บทที่ 3
อาชญากรรมคอมพิวเตอร์ และปัญหาในการปรับใช้กฎหมายว่าด้วยการส่งผู้ร้ายข้ามแดนในคดีอาชญากรรมคอมพิวเตอร์

จากการศึกษาถึงหลักเกณฑ์การส่งผู้ร้ายข้ามแดนในบทที่ 2 ไม่ว่าจะเป็นวิวัฒนาการ วิธีการและหลักเกณฑ์ในการพิจารณาส่งผู้ร้ายข้ามแดนแล้ว ในบทที่ 3 นี้ ผู้เขียนจะได้ศึกษาถึงปัญหาในทางปฏิบัติของรัฐในการปรับใช้หลักเกณฑ์ว่าด้วยการส่งผู้ร้ายข้ามแดนกับคดีอาชญากรรมคอมพิวเตอร์ ซึ่งเป็นอาชญากรรมที่มีลักษณะระหว่างประเทศและเป็นอาชญากรรมฐานใหม่ที่เกิดขึ้นจากความก้าวหน้าทางเทคโนโลยี อย่างไรก็ตาม ก่อนที่จะได้ศึกษาถึงปัญหาดังกล่าว จำต้องศึกษาถึงความหมาย ลักษณะและความผิดของอาชญากรรมคอมพิวเตอร์ก่อน เพื่อให้ทราบถึงลักษณะของอาชญากรรมคอมพิวเตอร์ว่า มีลักษณะพิเศษที่แตกต่างจากความผิดอาญาฐานอื่นๆอย่างไร ซึ่งจะนำไปสู่การศึกษาถึงปัญหาในทางปฏิบัติในการส่งผู้ร้ายข้ามแดนในคดีอาชญากรรมคอมพิวเตอร์ต่อไป

3.1 อาชญากรรมคอมพิวเตอร์

เป็นที่เข้าใจกันโดยทั่วไปว่า อาชญากรรมคอมพิวเตอร์ได้แก่การก่ออาชญากรรมที่เกี่ยวข้องกับการใช้คอมพิวเตอร์ในการกระทำความผิด แต่ความจริงแล้วการก่ออาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ อาจไม่ใช่อาชญากรรมคอมพิวเตอร์ในทุกกรณี ซึ่งการทำความเข้าใจถึงลักษณะของอาชญากรรมคอมพิวเตอร์อย่างชัดแจ้งว่ามีลักษณะของการกระทำเช่นไร ก็จำเป็นต้องศึกษาและทำความเข้าใจถึงความหมาย ลักษณะของอาชญากรรมคอมพิวเตอร์ก่อนดังต่อไปนี้

3.1.1 ความหมายและลักษณะของอาชญากรรมคอมพิวเตอร์

ในยุคเริ่มต้นที่มีการผลิตและใช้เครื่องคอมพิวเตอร์ ได้มีการกระทำความผิดต่อเครื่องคอมพิวเตอร์โดยตรง เช่น การลักขโมยเครื่องคอมพิวเตอร์ แผ่นดิสก์ โปรแกรมคอมพิวเตอร์ เป็นต้น ซึ่งในยุคนั้น ถือว่าการกระทำความผิดใดๆที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์ ไม่ว่าจะเป็นการกระทำต่อตัวเครื่องหรือโปรแกรมคอมพิวเตอร์ก็รวมเรียกว่าเป็นอาชญากรรมคอมพิวเตอร์ทั้งสิ้น ซึ่งมหาวิทยาลัย Michigan State ได้จำแนกลักษณะของการกระทำอาชญากรรมคอมพิวเตอร์ไว้ 4 ลักษณะ คือ

1. การกระทำที่เกี่ยวกับเครื่องคอมพิวเตอร์โดยตรง เช่น การทำลายเครื่องคอมพิวเตอร์ การขโมยส่วนประกอบหรือโปรแกรมคอมพิวเตอร์ เป็นต้น
2. การกระทำที่มีเครื่องคอมพิวเตอร์เป็นเป้าหมาย ได้แก่ การเข้าถึงฐานข้อมูลต่างๆ การทำให้ระบบสื่อสารข้อมูลขัดข้อง หรือการกระทำของนักก่อกวนคอมพิวเตอร์ เป็นต้น
3. การกระทำที่ใช้เครื่องคอมพิวเตอร์เป็นเครื่องมือ ได้แก่ การใช้เครื่องคอมพิวเตอร์เป็นเครื่องมือหรืออุปกรณ์ในการกระทำผิด เช่น การฉ้อโกงโดยใช้คอมพิวเตอร์ การส่งภาพลามกอนาจารผ่านระบบเครือข่ายคอมพิวเตอร์ การฟอกเงิน เป็นต้น
4. การกระทำที่นำเครื่องคอมพิวเตอร์เป็นเครื่องช่วยสนับสนุนในการประกอบอาชญากรรมอื่น ได้แก่การกระทำต่างๆที่มิได้นำเครื่องคอมพิวเตอร์ไปใช้โดยตรง แต่เครื่องคอมพิวเตอร์ได้ช่วยให้เกิดผล หรือพฤติกรรมอื่นๆที่ผิดกฎหมายตามมา นอกจากนี้การใช้เครื่องคอมพิวเตอร์ยังทำให้เกิดผลที่รุนแรงกว่าปกติ เช่น การก่ออาชญากรรมเกี่ยวกับเด็ก การข่มขู่ การล่วงเกินหรือรังควานทางเพศ หรือแม้แต่การฆาตกรรม[1]

ต่อมา เมื่อการใช้คอมพิวเตอร์เริ่มมีความแพร่หลายมากขึ้น จึงมีการให้คำจำกัดความหรือความหมายของอาชญากรรมคอมพิวเตอร์ที่เปลี่ยนแปลงไปจากเดิมให้มีความชัดเจน โดยการแยกอาชญากรรมคอมพิวเตอร์ออกจากอาชญากรรมธรรมดาหรืออาชญากรรมโดยทั่วไปที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์ ซึ่งมีผลทำให้การก่ออาชญากรรมธรรมดาหรืออาชญากรรมทั่วไปเป็นเพียงความผิดต่อกฎหมายอาญาธรรมดา โดยไม่เป็นอาชญากรรมคอมพิวเตอร์

ความหมายหรือคำจำกัดความของอาชญากรรมคอมพิวเตอร์ในปัจจุบันจึงได้แก่ การกระทำใดๆที่เป็นความผิดต่อกฎหมายอาญา ซึ่งต้องใช้ความรู้ความสามารถเกี่ยวกับคอมพิวเตอร์ในการกระทำความผิด โดยการกระทำดังกล่าวทำให้ผู้เสียหายได้รับความเสียหาย และทำให้

---

[1] มหาวิทยาลัยมิชิแกน, "เอกสารในการสัมมนาเรื่อง สภาพปัญหาและแนวโน้มอาชญากรรมคอมพิวเตอร์ เสนอที่เมืองพัทยา จังหวัดชลบุรี ระหว่างวันที่ 24-29 พฤศจิกายน 2539, อ้างถึงใน นันทชัย เพียรสนอง, "การใช้เทคโนโลยีสารสนเทศกับผลกระทบทางกฎหมาย," หน้า 27-34.

ผู้กระทำความผิดได้รับผลประโยชน์[2] ดังนั้น การกระทำอาชญากรรมคอมพิวเตอร์ จึงแตกต่างจากการประกอบอาชญากรรมทั่วไปตรงที่การก่ออาชญากรรมทั่วไปนั้น อาชญากรไม่จำเป็นต้องใช้ความรู้ความสามารถพิเศษในการประกอบอาชญากรรม แม้ว่าจะเป็นการกระทำต่อคอมพิวเตอร์หรือเกี่ยวข้องกับคอมพิวเตอร์ก็ตาม เช่น การขโมยเครื่องคอมพิวเตอร์ หรือการทำลายตัวเครื่องคอมพิวเตอร์ให้เสียหายไม่สามารถใช้งานได้ จากตัวอย่างจะเห็นได้ว่า การกระทำดังกล่าวเป็นอาชญากรรมธรรมดาไม่ใช่อาชญากรรมคอมพิวเตอร์ เนื่องจากการขโมยตัวเครื่องคอมพิวเตอร์และการทำลายตัวเครื่องคอมพิวเตอร์นั้น ผู้กระทำความผิดไม่จำต้องใช้ความรู้ความสามารถในเชิงคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ต่างๆ จึงเป็นเพียงการกระทำความผิดอาญาฐานลักทรัพย์และทำให้เสียทรัพย์ แต่หากการกระทำความผิดนั้นอาชญากรจำต้องมีความรู้ความสามารถเกี่ยวกับการใช้คอมพิวเตอร์เพื่อประกอบอาชญากรรม เช่น การขโมยข้อมูลอันเป็นความลับทางคอมพิวเตอร์ หรือการป้อนข้อมูลหรือทำลายชิ้นส่วนของคอมพิวเตอร์ที่ผู้กระทำรู้ว่าจะทำให้เครื่องคอมพิวเตอร์ทำงานหรือมีการประมวลผลผิดไป และเกิดความเสียหาย จึงถือเป็นอาชญากรรมคอมพิวเตอร์[3]

นอกจากนี้ เมื่อการใช้คอมพิวเตอร์ในปัจจุบันมีการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ต การก่ออาชญากรรมคอมพิวเตอร์ จึงได้ขยายขอบเขตไปสู่การกระทำความผิดผ่านเครือข่ายอินเทอร์เน็ตด้วย ดังนั้น อาชญากรรมใดๆที่กระทำผ่านเครือข่ายอินเทอร์เน็ต หรือกระทำต่อเครื่องหรือระบบคอมพิวเตอร์ผ่านเครือข่ายอินเทอร์เน็ต จึงเป็นอาชญากรรมคอมพิวเตอร์เช่นกัน[4] ซึ่งจากความหมายของอาชญากรรมคอมพิวเตอร์ที่ได้กล่าวมาทั้งหมดนี้ จะเห็นได้ว่า อาชญากรรมคอมพิวเตอร์เป็นการกระทำความผิดที่เกี่ยวข้องกับคอมพิวเตอร์ ไม่ว่าจะกระทำผ่านเครือข่ายอินเทอร์เน็ตหรือกระทำต่อเครื่องคอมพิวเตอร์เป้าหมายโดยตรง และต้องอาศัยความรู้

---

[2] นันทชัย เพียรสนอง, "การใช้เทคโนโลยีสารสนเทศกับผลกระทบทางกฎหมาย," (งานวิจัยในการอบรมหลักสูตรผู้บริหารกระบวนการยุติธรรมระดับสูง (บ.ย.ส.) วิทยาลัยการยุติธรรม กระทรวงยุติธรรม, 2539), หน้า 27.

[3] สถาบันกฎหมายอาญา, "รายงานการสัมมนาทางวิชาการ โครงการเวทีความคิดเพื่อการพัฒนากระบวนการยุติธรรมไทย เรื่อง กฎหมายอาชญากรรมทางคอมพิวเตอร์ : แนวทางในการแก้ไขปัญหาอาชญากรรมยุคไอที," บทบัณฑิตย์ 55,1(มีนาคม 2542): 183.

[4] United Nation, "Background Paper for the workshop on crimes related to the computer network," Tenth United Nations Congress on the Prevention of Crime and the Treatment of Ofenders, Vienna, 10-17 April 2000. (Document A/CONF.187/10)

ความสามารถของผู้กระทำความผิดในด้านคอมพิวเตอร์ด้วย ดังนั้น การก่ออาชญากรรมทั่วไปโดยไม่ได้ใช้ความรู้ความสามารถในด้านคอมพิวเตอร์ แต่เกี่ยวข้องกับคอมพิวเตอร์ ก็ไม่ถือว่าเป็นอาชญากรรมคอมพิวเตอร์ หากแต่เป็นเพียงการกระทำความผิดอาญาทั่วไปเท่านั้น

นอกจากลักษณะของอาชญากรรมคอมพิวเตอร์ที่พิจารณาในแง่ของการกระทำ ว่ามีลักษณะของการกระทำอย่างใดดังที่ได้กล่าวข้างต้นแล้ว ลักษณะของอาชญากรรมคอมพิวเตอร์ที่สำคัญอีกประการหนึ่งซึ่งเป็นผลสืบเนื่องจากลักษณะของเครือข่ายอินเทอร์เน็ตที่ไร้พรมแดน คือ อาชญากรรมคอมพิวเตอร์ที่กระทำผ่านเครือข่ายอินเทอร์เน็ตนั้นมีลักษณะเป็นอาชญากรรมที่มีลักษณะระหว่างประเทศหรือเป็นอาชญากรรมข้ามชาติ[5] กล่าวคือ การกระทำความผิดผ่านคอมพิวเตอร์ที่เชื่อมต่อกับเครือข่ายอินเทอร์เน็ต ย่อมทำให้ผลแห่งการกระทำความผิดนั้นขยายไปเกิดในดินแดนของรัฐอื่นๆได้โดยง่าย ซึ่งจากการกระทำความผิดในครั้งหนึ่งอาจทำให้มีรัฐมากกว่าหนึ่งรัฐที่มีความเกี่ยวพันและมีเขตอำนาจรัฐเหนือการกระทำความผิดดังกล่าว นอกจากนี้ สภาพของเครือข่ายอินเทอร์เน็ตที่ไม่มีลักษณะทางกายภาพ ทำให้การกระทำความผิดบนเครือข่ายอินเทอร์เน็ตไม่จำต้องอาศัยดินแดนดังเช่นการกระทำความผิดอาญาอื่นๆ ตลอดจนผู้กระทำความผิดบนเครือข่ายอินเทอร์เน็ตนั้น ก็ไม่ได้มีสภาพบุคคลเหมือนบุคคลธรรมดาที่กระทำความผิดอาญาทั่วไปบนดินแดน หากแต่เป็นการใช้คอมพิวเตอร์เป็นผู้ดำเนินกิจกรรมหรือกระทำความผิดบนเครือข่ายแทนบุคคล[6]

จากที่ได้กล่าวมาทั้งหมดนี้ อาจสรุปลักษณะของอาชญากรรมคอมพิวเตอร์ได้ว่า นอกจากอาชญากรรมคอมพิวเตอร์จะมีลักษณะระหว่างประเทศหรือมีลักษณะเป็นอาชญากรรมข้ามชาติแล้ว อาชญากรรมคอมพิวเตอร์ยังมีลักษณะของการกระทำที่หลากหลาย ไม่ว่าจะเป็นการ

---

[5] United Nations, 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]

[6] เขมชาติ ธีรพงษ์, "ปัญหากฎหมายและแนวทางการแก้ไขปัญหาอันเกิดจากการประกอบกิจกรรมบนเครือข่ายอิเล็กทรอนิกส์ : ปัญหาการใช้เขตอำนาจรัฐและปัญหาที่สืบเนื่องมาจากความไม่เพียงพอของกฎหมายที่มีอยู่ในปัจจุบัน," (วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2543), หน้า 15.

กระทำความผิดต่อระบบข้อมูลคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตโดยตรง และการกระทำความผิดอาญาดั้งเดิมผ่านคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ต โดยใช้คอมพิวเตอร์เป็นผู้กระทำความผิดแทนบุคคล ซึ่งการพิจารณาถึงลักษณะของอาชญากรรมคอมพิวเตอร์ดังกล่าวนี้ ทำให้ทราบถึงความแตกต่างระหว่างอาชญากรรมคอมพิวเตอร์กับอาชญากรรมทั่วไปได้อย่างชัดเจน

เมื่อการกระทำความผิดอาญาที่มีความเกี่ยวข้องกับคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตซึ่งมีลักษณะเป็นอาชญากรรมคอมพิวเตอร์ตามคำนิยามที่ได้กล่าวมาข้างต้นแล้ว ปัญหาที่เกิดขึ้นประการต่อมาคือ การกระทำดังกล่าวจะถือเป็นอาชญากรรมคอมพิวเตอร์ซึ่งเป็นการกระทำที่ผิดต่อกฎหมายอาญาได้นั้น ก็ต่อเมื่อการกระทำเช่นว่านั้นจะต้องได้รับการบัญญัติให้เป็นการกระทำที่เป็นความผิดตามกฎหมายภายในของรัฐเสียก่อน ซึ่งในการกำหนดให้การกระทำเช่นใดบ้างเป็นความผิดอาญานั้น จำต้องพิจารณาถึงแนวโน้มในทางระหว่างประเทศว่ามีการยอมรับความผิดฐานใดเป็นความผิดอาญาอย่างเป็นสากล ซึ่งในหัวข้อต่อไปผู้เขียนจะศึกษาถึงประเภทความผิดของอาชญากรรมคอมพิวเตอร์ที่ประเทศส่วนใหญ่บัญญัติกฎหมายภายในเพื่อกำหนดให้เป็นความผิดอาญา ดังจะกล่าวต่อไปนี้

3.1.2 ประเภทความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์

จากความหมายของอาชญากรรมคอมพิวเตอร์ที่ได้กล่าวมาแล้ว จะเห็นได้ว่าการกระทำอาชญากรรมคอมพิวเตอร์สามารถเกิดได้ในหลายลักษณะ เมื่อการใช้เครือข่ายอินเทอร์เน็ตแพร่หลาย จึงทำให้การกระทำความผิดบนเครือข่ายอินเทอร์เน็ตมีปริมาณสูงขึ้นตามไปด้วย ส่งผลให้เกิดความเสียหายและผลกระทบที่รุนแรงแก่องค์กรภาครัฐและธุรกิจของเอกชน ประเทศส่วนใหญ่จึงได้บัญญัติกฎหมายภายในขึ้นมารองรับสถานการณ์อาชญากรรมคอมพิวเตอร์ การกระทำความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์หลายฐาน และได้รับการยอมรับกันเป็นการทั่วไปว่าเป็นความผิดที่สมควรต้องบัญญัติกฎหมายไว้เพื่อลงโทษต่อผู้ฝ่าฝืน ซึ่งได้แก่ การเผยแพร่ภาพและสื่อลามกอนาจาร, การเผยแพร่ภาพลามกอนาจารเด็ก, การล่อลวงและอนาจารเด็ก, การข่มขู่และการคุกคามทางอินเทอร์เน็ต, การแสดงข้อความที่ก่อให้เกิดความเกลียดชังทางเชื้อชาติ, การกระทำอันเป็นการกระทบต่อความมั่นคงของรัฐ, การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ, การจารกรรมข้อมูลคอมพิวเตอร์, การทำให้เสียหายหรือทำลายข้อมูลหรือโปรแกรมคอมพิวเตอร์ และการฉ้อโกงทางคอมพิวเตอร์ ซึ่งผู้เขียนจะได้กล่าวในรายละเอียดดังต่อไปนี้

1) **การเผยแพร่ภาพและสื่อลามกอนาจาร** (Pornography)

การกระทำการเผยแพร่ภาพลามกอนาจารผ่านเครือข่ายอินเทอร์เน็ตนั้นถือเป็นการก่ออาชญากรรมคอมพิวเตอร์รูปแบบหนึ่ง โดยการนำเอาคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตเป็นช่องทางในการกระทำความผิด เช่น การเผยแพร่ภาพลามกผ่านสื่ออินเทอร์เน็ต การใช้อินเทอร์เน็ตเป็นสถานที่ในการรบกวนผู้อื่นด้วยข้อความหรือภาพที่ไม่เหมาะสม การใช้คอมพิวเตอร์ในการสร้างภาพลามกอนาจาร หรือการใช้คอมพิวเตอร์เป็นเครื่องมือเพื่อให้ความสะดวกในการก่ออาชญากรรมทางเพศ เป็นต้น[7]

วัตถุประสงค์ในการบัญญัติให้การเผยแพร่ภาพลามกอนาจารเป็นความผิดอาญานั้น เนื่องจากการศึกษาพบว่า การเผยแพร่ภาพลามก ส่งผลถึงมาตรฐานในทางศีลธรรมของประชาชนในสังคมเสื่อมทรามลง[8] นอกจากนี้ วัตถุลามกยังอาจเป็นสาเหตุหนึ่งที่ทำให้เกิดอาชญากรรมร้ายแรงประเภทอื่นตามมา เช่น การค้าหญิงและเด็ก การขายบริการทางเพศ การกระทำอนาจารหรือข่มขืนกระทำชำเรา เป็นต้น[9] ซึ่งเหล่านี้ถือเป็นอาชญากรรมที่เป็นภัยต่อสังคม อันจะกระทบต่อความสงบเรียบร้อยและศีลธรรมอันดีของประชาชนได้ การบัญญัติกฎหมายห้ามการเผยแพร่ภาพลามกอนาจารของประเทศต่างๆ จึงมีวัตถุประสงค์เพื่อป้องกันมิให้เกิดอาชญากรรมรวมทั้งปราบปรามและลงโทษผู้กระทำความผิดให้เกิดความเกรงกลัวต่อกฎหมายและไม่กระทำผิดอีก ซึ่งเมื่อการกระทำความผิดดังกล่าวขยายขอบเขตมากระทำบนคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ต ทำให้ประเทศต่างๆ จำต้องหามาตรการในการควบคุมการกระทำความผิด ซึ่งนอกจากมาตรการทางกฎหมายเพื่อปราบปรามผู้กระทำความผิดแล้วหลายประเทศก็มีนโยบายในการป้องกันมิให้เว็บไซต์จากต่างประเทศ ที่นำเสนอภาพลามกอนาจารเผยแพร่ภาพภายในประเทศ โดยการบังคับให้ผู้ให้บริการเครือข่ายอินเทอร์เน็ต (Internet Service Provider หรือ ISP) ตั้งโปรแกรมเพื่อป้องกันมิให้ผู้ใช้บริการภายในประเทศเข้าถึงเว็บไซต์ที่ทางการระบุว่าเป็นเว็บไซต์ที่ไม่เหมาะสม

---

[7] ฐนวรรษ นิติธรรมวิศรุต, "อาชญากรรมคอมพิวเตอร์ : ศึกษาเฉพาะกรณีการเผยแพร่ภาพและสื่อลามกผ่านอินเทอร์เน็ตที่มีคนไทยเป็นผู้เสียหาย," (วิทยานิพนธ์ปริญญามหาบัณฑิต สาขาวิชานิติศาสตร์ บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย, 2544), หน้า 53.

[8] ณรงค์ ใจหาญ, "ความหมายของสิ่งลามก," วารสารนิติศาสตร์, 19(มิถุนายน 2529) : 125.

[9] ธนะชัย มีผดุง, "มาตรการทางกฎหมายในการควบคุมการผลิตและเผยแพร่วัตถุหรือสิ่งของลามก," (วิทยานิพนธ์ปริญญามหาบัณฑิต สาขาวิชานิติศาสตร์ บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย, 2539), หน้า 3.

เช่น ประเทศจีน สิงคโปร์[10] หรือการตั้งโปรแกรมเพื่อตรวจสอบและรายงานต่อทางการ หากพบเว็บไซต์ที่เผยแพร่ข้อมูลผิดกฎหมาย หรือภาพลามก เช่น โปรแกรมที่ถูกเรียกว่า Internet Watch ที่ใช้อยู่ในประเทศอังกฤษ[11]

แม้ประเทศส่วนใหญ่จะมีมาตรการเพื่อยับยั้งการเผยแพร่ภาพลามกอนาจารผ่านอินเทอร์เน็ต แต่เนื่องจากมาตรฐานและกฎเกณฑ์ในเรื่องเกี่ยวกับเพศ และการแสดงออกทางเพศถูกสร้างขึ้นแตกต่างกันไปในแต่ละสังคม ทำให้มาตรการทางกฎหมายที่ใช้บังคับต่อสื่อลามกอนาจารมีมาตรฐานในการพิจารณาที่แตกต่างกันไปในแต่ละประเทศ[12] เนื่องจากสภาพสังคม เศรษฐกิจ การศึกษา วัฒนธรรม และศาสนาของแต่ละสังคมประเทศมีความแตกต่างกัน เช่น ในประเทศที่มีวัฒนธรรมเสรีนิยมทางเพศ เช่น เบลเยี่ยม[13] เนเธอร์แลนด์[14] เห็นว่า การแสดงออกทางเพศเป็นเรื่องปกติที่ไม่ถือว่าเป็นที่ขัดต่อความรู้สึกหรือเป็นสิ่งผิด ดังนั้น เว็บไซต์ที่เผยแพร่ภาพและการแสดงลามกจากผู้ให้บริการอินเทอร์เน็ตจากประเทศเหล่านี้ จึงสามารถกระทำได้โดยเสรีและไม่ผิดกฎหมาย อย่างไรก็ตาม แม้จะมีบางประเทศไม่ถือว่าการเผยแพร่ภาพลามกอนาจารผู้ใหญ่เป็นความผิดอาญา แต่ก็ยังมีหลายประเทศ ที่มีกฎหมายภายในที่บัญญัติให้การกระทำดังกล่าว เป็นความผิดอาญา เช่น ประเทศแคนาดา[15] อังกฤษ[16] เยอรมนี[17] เดนมาร์ก[18] ฟินแลนด์[19] ฝรั่งเศส[20]

---

[10] Antonette Desir, Pedophilia on the internet and in our society[Online],1999, May 5, Available from : http://www.loyola.edu/dept/philosophy/techne/desir.html [2002, Dec 18]

[11] Yaman Akdeniz, "The Regulation of Pornography and Child Pornography on the Internet," The Journal of Information, Law and Technology [Online], 1997, Feb 28. Available from : http://elj.warwick.ac.uk/jilt/internet/97_1akdz/akdeniz.htm [2002, Nov.21]

[12] ฐนวรรษ นิติธรรมวิศรุต, "อาชญากรรมคอมพิวเตอร์ : ศึกษาเฉพาะกรณีการเผยแพร่ภาพและสื่อลามกผ่านอินเทอร์เน็ตที่มีคนไทยเป็นผู้เสียหาย," หน้า 55.

[13] Laura J. Lederer, The protection Project, Commercial Sexual Exploitation of Woman and Children : A Human Rights Report[Online],(2001, Jan), Available from : http://209.190.246.239/protectionproject/Hrrpdf/Belgium.pdf [2002, Dec. 24]

[14] 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) : 340.

[15] Canada Criminal Code Section 163

สิงคโปร์[21] ฮ่องกง[22] ญี่ปุ่น[23] และประเทศไทย[24] เป็นต้น ซึ่งปัญหาความแตกต่างกันของกฎหมาย รวมถึงมาตรฐานการบังคับใช้กฎหมายของแต่ละประเทศนี้ ทำให้เกิดปัญหาการส่งผู้ร้ายข้ามแดน เนื่องจากการกระทำความผิดบนเครือข่ายอินเทอร์เน็ตมีลักษณะไร้พรมแดน ซึ่งผู้เขียนจะได้กล่าวถึงปัญหาดังกล่าวโดยละเอียดต่อไป

2) **การเผยแพร่ภาพลามกอนาจารเด็ก** (Child Pornography)

ลักษณะของการเผยแพร่ภาพลามกอนาจารเด็กผ่านเครือข่ายอินเทอร์เน็ตนั้นมีลักษณะที่คล้ายกับการเผยแพร่ภาพลามกอนาจารเด็กโดยทั่วไป โดยเป็นการแสดงภาพกิจกรรมทางเพศใด ๆ หรือภาพลามกที่นำเด็กมาเกี่ยวข้องด้วย ภาพลามกเด็กจึงไม่ได้จำกัดอยู่ที่ภาพเปลือยเด็ก แต่รวมไปถึงภาพการมีเพศสัมพันธ์กับเด็ก ภาพการข่มขืน และทารุณกรรมเด็ก ภาพถ่ายทอดสดของผู้ใหญ่กำลังกระทำชำเราเด็กด้วย อย่างไรก็ตาม เมื่อเป็นการกระทำผ่านเครือข่ายอินเทอร์เน็ต ยังมีการกระทำที่อาศัยเทคโนโลยีคอมพิวเตอร์ในการกระทำความผิด เช่น การสร้างภาพเสมือนจริง (Virtual Child Pornography) เป็นภาพลามกเด็ก ซึ่งการกระทำดังกล่าวยังเป็นปัญหาทางด้านกฎหมายของบางประเทศว่า กฎหมายห้ามการเผยแพร่ภาพลามกเด็ก จะ

---

[16] The Protection of Children Act Section 1 (1) แก้ไขเพิ่มเติมโดย The Criminal Justice and Public Order Act 1994 of UK

[17] German Criminal Code Section 184 (1) และ The Law on the Dissemination of Publications and Other Media Morally harmful to Youth. Section 1 , 21

[18] Danish Criminal Code Section 232-234

[19] Finnish Penal Code Chapter 20 Section 9

[20] France New Penal Code. Article 227-24 , 227-28 , R624-2

[21] 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 : 341.

[22] Ibid.

[23] Japan Penal Code Article 175

[24] ประมวลกฎหมายอาญา ม. 287 และ พ.ร.บ.ปรามการทำให้แพร่หลาย และการค้าวัตถุลามก พ.ศ.2471

ครอบคลุมถึงภาพเสมือนจริงเหล่านี้ หรือไม่[25] เนื่องจากแม้ภาพจากการสร้างของคอมพิวเตอร์ดังกล่าวจะดูเหมือนเป็นภาพลามกอนาจารเด็กจริงๆก็ตาม แต่การผลิตภาพดังกล่าวไม่ได้ใช้เด็กในการกระทำความผิด

การเผยแพร่ภาพลามกอนาจารเด็กผ่านเครือข่ายอินเทอร์เน็ตถือเป็นการล่วงละเมิดทางเพศแก่เด็กอย่างหนึ่งตามอนุสัญญาแห่งสหประชาชาติว่าด้วยสิทธิเด็ก ค.ศ.1989[26] ซึ่งในปัจจุบันประเทศต่างๆ เกือบทุกประเทศทั่วโลก ได้ลงนามเป็นภาคีในอนุสัญญาว่าด้วยสิทธิเด็กแล้ว แสดงให้เห็นถึงมาตรฐานในทางระหว่างประเทศที่นานาประเทศได้ยอมรับร่วมกันว่า การแสวงประโยชน์ทางเพศจากเด็ก เช่น การนำเด็กมามีส่วนร่วมในการแสดงภาพลามก หรือการบังคับให้เด็กมีส่วนร่วมในการแสดงทางเพศผ่านทางอินเทอร์เน็ตเป็นการกระทำที่ผิด และเป็นหน้าที่ของรัฐต่าง ๆ ต้องร่วมมือกันป้องกันและปราบปราม โดยรัฐภาคีต่างมีพันธกรณีตามอนุสัญญาที่ต้องมีมาตรการที่เหมาะสม ทั้งทางด้านนิติบัญญัติ บริหาร ตุลาการ และด้านสังคมอื่น ๆ ในการคุ้มครองเด็ก จากการถูกละเมิดสิทธิตามอนุสัญญา โดยไม่ถือว่าเป็นเรื่องของเสรีภาพในการแสดงออกทางเพศ Prof. Ulrich Sieber ระบุว่า แม้จะปรากฏว่าหลายประเทศมีบทบัญญัติแห่งรัฐธรรมนูญให้ความคุ้มครองเสรีภาพในการแสดงความเห็น แต่โดยทั่วไปแล้วทุกประเทศถือว่าภาพลามกอนาจารเด็กไม่อยู่ภายใต้ความคุ้มครองตามรัฐธรรมนูญดังกล่าว[27] ซึ่งในปัจจุบันประเทศส่วนใหญ่

---

[25] Michael Landau, The first amendment and virtual child pornography[Online], July 2002, Available from: http://www.gigalaw.com/articles/2002/landau-2002-07.html [2002, Nov 27]

[26] ข้อ 34 อนุสัญญาสิทธิเด็ก

" รัฐภาคี รับที่จะคุ้มครองเด็กจากการแสวงประโยชน์ทางเพศ และการกระทำทางเพศที่มิชอบทุกรูปแบบ เพื่อการนี้ รัฐภาคีจะดำเนินมาตรการที่เหมาะสมทั้งปวง ทั้งมาตรการภายในประเทศ และมาตรการทวิภาคีและพหุภาคี เพื่อป้องกัน

ก) การชักจูง หรือบีบบังคับเด็กให้มีส่วนร่วมในกิจกรรมทางเพศใดๆ ที่ไม่ชอบด้วยกฎหมาย

ข) การแสวงประโยชน์จากเด็กในการค้าประเวณี หรือการกระทำอื่นๆ ที่เกี่ยวกับเพศที่ไม่ชอบด้วยกฎหมาย

ค) การแสวงประโยชน์จากเด็กในการแสดงลามกอนาจาร และที่เกี่ยวกับสิ่งลามกอนาจาร"

[27] Ulrich Sieber, Criminal law provisions against child pornography

ตรากฎหมายภายในเพื่อกำหนดให้การเผยแพร่ภาพลามกอนาจารเด็กทางอินเทอร์เน็ตเป็นความผิดอาญา เช่น เบลเยี่ยม[28] เดนมาร์ก[29] เยอรมนี[30] ฟินแลนด์[31] ฝรั่งเศส[32] อิตาลี[33] ญี่ปุ่น[34] แคนาดา[35] เนเธอร์แลนด์[36]ออสเตรีย[37] สวีเดน[38] สวิตเซอร์แลนด์[39] อังกฤษ[40] และสหรัฐอเมริกา[41] เป็นต้น

ปัญหาการเผยแพร่ภาพลามกอนาจารเด็กผ่านเครือข่ายอินเทอร์เน็ตในปัจจุบันมิได้จำกัดขอบเขตของการกระทำความผิดเพียงแค่ในประเทศเท่านั้น หากแต่สามารถขยายขอบเขตของการกระทำเป็นความผิดข้ามชาติ ดังเช่นคดีของนาย Eric Frankin Rosser อายุ 48 ปี เชื้อสาย American ครูสอนดนตรีเด็กในกรุงเทพฯ ประเทศไทย ซึ่งตำรวจสืบสวนกลางสหรัฐ หรือ FBI สืบสวนพบว่า นาย Rosser ได้กระทำการผลิตและเผยแพร่ภาพและวีดีโอแสดงการมีเพศสัมพันธ์

[Online],1999, Available from : http://www.jura.Uni-wuerzburg.De [2002,Nov.21] p.8.

[28] Belgium Criminal Code Article 383 bis

[29] Danish Criminal Code Section 235

[30] Germany Criminal Code Section 184, Section 3-5

[31] Finnish Criminal Code Chapter 17 Section 18

[32] France New Penal Code Article 227-23

[33] Italy Penal Code Article 600 ter และ Article 600 quarter

[34] Japan Criminal Law on Child Prostitution and Child Pornography Article 7

[35] Canada Criminal Code Section 163.1

[36] Netherlands Criminal Code Article 240 b

[37] Austria Criminal Code Section 207 a

[38] Sweden Criminal Code Chapter 16 Section 10 a

[39] Swiss Criminal Code Article 197 Ziff. 3

[40] UK Protection of Children Act 1978 และ UK Criminal Justice Act 1988 Section 160

[41] U.S.C. Title 18 Section 2252 (1994)

ระหว่างเขากับเด็กหญิงอายุ 11 ปี ผ่านอินเทอร์เน็ต เจ้าหน้าที่ตำรวจของไทยค้นที่พักอาศัย ของนาย Rosser และพบภาพและวีดีโอลามกเด็กอายุไม่เกิน 15 ปี จำนวนมาก[42]

นอกจากรูปแบบการกระทำความผิดข้ามชาติที่ได้กล่าวมาข้างต้นแล้ว ในบางกรณีการกระทำความผิดยังมีรูปแบบเป็นการกระทำระหว่างกลุ่มสมาชิกที่นิยมการมีเพศสัมพันธ์กับเด็ก เช่น กลุ่มเครือข่าย Orchid Club โดยตำรวจของมลรัฐแคลิฟอร์เนีย ประเทศสหรัฐอเมริกา พบว่ากลุ่ม Orchid Club เป็นกลุ่มเครือข่ายผู้นิยมเด็ก ซึ่งแพร่กระจายอยู่ในหลายประเทศ เช่น สหรัฐอเมริกา ฟินแลนด์ ออสเตรเลีย แคนาดา เป็นต้น โดยสมาชิกจะติดต่อกันผ่านเครือข่ายอินเทอร์เน็ตเพื่อแลกเปลี่ยนประสบการณ์ทางเพศกับเด็กของตนให้สมาชิกอื่นทราบ รวมทั้งการเผยแพร่ Video Conference และภาพการแสดงกิจกรรมทางเพศร่วมกับเด็กผ่านทางอินเทอร์เน็ต ซึ่งในคดีนี้ คณะลูกขุนใหญ่แห่งมลรัฐแคลิฟอร์เนียได้มีคำสั่งอนุญาตให้ฟ้องคดีผู้ร่วมกันกระทำความผิดทั้งผู้กระทำความผิดที่อยู่ในประเทศสหรัฐอเมริกาและที่อยู่ในต่างเทศ ในข้อหาร่วมกันกระทำความผิดในการเผยแพร่ภาพลามกอนาจารเด็ก[43]

จากที่ได้กล่าวมาทั้งหมด จะเห็นได้ว่า แม้การเผยแพร่ภาพลามกอนาจารเด็กผ่านเครือข่ายอินเทอร์เน็ตจะกระทำกันในกลุ่มสมาชิก โดยไม่ได้เผยแพร่สู่สาธารณะชนโดยไม่มีขอบเขตจำกัด แต่เนื่องจากกฎหมายเกี่ยวกับภาพลามกอนาจารเด็ก มีวัตถุประสงค์ในการคุ้มครองการล่วงละเมิดทางเพศแก่เด็ก ดังนั้น ไม่ว่าจะเป็นการกระทำเฉพาะกลุ่มบุคคลก็ถือเป็นการกระทำที่เป็นความผิด ซึ่งการที่ประเทศส่วนใหญ่มีกฎหมายกำหนดให้การเผยแพร่ภาพลามกอนาจารเด็กเป็นความผิดตามกฎหมายภายใน ย่อมทำให้การส่งผู้ร้ายข้ามแดนในความผิดฐานนี้สามารถดำเนินไปได้โดยปราศจากอุปสรรคด้านความแตกต่างของกฎหมาย โดยจะได้กล่าวในรายละเอียดต่อไป

---

[42] The Association of Internet Hotline Provider in Europe, Child pornography [Online],(n.d.), Available from: http://www.inhope.org/english/problem/child.htm [2002, April 30]

[43] Yaman Akdeniz, United States section of regulation of child pornography on the internet : Cases and materials related to child pornorgraphy on the internet [Online],(n.d.), Available from: http://www.cyberrights.org/reports/uscases.htm [2002,Nov.21]

3) **การล่อลวงและอนาจารเด็ก** (Pedophilia)

ในปัจจุบันลักษณะของการล่อลวงและอนาจารเด็กเปลี่ยนแปลงรูปแบบจากการกระทำตามสถานที่ต่างๆ เช่น โรงเรียนหรือสวนสาธารณะ พัฒนาเป็นการกระทำโดยผ่านเครือข่ายอินเทอร์เน็ต โดยการล่อลวงเด็กผ่านเครือข่ายอินเทอร์เน็ตจะกระทำโดยใช้การสนทนากับเด็กผ่านทางห้องสนทนา (Chat Room) หรือทางช่องข่าว (News Group) ซึ่งผู้หลอกลวงจะอาศัยลักษณะพิเศษของการสนทนาทางอินเทอร์เน็ตที่ผู้สนทนาจะไม่รู้จักตัวตนที่แท้จริงของอีกฝ่ายหนึ่งเพื่อการล่อลวง ซึ่งเมื่อเด็กถูกลวงให้ออกไปนอกบ้านก็อาจถูกกระทำอนาจาร ข่มขืน ถูกบังคับให้ร่วมกิจกรรมทางเพศในรูปแบบต่าง ๆ การลักพาตัว หรือแม้แต่การฆาตกรรม ซึ่งคดีที่เคยเกิดขึ้น คือคดีการล่อลวงเด็กชายแซม แมนซี วัย 14 ปี โดยผู้เสียหายรู้จักกับจำเลยในห้องสนทนาทางอินเทอร์เน็ต จำเลยกระทำการล่อลวงผู้เสียหายให้ออกมาพบ ทำผู้เสียหายถูกจำเลยข่มขืน และถ่ายภาพเปลือยเก็บไว้ โดยนอกจากจำเลยจะได้กระทำความผิดต่อผู้เสียหายแล้ว เจ้าหน้าที่ตำรวจยังสืบทราบว่าจำเลยได้กระทำการข่มขืนและฆาตกรรมเด็กชายอีกรายหนึ่งอีกด้วย[44]

นอกจากคดีนี้แล้ว การกระทำความผิดฐานนี้ยังมีการกระทำการเป็นกลุ่มเครือข่ายที่กระจายกันอยู่ในหลายประเทศ เป็นการรวมตัวเป็นกลุ่มของบรรดาผู้นิยมเด็ก ซึ่งปัจจุบันเกิดเครือข่ายของกลุ่มผู้นิยมเด็กขึ้นหลายกลุ่ม เช่น กลุ่ม Orchid Club, กลุ่ม wOnderland กลุ่ม The Boylove Manifesto เป็นต้น เครือข่ายสมาชิกของกลุ่มจะกระจายกันอยู่หลายประเทศ มีความเชี่ยวชาญในการหลบหนีการจับกุมของเจ้าหน้าที่ตำรวจ โดยเว็บไซต์และห้องสนทนาเหล่านี้จะย้ายไปตามประเทศต่างๆ ทั่วโลกอยู่เสมอเพื่อป้องกันการแกะรอยไปยังต้นตอจากบรรดาเจ้าหน้าที่ตำรวจของแต่ละประเทศ ทำให้การติดตามจับกุมตัวผู้กระทำความผิดมีอุปสรรคมากยิ่งขึ้น อย่างไรก็ตาม ในที่สุดทีมสืบสวนสอบสวนร่วมระหว่างประเทศในกลุ่มสหภาพยุโรปและสหรัฐอเมริกา ได้ร่วมมือกันจับกุมกลุ่มบุคคลนิยมเด็กกลุ่มใหญ่ได้เป็นผลสำเร็จ โดยในคดีนี้ผู้กระทำผิดได้ร่วมกันล่วงละเมิดทางเพศเด็กกว่า 45 คน (37 คน เป็นเด็กชาวอเมริกัน) ซึ่งเด็กทั้งหมดมีอายุระหว่าง 2 ถึง14 ปี กลุ่มผู้กระทำความผิดถูกดำเนินคดีในศาลมลรัฐทางตะวันออกของมลรัฐแคลิฟอริเนีย (US. District Court in the Eastern District of California) มีผู้ต้องหา

---

[44] จิตราภรณ์ วนัสพงศ์, "อินเทอร์เน็ต : เทคโนโลยีใหม่ทำร้ายเด็ก," บทบัณฑิตย์ 55 (มีนาคม 2542): หน้า 58 – 59.

ทั้งหมด 15 คน เป็นชาวอเมริกัน 9 คน จาก 7 มลรัฐ และผู้ต้องหาอีก 6 คน เป็นชาวเดนมาร์ก สวิตเซอร์แลนด์ และเนเธอร์แลนด์[45]

การกระทำการล่อลวงเด็กเพื่อล่วงละเมิดทางเพศของกลุ่มนิยมเด็กนี้ มักมีความเกี่ยวพันอย่างใกล้ชิดกับการผลิตภาพลามกอนาจารเด็ก เนื่องจากการได้มาซึ่งภาพลามกเด็ก กลุ่มนิยมเด็กต้องใช้วิธีการล่อลวงเด็ก เพื่อให้มาร่วมกิจกรรมทางเพศกับตน เมื่อการล่อลวงเด็กผ่านเครือข่ายอินเทอร์เน็ตมีการกระทำมากขึ้น ดังนั้น ในปัจจุบันประเทศต่าง ๆ จึงมีความตื่นตัวในปัญหาการล่อลวงเด็กผ่านทางอินเทอร์เน็ตอย่างมาก เนื่องจากการกระทำเช่นนี้เป็นการกระทำที่นำไปสู่การก่ออาชญากรรมทางเพศต่อเด็ก ซึ่งกฎหมายภายในของประเทศต่างๆทั่วโลกก็ต่างกำหนดให้การข่มขืนและกระทำอนาจารต่อเด็กเป็นความผิดอาญาอยู่แล้ว นอกจากความผิดเกี่ยวกับเพศที่กระทำต่อเนื้อตัวร่างกายโดยตรงแล้ว กฎหมายอาญาของบางประเทศยังมีขอบเขตกว้างถึงขนาดกำหนดให้การพูดคุยกับเด็กผ่านทางอินเทอร์เน็ตในลักษณะแนะนำ ชักจูง เกี่ยวกับกิจกรรมทางเพศ หรือการส่งถ้อยคำลามกแก่เด็กเป็นความผิดอาญา แม้ว่าจะยังไม่มีการข่มขืนหรือกระทำอนาจารต่อเด็กในทางร่างกายเลยก็ตาม เช่น กฎหมายอาญาของประเทศแคนาดา[46] , เยอรมนี[47] และสหรัฐอเมริกา[48] เป็นต้น ซึ่งทำให้สามารถจับกุมผู้กระทำความผิดได้ทันที โดยไม่ต้องรอให้เกิดอาชญากรรมรุนแรงอื่นๆที่จะเกิดขึ้นต่อตัวเด็กก่อน

4) การข่มขู่ และการคุกคามทางอินเทอร์เน็ต (Cyber-stalking)

การข่มขู่และการคุกคามทางอินเทอร์เน็ต แปลมาจาก คำว่า Cyber-stalking ซึ่งคำๆนี้ ในต่างประเทศยังไม่มีการให้คำนิยามที่ชัดเจน แต่ Cyber-stalking ถูกใช้เรียกแทนการกระทำการข่มขู่ผู้อื่นโดยใช้อินเทอร์เน็ต จดหมายอิเล็กทรอนิกส์ (E-Mail) หรือเครื่องมือสื่อสารทาง

---

[45] Web child porn ring broken [Online],10 August 2002, Available from: http://www.cnn.com. [2003, Jan 5]

[46] Canada Criminal Code Section 163.1 (1) (b)

[47] German Criminal Code Section 176 (3)

[48] The Child Online Protection Act (COPA), U.S.C. Title 47 Section 223 (e)(6) และ U.S.C. Title 18 Section 2425

อิเล็กทรอนิกส์อื่นใด[49] ในอดีตการข่มขู่และการคุกคามผู้อื่นผ่านเครื่องมือสื่อสาร เช่น โทรศัพท์ เกิดขึ้นมานานแล้ว เมื่อเทคโนโลยีทางการสื่อสารด้านเครือข่ายอินเทอร์เน็ตพัฒนาขึ้น การกระทำดังกล่าวจึงขยายขอบเขตของการกระทำมายังอินเทอร์เน็ต

การกระทำการข่มขู่ผ่านเครือข่ายอินเทอร์เน็ตจะมีได้หลายรูปแบบ เช่น การข่มขู่ผ่านจดหมายอิเล็กทรอนิกส์ซึ่งมีลักษณะเหมือนการข่มขู่แบบเดิมทั่วไป เพียงแต่เปลี่ยนการใช้สื่อกลางมาเป็นการส่งจดหมายอิเล็กทรอนิกส์แทนการใช้โทรศัพท์หรือการใช้จดหมายธรรมดา นอกจากนี้ยังมีวิธีการข่มขู่ที่แตกต่างจากการกระทำในรูปแบบดั้งเดิม คือการข่มขู่โดยการคุกคามเหยื่อขณะที่อยู่บนระบบเครือข่าย หรือการสร้างข้อมูลเท็จที่สร้างความเสื่อมเสียแก่ชื่อเสียงของเหยื่อและเผยแพร่ทางอินเทอร์เน็ต รวมถึงการส่งไวรัสคอมพิวเตอร์ให้แก่เหยื่อเพื่อจงใจสร้างความเสียหายในลักษณะคุกคาม[50] เป็นต้น การกระทำเช่นนี้ ในหลายประเทศบัญญัติกฎหมายไว้ว่าเป็นความผิดเพื่อใช้บังคับกับการข่มขู่ซึ่งกระทำผ่านเครือข่ายอินเทอร์เน็ต เช่น ประเทศสหรัฐอเมริกา, อังกฤษ แคนาดาและออสเตรเลีย เป็นต้น[51]

ในประเทศสหรัฐอเมริกา มีกฎหมายหลายฉบับที่บัญญัติให้การข่มขู่ผ่านอินเทอร์เน็ตเป็นความผิดอาญา กฎหมายของรัฐบาลกลางสหรัฐอเมริกา กำหนดให้การส่งคำข่มขู่เพื่อเรียกค่าไถ่, การข่มขู่ว่าจะลักพาตัว หรือจะทำร้ายบุคคลใดๆ หรือการข่มขู่ว่าจะทำลายทรัพย์สิน หรือชื่อเสียงของบุคคลใดๆ ผ่านการสื่อสารไม่ว่าในรูปแบบใด เป็นความผิดอาญา[52]

---

[49] Justice Department, Cyber-stalking : A new challenge for law enforcement and industry, a report from the attorney general to the vice president [Online],August 1999, Available from: http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm [2002, June 20]

[50] Emma Ogilvie, Cyberstalking [Online],September 2000, Available from: http://www.aic.gov.au/publications/tandi/ti166.pdf [2002, June 14]

[51] John T. Soma, Thomas F. Muther , Jr. and Heidi M.L. Brissette. "Transnational extradition for computer crimes: Are new Treaties and laws needed ?" Harvard Journal on Legislation , 34 : 355.

[52] U.S.C. Title 18 Section 875

นอกจากประเทศสหรัฐอเมริกาแล้ว ในประเทศอังกฤษ มีกฎหมายที่กำหนดให้การข่มขู่ผ่านอินเทอร์เน็ตเป็นความผิดอาญาโดยกำหนดไว้ใน Section 1 The Malicious Communications Act 1998 ซึ่งกำหนดให้การส่งข้อความข่มขู่ผู้อื่นผ่านระบบการสื่อสารอิเล็กทรอนิกส์เป็นความผิดอาญา อย่างไรก็ตาม เนื่องจากความผิดตามพระราชบัญญัตินี้เป็นความผิดเล็กน้อยที่มีโทษต่ำเพียงจำคุกไม่เกิน 6 เดือน และปรับไม่เกิน 5,000 ปอนด์ พระราชบัญญัติฉบับนี้จึงใช้ถูกบังคับใช้ในชั้นเจ้าหน้าที่ตำรวจ (เพื่อเปรียบเทียบปรับผู้ต้องหา) มากกว่าในชั้นศาล อย่างไรก็ตาม ประเทศอังกฤษมีกฎหมายอีกฉบับหนึ่ง คือ The Protection from Harassment Act 1997 ซึ่งมีโทษสูงกว่ากล่าวคือ โทษจำคุกไม่เกิน 5 ปี และมีบทบัญญัติให้ศาลสามารถมีคำสั่งยับยั้งมิให้จำเลยติดต่อกับเหยื่ออีก[53] ซึ่งกฎหมายฉบับดังกล่าวของอังกฤษเป็นกฎหมายที่ใช้กับการข่มขู่โดยทั่วไปแต่บังคับใช้กฎหมายให้ครอบคลุมถึงการกระทำความผิดผ่านอินเทอร์เน็ตด้วย[54] ในขณะประเทศออสเตรเลีย บทบัญญัติเรื่องเดียวกันนี้บัญญัติอยู่ใน Criminal Code Stalking Amendment Act 1999 Chapter 33 A Section 359 B และในประเทศแคนาดาบัญญัติอยู่ใน Section 264 Canada's Criminal Code (แก้ไขเพิ่มเติม ปี ค.ศ.1993) กฎหมายทั้ง 2 ฉบับนี้ ได้รับการแก้ไขให้ครอบคลุมถึงการกระทำความผิดผ่านทางอินเทอร์เน็ตด้วย[55]

ดังนั้น จะเห็นได้ว่าแม้หลายประเทศมีกฎหมายเกี่ยวกับการข่มขู่ แต่มีเพียงไม่กี่ประเทศที่มีกฎหมายเกี่ยวกับการข่มขู่ผ่านเครือข่ายอินเทอร์เน็ตโดยเฉพาะ ในขณะที่อีกหลายประเทศนำกฎหมายอาญาดั้งเดิมมาบังคับใช้กับการข่มขู่ผ่านเครือข่ายอินเทอร์เน็ต[56] ซึ่งการปรับใช้กฎหมายทั่วไปกับการกระทำผ่านเครือข่ายอินเทอร์เน็ตของแต่ละประเทศจะก่อให้เกิดปัญหาข้อขัดข้องหรือความยุ่งยากในการปรับใช้อย่างไรซึ่งก็ขึ้นอยู่กับลักษณะกฎหมายและระบบ

---

[53] Neil Addison, UK cyberstalking law [Online],(n.d.), Available from : http://uk.wirepatrol.org/stalking/uk_stalkinglaw.html [2003, Jan 6]

[54] 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 : 355.

[55] Neil Addison, UK cyberstalking law [Online],(n.d.), Available from : http://uk.wirepatrol.org/stalking/uk_stalkinglaw.html [2003, Jan 6]

[56] 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 : 355.

กฎหมายของประเทศนั้นๆ อย่างไรก็ตาม การนำกฎหมายทั่วไปมาบังคับใช้กับการกระทำผ่านเครือข่ายอินเทอร์เน็ตย่อมไม่สมบูรณ์เท่ากับกฎหมายที่ถูกบัญญัติไว้เพื่อใช้กับกรณีอาชญากรรมคอมพิวเตอร์ เนื่องด้วยการกระทำความผิดแบบดั้งเดิมกับการกระทำผ่านเครือข่ายอินเทอร์เน็ตมีลักษณะที่แตกต่างกันนั่นเอง

5) **การแสดงข้อความที่ก่อให้เกิดความเกลียดชังทางเชื้อชาติ** (Hate Speech)

การแสดงข้อความที่ก่อให้เกิดความเกลียดชังทางเชื้อชาติ ในต่างประเทศใช้คำว่า Hate Speech ซึ่งหมายถึง การพูดหรือการแสดงความเห็นที่มีลักษณะโจมตี ขู่เข็ญ คุกคาม บุคคลหรือกลุ่มบุคคลอื่น หรือเป็นการกระตุ้น ยุยงส่งเสริมให้เกิดความเกลียดชังและการแบ่งแยก โดยมีมูลเหตุมาจากเชื้อชาติ สัญชาติ เผ่าพันธุ์ เพศ หรือ ศาสนา[57] Hate Speech จึงเป็นการแสดงความคิดเห็นหรือข้อความที่กระทบต่อความรู้สึกในทางจิตใจของกลุ่มเป้าหมายโดยตรง กล่าวคือ ทำให้ผู้ถูกกระทำรู้สึกว่าถูกละเมิดศักดิ์ศรีและสิทธิที่จะได้รับการยอมรับและปฏิบัติอย่างเท่าเทียม จากความเป็นมาในประวัติศาสตร์ทำให้ทราบว่า ความขัดแย้งทางด้านเชื้อชาติ ศาสนา ลัทธิทางการเมือง ความเกลียดชังกลุ่มบุคคลที่มีความแตกต่างจากกลุ่มของตน หรือความคิดชาตินิยม เป็นสาเหตุสำคัญของการเกิดสงคราม ในอดีตการเผยแพร่ข้อความที่ก่อให้เกิดความเกลียดชังทางด้านเชื้อชาติ มีขอบเขตจำกัดโดยสภาพภูมิศาสตร์ กล่าวคือ การเผยแพร่ข้อความจำกัดอยู่เพียงแค่ในประเทศเดียว จึงก่อให้เกิดผลกระทบในวงแคบ แต่ในปัจจุบัน ได้มีการขยายขอบเขตการกระทำความผิดผ่านเครือข่ายอินเทอร์เน็ต ซึ่งในปัจจุบัน เว็บไซต์ของกลุ่มเรียกร้องสิทธิ หรือกระดานแสดงความเห็นของฟรีเว็บไซต์ต่างๆ มีข้อความปลุกระดม และข้อความที่มีการแสดงความเห็นรุนแรง โดยนำเรื่องเชื้อชาติ ศาสนา มาเป็นประเด็นการเผยแพร่มีอยู่มากมาย และมีแนวโน้มเพิ่มสูงขึ้นเรื่อยๆ โดยลักษณะของความผิดฐานนี้จึงเป็นการกระทำที่มุ่งเข้าครอบงำและชี้นำความคิดของกลุ่มคนจำนวนมาก ๆ ซึ่งอาจส่งผลระทบที่รุนแรงได้ เนื่องจากการแพร่กระจายข้อความทางอินเทอร์เน็ตให้ผลในวงกว้าง สามารถเข้าถึงการรับรู้ของคนได้จำนวนมากๆ ในเวลาอันสั้น ดังนั้นกฎหมายอาญาของหลายประเทศจึงกำหนดให้การการเผยแพร่ข้อความที่มีลักษณะเป็นการเหยียดเชื้อชาติเป็นความผิดอาญา

---

[57] Winfried Brugger, "The treatment of hate speech in german constitutional law," XVI TH Congress of the International Academy of Comparative Law. Brisbane, 14TH - 20TH July 2002. p.15.

สาเหตุที่หลายประเทศกำหนดให้ Hate Speech ผ่านอินเทอร์เน็ตเป็นความผิดอาญาตามกฎหมายภายในนั้น มีเหตุผลสำคัญในเรื่องการป้องกันการเลือกปฏิบัติ เนื่องจากในหลายประเทศมีประชากรที่มีความแตกต่างด้านเชื้อชาติ ศาสนาและวัฒนธรรม ดังนั้น การป้องกันมิให้การเลือกปฏิบัติต่อกลุ่มเชื้อชาติหรือกลุ่มข้างน้อยในสังคมจึงต้องมีกฎเกณฑ์ใดที่ควบคุมการเผยแพร่ข้อความที่อาจก่อให้เกิดการเลือกปฏิบัติดังกล่าว[58] นอกจากนี้ ยังมีเหตุผลเกี่ยวกับการป้องกันอาชญากรรมที่สืบเนื่องจากความเกลียดชังทางเชื้อชาติที่มีความรุนแรงกว่าอาชญากรรมประเภทอื่นๆ[59] ในประเทศต่างๆ เช่น ประเทศอังกฤษ จึงถือว่า Hate Speech เป็นการกระทำที่ต้องห้าม โดยมีกฎหมายพิเศษที่ใช้บังคับกับการหมิ่นประมาทกลุ่มบุคคลและบทบัญญัติเกี่ยวกับการแสดงข้อความที่กระตุ้นหรือยั่วยุให้เกิดความเกลียดชังระหว่างกลุ่มเชื้อชาติไว้ใน The Public Order Act 1986 หรือ POA โดย POA บัญญัติห้ามการข่มขู่ กระทำทารุณ เหยียดผิว หรือ ใช้ถ้อยคำคุกคาม เพื่อมุ่งประสงค์ที่จะปลุกระดม หรือสร้างความเกลียดชังต่อกลุ่มบุคคลที่มีความแตกต่างกันทางเชื้อชาติ สัญชาติ สีผิว เผ่าพันธุ์ และถิ่นกำเนิด[60] เช่นเดียวกับประมวลกฎหมายอาญาแคนาดา ที่ห้ามการกระทำใด ๆ ที่เป็นการก่อให้เกิดความเกลียดชังต่อกลุ่มบุคคลใดโดยเจตนา (Identifiable Group)[61] กับการห้ามการกระทำใด ๆ ที่เป็นการกระตุ้นหรือการยุยงส่งเสริมให้เกิดความเกลียดชังต่อกลุ่มบุคคลใด ที่ซึ่งจะเป็นการฝ่าฝืนต่อความสงบเรียบร้อย[62] นอกจากนี้ยังมีอีกหลายประเทศที่ได้พัฒนากฎหมายภายในเพื่อห้ามการโฆษณาชวนเชื่อ หรือการเผยแพร่ข้อความอันก่อให้เกิดความเกลียดชัง เช่น ประเทศสวีเดน , เบลเยี่ยม , อาร์เซอร์ไบจัน , บราซิล , ไซปรัส , เชคโกสโลวาเกีย , ออสเตรีย , อิตาลี , เอสโทเนีย , ลิทัวเนีย , นิวซีแลนด์ , โรมาเนีย , รัสเซีย , สวิตเซอร์แลนด์ , ฮังการี และเนเธอร์แลนด์[63]

---

[58] Francine Aumueller, "Hate propaganda law and internet-based hate," The Criminal Law Quarterly, 44(2000) : 100.

[59] Winfried Brugger, "The treatment of hate speech in german constitutional law," p.4.

[60] The Public Order Act 1986 Section 17 – 18

[61] Canada Criminal Code Section 319 (1)

[62] Canada Criminal Code Section 319 (2)

[63] John T. Soma, Thomas F. Muther , Jr. and Heidi M.L. Brissette. "Transnational extradition for computer crimes: Are new Treaties and laws needed ?" Harvard Journal on Legislation , 34 : 344

นอกจากกฎหมายเกี่ยวกับการเผยแพร่ข้อความที่ก่อให้เกิดความเกลียดชังหรือเป็นการเหยียดเชื้อชาติในกรณีทั่วไปดังที่ได้กล่าวมาข้างต้นแล้ว ในประเทศเยอรมนีซึ่งเป็นประเทศที่ถูกปกครองโดยลัทธินาซีในสมัยสงครามโลกครั้งที่ 2 มีกฎหมายภายในที่มีลักษณะเด่นกว่ากฎหมายห้ามการเหยียดเชื้อชาติในประเทศอื่นๆ กล่าวคือ ประมวลกฎหมายอาญาเยอรมนี บัญญัติกฎหมายภายในห้ามการเผยแพร่สัญลักษณ์นาซี (เช่น เครื่องหมายสวัสดิกะ) หรือ การสนับสนุนลัทธินาซี ซึ่งเหล่านี้ถือว่าเป็นการกระทำ (Act) ที่เทียบเท่ากับเป็นการแสดงข้อความที่ผิดกฎหมาย หรือเป็น Hate Speech ที่ลงโทษได้ตามประมวลกฎหมายอาญาเยอรมนี[64] ซึ่งข้อกฎหมายทั้งในเรื่องการห้ามการแสดงข้อความเหยียดเชื้อชาติหรือการสนับสนุนลัทธินาซี ทำให้เกิดปัญหาทางกฎหมายเป็นอย่างมากเมื่อการกระทำดังกล่าวกระทำผ่านเครือข่ายอินเทอร์เน็ต เนื่องจากแม้การเผยแพร่ข้อความเหยียดเชื้อชาติหรือการสนับสนุนลัทธินาซีเป็นความผิดตามกฎหมายของบางประเทศดังที่ได้ยกตัวอย่างข้างต้น แต่กลับไม่เป็นความผิดอาญาตามกฎหมายของประเทศเสรีบางประเทศเช่นประเทศสหรัฐอเมริกา

ดังนั้น ในปัจจุบันอาจสรุปได้ว่าความผิดเกี่ยวกับการแสดงข้อความเหยียดเชื้อชาตินี้ยังคงได้รับการปฏิเสธที่จะกำหนดให้เป็นความผิดตามกฎหมายภายในของบางประเทศ เช่น สหรัฐอเมริกา เนื่องจากมีแนวคิดพื้นฐานว่าด้วยสิทธิของบุคคลแตกต่างกัน แต่โดยลักษณะพิเศษของเครือข่ายอินเทอร์เน็ต อาจทำให้ข้อความผิดกฎหมายดังกล่าวอาจเข้าไปแสดงอยู่ในประเทศที่ห้ามการกระทำดังกล่าวได้เสมอ โดยไม่สามารถเอาผิดกับผู้กระทำความผิดที่กระทำอยู่ภายใต้ดินแดนของประเทศที่ให้เสรีกับการกระทำดังกล่าวได้เลย

6) **การกระทำอันเป็นการกระทบต่อความมั่นคงของรัฐ** (Threats to National Security)

การกระทำการผ่านเครือข่ายอินเทอร์เน็ตที่มีความเกี่ยวข้องกับความมั่นคงของรัฐสามารถเกิดขึ้นได้ในหลายกรณี เนื่องจากในอดีต ระบบเครือข่ายอินเทอร์เน็ตเกิดขึ้นเพื่อใช้ในงานด้านการทหารของสหรัฐอเมริกาโดยเฉพาะเรียกว่า ระบบเครือข่าย ARPANET ซึ่งต่อมาเปลี่ยนชื่อเป็นระบบเครือข่ายอินเทอร์เน็ต ในปี ค.ศ.1983 มีการพัฒนาระบบเครือข่ายให้ใช้งานได้อย่างกว้างขวาง ขยายไปถึงการใช้งานโดยเอกชนด้วย มิได้จำกัดเพียงแค่การใช้งานด้านการทหาร

---

[64] German Penal Code Section 89 – 91 และ Crime Against the public Peace Act Section 123 – 145 d

เท่านั้น การเกิดขึ้นของระบบเครือข่ายอินเทอร์เน็ตที่เคยถูกใช้งานด้านการทหารทำให้เกิดความเชื่อว่า อินเทอร์เน็ตถูกออกแบบมาเพื่อควบคุมอาวุธนิวเคลียร์ เพื่อใช้ในการทำสงคราม หรือใช้ในการปฏิบัติงานด้านการทหาร แม้ว่าหน่วยงานทางการทหารสหรัฐอเมริกา จะอ้างว่าระบบทางการทหารที่สำคัญของหน่วยงานทางการทหาร รวมถึงไม่ได้มีการเชื่อมโยงกับระบบเครือข่ายอินเทอร์เน็ตแต่อย่างใด

อย่างไรก็ตาม แม้ว่าระบบเครือข่ายอินเทอร์เน็ตไม่มีความเชื่อมโยงกับอาวุธหรือระบบทางการทหาร แต่ในระบบสาธารณูปโภคหลักของบางประเทศ เช่น สหรัฐอเมริกา และประเทศพัฒนาหลายประเทศ ล้วนมีการใช้ระบบคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตในการควบคุมและเข้าถึงระบบ เช่น ระบบไฟฟ้าภายในประเทศ ระบบโทรคมนาคมและการสื่อสาร ระบบทางการเงินและการธนาคาร การประปา การขนส่ง การควบคุมท่อก๊าซและปิโตรเลียม การให้บริการหน่วยฉุกเฉิน รวมถึง บริการของหน่วยงานภาครัฐต่าง ๆ ซึ่งสาธารณูปโภคเหล่านี้ ถือเป็นสาธารณูปโภคหลักที่สำคัญของประเทศ ความสำคัญของระบบเครือข่ายอินเทอร์เน็ตในการใช้ควบคุมสาธารณูปโภคหลัก รวมถึงกิจการด้านความมั่นคง ทำให้อาชญากรคอมพิวเตอร์บางกลุ่มมุ่งโจมตีระบบความมั่นคงของรัฐ ในลักษณะการโจมตีระบบประเภท Cyber War หรือ Infowar ซึ่งเป็นการทำสงครามทางระบบเครือข่ายอิเล็กทรอนิกส์และข้อมูลข่าวสาร เช่น การเจาะระบบเพื่อขโมยข้อมูลอันเป็นความลับของประเทศ โดยเฉพาะอย่างยิ่งการกระทำการก่อการร้ายบนระบบเครือข่ายอินเทอร์เน็ต หรือ Cyber-Terrorism[65]

ความสำคัญของระบบเครือข่ายอินเทอร์เน็ตต่อระบบความมั่นคงของประเทศดังที่ได้กล่าวมา ทำให้หน่วยงานภาครัฐและผู้เชี่ยวชาญในองค์กรเอกชนเล็งเห็นว่า อินเทอร์เน็ตได้เข้ามามีส่วนในการควบคุมระบบสำคัญต่างๆ ของชาติและธุรกิจของเอกชน เช่น ระบบการเงินการธนาคาร หรือแม้แต่ตลาดหุ้น ดังนั้น ความพยายามในการสร้างระบบป้องกันเครือข่ายอินเทอร์เน็ตและการเข้าถึงข้อมูลจึงกลายเป็นเรื่องของความมั่นคงของชาติ ซึ่งทำให้การลักลอบโจมตีเครือข่ายหรือระบบคอมพิวเตอร์ที่เกี่ยวกับความมั่นคงของชาติกลายเป็นเหมือนการทำสงคราม ที่ซึ่งมีการเปลี่ยนแปลงจากการทำสงครามในแบบดั้งเดิมมาเป็นการทำสงครามแบบ Cyber War การทำสงครามบนเครือข่ายอินเทอร์เน็ตไม่ว่าจะโจมตีระบบเครือข่ายของรัฐหรือภาคธุรกิจสำคัญของเอกชน ก่อให้เกิดความยากลำบากในการป้องกันและรักษาความมั่นคงของรัฐ เนื่องจากประการ

---

[65] Gary Chapman, National security and the internet [Online], July 1998, Available from: http://www.utexas.edu/lbj/21cp[2002, July 21]

แรก รัฐที่เป็นเป้าหมายการโจมตีไม่สามารถทราบว่าการโจมตีจะกระทำเมื่อใด จากที่ไหน ใครเป็นผู้กระทำและมีมูลเหตุจูงใจในการกระทำ เคยมีรายงานว่า สหรัฐอเมริกาเคยประสบปัญหาจากการถูก Hacker เจาะระบบฐานข้อมูลคอมพิวเตอร์ ของ Pentagon ก่อนเกิดสงครามอ่าวเปอร์เซีย โดย Hacker นำข้อมูลไปขายให้แก่ซัดดัม ฮุสเซน[66]

นอกจากนี้ จากคำให้สัมภาษณ์ของเจ้าหน้าที่ทางการสหรัฐฯ ระบุว่ากลุ่มมุสลิมหัวรุนแรงทั่วโลกรวมทั้งนายโอซามา บิน ลาเดน ใช้เทคนิคการเข้ารหัสในการรับส่งข้อมูลผ่านอินเทอร์เน็ตเพื่อวางแผนโจมตีสหรัฐอเมริกาและพันธมิตร โดยแฟ้มข้อมูลภาพ แผนที่เป้าหมายการโจมตีและข้อความจดหมายอิเล็กทรอนิกส์ของกลุ่มก่อการร้ายได้รับการเข้ารหัสและส่งผ่านด้วยวิธีหลากหลายบนอินเทอร์เน็ตเช่นห้องสนทนา กระดานข่าวของเว็บลามก และเว็บไซต์ต่าง ๆ ซึ่งเจ้าหน้าที่สหรัฐกล่าวว่า อินเทอร์เน็ตกลายมาเป็นแหล่งใหม่ให้สายลับใช้ในการรับส่งข้อมูลลับโดยใช้โปรแกรมเข้ารหัสข้อมูลที่หาได้ทั่วไปจากบริษัทที่เปิดให้บริการบนอินเทอร์เน็ต นายจอร์จ ทีเน็ต ผู้อำนวยการซีไอเอเผยในรายงานต่อที่ประชุมคณะกรรมาธิการต่างประเทศแห่งวุฒิสภาสหรัฐอเมริกาว่า ปัจจุบันกลุ่มก่อการร้ายใช้เทคโนโลยีคอมพิวเตอร์ การเข้ารหัสแฟ้มข้อมูลและอีเมล์ในการปฏิบัติการก่อการร้ายต่างๆ[67] ซึ่งยากที่จะป้องกันหรือตรวจสอบถึงที่มาของการกระทำได้ทันท่วงที ประกอบกับปัญหาในเรื่องเขตอำนาจรัฐและความแตกต่างกันด้านกฎหมายก็เป็นอุปสรรคในการให้ความร่วมมือทางอาญาและนำตัวผู้กระทำผิดมาลงโทษ

ในประเทศสหรัฐอเมริกา ซึ่งประสบปัญหาการถูกทำลายระบบเครือข่ายคอมพิวเตอร์และมีผลกระทบต่อข้อมูลด้านความมั่นคงจากการกระทำภายในประเทศบ่อยครั้ง ทำให้มีคดีขึ้นสู่การพิจารณาของศาลอยู่เสมอ ซึ่งในคดีไวรัสคอมพิวเตอร์ Worm ซึ่งสร้างความเสียหายแก่ระบบคอมพิวเตอร์ของทางการสหรัฐอเมริกาอย่างมาก โดยในคดีนี้จำเลยคือนายโรเบิร์ด ที มอริส นักศึกษามหาวิทยาลัยคอร์แนล ได้สร้างไวรัสคอมพิวเตอร์ที่เป็นที่รู้จักในชื่อ Worm ซึ่งเป็นโปรแกรมชนิดหนึ่งที่ยากต่อการตรวจจับหรือทำลายโดยโปรแกรมเมอร์คนอื่น มอริสได้ใส่โปรแกรมไวรัสนี้เข้าไปในระบบปฏิบัติการยูนิกส์ (Unix) เมื่อวันที่ 2 พฤศจิกายน 1988 ที่ Massachusetts

---

[66] Ibid., p.6.

[67] สำนักงานตำรวจแห่งชาติ, มุสลิมหัวรุนแรงใช้อีเมล์เข้ารหัส ติดต่อวางแผนโจมตีสหรัฐ [Online], 2002, แหล่งที่มา : http://www.police.go.th/policenews/index.php?myaction=106&cat_id=2 [2003, Mar 16]

Institute of Technology เพราะต้องการอำพราง Worm แพร่กระจายไปอย่างรวดเร็วจนเครือข่ายอินเทอร์เน็ตสหรัฐอเมริกาล่มสลาย ทำให้เกิดผลกระทบไปถึงหน่วยงานทางทหาร และศูนย์วิจัยต่างๆ ในสหรัฐอเมริกาที่เชื่อมโยงกับเครือข่าย เครื่องคอมพิวเตอร์กว่า 1,000 เครื่อง ถูก Worm ทำลายรวมทั้งระบบข้อมูลของหน่วยงาน Pentagon ก็ถูกเจาะระบบกว่า 100 ครั้ง สร้างความเสียหายเป็นอันมาก ในที่สุดศาลสหรัฐฯได้ตัดสินให้นายมอริสจำคุก 3 ปี แต่ให้รอลงอาญา และบริการสังคมเป็นเวลา 400 ชั่วโมง ปรับเป็นเงิน 10,150 เหรียญสหรัฐอเมริกา[68]

การโจมตีระบบข้อมูลคอมพิวเตอร์ผ่านเครือข่ายอินเทอร์เน็ตเพื่อทำลายหรือขโมยข้อมูลอันเป็นความลับของประเทศนั้นมิได้เกิดขึ้นแต่เพียงในสหรัฐอเมริกาประเทศเดียว มีรายงานว่า พบหลักฐานที่บ่งชี้ว่ามีความพยายามในการทำลายระบบคอมพิวเตอร์ของโครเอเซีย ระหว่างสงครามเซอร์เบีย โดยผู้เชี่ยวชาญด้านความมั่นคงของโครเอเซียสงสัยว่า การเจาะระบบถูกกระทำโดยโปรแกรมเมอร์ชาวเซอร์เบีย[69]

นอกจากนี้ ในประเทศอังกฤษ ผู้ต้องหาการก่อการร้ายซึ่งเป็นนักคอมพิวเตอร์ที่มีชื่อว่านายโมฮัมเหม็ด อับดุลเลาะห์ อาซาม วัย 32 ปี ถูกจับที่บ้านพักของเขาในเมืองลูตั้นใกล้กับกรุงลอนดอน นักพัฒนาโปรแกรมคอมพิวเตอร์หรือโปรแกรมเมอร์รายนี้ ถูกจับกุมด้วยข้อหาเก็บรวบรวมข้อมูล หรือเผยแพร่ข้อมูล เพื่อช่วยเหลือการโจมตีโดยกลุ่มก่อการร้าย ตาม Terrorism Act 2000[70]

การลักลอบเข้าถึงฐานข้อมูลที่เป็นความลับของประเทศนั้น สามารถกระทำได้จากที่ใดในโลกก็ได้ เนื่องจากคุณสมบัติที่สามารถเชื่อมโยงข้อมูลถึงกันได้ของระบบเครือข่ายอินเทอร์เน็ต จากคดีที่เคยเกิดขึ้นโดยผู้กระทำความผิดใช้คอมพิวเตอร์จากในประเทศไทยในการลักลอบเข้าถึงฐานข้อมูลของฐานทัพอากาศสหรัฐอเมริกา เนื่องจากกองทัพอากาศสหรัฐฯมีระบบคอมพิวเตอร์ที่ใช้สำหรับการเก็บเอกสารในรูปแบบของข้อมูลต่างๆ โดยมีการรักษาความปลอดภัย (Security Measures) การเข้าถึงทั้งสถานที่และทางเทคโนโลยี (Physical and Electronic

---

[68] ทวีศักดิ์ กออนันตกูล , "อาชญากรรมในยุคโลกาภิวัฒน์," บทบัณฑิตย์ 55,1(มีนาคม 2542) : 33.

[69] Gary Chapman, National security and the internet [Online], July 1998, Available from: http://www.utexas.edu/lbj/21cp[2002, July 21]

[70] http://news. Mweb.Co.th/archive/index. Jsp (22/09/2545)

Security) โดยบุคลากรกองทัพอากาศที่ต้องได้รับอนุญาต และมีรหัสผ่านเพื่อการเข้าถึงระบบเครือข่ายคอมพิวเตอร์กองทัพสหรัฐอเมริกาเท่านั้น เมื่อวันที่ 19 พฤศจิกายน 2541 เจ้าหน้าที่ประจำศูนย์ข่าวสารสงครามกองทัพอากาศ (Air Force Information Warfare Center (AFIWC)) ฐานทัพอากาศเคลลี่ รัฐเท็กซัส สหรัฐอเมริกาตรวจพบการลักลอบติดต่อกับคอมพิวเตอร์ฐานทัพอากาศบรู๊คส์ (Brook Air Force Base) รัฐเท็กซัส ผ่านเครือข่ายอินเทอร์เน็ตจากเครื่องคอมพิวเตอร์ในประเทศไทย ซึ่งเป็นสมาชิกของบริษัท สามารถ อินโฟเน็ท จำกัด จากการตรวจสอบพบว่า ผู้ที่ลักลอบเข้าไปในระบบคอมพิวเตอร์ฐานทัพอากาศบรู๊คส์ โดยการใช้หมายเลขประจำตัวผู้ใช้ (User ID) และรหัสผ่าน (Password) ที่แท้จริงแล้วผู้ที่เป็นเจ้าของหมายเลขประจำตัวของผู้ใช้แจ้งว่าทำการเชื่อมต่อคอมพิวเตอร์เข้ากับมหาวิทยาลัยอียิปต์ (University of Egypt) โดยผู้ลักลอบได้เข้าถึงและเรียกใช้แฟ้มข้อมูล รวมทั้งทำการลบแฟ้มข้อมูลลับของสหรัฐอเมริกา จากคอมพิวเตอร์ในประเทศไทยโดยใช้นามแฝงว่า "hdyang" โดยได้ตั้งโปรแกรมการลบหลักฐานการติดต่อของตนกับระบบคอมพิวเตอร์ฐานทัพอากาศบรู๊คส์เพื่อมิให้ปรากฏหลักฐานการติดต่ออีกด้วย[71]

การกระทำดังกล่าวจึงเป็นความผิดตามกฎหมายของสหรัฐอเมริกา โดยประเทศสหรัฐอเมริกามีกฎหมายเกี่ยวกับการคุกคามความมั่นคงของรัฐผ่านเครือข่ายอินเทอร์เน็ตโดยถูกกำหนดให้เป็นความผิดทางอาญา ตาม Computer Fraud and Abuse Act Section 1030(a)(1) ซึ่งเป็นบทบัญญัติเฉพาะสำหรับการกระทำผ่านเครือข่ายอินเทอร์เน็ต โดยกำหนดห้ามการเข้าถึงข้อมูลที่เกี่ยวกับความปลอดภัยด้านความมั่นคงของชาติที่เป็นความลับโดยมิได้รับอนุญาต โดยเจตนาในการก่อให้เกิดความเสียหายแก่ประเทศสหรัฐอเมริกา หรือเป็นการนำข้อมูลที่ได้ไปเพื่อประโยชน์แก่ประเทศอื่น เช่นเดียวกับ Section 1030 (a) (3) ที่กำหนดให้การเจตนาเข้าถึงระบบคอมพิวเตอร์ของหน่วยงานหรือองค์กรใด ๆ ของรัฐ โดยไม่ได้รับอนุญาตเป็นความผิด เมื่อการกระทำดังกล่าวก่อให้เกิดผลกระทบต่อการทำงานของระบบคอมพิวเตอร์

กรณีการคุกคามต่อความมั่นคงของรัฐด้วยวิธีการแบบใหม่ผ่านทางเครือข่ายอินเทอร์เน็ตก่อให้เกิดความวิตกกังวลต่อภัยอันตรายของการคุกคามต่อความมั่นคงของประเทศผ่านทางเครือข่ายอินเทอร์เน็ตแก่ประเทศต่างๆ ในเอเชียหลายประเทศมีกฎหมายที่กำหนดให้การกระทำหลายประการเป็นความผิดต่อความมั่นคง เช่น ในประเทศเวียดนาม มีกฎหมายห้ามผู้ใช้อินเทอร์เน็ตในการทำซ้ำหรือป้อนข้อมูลใด ๆ อันอาจเป็นภัยหรืออาจมีผลกระทบต่อความมั่นคงของชาติ เช่นเดียวกับในประเทศเกาหลีใต้ โดยกฎหมายเกี่ยวกับความมั่นคงของชาติ ของประเทศ

---

[71] หนังสือพิมพ์มติชนรายวัน ฉบับลงวันที่ 4 กุมภาพันธ์ 2542 หน้า 2.

เกาหลีใต้ได้กำหนดให้การให้การสนับสนุน ส่งเสริม ยกย่องสรรเสริญ ระบอบการปกครองของประเทศเกาหลีเหนือเป็นความผิดอาญา นอกจากนี้ในประเทศพม่า กฎหมายแห่งรัฐบาลทหารกำหนดให้การเข้าถึงระบบเครือข่ายคอมพิวเตอร์ของรัฐบาล การครอบครอง ได้มา หรือเผยแพร่ข้อมูลอันเป็นความลับของประเทศ เป็นความผิดที่ต้องระวางโทษจำคุกตั้งแต่ 7 ถึง 15 ปี[72] ไม่ว่าจะเป็นเรื่องทางเศรษฐกิจ หรือสังคมก็ตาม

7) **การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ** (Unauthorized Access)

การจะกล่าวถึงการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบนั้น จะต้องศึกษาถึงความหมายของ "การเข้าถึง" (access) ก่อน โดยคำนิยามของ การเข้าถึง ที่กฎหมายของประเทศสหรัฐอเมริกานิยมใช้ ได้ให้ความหมายว่า การเข้าไปสู่ สั่ง สื่อสารกับใส่ข้อมูลเข้าไปเก็บไว้ ล้วงข้อมูลมาจาก หรืออีกนัยหนึ่ง เอาประโยชน์ใดๆของเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์มาใช้[73] หรือความหมายที่เข้าใจได้ง่าย คือ การฝ่าด่านรักษาความปลอดภัยเพื่อเข้าไปในระบบโดยไม่ได้รับอนุญาต โดยมีวัตถุประสงค์เพื่อหาประโยชน์จากข้อมูลที่ถูกเก็บรักษาอยู่ภายใน อย่างไรก็ตาม ในบางกรณีการกระทำดังกล่าวก็อาจมิใช่กระทำเพราะต้องการแสวงประโยชน์ทางทรัพย์สินเท่านั้น แต่เป็นเพียงการกระทำเพื่อความสนุกสนาน อยากทดลองหรืออยากรู้อยากเห็นข้อมูลอันเป็นความลับ ซึ่งทำให้ในปัจจุบันเจ้าของข้อมูลต้องมีภาระในการสร้างระบบรักษาความปลอดภัยเพื่อป้องกันผู้ลักลอบเข้าสู่ระบบ

ระบบรักษาความปลอดภัยที่นิยมใช้ส่วนใหญ่ จะเป็นการใส่รหัสเพื่อป้องกันโดยผู้ที่มีรหัสผ่านที่ถูกต้อง ก็จะเหมือนมีกุญแจไขเข้าไปได้ ดังนั้น การฝ่าด่านระบบรักษาความปลอดภัยหรือที่มักเรียกสั้น ๆ ว่า Hacking นั้น จำเป็นต้องใช้วิธีการต่าง ๆ เพื่อหลอกล่อให้คอมพิวเตอร์เกิดความสับสนในการทำงาน และอนุญาตให้เข้าสู่ระบบได้ เช่น การใช้โปรแกรม Superzap ซึ่งเป็นโปรแกรมที่เหมือนเป็นกุญแจผี เพื่อใช้เข้าสู่ระบบคอมพิวเตอร์ในกรณีฉุกเฉิน หรือการสร้าง Trap

---

[72] John T. Soma , Thomas F. Muther and Heidi M.L. Brissette , "Transnational extradition for computer crimes : Are new treaties and laws need ? ," Harvard Journal on Legislation , 34 : 353.

[73] เลิศชาย สุธรรมพร, "อาชญากรรมคอมพิวเตอร์ : ศึกษาเฉพาะกรณีความปลอดภัยของข้อมูล," (วิทยานิพนธ์ปริญญามหาบัณฑิต ภาควิชานิติศาสตร์ บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย, 2541), หน้า 46.

Doors คือ การเขียนโปรแกรมเลียนแบบหน้าจอปกติของเครื่องคอมพิวเตอร์ เพื่อลวงผู้ใช้ตัวจริงที่มีรหัสผ่าน ซึ่งเมื่อผู้ใช้ใส่รหัสผ่าน รหัสจะถูกจัดเก็บไว้ในแฟ้มลับของผู้เขียนโปรแกรม[74] เป็นต้น โดยการเข้าถึงข้อมูลสามารถกระทำได้แม้ไม่ได้เข้าไปในสถานที่ที่เครื่องคอมพิวเตอร์เป้าหมายตั้งอยู่แต่ก็สามารถใช้เครื่องคอมพิวเตอร์อื่นเชื่อมต่อกับระบบเครือข่ายเพื่อเข้าถึงข้อมูลที่อยู่ภายในเครื่องคอมพิวเตอร์เป้าหมายที่ต้องการได้ การเข้าถึงระบบข้อมูลหรือระบบคอมพิวเตอร์อาจกระทำไปโดยสาเหตุหรือเกิดจากมูลเหตุจูงใจในหลายกรณี เช่น กระทำโดยมีเจตนากระทำอาชญากรรมเพื่อต้องการได้ไปซึ่งข้อมูลอันเป็นความลับหรือเพื่อจะกระทำความผิดอื่นในระบบ หรือกระทำไปโดยความอยากทดลองหรือเพื่อทดสอบความสามารถการรักษาความปลอดภัยของระบบโดยไม่มีเจตนาที่จะก่อความเสียหายแต่อย่างใด[75] จึงเป็นการยากที่จะค้นหาเจตนาที่แท้จริงของผู้กระทำมีเจตนาชั่วหรือไม่ ประเด็นดังกล่าวกลายเป็นปัญหาข้อกฎหมายที่ยังคงเป็นข้อถกเถียงกันในหมู่นักกฎหมายในหลายประเทศว่า สมควรกำหนดให้การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบหรือโดยปราศจากอำนาจเป็นความผิดอาญาอีกฐานหนึ่ง แยกจากความผิดฐานอื่น ๆ ที่เกิดเมื่อผู้กระทำผิดได้เข้าสู่ระบบแล้ว หรือไม่

นักกฎหมายในกลุ่มแรก เห็นว่าการเข้าสู่ระบบคอมพิวเตอร์โดยการเจาะผ่านสิ่งปกป้องคุ้มครองข้อมูลเป็นไม่ความผิดทางอาญา เนื่องจากการเข้าไปดูเฉยๆเสมือนการที่เรามองดูข้อความในกระดาษของคนอื่นที่เขียนไว้บนโต๊ะ หรือการแอบดูข้อความต่างๆยังไม่มีเหตุผลพอที่จะเป็นความผิดอาญา เว้นแต่เป็นกรณีเจาะทะลุทะลวงผ่านระบบป้องกันเพื่อเข้าไปเอาข้อมูลบางอย่างออกมาขายหรือก่อให้เกิดความเสียหาย ดังนั้น กฎหมายของประเทศที่มีแนวคิดเช่นนี้จึงกำหนดองค์ประกอบความผิดโดยมีเจตนาในการเข้าสู่ระบบเพื่อกระทำความผิดหรือกระทำการอย่างอื่นที่มากกว่าการเข้าไปดูข้อมูลแต่เพียงอย่างเดียว เช่น ในประเทศเยอรมนี[76], ออสเตรีย, แคนาดา, ญี่ปุ่น[77] และไต้หวัน[78] เป็นต้น

---

[74] สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ (ฉบับปรับปรุงครั้งที่ 2), หน้า 53.

[75] ทวีศักดิ์ กออนันตกูล, "อาชญากรรมในยุคโลกาภิวัฒน์," บทบัณฑิตย์ 55,1 : 31.

[76] สุเนติ คงเทพ, "การไม่มีอำนาจเข้าสู่ระบบประมวลผล (Hacking)," บทบัณฑิตย์ 55 : 125.

[77] John T. Soma , Thomas F. Muther and Heidi M.L. Brissette , "Transnational extradition for computer crimes : Are new treaties and laws need ? ," Harvard Journal on Legislation, 34 : 348.

อย่างไรก็ตาม ในความเห็นของนักกฎหมายในกลุ่มที่สอง ซึ่งเป็นความเห็นส่วนใหญ่นั้นเห็นว่า มีความเห็นว่าสมควรกำหนดให้การเข้าสู่ระบบคอมพิวเตอร์ของผู้อื่นโดยมิชอบเป็นความผิดอาญาโดยไม่ต้องมีการกระทำความผิดฐานอื่นในระบบอีก ซึ่งเพียงแค่การเข้าสู่ระบบที่มีการป้องกันก็เป็นความผิดอาญาแล้ว ทั้งนี้โดยมีเหตุผลสืบเนื่องมาจาก ประการแรก การเข้าถึงระบบจำเป็นต้องมีการฝ่าด่านรักษาความปลอดภัย ทำให้ระบบเกิดความเสียหายและกลายเป็นภาระของเจ้าของระบบที่ต้องมีค่าใช้จ่ายในการวางระบบป้องกันรวมถึงค่าซ่อมแซม[79] ประการที่สอง การเข้าถึงระบบโดยมิชอบหรือโดยปราศจากอำนาจ ถือเป็นการละเมิดสิทธิส่วนบุคคลต่อเจ้าของระบบในข้อมูลที่ถูกสร้างขึ้นและเก็บไว้อยู่ในความเป็นส่วนตัว ประการที่สาม การเข้าไปในระบบ แม้เป็นเพียงการเข้าไปเพื่อดูอย่างเดียว โดยไม่ก่อให้เกิดความเสียหายอื่นใด ก็อาจถือเป็นการกระทำที่เป็นภัย อันถือได้ว่าเป็นความเสี่ยงต่อการเกิดความเสียหายต่อข้อมูลสารสนเทศได้[80] จากเหตุผลดังกล่าวทำให้หลายประเทศเห็นควรกำหนดให้การเข้าสู่ระบบคอมพิวเตอร์โดยมิชอบเป็นความผิดอาญาโดยไม่จำต้องมีข้อเท็จจริงว่าผู้ลักลอบเข้าสู่ระบบเพื่อการใด ดังนั้น เพียงการเข้าสู่ระบบคอมพิวเตอร์ที่มีการรักษาความปลอดภัยไว้ก็ถือเป็นความผิดอาญา[81] เช่น ประเทศออสเตรเลีย[82] แคนาดา[83] เดนมาร์ก[84] ฟินแลนด์[85] ฝรั่งเศส[86] ลักเซมเบิร์ก[87] เนเธอร์แลนด์[88] นอร์เวย์[89] สเปน[90] สวีเดน[91] สวิตเซอร์แลนด์[92] อังกฤษ[93] และสหรัฐอเมริกา[94]

---

[78] Tonya L. Putnam and David D. Elliott, Chapter 2 : International respond to cyber crime [Online],(n.d.), Available from: http://www.hoover.standford.edu/publications/books/fulltext/cybercrime/221.pdf. [2003,Jan 5]

[79] Ian Lloyd, Legal aspect of the information society (London : Butterword, 2000), p. 101.

[80] Ulrich Sieber, Computer crime and criminal information law - New trends in the international risk and information society[Online],(n.d.), Available from: http://www.jura.uni-muenchen.de/sieber/article/mitis/comcricrilnf.html. [11/01/03], p.13.

[81] สุเนติ คงเทพ, "การไม่มีอำนาจเข้าสู่ระบบประมวลผล (Hacking)," บทบัณฑิตย์ 55 : 124.

[82] Australian Crimes Act 1914 Section 76 A-E

[83] Canada Criminal Code Article 342.1

[84] Danish Penal Code Section 263 (2), (3)

[85] Finnish Penal Code Chapter 38 Section 8

แม้ว่าประเทศต่างๆจะมีความเห็นทางกฎหมายในการกำหนดองค์ประกอบความผิดที่แตกต่างกันบ้าง แต่การที่ประเทศต่างๆล้วนให้ความสำคัญแก่การกำหนดให้การลักลอบเข้าสู่ระบบคอมพิวเตอร์โดยมิชอบเป็นความผิดทางอาญา ก็เป็นผลสืบเนื่องมาจากสถิติคดีอาชญากรรมคอมพิวเตอร์ที่เพิ่มสูงขึ้น และก่อความรุนแรงมากขึ้นเป็นลำดับ ดังเช่นตัวอย่างในคดี Tristan มีข้อเท็จจริงในคดีว่า แฮกเกอร์ชาวเยอรมนีจำนวน 20 คนได้ประสพความสำเร็จในการเจาะระบบคอมพิวเตอร์เพื่อเข้าไปยังสถาบันวิจัยพลังงาน (High Energy Physics Research Institute) ของประเทศญี่ปุ่น ต่อมาได้เจาะระบบคอมพิวเตอร์เข้าไปในระบบประมวลผล (EDP) โดยเข้าไปใน Data Banks ของประเทศสหรัฐอเมริกา โดยเฉพาะอย่างยิ่ง ได้เข้าไปในเครื่องเมนเฟรมของ Lawreno Berkley ซึ่งเป็นเครื่องที่ทำหน้าที่เป็นประตูผ่านเข้าสู่ระบบเครื่องคอมพิวเตอร์ของหน่วยงานทางทหาร และของมลรัฐอื่น ๆ หลังจากนั้น บรรดาแฮกเกอร์ได้ขายความรู้ที่ได้จากการเจาะระบบและวิธีการเชื่อมต่อ Network รวมถึงเส้นทางที่ได้ทำการ Locked Out ไว้ ให้กับหน่วยสืบราชการลับ KGB ผ่านเจ้าหน้าที่ฑูตทางการค้า ในเบอร์ลินตะวันออก คดีดังกล่าวทำให้กลุ่มแฮกเกอร์ถูกฟ้องต่อศาลตามมาตรา 99 ประมวลกฎหมายอาญาเยอรมนี (STGB) ในข้อหาเป็นตัวแทนให้ชาวต่างชาติใช้บริการ โดยในวันที่ 10 กุมภาพันธ์ 1990 ศาล Celle Higher Regional Court ประเทศเยอรมนีได้มีคำพิพากษาให้บรรดา Hacker มีความผิดตามกฎหมายดังกล่าว โดยลงโทษจำคุกไม่เกิน 2 ปี[95]

---

[86] France Criminal Code Article 462-2

[87] Luxembourg Penal Code Article 509-1

[88] Netherlands Criminal Code Article 138 a (1), (2)

[89] Norway Penal Code Section 145

[90] Spain Criminal Code Article 256

[91] Sweden Data Protection Act Section 21

[92] Swiss Criminal Code Article 143 bis

[93] UK Computer Misuse Act 1990 Section 1, 2

[94] U.S.C. Title 18 Section 2510-2521, 2701-2710, 3117, 3121-3126 และU.S.C. Title 18 Section 1029 - 1030 (CFAA)

[95] สุเนติ คงเทพ, "การไม่มีอำนาจเข้าสู่ระบบประมวลผล (Hacking)," บทบัณฑิตย์ 55 : 128.

จากที่ได้กล่าวมาทั้งหมดนี้ อาจสรุปได้ว่า แม้ในปัจจุบันการเข้าสู่ระบบข้อมูลของผู้อื่นโดยมิชอบนั้น จะมีประเทศส่วนใหญ่กำหนดให้การกระทำดังกล่าวเป็นความผิดก็ตาม แต่เนื่องจากยังมีบางประเทศที่มีความเห็นที่แตกต่าง ทำให้ยังคงเกิดปัญหาในทางระหว่างประเทศว่า ในกรณีที่การกระทำความผิดมีลักษณะระหว่างประเทศ และมีความเกี่ยวพันกับเขตอำนาจของรัฐมากกว่า 1 รัฐแล้ว จะมีการลงโทษผู้กระทำความผิด ตลอดจนให้ความร่วมมือระหว่างประเทศในการส่งผู้ร้ายข้ามแดนระหว่างกันอย่างไร ซึ่งผู้เขียนจะได้กล่าวในรายละเอียดต่อไป

8) **การจารกรรมข้อมูลคอมพิวเตอร์** (Computer Espionage)

ด้วยคุณลักษณะของระบบอินเทอร์เน็ตมีความยืดหยุ่นสูง ซึ่งเป็นจุดอ่อนที่ทำให้บรรดามือดีทางด้านคอมพิวเตอร์เจาะเข้าสู่เครื่องคอมพิวเตอร์ที่เชื่อมอยู่กับระบบได้โดยไม่ยาก ทำให้เกิดการแสวงประโยชน์จากการเจาะระบบ โดยการจารกรรมข้อมูลที่เป็นความลับไปใช้ในทางที่จะก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลและก่อประโยชน์แก่ผู้กระทำ ลักษณะของการกระทำความผิดคือการที่ผู้กระทำความผิดจะเจาะเอาข้อมูลต่างๆ ซึ่งอาจจะเป็นข้อมูลสำคัญที่ถูกเก็บเป็นความลับจากหน่วยงานต่างๆไม่ว่าจะเป็นภาครัฐหรือเอกชน ซึ่งอาจทำให้ระบบการเงินและธุรกิจปั่นป่วน หรือ หากเป็นการกระทำต่อระบบฐานข้อมูลแห่งชาติอาจทำให้เกิดผลกระทบต่อความมั่นคงโดยรวม ซึ่งนอกจากความเสียหายที่เกิดกับภาครัฐแล้ว การได้มาซึ่งข้อมูลนั้นอาจเป็นการได้มาจากการเจาะระบบข้อมูลก่อน เพื่อนำข้อมูลออกมา ซึ่งเท่ากับได้กระทำความผิดเกี่ยวกับการเจาะระบบอีกกระทงหนึ่ง[96] หรืออาจได้ข้อมูลมาโดยวิธีการดักสกัดข้อมูลในระหว่างทาง (Computer Interception) "การได้มา" ซึ่งข้อมูลต่างๆนั้น จะปรากฏขึ้นเมื่อผู้กระทำผิดได้มีการเคลื่อนย้ายโอนถ่ายข้อมูลลงบนพาหะข้อมูลหรืออุปกรณ์ต่างๆ เช่น เอามาเก็บลงไว้ในดิสก์หรือ CD-ROM หรือเก็บไว้ในหน่วยความจำของตัวเครื่องเพื่อเปิดดูได้ภายหลัง[97]

การกระทำความผิดยังก่อให้เกิดความเสียหายที่สูง ยิ่งไปกว่านั้น จำเลยที่กระทำความผิดจำนวนไม่น้อยที่ยังเป็นผู้เยาว์ ยกตัวอย่างเช่น ในคดีระหว่าง United States of America v. Juvenile จำเลยใช้ชื่อในอินเทอร์เน็ตว่า "Comrade" ได้ทำการเจาะระบบเครือข่ายคอมพิวเตอร์

---

[96] เฉพาะในกรณีที่กฎหมายของประเทศนั้นๆ กำหนดให้การเจาะระบบคอมพิวเตอร์เป็นความผิดอาญาอีกฐานหนึ่งแยกจากการกระทำความผิดฐานอื่นในระบบ

[97] สุเนติ คงเทพ, "การไม่มีอำนาจเข้าสู่ระบบประมวลผล (Hacking)," บทบัณฑิตย์ 55 : 127.

ของ Defense Threat Reduction Agency (DTRA) ซึ่งเป็นหน่วยงานหนึ่งในกระทรวงกลาโหมสหรัฐฯ โดยไม่ได้รับอนุญาต โดยจำเลยได้ติดตั้ง backdoor[98] ไว้บน Server ซึ่งการติดตั้งโปรแกรม backdoor ทำให้สามารถดักฟัง (Intercept) ข้อความที่ส่งออกหรือเข้ามาของพนักงานในหน่วยงาน รวมทั้งดักฟังบัญชีรายชื่อผู้ใช้และรหัสผ่านคอมพิวเตอร์ของเจ้าหน้าที่ในหน่วยงาน นอกจากนี้ จำเลยยังเจาะเข้าไปในระบบคอมพิวเตอร์ของ NASA โดยไม่ได้รับอนุญาต และ download ซอฟต์แวร์ที่มีมูลค่าถึง 1.7 ล้านเหรียญสหรัฐฯขององค์การ NASA ที่ใช้ในการตรวจสภาพแวดล้อมในสถานีอวกาศไปอีกด้วย จากการกระทำดังกล่าวศาลแขวงมลรัฐไมอามีได้พิพากษาให้จำเลยมีความผิดตาม Title 18 U.S.C. Section 1030 แต่เนื่องจากจำเลยเป็นผู้เยาว์ศาลจึงลงโทษกักขังเป็นเวลา 6 เดือน[99]

ตัวอย่างในคดีดังกล่าวนั้นหากเกิดขึ้นในประเทศที่ไม่มีกฎหมายเฉพาะเกี่ยวกับอาชญากรรมคอมพิวเตอร์แล้ว อาจเกิดปัญหาในการบังคับใช้กฎหมายเพื่อการลงโทษผู้กระทำความผิด ซึ่งแม้ว่าแนวคิดของประเทศต่างๆมุ่งจะคุ้มครองข้อมูลคอมพิวเตอร์เทียบเท่ากับการคุ้มครองทรัพย์สินของบุคคล[100] ดังนั้น ในการคัดลอกโปรแกรมหรือข้อมูลคอมพิวเตอร์จึงเป็นความผิดฐานลักทรัพย์หรือ Theft ได้เช่นกัน ซึ่งบางประเทศสามารถปรับใช้กฎหมายอาญาดั้งเดิมกับการจารกรรมข้อมูลทางคอมพิวเตอร์ เช่นประเทศแคนาดา[101] ญี่ปุ่น[102] ฝรั่งเศส[103] เป็นต้น อย่างไรก็ตาม ก็มีหลายประเทศที่ไม่สามารถปรับใช้กฎหมายดั้งเดิมกับกรณีดังกล่าวได้ ประเทศเหล่านี้จึงต้องแก้ไขเพิ่มเติมกฎหมายเพื่อกำหนดให้การจารกรรมข้อมูลและโปรแกรมคอมพิวเตอร์

---

[98] ประตูลับ หรือ ทางลับที่จะเข้าไปในโปรแกรม เป็นช่องทางที่ผู้พัฒนาโปรแกรมสร้างทิ้งไว้ เหมือนกับรหัสผ่าน เพื่อใช้เจาะเข้าสู่ระบบโดยไม่ต้องผ่านระบบรักษาความปลอดภัยของเครื่องในภายหลัง

[99] สำนักงานเลขานุการ คณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, <u>โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ (ฉบับปรับปรุงครั้งที่ 2)</u> (กรุงเทพมหานคร : โรงพิมพ์เดือนตุลา, 2544), หน้า 67.

[100] เรื่องเดียวกัน, หน้า 130.

[101] Canada Criminal Code Section 283(1)

[102] Japan Penal Code Articles 235, 252, 253

[103] France Penal Code Section 379

เป็นความผิดอาญา เช่น ประเทศฟินแลนด์[104] เยอรมนี[105] กรีซ[106] เนเธอร์แลนด์[107] สวีเดน[108] จีน[109] และสหรัฐอเมริกา[110]

เมื่อการจารกรรมข้อมูลคอมพิวเตอร์เป็นการกระทำที่เกิดกับคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตโดยเฉพาะ ซึ่งอาจกล่าวได้ว่าเป็นความผิดฐานใหม่เช่นเดียวกับการเข้าสู่ระบบข้อมูลโดยมิชอบ ดังนั้น หลายประเทศจึงประสบปัญหาความไม่เพียงพอของกฎหมายภายในที่จะบังคับใช้กับความผิดดังกล่าว ซึ่งจะมีผลทำให้ไม่สามารถดำเนินคดีและลงโทษผู้กระทำความผิดได้

9) **การทำให้เสียหายหรือทำลายข้อมูลหรือโปรแกรมคอมพิวเตอร์** (Computer Sabotage)

การสร้างความเสียหายหรือทำลายระบบข้อมูลหรือโปรแกรมคอมพิวเตอร์ เป็นการแทรกแซงระบบข้อมูลและการทำงานของคอมพิวเตอร์ที่ได้รับความนิยมมากที่สุด วิธีการที่ใช้เพื่อทำลายที่ได้รับความนิยม เช่น การปล่อยไวรัส หรือหนอนคอมพิวเตอร์ เพื่อให้ไปทำลายระบบการทำงานของคอมพิวเตอร์ผู้อื่น การสร้างโปรแกรมม้าโทรจัน[111] หรือการทำให้ Web Site ปฏิเสธการให้บริการ เป็นต้น

การปล่อยไวรัส (Viruses) และหนอนคอมพิวเตอร์ (Worms) สร้างความเสียหายไม่แตกต่างกัน กล่าวคือ ทั้งไวรัสและหนอนคอมพิวเตอร์ ต่างเป็นโปรแกรมที่ถูกสร้างขึ้น เพื่อทำให้

---

[104] Finnish Penal Code Section 28:7

[105] German Penal Code Sections 201, 203(3), Federal Data Protection Act 1997 Section 43

[106] Greece Criminal Code Article 320(2)

[107] Netherlands Criminal Code Articles 98-98d

[108] Sweden Criminal Code Section 14 : 9

[109] China Criminal Code Articles 285-287

[110] U.S.C. Title 18 Section1030(a)

[111] โปรแกรมม้าโทรจัน คือ การเขียนโปรแกรมคอมพิวเตอร์ที่แฝงไว้ในโปรแกรมที่มีประโยชน์ เมื่อถึงเวลาโปรแกรมที่ไม่ดีจะปรากฏตัวขึ้นมาเพื่อปฏิบัติการทำลายข้อมูล วิธีนี้มักใช้กับการฉ้อโกงทางคอมพิวเตอร์หรือการทำลายระบบหรือข้อมูลคอมพิวเตอร์

การทำงานของเครื่องที่ติดเชื้อเปลี่ยนแปลงไป เมื่อเครื่องคอมพิวเตอร์หรือโปรแกรมติดเชื้อ ก็จะสามารถกระจายไปยังเครื่องอื่นได้ เนื่องจากโปรแกรมไวรัสและหนอนสามารถทำซ้ำตัวเองเพื่อแพร่กระจายได้ ไวรัสและหนอนที่มีชื่อเสียงเนื่องจากความสามารถในการทำลายคอมพิวเตอร์ไปทั่วโลกที่เคยเกิดขึ้น เช่น I Love U Bug ซึ่งมีส่วนประกอบของทั้งไวรัสและหนอน ให้ผลการแพร่กระจายเร็วกว่าไวรัสเมลิสซ่า (Melissa) ของสหรัฐอเมริกากว่า 9 เท่า มีผลทำให้เครื่องคอมพิวเตอร์มากกว่า 1 ล้านเครื่องในอเมริกาเหนือและประเทศต่าง ๆ ทั่วโลกที่ได้รับอีเมล์ I Love U Bug ได้รับความเสียหาย โดยเฉพาะอย่างยิ่งในประเทศสหรัฐอเมริกาที่ได้รับผลความเสียหายมากกว่าประเทศอื่น บริษัทธุรกิจยักษ์ใหญ่หลายบริษัท เช่น บริษัท AT&T, Ford Motor Co.,Ltd. Merrill Lynch & Co.,Ltd. ต้องปิดการให้บริการอีเมล์ของตนเองทั้งหมดเพื่อป้องกันการแพร่กระจายของ I Love U Bug จากการสืบสวนของเจ้าหน้าที่สหรัฐฯ พบว่า I Love U Bug ถูกปล่อยออกมาจากประเทศฟิลิปปินส์ แต่ทางการฟิลิปปินส์ไม่สามารถจัดการกับผู้กระทำความผิดรายนี้ได้ เนื่องจากไม่มีกฎหมายภายในใช้บังคับกับไวรัสคอมพิวเตอร์[112]

นอกจากนี้ ในคดีที่เกี่ยวกับการลำลายระบบคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตที่เป็นคดีใหญ่อีกคดีหนึ่งคือคดี United States v. Morris มีข้อเท็จจริงว่า จำเลยสร้างไวรัสที่มีชื่อว่า Melissa และส่งข้อความ (E-mail) ดังกล่าวไปยังกลุ่มที่มีการอภิปรายเรื่องเพศทางอินเทอร์เน็ต ซึ่งเครื่องที่เปิดข้อความดังกล่าวจะติดไวรัส ซึ่งจะส่งผลให้ระบบความปลอดภัยของเครื่องน้อยลง ทำให้ติดไวรัสชนิดอื่นง่ายขึ้น นอกจากนี้ โปรแกรมไวรัสถูกตั้งไว้ให้ทำซ้ำตัวเอง และอีเมล์ไปยังบุคคลอื่น โดยอัตโนมัติ ผลของไวรัสทำให้เครื่องติดไวรัสกว่า 1 ล้านเครื่องทั่วประเทศสหรัฐอเมริกา ทั้งภาคธุรกิจ, มหาวิทยาลัย และระบบงานที่สำคัญของรัฐบาลสหรัฐฯ ประมาณค่าความเสียหายกว่า 80 ล้านเหรียญสหรัฐฯ ซึ่งในคดีนี้ ศาลตัดสินให้จำเลยมีความผิด ตาม Title 18 US. Code Section 1030 (a)(5)(A)[113]

คดีที่ได้ยกตัวอย่างมาข้างต้นนั้น แสดงให้เห็นถึงความร้ายแรงของการทำลายโดยโปรแกรมไวรัสและหนอนคอมพิวเตอร์ อย่างไรก็ตาม ไม่เพียงแต่ไวรัสและหนอนคอมพิวเตอร์เท่านั้นที่ใช้ทำลายหรือสร้างความเสียหาย โปรแกรมโลจิกบอมบ์ และม้าโทรจัน ก็เป็นโปรแกรมที่

---

[112] นพมาศ ประสิทธิ์มณฑล, อาชญากรรมคอมพิวเตอร์ตามกฎหมาย US. [Online],(2002, May 27), แหล่งที่มา : http://www.geocities.com/elaw007/article/cybercrime270502.html [2003, Mar 16]

[113] ทวีศักดิ์ กออนันตกูล , "อาชญากรรมในยุคโลกาภิวัฒน์," บทบัณฑิตย์ 55,1 : 33.

ได้รับความนิยม โดยโลจิกบอมบ์คือโปรแกรมที่เหมือนระเบิดเวลาที่ฝังตัวอยู่เพื่อรอเวลาสร้างความเสียหายตามที่ถูกกำหนดไว้หรือเมื่อเกิดสถานการณ์ตามที่กำหนดไว้เกิดขึ้น ส่วนโปรแกรมม้าโทรจัน เป็นโปรแกรมแฝงในโปรแกรมที่มีประโยชน์เมื่อถึงเวลาที่กำหนด โปรแกรมที่ไม่ดีจะปรากฏตัวขึ้นมาเพื่อทำลายข้อมูลหรือระบบคอมพิวเตอร์[114] นอกจากการสร้างโปรแกรมเพื่อทำลายข้อมูลและระบบคอมพิวเตอร์แล้ว ยังมีวิธีการสร้างความเสียหายบนเครือข่ายอินเทอร์เน็ต โดยวิธีการทำให้ระบบปฏิเสธการให้บริการ หรือ Distributed Denial of Services (DDOS) การโจมตีด้วย DDOS เป็นการทำให้เว็บไซต์เป้าหมายไม่สามารถติดต่อกับคอมพิวเตอร์อื่นได้ โดยผู้กระทำจะติดรหัสไว้ที่ระบบเว็บไซต์เป้าหมาย ทำให้สามารถควบคุมระบบของเว็บไซต์ให้เกิดการติดขัดด้วยการหลั่งไหลของข้อมูลจำนวนมหาศาลจากแหล่งต่าง ๆ เสมือนว่ามีผู้ใช้บริการเว็บไซต์จำนวนมากมายทั้งที่ความเป็นจริงแล้วไม่มีผู้ใช้บริการ ทำให้เว็บไซต์เป้าหมายสูญเสียความสามารถในการให้บริการ การโจมตีแบบ DDOS เกิดขึ้นเมื่อเดือนกุมภาพันธ์ ค.ศ. 2000 เมื่อกลุ่มวัยรุ่นชาวแคนาดา ในนามว่า "MafiaBoy" ถูกกล่าวหาว่าใช้ DDOS โจมตี เพื่อปิดบริการของเว็บไซต์ชื่อดังหลายแห่ง เช่น Yahoo!, Buy.com, E*Trade, CNN.com และเว็บอื่น ๆ โดยปกติการติดตามผู้กระทำ DDOS มีความยากลำบาก เนื่องจากการท่วมของข้อมูลมหาศาล ในคดีนี้ Mofiaboy ได้สร้างเว็บไซต์ Dummy ขึ้น เพื่อเป็นต้นทางในการเรียกข้อความ ทำให้การติดตามยากขึ้นไปอีก อย่างไรก็ตาม FBI ได้สืบทราบข้อมูลของ Mafia Boy จาก Internet Chat Room ซึ่งเป็นสถานที่ที่ผู้กระทำผิดใช้ติดต่อกัน ในที่สุด ผู้กระทำความผิดซึ่งเป็นเด็กชายวัย 15 ปี ก็ถูกเจ้าหน้าที่ตำรวจแคนาดาจับกุมได้ และศาลได้พิพากษาให้จำเลยมีความผิดฐานทำให้เกิดความเสียหายแก่ข้อมูลคอมพิวเตอร์ (Mischeif of Data) [115]

การทำให้เกิดความเสียหายแก่ระบบคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตดังเช่นที่ได้กล่าวมาข้างต้นเป็นการกระทำที่เกิดขึ้นอย่างแพร่หลาย จึงทำให้หลายประเทศกำหนดเป็นความผิดอาญา เช่น ออสเตรีย[116] แคนาดา[117] เดนมาร์ก[118] เยอรมนี[119] ฟินแลนด์[120] ฝรั่งเศส[121] ญี่ปุ่น[122]

---

[114] สำนักงานเลขานุการ คณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ (ฉบับปรับปรุงครั้งที่ 2), : หน้า 53-54.

[115] นพมาศ ประสิทธิ์มณฑล, อาชญากรรมคอมพิวเตอร์ตามกฎหมาย US. [Online], (27May 2002), แหล่งที่มา : http://www.geocities.com/elaw007/article/cybercrime270502.html [2003, Mar 16]

[116] Austria Penal Code Selection 126a

[117] Canada Criminal Code Section 430 (1.1)

เนเธอร์แลนด์[123] สเปน[124] สวีเดน[125] สวิตเซอร์แลนด์[126] อังกฤษ[127] และสหรัฐอเมริกา[128] ซึ่งความผิดฐานนี้เป็นความผิดเฉพาะที่เกิดขึ้นกับคอมพิวเตอร์เท่านั้น ประเทศต่างๆจึงต้องแก้ไขปรับปรุงกฎหมายให้ทันต่อสภาพทางเทคโนโลยี แต่ในความเป็นจริงแล้ว ทุกประเทศยังไม่สามารถแก้ไขกฎหมายได้ทันกับความเจริญทางเทคโนโลยี ซึ่งในคดี I Love U Bug ประเทศฟิลิปปินส์ก็ประสบปัญหาการขาดกฎหมายเพื่อบังคับใช้ลงโทษผู้กระทำความผิด ซึ่งส่งผลทำให้ไม่สามารถส่งผู้ร้ายข้ามแดนให้กับประเทศสหรัฐอเมริกาซึ่งเป็นประเทศที่ประสบความเสียหายจากการกระทำดังกล่าวได้อีกด้วย ซึ่งในประเด็นนี้ผู้เขียนจะได้วิเคราะห์โดยละเอียดต่อไป

10) **การฉ้อโกงทางคอมพิวเตอร์** (Computer Fraud)

ในปัจจุบัน ความผิดฐานฉ้อโกง เป็นความผิดที่ทุกประเทศกำหนดให้เป็นความผิดอาญา เมื่อการฉ้อโกงพัฒนาจากรูปแบบดั้งเดิม ซึ่งเป็นการกระทำระหว่างบุคคลต่อบุคคลไปสู่การฉ้อโกงทางคอมพิวเตอร์ โดยการแสดงข้อความเท็จต่อคอมพิวเตอร์เพื่อให้คอมพิวเตอร์ที่ถูกตั้งโปรแกรมการทำงานอัตโนมัติมอบทรัพย์สินแก่ผู้กระทำ โดยการกระทำดังกล่าวทำให้ได้ไปซึ่งทรัพย์สินของผู้อื่น ดังนั้น แม้รูปแบบของการกระทำจะเปลี่ยนไป แต่ลักษณะและผลของการกระทำไม่แตกต่างกัน จึงมิอาจกล่าวได้ว่า การกระทำรูปแบบใหม่ไม่เป็นความผิด หากแต่บางประเทศ เช่น ประเทศไทย หรือประเทศในกลุ่มประมวลกฎหมายอื่น อาจประสบปัญหาการไม่สามารถปรับ

---

[118] Danish Penal Code Section 193

[119] German Penal Code Section 330 a และ 303 b

[120] Finnish Penal Code Chapter 35 Section 1-3 (แก้ไขปี ค.ศ. 1990) และ Chapter 34 Section 1 (แก้ไขปี ค.ศ. 1995)

[121] France Penal Code Article 462-3 และ 462-4

[122] Japan Penal Code Article 234-2, 258, 259

[123] Netherlands Criminal Code Article 350a, 350b

[124] Spain Criminal Code Article 264.2

[125] Sweden Data Protection Act Section 21

[126] Swiss Criminal Code Article 144 bis

[127] UK Computer Misuse Act 1990 Section 3

[128] U.S.C. Title 18 Section 1030 (a)(5)

ใช้กฎหมายอาญาดั้งเดิมกับการฉ้อโกงทางคอมพิวเตอร์ อันเนื่องมาจากปัญหาด้านการตีความกฎหมายลายลักษณ์อักษร อย่างไรก็ตาม แม้จะประสบปัญหาด้านการตีความ แต่โดยลักษณะของการกระทำแล้วก็ถือเป็นการกระทำฉ้อโกง ซึ่งเมื่อการกระทำความผิดฐานฉ้อโกงแบบดั้งเดิมเป็นการกระทำที่มีความผิดทางอาญา ดังนั้น การกระทำความผิดฐานฉ้อโกงที่เพียงแต่เปลี่ยนรูปแบบและวิธีการกระทำความผิด ก็ควรกำหนดให้เป็นความผิดอาญาเช่นกัน

การฉ้อโกงทางคอมพิวเตอร์ที่เกิดขึ้นส่วนใหญ่เป็นการฉ้อโกงด้านการเงิน เนื่องจากในปัจจุบัน การทำธุรกรรมด้านการเงินบนเครือข่ายอินเทอร์เน็ต รวมทั้งการถ่ายโอนข้อมูลด้านการเงิน การธนาคารผ่านเครือข่ายอินเทอร์เน็ตหรือการใช้รหัสบัตรเครดิตของผู้อื่นโดยอาชญากรจะดักสกัดรหัสและหมายเลขบัตรจากเจ้าของบัตรขณะใช้บัตรเพื่อซื้อสินค้าหรือบริการทางอินเทอร์เน็ตได้รับความนิยมสูง ตัวอย่างเช่น ธนาคารซิตี้แบงก์ของสหรัฐอเมริกา สูญเสียเงินเป็นจำนวนกว่า 10 ล้านเหรียญสหรัฐฯ เนื่องจากถูกนักเจาะระบบชาวรัสเซีย Vladimir Levin ฉ้อโกงเงินทางคอมพิวเตอร์ Levin ใช้เครื่องคอมพิวเตอร์จากลอนดอน เจาะระบบเข้าสู่ฐานข้อมูลของธนาคารซิตี้แบงก์ของสหรัฐอเมริกา เพื่อขโมยรหัสลูกค้าและรหัสผ่าน จากนั้นก็ใช้รหัสดังกล่าวโอนเงินออนไลน์เข้าบัญชีของเขาในประเทศสหรัฐอเมริกา ฟินแลนด์ เนเธอร์แลนด์ เยอรมนี และอิสราเอล Levin ถูกจับกุมที่กรุงลอนดอน ประเทศอังกฤษ และถูกส่งตัวข้ามแดนมาดำเนินคดีที่ประเทศสหรัฐอเมริกา โดยศาลตัดสินให้ลงโทษจำคุก 3 ปี และชดใช้ค่าเสียหายเป็นเงิน 240,015 เหรียญสหรัฐฯ[129]

แม้การกระทำดังกล่าวจะเห็นได้ชัดเจนว่าเป็นความผิดฐานฉ้อโกงซึ่งทุกประเทศบัญญัติไว้เป็นความผิดอาญา แต่เนื่องจากการเปลี่ยนแปลงของรูปแบบและวิธีการกระทำความผิดทำให้เกิดข้อจำกัดของกฎหมายอาญาดั้งเดิมของหลายประเทศ ที่ไม่สามารถปรับใช้กับการฉ้อโกงทางคอมพิวเตอร์ได้ เช่นเดียวกับข้อขัดข้องตามกฎหมายไทย เช่น ประเทศออสเตรีย เบลเยี่ยม เยอรมนี ฝรั่งเศส ญี่ปุ่น ลักเซมเบิร์ก และสวิตเซอร์แลนด์[130] ต่อมาเพื่อหลีกเลี่ยงปัญหาในการตีความกฎหมายอาญา หลายประเทศจึงบัญญัติกฎหมายการฉ้อโกงทางคอมพิวเตอร์ขึ้นโดยเฉพาะ เช่น ในประเทศออสเตรเลีย[131] ออสเตรีย[132] เดนมาร์ก[133] เยอรมนี[134] ฟินแลนด์[135] กรีซ[136]

---

[129] Russian hackers arrested[Online], 24 May 2001, Available from: http://www.cnn.com/2001/TECH/internet/05/24/russia.hackers/ [2002, Nov. 30]

[130] Ulrich Sieber, "Legal aspect of computer - Related crime in the information society - COMCRIME - study", p. 82.

[131] Australian Cybercrime Act 2001

ลักเซมเบิร์ก[137] ญี่ปุ่น[138] เนเธอร์แลนด์[139] นอร์เวย์[140] สเปน[141] สวีเดน[142] และสหรัฐอเมริกา[143] โดยการบัญญัติกฎหมายเฉพาะเพื่อจะแก้ปัญหาความขัดข้องของกฎหมายเดิมที่ไม่สามารถใช้บังคับได้ในกรณีที่ผู้ถูกหลอกลวงเป็นเครื่องคอมพิวเตอร์ไม่ใช่บุคคล ดังนั้น การเจาะระบบคอมพิวเตอร์ของธนาคาร หรือการขโมยข้อมูลบัตรเครดิต หรือการกระทำใดที่เป็นการกระทำการฉ้อโกงต่อระบบคอมพิวเตอร์เพื่อให้ได้มาซึ่งเงินหรือทรัพย์สิน ถือเป็นความผิดฐานฉ้อโกงทางคอมพิวเตอร์ทั้งสิ้น

คดีอาชญากรรมคอมพิวเตอร์ที่เกิดขึ้นทั้งหมดนี้ จะเห็นได้ว่า การก่ออาชญากรรมคอมพิวเตอร์นั้น เป็นการก่อความเสียหายในวงกว้างและส่งผลกระทบของการกระทำในหลายประเทศในคราวเดียวกัน ดังนั้น แม้ว่าจะไม่สามารถมองเห็นถึงความเสียหายที่เป็นรูปธรรมได้ชัดเจนเหมือนการก่ออาชญากรรมอื่นๆ ซึ่งการก่ออาชญากรรมอื่นๆนั้น บางครั้งจะปรากฏภาพความเสียหายที่ดูเหมือนรุนแรง แต่ความเสียหายในมูลค่าของทรัพย์สินมีไม่มากนัก ในขณะที่การก่ออาชญากรรมคอมพิวเตอร์ก่อให้เกิดความเสียหายที่ไม่เห็นโดยชัดเจน แต่ได้สร้างความเสียหายทางด้านทรัพย์สินแก่ผู้เสียหายมากจนประมาณค่าไม่ได้ ซึ่งมีความร้ายแรงกว่าอาชญากรรมอื่นๆมาก ทำให้อาชญากรรมคอมพิวเตอร์กลายเป็นปัญหาที่ประเทศทั้งหลายให้ความสนใจในการป้องกันและปราบปรามเป็นอย่างมาก

---

[132] Austria Criminal Code Section 148a

[133] Danish Penal Code Section 279a

[134] German Penal Code Section 263a

[135] Finnish Penal Code Chapter 36 Section 1

[136] Greece Criminal Code Article 386A

[137] Luxembourg Penal Code Article 509-2 และ 509-3

[138] Japan Penal Code Article 264-2

[139] Netherlands Criminal Code Article 326 C

[140] Norway Penal Code Section 270 (2)

[141] Spain Criminal Code Article 248.2, 239 en fine

[142] Sweden Criminal Code Chapter 9 Section 1

[143] U.S.C. Title 18 Section 1030 (a) (4)

จากการศึกษาถึงความหมาย ลักษณะและความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์มาทั้งหมดนี้ ทำให้ทราบว่า ระบบคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตมีลักษณะการทำงานที่พิเศษและซับซ้อน ซึ่งส่งผลให้การกระทำความผิดบนเครือข่ายสามารถเกิดได้มากมายหลายรูปแบบ ทั้งในกรณีที่เป็นการกระทำความผิดอาญาดั้งเดิมแต่กระทำผ่านสื่ออินเทอร์เน็ต และในกรณีความผิดที่เกิดขึ้นใหม่ซึ่งเป็นความผิดที่เกิดกับคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตโดยเฉพาะ ซึ่งทั้งหมดนี้ล้วนแต่ทำให้อาชญากรรมคอมพิวเตอร์เป็นความผิดฐานใหม่ที่มีลักษณะเฉพาะแตกต่างจากความผิดอาญาทั่วไป ซึ่งแม้หลายประเทศมีการพัฒนากฎหมายภายในเพื่อรองรับกับสถานการณ์อาชญากรรมคอมพิวเตอร์แล้ว แต่ยังคงมีหลายประเทศที่ยังไม่มีการพัฒนากฎหมายภายใน ทำให้ขาดกฎหมายภายในที่จะใช้กับอาชญากรรมคอมพิวเตอร์

การที่อาชญากรรมคอมพิวเตอร์เป็นความผิดฐานใหม่ที่มีลักษณะพิเศษเฉพาะดังกล่าว ประกอบกับการที่หลายประเทศขาดกฎหมายภายในที่จะบังคับใช้กับการกระทำเช่นว่านี้ ทำให้อาชญากรรมคอมพิวเตอร์เป็นความผิดที่ประเทศต่างๆประสบปัญหาในการให้ความร่วมมือระหว่างประเทศในการส่งผู้ร้ายข้ามแดน ซึ่งในส่วนต่อไปนี้ผู้เขียนจะได้ศึกษาต่อไปว่าจากการที่อาชญากรรมคอมพิวเตอร์เป็นความผิดฐานใหม่ที่มีลักษณะพิเศษเฉพาะนี้ จะก่อให้เกิดปัญหาและอุปสรรคในการให้ความร่วมมือระหว่างประเทศในการส่งผู้ร้ายข้ามแดนอย่างไร

3.2 ปัญหาในการปรับใช้กฎหมายว่าด้วยการส่งผู้ร้ายข้ามแดนในคดีอาชญากรรมคอมพิวเตอร์

จากที่ได้ทำการศึกษาถึงลักษณะของอาชญากรรมคอมพิวเตอร์ ทำให้ทราบว่านอกจากอาชญากรรมคอมพิวเตอร์จะเป็นความผิดอาญาฐานใหม่ที่มีลักษณะพิเศษเฉพาะแตกต่างจากความผิดอาญาฐานอื่นๆแล้ว อาชญากรรมคอมพิวเตอร์ยังมีลักษณะระหว่างประเทศเนื่องจากการกระทำความผิดบนเครือข่ายมีลักษณะไร้พรมแดน ทำให้การนำตัวผู้กระทำความผิดมาลงโทษตามกฎหมายนั้น ต้องกระทำโดยอาศัยความร่วมมือระหว่างประเทศในการส่งผู้ร้ายข้ามแดนเพื่อให้รัฐที่ได้รับความเสียหายจากการกระทำความผิดสามารถดำเนินคดีและลงโทษผู้กระทำความผิดได้ ซึ่งความร่วมมือระหว่างประเทศในการส่งผู้ร้ายข้ามแดนนั้น ก็ต้องอาศัยหลักเกณฑ์ว่าด้วยการส่งผู้ร้ายข้ามแดนมาปรับใช้กับคดีอาชญากรรมคอมพิวเตอร์ แต่จากการศึกษาพบว่าบ่อยครั้งที่รัฐประสบปัญหาในการนำหลักเกณฑ์ว่าด้วยการส่งผู้ร้ายข้ามแดนมาปรับใช้กับคดีอาชญากรรมคอมพิวเตอร์ ดังนั้น ในหัวข้อนี้ผู้เขียนจะได้ทำการศึกษาวิเคราะห์ถึงปัญหาและอุปสรรคที่เกิดจากการปรับใช้หลักเกณฑ์ว่าด้วยการส่งผู้ร้ายข้ามแดนในคดีอาชญากรรมคอมพิวเตอร์ ที่ทำให้รัฐไม่สามารถส่งผู้ร้ายข้ามแดนในคดีอาชญากรรมคอมพิวเตอร์ได้อย่างมีประสิทธิภาพ ดังจะได้กล่าวต่อไปนี้ คือ

3.2.1 ปัญหาที่สืบเนื่องจากหลักความผิดอาญาของทั้งสองประเทศ

จากการศึกษาหลักเกณฑ์ว่าด้วยการส่งผู้ร้ายข้ามแดนในบทที่ 2 ทำให้ทราบว่า หลักความผิดอาญาของทั้งสองประเทศซึ่งเป็นหลักเกณฑ์สำคัญในการพิจารณาส่งผู้ร้ายข้ามแดนในปัจจุบันนั้น ทำให้การส่งผู้ร้ายข้ามแดนต้องพิจารณากฎหมายภายในของทั้งสองรัฐเป็นสำคัญ จากหลักดังกล่าวทำให้การพิจารณาส่งผู้ร้ายข้ามแดนในกรณีอาชญากรรมคอมพิวเตอร์ต้องได้ความว่ากฎหมายภายในของรัฐผู้ร้องขอและของรัฐผู้รับคำขอมีการกำหนดให้อาชญากรรมคอมพิวเตอร์เป็นความผิดตามกฎหมายภายใน แต่จากการศึกษาพบว่า บทบัญญัติของกฎหมายภายในเกี่ยวกับอาชญากรรมคอมพิวเตอร์กลายเป็นปัญหาและอุปสรรคที่สำคัญประการหนึ่งที่ทำให้รัฐไม่สามารถส่งผู้ร้ายข้ามแดนได้อย่างมีประสิทธิภาพ ซึ่งในการศึกษาถึงปัญหาในส่วนนี้ ผู้เขียนจะได้หยิบยกกฎหมายอาชญากรรมคอมพิวเตอร์ของประเทศที่มีความแตกต่างจากกฎหมายของประเทศอื่นอย่างเด่นชัดขึ้นมาพิจารณาประกอบเพื่อให้เห็นถึงปัญหาได้อย่างชัดเจน และเพื่อความสะดวกในการวิเคราะห์ผู้เขียนได้แบ่งการพิจารณาเป็น 2 กรณีคือ กรณีที่ปัญหาเกิดขึ้นเนื่องจาก

การขาดแคลนกฎหมายภายในเกี่ยวกับอาชญากรรมคอมพิวเตอร์ และกรณีที่ปัญหาเกิดจากความไม่สอดคล้องกันของกฎหมายอาชญากรรมคอมพิวเตอร์ โดยมีรายละเอียดดังต่อไปนี้

3.2.1.1 การขาดแคลนกฎหมายภายในเกี่ยวกับอาชญากรรมคอมพิวเตอร์

จากการศึกษาถึงลักษณะของอาชญากรรมคอมพิวเตอร์ทำให้ทราบว่า อาชญากรรมคอมพิวเตอร์เป็นความผิดฐานใหม่ที่มีลักษณะพิเศษเฉพาะแตกต่างจากกฎหมายอาญาทั่วไป ดังนั้น รัฐจึงต้องตรากฎหมายภายในขึ้นบังคับใช้กับอาชญากรรมคอมพิวเตอร์ แต่จากการศึกษาพบว่าในหลายรัฐยังคงไม่มีการบัญญัติกฎหมายขึ้นมารองรับปัญหาอาชญากรรมคอมพิวเตอร์ ซึ่งนอกจากจะก่อให้เกิดปัญหาการขาดแคลนกฎหมายภายในที่จะนำมาใช้ปราบปรามอาชญากรรมในประเทศแล้ว ยังก่อให้เกิดปัญหาการไม่สามารถให้ความร่วมมือในทางระหว่างประเทศได้อีกด้วย ซึ่งในทางปฏิบัติของรัฐพบว่า เกิดปัญหาการส่งผู้ร้ายข้ามแดนในกรณีอาชญากรรมคอมพิวเตอร์เนื่องจากการขาดกฎหมายภายในเกี่ยวกับอาชญากรรมคอมพิวเตอร์ ซึ่งทำให้ไม่สามารถส่งผู้ร้ายข้ามแดนได้ ดังเช่นที่คดีการส่งผู้ร้ายข้ามแดนในกรณีอาชญากรรมคอมพิวเตอร์ซึ่งประเทศสหรัฐอเมริการ้องขอให้ประเทศฟิลิปปินส์ส่งตัวผู้กระทำความผิดในคดีไวรัส Love Bug แต่เนื่องจากในขณะนั้นประเทศฟิลิปปินส์ซึ่งเป็นประเทศผู้รับคำขอ ไม่มีกฎหมายภายในที่กำหนดให้การกระทำดังกล่าวเป็นความผิดอาญา ประเทศฟิลิปปินส์ปฏิเสธการส่งผู้ร้ายข้ามแดนในคดีไวรัส Love Bug ให้แก่ประเทศสหรัฐอเมริกาได้ โดยอ้างว่าการกระทำดังกล่าวไม่เป็นความผิดตามกฎหมายภายในของประเทศฟิลิปปินส์[144]

การปฏิเสธการส่งผู้ร้ายข้ามแดนอันเนื่องมาจากการขาดกฎหมายภายในเกี่ยวกับอาชญากรรมคอมพิวเตอร์นั้น เป็นการปฏิเสธการส่งผู้ร้ายข้ามแดนอันเนื่องมาจากหลักความผิดอาญาของทั้งสองประเทศ กรณีเช่นว่านี้ รัฐผู้รับคำขอจึงมีสิทธิในการอ้างหลักดังกล่าวเพื่อปฏิเสธ

---

[144] Seth Mydans, "Filipino suspect in love bug virus released," New York Times News Service[Online],2000, Oct 5, Available from : http://www.nctimes.com/news/051000/gg.html [2003, June 8]

การส่งผู้ร้ายข้ามแดนได้อย่างชอบธรรม อย่างไรก็ตาม การไม่สามารถส่งผู้ร้ายข้ามแดนในกรณีนี้ทำให้ผู้กระทำความผิดหลุดพ้นจากการลงโทษไปเลย เนื่องจากประเทศฟิลิปปินส์ไม่มีกฎหมายภายในเพื่อใช้ดำเนินคดีและลงโทษแก่ผู้กระทำความผิด ซึ่งเป็นไปตามหลักไม่มีโทษโดยไม่มีกฎหมาย

3.2.1.2 **ความไม่สอดคล้องกันของกฎหมายอาชญากรรมคอมพิวเตอร์**

นอกจากปัญหาการส่งผู้ร้ายข้ามแดนอันเนื่องมาจากการขาดกฎหมายภายในใช้บังคับแล้ว ปัญหาส่งผู้ร้ายข้ามแดนอาจเกิดขึ้นได้แม้ในประเทศที่มีกฎหมายอาชญากรรมคอมพิวเตอร์แล้ว เนื่องจากแต่ละประเทศต่างกำหนดกฎหมายเพื่อความสะดวกในการใช้บังคับเป็นการภายในของตน ทำให้เกิดปัญหาความไม่สอดคล้องกันของกฎหมายซึ่งมีผลทำให้เกิดช่องว่างในการประสานความร่วมมือระหว่างประเทศ ซึ่งผู้เขียนได้แบ่งการพิจารณาออกเป็น 2 กรณี คือ กรณีการขาดเอกภาพในการกำหนดให้การกระทำเป็นความผิดอาญา และกรณีที่มีความแตกต่างของขอบเขตการบังคับใช้ของกฎหมาย ดังจะได้กล่าวต่อไปนี้

1) **การขาดความเป็นเอกภาพในการกำหนดให้การกระทำเป็นความผิดอาญา**

ปัญหาการขาดความเป็นเอกภาพในการกำหนดการกระทำที่เป็นความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์เกิดขึ้นเนื่องจากความแตกต่างในด้านทัศนคติของแต่ละประเทศ อันสืบเนื่องมาจากความแตกต่างของสภาพสังคม วัฒนธรรม วิถีชีวิตของประชาชนในสังคม และความเป็นมาในทางประวัติศาสตร์ของแต่ละประเทศ ทำให้ในความผิดบางฐาน ได้แก่ ความผิดเกี่ยวกับการเผยแพร่ภาพลามกอนาจารผู้ใหญ่และความผิดเกี่ยวกับการก่อให้เกิดความเกลียดชังทางเชื้อชาติ ถูกบัญญัติเป็นความผิดในบางประเทศ ในขณะที่บางประเทศไม่ถือเป็นการกระทำที่เป็นความผิดอาญา ดังนั้น จึงอาจเกิดปัญหาในการส่งผู้ร้ายข้ามแดน ซึ่งจะได้กล่าวในรายละเอียดดังต่อไปนี้

ก) <u>ความผิดเกี่ยวกับการเผยแพร่ภาพลามกอนาจาร</u>

ความไม่เป็นเอกภาพของกฎหมายเกี่ยวกับการเผยแพร่ภาพลามกอนาจารผู้ใหญ่นั้นสามารถพิจารณาได้ใน 2 ประเด็น คือ ความไม่เป็นเอกภาพของกฎหมายที่เกิดจากกฎหมายของบางประเทศถือว่าการเผยแพร่ภาพลามกอนาจารผู้ใหญ่เป็นการกระทำที่ไม่ผิดกฎหมาย และ

ประเด็นเกี่ยวกับมาตรฐานในการพิจารณาขนาดของความลามกอนาจารซึ่งเป็นความผิดตามกฎหมาย

ความไม่เป็นเอกภาพของกฎหมายในประเด็นแรก คือ ความไม่เป็นเอกภาพของกฎหมายที่เกิดจากการที่กฎหมายของบางประเทศถือว่าการเผยแพร่ภาพลามกอนาจารผู้ใหญ่เป็นการกระทำที่ไม่เป็นความผิดตามกฎหมาย ซึ่งตัวอย่างที่เห็นได้อย่างชัดเจนได้แก่กฎหมายของประเทศเบลเยี่ยม[145] เนเธอร์แลนด์และบางประเทศในยุโรปตะวันออก[146] ซึ่งกำหนดให้การเผยแพร่ภาพลามกอนาจารเป็นการกระทำที่สามารถกระทำได้ตามกฎหมาย ดังนั้น การเผยแพร่ภาพลามกอนาจารผู้ใหญ่ผ่านอินเทอร์เน็ตจากเว็บไซต์ของประเทศเหล่านี้ จึงไม่เป็นความผิดตามกฎหมาย แต่เนื่องจากสภาพของเครือข่ายอินเทอร์เน็ตที่ภาพลามกสามารถเข้าสู่เครือข่ายและผู้ชมจากประเทศอื่นๆสามารถเข้าชมได้ เมื่อผู้ใช้บริการอินเทอร์เน็ตจากประเทศอื่นๆเปิดเว็บไซต์ของลามกของประเทศเบลเยี่ยมและเนเธอร์แลนด์ ทำให้ภาพลามกอนาจารเข้าไปเผยแพร่อยู่ในดินแดนของรัฐอื่นซึ่งอาจมีกฎหมายห้ามการเผยแพร่ภาพลามกอนาจารผู้ใหญ่ ผลจึงทำให้ประเทศที่ห้ามการเผยแพร่นั้น ไม่สามารถร้องขอให้ส่งตัวผู้เผยแพร่ภาพลามกซึ่งอยู่ในประเทศเบลเยี่ยมหรือเนเธอร์แลนด์นี้มาลงโทษได้ เนื่องจากการกระทำดังกล่าวไม่เป็นความผิดอาญาตามกฎหมายของอีกรัฐหนึ่ง

ปัญหาความไม่เป็นเอกภาพของกฎหมายอีกประการหนึ่งเป็นปัญหาที่เกิดขึ้นระหว่างประเทศที่มีกฎหมายควบคุมการเผยแพร่ภาพลามกอนาจาร ซึ่งเป็นความไม่เป็นเอกภาพของกฎหมายในประเด็นที่สอง ได้แก่ ประเด็นเกี่ยวกับมาตรฐานในการพิจารณาขนาดของความลามกอนาจารซึ่งเป็นความผิดตามกฎหมาย ซึ่งแต่ละประเทศก็มีมาตรฐานในการกำหนดความลามกอนาจารที่เป็นความผิดต่อกฎหมายแตกต่างกัน เป็นผลทำให้มาตรการทางกฎหมายที่ใช้บังคับกับสื่อลามกอนาจารมีความแตกต่างกันตามไปด้วย เนื่องจากการวินิจฉัยว่าสิ่งใดเป็นสิ่งลามก

---

[145] Laura J. Lederer, The protection project, commercial sexual exploitation of woman and children : A human rights report[Online],2001, Available from: http://209.190.246.239/protectionproject/Hrrpdf/Belgium.pdf [2002, Dec. 24]

[146] 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 : 340.

อนาจารซึ่งจะถือว่าผิดกฎหมายได้ ก็ต้องขึ้นอยู่กับมาตรฐานในสังคมที่มีการวินิจฉัยนั้น จึงทำให้เกิดความยากลำบากในการหามาตรฐานจากการกระทำบนเครือข่ายอินเทอร์เน็ต[147] ภาพที่ในประเทศหนึ่งเห็นว่าเป็นภาพลามกและเป็นความผิดอาญา จึงอาจไม่ใช่ภาพลามกตามมาตรฐานของสังคมในอีกรัฐหนึ่งก็ได้

ตัวอย่างของกฎหมายที่มีความเข้มงวดในการควบคุมการเผยแพร่ภาพลามกอนาจาร เช่น ประเทศสิงคโปร์ ที่มีกฎหมายเกี่ยวกับการเผยแพร่ภาพลามกอนาจารผู้ใหญ่ทางอินเทอร์เน็ตที่เข้มงวด โดยกฎหมายของสิงคโปร์ห้ามการเผยแพร่ภาพที่ก่อให้เกิดความเสื่อมเสียแก่สถานะภาพทางสังคมและศาสนา[148] ทำให้รัฐบาลสิงคโปร์ควบคุมสื่ออินเทอร์เน็ตอย่างเข้มงวดมิให้มีการนำภาพที่เข้าข่ายการก่อให้เกิดความเสื่อมเสียดังกล่าวเข้ามาเผยแพร่ในประเทศ ทำให้ความหมายของภาพลามกในประเทศสิงคโปร์มีความหมายที่กว้างขวางกว่าประเทศอื่นๆ อย่างไรก็ตาม กฎหมายของสิงคโปร์เป็นตัวอย่างในการควบคุมสื่ออินเทอร์เน็ตที่ทำให้ประเทศต่างๆในเอเชียหลายประเทศ เช่น ฮ่องกง และญี่ปุ่นถือปฏิบัติตาม[149]

จากที่กล่าวมานี้ เพื่อแสดงให้เห็นว่าการที่กฎหมายของประเทศต่างๆมีระดับความเข้มงวดในการควบคุมแตกต่างกันและมีมาตรฐานในการใช้ดุลพินิจเพื่อวินิจฉัยความลามกที่แตกต่างกัน ทำให้การส่งผู้ร้ายข้ามแดนกระทำได้ยากลำบากขึ้น เนื่องจากความลามกอนาจารขึ้นอยู่กับมาตรฐานของสังคม ซึ่งไม่อาจหาข้อสรุปได้ในทางระหว่างประเทศ ดังนั้น แม้รัฐผู้ร้องขอสามารถพิสูจน์ได้ว่าการกระทำของจำเลยเป็นการกระทำความผิดเกี่ยวกับการเผยแพร่ภาพลามกอนาจารตามกฎหมายของรัฐตน แต่การส่งผู้ร้ายข้ามแดนอาจถูกปฏิเสธ ถ้าหากรัฐผู้รับคำร้องขอเห็นว่าการกระทำดังกล่าวไม่ถือว่าเป็นความผิดเกี่ยวกับภาพลามกอนาจาร ไม่ว่าจะเนื่องด้วย

---

[147] Jason Kipness, "Revisiting Miller after the striking of the communications decency act : A proposed set of internet specific regulations for pornography on the information superhighway," Santa Clara Computer and High Technology Law Journal 14,391(June 1998) : 7.

[148] 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 : 341.

[149] Ibid., p.342.

เหตุผลที่ว่าการกระทำของจำเลยชอบด้วยกฎหมายของรัฐนั้น หรือภาพที่เผยแพร่ไม่จัดเป็นภาพลามกอนาจารซึ่งเป็นผลให้จำเลยไม่มีความผิดฐานเผยแพร่ภาพลามกอนาจาร

ข) ความผิดเกี่ยวกับการแสดงข้อความที่ก่อให้เกิดความเกลียดชังทางเชื้อชาติ

ความไม่เป็นเอกภาพของกฎหมายของประเทศต่างๆในความผิดเกี่ยวกับการแสดงข้อความที่ก่อให้เกิดความเกลียดชังทางเชื้อชาติ เป็นปัญหาที่สืบเนื่องจากความแตกต่างทางแนวคิดทางการเมืองการปกครองเรื่องสิทธิเสรีภาพของประชาชนในการแสดงความเห็นที่มีขอบเขตที่ต่างกัน ซึ่งผู้เขียนจะได้ยกตัวอย่างประเทศสหรัฐอเมริกา ซึ่งเป็นประเทศที่ให้สิทธิในการพูดหรือแสดงความเห็นอย่างกว้างขวาง จากคำตัดสินของศาลสูงสหรัฐอเมริกาในคดี Chaplinsky v. New Hampshire และคดี Brandenburg v. Ohio[150] แสดงให้เห็นถึงการให้ความสำคัญในการคุ้มครองเสรีภาพในการแสดงออกตามรัฐธรรมนูญสหรัฐอเมริกาอย่างมาก ดังนั้น แม้การแสดงความเห็นหรือการแสดงออกจะมีประเด็นทางด้านเชื้อชาติมาเกี่ยวข้องก็ตาม แต่ประเทศสหรัฐอเมริกาก็ไม่มีกฎหมายที่ควบคุมการแสดงออกของประชาชนเนื่องด้วยจะเป็นการขัดรัฐธรรมนูญ ในขณะที่หลายประเทศกำหนดให้การเผยแพร่ข้อความเหยียดเชื้อชาติ รวมถึงการเผยแพร่ข้อความที่มีความเกี่ยวข้องกับลัทธิการปกครองนาซี เป็นการกระทำที่ผิดกฎหมายอาญา แต่การกระทำดังกล่าวไม่ถือเป็นความผิดตามกฎหมายของประเทศสหรัฐอเมริกา ปัญหาที่เกิดขึ้นคือ หากผู้เผยแพร่ข้อความที่ผิดกฎหมายเนื่องจากมีข้อความเกี่ยวพันถึงเรื่องการเหยียดเชื้อชาติหรือการเผยแพร่ลัทธินาซีผ่านทางอินเทอร์เน็ตอยู่ในประเทศสหรัฐอเมริกา จะมีผลทำให้รัฐอื่นที่อ้างว่าการกระทำอันเป็นความผิดตามกฎหมายซึ่งได้เกิดขึ้นในดินแดนของตนจะไม่สามารถร้องขอให้สหรัฐอเมริกาส่งตัวบุคคลที่เผยแพร่ข้อความดังกล่าวได้

---

[150] คำพิพากษาทั้งสองฉบับนี้วางหลักการพิจารณาไว้อย่างชัดเจนว่า กรณีที่ศาลจะจำกัดเสรีภาพของประชาชน อันจะถือเป็นข้อยกเว้นของหลักเสรีภาพในการแสดงความคิดเห็นได้นั้น จะต้องเป็นการกระทำที่ "ก่อให้เกิดความเสียหายอย่างร้ายแรง หรือมีแนวโน้มที่จะส่งเสริมให้เกิดความไม่สงบสุขในสังคมอย่างฉับพลัน" โดยการจำกัดเสรีภาพต้องเป็น "กรณีจำเป็นเพื่อป้องกันภัยอันตรายหรือสิ่งชั่วร้ายที่คุกคามหรือใกล้จะถึง" รายละเอียดของคดีดูใน Barry Steinhardt, "Hate speech," in The internet, law and society, eds. Yaman Akdeniz, Clive Walker and David Wall (London : Dorset Press, 2000), pp. 253-255.

ปัญหาเช่นว่านี้เกิดขึ้นเป็นข้อพิพาทระหว่างประเทศสหรัฐอเมริกากับประเทศฝรั่งเศส แม้ว่าคดีนี้ไม่ใช่คดีเกี่ยวกับการส่งผู้ร้ายข้ามแดนโดยตรง แต่เป็นคดีที่แสดงให้เห็นถึงการขัดกันซึ่งอำนาจศาลในการวินิจฉัยการกระทำความผิดผ่านทางอินเทอร์เน็ตได้อย่างชัดเจน ข้อพิพาทเกิดขึ้นเนื่องจากการกระทำของคนชาติของประเทศสหรัฐอเมริกาถูกอ้างว่าอยู่ภายใต้เขตอำนาจศาลของรัฐอื่นเนื่องจากลักษณะไร้พรมแดนของเครือข่ายอินเทอร์เน็ต ในคดี Yahoo.com ที่ศาลฝรั่งเศสได้ตัดสินให้ Yahoo! ปิดกั้น (block) เนื้อหาที่เกี่ยวกับนาซี เพื่อป้องกันไม่ให้ผู้ใช้คอมพิวเตอร์ที่ใช้เครือข่ายของฝรั่งเศสเปิดดูได้นั้น โดยภายหลังศาลสหรัฐอเมริกาได้มีคำวินิจฉัยให้เนื้อหาออนไลน์ซึ่งผลิตภายในสหรัฐอเมริกาโดยกิจการชาวอเมริกันได้รับการคุ้มครอง ไม่ต้องปฏิบัติตามกฎหมายของประเทศที่มีความเข้มงวดเรื่องเสรีภาพในการแสดงออกมากกว่า[151] ซึ่งจากคำพิพากษาของศาลสหรัฐอเมริกาในประเด็นนี้ อาจวิเคราะห์ได้ว่าศาลสหรัฐอเมริกายังคงให้ความคุ้มครองเสรีภาพในการแสดงออกอย่างสูงแม้กรณีเป็นการกระทำผ่านเครือข่ายอินเทอร์เน็ตซึ่งการกระทำและผลแห่งการกระทำมิได้จำกัดขอบเขตลงเพียงแค่ในดินแดนของประเทศสหรัฐอเมริกา ทั้งยังเป็นการปฏิเสธไม่ยอมรับการจำกัดเสรีภาพในการแสดงออกตามกฎหมายของประเทศอื่นๆ คดีดังกล่าวสะท้อนให้เห็นว่า หากการแสดงข้อความเหยียดเชื้อชาติหรือการเผยแพร่ข้อความเกี่ยวกับนาซี กระทำขึ้นในประเทศสหรัฐอเมริกาผ่านเครือข่ายอินเทอร์เน็ต ผู้เผยแพร่ย่อมได้รับความคุ้มครองตามกฎหมายสหรัฐอเมริกา มีผลทำให้ผู้กระทำการเผยแพร่ข้อความเหยียดเชื้อชาติหรือการเผยแพร่ข้อความเกี่ยวกับนาซีซึ่งเป็นความผิดตามกฎหมายของประเทศอื่น จะได้รับความคุ้มครองภายใต้กฎหมายสหรัฐอเมริกา โดยสหรัฐอเมริกาก็จะไม่ส่งผู้ร้ายข้ามแดนในความผิดฐานนี้ให้แก่ประเทศอื่น

การไม่ส่งผู้ร้ายข้ามแดนในความผิดฐานนี้เคยเกิดขึ้นในปี ค.ศ.1995 ในคดีของนาย Gary Lauck ซึ่งประเด็นในคดีนี้มีอยู่ว่า นาย Gary Lauck ได้กระทำการเผยแพร่สิ่งพิมพ์ที่มีเรื่องราวเกี่ยวกับลัทธินาซี รวมถึงสิ่งพิมพ์ที่มีเนื้อหาแสดงความเกลียดชังคนเชื้อสายยิวและชาวต่างชาติ ซึ่งต่อมาเจ้าหน้าที่ตำรวจเยอรมนีออกหมายจับในความผิดตามประมวลกฎหมายอาญาเยอรมนี 5 ข้อหา นาย Lauck หลบหนีการจับกุมโดยการอาศัยอยู่ในประเทศสหรัฐอเมริกาที่ซึ่งการกระทำของเขาไม่ถือเป็นความผิดตามกฎหมายสหรัฐอเมริกา ภายใต้รัฐธรรมนูญว่าด้วย

---

[151] นพมาศ ประสิทธิ์มณฑล, ศาลฝรั่งเศสวางกฎเหล็กในการแสดงความคิดเห็นเหนือเขตอำนาจของตน(Cyber-jurisdiction) [Online],(2001, Nov 20), แหล่งที่มา : http://www.geocities.com/elaw007/article16/201_yahoo_fr.html [2003, Mar 16]

เสรีภาพในการแสดงออก ในที่สุดนาย Lauck ถูกจับกุมที่ประเทศเดนมาร์กขณะเข้าร่วมการชุมนุมนาซีนานาชาติ แม้ประเทศเดนมาร์กให้ความคุ้มครองเสรีภาพในการแสดงออกเช่นเดียวกับประเทศสหรัฐอเมริกา แต่เนื่องจากประเทศเดนมาร์กมีพันธกรณีเกี่ยวกับความร่วมมือทางอาญากับประเทศเยอรมนี จึงตกลงส่งตัวนาย Gary Lauck ให้แก่ประเทศเยอรมนี โดยศาลเยอรมนีพิพากษาให้ นาย Gary Lauck ได้รับโทษจำคุก 5 ปี ในความผิดฐานเผยแพร่ข้อความและเครื่องหมายนาซีซึ่งผิดกฎหมาย, โฆษณาชวนเชื่อและแสดงข้อความเพื่อก่อให้เกิดความเกลียดชังต่อกลุ่มเชื้อชาติ[152] เหตุการณ์ที่เกิดขึ้นจะเห็นได้ว่า นาย Gary Lauck ได้รับความคุ้มครองจากการส่งผู้ร้ายข้ามแดนขณะอาศัยอยู่ในประเทศสหรัฐอเมริกา โดยอาศัยหลักเกณฑ์เกี่ยวกับความผิดอาญาของทั้งสองประเทศ ทำให้นาย Gary Lauck ไม่ต้องถูกส่งตัวข้ามแดนจนกระทั่งเดินทางออกนอกประเทศสหรัฐอเมริกา และถูกส่งผู้ร้ายข้ามแดนในขณะอยู่ในประเทศเดนมาร์ก อย่างไรก็ตามคดีของนาย Gary Lauck ก่อให้เกิดประเด็นทางกฎหมายว่า สามารถอ้างเรื่องความผิดทางการเมืองเพื่อเป็นเหตุให้ไม่ต้องส่งตัวข้ามแดนได้หรือไม่ ซึ่งผู้เขียนจะได้วิเคราะห์ปัญหาดังกล่าวต่อไปในเรื่องปัญหาการส่งผู้ร้ายข้ามแดนที่สืบเนื่องจากความผิดทางการเมืองต่อไป

ปัญหาการไม่สามารถส่งผู้ร้ายข้ามแดนเนื่องจากการที่ประเทศสหรัฐอเมริกาไม่กำหนดให้การแสดงข้อความเหยียดเชื้อชาติเป็นความผิดอาญาดังเช่นในคดีของนาย Gary Lauck ไม่เพียงก่อให้เกิดปัญหาในการให้ความร่วมมือกับประเทศเยอรมนีเท่านั้น หากแต่ยังเป็นปัญหากับประเทศในประชาคมยุโรปส่วนใหญ่ ซึ่งมีกฎหมายเช่นเดียวกับเยอรมนี ยิ่งไปกว่านั้น การที่สภายุโรปได้เห็นชอบให้กำหนดเรื่องการเหยียดเชื้อชาติผ่านทางอินเทอร์เน็ตเป็นความผิดอาญาตามอนุสัญญาว่าด้วยอาชญากรรมคอมพิวเตอร์[153] ทำให้ประเทศภาคีสมาชิกของอนุสัญญากำหนดความผิดฐานนี้เป็นความผิดอาญาตามกฎหมายภายในทั้งสิ้น ซึ่งสิ่งที่จะเกิดขึ้นต่อไปในอนาคตเมื่อประเทศต่างๆ ไม่เพียงแต่ประเทศในกลุ่มยุโรปเริ่มให้ความสำคัญในการกำหนดให้การแสดงข้อความเหยียดเชื้อชาติเป็นความผิดอาญา เนื่องจากประชาคมโลกให้ความสำคัญกับเรื่องของความเท่าเทียมกันด้านสิทธิมนุษยชน ประเทศที่ให้เสรีภาพในการแสดงออกเช่นสหรัฐอเมริกาจะ

---

[152] 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 : 344-345.

[153] สำนักงานตำรวจแห่งชาติ, สภายุโรปเพิ่มเรื่องเหยียดผิวเป็นความผิดตามกฎหมายออนไลน์[Online],2000, แหล่งที่มา: http://www.police.go.th/policenews/index.[2003, Mar 16]

กลายเป็นสถานที่ที่ให้ความคุ้มครองแก่อาชญากรที่อาศัยช่องว่างทางกฎหมายหลบเลี่ยงการลงโทษ เนื่องจากการไม่สามารถส่งผู้ร้ายข้ามแดนในความผิดฐานนี้ได้

2) ความแตกต่างของขอบเขตการบังคับใช้ของกฎหมาย

นอกจากในกรณีที่ประเทศต่างๆ มีความเห็นในการกำหนดการกระทำที่เป็นความผิดที่แตกต่างกันซึ่งเป็นผลให้กฎหมายภายในของประเทศต่างๆมีความแตกต่างกันอย่างสิ้นเชิงแล้ว แม้ในกรณีความผิดที่ได้รับการยอมรับกันอย่างทั่วไปว่าเป็นความผิดอาญา ก็ยังมีความแตกต่างกันในขอบเขตการบังคับใช้ของกฎหมาย ซึ่งจะได้กล่าวในรายละเอียดดังต่อไปนี้

ก) การเผยแพร่ภาพลามกอนาจารเด็ก

แม้โดยหลักแล้ว ประเทศส่วนใหญ่จะกำหนดให้การเผยแพร่ภาพลามกอนาจารเด็กผ่านเครือข่ายอินเทอร์เน็ตเป็นความผิดอาญา[154] แต่เมื่อพิจารณาโดยละเอียดแล้วจะพบว่ากฎหมายภายในของประเทศต่างๆยังคงมีความแตกต่างกัน ซึ่งเป็นช่องว่างทางกฎหมายที่อาจส่งผลกระทบต่อการพิจารณาคดีส่งผู้ร้ายข้ามแดนใน 2 ประเด็น ได้แก่ ปัญหาเกี่ยวกับอายุของเด็กที่กฎหมายให้ความคุ้มครอง และปัญหาขอบเขตของกฎหมายในการกำหนดให้ภาพเสมือนจริงหรือการทำเทียมภาพลามกอนาจารเด็กโดยคอมพิวเตอร์ (Virtual Child Pornography) เป็นความผิดอาญา

ในกรณีของปัญหาเกี่ยวกับอายุของเด็กที่กฎหมายให้ความคุ้มครอง แม้ประเทศส่วนใหญ่จะมีการบัญญัติกฎหมายป้องกันและปราบปรามการเผยแพร่ภาพลามกอนาจารเด็ก แต่จากการศึกษาพบว่า กฎหมายของประเทศต่างๆกำหนดเงื่อนไขเกี่ยวกับอายุของเด็กที่ตกเป็นเหยื่อของการกระทำความผิดไว้แตกต่างกัน เงื่อนไขในเรื่องของอายุเด็กที่กฎหมายให้ความคุ้มครองนั้นจะมีผลถึงการกระทำความผิดของอาชญากรคอมพิวเตอร์ด้วย กล่าวคือ หากข้อเท็จจริงพบว่า บุคคลที่ปรากฏอยู่ในภาพลามกนั้นไม่ใช่เด็กตามความหมายของกฎหมายเกี่ยวกับภาพลามกอนาจารเด็กตามกฎหมายแล้ว ผู้เผยแพร่ภาพดังกล่าวก็ไม่มีความผิดเกี่ยวกับการเผยแพร่ภาพลามกอนาจารเด็ก และหากว่ากฎหมายของประเทศต่างๆกำหนดเงื่อนไขเรื่องอายุของเด็กที่แตกต่างกันแล้ว ก็จะ

---

[154] 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 : 336.

ส่งผลให้การกระทำความผิดหนึ่งๆเป็นความผิดอาญาในรัฐหนึ่งแต่อาจไม่เป็นความผิดอาญาในอีกรัฐหนึ่งได้ ผู้เขียนจะได้ยกตัวอย่างของกฎหมายเกี่ยวกับภาพลามกอนาจารเด็กในประเทศในกลุ่มยุโรปและสหรัฐอเมริกาเนื่องจากประเทศเหล่านี้ มีกฎหมายที่กำหนดการคุ้มครองภาพลามกอนาจารเด็กซึ่งครอบคลุมถึงการกระทำผ่านเครือข่ายอินเทอร์เน็ตที่ชัดเจน แต่ยังมีการกำหนดเงื่อนไขในเรื่องอายุที่แตกต่างกัน เช่น ในประเทศออสเตรียและเยอรมนี กำหนดอายุของเด็กที่กฎหมายคุ้มครองไว้ไม่เกิน 14 ปี ประเทศฝรั่งเศสและโปแลนด์ ไม่เกิน 15 ปี ประเทศเบลเยี่ยม, สวิตเซอร์แลนด์, เนเธอร์แลนด์, นอร์เวย์ และอังกฤษ ไม่เกิน 16 ปี และประเทศสหรัฐอเมริกา, แคนาดาและสวีเดน กำหนดอายุไม่เกิน 18 ปี[155] ซึ่งในกรณีที่เกิดการกระทำความผิดข้ามชาติ เช่น ในคดี Orchid Club หรือ กลุ่ม wOnderland ที่มีการส่งภาพลามกอนาจารเด็กเป็นเครือข่ายข้ามชาติ อายุของเด็กที่ตกเหยื่อย่อมต้องเป็นเงื่อนไขสำคัญที่อาจทำให้การกระทำของผู้กระทำความผิดไม่เป็นความผิดเกี่ยวกับการเผยแพร่ภาพลามกอนาจารเด็กในบางประเทศ ซึ่งส่งผลกระทบถึงการส่งผู้ร้ายข้ามแดน เนื่องจากไม่เป็นไปตามหลักความผิดอาญาของทั้งสองประเทศ

ปัญหาในประการที่สองที่ทำให้กฎหมายของแต่ละประเทศมีขอบเขตการบังคับใช้กฎหมายแตกต่างกันสืบเนื่องมาจากปัญหาทางกฎหมายเกี่ยวกับการกำหนดให้ภาพเสมือนจริงหรือภาพทำเทียมภาพลามกอนาจารเด็กโดยใช้คอมพิวเตอร์เป็นความผิดอาญา ดังที่ได้กล่าวมาแล้วว่า ภาพเสมือนจริงคือภาพที่ถูกสร้างขึ้นโดยคอมพิวเตอร์ ดังนั้น ภาพลามกอนาจารเด็กที่สร้างขึ้นโดยคอมพิวเตอร์จึงเป็นภาพที่ไม่มีการใช้เด็กจริงๆเข้ามาเป็นส่วนประกอบ ในทางระหว่างประเทศจึงยังคงเป็นที่ถกเถียงกันว่าการเผยแพร่ภาพเสมือนจริงนี้ จะถือเป็นการกระทำความผิดเกี่ยวกับการเผยแพร่ภาพลามกอนาจารด้วยหรือไม่ ซึ่งปัจจุบันนี้ยังไม่มีข้อสรุป ทำให้ในปัจจุบันกฎหมายของประเทศต่างๆยังลังเลที่จะบัญญัติให้ภาพเสมือนจริงหรือภาพเทียมภาพลามกอนาจารเด็กเป็นความผิดอาญา

อย่างไรก็ตาม ในประเทศพัฒนาแล้วเช่นประเทศสหรัฐอเมริกาและอังกฤษ มีกฎหมายภายในที่กำหนดสถานะของภาพเสมือนจริงหรือภาพทำเทียมภาพลามกอนาจารเด็กไว้โดยชัดแจ้ง โดยในประเทศอังกฤษมีกฎหมาย The Protection of Children Act 1978 แก้ไขเพิ่มเติมโดย The Criminal Justice and Public Order Act 1994 ให้คำจำกัดความของการทำ

---

[155] Ulrich Sieber, "Legal aspect of computer - related crime in the information society - COMCRIME - Study" Document prepared for the European Commission. Version 1.0 of 1st January 1998. pp. 91-92.

เทียมภาพว่า หมายถึงภาพที่ถูกทำขึ้นไม่ว่าจะโดยคอมพิวเตอร์ทางด้านภาพ (Computer-Graphics) หรืออุปกรณ์อื่นๆที่ทำให้ปรากฏออกมาเป็นภาพ ซึ่งหากการดัดแปลงหรือการทำเทียมภาพ ทำให้เกิดเป็นภาพลามกอนาจารเด็ก (Pseudo Child Photographs) การครอบครองรวมถึงการเผยแพร่ภาพดังกล่าว ถือการเผยแพร่ภาพลามกอนาจารอย่างหนึ่ง ซึ่งเป็นความผิดอาญาตามกฎหมายอังกฤษ[156]

ส่วนกฎหมายของประเทศสหรัฐอเมริกาบัญญัติอยู่ใน The Child Pornography Prevention Act 1996 หรือ CPPA กำหนดให้การผลิตภาพลามกอนาจารเด็กโดยใช้เทคโนโลยีคอมพิวเตอร์จัดทำให้เป็นภาพลามกอนาจารเด็ก หรือการซ้อนภาพเพื่อให้ดูเหมือนเป็นภาพเด็กซึ่งความจริงแล้วเป็นภาพผู้ใหญ่[157] เป็นความผิดอาญา ซึ่งนอกจากผู้ผลิตแล้ว การครอบครองและการเผยแพร่ภาพดังกล่าวก็เป็นความผิดอาญาตามกฎหมายนี้ด้วยเช่นกัน

เมื่อการกำหนดให้การครอบครองและเผยแพร่ภาพลามกอนาจารเด็กที่ผลิตจากเทคโนโลยีคอมพิวเตอร์เป็นความผิดเช่นเดียวกับกรณีของภาพลามกอนาจารโดยทั่วไปนั้นในปัจจุบันยังคงไม่เป็นที่แพร่หลาย จากการศึกษาพบว่าประเทศส่วนใหญ่ยังไม่มีการบัญญัติกฎหมายให้ครอบคลุมถึงภาพเสมือนจริงเหล่านี้ ทำให้มีเพียงประเทศส่วนน้อยที่มีกฎหมายเกี่ยวกับเรื่องนี้โดยเฉพาะ ซึ่งกรณีนี้ก็ยังคงเป็นปัญหาในการขอความร่วมมือในการส่งผู้ร้ายข้ามแดนอยู่ต่อไป

ข) <u>การเจาะระบบคอมพิวเตอร์และการกระทำความผิดฐานอื่นๆภายในระบบ</u>

ประเด็นความแตกต่างของขอบเขตการบังคับใช้กฎหมายของรัฐในความผิดฐานนี้ที่ก่อให้เกิดปัญหาในการส่งผู้ร้ายข้ามแดนสามารถแยกการวิเคราะห์ได้เป็นสองประเด็น กล่าวคือ ในประเด็นแรก เป็นปัญหาความแตกต่างของแนวคิดในการกำหนดให้การเจาะระบบคอมพิวเตอร์แต่เพียงอย่างเดียวโดยไม่มีการกระทำความผิดอย่างอื่นร่วมด้วยเป็นความผิดอาญาประการหนึ่ง ส่วนประเด็นที่สอง เป็นปัญหาเกี่ยวกับการจำกัดความรับผิดของผู้เจาะระบบคอมพิวเตอร์อันเนื่องมาจากสถานะของวัตถุที่กระทำต่อ

---

[156] Ian Lloyd, <u>Legal aspect of the information society</u>, p.117.

[157] ดู The Child Pornography Prevention Act 1996 Section 2256(8)(c)

ในประเด็นแรก คือ ปัญหาความแตกต่างของแนวคิดในการกำหนดให้การเจาะระบบคอมพิวเตอร์แต่เพียงอย่างเดียวโดยไม่มีการกระทำความผิดอย่างอื่นร่วมด้วยเป็นความผิดอาญา ซึ่งจากที่ได้ศึกษามาแล้วว่า กฎหมายภายในของบางประเทศ เช่น ประเทศเยอรมนี[158], ออสเตรีย, ญี่ปุ่น[159] และไต้หวัน[160] ไม่กำหนดให้การเจาะระบบคอมพิวเตอร์เพียงอย่างเดียวเป็นความผิดอาญา เว้นแต่มีการกระทำความผิดอย่างอื่นภายในระบบร่วมด้วย จึงจะเป็นการกระทำความผิดอาญา โดยจะกำหนดให้การเจาะระบบคอมพิวเตอร์เป็นส่วนหนึ่งของการกระทำความผิดฐานอื่นในระบบ ในขณะที่ประเทศอีกกลุ่มหนึ่ง เช่น ประเทศออสเตรเลีย[161] แคนาดา[162] เดนมาร์ก[163] ฟินแลนด์[164] ฝรั่งเศส[165] ลักเซมเบิร์ก[166] เนเธอร์แลนด์[167] นอร์เวย์[168] สเปน[169] สวีเดน[170] สวิตเซอร์แลนด์[171] อังกฤษ[172] และสหรัฐอเมริกา[173] กำหนดให้การเข้าสู่ระบบคอมพิวเตอร์ของผู้อื่น

---

[158] สุเนติ คงเทพ, "การไม่มีอำนาจเข้าสู่ระบบประมวลผล (Hacking)," บทบัณฑิตย์ 55: 125.

[159] John T. Soma , Thomas F. Muther and Heidi M.L. Brissette , "Transnational extradition for computer crimes : Are new treaties and laws need ? ," Harvard Journal on Legislation , 34 : 348.

[160] Tonya L. Putnam and David D. Elliott, Chapter 2 : International respond to cyber crime [Online],(n.d.), Available from : http://www.hoover.standford.edu/publications/books/fulltext/cybercrime/221.pdf. [2003,Jan 5]

[161] Australian Crimes Act 1914 Section 76 A-E

[162] Canada Criminal Code Article 342.1

[163] Danish Penal Code Section 263 (2), (3)

[164] Finnish Penal Code Chapter 38 Section 8

[165] France Criminal Code Article 462-2

[166] Luxembourg Penal Code Article 509-1

[167] Netherlands Criminal Code Article 138 a (1), (2)

[168] Norway Penal Code Section 145

[169] Spain Criminal Code Article 256

[170] Sweden Data Protection Act Section 21

[171] Swiss Criminal Code Article 143 bis

[172] UK Computer Misuse Act 1990 Section 1, 2

โดยมิชอบเป็นความผิดอาญาโดยไม่ต้องมีการกระทำความผิดฐานอื่นในระบบอีก ทำให้เพียงแค่การเข้าสู่ระบบที่มีการป้องกันก็เป็นความผิดอาญาแล้ว ความไม่สอดคล้องกันของกฎหมายในประเทศทั้งสองกลุ่มในประเด็นนี้ ทำให้เกิดปัญหาในการส่งผู้ร้ายข้ามแดนเนื่องจากความผิดดังกล่าวจะไม่เป็นความผิดอาญาตามแนวคิดของกลุ่มประเทศในกลุ่มแรก ซึ่งย่อมทำให้ประเทศในกลุ่มนี้ จะไม่ส่งผู้ร้ายข้ามแดนให้แก่ประเทศอื่น เนื่องจากการเจาะระบบคอมพิวเตอร์เพียงอย่างเดียวไม่ถือว่าเป็นการกระทำความผิดอาญาตามกฎหมายภายในของประเทศในกลุ่มนี้

ประเด็นที่สอง เป็นปัญหาเกี่ยวกับการจำกัดความรับผิดของผู้เจาะระบบคอมพิวเตอร์อันเนื่องมาจากสถานะของวัตถุที่กระทำต่อ กล่าวคือในกลุ่มประเทศที่มีการกำหนดให้การเจาะระบบคอมพิวเตอร์อย่างเดียวเป็นความผิดอาญาโดยเอกเทศ ไม่ว่าผู้กระทำจะได้มีการกระทำความผิดฐานอื่นร่วมด้วยหลังจากเข้าสู่ระบบแล้วหรือไม่นั้น ก็ยังมีความแตกต่างในขอบเขตของการบังคับใช้กฎหมาย กล่าวคือ กฎหมายภายในของบางประเทศ เช่น ประเทศออสเตรเลีย[174] จำกัดความรับผิดของผู้กระทำความผิดเฉพาะในกรณีเป็นการเจาะระบบขององค์กรหรือหน่วยงานของรัฐบาลกลางหรือมลรัฐเท่านั้น[175] ดังนั้น หากวัตถุที่ผู้กระทำความผิดกระทำต่อนั้นมีสถานะเป็นเพียงเครื่องคอมพิวเตอร์ของเอกชนแล้ว การกระทำดังกล่าวย่อมไม่เป็นความผิดอาญา ซึ่งกฎหมายของประเทศออสเตรเลียฉบับนี้มีความแตกต่างกับกฎหมายอาชญากรรมคอมพิวเตอร์ของหลายประเทศ เช่น แคนาดา[176] เดนมาร์ก[177] ฟินแลนด์[178] ฝรั่งเศส[179] ลักเซมเบิร์ก[180] เนเธอร์แลนด์[181]

---

[173] U.S.C. Title 18 Section 2510-2521, 2701-2710, 3117, 3121-3126 และU.S.C. Title 18 Section 1029 - 1030 (CFAA)

[174] The Australian Crimes Act 1914

[175] 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 : 348.

[176] Canada Criminal Code Article 342.1

[177] Danish Penal Code Section 263 (2), (3)

[178] Finnish Penal Code Chapter 38 Section 8

[179] France Criminal Code Article 462-2

[180] Luxembourg Penal Code Article 509-1

[181] Netherlands Criminal Code Article 138 a (1), (2)

นอร์เวย์[182] สเปน[183] สวีเดน[184] สวิตเซอร์แลนด์[185] อังกฤษ[186] และสหรัฐอเมริกา[187] ที่กำหนดให้การเจาะระบบเป็นความผิดอาญาไม่ว่าการระบบคอมพิวเตอร์ที่เป็นเป้าหมายในการกระทำความผิดนั้นจะเป็นของผู้ใด ดังนั้น หากการกระทำความผิดเป็นการกระทำต่อระบบคอมพิวเตอร์หรือระบบข้อมูลของเอกชนแล้ว การกระทำดังกล่าวจะไม่เป็นความผิดตามกฎหมายของประเทศออสเตรเลีย ทำให้ประเทศออสเตรเลียจะไม่สามารถส่งผู้ร้ายข้ามแดนในกรณีดังกล่าวได้ ยกตัวอย่างเช่น ในคดี Morris[188] ซึ่งสร้างโปรแกรม Worm ที่ทำลายคอมพิวเตอร์ทั่วโลก ซึ่งมีทั้งคอมพิวเตอร์ของภาครัฐและเอกชนจนทำให้เครื่องคอมพิวเตอร์เสียหายกว่า 6,200 เครื่อง ซึ่งในกรณีคดี Morris นี้ จะไม่ก่อให้เกิดปัญหาการส่งผู้ร้ายข้ามแดนเนื่องจากการกระทำดังกล่าว เป็นความผิดอาญาในทุกประเทศรวมทั้งประเทศออสเตรเลีย แต่หากข้อเท็จจริงเปลี่ยนเป็นว่าโปรแกรมชนิดนี้ได้ทำลายเครื่องคอมพิวเตอร์อื่นที่มิใช่ของรัฐบาลจนเกิดความเสียหาย กรณีนี้การกระทำของ Morris จะไม่เป็นความผิดตามกฎหมายของประเทศออสเตรเลีย เนื่องจากกฎหมายอาชญากรรมคอมพิวเตอร์ของประเทศออสเตรเลียจำกัดขอบเขตในการคุ้มครองเฉพาะระบบคอมพิวเตอร์ของรัฐบาลเท่านั้น ซึ่งทำให้ไม่สามารถส่งผู้ร้ายข้ามแดนในความผิดที่กระทำต่อเอกชนได้

ที่กล่าวมาทั้งหมดนี้แสดงให้เห็นว่า แม้ประเทศส่วนใหญ่จะบัญญัติให้การการเจาะระบบคอมพิวเตอร์และการกระทำความผิดในระบบเป็นความผิดอาญาตามกฎหมายภายใน แต่การขาดความเป็นอันหนึ่งอันเดียวกันของกฎหมายในเรื่องนี้ ทำให้กฎหมายของแต่ละประเทศมีขอบเขตในการบังคับใช้สำหรับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ลักษณะเดียวกันในระดับที่ต่างกัน ซึ่งทำให้เกิดปัญหาในการส่งผู้ร้ายข้ามแดน

---

[182] Norway Penal Code Section 145

[183] Spain Criminal Code Article 256

[184] Sweden Data Protection Act Section 21

[185] Swiss Criminal Code Article 143 bis

[186] UK Computer Misuse Act 1990 Section 1, 2

[187] U.S.C. Title 18 Section 2510 - 2521, 2701 - 2710, 3117, 3121 - 3126 และ U.S.C. Title 18 Section 1029 - 1030 (CFAA)

[188] 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 : 347.

ค) การกระทำที่กระทบต่อความมั่นคงของรัฐ

แม้การกระทำที่เป็นการกระทบต่อความมั่นคงของรัฐนั้น โดยทั่วไปทุกประเทศจะถือเป็นการกระทำที่เป็นความผิดอาญาอยู่แล้ว ไม่ว่าการกระทำนั้นจะเป็นการกระทำทางกายภาพหรือการกระทำผ่านเครือข่ายอินเทอร์เน็ต อย่างไรก็ตาม หลายประเทศก็ได้กำหนดให้การกระทำดังกล่าวที่กระทำผ่านเครือข่ายอินเทอร์เน็ตเป็นความผิดอาญาแล้ว แต่เนื่องจากแต่ละประเทศมีความเข้มงวดในการออกกฎเกณฑ์ในการป้องกันความมั่นคงของรัฐที่แตกต่างกัน ซึ่งทำให้กฎหมายเกี่ยวกับการควบคุมการกระทำที่อาจกระทบต่อความมั่นคงมีระดับความเข้มงวดแตกต่างกัน เช่น ในประเทศเกาหลีใต้ มีการลงโทษผู้ที่ทำการวิพากษ์วิจารณ์รัฐบาลเกาหลีใต้บนกระดานแสดงความคิดเห็น (Bulletin Board) โดยถูกจับกุมและดำเนินคดีภายใต้กฎหมายเกี่ยวกับความมั่นคงของชาติ ในขณะที่การวิพากษ์วิจารณ์รัฐบาลของประชาชนในประเทศอื่นๆ ไม่ถือเป็นการกระทำที่เป็นความผิดอาญา[189]

นอกจากขอบเขตของการกระทำอันเป็นความผิดของกฎหมายภายในที่แต่ละประเทศกำหนดไว้แตกต่างกันแล้ว โดยลักษณะของกฎหมายเกี่ยวกับความมั่นคงยังเป็นกฎหมายที่อาศัยดุลพินิจในการพิจารณาความผิดมากกว่าในความผิดฐานอื่นที่มีองค์ประกอบความผิดอาญาที่ชัดเจน กล่าวคือ กฎหมายเกี่ยวกับความมั่นคงส่วนใหญ่มักจะกำหนดขอบเขตกว้างๆ เช่น กฎหมายของประเทศเวียดนามและพม่าที่ห้ามผู้ใช้อินเทอร์เน็ตทำสำเนาหรือดาวน์โหลด (Down Load) ข้อมูลที่อาจกระทบต่อความมั่นคงของรัฐจากอินเทอร์เน็ต[190] ดังนั้น การใดที่อาจกระทบต่อความมั่นคงเป็นสิ่งที่รัฐเป็นผู้ใช้ดุลพินิจ และความเข้มงวดในการใช้ดุลพินิจก็มีความแตกต่างกันไปในแต่ละประเทศซึ่งขึ้นอยู่กับปัจจัยทางการเมืองประกอบอีกด้วย

ที่กล่าวมาทั้งหมดเป็นเหตุที่ทำให้การพิจารณาส่งผู้ร้ายข้ามแดนในความผิดฐานนี้กระทำได้ยาก อย่างไรก็ตาม ในการส่งผู้ร้ายข้ามแดนในความผิดเกี่ยวกับความมั่นคงของรัฐนั้นในทางปฏิบัติเกิดขึ้นน้อยมาก เนื่องจากการกระทำความผิดเกี่ยวกับความมั่นคงของรัฐอาจถูก

---

[189] 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 : 353.

[190] Ibid.

ตีความว่าเป็นความผิดทางการเมือง[191] ซึ่งตามหลักเกณฑ์ระหว่างประเทศเกี่ยวกับการส่งผู้ร้ายข้ามแดนถือว่าเป็นความผิดที่ต้องไม่ส่งผู้ร้ายข้ามแดนแก่กัน ซึ่งกรณีดังกล่าวจะได้กล่าวโดยละเอียดในเรื่องปัญหาการส่งผู้ร้ายข้ามแดนอันสืบเนื่องจากการตีความเรื่องความผิดทางการเมือง

<u>ง) การข่มขู่และคุกคามทางคอมพิวเตอร์</u>

การข่มขู่ผ่านเครือข่ายอินเทอร์เน็ตนั้น สามารถกระทำได้ในหลายรูปแบบดังที่ได้ศึกษามาแล้ว โดยอาจเป็นการข่มขู่ที่มีลักษณะการกระทำแบบเดิมเพียงแต่เปลี่ยนการใช้สื่อกลางมาเป็นการส่งจดหมายอิเล็กทรอนิกส์แทนการใช้โทรศัพท์หรือการใช้จดหมายธรรมดา ซึ่งวิธีนี้สามารถบังคับใช้กฎหมายอาญาดั้งเดิมเรื่องการข่มขู่ผ่านเครือข่ายอินเทอร์เน็ตได้โดยไม่ทำให้เกิดปัญหาทางกฎหมาย อย่างไรก็ตาม ในกรณีที่การข่มขู่ในลักษณะอื่นที่แตกต่างออกไปจากรูปแบบเดิมๆ เช่น กรณีการข่มขู่โดยการคุกคามเหยื่อขณะที่อยู่บนระบบเครือข่าย เช่น ในห้องสนทนาหรือตามเว็บไซต์ต่างๆเป็นประจำ หรือการสร้างข้อมูลเท็จที่สร้างความเสื่อมเสียแก่ชื่อเสียงของเหยื่อและเผยแพร่ทางอินเทอร์เน็ต รวมถึงการส่งไวรัสคอมพิวเตอร์ให้แก่เหยื่อเพื่อจงใจสร้างความเสียหายในลักษณะคุกคาม[192] การกระทำเหล่านี้ไม่สามารถกระทำได้ถ้าไม่ได้ใช้คอมพิวเตอร์และระบบเครือข่ายเป็นเครื่องมือ ดังนั้น กฎหมายที่เข้ามาควบคุมจึงต้องปรับใช้กับการกระทำผ่านเครือข่ายอินเทอร์เน็ตได้ด้วย ซึ่งกฎหมายที่กำหนดมาเพื่อใช้กับการข่มขู่ผ่านเครือข่ายอินเทอร์เน็ตโดยเฉพาะนั้น ย่อมทำให้การบังคับใช้กฎหมายไม่เกิดช่องว่างในการบังคับใช้มาก แต่การปรับใช้กฎหมายดั้งเดิมกับการกระทำผ่านอินเทอร์เน็ตอาจมีความไม่ครอบคลุมในบางประเด็น ซึ่งทำให้ขอบเขตของกฎหมายในการปรับกับปัญหาที่เกิดขึ้นมีความแตกต่างกัน ซึ่งจะมีผลถึงการไม่สามารถส่งผู้ร้ายข้ามแดนได้

ผู้เขียนจะได้ยกตัวอย่างประเทศอังกฤษซึ่งนำกฎหมายเรื่องการข่มขู่ทั่วไปมาใช้กับการข่มขู่ทางอินเทอร์เน็ต กล่าวคือ แม้กฎหมายของประเทศอังกฤษ[193]จะสามารถปรับใช้กับการกระทำผ่านอินเทอร์เน็ตได้ แต่ก็เกิดปัญหาในทางปฏิบัติเนื่องจากกฎหมายทั่วไปไม่สามารถครอบคลุมถึงในกรณีที่ผู้กระทำความผิดกระทำความผิดจากนอกราชอาณาจักรอังกฤษ การกระทำดังกล่าวไม่

---

[191] Ibid.

[192] Emma Ogilvie, <u>Cyberstalking</u>[Online],2000, Available from: <u>http://www.aic.gov.au/publications/tandi/ti166.pdf</u> [2002, June 14]

[193] The Protection from Harassment Act 1997

เป็นความผิดตามกฎหมายอังกฤษ ซึ่งขัดกับลักษณะของเครือข่ายอินเทอร์เน็ตซึ่งโยงใยไปทั่วโลก ดังนั้น การกระทำความผิดย่อมไม่จำกัดอยู่แต่เพียงในประเทศ หากการกระทำความผิดจากภายนอกประเทศไม่เป็นความผิดอาญาตามกฎหมายอังกฤษแล้ว ย่อมส่งผลทำให้การส่งผู้ร้ายข้ามแดนไม่สามารถดำเนินไปได้[194]

กรณีความไม่เพียงพอของการบังคับใช้กฎหมายทั่วไปกับการกระทำผ่านอินเทอร์เน็ต สามารถเกิดขึ้นได้กับประเทศไทยเช่นเดียวกัน โดยเมื่อพิจารณาประมวลกฎหมายอาญาของไทย มาตรา 392[195] ซึ่งเป็นบทบัญญัติที่กำหนดให้การข่มขู่ผู้อื่นเป็นความผิดอาญา โดยบทบัญญัติดังกล่าวเป็นบทบัญญัติทั่วไปไม่ใช่กฎหมายเฉพาะที่ใช้กับการกระทำความผิดผ่านเครือข่ายอินเทอร์เน็ต ทำให้มีข้อน่าพิจารณาว่า จะสามารถใช้บังคับกับการกระทำความผิดผ่านสื่ออินเทอร์เน็ตได้เพียงใด

ในกรณีที่การข่มขู่ผ่านอินเทอร์เน็ตใช้รูปแบบการกระทำเดิมคือการส่งข้อความหรือรูปภาพขู่เข็ญผู้อื่นเพื่อให้ผู้อื่นตกใจกลัว โดยใช้คอมพิวเตอร์เป็นเพียงสื่อกลางของการกระทำน่าจะถือได้ว่าเป็นการกระทำความผิดตามมาตรานี้ เนื่องจากข้อความตามมาตรา 392 ใช้ถ้อยคำอย่างกว้าง ดังนั้น ไม่ว่าจะเป็นการขู่เข็ญโดยการใช้ข้อความหรือรูปภาพผ่านเครือข่ายอินเทอร์เน็ต ก็น่าที่จะปรับใช้บทบัญญัติมาตรา 392 กับการกระทำดังกล่าวได้ หากการกระทำนั้น กระทำลงเพื่อให้ผู้อื่นเกิดความกลัวหรือตกใจ ทั้งนี้เป็นไปตามองค์ประกอบความผิดตามมาตรา 392 อย่างไรก็ตาม ในปัจจุบันก็ยังไม่มีคดีความในลักษณะนี้ขึ้นสู่การพิจารณาของศาลไทย

อย่างไรก็ตาม ดังที่ได้กล่าวมาแล้วว่า การข่มขู่ผ่านเครือข่ายอินเทอร์เน็ต มีการพัฒนารูปแบบการข่มขู่แบบใหม่ ซึ่งหากไม่มีคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตแล้ว การข่มขู่ในลักษณะนี้จะไม่สามารถเกิดขึ้นได้ กล่าวคือ การข่มขู่ผ่านอินเทอร์เน็ตที่เป็นการกระทำในลักษณะอื่นที่นอกเหนือจากที่กล่าวมาข้างต้น โดยเฉพาะอย่างยิ่งเป็นการกระทำที่ใช้คอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตเป็นเครื่องมือในการกระทำโดยตรง เช่น การส่งไวรัสเพื่อข่มขู่หรือคุกคาม

---

[194] Louise Ellison and Yaman Akdeniz, "Cyber-Stalking: The regulation of harassment on the internet," Criminal Law Review [1998], December Special Edition: Crime, Criminal Justice and the Internet : 29-48.

[195] มาตรา 392 "ผู้ใดทำให้ผู้อื่นเกิดความกลัว หรือความตกใจ โดยการขู่เข็ญ ต้องระวางโทษจำคุกไม่เกิน 1 เดือน ปรับไม่เกิน 1,000 บาท หรือทั้งจำทั้งปรับ"

หรือการคุกคามผู้อื่นขณะอยู่บนเครือข่ายอินเทอร์เน็ตไม่ว่าจะด้วยวิธีการอย่างไร ก็คงจะเกิดปัญหาว่า บทบัญญัติดังกล่าวจะสามารถครอบคลุมถึงการกระทำความผิดได้หรือไม่ เพียงใด ซึ่งโดยความเห็นของผู้เขียนเห็นว่า ไม่สามารถปรับใช้มาตรา 392 กับการกระทำดังกล่าวได้ เนื่องจากการกระทำความผิดตามมาตรานี้ต้องเป็นการกระทำในลักษณะขู่เข็ญ การกระทำอย่างอื่นแม้จะทำให้ผู้อื่นเกิดความตกใจกลัวก็ไม่เป็นความผิดตามมาตรานี้ นอกจากนี้ การจะตีความให้มาตรา 392 ครอบคลุมถึงการข่มขู่แบบใหม่ด้วยนั้น จะเป็นการตีความกฎหมายที่กว้างเกินถ้อยคำของตัวบทมากเกินไป ซึ่งเป็นการนอกเหนือจากวัตถุประสงค์ของกฎหมาย และขัดต่อหลักกฎหมายอาญาต้องตีความโดยเคร่งครัด

กฎหมายภายในที่ได้ยกตัวอย่างมาข้างต้นนั้น แสดงให้เห็นถึงสภาพปัญหาความแตกต่างของกฎหมายภายในของแต่ละประเทศในประเด็นที่แตกต่างกัน หากแต่มีความคล้ายคลึงกันตรงที่ความไม่เพียงพอของกฎหมายที่จะใช้บังคับกับอาชญากรรมคอมพิวเตอร์ ซึ่งมีผลทำให้ขอบเขตการบังคับใช้กฎหมายมีความแตกต่างกัน ซึ่งล้วนมีผลให้การส่งผู้ร้ายข้ามแดนในความผิดดังกล่าวเกิดความไม่สะดวก หรือไม่สามารถส่งผู้ร้ายข้ามแดนกันได้

จ) การฉ้อโกงทางคอมพิวเตอร์

จากที่ได้กล่าวมาแล้วว่า ความผิดเกี่ยวกับการฉ้อโกงถือเป็นการกระทำความผิดที่ทุกประเทศกำหนดให้เป็นความผิดอาญาอยู่แล้ว หากแต่ความแตกต่างของวิธีการและรูปแบบของการกระทำความผิดทำให้กฎหมายของหลายประเทศไม่สามารถปรับใช้กับการฉ้อโกงผ่านทางอินเทอร์เน็ตได้ ทำให้หลายประเทศได้มีการแก้ไขกฎหมายให้ใช้บังคับกับการกระทำความผิดผ่านเครือข่ายอินเทอร์เน็ตได้โดยเฉพาะ ซึ่งการแก้ไขกฎหมายให้ใช้กับการกระทำผ่านเครือข่ายอินเทอร์เน็ตได้โดยเฉพาะนี้ทำให้ความแตกต่างของกฎหมายในเรื่องนี้ลดลง เนื่องจากกฎหมายที่ได้รับการแก้ไขจะทำให้ปัญหาการตีความกฎหมายให้ครอบคลุมถึงการฉ้อโกงทางอินเทอร์เน็ตหมดไป ดังนั้น หากมีการส่งผู้ร้ายข้ามแดนกันระหว่างประเทศที่ได้มีการแก้ไขกฎหมายแล้ว ทำให้ไม่เกิดข้อขัดข้องในการส่งผู้ร้ายข้ามแดน

อย่างไรก็ตาม ในบางประเทศก็ไม่มีการบัญญัติกฎหมายเฉพาะเกี่ยวกับการฉ้อโกงทางอินเทอร์เน็ตขึ้นบังคับใช้ เช่น ประเทศอังกฤษ[196]และประเทศแคนาดา[197] เป็นต้น โดยทั้งสอง

---

[196] Theft (Amendment) Act 1996

ประเทศปรับใช้กฎหมาย Theft ซึ่งเป็นกฎหมายดั้งเดิมกับการฉ้อโกงทางอินเทอร์เน็ต เนื่องด้วยกฎหมายเรื่อง Theft ของ Common Law นั้น คำว่า Theft มีความหมายและกินความกว้างมาก ซึ่งเป็นเหตุผลที่ทำให้ศาล Common Law สามารถวางหลักกฎหมายปรับใช้กับกระทำผ่านเครือข่ายอินเทอร์เน็ตได้[198] โดยการกระทำการโอนเงินผ่านเครือข่ายอินเทอร์เน็ตเพื่อให้ไปเข้าบัญชีของผู้กระทำความผิดโดยมิชอบ ถือว่าเป็นการกระทำความผิดอาญาตามกฎหมายเรื่อง Theft[199] ซึ่งตัวการปรับใช้กฎหมายของประเทศอังกฤษเพื่อส่งผู้ร้ายข้ามแดนให้แก่ประเทศสหรัฐอเมริกาได้เกิดขึ้นในคดี Re Vladimir Levin (1997) แฮกเกอร์ชาวรัสเซีย ซึ่งฉ้อโกงเงินทางคอมพิวเตอร์โดยใช้เครื่องคอมพิวเตอร์จากลอนดอนเจาะระบบเข้าสู่ฐานข้อมูลของธนาคารซิตี้แบงก์ของสหรัฐอเมริกาและโอนเงินออนไลน์เข้าบัญชีของเขาในประเทศสหรัฐอเมริกา ฟินแลนด์ เนเธอร์แลนด์ เยอรมนี และอิสราเอล Levin ถูกจับกุมที่กรุงลอนดอน ประเทศอังกฤษ โดยศาลอังกฤษพิจารณาให้ส่งตัวข้ามแดนมาดำเนินคดีที่ประเทศสหรัฐอเมริกา โดยปรับใช้กฎหมายในเรื่อง Theft และ Computer Misuse Act 1990[200]

นอกจากการปรับใช้กฎหมายในเรื่อง Theft แล้ว ศาลอังกฤษเคยพิจารณาคดีส่งผู้ร้ายข้ามแดนในการฉ้อโกงเงินทางอินเทอร์เน็ตแก่ประเทศสหรัฐอเมริกา ในคดี Re Allison (1999) ซึ่งมีข้อเท็จจริงในคดีว่า Allison ซึ่งเป็นพนักงานของบริษัท อเมริกัน เอ็กซ์เพรส กระทำการเข้าสู่ระบบฐานข้อมูลบริษัทโดยใช้รหัสพนักงานและขโมยรหัสผ่านบัตรเครดิตของลูกค้า เพื่อนำรหัสบัตร

---

[197] Canada department of Justice, Conference on cybercrime, In Canada National Report[Online],2001, Nov 19, Available from: http://www.legal.coe.int/economiccrime/cybercrime/ConfCY(2001)Nat14Canada.pdf [2002,June 16]

[198] สุเนติ คงเทพ, "การไม่มีอำนาจเข้าสู่ระบบประมวลผล (Hacking)," บทบัณฑิตย์ 55 : 147.

[199] 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 : 353.

[200] House of Loads, Judgements – In Re Levin[Online],1997, June 19, Available from : http://www.hrothgar.co.uk/webcases/hol/reports/02/27.htm [2003,Sep 26]

เครดิตมาใช้[201] ในคดีนี้ ศาลอังกฤษไม่ได้ปรับใช้กฎหมายเรื่อง Theft แต่ปรับใช้ The Computer Misuse Act 1990 ซึ่งบัญญัติให้การเข้าถึงระบบข้อมูลหรือการแก้ไขเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาตเป็นความผิดอาญา นักกฎหมายอังกฤษมีความเห็นว่า กฎหมายฉบับดังกล่าวไม่ได้กำหนดให้ใช้กับการฉ้อโกงทางคอมพิวเตอร์โดยตรง ทำให้การส่งผู้ร้ายข้ามแดนในกรณีของ Allison อาศัยความผิดเกี่ยวกับการแก้ไขเปลี่ยนแปลงข้อมูลคอมพิวเตอร์โดยมิได้รับอนุญาต มิใช่การฉ้อโกงทางคอมพิวเตอร์[202]

การไม่มีกฎหมายเฉพาะของประเทศอังกฤษ ทำให้ในคดีดังกล่าวเกิดปัญหาในการตีความกฎหมายของศาล ซึ่งทำให้เกิดความไม่สะดวกในการให้ความร่วมมือ แต่ไม่ถึงกับทำให้เป็นอุปสรรคในการส่งผู้ร้ายข้ามแดน เนื่องจากแม้กฎหมายดังกล่าวจะสามารถปรับใช้ให้เข้ากับการกระทำผ่านเครือข่ายอินเทอร์เน็ตได้ก็ตาม แต่ศาลก็ต้องอาศัยการตีความอย่างกว้างเพื่อให้มีความครอบคลุมและเหมาะสมกับการกระทำความผิดที่มีการร้องขอให้ส่งผู้ร้ายข้ามแดน ซึ่งก่อความยุ่งยากในการบังคับใช้กฎหมาย อย่างไรก็ตาม มิใช่ทุกประเทศจะสามารถปรับใช้กฎหมายให้ครอบคลุมถึงกรณีดังกล่าวได้เสมอไป กฎหมายของประเทศในกลุ่ม Civil Law บางประเทศดังเช่นประเทศไทยไม่สามารถปรับใช้กฎหมายฉ้อโกงทั่วไปกับการฉ้อโกงทางอินเทอร์เน็ตได้เนื่องเป็นการแปลความที่ขัดต่อหลักกฎหมาย ดังนั้น หากไม่มีการบัญญัติกฎหมายเฉพาะขึ้นบังคับใช้แล้ว ย่อมก่อให้เกิดปัญหาไม่สามารถส่งผู้ร้ายข้ามแดน เนื่องจากไม่สามารถปรับใช้กฎหมายดั้งเดิมที่มีอยู่กับการฉ้อโกงทางอินเทอร์เน็ตได้ เท่ากับการกระทำดังกล่าวไม่เป็นความผิดตามกฎหมายของ

---

[201] ในคดีเช่นเดียวกันนี้ หากเกิดขึ้นในประเทศไทย มักมีการตั้งข้อหาในชั้นสอบสวนไปตามประมวลกฎหมายอาญาที่มีอยู่ เช่น ลักทรัพย์ หรือฉ้อโกงเป็นต้น อย่างไรก็ตาม ยังคงมีปัญหาในการที่ศาลจะปรับใช้ประมวลกฎหมายอาญากับคดีในลักษณะนี้เนื่องจากความไม่เพียงพอของประมวลกฎหมายอาญาของไทย การปรับบทกฎหมายในความผิดฐานลักทรัพย์และฉ้อโกง ยังคงเป็นปัญหาทางกฎหมายว่า จะสามารถกระทำได้เพียงใด เนื่องจากยังเกิดประเด็นปัญหาว่าข้อมูลคอมพิวเตอร์ไม่ถือเป็นทรัพย์ที่ได้รับความคุ้มครองตามประมวลกฎหมายอาญาจึงไม่อาจเป็นความผิดฐานลักทรัพย์ได้ นอกจากนี้ การกระทำความผิดฐานฉ้อโกงตามประมวลกฎหมายอาญาต้องเป็นการกระทำระหว่างบุคคลกับบุคคล ไม่รวมถึงการกระทำการฉ้อโกงต่อเครื่องคอมพิวเตอร์ ซึ่งทั้งหมดนี้ ทำให้ในปัจจุบัน ศาลไทยอาจประสบปัญหาการไม่สามารถใช้ประมวลกฎหมายอาญาเพื่อลงโทษแก่จำเลยในการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้

[202] Ian Lloyd, Legal aspect of the information society, pp. 107-108.

ประเทศไทย ทำให้ไม่สามารถส่งผู้ร้ายข้ามแดนได้เพราะไม่เป็นไปตามหลักเกณฑ์เกี่ยวกับความผิดอาญาของทั้งสองประเทศ

ที่กล่าวมาทั้งหมดนี้เป็นปัญหาการส่งผู้ร้ายข้ามแดนอันเนื่องมาจากความไม่สอดคล้องกันของกฎหมายอาชญากรรมคอมพิวเตอร์ในแต่ละประเทศ ซึ่งทำให้ขัดต่อหลักความผิดอาญาของทั้งสองประเทศ และเป็นสาเหตุสำคัญที่ทำให้กระบวนการส่งผู้ร้ายข้ามแดนของรัฐไม่อาจดำเนินไปได้ อย่างไรก็ตาม ปัญหาและอุปสรรคในการส่งผู้ร้ายข้ามแดนในคดีอาชญากรรมคอมพิวเตอร์ยังคงมีปัญหาที่เกิดขึ้นอีกหลายประการ ซึ่งจะได้กล่าวต่อไป

3.2.2 ปัญหาที่สืบเนื่องจากหลักความผิดที่สามารถส่งผู้ร้ายข้ามแดนได้

ปัญหาประการต่อมาในการส่งผู้ร้ายข้ามแดนในคดีอาชญากรรมคอมพิวเตอร์สืบเนื่องจากการที่ในปัจจุบัน สนธิสัญญาส่งผู้ร้ายข้ามแดนที่ประเทศต่างๆใช้อยู่นั้น มีอยู่ 2 ประเภท คือ สนธิสัญญาที่ระบุประเภทหรือรายชื่อความผิดโดยเฉพาะเจาะจง กับสนธิสัญญาประเภทระบุอัตราโทษขั้นต่ำ ซึ่งทั้งสองกรณีสร้างปัญหาในการให้ความร่วมมือในการส่งผู้ร้ายข้ามแดนในความผิดอาญาฐานใหม่ๆเช่นอาชญากรรมคอมพิวเตอร์ ซึ่งจะได้กล่าวในรายละเอียดดังต่อไปนี้

3.2.2.1 กรณีที่สนธิสัญญากำหนดฐานความผิดโดยเฉพาะเจาะจง

สนธิสัญญากำหนดฐานความผิดโดยเฉพาะเจาะจงซึ่งเป็นสนธิสัญญารูปแบบเก่า ซึ่งโดยส่วนใหญ่แล้วจะยังไม่มีการแก้ไขฐานความผิดให้รวมถึงความผิดอาชญากรรมคอมพิวเตอร์ ในกรณีดังกล่าวจึงก่อให้เกิดปัญหาการไม่สามารถส่งผู้ร้ายข้ามแดนได้ กรณีเช่นว่านี้เคยเกิดเป็นปัญหาการส่งผู้ร้ายข้ามแดน ในคดีการส่งผู้ร้ายข้ามแดนระหว่างประเทศอาร์เจนติน่ากับประเทศสหรัฐอเมริกา ในปี ค.ศ.1995 เมื่อนาย Julio Cesar Ardita แฮกเกอร์ชาวอาร์เจนติน่า ถูกทางการสหรัฐกล่าวหาว่า ได้กระทำความผิดกฎหมายสหรัฐฯโดยการเข้าสู่ระบบคอมพิวเตอร์ของหน่วยงานสหรัฐฯโดยมิได้รับอนุญาต นาย Ardita ได้เจาะระบบคอมพิวเตอร์ของสำนักงานวิจัยทางทหารของสหรัฐฯ, องค์การ NASA รวมถึงหน่วยงานของรัฐบาลกว่า 62 แห่ง สถาบันการศึกษา 136 แห่ง และองค์กรภาคเอกชน 31 แห่ง ในคดีนี้ รัฐบาลสหรัฐฯประสบปัญหาการไม่สามารถร้องขอให้รัฐบาลอาร์เจนติน่าส่งตัวนาย Ardita ข้ามแดนมาดำเนินคดีในสหรัฐฯได้ เนื่องจากความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์ไม่เป็นความผิดที่สามารถส่งข้ามแดนได้ตามสนธิสัญญาส่ง

ผู้ร้ายข้ามแดนระหว่างประเทศสหรัฐฯกับประเทศอาร์เจนติน่า อย่างไรก็ตาม ในคดีนี้นาย Ardita ได้สละสิทธิในข้อต่อสู้ดังกล่าว และได้เข้ารับการพิจารณาคดีในประเทศสหรัฐอเมริกาโดยสมัครใจ[203]

คดีที่เกิดระหว่างประเทศอาร์เจนติน่ากับสหรัฐอเมริกานั้น เป็นตัวอย่างที่แสดงให้เห็นถึงข้อขัดข้องในการส่งผู้ร้ายข้ามแดนที่สืบเนื่องมาจากสนธิสัญญาระบุฐานความผิดโดยเฉพาะเจาะจงของประเทศอาร์เจนติน่าและสหรัฐอเมริกาที่ยังไม่มีการเพิ่มเติมความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์เป็นความผิดที่สามารถส่งผู้ร้ายข้ามแดนได้ แม้ผลที่สุดประเทศสหรัฐอเมริกาจะได้ตัวผู้ต้องหาไปดำเนินคดีในประเทศสหรัฐอเมริกา แต่การได้ตัวผู้ต้องหาเป็นกรณีที่ผู้ต้องหาสมัครใจและยินยอมเข้าสู่การดำเนินคดีเอง จึงถือเป็นวิธีการอื่นซึ่งมิใช่เป็นไปด้วยกระบวนการส่งผู้ร้ายข้ามแดนโดยปกติ

สนธิสัญญาส่งผู้ร้ายข้ามแดนของประเทศส่วนใหญ่ในปัจจุบัน ยังไม่มีการแก้ไขสนธิสัญญาให้ครอบคลุมถึงอาชญากรรมคอมพิวเตอร์ซึ่งเป็นความผิดฐานใหม่ ซึ่งอาจสร้างปัญหาดังเช่นในกรณีประเทศสหรัฐอเมริกาและประเทศอาร์เจนติน่าได้อีก ดังเช่นในกรณีของประเทศไทย สนธิสัญญาประเภทเดียวกันนี้ยังคงมีใช้บังคับอยู่กับประเทศอังกฤษ[204] เบลเยี่ยม[205] อินโดนีเซีย[206] และฟิลิปปินส์[207] และยังไม่มีการแก้ไขสนธิสัญญาให้ครอบคลุมถึงความผิดฐานใหม่เช่น อาชญากรรมคอมพิวเตอร์ ดังนั้น แม้ต่อไปในอนาคตประเทศไทยจะได้ตรากฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์ขึ้นใช้บังคับ แต่ก็จะไม่สามารถส่งผู้ร้ายข้ามแดนได้เนื่องจากความขัดข้องในสนธิสัญญาส่งผู้ร้ายข้ามแดนที่ยังมิได้รับการแก้ไข

---

[203] Argentina hacker pleads guilty[Online], 1997, Available from : http://www.wired.com/news/technology/0,1282,8996,00.html [2003, April 28]

[204] สนธิสัญญาส่งผู้ร้ายข้ามแดนระหว่างกรุงสยามกับอังกฤษ ร.ศ.130

[205] อนุสัญญาว่าด้วยการส่งผู้ร้ายข้ามแดนระหว่างสยามและเบลเยี่ยม พ.ศ.2479

[206] สนธิสัญญาส่งผู้ร้ายข้ามแดนระหว่างราชอาณาจักรไทยกับสาธารณรัฐอินโดนีเซีย พ.ศ.2522

[207] สนธิสัญญาส่งผู้ร้ายข้ามแดนระหว่างราชอาณาจักรไทยกับสาธารณรัฐฟิลิปปินส์ พ.ศ. 2527

3.2.2.2 กรณีสนธิสัญญากำหนดอัตราโทษขั้นต่ำ

ปัญหาอันเกิดจากสนธิสัญญาระบุความผิดที่ส่งผู้ร้ายข้ามแดนประเภทนี้ เนื่องจากสนธิสัญญาประเภทนี้ส่วนใหญ่กำหนดอัตราโทษไว้ที่การลงโทษโดยการจำคุกไม่ต่ำกว่า 1 ปี หรือการลงโทษอื่นที่หนักกว่า มีผลทำให้ความผิดที่มีโทษต่ำกว่า 1 ปี ไม่อยู่ในขอบเขตที่จะส่งผู้ร้ายข้ามแดนได้[208] ซึ่งเมื่อพิจารณากฎหมายอาชญากรรมคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตของประเทศต่างๆแล้วพบว่า การกำหนดอัตราโทษสำหรับความผิดเกี่ยวกับคอมพิวเตอร์บางฐานที่อัตราโทษที่แตกต่างกันอย่างมาก เช่น ในความผิดเกี่ยวกับการเข้าสู่ระบบคอมพิวเตอร์โดยปราศจากอำนาจ (Unauthorized Access)นั้น ในบางประเทศกำหนดโทษสำหรับความผิดฐานนี้ในอัตราต่ำ เนื่องจากถือว่าไม่ใช่ความผิดที่ก่อความเสียหายร้ายแรง กรณีดังกล่าวแม้ถือว่าการเจาะระบบคอมพิวเตอร์เป็นความผิดอาญาตามกฎหมายของรัฐภาคีตามหลัก Double Criminality แต่ไม่อยู่ในหลักเกณฑ์ที่จะส่งผู้ร้ายข้ามแดนกันได้ หากประเทศใดประเทศหนึ่งกำหนดอัตราโทษต่ำกว่า 1 ปี

ตัวอย่างของกฎหมายอาชญากรรมคอมพิวเตอร์ที่กำหนดอัตราโทษสำหรับผู้กระทำความผิดต่ำกว่า 1 ปี เช่น The Australian Crime Act 1914 Part VIA Section 76 A-E ของประเทศออสเตรเลียกำหนดให้การเข้าสู่ระบบคอมพิวเตอร์โดยมิได้รับอนุญาตเป็นความผิดอาญา กฎหมายฉบับนี้จำกัดขอบเขตของความผิดอาญาไว้เฉพาะแต่การเข้าสู่ระบบคอมพิวเตอร์และระบบข้อมูลของรัฐบาลกลาง การเจาะระบบคอมพิวเตอร์เพียงอย่างเดียว โดยมิได้กระทำความผิดฐานอื่นๆภายในระบบ เป็นความผิดที่ต้องระวางโทษจำคุกไม่เกิน 6 เดือน เช่นเดียวกับประมวลกฎหมายอาญาของประเทศเนเธอร์แลนด์ โดย Article 138a(1)(2) กำหนดให้การเข้าสู่ระบบคอมพิวเตอร์ของผู้อื่นโดยมิชอบเป็นความผิดที่มีโทษจำคุกไม่เกิน 6 เดือน ในขณะที่กฎหมายของประเทศสหรัฐอเมริกาคือ The Computer Fraud and Abuse Act (CFAA) Section 1030 กำหนดให้การกระทำความผิดในลักษณะเดียวกันนี้เป็นความผิดอาญาที่มีโทษปรับและจำคุกไม่เกิน 20 ปี[209] ในกรณีดังกล่าวนี้ แม้ว่าทั้งประเทศสหรัฐอเมริกา ออสเตรเลียและเนเธอร์แลนด์ต่างมีกฎหมายภายในที่กำหนดให้การเข้าสู่ระบบคอมพิวเตอร์โดยมิชอบเป็นความผิดอาญา ตามหลัก

---

[208] The UN Model Treaty on Extradition 1990

[209] 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 : 348-349.

ความผิดอาญาของทั้งสองประเทศ แต่การกำหนดระวางโทษที่ต่ำกว่า 1 ปี ซึ่งหากต้องมีการพิจารณาคดีเพื่อการส่งผู้ร้ายข้ามแดนแล้ว อาจก่อให้เกิดปัญหา เนื่องจากสนธิสัญญาส่งผู้ร้ายข้ามแดนของประเทศสหรัฐอเมริกากับประเทศต่างๆทุกฉบับกำหนดความผิดที่ส่งผู้ร้ายข้ามแดนได้เป็นความผิดที่มีอัตราโทษจำคุกอย่างน้อย 1 ปีทั้งสิ้น การกำหนดโทษที่ต่ำเกินกว่าที่จะส่งผู้ร้ายข้ามแดนได้ จึงทำให้เกิดช่องว่างทางกฎหมายเนื่องจากความผิดนั้นไม่อยู่ภายใต้บังคับของหลักเกณฑ์ว่าด้วยการส่งผู้ร้ายข้ามแดน ทำให้รัฐที่ได้รับความเสียหายไม่สามารถนำตัวผู้กระทำความผิดมาลงโทษ ทั้งรัฐที่มีตัวผู้กระทำความผิดอยู่ในฐานะที่ไม่สามารถลงโทษผู้กระทำความผิดให้สมกับความเสียหายที่เกิดขึ้นได้อีกด้วย

จากตัวอย่างที่ได้ยกขึ้นกล่าวข้างต้นนั้น จะเห็นได้ว่า ยังมีหลายประเทศที่ยังกำหนดอัตราโทษที่จะลงแก่ผู้กระทำความผิดไว้ต่ำมาก ซึ่งย่อมมีผลโดยตรงต่อการให้ความร่วมมือในการส่งผู้ร้ายข้ามแดน ในส่วนของประเทศไทยนั้น ก็พบว่าสนธิสัญญาส่งผู้ร้ายข้ามแดนของไทยที่เป็นสนธิสัญญาประเภทระบุอัตราโทษขั้นต่ำกับประเทศต่างๆที่มีอยู่ในปัจจุบัน ได้กำหนดความผิดที่ส่งข้ามแดนได้เป็นความผิดที่อัตราโทษจำคุกอย่างน้อย 1 ปีหรือโทษอื่นที่หนักกว่าทั้งสิ้น[210] ดังนั้น หากประเทศไทยจะบัญญัติกฎหมายอาชญากรรมคอมพิวเตอร์ขึ้นบังคับใช้ ก็จำต้องกำหนดอัตราโทษที่จะลงแก่ผู้กระทำความผิดเป็นโทษจำคุกสูงกว่า 1 ปี หรือโทษอื่นที่หนักกว่า ซึ่งจะทำให้เป็นไปตามหลักเกณฑ์ของสนธิสัญญาและไม่ก่อปัญหาในการส่งผู้ร้ายข้ามแดน

---

[210] ดูสนธิสัญญาส่งผู้ร้ายข้ามแดนระหว่างราชอาณาจักรไทยกับสหรัฐอเมริกา พ.ศ.2533 ข้อ 2

สนธิสัญญาส่งผู้ร้ายข้ามแดนระหว่างราชอาณาจักรไทยกับสาธารณะรัฐประชาชนจีน พ.ศ. 2541 ข้อ 2

สนธิสัญญาส่งผู้ร้ายข้ามแดนระหว่างราชอาณาจักรไทยกับราชอาณาจักรกัมพูชา พ.ศ. 2543 ข้อ 1

สนธิสัญญาส่งผู้ร้ายข้ามแดนระหว่างราชอาณาจักรไทยกับสาธารณะรัฐประชาธิปไตยประชาชนลาว พ.ศ. 2543 ข้อ 2

สนธิสัญญาส่งผู้ร้ายข้ามแดนระหว่างราชอาณาจักรไทยกับสาธารณรัฐเกาหลี พ.ศ. 2543 ข้อ 2

สนธิสัญญาส่งผู้ร้ายข้ามแดนระหว่างราชอาณาจักรไทยกับสาธารณรัฐประชาชนบังคลาเทศ พ.ศ. 2543 ข้อ 2

อย่างไรก็ตาม แม้ประเด็นในเรื่องอัตราโทษที่จะลงแก่ผู้กระทำความผิดจะเป็นปัจจัยสำคัญในการพิจารณาส่งผู้ร้ายข้ามแดนตามหลักความผิดที่สามารถส่งผู้ร้ายข้ามแดนได้ แต่อาจเกิดปัญหาว่า การกำหนดอัตราโทษในความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์นั้น เป็นดุลพินิจเด็ดขาดของแต่ละรัฐที่จะกำหนดโทษในอัตราเท่าใดก็ได้ ในปัญหานี้อาจกล่าวได้ว่า แม้รัฐมีสิทธิเด็ดขาด ในการกำหนดอัตราโทษในกฎหมายภายในของตน แต่เมื่อพิจารณาในแง่ประโยชน์ในการสร้างมาตรฐานทางกฎหมายที่เป็นอันหนึ่งอันเดียวกัน เพื่อให้เกิดความสะดวกในการให้ความร่วมมือระหว่างประเทศแล้ว จึงควรที่ประเทศต่างๆจะกำหนดอัตราโทษขั้นต่ำให้สอดคล้องกับเงื่อนไขที่กำหนดไว้ในสนธิสัญญาส่งผู้ร้ายข้ามแดน แนวความคิดดังกล่าวนี้ ได้รับความสนับสนุนในเวทีสหประชาชาติ ที่เห็นควรให้ประเทศทั้งหลาย กำหนดอัตราโทษในความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์ที่สูงเพียงพอที่จะสามารถส่งผู้ร้ายข้ามแดนได้ โดยเฉพาะอย่างยิ่งในความผิดเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์โดยไม่ชอบ (Hacking) เนื่องจากการก่ออาชญากรรมคอมพิวเตอร์ในทุกกรณีเป็นการกระทำที่ก่อให้เกิดผลกระทบ ซึ่งสร้างความเสียหายแก่ชุมชนระหว่างประเทศ ไม่ว่าผู้ได้รับความเสียหายโดยตรงจากการกระทำความผิดจะเป็นเอกชนหรือรัฐก็ตาม[211] ดังนั้น จึงควรที่ประเทศทั้งหลายจะได้ให้ความร่วมมือในการกำหนดอัตราโทษในกฎหมายภายในให้สอดคล้องกับสนธิสัญญาส่งผู้ร้ายข้ามแดน ซึ่งโดยทั่วไปในทางปฏิบัติ จะกำหนดอัตราโทษจำคุกไม่ต่ำกว่า 1 ปี จึงจะเป็นความผิดที่สามารถส่งผู้ร้ายข้ามแดนได้ โดยความร่วมมือดังกล่าว จะช่วยลดปัญหา อุปสรรค และข้อขัดข้องในการส่งผู้ร้ายข้ามแดนลงได้

---

[211] 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]

3.2.3 ปัญหาที่สืบเนื่องจากเขตอำนาจศาลในคดีอาชญากรรมคอมพิวเตอร์[212]

ก่อนจะกล่าวถึงปัญหาอันเป็นอุปสรรคในการส่งผู้ร้ายข้ามแดนที่สืบเนื่องมาจากเขตอำนาจศาลในคดีอาชญากรรมคอมพิวเตอร์ จำต้องกล่าวถึงปัญหาเกี่ยวกับเขตอำนาจศาล ในคดีอาชญากรรมคอมพิวเตอร์ก่อน เพื่อให้เข้าใจถึงปัญหาการกำหนดเขตอำนาจศาลในคดีอาชญากรรมคอมพิวเตอร์ ซึ่งจะนำไปสู่ปัญหาการส่งผู้ร้ายข้ามแดนต่อไป อย่างไรก็ตาม การใช้เขตอำนาจของศาลในคดีอาชญากรรมคอมพิวเตอร์ในปัจจุบันยังคงต้องพิจารณาหลักกฎหมายระหว่างประเทศเกี่ยวกับเขตอำนาจศาลในคดีอาญา ซึ่งตามหลักกฎหมายระหว่างประเทศประเทศต่างๆใช้อำนาจศาลในคดีอาญาตามหลัก 3 ประการ คือ เขตอำนาจศาลตามหลักดินแดน เขตอำนาจศาลตามหลักบุคคล และเขตอำนาจศาลในหลักลงโทษสากล อย่างไรก็ตาม ในปัจจุบันการอ้างเขตอำนาจในคดีอาชญากรรมคอมพิวเตอร์ของรัฐต่างๆในการลงโทษผู้กระทำความผิดยังคงจำกัดอยู่เพียงเขตอำนาจเหนือดินแดนและบุคคล เนื่องจากการอ้างเขตอำนาจศาลในหลักลงโทษสากลนั้น เป็นกรณีที่รัฐใช้เขตอำนาจศาลในคดีอาญาแก่การกระทำความผิดที่ถือเป็นความผิดต่อนานาชาติ หรือเป็นความผิดตามกฎหมายระหว่างประเทศ อันเป็นความผิดต่อมวลชุมชน[213] ซึ่งผู้เขียนยังไม่พบว่ามีรัฐใดอ้างเขตอำนาจศาลเหนือการลงโทษสากลในการลงโทษอาชญากรคอมพิวเตอร์ เป็นแต่เพียงแนวความคิดของนักกฎหมายเพื่อให้เกิดความสะดวกในการลงโทษอาชญากร[214] ดังนั้น ในหัวข้อนี้การวิเคราะห์ปัญหาการส่งผู้ร้ายข้ามแดนที่สืบเนื่องจาก

---

[212] การใช้เขตอำนาจของรัฐ (Jurisdiction of States) ตามหลักกฎหมายระหว่างประเทศนั้น คือ การใช้เขตอำนาจของรัฐในทางอาญาไม่ว่าจะเป็นฝ่ายนิติบัญญัติ บริหารหรือตุลาการ แต่เขตอำนาจศาล(ในคดีอาชญากรรมคอมพิวเตอร์) ในความหมายของวิทยานิพนธ์ฉบับนี้ จะมีความหมายจำกัดเพียง ขอบเขตของการใช้อำนาจศาลเกี่ยวกับการกระทำความผิดอาญาของรัฐ โดยเป็นอำนาจทางตุลาการที่จะพิจารณาพิพากษาคดีอาญาของรัฐ ซึ่งเป็นส่วนหนึ่งของการใช้เขตอำนาจรัฐเท่านั้น ดังนั้น จึงไม่รวมถึงการใช้เขตอำนาจของรัฐในทางอาญา โดยฝ่ายบริหารและนิติบัญญัติแต่อย่างใด

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

[214] 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]

ปัญหาเขตอำนาจศาลในคดีอาชญากรรมคอมพิวเตอร์จะจำกัดอยู่เพียงเขตอำนาจศาลเหนือดินแดนและบุคคล ดังต่อไปนี้

ก) เขตอำนาจศาลในคดีอาชญากรรมคอมพิวเตอร์เหนือดินแดน

โดยทั่วไป เขตอำนาจศาลตามหลักดินแดนใช้ในกรณีที่การกระทำความผิดเริ่มต้นในรัฐนั้น แต่ไปสิ้นสุดที่รัฐอื่น และในกรณีที่การกระทำความผิดเริ่มต้นที่รัฐอื่นและสิ้นสุดลงที่รัฐนั้น[215] ซึ่งทั้งสองกรณีทำให้ทั้งรัฐที่การกระทำความผิดเกิดและรัฐที่ผลแห่งการกระทำความผิดเกิดต่างมีเขตอำนาจโดยอาศัยหลักดินแดนทั้งสิ้น อย่างไรก็ตาม หลักกฎหมายระหว่างประเทศเกี่ยวกับเขตอำนาจศาลตามหลักดินแดนนี้ ก่อให้เกิดปัญหาในการวินิจฉัยเขตอำนาจศาลในคดีอาชญากรรมคอมพิวเตอร์ โดยแยกการพิจารณาเป็น 2 กรณีคือ ในกรณีแรกเป็นการกระทำความผิดผ่านเครือข่ายอินเทอร์เน็ตโดยไม่มีการเจาะจงไปยังเครื่องคอมพิวเตอร์ปลายทางเครื่องใด เช่น ความผิดเกี่ยวกับการเผยแพร่ข้อความที่ผิดกฎหมายผ่านเครือข่ายอินเทอร์เน็ต ไม่ว่าจะเป็นภาพลามกอนาจาร หรือข้อความเกี่ยวกับการเหยียดเชื้อชาติ และในกรณีที่สองคือ กรณีที่การกระทำความผิดโดยมีวัตถุประสงค์ต่อเครื่องคอมพิวเตอร์เป้าหมายปลายทางโดยเจาะจง เช่น การกระทำความผิดฐานจารกรรมข้อมูลหรือการฉ้อโกงผ่านเครือข่ายอินเทอร์เน็ต

ประการแรก ความผิดเกี่ยวกับการเผยแพร่ข้อความที่ผิดกฎหมายผ่านเครือข่ายอินเทอร์เน็ตนั้น ในกรณีนี้สามารถกระทำได้หลายช่องทาง เช่น โดยใช้จดหมายอิเล็กทรอนิกส์หรือการกระทำผ่านเว็บไซต์ ซึ่งหากปรับใช้เขตอำนาจศาลตามหลักดินแดนแล้ว สถานที่ที่ผู้กระทำความผิดเผยแพร่ข้อความที่ผิดกฎหมายและสถานที่ที่ข้อความที่ผิดกฎหมายนั้นถูกเผยแพร่ ล้วนถือเป็นสถานที่ที่เกิดการกระทำความผิดทั้งสิ้น อย่างไรก็ตาม เนื่องจากลักษณะพิเศษของเครือข่ายอินเทอร์เน็ตที่ไม่มีพรมแดน และการเข้าถึงเครือข่ายอินเทอร์เน็ตสามารถกระทำจากในสถานที่ใดๆ ก็ได้ จึงทำให้ในบางกรณีการเผยแพร่ข้อความผิดกฎหมายดังกล่าวไม่สามารถพิสูจน์ได้ว่าผู้กระทำ

---

[215] จุมพต สายสุนทร, กฎหมายระหว่างประเทศ (กรุงเทพมหานคร : โรงพิมพ์เดือนตุลา, 2539), หน้า 244.

เป็นใครและส่งจดหมายอิเล็กทรอนิกส์หรือได้เผยแพร่ข้อความนั้นจากสถานที่ใด ซึ่งก่อให้เกิดปัญหาการไม่สามารถพิสูจน์ได้ว่าสถานที่ที่เกิดการกระทำความผิดเกิดขึ้นที่ใด[216]

นอกจากนี้ การที่รัฐต่างๆถือหลักในการอ้างเขตอำนาจที่แตกต่างกันทำให้เกิดความไม่แน่นอนว่า รัฐใดจะมีเขตอำนาจตามหลักดินแดนบ้าง ตัวอย่างเช่น ในคดี Braintech, Inc. v. Kostiuk ซึ่งศาลอุทธรณ์แคนาดาปฏิเสธการบังคับตามคำพิพากษาของศาลสหรัฐอเมริกา ในกรณีที่จำเลยชาวแคนาดาเผยแพร่ข้อความหมิ่นประมาทผู้อื่นผ่านกระดานแสดงความคิดเห็นบนอินเทอร์เน็ตซึ่งได้เผยแพร่ไปในประเทศสหรัฐอเมริกา โดยศาลแคนาดาวางหลักเกี่ยวกับการอ้างเขตอำนาจศาลในคดีอาชญากรรมคอมพิวเตอร์ว่า รัฐที่มีเขตอำนาจเหนือการกระทำความผิดตามหลักดินแดนนั้นจะต้องมีความเชื่อมโยงกันระหว่างมูลคดีกับศาล ข้อเท็จจริงเพียงว่าข้อความนั้นมีการเผยแพร่ในประเทศสหรัฐอเมริกาผ่านทางอินเทอร์เน็ตยังไม่เพียงพอฟังว่าศาลสหรัฐอเมริกามีเขตอำนาจเหนือคดีดังกล่าว เว้นแต่โจทก์จะพิสูจน์ว่า จำเลยได้กระทำการป้อนข้อมูลลงในคอมพิวเตอร์อันเป็นการเริ่มต้นการเผยแพร่ข้อความดังกล่าวในดินแดนของประเทศสหรัฐอเมริกา[217]

อย่างไรก็ตาม ในคดี Yahoo![218] ศาลฝรั่งเศสได้วินิจฉัยในทางตรงข้าม โดยศาลปฏิเสธประเด็นข้อโต้แย้งของจำเลยที่โต้แย้งเรื่องการไม่มีเขตอำนาจเหนือคดีของศาลฝรั่งเศส โดยให้เหตุผลว่า การที่ Yahoo! ปล่อยให้มีการเผยแพร่ข้อความและเปิดประมูลสินค้าที่ระลึกนาซีบน

---

[216] Stephan Wilske and Teresa Schiller, "International jurisdiction in cyberspace: which states may regulate the internet?," 50,117 Fed. Comm. L.J. [Online]1997. Available from: http://www.law.Indiana.edu/fclj/pubs/v50/no1/wilske.html [2003, May 11]

[217] Matthew E. Babcock and others, Internet jurisdiction, choice of law issues [Online],2002, July, Available from: http://www.ldrc.com/cyberspace/internet%20jurisdiction%20and%20choice%20of%20law%20issue.pdf[2003,Jan 23]

[218] รายละเอียดของคดี ดูหัวข้อ 3.2.1.2 1) ข)

อินเทอร์เน็ตที่เผยแพร่ในประเทศฝรั่งเศส ทำให้เกิดความเสียหายในดินแดนของประเทศฝรั่งเศส อันเป็นการละเมิดประมวลกฎหมายอาญาของฝรั่งเศส ศาลฝรั่งเศสจึงมีเขตอำนาจเหนือคดีนี้[219]

จากคำพิพากษาในเรื่องเขตอำนาจศาลในคดีอาชญากรรมคอมพิวเตอร์ของศาลแคนาดาและฝรั่งเศสที่ได้กล่าวข้างต้นนั้น ต่างเป็นกรณีที่วินิจฉัยเกี่ยวกับเขตอำนาจศาลตามหลักดินแดนเหมือนกัน กล่าวคือทั้งสองกรณีรัฐที่อ้างเขตอำนาจศาล เป็นเรื่องสถานที่ที่ผลแห่งการกระทำผิดเกิดขึ้น แต่มีหลักในการวินิจฉัยในเรื่องเขตอำนาจศาลเหนือคดีที่แตกต่างกัน การที่ศาลแคนาดาเห็นว่า การปรากฏขึ้นของข้อความที่ผิดกฎหมายผ่านจอคอมพิวเตอร์ในประเทศหนึ่งไม่ได้ทำให้ประเทศนั้นมีเขตอำนาจศาลในคดีอาชญากรรมคอมพิวเตอร์นั้นแต่อย่างใด ทำให้การพิจารณาเรื่องเขตอำนาจศาลในคดีอาชญากรรมคอมพิวเตอร์แคบลงเหลือเพียงประเทศที่มีจุดเกาะเกี่ยวกับสถานที่ที่เกิดการกระทำความผิดจริงๆ ในขณะที่คำตัดสินของศาลฝรั่งเศสอาจทำให้ทุกประเทศในโลกที่มีคอมพิวเตอร์เชื่อมโยงกับอินเทอร์เน็ตมีเขตอำนาจศาลเหนือการกระทำอันเดียวกันได้ คำพิพากษาของศาลฝรั่งเศสในคดี Yahoo! นี้ อาจกลายเป็นบรรทัดฐานต่อประเทศอื่นๆในการกำหนดเขตอำนาจศาลเหนือดินแดนในคดีการเผยแพร่ข้อความผิดกฎหมายต่างๆได้ ซึ่งการกำหนดเขตอำนาจศาลในแนวทางที่แตกต่างกันนี้ ทำให้การกำหนดเขตอำนาจศาลเหนือการกระทำดังกล่าวของประเทศต่างๆในปัจจุบันไม่เป็นไปในแนวทางเดียวกัน

ประการที่สอง กรณีความผิดเกี่ยวกับการจารกรรมข้อมูลและการฉ้อโกงทางคอมพิวเตอร์ ศาลของประเทศต่างๆก็มีปัญหาในการวินิจฉัยสถานที่ที่เกิดการกระทำความผิดที่ไม่เหมือนกัน ยกตัวอย่างเช่น ศาลของประเทศอังกฤษจะต้องพิจารณาว่า การได้มาซึ่งทรัพย์สินหรือข้อมูลซึ่งจะทำให้การกระทำเป็นความผิดสำเร็จนั้นเกิดขึ้นที่ใด ซึ่งจะส่งผลให้รัฐนั้นมีเขตอำนาจศาลเหนือการกระทำความผิดซึ่งต้องพิจารณาเป็นกรณีไป[220] ในขณะที่ประเทศสหรัฐอเมริกา ในคดี Commonwealth v. Kastafansas วางหลักในการพิจารณาโดยถือว่า หากเครื่องคอมพิวเตอร์ที่

---

[219] Matthew E. Babcock and others, Internet jurisdiction, choice of law issues [Online],2002, July, Available from: http://www.ldrc.com/cyberspace/internet%20jurisdiction%20and%20choice%20of%20law%20issue.pdf[2003,Jan 23]

[220] ดูคดี Thompson และ คดี Tomsett ใน Martin Wasik, Crime and the computer (Oxford: Clarendon Press, 1991) p.194.

ใช้เป็นเครื่องมือในการกระทำความผิดอยู่ที่ใด ให้ถือว่าที่นั้นเป็นสถานที่ที่เกิดการกระทำความผิด[221] โดยไม่จำต้องพิจารณาว่าการกระทำความผิดสำเร็จเกิดขึ้น ณ ที่ใด

ปัญหาการไม่สามารถระบุว่ารัฐใดมีเขตอำนาจเหนือการกระทำความผิดและความแตกต่างในการพิจารณาเขตอำนาจศาลเหนืออาชญากรรมคอมพิวเตอร์ของประเทศต่างๆดังที่กล่าวมาข้างต้นส่งผลทำให้เกิดปัญหาการส่งผู้ร้ายข้ามแดนในกรณีอาชญากรรมคอมพิวเตอร์ เนื่องจากสนธิสัญญาส่งผู้ร้ายข้ามแดนบางฉบับระบุให้เงื่อนไขเรื่องเขตอำนาจศาลของรัฐผู้ร้องขอและรัฐผู้รับคำขอเป็นเงื่อนไขในการส่งหรือไม่ส่งผู้ร้ายข้ามแดนด้วย เช่น สนธิสัญญาส่งผู้ร้ายข้ามแดนบางฉบับระบุว่าความผิดที่มีการส่งผู้ร้ายข้ามแดนได้ต้องอยู่ในอำนาจศาลของประเทศผู้ร้องขอด้วย[222] หรือในกรณีความผิดนั้นได้กระทำนอกเขตของรัฐภาคีทั้งสองฝ่ายและรัฐผู้รับคำขอไม่มีเขตอำนาจเหนือความผิดที่ได้กระทำนอกราชอาณาจักรนั้นตามกฎหมายของตนแล้ว รัฐผู้รับคำร้องขอสามารถปฏิเสธการส่งผู้ร้ายข้ามแดนได้[223] ดังนั้น ความเห็นของศาลของรัฐผู้รับคำร้องขอในการพิจารณาเรื่องเขตอำนาจศาลในคดีอาชญากรรมคอมพิวเตอร์เหนือดินแดนจึงมีความสำคัญต่อการพิจารณาคดีส่งผู้ร้ายข้ามแดนอย่างยิ่ง โดยเฉพาะในกรณีที่ยังมีความลักลั่นในการตีความเกี่ยวกับสถานที่ที่ความผิดเกิด หรือสถานที่ที่การกระทำเป็นความผิดสำเร็จแล้ว ยิ่งทำให้การพิจารณาเรื่องเขตอำนาจศาลในคดีอาญามีความไม่แน่นอน ซึ่งทำให้เป็นอุปสรรคในการส่งผู้ร้ายข้ามแดน

ข) <u>เขตอำนาจศาลในคดีอาชญากรรมคอมพิวเตอร์เหนือบุคคล</u>

การที่รัฐผู้รับคำร้องขอไม่สามารถอ้างเขตอำนาจศาลเหนือดินแดนในคดีอาชญากรรมคอมพิวเตอร์ได้ ซึ่งก่อให้เกิดปัญหาการไม่สามารถส่งผู้ร้ายข้ามแดนได้ตามที่ได้กล่าวมาข้างต้นนั้น มีประเด็นที่ควรพิจารณาต่อไปว่า หากรัฐผู้ร้องขออ้างเขตอำนาจศาลในคดีอาชญากรรมคอมพิวเตอร์เหนือบุคคล เพื่อขอให้ส่งผู้ร้ายข้ามแดนในกรณีอาชญากรรมคอมพิวเตอร์ จะกระทำได้หรือไม่เพียงใด ในการอ้างเขตอำนาจศาลในการกระทำความผิดเหนือบุคคลนี้ก็อาจเกิดปัญหาในการพิจารณาส่งผู้ร้ายข้ามแดนได้เช่นกัน เนื่องจากการที่แต่ละประเทศ

---

[221] Ibid., p.197

[222] ชัยเกษม นิติสิริ, "ความร่วมมือระหว่างประเทศในการส่งผู้ร้ายข้ามแดน," <u>บทบัณฑิตย์</u> 52,4(ธันวาคม 2539): 196.

[223] The UN Model Treaty on Extradition 1990, Article 4(e)

มีหลักการแตกต่างกันเกี่ยวกับเรื่องเขตอำนาจศาล กล่าวคือ ประเทศในกลุ่ม Civil Law ยอมรับการใช้เขตอำนาจศาลในคดีอาญาอย่างกว้างขวาง ซึ่งรวมถึงเขตอำนาจศาลในคดีอาญาเหนือบุคคล ในกรณีที่คนชาติกระทำความผิดนอกราชอาณาจักร เช่น ในประเทศเยอรมนี บังคับใช้กฎหมายอาญากับคนชาติของตนที่อยู่ในต่างประเทศในการกระทำความผิดเกี่ยวกับการเผยแพร่ภาพลามกอนาจารเด็กทางอินเทอร์เน็ต[224]ซึ่งทำให้ศาลเยอรมนีมีเขตอำนาจศาลเหนือการกระทำความผิดนั้นด้วย ในขณะที่ประเทศในกลุ่ม Common Law ถือหลักว่าเขตอำนาจในการดำเนินคดีของรัฐจะจำกัดเฉพาะกรณีที่ความผิดเกิดในรัฐของตนหรือเขตอำนาจศาลเหนือดินแดนเท่านั้น ซึ่งทำให้ประเทศในกลุ่ม Common Law ลังเลที่จะยอมรับเขตอำนาจศาลเหนือบุคคล[225] ดังนั้น ในประเทศที่กำหนดให้เขตอำนาจศาลเป็นเงื่อนไขของการส่งผู้ร้ายข้ามแดน หรือเป็นเหตุแห่งการปฏิเสธการส่งผู้ร้ายข้ามแดน ดังเช่นประเทศอังกฤษที่ถือว่าเขตอำนาจศาลเป็นองค์ประกอบของหลักความผิดอาญาของทั้งสองประเทศ ซึ่งหากรัฐผู้ร้องขออ้างเขตอำนาจศาลเหนือบุคคลโดยไม่มีเขตอำนาจศาลเหนือดินแดน รัฐผู้รับคำขออาจพิจารณาไม่ส่งผู้ร้ายข้ามแดนเนื่องจากถือว่ารัฐผู้ร้องขอไม่มีเขตอำนาจศาลเหนือคดีได้[226]

สำหรับการใช้เขตอำนาจศาลในคดีอาชญากรรมคอมพิวเตอร์ของศาลไทยเหนือดินแดน ประมวลกฎหมายอาญากำหนดการกระทำความผิดในราชอาณาจักรและการกระทำความผิดที่ถือว่ากระทำในราชอาณาจักรไว้ใน มาตรา 4 และมาตรา 5[227] โดยศาลไทยมีอำนาจ

---

[224] Stephan Wilske and Teresa Schiller, "International jurisdiction in cyberspace: which states may regulate the internet?," 50,117 Fed. Comm. L.J. [Online],1997, Available from: http://www.law.Indiana.edu/fclj/pubs/v50/no1/wilske.html [2003, May 11]

[225] ชัยเกษม นิติสิริ, "ความร่วมมือระหว่างประเทศในการส่งผู้ร้ายข้ามแดน," บทบัณฑิตย์ 52,4: 196.

[226] Geoff Gilbert, Aspect of extradition law, p.53..

[227] มาตรา 4 "ผู้ใดกระทำความผิดในราชอาณาจักร ต้องรับโทษตามกฎหมาย

การกระทำความผิดในเรือไทยหรืออากาศยานไทย ไม่ว่าอยู่ ณ ที่ใด ให้ถือว่ากระทำความผิดในราชอาณาจักร"

มาตรา 5 "ความผิดใดที่การกระทำแม้แต่ส่วนหนึ่งส่วนใดได้กระทำในราชอาณาจักรก็ดี ผลแห่งการกระทำเกิดในราชอาณาจักรโดยผู้กระทำประสงค์ให้ผลนั้นเกิดในราชอาณาจักรหรือโดยลักษณะแห่งการกระทำ ผลที่เกิดขึ้นนั้นควรเกิดในราชอาณาจักรหรือย่อมจะเล็งเห็นได้ว่าผลนั้นจะเกิดในราชอาณาจักรก็ดี ให้ถือว่าความผิดนั้นได้กระทำในราชอาณาจักร

พิจารณาพิพากษาลงโทษได้ ไม่ว่าจะเป็นความผิดประเภทใด อย่างไรก็ตาม ยังไม่เคยมีปรากฏว่าศาลไทยใช้เขตอำนาจศาลเหนือดินแดนในกรณีของอาชญากรรมคอมพิวเตอร์ แต่เมื่อประมวลกฎหมายบัญญัติให้ศาลไทยสามารถใช้เขตอำนาจศาลได้อย่างกว้างขวางเช่นนี้ ก็น่าที่จะใช้เขตอำนาจศาลเหนืออาชญากรรมคอมพิวเตอร์ได้เช่นกัน

ส่วนการใช้เขตอำนาจศาลเหนือบุคคลนั้น ประมวลกฎหมายอาญาของไทยบัญญัติไว้ในมาตรา 8[228] ซึ่งหลักเกณฑ์ตามมาตรานี้ คำนึงถึงตัวคนไทยซึ่งเป็นผู้กระทำความผิด หรือผู้เสียหายและฐานความผิดประกอบกัน และจะต้องมีการร้องขอให้ลงโทษด้วย โดยไม่จำเป็นที่การ

ในกรณีการตระเตรียมการ หรือพยายามกระทำการใดซึ่งกฎหมายบัญญัติเป็นความผิด แม้การกระทำนั้นจะได้กระทำนอกราชอาณาจักร ถ้าหากการกระทำนั้นจะได้กระทำตลอดไปจนถึงขั้นความผิดสำเร็จ ผลจะเกิดขึ้นในราชอาณาจักร ให้ถือว่าการตระเตรียมการหรือพยายามกระทำความผิดนั้นได้กระทำในราชอาณาจักร"

[228] มาตรา 8 ผู้ใดกระทำความผิดนอกราชอาณาจักร และ

(ก) ผู้กระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้น หรือผู้เสียหายได้ร้องขอให้ลงโทษ หรือ

(ข) ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็นผู้เสียหาย และผู้เสียหายได้ร้องขอให้ลงโทษ

ถ้าความผิดนั้นเป็นความผิดดังระบุไว้ต่อไปนี้ จะต้องรับโทษภายในราชอาณาจักร คือ

(1) ความผิดเกี่ยวกับการก่อให้เกิดภยันตรายต่อประชาชน ตามที่บัญญัติไว้ในมาตรา 217 มาตรา 218 มาตรา 221 ถึงมาตรา 223 ทั้งนี้เว้นแต่กรณีเกี่ยวกับมาตรา 220 วรรคแรก และมาตรา 224 มาตรา 226 มาตรา 228 ถึงมาตรา 232 มาตรา 237 และมาตรา 233 ถึงมาตรา 236 ทั้งนี้เฉพาะเมื่อเป็นกรณีต้องระวางโทษตามมาตรา 238

(2) ความผิดเกี่ยวกับเอกสาร ตามที่บัญญัติไว้ในมาตรา 264 มาตรา 265 มาตรา 266(1) และ (2) มาตรา 268 ทั้งนี้เว้นแต่กรณีเกี่ยวกับ มาตรา 267 และมาตรา 269

(3) ความผิดเกี่ยวกับเพศ ตามที่บัญญัติไว้ในมาตรา 276 มาตรา 280 และมาตรา 285 ทั้งนี้เฉพาะที่เกี่ยวกับมาตรา 276

(4) ความผิดต่อชีวิต ตามที่บัญญัติไว้ในมาตรา 288 ถึงมาตรา 290

(5) ความผิดต่อร่างกาย ตามที่บัญญัติไว้ในมาตรา 295 ถึงมาตรา 298

(6) ความผิดฐานทอดทิ้งเด็ก คนป่วยเจ็บหรือคนชรา ตามที่บัญญัติไว้ในมาตรา 306 ถึงมาตรา 308

กระทำนั้นจะเป็นความผิดตามกฎหมายของรัฐที่เกิดการกระทำความผิดหรือไม่ อย่างไรก็ตาม มาตรา 8 นี้ก็มีข้อจำกัดเกี่ยวกับการใช้เขตอำนาจศาลเหนือบุคคล เนื่องจากศาลจะสามารถใช้เขตอำนาจศาลเหนือบุคคลได้เฉพาะในความผิดที่ระบุไว้เท่านั้น ดังนั้น ในกรณีความผิดฐานใหม่ เช่น ในกรณีอาชญากรรมคอมพิวเตอร์ จึงไม่อยู่ในบังคับของมาตรา 8[229] เท่ากับศาลไทยจะไม่สามารถใช้เขตอำนาจเหนือบุคคลในความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์ได้

การมีเขตอำนาจศาลในคดีอาชญากรรมคอมพิวเตอร์ของศาลไทยหรือไม่นั้น มีผลในการพิจารณาส่งผู้ร้ายข้ามแดน เนื่องจากสนธิสัญญาส่งผู้ร้ายข้ามแดนของประเทศไทยที่ทำกับประเทศอื่นๆหลายฉบับมีข้อกำหนดเกี่ยวกับการใช้ดุลพินิจในการปฏิเสธการส่งผู้ร้ายข้ามแดน หากรัฐผู้รับคำร้องขอมีเขตอำนาจเหนือคดีที่ร้องขอ อย่างไรก็ตาม สนธิสัญญาส่งผู้ร้ายข้ามแดนแต่ละฉบับก็กำหนดขอบเขตของการอ้างเขตอำนาจศาลเหนือคดีเพื่อปฏิเสธการส่งผู้ร้ายข้ามแดนโดยมีขอบเขตแตกต่างกัน กล่าวคือ สนธิสัญญาส่งผู้ร้ายข้ามแดนระหว่างประเทศไทยกับประเทศฟิลิปปินส์[230] อินโดนีเซีย[231] เกาหลีใต้[232] บังคลาเทศ[233] และสหรัฐอเมริกา[234] กำหนดให้รัฐผู้รับคำขอ

---

(7) ความผิดต่อเสรีภาพ ตามที่บัญญัติไว้ในมาตรา 309 มาตรา 310 มาตรา 312 ถึงมาตรา 315 และมาตรา 317 ถึงมาตรา 320

(8) ความผิดฐานลักทรัพย์และวิ่งราวทรัพย์ ตามที่บัญญัติไว้ในมาตรา 334 ถึงมาตรา 336

(9) ความผิดฐานกรรโชก รีดเอาทรัพย์ ชิงทรัพย์ และปล้นทรัพย์ ตามที่บัญญัติไว้ในมาตรา 337 ถึงมาตรา 340

(10) ความผิดฐานฉ้อโกง ตามที่บัญญัติไว้ในมาตรา 341 ถึงมาตรา 344 มาตรา 346 และมาตรา 347

(11) ความผิดฐานยักยอก ตามที่บัญญัติไว้ในมาตรา 352 ถึงมาตรา 354

(12) ความผิดฐานรับของโจร ตามที่บัญญัติไว้ในมาตรา 357

(13) ความผิดฐานทำให้เสียทรัพย์ ตามที่บัญญัติไว้ในมาตรา 358 ถึงมาตรา 360

[229] รัฐ จำเดิมเผด็จศึก, "ปัญหาการส่งคนชาติข้ามแดนตามกฎหมายว่าด้วยการส่งผู้ร้ายข้ามแดนของประเทศไทย," (วิทยานิพนธ์ปริญญามหาบัณฑิต สาขาวิชานิติศาสตร์ บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย, 2539), หน้า 109.

[230] สนธิสัญญาส่งผู้ร้ายข้ามแดนระหว่างราชอาณาจักรไทยกับสาธารณรัฐฟิลิปปินส์ พ.ศ.2527 ข้อ 3

[231] สนธิสัญญาส่งผู้ร้ายข้ามแดนระหว่างราชอาณาจักรไทยกับสาธารณรัฐอินโดนีเซีย พ.ศ.2522 ข้อ 5

สามารถปฏิเสธการส่งผู้ร้ายข้ามแดนหากการกระทำความผิดที่ร้องขอนั้น ได้กระทำทั้งหมดหรือแต่บางส่วนในดินแดนของตน หรือในสถานที่ที่ถือว่าเป็นดินแดนของตน ซึ่งก็หมายความถึงการให้สิทธิรัฐผู้รับคำขอในการปฏิเสธการส่งผู้ร้ายข้ามแดนหากรัฐผู้รับคำขอมีเขตอำนาจศาลเหนือคดีโดยอาศัยหลักดินแดน ดังนั้น ในกรณีที่มีการร้องขอให้ส่งผู้ร้ายข้ามแดนในคดีอาชญากรรมคอมพิวเตอร์ รัฐผู้รับคำขออาจปฏิเสธการส่งผู้ร้ายข้ามแดนได้ตามสนธิสัญญาหากรัฐผู้รับคำขอนั้นถือว่า อาชญากรรมคอมพิวเตอร์ดังกล่าวเกิดขึ้นทั้งหมดหรือบางส่วนในดินแดนของตน

แต่เมื่อพิจารณาสนธิสัญญาส่งผู้ร้ายข้ามแดนระหว่างประเทศไทยกับประเทศจีน[235] ลาว[236]และกัมพูชา[237]แล้วพบว่า สนธิสัญญาบัญญัติให้สิทธิรัฐภาคีในการใช้ดุลพินิจปฏิเสธไม่ส่งผู้ร้ายข้ามแดนได้ โดยไม่จำกัดเพียงเขตอำนาจศาลเหนือคดีตามหลักดินแดน หากแต่สนธิสัญญาใช้ถ้อยคำอย่างกว้างว่า การส่งผู้ร้ายข้ามแดนอาจถูกปฏิเสธหากรัฐภาคีที่ได้รับการร้องขอมีเขตอำนาจตามกฎหมายเหนือความผิดที่อ้างถึงในคำร้องขอส่งผู้ร้ายข้ามแดน ดังนั้น หากตามกฎหมายภายในของรัฐผู้รับคำขอนั้นมีการยอมรับบังคับใช้เขตอำนาจศาลเหนือคดีโดยอาศัยหลักอื่นนอกจากหลักดินแดน เช่น หลักบุคคล หลักป้องกัน เป็นต้น ซึ่งทำให้รัฐสามารถอ้างเขตอำนาจศาลเหนือคดีที่มีการร้องขอส่งผู้ร้ายข้ามแดนได้แล้ว รัฐผู้รับคำขอนั้นก็สามารถมีดุลพินิจปฏิเสธการส่งผู้ร้ายข้ามแดนได้ตามบทบัญญัติของสนธิสัญญา

---

[232] สนธิสัญญาส่งผู้ร้ายข้ามแดนระหว่างราชอาณาจักรไทยกับสาธารณรัฐเกาหลี พ.ศ.2543 ข้อ 4

[233] สนธิสัญญาส่งผู้ร้ายข้ามแดนระหว่างราชอาณาจักรไทยกับสาธารณรัฐประชาชนบังคลาเทศ พ.ศ.2543 ข้อ 4

[234] สนธิสัญญาส่งผู้ร้ายข้ามแดนระหว่างราชอาณาจักรไทยกับสหรัฐอเมริกา พ.ศ.2533 ข้อ 4

[235] สนธิสัญญาส่งผู้ร้ายข้ามแดนระหว่างราชอาณาจักรไทยกับสาธารณรัฐประชาชนจีน พ.ศ.2541 ข้อ 4

[236] สนธิสัญญาส่งผู้ร้ายข้ามแดนระหว่างราชอาณาจักรไทยกับสาธารณรัฐประชาธิปไตยประชาชนลาว พ.ศ.2543 ข้อ 4

[237] สนธิสัญญาส่งผู้ร้ายข้ามแดนระหว่างราชอาณาจักรไทยกับราชอาณาจักรกัมพูชา พ.ศ.2543 ข้อ 4

จากที่กล่าวมาทั้งหมดนี้ แสดงให้เห็นว่าเขตอำนาจศาลเหนือคดีอาชญากรรมคอมพิวเตอร์มีความสำคัญในการพิจารณาส่งหรือไม่ส่งผู้ร้ายข้ามแดนระหว่างรัฐภาคีได้ตามข้อกำหนดของสนธิสัญญาส่งผู้ร้ายข้ามแดน ปัญหาการกำหนดเขตอำนาจศาลเหนือคดีอาชญากรรมคอมพิวเตอร์ มีสาเหตุมาจากหลักกฎหมายระหว่างประเทศเกี่ยวกับเขตอำนาจศาลในคดีอาญาที่ใช้กันอยู่ในปัจจุบัน ไม่ได้ถูกสร้างขึ้นมาเพื่อใช้กับสภาพของเครือข่ายอินเทอร์เน็ต ซึ่งมีลักษณะแตกต่างจากบริเวณที่มีลักษณะกายภาพที่รัฐเคยใช้เขตอำนาจศาลอยู่ในกรณีปกติ[238] ดังนั้น ความยากลำบากในการกำหนดเขตอำนาจศาลในคดีอาชญากรรมคอมพิวเตอร์และความเห็นที่แตกต่างกันของรัฐต่างๆในการกำหนดเขตอำนาจศาลในกรณีนี้ ทำให้เกิดการขัดแย้งกันซึ่งเขตอำนาจศาลในการพิจารณาคดี เป็นสาเหตุที่ทำให้การส่งผู้ร้ายข้ามแดนเกิดความไม่แน่นอน

3.2.4 ปัญหาที่สืบเนื่องจากหลักการไม่ดำเนินคดีอาญาซ้ำในการกระทำหรือความผิดเดียวกัน (Ne bis in idem)

แนวความคิดเกี่ยวกับการไม่ดำเนินคดีอาญาซ้ำในการกระทำหรือความผิดเดียวกันนี้เป็นหลักกฎหมายอาญาทั่วไปซึ่งได้รับการยอมรับในกฎหมายภายในของทุกประเทศ ส่วนในระดับระหว่างประเทศหลักเดียวกันนี้ก็ได้รับการรับรองไว้ในอนุสัญญาระหว่างประเทศว่าด้วยการส่งผู้ร้ายข้ามแดนหลายฉบับ[239] ซึ่งถือได้ว่าหลักกฎหมายดังกล่าวได้รับการยอมรับให้เป็นหลักเกณฑ์สำคัญประการหนึ่งในการพิจารณาคดีส่งผู้ร้ายข้ามแดน โดยเฉพาะอย่างยิ่งในการกระทำความผิดข้ามชาติดังเช่นอาชญากรรมคอมพิวเตอร์ ซึ่งการกระทำผิดบนเครือข่ายไม่มีพรมแดนแห่งรัฐมาจำกัด ดังนั้น ในการกระทำความผิดในดินแดนของรัฐหนึ่ง อาจส่งผลแห่งการกระทำความผิดไปยัง

---

[238] เขมชาติ ธีรพงษ์, "ปัญหากฎหมายและแนวทางการแก้ไขปัญหาอันเกิดจากการประกอบกิจกรรมบนเครือข่ายอิเล็กทรอนิกส์ : ปัญหาการใช้เขตอำนาจรัฐและปัญหาที่สืบเนื่องมาจากความไม่เพียงพอของกฎหมายที่มีอยู่ในปัจจุบัน," หน้า 11.

[239] Arab League Extradition Agreement 1952, Article 5

The European Extradition Convention 1957, Article 9

The Afro-Asian Convention 1960, Article 11

The Benelux Extradition Convention 1954, Article 8

The UN Model Treaty on Extradition 1990, Article 3(d), 4(b)

รัฐอื่นๆอีกหลายรัฐได้ในเวลาเดียวกัน ซึ่งอาจทำให้มีรัฐมากกว่าหนึ่งรัฐมีเขตอำนาจศาลในการลงโทษผู้กระทำความผิดได้ ดังที่ได้กล่าวมาแล้วในข้อ 3.2.2

ดังนั้น การที่มีรัฐมากกว่าหนึ่งรัฐสามารถลงโทษผู้กระทำความผิดในการกระทำความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์รัฐหนึ่ง และได้มีการลงโทษหรือดำเนินคดีกับผู้กระทำความผิดแล้ว โดยหลักย่อมส่งผลให้รัฐอื่นๆไม่สามารถลงโทษผู้กระทำความผิดในการกระทำหรือความผิดเดียวกันได้อีก ซึ่งทำให้รัฐที่ผู้กระทำความผิดอาศัยอยู่สามารถใช้เหตุดังกล่าวเป็นข้ออ้างในการปฏิเสธการส่งผู้ร้ายข้ามแดนได้ โดยเหตุแห่งการปฏิเสธดังกล่าวถูกรับรองในสนธิสัญญาส่งผู้ร้ายข้ามแดนหลายฉบับ[240] ปัญหาที่เกิดขึ้นคือ ในการวินิจฉัยว่าการกระทำหรือความผิดที่เกิดขึ้นนั้น ได้มีการดำเนินคดีอาญาในการกระทำหรือในความผิดเดียวกันแล้วหรือไม่ขึ้นอยู่กับการตีความทางกฎหมายและนโยบายของรัฐผู้รับคำขอ[241] ซึ่งหากรัฐผู้รับคำขอเห็นว่าความผิดที่ร้องขอเป็นการกระทำอย่างเดียวกันหรือเป็นความผิดอาญาฐานเดียวกันกับคดีที่ได้มีการดำเนินคดีไปแล้วหรืออยู่ระหว่างการดำเนินคดี ก็สามารถใช้เป็นข้ออ้างในการปฏิเสธไม่ส่งผู้ร้ายข้ามแดนได้ เมื่อการวินิจฉัยว่าการกระทำหรือความผิดที่เกิดขึ้นเป็นดุลพินิจของรัฐผู้รับคำร้องขอแล้ว การที่แต่ละรัฐสามารถมีดุลพินิจในการวินิจฉัยประเด็นดังกล่าว ทำให้เกิดความไม่ชัดเจนแน่นอนในการบังคับใช้หลักกฎหมายดังกล่าวในทางระหว่างประเทศ ซึ่งส่งผลทำให้การส่งผู้ร้ายข้ามแดนมีความไม่แน่นอนและให้ผลที่แตกต่างกันไปตามแนวทางการวินิจฉัยและระบบกฎหมายของแต่ละรัฐ

ปัญหาที่อาจเกิดขึ้นอีกประการหนึ่งที่สืบเนื่องจากหลักการไม่ดำเนินคดีซ้ำในการกระทำหรือความผิดเดียวกัน คือ ประเด็นในเรื่องความผิดเกี่ยวกับความมั่นคง เนื่องจากการก่ออาชญากรรมคอมพิวเตอร์อาจถูกตีความว่าเป็นการกระทำต่อความมั่นคงของรัฐ ซึ่งก่อนที่จะวิเคราะห์ถึงปัญหาในประเด็นนี้ ผู้เขียนจะขอกล่าวถึงหลักกฎหมายอันเป็นข้อยกเว้นของหลักการไม่ดำเนินคดีซ้ำในการกระทำหรือความผิดเดียวกันพอสังเขป

ข้อยกเว้นของหลักการไม่ดำเนินคดีซ้ำในการกระทำหรือความผิดเดียวกันนี้ ตามหลักกฎหมายระหว่างประเทศและทางปฏิบัติของนานารัฐนั้น ถือว่าความผิดอันเกี่ยวกับความมั่นคงของรัฐจะไม่อยู่ภายใต้หลักการไม่ดำเนินคดีซ้ำ กล่าวคือ รัฐที่ได้รับความเสียหายจากการกระทำ

---

[240] Ibid.

[241] Bassiouni M. Cherif, International extradition and world public order, p.459.

ความผิดสามารถลงโทษผู้กระทำความผิดซ้ำอีกในความผิดเกี่ยวกับความมั่นคงที่ได้กระทำต่อรัฐนั้นได้ แม้ว่าผู้กระทำความผิดจะได้รับการลงโทษในการกระทำนั้นมาแล้วก็ตาม ดังเช่นที่ปรากฏในมาตรา 10 ประมวลกฎหมายอาญาของไทย[242] ซึ่งได้บัญญัติห้ามมิให้ศาลลงโทษซ้ำในการกระทำความผิดซึ่งได้มีคำพิพากษาของศาลถึงที่สุดให้ปล่อยตัวหรือลงโทษผู้กระทำความผิดในศาลต่างประเทศแล้ว อย่างไรก็ตาม ในความผิดเกี่ยวกับความมั่นคงและการกระทำที่เป็นภัยต่อราชอาณาจักรตามมาตรา 7(1) นั้น มาตรา 10 มิได้บัญญัติห้ามมิให้ศาลลงโทษซ้ำ ดังนั้น ศาลไทยก็มีอำนาจในการพิจารณาพิพากษาลงโทษจำเลยได้อีก[243]

จากข้อยกเว้นที่กล่าวมาข้างต้นนั้น จะเห็นได้ว่า ในกรณีที่การก่ออาชญากรรมคอมพิวเตอร์เป็นการกระทำต่อความมั่นคงหรือเป็นภัยต่อรัฐ โดยหลักรัฐที่ได้รับความเสียหายจากการกระทำดังกล่าว ก็จะมีเขตอำนาจศาลในการพิจารณาพิพากษาคดีดังกล่าวอีก แม้ว่าจำเลยจะได้รับการลงโทษจากศาลในต่างประเทศมาแล้วก็ตาม แต่ปัญหาอาจเกิดขึ้นได้ว่า การพิจารณาว่าอาชญากรรมคอมพิวเตอร์ที่เกิดขึ้นเป็นการกระทำต่อความมั่นคงหรือความปลอดภัยของรัฐหรือไม่นั้น เป็นสิ่งที่พิจารณาได้ยาก เช่น การเจาะระบบคอมพิวเตอร์ของหน่วยงานทางการทหารหรือระบบคอมพิวเตอร์ของหน่วยงานของทางราชการของประเทศ จะถือเป็นการกระทำต่อความลับประเทศอันเกี่ยวกับความมั่นคงแห่งรัฐได้หรือไม่ ซึ่งโดยความเห็นส่วนตัวของผู้เขียนแล้ว เห็นว่าการเจาะระบบคอมพิวเตอร์อาจเกิดขึ้นได้โดยทั่วไป แม้เป้าหมายของการกระทำจะอยู่ที่ระบบคอมพิวเตอร์ของหน่วยงานทางราชการ ก็มิได้หมายความว่าเป็นการกระทำความผิดเกี่ยวกับความมั่นคงเสมอไป หากแต่จะต้องพิจารณาถึงเจตนาและมูลเหตุจูงใจที่แท้จริงของผู้กระทำว่า มีเจตนาจะกระทำความผิดเกี่ยวกับความมั่นคงหรือไม่ ซึ่งต้องพิจารณาเป็นรายกรณีไป

---

[242] มาตรา 10 "ผู้ใดกระทำการนอกราชอาณาจักรซึ่งเป็นความผิดตามมาตราต่างๆที่ระบุไว้ในมาตรา 7 (2) และ (3) มาตรา 8 และมาตรา 9 ห้ามมิให้ลงโทษผู้นั้นในราชอาณาจักรเพราะการกระทำนั้นอีก ถ้า

(1) ได้มีคำพิพากษาของศาลในต่างประเทศอันถึงที่สุดให้ปล่อยตัวผู้นั้น หรือ

(2) ศาลในต่างประเทศพิพากษาลงโทษและผู้นั้นได้พ้นโทษแล้ว

ถ้าผู้ต้องคำพิพากษาได้รับโทษสำหรับการกระทำนั้นตามคำพิพากษาของศาลในต่างประเทศมาแล้ว แต่ยังไม่พ้นโทษ ศาลจะลงโทษน้อยกว่าที่กฎหมายกำหนดไว้สำหรับความผิดนั้นเพียงใดก็ได้ หรือจะไม่ลงโทษเลยก็ได้ ทั้งนี้ โดยคำนึงถึงโทษที่ผู้นั้นได้รับมาแล้ว"

[243] สุผานิต มั่นศุข, "เขตอำนาจศาลในคดีอาญา," หน้า 239.

ความยากลำบากในการพิจารณาคดีในลักษณะนี้ อาจก่อให้เกิดปัญหาการส่งผู้ร้ายข้ามแดนได้ เนื่องจากหากรัฐผู้รับคำขอเห็นว่า การกระทำที่ถูกร้องขอนั้น เป็นเพียงความผิดที่เป็นอาชญากรรมคอมพิวเตอร์ธรรมดาที่ไม่มีส่วนเกี่ยวข้องกับเนื่องของความมั่นคงอันเป็นข้อยกเว้นของหลักการไม่ดำเนินคดีซ้ำแล้ว รัฐผู้รับคำขอนั้นอาจปฏิเสธการส่งผู้ร้ายข้ามแดนได้หากการกระทำนั้นได้มีการดำเนินคดีแล้ว กรณีดังกล่าว นอกจากจะทำให้ไม่สามารถส่งผู้ร้ายข้ามแดนได้แล้ว ยังอาจทำให้รัฐที่ได้รับความเสียหายไม่สามารถลงโทษผู้กระทำความผิดได้อย่างสาสมกับความเสียหายที่ตนได้รับอีกด้วย ดังนั้น การพิจารณาว่าการกระทำความผิดจะตกอยู่ภายใต้ข้อยกเว้นของหลักการไม่ดำเนินคดีซ้ำ ซึ่งส่งผลต่อการพิจารณาส่งผู้ร้ายข้ามแดนหรือไม่นี้ เป็นเรื่องที่รัฐผู้รับคำขอต้องตีความอย่างเคร่งครัดและเป็นธรรมแก่รัฐที่ได้รับความเสียหายด้วย

3.2.5 ปัญหาที่สืบเนื่องจากความผิดทางการเมือง

การกระทำความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์มีลักษณะการกระทำที่หลากหลายดังที่ได้กล่าวมาแล้วในตอนต้นของบทที่ 3 นี้ ซึ่งในหลายกรณีอาจถูกตีความว่าเป็นความผิดทางการเมืองเพื่อเป็นข้อยกเว้นในการส่งผู้ร้ายข้ามแดน เช่น การเจาะระบบหรือการกระทำต่อข้อมูลทางคอมพิวเตอร์ใดๆที่เกี่ยวกับข้อมูลด้านความมั่นคงของรัฐ ความผิดเกี่ยวกับเรื่องการเหยียดเชื้อชาติและลัทธิทางการเมือง หรือการกระทำอาชญากรรมคอมพิวเตอร์อื่นใดที่อ้างว่ามีมูลเหตุจูงใจหรือวัตถุประสงค์ทางการเมือง ซึ่งเป็นเจตนาภายในของผู้กระทำ เป็นต้น ซึ่งการอ้างเหตุความผิดทางการเมืองในคดีอาชญากรรมคอมพิวเตอร์ ทำให้ต้องพิจารณาหลักเกณฑ์ทั่วไปเกี่ยวกับความผิดทางการเมือง ซึ่งสามารถใช้อ้างเป็นเหตุเพื่อปฏิเสธการส่งผู้ร้ายข้ามแดนได้เช่นเดียวกับความผิดอาญาอื่นๆ

จากหลักเกณฑ์ในการพิจารณาความผิดในทางการเมืองของประเทศต่างๆ ซึ่งมีหลักต่างกัน เช่น หลัก Political-Incidence Theory ซึ่งใช้ในกลุ่มประเทศ Common Law โดยถือว่าความผิดทางการเมืองต้องเป็นการกระทำโดยตรงต่อองค์กรของรัฐหรือต่อสิทธิของประชาชน ซึ่งกฎหมายให้ความคุ้มครอง รวมถึงจะต้องพิจารณาถึงวัตถุประสงค์หรือแรงจูงใจของบุคคลซึ่งได้รับแรงกระตุ้นหรือปลุกเร้าจากความรู้สึกที่เห็นแก่ประโยชน์ส่วนรวมหรือความรักชาติ ซึ่งเป็นการพิจารณาทั้งข้อเท็จจริงภายนอกและภายในรวมกัน[244] นอกจากทฤษฎีนี้แล้ว ในประเทศฝรั่งเศสมี

---

[244]วิชญา ลิ่มวงศ์, "ความผิดทางการเมืองในการส่งผู้ร้ายข้ามแดน," (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2537), หน้า 39.

การใช้หลัก The Injured Rights โดยถือหลักว่าจะไม่มีการส่งผู้ร้ายข้ามแดนหากพฤติการณ์แวดล้อมแสดงให้เห็นว่าเป็นการกระทำโดยมีวัตถุประสงค์ในทางการเมือง ความผิดทางการเมืองตามหลักนี้จึงต้องเป็นการกระทำที่มีผลโดยตรงต่อความมั่นคงของรัฐและอธิปไตยของรัฐก่อให้เกิดการแทรกแซงการใช้อำนาจภายใน ซึ่งเป็นการพิจารณารูปแบบของการกระทำในด้านเนื้อหา โดยไม่พิจารณามูลเหตุจูงใจ[245] แนวทางของประเทศต่างๆในการวินิจฉัยในเรื่องความผิดทางการเมืองนั้น ส่วนใหญ่มีการพิจารณาองค์ประกอบในเรื่องรูปแบบการกระทำเป็นส่วนใหญ่ซึ่งจะต้องมีความชัดเจนว่า เป็นการกระทำเพื่อก่อผลทางการเมือง เช่น การจลาจล จึงอาจเกิดปัญหาว่า ลักษณะของคำนิยามเช่นนี้ จะปรับใช้กับอาชญากรรมคอมพิวเตอร์ได้เพียงใด

อย่างไรก็ตาม ดังที่ได้กล่าวมาแล้วว่า อาชญากรรมคอมพิวเตอร์บางฐานความผิดอาจถูกตีความให้เป็นความผิดทางการเมืองหรือเกี่ยวข้องกับทางการเมือง เช่นในกรณีการกระทำอาชญากรรมคอมพิวเตอร์ต่อระบบหรือฐานข้อมูลของรัฐบาลหรือที่เกี่ยวกับความมั่นคงของรัฐ การยกเหตุความผิดทางการเมืองขึ้นอ้างในคดีการส่งผู้ร้ายข้ามแดนในกรณีดังกล่าวนี้เกิดขึ้นในคดีของ Gary McKinnon ซึ่งประเด็นในคดีมีว่า Gary McKinnon ถูกกล่าวหาจากทางการสหรัฐอเมริกาว่า กระทำการเจาะระบบคอมพิวเตอร์ของหน่วยงานทางการทหาร เพนตากอน หน่วยงานทางอากาศยานและอวกาศแห่งชาติ กว่า 14 รัฐทั่วประเทศสหรัฐอเมริกา ซึ่งการกระทำครั้งนี้ถือเป็นการเจาะระบบที่ทำให้หน่วยงานราชการสหรัฐอเมริกาเสียหายมากที่สุดเท่าที่เคยตรวจสอบมา การกระทำของ Gary McKinnon ทำให้ศาลมลรัฐเวอร์จิเนียและนิวเจอร์ซีของสหรัฐอเมริกาตั้งข้อหาว่ากระทำอาชญากรรมคอมพิวเตอร์ และรัฐบาลสหรัฐอเมริกาขอให้รัฐบาลอังกฤษส่งตัว Gary McKinnon ข้ามแดนมายังสหรัฐอเมริกา ในคดีดังกล่าว Gary McKinnon อ้างว่าการกระทำของเขามีมูลเหตุจูงใจทางการเมือง ขอให้ทางการอังกฤษปฏิเสธการส่งผู้ร้ายข้ามแดน[246]

คดีที่ได้ยกตัวอย่างมาข้างต้น ปัจจุบันยังอยู่ระหว่างการพิจารณาของศาลอังกฤษ ซึ่งยังไม่มีข้อสรุปว่าศาลอังกฤษจะพิจารณาข้อต่อสู้ของจำเลยอย่างไร แต่คดีนี้ก็ได้รับการ

---

[245] เรื่องเดียวกัน

[246] Ted Bridis, Military-hacker suspect to fight extradition to U.S.[Online],2002, Nov.13, Available from: http://home.hamptonroads.com/stories/print.cfm?story=46540&ran=239902 (2003, June 18)

วิพากษ์วิจารณ์อย่างกว้างขวางถึงความเป็นไปได้ถึงมูลเหตุจูงใจในทางการเมือง เนื่องจากทางการสอบสวนของเจ้าหน้าที่ตำรวจอังกฤษไม่พบว่า จำเลยเสนอข้อมูลอันเป็นความลับของประเทศสหรัฐอเมริกาแก่รัฐบาลประเทศอื่นหรือกลุ่มองค์กรก่อการร้ายแต่อย่างใด[247] ซึ่งผู้เขียนเห็นว่า การเข้าถึงระบบข้อมูลคอมพิวเตอร์ของรัฐบาลไม่ได้แสดงว่าเป็นลักษณะของการกระทำความผิดทางการเมืองเสมอไป เว้นแต่จะมีพยานหลักฐานบ่งชี้อย่างชัดแจ้ง เนื่องจากในปัจจุบันการเข้าถึงระบบข้อมูลขององค์กรภาครัฐเกิดขึ้นอยู่เสมอและโดยส่วนใหญ่ก็มีสาเหตุมาจากความอยากทดลองความสามารถหรือความอยากรู้อยากเห็น อาจกล่าวได้ว่า ในกรณีการกระทำต่อระบบข้อมูลคอมพิวเตอร์ของหน่วยงานหรือองค์กรภาครัฐนั้นการจะวินิจฉัยว่าเป็นการกระทำความผิดทางการเมืองหรือไม่จึงยากกว่าความผิดอาญาอื่นๆ ทั้งในแง่ของการพิจารณารูปแบบของการกระทำทางเนื้อหาและการพิสูจน์วัตถุประสงค์หรือแรงจูงใจของผู้กระทำความผิด

นอกจากการกระทำต่อระบบฐานข้อมูลคอมพิวเตอร์ของรัฐบาลหรือต่อข้อมูลอันเป็นความลับของประเทศแล้ว ความผิดเกี่ยวกับเรื่องการเหยียดเชื้อชาติและลัทธิทางการเมืองผ่านเครือข่ายอินเทอร์เน็ตก็เป็นอีกกรณีหนึ่งที่อาจถูกตีความว่าเป็นความผิดทางการเมืองได้ เช่น คดีของนาย Gary Lauck[248] ซึ่งเผยแพร่สิ่งพิมพ์ที่มีเรื่องราวเกี่ยวกับลัทธินาซี รวมถึงสิ่งพิมพ์ที่มีเนื้อหาแสดงความเกลียดชังคนเชื้อสายยิวและชาวต่างชาติ และรัฐบาลเดนมาร์กได้ส่งตัวข้ามแดนแก่ประเทศเยอรมนีเพื่อพิจารณาลงโทษตามกฎหมายอาญาเยอรมนีนั้น เกิดประเด็นทางกฎหมายซึ่งโต้แย้งการพิจารณาส่งผู้ร้ายข้ามแดนของรัฐบาลเดนมาร์กว่า การกระทำการเผยแพร่ข้อความสนับสนุนลัทธิทางการเมืองและการเหยียดเชื้อชาติในกรณีนี้ของจำเลยในคดีนี้ มีความเห็นของนักกฎหมายว่า คดีนี้อาจถือได้ว่าเป็นความผิดทางการเมืองที่ต้องตกอยู่ภายใต้ข้อยกเว้นของการส่งผู้ร้ายข้ามแดน แต่ประเด็นดังกล่าวกลับไม่ถูกหยิบยกขึ้นมาพิจารณาในชั้นการพิจารณาส่งผู้ร้ายข้ามแดนเลย[249]

จากคดีดังกล่าวจะเห็นว่าประเด็นการพิจารณาการเผยแพร่ข้อความเหยียดเชื้อชาติและลัทธิทางการเมืองผ่านอินเทอร์เน็ตว่าเป็นความผิดทางการเมืองหรือไม่เริ่มมีความเห็นที่

---

[247] Ibid.

[248] ดูข้อเท็จจริงในคดี ในบทที่ 3 ข้อ 3.2.1.2 1) ข)

[249] 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 : 345.

แตกต่างกัน แน่นอนว่าในประเทศที่กำหนดให้การกระทำฐานนี้เป็นความผิดอาญาย่อมไม่ต้องการให้การกระทำดังความผิดดังกล่าวเข้าข่ายเป็นความผิดทางการเมือง ซึ่งในคดีดังกล่าวการที่ประเทศเยอรมนีร้องขอให้มีการส่งผู้ร้ายข้ามแดนในความผิดฐานนี้ และประเทศเดนมาร์กพิจารณาส่งผู้ร้ายข้ามแดนให้ย่อมแสดงให้เห็นว่ามีการยอมรับให้ความผิดฐานนี้เป็นความผิดที่สามารถส่งผู้ร้ายข้ามแดนกันได้และไม่เป็นความผิดทางการเมือง อย่างไรก็ตาม แนวโน้มของหลายประเทศต่อปัญหานี้ในปัจจุบันนั้น เนื่องจากอนุสัญญาว่าด้วยอาชญากรรมคอมพิวเตอร์ของคณะกรรมการยุโรป (Convention on Cybercrime 2001) ซึ่งเป็นอนุสัญญาโดยตรงเกี่ยวกับอาชญากรรมคอมพิวเตอร์ของภูมิภาคยุโรป กำหนดให้ความผิดเกี่ยวกับการเหยียดเชื้อชาติผ่านเครือข่ายอินเทอร์เน็ตเป็นความผิดตามอนุสัญญา ซึ่งมีผลทำให้ความผิดฐานนี้เป็นความผิดที่รัฐภาคีมีพันธกรณีที่จะต้องให้ความร่วมมือระหว่างประเทศในการส่งผู้ร้ายข้ามแดนระหว่างกัน[250]โดยปริยาย[251] ผลจากอนุสัญญาฉบับดังกล่าวทำให้กลุ่มประเทศในภูมิภาคยุโรปส่วนใหญ่จะต้องบัญญัติกฎหมายภายในให้ความผิดเกี่ยวกับการเหยียดเชื้อชาติเป็นความผิดอาญา และไม่ถือว่าความผิดฐานดังกล่าวเป็นความผิดทางการเมือง ซึ่งถือเป็นทางปฏิบัติที่จะได้รับการยอมรับต่อไปในอนาคตของภูมิภาคนี้

อย่างไรก็ตาม การพิจารณาว่ากรณีใดเป็นความผิดทางการเมืองยังคงขึ้นอยู่กับแนวการวินิจฉัยของรัฐแต่ละรัฐซึ่งอาจมีการตีความแตกต่างกันไปเนื่องจากในปัจจุบันยังคงไม่มีการกำหนดนิยามของการกระทำอาชญากรรมคอมพิวเตอร์ที่อาจถือเป็นความผิดทางการเมืองที่ชัดเจน ดังนั้น การชี้ว่าการกระทำอย่างใดเป็นความผิดทางการเมืองจึงเป็นสิทธิเด็ดขาดของรัฐที่

---

[250]Article 24 paragraph 1a "This article applies to extradition between Parties for the criminal offenses 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"

[251] ประเทศสมาชิก 43 ประเทศในสภายุโรปเห็นชอบในการเพิ่มเติมสนธิสัญญา โดยการรวมเรื่องการเหยียดเชื้อชาติในข้อตกลงหลัก ในขณะที่ประเทศสหรัฐอเมริกาไม่เห็นด้วยกับการกำหนดเรื่องเหยียดเชื้อชาติเป็นความผิดตามอนุสัญญาและไม่ร่วมลงนามในพิธีสารเพิ่มเติมดังกล่าว ทำให้สหรัฐอเมริกาไม่ผูกพันที่จะต้องส่งผู้ร้ายข้ามแดนในความผิดฐานนี้ให้กับรัฐภาคีอื่นๆ

ได้รับคำร้องขอ[252] นอกจากนี้ การนำทฤษฎีความผิดทางการเมืองมาใช้กับอาชญากรรมคอมพิวเตอร์ก็ดูจะไม่ค่อยเหมาะสมในทางปฏิบัติเนื่องด้วยลักษณะของอาชญากรรมคอมพิวเตอร์ที่ไม่มีการกระทำทางกายภาพที่เห็นชัดเจน ทำให้แนวทางการวินิจฉัยความผิดทางการเมืองในกรณีอาชญากรรมคอมพิวเตอร์อาจมีแตกต่างกันและเกิดความไม่แน่นอนอันเป็นอุปสรรคในการส่งผู้ร้ายข้ามแดน

จากการศึกษาในส่วนของบทที่ 3 นี้ ทำให้ทราบว่าในปัจจุบัน นอกจากปัญหาการส่งผู้ร้ายข้ามแดนจะมีที่มาจากประเด็นความไม่สอดคล้องกันของกฎหมายภายในของประเทศต่างๆ ซึ่งหมายรวมถึงทั้งกรณีการขาดกฎหมายภายในเกี่ยวกับอาชญากรรมคอมพิวเตอร์และการมีกฎหมายภายในเกี่ยวกับอาชญากรรมคอมพิวเตอร์ที่มีขอบเขตการบังคับใช้ต่างกัน ซึ่งก่อให้เกิดปัญหาการส่งผู้ร้ายข้ามแดนเพราะไม่เป็นความผิดอาญาของทั้งสองประเทศแล้ว ยังมีความขัดข้องในการส่งผู้ร้ายข้ามแดนที่สืบเนื่องมาจากปัญหาการบังคับใช้หลักเกณฑ์ระหว่างประเทศว่าด้วยการส่งผู้ร้ายข้ามแดนที่นานาประเทศถือปฏิบัติอยู่ในปัจจุบันกับคดีอาชญากรรมคอมพิวเตอร์อีกด้วย เนื่องจากอาชญากรรมคอมพิวเตอร์เป็นอาชญากรรมที่มีลักษณะพิเศษเฉพาะแตกต่างจากอาชญากรรมอื่นทั่วไป จึงทำให้หลักเกณฑ์ว่าด้วยการผู้ร้ายข้ามแดนดังกล่าวมีความไม่เหมาะสมที่จะบังคับใช้กับการส่งผู้ร้ายข้ามแดนในคดีความผิดเช่นว่านี้ ซึ่งเป็นผลให้เกิดปัญหาทางกฎหมายและอุปสรรคในการส่งผู้ร้ายข้ามแดน การศึกษาถึงปัญหาทางกฎหมายเหล่านี้ เพื่อจะนำไปสู่การศึกษาถึงวิธีการแก้ปัญหาอย่างมีประสิทธิภาพ ซึ่งแนวทางการแก้ปัญหานั้นผู้เขียนจะได้ศึกษาวิเคราะห์ในบทที่ 4 ต่อไป

---

[252]สุผานิต มั่นศุข, "เขตอำนาจศาลในคดีอาญา," หน้า 129.