บทที่ 4
กลไกการแก้ปัญหาการส่งผู้ร้ายข้ามแดนในกรณีอาชญากรรมคอมพิวเตอร์

จากการศึกษาในบทก่อนจะเห็นได้ว่า ในทางทฤษฎี หลักเกณฑ์ว่าด้วยการส่งผู้ร้ายข้ามแดนที่รัฐทั้งหลายถือปฏิบัติอยู่ในปัจจุบันนี้ เป็นแนวทางหนึ่งในการนำตัวผู้กระทำความผิดที่ไม่ได้อยู่ภายใต้เขตอำนาจของรัฐมาดำเนินคดีและลงโทษ อย่างไรก็ตาม จากการศึกษาพบว่า การนำหลักเกณฑ์ว่าด้วยการส่งผู้ร้ายข้ามแดนมาใช้บังคับกับอาชญากรรมชนิดใหม่เช่นอาชญากรรมคอมพิวเตอร์ กลับทำให้เกิดปัญหาและอุปสรรคในทางปฏิบัติ ดังนั้น ในบทนี้ผู้เขียนจะได้วิเคราะห์และศึกษาถึงกลไกการแก้ไขปัญหาและอุปสรรคที่เกิดขึ้นและอาจเกิดขึ้นดังกล่าว เพื่อให้รัฐสามารถให้ความร่วมมือในการส่งผู้ร้ายข้ามแดนในคดีอาชญากรรมคอมพิวเตอร์ได้อย่างมีประสิทธิภาพ โดยการศึกษาในบทนี้ ผู้เขียนได้แยกการศึกษาถึงกลไกการแก้ไขปัญหาในสองระดับ คือ ในระดับระหว่างประเทศและในระดับประเทศ

4.1 กลไกการแก้ปัญหาในระดับระหว่างประเทศ

กลไกการแก้ไขปัญหาในระดับระหว่างประเทศนี้ เป็นกลไกการแก้ปัญหาในส่วนของความตกลงระหว่างประเทศ ทั้งนี้จากการศึกษาพบว่า ปัญหาและอุปสรรคในการส่งผู้ร้ายข้ามแดนในกรณีอาชญากรรมคอมพิวเตอร์ส่วนหนึ่งมีที่มาจากสนธิสัญญาหรือความตกลงระหว่างประเทศเกี่ยวกับการส่งผู้ร้ายข้ามแดนมีเนื้อหาไม่ครอบคลุมถึงความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์ ซึ่งจากทางปฏิบัติที่เกิดขึ้นในประชาคมระหว่างประเทศ แนวทางในการแก้ไขปัญหาการส่งผู้ร้ายข้ามแดนในคดีอาชญากรรมคอมพิวเตอร์ ปรากฏอยู่สองแนวทางคือ ความร่วมมือระหว่างประเทศในรูปแบบความตกลงทวิภาคีและความร่วมมือระหว่างประเทศในรูปแบบความตกลงพหุภาคี

4.1.1 ความร่วมมือระหว่างประเทศในรูปแบบความตกลงทวิภาคี

การแก้ปัญหาการส่งผู้ร้ายข้ามแดนในกรณีอาชญากรรมคอมพิวเตอร์ ในปัจจุบัน รัฐต่างๆก็อาศัยความร่วมมือระหว่างประเทศในรูปแบบทวิภาคีซึ่งได้แก่ การบังคับใช้สนธิสัญญาทวิภาคีว่าด้วยการส่งผู้ร้ายข้ามแดนที่มีอยู่เพื่อส่งอาชญากรคอมพิวเตอร์ข้ามแดน ซึ่งได้กล่าวมาแล้วในบทที่ 3 ว่าการส่งผู้ร้ายข้ามแดนโดยอาศัยสนธิสัญญาส่งผู้ร้ายข้ามแดนที่มีอยู่ก่อให้เกิดปัญหาในทางปฏิบัติทำให้ไม่สามารถส่งผู้ร้ายข้ามแดนได้ เนื่องจากสนธิสัญญาทวิภาคีดังกล่าวมีช่องว่างในการส่งผู้ร้ายข้ามแดนในกรณีอาชญากรรมคอมพิวเตอร์ ไม่ว่าจะเป็นสนธิสัญญาประเภทการ

ระบุฐานความผิดหรือสนธิสัญญาประเภทกำหนดอัตราโทษ ที่ทำให้เกิดอุปสรรคในการส่งผู้ร้ายข้ามแดน เนื่องจากอาชญากรรมคอมพิวเตอร์เป็นความผิดฐานใหม่ที่ต้องได้รับการแก้ไขสนธิสัญญาเพื่อให้สามารถดำเนินการส่งผู้ร้ายข้ามแดนได้

4.1.1.1 กรณีสนธิสัญญาประเภทระบุฐานความผิด

ในกรณีรัฐมีสนธิสัญญาส่งผู้ร้ายข้ามแดนประเภทระบุฐานความผิดนั้น หากความผิดที่ร้องขอไม่เป็นความผิดตามสนธิสัญญาทวิภาคีแล้ว ย่อมเป็นสิทธิของรัฐผู้รับคำขอโดยเด็ดขาดที่จะพิจารณาส่งผู้ร้ายข้ามแดนให้หรือไม่ก็ได้ ดังนั้น แนวทางการแก้ไขปัญหาประการหนึ่งคือ การแก้ไขสนธิสัญญาให้ครอบคลุมถึงกรณีอาชญากรรมคอมพิวเตอร์ โดยการกำหนดให้อาชญากรรมคอมพิวเตอร์เป็นความผิดที่สามารถส่งผู้ร้ายข้ามแดนได้ตามสนธิสัญญา วิธีการแก้ไขปัญหาดังกล่าว เป็นแนวทางที่จะแก้ปัญหาช่องว่างของสนธิสัญญาส่งผู้ร้ายข้ามแดนเพื่อที่จะให้สามารถส่งผู้ร้ายข้ามแดนในความผิดฐานนี้ได้ การแก้ไขปัญหาโดยวิธีดังกล่าวเกิดขึ้นในสนธิสัญญาส่งผู้ร้ายข้ามแดนระหว่างประเทศเนปาลกับประเทศอินเดีย ที่มีการแก้ไขให้ความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์เป็นความผิดที่สามารถส่งผู้ร้ายข้ามแดนกันได้ระหว่างรัฐภาคี[1] ทั้งนี้เนื่องจากสนธิสัญญาฉบับเก่าไม่สามารถใช้กับความผิดอาญาฐานใหม่ได้ ซึ่งนอกจากสนธิสัญญาระหว่างประเทศเนปาลและอินเดียแล้วก็ยังไม่พบว่ามีประเทศใดแก้ไขสนธิสัญญาในลักษณะนี้ ซึ่งแนวทางการแก้ไขปัญหาโดยการกำหนดความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์ไว้ในสนธิสัญญาทวิภาคีเป็นแนวทางที่ทำให้สามารถนำตัวอาชญากรมาลงโทษได้โดยกระบวนการทางกฎหมายได้อย่างมีประสิทธิภาพ อย่างไรก็ตาม การแก้ไขสนธิสัญญาในลักษณะนี้ก็มีลักษณะเป็นการแก้ไขปัญหาเฉพาะหน้า ซึ่งไม่แน่ว่าต่อไปในอนาคตหากเกิดความผิดอาญาที่เกี่ยวเนื่องกับเทคโนโลยีเกิดขึ้น จะสามารถตีความให้ครอบคลุมกับความผิดฐานใหม่ได้หรือไม่

การแก้ไขสนธิสัญญาในอีกกรณีหนึ่งคือ การเปลี่ยนสนธิสัญญาประเภทระบุฐานความผิดดังกล่าวให้เป็นสนธิสัญญาประเภทระบุอัตราโทษซึ่งเป็นวิธีการที่แก้ปัญหาที่มีประสิทธิภาพมากกว่าเพียงการเพิ่มฐานความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์ลงใน

---

[1] Rekha Shrestha, "Nepal, India to revise extradition treaty," The Himalayan Times[Online],15 February 2003, Available from: http://nepalresearch.org/ht_excerpts/2003_02/ht_2003_0215.htm[2003, July 15]

สนธิสัญญากำหนดฐานความผิด[2] แต่หากจะแก้ไขสนธิสัญญาให้เป็นประเภทระบุอัตราโทษนี้ รัฐภาคีจะต้องมีความพร้อมทางด้านกฎหมายภายในเกี่ยวกับอาชญากรรมคอมพิวเตอร์ เนื่องจากการให้ความร่วมมือตามสนธิสัญญาประเภทนี้ จะต้องอาศัยกลไกของกฎหมายภายในของทั้งสองประเทศ ดังจะได้กล่าวในหัวข้อถัดไป

4.1.1.2 **กรณีสนธิสัญญาประเภทระบุอัตราโทษ**

การบังคับใช้สนธิสัญญาประเภทระบุอัตราโทษเพื่อส่งผู้ร้ายข้ามแดนนั้น โดยหลักจะต้องอาศัยกลไกทางกฎหมายภายในของทั้งสองประเทศสนับสนุนด้วยตามหลักความผิดอาญาของทั้งสองประเทศและหลักความผิดที่ส่งข้ามแดนได้ กล่าวคือ การส่งผู้ร้ายข้ามแดนตามสนธิสัญญาดังกล่าวขึ้นอยู่กับกฎหมายอาญาภายในของทั้งสองรัฐ ซึ่งต้องกำหนดให้อาชญากรรมคอมพิวเตอร์เป็นความผิดอาญาและมีอัตราโทษตามที่ระบุไว้ในสนธิสัญญา จึงจะเป็นเงื่อนไขที่ทำให้มีการส่งผู้ร้ายข้ามแดนกันได้

หลักการที่ถูกกำหนดไว้ดังกล่าวจึงกลายเป็นอุปสรรคสำคัญในการให้ความร่วมมือในการส่งผู้ร้ายข้ามแดนในกรณีอาชญากรรมคอมพิวเตอร์ ทั้งในกรณีที่รัฐใดรัฐหนึ่งยังไม่มีการพัฒนากฎหมายภายในเกี่ยวกับอาชญากรรมคอมพิวเตอร์และในกรณีที่รัฐมีกฎหมายอาชญากรรมคอมพิวเตอร์แล้วแต่มีความแตกต่างกันในเรื่องการกำหนดฐานความผิดและอัตราโทษที่จะลงแก่ผู้กระทำความผิดซึ่งทำให้ไม่เป็นไปตามหลักความผิดอาญาของทั้งสองประเทศและหลักอัตราโทษที่กำหนดในสนธิสัญญา

การแก้ไขปัญหาดังกล่าวอาจกระทำได้โดยการสร้างสนธิสัญญาที่มีความยืดหยุ่นในการบังคับใช้ จากแนวความคิดที่เป็นที่ยอมรับในการทำสนธิสัญญาระหว่างประเทศเกี่ยวกับความร่วมมือทางอาญาสมัยใหม่ มีหลักการว่า กฎหมายที่ใช้บังคับแก่การดำเนินการทั้งหลายให้ใช้กฎหมายของรัฐผู้รับคำร้องขอ แต่ก็กำหนดหลักการผ่อนคลายไว้ว่าให้รัฐผู้รับคำร้องขอดำเนินการตามที่รัฐผู้ร้องขอยื่นคำขอมา หากว่าการดำเนินการดังกล่าวไม่เป็นการขัดต่อกฎหมายภายในของรัฐผู้รับคำร้องขอ ซึ่งแนวความคิดนี้ช่วยแก้ปัญหาความแตกต่างกันของกฎหมายภายในของแต่ละ

---

[2] John T. Soma , Thomas F. Muther , Jr. and Heidi M.L. Brissette, " Transnational extradition for computer crimes : Are new treaties and laws need ?," Harvard Journal on Legislation , 34 (March 1997): 362.

ประเทศ[3] หลักดังกล่าวนี้จากการศึกษาพบว่าปรากฏอยู่ในสนธิสัญญาส่งผู้ร้ายข้ามแดนของกลุ่ม Nordic States[4] ซึ่งกำหนดให้การส่งผู้ร้ายข้ามแดนสามารถดำเนินไปได้หากปรากฏว่าความผิดที่ร้องขอเป็นความผิดที่ลงโทษได้ตามกฎหมายภายในของรัฐที่ร้องขอ โดยไม่จำต้องเป็นความผิดตามกฎหมายภายในของรัฐที่ได้รับคำร้องขอ[5]

นอกจากนี้ สนธิสัญญาเกี่ยวกับความร่วมมือทางอาญาในระยะหลังก็มีการผ่อนคลายข้อกำหนดในเรื่องความผิดอาญาของทั้งสองประเทศ (Double Criminality) อีกด้วย ซึ่งก็ถือเป็นการอาศัยหลักการเดียวกับหลักการที่กล่าวข้างต้น ดังจะเห็นได้จากสนธิสัญญาความร่วมมือระหว่างประเทศในทางอาญาระหว่างประเทศไทยและสหรัฐอเมริกา ซึ่งได้กำหนดยกเว้นหลักความผิดอาญาของทั้งสองประเทศ (Double Criminality) โดยการให้ความร่วมมือกระทำได้โดยไม่ต้องคำนึงถึงว่า การกระทำที่ร้องขอจะต้องห้ามตามกฎหมายของรัฐผู้รับคำร้องขอด้วยหรือไม่[6] ผู้เขียนเห็นว่า ตัวอย่างของข้อตกลงระหว่างประเทศดังกล่าวแม้ไม่ใช่สนธิสัญญาส่งผู้ร้ายข้ามแดน แต่เมื่อความร่วมมือในทางอาญาก็เป็นความร่วมมือชนิดหนึ่งซึ่งใช้หลักการเกี่ยวกับความผิดอาญาของทั้งสองประเทศเช่นเดียวกับการส่งผู้ร้ายข้ามแดน ดังนั้น จึงน่าจะนำหลักการดังกล่าวมาปรับใช้กับการส่งผู้ร้ายข้ามแดนได้เช่นเดียวกัน

หลักการที่ปรากฏอยู่ในสนธิสัญญาส่งผู้ร้ายข้ามแดนของกลุ่ม Nordic States และสนธิสัญญาความร่วมมือระหว่างประเทศในทางอาญาระหว่างประเทศไทยและสหรัฐอเมริกานั้น มีหลักการที่คลายคลึงกัน กล่าวคือ เป็นหลักของความร่วมมือทางอาญาสมัยใหม่ที่ยกเว้นหลักความผิดอาญาของทั้งสองประเทศ (Double Criminality) โดยการนำหลักการดังกล่าวมาบังคับใช้ก่อให้เกิดผลดีคือ ทำให้การส่งผู้ร้ายข้ามแดนดำเนินไปได้โดยสะดวก เนื่องจากเป็นการขจัดปัญหาที่สืบเนื่องมาจากความแตกต่างและความเหลื่อมล้ำของกฎหมายภายในของทั้งสองประเทศ ซึ่ง

---

[3] สุชาติ ไตรประสิทธิ์, "ความร่วมมือระหว่างประเทศทางอาญากับความมั่นคงแห่งชาติ," (เอกสารวิจัยส่วนบุคคล วิทยาลัยป้องกันราชอาณาจักร รุ่นที่ 33 ประจำปีการศึกษา พ.ศ.2533-2534), หน้า 28.

[4] The Nordic Extradition Treaty of 1962 ประกอบด้วยประเทศ เดนมาร์ก ฟินแลนด์ ไอซ์แลนด์ นอร์เวย์และสวีเดน อ้างถึงใน I.A. Shearer, Extradition in international law (Manchester: Oceana Publication Inc.,1971), pp.63-64.

[5] Ibid.

[6] สนธิสัญญาความร่วมมือทางอาญาระหว่างประเทศไทยและสหรัฐอเมริกา ข้อ 1(3)

เป็นอุปสรรคสำคัญที่ทำให้ไม่สามารถส่งผู้ร้ายข้ามแดนให้แก่กันได้[7] แต่เมื่อพิจารณาถึงผลเสียของการกำหนดความตกลงระหว่างประเทศโดยยกเว้นหลักความผิดอาญาของทั้งสองประเทศแล้ว ก็อาจกล่าวได้ว่า การส่งผู้ร้ายข้ามแดนโดยปราศจากหลักเกณฑ์ดังกล่าว ในทางทฤษฎีจะมีผลกระทบต่อสิทธิของจำเลยที่จะไม่ถูกลงโทษโดยผลของการกระทำที่ไม่เป็นความผิดอาญาตามกฎหมายภายในของรับผู้รับคำขอ

อย่างไรก็ตาม เมื่อพิเคราะห์ถึงผลดีและผลเสียดังกล่าวทั้งหมดแล้ว ผู้เขียนเห็นว่า ในกรณีของอาชญากรรมคอมพิวเตอร์ ซึ่งในปัจจุบันประเทศส่วนใหญ่กำหนดให้เป็นความผิดอาญาตามกฎหมายภายในแล้ว ทั้งยังได้รับการยอมรับในทางระหว่างประเทศว่าเป็นความผิดที่ทุกประเทศควรกำหนดให้เป็นความผิดอาญา[8] ดังนั้น หากจะนำแนวคิดในการผ่อนคลายหรือยกเว้นหลักความผิดอาญาของทั้งสองประเทศมาใช้กับสนธิสัญญาส่งผู้ร้ายข้ามแดนในคดีอาชญากรรมคอมพิวเตอร์ ก็ไม่น่าที่จะส่งผลกระทบต่อสิทธิของจำเลยดังที่ได้กล่าวมาแล้วมากนัก แต่กลับจะก่อให้เกิดผลดีในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ เนื่องจากหลักการดังกล่าวทำให้เกิดความสะดวกในการส่งผู้ร้ายข้ามแดนอย่างมาก โดยจะทำให้ความเหลื่อมล้ำและความแตกต่างของกฎหมายของทั้งสองประเทศไม่เป็นอุปสรรคอีกต่อไป ซึ่งย่อมจะทำให้การส่งผู้ร้ายข้ามแดนในคดีอาชญากรรมคอมพิวเตอร์เป็นไปได้อย่างมีประสิทธิภาพ

4.1.2 ความร่วมมือระหว่างประเทศในรูปแบบความตกลงพหุภาคี

จากความรุนแรงของปัญหาอาชญากรรมคอมพิวเตอร์ ประกอบกับปัญหาในทางปฏิบัติในการให้ความร่วมมือระหว่างประเทศในการส่งผู้ร้ายข้ามแดน ทำให้ประเทศต่างๆให้ความสำคัญของการจัดทำความร่วมมือระหว่างประเทศแบบพหุภาคี ซึ่งจะเป็นแนวทางที่ทำให้สามารถนำตัวผู้กระทำความผิดมาลงโทษได้อย่างมีประสิทธิภาพ แต่การจัดทำความร่วมมือระหว่างประเทศแบบพหุภาคีที่จะให้ผลในการแก้ปัญหาได้นั้น จะต้องเป็นความร่วมมือที่ประกอบด้วยประเทศสมาชิกที่มีจำนวนไม่น้อยจนเกินไป เนื่องจากปัญหาอาชญากรรมคอมพิวเตอร์เป็นปัญหาที่แพร่กระจายไปทั่วโลก มิใช่ปัญหาของประเทศหนึ่งประเทศใดเพียงประเทศเดียว ความร่วมมือพหุภาคีที่มีจำนวนสมาชิกน้อยจึงไม่ช่วยแก้ปัญหาได้ ดังนั้น หากการ

---

[7] สุชาติ ไตรประสิทธิ์, "ความร่วมมือระหว่างประเทศทางอาญากับความมั่นคงแห่งชาติ," หน้า 24.

[8] United Nations, Economic and Social Council, "Effective measures to prevent and control computer-related crime," 29 January 2002 (Document E/CN.15/2002/8)

จัดทำความร่วมมือดังกล่าวได้รับการสนับสนุนโดยองค์การระหว่างประเทศในระดับโลก ย่อมทำให้การแก้ไขปัญหาประสบผลสำเร็จ ในปัจจุบัน องค์การระหว่างประเทศที่มีบทบาทในการแก้ไขปัญหาคือ องค์การสหประชาชาติและ Council of Europe ซึ่งจะได้กล่าวในรายละเอียดดังต่อไปนี้

4.1.2.1 องค์การสหประชาชาติ

องค์การสหประชาชาติเริ่มมีบทบาทในการประสานความร่วมมือระหว่างประเทศในการแก้ไขปัญหาอาชญากรรมคอมพิวเตอร์มาตั้งแต่ปี ค.ศ.1985 โดยในการประชุมสหประชาชาติครั้งที่ 8 ว่าด้วยการป้องกันอาชญากรรมและการปฏิบัติต่อผู้กระทำความผิด ในปี ค.ศ. 1990 ประเทศแคนาดาได้เสนอให้มีการร่างข้อมติเกี่ยวกับปัญหาอาชญากรรมคอมพิวเตอร์ โดยมีเสียงสนับสนุนจากรัฐสมาชิกกว่า 21 ประเทศ และที่ประชุมก็ได้มีมติกำหนดมาตรการที่มิใช่บทบังคับทางกฎหมายให้รัฐสมาชิกสหประชาชาติพัฒนากฎหมายอาญาและกฎหมายวิธีพิจารณาความเพื่อให้แน่ใจว่า กฎหมายภายในที่มีอยู่สามารถบังคับใช้กับปัญหาอาชญากรรมคอมพิวเตอร์ได้ นอกจากนี้ ในกรณีที่ปรากฏว่าไม่มีกฎหมายภายในหรือกฎหมายภายในที่มีอยู่ไม่เพียงพอและไม่สามารถใช้บังคับกับอาชญากรรมคอมพิวเตอร์ได้นั้น รัฐสมาชิกจำต้องกำหนดฐานความผิด การสืบสวนสอบสวน และวิธีการเกี่ยวกับระบบพยานหลักฐานเกี่ยวกับคอมพิวเตอร์ในกรณีที่จำเป็นเพื่อความร่วมมือระหว่างประเทศในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์อย่างมีประสิทธิภาพ[9]

เป็นที่สังเกตได้ว่า ข้อมติจากการประชุมในครั้งนี้ เป็นเพียงการหารือเพื่อรับรองว่าปัญหาอาชญากรรมคอมพิวเตอร์เป็นปัญหาที่ควรได้รับการแก้ไข พร้อมทั้งยังกำหนดแนวทางกว้างๆในการแก้ไขปัญหา รวมถึงสมัชชาใหญ่แห่งองค์การสหประชาชาติยังมีเรียกร้องให้ประเทศภาคีให้ความร่วมมือในการพัฒนากฎหมายภายในให้ครอบคลุมถึงอาชญากรรมคอมพิวเตอร์ อย่างไรก็ตาม องค์การสหประชาชาติก็ยังไม่มีการกำหนดถึงคำนิยามและฐานความผิด รวมถึงองค์ประกอบความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์ที่ชัดเจน [10]

---

[9] United Nations, International review of criminal policy, Nos 43 and 44, 1994 (United Nations publication, Sales No. E.94IV.5) [Online],(n.d.), Available from: http://www.uncjin.org/documents/irpo4344.pdf[2003, April 29]

[10] Ibid.

ต่อมา ในการประชุมสหประชาชาติ ครั้งที่ 10 ว่าด้วยการป้องกันอาชญากรรมและการปฏิบัติต่อผู้กระทำความผิด (Tenth United Nations Congress on the prevention of crime and the treatment of offenders) ณ กรุงเวียนนา เมื่อวันที่ 10-17 เมษายน ค.ศ.2000 ได้มีการจัดให้อาชญากรรมคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตเป็น 1 ใน 4 วาระการประชุมหลักในการประชุมครั้งนี้ ซึ่งในการประชุมดังกล่าว รัฐภาคีต่างเห็นพ้องกันว่า การกระทำความผิดโดยใช้คอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตเป็นการกระทำที่ทุกประเทศควรกำหนดให้เป็นความผิดอาญา โดยกำหนดเป็นความผิดอาญาฐานใหม่ เนื่องจากโดยส่วนใหญ่แล้ว หลายประเทศประสบปัญหาการไม่สามารถใช้กฎหมายอาญาดั้งเดิมกับข้อมูลคอมพิวเตอร์ได้ ทำให้รัฐทั้งหลายเห็นพ้องในการที่จะต้องร่วมกันสร้างกฎหมายอาชญากรรมคอมพิวเตอร์ให้มีความสอดคล้องเป็นอันหนึ่งอันเดียวกันเพื่อความสะดวกในการให้ความร่วมมือระหว่างประเทศและการส่งผู้ร้ายข้ามแดน อย่างไรก็ตาม ประเด็นปัญหาเกี่ยวกับเขตอำนาจเหนือคดีอาชญากรรมคอมพิวเตอร์ยังเป็นที่ถกเถียง กล่าวคือ รัฐใดจะเป็นผู้ใช้เขตอำนาจเหนือคดี ซึ่งหากถือตามหลักสถานที่ที่ความผิดเกิด (Determination of Place) แล้ว ก็อาจเกิดความไม่ชัดเจน เนื่องจากการกระทำผิดผ่านเครือข่ายอินเทอร์เน็ตอาจทำให้ผลของการกระทำนั้นเกิดขึ้นได้ในหลายประเทศ[11]

จากการประชุมเพื่อหาแนวทางในการแก้ปัญหา ในที่สุดองค์การสหประชาชาติก็ได้จัดทำ United Nations Manual on the Prevention and Control of Computer-Related Crime ซึ่งคู่มือฉบับนี้จัดทำขึ้นโดยมีวัตถุประสงค์เพื่อให้รัฐภาคีสมาชิกสหประชาชาติใช้เป็นแนวทางในการพัฒนากฎหมายภายในให้มีความสอดคล้องกัน รวมถึงในเรื่องของการให้ความร่วมมือระหว่างประเทศ ซึ่งเอกสารดังกล่าวมีเนื้อหาครอบคลุมถึงนิยามและประเภทความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ต โดยเน้นย้ำว่าไม่เพียงแต่มาตรการทางกฎหมายภายในเท่านั้น แต่ยังต้องดำเนินมาตรการด้านความร่วมมือระหว่างประเทศควบคู่กันไป จึงจะทำให้การป้องกันและควบคุมอาชญากรรมคอมพิวเตอร์ประสพผลสำเร็จในทางปฏิบัติ เพื่อเป็นการส่งเสริมและสนับสนุนให้รัฐภาคีสมาชิกสหประชาชาติบัญญัติกฎหมายภายในเกี่ยวกับอาชญากรรมคอมพิวเตอร์ให้เป็นไปในแนวทางเดียวกัน ซึ่งจะนำไปสู่การให้ความร่วมมือระหว่าง

---

[11] United Nations, "Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders," Report of Committee II, Vienna, 10-17 April 2000. (Document A/CONF. 187/L.10). p. 2-3.

ประเทศรวมถึงการส่งผู้ร้ายข้ามแดนเป็นไปได้โดยสะดวกและไม่ขัดต่อหลักความผิดอาญาของทั้งสองประเทศ (Double Criminality)[12]

อย่างไรก็ตาม จะเห็นได้ว่ามาตรการดังกล่าวของสหประชาชาติเป็นมาตรการที่ส่งเสริมให้รัฐภาคีบัญญัติกฎหมายภายในให้สอดคล้องกัน เพื่อให้เกิดความสะดวกในการส่งผู้ร้ายข้ามแดนตามหลักความผิดอาญาของทั้งสองประเทศ ซึ่งมาตรการดังกล่าวนั้นก็เป็นเพียงมาตรการชี้แนะให้ประเทศต่างๆถือปฏิบัติ เนื่องจากในปัจจุบันองค์การสหประชาชาติก็ยังไม่มีกฎเกณฑ์ในรูปแบบของกฎหมายเพื่อแก้ปัญหาอาชญากรรมคอมพิวเตอร์ ดังนั้น หากรัฐต่างๆไม่ดำเนินการตามมาตรการดังกล่าว ความพยายามในการแก้ปัญหาก็ย่อมไม่เป็นผล ซึ่งจากการศึกษาในบทที่ 3 ทำให้ทราบว่ารัฐต่างๆมีกฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์แตกต่างกันเนื่องจากสภาพทางสังคม เศรษฐกิจ และวัฒนธรรมของประเทศต่างๆมีความแตกต่างกัน ความไม่สอดคล้องของกฎหมายดังกล่าว ทำให้การส่งผู้ร้ายข้ามแดนไม่อาจดำเนินไปได้ เนื่องจากขัดต่อหลักความผิดอาญาของทั้งสองประเทศ (Double Criminality) ปัญหาดังกล่าวเป็นปัญหาที่ไม่อาจแก้ไขได้ในระดับรัฐใดรัฐหนึ่งหรือเพียงกลุ่มใดกลุ่มหนึ่งหากแต่ต้องแก้ปัญหาแบบสากล จึงทำให้หลายฝ่ายมีความเห็นว่า ควรมีการจัดทำอนุสัญญาระหว่างประเทศเพื่อกำหนดการกระทำที่เป็นความผิดอาญา รวมถึงการกำหนดแนวทางในการให้ความร่วมมือระหว่างในทางอาญาและการส่งผู้ร้ายข้ามแดนให้ชัดเจน[13] ซึ่งไม่เพียงแต่จะขจัดความไม่สอดคล้องและความเหลื่อมล้ำของมาตรฐานทางกฎหมายของแต่ละประเทศแล้ว ยังสามารถกำหนดหลักเกณฑ์การให้ความร่วมมือในการส่งผู้ร้ายข้ามแดนที่ชัดเจนและเหมาะสมกับกรณีของอาชญากรรมคอมพิวเตอร์ อย่างไรก็ตาม ในทางปฏิบัติอนุสัญญาพหุภาคีเกิดขึ้นได้ยากเนื่องจากภาคีสมาชิกสหประชาชาติที่มีจำนวนมากย่อมก่อให้เกิดอุปสรรคในการเจรจาเพื่อร่างอนุสัญญาให้เป็นไปในทิศทางเดียวกันและสมประโยชน์ของทุกฝ่าย

---

[12] United Nations, International review of criminal policy, Nos 43 and 44, 1994 (United Nations publication, Sales No. E.94IV.5) [Online],(n.d.), Available from: http://www.uncjin.org/documents/irpo4344.pdf[2003, April 29]

[13] Abraham D. Sofaer, Chapter 6 : Toward an international convention on cyber security[Online],(n.d.), Available from: http://www.hoover.stanford.edu/publications/books/fulltext/cybercrime/221.pdf[2003, April 29]

นอกจากแนวทางในการแก้ปัญหาโดยการจัดทำอนุสัญญาระหว่างประเทศแล้ว อีกแนวทางหนึ่งที่ได้รับการเสนอขึ้นเพื่อแก้ปัญหาคือ การจัดทำกฎหมายแม่แบบ หรือ Model Law เกี่ยวกับอาชญากรรมคอมพิวเตอร์[14] จากการศึกษาพบว่า ในอดีตองค์การสหประชาชาติเคยจัดทำกฎหมายแม่แบบว่าด้วยการพาณิชย์อิเล็กทรอนิกส์ หรือ Model Law on Electronic Commerce 1996 โดยมุ่งหมายในการกำหนดหลักเกณฑ์ที่สำคัญที่ประเทศต่างๆนำไปใช้เป็นแนวทางในการตราหรือแก้ไขกฎหมายของตน เพื่อให้กฎหมายของประชาคมโลกเกี่ยวกับการพาณิชย์อิเล็กทรอนิกส์เป็นไปในทิศทางเดียวกัน[15] ทั้งยังกำหนดหลักเกณฑ์สำคัญประการอื่นๆ เช่น การกำหนดข้อสันนิษฐานเกี่ยวกับสถานที่ที่สัญญาเกิด เขตอำนาจศาล เป็นต้น ซึ่งในปัจจุบันหลักการในกฎหมายแม่แบบก็ได้รับการยอมรับจากประเทศต่างๆนำไปบัญญัติเป็นกฎหมายภายในและบังคับใช้หลักดังกล่าวเป็นมาตรฐานระหว่างประเทศเกี่ยวกับการพาณิชย์อิเล็กทรอนิกส์[16] ผู้เขียนเห็นว่า การกำหนดหลักเกณฑ์ต่างๆเกี่ยวกับการกระทำผ่านเครือข่ายอินเทอร์เน็ตในทางอาญา ก็สามารถทำได้เช่นเดียวกับในทางแพ่ง ซึ่งจะทำให้เกิดความชัดเจนแน่นอนมากยิ่งขึ้น

ไม่ว่าแนวทางการแก้ปัญหาที่เป็นรูปธรรมจะกระทำโดยการจัดทำเป็นสนธิสัญญาพหุภาคีหรือการจัดทำสนธิสัญญาแม่แบบของสหประชาชาติ ต่างเป็นความร่วมมือระหว่างประเทศในการสร้างมาตรฐานร่วมกันเพื่อกำหนดการกระทำที่เป็นความผิดอาญา และความร่วมมือระหว่างประเทศให้เป็นไปทิศทางเดียวกัน กล่าวคือ ในประการแรก การจัดทำกฎหมายแม่แบบหรืออนุสัญญาระหว่างประเทศทำให้สามารถกำหนดคำนิยาม ประเภทความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์ได้ชัดเจนและเป็นแนวทางเดียวกันเพื่อให้ประเทศต่างนำไปบัญญัติเป็นกฎหมายภายใน ซึ่งจะช่วยแก้ปัญหาความไม่สอดคล้องกันของกฎหมายภายในของประเทศต่างๆอันเป็นอุปสรรคในการส่งผู้ร้ายข้ามแดนสืบเนื่องจากหลักความผิดอาญาของทั้งสองประเทศ ประการ

---

[14] United Nations, Challenge of Borderless "Cyber-Crime" to International Efforts to Combat Transnational Organized Crime Discussed at Symposium[Online],(n.d.), Available from: http://www.unis.unvienna.org/en/news/2000/pressrels/LPMO10E.html [2003, july 13]

[15] อภิชัย ทองประสม, "สัญญาทางพาณิชย์อิเล็กทรอนิกส์," (วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2544), หน้า 20.

[16] Michael Power, Joan Remsu and John Gregory, Electronic Commerce-Overview[Online],September 1998, Available from: http://www.law.ualberta.ca/alri/ulc/current/eee98il.htm [2003, July 10]

ต่อมาคือกฎหมายแม่แบบหรือสนธิสัญญาระหว่างประเทศสามารถแก้ปัญหาเรื่องเขตอำนาจศาลที่ยังไม่มีความชัดเจนแน่นอนในปัจจุบัน โดยการกำหนดเรื่องการพิจารณาสถานที่ที่การกระทำความผิดเกิดและเขตอำนาจศาลให้ชัดเจนแน่นอน เพื่อให้รัฐต่างๆสามารถกำหนดเขตอำนาจศาลเหนืออาชญากรรมคอมพิวเตอร์ไปในทิศทางเดียวกัน ในประการสุดท้าย การจัดทำกฎหมายแม่แบบหรือสนธิสัญญาระหว่างประเทศสามารถกำหนดบทบัญญัติเกี่ยวกับการให้ความร่วมมือในทางอาญาและการส่งผู้ร้ายข้ามแดนที่สนองรับต่ออาชญากรรมคอมพิวเตอร์โดยเฉพาะ ซึ่งย่อมจะทำให้การส่งผู้ร้ายข้ามแดนในกรณีอาชญากรรมคอมพิวเตอร์ไม่ประสบปัญหาอีกต่อไป

แม้ว่าการจัดทำความร่วมมือระหว่างประเทศทั้งสองรูปแบบจะสามารถกำหนดบทบัญญัติเกี่ยวกับลักษณะความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์และกฎเกณฑ์ว่าด้วยการส่งผู้ร้ายข้ามแดนที่สนองรับต่อกรณีของอาชญากรรมคอมพิวเตอร์ที่มีความชัดเจนได้เหมือนกัน แต่การจัดทำความร่วมมือระหว่างประเทศในรูปอนุสัญญาและกฎหมายแม่แบบให้ผลในเรื่องของความผูกพันหรือพันธกรณีระหว่างประเทศที่แตกต่างกัน กล่าวคือ การจัดทำในรูปกฎหมายแม่แบบนั้น แม้เกิดขึ้นได้ง่ายแต่ต้องอาศัยความร่วมมือจากรัฐต่างๆในการรับเอากฎหมายไปบัญญัติไว้เป็นกฎหมายภายในของตน ซึ่งหากกฎหมายไม่เป็นที่ยอมรับ และไม่มีการรับเอาไปปฏิบัติ ความพยายามในการแก้ปัญหาก็จะไม่เกิดผล นอกจากนี้ กฎหมายแม่แบบจะไม่ทำให้เกิดพันธกรณีระหว่างประเทศที่ทำให้รัฐต้องให้ความร่วมมือในการส่งผู้ร้ายข้ามแดนแก่กัน จึงยังคงเป็นสิทธิโดยเด็ดขาดของรัฐที่จะให้ความร่วมมือแก่รัฐอื่นหรือไม่ก็ได้ เว้นแต่มีสนธิสัญญาทวิภาคีระหว่างกัน แต่หากความร่วมมือระหว่างประเทศจัดทำในรูปแบบของอนุสัญญาระหว่างประเทศย่อมก่อให้เกิดผลผูกพันรัฐภาคีแห่งอนุสัญญา ที่จะต้องบัญญัติกฎหมายภายในของตนให้เป็นไปตามอนุสัญญา รวมถึงพันธกรณีระหว่างประเทศที่ต้องให้ความร่วมมือในการส่งผู้ร้ายข้ามแดนแก่กันเมื่อรัฐภาคีอื่นร้องขอ ซึ่งย่อมจะทำให้การให้ความร่วมมือชัดเจนแน่นอนและประสบผลสำเร็จมากกว่า

อย่างไรก็ตาม แม้ว่าสนธิสัญญาจะมีผลดีในการสร้างพันธกรณีระหว่างประเทศมากกว่ากฎหมายแม่แบบ แต่ในทางปฏิบัติก็ไม่อาจปฏิเสธได้ว่า สนธิสัญญานั้นเกิดขึ้นได้ยาก ดังนั้น ในสภาวการณ์ที่ปัญหาอาชญากรรมคอมพิวเตอร์มีความรุนแรงและจำเป็นต้องมีมาตรการระหว่างประเทศมาใช้บังคับ การจัดทำกฎหมายแม่แบบจึงอาจเป็นแนวทางที่สามารถนำมาใช้แก้ไขปัญหาได้อย่างทันท่วงที แต่ทั้งนี้กฎหมายแม่แบบนั้น ต้องเป็นที่ยอมรับของนานาประเทศด้วย จึงจะทำให้การแก้ไขปัญหาเป็นไปได้อย่างมีประสิทธิภาพ

ประเด็นที่ควรพิจารณาอีกประการหนึ่งคือ เมื่อในปัจจุบันยังคงไม่มีกฎเกณฑ์สำหรับอาชญากรรมคอมพิวเตอร์โดยเฉพาะภายใต้กรอบองค์การสหประชาชาติ การแก้ปัญหาการส่งผู้ร้ายข้ามแดนในกรณีอาชญากรรมคอมพิวเตอร์สามารถนำอนุสัญญาระหว่างประเทศของสหประชาชาติว่าด้วยองค์กรอาชญากรรมข้ามชาติมาปรับใช้ในกรณีของอาชญากรรมคอมพิวเตอร์ซึ่งถือเป็นอาชญากรรมข้ามชาติได้หรือไม่ คำตอบคือในกรณีที่องค์กรอาชญากรรมใช้เครือข่ายอินเทอร์เน็ตในการกระทำความผิดตามอนุสัญญาฯ[17] หรือในกรณีที่การก่ออาชญากรรมคอมพิวเตอร์เป็นความผิดร้ายแรงที่มีลักษณะเป็นความผิดข้ามชาติและเกี่ยวข้องกับกลุ่มองค์กรอาชญากรรม ย่อมอยู่ในขอบเขตการบังคับใช้ของอนุสัญญาฉบับนี้เช่นกัน ซึ่งอนุสัญญาฯ กำหนดให้มีการส่งผู้ร้ายข้ามแดนกันระหว่างรัฐภาคีโดยพิจารณาจากความผิดมูลฐาน 4 ฐานที่ได้กำหนดในอนุสัญญาฯ หรือการกระทำความผิดอาญาร้ายแรงใดๆซึ่งเกี่ยวข้องกับกลุ่มอาชญากรที่มีการจัดตั้งในลักษณะองค์กร โดยบุคคลที่ถูกร้องขอให้มีการส่งผู้ร้ายข้ามแดนได้กระทำความผิดที่สามารถลงโทษได้ตามกฎหมายภายในของทั้งสองรัฐ[18] บทบัญญัติของอนุสัญญาดังกล่าวเป็นบทบัญญัติที่ส่งเสริมการส่งผู้ร้ายข้ามแดนที่มีอยู่แล้วในหลายๆภูมิภาคหรือระดับทวิภาคี ดังนั้นความสำคัญของบทบัญญัติดังกล่าวจึงเป็นการคาดหวังให้รัฐภาคีขยายความร่วมมือในการส่งผู้ร้ายข้ามแดนให้มีขอบเขตกว้างขึ้นกว่าที่เป็นอยู่[19]

อย่างไรก็ตาม แม้อาชญากรรมคอมพิวเตอร์จะเป็นอาชญากรรมข้ามชาติแต่มิใช่อาชญากรรมที่เกี่ยวข้องกับองค์กรอาชญากรรมเสมอไป ซึ่งในกรณีที่อาชญากรรมคอมพิวเตอร์กระทำโดยบุคคลที่มิได้เกี่ยวข้องกับองค์กรอาชญากรรมก็ไม่อยู่ภายใต้ขอบเขตการบังคับใช้ของ

---

[17] อนุสัญญาฯมีขอบเขตการบังคับใช้กับการกระทำความผิดมูลฐานที่มีลักษณะพิเศษ 4 กรณี (ได้แก่ การมีส่วนร่วมในองค์กรอาชญากรรม, การฟอกเงิน, การฉ้อราษฎรบังหลวง และการขัดขวางกระบวนการยุติธรรม) และการกระทำความผิดอาญาร้ายแรงที่มีลักษณะเป็นการข้ามชาติและเกี่ยวข้องกับกลุ่มอาชญากรที่มีการจัดตั้งในลักษณะขององค์กรอาชญากรรม (ข้อ 3 อนุสัญญาฯ)

[18] อนุสัญญาฯ ข้อ 16

[19] สถาบันกฎหมายอาญา สำนักงานอัยการสูงสุด, "รายงานการศึกษาวิจัยเรื่อง การพัฒนากฎหมายป้องกันและปราบปรามองค์กรอาชญากรรมข้ามชาติ," 6 ธันวาคม 2544.

อนุสัญญาฯฉบับนี้[20] ซึ่งก็มีผลทำให้ไม่สามารถนำเรื่องความร่วมมือระหว่างประเทศในการส่งผู้ร้ายข้ามแดนตามอนุสัญญาฯมาบังคับใช้ได้ การจัดการกับอาชญากรคอมพิวเตอร์ที่มิได้เกี่ยวข้องกับกลุ่มองค์กรอาชญากรรมจึงยังคงต้องอาศัยอนุสัญญาเฉพาะเกี่ยวกับอาชญากรรมคอมพิวเตอร์เพื่อสามารถแก้ไขปัญหาดังกล่าวได้อย่างมีประสิทธิภาพ[21]

แนวคิดในการสร้างมาตรฐานร่วมกันภายใต้องค์กรระดับโลกดังเช่นองค์การสหประชาชาติ จะทำให้กฎเกณฑ์ที่ถูกจัดทำขึ้นมีความเป็นสากลอย่างแท้จริงเนื่องจากเป็นกฎเกณฑ์กลางที่ใช้ได้กับทุกประเทศทั่วโลก มิใช่เพียงกฎเกณฑ์ในระดับภูมิภาคหรือเฉพาะกลุ่มประเทศใดประเทศหนึ่ง นอกจากนี้ ความเป็นองค์กรระดับโลกขององค์การสหประชาชาติที่มีสมาชิกมากมายนั้น ทำให้เกิดผลดีต่อความร่วมมือระหว่างประเทศเกี่ยวกับการส่งผู้ร้ายข้ามแดนอย่างดียิ่ง เนื่องจากหากทุกประเทศล้วนมีกฎหมายที่เอื้อต่อการให้ความร่วมมือในการส่งผู้ร้ายข้ามแดนแก่กันและกันแล้ว จะไม่มีสถานที่ใดที่อาชญากรจะใช้เป็นที่อาศัยในการหลบเลี่ยงการลงโทษจากการกระทำความผิดได้ดังเช่นที่เป็นอยู่ในปัจจุบัน

4.1.2.2 Council of Europe

นอกจากความพยายามในการสร้างความร่วมมือระหว่างประเทศในกรณีอาชญากรรมคอมพิวเตอร์ภายใต้เวทีของสหประชาชาติแล้ว ยังมีกรอบความร่วมมือส่วนภูมิภาคของกลุ่มสหภาพยุโรป ซึ่งได้มีแนวทางในการแก้ปัญหาดังกล่าวอย่างเป็นรูปธรรมแล้วโดยการจัดทำเป็นอนุสัญญาว่าด้วยอาชญากรรมคอมพิวเตอร์โดยเฉพาะ

อนุสัญญาคณะกรรมการยุโรปว่าด้วยอาชญากรรมคอมพิวเตอร์ หรือ Convention on Cybercrime เป็นอนุสัญญาเกี่ยวกับอาชญากรรมคอมพิวเตอร์ฉบับแรก โดยมีประเทศในกลุ่มสหภาพยุโรป สหรัฐอเมริกา แคนาดา ญี่ปุ่น และแอฟริกาใต้เข้าร่วมเป็นภาคีแห่งอนุสัญญา แม้อนุสัญญาฉบับนี้จะเป็นอนุสัญญาในระดับภูมิภาค แต่มีความสำคัญที่ควรศึกษาเนื่องจากการเป็นอนุสัญญาเฉพาะเกี่ยวกับอาชญากรรมคอมพิวเตอร์ฉบับเดียวของโลก และมีประเทศพัฒนาแล้วที่ไม่ใช่ประเทศสมาชิกของสหภาพยุโรปหลายประเทศเข้าร่วมเป็นภาคี อนุสัญญาดังกล่าวไม่เพียง

---

[20] United Nations, Transnational computer crime: The crime of tomorrow are on our doorstep[Online],(n.d.), Available from: http://www.unodc.org/palermo/cybercrime.htm [2003, July 9]

[21] Ibid.

วางกรอบในการกำหนดฐานความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์เพื่อให้รัฐภาคีรับเอาไปบัญญัติไว้เป็นกฎหมายภายในของตนให้เป็นไปในทิศทางเดียวกัน แต่ยังมีบทบัญญัติที่กำหนดหลักเกณฑ์เกี่ยวกับเขตอำนาจศาลเหนือคดีอาชญากรรมคอมพิวเตอร์รวมถึงการให้ความร่วมมือทางอาญาและการส่งผู้ร้ายข้ามแดนด้วย

อนุสัญญาแห่งสภายุโรปว่าด้วยอาชญากรรมคอมพิวเตอร์ เป็นอนุสัญญาแรกที่ถือกำเนิดขึ้นเพื่อแก้ปัญหาการแพร่กระจายของอาชญากรรมคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ต เมื่อคณะกรรมการผู้เชี่ยวชาญเกี่ยวกับอาชญากรรมบนเครือข่ายอินเทอร์เน็ต (The Committee of Experts on Crime in Cyber - Space (PC-CY)) เป็นคณะกรรมการที่ถูกจัดตั้งขึ้นเพื่อร่างอนุสัญญา ในปี ค.ศ. 1997 กระบวนการจัดทำอนุสัญญาเสร็จสิ้น เมื่อเดือนกรกฎาคม ค.ศ. 2000 และเข้าสู่การพิจารณาของคณะกรรมการยุโรปว่าด้วยปัญหาอาชญากรรม (The European Committee on Crime Problems (CDPC)) ซึ่งร่างอนุสัญญาได้รับการเห็นชอบจาก CDPC เมื่อเดือนมิถุนายน ค.ศ. 2001[22]

ในส่วนของการกำหนดคำนิยามและฐานความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์บัญญัติอยู่ใน บทที่ 2 มาตรา 2-13 เพื่อให้เป็นแนวทางในการบัญญัติกฎหมายภายในของแต่ละรัฐภาคี ให้มีแนวทางและมาตรฐานแบบเดียวกัน ส่งผลให้เกิดความสะดวกในการให้ความร่วมมือระหว่างประเทศ เช่น การส่งผู้ร้ายข้ามแดนระหว่างรัฐภาคี โดยครอบคลุมความผิดดังต่อไปนี้[23]

1. การเข้าถึงระบบข้อมูลหรือระบบคอมพิวเตอร์ โดยไม่มีอำนาจ (Illegal Access) หรือเป็นการโจมตี (Attack) ระบบข้อมูลหรือระบบคอมพิวเตอร์ที่มีการวางระบบรักษาความปลอดภัยไว้ เช่น การบุกรุกระบบคอมพิวเตอร์ หรือการ Hacking หรือ Cracking โดยการกระทำดังกล่าวนี้ถือเป็นความผิดในตัวเอง โดยไม่ต้องมีการกระทำความผิดฐานอื่นในระบบอีก เนื่องจากการกระทำ

---

[22] Cedric J. Magnin, "The 2001 Council of Europe Convention on Cyber-crime : an efficient tool to fight crime in cyber-space?," (LLM. dissertation, Santa Clara University, 2001), p. 42-43.

[23] European Committee on Crime Problem, Final activity report : Draft Convention on Cyber-crime and explanatory memorandum related thereto[Online], 29 June 2001, Available from : http://www.privacyinternational.org/issues/cybercrime/coe/cybercrimememo-final.html [2002, Jan 10], p.7-12.

ดังกล่าว อาจทำให้เกิดความขัดข้องในการทำงานของระบบคอมพิวเตอร์ และอาจเป็นการขัดขวางการทำงานของผู้มีอำนาจเข้าถึงระบบนั้น นอกจากนี้ยังทำให้ผู้กระทำความผิดได้รับรู้ข้อมูลที่เป็นความลับจากการเข้าถึงระบบโดยมิชอบอีกด้วย (มาตรา 2)

2. การดักสกัดข้อมูลโดยไม่มีอำนาจ (Illegal Interception) มาตรานี้บัญญัติเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวในการส่งข้อมูลผ่านเครือข่ายอินเทอร์เน็ต (เช่นเดียวกับ การกระทำการดักฟังโทรศัพท์แบบดั้งเดิม) สิทธิในความเป็นส่วนตัวนี้ ยังเป็นสิทธิที่ได้รับความคุ้มครองตามมาตรา 8 อนุสัญญายุโรปว่าด้วยสิทธิมนุษยชน (European Convention on Human Rights) อีกด้วย (มาตรา 3)

3. การแทรกแซงข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาต (Data Interference) เพื่อป้องกันการกระทำที่ก่อให้เกิดความเสียหายของข้อมูลคอมพิวเตอร์ การแทรกแซงนี้หมายถึง การกระทำที่เป็นผลทำให้ข้อมูลคอมพิวเตอร์ลบ หรือถูกทำลาย รวมถึงการแก้ไขเปลี่ยนแปลงข้อมูลที่ถูกบันทึกเก็บไว้ เช่น การปล่อยไวรัสเพื่อทำลาย, การใช้โปรแกรมม้าโทรจัน (Trojan Horse) เป็นต้น (มาตรา 4)

4. การแทรกแซงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต (System Interference) คือ การกระทำที่ก่อให้เกิดความเสียหายแก่ระบบคอมพิวเตอร์ โดยการทำให้ระบบทำงานผิดปกติ หรือขัดข้อง (มาตรา 5)

5. การนำสิ่งที่ได้จากคอมพิวเตอร์ไปใช้ในทางที่ผิด (Misuse of Devices) การกระทำความผิดตามมาตรา 2-5 ซึ่งเป็นผลให้ผู้กระทำได้ไปซึ่งข้อมูลหรือโปรแกรมคอมพิวเตอร์ ซึ่งผู้ครอบครองอาจนำข้อมูลอันเป็นความลับไปใช้เพื่อแสวงประโยชน์ ดังนั้น มาตรานี้จึงกำหนดให้การขาย การจัดหาให้ได้มา การนำเข้า เผยแพร่ ข้อมูลหรือโปรแกรมดังกล่าวเป็นความผิด ยกตัวอย่างเช่น การขาย เผยแพร่ จัดหา ข้อมูลอันเป็นความลับ, รหัสการเข้าระบบ, เส้นทางและวิธีการเข้าถึงระบบ เป็นต้น (มาตรา 6)

6. การใช้คอมพิวเตอร์เพื่อการปลอมแปลง (Computer-related Forgery) ความผิดตามมาตรานี้ เทียบได้กับความผิดเกี่ยวกับการปลอมแปลงเอกสาร วัตถุประสงค์ เพื่ออุดช่องว่างของกฎหมายอาญาดั้งเดิมในเรื่องเกี่ยวกับการปลอมแปลง ซึ่งอาจไม่สามารถใช้กับข้อมูลที่ถูกเก็บไว้ในรูปสื่ออิเล็กทรอนิกส์ได้ (มาตรา 7)

7. การใช้คอมพิวเตอร์ในการฉ้อโกง (Computer-related Fraud) โดยการป้อนข้อมูลที่ผิดเพื่อให้เครื่องประมวลผลผิดพลาด โดยทำให้ทรัพย์สินของผู้อื่นเสียหาย (Loss of Property) (มาตรา 8)

8. ความผิดเกี่ยวกับภาพลามกอนาจารเด็ก (Offences Related to Child Pornography) บัญญัติขึ้น เพื่อเป็นมาตรการปกป้องเด็กจากการแสวงประโยชน์ทางเพศ โดยใช้

คอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตเป็นเครื่องมือ เป็นการสอดรับกับนโยบายของสภายุโรป และแนวโน้มในทางระหว่างประเทศที่ห้ามการเผยแพร่ภาพลามกอนาจารเด็ก ทั้งยังสอดคล้องกับบทบัญญัติในอนุสัญญาแห่งสหประชาชาติว่าด้วยสิทธิเด็ก (The UN Convention on Rights of Child) อีกด้วย

ในความผิดทั้ง 8 ฐานความผิดข้างต้นนี้ อนุสัญญาฯได้กำหนดให้ฐานความผิดบางฐาน เป็น Optional List กล่าวคือ ประเทศภาคีสามารถตั้งข้อสงวนเพื่อเลือกที่จะไม่กำหนดความผิดบางฐานเป็นความผิดอาญาภายใน เนื่องจากฐานความผิดที่เป็น Optional List นี้ บางประเทศเห็นว่าไม่ควรกำหนดให้เป็นความผิดอาญา เช่น การแทรกแซงข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาต (Data Interference) ซึ่งบัญญัติในมาตรา 4, ความผิดเกี่ยวกับการนำสิ่งที่ได้จากคอมพิวเตอร์ไปใช้ในทางที่ผิด (Misuse of Devices) ในมาตรา 6 และความผิดเกี่ยวกับภาพลามกอนาจารเด็ก ตามมาตรา 9 เฉพาะข้อ 1(d)(e) และ ข้อ 2 (b)(c)

นอกเหนือจากความผิดตามข้อตกลงหลัก 8 ประการข้างต้น สภายุโรปกำลังร่างข้อตกลงเพิ่มเติมว่าด้วย การเหยียดเชื้อชาติ ผ่านเครือข่ายอินเทอร์เน็ต เป็นอาชญากรรมคอมพิวเตอร์เพิ่มขึ้นอีก 1 ฐานความผิดอีกด้วย โดยจัดทำเป็นพิธีสารแนบท้ายอนุสัญญาฯ ซึ่งการแก้ไขเพิ่มเติมเรื่องการเหยียดเชื้อชาตินี้ สืบเนื่องมาจากประเด็นความขัดแย้งระหว่างประเทศฝรั่งเศสกับสหรัฐอเมริกา เรื่องการประมูลสินค้าที่ระลึกจากพรรคนาซีในห้องประมูลออนไลน์ ของ Yahoo.com

เป็นที่แน่นอนว่าความผิดตามอนุสัญญาฯดังที่ได้กล่าวมาข้างต้นนั้น ย่อมเป็นความผิดที่ทุกรัฐภาคีต้องถือว่าเป็นความผิดอาญา ซึ่งนับเป็นการแก้ปัญหาความไม่สอดคล้องของกฎหมายภายในของรัฐต่างๆได้อย่างมาก ทำให้รัฐภาคีสามารถให้ความร่วมมือในการส่งผู้ร้ายข้ามแดนในความผิดที่กำหนดในอนุสัญญาระหว่างกันได้ง่ายขึ้น แต่เป็นที่สังเกตได้ว่าการกำหนดความผิดตามอนุสัญญาว่าด้วยอาชญากรรมคอมพิวเตอร์ของ Council of Europe ดังกล่าวไม่มีการให้คำนิยามที่ชัดเจนเกี่ยวกับการกระทำอาชญากรรมคอมพิวเตอร์เพื่อกระทำความผิดต่ออากาศยาน การก่อการร้ายและความผิดอื่นๆที่เกี่ยวเนื่องกับการเมือง[24] ซึ่งเท่ากับไม่มีการกำหนด

---

[24] Abraham D. Sofaer, Chapter 6 : Toward an international convention on cyber security[Online],(n.d.), Available from:

เกี่ยวกับความผิดทางการเมืองเป็นข้อยกเว้นในการส่งผู้ร้ายข้ามแดน ในประเด็นนี้อาจกล่าวได้ว่า แนวโน้มในปัจจุบันเกี่ยวกับแนวคิดเรื่องความผิดทางการเมืองนั้นเปลี่ยนแปลงไป กล่าวคือ เริ่มมีแนวคิดที่จะไม่นำกฎเกณฑ์เรื่องของความผิดทางการเมืองมาใช้ในการส่งผู้ร้ายข้ามแดน แนวโน้มดังกล่าว ได้รับการยอมรับจากประเทศในกลุ่มยุโรป เนื่องจากความผิดทางการเมืองมักถูกใช้เป็นข้ออ้างในความผิดเกี่ยวกับการก่อการร้าย (Terrorism) และความผิดเกี่ยวกับการเหยียดเชื้อชาติ (Hate Crime) นอกจากนี้ ประเทศในกลุ่มนี้ยังเห็นว่า การกระทำความผิดทางอาญาใดๆ ไม่จำเป็นต้องก่อให้เกิดผลกระทบต่อความเปลี่ยนแปลงทางการเมืองในประเทศเสมอไป[25] อย่างไรก็ตาม ในปัจจุบันการไม่ส่งผู้ร้ายข้ามแดนในความผิดทางการเมือง ซึ่งเป็นข้อยกเว้นของการส่งผู้ร้ายข้ามแดนระหว่างประเทศนั้น ก็ยังคงเป็นหลักเกณฑ์ทางกฎหมายและทางปฏิบัติของรัฐต่างๆอยู่

นอกจากการกำหนดถึงลักษณะความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์แล้ว บทบัญญัติในอนุสัญญาฯยังได้บัญญัติถึงเขตอำนาจศาลในคดีอาชญากรรมคอมพิวเตอร์[26] ซึ่งรัฐภาคีสามารถอ้างเขตอำนาจศาลในคดีอาชญากรรมคอมพิวเตอร์ได้ใน 4 กรณี[27] คือ เขตอำนาจ

---

http://www.hoover.stanford.edu/publications/books/fulltext/cybercrime/221.pdf[2003, April 29]

[25] John T. Soma , Thomas F. Muther , Jr. and Heidi M.L. Brissette, " Transnational extradition for computer crimes : Are new treaties and laws need ?," Harvard Journal on Legislation , 34 : 327.

[26] Article 22 paragraph 1 "Each party shall adopt such legislative and other measure as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed

a. in its teritory; or

b. on board a ship flying the flag of that Party; or

c. on board an aircraft registered under the laws of that Party; or

d. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is commiteed outside the territorial jurisdiction of any state"

[27] บทบัญญัติในอนุสัญญาฯ ใช้คำว่า Jurisdiction ซึ่งมีความหมายถึงการใช้เขตอำนาจรัฐในทางอาญาโดยฝ่ายนิติบัญญัติ บริหารและตุลาการ แต่การวิเคราะห์ของผู้เขียนในส่วนนี้ จะ

เหนือการกระทำความผิดตามหลักดินแดน เขตอำนาจตามหลักบุคคล เขตอำนาจเหนือเรือที่ชักธงของรัฐและเขตอำนาจเหนืออากาศยานที่จดทะเบียนตามกฎหมายของรัฐนั้น อย่างไรก็ตาม อนุสัญญาฯให้สิทธิแก่รัฐภาคีในการเลือกที่จะไม่ใช้บังคับเขตอำนาจศาลเหนือบุคคล เรือและอากาศยานที่มีสัญชาติของรัฐ ซึ่งก็หมายความถึงการที่รัฐอาจเลือกบังคับใช้เฉพาะเขตอำนาจศาลตามหลักดินแดนเพียงอย่างเดียว[28]

ดังที่ผู้เขียนได้วิเคราะห์ในบทที่ 3 แล้วว่า การอ้างเขตอำนาจศาลเหนือคดีอาชญากรรมคอมพิวเตอร์ของประเทศต่างๆในปัจจุบันยังคงมีปัญหาความแตกต่างกันในหลักการวินิจฉัย อาจกล่าวได้ว่าการใช้เขตอำนาจศาลของรัฐในคดีอาญาตามหลักกฎหมายระหว่างประเทศเกี่ยวกับเขตอำนาจศาล ไม่สามารถใช้กับกรณีของอาชญากรรมคอมพิวเตอร์ได้อย่างมีประสิทธิภาพ นอกจากนี้รัฐต่างๆยังคงอ้างเขตอำนาจศาลด้วยหลักการวินิจฉัยที่แตกต่างกัน ดังนั้น วิธีการแก้ปัญหาดังกล่าวคืออนุสัญญาระหว่างประเทศจำต้องกำหนดหลักเกณฑ์พิเศษขึ้นมาเสริมหลักทั่วไปในการกำหนดเขตอำนาจศาล เช่น การกำหนดสถานที่ที่ถือว่าความผิดเกิดขึ้น[29] ซึ่งจะทำให้การอ้างเขตอำนาจศาลมีความชัดเจนแน่นอนขึ้นและเป็นไปในแนวทางเดียวกันไม่ว่าเป็นการอ้างเขตอำนาจศาลโดยรัฐใด แต่บทบัญญัติเรื่องเขตอำนาจศาลเหนือคดีอาชญากรรมคอมพิวเตอร์ตามข้อ 22 แห่งอนุสัญญาฯนี้ ไม่ได้มีบทบัญญัติเพื่อแก้ไขปัญหาการขัดกันของเขตอำนาจศาลดังเช่นที่ได้กล่าวมา เนื่องจากอนุสัญญาฯ ไม่มีหลักเกณฑ์พิเศษใดๆ เพื่อใช้กับอาชญากรรมคอมพิวเตอร์โดยเฉพาะ เพียงแต่นำหลักกฎหมายระหว่างประเทศเกี่ยวกับเขตอำนาจศาลในคดีอาญามาบัญญัติไว้เท่านั้น ทำให้ความขัดแย้งในการวินิจฉัยเรื่องเขตอำนาจศาลของประเทศต่างๆจึงก็ยังคงมีอยู่ ซึ่งปัญหาดังกล่าวอาจถูกใช้เป็นข้ออ้างในการปฏิเสธการส่งผู้ร้ายข้ามแดนได้

จำกัดเพียงเฉพาะกรณีของเขตอำนาจศาล(ตุลาการ) ซึ่งเป็นส่วนหนึ่งของการใช้เขตอำนาจรัฐทั้ง 3 ประการเท่านั้น

[28]Article 22 paragraph 2 "Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraph 1.b through 1.d of this article or any part thereof."

[29] หลักการเดียวกันนี้ ได้รับการยอมรับนำไปบัญญัติไว้ในกฎหมายแม่แบบของสหประชาชาติว่าด้วยการพาณิชย์อิเล็กทรอนิกส์ ข้อ 15(4) นอกจากนี้จากการศึกษาพบว่าศาลสหรัฐอเมริกาก็ใช้หลักดังกล่าวในการวินิจฉัยเขตอำนาจเหนือคดีอาชญากรรมคอมพิวเตอร์ด้วยเช่นกัน รายละเอียดศึกษาได้ใน บทที่ 3

นอกจากนี้ วิธีการแก้ปัญหาการขัดกันของเขตอำนาจศาลในกรณีอาชญากรรมคอมพิวเตอร์อีกประการหนึ่งซึ่งไม่ปรากฏในอนุสัญญาคณะกรรมการยุโรปว่าด้วยอาชญากรรมคอมพิวเตอร์ที่ถูกหยิบยกขึ้นมาพิจารณาคือ การกำหนดให้อาชญากรรมคอมพิวเตอร์อยู่ภายใต้เขตอำนาจศาลในหลักลงโทษสากล เนื่องจากการกำหนดเขตอำนาจศาลก็ไม่ควรยอมรับเพียงเฉพาะเขตอำนาจศาลของรัฐที่ผู้กระทำความผิดเข้าสู่ระบบฐานข้อมูลหรือเว็บไซต์ของรัฐอื่นเพื่อกระทำความผิด เนื่องจากเมื่อเข้าสู่ระบบเครือข่ายแล้วผู้กระทำสามารถเป็นสาเหตุให้เกิดความผิดได้ในรัฐอื่นๆอีก รัฐจึงควรยอมรับเขตอำนาจศาลในหลักลงโทษสากลเหนือการกระทำความผิดอาชญากรรมคอมพิวเตอร์[30] จากแนวความคิดดังกล่าว ทำให้ต้องพิจารณาหลักเกณฑ์เรื่องเขตอำนาจศาลในหลักลงโทษสากลก่อนว่ามีลักษณะเช่นใด และการนำเขตอำนาจศาลในหลักลงโทษสากลมาใช้กับกรณีอาชญากรรมคอมพิวเตอร์จะสามารถกระทำได้หรือไม่เพียงใด

เขตอำนาจศาลในหลักลงโทษสากล (Universal Principle) หมายถึงการใช้เขตอำนาจของรัฐเพื่อดำเนินคดีและลงโทษผู้กระทำความผิดโดยไม่คำนึงถึงสัญชาติของผู้กระทำความผิด ไม่คำนึงถึงสัญชาติของผู้เสียหาย และไม่คำนึงถึงสถานที่ที่การกระทำความผิดเกิดขึ้น แต่ถือหลักอำนาจศาลของประเทศที่จับกุมผู้กระทำความผิดได้[31] แต่ทั้งนี้การใช้เขตอำนาจศาลในหลักลงโทษสากลจะต้องเป็นกรณีอาชญากรรมระหว่างประเทศที่เกี่ยวข้องกับสากล ที่ส่งผลกระทบต่อศีลธรรมอันดี ความสงบสุขและความปลอดภัยในผลประโยชน์ของประชาคมระหว่างประเทศเท่านั้น โดยอาชญากรรมเหล่านี้จะเป็นอาชญากรรมที่มีลักษณะแน่นอน และได้รับการรับรองว่าเป็นอาชญากรรมระหว่างประเทศที่รัฐสามารถใช้เขตอำนาจศาลในหลักลงโทษสากลได้ไม่ว่าจะเป็นการรับรองโดยจารีตประเพณีหรือโดยสนธิสัญญาระหว่างประเทศ[32]

---

[30] Abraham D. Sofaer, Chapter 6 : Toward an international convention on cyber security[Online],(n.d.), Available from: http://www.hoover.stanford.edu/publications/books/fulltext/cybercrime/221.pdf[2003, April 29]

[31] สุผานิต มั่นศุข, "เขตอำนาจศาลในคดีอาญา," (วิทยานิพนธ์ปริญญามหาบัณฑิต สาขาวิชานิติศาสตร์ บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย, 2517), หน้า 96.

[32] กิตติ โอสถเจริญผล, "เขตอำนาจรัฐสากลเหนืออาชญากรรมระหว่างประเทศ," (วิทยานิพนธ์ปริญญามหาบัณฑิต สาขาวิชานิติศาสตร์ บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย, 2544), หน้า 50-51.

จากหลักเกณฑ์ดังกล่าว จะเห็นได้ว่า รัฐไม่สามารถปรับใช้เขตอำนาจศาลในหลักลงโทษสากลกับอาชญากรรมได้ทุกประเภท หากแต่อาชญากรรมที่จะอยู่ภายใต้เขตอำนาจศาลในหลักลงโทษสากลต้องเป็นอาชญากรรมที่ได้รับการรับรองจากนานาประเทศว่า เป็นอาชญากรรมระหว่างประเทศ ดังนั้น ในกรณีของอาชญากรรมคอมพิวเตอร์นั้น การที่รัฐจะใช้เขตอำนาจศาลในหลักลงโทษสากลเหนืออาชญากรรมคอมพิวเตอร์ได้นั้น ต้องปรากฏว่า มีการยอมรับให้อาชญากรรมคอมพิวเตอร์เป็นอาชญากรรมระหว่างประเทศก่อน ซึ่งในปัจจุบัน ก็ยังไม่มีจารีตประเพณีระหว่างประเทศหรือสนธิสัญญาระหว่างประเทศใดๆ ที่รับรองว่าอาชญากรรมคอมพิวเตอร์เป็นอาชญากรรมระหว่างประเทศที่จะอยู่ภายใต้เขตอำนาจศาลในหลักลงโทษสากล ดังนั้น ในปัจจุบันจึงไม่อาจอ้างเขตอำนาจศาลในหลักลงโทษสากลเหนืออาชญากรรมคอมพิวเตอร์เพื่อลงโทษผู้กระทำความผิดได้

แต่เนื่องจากอาชญากรรมคอมพิวเตอร์มีลักษณะเป็นอาชญากรรมข้ามชาติ ที่ส่งผลกระทบต่อประชาคมระหว่างประเทศอย่างมาก จึงไม่แน่ว่าต่อไปในอนาคต รัฐทั้งหลายอาจให้การรับรองให้อาชญากรรมคอมพิวเตอร์เป็นอาชญากรรมระหว่างประเทศ และอยู่ภายใต้เขตอำนาจศาลในหลักลงโทษสากลได้ ซึ่งแนวคิดในการกำหนดให้อาชญากรรมคอมพิวเตอร์อยู่ภายใต้เขตอำนาจศาลในหลักลงโทษสากลมีข้อดีคือ เนื่องจากจะทำให้ปัญหาความขัดแย้งในเรื่องเขตอำนาจศาลเหนืออาชญากรรมคอมพิวเตอร์หมดไป และรัฐที่ผู้กระทำความผิดอยู่ในเขตอำนาจศาลสามารถใช้หลัก Aut Dedere Aut Judicare (Either Extradite or Prosecution) กล่าวคือรัฐที่ผู้กระทำความผิดอยู่ในเขตอำนาจต้องใช้เขตอำนาจสากลนี้เพื่อดำเนินคดีและลงโทษอาชญากรคอมพิวเตอร์เอง หากไม่มีการส่งผู้ร้ายข้ามแดนหรือการส่งผู้ร้ายข้ามแดนถูกปฏิเสธ[33] ไม่ว่าความผิดจะเกิดในรัฐใดและผู้กระทำความผิดเป็นคนชาติของรัฐใดก็ตาม ซึ่งในกรณีนี้แม้ไม่มีการส่งผู้ร้ายข้ามแดนให้แก่รัฐที่ได้รับความเสียหายหรือมีความเกี่ยวพันกับการกระทำความผิด ผู้กระทำความผิดก็จะต้องถูกดำเนินคดีอย่างแน่นอน

อย่างไรก็ตาม ข้อเสียที่อาจเกิดขึ้นคือ หากมีการใช้เขตอำนาจศาลในหลักลงโทษสากลเหนืออาชญากรรมคอมพิวเตอร์ รัฐที่ลงโทษผู้กระทำความผิด อาจไม่ใช่รัฐที่ได้รับความเสียหายโดยตรงจากการกระทำความผิด ซึ่งการให้รัฐที่ไม่ได้รับความเสียหายโดยตรงจากการกระทำความผิดเป็นผู้พิจารณาพิพากษาคดี ก็ไม่อาจแน่ใจได้ว่าผู้กระทำความผิดจะได้รับการลงโทษสมกับความผิดและผู้ความเสียหายจะรับการเยียวยาให้เพียงพอกับความเสียหายที่เกิดขึ้น

---

[33] เรื่องเดียวกัน, หน้า 60.

หรือไม่ ซึ่งรัฐที่มีตัวผู้กระทำความผิดอยู่ในเขตอำนาจ ควรที่จะดำเนินคดีและลงโทษผู้กระทำความผิดด้วยความเป็นธรรม โดยคำนึงถึงความเสียหายที่รัฐผู้ร้องขอได้รับด้วย

นอกเหนือบทบัญญัติในเรื่องของเขตอำนาจศาลในคดีอาชญากรรมคอมพิวเตอร์แล้ว ในส่วนบทบัญญัติที่เกี่ยวกับความร่วมมือระหว่างประเทศในการส่งผู้ร้ายข้ามแดนถูกบัญญัติอยู่ในข้อ 24 แห่งอนุสัญญาฯ ซึ่งเป็นบทบัญญัติที่สร้างพันธกรณีให้กับรัฐภาคีต้องดำเนินการส่งผู้ร้ายข้ามแดนแก่กัน เพื่อให้ความร่วมมือระหว่างประเทศเกี่ยวกับการส่งผู้ร้ายข้ามแดนมีการขยายขอบเขตกว้างกว่าที่เป็นอยู่รวมถึงเกิดความแน่นอนในทางปฏิบัติ โดยการส่งผู้ร้ายข้ามแดนดำเนินการได้โดยพิจารณาจากความผิดที่กำหนดในอนุสัญญาฯ ซึ่งต้องเป็นความผิดที่สามารถลงโทษได้ตามกฎหมายภายในของทั้งสองรัฐโดยมีอัตราโทษจำคุกไม่น้อยกว่า 1 ปีหรือโทษอื่นที่หนักกว่า[34]

อย่างไรก็ตาม มีข้อจำกัดบางประการในการส่งผู้ร้ายข้ามแดนตามข้อ 24 กล่าวคือ การพิจารณาส่งผู้ร้ายข้ามแดนตามข้อ 24 นี้ กำหนดให้การส่งผู้ร้ายข้ามแดนอยู่ภายใต้เงื่อนไขที่มีการกำหนดไว้โดยกฎหมายภายในของรัฐผู้ร้องขอและรัฐผู้รับคำร้องขอ ดังนั้น หลักการเรื่องความผิดอาญาของทั้งสองประเทศ (Double Criminality) และหลักโทษขั้นต่ำของความผิดอาญาที่มีการยึดถือกันก่อนหน้านี้ในกฎเกณฑ์ระหว่างประเทศว่าด้วยการส่งผู้ร้ายข้ามแดนโดยทั่วไป ซึ่งทำให้ไม่สามารถดำเนินการส่งผู้ร้ายข้ามแดนกันได้หากว่าไม่ตรงกับหลักการดังกล่าวยังคงใช้ได้ต่อไป ดังนั้น แม้ว่ารัฐภาคีจะผูกพันตามพันธกรณีในอนุสัญญาฯแต่หากยังไม่มีกฎหมายภายในกำหนดให้การกระทำที่ร้องขอเป็นความผิดที่มีโทษจำคุกไม่ต่ำกว่า 1 ปีหรือโทษอื่นที่หนักกว่าแล้วก็ไม่สามารถให้ความร่วมมือในการส่งผู้ร้ายข้ามแดนกันได้

จากที่ได้กล่าวถึงกลไกการแก้ไขปัญหาโดยอาศัยความร่วมมือระหว่างประเทศแบบพหุภาคีนี้ จะเห็นได้ว่า ไม่ว่าโดยความพยายามขององค์การสหประชาชาติ หรือ Council of

---

[34] Article 24 paragraph 1 "a This article applies to extradition between Parties for the criminal offences establish in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty"

Europe ล้วนแต่เป็นความพยายามในการกำหนดลักษณะความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์ให้เป็นไปในทิศทางเดียวกัน พร้อมทั้งกำหนดถึงความตกลงเกี่ยวกับการส่งผู้ร้ายข้ามแดนให้สนองรับกับกรณีอาชญากรรมคอมพิวเตอร์ด้วย ทำให้กลไกการแก้ไขปัญหาแบบพหุภาคีนี้สามารถแก้ปัญหาได้กว้างขวางกว่ากลไกการแก้ไขปัญหาโดยความตกลงทวิภาคี

แต่ไม่ว่าการแก้ปัญหาโดยอาศัยความตกลงแบบทวิภาคีหรือพหุภาคีนั้น จะเป็นเครื่องมือที่สามารถใช้แก้ไขปัญหาได้อย่างมีประสิทธิภาพได้นั้น จะต้องอาศัยความร่วมมือจากรัฐที่เกี่ยวข้องอย่างจริงจัง นอกจากนี้ การที่กลไกของความตกลงระหว่างประเทศนั้นจะดำเนินไปได้ก็ด้วยการที่รัฐทั้งหลายจะต้องปรับปรุงกฎหมายภายในของตนให้สนองรับกับความตกลงระหว่างประเทศดังกล่าวด้วยอีกประการหนึ่ง เพื่อให้รัฐสามารถปฏิบัติตามพันธกรณีในทางระหว่างประเทศได้อย่างมีประสิทธิภาพ

4.2 กลไกการแก้ปัญหาในระดับประเทศ

กลไกการแก้ปัญหาในระดับประเทศเป็นแนวทางการแก้ไขปัญหาภายในของรัฐ โดยการที่รัฐจะต้องบัญญัติกฎหมายภายในเพื่อให้รัฐสามารถปฏิบัติตามพันธกรณีระหว่างประเทศได้อย่างมีประสิทธิภาพ จากการศึกษาในบทที่ 3 ทำให้ทราบว่าปัญหาและอุปสรรคในการส่งผู้ร้ายข้ามแดนในคดีอาชญากรรมคอมพิวเตอร์ นอกจากจะมีสาเหตุมาจากการขาดแคลนข้อตกลงระหว่างประเทศแล้ว ยังมีสาเหตุมาจากความไม่เพียงพอของกฎหมายภายใน เป็นผลทำให้รัฐไม่อาจให้ความร่วมมือในการส่งผู้ร้ายข้ามแดนได้ ซึ่งการศึกษาในส่วนนี้จะมุ่งถึงกฎหมายภายในของรัฐในสองลักษณะคือ กฎหมายภายในเกี่ยวกับอาชญากรรมคอมพิวเตอร์และกฎหมายภายในเกี่ยวกับการส่งผู้ร้ายข้ามแดน

4.2.1 กฎหมายภายในเกี่ยวกับอาชญากรรมคอมพิวเตอร์

จากหลักเกณฑ์ระหว่างประเทศว่าด้วยการส่งผู้ร้ายข้ามแดน ทำให้ทราบว่ากระบวนการส่งผู้ร้ายข้ามแดนต้องอาศัยกลไกของกฎหมายภายในในการให้ความร่วมมือระหว่างประเทศ สืบเนื่องจากหลักการเรื่องความผิดอาญาของทั้งสองประเทศและโทษขั้นต่ำ ดังนั้น การตรากฎหมายภายในเกี่ยวกับอาชญากรรมคอมพิวเตอร์จึงมีความสำคัญในการให้ความร่วมมือในการส่งผู้ร้ายข้ามแดนในปัจจุบันอย่างยิ่ง ดังนั้น ประเทศที่ยังไม่มีกฎหมายอาชญากรรมคอมพิวเตอร์ จึงควรต้องพัฒนากฎหมายภายในเพื่อให้สามารถให้ความร่วมมือในการส่งผู้ร้ายข้าม

แดนได้ ซึ่งผู้เขียนจะได้ยกตัวอย่างของประเทศไทยในฐานะที่เป็นประเทศหนึ่งที่ได้รับผลกระทบจากอาชญากรรมคอมพิวเตอร์ จำต้องมีกฎหมายภายในเพื่อบังคับใช้กับการกระทำความผิดดังกล่าวด้วยเช่นกัน แต่จนถึงปัจจุบันประเทศไทยยังไม่มีการประกาศใช้กฎหมายอาชญากรรมคอมพิวเตอร์ คงมีเพียงประมวลกฎหมายอาญาซึ่งไม่สามารถใช้กับการกระทำความผิดทางคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตได้ ซึ่งทำให้ประเทศยังคงมีปัญหาในการให้ความร่วมมือในการส่งผู้ร้ายข้ามแดนในความผิดฐานนี้

ความจำเป็นเร่งด่วนต่อปัญหาอาชญากรรมคอมพิวเตอร์ทำให้ประเทศไทยได้ยกร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ. ... ที่ผ่านความเห็นชอบของคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ เมื่อวันที่ 2 พฤษภาคม 2545 ซึ่งในขณะนี้อยู่ระหว่างการเสนอเพื่อให้คณะรัฐมนตรีให้ความเห็นชอบในหลักการ โดยร่างพระราชบัญญัติดังกล่าวได้มีบทบัญญัติที่กำหนดให้การก่ออาชญากรรมคอมพิวเตอร์เป็นความผิดอาญา โดยได้บัญญัติไว้ในมาตรา 5-14 ซึ่งได้กำหนดการกระทำที่เป็นความผิดอาญาไว้ 7 ฐานความผิด ดังต่อไปนี้

1) <u>การเข้าถึงระบบคอมพิวเตอร์โดยไม่มีอำนาจ (มาตรา 5 และมาตรา 6)</u>

การกระทำความผิดฐานนี้ คือกรณีที่บุคคลได้กระทำการเข้าไปในระบบคอมพิวเตอร์โดยปราศจากอำนาจ ในลักษณะเป็นการฝ่าฝืนมาตรการรักษาความปลอดภัย หรือระบบที่มีการป้องกันการเข้าถึงโดยเฉพาะและมิได้มีไว้สำหรับตน ถือเป็นความผิดตามกฎหมาย อย่างไรก็ตามประเด็นปัญหาที่เกิดขึ้นคือ การกำหนดขอบเขตของคำว่า "เข้าถึง" มีความหมายครอบคลุมถึงการกระทำใดบ้าง และการกระทำใดที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่ไม่ถือเป็นการเข้าถึงระบบคอมพิวเตอร์ ซึ่งบทบัญญัติของมาตรานี้ก็ไม่ได้กำหนดความหมายหรือขอบเขตของการเข้าถึงอย่างชัดแจ้ง แต่จากคำอธิบายร่างพระราชบัญญัติอาชญากรรมคอมพิวเตอร์ของโครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศให้ความหมายของการเข้าถึง 3 กรณี[35]คือ

ก) การเข้าถึงทั้งในระดับกายภาพเช่นกรณีที่มีการกำหนดรหัสผ่านเพื่อป้องกันมิให้บุคคลอื่นใช้เครื่องคอมพิวเตอร์และผู้กระทำผิดดำเนินการด้วยวิธีใดวิธีหนึ่งเพื่อให้ได้รหัสผ่านนั้นมาและสามารถใช้เครื่องคอมพิวเตอร์นั้นได้โดยนั่งอยู่หน้าเครื่องคอมพิวเตอร์นั้นเองและหมายรวมถึงการ

---

[35] สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, <u>คำอธิบายร่างพระราชบัญญัติว่าด้วยอาชญากรรมคอมพิวเตอร์ พ.ศ....</u>[Online],2003, แหล่งที่มา: http://www.ecommerce.or.th/ictlaw/cc/explanation/part2.html [2003, July 17]

เข้าถึงระบบคอมพิวเตอร์หรือเข้าถึงข้อมูลคอมพิวเตอร์แม้ตัวบุคคลที่เข้าถึงจะอยู่ห่างโดยระยะทางกับเครื่องคอมพิวเตอร์แต่สามารถเจาะเข้าไปในระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่ตนต้องการได้

ข) การเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ทั้งหมดหรือแต่บางส่วนก็ได้ ดังนั้นจึงอาจหมายถึงการเข้าถึงฮาร์ดแวร์หรือส่วนประกอบต่างๆของคอมพิวเตอร์ข้อมูลที่ถูกบันทึกเก็บไว้ในระบบเพื่อใช้ในการส่งหรือโอนถึงอีกบุคคลหนึ่ง เช่น ข้อมูลจราจรทางคอมพิวเตอร์ เป็นต้น

ค) การเข้าถึงโดยผ่านทางเครือข่ายสาธารณะ เช่น อินเทอร์เน็ต อันเป็นการเชื่อมโยงระหว่างเครือข่ายหลายๆ เครือข่ายเข้าด้วยกัน และยังหมายถึง การเข้าถึงโดยผ่านระบบเครือข่ายเดียวกันด้วยก็ได้ เช่น ระบบ LAN (Local Area Network) อันเป็นเครือข่ายที่เชื่อมต่อคอมพิวเตอร์ที่ตั้งอยู่ในพื้นที่ใกล้ๆ กันเข้าด้วยกัน

ประเด็นที่จำเป็นต้องพิจารณาเกี่ยวกับการกระทำความผิดฐานนี้ คือ เพียงแค่มีการเข้าถึงโดยไม่ได้รับอนุญาตจะถือว่าเป็นการก่ออาชญากรรมได้หรือไม่ หรือผู้กระทำต้องมีมูลเหตุจูงใจที่จะกระทำให้เกิดความเสียหายด้วย ซึ่งประเด็นนี้ผู้เขียนได้กล่าวในบทที่ 3 แล้วว่า กฎหมายอาชญากรรมคอมพิวเตอร์ของประเทศต่างๆมีแนวทางในการกำหนดกฎหมายในประเด็นนี้แตกต่างกัน กล่าวคือบางประเทศกำหนดให้การกระทำเป็นความผิดต่อเมื่อมีเจตนาหรือมูลเหตุจูงใจให้เกิดความเสียหาย ในขณะที่หลายประเทศกำหนดให้การกระทำดังกล่าวเป็นความผิดโดยไม่ต้องมีเจตนาหรือมูลเหตุจูงใจดังกล่าว[36] ในประเด็นนี้ร่างพระราชบัญญัติมาตรา 5 และมาตรา 6 ได้กำหนดให้การเข้าถึงโดยมิชอบเป็นความผิด แม้ว่าผู้กระทำจะมิได้มีมูลเหตุจูงใจเพื่อก่อให้เกิดความเสียหายก็ตาม ทั้งนี้ เพราะเห็นว่าการกระทำดังกล่าวนั้นสามารถก่อให้เกิดการกระทำผิดฐานอื่นหรือฐานที่ใกล้เคียงค่อนข้างง่ายและอาจก่อให้เกิดความเสียหายร้ายแรง ทั้งการพิสูจน์มูลเหตุจูงใจทำได้ค่อนข้างยากและที่สำคัญจะต้องเป็นการเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่มีวิธีการป้องกันการเข้าถึงโดยเฉพาะจึงจะเป็นความผิดตามมาตรา 5 และมาตรา 6 ได้[37]

นอกประเด็นนี้แล้ว ยังมีข้อสังเกตอีกประการหนึ่งว่าการเข้าถึงข้อมูลคอมพิวเตอร์ตามมาตรา 6 นี้กฎหมายมิได้ใช้คำว่าได้ไปซึ่งข้อมูลโดยตรง ดังนั้น การเข้าถึงข้อมูลใดๆที่เป็นความลับนั้น แม้เพียงผู้กระทำความผิดเข้าถึง ซึ่งมีผลทำให้ผู้กระทำได้เห็นหรือรับรู้ข้อความที่ถูกเก็บหรือส่ง

---

[36] ดูรายละเอียดใน บทที่ 3 ข้อ 3.1.2 ข้อ 7)

[37] เรื่องเดียวกัน

โดยวิธีการทางอิเล็กทรอนิกส์แล้วก็ถือเป็นความผิด โดยไม่จำต้องมีการบันทึก ทำสำเนาหรือถ่ายโอนข้อมูลแต่อย่างใด

2) การลักลอบดักข้อมูลคอมพิวเตอร์โดยไม่มีอำนาจ (มาตรา 7)

การกระทำความผิดฐานนี้ คือกรณีการลักลอบดักข้อมูลที่มีการส่งผ่าน หรือถ่ายโอนข้อมูลคอมพิวเตอร์ผ่านระบบเครือข่าย ซึ่งการนำข้อมูลไปในลักษณะนี้สามารถกระทำได้โดยการทำสำเนาและนำข้อมูลนั้นไปได้โดยไม่มีการเคลื่อนย้ายข้อมูลแต่อย่างใด[38] วัตถุประสงค์ของกฎหมายก็เพื่อคุ้มครองสิทธิความเป็นส่วนตัวในการติดต่อสื่อสาร ทำนองเดียวกับการให้ความคุ้มครองความเป็นส่วนตัวแบบเดิมที่ห้ามการดักฟังโทรศัพท์และการแอบบันทึกเทปลับ[39]

การลักลอบดักข้อมูล จึงได้แก่การกระทำโดยวิธีการทางเทคนิค (Technical Means) เพื่อลักลอบดักฟังตรวจสอบหรือติดตามเนื้อหาสาระของข่าวสารที่สื่อสารถึงกันระหว่างบุคคล หรือกรณีเป็นการกระทำอันเป็นการล่อลวงหรือจัดหาข้อมูลดังกล่าวให้กับบุคคลอื่น รวมทั้งการแอบบันทึกข้อมูลที่สื่อสารถึงกันนั้นด้วย ทั้งนี้ วิธีการทางเทคนิค หมายถึง อุปกรณ์ที่มีสายเชื่อมต่อกับระบบเครือข่าย และหมายรวมถึงอุปกรณ์ประเภทไร้สาย เช่น การติดต่อผ่านทางโทรศัพท์มือถือ เป็นต้น อย่างไรก็ดี การกระทำที่เป็นความผิดฐานลักลอบดักข้อมูลนั้น ข้อมูลที่ส่งต้องมิใช่ข้อมูลที่ส่งและเปิดเผยให้สาธารณชนสามารถรับรู้ได้ (Non-public Transmissions) ทั้งนี้ การกระทำความผิดฐานนี้จึงจำกัดเฉพาะแต่เพียงวิธีการส่งที่ผู้ส่งข้อมูลประสงค์จะส่งข้อมูลนั้นให้แก่บุคคลหนึ่งบุคคลใดโดยเฉพาะเจาะจงเท่านั้น แม้จะเป็นการส่งข้อมูลผ่านทางเครือข่ายสาธารณะ เช่น การส่งผ่านทางอินเทอร์เน็ตก็ตาม ดังนั้น มาตรานี้จึงมิได้มีประเด็นที่ต้องพิจารณาถึงเนื้อหาสาระของข้อมูลที่ส่งด้วยแต่อย่างใด เพราะเนื้อหาสาระของข้อมูลที่ส่งนั้นอาจมีเนื้อหาสาระที่หาได้

---

[38]สำนักงานเลขานุการ คณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ (ฉบับปรับปรุงครั้งที่ 2)(กรุงเทพฯ : โรงพิมพ์เดือนตุลา, 2544), หน้า 59-60.

[39] สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, คำอธิบายร่างพระราชบัญญัติว่าด้วยอาชญากรรมคอมพิวเตอร์ พ.ศ....[Online],2003, แหล่งที่มา: http://www.ecommerce.or.th/ictlaw/cc/explanation/part2.html [2003, July 17]

โดยทั่วไปหรือมีอยู่ทั่วไป รวมทั้งข้อมูลที่เป็นความลับทางการค้า หรือเป็นข้อมูลส่วนบุคคลที่เจ้าของข้อมูลประสงค์จะปกปิดเป็นความลับก็ได้[40]

อนึ่ง หากพิจารณาลักษณะการกระทำความผิดฐานลักลอบดักข้อมูลและลักษณะการกระทำความผิดฐานเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์โดยไม่มีอำนาจนั้น จะเห็นได้ว่าค่อนข้างใกล้เคียงกันอย่างยิ่ง แต่ข้อที่ทำให้บทบัญญัติทั้งสามมาตรามีความแตกต่างกันก็คือ การกระทำความผิดฐานลักลอบดักข้อมูลเป็นการกระทำโดยมีมูลเหตุจูงใจเพื่อให้ได้ข้อมูลคอมพิวเตอร์ส่วนการกระทำความผิดฐานเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์โดยไม่มีอำนาจนั้น แม้กระทำโดยมิได้มีเจตนาต่อข้อมูลคอมพิวเตอร์หรือโปรแกรมหรือระบบคอมพิวเตอร์ใดโดยเฉพาะเจาะจง และแม้ไม่มีความเสียหายใดๆ เกิดขึ้น ผู้กระทำก็ต้องรับผิดในการกระทำดังกล่าว

3) <u>การรบกวนการทำงานของข้อมูลหรือระบบคอมพิวเตอร์โดยมิชอบ (มาตรา 8 และมาตรา9)</u>

ความผิดฐานรบกวนจะหมายถึงการรบกวนข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ตามร่างพระราชบัญญัติมาตรา 8 และมาตรา 9 กำหนดขึ้นเพื่อลงโทษผู้กระทำความผิดที่จงใจก่อให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์และโปรแกรมคอมพิวเตอร์ โดยประโยชน์ที่มุ่งประสงค์จะคุ้มครอง คือ ความครบถ้วนของข้อมูล และเสถียรภาพในการใช้งานหรือการใช้ข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ที่บันทึกเก็บไว้บนสื่อคอมพิวเตอร์ได้เป็นปกติ

ร่างพระราชบัญญัติมาตรา 8 เป็นบทบัญญัติที่ลงโทษบุคคลซึ่งทำความเสียหาย หรือทำให้ข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์เสื่อมค่าหรือไร้ประโยชน์ รวมถึงการลบหรือทำลายข้อมูลคอมพิวเตอร์ หรือกระทำการใดๆ ให้ไม่สามารถเข้าถึงข้อมูลคอมพิวเตอร์หรือใช้โปรแกรมคอมพิวเตอร์นั้นได้ รวมทั้งการเปลี่ยนแปลงข้อมูลใดๆ ที่มีอยู่ด้วย ตัวอย่างของการกระทำความผิดในฐานนี้ เช่น การป้อนโปรแกรมที่มีไวรัสทำลายข้อมูลหรือโปรแกรมคอมพิวเตอร์หรือการป้อนโปรแกรมม้าโทรจัน (Trojan Horse) เข้าไปในระบบเพื่อขโมยรหัสผ่านของผู้ใช้คอมพิวเตอร์

---

[40] เรื่องเดียวกัน

สำหรับใช้เพื่อเข้าไปลบ เปลี่ยนแปลงแก้ไขข้อมูลหรือกระทำการใดๆ อันเป็นการรบกวนข้อมูล เป็นต้น

นอกจากนั้น มาตรา 9 ยังคุ้มครองการทำงานของระบบคอมพิวเตอร์และระบบการติดต่อสื่อสารให้เป็นไปตามปกติโดยกำหนดบทลงโทษสำหรับการรบกวนหรือขัดขวางการทำงานของระบบคอมพิวเตอร์ ทั้งนี้ การรบกวนหรือขัดขวางหรือทำให้ระบบคอมพิวเตอร์ไม่สามารถทำงานได้เป็นปกตินั้น อาจเกิดขึ้นในขั้นตอนต่างๆ ตั้งแต่การป้อนข้อมูลเข้าไปในระบบ หรือในการส่ง ทำลาย ลบ หรือเปลี่ยนแปลงแก้ไขข้อมูลคอมพิวเตอร์ ซึ่งผลของการกระทำความผิดจะก่อให้เกิดความเสียหายที่ร้ายแรงหรือรุนแรงต่อการใช้ระบบดังกล่าวหรือต่อการติดต่อสื่อสารกับระบบอื่น เช่น การป้อนโปรแกรมที่ทำให้ระบบปฏิเสธการทำงาน (Denial of Service) หรือทำให้ระบบทำงานช้าลง หรือการรบกวนระบบของผู้รับข้อมูลคอมพิวเตอร์โดยการส่งจดหมายอิเล็กทรอนิกส์จำนวนมหาศาลไปยังผู้รับเพื่อให้ระบบคอมพิวเตอร์ทำงานหนักเกินไปจนในที่สุดก็ไม่สามารถทำงานได้อีกต่อไป

4) <u>การกระทำที่เกี่ยวกับความมั่นคงของรัฐ (มาตรา10)</u>

การกระทำความผิดตามมาตรา 5-9 นั้นหากกระทำต่อระบบคอมพิวเตอร์หรือข้อมูลที่เกี่ยวกับความมั่นคงของรัฐ ความสัมพันธ์ระหว่างประเทศ ความมั่นคงทางเศรษฐกิจและการคลัง กฎหมายกำหนดเพิ่มโทษสำหรับการกระทำดังกล่าวหนักกว่าการกระทำต่อข้อมูลเอกชนหรือข้อมูลโดยทั่วไป ทั้งนี้ การตระเตรียมและการพยายามกระทำความผิดจะต้องได้รับโทษเสมือนผู้กระทำความผิดสำเร็จ

5) <u>การปลอมแปลงข้อมูลคอมพิวเตอร์ (มาตรา 12)</u>

จากสภาพของข้อมูลอิเล็กทรอนิกส์ที่สามารถกระทำการแก้ไขเปลี่ยนแปลงได้โดยง่ายและยากที่จะตรวจสอบได้ ซึ่งการปลอมแปลงข้อมูลดังกล่าวอาจกระทำได้หลายกรณี เช่น การปลอมแปลงข้อมูล การปลอมแปลงตราประทับ การปลอมแปลงลายมือชื่ออิเล็กทรอนิกส์ ไม่ว่าทั้งหมดหรือบางส่วน โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน[41] มาตรานี้จึงบัญญัติขึ้น

---

[41]สำนักงานเลขานุการ คณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, <u>โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ (ฉบับปรับปรุงครั้งที่ 2)</u>, หน้า 61-62.

โดยมีวัตถุประสงค์เพื่อสร้างความเท่าเทียมกันและขจัดช่องว่างของประมวลกฎหมายอาญาสำหรับความผิดฐานปลอมแปลงเอกสารในระบบกระดาษ และการปลอมแปลงข้อมูลหรือข้อความที่จัดทำขึ้นในระบบอิเล็กทรอนิกส์ ทั้งนี้ เพื่อประโยชน์ในการรักษาความปลอดภัย (security) และความน่าเชื่อถือ (Reliability) ของข้อมูลอิเล็กทรอนิกส์

บทบัญญัติมาตรานี้หากเปรียบเทียบกับระบบเอกสารจะวางอยู่บนพื้นฐานของหลักเกี่ยวกับการยืนยันตัวบุคคลซึ่งเป็นเจ้าของเอกสาร และความถูกต้องแท้จริงของข้อความในเอกสาร และใช้บังคับกับทั้งกรณีที่ประชาชนทั่วไปจัดทำขึ้นและพนักงานเจ้าหน้าที่ของรัฐจัดทำขึ้น และการปลอมแปลงในที่นี้อาจจะกระทำโดยการนำเข้าหรือป้อนข้อมูลทั้งที่ถูกต้องหรือไม่ถูกต้องตั้งแต่เริ่มต้นและอาจเป็นการปลอมแปลงทั้งหมดหรือแต่บางส่วน รวมทั้งการลบข้อมูลโดยการย้ายข้อมูลออกจากสื่อที่ใช้ในการบันทึกข้อมูลนั้น ซึ่งทำให้ข้อมูลผิดไปจากต้นฉบับ โดยการกระทำในลักษณะดังกล่าวน่าที่จะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน ถ้าได้กระทำเพื่อให้ผู้หนึ่งผู้ใดหลงเชื่อว่าเป็นข้อมูลคอมพิวเตอร์ที่แท้จริง ถือว่าผู้นั้นกระทำความผิดเกี่ยวกับการปลอมแปลงข้อมูลคอมพิวเตอร์[42]

6) <u>การฉ้อโกงทางคอมพิวเตอร์ (มาตรา 13)</u>

บทบัญญัติมาตรานี้มีขึ้นเพื่อแก้ปัญหาความไม่เพียงพอของความผิดฐานฉ้อโกงตามประมวลกฎหมายอาญาที่ไม่สามารถบังคับใช้กับการฉ้อโกงที่เป็นการแสดงข้อความเท็จต่อคอมพิวเตอร์ที่ถูกตั้งโปรแกรมอัตโนมัติเพื่อให้ส่งมอบทรัพย์สินแก่บุคคลนั้นหรือบุคคลที่สาม ซึ่งผู้ถูกฉ้อโกงในกรณีนี้ไม่เป็นบุคคลตามกฎหมายหากแต่เป็นคอมพิวเตอร์ซึ่งทำงานแทนมนุษย์ ซึ่งลักษณะของการกระทำความผิดจะมีความแตกต่างจากการฉ้อโกงแบบดั้งเดิม กล่าวคือเป็นการกระทำโดยวิธีการแก้ไข เปลี่ยนแปลง ลบข้อมูลคอมพิวเตอร์หรือนำข้อมูลคอมพิวเตอร์เข้าสู่หรือรบกวนการทำงานของระบบคอมพิวเตอร์ของผู้อื่นและโดยการกระทำดังกล่าวทำให้ได้ประโยชน์ในลักษณะที่เป็นทรัพย์สินจากผู้นั้นหรือบุคคลที่สาม

---

[42] สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, <u>คำอธิบายร่างพระราชบัญญัติว่าด้วยอาชญากรรมคอมพิวเตอร์ พ.ศ....</u>[Online],2003, แหล่งที่มา: http://www.ecommerce.or.th/ictlaw/cc/explanation/part2.html [2003, July 17]

7) การเผยแพร่ภาพลามกอนาจาร (มาตรา 14)

บทบัญญัติตามมาตรานี้เป็นการกำหนดให้การเผยแพร่ภาพลามกอนาจารไม่ว่าจะเป็นภาพลามกผู้ใหญ่หรือเด็กอายุต่ำกว่า 18 ปี เป็นความผิดอาญา ซึ่งเป็นความผิดที่เกิดบนคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตโดยเฉพาะ ซึ่งการกระทำดังกล่าวนี้ไม่เป็นความผิดตามประมวลกฎหมายอาญา จึงนับเป็นการบัญญัติกฎหมายเพื่อเสริมความไม่เพียงพอของกฎหมายอาญา

อย่างไรก็ตาม ประเด็นในทางระหว่างประเทศปัจจุบันยังคงมีประเด็นในเรื่องของภาพเสมือนจริงซึ่งเป็นภาพลามกอนาจาร หรือที่เรียกว่า Virtual Pornography ซึ่งผู้เขียนได้กล่าวในบทที่ 3 แล้วว่า แม้หลายประเทศจะมีความลังเลในการกำหนดให้ภาพเสมือนจริงดังกล่าวเป็นความผิดอาญา แต่บางประเทศ เช่นประเทศอังกฤษและสหรัฐอเมริกากำหนดกฎหมายอย่างชัดเจนแล้วว่า การเผยแพร่ภาพเสมือนจริงถือเป็นความผิดอาญาเช่นเดียวกับการเผยแพร่ภาพลามกอนาจาร[43] แต่เมื่อพิจารณาร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของไทย มาตรา 14 ยังไม่มีความชัดเจนในประเด็นนี้ นอกจากนี้เมื่อพิเคราะห์ถ้อยคำตามวรรค 2 แล้ว อาจกล่าวได้ว่าเมื่อองค์ประกอบในเรื่องของอายุเป็นประเด็นสำคัญในการลงโทษผู้กระทำความผิด ไม่ว่าผู้กระทำจะรู้หรือไม่ แสดงให้เห็นลักษณะของภาพลามกที่จะเป็นความผิดตามมาตรานี้ได้ต้องเป็นภาพที่เกิดจากคนจริงๆปรากฏในภาพ ความไม่ชัดเจนในประเด็นนี้ ผู้เขียนเห็นว่าการกำหนดในเรื่องภาพเสมือนจริงให้ชัดเจนน่าจะเป็นวิธีการช่วยให้ลดความไม่แน่นอนในการตีความประเด็นดังกล่าวในกฎหมายไทย ทั้งยังเป็นการกำหนดแนวทางให้ชัดเจนว่า ประเทศไทยมีความเห็นในประเด็นนี้อย่างไร

จากที่ได้กล่าวมาทั้งหมดนี้ ผู้เขียนเห็นว่าร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ฉบับนี้ โดยส่วนใหญ่ครอบคลุมถึงความผิดอาญาเกี่ยวกับอาชญากรรมคอมพิวเตอร์ในประการสำคัญ ทั้งในความผิดเกี่ยวกับระบบคอมพิวเตอร์หรือความผิดเกี่ยวกับข้อมูลคอมพิวเตอร์ ซึ่งยังรวมทั้งความผิดเกี่ยวกับความมั่นคงของรัฐและบทบัญญัติเกี่ยวกับการเผยแพร่ภาพลามกอนาจาร อย่างไรก็ตาม ยังมีบางประเด็นที่ขาดหายไป เช่นในความผิดเกี่ยวกับ

---

[43] ประเทศอังกฤษบัญญัติไว้ใน The Protection of Children Act 1978 แก้ไขเพิ่มเติมโดย The Criminal Justice and Public Order Act 1994 และประเทศสหรัฐอเมริกาบัญญัติอยู่ใน The Child Pornography Prevention Act 1996 หรือ CPPA

การข่มขู่และคุกคามผ่านอินเทอร์เน็ต การกระทำความผิดฐานนี้ได้รับการกล่าวถึงในระหว่างประเทศมากถึงแนวทางการแก้ไขปัญหา ซึ่งทำให้ความผิดฐานนี้ในหลายประเทศมีบทบัญญัติกำหนดเป็นความผิดเฉพาะ หรือปรับใช้กฎหมายอาญาให้ครอบคลุมกับการกระทำผ่านสื่ออินเทอร์เน็ต[44]

นอกจากนี้ ในประเด็นเกี่ยวกับการเผยแพร่ภาพลามกอนาจารที่เป็นภาพเสมือนจริงหรือการทำเทียมภาพนั้น ดังที่ได้กล่าวมาแล้วข้างต้นว่า มาตรา 14 แห่งร่างพระราชบัญญัติฯฉบับนี้กำหนดไว้ไม่ชัดเจน และไม่อาจตีความว่าเป็นความผิดอาญาตามร่างพระราชบัญญัติดังกล่าวได้ การเผยแพร่ภาพประเภทนี้ จึงน่าจะยังไม่สามารถถือได้ว่าเป็นความผิดตามกฎหมายภายในของประเทศไทย การเผยแพร่ภาพลามกที่สร้างขึ้นจากคอมพิวเตอร์จึงไม่เป็นความผิดที่สามารถส่งผู้ร้ายข้ามแดนกันได้

อย่างไรก็ตาม ร่างพระราชบัญญัติดังกล่าวก็ถือได้ว่า เป็นกฎหมายที่กำหนดการกระทำอันเป็นความผิดเกี่ยวกับคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตซึ่งครอบคลุมถึงประเด็นความผิดสำคัญๆไว้ และมีบทกำหนดโทษสำหรับความผิดอาญาตามร่างพระราชบัญญัติไม่ต่ำกว่า 1 ปี ซึ่งกฎหมายฉบับนี้จะเป็นกลไกสำคัญในการช่วยลดอุปสรรคในการส่งผู้ร้ายข้ามแดนในกรณีอาชญากรรมคอมพิวเตอร์ ที่สืบเนื่องจากปัญหาเรื่องหลักความผิดอาญาของทั้งสองประเทศได้และอัตราโทษขั้นต่ำได้

นอกจากการที่รัฐจะบัญญัติกฎหมายภายในเกี่ยวกับอาชญากรรมคอมพิวเตอร์ให้ทันสมัยกับลักษณะพิเศษของอาชญากรรมทางคอมพิวเตอร์แล้ว รัฐจำต้องพัฒนากฎหมายเกี่ยวกับการส่งผู้ร้ายข้ามแดนให้สนองรับกับความผิดดังกล่าวข้างต้น เพื่อที่รัฐจะสามารถให้ความร่วมมือระหว่างประเทศในการส่งผู้ร้ายข้ามแดนได้

---

[44] ดู บทที่ 3 ข้อ 3.1.2 ข้อ 4)

4.2.2 กฎหมายภายในเกี่ยวกับการส่งผู้ร้ายข้ามแดน

เมื่อมีการบัญญัติกฎหมายภายในเกี่ยวกับอาชญากรรมคอมพิวเตอร์ เพื่อให้อาชญากรรมคอมพิวเตอร์เป็นความผิดอาญาตามกฎหมายภายใน รัฐยังต้องปรับปรุงกฎหมายภายในว่าด้วยการส่งผู้ร้ายข้ามแดนให้สนองรับกับกฎหมายอาชญากรรมคอมพิวเตอร์ โดยการแก้ไขกฎหมายส่งผู้ร้ายข้ามแดนให้เปิดช่องทางให้มีการส่งผู้ร้ายข้ามแดนในกรณีอาชญากรรมคอมพิวเตอร์ได้โดยสะดวก เพราะในการส่งผู้ร้ายข้ามแดนนั้น รัฐอาจต้องอาศัยบทบัญญัติแห่งกฎหมายภายในเพื่อให้อำนาจแก่รัฐในการใช้ดุลพินิจในการส่งผู้ร้ายข้ามแดนให้แก่ประเทศอื่น ในกรณีที่ไม่มีสนธิสัญญาส่งผู้ร้ายข้ามแดนหรือสนธิสัญญาไม่ครอบคลุมถึงความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์

ดังนั้น การบัญญัติกฎหมายภายในเกี่ยวกับข้อกำหนดเกี่ยวกับการส่งผู้ร้ายข้ามแดนในกรณีอาชญากรรมคอมพิวเตอร์จึงสามารถเป็นแนวทางหนึ่งในการแก้ปัญหาในกรณีที่ไม่มีสนธิสัญญาหรือสนธิสัญญาส่งผู้ร้ายข้ามแดนไม่ครอบคลุมถึงความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์ อย่างไรก็ตาม ในกรณีนี้ต้องพิจารณาทางปฏิบัติของรัฐประกอบด้วยว่า รัฐนั้นมีความเคร่งครัดในการส่งผู้กระทำความผิดข้ามแดนเพียงไร ซึ่งสามารถแยกพิจารณาเป็น 2 กรณี คือ

1) **ประเทศในกลุ่ม** Common Law

จากการศึกษาทำให้ทราบว่า แนวปฏิบัติของประเทศในกลุ่ม Common Law เช่น ประเทศสหรัฐอเมริกาและประเทศอังกฤษนั้น มักพิจารณาถึงสนธิสัญญากำหนดหน้าที่ของรัฐในการส่งตัวผู้กระทำความผิดข้ามแดนอย่างเคร่งครัด กล่าวคือ ประเทศในกลุ่มนี้จะไม่ส่งผู้ร้ายข้ามแดนในกรณีที่ไม่มีสนธิสัญญาหรือในกรณีที่สนธิสัญญาไม่ครอบคลุมถึงความผิดที่ร้องขอ อย่างไรก็ตาม ในระยะหลังแนวปฏิบัติดังกล่าวคลายความเคร่งครัดลง โดยเปิดโอกาสให้ฝ่ายนิติบัญญัติออกกฎหมายอันเป็นการสร้างความยืดหยุ่นและเปิดช่องให้มีการส่งผู้กระทำความผิดข้ามแดนได้[45] ในกรณีที่ไม่มีสนธิสัญญาหรือสนธิสัญญาไม่ครอบคลุม ซึ่งเป็นการกำหนดเพื่ออำนวยความสะดวกในการส่งผู้ร้ายข้ามแดนเป็นกรณีไป

---

[45] สุเทพ อัตถากร และสฤษดิ์ผล ชมไพศาล, คู่มือการศึกษากฎหมายระหว่างประเทศแผนกคดีบุคคลและคดีอาญา (กรุงเทพมหานคร : สำนักพิมพ์ไทยวัฒนาพานิช, 2516) หน้า 44-45.

แนวทางดังกล่าวนี้ปรากฏอยู่ในกฎหมาย The Computer Misuse Act 1990 ของประเทศอังกฤษ ซึ่งกฎหมายของประเทศอังกฤษฉบับนี้ นอกจากจะกำหนดให้การกระทำความผิดเกี่ยวกับคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตเป็นความผิดอาญาแล้ว ยังกำหนดให้ความผิดตามกฎหมายฉบับนี้เป็นความผิดที่สามารถส่งผู้ร้ายข้ามแดนได้อีกด้วย ซึ่งบทบัญญัติที่อนุญาตให้มีการส่งผู้ร้ายข้ามแดนได้นี้ มีความสำคัญในการให้ความร่วมมือระหว่างประเทศเป็นอย่างมาก เนื่องจากเป็นการขยายความร่วมมือในการส่งผู้ร้ายข้ามแดนโดยไม่ต้องมีการแก้ไขสนธิสัญญาส่งผู้ร้ายข้ามแดน และไม่จำต้องมีสนธิสัญญาว่าด้วยความร่วมมือพิเศษในทางอาญาแต่อย่างใด ซึ่งแนวทางการแก้ปัญหาเช่นนี้ มีประเทศในเครือจักรภพอังกฤษบางประเทศนำแนวทางดังกล่าวไปใช้เช่นกัน[46]

บทบัญญัติที่เป็นข้อกำหนดให้รัฐสามารถส่งผู้ร้ายข้ามแดนได้ ซึ่งได้บัญญัติไว้ในกฎหมายอาชญากรรมคอมพิวเตอร์นั้น มีผลทำให้รัฐสามารถส่งผู้ร้ายข้ามแดนในความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์ได้ ทั้งในกรณีที่ไม่มีสนธิสัญญาระหว่างประเทศกัน และในกรณีที่สนธิสัญญาประเภทระบุฐานความผิดไม่ครอบคลุมถึงความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์ นอกจากนี้ บทบัญญัติที่อนุญาตให้มีการส่งผู้ร้ายข้ามแดนกันได้นั้น ยังช่วยลดความไม่แน่นอนในการพิจารณาส่งผู้ร้ายข้ามแดน ในกรณีที่กฎหมายอาชญากรรมคอมพิวเตอร์ของทั้งสองประเทศมีข้อกำหนดในรายละเอียดที่แตกต่างกันในเรื่องของอัตราโทษ เช่นในความผิดเกี่ยวกับการเจาะระบบคอมพิวเตอร์ และความแตกต่างของกฎหมายทั้งสองประเทศในเรื่องมาตรฐานและขอบเขตการบังคับใช้ เช่นในความผิดเกี่ยวกับภาพลามกอนาจารเด็ก ข่มขู่ หรือ ความผิดเกี่ยวกับระบบคอมพิวเตอร์ เป็นต้น

อย่างไรก็ตาม แนวทางการกำหนดบทบัญญัติให้มีการส่งผู้ร้ายข้ามแดนในกฎหมายภายในนี้ ไม่สามารถแก้ปัญหาในกรณีที่ความผิดที่ร้องขอนั้นไม่เป็นความผิดที่มีลักษณะเป็นความผิดอาญาของทั้งสองประเทศ (Double Criminality)[47] เพราะบทบัญญัติที่เป็นข้อกำหนดให้รัฐสามารถส่งผู้ร้ายข้ามแดนได้นี้ เป็นเพียงบทบัญญัติที่ช่วยอำนวยความสะดวก ซึ่งต้องอยู่ภายใต้หลักเกณฑ์เกี่ยวกับเรื่องความผิดอาญาของทั้งสองประเทศซึ่งเป็นหลักเกณฑ์ที่ได้รับการยอมรับ

---

[46] John T. Soma , Thomas F. Muther , Jr. and Heidi M.L. Brissette, " Transnational extradition for computer crimes : Are new treaties and laws need ?," Harvard Journal on Legislation , 34 : 361.

[47] Ibid.

อย่างแพร่หลายในทางระหว่างประเทศ จนมีสถานะเป็นกฎหมายจารีตประเพณีระหว่างประเทศที่รัฐจำต้องผูกพันและถือปฏิบัติตาม ดังที่ได้ศึกษาแล้วในบทที่ 2 ทั้งนี้เพราะเหตุว่า ประเทศในกลุ่ม Common Law เช่นประเทศอังกฤษและสหรัฐอเมริกานั้น ถือว่า กฎหมายจารีตประเพณีระหว่างประเทศเป็นกฎหมายของประเทศนั้นๆโดยอัตโนมัติ[48] ดังนั้น ในการใช้กฎหมายที่ออกโดยรัฐสภานั้น ศาลจะตีความกฎหมายดังกล่าวไปในทางที่ไม่ขัดต่อกฎหมายระหว่างประเทศ[49]

2) **ประเทศในกลุ่ม** Civil Law

แนวปฏิบัติของประเทศในกลุ่มนี้ มีความยืดหยุ่นในการพิจารณาส่งผู้ร้ายข้ามแดนอยู่แล้ว เนื่องจากโดยส่วนใหญ่กฎหมายภายในเกี่ยวกับการส่งผู้ร้ายข้ามแดนของประเทศในกลุ่มนี้มักกำหนดให้รัฐสามารถส่งผู้ร้ายข้ามแดนให้แก่รัฐอื่นได้แม้ไม่มีสนธิสัญญาส่งผู้ร้ายข้ามแดน โดยอาศัยหลักปฏิบัติต่างตอบแทน ซึ่งเป็นการเปิดช่องทางให้รัฐสามารถส่งผู้ร้ายข้ามแดนแก่รัฐอื่นๆได้[50] ดังนั้น ในส่วนของกฎหมายภายในว่าด้วยการส่งผู้ร้ายข้ามแดนของประเทศในกลุ่ม Civil Law จึงไม่น่าจะเกิดปัญหาในทางปฏิบัติที่ก่อให้เกิดอุปสรรคในการส่งผู้ร้ายข้ามแดนในกรณีอาชญากรรมคอมพิวเตอร์มากนัก

อย่างไรก็ตาม หากกฎหมายภายในว่าด้วยการส่งผู้ร้ายข้ามแดนกำหนดเงื่อนไขเพิ่มเติม ซึ่งผู้เขียนจะได้ยกตัวอย่างในกรณีของประเทศไทย โดยพระราชบัญญัติว่าด้วยการส่งผู้ร้ายข้ามแดน พ.ศ. 2472 มาตรา 4 ซึ่งบัญญัติว่า "แม้จะไม่มีสัญญาส่งผู้ร้ายข้ามแดนก็ดี หากรัฐบาลสยามพิจารณาเห็นเป็นการสมควร ก็อาจส่งตัวบุคคลผู้ต้องหา หรือที่พิจารณาเป็นสัตย์ว่ากระทำความผิดมีโทษอาชญาภายในเขตอำนาจศาลของต่างประเทศใดๆ ให้แก่ประเทศนั้นๆได้ แต่การกระทำผิดเช่นว่านี้ ต้องเป็นความผิดซึ่งกฎหมายสยามกำหนดโทษจำคุกไม่น้อยกว่า 1 ปี"

บทบัญญัติมาตรา 4 ดังกล่าว กำหนดให้รัฐสามารถใช้ดุลพินิจในการส่งผู้ร้ายข้ามแดนได้ แต่ต้องเป็นไปตามเงื่อนไขที่พระราชบัญญัติว่าด้วยการส่งผู้ร้ายข้ามแดนกำหนดอีก

---

[48] M. Akehurst, A modern introduction to international law, 5th ed., George Allen and Unwin, 1984 อ้างถึงใน จุมพต สายสุนทร, กฎหมายระหว่างประเทศ (กรุงเทพมหานคร : โรงพิมพ์เดือนตุลา, 2539), หน้า 108.

[49] เรื่องเดียวกัน, หน้า110.

[50] I.A. Shearer, Extradition in international law, pp.31-32.

ประการหนึ่งคือ ความผิดที่ส่งต้องเป็นความผิดที่ลงโทษได้ตามกฎหมายของไทย โดยมีอัตราโทษจำคุกไม่เกิน1 ปี ดังนั้น หากประเทศไทยต้องการจะให้ความร่วมมือในการส่งผู้ร้ายข้ามแดนในกรณีอาชญากรรมคอมพิวเตอร์ ก็สามารถกระทำได้ หากแต่ประเทศไทยจะต้องมีกฎหมายภายในซึ่งกำหนดให้อาชญากรรมคอมพิวเตอร์เป็นความผิดตามกฎหมายภายในซึ่งมีอัตราโทษจำคุกไม่ต่ำกว่า 1 ปีด้วย

จากที่ได้ทำการศึกษามาทั้งหมดนี้ จะเห็นได้ว่า กระบวนการส่งผู้ร้ายข้ามแดนเป็นวิธีการที่จะนำตัวผู้กระทำความผิดมาลงโทษในรัฐที่มีความเกี่ยวพันกับมูลคดี ซึ่งจะทำให้ผู้กระทำความผิดได้รับการลงโทษ แต่หลักเกณฑ์การส่งผู้ร้ายข้ามแดนในปัจจุบันไม่อาจใช้บังคับกับอาชญากรรมคอมพิวเตอร์ซึ่งเป็นความผิดฐานใหม่ที่มีลักษณะพิเศษได้ เนื่องด้วยหลักเกณฑ์ว่าด้วยการส่งผู้ร้ายข้ามแดนไม่สามารถพัฒนาให้ทันกับความผิดเช่นว่านี้ได้ ประกอบกับประเทศต่างๆมีกฎหมายภายในในเรื่องนี้แตกต่างกัน ซึ่งก่อให้เกิดปัญหาในทางปฏิบัติหลายประการ

อย่างไรก็ตาม กลไกการแก้ไขปัญหาดังกล่าวก็มีอยู่หลายประการเช่นเดียวกัน ไม่ว่าจะเป็นกลไกการแก้ไขปัญหาในระดับระหว่างประเทศและในระดับประเทศ ซึ่งกลไกการแก้ไขปัญหาทั้งสองระดับจำต้องดำเนินไปควบคู่กัน ทั้งนี้เพื่อลดปัญหาและอุปสรรคในการส่งผู้ร้ายข้ามแดนในคดีอาชญากรรมคอมพิวเตอร์ และเพื่อให้การนำตัวผู้กระทำความผิดมาลงโทษภายใต้กรอบของกฎหมายเป็นไปได้อย่างมีประสิทธิภาพ