กลไกความร่วมมือทางอาญาระหว่างประเทศ ภายใต้กรอบของอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ของสภายุโรป

นายณัฐพัฒน์ เลิศประพจน์กุล

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญานิติศาสตรมหาบัณฑิต
สาขาวิชานิติศาสตร์
คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2555

INTERNATIONAL CRIMINAL COOPERATION MECHANISMS UNDER THE FRAMEWORK OF EUROPEAN COUNCIL'S CONVENTION ON CYBERCRIME

Mister Nattapat Lertprapotekul

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Laws

Faculty of Law

Chulalongkorn University

Academic Year 2013

หัวข้อวิทยานิพนธ์	กลไกความร่วมมือทางอาญาระหว่างประเทศภายใต้กรอบของอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของสภายุโรป
โดย	นายณัฐพัฒน์ เลิศประพจน์กุล
สาขาวิชา	นิติศาสตร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	ผู้ช่วยศาสตราจารย์ ดร. ศารทูล สันติวาสะ

คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

.....คณบดีคณะนิติศาสตร์
(ศาสตราจารย์ ดร.ศักดา ธนิตกุล)

คณะกรรมการสอบวิทยานิพนธ์

.....ประธานกรรมการ
(ผู้ช่วยศาสตราจารย์ สุผานิต เกิดสมเกียรติ)

.....อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(ผู้ช่วยศาสตราจารย์ ดร.ศารทูล สันติวาสะ)

.....กรรมการภายนอกมหาวิทยาลัย
(ผู้ช่วยศาสตราจารย์ ดร.พินัย ณ นคร)

.....กรรมการภายนอกมหาวิทยาลัย
(พันตำรวจเอก ญาณพล ยั่งยืน)

ณัฐพัฒน์ เลิศประพจน์กุล : กลไกความร่วมมือทางอาญาระหว่างประเทศภายใต้กรอบของอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของสภายุโรป (THE MECHANISMS FOR INTERNATIONAL COOPERATION IN CRIMINAL MATTERS UNDER THE FRAMEWORK OF COUNCIL OF EUROPE'S CONVENTION ON CYBERCRIME) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: ผศ.ดร.ศารทูล สันติวาสะ, 264 หน้า.

การวิจัยนี้มีจุดประสงค์เพื่อศึกษากลไกความร่วมมือทางอาญาระหว่างประเทศภายใต้อนุสัญญาว่าด้วยอาชญากรรรมทางคอมพิวเตอร์ของสภายุโรป หรืออนุสัญญากรุงบูดาเปสต์ ว่าสามารถตอบสนองต่ออาชญากรรมทางคอมพิวเตอร์ ซึ่งเป็นอาชญากรรมที่เกิดขึ้นใหม่ได้เพียงใด ทั้งนี้ การให้ความร่วมมือทางอาญาระหว่างประเทศ นับเป็นสิ่งที่จำเป็นยิ่งในการปราบปรามอาชญากรรมทางคอมพิวเตอร์ซึ่งเกิดขึ้นได้โดยไม่เกาะเกี่ยวกับเขตแดนทางกายภาพ

ผลการศึกษาวิจัยพบว่า อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของสภายุโรปมีบทบาทด้านการกำหนดมาตรฐานร่วมกันสำหรับกฎหมายภายในประเทศเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ อีกทั้งยังขยายขอบเขตความร่วมมือระหว่างประเทศให้ครอบคลุมอาชญากรรมทางคอมพิวเตอร์ด้วย อย่างไรก็ตาม อนุสัญญาฉบับนี้ยังจำเป็นต้องเพิ่มเติมรายละเอียดของกลไกความร่วมมือ เพื่อให้สามารถรองรับความซับซ้อนของอาชญากรรมทางคอมพิวเตอร์ที่ทวีขึ้นไปตามกาลเวลาได้

สาขาวิชา นิติศาสตร์ ลายมือชื่อนิสิต .....

ปีการศึกษา 2555 ลายมือชื่อ อ.ที่ปรึกษาวิทยานิพนธ์หลัก .....

5185971934 : MAJOR LAWS
KEYWORDS : INTERNATIONAL CRIMINAL COOPERATION / CYBERCRIME / EXTRADITION / MUTUAL LEGAL ASSISTANCE

NATTAPAT LERTPRAPOTEKUL : THE MECHANISMS FOR INTERNATIONAL COOPERATION IN CRIMINAL MATTERS UNDER THE FRAMEWORK OF COUNCIL OF EUROPE'S CONVENTION ON CYBERCRIME. ADVISOR : ASSIST. PROF. SARATOON SANTIVASA, Ph.D., 264 pp.

This research aims to study the international criminal cooperation mechanisms under the framework of European Council's Convention on Cybercrime. It will evaluate to what extent that the mechanisms provided can respond the phenomenon of cybercrime, which is considered as new category of crimes. It is noted that international criminal cooperation has a vital role in responding and suppressing cybercrime, which can occurred without any attachments to physical state boundaries.

The study reveals that European Council's Convention on Cybercrime does has a vital role in establishing the common standards for parties' domestic legislations related to cybercrime. Furthermore, the convention also extends international criminal cooperation mechanisms so that they can cover cybercrime. Nevertheless, more details and contents should be included in the convention so that it can effectively respond to cybercrime, which can become even more complex as the time goes by.

Field of Study : LAWS Student's Signature .....

Academic Year : 2012 Advisor's Signature .....

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สามารถสำเร็จลุล่วงไปได้ด้วยความช่วยเหลืออย่างดียิ่งของท่านผู้ช่วยศาสตราจารย์ ดร. ศารทูล สันติวาสะ อาจารย์ที่ปรึกษาวิทยานิพนธ์ ซึ่งท่านได้ให้คำแนะนำข้อคิดเห็นต่างๆ อันเป็นประโยชน์อย่างยิ่งต่อผู้เขียนตลอดระยะเวลาการทำวิจัยจวบจนวิทยานิพนธ์ฉบับนี้เสร็จสมบูรณ์ ผู้เขียนขอกราบขอบพระคุณเป็นอย่างสูง

ขอขอบพระคุณ ท่านผู้ช่วยศาสตราจารย์สุผานิต เกิดสมเกียรติ ท่านผู้ช่วยศาสตราจารย์ ดร. พินัย ณ นคร และท่านพันตำรวจเอก ญาณพล ยั่งยืน ที่ได้ให้คำแนะนำอันเป็นประโยชน์ต่อการปรับปรุงแก้ไขวิทยานิพนธ์ให้สมบูรณ์ยิ่งขึ้น โดยกรุณาสละเวลาช่วยตรวจสอบและแก้ไขข้อบกพร่อง อีกทั้งยังให้ข้อคิดอันมีคุณค่าเป็นอย่างมากต่อวิทยานิพนธ์ฉบับนี้

ขอขอบพระคุณเพื่อนๆ พี่ๆ น้องๆ ทุกคนที่ให้ความช่วยเหลือและให้กำลังใจจนวิทยานิพนธ์ฉบับนี้เสร็จสมบูรณ์

ท้ายนี้ผู้เขียนขอขอบพระคุณบิดา มารดา และน้องสาวของผู้เขียน ที่คอยให้ความช่วยเหลือ สนับสนุน ให้กำลังใจและห่วงใยผู้เขียนตลอดมา

หากการทำวิทยานิพนธ์ฉบับนี้จะมีประโยชน์ทางวิชาการอยู่บ้าง ผู้เขียนขอมอบให้เป็นกตเวทิตาแด่ บิดา มารดาของผู้เขียน รวมทั้งบูรพาจารย์ทุกท่านที่ประสิทธิประสาทวิชาความรู้และคุณธรรมแก่ผู้เขียนตลอดมา หากมีข้อบกพร่องประการใด ผู้เขียนขอน้อมรับไว้แต่เพียงผู้เดียว

สารบัญ

หน้า

หน้า

หน้า

หน้า

หน้า

หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของการวิจัย

เทคโนโลยีคอมพิวเตอร์ โดยเฉพาะในด้านเครือข่ายอินเตอร์เน็ตนั้น นับเป็นโครงสร้างพื้นฐานหนึ่งที่พัฒนาไปอย่างรวดเร็วที่สุดในปัจจุบัน ด้วยเครือข่ายอินเตอร์เน็ต ระบบคอมพิวเตอร์ต่างๆทั่วโลกที่ดำรงอยู่เป็นเอกเทศก็เชื่อมโยงเป็นเครือข่ายมากขึ้น ส่วนผู้ใช้งานคอมพิวเตอร์และเครือข่ายอินเตอร์เน็ตก็ได้ทวีจำนวนเพิ่มขึ้นตามไปด้วย นอกจากนี้ ผลิตภัณฑ์หรือบริการบางประเภทที่ไม่เคยพึ่งพาเทคโนโลยีทางคอมพิวเตอร์หรือเครือข่ายอินเตอร์เน็ตมาก่อน เช่น บริการสาธารณูปโภค บริการขนส่ง ล้วนถูกเชื่อมโยงเข้ากับเครือข่ายทางอินเตอร์เน็ตเพื่อให้สะดวกรวดเร็วในการบริหารจัดการมากขึ้น

พัฒนาการทางเทคโนโลยีเหล่านี้ ส่งผลให้เทคโนโลยีทางคอมพิวเตอร์และเครือข่ายอินเตอร์เน็ตเข้ามามีบทบาทสำคัญในสังคมมนุษย์อย่างที่ไม่เคยเป็นมาก่อน โดยในระดับปัจเจกบุคคลนั้น เทคโนโลยีทางคอมพิวเตอร์ช่วยให้บุคคลสามารถประกอบกิจกรรมได้อย่างสะดวกสบายมากขึ้น ไม่ว่าจะเป็นในด้านการทำงาน การทำธุรกรรม การติดต่อสื่อสาร หรือ การพักผ่อนหย่อนใจ ยกตัวอย่างเช่น จดหมายทางอิเล็คโทรนิกส์หรือ E-mail โปรแกรมสนทนา และโปรแกรมโทรศัพท์ทางอินเตอร์เน็ต เป็นต้น เทคโนโลยีเหล่านี้ สามารถอำนวยความสะดวกให้ผู้ใช้งานติดต่อสื่อสารกับผู้ใช้อีกรายได้ภายในระยะเวลาอันสั้น โดยปราศจากค่าใช้จ่าย และไม่จำเป็นต้องคำนึงถึงว่าอีกฝ่ายหนึ่งนั้นจะอยู่ ณ จุดใดของโลกก็ตาม นอกจากนี้ เทคโนโลยีด้านเครือข่ายทางสังคม (Social Network) ก็ยังเป็นพื้นที่ให้ผู้ใช้งานเครือข่ายอินเตอร์เน็ตรายต่างๆสามารถเข้าคบหาสมาคมกัน อีกทั้งยังสามารถแลกเปลี่ยนข้อมูลข่าวสารในรูปแบบต่างๆระหว่างกันได้อีกด้วย สำหรับภาครัฐ เทคโนโลยีเครือข่ายอินเตอร์เน็ตสามารถอำนวยความสะดวกด้านการบริหารจัดการให้แก่รัฐบาล อีกทั้งยังช่วยพัฒนาคุณภาพประชาชนด้วยการทำให้ประชาชนสามารถเข้าถึงข้อมูลและบริการสาธารณะของรัฐได้มากขึ้น

อย่างไรก็ตาม เทคโนโลยีเครือข่ายอินเตอร์เน็ตกลับเป็นช่องทางใหม่ที่อาชญากรสามารถนำไปใช้กระทำความผิดในรูปแบบต่างๆได้เช่นกัน อาชญากรรมชนิดใหม่ที่เกิดจากเทคโนโลยีเครือข่ายอินเตอร์เน็ตนั้นเรียกว่า อาชญากรรมทางคอมพิวเตอร์ (computer

crime หรือ cyber crime) โดยลักษณะพิเศษของเทคโนโลยีทางคอมพิวเตอร์และเครือข่ายทางอินเตอร์เน็ตจะส่งผลให้อาชญากรรมประเภทนี้ สร้างความเสียหายได้อย่างรวดเร็ว รุนแรง และกว้างขวางกว่าอาชญากรรมทั่วไป อีกทั้งยังยากลำบากแก่การติดตามจับกุมและดำเนินคดีต่อผู้กระทำผิด ดังนั้น การป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์จึงต้องอาศัยทั้งมาตรการทางเทคโนโลยีและมาตรการทางกฎหมายควบคู่กันไปด้วย

เมื่อพิจารณาด้านการบังคับใช้กฎหมายแล้ว จะพบว่า เครือข่ายทางอินเตอร์เน็ตนั้นปราศจากรูปร่างทางกายภาพ ไม่สามารถที่จะจับต้องได้ และไม่อยู่ภายใต้ข้อจำกัดทางด้านเขตแดนรัฐ ผู้กระทำความผิดจึงสามารถก่ออาชญากรรมทางคอมพิวเตอร์ในลักษณะข้ามแดนได้ อย่างไรก็ตาม กฎหมายภายในประเทศกลับมีขอบเขตการบังคับใช้จำกัดอยู่ภายในเขตแดนของรัฐเท่านั้น ทำให้กฎหมายระหว่างประเทศเกี่ยวกับความร่วมมือทางอาญาระหว่างประเทศจึงมีบทบาทสำคัญต่อการติดตามจับกุมอาชญากรทางคอมพิวเตอร์มาดำเนินคดี แม้กระนั้นก็ตาม ความร่วมมือทางอาญาระหว่างประเทศทั่วไป ซึ่งประกอบไปด้วยการส่งตัวผู้ร้ายข้ามแดนและการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายนั้น กลับไม่สามารถรองรับอาชญากรรมทางคอมพิวเตอร์ได้เท่าที่ควร

ด้วยเหตุนี้ ผู้วิจัยจึงเห็นความจำเป็นในการศึกษาวิเคราะห์ถึงความร่วมมือภายใต้กรอบอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของสภายุโรปหรืออนุสัญญากรุงบูดาเปสต์* เพื่อให้ทราบว่ากรอบความร่วมมือดังกล่าวสามารถตอบสนองต่ออาชญากรรมทางคอมพิวเตอร์ได้เพียงใด ทั้งนี้ อนุสัญญากรุงบูดาเปสต์ นับเป็นสนธิสัญญาระหว่างประเทศฉบับแรกด้านความร่วมมือทางอาญาสำหรับอาชญากรรมทางคอมพิวเตอร์โดยตรง ทั้งยังมีรัฐที่มาจากทั้งในและนอกภูมิภาคยุโรปเข้าร่วมเป็นภาคีด้วย อนึ่ง ความร่วมมือภายใต้กรอบอนุสัญญากรุงบูดาเปสต์นี้ยังครอบคลุมไปถึงพิธีสารเพิ่มเติมว่าด้วยการกระทำผ่านระบบคอมพิวเตอร์ที่มีลักษณะเหยียดหยามหรือเกลียดชังเชื้อชาติด้วย

ผลลัพธ์ที่ได้จากการศึกษาวิจัย ไม่เพียงจะแต่สามารถให้แนวทางสำหรับการพัฒนากฎหมายระหว่างประเทศที่เกี่ยวข้องต่อไปในอนาคตได้เท่านั้น หากแต่ยังเป็นประโยชน์

---

* เพื่อความสะดวกในการกล่าวถึง เนื้อหาส่วนต่อไปของวิทยานิพนธ์ฉบับนี้จะเรียกชื่ออนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของสภายุโรปว่า อนุสัญญากรุงบูดาเปสต์

ต่อประเทศไทยในอนาคต ทั้งนี้ ในปัจจุบัน ประเทศไทยนับเป็นประเทศหนึ่งที่มีความตื่นตัวและมีประสบการณ์ด้านอาชญากรรมทางคอมพิวเตอร์ ดังที่จะเห็นได้จากการจัดทำพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งได้กำหนดฐานความผิดสำหรับอาชญากรรมทางคอมพิวเตอร์ไว้ ดังนั้น ความรู้ที่ได้รับเกี่ยวกับความร่วมมือทางอาญาในกรอบอนุสัญญากรุงบูดาเปสต์ ย่อมแสดงให้ประเทศไทยทราบถึงประโยชน์ที่ตนจะได้รับจากการเข้าเป็นภาคีอนุสัญญาดังกล่าว อีกทั้งยังสามารถเรียนรู้แนวทางการปรับใช้อนุสัญญาดังกล่าวได้ด้วย

1.2 **สมมติฐานของการวิจัย**

อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของสภายุโรป มีบทบาทด้านการกำหนดมาตรฐานร่วมกันสำหรับกฎหมายภายในประเทศเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ อีกทั้งยังขยายขอบเขตความร่วมมือระหว่างประเทศให้ครอบคลุมอาชญากรรมทางคอมพิวเตอร์ด้วย อย่างไรก็ตาม อนุสัญญาฉบับนี้ยังจำเป็นต้องเพิ่มเติมรายละเอียดของกลไกความร่วมมือเพื่อให้สามารถรองรับความซับซ้อนของอาชญากรรมทางคอมพิวเตอร์ที่ทวีขึ้นไปตามกาลเวลาได้

1.3 **วัตถุประสงค์ของการวิจัย**

1. เพื่อให้ทราบถึงลักษณะพิเศษของอาชญากรรมทางคอมพิวเตอร์ ซึ่งก่อให้เกิดความจำเป็นในการใช้ความร่วมมือระหว่างทางอาญาประเทศเพื่อติดตามจับกุมผู้กระทำผิด
2. เพื่อศึกษาถึงเนื้อหาของความร่วมมือทางอาญาระหว่างประเทศภายใต้กรอบของอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของสภายุโรปหรืออนุสัญญากรุงบูดาเปสต์ และพิจารณาถึงบทบาทในการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ของกรอบความร่วมมือดังกล่าว
3. เพื่อวิเคราะห์หาความสำเร็จและข้อท้าทายจากการปรับใช้ความร่วมมือทางอาญาระหว่างประเทศภายใต้กรอบอนุสัญญากรุงบูดาเปสต์ ซึ่งจะเป็นแนวทางในการปรับปรุงและพัฒนากลไกความร่วมมือทางอาญาระหว่างประเทศสำหรับอาชญากรรมทางคอมพิวเตอร์ในอนาคต

4. เพื่อให้ประเทศไทยทราบถึงผลประโยชน์ที่ได้จากการเข้าเป็นภาคีอนุสัญญากรุงบูดาเปสต์และพิธีสารเพิ่มเติม อีกทั้งสามารถเรียนรู้แนวทางการปรับใช้ความร่วมมือภายใต้กรอบอนุสัญญาดังกล่าว

1.4 ขอบเขตของการวิจัย

เนื้อหาของวิทยานิพนธ์บทนี้ถูกแบ่งออกเป็นสี่ส่วน ส่วนที่หนึ่งจะอธิบายให้ผู้อ่านทราบถึงข้อมูลเบื้องต้นเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ การให้ความร่วมมือทางอาญาระหว่างประเทศโดยทั่วไป และความพยายามในการพัฒนาความร่วมมือทางอาญาสำหรับอาชญากรรมทางคอมพิวเตอร์ในช่วงก่อนหน้าการจัดทำอนุสัญญากรุงบูดาเปสต์และพิธีสารเพิ่มเติม หลังจากนั้น ส่วนที่สองของวิทยานิพนธ์จะอธิบายถึงความร่วมมือทางอาญาระหว่างประเทศ ภายใต้กรอบของอนุสัญญากรุงบูดาเปสต์และพิธีสารเพิ่มเติม และบทบาทของกรอบความร่วมมือดังกล่าวในการพัฒนาความร่วมมือทางอาญาระหว่างประเทศสำหรับอาชญากรรมทางคอมพิวเตอร์ ส่วนที่สามของวิทยานิพนธ์จะประเมินผลลัพธ์ของความร่วมมือทางอาญาระหว่างประเทศภายใต้กรอบอนุสัญญากรุงบูดาเปสต์ว่าสามารถตอบสนองต่ออาชญากรรมทางคอมพิวเตอร์ได้อย่างไร และมีข้อท้าทายใดบ้าง โดยจะพิจารณาจากการปรับใช้และความสอดคล้องต่อบริบททางข้อเท็จจริงและเทคโนโลยี ส่วนสุดท้ายของวิทยานิพนธ์จะเป็นบทสรุปและข้อเสนอแนะ

1.5 วิธีดำเนินการวิจัย

เป็นการวิจัยเชิงเอกสาร (Documentary research) โดยการศึกษาข้อมูลจากเอกสารที่เกี่ยวข้องได้แก่ หนังสือ ตำราทางวิชาการ ตัวบทกฎหมาย อนุสัญญา คดีตัวอย่างต่างๆ ตลอดจนข้อมูลทางอินเตอร์เน็ตที่เกี่ยวข้อง ทั้งภาษาไทยและภาษาต่างประเทศ เพื่อนำมาศึกษาและวิเคราะห์ถึงสภาพปัญหาและแนวทางการแก้ไขปัญหาที่ถูกต้องเหมาะสม

1.6 ประโยชน์ที่ได้รับจากการวิจัย

1. ทำให้ทราบและเข้าใจถึงลักษณะของอาชญากรรมทางคอมพิวเตอร์
2. ทำให้ทราบถึงเข้าใจกฎหมายระหว่างประเทศเกี่ยวกับความร่วมมือทางอาญาสำหรับอาชญากรรมทางคอมพิวเตอร์
3. ทำให้ทราบถึงและเข้าใจถึงเนื้อหา ความสำเร็จ และอุปสรรคจากการให้ความร่วมมือทางอาญาระหว่างประเทศภายใต้กรอบอนุสัญญากรุงบูดาเปสต์และพิธีสารเพิ่มเติม
4. ทำให้สามารถเสนอแนะถึงการปรับปรุงแก้ไขความร่วมมือทางระหว่างประเทศภายใต้กรอบอนุสัญญากรุงบูดาเปสต์ต่อไปในอนาคต
5. ทำให้ทราบถึงประโยชน์ด้านความร่วมมือระหว่างประเทศที่ประเทศไทยจะได้จากการเข้าร่วมเป็นภาคีของอนุสัญญากรุงบูดาเปสต์ อีกทั้งสามารถเรียนรู้แนวทางการปฏิบัติตามและปรับใช้กรอบความร่วมมือดังกล่าว

บทที่ 2
วิวัฒนาการความร่วมมือทางอาญาระหว่างประเทศสำหรับอาชญากรรมทางคอมพิวเตอร์

เนื้อหาของบทนี้แบ่งออกเป็นสี่ส่วน โดยส่วนที่หนึ่งนั้น จะอธิบายถึงข้อมูลเชิงข้อเท็จจริงเบื้องต้นเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ ทั้งนี้ เพื่อแสดงให้เห็นถึงความสามารถของอาชญากรรมทางคอมพิวเตอร์ที่ทวีความซับซ้อนขึ้นได้ไปตามกาลเวลาได้ โดยความซับซ้อนดังที่กล่าวมานี้ ได้ส่งผลกระทบเชิงกฎหมายให้ความร่วมมือทางอาญาระหว่างประเทศมีความจำเป็นสำหรับการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ด้วย

เนื้อหาส่วนที่สองของบทจะอธิบายกฎหมายว่าด้วยความร่วมมือทางอาญาระหว่างประเทศทั่วไป พร้อมทั้งปัญหาในการปรับใช้ในบริบทของอาชญากรรมทางคอมพิวเตอร์ หลังจากนั้น เนื้อหาส่วนที่สาม จะอธิบายถึงกรอบความร่วมมือทางอาญาระหว่างประเทศสำหรับอาชญากรรมทางคอมพิวเตอร์ในช่วงก่อนหน้าการจัดทำอนุสัญญากรุงบูดาเปสต์ พร้อมทั้งอุปสรรคที่ยังคงมีอยู่จากการปรับใช้ให้เข้ากับบริบทอาชญากรรมทางคอมพิวเตอร์

ท้ายที่สุด เนื้อหาส่วนที่สี่ของบท จะเป็นการนำข้อมูลที่ได้จากส่วนที่สองและสามของบทมาสรุปว่ากลไกความร่วมมือทางอาญาระหว่างประเทศสำหรับอาชญากรรมทางคอมพิวเตอร์นั้น ควรมีลักษณะประการใดบ้าง ความจำเป็นเหล่านี้ จะนำไปสู่การจัดทำอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของสภายุโรป หรืออนุสัญญากรุงบูดาเปสต์ ในปี 2001 เป็นลำดับถัดไป

2.1 ความเบื้องต้นเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์

2.1.1 นิยามของอาชญากรรมทางคอมพิวเตอร์

โดยทั่วไป อาชญากรรมคอมพิวเตอร์หมายถึงอาชญากรรมที่มีความสัมพันธ์กับเทคโนโลยีทางคอมพิวเตอร์สามรูปแบบ ซึ่งอาจเรียกได้ว่าเป็น อาชญากรรมต่อคอมพิวเตอร์ (Computer Crimes) อาชญากรรมที่อาศัยคอมพิวเตอร์ (Computer Facilitated Crimes)

และ อาชญากรรมที่ใช้เทคโนโลยีทางคอมพิวเตอร์สนับสนุน (Computer Supported Crimes)[1] ตามลำดับ

อาชญากรรมต่อคอมพิวเตอร์นั้น เป็นกรณีที่คอมพิวเตอร์หรือเครือข่ายทางคอมพิวเตอร์ตกเป็นเป้าหมายของการกระทำผิดโดยตรง[2] โดยอาชญากรอาศัยเทคโนโลยีทางคอมพิวเตอร์เพื่อให้ความผิดกระทำสำเร็จ หากอาชญากรใช้กำลังทางกายภาพอย่างเดียวเช่น การใช้กำลังทุบทำลายเครื่องคอมพิวเตอร์ หรือลักขโมยตัวเครื่องคอมพิวเตอร์ การกระทำที่เกิดจะเป็นเพียงความผิดทางอาญาโดยทั่วไปเท่านั้น[3] ตัวอย่างของอาชญากรรมต่อคอมพิวเตอร์ได้แก่ การเข้าถึงระบบคอมพิวเตอร์โดยผิดกฎหมาย การใช้โปรแกรมคอมพิวเตอร์ที่เป็นอันตราย (Malware) หรือการโจมตีให้ระบบคอมพิวเตอร์ปฏิเสธการให้บริการ (Denial of Service) เป็นต้น

อาชญากรรมที่อาศัยคอมพิวเตอร์ จะเป็นกรณีที่ผู้กระทำผิดจะใช้เทคโนโลยีทางคอมพิวเตอร์เพื่อกระทำความผิดอาญาทั่วไปบางประเภท[4] อาทิ การเผยแพร่สิ่งลามกอนาจารเด็ก การฉ้อโกง เป็นต้น การที่เทคโนโลยีทางคอมพิวเตอร์มีลักษณะพิเศษในการปฏิบัติการอย่างอัตโนมัติ และการย้อนทวนทำซ้ำกระบวนการต่างๆได้เองนั้น ส่งผลให้ความเสียหายที่เกิดกว้างขวางและรุนแรงกว่าอาชญากรรมทั่วไป

สำหรับอาชญากรรมที่สนับสนุนโดยคอมพิวเตอร์นั้น ผู้กระทำความผิดจะใช้เทคโนโลยีคอมพิวเตอร์ประกอบอาชญากรรมในลักษณะที่ไม่เกี่ยวข้องกับการทำให้ความผิดสำเร็จ ส่งผลให้

---

[1] Melanie Kowalki, “Cyber-crime*:* issues, data sources, and feasibility of collecting police-reported statistics”. (Ottawa: *Statistics* Canada, 2002), p.6 Cited in: Jonathan Clough, Principles of Cybercrime (UK: Cambridge University Press, 2010), p.10

[2]Richard W. Downing, “Shoring up the weakest link: What lawmakers around the world need to consider in developing comprehensive laws to combat cybercrime,” Columbia Journal of Transnational Law 43,705 (2005): 713.

[3]Jonathan Clough, Principles of Cybercrime, p.27

[4]Richard W. Downing, “Shoring up the weakest link: What lawmakers around the world need to consider in developing comprehensive laws to combat cybercrime,” Columbia Journal of Transnational Law 43,705: 711-712.

ข้อมูลทางคอมพิวเตอร์มีฐานะเป็นหลักฐานในการก่ออาชญากรรม[5] ตัวอย่างของหลักฐานดังกล่าว ได้แก่ ข้อมูลที่ตรวจพบในเครื่องคอมพิวเตอร์ของผู้ต้องสงสัยคดีฆาตกรรม เป็นต้น การที่ข้อมูลทางคอมพิวเตอร์เหล่านี้ขาดลักษณะทางกายภาพ จึงถูกทำลาย หลบซ่อน ดัดแปลง หรือลบทิ้ง ได้ง่ายกว่าหลักฐานวัตถุทั่วไป

แนวคิดเกี่ยวกับคำจำกัดความของอาชญากรรมทางคอมพิวเตอร์ดังข้างต้นนี้ ถูกสรุปขึ้นโดยกระทรวงยุติธรรมของประเทศสหรัฐอเมริกา[6] และมีการปรับใช้ในประเทศอื่นๆ อาทิ ออสเตรเลีย[7] แคนาดา[8] อังกฤษ[9] รวมไปถึงในระดับระหว่างประเทศ[10]ด้วย จากคำจำกัดความนี้จะสังเกตเห็นได้ว่า อาชญากรรมทางคอมพิวเตอร์จะครอบคลุมทั้งอาชญากรรมประเภทเก่าซึ่งอาศัยเทคโนโลยีทางคอมพิวเตอร์อันเป็นเครื่องมือชนิดใหม่ และอาชญากรรมชนิดใหม่ที่ยากแก่การนำมาเปรียบเทียบกับกฎหมายอาญาทั่วไป

2.1.2 ประเภทอาชญากรรมทางคอมพิวเตอร์

การกระทำที่จัดเป็นอาชญากรรมต่อคอมพิวเตอร์ อาชญากรรมที่อาศัยคอมพิวเตอร์ และอาชญากรรมที่สนับสนุนโดยคอมพิวเตอร์นั้น มีหลายประเภท อย่างไรก็ตาม เพื่อความสะดวก

---

[5] *Ibid*.,p.712-713

[6] Computer Crime and Intellectual Property Section, US Department of Justice, “The National Information Infrastructure Protection Act of 1996: Legislative analysis” (US Department of Justice, 2003), Cited in Jonathan Clough, Principles of Cybercrime p.10

[7] G. Urbas and K.R. Choo, “Resource material on technology-enabled crime”, technical and background paper no.28 (AIC, 2008), p.5 Cited in: Jonathan Clough, Principles of Cybercrime, p.10 fn.36

[8] Melanie Kowalki, “Cyber-crime: issues, data sources, and feasibility of collecting police-reported statistics”, p.6

[9] National Criminal Intelligence Service, Project Trawler: Crime on the information high-ways [Online]. 1999. Available from: www.cyber-rights.org/documents/trawler.htm [2013, May 7], Cited in Jonathan Clough, Principles of Cybercrime p.10

[10] A. Rathmell et al., Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries, Study for the European Commission Directorate-General Information Society (2002), p.16 Cited in: Jonathan Clough, Principles of Cybercrime, p.10

ในการศึกษา ผู้วิจัยจะจำแนกประเภทอาชญากรรมทางคอมพิวเตอร์ออกเป็นสี่ประเภท ตามแนวทางของอนุสัญญากรุงบูดาเปสต์* ดังนี้

- การกระทำผิดต่อความลับ ความสมบูรณ์ และความพร้อมใช้งานของข้อมูลและระบบคอมพิวเตอร์ (Offences against Confidentiality Integrity and Availability of Computer Data and Systems หรือ C.I.A. offences)
- การกระทำผิดที่เกี่ยวข้องกับคอมพิวเตอร์ (Computer-related offences)
- การกระทำความผิดที่เกี่ยวข้องกับเนื้อหา (Content-related offences)
- การกระทำผิดต่อทรัพย์สินทางปัญญา

2.1.2.1 การกระทำผิดต่อความลับ ความสมบูรณ์ และความพร้อมใช้งานของข้อมูลและระบบคอมพิวเตอร์

ภายใต้การกระทำความผิดประเภทนี้ ระบบและข้อมูลทางคอมพิวเตอร์ตกเป็นเป้าหมายของผู้กระทำผิดโดยตรง โดยการกระทำจะมุ่งเน้นไปยังความลับ ความสมบูรณ์ และ ความพร้อมในการใช้งาน ทั้งสามประการนี้นับเป็นหัวใจสำคัญของการรักษาความปลอดภัยให้ระบบและข้อมูลทางคอมพิวเตอร์[11]

ทั้งนี้ ภายใต้หลักการรักษาความลับ ข้อมูลและระบบทางคอมพิวเตอร์จะต้องรักษาความลับให้ได้ตามความประสงค์ของเจ้าของข้อมูล และจะถูกเปิดเผยได้เฉพาะกับบุคคลที่ได้รับอนุญาตเท่านั้น[12] ในขณะเดียวกัน ภายใต้หลักการรักษาความสมบูรณ์ ข้อมูลและแหล่งข้อมูลทางคอมพิวเตอร์จะต้องคงความน่าเชื่อถือ ความถูกต้องแม่นยำ อีกทั้งคงสภาพ

---

* อนุสัญญากรุงบูดาเปสต์บทที่ 2 Section 1 ซึ่งมีเนื้อหาเกี่ยวกับกฎหมายสารบัญญัติทางอาญานั้น ได้แบ่งประเภทฐานความผิดออกเป็นสี่ประเภทเช่นกัน ได้แก่ ความผิดต่อความลับ ความสมบูรณ์และความพร้อมใช้งานของข้อมูลและระบบคอมพิวเตอร์ (Offencces against the confidentiality, integrity and availability of computer data and systems) ความผิดที่เกี่ยวข้องกับคอมพิวเตอร์ (Computer-related offences) ความผิดที่เกี่ยวข้องกับเนื้อหา (Content-related offences) และความผิดที่เกี่ยวข้องกับการละเมิดลิขสิทธิ์และสิทธิที่เกี่ยวข้อง (Offences related to infringements of copyrights and related rights)

[11] John Chirillo and Edgar Danielyan, Sun certified security administrator for Solaris 9&10 study guide (Emeryville: McGraw-Hill, 2005), p.4

[12] *Ibid*.,p.5

สมบูรณ์ ปราศจากการถูกทำลายหรือดัดแปลงโดยไม่ได้รับอนุญาตด้วย[13] ท้ายที่สุด สำหรับหลักการความพร้อมใช้งานนั้น ผู้ใช้งานระบบคอมพิวเตอร์จะต้องสามารถเข้าถึงและใช้งานระบบคอมพิวเตอร์ได้ภายใต้กรอบเวลาที่เหมาะสมโดยปราศจากการรบกวนทำลาย[14]

ตัวอย่างการกระทำความผิดต่อความลับนั้นมีดังต่อไปนี้

- **การเข้าถึงระบบคอมพิวเตอร์โดยผิดกฎหมาย** (illegal access)* การเข้าถึงระบบโดยผิดกฎหมาย จะเป็นกรณีที่ผู้กระทำความผิดจะเข้าถึงระบบทางคอมพิวเตอร์โดยปราศจากสิทธิตามกฎหมาย เทคโนโลยีที่ใช้เข้าถึงระบบคอมพิวเตอร์โดยผิดกฎหมายมีอยู่หลายระดับ ตั้งแต่การใช้เทคโนโลยีที่ซับซ้อนสำหรับหลบเลี่ยงมาตรการรักษาความปลอดภัยโดยเฉพาะ ไปจนถึงวิธีการที่ไม่ใช้เทคโนโลยีเลย เช่นการล่อลวงให้ผู้ใช้งานคอมพิวเตอร์มอบรหัสผ่านให้ผู้กระทำผิดโดยตรง หรือการเข้าถึงข้อมูลโดยเกินขอบเขตจากที่ได้รับอนุญาตตามตำแหน่งหน้าที่ เป็นต้น การเข้าถึงระบบคอมพิวเตอร์โดยผิดกฎหมายยังสามารถนำไปสู่การกระทำความผิดต่อความลับ ความสมบูรณ์ และความพร้อมใช้งานของข้อมูลและระบบคอมพิวเตอร์ในรูปแบบอื่นๆ ต่อไป ยกตัวอย่างเช่น เหตุการณ์เจาะระบบ web site ของหน่วยงานรัฐบาลและสถาบันอื่นๆ อาทิ กระทรวงกลาโหม ศาลฎีกาและสถาบันเทคโนโลยีแห่งโตเกียวของญี่ปุ่นเมื่อวันที่ 19 กันยายน 2012 เนื่องด้วยเหตุการณ์ความขัดแย้งเรื่องดินแดนระหว่างจีนและญี่ปุ่น หลังจากที่เจาะระบบได้ฝ่ายผู้กระทำผิดได้ทำให้ web site ดังกล่าวไม่สามารถ

---

[13] Standards for security categorization of federal information and information systems [Online]. Gaithersburg: National insitute of standard and technology, Information technology laboratory, Computer secirity division, 2004. Available from: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf [2013, May 7], p.2

[14] *Ibid*.

* อนุสัญญากรุงบูดาเปสต์ได้กำหนดความผิดฐานนี้ไว้ในข้อ 2 ของอนุสัญญา

เข้าถึงได้ และ web site สถาบันเทคโนโลยีแห่งโตเกียวได้มีการแทนที่เนื้อหาด้วยรูปธงชาติของประเทศจีน อีกทั้งมีการขโมยข้อมูลส่วนตัวของบุคคลจำนวนกว่า 1000 คนด้วย[15]

- **การจารกรรมข้อมูลทางคอมพิวเตอร์** (data espionage) การจารกรรมข้อมูลทางคอมพิวเตอร์ เป็นความผิดต่อความลับที่เกิดหลังจากการเข้าถึงระบบโดยผิดกฎหมาย โดยผู้กระทำความผิดจะนำข้อมูลที่ได้จากการเข้าถึงระบบคอมพิวเตอร์โดยผิดกฎหมายไปแสวงประโยชน์โดยมิชอบหรือนำไปขายต่อบุคคลที่สาม[16] ข้อมูลทางคอมพิวเตอร์ที่ถูกจารกรรมครอบคลุมข้อมูลหลายรูปแบบ อาทิ ความลับทางการค้า ข้อมูลลับทางราชการ ข้อมูลเกี่ยวกับทรัพย์สินทางปัญญา รวมไปถึงข้อมูลส่วนตัวต่างๆ เช่นประวัติทางการแพทย์ หมายเลขบัตรเครดิต หรือหมายเลขประกันสังคม เป็นต้น ตัวอย่างคดีการจารกรรมข้อมูลได้แก่ คดี US v. Levine[17] ซึ่งฝ่ายจำเลยใช้ซอฟต์แวร์ถอดรหัสเพื่อเข้าถึงฐานข้อมูลบริษัทที่รับจัดเก็บข้อมูลลูกค้าสำหรับบริษัทต่างๆ จากนั้นจึงดาวน์โหลดข้อมูลส่วนบุคคลของลูกค้าของบริษัทผู้เสียหายเป็นจำนวนมากกว่าหนึ่งพันล้านราย

- **การดักรับข้อมูล** (Data interception)* การดักรับข้อมูล เป็นการกระทำความผิดต่อความลับที่แตกต่างไปจากการเข้าถึงโดยผิดกฎหมายและการจารกรรมข้อมูล เพราะเป็นข้อมูลที่ตกเป็นเป้าหมายไม่ได้ถูกจัดเก็บอยู่ในระบบคอมพิวเตอร์ หากแต่อยู่ระหว่าง

---

[15] "Chinese cyber attacks hit Japan over islands dispute," The globe and mail (19 September 2012) Available from: http://www.theglobeandmail.com/news/world/chinese-cyber-attacks-hit-japan-over-islands-dispute/article4553048/ [2013, May 7]

[16] Marco Gercke. Understanding cybercrime: A guide for developing countries [Online]. Geneva: International Telecommunication Union (ITU), ICT applications and cybersecurity division, 2009. Available from: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf

[2013, May 6] p.23-25

[17] US v Levine (ED Ark 2006) US Department of Justice, Press Release, 22 February 2006. Cited Jonathan Clough, Principles of Cybercrime, p.29

* อนุสัญญากรุงบูดาเปสต์ได้กำหนดความผิดฐานนี้ไว้ในข้อ 3 ของอนุสัญญา

การเดินทางจากระบบคอมพิวเตอร์หนึ่งไปยังอีกระบบหนึ่ง โดยฝ่ายผู้กระทำผิดจะพยายามหาช่องโหว่ในเส้นทางสื่อสารเพื่อดักรับข้อมูลในลักษณะคล้ายคลึงกับการดักฟังโทรศัพท์[18] การดักรับข้อมูลทางคอมพิวเตอร์สามารถกระทำโดยการติดตั้งอุปกรณ์พิเศษไปบนสายส่งสัญญาณสำหรับการสื่อสารแบบมีสาย ส่วนการดักรับข้อมูลคอมพิวเตอร์ในการสื่อสารแบบไร้สายสามารถกระทำโดยการเข้าไปในรัศมีทำการของระบบการสื่อสารและใช้อุปกรณ์สำหรับรวบรวมและบันทึกข้อมูลด้วยการตรวจจับคลื่นแม่เหล็กไฟฟ้าที่แผ่ออกจากระบบคอมพิวเตอร์[19]และนำไปประกอบเป็นข้อมูลใหม่ในภายหลัง[20]

การกระทำความผิดต่อความสมบูรณ์นั้นเรียกว่า การแทรกแซงข้อมูล (data interference))* ซึ่งครอบคลุมการกระทำหลายประการ ได้แก่ การลบข้อมูลสำคัญ การเปลี่ยนข้อมูลให้ผิดไปจากความเป็นจริงหรือตกอยู่ในสภาพที่ไม่สามารถเข้าถึงหรือใช้งานได้ ตัวอย่างหนึ่งของการดัดแปลงข้อมูลในลักษณะนี้ได้แก่ การดัดแปลงข้อมูลบน web site สำหรับจัดหาคู่ทางอินเตอร์เน็ต ให้พาผู้ใช้บริการไปยัง web site ลามกอนาจารแทน[21]

เครื่องมือที่ผู้กระทำผิดนิยมใช้ในการแทรกแซงข้อมูลทางคอมพิวเตอร์คือซอฟต์แวร์ที่เป็นอันตราย (Malicious Software หรือ Malware) การเผยแพร่ Malware สามารถกระทำได้โดยตรงเช่นการเปิดใช้งานแผ่นดิสค์ที่มี Malware บนเครื่องคอมพิวเตอร์ที่เป็นเป้าหมาย หรือด้วยการเผยแพร่ผ่านอินเตอร์เน็ตหรือเครือข่ายคอมพิวเตอร์ในรูปแบบของไฟล์ที่สามารถสั่งให้ทำหน้าที่ต่างๆได้ (Executable files) ประเภทของ Malware ที่สำคัญได้แก่ ไวรัสและหนอนคอมพิวเตอร์ ม้าโทรจัน บอทส์ และสปายแวร์

---

[18] Jonathan Clough, Principles of Cybercrime,p.135

[19] Scottish Law Commission, Report on Computer Crime, no.106 (1987), para. 2.10 . Cited Jonathan Clough, Principles of Cybercrime, p.137

[20] Council of Europe. Convention on cybercrime explanatory report[Online]. Available from: http://conventions.coe.int/Treaty/en/Reports/Html/185.htm [2013, May 6], Para.57

* อนุสัญญากรุงบูดาเปสต์ได้กำหนดความผิดฐานนี้ไว้ในข้อ 4 ของอนุสัญญา อย่างไรก็ตาม บทบัญญัติดังกล่าวจะไม่อ้างถึงเทคโนโลยีประเภทใดประเภทหนึ่งเป็นการเฉพาะ

[21] *YourNetDating LLC v. Mitchell*, 88 F Supp 2d 870 (ND III 2000). Cited in Jonathan Clough, Principles of Cybercrime, p.29

ไวรัสคอมพิวเตอร์และหนอนคอมพิวเตอร์เป็นโปรแกรมที่สามารถเข้าไปแพร่เชื้อในเครื่องคอมพิวเตอร์ที่ตกเป็นเป้าหมายโดยจะคัดลอกตัวเองและปฏิบัติหน้าที่ต่างๆ ตามที่ถูกกำหนดไว้ อาทิ การลบหรือดัดแปลงข้อมูล หรือดำเนินการติดตั้ง Malware ประเภทอื่น อย่างเช่น โทรจัน หรือบอทส์ เป็นต้น อย่างไรก็ตาม ข้อแตกต่างสำคัญระหว่างไวรัสและหนอนคอมพิวเตอร์คือ ไวรัสคอมพิวเตอร์จะต้องแพร่เชื้อในโปรแกรมคอมพิวเตอร์อื่นก่อนจึงจะทำงานได้ ในขณะที่หนอนคอมพิวเตอร์จะคัดลอกตัวเองเพื่อเพิ่มปริมาณได้[22] ตัวอย่างของการใช้งานไวรัสคอมพิวเตอร์ ได้แก่ ไวรัส Melissa ในปี 1999 ซึ่งในช่วงแรกเริ่มนั้นจะถูกติดไว้ในกลุ่มข่าวทางอินเตอร์เน็ต โดยมีการหลอกลวงผู้เข้าเยี่ยมชมกลุ่มข่าวดังกล่าวให้ดาวน์โหลดโปรแกรมที่ติดเชื้อไวรัสโดยอ้างว่าเป็นโปรแกรมเก็บรหัสผ่านสำหรับเข้าถึง web site ลามกอนาจาร หลังจากที่ได้มีการปิดใช้ไฟล์ดังกล่าว ไวรัสจะเข้าไปดัดแปลงโปรแกรม Microsoft Word ให้ file เอกสารที่ถูกสร้างโดย Microsoft Word ติดเชื้อไวรัสไปด้วย นอกจากนี้ ไวรัส Melissa ยังได้ดัดแปลงโปรแกรม Microsoft Outlook ให้ส่งจดหมายอิเล็กทรอนิกส์ที่ติดไวรัสทางคอมพิวเตอร์ไปยังผู้ใช้ 50 รายแรกตามบันทึกที่อยู่จดหมายทางอิเล็กทรอนิกส์ของผู้เสียหาย[23]

ม้าโทรจันเป็นโปรแกรมคอมพิวเตอร์ที่ดูเหมือนไม่มีอันตราย หากแต่มีหน้าที่ลับซ่อนไว้ อาทิ รวบรวมข้อมูลคอมพิวเตอร์ที่ผู้ใช้ส่งออกไปนอกระบบหรือรหัสต่างๆเพื่อส่งไปให้ผู้กระทำความผิด การดัดแปลงไม่ให้โปรแกรมป้องกันไวรัสสามารถพัฒนาตัวเองต่อไปได้ในอนาคต นอกจากนี้ ม้าโทรจันบางประเภทยังสามารถติดตั้งประตูลับ (trapdoor) ซึ่งเป็นช่องทางสำหรับให้ผู้กระทำความผิดสามารถเข้าไปใช้งานเครื่องคอมพิวเตอร์ที่เป็นเป้าหมายได้จากระยะไกล[24]

บอทส์เป็นโปรแกรมคอมพิวเตอร์อีกชนิดหนึ่งที่ทำให้คอมพิวเตอร์เป้าหมายติดเชื้อและถูกควบคุมได้จากระยะไกล โดยบรรดาคอมพิวเตอร์ที่ถูกควบคุมโดยบอทส์ จะถูกเรียกว่า bots

---

[22] Jonathan Clough, Principles of Cybercrime, p.33

[23] US v. Smith (D NK 2002) US Department of Justice, Press Release, 2 May 2002, www.cybercrime.gov/melissaSent.htm Cited in: Jonathan Clough, Principles of Cybercrime, p.33

[24] E.J. Sinrod and W.P. Reilly, "Cyber-crimes: A practical approach to the application of federal computer crime laws," Santa Clara Computer and High Tech Law Journal 16,177 (2000): 194-7 Cited in: Jonathan Clough, Principles of Cybercrime, p.34

หรือ zombies ซึ่งผู้กระทำผิดสามารถสั่งการให้คอมพิวเตอร์เหล่านี้ประสานงานกันทำหน้าที่บางอย่าง เช่น การโจมตีให้ระบบคอมพิวเตอร์ปฏิเสธการให้บริการ หรือการส่งจดหมายอิเล็กทรอนิกส์ที่ไม่พึงปรารถนา เป็นต้น[25]

สำหรับสปายแวร์นั้น จะเป็นโปรแกรมคอมพิวเตอร์ที่ใช้ลอบเฝ้าดูการใช้งานเครื่องคอมพิวเตอร์ที่ตกเป็นเป้าหมายได้ โปรแกรมสปายแวร์มีหลายประเภทอาทิ sniffer ซึ่งจะดักรับข้อมูลการกรอกรหัสผ่านของผู้ใช้งาน key loggers ซึ่งทำหน้าที่ลอบบันทึกการพิมพ์ข้อความต่างๆของผู้ใช้งาน หรือ cookies ซึ่งบันทึกการใช้งานอินเตอร์เน็ตของผู้ใช้งาน เป็นต้น[26] ตัวอย่างคดีการใช้ Spyware ได้แก่ คดี US v. Perez ซึ่งผู้กระทำผิดได้สร้างและวางจำหน่ายสปายแวร์ที่ใช้ชื่อว่า Loverspy โดยผู้ใช้งานจะสามารถเลือกส่งการ์ดอวยพรอิเล็กทรอนิกส์ไปยังที่อยู่จดหมายอิเล็กทรอนิกส์ที่กำหนดได้ เมื่อผู้รับจดหมายเปิดการ์ดอวยพร Loverspy จะถูกลอบติดตั้งลงไปบนคอมพิวเตอร์เครื่องนั้น ตัว Loverspy นั้นสามารถเฝ้าดูกิจกรรมทั้งหมดบนเครื่องได้ไม่ว่าเป็น การรับส่ง email รายชื่อ web site ที่เข้าชม และรหัสผ่านต่างๆ ซึ่งข้อมูลเหล่านี้จะถูกส่งไปยังผู้ซื้อสปายแวร์ต่อไป ในขณะเดียวกันผู้ที่ซื้อสปายแวร์นั้นยังสามารถควบคุมเครื่องคอมพิวเตอร์ของผู้เสียหายได้จากระยะไกลอีกด้วย[27]

การกระทำความผิดต่อความพร้อมใช้งานนั้น อาจเรียกได้ในอีกชื่อหนึ่งว่าการแทรกแซงระบบ (System interference)* ซึ่งผู้กระทำความผิดจะใช้วิธีการเพื่อให้ระบบคอมพิวเตอร์ไม่สามารถใช้งานได้ ตัวอย่างการแทรกแซงระบบที่อาชญากรทางคอมพิวเตอร์นิยมใช้ได้แก่ การโจมตีให้ระบบคอมพิวเตอร์ปฏิเสธการให้บริการ (Denial of Service) โดยทั่วไปแล้วระบบเครือข่ายคอมพิวเตอร์จะมีขั้นตอนต่างๆ เพื่อให้คอมพิวเตอร์สามารถติดต่อระหว่างกันได้และให้ข้อมูลเดินทางไปถึงที่หมายได้อย่างถูกต้องแม่นยำ โดยผู้ใช้งานคอมพิวเตอร์จะต้องส่งคำขอไปยัง server ที่จัดเก็บข้อมูลเพื่อให้ server ดำเนินการระบุตัวเองและตอบสนองกลับไป

---

[25] S. Morris, The Future of Netcrime Now: Part 1-threats and challenges, Hope office online report 62/04 (Home Office, 2004). p.23, Cited in: Jonathan Clough, Principles of Cybercrime, p.35

[26] Jonathan Clough, Principles of Cybercrime,p.36

[27] *US v. Prerez* (SD Cal 2005) US Department of Justice, Press Release, 26 August 2005 Cited in: Jonathan Clough, Principles of Cybercrime, p.36 fn.40

* อนุสัญญากรุงบูดาเปสต์ได้กำหนดความผิดฐานนี้ไว้ในข้อ 5 ของอนุสัญญา

เมื่อคอมพิวเตอร์ของผู้ใช้งานได้รับการตอบรับแล้ว ข้อมูลก็จะถูกส่งไปยังปลายทางได้[28] ภายใต้การโจมตีให้ระบบคอมพิวเตอร์ปฏิเสธการให้บริการนั้น ผู้กระทำความผิดจะส่งคำขอใช้บริการจำนวนมหาศาลไปยังระบบคอมพิวเตอร์เป้าหมายจนระบบไม่สามารถรองรับคำขอทั้งหมดได้และต้องปิดตัวลงไปในที่สุด ตัวอย่างของการโจมตีให้ระบบคอมพิวเตอร์ปฏิเสธการให้บริการนี้ ได้แก่ เหตุการณ์ในปี 2010 ที่บริษัทบัตรเครดิตรายใหญ่หลายแห่งเช่น Master Card ถูกโจมตีโดยผู้สนับสนุนของ wikileaks ซึ่งเป็นองค์กรที่มีบทบาทในการเผยแพร่ข้อมูลลับของรัฐบาลผ่านทางอินเตอร์เน็ต เพื่อเป็นการตอบโต้ที่ทางบริษัทไม่ยอมให้ผู้สนับสนุน wikileaks บริจาคเงินสนับสนุนไปยัง web site ดังกล่าวด้วยการใช้บัตรเครดิตของบริษัท[29][30]

เนื่องจากในปัจจุบัน อุปกรณ์ รหัสผ่าน หรือข้อมูลที่นำไปใช้ประกอบอาชญากรรมทางคอมพิวเตอร์ดังข้างต้น สามารถจัดหาซื้อได้จากทางอินเตอร์เน็ต[31] หรืออาจถูกแจกจ่ายโดยไม่คิดค่าตอบแทนใดๆ[32] การกระทำความผิดต่อความลับ ความสมบูรณ์ และความพร้อมใช้งานของข้อมูลและระบบคอมพิวเตอร์จึงครอบคลุมถึงการกระทำบางอย่างเช่น ซื้อขาย หรือเผยแพร่ อุปกรณ์ รหัสผ่าน หรือข้อมูลดังกล่าวด้วย โดยจะเรียกโดยรวมว่าเป็นการใช้อุปกรณ์โดยมิชอบ (Misuse of Device) * ข้อยุ่งยากประการหนึ่งที่พบได้ในการป้องกันและปราบปรามความผิดประเภทนี้คือ เทคโนโลยีสำหรับประกอบอาชญากรรมทางคอมพิวเตอร์บางประเภทนั้นสามารถใช้ประโยชน์ได้ทั้งในทางที่ชอบและมิชอบด้วยกฎหมาย (dual use) ส่งผลให้การจำกัดการใช้เทคโนโลยีบางประเภทส่งผลกระทบไปยังผู้ใช้งานโดยสุจริตด้วย

ด้วยความสามารถในการย้อนทวนกระบวนการโดยอัตโนมัติ อาชญากรรมทางคอมพิวเตอร์ประเภทนี้สามารถสร้างความเสียหายได้ในระดับที่เป็นไปไม่ได้เมื่อเทียบ

---

[28] Jonathan Clough, Principles of Cybercrime, p.38

[29] Jennifer Scott, "MasterCard site taken down in WikiLeaks revenge," ITPro (8 December 2010) Available from: http://www.itpro.co.uk/629251/mastercard-site-taken-down-in-wikileaks-revenge [2013, May 7]

[31] Marco Gercke. Understanding cybercrime: A guide for developing countries, p.51

[32] *Ibid*.

* อนุสัญญากรุงบูดาเปสต์ได้กำหนดความผิดฐานนี้ไว้ในข้อ 6 ของอนุสัญญา

กับอาชญากรรมทำนองเดียวกันที่ก่อขึ้นโดยปราศจากการอาศัยเทคโนโลยีทางคอมพิวเตอร์ ตัวอย่างหนึ่งที่แสดงให้เห็นประเด็นปัญหาดังกล่าวได้แก่เหตุการณ์ของการแพร่ไวรัสคอมพิวเตอร์ I love you ในปี 2000 ซึ่งแม้จะกระทำขึ้นโดยบุคคลคนเดียว แต่กลับสามารถสร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์จำนวนประมาณ 45 ล้านเครื่องทั่วโลก และคิดมูลค่าความเสียหายเป็นจำนวนเงินประมาณ 6, 700 ถึง 10,000ล้านเหรียญสหรัฐ[33]

2.1.2.2 การกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์

การกระทำความผิดประเภทนี้ คือการกระทำความผิดตามกฎหมายอาญาทั่วไปบางประเภทที่อาศัยเทคโนโลยีทางคอมพิวเตอร์เพื่อให้การกระทำความผิดสำเร็จ ตัวอย่างของความผิดเกี่ยวกับคอมพิวเตอร์ที่พบเห็นได้มากได้แก่ การปลอมแปลง* และการฉ้อโกงทางคอมพิวเตอร์** ซึ่งเทียบได้กับการปลอมแปลงและการฉ้อโกงตามกฎหมายอาญาทั่วไป

อย่างไรก็ดี การใช้เทคโนโลยีทางคอมพิวเตอร์นั้น ส่งผลให้ความเสียหายจากการกระทำความผิดขยายวงกว้างไปได้อย่างรวดเร็วกว่าการกระทำความผิดที่ไม่อาศัยเทคโนโลยีทางคอมพิวเตอร์ เพราะเทคโนโลยีทางคอมพิวเตอร์สามารถย้อนทวนกระบวนการต่างๆได้อย่างอัตโนมัติ นอกจากนี้ การที่ผู้เสียหายจากการกระทำผิดมีจำนวนมากยังส่งผลให้ผู้กระทำผิดสามารถปิดบังการกระทำของตนด้วยการถัวเฉลี่ยความเสียหายรายบุคคลให้น้อยลงจนไม่ตกเป็นที่สังเกต และไม่คุ้มค่าต่อการแจ้งความและดำเนินคดี[34] ตัวอย่างในเรื่องดังกล่าวนี้สามารถเห็นได้จากสถิติในปี 2006 ของคณะกรรมการการค้าที่เป็นธรรม (Federal Trade Commission) ของสหรัฐอเมริกาซึ่งบ่งชี้ว่า คณะกรรมการได้รับคำร้องเกี่ยวข้องกับการฉ้อโกงเงินจำนวนระหว่าง 0-25 เหรียญสหรัฐในอัตราเกือบ 50%[35] ของจำนวนคำร้องทั้งหมด

---

[33] “New virus named after Philippine president,” IOL News (1 September 2000) Available from: http://www.iol.co.za/news/world/new-virus-named-after-philippine-president-1.46738#.UYjCRYF0gdU [2013, May 7]

* อนุสัญญากรุงบูดาเปสต์ได้กำหนดความผิดฐานนี้ไว้ในข้อ 7 ของอนุสัญญา

** อนุสัญญากรุงบูดาเปสต์ได้กำหนดความผิดฐานนี้ไว้ในข้อ 8 ของอนุสัญญา

[34] Marco Gercke. Understanding cybercrime: A guide for developing countries, p.45

[35] *Ibid.*,p.45

การฉ้อโกงทางคอมพิวเตอร์มีอยู่หลายรูปแบบ หนึ่งในนั้นคือการฉ้อโกงค่าธรรมเนียมล่วงหน้า (Advance Fee Fraud) ซึ่งรู้จักกันภายใต้อีกชื่อหนึ่งคือ Nigerian Scam ภายใต้การฉ้อโกงประเภทนี้ ผู้กระทำผิดจะส่งข้อความชักจูงให้ผู้เสียหายช่วยเหลือตนโอนเงินจำนวนมหาศาลออกนอกประเทศ ด้วยการฝากเงินไปยังบัญชีธนาคารของผู้เสียหาย โดยสัญญาว่าจะให้ค่านายหน้าตอบแทนซึ่งไม่มีอยู่จริง ในขณะเดียวกัน ฝ่ายผู้กระทำผิดจะขอข้อมูลบัญชีธนาคารของผู้เสียหาย อีกทั้งขอให้อีกฝ่าย จ่ายเงินจำนวนหนึ่งเพื่อดำเนินการตามขั้นตอนต่างๆด้วย[36] เมื่อผู้เสียหายหลงเชื่อ ผู้กระทำผิดจะได้ทั้งข้อมูลทางธนาคารและเงินของอีกฝ่าย นอกจากนี้ การฉ้อโกงทางอินเตอร์เน็ตยังเกิดได้กับการทำธุรกรรมทางอินเตอร์เน็ตแบบต่างๆ อาทิ กรณีที่ผู้ขายสินค้าทางอินเตอร์เน็ตไม่ยอมส่งมอบสินค้า หรือกรณีที่ผู้ซื้อสินค้าทางอินเตอร์เน็ตไม่ยอมชำระค่าสินค้าตามที่ตกลงไว้ หรือการโกงประมูลทางอินเตอร์เน็ต[37] ภายใต้กรณีดังกล่าว ผู้กระทำผิดจะให้ข้อมูลทางธนาคารปลอมหรือนำหมายเลขบัตรเครดิตของบุคคลที่สามมาใช้ในการทำธุรกรรม ทั้งนี้ การซื้อขายผ่านทางอินเตอร์เน็ตจะไม่มีการตรวจสอบความถูกต้องของลายเซ็นหรือบัตรเครดิตอย่างเช่นการซื้อขายตามปกติ ฝ่ายผู้ขายเพียงแต่จะตรวจสอบว่า ข้อมูลที่ผู้ซื้อให้มามีอยู่จริงหรือไม่ หากแต่จะไม่ตรวจสอบว่าผู้ซื้อเป็นเจ้าของข้อมูลนั้นโดยแท้จริงหรือไม่แต่อย่างใด[38]

นอกจากการปลอมแปลงและฉ้อโกงทางคอมพิวเตอร์แล้ว ตัวอย่างของการกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์อีกประการหนึ่งได้แก่ การก่ออาชญากรรมทางข้อมูลระบุตัวตน (identity crime) ซึ่งผู้กระทำผิดจะใช้ตัวตนปลอมหรือขโมยข้อมูลเกี่ยวกับตัวตนของผู้อื่นผ่านทางอินเตอร์เน็ตเพื่อนำไปใช้แสวงหาเงิน บริการ หรือผลประโยชน์อื่นๆโดยที่ตนเองไม่มีสิทธิและให้เจ้าของข้อมูลแท้จริงแบกรับต่างๆแทน ข้อมูลระบุตัวตนที่ถูกโจรกรรมได้นั้นได้แก่ หมายเลขประกันสังคม หมายเลขหนังสือเดินทาง รหัสบัญชีธนาคาร หรือรหัสของบัญชีที่ไม่เกี่ยวข้องกับการเงินอย่าง เช่น บัญชีอีเมล์หรือเครือข่ายสังคม เป็นต้น[39] ตัวอย่างการขโมยข้อมูลระบุตัวตนได้แก่ คดี R. v. Zeihr ของประเทศอเมริกา[40] ซึ่งผู้กระทำผิดได้ปลอมแปลงใบแจ้ง

---

[36] Jonathan Clough, Principles of Cybercrime, p.183

[37] *Ibid*., p.185

[38] *Ibid*., p.186

[39] Marco Gercke. Understanding cybercrime: A guide for developing countries, p.49-50

[40] Jonathan Clough, Principles of Cybercrime, p191 fn41

เกิดและบัตรประจำตัวนักศึกษาปลอมจำนวนอย่างละ 41 ใบ เพื่อใช้ดำเนินการต่างๆเช่น เปิดบัญชีธนาคาร เพื่อทำบัตรเครดิตสำหรับใช้ในธุรกรรมต่างๆต่อไป

2.1.2.3 การกระทำผิดที่เกี่ยวข้องกับเนื้อหา

ภายใต้การกระทำความผิดรูปแบบนี้ ผู้กระทำความผิดจะเผยแพร่หรือแสดงข้อมูลที่ผิดกฎหมายโดยเนื้อหาของตัวเองอย่างเช่น สิ่งลามกอนาจาร การประกาศรับจ้างก่ออาชญากรรม โดยอาศัยอินเตอร์เน็ตเป็นช่องทางการติดต่อสื่อสารข้อมูลเหล่านั้น ตัวอย่างหนึ่งของความผิดทางเนื้อหาที่รัฐต่างๆให้ความสำคัญในการปราบปราม คือ การเผยแพร่สิ่งลามกอนาจารเด็ก*

สามารถกล่าวได้ว่า พัฒนาการทางเทคโนโลยีทางคอมพิวเตอร์มีส่วนส่งเสริมให้การกระทำความผิดประเภทนี้มีจำนวนมากขึ้นและเป็นไปโดยสะดวกมากขึ้น โดยผู้กระทำผิดจะสามารถเผยแพร่ข้อมูลหรือวัตถุผิดกฎหมายในรูปแบบข้อมูลดิจิตัลไปได้อย่างรวดเร็วโดยคงคุณภาพเดิมไว้ได้ ซึ่งเป็นผลมาจากการที่เครือข่ายอินเตอร์เน็ตและ web site ต่างๆสามารถรองรับข้อมูลได้ในปริมาณมากขึ้น นอกจากนี้ อุปกรณ์สำหรับเก็บข้อมูลทางคอมพิวเตอร์ในปัจจุบันยังมีราคาถูก พกพาง่ายและบรรจุข้อมูลผิดกฎหมายได้ในปริมาณมากด้วย[41] ในขณะเดียวกัน การที่ระบบอินเตอร์เน็ตสามารถเชื่อมต่อระบบคอมพิวเตอร์ทั่วโลกเข้าไว้ด้วยกัน ยังส่งผลให้มีผู้สามารถเข้าถึงข้อมูลผิดกฎหมายได้เป็นจำนวนมากภายในระยะเวลาไม่นานเท่านั้น นั่นจึงเป็นปัจจัยหนึ่งที่สร้างแรงจูงใจให้ผู้กระทำผิดเลือกเผยแพร่เนื้อหาผิดกฎหมายผ่านทางเครือข่ายอินเตอร์เน็ตมากขึ้นด้วย

แนวทางที่นิยมใช้ป้องกันปราบปรามการกระทำความผิดประเภทนี้ได้แก่ การปิดกั้น (block) เพื่อป้องกันไม่ให้ผู้ใช้งานคอมพิวเตอร์สามารถเข้าถึงข้อมูลที่ผิดกฎหมาย[42] อย่างไรก็ตาม ฝ่ายผู้ถูกปิดกั้นข้อมูลที่มีความรู้ทางคอมพิวเตอร์สูงเพียงพอจะสามารถแสวงหามาตรการหลบเลี่ยงมาตรการปิดกั้นต่างๆและเข้าถึงข้อมูลที่ผิดกฎหมายได้ต่อไป

---

* อนุสัญญากรุงบูดาเปสต์ได้กำหนดความผิดฐานนี้ไว้ในข้อ 9 ของอนุสัญญา

[41] Jonathan Clough, Principles of Cybercrime, p.248-249

[42] Marco Gercke. Understanding cybercrime: A guide for developing countries, p.30

อาทิ การใช้ proxy server เป็นต้น ในขณะเดียวกัน ผู้กระทำผิดบางรายสามารถนำข้อมูลต้องห้ามไปเผยแพร่ผ่าน web site ใหม่ หรือช่องทางใหม่ๆต่อไปได้

วิธีการที่ใช้ป้องกันกั้นไม่ให้ผู้ใช้คอมพิวเตอร์เข้าถึงข้อมูลที่ผิดกฎหมายได้อีกวิธีหนึ่งก็คือการติดตั้งโปรแกรมกลั่นกรองข้อมูล (filtering) เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลประเภทที่กำหนดไว้[43] โดยทั่วไปแล้วฝ่ายรัฐจะเป็นผู้ที่สั่งการให้ผู้บริการทางอินเตอร์เน็ตดำเนินการกลั่นกรองหรือปิดกั้น web site ต่างๆที่มีข้อมูลต้องห้ามบนอินเตอร์เน็ต อย่างไรก็ตามการเฝ้าตรวจตราระบบเครือข่ายคอมพิวเตอร์นั้นเป็นไปอย่างยากลำบากเพราะโครงสร้างพื้นฐานที่เกี่ยวข้องมีขนาดใหญ่ และมักมีเอกชนเป็นเจ้าของ หน่วยงานผู้บังคับใช้กฎหมายจึงต้องติดต่อประสานงานกับหน่วยงานภาคเอกชนจำนวนมาก[44]

อุปสรรคสำคัญอีกประการหนึ่งของอาชญากรรมคอมพิวเตอร์ประเภทนี้ก็คือ รัฐต่างๆมีค่านิยมที่แตกต่างกัน จึงส่งผลให้เนื้อหาที่ผิดกฎหมายของรัฐหนึ่ง อาจไม่ใช่สิ่งผิดกฎหมายของรัฐอื่น รัฐบางรัฐจะเห็นว่าสิ่งลามกอนาจารที่ไม่ใช้เด็กนั้นไม่ผิดกฎหมาย หากแต่ต้องมีการป้องกันไม่ให้บุคคลอายุต่ำกว่าเกณฑ์สามารถเข้าถึงได้ แต่รัฐอีกกลุ่มหนึ่งอาจเห็นว่าวัตถุเหล่านี้ผิดกฎหมายอย่างเด็ดขาด ค่านิยมประการหนึ่งที่เป็นเหตุให้เกิดความแตกต่างในการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ประเภทนี้ก็คือสิทธิมนุษยชน โดยเฉพาะอย่างยิ่งในประเด็นเรื่องเสรีภาพในการแสดงออก ยกตัวอย่างเช่น รัฐในทวีปยุโรปเห็นว่าการแสดงข้อความเหยียดผิว เหยียดเชื้อชาติ เป็นความผิดทางอาญา ส่วนรัฐกลุ่มอื่นเช่น สหรัฐอเมริกา จะเห็นว่าการแสดงออกดังกล่าวเป็นการใช้เสรีภาพในการแสดงออก (freedom of expression) ซึ่งชอบด้วยกฎหมายแล้ว

2.1.2.4 **การกระทำความผิดเกี่ยวกับทรัพย์สินทางปัญญา**

ตัวอย่างของความผิดประเภทนี้ได้แก่ การละเมิดลิขสิทธิ์ทางคอมพิวเตอร์* การที่ผลงานอันมีลิขสิทธิ์อาทิ วรรณกรรม ภาพวาด เพลง นั้นมีลักษณะเป็นการแสดงข้อมูลในรูปแบบต่างๆ

---

[43] *Ibid.*

[44] Jonathan Clough, Principles of Cybercrime,p.8

* อนุสัญญากรุงบูดาเปสต์ได้กำหนดความผิดฐานนี้ไว้ในข้อ 10 ของอนุสัญญา

ผลงานเหล่านี้ จึงสามารถถูกดัดแปลงให้อยู่ในรูปแบบข้อมูลดิจิตัล ซึ่งง่ายต่อการคัดลอก ทำซ้ำ ดัดแปลง หรือเผยแพร่ผ่านทางเครือข่ายอินเตอร์เน็ตได้ ถึงแม้ว่าในด้านหนึ่ง เจ้าของทรัพย์สินทางปัญญาจะอาศัยพัฒนาการทางเทคโนโลยีดังกล่าวในการแจกจ่ายและขายทรัพย์สินทางปัญญาของตนไปยังตลาดทั่วโลกได้ง่ายดายและรวดเร็วขึ้น ผู้ละเมิดสิทธิเหนือทรัพย์สินทางปัญญาสามารถละเมิดลิขสิทธิ์ได้อย่างสะดวกง่ายดายขึ้นเช่นกัน[45] ยกตัวอย่างเช่น ในภาคอุตสาหกรรมเพลง ได้มีการสำรวจในปี 2008โดย International Federation of Phonographic Industry ซึ่งพบว่า แผ่นซีดีเพลงที่ขายได้ทุก 1 แผ่นนั้นมีอัตราส่วนการดาวน์โหลดอย่างผิดกฎหมายถึง 20 ครั้ง[46]

พัฒนาการทางเทคโนโลยีคอมพิวเตอร์ไม่เพียงแต่ส่งเสริมให้การการกระทำความผิดที่เกี่ยวกับทรัพย์สินทางปัญญามีมากขึ้นเท่านั้น หากแต่ยังมีบทบาทสำคัญในการทำให้ความผิดสำเร็จด้วย ทั้งนี้ ในปัจจุบัน ฝ่ายผู้สร้างสรรค์ผลงานอันมีลิขสิทธิ์ได้พยายามแก้ไขปัญหาด้วยการพัฒนามาตรการปกป้องผลงานของตนจากการละเมิด ไม่ว่าจะเป็นการกำหนดให้ผู้ใช้กรอกรหัสผ่านเพื่อติดตั้งโปรแกรมคอมพิวเตอร์ รหัสผ่านดังกล่าวนี้จะส่งมาพร้อมกับสินค้าถูกลิขสิทธิ์เท่านั้น หรือการใช้โปรแกรมคอมพิวเตอร์เพื่อตรวจสอบความถูกต้องตามลิขสิทธิ์ ตัวอย่างของโปรแกรมดังกล่าวได้แก่ Windows Genuine Advantage (WGA) ของบริษัทไมโครซอฟต์ ซึ่งจะตรวจสอบความถูกต้องในการลงทะเบียนระบบปฏิบัติการไมโครซอฟต์วินโดว์ส ในขณะที่ผู้ใช้งานทำการอัพเดทข้อมูลวินโดวส์หรือดาวน์โหลดโปรแกรมเสริมต่างๆจากไมโครซอฟต์ เป็นต้น อย่างไรก็ดี ฝ่ายผู้ละเมิดลิขสิทธิ์เองก็ได้พัฒนาเทคโนโลยีเพื่อหลบเลี่ยงหรือกำจัดมาตรการป้องกันดังกล่าวเช่นเดียวกัน วิธีการหนึ่งที่ใช้ ได้แก่ Software Cracking ซึ่งจะเป็นการกำจัดมาตรการป้องกันการละเมิดลิขสิทธิ์ออกไปซอฟต์แวร์คอมพิวเตอร์เพื่อนำไปไปคัดลอก แจกจ่าย หรือวางขายในลำดับต่อไป

ตัวอย่างเทคโนโลยีที่มีบทบาทสำคัญในการละเมิดลิขสิทธิ์ทางคอมพิวเตอร์ได้แก่ เครือข่ายแบบ peer-to-peer (p2p) ในอดีตนั้น ฐานที่ตั้งของข้อมูลต่างๆมักจะมีการรวมศูนย์ไว้ที่คอมพิวเตอร์เครื่องใดเครื่องหนึ่ง ผู้ใช้คอมพิวเตอร์จำเป็นต้องเข้าสู่ web site กลางเพื่อติดต่อ

---

[45] Jonathan Clough, Principles of Cybercrime, p.221-222

[46] International Federation of the Phonographic Industry, IFPI Digital Music Report 2008, p.18 Cited in: Jonathan Clough, Principles of Cybercrime, p.222

ขอดาวน์โหลดข้อมูลที่ตนเองต้องการโดยตรง ส่วนในกรณีของเครือข่ายแบบ p2p นั้น ผู้ใช้งานคอมพิวเตอร์ที่มีอยู่จำนวนมากสามารถติดต่อระหว่างกันได้โดยตรง และสามารถนำไฟล์ไปจัดวางในพื้นที่ที่ใช้แบ่งปันกับผู้ใช้งานรายอื่นๆได้ ด้วยเหตุนี้ ผู้ใช้งานระบบคอมพิวเตอร์เป็นได้ทั้งผู้ขอและผู้จัดหาข้อมูลได้ในคราวเดียว อีกทั้งยังค้นหาและดาวน์โหลดไฟล์จากแหล่งข้อมูลหลายแหล่งได้พร้อมๆกัน[47] นับได้ว่าเทคโนโลยี p2p ส่งผลให้การละเมิดทรัพย์สินทางปัญญามีมูลค่าเทียบเท่ากับมูลค่าการค้าอย่างถูกกฎหมายเลยทีเดียว โดยการดาวน์โหลดซอฟต์แวร์เพื่อใช้งานระบบ p2p มีจำนวนในหลักล้านครั้ง และพบการแบ่งปันไฟล์ผ่านเครือข่าย p2p เป็นจำนวนหลักพันล้านไฟล์[48] นอกจากนี้เครือข่าย p2p ยังส่งผลให้การละเมิดลิขสิทธิ์เกิดขึ้นอยู่ในระดับข้ามประเทศด้วย ส่งผลให้ต้องอาศัยการให้ความร่วมมือระหว่างหน่วยงานผู้บังคับใช้กฎหมายจากประเทศต่างๆ ยกตัวอย่างเช่น ปฏิบัติการ Buccanneer ซึ่งดำเนินการโดยเจ้าหน้ากรมศุลกากรของประเทศสหรัฐอเมริกา ร่วมกับเจ้าหน้าที่รัฐจากประเทศออสเตรเลีย อังกฤษ ฟินแลนด์ สวีเดน และนอร์เวย์[49] โดยปฏิบัติการจะมุ่งเป้าไปยังกลุ่มองค์กรผู้แจกจ่ายซอฟต์แวร์อันมีลิขสิทธิ์ ซึ่งผ่านการกำจัดมาตรการป้องกันละเมิดลิขสิทธิ์ของผู้ผลิตแล้ว และวัตถุอันมีลิขสิทธิ์อื่นๆ

นอกจากลิขสิทธิ์แล้ว เครื่องหมายการค้าก็นับเป็นทรัพย์สินทางปัญญาอีกประเภทหนึ่งที่ถูกละเมิดด้วยเทคโนโลยีทางคอมพิวเตอร์เช่นกัน โดยวิธีการละเมิดเป็นที่นิยมได้แก่ การจดทะเบียน domain name ของ web site ตนให้คล้ายคลึงกับผู้ให้บริการหรือขายสินค้าที่มีชื่อเสียง เพื่อล่อลวงให้ผู้ใช้งานที่รู้เท่าไม่ถึงการณ์เข้าไปซื้อหรือใช้บริการของตนแทน หรือชิงจดทะเบียน domain name ที่ชื่อเดียวกันกับเจ้าของเครื่องหมายการค้าหรือเครื่องหมายบริการที่มีชือเสียง เพื่อเสนอขายเจ้าของเหล่านั้นด้วยราคาที่สูงต่อไป[50] วิธีการเช่นนี้เรียกว่า cyber squatting

---

[47] Jonathan Clough, Principles of Cybercrime, p.222

[48] Metro-Goldwyn-Mayer Studios Inc. v. Grokster Ltd., 545 US 923 (2005) Cited in: Jonathan Clough, Principles of Cybercrime, p.223

[49] Computer crime and intellectual property section, US department of justice, Operation Buccaneer: The Investigation, Cited in: Jonathan Clough, Principles of Cybercrime, p.224

[50] Marco Gercke. Understanding cybercrime: A guide for developing countries, p.44

2.1.3 ข้อท้าทายของอาชญากรรมทางคอมพิวเตอร์และผลกระทบเชิงกฎหมาย

เทคโนโลยีทางคอมพิวเตอร์นั้นมีบทบาทอย่างสำคัญในการก่ออาชญากรรมทางคอมพิวเตอร์ ดังที่จะเห็นได้จากนิยามของอาชญากรรมทางคอมพิวเตอร์ที่กล่าวไว้ข้างต้น เพราะฉะนั้น เมื่อเทคโนโลยีทางคอมพิวเตอร์พัฒนาขึ้นไปตามกาลเวลา อาชญากรรมทางคอมพิวเตอร์ก็สามารถทวีความซับซ้อนควบคู่ไปกับพัฒนาการทางเทคโนโลยีเช่นกัน โดยความซับซ้อนทางข้อเท็จจริงบางประการนั้น สามารถก่อให้เกิดผลกระทบในเชิงกฎหมายได้ทั้งในด้านกฎหมายสารบัญญัติ กฎหมายวิธีสบัญญัติ และกฎหมายระหว่างประเทศ รายละเอียดมีดังต่อไปนี้

สำหรับอาชญากรรมทางคอมพิวเตอร์ที่มีข้อมูลและระบบทางคอมพิวเตอร์เป็นเป้าหมายนั้น จะเห็นได้ว่าการที่เป้าหมายของอาชญากรรมขาดลักษณะทางกายภาพ ไม่สามารถจับต้องได้นั้น ก่อให้เกิดอุปสรรคในการตีความและปรับใช้กฎหมายอาญาทั่วไปกับความผิดที่เกิดขึ้น ตัวอย่างประเด็นปัญหาดังกล่าวได้แก่ การตีความว่าข้อมูลคอมพิวเตอร์มีฐานะเป็นทรัพย์สินหรือไม่ หรือการเปรียบเทียบว่าการเข้าถึงระบบคอมพิวเตอร์โดยผิดกฎหมายเป็นเช่นเดียวกับการบุกรุกตามกฎหมายอาญาทั่วไปหรือไม่ เป็นต้น ด้วยเหตุนี้รัฐจึงจำเป็นต้องกำหนดฐานความผิดสำหรับอาชญากรรมทางคอมพิวเตอร์เป็นการเฉพาะเจาะจงเพื่อกำจัดความยุ่งยากดังกล่าวในการปราบปรามอาชญากรรม

จากการศึกษาเกี่ยวกับประเภทของอาชญากรรมทางคอมพิวเตอร์ จะพบว่าความเปลี่ยนแปลงทางเทคโนโลยี สามารถก่อให้เกิดอาชญากรรมทางคอมพิวเตอร์ประเภทใหม่ๆ ดังที่จะเห็นได้จากในกรณีการกระทำความผิดที่เกี่ยวข้องกับเนื้อหา และการกระทำความผิดต่อทรัพย์สินทางปัญญา ในอดีตนั้น เทคโนโลยีทางคอมพิวเตอร์ ไม่สามารถอำนวยความสะดวกต่อการกระทำความผิดสองประเภทนี้ได้ โดยในด้านหนึ่ง เทคโนโลยีทางอินเตอร์เน็ตในอดีตยังไม่สามารถรองรับข้อมูลที่มีความซับซ้อนในปริมาณมากได้ ผู้กระทำความผิดจึงไม่สามารถเผยแพร่เนื้อหาผิดกฎหมายบางอย่างเช่น ภาพยนตร์ลามกอนาจารเด็ก หรือผลงานอันมีลิขสิทธิ์บางประเภทเช่น ภาพยนตร์ ได้มากและสะดวกรวดเร็วเท่ากรณีที่เผยแพร่ด้วยวิธีทั่วไป นอกจากนี้ ผู้ใช้งานอินเตอร์เน็ตในอดีตนั้นยังมีไม่มากเท่าในปัจจุบัน บุคคลที่จะมารับรู้เนื้อหาที่ผิดกฎหมายหรือรับชมผลงานอันละเมิดลิขสิทธิ์ของมีลิขสิทธิ์จึงมีน้อยเช่นกัน อย่างไรก็ตาม ในปัจจุบัน เทคโนโลยีทางอินเตอร์เน็ตสามารถรองรับข้อมูลได้ในจำนวนมากและซับซ้อนมากขึ้น

และผู้ใช้งานเครือข่ายอินเตอร์เน็ตมีจำนวนมากขึ้น สภาพการณ์จึงอำนวยให้เกิดการกระทำความผิดที่เกี่ยวข้องกับเนื้อหา และการกระทำความผิดต่อทรัพย์สินทางปัญญา ด้วยเหตุนี้เมื่อพิจารณาในเชิงกฎหมายแล้ว รัฐจำเป็นต้องบัญญัติกฎหมายสารบัญญัติของตนให้ครอบคลุมอาชญากรรมทางคอมพิวเตอร์ประเภทใหม่ๆด้วย

แนวโน้มของการเกิดอาชญากรรมทางคอมพิวเตอร์ประเภทใหม่ๆนั้น สามารถสะท้อนให้เห็นได้จากพัฒนาการของกฎหมายภายในที่เกี่ยวข้องกับอาชญากรรมของคอมพิวเตอร์ อาจแบ่งออกได้เป็นสี่ระยะ โดยในระยะแรก กฎหมายอาชญากรรมทางคอมพิวเตอร์จะเน้นไปยังการปกป้องข้อมูลส่วนบุคคลที่ถูกกักเก็บในอุปกรณ์ทางคอมพิวเตอร์ หลังจากนั้นกฎหมายในระยะต่อมาจะขยายเนื้อหาครอบคลุมไปถึงอาชญากรรมทางเศรษฐกิจด้วย ส่วนในระยะที่สามและสี่นั้น กฎหมายจะครอบคลุมถึงการปกป้องทรัพย์สินทางปัญญาโดยเฉพาะในด้านเทคโนโลยีทางคอมพิวเตอร์ และการเผยแพร่ข้อความเนื้อหาที่ผิดกฎหมายและมีอันตราย เช่น วัตถุลามกอนาจารเด็ก ตามลำดับ[51]

เมื่อเปรียบเทียบกับอาชญากรรมทั่วไปแล้ว อาชญากรทางคอมพิวเตอร์นั้นสามารถปฏิบัติการได้ภายใต้ภาวะนิรนาม (anonymity) กล่าวคือไม่ต้องระบุตัวตนที่แท้จริงลงไปในระหว่างใช้งาน และอีกทั้งยังสามารถใช้เทคโนโลยีทางคอมพิวเตอร์บางอย่างปิดบังตำแหน่งคอมพิวเตอร์ที่ตนเองใช้งานจริงได้ด้วย ยกตัวอย่างเช่น การใช้ bots หรือ zombies ซึ่งผู้กระทำความผิดสามารถสั่งการให้คอมพิวเตอร์เครื่องอื่นก่ออาชญากรรมทางคอมพิวเตอร์แทนตัวเองอีกทอดหนึ่งได้ หรือการใช้เทคโนโลยีเข้ารหัสเพื่อปิดบังตำแหน่งของตนเอง เป็นต้น เพราะฉะนั้นเจ้าหน้าที่ผู้สืบสวนคดีอาชญากรรมทางคอมพิวเตอร์จึงต้องมีขีดความสามารถทางเทคโนโลยีเพียงพอสำหรับติดตามจับกุมผู้กระทำความผิดได้ อีกทั้งยังต้องใช้เทคนิคนิติเวชทางดิจิตัลที่สลับซับซ้อนเพื่อแสวงหาและเก็บรักษาหลักฐานรูปแบบข้อมูลทางอิเล็กทรอนิกส์ และทำให้หลักฐานดังกล่าวรับฟังได้ในชั้นศาล[52]

---

[51] Marc D. Goodman and Susan W. Brenner, The emerging consensus on criminal conduct in cyberspace [Online]. Available from: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf [2013, May 7], pp.31-36

[52] Jonathan Clough, Principles of Cybercrime, p.7

ตัวอย่างของหลักฐานในรูปแบบข้อมูลอิเล็กทรอนิกส์ได้แก่ Internet Protocol Address (IP Address) ของคอมพิวเตอร์ซึ่งจำเป็นต่อการติดตามหาตำแหน่งทางกายภาพของผู้กระทำผิด IP address นี้จะเป็นตัวเลขพิเศษเฉพาะสำหรับคอมพิวเตอร์แต่ละเครื่องที่เชื่อมต่อกับเครือข่ายทางอินเตอร์เน็ตหรือเครือข่ายคอมพิวเตอร์อื่นๆ เมื่อมีการติดต่อสื่อสารผ่านทางอินเตอร์เน็ต คอมพิวเตอร์ที่สื่อสารกันจำเป็นที่จะต้องทราบถึง IP address ของอีกฝ่ายเสียก่อนเพื่อไม่ให้ปะปนสับสนกับคอมพิวเตอร์ที่เชื่อมต่อกับอินเตอร์เน็ตเครื่องอื่นๆ ดังนั้นเมื่อมีการก่ออาชญากรรมผ่านทางอินเตอร์เน็ต คอมพิวเตอร์ของผู้เสียหายก็จะบันทึก IP address ของคอมพิวเตอร์ที่ผู้กระทำความผิดใช้เพื่อติดต่อระหว่างกันด้วย

ในการสืบสวนคดีอาชญากรรมทางคอมพิวเตอร์นั้น หน่วยงานผู้บังคับใช้กฎหมายจะต้องประสานงานกับผู้ให้บริการทางอินเตอร์เน็ต (Internet Service Provider หรือ ISP) เพราะผู้ใช้งานอินเตอร์เน็ตจะต้องสมัครใช้บริการกับ ISP และให้ข้อมูลการติดต่อกับอีกฝ่าย โดย ISP จะจัดตัวเลข IP Address ให้แก่คอมพิวเตอร์ที่เชื่อมต่อกับอินเตอร์เน็ตและบันทึกว่าคอมพิวเตอร์เครื่องไหนได้รับ IP address อะไรไปในช่วงเวลาหนึ่งๆ ด้วยข้อมูลเหล่านี้ ISP จะสามารถติดตามร่องรอยไปถึงตำแหน่งทางกายภาพของผู้กระทำความผิดได้ ในการติดตามร่องรอยนี้ ผู้ติดตามต้องระบุตำแหน่งและเวลาการใช้งานของ IP address ที่ต้องสงสัยอย่างแม่นยำ เพราะในความเป็นจริง IP Address มีอยู่จำกัด แต่จำนวนผู้ใช้งานอินเตอร์เน็ตมีสูงกว่า ส่งผลให้ผู้ให้การทางอินเตอร์เน็ตต้องแบ่งปัน IP Address ชุดเดียวกันแก่คอมพิวเตอร์มากกว่าหนึ่งเครื่องที่เข้าใช้งานในเวลาแตกต่างกัน หากผู้ติดตาม IP address ไม่แม่นยำมากพอ ย่อมจะส่งผลให้ผู้บริสุทธิ์ถูกจับกุมแทนผู้กระทำความผิดได้ นอกจากนี้ถึงแม้ฝ่ายเจ้าหน้าที่รัฐจะระบุตำแหน่งที่มาของการสื่อสารได้ในภายหลังก็ตาม ผู้สืบสวนจะทราบเพียงเครื่องคอมพิวเตอร์ที่ใช้กระทำความผิดเท่านั้น ซึ่งนั่นไม่ได้หมายความว่าผู้กระทำผิดจะถูกระบุตัวได้เสมอไป ในขณะเดียวกัน การใช้งานคอมพิวเตอร์จากระบบไร้สายยังช่วยปิดบังตำแหน่งของผู้กระทำผิดได้อีกด้วย[53] เนื่องจากผู้กระทำความผิดสามารถใช้งานคอมพิวเตอร์ได้เมื่อเข้าไปอยู่ในรัศมีของตัวส่งสัญญาณเท่านั้น

การที่หลักฐานสำคัญในคดีอาชญากรรมทางคอมพิวเตอร์อยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์นั้น สามารถส่งผลกระทบเชิงกฎหมายวิธีสบัญญัติได้เช่นกัน

---

[53] Jonathan Clough, Principles of Cybercrime,p.6-7

ในการนี้ รัฐจำเป็นต้องเพิ่มเติมให้อำนาจการสืบสวนที่มีอยู่ตามกฎหมายวิธีพิจารณาความอาญาทั่วไปสามารถครอบคลุมบริบทอาชญากรรมทางคอมพิวเตอร์ด้วย ยกตัวอย่างเช่น ในการใช้อำนาจค้นและยึดในคดีอาชญากรรมทางคอมพิวเตอร์ เจ้าหน้าที่สืบสวนคดีจะต้องมีอำนาจกระทำการต่อข้อมูลหลักฐานที่อยู่ภายในเครื่องคอมพิวเตอร์หรือวัตถุเก็บข้อมูลที่ตนยึดมาได้ด้วย อาทิ การทำสำเนาและเก็บรักษาสำเนาข้อมูลที่ถูกเก็บไว้ หรือการทำให้ข้อมูลที่มีเนื้อหาผิดกฎหมายถูกลบทิ้งหรือเข้าถึงไม่ได้ เป็นต้น

นอกจากนี้ การที่หลักฐานของอาชญากรรมอยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์นั้น ยังส่งผลให้ ผู้กระทำผิดสามารถดัดแปลง หลบซ่อน หรือกำจัดหลักฐานดังกล่าวได้ง่ายและรวดเร็วกว่าหลักฐานที่เป็นวัตถุทางกายภาพ ด้วยเหตุนี้ กฎหมายวิธีสบัญญัติจึงควรอำนวยความสะดวกให้เจ้าหน้าที่รัฐสามารถดำเนินการปกป้องหลักฐานของอาชญากรรมได้อย่างทันสถานการณ์ อีกทั้งยังสามารถเก็บรักษาความลับของการสืบสวนคดีได้เพื่อไม่ให้ฝ่ายผู้กระทำผิดรู้ตัวและกระทำการที่ไม่พึงประสงค์ต่อหลักฐานได้

เนื่องด้วยในปัจจุบัน เครือข่ายอินเตอร์เน็ตสามารถเชื่อมโยงคอมพิวเตอร์ต่างๆทั่วโลกเข้าไว้ด้วยกัน อาชญากรรมทางคอมพิวเตอร์จึงมีมิติข้ามชาติ กล่าวคือ ผู้กระทำผิดสามารถสร้างความเสียหายแก่คอมพิวเตอร์เครื่องใดก็ได้ที่เชื่อมต่อกับอินเตอร์เน็ต โดยไม่ต้องเข้าไปอยู่ในพื้นที่เดียวกันกับผู้เสียหายแต่อย่างใด ในขณะเดียวกัน ข้อมูลจากการติดต่อสื่อสารผ่านระบบเครือข่ายอินเตอร์เน็ตนั้นจะต้องเดินทางผ่านจุดรับส่งสัญญาณภายใต้เขตอำนาจรัฐหลายเขตก่อนที่จะเดินทางไปถึงจุดหมายด้วย ลักษณะข้ามชาตินี้ ไม่เพียงแต่ส่งผลให้การติดตามเส้นทางการสื่อสารลำบากและใช้เวลายาวนานเท่านั้น หากยังเป็นเหตุให้กฎหมายว่าด้วยความร่วมมือทางอาญาระหว่างประเทศเข้ามามีบทบาทในการปราบปรามอาชญากรรมนอกเหนือไปจากกฎหมายภายในด้วย

ทั้งนี้ กฎหมายระหว่างประเทศกำหนดไว้ว่ารัฐต่างๆมีความเท่าเทียมกัน และต่างมีอำนาจอธิปไตยเป็นของตนเอง เพราะฉะนั้น การใช้อำนาจอธิปไตยต่างๆของรัฐ ไม่ว่าจะเป็นอำนาจทางนิติบัญญัติ อำนาจบริหาร อำนาจตุลาการ จะต้องไม่ไปก้าวก่ายอำนาจอธิปไตยของรัฐอื่นเป็นอันขาด โดยหลักทั่วไป อำนาจอธิปไตยของรัฐจะอยู่ในเขตแดนของรัฐเท่านั้น เมื่ออาชญากรรมทางคอมพิวเตอร์ส่งผลกระทบไปยังรัฐอีกรัฐหนึ่ง รัฐที่ได้รับความเสียหายจะไม่สามารถเข้าไปก้าวก่ายอำนาจอธิปไตยของรัฐอื่นๆด้วยการติดตามจับกุมผู้กระทำผิด หรือสอบสวนสืบสวนคดี

ภายในเขตแดนของรัฐอื่นๆได้ เพราะฉะนั้น รัฐที่ได้รับผลกระทบจากอาชญากรรมทางคอมพิวเตอร์จึงต้องดำเนินการขอความยินยอมจากรัฐอื่นในการจับกุมหรือสืบสวนสอบสวนคดีแทนตนเอง การดำเนินการดังกล่าวคือการให้ความร่วมมือกันทางอาญาระหว่างประเทศ ซึ่งจะสามารถช่วยให้การติดตามจับกุมผู้กระทำผิดมีขึ้นตามที่รัฐที่ความเสียหายเกิดขึ้นต้องการในขณะที่ยังรักษาอำนาจอธิปไตยของรัฐผู้รับการร้องขอความร่วมมือไว้ด้วยในคราวเดียวกัน

2.2 กลไกความร่วมมือทางอาญาระหว่างประเทศโดยทั่วไป

การให้ความร่วมมือทางอาญาระหว่างประเทศที่สำคัญมีอยู่สองรูปแบบ คือการส่งตัวผู้ร้ายข้ามแดนและการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมาย โดยจะมีรัฐผู้เกี่ยวข้องอยู่ด้วยกันสองฝ่าย คือฝ่ายรัฐผู้ร้องขอความช่วยเหลือ และฝ่ายรัฐผู้ให้ความช่วยเหลือ การดำเนินการสองรูปแบบนี้มีความสำคัญในการติดตามจับกุมและดำเนินคดีต่อผู้กระทำผิด แต่ในขณะเดียวกันก็มีส่วนเกี่ยวพันกับการใช้อำนาจอธิปไตยของรัฐอีกฝ่าย ดังนั้น กฎหมายระหว่างประเทศจึงต้องกำหนดหลักเกณฑ์ต่างๆเกี่ยวกับการให้ความร่วมมือทางอาญาระหว่างประเทศทั้งสองรูปแบบเอาไว้

นอกจากนี้ รัฐต่างๆที่เกี่ยวข้องในคดีอาชญากรรมทางคอมพิวเตอร์ยังสามารถให้ความช่วยเหลือรูปแบบอื่นๆ ที่ไม่เป็นการละเมิดอำนาจอธิปไตยของอีกฝ่ายได้เช่นกัน ยกตัวอย่างเช่นการสอบถามข้อมูลทั่วไป การฝึกอบรมเทคนิคให้แก่ฝ่ายเจ้าหน้าที่รัฐที่เกี่ยวข้อง หรือการปรึกษาหารือ เป็นต้น การดำเนินการตามความร่วมมือประเภทนี้จะไม่เป็นที่ทางการนักโดยหน่วยงานผู้บังคับใช้กฎหมายจะติดต่อกับหน่วยงานของอีกรัฐหนึ่งโดยตรง ส่งผลให้กระบวนการเป็นไปอย่างรวดเร็ว ไม่ซับซ้อน จึงนับได้ว่ามีประโยชน์ในฐานะทางเลือกสำหรับใช้ก่อนหน้าการขอความร่วมมืออย่างเป็นทางการ หรือใช้เป็นทางเลือกพิเศษหากรัฐผู้ร้องขอความช่วยเหลือนั้นนั้นไม่ได้ทำข้อตกลงความร่วมมือระหว่างประเทศไว้อย่างเป็นทางการมาตั้งแต่ต้น[54]

---

[54] ADB/OECD anti-corruption initiative for Asia and the Pacific, Mutual legal assistance , extradition and recovery of proceeds of corruption in Asia and Pacific[Online]. Asian development bank and organisation for economic co-operation and development, 2007. Available from: http://www.oecd.org/site/adboecdanti-corruptioninitiative/37900503.pdf [2013, May 7], p.77

เนื้อหาของวิทยานิพนธ์ส่วนนี้ จะอธิบายถึงหลักกฎหมายว่าด้วยการให้ความร่วมมือทางอาญาระหว่างประเทศโดยทั่วไปก่อน จากนั้นจึงจะวิเคราะห์ถึงอุปสรรคที่เกิดขึ้นจากการนำกลไกความร่วมมือทางอาญาระหว่างประเทศโดยทั่วไปมาปรับใช้ในบริบทอาชญากรรมทางคอมพิวเตอร์ อุปสรรคเหล่านี้จะนำไปสู่ความพยายามในการสร้างกลไกความร่วมมือสำหรับอาชญากรรมคอมพิวเตอร์โดยเฉพาะเจาะจงในลำดับถัดไป

2.2.1 ฐานทางกฎหมายในการให้ความร่วมมือ

ฐานทางกฎหมายที่เกี่ยวข้องกับการให้ความร่วมมือทางอาญาระหว่างประเทศนั้นจะปรากฏทั้งในรูปแบบที่ไม่เป็นและเป็นลายลักษณ์อักษร โดยฐานทางกฎหมายที่ไม่เป็นลายลักษณ์อักษรนั้น ได้แก่ กฎหมายจารีตประเพณี หรือหลักกฎหมายทั่วไปอย่างเช่นหลักไมตรีจิต (comity) หรือหลักต่างตอบแทน (reciprocity) ซึ่งฝ่ายรัฐผู้ร้องขอความร่วมมือนั้นจะให้คำมั่นว่าตนจะให้ความช่วยเหลือรูปแบบเดียวกันในคดีที่คล้ายคลึงกันในอนาคตแก่รัฐผู้ให้ความช่วยเหลือต่อไป อย่างไรก็ตามคำมั่นเช่นว่านี้ ไม่ก่อให้เกิดพันธะกรณีทางกฎหมายให้รัฐผู้รับคำร้องขอต้องให้ความช่วยเหลือตามคำขอแต่อย่างใด

ส่วนฐานทางกฎหมายที่เป็นลายลักษณ์อักษรนั้น พบได้จากสนธิสัญญาระหว่างประเทศเกี่ยวกับการส่งตัวผู้ร้ายข้ามแดน หรือการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมาย (Mutual Legal Assistance Treaty หรือ MLAT) สนธิสัญญาเหล่านี้ช่วยสร้างพันธะกรณีทางกฎหมายที่ชัดเจนให้กับบรรดารัฐที่เป็นภาคี และสามารถช่วยให้กระบวนการดำเนินการต่างๆ เป็นไปอย่างชัดเจนและรวดเร็วขึ้น[55] สนธิสัญญาเหล่านี้มีทั้งในรูปแบบพหุภาคีและทวิภาคี ตัวอย่างสนธิสัญญาแบบพหุภาคี ได้แก่ อนุสัญญาสหประชาชาติว่าด้วยองค์การอาชญากรรมข้ามชาติ (United Nations Convention on Transnational Organized Crime หรือ UNTOC) อนุสัญญาสภายุโรปว่าด้วยการให้ความช่วยเหลือในคดีอาญาปี 1959 และพิธีสารเพิ่มเติมหรืออนุสัญญาสหภาพยุโรปว่าด้วยการให้ความช่วยเหลือซึ่งกันและกันในคดีอาญา เป็นต้น ทั้งนี้ การดำเนินการตามสนธิสัญญาการให้ความร่วมมือทางอาญาระหว่างประเทศจะมีรูปแบบที่แตกต่างกันออกไป รัฐบางรัฐอาจจะใช้วิธีการนำเนื้อหาของสนธิสัญญามาจัดทำเป็นกฎหมายภายในโดยตรง ในขณะที่บางรัฐอาจจะตราบทบัญญัติกฎหมายโดยสังเขปเพื่อให้มาตรการ

---

[55] *Ibid*.,p.27

ตามกฎหมายภายในของตนมีผลบังคับใช้ในระดับระหว่างประเทศแทน นอกจากนี้ รัฐบางรัฐอาจเลือกที่จะไม่ปรับเปลี่ยนกฎหมายภายในของตนเลย หากแต่จะตีความกฎหมายที่มีอยู่ของตนให้สอดคล้องกับสนธิสัญญาระหว่างประเทศแทน[56]

ข้อตกลงแบบพหุภาคีนั้น สามารถส่งเสริมให้รัฐมีแนวทางปฏิบัติด้านการให้ความร่วมมือทางอาญาที่เสมอต้นเสมอปลายมากกว่า เมื่อเปรียบเทียบกับข้อตกลงทวิภาคีหลายๆฉบับกับรัฐจำนวนมาก อีกทั้งยังช่วยให้รัฐต่างๆสามารถรวบรวมทรัพยากรต่างๆเข้าไว้ด้วยกันและลดความเสี่ยงที่รัฐหนึ่งๆต้องแบกรับไว้เพียงรัฐเดียวด้วย นอกจากนี้ หากมีรัฐเข้าร่วมเป็นภาคีของสนธิสัญญาพหุภาคีทุกรัฐ (universal participation) ก็จะทำให้ผู้กระทำผิดไม่มีแหล่งหลบภัย (safe haven) ส่งผลให้ปริมาณการกระทำผิดลดลงในที่สุด อย่างไรก็ตาม การเจรจาต่อรองรายละเอียดของสนธิสัญญาความร่วมมือแบบทวิภาคีนั้น จะเป็นไปโดยสะดวกราบรื่นมากกว่าแบบพหุภาคี เพราะรัฐแต่ละรัฐนั้นมีแนวคิดและผลประโยชน์แตกต่างกัน ถ้าหากมีรัฐเกี่ยวข้องมากก็จะเจรจากันได้ยากลำบากและสิ้นเปลืองเวลา นอกจากนี้ การให้ความร่วมมือแบบทวิภาคียังเอื้ออำนวยให้รัฐๆสามารถกำหนดระดับของความร่วมมือได้ตามความไว้เนื้อเชื่อใจที่ตนมีต่อรัฐแต่ละรัฐ และเลือกที่จะให้ความร่วมมือเฉพาะกับรัฐที่มีระบบกฎหมายสอดคล้องกับตนได้

การให้ความร่วมมือทางอาญาระหว่างประเทศยังสามารถทำได้โดยอาศัยกฎหมายภายในของรัฐผู้รับคำร้องขอความร่วมมือ โดยกฎหมายภายในดังกล่าวจะระบุวิธีการสำหรับการรับส่งการพิจารณาและจัดการตามคำร้องขอเอาไว้ ข้อดีของการอาศัยกฎหมายภายในก็คือการดำเนินการได้อย่างรวดเร็วและเสียค่าใช้จ่ายน้อยกว่าการใช้กลไกระหว่างประเทศ อย่างไรก็ดีรัฐผู้รับคำร้องขอจะไม่มีพันธะกรณีตามกฎหมายระหว่างประเทศที่จะให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายแต่อย่างใด[57]

2.2.2 **การส่งตัวผู้ร้ายข้ามแดน**

การส่งตัวผู้ร้ายข้ามแดน จะเริ่มต้นขึ้นเมื่อรัฐฝ่ายที่ร้องขอสืบสวนคดีจนสามารถระบุตัวผู้กระทำผิดได้แล้ว หรือได้พิพากษาความผิดของบุคคลผู้นั้นได้เสร็จสิ้น หากแต่บุคคลนั้น

---

[56] *Ibid*.,p.28

[57] *Ibid*., p. 32

ได้หลบหนีไปยังดินแดนของรัฐอื่นเสียก่อน จึงต้องร้องขอให้รัฐอีกฝ่ายส่งตัวบุคคลผู้กระทำผิดมาให้แก่ตน การส่งตัวผู้ร้ายข้ามแดนนี้ เป็นการให้ความร่วมมือทางอาญาระหว่างประเทศที่ความสำคัญมาก เพราะการส่งตัวผู้ร้ายข้ามแดนไม่เพียงเกี่ยวข้องกับการใช้อำนาจฝ่ายบริหารในการจับกุมผู้กระทำผิดเท่านั้น หากแต่ยังเป็นการนำบุคคลออกไปจากดินแดนของรัฐด้วย ซึ่งส่งผลเป็นการลิดรอนการใช้อำนาจอธิปไตยของรัฐอีกฝ่ายเหนือบุคคลนั้น ด้วยเหตุนี้ เกณฑ์การส่งตัวผู้ร้ายจึงเข้มงวดกว่าการให้ความร่วมมือทางอาญาระหว่างประเทศรูปแบบอื่นๆ

2.2.2.1 **หลักกฎหมายเกี่ยวกับการส่งตัวผู้ร้ายข้ามแดน**

หลักกฎหมายเกี่ยวกับการส่งตัวผู้ร้ายข้ามแดน มีที่มาจากหลักกฎหมายว่าด้วยความยินยอมของรัฐและหลักนิติรัฐ เนื่องด้วยการส่งตัวผู้ร้ายข้ามแดนมีเป็นการให้รัฐผู้รับคำร้องขอใช้อำนาจอธิปไตยเพื่อส่งผู้กระทำความผิดไปให้รัฐผู้ร้องขอ ในการดังกล่าวรัฐผู้ร้องขอจะต้องให้ความยินยอมแก่รัฐผู้ร้องขอการส่งตัวเสียก่อน เพราะภายใต้กฎหมายระหว่างประเทศ รัฐต่างๆล้วนมีความเท่าเทียมกันและมีอำนาจอธิปไตยเป็นของตนเอง การที่รัฐๆหนึ่งจะดำเนินการในสิ่งใดนั้น รัฐผู้นั้นจะต้องมีความยินยอมในการดังกล่าวเสียก่อน การให้ความยินยอมดังกล่าวเกิดขึ้นได้จากปัจจัยทางข้อเท็จจริง ได้แก่ผลประโยชน์ของชาติหรือความเหมาะสมอื่นๆ แต่ในขณะเดียวกัน การให้ความยินยอมของรัฐนั้น จะต้องเป็นไปตามหลักนิติรัฐด้วย กล่าวคือต้องเป็นไปตามกฎหมายที่ตนเองผูกพันอยู่ ไม่ว่าจะเป็นกฎหมายระหว่างประเทศหรือกฎหมายภายในของตน หลักกฎหมายทั้งสองประการดังกล่าวถูกสะท้อนในหลักกฎหมายต่างๆที่เกี่ยวข้องกับการส่งตัวผู้ร้ายข้ามแดนดังต่อไปนี้

- **หลักฐานความผิดตรงกัน** หลักกฎหมายนี้มีรากฐานมาจากหลักกฎหมายอาญาทั่วไปว่า ไม่มีโทษโดยไม่มีกฎหมาย (Nulla Poena Sine Lege) ความผิดตามคำขอให้ส่งตัวผู้ร้ายข้ามแดนจะต้องเป็นความผิดทางอาญา ตามกฎหมายภายในของทั้งฝ่ายรัฐผู้ร้องขอและรัฐผู้รับคำขอ หากกฎหมายของรัฐผู้รับคำขอไม่ได้กำหนดให้ความผิดตามคำร้องขอให้เป็นความผิดทางอาญา รัฐผู้รับคำขอจะไม่มีอำนาจในการจับกุมบุคคลผู้ไม่มีความผิด เพื่อส่งตัวไปยังรัฐผู้ร้องขอได้ และในขณะเดียวกัน ถ้าหากฝ่ายรัฐผู้ร้องขอไม่มีกฎหมายไว้รองรับฐานความผิดที่ตามคำขอส่งตัวผู้ร้ายข้ามแดน แม้ฝ่ายรัฐผู้รับคำขอจะมีกฎหมายรองรับฐานความผิดดังกล่าว รัฐผู้รับคำขอนั้นไม่สามารถดำเนินการช่วยเหลือรัฐผู้ที่ไม่มีอำนาจตามกฎหมายได้เช่นกัน

ในอดีต การตีความหลักฐานความผิดตรงกันจะเป็นไปอย่างเคร่งครัด กล่าวคือ ศาลจะพิจารณาว่าชื่อเรียกฐานความผิดและองค์ประกอบความผิดของทั้งสองรัฐนั้นตรงกันหรือไม่ แต่ในยุคปัจจุบัน รัฐต่างๆได้พยายามผ่อนคลายหลักการนี้ให้น้อยลงด้วยการพิจารณาว่า การกระทำอันเป็นเหตุแห่งการร้องขอให้ส่งตัวผู้ร้ายข้ามแดนนั้นถือเป็นความผิดของรัฐทั้งสองฝ่ายหรือไม่ โดยไม่จำเป็นให้ฐานความผิดนั้นต้องมีชื่อเรียกหรือองค์ประกอบความผิดตรงกันแต่อย่างใด วิธีการนี้เรียกว่า Conduct-based approach[58] ทั้งนี้เพื่อป้องกันไม่ให้หลักฐานความผิดตรงกันสร้างอุปสรรคที่ไม่จำเป็นให้แก่การให้ความร่วมมือทางอาญาระหว่างประเทศ เพราะการตรวจสอบความถูกต้องตามหลักเกณฑ์ฐานความผิดตรงกันนั้น มักจะต้องผ่านการวินิจฉัยของศาลซึ่งใช้เวลายาวนาน ซึ่งศาลในแต่ละรัฐก็มีแนวทางตีความกฎหมายที่เคร่งครัดไม่เท่ากัน ตัวอย่างสนธิสัญญาส่งจังผู้ร้ายข้ามแดนทวิภาคีที่ใช้ Conduct-based approach ได้แก่ สนธิสัญญาระหว่างประเทศออสเตรเลียกับฟิลิปปินส์ ประเทศจีนกับไทย ประเทศไทยกับเกาหลี เป็นต้น[59] นอกจากนี้ วิธี Conduct-based approach ยังปรากฏในกฎหมายว่าด้วยการส่งตัวผู้ร้ายข้ามแดนของบางประเทศอาทิ ออสเตรเลีย ไทย จีน ญี่ปุ่น สิงคโปร์ ปากีสถาน อีกด้วย[60]

- **หลักฐานความผิดที่สามารถส่งตัวข้ามแดนได้** การทำข้อตกลงเกี่ยวกับการส่งตัวผู้ร้ายข้ามแดนนั้น จะมีการกำหนดฐานความผิดที่สามารถส่งตัวผู้ร้ายข้ามแดนได้อย่างเฉพาะเจาะจง ซึ่งจะช่วยให้รัฐคู่ภาคีสามารถจำกัดให้มีการให้ความร่วมมือกันเฉพาะในฐานความผิดที่สำคัญเท่านั้น[61] เพื่อไม่ให้เป็นการสิ้นเปลืองทรัพยากรจนเกินไป รัฐผู้ทำข้อตกลงส่งตัวผู้ร้ายข้ามแดนจะมีวิธีปฏิบัติในด้านนี้อยู่สองรูปแบบ ได้แก่ การระบุฐานความผิดไว้อย่างเฉพาะเจาะจง (Eunumerative Approach) และการระบุอัตราโทษขั้นต่ำ (Eliminative Approach) วิธีการแรกนั้นเป็นที่นิยมในอดีต หากแต่ขาดความยืดหยุ่นในการรองรับความผิดรูปแบบใหม่ๆที่เกิดขึ้นมาภายหลัง เพราะกระบวนการ

---

[58] *Ibid*., p.42

[59] *Ibid*.,p.42

[60] *Ibid*.,p42

[61] ตะวัน พึ่งพุทธารักษ์, "ปัญหาการส่งผู้ร้ายข้ามแดนในคดีอาญากรรมคอมพิวเตอร์", (วิทยานิพนธ์ปริญญามหาบัณฑิต สาขากฎหมายระหว่างประเทศ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2546), หน้า 14.

แก้ไขสนธิสัญญาต้องใช้เวลามากสำหรับการเจรจาระหว่างรัฐภาคี[62] ส่วนวิธีแบบที่สองนั้น แม้จะยืดหยุ่นมากกว่า แต่ก็อาจเกิดปัญหาได้หากความผิดที่ร้องขอไม่ได้เป็นไปตามหลักกฎหมายฐานความผิดตรงกัน[63]

- **หลักเขตอำนาจรัฐ** ภายใต้หลักการนี้ ฝ่ายรัฐผู้ร้องขอจำเป็นต้องแสดงให้รัฐผู้รับคำร้องขอยอมรับว่า ตนมีส่วนเกี่ยวข้องส่วนได้เสียกับการกระทำความผิดตามคำขอโดยแสดงให้เห็นว่าตนมีเขตอำนาจเหนือคดีนั้น ทั้งนี้ การกล่าวอ้างเขตอำนาจรัฐจะอาศัยหลักเกณฑ์สำคัญสามประการคือ หลักดินแดน (Territorial Jurisdiction) หลักบุคคล (Personal Jurisdiction) และหลักสากล (Universal Jurisdiction) แต่ละหลักเกณฑ์มีรายละเอียดดังต่อไปนี้[64]

ภายใต้หลักดินแดน รัฐมีอำนาจศาลในคดีอาญาและมีอำนาจลงโทษผู้กระทำความผิดทางอาญาที่เกิดขึ้นภายในดินแดนของตน ไม่ว่าผู้กระทำความผิดจะมีสัญชาติใดก็ตาม อาณาเขตของรัฐที่กล่าวมานี้ ยังครอบคลุมไปถึงน่านน้ำต่างๆ ตามกฎหมายระหว่างประเทศว่าด้วยทะเล และห้วงอากาศเหนือดินแดนดังกล่าว เนื่องจากรัฐต่างๆสามารถใช้อำนาจอธิปไตยได้อย่างเต็มที่ทั้งในด้านนิติบัญญัติ บริหาร ตุลาการ ภายในดินแดนของตน การกล่าวอ้างหลักดินแดนจึงสะท้อนถึงการมีส่วนได้เสียในการกระทำความผิดที่เกิดขึ้นอย่างมากที่สุด

นอกจากการพิจารณาจากสถานที่ที่กระทำความผิดเกิดขึ้นแล้ว รัฐบางส่วนอาจขยายขอบเขตการกล่าวอ้างเขตอำนาจด้วยหลักดินแดน ให้ครอบคลุมกรณีที่การกระทำที่ก่อให้เกิดองค์ประกอบความผิดเพียงส่วนใดส่วนหนึ่งเกิดขึ้นภายในรัฐ หรือกรณีที่ผลลัพธ์ของการกระทำความผิดนั้นเกิดขึ้นภายในรัฐได้[65]

---

[62] I.A. Shearer, Extradition in international law (Manchester: Manchester Press, 1997), p.134 p.134

[63] ตะวัน พึ่งพุทธารักษ์, “ปัญหาการส่งผู้ร้ายข้ามแดนในคดีอาญากรรมคอมพิวเตอร์”, หน้า 16-17.

[64] สุผานิต มั่นศุข, กฎหมายระหว่างประเทศแผนกคดีอาญา (กรุงเทพฯ : คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2523), หน้า 13-14

[65] Henrik W.K. Kaspersen, Cybercrime and internet jurisdiction [Online]. Strasbourg: Council of Europe, Directorate general of human rights and legal affairs, Economic crime division, 2009.

สืบเนื่องจากหลักดินแดน การกล่าวอ้างเขตอำนาจรัฐยังสามารถกระทำได้โดยใช้หลักกึ่งดินแดน (Quasi-territorial jurisdiction) ได้เช่นกัน โดยรัฐจะถือว่าการกระทำที่เกิดขึ้นภายในเรือที่ชักธงของตน หรือเกิดขึ้นภายในอากาศยานที่จดทะเบียนตามกฎหมายของตนนั้น นับเป็นการกระทำที่เกิดขึ้นภายในรัฐด้วย

การกล่าวอ้างเขตอำนาจด้วยหลักบุคคลนั้น มีรากฐานมาจากหน้าที่ตามกฎหมายของรัฐที่จะต้องปกครองและปกป้องคุ้มครองคนชาติของตนเองโดยสามารถจำแนกออกได้สองรูปแบบ ได้แก่ หลักสัญชาติผู้เสียหาย (Passive personality principle) และหลักสัญชาติผู้กระทำความผิด (Active personality principle) โดยภายใต้ หลักสัญชาติผู้เสียหายนั้น รัฐจะกล่าวอ้างเขตอำนาจเหนือการกระทำผิดที่กระทำต่อคนชาติของตน โดยไม่ต้องคำนึงถึงสัญชาติของผู้กระทำผิด หรือสถานที่ที่ความผิดเกิดขึ้นแต่อย่างใด อย่างไรก็ตาม การกระทำความผิดที่รัฐนำหลักการนี้มาปรับใช้ ต้องเป็นความผิดที่มีความร้ายแรงเพียงพอ อาทิ การล่วงละเมิดทางเพศต่อผู้เยาว์ เป็นต้น ส่วน หลักสัญชาติผู้กระทำความผิดนั้น จะเป็นกรณีที่รัฐกล่าวอ้างเขตอำนาจเหนือความผิดที่กระทำโดยคนชาติของตน[66]

สำหรับหลักสากล รัฐมีอำนาจศาลในการดำเนินคดีและลงโทษผู้กระทำความผิดได้โดยไม่ต้องคำนึงถึงสถานที่ที่ความผิดเกิดขึ้นหรือสัญชาติของบุคคลที่มีความเกี่ยวข้องกับการกระทำความผิด หลักสากลจะถูกหยิบยกขึ้นมาใช้สำหรับความผิดร้ายแรงบางชนิดที่กฎหมายจารีตประเพณีระหว่างประเทศหรือสนธิสัญญาระหว่างประเทศได้กำหนดไว้ อาทิ การกระทำอันเป็นโจรสลัด อาชญากรรมสงคราม หรือการฆ่าล้างเผ่าพันธุ์ เป็นต้น ความผิดเหล่านี้ถือว่าเป็นความผิดที่ส่งผลกระทบต่อความสงบเรียบร้อยและความมั่นคงของประชาคมระหว่างประเทศโดยรวม รัฐต่างๆจึงถือได้ว่าเป็นผู้มีส่วนเกี่ยวข้องได้เสียกับความผิดที่เกิดขึ้นเหมือนกันทั้งหมด

Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/2079repInternetJurisdictionrik1a%20_Mar09.pdf [2013, May 7], pp.8-9

[66] *Ibid*., p.10

จากหลักการกล่าวอ้างเขตอำนาจทั้งสามประการดังข้างต้น หลักดินแดนจะเป็นหลักทั่วไป ส่วนหลักบุคคลและหลักสากลเป็นเพียงข้อยกเว้นของหลักดินแดนเท่านั้น ที่เป็นเช่นนี้เพราะ สถานที่ที่เกิดเหตุนั้นย่อมได้รับผลกระทบจากการกระทำความผิดมากกว่าสถานที่อื่นๆ อีกทั้งการพิสูจน์ความผิดและรวบรวมพยานหลักฐานจากสถานที่เกิดเหตุก็เป็นไปได้ง่ายกว่าด้วย

- **หลักความเฉพาะเจาะจง** (rule of specialty) ภายใต้หลักกฎหมายนี้ รัฐผู้ร้องขอความร่วมมือจะต้องไม่ดำเนินคดีกับบุคคลผู้ถูกส่งตัวผู้ร้ายข้ามแดนในฐานความผิดอื่นๆ นอกเหนือคำร้องขอ และจะต้องไม่ส่งตัวบุคคลผู้นั้นไปยังรัฐที่สามโดยรัฐผู้รับคำขอไม่ยินยอม มิฉะนั้น รัฐผู้รับคำขอมีสิทธิประท้วงได้[67] จะเห็นได้ว่าหลักความเฉพาะเจาะจงนี้มีรากฐานมาจากหลักความยินยอม เพราะการให้ความยินยอมของรัฐผู้ส่งตัวข้ามแดนนั้นพิจารณาจากเนื้อหาในคำขอส่งตัวผู้ร้ายข้ามแดนเป็นสำคัญ รัฐผู้ส่งคำขอส่งตัวผู้ร้ายข้ามแดนต้องไม่กระทำการเกินความยินยอมที่ตนได้รับมาได้

อย่างไรก็ตาม มีข้อยกเว้นของหลักกฎหมายนี้ในบางกรณี ได้แก่ กรณีที่บุคคลตามคำขอได้เดินทางออกจากรัฐผู้ร้องขอภายหลังกระบวนการการส่งตัวผู้ร้ายข้ามแดนและกลับเดินทางเข้าไปในรัฐนั้นอีกโดยสมัครใจ กรณีที่การกระทำความผิดตามคำขอนั้นเป็นความผิดที่มีฐานความผิดอื่นๆปะปนอยู่ด้วย รัฐที่ร้องขอสามารถดำเนินคดีตามฐานความผิดอื่นๆที่ปะปนอยู่ในความผิดตามคำขอได้

- **หลักเกี่ยวกับความผิดที่ไม่สามารถให้ความช่วยเหลือได้** ความผิดที่ไม่สามารถส่งตัวผู้ร้ายข้ามแดนได้นั้น เป็นผลมาจากหนึ่งในปัจจัยสามประการ คือปัจจัยด้านบุคคลที่ถูกขอให้ส่งตัวข้ามแดน ปัจจัยด้านความผิดตามคำขอส่งตัวผู้ร้ายข้ามแดน และปัจจัยที่มาจากเหตุเฉพาะคดีที่อยู่ในคำร้องขอให้ส่งตัวผู้ร้ายข้ามแดน

กรณีที่เหตุแห่งบุคคลส่งผลให้ส่งตัวผู้ร้ายข้ามแดนไม่ได้มีอยู่สองกรณี คือกรณีที่บุคคลตามคำขอนั้นมีเอกสิทธิ์และความคุ้มกันทางการทูตตามกฎหมายระหว่างประเทศ

---

[67] Sir Robert Jennings and Sir Arthur Watts, eds. Oppenheim's International Law Vol. 1 (Essex :Longman Group U.K. Limited, 1992), p.961

หรือกรณีที่บุคคลตามคำขอนั้นเป็นคนชาติของผู้รับคำขอ เพราะรัฐผู้เป็นเจ้าของสัญชาติย่อมมีหน้าที่ปกป้องคนชาติของตน[68] อย่างไรก็ตาม ถ้าหากรัฐปฏิเสธคำขอส่งตัวผู้ร้ายข้ามแดนด้วยเหตุที่บุคคลนั้นเป็นคนชาติของตน รัฐนั้นมีหน้าที่ต้องดำเนินคดีต่อบุคคลที่ถูกขอให้ส่งตัวแทนรัฐผู้ร้องขอ ทั้งนี้เป็นไปตามหลักกฎหมาย Aut Dedere Aut Judicare ซึ่งแปลว่า หากไม่ส่งตัวข้ามแดนก็ต้องดำเนินคดีแทน

ในกรณีเหตุแห่งความผิดตามคำร้องขอนั้น โดยทั่วไปแล้วประเทศต่างๆ จะไม่ส่งตัวผู้ที่กระทำความผิดทางการเมือง เพราะหากกระทำการเช่นนั้นจะเป็นการแทรกแซงกิจการภายในของรัฐ ซึ่งนับเป็นการละเมิดอำนาจอธิปไตยตามกฎหมายระหว่างประเทศของรัฐอื่น ทั้งนี้ รัฐผู้รับคำขอเป็นผู้มีสิทธิ์ขาดในการวินิจฉัยว่าความผิดตามคำขอเป็นความผิดทางการเมืองหรือไม่ ซึ่งมักจะพิจารณากันเป็นรายคดีไป ความผิดทางการเมืองนี้ยังรวมไปถึงความผิดที่เกี่ยวเนื่องกับความผิดทางการเมือง (Related political offense) อีกด้วย

นอกจากนี้ รัฐผู้รับคำร้องขออาจไม่ส่งตัวผู้ร้ายข้ามแดนในความผิดที่ไม่ได้ระบุไว้ในสนธิสัญญาที่เกี่ยวข้องได้ เนื่องจากตนไม่มีพันธะกรณีตามกฎหมาย รัฐผู้รับคำร้องขอยังปฏิเสธการส่งตัวได้หากคำร้องขอมีสาเหตุมาจากเชื้อชาติ ศาสนา หรือความคิดเห็นทางการเมืองของบุคคลที่ถูกร้องขอให้ส่งตัวข้ามแดน[69] ข้อยกเว้นประการนี้ มีรากฐานมาจากกฎหมายสิทธิมนุษยชนระหว่างประเทศที่ห้ามไม่ให้รัฐดำเนินการเลือกปฏิบัติต่อคนในรัฐของตน โดยอาศัยเหตุแห่งเชื้อชาติ ศาสนา หรือความคิดเห็นทางการเมือง ดังที่จะเห็นได้จากตราสารระหว่างประเทศด้านสิทธิมนุษยชนฉบับต่างๆ เช่น ข้อ 2 ของปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights หรือ UDHR)[70] หรือ ข้อ 2 วรรค 1 ของกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิ

---

[68] สุผานิต มั่นศุข, กฎหมายระหว่างประเทศแผนกคดีอาญา, หน้า 163-165

[69] เรื่องเดียวกัน, หน้า 166-168

[70] Universal Declaration of Human Rights, Article 2:

Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. Furthermore, no distinction shall be made on the basis of the

ทางการเมือง[71] (International Covenant on Civil and Political Rights หรือ ICCPR) เป็นต้น

เหตุเฉพาะที่ทำให้ไม่สามารถส่งตัวผู้ร้ายข้ามแดนนั้น ได้แก่ กรณีที่ความผิดที่ถูกร้องขอมาเป็นความผิดที่ศาลของรัฐผู้รับคำขอได้พิจารณาพิพากษาผู้กระทำความผิดไปแล้ว ซึ่งเป็นไปตามหลักกฎหมายไม่พิจารณาลงโทษซ้ำสำหรับการกระทำเดียวกัน (Ne Bis In Idem) นอกจากนี้ รัฐผู้รับคำขอจะไม่สามารถส่งตัวผู้ร้ายข้ามแดนได้ในคดีที่หมดอายุความแล้ว อย่างไรก็ดี หากอายุความตามกฎหมายภายของรัฐผู้ร้องขอและรัฐผู้รับคำขอมีระยะเวลาไม่เท่ากัน ในทางปฏิบัติรัฐจะต้องปฏิบัติตามรายละเอียดที่ระบุในสนธิสัญญาที่เกี่ยวข้องแทน[72] จะเห็นได้ว่าทั้งหมดนี้เป็นไปตามหลักกฎหมายอาญาทั่วไปทั้งสิ้น

2.2.2.2 กระบวนการส่งตัวผู้ร้ายข้ามแดน

กระบวนการการส่งตัวผู้ร้ายข้ามแดนรูปแบบทั่วไปมีอยู่สามขั้นตอน โดยขั้นเริ่มแรกสุดจะเป็นการตรวจสอบความถูกต้องตามแบบของคำขอ โดยฝ่ายรัฐผู้ร้องขอจะส่งคำขอให้ดำเนินการส่งตัวผู้ร้ายข้ามแดนไปยังกระทรวงการต่างประเทศของรัฐผู้รับคำขอผ่านช่องทางทางการทูต (Diplomatic Channel) เพื่อให้อีกฝ่ายตรวจสอบความถูกต้องตามแบบของคำร้องขอ หลังจากนั้นในขั้นตอนที่สอง ฝ่ายรัฐผู้รับคำขอจะตรวจสอบความถูกต้องตามกฎหมายว่า ความผิดตามที่ร้องขอมานั้นสามารถส่งตัวผู้ร้ายข้ามแดนได้หรือไม่ ในขั้นตอนสุดท้าย ฝ่ายรัฐผู้รับคำร้องขอ

---

political, jurisdictional or international status of the country or territory to which a person belongs, whether it be independent, trust, non-self-governing or under any other limitation of sovereignty.

[71] International Covenant on Civil and Political Rights, Article 2:

1. Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

[72] Sir Robert Jennings and Sir Arthur Watts, eds. Oppenheim's International Law Vol. 1, p.962v

จะใช้ดุลยพินิจเพิ่มเติมโดยพิจารณาปัจจัยที่ไม่ใช่ข้อกฎหมาย อาทิ นโยบายของรัฐ ความสัมพันธ์ระหว่างประเทศ และผลประโยชน์ของรัฐ เป็นต้น[73]

หน่วยงานของรัฐผู้รับคำร้องขอที่รับผิดชอบในการการส่งตัวผู้ร้ายข้ามจะแแตกต่างไปตามวิธีปฏิบัติของแต่ละรัฐ โดยทั่วไปแล้ว รัฐมนตรีกระทรวงการต่างประเทศจะมีหน้าที่วินิจฉัยความถูกต้องตามแบบของคำร้องขอ แต่ในด้านการวินิจฉัยข้อกฎหมายนั้น รัฐบางรัฐ เช่น ฝรั่งเศส จะมอบหมายหน้าที่ให้กับรัฐมนตรีว่าการกระทรวงยุติธรรม ในขณะที่รัฐบางรัฐ เช่น ประเทศอังกฤษและสหรัฐอเมริกา จะมอบหมายให้ฝ่ายตุลาการจะเป็นผู้พิจารณาตามข้อกฎหมาย สำหรับการใช้ดุลยพินิจที่ไม่เกี่ยวกับข้อกฎหมายนั้น รัฐบางรัฐเช่น ประเทศเบลเยี่ยม ประเทศเนเธอร์แลนด์ และประเทศไทย จะกำหนดให้รัฐมนตรีว่าการกระทรวงยุติธรรมเป็นผู้มีหน้าที่รับผิดชอบ ในขณะที่รัฐบางรัฐ จะให้รัฐมนตรีว่าการกระทรวงการต่างประเทศเป็นผู้ทำหน้าที่แทน[74]

นอกเหนือจากกระบวนการข้างต้น ข้อตกลงส่งตัวผู้ร้ายข้ามแดนบางฉบับยังรองรับการการส่งตัวผู้ร้ายข้ามแดนแบบรวบรัดด้วย โดยบุคคลตามคำขอ จะแสดงยินยอมสละสิทธิของตน ที่จะได้รับกระบวนการพิจารณาส่งตัวผู้ร้ายข้ามแดน รวมทั้งข้อกำหนดหรือสิทธิอื่นๆที่ตนพึงได้รับตามกฎหมายภายใน หรือสนธิสัญญาการส่งตัวผู้ร้ายข้ามแดน โดยความยินยอมดังกล่าวมีลักษณะที่เพิกถอนไม่ได้ (Irrevocable consent) [75] สิทธิที่สละดังกล่าวได้แก่ สิทธิที่จะโต้แย้งว่า ความผิดตามคำร้องขอนั้น ไม่ใช่ความผิดที่สามารถส่งตัวข้ามแดนได้ เป็นต้น

ในทางปฏิบัติ รัฐบางรัฐอาจให้บุคคลตามคำขอนั้นลงชื่อให้ความยินยอมต่อหน้าศาล[76] เพื่อให้แน่ใจว่า บุคคลนั้นทราบถึงรายละเอียดเกี่ยวกับสิทธิของตนอย่างครบถ้วนและได้สมัครใจที่จะสละสิทธิ์ดังข้างต้น อย่างไรก็ตาม ความยินยอมดังข้างต้นนั้น อาจเพิกถอนได้ในสถานการณ์

---

[73] ตะวัน พึ่งพุทธารักษ์, “ปัญหาการส่งผู้ร้ายข้ามแดนในคดีอาญากรรมคอมพิวเตอร์”, p.23-25

[74] เรื่องเดียวกัน. p.23-25

[75] พรชัย ด่านวิวัฒน์, กฎหมายอาญาระหว่างประเทศ (กรุงเทพฯ : วิญญูชน, 2551), หน้า 60

[76] Tadashi Morishita, “Some Proposals for the Improvement of Extradition Among the ASEAN Countries”, Paper presented at the 4th ACPF Meetings, Held in Bangkok, Thailand,15-17 November 1995.

พิเศษบางประเภท อาทิ เมื่อมีการเปลี่ยนแปลงรัฐบาลของรัฐผู้ร้องขอใหม่ หรือมีหลักฐานที่น่าเชื่อถือว่า บุคคลตามคำขอนั้น อาจไม่ถูกดำเนินคดีโดยยุติธรรม เป็นต้น ทั้งนี้ ฝ่ายบริหารจะยังคงเป็นผู้ใช้ดุลยพินิจในการส่งตัวผู้ร้ายข้ามแดนในขั้นสุดท้าย[77]

การส่งตัวผู้ร้ายข้ามแดนการให้ความยินยอมนี้ จะยังตกอยู่ภายใต้หลักเกณฑ์ Rule of Specialty อย่างเคร่งครัด[78] เพื่อคุ้มครองสิทธิของบุคคลที่ให้ความยินยอมของตนเพียงเพื่อไปต่อสู้คดีใดคดีหนึ่งโดยเฉพาะ นอกจากนี้ ยังเป็นการเคารพสิทธิของรัฐที่ได้รับการร้องขอว่าได้ใช้ดุลยพินิจอนุญาตให้ส่งตัวผู้ร้ายข้ามแดนเฉพาะในฐานความผิดดังกล่าวตามสนธิสัญญาหรือกฎหมายภายในของตนเท่านั้น ตัวอย่างของของกระบวนการส่งตัวผู้ร้ายข้ามแดนด้วยความยินยอม สามารถเห็นได้จากกฎหมายภายในของออสเตรเลีย มาเลเซีย ฟิจิ และสนธิสัญญาส่งตัวผู้ร้ายข้ามแดนระหว่าง ออสเตรเลียและอินโดนีเซีย ออสเตรเลียและฟิลิปปินส์ เกาหลีและไทย อินเดียและเกาหลี เป็นต้น[79]

ระบบกฎหมายภายในของบางรัฐ ยังได้กำหนดการส่งตัวผู้ร้ายข้ามแดนแบบรวบรัดอีกวิธีหนึ่ง ซึ่งก็คือการรับรองหมายศาล ในกรณีนี้ รัฐผู้ร้องคำขอจะส่งหมายจับบุคคลที่ต้องการให้ส่งตัวผู้ร้ายข้ามแดนไปยังรัฐผู้รับคำขอ หลังจากนั้นฝ่ายเจ้าหน้าที่รัฐฝ่ายตุลาการของรัฐผู้รับคำร้องขอจะรับรองหมายศาลดังกล่าว ส่งผลให้รัฐผู้รับคำร้องขอสามารถดำเนินการตามหมายจับได้เหมือนกับว่าหมายศาลนั้นถูกออกภายในรัฐของตนเอง เมื่อบุคคลตามคำขอถูกนำตัวมาที่ศาลแล้ว ศาลจะพิจารณาเงื่อนไขที่เกี่ยวข้องอาทิ บุคคลที่ถูกจับกุมเป็นบุคคลตามหมายศาลนั้นจริงหรือไม่ ซึ่งถ้าเป็นไปตามเงื่อนไขดังกล่าวแล้ว บุคคลนั้นก็จะถูกส่งตัวไปยังรัฐผู้ร้องขอ อย่างไรก็ตาม การดำเนินการด้วยวิธีนี้ มิได้มีฐานทางกฎหมายมาจากสนธิสัญญาระหว่างประเทศแต่อย่างใด และใช้ระหว่างประเทศที่มีระบบกฎหมายใกล้เคียงกันเท่านั้น[80] ตัวอย่างประเทศ

---

[77] พรชัย ด่านวิวัฒน์, กฎหมายอาญาระหว่างประเทศ, p.59

[78] เรื่องเดียวกัน, p. 60

[79] ADB/OECD anti-corruption initiative for Asia and the Pacific, Mutual legal assistance , extradition and recovery of proceeds of corruption in Asia and Pacific, p.74

[80] *Ibid*., p.50

ที่ใช้วิธีการรับรองหมายศาลสามารถพบได้จากการส่งตัวผู้ร้ายข้ามแดนระหว่าง มาเลเซียและสิงคโปร์ หรือประเทศหมู่เกาะในมหาสมุทรแปซิฟิคเช่น ฟิจิ ปาปัวนิวกินี และวานูอาตู เป็นต้น[81]

2.2.3 การให้ความช่วยเหลือซึ่งกันและกันทางกฎหมาย

การให้ความช่วยเหลือซึ่งกันและทางกฎหมาย จะมีขึ้นในกรณีที่รัฐเกิดความเสียหายขึ้นได้ร้องขอให้รัฐอีกรัฐหนึ่งช่วยดำเนินการรวบรวมพยานหลักฐานต่างๆที่จำเป็นต่อการดำเนินคดีอาทิ การสอบพยานบุคคล การส่งพยานบุคคล พยานวัตถุ[82] หรือการให้ความช่วยเหลือด้านเอกสารต่างๆ[83] จะเห็นได้ว่า การให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายนี้ มีความเกี่ยวพันกับการใช้อำนาจฝ่ายบริหารของรัฐเช่นกัน อย่างไรก็ดี การให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายจะส่งผลกระทบต่ออำนาจอธิปไตยของรัฐผู้รับคำร้องขอน้อยกว่า เพราะยังไม่มีการนำตัวบุคคลออกไปนอกดินแดนของรัฐ ซึ่งจะทำให้บุคคลนั้นพ้นไปจากอำนาจอธิปไตยของรัฐผู้รับคำร้องขอแต่อย่างใด

2.2.3.1 หลักกฎหมายเกี่ยวกับการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมาย

หลักกฎหมายส่วนใหญ่เกี่ยวกับการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายจะคล้ายคลึงกันกับการส่งตัวผู้ร้ายข้ามแดน อย่างไรก็ดี เนื่องจากการให้ความช่วยเหลือทางอาญาระหว่างประเทศลักษณะนี้ รุกล้ำอำนาจอธิปไตยน้อยกว่าการส่งตัวผู้ร้ายข้ามแดน ข้อตกลงเกี่ยวกับการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายในปัจจุบัน จึงได้พยายามผ่อนปรนหลักฐานความผิดตรงกันลงไปเพื่อให้รัฐช่วยเหลือกันได้สะดวกมากขึ้นเช่นกัน[84] นอกจากนี้การให้ความช่วยเหลือร่วมกันทางกฎหมายจะมีหลักการจำกัดการใช้ (limitation of uses)นั้นจะคล้ายกับหลักเฉพาะเจาะจงในการส่งตัวผู้ร้ายข้ามแดน[85]

---

[81] *Ibid*., p.50

[82] European Convention on International Mutual Legal Assistance 1950, Art.3

[83] *Ibid*., Art. 13, Para. 1,2

[84] ADB/OECD anti-corruption initiative for Asia and the Pacific, Mutual legal assistance , extradition and recovery of proceeds of corruption in Asia and Pacific. p.42

[85] *Ibid*., p.49

เหตุแห่งการปฏิเสธไม่ให้ความช่วยเหลือร่วมกันทางกฎหมายนั้น รัฐผู้รับคำร้องขอสามารถปฏิเสธการให้ความช่วยเหลือได้ในกรณีความผิดทางการเมือง ความผิดทางทหาร หรือกรณีที่คำขอมีลักษณะละเมิดต่อรัฐธรรมนูญหรือขัดต่อกฎหมายภายในของประเทศผู้รับคำร้องขอ เพราะย่อมส่งผลกระทบต่ออำนาจอธิปไตยของรัฐผู้รับคำร้องขอ นอกจากนี้รัฐที่รับคำขอความร่วมมือทางอาญาระหว่างประเทศอาจจะปฏิเสธการให้ความช่วยเหลือได้หากตนกำลังสืบสวนหรือดำเนินคดีเดียวกันในชั้นศาลได้ ทั้งนี้ รัฐผู้รับคำขอเป็นผู้มีดุลยพินิจในการวินิจฉัยว่าตนจะดำเนินการให้ความช่วยเหลือหรือไม่ จะสังเกตเห็นได้ว่าการให้ความช่วยเหลือจะต้องเป็นไปตามหลักนิติรัฐ กล่าวคือต้องอยู่ภายในขอบเขตของข้อตกลงระหว่างประเทศที่เกี่ยวข้องและกฎหมายภายในของรัฐผู้รับคำขอเช่นกัน

2.2.3.2 **กระบวนการสำหรับการให้การช่วยเหลือซึ่งกันและกันทางกฎหมาย**

การให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายสามารถทำได้สามรูปแบบ ได้แก่ การใช้หนังสือส่งประเด็นสืบพยาน (Letter Rogatory) ซึ่งเป็นวิธีการแบบดั้งเดิม การใช้ดำเนินการผ่านทางหน่วยงานกลาง และการติดต่อระหว่างหน่วยงานผู้บังคับใช้กฎหมายโดยตรง

การใช้หนังสือส่งประเด็นสืบพยานเป็นการขอความช่วยเหลือซึ่งกันและกันทางกฎหมายระหว่างผู้พิพากษาของรัฐทั้งสองฝ่าย โดยฝ่ายรัฐผู้ให้ความช่วยเหลือจะแบกรับค่าใช้จ่ายสำหรับดำเนินการตามคำขอนั้นเอง[86] กระบวนนี้มีที่มาจากหลักไมตรีจิตระหว่างรัฐและมีจุดมุ่งหมายให้ผู้พิพากษารัฐต่างๆให้ความช่วยเหลือซึ่งกันและกัน ในการดำเนินการผู้พิพากษาก็จะออกหนังสือส่งประเด็นสืบพยานให้กับตำรวจหรืออัยการเพื่อรวบรวมหลักฐานในคดีอาญาด้วย อย่างไรก็ตาม วิธีการนี้มักเป็นเพียงการให้ความช่วยเหลือทางเอกสารหรือคำให้การของพยานเท่านั้น โดยเฉพาะอย่างยิ่งในกรณีที่รัฐผู้ถูกร้องขอเป็นรัฐ common law ที่ผู้พิพากษาไม่เข้าไปเกี่ยวข้องในการสืบสวนคดี

---

[86] สุผานิต มั่นศุข, กฎหมายระหว่างประเทศแผนกคดีอาญา,หน้า 215

นอกจากนี้ หนังสือส่งประเด็นสืบพยานยังมีความล่าช้ามาก[87] เพราะจะดำเนินการผ่านช่องทางการทูต (Diplomatic Channel) ซึ่ง หนังสือส่งประเด็นสืบพยาน จะถูกส่งไปยังเจ้าหน้าที่ทางการทูตของรัฐตนเพื่อส่งต่อคำขอไปยังเจ้าหน้าที่ทางการทูตของผู้รับคำร้องขอต่อไป หลังจากนั้น เจ้าหน้าที่ทางการทูตของฝ่ายรัฐผู้ร้องขอจะส่งผ่านคำขอไปยังหน่วยงานผู้บังคับใช้กฎหมายหรือเจ้าหน้าที่ฝ่ายอัยการเพื่อจัดการตามคำขอนั้น เมื่อดำเนินการต่างๆแล้ว หลักฐานต่างๆที่ได้ตามคำขอนี้ก็จะถูกส่งกลับไปด้วยช่องทางการทูตเช่นกัน ปัญหาความล่าช้าอาจมีเพิ่มขึ้นอีกหากเจ้าหน้าที่ทางการทูตที่เกี่ยวข้องมีกำลังคนไม่เพียงพอหรือมีภาระหน้าที่จำนวนมาก[88]

เพื่อเป็นการแก้ไขปัญหาที่เกิดจากการส่งหนังสือประเด็นสืบพยาน ข้อตกลงด้านการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายในปัจจุบัน จึงตั้งหน่วยงานกลาง (Central Authority) ขึ้นมาเพื่อส่งหรือดำเนินการตามคำขอนั้น โดยทั่วไปนั้น หน่วยงานกลางจะตั้งอยู่ในกระทรวงการยุติธรรมหรือสำนักงานอัยการสูงสุด การติดต่อกันสื่อสารโดยตรงระหว่างหน่วยงานกลางลดความล่าช้าได้เพราะฝ่ายรัฐผู้ร้องขอความร่วมมือสามารถระบุจุดติดต่อได้อย่างแน่นอน และหน่วยงานกลางจะสามารถทราบถึงหน่วยงานที่สามารถจัดการตามคำขอด้วย และหากหน่วยงานกลางเป็นหน่วยงานที่สามารถบังคับใช้กฎหมายได้โดยตรง คำขอความช่วยเหลือจะถูกจัดการอย่างรวดเร็วขึ้นไปอีก นอกจากนี้ หน่วยงานกลางยังสามารถเฝ้าติดตามผลการส่งและจัดการตามคำขอได้ด้วย[89]

ในทางปฏิบัติ หน่วยงานกลางบางแห่งก็จะมี web site เป็นภาษาต่างประเทศที่ใช้กันกว้างขวางและสามารถให้ข้อมูลที่สำคัญบางประการได้ อาทิ ข้อกฎหมายหรือสนธิสัญญาที่เกี่ยวข้องกับการขอความช่วยเหลือ ตัวอย่างคำขอ รายละเอียดการให้ความช่วยเหลือและรายละเอียดการติดต่อหน่วยงาน เป็นต้น นอกจากนี้ หน่วยงานกลางยังสามารถให้คำปรึกษาด้านการให้ความช่วยเหลือได้ทั้งประเด็นทางเทคนิคและประเด็นข้อกฎหมาย[90] อย่างไรก็ตาม

---

[87] ADB/OECD anti-corruption initiative for Asia and the Pacific, Mutual legal assistance , extradition and recovery of proceeds of corruption in Asia and Pacific,p.33-34

[88] *Ibid*., p.63

[89] *Ibid*., p.64-65

[90] *Ibid*., p.65

ถ้าหน่วยงานกลางไม่มีทรัพยากรเพียงพอ คำขอก็อาจจะล่าช้าลง นอกจากนี้ บางประเทศก็อาจจะตั้งหน่วยงานกลางที่แตกต่างกันออกไปตามคดีต่างๆส่งผลให้เกิดความสับสนในการติดต่อและเกิดความทับซ้อนในการประสานงานและติดต่องานเพิ่มขึ้น[91]

การติดต่อสื่อสารระหว่างหน่วยงานผู้บังคับใช้กฎหมายโดยตรง เป็นกรณีที่อัยการหรือหน่วยงานผู้สืบสวนคดีของรัฐผู้ร้องขอความช่วยเหลือจะส่งคำขอไปยังหน่วยงานที่เทียบเท่าในรัฐผู้ร้องขอ วิธีนี้จะเป็นวิธีการติดต่อที่รวดเร็วที่สุด แต่ปัญหาก็อาจจะเกิดได้ ถ้าประเทศผู้รับคำร้องขอมีหน่วยงานผู้บังคับใช้กฎหมายที่หลากหลาย ทำให้เกิดความกระจัดกระจายในการให้ความช่วยเหลือและขาดแหล่งรวมทรัพยากรและผู้เชี่ยวชาญ[92]

2.2.4 อุปสรรคจากการปรับใช้ความร่วมมือทางอาญาระหว่างประเทศทั่วไปกับบริบทของอาชญากรรมทางคอมพิวเตอร์

เมื่อพิจารณาจากเงื่อนไขและกระบวนการของการส่งตัวผู้ร้ายข้ามแดนและการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายแล้ว จะพบว่าการปรับใช้กลไกความร่วมมือทางอาญาระหว่างประเทศทั่วไปกับอาชญากรรมทางคอมพิวเตอร์นั้น ยังคงมีอุปสรรคอยู่หลายประการ โดยสาเหตุของอุปสรรคดังกล่าวจะมีที่มาจากปัจจัยด้านกฎหมายภายในประเทศและกฎหมายระหว่างประเทศ

2.2.4.1 อุปสรรคจากกฎหมายภายในประเทศ

ดังที่ได้กล่าวไว้เกี่ยวกับข้อท้าทายเชิงกฎหมายของอาชญากรรมทางคอมพิวเตอร์ อาชญากรรมประเภทนี้ไม่เพียงแต่ทำให้รัฐต้องให้ความร่วมมือทางอาญาระหว่างกันเท่านั้น หากแต่ยังผลักดันให้รัฐต่างๆต้องปรับปรุงกฎหมายภายในรัฐทั้งในด้านกฎหมายสารบัญญัติและกฎหมายวิธีสบัญญัติด้วย เพราะฉะนั้น หากกฎหมายภายในของรัฐที่เกี่ยวข้องไม่สามารถรองรับอาชญากรรมทางคอมพิวเตอร์ได้แล้วการให้ความร่วมมือทางอาญาระหว่างประเทศย่อมประสบปัญหาตามไปด้วย

---

[91] *Ibid*., p 66

[92] *Ibid*., p.66

ในด้านกฎหมายสารบัญญัติ หากรัฐไม่ได้กำหนดให้อาชญากรรมทางคอมพิวเตอร์เป็นความผิดตามกฎหมายอาญาของตนแล้ว รัฐผู้รับคำขอความร่วมมือทางอาญาจะไม่สามารถให้ความร่วมมือได้ เพราะไม่ตรงตามเงื่อนไขเรื่องฐานความผิดตรงกัน และการนำกฎหมายอาญาทั่วไปมาปรับใช้แทนก็ก่อให้เกิดอุปสรรคในการตีความให้รองรับอาชญากรรมทางคอมพิวเตอร์ที่เกิดได้ ด้วยปัญหาเหล่านี้ ผู้กระทำความผิดจึงสามารถจะอาศัยรัฐที่ขาดแคลนกฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์เป็นสถานที่กระทำความผิดและแหล่งหลบภัย (Safe Haven) ได้

ตัวอย่างของปัญหาการขาดแคลนกฎหมายสารบัญญัตินี้ สามารถเห็นได้จากกรณีของ ไวรัสคอมพิวเตอร์ I love you ในปี 2000 ซึ่งสร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์จำนวนมหาศาลทั่วโลก ในภายหลังหน่วยงานสืบสวนกลางสหรัฐ (Federal Bureau of Investigation หรือ FBI) ได้พยายามติดตามร่องรอยของผู้กระทำผิด จนสามารถระบุตัวผู้กระทำผิดได้และทราบว่าผู้ต้องสงสัยรายนี้อาศัยอยู่ในประเทศฟิลิปปินส์ อย่างไรก็ตามในขณะนั้นในประเทศฟิลิปปินส์ยังมิได้มีกฎหมายภายในว่าด้วยอาชญากรรมทางคอมพิวเตอร์แต่อย่างใด จึงเกิดอุปสรรคในการขอหมายศาลจากศาลฟิลิปินส์เพื่อค้นที่อยู่ผู้ต้องสงสัยเพื่อแสวงหาหลักฐานในการสร้างและเผยแพร่ไวรัสคอมพิวเตอร์ หลังจากนั้น เมื่อสามารถจับกุมผู้ต้องสงสัยได้แล้ว ฝ่ายเจ้าหน้าที่รัฐก็ไม่สามารถตั้งข้อหาที่เหมาะสมได้เนื่องจากขาดแคลนกฎหมายภายใน ในการนี้ทางการของประเทศฟิลิปปินส์ได้พยายามนำข้อหาที่ใกล้เคียงที่สุดมาปรับใช้ โดยตั้งข้อหาว่าผู้กระทำผิดนั้นได้ทำความผิดฐานกลฉ้อฉลและขโมยบัตรเครดิต เพราะไวรัสที่ถูกสร้างขึ้นได้รวบรวมรหัสผ่านของผู้ใช้คอมพิวเตอร์ไว้ ซึ่งผู้กระทำผิดสามารถนำไปใช้บริการทางอินเตอร์เน็ตหรือแสวงหาสิ่งมีค่าอื่นๆ ได้โดยมิชอบ อย่างไรก็ตามศาลฟิลิปปินส์ได้ปฏิเสธข้อหาดังกล่าวเพราะขาดฐานทางกฎหมายเพียงพอ ส่งผลให้ฟิลิปปินส์ไม่สามารถดำเนินคดีต่อผู้กระทำความผิดอีกทั้งยังไม่สามารถส่งตัวผู้กระทำความผิดข้ามแดนไปยังรัฐอื่นที่ได้รับความเสียหายด้วย

ในขณะเดียวกัน การที่รัฐต่างๆมีทั้งปูมหลังจากสภาพสังคม วัฒนธรรม วิถีชีวิตและประวัติศาสตร์ ไม่เหมือนกัน ส่งผลให้บางรัฐจึงไม่การกระทำบางประการไม่เป็นความผิดทางกฎหมายอาญาของตน ยกตัวอย่างเช่น ประเทศอเมริกาจะไม่มีกฎหมายห้ามการแสดงความเห็นก่อความเกลียดชังทางทางเชื้อชาติไว้ เนื่องจากเห็นว่าอยู่ในขอบเขตของเสรีภาพในการแสดง

ความคิดเห็น ยกเว้นเฉพาะกรณีที่ก่อความเสียหายอย่างร้ายแรง หรือมีแนวโน้มที่จะส่งเสริมให้เกิดความไม่สงบขึ้นในสังคมอย่างฉับพลัน[93] ในทางกลับกัน ประเทศส่วนใหญ่ที่อยู่ในภูมิภาคยุโรปจะกำหนดให้การเผยแพร่ข้อความเหยียดหยามเชื้อชาติเป็นการกระทำความผิดทางอาญา โดยเฉพาะอย่างยิ่งในกรณีที่ข้อความดังกล่าวเกี่ยวข้องกับลัทธินาซี[94] นอกจากนี้ ในประเด็นเรื่องสิ่งลามกอนาจาร รัฐบางรัฐเห็นว่าสิ่งลามกอนาจารที่ไม่ใช่เด็กสามารถมีได้ตามกฎหมาย หากแต่ต้องป้องกันไม่ให้ผู้ชมอายุต่ำกว่ากฎหมายเข้าถึงได้ ในทางกลับกัน รัฐอีกจำนวนหนึ่งจะห้ามสิ่งลามกอนาจารอย่างเด็ดขาด

สำหรับกฎหมายวิธีสบัญญัตินั้น รัฐที่เกี่ยวข้องกับการให้ความร่วมมือทางอาญานั้นอาจประสบปัญหาขาดแคลนทั้งมาตรการทางวิธีสบัญญัติที่เหมาะสมแก่การสืบสวนคดีอาชญากรรมทางคอมพิวเตอร์ และทรัพยากรต่างๆสำหรับดำเนินการที่เกี่ยวข้อง[95] เมื่อหลักฐานในคดีอาชญากรรมทางคอมพิวเตอร์ส่วนใหญ่อยู่ในรูปแบบข้อมูลทางอิเล็กทรอนิกส์ ไม่มีลักษณะทางกายภาพ ไม่สามารถมองเห็นได้ด้วยตาเปล่า อีกทั้งยังง่ายต่อการลบทิ้ง ทำลาย หรือแก้ไขภายในระยะเวลาอันสั้น หากรัฐผู้รับคำขอความช่วยเหลือซึ่งกันและกันทางกฎหมายขาดความสามารถในการรวบรวมและค้นหาหลักฐานเหล่านี้ได้อย่างทันท่วงทีแล้ว ผู้กระทำความผิดก็อาจจะทำลายหลักฐานทั้งหมดได้

นอกจากนี้ ถึงแม้รัฐที่เกี่ยวข้องในการให้ความร่วมมือทางอาญาจะมีกฎหมายภายในที่คล้ายคลึงกัน และสามารถรองรับอาชญากรรมทางคอมพิวเตอร์ได้ก็ตาม การให้ความร่วมมือทางอาญาระหว่างประเทศยังคงสามารถเกิดอุปสรรคได้จากการที่รัฐมีแนวทางการตีความและปรับใช้กฎหมายแตกต่างกันไป ยกตัวอย่างเช่น ในประเด็นเรื่องสิ่งลามกอนาจาร รัฐต่างๆมีแนวทางที่แตกต่างกันในการตีความว่า สิ่งใดเข้าข่ายลามกอนาจารบ้าง[96] แม้แต่ในกรณี

---

[93] Barry Steinhardt, “Hate Speech,” in The internet, law, and society, eds. Yaman Akdeniz, Clive Walker and David Wall (London: Dorset Press, 2000), pp. 253-255

[94] ตะวัน พึ่งพุทธารักษ์, “ปัญหาการส่งผู้ร้ายข้ามแดนในคดีอาญากรรมคอมพิวเตอร์”, หน้า 69

[95] Amalie M. Weber, “The council of Europe’s convention on cybercrime,” Berkeley Technology Law Journal Annual Review of Law and Technology 18,425 (2003): 1

[96] John T. Soma, Thomas F. Muther, Jr. and Heidi M.L.Brisette, “Transnational extradition for computer crimes: Are new treaties and laws needed?,” Harvard Journal on Legislation 34,2 (1997): 340-341

สิ่งลามกอนาจารเด็ก ซึ่งรัฐต่างเห็นพ้องตรงกันว่าผิดกฎหมายนั้น รัฐยังคงมีความเห็นต่างกันว่า ภาพเสมือนจริง ภาพที่ทำเทียมสิ่งลามกอนาจาร หรือวัตถุลามกอนาจารที่ปรากฏบุคคลที่สรีระหน้าตาคล้ายคลึงกับเด็ก แต่อายุสูงกว่าเกณฑ์ของเด็กนั้น จัดว่าเป็นสิ่งลามกอนาจารเด็กได้หรือไม่[97]

ความแตกต่างด้านการตีความและปรับใช้กฎหมายยังสามารถปรากฏได้ในกรณีที่ฐานความผิดไม่มีความเกี่ยวข้องกับวัฒนธรรมแต่อย่างใด ยกตัวอย่างเช่น ในความผิดฐานการเข้าสู่ระบบคอมพิวเตอร์โดยผิดกฎหมาย ประเทศบางประเทศ เช่นเยอรมนี ออสเตรีย ญี่ปุ่น ไต้หวัน เห็นว่าการเจาะระบบคอมพิวเตอร์เพียงอย่างเดียว โดยไม่สร้างความหายอย่างอื่นต่อ ไม่ถือว่าเป็นความผิดทางอาญา ในขณะที่ประเทศอีกกลุ่มหนึ่ง อาทิ แคนาดา อังกฤษ และสหรัฐอเมริกา กลับมีความเห็นในทางตรงกันข้าม[98] ในประเทศกลุ่มที่สองนี้ ยังคงมีขอบเขตการบังคับใช้กฎหมายที่แตกต่างกันไปอีก ยกตัวอย่างเช่น ประเทศออสเตรเลีย จะกำหนดให้มีความผิดเฉพาะการเจาะระบบคอมพิวเตอร์ขององค์การหรือหน่วยงานของรัฐบาล ในขณะที่กฎหมายของประเทศอื่นๆ ไม่ได้จำกัดไว้ว่าระบบคอมพิวเตอร์ที่ถูกเข้าถึงโดยผิดกฎหมายนั้นว่าจะต้องเป็นของหน่วยงานใด[99] จะเห็นได้ว่า ในกรณีดังกล่าว รัฐที่เกี่ยวข้องกับการให้ความร่วมมือทางอาญาจะไม่สามารถดำเนินการได้ถ้าแนวทางการตีความและปรับใช้กฎหมายไม่เหมือนกัน เพราะความผิดที่เกิดขึ้นไม่ได้เป็นไปตามหลักกฎหมายว่าด้วยฐานความผิดตรงกัน (dual criminality)

2.2.4.2 **อุปสรรคจากกฎหมายระหว่างประเทศ**

แม้รัฐที่เกี่ยวข้องในคดีอาชญากรรมทางคอมพิวเตอร์ จะมีกฎหมายสารบัญญัติและกฎหมายวิธีสบัญญัติที่รองรับอาชญาคอมพิวเตอร์ได้เพียงพอแล้ว การให้ความร่วมมือทางอาญาระหว่างประเทศยังเกิดอุปสรรคได้ หากข้อตกลงความร่วมมือทางอาญาระหว่างประเทศที่มีผลบังคับใช้ระหว่างสองฝ่ายนั้น ไม่ครอบคลุมถึงอาชญากรรมทางคอมพิวเตอร์แต่อย่างใด ในทางปฏิบัตินั้น ความร่วมมือทางอาญาระหว่างประเทศจะปรากฏอยู่ในรูปแบบของข้อตกลง

---

[97] ตะวัน พึ่งพุทธารักษ์, “ปัญหาการส่งผู้ร้ายข้ามแดนในคดีอาญากรรมคอมพิวเตอร์”, หน้า71-72

[98] เรื่องเดียวกัน, หน้า 73-74

[99] เรื่องเดียวกัน, หน้า 74-75

ระหว่างประเทศ รัฐต่างๆจึงมีพันธะกรณีผูกพันเฉพาะตามเนื้อหาที่ระบุไว้ในข้อตกลงตามหลักกฎหมาย สัญญาต้องเป็นสัญญา (Pacta Sunt Servanda) หากข้อตกลงระหว่างประเทศที่เกี่ยวข้อง ไม่กำหนดให้อาชญากรรมทางคอมพิวเตอร์เป็นความผิดที่สามารถส่งตัวผู้ร้ายข้ามแดนหรือให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายได้ รัฐผู้รับคำขอก็สามารถที่จะปฏิเสธไม่ให้ความร่วมมือทางอาญาที่ขอมาได้เช่นกัน[100]

กรณีตัวอย่างของประเด็นปัญหานี้ได้แก่ เหตุการณ์ในช่วงฤดูใบไม้ผลิ ค.ศ. 2000 ซึ่งมีผู้เจาะข้อมูล (hacker) บุกเข้าไปในระบบคอมพิวเตอร์ของธนาคารและบริษัทเครดิตการ์ดในประเทศสหรัฐอเมริกาจำนวนหลายแห่ง ผู้เจาะข้อมูลได้นำข้อมูลได้จากการเจาะข้อมูลไปขู่กรรโชกเอาเงินจากลูกค้าของบริษัทเหล่านั้น ในคดีนี้ ถึงแม้หน่วย FBI ของสหรัฐอเมริกาสามารถระบุตัวผู้ต้องสงสัยได้สองคน และทราบว่าผู้ต้องสงสัยทั้งสองอยู่ในประเทศรัสเซีย แต่ฝ่ายเจ้าหน้าที่ของรัสเซียก็ปฏิเสธที่จะให้ความร่วมมือกับ FBI เพราะสนธิสัญญาการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมาย (Mutual Legal Assistance Treaties หรือ MLATs) ที่รัสเซียทำกับสหรัฐอเมริกาไม่ได้มีเนื้อหาครอบคลุมถึงอาชญากรรมทางคอมพิวเตอร์แต่อย่างใด[101]

ในทางปฏิบัติ การจัดทำข้อตกลงความร่วมมือทางอาญาด้วยวิธีกำหนดอัตราโทษขั้นต่ำสามารถแก้ไขปัญหาดังข้างต้นได้ แต่อัตราโทษที่แตกต่างกันออกไปในแต่ละประเทศนั้นก็ยังคงสามารถสร้างอุปสรรคในการให้ความร่วมมือได้เช่นกัน[102]

เช่นเดียวกันกับปัญหาเกิดจากกฎหมายภายในรัฐ รัฐที่เกี่ยวข้องกับการให้ความร่วมมือทางอาญาระหว่างประเทศ ยังคงมีความแตกต่างกันในการปรับใช้กฎหมายในหลายประเด็น อาทิ การกล่าวอ้างเขตอำนาจรัฐ การตีความเรื่องความผิดทางการเมือง ซึ่งนับเป็นประเด็นที่ส่งผลกระทบต่ออำนาจอธิปไตยของรัฐเป็นพิเศษ

---

[100] Amalie M. Weber, “The council of Europe’s convention on cybercrime,” Berkeley Technology Law Journal Annual Review of Law and Technology 18,425:.2

[101] Robert Lemos, “Lawyers slam FBI ‘Hack’,” ZD Net News (1 May 2001) Available from: http://www.zdnetasia.com/lawyers-slam-fbi-hack-21200883.htm [2013, May 7]

[102] ตะวัน พึ่งพุทธารักษ์, “ปัญหาการส่งผู้ร้ายข้ามแดนในคดีอาญากรรมคอมพิวเตอร์”, หน้า 84-85

สำหรับกล่าวอ้างเขตอำนาจรัฐนั้น การอ้างเขตอำนาจของรัฐเหนือคดีอาชญากรรมทางคอมพิวเตอร์ในปัจจุบันจะยังคงจำกัดอยู่เฉพาะการอ้างเขตอำนาจตามหลักดินแดนหรือหลักบุคคล เป็นหลัก อย่างไรก็ตาม รายละเอียดในการอ้างเขตอำนาจตามหลักการดังกล่าวของรัฐต่างๆ ยังคงมีความแตกต่างกัน

ในกรณีการอ้างเขตอำนาจด้วยหลักดินแดน ถ้าหากอาชญากรรมทางคอมพิวเตอร์ที่เกิดไม่ได้เจาะจงไปยังคอมพิวเตอร์ปลายทางเครื่องใดเครื่องหนึ่ง ได้แก่ กรณีของการกระทำความผิดทางเนื้อหา เป็นต้น ก็จะเกิดปัญหาในการตีความว่าความผิดเกิดขึ้นที่ใด เพราะผู้ใช้คอมพิวเตอร์นั้นสามารถเข้าถึงระบบอินเตอร์เน็ตจากสถานที่ใดๆก็ได้ ในการนี้ รัฐบางรัฐ เช่น แคนาดา จะตีความว่า การที่ข้อความผิดกฎหมายปรากฏบนหน้าจอคอมพิวเตอร์ที่อยู่ในรัฐใดนั้น ไม่ได้ส่งผลให้รัฐดังกล่าวมีเขตอำนาจเหนือการกระทำความผิดแต่อย่างใด ในขณะที่รัฐบางรัฐกลับเห็นว่า ตนมีเขตอำนาจเหนือการกระทำความผิดแล้ว นอกจากนี้ ในกรณีที่อาชญากรรมทางคอมพิวเตอร์ที่เจาะจงไปยังระบบคอมพิวเตอร์ปลายทาง อาทิ การจารกรรมข้อมูลและกลฉ้อโกงทางคอมพิวเตอร์นั้น รัฐก็มีแนวทางการตีความที่แตกต่างกันออกไปเช่นกัน ยกตัวอย่างเช่น ศาลของสหรัฐอเมริกา วางหลักว่า สถานที่ความผิดเกิดขึ้นคือสถานที่ที่คอมพิวเตอร์ที่ถูกใช้เป็นเครื่องมือในการก่ออาชญากรรมตั้งอยู่ โดยไม่ต้องคำนึงว่าความผิดเกิดผลสำเร็จ ณ ที่ไหน ส่วนศาลของประเทศอังกฤษจะพิจารณาว่า การได้มาซึ่งทรัพย์สิน หรือข้อมูลอันเป็นผลที่ทำให้ความผิดสำเร็จนั้นเกิดขึ้นที่ใด[103]

สำหรับการอ้างเขตอำนาจด้วยหลักบุคคลนั้น ประเทศในกลุ่ม Civil Law จะยอมรับการกล่าวอ้างตามหลักดังกล่าวสำหรับคดีที่คนชาติของตนกระทำความผิดนอกดินแดน ในขณะที่ประเทศกลุ่ม Common Law มักจะลังเลที่จะยอมรับเขตอำนาจเหนือบุคคล นอกจากนี้ ในทางปฏิบัติ ข้อตกลงระหว่างประเทศด้านการให้ความร่วมมือกันทางอาญาก็กำหนดขอบเขตการกล่าวอ้างเขตอำนาจที่ต่างกันออกไปอีกด้วย[104]

---

[103] ตะวัน พึ่งพุทธารักษ์, “ปัญหาการส่งผู้ร้ายข้ามแดนในคดีอาญากรรมคอมพิวเตอร์”,หน้า 90-91

[104] เรื่องเดียวกัน, หน้า 91-95

ความแตกต่างในการกล่าวอ้างเขตอำนาจดังข้างต้น อาจก่อให้เกิดปัญหาการขัดกันของเขตอำนาจรัฐเชิงบวก (positive conflict of jurisdiction) ได้* ถ้าอาชญากรรมทางคอมพิวเตอร์ส่งผลกระทบต่อรัฐจำนวนมากในอาชญากรรมทางคอมพิวเตอร์เดียวกัน โดยรัฐผู้รับร้องขอความช่วยเหลือความร่วมมือจะเกิดความสับสนว่าจะต้องดำเนินการให้แก่รัฐใดก่อน เพื่อไม่ให้ดำเนินการซ้ำซ้อน ซึ่งจะเป็นการสิ้นเปลืองต่อเวลาและทรัพยากรได้

นอกจากนี้ รัฐต่างๆก็มีดุลยพินิจในการตีความและบังคับใช้หลักกฎหมายไม่พิจารณาลงโทษซ้ำสำหรับการกระทำเดียวกัน (Ne Bis In Idem) ที่แตกต่างกันว่าอาชญากรได้ถูกดำเนินคดีทางอาญาหรือลงโทษในการกระทำความผิดเดียวกันหรือไม่[105] อีกทั้งยังเกิดปัญหาในการพิจารณาและตีความตามข้อยกเว้นของหลักกฎหมาย Ne Bis In Idem สำหรับความผิดต่อความมั่นคงของรัฐ ซึ่งรัฐผู้รับความเสียหายสามารถลงโทษผู้กระทำผิดซ้ำอีกได้ ทั้งนี้แม้เป้าหมายของการกระทำความผิดจะเป็นระบบคอมพิวเตอร์ของราชการก็ตาม นั่นก็ไม่ได้หมายความว่าอาชญากรรมคอมพิวเตอร์ดังกล่าวเป็นความผิดต่อความมั่นคงรัฐเสมอไป ทั้งนี้จะต้องพิจารณาเจตนาและแรงจูงใจของอาชญากรเพิ่มเติมด้วย[106]

ในขณะเดียวกัน รัฐต่างๆยังประสบปัญหาการตีความเกี่ยวกับความผิดทางการเมือง ซึ่งรัฐจะมีแนวทางการตีความที่แตกต่างกันและไม่แน่นอน เพราะในปัจจุบันรัฐยังไม่ได้กำหนดนิยามของอาชญากรรมทางคอมพิวเตอร์ที่อาจถือเป็นความผิดทางการเมืองแต่อย่างใด[107] ยกตัวอย่างเช่นในกรณีศึกษาหนึ่งจากประเทศเอสโตเนีย ซึ่งได้ขอความร่วมมือจากองค์การตำรวจสากล(Interpol) ในคดีที่ผู้กระทำผิดได้ตีพิมพ์บทความทางอินเตอร์เน็ตที่มีเนื้อหาต่อต้าน

---

* ยังมีการขัดกันทางเขตอำนาจรัฐอีกรูปแบบหนึ่งเรียกว่า การขัดกันของเขตอำนาจรัฐเชิงลบ (negative conflict of jurisdiction) ซึ่งจะเป็นกรณีที่รัฐต่างๆ ที่เกี่ยวข้องกับการกระทำความผิด ไม่มีเขตอำนาจเหนือการกระทำความผิดที่เกิดขึ้นด้วยสาเหตุที่ตนไม่ได้กำหนดให้ความผิดที่เกิดขึ้นอยู่ภายใต้เขตอำนาจของตน ส่งผลให้ไม่มีฝ่ายใดสามารถดำเนินคดีและลงโทษผู้กระทำความผิดได้

[105] ตะวัน พึ่งพุทธารักษ์, “ปัญหาการส่งผู้ร้ายข้ามแดนในคดีอาญากรรมคอมพิวเตอร์”, หน้า 96-97

[106] เรื่องเดียวกัน, หน้า 97-98

[107] เรื่องเดียวกัน, หน้า 102-103

ประเทศเอสโตเนีย แต่กลับถูก Interpol ปฏิเสธโดยเหตุที่ว่าความผิดที่เกิดขึ้นเป็นความผิดทางการเมือง[108]

2.3 การพัฒนากลไกความร่วมมือทางอาญาระหว่างประเทศสำหรับอาชญากรรมทางคอมพิวเตอร์ในช่วงก่อนหน้าการจัดทำอนุสัญญากรุงบูดาเปสต์

จากเนื้อหาส่วนที่แล้ว จะพบว่ากลไกเกี่ยวกับความร่วมมือทางอาญาระหว่างประเทศทั่วไปนั้นยังไม่เพียงพอแก่การตอบสนองอาชญากรรมทางคอมพิวเตอร์ โดยอุปสรรคที่เกิดขึ้นนั้นเป็นผลมาจากการที่กลไกความร่วมมือทางอาญาระหว่างประเทศทั่วไปนั้น ถูกจัดทำขึ้นมาสำหรับคดีความผิดทางอาญาทั่วไปทุกประเภท ไม่ได้ครอบคลุมอาชญากรรมทางคอมพิวเตอร์โดยเฉพาะเจาะจงแต่อย่างใด รัฐผู้เกี่ยวข้องกับการให้ความร่วมมือบางส่วนจึงยังคงขาดแคลนกฎหมายสารบัญญัติหรือกฎหมายวิธีสบัญญัติด้านอาชญากรรมทางคอมพิวเตอร์ในระดับภายในรัฐ อีกทั้งประสบปัญหาการขาดแคลนข้อตกลงด้านความร่วมมือทางอาญาที่ครอบคลุมอาชญากรรมทางคอมพิวเตอร์ในระดับระหว่างประเทศด้วย นอกจากนี้ ความแตกต่างด้านการตีความและปรับใช้กฎหมายที่เกี่ยวข้องทั้งในระดับภายในรัฐและระดับระหว่างประเทศยังก่ออุปสรรคในการให้ความร่วมมือระหว่างรัฐที่มีความพร้อมทางกฎหมายภายในอยู่แล้วเช่นเดียวกัน อุปสรรคเหล่านี้ได้ผลักดันให้องค์การระหว่างประเทศหลายแห่งพยายามดำเนินการพัฒนาให้ความร่วมมือทางอาญาระหว่างประเทศสามารถรองรับอาชญากรรมทางคอมพิวเตอร์ได้มากยิ่งขึ้น

เนื้อหาของวิทยานิพนธ์ส่วนนี้ จะอธิบายรายละเอียดของความพยายามดังกล่าวที่มีขึ้นก่อนหน้าการจัดทำอนุสัญญากรุงบูดาเปสต์ อีกทั้งยังจะประเมินผลลัพธ์ว่า ความพยายามเหล่านี้มีบทบาทและอุปสรรคในการรองรับอาชญากรรมทางคอมพิวเตอร์อย่างไรบ้าง

---

[108] Pedro Verdelho. The effectiveness of international co-operation against cybercrime: examples of good practice [online]. Strasbourg: Council of Europe, Directorate general of human rights and legal affairs, Economic crime division, 2008. Available from: http://www.coe.int/t/dghl/standardsetting/t-cy/T-CY%20%282008%29%20DOC%20The%20effectiveness%20of%20international%20co-operation%20against%20cybercrime%20examples%20of%20good%20practice%20E.PDF [2013, May 6],, p. 26

2.3.1 ความร่วมมือทางอาญาระหว่างประเทศสำหรับอาชญากรรมทางคอมพิวเตอร์ในช่วงก่อนหน้าการจัดทำอนุสัญญากรุงบูดาเปสต์

ก่อนหน้าที่อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์หรืออนุสัญญากรุงบูดาเปสต์จะเปิดให้ลงนามในวันที่ 23 พฤศจิกายน ปี 2001 นั้น องค์การระหว่างประเทศต่างๆ อาทิ องค์การตำรวจสากล (Interpol) องค์การ กลุ่มประเทศที่พัฒนาแล้วทางอุตสาหกรรม 8 ประเทศ (G8) เพื่อความร่วมมือทางเศรษฐกิจและด้านการพัฒนา (OECD) และสภายุโรป ได้พยายามแก้ไขปัญหาที่เกิดจากการปรับใช้กลไกความร่วมมือทางอาญาระหว่างประเทศในคดีอาชญากรรมทางคอมพิวเตอร์ แก่บรรดารัฐสมาชิกด้วยการกำหนดคำแนะนำและแนวทาง (guideline) ต่างๆ ความพยายามดังกล่าวนี้จะให้ความสำคัญแก่การพัฒนากฎหมายภายในเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ และการกำหนดกรอบความร่วมมือระหว่างประเทศให้ครอบคลุมอาชญากรรมทางคอมพิวเตอร์ รายละเอียดมีดังต่อไปนี้

2.3.1.1 การดำเนินการภายใต้กรอบขององค์การตำรวจสากล (Interpol)[109]

ภายในงานสัมมนาสำหรับการฝึกผู้สืบสวนคดีอาชญากรรมทางคอมพิวเตอร์ในวันที่ 7-11 ธันวาคม 1981 องค์การตำรวจสากลได้สรุปคำตอบของแบบสอบถามที่ตนได้ส่งไปยังบรรดารัฐสมาชิกว่า กฎหมายอาญาของประเทศสมาชิกยังไม่ครอบคลุมการกระทำดังต่อไปนี้

- การดัดแปลงหรือการลบข้อมูล หรือการกระทำอื่นๆที่ส่งผลกระทบต่อการประมวลผลข้อมูล โดยที่ผู้กระทำการดังข้างต้นมีเจตนาในการทำลายข้อมูลนั้น
- การได้มาซึ่งข้อมูลของผู้อื่น โดยที่ผู้กระทำการมีเจตนาที่จะแสวงหาประโยชน์ให้กับตน
- การเข้าใช้บริการทางคอมพิวเตอร์หรือคอมพิวเตอร์ของผู้อื่นโดยที่ไม่ได้รับอนุญาตเพื่อจุดประสงค์ส่วนตน
- การดัดแปลงข้อมูลด้วยเจตนาฉ้อฉล หรือด้วยเจตนาที่จะนำข้อมูลที่ถูกดัดแปลงไปทำธุรกรรมทางกฎหมาย

---

[109] Stein Schjolberg. The history of global harmonization on cybercrimelLegislation-The Road to Geneva [Online]. 2008. Available from: http://www.cybercrimelaw.net/documents/cybercrime_history.pdf. [2013, May 7] p.3

- การเปิดเผยข้อมูลโดยที่ปราศจากอำนาจ

2.3.1.2 คำแนะนำขององค์การเพื่อความร่วมมือทางเศรษฐกิจและด้านการพัฒนา (Organization for Economic Co-operation and Development หรือ OECD) ในปี 1986[110]

ภายใต้คำแนะนำดังฉบับนี้ คณะกรรรมการด้านข้อมูล การสื่อสาร และนโยบายคอมพิวเตอร์ (Committee on Information, Communication, and Computer Policy หรือ ICCP) ขององค์การเพื่อความร่วมมือทางเศรษฐกิจและด้านการพัฒนาหรือ OECD ได้กำหนดรายการของการกระทำที่เป็นอาชญากรรมทางคอมพิวเตอร์ดังต่อไปนี้

- การใส่ข้อมูล ดัดแปลง ลบทิ้ง หรือระงับยับยั้งการใช้งานข้อมูลทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์โดยเจตนา และเป็นไปเพื่อโอนเงินหรือสิ่งมีค่าอื่นโดยผิดกฎหมาย
- การใส่ข้อมูล ดัดแปลง ลบทิ้งหรือระงับยับยั้งการใช้งานข้อมูลทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์โดยเจตนา และเป็นไปเพื่อทำการปลอมแปลง
- การใส่ข้อมูล ดัดแปลง ลบทิ้ง หรือระงับการใช้งานข้อมูลทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือการแทรกแซงระบบคอมพิวเตอร์ด้วยวิธีการอื่นๆ โดยผู้กระทำผิดกระทำการโดยเจตนาและมุ่งหมายที่จะขัดขวางการทำงานของระบบคอมพิวเตอร์หรือระบบทางโทรคมนาคม
- การละเมิดสิทธิเฉพาะตนของผู้เป็นเจ้าของโปรแกรมทางคอมพิวเตอร์ที่ได้รับการปกป้องตามกฎหมายทรัพย์สินทางปัญญา โดยผู้กระทำผิดมีเจตนานำโปรแกรมคอมพิวเตอร์ดังกล่าวไปใช้ประโยชน์ทางการค้า และวางตลาดโปรแกรมคอมพิวเตอร์ดังกล่าว
- การเข้าถึงหรือดักรับข้อมูลคอมพิวเตอร์หรือระบบโทรคมนาคมด้วยเจตนาทุจริตหรือประสงค์ที่จะก่อความเสียหาย โดยที่ผู้กระทำผิดทราบว่าตนดำเนินการไป

---

[110] Computer-related criminality: Analysis of Legal Politics in the OECD Area (1986) Cited in: Stein Schjolberg. The history of global harmonization on cybercrimelLegislation-The Road to Geneva, p. 6,fn.23

โดยไม่ได้รับอนุญาตจากบุคคลผู้มีหน้าที่รับผิดชอบต่อระบบนั้น และได้ละเมิดระบบรักษาความปลอดภัยเพื่อการดังกล่าว

จะเห็นได้ว่า คำแนะนำของ OECD นั้นจะมีเป้าหมายให้รัฐภาคีพยายามแก้ไขกฎหมายภายในของตนโดยชัดเจนกว่าความพยายามที่มีอยู่ก่อนหน้าของ Interpol ซึ่งจะมีลักษณะเป็นการรายงานข้อมูลเสียมากกว่า

นอกจากนี้ ในด้านของความผิดที่เกี่ยวข้องกับคอมพิวเตอร์ คำแนะนำของ OECD จะเพิ่มเติมความผิดฐานการฉ้อโกงทางคอมพิวเตอร์เพิ่มไปจากการปลอมแปลงทางคอมพิวเตอร์ ดังที่ปรากฏอยู่ในแบบสอบถามขององค์การตำรวจสากล นอกจากนี้ คำแนะนำของ OECD ในปี 1986 ยังได้เพิ่มเติมความผิดต่อทรัพย์สินทางปัญญาขึ้นมาด้วย หากแต่จะครอบคลุมเพียงโปรแกรมคอมพิวเตอร์เท่านั้น ไม่ได้รวมไปถึงทรัพย์สินทางปัญญาประเภทอื่นๆ แต่อย่างใด

2.3.1.3 **คำแนะนำของสภายุโรปในปี** 1989

ในวันที่ 13 กันยายน 1989 สภายุโรปได้รับรองคำแนะนำว่าด้วยการกระทำที่เป็นอาชญากรรมทางคอมพิวเตอร์ หมายเลข R 89 (9) ซึ่งจะแนะนำให้รัฐสมาชิกทบทวนกฎหมายด้านอาชญากรรมทางคอมพิวเตอร์ของตนที่มีอยู่แล้ว หรือจัดทำกฎหมายใหม่ด้านอาชญากรรมทางคอมพิวเตอร์ โดยให้นำข้อมูลจากรายงานของคณะกรรมการด้านปัญหาอาชญากรรมของสภายุโรป (European Committee on Crime Problems) ว่าด้วยอาชญากรรมทางคอมพิวเตอร์มาพิจารณาประกอบด้วย โดยเฉพาะอย่างยิ่งในส่วนคำแนะนำด้านการบัญญัติกฎหมายของรายงานดังกล่าว ทั้งนี้ ให้รัฐรายงานความคืบหน้าเกี่ยวกับกฎหมายภายในของตน วิธีปฏิบัติทางกฎหมาย และประสบการณ์ด้านการให้ความร่วมมือด้านอาชญากรรมทางคอมพิวเตอร์ต่อเลขาธิการสภายุโรปในปี 1993[111]

ฐานความผิดภายใต้คำแนะนำฉบับนี้ จะแบ่งออกเป็นสองส่วน ส่วนแรกคือ Minimum list ซึ่งจะเป็นรายการของการกระทำความผิดที่รัฐสมาชิกของสภายุโรปควรที่จะนำไปกำหนด

---

[111] Computer-related Crime: Recommendation No. R (89) 9 , adopted by the Committee of Ministers of the Council of Europe on 13 September 1989

เป็นความผิดทางอาญา ได้แก่ การฉ้อโกง ทางคอมพิวเตอร์ การปลอมแปลงทางคอมพิวเตอร์ การสร้างความเสียหายให้แก่ข้อมูลคอมพิวเตอร์หรือโปรแกรมทางคอมพิวเตอร์ ,การก่อวินาศกรรมทางคอมพิวเตอร์ การเข้าสู่ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต การดักรับข้อมูลโดยปราศจากสิทธิตามกฎหมาย การทำซ้ำโปรแกรมคอมพิวเตอร์ที่ได้รับการปกป้องตามกฎหมายโดยที่ผู้กระทำไม่ได้รับอนุญาต และการทำซ้ำซึ่งผังวงจรรวม (Topography) โดยที่ผู้กระทำไม่ได้รับอนุญาต จะเห็นได้ว่า คำแนะนำของสภายุโรปปี 1989 จะมีการความผิดกำหนดฐานการเข้าสู่ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต และความผิดฐานการก่อวินาศกรรมทางคอมพิวเตอร์ซึ่งนับเป็นการแทรกแซงระบบ (system interference) และความผิดฐานการทำซ้ำซึ่งแผงวงจรรวมเข้ามาด้วย เมื่อเปรียบเทียบกับคำแนะนำของ OECD ในปี 1986

เนื้อหาส่วนที่สองคือ Optional list ซึ่งเป็นส่วนที่แนะนำให้รัฐสมาชิกนำประเด็นเกี่ยวกับการกระทำความผิดในรายการนี้ไปพิจารณาสำหรับการจัดทำกฎหมายใหม่ การกระทำตาม Optional list นี้ได้แก่ การดัดแปลงข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์โดยไม่ได้รับอนุญาต การจารกรรมทางคอมพิวเตอร์ การใช้คอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์โดยไม่ได้รับอนุญาต และการใช้โปรแกรมคอมพิวเตอร์ที่ได้รับการปกป้องสิทธิโดยไม่ได้รับอนุญาต คำแนะนำของสภายุโรปปี 1989 มีการกำหนดฐานความผิดฐานการจารกรรมข้อมูลเพิ่มเข้ามา ความผิดฐานการใช้คอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์โดยไม่ได้รับอนุญาต, การใช้โปรแกรมคอมพิวเตอร์ที่ได้รับการปกป้องสิทธิโดยไม่ได้รับอนุญาต เพิ่มเติมขึ้นมาจากคำแนะนำของ OECD ในปี 1986 การกำหนดรายการอาชญากรรมทางคอมพิวเตอร์ออกมาเป็น Optional List นี้ แสดงให้เห็นว่า รัฐยังมีความเห็นที่แตกต่างกันเกี่ยวกับการกำหนดฐานความผิดบางประเภท

น่าสังเกตว่า คำแนะนำของสภายุโรปในปี 1989 ยังไม่ได้ครอบคลุมถึงความผิดที่เกี่ยวข้องกับเนื้อหาแต่เพียงอย่างใด และถึงแม้จะมีการกล่าวถึงถึงความผิดต่อทรัพย์สินทางปัญญามากขึ้น ทรัพย์สินทางปัญญาที่คำแนะนำฉบับนี้ครอบคลุมจะยังคงจำกัดอยู่เพียงโปรแกรมคอมพิวเตอร์และแผงวงจรรวมเท่านั้น

2.3.1.4 **คำแนะนำของสภายุโรปในปี** 1995[112]

คำแนะนำของสภายุโรปในปี 1995 ได้วางหลักการเกี่ยวกับปัญหาทางกฎหมายวิธีพิจารณาความอาญาที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศไว้ในภาคผนวก โดยเนื้อหาจะแบ่งออกเป็น 7 บทดังต่อไปนี้

1. การค้นและยึด
2.การเฝ้าระวังทางเทคนิค (Technical Surveillance)
3.พันธะกรณีในการให้ความร่วมมือกับหน่วยงานผู้สืบสวน
4. หลักฐานทางอิเล็กทรอนิกส์
5. การเข้ารหัส
6. การวิจัย การบันทึกสถิติและการฝึกอบรม
7.ความร่วมมือระหว่างประเทศ

สำหรับการใช้อำนาจการค้นและการยึด คำแนะนำของสภายุโรปเห็นว่าอำนาจสืบสวนเหล่านี้ควรมีฐานทางกฎหมายวิธีพิจารณาความทางอาญารองรับและต้องเป็นไปตามเงื่อนไขเช่นเดียวกับการค้นและยึดทั่วไป โดยฝ่ายเจ้าหน้าที่รัฐต้องมีการแจ้งไปยังผู้ดูแลระบบถึงการค้นที่เกิดขึ้นและประเภทข้อมูลที่จะยึด อีกทั้งมีการเยียวยาตามกฎหมาย และถ้าหากข้อมูลที่ผ่านการประมวลผลโดยอัตโนมัติทำหน้าที่เป็นเช่นเดียวกับเอกสาร ให้นำหลักกฎหมายเรื่องการค้นและยึดเอกสารมาปรับใช้ สำหรับกรณีเร่งด่วนนั้น หน่วยงานผู้ทำการสืบสวนควรมีอำนาจที่จะขยายการค้นไปยังระบบคอมพิวเตอร์อื่นที่เชื่อมต่อกับระบบคอมพิวเตอร์ที่ค้นอยู่พร้อมทั้งยึดข้อมูลคอมพิวเตอร์ภายในได้ อย่างไรก็ตาม ระบบคอมพิวเตอร์ที่ถูกขยายการค้นนั้นจะต้องอยู่ภายในเขตอำนาจรัฐเดียวกัน และต้องมีมาตรการป้องกันที่เหมาะสมประกอบด้วย

คำแนะนำของสภายุโรปในปี 1995 ได้แนะนำให้มีการทบทวนแก้ไขกฎหมายที่เกี่ยวข้องกับการเฝ้าระวังทางเทคนิคสำหรับการสืบสวนคดีอาญา อาทิ การดักรับการสื่อสาร

---

[112] Council of Europe: Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law connected with Information Technology, adopted by the Committee of Ministers on 11 September 1995.

ทางโทรคมนาคม เพื่อให้รองรับบริบทของเทคโนโลยีสารสนเทศด้วย โดยหน่วยงานผู้สืบสวนควรมีอำนาจรวบรวมข้อมูลจราจรในการสืบสวนคดีอาญา โดยข้อมูลที่ถูกเก็บรวมรวมได้จากการดักรับนั้นควรถูกเก็บไว้ในสภาพที่ปลอดภัย ด้วยวิธีการที่เหมาะสม นอกจากนี้ เจ้าหน้าที่รัฐควรมีอำนาจดักรับข้อมูลโทรคมนาคมและรวบรวมข้อมูลจราจร ในคดีความผิดร้ายแรงที่กระทำต่อความลับ ความสมบูรณ์ และความพร้อมใช้งานของระบบคอมพิวเตอร์หรือระบบโทรคมนาคม โดยได้รับความร่วมมือจากผู้ให้บริการเครือข่ายอินเตอร์เน็ต

คำแนะนำปี 1995 ของสภายุโรปยังได้แนะนำให้รัฐให้อำนาจแก่เจ้าหน้าที่รัฐเพื่อสั่งการให้บุคคลส่งมอบข้อมูลภายในระบบคอมพิวเตอร์ของตนตามที่เจ้าหน้าที่ได้ระบุไว้ หรือให้ข้อมูลที่จำเป็นต่อการเข้าถึงระบบคอมพิวเตอร์และข้อมูลที่อยู่ภายใน โดยการใช้อำนาจต้องอยู่ภายในกรอบของสิทธิพิเศษและการป้องกันทางกฎหมาย นอกจากนี้ เจ้าหน้าที่รัฐควรมีอำนาจสั่งการให้บุคคลผู้มีความรู้ด้านการทำงานของเครื่องคอมพิวเตอร์และมาตรการรักษาความภัยสำหรับข้อมูลในเครื่องคอมพิวเตอร์เพื่อให้ความร่วมมือได้ ในขณะเดียวกัน ผู้ให้บริการควรหน้าที่ให้ข้อมูลสำหรับระบุตัวผู้ใช้งานเมื่อได้รับคำสั่งจากหน่วยงานรัฐผู้สืบสวนคดีด้วย

สำหรับหลักฐานทางอิเล็กทรอนิกส์นั้น คำแนะนำปี 1995 ของสภายุโรปแนะนำให้รัฐดำเนินการพัฒนากระบวนการและมาตรการทางเทคนิคในการดูแลหลักฐานอิเล็กทรอนิกส์ ไม่ว่าจะเป็นการรวบรวม เก็บรักษา และนำเสนอหลักฐาน เพื่อให้หลักฐานเหล่านั้นคงความสมบูรณ์และเชื่อถือได้ อีกทั้งยังเป็นไปโดยสอดคล้องกันกับกระบวนการและมาตรการของรัฐอื่นๆ โดยให้นำบทบัญญัติทางกฎหมายวิธีพิจารณาความทางอาญาว่าด้วยหลักฐานที่เป็นเอกสารมาปรับใช้กับข้อมูลที่อยู่ในระบบคอมพิวเตอร์ด้วย

ในด้านการพัฒนาขีดความสามารถของฝ่ายเจ้าหน้าที่รัฐนั้น คำแนะนำของสภายุโรปในปี 1995 ได้แนะนำให้รัฐพัฒนามาตรการเพื่อลดความเสียหายจากระบบการเข้ารหัสที่มีต่อการสืบสวนคดีอาชญากรรม โดยที่ไม่ให้ส่งผลกระทบต่อผู้ใช้งานที่ถูกกฎหมายจนเกินจำเป็น

นอกจากนี้ รัฐต่างๆควรดำเนินการประเมินความเสี่ยงในการก่ออาชญากรรมที่เกิดจากการพัฒนาและใช้งานเทคโนโลยีสารสนเทศอย่างต่อเนื่อง ในการนี้ รัฐต่างๆควรจะดำเนินการรวบรวมและวิเคราะห์ข้อมูลที่เกี่ยวข้องกับการกระทำความผิด อาทิ แนวทางดำเนินการ

ของผู้กระทำผิด และข้อมูลทางเทคนิค นอกจากนี้ รัฐต่างๆควรพิจารณาจัดตั้งหน่วยงานเฉพาะกิจที่มีความเชี่ยวชาญพิเศษด้านเทคโนโลยีข้อมูล และจัดโครงการฝึกอบรมให้บุคคลากรที่เกี่ยวข้อง

สำหรับการให้ความร่วมมือระหว่างประเทศนั้น คำแนะนำฉบับนี้ให้ความสำคัญแก่การขยายอำนาจการค้นข้อมูลไปยังระบบคอมพิวเตอร์ที่อยู่นอกเขตอำนาจรัฐ โดยชี้แนะให้รัฐต่างๆเจรจาจัดทำข้อตกลงระหว่างประเทศเพื่อเป็นฐานทางกฎหมายที่ชัดเจนสำหรับการค้นและยึดข้อมูลข้ามประเทศโดยที่ไม่ละเมิดอำนาจอธิปไตยของรัฐอื่นๆ โดยรัฐต่างๆต้องจัดเตรียมระบบการดำเนินงานและรับเรื่องที่รวดเร็วเพียงพอ เพื่อให้เจ้าหน้าที่รัฐสามารถรวบรวมหลักฐานได้ทันท่วงที ด้วยการเพิ่มเติมกลไกการให้ความช่วยเหลือทางกฎหมายให้ฝ่ายเจ้าหน้าที่รัฐผู้รับคำร้องขอความช่วยเหลือมีอำนาจต่างๆเพิ่มขึ้น อาทิ การค้นระบบคอมพิวเตอร์และยึดข้อมูลทางคอมพิวเตอร์ การจัดหาข้อมูลจราจรของการสื่อสารโทรคมนาคมที่ถูกระบุมา การดักรับหรือตามหาต้นตอของการสื่อสาร เป็นต้น

สภายุโรปได้แนะนำให้รัฐภาคีนำหลักการดังข้างต้นนี้ไปเป็นแนวทางในการทบทวนกฎหมายภายในและวิธีปฏิบัติที่เกี่ยวข้องของตน ในขณะเดียวกัน สภายุโรปยังได้แนะนำให้รัฐภาคีพยายามรับประกันให้หลักการเหล่านี้ถูกเผยแพร่ไปยังหน่วยงานรัฐผู้สืบสวนคดีอาญาและหน่วยงานผู้เชี่ยวชาญอื่นๆที่เกี่ยวข้อง โดยเฉพาะหน่วยงานด้านเทคโนโลยีสารสนเทศด้วย

2.3.1.5 **หลักการสิบข้อในการปราบปรามอาชญากรรมที่ใช้เทคโนโลยีขั้นสูงของกลุ่มประเทศทางอุตสาหกรรมที่พัฒนาแล้ว 8 ประเทศ** (G8)[113]

ระหว่างวันที่ 9-10 ธันวาคม ปี 1997 รัฐมนตรีกระทรวงยุติธรรมและกระทรวงมหาดไทยของประเทศกลุ่ม G8 ได้ประชุมกัน ณ กรุงวอชิงตัน ประเทศสหรัฐอเมริกา และได้ออกหนังสือแถลงการณ์ (Communique) ร่วมกันเกี่ยวกับอาชญากรรมที่ใช้เทคโนโลยีขั้นสูง (High Tech Crime) ภาคผนวกของ หนังสือแถลงการณ์ฉบับดังกล่าวได้วางหลักการเกี่ยวกับการปราบปรามอาชญากรรมที่ใช้เทคโนโลยีขั้นสูง 10 ข้อ รายละเอียดมีดังต่อไปนี้

---

[113] Meeting of the justice and interior ministers of the eight communiqué[Online].1997. Availble from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/points%20of%20contact/24%208%20Communique_en.pdf [2013, May 7]

I. จะต้องไม่มีสถานที่หลบภัยสำหรับผู้ที่นำเทคโนโลยีสารสนเทศไปสร้างความเสียหาย

II. จะต้องมีการประสานงานกันระหว่างรัฐในการสืบสวนและการดำเนินคดีอาชญากรรมที่เกี่ยวข้องกับเทคโนโลยีขั้นสูง ไม่ว่าอาชญากรรมจะกระทำขึ้น ณ ที่ใด

III. เจ้าหน้าที่ผู้บังคับใช้กฎหมายจะต้องได้รับการฝึกฝนและมีอุปกรณ์พร้อมในการรับมืออาชญากรรมที่เกี่ยวข้องกับเทคโนโลยีขั้นสูง

IV. ระบบกฎหมายต้องปกป้องกับความลับ ความสมบูรณ์และความพร้อมใช้ของข้อมูลและระบบไม่ให้ถูกทำให้เสียหายโดยปราศจากการอนุญาต อีกทั้งรับรองว่าการละเมิดสิทธิ์ดังกล่าวอย่างร้ายแรงจะมีโทษทางอาญา

V. ระบบกฎหมายควรอนุญาตให้มีการเก็บรักษาข้อมูลและการเข้าถึงข้อมูลอิเล็กทรอนิกส์อย่างรวดเร็ว เพราะความสำคัญต่อความสำเร็จการสืบสวนอาชญากรรม

VI. การให้ความช่วยเหลือซึ่งกันและกันทางกฎหมาย จะต้องมีกระบวนการรวบรวมและแลกเปลี่ยนหลักฐานอย่างทันสถานการณ์ในคดีที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยีขั้นสูง

VII. หน่วยงานผู้บังคับใช้กฎหมายควรเข้าถึงข้อมูลทางอิเล็กทรอนิกส์ที่เข้าถึงได้โดยสาธารณะ ในลักษณะข้ามประเทศได้ ไม่จำเป็นต้องได้รับการอนุญาตจากรัฐที่เป็นที่ตั้งของข้อมูลนั้น

VIII. ต้องมีการพัฒนาและการใช้มาตรฐานทางนิติเวชสำหรับการได้มาและตรวจสอบข้อมูลทางอิเล็กทรอนิกส์เพื่อนำไปใช้ในการสืบสวนและดำเนินคดีอาชญากรรม

IX. ระบบข้อมูลและ โทรคมนาคมควรที่จะได้รับการออกแบบเพื่อช่วยป้องกันและตรวจจับการละเมิดเครือข่ายให้มากที่สุดเท่าที่จะทำได้ และควรให้ความสะดวกในการตรวจจับสะกดรอยอาชญากรและรวบรวมหลักฐาน

X. การทำงานในประเด็นดังกล่าวนี้ควรจะมีการประสานงานกับเวทีทางระหว่างประเทศอื่นๆที่มีส่วนเกี่ยวข้องเพื่อที่จะรับรองได้ว่ามีการนำความพยายามต่างๆไปใช้

2.3.1.6 เครือข่ายจุดติดต่อตลอดเวลา (24/7 network) ของกลุ่มประเทศทางอุตสาหกรรมที่พัฒนาแล้ว 8 ประเทศ (G8)[114]

เครือข่ายนี้ถูกจัดตั้งขึ้นเมื่อปี 1998 โดยกลุ่มย่อยด้านอาชญากรรมทางเทคโนโลยีขั้นสูง ซึ่งอยู่ในสังกัดอยู่กลุ่มผู้เชี่ยวชาญอาวุโสด้านองค์การอาชญากรรมข้ามชาติประจำกลุ่ม G8 โดยมีรัฐผู้เข้าร่วมเครือข่ายทั้งจากภายในและภายนอกกลุ่ม G8 เครือข่ายจุดติดต่อตลอดเวลานี้จะประกอบไปด้วยผู้เชี่ยวชาญที่จะปฏิบัติหน้าที่ตลอดเวลาเพื่อให้ช่วยเหลือในการสืบสวนคดีอาชญากรรมทางคอมพิวเตอร์อย่างทันท่วงที และกำจัดประเทศที่หลบภัยของอาชญากรทางคอมพิวเตอร์ นอกจากนี้ เครือข่ายจุดติดต่อตลอดเวลายังสามารถสร้างความพร้อมทางด้านเทคนิคและมาตรการทางวิธีสบัญญัติ ในการติดตามจับกุมหาอาชญากรทางคอมพิวเตอร์มาดำเนินคดีด้วย

2.3.1.7 หลักการว่าด้วยการเข้าถึงข้อมูลคอมพิวเตอร์ที่ถูกเก็บไว้ในลักษณะข้ามแดน ของกลุ่มประเทศทางอุตสาหกรรมที่พัฒนาแล้ว 8 ประเทศ (G8) ในปี 1999[115]

หลักการว่าด้วยการเข้าถึงข้อมูลคอมพิวเตอร์ที่ถูกเก็บไว้ในลักษณะข้ามแดนนั้นจะปรากฏอยู่ในภาคผนวกของ Communique จากการประชุมของกลุ่ม G8 ในปี 1999 โดยเนื้อหาของหลักการจะกล่าวถึงการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายด้วยการเก็บรักษาข้อมูล การให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายอย่างรวดเร็ว และการเข้าถึงข้อมูลข้ามแดนได้โดยที่ไม่ต้องขอความช่วยเหลือจากรัฐอื่นที่เกี่ยวข้อง

สำหรับการเก็บรักษาข้อมูลนั้น รัฐควรมีความสามารถในการเก็บรักษาข้อมูลที่ถูกเก็บไว้ในระบบคอมพิวเตอร์อย่างรวดเร็ว โดยเฉพาะอย่างยิ่งในกรณีที่ผู้เก็บข้อมูลเป็นบุคคลภายนอก อย่างเช่น ผู้ให้บริการทางอินเตอร์เน็ต เพื่อเป็นการปกป้องให้ข้อมูลดังกล่าวสามารถเข้าถึง ค้นหา ทำสำเนา เปิดเผย หรือยึดได้ในภายหลัง อำนาจการเก็บรักษาข้อมูลอย่างรวดเร็วควรครอบคลุม

---

[114] VOA news report [Online]. 12 October 1997. Available from: http://www.fas.org/irp/news/1997/g-8_cyber_crime.htm [2013, May 7]

[115] Ministerial Conference of the G-8 Countries in Combating Transnational Organized Crime, Moscow October 19-20,1999, Annex 1.

ไปถึงข้อมูลที่ต้องถูกกักไว้ในระยะสั้นตามวิธีปฏิบัติ และข้อมูลที่เสี่ยงต่อการสูญหายหรือถูกดัดแปลงด้วย นอกจากนี้ รัฐต้องสามารถใช้อำนาจการเก็บรักษาข้อมูลเพื่อให้ความช่วยเหลือรัฐอื่นได้อีกด้วย โดยเมื่อมีการขอความช่วยเหลือให้เก็บรักษาข้อมูลอย่างรวดเร็ว รัฐผู้รับคำขอจะต้องเก็บรักษาข้อมูลตามคำขออย่างรวดเร็วโดยสอดคล้องกับกฎหมายภายในของตน ทั้งนี้ ระยะเวลาการเก็บรักษาข้อมูลจะต้องนานเพียงพอที่จะให้รัฐอีกฝ่ายสามารถทำคำขออย่างเป็นทางการ (formal request) อีกฉบับไปยังรัฐผู้รับคำขอ เพื่อขอดำเนินการค้นหา คัดลอก หรือเปิดเผยข้อมูลที่ถูกรักษาไว้ในภายหลัง

ในการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายนั้น เมื่อรัฐได้รับคำขออย่างเป็นทางการแล้ว ให้ดำเนินการตามคำขออย่างรวดเร็วที่สุดเท่าที่ทำได้ โดยให้เป็นไปตามกฎหมายภายในของตน นอกจากนี้ หลักการว่าด้วยการเข้าถึงข้อมูลคอมพิวเตอร์ที่ถูกเก็บไว้ในลักษณะข้ามแดนของกลุ่ม G8 จะอนุญาตให้รัฐทั้งสองฝ่ายอาศัยช่องทางการสื่อสารที่รวดเร็วและเชื่อถือได้ อาทิ โทรศัพท์ โทรสารหรือ จดหมายอิเล็กทรอนิกส์ เพื่อเพิ่มความยืดหยุ่นในการดำเนินการมากขึ้น นอกจากนี้ หากมีการร้องขอคำยืนยันเป็นลายลักษณ์อักษร อนุญาตให้รัฐส่งคำยืนยันนั้นไปภายหลังได้

หลักการว่าด้วยการเข้าถึงข้อมูลคอมพิวเตอร์ที่ถูกเก็บไว้ในลักษณะข้ามแดนของกลุ่ม G8 ยังได้กำหนดกรณีพิเศษที่ รัฐสามารถเข้าถึงข้อมูลที่อยู่ภายในดินแดนของอีกรัฐหนึ่งโดยไม่ต้องร้องขออีกฝ่ายไว้ในสองกรณี ได้แก่กรณีที่ข้อมูลดังกล่าวสามารถเข้าถึงได้เป็นการสาธารณะ (Open Source) และในกรณีที่รัฐผู้เข้าถึงข้อมูลได้รับความยินยอมโดยชอบด้วยกฎหมายจากผู้มีอำนาจเปิดเผยข้อมูลนั้น อย่างไรก็ดี ในกรณีหลังนั้น รัฐผู้เข้าถึงข้อมูลควรที่จะแจ้งให้รัฐอีกฝ่ายทราบ ถ้าหากการกระทำเช่นนั้นอยู่ภายในขอบเขตกฎหมายของตน และข้อมูลดังกล่าวนั้น ได้เปิดเผยให้เห็นการละเมิดกฎหมายภายในดินแดนของอีกฝ่ายหรืออาจเป็นประโยชน์ต่ออีกฝ่ายในทางใดทางหนึ่ง

2.3.2 การประเมินผลลัพธ์ของความพยายามด้านการพัฒนาความร่วมมือทางอาญาสำหรับอาชญากรรมทางคอมพิวเตอร์ในช่วงก่อนหน้าการจัดทำอนุสัญญากรุงบูดาเปสต์

เมื่อพิจารณาเนื้อหาของหลักการและคำแนะนำดังข้างต้นแล้ว ความพยายามด้านความร่วมมือทางอาญาสำหรับอาชญากรรมทางคอมพิวเตอร์ในช่วงก่อนหน้าการจัดทำอนุสัญญากรุงบูดาเปสต์นั้น สามารถส่งเสริมให้รัฐต่างๆพัฒนาความพร้อมด้านกฎหมายภายในของตนให้สามารถรองรับอาชญากรรมทางคอมพิวเตอร์ได้ อีกทั้งยังผลักดันให้การให้ความร่วมมือทางอาญาระหว่างประเทศของรัฐครอบคลุมอาชญากรรมทางคอมพิวเตอร์ด้วย อย่างไรก็ตาม ความพยายามต่างๆก่อนหน้าการจัดทำอนุสัญญาบูดาเปสต์เหล่านี้ยังคงมีข้อจำกัดอยู่เช่นเดียวกัน

ในด้านกฎหมายสารบัญญัตินั้น หลักการและคำแนะนำที่มีก่อนหน้าการจัดทำอนุสัญญากรุงบูดาเปสต์ ได้แนะนำให้รัฐกำหนดฐานความผิดสำหรับอาชญากรรมทางคอมพิวเตอร์ประเภทต่างๆ โดยจะครอบคลุมอาชญากรรมต่อความลับ ความสมบูรณ์ และความพร้อมใช้งานของข้อมูลและระบบคอมพิวเตอร์ ความผิดที่เกี่ยวข้องกับคอมพิวเตอร์ และความผิดต่อทรัพย์สินทางปัญญา

อย่างไรก็ตาม ความผิดต่อทรัพย์สินทางปัญญานั้น จะจำกัดอยู่เฉพาะความผิดที่กระทำต่อโปรแกรมทางคอมพิวเตอร์และแผงวงจรรวมเป็นสำคัญ หากแต่ไม่ครอบคลุมไปถึงผลงานอันมีลิขสิทธิ์ประเภทอื่นๆ อาทิ ภาพยนตร์ หรือเพลง ไปด้วย นอกจากนี้ ฐานความผิดตามหลักการและคำแนะนำที่มีขึ้นก่อนหน้าอนุสัญญากรุงบูดาเปสต์ยังไม่ครอบคลุมความผิดที่เกี่ยวข้องกับเนื้อหาด้วย เหตุผลที่เป็นเช่นนั้น เพราะเทคโนโลยีทางคอมพิวเตอร์ที่มีอยู่ในขณะที่จัดทำหลักการและคำแนะนำเหล่านั้น ยังไม่เอื้ออำนวยต่อการกระทำความผิดที่เกี่ยวข้องกับเนื้อหาหรือการละเมิดสิทธิเหนือทรัพย์สินทางปัญญาที่ไม่ใช่โปรแกรมทางคอมพิวเตอร์และแผงวงจรแต่อย่างใด

สำหรับด้านกฎหมายวิธีสบัญญัติ หลักการและคำแนะนำที่มีก่อนหน้าการจัดทำอนุสัญญากรุงบูดาเปสต์ได้สนับสนุนให้รัฐตระหนักถึงความสำคัญของหลักฐานที่เป็นข้อมูลทางอิเล็กทรอนิกส์ โดยแนะนำให้รัฐมีอำนาจการสืบสวนอาชญากรรมประเภทใหม่ๆ อาทิ การเก็บรักษาข้อมูลอย่างรวดเร็วเพื่อป้องกันไม่ให้หลักฐานในคดีอาชญากรรม

ทางคอมพิวเตอร์ได้ถูกดัดแปลงหรือทำลายโดยผู้กระทำผิด หรือการเฝ้าระวังทางเทคนิคเพื่อป้องกันและตรวจจับการกระทำความผิด เป็นต้น ในขณะเดียวกัน อำนาจการสืบสวนดั้งเดิม เช่น การค้น ได้รับการปรับปรุงให้สามารถขยายขอบเขตการค้นไปยังระบบคอมพิวเตอร์อื่นที่เชื่อมต่อกับระบบคอมพิวเตอร์ที่ค้นอยู่พร้อมทั้งยึดข้อมูลคอมพิวเตอร์ภายในได้ โดยระบบคอมพิวเตอร์ที่ถูกขยายการค้นนั้นจะต้องอยู่ภายในเขตอำนาจรัฐเดียวกัน จะเห็นได้ว่าความสามารถในการขยายขอบเขตการค้นนี้ สามารถลดเวลาในการดำเนินตามขั้นตอนที่กฎหมายกำหนด อาทิ การขอหมายศาลได้

หลักการและคำแนะนำที่มีขึ้นก่อนหน้าอนุสัญญากรุงบูดาเปสต์นั้น ได้กำหนดให้รัฐต่างๆ ใช้อำนาจสืบสวนอาชญากรรมทางคอมพิวเตอร์โดยอยู่ภายใต้มาตรการป้องกันทางกฎหมายด้วย ทั้งนี้เพื่อเป็นการสร้างความสมดุลระหว่างประสิทธิภาพในการสืบสวนอาชญากรรมและการปกป้องสิทธิมนุษยชนของผู้ใช้คอมพิวเตอร์ อย่างไรก็ดี มาตรการป้องกันทางกฎหมายที่หลักการและคำแนะนำก่อนหน้าอนุสัญญากรุงบูดาเปสต์กล่าวถึงนั้น จะหมายถึงมาตรการป้องกันทางกฎหมายตามกฎหมายภายในรัฐ การที่รัฐต่างๆมีแนวคิดด้านสิทธิมนุษยชนและกฎหมายแตกต่างกัน จึงส่งผลให้การปรับใช้อำนาจสืบสวนอาชญากรรมทางคอมพิวเตอร์ขาดความสอดคล้องกันได้

สำหรับด้านการให้ความร่วมมือระหว่างประเทศ หลักการและคำแนะนำก่อนหน้าอนุสัญญากรุงบูดาเปสต์นั้น ได้พยายามให้การให้ความร่วมมือทางอาญาสำหรับอาชญากรรมทางคอมพิวเตอร์เป็นไปอย่างรวดเร็วมากขึ้น ไม่ว่าจะเป็น การกำหนดช่องทางการติดต่อด้วยการใช้โทรศัพท์ โทรสาร จดหมายอิเล็กทรอนิกส์เพิ่มเติมไปจากเอกสารที่เป็นลายลักษณ์อักษร การจัดตั้งเครือข่ายจุดติดต่อตลอดเวลาเพื่อให้เจ้าหน้าที่ของรัฐสามารถติดต่อกันและตอบสนองต่อคำขอความร่วมมือทางอาญาระหว่างประเทศได้อย่างทันท่วงที ในขณะเดียวกัน หลักการและคำแนะนำก่อนหน้าอนุสัญญากรุงบูดาเปสต์ ยังอนุญาตให้หน่วยงานผู้บังคับใช้กฎหมายสามารถเข้าถึงข้อมูลหลักฐานที่ตั้งอยู่ในต่างประเทศได้โดยไม่ต้องติดต่อรัฐอีกรัฐหนึ่งก่อนถ้าหากข้อมูลนั้นสามารถเข้าถึงได้โดยสาธารณะ(open source) หรือได้รับความยินยอมโดยชอบด้วยกฎหมายจากผู้มีอำนาจเปิดเผยข้อมูลนั้น นอกจากนี้ หลักการและคำแนะนำก่อนหน้าอนุสัญญากรุงบูดาเปสต์ยังพยายามส่งเสริมให้มีการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายด้วยวิธีเฉพาะอาทิ การเก็บรักษาข้อมูลอย่างรวดเร็ว การค้นระบบคอมพิวเตอร์และ

ยึดข้อมูลทางคอมพิวเตอร์ การจัดหาข้อมูลจราจรของการสื่อสารโทรคมนาคมที่ถูกระบุมา การดักรับหรือตามหาต้นตอของการสื่อสาร เป็นต้น

อย่างไรก็ดี จะเห็นได้ว่า หลักการและคำแนะนำก่อนหน้าอนุสัญญากรุงบูดาเปสต์ไม่ได้สร้างฐานทางกฎหมายใหม่สำหรับการให้ความร่วมมือทางอาญาระหว่างประเทศโดยตรง การปรับใช้หลักการและคำแนะนำเหล่านี้ต้องอาศัยการแก้ไขปรับปรุงฐานทางกฎหมายสำหรับการให้ความร่วมมือทางอาญาระหว่างประเทศโดยทั่วไป ซึ่งประกอบไปด้วย ข้อตกลงระดับทวิภาคีและพหุภาคีจำนวนหลายฉบับ จะเห็นได้ว่าการแก้ไขให้ข้อตกลงเหล่านี้สามารถรองรับอาชญากรรมทางคอมพิวเตอร์ได้ทุกฉบับย่อมยุ่งยาก และเสียเวลามาก นอกจากนี้ ในกรณีที่รัฐเลือกจัดทำข้อตกลงความร่วมมือด้านอาชญากรรมทางคอมพิวเตอร์ขึ้นมาใหม่นั้น ข้อตกลงแบบทวิภาคีจะรองรับการให้ความร่วมมือทางอาชญากรรมคอมพิวเตอร์ได้อย่างจำกัด เพราะอาชญากรรมทางคอมพิวเตอร์สามารถเกิดได้โดยไม่อยู่ภายใต้ข้อจำกัดของเขตแดนรัฐแต่อย่างใด ส่วนการจัดทำสนธิสัญญาความร่วมมือแบบพหุภาคีขึ้นมาใหม่นั้น ก็ต้องใช้เวลาและทรัพยากรในการเจรจาและจัดทำสนธิสัญญาเป็นอย่างมาก

นอกจากนี้ จะเห็นได้ว่า หลักการหรือคำแนะนำที่จัดทำขึ้นมาก่อนหน้าอนุสัญญากรุงบูดาเปสต์นั้น จะมีฐานะเป็นเพียงแนวโน้มของกฎหมาย (Soft law) เท่านั้น ทั้งนี้ Soft law จะเป็นตราสารที่กำหนดกฎเกณฑ์ด้านแนวทางปฏิบัติ หากแต่ผู้จัดทำไม่ได้มีเจตนาที่จะทำให้ตราสารเช่นว่านั้นมีผลผูกพันทางกฎหมายโดยตรงแต่อย่างใด เพราะฉะนั้น Soft law จึงไม่ก่อให้เกิดพันธะกรณีทางกฎหมายระหว่างประเทศเช่นเดียวกับกรณีของกฎหมายสนธิสัญญา และไม่ได้เป็นสิ่งที่รัฐยึดถือว่าเป็นกฎหมาย อย่างไรก็ดี Soft law จะมีบทบาทในการสร้างแนวทางความสัมพันธ์ระหว่างประเทศ และอาจจะพัฒนาต่อไปเป็นกฎหมายจารีตประเพณีในภายหลัง หรืออาจถูกรัฐที่สนใจนำไปใช้เป็นฐานในการจัดทำสนธิสัญญาก็ได้[116]

การที่สิ่งเหล่านี้ขาดผลผูกพันทางกฎหมายระหว่างประเทศนั้น ยังส่งผลให้การปฏิบัติตามกรอบความร่วมมือจึงขึ้นกับดุลยพินิจของรัฐ โดยรัฐจะเลือกปฏิบัติตามเนื้อหาของหลักการหรือคำแนะนำเหล่านั้นมากน้อยเพียงใดก็ได้ตามที่ต้องการ โดยปราศจาก

---

[116] D.J. Harris, Cases and materials on international law, 6th edition (London: Sweet and Maxwell, 2004), p.62

การประสานงานกัน ในขณะเดียวกัน การที่คำแนะนำหรือหลักการดังข้างต้นได้ให้กรอบของรายละเอียดไว้เพียงกว้างๆ ยังส่งผลให้การนำหลักการไปปรับใช้ขาดความสอดคล้องกันอีกด้วย

2.4 แนวทางการพัฒนากลไกความร่วมมือทางอาญาสำหรับอาชญากรรมทางคอมพิวเตอร์

เมื่อพิจารณาจากบทบาทและข้อจำกัดของหลักการและคำแนะนำที่จัดทำขึ้นก่อนหน้าอนุสัญญากรุงบูดาเปสต์แล้ว จะเห็นได้ว่า การพัฒนากลไกความร่วมมือทางอาญาระหว่างประเทศ ให้สามารถรองรับอาชญากรรมทางคอมพิวเตอร์ได้นั้น ควรคำนึงถึงคุณสมบัติสำคัญดังต่อไปนี้

2.4.1 การสร้างมาตรฐานร่วมกันสำหรับกฎหมายภายในประเทศด้านอาชญากรรมทางคอมพิวเตอร์

นอกจากบทบาทในการพัฒนากฎหมายสารบัญญัติและกฎหมายวิธีสบัญญัติภายในรัฐให้รองรับอาชญากรรมทางคอมพิวเตอร์ได้แล้ว กลไกความร่วมมือทางอาญาสำหรับอาชญากรรมทางคอมพิวเตอร์ควรส่งเสริมให้รัฐพัฒนากฎหมายภายในของตนไปในทิศทางเดียวกัน ซึ่งจะเป็นประโยชน์ในการให้ความร่วมมือทางอาญาระหว่างประเทศในลำดับต่อไปด้วย

ในการนี้ ต้องตระหนักถึงความเป็นจริงด้วยว่า เทคโนโลยีทางคอมพิวเตอร์สามารถเปลี่ยนแปลงและพัฒนาไปได้อย่างรวดเร็ว และรัฐต่างๆ ยังคงมีความคิดที่แตกต่างกันสำหรับการกำหนดฐานความผิดบางฐาน รวมไปถึงการปรับใช้และตีความข้อกฎหมายบางเรื่อง ดังนั้น จึงนับเป็นเรื่องยากยิ่ง ที่กลไกความร่วมมือทางอาญาสำหรับอาชญากรรมทางคอมพิวเตอร์จะมีเนื้อหาครอบคลุมการกระทำความผิดทุกรูปแบบหรือการใช้อำนาจสืบสวนอาชญากรรมทางคอมพิวเตอร์ได้ในทุกประเภท เพราะฉะนั้นกลไกความรวมมือทางอาญาสำหรับอาชญากรรมทางคอมพิวเตอร์ควรจะสร้างมาตรฐานขั้นต่ำทางกฎหมายภายในร่วมกัน โดยให้มีเนื้อหาครอบคลุมประเด็นที่บรรดารัฐที่เกี่ยวข้องสามารถตกลงกันได้

2.4.2 การขยายขอบเขตความร่วมมือระหว่างประเทศให้ครอบคลุมอาชญากรรมทางคอมพิวเตอร์

นอกจากการสร้างมาตรฐานทางกฎหมายภายในประเทศด้านอาชญากรรมทางคอมพิวเตอร์แล้ว กลไกความร่วมมือทางอาญาสำหรับคอมพิวเตอร์ควรขยายผลของกฎหมายภายในเหล่านั้น ให้สามารถนำมาใช้ได้ในการให้ความร่วมมือทางอาญา อีกทั้งยังต้องปรับปรุงให้กระบวนการให้ความร่วมมือรวดเร็วและยืดหยุ่นมากขึ้นด้วย เพื่อให้ตอบสนองต่ออาชญากรรมทางคอมพิวเตอร์ได้อย่างทันต่อสถานการณ์

ในขณะเดียวกัน กลไกความร่วมมือทางอาญาสำหรับคอมพิวเตอร์ควรจัดทำขึ้นในรูปแบบสนธิสัญญาระหว่างประเทศ ซึ่งจะเป็นการสร้างฐานทางกฎหมายใหม่สำหรับการให้ความร่วมมือแก่บรรดารัฐที่เกี่ยวข้อง การกระทำดังกล่าวย่อมใช้เวลาน้อยกว่าการการแก้ไขปรับปรุงข้อตกลงความร่วมมือทางอาญาแบบทวิภาคีและแบบพหุภาคีที่มีแต่เดิมเป็นจำนวนหลายฉบับ นอกจากนี้เนื่องจากอาชญากรรมทางคอมพิวเตอร์สามารถส่งผลกระทบต่อรัฐจำนวนมากในคราวเดียวกัน สนธิสัญญาความร่วมมือทางอาญาสำหรับคอมพิวเตอร์ควรเป็นสนธิสัญญาพหุภาคี ซึ่งจะสามารถรวบรวมทรัพยากรของรัฐต่างๆ ในการปราบปรามอาชญากรรมทางคอมพิวเตอร์ และกำหนดแนวทางการปรับใช้กลไกของรัฐภาคีให้เป็นไปโดยสอดคล้องกันมากขึ้น

2.4.3 ความสามารถในการรองรับความซับซ้อนของอาชญากรรมทางคอมพิวเตอร์ที่ทวีขึ้นไปตามกาลเวลา

เนื่องจากอาชญากรรมทางคอมพิวเตอร์สามารถทวีความซับซ้อนขึ้นไปตามพัฒนาการของเทคโนโลยี และก่อให้เกิดผลกระทบทางกฎหมายบางประการได้ ดังนั้น กลไกความร่วมมือทางอาญาสำหรับอาชญากรรมทางคอมพิวเตอร์จึงควรมีความยืดหยุ่นพอที่จะเพิ่มเติมหรือเปลี่ยนแปลงรายละเอียดได้ต่อไปในภายหลัง อีกทั้งยังต้องมีความเป็นกลางทางเทคโนโลยี กล่าวคือไม่มีความเชื่อมโยงกับเทคโนโลยีประเภทใดประเภทหนึ่งอย่างเป็นการเฉพาะเจาะจง ในขณะเดียวกัน กลไกความร่วมมือทางอาญาสำหรับคอมพิวเตอร์นั้น ควรมีช่องทางอำนวยโอกาสให้รัฐต่างๆ ที่เกี่ยวข้องกับการให้ความร่วมมือนั้น สามารถติดตามและรับทราบถึงความเปลี่ยนแปลงที่เป็นผลมาจากพัฒนาการทางเทคโนโลยีเหล่านั้นได้

จากการศึกษาวิจัยในบทนี้ จะพบว่า ลักษณะพิเศษของอาชญากรรมทางคอมพิวเตอร์นั้น ส่งผลให้การป้องกันและปราบปรามอาชญากรรมต้องอาศัยการให้ความร่วมมือทางอาญาระหว่างประเทศ ควบคู่ไปกับการพัฒนากฎหมายสารบัญญัติและวิธีสบัญญัติภายในประเทศสำหรับอาชญากรรมทางคอมพิวเตอร์

กลไกความร่วมมือทางอาญาระหว่างประเทศทั่วไป ซึ่งประกอบไปด้วยการส่งตัวผู้ร้ายข้ามแดนและการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายนั้น ยังไม่เพียงพอต่อการตอบสนองอาชญากรรมทางคอมพิวเตอร์ เพราะ รัฐที่เกี่ยวข้องกับการให้ความร่วมมือทางอาญานั้นอาจขาดแคลนกฎหมายภายในด้านอาชญากรรมทางคอมพิวเตอร์หรือมีแนวทางการตีความหรือปรับใช้กฎหมายที่แตกต่างกัน จึงส่งผลให้การให้ความร่วมมือไม่สามารถเกิดขึ้นได้หรือไม่บรรลุผลในที่สุด ในขณะเดียวกัน ข้อตกลงส่งตัวผู้ร้ายข้ามแดน หรือข้อตกลงด้านการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายบางฉบับ จะกำหนดฐานความผิดที่สามารถให้ความร่วมมือได้ไว้อย่างเฉพาะเจาะจง และไม่ได้ครอบคลุมอาชญากรรมทางคอมพิวเตอร์แต่อย่างใด ปัญหาที่เกิดขึ้นเหล่านี้ เป็นผลมาจากการที่กลไกความร่วมมือทางอาญาระหว่างประเทศทั่วไป จะถูกจัดทำขึ้นมาเพื่อรองรับการให้ความร่วมมือทางอาญาในกรณีทั่วไปเท่านั้น แต่ไม่ได้คำนึงถึงอาชญากรรมทางคอมพิวเตอร์อย่างเป็นการเฉพาะเจาะจง

ในการนี้ องค์การระหว่างประเทศหลายแห่ง องค์การระหว่างประเทศบางแห่งเช่น องค์การตำรวจสากล (Interpol) กลุ่ม G7 และสภายุโรป ได้พยายามดำเนินการพัฒนาให้กลไกความร่วมมือทางอาญาระหว่างประเทศเหมาะแก่การปรับใช้ในบริบทอาชญากรรมทางคอมพิวเตอร์มากขึ้น ด้วยการจัดทำคำแนะนำหรือหลักการต่างๆ เพื่อให้รัฐต่างๆ สามารถพัฒนากฎหมายภายในของตนให้สามารถรองรับอาชญากรรมทางคอมพิวเตอร์และร่วมมือกันในเรื่องดังกล่าวได้มากขึ้น ซึ่งรวมไปถึงการจัดตั้งเครือข่ายจุดติดต่อตลอดเวลาเพื่อให้การติดต่อประสานงานเป็นไปอย่างรวดเร็วทันสถานการณ์ด้วย

อย่างไรก็ตาม ความพยายามก่อนหน้าความร่วมมือกรอบอนุสัญญากรุงบูดาเปสต์นั้น จะปรากฏอยู่ในรูปของคำแนะนำหรือหลักการที่ไม่มีผลผูกพันตามกฎหมายระหว่างประเทศ อีกทั้งวางกรอบรายละเอียดไว้เพียงกว้างๆ อาจส่งผลให้การนำหลักการไปปรับใช้โดยรัฐต่างๆ

ไม่สอดคล้องกัน เพราะรัฐต่างๆ อาจเลือกปฏิบัติตามเนื้อหาของคำแนะนำเหล่านี้มากน้อยเพียงใดก็ได้ นอกจากนี้ เนื้อหาบางส่วนของความพยายามเหล่านี้ ยังไม่ครอบคลุมปัญหาบางประเด็นอันเป็นผลมาจากการเปลี่ยนแปลงทางเทคโนโลยี เช่น ความผิดที่เกี่ยวข้องกับเนื้อหา หรือความผิดที่เกี่ยวข้องกับการละเมิดผลงานอันมีลิขสิทธิ์ที่ไม่ใช่โปรแกรมคอมพิวเตอร์ หรือแผงวงจรรวม เป็นต้น

เพราะฉะนั้น จึงกล่าวสรุปได้ว่า กลไกความร่วมมือทางอาญาระหว่างประเทศนั้นควรที่จะมีบทบาทในการสร้างมาตรฐานร่วมกันสำหรับกฎหมายภายในประเทศด้านอาชญากรรมทางคอมพิวเตอร์ การขยายขอบเขตความร่วมมือระหว่างประเทศให้ครอบคลุมอาชญากรรมทางคอมพิวเตอร์ และการรองรับความซับซ้อนของอาชญากรรมทางคอมพิวเตอร์ที่ทวีขึ้นไปตามกาลเวลา คุณสมบัติสำคัญทั้งสามประการดังข้างต้นนี้ ได้นำไปสู่การจัดทำสนธิสัญญาด้านความร่วมมือทางอาญาสำหรับอาชญากรรมทางคอมพิวเตอร์ในเวลาต่อมา สนธิสัญญานั้นก็คืออนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของสภายุโรป หรืออนุสัญญากรุงบูดาเปสต์นั่นเอง

บทที่ 3
กลไกความร่วมมือทางอาญาระหว่างประเทศสำหรับอาชญากรรมทางคอมพิวเตอร์ภายใต้กรอบอนุสัญญากรุงบูดาเปสต์

เนื้อหาของวิทยานิพนธ์ในบทนี้ จะแบ่งออกเป็น 5 ส่วน โดยส่วนที่หนึ่งนั้นจะอธิบายรายละเอียดเกี่ยวกับข้อมูลเบื้องต้นเกี่ยวกับความร่วมมือทางอาญาในกรอบอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของสภายุโรปหรืออนุสัญญากรุงบูดาเปสต์ ซึ่งเป็นสนธิสัญญาฉบับแรกด้านความร่วมมือทางอาญาสำหรับอาชญากรรมทางคอมพิวเตอร์โดยตรง ทั้งนี้ ความร่วมมือทางอาญาในกรอบอนุสัญญากรุงบูดาเปสต์ จะครอบคลุมไปถึงพิธีสารเพิ่มเติมว่าด้วยการกระทำผ่านระบบคอมพิวเตอร์ที่มีลักษณะเป็นการเหยียดหยามหรือเกลียดชังเชื้อชาติอีกด้วย

หลังจากนั้น ส่วนที่สองถึงสี่ของบทจะอธิบายถึงกลไกความร่วมมือทางอาญาสำหรับอาชญากรรมทางคอมพิวเตอร์ภายใต้กรอบอนุสัญญากรุงบูดาเปสต์ ซึ่งจะประกอบไปด้วยการส่งตัวผู้ร้ายข้ามแดน การให้ความช่วยเหลือซึ่งกันและกันทางกฎหมาย และการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายด้วยวิธีการเฉพาะตามลำดับ

เนื้อหาส่วนสุดท้ายของบทที่ 3 นี้จะเป็นการวิเคราะห์บทบาทของความร่วมมือทางอาญาภายใต้กรอบอนุสัญญากรุงบูดาเปสต์ในการสร้างมาตรฐานร่วมกันสำหรับกฎหมายภายในประเทศด้านอาชญากรรมทางคอมพิวเตอร์ การขยายขอบเขตความร่วมมือระหว่างประเทศให้ครอบคลุมอาชญากรรมทางคอมพิวเตอร์ และการรองรับความซับซ้อนของอาชญากรรมทางคอมพิวเตอร์ที่ทวีขึ้นไปตามกาลเวลา คุณสมบัติทั้งสามประการนี้นับว่ามีความสำคัญต่อการพัฒนาความร่วมมือทางอาญาสำหรับอาชญากรรมคอมพิวเตอร์โดยเฉพาะเจาะจง ดังที่ได้กล่าวไว้ในท้ายบทที่ 2

3.1 ความเบื้องต้น

เนื้อหาส่วนนี้จะอธิบายถึงความเป็นมาของอนุสัญญากรุงบูดาเปสต์และพิธีสารเพิ่มเติม ซึ่งจะครอบคลุมถึงข้อมูลเบื้องต้นเกี่ยวกับสภายุโรป รวมไปถึงกระบวนการจัดทำและโครงสร้างเนื้อหาของอนุสัญญาและพิธีสารเพิ่มเติมดังกล่าวด้วย

3.1.1 สภายุโรป

สภายุโรป (Council of Europe) ซึ่งเป็นองค์การระหว่างประเทศที่จัดตั้งโดยรัฐในภูมิภาคทวีปยุโรปจำนวน 10 รัฐเมื่อวันที่ 5 พฤษภาคม ค.ศ. 1949 โดยมีวัตถุประสงค์เพื่อสร้างเอกภาพและส่งเสริมความร่วมมือกันภายในภูมิภาคด้านต่างๆได้แก่ การปกป้องสิทธิมนุษยชนหรือการปฏิบัติตามกฎหมาย การส่งตัวผู้ร้ายข้ามแดน การให้ความช่วยเหลือซึ่งกันและกันทางกฎหมาย เป็นต้น ในปัจจุบัน สภายุโรปมีรัฐสมาชิกเป็นจำนวน 47 ประเทศ และมีสำนักงานเลขาธิการตั้งอยู่ที่กรุง Strasbourg ประเทศฝรั่งเศส

องคาพยพหนึ่งที่สำคัญของสภายุโรปได้แก่คณะมนตรี (Committee of Ministers) ซึ่งมีหน้าที่ในการตัดสินในเรื่องต่างๆ และมีสมาชิกเป็นรัฐมนตรีประจำกระทรวงการต่างประเทศของบรรดารัฐสมาชิก และมีผู้แทนทางการทูตถาวรประจำที่ กรุงสตราสบูร์ก ทั้งนี้ ข้อ 15 ของธรรมนูญก่อตั้งสภายุโรปกำหนดให้คณะมนตรีมีหน้าที่รับรองเนื้อหาของสนธิสัญญาในขั้นตอนสุดท้ายของกระบวนการจัดทำอนุสัญญาและข้อตกลงต่างๆ[1] โดยการลงคะแนนเสียงเพื่อรับรองสนธิสัญญาต้องอาศัยคะแนนเสียงข้างมากซึ่งคิดเป็นอัตรา 2 ใน 3 ของผู้แทนที่ได้ลงคะแนนเสียงทั้งหมด และเป็นเสียงส่วนใหญ่ของผู้มีสิทธิในการลงคะแนนเสียงทั้งหมดด้วย ดังที่กำหนดไว้ในข้อ 20 ของธรรมนูญก่อตั้งสภายุโรป[2] นอกจากนี้ การลงคะแนนเสียงเพื่ออนุญาตให้ตีพิมพ์รายงานคำอธิบายประกอบสนธิสัญญาต้องอาศัยคะแนนเสียงข้างมากตามหลักเกณฑ์เดียวกันด้วย นอกจากการจัดทำสนธิสัญญาแล้ว ข้อ 15b ของธรรมนูญก่อตั้งสภายุโรปกำหนดให้คณะมนตรีมีหน้าที่รับรองคำแนะนำต่างๆให้บรรดารัฐสมาชิกในเรื่องที่คณะมนตรีเห็นพ้องต้องตรงกันว่าเป็นนโยบายร่วมกันระหว่างรัฐสมาชิก แต่คำแนะนำนั้นจะไม่ก่อให้เกิดผลผูกพันทางกฎหมายแต่อย่างใด[3]

---

[1] Statute of the Council of Europe, Art. 15

[2] *Ibid*., Art. 20

[3] *Ibid*., Art.15 b

3.1.2 กระบวนการจัดทำอนุสัญญากรุงบูดาเปสต์

อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์หรืออนุสัญญากรุงบูดาเปสต์มีที่มาจากคำแนะนำของสภายุโรปในปี 1989 เกี่ยวกับการกำหนดฐานความผิดด้านอาชญากรรมทางคอมพิวเตอร์และคำแนะนำของสภายุโรปเกี่ยวกับมาตรการทางวิธีสบัญญัติด้านอาชญากรรมทางคอมพิวเตอร์ในปี 1995 การจัดทำอนุสัญญากรุงบูดาเปสต์ได้เริ่มขึ้นเมื่อเดือนพฤศจิกายน ค.ศ. 1996 เมื่อคณะกรรมการด้านปัญหาอาชญากรรมของสภายุโรป (CDPC) ได้ออกคำวินิจฉัยหมายเลข CDPC/103/211196ว่า ควรมีการจัดตั้งคณะกรรมการผู้เชี่ยวชาญ ไว้เพื่อแก้ไขปัญหาอาชญากรรมทางคอมพิวเตอร์ซึ่งสามารถข้ามเขตแดนรัฐและก่อปัญหาการบังคับใช้กฎหมายให้แก่หน่วยงานของรัฐได้[4] โดยการจัดทำตราสารระหว่างประเทศที่มีผลผูกพันทางกฎหมายนั้นจะสามารถตอบสนองประเด็นปัญหาที่เกี่ยวข้องได้ ไม่ว่าจะเป็นด้านมาตรการด้านความร่วมมือระหว่างประเทศ กฎหมายสารบัญญัติและวิธีสบัญญัติ และประเด็นปัญหาอื่นๆที่มีความเชื่อมโยงใกล้ชิดกับเทคโนโลยีทางคอมพิวเตอร์[5]

หลังจากนั้น เมื่อวันที่ 4 กุมภาพันธ์ ปี 1997 ได้มีการจัดตั้งคณะกรรมการผู้เชี่ยวชาญด้านอาชญากรรมบนเครือข่ายอินเตอร์เน็ต (PC-CY) ภายใต้คำวินิจฉัยของคณะมนตรีสภายุโรป เลขที่ CM/Del/Dec(97)583 และในเดือนเมษายนปีเดียวกันนั้น คณะกรรมการ PC- CY ได้เริ่มต้นการเจรจาจัดทำร่างอนุสัญญาอนุสัญญากรุงบูดาเปสต์ โดยมีข้อกำหนดโครงการให้คณะกรรมการดำเนินการเสร็จสิ้นภายใน 31 ธันวาคม 1999 และได้มีการขยายกำหนดเวลาดังกล่าวไปจนถึงวันที่ 31 ธันวาคม 2000 ในภายหลัง[6] สำหรับการร่างอนุสัญญากรุงบูดาเปสต์นั้น คณะกรรมการ PC-CY ได้ให้ความสำคัญแก่ประเด็นปัญหา 5 ประการ ได้แก่ การก่ออาชญากรรมทางคอมพิวเตอร์ผ่านทางเครือข่ายโทรคมนาคม การสร้างความสอดคล้องกันในด้านกฎหมายสารบัญญัติ อำนาจการสืบสวนคดีอาชญากรรมทางคอมพิวเตอร์ การขัดกันทางกฎหมาย และการให้ความร่วมมือในระดับระหว่างประเทศ[7] ในขณะเดียวกัน แม้ว่าสภายุโรปจะเป็นผู้ดำเนินการ

---

[4] Council of Europe. Convention on cybercrime explanatory report[Online]. Available from: http://conventions.coe.int/Treaty/en/Reports/Html/185.htm [2013, May 6] Para.8

[5] *Ibid*., Para. 9

[6] *Ibid*., Para. 12

[7] Ryan M.F. Baron, “A critique of the international cybercrime treaty,” Commlaw Conspectus, 10,263 (2002):2

จัดทำอนุสัญญาฉบับนี้ก็ตาม รัฐนอกกลุ่มสภายุโรปบางแห่ง อาทิ สหรัฐอเมริกา แคนาดา ญี่ปุ่น และแอฟริกาใต้ ได้เข้ามามีส่วนร่วมในการร่างอนุสัญญาด้วย

ระหว่างการเจรจาและจัดทำอนุสัญญานั้น คณะกรรมการ PC- CY ได้จัดประชุมใหญ่ 10 ครั้ง และจัดประชุมการร่างแบบปลายเปิด 15 ครั้ง[8]โดยในเดือนเมษายน 2000 สภายุโรปได้เปิดเผยร่างอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ออกสู่สาธารณชนเป็นครั้งแรก โดยแนบแถลงการณ์สำหรับสื่อมวลชน (Press release) ซึ่งอธิบายองค์ประกอบพื้นฐานทางกฎหมายและหลักกฎหมายที่อยู่เบื้องหลังอนุสัญญา อีกทั้งยังเรียกร้องให้ภาคส่วนต่างๆ ให้ออกความเห็นต่างๆเกี่ยวกับร่างอนุสัญญากรุงบูดาเปสต์ด้วย นับจากนั้นเป็นต้นมา ร่างอนุสัญญาฉบับต่างๆจะถูกเผยแพร่ออกสู่สาธารณชนภายหลังการประชุมใหญ่แต่ละครั้ง เพื่อให้รัฐผู้ร่วมการเจรจาสามารถปรึกษาหารือกับผู้มีส่วนได้เสียฝ่ายต่างๆด้วย[9] หลังจากนั้น ในเดือนธันวาคมปี 2000 ผู้เชี่ยวชาญต่างๆ ยังจัดการประชุมเพิ่มเติมอีกสามครั้งเพื่อทำบันทึกอธิบายร่างอนุสัญญาและทำการทบทวนร่างอนุสัญญาโดยอาศัยความเห็นเพิ่มเติมของ Parliamentary Assembly[10]

ร่างอนุสัญญาฉบับสุดท้ายที่ผ่านการทบทวนแล้ว พร้อมบันทึกอธิบายร่างอนุสัญญานั้น ถูกเสนอไปให้คณะกรรมการ CDPC อนุมัติในการประชุมใหญ่คณะกรรมการครั้งที่ 50 ในเดือนมิถุนายน ปี 2001 หลังจากนั้น ในวันที่ 8 พฤศจิกายน 2001 คณะมนตรีสภายุโรปได้รับรองอนุสัญญาและเปิดให้รัฐต่างๆเข้าร่วมลงนามอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์[11]

อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของสภายุโรปหรืออนุสัญญากรุงบูดาเปสต์นั้น มีผลบังคับใช้ตั้งวันที่ 1 มกราคม 2004[12] ซึ่งเป็นช่วงเวลาสามเดือน

---

[8] Council of Europe. Convention on cybercrime explanatory report Para. 13

[9] *Ibid*., Para. 14

[10] *Ibid*., Para. 13

[11] Sara L.Marler, “The convention on cyber-crime: Should the United States ratify?, New England Law Review 37,183 (2002) :6

[12] Convention on cybercrime CETS No. 185, Status as of 6/5/2013 [Online], Available from: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG

หลังจากที่ มีรัฐจำนวนครบห้ารัฐได้แสดงความยินยอมที่จะผูกพันตามอนุสัญญานี้ โดยที่ในกลุ่มดังกล่าวมีรัฐสมาชิกสภายุโรปเป็นจำนวนอย่างน้อยสามประเภทรวมอยู่ด้วย ทั้งหมดนี้เป็นไปตามที่กำหนดไว้ในอนุสัญญามาตรา 36 (3) แห่งอนุสัญญาว่ากรุงบูดาเปสต์ ในปัจจุบัน อนุสัญญากรุงบูดาเปสต์ มีรัฐที่เข้าเป็นภาคีอนุสัญญาฉบับนี้เป็นจำนวน 39 รัฐ อีกทั้งยังมีรัฐอีก 12 รัฐที่ได้ลงนามแล้วแต่ยังไม่ได้ให้สัตยาบัน[13]

3.1.3 กระบวนการจัดทำพิธีสารเพิ่มเติมอนุสัญญากรุงบูดาเปสต์

ในระยะเริ่มแรก คณะกรรมการผู้ร่างอนุสัญญากรุงบูดาเปสต์ ได้เสวนาเกี่ยวกับการกำหนดฐานความผิดที่เกี่ยวข้องกับเนื้อหาประการอื่นๆ ได้แก่ การเผยแพร่โฆษณาชวนเชื่อให้เหยียดหยามเชื้อชาติผ่านทางอินเตอร์เน็ตไว้ไปในอนุสัญญาด้วย อย่างไรก็ตาม คณะกรรมการผู้ร่างอนุสัญญาไม่สามารถหาข้อตกลงอย่างเป็นเอกฉันท์ได้ เพราะผู้แทนในคณะกรรมการบางส่วนมีความกังวลในประเด็นเรื่องเสรีภาพในการแสดงออก ด้วยปัญหานี้ คณะกรรมการผู้ร่างอนุสัญญาจึงเสนอเรื่องเข้าสู่คณะกรรมการ CDPC เพื่อจัดทำพิธีสารเพิ่มเติมอนุสัญญากรุงบูดาเปสต์แทน แนวคิดการร่างพิธีสารเพิ่มเติมดังกล่าวนี้ ได้รับการสนับสนุนโดยความเห็นของ Parliamentary Assembly ที่ 226 (2001) ซึ่งแนะนำให้มีการร่างพิธีสารเพิ่มเติมเพื่อให้อนุสัญญากรุงบูดาเปสต์มีขอบเขตครอบคลุมการกระทำความผิดลักษณะใหม่ๆ โดยพิธีสารจะให้ความสำคัญแก่การให้คำจำกัดความและกำหนดฐานความผิดสำหรับการเผยแพร่โฆษณาชวนเชื่อให้เหยียดหยามเชื้อชาติผ่านทางอินเตอร์เน็ต

ด้วยเหตุนี้ คณะมนตรีสภายุโรปจึงมอบหมายให้คณะกรรมการผู้เชี่ยวชาญด้านการกำหนดความผิดทางอาญาสำหรับการกระทำผ่านทางระบบคอมพิวเตอร์ที่มีลักษณะเหยียดหยามหรือเกลียดชังเชื้อชาติ (Committee of Experts on the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems หรือ PC-RX) ซึ่งอยู่ภายใต้สังกัดคณะกรรมการ CDPC ให้จัดเตรียมร่างพิธีสารเพิ่มเติมต่อไป

[2013, May 6]

[13] *Ibid.*

เนื้อหาของพิธีสารเพิ่มเติมนี้เกี่ยวข้องกับการกำหนดคำจำกัดความและกำหนดองค์ประกอบความผิดสำหรับการเหยียดหยามหรือเกลียดชังเชื้อชาติผ่านทางระบบคอมพิวเตอร์ อีกทั้งยังได้ขยายขอบเขตการปรับใช้อนุสัญญากรุงบูดาเปสต์ทั้งในส่วนกฎหมายสารบัญญัติ กฎหมายวิธีสบัญญัติ และการให้ความร่วมมือระหว่างประเทศ ให้ครอบคลุมการสืบสวนและดำเนินคดีต่อผู้กระทำความผิดตามพิธีสารเพิ่มเติมด้วย

พิธีสารเพิ่มเติมว่าด้วยการกระทำผ่านระบบคอมพิวเตอร์ที่มีลักษณะเหยียดหยามหรือเกลียดชังเชื้อชาตินั้น ได้เปิดให้มีการลงนามเมื่อวันที่ 28 มกราคม 2003 ที่กรุงสตราสบูร์ก ประเทศฝรั่งเศส และมีผลบังคับใช้เมื่อวันที่ 1 มีนาคม 2006 หลังจากที่มีรัฐให้สัตยาบันครบ 5 รัฐ ได้เป็นเวลา 3 เดือน ในปัจจุบัน พิธีสารเพิ่มเติมฉบับนี้มีรัฐเข้าร่วมลงนามแต่ไม่ได้ให้สัตยาบัน จำนวน 16 รัฐ โดยมีประเทศนอกภูมิภาคยุโรปอย่างแคนาดาและแอฟริกาใต้รวมอยู่ด้วย ส่วนรัฐที่ให้สัตยาบันหรือเข้าภาคยานุวัติพิธีสารเพิ่มเติมมีจำนวน 20 รัฐ[14]

3.1.4 โครงสร้างของอนุสัญญากรงบูดาเปสต์

อารัมภบทของอนุสัญญากรุงบูดาเปสต์ได้กล่าวถึงวัตถุประสงค์สำคัญของอนุสัญญาสามประการ ซึ่งประกอบไปด้วย การสร้างนโยบายร่วมกันทางด้านอาชญากรรมทางคอมพิวเตอร์ภายในกลุ่มรัฐภาคี การสร้างความสอดคล้องให้แก่กฎหมายสารบัญญัติและกฎหมายวิธีสบัญญัติของรัฐภาคี และการส่งเสริมความร่วมมือระหว่างประเทศ ทั้งหมดนี้จะอำนวยความสะดวกให้แก่การสืบสวนคดีอาชญากรรมทางคอมพิวเตอร์ระหว่างประเทศต่อไป

---

[14] Additional protocol to the convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems CETS No. 185, Status as of 17/4/2013 [online], Available from : http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=4&DF=&CL=ENG [2013, May 6]

เนื้อหาของอนุสัญญากรุงบูดาเปสต์ แบ่งออกเป็นสี่บท โดยบทที่หนึ่งจะให้คำจำกัดความของคำศัพท์สำคัญในอนุสัญญา ได้แก่ ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ผู้ให้บริการ (Service provider) และข้อมูลจราจร (Traffic Data)

ทั้งนี้ ข้อ 1a ของอนุสัญญาให้นิยามของระบบทางคอมพิวเตอร์ว่า เป็นอุปกรณ์หรือกลุ่มของอุปกรณ์ที่เชื่อมโยงหรือเกี่ยวข้องกัน โดยอุปกรณ์หรือกลุ่มอุปกรณ์เหล่านี้ สามารถตั้งโปรแกรมให้สามารถประมวลผลข้อมูลได้อย่างเป็นอัตโนมัติได้ ส่วน ข้อ 1 b ได้ให้นิยามเกี่ยวกับข้อมูลทางคอมพิวเตอร์ว่า หมายถึง ข้อเท็จจริง ข้อมูล หรือแนวคิดที่ถูกนำเสนอในรูปแบบที่สามารถนำไปประมวลผลด้วยระบบคอมพิวเตอร์ได้ อีกทั้งยังรวมไปถึงโปรแกรมที่ทำให้ระบบคอมพิวเตอร์สามารถทำหน้าที่ได้ด้วย คำนิยามเกี่ยวกับระบบคอมพิวเตอร์และข้อมูลทางคอมพิวเตอร์มีความสำคัญในอนุสัญญาฉบับนี้เพราะ การกระทำความผิดและการสืบสวนหาผู้กระทำความผิดนั้นต้องอาศัยระบบคอมพิวเตอร์และข้อมูลทางคอมพิวเตอร์ทั้งสิ้น

นอกจากนี้ ข้อ 1 c ได้ว่านิยามว่า ผู้ให้บริการเป็นหน่วยงานทางภาครัฐหรือภาคเอกชนใดๆที่ให้บริการด้านการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์แก่ผู้ใช้บริการได้ ทั้งนี้ ไม่ต้องคำนึงว่าผู้ให้บริการจะเรียกเก็บค่าบริการและให้บริการต่อสาธารณชนหรือไม่[15] ในขณะเดียวกันผู้ให้บริการ ยังหมายถึงหน่วยงานอื่นที่ประมวลผลหรือจัดเก็บข้อมูลทางคอมพิวเตอร์ให้กับผู้ใช้บริการหรือผู้ให้บริการสื่อสารผ่านทางระบบคอมพิวเตอร์รายอื่น ผู้ให้บริการมีบทบาทสำคัญในการสืบสวนคดีอาชญากรรมทางคอมพิวเตอร์ไม่ว่าจะเป็นในการพิสูจน์ถึงความผิดที่เกิดขึ้น การแสวงหาหลักฐานในการกระทำความผิดและระบุตัวผู้กระทำผิด ทั้งนี้ จะเห็นได้ว่าในรัฐจำนวนมากหน่วยงานทางภาครัฐจะไม่ได้ควบคุมดูแลการให้บริการทางคอมพิวเตอร์โดยตรงแต่อย่างใด หากแต่จะให้หน่วยงานทางเอกชนจัดการแทน

ข้อ 1 d ได้ให้นิยามข้อมูลจราจรว่า เป็นข้อมูลทางคอมพิวเตอร์ที่ถูกสร้างขึ้นโดยระบบคอมพิวเตอร์ และทำหน้าที่ระบุรายละเอียดที่เกี่ยวข้องกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์แต่ละครั้งได้แก่ ต้นกำเนิด ปลายทาง เส้นทาง เวลาและวันที่สื่อสาร ขนาด ระยะเวลา หรือประเภทของบริการที่ใช้ในการสื่อสาร ทั้งนี้ ตัวอย่างบริการที่ใช้ภายในการสื่อสารได้แก่ การส่งไฟล์ข้อมูล การรับส่งจดหมายอิเล็กทรอนิกส์ หรือการส่งแลกเปลี่ยนข้อความ

---

[15] Council of Europe. Convention on cybercrime explanatory report. Para.26

ตามเวลาจริง (instant messaging) เป็นต้น[16] ข้อมูลจราจรนับว่ามีความสำคัญในการสืบสวนคดีอาชญากรรมทางคอมพิวเตอร์เช่นเดียวกัน โดยเฉพาะอย่างยิ่งในการติดตามที่มาของการสื่อสารและเปิดเผยตัวผู้กระทำความผิด เพราะข้อมูลดังกล่าวจะนำไปสู่การรวบรวมหลักฐานอย่างอื่นๆ ในลำดับถัดไป อย่างไรก็ดี ข้อมูลจราจรนั้นจะถูกเก็บไว้ในช่วงเวลาสั้นๆ จึงจำเป็นต้องมีการรักษาข้อมูลอย่างรวดเร็วไว้ก่อน จากนั้นจึงเปิดเผยข้อมูลจราจรเพื่อติดตามเส้นทางการสื่อสารต่อไป[17]

บทที่สองของอนุสัญญา จะกำหนดรายละเอียดเกี่ยวกับการทำให้กฎหมายภายในรัฐด้านอาชญากรรมทางคอมพิวเตอร์สอดคล้องกัน โดยในด้านกฎหมายสารบัญญัติ อนุสัญญากรุงบูดาเปสต์จะกำหนดฐานความผิดสำหรับการกระทำ 9 รูปแบบไว้ในข้อ 2-10 ได้แก่ การเข้าสู่ระบบโดยผิดกฎหมาย การดักรับข้อมูลโดยผิดกฎหมาย การเข้าแทรกแซงข้อมูล การเข้าแทรกแซงระบบ การใช้อุปกรณ์โดยมิชอบ การปลอมแปลงที่เกี่ยวข้องกับคอมพิวเตอร์ การฉ้อโกงที่เกี่ยวข้องกับคอมพิวเตอร์ การกระทำความผิดเกี่ยวกับสิ่งลามกอนาจารเด็ก และการกระทำความผิดเกี่ยวกับทรัพย์สินทางปัญญา การกระทำที่จะตกเป็นความผิดนั้นจะต้องกระทำไปโดยเจตนาและปราศจากสิทธิ

การกระทำโดยปราศจากสิทธินั้น หมายถึง การกระทำที่ปราศจากอำนาจ ไม่ว่าจะเป็นอำนาจด้านนิติบัญญัติ บริหาร ปกครอง ตุลาการ หรืออำนาจตามสัญญาหรือการได้รับความยินยอม อีกทั้งยังรวมไปถึงการกระทำที่ไม่ได้รับยกเว้นความรับผิดตามหลักกฎหมายภายในด้วย อาทิ การป้องกัน หรือการกระทำด้วยเหตุจำเป็น เป็นต้น[18] ดังนั้น ความผิดจะไม่เกิดขึ้นในกรณีของการกระทำที่ชอบด้วยกฎหมายของเจ้าหน้าที่รัฐ กิจกรรมทั่วไปที่ชอบด้วยกฎหมายสำหรับอการอกแบบเครือข่ายคอมพิวเตอร์ หรือวิธีปฏิบัติหรือการดำเนินการทั่วไปทางการค้า[19] นอกจากนี้ อนุสัญญาข้อ 11-12 ได้กำหนดรายละเอียดเกี่ยวกับความผิดฐานผู้ใช้ ผู้สนับสนุน ความรับผิดของนิติบุคคลไว้ด้วย

---

[16] *Ibid*.,Para.30

[17] *Ibid*.,Para.29

[18] *Ibid*.,Para.8

[19] *Ibid*.,Para.8

ข้อ 13 วรรค 1 กำหนดให้รัฐภาคีดำเนินมาตรการบังคับทางอาญาต่อผู้กระทำผิด ซึ่งรวมไปถึงมาตรการกักขังจำคุก ในกรณีที่ผู้กระทำผิดเป็นนิติบุคล ข้อ 13 วรรค 2 กำหนดให้รัฐภาคีดำเนินมาตรการบังคับหรือมาตรการอื่นๆต่อนิติบุคคลผู้กระทำผิด โดยจะเป็นมาตรการทางอาญาหรือไม่ก็ได้ ทั้งนี้ให้รวมไปถึงการดำเนินมาตรการบังคับทางการเงินด้วย

สำหรับด้านกฎหมายวิธีสบัญญัติ ข้อ 14 ของอนุสัญญากรุงบูดาเปสต์ได้กำหนดให้รัฐภาคีให้อำนาจสำหรับการสืบสวนและดำเนินคดีอาชญากรรมคอมพิวเตอร์ด้วยมาตรการทางนิติบัญญัติและมาตรการอื่นๆ แก่หน่วยงานผู้บังคับใช้กฎหมายของตน อำนาจในการสืบสวนดังกล่าวได้แก่ การเก็บรักษาข้อมูลคอมพิวเตอร์ที่ถูกเก็บไว้อย่างรวดเร็ว การเก็บรักษาและเปิดเผยข้อมูลจราจรอย่างรวดเร็ว การออกคำสั่งให้แสดงข้อมูลสำคัญ การค้นและยึดข้อมูลคอมพิวเตอร์ที่ถูกเก็บไว้ การรวบรวมข้อมูลจราจรตามเวลาจริง และการดักรับข้อมูลทางเนื้อหาดังที่จะปรากฏในข้อ16ถึง 21 ของอนุสัญญานอกจากนี้ ข้อ 14 วรรค 2 ยังกำหนดให้อำนาจการสืบสวนอาชญากรรมทางคอมพิวเตอร์เหล่านี้ ยกเว้นการดักรับข้อมูลทางเนื้อหา มีขอบเขตการปรับใช้ครอบคลุมการกระทำความผิดตาม ข้อ 2-11 ของอนุสัญญา อาชญากรรมประเภทอื่นๆที่กระทำโดยใช้ระบบคอมพิวเตอร์ อีกทั้งรวมไปถึงการรวบรวมหลักฐานการกระทำความผิดทางอาญาที่อยู่ในรูปแบบข้อมูลทางอิเล็กทรอนิกส์ด้วย

ข้อ 15 วรรค 1 ได้กำหนดให้ การดำเนินการตามมาตรการเหล่านี้ต้องประกอบไปด้วยเงื่อนไขและมาตรการป้องกันตามกฎหมายภายใน เพื่อป้องกันสิทธิมนุษยชนและเสรีภาพพื้นฐาน โดยให้รัฐคำนึงถึงตราสารด้านสิทธิมนุษยชนที่สำคัญได้แก่ บทบัญญัติของอนุสัญญายุโรปปี 1950 ว่าด้วยการปกป้องสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐาน (1950 European Convention for the Protection of Human Rights and Fundamental Freedoms) กติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (International Covenant on Civil and Political Rights) หรือสนธิสัญญาด้านสิทธิมนุษยชนอื่นๆที่มีผลบังคับใช้ อีกทั้งให้คำนึงถึงหลักความได้สัดส่วนด้วย นอกจากนี้ข้อ 15 วรรค 2 ได้ยกตัวอย่างของเงื่อนไขและมาตรการป้องกันข้างต้นว่ารวมไปถึง การควบคุมดูแลโดยฝ่ายตุลาการหรือหน่วยงานอิสระ การกำหนดให้มีเหตุรองรับเพียงพอก่อนปรับใช้มาตรการสอบสวน หรือการจำกัดขอบเขตหรือระยะเวลาในการใช้อำนาจหรือกระบวนการสืบสวนดังกล่าว ส่วนข้อ 15 วรรค 3 ได้กำหนดให้รัฐภาคีพิจารณาผลกระทบที่อำนาจและกระบวนการสืบสวนมีต่อสิทธิ ความรับผิดชอบ และผลประโยชน์

โดยชอบด้วยกฎหมายของบุคคลที่สามโดยควบคู่ไปกับผลประโยชน์ส่วนรวม และการบริหารกระบวนการยุติธรรม

บทที่สามของอนุสัญญานั้นจะกล่าวถึงการให้ความร่วมมือทางอาญาระหว่างประเทศ โดยข้อ 23 ได้กำหนดหลักทั่วไปให้รัฐภาคีให้ความร่วมมือทางอาญาระหว่างประเทศให้กว้างที่สุดเท่าที่จะทำได้ อีกทั้งให้ลดอุปสรรคในการให้ความร่วมมือให้มากที่สุด เพื่อให้การดำเนินการต่างๆ นั้นสามารถรวบรวมหลักฐานสำคัญได้ทันท่วงที ข้อ 23 ของอนุสัญญายังกำหนดให้ความร่วมมือทางอาญาครอบคลุมไปถึงการก่ออาชญากรรมตามฐานความผิดที่กำหนดไว้ในข้อ 2-11 ของอนุสัญญาและอาชญากรรมประเภทอื่นๆที่ใช้คอมพิวเตอร์เป็นเครื่องมือ อีกทั้งยังรวมไปถึงการรวบรวมหลักฐานที่อยู่ในรูปแบบข้อมูลคอมพิวเตอร์ของอาชญากรรมทุกประเภท

ในทางปฏิบัติ รัฐต่างๆได้ทำข้อตกลงความร่วมมือทางอาญาระหว่างประเทศทั่วไปไว้ก่อนหน้าการจัดทำอนุสัญญากรุงบูดาเปสต์แล้ว เพื่อไม่ให้ส่งผลกระทบต่อข้อตกลงเหล่านั้น ข้อ 23 จึงกำหนดให้การให้ความร่วมมือทางอาญาระหว่างประเทศเป็นไปโดยอาศัยการปรับใช้กฎหมายที่เกี่ยวข้องและมีผลบังคับใช้กับรัฐภาคีทั้งในระดับภายในและระหว่างประเทศ อย่างไรก็ตาม ถ้าหากทั้งอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์และกฎหมายที่มีผลบังคับใช้อื่นๆ กล่าวถึงเรื่องเดียวกันให้ยึดตามเนื้อหาของอนุสัญญา

การให้ความร่วมมือทางอาญาระหว่างประเทศภายใต้อนุสัญญากรุงบูดาเปสต์นี้ จะประกอบไปด้วยการส่งตัวผู้ร้ายข้ามแดนและการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมาย อีกทั้งยังมีการจัดตั้งเครือข่ายจุดติดต่อตลอดเวลา ไว้เป็นจุดติดต่อประสานงานกันระหว่างรัฐภาคี เพื่อให้ความช่วยเหลือในด้านต่างๆที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์ได้อย่างทันท่วงที

เนื้อหาบทสุดท้ายของอนุสัญญา จะเป็นบทบัญญัติท้ายอนุสัญญา (final provisions) ซึ่งจะเกี่ยวข้องกับการบริหารอนุสัญญาโดยทั่วไป ได้แก่ บทบัญญัติเกี่ยวกับการเข้าผูกพันตามอนุสัญญาด้วยการลงนามหรือการเข้าภาคยานุวัติ บทบัญญัติที่จำกัดผลการบังคับใช้อนุสัญญาด้วยการตั้งข้อสงวน การประกาศเขตแดนบังคับใช้ การประกาศตีความรายละเอียดอนุสัญญาบางส่วน การปรับปรุงแก้ไขอนุสัญญา การระงับข้อพิพาท เป็นต้น

ในด้านการเข้าผูกพันตามอนุสัญญานั้น ข้อ 37 วรรคหนึ่งของอนุสัญญาได้เปิดโอกาสให้รัฐที่ไม่เป็นสมาชิกสภายุโรปและไม่ได้เข้าร่วมเจรจาร่างอนุสัญญาสามารถภาคยานุวัติอนุสัญญาหลังจากอนุสัญญามีผลบังคับใช้ได้ โดยต้องได้รับคำเชิญจากคณะมนตรีสภายุโรปเสียก่อน และผ่านการอนุญาตให้รัฐเข้าภาคยานุวัติจะเป็นไปโดยอาศัยเสียงข้างมากตาม ข้อ 20 d ของธรรมนูญก่อตั้งสภายุโรป[20]

นอกจากนี้ ข้อ 39 ยังได้กำหนดความสัมพันธ์ระหว่างตัวอนุสัญญากรุงบูดาเปสต์กับ สนธิสัญญาหรือข้อตกลงต่างๆระหว่างรัฐภาคีด้านความร่วมมือทางอาญาระหว่างประเทศอื่นๆ อาทิ อนุสัญญาสภายุโรปว่าด้วยการส่งผู้ร้ายข้ามแดน (ETS No. 24) อนุสัญญาสภายุโรปว่าด้วยการให้ความช่วยเหลือซึ่งกันและกันในคดีอาญา (ETS No. 30) และพิธีสารเพิ่มเติมอนุสัญญาสภายุโรปว่าด้วยการให้ความช่วยเหลือซึ่งกันและกันในคดีอาญา (ETS No.99) โดยอนุสัญญากรุงบูดาเปสต์จะมีวัตถุประสงค์เพื่อสนับสนุนสนธิสัญญาหรือข้อตกลงเหล่านั้น โดยที่บทบัญญัติของอนุสัญญากรุงบูดาเปสต์จะไม่ส่งผลกระทบต่อสิทธิ ข้อจำกัด พันธะกรณี และความรับผิดชอบประการอื่นๆของรัฐภาคีแต่อย่างใด รัฐภาคีของอนุสัญญากรุงบูดาเปสต์นั้นจะสามารถปรับใช้และดำเนินการตามสนธิสัญญาฉบับอื่นๆได้ตามปกติ หากแต่ต้องเป็นไปโดยสอดคล้องกับหลักการและวัตถุประสงค์ของอนุสัญญากรุงบูดาเปสต์ด้วย จะเห็นได้ว่าอนุสัญญากรุงบูดาเปสต์นั้นจะมีลักษณะเป็นกฎหมายเฉพาะ (Lex Specialis) เพื่อมาส่งเสริมข้อตกลงฉบับอื่นๆซึ่งมีลักษณะเป็นกฎหมายทั่วไป (Lex Generalis)

ข้อ 46 วรรค 1 กำหนดให้รัฐภาคีมีหน้าที่ปรึกษาหารือกันตามระยะเวลาที่เหมาะสม เพื่อให้การใช้งานและดำเนินการตามอนุสัญญามีประสิทธิภาพมากขึ้น เนื้อหาของการปรึกษาหารือนั้นจะครอบคลุมประเด็นต่างๆ อาทิ อุปสรรคที่เกิดจากการตั้งข้อสงวนหรือการประกาศการตีความรายละเอียดอนุสัญญาบางส่วน การแลกเปลี่ยนข้อมูลเกี่ยวกับ

---

[20] Statute of the Council of Europe, Art. 20d:

All other resolutions of the Committee, including adoption of the budget, of rules of procedure and of financial and administrative regulations, recommendations for the amendment of articles of this Statute, other than those mentioned in paragraph a.v above, and deciding in case of doubt which paragraph of this article applies, require a two-thirds majority of the representatives casting a vote and of a majority of the representatives entitled to sit on the Committee.

พัฒนาการด้านกฎหมาย นโยบาย หรือเทคโนโลยี ที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์ และกระบวนการรวบรวมหลักฐานทางอิเล็คทรอนิกส์ และการพิจารณาถึงความเป็นไปได้ในการเพิ่มเติมหรือแก้ไขอนุสัญญา โดยให้แจ้งผลลัพธ์จากการหารือไปยัง คณะกรรมาธิการด้านปัญหาอาชญากรรมของสภายุโรป (CDPC) นอกจากนี้ ข้อ 46 วรรค 3 กำหนดให้คณะกรรมการ CDPC ร่วมมือกับรัฐภาคีเพื่อทบทวนบทบัญญัติของอนุสัญญา พร้อมทั้งเสนอการแก้ไขบทบัญญัติตามที่จำเป็นภายใน 3 ปีแรกนับตั้งแต่อนุสัญญามีผลบังคับใช้ จะเห็นได้ว่าการปรึกษาหารือนี้จะมีบทบาทช่วยให้รัฐภาคีทั้งหลายเข้ามีส่วนร่วมในการติดตามผลของอนุสัญญาได้อย่างเท่าเทียมกัน[21]

3.1.5 โครงสร้างของพิธีสารเพิ่มเติมอนุสัญญากรงบูดาเปสต์

พิธีสารเพิ่มเติมอนุสัญญากรุงบูดาเปสต์ว่าด้วยการกระทำผ่านระบบคอมพิวเตอร์ที่มีลักษณะเหยียดหยามหรือเกลียดชังเชื้อชาตินั้น จะแบ่งเนื้อหาออกเป็น 4 บท โดยบทแรกจะเป็นบทบัญญัติร่วม (common provisions) ซึ่งจะกล่าวถึงจุดประสงค์ของพิธีสารว่าเป็นไปเพื่อเสริมเนื้อหาของอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของสภายุโรป และการให้คำจำกัดความของคำว่าวัตถุที่มีลักษณะเหยียดหยามหรือเกลียดชังเชื้อชาติ

ภายใต้ข้อ 2 ของพิธีสารเพิ่มเติมนั้น วัตถุที่มีลักษณะเหยียดหยามหรือเกลียดชังเชื้อชาตินั้นหมายถึงวัตถุที่มีเนื้อหาสนับสนุน ส่งเสริม หรือกระตุ้นให้เกิดความเกลียดชัง เลือกปฏิบัติหรือก่อความรุนแรงต่อบุคคลหรือกลุ่มบุคคล โดยอาศัยเหตุแห่งเชื้อชาติ สีผิว เชื้อสายบรรพบุรุษ เชื้อชาติ หรือเผ่าพันธุ์ ซึ่งรวมไปถึงเหตุแห่งศาสนาด้วย ในกรณีที่ศาสนาถูกนำไปใช้เชื่อมโยงกับเหตุปัจจัยประการอื่นๆดังข้างต้น ทั้งนี้ วัตถุที่มีลักษณะเหยียดหยามหรือเกลียดชังเชื้อชาติอาจจะนำเสนอออกมาในรูปแบบเป็นลายลักษณ์อักษร รูปภาพ หรือรูปแบบอื่นๆได้

บทที่สองของพิธีสารเพิ่มเติม จะกล่าวถึงฐานความผิดที่รัฐภาคีจะต้องกำหนดให้เป็นความผิดทางอาญาตามกฎหมายภายในของตน การกระทำที่พิธีสารเพิ่มเติมฉบับนี้ครอบคลุมประกอบไปด้วย การเผยแพร่วัตถุที่มีลักษณะเหยียดหยามหรือเกลียดชังเชื้อชาติผ่านทางระบบคอมพิวเตอร์ การข่มขู่ที่มีลักษณะเหยียดหยามหรือเกลียดชังเชื้อชาติ

---

[21] Council of Europe. Convention on cybercrime explanatory report Para.328

การสบประมาทที่มีลักษณะเหยียดหยามหรือเกลียดชังเชื้อชาติ และการปฏิเสธ บิดเบือน ยอมรับหรือแก้ต่างให้กับการฆ่าล้างเผ่าพันธุ์หรืออาชญากรรมต่อมนุษยชาติ

นอกจากนี้ ข้อ 7 ของพิธีสารเพิ่มเติม ได้ให้รัฐภาคีกำหนดความผิดทางอาญาสำหรับผู้ใช้และผู้สนับสนุนในการกระทำตามฐานความผิดของพิธีสารเพิ่มเติมด้วย ผู้กระทำการตามฐานความผิดดังข้างต้นนี้ จะต้องกระทำการโดยเจตนาและปราศจากสิทธิ์ ทั้งนี้ ความหมายของการกระทำโดยเจตนานั้น ให้เป็นไปตามการตีความของแต่ละรัฐ[22]นอกจากนี้ ผู้ให้บริการไม่มีหน้าที่ที่จะต้องตรวจตราการกระทำภายใน web site ของตนแต่อย่างใด[23]

เนื้อหาบทที่สามของพิธีสารเพิ่มเติม จะกำหนดลักษณะความสัมพันธ์ระหว่างอนุสัญญากรุงบูดาเปสต์และพิธีสารเพิ่มเติม โดยข้อ 8 วรรค 1 กำหนดให้ บทบัญญัติบางส่วนของอนุสัญญากรุงบูดาเปสต์มีผลบังคับใช้ในพิธีสารเพิ่มเติมด้วย บทบัญญัติดังกล่าวได้แก่ บทบัญญัติว่าด้วยคำจำกัดความ ความรับผิดของนิติบุคคล มาตรการบังคับ เขตอำนาจรัฐ (Federal clause) การแก้ไขปรับปรุงอนุสัญญา การระงับข้อพิพาท และการปรึกษาหารือระหว่างรัฐภาคี ในขณะเดียวกัน ข้อ 8 วรรค 2 ได้กำหนดให้รัฐภาคีของพิธีสารเพิ่มเติมนำมาตรการสืบสวนคดีอาชญากรรมทางคอมพิวเตอร์ตาม ข้อ 14-21 และบทบัญญัติว่าด้วยการให้ความร่วมมือระหว่างประเทศตาม ข้อ 23-35 ของอนุสัญญากรุงบูดาเปสต์มาปรับใช้ด้วย

สำหรับบทสุดท้ายของพิธีสารเพิ่มเติม จะเป็นบทบัญญัติด้านการบริหารพิธีสารโดยทั่วไป อาทิ บทบัญญัติเกี่ยวกับการเข้าผูกพันตามพิธีสารเพิ่มเติมด้วยการลงนามหรือการเข้าภาคยานุวัติ บทบัญญัติที่จำกัดผลการบังคับใช้พิธีสารเพิ่มเติมด้วยการตั้งข้อสงวน การประกาศเขตแดนบังคับใช้ การประกาศตีความรายละเอียดบางส่วน การประกาศเพิกถอนความผูกพันตามพิธีสารเพิ่มเติม และการแจ้งข้อมูลสำคัญต่างๆ บทบัญญัติในการบริหารพิธีสารนี้ มีที่มาจากตัวอย่างบทบัญญัติท้ายสนธิสัญญา (Model Final Clauses) สำหรับอนุสัญญาและข้อตกลงที่จัดทำโดย สภายุโรป ซึ่งได้รับอนุมัติโดยคณะมนตรีสภายุโรปเมื่อเดือน กุมภาพันธ์ 1980 ในที่ประชุม

---

[22] Council of Europe. Additional protocol to the convention on cybercrime explanatory report [Online].

Available from: http://conventions.coe.int/Treaty/EN/Reports/Html/189.htm [2013, May 6], Para.25

[23] *Ibid.*

ผู้แทนครั้งที่ 315[24] ทั้งนี้ พิธีสารเพิ่มเติมจะเปิดให้รัฐที่ลงนามในอนุสัญญากรุงบูดาเปสต์แล้วทำการลงนามเท่านั้น

3.2 การส่งตัวผู้ร้ายข้ามแดนภายใต้กรอบอนุสัญญากรุงบูดาเปสต์และพิธีสารเพิ่มเติม

ข้อ 24 วรรค 5 ของอนุสัญญาได้กำหนดให้เงื่อนไขทั่วไปในการส่งตัวผู้ร้ายข้ามแดน อาทิ เหตุแห่งการปฏิเสธไม่ดำเนินการตามคำขอส่งตัวผู้ร้ายข้ามแดนนั้น เป็นไปตามกฎหมายภายในของรัฐผู้รับคำร้องขอ หรือตามสนธิสัญญาการส่งตัวผู้ร้ายข้ามแดนที่มีผลบังคับใช้ ที่เป็นเช่นนี้เพราะอนุสัญญากรุงบูดาเปสต์ ต้องการให้รัฐภาคีต่างๆสามารถดำเนินการตามอนุสัญญาได้อย่างยืดหยุ่นโดยเฉพาะอย่างยิ่งในกรณีที่รัฐมีกฎหมายภายในเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ไว้ก่อนแล้ว อย่างไรก็ตาม ยังมีหลักเกณฑ์เกี่ยวกับการส่งตัวผู้ร้ายข้ามแดนบางประการ ที่อนุสัญญากรุงบูดาเปสต์ได้กำหนดรายละเอียดไว้อย่างเฉพาะเจาะจง บทบัญญัติดังกล่าว มีดังต่อไปนี้

3.2.1 ความผิดที่สามารถส่งตัวผู้ร้ายข้ามแดนได้ตามอนุสัญญากรุงบูดาเปสต์

ข้อ 24 วรรค 1 a ให้รัฐภาคีกำหนดให้ฐานความผิดที่ระบุไว้ในข้อ 2-11 แห่งอนุสัญญาเป็นความผิดที่ถูกส่งตัวข้ามแดนได้ฐานความผิดเหล่านี้จะต้องเป็นความผิดที่สามารถดำเนินการลงโทษได้ตามกฎหมายภายในของรัฐทั้งสองฝ่าย ทั้งนี้ โทษที่ได้รับจากฐานความผิดเหล่านี้ต้องการลงโทษด้วยการจำกัดอิสรภาพที่มีระยะเวลา 1 ปีเป็นอย่างน้อย อย่างไรก็ตาม หากรัฐภาคีมีสนธิสัญญาสัญญาส่งตัวผู้ร้ายข้ามแดนหรือมีข้อตกลงที่มีฐานมาจากกฎหมายในลักษณะต่างตอบแทนซึ่งกำหนดมาตรฐานโทษขั้นต่ำไว้เป็นอย่างอื่น ข้อ 24 วรรค 1 b กำหนดให้รัฐภาคียึดหลักการตามสนธิสัญญาหรือข้อตกลงเหล่านั้นแทน

ข้อ 24 วรรค 2 ของอนุสัญญาจะกำหนดให้ฐานความผิดดังกล่าว เป็นฐานความผิดที่ส่งตัวผู้ร้ายข้ามแดนได้ตามสนธิสัญญาด้านการส่งตัวผู้ร้ายข้ามแดนฉบับใดๆที่มีผลบังคับใช้กันระหว่างรัฐภาคีในปัจจุบัน และในฉบับที่รัฐภาคีจะทำขึ้นต่อไปในอนาคตด้วย ในขณะเดียวกัน ข้อ 24 วรรค 3 กำหนดให้อนุสัญญากรุงบูดาเปสต์เป็นฐานทางกฎหมายสำหรับรัฐที่กำหนดให้

---

[24] *Ibid*., para.48

สนธิสัญญาเป็นเงื่อนไขในการส่งตัวผู้ร้ายข้ามแดนไว้พิจารณาคำร้องขอจากรัฐที่ไม่ได้ทำสนธิสัญญาดังกล่าวกับตนไว้ นอกจากนี้ ข้อ 24 วรรค 4 ยังกำหนดให้รัฐภาคีรับรองให้ความผิดตามข้อ 2-11 ของอนุสัญญาเป็นความผิดที่ส่งตัวข้ามแดนได้ ถ้าหากรัฐเหล่านั้นไม่ได้กำหนดให้สนธิสัญญาส่งตัวผู้ร้ายข้ามแดนเป็นเงื่อนไขสำหรับการดำเนินการ

ฐานความผิดที่ส่งตัวผู้ร้ายข้ามแดนตามอนุสัญญากรุงบูดาเปสต์นั้น แบ่งออกได้เป็นสี่ประเภทได้แก่ ความผิดต่อความลับ ความสมบูรณ์ และความพร้อมใช้งานของข้อมูลและระบบคอมพิวเตอร์ (Offences against Confidentiality Integrity and Availability หรือ C.I.A. offences) การกระทำผิดที่เกี่ยวข้องกับคอมพิวเตอร์ (Computer-related offences) การกระทำความผิดที่เกี่ยวข้องกับเนื้อหา (Content-related offences) และการกระทำผิดที่เกี่ยวข้องกับการละเมิดลิขสิทธิ์และสิทธิข้างเคียง โดยมีรายละเอียดมีดังต่อไปนี้

3.2.1.1 ความผิดต่อความลับ ความสมบูรณ์ และความพร้อมใช้งานของข้อมูลและระบบคอมพิวเตอร์

- **การเข้าถึงโดยผิดกฎหมาย** (Illegal access) ภายใต้ ข้อ 2 ของอนุสัญญากรุงบูดาเปสต์ การเข้าถึงโดยผิดกฎหมายเป็นการเข้าถึงระบบคอมพิวเตอร์บางส่วนหรือทั้งระบบโดยปราศจากสิทธิ์ อย่างไรก็ตาม รัฐภาคีของอนุสัญญาสามารถระบุองค์ประกอบความผิดบางประการเพิ่มเติมได้บางประการ อาทิ การละเมิดมาตรการรักษาความปลอดภัยเพื่อเข้าถึงระบบเป้าหมาย เจตนาในการได้มาซึ่งข้อมูลทางคอมพิวเตอร์จากการเข้าถึงระบบโดยผิดกฎหมาย เจตนาทุจริต หรือการกำหนดให้ระบบคอมพิวเตอร์ที่ถูกเข้าถึงนั้นเชื่อมโยงกับระบบคอมพิวเตอร์อื่นๆ

  ทั้งนี้ การกระทำความผิดฐานนี้ไม่ต้องคำนึงว่า ผู้บุกรุกจะกระทำการอย่างอื่นหลังการเข้าถึงโดยผิดกฎหมายต่อไปหรือไม่ ทั้งนี้ เพราะการกระทำดังกล่าวสามารถสร้างความขัดข้องให้แก่การทำงานของระบบคอมพิวเตอร์และขัดขวางการทำงานของผู้มีอำนาจเข้าถึงระบบคอมพิวเตอร์ได้แล้ว นอกจากนี้ การเข้าถึงระบบข้อมูลคอมพิวเตอร์โดยผิดกฎหมายยังส่งผลให้อาชญากรรับรู้ถึงข้อมูลที่อยู่ภายในระบบคอมพิวเตอร์โดยมิชอบได้

- **การดักรับข้อมูลโดยผิดกฎหมาย** (Illegal Interception) ข้อ 3 ของอนุสัญญากำหนดให้ความผิดฐานนี้เป็นการใช้วิธีการทางเทคนิคเพื่อดักรับข้อมูลคอมพิวเตอร์ที่ถูกส่งผ่านกันภายในหรือระหว่างระบบคอมพิวเตอร์ในลักษณะที่ไม่ได้เปิดเผยสู่สาธารณะ ซึ่งรวมไปถึงการดักรับคลื่นแม่เหล็กไฟฟ้าที่แผ่มาจากระบบคอมพิวเตอร์ที่มีระบบคอมพิวเตอร์นั้นอยู่ด้วย การดักรับข้อมูลที่เป็นความผิดต้องกระทำโดยเจตนาและปราศจากสิทธิ ตัวอย่างของการใช้วิธีการทางเทคนิคได้แก่ การติดตั้งอุปกรณ์บนสายส่งการสื่อสาร การใช้เครื่องมือเพื่อรวบรวมและบันทึกการสื่อสารแบบไร้สาย และการใช้ซอฟต์แวร์ รหัสผ่าน และรหัสอื่นๆ องค์ประกอบด้านการใช้วิธีการทางเทคนิคนั้นขึ้นเพื่อไม่ให้ฐานความผิดมีขอบเขตกว้างเกินไป[25]

  นอกจากนี้ รัฐภาคีอนุสัญญายังสามารถกำหนดองค์ประกอบความผิดเพิ่มเติมได้ในเรื่องเจตนาทุจริต หรือกำหนดเพิ่มเติมว่าระบบคอมพิวเตอร์ที่เป็นเป้าหมายนั้นเชื่อมโยงกับระบบคอมพิวเตอร์อื่นได้ จะเห็นได้ว่าการกระทำความผิดในฐานนี้สามารถเทียบเคียงได้กับกรณีการดักฟังโทรศัพท์เพื่อฟังบทสนทนาของคู่สนทนา ตามกฎหมายอาญาแบบดั้งเดิม[26]

- **การเข้าแทรกแซงข้อมูลคอมพิวเตอร์** (Data Interception) ข้อ 4 ของอนุสัญญาได้กำหนดให้การแทรกแซงข้อมูลเป็นการสร้างความเสียหาย การลบทิ้ง การทำลาย การดัดแปลง หรือการระงับยับยั้งข้อมูลทางคอมพิวเตอร์โดยปราศจากสิทธิ ทั้งนี้ การสร้างความเสียหายและการทำลาย หมายถึงการสร้างผลกระทบเชิงลบให้แก่บูรณภาพของเนื้อหาของข้อมูลและโปแกรมคอมพิวเตอร์ การลบทิ้งเป็นการทำลายข้อมูลทั้งหมดและทำให้ผู้ใช้ไม่สามารถข้อมูลดังกล่าวได้ ส่วนการระงับยับยั้งข้อมูลหมายถึงการทำให้ข้อมูลดังกล่าวไม่อยู่ในสภาพพร้อมใช้งานสำหรับบุคคลผู้ใช้คอมพิวเตอร์หรือใช้สื่อกลางที่เก็บข้อมูลนั้นไว้ สำหรับคำว่าดัดแปลงนั้น หมายถึงการเปลี่ยนข้อมูลที่มีอยู่ให้แตกต่างไปจากเดิม[27]

---

[25] Council of Europe. Convention on cybercrime explanatory report , Para.53

[26] *Ibid*., Para. 51

[27] *Ibid*., Para. 61

อย่างไรก็ดี รัฐภาคีสามารถระบุองค์ประกอบความผิดเพิ่มเติมไปได้ว่าการกระทำเหล่านี้ต้องก่อให้เกิดความเสียหายร้ายแรงเสียก่อนถึงจะเป็นความผิดได้ ตัวอย่างของการกระทำนี้ได้แก่ การปล่อยไวรัสเพื่อทำลายข้อมูลทางคอมพิวเตอร์ หรือการใช้โปรแกรมม้าโทรจัน เป็นต้น

- **การแทรกแซงระบบทางคอมพิวเตอร์** ข้อ 5 ของอนุสัญญาได้กำหนดรายละเอียดของการกระทำผิดฐานนี้ไว้ว่าเป็นการขัดขวางการทำงานของระบบคอมพิวเตอร์อย่างร้ายแรงด้วยการกระทำการต่างๆต่อข้อมูลคอมพิวเตอร์โดยเจตนา ไม่ว่าจะเป็นการใส่ข้อมูล ส่งข้อมูล ทำให้ข้อมูลเสียหาย ลบทิ้ง ทำให้เสื่อมสภาพ ดัดแปลง หรือระงับยับยั้งข้อมูล ทั้งนี้ รัฐภาคีจะต้องพิจารณาเกณฑ์ในการกำหนดว่า การขัดขวางการทำงานนั้นร้ายแรงหรือไม่ อาทิ การกำหนดจำนวนความเสียหายขั้นต่ำ ขอบเขตระบบคอมพิวเตอร์ที่ได้รับผลกระทบ หรือความระยะเวลาของผลกระทบ เป็นต้น[28] ในขณะเดียวกัน ผู้ร่างสัญญาเห็นว่าความร้ายแรง สามารถพิจารณาได้จากรูปแบบ ขนาด และความถี่ของการส่งข้อมูลไปแทรกแซงระบบคอมพิวเตอร์ที่เป็นเป้าหมายด้วย[29] สำหรับงการส่งสแปมนั้น จะเป็นการส่งจดหมายที่ไม่พึงประสงค์เพื่อจุดประสงค์ต่างๆ ในปริมาณมากด้วยความถี่สูง อย่างไรก็ตาม ผู้ร่างอนุสัญญาได้ให้ความเห็นว่าการกระทำดังกล่าวจะเป็นความผิดทางอาญาตามความผิดฐานนี้ต่อเมื่อการสื่อสารของระบบคอมพิวเตอร์เป้าหมายนั้นถูกทำให้ขัดข้องอย่างร้ายแรงโดยที่ผู้กระทำผิดมีเจตนาเท่านั้น[30]

- **การใช้อุปกรณ์ในทางมิชอบ** ข้อ 6 วรรค 1 ของอนุสัญญากำหนดนิยามของอุปกรณ์ที่ใช้ในการก่ออาชญากรรมทางคอมพิวเตอร์ไว้ว่า เป็นอุปกรณ์ซึ่งรวมไปถึงโปรแกรมคอมพิวเตอร์ที่ถูกออกแบบหรือดัดแปลงเพื่อกระทำความผิดฐานต่างๆที่ละเมิดต่อความลับ บูรณภาพ และความพร้อมใช้งาน ได้แก่การเข้าถึงระบบคอมพิวเตอร์ การดักรับข้อมูลโดยผิดกฎหมาย ฯการเข้าแทรกแซงข้อมูลและระบบคอมพิวเตอร์ อุปกรณ์เหล่านี้ยังรวมไปถึงรหัสผ่านคอมพิวเตอร์หรือข้อมูลลักษณะคล้ายคลึงกันสำหรับเข้าถึงระบบคอมพิวเตอร์ทั้งหมดหรือบางส่วน

---

[28] *Ibid*., Para. 67

[29] *Ibid*., Para. 67

[30] *Ibid*., Para. 69

การทำความผิดฐานใช้อุปกรณ์โดยมิชอบจะแบ่งออกเป็นสองกรณี กรณีแรกคือการผลิต ขาย จัดซื้อเพื่อนำมาใช้งาน ส่งออก จัดจำหน่าย หรือจัดหาซึ่งอุปกรณ์ดังกล่าวโดยเจตนาและปราศจากสิทธิ ส่วนกรณีที่สองนั้นคือการครอบครองอุปกรณ์ดังกล่าวโดยมีเจตนาและปราศจากสิทธิ เพื่อนำไปใช้กระทำความผิดฐานการเข้าถึงระบบคอมพิวเตอร์ การดักรับข้อมูลโดยผิดกฎหมาย การเข้าแทรกแซงข้อมูลและระบบคอมพิวเตอร์ ในส่วนนี้ รัฐภาคีสามารถกำหนดจำนวนขั้นต่ำของอุปกรณ์ที่มีในครอบครองที่ก่อให้เกิดความผิดได้ อย่างไรก็ดี ถ้าการกระทำดังข้างต้นไม่มีเจตนาเพื่อกระทำความผิดอยู่ด้วย อาทิ เพื่อทำการทดสอบโดยได้รับอนุญาต หรือเพื่อการป้องระบบคอมพิวเตอร์ การกระทำเหล่านั้นย่อมไม่นับว่าผิดกฎหมาย

ข้อ 6 วรรคสามของอนุสัญญากำหนดให้รัฐภาคีสามารถตั้งข้อสงวนในความผิดฐานการใช้อุปกรณ์ในทางมิชอบตามข้อ 6 วรรค 1 ของอนุสัญญาได้ อย่างไรก็ตามข้อสงวนดังกล่าวจะต้องไม่เกี่ยวกับการขาย การจัดจำหน่าย หรือการจัดหารหัสผ่านคอมพิวเตอร์หรือข้อมูลลักษณะคล้ายคลึงกันที่ใช้ในการเข้าถึงระบบคอมพิวเตอร์ทั้งหมดหรือบางส่วน

3.2.1.2 **การกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์**

- **การปลอมแปลงที่เกี่ยวข้องกับคอมพิวเตอร์** ข้อ 7 ของอนุสัญญาได้กำหนดว่าการปลอมแปลงที่เกี่ยวข้องกับคอมพิวเตอร์คือ การใส่ข้อมูล ดัดแปลง ลบทิ้งหรือระงับยับยั้งข้อมูลทางคอมพิวเตอร์โดยเจตนาและปราศจากสิทธิ ซึ่งส่งผลให้ได้มาซึ่งข้อมูลที่ถูกปลอมแปลง โดยผู้กระทำความผิดมีเจตนาพิเศษที่ให้ข้อมูลปลอมได้รับการพิจารณาหรือนำไปดำเนินการเพื่อวัตถุประสงค์ทางกฎหมายราวกับว่าข้อมูลดังกล่าวเป็นของจริง ทั้งนี้ ไม่ต้องคำนึงว่าข้อมูลนั้นจะอ่านได้โดยตรงหรือสามารถเป็นที่เข้าใจได้ดีหรือไม่ สำหรับความผิดฐานนี้ รัฐภาคีสามารถกำหนดองค์ประกอบความผิดเพิ่มเติมให้ผู้กระทำผิดมีเจตนาฉ้อฉลหรือเจตนาทุจริตเพิ่มเติมเข้าไปด้วยได้

- **การฉ้อโกงที่เกี่ยวกับคอมพิวเตอร์** ข้อ 8 ของอนุสัญญากำหนดไว้ว่าความผิดฐานนี้คือการทำให้ผู้อื่นเสียทรัพย์โดยเจตนาและปราศจากสิทธิ ด้วยวิธีการใส่ ดัดแปลง ลบทิ้ง

หรือ ระงับยับยั้งข้อมูลทางคอมพิวเตอร์ หรือการแทรกแซงการทำงานของระบบคอมพิวเตอร์ ทั้งนี้ ผู้กระทำผิดต้องมีเจตนาพิเศษให้ตนเองหรือบุคคลที่สามได้รับผลประโยชน์ทางเศรษฐกิจโดยปราศจากสิทธิ

3.2.1.3 **การกระทำผิดที่เกี่ยวข้องกับเนื้อหา**

- **การกระทำความผิดเกี่ยวกับวัตถุลามกอนาจารเด็ก** ข้อ 9 วรรค 2 ได้นิยามว่าวัตถุลามกอนาจารเด็กนั้นครอบคลุมถึงวัตถุลามกอนาจารที่แสดงให้เห็นภาพผู้เยาว์ บุคคลที่ดูคล้ายผู้เยาว์ หรือภาพเสมือนจริงของผู้เยาว์ ที่กำลังเข้าร่วมกิจกรรมทางเพศอย่างเปิดเผย ทั้งนี้ข้อ 9 วรรค 3 ได้กำหนดกรอบอายุไว้ว่า"ผู้เยาว์"คือบุคคลที่อายุต่ำกว่า 18 ปี อย่างไรก็ดี รัฐภาคีสามารถกำหนดขอบเขตอายุให้ต่ำกว่าที่อนุสัญญากำหนดได้ แต่ต้องไม่ต่ำไปกว่า 16 ปี

การกระทำที่เป็นความผิดเกี่ยวกับวัตถุลามกอนาจารเด็กตามอนุสัญญาฉบับนี้ ประกอบด้วย การผลิตเพื่อเผยแพร่ผ่านทางระบบคอมพิวเตอร์ นำเสนอหรือจัดหาผ่านทางระบบคอมพิวเตอร์ เผยแพร่หรือส่งผ่านระบบคอมพิวเตอร์ การทำให้ได้มาซึ่งวัตถุลามกอนาจารผ่านทางระบบคอมพิวเตอร์เพื่อตัวเองหรือบุคคลอื่น และการมีวัตถุลามกอนาจารไว้ในครอบครองในระบบคอมพิวเตอร์หรือตัวกลางสำหรับเก็บข้อมูลทางคอมพิวเตอร์

อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ข้อ 9 วรรค 4 ได้อนุญาตให้ รัฐภาคีตั้งข้อสงวนที่จะไม่นำบทบัญญัติว่าด้วยความผิดสำหรับการทำให้ได้มาซึ่งวัตถุลามกอนาจารผ่านทางระบบคอมพิวเตอร์เพื่อตัวเองหรือบุคคลอื่น และการมีวัตถุลามกอนาจารไว้ในครอบครองในระบบคอมพิวเตอร์หรือตัวกลางสำหรับเก็บข้อมูลทางคอมพิวเตอร์มาปรับใช้ทั้งหมดหรือบางส่วนด้วย นอกจากนี้ รัฐภาคียังสามารถตั้งข้อสงวนทั้งหมดหรือบางส่วนในกรณีของบุคคลที่ดูคล้ายผู้เยาว์ หรือภาพเสมือนจริงของผู้เยาว์ได้ด้วย

3.2.1.4 การกระทำผิดที่เกี่ยวข้องกับการละเมิดลิขสิทธิ์และสิทธิข้างเคียง

ข้อ 10 ของอนุสัญญากำหนดให้ความผิดฐานนี้เป็นการละเมิดลิขสิทธิ์และสิทธิข้างเคียงตามสนธิสัญญากฎหมายทรัพย์สินทางปัญญา ต่างๆที่รัฐเป็นภาคี สนธิสัญญาดังกล่าวได้แก่ อนุสัญญาลิขสิทธิ์สากลฉบับแก้ไข ณ กรุงปารีส เมื่อวันที่ 24 กรกฎาคม พ.ศ. 2514 ความตกลงว่าด้วยสิทธิในทรัพย์สินทางปัญญาด้านการค้า(ทริปส์),สนธิสัญญาลิขสิทธิ์และสนธิสัญญาการแสดงและสิ่งบันทึกเสียงขององค์การทรัพย์สินทางปัญญาแห่งโลก(WIPO) แต่ไม่รวมไปถึงส่วนของธรรมสิทธิ์ (moral rights) ตามสนธิสัญญาดังกล่าว การละเมิดลิขสิทธิ์และสิทธิข้างเคียงนั้นจะต้องอยู่ในระดับทัดเทียมการค้า (on a commercial scale) นอกจากนี้ยังต้องได้ใช้วิธีการด้านระบบคอมพิวเตอร์ประกอบการละเมิดด้วย สำหรับความผิดฐานนี้ รัฐภาคีสามารถตั้งข้อสงวนได้ หากแต่ต้องมีหนทางการเยียวยาที่มีประสิทธิภาพเตรียมเอาไว้และข้อสงวนดังกล่าวจะต้องไม่เป็นส่งผลกระทบต่อพันธะกรณีตามสนธิสัญญาด้านทรัพย์สินทางปัญญาระหว่างประเทศดังข้างต้น

นอกจากฐานความผิดทั้ง 4 ประเภทดังข้างต้นแล้ว ข้อ 11 วรรค 1 ของอนุสัญญาได้กำหนดให้ผู้สนับสนุนหรือผู้ใช้ในการก่ออาชญากรรมโดยเจตนาต้องรับผิดด้วย ในขณะเดียวกันข้อ 11 วรรค 2 กำหนดให้รัฐภาคีกำหนดความผิดทางอาญาให้แก่ผู้ที่พยายามทำความผิดตามข้อ 3-5, 7,8, และ 9 วรรค 1 a และ c ของอนุสัญญา อย่างไรก็ตาม รัฐภาคีสามารถตั้งข้อสงวนในส่วนผู้พยายามกระทำความผิดได้เช่นกัน

3.2.2 ความผิดที่สามารถส่งตัวผู้ร้ายข้ามแดนได้ตามตามพิธีสารเพิ่มเติมอนุสัญญากรุงบูดาเปสต์

3.2.2.1 การเผยแพร่วัตถุที่มีลักษณะเหยียดหยามหรือเกลียดชังเชื้อชาติผ่านทางระบบคอมพิวเตอร์

ภายใต้ข้อ 3 วรรค 1 ของพิธีสารเพิ่มเติม การกระทำความผิดลักษณะนี้ คือการเผยแพร่หรือจัดหาวัตถุที่มีลักษณะเหยียดหยามหรือเกลียดชังเชื้อชาติผ่านทางระบบคอมพิวเตอร์ออกสู่สาธารณชน ทั้งนี้ ความหมายของการจัดหานั้นครอบคลุมไปถึง การสร้างหรือรวบรวมช่องทางพิเศษสำหรับอำนวยความสะดวกให้ผู้อื่นเข้าถึงวัตถุที่มีลักษณะเหยียดหยาม

หรือเกลียดชังเชื้อชาติด้วย[31] อย่างไรก็ตาม หากการเผยแพร่วัตถุดังกล่าวนั้น กระทำผ่านทางช่องทางการสื่อสารส่วนบุคคล จะไม่ตกเป็นความผิดตามบทบัญญัตินี้ เนื่องจากได้รับการปกป้องในฐานะสิทธิส่วนบุคคลตาม ข้อ 8 ของอนุสัญญาสิทธิมนุษยชนแห่งยุโรป (European Convention on Human Rights)[32] การพิจารณาว่าผู้กระทำผิดได้ใช้ช่องทางการสื่อสารส่วนตัวหรือเผยแพร่สู่สาธารณชนนั้น ให้พิจารณาจากปัจจัยแวดล้อมต่างๆ อาทิ เจตนาของผู้กระทำการว่า ตนตั้งใจให้วัตถุดังกล่าวไปถึงเฉพาะผู้รับที่ต้องการหรือไม่ ตัวเนื้อหา เทคโนโลยีที่ใช้ส่งข้อมูล มาตรการรักษาความปลอดภัยที่ใช้ประกอบ และบริบทในขณะที่มีการส่งข้อมูลนั้น เป็นต้น[33]

ข้อ 3 วรรค 2 อนุญาตให้รัฐภาคีสามารถตั้งข้อสงวนได้ หากวัตถุดังกล่าว ส่งเสริม สนับสนุน หรือกระตุ้นให้เกิดการเลือกปฏิบัติในลักษณะที่ไม่เกี่ยวข้องกับความเกลียดชังหรือการใช้ความรุนแรง หากแต่ต้องเตรียมมาตรการเยียวยาอื่นๆที่มีประสิทธิภาพ เช่น มาตรการเยียวยาทางแพ่งหรือทางปกครอง ไว้รองรับ[34] นอกจากนี้ ข้อ 3 วรรค3 อนุญาตให้รัฐภาคีสามารถตั้งข้อสงวนที่จะไม่กำหนดฐานความผิดสำหรับการเลือกปฏิบัติที่รัฐไม่สามารถกำหนดมาตรการเยียวยาอื่นมารองรับ อันเป็นผลมาจากหลักกฎหมายภายในว่าด้วยเสรีภาพในการแสดงออก

---

[31] Council of Europe. Additional protocol to the convention on cybercrime explanatory report, Para.28

[32] European Convention on Human Rights, Art.8:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[33] Council of Europe. Additional protocol to the convention on cybercrime explanatory report, Para.30

[34] *Ibid*., para. 31

3.2.2.2 การข่มขู่ที่มีลักษณะเหยียดหยามหรือเกลียดชังเชื้อชาติ

ข้อ 4 ของพิธีสารเพิ่มเติม กำหนดให้ความผิดลักษณะนี้ คือการข่มขู่บุคคลหรือกลุ่มบุคคลผ่านทางระบบคอมพิวเตอร์ว่าจะกระทำการที่เป็นความผิดร้ายแรงตามกฎหมายภายในรัฐภาคี โดยอาศัยเหตุแห่งเชื้อชาติสีผิว เชื้อสายบรรพบุรุษ เชื้อชาติ หรือเผ่าพันธุ์ของฝ่ายผู้ถูกข่มขู่ อีกทั้งรวมไปถึงเหตุแห่งศาสนาด้วยในกรณีที่ศาสนาถูกนำไปใช้เป็นเชื่อมโยงกับเหตุปัจจัยประการอื่นๆดังข้างต้น

3.2.2.3 การดูหมิ่นที่มีลักษณะเหยียดหยามหรือเกลียดชังเชื้อชาติ

ข้อ 5 วรรค 1 กำหนดให้ความผิดลักษณะนี้คือการดูหมิ่นบุคคลหรือกลุ่มบุคคลผ่านทางระบบคอมพิวเตอร์อย่างเปิดเผยสู่สาธารณะ ทั้งนี้โดยอาศัยเหตุแห่งเชื้อชาติ สีผิว เชื้อสายบรรพบุรุษ เชื้อชาติ หรือเผ่าพันธุ์ของฝ่ายผู้ถูกข่มขู่ ทั้งนี้ รวมไปถึงเหตุแห่งศาสนาด้วยในกรณีที่ศาสนาถูกนำไปใช้เชื่อมโยงกับเหตุปัจจัยประการอื่นๆดังข้างต้น จะสังเกตเห็นได้ว่าหากการดูหมิ่นที่กระทำผ่านช่องทางสื่อสารส่วนตัว จะไม่เป็นความผิดตามข้อ 5 วรรค 1 นี้[35]

อย่างไรก็ดี ข้อ 5 วรรค 2 a อนุญาตให้รัฐภาคี กำหนดองค์ประกอบความผิดเพิ่มเติมได้ว่าการดูหมิ่นดังข้างต้นจะต้องส่งผลกระทบให้ฝ่ายผู้ถูกดูหมิ่นเสี่ยงต่อการถูกรังเกียจ ดูถูกเหยียดหยาม หรือล้อเลียน นอกจากนี้ข้อ 5 วรรค 2 b อนุญาตให้รัฐภาคีตั้งข้อสงวนสำหรับการกระทำความผิดฐานนี้ได้ทั้งหมดหรือบางส่วนด้วย

3.2.2.4 การปฏิเสธ บิดเบือน เห็นด้วย หรือแก้ต่างให้กับการฆ่าล้างเผ่าพันธุ์หรืออาชญากรรมต่อมนุษยชาติ

ข้อ 6 วรรค 1 ของพิธีสารเพิ่มเติมได้กำหนดฐานความผิดสำหรับการแจกจ่ายหรือจัดหาวัตถุออกสู่สาธารณชนผ่านทางระบบคอมพิวเตอร์ เนื้อหาของวัตถุดังกล่าวนี้ต้องเป็นการกล่าวปฏิเสธ การลดความรุนแรงอย่างร้ายแรง การเห็นด้วยหรือแก้ต่างให้กับการกระทำที่เป็นการฆ่าล้างเผ่าพันธุ์หรืออาชญากรรมต่อมวลมนุษยชาติ ทั้งนี้ ให้พิจารณาคำจำกัดความ

---

[35] *Ibid*., Para 36

ของการฆ่าล้างเผ่าพันธุ์หรืออาชญากรรมต่อมวลมนุษยชาติได้จากกฎหมายระหว่างประเทศ และจากคำพิพากษาที่ถึงที่สุดและมีผลผูกพันของศาลระหว่างประเทศต่างๆ ที่ถูกจัดตั้งโดยตราสารระหว่างประเทศเช่นสนธิสัญญาพหุภาคี อีกทั้งได้รับการรับรองเขตอำนาจศาลโดยรัฐภาคีด้วย ตัวอย่างของศาลเหล่านี้ได้แก่ คณะตุลาการทหารระหว่างประเทศที่จัดตั้งโดยข้อตกลงกรุงลอนดอน เมื่อวันที่ 8 สิงหาคม 1945 หรือคณะตุลาการนูเรมเบิร์ก คณะตุลาการอาญาระหว่างประเทศสำหรับอดีตประเทศยูโกสลาเวีย (ICTY) คณะตุลาการอาญาระหว่างประเทศสำหรับประเทศรวันดา(ICTR) หรือ ศาลอาญาระหว่างประเทศ (ICC) เป็นต้น

อย่างไรก็ดี ข้อ 6 วรรค 2 ได้อนุญาตให้รัฐภาคี สามารถกำหนดรายละเอียดสำหรับการกล่าวปฏิเสธ หรือลดความรุนแรงของการฆ่าข้างเผ่าพันธุ์อย่างร้ายแรงได้ว่าผู้กระทำความผิดต้องมีเจตนากระตุ้นให้เกิดความเกลียดชัง การเลือกปฏิบัติ หรือการก่อความรุนแรงแก่บุคคลหรือกลุ่มโดยอาศัยเหตุแห่งเชื้อชาติ สีผิว เชื้อสายบรรพบุรุษ เชื้อชาติหรือเผ่าพันธุ์ ทั้งนี้ รวมไปถึงเหตุแห่งศาสนาด้วยในกรณีที่ศาสนาถูกนำไปใช้เชื่อมโยงกับเหตุปัจจัยดังข้างต้น

3.2.3 **การกล่าวอ้างเขตอำนาจรัฐ**

เขตอำนาจรัฐเป็นปัจจัยสำคัญในการให้ความร่วมมือกันทางอาญาระหว่างประเทศ เพราะรัฐผู้รับคำขอส่งตัวผู้ร้ายข้ามแดนหรือคำขอความช่วยเหลือร่วมกันทางกฎหมายนั้นจะต้องยอมรับว่ารัฐผู้ส่งคำร้องขอดังกล่าวนั้นมีเขตอำนาจเหนือคดีตามคำขอเสียก่อน ในการนี้ข้อ 22 ของอนุสัญญาจึงวางแนวทางการกล่าวอ้างเขตอำนาจของรัฐภาคีไว้ในทิศทางเดียวกัน โดยทางผู้ร่างอนุสัญญาพยายามที่จะนำหลักกฎหมายระหว่างประเทศเรื่องเขตอำนาจมาปรับใช้กับบริบทของอาชญากรรมทางคอมพิวเตอร์ แทนที่จะเลือกกำหนดหลักการแบบพิเศษเฉพาะบริบทของอาชญากรรมประเภทนี้ เพื่อไม่ให้ส่งผลกระทบต่อกฎหมายเดิมของรัฐต่างๆ และหลีกเลี่ยงความยุ่งยากจากการเจรจาระหว่างรัฐภาคีเพื่อแสวงหาหลักกฎหมายใหม่สำหรับอาชญากรรมทางคอมพิวเตอร์ได้

ทั้งนี้ ข้อ22 a กำหนดให้รัฐภาคีกำหนดเขตอำนาจเหนือฐานความผิดตาม ข้อ 2-11 ที่กระทำขึ้นในดินแดนของตน ซึ่งเป็นไปตามหลักดินแดนในหลักกฎหมายเรื่องเขตอำนาจรัฐ

ในการนี้ รัฐผู้กำหนดเขตอำนาจรัฐอาจจะพิจารณาตำแหน่งของผู้ที่กระทำความผิดหรือตำแหน่งของคอมพิวเตอร์ที่ได้รับความเสียหายจากการกระทำความผิดก็ได้[36] เพื่อไม่ให้เกิดความยุ่งยากในปฏิบัติตามอนุสัญญา ผู้ร่างอนุสัญญาตัดสินใจไม่กำหนดให้หน่วยงานผู้บังคับใช้กฎหมายของรัฐๆหนึ่ง ต้องขอหมายศาลจากรัฐทุกรัฐที่สัญญาณทางอิเล็กทรอนิกส์เดินทางผ่าน เพราะยุ่งยากและเสียเวลา ในขณะที่การรวบรวมข้อมูลหลักฐานและระบุตัวอาชญากรทางคอมพิวเตอร์นั้นต้องกระทำภายใต้เวลาอันจำกัด[37] นอกจากนี้ แม้ในปัจจุบัน ดาวเทียมจะมีบทบาทในการรับส่งสัญญาณและติดต่อสื่อสารกันทางคอมพิวเตอร์ ผู้ร่างอนุสัญญาเห็นว่าไม่จำเป็นต้องนำประเด็นสัญชาติของดาวเทียมมาพิจารณาในประเด็นการกำหนดเขตอำนาจรัฐ เพราะจุดเริ่มต้นและปลายทางการสื่อสารยังคงอยู่บนพื้นโลก[38]

ข้อ 22 b และ c ยังกำหนดให้รัฐภาคีกำหนดเขตอำนาจสำหรับการกระทำความผิดบนเรือที่ชักธงของตน หรือเครื่องบินที่จดทะเบียนตามกฎหมายภายในของตนตามหลักกึ่งดินแดน (Quasi territorial jurisdiction) ซึ่งถือว่ารัฐมีอำนาจเหนือเรือที่ชักธงของตนและอากาศยานที่จดทะเบียนตามกฎหมายของตน รวมไปถึงบุคคลและทรัพย์สินที่อยู่ในพาหนะเหล่านั้น

ส่วนข้อ 22 d ได้กำหนดเพิ่มเติมให้รัฐภาคีกำหนดเขตอำนาจสำหรับการกระทำความผิดโดยคนชาติของตนที่เกิดนอกเขตแดนรัฐได้ในกรณีที่ความผิดดังกล่าวเป็นความผิดที่ลงโทษได้ตามกฎหมายภายในของรัฐที่ซึ่งความผิดได้เกิดขึ้น หรือในกรณีที่การกระทำผิดเกิดนอกเขตอำนาจทางดินแดนของรัฐใดๆ ทั้งนี้ รัฐภาคีสามารถตั้งข้อสงวนเกี่ยวกับการกล่าวอ้างเขตอำนาจตามข้อ 22 b,c,d

ข้อ 22 วรรค 3 ของอนุสัญญา ได้กำหนดให้รัฐภาคีดำเนินมาตรการเท่าที่จำเป็นเพื่อให้ตนสามารถมีเขตอำนาจเหนือฐานความผิดตามข้อ 2-11 ของอนุสัญญา อีกทั้งยังสามารถดำเนินคดีต่อบุคคลที่ตนได้ปฏิเสธคำขอส่งตัวผู้ร้ายข้ามแดนโดยอาศัยเหตุแห่งสัญชาติได้

---

[36] Council of Europe. Convention on cybercrime explanatory report, Para. 233

[37] Shannon L. Hopkins, “Cybercrime convention: A positive beginning to a long road ahead” Journal of High Technology Law, 2,101 (2003): 7

[38] Council of Europe. Convention on cybercrime explanatory report, Para. 234

หลักกฎหมายในข้อนี้เป็นไปตามหลัก Aut Dedere Aut Judicare ที่กำหนดให้รัฐสามารถดำเนินการสืบสวนและดำเนินคดีต่อบุคคลตามคำขอถ้าหากตนได้ปฏิเสธการส่งตัวผู้ร้ายข้ามแดน

แนวทางการกล่าวอ้างเขตอำนาจรัฐเหนือคดีอาชญากรรมทางคอมพิวเตอร์ตามข้อ 22 ของอนุสัญญาจะครอบคลุมเฉพาะฐานความผิด ตามข้อ 2-11 ของอนุสัญญาเท่านั้น ไม่ได้ครอบคลุมกรณีประเภทอื่นๆที่ใช้คอมพิวเตอร์เป็นเครื่องมือแต่อย่างใด

นอกจากวิธีการที่อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์กำหนดแล้ว ข้อ 22 วรรค 4 อนุญาตให้รัฐภาคีสามารถนำหลักเกณฑ์อื่นที่สอดคล้องกับกฎหมายภายในมากล่าวอ้างเขตอำนาจของตนได้อีกด้วย

ท้ายที่สุด อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์กำหนดให้รัฐต่างๆ ที่ได้รับผลกระทบจากอาชญากรรมทางคอมพิวเตอร์ปรึกษาหารือกันเพื่อหารัฐที่เหมาะสมต่อการดำเนินคดีต่อผู้กระทำผิด ซึ่งจะช่วยลดการดำเนินการซ้ำซ้อนกันระหว่างหน่วยงานของแต่ละรัฐ ในขณะเดียวกัน รัฐภาคีสามารถที่จะเลือกแบ่งกันดำเนินคดีต่อผู้กระทำผิดได้หากก่อให้เกิดผลดีกว่า[39] การปรึกษาหารือดังข้างต้นต้องอาศัยความยินยอมของรัฐที่เกี่ยวข้องและรัฐภาคีไม่ได้มีหน้าที่อย่างเด็ดขาดในการปรึกษาหารือในเรื่องดังกล่าว อย่างไรก็ดี อนุสัญญาไม่ได้กำหนดรายละเอียดเกี่ยวกับวิธีดำเนินการในกรณีที่รัฐไม่ยอมปรึกษาหารือระหว่างกันแต่อย่างใด

3.2.4 การปฏิเสธการส่งตัวผู้ร้ายข้ามแดนด้วยเหตุแห่งสัญชาติ

หากรัฐผู้ร้องขอตัดสินใจปฏิเสธการส่งตัวผู้ร้ายข้ามแดนโดยเหตุแห่งสัญชาติของบุคคลตามคำขอหรือโดยเหตุที่ตนมีเขตอำนาจเหนือความผิดที่เกิด ข้อ 24 วรรค 6 กำหนดให้รัฐผู้รับคำร้องต้องนำคดีดังกล่าวขึ้นสู่ผู้มีอำนาจหน้าที่ดำเนินการเพื่อดำเนินคดีต่อผู้กระทำผิดหน่วยงานรัฐผู้มีอำนาจหน้าที่จะต้องตัดสินคดีและดำเนินการสืบสวนหรือดำเนินกระบวนการพิจารณาคดีเสมือนดังคดีความผิดตามกฎหมายภายในของตน อีกทั้งรายงานผลลัพธ์สุดท้ายให้ฝ่ายรัฐผู้ร้องขอให้ส่งตัวผู้ร้ายข้ามแดนทราบภายในระยะเวลาอันเหมาะสม

---

[39] *Ibid*., Para.239

3.2.5 กระบวนการส่งตัวผู้ร้ายข้ามแดน

เพื่อให้รัฐภาคีดำเนินการด้านการส่งตัวผู้ร้ายข้ามแดนได้อย่างสะดวกรวดเร็วมากขึ้น ข้อ 24 วรรค 7 กำหนดให้รัฐภาคีมีหน้าที่แจ้งชื่อและที่อยู่ของหน่วยงานที่รับส่งและจัดการตามคำขอส่งตัวผู้ร้ายข้ามแดนและจับกุมชั่วคราวไปยังเลขาธิการในขณะที่เข้าเป็นภาคี ไม่ว่าจะด้วยการให้สัตยาบัน หรือภาคยานุวัติ เพื่อให้รัฐต่างๆทราบถึงหน่วยงานที่ตนต้องติดต่อ ทั้งนี้ เลขาธิการสภายุโรปมีหน้าที่รับลงทะเบียนและทำให้ฐานข้อมูลเกี่ยวกับหน่วยงานดังกล่าวให้เป็นปัจจุบัน อย่างไรก็ดี รัฐภาคีก็ยังมีสิทธิที่จะดำเนินการตามช่องทางการทูตอยู่ด้วย[40]

3.3 การให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายทั่วไปใต้กรอบอนุสัญญากรุงบูดาเปสต์

ข้อ 25 วรรค 1 ของอนุสัญญากรุงบูดาเปสต์กำหนดหลักทั่วไปเกี่ยวกับการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายว่า รัฐภาคีต้องให้ความช่วยเหลืออย่างกว้างขวางที่สุดเท่าที่จะทำได้ โดยการให้ความช่วยเหลือจะครอบคลุมอาชญากรรมทุกประเภทที่เกี่ยวข้องกับการใช้ระบบคอมพิวเตอร์และข้อมูลทางคอมพิวเตอร์ อีกทั้งยังรวมไปถึงการรวบรวมหลักฐานในรูปแบบอิเล็กทรอนิกส์ในคดีอาชญากรรมต่างๆจะสังเกตเห็นได้ว่า ขอบเขตดังกล่าวจะกว้างขวางกว่าในกรณีการส่งตัวผู้ร้ายข้ามแดน เพราะการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายนั้น เป็นไปเพื่อการแสวงหาหลักฐานเพื่อระบุตัว จับกุม และดำเนินคดีผู้กระทำความผิด จึงต้องเป็นไปอย่างเร่งด่วนกว่าการส่งตัวผู้ร้ายข้ามแดน ซึ่งตัวผู้กระทำผิดถูกระบุตัวและตัดสินลงโทษแล้ว

ทั้งนี้ ข้อ 25 วรรค 4 ได้กำหนดให้เงื่อนไขสำหรับให้ความช่วยเหลือร่วมกันทางกฎหมายโดยทั่วไป และเหตุแห่งการปฏิเสธความช่วยเหลือ ตามกฎหมายภายในของรัฐผู้รับคำขอความช่วยเหลือ หรือสนธิสัญญาว่าด้วยการให้ความช่วยเหลือร่วมกันทางกฎหมายที่มีผลบังคับใช้ระหว่างรัฐภาคีด้วย เว้นแต่บทบัญญัติของอนุสัญญาจะกำหนดเป็นอย่างอื่น สำหรับการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายโดยทั่วไป หลักเกณฑ์ที่กำหนดไว้โดยเฉพาะเจาะจงมีดังนี้

---

[40] *Ibid*., Para.252

3.3.1 วิธีการดำเนินการให้ความช่วยเหลือ

ข้อ 25 วรรค 3 ได้อนุญาตให้รัฐภาคีสามารถดำเนินการติดต่อหรือร้องขอความช่วยเหลือที่เกี่ยวข้องด้วยการใช้วิธีการติดต่อสื่อสารที่รวดเร็ว อาทิ โทรสาร หรือจดหมายอิเล็กทรอนิกส์ในกรณีที่มีความจำเป็นเร่งด่วน หากแต่ต้องมีการรักษาความปลอดภัยและรับรองความถูกต้อง อาทิ การเข้ารหัสข้อมูลในระดับที่เหมาะสม จากนั้นจึงส่งคำยืนยันอย่างเป็นทางการตามไปภายหลังถ้าหากฝ่ายผู้รับคำขอความช่วยเหลือต้องการ ในทางกลับกัน ฝ่ายผู้รับร้องขอความช่วยเหลือต้องตอบรับคำขอด้วยวิธีการติดต่ออย่างรวดเร็วดังข้างต้นเช่นเดียวกัน

3.3.2 ความผิดที่ไม่สามารถให้ความช่วยเหลือได้

ข้อ 25 ววรค 4ของอนุสัญญาไม่อนุญาตให้รัฐภาคี ปฏิเสธการให้ความช่วยเหลือสำหรับความผิดตาม ข้อ 2-11 ด้วยเพียงเหตุที่การกระทำความผิดตามคำขอนั้นเป็นความผิดทางการเงิน (fiscal offence)

3.3.3 หลักความผิดสองประเทศ

ข้อ 25 วรรค 5 ได้ระบุรายไว้ว่า หากรัฐผู้รับคำขอความช่วยเหลือกำหนดให้หลักความผิดสองประเทศเป็นเงื่อนไขในการให้ความช่วยเหลือ ให้พิจารณาว่าการกระทำที่อยู่เบื้องหลังการกระทำความผิดตามคำขอนั้นเป็นความผิดทางอาญาทางกฎหมายของตนหรือไม่ โดยไม่ต้องพิจารณาต่อไปว่า ความผิดตามคำขอนั้นจัดอยู่ในความผิดประเดียวกัน หรือมีถ้อยคำเรียกฐานความผิดอย่างเดียวกันหรือไม่

จะเห็นได้ว่าอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ได้พยายามผ่อนคลายหลักความผิดสองประเทศ ในการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมาย เพื่อให้ความช่วยเหลือดำเนินไปโดยเร็วกว่ากรณีอาชญากรรมทั่วไป เพราะหลักความผิดสองประเทศนี้ถูกวิจารณ์ว่าเป็นปัจจัยที่สร้างอุปสรรคให้แก่การให้ความร่วมมือทางอาญาระหว่างประเทศ

3.3.4 **การให้ข้อมูลอย่างอย่างทันที** (Spontaneous Information)

ภายใต้ ข้อ 26 ของอนุสัญญา การให้ความช่วยเหลือด้วยวิธีนี้มีลักษณะพิเศษที่ฝ่ายรัฐผู้ให้ความช่วยเหลือเป็นผู้ให้ความช่วยเหลือก่อน แทนที่จะรอรับคำขอความช่วยเหลือแล้วปฏิบัติตามภายหลัง การให้ข้อมูลอย่างทันทีจะเกิดขึ้นเมื่อรัฐภาคีผู้ให้ความช่วยเหลือได้ข้อมูลจากการสืบสวนคดีของตน และเห็นว่าข้อมูลดังกล่าวนี้สามารถช่วยให้รัฐภาคีอื่นสามารถเริ่มต้นหรือดำเนินการสืบสวนหรือดำเนินคดีในฐานความผิดที่สอดคล้องกับอนุสัญญา หรือ อาจนำไปสู่การร้องขอความช่วยเหลือต่อไป

การให้ข้อมูลอย่างทันทีนี้ ได้รับแนวคิดมาจากอนุสัญญาของสภายุโรปฉบับอื่นๆ[41] ได้แก่ ข้อ 10 ของ Convention on the Laundering, Search, Seizure, and Confiscation of the Proceeds of the Crime (ETS. No. 141)[42] และข้อ 28 ของ Criminal Law Convention on Corruption (ETS No. 173)[43] นับได้ว่า การให้ข้อมูลโดยทันทีส่งผลให้การให้ความช่วยเหลือ

---

[41] *Ibid*., Para.260

[42] Convention on the Laundering, Search, Seizure, and Confiscation of the Proceeds of the Crime, Art. 10:

Without prejudice to its own investigations or proceedings, a Party may without prior request forward to another Party information on instrumentalities and proceeds, when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings or might lead to a request by that Party under this chapter.

[43] Criminal Law Convention on Corruption, Art. 28:

Without prejudice to its own investigations or proceedings, a Party may without prior request forward to another Party information on facts when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request by that Party under this chapter.

เป็นไปอย่างรวดเร็วและกว้างขวางมากขึ้น จึงนับเป็นประโยชน์อย่างยิ่งต่อการปราบปรามอาชญากรรมทางคอมพิวเตอร์ที่มีลักษณะข้ามชาติ

ข้อ 26 วรรค 1 และ 2 กำหนดให้รัฐภาคีผู้ให้ข้อมูลโดยทันทีดำเนินการในขอบเขตกฎหมายภายใน และสามารถกำหนดเงื่อนไขให้รัฐผู้รับข้อมูลรักษาความลับหรือกำหนดเงื่อนไขอื่นๆประกอบด้วยได้ หากรัฐผู้รับข้อมูลไม่สามารถปฏิบัติตามเงื่อนไขดังกล่าว ให้แจ้งให้ฝ่ายรัฐผู้ให้ข้อมูลทราบ เพื่อที่จะตัดสินใจในขั้นต่อไปว่าจะให้ข้อมูลดังกล่าวหรือไม่ อย่างไรก็ตาม หากมีการตกลงกัน เงื่อนไขดังกล่าวย่อมมีผลผูกพันทั้งสองฝ่าย ทั้งนี้ รัฐผู้ส่งข้อมูลยังมีสิทธิ์สืบสวนหรือดำเนินคดีต่อผู้กระทำผิดในคดีที่เกี่ยวข้องกับข้อมูลที่ตนส่งไปได้ หากตนมีเขตอำนาจเหนือคดีนั้น[44]

3.3.5 **การให้ความช่วยเหลือในกรณีที่รัฐคู่กรณีไม่ได้ทำข้อตกลงที่เกี่ยวข้องไว้**

ในกรณีที่รัฐภาคีไม่ได้ทำสนธิสัญญาด้านการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมาย หรือข้อตกลงที่มีมีฐานทางกฎหมายในลักษณะต่างตอบแทนในรูปแบบเดียวกันอื่นๆ ซึ่งมีผลบังคับใช้เอาไว้ อนุสัญญาว่าด้วยอาชญากรรมคอมพิวเตอร์ได้กำหนดกฎเกณฑ์พื้นฐานในเรื่องดังกล่าวเอาไว้ในข้อ 27 วรรค 2 ถึง 9 เพื่อให้รัฐนำมาปรับใช้แทน

ในขณะเดียวกัน รัฐภาคีที่ได้จัดทำสนธิสัญญา ข้อตกลงหรือบทบัญญัติทางกฎหมายที่มีผลบังคับใช้ไว้แล้ว สามารถตกลงกันเพื่อนำบทบัญญัติตามข้อ 27 วรรค 2-9 มาใช้ทั้งหมดหรือบางส่วนได้ ทั้งนี้ การปฏิบัติตามกระบวนการที่ข้อ 27 วรรค 2-9 ของอนุสัญญาจะต้องเป็นไปโดยสอดคล้องกับกระบวนการที่ระบุมาโดยรัฐผู้ร้องขอความช่วยเหลือ เว้นเสียแต่ว่าจะขัดกับกฎหมายของรัฐผู้รับคำขอความช่วยเหลือเสียเอง

3.3.5.1 **การจัดตั้งหน่วยงานกลาง**

ข้อ 27 วรรค 2 ของอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์กำหนดให้รัฐภาคีจัดตั้งหน่วยงานกลางขึ้นมาเพื่อทำหน้าที่รับส่งคำขอความช่วยเหลือซึ่งกันและกันทางกฎหมาย อีกทั้งดำเนินการจัดการตามคำขอที่รับมา อย่างไรก็ตาม ถ้าหน่วยงานที่มีอำนาจหน้าที่จัดการ

---

[44] Council of Europe. Convention on cybercrime explanatory report, Para.260

ตามคำขอความช่วยเหลือเป็นหน่วยงานอื่น ให้หน่วยงานกลางที่มีหน้าที่ส่งคำขอไปยังหน่วยงานดังกล่าวเพื่อดำเนินการต่อไป ทั้งนี้ ข้อ 27 วรรค 2 b กำหนดให้หน่วยงานกลางภาคีติดต่อระหว่างกันโดยตรง

นอกจากนี้ เพื่อให้หน่วยงานกลางของรัฐภาคีติดต่อระหว่างกันโดยสะดวกรวดเร็ว อนุสัญญาข้อ 27 วรรค 2 c จึงกำหนดให้รัฐภาคีส่งมอบชื่อและที่อยู่ติดต่อของหน่วยงานที่ทำหน้าที่เป็นหน่วยงานกลางไปยังเลขาธิการของสภายุโรป ในขณะที่ตนเข้าเป็นภาคีอนุสัญญา ทั้งนี้ เลขาธิการสภายุโรปมีหน้าที่รับลงทะเบียนและทำให้ฐานข้อมูลเกี่ยวกับหน่วยงานดังกล่าวให้เป็นปัจจุบัน นอกจากนี้ เพื่อประสิทธิภาพในการดำเนินการ อนุสัญญาข้อ 27 วรรค 9 e กำหนดให้รัฐภาคีแจ้งข้อมูลไปยังเลขาธิการสภายุโรปเมื่อเข้าเป็นภาคีว่า มีคำขอใดบ้างที่ต้องติดต่อไปยังหน่วยงานกลาง ด้วยข้อมูลเหล่านี้ รัฐภาคีสามารถทราบได้ว่าตนต้องติดต่อหน่วยงานใดในกรณีไหนบ้าง

3.3.5.2 **การปฏิเสธและการเลื่อนการให้ความช่วยเหลือ**

ข้อ 24 วรรค 4 แบ่งเหตุแห่งการปฏิเสธการช่วยเหลือเป็นสองกรณี ได้แก่กรณีที่ความผิดทางการเมืองหรือความผิดที่เกี่ยวข้องกับความผิดทางการเมือง และกรณีที่การจัดการตามคำขอนั้นอาจจะกระทบต่ออำนาจอธิปไตย ความมั่นคง ความสงบเรียบร้อยของสังคม หรือผลประโยชน์สำคัญของฝ่ายรัฐผู้รับคำร้องขอความช่วยเหลือ นอกจากนี้ ข้อ 27 วรรค 5 ของอนุสัญญาได้กำหนดให้รัฐผู้รับคำร้องขอเลื่อนกำหนดการปฏิบัติตามร้องขอได้ ถ้าการกระทำดังกล่าวจะส่งผลกระทบต่อการสืบสวนคดีทางอาญาหรือการดำเนินคดีทางอาญาโดยเจ้าหน้าที่รัฐของตน

ในการปฏิเสธหรือเลื่อนกำหนดการให้ความช่วยเหลือ ข้อ 27 วรรค 6 กำหนดให้รัฐผู้รับคำร้องขอต้องปรึกษาฝ่ายผู้ส่งคำขอเสียก่อน เพื่อที่แสวงหาแนวทางที่จะดำเนินการตามคำขอแต่เพียงบางส่วน หรือกำหนดเงื่อนไขอื่นสำหรับการดำเนินการตามที่จำเป็นได้ ข้อกำหนดนี้มีส่วนช่วยให้การให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายเป็นไปอย่างยืดหยุ่นมากขึ้น ในขณะเดียวกัน ข้อ 27 วรรค 7 กำหนดให้รัฐภาคีชี้แจงเหตุผลประกอบการปฏิเสธหรือการเลื่อนการให้ความช่วยเหลือ ซึ่งจะเป็นประโยชน์ต่อการปรึกษาหารือระหว่างกันต่อไป

เมื่อจัดการตามคำขอ ข้อ 27 วรรค 7 กำหนดให้รัฐผู้รับคำร้องขอชี้แจงผลลัพธ์ของการดำเนินการโดยเร็ว ถ้าหากการจัดการตามคำขอตกเป็นพ้นวิสัยหรือต้องล่าช้าอย่างมีนัยยะสำคัญ โดยให้รัฐผู้รับคำร้องขอชี้แจงเหตุผลไปยังรัฐผู้ร้องขอด้วย การชี้แจงเหตุผลให้ฝ่ายรัฐผู้ร้องขอนั้นนับว่ามีส่วนช่วยให้กระบวนการให้ความช่วยเหลือเป็นไปอย่างโปร่งใสมากขึ้น อีกทั้งช่วยกำหนดแนวทางสำหรับการร้องขอความช่วยเหลือในโอกาสต่อไปสำหรับคดีที่คล้ายคลึงกัน

3.3.5.3 **การเก็บรักษาความลับระหว่างดำเนินการให้ความช่วยเหลือ**

ข้อ 27 วรรค วรรค 8 อนุญาตให้รัฐภาคีสามารถกำหนดให้รัฐผู้รับคำร้องขอเก็บข้อเท็จจริงและหัวเรื่องตามคำร้องไว้เป็นความลับได้ เว้นเสียแต่ว่าจะจำเป็นต่อการจัดการตามคำขอนั้น หากฝ่ายรัฐผู้รับคำร้องขอไม่สามารถรักษาความลับไว้ได้ อนุสัญญากำหนดให้ฝ่ายรัฐผู้รับคำร้องขอแจ้งกลับไปยังรัฐผู้ร้องขอโดยพลัน เพื่อให้อีกฝ่ายตัดสินใจว่าจะให้ดำเนินการต่อไปหรือไม่ จะเห็นได้ว่ามาตรการต่างๆตามมาตรา 27 ของอนุสัญญานั้นเป็นตัวอย่างของการพยายามให้การให้ความช่วยเหลือร่วมกันทางกฎหมายกว้างขวางที่สุดเท่าที่จะเป็นได้

3.3.5.4 **ช่องทางการติดต่อประสานงานการให้ความช่วยเหลือ**

แม้หน่วยงานกลางของรัฐภาคีมีหน้าที่เป็นผู้รับส่งและดำเนินการที่เกี่ยวข้องกับการจัดการตามคำขอก็ตาม ในกรณีฉุกเฉิน ข้อ 29 วรรค 9 a อนุญาตให้มีการติดต่อสื่อสารกันระหว่างหน่วยงานทางตุลาการของฝ่ายรัฐผู้ร้องและผู้รับคำขอได้โดยตรง พร้อมให้ส่งสำเนาการติดต่อระหว่างหน่วยงานกลางของทั้งสองฝ่ายไปในขณะเดียวกัน ทั้งนี้ การติดต่อสื่อสารหรือการส่งคำร้องขอในกรณีดังกล่าวสามารถทำผ่านช่องทางของหน่วยงานตำรวจสากล (Interpol) ได้ อย่างไรก็ดี ถ้าหน่วยงานฝ่ายตุลาการไม่สามารถที่จะจัดการตามคำขอได้ ให้หน่วยงานนั้นส่งเรื่องต่อไปยังหน่วยงานที่มีอำนาจหน้าที่โดยตรง พร้อมทั้งแจ้งไปยังฝ่ายรัฐผู้ร้องขอให้ทราบถึงการดังกล่าว

นอกจากการติดต่อกันระหว่างหน่วยงานฝ่ายตุลาการแล้ว อนุสัญญาข้อ 29 วรรค 9 d ได้อนุญาตให้รัฐภาคีติดต่อกันโดยตรงระหว่างหน่วยงานผู้มีอำนาจหน้าที่ของทั้งสองฝ่าย เพื่อติดต่อหรือรับส่งคำขอที่ไม่เกี่ยวข้องกับมาตรการที่รุกล้ำสิทธิได้

3.3.6 การรักษาความลับและจำกัดวิธีการใช้

ข้อ 28 ของอนุสัญญา อนุญาตให้รัฐภาคีสามารถเงื่อนไขให้อีกฝ่ายรักษาความลับและจำกัดการใช้ข้อมูลได้ หากข้อมูลหรือสิ่งที่ตนมีอยู่นั้นมีความอ่อนไหว โดยข้อ 28 วรรค 2 ถึง 4 ได้กำหนดหลักเกณฑ์เกี่ยวกับการตั้งเงื่อนไขดังกล่าวไว้ อย่างไรก็ดี ข้อ 28 วรรค 1 ระบุว่าหลักเกณฑ์เหล่านี้จะมีผลบังคับใช้เฉพาะในกรณีที่ รัฐภาคีไม่ได้ทำสนธิสัญญาด้านการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมาย ข้อตกลงที่มีมีฐานทางกฎหมายในลักษณะต่างตอบแทนในรูปแบบเดียวกันอื่นๆ ซึ่งมีผลบังคับใช้เท่านั้น มิฉะนั้น รัฐภาคีที่เกี่ยวข้องในการให้ความช่วยเหลือจะต้องแสดงความยินยอมที่จะนำหลักกฎหมายตามข้อ 28 วรรค 2-4 มาปรับใช้ทั้งหมดหรือบางส่วนเสียก่อน

ในการให้ข้อมูลหรือวัตถุตามคำร้องขอความช่วยเหลือซึ่งกันและกันทางกฎหมาย ข้อ 28 วรรค 2 a ได้อนุญาตให้รัฐกำหนดเงื่อนไขในแก่รัฐผู้ร้องขอให้เก็บข้อมูลเป็นความลับและจะไม่ให้ความช่วยเหลือทางกฎหมายหากอีกฝ่ายไม่ทำตามเงื่อนไขดังกล่าว นอกจากนี้ ข้อ 28 วรรค 2 b อนุญาตให้รัฐกำหนดเงื่อนไขจำกัดไม่ให้อีกฝ่ายนำข้อมูลหรือวัตถุดังกล่าวไปใช้ในการสืบสวนหรือดำเนินคดีอื่นที่ไม่ได้ระบุไว้ในคำขอความช่วยเหลือ

หากรัฐผู้รับความช่วยเหลือไม่สามารถปฏิบัติตามเงื่อนไขได้ ข้อ 28 วรรค 3 ให้รัฐผู้ร้องขอแจ้งให้ฝ่ายรัฐผู้ช่วยเหลือทราบ เพื่อที่จะตัดสินใจต่อไปว่าจะดำเนินการต่อหรือไม่ อย่างไรก็ตาม หากรัฐทั้งสองฝ่ายสามารถตกลงกันได้ เงื่อนไขดังกล่าวย่อมมีผลผูกพันทั้งสองฝ่าย นอกจากนี้ ข้อ 28 วรรค 4 ยังอนุญาตให้ฝ่ายรัฐผู้ส่งมอบข้อมูลหรือวัตถุเรียกร้องให้อีกฝ่ายให้อธิบายถึงการนำข้อมูลหรือวัตถุดังกล่าวไปใช้ได้ด้วย

การกำหนดเงื่อนไขตามข้อ 28 ไม่เพียงเพิ่มความยืดหยุ่นในการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายระหว่างรัฐภาคีเท่านั้น หากแต่ยังมีจุดมุ่งหมายเพื่อให้มาตรการปกป้องตามหลักการเกี่ยวกับการปกป้องข้อมูลด้วย[45] ทั้งนี้ การรักษาความลับมีความสำคัญในการ

[45] *Ibid*., Para. 275

สืบสวนคดีอาชญากรรมทางคอมพิวเตอร์มากกว่าอาชญากรรมทั่วไป เพราะหากผู้กระทำผิดสามารถรับรู้ถึงการสืบสวนคดี ผู้กระทำความผิดจะสามารถเข้าถึงหลักฐานเพื่อปิดบัง หรือทำลายได้อย่างรวดเร็วง่ายดายกว่าปกติ

3.4 การให้ความช่วยเหลือด้วยวิธีการเฉพาะภายใต้กรอบอนุสัญญากรุงบูดาเปสต์

การให้ความช่วยเหลือด้วยวิธีการเฉพาะนั้นถูกกำหนดไว้ในข้อ 29 ถึง 32 ของอนุสัญญากรุงบูดาเปสต์ และจะเป็นการนำอำนาจการสืบสวนอาชญากรรมทางคอมพิวเตอร์ตาม ข้อ 16,17, 19,20,21 ของอนุสัญญา มาปรับใช้ในบริบทการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมาย การให้ความช่วยเหลือด้วยวิธีเฉพาะนั้นแตกต่างจากการให้ความช่วยเหลือทั่วไป โดยรัฐผู้ให้ความช่วยเหลือส่วนใหญ่จะสั่งการไปยังผู้ให้บริการทางอินเตอร์เน็ตเพื่อดำเนินการตามบทบัญญัติเฉพาะต่างๆอีกขั้นหนึ่งแทนฝ่ายเจ้าหน้าที่ของรัฐ แทนที่จะดำเนินการแต่ฝ่ายเดียว อย่างเช่นกรณีปกติ การให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายด้วยวิธีเฉพาะ มีรายละเอียดดังต่อไปนี้

3.4.1 การรักษาข้อมูลที่ถูกเก็บไว้อย่างรวดเร็ว

การเก็บรักษาข้อมูลที่ถูกเก็บไว้อย่างรวดเร็วเป็นการป้องกันไม่ให้ข้อมูลหลักฐานสำคัญในอาชญากรรมทางคอมพิวเตอร์ให้ปลอดภัยเสียก่อนที่เจ้าหน้าที่รัฐผู้สืบสวนจะทำการค้น เข้าถึง ยึด หรือทำให้ข้อมูลที่เกี่ยวข้องปลอดภัยในลำดับต่อไป โดยภายใต้ ข้อ 16 วรรคหนึ่ง ของอนุสัญญา การเก็บรักษาข้อมูลจะเกิดเมื่อหน่วยงานรัฐเห็นว่าข้อมูลทางคอมพิวเตอร์บางอย่าง หรือข้อมูลจราจรนั้นเสี่ยงต่อการสูญเสียหรือการถูกดัดแปลง การเก็บรักษาอาจกระทำโดยหน่วยงานรัฐหรือสั่งการให้ผู้ให้บริการเก็บรักษาข้อมูลทางคอมพิวเตอร์ที่ระบุไว้แทนก็ได้

ทั้งนี้ ข้อมูลที่เกี่ยวข้องในการสืบสวนคดีอาชญากรรมทางคอมพิวเตอร์มีอยู่สองรูปแบบ คือ ข้อมูลเนื้อหาซึ่งจะพิสูจน์ถึงอาชญากรรมที่เกิดขึ้น และข้อมูลจราจรซึ่งจะระบุถึงเส้นทางการเดินทางของข้อมูลของคอมพิวเตอร์ ว่ามาจากที่ไหน โดยผู้ให้บริการทางอินเตอร์เน็ตรายใด[46]

---

[46] Marco Gercke. Understanding cybercrime: A guide for developing countries [Online]. Geneva: International Telecommunication Union (ITU), ICT applications and cybersecurity division, 2009.

การเปิดเผยข้อมูลจราจรจะช่วยให้เจ้าหน้าที่รัฐ สามารถตามร่องรอยของอาชญากรรมทางคอมพิวเตอร์ได้[47]

ในกรณีที่การเก็บรักษาข้อมูลถูกนำมาใช้ในบริบทการให้ความร่วมมือทางอาญาระหว่างประเทศ ข้อ 29 วรรค 1 กำหนดให้รัฐภาคีร้องขอรัฐอีกฝ่ายเก็บรักษาข้อมูลอย่างรวดเร็วได้หากข้อมูลนั้นตั้งอยู่ในดินแดนของอีกฝ่าย อย่างไรก็ตาม รัฐผู้ร้องขอต้องมีเจตนาที่จะส่งคำขอเพื่อดำเนินการเพิ่มเติม อาทิ การเข้าถึง การยึด การทำให้ปลอดภัย การเปิดเผย ในขั้นตอนต่อไป เพราะการเก็บรักษาข้อมูลเป็นเพียงมาตรการชั่วคราวเท่านั้น

การเก็บรักษาข้อมูลที่ถูกเก็บไว้อย่างรวดเร็วมีความสำคัญในการป้องกันหลักฐานไม่ให้ถูกทำลายในระหว่างที่รัฐผู้ร้องขอความช่วยเหลือกำลังจัดเตรียมคำขอความช่วยเหลือซึ่งกันและกันทางกฎหมาย ซึ่งเป็นขั้นตอนที่ใช้เวลาพอสมควร นอกจากความรวดเร็วแล้ว การเก็บรักษาข้อมูลยังจัดเป็นมาตรการที่รุกล้ำสิทธิ์น้อยที่สุด เพราะจะป้องกันความปลอดภัยให้แก่ข้อมูลโดยไม่เปิดเผยรายละเอียดของข้อมูล หรือแหล่งที่มาในการรับส่งข้อมูลจนกว่าจะมีคำสั่งจากฝ่ายเจ้าหน้าที่รัฐให้เปิดเผยในภายหลัง[48] ในขณะเดียวกัน มาตรการนี้ยังลดภาระไม่ให้ฝ่ายผู้ให้บริการทางอินเตอร์เน็ตต้องเก็บข้อมูลของผู้ใช้บริการทั้งหมดเอาไว้ เพียงแต่ป้องกันข้อมูลตามที่ฝ่ายเจ้าหน้าที่รัฐระบุมาเท่านั้น อย่างไรก็ตาม หากข้อมูลสำคัญ ถูกทำลายไปก่อนที่จะดำเนินการรักษาข้อมูล มาตรการรักษาข้อมูลก็จะไม่เป็นผล[49]

นอกจากมาตรการเก็บรักษาข้อมูล มีวิธีการเก็บรักษาข้อมูลอีกประการหนึ่งเรียกว่าการกักข้อมูล (Data Retention) ซึ่งผู้ให้บริการทางอินเตอร์เน็ตจะได้รับคำสั่งจากรัฐให้เก็บข้อมูลสักระยะหนึ่ง ทั้งนี้ เพื่อให้หน่วยงานผู้บังคับใช้กฎหมายสามารถเข้าถึงข้อมูลที่จำเป็นต่อการระบุตัวผู้กระทำความผิดได้แม้เหตุการณ์จะทิ้งช่วงหลังจากการกระทำผิดไปพอสมควรก็ตาม[50]

Available from: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf [2013, May 6], p.195

[47] *Ibid.*

[48] Council of Europe. Convention on cybercrime explanatory report, Para.287

[49] Marco Gercke. Understanding cybercrime: A guide for developing countries, p.179

[50] *Ibid.*, p.177

อย่างไรก็ดี อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของสภายุโรปจะไม่ได้ให้รายละเอียดเกี่ยวกับการกักข้อมูลไว้

การรักษาข้อมูลที่ถูกเก็บไว้อย่างรวดเร็วและการกักข้อมูล นั้นมีความแตกต่างกันหลายด้าน[51] วัตถุประสงค์ของการรักษาข้อมูลที่ถูกเก็บไว้อย่างรวดเร็วจะเป็นเพียงมาตรการชั่วคราวเพื่อให้เจ้าหน้าที่รัฐมีเวลาเพียงพอที่จะดำเนินการเพื่อให้ได้มาหลักฐานทางอิเล็กทรอนิกส์และจะมีคำสั่งเฉพาะเจาะจงไปยังข้อมูลที่จะรักษาไว้เท่านั้น ในทางกลับกันการกักข้อมูลจะเป็นไปอย่างอัตโนมัติเพื่อให้ข้อมูลต่างๆมีพร้อมสำหรับการสอบสวน ตรวจจับและดำเนินคดีในอาชญากรรมที่ร้ายแรงเท่านั้น สำหรับขอบเขตดำเนินการนั้น การรักษาข้อมูลที่ถูกเก็บไว้อย่างรวดเร็วจะครอบคลุมข้อมูลทุกชนิดซึ่งรวมไปถึงข้อมูลทางเนื้อหาด้วย และสามารถดำเนินการได้กับอาชญากรรมทุกชนิดที่มีหลักฐานในรูปแบบอิเล็กทรอนิกส์ แต่ข้อมูลจากการกักข้อมูลนั้นจะถูกนำมาใช้ประโยชน์เฉพาะกรณีอาชญากรรมร้ายแรง และจะเก็บเฉพาะข้อมูลจราจรและผู้ใช้บริการเท่านั้น ไม่ได้ครอบคลุมถึงข้อมูลเนื้อหาแต่อย่างใด นอกจากนี้ ฝ่ายเจ้าหน้าที่รัฐจะสามารถออกคำสั่งรักษาข้อมูลที่ถูกเก็บไว้อย่างรวดเร็วได้กับบุคคลธรรมดาและนิติบุคคลทุกประเภท ไม่ได้จำกัดเฉพาะผู้ให้บริการทางอินเตอร์เน็ตอย่างเช่นในกรณีของการกักข้อมูล

3.4.1.1 **รายละเอียดที่ต้องระบุไว้ในคำขอความช่วยเหลือ**

ข้อ 29 วรรค 2 กำหนดให้รัฐภาคีส่งคำขอที่ระบุรายละเอียดต่างๆที่เกี่ยวข้องกับคดีอาชญากรรมทางคอมพิวเตอร์ 6 ประการ ได้แก่

1. หน่วยงานที่ร้องขอให้มีการเก็บรักษาข้อมูล

2. การกระทำความผิดที่เป็นเหตุให้มีการสืบสวนคดี และบทสรุปย่อข้อเท็จจริงที่เกี่ยวข้องกับการกระทำความผิดนั้นๆ

3. ข้อมูลคอมพิวเตอร์ที่รัฐผู้ขอประสงค์ที่จะให้มีการเก็บรักษา และความเกี่ยวข้องของข้อมูลดังกล่าวต่ออาชญากรรมที่เกิด

---

[51] The cybercrime convention committee (T-CY). 7th plenary abridged meeting report [Online]. Strasbourg: Council of Europe, 2012. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY2012/T-CY_2012_26E_PlenAbrMeetRep_V5.pdf [2013, May 6], p.11

4. ข้อมูลระบุตัวผู้ให้บริการทางอินเตอร์เน็ตที่เก็บข้อมูล หรือข้อมูลเกี่ยวกับสถานที่ที่ระบบคอมพิวเตอร์ที่เก็บข้อมูลนั้นตั้งอยู่ (ถ้ามี)

5. ความจำเป็นที่ในการเก็บรักษาข้อมูลนั้น

6. ข้อความที่แสดงเจตนาของรัฐผู้ร้องขอว่า ตนจะขอความช่วยเหลือทางกฎหมายเพื่อค้น เข้าถึง ยึด ทำให้ปลอดภัย หรือเปิดเผยข้อมูลดังกล่าวต่อไป

3.4.1.2 **หลักความผิดสองประเทศ**

การเก็บรักษาข้อมูลทางคอมพิวเตอร์ที่ถูกเก็บไว้อย่างรวดเร็วนั้นเร่งด่วนและรุกล้ำสิทธิน้อย อนุสัญญาข้อ 29 วรรค 3 จึงกำหนดให้หลักความผิดสองประเทศ ไม่รวมเป็นเงื่อนไขการให้ความช่วยเหลือรูปแบบนี้ อย่างไรก็ดี รัฐภาคียังคงสามารถกำหนดหลักความผิดสองประเทศสำหรับคำขอเพื่อดำเนินการเพิ่มเติมในภายหลัง อาทิ การเข้าถึง การยึด การทำให้ปลอดภัย หรือการเปิดเผยข้อมูลได้

หากรัฐภาคีได้กำหนดหลักความผิดสองประเทศไว้เป็นเงื่อนไขสำหรับการให้ความช่วยเหลือภายหลังการเก็บรักษาข้อมูลไว้ อนุสัญญาข้อ 29 วรรค 4 อนุญาตให้รัฐนั้นสามารถปฏิเสธการเก็บรักษาข้อมูลได้หาก ฐานความผิดตามคำขอนั้นไม่อยู่ใน ข้อ 2-11 แห่งอนุสัญญา และรัฐผู้รับคำร้องขอมีเหตุผลอันควรเชื่อว่ารัฐผู้ร้องขอไม่สามารถบรรลุเงื่อนไขตามหลักความผิดสองประเทศ ได้ภายในเวลาที่เปิดเผยข้อมูล

3.4.1.3 **เหตุแห่งการปฏิเสธการช่วยเหลือ**

ข้อ 29 วรรค 5 กำหนดเหตุแห่งการปฏิเสธการให้ความช่วยเหลือรูปแบบนี้ไว้ในกรณีที่ความผิดตามคำขอเป็นความผิดทางการเมืองหรือเกี่ยวข้องกับความผิดทางการเมือง และกรณีที่การขอความช่วยเหลือนั้นอาจส่งผลกระทบต่ออำนาจอธิปไตย ความมั่นคง หรือความสงบเรียบร้อยในสังคมของรัฐผู้รับคำขอ

นอกจากนี้ หากรัฐผู้ดำเนินการเก็บรักษาข้อมูลเห็นว่าการเก็บรักษาไม่อาจรับรองถึงการมีอยู่พร้อมใช้ของข้อมูลดังกล่าวในอนาคต หรืออาจส่งผลกระทบต่อความลับหรือสร้างผลกระทบอื่นๆของการสืบสวนคดีของรัฐผู้ร้องขอ ข้อ 29 วรรค 6 อนุญาตให้ฝ่ายรัฐ

ผู้รับคำร้องขอแจ้งกลับไปยังฝ่ายผู้ร้องขอโดยพลัน เพื่อที่จะพิจารณาต่อไปว่าควรดำเนินการต่อหรือไม่

3.4.1.4 ระยะเวลาในการเก็บรักษาข้อมูล

ข้อ 29 วรรค 7 ระบุให้ระยะเก็บรักษาข้อมูลตามคำขอไม่น้อยไปกว่า 60 วัน เพื่อให้รัฐผู้ร้องขอความช่วยเหลือสามารถทำคำขออย่างเป็นทางการสำหรับการให้ความช่วยเหลือรูปแบบอื่นๆตามมาอีกได้ ระยะเวลาดังกล่าวสามารถขยายต่อไปได้อีก หากรัฐผู้ร้องขอส่งคำขออย่างเป็นทางการตามมาแล้ว สำหรับการดำเนินการภายในประเทศนั้น ข้อ 16 วรรค 2 ได้กำหนดกรอบระยะเวลาในการเก็บรักษาข้อมูลโดยผู้ให้บริการทางอินเตอร์เน็ตว่า ให้ผู้ให้บริการสามารถเก็บรักษาและคงไว้ซึ่งความสมบูรณ์ของข้อมูลไว้เป็นเวลานานที่สุดเท่าที่ทำได้ โดยมีระยะเวลาสูงสุด 90 วัน แต่รัฐภาคีสามารถออกคำสั่งขยายระยะเวลาในภายหลังได้เช่นกัน

3.4.2 การเปิดเผยข้อมูลจราจรอย่างรวดเร็ว

การเปิดเผยข้อมูลจราจรอย่างรวดเร็วระหว่างประเทศ จะเกิดขึ้นเมื่อรัฐผู้เก็บรักษาข้อมูลจราจรอย่างรวดเร็วพบว่า เส้นทางการสื่อสารของข้อมูลจราจรที่ถูกเก็บรักษานั้นถูกส่งผ่านผู้ให้บริการในรัฐที่สาม ในการนี้ ข้อ 30 แห่งอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์กำหนดให้รัฐผู้เปิดเผยข้อมูลจราจรแจ้งให้อีกฝ่ายหนึ่งทราบเพื่อดำเนินการต่อไป[52] ด้วยการเปิดเผยข้อมูลจราจรอย่างรวดเร็ว ข้อมูลที่เปิดเผยนั้นต้องมีรายละเอียดเพียงพอที่จะให้อีกฝ่ายหนึ่งทราบถึงตัวตนของผู้ให้บริการข้อมูลดังกล่าว และเส้นทางของการสื่อสารถูกส่งผ่าน

การปฏิเสธความช่วยเหลือรูปแบบนี้สามารถกระทำได้สองกรณีคือ กรณีที่ความผิดตามคำขอเป็นความผิดทางการเมืองหรือเกี่ยวข้องกับความผิดทางการเมือง และกรณีที่คำขอความช่วยเหลือนั้นส่งผลกระทบต่ออำนาจอธิปไตย ความมั่นคง หรือความสงบเรียบร้อยของรัฐผู้รับคำขอ

---

[52]Council of Europe. Convention on cybercrime explanatory report,Para.290

3.4.3 การให้ความช่วยเหลือในการเข้าถึงข้อมูลทางคอมพิวเตอร์ที่ถูกเก็บไว้

การเข้าถึงข้อมูลทางคอมพิวเตอร์ที่ถูกเก็บไว้ คือการนำหลักกฎหมายเกี่ยวกับการค้นและยึดตามกฎหมายวิธีพิจารณาความอาญามาใช้ในบริบทอาชญากรรมทางคอมพิวเตอร์ เพื่อให้ฝ่ายเจ้าหน้าที่รัฐไม่เพียงแต่สามารถยึดอุปกรณ์คอมพิวเตอร์ทางกายภาพเท่านั้น หากสามารถกระทำการต่างๆกับข้อมูลทางคอมพิวเตอร์ที่อยู่ภายในอาทิ การค้น เข้าถึง ยึด ทำให้ปลอดภัย หรือเปิดเผยข้อมูลที่ถูกกักเก็บไว้ในคอมพิวเตอร์ได้ ซึ่งจะช่วยให้เจ้าหน้าที่รัฐสามารถวิเคราะห์ข้อมูลที่อยู่ภายในอุปกรณ์คอมพิวเตอร์ที่ถูกยึดมาด้วยวิธีที่มีประสิทธิภาพมากกว่าการเข้าถึงข้อมูลจากระยะไกลได้[53] จึงมีบทบาทสำคัญในการสืบสวนอาชญากรรมทางคอมพิวเตอร์ไม่น้อยไปกว่าการใช้วิธีการทางเทคนิคเพื่อระบุตัวผู้กระทำผิดจากระยะไกลเช่น การรวบรวมข้อมูลตามเวลาจริงและการใช้ software ทางนิติเวช อย่างไรก็ตามการเข้าถึงข้อมูลคอมพิวเตอร์นี้จะรุกล้ำสิทธิมากกว่าการเก็บรักษาข้อมูล เพราะจะมีการกระทำกับข้อมูลทางคอมพิวเตอร์และเครื่องคอมพิวเตอร์ของผู้อื่นโดยตรง

สำหรับการดำเนินการภายในประเทศนั้น อนุสัญญาข้อ 19 วรรค 1 กำหนดให้รัฐภาคีให้อำนาจเจ้าหน้าที่รัฐในการค้นหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลภายในระบบคอมพิวเตอร์หรือสื่อกลางที่ใช้เก็บข้อมูลทางคอมพิวเตอร์ที่ตั้งอยู่ภายในดินแดนของตนได้ ในขณะเดียวกันข้อ 19 วรรค 2 อนุญาตให้ฝ่ายเจ้าหน้าที่รัฐสามารถขยายอำนาจการค้นหรือการเข้าถึงไปยังระบบคอมพิวเตอร์อื่นที่อยู่ในดินแดนของรัฐจนได้ หากวินิจฉัยพบว่าข้อมูลที่เสาะหาอยู่นั้นอยู่ภายในระบบคอมพิวเตอร์อื่นซึ่งสามารถเข้าถึงได้โดยถูกต้องตามกฎหมายจากระบบที่ตนกำลังตรวจค้นอยู่

หลังจากการค้นและเข้าถึงข้อมูล ข้อ 19 วรรค 3 ได้กำหนดให้ฝ่ายเจ้าหน้าที่รัฐสามารถใช้มาตรการต่างๆเพื่อยึดหรือทำให้ข้อมูลทางคอมพิวเตอร์ที่ถูกเข้าถึงอยู่ในภาวะปลอดภัยได้ โดยมาตรการดังกล่าวนั้นได้แก่ การยึดระบบหรือทำให้ปลอดภัยซึ่งคอมพิวเตอร์ทั้งหมดหรือบางส่วน หรือสื่อกลางสำหรับเก็บข้อมูลทางคอมพิวเตอร์ การคัดลอกสำเนาข้อมูลทางคอมพิวเตอร์และเก็บรักษาไว้ การรักษาความสมบูรณ์ของข้อมูลทางคอมพิวเตอร์

---

[53] Marco Gercke. Understanding cybercrime: A guide for developing countries, pp.186-187

ที่เกี่ยวข้องที่ถูกเก็บไว้ และการทำให้ข้อมูลทางคอมพิวเตอร์ดังกล่าวนั้นเข้าถึงไม่ได้ หรือถูกย้ายออกไปจากระบบคอมพิวเตอร์ที่ทำการเข้าถึง

นอกจากนี้ ข้อ 19 วรรค 4 ให้อำนาจเจ้าหน้าที่รัฐในการสั่งให้ผู้ให้บริการให้ข้อมูลที่มีความจำเป็นหรือให้ความช่วยเหลืออื่นๆตามสมควรแก่เจ้าหน้าที่รัฐ ซึ่งรวมไปถึงการเปิดเผยรหัสผ่านหรือเปิดมาตรการรักษาความปลอดภัยต่างๆ ให้เจ้าหน้าที่ผู้สืบสวนคดีอาชญากรรมทางคอมพิวเตอร์[54] อย่างไรก็ตาม การให้ความช่วยเหลือจากฝ่ายผู้ให้บริการทางคอมพิวเตอร์นั้นจะต้องไม่คุกคามต่อสิทธิของผู้ใช้บริการทางอินเตอร์เน็ตโดยปราศจากเหตุอันควร หรือเปิดเผยข้อมูลอื่นๆนอกเหนือจากข้อมูลที่ค้น

สำหรับการดำเนินการให้ความช่วยเหลือระหว่างประเทศนั้น ข้อ 31 กำหนดให้รัฐภาคีร้องขอให้รัฐอีกฝ่ายค้น เข้าถึง ยึด หรือทำให้ปลอดภัย หรือเปิดเผยข้อมูลที่เก็บไว้ในระบบคอมพิวเตอร์ภายในดินแดนของอีกฝ่าย โดยข้อมูลดังกล่าวนั้นรวมไปถึงข้อมูลที่ถูกเก็บรักษาไว้ด้วย

หลักเกณฑ์ต่างๆ ในการให้ความช่วยเหลือในรูปแบบนี้ ข้อ 31 วรรค 2 กำหนดให้เป็นไปตามการปรับใช้ ข้อตกลงระหว่างประเทศ ข้อตกลงอื่นๆ หรือกฎหมายที่มีผลบังคับใช้กับรัฐภาคีและบทบัญญัติอื่นๆตามอนุสัญญาฉบับนี้ อย่างไรก็ตาม อนุสัญญา ข้อ 31 วรรค 3 กำหนดให้รัฐผู้รับคำร้องขอตอบรับคำขออย่างรวดเร็ว เมื่อมีเหตุอันควรเชื่อได้ว่า ข้อมูลที่ระบุมาตามคำขอนั้นมีความเสี่ยงที่จะถูกลบทิ้งหรือดัดแปลง หรือสถานการณ์เป็นไปตามบทบัญญัติข้อตกลงระหว่างประเทศ ข้อตกลงอื่นๆ หรือกฎหมายที่มีผลบังคับใช้ระหว่างรัฐภาคี

3.4.4 การเข้าถึงข้อมูลข้ามแดน

การเข้าถึงข้อมูลข้ามแดนเป็นกรณีพิเศษ ที่รัฐภาคีสามารถเข้าถึงข้อมูลที่อยู่ในระบบคอมพิวเตอร์ที่อยู่ในรัฐภาคีอื่นได้โดยไม่ต้องขอความช่วยเหลือจากอีกฝ่ายล่วงหน้า การกระทำเช่นนี้ช่วยให้การสืบสวนคดีอาชญากรรมคอมพิวเตอร์ของรัฐภาคีรวดเร็วมากขึ้นเพราะไม่ต้องผ่านกระบวนการที่ไม่จำเป็น

---

[54] Council of Europe. Convention on cybercrime explanatory report, Para.202

ทั้งนี้ ข้อ 32 a ของอนุสัญญาอนุญาตให้รัฐภาคีสามารถเข้าถึงข้อมูลที่เปิดเผยสู่สาธารณะ(open source) ได้โดยไม่ต้องพิจารณาตำแหน่งที่ตั้งของข้อมูล เพราะบุคคลทั่วไปสามารถเข้าถึงข้อมูลดังกล่าวได้โดยอิสระ หากหน่วยงานผู้สืบสวนคดีอาชญากรรมทางคอมพิวเตอร์ถูกจำกัดสิทธิการเข้าถึงข้อมูลเช่นว่านี้ การสืบสวนก็จะยุ่งยากยิ่งขึ้น[55]นอกจากนี้ ข้อ 32b อนุญาตให้รัฐภาคีสามารถเข้าถึงหรือรับข้อมูลทางคอมพิวเตอร์ที่ถูกเก็บไว้ในดินแดนของรัฐภาคีอื่นได้ผ่านทางระบบคอมพิวเตอร์ของในดินแดนของตน หากต้องได้รับความยินยอมโดยสมัครใจและชอบด้วยกฎหมายจากผู้มีอำนาจเปิดเผยข้อมูลผ่านทางระบบคอมพิวเตอร์นั้น

การเข้าถึงข้อมูลข้ามแดนตามข้อ 32 นี้จะเป็นประโยชน์ถ้าหากรัฐผู้ร้องขอนั้นมีความพร้อมและความสามารถทางเทคโนโลยีในการสืบสวนคดีอาชญากรรมทางคอมพิวเตอร์ได้ดีกว่าฝ่ายรัฐผู้รับคำขอ เพราะนั่นย่อมจะช่วยให้ฝ่ายเจ้าหน้าที่มีโอกาสจับกุมผู้กระทำความผิดได้สูงขึ้น

อย่างไรก็ดี กรณีสองกรณีตามข้อ 32 นี้ เป็นเพียงประเด็นที่รัฐต่างๆ สามารถตกลงกันได้ในช่วงการร่างสัญญาเท่านั้น เพราะรัฐภาคีต่างๆยังขาดประสบการณ์ในประเด็นปัญหาเหล่านี้[56] อนุสัญญาจึงไม่ได้ระบุรายละเอียดของกรณีอื่นๆนอกเหนือไปจากนี้ แต่ก็ไม่ได้ปฏิเสธความเป็นไปได้ที่รัฐภาคีจะใช้วิธีการเข้าถึงข้ามแดนที่ข้อ 32 ไม่ได้ระบุไว้เช่นกัน น่าสังเกตว่าสาเหตุที่การตกลงในประเด็นดังกล่าวของรัฐภาคีเป็นอย่างยากลำบากนั้นเป็นเพราะว่าการเปิดโอกาสให้รัฐอื่นเข้าถึงข้อมูลทางคอมพิวเตอร์ที่อยู่ในเขตแดนของตนโดยไม่ต้องส่งคำขอมาก่อนนั้น ย่อมเสี่ยงต่อการถูกละเมิดอำนาจอธิปไตยได้

3.4.5 การรวบรวมข้อมูลจราจรตามเวลาจริง

ข้อ 20 ของอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของสภายุโรป ได้กำหนดให้การรวบรวมข้อมูลจราจรตามเวลาจริง สามารถกระทำได้สองวิธี โดยข้อ 20 a กำหนดให้รัฐภาคีมอบอำนาจแก่เจ้าหน้าที่ของตนในการใช้วิธีทางเทคนิคเพื่อรวบรวมหรือบันทึกข้อมูลจราจรที่เกี่ยวข้องกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์ที่ถูกระบุไว้ ซึ่งในทางปฏิบัติ ฝ่ายเจ้าหน้าที่

---

[55] Marco Gercke. Understanding cybercrime: A guide for developing countries, p.213

[56] Council of Europe. Convention on cybercrime explanatory report, Para.293,

รัฐจะกำหนดให้ผู้ให้บริการทางอินเตอร์เน็ตอนุญาตให้ตนเข้ามารวบรวมข้อมูลได้โดยตรง โดยผู้ให้บริการทางอินเตอร์เน็ตจะสร้าง interface สำหรับเจ้าหน้าที่รัฐในการเข้าถึงระบบโครงสร้างพื้นฐานของผู้ให้บริการทางอินเตอร์เน็ต[57] สำหรับวิธีที่สองนั้น ข้อ 20 b กำหนดให้รัฐภาคีให้อำนาจเจ้าหน้าที่รัฐของตนสำหรับสั่งการให้ผู้ให้บริการทางอินเตอร์เน็ตใช้ขีดความสามารถทางเทคนิคที่มีอยู่ในการรวบรวมหรือบันทึกข้อมูลจราจรตามเวลาจริง หรือให้ความร่วมมือและช่วยเหลือฝ่ายเจ้าหน้าที่รัฐในการดำเนินการดังกล่าว

เมื่อนำมาเปรียบเทียบกัน วิธีการแรกจะเหมะสมกว่าถ้าผู้ให้บริการทางอินเตอร์เน็ตขาดความพร้อมทางเทคโนโลยี[58] ในขณะที่วิธีการที่สองจะมีประโยชน์หากเจ้าหน้าที่รัฐสามารถใช้ประโยชน์จากขีดความสามารถทางเทคโนโลยีของตนควบคู่ไปกับความรู้ของผู้ให้บริการทางอินเตอร์เน็ตได้ในคราวเดียวกัน

นอกจากนี้ ข้อ 20 วรรค 3 ได้อนุญาตให้รัฐภาคีของให้ผู้ให้บริการทางอินเตอร์เน็ตปกปิดข้อมูลเกี่ยวกับการสืบสวนอาชญากรรมทางคอมพิวเตอร์ให้เป็นความลับไว้ ที่เป็นเช่นนี้เพราะการรวบรวมข้อมูลจราจรตามเวลาจริงนี้จะเป็นประโยชน์ต่อเมื่อหากอาชญากรไม่ทราบถึงการสืบสวนคดีที่ดำเนินอยู่

อย่างไรก็ดี การรวบรวมข้อมูลจราจรตามเวลาจริงยังมีข้อจำกัดอยู่เช่นเดียวกัน ในกรณีที่ผู้กระทำความผิดใช้เทคโนโลยีการสื่อสารที่ไม่เปิดเผยตัว ฝ่ายเจ้าหน้าที่รัฐจะไม่สามารถวิเคราะห์ข้อมูลทางจราจรและระบุตัวผู้กระทำผิดได้[59]

สำหรับการให้ความช่วยเหลือระดับระหว่างประเทศนั้น ข้อ 33 วรรค 1 กำหนดให้เงื่อนไขเบื้องต้นและกระบวนการเกี่ยวกับการให้ความช่วยเหลือในรูปแบบนี้เป็นไปตามเงื่อนไขและกระบวนการตามกฎหมายภายในของรัฐผู้ให้ความช่วยเหลือ

---

[57] *Ibid*., Para.220

[58] *Ibid*., Para.223,

[59] Marco Gercke. Understanding cybercrime: A guide for developing countries, p.196

ในทางปฏิบัติ รัฐภาคีตีความการดำเนินการตามมาตรการนี้แตกต่างกันออกไป รัฐบางรัฐตีความการใช้มาตรการนี้อย่างกว้างขวาง เพราะเห็นว่าการรวบรวมข้อมูลจราจรตามเวลาจริงจัดเป็นมาตรการที่เป็นการรุกล้ำสิทธิที่น้อยกว่ามาตรการอื่นๆอย่างเช่นการดักรับข้อมูลหรือการค้นและยึดข้อมูล ในขณะที่รัฐบางรัฐตีความการใช้มาตรการนี้อย่างแคบ[60] ด้วยเหตุนี้ขอบเขตของการให้ความช่วยเหลือด้วยการรวบรวมข้อมูลจราจรตามเวลาจริงแตกต่างไปจากการให้ความช่วยเหลือรูปแบบอื่น โดยข้อ 33 วรรค 2 กำหนดจะขอบเขตขั้นต่ำให้รัฐภาคีให้ความช่วยเหลือในกรณีที่ฐานความผิดตามคำขอนั้น เป็นฐานความผิดที่สามารถสามารถรวบรวมข้อมูลจราจรตามเวลาจริงได้ตามกฎหมายภายใน

3.4.6 การดักรับข้อมูลทางเนื้อหาตามเวลาจริง

การดักรับข้อมูลทางเนื้อหาคือการที่ฝ่ายเจ้าหน้าที่รัฐบันทึกข้อมูลที่มีการสื่อสารระหว่างกันและดำเนินการวิเคราะห์เนื้อหาของข้อมูลที่อยู่ภายใน อย่างไรก็ตาม การดักรับข้อมูลเชิงเนื้อหาอาจจะประสบปัญหาได้ หากผู้กระทำผิดใช้เทคโนโลยีการเข้ารหัส ปกปิดไม่ให้ผู้สืบสวนคดีอาชญากรรมทางคอมพิวเตอร์ถึงข้อมูลที่ต้องการได้ อีกทั้งการถอดรหัสก็ใช้ระยะเวลานานมาก

ในระดับภายในประเทศ ข้อ 21 a และ b ของอนุสัญญากำหนดให้รัฐภาคีให้อำนาจแก่ฝ่ายเจ้าหน้าที่รัฐดำเนินการทางเทคนิคเพื่อรวบรวมหรือบันทึกข้อมูลเนื้อหาที่เกี่ยวข้องกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์ที่ถูกระบุไว้ หรือสั่งการให้ผู้ให้บริการดำเนินการแทนหรือให้ความร่วมมือและช่วยเหลือฝ่ายเจ้าหน้าที่รัฐ อย่างไรก็ตาม หากรัฐภาคีไม่สามารถดำเนินมาตรการดังกล่าวได้ด้วยเหตุจากหลักการพื้นฐานตามกฎหมายภายใน ข้อ 21 วรรค 2 กำหนดให้ รัฐภาคีมีมาตรการทางกฎหมายหรือมาตรการอื่นเท่าที่จำเป็นเพื่อให้สามารถดำเนินการรวบรวม หรือบันทึกข้อมูลเนื้อหาของการสื่อสารที่ระบุไว้ในดินแดนของตน ด้วยวิธีการทางเทคนิคได้ นอกจากนี้ ข้อ 21 วรรค 3 ได้อนุญาตให้รัฐภาคีของให้ผู้ให้บริการทางอินเตอร์เน็ตปกปิดข้อมูลเกี่ยวกับการสืบสวนอาชญากรรมทางคอมพิวเตอร์ให้เป็นความลับไว้ด้วย

---

[60] Council of Europe. Convention on cybercrime explanatory report, Para.296

ข้อ 34 ของอนุสัญญากำหนดให้เงื่อนไขเบื้องต้นและกระบวนการเกี่ยวกับการให้ความช่วยเหลือทางกฎหมายในรูปแบบนี้เป็นไปตามข้อตกลงระหว่างประเทศหรือกฎหมายภายในที่มีผลบังคับใช้

นอกจากนี้ การดักรับข้อมูลจะต้องเป็นไปมาตรการปกป้องที่กำหนดไว้ในข้อ15 แห่งอนุสัญญาฉบับนี้ด้วยและรวมไปถึงคำแนะนำของสภายุโรป No. R (85) 1 ว่าด้วยการปรับใช้ European Convention on Mutual Assistance in Criminal Matters ในกรณีของการส่งหนังสือส่งประเด็นสืบพยาน (letter rogatory) สำหรับการดักรับการสื่อสารทางโทรคมนาคม[61]

3.4.7 **เครือข่ายจุดติดต่อตลอดเวลา**

เครือข่ายจุดติดต่อตลอดเวลา นับเป็น มาตรการความร่วมมือทางอาญาระหว่างประเทศที่สำคัญที่สุดมาตรการหนึ่งภายใต้อนุสัญญากรุงบูดาเปสต์[62] เครือข่ายจุดติดต่อตลอดเวลานี้ได้รับแนวคิดมาจากเครือข่ายลักษณะเดียวกันของกลุ่ม G8 เพื่อให้หน่วยงานผู้บังคับใช้กฎหมายดำเนินการปราบปรามอาชญากรรมทางคอมพิวเตอร์และรวบรวมหลักฐานได้อย่างรวดเร็ว

ข้อ 35 วรรค 1 ของอนุสัญญากำหนดให้รัฐภาคีกำหนดจุดติดต่อสำหรับให้ความช่วยเหลืออย่างเร่งด่วนสำหรับการสืบสวนหรือดำเนินคดีเกี่ยวกับข้อมูลและอาชญากรรมทางคอมพิวเตอร์หรือการรวบรวมหลักฐานทางอิเล็กทรอนิกส์ในความผิดทางอาญา โดยจุดติดต่อดังกล่าวต้องมีความพร้อมตลอดเวลายี่สิบสี่ชั่วโมงต่อวัน เจ็ดวันต่อหนึ่งสัปดาห์ การให้ความช่วยเหลือดังข้างต้นนี้ รวมไปถึง การให้คำปรึกษาทางเทคนิค การเก็บรักษาข้อมูลตามที่กำหนดในข้อ 29 และ 30 การรวบรวมหลักฐานต่างๆ การให้ข้อมูลทางกฎหมาย และการระบุตำแหน่งผู้ต้องสงสัยเป็นต้น โดยจุดติดต่ออาจดำเนินการดังกล่าวโดยตรง หรือให้ความสะดวกในการดำเนินการก็ได้

ข้อ 35 วรรค 2 ได้กำหนดให้จุดติดต่อของรัฐภาคีมีขีดความสามารถในการติดต่อกับจุดติดต่อของรัฐภาคีอื่นได้อย่างรวดเร็ว ในขณะเดียวกัน หากจุดติดต่อดังกล่าวไม่มีหน้าที่

---

[61] *Ibid*., Para.297

[62] *Ibid*., Para.300

รับผิดชอบในการให้ความช่วยเหลือซึ่งกันและกันหรือส่งตัวผู้ร้ายข้ามแดนโดยตรง จุดติดต่อนั้นต้องสามารถประสานงานกับหน่วยงานรัฐที่มีหน้าที่รับผิดชอบได้อย่างรวดเร็ว

เพื่อให้จุดติดต่อสามารถดำเนินงานได้อย่างมีประสิทธิภาพ ข้อ35 วรรค 3 ของอนุสัญญาจึงกำหนดให้จุดติดต่อมีความพร้อมเพื่อให้ดำเนินงานได้อย่างลื่นไหลและสอดคล้องกับพัฒนาการทางเทคโนโลยี นอกจากนี้ ฝ่ายบุคลากรที่ประจำจุดติดต่อเองก็ต้องได้รับการฝึกฝนที่เหมาะสมเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ด้วย

ในการตั้งจุดติดต่อตามข้อ 35 รัฐภาคีมีดุลยพินิจว่า จะให้หน่วยงานใดทำหน้าที่ดังกล่าว บางรัฐอาจให้จุดติดต่ออยู่ในหน่วยงานกลางสำหรับการให้ความช่วยเหลือร่วมกันทางกฎหมาย ในขณะที่บางรัฐอาจให้จุดติดต่อของตนอยู่ในหน่วยงานตำรวจผู้เชี่ยวชาญด้านอาชญากรรมทางคอมพิวเตอร์โดยตรง อย่างไรก็ตาม รัฐภาคีควรคำนึงถึงความจำเป็นสำหรับการใช้ภาษาต่างประเทศในการติดต่อประสานงานกับจุดติดต่อของรัฐอื่นด้วย[63] นอกจากนี้ เครือข่าย 24/7 ของอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของสภายุโรป เปิดรับรัฐอื่นที่ไม่ได้ลงนามหรือให้สัตยาบันในอนุสัญญา ให้เข้าร่วมเป็นส่วนหนึ่งของเครือข่ายได้ด้วย[64]

3.5 บทบาทในการพัฒนากลไกความร่วมมือทางอาญาระหว่างประเทศสำหรับอาชญากรรมทางคอมพิวเตอร์ของความร่วมมือทางอาญาระหว่างประเทศภายใต้กรอบอนุสัญญากรุงบูดาเปสต์

หลังจากที่ได้อธิบายถึงเนื้อหาของกลไกความร่วมมือทางอาญาระหว่างประเทศภายใต้กรอบอนุสัญญากรุงบูดาเปสต์แล้ว ส่วนนี้ของวิทยานิพนธ์จะวิเคราะห์ต่อไปว่าความร่วมมือทางอาญากรอบนี้ จะสามารถ พัฒนากลไกความร่วมมือทางอาญาระหว่างประเทศสำหรับอาชญากรรมทางคอมพิวเตอร์ได้อย่างไรบ้าง หลักเกณฑ์ที่จะนำมาใช้ประกอบการวิเคราะห์จะประกอบไปด้วย ความสามารถในการสร้างมาตรฐานร่วมกันสำหรับกฎหมายภายในประเทศด้านอาชญากรรมทางคอมพิวเตอร์ ความสามารถในการขยายขอบเขต

---

[63] *Ibid*., Para.298,

[64] The cybercrime convention committee (T-CY). 2nd multilateral consultation of the parties report [Online]. Strasbourg: Council of Europe, 2007. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/T-CY%20%282007%29%2003%20E.pdf [2013, May 6], Para. 35

ความร่วมมือระหว่างประเทศให้ครอบคลุมอาชญากรรมทางคอมพิวเตอร์ และความสามารถในการรองรับความซับซ้อนของอาชญากรรมทางคอมพิวเตอร์ที่ทวีขึ้นไปตามกาลเวลา ซึ่งเป็นคุณสมบัติสำคัญสำหรับกลไกความร่วมมือทางอาญาสำหรับอาชญากรรมทางคอมพิวเตอร์ ดังที่ได้อธิบายไว้แล้วในท้ายบทที่ 2

เมื่อเปรียบเทียบกับคำแนะนำหรือหลักการด้านอาชญากรรมทางคอมพิวเตอร์ที่มีอยู่ก่อนหน้าแล้วอนุสัญญากรุงบูดาเปสต์ จะมีข้อแตกต่างอย่างสำคัญฐานะที่เป็นกฎหมายสนธิสัญญาระหว่างประเทศซึ่งสร้างพันธะกรณีระหว่างรัฐภาคี ดังนั้น ปัจจัยที่จะนำมาวิเคราะห์ในส่วนนี้จะไม่จำกัดเฉพาะเนื้อหาของอนุสัญญากรุงบูดาเปสต์และพิธีสารเพิ่มเติมเท่านั้น หากยังครอบคลุมไปถึงความเป็นสนธิสัญญาระหว่างประเทศของตราสารทั้งสองฉบับด้วย

3.5.1 บทบาทด้านการสร้างมาตรฐานร่วมกันสำหรับกฎหมายภายในประเทศด้านอาชญากรรมทางคอมพิวเตอร์

ในเบื้องต้น การที่อนุสัญญากรุงบูดาเปสต์และพิธีสารเพิ่มเติมมีฐานะเป็นสนธิสัญญาระหว่างประเทศนั้น สามารถส่งผลให้แนวทางการปรับใช้กลไกความร่วมมือทางอาญาระหว่างประเทศสอดคล้องกันมากขึ้น เพราะการเข้าเป็นภาคีของสนธิสัญญาเหล่านี้ด้วยการภาคยานุวัติหรืออนุวัติการนั้น เป็นการแสดงความยินยอมที่จะผูกพันตามอนุสัญญาและพิธีสารเพิ่มเติมแล้ว นอกจากนี้ รัฐผู้ลงนามแต่เพียงอย่างเดียวยังคงมีพันธะกรณีตามกฎหมายจารีตประเพณีระหว่างประเทศที่จะไม่ทำการใดๆ อันเป็นการขัดต่อวัตถุประสงค์ของอนุสัญญาอย่างสำคัญด้วย[65] คุณสมบัติข้อนี้นับว่าแตกต่างจากคำแนะนำหรือหลักการที่มีอยู่ก่อนหน้าการจัดทำอนุสัญญา ซึ่งจะเป็นเพียงการกำหนดกฎหมายที่ควรจะเป็น (*Lex Ferenda*) เท่านั้น โดยรัฐต่างๆที่เกี่ยวข้องยังไม่ได้แสดงความยินยอมที่จะผูกพันแต่อย่างใด

เมื่อเปรียบเทียบกับคำแนะนำหรือหลักการที่มีอยู่ก่อนหน้าแล้ว อนุสัญญากรุงบูดาเปสต์และพิธีสารเพิ่มเติม ยังสามารถสร้างมูลค่าเพิ่มในการสร้างมาตรฐานทางกฎหมายภายในได้หลายประการ รายละเอียดมีดังต่อไปนี้

---

[65] Vienna Convention on Law of Treaties, Art. 18

3.5.1.1 การสร้างมาตรฐานด้านกฎหมายสารบัญญัติ

ฐานความผิดตามอนุสัญญากรุงบูดาเปสต์นั้นนับว่าครอบคลุมด้านความผิดต่อความลับ ความสมบูรณ์ และบูรณภาพของข้อมูลและระบบคอมพิวเตอร์ และความผิดที่เกี่ยวข้องกับคอมพิวเตอร์ ดังที่ได้ปรากฏอยู่ในคำแนะนำและหลักการที่มีอยู่ก่อนหน้าการจัดทำอนุสัญญา อย่างไรก็ดี อนุสัญญากรุงบูดาเปสต์จะกำหนดองค์ประกอบความผิดสำหรับฐานความผิดต่างๆ อาทิ องค์ประกอบด้านการกระทำโดยปราศจากสิทธิ เจตนาพิเศษ ให้มีรายละเอียดมากขึ้น อีกทั้งยังมีการเพิ่มเติมบทบัญญัติเกี่ยวกับความรับผิดต่างๆด้วย อาทิ ความรับผิดสำหรับนิติบุคคล หรือความผิดในขั้นพยายามกระทำผิด ความผิดฐานะผู้ใช้และผู้สนับสนุนเป็นต้น ด้วยเหตุนี้รัฐภาคีจึงมีแนวทางการปรับใช้ที่ชัดเจนมากขึ้น

อนุสัญญากรุงบูดาเปสต์และพิธีสารเพิ่มเติมยังได้เพิ่มเติมฐานความผิดบางอย่างเพื่อให้สอดคล้องกับความเปลี่ยนแปลงทางเทคโนโลยีด้วย โดยฐานความผิดที่เกี่ยวข้องกับเนื้อหานั้นถูกกำหนดขึ้นมาเนื่องจากเครือข่ายอินเตอร์เน็ตสามารถรองรับและแสดงเนื้อหาที่มีปริมาณและความซับซ้อนมากขึ้น อีกทั้งยังมีผู้เข้าใช้งานในปริมาณที่สูงขึ้นตามไปด้วย ข้อเท็จจริงดังกล่าวยังส่งผลให้อนุสัญญากรุงบูดาเปสต์กำหนดฐานความผิดที่เกี่ยวข้องกับการละเมิดลิขสิทธิ์และสิทธิข้างเคียงไว้ในข้อ 10 ซึ่งจะครอบคลุมผลงานอันมีลิขสิทธิ์และสิทธิข้างเคียงตามที่กำหนดไว้ในข้อตกลงระหว่างประเทศด้านทรัพย์สินทางปัญญาฉบับต่างๆ โดยไม่ได้จำกัดอยู่เฉพาะโปรแกรมคอมพิวเตอร์หรือแผงวงจรรวมเช่นเดิมแต่อย่างใด ในขณะเดียวกัน เนื่องด้วยเทคโนโลยีทางคอมพิวเตอร์ในปัจจุบันอำนวยความสะดวกให้อาชญากรทางคอมพิวเตอร์เข้ามามีปฏิสัมพันธ์และซื้อขายแลกเปลี่ยน อนุสัญญาทางคอมพิวเตอร์จึงได้เพิ่มเติมฐานความผิดเกี่ยวกับการใช้อุปกรณ์ในทางที่ผิดไว้ในข้อ 6 ด้วย

นอกจากนี้ อนุสัญญากรุงบูดาเปสต์และพิธีสารเพิ่มเติมได้ตระหนักว่า รัฐต่างๆ อาจมีแนวทางการตีความและปรับใช้กฎหมายแตกต่างกันไป ถึงแม้จะมีกฎหมายภายในที่คล้ายคลึงกันก็ตาม เพราะฉะนั้น อนุสัญญาจึงยังคงอนุญาตให้รัฐภาคีสามารถตั้งข้อสงวนเกี่ยวกับองค์ประกอบความผิดบางประการในฐานความผิดต่างๆได้ ยกตัวอย่างเช่น กรณีการกำหนดฐานความผิดสำหรับวัตถุลามกอนาจารที่ปรากฏภาพเสมือนจริงของผู้เยาว์หรือบุคคลที่อายุเกินกว่าเกณฑ์แต่มีรูปร่างหน้าตาดูคล้ายผู้เยาว์ เป็นต้น แม้ว่าข้อสงวนเหล่านี้จะส่งผลจำกัดการให้ความร่วมมือทางอาญาได้ในระดับหนึ่งก็ตาม แต่ในอีกด้านหนึ่ง ก็จัดได้ว่า

อนุสัญญากรุงบูดาเปสต์สร้างความยืดหยุ่นแก่รัฐภาคีที่มีความแตกต่างกันทางแนวคิดด้านการตีความและปรับใช้กฎหมาย ให้สามารถเข้ามาให้ความร่วมมือทางอาญาด้านอาชญากรรมทางคอมพิวเตอร์ภายใต้ฐานทางกฎหมายเดียวกันได้ นอกจากนี้ การที่อนุสัญญากรุงบูดาเปสต์และพิธีสารเพิ่มเติมได้กำหนดให้รัฐที่ตั้งข้อสงวนแจ้งเรื่องไปยังเลขาธิการสภายุโรปนั้น จะช่วยให้รัฐอื่นๆ สามารถทราบข้อมูลดังกล่าวและอาจวางแผนการดำเนินการไว้รองรับล่วงหน้าได้เช่นกัน

ในขณะเดียวกัน อนุสัญญากรุงบูดาเปสต์ยังคงพยายามที่จะลดความแตกต่างด้านการตีความและปรับใช้กฎหมายของรัฐภาคีควบคู่ไปด้วยด้วย โดยในกรณีการตั้งข้อสงวนนั้น อนุสัญญาข้อ 43 วรรค 2 กำหนดให้รัฐที่ตั้งข้อสงวน ทำการเพิกถอนข้อสงวนที่ตนตั้งไว้ทั้งหมดหรือบางส่วนในทันทีที่สถานการณ์เอื้ออำนวย ส่วน 43 วรรค 3 นั้น จะอนุญาตให้เลขาธิการสภายุโรปดำเนินการสอบถามรัฐภาคีที่ตั้งข้อสงวนไว้เป็นระยะๆเพื่อให้ทราบถึงความเป็นไปได้ในการเพิกถอนข้อสงวนดังกล่าวด้วย

นอกจากนี้ กลไกความร่วมมือทางอาญาภายใต้กรอบอนุสัญญากรุงบูดาเปสต์ยังสามารถลดปัญหาที่เกิดจากความแตกต่างแนวคิดทางกฎหมายด้วยการจัดทำพิธีสารเพิ่มเติมรายละเอียดของอนุสัญญา ทั้งนี้ ความผิดที่เกี่ยวข้องกับการเหยียดหยามดูหมิ่นเชื้อชาติที่ปรากฏในพิธีสารเพิ่มเติม นับเป็นหนึ่งในประเด็นปัญหาที่รัฐมีความเห็นไม่ตรงกันว่าควรกำหนดให้เป็นฐานความผิดทางอาญาหรือไม่ การจัดทำพิธีสารเพิ่มเติมจึงเพิ่มความยืดหยุ่นให้รัฐที่กำหนดฐานความผิดเกี่ยวกับการเหยียดหยามเชื้อชาติสามารถให้ความร่วมมือทางอาญาระหว่างกันได้ ในขณะที่ยังคงสามารถให้ความร่วมมือในประเด็นอื่นๆ กับรัฐที่มีความเห็นแตกต่างออกไปได้เช่นเดียวกัน

3.5.1.2 **การสร้างมาตรฐานด้านกฎหมายวิธีสบัญญัติ**

สำหรับด้านกฎหมายวิธีสบัญญัติ อนุสัญญากรุงบูดาเปสต์ได้นำอำนาจการสืบสวนจากคำแนะนำหรือหลักการที่มีอยู่ก่อนหน้ามาบัญญัติรวบรวมไว้เช่นกัน ไม่ว่าจะเป็นการเก็บรักษาข้อมูลทางคอมพิวเตอร์อย่างรวดเร็ว การค้นและยึดข้อมูล การดักรับข้อมูล การกำหนดหน้าที่ของผู้ให้บริการในการให้ความร่วมมือกับเจ้าหน้าที่รัฐ อย่างไรก็ตาม อนุสัญญากรุงบูดาเปสต์จะเพิ่มเติมรายละเอียดด้านการดำเนินการต่างๆ ระยะเวลา และเงื่อนไขอื่นๆ ส่งผลให้รัฐภาคีมีแนวทางการปฏิบัติตามที่ชัดเจนมากขึ้น

นอกจากนี้ จะเห็นได้ว่า อนุสัญญากรุงบูดาเปสต์และพิธีสารเพิ่มเติมได้กำหนดกรอบเงื่อนไขและมาตรการป้องกันสิทธิมนุษยชนและเสรีภาพไว้ในข้อ 15 ด้วย เพื่อให้การสืบสวนคดีอาชญากรรมทางคอมพิวเตอร์นั้นสามารถรักษาความสมดุลระหว่างการหาตัวผู้กระทำความผิดและการรักษาสิทธิส่วนบุคคลของผู้ที่เกี่ยวข้องไว้ได้ โดยหลักเกณฑ์ที่ข้อ 15 อ้างอิงถึงจะเป็นสนธิสัญญาระหว่างประเทศด้านสิทธิมนุษยชน อาทิ อนุสัญญายุโรปปี 1950 ว่าด้วยการปกป้องสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐาน (1950 European Convention for the Protection of Human Rights and Fundamental Freedoms) กติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (International Covenant on Civil and Political Rights) เป็นต้น เมื่อเทียบกับหลักการและคำแนะนำก่อนหน้าอนุสัญญากรุงบูดาเปสต์แล้ว รัฐจะถูกแนะนำให้ใช้มาตรการสืบสวนคดีอาชญากรรมทางคอมพิวเตอร์โดยมีมาตรการป้องกันสิทธิมนุษยชนและเสรีภาพเช่นเดียวกัน หากแต่จะหมายถึงมาตรการป้องกันทางกฎหมายตามกฎหมายภายในรัฐ ไม่ได้มีการอ้างอิงหลักเกณฑ์ระหว่างประเทศใดเป็นการเฉพาะเจาะจง เพราะฉะนั้น ข้อ 15 ของอนุสัญญากรุงบูดาเปสต์สามารถส่งเสริมให้รัฐมีแนวทางด้านกฎหมายวิธีสบัญญัติที่สอดคล้องกันมากขึ้น

3.5.2 บทบาทด้านการขยายขอบเขตความร่วมมือระหว่างประเทศให้ครอบคลุมอาชญากรรมทางคอมพิวเตอร์

จะเห็นได้ว่า อนุสัญญากรุงบูดาเปสต์ได้ทำหน้าที่เป็นฐานทางกฎหมายสำหรับการให้ความร่วมมือทางอาญาระหว่างประเทศโดยตรง โดยข้อ 23 จะกำหนดหน้าที่ให้รัฐภาคีต่างๆ ให้ความร่วมมือระหว่างกันตามบทบัญญัติของอนุสัญญาเกี่ยวกับการส่งตัวผู้ร้ายข้ามแดน การให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายโดยทั่วไปและโดยวิธีการเฉพาะสำหรับการส่งตัวผู้ร้ายข้ามแดนนั้น ข้อ 24 วรรค 2 ถึง 4 จะกำหนดให้ความผิดตามข้อ 2-11 ของอนุสัญญา เป็นความผิดที่ส่งตัวผู้ร้ายข้ามแดนได้ระหว่างรัฐภาคีได้ ในขณะเดียวกัน ข้อ 27 ของอนุสัญญาจะกำหนดเงื่อนไขและกระบวนการสำหรับให้ความช่วยเหลือในกรณีที่รัฐภาคีของอนุสัญญาไม่ได้ทำข้อตกลงด้านการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายไว้ระหว่างกันอีกด้วย

เมื่อเปรียบเทียบกับกลไกการให้ความร่วมมือทางอาญาระหว่างประเทศโดยทั่วไปแล้ว อนุสัญญากรุงบูดาเปสต์ได้กำหนดให้รัฐภาคีรายงานข้อมูลเกี่ยวกับหน่วยงานที่ทำหน้าที่จัดการ

ด้านการส่งตัวผู้ร้ายข้ามแดน และหน่วยงานกลางสำหรับให้ความช่วยเหลือซึ่งกันและกันทางกฎหมาย ไปยังเลขาธิการสภายุโรป โดยเลขาธิการสภายุโรปจะต้องจัดทำรายชื่อหน่วยงานดังกล่าวและทำให้ข้อมูลเป็นปัจจุบันอยู่เสมอ การกระทำเช่นนี้ ย่อมช่วยให้รัฐภาคีสามารถติดต่อระหว่างกันได้สะดวกยิ่งขึ้น

สำหรับการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายโดยทั่วไปนั้น จะเห็นได้ว่าอนุสัญญากรุงบูดาเปสต์ส่งเสริมให้การให้ความช่วยเหลือเป็นไปอย่างรวดเร็ว และยืดหยุ่นมากขึ้น โดยข้อ 27 วรรค 5,6,7 ให้รัฐภาคีปรึกษาหารือกันเพื่อเลื่อนกำหนดการให้ความช่วยเหลือหรือให้ความช่วยเหลือเพียงบางส่วนได้ นอกจากนี้ อนุสัญญากรุงบูดาเปสต์ยังรองรับให้รัฐภาคีสามารถให้ความช่วยเหลือกันทั้งผ่านทางหน่วยงานกลาง การติดต่อสื่อสารกันระหว่างหน่วยงานทางตุลาการ และการติดต่อกันโดยตรงระหว่างหน่วยงานผู้มีอำนาจหน้าที่ การกำหนดช่องทางการติดต่อประสานงานที่แตกต่างกันออกไปนี้ ไม่เพียงแต่ส่งเสริมให้รัฐภาคีติดต่อกันได้รวดเร็วขึ้นเท่านั้น หากยังสามารถช่วยให้รัฐภาคีเลือกใช้ช่องทางที่เหมาะสมตามสถานการณ์ได้

อนุสัญญากรุงบูดาเปสต์ยังได้กำหนดการให้ความช่วยเหลือด้วยการให้ข้อมูลโดยทันทีไว้ในข้อ 26 ซึ่งรัฐผู้ให้ความช่วยเหลือสามารถให้ความช่วยเหลือไปก่อนโดยไม่ต้องรอคำขอความช่วยเหลือ ส่งผลให้การให้ความร่วมมือซึ่งกันและกันทางกฎหมายสำหรับอาชญากรรมทางคอมพิวเตอร์เป็นไปอย่างรวดเร็วและกว้างขวางขึ้น อีกทั้งส่งเสริมความร่วมมือระหว่างรัฐภาคีกันต่อไปในระยะยาว นอกจากนี้ การกำหนดเงื่อนไขเกี่ยวกับการรักษาความลับและจำกัดวิธีการใช้ตามข้อ 28 ยังส่งเสริมให้การสืบสวนคดีอาชญากรรมทางคอมพิวเตอร์เป็นไปอย่างปลอดภัยมากขึ้นอีกด้วย

สำหรับการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายด้วยวิธีการเฉพาะนั้น อนุสัญญากรุงบูดาเปสต์จะนำวิธีการต่างๆ จากกรอบความร่วมมือที่มีอยู่ก่อนหน้ามาบัญญัติรวบรวมไว้ ไม่ว่าจะเป็นการให้ความช่วยเหลือด้วยการเก็บรักษาข้อมูลทางคอมพิวเตอร์อย่างรวดเร็ว การค้นและยึดข้อมูลทางคอมพิวเตอร์ การดักรับข้อมูล การติดตามที่มาของการสื่อสาร การเข้าถึงข้อมูลข้ามแดนในรูปแบบที่ไม่ต้องร้องขอความช่วยเหลือจากรัฐอื่นล่วงหน้า หรือการจัดตั้งเครือข่ายจุดติดต่อตลอดเวลา

วิธีการเฉพาะเหล่านี้ นับว่าเป็นการนำอำนาจสืบสวนคดีอาชญากรรมทางอาชญากรรมทางคอมพิวเตอร์ มาขยายผลในการให้ความร่วมมือทางอาญาระหว่างประเทศด้วย อย่างไรก็ตาม อนุสัญญากรุงบูดาเปสต์จะดำเนินการขยายรายละเอียดของบทบัญญัติเหล่านี้ เพื่อให้การสืบสวนคดีอาชญากรรมทางคอมพิวเตอร์รวดเร็วทันต่อสถานการณ์มากขึ้น โดยในด้านการให้ความช่วยเหลือด้วยการเก็บรักษาข้อมูลภายใต้ข้อ 29 นั้น อนุสัญญากรุงบูดาเปสต์จะกำหนดขั้นตอน เงื่อนไขและระยะเวลาในการให้ความช่วยเหลือไว้อย่างชัดเจน ส่วนอนุสัญญาข้อ 35 ก็จะกำหนดหน้าที่และคุณสมบัติของหน่วยงานที่จะเป็นจุดติดต่อประจำเครือข่ายไว้เช่นเดียวกัน

นอกจากนี้ อนุสัญญากรุงบูดาเปสต์ยังมีความยืดหยุ่นไว้สำหรับรัฐภาคีให้สามารถให้ความร่วมมือทางอาญาระหว่างประเทศในลักษณะที่อนุสัญญาไม่ครอบคลุมได้ในระดับหนึ่ง อาทิ การส่งตัวผู้ร้ายข้ามแดนในอาชญากรรมผิดที่อยู่นอกเหนือฐานความผิดตามข้อ 2 ถึง11 หรือการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายด้วยวิธีการที่อนุสัญญาไม่กล่าวถึงไว้ ดังที่จะเห็นได้จากหลักทั่วไปในการให้ความร่วมมือทางระหว่างประเทศในข้อ 23 ซึ่งกำหนดให้รัฐภาคีให้ความร่วมมือกันโดยการปรับใช้กฎหมายที่เกี่ยวข้องและมีผลบังคับใช้กับรัฐภาคีทั้งในระดับภายในและระหว่างประเทศ ควบคู่ไปกับการปฏิบัติตามบทบัญญัติด้านความร่วมมือระหว่างประเทศในข้อ 23-35 ของอนุสัญญา นอกจากนี้ หลักทั่วไปในการส่งตัวผู้ร้ายข้ามแดนในข้อ 24 วรรค 5 ยังกำหนดให้เงื่อนไขต่างๆในการส่งตัวผู้ร้ายข้ามแดนเป็นไปตามกฎหมายของรัฐผู้รับคำขอให้ส่งตัวข้ามแดนหรือตามสนธิสัญญาด้านการส่งตัวผู้ร้ายข้ามแดนที่มีผลบังคับใช้

เพราะฉะนั้น หากรัฐภาคีมีกฎหมายภายในหรือได้จัดทำสนธิสัญญาที่เอื้ออำนวยให้สามารถส่งตัวผู้ร้ายข้ามแดนได้ในฐานความผิดที่อนุสัญญากรุงบูดาเปสต์ไม่ครอบคลุม หรือ อนุญาตให้รัฐให้ความช่วยเหลือด้วยวิธีการนอกอนุสัญญา รัฐภาคียังคงสามารถดำเนินการตามกฎหมายภายในของตนหรือสนธิสัญญาฉบับอื่นๆได้ แนวคิดดังกล่าวนี้ ยังสะท้อนให้เห็นได้จากข้อ 39 ของอนุสัญญาซึ่งอนุญาตรัฐภาคีสามารถปรับใช้และดำเนินการตามสนธิสัญญาด้านความร่วมมือทางอาญาฉบับอื่นๆได้ตามปกติ หากแต่ต้องเป็นไปโดยสอดคล้องกับหลักการและวัตถุประสงค์ของอนุสัญญากรุงบูดาเปสต์

3.5.3 บทบาทในการรองรับความซับซ้อนของอาชญากรรมทางคอมพิวเตอร์ที่ทวีขึ้นไปตามกาลเวลา

พัฒนาการของเทคโนโลยีทางคอมพิวเตอร์สามารถส่งผลให้อาชญากรรมทางคอมพิวเตอร์ซับซ้อนมากขึ้น และอาจส่งผลให้หลักเกณฑ์ที่มีอยู่ในปัจจุบันไม่เพียงพอต่อการรองรับอาชญากรรมได้ ถึงแม้ในความเป็นจริงนั้น ผู้จัดทำกลไกความร่วมมือทางอาญาจะไม่สามารถคาดเดาความเปลี่ยนแปลงทางเทคโนโลยีและผลกระทบเชิงกฎหมายได้ครบทุกประเด็นปัญหาก็ตาม กลไกความร่วมมือทางอาญาสำหรับอาชญากรรมทางคอมพิวเตอร์ก็ควรที่จะยืดหยุ่นต่อการแก้ไขเพิ่มเติมรายละเอียด อีกทั้งยังมีช่องทางให้รัฐภาคีสามารถติดตามความเปลี่ยนแปลงทาเทคโนโลยีและทราบถึงผลกระทบที่ตามมาได้ ในการนี้ กลไกความร่วมมือทางอาญาภายใต้กรอบอนุสัญญากรุงบูดาเปสต์ได้มีมาตรการรองรับไว้ในหลายรูปแบบด้วยกัน

ในประการแรก อนุสัญญากรุงบูดาเปสต์ได้ใช้ถ้อยคำที่เป็นกลางทางเทคโนโลยีไว้ทั้งในบทบัญญัติด้านกฎหมายสารบัญญัติ กฎหมายวิธีสบัญญัติ และความร่วมมือระหว่างประเทศ โดยจะเห็นได้ว่าบทบัญญัติในด้านการกำหนดฐานความผิดต่างๆนั้นจะระบุไปยังผลลัพธ์ที่เกิดจากการกระทำความผิดเป็นสำคัญ ถึงแม้ว่าเทคโนโลยีต่างๆจะเปลี่ยนแปลงไป แต่ผลกระทบที่เกิดกับข้อมูลและระบบคอมพิวเตอร์ การสูญเสียทรัพย์สิน การเผยแพร่วัตถุต้องห้าม หรือการถูกละเมิดลิขสิทธิ์ ก็จะยังเกิดขึ้นในขั้นสุดท้ายอยู่ดี สำหรับด้านกฎหมายวิธีสบัญญัติและการให้ความร่วมมือระหว่างประเทศนั้น ก็เป็นเช่นกัน กล่าวคืออนุสัญญาจะมุ่งเน้นไปยังผลลัพธ์ที่จะเกิดขึ้นกับหลักฐาน มากกว่าการใช้เทคโนโลยีประเภทใดประเภทหนึ่งเป็นการเฉพาะเจาะจง

นอกจากนี้ ในด้านการใช้อำนาจสืบสวนอาชญากรรมทางคอมพิวเตอร์และการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายนั้น ขอบเขตการปรับใช้ไม่ได้จำกัดเฉพาะฐานความผิดที่อนุสัญญากำหนดไว้เท่านั้น หากแต่ยังครอบคลุมถึงอาชญากรรมทุกประเภทที่ใช้เทคโนโลยีทางคอมพิวเตอร์ และการรวบรวมหลักฐานทางอาชญากรรมที่อยู่ในข้อมูลอิเล็กทรอนิกส์ เพราะฉะนั้น จะเห็นได้ว่า การใช้อำนาจสืบสวนอาชญากรรมทางคอมพิวเตอร์และการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายภายใต้อนุสัญญา สามารถรองรับอาชญากรรมประเภทใหม่ๆ ต่อไปในอนาคตได้ด้วย

ในขณะเดียวกัน ด้วยการปรึกษาหารือกันระหว่างรัฐภาคีตามอนุสัญญาข้อ 46 รัฐภาคีต่างๆยังสามารถแลกเปลี่ยนประสบการณ์การปรับใช้อนุสัญญา และระบุประเด็นปัญหาใหม่ๆ ที่เป็นผลมาจากพัฒนาการสำคัญในด้านกฎหมาย ด้านนโยบาย หรือด้านเทคโนโลยีที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์ และกระบวนการรวบรวมหลักฐานทางอิเล็กทรอนิกส์ จะเห็นได้ว่ากระบวนการปรึกษาหารือนี้มีบทบาทส่งเสริมการปรับปรุงแก้ไขอนุสัญญา และช่วยให้รัฐภาคีทั้งหลายเข้ามีส่วนร่วมในการติดตามผลของอนุสัญญาได้อย่างเท่าเทียมกัน[66]

จากที่ได้ปรึกษาหารือระหว่างกัน หากรัฐภาคีพบว่า อนุสัญญาส่วนใดไม่สามารถรองรับกับบริบททางเทคโนโลยีที่เปลี่ยนแปลงไปได้ ผลลัพธ์ดังกล่าวจะนำไปสู่การปรับปรุงแก้ไขอนุสัญญาต่อไป โดยอาจจะอาศัยวิธีการจัดทำพิธีสารเพิ่มเติม หรือแก้ไขตัวอนุสัญญาตามขั้นตอนในข้อ 44 ได้

ในการนี้ ข้อ 44 วรรค 1 แห่งอนุสัญญากรุงบูดาเปสต์ ได้อนุญาตให้รัฐภาคีใดๆ สามารถยื่นเสนอแก้ไขเปลี่ยนแปลงอนุสัญญา โดยให้เลขาธิการสภายุโรปติดต่อแจ้งเรื่องดังกล่าวไปยังบรรดารัฐสมาชิกของสภายุโรป และบรรดารัฐที่ไม่ได้เป็นสมาชิกสภายุโรปแต่ได้เข้าร่วมเจรจาจัดทำอนุสัญญา รัฐที่เข้าภาคยานุวัติและรัฐที่ได้รับเชิญให้เข้าภาคยานุวัติอนุสัญญา

ข้อเสนอในการแก้ไขนั้น จะถูกส่งไปยังคณะกรรมาธิการด้านปัญหาอาชญากรรมของสภายุโรป (CDPC) โดยทางคณะกรรมการจะส่งเรื่องพร้อมความเห็นของตนไปยังคณะมนตรีสภายุโรปต่อไป ตามข้อ 44 วรรค 2 หลังจากนั้น คณะมนตรีจะพิจารณาคำเสนอแก้ไขประกอบความเห็นของกรรมการ CDPC อีกทั้งปรึกษาหารือกับรัฐภาคีที่ไม่ใช่สมาชิกสภายุโรป เพื่อตัดสินใจรับรองการแก้ไขดังกล่าว ท้ายที่สุด ทางคณะมนตรีจะต้องส่งเนื้อหาที่ได้รับการแก้ไขไปให้รัฐภาคีต่างๆรับรองต่อไป และการแก้ไขอนุสัญญาจะมีผลบังคับใช้หลังจากที่รัฐภาคีทุกรัฐได้แสดงเจตจำนงรับรองการแก้ไขไปยังเลขาธิการสภาได้ยุโรปเป็นเวลา 13 วัน ซึ่งเป็นไปตามข้อ 44 วรรค 5

---

[66] Council of Europe. Convention on cybercrime explanatory report,Para.328

จากการศึกษาวิจัยในบทที่ 3 จะพบว่า เนื้อหาของกลไกความร่วมมือกรอบอนุสัญญากรุงบูดาเปสต์นั้น จะสร้างมาตรฐานทางกฎหมายสารบัญญัติและกฎหมายวิธีสบัญญัติภายในประเทศ โดยนำแนวทางของคำแนะนำและหลักการที่จัดทำขึ้นมาก่อนหน้ามารวบรวมไว้ หากแต่จะกำหนดรายละเอียดบางส่วนเพิ่มเติมเพื่อให้แนวทางการปรับใช้ของรัฐชัดเจนมากยิ่งขึ้น

โดยส่วนกฎหมายสารบัญญัตินั้น จะกำหนดองค์ประกอบความผิดและเพิ่มเติมบทบัญญัติเกี่ยวกับความรับผิดของความผิดฐานต่างๆ อีกทั้งเพิ่มฐานความผิดที่เกี่ยวข้องกับเนื้อหาและขยายขอบเขตของฐานความผิดที่เกี่ยวกับการละเมิดลิขสิทธิ์ให้กว้างยิ่งขึ้น บทบัญญัติเหล่านี้ยังอนุญาตให้รัฐภาคีสามารถตั้งข้อสงวนบางประการ เพื่อสร้างความยืดหยุ่นแก่รัฐภาคีที่มีแนวคิดแตกต่างกัน สำหรับด้านกฎหมายวิธีสบัญญัตินั้น จะมีการกำหนดกรอบเงื่อนไขและมาตรการป้องกันสิทธิมนุษยชนและเสรีภาพ เพื่อรักษาความสมดุลระหว่างการหาตัวผู้กระทำความผิด และการรักษาสิทธิส่วนบุคคลของผู้ที่เกี่ยวข้องในการสืบสวนคดีอาชญากรรมทางคอมพิวเตอร์ ไว้ในข้อ 15 ของอนุสัญญาอีกด้วย

สำหรับด้านการให้ความร่วมมือระหว่างประเทศนั้น อนุสัญญากรุงบูดาเปสต์ไม่เพียงแต่ทำให้รัฐภาคีสามารถส่งตัวผู้ร้ายข้ามแดนและให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายในคดีอาชญากรรมทางคอมพิวเตอร์ได้เท่านั้น หากแต่ยังกำหนดเงื่อนไข และวิธีการให้ความช่วยเหลือด้วยบทบัญญัติเฉพาะเพื่อให้การดำเนินการเป็นไปอย่างรวดเร็ว ยืดหยุ่น และปลอดภัย สามารถรองรับกับบริบทของอาชญากรรมทางคอมพิวเตอร์ได้ดีขึ้น

ในขณะเดียวกัน อนุสัญญากรุงบูดาเปสต์จะมีความยืดหยุ่นในการรองรับต่อพัฒนาการทางเทคโนโลยีด้วย โดยบทบัญญัติเกี่ยวกับฐานความผิดและอำนาจการสืบสวนของอนุสัญญานั้นจะไม่อ้างอิงกับเทคโนโลยีประเภทใดประเภทหนึ่งเป็นการเฉพาะ ส่วนขอบเขตการปรับใช้อำนาจการสืบสวนและการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายนั้น ก็จะไม่จำกัดเฉพาะฐานความผิดที่อนุสัญญาและพิธีสารเพิ่มเติมบัญญัติไว้เท่านั้น หากแต่ครอบคลุมอาชญากรรมที่ใช้คอมพิวเตอร์เป็นเครื่องมือทุกประเภท และการรวบรวมหลักฐานที่อยู่ในรูปแบบข้อมูลคอมพิวเตอร์ของอาชญากรรมด้วย

นอกจากเนื้อหาของบทบัญญัติต่างๆแล้ว จะเห็นได้ว่าการที่อนุสัญญากรุงบูดาเปสต์มีผลผูกพันรัฐภาคีในฐานะสนธิสัญญาระหว่างประเทศ อีกทั้งเป็นฐานทางกฎหมายในการให้ความร่วมมือทางอาญาระหว่างประเทศโดยตรงนั้น จะยิ่งส่งเสริมให้การสร้างมาตรฐานทางกฎหมายภายในประเทศ และการให้ความร่วมมือระหว่างประเทศมีประสิทธิภาพและสอดคล้องกันยิ่งขึ้น ส่วนกลไกการปรึกษาหารือระหว่างรัฐภาคีและการแก้ไขอนุสัญญาของอนุสัญญากรุงบูดาเปสต์นั้น ก็ทำให้กลไกความร่วมมือสามารถติดตามผลการปรับใช้ และปรับปรุงเนื้อหาของตัวเองต่อไปได้ในระยะยาว นอกจากนี้ รัฐภาคียังสามารถติดต่อกันได้สะดวกมากขึ้นได้เนื่องจากอนุสัญญากำหนดหน้าที่ในการรายงานข้อมูลเกี่ยวกับหน่วยงานที่เกี่ยวข้องกับการให้ความร่วมมือระหว่างประเทศ ท้ายที่สุด การจัดทำพิธีสารเพิ่มเติมก็เป็นทางเลือกที่สร้างความยืดหยุ่นให้กับรัฐที่มีแนวคิดทางกฎหมายแตกต่างกันไปได้ด้วย

เพราะฉะนั้น จะสรุปได้ว่า กลไกความร่วมมือทางอาญาภายใต้กรอบอนุสัญญากรุงบูดาเปสต์นั้น มีบทบาททั้งในด้านการสร้างมาตรฐานร่วมกันสำหรับกฎหมายภายในประเทศด้านอาชญากรรมทางคอมพิวเตอร์ การขยายขอบเขตความร่วมมือระหว่างประเทศให้ครอบคลุมอาชญากรรมทางคอมพิวเตอร์ และการรองรับความซับซ้อนของอาชญากรรมทางคอมพิวเตอร์ที่ทวีขึ้นไปตามกาลเวลา ส่วนการประเมินผลลัพธ์ว่า บทบาทเหล่านี้ของกลไกความร่วมมือภายใต้กรอบอนุสัญญากรุงบูดาเปสต์จะตอบสนองต่ออาชญากรรมทางคอมพิวเตอร์ได้เพียงใดนั้น จะ ได้รับการนำเสนอในบทถัดไป

บทที่ 4

การประเมินผลลัพธ์ของกลไกความร่วมมือทางอาญา ภายใต้กรอบอนุสัญญากรุงบูดาเปสต์

จากเนื้อหาบทที่แล้ว จะเห็นได้ว่ากลไกความร่วมมือทางอาญาภายใต้กรอบอนุสัญญาบูดาเปสต์ได้สร้างมูลค่าเพิ่มขึ้นมาจากกลไกความร่วมมือทางอาญาระหว่างประเทศทั่วไปอยู่หลายประการ เพราะกลไกความร่วมมือกรอบนี้สามารถสร้างมาตรฐานร่วมกันด้านกฎหมายภายในเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ให้แก่รัฐภาคี อีกทั้งยังได้ขยายขอบเขตความร่วมมือระหว่างประเทศให้ครอบคลุมอาชญากรรมทางคอมพิวเตอร์ และสามารถรองรับความซับซ้อนของอาชญากรรมทางคอมพิวเตอร์ที่ทวีขึ้นไปตามกาลเวลาได้อีกด้วย อย่างไรก็ดี กลไกความร่วมมือทางอาญาภายใต้กรอบอนุสัญญากรุงบูดาเปสต์ ยังจำเป็นต้องได้รับการประเมินผลลัพธ์ต่อไปอีกว่า สามารถตอบสนองอาชญากรรมทางคอมพิวเตอร์ได้มากน้อยเพียงใด

เนื้อหาของบทที่ 4 นี้จะแบ่งออกเป็นหกส่วน โดยส่วนที่หนึ่งถึงสามจะอธิบายถึงแนวทางการปรับใช้อนุสัญญากรุงบูดาเปสต์โดยรัฐภาคีในด้านการส่งตัวผู้ร้ายข้ามแดน การให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายโดยทั่วไป และการให้ความช่วยเหลือด้วยวิธีเฉพาะตามลำดับ หลังจากนั้น ส่วนที่สี่ของบทจะอธิบายถึงการปรับใช้อนุสัญญากรุงบูดาเปสต์ในระดับระหว่างประเทศ สำหรับส่วนที่ห้านั้น จะเป็นการประเมินผลลัพธ์กลไกความร่วมมือทางอาญาภายใต้กรอบอนุสัญญากรุงบูดาเปสต์ ซึ่งจะพิจารณาจากปัจจัยสามประการ ได้แก่ ความสอดคล้องระหว่างเนื้อหาของกลไกความร่วมมือกับบริบททางเทคโนโลยีและข้อเท็จจริง แนวทางการปรับใช้โดยรัฐภาคี และแนวทางการปรับใช้ระดับระหว่างประเทศ ท้ายที่สุด เนื้อหาส่วนที่หกจะวิเคราะห์ถึงแนวทางสำหรับตอบสนองอุปสรรคที่ได้จากการประเมินผลลัพธ์กลไกความร่วมมือทางอาญาภายใต้กรอบอนุสัญญากรุงบูดาเปสต์

4.1 การปรับใช้กลไกการส่งตัวผู้ร้ายข้ามแดนภายใต้กรอบอนุสัญญากรุงบูดาเปสต์

นอกเหนือจากอนุสัญญากรุงบูดาเปสต์แล้ว ข้อตกลงเกี่ยวกับการส่งตัวผู้ร้ายข้ามแดนฉบับอื่นที่มีผลบังคับใช้กันระหว่างรัฐภาคีในภูมิภาคยุโรปได้แก่ อนุสัญญาว่าด้วยการส่งตัวผู้ร้ายข้ามแดนของสภายุโรป (ETS No.24) อีกทั้งยังมีการนำหมายจับภูมิภาคยุโรป (European Arrest Warrant) มาปรับใช้เพื่อให้รัฐต่างๆในสหภาพยุโรปสามารจับกุมผู้กระทำผิดที่เดินทางเข้ามาในดินแดน

ของตนได้ ส่วนการส่งตัวผู้ร้ายข้ามแดนระหว่างรัฐภาคีภายในและภายนอกภูมิภาคยุโรปจะอาศัยข้อตกลงทวิภาคีระหว่างรัฐที่เกี่ยวข้อง ซึ่งอาจส่งผลให้เกิดความแตกต่างกันเรื่องหลักเกณฑ์การส่งตัวผู้ร้ายข้ามแดนระหว่างประเทศที่เป็นสมาชิกสภายุโรปและประเทศที่ไม่ได้เป็นสมาชิก

ในระดับรัฐภาคีนั้น รัฐส่วนใหญ่ใช้หลักเกณฑ์การส่งตัวผู้ร้ายข้ามแดนทั่วไปตามกฎหมายภายในหรือข้อตกลงระหว่างประเทศซึ่งครอบคลุมอาชญากรรมทุกประเภท และให้เนื้อหาของอนุสัญญากรุงบูดาเปสต์มีผลปรับใช้โดยตรง (direct applicability) หลังจากที่ได้ให้สัตยาบันอนุสัญญาแล้ว ในขณะเดียวกัน อนุสัญญาว่าด้วยการส่งตัวผู้ร้ายข้ามแดนของสภายุโรปและกฎหมายภายในของรัฐ ยังได้กำหนดมาตรการจับกุมชั่วคราว (provisional arrest) ไว้สำหรับจับกุมบุคคลตามคำขอในกรณีเร่งด่วนเพื่อป้องกันการหลบหนีด้วย[1]

4.1.1 เงื่อนไขการส่งตัวผู้ร้ายข้ามแดน

4.1.1.1 การกล่าวอ้างเขตอำนาจรัฐ

สำหรับการกล่าวอ้างเขตอำนาจของรัฐเหนือคดีอาชญากรรมทางคอมพิวเตอร์นั้น รัฐภาคีจะกล่าวอ้างเขตอำนาจตามหลักกฎหมายอาญาทั่วไป อาทิ หลักดินแดนและหลักกึ่งดินแดน สำหรับหลักดินแดนนั้น รัฐภาคีบางรัฐจะขยายความเพิ่มเติมว่า สถานการณ์ใดที่นับเป็นกรณีที่ความผิดเกิดขึ้นในดินแดนของตน ทั้งนี้ รัฐบางแห่งจะพิจารณาจากสถานที่ที่ความผิดนั้นเกิดขึ้น ในขณะที่รัฐบางรัฐจะพิจารณาจากสถานที่ที่การกระทำผิดดำเนินไปหรือผลแห่งการกระทำความผิดเกิดขึ้น[2]

นอกจากนี้ กฎหมายของประเทศอังกฤษนั้น จะพิจารณาจากตำแหน่งที่ตั้งของคอมพิวเตอร์ที่ใช้ในการกระทำความผิดด้วย[3] ส่วนกฎหมายของประเทศมอนเตเนโกร[4]

---

[1] European Convention on Extradition, Art.16; Bulgarian Law on Extradition and European Arrest Warrant, Art.25 (1); Macedonian Criminal Code Art. 513

[2] Armeninan Criminal Code, Art.14 (1); Czech Criminal Code No 140/1961, Section 17 (2)b; German Criminal Code (Strafgesetzbuch), 2009, Section 9; Portugal Penal Code, Art.7; Romanian Criminal Code , Art. 143 (2)

[3] UK Computer Misdemeanors Act 1990, Art. 5

ได้กำหนดหลักเกณฑ์การกำหนดเขตอำนาจเหนืออาชญากรรมที่กระทำโดยการมใช้สื่อไว้ว่า สถานที่ที่ความผิดเกิดขึ้นนั้น ก็คือสถานที่ที่จัดทำสื่อที่ผิดกฎหมาย ส่วนในกรณีที่ไม่ทราบถึงสถานที่จัดทำ ให้พิจารณาจากสถานที่ที่สื่อนั้นถูกแจกจ่าย และในกรณีที่ผู้จัดทำสื่อดังกล่าวต้องรับผิดชอบการกระทำดังข้างต้น ให้พิจารณาเขตอำนาจจากสภานที่ที่บุคคลนั้นพำนักอาศัยเป็นการถาวร สำหรับกฎหมายของประเทศโปรตุเกส[5]นั้น ได้กำหนดเขตอำนาจเหนืออาชญากรรมทางคอมพิวเตอร์ไว้เป็นการเฉพาะว่า โปรตุเกสจะมีเขตอำนาจเหนืออาชญากรรมที่มีการกระทำทางกายภาพเกิดขึ้นในดินแดนโปรตุเกส โดยไม่ต้องคำนึงว่าระบบคอมพิวเตอร์ที่เป็นเป้าหมายจะอยู่ที่ใด และในกรณีที่ระบบคอมพิวเตอร์ภายในดินแดนโปรตุเกสตกเป็นเป้าหมาย โดยในกรณีหลังนี้ ไม่ต้องคำนึงว่าการกระทำทางกายภาพนั้นเกิดขึ้นที่ใด

นอกจากนี้ หลักดินแดนยังปรากฏในข้อ 7 วรรคหนึ่งของ อนุสัญญาว่าด้วยการส่งตัวผู้ร้ายข้ามแดนของสภายุโรปซึ่งอนุญาตให้รัฐผู้รับคำร้องขอส่งตัวผู้ร้ายข้ามแดนปฏิเสธการส่งตัวผู้ร้ายข้ามแดนได้ หากความผิดดังกล่าวถูกกระทำขึ้นในดินแดนของตนได้

สำหรับการกล่าวอ้างเขตอำนาจรัฐโดยหลักบุคคลนั้น พบว่ารัฐภาคีจะอาศัยหลักสัญชาติผู้กระทำความผิด (Active Personality Principle)* กล่าวอ้างเขตอำนาจเหนือคดีอาชญากรรมทางคอมพิวเตอร์ที่กระทำโดยคนชาติของตน[6] ส่วนบางรัฐจะกล่าวอ้างเขตอำนาจเหนือความผิดตามหลักสัญชาติผู้เสียหาย (Passive personality principle)** ด้วย ซึ่งรัฐบางรัฐในกลุ่มนี้จะกำหนดให้ครอบคลุมฐานความผิดสำคัญบางประการอาทิ ความผิดฐานการปลอมแปลง

---

[4] Montenegro Criminal Procedural Code , Art.27 (1)-(3)

[5] Portugal Cybercrime Law - Law nr 109/2009 (15th of September), Art. 27 para.1 (c), (d)

* หลักสัญชาติผู้กระทำความผิดนั้น จะเป็นกรณีที่รัฐกล่าวอ้างเขตอำนาจเหนือความผิดที่กระทำโดยคนชาติของตน

[6] Czech Criminal Code No 140/1961, Section 18; Estonian Penal Code, Section 7 (1) para.3; German Criminal Code (Strafgesetzbuch), 2009, Section 7 (2); Romanian Criminal Code, Art. 4; Turkish Penal Code no 5237/2005, Art.11

** ภายใต้หลักสัญชาติผู้เสียหายนั้น รัฐจะกล่าวอ้างเขตอำนาจเหนือการกระทำผิดที่มีต่อคนชาติของตน โดยไม่ต้องคำนึงถึงสัญชาติของผู้กระทำผิด หรือสถานที่ที่ความผิดเกิดขึ้นแต่อย่างใด

หรือความผิดที่เกี่ยวข้องกับสิ่งลามกอนาจาร เป็นต้น[7] ทั้งนี้ ในการอ้างเขตอำนาจตามเกณฑ์บุคคล กฎหมายของตุรกีจะนำอัตราโทษมาพิจารณาประกอบด้วย[8]

อย่างไรก็ตาม ข้อ 7 วรรค 2 ของอนุสัญญาว่าด้วยการส่งตัวผู้ร้ายข้ามแดนของสภายุโรป ได้กำหนดให้รัฐปฏิเสธคำขอส่งตัวผู้ร้ายข้ามแดนจากรัฐที่กล่าวอ้างเขตอำนาจเหนือความผิดที่กระทำนอกดินแดนของตนได้ เฉพาะในกรณีที่กฎหมายของรัฐผู้รับคำขอไม่อนุญาตให้ดำเนินคดีต่อความผิดประการเดียวกันที่กระทำขึ้นนอกดินแดนของตน[9] หรือในกรณีที่กฎหมายของตนไม่สามารถดำเนินคดีต่อฐานความผิดดังกล่าวได้

มีรัฐภาคีที่ตั้งข้อสงวนภายใต้อนุสัญญาข้อ 22 นี้ไว้สองรัฐ คือฝรั่งเศสและสหรัฐอเมริกา โดยฝรั่งเศสจะไม่กล่าวอ้างเขตอำนาจเหนือการกระทำความผิดเกิดขึ้นนอกเขตอำนาจตามหลักดินแดนของรัฐอื่นรัฐใด นอกจากนี้ถ้าหากการกระทำความผิดสามารถลงโทษได้ตามกฎหมายภายในของรัฐที่ความผิดได้เกิดขึ้น ฝรั่งเศสก็ได้กำหนดขั้นตอนในการร้องขอความร่วมมือทางอาญาระหว่างประเทศว่า รัฐผู้ทำการร้องขอนั้นจะต้องให้อัยการของรัฐเป็นผู้ส่งคำขอ อีกทั้งต้องส่งคำร้องเรียนของผู้เสียหายหรือคำร้องเรียนอย่างเป็นทางการจากเจ้าหน้าที่รัฐที่การกระทำความผิดเกิดขึ้นมาล่วงหน้าอีกด้วย[10] ส่วนประเทศอเมริกานั้น ได้กำหนดข้อสงวนว่าตนจะไม่กล่าวอ้างเขตอำนาจในการดำเนินคดี สำหรับความผิดที่คนชาติของตนได้กระทำขึ้น

---

[7] Austrian Penal Code, Section 64(1); German Criminal Code (Strafgesetzbuch), 2009 Section 6, para.6-7

[8] Turkish Penal Code, Art. 11-12

[9] European Convention on Extradition, Art. 7, para.2; Bulgarian Law on Extradition and European Arrest Warrant, Art.8 para. 5; Croatian Law about international legal aid in criminal matters(OG 178/04.), Art.44

[10] Pedro Verdelho. The effectiveness of international co-operation against cybercrime: examples of good practice [online]. Strasbourg: Council of Europe, Directorate general of human rights and legal affairs, Economic crime division, 2008. Available from: http://www.coe.int/t/dghl/standardsetting/t-cy/T-CY%20%282008%29%20DOC%20The%20effectiveness%20of%20international%20co-operation%20against%20cybercrime%20examples%20of%20good%20practice%20E.PDF [2013, May 6], p.12

นอกดินแดนสหรัฐอเมริกา และในกรณีที่ความผิดได้เกิดขึ้นในเรือที่ชักธงของสหรัฐอเมริกา หรืออากาศยานที่จดทะเบียนตามกฎหมายของสหรัฐอเมริกา[11]

ในขณะเดียวกัน มีรัฐภาคีอีกสองรัฐที่ได้ประกาศจำกัดขอบเขตการปรับใช้ของอนุสัญญากรุงบูดาเปสต์ภายในดินแดนของตน ด้วยอำนาจตามข้อ 38 ว่าด้วยการกำหนดเขตแดนในการปรับใช้อนุสัญญา[12] โดยที่ประเทศเดนมาร์กได้ประกาศว่าอนุสัญญาจะไม่มีผลบังคับใช้ในพื้นที่ของกรีนแลนด์และหมู่เกาะ Faeroe ส่วนประเทศเนเธอร์แลนด์ได้ประกาศว่า อนุสัญญาจะมีผลบังคับใช้เฉพาะกับดินแดนของตนในทวีปยุโรปเท่านั้น[13] ดังนั้น คดีอาชญากรรมทางคอมพิวเตอร์ที่ตกอยู่ในขอบเขตข้อสงวนและการประกาศจำกัดขอบเขตการบังคับใช้เหล่านี้ หากไม่มีรัฐอื่นๆกล่าวอ้างเขตอำนาจที่ครอบคลุมกรณีดังกล่าว

การตั้งข้อสงวนและการประกาศจำกัดขอบเขตการปรับใช้อนุสัญญาแสดงให้เห็นว่าในการกำหนดเขตอำนาจรัฐนั้น ในด้านหนึ่งรัฐจะต้องกำหนดเขตอำนาจให้กว้างขวางเพียงพอเพื่อเป็นการปกป้องผลประโยชน์ส่วนได้เสียของรัฐให้ได้ แต่ในขณะเดียวกัน การกำหนดเขตอำนาจรัฐให้ครอบคลุมกว้างขวางเกินไปอาจส่งผลให้รัฐต้องแบกรับภาระในการดำเนินคดีมากเกินจำเป็นได้เช่นกัน

ในกรณีที่มีรัฐมากกว่าหนึ่งรัฐ ได้กล่าวอ้างเขตอำนาจรัฐของตนเหนือคดีอาชญากรรมทางคอมพิวเตอร์ที่เกิดขึ้นนั้น รัฐบางรัฐเช่น โปรตุเกส[14]ได้กำหนดให้ดำเนินการเจรจากันระหว่างรัฐผู้เกี่ยวข้องเพื่อแสวงหารัฐที่เหมาะสมแก่การดำเนินคดีผู้กระทำผิดมากที่สุด ดังเช่นที่ข้อ 22 แห่งอนุสัญญาได้กำหนดไว้ในขณะที่รัฐบางรัฐเช่นจะกำหนดลำดับความสำคัญของรัฐผู้เกี่ยวข้องไว้[15] ยกตัวอย่างเช่น กฎหมายของโครเอเชียกำหนดให้ดำเนินการส่งตัวผู้ร้ายข้ามแดนแก่รัฐที่ความผิดได้กระทำขึ้น หรือแก่รัฐที่ความผิดส่วนใหญ่ได้ถูกกระทำขึ้น สำหรับกรณีที่รัฐหลายรัฐส่งคำขอที่มีฐานความผิดที่แตกต่างกัน ให้รัฐผู้รับคำขอพิจารณาจากปัจจัยเฉพาะคดี

---

[11] *Ibid.*

[12] *Ibid.*

[13] *Ibid.*

[14] Portugal Cybercrime Law - Law nr 109/2009 (15th of September), Art. 27 para.2

[15] French Criminal Procedure Code, Art. 696-5; Macedonian Criminal Code Art. 521; Montenegro Criminal Procedural Code, Art.25 (3); Portugal Cybercrime Law - Law nr 109/2009 (15th of September), Art. 27 para.3-5

อาทิ ความร้ายแรง วันที่ได้รับคำขอความช่วยเหลือ สัญชาติของบุคคลตามคำขอ ลักษณะการลงโทษ และความเป็นไปได้ในการส่งตัวผู้ร้ายข้ามแดนไปยังรัฐอื่นๆในภายหลัง[16]

อนึ่ง ข้อ 17 แห่งอนุสัญญาว่าด้วยการส่งตัวผู้ร้ายข้ามแดนของสภายุโรป ได้กำหนดให้รัฐผู้รับคำขอความช่วยเหลือพิจารณาปัจจัยแวดล้อมต่างๆประกอบด้วย โดยเฉพาะอย่างยิ่งให้มีการพิจารณาปัจจัยด้านความร้ายแรง สถานที่กระทำความผิด วันที่ได้รับคำขอความช่วยเหลือสัญชาติของบุคคลตามคำขอ และความเป็นไปได้ในการส่งตัวผู้ร้ายข้ามแดนไปยังรัฐอื่นๆในภายหลัง[17]

จะเห็นได้ว่า การกำหนดลำดับความสำคัญของรัฐผู้กล่าวอ้างเขตอำนาจนั้น จัดว่ามีประโยชน์ให้การให้ความร่วมมือทางอาญาระหว่างประเทศในกรณีที่มีรัฐผู้เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์หลายรายเป็นไปอย่างรวดเร็ว อย่างไรก็ตาม การเจรจากันระหว่างรัฐผู้กล่าวอ้างเขตอำนาจยังคงความสำคัญในกรณีที่รัฐผู้เกี่ยวข้องมีความพร้อมทางเทคโนโลยีแตกต่างกัน โดยรัฐผู้กล่าวอ้างเขตอำนาจรัฐที่มีลำดับความสำคัญลำดับแรกมีความพร้อมด้านเทคโนโลยีน้อยกว่ารัฐที่มีลำดับความสำคัญลำดับหลัง

นอกจากหลักความผิดสองประเทศแล้ว แนวปฏิบัติของรัฐภาคีบางรัฐได้กำหนดให้พิจารณาอัตราโทษของความผิดตามคำขอประกอบด้วย ยกตัวอย่างเช่น กฎหมายของโครเอเชีย[18]เอสโตเนีย[19]และเยอรมนี[20] กำหนดให้การส่งตัวผู้ร้ายข้ามแดนกระทำได้เฉพาะในกรณีที่ความผิดดังกล่าวมีโทษจำคุกหรือกักขังสูงสุดตั้งแต่หนึ่งปีขึ้นไป ส่วนกฎหมายของฝรั่งเศสกำหนดให้ อัตราโทษสูงสุดขั้นต่ำอยู่ที่ 2 ปีขึ้นไป[21]

---

[16] Croatian Law about international legal aid in criminal matters(OG 178/04.), Art.39 (1)-(2)

[17] European Convention on Extradition, Art.17

[18] Croatian Law about international legal aid in criminal matters(OG 178/04.), Art.34 (2)

[19] Estonian Criminal Procedure Code, Art. 439(1)

[20] German Act on International Legal Assistance in Criminal Matters (Gesetz über die internationale Rechtshilfe in Strafsachen), 2007 (“IRG”), Section 3 (2)

[21] French Criminal Procedure Code, Art. 696-3

4.1.1.2 ฐานความผิดที่สารถส่งตัวผู้ร้ายข้ามแดนได้

นอกจากหลักความผิดสองประเทศแล้ว แนวปฏิบัติของรัฐภาคีบางรัฐได้กำหนดให้พิจารณาอัตราโทษของความผิดตามคำขอประกอบด้วย ยกตัวอย่างเช่น กฎหมายของโครเอเชีย[22] เอสโตเนีย[23]และเยอรมนี[24] กำหนดให้การส่งตัวผู้ร้ายข้ามแดนกระทำได้เฉพาะในกรณีที่ความผิดดังกล่าวมีโทษจำคุกหรือกักขังสูงสุดตั้งแต่หนึ่งปีขึ้นไป ส่วนกฎหมายของฝรั่งเศสกำหนดให้อัตราโทษสูงสุดขั้นต่ำอยู่ที่ 2 ปีขึ้นไป[25]

4.1.1.3 กรณีที่ไม่สามารถส่งตัวผู้ร้ายข้ามแดนได้

ทั้งอนุสัญญาว่าด้วยการส่งตัวผู้ร้ายข้ามแดนของสภายุโรปและวิธีปฏิบัติของรัฐภาคีต่างๆ ได้กำหนดเหตุแห่งการปฏิเสธการส่งตัวผู้ร้ายข้ามแดนที่ครอบคลุมทั้งเหตุบุคคล เหตุแห่งฐานความผิด และเหตุแห่งคดี โดยบุคคลที่ไม่สามารถส่งตัวผู้ร้ายข้ามแดนได้นั้นได้แก่บุคคลที่มีเอกสิทธิ์และความคุ้มกันตามกฎหมายระหว่างประเทศ อาทิ เจ้าหน้าที่ทางการทูต บุคคลผู้ลี้ภัยทางการเมือง[26] เป็นต้น และคนชาติของรัฐผู้รับคำร้องขอ[27]ด้วย อย่างไรก็ตาม รัฐบางรัฐเช่น บัลแกเรียได้กำหนดละเว้นข้อกำหนดเรื่องคนชาติในกรณีที่ข้อตกลงที่บัลแกเรียเป็นภาคี ตกลงไว้เป็นอย่างอื่น[28]

---

[22] Croatian Law about international legal aid in criminal matters(OG 178/04.), Art.34 (2)

[23] Estonian Criminal Procedure Code, Art. 439(1)

[24] German Act on International Legal Assistance in Criminal Matters (Gesetz über die internationale Rechtshilfe in Strafsachen), 2007 (“IRG”), Section 3 (2)

[25] French Criminal Procedure Code, Art. 696-3

[26] Macedonian Criminal Code Art. 518 (2)

[27] Croatian Law about international legal aid in criminal matters(OG 178/04.), Art.32 (1), Art.35 (1)Para.1; French Criminal Procedure Code, Art. 696-4 para.1; Macedonian Criminal Code Art. 510 (1); Turkish Penal Code no 5237/2005 Art.18 (2)

[28] Bulgarian Law on Extradition and European Arrest Warrant, Art.6 (1)

ความผิดที่ไม่สามารถส่งตัวผู้ร้ายข้ามแดนนั้น ได้แก่ ความผิดทางการเมืองและความผิดที่เกี่ยวข้องกับความผิดทางการเมือง[29] ความผิดตามกฎหมายทหาร (military offence) ที่ไม่มีลักษณะเป็นความผิดทางอาญาทั่วไป[30] โดยรัฐบางรัฐจะเห็นว่าความผิดทางการเมืองนั้นไม่รวมไปถึงความผิดที่กำหนดไว้ในสนธิสัญญาระหว่างประเทศที่ตนเข้าเป็นภาคีด้วย[31]

สำหรับเหตุแห่งคดี คำขอส่งตัวผู้ร้ายข้ามแดนจะไม่ได้รับการดำเนินการหากคดีดังกล่าวหมดอายุความ[32]หรือมีถึงที่สุดแล้ว[33] หรือเป็นคดีที่อยู่ในอำนาจของศาลผู้รับคำร้องขอ[34] นอกจากนี้ คำขอส่งตัวผู้ร้ายข้ามแดนจะถูกปฏิเสธหากบุคคลตามคำขอจะถูกส่งตัวไปดำเนินคดีในศาลพิเศษ[35] หรืออาจถูกตัดสินโทษประหารชีวิต[36] ถูกทรมาน หรือถูกปฏิบัติโดยโหดร้ายทารุณ[37]

---

[29] Estonian Criminal Procedure Code, Art. 440(1) (1); French Criminal Procedure Code, Art. 696-4. para. 2; Japanese Law n°84 of 2004, Art. 2 (1);Macedonian Criminal Code Art. 518 (2)

[30] Estonian Criminal Procedure Code, Art. 440(2);French Criminal Procedure Code, Art. 696-4, para.8; Macedonian Criminal Code Art. 518 (2)

[31] Bulgarian Law on Extradition and European Arrest Warrant, Art.7 para. 1

[32] Austrian Penal Code, Section 65(4) para.1;Bulgarian Law on Extradition and European Arrest Warrant, Art.7 para. 6; Croatian Law about international legal aid in criminal matters(OG 178/04.), Art.35(1) para.4 ; Estonian Criminal Procedure Code, Art. 440(1) (3); French Criminal Procedure Code, Art. 696-4, para.5; Macedonian Criminal Code Art. 510 (4)

[33] Austrian Penal Code, Section 65(4) para.2-3; Bulgarian Law on Extradition and European Arrest Warrant, Art.7 para. 7; Croatian Law about international legal aid in criminal matters(OG 178/04.), Art.35 (1) para.5; Estonian Criminal Procedure Code, Art. 440(1) (2); French Criminal Procedure Code, Art. 696-4, para. 4

[34] Bulgarian Law on Extradition and European Arrest Warrant, Art.8 para. 1,3; Croatian Law about international legal aid in criminal matters(OG 178/04.), Art.35(2); Macedonian Criminal Code Art. 510 (5)

[35] Bulgarian Law on Extradition and European Arrest Warrant, Art.7 para. 3; Croatian Law about international legal aid in criminal matters(OG 178/04.), Art.37 (1) para. 3; French Criminal Procedure Code, Art. 696-4, para.7

[36] Bulgarian Law on Extradition and European Arrest Warrant, Art.7 para. 8; Estonian Criminal Procedure Code, Art. 440(3); French Criminal Procedure Code, Art. 696-4, para.6; Macedonian Criminal Code Art. 518 (3); UK Extradition Act 2003, Art.1 (3)

หรือถูกตัดสินโทษด้วยเหตุแห่งเชื้อชาติ เผ่าพันธุ์ เพศ แนวคิดทางการเมือง[38] กรณีที่บุคคลตามคำขอได้รับการลงโทษแล้วตามหลักกฎหมายไม่พิจารณาลงโทษซ้ำสำหรับการกระทำเดียวกัน (Ne Bis in Idem) [39] เป็นต้น

4.1.1.4 เงื่อนไขประการอื่น ๆ

แนวปฏิบัติของรัฐภาคีกำหนดให้การส่งตัวผู้ร้ายข้ามแดนต้องอยู่ภายใต้หลักความเฉพาะเจาะจง (Rule of Specialty)[40] โดยรัฐผู้ส่งคำขอจะไม่สามารถดำเนินคดีนอกเหนือจากคำขอต่อบุคคลที่ถูกส่งตัวได้ อีกทั้งไม่สามารถส่งบุคคลดังกล่าวไปยังรัฐที่สามได้ด้วย นอกจากนี้ ในบางกรณี การส่งตัวผู้ร้ายข้ามแดนจะสามารถเลื่อนกำหนดเวลาดำเนินการหรือจัดการส่งตัวผู้ร้ายข้ามแดนในลักษณะชั่วคราวได้[41]

4.1.2 กระบวนการส่งตัวผู้ร้ายข้ามแดน

ขั้นตอนการพิจารณาส่งตัวผู้ร้ายข้ามแดนจะแบ่งออกเป็นสามขั้นตอนได้แก่ การพิจารณาความถูกต้องตามแบบพิธี การพิจารณาความถูกต้องตามข้อกฎหมาย และการพิจารณาปัจจัยที่ไม่ใช่ข้อกฎหมายในขั้นสุดท้าย โดยมีหน่วยงานผู้รับผิดชอบแตกต่างออกไปตามแต่ละประเทศ

---

[37] Bulgarian Law on Extradition and European Arrest Warrant, Art.7 para. 5; French Criminal Procedure Code, Art. 696-4, para.6; Macedonian Criminal Code Art. 518 (3)

[38] Bulgarian Law on Extradition and European Arrest Warrant, Art.7 para. 4; Estonian Criminal Procedure Code, Art. 436(3); Turkish Penal Code no 5237/2005, Art.18(3)

[39] Austrian Penal Code, Section 65(4) para.4; Croatian Criminal Code, Art.16 (1)

[40] Bulgarian Law on Extradition and European Arrest Warrant, Art.31-32; Croatian Law about international legal aid in criminal matters(OG 178/04.), Art.37 (1) para.1; French Criminal Procedure Code, Art. 696-6; Macedonian Criminal Code Art. 519 (1); Macedonian Criminal Code Art. 524 (1); Turkish Penal Code no 5237/2005, Art.18 (8)

[41] Croatian Law about international legal aid in criminal matters(OG 178/04.), Art.60; French Criminal Procedure Code, Art. 696-7

ในการติดต่อและส่งคำขอส่งตัวผู้ร้ายข้ามแดนนั้น ช่องทางหลักที่ใช้ได้แก่ช่องทางการทูต[42] อย่างไรก็ตาม ในกรณีพิเศษเช่นการร้องขอให้จับกุมชั่วคราวนั้น รัฐภาคีสามารถติดต่อโดยอาศัยช่องทางการติดต่อโดยตรงที่มีหลักฐานเป็นลายลักษณ์อักษรและได้รับการยอมรับจากรัฐผู้รับคำขอเช่น จดหมาย โทรเลข หรือช่องทางการติดต่อขององค์การตำรวจสากลได้[43] นอกจากนี้แนวปฏิบัติของรัฐภาคียังรับรองกระบวนการส่งตัวผู้ร้ายข้ามแดนแบบรวบรัด โดยให้บุคคลตามคำขอให้ความยินยอมในลักษณะที่ไม่อาจเพิกถอนได้ต่อหน้าศาล[44]

4.2 การปรับใช้กลไกการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายโดยทั่วไปภายใต้กรอบอนุสัญญากรุงบูดาเปสต์

จากประสบการณ์ของรัฐภาคี บทที่สามว่าด้วยการให้ความร่วมมือระหว่างประเทศของอนุสัญญากรุงบูดาเปสต์จะไม่ถูกหยิบยกเป็นฐานทางกฎหมายในการส่งคำขอความช่วยเหลือในคดีอาชญากรรมทางคอมพิวเตอร์โดยตรงตามข้อ 27 [45] หากแต่จะอาศัยกฎหมายภายในของรัฐ หรือโดยข้อตกลงว่าด้วยการให้ความช่วยเหลือซึงกันและกันทางกฎหมายที่มีผลบังคับใช้แทน[46]

---

[42] Macedonian Criminal Code Art. 511 (2), 520

[43] European Convention on Extradition, Art.16 (3)

[44] Bulgarian Law on Extradition and European Arrest Warrant, Art.17(2), Art.19 ; Croatian Law about international legal aid in criminal matters(OG 178/04.), Art.52 (1), 54

[45] The cybercrime convention committee (T-CY). Full meeting report of the 4th multilateral consultation among the contracting states to the convention on cybercrime [online]. Strasbourg: Council of Europe, 2009. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TC-Y%282009%2906E.pdf [2013, May 6], Para.14

[46] Committee of experts on the operation of European conventions on co-operation in criminal matters (PC-OC). Summary of the replies to the questionnaire on mutual legal assistance in computer-related cases [Online]. Strasbourg: Council of Europe, European committee on crime problems (CDPC), 2009. Available from: http://www.coe.int/t/dghl/standardsetting/t-cy/PC-OC%20%282009%29%2005%20E.pdf [2013, May 6], p.5

ทั้งนี้ ข้อตกลงการให้ความช่วยเหลือทางกฎหมายผลบังคับใช้ระหว่างรัฐภาคีในภูมิภาคยุโรปมีอยู่สองฉบับ ฉบับแรกคืออนุสัญญาว่าด้วยการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายในคดีอาญาของสภายุโรปในปี 1959 (1959 European Convention on Mutual Legal Assistance in Criminal Matters) จุดเด่นสำคัญของอนุสัญญาฉบับนี้ก็คือกำหนดให้รัฐติดต่อกันผ่านหน่วยงานกลางในการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมาย อย่างไรก็ตาม เนื้อหาอนุสัญญาไม่ได้กำหนดกลไกอื่นใดเพื่อดำเนินการในกรณีเร่งด่วนเอาไว้[47] ส่วนข้อตกลงความช่วยเหลือทางกฎหมายฉบับที่สองนั้นได้แก่ ข้อตกลงด้านการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายของสหภาพยุโรปในปี 2000 ซึ่งรัฐสมาชิกทั้งหมดของสหภาพยุโรปได้เข้าเป็นภาคีของข้อตกลงฉบับนี้นับตั้งแต่ เดือนธันวาคม ปี 2007 ข้อตกลงฉบับนี้ ได้ให้ความสำคัญกับการให้หน่วยงานรัฐฝ่ายตุลาการ ได้แก่ ผู้พิพากษาหรืออัยการ สามารถติดต่อระหว่างกันได้โดยตรง ส่วนหน่วยงานกลางนั้นจะดำเนินการติดต่อกันเฉพาะในคดีเฉพาะเจาะจงบางคดี เช่นการเคลื่อนย้ายผู้ต้องโทษคำพิพากษาเป็นการชั่วคราว[48]

สำหรับการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายระหว่างรัฐภาคีที่อยู่ภายในและภายนอกทวีปยุโรปนั้น ข้อตกลงการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายมักจะเป็นรูปแบบทวิภาคี ซึ่งกำหนดให้คู่ภาคีติดต่อระหว่างหน่วยงานกลางโดยตรง ส่วนสนธิสัญญาพหุภาคีที่ถูกนำมาใช้เป็นฐานทางกฎหมายก็คือข้อ 18 ของอนุสัญญาด้านการต่อต้านองค์กรอาชญากรรมข้ามชาติของสหประชาชาติ (United Nations Convention against Transnational Organized Crime)[49] แต่ก็จะมีข้อจำกัดคือคดีที่มีการร้องขอภายใต้

---

[47] Committee of experts on the operation of European conventions on co-operation in criminal matters (PC-OC). Replies on mutual legal assistance in computer-related cases [Online]. Strasbourg: Council of Europe, European committee on crime problems (CDPC), 2008. Available from: http://www.coe.int/t/dghl/standardsetting/t-cy/PC-OC%20%282009%29%2005%20E.pdf [2013, May 6], p.27

[48] *Ibid*., p. 28

[49] Committee of experts on the operation of European conventions on co-operation in criminal matters (PC-OC). Summary of the replies to the questionnaire on mutual legal assistance in computer-related cases, p.5

อนุสัญญานั้นจะต้องมีความเกี่ยวข้องกับองค์กรอาชญากรรม (organized crime) เท่านั้น นอกจากนี้ 2nd additional protocol to the convention on mutual legal assistance in criminal matters (ETS. No.182) ยังสามารถนำมาใช้สนับสนุนการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายได้เช่นกัน[50]

4.2.1 ขอบเขตการให้ความช่วยเหลือทั่วไป

รัฐภาคีอนุสัญญากรุงบูดาเปสต์จะกำหนดขอบเขตของการให้ความช่วยเหลือไว้ในกฎหมายของตนว่าครอบคลุมการกระทำใดบ้าง ยกตัวอย่างเช่น กฎหมายของบัลแกเรีย[51] กำหนดให้การให้ความช่วยเหลือครอบคลุมการอำนวยความสะดวกในการดำเนินกระบวนการการสืบสวนคดี การรวบรวมหลักฐาน การจัดหาข้อมูล และการให้ความช่วยเหลืออื่นๆ ตามที่กำหนดไว้ในข้อตกลงระหว่างประเทศที่บัลแกเรียหรือผูกพันหรือในกรณีที่มีลักษณะต่างตอบแทน ส่วนกฎหมายภายในของประเทศมอนเตเนโกร[52] จะกำหนดให้การให้ความช่วยเหลือครอบคลุมการดำเนินคดีทางอาญา การบังคับตามคำพิพากษาคดีอาญาของศาลระหว่างประเทศ การส่งเอกสาร หรือหมายต่างๆ หรือการดำเนินการที่เกี่ยวข้องกับการดำเนินคดีทางอาญาจากรัฐผู้ร้องขอความช่วยเหลือ ซึ่งรวมไปถึงการดำเนินมาตรการตามกฎหมายวิธีพิจารณาความทางอาญาบางประการเช่น การรับฟังคำให้การจากจำเลย พยาน หรือผู้เชี่ยวชาญ การสืบคดีในพื้นที่เกิดเหตุ การเข้าค้นสถานที่เกิดเหตุ การค้นตัวบุคคล และการยึดสิ่งของเป็นการชั่วคราว

---

[50] The cybercrime convention committee (T-CY). Meeting report of the 3rd consultation of the parties to the convention on cybercrime [Online]. Strasbourg: Council of Europe, 2008. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/T-CY%20%282008%29%2004%20E.pdf [2013, May 6], Para.25

[51] Bulgarian Penal Procedure Code, Art. 471(2)

[52] Montenegro Law on International Legal Assistance in Criminal Matters, Art.4

ในขณะเดียวกัน รัฐภาคีบางส่วน[53]จะกำหนดขอบเขตการให้ความช่วยเหลือไว้อย่างยืดหยุ่นมากกว่า โดยจะกำหนดให้ การให้ความช่วยเหลือทางกฎหมายครอบคลุมการให้ความช่วยเหลือทุกประเภทสำหรับกระบวนการดำเนินคดีทางอาญาของต่างประเทศตามที่รัฐผู้ร้องขอดำเนินการขอมา หากแต่ต้องเป็นไปตามเงื่อนไขทางกฎหมายที่ศาลหรือหน่วยงานทางกฎหมายสามารถให้ความช่วยเหลือ หรือไม่ขัดต่อหลักกฎหมายภายในหรือมีข้อตกลงระหว่างประเทศกำหนดเป็นอย่างอื่น สำหรับประเทศโปรตุเกส[54]และโรมาเนีย[55]นั้นได้กำหนดการขอบเขตการให้ความช่วยเหลือทางกฎหมายสำหรับอาชญากรรมทางคอมพิวเตอร์ไว้โดยตรงด้วย

4.2.2 เงื่อนไขการให้ความช่วยเหลือ

รัฐบางส่วนได้มีข้อกำหนดเรื่อง Dual Criminality ไว้ในกฎหมายภายในของตน[56] โดยบางรัฐจะกำหนดข้อยกเว้นในกรณีที่ข้อตกลงระหว่างประเทศที่ตนเองเข้าผูกพันกำหนดไว้เป็นประการอื่น[57] นอกจากนี้ บทบัญญัติตามกฎหมายภายในของรัฐภาคียังกำหนดให้ฝ่ายผู้รับความช่วยเหลือรักษาความลับ และจำกัดการใช้ข้อมูลที่ได้จากการช่วยเหลือด้วย[58]

---

[53] Croatian Law about international legal aid in criminal matters (OG 178/04.), Art. 10(1); French Criminal Procedure Code , Art. 694-3 ,German Act on International Legal Assistance in Criminal Matters 2007 (“IRG”), Art.59 (2)-(3)

[54] Portugal Law nr 109/2009, Art. 20

[55] Romania Law no 161/2003, Art.61

[56] Croatian Law about international legal aid in criminal matters (OG178/04.), Art. 1(3); Japanese Law n°89 of 2004, Art.2 (2); Montenegro Law on International Legal Assistance in Criminal Matters, Art.6 ; Slovakia Code of Criminal Procedure Act no 301/2005, Section 537 (3)

[57] Japanese Law n°89 of 2004, Art.2(2)

[58] Bulgarian Law on Protection of the Classified Information, Art. 115 (1)Croatian Law about international legal aid in criminal matters (OG 178/04.), Art. 21 (1)-(2);Estonian Criminal Procedure Code, Art, 433(4); Lithuanian Criminal Procedure Code, Art.177; Romanian Law no. 302/2004 on international judicial co-operation in criminal matters as amended and supplemented by Law No. 224/2006, Art.12 ;Serbian Criminal Procedure Code, Art. 147. para.4-5; Slovakia Code of Criminal

สำหรับเหตุแห่งการปฏิเสธการให้ความช่วยเหลือนั้น รัฐภาคีอนุสัญญากรุงบูดาเปสต์จะปฏิเสธดำเนินการตามคำขอที่เกี่ยวข้องกับความผิดทางการเมือง[59] หรือมีลักษณะคุกคามต่ออำนาจอธิปไตย ความมั่นคงของรัฐ ความสงบเรียบร้อยของสังคม หรือผลประโยชน์อื่นๆของรัฐที่ได้รับการปกป้องโดยกฎหมาย[60] นอกจากนี้เหตุแห่งการปฏิเสธคำขอยังรวมไปถึงกรณีที่คำขอดังกล่าวขัดต่อหลักกฎหมายของรัฐผู้รับคำขอ[61] หรือมีลักษณะที่เป็นไปเพื่อดำเนินคดีต่อบุคคลโดยอาศัยเหตุแห่งเชื้อชาติ เผ่าพันธุ์ ความเชื่อทางการเมืองหรือทางศาสนา[62] หรือกรณีที่เป็นคดีความผิดเล็กน้อย[63]

นอกจากนี้ การปฏิเสธคำขอความช่วยเหลือซึ่งกันและกันทางกฎหมายยังกระทำได้ในกรณีที่ บุคคลผู้ดำเนินคดีตามคำขอ ได้พ้นโทษจากความผิดในคดีดังกล่าวในรัฐของผู้รับคำขอแล้ว[64] หรืออยู่ระหว่างการพิจารณาคดีของรัฐผู้รับคำขอ[65] ในกรณีที่มีการปฏิเสธ ให้รัฐผู้รับคำขอชี้แจงเหตุผลประกอบการปฏิเสธด้วย[66]

ในขณะเดียวกัน รัฐผู้รับคำขอสามารถเลือกดำเนินการตามคำขอเพียงบางส่วน[67] หรือ เลื่อนการให้ความช่วยเหลือได้ในกรณีที่การให้ความช่วยเหลือจะส่งผลกระทบต่อการสืบสวน

Procedure Act no 301/2005, Section 482 (2); UK Crime (International Co-operation) Act 2003, Art.9 (2)

[59] Japanese Law n°89 of 2004, Art.2(1)

[60] Bulgarian Penal Procedure Code, Art..472; Estonian Criminal Procedure Code, Art. 436 (1) para.1; Slovakia Code of Criminal Procedure Act no 301/2005, Section 537 (2)

[61] Estonian Criminal Procedure Code, Art. 436 (1) para.2

[62] Croatian Law about international legal aid in criminal matters (OG 178/04.), Art. 12(4); Estonian Criminal Procedure Code, Art. 436 (1) para.3

[63] Croatian Law about international legal aid in criminal matters (OG 178/04.), Art. 12 (1) para.5

[64] *Ibid*., Art. 13 (1) para.1

[65] *Ibid*., Art. 13 (1) para.2

[66] *Ibid*., Art. 14

[67] *Ibid*., Art. 16

หรือดำเนินคดีของตน[68] ส่วนในกรณีที่รัฐผู้รับคำขอไม่สามารถดำเนินตามคำขอได้ตามเงื่อนไขหรือตามกรอบเวลาที่กำหนด ให้แจ้งไปยังผู้ส่งคำขอเพื่อเจรจาเปลี่ยนแปลงเงื่อนไขเงื่อนเวลาได้[69]

4.2.3 กระบวนการให้ความช่วยเหลือ

หน่วยงานผู้รับผิดชอบในการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายในคดีอาชญากรรมทางคอมพิวเตอร์ สามารถแบ่งออกเป็นหน่วยงานที่ทำหน้าที่ติดต่อรับส่งคำร้องขอความช่วยเหลือ และหน่วยงานผู้บังคับใช้กฎหมาย ซึ่งจะดำเนินการตามคำขอที่ได้รับมา

จากวิธีปฏิบัติของรัฐต่างๆ หน่วยงานกลางที่รับผิดชอบจะมีอยู่หลายประเภท ทั้งนี้ รัฐภาคีบางรัฐจะแยกหน่วยงานไปตามขั้นตอนการดำเนินคดี และตามลักษณะของคดีที่เกี่ยวข้อง ยกตัวอย่างเช่น ในประเทศโรมาเนีย หากคำขอความช่วยเหลือซึ่งกันและกันทางกฎหมายที่ส่งมาเกี่ยวข้องกับการสอบสวนก่อนหน้าที่จะเริ่มการไต่สวนในชั้นศาล สำนักอัยการจะเป็นหน่วยงานกลางในการส่งและตอบรับคำขอความช่วยเหลือซึ่งกันและกันทางกฎหมาย ในขณะที่กระทรวงการยุติธรรม จะเป็นหน่วยงานกลางสำหรับคำขอความช่วยเหลือที่เกี่ยวกับการไต่สวนคดีและจัดการตามคำพิพากษาลงโทษ ส่วนในกรณีของประเทศฝรั่งเศส ถ้าไม่มีข้อตกลงระหว่างประเทศที่นำมาปรับใช้ได้ กระทรวงการต่างประเทศจะเป็นหน่วยงานกลางในการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายและการส่งตัวผู้ร้ายข้ามแดน หากแต่อัยการจะเป็นจุดติดต่อสำหรับคำขอเกี่ยวข้องกับการจับกุมชั่วคราว (Provisional Arrest) [70]

นอกจากนี้ สำหรับประเทศฝรั่งเศส หากคดีที่เกี่ยวข้องเป็นการเผยแพร่สิ่งลามกอนาจารเด็กทางอินเตอร์เน็ต หน่วยงานที่ดำเนินการสืบสวนคดีภายในประเทศจะเป็น the Office Central Pour la Repression des Violences aux Personnes ซึ่งเป็นหน่วยงานทางตำรวจหน่วยงานหนึ่ง ส่วนในคดีอาชญากรรมทางคอมพิวเตอร์ประเภทอื่นๆ การดำเนินการภายในประเทศจะอยู่ภายใต้

---

[68] *Ibid*., Art.15

[69] *Ibid*., Art. 10 (2)-(4)

[70] Pedro Verdelho. The effectiveness of international co-operation against cybercrime: examples of good practice, pp.21-24

ความรับผิดชอบของ The Office Central de Lutte contre La Criminalite Liee aux technologies de l'information et de la communication (OCLTIC) ซึ่งเป็นหน่วยงานหนึ่งของตำรวจเช่นเดียวกัน[71]

สำหรับหน่วยงานกลางของประเทศอื่นๆ นั้น ประเทศบอสเนียและเฮอร์เซโกวินาและประเทศมอลตา มีหน่วยงานกลางเป็นสำนักงานอัยการสูงสุด ประเทศตุรกีมีหน่วยงานกลางเป็น General Directorate of International Law and Foreign Relations ประจำกระทรวงยุติธรรม ส่วนหน่วยงานกลางของประเทศยูเครนคือ General Prosecutor's office for Requests of Pretrial Bodies, Ministry of Justice for Request of Courts[72].

โดยทั่วไปแล้ว การติดต่อรัฐอีกฝ่ายในการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายจะกระทำโดยการส่งหนังสือส่งประเด็นสืบพยาน (letter rogatory) ผ่านช่องทางการทูต[73] ส่วนช่องทางการสื่อสารอื่นๆให้เป็นไปตามพันธะกรณีในข้อตกลงระหว่างประเทศ นอกจากนี้กฎหมายภายในของรัฐภาคีบางรัฐได้รับรองคำขอที่รับส่งผ่านโทรสารหรือจดหมายอิเล็กทรอนิกส์ด้วย โดยมีเงื่อนไขว่าฝ่ายรัฐผู้รับคำขอสามารถขอให้มีการรับรองความถูกต้องของคำขอดังกล่าวหรือร้องขอเอกสารฉบับจริงในภายหลัง[74] รัฐภาคีบางรัฐยังอนุญาตให้ใช้ช่องทางการติดต่อ

---

[71] *Ibid.*

[72] Committee of experts on the operation of European conventions on co-operation in criminal matters (PC-OC). Summary of the replies to the questionnaire on mutual legal assistance in computer-related cases, p.3, fn.2

[73] Bulgarian Penal Procedure Code, Art. 475 (1), (2); ; French Criminal Code, Art.694; Montenegro Law on International Legal Assistance in Criminal Matters, Art.4; Macedonian Criminal Code, Art.503

[74] Bulgarian Penal Procedure Code, Art. 476 (2); Croatian Law about international legal aid in criminal matters (OG 178/04.), Art. 8(2)

ทางหน่วยงานตำรวจสากล [75] หรือการติดต่อกันโดยตรงระหว่างหน่วยงานผู้บังคับใช้กฎหมาย[76] ในกรณีเร่งด่วนด้วยเช่นกัน

รัฐหลายรัฐจะกำหนดให้ฝ่ายรัฐผู้ร้องขอแปลคำขอความช่วยเหลือเป็นภาษาราชการของตนหรือภาษาอังกฤษเสียก่อน อาทิ ประเทศสวีเดนได้กำหนดให้คำขอความช่วยเหลือและเอกสารที่แนบมาต้องผ่านการแปลเป็นภาษา สวีดิช เดนิช หรือภาษานอร์วิเจียน ฝ่ายเจ้าหน้าที่รัฐของสวีเดนมีสิทธิยกเว้นข้อกำหนดดังกล่าวได้ ส่วนประเทศญี่ปุ่น กำหนดให้รัฐผู้ร้องขอความช่วยเหลือนั้นส่งภาษาญี่ปุ่นแนบมากับคำขอความช่วยเหลือด้วย แต่ก็จะรับพิจารณาคำขอภาษาอังกฤษในกรณีเร่งด่วน[77]

ประเทศภาคีของอนุสัญญากรุงบูดาเปสต์ที่เป็นสมาชิกของสหภาพยุโรปจะให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายรูปแบบการให้ข้อมูลอย่างรวดเร็วผ่านทางองค์การตำรวจสหภาพยุโรป (Europol) ทั้งนี้ Europol เป็นองค์การตำรวจภายใต้สหภาพยุโรปที่มีบทบาทในการเพิ่มประสิทธิภาพในการให้ความร่วมมือกันระหว่างหน่วยงานผู้บังคับใช้กฎหมายของรัฐสมาชิก กิจกรรมที่สำคัญของ Europol ได้แก่ การวิเคราะห์ข้อมูลทางอาชญากรรมและแลกเปลี่ยนข้อมูลกันระหว่างรัฐสมาชิก[78]

---

[75] Croatian Law about international legal aid in criminal matters (OG 178/04.), Art. 6(6)-(7);Montenegro Law on International Legal Assistance in Criminal Matters, Art.4; UK Crime (International Cooperation) Act 2003, Art. 8 (3)

[76] Croatian Law about international legal aid in criminal matters (OG 178/04.), Art. 6(4)

[77] Committee of experts on the operation of European conventions on co-operation in criminal matters (PC-OC). Summary of the replies to the questionnaire on mutual legal assistance in computer-related cases, p.3

[78] Pedro Verdelho. The effectiveness of international co-operation against cybercrime: examples of good practice, p. 19

4.2.4 **การให้ข้อมูลโดยทันที** (Spontaneous Information)

รัฐภาคีบางส่วนมีกฎหมายภายในที่รับรองการให้ความช่วยเหลือด้วยการให้ข้อมูลแก่รัฐอื่นไว้โดยตรง[79] ในขณะที่รัฐภาคีอื่นๆจะใช้วิธีการปรับใช้บทบัญญัติทั่วไป[80]แทน ทั้งนี้ กฎหมายของประเทศเยอรมนี จะกำหนดเงื่อนไขเกี่ยวกับอัตราโทษของความผิดที่เกี่ยวข้อง นอกจากนี้ ผู้รับข้อมูลจะต้องปฏิบัติตามหลักเฉพาะเจาะจงและจะต้องทำลายข้อมูลดังกล่าวทิ้งภายในระยะเวลาที่กำหนดด้วย[81]

รัฐภาคีของอนุสัญญาให้ความเห็นว่า การให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายด้วยการให้ข้อมูลอย่างรวดเร็ว เป็นประโยชน์ในการให้ความร่วมมือทางระหว่างประเทศและสามารถนำไปสู่การจับกุมผู้กระทำความผิดในหลายๆคดีได้[82]

4.3 **การปรับใช้กลไกการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายด้วยวิธีเฉพาะภายใต้กรอบอนุสัญญากรุงบูดาเปสต์**

ผู้มีบทบาทสำคัญในการให้ความช่วยเหลือซึ่งกันและทางกฎหมายด้วยวิธีการเฉพาะนั้นจะประกอบไปด้วยหน่วยงานผู้บังคับใช้กฎหมายและผู้ให้บริการทางอินเตอร์เน็ต ซึ่งต้องให้ความร่วมมือระหว่างกันด้วย โดยรัฐบางรัฐจะมีอำนาจตามกฎหมายในการสั่งการ

---

[79] Bulgarian Ministry of Interior Act, Art. 57 (2) in connection with Art. 55 (6) of the Regulation for the implementation of the Ministry of Interior Act; Bulgarian Penal Procedure Code, Art.471(2); Croatian Law about international legal aid in criminal matters (OG 178/04.), Art.18; Croatian Law about international legal aid in criminal matters (OG 178/04.), Art. 18 (1)-(3) Estonian Criminal Procedure Code, Section 473; German Act on International Legal Assistance in Criminal Matters 2007, Section 61a, 92; Romanian Law no. 302/2004 on international judicial co-operation in criminal matters as amended and supplemented by Law No. 224/2006, Art.166

[80] French Criminal Procedure Code, Art.695-10; Montenegro Law on International Legal Assistance in Criminal Matters, Art.3 ; Slovak Code of Criminal Procedure Act no 301/2005, Art. 484 (2)

[81] German Act on International Legal Assistance in Criminal Matters 2007, Section 61a, 92

[82] Pedro Verdelho. The effectiveness of international co-operation against cybercrime: examples of good practice, p.26-28

ผู้ให้บริการทางอินเตอร์เน็ต ในขณะที่รัฐบางส่วนจะใช้วิธีการทำสัญญาหรือบันทึกความเข้าใจ (Memorandum of Understanding) ระหว่างกันแทน นอกจากนี้ผู้ให้บริการทางอินเตอร์เน็ตออกกฎเกณฑ์ควบคุมตัวเอง (self regulation) เนื่องจากความสัมพันธ์ระหว่างทั้งสองฝ่ายนี้มีหลายลักษณะด้วยกัน จึงเกิดประเด็นปัญหาว่า ขอบเขตความรับผิดชอบของผู้ให้บริการทางอินเตอร์เน็ตนั้นควรมีเพียงใด และในกรณีที่ผู้ให้บริการทางอินเตอร์เน็ตไม่สามารถให้ความร่วมมือได้นั้น ผลลัพธ์ที่ตามมาควรเป็นอย่างไรบ้าง

รัฐภาคีจะมีหน่วยงานเฉพาะทางด้านอาชญากรรมทางคอมพิวเตอร์ (specialized cybercrime unit) โดยหน่วยงานพิเศษนี้จะดำเนินการสืบสวน และ/หรือดำเนินคดีต่อผู้กระทำผิดต่อข้อมูลและระบบคอมพิวเตอร์ หรือผู้กระทำผิดฐานอื่นๆโดยใช้ข้อมูลและระบบคอมพิวเตอร์เป็นเครื่องมือ อีกทั้งยังดำเนินกระบวนการนิติเวชทางคอมพิวเตอร์เพื่อแสวงหาหลักฐานทางอิเล็กทรอนิกส์ด้วย[83]

หน่วยงานเฉพาะทางด้านอาชญากรรมทางคอมพิวเตอร์มีอยู่หลายรูปแบบ รูปแบบแรกคือ หน่วยอาชญากรรมทางคอมพิวเตอร์ (cybercrime unit) หน่วยงานทางคอมพิวเตอร์นี้จะมีหน้าที่รับผิดชอบในการสืบสวนอาชญากรรมทางคอมพิวเตอร์ทุกประเภท และอาชญากรรมที่ก่อขึ้นโดยใช้ข้อมูลและระบบคอมพิวเตอร์เป็นเครื่องมือ ทั้งนี้ หน่วยอาชญากรรมทางคอมพิวเตอร์ยังดำเนินหน้าที่นิติเวชทางคอมพิวเตอร์ด้วยตัวเองด้วย[84] ทั้งนี้ประเทศที่มีหน่วยงานประเภทนี้ในหน่วยงานตำรวจของตนได้แก่ ไซปรัส สาธารณรัฐเชค ฝรั่งเศส มอริเชียส โรมาเนีย และสเปน อย่างไรก็ตามในบางประเทศ เช่น โครเอเชีย และมอนเตเนโกร

---

[83] Cybercrime@IPA project of the Council of Europe and the European Union, Global project on cybercrime of the Council of Europe, and European Union cybercrime task force. Specialised cybercrime units: Good practice study [Online]. Strasbourg: Council of Europe, Directorate general of human rights and rule of law, Data protection and cybercrime division, 2011. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/Octopus2011/2467_HTCU_study_V30_9Nov11.pdf [2013, May 6] , p.4

[84] *Ibid*., p.5

จะมอบหมายหน้าที่ให้อยู่ในความรับผิดชอบกลุ่มเจ้าหน้าที่ผู้เชี่ยวชาญโดยไม่ต้องแยกออกเป็นหน่วยพิเศษแต่อย่างใด[85]

รูปแบบต่อมาของหน่วยงานเฉพาะทางด้านอาชญากรรมทางคอมพิวเตอร์คือหน่วยอาชญากรรมทางเทคโนโลยีขั้นสูง (High Tech Crime Units) ซึ่งจะมีอำนาจการดำเนินงานที่เน้นไปที่การสืบสวนอาชญากรรมต่อระบบและข้อมูลทางคอมพิวเตอร์ และจะมีหน้าที่ด้านนิติเวชทางคอมพิวเตอร์ด้วย หน่วยงานประเภทนี้จะไม่มีอำนาจรับผิดชอบอาชญากรรมอื่นๆที่ใช้เครื่องมือหรือระบบคอมพิวเตอร์เป็นเครื่องมืออย่างเช่น การฉ้อโกงทางอินเตอร์เน็ต อย่างไรก็ตามในคดีดังกล่าวหน่วยอาชญากรรมทางเทคโนโลยีขั้นสูงยังคงให้ความช่วยเหลือทางเทคนิคให้แก่หน่วยงานอื่นๆได้ ตัวอย่างประเทศที่มีหน่วยอาชญากรรมทางเทคโนโลยีขั้นสูงได้แก่ ออสเตรีย เบลเยียม ไอร์แลนด์ และลักเซมเบิร์ก อย่างไรก็ดี แนวปฏิบัติดังกล่าวนี้ อาจมีปัญหาด้านประสิทธิภาพได้เพราะอาชญากรรมทางคอมพิวเตอร์ที่กระทำต่อระบบและข้อมูลทางคอมพิวเตอร์และอาชญากรรมที่ทำด้วยวิธีการทางคอมพิวเตอร์มักมีความเกี่ยวพันกันเสมอ ยกตัวอย่างเช่น ผู้กระทำผิดอาจใช้วิธีการเข้าถึงโดยผิดกฎหมาย หรือการดักรับโดยผิดกฎหมายเพื่อทำการฉ้อโกงทางอินเตอร์เน็ตได้[86] ส่วนหน่วยงานด้านนิติเวชคอมพิวเตอร์ (Computer forensic units) นั้นจะทำหน้าที่รวบรวมและวิเคราะห์หลักฐานทางอิเล็กทรอนิกส์เป็นการเฉพาะ[87]

หน่วยงานเฉพาะทางด้านอาชญากรรมทางคอมพิวเตอร์อีกรูปแบบหนึ่งคือหน่วยงานกลาง (central units) ซึ่งจะไม่มีอำนาจหน้าที่ในการสืบสวน หากแต่จะมีความรับผิดชอบในการประสานงาน และทำหน้าที่ด้านยุทธศาสตร์และข่าวกรอง[88]

นอกจากนี้ รัฐบางรัฐจะตั้งหน่วยงานที่มีหน้าที่รับผิดชอบในอาชญากรรมเฉพาะประเภท (Crime Specific Units) ซึ่งมักจะเป็นคดีสิ่งลามกอนาจารเด็ก หรือคดีการละเมิดหรือใช้ประโยชน์โดยมิชอบทางเพศต่อเด็กประการอื่นๆ นอกจากนี้ยังมีบางหน่วยงานที่รับผิดชอบคดี

---

[85] *Ibid*., p.13

[86] *Ibid*., p.13-14

[87] *Ibid.* p.14

[88] *Ibid.*

ละเมิดทรัพย์สินทางปัญญาหรือการฉ้อโกงบางประเภท ตัวอย่างของหน่วยงานประเภทนี้ได้แก่ หน่วยปกป้องการล่วงละเมิดเด็กทางอินเตอร์เน็ต (Child Exploitation Online Protection หรือ CEOP) ของอังกฤษซึ่งมีหน้าที่รับผิดชอบหลักด้านการล่วงละเมิดทางอินเตอร์เน็ตต่อเด็ก โดยหน่วยงาน CEOP นี้จะมีหน้าที่ครอบคลุมทั้งการสืบสวนคดี การป้องกันอาชญากรรม และการให้ความร่วมมือระหว่างประเทศ[89]

ในขณะที่รัฐส่วนใหญ่จะมีหน่วยงานเฉพาะทางอาชญากรรมทางคอมพิวเตอร์ที่มีลักษณะเป็นหน่วยงานตำรวจ แต่ประเทศบางประเทศเช่นโรมาเนียและเซอร์เบียจะมีหน่วยงานอัยการเฉพาะด้านอาชญากรรมคอมพิวเตอร์ด้วย นอกจากนี้ประเทศบางประเทศจะจัดตั้งหน่วยงานร่วมระหว่างเจ้าหน้าที่ตำรวจและอัยการ เพื่อให้เจ้าหน้าที่ทั้งสองฝ่ายสามารถปฏิบัติงานได้จากภายใต้โครงสร้างเดียวกัน ตัวอย่างจะเห็นได้จากประเทศนอร์เวย์ ซึ่งจัดตั้งฝ่ายงานสืบสวนอาชญากรรมทางคอมพิวเตอร์ไว้ภายในกรมอาชญากรรมที่ใช้เทคโนโลยีชั้นสูงของหน่วยงานสืบสวนอาชญากรรมแห่งชาตินอร์เวย์[90]

หน่วยงานต่างๆเหล่านี้ จะมีแนวทางการปฏิบัติงานที่ต่างกัน โดยในบางประเทศ เช่น โรมาเนียจะยึดถือหลักบังคับ (compulsoriness) ซึ่งจะดำเนินการตรวจสอบรายงานทุกชนิดที่ได้รับมาโดยไม่พิจารณาลำดับความสำคัญหรือต้นทุนในการสืบสวน ในขณะที่บางประเทศจะยึดถือหลักโอกาส (Opportunity) ซึ่งจะเลือกดำเนินการเฉพาะคดีที่มีความสำคัญมากพอเท่านั้น ยกตัวอย่างเช่น ประเทศอังกฤษจะไม่ให้ความช่วยเหลือในคดีฉ้อโกงทางอินเตอร์เน็ตที่มีความเสียหายคิดเป็นจำนวนเงินต่ำกว่า 5000 ปอนด์ เป็นต้น ความแตกต่างดังกล่าวนี้ส่งผลกระทบต่อการให้ความร่วมมือระหว่างประเทศได้ หากความผิดตามคำขอความช่วยเหลือไม่เป็นไปตามเกณฑ์ของรัฐผู้คำร้องขอ[91]

---

[89] *Ibid.*

[90] *Ibid.*

[91] *Ibid.*

ปัญหาส่วนใหญ่ที่หน่วยงานเฉพาะทางอาชญากรรมทางคอมพิวเตอร์เหล่านี้ประสบร่วมกันได้แก่ การขาดแคลนกำลังคน การขาดแคลนทรัพยากรเพื่อการฝึกอบรม และความล่าช้าในการให้ความร่วมมือกับประเทศที่สาม[92]

การดำเนินการตามบทบัญญัติด้านการให้ความช่วยเหลือโดยวิธีการเฉพาะของรัฐภาคีอนุสัญญากรุงบูดาเปสต์นั้น มีรายละเอียดดังต่อไปนี้

4.3.1 การรักษาข้อมูลที่ถูกเก็บไว้อย่างรวดเร็ว

สำหรับการเก็บรักษาข้อมูลอย่างรวดเร็วนั้น จะเห็นได้ว่ามีรัฐจำนวนหนึ่งที่มีบทบัญญัติสำหรับอำนาจสืบสวนดังกล่าวไว้โดยเฉพาะเจาะจงโดยจะมีกฎหมายภายในที่กำหนดให้มีการเก็บรักษาข้อมูลทางคอมพิวเตอร์อย่างรวดเร็วไว้ด้วยการให้อำนาจเจ้าหน้าที่รัฐผู้มีอำนาจอาทิ อัยการ เป็นต้น ในการสั่งให้ผู้ให้บริการทางคอมพิวเตอร์เป็นผู้ดำเนินการต่างๆ[93] และจะมีความรับผิดทางกฎหมายหากไม่ยอมปฏิบัติตาม

ส่วนรัฐบางกลุ่มจะเลือกปรับใช้อำนาจการสืบสวนโดยทั่วไปอย่างเช่นการค้นและยึดแทนโดยยอมรับว่าข้อมูลคอมพิวเตอร์ต่างๆนั้น มีฐานะเป็นหลักฐานประเภทหนึ่งที่จำเป็นต่อการสืบสวนคดีอาญา และให้อำนาจแก่เจ้าหน้าที่ผู้สืบสวนคดีให้ค้นและยึดข้อมูลคอมพิวเตอร์ได้[94] แนวปฏิบัติของรัฐกลุ่มนี้จะยังคงสอดคล้องกับอนุสัญญาอยู่ ตราบใดที่รัฐเหล่านั้น สามารถ

---

[92] *Ibid*.,p.54

[93] Albanian Criminal Procedure Code, Article 299/a, 299/b ; Bulgarian Penal Procedure Code , Art. 59; Croatian Criminal Procedure Act, Art.257 (2); Finland Coercive Measures Act, Chapter 4, Sections 4b; French Criminal Procedure Code, Art.60-2, para.2 ; Portugal Cybercrime Law nr 109/2009, Art.12-13; Romania Law no 161/2003, Art.54; Slovakia Code of Criminal Procedure Act no 301/2005, Section. 90(1)

[94] Project on cybercrime. Cybercrime legislation-country profile: Armenia [Online]. Strasbourg: Council of Europe, Directorate general of human rights and legal affairs, Economic crime division, 2007. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/countryprofiles/cyber_cp_Armenia_2007_June.pdf [2013, May 8]; Estonian Criminal Procedure Code, Art. 215; German

ดำเนินการรักษาความปลอดภัยให้แก่ข้อมูลอิเล็กทรอนิกส์อย่างรวดเร็ว[95] อย่างไรก็ดี บทบัญญัติที่ให้อำนาจอย่างเฉพาะเจาะจงนั้นย่อมมีประสิทธิภาพมากกว่า เพราะรัฐที่ใช้อำนาจการสืบสวนอื่น เช่นการค้น การยึด และการสั่งให้แสดงหลักฐาน เพื่อเก็บรักษาข้อมูลนั้นจะต้องเป็นไปตามเงื่อนไขและมาตรการปกป้องสิทธิที่เข้มงวดกว่า อาทิ การขอคำสั่งศาล จึงก่อให้เกิดความล่าช้าและมีความเสี่ยงที่จะทำให้ผู้ต้องสงสัยรู้ตัวได้[96] ทั้งนี้ การออกคำสั่งด้วยอำนาจศาลอาจดำเนินการได้ภายใน 24 ชั่วโมงหรืออาจใช้เวลานานถึงหลายสัปดาห์ได้แล้วแต่กรณี[97]

การเก็บรักษาข้อมูลของบรรดารัฐภาคีนั้นครอบคลุมทั้งข้อมูลจราจร ข้อมูลเนื้อหาและข้อมูลผู้ใช้บริการตามที่อนุสัญญากรุงบูดาเปสต์ได้กำหนดไว้ อย่างไรก็ตามรัฐบางรัฐ เช่น อาร์เมเนีย จะจำกัดขอบเขตไว้เฉพาะข้อมูลจราจรเท่านั้น[98] ส่วนประเทศเยอรมนีจะแยกบทบัญญัติสำหรับการค้นและยึดข้อมูลจราจรและข้อมูลประเภทอื่นๆออกจากกัน[99]

อย่างไรก็ตาม ระยะเวลาสำหรับการเก็บรักษาข้อมูลของรัฐแต่ละรัฐมีความแตกต่างกัน ทั้งนี้ รัฐภาคีบางส่วนเห็นว่า ระยะเวลา 60 วัน ตามที่อนุสัญญาระบุไว้นั้นสั้นเกินกว่าที่รัฐผู้ร้องขอความช่วยเหลือจะดำเนินการส่งคำร้องอย่างเป็นทางการได้ ดังจะเห็นได้จากวิธีปฏิบัติของประเทศโรมาเนียซึ่งอนุญาตให้การเก็บรักษาข้อมูลนั้นสามารถทำได้เป็นระยะเวลา 90 วัน

Code of Criminal Procedure, Sections 94, 95 and 98; Montenegro Criminal Procedure Code, Art.75, 85(4)

[95] The cybercrime convention committee (T-CY). Assessment report: Implementation of the preservation provisions of the Budapest convention on cybercrime [Online]. Strasbourg: 2012. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/TCY2013/TCYreports/TCY_2012_10_Assess_report_v30_public.pdf [2013, May 6], p.7

[96] The cybercrime convention committee (T-CY). Abridged meeting report of the seventh plenary [Online]. Strasbourg: Council of Europe, 2012. Available from: http://www.coe.int/t/dghl/standardsetting/tcy/TCY2012/TCY_2012_14E_PlenAbrMeetRep_V7_21june2012.pdf [2013, May 8], Para.4

[97] The cybercrime convention committee (T-CY). Assessment report: Implementation of the preservation provisions of the Budapest convention on cybercrime, p.10

[98] *Ibid*., p.8

[99] *Ibid.*

เช่นเดียวกับอัลบาเนีย[100] หรือฟินแลนด์[101] แต่ทางคำขอความช่วยเหลือซึ่งกันและกันทางกฎหมายอย่างเป็นทางการก็ไม่ถูกส่งมาตามกำหนดเวลา ในขณะเดียวกันทางประเทศฝรั่งเศสได้กล่าวถึงประสบการณ์ของตนว่า ในบางครั้งกระบวนการการทำคำขอความช่วยเหลือซึ่งกันและกันทางกฎหมายอย่างเป็นทางการนั้นอาจใช้เวลาถึงหนึ่งปี ด้วยเหตุดังกล่าว ฝรั่งเศสจึงได้นำ European Union Framework Decision on Data Retention มาปรับใช้กับกฎหมายภายในประเทศโดยกำหนดให้ ผู้ให้บริการทางอินเตอร์เน็ตและผู้ดำเนินการอื่นๆ มีพันธะกรณีในการเก็บรักษาข้อมูลเป็นระยะเวลานานถึงหนึ่งปี สำหรับโรมาเนียก็มีความพยายามที่จะขยายเวลาในการเก็บรักษาข้อมูลเพิ่มเป็นเวลาหนึ่งปีเช่นเดียวกัน

นอกจากนี้รัฐบางรัฐ เช่น สาธารณรัฐเชค[102] มีวิธีปฏิบัติที่ฝ่ายเจ้าหน้าที่รัฐกำหนดให้ผู้ให้บริการทางอินเตอร์เน็ตสร้างแผงควบคุม (interface) ให้ฝ่ายเจ้าหน้าที่รัฐสามารถเข้าควบคุมและดำเนินการภายในระบบของผู้ให้บริการทางอินเตอร์เน็ต ซึ่งจะลดระยะเวลาการเก็บรักษาข้อมูลคอมพิวเตอร์ได้ อย่างไรก็ตาม วิธีดังกล่าวนับได้ว่าสร้างภาระให้แก่ผู้ให้บริการทางอินเตอร์เน็ตในขณะเดียวกันด้วย

ในบริบทของการให้ความร่วมมือทางอาญาระหว่างประเทศ รัฐส่วนใหญ่เพียงนำบทบัญญัติเกี่ยวกับการให้ความช่วยเหลือทางอาญาทั่วไปมาปรับใช้กับการเก็บรักษาข้อมูล โดยอาศัยผลแห่งการให้สัตยาบันอนุสัญญากรุงบูดาเปสต์เท่านั้น[103] ในขณะเดียวกันกฎหมายภายในของรัฐบางรัฐเช่น โปรตุเกส[104] โรมาเนีย[105]จะกำหนดบทบัญญัติ

---

[100] Albanian Criminal Procedure Code, Article 299/a, para.2

[101] Finland Coercive Measures Act, Chapter 4, Section 4c

[102] Czech Code on Electronic Communication No 127/2005, Section 97 (1)

[103] Croatian Law about international legal aid in criminal matters, Art.4,10; Estonian Criminal Procedure Code, Art. 433 ; French Criminal Procedure Code, Article 695-10; German Act on International Legal Assistance in Criminal Matter, Art.66, 67; Macedonian Criminal Code, Art. 505-a(1)

[104] Portugal Cybercrime Law nr 109/2009, Art.22-23

[105] Romania Law no 161/2003, Art.63, 64

เกี่ยวกับการให้ความช่วยเหลือด้วยการเก็บรักษาข้อมูลเป็นการเฉพาะ ด้วยการกำหนดรายละเอียดที่เกี่ยวข้อง อาทิ รายละเอียดของคำขอเก็บรักษาข้อมูล เหตุแห่งการปฏิเสธคำขอ และการระบุความผูกพันที่จะส่งคำขอให้ค้นและยึดข้อมูลตามมาในภายหลัง ซึ่งนับว่าสอดคล้องกับบทบัญญัติข้อ 29, 30 แห่งอนุสัญญากรุงบูดาเปสต์

การรักษาข้อมูลทางคงคอมพิวเตอร์ที่ถูกกักเก็บไว้อย่างรวดเร็วนับเป็นการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายที่ใช้กันมากที่สุด โดยรัฐภาคีเองก็จะใช้มาตรการกักข้อมูล ซึ่งอนุสัญญาไม่ได้ระบุไว้ควบคู่ไปด้วย[106] จะเห็นได้ว่ารัฐภาคีของอนุสัญญากรุงบูดาเปสต์ส่วนใหญ่ ยกเว้น อาร์เมเนีย เยอรมนี นอร์เวย์และสหรัฐอเมริกาที่ใช้วิธีการกักข้อมูล (data retention) เป็นสำคัญ อย่างไรก็ดีการกักข้อมูลจะครอบคลุมเฉพาะข้อมูลจราจรเท่านั้น และต้องเป็นไปเพื่อการสืบสวนอาชญากรรมร้ายแรงเท่านั้น[107] ในขณะเดียวกัน รัฐภาคีบางส่วนยังกำหนดเงื่อนไขในการเข้าถึงข้อมูลที่ถูกกักไว้ ในลักษณะที่ส่งผลให้การเปิดเผยข้อมูลจราจรนั้นเป็นไปได้ยากกว่าการเปิดเผยข้อมูลทางเนื้อหาที่มีผลกระทบต่อสิทธิส่วนบุคคล[108] ทั้งนี้มาตรการกักข้อมูลจะเป็นผลมาจากการที่รัฐมีพันธะกรณีตาม Data Retention Directive ของสหภาพยุโรปเมื่อปี 2006[109]

มาตรการกักข้อมูลภายใต้ Data Retention Directive ของสหภาพยุโรปนั้นนับว่ามีบทบาทในการส่งเสริมการเก็บรักษาข้อมูลได้ เพราะการกักข้อมูลจะช่วยให้ข้อมูลที่เกี่ยวข้องกับการจราจร หรือข้อมูลผู้ใช้งานนั้นยังคงมีอยู่พร้อมในขณะที่มีการออกคำสั่งให้เก็บ

---

[106] Albanian Law no. 9918, Art.101; Croatian Criminal Procedure Act, Art. 263; Czech Code on Electronic Communication No 127/2005, Section 97 (3); Turkish Code Number 5651/2007, Art. 6 (1)(b); 18 U.S.C. § 2703 (f)

[107] The cybercrime convention committee (T-CY). Assessment report: Implementation of the preservation provisions of the Budapest convention on cybercrime, p.9

[108] The cybercrime convention committee (T-CY). Abridged meeting report of the seventh plenary, Para.7

[109] The cybercrime convention committee (T-CY). Assessment report: Implementation of the preservation provisions of the Budapest convention on cybercrime, p.9

รักษาข้อมูลในภายหลัง นอกจากนี้ ถ้าหากการกักข้อมูลนั้นครบกำหนดเวลาตามกฎหมายแล้ว คำสั่งให้เก็บรักษาข้อมูลก็จะทำให้ข้อมูลที่ถูกกักไว้บางส่วนที่ถูกระบุมา ได้รับการปกป้องต่อไปได้ ในขณะเดียวกัน การสืบสวนคดีอาชญากรรมทางคอมพิวเตอร์ยังเป็นการยากที่จะระบุได้โดยเร็วว่าอาชญากรรมนั้นจัดอยู่ในขั้นร้ายแรงหรือไม่ ยกตัวอย่างเช่น การสืบคดีฉ้อโกงทางคอมพิวเตอร์รายย่อยในบางครั้ง อาจจะทำให้รัฐผู้สืบสวนคดีได้มาซึ่ง IP Address ที่เกี่ยวกันกับปฏิบัติการอาชญากรรมทางคอมพิวเตอร์ขนาดใหญ่ได้ เพราะฉะนั้น การใช้มาตรการเก็บรักษาข้อมูลซึ่งครอบคลุมข้อมูลในกรณีที่ไม่ใช่อาชญากรรมร้ายแรง ย่อมสามารถส่งเสริมมาตรการกักข้อมูลได้[110] เพราะฉะนั้น จะเห็นได้ว่ามาตรการกักข้อมูลนั้น มีประโยชน์ในฐานะมาตรการเสริมการเก็บรักษาข้อมูลอย่างรวดเร็วเท่านั้น แต่ไม่ควรนำใช้แทนกันแต่อย่างใด[111]

ระหว่างการเก็บรักษาข้อมูล รัฐส่วนมากสามารถสั่งการให้ผู้เก็บรักษาข้อมูลรักษาความลับของการดำเนินการไว้ได้ อย่างไรก็ตาม ในกรณีของประเทศนอร์เวย์นั้น หน่วยงานผู้บังคับใช้กฎหมายจะต้องแจ้งให้ผู้เก็บรักษาข้อมูลทราบถ้าหากฝ่ายตนกำลังเข้าถึงข้อมูลดังกล่าว เว้นเสียแต่จะได้รับคำสั่งศาลให้เป็นอย่างอื่น[112]

หลักฐานที่อยู่ในรูปแบบข้อมูลทางอิเล็กทรอนิกส์ที่หน่วยงานรัฐต้องการในการสืบสวนคดีอาชญากรรมทางคอมพิวเตอร์นั้น จะอยู่ในควบคุมของผู้ให้บริการทางอินเตอร์เน็ตเสียเป็นส่วนใหญ่ ในการนี้กฎหมายของรัฐภาคีอนุสัญญากรุงบูดาเปสต์ส่วนมากได้ให้อำนาจเจ้าหน้าที่รัฐสั่งการให้ผู้ให้บริการทางอินเตอร์เน็ตเก็บรักษาข้อมูล หรือให้สามารถเข้าถึงข้อมูลเหล่านั้นได้ อย่างไรก็ดี อำนาจดังกล่าวตามกฎหมายของรัฐภาคีบางประเทศจะไม่รวมไปถึง

---

[110] *Ibid*., p.75

[111] The cybercrime convention committee (T-CY). Abridged meeting report of the seventh plenary, para.6

[112] The cybercrime convention committee (T-CY). Assessment report: Implementation of the preservation provisions of the Budapest convention on cybercrime, p.9

การสั่งการนิติบุคคลหรือบุคคลธรรมดาที่เกี่ยวข้องกับการสืบสวนคดี ซึ่งเป็นกรณีที่ข้อ 16 ของอนุสัญญากรุงบูดาเปสต์ครอบคลุมแต่อย่างใด[113]

นอกจากนี้ ผู้ให้บริการทางอินเตอร์เน็ต หรือบุคคลธรรมดาหรือนิติบุคคลที่เกี่ยวข้องกับการสืบสวนในบางประเทศนั้นได้ให้ความยินยอมที่จะเก็บรักษาข้อมูลอย่างรวดเร็วหากได้รับคำสั่งจากเจ้าหน้าที่รัฐ ผ่านทางการจัดทำบันทึกความเข้าใจ หรือข้อตกลงระหว่างภาครัฐและภาคเอกชน เช่นในประเทศลิธัวเนีย ที่ผู้ให้บริการทางอินเตอร์เน็ตรายใหญ่ตกลงที่จะให้หน่วยงานผู้บังคับใช้กฎหมายสามารถเข้าถึงข้อมูลจราจรและข้อมูลผู้ใช้บริการได้ ส่วนในกรณีประเทศนอร์เวย์นั้น ผู้ให้บริการทางอินเตอร์เน็ตรายใหญ่ที่สุดของประเทศได้ตกลงให้ความร่วมมือกับจุดติดต่อตามเครือข่าย 24/7 ในการปฏิบัติตามคำขอความช่วยเหลือโดยต้องเป็นไปตามเงื่อนไขที่กำหนด[114]

ปัญหาอีกประการที่รัฐภาคีพบก็คือหลังจากที่รัฐผู้รับคำขอดำเนินการรักษาข้อมูลทางคอมพิวเตอร์อย่างรวดเร็วแล้ว รัฐผู้ส่งคำขอก็มิได้ส่งคำขออย่างเป็นทางการเพิ่มเติมมาภายหลังแต่เพียงอย่างใด[115]

4.3.2 การเปิดเผยข้อมูลจราจรอย่างรวดเร็ว

สำหรับการให้ความช่วยเหลือด้วยการเปิดเผยข้อมูลจราจรอย่างรวดเร็วตามข้อ 17 ของอนุสัญญากรุงบูดาเปสต์นั้น รัฐบางส่วนจะมีบทบาทไว้รองรับอำนาจสืบสวนดังกล่าวไว้โดยเฉพาะเจาะจงเช่นกัน ในขณะที่รัฐอีกกลุ่มจะยังคงอาศัยมาตรการอื่น ซึ่งมักจะเป็นอำนาจสั่งให้แสดงหลักฐานแทนในการเปิดเผยข้อมูลที่ระบุเส้นทางการสื่อสารโดยอาศัยคำสั่งจากศาล

---

[113] *Ibid.,*

[114] *Ibid.,* p.8

[115] Pedro Verdelho. The effectiveness of international co-operation against cybercrime: examples of good practice, pp.29-31

เป็นสำคัญ การดำเนินการของรัฐกลุ่มที่สองนี้ จะยังนับว่าสอดคล้องต่ออนุสัญญา หากกระบวนการเป็นไปอย่างรวดเร็วและไม่ซับซ้อนจนเกินไป[116]

อย่างไรก็ตาม ในทางปฏิบัติแล้ว มีรัฐไม่กี่แห่งอาทิ มอลโดวา นอร์เวย์ และสหรัฐอเมริกา ที่ใช้การเปิดเผยข้อมูลจราจรอย่างรวดเร็วอย่างสม่ำเสมอ[117] ส่วนรัฐเช่น โรมาเนียและโปรตุเกส จะกำหนดให้การเปิดเผยข้อมูลจราจรบางส่วนถูกรวมอยู่ในขั้นตอนการเก็บรักษาข้อมูลด้วย กล่าวคือผู้ที่ได้รับคำสั่งให้เก็บรักษาข้อมูลจะมีหน้าที่เปิดเผยข้อมูลจราจรด้วยโดยไม่ต้องอาศัยคำสั่งอีกฉบับแต่อย่างใด[118]

นอกจากนี้ ยังมีรัฐบางส่วนที่อาศัยเพียงแต่อำนาจการกักข้อมูลตามพันธะกรณีที่ตนมีต่อ Data Retention Directive ของสหภาพยุโรปในการดำเนินการ จึงก่อให้เกิดอุปสรรคในการสืบสวนคดีเพราะการกักข้อมูลจะใช้ได้เฉพาะในกรณีที่เกี่ยวข้องกับอาชญากรรมร้ายแรงเท่านั้น[119]

สำหรับการให้ความช่วยเหลือตามข้อ 30 ว่าด้วยการเปิดเผยข้อมูลจราจรอย่างรวดเร็วของอนุสัญญานั้น พบว่ามีรัฐภาคีไม่กี่แห่งที่ให้ความช่วยเหลือด้วยวิธีดังกล่าว โดยประเทศที่ใช้งานจริงจะมีเพียงบัลแกเรีย มอลโดวา และนอร์เวย์เท่านั้น โดยในกรณีของประเทศนอร์เวย์ หากฝ่ายเจ้าหน้าที่รัฐรับข้อมูลจราจรที่มีความสำคัญในการสืบสวนคดีของตน เจ้าหน้าที่รัฐสามารถแบ่งปันข้อมูลจราจรนั้นไปยังหน่วยงานรัฐที่ร้องขอความช่วยเหลือได้ สำหรับรัฐส่วนมากนั้น จะยังคงดำเนินการเปิดเผยข้อมูลจราจรผ่านกระบวนการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายทั่วไป ซึ่งยังไม่รวดเร็วเพียงพอ[120]

---

[116] The cybercrime convention committee (T-CY). Assessment report: Implementation of the preservation provisions of the Budapest convention on cybercrime, p.51

[117] *Ibid.*

[118] *Ibid.*

[119] *Ibid.*

[120] *Ibid.*, p.52

4.3.3 การเข้าถึงข้อมูลทางคอมพิวเตอร์ที่ถูกเก็บไว้

สำหรับการค้นและยึดข้อมูลนั้น รัฐภาคีต่างๆได้มี มาตรการด้านการค้นและยึดที่ครอบคลุมไปถึงหลักฐานทางอิเล็กทรอนิกส์ในคดีอาชญากรรมทางคอมพิวเตอร์ ทั้งนี้ กฎหมายบางรัฐจะขยายให้อำนาจการค้นและยึดตามกฎหมายวิธีพิจารณาความอาญาครอบคลุมถึงข้อมูลทางคอมพิวเตอร์ด้วย[121] ส่วนกฎหมายภายในของรัฐภาคีบางรัฐจะกำหนดหลักเกณฑ์การค้นและยึดข้อมูลทางคอมพิวเตอร์โดยเฉพาะ[122] ซึ่งจะครอบคลุมไปยังมาตรการต่างๆ อาทิ การเข้าถึงและค้นหาข้อมูล การทำสำเนาและเก็บรักษาสำเนาข้อมูลทางคอมพิวเตอร์ การทำให้ข้อมูลคอมพิวเตอร์เข้าถึงไม่ได้ การระงับกิจกรรมภายในระบบคอมพิวเตอร์ การยึดระบบคอมพิวเตอร์บางส่วน หรือการยึดสื่อกลางสำหรับเก็บข้อมูลประเภทอื่นๆ เป็นต้น[123] อีกทั้งยังอนุญาตให้ฝ่ายเจ้าหน้าที่รัฐขยายขอบเขตการยึดไปยังระบบคอมพิวเตอร์อื่นได้ หากมีเหตุอันควรเชื่อว่าข้อมูลที่ตนหาอยู่ในระบบคอมพิวเตอร์อื่นซึ่งสามารถเข้าถึงได้โดยชอบด้วยกฎหมายจากระบบคอมพิวเตอร์ที่ตนกำลังดำเนินการค้นอยู่[124] เป็นต้น นอกจากนี้ถึงแม้บทบัญญัติกฎหมายภายในว่าด้วยการค้นและยึดจะสามารถรองรับการให้ความร่วมมือทางอาญาระหว่างประเทศได้ กฎหมายของรัฐภาคีบางส่วนเช่น โปรตุเกส และโรมาเนียได้มีบทบัญญัติเกี่ยวกับการให้ความช่วยเหลือด้านการค้นและยึดข้อมูลทางคอมพิวเตอร์เป็นการเฉพาะด้วย[125]

---

[121] Bosnia and Herzegovina Criminal Procedural Law, Art.51(2); Bulgarian Penal Procedure Code, Art. 159, Art. 160 (1), Art. 165 (5); 18 U.S.C. § 2513

[122] Portugal Cybercrime Law nr 109/2009, Art. 15-17; Turkish Criminal Procedure Code no 5271/2005, Art.134

[123] Albania Criminal Procedural Law, Art. 208/1 para.3; Croatia Criminal Procedure Act, Article 257, 261 and 263; France Criminal Procedure Code, Art.56, Art.97 para.3-4; Portugal Cybercrime Law nr 109/2009, Art.16 para.7; Romania Law no 161/2003, Art. 55

[124] Albania Criminal Procedural Law, Art. 208/1 para.2; Portugal Cybercrime Law nr 109/2009, Art. 15 para.5 ; Romania Law no 161/2003, Art. 56(3)

[125] Portugal Cybercrime Law nr 109/2009, Art. 24; Romania Law no 161/2003, Art.60

4.3.4 การเข้าถึงข้อมูลข้ามแดน

มีรัฐภาคีเพียงบางส่วนเช่น เอสโตเนีย โปรตุเกส โรมาเนีย ที่นำข้อ 32 แห่งอนุสัญญากรุงบูดาเปสต์มาบัญญัติไว้โดยตรงในกฎหมายภายในเกี่ยวกับการให้ความร่วมมือทางอาญาระหว่างประเทศ[126] ในขณะที่รัฐภาคีอื่นจะอาศัยการปรับใช้หลักกฎหมายทั่วไปเกี่ยวกับการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายแทน[127]

สำหรับอนุสัญญาข้อ 32a นั้น จะเห็นได้ว่าการเข้าถึงข้อมูลที่สามารถเข้าถึงได้โดยสาธารณชนโดยไม่ต้องขอความช่วยเหลือของรัฐอื่นนั้น นับได้ว่าเป็นแนวปฏิบัติของรัฐที่ถูกยอมรับเป็นการสากล อีกทั้งยังจัดได้ว่าเป็นกฎหมายจารีตประเพณีระหว่างประเทศซึ่งมีผลบังคับใช้กับรัฐที่ไม่ใช่ภาคีของอนุสัญญากรุงบูดาเปสต์ด้วย[128]

สำหรับอนุสัญญาข้อ 32 b นั้น รัฐภาคีต่างๆ ได้ให้ความเห็นเกี่ยวกับเนื้อหาและการตีความที่แตกต่างกันออกไป บางรัฐเช่น เยอรมนีจะตีความว่า เจ้าหน้าที่รัฐสามารถกระทำการตามข้อ 32 b ได้โดยไม่ต้องส่งคำขอความช่วยเหลือทางกฎหมายหากบุคคลที่มีอำนาจตามกฎหมายในการส่งข้อมูลดังกล่าวต่อเจ้าหน้าที่รัฐของตนนั้น จะต้องให้ความยินยอมโดยสมัครใจและถูกต้องตามกฎหมาย[129] ในขณะที่รัฐภาคีบางรัฐเช่นลัตเวีย จะตีความว่าผู้ให้บริการหรือผู้ดำเนินการระบบคอมพิวเตอร์ต้องมีความยินยอมจากผู้ใช้บริการเสียก่อน

---

[126] Estonia Criminal Procedure Code, Art. 64,65; Portugal Cybercrime Law nr 109/2009 , Article 25; Romania Law no 161/2003, Art.65

[127] Croatia Law about international legal aid in criminal matters, article 4,10; French Criminal Procedure Code, Art. 695-10 ; Slovakia Code of Criminal Procedure Act no 301/2005, Section 537

[128] Ad-hoc sub-group on jurisdiction and transborder access to data. Transborder access and jurisdiction: What are the options? [Online]. Strasbourg: Council of Europe, The cybercrime convention committee (T-CY), 2012. Available from: http://www.coe.int/t/dghl/standardsetting/t-cy/TCY2012/TCY_2012_3_transborder_rep_V30public_7Dec12.pdf [2013, May 6], Para. 293

[129] Committee of experts on the operation of European conventions on co-operation in criminal matters (PC-OC). Summary of the replies to the questionnaire on mutual legal assistance in computer-related cases, p.5

จึงจะจัดหาข้อมูลให้หน่วยงานของรัฐอื่นตามข้อ 32b ได้[130] ส่วนรัฐภาคีเช่น ฟินแลนด์ให้ความเห็นว่า การดำเนินการตามข้อ 32 b จะต้องพิจารณาจากผู้ที่ให้ข้อมูลเป็นสำคัญ กล่าวคือ หากผู้ที่ให้ข้อมูลเป็นผู้ให้บริการทางอินเตอร์เน็ต อาทิ Google รัฐผู้ร้องขอจะต้องใช้ช่องทางการขอความช่วยเหลือซึ่งกันและกันทางกฎหมายตามปกติ แต่ในกรณีที่ผู้ให้ข้อมูลไม่ใช่ผู้ให้บริการทางอินเตอร์เน็ต ฝ่ายเจ้าหน้าที่รัฐสามารถเข้าถึงข้อมูลต่างๆอาทิ email ของบุคคลโดยไม่ต้องพึ่งพาการช่วยเหลือ การเกี่ยวข้อง หรือบทบาทของรัฐที่ข้อมูลตั้งอยู่ได้ หากบุคคลผู้นั้นได้ให้อนุญาตโดยถูกต้องตามกฎหมาย[131]

ในทางกลับกัน รัฐภาคีบางส่วนให้ความเห็นว่า รัฐผู้เข้าถึงข้อมูลตามข้อ 32b จะต้องดำเนินการผ่านเจ้าหน้าที่ของรัฐอื่นด้วย โดยประเทศ สโลวาเกียให้ความเห็นว่า การเข้าถึงข้อมูลข้ามแดนตามข้อ 32b ในทุกกรณีนั้นจะต้องได้รับอนุญาตจากหน่วยงานทางตุลาการของรัฐที่ข้อมูลนั้นตั้งอยู่เสียก่อน[132] ในขณะที่ประเทศยูเครน ให้ความเห็นว่า ในการดำเนินการตามข้อ 32b นั้น เจ้าหน้าที่ของรัฐที่ข้อมูลนั้นตั้งอยู่จะต้องเป็นผู้ส่งข้อมูล และการเข้าถึงข้อมูลข้ามแดนโดยปราศจากความยินยอมของผู้เป็นเจ้าของจะเป็นการละเมิดกฎหมาย[133]

นอกจากนี้ ในการเข้าถึงข้อมูลข้ามแดนภายใต้ ข้อ 32 b นั้นรัฐส่วนใหญ่ไม่เห็นด้วยกับการอนุญาตให้บุคคลหรือนิติบุคคลที่อยู่ในดินแดนของตนยอมทำตามคำขอที่ส่งมาโดยตรงจากหน่วยงานผู้บังคับใช้กฎหมายของรัฐอื่น[134] โดยรัฐบางรัฐจะกำหนดความผิดทางอาญาไว้ด้วย ยกตัวอย่างเช่น กฎหมายของประเทศสหรัฐอเมริกา จะกำหนดโทษทางอาญาถ้าหากผู้ให้บริการอินเตอร์เน็ตทางการค้าของตนเปิดเผยข้อมูลทางเนื้อหาให้แก่ผู้อื่นหรือรัฐบาลต่างชาติ ส่วนกฎหมายของประเทศฝรั่งเศสก็ห้ามคนชาติ คนที่อาศัยอยู่ในดินแดนรัฐ หรือลูกจ้างนิติบุคคลที่มีสถานประกอบการ ไม่ว่าจะเป็นสำนักงานใหญ่หรือสาขาอยู่ในประเทศฝรั่งเศส

---

[130] *Ibid.*

[131] *Ibid.*

[132] *Ibid.*,p.6

[133] *Ibid.*

[134] Ad-hoc sub-group on jurisdiction and transborder access to data. Transborder access and jurisdiction: What are the options?, Para.118

ในการส่งเอกสาร หรือสื่อสารข้อมูลสำคัญไปยังเจ้าหน้าที่ของรัฐอื่นในลักษณะที่อาจสร้างความเสียหายต่ออำนาจอธิปไตย ความมั่นคง หรือผลประโยชน์สำคัญธุรกิจของฝรั่งเศส หรือในลักษณะที่ขัดต่อนโยบายสาธารณะของรัฐ โดยข้อมูลดังกล่าวนั้นครอบคลุมข้อมูลทางเศรษฐกิจ การพาณิชย์ อุตสาหกรรม การเงิน หรือเรื่องทางเทคนิคอื่นๆ[135]

จะเห็นได้ว่า ความแตกต่างดังกล่าวเป็นผลมาจากการที่ รัฐภาคีเห็นว่าอนุสัญญาข้อ 32 b อาจส่งผลกระทบต่อการใช้อำนาจอธิปไตยของตนได้ โดยเฉพาะอย่างยิ่งอำนาจสืบสวนของหน่วยงานผู้บังคับใช้กฎหมายที่มีอยู่เหนือผู้ให้บริการทางอินเตอร์เน็ต ในขณะเดียวกันการเข้าถึงข้อมูลข้ามแดน อาจส่งผลกระทบต่อปฏิบัติการบังคับใช้กฎหมายของรัฐอื่นด้วย ไม่ว่าจะเป็นในระดับภายในหรือระหว่างประเทศ เพราะโดยหลักแล้วการสืบสวนอาชญากรรมทางคอมพิวเตอร์ จะต้องพึ่งพาการรักษาความลับ และความร่วมมือจากฝ่ายบุคคลที่สามอาทิ ผู้ให้บริการทางอินเตอร์เน็ต ด้วย การเข้าถึงข้อมูลข้ามแดนบางประเภท อาจทำให้หน่วยงานของรัฐอื่นไม่สามารถประสานงานกันได้ หรือส่งผลให้ข้อมูลที่อีกฝ่ายกำลังแสวงหาตกอยู่ในสภาพที่ไม่พร้อมใช้ได้ด้วย หรืออาจทำให้ผู้ต้องสงสัยที่แท้จริงทราบถึงการสืบสวนอาชญากรรมทางคอมพิวเตอร์ได้ นอกจากนี้ ยังมีบางกรณีที่หน่วยงานผู้บังคับใช้กฎหมายจากต่างรัฐกันเกิดความเข้าใจผิดว่าอีกฝ่ายเป็นอาชญากร และดำเนินการสืบสวนระหว่างกันเอง[136]

อย่างไรก็ตาม สำนักงานสาขาในยุโรปของผู้ให้บริการทางอินเตอร์เน็ตสัญชาติสหรัฐบางรายนั้น จะเลือกจัดทำข้อตกลงโดยสมัครใจกับหน่วยงานผู้บังคับใช้กฎหมายของรัฐในการเปิดแผยข้อมูลให้อีกฝ่ายโดยไม่ต้องผ่านกระบวนการขอความช่วยเหลือซึ่งกันและกันทางกฎหมาย อย่างไรก็ตามการเปิดเผยดังกล่าวจะต้องเป็นไปตามเงื่อนไขที่กำหนด โดยคำร้องขอจะต้องมาจากหน่วยงานที่มีอำนาจตามกฎหมายและชอบด้วยกฎหมาย อีกทั้งยังมีการวางกรอบเกี่ยวกับการสืบสวนและการรวบรวมข้อมูลทางอิเล็กทรอนิกส์ที่ต้องการด้วย ในขณะเดียวกันข้อมูลที่เปิดเผยนั้นจะต้องมีความเชื่อมโยงกับดินแดนของหน่วยงานรัฐผู้ร้องขอ และครอบคลุมเฉพาะข้อมูลจราจรและข้อมูลผู้ให้บริการเท่านั้น นอกจากนี้ การกระทำความผิดที่ถูกสืบสวน

---

[135] *Ibid.*,Para.59

[136] *Ibid.*,Para. 72

นั้นจะต้องเป็นความผิดตามกฎหมายของสหรัฐอเมริกา และระบบกฎหมายของหน่วยงานรัฐผู้ร้องขอจะต้องเคารพต่อหลักสิทธิมนุษยชนโดยเฉพาะอย่างยิ่งการปกป้องสิทธิส่วนบุคคลรวมไปถึงหลักนิติธรรมด้วย[137]

สำหรับประเด็นปัญหาที่เกิดขึ้นจากการเข้าถึงข้อมูลข้ามแดนนั้น รัฐสมาชิกต่างๆ ยังไม่ค่อยมีประสบการณ์ในการปรับใช้ตามข้อ 32b ของอนุสัญญาอย่างเป็นรูปธรรม และยังไม่เห็นถึงความจำเป็นที่จะต้องเปลี่ยนแปลงกฎหมายภายในของตนเพื่อรองรับอนุสัญญาข้อ 32 bนี้แต่อย่างใด[138] นอกจากนี้ รัฐภาคียังเกิดอุปสรรคในการระบุตัว Server และเจ้าของ Server[139] อีกทั้งในหลายกรณี servers ยังสามารถเคลื่อนย้ายตำแหน่งจากรัฐหนึ่งไปยังอีกรัฐหนึ่งได้อย่างง่ายดาย อีกทั้งยังมีการใช้ bots* ในการกระทำผิดในหลายกรณีอีกด้วย[140] ในขณะเดียวกัน การเข้าถึงข้อมูลข้ามแดนนั้น ยังเกิดความสับสนได้ในกรณีที่บุคคลผู้มีอำนาจจัดการข้อมูลอยู่ในดินแดนของรัฐผู้ดำเนินการสอบสวนอาชญากรรมทางคอมพิวเตอร์ แต่ข้อมูลดังกล่าวยังคงอยู่ในดินแดนของรัฐอื่น หรือในกรณีที่ IP Address ที่เกี่ยวข้องกับการสื่อสาร

---

[137] *Ibid*., Para.239

[138] Committee of experts on the operation of European conventions on co-operation in criminal matters (PC-OC). Summary of the replies to the questionnaire on mutual legal assistance in computer-related cases, p.5

[139] The cybercrime convention committee (T-CY). Report of the 2nd multilateral consultation of the parties[Online]. Strasbourg: Council of Europe, 2007. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/T-CY%20%282007%29%2003%20E.pdf [2013, May 7], Para.34

* โปรแกรมคอมพิวเตอร์ที่ทำให้คอมพิวเตอร์เป้าหมายติดเชื้อและถูกควบคุมได้จากระยะไกลโดยผู้กระทำผิด คอมพิวเตอร์ที่ถูกควบคุมโดยบอทส์สามารถถูกสั่งการให้ประสานงานกันทำหน้าที่บางอย่างได้ เช่น การโจมตีให้ระบบคอมพิวเตอร์ปฏิเสธการให้บริการ หรือการส่งจดหมายอิเล็กทรอนิกส์ที่ไม่พึงปรารถนา

[140] The cybercrime convention committee (T-CY). Meeting report of the 3rd consultation of the parties to the convention on cybercrime Para.29

ที่ถูกสอบสวนนั้นอยู่ในดินแดนของรัฐผู้สืบสวน แต่ข้อมูลที่จะเข้าถึงกลับถูกเก็บไว้ในดินแดนของรัฐอื่น[141]

นอกจากนี้ การที่ผู้ให้บริการทางอินเตอร์เน็ตหลายรายดำเนินการภายใต้เขตอำนาจของรัฐมากกว่าหนึ่งแห่ง ยังส่งผลให้ผู้ให้บริการดังกล่าวต้องประสบปัญหาเกี่ยวกับข้อกำหนดต่างๆ ที่แตกต่างกันไปด้วย โดยการทำตามคำขอที่ถูกกฎหมายของรัฐๆหนึ่ง อาจส่งผลเป็นการละเมิดต่อกฎหมายของรัฐอีกแห่งได้[142]

ในขณะเดียวกัน การเข้าถึงข้อมูลในลักษณะข้ามแดนและการนำข้อมูลดังกล่าวไปใช้ในกระบวนวิธีพิจารณาความอาญานั้นจะต้องเป็นไปตามเงื่อนไขและข้อป้องกัน (safeguards) ของรัฐผู้สืบสวนคดีด้วย ในการนี้ วิธีปฏิบัติ กระบวนวิธี เงื่อนไข และข้อป้องกันต่างๆ ของรัฐยังคงแตกต่างกันอยู่[143]

นอกจากวิธีการที่บัญญัติไว้ในข้อ 32 ของอนุสัญญากรุงบูดาเปสต์แล้ว พบว่า รัฐภาคียังมีวิธีการเข้าถึงข้อมูลข้ามแดนอีก 4 รูปแบบ โดยรูปแบบแรกจะเป็นกรณีที่ รัฐดำเนินการเข้าถึงข้อมูลในระหว่างทำการตรวจค้น โดยเจ้าหน้าที่รัฐภาคีส่วนใหญ่ ได้แก่ ฟินแลนด์ ลิธัวเนีย โปรตุเกส โปแลนด์ สวีเดน ตุรกี ชิลี บอสเนียและเฮอร์เซโกวีนา มอนเตเนโกร ไซปรัส ญี่ปุ่น ฮังการี อเมริกา จะสามารถเข้าถึงข้อมูลทางคอมพิวเตอร์จากเครื่องคอมพิวเตอร์ของผู้ต้องสงสัย หรือใช้รหัสผ่านของผู้ต้องสงสัยได้ ถ้าหากความไม่ปรากฏชัดว่า ข้อมูลทางคอมพิวเตอร์ที่จะเข้าถึงนั้นตกอยู่ในเขตอำนาจของรัฐใด[144] ส่วนในกรณีที่ความปรากฏชัดว่าข้อมูลดังกล่าวอยู่ภายใต้เขตอำนาจรัฐอื่น ประเทศฟินแลนด์ โปรตุเกส โปแลนด์ ชิลี มอนเตเนโกร ญี่ปุ่น และอเมริกา เห็นว่าฝ่ายเข้าหน้าที่รัฐยังคงสามารถเข้าถึงข้อมูลคอมพิวเตอร์ต่อไปได้ ในขณะที่รัฐอีกส่วนหนึ่งเห็นว่า

---

[141] Ad-hoc sub-group on jurisdiction and transborder access to data. Transborder access and jurisdiction: What are the options?, Para. 135

[142] I*bid,* Para.301

[143] *Ibid.*

[144] *Ibid*., Para.138

ต้องอาศัยความยินยอมตามข้อ 32 b ของอนุสัญญาแทน[145] ในการเข้าถึงข้อมูล ในระหว่างทำการตรวจค้นนี้ รัฐภาคีเช่น สาธารณรัฐเชค โปรตุเกส โปแลนด์ ชิลี บอสเนีย และเฮอร์เซโกวีนา และมอนเตเนโกรให้ความเห็นว่าจะต้องทำการแจ้งไปยังเจ้าหน้าที่รัฐต่างชาติที่เกี่ยวข้องด้วย ในขณะที่ประเทศลิธัวเนีย สวีเดน และตุรกีกลับเห็นว่าไม่จำเป็น อีกทั้งยังมีรัฐบางส่วนเห็นว่าควรพิจารณาตามสภาวการณ์เป็นสำคัญ[146]

วิธีการรูปแบบที่สองคือการเข้าถึงข้อมูลข้ามแดนโดนอาศัยรหัสผ่านที่ตนได้รับมาโดยชอบด้วยกฎหมาย โดยรหัสผ่านดังกล่าวมีไว้ใช้เข้าถึงข้อมูลคอมพิวเตอร์ที่มีเนื้อหาผิดกฎหมายหรือหลักฐานการกระทำความผิดอาญาอยู่ ทั้งนี้หน่วยงานผู้บังคับใช้กฎหมายของรับส่วนใหญ่จะสามารถเข้าถึงได้ข้อมูลได้ทั้งในกรณีที่ไม่ปรากฏชัดว่าข้อมูลนั้นอยู่ภายใต้เขตอำนาจใดและในกรณีที่ปรากฏชัดว่าข้อมูลนั้นอยู่ในเขตอำนาจรัฐต่างขาติ ยกเว้นกรณีของประเทศสาธารณรัฐเชค ลิธัวเนีย สวีเดน ฮังการี เอสโตเนีย และเนเธอร์แลนด์[147] สำหรับการเข้าถึงข้อมูลข้ามแดนโดนอาศัยรหัสผ่านนี้ รัฐบางรัฐเห็นว่าจะต้องดำเนินการโดยแจ้งเจ้าหน้าที่รัฐต่างชาติผู้เกี่ยวข้องด้วย ในขณะที่รัฐบางรัฐเห็นว่าการดังกล่าวไม่จำเป็น หรือเห็นว่าการแจ้งเจ้าหน้าที่รัฐต่างชาติจะต้องคำนึงถึงสถานการณ์แวดล้อมด้วย[148]

วิธีการรูปแบบที่สามคือการเข้าถึงข้อมูลข้ามแดนโดยอาศัยวิธีการทางเทคนิคหรือใช้ซอฟต์แวร์พิเศษ ทั้งนี้ จะมีรัฐเพียงไม่กี่รัฐที่อนุญาตให้ใช้วิธีการนี้ได้ภายใต้สถานการณ์ที่จำกัดเท่านั้น และหากความปรากฏชัดว่าระบบคอมพิวเตอร์ที่จะเขาถึงอยู่ในเขตอำนาจรัฐต่างชาติ รัฐภาคีเกือบทั้งหมดยกเว้น บอสเนียและเฮอร์เซโกวีนา ญี่ปุ่น และชิลี จะเห็นว่าวิธีการเช่นว่านี้ไม่สามารถใช้ได้เลย[149]

---

[145] *Ibid*., Para.139

[146] *Ibid*., Para.140

[147] *Ibid*., Para.143-144

[148] *Ibid.,* Para.145

[149] *Ibid.,* Para.148-149

วิธีการรูปแบบที่สี่ เป็นกรณีการให้ผู้ให้บริการทางอินเตอร์เน็ตดำเนินการจัดหาข้อมูลเกี่ยวกับผู้ต้องสงสัยให้ฝ่ายเจ้าหน้าที่รัฐ ทั้งนี้ หากข้อมูลที่เจ้าหน้าทีรัฐตามหาอยู่เป็นข้อมูลเกี่ยวกับคนชาติของตนหรือเป็นข้อมูลเกี่ยวกับคนต่างชาติที่กระทำความผิดในดินแดนของตน แต่ข้อมูลดังกล่าวกลับตั้งอยู่และถูกจัดการดูแลในดินแดนรัฐอื่น หน่วยงานผู้บังคับใช้กฎหมายจะต้องดำเนินการร้องขอความช่วยเหลือซึ่งกันและกันทางกฎหมาย[150] อย่างไรก็ตามในปัจจุบันได้มีผู้ให้บริการทางอินเตอร์เน็ตข้ามชาติบางรายที่ดำเนินการเปลี่ยนนโยบายใหม่ โดยจะกำหนดเงื่อนไขสำหรับการเปิดเผยข้อมูลผู้ใช้บริการและข้อมูลจราจรให้กับเจ้าหน้าที่รัฐ แม้จะเป็นกรณีที่ข้อมูลดังกล่าวตั้งอยู่ในเขตอำนาจของรัฐอื่นก็ตาม[151]

4.3.5 การรวบรวมข้อมูลจราจรตามเวลาจริง และการดักรับข้อมูลทางเนื้อหา

รัฐบางรัฐ ได้บัญญัติกฎหมายภายในที่รองรับการรวบรวมข้อมูลจราจรและการดักรับข้อมูลเนื้อหาทางคอมพิวเตอร์ไว้โดยตรง[152] ซึ่งจะได้กำหนดหลักเกณฑ์ทั่วไปเกี่ยวกับการเข้าสู่ระบบคอมพิวเตอร์ การดักรับหรือการบันทึกการสื่อสารที่มีขึ้นโดยอาศัยระบบคอมพิวเตอร์ เป็นต้น ในขณะที่รัฐภาคีบางส่วนจะอาศัยการปรับใช้กฎเกณฑ์เกี่ยวกับการดักฟังจากกฎหมายวิธีพิจารณาความทางอาญา[153] ทั้งนี้ การดำเนินการจะต้องได้รับหมายศาลเสียก่อน สำหรับรัฐที่ปรับนำกฎหมายเกี่ยวกับการดักฟังมาปรับใช้นั้น รัฐบางรัฐจะระบุให้มาตรการดังกล่าวสามารถปรับใช้ได้เฉพาะฐานความผิดสำคัญบางประเภท อาทิ อาชญากรรมต่อความลับ

---

[150] *Ibid*., Para. 155-156

[151] *Ibid*., p.31 fn.79

[152] Albanian Criminal Procedure Code, Art.221-222; Bosnia and Herzegovina Criminal Procedure Code, Art.116; Bulgaria Penal Procedure Code, Art.172; Croatia Criminal Procedure Art.332-335; Czech Code of Criminal Procedure, Section 88, Estonian Criminal Procedure Code, Art.117-118; Finland Coercive Measures Act, Chapter5a ; France Criminal Procedure Code, Art.706-95; German Code of Criminal Procedure, Section 100b,100g; Portugal Cybercrime Law nr 109/2009, Art.18; Romania Law no 161/2003, Art.57; 18 U.S.C. § 2704; 18 U.S.C. § 2511,3121 - § 3127

[153] Bulgaria Penal Procedure Code, Art.163, 165; Croatia Criminal Procedure Code. Art.332-335; Turkish Criminal Procedure Code no 5271/2005. Art. 135

บูรณภาพ และความพร้อมใช้งานของข้อมูลคอมพิวเตอร์ สิ่งลามกอนาจารเด็ก การปลอมแปลงเป็นต้น[154] ในขณะที่รัฐบางกลุ่มจะพิจารณาจากอัตราโทษแทน เช่น ฝรั่งเศส จะอนุญาตให้ดักข้อมูลหากมีโทษจำตุกตั้งแต่สองปีขึ้นไป[155]

ข้อแตกต่างสำคัญอีกประการหนึ่งในการปรับใช้อนุสัญญาส่วนนี้ได้แก่ระยะเวลาในการดักรับข้อมูลที่จะยาวนานแตกต่างออกไป ยกตัวอย่างเช่น ประเทศโครเอเชีย[156] จะมีกำหนดเวลา 6 เดือน และสามารถดำเนินการขอยื่นเวลาไปอีก 6 เดือนได้ ส่วนประเทศมอนเตเนโกร[157]นั้นจะกำหนดระยะเวลาสูงสุดอยู่ที่ 4 เดือน ส่วนประเทศฝรั่งเศสจะมีกำหนดการดักรับข้อมูลสูงสุดไม่เกิน 15 วัน และต่ออายุได้เพียง 1 ครั้ง[158] เป็นต้น

ในขณะเดียวกัน กฎหมายอาชญากรรมทางคอมพิวเตอร์ของประเทศโปรตุเกส[159] ได้กำหนดบทบัญญัติสำหรับการให้ความช่วยเหลือสำหรับการดักรับข้อมูลไว้โดยเฉพาะซึ่งรองรับการดำเนินการให้ความช่วยเหลืออย่างเร่งด่วนด้วย[160]

อย่างไรก็ตาม รัฐภาคียังขาดประสบการณ์สำหรับการส่งหรือจัดการตามคำขอที่เกี่ยวข้องกับการดักรับข้อมูลทางคอมพิวเตอร์ มีแต่คำขอความร่วมมือในด้านการดักฟังโทรศัพท์เป็นบางครั้งบางคราว หรือคำขอในการค้นและยึดข้อมูลเท่านั้น โดยยังไม่เกิดประเด็นปัญหาทางกฎหมายหรือในทางปฏิบัติใดๆ[161]

---

[154] Croatia Criminal Procedure Code, Art.334 ; German Code of Criminal Procedure, Section 100a(2); Montenegro Criminal Procedure Code, Art. 157, 158

[155] France Criminal Procedure Code, Art.100

[156] Croatia Criminal Procedure Code, Art.335 (3)

[157] Montenegro Criminal Procedure Code,Art.159 (5)

[158] France Criminal Procedure Code, Art. 706-95

[159] Portugal Cybercrime Law nr 109/2009, Art. 26

[160] Portugal Cybercrime Law nr 109/2009, Art. 26(3)

[161] Pedro Verdelho. The effectiveness of international co-operation against cybercrime: examples of good practice, p.32-33

4.3.6 เครือข่ายจุดติดต่อตลอดเวลา

รัฐต่างๆสามารถเข้าร่วมเครือข่ายจุดติดต่อตลอดเวลา ได้โดยไม่ต้องเข้าเป็นภาคีของอนุสัญญาเสียก่อน[162] ทั้งนี้ นับจากเดือนธันวาคม 2011 รัฐภาคีทั้งหมดของอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ได้จัดตั้งจุดติดต่อตลอดเวลาแล้ว[163]

ในบรรดารัฐภาคีของอนุสัญญานั้น จุดติดต่อที่กำหนดมาส่วนใหญ่จะเป็นหน่วยงานตำรวจ ซึ่งรัฐบางรัฐจะกำหนดให้ตำรวจที่ดูแลคดีอาชญากรรมคอมพิวเตอร์โดยเฉพาะเป็นจุดติดต่อ ในขณะที่รัฐบางรัฐจะกำหนดให้ตำรวจทั่วไปมีหน้าที่รับผิดชอบดังกล่าว อย่างไรก็ตาม ในกรณีของประเทศมาเซโดเนีย โรมาเนีย เนเธอร์แลนด์ และสหรัฐอเมริกา หน่วยงานอัยการจะทำหน้าที่เป็นเครือข่ายในเครือข่ายจุดติดต่อตลอดเวลาแทน[164] อนึ่ง รัฐบางรัฐจะกำหนดให้เจ้าหน้าที่รัฐคนใดคนหนึ่งดูแลแทนที่จะเป็นหน่วยงานทั้งหน่วยงาน ยกตัวอย่างเช่น ประเทศเอสโตเนีย ได้กำหนดให้เจ้าหน้าที่ของ Central Criminal Police ในแผนกข่าวกรองด้านอาชญากรรม เป็นจุดติดต่อของเครือข่ายจุดติดต่อ ตามข้อ 35 แห่งอนุสัญญากรุงบูดาเปสต์ โดยที่เจ้าหน้าที่คนดังกล่าวนั้นจะทำหน้าที่เป็นจุดติดต่อขององค์การตำรวจสากล และองค์การตำรวจสหภาพยุโรปด้วย[165]

จะเห็นได้ว่าการแต่งตั้งหน่วยงานตำรวจเป็นจุดติดต่อนั้น สามารถอำนวยความสะดวกให้แก่การดำเนินมาตรการสืบสวนคดีอาชญากรรมทางคอมพิวเตอร์ได้ เพราะเป็นการติดต่อ

---

[162] The cybercrime convention committee (T-CY). Report of the 2nd multilateral consultation of the parties Para.35

[163] Data protection and cybercrime division. Global project on cybercrime (phase 2) 1 March 2009-11 December 2011 final report [Online]. Strasbourg: Council of Europe, Directorate genral of human rights and rule of law, Information society and action against crime directorate, 2012. Available from: http://www.coe.int/t/dghl/standardsetting/t-cy/TCY2012/2079_adm_finalreport_V12_9apr12.pdf [2013, May 8], p.16

[164] Pedro Verdelho. The effectiveness of international co-operation against cybercrime: examples of good practice., p.11-12

[165] *Ibid*., p.24

ไปยังหน่วยงานผู้ดำเนินการบังคับใช้มาตรการสืบสวนโดยตรง แต่ในขณะเดียวกัน การแต่งตั้งอัยการเป็นจุดติดต่อนั้น สามารถช่วยอำนวยความสะดวกในกรณีที่หน่วยงานรัฐผู้มีอำนาจสืบสวนต้องร้องขอการอนุญาตจากหน่วยงานตุลาการ

ช่องทางเครือข่ายจุดติดต่อตลอดเวลานี้มักจะถูกใช้คำร้องขอความช่วยเหลือซึ่งกันและกันทางกฎหมายในการเก็บรักษาข้อมูลจราจรและในบางกรณีช่องทางนี้จะถูกใช้ในการแลกเปลี่ยนข้อมูลและข่าวกรองกันระหว่างตำรวจอีกด้วย อย่างไรก็ดี รัฐภาคีให้ความเห็นว่า ช่องทางการติดต่อผ่านทางเครือข่าย จุดติดต่อตลอดเวลานั้น ยังไม่ถูกใช้มากนัก และคำขอที่ส่งไปก็ไม่ถูกตอบรับในบางครั้ง เพราะบุคลากรขาดความเข้าใจชัดเจนว่า หน้าที่ที่แท้จริงของเครือข่าย 24/7 นั้นคืออะไร และรัฐภาคีสามารถดำเนินการใดผ่านทางเครือข่ายนี้ได้บ้าง

สำหรับการใช้เครือข่ายจุดติดต่อตลอดเวลาเพื่อให้ความช่วยเหลือตามข้อ 29,30 ของอนุสัญญากรุงบูดาเปสต์นั้น จุดติดต่อบางส่วนได้มีบทบาทในการรับส่งและติดตามคำขอให้เก็บรักษาข้อมูลอย่างสม่ำเสมอ ในขณะที่จุดติดต่อบางส่วนที่แม้จะมีอำนาจในการดำเนินการดังข้างต้นแต่กลับไม่ดำเนินการมากนักในความเป็นจริง[166] นอกจากนี้ จุดติดต่อจำนวนหนึ่ง เช่นในกรณีของประเทศลิธัวเนีย หรืออาร์เมเนีย ที่ไม่สามารถรับส่ง หรือติดตามผลคำขอเกี่ยวกับการเก็บรักษาข้อมูลได้[167] เพราะฐานทางกฎหมายเกี่ยวกับการเก็บรักษาข้อมูลยังขาดความชัดเจนและมีกระบวนการซับซ้อน สำหรับจุดติดต่อของไซปรัสนั้น จุดติดต่อมีหน้าที่ในการรับคำขอและส่งต่อไปให้กระทรวงยุติธรรมตรวจสอบความถูกต้องและดำเนินการในขั้นต่อไปเท่านั้น[168]

ในการใช้งานจุดติดต่อตามเครือข่ายจุดติดต่อตลอดเวลาเพื่อเก็บรักษาข้อมูลนั้น จุดติดต่อจะเป็นฝ่ายรับคำร้องขอความช่วยเหลือระหว่างประเทศและสั่งการให้ผู้ให้บริการทางอินเตอร์เน็ตหรือนิติบุคคลหรือบุคคลที่เกี่ยวข้องเก็บรักษาข้อมูลต่อไป หลังจากนั้นเมื่อรัฐได้รับคำร้องขอ

---

[166] The cybercrime convention committee (T-CY). Assessment report: Implementation of the preservation provisions of the Budapest convention on cybercrime, p.13

[167] *Ibid*., p.14-15

[168] *Ibid*.,p.14

ความช่วยเหลือซึ่งกันและกันทางกฎหมาย และศาลได้ออกคำสั่งศาลแล้ว ฝ่ายผู้ให้บริการทางอินเตอร์เน็ตหรือผู้เก็บรักษาข้อมูลก็จะเปิดเผยข้อมูลนั้นให้เจ้าหน้าที่รัฐ ซึ่งจะส่งต่อข้อมูลไปยังรัฐผู้ร้องขอความช่วยเหลือในลำดับถัดไป[169]

มีการตั้งข้อสังเกตว่า การใช้เครือข่ายจุดติดต่อตลอดเวลา ทำให้ความสัมพันธ์ระหว่างหน่วยงานต่างๆมีความเป็นทางการน้อยลง ซึ่งช่วยให้ความร่วมมือระหว่างกันเป็นไปด้วยดีมากขึ้น แต่ในขณะเดียวกันหน่วยงานต่างๆก็ไม่มีหลักประกันแน่นอนว่า คำขอที่ถูกส่งไปนั้นจะได้รับการตอบรับที่เหมาะสมจากจุดติดต่ออื่นๆหรือไม่[170]

รัฐภาคีและรัฐผู้ลงนามของอนุสัญญากรุงบูดาเปสต์ได้เข้าร่วมเครือข่ายของกลุ่มประเทศทางอุตสาหกรรมที่พัฒนาแล้ว 8 ประเทศ (G8) ซึ่งมีกลุ่มย่อยด้านอาชญากรรมที่ใช้เทคโนโลยีขั้นสูงเป็นผู้รวบรวมและดูแลจัดการรายชื่อของจุดติดต่อต่างๆ อีกทั้งเปิดรับประเทศนอกกลุ่ม G8 เข้าเป็นสมาชิก ทั้งนี้ จะมีบางรัฐ เช่น เยอรมนี ที่เป็นสมาชิกในเครือข่ายของกลุ่ม G8 หากยังไม่ได้กำหนดจุดติดต่อตามอนุสัญญากรุงบูดาเปสต์แต่อย่างใด สำหรับการใช้งานจริงนั้นกลุ่มย่อยด้านอาชญากรรมที่ใช้เทคโนโลยีขั้นสูงของ G8 ได้ให้ความเห็นว่าปริมาณของคำขอภายในเครือข่ายยังมีไม่มากนัก แต่ก็สามารถให้ความช่วยเหลือในคดีที่สำคัญมากบางคดีได้เป็นอย่างดี[171]

นอกจากนี้เครือข่ายจุดติดต่อตลอดเวลาตามข้อ 35 ของอนุสัญญากรุงบูดาเปสต์นั้นยังดำเนินการควบคู่กันไปกับ เครือข่ายจุดติดต่อตลอดเวลาขององค์การตำรวจสากล (Interpol) ที่เรียกว่า Interpol National Central Reference Points (NRCP) ซึ่งดำเนินการช่วยเหลือบรรดาประเทศสมาชิกเป็นการถาวรด้วย เครือข่าย NRCP มีจุดประสงค์เพื่อให้ หน่วยงานตำรวจสามารถระบุตัวผู้เชี่ยวชาญจากประเทศต่างๆสำหรับให้ความช่วยเหลือ ในการสืบสวนและรวบรวมคดีหลักฐานในคดีที่เกี่ยวข้องกับคอมพิวเตอร์ได้อย่างทันท่วงที ทั้งนี้ จุดติดต่อของ NRCP บางจุด

---

[169] *Ibid*., p.16

[170] Pedro Verdelho. The effectiveness of international co-operation against cybercrime: examples of good practice, p.33-34

[171] *Ibid*., p.13-14

จะเป็นจุดติดต่อเดียวกันกับเครือข่ายของกลุ่ม G8 และของอนุสัญญากรุงบูดาเปสต์ แต่บางจุดก็ไม่ตรงกันแต่เพียงอย่างใด[172] ในทางปฏิบัตินั้น เครือข่ายขององค์การตำรวจสากลยังไม่สามารถดำเนินการต่อคำขอที่มีความเร่งด่วนสูงเช่น ในกรณีของการเก็บรักษาข้อมูลได้ และลักษณะของการให้ความร่วมมือต่างๆตามเครือข่ายนี้ จะดำเนินการตามหลักในการให้ความร่วมมือกันโดยทั่วไปขององค์การตำรวจสากล [173]

4.4 การปรับใช้อนุสัญญากรุงบูดาเปสต์ในระดับระหว่างประเทศ

การปรับใช้อนุสัญญากรุงบูดาเปสต์ในระดับระหว่างประเทศมีบทบาทสำคัญต่อการสนับสนุนให้รัฐจัดทำกฎหมายที่สอดคล้องกับอนุสัญญาเพื่อการเข้าเป็นภาคีเข้าภาคยานุวัติ หรือปรับใช้อนุสัญญา ที่เป็นเช่นนี้เพราะ การปรับใช้อนุสัญญากรุงบูดาเปสต์ในระดับระหว่างประเทศจะนำรัฐต่างๆและผู้มีส่วนได้เสียอื่นๆ มาปรึกษาหารือกัน[174] อีกทั้งยังดำเนินการให้ความช่วยเหลือทางเทคนิคและเสริมสร้างขีดความสามารถระหว่างกันอีกด้วย รายละเอียดของการปรับใช้อนุสัญญากรุงบูดาเปสต์ในระดับระหว่างประเทศมีดังต่อไปนี้

---

[172] *Ibid*., p.19

[173] *Ibid*., p.19

[174] Henrik Kaspersen, Joseph Schwerha, and Drazen Dragizevic. Article 15: conditions and safeguards under the Budapest convention on cybercrime [Online]. Strasbourg: Council of Europe, Directorate general of human rights and rule of law, Cybercrime division, 2012. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/2467_SafeguardsRep_v18_29mar12.pdf [2013, May 8]

4.4.1 การประชุมคณะกรรมการอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ (Convention on Cybercrime Committee หรือ T-CY)

การประชุมคณะกรรมการอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ จะมีขึ้นเพื่อปรึกษาหารือกันระหว่างรัฐภาคีและทบทวนบทบัญญัติต่างๆ ดังที่กำหนดไว้ในข้อ 46 ของอนุสัญญากรุงบูดาเปสต์[175]

การประชุมของคณะกรรมการอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์จะมีขึ้นปีละ 2 ครั้ง โดยสมาชิกของคณะกรรมการจะประกอบไปด้วยตัวแทนจากรัฐภาคีของอนุสัญญากรุงบูดาเปสต์ รัฐผู้ลงนามและรัฐที่ได้รับคำเชิญให้เข้าภาคยานุวัติอนุสัญญา[176] ในขณะเดียวกันตัวแทนจากรัฐสมาชิกอื่นๆของสภายุโรป และองค์การระหว่างประเทศต่างๆอาทิ คณะกรรมการสหภาพแอฟริกัน (African Union Commission) สหภาพยุโรป องค์การตำรวจสหภาพยุโรป สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union หรือ ITU) องค์การตำรวจสากล องค์การเพื่อความร่วมมือทางเศรษฐกิจและด้านการพัฒนา , องค์การรัฐอเมริกัน (Organisation of American States หรือOAS) สำนักงานสหประชาชาติด้านอาชญากรรมและยาเสพติด (United Nations Office on Drug and Crime หรือ UNODC) จะได้รับเชิญเข้ามาในฐานะผู้สังเกตการณ์ด้วย[177]

4.4.1.1 สำนักงานประจำคณะกรรมการอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ (The Bureau)

สำนักงานประจำคณะกรรมการอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ (The Bureau) จะเป็นผู้มีบทบาทชี้แนะและสนับสนุนคณะกรรมการอนุสัญญาอาชญากรรมทางคอมพิวเตอร์ในการดำเนินการประชุม ในการนี้ ทางสำนักงานจะการจัดเตรียมงาน

---

[175] Cybercrime convention committee (T-CY) [Online]. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/Default_TCY_en.asp [2013, May 8]

[176] *Ibid.*

[177] *Ibid.*

ในด้านต่างๆได้แก่ การร่างเอกสารทางกฎหมายหรือความเห็นของคณะกรรมการ การจัดเตรียมและร่างความเห็นเกี่ยวกับเรื่องที่หน่วยงานอื่นๆของสภายุโรปร้องขอมา การจัดเตรียมรายงานโดยนำความเห็นของตัวแทนคณะกรรมการอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์มาพิจารณาประกอบด้วย การวางแผนเกี่ยวกับกิจกรรมของคณะกรรมการพร้อมกำหนดลำดับความสำคัญ เป็นต้น[178]

ในขณะเดียวกัน สำนักงานประจำคณะกรรมการ ยังมีหน้าที่ทางด้านธุรการอื่นๆด้วย อาทิ การทบทวนวาระการประชุมของคณะกรรมการพร้อมเสนอวิธีการดำเนินงาน การเชิญวิทยากรผู้ทรงคุณวุฒิจากภายนอกการแต่งตั้งผู้เชี่ยวชาญให้ไปดำเนินกิจกรรมที่ได้กำหนดไว้ และการนัดหมายประสานงานกับหน่วยงานอื่นๆของสภายุโรป การรายงานกิจกรรมของสำนักงานกลับไปยังคณะกรรมการอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ เป็นต้น นอกจากนี้ทางสำนักงานยังมีหน้าที่จัดการตามเรื่องอื่นๆที่ทางคณะกรรมการมอบหมายมาโดยตรงอีกด้วย[179]

สมาชิกของสำนักงานประจำคณะกรรมการอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์นั้น จะประกอบไปด้วย ประธาน รองประธาน และสมาชิกทั่วไปจำนวน 4 คน เป็นอย่างน้อย สมาชิกเหล่านี้จะมีที่มาจากการเลือกตั้งภายในคณะกรรมการอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ โดยวาระดำรงตำแหน่งของสมาชิกของสำนักงานประจำคณะกรรมการจะอยู่ที่ 2 ปี โดยผู้ดำรงตำแหน่งประธานหรือรองประธานนั้นสามารถลงเลือกตั้งหลังหมดวาระได้อีกหนึ่งครั้ง นอกจากนี้ ประธานสำนักงานผู้พ้นจากตำแหน่งจะยังคงเป็นสมาชิกโดยนิตินัยของสำนักงานด้วย ในระหว่างที่ประธานคนใหม่เข้าดำรงตำแหน่งในสมัยแรก[180]

---

[178] The cybercrime convention committee (T-CY). Rules of procedure for the bureau [Online]. Strasbourg: Council of Europe, 2012. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/TCY_2012_24E_BU_Rules_Revised_Dec12%20.pdf [2013, May 8], Art.4

[179] *Ibid.*

[180] *Ibid.*, Art. 2

4.4.1.2 บทบาทของคณะกรรมการอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์

จากบทบัญญัติข้อ 46 ของอนุสัญญากรุงบูดาเปสต์ จะเห็นได้ว่าคณะกรรมการอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์นี้ จะมีหน้าที่สามประการ ได้แก่ การสนับสนุนให้การปรับใช้อนุสัญญาเป็นไปอย่างมีประสิทธิภาพ การแลกเปลี่ยนข้อมูล และการพิจารณาหาความเป็นไปได้ในการเพิ่มเติมหรือปรับปรุงแก้ไขอนุสัญญากรุงบูดาเปสต์

ในด้านการสนับสนุนการปรับใช้อนุสัญญานั้น คณะกรรมการอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์จะจัดทำ บันทึกแนวทางการตีความ (Guidance Note) ไว้ให้รัฐภาคีสามารถใช้อนุสัญญากรุงบูดาเปสต์ตอบสนองต่อข้อท้าทายใหม่ๆได้ โดยในปัจจุบัน บันทึกแนวทางการตีความของคณะกรรมการอาชญากรรมทางคอมพิวเตอร์ครอบคลุมประเด็นปัญหา 4 เรื่อง ได้แก่ ระบบคอมพิวเตอร์ บอทเน็ทส์ การเข้าถึงข้อมูลข้ามแดน และเรื่องการกระทำผิดด้วยวิธีโจรกรรมข้อมูลระบุตัวตนหรือ Phishing

ทั้งนี้ รัฐภาคีได้ให้ความเห็นว่า คำว่าระบบคอมพิวเตอร์ ในอนุสัญญากรุงบูดาเปสต์นั้นจะครอบคลุมไปยังเทคโนโลยีอื่นๆ นอกเหนือไปจากเครื่องคอมพิวเตอร์ทั่วไป อาทิ โทรศัพท์มือถือรุ่นใหม่ หรือคอมพิวเตอร์แท็บเล็ต เป็นต้น[181] นอกจากนี้ บทบัญญัติเกี่ยวกับฐานความผิดของอนุสัญญายังสามารถนำมาปรับใช้กับความผิดประเภทใหม่ๆ อาทิ การใช้บอทเน็ตส์และการโจรกรรมตัวตนได้[182] ส่วนในบันทึกแนวทางการตีความเรื่องการเข้าถึงข้อมูลข้ามแดนนั้น

---

[181] The cybercrime convention committee (T-CY). T-CY guidance note#1 On the notion of “Computer System” Art.1a Budapest convention on cybercrime [Online]. Strasbourg: Council of Europe,2012. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY2012/T-CY%282012%2921E_guidanceNote1_article1_final.pdf [2013, May 8]

[182] The cybercrime convention committee (T-CY). T-CY guidance note#2 Provisions of the Budapest convention covering botnets [Online]. Strasbourg: Council of Europe,2013. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/TCY_20

รัฐภาคีจะทำการตีความองค์ประกอบต่างๆของการเข้าถึงข้อมูลข้ามแดนตามข้อ 32b ของอนุสัญญากรุงบูดาเปสต์เอาไว้ อาทิ ความหมายของคำว่า การเข้าถึงโดยไม่ต้องขออนุญาตรัฐภาคีอีกฝ่าย ความหมายของการให้ความยินยอม กฎหมายที่บังคับใช้ในการเข้าถึงข้อมูลข้ามแดน ตัวตนและตำแหน่งของผู้ให้ความยินยอมที่จะจัดหากหรือเปิดเผยข้อมูล เป็นต้น[183]

เนื้อหาของบันทึกคำแนวทางแต่ละฉบับนั้น จะเป็นการแสดงให้เห็นว่ารัฐภาคีของอนุสัญญากรุงบูดาเปสต์ มีความเข้าใจร่วมกันอย่างไรบ้างในการปรับใช้อนุสัญญากับประเด็นปัญหาอาชญากรรมทางคอมพิวเตอร์เรื่องใดเรื่องหนึ่ง[184] ดังนั้น การจัดบันทึกคำแนวทางนี้จึงช่วยเป็นการแสดงวิธีปฏิบัติของบรรดารัฐภาคีเพื่อให้การปรับใช้อนุสัญญามีความชัดเจนและเป็นไปในทิศทางเดียวกันมากขึ้น

สำหรับการสำรวจและทบทวนอนุสัญญานั้น ที่ประชุมคณะกรรมการ จะตกลงบทบัญญัติที่จะดำเนินการทบทวนในการประชุมรอบถัดไปเป็นลำดับแรก หลังจากนั้น สำนักงานประจำคณะกรรมการจะจัดทำแบบสอบถามเกี่ยวกับบทบัญญัติของอนุสัญญาที่ต้องการทบทวนไปยังบรรดารัฐต่างๆ เมื่อได้รับคำตอบจากรัฐแล้วทางสำนักงานและสมาชิกคณะกรรมการจะรวบรวมคำตอบและจัดทำรายงานไว้ให้ที่ประชุมคณะกรรมการ เสวนาและให้คำแนะนำที่เกี่ยวข้องกับบทบัญญัติดังกล่าว ท้ายที่สุดจะมีการจัดทำรายงานเพื่อเผยแพร่ข้อมูลเกี่ยวกับวิธีปฏิบัติของรัฐและบทเรียนที่ได้รับ[185] โดยในปี 2012 ได้มีการทบทวน การปรับใช้บทบัญญัติข้อ

13_6E_GN2_botnets_V5public.pdf [2013, May 8]; The cybercrime convention committee (T-CY). T-CY guidance note#4 Identity theft and phishing related to fraud [Online]. Strasbourg: Council of Europe, 2013. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY_2013_8E_guidanceNote4_id%20theft_V8.pdf [2013, May 8]

[183] The cybercrime convention committee (T-CY). T-CY guidance note#3 Transborder access to data (article 32) [Online]. Strasbourg: Council of Europe,2013. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/TCY_2013_7E_GN3_transborder_V2public.pdf [2013, May 8]

[184] *Ibid.,* p.1,4

[185] The cybercrime convention committee (T-CY). Abridged meeting report of the sixth plenary, p.10

16, 17, 29, 30 ของอนุสัญญากรุงบูดาเปสต์ ซึ่งมีเนื้อหาเกี่ยวกับการรักษาข้อมูลที่ถูกเก็บไว้อย่างรวดเร็ว การเปิดเผยข้อมูลจราจรอย่างรวดเร็ว และการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายด้วยวิธีดังกล่าว[186] นอกจากนี้ คณะกรรมการอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ได้ตกลงที่จะประเมินการปรับใช้ข้อ 31 ของอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ต่อไปในที่ประชุมปี 2013 ต่อไป ในการนี้ คณะกรรมการเห็นว่า การให้ความช่วยเหลือในการรักษาข้อมูลที่ถูกเก็บไว้อย่างรวดเร็วตาม ข้อ 29 และ 30 ของอนุสัญญานั้นถูกใช้อย่างจำกัด ซึ่งปัจจัยหนึ่งเป็นผลมาจากรัฐภาคีประสบความยากลำบากในการส่งคำขอเข้าถึงข้อมูลอย่างเป็นทางการตามมาภายหลัง[187]

ในด้านการพิจารณาความเป็นไปได้ในการเพิ่มเติมหรือปรับปรุงเนื้อหาของอนุสัญญานั้น ที่ประชุมคณะกรรมการอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ในปี 2011 ได้ดำเนินการจัดตั้งกลุ่มย่อยเฉพาะกิจเพื่อเตรียมร่างกฎเกณฑ์เพิ่มเติมเกี่ยวกับการเข้าถึงข้อมูลข้ามแดนตามข้อ 32 ของอนุสัญญากรุงบูดาเปสต์ โดยกฎเกณฑ์เพิ่มเติมนั้นอาจจะจัดทำออกมาในรูปแบบการแก้ไขเนื้อหาอนุสัญญา หรือพิธีสารเพิ่มเติม หรือในรูปแบบคำแนะนำแล้วแต่ความเหมาะสม[188] ทั้งนี้ ในช่วงเวลาที่ร่างเนื้อหาของข้อ 32 ในอนุสัญญานั้น รัฐต่างๆยังขาดประสบการณ์ในการดำเนินการสืบสวนคดีอาชญากรรมทางคอมพิวเตอร์ข้ามประเทศ ตัวเนื้อหาของข้อ 32 ที่เป็นอยู่ในปัจจุบันจึงครอบคลุมเฉพาะประเด็นที่บรรลุข้อตกลงได้และเป็นเพียงมาตรฐานขั้นต่ำเท่านั้น[189]

---

[186] The cybercrime convention committee (T-CY). Abridged meeting report of the seventh plenary, p.8

[187] *Ibid*., Para.11

[188] The cybercrime convention committee (T-CY). Abridged meeting report of the sixth plenary [Online]. Strasbourg: Council of Europe, 2011. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/TCY_2011_10E_PlenAbrMeetRep_V4%20_28Nov2011.pdf [2013, May 8], p.14

[189] *Ibid*., p.13

ประเด็นที่ทางกลุ่มย่อยเฉพาะกิจจะดำเนินการตรวจสอบได้แก่ การปรับใช้บทบัญญัติข้อ 19,22, และ 32 ของอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ความจำเป็นและข้อควรระวังในการเข้าถึงข้อมูลข้ามแดน แนวปฏิบัติในการเข้าถึงข้อมูลข้ามแดนภายใต้สถานการณ์ต่างๆ ไม่ว่าจะเป็นกรณีที่การเข้าถึงที่กระทำโดยหน่วยงานผู้บังคับใช้กฎหมายโดยตรง หรือกรณีที่การเข้าถึงข้ามแดนดำเนินการโดยผู้ให้บริการทางอินเตอร์เน็ตหรือนิติบุคคลอื่นๆจากภาคเอกชน[190]

4.4.2 การสนับสนุนการปรับใช้อนุสัญญาโดยสภายุโรป

ในขณะเดียวกัน สภายุโรป ซึ่งเป็นผู้จัดทำอนุสัญญากรุงบูดาเปสต์และพิธีสารเพิ่มเติมนั้น ยังได้ดำเนินกิจกรรมเพื่อสนับสนุนการปรับใช้อนุสัญญาโดยการจัดประชุม Octopus Interface Conference และดำเนินโครงการอาชญากรรมทางคอมพิวเตอร์สากล (Global Project on Cybercrime) อีกด้วย รายละเอียดของแต่ละกิจกรรมนั้น มีดังต่อไปนี้

4.4.2.1 Octopus Interface Conference

การประชุม Octopus Interface เป็นการประชุมเกี่ยวกับความร่วมมือด้านอาชญากรรมทางคอมพิวเตอร์ระหว่างผู้เชี่ยวชาญด้านอาชญากรรมทางคอมพิวเตอร์ที่มาจากทั้งภาครัฐ ภาคเอกชน และองค์การระหว่างประเทศทั่วโลก การประชุมนี้จะมีบทบาทในการระบุและศึกษาถึงประเด็นปัญหาต่างๆด้านอาชญากรรมทางคอมพิวเตอร์และการให้ความร่วมมือทางระหว่างประเทศ นอกจากนี้ ที่ประชุมยังดำเนินการทบทวนประสิทธิภาพของกฎหมายภายในด้านอาชญากรรมทางคอมพิวเตอร์ด้วย

การประชุมจะแบ่งออกเป็นการรายงานความเปลี่ยนแปลง (update sesssion) และการอบรมเชิงปฏิบัติการ (workshop) และการประชุมเกี่ยวกับแนวโน้มในอนาคต (outlook session) นับได้ว่าการประชุม Octopus Interface มีบทบาทสนับสนุนให้มีรัฐภาคีสามารถพัฒนา

---

[190] The cybercrime convention committee (T-CY). Abridged meeting report of the seventh plenary, p.14

วิธีปฏิบัติหรือกฎหมายภายในให้สามารถรองรับประเด็นปัญหาใหม่ๆได้ก่อนที่จะเกิดคดีความขึ้นจริงในภายหลัง

เรื่องที่ได้รับการหารือในที่ประชุม Octopus Interface ครอบคลุมหลายประการ อาทิ เรื่องความสัมพันธ์ระหว่างรัฐและผู้ให้บริการทางอินเตอร์เน็ต ซึ่งมีความสำคัญมากในการสืบสวนคดีอาชญากรรมทางคอมพิวเตอร์ โดยในปี 2008 ทางที่ประชุมได้รับรองแนวทาง (Guidelines) เกี่ยวกับการให้ความร่วมมือระหว่างหน่วยงานผู้บังคับใช้กฎหมายและผู้ให้บริการทางอินเตอร์เน็ตในการสืบสวนอาชญากรรมทางคอมพิวเตอร์[191] ทางที่ประชุมยังเห็นว่าควรนำคำแนะนำดังกล่าวไปให้ทางคณะกรรมการอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์และรัฐอื่นๆพิจารณาด้วย[192]

นอกจากนี้ ที่ประชุม Octopus Interface ยังได้ให้ความสำคัญเกี่ยวกับการศึกษาเขตอำนาจรัฐเหนือคดีอาชญากรรมทางคอมพิวเตอร์ ในปี 2009[193] และ ปี 2010[194] ที่ประชุม Octopus Interface Conference ได้หยิบยกประเด็นปัญหา เกี่ยวกับเขตอำนาจ เขตแดนรัฐ และการบังคับใช้กฎหมาย ในบริบทของ Cloud Computing ภายใต้กรณีดังกล่าว ข้อมูลทางคอมพิวเตอร์และบริการทางคอมพิวเตอร์จะถูกเคลื่อนย้ายจากคอมพิวเตอร์ที่สามารถระบุตัว

---

[191] Octopus interface conference on cooperation against cybercrime. Conference conclusions [Online]. Strasbourg: Council of Europe, 2008. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_Interface2008/567_IF08-d-concl1c.pdf [2013, May 8])

[192] *Ibid.*

[193] Octopus interface conference on cooperation against cybercrime. Conference summary [Online]. Strasbourg: Council of Europe, 2009. Available from: http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy%20activity%20interface%202009/2079%20if09_SUMMARY1.pdf [2013, May 8], Para.7

[194] Octopus interface conference: cooperation against cybercrime. Messages from the Octopus conference [Online]. Strasbourg, Council of Europe, 2010. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy-activity-Interface-2010/2079_IF10_messages_1p%20key%20prov%20_26%20mar%2010_.pdf [2013, May 8],p.2

ได้เพียงเครื่องใดเครื่องหนึ่ง ไปยังระบบ server ที่เรียกว่า Clouds ซึ่งเป็น server จำนวนมหาศาล ที่เชื่อมต่อกันและกันและเข้าถึงได้ผ่านทางอินเตอร์เน็ต ข้อมูลถูกเก็บไว้จะไม่สามารถระบุตำแหน่งได้แน่นอน เนื่องจากข้อมูลเหล่านั้นจะเคลื่อนที่ไปมาอย่างต่อเนื่องเพื่อให้มีความพร้อมใช้สูงสุด และลดต้นทุนให้น้อยที่สุด ตัวอย่างของการใช้ Clouds ได้แก่ กล่องจดหมายอิเล็กทรอนิกส์ทางอินเตอร์เน็ตอย่าง Google mail หรือ web site ฝากข้อมูลอย่าง dropbox เป็นต้น[195]

นอกจากประเด็นสำคัญเรื่องปฏิสัมพันธ์ระหว่างรัฐและเอกชน หรือเขตอำนาจรัฐแล้ว เนื้อหาในการประชุม Octopus Interface ยังครอบคลุมการรายงานเกี่ยวกับกฎหมายอาชญากรรมทางคอมพิวเตอร์ในประเทศต่างๆ ทั้งในและนอกสภายุโรป ประเด็นด้านสิทธิส่วนบุคคล ยุทธศาสตร์ด้านอาชญากรรมทางคอมพิวเตอร์ อาชญากรรมคอมพิวเตอร์ในบางฐานความผิด เป็นต้น

ที่ประชุม Octopus Interface ได้อ้างอิงถึงและให้การสนับสนุนอนุสัญญากรุงบูดาเปสต์ในหลายโอกาสด้วยกัน โดยวัตถุประสงค์ประการหนึ่งของการประชุมในปี 2007 นั้นจะเป็นไปเพื่อส่งเสริมให้มีการใช้อนุสัญญากรุงบูดาเปสต์และพิธีสารเพิ่มเติมเป็นแนวทางในการพัฒนากฎหมายภายในประเทศ และสนับสนุนให้รัฐต่างๆ ให้สัตยาบันหรือเข้าภาคยานุวัติสนธิสัญญาเหล่านี้กันอย่างกว้างขวางและรวดเร็ว[196] หลังจากนั้นในปี 2008 ที่ประชุมให้ความเห็นว่า อนุสัญญากรุงบูดาเปสต์มีความจำเป็นและสามารถตอบสนองต่ออาชญากรรมทางคอมพิวเตอร์ใหม่ๆ ได้

---

[195] Jan Spoenle. Cloud computing and cybercrime investigations: Territoriality vs. the power of disposal? [Online]. Strasbourg: Council of Europe, Directorate general of human rights and legal affairs, economic crime division, 2010. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf [2013, May 8], p.1-2

[196] Octopus interface conference on cooperation against cybercrime. Conference summary [Online]. Strasbourg: Council of Europe, 2007. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity%20Interface2007/567%20IF%202007-d-sumconclusions1g%20Provisional.pdf [2013, May 8], p.1

อย่างครอบคลุม[197] ส่วนที่ประชุมในปี 2010 ได้ให้ความเห็นว่า อนุสัญญากรุงบูดาเปสต์ควรได้รับการจัดตั้งเป็นมาตรฐานสากลในด้านอาชญากรรมทางคอมพิวเตอร์ โดยที่มีคณะกรรมการอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์เป็นเวทีในการแบ่งปันข้อมูล กำหนดนโยบายและมาตรฐานที่เกี่ยวข้อง[198] อีกทั้งยังสามารถให้รัฐเข้ามาปรึกษาหารือและเสนอมาตรฐานประการใหม่ๆได้[199]

4.4.2.2 โครงการอาชญากรรมทางคอมพิวเตอร์สากล

โครงการอาชญากรรมทางคอมพิวเตอร์สากลนี้มีต้นกำเนิดมาจาก Octopus Interface Conference ในปี 2004 โดยมีวัตถุประสงค์เพื่อให้ อนุสัญญากรุงบูดาเปสต์และพิธีสารเพิ่มเติมถูกนำไปปรับใช้อย่างกว้างขวางโดยรัฐต่างๆ ทั่วโลก[200]

กิจกรรมของโครงการจะมุ่งเน้นไปที่การสร้างขีดความสามารถด้านต่างๆของรัฐทั้งทางด้านกฎหมายและบุคคลากรผ่านทางการประชุม การฝึกอบรม การวิเคราะห์กฎหมายภายใน และการให้ทรัพยากรสนับสนุนการดำเนินกิจกรรมต่างๆที่เกี่ยวข้อง ไม่ว่ากิจกรรมนั้นจะจัดขึ้นโดยสภายุโรปหรือองค์การอื่นๆ อีกทั้งยังจัดทำรายงานด้านอาชญากรรมทางคอมพิวเตอร์และรวบรวมข้อมูลต่างๆที่เกี่ยวข้อง ด้วย ตัวอย่างหัวข้อที่โครงการอาชญากรรมทางคอมพิวเตอร์สากลศึกษา ได้แก่ แนวโน้มทางด้านอาชญากรรมทางคอมพิวเตอร์ กฎหมายภายในด้านอาชญากรรมทางคอมพิวเตอร์ บทบาทของผู้ให้บริการทางอินเตอร์เน็ต การให้ความร่วมมือระหว่างประเทศ เขตอำนาจรัฐ เครือข่ายจุดติดต่อตลอดเวลา และการโจรกรรมตัวตน

---

[197] Octopus interface conference on cooperation against cybercrime. Conference conclusions. 2008.

[198] Octopus interface conference on cooperation against cybercrime. Messages from the Octopus conference. 2010., p.1-2

[199] *Ibid.*

[200] Project on cybercrime [Online]. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20Project/projectcyber_en.asp [2013, May 8]

ทางอินเตอร์เน็ต เป็นต้น[201] เอกสารที่ทางโครงการอาชญากรรมทางคอมพิวเตอร์สากลจัดทำนั้นจะถูกส่งไปยังคณะกรรมการอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ที่ประชุม Octopus Interface และกิจกรรมด้านอาชญากรรมทางคอมพิวเตอร์อื่นๆด้วย นอกจากนี้ โครงการอาชญากรรมทางคอมพิวเตอร์สากลยังได้จัดทำรายงานตามคำร้องขอของคณะกรรมการอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ในบางประเด็น ยกตัวอย่างเช่นกัน เรื่องเครือข่ายจุดติดต่อตลอดเวลา หรือเรื่องเขตอำนาจรัฐ เป็นต้น[202]

โครงการอาชญากรรมทางคอมพิวเตอร์สากล ขั้นที่ 1[203] มีเป้าหมายในการเพิ่มจำนวนรัฐภาคีของอนุสัญญากรุงบูดาเปสต์ และทำให้กฎหมายภายในของรัฐต่างๆสอดคล้องกับอนุสัญญามากขึ้น การเสริมสร้างขีดความสามารถของระบบยุติธรรมภายในประเทศ การให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายและจุดติดต่อต่างๆตามเครือข่ายจุดติดต่อตลอดเวลา ภายใต้อนุสัญญา โครงการในขั้นนี้ มีระยะเวลาดำเนินการตั้งแต่ วันที่ 1 กันยายน 2006 จนถึงวันที่ 28 กุมภาพันธ์ 2009 นับระยะเวลาดำเนินการทั้งสิ้น 30 เดือน

หลังจาก โครงการอาชญากรรมทางคอมพิวเตอร์สากล ขั้นที่ 1 สิ้นสุดลง โครงการขั้นที่ 2[204] ก็ถูกออกแบบขึ้นมาเพื่อดำเนินกิจกรรมต่างๆต่อไปในประเด็นที่เฉพาะเจาะจงมากยิ่งขึ้น ทั้งนี้ ในระดับภายในประเทศ โครงการอาชญากรรมทางคอมพิวเตอร์สากลขั้นที่สองมุ่งเน้นความสำคัญในการร่วมมือกันระหว่างภาครัฐและเอกชนแบะการรักษาความสมดุลระหว่างการรักษาความปลอดภัยบนอินเตอร์เน็ตและการปกป้องข้อมูลและคุ้มครองสิทธิส่วนบุคคล นอกจากนี้

---

[201] The economic crime division of the directorate general of human rights and legal affairs. Project on cybercrime: Final report [Online]. Strasbourg: Council of Europe, 2009. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20Project/567-d-final%20report1i%20final%20_15%20june%2009_.pdf [2013, May 8], p. 38

[202] *Ibid*., p.39

[203] *Ibid.*

[204] Project on cybercrime. Global project on cybercrime (phase 2) summary [Online]. Strasbourg: Council of Europe, 2011. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20Project%20global%20phase%202/2079%20adm%20pro%20summary%20_26%20Sep%202011_.pdf [2013, May 8]

โครงการยังพยายามเพิ่มขีดความสามารถของผู้พิพากษาและอัยการในการดำเนินคดีอาชญากรรมทางคอมพิวเตอร์และหลักฐานทางคอมพิวเตอร์

นอกเหนือไปจากเนื้อหาของอนุสัญญาที่มีอยู่เดิม โครงการอาชญากรรมทางคอมพิวเตอร์สากลยังพยายามศึกษาและดำเนินการต่างๆเกี่ยวกับการสืบสวนด้านการเงินผ่านทางอินเตอร์เน็ตและด้านการแสวงหาประโยชน์โดยมิชอบ และการล่วงละเมิดทางเพศต่อเด็ก และการค้ามนุษย์ผ่านทางอินเตอร์เน็ตด้วย

ในด้านความร่วมมือระหว่างประเทศ โครงการอาชญากรรมทางคอมพิวเตอร์สากลให้ความสำคัญต่อการเพิ่มขีดความสามารถของจุดติดต่อของเครือข่ายจุดติดต่อตลอดเวลาและหน่วยงานที่เกี่ยวข้องกับการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายด้วยวิธีการต่างๆ อาทิ การปรับปรุงข้อมูลของจุดติดต่อให้เป็นปัจจุบันอย่างสม่ำเสมอ และการร่วมมือกับกลุ่มย่อยด้านอาชญากรรมที่ใช้เทคโนโลยีขั้นสูงของกลุ่ม G8 เป็นต้น

กิจกรรมของ โครงการอาชญากรรมทางคอมพิวเตอร์สากลขั้นที่สองมีอยู่หลายประการ ได้แก่การวิเคราะห์และศึกษากฎหมายภายในของรัฐที่เกี่ยวข้อง การทำความเห็นทางกฎหมายและร่างกฎหมาย การให้คำปรึกษา การจัดประชุมและฝึกอบรม การจัดทำคู่มือและข้อเสนอต่างๆ การรวบรวมข้อมูลและจัดทำประวัติย่อของประเทศต่างๆในด้านอาชญากรรมทางคอมพิวเตอร์ เป็นต้น

ระยะของโครงการอาชญากรรมทางคอมพิวเตอร์สากล ขั้นที่สอง เริ่มต้นตั้งแต่วันที่ 1 มีนาคม 2009 ถึง 30 มิถุนายน 2011 รวมเป็นระยะเวลาทั้งสิ้น 28 เดือน

เนื่องด้วย ในปัจจุบัน การรวบรวมวิธีปฏิบัติของรัฐยังไม่ครอบคลุมบทบัญญัติของอนุสัญญาทุกข้อแต่อย่างใด ด้วยเหตุดังกล่าว ทางสภายุโรปจึงจัดตั้งโครงการอาชญากรรมทางคอมพิวเตอร์สากลขั้นที่ 3 ขึ้นเพื่อดำเนินการบันทึกและรวบรวมวิธีปฏิบัติต่างๆไว้แลกเปลี่ยนกันทั้งในระดับระหว่างรัฐและระหว่างภาครัฐและภาคเอกชน ทั้งนี้ ทางสภายุโรปได้มอบหมายให้ ฝ่ายการปกป้องข้อมูลและอาชญากรรมทางคอมพิวเตอร์ ของสำนักเลขาธิการด้านสิทธิมนุษยชนและนิติธรรมแห่งสภายุโรปเป็นผู้ดำเนินการร่วมกับคณะกรรมการอนุสัญญา

ว่าด้วยอาชญากรรมทางคอมพิวเตอร์ (T-CY) ภายใต้กรอบเวลาระหว่างวันที่ 1 มกราคม 2012 ถึง 31 ธันวาคม 2013[205]

นอกจากโครงการอาชญากรรมทางคอมพิวเตอร์สากลทั้งสามขั้นแล้ว สภายุโรปยังได้ดำเนินโครงการอาชญากรรมทางคอมพิวเตอร์ในระดับภูมิภาคด้วย ได้แก่ โครงการอาชญากรรมทางคอมพิวเตอร์ในรัฐจอร์เจีย[206] ซึ่งจัดขึ้นร่วมกันระหว่างหน่วยงานรัฐของประเทศจอร์เจีย คณะกรรมการยุโรป และสภายุโรป โดยเริ่มดำเนินการตั้งแต่วันที่ 1 มิถุนายน 2009 ถึง 31 พฤษภาคม 2010 โครงการอาชญากรรมทางคอมพิวเตอร์สำหรับภูมิภาคยุโรปตะวันออกเฉียงใต้ (Cybercrime@IPA)[207] โครงการความร่วมมือด้านอาชญากรรมทางคอมพิวเตอร์ในภูมิภาคยุโรปตะวันออก (Cyber@EAP)[208] เป็นต้น

---

[205] The cybercrime convention committee (T-CY). Abridged meeting report of the sixth plenary,p.21

[206] The economic crime division of the directorate general of human rights and legal affairs. Project on cybercrime in Georgia summary [Online]. Strasbourg: Council of Europe, 2009. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_project_in_georgia/2215%20adm%20pro%20summary.pdf [2013, May 8]

[207] The economic crime division of the directorate general of human rights and legal affairs. Project on regional cooperation against cybercrime in south eastern Europe (Cybercrime@IPA) : Project summary [Online]. Strasbourg: Council of Europe, 2010. Available from: http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy%20project%20balkan/2467_gen_summary_Feb2011.pdf [2013, May 8]

[208] Data protection and cybercrime division of the directorate general of human rights and legal affairs. Eastern partnership-council of Europe facility cooperation against cybercrime (Cyber@EAP): Project summary [Online]. Strasbourg, Council of Europe, 2011. Available from: http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_Project_EaP/2523_eap_cyber_summary1_%2818_June_12%29.pdf [2013, May 8]

4.5 การประเมินผลลัพธ์ของกลไกความร่วมมือทางอาญาระหว่างประเทศภายใต้กรอบอนุสัญญากรุงบูดาเปสต์

การประเมินว่าความร่วมมือทางอาญาระหว่างประเทศภายใต้กรอบอนุสัญญาบูดาเปสต์จะสามารถตอบสนองต่อปัญหาอาชญากรรมทางคอมพิวเตอร์ได้มากน้อยเพียงใดนั้น สามารถพิจารณาได้จากปัจจัยสามประการ ได้แก่ ความสอดคล้องระหว่างเนื้อหาของกลไกความร่วมมือกับบริบททางเทคโนโลยีและข้อเท็จจริง แนวทางการปรับใช้กลไกความร่วมมือโดยรัฐภาคี และแนวทางการปรับใช้กลไกความร่วมมือในระดับระหว่างประเทศ รายละเอียดเกี่ยวกับผลลัพธ์ที่ได้มีดังต่อไปนี้

4.5.1 การประเมินผลลัพธ์ความสอดคล้องระหว่างเนื้อหาของกลไกความร่วมมือกับบริบททางเทคโนโลยีและข้อเท็จจริง

กลไกความร่วมมือทางอาญาภายใต้กรอบอนุสัญญาบูดาเปสต์นั้น สามารถที่จะรองรับความซับซ้อนของอาชญากรรมทางคอมพิวเตอร์ที่ทวีขึ้นไปตามกาลเวลาได้ ดังที่กล่าวไว้แล้วท้ายบทที่ 3 อย่างไรก็ดี ความสามารถดังกล่าวนั้น เป็นผลมาจากบทบัญญัติที่มีความยืดหยุ่นขอบเขตการปรับใช้ที่กว้างขวาง อีกทั้งยังมีช่องทางสำหรับปรึกษาหารือการปรับใช้ และกลไกในการปรับปรุงแก้ไขเนื้อหาด้วย

ดังนั้น จึงจำเป็นที่จะต้องประเมินต่อไปว่า มาตรฐานร่วมกันทางกฎหมายที่อนุสัญญากรุงบูดาเปสต์และพิธีสารเพิ่มเติมได้กำหนดนั้น มีความสอดคล้องกับบริบททางเทคโนโลยีและข้อเท็จจริงด้านอื่นๆในปัจจุบันหรือไม่ ทั้งนี้ ประเด็นที่ไม่สอดคล้องกับกับบริบททางเทคโนโลยีและข้อเท็จจริงสมควรได้รับการปรับปรุงแก้ไขต่อไป

4.5.1.1 การประเมินเนื้อหาด้านกฎหมายสารบัญญัติ

อนุสัญญากรุงบูดาเปสต์นั้น ครอบคลุมการกระทำความผิดฐานสำคัญที่เกี่ยวข้องกับคอมพิวเตอร์หรือเครือข่ายอินเตอร์เน็ตได้เป็นส่วนใหญ่[209] ทั้งนี้ การที่ฐานความผิดต่างๆ ถูกกำหนดด้วยถ้อยคำที่กว้างๆไม่อ้างอิงเทคโนโลยีประเภทใดประเภทหนึ่งอย่างเฉพาะเจาะจง จึงส่งผลให้อนุสัญญามีความยืดหยุ่นต่อความผิดใหม่ๆที่อาจเกิดอีกในอนาคตได้ด้วย[210] ยกตัวอย่างเช่นในกรณีการกระทำความผิดโดยวิธี Phishing ซึ่งเป็นการหลอกลวงให้ผู้เสียหายเปิดเผยข้อมูลลับ หรือ การโจรกรรมตัวตน ความผิดทั้งสองรูปแบบนี้ ไม่ได้มีฐานความผิดกำหนดไว้ในอนุสัญญาโดยตรง แต่อนุสัญญาก็สามารถนำบทบัญญัติมาปรับใช้ได้ โดยในกรณี phishing อนุสัญญากรุงบูดาเปสต์สามารถนำข้อ 7 ว่าด้วยการปลอมแปลงทางคอมพิวเตอร์มาปรับใช้ ส่วนการโจรกรรมตัวตนนั้น จะเห็นได้ว่าบทบัญญัติของอนุสัญญาก็สามารถนำมาปรับใช้ได้กับการกระทำที่เกี่ยวข้องกับการโจรกรรมตัวตนบางประเภทได้เช่นกัน ยกตัวอย่างเช่น การเข้าสู่ระบบคอมพิวเตอร์เพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคล หรือการนำข้อมูลตัวตนที่ได้มาไปทำการฉ้อโกงที่เกี่ยวข้องกับคอมพิวเตอร์ เป็นต้น[211]

อย่างไรก็ตาม จะเห็นได้ว่า อนุสัญญาไม่ได้กำหนดรายละเอียดชัดเจนเกี่ยวกับความรับผิดของรัฐที่มีส่วนร่วมในการก่ออาชญากรรมทางคอมพิวเตอร์ ทั้งนี้ ในหลายกรณีรัฐเป็นฝ่ายสนับสนุนหรือมีส่วนร่วมในก่ออาชญากรรมทางคอมพิวเตอร์เสียเอง และจะหาข้อกล่าวอ้างต่างๆในการปฏิเสธคำขอความช่วยเหลือจากรัฐอื่นๆด้วย[212] การจำแนก

---

[209]Cormack Callanan and Marco Gercke. Cooperation between law enforcement and internet service providers against cybercrime: Towards common guidelines, p.13

[210]Council of Europe. Convention on cybercrime explanatory report[Online]. Available from: http://conventions.coe.int/Treaty/en/Reports/Html/185.htm [2013, May 6], Para. 36

[211]Cormack Callanan and Marco Gercke. Cooperation between law enforcement and internet service providers against cybercrime: Towards common guidelines, p.14-15

[212] Seymour E. Goodman, Pamela B. Hassebroek, Davis King, and Andy Ozment. International coordination to increase the security of critical network infrastructures [Online]. Seoul: International

ว่าอาชญากรรมทางคอมพิวเตอร์คดีใดบ้างที่กระทำโดยรัฐ หรือมีรัฐสนับสนุนนั้นยากลำบาก และ ผลลัพธ์ที่เกิดขึ้นกับผู้เสียหายก็อาจไม่แตกต่างกันมากนัก ปัจจัยดังกล่าวจึงส่งเสริมให้รัฐผู้เกี่ยวข้องกับการก่ออาชญากรรมคอมพิวเตอร์ไม่ยอมรับความเกี่ยวข้องของตนกับอาชญากรรม

ตัวอย่างกรณีดังกล่าวอาจเห็นได้จาก กรณีการโจมตีเครือข่ายคอมพิวเตอร์ของประเทศเอสโตเนียในปี 2007 ซึ่งมีเป้าหมายครอบคลุม web site จำนวนมากทั่วทั้งประเทศ อาทิ web site ของหน่วยงานรัฐบาล ธนาคาร หรือสำนักงานข่าว เป็นต้น เนื่องจากประเทศเอสโตเนีย นับเป็นประเทศที่เชื่อมโยงกับเครือข่ายอินเตอร์เน็ตมากที่สุดประเทศหนึ่งในทวีปยุโรป โดยจะมีการดำเนินกิจกรรมสำคัญ อาทิ บริการธนาคารซึ่งคิดเป็นสัดส่วนกว่า 90% การเลือกตั้งสมาชิกสถาผู้แทนราษฎร หรือการยื่นแบบเสียภาษีผ่านทางระบบอินเตอร์เน็ตเป็นจำนวนมาก ผลกระทบที่เกิดจากเหตุการณ์โจมตีจึงคิดเป็นมูลค่าเทียบเท่าการถูกโจมตีด้วยกองกำลังติดอาวุธจริง ทั้งนี้ ทางการประเทศเอสโตเนีย ได้สงสัยว่ารัฐบาลรัสเซียมีส่วนเกี่ยวข้องกับเหตุการณ์โจมตี เนื่องจาก ผู้ต้องสงสัยในเหตุการณ์จำนวนมากเป็นแฮ็คเกอร์ชาวรัสเซีย และการโจมตีเป็นไปอย่างเป็นระบบและกว้างขวางในระดับที่ยากจะเกิดขึ้นได้หากหน่วยงานรัฐของรัสเซียไม่ได้สนับสนุนหรือมีส่วนรู้เห็น นอกจากนี้ เมื่อประเทศเอสโตเนียได้ส่งคำขอความช่วยเหลือซึ่งกันและกันทางกฎหมายไปยังรัสเซียโดยอาศัยฐานทางกฎหมายจากสนธิสัญญาด้านการให้ความช่วยเหลือระหว่างกัน ประเทศรัสเซียกลับให้การปฏิเสธการให้ความร่วมมือ[213]

นอกจากนี้ กรณีที่รัฐมีส่วนเกี่ยวข้องกับการก่ออาชญากรรมทางคอมพิวเตอร์นั้น มีมิติทางด้านการเมืองและการทหารเข้ามาเกี่ยวข้องสูงกว่ามิติทางด้านการป้องกันอาชญากรรมทางคอมพิวเตอร์และการดำเนินกระบวนการทางอาญา เนื่องจากจะเน้นความสำคัญไปกับการปกป้องโครงสร้างพื้นฐานและความมั่นคงของรัฐ ด้วยเหตุนี้ จึงกล่าวได้ว่ากรณีที่รัฐ

---

telecommunication union workshop on creating trust in critical network structures, 2002. Available from: http://www.itu.int/osg/spu/ni/security/docs/cni.04.pdf [2013, May 8], p.25

[213] Joshua Davis, "Hackers take down the most wired country in Europe," WIRED MAGAZINE (21 August 2007). Cited in Scott Shackelford, "From nuclear war to net war: Analogizing cyber attacks in international law", Berkeley Journal of International Law 27,1 (2008):191

มีส่วนเกี่ยวข้องกับการก่ออาชญากรรมทางคอมพิวเตอร์นั้น จะเป็นประเด็นเรื่องความมั่นคงทางคอมพิวเตอร์(Cybersecurity) ซึ่งเป็นเรื่องที่แตกต่างออกไปจากอาชญากรรมทางคอมพิวเตอร์และไม่อยู่ในขอบเขตของอนุสัญญากรุงบูดาเปสต์แต่อย่างใด[214] ในขณะเดียวกัน ถึงแม้จะมีการจัดทำสนธิสัญญาด้านความมั่นคงทางคอมพิวเตอร์แยกออกมาจากอนุสัญญากรุงบูดาเปสต์ก็ตาม ก็จะยังเกิดปัญหาตามมาว่า จะมีรัฐใดบ้าง ที่ยินยอมเข้ามาเป็นภาคีและทำตามพันธะกรณีภายใต้สนธิสัญญาดังกล่าว[215]

4.5.1.2 การประเมินเนื้อหาด้านกฎหมายวิธีสบัญญัติ

อนุสัญญากรุงบูดาเปสต์ ได้พัฒนามาตรฐานด้านกฎหมายวิธีสบัญญัติ ด้วยการนำอำนาจสืบสวนคดีอาญาทั่วไปเช่น การค้นและยึด มาปรับให้กับบริบททางเทคโนโลยีคอมพิวเตอร์และกำหนดมาตรการทางเทคนิคใหม่ๆ อาทิ การเก็บรักษาข้อมูลคอมพิวเตอร์ที่ถูกเก็บไว้อย่างรวดเร็ว การเก็บรักษาและเปิดเผยข้อมูลจราจรอย่างรวดเร็ว การรวบรวมข้อมูลจราจรตามเวลาจริง และการดักรับข้อมูลทางเนื้อหา เพื่อให้เจ้าหน้าที่รัฐจึงสามารถปฏิบัติหน้าที่ได้อย่างทันต่อสถานการณ์[216] ขอบเขตของอำนาจสืบสวนเหล่านี้ ครอบคลุมไปถึงอาชญากรรมทุกประเภทที่ใช้เทคโนโลยีทางคอมพิวเตอร์เป็นเครื่องมือ และหลักฐานทางอาชญากรรมที่อยู่ในรูปแบบอิเล็กทรอนิคส์ทุกประเภท การใช้อำนาจสืบสวนเหล่านี้จึงสามารถรองรับเทคโนโลยีที่เกิดขึ้นใหม่ได้เช่นกัน

นอกจากนี้ อนุสัญญากรุงบูดาเปสต์ยังได้กำหนดกรอบทางด้านสิทธิมนุษยชนและมาตรการป้องกันไว้ในข้อ 15 บทบัญญัติดังกล่าว ย่อมรักษาสมดุลให้การดำเนินการ

---

[214] Alexander Seger, The Budapest convention on cybercrime 10 years on: Lessons learnt of the web is a web[Online]. Strasbourg: Council of Europe, 2012. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/AS_UNISPAweb_V6_16feb12.pdf [2013, May 8], p.2

[215] Jason Barkham, “Information warfare and international law on the use of force,” International Law and Politics 34,57 (2001):109-111.

[216] Council of Europe. Convention on cybercrime explanatory report Para. 134

ของฝ่ายเจ้าหน้าที่รัฐไม่ส่งผลกระทบต่อความสามารถของผู้ให้บริการทางอินเตอร์เน็ตในการให้บริการผู้ใช้บริการ หรือกระทบต่อสิทธิส่วนบุคคลต่อผู้ใช้งาน อีกทั้งยังเป็นการรับประกันว่าการดำเนินการของรัฐภาคีนั้น สอดคล้องกับมาตรฐานระหว่างประเทศ โดยเฉพาะอย่างยิ่งในด้านหลักกฎหมายเกี่ยวกับความชอบด้วยกฎหมายของวิธีพิจารณาความ หลักนิติธรรม หลักความได้สัดส่วน และหลักความจำเป็น[217]

อย่างไรก็ดี ข้อ 15 ของอนุสัญญากรุงบูดาเปสต์นั้นจะอ้างอิงถึงสนธิสัญญาด้านสิทธิมนุษยชนทั่วไป เช่น อนุสัญญาว่าด้วยการปกป้องสิทธิมนุษยชนและเสรีภาพพื้นฐานของสภายุโรป (Council of Europe Convention for the Protection of Human Rights and Fundamental Freedom) หรือกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (International Covenant on Civil and Political Rights ICCPR) หรือตราสารด้านสิทธิมนุษยชนอื่นๆ ที่มีผลบังคับใช้เท่านั้น กรอบที่อนุสัญญากรุงบูดาเปสต์กำหนดไว้อย่างกว้างๆดังข้างต้น อาจก่อให้เกิดความสับสนในการตีความว่าอนุสัญญากรุงบูดาเปสต์นั้น รองรับหลักกฎหมายเกี่ยวกับการปกป้องข้อมูลส่วนบุคคล (Data Protection)ด้วยหรือไม่

หลักกฎหมายเรื่องการปกป้องข้อมูลส่วนบุคคลนั้น จัดเป็นส่วนขยายของการปกป้องสิทธิส่วนบุคคล (Right to Privacy) ซึ่งนับเป็นสิทธิที่ได้รับการคุ้มครองตามตราสารด้านสิทธิมนุษยชนระหว่างประเทศที่สำคัญ อาทิ อนุสัญญาว่าด้วยการปกป้องสิทธิมนุษยชนและเสรีภาพพื้นฐานของสภายุโรป หรือ กติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมืองอยู่แล้ว อย่างไรก็ตาม หลักกฎหมายเรื่องการปกป้องข้อมูลส่วนบุคคล ได้ถูกพัฒนาขึ้นมาเพื่อคุ้มครองสิทธิส่วนบุคคลด้านการประมูลข้อมูลส่วนบุคคล การประมวลข้อมูล ซึ่งประกอบไปด้วยการรวบรวม จัดเก็บ ใช้งาน และสื่อสารเผยแพร่ข้อมูลนั้น จัดเป็นกิจกรรมสำคัญประการหนึ่งที่เกี่ยวข้อง

---

[217] Project on Cybercrime. Guidelines for the cooperation between law enforcement and internet providers against cybercrime[Online]. Strasbourg, Council of Europe, Directorate general of human rights and legal affairs, Economic crime division, 2008, Available from: http://www.coe.int/t/informationsociety/documents/Guidelines_cooplaw_ISP_en.pdf [2013, May 8], para.5

กับการใช้งานทางคอมพิวเตอร์และเครือข่ายอินเตอร์เน็ต และการสืบสวนอาชญากรรมทางคอมพิวเตอร์ด้วย

ในระดับระหว่างประเทศ ตัวอย่างของตราสารด้านการปกป้องข้อมูลส่วนบุคคลนั้น ได้แก่ อนุสัญญาสำหรับการปกป้องสิทธิของปัจเจกบุคคลในด้านการประมวลผลข้อมูลส่วนตัวโดยอัตโนมัติ ของสภายุโรป(the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data หรือ CETS 108) และ คำแนะนำของสภายุโรป เลขที่ R (87)15 ด้านการกำหนดกฎเกณฑ์การใช้ข้อมูลส่วนบุคคลโดยตำรวจ (Recommendation regulating the use of personal data in the police sector) เป็นต้น นอกจากนี้ รัฐบางรัฐยังมีกฎหมายภายในเกี่ยวกับการปกป้องข้อมูลส่วนบุคคลด้วย ในขณะที่รัฐบางรัฐ จะไม่มีกฎหมายภายในดังกล่าวแต่อย่างใด

ภายใต้หลักเกณฑ์เกี่ยวกับการปกป้องข้อมูลส่วนบุคคลนั้น หน่วยงานที่มีอำนาจสืบสวนอาชญากรรมจะต้องปฏิบัติตามหลักการในการค้นคว้า ใช้งาน หรือประมวลผลข้อมูลส่วนบุคคลดังต่อไปนี้[218]

- ข้อมูลส่วนบุคคลจะต้องถูกรวบรวมด้วยวิธีการที่เป็นธรรมและชอบด้วยกฎหมาย (Fair Collection Principle)
- ข้อมูลส่วนบุคคลที่ถูกรวบรวมนั้น จะต้องถูกจำกัดปริมาณเท่าที่จำเป็นต่อการบรรลุวัตถุประสงค์ของการรวบรวมข้อมูลเท่านั้น (Minimality Principle)
- การประมวลผลข้อมูลส่วนบุคคลนั้น จะต้องเป็นไปโดยสอดคล้องกับวัตถุประสงค์ดังกล่าว (Purpose Specification Principle)

---

[218] Rob van den Hoven van Genderen. Cybercrime investigation and the protection of personal data and privacy [Online]. Strasbourg, Council of Europe, Directorate general of human rights and legal affairs, Economic crime division, 2008. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/567%20study5-d-provisional.pdf [2013, May 8], p.11

- การนำข้อมูลส่วนบุคคลไปใช้นอกเหนือวัตถุประสงค์ที่ระบุไว้จะต้องได้รับความยินยอมจากผู้เป็นเจ้าของข้อมูลเสียก่อน หรือต้องกระทำไปโดยมีอำนาจตามกฎหมาย (Use limitation Principle)
- ข้อมูลส่วนบุคคลที่มีความอ่อนไหว อาทิ ข้อมูลที่เปิดเผยชาติกำเนิด ความเห็นทางการเมือง ความเชื่อทางศาสนา ข้อมูลส่วนบุคคลด้านสุขภาพหรือพฤติกรรมทางเพศ หรือข้อมูลเกี่ยวกับการรับโทษทางอาญา จะต้องไม่ถูกนำไปประมวลผลโดยอัตโนมัติ เว้นเสียแต่ว่า กฎหมายภายรัฐจะมีมาตรการคุ้มครองสิทธิที่เหมาะสมไว้
- ข้อมูลส่วนบุคคลที่ถูกนำไปประมวลผลจะต้องมีความถูกต้องแม่นยำ สมบูรณ์และเกี่ยวข้องกับวัตถุประสงค์ของการประมวลผลด้วย (Data Quality Principle)
- ข้อมูลส่วนบุคคลจะต้องได้รับการปกป้องไม่ให้ถูกเปิดเผย ทำลาย หรือถูกดัดแปลงโดยอุบัติเหตุหรือโดยไม่ได้รับอนุญาต (Security Principle)
- บุคคลที่เป็นเจ้าของข้อมูล (data subjects) ควรได้รับแจ้งเกี่ยวกับข้อมูลของตนที่ถูกประมวลผลโดยผู้อื่น อีกทั้งสามารถเข้าถึงข้อมูลเหล่านั้นได้ นอกจากนี้ในกรณีข้อมูลส่วนบุคคลมีรายละเอียดไม่ถูกต้องหรืออาจก่อให้เกิดความเข้าใจผิดได้ ผู้เป็นเจ้าของข้อมูลควรจะสามารถแก้ไขข้อมูลได้ (individual participation principle)
- ผู้มีส่วนเกี่ยวข้องในการประมวลข้อมูลนั้น จะต้องมีความรับผิดชอบในการปฏิบัติตามหลักการดังข้างต้น (accountability principle)

กลไกความร่วมมือทางอาญาภายใต้กรอบอนุสัญญากรุงบูดาเปสต์ควรจะรับรองหลักการปกป้องข้อมูลส่วนบุคคลไว้เป็นการเฉพาะเจาะจงด้วย เพื่อให้การใช้อำนาจสืบสวนอาชญากรรมทางคอมพิวเตอร์เป็นไปในแนวทางเดียวกันมากขึ้น อีกทั้งมีความสมดุลระหว่างการสืบสวนคดีและการคุ้มครองสิทธิของบุคคลผู้เกี่ยวข้องได้อย่างรัดกุมขึ้น

ความสัมพันธ์ระหว่างหน่วยงานรัฐและผู้ให้บริการทางอินเตอร์เน็ต ก็นับเป็นประเด็นปัญหาอีกประการในด้านกฎหมายวิธีสบัญญัติด้วย เพราะโดยทั่วไปแล้ว ฝ่ายเจ้าหน้าที่รัฐจะไม่ได้ดำเนินการใช้อำนาจสืบสวนอาชญากรรมทางคอมพิวเตอร์ อาทิ การรักษาข้อมูลที่ถูกกักเก็บไว้อย่างรวดเร็ว การดักรับข้อมูล ด้วยตัวเองแต่อย่างใด หากแต่จะสั่งการลงไปให้

ผู้ให้บริการทางอินเตอร์เน็ตดำเนินมาตรการเหล่านั้นแทน จากนั้นจึงติดตามผลและดำเนินการอื่นๆ ต่อจากการดำเนินการของฝ่ายผู้ให้บริการทางอินเตอร์เน็ต อย่างไรก็ตาม บทบัญญัติด้านกฎหมายวิธีสบัญญัติของอนุสัญญากรุงบูดาเปสต์นั้น กลับกล่าวเพียงว่า ฝ่ายเจ้าหน้าที่รัฐมีอำนาจสั่งการเช่นไรกับผู้ให้บริการทางอินเตอร์เน็ตเท่านั้น หากแต่ไม่ได้ระบุรายละเอียดต่อไปว่า ผู้ให้บริการทางอินเตอร์เน็ตมีหน้าที่และความรับผิดเช่นใด และในการประสานงานระหว่างทั้งสองฝ่ายนั้นจำเป็นต้องมีเงื่อนไขและกระบวนการเช่นใดบ้าง ยกตัวอย่างเช่น ในกรณีของการเก็บรักษาและเปิดเผยข้อมูลนั้น หน่วยงานผู้บังคับใช้กฎหมายจะต้องพิสูจน์ข้อเท็จจริงประการใดก่อนที่จะดำเนินการกับข้อมูลที่ตนต้องการ[219] เป็นต้น

การขาดแคลนรายละเอียดเกี่ยวกับเรื่องดังกล่าวนี้ ก่อให้เกิดอุปสรรคในการสืบสวนอาชญากรรมทางคอมพิวเตอร์ได้หลายประการด้วยกัน ถ้าหากรายละเอียดเกี่ยวกับหน้าที่และความรับผิดของผู้ให้บริการทางอินเตอร์เน็ต หรือเงื่อนไขในการให้ความร่วมมือระหว่างหน่วยงานรัฐกับผู้ให้บริการไม่ชัดเจน ฝ่ายผู้ให้บริการทางอินเตอร์เน็ตก็อาจจะไม่ให้ความร่วมมือโดยให้เหตุผลว่าเป็นการปกป้องสิทธิของผู้ใช้บริการของตนได้ เพราะฉะนั้น หน่วยงานรัฐจึงควรจัดทำกระบวนการด้านการให้ความร่วมมือกับผู้ให้บริการทางอินเตอร์เน็ตไว้เป็นลายลักษณ์อักษรแน่นอน[220] สำหรับการออกและพิจารณาคำขอความร่วมมือที่มีผลผูกพันทางกฎหมาย ทั้งนี้ กระบวนการดังกล่าวมีมาตรการด้านการตรวจสอบความถูกต้องที่เหมาะสม[221] อีกทั้งยังควรถูกจัดทำให้มีมาตรฐานเป็นไปในทิศทางเดียวกันด้วย[222]

เนื่องจากการสืบสวนอาชญากรรมทางคอมพิวเตอร์ต้องเป็นไปอย่างรวดเร็วทันสถานการณ์ หน่วยงานรัฐจึงควรที่จะจัดลำดับความสำคัญของคำขอที่ส่งไปให้ผู้ให้บริการ

---

[219] Shannon L. Hopkins, “Cybercrime convention: A positive beginning to a long road ahead” Journal of High Technology Law, 2,101: 6

[220] Project on Cybercrime. Guidelines for the cooperation between law enforcement and internet providers against cybercrime, Para.12

[221] *Ibid.*, Para.18

[222] *Ibid.* Para.26,53

ทางอินเตอร์เน็ตดำเนินการต่อไป[223] นอกจากนี้ หน่วยงานรัฐและผู้ให้บริการทางอินเตอร์เน็ตยังควรที่จะจัดตั้งจุดติดต่อไว้สำหรับติดต่อประสานงานระหว่างกัน[224] โดยเฉพาะอย่างยิ่งในกรณีที่มีความจำเป็นเร่งด่วน[225]ไว้ด้วย

ต้นทุนในการดำเนินการนั้น ก็นับเป็นประเด็นสำคัญในการให้ความร่วมมือระหว่างกันระหว่างหน่วยงานรัฐและผู้ให้บริการทางอินเตอร์เน็ตเช่นกัน ทั้งนี้ ถ้าผู้ให้บริการทางอินเตอร์เน็ตต้องแบกรับภาระมากเกินไป ธุรกิจของผู้ให้บริการก็อาจจะประสบปัญหา อีกทั้งส่งผลกระทบต่อคุณภาพของความร่วมมือที่หน่วยงานรัฐจะได้รับจากผู้ให้บริการทางอินเตอร์เน็ตด้วย[226]

เพราะฉะนั้น จึงควรที่จะมีการจัดทำเงื่อนไขและกระบวนการสำหรับการแบ่งและชดเชยค่าใช้จ่ายที่เกิดจากการสืบสวนอาชญากรรมทางคอมพิวเตอร์อย่างเป็นธรรม[227] นอกจากนี้ คำขอความร่วมมือที่หน่วยงานรัฐส่งไปยังผู้ให้บริการทางอินเตอร์เน็ตดำเนินการนั้น ควรจะระบุรายละเอียดไว้อย่างชัดเจน แม่นยำ และมีความเฉพาะเจาะจงด้วย[228]

4.5.1.3 การประเมินเนื้อหาด้านการให้ความร่วมมือระหว่างประเทศ

ในด้านการกำหนดเขตอำนาจรัฐนั้น การแก้ไขปัญหาการขัดกันของการกล่าวอ้างเขตอำนาจรัฐ (Conflict of Jurisdiction) นับว่ามีความสำคัญสำหรับอาชญากรรม

---

[223] *Ibid.*, Para. 30

[224] *Ibid*, para. 21,47,49

[225] *Ibid*,para.34,48

[226] Cormack Callanan and Marco Gercke. Cooperation between law enforcement and internet service providers against cybercrime: Towards common guidelines [Online]. Strasbourg: Council of Europe, Directorate general of human rights and legal affairs, Economic crime division, 2008. Available from http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/567%20prov-d-wg%20STUDY%20final%20_25%20june%202008_.pdf [2013, May 8], p.58

[227] Project on Cybercrime. Guidelines for the cooperation between law enforcement and internet providers against cybercrime, Para. 16

[228] *Ibid.*, Para. 27

ทางคอมพิวเตอร์มาก เพราะผู้ก่ออาชญากรรมทางคอมพิวเตอร์สามารถใช้ประโยชน์จากเครือข่ายอินเตอร์เน็ตที่เชื่อมโยงกันเพื่อสร้างผลกระทบแก่รัฐจำนวนมากได้ภายในคราวเดียวกัน นอกจากนี้การก่ออาชญากรรมทางคอมพิวเตอร์ในบางครั้งยังประกอบไปด้วยความผิดจำนวนหลายฐานในคราวเดียวกันด้วย ดังนั้น รัฐที่กล่าวอ้างเขตอำนาจรัฐเหนืออาชญากรรมทางคอมพิวเตอร์ในบางกรณีจึงอาจมีจำนวนมาก ซึ่งนำไปสู่การดำเนินที่ทับซ้อนกันระว่างหน่วยงานรัฐผู้สืบสวนอาชญากรรมทางคอมพิวเตอร์ อีกทั้งยังจะสร้างความยุ่งยากที่ไม่จำเป็นให้แก่ผู้เป็นพยานหรือผู้จัดหาหลักฐานของอาชญากรรมอีกด้วย[229]

ถึงแม้ข้อ 22 ของอนุสัญญากรุงบูดาเปสต์ จะได้กำหนดให้รัฐภาคีทำการปรึกษาหารือเพื่อหารัฐที่เหมาะสมต่อการดำเนินคดีต่อผู้กระทำผิด อย่างไรก็ตาม จะเห็นว่าแนวทางดังกล่าวนั้นต้องอาศัยความยินยอมของรัฐที่เกี่ยวข้องเป็นสำคัญ หากแต่ไม่ได้กำหนดหลักเกณฑ์ไว้แน่นอนว่า รัฐภาคีควรจะจัดลำดับความสำคัญในการกล่าวอ้างเขตอำนาจรัฐไว้อย่างใดบ้าง จึงอาจก่อให้เกิดปัญหาได้ในกรณีที่รัฐที่เกี่ยวข้องไม่ยินยอมที่จะปรึกษาหารือกันตามที่ข้อ 22 ได้กำหนดไว้

ด้วยเหตุนี้ อนุสัญญากรุงบูดาเปสต์จึงควรที่จะมีการกำหนดแนวทางสำหรับการจัดลำดับความสำคัญของเขตอำนาจรัฐให้ชัดเจนมากขึ้น โดยตัวอย่างของเกณฑ์ที่ควรนำมาใช้พิจารณาได้แก่ สถานที่ที่กระทำความผิด ลักษณะและความรุนแรงของความเสียหาย สัญชาติของผู้กระทำความผิด ความเป็นไปได้ในการที่จะดำเนินคดีไปได้อย่างลุล่วง หรือคุณภาพของกฎหมายวิธีพิจารณาความอาญาและการปกป้องสิทธิมนุษยชน เป็นต้น[230] โดยจะเห็นได้ว่าเกณฑ์บางข้อนั้นมีน้ำหนักมากกว่าเกณฑ์ประการอื่น ยกตัวอย่างเช่น รัฐที่ความเสียหายเกิดขึ้น มีเขตอำนาจที่ดีกว่า

---

[229] Henrik W.K. Kaspersen, Cybercrime and internet jurisdiction [Online]. Strasbourg: Council of Europe, Directorate general of human rights and legal affairs, Economic crime division, 2009. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/2079repInternetJurisdictionrik1a%20_Mar09.pdf [2013, May 7], Para.10

[230] *Ibid*.,Para.62-65

รัฐที่การกระทำผิดเกิดขึ้น[231] ในขณะเดียวกัน รัฐเจ้าของสัญชาติผู้เสียหาย ควรมีน้ำหนักน้อยในการกล่าวอ้างเขตอำนาจในกรณีที่อาชญากรรมทางคอมพิวเตอร์ไม่ได้มุ่งเป้าหมายไปยังคนชาติใดชาติหนึ่งชัดเจน[232]

การที่อนุสัญญานั้นยังอาศัยหลักดินแดนเป็นสำคัญนั้น ยังก่อให้เกิดอุปสรรคใน การติดตามจับกุมอาชญากรที่ใช้ clouds และแสวงหาหลักฐานอิเล็กทรอนิกส์จากการกระทำความผิดได้ด้วย ภายใต้การใช้งานคอมพิวเตอร์ภายใต้ระบบ Cloud (Cloud Computing) นั้น ข้อมูลทางคอมพิวเตอร์จะไม่ถูกกักเก็บไว้ใน server คอมพิวเตอร์เพียงเครื่องใดเครื่องหนึ่ง ดังเช่นในอดีต เพราะระบบ Cloud จะประกอบไปด้วย server computer จำนวนมากที่กระจายกันไปทั่วโลก ส่วนข้อมูลที่อยู่ในระบบนั้นจะเคลื่อนที่ไปมาระหว่าง server ที่อยู่ภายในเขตอำนาจของรัฐต่างๆ

นอกจากนี้ เพื่อความปลอดภัยและรับรองความพร้อมใช้งานของของข้อมูลเหล่านี้ ข้อมูลจะถูกจัดทำสำเนาเพื่อสำรองไว้ใน server ต่างๆด้วย ส่งผลให้ข้อมูลดังกล่าวตกอยู่ภายใต้เขตอำนาจรัฐมากกว่าหนึ่งรัฐในระยะเวลาเดียวกัน ส่วนข้อมูลบางประเภทก็จะถูกแยกส่วนเก็บไว้ตาม server แหล่งต่างๆ และถูกนำมารวมกันใหม่อีกครั้งเมื่อมีถูกเรียกใช้งาน เพราะฉะนั้นจะเห็นได้ว่า ภายใต้บริบทของ Cloud Computing นั้น ที่ตั้งของข้อมูลไม่มีความแน่นอนแต่อย่างใด การนำหลักเกณฑ์ดั้งเดิมมาปรับใช้จึงเกิดอุปสรรคได้[233]

นอกจากนี้ การเข้าถึงข้อมูลข้ามแดนภายใต้ ข้อ 32 b ของอนุสัญญากรุงบูดาเปสต์จะต้องทราบตำแหน่งที่ตั้งของข้อมูลอย่างแน่นอน ทั้งนี้จะสังเกตได้จากถ้อยคำของบทบัญญัติ

---

[231] Shannon L. Hopkins, “Cybercrime convention: A positive beginning to a long road ahead” Journal of High Technology Law, 2,101 (2003): 8

232 Henrik W.K. Kaspersen, Cybercrime and internet jurisdiction, Para.64

[233] Ad-hoc sub-group on jurisdiction and transborder access to data. Transborder access and jurisdiction: What are the options? Para.35-38

ที่ว่า ข้อมูลที่ถูกเก็บไว้ในดินแดนรัฐภาคีอื่น ดังนั้นมาตรการดังข้างต้นจึงไม่สามารถนำมาใช้กับบริบทของ Cloud Computing ซึ่งไม่อาจระบุตำแหน่งของข้อมูลได้แน่นอนเช่นเดียวกัน[234]

ในการพัฒนากฎเกณฑ์ใหม่เพื่อรองรับการใช้ระบบ Cloud นั้น ได้มีการเสนอให้ใช้อำนาจในการจัดการข้อมูล (Power of Disposal) เป็นเกณฑ์พิจารณาจุดเกาะเกี่ยวแทน หลักเกณฑ์ดังกล่าวนี้ จะพิจารณาจากบุคคลผู้มีอำนาจจัดการข้อมูลเป็นสำคัญ โดยตัวอย่างของการใช้อำนาจจัดการข้อมูลนี้ ได้แก่ การดัดแปลง ลบ ระงับยับยั้ง ทำให้ข้อมูลใช้การไม่ได้ หรือป้องกันไม่ให้บุคคลอื่นสามารถเข้าถึงข้อมูลได้ เป็นต้น ทั้งนี้ จะเห็นได้ว่า บุคคลผู้มีอำนาจจัดการข้อมูลจะยังคงอยู่ในดินแดนของรัฐใดรัฐหนึ่ง และถือสัญชาติของรัฐใดรัฐหนึ่ง ซึ่งต่างจากข้อมูลที่ไม่สามารถระบุตำแหน่งได้แน่นอน[235]

ตัวอย่างการใช้เกณฑ์อำนาจการจัดการนั้น จะเห็นได้จากในกรณีของสหรัฐอเมริกา ถ้าผู้ให้บริการระบบคอมพิวเตอร์ Cloud อยู่ภายใต้เขตอำนาจสหรัฐอเมริกา หน่วยงานผู้บังคับใช้กฎหมายจะมีอำนาจขอข้อมูลจากผู้ให้บริการรายนั้นได้โดยไม่ต้องพิจารณาว่าข้อมูลนั้นมีตำแหน่งที่ตั้งอยู่ที่ดินแดนของรัฐใด[236] ทั้งนี้ ควรกำหนดเงื่อนไขและมาตรการป้องกันที่เกี่ยวข้องเพิ่มเติมด้วย[237] ตัวอย่างของเงื่อนไขและมาตรการป้องกันเหล่านี้ได้แก่ การกำหนดขอบเขตให้ปรับใช้วิธีการดังกล่าวได้เฉพาะกรณีฉุกเฉินที่หลักฐานทางอิเล็กทรอนิกส์เสี่ยงต่อการถูกทำลาย การกำหนดให้การดำเนินการเช่นว่านั้นต้องอาศัยคำสั่งศาล การกำหนดหน้าที่ให้หน่วยงานรัฐแจ้งไปยังบุคคลที่เกี่ยวข้อง อาทิ เจ้าของบัญชีและผู้ให้บริการทางอินเตอร์เน็ต เว้นเสียแต่ในกรณีที่ผลลัพธ์ของการสืบสวนอาจจะได้รับผลกระทบต่อการแจ้งนั้น หรือ การระบุอย่างชัดเจนว่าข้อมูลที่ต้องการนั้นถูกยึดมาแล้ว และจะถูกลบทิ้งไปภายในระยะเวลาที่กำหนด[238]

---

[234] *Ibid*., p.21,50

[235] *Ibid*.,p.50

[236] *Ibid.*

[237] Jan Spoenle. Cloud computing and cybercrime investigations: Territoriality vs. the power of disposal?, p.10-12

[238] *Ibid.,* p. 12

แนวทางอีกประการหนึ่งในการเข้าถึงข้อมูลข้ามแดนภายใต้บริบทของการขยายอำนาจการค้นและยึด ดังที่จะเห็นได้จากแนวปฏิบัติของประเทศเบลเยียม โดยกฎหมายวิธีพิจารณาความอาญาจะอนุญาตให้ผู้พิพากษาสืบสวน (Investigating Judge) ซึ่งหน้าที่และอำนาจในการสืบสวนตามกฎหมายนั้น สามารถออกคำสั่งค้นข้อมูลภายในระบบคอมพิวเตอร์ได้ โดยการค้นข้อมูลดังกล่าวอาจจะถูกสั่งให้ขยายไปยัง ระบบคอมพิวเตอร์อื่นหรือส่วนใดส่วนหนึ่งของระบบคอมพิวเตอร์อื่นที่สามารถเข้าถึงได้โดยผู้ใช้ระบบคอมพิวเตอร์แรกที่ถูกค้นได้ ทั้งนี้ผู้ดำเนินค้นไม่ต้องคำนึงว่าว่าระบบอื่นนั้นจะอยู่ภายในดินแดนไหน โดยในกรณีที่ข้อมูลที่ถูกค้นไม่ได้อยู่ภายในดินแดนประเทศเบลเยียมนั้น ให้ผู้สืบสวนทำสำเนาข้อมูลไว้ หลังจากนั้นผู้พิพากษาสืบสวนจะดำเนินการแจ้งเรื่องไปยังกระทรวงการยุติธรรม ซึ่งจะส่งเรื่องไปยังรัฐอื่นต่อไป การขยายของเขตการค้นดังกล่าวนั้นจะมีได้ในกรณีที่มีความจำเป็นซึ่งมาตรการอื่นใช้ไม่ได้ผลหรือมีความเสี่ยงโดยชัดเจนว่าหลักฐานจะสูญหาย[239]

วิธีปฏิบัตินี้ดังกล่าวสามารถรองรับกรณีของการใช้คอมพิวเตอร์ระบบ Cloud ได้เพราะรัฐสามารถดำเนินการโดยไม่ต้องพิจารณาว่าข้อมูลอยู่ที่ไหน เพราะอาศัยการพิจารณาตำแหน่งที่สามารถเข้าถึงข้อมูลได้แทน[240] นอกจากประเทศเบลเยียมแล้ว ประเทศโปรตุเกส ฝรั่งเศส สหราชอาณาจักร และเดนมาร์ก ก็มีวิธีปฏิบัติทำนองเดียวกัน[241]

การขยายอำนาจการค้นดังข้างต้นนั้น มีความคล้ายคลึงกับ ข้อ 19 วรรค 2 ของอนุสัญญาที่อนุญาตให้ฝ่ายเจ้าหน้าที่รัฐสามารถขยายอำนาจการค้นหรือการเข้าถึงไปยังระบบคอมพิวเตอร์อื่น หากวินิจฉัยพบว่าข้อมูลที่เสาะหาอยู่นั้นอยู่ภายในระบบคอมพิวเตอร์อื่นซึ่งสามารถเข้าถึงได้โดยถูกต้องตามกฎหมายจากระบบที่ตนกำลังตรวจค้นอยู่ อย่างไรก็ตาม การขยายอำนาจการค้นตามอนุสัญญากรุงบูดาเปสต์จะจำกัดอยู่เฉพาะภายในดินแดนรัฐเดียวกันเท่านั้น

---

[239] Ad-hoc sub-group on jurisdiction and transborder access to data. Transborder access and jurisdiction: What are the options?, Para. 163-164

[240] *Ibid*., p.33

[241] *Ibid*.,p.47-48

4.5.2 การประเมินผลลัพธ์จากการปรับใช้โดยรัฐภาคี

การปรับใช้อนุสัญญากรุงบูดาเปสต์ระดับภายในประเทศจะแบ่งออกเป็นสามส่วน โดยในส่วนแรกรัฐภาคีหรือรัฐผู้ลงนามในอนุสัญญาจะปรับใช้อนุสัญญาผ่านกฎหมายภายในของตน ซึ่งแบ่งออกได้เป็นกฎหมายสารบัญญัติ กฎหมายวิธีสบัญญัติ และกฎหมายเกี่ยวกับการให้ความร่วมมือทางอาญาระหว่างประเทศ

สำหรับการปรับใช้อนุสัญญาระดับภายในประเทศส่วนที่สองนั้น รัฐภาคีหรือรัฐผู้ลงนามจะมอบหมายให้หน่วยงานต่างๆของตนทำหน้าที่ให้ความร่วมมือทางอาญาตามที่อนุสัญญากรุงบูดาเปสต์กำหนดไว้ ไม่ว่าจะเป็นหน่วยงานสำหรับการรับส่งคำร้องขอส่งตัวผู้ร้ายข้ามแดนหรือการช่วยเหลือซึ่งกันและกันทางกฎหมาย หน่วยงานผู้พิจารณาและจัดการตามคำขอหรือหน่วยงานที่ทำหน้าที่เป็นจุดติดต่อในเครือข่ายจุดติดต่อตลอดเวลา ตามข้อ 35 ของอนุสัญญาเป็นต้น

ท้ายที่สุดการปรับใช้อนุสัญญาระดับภายในประเทศส่วนที่สาม จะเป็นแนวปฏิบัติของรัฐในการตีความอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์และปรับใช้อนุสัญญากับคดีอาชญากรรมทางคอมพิวเตอร์ที่เกิดขึ้น ซึ่งสะท้อนให้เห็นได้จากคดีต่างๆ และวิธีปฏิบัติของหน่วยงานรัฐผู้มีอำนาจเกี่ยวข้อง ข้อมูลเหล่านี้จะค้นหาอ้างอิงได้ยากกว่ากฎหมายที่บัญญัติไว้แน่นอน

การประเมินแนวทางการปรับใช้กลไกความร่วมมือทางอาญาภายใต้กรอบอนุสัญญากรุงบูดาเปสต์โดยรัฐภาคีนั้น สามารถกระทำด้วยโดยการพิจารณาว่า รัฐภาคีของอนุสัญญามีอำนาจตามกฎหมายในการปฏิบัติตามมาตรการของอนุสัญญาได้มากน้อยเพียงใด และได้มีการใช้งานโดยแท้จริงมากน้อยเท่าไรบ้าง[242]

---

[242] The cybercrime convention committee (T-CY). Assessment report: Implementation of the preservation provisions of the Budapest convention on cybercrime,p.7

เมื่อพิจารณาอำนาจตามกฎหมายของรัฐภาคีในการปฏิบัติตามอนุสัญญาแล้ว จะแบ่งประเภทของรัฐออกได้เป็นสามประเภท โดยรัฐกลุ่มแรกนั้น จะเรียกว่าเป็นรัฐที่ปฏิบัติตามอนุสัญญาได้อย่างสอดคล้อง (in line) เพราะจะจัดทำกฎหมายเฉพาะขึ้นมารองรับอนุสัญญากรุงบูดาเปสต์โดยตรง จึงสามารถรับรองถึงการปฏิบัติติตามเนื้อหาอนุสัญญากรุงบูดาเปสต์ได้อย่างชัดเจน เพราะเนื้อหาของกฎหมายเฉพาะย่อมปรากฏออกมาเป็นลายลักษณ์อักษรแน่นอน สามารถตรวจสอบและอ้างอิงโดยรัฐภาคีอื่นๆได้สะดวก

รัฐกลุ่มที่สองจะเป็นรัฐที่มีอำนาจตามกฎหมายในลักษณะที่สอดคล้องบางส่วน (partially in line) กับอนุสัญญากรุงบูดาเปสต์ รัฐกลุ่มนี้จะเลือกปรับใช้กฎหมายที่มีอยู่แล้วแทนการจัดทำกฎหมายขึ้นมาใหม่ โดยจะอ้างอิงบทบัญญัติเกี่ยวกับอำนาจการสืบสวนทั่วไปมาตีความให้ครอบคลุมบทบัญญัติของอนุสัญญากรุงบูดาเปสต์ ยกตัวอย่างเช่น การนำบทบัญญัติเรื่องการค้นและยึด มาตีความให้ครอบคลุมกรณีการเก็บรักษาข้อมูลอย่างรวดเร็ว เป็นต้น แนวปฏิบัติของรัฐกลุ่มนี้จะยังคงสอดคล้องกับอนุสัญญาอยู่ ตราบใดที่รัฐเหล่านั้น สามารถดำเนินการตามบทบัญญัติของอนุสัญญาได้จริง ทั้งนี้ต้องอาศัยการพิจารณาจากรูปแบบคดีต่างๆ และวิธีปฏิบัติของหน่วยงานรัฐผู้มีอำนาจเกี่ยวข้อง ซึ่งค้นหาอ้างอิงได้ยากกว่ากฎหมายที่บัญญัติไว้แน่นอน

รัฐกลุ่มที่สามจะเป็นรัฐที่ไม่ได้เปลี่ยนแปลงกฎหมายภายในของตัวเองเช่นเดียวกับกลุ่มที่สอง และไม่สามารถกระทำการตามตามบทบัญญัติของอนุสัญญาได้ เรียกว่าเป็นกลุ่มที่ไม่สอดคล้องกับอนุสัญญา (not in line)

นอกจากรัฐสามกลุ่มที่ได้กล่าวมาข้างต้นแล้ว รัฐบางส่วนจะมีอำนาจด้านการสืบสวนอาชญากรรมทางคอมพิวเตอร์ที่อนุสัญญากรุงบูดาเปสต์ไม่ได้ระบุไว้ เช่น การใช้วิธีการกักข้อมูล (data retention) และการเข้าถึงข้อมูลข้ามแดนด้วยวิธีการที่ข้อ 32 ของอนุสัญญาไม่ได้กล่าวถึงไว้เป็นต้น

ความแตกต่างของแนวทางการบัญญัติกฎหมายดังข้างต้นนี้ ส่วนหนึ่งเป็นผลมาจากการที่รัฐบางส่วนยังจัดทำกฎหมายด้านอาชญากรรมทางคอมพิวเตอร์ขึ้นมาใหม่ได้ไม่เสร็จสิ้น

แต่รัฐอีกกลุ่มจะเห็นว่าการปรับใช้กฎหมายเดิมที่มีอยู่แล้ว สามารถช่วยประหยัดเวลาและค่าใช้จ่ายในการจัดทำกฎหมายใหม่ขึ้นมาเป็นการเฉพาะได้ แนวคิดด้านเทคนิคในการจัดทำกฎหมายที่แตกต่างกันออกไปนี้ นับเป็นสิ่งที่อนุสัญญากรุงบูดาเปสต์ไม่สามารถเข้ามาแทรกแซงให้สอดคล้องกันได้แต่อย่างใด[243]

สำหรับการใช้งานจริงนั้น ปัญหาที่เกิดขึ้นก็คือ รัฐภาคีบางส่วนไม่ได้ใช้งานบทบัญญัติของอนุสัญญากรุงบูดาเปสต์ในการสืบสวนอาชญากรรมทางคอมพิวเตอร์และการให้ความร่วมมือทางอาญาระหว่างประเทศมากนัก นอกเหนือจากแนวคิดที่แตกต่างออกไปจองแต่ละรัฐแล้ว ปัจจัยหนึ่งที่ก่อให้เกิดปัญหาดังกล่าวคือการที่รัฐบางส่วนไม่ได้บัญญัติกฎหมายที่มีเนื้อหาสอดคล้องกับอนุสัญญากรุงบูดาเปสต์โดยตรง หากแต่อาศัยการปรับใช้หลักกฎหมายที่มีอยู่เดิมแทน ซึ่งดำเนินการได้ไม่สะดวกนัก

นอกจากนี้ การไม่ใช้งานบทบัญญัติของอนุสัญญากรุงบูดาเปสต์ยังเป็นผลมาจากการที่เจ้าหน้าที่รัฐขาดประสบการณ์ในเรื่องที่เกี่ยวข้อง ยกตัวอย่างเช่น ในกรณีของการดักรับข้อมูลทางคอมพิวเตอร์หรือกรณีของเครือข่ายจุดติดต่อตลอดเวลา เป็นต้น

4.5.3 การประเมินผลลัพธ์จากการปรับใช้ในระดับระหว่างประเทศ

การปรับใช้กลไกความร่วมมือกรอบอนุสัญญากรุงบูดาเปสต์ในระดับระหว่างประเทศนั้น มีประโยชน์อยู่หลายประการด้วยกัน

โดยบทบาทประการแรกของการปรับใช้อนุสัญญาในระดับระหว่างประเทศนั้นคือการเพิ่มองค์ความรู้ด้านอาชญากรรมทางคอมพิวเตอร์ให้แก่รัฐมากขึ้นด้วยกิจกรรมหลายรูปแบบ ไม่ว่าจะเป็นการรวบรวมข้อมูลเกี่ยวกับกฎหมายด้านอาชญากรรมทางคอมพิวเตอร์ของรัฐ การจัดทำรายงานเกี่ยวกับประเด็นปัญหาด้านอาชญากรรมทางคอมพิวเตอร์ หรือการแลกเปลี่ยนข้อมูลและข้อคิดเห็นในที่ประชุม เป็นต้น ด้วยองค์ความรู้เหล่านี้ รัฐจะสามารถระบุถึงประเด็นปัญหาใหม่ๆที่เกิดจากอาชญากรรมทางคอมพิวเตอร์ และทราบแนวทางการปรับใช้อนุสัญญา

---

[243] Henrik Kaspersen, Joseph Schwerha, and Drazen Dragizevic. Article 15: conditions and safeguards under the Budapest convention on cybercrime, p.16

กรุงบูดาเปสต์ได้อย่างชัดเจนมากขึ้น ในขณะเดียวกัน ความรู้ความเข้าใจเกี่ยวกับกฎหมายภายในของประเทศต่างๆ ย่อมส่งผลให้รัฐบางส่วนสามารถพัฒนากฎหมายด้านอาชญากรรมทางคอมพิวเตอร์ของตนให้มีประสิทธิภาพมากขึ้น อีกทั้งสามารถคิดหาวิธีดำเนินการขอความช่วยเหลือซึ่งกันและกันทางกฎหมายจากอีกฝ่ายได้อย่างเหมาะสม

ทั้งนี้ บันทึกแนวทางการตีความ (Guidance Note) ของคณะกรรมการอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์นับว่า มีบทบาทในการทำให้รัฐมีแนวทางการปฏิบัติตามอนุสัญญากรุงบูดาเปสต์ไปในทิศทางเดียวกันมากขึ้น ทั้งในด้านการตีความบทบัญญัติของอนุสัญญาและการปรับใช้อนุสัญญากับปัญหาข้อเท็จจริง

บทบาทประการต่อมาของการปรับใช้อนุสัญญาในระดับระหว่างประเทศก็คือการส่งเสริมขีดความสามารถให้แก่บุคลากรของรัฐที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์ ยกตัวอย่างเช่น โครงการอาชญากรรมทางคอมพิวเตอร์สากลนั้น ได้ดำเนินการฝึกอบรมบุคลากรต่างๆ ที่เกี่ยวข้อง ได้แก่เจ้าหน้าที่ตำรวจ ผู้พิพากษา หรืออัยการ มาอย่างสม่ำเสมอระหว่างดำเนินโครงการ การให้ความช่วยเหลือทางเทคโนโลยีและการแบ่งปันทรัพยากรนี้ จึงจำเป็นอย่างมากที่จะทำให้รัฐที่ด้อยพัฒนาสามารถดำเนินการตามคำร้องขอความช่วยเหลือทางกฎหมายของรัฐอื่นๆได้[244]

การปรับใช้อนุสัญญาในระดับระหว่างประเทศสามารถเพิ่มจำนวนรัฐที่เข้ามาเป็นภาคีอนุสัญญากรุงบูดาเปสต์ให้มากขึ้นอีกด้วย ดังที่จะเห็นได้จากโครงการอาชญากรรมทางคอมพิวเตอร์สากล ที่มีวัตถุประสงค์ในการส่งเสริมให้อนุสัญญากรุงบูดาเปสต์และพิธีสารเพิ่มเติมได้รับการปฏิบัติตามอย่างกว้างขวางขึ้น ทั้งนี้ ในปัจจุบัน อนุสัญญากรุงบูดาเปสต์มีรัฐภาคีเป็นจำนวน 39 รัฐ และรัฐผู้ลงนามแต่ยังไม่ได้ให้สัตยาบันเป็นจำนวน 12 รัฐ ในจำนวนเหล่านี้ มีรัฐนอกสภายุโรปที่เข้าเป็นภาคีอนุสัญญาแล้ว 4 รัฐ ได้แก่ ออสเตรเลีย สาธารณรัฐโดมินิกัน ญี่ปุ่น และสหรัฐอเมริกา ส่วนรัฐนอกสภายุโรปที่ลงนามแล้วแต่ยังไม่ได้ให้สัตยาบันได้แก่ แคนาดา และแอฟริกาใต้[245] ในขณะเดียวกัน รัฐที่ไม่ได้เป็นภาคีอนุสัญญา

---

[244] Seymour E. Goodman, Pamela B. Hassebroek, Davis King, and Andy Ozment. International coordination to increase the security of critical network infrastructures, p.26

[245] Convention on cybercrime CETS No. 185, Status as of 6/5/2013 [Online],

จำนวนมากยังได้อาศัยอนุสัญญากรุงบูดาเปสต์ไปเป็นแบบในการจัดทำกฎหมายภายในของตนด้วย สิ่งเหล่านี้ย่อมสะท้อนให้เห็นว่า กลไกความร่วมมือทางอาญาระหว่างประเทศภายใต้กรอบอนุสัญญากรุงบูดาเปสต์นั้นได้รับการยอมรับอย่างกว้างขวางขึ้นในประชาคมโลก

อย่างไรก็ดี การปรับใช้อนุสัญญาในระดับระหว่างประเทศยังมีข้อจำกัดอยู่เช่นกัน เพราะกิจกรรมเหล่านี้ขาดปราศจากผลผูกพันทางกฎหมายระหว่างประเทศ รัฐจึงไม่มีพันธะกรณีที่จำต้องดำเนินการตามแต่อย่างใด นอกจากนี้ กิจกรรมสำคัญบางประการ เช่น การประเมินการปรับใช้บทบัญญัติอนุสัญญากรุงบูดาเปสต์ หรือบันทึกแนวทางการตีความ ซึ่งจัดทำโดยคณะกรรมการอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ (T-CY) นั้น ต้องใช้เวลานานในการจัดทำเพื่อให้ครอบคลุมบทบัญญัติทุกบทของอนุสัญญากรุงบูดาเปสต์

ในขณะเดียวกัน รัฐที่เข้ามามีส่วนร่วมในอนุสัญญาทั้งในรูปแบบการลงนามและการเข้าเป็นภาคี ก็ไม่ได้เป็นประเทศที่เป็นแหล่งกำเนิดของอาชญากรรมทางคอมพิวเตอร์[246] ส่งผลให้ผู้กระทำผิดยังคงสามารถหลบหนีไปยังประเทศที่ยังไม่มีความพร้อมทางกฎหมายหรือไม่ให้ความร่วมมือด้านอาชญากรรมทางคอมพิวเตอร์บางแห่งได้[247] ตัวอย่างของประเทศที่เป็นแหล่งของอาชญากรรมทางคอมพิวเตอร์ได้แก่ จีน บราซิล และรัสเซียซึ่งไม่ได้เป็นสมาชิกของสภายุโรป โดยเฉพาะในกรณีของประเทศรัสเซียนั้น เป็นที่กล่าวกันว่า อาชญากรทางคอมพิวเตอร์ชาวรัสเซียนั้นอยู่เบื้องหลังอาชญากรรมทางคอมพิวเตอร์หลายประเภท อีกทั้งยังมี

Available from: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG [2013, May 6]

[246] Dan Robel. International cybercrime treaty: Looking beyond ratification[Online]. Bethesda: SANS Institute, 2007. Available from: http://www.sans.org/reading_room/whitepapers/honors/international-cybercrime-treaty-ratification_1756 [2013, May 8], p.26

[247] Kristine Archik. Cybercrime: The council of Europe convention [Online]. United States: The library of congress, congressional research service, 2002. Available from: http://eee.iwar.org.uk/news-archive/crs/10088.pdf [2013, May 8]

เครือข่ายที่กว้างขวางและมีองค์กรอาชญากรรมสนับสนุนอยู่เบื้องหลังด้วย[248] นอกจากนี้ รัฐบางส่วนยังไม่เห็นด้วยกับการเข้าเป็นภาคีอนุสัญญาเนื่องจากเห็นว่าตนไม่ได้เข้าร่วมในการเจรจาจัดทำอนุสัญญา อีกทั้งองค์การระหว่างประเทศที่จัดทำไม่ใช่สหประชาชาติด้วย[249] ส่วนรัฐบางส่วนก็มีความล่าช้าในการเข้าเป็นภาคีเพราะผู้มีอำนาจตัดสินใจในรัฐบางรัฐไม่ได้ให้ความสนใจในด้านอาชญากรรมทางคอมพิวเตอร์[250]

4.6 แนวทางตอบสนองต่ออุปสรรคของกลไกความร่วมมือทางอาญาระหว่างประเทศภายใต้กรอบอนุสัญญากรุงบูดาเปสต์

เมื่อประเมินผลลัพธ์ของกลไกความร่วมมือทางอาญาภายใต้กรอบอนุสัญญากรุงบูดาเปสต์แล้ว จะพบว่ากลไกความร่วมมือยังขาดรายละเอียดบางประการ ซึ่งนั่นเป็นปัจจัยสำคัญที่ก่อให้เกิดอุปสรรคขึ้น โดยบทบัญญัติบางส่วนนั้น ยังขาดความสอดคล้องกับพัฒนาการทางเทคโนโลยีที่เกิดขึ้นหลังการจัดทำอนุสัญญา ยกตัวอย่างเช่น กรณีของการเข้าถึงข้อมูลข้ามแดนตามข้อ 32b กับระบบคอมพิวเตอร์ cloud เป็นต้น ในขณะบทบัญญัติบางส่วนนั้นจะวางกรอบเนื้อหาไว้กว้างเกินไปทั้งที่มีความสำคัญต่อการสืบสวนอาชญากรรมทางคอมพิวเตอร์และการให้ความร่วมมือซึ่งกันและกันทางกฎหมาย ยกตัวอย่างเช่น บทบัญญัติเรื่องเงื่อนไขและมาตรการป้องกันในข้อ 15 ของอนุสัญญา หรือเนื้อหาเกี่ยวกับความร่วมมือกันระหว่างหน่วยงานรัฐและผู้ให้บริการทางอินเตอร์เน็ต เป็นต้น นอกจากนี้ ความคลุมเครือของบทบัญญัติดังกล่าว สามารถส่งผลให้แนวทางการปรับใช้อนุสัญญากรุงบูดาเปสต์ดำเนินไปโดยไม่สอดคล้องกันได้ ในขณะเดียวกัน การที่บทบัญญัติบางส่วนของอนุสัญญาขาดรายละเอียดยังส่งผลให้ เจ้าหน้าที่รัฐภาคีลังเลที่จะใช้มาตรการตามอนุสัญญาในการให้ความช่วยเหลือจริงได้เช่นกัน ดังที่จะเห็นได้จากกรณีการให้ความช่วยเหลือด้วยการดักรับข้อมูลทางคอมพิวเตอร์หรือการใช้เครือข่ายจุดติดต่อตลอดเวลา เป็นต้น

---

[248] Dan Robel. International cybercrime treaty: Looking beyond ratification, p.31

[249] Alexander Seger, The Budapest convention on cybercrime 10 years on: Lessons learnt of the web is a web , p.5

[250] *Ibid*.,p.12

ด้วยเหตุนี้ การเพิ่มเติมรายละเอียดของเนื้อหากลไกความร่วมมือกรอบอนุสัญญากรุงบูดาเปสต์ จึงมีความสำคัญต่อการตอบสนองอุปสรรคที่เกิดขึ้นจากกลไกความร่วมมือในการนี้ จะพบว่ามีแนวทางในการดำเนินการอยู่หลายรูปแบบด้วยกัน ดังต่อไปนี้

ในเบื้องต้น การปรับใช้อนุสัญญากรุงบูดาเปสต์ในระดับระหว่างประเทศนั้น สามารถช่วยให้การปรับใช้อนุสัญญาในระดับภายในรัฐเป็นไปอย่างมีประสิทธิภาพมากขึ้นได้ โดยการแลกเปลี่ยนความคิดเห็นในกิจกรรมการประชุม Octopus Interface Conference หรือการประชุมคณะกรรมการอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ จะมีบทบาทในการระบุประเด็นปัญหา ทั้งที่เกิดจากการปรับใช้อนุสัญญาโดยทั่วไป และที่เกิดจากความเปลี่ยนแปลงทางเทคโนโลยีได้ อีกทั้งยังเป็นสถานที่นำเสนอประเด็นเกี่ยวกับเนื้อหาของกลไกความร่วมมือที่สมควรได้รับการเพิ่มเติมแก้ไขด้วย

ส่วนกิจกรรมของโครงการอาชญากรรมทางคอมพิวเตอร์สากล อาทิ การจัดทำรายงานศึกษาประเด็นต่างๆ ด้านอาชญากรรมทางคอมพิวเตอร์ นั้น ก็จะเป็นการรวบรวมข้อมูลเกี่ยวกับประเด็นปัญหาให้มีรายละเอียดมากขึ้น นอกจากนี้ การจัดทำรายงานประเมินการปรับใช้อนุสัญญาของคณะกรรมการอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์นั้น จะสามารถระบุปัญหาจากการปรับใช้อนุสัญญาได้ในอีกทางหนึ่งเช่นกัน อีกทั้งยังเป็นการแลกเปลี่ยนข้อมูลเกี่ยวกับกฎหมายภายในและแนวปฏิบัติทางอาชญากรรมทางคอมพิวเตอร์ของรัฐภาคีอีกด้วย

หลังจากนั้น หากเนื้อหาของกลไกความร่วมมือในส่วนที่ต้องการแก้ไขเพิ่มเติมเป็นการเพิ่มเติมรายละเอียดในการตีความบทบัญญัติที่มีอยู่แล้วของอนุสัญญา การจัดทำแนวทางการตีความ (Guidance Note) ของคณะกรรมการอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์นับเป็นทางเลือกที่เหมาะสมในระยะสั้น เพราะสามารถจัดทำได้อย่างรวดและเร็ว[251] อีกทั้งยังส่งเสริมให้รัฐภาคีสามารถมีความเห็นในการตีความบทบัญญัติของอนุสัญญาไปในทิศทางเดียวกันได้ นอกจากนี้ การจัดทำแนวทางการตีความยังเปิดช่องทางให้ผู้ให้บริการ

[251] Ad-hoc sub-group on jurisdiction and transborder access to data. Transborder access and jurisdiction: What are the options?, Para.278

ทางอินเตอร์เน็ตจากภาคเอกชนและผู้ที่ส่วนได้เสียอื่นเข้ามามีส่วนร่วมด้วย อย่างไรก็ตาม แนวทางเหล่านี้จะไม่มีผลผูกพันตามกฎหมายแต่อย่างใด[252]

สำหรับการดำเนินการในระยะยาวนั้น การเพิ่มเติมรายละเอียดของเนื้อหากลไกความร่วมมือสามารถกระทำได้ด้วยการแก้ไขเพิ่มเติมบทบัญญัติของอนุสัญญากรุงบูดาเปสต์โดยตรง หรือการจัดทำพิธีสารเพิ่มเติมของอนุสัญญาแทน ซึ่งสองวิธีนี้จะก่อให้เกิดพันธะกรณีตามกฎหมายระหว่างประเทศ แต่จะมีข้อดีและข้อจำกัดที่แตกต่างออกไป

การแก้ไขบทบัญญัติของอนุสัญญาโดยตรง สามารถกระทำได้โดยอาศัยวิธีการตามข้อ 44 ของอนุสัญญากรุงบูดาเปสต์ หรืออาศัยวิธีการจัดทำพิธีสารเพื่อแก้ไขอนุสัญญาโดยสภายุโรป ซึ่งการแก้ไขจะมีผลบังคับใช้ได้ ก็ต่อเมื่อรัฐภาคีของอนุสัญญาทุกฝ่ายให้การยอมรับเท่านั้น ข้อดีของรูปแบบนี้ ก็คือ ผู้เกี่ยวข้องทุกฝ่ายล้วนมีส่วนในการเจรจาเพิ่มเติมรายละเอียด ทำให้มีผลผูกพันต่อรัฐภาคีของอนุสัญญาทุกรัฐในปัจจุบัน และรัฐที่จะเข้ามาเป็นภาคีในอนาคต อย่างไรก็ตาม กระบวนการดังกล่าวย่อมใช้เวลายาวนานมาก[253] ดังนั้น การแก้ไขบทบัญญัติของอนุสัญญาโดยตรงจึงเหมาะกับการขยายความหรือปรับปรุงรายละเอียดที่อนุสัญญากรุงบูดาเปสต์ได้กล่าวถึงไว้แล้ว หรือประเด็นที่รัฐภาคีมีความเห็นตรงกันในระดับหนึ่งผ่านการจัดทำแนวทางการตีความของคณะกรรมการอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์

การจัดทำพิธีสารเพิ่มเติมสำหรับอนุสัญญากรุงบูดาเปสต์จะมีข้อดีที่มีความยืดหยุ่น อีกทั้งสามารถเข้ามามีผลบังคับใช้หลังจากที่มีจำนวนรัฐยินยอมเข้าเป็นภาคีตามที่ได้กำหนดไว้[254] โดยไม่ต้องรอให้รัฐภาคีทุกรัฐยินยอมดังเช่นกรณีการแก้ไขอนุสัญญาโดยตรงแต่อย่างใด หากแต่จะมีข้อจำกัดที่จำนวนรัฐภาคีของพิธีสารเพิ่มเติมนั้น อาจมีไม่ครบเต็มจำนวนรัฐภาคีของอนุสัญญากรุงบูดาเปสต์ได้ ด้วยเหตุนี้ การจัดทำพิธีสารเพิ่มเติมจึงเหมาะแก่การเพิ่มเติมรายละเอียดในส่วนที่บทบัญญัติของอนุสัญญากรุงบูดาเปสต์ไม่มีเนื้อหาครอบคลุมมาก่อน หรือเนื้อหาในประเด็นที่รัฐมีความเห็นไม่ตรงกัน ดังที่จะเห็นได้จากกรณีพิธีสารเพิ่มเติม

---

[252] *Ibid.*

[253] *Ibid.*, Para.268-270

[254] *Ibid.*, Para.275-276

ว่าด้วยการกระทำผ่านระบบคอมพิวเตอร์ที่มีลักษณะเหยียดหยามหรือเกลียดชังเชื้อชาติของบูดาเปสต์ เป็นต้น

จากการศึกษาวิจัยในบทนี้ จะพบว่า เนื้อหาบางส่วนของกลไกความร่วมมือกรอบอนุสัญญากรุงบูดาเปสต์นั้น ยังไม่สอดคล้องกับบริบททางเทคโนโลยีทางคอมพิวเตอร์ที่เกิดขึ้นหลังการจากอนุสัญญามีผลบังคับใช้แล้ว เช่น ระบบคอมพิวเตอร์ Cloud นอกจากนี้ บทบัญญัติบางส่วนของอนุสัญญายังกำหนดรายละเอียดไว้อย่างกว้างเกินไป จึงส่งผลให้รัฐภาคีขาดแนวทางการปรับใช้ที่ชัดเจน และทำให้รัฐภาคีบางส่วนไม่นำมาตรการที่อนุสัญญาไปใช้มากเท่าที่ควร ด้วยเหตุนี้ การเพิ่มเติมรายละเอียดของกลไกความร่วมมือจึงจำเป็นอย่างยิ่งในการแก้ไขอุปสรรคที่เกิดขึ้น โดยการดำเนินการดังกล่าว จะสามารถทำได้ทั้งในรูปแบบที่ไม่มีและมีผลผูกพันทางกฎหมายระหว่างประเทศ

การดำเนินการในรูปแบบที่ไม่มีผลผูกพันทางกฎหมายนั้น ได้แก่ การประชุมของคณะกรรมการอนุสัญญาว่าด้วยอาชญากรรมคอมพิวเตอร์ การประชุม Octopus Interface Conference และโครงการอาชญากรรมทางคอมพิวเตอร์สากล ซึ่งเป็นการปรับใช้อนุสัญญากรุงบูดาเปสต์ในระดับระหว่างประเทศ ทั้งนี้ การดำเนินการที่ไม่มีผลผูกพันทางกฎหมายจะสามารถทำได้อย่างรวดเร็ว และมีประโยชน์ในการระบุประเด็นปัญหาจากการปรับใช้ และรวบรวมข้อมูลเกี่ยวกับประเด็นปัญหาดังกล่าว

การดำเนินการในรูปแบบที่มีผลผูกพันทางกฎหมายจะประกอบไปด้วย การแก้ไขบทบัญญัติของอนุสัญญาโดยตรงและการจัดทำพิธีสารเพิ่มเติม โดยการแก้ไขบทบัญญัติของอนุสัญญาโดยตรงจึงเหมาะสมกับการขยายความหรือปรับปรุงรายละเอียดที่อนุสัญญากรุงบูดาเปสต์ได้กล่าวถึงไว้แล้ว หรือประเด็นที่รัฐภาคีมีความเห็นตรงกันในระดับหนึ่ง ส่วนพิธีสารเพิ่มเติมจะเหมาะแก่การเพิ่มเติมรายละเอียดในส่วนที่บทบัญญัติของอนุสัญญากรุงบูดาเปสต์ไม่มีเนื้อหาครอบคลุมมาก่อน หรือเนื้อหาในประเด็นที่รัฐมีความเห็นไม่ตรงกัน

บทที่ 5
บทสรุปและข้อเสนอแนะ

5.1 บทสรุป

อาชญากรรมทางคอมพิวเตอร์นั้น มีเทคโนโลยีทางคอมพิวเตอร์เข้ามาเกี่ยวข้องในการก่ออาชญากรรมอย่างมีนัยยะสำคัญ อาชญากรรมประเภทนี้ จึงมีลักษณะพิเศษต่างไปจากอาชญากรรมทั่วไปหมายประการ ไม่ว่าจะเป็นความเสียหายที่เกิดขึ้นอย่างรวดเร็วและกว้างขวาง ความยากลำบากในการระบุตัวผู้กระทำผิด ความอ่อนไหวของหลักฐานที่อยู่ในรูปแบบข้อมูลทางอิเล็กทรอนิกส์ และความสามารถในการก่ออาชญากรรมที่ไม่จำกัดอยู่ภายใต้เขตแดนทางกายภาพ เป็นต้น ลักษณะพิเศษดังกล่าวยังส่งผลกระทบให้รัฐต่างๆ จำเป็นต้องพัฒนาปรับปรุงกฎหมายเพื่อรองรับอาชญากรรมประเภทนี้ทั้งในระดับภายในประเทศและระหว่างประเทศควบคู่กันไป

ทั้งนี้ แม้ว่ารัฐบางแห่งมีความพร้อมทางด้านกฎหมายสารบัญญัติและวิธีสบัญญัติภายในประเทศแล้วก็ตาม การรวบรวมหลักฐานและติดตามจับกุมผู้กระทำความผิดมาลงโทษยังสามารถเกิดอุปสรรคได้หากผู้กระทำผิดหรือหลักฐานที่เกี่ยวข้องนั้นตั้งอยู่ในดินแดนของรัฐอื่น เพราะรัฐต่างๆจะสามารถบังคับใช้อำนาจอธิปไตยของตนได้เฉพาะในเขตแดนรัฐเท่านั้น อีกทั้งยังต้องเคารพในอำนาจอธิปไตยของรัฐอื่นด้วย ด้วยเหตุดังกล่าว การให้ความร่วมมือทางอาญาระหว่างประเทศซึ่งประกอบไปด้วยการส่งตัวผู้ร้ายข้ามแดน และการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายนั้น จึงมีความสำคัญต่อการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ ในการนี้ ถ้ากลไกการให้ความร่วมมือทางอาญาระหว่างประเทศที่มีผลบังคับใช้กับรัฐนั้น ไม่ได้ครอบคลุมอาชญากรรมทางคอมพิวเตอร์ การให้ความร่วมมือทางอาญาก็อาจจะไม่เกิดขึ้นได้

ในทางกลับกัน หากรัฐที่เกี่ยวข้องกับการอาชญากรรมทางคอมพิวเตอร์นั้นขาดความพร้อมด้านกฎหมายภายในสำหรับอาชญากรรมทางคอมพิวเตอร์แล้ว การให้ความร่วมมือทางอาญาระหว่างประเทศในอาชญากรรมทางคอมพิวเตอร์ก็เกิดอุปสรรคได้เช่นกัน โดยในกรณีที่รัฐขาดแคลนกฎหมายสารบัญญัติหรือมีแนวทางการตีความปรับใช้กฎหมายที่ไม่สอดคล้องกันแล้ว การให้ความร่วมมือระหว่างรัฐอาจไม่สามารถดำเนินการได้

เนื่องจากไม่เป็นไปตามหลักความผิดสองประเทศ (double criminality) นอกจากนี้ หากรัฐขาดกฎหมายวิธีสบัญญัติสำหรับอาชญากรรมทางคอมพิวเตอร์แล้ว การให้ความร่วมมือก็อาจจะไม่บรรลุผลได้ เพราะเจ้าหน้าที่รัฐไม่สามารถได้มาซึ่งหลักฐานในการก่ออาชญากรรมทางคอมพิวเตอร์ได้อย่างทันท่วงที

จะเห็นได้ว่า กลไกความร่วมมือทางอาญาระหว่างประเทศทั่วไปนั้น ยังไม่เหมาะสมกับการนำไปปรับใช้ในบริบทของอาชญากรรมทางคอมพิวเตอร์แต่อย่างใด เพราะกลไกเหล่านี้จะเน้นไปยังการให้ความร่วมมือทางอาญาระหว่างประเทศในกรณีทั่วไป หากแต่ไม่ได้ส่งเสริมให้มีการแก้ไขปรับปรุงกฎหมายภายในรัฐด้านอาชญากรรมทางคอมพิวเตอร์อย่างเป็นการเฉพาะเจาะจง

ดังนั้น กลไกความร่วมมือทางอาญาระหว่างประเทศสำหรับอาชญากรรมทางคอมพิวเตอร์ จึงต้องมีบทบาทด้านการกำหนดมาตรฐานร่วมกันสำหรับกฎหมายภายในประเทศเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ อีกทั้งยังขยายขอบเขตความร่วมมือระหว่างประเทศให้ครอบคลุมอาชญากรรมทางคอมพิวเตอร์ด้วย ในขณะเดียวกัน กลไกความร่วมมือทางอาญาสำหรับอาชญากรรมทางคอมพิวเตอร์ยังต้องสามารถรองรับความซับซ้อนของอาชญากรรมทางคอมพิวเตอร์ที่ทวีขึ้นไปตามพัฒนาการของเทคโนโลยีได้ด้วย ความจำเป็นทั้งสามด้านนี้ ได้นำไปสู่การจัดทำอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ หรืออนุสัญญากรุงบูดาเปสต์ในเวลาต่อมา

เมื่อพิจารณาจากกลไกความร่วมมือภายใต้กรอบอนุสัญญากรุงบูดาเปสต์แล้ว จะพบว่าเนื้อหาของอนุสัญญา สามารถตอบสนองต่อความจำเป็นทั้งสามด้านดังข้างต้น

โดยในส่วนการกำหนดมาตรฐานร่วมกันสำหรับกฎหมายภายในประเทศนั้น จะพบว่าอนุสัญญากรุงบูดาเปสต์ได้กำหนดฐานความผิดที่ครอบคลุมด้านความผิดต่อความลับ ความสมบูรณ์ และบูรณภาพของข้อมูลและระบบคอมพิวเตอร์ ความผิดที่เกี่ยวข้องกับคอมพิวเตอร์ ความผิดที่เกี่ยวข้องกับเนื้อหา และความผิดที่เกี่ยวข้องกับการละเมิดลิขสิทธิ์ นอกจากนี้ อนุสัญญากรุงบูดาเปสต์ยังได้กำหนดองค์ประกอบความผิดและเพิ่มเติมบทบัญญัติเกี่ยวกับความรับผิด เพื่อให้รัฐภาคีมีแนวทางการปรับใช้ชัดเจนมากขึ้น ในขณะเดียวกัน อนุสัญญา

ยังอนุญาตให้รัฐภาคีสามารถตั้งข้อสงวนเกี่ยวกับองค์ประกอบความผิดบางประการ เพื่อสร้างความยืดหยุ่นแก่รัฐภาคีที่มีความแตกต่างกันเข้ามาให้ความร่วมมือทางอาญาภายใต้กรอบความร่วมมือเดียวกันได้

ในด้านกฎหมายวิธีสบัญญัตินั้น อนุสัญญากรุงบูดาเปสต์ได้กำหนดอำนาจการสืบสวนอาชญากรรมประเภทใหม่ อาทิ การเก็บรักษาข้อมูลอย่างรวดเร็วเพื่อป้องกันไม่ให้หลักฐานในคดีอาชญากรรมทางคอมพิวเตอร์ได้ถูกดัดแปลงหรือถูกทำลายโดยผู้กระทำผิด หรือการเฝ้าระวังทางเทคนิคเพื่อป้องกันและตรวจจับการกระทำความผิด เป็นต้น เพื่อให้สามารถรองรับบริบทของหลักฐานข้อมูลทางอิเล็กทรอนิกส์ได้ ในขณะเดียวกัน อนุสัญญายังได้ปรับปรุงอำนาจการสืบสวนดั้งเดิมเช่น การค้นและยึดให้สอดคล้องกับอาชญากรรมทางคอมพิวเตอร์ด้วย นอกจากนี้ ข้อ 15 ของอนุสัญญากรุงบูดาเปสต์ยังได้กำหนดกรอบเงื่อนไขและมาตรการป้องกันสิทธิมนุษยชนและเสรีภาพเพื่อรักษาความสมดุลระหว่างการหาตัวผู้กระทำความผิด และการรักษาสิทธิส่วนบุคคลของผู้ที่เกี่ยวข้องในการสืบสวนคดีอาชญากรรมทางคอมพิวเตอร์ ไว้อีกด้วย

สำหรับการให้ความร่วมมือระหว่างประเทศ อนุสัญญากรุงบูดาเปสต์จะรองรับการส่งตัวผู้ร้ายข้ามแดนสำหรับฐานความผิดที่อนุสัญญาและพิธีสารเพิ่มเติมได้กำหนดไว้ อีกทั้งส่งเสริมให้การให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายเป็นไปอย่างรวดเร็ว และยืดหยุ่นมากขึ้น อีกทั้งยังมีการรักษาความลับและจำกัดการใช้ในการดำเนินการด้วย นอกจากนี้ อนุสัญญากรุงบูดาเปสต์จะครอบคลุมการให้ความช่วยเหลือด้วยวิธีเฉพาะซึ่งเป็นการนำอำนาจสืบสวนคดีอาชญากรรมทางคอมพิวเตอร์มาขยายผลในการให้ความร่วมมือทางอาญาระหว่างประเทศ อีกทั้งยังจัดตั้งเครือข่ายจุดติดต่อตลอดเวลาเพื่อให้รัฐภาคีติดต่อประสานงานกันได้อย่างรวดเร็ว

อนุสัญญากรุงบูดาเปสต์ยังมีความยืดหยุ่นในการรองรับความเปลี่ยนแปลงทางเทคโนโลยีที่จะเกิดขึ้นต่อไปในอนาคตได้ เนื่องจากอนุสัญญาได้ใช้ถ้อยคำที่เป็นกลางทางเทคโนโลยีในการกำหนดฐานความผิดและมาตรการสืบสวนอาชญากรรมทางคอมพิวเตอร์ ส่วนการใช้อำนาจสืบสวนอาชญากรรมทางคอมพิวเตอร์และการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายภายใต้อนุสัญญานั้น จะมีขอบเขตปรับใช้ที่ครอบคลุมอาชญากรรมที่ใช้คอมพิวเตอร์

เป็นเครื่องมือทุกประเภท และการรวบรวมหลักฐานที่อยู่ในรูปแบบข้อมูลคอมพิวเตอร์ของอาชญากรรมทุกกรณี

การที่อนุสัญญากรุงบูดาเปสต์มีฐานะเป็นกฎหมายสนธิสัญญาระหว่างประเทศยังสามารถส่งเสริมบทบาททั้งสามด้านให้บรรลุผลมากขึ้นไปอีก เพราะรัฐภาคีมีพันธะกรณีตามกฎหมายระหว่างประเทศที่จะต้องปฏิบัติตาม อีกทั้งยังเป็นฐานทางกฎหมายในการให้ความร่วมมือทางอาญาระหว่างประเทศโดยตรง นอกจากนี้ อนุสัญญากรุงบูดาเปสต์ยังมีบทบัญญัติเกี่ยวกับการปรึกษาหารือระหว่างรัฐภาคีและการแก้ไขอนุสัญญา จึงทำให้กลไกความร่วมมือกรอบอนุสัญญากรุงบูดาเปสต์สามารถติดตามผลการปรับใช้ และปรับปรุงเนื้อหาของตัวเองต่อไปในอนาคตได้ ในขณะเดียวกัน หน้าที่ของรัฐภาคีในการรายงานข้อมูลไปยังเลขาธิการสภายุโรปเกี่ยวกับหน่วยงานที่ทำหน้าที่จัดการด้านการส่งตัวผู้ร้ายข้ามแดน และหน่วยงานกลางสำหรับให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายนั้น ย่อมช่วยให้รัฐภาคีสามารถติดต่อระหว่างกันได้สะดวกยิ่งขึ้น

อนึ่ง การจัดทำพิธีสารเพิ่มเติมยังสามารถลดปัญหาที่เกิดจากความแตกต่างแนวคิดทางกฎหมายได้ ดังที่จะเห็นจากกรณีของการกำหนดความผิดที่เกี่ยวข้องกับการเหยียดหยามดูหมิ่นเชื้อชาติไว้ในพิธีสารเพิ่มเติม

อย่างไรก็ตาม กลไกความร่วมมือทางอาญาภายใต้กรอบอนุสัญญากรุงบูดาเปสต์ยังจำเป็นต้องได้รับการประเมินผลลัพธ์ต่อไปอีกว่า สามารถตอบสนองอาชญากรรมทางคอมพิวเตอร์ได้มากน้อยเพียงใด ทั้งนี้ โดยพิจารณาจากความสอดคล้องระหว่างเนื้อหาของกลไกความร่วมมือกับบริบททางเทคโนโลยีและข้อเท็จจริง และแนวทางการปรับใช้

เมื่อพิจารณาจากการเนื้อหากลไกอนุสัญญาแล้ว จะพบว่าบทบัญญัติบางส่วนนั้นควรได้รับการปรับปรุงให้สอดคล้องกับบริบททางเทคโนโลยีและข้อเท็จจริง และเพิ่มเติมรายละเอียดให้รัฐภาคีมีแนวทางการปรับใช้ที่ชัดเจนมากขึ้น

ในการนำอนุสัญญาไปปรับใช้นั้น รัฐภาคียังคงมีแนวปฏิบัติที่แตกต่างกันไป โดยรัฐบางส่วนจะจัดทำกฎหมายพิเศษขึ้นมารองรับอนุสัญญาเป็นการเฉพาะเจาะจง ซึ่งมีเนื้อหา

มาจากอนุสัญญากรุงบูดาเปสต์โดยตรง ในขณะที่รัฐอีกส่วนหนึ่งจะเลือกปรับใช้กฎหมายภายในที่มีอยู่แล้วแทน เพื่อประหยัดเวลาและค่าใช้จ่าย ในรัฐกลุ่มหลังนี้ การปรับใช้ตามอนุสัญญาจะสะท้อนผ่านทางวิธีปฏิบัติภายในองค์การต่างๆและคำพิพากษาซึ่งมีอยู่กระจัดกระจายทำให้สืบค้นได้ยาก นอกจากนี้ ยังพบว่า แม้รัฐบางส่วนจะมีกฎหมายรองรับการปฏิบัติตามอนุสัญญาก็ตาม รัฐกลุ่มนั้นกลับไม่ใช้มาตรการที่อนุสัญญากำหนดไว้มากนัก

เพราะฉะนั้น อนุสัญญากรุงบูดาเปสจ์ยังจำเป็นต้องเพิ่มเติมรายละเอียดของกลไกความร่วมมือ เพื่อแก้ไขปัญหาที่เกิดขึ้น การเพิ่มเติมรายละเอียดนี้ สามารถทำได้ในรูปแบบที่ไม่มีผลผูกพันทางกฎหมายระหว่างประเทศ เช่น การประชุมของคณะกรรมการอนุสัญญาว่าด้วยอาชญากรรมคอมพิวเตอร์ การประชุม Octopus Interface Conference และ โครงการอาชญากรรมทางคอมพิวเตอร์สากล เป็นต้น นอกจากนี้ การเพิ่มเติมรายละเอียดยังสามารถกระทำได้ด้วยการแก้ไขบทบัญญัติของอนุสัญญาโดยตรงและการจัดทำพิธีสารเพิ่มเติม ซึ่งจะมีผลผูกพันทางกฎหมาย วิธีการต่างๆเหล่านี้จะมีความเหมาะสมแตกต่างกันไป

สำหรับประเทศไทยนั้น แม้จะได้จัดทำกฎหมายภายในด้านอาชญากรรมทางคอมพิวเตอร์ ซึ่งก็คือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไว้แล้วก็ตาม แต่การเข้าเป็นภาคีอนุสัญญากรุงบูดาเปสต์ ย่อมจะเป็นประโยชน์ต่อประเทศไทยมากกว่าการพึ่งพากลไกความร่วมมือทางอาญาระหว่างประเทศที่มีอยู่แต่เดิม ซึ่งประกอบไปด้วยข้อตกลงด้านการส่งตัวผู้ร้ายข้ามแดนและการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายจำนวนหลายฉบับ ทั้งนี้ อนุสัญญากรุงบูดาเปสต์จะเป็นฐานทางกฎหมายรองรับการให้ความร่วมมือทางอาญาระหว่างประเทศไทยกับบรรดารัฐภาคีโดยประเทศไทยนั้นไม่จำเป็นต้องทบทวนแก้ไขเนื้อหาข้อตกลงที่ตนได้ทำไว้แล้ว หรือเสียเวลาและทรัพยากรในการจัดทำข้อตกลงฉบับใหม่กับรัฐอื่นๆ แต่อย่างใด โดยมาตรฐานด้านการให้ความร่วมมือที่อนุสัญญากำหนดไว้นี้ นับว่ามีความรวดเร็ว ยืดหยุ่น ปลอดภัย และมีประสิทธิภาพในการปราบปรามอาชญากรรมทางคอมพิวเตอร์ ในขณะเดียวกัน จะเห็นได้ว่าอนุสัญญากรุงบูดาเปสต์ได้มีรัฐเข้ามาลงนามและเป็นภาคีในจำนวนมากขึ้นเรื่อยๆ โดยที่บางส่วนก็มาจากนอกภูมิภาคยุโรปด้วย หากประเทศไทยได้เข้าเป็นภาคีอนุสัญญา ประโยชน์จะได้จากกรอบความร่วมมือนี้ก็จะเพิ่มมากขึ้นไปด้วยเช่นกัน

นอกจากนี้ เมื่อได้เข้าเป็นภาคีอนุสัญญากรุงบูดาเปสต์แล้ว ประเทศไทยก็จะได้เข้าเป็นส่วนหนึ่งของคณะกรรมการอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ (T-CY) ซึ่งจะมีบทบาทในการแลกเปลี่ยนข้อมูล เสริมประสิทธิภาพในการปรับใช้อนุสัญญา และปรับปรุงพัฒนาเนื้อหาอนุสัญญา เพราะฉะนั้น ประเทศไทยจะสามารถนำเสนอประเด็นปัญหาที่ตนให้ความสนใจไปยังที่ประชุมคณะกรรมการได้ ซึ่งจะนำไปสู่การดำเนินการแก้ไขปัญหานั้นในลำดับต่อไป

5.2 **ข้อเสนอแนะ**

1. รัฐต่างๆ ควรรณรงค์ที่จะไม่ให้การสนับสนุนหรือร่วมลงมือก่ออาชญากรรมทางคอมพิวเตอร์ เพื่อลดอุปสรรคในการสืบสวนและดำเนินคดีต่อผู้ก่ออาชญากรรมทางคอมพิวเตอร์

2. คณะกรรมการอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ (T-CY) ควรจัดทำแนวทางการตีความข้อ 15 ของอนุสัญญาว่า มาตรการป้องกันภายใต้บทบัญญัตินี้ ครอบคลุมถึงหลักการปกป้องข้อมูลส่วนบุคคลด้วยหรือไม่ อีกทั้งควรจัดทำรายงานประเมินการปรับใช้อนุสัญญาข้อ 15 ควบคู่ไปด้วย เพื่อให้รัฐแนวทางการปรับใช้อนุสัญญาได้อย่างชัดเจนมากขึ้น สำหรับการดำเนินการในระยะยาวนั้น ควรแก้ไขให้ข้อ 15 ของอนุสัญญากล่าวถึงหลักการปกป้องข้อมูลส่วนบุคคลไว้อย่างเป็นการเฉพาะเจาะจง

3. ควรมีการจัดทำพิธีสารเพิ่มเติมอนุสัญญากรุงบูดาเปสต์ในด้านการปฏิสัมพันธ์ระหว่างหน่วยงานรัฐผู้สืบสวนคดีอาชญากรรมทางคอมพิวเตอร์และผู้ให้บริการทางอินเตอร์เน็ต โดยให้พิธีสารดังกล่าวนั้น กำหนดเงื่อนไข และกระบวนการให้ความร่วมมือระหว่างเจ้าหน้าที่รัฐและผู้ให้บริการทางอินเตอร์เน็ต อีกทั้งมีรายละเอียดเกี่ยวกับการกำหนดจุดติดต่อ และการแบ่งภาระค่าใช้จ่ายระหว่างทั้งสองฝ่ายด้วย

4. ควรแก้ไขบทบัญญัติข้อ 22 วรรค 5 ของอนุสัญญากรุงบูดาเปสต์ว่า ในกรณีที่รัฐภาคีจำนวนมากกว่าหนึ่งรัฐได้กล่าวอ้างเขตอำนาจของตนเหนือการกระทำความผิดที่เกิดขึ้น แต่รัฐเหล่านั้นไม่ได้ดำเนินการปรึกษาหารือกันเพื่อหารัฐที่เหมาะสมต่อการดำเนินคดีต่อผู้กระทำผิด ให้รัฐผู้รับคำขอความร่วมมือทางอาญาพิจารณาหารัฐที่เหมาะสมจากปัจจัยเฉพาะคดีนั้น อาทิ ความร้ายแรง วันที่ได้รับคำขอความช่วยเหลือ สัญชาติ

ของบุคคลตามคำขอ ลักษณะการลงโทษ และความเป็นไปได้ในการส่งตัวผู้ร้ายข้ามแดนไปยังรัฐอื่นๆในภายหลัง เป็นต้น

5. รัฐภาคีอนุสัญญากรุงบูดาเปสต์ ควรปรับปรุงกฎหมายภายในให้ให้มีบทบัญญัติเฉพาะสำหรับรองรับการใช้อำนาจการสืบสวนอาชญากรรมทางคอมพิวเตอร์ตามอนุสัญญากรุงบูดาเปสต์ อาทิ การเก็บรักษาข้อมูล และการเปิดเผยข้อมูลทางจราจรบางส่วน เป็นต้น ทั้งนี้ เพื่อส่งเสริมให้หน่วยงานของรัฐใช้อำนาจสืบสวนดังกล่าวเพิ่มขึ้นทั้งในระดับภายในประเทศและระหว่างประเทศ

6. ควรมีการจัดทำพิธีสารเพิ่มเติมด้านการเข้าถึงข้อมูลทางอิเล็กทรอนิกส์ เพื่อให้สามารถรองรับกับระบบคอมพิวเตอร์ cloud ที่ข้อมูลที่เป็นหลักฐานอาชญากรรมนั้นจะเคลื่อนที่ไปมาหรือถูกกักเก็บไว้ในเขตอำนาจของรัฐหลายแห่ง หรือในกรณีที่ที่ตั้งของข้อมูลดังกล่าวไม่สามารถระบุได้อย่างชัดเจน เนื้อหาของพิธีสารเพิ่มเติมนี้ควรครอบคลุมมาตรการใหม่ดังต่อไปนี้

- การเข้าถึงข้อมูลข้ามแดนโดยอาศัยความยินยอมตามข้อ 32 b อนุสัญญากรุงบูดาเปสต์หากแต่ตัดข้อจำกัดที่รัฐต้องทราบถึงที่ตั้งของข้อมูลได้อย่างแน่นอนออกไป
- การเข้าถึงข้อมูลข้ามแดนโดยไม่ต้องอาศัยความยินยอมตามข้อ 32 b อนุสัญญากรุงบูดาเปสต์ แต่ให้อาศัยข้อมูลระบุตัว (credentials) อาทิ username หรือ password ที่ได้มาโดยชอบด้วยกฎหมายแทน แต่ยังต้องแจ้งไปให้รัฐอีกฝ่ายทราบด้วย
- การเข้าถึงข้อมูลข้ามแดนโดยไม่ต้องอาศัยความยินยอมตาม ข้อ 32 b อนุสัญญากรุงบูดาเปสต์ หากแต่ต้องเป็นไปตามเงื่อนไขว่า ผู้ดำเนินการจะต้องทำการโดยเจตนาสุจริต กล่าวคือ ไม่สามารถทราบได้ว่าข้อมูลที่จะถูกเข้าถึงนั้นตั้งอยู่ที่รัฐใด นอกจากนี้ให้รวมไปถึงกรณีฉุกเฉินด้วย
- การขยายขอบเขตการค้นข้อมูลจากคอมพิวเตอร์เครื่องที่ค้นอยู่ไปยังระบบคอมพิวเตอร์ที่เชื่อมต่อกับคอมพิวเตอร์เครื่องนั้นได้ หากแต่ไม่ต้องจำกัดว่าระบบคอมพิวเตอร์อื่นนั้นจะต้องอยู่ภายในดินแดนรัฐเดียวกันดังเช่นที่เคยปรากฏในข้อ 19 วรรค 2 ของอนุสัญญา

7. คณะกรรมการอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ควรปรึกษาหารือและทำรายงานประเมินการปรับใช้บทบัญญัติของอนุสัญญาด้านการรวบรวมข้อมูลจราจรตามเวลาจริงและการดักรับข้อมูลเนื้อหา เพื่อระบุประเด็นปัญหาจากการปรับใช้ และรวบรวมข้อมูลสำหรับการเพิ่มเติมรายละเอียดของอนุสัญญากรุงบูดาเปสต์ในเรื่องดังกล่าวต่อไป

8. รัฐภาคีควรจะดำเนินการต่างๆเพื่อให้หน่วยงานภายในด้านอาชญากรรมทางคอมพิวเตอร์ ทราบถึงทางเลือกในการใช้เครือข่ายจุดติดต่อตลอดเวลาเพื่อขอความร่วมมือระหว่างประเทศด้านอาชญากรรมทางคอมพิวเตอร์และหลักฐานทางอิเล็กทรอนิกส์ ทั้งนี้โดยอาศัยการฝึกอบรมเจ้าหน้าที่บุคลากรที่เกี่ยวข้องโดยโครงการอาชญากรรมทางคอมพิวเตอร์สากล ในขณะเดียวกันคณะกรรมการอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์นั้น ควรจัดทำแนวทางการตีความพื่อให้รัฐภาคีสามารถพิจารณาว่ามีกรณีใดบ้างที่ต้องอาศัยการดำเนินการอย่างเร่งด่วนผ่านทางเครือข่ายจุดติดต่อตลอดเวลา

9. ประเทศไทยควรพิจารณาเข้าเป็นภาคีอนุสัญญากรุงบูดาเปสต์ เพื่อให้สามารถใช้ประโยชน์จากกลไกความร่วมมือภายใต้กรอบอนุสัญญากับบรรดารัฐภาคีที่มีอยู่เป็นจำนวนมาก และกำลังเพิ่มจำนวนขึ้นเรื่อยๆ โดยไม่ต้องเสียเวลาและทรัพยากรในการทบทวนข้อตกลงความร่วมมือทางอาญาที่ตนมีอยู่ หรือจัดทำข้อตกลงฉบับใหม่กับรัฐอื่นไปทีละราย นอกจากนี้ ประเทศไทยจะสามารถเข้าเป็นส่วนหนึ่งของคณะกรรมการอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ซึ่งมีบทบาทในการแบ่งปันข้อมูลพัฒนาการปรับใช้ และปรับปรุงพัฒนาเนื้อหาของอนุสัญญาได้

รายการอ้างอิง

ภาษาไทย

พรชัย ด่านวิวัฒน์, กฎหมายอาญาระหว่างประเทศ (กรุงเทพฯ : วิญญูชน, 2551), หน้า 60

ตะวัน พึ่งพุทธารักษ์. ปัญหาการส่งผู้ร้ายข้ามแดนในคดีอาญากรรมคอมพิวเตอร์. วิทยานิพนธ์ปริญญามหาบัณฑิต สาขากฎหมายระหว่างประเทศ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2546.

สุผานิต มั่นศุข. กฎหมายระหว่างประเทศแผนกคดีอาญา. กรุงเทพฯ : คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2523.

ภาษาอังกฤษ

Ad-hoc sub-group on jurisdiction and transborder access to data. Transborder access and jurisdiction: What are the options? [Online]. Strasbourg: Council of Europe, The cybercrime convention committee (T-CY), 2012. Available from: http://www.coe.int/t/dghl/standardsetting/t-cy/TCY2012/TCY_2012_3_transborder_rep_V30public_7Dec12.pdf [2013, May 6]

ADB/OECD anti-corruption initiative for Asia and the Pacific. Mutual legal assistance , extradition and recovery of proceeds of corruption in Asia and Pacific[Online]. Asian development bank and organisation for economic co-operation and development, 2007. Available from: http://www.oecd.org/site/adboecdanti-corruptioninitiative/37900503.pdf [2013, May 7]

Archik,K. Cybercrime: The council of Europe convention [Online]. United States: The library of congress, congressional research service, 2002. Available from: http://eee.iwar.org.uk/news-archive/crs/10088.pdf [2013, May 8]

Baron, R.M.F. A critique of the international cybercrime treaty. Commlaw Conspectus 10,263 [Online] (2002). Available from: www.westlaw.com [2013, May 10]

Barkham,J. Information warfare and international law on the use of force. International Law and Politics 34,57 (2001):57-113.

Callanan C. and Gercke, M. Cooperation between law enforcement and internet service providers against cybercrime: Towards common guidelines [Online]. Strasbourg: Council of Europe, Directorate general of human rights and legal affairs, Economic crime division, 2008. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/567%20prov-d-wg%20STUDY%20final%20_25%20june%202008_.pdf [2013, May 8]

Chirillo, J. and Danielyan, E. Sun certified security administrator for Solaris 9&10 study guide. Emeryville: McGraw-Hill, 2005.

Clough, J. Principles of cybercrime. UK: Cambridge University Press, 2010.

Committee of experts on the operation of European conventions on co-operation in criminal matters (PC-OC). Replies on mutual legal assistance in computer-related cases [Online]. Strasbourg: Council of Europe, European committee on crime problems (CDPC), 2008. Available from: http://www.coe.int/t/dghl/standardsetting/t-cy/PC-OC%20%282009%29%2005%20E.pdf [2013, May 6]

Committee of experts on the operation of European conventions on co-operation in criminal matters (PC-OC). Summary of the replies to the questionnaire on mutual legal assistance in computer-related cases [Online]. Strasbourg: Council of Europe, European committee on crime problems (CDPC), 2009. Available from: http://www.coe.int/t/dghl/standardsetting/t-cy/PC-OC%20%282009%29%2005%20E.pdf [2013, May 6]

Computer crime and intellectual property section, US department of justice, Operation Buccaneer: The Investigation, Cited in Clough, J. Principles of cybercrime. UK: Cambridge University Press, 2010.

Computer crime and intellectual property section, US department of justice. The National Information Infrastructure Protection Act of 1996: Legislative analysis. US Department of Justice, 2003. Cited in Clough, J. Principles of cybercrime. UK: Cambridge University Press, 2010.

Council of Europe. Additional protocol to the convention on cybercrime explanatory report [Online]. Available from: http://conventions.coe.int/Treaty/EN/Reports/Html/189.htm [2013, May 6]

Council of Europe. Convention on cybercrime explanatory report [Online]. Available from: http://conventions.coe.int/Treaty/en/Reports/Html/185.htm [2013, May 6]

Cybercrime@IPA project of the Council of Europe and the European Union, Global project on cybercrime of the Council of Europe, and European Union cybercrime task force. Specialised cybercrime units: Good practice study [Online]. Strasbourg: Council of Europe, Directorate general of human rights and rule of law, Data protection and cybercrime division, 2011. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/Octopus2011/2467_HTCU_study_V30_9Nov11.pdf [2013, May 6]

Data protection and cybercrime division. Global project on cybercrime (phase 2) 1 March 2009- 11 December 2011 final report [Online]. Strasbourg: Council of Europe, Directorate genral of human rights and rule of law, Information society and action against crime directorate, 2012. Available from: http://www.coe.int/t/dghl/standardsetting/t-cy/TCY2012/2079_adm_finalreport_V12_9apr12.pdf [2013, May 8]

Downing, R. W. Shoring up the weakest link: What lawmakers around the world need to consider in developing comprehensive laws to combat cybercrime Columbia Journal of Transnational Law 43,705 [Online] (2005). Available from: www.westlaw.com [2013, May 10]

Genderen, R.H. Cybercrime investigation and the protection of personal data and privacy [Online]. Strasbourg, Council of Europe, Directorate general of human rights and legal affairs, Economic crime division, 2008. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/567%20study5-d-provisional.pdf [2013, May 8]

Gercke, M. Understanding cybercrime: A guide for developing countries [Online]. Geneva: International Telecommunication Union (ITU), ICT applications and cybersecurity division, 2009. Available from: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf [2013, May 6]

Goodman, M.D., and Brenner, S.W. The emerging consensus on criminal conduct in cyberspace [Online]. 2002. Available from: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf [2013, May 7].

Goodman, S.E., Hassebroek, P.B., King, D.,and Ozment, A. International coordination to increase the security of critical network infrastructures [Online]. Seoul: International telecommunication union workshop on creating trust in critical network structures, 2002. Available from: http://www.itu.int/osg/spu/ni/security/docs/cni.04.pdf [2013, May 8]

Harris, D.J. Cases and materials on international law, 6th edition. London: Sweet and Maxwell, 2004.

Hopkins, S.L. Cybercrime convention: A positive beginning to a long road ahead. Journal of High Technology Law, 2,101 [Online] (2003). Available from: www.westlaw.com [2013, May 10]

Jennings,R., and Watts, A. eds. Oppenheim's International Law Vol. 1 Essex :Longman Group U.K. Limited, 1992.

Kaspersen,H. ,Schwerha,J., and Dragizevic,D. Article 15: conditions and safeguards under the Budapest convention on cybercrime [Online]. Strasbourg: Council of Europe, Directorate general of human rights and rule of law, Cybercrime division, 2012. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/2467_SafeguardsRep_v18_29mar12.pdf [2013, May 8]

Kowalki, M. Cyber-crime: issues, data sources, and feasibility of collecting police-reported statistics. Ottawa: *Statistics* Canada, 2002. Cited in Clough,J. Principles of cybercrime. UK: Cambridge University Press, 2010.

Marler, S.L. The convention on cyber-crime: Should the United States ratify? New England Law Review 37,183 [Online](2002). Available from: www.westlaw.com [2013, May10]

Morishita,T. Some Proposals for the Improvement of Extradition Among the ASEAN Countries. Paper presented at the 4th ACPF Meetings, Held in Bangkok, Thailand,15-17 November 1995.

Morris,S. The Future of Netcrime Now: Part 1-threats and challenges. Hope office online report 62/04. Home Office, 2004. Cited in Clough, J. Principles of cybercrime. UK: Cambridge University Press, 2010.

National Criminal Intelligence Service. Project Trawler: Crime on the information high-ways [Online]. 1999. Available from: www.cyber-rights.org/documents/trawler.htm [2013, May 7] Cited in Clough, J. Principles of cybercrime. UK: Cambridge University Press, 2010.

National Institute of Standard and Technology. Standards for security categorization of federal information and information systems [Online]. Gaithersburg: National insitute of standard and technology, Information technology laboratory, Computer secirity division, 2004. Available from: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf [2013, May 7]

Octopus interface conference: cooperation against cybercrime. Messages from the Octopus conference [Online]. Strasbourg, Council of Europe, 2010. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy-activity-Interface-2010/2079_IF10_messages_1p%20key%20prov%20_26%20mar%2010_.pdf [2013, May 8]

Octopus interface conference on cooperation against cybercrime. Conference conclusions [Online]. Strasbourg: Council of Europe, 2008. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_Interface2008/567_IF08-d-concl1c.pdf [2013, May 8])

Octopus interface conference on cooperation against cybercrime. Conference summary [Online]. Strasbourg: Council of Europe, 2007. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity%20Interface2007/567%20IF%202007-d-sumconclusions1g%20Provisional.pdf [2013, May 8]

Octopus interface conference on cooperation against cybercrime. Conference summary [Online]. Strasbourg: Council of Europe, 2009. Available from: http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy%20activity%20interface%202009/2079%20if09_SUMMARY1.pdf [2013, May 8]

Project on cybercrime. Global project on cybercrime (phase 2) summary [Online]. Strasbourg: Council of Europe, 2011. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20Project%20global%20phase%202/2079%20adm%20pro%20summary%20_26%20Sep%202011_.pdf [2013, May 8]

Project on Cybercrime. Guidelines for the cooperation between law enforcement and internet providers against cybercrime[Online]. Strasbourg, Council of Europe, Directorate general of human rights and legal affairs, Economic crime division, 2008, Available from: http://www.coe.int/t/informationsociety/documents/Guidelines_cooplaw_ISP_en.pdf [2013, May 8]

Robel,D. International cybercrime treaty: Looking beyond ratification[Online]. Bethesda: SANS Institute, 2007. Available from: http://www.sans.org/reading_room/whitepapers/honors/international-cybercrime-treaty-ratification_1756 [2013, May 8]

Schjolberg,S. The history of global harmonization on cybercrime Legislation-The Road to Geneva [Online]. 2008. Available from: http://www.cybercrimelaw.net/documents/cybercrime_history.pdf.[2013, May 7]

Seger,A. The Budapest convention on cybercrime 10 years on: Lessons learnt of the web is a web[Online]. Strasbourg: Council of Europe, 2012. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/AS_UNISPAweb_V6_16feb12.pdf [2013, May 8], p.2

Shackelford,S. From nuclear war to net war: Analogizing cyber attacks in international law. Berkeley Journal of International Law 27,1 (2008):191-251

Shearer, I.,A. Extradition in international law. Manchester: Manchester Press, 1997

Sinrod, E.J. and Reilly, W.P. Cyber-crimes: A practical approach to the application of federal computer crime laws. Santa Clara Computer and High Tech Law Journal 16,177 (2000): 194-7 Cited in: Clough, J. Principles of cybercrime. UK: Cambridge University Press, 2010.

Soma, J.T., Muther, T.F.Jr., and Brisette, H.M.L. Transnational extradition for computer crimes: Are new treaties and laws needed?. Harvard Journal on Legislation 34,2 (1997): 317-371.

Spoenle, Jan. Cloud computing and cybercrime investigations: Territoriality vs. the power of disposal? [Online]. Strasbourg: Council of Europe, Directorate general of human rights and legal affairs, economic crime division, 2010. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf [2013, May 8]

Steinhardt, B. Hate Speech. in Y. Akdeniz,Y., C. Walker, and D. Wall (eds.), The internet, law, and society, pp.249-272 London: Dorset Press, 2000.

The cybercrime convention committee (T-CY). Abridged meeting report of the sixth plenary [Online]. Strasbourg: Council of Europe, 2011. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/TCY_2011_10E_PlenAbrMeetRep_V4%20_28Nov2011.pdf [2013, May 8]

The cybercrime convention committee (T-CY). Abridged meeting report of the seventh plenary [Online]. Strasbourg: Council of Europe, 2012. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/TCY_2012_14E_PlenAbrMeetRep.pdf [2013, May 8]

The cybercrime convention committee (T-CY). Assessment report: Implementation of the preservation provisions of the Budapest convention on cybercrime [Online]. Strasbourg: 2012. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/TCY2013/TCYreports/TCY_2012_10_Assess_report_v30_public.pdf [2013, May 6]

The cybercrime convention committee (T-CY). Full meeting report of the 4th multilateral consultation among the contracting states to the convention on cybercrime [online]. Strasbourg: Council of Europe, 2009. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TC-Y%282009%2906E.pdf [2013, May 6]

The cybercrime convention committee (T-CY). Meeting report of the 3rd consultation of the parties to the convention on cybercrime [Online]. Strasbourg: Council of Europe, 2008. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/T-CY%20%282008%29%2004%20E.pdf [2013, May 6]

The cybercrime convention committee (T-CY). Report of the 2nd multilateral consultation of the parties[Online]. Strasbourg: Council of Europe, 2007. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/T-CY%20%282007%29%2003%20E.pdf [2013, May 7]

The cybercrime convention committee (T-CY). Rules of procedure for the bureau [Online]. Strasbourg: Council of Europe, 2012. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/TCY_2012_24E_BU_Rules_Revised_Dec12%20.pdf [2013, May 8]

The economic crime division of the directorate general of human rights and legal affairs. Project on cybercrime: Final report [Online]. Strasbourg: Council of Europe, 2009. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20Project/567-d-final%20report1i%20final%20_15%20june%2009_.pdf [2013, May 8]

Urbas,G. and Choo, K.R. Resource material on technology-enabled crime. Technical and background paper no.28. AIC, 2008. Cited in Clough, J. Principles of cybercrime. UK: Cambridge University Press, 2010.

Verdelho,P. The effectiveness of international co-operation against cybercrime: examples of good practice [online]. Strasbourg: Council of Europe, Directorate general of human rights and legal affairs, Economic crime division, 2008. Available from: http://www.coe.int/t/dghl/standardsetting/t-cy/T-CY%20%282008%29%20DOC%20The%20effectiveness%20of%20international%20co-operation%20against%20cybercrime%20examples%20of%20good%20practice%20E.PDF [2013, May 6]

Weber, A.M. The council of Europe's convention on cybercrime. Berkeley Technology Law Journal Annual Review of Law and Technology 18,425 [Online] (2003). Available from: www.westlaw.com [2013, May 10]

ภาคผนวก

ภาคผนวก ก

Convention on Cybercrime

Budapest, 23.XI.2001

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia,* by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;

Recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of copyright and neighbouring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and

11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

Chapter I – Use of terms

Article 1 – Definitions

For the purposes of this Convention:

a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

c "service provider" means:

i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii any other entity that processes or stores computer data on behalf of such communication service or users of such service.

d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of devices

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a the production, sale, procurement for use, import, distribution or otherwise making available of:

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Title 2 – Computer-related offences

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a any input, alteration, deletion or suppression of computer data,

b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Title 3 – Content-related offences

Article 9 – Offences related to child pornography

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

a producing child pornography for the purpose of its distribution through a computer system;

b offering or making available child pornography through a computer system;

c distributing or transmitting child pornography through a computer system;

d procuring child pornography through a computer system for oneself or for another person;

e possessing child pornography in a computer system or on a computer-data storage medium.

2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:

a a minor engaged in sexually explicit conduct;

b a person appearing to be a minor engaged in sexually explicit conduct;

c realistic images representing a minor engaged in sexually explicit conduct.

3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

Title 4 – Offences related to infringements of copyright and related rights

Article 10 – Offences related to infringements of copyright and related rights

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international

obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Title 5 – Ancillary liability and sanctions

Article 11 – Attempt and aiding or abetting

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 12 – Corporate liability

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

a a power of representation of the legal person;

b an authority to take decisions on behalf of the legal person;

c an authority to exercise control within the legal person.

2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13 – Sanctions and measures

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Section 2 – Procedural law

Title 1 – Common provisions

Article 14 – Scope of procedural provisions

1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

a the criminal offences established in accordance with Articles 2 through 11 of this Convention;

b other criminal offences committed by means of a computer system; and

c the collection of evidence in electronic form of a criminal offence.

3 a. Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:

i is being operated for the benefit of a closed group of users, and

ii does not employ public communications networks and is not connected with another computer system, whether public or private,

that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15 – Conditions and safeguards

1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Title 2 – Expedited preservation of stored computer data

Article 16 – Expedited preservation of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17 – Expedited preservation and partial disclosure of traffic data

1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 3 – Production order

Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a

service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a the type of communication service used, the technical provisions taken thereto and the period of service;

b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Title 4 – Search and seizure of stored computer data

Article 19 – Search and seizure of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a a computer system or part of it and computer data stored therein; and

b a computer-data storage medium in which computer data may be stored

in its territory.

2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

a seize or similarly secure a computer system or part of it or a computer-data storage medium;

b make and retain a copy of those computer data;

c maintain the integrity of the relevant stored computer data;

d render inaccessible or remove those computer data in the accessed computer system.

4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5 – Real-time collection of computer data

Article 20 – Real-time collection of traffic data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party; or

ii to co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 – Interception of content data

1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party, or

ii to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Section 3 – Jurisdiction

Article 22 – Jurisdiction

1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

a in its territory; or

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

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

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

2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Chapter III – International co-operation

Section 1 – General principles

Title 1 – General principles relating to international co-operation

Article 23 – General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or

reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Title 2 – Principles relating to extradition

Article 24 – Extradition

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

b. Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7 a. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.

b. The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Title 3 – General principles relating to mutual assistance

Article 25 – General principles relating to mutual assistance

1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same

terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 26 – Spontaneous information

1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 a. Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

b. The central authorities shall communicate directly with each other;

c. Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;

d. The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9 a. In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b. Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c. Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d. Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e. Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28 – Confidentiality and limitation on use

1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:

a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

b not used for investigations or proceedings other than those stated in the request.

3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Section 2 – Specific provisions

Title 1 – Mutual assistance regarding provisional measures

Article 29 – Expedited preservation of stored computer data

1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2 A request for preservation made under paragraph 1 shall specify:

a the authority seeking the preservation;

b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

c the stored computer data to be preserved and its relationship to the offence;

d any available information identifying the custodian of the stored computer data or the location of the computer system;

e the necessity of the preservation; and

f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5 In addition, a request for preservation may only be refused if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

Article 30 – Expedited disclosure of preserved traffic data

1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

2 Disclosure of traffic data under paragraph 1 may only be withheld if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

Title 2 – Mutual assistance regarding investigative powers

Article 31 – Mutual assistance regarding accessing of stored computer data

1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.

3 The request shall be responded to on an expedited basis where:

a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 33 – Mutual assistance regarding the real-time collection of traffic data

1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.

2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34 – Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

Title 3 – 24/7 Network

Article 35 – 24/7 Network

1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a the provision of technical advice;

b the preservation of data pursuant to Articles 29 and 30;

c the collection of evidence, the provision of legal information, and locating of suspects.

2 a. A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b. If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

Chapter IV – Final provisions

Article 36 – Signature and entry into force

1 This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2 This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

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.

4 In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37 – Accession to the Convention

1 After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of

Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2 In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 38 – Territorial application

1 Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2 Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3 Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 39 – Effects of the Convention

1 The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:

– the European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24);

– the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30);

– the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).

2 If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

3 Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Article 40 – Declarations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27, paragraph 9.e.

Article 41 – Federal clause

1 A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.

2 When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.

3 With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

Article 42 – Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

Article 43 – Status and withdrawal of reservations

1 A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2 A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.

3 The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

Article 44 – Amendments

1 Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

2 Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3 The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.

4 The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

5 Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 45 – Settlement of disputes

1 The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.

2 In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46 – Consultations of the Parties

1 The Parties shall, as appropriate, consult periodically with a view to facilitating:

a the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

b the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

c consideration of possible supplementation or amendment of the Convention.

2 The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3 The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.

4 Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5 The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

Article 47 – Denunciation

1 Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2 Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 48 – Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

a any signature;

b the deposit of any instrument of ratification, acceptance, approval or accession;

c any date of entry into force of this Convention in accordance with Articles 36 and 37;

d any declaration made under Article 40 or reservation made in accordance with Article 42;

e any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.

ภาคผนวก ข

Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems

Strasbourg, 28.I.2003

The member States of the Council of Europe and the other States Parties to the Convention on Cybercrime, opened for signature in Budapest on 23 November 2001, signatory hereto;

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recalling that all human beings are born free and equal in dignity and rights;

Stressing the need to secure a full and effective implementation of all human rights without any discrimination or distinction, as enshrined in European and other international instruments;

Convinced that acts of a racist and xenophobic nature constitute a violation of human rights and a threat to the rule of law and democratic stability;

Considering that national and international law need to provide adequate legal responses to propaganda of a racist and xenophobic nature committed through computer systems;

Aware of the fact that propaganda to such acts is often subject to criminalisation in national legislation;

Having regard to the Convention on Cybercrime, which provides for modern and flexible means of international co-operation and convinced of the need to harmonise substantive law provisions concerning the fight against racist and xenophobic propaganda;

Aware that computer systems offer an unprecedented means of facilitating freedom of expression and communication around the globe;

Recognising that freedom of expression constitutes one of the essential foundations of a democratic society, and is one of the basic conditions for its progress and for the development of every human being;

Concerned, however, by the risk of misuse or abuse of such computer systems to disseminate racist and xenophobic propaganda;

Mindful of the need to ensure a proper balance between freedom of expression and an effective fight against acts of a racist and xenophobic nature;

Recognising that this Protocol is not intended to affect established principles relating to freedom of expression in national legal systems;

Taking into account the relevant international legal instruments in this field, and in particular the Convention for the Protection of Human Rights and Fundamental Freedoms and its Protocol No. 12 concerning the general prohibition of discrimination, the existing Council of Europe conventions on co-operation in the penal field, in particular the Convention on Cybercrime, the United Nations International Convention on the Elimination of All Forms of Racial Discrimination of 21 December 1965, the European Union Joint Action of 15 July 1996 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, concerning action to combat racism and xenophobia;

Welcoming the recent developments which further advance international understanding and co-operation in combating cybercrime and racism and xenophobia;

Having regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10-11 October 1997) to seek common responses to the developments of the new technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

Chapter I – Common provisions

Article 1 – Purpose

The purpose of this Protocol is to supplement, as between the Parties to the Protocol, the provisions of the Convention on Cybercrime, opened for signature in Budapest on 23 November 2001 (hereinafter referred to as “the Convention”), as regards the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

Article 2 – Definition

1 For the purposes of this Protocol:

> *"racist and xenophobic material"* means any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.

2 The terms and expressions used in this Protocol shall be interpreted in the same manner as they are interpreted under the Convention.

Chapter II – Measures to be taken at national level

Article 3 – Dissemination of racist and xenophobic material through computer systems

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

distributing, or otherwise making available, racist and xenophobic material to the public through a computer system.

2 A Party may reserve the right not to attach criminal liability to conduct as defined by paragraph 1 of this article, where the material, as defined in Article 2, paragraph 1, advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available.

3 Notwithstanding paragraph 2 of this article, a Party may reserve the right not to apply paragraph 1 to those cases of discrimination for which, due to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies as referred to in the said paragraph 2.

Article 4 – Racist and xenophobic motivated threat

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

threatening, through a computer system, with the commission of a serious criminal offence as defined under its domestic law, (i) persons for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or (ii) a group of persons which is distinguished by any of these characteristics.

Article 5 – Racist and xenophobic motivated insult

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

insulting publicly, through a computer system, (i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or (ii) a group of persons which is distinguished by any of these characteristics.

2 A Party may either:

a require that the offence referred to in paragraph 1 of this article has the effect that the person or group of persons referred to in paragraph 1 is exposed to hatred, contempt or ridicule; or

b reserve the right not to apply, in whole or in part, paragraph 1 of this article.

Article 6 – Denial, gross minimisation, approval or justification of genocide or crimes against humanity

1 Each Party shall adopt such legislative measures as may be necessary to establish the following conduct as criminal offences under its domestic law, when committed intentionally and without right:

distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity, as defined by international law and recognised as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 August 1945, or of any other international court established by relevant international instruments and whose jurisdiction is recognised by that Party.

2 A Party may either

a require that the denial or the gross minimisation referred to in paragraph 1 of this article is committed with the intent to incite hatred, discrimination or violence against any individual or group of individuals, based on race, colour, descent or

national or ethnic origin, as well as religion if used as a pretext for any of these factors, or otherwise

b reserve the right not to apply, in whole or in part, paragraph 1 of this article.

Article 7 – Aiding and abetting

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, aiding or abetting the commission of any of the offences established in accordance with this Protocol, with intent that such offence be committed.

Chapter III – Relations between the Convention and this Protocol

Article 8 – Relations between the Convention and this Protocol

1 Articles 1, 12, 13, 22, 41, 44, 45 and 46 of the Convention shall apply, *mutatis mutandis*, to this Protocol.

2 The Parties shall extend the scope of application of the measures defined in Articles 14 to 21 and Articles 23 to 35 of the Convention, to Articles 2 to 7 of this Protocol.

Chapter IV – Final provisions

Article 9 – Expression of consent to be bound

1 This Protocol shall be open for signature by the States which have signed the Convention, which may express their consent to be bound by either:

a signature without reservation as to ratification, acceptance or approval; or

b subject to ratification, acceptance or approval, followed by ratification, acceptance or approval.

2 A State may not sign this Protocol without reservation as to ratification, acceptance or approval, or deposit an instrument of ratification, acceptance or approval, unless it has already deposited or simultaneously deposits an instrument of ratification, acceptance or approval of the Convention.

3 The instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

Article 10 – Entry into force

1 This Protocol 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 have expressed their consent to be bound by the Protocol, in accordance with the provisions of Article 9.

2 In respect of any State which subsequently expresses its consent to be bound by it, the Protocol shall enter into force on the first day of the month following the expiration of a period of three months after the date of its signature without reservation as to ratification, acceptance or approval or deposit of its instrument of ratification, acceptance or approval.

Article 11 – Accession

1 After the entry into force of this Protocol, any State which has acceded to the Convention may also accede to the Protocol.

2 Accession shall be effected by the deposit with the Secretary General of the Council of Europe of an instrument of accession which shall take effect on the first day of the month following the expiration of a period of three months after the date of its deposit.

Article 12 – Reservations and declarations

1 Reservations and declarations made by a Party to a provision of the Convention shall be applicable also to this Protocol, unless that Party declares otherwise at the time of

signature or when depositing its instrument of ratification, acceptance, approval or accession.

2 By a written notification addressed to the Secretary General of the Council of Europe, any Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Articles 3, 5 and 6 of this Protocol. At the same time, a Party may avail itself, with respect to the provisions of this Protocol, of the reservation(s) provided for in Article 22, paragraph 2, and Article 41, paragraph 1, of the Convention, irrespective of the implementation made by that Party under the Convention. No other reservations may be made.

3 By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for in Article 5, paragraph 2.a, and Article 6, paragraph 2.a, of this Protocol.

Article 13 – Status and withdrawal of reservations

1 A Party that has made a reservation in accordance with Article 12 above shall withdraw such reservation, in whole or in part, as soon as circumstances so permit. Such withdrawal shall take effect on the date of receipt of a notification addressed to the Secretary General of the Council of Europe. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2 The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations in accordance with Article 12 as to the prospects for withdrawing such reservation(s).

Article 14 – Territorial application

1 Any Party may at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Protocol shall apply.

2 Any Party may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Protocol to any other territory specified in the declaration. In respect of such territory, the Protocol shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3 Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 15 – Denunciation

1 Any Party may, at any time, denounce this Protocol by means of a notification addressed to the Secretary General of the Council of Europe.

2 Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 16 – Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Protocol as well as any State which has acceded to, or has been invited to accede to, this Protocol of:

a any signature;

b the deposit of any instrument of ratification, acceptance, approval or accession;

c any date of entry into force of this Protocol in accordance with its Articles 9, 10 and 11;

d any other act, notification or communication relating to this Protocol.

In witness whereof the undersigned, being duly authorised thereto, have signed this Protocol.

Done at Strasbourg, this 28th day of January 2003, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Protocol, and to any State invited to accede to it.

ประวัติผู้เขียนวิทยานิพนธ์

นายณัฐพัฒน์ เลิศประพจน์กุล เกิดวันที่ 1 กุมภาพันธ์ 2529 ที่กรุงเทพมหานคร สำเร็จการศึกษาปริญญาตรี นิติศาสตรบัณฑิต จากคณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย เมื่อปีการศึกษา 2550 หลังจากนั้นจึงเข้ารับการศึกษาต่อในหลักสูตรนิติศาสตรมหาบัณฑิตที่จุฬาลงกรณ์มหาวิทยาลัย เมื่อ พ.ศ. 2551