์ เช่น การจัดแข่งขันเจาะระบบคอมพิวเตอร์ เป็นต้น ห้ามติดต่อหรือปฏิสัมพันธ์กับกลุ่มเพื่อนที่อยู่ในกลุ่มเสี่ยงทั้งในทางกายภาพและทางอิเล็กทรอนิกส์ ทั้งนี้ศาลอาจกำหนดมาตรการต่าง ๆ เหล่านี้เป็นส่วนหนึ่งของเงื่อนไขเพื่อคุมความประพฤติของผู้กระทำผิด

(จ) กรณีผู้กระทำผิดซ้ำ

ในกรณีผู้กระทำผิดซ้ำ นอกเหนือจากมาตรการเพิ่มโทษทั่วไปให้มากขึ้น เพื่อเป็นการข่มขู่ยับยั้งพฤติกรรมผู้กระทำผิดให้เกิดความเกรงกลัวและเข็ดหลาบแล้ว ผู้เขียนเห็นว่าศาลควรมีมาตรการเสริมขั้นรุนแรงออกมารองรับพฤติกรรมการกระทำผิดซ้ำของผู้กระทำผิดด้วย ยกตัวอย่างเช่น ห้ามทำงานในด้านไอทีหรืองานอื่นใดที่ต้องใช้ระบบคอมพิวเตอร์และอินเทอร์เน็ต ห้ามครอบครองอุปกรณ์คอมพิวเตอร์หรือใช้งานระบบคอมพิวเตอร์และอินเทอร์เน็ตโดยเด็ดขาด หรือห้ามมิให้ผู้ใด ไม่ว่าจะเป็นผู้ให้บริการด้านอินเทอร์เน็ต ร้านอินเทอร์เน็ตคาเฟ่ หรือบุคคลใด ๆ จัดให้ให้บริการ หรือช่วยเหลือ สนับสนุนให้ผู้กระทำผิดสามารถเข้าถึงระบบอินเทอร์เน็ตได้ โดยผู้ที่ฝ่าฝืนจะต้องได้รับโทษ เป็นต้น

ประเด็นปัญหาในด้านของการวางแนวทางการกำหนดมาตรการทางอาญาที่จำเป็นแก่ผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ ผู้เขียนมีความเห็นว่าแนวทางที่ถูกต้องสำหรับ

การแก้ไขปัญหาดังกล่าว นอกจากการพิจารณาถึงความเหมาะสมในด้านการบรรลุวัตถุประสงค์ในการลงโทษแล้ว การศึกษาถึงรูปแบบและวิธีการบังคับทางอาญาที่นำมาใช้ในคดีการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในต่างประเทศก็เป็นอีกแนวทางหนึ่งในการนำมาพิจารณาถึงความเหมาะสม ข้อดีและข้อจำกัดในแต่ละรูปแบบ แต่ละมาตรการว่าแนวทางดังกล่าวส่งผลในทางปฏิบัติงานหรือมีผลต่อผู้กระทำผิดไปในทิศทางเช่นไร ทั้งนี้เพื่อนำเอาข้อเท็จจริงดังกล่าวมาประเมิน รวมถึงศึกษาความเป็นไปได้ในการนำมาปรับใช้กับคดีการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในประเทศไทยที่จะเกิดขึ้นในอนาคต ซึ่งผู้เขียนจะวิเคราะห์และเสนอแนะแนวทางดังกล่าวโดยจำแนกตามรูปแบบของมาตรการบังคับทางอาญา ดังต่อไปนี้

4.1 โทษจำคุก

โทษจำคุกเป็นโทษหลักที่มีบัญญัติไว้ในกฎหมายเกี่ยวกับการเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในต่างประเทศหลายประเทศ เช่นเดียวกันกับกฎหมายว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ของไทยได้บัญญัติโทษจำคุกเป็นโทษหลักสำหรับฐานความผิดเกี่ยวกับการเข้าถึงข้อมูลของผู้อื่นโดยมิชอบไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 5 ความผิดฐานเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ[9] และในมาตรา 7 ความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ[10] ซึ่งจากการศึกษาพบว่าอัตราโทษจำคุกในความผิดที่เกี่ยวข้องกับการเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในแต่ละประเทศนั้นมีการบัญญัติอัตราขั้นสูงสุดของโทษจำคุกที่ผู้กระทำผิดอาจได้รับแตกต่างกันออกไป รายละเอียดดังตารางเปรียบเทียบต่อไปนี้

---

[9] มาตรา 5 ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

[10] มาตรา 7 ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกิน สี่หมื่นบาทหรือทั้งจำทั้งปรับ

ตารางที่ 4.2

เปรียบเทียบอัตราโทษจำคุกสำหรับความผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในแต่ละประเทศ[11]

ประเทศ	อัตราโทษจำคุก
ออสเตรเลีย	ไม่เกิน 2 ปี
แคนาดา	ไม่เกิน 10 ปี
ฝรั่งเศส	1 ปี (หากส่งผลเสียหายหรือแก้ไขเปลี่ยนแปลง 2 ปี)
เยอรมนี	ไม่เกิน 3 ปี กรณีจารกรรมข้อมูล ไม่เกิน 2 ปี กรณีแก้ไขข้อมูล ไม่เกิน 5 ปี กรณีแทรกแซงการทำงานคอมพิวเตอร์
กรีซ	ไม่เกิน 3 เดือน
อินเดีย	ไม่เกิน 3 ปี
ไอร์แลนด์	ไม่เกิน 3 เดือน
อิสราเอล	ไม่เกิน 2 ปี
อิตาลี	ไม่เกิน 3 ปี
ญี่ปุ่น	ไม่เกิน 1 ปี
ลักเซมเบิร์ก	2 เดือน – 1 ปี (กรณีเสียหาย 2 เดือน – 2 ปี)
มาเลเซีย	ไม่เกิน 5 ปี
เนเธอร์แลนด์	ไม่เกิน 6 เดือน
นิวซีแลนด์	ไม่เกิน 2 ปี
สิงคโปร์	ไม่เกิน 2 ปี
ไทย	ไม่เกิน 6 เดือน (เข้าถึงระบบคอมพิวเตอร์โดยมิชอบ) ไม่เกิน 2 ปี (เข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ)
อังกฤษ	ไม่เกิน 6 เดือน
สหรัฐอเมริกา	มีอัตราสูงสุดหลายอัตรา ตั้งแต่ 1-20 ปีหรืออาจจำคุกตลอดชีวิต(กรณีทำให้ผู้อื่นถึงแก่ความตาย)

[11] โปรดดูรายละเอียดใน ผนวก ค.

จากตารางเปรียบเทียบอัตราโทษขั้นสูงสุดของโทษจำคุกในแต่ละประเทศข้างต้น แสดงให้เห็นว่ากฎหมายเกี่ยวกับการเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในแต่ละประเทศมีการบัญญัติอัตราขั้นสูงสุดของโทษจำคุกที่ผู้กระทำผิดอาจได้รับไว้หลากหลายอัตราต่างกันไป โดยมีอัตราขั้นสูงสุดของโทษจำคุกตั้งแต่ 3 เดือน ไปจนถึง 20 ปี หรืออาจถึงขั้นจำคุกตลอดชีวิตตามกฎหมายของประเทศสหรัฐอเมริกาในกรณีที่การกระทำผิดนั้นทำให้ผู้อื่นถึงแก่ความตาย

ผู้เขียนมีความเห็นว่า มาตรการลงโทษจำคุกผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ เป็นมาตรการที่จำเป็นสำหรับผู้กระทำผิดที่มีแรงจูงใจทางการเงินและมีลักษณะการกระทำความผิดที่โน้มเอียงไปในทางอาชญากร ทั้งนี้เพื่อวัตถุประสงค์ในการตัดโอกาสที่จะกระทำความผิดต่อไป แต่อย่างไรก็ตามการนำโทษจำคุกมาใช้กับผู้กระทำความผิดซึ่งเป็นอาชญากรคอมพิวเตอร์จะต้องมีการวางมาตรการป้องกันในด้านการเข้าถึงระบบคอมพิวเตอร์ของตัวผู้ต้องขังด้วย ทั้งนี้เนื่องจากในเรือนจำบางแห่งอาจมีการให้ความรู้ หรือให้บริการด้านคอมพิวเตอร์หรืออินเทอร์เน็ตแก่ผู้ต้องขัง ซึ่งหากยอมให้ผู้ต้องขังที่เป็นอาชญากรคอมพิวเตอร์สามารถเข้าถึงคอมพิวเตอร์หรือระบบอินเทอร์เน็ตเช่นนี้แล้วย่อมไม่อาจบรรลุต่อวัตถุประสงค์ในการตัดโอกาสในการกระทำผิดได้อย่างแท้จริง

4.2 โทษปรับ

โทษปรับเป็นมาตรการลงโทษหลักที่มีบัญญัติไว้ในกฎหมายเกี่ยวกับการเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในต่างประเทศหลายประเทศเช่นเดียวกันกับโทษจำคุก โดยในกฎหมายว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ในแต่ละประเทศต่างกำหนดอัตราสูงสุดของโทษปรับที่ผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบอาจได้รับไว้แตกต่างกันออกไป ดังตารางเปรียบเทียบต่อไปนี้

ตารางที่ 4.3
เปรียบเทียบอัตราโทษปรับสำหรับความผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในแต่ละประเทศ[12]

ประเทศ	อัตราโทษปรับ[13]
จีน	ไม่เกิน 5,000 เรนมินบิ (22,300 บาท)
ฝรั่งเศส	ไม่เกิน 15,000 ยูโร (727,500 บาท) หากส่งผลเสียหายหรือแก้ไขเปลี่ยนแปลง ไม่เกิน 30,000 ยูโร (1,455,000 บาท)
อินเดีย	ไม่เกิน 200,000 รูปี (164,000 บาท)
ไอร์แลนด์	ไม่เกิน 500 เหรียญ
ญี่ปุ่น	ไม่เกิน 500,000 เยน (150,000 บาท)
ลักเซมเบิร์ก	10,000 – 250,000 เหรียญ (กรณีเสียหาย 50,000 – 500,000 เหรียญ)
มาเลเซีย	ไม่เกิน 500,000 ริงกิต (5,150,000 บาท)
เนเธอร์แลนด์	ไม่เกิน 10,000 เหรียญ
สิงคโปร์	ไม่เกิน 5,000 เหรียญ (114,500 บาท)
ไทย	ไม่เกิน 10,000 บาท (เข้าถึงระบบคอมพิวเตอร์โดยมิชอบ) , ไม่เกิน 40,000 บาท (เข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ)
อังกฤษ	ไม่เกินระดับ 5 ตามตารางมาตรฐาน (ปัจจุบันคือ 5,000 ปอนด์) (316,000 บาท)

จากตารางเปรียบเทียบข้างต้นแสดงให้เห็นว่าแต่ละประเทศได้กำหนดอัตราขั้นสูงสุดของโทษปรับสำหรับการกระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบไว้ในอัตราที่แตกต่างกันไป ซึ่งหากสังเกตจากอัตราโทษปรับในต่างประเทศหลายประเทศจะเห็นว่ามีการกำหนดอัตราขั้นสูง

---

[12] โปรดดูรายละเอียดใน ผนวก ค.

[13] เทียบเคียงหน่วยเงินตราต่างประเทศตามอัตราแลกเปลี่ยนเงินตราต่างประเทศประจำวันที่ 6 มีนาคม 2551

สุดของโทษไว้สูงกว่าอัตราโทษปรับของประเทศไทยมาก ตัวอย่างเช่น ในประเทศฝรั่งเศส กำหนดโทษปรับไม่เกิน 15,000 ยูโร (727,500 บาท) หากส่งผลเสียหายหรือแก้ไขเปลี่ยนแปลง ปรับไม่เกิน 30,000 ยูโร (1,455,000 บาท) ประเทศมาเลเซีย กำหนดโทษปรับไม่เกิน 500,000 ริงกิต (5,150,000 บาท) ส่วนประเทศสิงคโปร์กำหนดโทษปรับ ไม่เกิน 5,000 เหรียญ (114,500 บาท) ซึ่งเมื่อเทียบกับอัตราโทษปรับขั้นสูงสุดตามกฎหมายไทยซึ่งกำหนดโทษปรับไม่เกิน 10,000 บาท (กรณีเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ) หรือไม่เกิน 40,000 บาท (กรณีเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ) แสดงให้เห็นถึงความแตกต่างกันของการกำหนดอัตราโทษปรับในฐานความผิดลักษณะดังกล่าวได้อย่างชัดเจน

ผู้เขียนเห็นว่ามาตรการนี้เป็นมาตรการทางอาญาอีกประการหนึ่งที่มีความจำเป็นแก่ผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ โดยเฉพาะอย่างยิ่งกรณีผู้กระทำผิดที่มีแรงจูงใจหลักมาจากผลประโยชน์ทางการเงิน โดยการนำเอามาตรการนี้มาใช้จะสามารถบรรลุวัตถุประสงค์ในการข่มขู่ยับยั้งพฤติกรรมการกระทำความผิดในลักษณะนี้ได้ แต่อย่างไรก็ตามสำหรับผู้กระทำผิดที่ไม่ได้มีแรงจูงใจหลักมาจากผลประโยชน์ทางการเงิน ผู้เขียนเห็นว่าการนำเอามาตรการเช่นนี้มาปรับใช้อาจไม่มีความจำเป็นและไม่สามารถบรรลุวัตถุประสงค์ในการลงโทษเช่นว่านั้นได้ ปัญหาของรูปแบบในการลงโทษปรับผู้กระทำผิดซึ่งไม่ได้มีแรงจูงใจหลักมาจากผลประโยชน์ทางการเงินนั้นจึงอยู่ที่ในบางกรณีผู้กระทำความผิดทางคอมพิวเตอร์เป็นเพียงเด็กวัยรุ่นซึ่งอาจไม่มีรายได้เพียงพอในการชำระค่าปรับ ผู้เขียนเห็นว่าควรที่จะนำเอารูปแบบของมาตรการบังคับอื่นมาใช้แทน ซึ่งตามประมวลกฎหมายอาญา มาตรา 30/1- 30/3[14] เป็นบทบัญญัติที่ได้มีการแก้ไขเพิ่มเติม

---

[14] มาตรา 30/1 “ในกรณีที่ศาลพิพากษาปรับไม่เกินแปดหมื่นบาท ผู้ต้องโทษปรับซึ่งมิใช่นิติบุคคลและไม่มีเงินชำระค่าปรับอาจยื่นคำร้องต่อศาลชั้นต้นที่พิพากษาคดีเพื่อขอทำงานบริการสังคมหรือทำงานสาธารณประโยชน์แทนค่าปรับ

การพิจารณาคำร้องตามวรรคแรก เมื่อศาลได้พิจารณาถึงฐานะการเงิน ประวัติและสภาพความผิดของผู้ต้องโทษปรับแล้ว เห็นเป็นการสมควร ศาลจะมีคำสั่งให้ผู้นั้นทำงานบริการสังคมหรือทำงานสาธารณประโยชน์แทนค่าปรับก็ได้ ทั้งนี้ ภายใต้การดูแลของพนักงานคุมประพฤติ เจ้าหน้าที่ของรัฐ หน่วยงานของรัฐ หรือองค์การซึ่งมีวัตถุประสงค์เพื่อการบริการสังคม การกุศลสาธารณะหรือสาธารณประโยชน์ที่ยินยอมรับดูแล

กรณีที่ศาลมีคำสั่งให้ผู้ต้องโทษปรับทำงานบริการสังคมหรือทำงานสาธารณประโยชน์แทนค่าปรับให้ศาลกำหนดลักษณะหรือประเภทของงาน ผู้ดูแลการทำงาน วันเริ่มทำงาน

ให้มีการทำงานบริการสังคมแทนค่าปรับได้ ซึ่งผู้เขียนเห็นว่าเป็นแนวทางที่เหมาะสมและเป็นประโยชน์อย่างยิ่ง ทั้งนี้เพราะกรณีผู้กระทำผิดที่ไม่ได้มีแรงจูงใจที่เกี่ยวข้องกับผลประโยชน์ทางการเงิน การนำมาตรการลงโทษปรับมาใช้กับกรณีดังกล่าว นอกจากไม่อาจบรรลุวัตถุประสงค์ในการลงโทษได้แล้วยังอาจส่งผลร้ายต่อการแก้ไขฟื้นฟูผู้กระทำผิดซึ่งเป็นเยาวชนได้อีกด้วย ฉะนั้นแนว

ระยะเวลาทำงาน และจำนวนชั่วโมงที่ถือเป็นการทำงานหนึ่งวัน ทั้งนี้ โดยคำนึงถึงเพศอายุ ประวัติการนับถือศาสนาความประพฤติ สติปัญญา การศึกษาอบรม สุขภาพ ภาวะแห่งจิต นิสัย อาชีพ สิ่งแวดล้อมหรือสภาพความผิดของผู้ต้องโทษปรับประกอบด้วยและศาลจะกำหนดเงื่อนไขอย่างหนึ่งอย่างใดให้ผู้ต้องโทษปรับปฏิบัติเพื่อแก้ไขฟื้นฟูหรือป้องกันมิให้ผู้นั้นกระทำความผิดขึ้นอีกก็ได้

ถ้าภายหลังความปรากฏแก่ศาลว่าพฤติการณ์เกี่ยวกับการทำงานบริการสังคมหรือทำงานสาธารณประโยชน์ของผู้ต้องโทษปรับได้เปลี่ยนแปลงไป ศาลอาจแก้ไขเปลี่ยนแปลงคำสั่งที่กำหนดไว้นั้นก็ได้ตามที่เห็นสมควร

ในการกำหนดระยะเวลาทำงานแทนค่าปรับตามวรรคสาม ให้นำบทบัญญัติมาตรา 30 มาใช้บังคับโดยอนุโลม และในกรณีที่ศาลมิได้กำหนดให้ผู้ต้องโทษปรับทำงานติดต่อ กันไปการทำงานดังกล่าวต้องอยู่ภายในกำหนดระยะเวลาสองปีนับแต่วันเริ่มทำงานตามที่ศาลกำหนด

เพื่อประโยชน์ในการกำหนดจำนวนชั่วโมงทำงานตามวรรคสาม ให้ประธานศาลฎีกามีอำนาจออกระเบียบราชการฝ่ายตุลาการศาลยุติธรรมกำหนดจำนวนชั่วโมงที่ถือเป็นการทำงานหนึ่งวัน สำหรับงานบริการสังคมหรืองานสาธารณประโยชน์แต่ละประเภทได้ตามที่เห็นสมควร”

มาตรา **30/2** “ถ้าภายหลังศาลมีคำสั่งอนุญาตตามมาตรา 30/1 แล้ว ความปรากฏแก่ศาลเองหรือความปรากฏตามคำแถลงของโจทก์หรือเจ้าพนักงานว่า ผู้ต้องโทษปรับมีเงินพอชำระค่าปรับได้ในเวลาที่ยื่นคำร้องตามมาตรา 30/1 หรือฝ่าฝืนหรือไม่ปฏิบัติตามคำสั่งหรือเงื่อนไขที่ศาลกำหนดศาลจะเพิกถอนคำสั่งอนุญาตดังกล่าวและปรับ หรือกักขังแทนค่าปรับ โดยให้หักจำนวนวันที่ทำงานมาแล้วออกจากจำนวนเงินค่าปรับก็ได้

ในระหว่างการทำงานบริการสังคมหรือทำงานสาธารณประโยชน์แทนค่าปรับ หากผู้ต้องโทษปรับไม่ประสงค์จะทำงานดังกล่าวต่อไปอาจขอเปลี่ยนเป็นรับโทษปรับ หรือกักขังแทนค่าปรับก็ได้ ในกรณีนี้ให้ศาลมีคำสั่งอนุญาตตามคำร้อง โดยให้หักจำนวนวันที่ทำงานมาแล้วออกจากจำนวนเงินค่าปรับ “

มาตรา **30/3** “คำสั่งศาลตามมาตรา 30/1 และมาตรา 30/2 ให้เป็นที่สุด”

ทางการใช้มาตรการทำงานบริการสังคมแทนค่าปรับแก่ผู้กระทำผิดที่ไม่ได้มีแรงจูงใจที่เกี่ยวข้องกับผลประโยชน์ทางการเงินผู้เขียนเห็นว่าเป็นมาตรการที่จำเป็น ซึ่งทำให้สามารถบรรลุตามวัตถุประสงค์ในการแก้ไขฟื้นฟูผู้กระทำความผิดได้มากกว่าการใช้โทษปรับ

4.3 โทษริบทรัพย์สิน

การริบทรัพย์สินในคดีการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในประเทศสหรัฐอเมริกาเป็นมาตรการริบทรัพย์สินทางอาญา (criminal forfeiture) ซึ่งกำหนดให้ริบทรัพย์สินที่ใช้ในการกระทำความผิด ซึ่งได้แก่ เครื่องคอมพิวเตอร์และอุปกรณ์ในการเชื่อมต่อและสนับสนุนต่างๆ ให้ตกเป็นของรัฐ โดยมาตรการดังกล่าวมีหลักการเช่นเดียวกันกับมาตรการริบทรัพย์สินที่ใช้หรือมีไว้เพื่อใช้ในการกระทำผิดตามมาตรา 33[15] แห่งประมวลกฎหมายอาญา ซึ่งเป็นโทษที่อยู่ในดุลพินิจของศาลที่จะมีคำสั่งให้ริบทรัพย์สินหรือไม่ก็ได้ นอกเหนือจากที่กฎหมายมีบัญญัติไว้เป็นการเฉพาะ

โทษริบทรัพย์สินที่ใช้ในการกระทำผิดแม้ว่าจะมีวัตถุประสงค์เพื่อตัดโอกาสของผู้กระทำความผิดในการใช้ประโยชน์จากทรัพย์สินนั้นเพื่อการประกอบอาชญากรรมซ้ำอีก แต่หากพิจารณาจากสภาพความเป็นจริง แม้ว่าจะมีการริบอุปกรณ์คอมพิวเตอร์ของผู้กระทำความผิดไปแล้ว ก็ไม่อาจขจัดโอกาสในการกระทำความผิดของผู้นั้นได้อย่างสิ้นเชิง เนื่องจากปัจจุบันยังมีช่องทางที่เอื้อต่อการก่ออาชญากรรมคอมพิวเตอร์ได้อย่างกว้างขวางและสามารถเข้าถึงได้โดยง่าย ทั้งในส่วนของอินเทอร์เน็ตคาเฟ่ บริการคอมพิวเตอร์และอินเทอร์เน็ตของหน่วยงานต่างๆ เช่น ห้องสมุด สถานศึกษาและตามสถานที่ท่องเที่ยวทั่ว ๆ ไป ผู้กระทำผิดยังคงมีโอกาสในการก่ออาชญากรรมคอมพิวเตอร์ได้อย่างสะดวกสบาย และนอกจากนี้โทษในลักษณะดังกล่าวอาจส่งผลกระทบทางอ้อมต่อผู้ที่ไม่ได้กระทำความผิดอีกด้วย กล่าวคือ การริบอุปกรณ์คอมพิวเตอร์ของผู้

---

[15] มาตรา 33 “ในการริบทรัพย์สิน นอกจากศาลจะมีอำนาจริบตามกฎหมายที่บัญญัติไว้โดยเฉพาะแล้ว ให้ศาลมีอำนาจสั่งให้ริบทรัพย์สินดังต่อไปนี้อีกด้วย คือ

(1) ทรัพย์สินซึ่งบุคคลได้ใช้ หรือมีไว้เพื่อใช้ในการกระทำความผิด หรือ

(2) ทรัพย์สินซึ่งบุคคลได้มาโดยได้กระทำความผิด

เว้นแต่ทรัพย์สินเหล่านี้เป็นทรัพย์สินของผู้อื่นซึ่งมิได้รู้เห็นเป็นใจด้วยในการกระทำความผิด”

กระทำผิด อาจจะส่งผลกระทบต่อบุคคลอื่นมากกว่าตัวผู้กระทำผิดได้ ตัวอย่างเช่น หากอุปกรณ์คอมพิวเตอร์นั้นเป็นเครื่องคอมพิวเตอร์ประจำบ้าน ซึ่งสมาชิกในบ้านคนอื่นๆ ใช้สำหรับทำงานต่างๆ ด้วย ฉะนั้นการริบอุปกรณ์คอมพิวเตอร์ดังกล่าวแม้ว่าตามประมวลกฎหมายอาญา มาตรา 33 บัญญัติไว้ให้ริบทรัพย์สินดังกล่าวได้ แต่มาตรการดังกล่าวก็มิอาจตัดโอกาสหรือยับยั้งพฤติกรรมการกระทำผิดดังกล่าวได้ตามวัตถุประสงค์ในการลงโทษอย่างแท้จริง ทั้งยังอาจส่งผลต่อบุคคลอื่น ๆ ได้อีกด้วย แนวทางที่เหมาะสมในการตัดโอกาสกระทำผิดซ้ำ ผู้เขียนเห็นว่าควรจะมุ่งเน้นมาตรการในการจำกัดหรือควบคุมการเข้าถึงหรือใช้งานคอมพิวเตอร์และอินเทอร์เน็ตของผู้กระทำผิดเป็นหลัก[16]

4.4 เงื่อนไขเพื่อคุมความประพฤติ

เงื่อนไขเพื่อคุมความประพฤติผู้กระทำผิดเกี่ยวกับคอมพิวเตอร์เป็นมาตรการที่จำเป็นประการหนึ่งในการควบคุมสอดส่องพฤติกรรมของผู้กระทำผิดในฐานะผู้ถูกคุมความประพฤติ โดยมีวัตถุประสงค์ที่สำคัญ คือ เพื่อควบคุมพฤติกรรมของผู้ถูกคุมความประพฤติไม่ให้ละเมิดเงื่อนไขของศาลหรือกระทำผิดซ้ำอีก และยังเป็นการแก้ไขและบำบัดผู้กระทำผิดที่มิใช่อาชญากรโดยนิสัยให้เกิดการเปลี่ยนแปลงทัศนคติและพฤติกรรมให้อยู่ในบรรทัดฐานของสังคม[17] โดยมาตรการนี้เมื่อเปรียบเทียบกับมาตรการทางอาญาของไทยจะมีลักษณะสอดคล้องกับการกำหนดเงื่อนไขเพื่อคุมความประพฤติตามประมวลกฎหมายอาญา มาตรา 56[18]

---

[16] Russell G. Smith, *supra note* 19.

[17] กรมคุมประพฤติ กระทรวงยุติธรรม, คู่มือตุลาการเกี่ยวกับงานคุมประพฤติ, (กรุงเทพมหานคร : โรงพิมพ์ดอกเบี้ย, 2540), น.4.

[18] ประมวลกฎหมายอาญา มาตรา 56 บัญญัติว่า

"ผู้ใดกระทำความผิดซึ่งมีโทษจำคุก และในคดีนั้นศาลจะลงโทษจำคุกไม่เกินสามปี ถ้าไม่ปรากฏว่าผู้นั้นได้รับโทษจำคุกมาก่อน หรือปรากฏว่าได้รับโทษจำคุกมาก่อน แต่เป็นโทษสำหรับความผิดที่ได้กระทำโดยประมาท หรือความผิดลหุโทษ เมื่อศาลได้คำนึงถึงอายุ ประวัติความประพฤติ สติปัญญา การศึกษาอบรม สุขภาพ ภาวะแห่งจิต นิสัย อาชีพ และสิ่งแวดล้อมของผู้นั้น หรือสภาพความผิด หรือเหตุอื่นอันควรปรานีแล้ว เห็นเป็นการสมควร ศาลจะพิพากษาว่าผู้นั้นมีความผิดแต่รอการกำหนดโทษไว้ หรือกำหนดโทษแต่รอการลงโทษไว้แล้วปล่อยตัวไป เพื่อให้

ในต่างประเทศหน่วยงานด้านคุมประพฤติมีการกำหนดเงื่อนไขเพื่อคุมความประพฤติผู้กระทำผิดเกี่ยวกับคอมพิวเตอร์ทั้งในส่วนของเงื่อนไขทั่วไปและเงื่อนไขที่เกี่ยวข้องกับการใช้คอมพิวเตอร์ของผู้ถูกคุมความประพฤติไว้หลายประการ[19] มาตรการทางอาญาที่จำเป็นแก่ผู้กระทำผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบที่จัดอยู่ในกลุ่มของเงื่อนไขในการคุมประพฤติที่สำคัญ ได้แก่ การทำงานบริการสังคม การจำกัดการเข้าถึง การใช้งานคอมพิวเตอร์และอินเทอร์เน็ต การควบคุม สอดส่องพฤติกรรมการใช้งานคอมพิวเตอร์และอินเทอร์เน็ต

โอกาสผู้นั้นกลับตัวภายในระยะเวลาที่ศาลจะได้กำหนด แต่ต้องไม่เกินห้าปีนับแต่วันที่ศาลพิพากษา โดยจะกำหนดเงื่อนไขเพื่อคุมความประพฤติของผู้นั้นด้วยหรือไม่ก็ได้

เงื่อนไขเพื่อคุมความประพฤติของผู้กระทำความผิดนั้น ศาลอาจกำหนดข้อเดียวหรือหลายข้อ ดังต่อไปนี้

(1) ให้ไปรายงานตัวต่อเจ้าพนักงานที่ศาลระบุไว้เป็นครั้งคราว เพื่อเจ้าพนักงานจะได้สอบถาม แนะนำ ช่วยเหลือ หรือตักเตือนตามที่เห็นสมควรในเรื่องความประพฤติและการประกอบอาชีพ หรือจัดให้กระทำกิจกรรมบริการสังคมหรือสาธารณประโยชน์ตามที่เจ้าพนักงานและผู้กระทำความผิดเห็นสมควร

(2) ให้ฝึกหัดหรือทำงานอาชีพอันเป็นกิจจะลักษณะ

(3) ให้ละเว้นการคบหาสมาคมหรือการประพฤติใดอันอาจนำไปสู่การกระทำความผิดในทำนองเดียวกันอีก

(4) ให้ไปรับการบำบัดรักษาการติดยาเสพติดให้โทษ ความบกพร่องทางร่ายกายหรือจิตใจ หรือความเจ็บป่วยอย่างอื่น ณ สถานที่และตามระยะเวลาที่ศาลกำหนด

(5) เงื่อนไขอื่น ๆ ตามที่ศาลเห็นสมควรกำหนดเพื่อแก้ไขฟื้นฟูหรือป้องกันมิให้ผู้กระทำความผิดกระทำหรือมีโอกาสกระทำความผิดขึ้นอีก

เงื่อนไขตามที่ศาลได้กำหนดตามความในวรรคก่อนนั้น ถ้าภายหลังความปรากฏแก่ศาลตามคำขอของผู้กระทำความผิด ผู้แทนโดยชอบธรรมของผู้นั้น ผู้อนุบาลของผู้นั้น พนักงานอัยการหรือพนักงานว่า พฤติการณ์ที่เกี่ยวแก่การควบคุมความประพฤติของผู้กระทำความผิดได้เปลี่ยนแปลงไป เมื่อศาลเห็นสมควร ศาลอาจแก้ไขเพิ่มเติมหรือเพิกถอนข้อหนึ่งข้อใดเสียก็ได้ หรือจะกำหนดเงื่อนไขข้อใด ตามที่กล่าวในวรรคก่อนที่ศาลยังมิได้กำหนดไว้เพิ่มเติมขึ้นอีกก็ได้”

[19] โปรดดูรายละเอียดในภาคผนวก ข.

การทำงานบริการสังคม เป็นรูปแบบหนึ่งของมาตรการบังคับทางอาญาที่ผู้เขียนเห็นว่าเป็นมาตรการที่จำเป็นแก่ผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ โดยเฉพาะอย่างยิ่งสำหรับผู้กระทำผิดซึ่งไม่ได้มีแรงจูงใจที่เกี่ยวข้องกับผลประโยชน์ทางการเงิน ทั้งนี้เนื่องจากมาตรการดังกล่าวมีความสอดคล้องกับวัตถุประสงค์ในการลงโทษเพื่อการแก้ไขฟื้นฟูผู้กระทำความผิด ทำให้ผู้กระทำความผิดเปลี่ยนทัศนคติและสำนึกผิดในการกระทำความผิดของตน พร้อมที่จะกลับตนเป็นคนดีของสังคมได้ในอนาคต ดังจะเห็นได้จากตัวอย่างคดีเกี่ยวกับการกระทำความผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในต่างประเทศซึ่งได้นำเอารูปแบบของการทำงานบริการสังคมมาใช้ในหลายคดี ส่วนประเด็นเรื่องรูปแบบของการทำงานบริการสังคมที่เหมาะสมกับคดีการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ผู้เขียนเห็นว่า ควรเป็นรูปแบบที่ให้ผู้กระทำผิดได้อาศัยความรู้ความสามารถในด้านคอมพิวเตอร์ของตนให้เป็นประโยชน์ต่อสังคมส่วนรวม ซึ่งวิธีการดังกล่าวนี้นอกจากจะทำให้ผู้กระทำความผิดได้มีโอกาสในการบำเพ็ญประโยชน์ให้แก่ชุมชนและสังคมแล้ว ยังส่งผลให้ผู้กระทำความผิดเห็นคุณค่าของตนเองในการนำความรู้ที่ตนมีมาสร้างสรรค์ในสิ่งที่ดีงาม ก่อให้เกิดความภาคภูมิใจได้ดีกว่าการนำความรู้ดังกล่าวไปใช้ในการกระทำความผิด ยกตัวอย่างรูปแบบของการทำงานบริการสังคมในลักษณะเช่นนี้ เช่น

คดีแรก U.S. v. David Smith[20] ในคดีนี้ศาลลงโทษให้จำเลยช่วยเหลือเจ้าหน้าที่ตำรวจในการสืบสวนคดีอาชญากรรมคอมพิวเตอร์ ซึ่งถือว่าประสบผลสำเร็จเป็นอย่างดีเนื่องจากสามารถติดตามแกะรอยจนสามารถจับกุมตัวนาย Jan Dewit ผู้สร้างไวรัสคอมพิวเตอร์ที่ชื่อ “ Anna Kournikova “ ได้ในประเทศเนเธอร์แลนด์ เมื่อวันที่ 27 กันยายน ค.ศ. 2001 รวมทั้งสามารถจับกุมนาย Simon Vallor ผู้สร้าง ไวรัสคอมพิวเตอร์ “ Gokar” ได้ในกรุงลอนดอน ประเทศอังกฤษ เมื่อวันที่ 21 มกราคม ค.ศ. 2003

คดีที่สอง U.S. v. Richard W. Gerhardt[21] ในคดีนี้จำเลยกระทำความผิดเกี่ยวกับการจารกรรมข้อมูลอิเล็กทรอนิกส์ District Court of Western District of Missouri พิพากษาคดีนี้ใน

---

[20] United States v. David Smith, Case Number: 2:99-CR-730-01, Distric of New Jersey, United States District Court , (May 3, 2002)(Unpublished), available at <http://www.rbs2.com/dls.htm>; and see also Creator of Melissa Computer Virus Sentenced to 20 Months in Federal Prison, < http://www.usdoj.gov/criminal/cybercrime/melissaSent.htm >, 1 May 2001.

[21] “St.Joseph Man Charged in District's First Computer Hacking Indictment,”

วันที่ 13 มีนาคม ค.ศ.2003 ลงโทษให้จำเลยสอนหนังสือให้ความรู้ในโรงเรียนและชุมชน โดยสอนถึงภัยที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ รวมทั้งประชาสัมพันธ์ต่อต้านการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ การลงโทษในลักษณะเช่นนี้จะทำให้ผู้กระทำความผิดสามารถนำความรู้ความสามารถที่เกี่ยวกับคอมพิวเตอร์และเทคโนโลยีสารสนเทศของตนมาใช้ประโยชน์ในงานบริการสังคมได้ ภายใต้การควบคุมสอดส่องของพนักงานคุมประพฤติ[22]

ส่วนการจำกัดการเข้าถึงและการใช้งานคอมพิวเตอร์และอินเทอร์เน็ต การควบคุมสอดส่องพฤติกรรมการใช้งานคอมพิวเตอร์และอินเทอร์เน็ตของผู้กระทำผิด มีวัตถุประสงค์ในการป้องกันสังคมให้ได้รับความปลอดภัยจากการกระทำความผิดซ้ำของผู้ถูกคุมความประพฤติ แต่อย่างไรก็ตามรูปแบบดังกล่าวก่อให้เกิดข้อถกเถียงในต่างประเทศว่า ศาลนำมาตรการดังกล่าวมาใช้ควบคุมจำเลยอย่างเข้มงวดเกินไปหรือไม่[23] ซึ่งปัญหาในเรื่องนี้อาจพิจารณาได้ 2 ด้าน คือ ในด้านของการป้องกันสังคมส่วนรวม มาตรการดังกล่าวย่อมมีความจำเป็นในการสร้างความเชื่อมั่นให้กับคนในสังคมว่าผู้ถูกคุมความประพฤติจะไม่กลับมากระทำความผิดซ้ำสร้างความเสียหายให้แก่คนในสังคมอีก แต่ในด้านตรงกันข้าม คือ สิทธิของผู้ถูกคุมความประพฤติซึ่งต้องถูกลิดรอนไป อาจส่งผลให้ผู้ถูกคุมความประพฤติเสียโอกาสในการได้รับบริการบางประการ เช่น บริการต่าง ๆ ในอินเทอร์เน็ต หรืออาจทำให้ต้องตกงานในกรณีที่ผู้กระทำความผิดทำงานที่จำต้องอาศัยคอมพิวเตอร์และอินเทอร์เน็ตเป็นหลัก เช่น โปรแกรมเมอร์ เจ้าหน้าที่ดูแลระบบคอมพิวเตอร์ เป็นต้น ซึ่งแน่นอนว่าผลกระทบดังกล่าวอาจเป็นผลร้ายอย่างยิ่งในการแก้ไขฟื้นฟูผู้กระทำความผิด กล่าวคือ ผู้กระทำผิดหรือผู้ถูกคุมประพฤติอาจจะต่อต้านโดยฝ่าฝืนเงื่อนไขดังกล่าว หรือพยายามหลบเลี่ยงการควบคุมสอดส่องของเจ้าหน้าที่ ซึ่งในที่สุดจะนำไปสู่การกระทำความผิดซ้ำในอนาคต ดังเช่นกรณีที่เคยเกิดขึ้นในคดีของนายเควิน มิตนิก[24] แต่อย่างไรก็ดี ผู้เขียนมีความเห็นว่ามาตรการดังกล่าวยังคงมีความจำเป็นแก่ผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ เพียงแต่แนวทางปฏิบัติและขอบเขตของการควบคุมสอดส่องดังกล่าวจะต้องไม่ก้าวล่วงสิทธิของผู้ถูกคุมความประพฤติมากจนเกินไป ซึ่งหน่วยงานที่รับผิดชอบในเรื่องนี้จะต้องมีการกำหนดกรอบหรือ

< http://www.usdoj.gov/criminal/cybercrime/gerhardtPlea.htm >, 20 December 2002.

[22] Russell G. Smith, *supra note* 19.

[23] Christopher M.E. Painter, “Supervised Release and Probation Restrictions in Hacker Cases,” <http://www.usdoj.gov/criminal/cybercrime/usamarch2001_7.htm>

[24] United States v. Mitnick, 145 F. 3d 1342 (9th Cir. 1998).

ขอบเขตของรายละเอียดเหล่านี้ออกมาเป็นรูปธรรมอย่างชัดเจนเพื่อให้ผู้ถูกคุมความประพฤติได้รับทราบถึงเงื่อนไขเพื่อคุมความประพฤติดังกล่าว นอกจากนี้มาตรการดังกล่าวข้างต้นจะต้องอาศัยบุคลากรที่มีศักยภาพเพียงพอในการควบคุมสอดส่องพฤติกรรมของผู้ถูกคุมความประพฤติได้ โดยเฉพาะอย่างยิ่งควรจะต้องได้รับการฝึกอบรมและมีความรู้ความเชี่ยวชาญในด้านคอมพิวเตอร์พอสมควร ซึ่งในสภาพของความเป็นจริงลักษณะของงานดังกล่าวอาจจะก่อภาระที่หนักมากหากจะให้พนักงานคุมประพฤติต้องปฏิบัติงานดังกล่าว และอาจจะส่งผลให้การคุมประพฤติผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบไม่ประสบผลสำเร็จเท่าที่ควร

4.5 มาตรการอื่น

นอกเหนือจากมาตรการบังคับทางอาญาดังกล่าวข้างต้นแล้ว ในต่างประเทศมีการนำเอาวิธีการกักขังที่บ้าน (House Arrest หรือ Home confinement หรือ Home Detention) และการควบคุมด้วยเครื่องอิเล็กทรอนิกส์ มาใช้ในคดีเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ด้วย โดยวิธีการกักขังที่บ้านเป็นการกำหนดให้ผู้กระทำผิดอยู่ในบ้านของตนเองทุกวันในช่วงระยะเวลาหนึ่ง จะออกไปนอกบ้านได้เฉพาะกรณีที่ไปทำงาน หรือไปเรียนหนังสือ หรือไปรับคำปรึกษาแนะนำ วิธีการนี้มักจะให้เป็นเงื่อนไขหนึ่งในการคุมความประพฤติแบบเข้มงวด (Intensive Probation Supervision – IPS หรือ Intensive Supervision Probation - ISP) สามารถใช้ได้กับผู้กระทำความผิดที่เป็นทั้งเด็กและผู้ใหญ่ การใช้วิธีการกักขังที่บ้านนี้อาจตรวจสอบผ่านทางโทรศัพท์และการออกไปสอดส่องที่บ้านของผู้กระทำผิด หรืออาจผ่านทางเครื่องมืออิเล็กทรอนิกส์ ที่มักจะเรียกว่า “การควบคุมด้วยเครื่องมืออิเล็กทรอนิกส์” (Electronics Monitoring – EM หรือ Electronics Surveillance)[25]

แม้ว่าประเทศไทยในปัจจุบันยังไม่มีการใช้โทษกักขังที่บ้านและการควบคุมด้วยเครื่องอิเล็กทรอนิกส์ แต่ก็มีนักกฎหมายไทย[26] ได้ให้ความเห็นว่ามาตรการดังกล่าวสามารถนำมาปรับใช้

---

[25] ศักดิ์ชัย เลิศพานิชพันธุ์, “การปฏิบัติต่อผู้กระทำผิดในชุมชนกับการใช้มาตรการลงโทษระดับกลาง,” ใน กระบวนทัศน์ใหม่ของกระบวนการยุติธรรมในการปฏิบัติต่อผู้กระทำผิด การประชุมทางวิชาการระดับชาติว่าด้วยงานยุติธรรม ครั้งที่ 1 (กรุงเทพมหานคร: โรงพิมพ์คุรุสภา, 2547), น.265-267.

[26] *เพิ่งอ้าง*, น.274-275.

กับกระบวนการยุติธรรมของไทยได้โดยอาศัยบทบัญญัติตามมาตรา 24[27] แห่งประมวลกฎหมายอาญามาใช้ โดยศาลอาจมีคำพิพากษาให้กักขังผู้กระทำความผิดไว้ที่บ้าน และในส่วนของการบังคับใช้วิธีการนี้ให้ได้ผล น่าจะนำมาตรา 26[28] แห่งประมวลกฎหมายอาญา ซึ่งได้ให้อำนาจศาลในการกำหนดเงื่อนไขให้ผู้ต้องโทษกักขังปฏิบัติอย่างหนึ่งอย่างใดหรือไม่ก็ได้ นั่นคือ ศาลอาจจะกำหนดเงื่อนไขให้ผู้ต้องโทษกักขังอยู่ในความดูแลของพนักงานคุมประพฤติ เพราะมาตรา 6 อนุมาตรา 7 แห่งพระราชบัญญัติวิธีดำเนินการคุมความประพฤติตามประมวลกฎหมายอาญา พ.ศ. 2522[29] ได้เปิดช่องให้พนักงานคุมประพฤติทำหน้าที่อื่นเกี่ยวกับการคุมความประพฤติตามที่

---

[27] มาตรา 24 “ผู้ใดต้องโทษกักขัง ให้กักตัวไว้ในสถานที่กักขังซึ่งกำหนดไว้อันมิใช่เรือนจำสถานีตำรวจ หรือสถานที่ควบคุมผู้ต้องหาของพนักงานสอบสวน

ถ้าศาลเห็นเป็นการสมควร จะสั่งในคำพิพากษาให้กักขังผู้กระทำความผิดไว้ในที่อาศัยของผู้นั้นเอง หรือของผู้อื่นที่ยินยอมรับผู้นั้นไว้ หรือสถานที่อื่นที่อาจกักขังได้ เพื่อให้เหมาะสมกับประเภทหรือสภาพของผู้ถูกกักขังก็ได้

ถ้าความปรากฏแก่ศาลว่า การกักขังผู้ต้องโทษกักขังไว้ในสถานที่กักขังตามวรรคหนึ่งหรือวรรคสองอาจก่อให้เกิดอันตรายต่อผู้นั้น หรือทำให้ผู้ซึ่งต้องพึ่งพาผู้ต้องโทษกักขังในการดำรงชีพได้รับความเดือดร้อนเกินสมควร หรือมีพฤติการณ์พิเศษประการอื่นที่แสดงให้เห็นว่าไม่สมควรกักขังผู้ต้องโทษกักขังในสถานที่ดังกล่าว ศาลจะมีคำสั่งให้กักขังผู้ต้องโทษกักขังในสถานที่อื่นซึ่งมิใช่ที่อยู่อาศัยของผู้นั้นเองโดยได้รับความยินยอมจากเจ้าของหรือผู้ครอบครองสถานที่ก็ได้

กรณีเช่นว่านี้ให้ศาลมีอำนาจกำหนดเงื่อนไขอย่างหนึ่งอย่างใดให้ผู้ต้องโทษกักขังปฏิบัติ และหากเจ้าของหรือ ผู้ครอบครองสถานที่ดังกล่าวยินยอม ศาลอาจมีคำสั่งแต่งตั้งผู้นั้นเป็นผู้ควบคุมดูแลและให้ถือว่าผู้ที่ได้รับแต่งตั้งเป็นเจ้าพนักงานตามประมวลกฎหมายนี้ ”

[28] มาตรา 26 “ถ้าผู้ต้องโทษกักขังถูกกักขังในที่อาศัยของผู้นั้นเองหรือของผู้อื่นที่ยินยอมรับผู้นั้นไว้ ผู้ต้องโทษกักขังนั้นมีสิทธิที่จะดำเนินการในวิชาชีพหรืออาชีพของตนในสถานที่ดังกล่าวได้ ในการนี้ศาลจะกำหนดเงื่อนไขให้ผู้ต้องโทษกักขังปฏิบัติอย่างหนึ่งอย่างใดหรือไม่ก็ได้แล้วแต่ศาลจะเห็นสมควร”

[29] ตามมาตรา 6 อนุมาตรา 7 แห่งพระราชบัญญัติวิธีดำเนินการคุมความประพฤติตามประมวลกฎหมายอาญา พ.ศ. 2522 บัญญัติไว้ว่า “ ให้พนักงานคุมประพฤติมีอำนาจหน้าที่ตามพระราชบัญญัตินี้และกฎหมายอื่นและโดยเฉพาะให้มีอำนาจหน้าที่ดังต่อไปนี้...

(7) ทำหน้าที่อื่นเกี่ยวกับการคุมความประพฤติตามที่ศาลเห็นสมควร”

ศาลกำหนด และนอกจากนี้ ในปัจจุบันยังมีการเพิ่มเติมมาตรการควบคุมผู้ต้องขังนอกเรือนจำ โดยมีการออกพระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายวิธีพิจารณาความอาญา (ฉบับที่ 25) พ.ศ. 2550 เพื่อปรับปรุงวิธีการขังโดยกำหนดวิธีการหรือสถานที่ในการขังนอกเรือนจำให้เหมาะสมกับสภาพของผู้ต้องขัง ทั้งนี้เพื่อแก้ไขปัญหาคนล้นคุกและยังสามารถบรรลุวัตถุประสงค์ในการแก้ไขฟื้นฟูผู้กระทำผิดให้สามารถกลับคืนสู่สังคมได้อย่างมีคุณภาพ โดยในมาตรา 89/1[30] แห่งประมวลกฎหมายวิธีพิจารณาความอาญา เป็นกรณีของผู้ต้องหาที่อยู่ระหว่างการสอบสวนหรือการพิจารณา ให้ศาลอาจสั่งให้ควบคุมผู้ต้องหาในสถานที่อื่นนอกเรือนจำได้ แต่ต้องอยู่ในความควบคุมของผู้ร้องขอหรือเจ้าพนักงานที่ศาลกำหนด ผู้เขียนมีความเห็นว่ามาตรการดังกล่าวเป็นอีกหนึ่งมาตรการที่มีความจำเป็นแก่ผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ ทั้งนี้เพราะมาตรการดังกล่าวนอกจากจะเอื้อประโยชน์ในการแก้ไขฟื้นฟูผู้กระทำผิดได้เป็นอย่างดีแล้ว ยังสามารถบรรลุวัตถุประสงค์ในการตัดโอกาสกระทำความผิดซ้ำได้เช่นเดียวกับคุมขังในเรือนจำ

การกังขังที่บ้านและการควบคุมด้วยเครื่องมืออิเล็กทรอนิกส์นี้ ผู้เขียนเห็นว่าแม้จะเป็นมาตรการสมัยใหม่ แต่ก็มีความจำเป็นแก่ผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ เนื่องจากหลักการดังกล่าวเหมาะสมที่จะนำมาใช้กับผู้กระทำผิดที่ไม่ได้มีแรงจูงใจมาจากผลประโยชน์

---

[30] มาตรา 89/1 “ ในกรณีที่มีเหตุจำเป็นระหว่างสอบสวนหรือพิจารณา เมื่อพนักงานสอบสวน พนักงานอัยการ ผู้บัญชาการเรือนจำ หรือเจ้าพนักงานผู้มีหน้าที่จัดการตามหมายขังร้องขอ หรือเมื่อศาลเห็นสมควร ศาลจะมีคำสั่งให้ขังผู้ต้องหาหรือจำเลยไว้ในสถานที่อื่นตามที่บุคคลดังกล่าวร้องขอ หรือตามที่ศาลเห็นสมควรนอกจากเรือนจำก็ได้ โดยให้อยู่ในความควบคุมของผู้ร้องขอ หรือเจ้าพนักงานตามที่ศาลกำหนด ในการนี้ ศาลจะกำหนดระยะเวลาตามที่ศาลเห็นสมควรก็ได้

ในการพิจารณาเพื่อมีคำสั่งตามวรรคหนึ่ง ศาลจะดำเนินการไต่สวนหรือให้ผู้เสียหายหรือเจ้าพนักงานที่เกี่ยวข้องตามหมายขังคัดค้านก่อนมีคำสั่งก็ได้

สถานที่อื่นตามวรรคหนึ่งต้องมิใช่สถานีตำรวจ หรือสถานที่ควบคุมผู้ต้องหาของพนักงานสอบสวน โดยมีลักษณะตามที่กำหนดในกฎกระทรวงซึ่งต้องกำหนดวิธีการควบคุมและมาตรการเพื่อป้องกันการหลบหนีหรือความเสียหายที่อาจเกิดขึ้นด้วย

เมื่อศาลมีคำสั่งตามวรรคหนึ่งแล้ว หากภายหลังผู้ต้องหาหรือจำเลยไม่ปฏิบัติตามวิธีการหรือมาตรการตามวรรคสามหรือพฤติการณ์ได้เปลี่ยนแปลงไป ให้ศาลมีอำนาจเปลี่ยนแปลงคำสั่งหรือให้ดำเนินการตามหมายขังได้ ”

ทางการเงิน ทั้งนี้เพื่อวัตถุประสงค์ในการแก้ไขฟื้นฟูจิตใจและพฤติกรรมของผู้กระทำผิด ทั้งยังสามารถควบคุมพฤติกรรมในการเข้าถึงคอมพิวเตอร์หรือระบบอินเทอร์เน็ตจากภายนอกบ้านอันเป็นช่องทางในการกระทำผิดซ้ำได้ในอนาคต แต่อย่างไรก็ตามเนื่องจากปัญหาบางประการอาจส่งผลให้มาตรการดังกล่าวไม่อาจจะนำมาใช้ในประเทศไทยได้ กล่าวคือ มาตรการดังกล่าวจำต้องมีค่าใช้จ่ายในการดำเนินการ รวมทั้งจะต้องจัดซื้ออุปกรณ์ต่างๆ จากต่างประเทศ ซึ่งจะต้องอาศัยงบประมาณเป็นจำนวนมาก รวมทั้งจะต้องมีการฝึกอบรมเจ้าหน้าที่ ประกอบกับมีการประสานงานระหว่างหน่วยงานที่เกี่ยวข้อง อย่างไรก็ดีในอนาคตหากมีการนำเอามาตรการนี้มาใช้ในประเทศไทย ผู้เขียนขอตั้งข้อสังเกตในการนำมาตรการดังกล่าวมาใช้กับคดีการกระทำความผิดของอาชญากรคอมพิวเตอร์ คือ มาตรการนี้เมื่อนำมาใช้กับผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ ควรมีการนำเอามาตรการควบคุมการเข้าถึงคอมพิวเตอร์และระบบอินเทอร์เน็ตภายในบ้านมาใช้ควบคู่กันไปด้วย ทั้งนี้เพื่อตัดโอกาสที่ผู้กระทำผิดจะอาศัยคอมพิวเตอร์ภายในบ้านเป็นเครื่องมือในการกระทำความผิดซ้ำ และนอกจากนี้ระบบของการควบคุมตัวผู้กระทำความผิดซึ่งเป็นผู้ที่มีความเชี่ยวชาญในด้านเทคโนโลยี จะต้องมีการพิจารณาอย่างถี่ถ้วนว่าเครื่องมือดังกล่าวมีประสิทธิภาพเพียงพอที่จะควบคุมผู้กระทำความผิดในลักษณะเช่นนี้ได้หรือไม่ มิฉะนั้นการดำเนินการดังกล่าวอาจต้องเสียทั้งเวลาและงบประมาณไปโดยเปล่าประโยชน์

โดยสรุป จากการศึกษาเปรียบเทียบมาตรการทางอาญาที่นำมาใช้ในการกระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในต่างประเทศกับมาตรการทางอาญาของไทย พบว่ามีมาตรการทางอาญาหลายรูปแบบที่สอดคล้องและอาจนำมาปรับใช้กับคดีการกระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในประเทศไทยได้ มาตรการเหล่านี้ ได้แก่ โทษจำคุก ปรับ ริบทรัพย์สินที่ใช้ในการกระทำผิด และมาตรการควบคุมความประพฤติหรือเงื่อนไขเพื่อคุมความประพฤติ

แต่อย่างไรก็ตามการนำมาตรการดังกล่าวมาปรับใช้กับผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบนั้นจะต้องคำนึงถึงความเหมาะสมกับวัตถุประสงค์ในการลงโทษ ลักษณะความผิด รวมถึงสภาพของตัวผู้กระทำผิดควบคู่กันไปด้วยเสมอ ทั้งนี้เพื่อให้การนำเอามาตรการดังกล่าวมาใช้นั้นมีประสิทธิภาพและสามารถบรรลุวัตถุประสงค์ได้อย่างแท้จริง การศึกษาในครั้งนี้จึงมีข้อเสนอแนะ ดังนี้ <u>ประการแรก</u> กรณีโทษจำคุกที่จะนำมาใช้กับผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบจะต้องมีการวางมาตรการในการจำกัดการเข้าถึงระบบคอมพิวเตอร์ของผู้ต้องขังเพื่อเป็นการตัดโอกาสในการกระทำผิดซ้ำในขณะที่อยู่ในเรือนจำ <u>ประการที่สอง</u> มาตรการริบทรัพย์สินที่ใช้ในการกระทำผิด อันได้แก่ เครื่องคอมพิวเตอร์และอุปกรณ์เชื่อมต่อสำหรับกรณีกระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ มาตรการนี้เป็นมาตรการที่ไม่สามารถ

ตัดโอกาสในการกระทำผิดซ้ำและยับยั้งพฤติกรรมการกระทำผิดในลักษณะนี้ได้ตามวัตถุประสงค์ในการลงโทษอย่างแท้จริง เนื่องจากแม้จะริบทรัพย์สินดังกล่าวแล้วผู้กระทำผิดยังมีช่องทางหลายช่องทางที่เอื้อในการกลับไปกระทำความผิดซ้ำได้โดยง่าย รวมทั้งการนำเอามาตรการนี้มาใช้อาจส่งผลกระทบต่อผู้อื่นได้อีกด้วย ฉะนั้นในกรณีผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ การตัดโอกาสหรือยับยั้งพฤติกรรมการกระทำผิดซ้ำควรมุ่งเน้นการใช้แนวทางการจำกัดหรือควบคุมพฤติกรรมการเข้าถึงหรือใช้งานคอมพิวเตอร์และอินเทอร์เน็ตเป็นหลัก ประการที่สาม มาตรการเพื่อคุมความประพฤติผู้กระทำผิด การนำมาปรับใช้กับผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบนั้นควรเลือกใช้รูปแบบที่เหมาะสมกับผู้กระทำผิดเป็นรายบุคคล เช่น การให้ทำงานบริการสังคม โดยเลือกรูปแบบของงานที่อาศัยความสามารถของผู้กระทำผิดมาใช้ให้เกิดประโยชน์ต่อสังคมส่วนรวม เป็นต้น และนอกจากนี้หน่วยงานที่รับผิดชอบจะต้องเตรียมความพร้อมทั้งในด้านบุคลากรและอุปกรณ์เครื่องมือที่จำเป็นในการนำมาใช้เพื่อควบคุมความประพฤติผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบได้อย่างมีประสิทธิภาพสูงสุด และ ประการสุดท้าย ศาลควรนำมาตรการเสริมมาใช้ควบคู่กับมาตรการทางอาญาทั่วไปด้วย เช่น กำหนดให้ผู้ปกครองและครูอาจารย์เข้ามามีส่วนร่วมในการควบคุมความประพฤติด้านการใช้คอมพิวเตอร์ของผู้กระทำผิดที่เป็นเด็กและเยาวชน กำหนดให้ผู้กระทำผิดต่อนายจ้างต้องเปิดเผยข้อมูลประวัติการกระทำผิดให้นายจ้างใหม่รับทราบก่อนรับเข้าทำงาน หรือกำหนดห้ามไม่ให้ เข้าร่วมหรือมีปฏิสัมพันธ์กับกลุ่มแฮกเกอร์ทั้งในทางกายภาพและทางอิเล็กทรอนิกส์ เป็นต้น