บทที่ 3

ปัญหาและอุปสรรคในการปฏิบัติตามพันธกรณีแห่งอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 ของประเทศที่เป็นภาคี

จากการศึกษาในบทที่ผ่านมาทำให้ทราบถึงมาตรการและหลักการต่างๆของอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 (Convention on Cyber Crime 2001) รวมถึงประเทศภาคีสมาชิกทั้งที่มีการลงนามและให้สัตยาบัน และยังมิได้มีการให้สัตยาบัน ซึ่งในบทที่ 3 นี้ ผู้เขียนจะขอยกตัวอย่างประเทศที่ไม่ได้เป็นสมาชิกของสภายุโรปแต่ได้มีการลงนามเป็นภาคีและให้สัตยาบันอนุสัญญาดังกล่าว คือ ประเทศสหรัฐอเมริกา และประเทศที่เป็นสมาชิกของสภายุโรปที่มีการลงนามและให้สัตยาบันอนุสัญญาดังกล่าว คือ ประเทศฝรั่งเศส ทั้งนี้ เพื่อแสดงให้เห็นถึงการปฏิบัติตามพันธกรณีของประเทศภาคีอนุสัญญา และนำมาใช้เป็นแนวทางสำหรับประเทศไทย

3.1 ประเทศสหรัฐอเมริกา

อย่างที่ทราบกันดีอยู่แล้วว่าประเทศสหรัฐอเมริกาเป็นประเทศมหาอำนาจและมีความเจริญก้าวหน้าทางเทคโนโลยีสารสนเทศ ทั้งที่ไม่ได้เป็นประเทศสมาชิกของสภายุโรป แต่ประเทศสหรัฐอเมริกาก็ได้มีการลงนามและให้สัตยาบันอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 ให้มีผลบังคับใช้ ถือเป็นการแสดงเจตนารมณ์อันแท้จริงที่แสดงออกอย่างชัดเจนในรูปแบบลายลักษณ์อักษร ทั้งที่อนุสัญญาดังกล่าวไม่ได้มีบทบัญญัติที่มีลักษณะบังคับทางกฎหมายให้ประเทศสมาชิกต้องปฏิบัติตามภายในเงื่อนไขทางด้านเวลา หรือบทลงโทษหากไม่ปฏิบัติตามเงื่อนไข แต่หากอนุสัญญาดังกล่าวเป็นเพียงการกำหนดแนวทางปฏิบัติให้แก่ประเทศภาคีเพื่อต้องการให้เกิดความสอดคล้องทางด้านกฎหมายสารบัญญัติ กฎหมายสบัญญัติและช่วยสนับสนุนมาตรการทางด้านความร่วมมือระหว่างประเทศที่รวดเร็วและมีประสิทธิภาพแก่ประเทศสมาชิก ในทางปฏิบัติระหว่างประเทศภาคีอนุสัญญาส่วนใหญ่ที่มีการแสดงเจตนารมณ์อย่างชัดแจ้งในข้อตกลงใดก็มักจะต้องปฏิบัติตามพันธกรณีที่เกิดขึ้นตามข้อตกลงดังกล่าว ซึ่งเป็นการสะท้อนให้เห็นถึงเจตนารมณ์ของประเทศภาคีสมาชิกว่าหากไม่ปฏิบัติตามอาจได้รับผลกระทบทางด้านอื่นๆ เช่น อาจได้รับแรงกดดันทางการเมือง หรือทางเศรษฐกิจ จึงทำให้ประเทศภาคีต้องผูกพันโดยอ้อมอยู่แล้ว แต่การแสดงออกอย่างชัดแจ้งของประเทศสหรัฐอเมริกาที่มีการลงนามและให้สัตยาบันอนุสัญญาดังกล่าวทำให้ประเทศสหรัฐอเมริกามีพันธกรณีที่ต้องดำเนินการเกี่ยวกับมาตรการต่างๆตามที่กำหนดในอนุสัญญา โดยต้องสอดคล้องและไม่ก่อให้เกิดอุปสรรคในการปฏิบัติตามความร่วมมือระหว่างประเทศ แต่จากความแตกต่างในหลายด้านของประเทศใน

แถบยุโรปและอเมริกาเอง รวมทั้งแนวคิดทางด้านการเมือง การปกครอง สังคม รวมถึงการคุ้มครองสิทธิเสรีภาพที่แตกต่างกัน อาจทำให้เกิดปัญหาหรืออุปสรรคต่อการปฏิบัติตามพันธกรณีได้ ดังนั้น จึงควรศึกษาถึงสถานการณ์เกี่ยวกับปัญหาอาชญากรรมเกี่ยวกับคอมพิวเตอร์และอินเทอร์เน็ตในประเทศสหรัฐอเมริกา รวมถึงแนวทางในการปฏิบัติเพื่อป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ ปัญหาและอุปสรรคในการปฏิบัติตามพันธกรณี และผลกระทบจากการปฏิบัติตามพันธกรณีแห่งอนุสัญญาดังกล่าว เพื่อนำมาเป็นแนวทางสำหรับประเทศไทย

3.1.1 สถานการณ์เกี่ยวกับปัญหาอาชญากรรมเกี่ยวกับคอมพิวเตอร์และอินเทอร์เน็ตในประเทศสหรัฐอเมริกา

ประเทศสหรัฐอเมริกาเป็นประเทศที่มีความเจริญก้าวหน้าทางเทคโนโลยีมากกว่าประเทศอื่นๆรวมถึงมีการเชื่อมโยงเทคโนโลยีสารสนเทศเข้ากับเศรษฐกิจยุคใหม่ได้อย่างมีประสิทธิภาพ แต่ในทางตรงข้ามประเทศสหรัฐอเมริกาก็เป็นประเทศที่มีการก่ออาชญากรรมทางคอมพิวเตอร์มากกว่าประเทศอื่นเช่นเดียวกัน เห็นได้จากรายงานของสถาบันความปลอดภัยคอมพิวเตอร์ (Computer Security Institute : CSI) และหน่วยงานด้านการบุกรุกคอมพิวเตอร์ (Computer Intrusion Squad) ของ FBI สาขาซานฟรานซิสโก เผยผลการสำรวจเรื่องความปลอดภัยทางคอมพิวเตอร์จากผู้เชี่ยวชาญด้านความปลอดภัยคอมพิวเตอร์ 494 คน จากหน่วยงานภาครัฐ ภาคเอกชน และสถาบันการศึกษา พบว่า 15 อันดับ อาชญากรรมทางคอมพิวเตอร์ที่ก่อให้เกิดความเสียหายแก่ประเทศสหรัฐอเมริกามากที่สุดในปี 2550 ได้แก่[1]

1. การเข้าใช้อินเทอร์เน็ตในทางที่ผิดของพนักงานเจ้าหน้าที่

2. ไวรัส

3. ความเสียหายเกี่ยวกับคอมพิวเตอร์แบบพกพาหรืออุปกรณ์เคลื่อนที่ เช่น สมาร์ทโฟน

4. การหลอกขอข้อมูล

5. การใช้ข้อความแบบทันทีในทางที่ผิด (Instant Messaging Misuse) การปฏิเสธการให้บริการและการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

---

[1] ศูนย์บริการความรู้ทางวิทยาศาสตร์และเทคโนโลยี สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ, CSI เผย 15 อันดับอาชญากรรมคอมพิวเตอร์[ออนไลน์], 2550, แหล่งที่มา: http://www.stks.or.th/web/index.php?option=com_content&task=view&id=1442&Itemid=156 [2552, มกราคม 11]

6. การเข้าควบคุมเครื่องคอมพิวเตอร์

7. การขโมยข้อมูลลูกค้าและการใช้เครือข่ายไร้สายในทางที่ผิด

8. การเจาะระบบ

9. การฉ้อโกงทางการเงิน

10. การดักขโมยรหัสผ่านและการเปลี่ยนหน้าเว็บไซต์

11. การใช้เว็บไซต์ให้บริการทั่วไปในทางที่ผิด

12. ความเสียหายเกี่ยวกับข้อมูลที่เป็นกรรมสิทธิ์

13. ความเสียหายที่เกี่ยวกับแม่ข่าย DNS

14. การฉ้อโกงทางโทรคมนาคม

15. การก่อวินาศกรรม

3.1.2 แนวทางในการปฏิบัติในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์

การลงนามเป็นภาคีอนุสัญญาของประเทศสหรัฐอเมริกาเริ่มต้นจากการที่ประเทศสหรัฐอเมริกามีบทบาทสำคัญในการร่างอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 โดยสภายุโรปได้ส่งคำเชื้อเชิญให้ประเทศสหรัฐอเมริกาเข้าร่วมเป็นผู้สังเกตการณ์ในปี ค.ศ. 1989 และปี ค.ศ. 1995 เมื่อมีข้อเสนอแนะครั้งแรกเกิดขึ้นประเทศสหรัฐอเมริกาเป็นเพียงผู้สังเกตการณ์ในขณะที่มีการร่างอนุสัญญา ต่อมาสภายุโรปได้เชื้อเชิญให้เข้าร่วมในการเจรจาเกี่ยวกับอนุสัญญาจึงได้ตอบตกลง จากการที่เข้าร่วมการเจรจาครั้งนี้ทำให้สภายุโรปให้สิทธิแก่ประเทศสหรัฐอเมริกาในการลงนามเป็นภาคีสมาชิกในอนุสัญญา แต่สิ่งสำคัญคือ ประเทศสหรัฐอเมริกาเองก็ไม่จำเป็นต้องผูกพันในการลงนามอนุสัญญาเนื่องจากเป็นเพียงผู้เข้าร่วมการเจรจาเท่านั้น ทั้งนี้ สภายุโรปยังให้สิทธิในการออกเสียงในการร่างอนุสัญญาดังกล่าวแก่ประเทศสหรัฐอเมริกาด้วย ในที่สุดประเทศสหรัฐอเมริกาจึงตัดสินใจที่จะลงนามและให้สัตยาบันอนุสัญญาดังกล่าวโดยเหตุผลที่ทำให้ประเทศสหรัฐอเมริกายินยอมลงนามใน

อนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 ทั้งที่มิได้เป็นสมาชิกสภายุโรปมี 8 ประการ[2] ดังนี้

1. อนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 ได้บัญญัติมาตรการทางกฎหมายที่จำเป็นให้มีผลบังคับใช้เพื่ออุดช่องโหว่ของอาชญากรรมทางคอมพิวเตอร์ระหว่างประเทศ การติดต่อสื่อสารรวมถึงการถ่ายทอดข้อมูลข่าวสารทุกอย่างที่กระทำผ่านทางคอมพิวเตอร์และระบบเครือข่ายอินเทอร์เน็ตได้แพร่หลายไปทั่วโลก การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ระหว่างประเทศสามารถเกิดขึ้นได้อย่างรวดเร็ว ประเทศใดประเทศหนึ่งจึงไม่สามารถพัฒนากฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ได้โดยลำพัง ไม่ว่าจะเป็นในเรื่องความร่วมมือระหว่างประเทศและการให้ความช่วยเหลือซึ่งกันและกันในการค้นหา การเก็บรวบรวมพยานหลักฐาน และการดำเนินคดีกับผู้กระทำความผิด ดังนั้น จึงไม่มีทางเลือกอื่นสำหรับประเทศที่มีปัญหาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ นอกเหนือไปจากการทำความตกลงระหว่างประเทศดังเช่นอนุสัญญานี้

2. อนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 ได้มีบทบัญญัติในการป้องกันและคุ้มครองข้อมูลส่วนบุคคลรวมถึงสิทธิมนุษยชน โดยในอรัมภบทของอนุสัญญาได้ยอมรับมาตรการที่สำคัญเกี่ยวกับข้อมูลส่วนบุคคลรวมถึงสิทธิมนุษยชนตามที่ปรากฏในบทบัญญัติของความตกลงต่างๆ รวมถึงองค์กร สถาบันระหว่างประเทศ โดยประเทศที่ลงนามเป็นภาคีสมาชิกจะต้องมีการแสดงออกถึงความสำคัญดังกล่าวเป็นนโยบายระดับประเทศ

3. อนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 เป็นบทบัญญัติที่มีวัตถุประสงค์เฉพาะการกระทำที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ ที่ประกอบด้วยมาตรการป้องกันการกระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ การค้นหาและพิสูจน์พยานหลักฐานที่จำเป็นเกี่ยวกับการดำเนินคดีประเภทนี้

4. อนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 เป็นสิ่งสำคัญที่สามารถสะท้อนให้เห็นถึงกฎหมายที่มีอยู่ของรัฐและมลรัฐต่างๆในประเทศสหรัฐอเมริกา ซึ่งอนุสัญญาดังกล่าวนี้มีลักษณะพิเศษเพราะสามารถสะท้อนให้เห็นถึงกฎหมายและกระบวนการต่างๆในประเทศสหรัฐอเมริกาไม่ว่าจะเป็นกฎหมายสารบัญญัติและกฎหมายสบัญญัติและ

---

[2] Eight Reasons the U.S Should Ratify the Cybercrime Treaty the Convention on Cybercrime[Online].2009, Available from : www.gliif.org/Ratify Now /reason.htm[2009, May 23]

หลักเกณฑ์เกี่ยวกับกฎหมายวิธีพิจารณาความอาญา ทั้งนี้ยังรวมถึงกฎหมายรัฐธรรมนูญ กระบวนการที่ชอบด้วยกฎหมาย และการป้องกันสิ่งที่ไม่เป็นธรรม

5. อนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 นี้เป็นเครื่องมือในการแก้ไขปัญหาเรื่องกระบวนการและกฎหมายขัดกันในเรื่องที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ โดยในอนุสัญญาดังกล่าวได้กำหนดมาตรการที่หลากหลายไม่ว่าจะเป็นหลักเกณฑ์เกี่ยวกับกฎหมายวิธีพิจารณาความอาญา ในส่วนของบทบัญญัติเกี่ยวกับขั้นตอนต่างๆยังได้กำหนดเกี่ยวกับการให้สัตยาบัน การภาคยานุวัติ การแสดงเจตจำนงของรัฐ หรือการสงวนสิทธิในการปฏิบัติตามพันธกรณีภายใต้มาตรการที่อนุสัญญานี้ได้กำหนดไว้ โดยข้อสงวนสิทธิดังกล่าว จะต้องอยู่ภายใต้หลักการพื้นฐานของประเทศนั้นว่าด้วยความสัมพันธ์ระหว่างรัฐบาลกลางและมลรัฐหรือหน่วยอาณาเขตอย่างอื่นในทำนองเดียวกันภายใต้เงื่อนไขที่ว่าประเทศนั้นยังคงสามารถให้ความร่วมมือระหว่างประเทศได้

6. อนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 ได้เรียกร้องให้ประเทศภาคีสมาชิกปฏิบัติตามพันธกรณีที่ประเทศตนมีอยู่ภายใต้การยอมรับเอาข้อตกลงที่เกี่ยวกับทรัพย์สินทางปัญญาไม่ว่าจะเป็น ข้อตกลงว่าด้วยหลักเกณฑ์ที่เกี่ยวข้องกับการค้าในสิทธิแห่งทรัพย์สินทางปัญญา และสนธิสัญญาขององค์การทรัพย์สินทางปัญญาของโลกว่าด้วยลิขสิทธิ์

7. อนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 ได้กำหนดหลักเกณฑ์พื้นฐานเกี่ยวกับขอบเขตอำนาจหน้าที่ในการสืบสวนสอบสวนที่มีผลบังคับใช้นับตั้งแต่เริ่มมีการสื่อสารทางอิเล็กทรอนิกส์ การเก็บรักษาที่รวดเร็วของข้อมูลคอมพิวเตอร์ การเข้าถึง ข้อมูลในส่วนที่เป็นเนื้อหา โดยกระบวนการทั้งหมดจะต้องเป็นกระบวนการที่ชอบด้วยกฎหมายและไม่กระทบต่อนโยบายความเป็นส่วนตัวและข้อมูลส่วนบุคคล

8. อนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 ได้มีการเตรียมการอย่างเหมาะสมโดยผู้เชี่ยวชาญทั่วโลกที่มีประสบการณ์และมีความรู้เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์และยังได้รับการสนับสนุนจากหลายฝ่าย

กระทรวงยุติธรรมของประเทศสหรัฐอเมริกาจึงได้มีการดำเนินการ ดังนี้[3]

---

[3] สุปรียา อภิวัฒนากร. อาชญากรรมทางคอมพิวเตอร์ : ศึกษากรณีการหลอกลวงทางอินเทอร์เน็ต. (วิทยานิพนธ์ปริญญามหาบัณฑิต สาขาวิชานิติศาสตร์ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2545), หน้า 171-173.

1. การให้ความร่วมมือระหว่างองค์กรผู้บังคับใช้กฎหมายในการปราบปรามอาชญากรรมทางคอมพิวเตอร์และอินเทอร์เน็ต โดยเริ่มต้นความร่วมมือในวันที่ 26 กุมภาพันธ์ ค.ศ. 1999 ซึ่งเป็นความร่วมมือระหว่างหน่วยงานของชาติเพื่อประสานงานและสืบสวนสอบสวนเพื่อปราบปรามอาชญากรรมทางคอมพิวเตอร์และอินเทอร์เน็ต ซึ่งมีวัตถุประสงค์หลัก 6 ประการ คือ

1) ศึกษาข้อมูลเกี่ยวกับลักษณะ วิธีการและขอบเขตของอาชญากรรมทางคอมพิวเตอร์และอินเทอร์เน็ต โดยเป็นความร่วมมือกับสมาพันธ์คุ้มครองผู้บริโภคแห่งชาติของสหรัฐอเมริกาในการศึกษาข้อมูลดังกล่าว รวมถึงแนวโน้มของการแพร่หลายและผลกระทบจากอาชญากรรมทางคอมพิวเตอร์และอินเทอร์เน็ตที่จะเกิดขึ้นในอนาคตด้วย

2) พัฒนาและให้คำแนะนำแก่อัยการและเจ้าพนักงานในการบังคับใช้กฎหมาย รวมถึงบุคลากรของรัฐในการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์และอินเทอร์เน็ต โดยจัดให้มีการฝึกอบรมให้ความรู้เฉพาะทางเกี่ยวกับระบบคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตผ่านทาง National Advocacy Center (NAC) ที่จัดฝึกอบรมให้ความรู้ทั้งในระดับพื้นฐานและในระดับสูง นอกจากนี้ยังฝึกอบรมเรื่องดังกล่าวให้กับองค์กรผู้บังคับใช้กฎหมายในแต่ละมลรัฐ เพื่อสามารถนำความรู้ไปป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์และอินเทอร์เน็ตในแต่ละมลรัฐได้อีกด้วย

3) สนับสนุนและพัฒนาในเรื่องการสืบสวนสอบสวน การวิเคราะห์ถึงการกระทำความผิด ตลอดจนการนำตัวผู้กระทำความผิดมาลงโทษ และก่อตั้งศูนย์ร้องเรียนเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์และอินเทอร์เน็ต

4) เสนอแนะและอำนวยความสะดวกให้กับหน่วยงานบังคับใช้กฎหมายระดับท้องถิ่นในการให้ความร่วมมือระหว่างรัฐเกี่ยวกับการสืบสวนสอบสวนคดีอาชญากรรมทางคอมพิวเตอร์

5) สนับสนุนและให้คำแนะนำในการดำเนินคดีเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์และอินเทอร์เน็ต

6) ริเริ่มให้มีการให้ความรู้แก่ประชาชนในการหลีกเลี่ยงการก่ออาชญากรรมทางคอมพิวเตอร์และอินเทอร์เน็ต รวมทั้งวิธีการทางเทคโนโลยีในการป้องกันและขยายมาตรการในการป้องกันและปราบปรามอาชญากรรมดังกล่าวทั้งในหน่วยงานของรัฐและเอกชน

2. การจัดตั้งหน่วยรับเรื่องร้องเรียนเกี่ยวกับการหลอกลวงทางอินเทอร์เน็ต (Internet Fraud Complain Center : IFCC) ซึ่งเป็นความร่วมมือกับ FBI และ National Collar Crime Center เป็นหน่วยงานที่รับเรื่องร้องเรียนให้กับองค์กรที่บังคับใช้กฎหมายของรัฐบาลสหรัฐอเมริกา และองค์กรบังคับใช้กฎหมายในระดับท้องถิ่น นอกจากนี้ยังมีการจัดตั้งหน่วยงานรับเรื่องร้องเรียนเกี่ยวกับการหลอกลวงทางอินเทอร์เน็ตขององค์กรภาคเอกชนอีกด้วย เช่น การก่อตั้ง The National Fraud Information Center (NFIC) ในปี ค.ศ. 1992 โดยสมาคมผู้บริโภคแห่งชาติ (National Consumers League : NCL) ซึ่งถือเป็นหน่วยงานเก่าแก่ในการคุ้มครองผู้บริโภคของประเทศสหรัฐอเมริกา ทำงานในลักษณะองค์กรที่ไม่แสวงหากำไร เพื่อปราบปรามการหลอกลวงทุกประเภท ซึ่งรวมถึงการหลอกลวงทางอินเทอร์เน็ตด้วย[4]

3.1.2.1 มาตรการทางสารบัญญัติ

ภายหลังจากที่มีการลงนามในอนุสัญญาดังกล่าวแล้วพันธกรณีที่มีต่อประเทศสหรัฐอเมริกาคือต้องมีการกำหนดการกระทำความผิดอาชญากรรมทางคอมพิวเตอร์ให้เป็นความผิดทางอาญาตามกฎหมายภายในประเทศ และมีการกำหนดโทษให้ได้สัดส่วนเหมาะสมกับการกระทำความผิดและความเสียหายที่เกิดขึ้น ประเทศสหรัฐอเมริกาก็ได้ดำเนินการเกี่ยวกับมาตรการทางสารบัญญัติที่เกี่ยวกับกฎหมายเทคโนโลยีสารสนเทศ ผู้เขียนขอยกตัวอย่างกฎหมายเทคโนโลยีสารสนเทศของประเทศสหรัฐอเมริกาซึ่งเป็นกฎหมายของรัฐบาลกลาง[5] เช่น

1. กฎหมายกลฉ้อฉลและการกระทำที่ไม่ถูกต้องทางคอมพิวเตอร์
2. กฎหมายสิทธิทางการศึกษาของครอบครัวและความเป็นส่วนตัว
3. กฎหมายรัฐบาลกลางเกี่ยวกับความเป็นส่วนตัว
4. กฎหมายความเป็นส่วนตัวในการสื่อสารอิเล็กทรอนิกส์
5. กฎหมายการป้องกันความเป็นส่วนตัวในการหาคู่ทางคอมพิวเตอร์
6. กฎหมายคุ้มครองความเป็นส่วนตัวของผู้ขับขี่

---

[4] เรื่องเดียวกัน, หน้า 173.

[5] ศรีศักดิ์ จามรมาน, สู่มิติใหม่แห่งการเรียนรู้ เอกสารประกอบการอบรมสำหรับสมาชิก NTU หลักสูตร การบริหารจัดการสมัยใหม่ เรื่อง ความผิดตามพ.ร.บ.คอมพิวเตอร์ ที่ทุกคนควรทราบ, ธนาคารกรุงเทพ จำกัด มหาชน, 12 พฤศจิกายน 2552. หน้า 4.

7. กฎหมายเกี่ยวกับการประกันสุขภาพและภาระความรับผิดชอบ

8. กฎหมายคุ้มครองความเป็นส่วนตัวทางวีดีทัศน์

9. กฎหมายระดับรัฐบาลกลางยับยั้งการขโมยข้อมูลส่วนบุคคล

10. กฎหมายเกี่ยวกับอีเมล์ขยะ

11. กฎหมายเกี่ยวกับการทวงหนี้อย่างยุติธรรม

12. กฎหมายบริการการเงินสมัยใหม่ หรือ แกรมม์ ลีช บลิเลย์

13. กฎหมายเกี่ยวกับการคุ้มครองความเป็นส่วนตัวของเด็ก

14. กฎหมายรายงานเครดิตอย่างยุติธรรม

15. กฎหมายคุ้มครองผู้ใช้โทรศัพท์

16. กฎหมายการฉ้อโกงเกี่ยวกับอุปกรณ์การเข้าถึง

ส่วนกฎหมายระดับมลรัฐ มี 26 มลรัฐที่ได้มีการดำเนินการเกี่ยวกับมาตรการทางสารบัญญัติที่เกี่ยวกับกฎหมายเทคโนโลยีสารสนเทศ คือ อลาบามา อลาสกา อริโซนา แคลิฟอร์เนีย โคโลราโด คอนเน็กติกัต เดลาแวร์ ฟลอริดา จอร์เจีย ฮาวาย ไอดาโฮ อิลลินอยส์ อินเดียนา ไอโอวา แมรี่แลนด์ มินเนโซตา นิวเจอร์ซีย์ นิวเม็กซิโก นิวยอร์ค นอร์ทแคโรไลนา โอเรกอน เท็กซัส เวอร์จิเนีย วอชิงตัน เวสต์เวอร์จิเนีย และวิสคอนซิน

จากกฎหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศดังกล่าวผู้เขียนจึงทำการศึกษาเฉพาะกฎหมายที่สอดคล้องกับบทบัญญัติในอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 ที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์และอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ การใช้คอมพิวเตอร์กระทำความผิด เพื่อให้ทราบถึงแนวทางในการกำหนดคำนิยามว่าสอดคล้องและเป็นไปในทิศทางที่ไม่ก่อให้เกิดอุปสรรคหากประเทศสหรัฐอเมริกาต้องปฏิบัติตามพันธกรณีที่เกิดจากการลงนามและให้สัตยาบันในอนุสัญญาดังกล่าว ซึ่งกฎหมายดังกล่าวคือ

ก. กฎหมายเกี่ยวกับการฉ้อฉลและการกระทำที่ไม่ถูกต้องเกี่ยวกับคอมพิวเตอร์ (Computer Fraud and Abuse Act of 1984 : CFAA)

กฎหมาย Computer Fraud and Abuse Act ฉบับปัจจุบันฉบับนี้ได้กำหนดฐานความผิดเกี่ยวกับการฉ้อฉลและการกระทำความผิดที่เกี่ยวเนื่องกับคอมพิวเตอร์ไว้ใน Title 18 U.S.C. § 1030 โดยกำหนดฐานความผิดไว้ 7 ฐาน ซึ่งกฎหมายนี้ใช้ดำเนินคดีกับบุคคลซึ่งมีเจตนาในเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต และคอมพิวเตอร์ดังกล่าวเป็นคอมพิวเตอร์อยู่ในการปกป้องของรัฐบาลสหรัฐอเมริกา (Title 18 U.S.C. § 1030 (e)(2))[6] ทั้งนี้ผู้เขียนได้ศึกษาโดยเทียบเคียงกับมาตรการทางด้านต่างๆในอนุสัญญาดังนี้

1. คำจำกัดความและความหมาย

1). การกระทำโดยปราศจากอำนาจในการเข้าถึง หรือเกินขอบอำนาจที่กำหนด (Title 18 U.S.C. § 1030 (e)(6)) การกระทำความผิดตามกฎหมายนี้ได้มีหลายความผิดที่กำหนดให้มีถ้อยคำเช่นนี้ คำว่า ปราศจากอำนาจในการเข้าถึง (without authorization) ถ้อยคำดังกล่าวนี้ไม่ได้มีคำจำกัดความไว้ในกฎหมายแต่พบได้จากคำพิพากษาของศาลซึ่งยากที่จะอธิบาย เช่น กรณีถือได้ว่าได้รับอนุญาตให้เข้าถึงระบบคอมพิวเตอร์ แม้ว่าการเข้าถึงดังกล่าวละเมิดเงื่อนไขของข้อตกลงมีผลผูกพันผู้ใช้งานระบบ ที่ให้อนุญาตให้ผู้ใช้งานสามารถเข้าถึงระบบคอมพิวเตอร์ได้[7]

และคำว่า เกินขอบอำนาจที่กำหนด ถ้อยคำดังกล่าวนี้ได้กำหนดไว้ในกฎหมายหมายถึง การได้รับอนุญาตให้เข้าถึงคอมพิวเตอร์ หรือได้รับอนุญาตให้ใช้งานคอมพิวเตอร์ แต่ไม่ได้รวมถึงการเข้าถึงเพื่อให้ได้มาซึ่งข้อมูลในคอมพิวเตอร์หรือแก้ไขข้อมูลในคอมพิวเตอร์ โดยผู้ที่เข้าถึงดังกล่าวไม่มีสิทธิในการได้มาซึ่งข้อมูลและไม่มีสิทธิในการแก้ไขข้อมูลดังกล่าว (Title 18 U.S.C. § 1030 (e)(6))

จากการคาดการณ์ของสภาคองเกรสว่าผู้ที่กระทำเกินอำนาจในการเข้าถึงคอมพิวเตอร์มีแนวโน้มที่จะเป็นบุคคลภายในองค์กร และในขณะที่บุคคลผู้กระทำโดยปราศจากอำนาจนั้นมีแนวโน้มที่จะเป็นบุคคลภายนอกองค์กร เป็นผลให้สภาคองเกรสจำกัดพฤติการณ์ของ

---

[6] โครงสร้างทางกฎหมายสหรัฐอเมริกา ด้านการก่อการร้ายและอาชญากรรมทางไซเบอร์[ออนไลน์], 2553, แหล่งที่มา: http://www.police.go.th[2553, มกราคม 11]

[7] คดี EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582 n.10 (1st Cir. 2001) (dicta); see also SecureInfo Corp. v. Telos Corp., 387 F. Supp. 2d 593 (E.D. Va. 2005) : holding that defendants had authorization to use a computer system even though such access violated the terms of a license agreement binding the user who provided them with access to the system อ้างถึงใน Chapter 1 Computer Fraud and Abuse Act[Online], Available from : http://www.cybercrime.gov/ccmanual/01ccma.pdf[2010, January 11]

คนในองค์กรว่า หมายถึง บุคคลที่ได้รับอนุญาตให้เข้าถึงไม่ถือว่าละเมิด แต่ถ้าหากบุคคลนั้นตั้งใจจะทำให้เกิดความเสียหายต่อคอมพิวเตอร์ไม่ใช่เพียงแค่การกระทำโดยไม่เจตนาหรือโดยประมาทถือเป็นการกระทำความผิด (Title 18 U.S.C. § 1030 (a)(1)-(5))

ในทางตรงข้าม บุคคลภายนอก อาจต้องได้รับโทษหากทำการเข้าถึงคอมพิวเตอร์โดยเจตนา หรือความเสียหายอย่างอื่นที่เกิดจากการกระทำของตน เช่น กรณีที่มีการพบว่าพนักงานสรรพากรมีการใช้อำนาจเกินขอบเขตที่กำหนด โดยเข้าถึงระบบคอมพิวเตอร์เพื่อดูข้อมูลผู้เสียภาษี หรือเพื่อวัตถุประสงค์ส่วนบุคคล[8] และกรณีของผู้กระทำความผิดชาวรัสเซียที่ทำการเข้าถึงข้อมูลลูกค้าของบริษัทชาวอเมริกันโดยไม่ได้รับอนุญาต[9] จึงเป็นเรื่องยากที่ให้คำจำกัดความ เนื่องจากการที่บุคคลที่ได้รับอนุญาตตามกฎหมายให้เข้าถึงคอมพิวเตอร์ว่ามีการกระทำเกินขอบอำนาจในการเข้าถึงหรือไม่

2). คอมพิวเตอร์ซึ่งอยู่ในการปกป้องคุ้มครองของรัฐบาลสหรัฐอเมริกา (Title 18 U.S.C. § 1030 (e)(2)) เป็นถ้อยคำที่กำหนดไว้ในกฎหมาย ครอบคลุมถึงเครื่องคอมพิวเตอร์ที่ใช้ในการค้าระหว่างรัฐหรือการค้ากับต่างประเทศซึ่งได้ถูกระบุไว้โดยรัฐบาลว่าเป็นคอมพิวเตอร์ที่เกี่ยวข้องกับการพาณิชย์ระหว่างมลรัฐและคอมพิวเตอร์ของรัฐบาลกลางและสถาบันการเงิน

ตั้งแต่ปี ค.ศ. 1996 สภาคองเกรสได้ให้นิยามว่า คอมพิวเตอร์นั้นเป็นคอมพิวเตอร์ที่ใช้งานโดยรัฐบาลกลางหรือสถาบันการเงินซึ่งจะใช้ในการค้าระหว่างรัฐหรือระหว่างประเทศ* จากนิยามดังกล่าวนี้ยังมีความไม่ชัดเจนว่า ได้หมายความรวมถึง กรณีที่ผู้กระทำความผิดอยู่ในประเทศสหรัฐอเมริกาที่ได้มีการกระทำความผิดโจมตีต่อระบบคอมพิวเตอร์ที่อยู่ต่างประเทศด้วยหรือไม่ นอกจากนี้ความหมายนี้ไม่สามารถใช้ได้กับกรณีที่บุคคลซึ่งอยู่ใน

---

[8] คดี United States v. Czubinski, 106 F.3d 1069 (1st Cir. 1997) : where an Internal Revenue Service employee was found to have exceeded his authorized access to IRS computer systems when he looked at taxpayer records for personal purposes, อ้างถึงใน Chapter 1 Computer Fraud and Abuse Act[Online], Available from : http://www.cybercrime.gov/ccmanual/01ccma.pdf[2010, January 11]

[9] คดี United States v. Ivanov, 175 F. Supp. 2d 367 (D. Conn. 2001) : where a Russian intruder broke into an American company's customer databases and was found to have acted without authorization, อ้างถึงใน Chapter 1 Computer Fraud and Abuse Act[Online], Available from : http://www.cybercrime.gov/ccmanual/01ccma.pdf[2010, January 11]

* Title 18 U.S.C. 1030(e)(2) (1996) protected computer as a computer used by the federal government or a financial institution, or one which is used in interstate or foreign commerce.

ต่างประเทศแต่ได้ทำการเจาะระบบคอมพิวเตอร์โดยได้กำหนดเส้นทางการสื่อสารผ่านทางประเทศสหรัฐอเมริกาไปยังอีกประเทศหนึ่งหรือไม่

2. **ฐานความผิดและองค์ประกอบความผิด**

จากการที่อนุสัญญาให้ประเทศภาคีกำหนดการกระทำความผิดอาชญากรรมทางคอมพิวเตอร์ทั้ง 9 ฐาน เป็นความผิดทางอาญาตามกฎหมายภายในประเทศ ผู้เขียนเห็นว่ามาตรการในข้อนี้ถือเป็นสิ่งสำคัญของการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ซึ่งประเทศภาคีจะต้องดำเนินการโดยเร่งด่วน ซึ่งประเทศสหรัฐอเมริกาได้ดำเนินการกำหนดการกระทำความผิดดังนี้

1). การเข้าถึงคอมพิวเตอร์ทำให้ได้มาซึ่งข้อมูลความมั่นคงแห่งชาติ ความผิดนี้ได้ถูกกำหนดไว้ใน (Title 18 U.S.C. § 1030 (a)(2)) โดยกำหนดให้มีการลงโทษการกระทำความผิดเกี่ยวกับการเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจในการเข้าถึงหรือเกินขอบอำนาจที่กำหนดไว้ในการเข้าถึงดังกล่าว ทำให้ได้มาซึ่งข้อมูลความมั่นคงของชาติ โดยมีเจตนาให้หรือพยายามให้ข้อมูลแก่ที่ผู้รับที่ไม่ได้รับอนุญาต หรือโดยมีเจตนาในการเก็บรักษาข้อมูลนั้นไว้ โดยมีองค์ประกอบความผิด ดังนี้

เจตนาในการเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจในการเข้าถึงหรือเกินขอบอำนาจที่กำหนดไว้ การกระทำละเมิดในส่วนนี้ต้องทำการพิสูจน์จากข้อเท็จจริงว่าจำเลยรู้ถึงการเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจในการเข้าถึงหรือเกินขอบอำนาจที่กำหนดไว้ดังกล่าว กรณีดังกล่าวครอบคลุมทั้งกรณีของบุคคลที่ไม่ได้รับอนุญาตให้เข้าถึงคอมพิวเตอร์ที่มีข้อมูลความมั่นคงแห่งชาติ และกรณีบุคคลภายในที่มีการจำกัดสิทธิในการจัดการการเข้าถึงคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ ซึ่งขอบเขตของคำว่าอนุญาต ขึ้นอยู่กับข้อเท็จจริงเป็นกรณีไป อย่างไรก็ตาม ไม่มีประโยชน์ที่จะพิจารณาว่าคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ที่มีข้อมูลความมั่นคงของชาตินั้นเป็นข้อมูลปกติและมีการรักษาความปลอดภัยและควบคุมการเข้าถึงหรือไม่[10]

การได้มาซึ่งข้อมูลความมั่นคงแห่งชาติ หมายถึง ข้อมูลที่ได้มาที่จะถือเป็นความผิดจะต้องเป็นข้อมูลความมั่นคงของชาติ ข้อมูลที่ได้รับพิจารณาจากรัฐบาลสหรัฐอเมริกาตามคำสั่งของผู้บริหารระดับสูง หรือข้อมูลที่ไม่ต้องการให้มีการเปิดเผยโดยไม่ได้รับอนุญาตเพื่อเหตุผลในการป้องกันประเทศหรือความสัมพันธ์ระหว่างประเทศ หรือข้อมูลที่จำกัดการเข้าถึง

---

[10] Chapter 1 Computer Fraud and Abuse Act[Online]. Available from : http://www.cybercrime.gov/ccmanual/01ccma.pdf[2010, January 11]

ข้อมูลที่ได้มาอาจก่อให้เกิดผลร้ายต่อความมั่นคงของชาติและความปลอดภัยของประชาชน องค์ประกอบความผิดในข้อนี้อาจต้องทำการพิสูจน์จากข้อเท็จจริงว่าผู้กระทำความผิดมีเหตุผลอันควรเชื่อได้ว่าข้อมูลที่ได้รับมาดังกล่าวเป็นข้อมูลที่ใช้ในการรักษาความปลอดภัยแห่งชาติ หรือใช้ในการก่อให้เกิดผลร้ายต่อความมั่นคงของชาติ หรือก่อให้เกิดผลร้ายต่อผลประโยชน์ของต่างประเทศ และอาจต้องดูจากข้อเท็จจริงที่ว่าข้อมูลดังกล่าวเป็นข้อมูลที่เกี่ยวกับการรักษาความปลอดภัยแห่งชาติประเภทใด

การกระทำโดยจงใจหรือมีเจตนาในการติดต่อสื่อสาร การส่งข้อมูล การถ่ายทอดข้อมูล หรือการยึดถือข้อมูลไว้เพื่อตน องค์ประกอบความผิดในข้อนี้อาจต้องทำการพิสูจน์จากข้อเท็จจริงว่าผู้กระทำความผิดจงใจที่จะกระทำการติดต่อสื่อสาร ส่งข้อมูล ถ่ายทอดข้อมูลความมั่นคงแห่งชาติ หรือมีเจตนาในการเก็บรักษาข้อมูลไว้แทนผู้อื่น เพื่อกระทำการส่งต่อไปตามเจตนาของผู้รับ ซึ่งการกระทำที่จงใจหรือไม่นั้นอาจพิสูจน์หลักฐานที่แสดงให้เห็นว่าจำเลยกระทำการใดๆ เช่น จงใจติดต่อสื่อสาร จงใจส่งหรือการถ่ายทอดข้อมูลการรักษาความปลอดภัยแห่งชาติหรือ ทำให้ข้อมูลถูกสื่อสาร ถูกส่ง หรือถ่ายทอดไปยังบุคคลใดที่ไม่มีสิทธิจะรับข้อมูลดังกล่าว การพยายามติดต่อสื่อสาร พยายามส่งหรือการพยายามถ่ายทอดข้อมูลการรักษาความปลอดภัยแห่งชาติหรือพยายามทำให้ข้อมูลนั้นถูกสื่อสาร ถูกส่ง หรือถ่ายทอดไปยังบุคคลใดที่ไม่มีสิทธิจะรับข้อมูลดังกล่าว หรือการมีเจตนาที่จะเก็บข้อมูลความมั่นคงของชาติและไม่นำส่งข้อมูลดังกล่าวให้กับเจ้าหน้าที่หรือพนักงานเจ้าหน้าที่ที่มีสิทธิได้รับข้อมูลดังกล่าวตามการปฏิบัติตามหน้าที่

2). การเข้าถึงคอมพิวเตอร์ทำให้ได้มาซึ่งข้อมูลสถาบันการเงิน หรือหน่วยงานของรัฐ (Title 18 U.S.C. § 1030 (a)(2)) การกระทำนี้เป็นการกระทำความผิดอาญาที่กระทำต่อข้อมูลและคอมพิวเตอร์ซึ่งผู้กระทำความผิดอาจกระทำความผิดมากกว่า 1 ฐานความผิด เช่น การเข้าถึงคอมพิวเตอร์ของพนักงานเจ้าหน้าที่ กฎหมายไม่ได้กำหนดหลักเกณฑ์ในการพิจารณาว่าการกระทำใดเป็นการเข้าถึง ซึ่งอาจต้องยอมรับความจริงที่ว่าการละเมิดสิทธิส่วนบุคคลในข้อนี้ไม่ได้นำไปสู่ความสูญเสียทางด้านการเงิน แต่การที่ประเทศสหรัฐอเมริกาได้กำหนดให้มีการคุ้มครองข้อมูลดังกล่าวนี้อาจเหตุผลสมควรกำหนดขึ้นเพื่อเป็นการปกป้องประเทศ การเข้าถึงข้อมูลที่เป็นความลับหากไม่ได้รับอนุญาต เช่น ทำการดาวน์โหลดข้อมูลบุคคลสำคัญของบริษัทหรือรวบรวมข้อมูลส่วนตัวจากศูนย์ข้อมูลอาชญากรรมแห่งชาติ ทั้งการละเมิดข้อมูลส่วนบุคคลจึงเป็นเรื่องยากที่จะประเมินค่าความเสียหายเป็นตัวเงิน มูลค่าของข้อมูลที่ได้รับในการกระทำความผิดต่างหากที่เป็นสิ่งสำคัญเมื่อต้องการระบุว่าการกระทำความผิดดังกล่าวเป็นความผิดอาญานั้นร้ายแรงหรือไม่เพียง

การกระทำตามที่กำหนดนี้ต้องกระทำโดยปราศจากอำนาจในการเข้าถึง เพื่อให้ได้มาซึ่งข้อมูล คำว่า เพื่อให้ได้มาซึ่งข้อมูล เป็นถ้อยคำที่มีความหมายกว้างมาก อาจรวมถึงการแสดงข้อมูลโดยไม่ต้องมีการดาวน์โหลดหรือคัดลอกข้อมูลดังกล่าวก็ได้ มีคำพูดที่ว่า ข้อมูลอิเล็กทรอนิกส์นั้นสามารถเก็บไว้ได้ไม่เพียงโดยการขโมยทางกายภาพเท่านั้น[11] เพียงแค่การเก็บข้อมูลก็ถือเป็นความผิดตามที่กำหนดซึ่งเรียกว่า การกระทำความผิดเกี่ยวกับคอมพิวเตอร์เพื่อให้ได้มาซึ่งข้อมูล

คำว่า ข้อมูลที่เป็นความผิดตามที่กฎหมายกำหนดนี้ ต้องเป็นทรัพย์สินที่ไม่มีรูปร่างหรือไม่ เห็นได้จากคำตัดสินของศาลอุทธรณ์ ในคดีของ United States v. Brown ที่ว่า ทรัพย์สินทางปัญญาถือได้ว่าเป็นทรัพย์สินที่ไม่มีรูปร่าง เช่น โปรแกรมคอมพิวเตอร์ ไม่ได้เป็นสินค้าหรือบริการที่สามารถขโมยหรือแปลงได้[12] จากความสับสนในส่วนนี้สภาคองเกรสได้มีการแก้ไขปัญหาดังกล่าว โดยได้กำหนด ให้การขโมยข้อมูลที่ไม่มีรูปร่างโดยไม่ได้รับอนุญาตด้วยวิธีการใช้คอมพิวเตอร์ในการกระทำความผิด ถือเป็นความผิดในทำนองเดียวกับการโจรกรรมสินค้าทางกายภาพ

ข้อมูลสถาบันการเงิน หรือ สถาบันคุ้มครองผู้บริโภค ข้อมูลที่ได้มาตามมาตรานี้หมายถึงข้อมูลที่เกี่ยวข้องกับการรายงานข้อมูลเครดิตของลูกค้าสถาบันการเงิน ซึ่งเป็นเรื่องยากที่รัฐบาลต้องแสดงให้เห็นว่าผู้กระทำความผิดรู้และเจตนาในการกระทำความผิดโดยไม่คำนึงถึงสิทธิของผู้บริโภค[13]

ข้อมูลของหน่วยงานรัฐบาลสหรัฐอเมริกา เป็นที่น่าสังเกตว่าข้อมูลของบริษัทเอกชนที่ทำงานในฐานะผู้รับจ้างของรัฐบาล อยู่ในความหมายของคำว่าหน่วยงานของ

---

[11] America Online, Inc. v. National Health Care Discount, Inc., 121 F. Supp. 2d 1255 (N.D. Iowa 2000). : Information stored electronically can be obtained not only by actual physical theft, but by "mere observation of the data." อ้างถึงใน Chapter 1 Computer Fraud and Abuse Act[Online]. Available from : http://www.cybercrime.gov/ccmanual/01ccma.pdf[2010, January 11]

[12] United States v. Brown, 925 F.2d 1301, 1308 (10th Cir. 1991) : the appellate court held that purely intangible intellectual property, such as a computer program, อ้างถึงใน Chapter 1 Computer Fraud and Abuse Act[Online]. Available from : http://www.cybercrime.gov/ccmanual/01ccma.pdf[2010, January 11]

[13] Ausherman v. Bank of America Corp., 352 F.3d 896 at 900 n.4 (4th Cir. 2003) : To prove willfulness under the FCRA, the government must show that the defendant knowingly and intentionally committed an act in conscious disregard for the rights of a consumer., อ้างถึงใน Chapter 1 Computer Fraud and Abuse Act[Online]. Available from : http://www.cybercrime.gov/ccmanual/01ccma.pdf[2010, January 11]

รัฐบาลหรือไม่ ซึ่งยังไม่ได้มีคำพิพากษาของศาลใดตัดสินในเรื่องดังกล่าว อย่างไรก็ตาม มีข้อโต้แย้งในเรื่องดังกล่าวว่าการที่กฎหมายกำหนดเช่นนี้มีวัตถุประสงค์ที่จะกำหนดให้ครอบคลุมกรณีดังกล่าวหรือไม่ รวมถึงการอนุญาตให้มีการฟ้องร้องคดีอาญาเกี่ยวกับการบุกรุกเข้าสู่ระบบคอมพิวเตอร์ของทางราชการและระบบคอมพิวเตอร์เอกชน ถ้าพฤติกรรมของบริษัทเอกชนดังกล่าวแสดงผลว่าถูกใช้โดยหรือใช้เพื่อรัฐบาลประเทศสหรัฐอเมริกา

3). การกระทำความผิดโดยการบุกรุกเข้าไปในระบบคอมพิวเตอร์ของรัฐบาล (Title 18 U.S.C. § 1030 (a)(3)) การบุกรุกดังกล่าวกระทำโดยบุคคลภายนอกที่ทำการบุกรุกเข้าไปในระบบคอมพิวเตอร์ของรัฐบาลแม้ว่าจะไม่ได้รับข้อมูลคอมพิวเตอร์จากการบุกรุกดังกล่าว แต่ตามวัตถุประสงค์คือต้องการบังคับใช้กับบุคคลภายนอกที่ไม่ได้เกี่ยวข้องโดยเป็นพนักงานเจ้าหน้าที่ของรัฐ[14] ซึ่งการบุกรุกดังกล่าวต้องเป็นกระทำโดยเจตนาและปราศจากอำนาจ

ทั้งนี้ การบุกรุกที่ถือเป็นความผิดต้องเป็นการกระทำต่อคอมพิวเตอร์ของรัฐ ประกอบด้วยคอมพิวเตอร์ทั้งหมดของรัฐบาลสหรัฐอเมริกา หมายถึงต้องสามารถควบคุม โดยกระทรวงหรือหน่วยงานของสหรัฐอเมริกา ใช้งานเพื่อประโยชน์ของรัฐ หรืออย่างน้อยที่สุดต้องใช้โดยหรือใช้เพื่อรัฐบาลสหรัฐอเมริกาในบางหน้าที่ เช่น หากประเทศสหรัฐอเมริกาได้รับบัญชี ในเซิร์ฟเวอร์ของบริษัทเอกชน ก็อยู่ในความหมายที่ว่า ใช้โดยรัฐบาลสหรัฐอเมริกา แม้เซิร์ฟเวอร์ดังกล่าวจะไม่เป็นของสหรัฐอเมริกา เช่นในกรณีบริษัทเอกชนที่ทำงานในฐานะผู้รับจ้างของรัฐบาล

การบุกรุกดังกล่าวต้องส่งผลกระทบต่อการใช้งานคอมพิวเตอร์ของรัฐ การบุกรุกเครือข่ายคอมพิวเตอร์เกือบทุกประเภทล้วนมีผลกระทบต่อการใช้งานคอมพิวเตอร์ เนื่องจากการบุกรุกดังกล่าวอาจมีผลต่อความลับและความสมบูรณ์ของข้อมูลของรัฐบาล เป็นที่น่าสังเกตว่าผู้กระทำความผิดโดยเข้าถึงข้อมูลระบบคอมพิวเตอร์และผู้กระทำความผิดโดยการบุกรุกเพื่อทำให้คอมพิวเตอร์ได้รับความเสียหาย ไม่จำเป็นต้องแสดงให้เห็นว่าการกระทำของผู้เข้าถึงและผู้บุกรุกดังกล่าวเป็นผลร้ายกระทบต่อกระบวนการทำงานของรัฐ เพราะเพียงแค่มีการเข้าถึงและมีการบุกรุกเข้าไปในคอมพิวเตอร์ของรัฐบาลก็ถือเป็นความผิด

4). การเข้าถึงคอมพิวเตอร์เพื่อการฉ้อโกงและได้มาซึ่งสิ่งมีค่า (Title 18 U.S.C. § 1030 (a)(4)) การกระทำความผิดนี้ผู้กระทำต้องรู้ถึงการเข้าถึงคอมพิวเตอร์ดังกล่าวว่าได้กระทำโดยไม่ได้รับอนุญาตหรือเกินขอบอำนาจ และมีเจตนาในการฉ้อโกง

---

[14] Prosecuting Computer Crimes, อ้างถึงใน Chapter 1 Computer Fraud and Abuse Act[Online], Available from : http://www.cybercrime.gov/ccmanual/01ccma.pdf[2010,. January 11]

ในกฎหมายไม่ได้มีการกำหนดนิยามของคำว่า การรู้ถึงและมีเจตนาในการฉ้อโกง ขึ้นอยู่กับศาลว่าจะตีความอย่างไร ในทางหนึ่งศาลอาจตีความว่า เจตนาในการฉ้อโกงว่าต้องมีการพิสูจน์ตามกฎหมายทั่วไป[15] ในอีกทางหนึ่ง ศาลอาจกำหนดให้มีความหมายกว้างขึ้นและให้แสดงหลักฐานการกระทำความผิดหรือความไม่สุจริตให้เพียงพอ ศาลตีความคำว่าเจตนาในการฉ้อโกงซึ่งมีความหมายกว้างมากในคดีแพ่งคดีหนึ่งว่า เป็นการกระทำที่ไม่ถูกต้องซึ่งไม่จำต้องพิสูจน์องค์ประกอบความผิดฐานฉ้อโกงตามกฎหมายทั่วไป[16] คดีนี้โจทก์ระบุถึงสาเหตุที่พอเพียงโดยกล่าวหาว่าจำเลยมีส่วนร่วมในการทุจริตเพื่อรับข้อมูลที่เป็นความลับของโจทก์เท่านั้น

การกระทำที่เป็นการฉ้อโกงต้องมีการกระทำความผิดต่อคอมพิวเตอร์ที่มีการป้องกันเพื่อให้ได้รับสิ่งมีค่าจากอีกบุคคลหนึ่ง ซึ่งสภาคองเกรสได้ระบุไว้ว่า สิ่งที่ต้องการกำหนดตามอนุมาตรานี้คือ รู้และมีเจตนาฉ้อโกง ซึ่งมีมาตรฐานเหมือนกับที่กำหนดไว้ใน Title 18 U.S.C. § 1029 เกี่ยวกับการฉ้อโกงบัตรเครดิต แต่ไม่มีรายงานเกี่ยวกับคำว่าฉ้อโกงใน Title 18 U.S.C. § 1029[17]

การกระทำความผิดต้องเจตนาในการฉ้อโกง โดยต้องมีการเข้าถึงคอมพิวเตอร์โดยไม่ได้รับอนุญาตหรือเข้าถึงเกินขอบอำนาจ และสามารถใช้การเข้าถึงดังกล่าวเพื่อการฉ้อโกงในหลายกรณี เช่น กรณีที่ผู้กระทำความผิดทำการเปลี่ยนแปลง หรือลบข้อมูลในเครื่องคอมพิวเตอร์และได้รับสิ่งมีค่าตอบแทนจากบุคคลที่ถูกหลอกลวง หรือกรณีที่ผู้กระทำผิดได้รับข้อมูลจากคอมพิวเตอร์และหลังจากนั้นก็มีการใช้ข้อมูลดังกล่าวเพื่อกระทำการฉ้อโกง หรือกรณีที่

---

[15] United States v. Kiefer, 228 F.2d 448 (D.C. Cir. 1955) : The elements of common law fraud are: "(1) a false representation (2) in reference to a material fact (3) made with knowledge of its falsity (4) and with intent to deceive (5) with action taken in reliance upon the representation.", อ้างถึงใน Chapter 1 Computer Fraud and Abuse Act[Online], Available from : http://www.cybercrime.gov/ccmanual/01ccma.pdf[2010, January 11]

[16] Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1123 (W.D. Wash. 2000) : In that case, the court favored an expansive interpretation of "intent to defraud." In denying the defendant's motion to dismiss, the court held that the word "fraud" as used in section 1030(a)(4) simply means "wrongdoing" and does not require proof of the common law elements of fraud, อ้างถึงใน Chapter 1 Computer Fraud and Abuse Act[Online], Available from : http://www.cybercrime.gov/ccmanual/01ccma.pdf[2010, January 11]

[17] Prosecuting Computer Crimes, อ้างถึงใน Chapter 1 Computer Fraud and Abuse Act[Online], Available from : http://www.cybercrime.gov/ccmanual/01ccma.pdf[2010, January 11]

ใช้คอมพิวเตอร์ในการผลิตเอกสารปลอมเพื่อใช้ในการฉ้อโกง เช่น การแก้ตัวเลขในสลากกินแบ่งแล้วนำไปรับเงินรางวัล[18]

ทั้งนี้ การกระทำความผิดโดยใช้คอมพิวเตอร์จะต้องเชื่อมโยงโดยตรงกับเจตนาในการฉ้อโกง เพื่อได้มาซึ่งสิ่งมีค่า อาจหมายถึง เงินสด หรือการได้รับสินค้าและการบริการที่ดี ซึ่งทั้งสองกรณีนี้ยากที่จะเกิดขึ้นเมื่อผู้กระทำความผิดได้รับเพียงประโยชน์จากการใช้เครื่องคอมพิวเตอร์และได้รับเพียงข้อมูลจากเครื่องคอมพิวเตอร์ เช่น การใช้คอมพิวเตอร์ในฐานะสิ่งมีค่า เนื่องจากประโยชน์ของเครื่องคอมพิวเตอร์เป็นสิ่งที่มีค่าแต่องค์ประกอบข้อนี้ได้กำหนดให้เพียงมูลค่าที่เกิดจากการใช้งานที่มีค่าใช้จ่ายในช่วงเวลา 1 ปี มากกว่า 5000 ดอลลาร์ ซึ่งเงื่อนไขนี้ค่อนข้างยากที่จะพิจารณา แต่ถือได้ว่าเป็นเรื่องปกติของเจ้าของคอมพิวเตอร์ที่มีรายได้จากการที่ให้เช่าคอมพิวเตอร์และโปรแกรมคอมพิวเตอร์ การสนับสนุนให้ใช้งานคอมพิวเตอร์ที่ทันสมัยและราคาแพงบ่อยๆอาจทำให้ผู้ให้บริการหรือเจ้าของคอมพิวเตอร์ได้รับการคุ้มครองตามหลักเกณฑ์ที่กฎหมายกำหนดได้

ฐานข้อมูลหรือข้อมูลคอมพิวเตอร์ ในฐานะที่เป็นสิ่งมีค่า นอกเหนือจากการใช้งานคอมพิวเตอร์ที่ได้กำหนดจำนวนเงินต่ำสุด แต่ฐานข้อมูลหรือข้อมูลคอมพิวเตอร์บางประเภทก็ไม่ได้มีค่าพอที่จะมีคุณสมบัติเช่นว่า เจตนาในการเข้าถึงข้อมูลคอมพิวเตอร์ของบุคคลอื่นแต่ได้รับข้อมูลน้อยมาก โทษที่ได้รับจึงควรจะเป็นเพียงแค่การบุกรุกหรือเข้าถึงแบบง่ายๆ ผู้เขียนให้ข้อสังเกตว่าหากข้อมูลดังกล่าวที่ได้รับมาเป็นเพียง User Name ก็ไม่อาจนับเป็นสิ่งที่มีค่าหรือไม่

5). การทำให้เสียหายซึ่งคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ (Title 18 U.S.C. § 1030 (a)(5)) การกระทำความผิดในลักษณะนี้สามารถก่อให้เกิดอันตรายกับคอมพิวเตอร์ได้ในหลากหลายวิธี เช่น การเข้าถึงคอมพิวเตอร์และทำการส่งคำสั่งให้ลบข้อมูลในระบบคอมพิวเตอร์ดังกล่าว หรือสั่งให้ปิดเครื่องคอมพิวเตอร์ หรือที่เรียกว่า การโจมตีโดยการปฏิเสธการให้บริการ หรือในกรณีที่ผู้ใช้งานได้รับข้อมูลที่ไร้ประโยชน์จำนวนมากทำให้ไม่สามารถเข้าถึงข้อมูลที่ตนเองต้องการได้ กรณีของไวรัสหรือเวิร์มที่สามารถใช้งานเกี่ยวกับการสื่อสารที่มีการใช้เครือข่ายขององค์กรเมื่อเข้าไปถึงขั้นตอนของการรักษาความปลอดภัยของคอมพิวเตอร์ก็สามารถลบข้อมูลได้ การทำการติดตั้งซอฟร์แวร์อันตราย หรือการกระทำอื่นใดที่กระทบต่อความเที่ยงตรงของข้อมูล

---

[18] United States v. Bae, 250 F.3d 774 (D.C. Cir. 2001), the defendant used a lottery terminal to produce back-dated tickets with winning numbers, and then turned those tickets in to collect lottery prizes., อ้างถึงใน Chapter 1 Computer Fraud and Abuse Act[Online], Available from : http://www.cybercrime.gov/ccmanual/01ccma.pdf[2010, January 11]

การกระทำความผิดอาจทำให้ผู้ใช้งานไม่สามารถปฏิบัติงานต่อไปได้ หรือทำให้งานที่ทำล้มเหลว ทั้งนี้ความเสียหายที่เกิดขึ้นอาจส่งผลกระทบในวงกว้าง เช่น กรณีนักธุรกิจไม่สามารถทำงานได้หากคอมพิวเตอร์หยุดทำงาน หรืออาจต้องเสียลูกค้าหากไม่สามารถเรียกข้อมูลในฐานข้อมูลลูกค้าได้ หรืออาจส่งผลให้มีคนบาดเจ็บหรือมีการตายเกิดขึ้นหากคอมพิวเตอร์ที่ควบคุมระบบโทรศัพท์ของสถานีตำรวจหยุดทำงาน ความเสียหายกับคอมพิวเตอร์อาจเกิดขึ้นหากทำการบุกรุกคอมพิวเตอร์สำเร็จ หรืออาจเกิดขึ้นโดยที่ไม่เกี่ยวกับการเข้าถึงคอมพิวเตอร์โดยไม่ได้รับอนุญาต

การที่จะก่อให้เกิดความเสียหายต่อคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ต้องมีการเข้าถึง โดยผู้กระทำต้องรู้ถึงการกระทำในการส่งผ่านโปรแกรม ข้อมูล รหัส หรือคำสั่ง และผลในการกระทำดังกล่าวมีเจตนาให้เกิดความเสียหายกับคอมพิวเตอร์ที่อยู่ในการปกป้องของรัฐบาลสหรัฐอเมริกา และยังหมายความรวมถึงการที่ผู้กระทำความผิดได้รับอนุญาตให้ใช้งานคอมพิวเตอร์ของเหยื่อโดยได้รับอนุญาตกรณีที่เป็นบุคคลภายในองค์กร และกรณีที่ไม่ได้รับอนุญาต

คำว่า โปรแกรม ข้อมูล รหัส หรือคำสั่ง หมายถึง ทุกอย่างที่สามารถส่งผลใดๆ ต่อการทำงานของระบบคอมพิวเตอร์ รวมถึง รหัสซอฟต์แวร์ คำสั่งซอฟต์แวร์ และเครือข่ายที่ถูกออกแบบมาเพื่อใช้ประโยชน์จากคอมพิวเตอร์ การกระทำความผิดนี้ไม่รวมถึงการกระทำทางกายภาพ เช่น การปิดคอมพิวเตอร์ การปิดสวิตซ์ไฟฟ้า

ผู้กระทำความผิดไม่ต้องทำการส่งผ่านโดยตรงเพียงแต่เขียนตามคำสั่งให้ส่งผ่านข้อมูลดังกล่าวเข้าสู่ระบบคอมพิวเตอร์ เช่น การที่ผู้กระทำความผิดใส่รหัสที่เป็นอันตรายลงในโปรแกรมซอฟต์แวร์ที่เขียนขึ้นให้ทำงานในเครือข่ายคอมพิวเตอร์ของนายจ้างโดยอัตโนมัติ[19] หลังจากนั้นสี่เดือน รหัสอันตรายดังกล่าวก็เริ่มทำงานโดยทำการดาวน์โหลดรหัสอันตรายประเภทอื่นเข้าสู่คอมพิวเตอร์พกพาของพนักงานในบริษัททำให้ไม่สามารถทำงานได้ คดีนี้ศาลตัดสินว่าจำเลยรู้ถึงการกระทำดังกล่าวว่าเป็นความผิด

การกระทำต้องเป็นการก่อให้เกิดความเสียหายต่อคอมพิวเตอร์ที่อยู่ในการปกป้องของรัฐบาลสหรัฐอเมริกา การกระทำความผิดนี้ต้องการเพียงการกระทำที่ทำให้เกิดความ

---

[19] United States v. Sullivan, 40 Fed. Appx. 740 (4th Cir. 2002) : a defendant inserted malicious code into a software program he wrote to run on his employer's computer network อ้างถึงใน Chapter 1 Computer Fraud and Abuse Act[Online], Available from : http://www.cybercrime.gov/ccmanual/01ccma.pdf[2010, January 11]

เสียหายกับคอมพิวเตอร์ที่อยู่ในการปกป้องของรัฐบาลสหรัฐอเมริกา จึงไม่จำเป็นต้องมีการพิสูจน์ว่าคอมพิวเตอร์ที่อยู่ในการปกป้องของรัฐบาลสหรัฐอเมริกาที่ได้รับความเสียหายนั้นเป็นคอมพิวเตอร์เครื่องเดียวกันกับที่จำเลยเข้าหรือไม่ เช่น ผู้กระทำความผิดอาจกระทำความผิดจากเครื่องคอมพิวเตอร์อื่น แต่ได้มีการเขียนคำสั่งอันตรายให้ทำงานกับคอมพิวเตอร์ที่อยู่ในการปกป้องของรัฐบาลสหรัฐอเมริกา

ความหมายของคำว่า ความเสียหายที่เกิดขึ้นต้องกระทบกับความสมบูรณ์หรือความพร้อมของฐานข้อมูล โปรแกรม ระบบ หรือข้อมูลเสียหาย (Title 18 U.S.C. § 1030 (e)(8)) แม้ความหมายดังกล่าวนี้จะกว้างมาก เนื่องจากต้องการให้สามารถใช้ได้กับหลายสถานการณ์ ซึ่งความหมายของคำว่าความเสียหายที่เกิดขึ้นนี้แตกต่างจากความเสียหายต่อทรัพย์สินที่มีรูปร่าง ความเสียหายต้องกระทบต่อความสมบูรณ์ของฐานข้อมูล โปรแกรม ระบบ หรือข้อมูล เช่น อาจทำให้ความสมบูรณ์ดังกล่าวลดน้อยลง ส่วนหนึ่งของนิยามนี้อาจต้องการประยุกต์ใช้กับการกระทำที่ทำให้ข้อมูลถูกลบหรือเปลี่ยนแปลง เช่น ผู้กระทำความผิดที่เข้าถึงคอมพิวเตอร์และต้องการลบข้อมูลหรือเปลี่ยนแปลงฐานข้อมูลของธนาคาร หรือสถาบันการเงิน

ในทำนองเดียวกับคำว่า ความเสียหาย อาจเกิดขึ้นเมื่อผู้เข้าถึงคอมพิวเตอร์เปลี่ยนให้คอมพิวเตอร์ทำงานตามที่สั่งการ เช่น การติดตั้งซอฟต์แวร์ในคอมพิวเตอร์แต่ความเสียหายยังคงเกิดขึ้นหากผู้เข้าถึงคอมพิวเตอร์ทำการแก้ไขซอฟต์แวร์ในการรักษาความปลอดภัยของคอมพิวเตอร์เพื่อทำให้ระบบตรวจสอบความปลอดภัยของคอมพิวเตอร์ล้มเหลว[20] ซึ่งความเสียหายต้องกระทบต่อความสมบูรณ์ของฐานข้อมูล โปรแกรม ระบบ หรือข้อมูล นิยาม ของความเสียหายยังรวมถึงการกระทำที่ทำให้ข้อมูลหรือคอมพิวเตอร์ไม่พร้อมใช้งาน

การกระทำที่ก่อให้เกิดความเสียอาจเป็นความเสียหายต่อสิ่งอื่นๆตามที่กำหนดใน (Title 18 U.S.C. § 1030 (e)(11)) โดยแยกประเภทของการกระทำที่ทำให้เกิดความเสียหายซึ่งรัฐบาลจะต้องพิสูจน์ถึงผลของความเสียหายที่เกิดขึ้นดังต่อไปนี้ ไม่ว่าจะเป็น ความเสียหายทางธุรกิจที่มีมูลค่า 5,000 ดอลลาร์ ภายใน 1 ปี ผลกระทบที่เกิดขึ้นในการรักษาพยาบาลหรือมีผลกระทบต่อประสิทธิภาพในการรักษาพยาบาล ทำให้บุคคลได้รับบาดเจ็บทางกายภาพเป็นภัยคุกคามต่อสุขภาพหรือความปลอดภัยของประชาชน หรือความเสียหายต่อคอมพิวเตอร์ที่ใช้ในการบริหารงานยุติธรรม การป้องกันประเทศ หรือความมั่นคงของชาติ

---

[20] United States v. Middleton, 231 F.3d 1207, 1213-14 (9th Cir. 2000) อ้างถึงใน Chapter 1 Computer Fraud and Abuse Act[Online], Available from : http://www.cybercrime.gov/ccmanual/01ccma.pdf[2010, January 11]

ข้อสังเกตประการหนึ่ง กฎหมายนี้ไม่ได้มีการกำหนดความเสียหายที่กระทบทางด้านจิตใจ ซึ่งอาจเป็นผลที่เกิดจากการกระทำความผิดนี้ได้ ทั้งนี้ เช่น กรณีเกิดขึ้นโดยรัฐบาลไม่จำเป็นต้องพิสูจน์ว่าผู้กระทำมีเจตนาก่อให้เกิดผลของความเสียหายโดยเฉพาะตามที่กำหนด เพียงแต่พิสูจน์ว่าผู้กระทำได้ก่อให้เกิดความเสียหายจริง[21]

ความเสียหายทางธุรกิจ เป็นความเสียหายอีกประการหนึ่งที่กฎหมายมุ่งคุ้มครอง ซึ่งเป็นความเสียหายที่พบมากที่สุด โดยกฎหมายได้กำหนดคำว่า ความเสียหายทางธุรกิจค่อนข้างกว้าง เช่น ค่าใช้จ่ายที่เหมาะสมของเหยื่อ รวมทั้งค่าใช้จ่ายที่เกิดจากการกระทำความผิด การประเมินค่าความเสียหาย ค่าใช้จ่ายในการเรียกคืนฐานข้อมูล โปรแกรม ระบบ หรือข้อมูลให้มีสภาพตามเดิมก่อนที่จะมีการเข้าถึง และการสูญเสียรายได้ ค่าใช้จ่ายที่เกิดขึ้น หรือความเสียหายที่สำคัญอื่นๆ ที่เกิดขึ้นจากการกระทำความผิด เช่น กรณีที่ผู้ดูแลระบบการจ่ายเงินเดือนพนักงานต้องทำการเรียกคืนการสำรองข้อมูลที่ถูกลบ ผู้ดูแลระบบต้องการตรวจสอบข้อมูลเกี่ยวกับค่าจ้างรายชั่วโมงของพนักงานเพื่อให้เกิดความแน่ใจว่าข้อมูลนั้นไม่ได้รับการแก้ไข ซึ่งค่าใช้จ่ายในการติดตั้งซอฟต์แวร์ระบบใหม่ถือได้ว่าเป็นค่าใช้จ่าย และค่าใช้จ่ายในการติดตั้งระบบรักษาความปลอดภัยของคอมพิวเตอร์เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นอีก[22] โดยค่าใช้จ่ายในการเรียกคืนระบบนี้ ให้รวมอยู่ในความหมายของคำว่า ความเสียหายที่สำคัญอื่นๆที่เกิดขึ้นจากการกระทำความผิด แม้ว่าจำนวนเงินที่เหยื่อได้จ่ายเพื่อทำให้ระบบดีขึ้นและปลอดภัยขึ้นกว่าเดิมจะไม่เหมาะสมในบางกรณี การคำนวณค่าเสียหายอาจจะไม่รวมค่าใช้จ่ายที่เกิดขึ้นเพื่อช่วยเหลือผู้ประสบภัยเบื้องต้นของรัฐบาลในการฟ้องร้องหรือตรวจสอบการกระทำผิด[23]

---

[21] United States v. Suplita,Case No. 01cr3650, Order Denying Motion to Dismiss Indictment, at 4 (S.D. Cal. July 23, 2002). Prior to 2001, because the definition of damage contained the "enumerated harms" (now found in 1030(a)(5)(B)), an argument could be made that the crime required, for example, proof of the intent to cause $5,000 in loss or a threat to public health or safety. By moving these subsections out of the definition of damage, Congress clarified that the government must prove the actor's mental state with respect to damage and not with respect to loss or other harms. อ้างถึงใน Chapter 1 Computer Fraud and Abuse Act[Online], Available from : http://www.cybercrime.gov/ccmanual/01ccma.pdf[2010, January 11]

[22] United States v. Middleton, 231 F.3d 1207, 1213-14 (9th Cir. 2000) (interpreting ง 1030(a)(5) before addition of the definition of damage) อ้างถึงใน Chapter 1 Computer Fraud and Abuse Act[Online], Available from : http://www.cybercrime.gov/ccmanual/01ccma.pdf[2010, January 11]

[23] U.S.S.G. § 2B1.1, cmt. n. 3(D)(ii); United States v. Schuster, 467 F.3d 614 (7th Cir. 2006). อ้างถึงใน Chapter 1 Computer Fraud and Abuse Act[Online], Available from : http://www.cybercrime.gov/ccmanual/01ccma.pdf[2010, January 11]

ความเสียหายที่เกิดกับการดูแลรักษาพยาบาล ความเสียหายดังกล่าวนี้เกี่ยวกับการดัดแปลง หรือการทำให้เสียหาย หรือการเปลี่ยนแปลงค่ารักษาในการตรวจวินิจฉัยทางการแพทย์ หรือการทำให้ประสิทธิภาพในการรักษาพยาบาลลดลง (Title 18 U.S.C. § 1030 (c)(4)(A)(i)(II)) ซึ่งเป็นการกำหนดขึ้นเพื่อป้องกันเครือข่ายคอมพิวเตอร์ในโรงพยาบาล คลินิก และสถานพยาบาลอื่นๆ เนื่องจากข้อมูลที่มีอยู่ในระบบคอมพิวเตอร์เหล่านั้นมีความสำคัญ ความเสียหายประเภทนี้ ไม่จำเป็นต้องมีการแสดงถึงความสูญทางการเงินแต่อย่างใด การเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ในลักษณะนี้สามารถกระทำได้โดยง่ายแต่ทำให้เกิดความรับผิดทางอาญา เพียงแค่มีหลักฐานที่แสดงว่าการรักษาพยาบาลผู้ป่วยได้รับผลกระทบที่เป็นมาจากการเข้าถึงข้อมูลในระบบคอมพิวเตอร์ดังกล่าว

จากตัวอย่างดังกล่าวถึงแม้ว่าจะไม่มีอันตรายที่เกิดขึ้นจริง เนื่องจากการทำให้ประสิทธิภาพในระบบลดลง ซึ่งกรณีนี้อาจต้องใช้จินตนาการเพื่อแสดงให้เห็นถึงความแตกต่างจากการที่สามารถเข้าถึงระบบคอมพิวเตอร์ซึ่งจะมีผลกระทบกับการรักษาพยาบาลผู้ป่วยกับกรณีปกติที่ไม่มีการเข้าถึงข้อมูลในระบบ ทั้งนี้ แพทย์ที่ทำการรักษาอาจยืนยันได้ว่าการดูแลรักษาผู้ป่วยอาจมีการเปลี่ยนแปลงได้ รัฐบาลก็สามารถพิสูจน์ความเสียหายนี้ได้

ความเสียหายที่เกิดการบาดเจ็บทางกายภาพ (Title 18 U.S.C. § 1030 (c)(4)(A)(i)(III)) ความเสียหายประเภทนี้เกิดขึ้นเมื่อเกิดความเสียหายกับคอมพิวเตอร์และส่งผลทำให้เกิดการบาดเจ็บทางกายภาพกับบุคคลใด โดยใช้เครือข่ายระบบคอมพิวเตอร์ควบคุมระบบสำคัญอื่นๆในสังคม เช่น การควบคุมการจราจรทางอากาศ และบริการโทรศัพท์ฉุกเฉิน 911 การทำลายระบบคอมพิวเตอร์เหล่านี้อาจทำให้เกิดการบาดเจ็บทางร่างกาย สิ่งที่ต้องทำการพิจารณาว่าความเกี่ยวพันระหว่างความเสียหายของคอมพิวเตอร์และการบาดเจ็บในการที่ศาลใช้ตัดสินความรับผิดทางอาญา แม้กฎหมายจะไม่ได้กำหนดอย่างชัดเจนว่าต้องเกิดการบาดเจ็บ ศาลอาจต้องใช้ประสบการณ์อย่างมากในการประยุกต์ใช้กฎหมายและหลักกฎหมายตราบใดที่มีการเชื่อมต่อระหว่างความเสียหายของคอมพิวเตอร์และการบาดเจ็บทางกายภาพ เช่น ผู้กระทำความผิดเข้าถึงระบบคอมพิวเตอร์ที่เกี่ยวกับสาธารณูปโภคไฟฟ้าและทำการปิดไฟในพื้นที่ที่มีการจราจรพลุกพล่านทำให้ไฟจราจรปิด และทำให้เกิดอุบัติเหตุหากผู้ขับขี่ประสบอุบัติเหตุและได้รับบาดเจ็บ อาจถูกลงโทษตามมาตรานี้

ความเสียหายที่เกิดจากการโจมตีด้านสาธารณสุขหรือความมั่นคง (Title 18 U.S.C. § 1030 (c)(4)(A)(i)(IV)) ความเสียหายที่เกิดขึ้นนี้จะต้องมีความเกี่ยวข้องกับร่างกายโดยต้องมีการคุกคามด้านสาธารณสุขหรือความปลอดภัย เนื่องจากรัฐบาลไม่จำเป็นต้องพิสูจน์ความ

เสียหายทางกายภาพที่เกิดขึ้นกับบุคคล เพราะมาตรานี้ใช้กับสถานการณ์ที่กว้างมาก เครือข่ายคอมพิวเตอร์ใช้ควบคุมโครงสร้างพื้นฐานที่สำคัญของประเทศ เช่น การไฟฟ้า การจำหน่ายก๊าซ น้ำสะอาด พลังงานนิวเคลียร์ และการขนส่ง ความเสียหายที่เกิดขึ้นกับคอมพิวเตอร์ที่ใช้ควบคุมการทำงานระบบ ควบคุมกลไกรักษาความปลอดภัยต่างๆเหล่านี้ ทำให้เกิดความเสียหายกับคนจำนวนมากในการกระทำครั้งเดียว

ความเสียหายที่เกิดขึ้นกับผู้พิพากษา การป้องกันราชอาณาจักร การรักษาความปลอดภัยแห่งชาติ (Title 18 U.S.C. § 1030 (c)(4)(A)(i)(V)) ความเสียหายที่เกิดขึ้นตามข้อนี้เป็นความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ที่ใช้ในองค์กรของรัฐไม่ว่าจะเป็นการบริหารงานยุติธรรม หน่วยงานรักษาความมั่นคงแห่งชาติ หรือหน่วยงานรักษาความปลอดภัยแห่งชาติ การกระทำดังกล่าวนี้ส่งผลให้เกิดความเสียหายกับหน้าที่ที่สำคัญ เช่น การเข้าถึงระบบคอมพิวเตอร์ของศาลเพื่อทำการแก้ไขคำพิพากษาของศาล ดังนั้นอาจไม่ใช่เรื่องง่ายในการประเมินค่าความเสียหายทางเศรษฐกิจ

คอมพิวเตอร์ที่เกี่ยวข้องกับการบริหารงานยุติธรรม ประกอบด้วย ระบบคอมพิวเตอร์ของศาลแต่ก็ยังสามารถขยายความรวมถึงคอมพิวเตอร์ที่เป็นของรัฐหรือหน่วยงานบังคับใช้กฎหมายรัฐบาลกลาง อัยการและสำนักงานคุมประพฤติ รวมถึงเครือข่ายระบบคอมพิวเตอร์ของกระทรวงกลาโหม มาตรานี้ไม่ประสงค์ให้ขยายความรวมถึงคอมพิวเตอร์ที่รัฐบาลเป็นเจ้าของหรือดำเนินการโดยรัฐบาล หรือคอมพิวเตอร์ที่เป็นคู่สัญญากับรัฐ คอมพิวเตอร์ที่ใช้ในการทหารหรือที่ใช้ในการส่งเสริมความปลอดภัยแห่งชาติ ในขณะเดียวกันไม่ได้หมายความรวมถึงทุกหน่วยงานในกระทรวงกลาโหม เช่น คอมพิวเตอร์ที่ใช้ในตึกเพนทากอน[24]

6). การจำหน่ายรหัสในการเข้าถึงข้อมูลในระบบคอมพิวเตอร์ (Title 18 U.S.C. § 1030 (a)(6)) กฎหมายได้ห้ามมิให้บุคคลที่รู้และมีเจตนาในการฉ้อโกงทำการจำหน่ายรหัสผ่านในการเข้าถึงข้อมูลในระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่คล้ายกัน เมื่อการจำหน่ายดังกล่าวอาจส่งผลต่อการค้าระหว่างรัฐและการค้าระหว่างประเทศ หรือรหัสผ่านนั้นอาจถูกใช้เพื่อเข้าถึงโดยไม่ได้รับอนุญาตซึ่งคอมพิวเตอร์ที่ใช้โดยหรือเพื่อประโยชน์ของรัฐบาล

การกระทำความผิดในลักษณะนี้ หมายถึง โอน หรือจำหน่ายไปยังบุคคลอื่นหรือรับเอาโดยมีเจตนาที่จะโอนหรือจำหน่าย โดยไม่คำนึงถึงผลกำไร รวมถึงการครอบครอง

---

[24] Chapter 1 Computer Fraud and Abuse Act[Online], Available from : http://www.cybercrime.gov/ccmanual/01ccma.pdf[2010, January 11]

รหัสผ่านถ้าไม่มีเจตนาในการโอนหรือจำหน่าย แต่การที่บุคคลใช้รหัสผ่านของตนเองไม่ถือว่าเป็นความผิด

การจำหน่ายที่ถือเป็นความผิดต้องเป็นการจำหน่าย รหัสผ่าน หรือสิ่งอื่นที่มีลักษณะคล้ายกัน ไม่ได้หมายความถึงคำหรือวลีหนึ่งที่ช่วยในการเข้าถึงคอมพิวเตอร์[25] อาจประกอบด้วยชุดคำสั่ง ใช้ในความหมายกว้างที่อาจหมายถึงสิ่งใดๆที่ป้องกันการเข้าถึงคอมพิวเตอร์ รหัส ชื่อที่เข้าใช้งาน หรือวิธีการอื่นๆ หรือการผสมผสานวิธีการโดยผู้ใช้งานคอมพิวเตอร์ที่รู้ถึงการกระทำและมีเจตนาในการเข้าถึงข้อมูลโดยการฉ้อฉล ซึ่งการจำหน่ายดังกล่าวต้องส่งผลต่อการค้าระหว่างรัฐและการค้าระหว่างประเทศ การตีความนิยามดังกล่าวนี้ศาลมักตีความอย่างกว้างเช่น จำเลยครอบครองบัญชีหมายเลขบัตรเครดิตซึ่งถือได้ว่าเป็นการฉ้อโกงบัตรเครดิตที่มีผลต่อการค้า เนื่องจากเป็นช่องทางในการที่ธนาคารอนุมัติให้ได้รับค่าใช้จ่าย[26]

ทั้งนี้ คอมพิวเตอร์ที่มีการเข้าถึงต้องใช้โดยหรือใช้เพื่อประโยชน์ของรัฐบาล และข้อมูลหรือสิ่งอื่นที่คล้ายกันดังกล่าวต้องมีการใช้ในการเข้าถึงโดยไม่ได้รับอนุญาตซึ่งคอมพิวเตอร์ที่ใช้โดยหรือเพื่อประโยชน์ของรัฐบาล เช่น คอมพิวเตอร์ที่ใช้การติดต่อธุรกิจอย่างเป็นทางการสำหรับรัฐบาล ไม่ว่าโดยลูกจ้างรัฐบาลหรือในนามของรัฐบาลเอง

7). การข่มขู่ว่าจะก่อให้เกิดความเสียหายแก่คอมพิวเตอร์ (Title 18 U.S.C. § 1030 (a)(7)) ในสถานการณ์ที่ผู้บุกรุกหรือเข้าถึงระบบทำการเจาะระบบและการเข้าถึงรหัสหรือลบฐานข้อมูล หรือสถานการณ์อื่นที่เกี่ยวกับการข่มขู่ว่าจะกระจายการปฏิเสธการให้บริการโดยจะทำการปิดระบบเครือข่ายของเหยื่อ อาจมีเจตนากรรโชกเพื่อให้ได้รับเงินหรือสิ่งอื่นใดที่มีค่า จึงไม่จำเป็นต้องพิสูจน์ว่าจำเลยได้รับเงินจริงหรือไม่หรือจำเลยตั้งใจจริงที่จะดำเนินการคุกคามดังกล่าวหรือไม่ ทั้งนี้ กรรโชก โดยทั่วไปหมายถึง เจตนาเพื่อขอรับเงินหรือสิ่งอื่นที่มีค่าจากความยินยอมของบุคคลโดยผิดกฎหมายจากความกลัว การคุกคามโดยการขู่กรรโชก หรือการบังคับ

การขู่กรรโชกจะต้องผ่านการสื่อสารการค้าระหว่างรัฐและการค้าระหว่างประเทศ แต่ไม่จำเป็นต้องเป็นการส่งข้อมูลอิเล็กทรอนิกส์ ภัยคุกคามที่เกิดขึ้นกับระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ อาจเป็นการขู่กรรโชกทางไปรษณีย์ โทรศัพท์

---

[25] Ibid,. p 47.

[26] United States v. Rushdan, 870 F.2d 1509, 1514 (9th Cir. 1989). อ้างถึงใน Chapter 1 Computer Fraud and Abuse Act[Online], Available from : http://www.cybercrime.gov/ccmanual/01ccma.pdf[2010, January 11]

จดหมายอิเล็กทรอนิกส์ หรือผ่านบริการส่งข้อความคอมพิวเตอร์ ซึ่งการโจมตีที่ก่อให้เกิดความเสียหายกับเครื่องคอมพิวเตอรที่อยู่ในการปกป้องของรัฐบาลสหรัฐอเมริกา ภัยคุกคามที่ผิดกฎหมายดังกล่าวต้องก่อให้เกิดความเสียหาย รวมถึงการรบกวนการทำงานปกติใดๆของเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์ การปฏิเสธการเข้าถึงของผู้ใช้บริการที่มีอำนาจในการเข้าถึง การลบข้อมูลหรือทำให้ข้อมูลเสียหาย หรือทำให้โปรแกรมลดประสิทธิภาพในการทำงานของเครื่องคอมพิวเตอร์และลดระดับการทำงานของระบบคอมพิวเตอร์ หรือการเข้ารหัสข้อมูลและการเรียกร้องเงินจากการถอดรหัสสำหรับเข้าถึงคอมพิวเตอร์

ข. กฎหมายการหลอกลวงเกี่ยวกับบัตรเครดิต (The Credit Billing Act : FCBA)

ประเทศสหรัฐอเมริกาได้บัญญัติกฎหมายการหลอกลวงเกี่ยวกับบัตรเครดิตไว้ใน The Credit Billing Act (FCBA) ซึ่งในกฎหมายดังกล่าวนี้ ได้กำหนดให้กรณีที่เจ้าของบัตรไม่ได้ใช้จ่ายบัตรเครดิตด้วยตัวเอง หรือว่าบัตรเครดิตสูญหายหรือถูกขโมย เจ้าของบัตรเครดิตไม่ต้องรับผิดชอบค่าใช้จ่ายที่เกิดจากบัตรเครดิตดังกล่าว ทั้งนี้เจ้าของบัตรจะต้องแจ้งสูญหายให้บริษัทเจ้าของบัตรทราบทันทีที่ได้ทราบถึงการสูญหาย โดยบริษัทส่วนใหญ่จะมีบริการรับแจ้งบัตรเครดิตหายหรือถูกขโมยตลอด 24 ชั่วโมง แต่ถ้าเจ้าของบัตรเครดิตไม่ได้แจ้งให้บริษัททราบหรือแจ้งหลังจากบัตรเครดิตนั้นได้ถูกนำไปใช้แล้ว เจ้าของบัตรจะต้องรับผิดชอบต่อค่าใช้จ่ายที่เกิดขึ้นเป็นจำนวนเงินไม่เกิน 50 ดอลลาร์สหรัฐ

สำหรับกรณีที่ปรากฏในใบแจ้งหนี้ว่ามียอดค่าใช้จ่ายที่เจ้าของบัตรเครดิตไม่ได้จ่ายนั้น กฎหมายได้กำหนดให้เจ้าของบัตรเครดิตไม่จำต้องรับผิดชอบในค่าใช้จ่ายที่เกิดขึ้น[27] แม้ว่าจะมีกฎหมายให้ความคุ้มครองเจ้าของบัตรเครดิตไม่ต้องรับผิดชอบเกี่ยวกับค่าใช้จ่ายที่เกิดจากบัตรเครดิตที่ตนไม่ได้ใช้ก็ตาม แต่การพิสูจน์ว่าตนไม่ได้เป็นผู้ใช้บัตรเครดิตดังกล่าวหรือการขอรับเงินคืนจากธนาคารก็จะเสียเวลาในการดำเนินการมาก

อย่างไรก็ดีกฎหมายระดับรัฐบาลกลางสหรัฐได้ป้องกันและปราบปรามการกระทำความผิดทางอาญาเกี่ยวกับบัตรเครดิตไว้ใน Credit Card Fraud Act 1984 โดยมี

---

[27] FTC, Bill for Merchandise You Never Received[Online], Available from : Http://www.ftc./gov/bcp/conline/pubs/credit/billed.htm[2002, September 30]

วัตถุประสงค์เพื่อให้ครอบคลุมการฉ้อฉลและการกระทำที่เกี่ยวกับบัตรเครดิต (Title 18 U.S.C. § 1029 (e)(1))* ซึ่งมีสาระสำคัญที่กำหนดบทบัญญัติดังต่อไปนี้

1. กำหนดให้การใช้หมายเลขบัตรเครดิตโดยทุจริตเป็นความผิดโดยไม่ต้องคำนึงว่าจะใช้ร่วมกับตัวบัตรเครดิตหรือไม่ เนื่องจากได้กำหนดให้หมายเลขบัตรเครดิตเป็นอุปกรณ์การเข้าถึงอย่างหนึ่ง ดังนั้น เพียงใช้หมายเลขบัตรเครดิตก็ถือเป็นการใช้อุปกรณ์เข้าถึงแล้ว

2.·...

3. กำหนดบทบัญญัติที่เกี่ยวข้องกับการใช้อุปกรณ์การเข้าถึงที่ปราศจากอำนาจ เช่น การได้มาโดยเจตนาที่จะฉ้อฉลอันได้แก่การให้ข้อมูลในการแสดงตนที่ไม่ถูกต้อง เมื่อมีการใช้จ่ายผ่านอุปกรณ์ดังกล่าวโดยทุจริต ไม่ว่าจะเป็นจำนวนเท่าใดก็ถือว่าเป็นความผิด

อุปกรณ์ หมายถึง บัตรใดๆ แผ่นรหัส หมายเลขบัญชี หรือสิ่งอื่นใดก็ตามที่สามารถเข้าสู่บัญชีโดยตัวเองหรือใช้กับอุปกรณ์อื่นๆ เพื่อที่จะครอบครองเงิน สินค้า หรือสิ่งอื่นๆ ที่มีมูลค่า หรือสามารถนำไปใช้เพื่อที่จะโอนเงิน

4. กำหนดความผิดสำหรับผู้ผลิตบัตรเครดิตปลอมและผู้มีเครื่องมือสำหรับการปลอมไว้ในการครอบครอง (Title 18 U.S.C § 1029 (a)(1))**

บทกำหนดโทษสำหรับความผิดดังกล่าวข้างต้น โดยทั่วไปเป็นมาตรการทางอาญาทั้งสิ้น ซึ่งจะมีโทษปรับและโทษจำคุกแล้วแต่กรณี เช่น กรณีการปลอมแปลง การใช้บัตรปลอม การจำหน่ายบัตรปลอม การจ่ายผ่านบัตรที่ได้มาโดยทุจริต รวมทั้งการใช้หมายเลขบัตรเครดิตโดยทุจริต และการมีไว้ในครอบครองซึ่งบัตรที่ได้มาโดยทุจริตหรือบัตรปลอมเกิน 15 ใบ ในส่วนของ

---

* Title 18 U.S.C. § 1029 (e)(1) of Fraud and related activity in connection with access devices

...(e) As used in this section

.(1) the term "access device" means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument);...

** Title 18 U.S.C § 1029 (a)(1) of Fraud and related activity in connection with access devices

(a) Whoever

...(1) knowingly and with intent to defraud produces, uses, or traffics in one or more counterfeit access devices;...

การฉ้อฉลโดยการใช้บัตรเครดิต ซึ่งมีโทษปรับไม่เกิน 10,000 ดอลลาร์สหรัฐ หรือจำคุกไม่เกิน 10 ปี หรือทั้งจำทั้งปรับ (Title 18 U.S.C Section 1029 (c) (1) (a) (i))*

ค. กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับจดหมายโฆษณา (Can Spam Act of 2003)

ในหลายปีที่ผ่านมาปัญหาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ได้เพิ่มขึ้นทั่วทุกมุมโลก พรมแดนทางภูมิศาสตร์ไม่มีอีกต่อไปในโลกของอินเทอร์เน็ตหรือที่เรียกกันว่า โลกไร้พรมแดน การที่ไม่มีกฎหมายที่มีผลบังคับใช้ที่สามารถประยุกต์ใช้กับอาชญากรที่กระทำความผิดเกี่ยวกับคอมพิวเตอร์ระหว่างประเทศส่งผลให้เกิดการกระทำความผิดมากมาย[28] จดหมายโฆษณา (Spam Mail) เป็นลักษณะจดหมายอิเล็กทรอนิกส์ประเภทหนึ่งที่จัดอยู่ในประเภทของจดหมายขยะ (Junk Mail)

วิวัฒนาการในการแก้ไขปัญหา Spam Mail ในประเทศสหรัฐอเมริกามีพัฒนาการมายาวนาน ในระยะเริ่มแรกการแก้ไขปัญหากระทำด้วยวิธีการทางเทคนิค โดยการควบคุมตรวจสอบกันเองของผู้ให้บริการ รวมถึงการพัฒนาเทคโนโลยีคอมพิวเตอร์ในการควบคุมแต่ไม่ประสบความสำเร็จ เนื่องจากค่าใช้จ่ายในการส่ง Spam Mail ต่ำมากเมื่อเทียบกับการส่งจดหมายทางไปรษณีย์ อีกทั้งการดำเนินการทางกฎหมายยังไม่มีความชัดเจน เพราะไม่มีกฎหมายควบคุมการใช้ Spam Mail โดยเฉพาะ จึงมีแนวความคิดในการออกกฎหมายเพื่อแก้ไขปัญหาจากการใช้ Spam Mail รัฐต่างๆของประเทศสหรัฐอเมริกาได้ออกกฎหมายมาบังคับใช้กับ Spam Mail ซึ่งรัฐแรกที่ออกกฎหมายมาบังคับใช้กับ Spam Mail ได้แก่ รัฐเนวาดา (Nevada)[29] ออกกฎหมาย Liability of Person Who Transmit Items of Electronic Mail

---

* Title 18 U.S.C Section 1029 (c) (1) (a) (i) of Fraud and related activity in connection with access devices

(c) Penalties.

(1) Generally. The punishment for an offense under subsection (a) of this section is

(A) in the case of an offense that does not occur after a conviction for another offense under this section

(i) if the offense is under paragraph (1), (2), (3), (6), (7), or (10) of subsection (a), a fine under this title or imprisonment for not more than 10 years, or both; and...

[28] Global LI Industry Forum, Inc., Eight Reasons the U.S Should Ratify the Cybercrime Treaty The Convention on Cybercrime. [Online]. 2007, Available from : http://www.gliif.org/RatifyNow/reasons.htm. [2009, January 20]

[29] Available from : "Spam Law Summary", HTTP://www.spamlawscom/state/nv.html, February 2005 [2009, January 20]

that Include Advertisement ในปี ค.ศ. 1997 และมีการแก้ไขเพิ่มเติมในปี ค.ศ. 2001 และ ค.ศ. 2003 กฎหมายฉบับนี้ บัญญัติให้การส่ง Spam Mail เป็นความผิด เว้นแต่จะได้มีการระบุที่ตอนต้นของชื่อเรื่องว่า "ADV" หรือ "Advertisement" รวมทั้งต้องระบุชื่อ ที่อยู่ทางไปรษณีย์และที่อยู่จดหมายอิเล็กทรอนิกส์ และต้องมีการแจ้งให้ผู้รับสามารถบอกเลิกการรับจดหมายดังกล่าวได้ด้วย ต่อมารัฐอื่นๆก็ได้มีการบัญญัติกฎหมายเพื่อบังคับใช้กับจดหมายโฆษณา เช่น รัฐมินเนโซต้า (Minnesota) ได้บัญญัติกฎหมาย Minnesota Law 2002, Ch.395 รัฐนอร์ธแคโรไลน่า (North Carolina) ได้บัญญัติกฎหมาย North Carolina General Statues, Section 14-453 รัฐโอกลาโฮมา (Oklahoma) ได้บัญญัติกฎหมาย Oklahoma Statues Title 15 Contracts Section 776 เป็นต้น แต่กฎหมายของรัฐต่างๆหล่านี้ เป็นการบัญญัติขึ้นมาเพื่อบังคับใช้กับผู้ใช้คอมพิวเตอร์ที่อยู่ในเครือข่ายคอมพิวเตอร์ของรัฐเท่านั้น[30]

เนื่องจากกฎหมายของแต่ละรัฐมีข้อกำหนดและมาตรฐานที่แตกต่างกัน ทำให้การแก้ไขปัญหาการใช้ Spam Mail เป็นไปได้อย่างลำบาก และเนื่องจากจดหมายอิเล็กทรอนิกส์สามารถส่งไปได้ในหลายประเทศ โดยไม่อาจระบุได้ว่าส่งมาจากสถานที่ใด จึงเป็นการยากที่ผู้ส่งจดหมายอิเล็กทรอนิกส์จะทราบได้ว่าจะต้องปฏิบัติตามกฎหมายของรัฐใด ด้วยเหตุนี้เพื่อให้เป็นมาตรฐานเดียวกัน ประเทศสหรัฐอเมริกาจึงพยายามร่างกฎหมายเพื่อแก้ไขปัญหาและควบคุมเกี่ยวกับการใช้ Spam Mail โดยเนื้อหาของกฎหมายที่เสนอต่อสภาคองเกรสหลายฉบับจะมีแนวทางคล้ายๆกัน กล่าวคือ การใช้ชื่อและที่อยู่ของผู้ส่งที่ไม่เป็นจริงถือว่าผิดกฎหมาย การส่ง Spam Mail ต้องแจ้งให้ผู้รับทราบว่าจดหมายนั้นเป็น Spam Mail การปฏิบัติตามนโยบายของผู้ให้บริการเครือข่ายอินเทอร์เน็ตอย่างเคร่งครัดรวมทั้งการแจ้งให้ผู้รับ Spam Mail เลือกที่จะปฏิเสธไม่รับ Spam Mail ในโอกาสต่อไปได้

กฎหมายเกี่ยวกับ Spam Mail ที่ใช้บังคับในปัจจุบันคือ Can Spam Act of 2003 (S. 877) หรือ Controlling the Assult of Non-solicited Pornography and Marketing Act of 2003 กฎหมายฉบับนี้ได้ถูกใช้แทนกฎหมายของรัฐต่างๆของประเทศสหรัฐอเมริกาที่เกี่ยวข้องกับการควบคุมการใช้จดหมายโฆษณา

ทั้งนี้ การฟ้องคดีตามกฎหมายฉบับนี้ บุคคลทั่วไปไม่สามารถฟ้องคดีตามกฎหมายนี้ได้โดยการฟ้องคดีสามารถกระทำได้โดย Federal Trade Commission (FTC) อัยการสูงสุดหรือหน่วยงานของรัฐและผู้ให้บริการอินเตอร์เน็ตเท่านั้น ตัวอย่างคดีที่เกี่ยวกับการกระทำ

---

[30] ฉันทพิมพ์ บรรจงจิตร์ และปกรณ์ ยิ่งวรการ, งานวิจัยฉบับสมบูรณ์ เรื่อง กฎหมายป้องกัน Spam Mail ของสหรัฐอเมริกา เสนอต่อสำนักงานคณะกรรมการกฤษฎีกา, หน้า 19.

ความผิดโดยใช้ Spam Mail ที่ฝ่าฝืนกฎหมาย Can Spam Act of 2003 คดีที่เกิดขึ้นหลังจากประกาศใช้กฎหมายฉบับนี้ปรากฏในหลายคดีซึ่งอยู่ในระหว่างการพิจารณาคดีของศาล โดยคดีที่ผู้ให้บริการอินเทอร์เน็ตเป็นโจทก์ฟ้องคดี[31] ได้แก่

- คดี America Online, Inc v. John Does 1-40 (March 9, 2004)

- คดี America Online, Inc v. Davis Wolfgang Hawke, et al. (March 9, 2004)

- คดี Earthlink, Inc, v. John Does 1-25, et al. (March 9, 2004)

- คดี Microsoft Corp. v. JDO Media, Inc., et al. (March 9, 2004)

- คดี Microsoft Corp. v. John Does 1-50, d/b/a Super Viagra Group (March 9, 2004)

- คดี Yahoo!, Inc, v. Eric Head, et al. (March 9, 2004)

ส่วนคดีที่ Federal Trade Commission (FTC) เป็นโจทก์ฟ้องคดี ได้แก่

- คดี FTC v. Phoenix Avartar[32] ซึ่งคดีนี้ FTC เป็นโจทก์ฟ้องคดีต่อ Phoenix Avartar เนื่องจากได้ส่ง Spam Mail โดยผิดกฎหมาย กล่าวคือ จดหมายโฆษณามีรายละเอียดเป็นการโฆษณาขายผ้าปิดบนร่างกายเพื่อลดความอ้วน ลูกค้าที่ต้องการจะซื้อสามารถกดปุ่มตกลงจากข้อความในจดหมายโฆษณา โดยการกดปุ่มดังกล่าวจะทำให้มีการเชื่อมโยงไปยังเว็บไซต์ของจำเลย FTC ได้มีการกล่าวอ้างว่า จำเลยได้รับเงินจากการขายสินค้าด้วยวิธีดังกล่าวกว่า 1 แสนเหรียญต่อเดือน และอ้างว่าผ้าดังกล่าวไม่มีผลต่อการลดความอ้วน

---

[31] FindLaw. Spam Litigation. [Online]. A Thomson Reuters business, Available from: http://fl1.findlaw.com/news.findlaw.com/hdocs/docs/cyberlaw/aoldoes30904cmp.pdf, อ้างถึงใน จันทร์พิมพ์ บรรจงจิตร์ และปกรณ์ ยิ่งวรการ, รายงานวิจัยฉบับสมบูรณ์ เรื่อง กฎหมายป้องกัน Spam Mail ของสหรัฐอเมริกา, หน้า 38

[32] Federal Trade Commission. 2007. [Online]. Federal Trade Commission, plaintiff, v. Phoenix Avatar, LLC doing business as Avatar Nutrition, DJL, LLC, Daniel J. Lin, Mark M. Sadek, James Lin, and Christopher M. Chung doing business as A I T Herbal Marketing, defendants. United States District Court for the Northern District of Illinois, Eastern Division. Available from: http://www.ftc.gov/os/caselist/0423084/050331stip0423084.pdf. [2010, January 11]

นอกจากนี้ยังปรากฏว่าจำเลยได้ส่ง Spam Mail โดยการปิดบังที่อยู่โดยใช้จดหมายอิเล็กทรอนิกส์ของบุคคลอื่นในช่อง Reply to หรือ From ซึ่งจดหมายใดหากยังไม่ได้ก็จะถูกตอบกลับไปยังจดหมายอิเล็กทรอนิกส์ของบุคคลที่สาม ทำให้บุคคลที่สามเข้าใจผิดว่าเป็นผู้ส่งและจดหมายโฆษณาดังกล่าวก็ไม่มีการแจ้งให้ผู้รับจดหมายอิเล็กทรอนิกส์สามารถปฏิเสธที่จะรับจดหมายดังกล่าวในโอกาสต่อไปได้ คดีนี้ FTC ได้ฟ้องคดีโดยกล่าวหาว่า การกระทำความผิดดังกล่าวเป็นการกระทำความผิดตาม Federal Trade Commission Act และ Can Spam Act of 2003 และได้ขอให้มีการคุ้มครองชั่วคราวก่อนศาลพิพากษาโดยการให้หยุดส่งจดหมายโฆษณาและสินค้าหลอกลวง รวมถึงยึดทรัพย์ของจำเลย และการดำเนินคดีอาญา

- คดี FTC v. Global Web Promotions[33] (การฟ้องคดีนี้ต้องอาศัยความร่วมมือจากหลายฝ่ายคือ FTC, สำนักงานอัยการในเมืองดีทรอยด์ การให้บริการการสืบสวนทางไปรษณีย์ของสหรัฐอมริกา และผู้ให้บริการอิเทอร์เน็ตต่างๆ) คดีนี้ FTC เป็นโจทก์ฟ้องคดีต่อ Global Web Promotions ซึ่งเป็นบริษัทของประเทศออสเตรเลียว่ามีการส่งจดหมายโฆษณาจำนวนมากมายังประเทศสหรัฐอเมริกา โดยจดหมายโฆษณามีข้อความในการโฆษณาขายผ้าปิดบนร่างกายเพื่อลดความอ้วน รวมถึงสินค้าเพิ่มฮอร์โมนของมนุษย์ ชื่อ HGH และ Natural HGH ที่มีคุณสมบัติชะลอความแก่ ทำให้ดูอ่อนเยาว์ ซึ่งเป็นข้อความอันเป็นเท็จ เนื่องจากสินค้าดังกล่าวมิได้มีส่วนประกอบของฮอร์โมนในการสร้างความเจริญเติบโตใดๆ

FTC ได้กล่าวหาว่า การกระทำความผิดดังกล่าวเป็นการกระทำความผิดตาม Federal Trade Commission Act และ Can Spam Act of 2003 และได้ขอใช้วิธีการคุ้มครองชั่วคราวก่อนมีคำพิพากษาโดยการให้หยุดส่งจดหมายโฆษณาและสินค้าหลอกลวง

จะเห็นได้ว่าทั้งสองคดีนี้ FTC ได้ใช้พยานหลักฐานในการพิสูจน์ความผิดโดยการนำจดหมายโฆษณาจำนวนมากที่ส่งมายังผู้ให้บริการอินเทอร์เน็ต เช่น AOL Microsoft Network บริษัทอื่นๆ และบุคคลทั่วๆไป อันเนื่องมาจากการส่งจดหมายตอบกลับไปยังบุคคลที่สามจำนวนมากทำให้คอมพิวเตอร์เซิร์ฟเวอร์ของผู้ให้บริการอินเทอร์เน็ตเต็ม และรบกวนการดำเนินการตามปกติของระบบ

ง. กฎหมายว่าด้วยการควบคุมการเผยแพร่ภาพและสื่อลามกอนาจาร

---

[33] Federal Trade Commission'[Online]. Federal Trade Commission, plaintiff, v. Global Web Promotions Pty Ltd., Michael John Anthony Van Essen, and Lance Thomas Atkinson, defendants., United States District Court for the Northern District of Illinois, Eastern Division. Available from: http://www.ftc.gov/os/caselist/0423086/050920defjudg0423086.pdf. [2010, January 11]

ประเทศสหรัฐอเมริกาเป็นประเทศแรกที่ได้ดำเนินการบัญญัติกฎหมายออกมาเพื่อควบคุมการเผยแพร่ภาพและสื่อลามกในระบบเครือข่ายอินเทอร์เน็ต คือกฎหมาย The Communication Decency Act : CDA เมื่อวันที่ 8 กุมภาพันธ์ พ.ศ. 2539 ซึ่งเป็นส่วนหนึ่งของกฎหมาย The Communication Decency Act 1996 (กฎหมายดังกล่าว ปัจจุบันล้มเลิกไปแล้วเนื่องจากองค์กร American Civil Liberty Union ที่ทำหน้าที่เกี่ยวกับการคุ้มครองเสรีภาพพลเมืองแห่งอเมริกา ได้ประท้วงไปยังศาลฎีกาประเทศสหรัฐอเมริกาว่าเนื้อหาของกฎหมายดังกล่าวขัดแย้งกับบทแก้ไขรัฐธรรมนูญสหรัฐครั้งที่ 1 (The First Amendment)[34] โดยกฎหมายดังกล่าวได้กำหนดการควบคุมการสื่อสารและเรื่องราวเนื้อหาบนอินเทอร์เน็ตเพื่อลงโทษแก่บุคคลที่ทำการเผยแพร่ภาพหรือสื่อลามกทางเครือข่ายอินเทอร์เน็ต โดยบุคคลใดก็ตามที่ทำ สร้าง ชักชวน หรือริเริ่มให้มีการส่งผ่านไปซึ่งความเห็น ความต้องการ ข้อเสนอ ภาพ หรือวิธีการสื่อสารอื่นๆอันเป็นการลามก โดยรู้ว่าผู้รับการสื่อสารนั้นคือบุคคลที่อายุต่ำกว่า 18 ปี บุคคลใดกระทำการดังกล่าวมีความผิด ต้องรับโทษ นอกจากนี้กฎหมายยังห้ามการส่ง หรือแสดงโดยใช้บริการสื่อสารทางเครือข่ายอินเทอร์เน็ต ด้วยข้อความเห็น ความต้องการ ภาพ หรือข้อมูลประการอื่นในลักษณะของเนื้อหาที่แสดงถึงเรื่องกิจกรรมทางเพศ หรืออวัยวะเพศ แก่บุคคลอายุไม่เกิน 18 ปี หากผู้ใดกระทำการดังกล่าวต้องรับโทษ การที่กฎหมาย CDA กำหนดบทบัญญัติให้มีการควบคุมเนื้อหาที่มีลักษณะลามกที่ปรากฏอยู่ในระบบสื่อสารทางเครือข่ายอินเทอร์เน็ต ก็เพื่อคุ้มครองเด็ก หรือบุคคลที่มีอายุ ไม่เกิน 18 ปี และกฎหมายนี้ยังครอบคลุมไปถึง สิ่งที่ไม่เหมาะสม ซึ่งอาจเป็นอันตรายสำหรับเด็กด้วย

จากบทบัญญัติในอนุสัญญาที่ต้องการให้ประเทศภาคีให้ความคุ้มครองเด็กโดยให้ประเทศภาคีกำหนดให้การกระทำที่เกี่ยวกับสื่อลามกอนาจารเกี่ยวกับเด็กเป็นความผิดนั้น ประเทศสหรัฐอเมริกาเองก็ได้มีความพยายามในการควบคุมเนื้อหาของการติดต่อสื่อสารทางอินเทอร์เน็ตโดยการควบคุมการเผยแพร่ภาพหรือสื่อลามกทางเครือข่ายอินเทอร์เน็ต แต่อย่างที่กล่าวไว้ข้างต้นว่ากฎหมายฉบับดังกล่าวนั้นบัญญัติไว้ค่อนข้างกว้างได้รับการต่อต้าน แต่ในปัจจุบันประเทศสหรัฐอเมริกาก็ได้มีการบัญญัติกฎหมายที่เกี่ยวกับการควบคุมการเผยแพร่ภาพหรือสื่อลามกทางเครือข่ายอินเทอร์เน็ต (Title 18 U.S.C. § 1466A) ซึ่งการกระทำความไม่ว่าจะเป็นการจำหน่าย การรับหรือส่งต่อ ถ่ายทอด การแสดงออกโดยภาพวาด การ์ตูน ประติมากรรม หรือโดยจิตรกรรม ที่แสดงถึงการร่วมเพศอย่างชัดเจน ทั้งนี้ สื่อลามกยังรวมถึง

---

[34] พิรงรอง รามสูต รณะนันทน์ และนิธิมา คณานิธินันท์, รายงานวิจัยฉบับสมบูรณ์เรื่อง การกำกับดูแลเนื้อหาอินเทอร์เน็ต (โครงการ "การปฏิรูประบบสื่อ: การกำกับดูแลเนื้อหาโดยรัฐ การกำกับดูแลตนเอง และสื่อภาคประชาชน"), มีนาคม 2547, หน้า 12.

ภาพหรือสิ่งต่างๆที่แสดงออกถึงการมีเพศสัมพันธ์หรือการล่วงละเมิดทางเพศโดยใช้อวัยวะส่วนอื่นอีกด้วย

3.1.2.2 **มาตรการทางสบัญญัติ**

หลักเกณฑ์ในการนำตัวผู้กระทำความผิดมาลงโทษนี้ได้กำหนดไว้ในกฎหมาย Can Spam Act of 2003 เมื่อผู้ส่งจดหมายโฆษณากระทำการฝ่าฝืนบทบัญญัติของกฎหมาย ศาลจะนำตัวผู้กระทำความผิดมาลงโทษได้ต้องปรากฏว่าศาลมีเขตอำนาจเหนือตัวผู้ส่งจดหมายอิเล็กทรอนิกส์ (Personal Jurisdiction) ซึ่งการส่งจดหมายโฆษณาดังกล่าวสามารถส่งไปยังผู้รับได้ทั่วทุกมุมโลก ผู้เขียนจึงเห็นว่าอาจสามารถนำหลักเกณฑ์ในกฎหมายดังกล่าวมาปรับใช้กับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้เช่นกัน โดยกฎหมายดังกล่าวหลักเกณฑ์ ดังนี้

ก. เขตอำนาจศาล

เขตอำนาจศาลโดยทั่วไปของประเทศสหรัฐอเมริกา แบ่งได้ 2 กรณี

กรณีที่ 1 เขตอำนาจศาลในแง่ของอำนาจศาล ซึ่งหมายถึง อำนาจในการพิจารณาคดีของศาล โดยพิจารณาจากเนื้อหาสาระของคดี ว่าศาลมีอำนาจที่จะรับฟ้องหรือไม่เพียงใด และ

กรณีที่ 2 เขตอำนาจศาลในแง่ของเขตศาล ซึ่งหมายถึง พื้นที่หรือท้องที่ทางภูมิศาสตร์ที่ศาลมีอำนาจพิจารณาคดีและอำนาจตามชั้นของศาล ในส่วนนี้ ผู้เขียนจะกล่าวถึงเขตอำนาจศาลในแง่ของอำนาจศาลในการพิจารณาคดี ซึ่งศาลได้วางหลักกฎหมายในการพิจารณา ดังนี้

หลักเกณฑ์ในการกำหนดเขตอำนาจศาลกรณีดั้งเดิม การกำหนดเขตอำนาจของศาลในการพิจารณาคดีอาจแบ่งได้[35] ดังนี้

(1) เขตอำนาจศาลโดยทั่วไป เป็นเขตอำนาจศาลที่พิจารณาจากความเกี่ยวพันของผู้ถูกฟ้องคดีกับเขตอำนาจศาล โดยผู้ถูกฟ้องคดีปรากฏอยู่ในเขตอำนาจศาล หรือมีการติดต่ออยู่ในเขตอำนาจศาลนั้น เช่น มีถิ่นที่อยู่หรือภูมิลำเนาหรือเป็นผู้มีสัญชาติ หรือมี

---

[35] Media Law Resource Center, Inc. Matthew E. Babcock, Wesley R. Powell, Madeleine Schachter, Andrew J. Schell and David A. Schulz. Internet Jurisdiction, Choice of Law Issues, [Online]. 2001. Available from: http://www.medialaw.org/Template.cfm?Section=Archive7&Template=/ContentManagement/ContentDisplay.cfm&ContentID=1065. [2009, July 20]

ทรัพย์สินอยู่ในดินแดนของรัฐ หรืออย่างน้อยต้องมีความสัมพันธ์บางอย่างกับรัฐอย่างเป็นระบบและต่อเนื่อง

(2) เขตอำนาจศาลโดยเฉพาะ เป็นเขตอำนาจศาลที่พิจารณาจากมูลคดีโดยผู้ถูกฟ้องคดีมิได้ปรากฏอยู่ในเขตอำนาจศาลในรัฐนั้น และไม่มีความเกี่ยวกันกับรัฐนั้นโดยตรง แต่มีการกระทำซึ่งมุ่งประสงค์ต่อรัฐนั้น หรือมีความมุ่งหมายต่อรัฐนั้น ซึ่งในการฟ้องคดีต้องแสดงให้เห็นว่าผู้ถูกฟ้องคดีมีความสัมพันธ์ขั้นต่ำ ต่อเขตอำนาจศาลในรัฐนั้น การใช้เขตอำนาจศาล โดยเฉพาะนี้ ศาลได้ขยายอำนาจของตนเหนือผู้ถูกฟ้องคดีที่มิได้อยู่ในรัฐนั้น ดังนั้นศาลจึงต้องคำนึงถึงการต่อสู้คดีของผู้ถูกฟ้องคดีด้วย โดยจะต้องไม่เป็นการฝ่าฝืนหลักการดำเนินกระบวนพิจารณาที่ชอบตามรัฐธรรมนูญ กล่าวคือ การกล่าวอ้างเขตอำนาจศาลของตนต้องไม่ฝ่าฝืนต่อหลักการดำเนินการอย่างเป็นธรรมและเคารพต่อความยุติธรรมโดยเคร่งครัด (Fair play and substantial Justice)[36]

ศาลได้วางหลักเกณฑ์การใช้เขตอำนาจเหนือจำเลยที่ไม่มีภูมิลำเนาในประเทศไว้ในคดีต่างๆ เช่น คดี Pennoyer v. Neff 95 U.S. 714 (1877)[37] กล่าวคือ ต้องปรากฏว่าจำเลยปรากฏอยู่ในเขตที่ศาลตั้งอยู่และสามารถส่งหมายและคำฟ้องให้แก่จำเลยได้

อย่างไรก็ดี ในเวลาต่อมาจำเลยมักหลบหนีออกไปจากเขตที่ศาลตั้งอยู่เพื่อมิให้ถูกฟ้องคดีได้ ศาลจึงได้วางหลักเกณฑ์การใช้เขตอำนาจศาลกรณีที่จำเลยไม่ปรากฏในเขตอำนาจศาลในคดี International Shoe Co v. Washington 326 U.S. 310 (1945)[38] โดยคดีนี้ ศาลสูงของรัฐวอชิงตันใช้เขตอำนาจศาลเหนือบริษัทอินเตอร์เนชั่นแนล ชูส์ ที่มิได้เกี่ยวข้องกับรัฐวอชิงตัน ศาลสูงของสหรัฐอเมริกาเห็นว่า ศาลสูงของรัฐวอชิงตันมีเขตอำนาจเหนือบริษัทเพราะบริษัทได้ทำธุรกรรมในรัฐวอชิงตันโดยรับคำสั่งซื้อสินค้าจากลูกค้าในรัฐวอชิงตัน ทำให้บริษัทมี

---

[36] Gerald R. Ferrera, Cyber Law Text and Cases (Cincinnati, Ohio: West/Thomson Learning, 2001), p 18-21 อ้างถึงใน จันทร์พิมพ์ บรรจงจิตร์ และปกรณ์ ยิ่งวรการ, รายงานวิจัยฉบับสมบูรณ์ เรื่อง กฎหมายป้องกัน Spam Mail ของสหรัฐอเมริกา, หน้า 41.

[37] FindLaw. a Thomson Reuters business. U.S. Supreme Court PENNOYER v. NEFF, 95 U.S. 714 (1877) 95 U.S. 714 PENNOYER v. NEFF. http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?linkurl=%3C%linkurl%%3E&graphurl=%3C%graphurl%%3E&friend=%3C%20riend%%3E&court=us&vol=95&invol=714 . อ้างถึงใน จันทร์พิมพ์ บรรจงจิตร์ และปกรณ์ ยิ่งวรการ, รายงานวิจัยฉบับสมบูรณ์ เรื่อง กฎหมายป้องกัน Spam Mail ของสหรัฐอเมริกา, หน้า 41.

[38] เรื่องเดียวกัน, หน้า 42.

ความสัมพันธ์ขั้นต่ำ (Minimum Contacts) กับเขตอำนาจศาลวอชิงตันและทำให้การฟ้องคดีไม่ขัดต่อหลักการดำเนินกระบวนพิจารณาที่ชอบธรรม

นอกจากนี้ในคดี Calder v. Jones 469 U.S. 783 (1984)[39] ข้อเท็จจริงคือ โจทก์อาศัยและทำงานอยู่ในรัฐแคลิฟอร์เนีย ส่วนจำเลยอาศัยและทำงานอยู่ในรัฐฟลอริด้า จำเลยได้รายงานข่าวโดยเขียนและแก้ไขบทความลงในหนังสือพิมพ์ National Enquirer ซึ่งมีการเผยแพร่ที่รัฐแคลิฟอร์เนีย ศาลว่ารัฐแคลิฟอร์เนียมีเขตอำนาจ เนื่องจากการกระทำของจำเลยมีการกระทำซึ่งมุ่งประสงค์ (Purposefully directed) เพื่อให้เกิดความเสียหายแก่ชื่อเสียงของโจทก์ที่รัฐแคลิฟอร์เนีย ซึ่งคดีนี้ศาลได้วางหลักเกณฑ์เกี่ยวกับความสัมพันธ์ขั้นต่ำ (Minimum Contacts) ไว้ว่าต้องพิจารณาถึง

1. จำเลยที่ไม่มีภูมิลำเนาได้กระทำหรือทำธุรกรรมที่เสร็จสิ้นในเขตอำนาจศาล หรือได้ปฏิบัติเพื่อให้ได้ประโยชน์ตามความประสงค์ของจำเลย (Purposefully availment)

2. การเรียกร้องต่อจำเลยเกิดขึ้นหรือเป็นผลมาจากการกระทำของจำเลย

3. มีความสัมพันธ์ในสาระสำคัญระหว่างการกระทำของจำเลยกับเขตอำนาจของศาลที่จะใช้เขตอำนาจเหนือจำเลยอย่างสมเหตุสมผล การใช้เขตอำนาจศาลเหนือจำเลยที่ไม่มีภูมิลำเนาในเขตอำนาจศาลจะต้องทำอย่างสมเหตุสมผล เนื่องจากต้องคำนึงถึงความยุติธรรมหรือความสะดวกของจำเลยที่จะถูกฟ้องคดียังสถานที่อื่นนอกภูมิลำเนาของจำเลยด้วย ดังนี้ศาลจึงต้องพิจารณาถึงภาระของจำเลยในการต่อสู้คดี การปรับใช้กฎหมายของศาล การได้รับชดใช้ความเสียหายของโจทก์ และประโยชน์ของรัฐอื่นในการตัดสินคดีได้อย่างมีประสิทธิภาพ

หลักเกณฑ์ในการกำหนดเขตอำนาจศาลกรณีอินเทอร์เน็ต ศาลได้ใช้หลักเกณฑ์ในการพิจารณาเขตอำนาจศาลกรณีดั้งเดิมมาปรับใช้กับกรณีอินเทอร์เน็ต โดยศาลอาจกำหนดเขตอำนาจศาลเหนือจำเลยที่ไม่มีภูมิลำเนาได้ ดังนี้[40]

---

[39] J.T. Westermeier Personal Jurisdiction: Today' s Hot Issue In E-Commerce, http://www.elj.warwick.ac.uk/jilt/98-3/westermrier.html, 24 February 2005. อ้างถึงใน จันทร์พิมพ์ บรรจงจิตร์ และปกรณ์ ยิ่งวรการ, รายงานวิจัยฉบับสมบูรณ์ เรื่อง กฎหมายป้องกัน Spam Mail ของสหรัฐอเมริกา, หน้า 41.

[40] Media Law Resource Center, Inc. Matthew E. Babcock, Wesley R. Powell, Madeleine Schachter, Andrew J. Schell and David A. Schulz. supra note 24.

1. จำเลยมีความสัมพันธ์โดยรวมในเขตอำนาจศาล ซึ่งกรณีที่จะถือว่ามีความสัมพันธ์โดยรวมนั้น ศาลได้วางหลักเกณฑ์กรณีของการเผยแพร่ทางเว็บไซต์ เช่น

คดี Compuserve, Inc. V Patterson 89 F.3d 1257 (1996)[41] คดีนี้โจทก์เป็นผู้ให้บริการอินเทอร์เน็ตมี shareware อยู่ที่รัฐโอไฮโอ จำเลยมีภูมิลำเนาอยู่ในรัฐเท็กซัส จำเลยได้ขายโปรแกรมคอมพิวเตอร์ผ่าน shareware ของโจทก์อยู่ที่รัฐโอไฮโอ โจทก์ฟ้องคดีต่อจำเลยที่ศาลรัฐโอไฮโอ เนื่องจากจำเลยละเมิดเครื่องหมายการค้าโดยการขายโปรแกรมคอมพิวเตอร์ซึ่งมีสินค้าเหมือนที่โจทก์ขาย จำเลยปฏิเสธว่าศาลไม่มีเขตอำนาจ คดีนี้ศาลเห็นว่าศาลมีเขตอำนาจเหนือจำเลยเนื่องจาก จำเลยได้กระทำให้เกิดประโยชน์ตามความประสงค์การทำธุรกิจในรัฐโอไฮโอ มูลคดีเกิดจากการกระทำของจำเลย และการกระทำและผลแห่งการกระทำของจำเลยมีความเกี่ยวพันในสาระสำคัญอย่างเพียงพอที่ศาลจะสามารถใช้เขตอำนาจเหนือจำเลย

คดี Zippo Mfg Co. V. Zippo Dot Com,Inc. 952 F. Supp. 1991 (W.D. Pa. 1997)[42] ศาลได้พิจารณาเขตอำนาจศาลจากการกระทำโดยเว็บไซต์ ซึ่งศาลได้แบ่งเว็บไซต์เป็นสองประเภท คือเว็บไซต์ที่มีการติดต่อสื่อสารกันระหว่างผู้รับข้อมูลกับเว็บไซต์นั้นได้ ลักษณะของเว็บไซต์นี้ เช่น เว็บไซต์ที่ใช้ในการติดต่อสื่อสารทางธุรกิจ โดยมีการทำสัญญาเกิดขึ้นโดยใช้สื่ออินเทอร์เน็ตยังภูมิลำเนาของเขตอำนาจศาลต่างประเทศและมีการส่งผ่านข้อมูลซ้ำของคอมพิวเตอร์ยังศาลที่อ้างเขตอำนาจ และอีกกรณีคือเว็บไซต์ที่มีการส่งข้อมูลโดยใช้สื่ออินเทอร์เน็ต โดยผู้ใช้สามารถอ่านได้ในเขตอำนาจศาลแต่ไม่สามารถติดต่อสื่อสารโดยการโต้ตอบกับเขตอำนาจศาลนั้นได้ ซึ่งการที่ศาลจะอ้างเขตอำนาจเหนือการกระทำนั้นได้ โดยหลักต้องเป็นเว็บไซต์ที่มีลักษณะของการติดต่อสื่อสารตลอดเวลา

คดี Smith V. Hobby Lobby Stoves 968F. Supp 1356 (W.D.Ark.1997)[43] จำเลยซึ่งเป็นชาวฮ่องกงได้ผลิตต้นคริสมาสต์เทียมและได้ประกาศขายโฆษณาทางอินเทอร์เน็ตแต่มิได้มีการขายสินค้าหรือบริการในรัฐอาคันซอ ส่วนห้าง Hobby เป็น

---

[41] Gerald R. Ferrera, supra note 25, pp. 27-29.

[42] The Journal Of The Torts, Insurance And Compensation Law Section Of The New York State Bar Association. Thomas A. Dickerson. 2000. Consumer Law : The Internet and Its Impact upon Personal Jurisdiction[Online]. Available from: http://www.courts.state.ny.us/tandv/JurisdictionAndTheInternet.htm#anchor4367[2009, May 23]

[43] Social Science Electronic Publishing, Inc. University of Cincinnati Law Review, Vol. 66, No. 2, 1998 . 2007. Katherine C. Sheehan . Predicting the Future: Personal Jurisdiction for the Twenty-First Century[Online]. Available from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=139231##[2009, May 23]

ผู้ขายต้นคริสมาสต์ดังกล่าว ปรากฏว่าต้นคริสมาสต์เทียมเกิดเพลิงไหม้ เป็นเหตุให้มีบุคคลถึงแก่ความตาย ห้าง Hobby มีสำนักงานที่รัฐโอกลาโฮมา และมีสาขาที่รัฐอาคันซอ จำเลยมิได้มีการติดต่อกับห้างที่รัฐอาคันซอ โดยจะติดต่อเฉพาะที่รัฐโอกลาโฮมาเท่านั้น ห้าง Hobby ทำให้จำเลยมีความสัมพันธ์ขั้นต่ำ ศาลเห็นว่าคดีนี้ จำเลยเพียงโฆษณาสินค้าผ่านเว็บไซต์ มิได้มีการทำ สัญญาขายสินค้าหรือบริการแก่คนในรัฐอาคันซอในเว็บไซต์แต่อย่างใด ศาลจึงปฏิเสธการใช้เขตอำนาจเหนือจำเลย

คดี Maritz., Inc V. Cybergold, Inc., 947 F.Supp.1328 (E.D.Mo.1996)[44] คดีนี้จำเลยได้โฆษณาทางเว็บไซต์มีคอมพิวเตอร์เซิร์ฟเวอร์ที่รัฐแคลิฟอร์เนีย และให้บริการกลุ่มจดหมายส่งให้แก่ลูกค้าผ่านทางจดหมายอิเล็กทรอนิกส์ ศาลกล่าวว่าการกระทำของจำเลยแม้อยู่นอกรัฐมิสซูรี่ แต่เมื่อพิจารณาถึงลักษณะของกิจกรรมที่เกิดในเว็บไซต์และอินเทอร์เน็ต แล้วเห็นว่า จำเลยทำเว็บไซต์เพื่อให้ผู้ใช้บริการเข้ามามีส่วนร่วมได้ในรัฐมิสซูรี่ และให้บริการกลุ่มจดหมายเว็บไซต์ที่มีโปรแกรมอัตโนมัติในการตอบสนองแก่ผู้เข้ามาใช้บริการ และจำเลยก็ส่งโฆษณาโดยรู้ให้แก่ผู้เข้าชม การเสนอขายหรือประกาศดังกล่าวก่อให้เกิดความสัมพันธ์ขั้นต่ำ ซึ่งเพียงพอที่ศาลจะใช้เขตอำนาจเหนือจำเลยที่ไม่มีภูมิลำเนาในเขตอำนาจศาล ดังนั้นหากจำเลยก่อให้เกิดความเสียหายในรัฐมิสซูรี่ ทำให้ศาลมิสซูรี่มีเขตอำนาจเหนือจำเลย และสอดคล้องกับการใช้หลักการดำเนินกระบวนพิจารณาที่ชอบธรรมตามรัฐธรรมนูญ

2. การกระทำก่อให้เกิดผลในเขตอำนาจศาล การพิจารณาเรื่องผลของการกระทำนั้นโจทก์หรือผู้เสียหายต้องพิสูจน์ให้ศาลเห็นว่า มีการเผยแพร่ข้อมูลมายังเขตอำนาจศาล ซึ่งผู้กระทำรู้ว่าผลจะเกิดและต้องการให้เกิดผลโดยมีการกระทำมุ่งประสงค์ต่อรัฐนั้น และโจทก์ได้รับความเสียหายจากการกระทำดังกล่าว เช่น

คดี Blumental V. Druge 992 F. Supp. 44 (D.D.C.1998)[45] คดีนี้ จำเลยได้เขียนข้อความหมิ่นประมาทโจทก์ไว้ในเว็บไซต์ของจำเลย ศาลในรัฐโคลัมเบียเห็นว่า ศาลมีเขตอำนาจเพราะจำเลยได้กระทำการให้เกิดผลในเขตอำนาจศาลรัฐโคลัมเบีย โดยเว็บไซต์ของจำเลยสามารถแลกเปลี่ยนข้อมูลผู้ใช้บริการอินเทอร์เน็ตได้ (Active Sites) และมีการส่งจดหมายอิเล็กทรอนิกส์เก็บค่าสมาชิกจากผู้ใช้ในรัฐโคลัมเบียที่เข้าชมเว็บไซต์ด้วย

---

[44] Cyberspace Law Institute. 1998. David G. Post. Personal Jurisdiction on the Internet - A Survey of the Cases[Online]. Available from: http://cyber.law.harvard.edu/metaschool/fisher/domain/dncases/zippo.htm[2009, May 23]

[45] Matthew E. Babcock, Wesley R. Powell, Madeleine Schachier, Andrew J.Scheil and David A. Schulz, supra note 24.

3. มีหลักฐานมาแสดงได้ว่ามีการเผยแพร่ข้อมูลโดยตั้งใจและต่อเนื่อง โดยมีเป้าหมายที่เขตอำนาจศาลนั้น การใช้อำนาจของศาลต้องแสดงให้เห็นได้ว่า จำเลยได้เผยแพร่ข้อความเหล่านั้นมาอย่างต่อเนื่องโดยเจตนาในเขตอำนาจศาล โดยมีประโยชน์ตามความประสงค์ให้เกิดในเขตอำนาจศาลนั้น ศาลได้วางหลักไว้ในคดีต่างๆ เช่น

คดี World Wide Volkswagen V. Woodson 444 U.S. 286 (1980)[46] คดีนี้ โจทก์ฟ้องคดีต่อศาลรัฐโอกลาโอมา เนื่องจากซื้อของมาจากจำเลยมีความบกพร่องและเกิดอุบัติเหตุในรัฐดังกล่าว จำเลยปฏิเสธเขตอำนาจศาลของรัฐโอกลาโฮมา คดีนี้ศาลเห็นว่าโอกลาโฮมาไม่มีเขตอำนาจเนื่องจาก จำเลยมิได้มุ่งหมายให้เกิดความเสียหายเกิดขึ้นรัฐนั้น

คดีนี้ศาลพิจารณาว่าจำเลยมีการเผยแพร่ข้อมูลโดยตั้งใจและต่อเนื่องโดยมีเป้าหมายที่เขตอำนาจศาลหรือไม่นั้น เช่น

คดี Weber V. Jolly Hotels. 977 F. Supp 327 (O.N.J. 1997)[47] จำเลยเป็นบริษัทอิตาลี โจทก์ได้รับบาดเจ็บจากการเข้าพักในโรงแรมจำเลยในอิตาลี จำเลยมิได้ทำธุรกิจใดๆในรัฐนิวเจอร์ซี แต่จำเลยได้เผยแพร่เว็บไซต์แสดงรูปภาพโรงแรมของจำเลยในประเทศอิตาลี ประกอบด้วยภาพห้องพักสิ่งอำนวยความสะดวกต่างๆ ข้อมูลของจำนวนห้องและเบอร์โทรศัพท์ติดต่อ ศาลในคดีนี้เห็นว่า การที่จำเลยเผยแพร่โฆษณาในเว็บไซต์มีลักษณะเช่นเดียวกับการเผยแพร่ทางนิตยสาร และไม่ก่อให้เกิดการติดต่ออย่างต่อเนื่องและพอสมควร ทั้งนี้ การกระทำของจำเลยไม่ได้กระทำโดยก่อให้เกิดประโยชน์ตามความประสงค์ของจำเลย ศาลจึงไม่มีเขตอำนาจศาลเหนือจำเลยในคดีนี้ และหากศาลใช้อำนาจดังกล่าวย่อมเป็นการละเมิดหลักการดำเนินกระบวนพิจารณาที่ชอบตามรัฐธรรมนูญ (Due Process)

คดี Resuscitation Technologies, Inc V. Continental Health Care Corp. , 1997 U.S. Dist. LEXIS 3532 (S.D. Ind. March 24, 1997)[48] โจทก์เป็นบริษัทในรัฐอินเดียนาขายอุปกรณ์ทางการแพทย์ จำเลยไม่มีสำนักงานและมิได้ทำธุรกิจในรัฐอินเดียนา จำเลยได้ติดต่อโจทก์ผ่านทางจดหมายอิเล็กทรอนิกส์กว่า 80 ฉบับและทางโทรศัพท์จำนวน 2

---

[46] Gerald R. Ferrera, supra note 25, p. 23

[47] J.T. Westermeier Personal Jurisdiction: Today' s Hot Issue In E-Commerce, supra note 28, และดู ผาสุก เจริญเกียรติ, เขตอำนาจศาลเหนือข้อพิพาททางอินเทอร์เน็ต, บทบัณฑิตย์, เล่ม 58, ตอน 2, หน้า 28-29, (มิถุนายน 2545).

[48] Martin H. Samson. Internet Library of Law and Court Decisions. Resuscitation Technologies Inc. v. Continental Health Care Corp. IP 96-1457-C-M/S, 1997 U.S. Dist. Lexis 3523 (So. Dist. Indiana, March 24, 1997). [Online]. Available from: http://www.internetlibrary.com/cases/lib_case183.cfm[2010, January 11]

ครั้ง และจำเลยได้เสนอทำข้อตกลงลับที่จะร่วมกิจการกับโจทก์นอกอินเดียนา ต่อมาโจทก์ยกเลิกการเจรจา จำเลยกล่าวหาว่าโจทก์ละเมิดข้อตกลง โจทก์โต้แย้งว่ายังไม่มีความสัมพันธ์ทางสัญญาระหว่างคู่เจรจา จำเลยขอให้ยกฟ้องเพราะศาลไม่มีเขตอำนาจ ศาลอินเดียนาบอกว่าศาลมีเขตอำนาจเนื่องจาก มีการติดต่อสื่อสารทางจดหมายอิเล็กทรอนิกส์จำนวนมากและต่อเนื่องในช่วงเดือนนั้น

การกำหนดหลักเกณฑ์การนำตัวผู้กระทำความผิดมาลงโทษ เกี่ยวข้องกับการใช้จดหมายอิเล็กทรอนิกส์ในการไม่ปฏิบัติให้เป็นไปตามข้อกำหนดของกฎหมายในการส่งข้อความในจดหมายอิเล็กทรอนิกส์ ซึ่งหากนำแนวคำพิพากษาของศาลในคดีต่างๆมาปรับใช้กับการกระทำความผิดแล้วอาจพิจารณาตามได้ ดังนี้

1. กรณีผู้กระทำความผิดอยู่ในประเทศสหรัฐอเมริกา ได้กระทำความผิดต่อบุคคลที่อยู่ในประเทศสหรัฐอเมริกา แสดงให้เห็นว่า ผู้กระทำความผิดมีความเกี่ยวพันกันกับเขตอำนาจศาล โดยปรากฏอยู่ในเขตอำนาจศาล เนื่องจากได้กระทำความผิดโดยมีถิ่นที่อยู่ในประเทศสหรัฐอเมริกา กรณีดังกล่าว ศาลจึงมีเขตอำนาจทั่วไป (General Jurisdiction) เหนือผู้กระทำความผิด และสามารถนำตัวผู้กระทำความผิดมาลงโทษได้

2. กรณีผู้กระทำความผิดอยู่ในประเทศสหรัฐอเมริกา กระทำความผิดต่อบุคคลที่อยู่นอกประเทศสหรัฐอเมริกา เมื่อบุคคลที่อยู่นอกประเทศสหรัฐอเมริกาได้รับความเสียหาย การที่บุคคลที่อยู่นอกประเทศสหรัฐอเมริกาจะฟ้องคดีให้ผู้กระทำความผิดได้รับโทษตามกฎหมายนั้น จะต้องฟ้องคดีต่อศาลในประเทศสหรัฐอเมริกาและตกอยู่ภายใต้หลักเกณฑ์เขตอำนาจศาล และการที่ผู้กระทำความผิดได้กระทำความผิดโดยมีถิ่นที่อยู่ในประเทศสหรัฐอเมริกา ผู้กระทำความผิดจึงมีความเกี่ยวพันกับเขตอำนาจศาลที่ปรากฏอยู่ในเขตอำนาจศาลแล้ว และทำให้ศาลมีเขตอำนาจทั่วไป (General Jurisdiction) เหนือผู้กระทำความผิดและสามารถนำตัวผู้กระทำความผิดมาลงโทษได้

3. กรณีผู้กระทำความผิดอยู่นอกประเทศสหรัฐอเมริกา กระทำความผิดต่อบุคคลที่อยู่ในประเทศสหรัฐอมเริกา แสดงให้เห็นว่า ผู้กระทำความผิดมิได้มีความเกี่ยวพันกับเขตอำนาจศาลโดยตรง ซึ่งศาลจะใช้เขตอำนาจเหนือตัวจำเลยได้นั้น จะเป็นไปตามหลักของการกำหนดเขตอำนาจศาลโดยเฉพาะ (Specific Jurisdiction) กล่าวคือ ต้องปรากฏว่า จำเลยมีความสัมพันธ์โดยรวมอยู่ในเขตอำนาจศาลนั้น การกระทำก่อให้เกิดผลในเขตอำนาจศาลโดยการเผยแพร่ข้อมูลมายังเขตอำนาจศาลโดยมุ่งประสงค์ต่อรัฐนั้น (Purposefully Directed) และมีการเผยแพร่ข้อมูลโดยตั้งใจและต่อเนื่อง มีเป้าหมายให้ผลแห่งการกระทำความผิดเกิดในเขต

อำนาจศาลหรือมีผลประโยชน์ตามความประสงค์ (Purposefully Availment) เกิดขึ้นในเขตอำนาจศาล

ดังนั้น ในการนำตัวผู้กระทำความผิดมาลงโทษ ผู้เสียหายก็จะต้องพิสูจน์ให้ศาลเห็นถึงเหตุที่ศาลจะสามารถใช้เขตอำนาจเหนือตัวผู้กระทำความผิดที่อยู่นอกประเทศสหรัฐอเมริกา คือ ผู้กระทำความผิดนั้นมีความสัมพันธ์ขั้นต่ำ (Minimum Contacts) กับเขตอำนาจศาล การกระทำความผิดก่อให้เกิดผลในเขตอำนาจศาลโดยผู้กระทำความผิดได้มีประโยชน์ตามความประสงค์เกิดในเขตอำนาจศาล ซึ่งศาลก็จะพิจารณาการใช้เขตอำนาจศาลโดยเฉพาะ (Specific Jurisdiction) เหนือผู้กระทำความผิด และต้องพิจารณาด้วยว่า การใช้เขตอำนาจศาลกรณีดังกล่าวต้องไม่ฝ่าฝืนหลักการดำเนินกระบวนพิจารณาที่ชอบธรรมตามรัฐธรรมนูญ

ทั้งนี้ นอกจากการพิจารณาว่าศาลว่าเขตอำนาจ เหนือผู้กระทำความผิดที่ส่งจดหมายโฆษณาแล้ว การนำตัวผู้กระทำความผิดมาลงโทษต้องพิจารณาเขตอำนาจศาลในแง่ของเขตอำนาจศาลทางภูมิศาสตร์ด้วย

3.1.3 ปัญหาและอุปสรรคในการปฏิบัติตามพันธกรณีแห่งอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001

จากการลงนามและให้สัตยาบันอนุสัญญาดังกล่าว ก่อได้เกิดปัญหาและอุปสรรคในการปฏิบัติตามพันธกรณีแห่งอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 ในประเด็นปัญหาเกี่ยวกับสิทธิมนุษยชน

เนื่องจากหลายๆ องค์กรที่ทำงานด้านสิทธิมนุษยชนในประเทศสหรัฐอเมริกาได้มีการพูดถึงเนื้อหาของอนุสัญญานี้ ไม่ว่าจะเป็น Global Internet Liberty Campaign หรือ American Civil Liberties Union ที่ทำการรณรงค์คัดค้านและต่อต้านอนุสัญญา ด้วยเหตุผลที่ว่าอนุสัญญานี้จะคุกคามอย่างร้ายแรงต่อสิทธิทั้งหลายของประชาชนตามที่ได้กำหนดไว้ในรัฐธรรมนูญ ซึ่งองค์กรเหล่านี้ต้องการให้สิทธิส่วนบุคคลมีความสอดคล้องกันกับบัญญัติกฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ อย่างไรก็ตามองค์กรดังกล่าวยังคงเห็นว่าอนุสัญญาฉบับนี้จะมีผลกระทบต่อการคุ้มครองข้อมูลส่วนบุคคลและสิทธิเสรีภาพในการแสดงความคิดเห็น[49]

---

[49] Westlaw. Sara L. Marler. New England School of Law. 2002. The Convention on Cyber-crime : should the United States ratify?[Online]. Available from: http://web2.westlaw.com/result/documenttext.aspx?rs=WLW9.06&ss=CNT&rp=%2fWelcome%2fWorldJour

เช่น กรณีสุนทรพจน์แห่งความเกลียดชัง (Hate Speech) ที่ถือว่าเป็นการแสดงความคิดเห็นในจังหวะการชุมนุม เรียกร้อง แสดงความคิดเห็นในที่สาธารณะสามารถพบเห็นผู้กล่าวปราศรัยที่คอยผลัดเปลี่ยน หมุนเวียนสลับบทบาทขึ้นบนเวทีอย่างสม่ำเสมอ วัตถุประสงค์ของการกล่าวปราศรัย คือเพื่อแสดงจุดยืนทางความคิด รวมทั้งพูดให้ผู้ชุมนุมเกิดความคึกคึ้น บางครั้งจึงมีการใช้ถ้อยคำหยาบคายและพูดเข้าข่ายการละเมิด ดูหมิ่นหรือประณามกระทำของฝ่ายที่ถูกตั้งให้เป็นปรปักษ์ก็เพื่อสร้างแรงจูงใจให้กับฝ่ายตน[50]

คำกล่าวเหล่านั้นถูกเรียกว่า Hate Speech หรือ สุนทรพจน์แห่งความเกลียดชัง หมายถึง คำจำกัดความของการกล่าวโจมตี แสดงความดูถูกกลุ่มคนเพราะสถานะที่แตกต่างในสังคมหรือความแตกต่างทางเชื้อชาติของพวกเขา ดังเช่น การเหยียดหยามชนชาติ การข่มเหงทางเพศ การนำเอาเรื่องของอายุ เชื้อ ชาติเผ่าพันธุ์ ศาสนา มาเป็นประเด็นโจมตี ไม่ว่าจะเป็นการเบี่ยงเบนทางเพศ ความทุพพลภาพของร่างกาย ความสามารถทางภาษา อุดมการณ์ทางความคิด ชนชั้นทางสังคม หรือลักษณะที่ปรากฏบางอย่าง เช่น ทรงผม ความสูง น้ำหนัก สีผิว เป็นต้น คำจำกัดความนี้ครอบคลุมถึงการเขียน การใช้วาจาและพฤติกรรมซึ่งแสดงออกต่อสาธารณะด้วย ทั้งนี้ คำดูถูก เหยียดหยามทั้งหลายนี้ ในหลายประเทศมีบทลงโทษเป็นการเฉพาะอย่างกฎหมาย ที่เรียกว่า Sedition Act ในประเทศสหรัฐอเมริกา ที่มีบทลงโทษจำคุกสูงถึง 2 ปี การกระทำผิดใดที่พูดหรือเผยแพร่โดยการเขียนหรือบทความที่ต่อต้านรัฐบาลของสหรัฐอเมริกา รัฐสภาหรือประธานาธิบดีด้วยเจตนาที่จะดูหมิ่น ดูถูกหรือแสดงความจงเกลียดจงชัง หากทำการพิจารณาจะเห็นว่ากฎหมายนี้มีไว้เพื่อป้องกันและปกป้องการกระทำละเมิดต่อผู้อื่นอันอาจก่อให้เกิดความไม่ปรองดองและสมานฉันท์ มิใช่กฎหมายเพื่อการส่งเสริมให้มุ่งเอาผิดหรือเอาความเพื่อล้างแค้นในบริบทของสังคมที่เปลี่ยนไป

เห็นได้สิทธิเสรีภาพในการแสดงความคิดเห็นก็เป็นสิทธิอย่างหนึ่งที่ประเทศสหรัฐอเมริกาทำการคุ้มครอง แต่สิทธิส่วนบุคคลที่กฎหมายทำการคุ้มครองนั้นจะต้องพิจารณาว่าเป็นสิทธิที่กำหนดไว้ในรัฐธรรมนูญหรือไม่ ก่อนที่จะกล่าวถึงว่าอนุสัญญานี้มีส่วนที่ละเมิดสิทธิส่วนบุคคล

---

nals%2fdefault.wl&origin=Search&sv=Split&cfid=1&fn=_top&rlt=CLID_QRYRLT233757561014 6&n=6&sskey=CLID_SSSA8346535610146&mt=WorldJournals&eq=Welcome%2fWorldJournals&method=WIN&query=convention+cyber+crime&effdate=1%2f1%2f0001+12%3a00%3a00+AM&db=WORLD-JLR%2cLAWREV-PRO%2cCLMLR%2cHVLR%2cYLJ%2cAMJIL%2cASPAMLJ%2cSTJIL%2cECLR%2cEURLR&rlti=1&vr=2.0&fmqv=c&service=Search&cnt=DOC&scxt=WL&cxt=RL&rltdb=CLID_DB772995356101 46&utid=%257#FN:B290[2009, June 15]

[50] สำนักงานพัฒนาสังคมและความมั่นคงของมนุษย์จังหวัดพะเยา. 2552. [Online]. แหล่งข้อมูล: http://www.phayao.m-society.go.th/main/docs/notice/2009/10/03children-phayao_20oct09.pdf. [2553, มกราคม 11]

ผู้เขียนเห็นว่าควรจะต้องพิจารณาถึงที่มาของสิทธิส่วนบุคคลเหล่านี้ของประเทศสหรัฐอเมริกาว่าเป็นสิทธิขั้นพื้นฐานตามที่กฎหมายกำหนดหรือไม่ โดยขอยกตัวอย่างในคดีดังต่อไปนี้

คดี Griswold V. Connecticut[51] เป็นกรณีที่เกี่ยวข้องกับการดำเนินคดีอาญาของ Estelle Griswold ซึ่งเป็นแพทย์และดำรงตำแหน่งเป็นผู้อำนวยการศูนย์การวางแผนครอบครัว โดย Griswold ถูกดำเนินคดีเกี่ยวกับการจำหน่ายยาคุมกำเนิดให้กับหญิงที่แต่งงานแล้ว ซึ่งการจำหน่ายยาคุมกำเนิดดังกล่าวนั้นถือได้ว่าเป็นความผิดภายใต้กฎหมายของรัฐ Connecticut ในขณะนั้น ซึ่งศาลฎีกาได้ตัดสินว่า กฎหมายของรัฐ Connecticut ในเรื่องที่ห้ามจำหน่ายและใช้ยาคุมกำเนิดนั้นไม่ถูกต้องและขัดกับรัฐธรรมนูญโดยให้เหตุผลว่าเป็นการละเมิดสิทธิส่วนบุคคลและสิทธิส่วนบุคคลดังกล่าวเป็นสิทธิขั้นพื้นฐาน โดยสิ่งสำคัญที่ต้องตระหนักถึงในเรื่องสิทธิส่วนบุคคลต้องทำการพิจารณาด้วยว่าสิทธิดังกล่าวเป็นสิทธิข้างเคียงอันจำเป็น (Penumbras) ซึ่งเป็นสิทธิตามกฎหมายกำหนดไว้อย่างหนึ่งซึ่งสิทธิดังกล่าวได้ขยายขอบเขตไปถึงกิจกรรมที่เกี่ยวข้องกับการสมรส การให้กำเนิดบุตร การคุมกำเนิด[52]

สิ่งที่ต้องพิจารณาต่อไปว่าสิทธิส่วนบุคคลนี้อาจถูกคุกคามโดยอนุสัญญา กลุ่มองค์กรที่เกี่ยวกับสิทธิมนุษยชนและกลุ่มอื่นๆโต้แย้งว่าวิธีการสืบสวนสอบสวนที่กำหนดไว้ในอนุสัญญานั้นอาจเป็นอันตรายกับสิทธิส่วนบุคคล โดยได้กล่าวว่าสภายุโรปได้ละเลยเรื่องสิทธิส่วนบุคคล และในบทบัญญัติของส่วนที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลนั้นไม่ชัดเจนและไม่เพียงพอ โดยเฉพาะอย่างยิ่งเกี่ยวกับอำนาจของพนักงานเจ้าหน้าที่ เช่น อำนาจในการขอรับข้อมูลจากผู้ให้บริการอินเทอร์เน็ตและเจ้าหน้าที่ของรัฐที่ใช้อำนาจดังกล่าว การออกคำสั่งให้ส่งข้อมูลที่อยู่ในระบบการค้นและยึดข้อมูลคอมพิวเตอร์ที่ถูกเก็บไว้ หรือแม้แต่หลักการดักข้อมูลที่เป็นเนื้อหา

ภายใต้บทบัญญัติของอนุสัญญานี้ไม่ว่าจะเป็นหน่วยงานบังคับใช้กฎหมายของประเทศสหรัฐอเมริกาและหน่วยงานบังคับใช้กฎหมายในประเทศแถบยุโรปจะมีอำนาจเพิ่มขึ้นในการสืบสวนสอบสวนและดำเนินคดีเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ และสิ่งที่องค์กรเหล่านี้กังวลคืออำนาจหน้าที่ที่เพิ่มขึ้นเหล่านี้อาจมากเกินไปและอาจละเมิดสิทธิส่วนบุคคล เช่น การที่อนุสัญญาให้ผู้มีอำนาจแต่ละคนต้องเปิดเผยรหัสผ่านที่อนุญาตให้มีการเข้าถึงเนื้อหา เข้าถึงรหัสต่างๆและเข้าถึงฐานข้อมูลขององค์กร

---

[51] Sara L. Marler. The Convention on Cyber – crime : should the United States ratify?. New England School of Law. p8

[52] สรวิศ ลิมปรังษี, สัมผัสคดีเรื่องสิทธิในการทำแท้งที่เป็นใจกลางความขัดแย้งระหว่างฝ่ายเสรีนิยมและอนุรักษ์นิยมในประเทศสหรัฐอเมริกา,วารสารห้องสมุดอิเล็กทรอนิกส์ศาลยุติธรรม, หน้า 4.

ปัญหาอีกอย่างหนึ่งที่ต้องพูดถึงคือ บทบัญญัติของอนุสัญญานี้ได้กำหนดให้ผู้ให้บริการอินเทอร์เน็ตและบริษัทที่ดูแลเว็บไซต์ต้องเก็บรักษาข้อมูลของผู้ใช้บริการ บทบัญญัติดังกล่าวอาจเป็นการละเมิดสิทธิส่วนบุคคลได้ เนื่องจากข้อมูลของผู้ใช้บริการที่เก็บรักษา เจ้าของข้อมูลดังกล่าวอาจไม่ต้องการเปิดเผย หากแต่การใช้งานในระบบคอมพิวเตอร์ได้กำหนดให้มีการระบุข้อมูลดังกล่าวไว้ หรือหากผู้ให้บริการต้องการเปิดเผยต้องได้รับความยินยอมจากเจ้าของข้อมูลโดยชัดแจ้ง

3.1.4 ผลกระทบจากการการปฏิบัติตามพันธกรณีแห่งอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001

การบังคับใช้กฎหมายสำหรับความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ในรูปแบบใหม่นี้ต้องอาศัยกลไกหลายประการร่วมกัน นอกจากนี้อุปสรรคที่สำคัญสำหรับการบัญญัติกฎหมายในรูปแบบนี้ คือต้องมีการบัญญัติกฎหมายใหม่เพื่อรองรับให้ทันกับเทคโนโลยีที่มีการเปลี่ยนแปลงตลอดเวลาซึ่งเป็นเรื่องยาก และไม่มีหน่วยงานที่ดูแลชัดเจน

กรณีของประเทศสหรัฐอเมริกาเองในการให้บริการทางอิเทอร์เน็ตส่วนใหญ่มักจะมีการขอข้อมูลของผู้ใช้บริการ ซึ่งการกรอกข้อมูลดังกล่าวมักจะมีกติกาของผู้ให้บริการโดยแสดงเป็นข้อความเกี่ยวกับวัตถุประสงค์ในการเก็บและใช้ข้อมูลเอาไว้ด้วย เช่น การให้บริการโทรศัพท์ ซึ่งจะมีการแจ้งผู้ขอใช้บริการว่าบริษัทจะทำหรือไม่ทำอะไรกับข้อมูล และจะมีการนำข้อมูลที่ผู้ขอใช้บริการกรอกไปใช้เพื่อวัตถุประสงค์ทางด้านการออกใบแจ้งหนี้ การให้บริการอื่นหรือการเปลี่ยนแปลงการใช้บริการ รวมทั้งเพื่อใช้ในกรณีที่เป็นเรื่องเฉพาะเจาะจง เพื่อแก้ปัญหาการให้บริการที่เกี่ยวข้องโดยเฉพาะการให้ข้อมูลข้างต้นทำให้ผู้ให้บริการทราบว่าผู้ใช้บริการอยู่ที่ใดและมีสายเคเบิ้ลโทรศัพท์อยู่ที่ไหน หรือกรณีหากสายโทรศัพท์มีปัญหาก็จะดำเนินการส่งช่างมาซ่อม หรือในกรณีที่มีบริการใหม่เกิดขึ้น ก็สามารถใช้ข้อมูลเหล่านั้นในการส่งข่าวสารระหว่างผู้ให้บริการและผู้ใช้บริการได้ ทั้งนี้ โดยทั่วไปมักจะมีการประกาศอย่างชัดแจ้งว่าจะไม่นำข้อมูลของผู้ขอใช้บริการไปให้บุคคลที่สาม[53]

แม้ว่าปัจจุบันจะมีการนำคอมพิวเตอร์มาใช้ในการเก็บข้อมูล หรือให้บริการต่างๆ มากขึ้น แต่ผู้ให้บริการแต่ละรายจะมีวิธีการหรือมาตรการในการเก็บรักษา ใช้ หรือเปิดเผยข้อมูลที่แตกต่างกันโดยขึ้นอยู่กับนโยบายของแต่ละบริษัท เช่น บริษัทที่ให้บริการ โทรศัพท์แห่งหนึ่งใน

---

[53] NECTEC. 2003. โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ. กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Law)[Online]. แหล่งข้อมูล: http://www.ecommerce.or.th/ictlaw/dp/general_info.html[2553, มกราคม 11]

ประเทศสหรัฐอเมริกาได้สนับสนุนให้ผู้ใช้บริการโทรศัพท์เปลี่ยนรูปแบบการชำระค่าบริการรายเดือนเป็นการโอนเงินแบบออนไลน์ โดยจะมีนโยบายของบริษัทกำหนดรายละเอียดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล เช่น จะไม่นำข้อมูลที่กรอกซึ่งมีลักษณะเป็น Customer Identifiable Information จากที่ลงทะเบียนไปขาย แลกเปลี่ยน หรือให้บุคคลที่สาม เพื่อให้ผู้ใช้บริการไว้วางใจและใช้บริการเพิ่มขึ้น[54]

ประเด็นเรื่องขอบเขตการใช้บังคับ จะพบว่ากฎหมายดังกล่าวถือว่ามีขอบเขตที่มีลักษณะทั่วไป คือ มีขอบเขตที่ครอบคลุมในการใช้บังคับทั้งเรื่องการประมวลผล สัญชาติของเจ้าของข้อมูล เป็นต้น ทำให้การใช้บังคับไม่ใช้เฉพาะแต่เรื่องใดเรื่องหนึ่ง มิฉะนั้นอาจจะเกิดปัญหาเหมือนกับประเทศสหรัฐอเมริกาที่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่มีลักษณะเฉพาะทำให้นานาประเทศ โดยเฉพาะสหภาพยุโรปไม่ยอมรับในตัวกฎหมายดังกล่าวของสหรัฐอเมริกาจนต้องทำข้อตกลงระหว่างประเทศที่เรียกว่า The Safe Harbor Agreement[55] เนื่องจากมาตรฐานของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหรัฐอเมริกามีข้อบกพร่องบางประการทำให้การคุ้มครองไม่เพียงพอต่อความต้องการของสหภาพยุโรปจนเกิดแรงกดดันให้ทำข้อตกลงระหว่างประเทศดังกล่าว

จากปัญหาและอุปสรรคที่เกิดขึ้นได้ส่งผลกระทบเกี่ยวกับสิทธิส่วนบุคคลที่ประเทศสหรัฐอเมริกาให้การคุ้มครอง ซึ่งสิทธิส่วนบุคคลเป็นสิ่งที่ประเทศสหรัฐอเมริกาให้ความสำคัญกับเรื่องของความเป็นส่วนตัวค่อนข้างมาก แต่ในขณะเดียวกันถึงแม้จะไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลในลักษณะของกฎหมายทั่วไปที่วางหลักการและรวบรวมการใช้ การเปิดเผยข้อมูล แต่ก็มีบทบัญญัติที่ให้ความคุ้มครองความเป็นส่วนตัว โดยประเทศสหรัฐอเมริกาได้มีการเจรจาข้อตกลงร่วมกับ The European Commission ที่ชื่อ หลักการรักษาข้อมูลส่วนบุคคลของสหรัฐอเมริกา (US Safe Harbor) ขึ้นเพื่อเป็นการสร้างความมั่นใจในการส่งหรือโอนข้อมูลส่วนบุคคลข้ามประเทศให้สามารถดำเนินการได้ แนวคิดดังกล่าวคือ การที่บริษัทเอกชนของสหรัฐอเมริกาสมัครใจเข้าร่วมปฏิบัติตามหลักการคุ้มครองความเป็นส่วนตัว privacy principle ที่กำหนดขึ้นโดย Department of Commerce ของสหรัฐอเมริกา โดยบริษัทที่ปฏิบัติตามหลักการดังกล่าวจะได้รับข้อสันนิษฐานเบื้องต้นว่ามีระดับการคุ้มครองความเป็นส่วนตัวในระดับที่เหมาะสมและสามารถรับข้อมูลส่วนบุคคลจากสหภาพยุโรปได้ บริษัทที่เข้าร่วมจะต้องใช้หลัก

---

[54] Ibid.,

[55] สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ, "แนวทางการจัดทำกฎหมายข้อมูลส่วนบุคคล", ธันวาคม 2546, หน้า 56-58

ความชัดเจนในการแจ้งประเภทของข้อมูลที่มีการจัดเก็บ วัตถุประสงค์ของการนำข้อมูลไปใช้ และบุคคลที่ต้องการให้เปิดเผยข้อมูลให้ ซึ่งการแจ้งข้อมูลเหล่านี้จะต้องแจ้งให้ทราบในเวลาที่มีการเก็บรวบรวมหรือในทันทีที่สามารถปฏิบัติได้ เจ้าของข้อมูลจะต้องสามารถเลือก (opt-out) ที่จะไม่ให้มีการเก็บรวบรวมข้อมูลส่วนบุคคลของตนอีกต่อไป หากข้อมูลดังกล่าวจะถูกนำไปใช้หรือเปิดเผยต่อบุคคลอื่นนอกเหนือจากวัตถุประสงค์เดิมที่เคยให้ไว้ และในกรณีที่เป็นข้อมูลพิเศษ (sensitive data) บุคคลจะต้องให้ความยินยอมโดยชัดแจ้งในการเก็บรวบรวมข้อมูลนั้น นอกจากนี้บริษัทหรือองค์กรที่เข้าร่วมในข้อตกลงดังกล่าว จะต้องปฏิบัติตามเงื่อนไขอื่นๆ เพิ่มเติม เช่น ต้องมีมาตรการรักษาความปลอดภัยข้อมูลมิให้สูญหายหรือนำไปใช้ในทางมิชอบ ต้องให้สิทธิแก่เจ้าของข้อมูลในการเข้าถึงข้อมูลส่วนบุคคลที่เกี่ยวกับตนหรือสามารถแก้ไขข้อมูลให้ถูกต้องได้ และต้องมีกลไกการสืบสวนสอบสวนข้อร้องเรียนหรือชดใช้ค่าเสียหาย เป็นต้น อย่างไรก็ตาม ข้อตกลงดังกล่าวยังคงมีประเด็นที่ยังไม่ชัดเจนในเรื่องเกี่ยวกับการระงับข้อพิพาทที่คำวินิจฉัยเกี่ยวกับข้อร้องเรียนต่างๆ ในข้อตกลงยังไม่สามารถใช้บังคับได้[56]

ทั้งนี้ ประเทศสหรัฐอเมริกายังคงให้ความสำคัญกับการความเป็นส่วนตัว โดยกฎหมายที่บัญญัตินั้นต้องสามารถควบคุมและจำกัดข้อมูลที่สามารถจัดเก็บ ประมวลผล โอนย้าย เก็บรักษา ใช้งานหรือเผยแพร่ ดังนั้น จึงเป็นเรื่องสำคัญที่นอกจากระบบจัดการข้อมูลที่มีประสิทธิภาพจะต้องมีความสามารถในการเก็บรักษาและเก็บถาวรข้อมูลเมื่อจำเป็น และติดตามตรวจสอบการเข้าถึงข้อมูลส่วนบุคคล จึงได้เกิดกฎหมายที่เกี่ยวข้องกับการปกป้องข้อมูลส่วนบุคคลที่สำคัญ[57] เช่น

Children's Online Privacy Protection Act of 1998 เป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลของเด็กมีเนื้อหาสำคัญคือเพื่อคุ้มครองข้อมูลส่วนบุคคลหรือความเป็นส่วนตัวของเด็กที่มีอายุต่ำกว่า 13 ปี โดยควบคุมการเก็บและการใช้ข้อมูลดังกล่าวของผู้ประกอบธุรกิจทางอินเทอร์เน็ตที่เป็นผู้ให้บริการผ่านเว็บไซต์หรือระบบการให้บริการผ่านระบบออนไลน์ต่างๆโดยผู้ให้บริการต้องขออนุญาตจากผู้ปกครองเด็กล่วงหน้า

Gramm – Leach – Bliley Act of 1999 ที่กำกับดูแลการปกป้องความเป็นส่วนตัวสำหรับการขายข้อมูลทางการเงินส่วนบุคคล การป้องกันการสร้างสถานการณ์หลอกลวงเพื่อเอา

---

[56] เรื่องเดียวกัน, หน้า 58.

[57] Cynthia L. Jackson, คู่มือการปฏิบัติตามกฎระเบียบสำหรับธุรกิจ, Baker & McKenzie (2007), หน้า 33-35

ข้อมูลทางการเงินส่วนบุคคล นอกจากนี้ยังกำหนดให้สถาบันการเงินต้องมีโปรแกรมรักษาความปลอดภัยของข้อมูล

Health Insurance Portability and Accountability Act กำกับดูแลการรวบรวมการใช้งาน และการเข้าถึงข้อมูลเกี่ยวกับสุขภาพไม่ว่าจะเป็นแผนสุขภาพ ควบคุมการใช้งานและการเปิดเผยข้อมูลด้านสุขภาพที่ได้รับการปกป้องซึ่งจัดเก็บอยู่ในรูปแบบใดๆ

The Fair Credit Reporting Act การควบคุมการใช้งานและการเปิดเผยข้อมูลในรายงานผู้บริโภคปกป้องความถูกต้องสมบูรณ์ของข้อมูลที่รวบรวมและเผยแพร่ รวมทั้งการเข้าถึงอินเทอร์เน็ตเพื่อใช้งานข้อมูลดังกล่าว

จากเหตุผลดังกล่าวเห็นได้ว่าการคุ้มครองสิทธิส่วนบุคคลนั้นเป็นสิ่งสำคัญสำหรับการใช้งานระบบคอมพิวเตอร์ หากไม่มีกฎหมายที่เกี่ยวกับการคุ้มครองสิทธิส่วนบุคคลที่เพียงพออาจก่อให้เกิดอุปสรรคต่อการปฏิบัติตามพันธกรณีหากต้องมีโอนย้ายข้อมูลเพื่อความจำเป็นในการสืบสวนสอบสวน หรือการดำเนินคดีไปยังต่างประเทศหรือโอนไปยังประเทศที่ไม่มีกฎหมายในการคุ้มครองข้อมูลส่วนบุคคล

3.2 ประเทศฝรั่งเศส

ความเจริญก้าวหน้าทางเทคโนโลยีสารสนเทศในประเทศฝรั่งเศสจะเห็นได้จากวิศวกรชาวฝรั่งเศสซึ่งนับว่าเป็นหนึ่งในผู้เชี่ยวชาญด้านคอมพิวเตอร์ในระดับแนวหน้า และจากความสำเร็จอันท่วมท้นของนานาบริษัท รวมถึงศูนย์ปฏิบัติการวิจัยของบริษัทต่างๆที่มีส่วนสำคัญในการช่วยพัฒนาเทคโนโลยีแบบใหม่ โดยการประสิทธิภาพรวมถึงการคิดค้นเทคนิคใหม่ๆ และความสามารถในการรวมระบบต่างๆเข้าด้วยกัน และมีส่วนร่วมในการพัฒนาภาคอุตสาหกรรมและภาคธุรกิจการบริการมากมายหลายประเภท เช่น อุตสาหกรรมการบิน การคมนาคมขนส่งทางบก กิจการธนาคาร หน่วยงานราชการและธุรกิจการค้า ตัวอย่างที่เห็นได้ชัดเจน คือกลุ่มบริษัทบูล (Bull) ซึ่งเป็นบริษัทผู้ผลิตคอมพิวเตอร์อันดับหนึ่งของประเทศฝรั่งเศส และจัดอยู่ในอันดับที่สองของยุโรป และอยู่ในอันดับที่สิบของโลกในด้านการผลิตซอฟต์แวร์และการให้บริการ กลุ่มบริษัท SSII แห่งฝรั่งเศสจัดอยู่ในอันดับที่สองของโลกรองจากประเทศสหรัฐอเมริกา ที่ได้เสนอวิธีการแก้ปัญหาทางคอมพิวเตอร์โดยรวมให้แก่บริษัทต่างๆซึ่งได้รับการดัดแปลงให้เหมาะสมกับความต้องการของแต่ละบริษัท หน่วยงานราชการ และบริษัทเอกชนในหลายประเทศได้นำแนวทางการแก้ปัญหาดังกล่าวไปใช้เช่นกัน เช่น ศาลฎีกาที่รัฐแมสซาชูเซ็ทส์ ศาลยุติธรรมที่รัฐโอไฮโอของประเทศสหรัฐอเมริกา ระบบการจำหน่ายสินค้าในประเทศเนเธอร์แลนด์ ธนาคารใหญ่

ของประเทศฮังการี หน่วยงานด้านการคลังในประเทศโปแลนด์ ที่ตั้งกองบัญชาการตำรวจฝ่ายอาชญากรรม (CID) ที่เบอร์มิงแฮม ประเทศอังกฤษ หน่วยงานราชการและเอกชนหลายแห่งในประเทศอิตาลี สเปน เยอรมัน เบลเยี่ยม เดนมาร์ก และนอร์เวย์[58]

วิศวกรชาวฝรั่งเศสได้ขยายงานวิจัยทางคอมพิวเตอร์ให้ครอบคลุมถึงชีวิตประจำวันเพื่อให้มีความสะดวกสบายยิ่งขึ้นตามนิสัยของชาวฝรั่งเศสที่ชอบความสะดวกสบายในประเทศฝรั่งเศสมีการติดตั้งเครื่องอัตโนมัติที่พูดได้เพื่อจำหน่ายบัตรโดยสารเครื่องบิน การบริการด้านการเงิน กรมธรรม์ประกันภัยหรือการจองห้องพักโรงแรม เครื่องให้บริการอัตโนมัติเพื่อรับทราบตารางเวลาของรถโดยสารประจำทาง ส่วนที่เมืองปารีสมีการควบคุมมีการควบคุมการจราจรด้วย ระบบชำนาญการที่ประสานการให้จังหวะสัญญาณไฟจราจร โดยระบบดังกล่าวคาดว่าสามารถทำให้ผู้ขับขี่รถยนต์ในเมืองหลวงสามารถประหยัดเวลาในการเดินทาง

สถาบันการวิจัยด้านคอมพิวเตอร์และระบบอัตโนมัติแห่งประเทศฝรั่งเศสได้ทุ่มเทงบประมาณและทรัพยากรบุคคลเพื่อการวิจัยขั้นมูลฐานและการวิจัยเพื่อการประยุกต์ใช้ รวมทั้งได้ทดลองใช้ระบบใหม่ๆ ยิ่งกว่านั้นศูนย์กลางเพื่อการวิจัยในมหาวิทยาลัยหลายแห่ง เช่น ที่เมืองตูลูส เมืองเกรอนอบ เมืองนองซี และกรุงปารีส ยังได้ร่วมมือกับศูนย์วิจัยทางวิทยาศาตร์แห่งชาติ (CNRS) เพื่อพัฒนาความเป็นเลิศของประเทศฝรั่งเศสในด้านวิศวกรรมคอมพิวเตอร์ คอมพิวเตอร์เพื่อการเรียนภาษาและระบบหุ่นยนต์ควบคู่ไปกับสถาบันการวิจัยด้านคอมพิวเตอร์และระบบอัตโนมัติแห่งประเทศฝรั่งเศสด้วย[59]

3.2.1 สถานการณ์เกี่ยวกับปัญหาอาชญากรรมเกี่ยวกับคอมพิวเตอร์และอินเทอร์เน็ตในประเทศฝรั่งเศส

เมื่อไม่นานมานี้ประเทศฝรั่งเศสได้มีการประกาศเลิกใช้คอมพิวเตอร์ของบริษัทแบล็คเบอร์รี่ (Blackberry) โดยหนังสือพิมพ์เลอ มงต์ ของประเทศฝรั่งเศสรายงานว่ากระทรวงต่างๆ และหน่วยงานรัฐบาลของประเทศได้ยกเลิกการใช้คอมพิวเตอร์แบบพกพาของบริษัทแบล็คเบอร์รี่ ซึ่งผลิตโดยบริษัทในประเทศแคนาดาชื่อบริษัทรีเสิร์ช อิน โมชั่น เนื่องจากเกรงว่าจะถูกประเทศสหรัฐอเมริกาล้วงความลับ เพราะจดหมายอิเล็กทรอนิกส์ที่ส่งจากเครื่องของแบล็คเบอร์รี่นั้นจะต้องผ่านเซิร์ฟเวอร์ในประเทศสหรัฐอเมริกาและประเทศอังกฤษ ซึ่งมีความเสี่ยงที่จะถูกล้วง

---

[58] การพัฒนาเทคโนโลยีของฝรั่งเศส. [Online]. 2545. แหล่งข้อมูล: http://www.school.net.th/library/create-web/10000/generality/10000-4465.html[2553, มกราคม 11]

[59] Ibid.

ความลับโดยหน่วยงานข่าวกรองของประเทศสหรัฐอเมริกา และต่อมานายอแลง จูเลียต เจ้าหน้าที่ข่าวกรองด้านเศรษฐกิจของประเทศฝรั่งเศส ได้กล่าวว่าแบล็คเบอร์รี่มีปัญหาในการปกป้องข้อมูลและเสี่ยงต่อการถูกลักลอบข้อมูล ทั้งนี้ ในการประชุม G8 ที่ประเทศเยอรมนี บรรดาระดับผู้ช่วยของรัฐบาลของประเทศสหรัฐอเมริกาถูกแนะนำให้งดเว้นการใช้คอมพิวเตอร์ที่ใช้เครือข่ายอินเตอร์เน็ตแบบไร้สายเพราะเกรงว่าประเทศรัสเซียจะแอบล้วงความลับขณะส่งจดหมายอิเล็กทรอนิกส์เช่นกัน[60]

ด้านบริษัทที่ทำการผลิตได้ทำการชี้แจงต่อปัญหาดังกล่าวว่า จดหมายอิเล็กทรอนิกส์ที่ส่งจากเครื่องแบล็คเบอร์รี่ไม่สามารถถูกลักลอบหรืออ่านโดยหน่วยงานจารกรรมใดๆทั้งสิ้น แม้แต่บริษัทเองก็ยังไม่สามารถดูเนื้อหาหรือข้อมูลใดๆที่ส่งผ่านแบล็คเบอร์รี่ได้ อีกทั้งระบบของแบล็คเบอร์รี่ก็ได้รับการรับรองจากหน่วยงานด้านความมั่นคงในหลายประเทศ เช่น ประเทศสหรัฐอเมริกา ประเทศออสเตรเลีย ประเทศนิวซีแลนด์ ประเทศออสเตรีย และประเทศแคนาดา[61]

แม้ว่าจะมีหลายปัจจัยที่ส่งผลให้อาชญากรรมทางคอมพิวเตอร์เพิ่มขึ้น แต่ปัจจัยหลักที่ส่งผลกระทบต่อประเทศฝรั่งเศสมากที่สุดคือ[62]

1. จำนวนผู้ใช้อินเทอร์เน็ตที่เพิ่มขึ้นอย่างรวดเร็ว ในเดือนกุมภาพันธ์ ปี ค.ศ. 2005 คาดหมายว่าจำนวนผู้ใช้อินเทอร์เน็ตจะมีมากถึง 25 ล้านคน ซึ่งมากกว่าปี ค.ศ. 2000 ถึง 8,500,000 คน ถือเป็น 41.2 เปอร์เซ็นต์ ของประชากรทั้งหมดในประเทศ ในจำนวนทั้งหมด 25 ล้านคน มีถึง 7 ล้านคนที่ทำการเชื่อมต่อข้อมูลอินเทอร์เน็ตความเร็วสูง เช่น ADSL หรือเคเบิ้ลโมเด็มที่มีความเร็วมากกว่าอินเทอร์เน็ตปกติถึง 100 เท่า แต่จ่ายค่าบริการเพียง 20 ยูโรต่อเดือน

2. เครื่องคอมพิวเตอร์ในร้านอินเทอร์เน็ตคาเฟ่ รวมถึงเซิร์ฟเวอร์ในประเทศฝรั่งเศสที่มีการติดตั้งและทำการเชื่อมต่ออินเทอร์เน็ตความเร็วสูง โดยมีค่าธรรมเนียมในการใช้บริการเพียง 1 ยูโรต่อชั่วโมง ซึ่งร้านอินเทอร์เน็ตคาเฟ่เหล่านี้อาจถูกใช้ในการกระทำความผิดเกี่ยวกับ

---

[60] หนังสือพิมพ์มติชน. มติชน[ออนไลน์]. 22 มิถุนายน 2550. Available from: http://news.sanook.com/world/world_149353.php [2553, มกราคม 11]

[61] Ibid.,

[62] Mohamed Chawki, 2005. Cybercrime in France : An Overview, Computer Crime Research Center[Online]. Available from : http://www.crime-research.org/articles/cybercrime-in-france-overview/3[2010, January 11]

คอมพิวเตอร์ เช่น การฉ้อโกง การโจมตีระบบและเครือข่ายคอมพิวเตอร์ ที่จะช่วยให้ผู้กระทำความผิดสามารถหลอกลวงเหยื่อผู้เสียหายได้เนื่องจากมีขนาดใหญ่และกระจายในวงกว้างมาก

3. ผู้ใช้บริการอินเทอร์เน็ตได้รวมตัวกันเป็นชุมชนชาวไซเบอร์ที่มีการติดต่อกันผ่านเครือข่ายอินเทอร์เน็ตและร่วมกันกระทำความผิด ซึ่งการกระทำหรือกิจกรรมที่ผิดกฎหมายดังกล่าว เช่น การขายสินค้าละเมิดลิขสิทธิ์ หรือ การขายของผิดกฎหมาย อุปกรณ์เกี่ยวกับการกระทำทางเพศและสื่อลามกต่างๆ ชุมชนเหล่านี้ยังใช้เป็นสถานที่แลกเปลี่ยนเทคโนโลยีและประสบการณ์เกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

4. การพัฒนาอุตสาหกรรมเครือข่ายเกมมัลติมีเดียก็มีผลกระทบทำให้อาชญากรรมทางคอมพิวเตอร์เพิ่มขึ้น ผู้ใช้บริการประเภทนี้มักมีความสับสนระหว่างชีวิตจริงและชีวิตในโลกของคอมพิวเตอร์ พวกเขาต้องการการพัฒนาระดับที่สูงขึ้นไปในโลกไซเบอร์ บางคนต้องการอำนาจในความเป็นจริงให้เสมือนกับการเล่นเกมออนไลน์ ที่ต้องการมีซื้ออาวุธบางอย่างและต้องจ่ายเงินจำนวนมากเพื่อการซื้ออาวุธดังกล่าว

การกระทำความผิดที่ถือเป็นอาชญากรรมทางคอมพิวเตอร์นั้นมีทั้งประเภทที่มีความรุนแรง อาชญากรมีความสามารถสูงความผิดประเภทนี้อาจก่อให้เกิดอันตรายทางกายภาพกับบุคคล เช่น การก่อการร้ายทางคอมพิวเตอร์ ความผิดฐานข่มขู่ทางอินเตอร์เน็ต ความผิดเกี่ยวกับสื่อลามกอนาจารเกี่ยวกับเด็ก และประเภทที่ไม่รุนแรงไม่ก่อให้เกิดการทำลาย เป็นการกระทำความผิดต่อเครือข่ายคอมพิวเตอร์ที่ใช้งานอยู่

อย่างไรก็ตามอาชญากรรมประเภทที่ไม่รุนแรงในความเป็นจริงพบว่าเกิดจากในโลกคอมพิวเตอร์สามารถติดต่อสื่อสารโดยไม่ต้องทำการพบปะ ไม่รู้จักชื่อจริงและไม่รู้จักตัวตนที่แท้จริง ซึ่งเป็นเสมือนองค์ประกอบที่ทำให้โลกเทคโนโลยีเช่นนี้เหมาะแก่การกระทำความผิดและก่ออาชญากรรมทางคอมพิวเตอร์ อาชญากรรมทางคอมพิวเตอร์ที่เป็นประเภทไม่รุนแรง เช่น การบุกรุกทางคอมพิวเตอร์ การโจรกรรมทางคอมพิวเตอร์ การฉ้อโกงทางคอมพิวเตอร์

จากการรายงาน Rapport Senat n° 321[63] ที่ทำการเผยแพร่โดยองค์กรที่ทำหน้าที่ต่อต้านอาชญากรรมเกี่ยวกับเทคโนโลยีสารสนเทศและการสื่อสารที่ชื่อ Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (O.C.L.C.T.I.C.) ทำการเปิดเผยตัวเลขของการกระทำความผิดเกี่ยวกับ

---

[63] Ibid, p 2.

คอมพิวเตอร์ ในปี 2004 พบว่ามีการกระทำความผิดเกิดขึ้นทั้งหมด 59,964 ความผิด โดยแบ่งเป็น

- ความผิดทางคอมพิวเตอร์ที่เกี่ยวกับบัตรเครดิต เช่น การปลอมแปลงบัตรเครดิต 49,914 ความผิด

- การใช้ข้อมูลบัตรเครดิตกระทำความผิดผ่านทางคอมพิวเตอร์ 8,470 ความผิด

- ความผิดเกี่ยวกับสื่อลามกอนาจารผ่านทางคอมพิวเตอร์ 576 ความผิด

- การหมิ่นประมาทและการคุกคามทางเพศผ่านทางคอมพิวเตอร์ 333 ความผิด

- การบุกรุกทางคอมพิวเตอร์ 285 ความผิด

- การละเมิดลิขสิทธิ์ ซอฟต์แวร์ 268 ความผิด

- ความผิดเกี่ยวกับคอมพิวเตอร์ประเภทอื่นๆ 118 ความผิด

3.2.2 แนวทางในการปฏิบัติในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์

ประเทศฝรั่งเศสได้เริ่มกระบวนการในการให้สัตยาบันอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 (Convention on Cyber Crime 2001) เมื่อวันที่ 11 มิถุนายน ค.ศ. 2003 โดยนาย Dominique de Villepin รัฐมนตรีว่าการกระทรวงการต่างประเทศ[64] ในขณะนั้น ได้นำเสนอร่างกฎหมายต่อสภารัฐมนตรีเพื่อการให้สัตยาบันต่ออนุสัญญา ประเทศฝรั่งเศสถือได้ว่าเป็นประเทศแรกของสหภาพยุโรป (European Union : EU) ที่ทำการให้สัตยาบันอนุสัญญาดังกล่าว ซึ่งในขณะนั้นมีประเทศสมาชิกของสภายุโรป (Council of Europe : CoE) เพียงสามประเทศเท่านั้น คือ ประเทศแอลแบเนีย ประเทศโครเอเชีย และประเทศเอสโตเนีย ที่ให้สัตยาบันอนุสัญญา ซึ่งตามบทบัญญัติในอนุสัญญาได้กำหนดให้อนุสัญญาสามารถมีผลบังคับใช้ได้ก็ต่อเมื่อมีรัฐให้สัตยาบันแก่อนุสัญญาไปแล้ว 5 รัฐ โดยในจำนวนดังกล่าวจะต้องมีประเทศสมาชิกของสภายุโรปอย่างน้อยสามประเทศ*

---

[64] European Digital Rights. 2003. France ready to ratify Cybercrime convention[Online]. Available from: http://www.edri.org/edrigram/number11/cybercrime-convention-france[2010, January 11]

* Article 36 – Signature and entry into force of Convention on Cybercrime

ทั้งนี้ ประเทศฝรั่งเศสได้มีการให้สัตยาบันเมื่อวันที่ 10 มกราคม ค.ศ. 2006[65] โดยไม่ได้มีการบัญญัติกฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ไว้โดยเฉพาะ แต่ได้มีการบัญญัติเพิ่มเติมในส่วนของกฎหมายอาญาที่เกี่ยวกับเทคโนโลยีสารสนเทศและการสื่อสารและได้มีการจัดตั้งหน่วยงานที่มีอำนาจหน้าที่ในการบังคับใช้กฎหมายทั่วไป คือ กองกำลังตำรวจแห่งชาติของฝรั่งเศส Police Nationale เป็นกองกำลังกึ่งทหารตำรวจ แบ่งออกเป็น Police Nationale ซึ่งรับผิดชอบในเขตเมือง และ gendarmerie ซึ่งรับผิดชอบเขตห่างไกลนอกเมือง นอกจากนี้ตามเมืองใหญ่ๆยังมีตำรวจท้องถิ่น เรียกว่า La Police Municipale ซึ่งมีอำนาจจำกัด[66] และหน่วยงานที่อยู่ภายใต้กองกำลังตำรวจแห่งชาติฝรั่งเศสที่ทำหน้าที่ในการกำกับดูแลการกระทำความผิดเกี่ยวกับเทคโนโลยีและกิจการโทรคมนาคม และโดยเฉพาะการกระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ ตามบทบัญญัติและพันธกรณีอนุสัญญาดังกล่าว

ทั้งนี้ ผู้เขียนได้ทำการศึกษาในส่วนที่สอดคล้องกับบทบัญญัติที่กำหนดในอนุสัญญาและส่วนที่เกี่ยวข้องกับคอมพิวเตอร์ดังนี้

3.2.2.1 **มาตรการทางสารบัญญัติ**

จากการที่อนุสัญญาให้ประเทศภาคีกำหนดการกระทำความผิดอาชญากรรมทางคอมพิวเตอร์เป็นความผิดทางอาญาตามกฎหมายภายในประเทศ ประเทศฝรั่งเศสได้มีการบัญญัติกฎหมายที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์โดยตรง และการกระทำความผิดบางลักษณะที่เกี่ยวกับคอมพิวเตอร์โดยอ้อม ดังนี้

ก. กฎหมายอาญา (Penal Code)

จากการที่ประเทศฝรั่งเศสได้มีการลงนามและให้สัตยาบันอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 ประเทศฝรั่งเศสจึงต้องมีการอนุวัติการตามอนุสัญญา โดยประเทศฝรั่งเศสเองไม่ได้มีการบัญญัติกฎหมายการกระทำความผิดเกี่ยวกับ

...3. This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

[65] The effectiveness of international co-operation against cybercrime : examples of good practice. Project on Cybercrime. March 12, 2008, [Online]. Available from : http://www.coe.int/cybercrime[2010, January 11]

[66] ธวัชชัย กาญจนรินทร์ และนางจันทร์เพ็ญ เล็กเลิศ, ระบบบริการทางการแพทย์ฉุกเฉินของประเทศฝรั่งเศส, หน้า 1 แหล่งข้อมูล: http://www.niems.go.th/userfiles/france.doc[2553, มกราคม 11]

คอมพิวเตอร์ไว้โดยเฉพาะ แต่ได้มีการแก้ไขเพิ่มเติมในกฎหมายอาญา โดยบัญญัติให้การกระทำความมผิดเกี่ยวกับคอมพิวเตอร์เป็นความผิดตามกฎหมายอาญา

กฎหมายอาญาของประเทศฝรั่งเศสได้บัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ไว้หลายประการ ตามลักษณะของการกระทำความผิด ดังนี้

1. การเข้าถึงระบบประมวลผลข้อมูลอัตโนมัติโดยปราศจากอำนาจ ซึ่งเป็นการกระทำความผิดโดยการเข้าถึงระบบการประมวลผลข้อมูลอัตโนมัติ ไม่ว่าทั้งหมดหรือบางส่วนของระบบดังกล่าวและหากการเข้าถึงระบบดังกล่าวทำให้เกิดการยกเลิกและแก้ไขข้อมูลที่อยู่ในระบบหรือก่อให้เกิดการเปลี่ยนแปลงการทำงานของระบบการประมวลผลข้อมูลดังกล่าว (Article 323-1) ความผิดตามบทบัญญัตินี้มีความสอดคล้องกับบทบัญญัติของอนุสัญญาที่กล่าวถึงกระทำความผิดโดยการเข้าถึงระบบและข้อมูลคอมพิวเตอร์ ซึ่งการเข้าถึงดังกล่าวต้องเป็นการเข้าถึงโดยปราศจากอำนาจ หรือไม่ได้รับอนุญาตให้มีการเข้าถึงระบบและข้อมูลคอมพิวเตอร์

2. การกระทำโดยการขัดขวางการทำงานของระบบหรือการรบกวนการทำงานของระบบประมวลผลข้อมูลอัตโนมัติ (Article 323-2) การกระทำความผิดตามที่กำหนดในกฎหมายอาญาฝรั่งเศสนี้ ถือได้ว่าเป็นการกระทำความผิดโดยการแทรกแซงต่อข้อมูลและระบบคอมพิวเตอร์ตามที่กำหนดไว้ในอนุสัญญา ซึ่งการกระทำที่เป็นการแทรกแซงต่อข้อมูลและระบบถือเป็นการขัดขวางการทำงานระบบคอมพิวเตอร์ หรืออาจทำให้ระบบคอมพิวเตอร์ทำงานช้าลงหรือทำงานได้ไม่เป็นปกติ ทั้งนี้ อาจโดยการนำเข้าข้อมูล การแก้ไข ดัดแปลง หรือการทำลายซึ่งข้อมูลในระบบดังกล่าว เช่น การนำเข้าโค้ดอันตราย หรือการปฏิเสธการให้บริการ

3. การกระทำความผิดโดยนำเข้า เผยแพร่ แก้ไข รับหรือส่งต่อข้อมูลในระบบการประมวลผลข้อมูลอัตโนมัติ หรือการก่อให้เกิดการหลอกลวงและการเปลี่ยนแปลงข้อมูลที่มีอยู่ในระบบการประมวลผลโดยอัตโนมัติ (Article 323-3) ซึ่งการกระทำดังกล่าวเป็นการเปลี่ยนแปลง แก้ไขข้อมูลโดยปราศจากอำนาจ ทั้งนี้ อาจเป็นการกระทำความผิดโดยการใช้บัญชีคอมพิวเตอร์ของบุคคลอื่นโดยไม่ได้รับอนุญาต เช่น การใช้รหัสในการเข้าถึงข้อมูล การเข้าถึงดังกล่าวอาจทำให้ข้อมูลของเหยื่อเกิดการสูญหาย เกิดการขโมยข้อมูลและการให้บริการ[67]

---

[67] RAND EUROPE and LAWFORT, Update to the Handbook of Legal Procedures of Computer and Network Misuse in EU Countries for assisting CRIRTs, [December, 2005]

ทั้งนี้ กฎหมายอาญาฝรั่งเศสยังได้กำหนดให้การกระทำความผิดโดยที่ไม่มีมูลเหตุจูงใจที่ถูกกฎหมาย ซึ่งเป็นการนำเข้า การครอบครอง การเสนอขายหรือการผลิตอุปกรณ์ใดๆ โปรแกรมคอมพิวเตอร์ หรือข้อมูลใดๆที่ออกแบบหรือดัดแปลงเพื่อใช้กระทำความผิดตาม Article 323-1 ถึง Article 323-3 (Article 323-3-1) และการมีส่วนร่วมในการกระทำความผิดหรือมีส่วนร่วมในการเตรียมการเพื่อกระทำความผิดตาม Article 323-1 ถึง Article 323-3 ต้องรับโทษตามที่กฎหมายกำหนดเช่นกัน (Article 323-4) ตัวอย่างคดีที่เกิดขึ้น เช่น

คดีการฉ้อโกงเกี่ยวกับคอมพิวเตอร์ GCB V. Humpich[68] นาย Serge Humpich อายุ 36 ปี เป็นวิศวกรที่ค้นพบการเจาะข้อมูลในชิพ (chips) ที่ใช้รักษาความปลอดภัยของข้อมูลในบัตรเครดิตในประเทศฝรั่งเศส ถูกพิพากษาในเดือนกุมภาพันธ์ ค.ศ. 2000 ในกรุงปารีส โดยศาลพิพากษาโทษจำคุก 10 เดือน และค่าปรับเป็นเงินจำนวน 12,000 ฟรังค์ตามหลักเกณฑ์ของกรมราชทัณฑ์ ถือเป็นคดีหนึ่งสร้างความความเสียหายสำหรับ Groupement des Cartes Bancaires เจ้าหน้าที่ได้ทำการยึดเครื่องคอมพิวเตอร์และอุปกรณ์ รวมถึงข้อมูลที่เขาได้ยื่นต่อสำนักงานทรัพย์สินอุตสาหกรรมฝรั่งเศส (Institut National de Propriété Industrielle : INPI) ซึ่งเป็นหน่วยงานของรัฐที่ทำหน้าที่เก็บค่าธรรมเนียมสิทธิทรัพย์สินอุตสาหกรรม ได้แก่ ค่าสิทธิบัตร เครื่องหมายการค้า

คดีเริ่มต้นจากการที่นาย Humpich ได้เริ่มทำการศึกษาเกี่ยวกับการรักษาความปลอดภัยของข้อมูลบัตรเครดิตเมื่อประมาณ 4 ปีที่ผ่านมา จนได้ค้นพบการเจาะข้อมูลในระบบที่สำคัญในการตรวจสอบข้อมูลในระบบ เขาได้ทำการติดต่อไปยัง Groupement des Cartes Bancaires ผ่านทางทนายความของบริษัทเพื่อทำการเจรจาถ่ายทอดเทคโนโลยีที่เขาค้นพบ ซึ่งจำนวนเงินซื้อขายในการกระทำความผิดดังกล่าวครั้งนี้ไม่ได้รับการเปิดเผยและยืนยันจากบุคคลทั้งถึงจำนวนที่แน่นอน แต่จากการประมาณการมีจำนวนมากถึง 20 ล้านยูโร ในระหว่างการพิจารณาของศาลได้รับการเปิดเผยว่านาย Humpich กระทำความผิดเพียงการหลอกลวงให้ GCB ใช้บัตรเครดิตที่เขาทำการคิดค้นขึ้นซึ่งไม่มีข้อมูลในบัตร ซึ่งรู้แต่เพียงว่ามีการติดต่อตัวแทนของ GCB โดยการดักฟังการติดต่อทางโทรศัพท์ ทำให้นาย Humpich ถูกเจ้าหน้าที่ตำรวจจับกุมและทำการค้นบ้านและยึดอุปกรณ์รวมทั้งสำนักงานทนายความ

4. การดักรับข้อมูล การเข้าถึงข้อมูลโดยปราศจากอำนาจที่ถือเป็นความผิดอีกประการหนึ่งคือ การดักรับข้อมูลที่มีการติดต่อสื่อสารผ่านทางโทรคมนาคม หรือโดยการติดตั้ง

---

[68] Computer Crime Research Center. 2004. MOHAMED CHAWKI. Cybercrime in France: An Overview[Online]. Available from: http://www.crime-research.org/articles/cybercrime-in-france-overview/[2010, January 11]

อุปกรณ์ ถือเป็นการละเมิดความลับและความเป็นส่วนตัวของบุคคล (Article 226-15) การกำหนดให้การดักรับข้อมูลเป็นความผิดนี้ได้สอดคล้องกับบทบัญญัติของอนุสัญญา ซึ่งการกระทำความผิดโดยการดักรับข้อมูลนี้อาจเป็นการกระทำที่ก่อให้เกิดความล่าช้า หรือทำให้การติดต่อสื่อสารที่ส่งไปยังบุคคลที่สามเกิดความคลาดเคลื่อน การกระทำความผิดต้องเป็นการกระทำที่ประสงค์ร้าย มุ่งทำลาย หรือไม่ว่าจะกระทำโดยวิธีการใดก็ตาม หรือเป็นการกระทำโดยวิธีใดก็ตามเพื่อให้ได้รับทราบข้อมูลการติดต่อสื่อสารระหว่างบุคคล ทั้งนี้ กฎหมายยังกำหนดให้การดักรับข้อมูลที่ถือเป็นความผิดตามกฎหมายให้รวมถึงการกระทำที่เป็นการดักรับข้อมูลเพื่อทำให้เกิดความคลาดเคลื่อนระหว่างการติดต่อสื่อสารระหว่างบุคคล หรือการเปิดเผยซึ่งการติดต่อสื่อสาร การถ่ายทอดข้อมูล การได้รับข้อมูลจากการติดต่อสื่อสารผ่านทางโทรคมนาคม หรือการได้รับข้อมูลโดยการติดตั้งอุปกรณ์พิเศษเพื่อการดักรับข้อมูลการติดต่อสื่อสารระหว่างบุคคล ตัวอย่างคดีที่เกี่ยวกับการดักรับข้อมูลที่มีการติดต่อผ่านทางโทรคมนาคม เช่น

คดีการดักฟังโทรศัพท์ของหน่วยต่อต้านการก่อการร้าย[69] ซึ่งเป็นหน่วยงานที่ก่อตั้งขึ้นโดยประธานาธิบดี François Mitterrand ในคดีนี้ผู้มีส่วนเกี่ยวข้องกับการดักฟังโทรศัพท์จำนวน 11 รายถูกฟ้องในข้อหาละเมิดชีวิตส่วนตัวของผู้อื่น คดีนี้นำขึ้นสู่ศาลและมีการตัดสินในปี ค.ศ. 2002 ส่วนหนึ่งเพราะในการสืบสวนสอบสวนหลายฝ่ายที่เกี่ยวข้องได้ยกเอาเรื่องความลับเพื่อความมั่นคงของประเทศ มาเป็นข้ออ้างในการไม่ต้องให้ข้อมูลกับฝ่ายตุลาการ

สาเหตุที่ทำให้ผู้เกี่ยวข้องต้องถูกดำเนินคดีในครั้งนี้ คือ การที่หน่วยต่อต้านการก่อการร้ายได้ทำการดักฟังโทรศัพท์บุคคลหลากหลายอาชีพ ที่มิได้มีส่วนเกี่ยวข้องกับการก่อการร้ายแต่อย่างใด เช่น ทนายความ นักเขียน นักหนังสือพิมพ์ นักการเมือง และนักแสดง เป็นจำนวนอย่างน้อย 150 ราย ในระหว่างเดือนมกราคม ค.ศ. 1983 ถึงเดือนมีนาคม ค.ศ. 1986 โดยปราศจากมาตรการที่จะให้ความคุ้มครองแก่ผู้ที่ถูกดักฟัง นอกไปจากนี้ การดังฟังโทรศัพท์ของหน่วยต่อต้านการก่อการร้ายยังไม่ได้รับการควบคุมตรวจสอบจากหน่วยงานใดทั้งสิ้น การกระทำดังกล่าวถือว่าเป็นการละเมิดสิทธิในการมีชีวิตส่วนตัวของผู้ที่ถูกดังฟัง ส่วนสาเหตุที่บุคคลบางกลุ่มถูกดักฟังบทสนทนาทางโทรศัพท์ ในครั้งนี้เป็นเพราะความกังวลว่าบุคคลเหล่านี้จะนำเรื่องบางเรื่อง หรือความลับบางอย่าง เช่น เรื่องของ Mazarine ลูกสาวนอกสมรสของประธานาธิบดี François Mitterrand ปัญหาสุขภาพของประธานาธิบดีที่ปกปิดว่าตนเองเป็นโรคมะเร็ง ข้อเท็จจริงของคดี les Irandais de Vincennes ที่เจ้าหน้าที่ตำรวจได้ทำการจับกุม

---

[69] พิมพ์ดาว จันทรชันตี, คดีการดักฟังโทรศัพท์และสิทธิในการมีชีวิตส่วนตัว (Le procès des écoutes de l'Elysée et le droit à la vie privée), (เผยแพร่วันที่ 27 ธันวาคม 2547)

ผู้ก่อการร้ายชาวไอร์แลนด์พร้อมหลักฐานที่ประกอบไปด้วยระเบิดและอาวุธปืนจำนวนหนึ่งแต่ปรากฏว่าหลักฐานดังกล่าวเป็นหลักฐานที่เจ้าหน้าที่ตำรวจได้จัดทำขึ้นไปเผยแพร่แก่ประชาชน

และสิ่งที่กังวลมากกว่านั้น คือ หลักฐานบางประการทำให้สามารถระบุได้ว่าการดักฟังบทสนทนาทางโทรศัพท์ของนักหนังสือพิมพ์บางรายได้รับคำสั่งโดยตรงมาจากประธานาธิบดี François Mitterrand เอง เพราะมีลายเซ็นต์รับทราบของท่านประธานาธิบดีปรากฏอยู่บนเอกสาร แต่อย่างไรก็ตามประธานาธิบดีได้ปฏิเสธถึงการกระทำดังกล่าวว่าทำเนียบประธานาธิบดีไม่เคยใช้ระบบการดักฟังโทรศัพท์และตนเองไม่เคยได้อ่านบทสนทนาทางโทรศัพท์เหล่านั้น ท่าทีและคำพูดดังกล่าวของประธานาธิบดี François Mitterrand ถือเป็นการโกหกที่ร้ายแรงของผู้นำรัฐ ยิ่งเมื่อถูกนำไปเทียบกับคดี Watergate ของประเทศสหรัฐอเมริกา ในกรณีที่ประธานาธิบดี Richard Nixon ภายหลังจากที่ข้อเท็จจริงเกี่ยวกับการดักฟังโทรศัพท์ได้ถูกเปิดเผยต่อสาธารณะชน ประธานาธิบดี Richard Nixon ได้แสดงความรับผิดชอบด้วยการลาออกจากตำแหน่ง อย่างไรก็ตามการเปิดเผยข้อมูลว่ามีการดักฟังโทรศัพท์ของหน่วยงานของทำเนียบประธานาธิบดีได้นำมาซึ่งจุดสิ้นสุดของหน่วยต่อต้านการก่อการร้ายในเดือนกันยายน ค.ศ. 1988

การดักฟังโทรศัพท์โดยไม่มีมาตรการคุ้มครองผู้ที่ถูกดังฟัง และขาดการควบคุมตรวจสอบโดยหน่วยงานใดหน่วยงานหนึ่ง เช่นการกระทำที่หน่วยต่อต้านการก่อการร้ายได้กระทำนั้นถือเป็นการละเมิดสิทธิเสรีภาพขั้นพื้นฐานของมนุษย์ในการที่จะได้รับความเคารพในชีวิตส่วนตัวและชีวิตครอบครัว* ตามที่กฎหมายกำหนดไว้ว่า หากฝ่ายปกครองหรือหน่วยงานของรัฐจะเข้าไปแทรกแซงในการใช้สิทธิดังกล่าว การแทรกแซงต้องได้รับการบัญญัติไว้ในรัฐบัญญัติ และการแทรกแซงจะต้องเป็นมาตรการที่จำเป็นต่อความความมั่นคงและปลอดภัยของประเทศ ไม่ว่าจะเป็นความปลอดภัยทางเศรษฐกิจของประเทศ การรักษาความสงบเรียบร้อยของสังคมและการป้องกันอาชญากรรม การคุ้มครองสุขภาพและศีลธรรม และการคุ้มครองสิทธิและเสรีภาพของผู้อื่น

กฎหมายภายในของประเทศฝรั่งเศสแบ่งการดักฟังโทรศัพท์ออกเป็น 2 ประเภท คือ การดักฟังโดยฝ่ายตุลาการ (Lesécoutes judiciaires) และการดักฟังโดยฝ่ายปกครอง

---

* The European Convention on Human Rights of Council of Europe

Article 8

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. ...

(Lesécoutes administratives) ดังนั้น การดักฟังโทรศัพท์โดยบุคคลทั่วไปจึงถือเป็นการกระทำที่ผิดกฎหมายอาญาฝรั่งเศส*

นอกไปจากนี้ยังได้ระบุอีกว่า วัตถุประสงค์ในการดักฟังโทรศัพท์สามารถกระทำได้เพื่อความมั่นคงของประเทศ เพื่อคุ้มครองขีดความสามารถทางด้านวิทยาศาสตร์และเศรษฐกิจของชาติ เพื่อป้องกันการก่อการร้ายและการก่ออาชญากรรม เทปที่บันทึกบทสนทนาทางโทรศัพท์จะต้องถูกระบุไว้ในบัญชีที่จัดทำขึ้นภายใต้การควบคุมดูแลของนายกรัฐมนตรี บัญชีดังกล่าวจะครอบคลุมรายละเอียดต่างๆ ที่เกี่ยวข้องกับการดักฟัง และจะต้องถูกทำลายภายใน 10 วัน หลังจากที่มีการดักฟังเกิดขึ้น สิ่งเดียวที่สามารถถูกถอดออกมาเป็นข้อความและสามารถเก็บรักษาไว้ได้คือ เทปบันทึกที่มีส่วนเกี่ยวข้องหรือมีความสัมพันธ์กับวัตถุประสงค์ของการขอดักฟังโทรศัพท์ เช่น บทสนทนาที่พูดถึงการเตรียมการเพื่อกระทำการก่อการร้ายซึ่งเกี่ยวพันกับวัตถุประสงค์ที่ว่าด้วยความมั่นคงของประเทศและการปราบปรามการก่อการร้าย อย่างไรก็ตาม ข้อความที่ถูกถอดออกมาจะต้องถูกทำลายในทันทีที่ไม่มีความจำเป็นจะต้องเก็บรักษาข้อมูลนั้นไว้อีกต่อไป

จะเห็นได้ว่าประเทศฝรั่งเศสได้เห็นถึงความสำคัญของสิทธิในการมีชีวิตส่วนตัวและสิทธิในการที่จะได้รับความเคารพในชีวิตส่วนตัวและชีวิตครอบครัวของประชาชน และยังประสบความสำเร็จในการใช้การดักฟังโทรศัพท์เพื่อสืบหาตัวคนร้ายและเพื่อปกป้องความมั่นคงของประเทศ ในขณะเดียวกันกับที่สามารถให้การคุ้มครองสิทธิของประชาชนในการมีชีวิตส่วนตัวได้อีกด้วย

ข. กฎหมายการกระทำความผิดเกี่ยวกับ Spam Mail

การกระทำความผิดในลักษณะนี้ได้ถูกกำหนดไว้ใน Mail Posts and Telecommunications Code การกระทำความผิดประเภทนี้บัญญัติไว้ในกฎหมายการกระทำ

---

* Article 226-1 of Penal Code

A penalty of one year's imprisonment and a fine of □45,000 is incurred for any willful violation of the intimacy of the private life of other persons by resorting to any means of:

1. intercepting, recording or transmitting words uttered in confidential or private circumstances, without the consent of their speaker;

2. taking, recording or transmitting the picture of a person who is within a private place, without the consent of the person concerned ...

ความผิดเกี่ยวกับไปรษณีย์และการโทรคมนาคม บทบัญญัติทั่วไป (Article L34-5) ซึ่งบัญญัติเกี่ยวกับการให้บริการโทรคมนาคม

ค. กฎหมายทรัพย์สินทางปัญญา (Intellectual Property Code)

การให้ความคุ้มครองทรัพย์สินทางปัญญาผู้เขียนจะกล่าวถึงเฉพาะในกรณีงานอันมีลิขสิทธิ์เพื่อแสดงให้เห็นถึงการปฏิบัติตามพันธกรณีของอนุสัญญาที่กำหนดให้ประเทศภาคีมีหน้าที่ตามความตกลงระหว่างประเทศที่ตนเป็นภาคี ดังนั้น การคุ้มครองงานอันมีลิขสิทธิ์และสิทธิ์ข้างเคียงของประเทศฝรั่งเศสจึงเป็นไปตามความตกลงระหว่างประเทศที่ก่อให้เกิดพันธกรณี คือ อนุสัญญากรุงเบิร์น (Berne Convention of September 9th, 1886) อนุสัญญาทั่วไปของกรุงเจนีวา (Universal Convention of Geneva of September 6th, 1952) อนุสัญญากรุงโรม (Rome Convention of October 26, 1961) ความตกลงว่าด้วยสิทธิในทรัพย์สินทางปัญญาที่เกี่ยวกับการค้า (TRIPs Agreement of April 15th, 1994)

การคุ้มครองในอันมีงานลิขสิทธิ์ไม่ว่าจะเป็น นาฏกรรม ศิลปกรรม ดนตรีกรรม โสตทัศนวัสดุ ภาพยนตร์ สิ่งบันทึกเสียง งานแพร่เสียงแพร่ภาพ หรืองานอื่นใดในแผนกวรรณคดี วิทยาศาสตร์หรือแผนกศิลปะ ไม่ว่าจะแสดงออกโดยวิธีหรือรูปแบบใด การคุ้มครองซึ่งงานอันมีลิขสิทธิ์เหล่านี้ประเทศฝรั่งเศสให้คุ้มครองทันทีที่มีการสร้างสรรค์ผลงาน ทั้งนี้ ไม่มีข้อบังคับในการจดทะเบียนเพื่อให้ได้รับความคุ้มครองในงานอันมีลิขสิทธิ์ตามกฎหมาย Intellectual Property Code ผู้สร้างสรรค์งานที่เป็นทรัพย์สินทางปัญญาจะมีสิทธิแต่เพียงผู้เดียว ซึ่งสามารถใช้บังคับต่อบุคคลทั่วไปได้ งานอันมีลิขสิทธิ์รวมถึงงานที่ถูกสร้างสรรค์ขึ้น ที่มีแนวความคิดของผู้สร้างสรรค์ร่วมอยู่ด้วย แม้ว่างานดังกล่าวจะยังไม่เสร็จสมบูรณ์และโดยไม่คำนึงว่างานดังกล่าวจะได้รับการเปิดเผยต่อสาธารณชนแล้วหรือไม่ สิทธิในทรัพย์สินทางปัญญา (Intellectual Property Rights) เป็นสิทธิในการหาประโยชน์ทางเศรษฐกิจจากทรัพย์สินทางปัญญา ซึ่งอาจประกอบด้วยการโอนสิทธิหรืออนุญาตให้ใช้สิทธิตลอดจนสิทธิต่างๆ เพื่อการใช้ประโยชน์แก่ตนเอง ดังเช่นการผลิต การทำซ้ำหรือดัดแปลง การนำงานออกเผยแพร่ต่อสาธารณชน ทั้งนี้ ขึ้นอยู่กับบทบัญญัติของกฎหมายอันเกี่ยวกับทรัพย์สินทางปัญญาแต่ละประเภทได้กำหนดหลักเกณฑ์และขอบเขตแห่งสิทธิไว้เพื่อรองรับ ซึ่งโดยทั่วไปแล้วกฎหมายจะกำหนดให้เป็นสิทธิแต่ผู้เดียว (exclusive right) ของเจ้าของทรัพย์สินทางปัญญาเหล่านั้น[70] กฎหมายจึงต้องการคุ้มครองงานอันมีลิขสิทธิ์ดังกล่าวโดยได้กำหนดให้การกระทำในลักษณะดังกล่าวต่อไปนี้เป็นความผิดตามกฎหมาย

---

[70] ไชยยศ เหมะรัชตะ, ข้อตกลงเกี่ยวกับสิทธิในทรัพย์สินทางปัญญา[Online]. แหล่งข้อมูล: http://www.ftadigest.com/fta/pdf/SME05_IP.pdf[2553, มกราคม 11]

1. การกำหนดให้เจ้าหน้าที่มีอำนาจยึดสิ่งบันทึกเสียงและสิ่งที่บันทึกภาพที่มีการทำผิดกฎหมายโดยการทำซ้ำซึ่งสิ่งบันทึกเสียงและสิ่งบันทึกภาพ ผลิตภัณฑ์ที่ได้จากการคัดลอกเลียนแบบ ทำสำเนา ทำแม่พิมพ์บันทึกเสียงและบันทึกภาพจากต้นฉบับหรือสำเนา หรือนำเข้าอย่างผิดกฎหมาย และติดตั้งอุปกรณ์พิเศษเพื่อวัตถุประสงค์ในการยึดสิ่งของ อุปกรณ์และผลิตภัณฑ์ที่เกิดจากการกระทำโดยการละเมิดลิขสิทธิ์ (Article L335-1) การดัดแปลง, ทำซ้ำ, เผยแพร่งานสู่สาธารณะชน

2. การทำซ้ำ การสื่อสาร หรือการให้บริการแก่สาธารณะโดยไม่มีค่าใช้จ่ายและไม่มีการเรียกเก็บ หรือการเผยแพร่งานที่มีลิขสิทธิ์ ไม่ว่าจะป็นสิ่งบันทึกเสียงและสิ่งบันทึกภาพหรือโปรแกรมต่างๆ โดยไม่ได้รับอนุญาตจากผู้ผลิต ผู้เป็นเจ้าของสิ่งบันทึกเสียงและสิ่งบันทึกภาพ รวมถึงบริษัทซึ่งเป็นเจ้าของงานโสตทัศน์ เช่น ภาพยนตร์โทรทัศน์ วิทยุ และกฎหมายยังกำหนดให้การกระทำที่ละเมิดลิขสิทธิ์รวมไปถึง การนำเข้าหรือส่งออกซึ่งสิ่งบันทึกเสียงและสิ่งบันทึกภาพโดยไม่ได้รับอนุญาตจากเจ้าของงานดังกล่าว และการไม่จ่ายค่าตอบแทนในการใช้งานลิขสิทธิ์ให้แก่ผู้ผลิต ผู้เป็นเจ้าของสิ่งบันทึกเสียงและสิ่งบันทึกภาพ รวมถึงบริษัทซึ่งเป็นเจ้าของงานโสตทัศน์ (Article L335-4)

3. การทำซ้ำ การเผยแพร่งานหรือการทำให้แพร่หลายซึ่งงานที่แสดงออกทางความคิดไม่ว่าโดยวิธีใดก็ตามถือว่าเป็นการละเมิดลิขสิทธิ์ (Article L335-3) ตัวอย่างคดีการกระทำความผิดเกี่ยวกับเครื่องหมายการค้า ที่เป็นคดีการละเมิดลิขสิทธิ์ เช่น

คดี France Bater v. Alain Oddoz[71] คดีนี้เกิดขึ้นเมื่อเดือนกุมภาพันธ์ ค.ศ. 2005 อาจารย์ชาวฝรั่งเศสชื่อ นาย Aliain Oddoz อายุ 28 ปี ได้รับโทษปรับเป็นจำนวนเงิน 10,200 ยูโร ถือได้ว่าเป็นการดำเนินครั้งใหญ่กับการกระทำความผิดในข้อหาละเมิดลิขสิทธิ์จากการใช้แฟ้มข้อมูลคอมพิวเตอร์ร่วมกันอย่างผิดกฎหมาย ถูกจับกุมเมื่อวันที่ 18 สิงหาคม ค.ศ. 2004 ซึ่งมีการติดต่อสอบสวนของหน่วยงานที่มีอำนาจตามกฎหมายในฝรั่งเศสในเว็บไซต์ที่มีการละเมิดลิขสิทธิ์เพลงในคอมพิวเตอร์ โดยนาย Aliain เป็นผู้ใช้บริการทั่วไปของเว็บไซต์ดังกล่าว และถูกกล่าวหาว่ามีการละมิดลิขสิทธิ์เพลงโดยผิดกฎหมายมากถึงจำนวน 30 กิกะไบต์ นาย Aliain จ่ายเงินเป็นค่าประกันตัว 3000 ยูโร ตัวแทนของอุตสาหกรรมเพลงได้ขอให้ศาลกำหนดค่าความเสียหายเป็นค่าปรับด้วย ทั้งนี้ ศาลอุทธรณ์ได้ทำการเปิดเผยข้อมูลว่ามีผู้ถูกดำเนินคดีเกี่ยวกับการละเมิดลิขสิทธิ์และคัดลอกภาพยนตร์เป็นจำนวนมากถึง 500 ร้อยเรื่องบน

---

[71] Computer Crime Research Center. MOHAMED CHAWKI. Cybercrime in France: An Overview[Online]. 2004.

อินเทอร์เน็ต และทำการแบ่งปันข้อมูลผิดกฎหมายดังกล่าวบุคคลอื่น โดยศาลได้ตัดสินตาม Article L-122-5 ตามกฎหมายทรัพย์สินทางปัญญา ที่กำหนดว่า ห้ามทำสำเนาหรือทำซ้ำซึ่งที่มีวัตถุประสงค์ในการใช้ส่วนบุคคล แม้ว่าการตัดสินในครั้งนี้จะแสดงให้เห็นว่าอาจป้องกันการละเมิดลิขสิทธิ์ได้ที่มีประมาณ 50 คดี ที่รอการตัดสินและในอดีตที่ผ่านมาศาลได้มีคำพิพากษาเกี่ยวกับคดีละเมิดลิขสิทธิ์

ง. กฎหมายเกี่ยวกับบัตรเครดิต

ในประเทศฝรั่งเศสมีกฎหมายที่ใช้บังคับกับการประกอบธุรกิจบัตรเครดิตโดยมิได้มีการบัญญัติไว้เป็นการเฉพาะกฎหมาย ซึ่งกฎหมายที่ใช้บังคับกับการประกอบธุรกิจบัตรเครดิตได้แก่ประมวลกฎหมายเงินตราและการเงิน (Code monétaire et financier) ซึ่งได้กำหนดหลักเกณฑ์ทั่วไปเกี่ยวกับบัตรจ่ายเงินและบัตรเครดิต ดังนี้

คำจำกัดความและความหมาย (Article L 131-1) ความหมายของคำว่า "บัตรจ่ายเงิน" และ"บัตรถอนเงิน" โดยกฎหมายบัญญัติให้ "บัตรจ่ายเงิน" หมายถึง บัตรที่ออกโดยสถาบันการเงิน สถาบันหรือหน่วยงานตามที่กฎหมายกำหนด ซึ่งเจ้าของบัตรนั้น (ผู้ถือบัตร) สามารถใช้บัตรถอนหรือโอนเงินได้

ส่วน "บัตรถอนเงิน" ได้แก่ บัตรที่ออกโดยสถาบันการเงิน สถาบันหรือหน่วยงานตามที่กฎหมายกำหนด ซึ่งเจ้าของบัตรหรือผู้ถือบัตรสามารถใช้บัตรนั้นถอนเงินได้

ทั้งนี้ การจ่ายเงินด้วยบัตรเครดิตไม่อาจถอนคืนได้และจะสามารถคัดค้านการจ่ายเงินได้เฉพาะกรณีที่บัตรสูญหาย ถูกขโมย หรือมีการใช้บัตรโดยฉ้อฉล หรือโดยกระบวนการพิทักษ์ทรัพย์เท่านั้น (Article L 132-2)

หลักเกณฑ์ความรับผิดชอบในกรณีบัตรหายหรือถูกขโมยได้กำหนดไว้ว่าหากยังไม่แจ้งคัดค้านผู้ถือบัตรต้องรับผิดชอบในการจ่ายเงินภายในวงเงินที่จำกัดตามกฎหมาย เว้นแต่จะเป็นกรณีที่ผู้ถือบัตรประมาทเลินเล่ออย่างร้ายแรงหรือมิได้แจ้งคัดค้านการจ่ายเงินภายในระยะเวลาที่เหมาะสม ซึ่งกฎหมายได้กำหนดระยะเวลาการคัดค้านดังกล่าวเป็นไปตามที่กำหนดในสัญญา แต่จะต้องไม่ต่ำกว่า 2 วัน (Article L 132-3)

ข้อยกเว้นความรับผิดของผู้ถือบัตร หากมีการจ่ายเงินโดยฉ้อฉล ณ สถานที่อื่นโดยที่ไม่มีการใช้บัตรนั้นจริงและในกรณีที่มีการใช้บัตรปลอม (Article L 132-4) การกำหนดให้ผู้ออกบัตรคืนค่าธรรมเนียมธนาคารให้แก่ผู้ถือบัตรที่มีการใช้บัตรโดยฉ้อฉล (Article L 132-5)

กำหนดระยะเวลาการใช้สิทธเรียกร้องของผู้ถือบัตรที่จะต้องใช้สิทธิดังกล่าวภายในเจ็ดสิบวันนับแต่วันที่มีการใช้บัตรซึ่งเป็นกรณีที่ผู้ถือบัตรจะโต้แย้งการจ่ายเงินได้ ระยะเวลาดังกล่าวอาจขยายออกไปได้ตามข้อกำหนดของสัญญา แต่จะต้องไม่เกินกว่าหนึ่งร้อยยี่สิบวัน (Article L 132-6)

กฎหมายกำหนดความผิดเกี่ยวกับบัตรเครดิตไว้ 3 กรณีด้วยกันคือ (Article L 163-4) การปลอมแปลงบัตรจ่ายเงินหรือบัตรถอนเงิน การใช้หรือพยายามใช้บัตรจ่ายเงินปลอมหรือบัตรจ่ายเงินปลอม และการยอมรับการชำระเงินโดยใช้บัตรจ่ายเงินปลอม

ความผิดเกี่ยวกับเครื่องมือหรือวัสดุที่ใช้ในการทำบัตรปลอม ซึ่งได้แก่ กรณีผลิต รับมา ครอบครอง โอน ให้ หรือจัดให้มีเครื่องมือ อุปกรณ์ โปรแกรมคอมพิวเตอร์หรือข้อมูลต่างๆที่ได้มาหรือทำขึ้นโดยเฉพาะ เพื่อการทำบัตรจ่ายเงินหรือบัตรถอนเงินปลอม (Article L 163-4-1)

ความผิดฐานใช้เช็คปลอม การใช้บัตรจ่ายเงินหรือบัตรถอนเงินปลอม และการผลิตหรือมีเครื่องมือหรืออุปกรณ์ต้องรับโทษตามกฎหมาย (Article L 163-4-2)

กฎหมายยังบัญญัติให้ริบวัตถุที่ใช้ในการกระทำความผิด ซึ่งได้แก่บัตรจ่ายเงินหรือบัตรถอนเงินปลอม รวมทั้งเครื่องมือและอุปกรณ์ที่ใช้ในการผลิตบัตรปลอม เพื่อนำไปทำลาย ทั้งนี้ เว้นแต่เจ้าของทรัพย์สินนั้นจะไม่ได้รู้เห็นในการกระทำความผิดด้วย (Article L 163-5) และสามารถกำหนดโทษเพิ่มเติมสำหรับกรณีการกระทำความผิดเกี่ยวกับบัตรเครดิต ซึ่งได้แก่ความผิดปลอมบัตรจ่ายเงินหรือบัตรถอนเงิน ใช้บัตรจ่ายเงินหรือบัตรถอนเงินปลอม รับชำระเงินที่จ่ายโดยการใช้บัตรปลอม และผลิต มีไว้ในครอบครอง จำหน่ายเครื่องมือหรืออุปกรณ์ที่ใช้ในการทำบัตรปลอม (Article L 163-6) โดยกำหนดให้ศาลสามารถสั่งลงโทษด้วยการห้ามมิให้ใช้สิทธิพลเมือง เช่น สมัครหรือลงคะแนนเลือกตั้ง สิทธิในทางแพ่ง เช่น การเป็นพยานในศาล และสิทธิในครอบครัว เช่น การเป็นผู้ปกครองหรือผู้อนุบาล และห้ามมิให้ประกอบอาชีพหรือกิจกรรมทางสังคมได้ ทั้งนี้ ภายในระยะเวลาไม่เกินห้าปี

ส่วนการกำหนดโทษในทางอาญาสำหรับการกระทำความผิดของนิติบุคคลในกรณีที่ผู้กระทำความผิดเกี่ยวกับบัตรจ่ายเงินหรือบัตรถอนเงินเป็นนิติบุคคล โดยกำหนดโทษปรับหรือโทษอื่น เช่น การยกเลิกนิติบุคคลนั้น หรือห้ามดำเนินกิจการอย่างหนึ่งอย่างใดอย่างเด็ดขาดหรือภายในระยะเวลาที่กำหนด ห้ามทำสัญญากับหน่วยงานของรัฐ หรือริบทรัพย์สิน (Article L 163-10-1) การกำหนดความผิดและโทษในกรณีที่มีการใช้ข้อมูลข่าวสารที่รวบรวมไว้โดย

ธนาคารแห่งชาติฝรั่งเศส นอกเหนือไปจากวัตถุประสงค์ที่กฎหมายบัญญัติไว้ โดยกำหนดให้ได้รับโทษในอัตราเดียวกันกับความผิดฐานใช้ข้อมูลข่าวสารผิดวัตถุประสงค์ตามกฎหมายอาญา (Article L 163-11)

กล่าวโดยสรุป กำหนดฐานความผิดเกี่ยวกับบัตรเครดิตไว้ 5 กรณีด้วยกันคือ การปลอมแปลงบัตร การใช้บัตรปลอม การยอมรับการใช้บัตรปลอม การผลิต ครอบครอง หรือจำหน่าย เครื่องมือหรืออุปกรณ์ที่ใช้ในการทำบัตรปลอม และใช้ข้อมูลข่าวสารที่ได้มาจากการประกอบธุรกิจบัตรผิดวัตถุประสงค์

จากกฎหมายที่ได้กล่าวไปข้างต้น ปัจจุบันประเทศฝรั่งเศสยังได้มีการเสนอให้นำกฎหมายเกี่ยวกับการตัดการเชื่อมต่ออินเทอร์เน็ตในกรณีดาวน์โหลดผิดกฎหมายลิขสิทธิ์ (Hadopi 2) เข้าสู่สภา ล่าสุดกฎหมายดังกล่าวได้ผ่านการลงมติของสภาฝรั่งเศส (National Assembly of France) ไปด้วยคะแนน 285 ต่อ 225 ซึ่งกฎหมายดังกล่าวอยู่ระหว่างประกาศใช้ในฝรั่งเศส[72] โดยพรรคฝ่ายขวาที่ครองเสียงข้างมาก Union for a Popular Movement ของประธานาธิบดีนิโคลา ซาร์โกซี สนับสนุนกฎหมายฉบับนี้ ส่วนพรรคสังคมนิยมฝรั่งเศส (Parti socialiste : PS) ซึ่งเป็นพรรคฝ่ายค้านในปัจจุบัน ได้ร้องต่อศาลรัฐธรรมนูญให้พิจารณาความสอดคล้องต่อรัฐธรรมนูญของร่างกฎหมายเกี่ยวกับการตัดการเชื่อมต่ออินเทอร์เน็ตของฝรั่งเศส

ผู้แทนฝ่ายค้าน ให้เหตุผลว่ากฎหมายดังกล่าว แม้ว่าจะได้แก้ไขร่างเดิมที่ให้อำนาจเจ้าหน้าที่ฝ่ายปกครองในการตัดการเชื่อมต่ออินเทอร์เน็ตมาเป็นการให้อำนาจกับศาลแล้วก็ตาม แต่ก็ยังไม่เคารพสิทธิเสรีภาพมูลฐานในด้านศาล โดยเฉพาะหลักสำคัญในการสันนิษฐานว่าจำเลยเป็นผู้บริสุทธิ์ กล่าวคือร่างกฎหมายที่บัญญัติให้ใช้ "กระบวนการทางศาลแบบง่าย" คือใช้ผู้พิพากษาเพียงคนเดียวในการตัดสินคดี (ตัดสินว่าจะต้องตัดการเชื่อมต่ออินเทอร์เน็ตหรือไม่) รวมถึง ไม่ให้สิทธิกับจำเลยในการโต้แย้ง (contradictory procedure) หรือไม่ออกนั่งบัลลังก์เหมือนคดีทั่วไป กฎหมายฉบับนี้กำหนดว่า หากจับได้ว่ามีการแชร์ไฟล์แบบผิดกฎหมาย ให้หน่วยงานที่มีอำนาจดำเนินการ 3 ขั้นตอนดังนี้

1. แจ้งเตือนทางอีเมลล์

2. แจ้งเตือนทางจดหมาย

3. ทำการตัดอินเทอร์เน็ต หากพบว่ายังแชร์ไฟล์ผิดกฎหมายอยู่

---

[72] สำนักข่าว BBC[Online]. Available from : http://www.blognone.com/topics/law[2010, January 11]

การดำเนินการดังกล่าวข้างต้น หมายถึง ในชั้นแรกกฎหมายดังกล่าวจะกำหนดให้ทางการแจ้งเตือนผู้ดาวน์โหลดผิดกฎหมายให้หยุดการกระทำที่ฝ่าฝืนลิขสิทธิ์ โดยหากไม่ปฏิบัติตามก็อาจจะโดนลดแบนด์วิธการดาวน์โหลด หรือโดนตัดการเชื่อมต่ออินเทอร์เน็ตในที่สุด ดังนั้นเมื่อมีผู้ยื่นร่างกฎหมายฉบับนี้ให้ศาลรัฐธรรมนูญพิจารณาแบบนี้ การประกาศใช้กฎหมายนี้ก็ต้องเลื่อนออกไปก่อนจนกระทั่งศาลรัฐธรรมนูญมีคำวินิจฉัยแล้ว[73] ต่อมาเมื่อศาลรัฐธรรมนูญได้มีคำวินิจฉัยแล้วว่าร่างกฎหมายดังกล่าวไม่ขัดต่อรัฐธรรมนูญ ซึ่งในคำวินิจฉัยเดียวกันศาลรัฐธรรมนูญได้ตัดสินว่า บทบัญญัติของกฎหมายดังกล่าวในส่วนที่ให้อำนาจรัฐบาลในการกำหนดเงื่อนไขสำหรับการจ่ายค่าสินไหมทดแทนให้เจ้าของลิขสิทธิ์โดยผู้กระทำผิดนั้น ขัดต่อรัฐธรรมนูญและให้แก้ไขบทบัญญัติดังกล่าวให้กำหนดเงื่อนไขลงไปในตัวกฎหมายเอง[74]

อนึ่ง หลังการประกาศใช้กฎหมายฉบับนี้ผู้ใช้อินเทอร์เน็ตรายใดในประเทศฝรั่งเศสที่ทำการดาวน์โหลดข้อมูลต่างๆแบบผิดกฎหมายก็จะได้รับแจ้งให้หยุดการกระทำผิดกฎหมายนั้นและหากไม่ปฏิบัติตามการเชื่อมต่ออินเทอร์เน็ตของผู้ใช้รายนั้นก็จะถูกระงับในที่สุด และภายหลังจากที่กฎหมายเกี่ยวกับการตัดการเชื่อมต่ออินเทอร์เน็ตในฝรั่งเศสกำลังจะมีผลบังคับใช้ ประเทศอังกฤษก็กำลังเตรียมร่างกฎหมายประเภทเดียวกัน

3.2.2.2 มาตรการทางด้านความร่วมมือระหว่างประเทศ

หลักการส่งผู้ร้ายข้ามแดนในประเทศฝรั่งเศส[75] โดยทั่วไปกำหนดไว้ดังนี้

หลักการเกี่ยวกับการห้ามส่งคนชาติ ประเทศฝรั่งเศสเป็นประเทศแม่แบบของแนวความคิดการไม่ส่งคนชาติข้ามแดน ดังตามที่ปรากฏใน The Brabantine Bull และตามแนวปฏิบัติระหว่างประเทศฝรั่งเศสกับเนเธอร์แลนด์ ในกรณีการส่งผู้ร้ายข้ามแดนที่เกิดขึ้นเมื่อ ค.ศ. 1736 แต่การปฏิบัติดังกล่าวก็มีข้อโต้แย้งว่าในการปฏิบัติไม่ได้มีการห้ามอย่างเด็ดขาดไม่ให้ส่งคนชาติข้ามแดน กล่าวคือ แนวปฏิบัติของประเทศฝรั่งเศสกับเนเธอร์แลนด์มิได้เป็นสนธิสัญญา แต่เป็นเพียงหลักต่างตอบแทนโดยขึ้นอยู่กับกฎหมายภายในของทั้งสองประเทศ ซึ่งมี

---

[73] Le Monde หนังสือพิมพ์ภาษาฝรั่งเศส[ออนไลน์]. 2553, แหล่งข้อมูล: http://www.lemonde.fr/technologies/article/2009/09/28/hadopi-2-le-ps-saisit-le-conseil-constitutionnel_1246409_651865.html#xtor=RSS-3208[2553, มกราคม 11]

[74] แถลงข่าวโดยศาลรัฐธรรมนูญฝรั่งเศส[Online] แหล่งข้อมูล : http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/decisions/2009590dc/compresse_590dc.pdf[2553, มกราคม 11]

[75] ชัชวาลย์ สุขสมจิตร์, งานวิจัยหลักสูตรผู้บริหารกระบวนการยุติธรรมระดับสูง อาชญากรรมทางเศรษฐกิจกับการบังคับใช้กฎหมาย, วิทยาลัยการยุติธรรม สถาบันพัฒนาข้าราชการฝ่ายตุลาการศาลยุติธรรม สำนักงานศาลยุติธรรม, หน้า 14-16.

องค์ประกอบในขณะนั้นที่จะต้องพิจารณาประกอบด้วย เช่น ศาสนา ประวัติศาสตร์ และสภาพทางภูมิศาสตร์ จากแนวปฏิบัติตามสนธิสัญญาที่ประเทศฝรั่งเศสทำไว้กับประเทศต่างๆแสดงให้เห็นการผ่อนคลายหลักการเกี่ยวกับการส่งคนชาติ โดยจะมีการพิจารณาถึงความเหมาะสมและนโยบายทางการเมืองด้วย เช่น สนธิสัญญาระหว่างประเทศฝรั่งเศสและประเทศสเปนได้ระบุไว้ในสนธิสัญญาว่าสนธิสัญญาฉบับนี้บังคับใช้กับคนชาติของคู่ภาคีเช่นเดียวกันบุคคลในรัฐอื่น ซึ่งก็หมายความว่าทั้งประเทศสเปนและฝรั่งเศสสามารถส่งคนชาติได้

สนธิสัญญาระหว่างประเทศฝรั่งเศสกับสาธารณรัฐเฮลเวติก ได้ระบุไว้ว่าจะไม่ส่งคนชาติของตนให้แก่กันและกัน เว้นแต่อาชญากรรมที่คุกคามต่อสาธารณะ ซึ่งก็ได้ระบุข้อความที่คล้ายกันนี้ในสนธิสัญญาที่มีกับ Basle ในปี ค.ศ. 1780 ต่อมาได้มีการเพิ่มเติมบทบัญญัติของสนธิสัญญาระหว่างประเทศฝรั่งเศสกับ Basle ในปี ค.ศ. 1781 ให้มีการส่งคนชาติในกรณีที่เป็นอาชญากรรมที่ไม่ร้ายแรงด้วย (minor crime) เช่น ความผิดฐานลักขโมย เป็นต้น และให้คู่ภาคีมีการบังคับตามคำพิพากษาของศาลที่ความผิดเกิดขึ้น ในปี ค.ศ. 1811 จักรพรรดินโปเลียนได้มีประกาศ (decree) ว่าสามารถส่งคนชาติฝรั่งเศสในฐานะผู้ร้ายข้ามแดนไปยังประเทศอื่นได้ แต่อย่างไรก็ดีไม่ได้ มีการปฏิบัติตามประกาศนี้ซึ่งทำให้มีข้อถกเถียงกันมาก โดยฝ่ายที่ไม่เห็นด้วยให้เหตุผลว่าการส่งคนชาติมีข้อห้ามอยู่ในกฎหมายมหาชนของฝรั่งเศสในช่วงปี ค.ศ. 1788 แต่ต่อมาได้มีการกล่าวถึงในรัฐสภาของปารีสในปี ค.ศ. 1814 ว่าสามารถส่งคนชาติได้แต่ในประเด็นนี้ก็ยังมีข้อโต้แย้งกันอยู่ จนกระทั่ง ค.ศ. 1841 กระทรวงยุติธรรมได้มีหนังสือเวียน ห้ามรัฐบาลฝรั่งเศสส่งคนชาติฝรั่งเศสไปยังประเทศอื่น หลังจากนั้นเป็นต้นมารัฐบาลฝรั่งเศสได้มีการเจรจาจัดทำสนธิสัญญากับประเทศอังกฤษ และประเทศสหรัฐอเมริกา ซึ่งแม้ว่าจะไม่มีการระบุเกี่ยวกับการยกเว้นการส่งคนชาติ แต่ในทางปฏิบัติแล้วรัฐบาลฝรั่งเศสก็ไม่ได้ส่งคนชาติของตนให้ประเทศอื่นๆเลย หลังจากปี ค.ศ. 1844 การปฏิบัติและการจัดทำสนธิสัญญาของฝรั่งเศสกับยึดกับหลักการไม่ส่งคนชาติของตนข้ามแดนอย่างสม่ำเสมอ จากแนวคิดดังกล่าว อาจถือได้ว่าฝรั่งเศสเป็นผู้วางรากฐานแนวความคิดนี้และมีอิทธิพลกับประเทศที่ยึดถือระบบประมวลกฎหมาย โดยพิจารณาได้จากสนธิสัญญาที่อยู่ใน United Nations Treaty Series Volumes 1–550 ซึ่งมีจำนวนทั้งสิ้น 163 ฉบับ โดยใน 98 ฉบับห้ามการส่งคนชาติข้ามแดนอย่างเด็ดขาด ส่วนอีก 57 ฉบับ ให้อำนาจกับรัฐผู้ร้องขอในการใช้ดุลพินิจส่งคนชาติตนข้ามแดนมีเพียง 8 ฉบับที่บัญญัติไว้ให้ส่งผู้ร้ายข้ามแดนได้โดยไม่ต้องคำนึงถึงสัญชาติของผู้ถูกกล่าวหาอย่างไรก็ดีประเทศฝรั่งเศสมีระบบการใช้กฎหมายอาญาแบบอำนาจเหนือบุคคล (Personal Jurisdiction) ซึ่งกฎหมายระหว่างประเทศมีการยอมรับอำนาจของรัฐที่มีบุคคลต่างด้าวมากระทำผิดในดินแดนและยอมรับอำนาจพิเศษเหนือบุคคลที่มีสัญชาติกระทำผิดในต่างประเทศ เรื่องสัญชาติจึงเป็น

รากฐานสำหรับการใช้อำนาจเหนือบุคคล ในคดีอาญามีการยอมรับในยุโรปและลาตินอเมริกา ทำให้ประเทศเหล่านี้สามารถฟ้องบุคคลที่มีสัญชาติตนในประเทศได้

แบบพิธีการส่งผู้ร้ายข้ามแดนของประเทศฝรั่งเศส[76] กรณีแบบฝรั่งเศสเป็นแบบพิธีการซึ่งไม่ยอมให้อำนาจทางตุลาการเข้ามาพัวพัน กล่าวคือ ศาลไม่มีสิทธิเข้ามามีส่วนในการพิจารณาคำร้องขอให้ส่งผู้ร้ายข้ามแดน แนวปฏิบัติของฝรั่งเศส มีดังนี้

1. คำร้องขอส่งผู้ร้ายข้ามแดนปกติจะกระทำผ่านรัฐมนตรีกระทรวงการต่างประเทศโดยผู้แทนทางการทูต โดยเมื่อรัฐมนตรีกระทรวงการต่างประเทศรับคำขอการพิจารณาของรัฐมนตรีกระทรวงการต่างประเทศนั้นก็จะพิจารณาคำร้องนั้นว่าถูกต้องตามแบบหรือไม่ กล่าวคือ คำร้องนั้นได้กระทำตามกระบวนการต่างๆที่กำหนดไว้ในแบบพิธีการปฏิบัติการทางทูตถูกต้องหรือไม่

2. หากรัฐมนตรีกระทรวงการต่างประเทศเห็นว่ากระบวนการยื่นคำร้องนั้นไม่ถูกต้องก็จะส่งคำร้องคืนไปยังประเทศผู้ร้องขอ โดยปฏิเสธไม่ยอมส่งผู้ร้ายข้ามแดน

3. หากคำร้องนั้นถูกต้องปฏิบัติตามแบบทุกอย่าง ก็จะส่งคำร้องไปยังรัฐมนตรีกระทรวงยุติธรรมซึ่งจะพิจารณาเฉพาะปัญหาข้อกฎหมายเท่านั้น อันได้แก่ หลักฐานเกี่ยวกับหมายจับพยานบุคคลต่างๆ ข้อหา อายุความ ข้อความต่างๆที่มีอยู่ในสนธิสัญญากฎหมายผู้ร้ายข้ามแดน และเป็นบุคคลผู้กระทำผิดจริงหรือไม่ เป็นต้น

4. การที่รัฐมนตรีกระทรวงยุติธรรมพิจารณาปัญหาข้อกฎหมายนี้ อาจจะให้พนักงานอัยการ (ในประเทศฝรั่งเศสพนักงานขึ้นอยู่กับกระทรวงยุติธรรม) พิจารณาว่าข้อกฎหมายเพียงพอหรือยังที่จะส่งบุคคลนั้นข้ามแดน

5. หากไม่มีข้อบกพร่องเกี่ยวกับปัญหาข้อกฎหมายแล้ว รัฐมนตรีกระทรวงยุติธรรมก็รายงานไปยังรัฐมนตรีกระทรวงการต่างประเทศ เพื่อสั่งขังบุคคลผู้กระทำผิดรอการส่งผู้ร้ายข้ามแดนต่อไป

6. รัฐมนตรีกระทรวงการต่างประเทศเป็นผู้ดำเนินการใช้ดุลพินิจ ส่วนการออกคำสั่งให้ประธานาธิบดีลงนามนั้นเป็นเรื่องเกี่ยวกับระเบียบวิธีในการบริหารราชการแผ่นดิน แม้ว่ารัฐมนตรีกระทรวงยุติธรรมจะวินิจฉัยปัญหาข้อกฎหมายถูกต้องทุกอย่างก็ตาม ไม่ได้หมายความ

---

[76] เรื่องเดียวกัน, หน้า 16.

ว่ารัฐมนตรีต่างประเทศจะปฏิเสธไม่ได้ ดุลพินิจขั้นสุดท้ายนั้นอยู่กับรัฐมนตรีต่างประเทศเพราะถือว่าการส่งผู้ร้ายข้ามแดนเป็นเรื่องของความสัมพันธ์ระหว่างประเทศอย่างหนึ่ง ซึ่งต้องอาศัยการดำเนินนโยบายของแต่ละประเทศเป็นสำคัญ

การห้ามส่งผู้ร้ายข้ามแดนเกี่ยวกับความผิดทางการเมือง ประเทศฝรั่งเศสใช้หลักว่าด้วยการกระทำที่กระทบกระเทือนต่ออำนาจอธิปไตยของประเทศ ในการพิจารณาว่าคดีใดเป็นคดีการเมืองหรือไม่ ซึ่งหลักการดังกล่าวหมายถึง หากการกระทำความผิดใดที่ได้กระทำเพื่อเปลี่ยนแปลงอำนาจการปกครองของประเทศไม่ว่าจะเป็น อำนาจนิติบัญญัติ อำนาจบริหาร อำนาจตุลาการ หรือหากการกรพทำความผิดนั้นเกิดขึ้นเพราะต้องการเปลี่ยนแปลง ยกเลิกอำนาจดังกล่าวถือว่าเป็นคดีการเมือง

3.2.3 ปัญหาและอุปสรรคในการปฏิบัติตามพันธกรณีแห่งอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001

สิทธิส่วนบุคคล (Droit de la vie Privée) กฎหมายฝรั่งเศสได้ยอมรับและให้ความสำคัญเกี่ยวกับเรื่องสิทธิส่วนบุคคล ขอบเขตสิทธิส่วนบุคคลถูกกำหนดภายใต้ประโยชน์ส่วนรวมเป็นหลัก การกระทำความผิดโดยการหมิ่นประมาท ในกฎหมายฝรั่งเศสได้กำหนดไว้แตกต่างจากกฎหมายทั่วไป เนื่องจากกฎหมายอาญาฝรั่งเศสได้กำหนดไว้เป็นการเฉพาะเจาะจงให้หมายถึง การห้ามกระทำที่เป็นการแบ่งแยกเชื้อชาติ หรือเลือกปฏิบัติโดยมีเหตุจากความแตกต่างทางด้านเชื้อชาติ เสรีภาพด้านการแสดงความคิดเห็น การแสดงออก และด้านข่าวสารถือเป็นสิ่งสำคัญของสังคมประชาธิปไตย แต่ในความเป็นจริงเสรีภาพดังกล่าวถูกริดรอนในรูปแบบต่างๆ ไม่ว่าจะเป็นการห้าม การจับกุม การดำเนินการทางกฎหมาย การข่มขู่ หรือการกระทำบางอย่างซึ่งมีผลต่อชีวิต โครงการขององค์กรเอ็นจีโอซึ่งจะเสนอผลงานหรือโครงการเข้ารับรางวัลจะต้องมีวัตถุประสงค์ที่จะส่งเสริมความเคารพในเสรีภาพดังกล่าว โดยใช้สื่อต่างๆ ไม่ว่าจะเป็นหนังสือพิมพ์ วิทยุ มัลติมีเดีย และโดยเฉพาะอย่างยิ่งอินเทอร์เน็ต ทั้งนี้ อาจเป็นโครงการอบรมหรือโครงการประชาสัมพันธ์แก่บุคคลทั่วไปให้ทราบเกี่ยวกับเสรีภาพด้านข่าวสาร ซึ่งเป็นการปกป้องบุคคลซึ่งถูกคุกคาม จำกัดเสรีภาพ หรือถูกจับกุม นอกจากนี้ องค์กรเอ็นจีโอยังต้องทำหน้าที่รายงานประเทศต่างๆ ให้ทราบถึงความสำคัญของปัญหาที่เกิดขึ้น และกระตุ้นให้มีการต่อสู้เพื่อเสรีภาพดังกล่าว[77] ตัวอย่างคดี เช่น

---

[77] สถานเอกอัครราชทูตฝรั่งเศส ประจำประเทศไทย (Embassy of France in Thailand)[ออนไลน์]. 2553, แหล่งข้อมูล : http://www.france.or.th/th/article.php3?id_article=761[2553, มกราคม 11]

คดีบริษัท Yahoo ศาลอาญาของฝรั่งเศสได้เปิดเผยว่า ได้เตรียมทำการฟ้องดำเนินคดีกับเว็บไซต์ Yahoo.com และ Timothy Koogle ผู้บริหารระดับสูงของ Yahoo.com เนื่องจากกระทำความผิดโดยละเมิดกฎหมายฝรั่งเศสในการเปิดประมูลและจำหน่ายสินค้าของกลุ่มนาซีสมัยสงครามโลกครั้งที่ 2 ซึ่งถือว่าเป็นกลุ่มอาชญากรสงคราม โดยถ้า Timothy Koogle ถูกศาลอาญาตัดสินว่ามีความผิดก็อาจจะถูกจำคุกถึง 5 ปี และเสียค่าปรับถึง 39,800 ดอลลาร์สหรัฐ โดยก่อนหน้านี้ในช่วงเดือนพฤศจิกายนปี ค.ศ. 2000 รัฐบาลฝรั่งเศสได้ทำหนังสือขอให้เว็บไซต์ Yahoo.com ระงับการประมูล และหยุดจำหน่ายสินค้าของกลุ่มนาซีให้กับประชาชนฝรั่งเศส เนื่องจากการจำหน่ายและแสดงสินค้าที่เกี่ยวกับการเหยียดเชื้อชาตินั้นเป็นการละเมิดกฎหมายของฝรั่งเศส แต่ Yahoo.com ก็ได้เพิกเฉยไม่ได้กระทำการช่วยเหลือใดๆทั้งสิ้น

ทั้งนี้ Yahoo ได้ยื่นคำร้องต่อศาลสหรัฐโต้คำสั่งศาลฝรั่งเศส Yahoo ได้ยื่นคำร้องให้ศาลประเทศสหรัฐอเมริกามีคำสั่งว่ารัฐบาลประเทศฝรั่งเศสไม่มีสิทธิ์ในการควบคุมการทำงานของบริษัท และ Yahoo ได้ยื่นคำร้องต่อศาลประเทศสหรัฐอเมริกาให้มีคำสั่งว่าศาลประเทศฝรั่งเศสไม่มีสิทธิ์ที่จะปรับเงินกับบริษัท Yahoo ซึ่งอยู่ในประเทศอเมริกา หลังจากที่ศาลฝรั่งเศสได้มีคำสั่งให้ Yahoo คิดระบบป้องกันไม่ให้มีการประมูลสินค้าเกี่ยวกับลัทธินาซีในประเทศฝรั่งเศส และจะปรับ Yahoo เป็นจำนวน 13905 เหรียญต่อวันถ้ามีการนำสินค้าเกี่ยวกับนาซีขึ้นบนส่วนประมูลของ Yahoo ซึ่งทาง Yahoo ได้โต้แย้งว่าศาลฝรั่งเศสสามารถที่จะควบคุมได้เฉพาะบริษัทที่ดูแล Yahoo ในฝรั่งเศสเท่านั้น[78]

และเนื่องจากฝรั่งเศสเป็นประเทศที่มีจำนวนชาวมุสลิมและชาวยิวอยู่มากปัญหาการเหยียดสีผิวและการแบ่งแยกชนชาติจึงมีความรุนแรง นับตั้งแต่เกิดสถานการณ์ที่มีการก่อการร้ายในตอนกลางของภาคตะวันออกของประเทศฝรั่งเศส ทำให้ชาวยิวไม่มีความปลอดภัยในชีวิตและทรัพย์สิน ซึ่งผลกระทบที่เกิดขึ้นหลังจากเกิดวิกฤตการณ์ดังกล่าว คือ การรังเกียจและกีดกันเด็กชาวมุสลิมในประเทศฝรั่งเศสจากเด็กชาวฝรั่งเศส เช่น การต่อต้านและรังเกียจนักเรียนชาวมุสลิมที่โพกผ้าคลุมศีรษะในโรงเรียน ฝรั่งเศสจึงพยายามเสาะหาวิธีการยับยั้งการแพร่กระจายของแนวคิดต่อต้านชาวมุสลิมของเด็กๆอยู่ตลอด โดยได้มีการใช้การติดต่อสื่อสารทางอินเทอร์เน็ตโดยมีเจตนาปลุกระดมให้เกิดการต่อต้านและแบ่งแยกชนชาติ

จากปัญหาที่เกิดขึ้นจะเห็นได้ว่าสิทธิเสรีภาพในการสื่อสารและการแสดงออกซึ่งความคิดเห็นผ่านการเขียนและสิ่งพิมพ์ได้รับการคุ้มครองตามรัฐธรรมนูญของประเทศฝรั่งเศส ส่วนการ

---

[78] Available from: http://www.pantip.com/tech/newscols/news/270202i.shtml. [2010, January 11]

คุ้มครองข้อมูลและสิทธิส่วนบุคคลนั้นได้ถูกบัญญัติให้ได้รับการคุ้มครองตามกฎหมายเฉพาะ คือ บทบัญญัติเกี่ยวกับเสรีภาพในการสื่อสารผ่านทางกฎหมายอินเทอร์เน็ต ซึ่งกฎหมายนี้ใช้กับการหมิ่นประมาทผ่านทางอินเทอร์เน็ต รวมทั้งการแสดงออกถึงการเกลียดชังและการแสดงสื่อลามกอนาจารเกี่ยวกับเด็ก ได้มีการจัดตั้งองค์กรที่มีอำนาจหน้าที่เกี่ยวกับการรับเรื่องร้องเรียน การแนะนำปัญหา การเผยแพร่รายงานประจำปี และเป็นองค์กรที่ทำหน้าที่เป็นนายทะเบียนควบคุมการประมวลผลข้อมูลต่างๆ เกี่ยวกับข้อมูลส่วนบุคคลซึ่งองค์กรดังกล่าว คือ The National Commission on Informatics and Liberties (Commission Nationale Informatique et Libertés) โดยมีหลักการสำคัญในการควบคุมการประมวลผลข้อมูลส่วนบุคคล การห้ามเก็บข้อมูลที่ผิดกฎหมายทุกประเภท การกำหนดวัตถุประสงค์ในการเก็บข้อมูลอย่างชัดเจน[79]

3.2.4 ผลกระทบจากการการปฏิบัติตามพันธกรณีแห่งอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001

รัฐธรรมนูญของประเทศฝรั่งเศสฉบับลงวันที่ 4 ตุลาคม ค.ศ. 1958 ได้บัญญัติไว้โดยเฉพาะถึงกรณีของสนธิสัญญาในลักษณะ VI (Titre VI) ว่าด้วยสนธิสัญญาและความตกลงระหว่างประเทศ (Des traités et accords internationaux) โดยมาตรา 52* แห่งรัฐธรรมนูญฉบับดังกล่าวให้อำนาจประธานาธิบดีของสาธารณรัฐที่จะเจรจาและให้สัตยาบันแก่สนธิสัญญาและการเจรจาทั้งปวงซึ่งนำไปสู่การทำความตกลงระหว่างประเทศที่ไม่ต้องการให้สัตยาบันก็จะต้องแจ้งให้ประธานาธิบดีทราบ[80]

มาตรา 53** แห่งรัฐธรรมนูญของฝรั่งเศสเดียวกันนั้นก็บัญญัติไว้อย่างชัดเจนว่าสนธิสัญญาประเภทใดบ้างที่ต้องได้รับการให้สัตยาบันหรือได้รับความเห็นชอบโดยการออกเป็น

---

[79] Available from: http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-103764. [2010, January 11]

* Article 52.

Le Président de la République négocie et ratifie les traités.

Il est informé de toute négociation tendant à la conclusion d'un accord international non soumis à ratification.

คำแปล มาตรา 52

ประธานาธิบดีแห่งสาธารณรัฐเป็นผู้เจรจาและให้สัตยาบันสนธิสัญญาทั้งหลาย

ประธานาธิบดีแห่งสาธารณรัฐต้องได้รับรายงานผลการเจรจาเพื่อการทำข้อตกลงระหว่างประเทศที่ไม่ต้องมีการให้สัตยาบัน

[80] จุมพต สายสุนทร, กฎหมายระหว่างประเทศ เล่ม 1, พิมพ์ครั้งที่ 6 (กรุงเทพฯ: สำนักพิมพ์วิญญูชน, 2549), หน้า 129.

** Article 53.

กฎหมาย และผู้ที่จะให้สัตยาบันแก่สนธิสัญญาดังกล่าวได้แก่ประธานาธิบดีของสาธารณะรัฐตามมาตรา 52 ดังกล่าวข้างต้น เมื่อมีการให้สัตยาบันดังกล่าวแล้ว สนธิสัญญาเช่นว่านั้นจะมีผลผูกพันฝรั่งเศสในฐานะที่เป็นภาคีแห่งสนธิสัญญา และเมื่อมีการออกกฎหมายเพื่ออนุวัติการสนธิสัญญาดังกล่าวแล้ว สนธิสัญญานั้นจึงจะมีผลบังคับใช้ในฐานะที่เป็นกฎหมายภายในของประเทศฝรั่งเศส

และตามมาตรา 55* แห่งรัฐธรรมนูญของฝรั่งเศสเดียวกันนั้นก็บัญญัติไว้ในกรณีที่ว่าสนธิสัญญาและความตกลงซึ่งได้รับการให้สัตยาบันหรือได้รับความเห็นชอบและประกาศใช้แล้วนั้นจะมีผลบังคับใช้สูงกว่ากฎหมายภายในของฝรั่งเศสหรือไม่นั้นขึ้นอยู่กับว่า ภาคีอีกฝ่ายหนึ่งแห่งสนธิสัญญาหรือภาคีอื่นๆ แห่งสนธิสัญญาและความตกลงเช่นว่านั้นจะยอมใช้บังคับสนธิสัญญาและความตกลงเช่นว่านั้นสูงกว่ากฎหมายภายในของตนหรือไม่ กล่าวอีกนัยหนึ่งคือฝรั่งเศสใช้หลักถ้อยทีถ้อยปฏิบัติ[81] ในการใช้บังคับสนธิสัญญาและความตกลงระหว่างประเทศในฐานะที่เป็นกฎหมายภายใน ซึ่งถ้าหากรัฐภาคีอื่นๆแห่งสนธิสัญญาและความตกลงนั้นยอมใช้บังคับสนธิสัญญาและความตกลงเช่นว่านั้นเหนือหรือสูงกว่ากฎหมายภายในของภาคี ฝรั่งเศสจึงจะยอมใช้บังคับสนธิสัญญาและความตกลงนั้นสูงกว่ากฎหมายภายในของตนเช่นกัน ซึ่งนั่นย่อมหมายความว่าหากภาคีรัฐอื่นๆ แห่งสนธิสัญญาและความตกลงนั้นไม่ยอมใช้บังคับสนธิสัญญา

Les traités de paix, les traités de commerce, les traits ou accords relatifs à l'organisation internationale, ceux qui engagent les finances de l'État, ceux qui modifient des dispositions de nature législative, ceux qui sont relatifs à l'état des personnes, ceux qui comportent cession, échange ou adjonction de territoire, ne peuvent être ratifiés ou approuvés qu'en vertu d'une loi. Ils ne prennent effet qu'après avoir été ratifiés ou approuvés. Nulle cession, nul échange, nulle adjonction de territoire n'est valable sans le consentement des populations intéressées.

คำแปล มาตรา 53

สนธิสัญญาสงบศึก สนธิสัญญาทางการค้า สนธิสัญญาหรือความตกลงเกี่ยวกับองค์การระหว่างประเทศ สนธิสัญญาหรือข้อตกลงที่มีผลผูกพันทางด้านการเงินต่อรัฐ สนธิสัญญาหรือข้อตกลงที่แก้ไขเปลี่ยนแปลงบทบัญญัติที่มีลักษณะเป็นรัฐบัญญัติ สนธิสัญญาหรือข้อตกลงเกี่ยวกับสถานภาพของบุคคล สนธิสัญญาหรือข้อตกลงเกี่ยวกับการยกให้ การแลกเปลี่ยน หรือการผนวกดินแดน จะได้รับการให้สัตยาบันหรือความเห็นชอบได้ก็โดยผลของรัฐบัญญัติ สนธิสัญญาหรือข้อตกลงดังกล่าวจะมีผลใช้บังคับได้ ก็ต่อเมื่อได้รับการให้สัตยาบันหรือความเห็นชอบแล้วการยกให้ การแลกเปลี่ยนหรือการผนวกดินแดนใด จะมีผลใช้บังคับได้ก็ต่อเมื่อได้รับความยินยอมจากประชาชนที่เกี่ยวข้องแล้ว

* Article 55.

Les traités ou accords régulièrement ratifiés ou approuvés ont, dès leur publication, une autorité supérieure à celle des lois, sous réserve, pour chaque accord ou traité, de son application par l'autre partie.

คำแปล มาตรา 55 สนธิสัญญาหรือข้อตกลงที่ได้รับการให้สัตยาบันแล้วหรือได้รับความเห็นชอบโดยชอบแล้วให้มีผลใช้บังคับนับตั้งแต่ที่ได้มีการประกาศใช้บังคับ ย่อมมีฐานะทางกฎหมายสูงกว่ารัฐบัญญัติ ทั้งนี้ ภายใต้ข้อสงวนที่ว่าคู่สัญญาอีกฝ่ายหนึ่งจะต้องบังคับใช้สนธิสัญญาหรือข้อตกลงนั้นเช่นเดียวกัน

[81] จุมพต สายสุนทร, กฎหมายระหว่างประเทศ เล่ม 1, หน้า 130.

และความตกลงนั้นเหนือกว่าหรือสูงกว่ากฎหมายภายในของตน ฝรั่งเศสก็จะไม่ถือว่าสนธิสัญญาและความตกลงเช่นว่านั้นมีฐานะสูงกว่ากฎหมายของตนตามมาตรา 55 ของรัฐธรรมนูญฝรั่งเศส

ทั้งนี้ ในกรณีที่สนธิสัญญาและความตกลงที่ได้ประกาศใช้แล้วตามมาตรา 55 และมีผลบังคับสูงกว่ากฎหมายภายในตามเงื่อนไขที่กำหนด สนธิสัญญาและความตกลงเช่นว่านั้นย่อมมีผลบังคับเหนือกว่ากฎหมายภายในที่มีบทบัญญัติในเรื่องเดียวกันและกฎหมายภายในเช่นว่านั้นจะขัดหรือยกเลิกสนธิสัญญาและความตกลงเช่นว่านั้นมิได้ ไม่ว่ากฎหมายภายในเช่นว่านั้นจะมีผลใช้บังคับอยู่แล้วก่อนหรือหลังการประกาศใช้สนธิสัญญาและความตกลงก็ตาม

จากการลงนามในอนุสัญญาดังกล่าวปัญหาและอุปสรรคที่เกิดขึ้นได้ส่งผลกระทบเกี่ยวกับสิทธิส่วนบุคคลที่ประเทศฝรั่งเศสให้การคุ้มครองเช่นเดียวกับประเทศสหรัฐอเมริกา ประเทศฝรั่งเศสได้มีการออกกฎหมายห้ามมิให้มีการเก็บข้อมูลส่วนบุคคลโดยไม่เป็นธรรมหรือโดยผิดกฎหมาย (Article 226-18 of the Criminal Code) การประมวลผลของคอมพิวเตอร์จะต้องเป็นการดำเนินการตามวัตถุประสงค์ที่กำหนดไว้อย่างชัดเจน วัตถุประสงค์ดังกล่าวต้องมีการวางไว้อย่างเหมาะสมและเพียงพอ หมายถึงการเลือกเก็บข้อมูลบางประเภทภายใต้ระยะเวลาในการเก็บรักษาข้อมูลที่เหมาะสม การใช้ข้อมูลส่วนบุคคลจะต้องใช้เพื่อวัตถุประสงค์ที่ได้กำหนดไว้ หากมีการใช้ข้อมูลดังกล่าวผิดวัตถุประสงค์หรือเกินกว่าวัตถุที่กำหนดไว้ กฎหมายฝรั่งเศสได้กำหนดการกระทำดังกล่าวเป็นความผิดทางอาญา* และได้มีการบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคล The Daily Safety Law (Loi sur la sécurité quotidienne : LSQ)

ประเทศฝรั่งเศสยังมีการใช้มาตรการทางเทคนิคโดยการประกาศแผนติดตั้งระบบป้องกันเยาวชนจากภัยอินเตอร์เน็ตทั่วประเทศ เพื่อปิดกั้นไม่ให้เยาวชนเข้าสู่เว็บไซต์ที่มีเนื้อหาเกี่ยวกับลัทธิเหยียดสีผิวหรือลัทธิต่อต้านชาวยิว ซึ่งถือเป็นการแก้ไขปัญหาอาชญากรรมที่เกิดจากการเหยียดสีผิวในฝรั่งเศส โดยระบบนี้จะตรวจจับรายชื่อเว็บไซต์ที่เข้าข่ายต้องห้ามแล้วเก็บไว้ในฐานข้อมูล จากนั้นจะทำการตรวจสอบรายชื่อทุกวันโดยผู้ให้บริการอินเตอร์เน็ตที่เป็นสมาชิกในกลุ่มองค์กรต่อต้านการเหยียดสีผิวของฝรั่งเศส จากนั้นจะส่งต่อไปยังสำนักงานตำรวจแห่งชาติฝรั่งเศส เพื่อสืบสวนหาตัวผู้จัดตั้งเว็บไซต์และลงโทษขั้นเด็ดขาดต่อไป

---

* Article 226-21 and Article 226-20 of the Criminal Code : using personal data for purposes other than those that justified their collection, or storing them beyond a date justified by the purpose of the processing is punished, respectively, by 5 years' imprisonment...

จากที่กล่าวในบทนี้จะเห็นได้ว่าสถานการณ์ต่างๆที่เกิดขึ้นของทั้งสองประเทศมีความคล้ายคลึงกัน จากพันธกรณีที่เกิดขึ้นกับประเทศภาคีสมาชิกทั้งสองประเทศจะเห็นได้ว่าได้มีการดำเนินการตามบทบัญญัติของอนุสัญญาทั้งในส่วนของมาตรการทางสารบัญญัติและมาตรการทางสบัญญัติ ทั้งนี้ แม้มาตรการทางด้านความร่วมมือระหว่างประเทศเกี่ยวกับการดำเนินการเพื่อป้องกันและปราบปรามผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์จะยังไม่ชัดเจน แต่ประเทศภาคีทั้งสองต่างสามารถแก้ไขข้อขัดข้องที่อาจเกิดขึ้นได้โดยบังคับใช้กฎหมายในส่วนของความร่วมมือระหว่างประเทศตามที่กำหนดในอนุสัญญา

ในส่วนผลกระทบที่เกิดจากการลงนามเป็นภาคีของทั้งของประเทศนั้นจากเหตุผลที่ผู้เขียนได้กล่าวไปว่าทั้งสองประเทศให้ความกังวลเกี่ยวกับการคุ้มครองสิทธิส่วนบุคคลอันจะเป็นผลกระทบจากการดำเนินมาตรการทางด้านสบัญญัติขององค์กร หน่วยงาน หรือเจ้าหน้าที่ที่เกิดขึ้นตามบทบัญญัติในอนุสัญญา แต่ประเทศภาคีทั้งสองก็ได้ดำเนินมาตรการบัญญัติกฎหมายเกี่ยวกับการคุ้มครองสิทธิส่วนบุคคลอันอาจเกิดผลกระทบจากอนุสัญญาดังกล่าว ทั้งนี้ ผู้เขียนให้ข้อสังเกตเกี่ยวกับการแก้ไขข้อขัดข้องที่เกิดขึ้นไม่ว่าจะเป็นการสร้างความสามารถของรัฐในการคุ้มครองประชาชนจากภัยคุกคามต่างๆที่เกี่ยวกับการคุ้มครองความเป็นอยู่ส่วนตัว สิทธิและเสรีภาพในการสื่อสาร หากรัฐไม่มีการบัญญัติกฎหมายที่ให้ความคุ้มครองในเรื่องดังกล่าว บุคคลต่างๆไม่จำกัดเพศ ไม่จำกัดอายุสามารถใช้เทคโนโลยีดังกล่าวอย่างเสรีโดยไม่มีข้อจำกัดแล้ว รัฐอาจประสบปัญหาในการบังคับใช้กฎหมายในการตรวจจับการสื่อสารของผู้กระทำความผิดในทางตรงกันข้ามหากรัฐมีนโยบายในการควบคุมการใช้งานระบบคอมพิวเตอร์ดังกล่าว อย่างเข้มงวดเกินไป ก็อาจละเมิดความเป็นอยู่ส่วนตัว และเสรีภาพในการสื่อสารของประชาชน