บทที่ 2

อนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001

(Convention on Cyber Crime 2001)

แนวความคิดในการแก้ไขปัญหาทางคอมพิวเตอร์มีขึ้นมานานแล้ว ในระยะเริ่มแรกช่วงทศวรรษที่ 60 (ช่วงปี ค.ศ .1960-1970) มีการชี้ให้เห็นถึงอันตรายจากการกระทำความผิดผ่านทางคอมพิวเตอร์ ทั้งนี้ เนื่องจากหลายประเทศในแถบตะวันตกเริ่มมีการใช้คอมพิวเตอร์เป็นอุปกรณ์สำหรับเก็บบันทึก ถ่ายทอด และเชื่อมโยงฐานข้อมูลส่วนบุคคลของประชาชนในรัฐเข้าด้วยกัน ด้วยความกลัวว่ารัฐจะเริ่มคุกคามความเป็นส่วนตัวของประชาชน หรือจะถูกใช้เป็นเครื่องมือในควบคุมตรวจสอบพฤติกรรมของประชาชนโดยรัฐมากขึ้นเรื่อยๆ ความเข้าใจที่มีต่อการกระทำความผิดโดยมีคอมพิวเตอร์เข้าไปเกี่ยวข้อง จึงยังไม่ได้มีความหมายทำนองเดียวกับ "อาชญากรรมคอมพิวเตอร์" ที่เข้าใจกันในปัจจุบัน แต่หมายถึง "การกระทำความผิดใดๆที่เป็นอันตรายต่อข้อมูลข่าวสารและระดับความลับ หรือความเป็นส่วนตัวของแต่ละบุคคลที่อาจไม่ได้ต้องการเปิดเผยให้ผู้อื่นได้รับรู้" จะเห็นได้ว่าความผิดที่เกิดขึ้นจึงมักปรากฏในรูปแบบของการละเมิดข้อมูลส่วนบุคคลผ่านทางคอมพิวเตอร์ กฎหมายที่เกี่ยวข้องในยุคนี้ จึงมุ่งเน้นไปที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลไม่ใช่กฎหมายเพื่อป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์[1]

ยุคที่ 2 ในช่วงทศวรรษที่ 70 (ช่วงปี ค.ศ. 1970-1980) หรือที่เรียกว่า ยุคของอาชญากรรมเศรษฐกิจ[2] เนื่องจากการกระทำความผิดในช่วงเวลานั้นมีคอมพิวเตอร์เข้าไปเกี่ยวข้อง ซึ่งเป็นที่รู้จักกันในนาม White Collar Crimes หรือ อาชญากรรมเชิ้ตขาว[3] ผู้กระทำความผิดเป็นกลุ่มคนทำงานดี แต่งตัวดี หรือมีความรู้ความสามารถ ความเสียหายที่เกิดขึ้นจากการกระทำความผิดเกี่ยวข้องกับเศรษฐกิจของปัจเจกชน และประเทศชาติสังคมส่วนรวมเป็นลักษณะของการทำลายความเชื่อถือ ความมั่นคงทางเศรษฐกิจ เช่น ความผิดเกี่ยวกับการปลอมแปลงเงินตรา การปั่นหุ้น ความผิดเกี่ยวกับภาษีอากร องค์กรทางธุรกิจ สถาบันการเงิน หรือ

---

[1] Ulrich Sieber, Information Technology Crime: National Legislation and Internation Initiatives[online], 1994, Available from : http://www.datenschutzzentrum.de/vortraege/041118_weichert_dafta.htm[2009, March 7]

[2] พรทิพย์ ย่องอั้น, อาชญากรรมคอมพิวเตอร์ วิวัฒนาการของอาชญากรรมคอมพิวเตอร์[Online], แหล่งที่มา: http://learners.in.th/blog/mai8/177196[2552, มีนาคม 7]

[3] เรื่องเดียวกัน.

ธุรกิจการเงินนอกระบบ เป็นต้น[4] การกระทำความผิดอาจทำได้โดยอาศัยวิธีการเปลี่ยนแปลงข้อมูลผ่านคอมพิวเตอร์ไม่ว่าจะเป็นข้อมูลทางด้านการเงินของสถาบันการเงินหรือลูกค้าสถาบันการเงิน การเปลี่ยนแปลงรายรับและรายจ่ายของบริษัท หรือการเปลี่ยนแปลงงบดุลบัญชีบริษัท

จากสิ่งที่กล่าวมาจะเห็นได้ว่าการกระทำความผิดในยุคที่ 2 นั้น อาจเนื่องมาจากการที่ข้อมูลต่างๆโดยเฉพาะข้อมูลทางด้านการเงิน การบัญชี ข้อมูลลูกค้า ผลิตภัณฑ์ดิจิทัล โปรแกรม เกม เพลง ภาพยนตร์ หรือข้อมูลอื่นๆ ล้วนแต่มีคอมพิวเตอร์เป็นเครื่องมือสำคัญในการเก็บบันทึกและประมวลผล บวกกับความก้าวหน้าของเทคโนโลยีเครือข่ายคอมพิวเตอร์ การขยายตัวอย่างรวดเร็วของอินเทอร์เน็ต เครื่องมือต่างๆในการกระทำความผิดได้รับการพัฒนามากขึ้น วิธีการ และเป้าหมายแห่งการกระทำความผิดเปลี่ยนแปลงไปจากข้อมูลส่วนบุคคลไปสู่ข้อมูลระดับชาติและข้อมูลของสถาบันทางเศรษฐกิจที่สามารถสร้างความเสียหายในวงกว้างและมีมูลค่ามากมายมหาศาล

ยุคที่ 3 ทศวรรษที่ 70 (ช่วงปี ค.ศ. 1970-1980) กระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่เกิดขึ้นในยุคนี้ส่งผลกระทบต่อเศรษฐกิจโดยรวมของประเทศ โดยเฉพาะอย่างยิ่งในกลุ่มธุรกิจการเงิน ไม่ว่าจะเป็นการละเมิดลิขสิทธิ์ซอร์ฟแวร์ รวมถึงการละเมิดผลิตภัณฑ์ที่มีลิขสิทธิ์อื่นๆ ผ่านทางคอมพิวเตอร์ เช่น เพลง ภาพยนตร์ และเกมคอมพิวเตอร์

ยุคที่ 4 ทศวรรษที่ 80 (ช่วงปี ค.ศ. 1980-1990) มีการพัฒนาระบบคอมพิวเตอร์เพื่อใช้งานร่วมกับเครื่องมืออื่นๆ เช่น เครื่องเบิกเงินอัตโนมัติ หรือตู้เอทีเอ็ม รวมทั้งบัตรอิเล็กทรอนิกส์ประเภทต่างๆ เป้าหมายหลักของผู้กระทำความผิดจึงยังมุ่งไปที่ข้อมูลทางบัญชีของสถาบันการเงินการธนาคาร ในยุคนี้มีผู้เริ่มใช้งานระบบคอมพิวเตอร์ส่วนบุคคลมากขึ้นการละเมิดลิขสิทธิ์ซอร์ฟแวร์ไม่ว่าจะเป็นการทำซ้ำโปรแกรมซอร์ฟแวร์เพื่อจำหน่ายเนื่องจากทำให้มีราคาถูก จึงเพิ่มขึ้นตามไปด้วย

ทศวรรษที่ 90 จนถึงปัจจุบัน หรือที่เรียกได้ว่าเป็นยุคของอาชญากรรมไซเบอร์ (Cyber Crime)[5] เมื่อระบบคอมพิวเตอร์มีการเชื่อมต่อเครือข่ายมากขึ้น รวมถึงมีการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ต การกระทำความผิดที่เกิดขึ้นจึงมุ่งหมายไปยังสิ่งที่กฎหมายประสงค์จะคุ้มครอง เช่น

---

[4] วีระพงษ์ บุญโญภาส, อาชญากรรมทางเศรษฐกิจ Economic crime, พิมพ์ครั้งที่ 5 แก้ไขเพิ่มเติม-ปรับปรุงใหม่ (กรุงเทพมหานคร : นิติธรรม, 2549), หน้า 4-5.

[5] Ulrich Sieber, Information Technology Crime: National Legislation and Internation Initiatives[online]

การสร้างความเสียหายต่อประโยชน์สาธารณะ ค่านิยม แนวคิด สังคม รวมทั้งพัฒนาการของเด็กและเยาวชนโดยอาศัยระบบเครือข่ายอินเทอร์เน็ต และบางทีด้วยการติดต่อสื่อสารกันแบบนี้เองที่ทำให้เกิดการกระทำความผิดโดยการล่อลวงออกไปกระทำละเมิดในโลกทางกายภาพ ซึ่งการกระทำความผิดที่เกิดขึ้น ได้แก่ การเผยแพร่ข้อมูลที่ไม่ชอบด้วยกฎหมายไม่ว่าจะเป็นภาพลามกอนาจารเด็ก การพนันออนไลน์ การเผยแพร่ข้อมูลที่มีเนื้อหาหมิ่นประมาท

จากปัญหาในยุคต่างๆที่เกิดขึ้นเรื่อยมาจนถึงปัจจุบัน ความผิดที่เกิดขึ้นได้ถูกพัฒนาให้ควบคู่ไปกับความเจริญก้าวหน้าทางเทคโนโลยี สิ่งหนึ่งที่สามารถมองเห็นได้คือ การกระทำความผิดได้แพร่ขยายสู่วงกว้างจากระดับบุคคล ระดับประเทศ จนกระทั่งสามารถกระทำความผิดข้ามประเทศได้โดยผ่านทางเครือข่ายอินเทอร์เน็ต ปัญหาอาชญากรรมทางคอมพิวเตอร์ที่เกิดขึ้นจึงกลายเป็นปัญหาระดับนานาชาติที่ต้องตระหนักร่วมกัน จะเห็นได้จากการที่องค์กรระหว่างประเทศหลายองค์กรได้ให้ความสนใจเกี่ยวกับปัญหาอาชญากรรมทางคอมพิวเตอร์และได้ดำเนินการเพื่อหาแนวทางในการแก้ไขปัญหาร่วมกันทั้งในระดับพหุภาคี และทวิภาคีตามที่ผู้เขียนได้อธิบายในบทที่ 1 และสภายุโรป (Council of Europe : CoE)[6] ก็เป็นองค์กรหนึ่งที่ตระหนักถึงปัญหาอาชญากรรมทางคอมพิวเตอร์ดังกล่าว

ทั้งนี้ สภายุโรป[7] (Council of Europe : CoE) เป็นองค์กรหนึ่งที่เกิดจากความร่วมมือระหว่างประเทศในทวีปยุโรป ก่อตั้งขึ้นเมื่อวันที่ 5 พฤษภาคม ค.ศ. 1949 มีประเทศเริ่มก่อตั้ง 10 ประเทศ ซึ่งเป็นประเทศที่มีความต้องการรวมประเทศยุโรปเข้าด้วยกันเพื่อสถาปนาเป็นสหพันธรัฐยุโรป (European Federation) โดยวัตถุประสงค์หลักคือ การปกป้องสิทธิมนุษยชน การรวมประชาธิปไตยหลายฝ่ายเข้าด้วยกัน และการปฏิบัติตามกฎหมายร่วมกัน สมาชิกของสภายุโรปมีทั้งหมด 47 ประเทศ มีสำนักเลขาธิการตั้งอยู่ที่เมืองสตราสบูร์ก (Strasbourg) ประเทศฝรั่งเศส สภายุโรปมีการประชุมศาลสิทธิมนุษยชนแห่งยุโรปและสมาคมสิทธิมนุษยชนยุโรป โดยได้มีสัญญาร่วมกันในการระงับการก่อการร้าย องค์กรอาชญากรรม การรับรองการอพยพแรงงาน และการพิทักษ์สิทธิส่วนบุคคลของประชาชน รวมถึงการให้ความร่วมมือระหว่าง

---

[6] Council of Europe หมายถึง สภายุโรป ตั้งขึ้นโดยมีวัตถุประสงค์ในการสร้างความเป็นเอกภาพและเสริมสร้างความร่วมมือกันในยุโรป และมีบทบาทหน้าที่เฉพาะด้านการปกป้องคุ้มครองสิทธิมนุษยชน ปัญหาสังคมการศึกษาและวัฒนธรรม ส่วน Council of the European Union หมายถึง องค์กรสูงสุดของสหภาพยุโรป ประกอบด้วยผู้แทนระดับรัฐมนตรีของประเทศสมาชิก นอกจากนั้นยังมีการประชุมของผู้นำรัฐบาลปีละ 2 ครั้ง เพื่อกำหนดนโยบายสำคัญและพิจารณาเรื่องในกรอบความร่วมมือทางการเมือง อ้างถึงใน คณะกรรมการร่วม WTO สภาหอการค้าแห่งประเทศไทย สภาอุตสาหกรรมแห่งประเทศไทย สมาคมธนาคารไทย, [ออนไลน์], 2553, แหล่งที่มา: http://www.wtothailand.or.th/glossary.php?glossary_flag=c.[2553, มกราคม 11]

[7] หนังสือพิมพ์สยามรัฐ, สยามรัฐออนไลน์[ออนไลน์], 2007, แหล่งที่มา: http://www.siamrath.co.th/uifont/ArticleDetail.aspx?acid=4731[2009, December 8]

ประเทศ[8] เป็นต้น เมื่อทราบถึงองค์กรที่มีความสำคัญต่ออนุสัญญาฉบับนี้แล้วต่อไปในบทนี้จะได้ศึกษาถึงความเป็นมา แนวคิด ขอบเขตและวัตถุประสงค์ รวมถึงหลักกฎหมายและสาระสำคัญของอนุสัญญาเพื่อใช้เป็นแนวทางในการพิจารณาว่าประเทศไทยควรเข้าร่วมเป็นภาคีอนุสัญญาดังกล่าวนี้หรือไม่

2.1 ความเป็นมาของอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001

ปัญหาสำคัญในการบังคับใช้กฎหมายเพื่อป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์คือความบกพร่องของกฎหมายสารบัญญัติและกฎหมายสบัญญัติที่ไม่สอดคล้องและเป็นอุปสรรคต่อการดำเนินคดีกับอาชญากร และความบกพร่องของการให้ความร่วมมือในการดำเนินคดีกับอาชญากร[9] ซึ่งในปัจจุบันมีรูปแบบอาชญากรรมคอมพิวเตอร์รูปแบบใหม่มากมาย ด้วยเหตุนี้ทำให้สภายุโรป (Council of Europe) เล็งเห็นความสำคัญของปัญหาจึงได้จัดทำอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 (Convention on Cyber Crime 2001) ที่เปิดกว้างให้ทุกประเทศสามารถเป็นสมาชิกได้ อนุสัญญานี้นับว่าเป็นอนุสัญญาฉบับแรกที่ได้เล็งเห็นถึงความสำคัญในการแก้ไขปัญหาต่างๆในคดีอาชญากรรมทางคอมพิวเตอร์ที่จำเป็นต้องอาศัยกลไกทางกฎหมายที่ทันต่อสภาพทางเทคโนโลยีที่มีการพัฒนาอย่างรวดเร็วและต่อเนื่อง[10] เพื่อทำให้สามารถกำหนดหลักเกณฑ์และแนวทางในการแก้ไขปัญหาได้อย่างมีประสิทธิภาพ

---

[8] Bangkok Online[Online], 2009, Available from: http://www.bkkonline.com/library/words/c3.html[2009, May 12]

[9] Amalie M. Weber, The Council of Europe's Convention on Cybercrime. Berkeley Technology Law Journal[Online], 2009, Available from: http://web2.westlaw.com/find/default.wl?vc=0&ordoc=0294482133&rp=%2ffind%2fdefault.wl&DB=PROFILER%2DWLD&DocName=0359039001&FindType=h&AP=&rs=WLW9.06&ifm=NotSet&fn=_top&sv=Split&mt=WorldJournals&utid=%7b36BA29DA-8CCF-4AA9-944F-4DE19F7D6615%7d&vr=2.0&pbc=576C45B[2009, January 22], p 2.

[10] Shannon L. Hopkins, Cybercrime Convention : a Positive Beginning to a Long Road Ahead. Journal of High Technology Law. [Online], 2003, Available from http://web2.westlaw.com/Find/Default.wl?DB=PROFILER%2DWLD&DocName=0344186601&FindType=h&AP=&mlac=FY&rs=WLW9.06&ifm=NotSet&fn=_top&sv=Split&mt=WorldJournals&utid=%7b36BA29DA-8CCF-4AA9-944F-4DE19F7D6615%7d&vr=2.0&pbc=B8E07AFE[2009, January 22], p 1.

อนุสัญญานี้เริ่มต้นจากการที่สภายุโรปได้จัดตั้งคณะกรรมาธิการผู้เชี่ยวชาญด้านอาชญากรรมทางคอมพิวเตอร์ (Committee of Experts for Computer-related Crime) ขึ้นในปี ค.ศ. 1985 เพื่อพิจารณามาตรการและแนวทางในการบัญญัติกฎหมายโดยคณะกรรมาธิการได้หารือและจัดทำ Recommendation No. R (89) 9 และได้รับการรับรองจากที่ประชุมคณะมนตรีเมื่อวันที่ 13 กันยายน ค.ศ. 1989 ซึ่ง Recommendation ดังกล่าว มีวัตถุประสงค์เพื่อกำหนดกรอบในการพิจารณาทบทวนกฎหมายภายในของประเทศสมาชิก ให้ครอบคลุมลักษณะการกระทำที่ควรบัญญัติเป็นความผิดอย่างน้อยจำนวน 8 ฐานความผิด (Minimum List) ได้แก่ การฉ้อโกงทางคอมพิวเตอร์ การปลอมแปลงทางคอมพิวเตอร์ การทำลายข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ การรบกวนการทำงานของคอมพิวเตอร์หรือระบบโทรคมนาคม การเข้าถึงโดยมิชอบ การดักรับข้อมูลโดยมิชอบ การทำซ้ำโปรแกรมคอมพิวเตอร์โดยมิชอบ และการทำซ้ำลายพิมพ์วงจรโดยมิชอบ (Unauthorized Reproduction of a Topography) และยังมีความผิดอื่นที่กำหนดให้เป็นทางเลือกที่จะบัญญัติเป็นกฎหมายภายในอีก 4 ฐานความผิด ได้แก่ การเปลี่ยนแปลงข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ การจารกรรมทางคอมพิวเตอร์ การใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์โดยมิชอบ และการใช้โปรแกรมคอมพิวเตอร์ที่ได้รับความคุ้มครองโดยมิชอบ นอกจากนี้ ได้กำหนดมาตรการเพื่อให้ประเทศสมาชิกรายงานเกี่ยวกับการพัฒนากฎหมายภายในที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ต่อคณะกรรมาธิการด้านปัญหาอาชญากรรม (European Committee on Crime Problems : CDPC) และรายงานผลการพัฒนากฎหมาย แนวคำตัดสินของศาลและประสบการณ์ด้านความร่วมมือระหว่างประเทศที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ในช่วงปี 1993 ต่อเลขาธิการสภายุโรป[11]

ต่อมาในปี ค.ศ. 1995 คณะกรรมาธิการผู้เชี่ยวชาญด้านอาชญากรรมทางคอมพิวเตอร์ ก็ได้ออก Recommendation No. R (95) 13* เพื่อชี้ให้เห็นถึงปัญหาและแนวทางการแก้ไขปัญหา

---

[11] สำนักงานเลขาธิการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, แนวทางการจัดทำกฎหมายอาชญากรรมทางคอมพิวเตอร์, [ออนไลน์], 11 มกราคม 2553, แหล่งที่มา http://www.lawreform.go.th, หน้า 53.

* Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with Information Technology

I. Search and seizure

2. Criminal procedure laws should permit investigating authorities to search computer systems and seize data under similar conditions as under traditional powers of search and seizure...

II. Technical Surveillance

5. ....., law pertaining to technical surveillance for the purpose of criminal investigations, such as interception of telecommunications, should be reviewed and amended, where necessary, to ensure their applicability

และแนวทางแก้ไขกฎหมายวิธีพิจารณาความที่เกี่ยวกับเทคโนโลยีสารสนเทศ เช่น อำนาจการตรวจค้น การยึด และการใช้วิธีการทางเทคนิคในการสืบสวนสอบสวน เช่น การดักฟังการติดต่อผ่านระบบโทรคมนาคม การรวบรวมข้อมูลจราจรทางคอมพิวเตอร์ การเข้ารหัสลับข้อมูล รวมไปถึงการเก็บรวบรวมและนำเสนอพยานหลักฐานที่อยู่ในรูปอิเล็กทรอนิกส์ การตั้งหน่วยงานพิเศษเพื่อการสืบสวนสอบสวนการกระทำความผิด และโครงการฝึกอบรมบุคลากรที่เกี่ยวข้องกับกระบวนการยุติธรรมให้มีความเชี่ยวชาญเฉพาะทางด้านอาชญากรรมทางคอมพิวเตอร์ อีกทั้งยังได้กล่าวถึงความร่วมมือระหว่างประเทศในการสืบสวนสอบสวนด้วย

นอกจาก Recommendation ทั้ง 2 ข้อดังกล่าวที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์โดยตรงแล้ว อนุสัญญานี้ยังให้ความสำคัญกับข้อเสนอแนะอื่นๆที่เกี่ยวข้อง ไม่ว่าจะเป็น Recommendations No. R (85) 10 เกี่ยวกับการบังคับใช้ในทางปฏิบัติของอนุสัญญาของสภายุโรปว่าด้วยการช่วยเหลือซึ่งกันและกันในคดีอาญาสำหรับประเด็นว่าด้วยการดักข้อมูลของการติดต่อสื่อสารทางโทรคมนาคม Recommendations No. R (88) 2 ว่าด้วยการละเมิดลิขสิทธิ์และสิทธิข้างเคียง Recommendations No. R (87) 15 ว่าด้วยหลักเกณฑ์การใช้ข้อมูลส่วนบุคคลโดยตำรวจ และ Recommendations No. R (95) 4 ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในกิจการโทรคมนาคมเฉพาะในกิจการโทรศัพท์*

ต่อมาได้มีมติรับเอาบันทึกหลักการ (Explanatory Report) แห่งร่างอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ในสมัยประชุมที่ 109 เมื่อวันที่ 8 พฤศจิกายน ค.ศ. 2001 และได้เปิดให้ประเทศต่างๆลงนาม ณ กรุงบูดาเปส ประเทศฮังการี เมื่อวันที่ 23 พฤศจิกายน ค.ศ. 2001 โดยอนุสัญญาฉบับนี้เริ่มมีผลบังคับใช้ตั้งแต่วันที่ 1 กรกฎาคม ค.ศ. 2004 เมื่อมีรัฐให้สัตยาบันแก่อนุสัญญาไปแล้ว 5 รัฐ โดยในจำนวนดังกล่าวต้องมีประเทศสมาชิกของสภายุโรป

III. Obligations to co-operate with the investigating authorities...

IV. Electronic Evidence...

VII. International Cooperation...

* Preamble of Convention on Cyber Crime 2001

...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...

อย่างน้อยสามประเทศ* ทั้งนี้อนุสัญญาฉบับนี้ได้เปิดกว้างให้ทั้งประเทศสมาชิกและประเทศอื่นๆ ที่มิได้เป็นสมาชิกของสภายุโรปลงนามในอนุสัญญา**

อนุสัญญาฉบับนี้มีประเทศภาคีสมาชิกรวมทั้งสิ้น 46 ประเทศ*** โดยแบ่งเป็นประเทศที่มีการลงนามแต่ยังมิได้มีการให้สัตยาบัน และประเทศที่มีการลงนามและให้สัตยาบัน ดังนี้

1. ประเทศที่มีการลงนามแต่ยังมิได้มีการให้สัตยาบัน จำนวน 20 ประเทศ ดังนี้ ออสเตรีย อาเซอร์ไบจาน เบลเยี่ยม สาธารณรัฐเช็ก จอร์เจีย กรีซ ไอร์แลนด์ ลิกเตนสไตน์ ลักแซมเบิร์ก มอลตา มอนเตนิโกร โปแลนด์ โปรตุเกส สเปน สวีเดน สวิตเซอร์แลนด์ สหราชอาณาจักร แคนาดา ญี่ปุ่น แอฟฟริกาใต้

2. ประเทศที่มีการลงนามและให้สัตยาบัน จำนวน 26 ประเทศ ดังนี้ แอลแบเนีย อาร์เมเนีย บอสเนียและเฮอร์เซโกวินา บัลแกเรีย โครเอเชีย ไซปรัส เดนมาร์ก เอสโตเนีย ฟินแลนด์ ฝรั่งเศส เยอรมัน ฮังการี ไอซ์แลนด์ อิตาลี ลัตเวีย ลิทัวเนีย มอลโดวา เนเธอร์แลนด์ นอร์เวย์ โรมาเนีย เซอร์เบีย สโลวาเกีย สโลวีเนีย มาซิโดเนีย ยูเครน สหรัฐอเมริกา

จากหลักการต่างๆที่อนุสัญญาได้คำนึงถึงในขั้นตอนการร่างอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 จึงถือได้ว่าเป็นอนุสัญญาที่มีความสำคัญมีการวางกรอบในการกำหนดการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ รวมถึงวิธีการปฏิบัติทางด้านกฎหมาย ทั้งนี้ การจัดทำอนุสัญญาดังกล่าวยังมีเหตุผลอันเนื่องจากเห็นว่าการเปลี่ยนแปลงของสังคมในเชิงลึกที่เกิดจากระบบของตัวเลข (Digitalization) การหลอมรวมสื่อ (Convergence) และการพัฒนาของโลกอย่างต่อเนื่องเกี่ยวกับระบบเครือข่ายคอมพิวเตอร์**** ส่งผลให้ประเทศ

---

* Article 36 – Signature and entry into force

...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.

** 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

*** ตารางที่ 1 รายชื่อประเทศภาคีและหน่วยงานที่มีอำนาจหน้าที่ตามอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 ท้ายบทที่ 2, หน้า 78.

**** เครือข่ายคอมพิวเตอร์ เกิดจากการนำเครื่องคอมพิวเตอร์ตั้งแต่ 2 เครื่องขึ้นไปมาต่อพ่วงกันเพื่อประโยชน์ในการส่งหรือรับข้อมูลอิเล็กทรอนิกส์ โดยสามารถจำแนกตามระยะทางของการเชื่อมต่อระหว่างอุปกรณ์สื่อสารได้เป็น 3 ประเภท ดังนี้

ต่างๆ เกิดความกังวลว่าเครือข่ายของคอมพิวเตอร์และข้อมูลอิเล็กทรอนิกส์นั้นอาจถูกใช้เพื่อการกระทำความผิดทางอาญา และเกิดความเสี่ยงเกี่ยวกับพยานหลักฐานที่เกี่ยวเนื่องกับการกระทำความผิดอาจจะถูกเก็บหรือส่งต่อทางเครือข่ายคอมพิวเตอร์ จึงมีความจำเป็นที่จะต้องแสวงหานโยบายร่วมกันทางอาญาที่มุ่งหมายในการคุ้มครองสังคมให้ปลอดภัยจากอาชญากรรมทางคอมพิวเตอร์ โดยนอกจากวิธีการอื่นๆ แล้ว ต้องจัดให้มีบทบัญญัติทางกฎหมายที่เหมาะสมและสอดคล้องกันและการให้การสนับสนุนทางด้านความร่วมมือระหว่างประเทศ ไม่ว่าจะเป็นความร่วมมือระหว่างประเทศและความร่วมมือระหว่างกิจการภาคเอกชนในการต่อต้านอาชญากรรมทางคอมพิวเตอร์ และความจำเป็นที่จะต้องคุ้มครองผลประโยชน์อันชอบธรรมในการใช้และการพัฒนาเทคโนโลยีสารสนเทศ* เพื่อให้สามารถเก็บรวบรวมพยานหลักฐานเกี่ยวกับการกระทำความผิดได้ทันเวลา

2.2 ขอบเขตและวัตถุประสงค์ของอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001

อนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 เป็นอนุสัญญาที่จัดทำขึ้นโดยมีความต้องการเพื่อที่จะยับยั้งการกระทำที่จะก่อให้เกิดผลกระทบโดยตรงต่อข้อมูลความลับ ความเที่ยงตรง และความมีอยู่ของระบบคอมพิวเตอร์ เครือข่ายและข้อมูลคอมพิวเตอร์ตลอดจนการกระทำที่เป็นการใช้ระบบเครือข่ายและข้อมูลดังกล่าวโดยมิชอบ การปราบปรามอาชญากรรมโดยกำหนดให้ประเทศภาคีของอนุสัญญากำหนดให้การกระทำดังกล่าวเป็นความผิด

---

1. Local Area Network : LAN เป็นระบบที่มีการเชื่อมต่ออุปกรณ์สื่อสารในระยะทางที่จำกัด ซึ่งมีความเร็วในการแลกเปลี่ยนข้อมูลสูงเป็นเครือข่ายที่ใช้ในหน่วยงานต่างๆเฉพาะกลุ่ม จึงเป็นระบบเครือข่ายแบบปิด (Close Network) เช่น ระบบอินทราเน็ต (Intranet) เป็นต้น

2. Metropolitan Area Network : MAN เป็นระบบเครือข่ายคอมพิวเตอร์ขนาดใหญ่ครอบคลุมพื้นที่มากกว่าระบบเครือข่ายแบบ LAN เครือข่ายนี้เกิดจากการเชื่อมต่อของเครือข่ายคอมพิวเตอร์แบบ LAN ตั้งแต่ 2 เครือข่ายเข้าด้วยกัน

3. Wide Area Network : WAN เป็นระบบเครือข่ายคอมพิวเตอร์ที่มีขนาดใหญ่ ประกอบด้วยเครือข่ายทั้งแบบ LAN และ MAN พื้นที่ของเครือข่ายสามารถครอบคลุมพื้นที่ได้ในระดับประเทศ หรือระดับโลก และเป็นเครือข่ายแบบเปิด (Open Network) เช่น ระบบเครือข่ายอินเทอร์เน็ต (Internet)

* Preamble of Convention on Cyber Crime 2001

...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...

ทางอาญาเพื่อบังคับใช้กับบุคคลธรรมดาและนิติบุคคลที่อยู่ภายในอาณาเขตหรือเขตอำนาจของประเทศภาคี รวมทั้งการกำหนดมาตรการเกี่ยวกับหน่วยงานที่มีอำนาจหน้าที่ในการปราบปรามการกระทำความผิดทางอาญาดังกล่าวโดยการตรวจสอบ การสืบสวนสอบสวน การฟ้องร้องดำเนินคดีทั้งในระดับประเทศและระดับระหว่างประเทศ และมาตรการด้านความร่วมมือระหว่างประเทศ ทั้งการส่งผู้ร้ายข้ามแดน การช่วยเหลือซึ่งกันและกัน ทั้งนี้ การใช้อำนาจดังกล่าวยังขยายขอบเขตการบังคับใช้กฎหมายให้ครอบคลุมถึงการกระทำความผิดของบุคคลที่มีสัญชาติของประเทศภาคีซึ่งได้กระทำนอกอาณาเขตของตน* ให้ได้รับการลงโทษ

อนุสัญญาฉบับนี้ มีวัตถุประสงค์หลัก 3 ประการ[12] ด้วยกันคือ

1. ความต้องการให้เกิดความสอดคล้องของกฎหมายภายในของประเทศภาคี ทั้งทางด้านกฎหมายสารบัญญัติในการกำหนดฐานความผิด องค์ประกอบความผิด และมาตรการอื่นที่เกี่ยวข้อง ซึ่งเป็นการพยายามวางมาตรฐานขั้นต่ำ หรือการกำหนดฐานความผิดทั้งหลายที่เกี่ยวกับคอมพิวเตอร์อันบรรดาประเทศสมาชิกที่ลงนามไว้แล้ว จะต้องนำกลับไปพิจารณาและบัญญัติไว้ในกฎหมายภายในประเทศตน เพื่อให้ฐานความผิดต่างๆมีความสอดคล้องต้องกันและมีความยืดหยุ่นเพียงพอสำหรับเทคโนโลยีที่มีการพัฒนาอย่างต่อเนื่อง

2. การกำหนดมาตรการเกี่ยวกับอำนาจหน้าที่ที่เพียงพอต่อการดำเนินการปราบปรามความผิดทางอาญาในส่วนของความผิดที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ ไม่ว่าจะเป็นมาตรการในการสืบสวนสอบสวน การเก็บรวบรวมพยานหลักฐานที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์เพื่อให้สามารถฟ้องร้องดำเนินคดีกับผู้กระทำความผิด

3. การพัฒนาหลักความร่วมมือระหว่างประเทศให้มีความรวดเร็วและมีประสิทธิภาพทั้งในกรณีการให้ความช่วยเหลือในทางอาญา การส่งผู้ร้ายข้ามแดน และปัญหาเรื่องเขตอำนาจศาล เป็นต้น

---

* 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:...

...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.

[12] Shannon L. Hopkins, Cybercrime Convention : a Positive Beginning to a Long Road Ahead, Journal of High Technology Law. [Online], 2003, p 2.

2.3 หลักการและสาระสำคัญของอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001

อนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 เป็นอนุสัญญาที่กำหนดให้มีข้อพึงปฏิบัติของประเทศภาคีหลายประการไม่ว่าจะเป็น การกำหนดฐานความผิดเกี่ยวกับคอมพิวเตอร์เพื่อคุ้มครองความปลอดภัยของข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ มาตรการที่ประเทศภาคีพึงจัดให้มีภายในประเทศทางด้านต่างๆไม่ว่าจะเป็นมาตรการทางด้านความร่วมมือระหว่างประเทศ มาตรการในการส่งผู้ร้ายข้ามแดน จะเห็นได้ว่าข้อกำหนดต่างๆในอนุสัญญาได้บัญญัติไว้ค่อนข้างกว้าง พันธกรณีที่เกิดแก่รัฐภาคีมักจะปรากฏวลีที่ว่า "ในขอบเขตที่กว้างที่สุดเท่าที่จะเป็นไปได้" (...to the widest extent possible for the propose...)* บางบทบัญญัติก็กำหนดพันธกรณีให้ตกอยู่ภายใต้บทบัญญัติทางกฎหมายภายในของรัฐที่เป็นประเทศภาคี อย่างไรก็ตามในการทำความเข้าใจอนุสัญญานี้ สิ่งที่สำคัญจะต้องทราบคือความหมายและคำจำกัดความ รวมถึงมาตรการต่างๆที่ก่อให้เกิดพันธกรณีกับประเทศภาคี เพื่อการปฏิบัติให้สอดคล้องกันตามวัตถุประสงค์ของอนุสัญญา

2.3.1. ความหมายและคำจำกัดความ

อนุสัญญานี้มุ่งคุ้มครองข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ จึงได้ให้นิยามเกี่ยวกับสิ่งต่างๆ ไว้ดังนี้

1. ระบบคอมพิวเตอร์ (Computer System) หมายถึง อุปกรณ์ (Device) หรือกลุ่มของอุปกรณ์ที่มีเชื่อมโยงระหว่างกันหรือมีความเกี่ยวข้องกัน การเชื่อมโยงกันของอุปกรณ์อันหนึ่งหรือหลายอันในกลุ่มนั้นเป็นไปตามโปรแกรมคอมพิวเตอร์ ซึ่งทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ (Article 1 (a))

จากความหมายดังกล่าวข้างต้นที่กำหนดไว้ในอนุสัญญายังไม่มีการจำกัดความและขอบเขตของคำว่า อุปกรณ์หรือกลุ่มอุปกรณ์ ว่าควรหมายถึงสิ่งใดบ้าง ด้วยเหตุนี้ ไม่ว่าจะเป็นโทรศัพท์เคลื่อนที่ หรือเคเบิ้ลทีวี อาจอยู่ภายใต้ความหมายของคำว่าอุปกรณ์หรือกลุ่มอุปกรณ์

---

* Article 23

The Parties shall co-operate with each other,..., to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data,....

Article 25

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,...

ดังกล่าวได้เช่นกัน[13] แต่ทั้งนี้ จากวัตถุประสงค์ของอนุสัญญาที่ต้องการให้การกำหนดฐานความผิดมีความยืดหยุ่นพอสำหรับเทคโนโลยีที่มีการพัฒนาอย่างต่อเนื่อง อุปกรณ์และกลุ่มของอุปกรณ์ที่เชื่อมโยงระหว่างกันหรือเกี่ยวข้องกันใดๆ จึงน่าจะหมายความรวมถึงการพัฒนาทางเทคโนโลยีของโทรศัพท์เคลื่อนที่และอุปกรณ์เคลื่อนที่ต่างๆ ที่ทำงานผ่านเครือข่ายไร้สายในปัจจุบัน ที่สามารถรองรับการเชื่อมต่ออินเทอร์เน็ตและสามารถทำการประมวลผลได้เช่นเดียวกับคอมพิวเตอร์ซึ่งอาจขึ้นอยู่กับข้อเท็จจริงหากมีการกระทำความผิดเกิดขึ้น

ทั้งนี้ จากคำจำกัดความถึงนิยามของคำว่า ระบบคอมพิวเตอร์ ดังกล่าวข้างต้น จะเห็นได้ว่าอนุสัญญานี้มุ่งคุ้มครองและป้องกันการเกิดอาชญากรรมทางคอมพิวเตอร์โดยเฉพาะ จากความหมายของ ระบบคอมพิวเตอร์ ข้างต้นจึงน่าจะหมายถึงอุปกรณ์และกลุ่มอุปกรณ์ที่มีความเกี่ยวข้องกับคอมพิวเตอร์ หรือที่เชื่อมโยงระหว่างการใช้งานเกี่ยวกับคอมพิวเตอร์เท่านั้น ซึ่งได้แก่ ฮาร์ดแวร์และซอฟแวร์ที่พัฒนาขึ้นเพื่อประมวลผลข้อมูลดิจิทัล ประกอบด้วยเครื่องคอมพิวเตอร์และอุปกรณ์รอบข้าง ที่ใช้ในการรับเข้าหรือป้อนข้อมูล นำออกหรือแสดงผลข้อมูล และบันทึกหรือเก็บข้อมูล ซึ่งในทางปฏิบัติทั่วไปคอมพิวเตอร์ไม่ว่าจะอยู่ในรูปแบบใดก็ตาม จะมีการทำงานเป็นระบบ ซึ่งจะประกอบด้วยการทำงานของ 3 ระบบ รวมกัน ได้แก่

1) ฮาร์ดแวร์ เป็นอุปกรณ์ที่ประกอบเป็นคอมพิวเตอร์ และอุปกรณ์เสริมอื่นๆ ที่เกี่ยวข้องกับคอมพิวเตอร์ ซึ่งสามารถมองเห็นและจับต้องได้ เช่น เครื่องพิมพ์ จอภาพ เครื่องอ่าน/เขียนแผ่นซีดี เป็นต้น

2) ซอฟแวร์ เป็นชุดคำสั่งหรือโปรแกรมที่สั่งการให้คอมพิวเตอร์ทำงานตามที่ต้องการ

3) บุคลากรทางคอมพิวเตอร์ ได้แก่บุคคลที่ทำงานเกี่ยวข้องกับคอมพิวเตอร์

ทั้งนี้ มีเครือข่ายเป็นสิ่งที่เชื่อมต่อระหว่างกันของทั้งสามระบบ

2. ข้อมูลคอมพิวเตอร์ (Computer Data) หมายถึง สิ่งที่ใช้เป็นตัวแสดงออกของข้อเท็จจริง ข้อมูลหรือความคิด ในรูปแบบที่เหมาะจะใช้ในการประมวลผล ลงในระบบคอมพิวเตอร์ รวมถึงโปรแกรมคอมพิวเตอร์ในรูปแบบที่เหมาะจะทำให้ระบบคอมพิวเตอร์ทำงานได้ (Article 1 (b))

---

[13] Shannon L. Hopkins, Cybercrime Convention : a Positive Beginning to a Long Road Ahead. Journal of High Technology Law. [Online], 2003, p. 4.

จากความหมายดังกล่าวข้างต้นยังมีความไม่ชัดเจนและคงเป็นเรื่องยากที่จะบอกว่าสิ่งที่ใช้แสดงออกของข้อมูลและทำให้คอมพิวเตอร์สามารถประมวลผลหรือทำหน้างานได้นั้นหมายถึงสิ่งใด ตัวอย่างเช่น Barcode ที่ติดไว้กับสินค้าเพื่อทำการสแกนในร้านค้าหรือซุปเปอร์มาร์เก็ตจะรวมอยู่ในความหมายของข้อมูลคอมพิวเตอร์หรือไม่[14] ทั้งนี้ ผู้เขียนให้ข้อสังเกตว่าข้อมูลสุดท้ายที่มีการเตรียมในกระดาษก่อนทำการบันทึกและจัดเก็บในคอมพิวเตอร์จะถือว่าเป็นสิ่งที่อยู่ในรูปแบบที่เหมาะจะใช้ในการประมวลผลหรือไม่

3. ผู้ให้บริการ (Service Provider) หมายถึง หน่วยงานของรัฐหรือของเอกชน ซึ่งจัดให้ผู้ใช้บริการสามารถติดต่อสื่อสารกันได้โดยวิธีการของระบบคอมพิวเตอร์ และรวมถึงหน่วยงานอื่นๆที่ทำหน้าที่ประมวลผลข้อมูลคอมพิวเตอร์ในนามของการให้บริการทางการติดต่อสื่อสาร หรือหน่วยงานที่ทำหน้าที่เก็บรักษาข้อมูลของผู้ใช้บริการคอมพิวเตอร์ในนามของการให้บริการทางการติดต่อสื่อสาร (Article 1 (c))

การที่อนุสัญญานี้ต้องมีการให้คำนิยามเกี่ยวกับผู้ให้บริการนั้น อาจเนื่องจากผู้ให้บริการอินเทอร์เน็ตมีความสำคัญในการติดต่อสื่อสาร หากผู้ใช้งานระบบคอมพิวเตอร์มีความต้องการในการเชื่อมต่อเครือข่ายหรือต้องการเชื่อต่ออินเทอร์เน็ต จะต้องทำผ่านองค์กรที่เรียกว่าผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider : ISP) ซึ่งสามารถแบ่งประเภทของผู้ให้บริการได้ดังนี้[15]

1) ผู้ให้บริการอินเทอร์เน็ตระหว่างประเทศ (International Service Providers) เป็นผู้ให้บริการอินเทอร์เน็ตระดับชั้นบนสุด ซึ่ง ISP ประเภทนี้จะทำการเชื่อมต่อเครือข่ายกันในระดับระหว่างประเทศ เช่น ระหว่าง ISP ในประเทศไทย กับ ISP ในประเทศสหรัฐอเมริกา เป็นต้น

2) ผู้ให้บริการอินเทอร์เน็ตภายในประเทศ (National Service Providers : NSP) เป็นผู้ให้บริการสำหรับภายในประเทศนั้นๆ โดยจะสร้างเป็นเครือข่ายหลักของแต่ละประเทศ ในแต่ละประเทศสามารถมีผู้ให้บริการอินเทอร์เน็ตภายในประเทศได้หลายหน่วยงาน เช่น ในประเทศสหรัฐอเมริกามีบริษัท SprintLink, PSINet, UUNet Technology, MCI เป็นต้น ทั้ง

---

[14] Ibid., p. 4.

[15] ฟอโรซาน, บีห์รูซ เอ. แปลโดย จักกริช พฤษการ, การสื่อสารข้อมูลและเครือข่ายคอมพิวเตอร์, (กรุงเทพ : ท้อป, 2549) หน้า 12-13.

เครือข่ายของผู้ให้บริการอินเทอร์เน็ตระหว่างประเทศและภายในประเทศสามารถเชื่อมต่อกันได้โดยกระทำผ่าน Network Access Point (NAP)

3) ผู้ให้บริการอินเทอร์เน็ตภายในภูมิภาค (Regional Internet Service Providers) ในประเทศใหญ่จะมีผู้ให้บริการอินเทอร์เน็ตในแต่ละภูมิภาคด้วย ซึ่งจะเป็นบริษัทที่มีขนาดไม่ใหญ่มากนัก เนื่องจากจะให้บริการสำหรับภูมิภาคนั้นๆ โดยที่เครือข่ายของผู้ให้บริการอินเทอร์เน็ตภายในภูมิภาคนั้นจะต้องทำการเชื่อมต่อกับ NSP เพื่อที่จะให้สามารถรับส่งข้อมูลกันได้ทั้งระหว่างประเทศและภายในประเทศด้วย

4) ผู้ให้บริการอินเทอร์เน็ตภายในท้องถิ่น (Local Internet Service Providers) โดยปกติแล้วผู้ใช้บริการทั่วไปจะทำการเชื่อมต่อคอมพิวเตอร์ของตนเองเข้ากับผู้ให้บริการอินเทอร์เน็ตภายในท้องถิ่น ซึ่งเครือข่ายภายในท้องถิ่นจะเชื่อมต่อเครือข่ายของตนเองไปยังระดับภูมิภาค และระดับประเทศต่อไป ผู้ให้บริการอินเทอร์เน็ตภายในท้องถิ่นนั้นอาจเป็นบริษัทขนาดเล็กที่ให้บริการอินเทอร์เน็ตในท้องที่นั้นๆ หรือองค์กรต่างๆ ภายในพื้นที่ที่สามารถให้บริการอินเทอร์เน็ตได้ เช่น โรงเรียน วิทยาลัย หรือมหาวิทยาลัย เป็นต้น

จากประเภทของผู้ให้บริการเห็นได้ว่าความเชื่อมโยงของการกระทำความผิดระหว่างประเทศสามารถเกิดขึ้นได้โดยง่าย เนื่องจากมีการเชื่อมต่อระหว่างเครือข่ายของผู้ให้บริการในระดับต่างๆนั่นเอง อีกทั้งในอนุสัญญาได้มีการกำหนดให้ประเทศภาคีกำหนดให้มีหน่วยงานที่ทำหน้าที่เก็บรักษาข้อมูล ซึ่งหน่วยงานที่ว่าได้แก่ ผู้ให้บริการ การกำหนดให้ผู้ให้บริการมีหน้าที่เก็บรักษาข้อมูล เนื่องจากข้อมูลที่ทำการเก็บรักษานั้นมีความสำคัญในการสืบสวนสอบสวนและรวบรวมพยานหลักฐานเพื่อดำเนินคดีกับผู้กระทำความผิด ซึ่งผู้เขียนจะได้อธิบายต่อไป

4. ข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) หมายถึง ข้อมูลคอมพิวเตอร์ใดๆที่เกี่ยวข้องกับการติดต่อสื่อสารโดยวิธีการทางคอมพิวเตอร์ ซึ่งเกิดขึ้นโดยระบบคอมพิวเตอร์และถูกจัดอยู่ในรูปแบบของเส้นทางที่เชื่อมโยงการสื่อสาร สามารถบ่งชี้ถึงแหล่งกำเนิด ทิศทาง เส้นทาง เวลา วันที่ ขนาด ระยะเวลา หรือประเภทของการบริการที่ผู้ใช้งาน (Article 1 (d))

การที่อนุสัญญาได้กำหนดนิยามดังกล่าว เนื่องจากข้อมูลจราจรทางคอมพิวเตอร์ถือได้ว่าเป็นพยานหลักฐานสำคัญหากมีการกระทำความผิดอาชญากรรมทางคอมพิวเตอร์เกิดขึ้น ข้อมูลในการติดต่อสื่อสารที่กระทำผ่านทางคอมพิวเตอร์จะต้องถูกเก็บอยู่ในรูปแบบของข้อมูลจราจรทางคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการติดต่อในรูปแบบของการส่งข้อมูล (File Transfer)

จดหมายอิเล็กทรอนิกส์ (Electronic Mail) การส่งข้อความสั้น (Instant Massage) หรือรูปแบบอื่นๆที่มีการติดต่อผ่านระบบคอมพิวเตอร์

2.3.2 มาตรการทางด้านสารบัญญัติ การกำหนดฐานความผิดและองค์ประกอบความผิด

อนุสัญญาฉบับนี้ได้กำหนดให้ประเทศภาคีแต่ละประเทศพึงจัดให้มีมาตรการทางนิติบัญญัติ และมาตรการอื่นที่จำเป็นในการกำหนดฐานความผิดและองค์ประกอบความผิดสำหรับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ให้เป็นความผิดทางอาญาภายใต้กฎหมายภายในประเทศนั้น ทั้งนี้ การกำหนดฐานความผิดหรือชนิดของความผิดจะต้องสอดคล้องกันระหว่างประเทศภาคี เพื่อให้เป็นไปตามแนวทาง Recommendation No. R (89) 9 ฐานความผิดที่กำหนดในอนุสัญญาเป็นฐานความผิดที่มุ่งกระทำต่อความลับความเที่ยงตรงและความมีอยู่ของข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ ความผิดเกี่ยวกับคอมพิวเตอร์ ความผิดเกี่ยวกับเนื้อหา ความผิดเกี่ยวกับการละเมิดลิขสิทธิ์และสิทธิที่เกี่ยวข้อง ซึ่งอนุสัญญานี้กำหนดไว้ 9 ฐานความผิดได้แก่

1. การเข้าถึงโดยมิชอบ (Article 2) ไม่ว่าทั้งหมดหรือบางส่วนของระบบคอมพิวเตอร์ ซึ่งการกระทำที่เป็นการเข้าถึงดังกล่าวจะต้องกระทำโดยเจตนา (Intentionally) และโดยไม่มีสิทธิ (Without Right) ในการเข้าถึงระบบ จากการวิเคราะห์บทบัญญัติดังกล่าวของอนุสัญญาสามารถแยกองค์ประกอบความผิด ดังนี้

ก. การเข้าถึง (Access) ระบบคอมพิวเตอร์ จากนิยามดังกล่าวในอนุสัญญาการเข้าถึงระบบคอมพิวเตอร์ดังกล่าวต้องเป็นการเข้าถึงอุปกรณ์หรือกลุ่มของอุปกรณ์ที่เชื่อมต่อกันระหว่างระบบคอมพิวเตอร์ ไม่ว่าจะเป็นการเข้าถึงทั้งหมด หรือว่าบางส่วนของอุปกรณ์หรือกลุ่มอุปกรณ์ดังกล่าว

ข. กระทำโดยเจตนา (Intentionally) หมายความว่า การเข้าถึงระบบคอมพิวเตอร์ต้องมีเจตนาในการกระทำความผิด หากไม่มีเจตนาในการเข้าถึงระบบดังกล่าวย่อมไม่เป็นความผิด เนื่องจากในอนุสัญญาไม่ได้กำหนดความหมายหรือขอบเขตของคำว่า เจตนา แต่อย่างไรก็ตามการตีความถึงเจตนาควรตีความตามความหมายซึ่งเป็นที่ยอมรับกันในทางอาญาของสังคมระหว่างประเทศ เพื่อมิให้การตีความบทบัญญัติเป็นอุปสรรคต่อการบังคับใช้กฎหมายต่อไป

ค. กระทำโดยไม่มีสิทธิ หรือโดยปราศจากอำนาจ (Without Right) หมายความว่า การเข้าถึงระบบคอมพิวเตอร์ดังกล่าวต้องเป็นการกระทำโดยไม่มีสิทธิในระบบคอมพิวเตอร์นั้น การกระทำโดยไม่มีสิทธิดังกล่าวอาจทำโดยฝ่าฝืนรหัสการเข้าถึงข้อมูล (Password) ของบุคคลอื่น

การกระทำความผิดที่เป็นการเข้าถึงข้อมูล เช่น การเจาะระบบและข้อมูล ผู้กระทำอาจเป็นบุคคลหรือเป็นคอมพิวเตอร์ที่ถูกสั่งการให้กระทำโปรแกรมคอมพิวเตอร์ การเข้าถึงอาจเป็นความผิดสำเร็จได้ด้วยทางอิเล็กทรอนิกส์ เช่น เข้าถึงโดยผ่านทางรหัส (Password)[16] และโดยกลไกอื่นๆ หรืออาจเป็นความผิดสำเร็จได้ด้วยทางกายภาพ เช่น การลักรหัสประจำตัว (Personal Identification Password : PIN)[17] เพื่อใช้ในการเข้าถึงระบบและข้อมูล โดยทั่วไปผู้กระทำผิดในลักษณะนี้จะมีมูลเหตุจูงใจที่แตกต่างกันในการเข้าถึงข้อมูลแต่ละประเภท เช่น ผู้กระทำความผิดที่มีมูลเหตุจูงใจทางการเงิน จะเข้าถึงข้อมูลลิขสิทธิ์หรือความลับทางการค้า รวมถึงข้อมูลลูกค้าของสถาบันการเงิน ผู้กระทำความผิดที่ทำเพื่อสนองความพอใจส่วนตัว จะเข้าถึงข้อมูลส่วนบุคคล อาจเป็นการสืบความลับของคู่รักหรือศัตรู รวมไปถึงผู้กระทำความผิดประเภทที่ต้องการท้าทายกฎหมายโดยการแอบอ้างตัวเอง หรือผู้กระทำความผิดประเภทที่เกิดความแค้นซึ่งโดยมากมักเป็นลูกจ้างหรืออดีตลูกจ้างที่ต้องการแก้แค้นนายจ้างตัวเอง

นอกจากนี้การเข้าถึงข้อมูลคอมพิวเตอร์ยังอาจรองรับอาชญากรรมทางคอมพิวเตอร์ในรูปแบบอื่นๆ เช่น การปลอมแปลง การก่อการร้ายทางคอมพิวเตอร์[18] ที่มีผลสืบเนื่องจากการกระทำโดยที่มีจุดมุ่งหมายเพื่อสร้างความหวาดกลัว เช่นเดียวกับการก่อการร้ายทั่วไป โดยการกระทำที่เข้าข่ายการก่อการร้ายทางอิเล็กทรอนิกส์ (E-terrorism) จะเกี่ยวข้องกับการเจาะระบบคอมพิวเตอร์เพื่อก่อเหตุรุนแรงต่อบุคคลหรือทรัพย์สิน หรืออย่างน้อยก็มีจุดมุ่งหมายเพื่อสร้างความหวาดกลัว

2. การดักรับข้อมูลโดยมิชอบ (Article 3) วัตถุประสงค์ของบทบัญญัตินี้เพื่อปกป้องสิทธิส่วนบุคคลความเป็นส่วนตัวในการติดต่อสื่อสาร จึงกำหนดให้การดักรับการส่งข้อมูลคอมพิวเตอร์ที่มิใช่ข้อมูลสาธารณะ (Non-public) ที่ส่งไปยังระบบคอมพิวเตอร์อื่น หรือส่ง

---

[16] ทวีศักดิ์ กออนันตกูล, "โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ อาชญากรรมทางคอมพิวเตอร์," ไอทีปริทัศน์ ปีที่ 6 ฉบับที่ 9 (ธันวาคม 2541): 1.

[17] เรื่องเดียวกัน

[18] การประชุมสหประชาชาติครั้งที่ 10 ว่าด้วยการป้องกันอาชญากรรมและการปฏิบัติต่อผู้กระทำผิด (The Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders), กรุงเวียนนา วันที่ 10-17 เมษายน 2543

จากระบบคอมพิวเตอร์หนึ่งไปยังอีกระบบหนึ่ง หรือแม้กระทั่งการส่งข้อมูลภายในระบบคอมพิวเตอร์นั้นเอง โดยการดักรับข้อมูลดังกล่าวอาจกระทำด้วยวิธีการทางเทคนิคหรือการแผ่รังสีทางแม่เหล็กไฟฟ้าจากระบบคอมพิวเตอร์ แต่การดักรับข้อมูลนี้จะเป็นความผิดก็ต่อเมื่อกระทำโดยเจตนาและโดยไม่มีสิทธิต่อข้อมูลส่วนบุคคล ทั้งนี้ อนุสัญญายังได้กำหนดให้ประเทศภาคีอาจกำหนดให้การดักรับข้อมูลเป็นความผิดเฉพาะกรณีที่ได้กระทำโดยเจตนาทุจริต หรือเฉพาะกรณีที่เป็นการกระทำเกี่ยวกับคอมพิวเตอร์ที่เชื่อมโยงกับระบบคอมพิวเตอร์อื่น* จากการวิเคราะห์บทบัญญัติดังกล่าวของอนุสัญญาผู้เขียนแยกองค์ประกอบความผิด ดังนี้

การดักรับข้อมูลที่ส่งไปหรือส่งจากระบบคอมพิวเตอร์หนึ่งไปยังอีกระบบหนึ่ง หรือการส่งภายในระบบคอมพิวเตอร์ การติดต่อสื่อสารที่เกิดขึ้นอาจเป็นการติดต่อสื่อสารระหว่างคอมพิวเตอร์หรือแม้กระทั่งการส่งข้อมูลภายในคอมพิวเตอร์เพียงเครื่องเดียว เช่น การส่งข้อมูลให้มีการแสดงผลบนหน้าจอ หรือการส่งข้อมูลเพื่อสั่งพิมพ์ข้อมูลที่เครื่องพิมพ์ การดักรับข้อมูลที่เป็นการกระทำความผิดจะต้องกระทำโดยเจตนา กระทำโดยไม่มีสิทธิหรือโดยปราศจากอำนาจเช่นเดียวกับความผิดอื่น

3. การแทรกแซงต่อข้อมูลไม่ว่าจะเป็นการทำให้เสียหาย การลบ การทำให้เสื่อมเสีย การแก้ไขดัดแปลงที่เป็นการแก้ไขดัดแปลงข้อมูลที่มีอยู่ในขณะนั้น หรือการทำลาย การแทรกแซงต่อข้อมูลเป็นการกระทำที่ส่งผลในทางลบแก่ข้อมูล เป็นการขัดขวางการทำงานของข้อมูล การกระทำความผิดต้องเป็นการกระทำโดยเจตนาและโดยไม่มีสิทธิที่จะกระทำ ส่งผลให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ (Article 4)

การกระทำความผิดในลักษณะนี้ได้แก่ การใช้ชุดคำสั่งในทางมิชอบ การแพร่กระจายไวรัสคอมพิวเตอร์และโค้ดอันตรายต่างๆ เช่น Trojan Horses เป็นการเขียนโปรแกรมที่แฝงไว้ในโปรแกรมที่มีประโยชน์อื่น จะปฏิบัติการเมื่อโปรแกรมดังกล่าวถูกเรียกใช้ ซึ่งมักจะใช้เพื่อการการฉ้อโกงทางคอมพิวเตอร์หรือการทำลายข้อมูลและระบบคอมพิวเตอร์ Trap Doors เป็นการเขียนโปรแกรมหน้าจอเพื่อลวงเอาข้อมูลการเข้าสู่ระบบ Salami Techniques เป็นการเขียนโปรแกรมในการปัดเศษทศนิยม[19] Logic Bombs เป็นการเขียนโปรแกรมให้

---

* Article 3 - Illegal interception

...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.

[19] ทวีศักดิ์ กออนันตกูล. "โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ อาชญากรรมทางคอมพิวเตอร์," ไอทีปริทัศน์ ปีที่ 6 ฉบับที่ 9, หน้า 3.

ปฏิบัติการเมื่อเกิดเงื่อนไขตามที่ต้องการ Worms และ Viruses เป็นการเขียนโปรแกรมให้ทำลายข้อมูล สั่งให้คอมพิวเตอร์ไม่ทำงาน หรือทำให้ระบบเกิดความเสียหาย[20]

อนุสัญญานี้ยังเปิดโอกาสให้ประเทศภาคีสามารถสงวนสิทธิในการกำหนดให้การกระทำที่เป็นการแทรกแซงข้อมูลจะถือเป็นความผิดก็ต่อเมื่อเป็นกรณีของการกระทำที่ก่อให้เกิดความเสียหายอย่างร้ายแรง (Serious Harm) โดยต้องยื่นเป็นหนังสือแจ้งข้อสงวนดังกล่าวต่อเลขาธิการสภายุโรป และควรชี้แจงถึงการตีความความหมายของคำว่า ความเสียหายอย่างร้ายแรงด้วย

4. การแทรกแซงต่อระบบ การกระทำความผิดตามบทบัญญัตินี้เป็นไปตาม Recommendation No. R (89) 9 ในส่วนที่เกี่ยวกับการก่อวินาศกรรมทางคอมพิวเตอร์ เป็นการกระทำที่กีดขวางหรือขัดขวางการทำงานของระบบคอมพิวเตอร์อย่างร้ายแรง โดยวิธีการใส่เข้า การส่งต่อ การทำให้เสียหาย การลบ การทำให้เสื่อมเสีย การแก้ไขดัดแปลง หรือการทำลายข้อมูลคอมพิวเตอร์ ซึ่งกระทำโดยเจตนาและโดยไม่มีสิทธิที่จะกระทำเช่นนั้น (Article 5)

การกระทำความผิดในลักษณะนี้ ได้แก่ การปฏิเสธการให้บริการ (Denial of Service)[21] การโจมตีระบบคอมพิวเตอร์ด้วยการแพร่กระจายไวรัสคอมพิวเตอร์และโค้ดอันตรายต่างๆ การกระทำดังกล่าวไม่เพียงเป็นการทำลายระบบแต่อาจเป็นการทำให้ระบบทำงานได้ช้าลง เช่น การส่งข้อมูลจดหมายอิเล็กทรอนิกส์ขนาดใหญ่ไปยังผู้รับก็ถือเป็นการกระทำความผิดตามลักษณะนี้เช่นกัน รูปแบบการโจมตีระบบเริ่มเปลี่ยนจากระดับที่รวดเร็วและวงกว้างไปเป็นการโจมตีที่ชาญฉลาดขึ้นโดยเน้นไปที่กลุ่มเป้าหมายที่เฉพาะเจาะจง

5. การนำสิ่งที่ได้จากคอมพิวเตอร์ไปใช้ในทางมิชอบ หมายถึง การผลิต การขาย การจัดให้มีใช้เพื่อประโยชน์ การนำเข้า การจำหน่ายจ่ายแจก หรือการทำให้มีขึ้นซึ่งอุปกรณ์โปรแกรมคอมพิวเตอร์ที่ถูกออกแบบหรือดัดแปลงขึ้น โดยมีวัตถุประสงค์หลักเพื่อใช้ในการกระทำความผิดประเภทอื่นตามที่ได้กำหนดไว้ข้างต้น รวมถึงการผลิต การขาย การจัดให้มีใช้เพื่อประโยชน์ การนำเข้า การจำหน่ายจ่ายแจก หรือการทำให้มีขึ้นซึ่งรหัสผ่านคอมพิวเตอร์ (Password) รหัสการเข้าถึงคอมพิวเตอร์ (Access Code) หรือข้อมูลอื่นที่มีลักษณะในทำนอง

---

[20] ญาณพล ยั่งยืน, อาชญากรรมทางคอมพิวเตอร์ (Computer Related Crime)[ออนไลน์], แหล่งที่มา: http://www.ssru.ac.th/linkssru/Subject New/4000108/hum07/topic8/linkfile/print5.htm[2553, มกราคม 11]

[21] เลอศักดิ์ ลิ้มวิวัฒน์กุล, Denial of Service Attacks หรือ DoS[ออนไลน์], 2549, แหล่งที่มา: http://www.thaicert.org/paper/DoS/DoS.php[2553, มกราคม 11]

เดียวกันนี้ที่ทำให้สามารถเข้าถึงระบบคอมพิวเตอร์ โดยมีเจตนาที่จะใช้เพื่อการกระทำความผิดประเภทอื่น และประเทศภาคีอาจกำหนดจำนวนของการมีไว้ครอบครองซึ่งอุปกรณ์และรหัสดังกล่าวว่าต้องครอบครองตั้งแต่จำนวนเท่าใดจึงจะถือว่าเป็นความผิด (Article 6 (1) (b))

ข้อยกเว้นการกระทำความผิดหากเป็นกรณีการผลิต การขาย การจัดให้มีใช้เพื่อประโยชน์ การนำเข้า การจำหน่ายจ่ายแจก หรือการทำให้มีขึ้นซึ่งอุปกรณ์และรหัสดังกล่าวไม่ได้มีวัตถุประสงค์ในการกระทำความผิดประเภทอื่น เช่น การกระทำที่มีวัตถุประสงค์เพื่อการทดสอบหรือคุ้มครองระบบคอมพิวเตอร์ที่ได้รับอนุญาตโดยชอบ (Article 6 (2))

การกระทำความผิดในลักษณะดังกล่าวนี้อาจสืบเนื่องมาจากการเข้าถึงข้อมูลความลับทางการค้าของบริษัทซึ่งเป็นการล่วงรู้โดยมิชอบต่อความลับทางการค้าของธุรกิจคู่แข่ง หากผู้กระทำความผิดนำข้อมูลดังกล่าวไปเผยแพร่ หรือจำหน่ายต่อคู่แข่งทางการค้าของเหยื่อโดยหวังผลประโยชน์ทางการเงินจากการเข้าถึงข้อมูลดังกล่าว

ทั้งนี้ ประเทศภาคีอาจสงวนสิทธิภายใต้เงื่อนไขที่ว่าหากมิใช่การกระทำที่เกี่ยวกับการขาย การจำหน่ายจ่ายแจกหรือการทำให้มีขึ้นซึ่งอุปกรณ์และรหัสดังกล่าวแล้วก็ไม่เป็นความผิด (Article 6 (3))

6. การกระทำความผิดเกี่ยวกับการปลอมแปลงเกี่ยวกับคอมพิวเตอร์ (Article 7) การกระทำที่เป็นการปลอมแปลงไม่ว่าจะเป็นการใส่เข้า การแก้ไขดัดแปลง การลบ หรือการทำลายข้อมูลคอมพิวเตอร์ ที่ส่งผลให้ข้อมูลคลาดเคลื่อน โดยต้องการที่จะทำให้เห็นว่าข้อมูลที่ถูกกระทำดังกล่าวนั้นเป็นข้อมูลที่ถูกต้อง หรือต้องการที่จะใช้ในทางกฎหมายในลักษณะเหมือนกับว่าข้อมูลดังกล่าวนั้นเป็นข้อมูลที่ถูกต้อง ทั้งนี้ การกระทำดังกล่าวไม่ได้คำนึงถึงว่าข้อมูลนั้นสามารถอ่านหรือเข้าใจได้โดยตรงหรือไม่ก็ตาม และการกระทำดังกล่าวจะเป็นความผิดก็ต่อเมื่อได้กระทำโดยเจตนาและไม่มีสิทธิ ทั้งนี้ ประเทศภาคีอาจกำหนดให้การกระทำดังกล่าวเป็นความผิดเฉพาะกรณีที่ได้กระทำโดยมีเจตนาที่จะฉ้อโกงหรือมีเจตนาทุจริตอย่างอื่นในลักษณะทำนองเดียวกันกับการฉ้อโกง

การกระทำความผิดในลักษณะนี้ เช่น การขโมยลักษณะบ่งเฉพาะ (Theft of Identity)[22] ซึ่งเป็นการแอบอ้างตัวของผู้กระทำผิดต่อบุคคลที่สามว่าตนเป็นอีกคนหนึ่งซึ่งผู้กระทำ

---

[22] Howard, John D. and Thomas A. Longstaff, A Common Language for Computer SecurityIncidents, SANDIA REPORT, SAND98-8667, Oct.1998 แปลโดย ปนิวัธน์ ทรัพย์รุ่งเรือง. NSA Glossary of Terms Used in Security and Intrusion Detection[ออนไลน์]. แหล่งที่มา: http://www.thaicert.org/paper/basic/terms.htm[2552, เมษายน 23]

ผิดสามารถใช้ลักษณะเฉพาะของผู้ถูกแอบอ้าง หรือของเหยื่อ ซึ่งการกระทำรูปแบบนี้อาจเชื่อมโยงให้เกิดการกระทำความผิดในลักษณะอื่นได้

7. ความผิดเกี่ยวกับการใช้คอมพิวเตอร์ในการฉ้อโกง (Article 8) เป็นการกระทำที่ก่อให้เกิดความสูญเสียในทรัพย์สินของบุคคลอื่นโดยการใส่เข้า การแก้ไขดัดแปลง การลบ หรือการทำลายข้อมูลคอมพิวเตอร์ และการแทรกแซงต่อการทำงานของระบบคอมพิวเตอร์ โดยมีเจตนาในทางฉ้อโกงหรือเจตนาทุจริตที่ทำให้ได้รับประโยชน์ทางเศรษฐกิจไม่ว่าการกระทำนั้นจะได้กระทำเพื่อตนเองหรือบุคคลอื่นก็ตาม

การกระทำความผิดในลักษณะนี้อาจสืบเนื่องจากการกระทำความผิดเกี่ยวกับการปลอมแปลงเกี่ยวกับคอมพิวเตอร์ เช่น การหลอกลวงเกี่ยวกับบัตรเครดิตโดยใช้หมายเลขบัตรเครดิต เลขบัญชีธนาคาร ที่อยู่ ข้อมูลส่วนบุคคลอื่นของเหยื่อ ทำให้เกิดความเสียหาย

8. การกระทำที่เป็นความผิดเกี่ยวกับสื่อลามกอนาจารเกี่ยวกับเด็ก (Article 9) ปัจจุบันภาพและสื่อลามกต่างๆได้มีการแพร่หลายไปสู่สังคมของทุกประเทศทั่วโลก โดยการเผยแพร่ภาพและสื่อลามกได้มีการพัฒนารูปแบบให้มีความหลากหลายมากขึ้น เช่น การเผยแพร่ภาพและสื่อลามกอนาจารผ่านโปรแกรม Camfrog ซึ่งเป็นการพัฒนามาจากระบบ Video Conference เมื่อเทคโนโลยีสารสนเทศที่สื่อสารผ่านทางระบบเครือข่ายอินเทอร์เน็ตได้พัฒนาก้าวหน้ามากขึ้น ยิ่งทำให้ภาพและสื่อลามกต่างๆสามารถแพร่หลายไปสู่สังคมของประเทศต่างๆทั่วโลกได้อย่างรวดเร็วจนยากที่จะป้องกัน ทั้งนี้ ได้มีมาตรการในการกำกับดูแลการเผยแพร่ภาพและสื่อลามกอนาจารที่ผ่านโปรแกรม Camfrog โดยรูปแบบการกำกับดูแลดังกล่าวได้มาจากบันทึกข้อตกลงว่าด้วยการกำกับดูแลเนื้อหาบนอินเทอร์เน็ต (Memorandum on the Regulation of Internet Content) ที่ประมวลและร่างขึ้นโดย ศูนย์วิจัยสื่อของมูลนิธิเบอร์เธลส์แมน (Berteismann Foundation) ในประเทศเยอรมันนี[23] ซึ่งเป็นรูปแบบที่ได้รับการยอมรับให้ใช้ในประเทศสมาชิกของสหภาพยุโรป (European Union : EU) โดยจะปรากฏสาระสำคัญของบันทึกดังกล่าวอยู่ในแผนการสร้างอินเทอร์เน็ตที่ปลอดภัยยิ่งขึ้นของสหภาพยุโรป (EU Safer Internet Action Plan) การร่างบันทึกดังกล่าวเป็นผลมาจากความร่วมมือกันของผู้เชี่ยวชาญจากนานาชาติในสาขาวิชาและความสนใจด้านต่างๆกันไม่ว่าจะเป็น การเมือง เศรษฐกิจ กฎหมาย และสังคมศาสตร์ จุดมุ่งหมายหลักคือ เพื่อหาทางป้องกันเด็กและเยาวชนจากเนื้อหาที่เป็นอันตรายบนอินเทอร์เน็ตให้ดียิ่งขึ้น ทั้งนี้ จากความร่วมมือดังกล่าวสิ่งหนึ่งที่ผู้เชี่ยวชาญ

---

[23] อำนาจ เนตยสุภา และอรวรรณ เดชโชติวุฒิ, มาตรการทางกฎหมายในการป้องกันและปราบปรามการกระทำความผิดที่เกิดขึ้นในโปรแกรม Camfrog, บทบัณฑิตย์ เล่มที่ 63 ตอนที่ 3 (กันยายน 2550): หน้า 108.

สามารถสรุปเบื้องต้นได้ว่า ความร่วมมือกันในการแก้ไขปัญหาสื่อระดับโลกอย่างอินเทอร์เน็ตไม่สามารถจะพึ่งพาเพียงภาครัฐ ภาคเอกชน หรือองค์กรพัฒนาเอกชนฝ่ายใดฝ่ายหนึ่งเพื่อปกป้องผู้เยาว์ได้ ดังนั้นแนวทางที่ควรจะเป็นคือการประสานความร่วมมือของหลายๆฝ่าย ทั้งในระดับประเทศและระดับสากล โดยต้องอยู่บนฐานความรับผิดชอบร่วมกัน ไม่ว่าจะเป็น การกำกับดูแลตนเองของภาคอุตสาหกรรมอินเทอร์เน็ต การแบ่งประเภทของเนื้อหาโดยผู้ผลิตเนื้อหาและการใช้ระบบการกลั่นกรองเนื้อหาโดยผู้ใช้งาน การมีสายด่วนให้ผู้ใช้บริการ การบังคับใช้กฎหมายและการดำเนินการตามกฎหมายเพื่อส่งเสริมการกำกับดูแลตนเอง และการส่งเสริมความรู้ให้เท่าทันสื่อ[24] ซึ่งนอกจากมาตรการในการปกป้องผู้เยาว์โดยบันทึกฯดังกล่าวแล้ว ยังมีการกำหนดให้การกระทำเกี่ยวกับสื่อลามกอนาจารเกี่ยวกับเด็กถือเป็นการกระทำความผิดอาญาตามที่บัญญัติไว้ในอนุสัญญาฉบับนี้ด้วย จากวัตถุประสงค์ของอนุสัญญาช่วงอายุของเด็กและเยาวชนที่อนุสัญญามุ่งคุ้มครอง คือ บุคคลที่มีอายุไม่ถึง 18 ปี แต่ต้องไม่น้อยกว่า 16 ปี (Article 9 (3))

ความหมายโดยทั่วไปของคำว่า "สื่อลามกอนาจารเกี่ยวกับเด็ก" หมายถึง สิ่งลามกที่สามารถมองเห็นได้ด้วยตาเปล่าที่แสดงถึงการกระทำกิจกรรมทางเพศโดยชัดแจ้งของเด็ก บุคคลที่ปรากฏในสื่อนั้นเป็นเด็กซึ่งกระทำกิจกรรมทางเพศโดยชัดแจ้ง รวมถึงภาพเหมือนจริงที่แสดงภาพของเด็กซึ่งกระทำกิจกรรมทางเพศโดยชัดแจ้ง (Article 9 (2) (a) (b) (c))

การกระทำที่ถือเป็นความผิดตามอนุสัญญาดังกล่าวนี้ ได้แก่ การผลิตสื่อลามกอนาจารเกี่ยวกับเด็ก และการผลิตดังกล่าวต้องมีวัตถุประสงค์ในการเผยแพร่ผ่านระบบคอมพิวเตอร์ การเสนอ การทำ การเผยแพร่ หรือการส่งต่อสื่อลามกอนาจารเกี่ยวกับเด็กผ่านระบบคอมพิวเตอร์ การจัดหาสื่อลามกอนาจารเกี่ยวกับเด็กสำหรับตนเองหรือบุคคลอื่นผ่านทางระบบคอมพิวเตอร์ การครอบครองสื่อลามกอนาจารเกี่ยวกับเด็กในระบบคอมพิวเตอร์หรือในสื่อกลางสำหรับบรรจุข้อมูลคอมพิวเตอร์ (Article 9 (1) (a) (b) (c) (d) (e))

ประเทศภาคีอาจสงวนสิทธิในการบัญญัติให้ การจัดหาสื่อลามกอนาจารเกี่ยวกับเด็กสำหรับตนเองหรือบุคคลอื่นผ่านทางระบบคอมพิวเตอร์ การครอบครองสื่อลามกอนาจารเกี่ยวกับเด็กในระบบคอมพิวเตอร์หรือในสื่อกลางสำหรับบรรจุข้อมูลคอมพิวเตอร์ หรือสื่อลามกที่แสดงให้เห็นว่าบุคคลที่ปรากฏในสื่อนั้นเป็นเด็กซึ่งกระทำกิจกรรมทางเพศโดยชัดแจ้ง รวมถึง

---

[24] เรื่องเดียวกัน, หน้า 108.

ภาพเหมือนจริงที่แสดงภาพของเด็กซึ่งกระทำกิจกรรมทางเพศโดยชัดแจ้ง ไม่ถือว่าเป็นการกระทำความผิดทางอาญา (Article 9 (4))

9. การละเมิดลิขสิทธิ์และสิทธิที่เกี่ยวข้องกับลิขสิทธิ์ ทั้งนี้ การกำหนดความผิดดังกล่าวจะต้องเป็นการละเมิดลิขสิทธิ์ตามความหมายที่ระบุในกฎหมายภายในของประเทศนั้นๆ โดยให้เป็นไปตามหน้าที่กำหนดไว้ในบทบัญญัติแห่งกรุงปารีส ลงวันที่ 24 กรกฎาคม ค.ศ. 1971 ซึ่งปรับปรุงแก้ไขอนุสัญญากรุงเบิร์นว่าด้วยการคุ้มครองวรรณกรรมและงานศิลปะ ข้อตกลงว่าด้วยหลักเกณฑ์ที่เกี่ยวข้องกับการค้าในสิทธิแห่งทรัพย์สินทางปัญญา และสนธิสัญญาขององค์การทรัพย์สินทางปัญญาของโลกว่าด้วยลิขสิทธิ์ (Article 10 (1)) ยกเว้นธรรมสิทธิ์ตามที่กำหนดไว้ในข้อตกลงดังกล่าวข้างต้น ทั้งนี้ การละเมิดลิขสิทธิ์ดังกล่าวได้กระทำโดยเจตนาเพื่อการค้าและโดยวิธีการของระบบคอมพิวเตอร์

การละเมิดสิทธิที่เกี่ยวข้องกับลิขสิทธิ์ หมายถึง การละเมิดสิทธิที่เกี่ยวข้องกับลิขสิทธิ์ตามความหมายที่ระบุในกฎหมายของประเทศนั้นๆ โดยให้เป็นไปตามที่กำหนดไว้ในอนุสัญญาระหว่างประเทศว่าด้วยการคุ้มครองผู้แสดง ผู้ผลิตเสียง และองค์กรวิทยุกระจายเสียง (อนุสัญญากรุงโรม) ข้อตกลงว่าด้วยหลักเกณฑ์ที่เกี่ยวข้องกับการค้าในสิทธิแห่งทรัพย์สินทางปัญญา และสนธิสัญญาขององค์การทรัพย์สินทางปัญญาของโลกว่าด้วยผู้แสดงและผู้ผลิตเสียง ยกเว้นธรรมสิทธ์ตามที่กำหนดไว้ในบรรดาข้อตกลงดังกล่าวได้กระทำโดยเจตนาเพื่อการค้าและโดยวิธีการของระบบคอมพิวเตอร์ (Article 10 (2))

ประเทศภาคีอาจสงวนสิทธิได้ว่าจะไม่กำหนดให้การกระทำดังกล่าวข้างต้นนี้เป็นความผิดก็ได้หากมีวิธีการเยียวยาอื่นๆ และการสงวนสิทธิดังกล่าวต้องไม่ทำให้หน้าที่ระหว่างประเทศตามที่ได้ตกลงไว้ในความตกลงที่กล่าวไว้ต้องลดลง (Article 10 (3))

จากฐานความผิดดังกล่าวข้างต้น สามารถสรุปได้ว่าความผิดที่กระทำต่อความลับความเที่ยงตรงและความมีอยู่ของข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ ได้แก่ การเข้าถึงโดยมิชอบ การดักรับข้อมูลโดยมิชอบ การแทรกแซงต่อข้อมูล การแทรกแซงต่อระบบ การนำสิ่งที่ได้จากคอมพิวเตอร์ไปใช้ในทางมิชอบ ความผิดเกี่ยวกับคอมพิวเตอร์ ได้แก่ การกระทำความผิดเกี่ยวกับการปลอมแปลงเกี่ยวกับคอมพิวเตอร์ ความผิดในการใช้คอมพิวเตอร์ในการฉ้อโกง ความผิดเกี่ยวกับเนื้อหา ได้แก่ การกระทำที่เป็นความผิดเกี่ยวกับสื่อลามกอนาจารเกี่ยวกับเด็ก ความผิดเกี่ยวกับการละเมิดลิขสิทธิ์และสิทธิที่เกี่ยวข้อง ได้แก่ การละเมิดลิขสิทธิ์และสิทธิที่เกี่ยวข้องกับลิขสิทธิ์

แต่จะเห็นได้ว่าการกระทำความผิดทุกฐานความผิดได้กำหนดให้องค์ประกอบหนึ่งของการกระทำความผิดคือ การกระทำดังกล่าวต้องกระทำโดยเจตนา ถึงแม้อนุสัญญามิได้กำหนดขอบเขตหรือความหมายของคำว่า เจตนา แต่เพื่อให้เป็นไปตามวัตถุประสงค์และจุดมุ่งหมายของอนุสัญญาที่ต้องการให้มาตรการทางด้านสารบัญญัติเกี่ยวกับการกำหนดฐานความผิดของประเทศภาคีเป็นไปในทิศทางเดียวกันและมีความสอดคล้องกัน ไม่เป็นอุปสรรคต่อการบังคับใช้กฎหมาย ประเทศภาคีจึงควรตีความความหมายของคำว่า เจตนา ให้สอดคล้องตามบริบทในทางระหว่างประเทศ

นอกจากความผิดทั้ง 9 ฐาน ดังกล่าวแล้ว อนุสัญญายังได้บัญญัติถึงความรับผิด ความรับผิดฐานการพยายาม การช่วยเหลือสนับสนุน การใช้ให้กระทำความผิด รวมถึงความรับผิดของนิติบุคคล ซึ่งทำให้สามารถลงโทษผู้กระทำความผิดที่มีสถานะดังกล่าวได้ เช่น ผู้ให้บริการ ซึ่งอาจก่อให้เกิดการกระทำความผิดร่วมกับบุคคลธรรมดาได้ หรืออาจกระทำความผิดการช่วยเหลือสนับสนุนการกระทำความผิด โดยกำหนดให้การกระทำของบุคคลธรรมดาที่ได้กระทำเพื่อประโยชน์ของนิติบุคคลไม่ว่าจะกระทำโดยตนเองหรือโดยเป็นส่วนหนึ่งของนิติบุคคลในฐานะที่เป็นผู้แทนนิติบุคคลที่มีอำนาจกระทำการแทน ตัดสินใจ หรือควบคุมภายในนิติบุคคลนั้น รวมถึงมาตรการอื่นๆ ที่กำหนดให้นิติบุคคลมีความรับผิดได้ในกรณีที่ขาดการควบคุมหรือดูแลโดยบุคคลธรรมดา โดยความรับผิดดังกล่าวอาจเป็นความรับผิดทางอาญา ทางแพ่ง หรือทางปกครอง แต่ความรับผิดดังกล่าวจะต้องไม่กระทบต่อความรับผิดทางอาญาของบุคคลธรรมดาที่ได้กระทำความผิด ทั้งนี้ ประเทศภาคีสามารถกำหนดมาตรการลงโทษอย่างอื่นที่มีประสิทธิผลได้สัดส่วนที่เหมาะสมและมีผลยับยั้งการกระทำความผิด เช่นการลงโทษโดยใช้วิธีจำกัดอิสรภาพการกักขัง และหากเป็นความรับผิดของนิติบุคคล อาจเป็นโทษปรับที่มีสัดส่วนที่เหมาะสมกับการกระทำความผิด

2.3.3 มาตรการทางด้านสบัญญัติ

รูปแบบของการก่ออาชญากรรมทางคอมพิวเตอร์ในปัจจุบันมีความซับซ้อนมากขึ้น ความเสียหายที่เกิดขึ้นจากการกระทำดังกล่าวได้ทวีความรุนแรงและมีมูลค่าความเสียหายมากขึ้นตามไปด้วยเช่นกัน รูปแบบของความซับซ้อนในการกระทำความผิดนี้เองที่ทำให้การบังคับใช้กฎหมายอาชญากรรมทางคอมพิวเตอร์รวมถึงการทำหน้าที่ของเจ้าหน้าที่สืบสวนสอบสวนเกี่ยวกับการกระทำความผิดมีความยากลำบาก ไม่ว่าจะเป็นปัญหาเรื่องพยานหลักฐานที่สามารถเปลี่ยนแปลงได้ตลอดเวลาและกระทำความผิดได้โดยง่ายและรวดเร็ว แต่ก็สามารถสูญหายได้ง่ายอย่างรวดเร็วเช่นกัน เช่น ข้อมูลที่ถูกบันทึกอยู่ในสื่อบันทึกข้อมูลถาวรของเครื่อง (Hard Disk)

หากระหว่างการเคลื่อนย้ายได้รับความกระทบกระเทือนหรือเกิดการกระแทก หรือเคลื่อนย้ายจุดที่เป็นสนามแม่เหล็ก ข้อมูลดังกล่าวอาจเกิดการสูญหายได้[25]

อุปสรรคอีกประการหนึ่งสำหรับการบังคับใช้กฎหมาย คือ การกระทำส่วนใหญ่ไม่สามารถเห็นตัวผู้กระทำความผิดได้ (invisible) ถึงแม้ว่าผู้กระทำความผิดอาจทิ้งร่องรอยที่เรียกว่า รอยเท้าอิเล็กทรอนิกส์ (electronic footprints) แต่หลักฐานทางอิเล็กทรอนิกส์ดังกล่าวนี้ยากต่อการแยกแยะหรือชี้ตัวผู้กระทำความผิด โดยเฉพาะการกระทำความผิดผ่านทางอินเทอร์เน็ตซึ่งมีการส่งผ่านข้อมูลได้ทันที ดังนั้น การสืบสวนสอบสวนคดีที่กระทำผ่านทางอินเทอร์เน็ตจึงมีความยากลำบากมากเช่นกัน เนื่องจาก ความสามารถของอินเทอร์เน็ตที่ทำให้การติดต่อระหว่างเครือข่ายคอมพิวเตอร์สามารถส่งผ่านข้อมูลได้ทันที อาชญากรสามารถส่งคำสั่งเปลี่ยนแปลง หรือลบข้อมูลที่ก่อให้เกิดการกระทำความผิดก่อนที่เจ้าหน้าที่จะสืบหาตัวตนได้ ทำให้ยากต่อการเก็บรวบรวมพยานหลักฐานและการสืบสวนสอบสวน เช่น ผู้กระทำความผิดทำการเปลี่ยนชื่อผู้ส่งจดหมายอิเล็กทรอนิกส์ ทำให้ผู้รับไม่ทราบถึงตัวตนที่แท้จริง หรือผู้กระทำความผิดอาจใช้ประโยชน์จากระบบคอมพิวเตอร์ทำการลบข้อมูลในการสืบสวนสอบสวน ด้วยเหตุนี้เอง ทำให้พยานหลักฐานดังกล่าวจึงเป็นสิ่งที่มีมูลค่ามากมาย[26] ดังนั้น การบังคับใช้กฎหมายที่เกี่ยวกับการสืบสวนสอบสวนเกี่ยวกับอาชญากรรมประเภทนี้ควรมีมาตรการเฉพาะเพิ่มเติมจากมาตรการสืบสวนสอบสวนการกระทำความผิดทางกายภาพในรูปแบบเดิม ซึ่งจะเห็นได้จากบทบัญญัติของอนุสัญญาดังต่อไปนี้

2.3.3.1 **มาตรการการสืบสวนสอบสวนและการดำเนินคดี**

จากเหตุผลดังกล่าวข้างต้น อนุสัญญานี้จึงต้องการให้ประเทศภาคีสมาชิกดำเนินการบัญญัติกฎหมายวิธีพิจารณาความอาญาเพื่อการเก็บรวบรวมพยานหลักฐานในการสืบสวนสอบสวนและการดำเนินคดี ไม่ว่าจะเป็นวิธีการค้นหาข้อมูลอย่างรวดเร็ว การยึดและเก็บรักษาข้อมูล และยังต้องการให้ประเทศสมาชิกบัญญัติเกี่ยวกับวิธีการใช้กระบวนการดังกล่าว ทั้งนี้ อนุสัญญาไม่ได้กำหนดถึงค่าใช้จ่ายในการค้นหาข้อมูล การยึด และการเก็บรักษาข้อมูลดังกล่าว อนุสัญญาได้ตระหนักถึงประเด็นในความแตกต่างทางวัฒนธรรมและระบบกฎหมาย

---

[25] Shannon L. Hopkins, Cybercrime Convention : a Positive Beginning to a Long Road Ahead. Journal of High Technology Law. [Online], 2003, p 2.

[26] Ibid., p 2.

ตัวอย่างเช่น ความแตกต่างในเรื่องการคุ้มครองสิทธิส่วนบุคคล และการคุ้มครองสิทธิในการแสดงความคิดเห็นของแต่ละประเทศที่แตกต่างกัน

อนุสัญญานี้ได้กำหนดหลักการทั่วไปเกี่ยวกับขอบเขตอำนาจหน้าที่และวิธีพิจารณาความอาญาเพื่อวัตถุประสงค์ในการสืบสวนสอบสวน การดำเนินคดีอาญาในเรื่องอาชญากรรมทางคอมพิวเตอร์ไว้โดยเฉพาะซึ่งการสืบสวนสอบสวนดังกล่าวได้ครอบคลุมความผิดที่กำหนดไว้ในอนุสัญญานี้ทั้งหมด รวมถึงความผิดทางอาญาอื่นๆที่ได้กระทำโดยวิธีการของระบบคอมพิวเตอร์และการรวบรวมพยานหลักฐานที่อยู่ในรูปของอิเล็กทรอนิกส์สำหรับความผิดอาญานั้นๆ ยกเว้นการกระทำความผิดฐานดักรับข้อมูลโดยมิชอบที่ได้มีการบัญญัติไว้แล้วโดยเฉพาะ

ทั้งนี้ ประเทศภาคีอาจมีการสงวนสิทธิในการใช้มาตรการรวบรวมข้อมูลจราจรทางคอมพิวเตอร์ตามเวลาที่ใช้ในการประมวลข้อมูลโดยอัตโนมัติโดยมีข้อแม้ว่า การสงวนสิทธิดังกล่าวต้องไม่เป็นจำกัดการรวบรวมข้อมูล โดยต้องเปิดให้มีการใช้มาตรการในการรวบรวมข้อมูลให้กว้างที่สุด ถึงแม้ว่ากฎหมายภายในของแต่ละประเทศจะได้จำกัดเรื่องการดักรับข้อมูลและการรวบรวมข้อมูลอาจกำหนดให้ไม่สามารถใช้วิธีการดังกล่าวเพื่อประโยชน์ของผู้ใช้บริการเฉพาะกลุ่ม และที่ใช้เครือข่ายการติดต่อสาธารณะและได้เชื่อมโยงกับระบบคอมพิวเตอร์อื่นไม่ว่าของรัฐหรือเอกชน

จากวัตถุประสงค์และความมุ่งหมายของอนุสัญญาที่ระบุไว้ในส่วนอรัมภบทได้เล็งเห็นความสำคัญของมาตรการเกี่ยวกับอำนาจหน้าที่ที่เพียงพอแก่การปราบปรามความผิดอาชญากรรมทางคอมพิวเตอร์ได้อย่างมีประสิทธิภาพ ไม่ว่าจะเป็นการตรวจสอบ การสอบสวน การฟ้องร้องคดี แต่สิ่งหนึ่งที่ประเทศภาคีจะต้องใส่ใจ คือในการกำหนดเงื่อนไข การดำเนินการสืบสวนสอบสวน และการบังคับใช้อำนาจหน้าที่ รวมถึงวิธีพิจารณาความทางอาญาเกี่ยวกับความผิดที่เกิดจากอาชญากรรมทางคอมพิวเตอร์จะต้องไม่ละเมิดต่อสิทธิมนุษยชนและเสรีภาพของประชาชน จะต้องทำให้เกิดความแน่นอนว่าจะมีความสมดุลระหว่างประโยชน์ของการบังคับใช้กฎหมายกับการเคารพต่อสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐาน* ซึ่งอนุสัญญาได้กำหนดให้

---

* Preamble of Convention on Cyber Crime 2001

...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...

ประเทศต้องมีการคุ้มครองตามสมควรต่อสิทธิมนุษยชนและเสรีภาพของประชาชน รวมถึงสิทธิอย่างอื่นที่ได้รับความคุ้มครองตามอนุสัญญาของสภายุโรปว่าด้วยการคุ้มครองสิทธิมนุษยชนและเสรีภาพขั้นพื้นฐาน ค.ศ. 1950 (Council of Europe Convention for the Protection of Human Rights 1950)* กติการะหว่างประเทศขององค์การสหประชาชาติว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง ค.ศ. 1966 (United Nations International Covenant on Civil and Political Rights 1966)** และความตกลงระหว่างประเทศว่าด้วยสิทธิมนุษยชนฉบับอื่นๆ ที่ใช้บังคับอยู่ ซึ่งความตกลงระหว่างประเทศดังกล่าวต่างได้ยืนยันถึงสิทธิของบุคคลทุกคนที่จะมีความคิดเห็นของตนเองได้โดยปราศจากการแทรกแซง ตลอดจนสิทธิเสรีภาพในการแสดงออก สิทธิเสรีภาพที่จะแสวงหา รับและถ่ายทอดข้อมูลข่าวสารความคิดเห็นทุกชนิดโดยไม่มีพรมแดนของประเทศมาขวางกั้น และรวมถึงสิทธิที่จะได้รับการเคารพในความเป็นส่วนตัวของบุคคล

หลักการดังกล่าวข้างต้น เป็นสิทธิเกี่ยวกับการติดต่อสื่อสารที่กำหนดไว้ในกติการะหว่างประเทศขององค์การสหประชาชาติว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง ค.ศ. 1966 มีหลักการว่า การกำหนดว่าบุคคลจะถูกแทรกสอดในการติดต่อสื่อสารโดยพลการหรือมิชอบด้วยกฎหมายหาได้ไม่ และบุคคลทุกคนมีสิทธิในเสรีภาพแห่งการแสดงออก สิทธินี้รวมถึงเสรีภาพที่จะ

---

* Article 8 Right to respect for private and family life of Convention for the Protection of Human Rights and Fundamental Freedoms

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.

** Article 19 of International Covenant on Civil and Political Rights

1. Everyone shall have the right to hold opinions without interference.

2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

(a) For respect of the rights or reputations of others;...

แสวงหา รับและกระจายข่าวสารและความคิดเห็นทุกรูปแบบ โดยไม่คำนึงถึงพรมแดน ทั้งนี้ ไม่ว่าด้วยวาจาเป็นลายลักษณ์อักษรหรือการตีพิมพ์ในรูปของศิลปะหรือโดยอาศัยสื่อประการอื่น[27]

การคุ้มครองตามสมควรต่อสิทธิมนุษยชนและเสรีภาพของประชาชนนั้น ตามบทบัญญัติของอนุสัญญาให้รวมถึงการใช้อำนาจหน้าที่ต่างๆที่เกี่ยวกับวิธีพิจารณาความอาญานั้นต้องมีการควบคุมดูแลโดยศาลหรือหน่วยงานอิสระ และต้องมีเหตุผลรองรับการบังคับใช้ มีข้อจำกัดว่าด้วยขอบเขตและระยะเวลาของการใช้อำนาจหน้าที่และวิธีพิจารณา ทั้งนี้ เงื่อนไขและวิธีพิจารณาที่ใช้ในเรื่องเกี่ยวกับผลประโยชน์สาธารณะ โดยเฉพาะอย่างยิ่งในการบริหารกระบวนการยุติธรรม ประเทศภาคีควรต้องมีการพิจารณาถึงผลกระทบของอำนาจหน้าที่ที่มีต่อสิทธิ ความรับผิดชอบ และผลประโยชน์อันชอบธรรมของบุคคลที่สามด้วย (Article 15)

สิทธิที่ได้รับการคุ้มครองอีกประการหนึ่ง คือสิทธิที่จะได้รับการคุ้มครองในข้อมูลส่วนบุคคลตามที่กำหนดไว้ในอนุสัญญาของสภายุโรปว่าด้วยการคุ้มครองบุคคลในเรื่องที่เกี่ยวกับการประมวลข้อมูลของบุคคลโดยระบบอัตโนมัติ ค.ศ. 1981* ซึ่งมีวัตถุประสงค์ให้ประเทศสมาชิกออกกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลขึ้นมาใช้บังคับ โดยต้องตระหนักถึงการให้ความคุ้มครองข้อมูลส่วนบุคคลขั้นพื้นฐานและมีการห้ามการส่งข้อมูลออกไปยังประเทศที่ไม่ใช่สมาชิกหรือประเทศที่ไม่มีการคุ้มครองข้อมูลส่วนบุคคลอย่างเพียงพอ**

---

[27] พันธุ์ทิพย์ กาญจนะจิตรา สายสุนทร, กติการะหว่างประเทศว่าด้วยสิทธิทางแพ่ง (พลเมือง) และทางการเมือง[Online], 2551, แหล่งที่มา: www.archanwell.org/office/download.php?file=537.pdf&fol[2552, ธันวาคม 12]

* Preamble of Convention on Cyber Crime 2001

...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;...

** Article 3 Scope of Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981

...a. that it will not apply this convention to certain categories of automated personal data files, a list of which will be deposited. In this list it shall not include, however, categories of automated data files subject under its domestic law to data protection provisions. Consequently, it shall amend this list by a new declaration whenever additional categories of automated personal data files are subjected to data protection provisions under its domestic law;...

และ Article 7 Data security of Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981

Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.

จะเห็นได้ว่าในบรรดาสิทธิที่เกี่ยวข้องกับสิทธิมนุษยชนทั้งหมด สิทธิความเป็นส่วนตัว นับเป็นสิทธิลักษณะหนึ่งที่ต้องให้ความสำคัญ ในบางประเทศแนวคิดของความเป็นส่วนตัว ได้รวมถึงการคุ้มครองข้อมูลส่วนบุคคล อย่างไรก็ตาม คำว่า "ความเป็นส่วนตัว" เป็นคำที่มีความหมายกว้างและครอบคลุมถึงสิทธิต่างๆ หลายประการ เช่น ความเป็นส่วนตัวเกี่ยวกับข้อมูล (Information Privacy) เป็นการให้ความคุ้มครองข้อมูลส่วนบุคคลโดยการวางหลักเกณฑ์เกี่ยวกับการเก็บรวบรวมและการบริหารจัดการข้อมูลส่วนบุคคล ความเป็นส่วนตัวในการติดต่อสื่อสาร (Communication Privacy)[28] เป็นการให้ความคุ้มครองในความปลอดภัย และความเป็นส่วนตัวในการติดต่อสื่อสารทางจดหมาย โทรศัพท์ ไปรษณีย์อิเล็กทรอนิกส์ หรือวิธีการติดต่อสื่อสารอื่นใด ที่ผู้อื่นจะล่วงรู้มิได้อย่างไรก็ตาม แม้ว่าสิทธิความเป็นส่วนตัวจะมีหลายประการ แต่ความเป็นส่วนตัวที่นานาประเทศต่างให้ความสำคัญอย่างมากอันเนื่องจากพัฒนาการทางเทคโนโลยีสารสนเทศที่ก้าวหน้าไปอย่างรวดเร็ว คือความเป็นส่วนตัวในข้อมูลส่วนบุคคลดังจะเห็นได้จากบทบัญญัติของความตกลงระหว่างประเทศฉบับต่างๆ ทั้งนี้ เพราะพัฒนาการล้ำยุคของคอมพิวเตอร์ส่งผลให้การติดต่อสื่อสารและการเผยแพร่ข้อมูลต่าง ๆ สามารถเคลื่อนย้ายและเชื่อมโยงกันได้โดยไม่จำกัดเวลาและสถานที่อีกต่อไป ทำให้การประมวลผล การจัดเก็บ หรือการเปิดเผยข้อมูลส่วนบุคคลสามารถทำได้โดยง่าย สะดวก และรวดเร็ว ในทางกลับกันอาชญากรคอมพิวเตอร์ก็อาจมีการนำประโยชน์ของเทคโนโลยีเหล่านี้ไปใช้ในการกระทำความผิดได้เช่นกัน

หลักการเรื่องการเคารพต่อสิทธิของบุคคลในการติดต่อสื่อสารนั้นเป็นสิ่งที่ได้รับการยอมรับกันเป็นสากล เพราะการละเมิดต่อสิทธิดังกล่าวถือเป็นการละเมิดต่อสิทธิของปัจเจกชนที่จะแลกเปลี่ยนความคิดหรือความรู้สึกที่เป็นความลับทางการติดต่อสื่อสารกับบุคคลอื่น แนวความคิดเสรีภาพส่วนบุคคลนั้นตั้งอยู่บนสมมุติฐานที่ว่าทุกคนมีขอบเขตกิจกรรมส่วนตัวและมีอำนาจที่จะห้ามบุคคลอื่นเข้ามาล่วงล้ำขอบเขตกิจกรรมส่วนตัวดังกล่าว เสรีภาพในชีวิตส่วนบุคคลนั้นได้รับการปกป้อง และจากหลักการพื้นฐานในการให้ความคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในรูปข้อมูลอิเล็กทรอนิกส์ จะเห็นได้ว่าข้อมูลส่วนบุคคลจะต้องได้รับความคุ้มครองที่เหมาะสมในทุกขั้นตอน ตั้งแต่การเก็บรวบรวม การใช้ การเก็บรักษา และการเปิดเผย การคุ้มครองข้อมูลส่วนบุคคลนั้นอาจมีความแตกต่างกัน ทั้งนี้ ขึ้นอยู่กับวัฒนธรรม พฤติการณ์แวดล้อม แนวคิดและสภาพสังคมของแต่ละประเทศ ดังนั้น การกำหนดหลักการเกี่ยวกับกฎหมายวิธีพิจารณา

---

[28] โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ, เอกสารเปรียบเทียบร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....กับพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 (สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ : 2544), หน้า 30.

ความอาญาในการเก็บรวบรวมพยานหลักฐานในการสืบสวนสอบสวนและการดำเนินคดีที่กำหนดไว้ในอนุสัญญานี้จะต้องมีการคำนึงถึงสิทธิมนุษชนและเสรีภาพขั้นพื้นฐานตามที่ผู้เขียนได้ให้เหตุผล ซึ่งหลักการดังกล่าวแบ่งออกเป็น 6 หลักการ ดังนี้

1. หลักการเก็บรักษาข้อมูลคอมพิวเตอร์ที่อยู่ในระบบอย่างรวดเร็ว เป็นหลักการสำหรับการเก็บรวบรวมพยานหลักฐาน เพราะข้อมูลคอมพิวเตอร์ถือเป็นพยานหลักฐานที่สำคัญต่อการสืบสวนสอบสวน โดยประเทศภาคีอาจกำหนดให้มีหน่วยงานภายในประเทศที่มีอำนาจหน้าที่ในการออกคำสั่งให้มีการเก็บรักษาข้อมูลคอมพิวเตอร์ที่เฉพาะเจาะจง รวมถึงข้อมูลจราจรทางคอมพิวเตอร์ ซึ่งข้อมูลดังกล่าวจะต้องถูกเก็บไว้ด้วยวิธีการของระบบคอมพิวเตอร์ที่รวดเร็ว โดยเฉพาะอย่างยิ่งเมื่อมีเหตุผลอันควรเชื่อได้ว่าข้อมูลคอมพิวเตอร์ดังกล่าวนั้นมีความเสี่ยงที่จะสูญหายหรือถูกแก้ไขดัดแปลง

ทั้งนี้ คำสั่งให้มีการเก็บรักษาข้อมูลดังกล่าวอาจกำหนดระยะเวลาในการเก็บรักษาข้อมูลเท่าที่จำเป็นแต่ไม่เกินเก้าสิบวัน ซึ่งหน่วยงานที่มีหน้าที่ในเก็บรักษาข้อมูลคอมพิวเตอร์จะต้องดูแลข้อมูลดังกล่าวให้มีความถูกต้องตลอดระยะเวลาที่กำหนด เพื่อให้หน่วยงานที่มีหน้าที่เกี่ยวข้องกับการสืบสวนสอบสวนสามารถแสวงหาข้อเท็จจริงจากข้อมูลดังกล่าวได้ แต่ระยะเวลาดังกล่าวสามารถขยายได้ อย่างไรก็ตามการเก็บรักษาข้อมูลคอมพิวเตอร์จะต้องเก็บไว้เป็นความลับเฉพาะในเรื่องที่มีการสืบสวนสอบสวน การดำเนินคดี และเฉพาะช่วงระยะเวลาที่กำหนดไว้ตามกฎหมายเท่านั้น (Article 16)

2. หลักการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ที่อยู่ในระบบอย่างรวดเร็วและการเปิดเผยบางส่วนของข้อมูลจราจรทางคอมพิวเตอร์ หลักการนี้เป็นการเข้าเก็บรักษาข้อมูลจราจรที่มีหลักการเดียวกันกับข้อมูลคอมพิวเตอร์ทั่วไป วิธีการที่รวดเร็วในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ดังกล่าวนั้น จะต้องสามารถดำเนินการจริงตามที่กำหนด โดยไม่คำนึงว่าจะมีผู้ให้บริการจำนวนหนึ่งหรือหลายรายมีส่วนเกี่ยวข้องกับการส่งต่อของการติดต่อสื่อสารนั้นหรือไม่ ทั้งนี้ วิธีการในการเปิดเผยข้อมูลจราจรทางคอมพิวเตอร์ดังกล่าวก็เช่นกัน จะต้องเป็นวิธีการที่สามารถดำเนินการได้จริง และข้อมูลที่ทำการเปิดเผยนั้นจะต้องเป็นข้อมูลที่มีจำนวนเพียงพอสำหรับหน่วยงานหรือบุคคลที่ได้รับมอบหมายที่มีอำนาจหน้าที่ในการสืบสวนสอบสวน ซึ่งการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ดังกล่าวนั้นต้องสามารถระบุได้ว่าผู้ให้บริการการติดต่อสื่อสารรายใดและเส้นทางการติดต่อสื่อสารเส้นทางใดมีการส่งข้อมูลในการติดต่อสื่อสาร (Article 17)

3. หลักการเกี่ยวกับการออกคำสั่งให้ส่งข้อมูลที่อยู่ในระบบ หลักการดังกล่าวนี้เป็นการกำหนดให้มีหน่วยงานที่มีอำนาจหน้าที่ในการออกคำสั่ง ให้ผู้ที่ครอบครองและควบคุมข้อมูลคอมพิวเตอร์ส่งข้อมูลดังกล่าวให้หน่วยงานนั้น โดยผู้ที่ครอบครองและควบคุมข้อมูลจะต้องเป็นหน่วยงานหรือบุคคลที่อยู่ภายในอาณาเขตของประเทศตน ทั้งนี้ ข้อมูลคอมพิวเตอร์ที่ต้องการให้มีการส่งจะต้องมีการระบุเฉพาะเจาะจงว่าข้อมูลดังกล่าวคือข้อมูลชนิดใด ข้อมูลที่อยู่ในความครอบครองหรือควบคุมของนั้นต้องเก็บอยู่ในระบบคอมพิวเตอร์หรือในสื่อกลางที่ใช้เก็บข้อมูลนั้น รวมถึงการออกคำสั่งดังกล่าวยังรวมถึงการออกคำสั่งให้ผู้ให้บริการที่อยู่ในอาณาเขตของประเทศส่งข้อมูลของสมาชิก หรือผู้รับบริการที่อยู่ในความครอบครองและหรือควบคุมของผู้ให้บริการรายนั้นไปให้ (Article 18)

ในการออกคำสั่งให้ส่งข้อมูลนั้น อาจมีการกำหนดชนิดของการให้บริการติดต่อสื่อสาร ข้อกำหนดโดยเฉพาะที่ใช้กับการให้บริการติดต่อสื่อสารแต่ละประเภท และกำหนดระยะเวลาของการให้บริการ รวมถึงการกำหนดให้มีรายละเอียดข้อมูลที่จะทำให้สามารถบ่งชี้ถึงผู้สมัครเป็นสมาชิกได้ เช่น ที่อยู่ หมายเลขโทรศัพท์และหมายเลขอื่นๆ ที่จะสามารถติดต่อได้ ข้อมูลเกี่ยวกับการเรียกเก็บเงินและการชำระเงิน รวมถึงข้อมูลอื่นๆ ที่เกี่ยวข้องกับการติดตั้งอุปกรณ์การติดต่อสื่อสาร ประเทศภาคีต้องทำการกำหนดข้อมูลต่างๆเหล่านี้เป็นข้อมูลพื้นฐานในข้อตกลงในการให้บริการหรือสิ่งที่ผู้ใช้บริการหรือสมาชิกต้องปฏิบัติในการให้บริการ (Article 18 (3) (a) (b) (c))

ทั้งนี้ เพื่อให้มาตรการดังกล่าวของประเทศภาคีเป็นไปในทิศทางเดียวกัน และไม่ก่อให้เกิดอุปสรรคในการบังคับใช้กฎหมาย อนุสัญญาจึงได้กำหนดความหมายของคำว่า "ข้อมูลของผู้สมัครเป็นสมาชิก" หมายถึง ข้อมูลใดๆที่ถูกบรรจุในรูปแบบของข้อมูลคอมพิวเตอร์หรือรูปแบบอื่นๆที่ผู้ให้บริการได้จัดไว้ ซึ่งเกี่ยวข้องกับผู้สมัครเป็นสมาชิก นอกเหนือไปจากข้อมูลจราจรทางคอมพิวเตอร์หรือข้อมูลที่เป็นเนื้อหาของการติดต่อสื่อสาร (Article 18 (3))

4. หลักการค้นและยึดข้อมูลคอมพิวเตอร์ที่ถูกเก็บไว้ หลักการดังกล่าวนี้เป็นการกำหนดให้มีหน่วยงานที่มีอำนาจหน้าที่ในการค้นหรือวิธีอื่นลักษณะทำนองเดียวกันกับการค้นเพื่อเข้าถึงระบบคอมพิวเตอร์หรือบางส่วนของระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์ที่ถูกเก็บไว้ในระบบคอมพิวเตอร์นั้น รวมถึงการค้นเพื่อเข้าถึงสื่อกลางที่ใช้เก็บข้อมูลคอมพิวเตอร์ในกรณีที่ข้อมูลคอมพิวเตอร์นั้นถูกเก็บไว้ภายในอาณาเขตของประเทศตน (Article 19 (1) (a) (b))

การกำหนดมาตรการในการค้นหรือใช้วิธีการอื่นในทำนองเดียวกันกับการค้นเพื่อเข้าถึงระบบคอมพิวเตอร์หรือบางส่วนของระบบคอมพิวเตอร์ หน่วยงานที่มีอำนาจหน้าที่ในการ

ค้นจะใช้อำนาจหน้าที่ดังกล่าวได้ก็ต่อเมื่อมีเหตุอันควรเชื่อได้ว่าข้อมูลที่ต้องการถูกเก็บไว้ในระบบหรือในบางส่วนของระบบคอมพิวเตอร์อีกระบบหนึ่งภายในอาณาเขตของประเทศ และข้อมูลดังกล่าวสามารถเข้าถึงได้โดยชอบหรือเป็นข้อมูลที่มีอยู่แล้วในระบบ ก็ให้หน่วยงานดังกล่าวสามารถยึดหรือเข้าถึงระบบคอมพิวเตอร์นั้นได้ทันที (Article 19 (2))

การเก็บรักษาข้อมูลที่ถูกเก็บในระบบคอมพิวเตอร์ อนุสัญญาได้กำหนดให้หน่วยงานที่มีอำนาจหน้าที่สามารถยึดหรือใช้วิธีการอื่นในทำนองเดียวกันกับการยึด รวมถึงการทำหรือเก็บข้อมูลคอมพิวเตอร์ไว้ การรักษาความถูกต้องของข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องซึ่งเก็บอยู่นั้น การทำให้ข้อมูลที่อยู่ในระบบคอมพิวเตอร์นั้นไม่สามารถเข้าถึงได้ และการสั่งการด้วยเหตุผลให้ผู้ที่มีความรู้เกี่ยวกับการทำงานของระบบคอมพิวเตอร์ให้ข้อมูลที่จำเป็นเพื่อให้หน่วยงานสามารถดำเนินการดังกล่าวได้ ซึ่งวิธีการเหล่านี้จะต้องกระทำเพื่อรักษาระบบหรือบางส่วนของระบบคอมพิวเตอร์หรือสื่อกลางที่ใช้เก็บข้อมูลคอมพิวเตอร์ (Article 19 (2) (a) (b) (c))

5. หลักการรวบรวมข้อมูลคอมพิวเตอร์ตามเวลาที่ใช้ในการประมวลข้อมูลโดยอัตโนมัติ หลักการดังกล่าวนี้เกี่ยวข้องกับการกำหนดอำนาจให้แก่หน่วยงานที่มีอำนาจหน้าที่ในการรวบรวมข้อมูลจราจรทางคอมพิวเตอร์หรือหน้าที่ในการบันทึกข้อมูลจราจรทางคอมพิวเตอร์โดยใช้วิธีการทางเทคนิคในอาณาเขตของประเทศ รวมถึงการสั่งให้ผู้ให้บริการดำเนินการตามความสามารถทางเทคนิคที่มีอยู่เพื่อให้รวบรวมข้อมูลจราจรทางคอมพิวเตอร์หรือให้ความร่วมมือและช่วยเหลือหน่วยงานที่มีอำนาจหน้าที่ดังกล่าวในการรวบรวมหรือบันทึกตามเวลาที่ใช้ในการประมวลผลข้อมูลโดยอัตโนมัติ โดยข้อมูลจราจรทางคอมพิวเตอร์ดังกล่าวเป็นข้อมูลที่ระบุไว้โดยเฉพาะเจาะจงภายในอาณาเขตของประเทศนั้น ทั้งนี้ข้อมูลจราจรทางคอมพิวเตอร์ดังกล่าวจะต้องถูกส่งโดยวิธีการของระบบคอมพิวเตอร์ (Article 20 (1) (a) (b) (i) (ii))

หากประเทศภาคีใดไม่สามารถจัดให้มีมาตรการรวบรวมหรือบันทึกข้อมูลจราจรทางคอมพิวเตอร์โดยใช้วิธีการทางเทคนิคภายในอาณาเขตได้จะต้องจัดให้มีมาตรการอื่นที่จำเป็นมาใช้แทน เพื่อให้เกิดความแน่นอนว่าจะสามารถดำเนินการรวบรวมหรือบันทึกข้อมูลตามเวลาที่ใช้ในการประมวลผลโดยอัตโนมัติ เกี่ยวกับข้อมูลจราจรที่เกี่ยวข้องกับการติดต่อสื่อสารที่ระบุไว้โดยเฉพาะเจาะจงที่มีการส่งในอาณาเขตของประเทศนั้น โดยผ่านการใช้วิธีการทางเทคนิคในอาณาเขตของประเทศ ทั้งนี้ จะต้องมีการกำหนดผู้ให้บริการมีหน้าที่จะต้องเก็บรักษาข้อเท็จจริงหรือข้อมูลใดที่เกี่ยวข้องไว้เป็นความลับเกี่ยวกับการใช้อำนาจหน้าที่ดังกล่าว (Article 20 (2) (3) (4))

6. หลักการดักข้อมูลที่เป็นเนื้อหา มาตรการต่างๆที่อนุสัญญาต้องการให้ประเทศภาคีสมาชิกกำหนดนั้นต้องสัมพันธ์กับระดับความร้ายแรงของความผิดภายในประเทศ เนื่องจากมาตรการเหล่านี้อาจส่งผลกระทบกับสิทธิและเสรีภาพของบุคคล โดยประเทศภาคีจะต้องกำหนดอำนาจหน้าที่ให้แก่หน่วยงานใดหน่วยงานหนึ่งให้มีหน้าที่รวบรวมหรือบันทึกข้อมูลคอมพิวเตอร์โดยใช้วิธีทางเทคนิคภายในอาณาเขตของประเทศตน และกำหนดหน่วยงานที่มีอำนาจสั่งการให้ผู้ให้บริการใช้วิธีการทางเทคนิคตามความสามารถที่มีอยู่เพื่อรวบรวมหรือบันทึกข้อมูลภายในอาณาเขตของประเทศ รวมถึงการสั่งการให้ผู้ให้บริการให้ความร่วมมือและช่วยเหลือหน่วยงานที่มีอำนาจหน้าที่เกี่ยวข้องในการรวบรวมหรือบันทึกตามเวลาที่ใช้ในการประมวลผลข้อมูลโดยอัตโนมัติ เกี่ยวกับข้อมูลที่มีเนื้อหาของการติดต่อสื่อสารที่ระบุไว้โดยเฉพาะเจาะจงในอาณาเขตของประเทศนั้นซึ่งถูกส่งโดยวิธีการของระบบคอมพิวเตอร์ (Article 21 (1) (a) (b) (i) (ii))

หากประเทศภาคีใดไม่สามารถกำหนดมาตรการดังกล่าวได้ จะต้องจัดให้มีมาตรการอื่นทางเทคนิคที่จำเป็นมาใช้แทน เพื่อทำให้เกิดความแน่นอนว่าจะสามารถดำเนินการรวบรวมหรือบันทึกเนื้อหาที่เกี่ยวกับการติดต่อสื่อสารตามเวลาที่ใช้ในการประมวลผลข้อมูลโดยอัตโนมัติ ซึ่งข้อมูลที่เป็นเนื้อหาของการติดต่อสื่อสารจะต้องเป็นเนื้อหาที่ระบุไว้โดยเฉพาะเจาะจงและอยู่ภายในอาณาเขตของประเทศตน ทั้งนี้ ต้องมีการกำหนดผู้ให้บริการมีหน้าที่จะต้องเก็บรักษาข้อเท็จจริงและข้อมูลใดที่เกี่ยวกับการใช้อำนาจหน้าที่ไว้เป็นความลับ (Article 21 (2) (3))

เมื่อทราบถึงมาตรการที่จำเป็นในการสืบสวนสอบสวนเพื่อค้นหาพยานหลักฐานในการดำเนินคดีและการบังคับใช้อำนาจตามกฎหมายตามที่อนุสัญญาได้กำหนดไว้แล้วขั้นตอนต่อไปคือการดำเนินคดีกับผู้กระทำความผิดซึ่งจะต้องคำนึงถึงเขตอำนาจศาลในการดำเนินคดีด้วยว่าศาลใดมีเขตอำนาจในการดำเนินคดีกับผู้กระทำความผิด ซึ่งอนุสัญญานี้ได้กำหนดเขตอำนาจศาลในการดำเนินคดีเกี่ยวกับผู้กระทำความผิดไว้ซึ่งผู้เขียนจะได้อธิบายต่อไป

2.3.3.2 เขตอำนาจในการดำเนินคดีเกี่ยวกับการกระทำความผิด

หลักการทั่วไปเกี่ยวกับการกำหนดเขตอำนาจศาลในการดำเนินคดีที่กฎหมายระหว่างประเทศรับรอง[29] ได้แก่

---

[29] Harvard Research on International Law, Jurisdiction with Respect to Crime, A.J.I.L. vol. 29, Supp. 435, 440 (1935), อ้างถึงใน จุมพต สายสุนทร, กฎหมายระหว่างประเทศ เล่ม 1, พิมพ์ครั้งที่ 6 (กรุงเทพมหานคร: วิญญูชน, 2549), หน้า 281.

1. การใช้เขตอำนาจโดยอาศัยหลักดินแดน (Territorial Principle) หรือ หลักพื้นที่ (Spatiality Principle) การใช้อำนาจตามหลักนี้มิได้จำกัดเฉพาะเขตอำนาจเหนือดินแดนส่วนที่เป็นแผ่นดินเท่านั้น แต่ยังหมายความรวมถึงเขตอำนาจเหนือส่วนของทะเลที่รัฐสามารถใช้เขตอำนาจได้ตามกฎหมายระหว่างประเทศอีกด้วย

2. การใช้เขตอำนาจโดยอาศัยหลักสัญชาติ (Nationality Principle) สัญชาติเป็นจุดเกาะเกี่ยวอีกประการหนึ่งที่ทำให้รัฐเจ้าของสัญชาติสามารถใช้เขตอำนาจเหนือบุคคลและทรัพย์สินที่มีสัญชาตินั้นได้ ไม่ว่าบุคคลหรือทรัพย์สินนั้นจะอยู่ที่ใดก็ตาม และโดยหลักกฎหมายระหว่างประเทศแล้ว รัฐแต่ละรัฐย่อมมีอำนาจที่จะออกกฎหมายเพื่อกำหนดหลักเกณฑ์ในการให้สัญชาติแก่บุคคลได้ แต่ต้องไม่ขัดกับสิทธิของรัฐอื่นตามกฎหมายระหว่างประเทศ จากแนวปฏิบัติของรัฐทั้งหลายที่ยอมรับเป็นการทั่วไปนั้น รัฐอาจให้สัญชาติแก่ทรัพย์บางประเภทได้ เช่น เรือ อากาศยานและอวกาศยาน เป็นต้น การใช้เขตอำนาจศาลในคดีอาญาเหนือบุคคล แบ่งออกเป็น 2 ประเภท คืออำนาจเหนือผู้กระทำความผิด และอำนาจเหนือบุคคลผู้เสียหาย

3. การใช้เขตอำนาจโดยอาศัยหลักป้องกัน (Protective Principle) ตามกฎหมายระหว่างประเทศนั้น รัฐย่อมมีเขตอำนาจเหนือการกระทำความผิดบางประเภทซึ่งกระทำภายนอกดินแดนของรัฐนั้น แต่เป็นการกระทำความผิดที่มุ่งต่อความมั่นคงของรัฐหรือต่อรัฐบาลของรัฐนั้น หรือต่อความมั่นคงทางเศษรฐกิจของรัฐนั้น ทั้งนี้ โดยไม่ต้องคำนึงว่าผู้กระทำความผิดดังกล่าวจะมีสัญชาติของรัฐนั้นหรือไม่ กฎหมายภายในของบางประเทศได้มีการกำหนดเพิ่มเติมว่า การกระทำความผิดนอกดินแดนของรัฐที่รัฐจะใช้เขตอำนาจลงโทษเช่นว่านั้นได้ต้องไม่ปรากฏว่า การกระทำความผิดดังกล่าวเป็นการกระทำที่กฎหมายภายในของรัฐที่ความผิดนั้นเกิดขึ้นให้การรับรองว่าผู้นั้นมีเสรีภาพที่จะกระทำได้ เช่น ข้อ 7 แห่ง Harvard Research on International Law ในส่วนที่เกี่ยวกับการใช้เขตอำนาจของรัฐเหนือการกระทำความผิดทางอาญา โดยกำหนดว่า รัฐมีเขตอำนาจเกี่ยวกับการกระทำความผิดอาญาใดๆ นอกอาณาเขตของตนโดยคนต่างด้าวต่อความมั่นคง บูรณภาพแห่งดินแดน หรือเอกราชทางการเมือง ของรัฐนั้น ทั้งนี้ การกระทำอันเป็นความผิดอาญานั้นต้องมิใช่เป็นการกระทำโดยการใช้เสรีภาพ ซึ่งกฎหมายแห่งสถานที่ที่การกระทำเช่นว่านั้นได้ประกันรับรองไว้

4. การใช้เขตอำนาจโดยอาศัยหลักสากล (Universality Principle) หลักการได้กำหนดความผิดที่เกิดขึ้นเป็นความผิดต่อรัฐทุกรัฐและจะไม่ได้รับความคุ้มครองจากรัฐใดๆ รัฐทุกรัฐย่อมมีเขตอำนาจในการจับกุมผู้กระทำความผิดและดำเนินคดีกับผู้กระทำความผิด โดยมิต้องคำนึงว่าผู้กระทำความผิดจะมีสัญชาติใด รัฐที่จับกุมผู้กระทำความผิดได้ก่อนย่อมมีเขตอำนาจ

ก่อนรัฐอื่นใดที่ดำเนินการฟ้องร้องผู้กระทำความผิดดังกล่าวในรัฐของตน โดยมิจำเป็นต้องส่งตัวผู้กระทำความผิดดังกล่าวให้แก่รัฐอื่นซึ่งร้องขอให้ส่งตัวผู้กระทำความผิดนั้นไปลงโทษ เช่น ความผิดจากการกระทำอันเป็นโจรสลัด

5. การใช้เขตอำนาจโดยอาศัยหลักสนธิสัญญา (Treaty Principle) หลักการนี้เป็นที่ยอมรับของกฎหมายระหว่างประเทศว่า รัฐหนึ่งสามารถออกและบังคับใช้กฎหมายของตนในดินแดนของรัฐอีกรัฐหนึ่งได้ หากรัฐเช่นว่านั้นยินยอมและความยินยอมเช่นว่านั้นมักปรากฏในรูปของสนธิสัญญา เช่น อนุสัญญา Hay-Parilla ค.ศ. 1903 ระหว่างสหรัฐอเมริกาและสาธารณรัฐปานามา

จากที่ผู้เขียนได้กล่าวไว้แล้วในบทที่ 1 ว่าอาชญากรรมทางคอมพิวเตอร์สามารถเกิดขึ้นได้โดยง่าย กล่าวคือ สามารถเกิดขึ้นได้ ณ เวลา และสถานที่ใดๆบนโลกก็ได้โดยอาจเป็นการกระทำความผิดจากระยะไกลซึ่งผู้กระทำความผิดไม่ต้องอยู่ในสถานที่เกิดเหตุเหมือนอาชญากรรมรูปแบบเดิม หรืออาจเป็นการกระทำความผิดข้ามประเทศก็ได้ ซึ่งสิ่งที่ทำให้การกระทำความผิดมีรูปแบบที่เปลี่ยนแปลงไปคือการเชื่อมต่อของระบบคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ต ซึ่งอาชญากรรมทางคอมพิวเตอร์ที่ได้กระทำผ่านทางอินเทอร์เน็ตทำให้การบังคับใช้กฎหมายเปลี่ยนแปลงไปด้วย เพราะการบังคับใช้กฎหมายจะต้องสามารถดำเนินคดีกับการไร้พรมแดนของการกระทำความผิดในรูปแบบนี้ได้ ประเด็นเรื่องเขตอำนาจศาลจึงเป็นประเด็นที่นานาประเทศให้ความสำคัญ เนื่องจากผลของการกระทำความผิดอาจเกิดขึ้นในเขตแดนหลายประเทศ เขตอำนาจศาลในการดำเนินคดีอาจมีความเกี่ยวเนื่องกัน ทำให้เกิดปัญหาว่าความผิดที่เกิดขึ้นนั้นอยู่ในเขตอำนาจศาลของประเทศใด ในอนุสัญญาบัญญัติเขตอำนาจศาลที่มีความยืดหยุ่นสำหรับหลายประเทศในการตัดสินประเด็นเรื่องเขตอำนาจศาลที่เกี่ยวเนื่องกัน[30]

อนุสัญญานี้จึงได้กำหนดให้มีเขตอำนาจศาลของการดำเนินคดีของแต่ละประเทศเหนือความผิดทั้งหมดตามที่กำหนดในอนุสัญญา โดยเขตอำนาจศาลที่ประเทศภาคีสามารถอ้างได้ 4 กรณี ดังนี้

1) เขตอำนาจเหนือการกระทำความผิดตามหลักดินแดน หมายถึง ความผิดที่ได้กระทำลงในอาณาเขตของประเทศ (Article 22 (1) (a)) หรือ

---

[30] Shannon L. Hopkins, Cybercrime Convention : a Positive Beginning to a Long Road Ahead, Journal of High Technology Law. [Online], 2003, p 2.

2) เขตอำนาจเหนือเรือที่ชักธงของรัฐ หมายถึง ความผิดที่ได้กระทำลงในเรือที่ชักธงของประเทศนั้น (Article 22 (1) (b)) หรือ

3) เขตอำนาจเหนืออากาศยานที่จดทะเบียนตามกฎหมายของรัฐ หมายถึง ความผิดที่ได้กระทำลงในอากาศยานที่จดทะเบียนภายใต้กฎหมายของประเทศนั้น (Article 22 (1) (c)) หรือ

4) เขตอำนาจเหนือผู้กระทำความผิดตามหลักบุคคล หมายถึง ความผิดที่ได้กระทำโดยคนในสัญชาติของประเทศนั้น ในกรณีที่บุคคลดังกล่าวมีการกระทำความผิดนอกอาณาเขตของประเทศและความผิดที่ได้กระทำลงเป็นความผิดที่สามารถลงโทษได้ตามกฎหมายอาญาภายในประเทศ (Article 22 (1) (d))

อย่างไรก็ตามอนุสัญญานี้ให้สิทธิแก่ประเทศภาคีในการที่จะไม่เลือกใช้เขตอำนาจศาลเหนือบุคคล เรือ และอากาศยานที่มีสัญชาติของรัฐ ซึ่งก็หมายความถึงการที่ประเทศภาคีอาจเลือกบังคับใช้เฉพาะเขตอำนาจศาลตามหลักดินแดนเพียงอย่างเดียวก็ได้ (Article 22 (2))

ทั้งนี้ การกำหนดเขตอำนาจศาลตามอนุสัญญาก็มิได้ลบล้างเขตอำนาจศาลในการดำเนินคดีอาญาตามกฎหมายภายในของประเทศภาคีนั้น และหากเกิดกรณีที่หลายประเทศมีการอ้างเขตอำนาจในการดำเนินคดีเหนือความผิดที่มีการกล่าวหา ให้ประเทศภาคีทั้งหลายนั้นปรึกษาหารือกันตามสมควรเพื่อพิจารณาว่าเขตอำนาจการดำเนินคดีของประเทศใดมีความเหมาะสมที่สุดที่จะใช้เพื่อการฟ้องร้องดำเนินคดีอาญากับผู้กระทำความผิดนั้น (Article 22 (3) (4) (5))

อย่างไรก็ดี หลักการเรื่องเขตอำนาจศาลที่กำหนดในอนุสัญญาได้ขจัดอุปสรรคในการดำเนินคดีกับผู้กระทำความผิดที่ไม่ได้รับการส่งตัวในฐานะผู้ร้ายข้ามแดน อันเนื่องจากเหตุผลเรื่องสัญชาติ ไว้ว่า หากเป็นกรณีที่ผู้กระทำความผิดได้ปรากฏตัวในอาณาเขตประเทศ และไม่ได้ทำการส่งตัวผู้กระทำความผิดให้แก่ประเทศอื่นด้วยเหตุผลเรื่องสัญชาติของผู้กระทำความผิด ประเทศที่ผู้กระทำความผิดได้ปรากฏตัวนั้นจะต้องมีมาตรการที่จำเป็นเพื่อกำหนดเขตอำนาจศาลเหนือการกระทำความผิดดังกล่าว เพื่อให้สามารถลงโทษผู้กระทำความผิดได้หากแม้ไม่มีการส่งผู้ร้ายข้ามแดน (Article 22 (3))

จากการกำหนดเขตอำนาจศาลในอนุสัญญานี้ สิ่งที่น่าสนใจคือ อนุสัญญาได้กำหนดเขตอำนาจศาลตามหลักกฎหมายระหว่างประเทศไว้บางหลัก คือ การกำหนดเขตอำนาจศาลเหนือการกระทำความผิดตามหลักดินแดน และการใช้เขตอำนาจศาลโดยอาศัยหลักสัญชาติ

และถึงแม้จะไม่มีบทบัญญัติที่แน่นอนในการแก้ไขเรื่องเขตอำนาจศาลที่เกี่ยวเนื่องกัน เพราะได้กำหนดแต่เพียงว่า หากเกิดกรณีที่มีการอ้างเกี่ยวกับเขตอำนาจศาลที่เกี่ยวเนื่องกันให้ประเทศสมาชิกทำการปรึกษาหารือเพื่อพิจารณาว่าเขตอำนาจการดำเนินคดีของประเทศใดมีความเหมาะสมที่สุด แต่ทั้งนี้ อนุสัญญาก็มีการกำหนดมาตรการที่สามารถขจัดอุปสรรคในการดำเนินคดีกับผู้กระทำความผิดไว้ตามเหตุผลดังกล่าวข้างต้น

2.3.4 มาตรการทางด้านความร่วมมือระหว่างประเทศ

อาชญากรรมทางคอมพิวเตอร์ที่มีลักษณะข้ามประเทศหรือมีการกระทำเกิดขึ้นในพรมแดนของรัฐมากกว่าหนึ่งรัฐ และผู้กระทำความผิดหรือเหยื่อของการกระทำความผิดเป็นพลเมืองของรัฐที่เข้ามาเกี่ยวข้องมากกว่าหนึ่งรัฐ การที่จะปราบปรามอาชญากรรมดังกล่าวให้ได้ผลอย่างจริงจัง มีแนวคิดของนักกฎหมายได้เสนอไว้ว่าให้กำหนดเป็นกฎหมายทั่วไปของทุกรัฐว่า ถ้าไม่ส่งตัวผู้ต้องหาที่กระทำความผิดในรัฐอื่นให้แก่รัฐที่ต้องการตัว ก็ต้องดำเนินคดีกับผู้ต้องหานั้นด้วยตนเอง[31] แต่แนวคิดดังกล่าวก็เป็นไปได้ยากยิ่ง รัฐจึงมีความจำเป็นที่จะต้องมีมาตรการให้ความร่วมมือระหว่างกันในทางอาญาโดยไม่มีรัฐใดที่จะมีอำนาจอธิปไตยเหนือรัฐอื่นนอกเขตแดนของตน หากต้องการความร่วมมือระหว่างประเทศก็ต้องกระทำโดยมาตรการของประเทศนั้นๆ ซึ่งอนุสัญญานี้ได้ตระหนักถึงวิธีการดังกล่าว จึงได้มีการบัญญัติมาตรการด้านความร่วมมือระหว่างประเทศไว้ซึ่งผู้เขียนจะอธิบายโดยแบ่งออกเป็น 3 หลักการ ได้แก่

ก. หลักการเกี่ยวกับความร่วมมือระหว่างประเทศ

ข. หลักการเกี่ยวกับการส่งผู้ร้ายข้ามแดน

ค. หลักการเกี่ยวกับการช่วยเหลือซึ่งกันและกัน

2.3.4.1 หลักการเกี่ยวกับความร่วมมือระหว่างประเทศ

ก. หลักการทั่วไปเกี่ยวกับความร่วมมือระหว่างประเทศ จากหลักการของอนุสัญญาที่ตั้งอยู่บนจุดมุ่งหมายที่ต้องการความเป็นเอกภาพในการคุ้มครองสังคมให้ปลอดภัยจากอาชญากรรมทางคอมพิวเตอร์ ซึ่งหลักการดังกล่าวได้บัญญัติไว้ในอรัมภบทของอนุสัญญา รวมถึงต้องการสนับสนุนและเล็งเห็นความจำเป็นของความร่วมมือระหว่างประเทศไม่ว่าจะเป็นทั้งทางภาครัฐและภาคเอกชนในการต่อสู้กับอาชญากรรมทางคอมพิวเตอร์อย่างรวดเร็วและมี

---

[31] สำนักงานอัยการสูงสุด สำนักงานต่างประเทศ, ข้อสังเกตเบื้องต้นในการดำเนินงานตามพระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. 2535[ออนไลน์], แหล่งที่มา: http://www.inter.ago.go.th/law/page8.html[2553, มกราคม 11]

ประสิทธิภาพ และยังมุ่งเน้นให้อนุสัญญานี้ต้องเป็นส่วนเสริมให้หลักเกณฑ์ระหว่างประเทศว่าด้วยความร่วมมือระหว่างประเทศในทางอาญา ตลอดจนแนวทางในการปฏิบัติที่มีการตกลงกันไว้เป็นหลักการโดยบทบัญญัติที่เป็นลายลักษณ์อักษรหรือโดยถ้อยทีถ้อยปฏิบัติต่อกันและกฎหมายภายในของแต่ละประเทศภาคี เหล่านั้นสามารถทำให้การสอบสวนและดำเนินคดีอาชญากรรมทางคอมพิวเตอร์มีประสิทธิภาพมากขึ้น โดยต้องสามารถรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์ที่เกี่ยวกับการกระทำความผิดให้เพียงพอที่จะดำเนินคดีกับอาชญากรได้* ซึ่งบทบัญญัติเกี่ยวกับหลักการทั่วไปเกี่ยวกับความร่วมมือระหว่างประเทศ ตาม Article 23 เป็นไปตามวัตถุประสงค์ของอนุสัญญา เพราะได้กำหนดให้การบังคับใช้หลักเกณฑ์ระหว่างประเทศว่าด้วยความร่วมมือระหว่างประเทศในทางอาญา จะต้องบังคับใช้ในขอบเขตที่กว้างที่สุดเท่าที่จะเป็นไปได้ (...to the widest extent possible for the propose...) รวมถึงหลักเกณฑ์ในการปฏิบัติที่มีการตกลงกันไว้เป็นลายลักษณ์อักษร และไม่เป็นลายลักษณ์อักษรแต่บังคับใช้ตามแนวทางในการปฏิบัติระหว่างกันโดยถ้อยทีถ้อยปฏิบัติ และการบังคับใช้ในขอบเขตที่กว้างที่สุดนี้ยังหมายความรวมถึงกฎหมายภายในของประเทศภาคีเองก็ต้องบังคับใช้ในขอบเขตที่กว้างที่สุดเท่าที่จะเป็นไปได้เช่นกัน ทั้งนี้ก็เพื่อวัตถุประสงค์ในการสืบสวนสอบสวน การดำเนินคดีอาชญากรรมทางคอมพิวเตอร์ และการรวบรวมพยานหลักฐานที่อยู่ในรูปของอิเล็กทรอนิกส์

จากหลักการที่บัญญัติไว้ผู้เขียนให้ข้อสังเกตว่า การบังคับใช้ความร่วมมือระหว่างประเทศภายใต้หลักที่ว่า ต้องบังคับใช้ในขอบเขตที่กว้างที่สุดเท่าที่จะเป็นไปได้ (...to the widest extent possible for the propose...) นั้น เป็นการบัญญัติถ้อยคำที่กว้างซึ่งอาจก่อให้เกิดปัญหาในการพิจารณาถ้อยคำดังกล่าวของแต่ละประเทศภาคีว่าแนวทางในการปฏิบัติของประเทศตนนั้นบังคับใช้ในขอบเขตที่กว้างที่สุดแล้วหรือไม่ แต่ทั้งนี้ ปัญหาดังกล่าวประเทศภาคีอาจต้องคำนึงถึงวัตถุประสงค์ของอนุสัญญาเป็นสำคัญว่าความร่วมมือดังกล่าวสามารถทำให้เกิดการสอบสวนและดำเนินคดีอาชญากรรมทางคอมพิวเตอร์มีประสิทธิภาพมากขึ้น โดยสามารถ

---

* Preamble of Convention on Cyber Crime 2001

...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;... 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:

รวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์ที่เกี่ยวกับการกระทำความผิดได้เพียงพอที่จะดำเนินคดีกับอาชญากรหรือไม่

2.3.4.2 หลักการเกี่ยวกับการส่งผู้ร้ายข้ามแดน

แนวคิดเกี่ยวกับการส่งผู้ร้ายข้ามแดนในคดีอาชญากรรมทางคอมพิวเตอร์ เกิดขึ้นเนื่องจากลักษณะของการก่ออาชญากรรมที่มีความซับซ้อนขึ้นเรื่อยๆ ส่งผลให้การกระทำความผิดต่างๆสามารถกระทำข้ามพรมแดนระหว่างประเทศสองประเทศหรือมากกว่านั้น ผลที่เกิดจากการกระทำความผิดก็อาจเกิดขึ้นได้ในหลายประเทศเช่นกัน ปัญหาที่เกิดขึ้นตามมา คือหากการกระทำความผิดดังกล่าวเป็นการกระทำความผิดข้ามพรมแดน การนำตัวผู้กระทำความผิดมาลงโทษ ไม่ว่าจะเป็นกรณีที่ผู้กระทำผิดหลบหนีหรือหลบซ่อนตัวยังอีกประเทศหนึ่งประเทศผู้เสียหายก็ย่อมไม่มีทางที่จะดำเนินคดีความผิดทางอาญากับบุคคลดังกล่าวได้ เพราะการที่จะไปจับกุมตัวผู้กระทำความผิดในประเทศอื่นถือเป็นการล่วงละเมิดอำนาจอธิปไตยของประเทศอื่น และจากเงื่อนไขสำคัญในการดำเนินคดีอาญา คือ การนำตัวบุคคลผู้กระทำความผิดมาปรากฏตัวต่อศาล เพราะการฟ้องคดีอาญานั้นศาลไม่อาจลงโทษแก่บุคคลที่ไม่มาปรากฏตัวแก่ศาลไม่ได้หรือไม่อาจพิพากษาไปเพียงฝ่ายเดียวได้ ดังนั้น วิธีการที่สามารถเยียวยาปัญหาดังกล่าวได้ คือ ความร่วมมือระหว่างประเทศ ที่เรียกว่า การส่งผู้ร้ายข้ามแดน

วัตถุประสงค์ในการส่งผู้ร้ายข้ามแดนเพื่อประโยชน์ในการปราบปรามอาชญากรรมทางคอมพิวเตอร์โดยการส่งตัวผู้กระทำความผิดที่หลบหนีไปยังประเทศอื่นกลับไปยังประเทศที่ความผิดเกิดขึ้น หรือประเทศที่มีเขตอำนาจการดำเนินคดีเหมาะสมกับความผิดที่เกิดขึ้นมากที่สุด เพื่อฟ้องร้องดำเนินคดีอาญากับผู้กระทำความผิด ซึ่งตามปกติเขตอำนาจศาลที่สามารถร้องขอให้ส่งผู้ร้ายข้ามแดนจะเกิดขึ้นเมื่อการกระทำความผิดนั้นได้กระทำลงในเขตอำนาจศาลของประเทศที่ร้องขอและบุคคลที่กระทำความผิดได้หลบหนีมาอยู่ในเขตอำนาจศาลของประเทศที่รับคำร้องขอ ซึ่งหลักเกณฑ์ทั่วไปในการพิจารณาส่งผู้ร้ายข้ามแดนที่ได้รับการยอมรับในทางระหว่างประเทศ[32] มีดังนี้

1. หลักความผิดอาญาของทั้งสองประเทศ (Double Criminality) ความผิดอาญาที่สามารถดำเนินการร้องขอให้มีการส่งผู้ร้ายข้ามแดนต้องปรากฏว่าเป็นความผิดตามกฎหมาย

---

[32] การผนึกกำลังและการโต้ตอบ : การดำเนินกลยุทธ์ร่วมกันในการป้องกันอาชญากรรมและความยุติธรรมทางอาญา, ใน รายงานของประเทศไทย การประชุมสหประชาชาติว่าด้วยการป้องกันอาชญากรรมและความยุติธรรมทางอาญา ครั้งที่ 11, หน้า 50. วันที่ 18-25 เมษายน พ.ศ. 2548 ประเทศไทย, 2548.

ภายในของทั้งสองรัฐคือรัฐผู้ร้องขอและรัฐผู้รับคำร้องขอ แต่ในปัจจุบันได้มีการผ่อนคลายหลักนี้ลงไปอย่างมาก เนื่องจากเป็นการสร้างภาระของรัฐในการพิจารณาและตรวจสอบว่าความผิดที่มีการร้องขอนั้นเป็นความผิดตามกฎหมายภายในของรัฐผู้ร้องขอหรือไม่ ทั้งยังสร้างความยากลำบากให้ศาลของบางประเทศในการตรวจสอบและเปรียบเทียบถึงความแตกต่างกันในรายละเอียดของทั้งสองประเทศ ส่งผลให้การส่งผู้ร้ายข้ามแดนไม่ก่อให้เกิดผลในทางปฏิบัติ

2. หลักการกำหนดฐานความผิดและกำหนดโทษขั้นต่ำ หมายถึง กรณีที่รัฐทั้งสองได้มีการทำสนธิสัญญาการส่งผู้ร้ายข้ามแดนระหว่างกันและได้กำหนดประเภทหรือฐานความผิดโดยเฉพาะเจาะจงไว้ในสนธิสัญญา ซึ่งวิธีนี้ก่อให้เกิดปัญหาคือ สนธิสัญญาที่มีอยู่ไม่เพียงพอและไม่ครอบคลุมถึงความผิดที่เกิดขึ้นใหม่ บางประเทศจึงได้หันมาใช้วิธีการระบุอัตราโทษขั้นต่ำแทนการกำหนดฐานความผิด ซึ่งอัตราโทษขั้นต่ำดังกล่าวขึ้นอยู่กับการตกลงระหว่างรัฐภาคีสนธิสัญญา

3. หลักการดำเนินคดีตามที่ได้ระบุในคำร้องขอ หมายถึง การที่รัฐผู้ร้องขอไม่อาจดำเนินคดีกับผู้กระทำความผิดในฐานความผิดอื่น หากไม่ใช่ความผิดตามที่ระบุไว้ในคำร้องขอให้มีการส่งผู้ร้ายข้ามแดน

4. หลักการเรื่องเขตอำนาจศาล หมายถึง การที่รัฐผู้ร้องขอจะต้องเป็นรัฐที่มีเขตอำนาจศาลในการดำเนินคดีกับผู้กระทำความผิด

ข้อยกเว้นของการส่งผู้ร้ายข้ามแดน ได้แก่ หลักเกณฑ์เรื่องความผิดทางการเมืองและหลักเกณฑ์ในเรื่องผู้กระทำความผิดเป็นบุคคลในสัญชาติผู้รับคำร้องขอ ทั้งสองหลักเกณฑ์ดังกล่าวนี้ถือได้ว่าเป็นเหตุผลแห่งการปฏิเสธในการไม่ส่งผู้ร้ายข้ามแดน

เจตนารมณ์ของการส่งผู้ร้ายข้ามแดนก็เพื่อรักษาความสงบเรียบร้อยในสังคมทุกประเทศทั่วโลกจำเป็นต้องมีส่วนร่วม คือต้องให้ความช่วยเหลือซึ่งกันและกันในการปราบปรามอาชญากรรม ซึ่งอนุสัญญานี้ได้เล็งเห็นถึงความสำคัญของการกำหนดหลักการเฉพาะเจาะจงสำหรับการปราบปรามอาชญากรที่กระทำความผิดเกี่ยวกับคอมพิวเตอร์ จึงได้กำหนดหลักเกณฑ์เกี่ยวกับการส่งผู้ร้ายข้ามแดนในคดีอาชญากรรมทางคอมพิวเตอร์ไว้ว่า การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่กำหนดไว้ในอนุสัญญาทั้ง 9 ฐานความผิด สามารถส่งผู้ร้ายข้ามแดนได้หากประเทศภาคีได้กำหนดความผิดการกระทำความผิดดังกล่าวเป็นความผิดทางอาญาตามกฎหมายภายในของประเทศภาคีทั้งสอง และได้กำหนดโทษสำหรับความผิดดังกล่าวถึงขั้นจำคุก

ในอัตราขั้นสูงมีกำหนดตั้งแต่หนึ่งปีขึ้นไป หรืออัตราโทษที่หนักกว่านั้น ก็สามารถพิจารณาส่งผู้ร้ายข้ามแดนระหว่างกันได้

จากหลักเกณฑ์ดังกล่าวหากผู้กระทำความผิดได้กระทำความผิดในเขตอำนาจศาล ไม่ว่าจะเป็นความผิดฐานการเข้าถึงโดยมิชอบ การดักรับข้อมูลโดยมิชอบ การแทรกแซงต่อข้อมูล การแทรกแซงต่อระบบ การนำสิ่งที่ได้จากคอมพิวเตอร์ไปใช้ในทางมิชอบ การปลอมแปลงเกี่ยวกับคอมพิวเตอร์ ความผิดเกี่ยวกับการใช้คอมพิวเตอร์ในการฉ้อโกง การกระทำที่เป็นความผิดเกี่ยวกับสื่อลามกอนาจารเกี่ยวกับเด็ก และการละเมิดลิขสิทธิ์และสิทธิที่เกี่ยวข้องกับลิขสิทธิ์ ประเทศภาคีในฐานะผู้รับคำร้องขอและผู้รับคำร้องขอได้กำหนดอัตราโทษจำคุกขั้นสูงที่มีกำหนดตั้งแต่ 1 ปี ขึ้นไป หรือหนักกว่านั้นสำหรับความผิดดังกล่าว ประเทศภาคีสมาชิกทั้งสองประเทศก็สามารถส่งผู้ร้ายข้ามแดนระหว่างกันได้ (Article 24 (1) (a))

สำหรับความผิดที่มีการกำหนดอัตราโทษขั้นต่ำไว้แตกต่างกันอนุสัญญานี้ก็ได้กำหนดให้สามารถส่งผู้ร้ายข้ามแดนระหว่างประเทศภาคีสมาชิกได้ ถ้าหากอัตราโทษขั้นต่ำที่ว่านั้นมีการนำมาใช้เป็นแนวปฏิบัติ โดยอาจมีการตกลงกันเป็นลายลักษณ์อักษร เช่น สนธิสัญญาว่าด้วยการส่งผู้ร้ายข้ามแดน หรือในกรณีที่ไม่มีสนธิสัญญาการส่งผู้ร้ายข้ามแดนระหว่างกันแต่ได้นำมาใช้โดยถ้อยทีถ้อยปฏิบัติต่อกัน หรือนำมาใช้ภายใต้สนธิสัญญาว่าด้วยการส่งผู้ร้ายข้ามแดน ทั้งนี้ แนวปฏิบัติดังกล่าวให้รวมถึงอนุสัญญาของสภายุโรปว่าด้วยการส่งผู้ร้ายข้ามแดน ลำดับที่ 24 (European Convention on Extradition : ETS No. 24)* ซึ่งแนวปฏิบัติเหล่านั้นสามารถใช้บังคับได้ระหว่างประเทศภาคีตั้งแต่สองประเทศหรือมากกว่านั้น อนุสัญญาได้กำหนดให้ประเทศภาคีสมาชิกที่มีการตกลงกันภายใต้แนวปฏิบัติดังกล่าวสามารถส่งผู้ร้ายข้ามแดนระหว่างกันได้ (Article 24 (1) (b))

การที่อนุสัญญากำหนดหลักเกณฑ์เช่นนี้ ถือได้ว่าสามารถแก้ปัญหาเกี่ยวกับหลักเกณฑ์การส่งผู้ร้ายข้ามแดนในกรณีที่รัฐทั้งสองได้มีการทำสนธิสัญญาในการส่งผู้ร้ายข้ามแดนระหว่างกันและได้กำหนดประเภทความผิดโดยเฉพาะเจาะจงไว้ในสนธิสัญญา โดยมีเหตุผลตามที่ผู้เขียนได้เสนอไปคือ สนธิสัญญาดังกล่าวอาจไม่เพียงพอและไม่ครอบคลุมถึงความผิดที่เกิดขึ้น

---

* Article 2 Extraditable offences of European Convention on Extradition

1. Extradition shall be granted in respect of offences punishable under the laws of the requesting Party and of the requested Party by deprivation of liberty or under a detention order for a maximum period of at least one year or by a more severe penalty. Where a conviction and prison sentence have occurred or a detention order has been made in the territory of the requesting Party, the punishment awarded must have been for a period of at least four months...

ใหม่ การระบุอัตราโทษขั้นต่ำแทนการกำหนดฐานความผิดจึงเป็นทางเลือกที่ดีสำหรับการส่งผู้ร้ายยข้ามแดน

ในกรณีที่ประเทศภาคีสมาชิกได้มีสนธิสัญญาว่าด้วยการส่งผู้ร้ายข้ามแดนระหว่างกัน อนุสัญญาได้กำหนดให้ประเทศภาคีดังกล่าวระบุให้ความผิดเกี่ยวกับคอมพิวเตอร์เป็นความผิดประเภทที่อาจมีการส่งผู้ร้ายข้ามแดนระหว่างกันได้ ทั้งนี้ หากประเทศภาคีสมาชิกอยู่ในระหว่างการตกลงเกี่ยวกับสนธิสัญญาส่งผู้ร้ายข้ามแดนระหว่างกัน ก็ให้ระบุให้ความผิดเกี่ยวกับคอมพิวเตอร์เป็นความผิดประเภทที่มีการส่งผู้ร้ายข้ามแดนระหว่างกันไว้ในสนธิสัญญานั้นด้วย (Article 24 (2))

ในกรณีที่ประเทศภาคีสมาชิกที่ต้องการให้มีการส่งผู้ร้ายข้ามแดนแต่มิได้มีการทำสนธิสัญญาว่าด้วยการส่งผู้ร้ายข้ามแดนระหว่างกัน ประเทศภาคีผู้รับคำร้องขออาจพิจารณาใช้อนุสัญญาฉบับนี้เป็นแนวทางของกฎหมายในการส่งผู้ร้ายข้ามแดนสำหรับกรณีความผิดทางอาญาที่มีโทษจำคุกในอัตราขั้นสูงที่มีกำหนดตั้งแต่หนึ่งปีขึ้นไป หรืออัตราโทษที่หนักกว่านั้น (Article 24 (3))

หากประเทศภาคีไม่ได้กำหนดหลักเกณฑ์เกี่ยวกับการส่งผู้ร้ายข้ามแดนว่าจะต้องเป็นไปตามเงื่อนไขที่ระบุไว้ในสนธิสัญญาที่มีอยู่นั้น ให้ถือว่าความผิดทางอาญาที่มีโทษจำคุกในอัตราขั้นสูงที่มีกำหนดตั้งแต่หนึ่งปีขึ้นไป หรืออัตราโทษที่หนักกว่านั้น เป็นความผิดที่สามารถดำเนินการส่งผู้ร้ายข้ามแดนได้ในระหว่างประเทศภาคี (Article 24 (4))

การพิจารณาหลักเกณฑ์เกี่ยวกับการส่งผู้ร้ายข้ามแดนให้เป็นไปตามเงื่อนไขที่ระบุไว้ในกฎหมายของประเทศภาคีที่รับคำร้องขอ หรือให้เป็นไปตามที่กำหนดไว้ในสนธิสัญญาส่งผู้ร้ายข้ามแดน รวมถึงเหตุผลที่ประเทศภาคีผู้รับคำร้องขอจะสามารถปฏิเสธไม่ส่งผู้ร้ายข้ามแดนด้วย (Article 24 (5))

กรณีที่มีการร้องขอให้ส่งผู้ร้ายข้ามแดนในความผิดประเภทที่มีโทษจำคุกในอัตราขั้นสูงที่มีกำหนดตั้งแต่หนึ่งปีขึ้นไป หรืออัตราโทษที่หนักกว่านั้น แต่ประเทศผู้รับคำร้องขอปฏิเสธด้วยเหตุผลเรื่องสัญชาติของบุคคลที่กระทำความผิดว่าเป็นคนชาติในรัฐผู้รับคำร้องขอ หรืออาจปฏิเสธเพราะเห็นว่ามีเขตอำนาจการดำเนินคดีเหนือความผิดนั้นเช่นกัน ประเทศภาคีที่รับคำร้องขอจะต้องส่งคดีนั้นไปให้หน่วยงานที่มีอำนาจหน้าที่ในการฟ้องร้องดำเนินดคีของประเทศภาคีที่รับคำร้องขอเพื่อดำเนินการต่อไป ยกเว้น จะมีการตกลงกันเป็นอย่างอื่นกับประเทศภาคีที่ร้องขอ

นั้น และหากได้มีการดำเนินคดีจนถึงที่สุดแล้ว ประเทศผู้รับคำร้องขอจะต้องส่งรายงานผลที่สุดของคดีไปให้ประเทศภาคีที่ร้องขอได้ทราบตามสมควร

ทั้งนี้ อนุสัญญายังได้กำหนดให้ประเทศภาคีกำหนดหน่วยงานที่มีอำนาจหน้าที่ในการตัดสินใจและการปฏิบัติเกี่ยวกับการสอบสวนและการดำเนินคดี ให้อยู่ในมาตรฐานเดียวกันกับที่ประเทศภาคีดำเนินการต่อความผิดอื่นๆ ที่มีลักษณะในทำนองเดียวกันภายใต้กฎหมายภายในของประเทศนั้น ซึ่งชื่อและที่ตั้งของหน่วยงานที่มีหน้าที่รับผิดชอบในการจัดหาหรือรับคำร้องขอเกี่ยวกับการส่งผู้ร้ายข้ามแดนหรือการจับกุมบุคคลในกรณีที่ไม่มีสนธิสัญญาที่เกี่ยวข้อง ประเทศภาคีต้องแจ้งให้เลขาธิการของสภายุโรปทราบ และจะต้องดำเนินการให้เกิดความแน่นอนว่าข้อมูลรายละเอียดที่แจ้งไว้ความถูกต้องอยู่เสมอ โดยการแจ้งถึงข้อมูลรายละเอียดหน่วยงานดังกล่าวนั้นให้แจ้งในเวลาที่มีการลงนามเป็นภาคีหรือยื่นเอกสารหลักฐานของการให้สัตยาบัน การยอมรับ การเห็นชอบ หรือการภาคยานุวัติ โดยเลขาธิการของสภายุโรปจะต้องจัดทำและเก็บรักษาทะเบียนรายการเกี่ยวกับหน่วยงานดังกล่าวไว้ด้วย (Article 24 (6) (7))

จากมาตรการดังกล่าวที่อนุสัญญากำหนดในเรื่องการส่งผู้ร้ายข้ามแดน ผู้เขียนมีข้อสังเกตดังนี้ คือ สิทธิในการร้องขอให้มีการส่งผู้ร้ายข้ามแดนตามที่ปรากฏในอนุสัญญาจำกัดเฉพาะประเทศภาคีสมาชิกเท่านั้น ส่วนประเทศที่ไม่ได้เป็นภาคีอนุสัญญาหากผู้กระทำความผิดได้หลบหนีเข้ามายังประเทศภาคีอีกทั้งประเทศดังกล่าวมิได้มีสนธิสัญญาว่าด้วยการส่งผู้ร้ายข้ามแดนระหว่างกันกับประเทศภาคี ก็ไม่อาจได้รับความร่วมมือระหว่างประเทศเกี่ยวกับมาตรการนี้

2.3.4.3 หลักการเกี่ยวกับการช่วยเหลือซึ่งกันและกัน

หลักการเกี่ยวกับการช่วยเหลือซึ่งกันและกันก็เช่นเดียวกันกับหลักการอื่นๆ ที่จะต้องคำนึงถึงวัตถุประสงค์ของอนุสัญญาที่ต้องการให้ประเทศภาคีสามารถใช้วิธีการที่รวดเร็วและมีประสิทธิภาพในการสืบสวนสอบสวนเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ ซึ่งถือได้ว่าเป็นอาชญากรรมรูปแบบใหม่ที่นานาประเทศกำลังเผชิญ วิธีการที่รวดเร็วและมีประสิทธิภาพในการสืบสวนสอบสวนอาชญากรรมรูปแบบใหม่จำต้องกำหนดหลักเกณฑ์โดยเฉพาะเจาะจงสำหรับการป้องกันและปราบปราม

ความร่วมมือระหว่างประเทศที่กำหนดไว้ในอนุสัญญาอีกประการหนึ่งคือการช่วยเหลือซึ่งกันและกันทางอาญา ซึ่งการช่วยเหลือซึ่งกันและกันดังกล่าวเป็นการช่วยเหลือเพื่อวัตถุประสงค์ในการสอบสวน หรือดำเนินคดีต่อความผิดทางอาญาที่เกี่ยวกับระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ หรือเพื่อรวบรวมพยานหลักฐานที่อยู่ในรูปของอิเล็กทรอนิกส์เกี่ยวกับการ

กระทำความผิดทางอาญา อนุสัญญานี้ได้บัญญัติหลักเกณฑ์ในการให้ความช่วยเหลือซึ่งกันและกันระหว่างประเทศภาคีว่าต้องให้การช่วยเหลือซึ่งกันและกันในขอบเขตที่กว้างขวางที่สุดเท่าที่จะเป็นไปได้ (Article 25 (1))

ก. หลักเกณฑ์ทั่วไปในการให้การช่วยเหลือซึ่งกันและกันจึงทำได้ 2 วิธี คือ

1. กรณีที่มีสนธิสัญญาหรือแนวทางปฏิบัติที่บัญญัติเป็นลายลักษณ์อักษร หรือหลักการถ้อยทีถ้อยปฏิบัติต่อกันในเรื่องการช่วยเหลือซึ่งกันและกันที่จะนำมาใช้บังคับได้ในระหว่างประเทศ ประเทศภาคีจะต้องดำเนินการให้มีมาตรการต่างๆ ตามที่กำหนดในหลักเกณฑ์ทั่วไปเกี่ยวกับการช่วยเหลือซึ่งกันและกัน และเงื่อนไขในการช่วยเหลือซึ่งกันและกันให้เป็นไปตามกฎหมายภายในของประเทศภาคีที่ถูกร้องขอ หรือเป็นไปตามสนธิสัญญาว่าด้วยการช่วยเหลือซึ่งกันและกันที่ใช้บังคับอยู่ ดังนั้น ประเทศภาคีที่สามารถให้การช่วยเหลือซึ่งกันและกันในกรณีนี้ได้ต้องปรากฏว่าประเทศภาคีมีสนธิสัญญาว่าด้วยความช่วยเหลือซึ่งกันและกันระหว่างกัน หรือถ้าไม่มีสนธิสัญญาดังกล่าวก็ต้องปรากฏว่าประเทศภาคีจะให้ความช่วยเหลือทำนองเดียวกันเมื่อประเทศภาคีอื่นร้องขอตามหลักการถ้อยทีถ้อยปฏิบัติต่อกันในเรื่องการช่วยเหลือซึ่งกันและกัน (Article 27 (1) (3))

อนุสัญญานี้ยังได้บัญญัติให้มีการผ่อนคลายหลักความผิดอาญาของทั้งสองประเทศ (Double Criminality) นั่นหมายความว่า หากประเทศที่ถูกร้องขอมีการระบุเงื่อนไขในการให้ความช่วยเหลือซึ่งกันและกันว่าจะต้องเป็นความผิดอาญาของทั้งสองประเทศคือประเทศที่ร้องขอและประเทศผู้รับคำร้องขอแล้ว หากว่าการกระทำความผิดอันเป็นมูลฐานให้มีการร้องขอให้ช่วยเหลือซึ่งกันและกันนั้นเป็นความผิดทางอาญาตามกฎหมายภายในของประเทศที่ถูกร้องขอ ทั้งนี้ ไม่คำนึงถึงว่ากฎหมายภายในของประเทศที่ถูกร้องขอได้กำหนดให้การกระทำความผิดนั้นจัดอยู่ในประเภทของความผิด หรือฐานความผิดอย่างเดียวกันกับตามกฎหมายของประเทศที่ร้องขอหรือไม่ก็ตาม ก็ให้ถือว่าความผิดดังกล่าวนั้นเป็นไปตามหลักความผิดอาญาของทั้งสองประเทศแล้ว (Article 25 (5))

เพื่อเป็นการส่งเสริมการช่วยเหลือซึ่งกันและกันในการสอบสวนหรือดำเนินคดีให้มีความรวดเร็วและมีประสิทธิภาพ อนุสัญญายังได้บัญญัติอีกว่า ประเทศภาคีประเทศหนึ่งอาจจัดส่งข้อมูลตามธรรมดาที่ได้จากการสอบสวนไปให้ประเทศภาคีอีกประเทศหนึ่ง ในกรณีที่พิจารณาตามกฎหมายภายในของตนแล้วเห็นว่า การเปิดเผยข้อมูลดังกล่าวจะเป็นการช่วยเหลือประเทศภาคีที่ได้รับข้อมูลสามารถเริ่มต้นหรือการดำเนินคดีเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ตามที่ระบุไว้ในอนุสัญญาฉบับนี้ หรือข้อมูลดังกล่าวอาจนำไปสู่การร้องขอความร่วมมือต่อไปจาก

ประเทศภาคีที่ได้รับข้อมูลโดยไม่จำเป็นต้องมีคำร้องขอมาก่อน ทั้งนี้ ก่อนที่จะมีการจัดส่งข้อมูลธรรมดานั้นประเทศภาคีที่จัดส่งข้อมูลอาจแจ้งว่าขอให้ประเทศภาคีที่รับข้อมูลนั้นเก็บเป็นความลับหรือใช้ข้อมูลนั้นภายใต้เงื่อนไขที่กำหนด หากประเทศภาคีที่รับข้อมูลไม่สามารถที่จะปฏิบัติตามเงื่อนไขนั้นได้ก็ให้แจ้งไปให้ประเทศภาคีที่จัดส่งข้อมูลทราบ เพื่อประเทศที่จัดส่งข้อมูลจะได้พิจารณาต่อไปว่าจะยังคงยินยอมจัดส่งข้อมูลดังกล่าวนั้นไปให้หรือไม่ แต่หากประเทศภาคีที่จะรับข้อมูลนั้นยอมรับที่จะปฏิบัติตามเงื่อนไขนั้นก็จะผูกพันให้ต้องมีหน้าที่ปฏิบัติตามเงื่อนไขนั้น (Article 26)

หากเป็นกรณีฉุกเฉิน อนุสัญญาก็ได้กำหนดมาตรการในการช่วยเหลือซึ่งกันและกันในกรณีฉุกเฉิน โดยได้กำหนดหลักเกณฑ์เฉพาะสำหรับการช่วยเหลือซึ่งกันและกัน ว่าการทำคำร้องให้มีการช่วยเหลือซึ่งกันและกันหรือการติดต่อสื่อสารที่เกี่ยวข้องกับการช่วยเหลือซึ่งกันและกันในกรณีฉุกเฉินสามารถกระทำด้วยวิธีการอันรวดเร็ว อันได้แก่ การส่งโทรสาร หรือจดหมายอิเล็กทรอนิกส์ วิธีการดังกล่าวจะต้องมีระดับที่เหมาะสมของความปลอดภัยและความถูกต้อง (รวมถึงการใช้วิธีเข้ารหัสข้อมูลในกรณีที่จำเป็น) โดยอาจมีการยืนยันโดยทำเป็นลายลักษณ์อักษรอย่างเป็นทางการในภายหลังได้หากประเทศภาคีที่ถูกร้องขอนั้นต้องการ ซึ่งประเทศภาคีที่ถูกร้องขอพึงให้การยอมรับและให้คำตอบสำหรับคำร้องขอดังกล่าวโดยวิธีการที่รวดเร็วเช่นกัน ซึ่งวิธีการดังกล่าวนั้นก็ต้องมีระดับที่เหมาะสมของความปลอดภัยและความถูกต้อง (รวมถึงการใช้วิธีเข้ารหัสข้อมูลในกรณีที่จำเป็น) (Article 25 (3))

2. กรณีที่ไม่มีสนธิสัญญาหรือแนวทางปฏิบัติที่บัญญัติเป็นลายลักษณ์อักษรหรือหลักการถ้อยทีถ้อยปฏิบัติต่อกันในเรื่องการช่วยเหลือซึ่งกันและกันที่จะนำมาใช้บังคับได้ในระหว่างประเทศ ประเทศผู้ร้องขอต้องจัดทำคำร้องขอตามวิธีพิจารณาความที่กำหนดไว้โดยเฉพาะตามกฎหมายภายในประเทศตน ยกเว้นในกรณีที่การจัดทำคำร้องขอดังกล่าวเป็นการไม่สอดคล้องกับกฎหมายของประเทศภาคีที่ถูกร้องขอไม่สามารถทำได้ และเมื่อจัดทำคำร้องขอแล้วเวร็จให้ส่งคำร้องดังกล่าวไปยังหน่วยงานกลางที่ตั้งขึ้นโดยประเทศผู้รับคำร้องขอ เพื่อทำหน้าที่รับผิดชอบในการส่งและตอบคำร้องขอในการช่วยเหลือซึ่งกันและกัน ซึ่งหน่วยงานกลางดังกล่าวต้องมีการจัดการให้เป็นไปตามคำร้องดังกล่าว หรือการจัดส่งคำร้องขอดังกล่าวต่อไปให้หน่วยงานที่มีอำนาจหน้าที่เกี่ยวข้องเพื่อจัดการดังกล่าว (Article 27 (1))

หน่วยงานกลางของแต่ละประเทศภาคีจะทำหน้าที่ประสานงานและทำการติดต่อสื่อสารระหว่างกันโดยตรงเพื่อรับผิดชอบในการส่งและตอบคำร้องขอในการช่วยเหลือซึ่งกันและกัน เมื่อหน่วยงานดังกล่าวได้รับคำร้องขอแล้วต้องทำการพิจารณาพร้อมทั้งแจ้งไปให้

หน่วยงานกลางประเทศภาคีที่ร้องขอให้ทราบอย่างทันท่วงทีถึงผลของการจัดการให้เป็นไปตามคำร้องขอความช่วยเหลือนั้น หากสามารถดำเนินการได้ตามคำร้องขอหรือหากสามารถดำเนินการได้แต่เกิดความล่าช้าต้องแจ้งเหตุผลจำเป็นต้องเกิดความล่าช้า และหากเป็นเรื่องที่ไม่สามารถทำได้หรือจำเป็นต้องเกิดความล่าช้าอย่างมากต้องแจ้งถึงเหตุผลของการปฏิเสธหรือการเลื่อนการจัดการตามคำร้องขอนั้นด้วย (Article 27 (2))

ทำนองเดียวกับการส่งผู้ร้ายข้ามแดนหากมีการตั้งหน่วยงานกลางของแต่ละประเทศภาคีให้ทำหน้าที่รับผิดชอบในการส่งและตอบคำร้องขอในการช่วยเหลือซึ่งกันและกัน ประเทศภาคีต้องแจ้งให้เลขาธิการของสภายุโรปทราบ และจะต้องดำเนินการให้เกิดความแน่นอนว่าข้อมูลรายละเอียดที่แจ้งไว้ความถูกต้องอยู่เสมอ โดยการแจ้งถึงข้อมูลรายละเอียดหน่วยงานดังกล่าวนั้นให้แจ้งในเวลาที่มีการลงนามเป็นภาคีหรือยื่นเอกสารหลักฐานของการให้สัตยาบัน การยอมรับ การเห็นชอบ หรือการภาคยานุวัติ โดยเลขาธิการของสภายุโรปจะต้องจัดทำและเก็บรักษาทะเบียนรายการเกี่ยวกับหน่วยงานดังกล่าวไว้ด้วย (Article 27 (2) (c))

เนื่องจากการช่วยเหลือซึ่งกันและกันต้องมีความรวดเร็ว การเลื่อนการจัดการตามคำร้องอาจมีผลกระทบกับพยานหลักฐาน การสืบสวนสอบสวนและการดำเนินคดีได้ การเลื่อนการจัดการจึงต้องมีเหตุผลที่จำเป็นซึ่งเหตุผลดังกล่าวจะต้องเป็นเหตุผลที่หากประเทศที่รับคำร้องขอได้มีการจัดการตามคำร้องขอนั้นจะส่งผลกระทบต่อการสอบสวนหรือการดำเนินคดีอาญาที่ดำเนินการโดยหน่วยงานของประเทศภาคีที่ถูกร้องขอ ดังนั้น ก่อนที่จะมีการปฏิเสธหรือเลื่อนการให้ความช่วยเหลือดังกล่าวประเทศภาคีที่ถูกร้องขอเมื่อได้ปรึกษาหารือกับประเทศภาคีที่ร้องขอตามที่เห็นสมควรแล้วพิจารณาต่อไปว่าจะดำเนินการตามคำร้องขอนั้นบางส่วนได้หรือไม่ หรือว่าจะให้อยู่ภายใต้เงื่อนไขประการใดตามที่ประเทศภาคีที่ถูกร้องขอนั้นเห็นว่าจำเป็น (Article 27 (6) (7))

ประเทศภาคีที่ร้องขออาจขอให้ประเทศภาคีที่ถูกร้องขอเก็บเป็นความลับซึ่งข้อเท็จจริงของการร้องขอใดที่มีการร้องขอตามบัญญัติในส่วนนี้ตลอดจนเนื้อเรื่องในคำร้องขอนั้น เว้นแต่ในขอบเขตของความจำเป็นเพื่อการจัดการให้เป็นไปตามคำร้องขอ ในกรณีที่ประเทศภาคีที่ถูกร้องขอไม่สามารถทำตามคำขอที่ให้เก็บเป็นความลับดังกล่าวได้ก็ให้แจ้งไปให้ประเทศภาคีที่ร้องขอได้ทราบอย่างทันท่วงทีเพื่อประเทศภาคีที่ร้องขอจะได้พิจารณาต่อไปว่าจะยังคงประสงค์ให้ประเทศภาคีที่ถูกร้องขอดำเนินการตามคำร้องขอนั้นอยู่หรือไม่ (Article 27 (8))

วัตถุประสงค์ของอนุสัญญาตามที่ได้กล่าวมาแล้ว แม้อนุสัญญานี้จะเปิดโอกาสให้การให้ความช่วยเหลือซึ่งกันและกันสามารถบังคับใช้ภายใต้เงื่อนไขที่กำหนดไว้ในกฎหมายของ

ประเทศภาคีที่ถูกร้องขอ ดังนั้น เพื่อให้บรรลุวัตถุประสงค์ของอนุสัญญา และรวมถึงพันธกรณีของประเทศภาคีที่จะต้องสนับสนุนให้หลักการต่างๆที่บัญญัติไว้ในอนุสัญญาสามารถป้องกันและปราบปรามรวมถึงนำตัวผู้กระทำความผิดมาลงโทษได้ ประเทศภาคีที่ถูกร้องขอจึงไม่พึงใช้สิทธิในการปฏิเสธการช่วยเหลือซึ่งกันและกันเกี่ยวกับความผิดประเภทที่ระบุไว้ในอนุสัญญาทั้งหมดเพียงเพราะเหตุผลที่ว่าคำร้องขอดังกล่าวเกี่ยวข้องกับความผิดทางภาษีอากร แต่ทั้งนี้ ประเทศที่รับคำร้องขออาจปฏิเสธไม่ให้ความช่วยเหลือได้ถ้าประเทศภาคีที่รับคำร้องขอพิจารณาแล้วเห็นว่าคำร้องขอนั้นเกี่ยวกับความผิดทางการเมือง หรือเป็นความผิดที่เกี่ยวเนื่องกับความผิดทางการเมือง หรือหากมีการให้ความช่วยเหลือตามคำร้องขอนั้นมีความเป็นไปได้ที่จะส่งผลกระทบต่ออธิปไตย ความมั่งคงปลอดภัย ความสงบเรียบร้อยของประชาชนหรือผลประโยชน์อันสำคัญอย่างอื่นของประเทศ (Article 27 (4))

ในกรณีฉุกเฉินอนุสัญญาในได้กำหนดวิธีปฏิบัติโดยให้มีการส่งคำร้องขอให้มีการช่วยเหลือซึ่งกันและกันหรือการติดต่อสื่อสารที่เกี่ยวข้องกับคำร้องขอนั้น อาจจัดส่งโดยตรงโดยองค์กรศาลของประเทศที่ร้องขอไปยังองค์กรศาลของประเทศที่รับคำร้องขอ แต่ต้องมีการส่งสำเนาของเอกสารดังกล่าวไปให้หน่วยงานกลางของประเทศที่รับคำร้องขอผ่านหน่วยงานกลางของประเทศที่ร้องขอในขณะเดียวกันด้วย หรืออาจดำเนินการผ่านทางองค์การตำรวจสากลก็ได้

และหากองค์กรศาลดังกล่าวไม่มีอำนาจหน้าที่ที่จะดำเนินการเกี่ยวกับคำร้องขอก็ให้องค์กรศาลดังกล่าวส่งคำร้องขอต่อไปให้หน่วยงานแห่งชาติที่มีอำนาจหน้าที่ และแจ้งโดยตรงไปให้ประเทศภาคีที่ร้องขอได้ทราบถึงการส่งต่อคำร้องขอดังกล่าวด้วย หากเป็นคำร้องขอหรือการการติดต่อสื่อสารที่ไม่เกี่ยวข้องกับการใช้อำนาจบังคับ ก็ให้จัดส่งโดยตรงโดยหน่วยงานที่มีอำนาจหน้าที่เกี่ยวข้องของประเทศที่ร้องขอไปยังหน่วยงานที่มีอำนาจหน้าที่เกี่ยวข้องของประเทศที่รับคำร้องขอ (Article 27 (9))

ประเทศภาคีที่รับคำร้องขออาจส่งข้อมูลหรือสิ่งที่จะเป็นการตอบสนองต่อคำร้องขอนั้นโดยกำหนดเงื่อนไขให้เก็บข้อมูลหรือสิ่งนั้นเป็นความลับ ในกรณีที่หากไม่เก็บข้อมูลหรือสิ่งนั้นเป็นความลับแล้วจะทำให้ไม่สามารถดำเนินการตามคำร้องขอให้ช่วยเหลือซึ่งกันและกันนั้นได้หรือไม่ให้นำข้อมูลหรือสิ่งนั้นไปใช้ในการสอบสวนหรือดำเนินคดีอื่นนอกจากคดีที่ระบุไว้ในคำร้องขอนั้น ในกรณีที่ประเทศภาคีที่ร้องขอไม่สามารถปฏิบัติตามเงื่อนไขดังกล่าวได้ประเทศภาคีที่ร้องขอต้องแจ้งให้ประเทศภาคีที่รับคำร้องขอได้ทราบอย่างทันท่วงที เพื่อประเทศภาคีที่รับคำร้องขอจะได้พิจารณาต่อไปว่าสมควรที่จะส่งข้อมูลดังกล่าวนั้นให้หรือไม่ แต่หากประเทศภาคีที่ร้องขอยอมรับในเงื่อนไขดังกล่าวนั้นก็จะต้องผูกพันโดยปฏิบัติตามเงื่อนไขดังกล่าวนั้น

ประเทศภาคีใดที่ส่งข้อมูลหรือสิ่งซึ่งได้กำหนดไว้ในเงื่อนไขของการใช้ ประเทศภาคีนั้นอาจกำหนดให้ประเทศภาคีที่ได้รับข้อมูลหรือสิ่งดังกล่าวต้องแจ้งรายละเอียดให้ทราบว่าได้มีการใช้ข้อมูลหรือสิ่งดังกล่าวนั้นภายใต้เงื่อนไขของการใช้ดังกล่าวแล้ว (Article 28)

ข. หลักการเฉพาะเกี่ยวกับในการให้การช่วยเหลือซึ่งกันและกันกำหนดไว้ 6 หลักการ ดังนี้

1. หลักการเข้าเก็บรักษาข้อมูลคอมพิวเตอร์ที่ถูกเก็บไว้โดยทันที หลักการดังกล่าวนี้ได้กำหนดให้ประเทศภาคีหนึ่งอาจร้องขอให้ประเทศภาคีอีกประเทศหนึ่งออกคำสั่งเพื่อให้ได้มาซึ่งข้อมูลที่ถูกเก็บไว้ หรือดำเนินการให้ได้มาข้อมูลที่ถูกเก็บไว้ด้วยวิธีการของระบบคอมพิวเตอร์โดยเร็ว ในกรณีข้อมูลดังกล่าวอยู่ในอาณาเขตของประเทศภาคีที่ถูกร้องขอ ทั้งนี้ประเทศภาคีที่ร้องขอดังกล่าวประสงค์จะยื่นคำร้องขอความช่วยเหลือต่อไปเกี่ยวกับการค้นหรือวิธีการอื่นในลักษณะทำนองเดียวกันในการเข้าถึงการยึดหรือวิธีการอื่นในลักษณะทำนองเดียวกันในการเก็บรักษาหรือการเปิดเผยซึ่งข้อมูล (Article 29 (1))

คำร้องขอเพื่อให้มีการเก็บรักษาข้อมูลจะต้องมีการระบุรายละเอียดให้ทราบถึงหน่วยงานที่ประสงค์จะให้มีการเก็บรักษาข้อมูล ความผิดซึ่งอยู่ภายใต้การสอบสวนหรือการดำเนินคดีอาญาในเรื่องนั้นและข้อเท็จจริงที่เกี่ยวข้องโดยสรุป ข้อมูลคอมพิวเตอร์ที่ประสงค์จะให้มีการเก็บรักษาและความเกี่ยวพันกับความผิดอย่างไร ข้อมูลคอมพิวเตอร์ที่ต้องการใครเป็นผู้ครอบครอง หรือสถานที่ตั้งของระบบคอมพิวเตอร์ที่เก็บข้อมูลคอมพิวเตอร์นั้น ความจำเป็นที่จะต้องมีการเก็บรักษา ข้อความที่แสดงว่าประเทศภาคีนั้นประสงค์ที่จะยื่นคำร้องขอความช่วยเหลือต่อไปเกี่ยวกับการค้นหาหรือวิธีการอื่นในลักษณะทำนองเดียวกันกับการเข้าถึง การยึดหรือวิธีการอื่นในลักษณะทำนองเดียวกันในการเก็บรักษา หรือการเปิดเผยซึ่งข้อมูลนั้น (Article 29 (2))

เมื่อประเทศภาคีหนึ่งได้รับคำร้องขอจากประเทศภาคีอีกประเทศหนึ่งเกี่ยวกับมาตรการดังกล่าวแล้ว ให้ประเทศภาคีที่รับคำร้องขอดำเนินการตามมาตรการทั้งหมดที่เหมาะสมเพื่อเก็บรักษาข้อมูลโดยเฉพาะเจาะจงตามคำร้องขอในทันที ตามหลักเกณฑ์ของกฎหมายภายในของประเทศภาคีที่รับคำร้องขอนั้น โดยไม่ให้นำหลักการเรื่องความผิดทางอาญาของประเทศทั้งสองประเทศมาเป็นเงื่อนไขของการที่จะเก็บรักษาข้อมูล (Article 29 (3))

แต่หากเป็นความผิดที่อยู่นอกเหนืออนุสัญญา แต่ประเทศภาคีได้กำหนดให้นำหลักการเรื่องความผิดทางอาญาของประเทศทั้งสองฝ่ายมาเป็นเงื่อนไขของการที่จะตอบสนองคำ

ร้องขอให้ช่วยเหลือเกี่ยวกับการค้นหรือวิธีการอื่นในลักษณะทำนองเดียวกันในการเข้าถึง การยึดหรือวิธีการอื่นในลักษณะทำนองเดียวกันในการเก็บรักษา หรือการเปิดเผยซึ่งข้อมูลนั้นแล้ว อาจทำการสงวนสิทธิที่จะปฏิเสธไม่ทำตามคำร้องขอให้เก็บรักษาข้อมูลดังกล่าวนั้นได้ หากว่ามีเหตุผลอันควรเชื่อว่าในเวลาที่จะเปิดเผยซึ่งข้อมูลนั้นปรากฏว่ามิได้เป็นไปตามเงื่อนไขความผิดทางอาญาของประเทศทั้งสองฝ่ายนั้น

ทั้งนี้ ประเทศภาคีผู้รับคำร้องขอสามารถปฏิเสธคำร้องขอให้เก็บรักษาข้อมูลดังกล่าวได้หากว่า ความผิดตามที่ระบุไว้ในคำร้องขอนั้นประเทศภาคีผู้รับคำร้องขอพิจารณาแล้วเห็นว่าเป็นความผิดทางการเมืองหรือเกี่ยวเนื่องกับความผิดทางการเมือง หรือประเทศภาคีผู้รับคำร้องขอพิจารณาแล้วเห็นว่าหากมีการจัดการให้เป็นไปตามคำร้องขออาจจะส่งผลกระทบต่ออธิปไตย ความมั่นคงปลอดภัย ความสงบเรียบร้อยของประชาชนหรือผลประโยชน์อันสำคัญประการอื่นต่อประเทศได้ และในกรณีที่เชื่อว่าการเก็บรักษาข้อมูลดังกล่าวไม่ได้ทำให้เกิดความแน่นอนว่าข้อมูลดังกล่าวจะยังคงมีอยู่ต่อไปในอนาคตหรืออาจจะเป็นภัยต่อความลับ หรือมิฉะนั้นอาจส่งผลกระทบต่อการสอบสวนของประเทศภาคีที่ร้องขอนั้นเองแล้ว ให้ประเทศภาคีผู้รับคำร้องขอแจ้งไปยังประเทศภาคีที่ร้องขออย่างทันท่วงทีเพื่อประเทศภาคีที่ร้องขอจะได้พิจารณาต่อไปว่าจะยังคงประสงค์ให้จัดการตามคำร้องขอนั้นหรือไม่ (Article 29 (5) (6))

ขอบเขตระยะเวลาในการเก็บรักษาข้อมูลตามคำร้องขอดังกล่าว ให้มีกำหนดระยะเวลาไม่น้อยกว่าหกสิบวัน เพื่อให้ประเทศภาคีที่ร้องขอสามารถที่จะยื่นคำร้องขอความช่วยเหลือต่อไปเกี่ยวกับกับการค้นหรือวิธีการอื่นในลักษณะทำนองเดียวกันในการเข้าถึง การยึดหรือวิธีการอื่นในลักษณะทำนองเดียวกันในการเก็บรักษา หรือการเปิดเผยซึ่งข้อมูลนั้น

2. หลักการเปิดเผยข้อมูลคอมพิวเตอร์ที่เก็บรักษาไว้โดยทันที หลักการนี้เป็นหลักการต่อเนื่องภายหลังจากที่มีการจัดการตามคำร้องขอให้เก็บข้อมูลคอมพิวเตอร์ หากคำร้องขอให้เก็บข้อมูลคอมพิวเตอร์นั้นเป็นการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ที่เกี่ยวข้องกับการติดต่อสื่อสารที่เฉพาะเจาะจง และประเทศภาคีที่รับคำร้องขอพบว่าผู้ให้บริการในอีกประเทศหนึ่งมีส่วนเกี่ยวข้องกับการส่งต่อซึ่งการติดต่อสื่อสารนั้นแล้ว ให้ประเทศภาคีผู้รับคำร้องขอเปิดเผยโดยทันทีให้ประเทศภาคีที่ร้องขอทราบถึงข้อมูลจราจรทางคอมพิวเตอร์ในจำนวนที่เพียงพอที่จะสามารถบ่งบอกได้ว่าผู้ให้บริการและเส้นทางใดที่ได้มีการส่งผ่านการติดต่อสื่อสาร

ทั้งนี้ อาจมีการปฏิเสธได้ว่าไม่สามารถดำเนินการเปิดเผยข้อมูลจราจรทางคอมพิวเตอร์ หากเมื่อพิจารณาแล้วพบว่าความผิดที่ระบุในคำร้องขอนั้นเป็นความผิดทางการเมือง หรือเกี่ยวเนื่องกับความผิดทางการเมือง หรือหากมีการจัดการให้เป็นไปตามคำร้องขอ

อาจส่งผลกระทบต่ออธิปไตย ความมั่นคงปลอดภัย ความสงบเรียบร้อยของประชาชนหรือผลประโยชน์อันสำคัญประการอื่นของประเทศได้ (Article 30)

3. หลักการช่วยเหลือซึ่งกันและกันเกี่ยวกับการเข้าถึงข้อมูลคอมพิวเตอร์ที่ถูกเก็บไว้ หลักการนี้เป็นหลักการช่วยเหลือซึ่งกันและกันเกี่ยวกับการสืบสวนสอบสวน โดยประเทศภาคีหนึ่งอาจทำคำร้องขอต่อประเทศภาคีอีกประเทศหนึ่ง เพื่อดำเนินการค้นหรือกระทำโดยวิธีการอื่นในลักษณะทำนองเดียวกันในการเข้าถึง ดำเนินการยึดหรือโดยวิธีการอื่นในลักษณะทำนองเดียวกันในการเก็บรักษา หรือดำเนินการเปิดเผยข้อมูลที่ถูกเก็บไว้โดยวิธีการของระบบคอมพิวเตอร์ที่ตั้งอยู่ในอาณาเขตของประเทศภาคีที่รับคำร้องขอ รวมถึงข้อมูลที่มีการขอให้เก็บรักษาโดยทันที

ประเทศภาคีผู้รับคำร้องขอจะต้องให้คำตอบต่อคำร้องขอนั้นโดยนำหลักเกณฑ์ระหว่างประเทศ แนวทางปฏิบัติและกฎหมายมาใช้พิจารณา ทั้งนี้ จะต้องสอดคล้องกับบทบัญญัติอื่นที่เกี่ยวข้องในการให้ความช่วยเหลือซึ่งกันและกัน คำร้องดังกล่าวจะต้องได้รับการพิจารณาอย่างรวดเร็วเพื่อที่จะให้ได้รับคำตอบโดยเร่งด่วนในกรณีที่มีเหตุผลอันควรเชื่อได้ว่าข้อมูลนั้นความเสี่ยงที่จะสูญหายหรือถูกแก้ไขดัดแปลง หรือหากมีการกำหนดไว้ในหลักเกณฑ์แนวทางปฏิบัติและกฎหมายในการให้ความช่วยเหลือซึ่งกันและกันว่าต้องให้ความร่วมมือโดยเร่งด่วน (Article 31)

ทั้งนี้ การเข้าถึงข้อมูลคอมพิวเตอร์โดยกระทำข้ามพรมแดนนั้น ประเทศภาคีหนึ่งสามารถเข้าถึงข้อมูลที่ถูกเก็บไว้โดยกระทำข้ามพรมแดนได้ไม่ต้องได้รับอนุญาต และไม่คำนึงว่าข้อมูลดังกล่าวจะถูกเก็บไว้ในประเทศใดหากข้อมูลดังกล่าวได้มีการเผยแพร่โดยทั่วไป และหากได้รับอนุญาตจากเจ้าของข้อมูลหรือบุคคลซึ่งมีสิทธิในข้อมูลดังกล่าว การอนุญาตให้เข้าถึงข้อมูลต้องเป็นความยินยอมโดยชอบและโดยสมัครใจ ก็สามารถเข้าถึงข้อมูลดังกล่าวโดยผ่านทางระบบคอมพิวเตอร์ (Article 32)

4. หลักการเปิดเผยข้อมูลทางคอมพิวเตอร์ที่เก็บรักษาไว้โดยทันที หมายถึงกรณีที่มีการข้ามพรมแดนข้อมูลคอมพิวเตอร์ที่เก็บไว้โดยได้รับอนุญาต หรือเมื่อมีการเผยแพร่ทั่วไป ประเทศภาคีประเทศหนึ่งอาจดำเนินการเข้าถึงข้อมูลคอมพิวเตอร์ซึ่งมีการเปิดเผยโดยทั่วไปซึ่งเป็นข้อมูลเปิด โดยไม่คำนึงถึงว่าข้อมูลนั้นเก็บอยู่ในอาณาเขตของประเทศใด รวมถึงเข้าถึงหรือรับโดยผ่านทางระบบคอมพิวเตอร์ในประเทศนั้น ซึ่งข้อมูลคอมพิวเตอร์ที่เก็บอยู่ในประเทศภาคีอีกประเทศหนึ่ง หากว่าประเทศนั้นได้รับความยินยอมโดยชอบและโดยสมัครใจจากบุคคลที่

มีสิทธิโดยชอบในการเปิดเผยข้อมูลต่อประเทศนั้นผ่านทางระบบคอมพิวเตอร์ เช่น เจ้าของข้อมูลโดยไม่ต้องได้รับอนุญาตจากประเทศภาคีอีกประเทศหนึ่ง (Article 30)

5. หลักการช่วยเหลือซึ่งกันและกันในการรวบรวมข้อมูลจราจรทางคอมพิวเตอร์โดยทันที หลักการดังกล่าวนี้ได้กำหนดให้ประเทศภาคีต้องจัดให้มีความช่วยเหลือซึ่งกันและกันในการรวบรวมข้อมูลจราจรทางคอมพิวเตอร์ที่เกี่ยวข้องกับการติดต่อสื่อสารที่เฉพาะเจาะจงซึ่งอยู่ในอาณาเขตของประเทศภาคีที่มีการส่งต่อโดยวิธีการของระบบคอมพิวเตอร์ โดยวิธีการในการให้ความช่วยเหลือนี้ให้เป็นไปตามเงื่อนไขและวิธีพิจารณาที่กำหนดไว้ในกฎหมายภายในของประเทศภาคี

ประเทศภาคีแต่ละประเทศพึงจัดให้มีความช่วยเหลือดังกล่าวอย่างน้อยที่สุดในเรื่องเกี่ยวกับความผิดทางอาญา โดยการรวบรวมข้อมูลจราจรทางคอมพิวเตอร์ในทันที ซึ่งข้อมูลจราจรทางคอมพิวเตอร์นั้นสามารถรวบรวมได้โดยดำเนินการอย่างเดียวกันกับกรณีที่เกิดคดีที่มีลักษณะเดียวกันภายในประเทศของตน (Article 33)

6. หลักการช่วยเหลือซึ่งกันและกันเกี่ยวกับการดักข้อมูลที่เป็นเนื้อหา หลักการดังกล่าวนี้ได้กำหนดให้ประเทศภาคีจะต้องจัดให้มีความช่วยเหลือซึ่งกันและกันในการรวบรวมข้อมูลที่เป็นเนื้อหา หรือบันทึกข้อมูลที่เป็นเนื้อหาของการติดต่อสื่อสารที่เฉพาะเจาะจงซึ่งมีการส่งต่อโดยวิธีการของระบบคอมพิวเตอร์โดยทันที ภายในขอบเขตที่กำหนดในสนธิสัญญาและกฎหมายภายในของประเทศนั้นที่อนุญาตให้กระทำได้ (Article 34)

2.3.5 การกำหนดองค์กรที่มีเครือข่าย 24 ชั่วโมง

หลักการในการกำหนดองค์กรที่มีเครือข่าย 24 ชั่วโมง และตลอด 7 วันในสัปดาห์ที่อนุสัญญาได้บัญญัติให้ประเทศภาคีกำหนดขึ้นนั้น ก็เพื่อความรวดเร็วและมีประสิทธิภาพเกี่ยวกับมาตรการในการดำเนินการตามที่กำหนดไว้ในอนุสัญญา ไม่ว่าจะเป็นการช่วยเหลือโดยทันทีเพื่อวัตถุประสงค์ในการสอบสวนหรือการดำเนินคดีต่อความผิดทางอาญาเกี่ยวกับระบบและข้อมูลคอมพิวเตอร์ หรือเพื่อการรวบรวมพยานหลักฐานในรูปอิเล็กทรอนิกส์เกี่ยวกับความผิดทางอาญาในการช่วยเหลือดังกล่าวจะต้องอำนวยความสะดวก และในกรณีที่ตามกฎหมายภายในและแนวทางในการปฏิบัติของประเทศนั้นอนุญาตให้กระทำได้ก็อาจดำเนินการโดยตรงในมาตรการการให้คำปรึกษา การเก็บรักษาข้อมูล การเก็บรวบรวมพยานหลักฐาน การให้ข้อมูลในทางกฎหมาย และการสืบหาที่อยู่ของผู้ต้องสงสัย (Article 35 (1))

โดยศูนย์ติดต่อประสานงานดังกล่าวจะต้องมีสมรรถภาพเพียงพอที่จะติดต่อสื่อสารกับศูนย์ติดต่อประสานงานของประเทศภาคีอื่นโดยวิธีการที่รวดเร็ว และในกรณีที่ศูนย์ติดต่อประสานงานดังกล่าวไม่ได้เป็นส่วนหนึ่งของหน่วยงานที่ทำหน้าที่รับผิดชอบเกี่ยวกับการช่วยเหลือซึ่งกันและกันระหว่างประเทศและการส่งผู้ร้ายข้ามแดน ศูนย์ดังกล่าวจะต้องทำให้เกิดความแน่นอนว่าสามารถที่จะติดต่อประสานงานกับหน่วยงานดังกล่าวโดยวิธีการที่รวดเร็วทันทีได้ ทั้งนี้ต้องมีดำเนินการให้เกิดความแน่นอนว่ามีบุคคลากรที่ผ่านการฝึกฝนและมีความพร้อมในจำนวนที่เพียงพอสำหรับเข้าปฏิบัติงานในเครือข่ายการติดต่อประสานงานดังกล่าว (Article 35 (2))

2.3.6 การระงับข้อพิพาท

การระงับข้อพิพาทที่อาจเกิดขึ้นเกี่ยวกับการตีความ (Interpretation) หรือการใช้บังคับ (Application) อนุสัญญานี้มีข้อกำหนดว่า หากมีข้อพิพาทเกิดขึ้นให้ประเทศภาคีแจ้งต่อคณะกรรมาธิการของสภายุโรปว่าด้วยปัญหาอาชญากรรม (The European Committee on Crime Problems : CDPC) และอนุสัญญาได้กำหนดให้ประเทศภาคีจัดการปัญหาข้อพิพาทโดยวิธีการเจรจาหารือหรือโดยใช้สันติวิธีอื่นๆตามที่จะตกลงกัน (...or any other peaceful means of their choice...) รวมถึงการส่งพิพาทนั้นไปให้คณะกรรมาธิการของสภายุโรปว่าด้วยปัญหาอาชญากรรม หรือคณะอนุญาโตตุลาการ หรือส่งข้อพิพาทนั้นไปให้ศาลยุติธรรมระหว่างประเทศ (International Court of Justice) และคำตัดสินชี้ขาดที่เกิดขึ้นนั้นจะมีผลผูกพันประเทศคู่พิพาท

เมื่ออนุสัญญานี้ได้มีการระบุไว้อย่างชัดเจน ดังนั้น หากมีข้อพิพาทเกิดขึ้นเกี่ยวกับการตีความหรือการใช้บังคับอนุสัญญา สิ่งที่ประเทศคู่พิพาทจะต้องกระทำคือ จะต้องระงับข้อพิพาทโดยวิธีการเจรจาหารือหรือโดยสันติวิธี ซึ่งวิธีการดังกล่าวนั้นเป็นวิธีการที่ได้รับการยอมรับในทางกฎหมายระหว่างประเทศ เนื่องจากเป็นวิธีการที่คำนึงถึงเรื่องสันติภาพ ความมั่นคง และความยุติธรรมระหว่างประเทศด้วย ซึ่งในระบบกฎหมายระหว่างประเทศนั้น เมื่อกล่าวถึงการระงับข้อพิพาทระหว่างประเทศอาจแบ่งการระงับข้อพิพาทได้เป็น 2 วิธี[33] คือ

1. การระงับข้อพิพาทระหว่างประเทศโดยวิธีการที่มีลักษณะทางตุลาการ เช่น อนุญาโตตุลาการ (Arbitration) หรือศาลยุติธรรมระหว่างประเทศ (International Court of Justice) ซึ่งจะต้องมีการทำคำชี้ขาด (Award) หรือคำวินิจฉัย (Decision) แล้วแต่กรณีและคำชี้ขาดและคำวินิจฉัยเช่นว่านั้นมีผลผูกพันคู่พิพาท ซึ่งมีหลักการและวิธีการดังต่อไปนี้

---

[33] จุมพต สายสุนทร, กฎหมายระหว่างประเทศ เล่ม 2, พิมพ์ครั้งที่ 5 (กรุงเทพมหานคร: วิญญูชน, 2548), หน้า 424.

1) อนุญาโตตุลาการ (Arbitration) ในที่นี้หมายถึงเฉพาะอนุญาโตตุลาการระหว่างประเทศที่มีหน้าที่ชี้ขาดข้อพิพาทระหว่างรัฐโดยอาศัยหลักกฎหมายระหว่างประเทศ การระงับข้อพิพาทวิธีนี้เป็นการระงับข้อพิพาทโดยบุคคลที่สามซึ่งได้รับการคัดเลือกจากคู่พิพาทเพื่อให้ระงับข้อพิพาทโดยคู่พิพาทตกลงยินยอมที่จะผูกพันตามคำชี้ขาดโดยที่คู่พิพาทไม่มีอำนาจสั่งการใดๆแก่อนุญาโตตุลาการที่ได้ตั้งขึ้นและอนุญาโตตุลาการก็ไม่จำเป็นต้องเชื่อฟังคำสั่งใดๆของคู่พิพาทฝ่ายที่เลือกตนด้วย ซึ่งการระงับข้อพิพาทด้วยวิธีนี้แตกต่างจากการระงับข้อพิพาทโดยศาลยุติธรรมระหว่างประเทศ เนื่องจากการที่คู่พิพาทสามารถเลือกบุคคลที่จะทำหน้าที่เป็นอนุญาโตตุลาการได้แล้ว ยังสามารถเลือกใช้กระบวนพิจารณาของอนุญาโตตุลาการได้

2) ศาลยุติธรรมระหว่างประเทศ (International Court of Justice) เป็นองค์กรหลักของสหประชาชาติและมีเขตอำนาจและหน้าที่ตามที่บัญญัติไว้ในธรรมนูญศาลยุติธรรมระหว่างประเทศ (Statute of the International Court of Justice) โดยทั่วไปแล้วศาลยุติธรรมระหว่างประเทศจะเปิดให้แก่รัฐซึ่งเป็นภาคีแห่งธรรมนูญศาลยุติธรรมระหว่างประเทศส่วนรัฐซึ่งมิได้เป็นภาคีก็สามารถนำข้อพิพาทขึ้นสู่การพิจารณาของศาลยุติธรรมระหว่างประเทศได้เช่นกัน แต่ต้องปฏิบัติตามเงื่อนไขที่คณะมนตรีความมั่นคงได้กำหนดไว้และข้อกำหนดเช่นว่านั้นจะต้องไม่ทำให้เกิดความไม่เสมอภาค (Inequality) ระหว่างคู่พิพาท

2. การระงับข้อพิพาทระหว่างประเทศโดยวิธีการที่ไม่มีลักษณะทางตุลาการ วิธีนี้ที่ถือได้ว่าได้รับการยอมรับในทางกฎหมายระหว่างประเทศ เพราะถือว่าเป็นการใช้สันติวิธี เป็นวิธีการระงับข้อพิพาทระหว่างประเทศที่มีลักษณะทางการเมือง หรือทางการทูตระหว่างประเทศโดยไม่จำเป็นต้องอาศัยพื้นฐานทางกฎหมายระหว่างประเทศ กล่าวคือ ไม่จำเป็นต้องอาศัยหลักกฎหมายระหว่างประเทศในการระงับข้อพิพาทและจะไม่มีข้อเสนอแนะ หรือข้อวินิจฉัยใดที่ผูกพันคู่พิพาท แต่เป็นวิธีการระงับข้อพิพาทระหว่างกันเองโดยตรงโดยไม่มีบุคคลที่สามเข้ามาเกี่ยวข้องโดยการเจรจาระหว่างคู่พิพาท (Negotiation) วิธีการตั้งคณะทำงานร่วมกันเพื่อไต่สวนข้อเท็จจริง (Inquiry) วิธีการโดยเชิญบุคคลที่สามเข้าร่วมในการเจรจาระงับข้อพิพาทในฐานะผู้ไกล่เกลี่ย (Mediation) หรือโดยการประนีประนอม (Conciliation) ซึ่งมีหลักการและวิธีการดังต่อไปนี้

1) การเจรจา (Negotiation) การระงับข้อพิพาทโดยการเจรจานั้นจัดได้ว่าเป็นขั้นตอนแรกของการระงับข้อพิพาท ทั้งนี้ เพราะการเจรจาโดยตรงระหว่างคู่พิพาทจะทำให้คู่พิพาทเข้าใจถึงปัญหาที่แท้จริงอันเป็นที่มาของข้อพิพาทดังกล่าวและอาจเสนอวิธีการแก้ไขปัญหานั้นได้ตรงกับความต้องการและพร้อมที่จะระงับข้อพิพาทเช่นว่านั้น บทบาทและความสำคัญของการเจรจา ในฐานะที่เป็นวิธีการที่สามารถตอบสนองได้อย่างรวดเร็วและยืดหยุ่น

ต่อข้อพิพาท ไม่ว่าข้อพิพาทนั้นจะมีลักษณะทางกฎหมายหรือลักษณะอื่นใด จึงอาจนับได้ว่าการเจรจาเป็นวิธีการระงับข้อพิพาทระหว่างประเทศโดยสันติวิธีที่ถือว่ามีประสิทธิภาพมากที่สุด[34] นอกจากนี้ การเจรจาโดยตรงระหว่างคู่พิพาทนอกจากจะสามารถระงับข้อพิพาทได้แล้วยังอาจช่วยเสริมความสัมพันธ์และความเข้าใจอันดีระหว่างคู่พิพาทได้อีกทางหนึ่ง แต่ก็ไม่ได้หมายความว่าการเจรจาจะนำไปสู่การระงับข้อพิพาทที่เป็นธรรมระหว่างคู่พิพาทเสมอไป ทั้งนี้ เพราะการเจรจานั้นมักมีปัจจัยอย่างอื่นเข้ามาเกี่ยวข้องไม่ว่าจะเป็นปัจจัยทางด้านการเมืองหรืออำนาจต่อรองระหว่างคู่พิพาทเพราะคู่พิพาทที่มีอำนาจต่อรองน้อยกว่าย่อมอยู่ในสถานะที่เสียเปรียบก็ได้

2) การไต่สวนข้อเท็จจริง (Inquiry) หมายถึง การไต่สวนข้อเท็จจริงโดยรัฐที่สามเพื่อนำไปสู่ข้อยุติในทางข้อเท็จจริง หากคู่พิพาทไม่สามารถตกลงร่วมกันได้เกี่ยวกับข้อเท็จจริงอันเป็นต้นเหตุแห่งข้อพิพาทแล้ว ก็เป็นการยากที่จะให้คู่พิพาทระงับข้อพิพาทในประเด็นทางกฎหมายซึ่งต้องอาศัยข้อเท็จจริงที่เป็นที่ยุติก่อน ดังนั้นคู่พิพาทจึงอาจตกลงกันในรูปของข้อตกลงเฉพาะกิจเพื่อให้มีการจัดตั้งคณะทำงานร่วมกันในลักษณะของคณะกรรมาธิการร่วมเพื่อสอบสวนข้อเท็จจริงอันเป็นต้นเหตุของข้อพิพาทและทำรายงานการสอบสวนข้อเท็จจริงเช่นว่านั้นเสนอต่อคู่พิพาท โดยไม่มีอำนาจในการทำข้อเสนอแนะ (Recommendation) แต่ประการใด

3) การไกล่เกลี่ย (Mediation) เป็นวิธีการระงับข้อพิพาทระหว่างประเทศอีกวิธีหนึ่งซึ่งจะมีรัฐที่สามในฐานะผู้ไกล่เกลี่ยอาจเป็นรัฐเดียวหรือหลายรัฐก็ได้ที่จะเข้าร่วมในการเจรจาระงับข้อพิพาทโดยจำทำหน้าที่ในการสืบสวนหาข้อเท็จจริงและทำรายงาน พรอมทั้งทำคำเสนอแนะเพื่อให้คู่พิพาทพิจารณา ทั้งนี้ รายงานและคำเสนอแนะดังกล่าวไม่ถือว่าเป็นคำตัดสินชี้ขาดตัดสินหรือมีผลผูกพันคู่พิพาทแต่ประการใด คู่พิพาทยังมีเสรีภาพในการที่จะใช้ดุลพินิจว่าจะยอมรับรายงานหรือข้อเสนอแนะดังกล่าวหรือไม่ วิธีการไกล่เกลี่ยนี้ไม่เป็นที่นิยมมากนักเนื่องจากการระงับข้อพิพาทจะต้องมีรัฐที่สามเข้ามาเกี่ยวข้องอยู่แล้ว หากคำวินิจฉัยชี้ขาดของรัฐที่สามจะมีลักษณะที่มีผลผูกพันคู่พิพาท ก็จะทำให้การระงับระหว่างประเทศดังกล่าวมีความแน่นอนชัดเจนมากกว่าวิธีการไกล่เกลี่ย เพราะข้อเสนอแนะไม่มีผลผูกพันคู่พิพาทแต่ประการใด แต่ทั้งนี้ การไกล่เกลี่ยอาจมีความยืดหยุ่นมากกว่าเพราะอาจนำข้อเสนอแนะไปพิจารณาก่อนที่จะนำไปปฏิบัติตามหรือไม่ก็ได้

4) การประนีประนอม (Conciliation) เป็นวิธีการระงับข้อพิพาทระหว่างประเทศอีกวิธีหนึ่งที่ต้องมีรัฐที่สามเข้ามามีบทบาทในการเจรจาระงับข้อพิพาทในลักษณะของผู้

---

[34] เรื่องเดียวกัน, หน้า 425.

ประนีประนอม ซึ่งจะมีบทบาทและหน้าที่มากเพราะต้องเข้าร่วมในการเจรจาระหว่างคู่พิพาทด้วย การทำข้อเสนอเพื่อนำไปสู่การระงับข้อพิพาท แต่ข้อเสนอย่อมไม่ผูกพันคู่พิพาทเพราะถือว่าเป็นเพียงข้อเสนอแนะเท่านั้น พร้อมทั้งพยายามโน้มน้าวให้รัฐคู่พิพาทระงับข้อพิพาทระหว่างกันฉันท์มิตร[35]

วิธีการในการระงับข้อพิพาทที่ถือเป็นการกระทำในทางการเมืองและไม่ตกอยู่ภายใต้กรอบของกฎหมายระหว่างประเทศอีกวิธีหนึ่งคือ Good Offices หมายถึงการชักชวนให้คู่พิพาทเข้าทำการเจรจาโดยมีบุคคลที่สามแต่ไม่ได้เข้าร่วมการเจรจาเพื่อระงับข้อพิพาท แต่จะทำการอำนวยความสะดวกด้านอื่นๆ ให้คู่พิพาทซึ่งจัเป็นการระงับข้อพิพาทโดยการเจรจาระหว่างคู่พิพาทโดยตรง หากแต่การเจรจาเช่นว่านั้นเกิดจากการชักชวนของรัฐที่สาม ซึ่งกฎหมายระหว่างประเทศไม่ได้บังคับหรือกำหนดว่าจะต้องมีการระงับข้อพิพาทโดยวิธี Good Offices เพียงแต่มีการยอมรับว่า การระงับข้อพิพาทโดยวิธี Good Offices นั้นสามารถกระทำได้ตามกฎหมายระหว่างประเทศ ดังเช่นที่ปรากฏในอนุสัญญากรุงเฮกเพื่อการระงับข้อพิพาทระหว่างประเทศโดยสันติ ค.ศ. 1907 ซึ่งยอมรับการระงับข้อพิพาทโดยวิธี Good Offices โดยไม่ถือว่าเป็นการกระทำอันไม่เป็นมิตร[36]

วิธีการระงับข้อพิพาทที่กล่าวถึงมาทั้งหมดนี้เป็นวิธีการระงับข้อพิพาทตามกฎหมายระหว่างประเทศที่ผู้เขียนเห็นว่าสามารถใช้ในการระงับข้อพิพาทที่เกิดจากการตีความ หรือการใช้บังคับของอนุสัญญานี้ เนื่องจากเป็นวิธีการที่อยู่ในความหมายของการระงับข้อพิพาทโดยการเจรจาหารือและโดยสันติวิธีตามแนวทางปฏิบัติระหว่างประเทศ รวมไปถึงวิธีการ Good Offices ที่ถึงแม้จะเป็นวิธีทางการเมืองแต่ก็เป็นที่ยอมรับว่าสามารถกระทำได้ตามเหตุผลที่กล่าวมาข้างต้น

2.3.6 บทบัญญัติเกี่ยวกับขั้นตอนต่าง ๆของอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001

1. การลงนามและการมีผลบังคับใช้ (Article 36) การลงนามในอนุสัญญาเป็นการแสดงเจตนาในการให้ความยินยอมของรัฐเพื่อผูกพันตามอนุสัญญา ซึ่งอนุสัญญาฉบับนี้เปิดให้ประเทศสมาชิกของสภายุโรป และประเทศที่ไม่ใช่สมาชิกของสภายุโรปแต่มีส่วนร่วมดำเนินการใน

---

[35] อารีรัตน์ โกสิทธิ์, "ผลกระทบทางด้านกฎหมายต่อประเทศไทยในการเข้าเป็นภาคีอนุสัญญาว่าด้วยการห้ามพัฒนา ผลิต สะสม และใช้อาวุธเคมี และว่าด้วยการทำลายอาวุธเหล่านี้ ค.ศ. 1993", (วิทยานิพนธ์ปริญญามหาบัณฑิต สาขาวิชานิติศาสตร์ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2546), หน้า 65.

[36] Article III of the Hague Convention for the Pacific Settlement of International Dispute, อ้างถึงใน จุมพต สายสุนทร, กฎหมายระหว่างประเทศ เล่ม 2, หน้า 429.

รายละเอียดของอนุสัญญานี้ได้ลงนามเป็นภาคีของอนุสัญญา เช่น ประเทศสหรัฐอเมริกาที่อยู่ในฐานะผู้สังเกตการณ์ ผู้ร่วมเจรจาในร่างอนุสัญญา ซึ่งผู้เขียนจะได้อธิบายในบทถัดไป การลงนามในอนุสัญญาซึ่งมีผลให้อนุสัญญานั้นมีผลผูกพันและบังคับใช้ระหว่างประเทศภาคีที่ได้ลงนามจะต้องอยู่ภายใต้บังคับที่จะมีการให้สัตยาบัน การยอมรับ หรือการเห็นชอบ เหตุที่ต้องมีการกำหนดเช่นนี้เพราะหลักการทั่วไปในทางปฏิบัติระหว่างประเทศในการให้ความยินยอมของรัฐเพื่อผูกพันตามอนุสัญญาเป็นไปได้ที่รัฐบางรัฐอาจไม่ถือว่าการลงนามของผู้แทนที่ทำการลงนามในอนุสัญญาเป็นการให้ความยินยอมของรัฐเพื่อผูกพันตามอนุสัญญาจนกว่าจะได้มีการให้สัตยาบัน การยอมรับ หรือการให้ความเห็นชอบจากรัฐอีกครั้งหนึ่ง อาจเรียกได้ว่า การลงนามแบบมีเงื่อนไข (Signature ad Referendum) และในขณะเดียวกันก็อาจมีบางรัฐที่ถือว่าการลงนามของผู้แทนมีผลเท่ากับเป็นการให้ความยินยอมเพื่อผูกพันตามอนุสัญญาแล้ว ซึ่งในกรณีนี้ก็ไม่มีความจำเป็นที่จะต้องรอให้มีการให้สัตยาบัน ยอมรับหรือให้ความเห็นชอบอีกครั้งหนึ่ง[37]

แม้ว่าอนุสัญญานี้จะมิได้กำหนดหน้าที่ของประเทศภาคีที่จะไม่ทำให้วัตถุประสงค์ของอนุสัญญาเสื่อมเสียไปก่อนที่อนุสัญญาจะมีผลใช้บังคับ แต่หากเมื่อประเทศภาคีได้ลงนามแบบมีเงื่อนไขที่จะต้องมีการให้สัตยาบัน การยอมรับ หรือให้ความเห็นชอบอีกครั้งหนึ่ง ก็อาจถือได้ว่าย่อมมีพันธกรณีตามหลักการในทางระหว่างประเทศที่ต้องละเว้นการกระทำใดๆ ที่เป็นการทำให้วัตถุประสงค์หรือความมุ่งหมายของอนุสัญญานั้นเสื่อมเสียไป จนกว่ารัฐนั้นจะแสดงเจตนาชัดโดยการแจ้งว่าจะไม่เป็นภาคีอนุสัญญานี้ ซึ่งอนุสัญญานี้ได้กำหนดวิธีการบอกเลิกการเป็นภาคี (Article 47) โดยประเทศภาคีอาจบอกเลิกการเป็นภาคีของอนุสัญญาฉบับนี้ในเวลาใดก็ได้โดยแจ้งไปยังเลขาธิการสภายุโรปให้ได้รับแจ้งการบอกเลิกนั้น การบอกเลิกดังกล่าวให้มีผลภายหลังจากวันที่เลขาธิการสภายุโรปได้รับแจ้งการบอกเลิกครบสามเดือน

ดังนั้น ในขณะที่อนุสัญญายังไม่มีผลบังคับใช้ เช่น จำนวนประเทศภาคีที่ให้สัตยาบันยังไม่ครบตามจำนวนที่ระบุไว้ในเงื่อนไขของการมีผลบังคับใช้ ประเทศภาคีย่อมมีพันธกรณีที่จะต้องละเว้นการกระทำใดๆอันเป็นการทำให้วัตถุประสงค์ของอนุสัญญาเสื่อมเสียไป

ทั้งนี้ เงื่อนไขของการมีผลบังคับใช้อนุสัญญา (Article 36 (3)) ได้กำหนดไว้ว่าอนุสัญญานี้ให้มีผลบังคับใช้เมื่อมีประเทศจำนวนห้าประเทศแสดงความยินยอมที่จะผูกพันตามอนุสัญญานี้ โดยในจำนวนห้าประเทศดังกล่าวจะต้องมีประเทศสมาชิกของสภายุโรปอย่างน้อย

---

[37] เรื่องเดียวกัน, หน้า 117.

สามประเทศรวมอยู่ด้วย ซึ่งสามารถบังคับใช้ได้ภายหลังจากที่มีการแสดงความยินยอมเช่นว่านั้นครบสามเดือน

และการมีผลบังคับใช้ในประเทศที่ลงนามแสดงความยินยอมที่จะผูกพันตามอนุสัญญานี้ก็สามารถใช้บังคับภายหลังจากวันที่ประเทศภาคีได้แสดงความยินยอมครบสามเดือน ซึ่งการแสดงความยินยอมที่จะผูกพันตามอนุสัญญาฉบับนี้ต้องเป็นไปตามหลักเกณฑ์ของประเทศนั้น ทั้งนี้ เอกสารหลักฐานที่เกี่ยวข้องกับการให้สัตยาบัน การยอมรับหรือการเห็นชอบนั้นให้ยื่นต่อเลขาธิการสภายุโรป (Article 36 (4))

โดยทั่วไปแล้ว อนุสัญญาย่อมมีผลบังคับใช้แก่ประเทศภาคีภายในดินแดนทั้งหมดของประเทศภาคีซึ่งรวมถึงดินแดนของรัฐในส่วนที่เป็นทะเลอาณาเขต และห้วงอากาศ เหนือทะเลอาณาเขตตลอดทั้งพื้นดินท้องทะเล กับดินใต้ผิวดินของทะเลอาณาเขต ซึ่งเป็นเขตที่รัฐมีอำนาจอธิปไตย ยกเว้นจะมีการแสดงเจตนาไว้เป็นอย่างอื่น เช่น การกำหนดให้สนธิสัญญามีผลบังคับใช้ในดินแดนที่เป็นอาณานิคม (Colonies)[38] ดังนั้น อนุสัญญาฉบับนี้จึงได้กำหนดให้ประเทศภาคีอาจแสดงเจตจำนงต่อเลขาธิการสภายุโรป ให้อนุสัญญานี้มีผลใช้บังคับเฉพาะอาณาเขตหรือดินแดนส่วนใดส่วนหนึ่งของประเทศก็ได้ (Article 38) เจตจำนงดังกล่าวให้ยื่นในเวลาที่ได้มีการลงนามหรือยื่นเอกสารหลักฐานของการให้สัตยาบัน การยอมรับ การเห็นชอบหรือการภาคยานุวัติ และหากในเวลาหลังจากนั้นประเทศภาคีอาจขอขยายการบังคับใช้อนุสัญญาไปยังอาณาเขตหรือดินแดนส่วนอื่นๆของประเทศนั้นก็ได้ ซึ่งการมีผลบังคับใช้กับอาณาเขตดังกล่าวจะมีผลภายหลังจากครบกำหนดสามเดือนนับจากวันที่เลขาธิการสภายุโรปได้รับคำแสดงเจตจำนง

การแสดงเจตจำนงที่เกี่ยวกับอาณาเขตอาจเพิกถอนได้โดยแจ้งไปยังเลขาธิการสภายุโรป การเพิกถอนดังกล่าวให้มีผลตั้งแต่วันแรกของเดือนที่ถัดจากครบกำหนดเวลาสามเดือนหลังจากวันที่เลขาธิการได้รับแจ้งดังกล่าว (Article 38 (3))

2. การภาคยานุวัติ ในกรณีของการภาคยานุวัตินั้นแม้จะมีผลตามกฎหมายระหว่างประเทศเช่นเดียวกับการให้สัตยาบันที่ถือได้ว่าเป็นการให้ความยินยอมของรัฐเพื่อผูกพันตามอนุสัญญา แต่ก็มีความแตกต่างกันในแง่ของขั้นตอน กล่าวคือ การภาคยานุวัตินั้นจะใช้ในกรณีที่รัฐซึ่งให้ความยินยอมเพื่อผูกพันตามอนุสัญญานั้นมิได้มีส่วนเข้าร่วมในการเจรจาทำอนุสัญญามาก่อนและมิได้ลงนามในอนุสัญญามาก่อน แต่ได้มีการให้ความยินยอมเพื่อผูกพันตามอนุสัญญา

---

[38] ข้อ 4 อนุสัญญาว่าด้วยความหลากหลายทางชีวภาพ ค.ศ. 1992, อ้างถึงใน จุมพต สายสุนทร, กฎหมายระหว่างประเทศ เล่ม 2, หน้า 142.

เมื่ออนุสัญญานั้นเปิดโอกาสให้รัฐซึ่งมิได้เข้าร่วมในการเจรจาทำอนุสัญญาหรือมิได้ลงนามในอนุสัญญาสามารถให้ความยินยอมเพื่อผูกพันตามอนุสัญญาได้

ปัญหาที่เกิดขึ้นของการภาคยานุวัติในทางปฏิบัติของรัฐคือ รัฐจะสามารถเข้าภาคยานุวัติอนุสัญญาซึ่งมิได้มีส่วนร่วมในการเจรจาและลงนามมาก่อนในขณะใด ก่อนหรือหลังจากที่อนุสัญญานั้นมีผลใช้บังคับ[39] ซึ่งอนุสัญญานี้ได้ขจัดปัญหาดังกล่าวโดยกำหนดหลักเกณฑ์ในการภาคยานุวัติ (Article 37) ไว้ว่า ภายหลังจากที่อนุสัญญาฉบับนี้มีผลบังคับใช้แล้ว คณะมนตรีแห่งสภายุโรปเมื่อได้มีการปรึกษากันและได้รับความยินยอมโดยเอกฉันท์จากประเทศคู่สัญญาแล้ว อาจเชื้อเชิญประเทศใดซึ่งมิใช่ประเทศสมาชิกของสภายุโรป และมิได้มีส่วนร่วมดำเนินการในรายละเอียดของอนุสัญญาฉบับนี้ได้มีการภาคยานุวัติในอนุสัญญาฉบับนี้ การตัดสินว่าควรอนุญาตให้ประเทศอื่นเข้าเป็นภาคีนั้นต้องเป็นเสียงข้างมากของบทบัญญัติแห่งสภายุโรป และโดยมติเป็นเอกฉันท์ของผู้แทนของประเทศคู่สัญญาของอนุสัญญาฉบับนี้ ที่มีตำแหน่งในคณะมนตรีแห่งสภายุโรป

สำหรับประเทศที่มีการภาคยานุวัติแล้ว ให้อนุสัญญาฉบับนี้มีผลบังคับใช้ภายหลังจากวันที่มีการยื่นเอกสารหลักฐานการภาคยานุวัติครบสามเดือน

3. การแสดงเจตจำนงในการกำหนดองค์ประกอบความผิดเพิ่มเติม หากประเทศภาคีสมาชิกประเทศใดที่ต้องการกำหนดองค์ประกอบเพิ่มเติมเกี่ยวกับความผิดฐานเข้าถึงโดยมิชอบ (Article 2) การดักรับข้อมูลโดยมิชอบ (Article 3) การกำหนดจำนวนการครอบครองสิ่งผิดกฎหมายตามที่อนุสัญญากำหนดไว้ในความผิดฐานนำสิ่งที่ได้จากคอมพิวเตอร์ไปใช้ในทางมิชอบว่าต้องมีจำนวนเท่าใดจึงจะเป็นความผิด (Article 6 (1) (b)) การปลอมแปลงเกี่ยวกับคอมพิวเตอร์ (Article 7) การกำหนดเกณฑ์อายุเด็กที่ได้รับความคุ้มครองตามอนุสัญญาในฐานความผิดเกี่ยวกับสื่อลามกอนาจารเกี่ยวกับเด็ก (Article 9 (3)) การจัดส่งคำร้องให้มีการช่วยเหลือซึ่งกันและกันในกรณีฉุกเฉิน (Article 27 (9) (e)) อนุสัญญาได้กำหนดให้ประเทศภาคีสมาชิกดังกล่าว สามารถยื่นเป็นหนังสือแจ้งต่อเลขาธิการสภายุโรปว่าประเทศนั้นจะไปพิจารณาเองถึงความเป็นไปได้ในการกำหนดองค์ประกอบเพิ่มเติมของหลักเกณฑ์ที่กำหนด สำหรับกฎหมายภายในของประเทศ การยื่นหนังสือแสดงเจตจำนงดังกล่าวให้ยื่นในเวลาที่มีการลงนามหรือการยื่นเอกสารหลักฐานของการให้สัตยาบัน การยอมรับ การเห็นชอบ หรือการภาคยานุวัติ (Article 40)

---

[39] เรื่องเดียวกัน, หน้า 122.

4. บทบัญญัติสำหรับสหพันธรัฐ สำหรับประเทศที่เป็นสหพันธรัฐอาจสงวนสิทธิที่จะดำเนินการให้มีมาตรการที่ต้องจัดให้มีภายในประเทศ ไม่ว่าจะเป็นมาตรการในทางนิติบัญญัติหรือมาตรการอื่นที่จำเป็นในการกำหนดฐานความผิด ความรับผิดและมาตรการการลงโทษในความผิดฐานพยายาม การช่วยเหลือสนับสนุนหรือการใช้ให้กระทำความผิด ความรับผิดของนิติบุคคล มาตรการการลงโทษหรือมาตรการอื่นๆโดยให้เป็นไปตามแนวทางที่สอดคล้องกับหลักการพื้นฐานของประเทศว่าด้วยความสัมพันธ์ระหว่างรัฐบาลกลางและมลรัฐหรือหน่วยอาณาเขตอย่างอื่นในทำนองเดียวกัน ภายใต้เงื่อนไขที่ว่าประเทศที่เป็นสหพันธรัฐนั้นต้องยังคงสามารถให้ความร่วมมือระหว่างประเทศได้

เมื่อได้ทำการสงวนสิทธิดังกล่าวแล้วประเทศที่เป็นสหพันธรัฐดังกล่าวไม่อาจเอาการสงวนสิทธิมาลบล้างหรือตัดทอนหน้าที่ของประเทศในการที่จะต้องจัดมาตรการตามที่กำหนดในอนุสัญญา ประเทศดังกล่าวจะต้องมีการจัดเตรียมศักยภาพของการบังคับใช้กฎหมายอย่างกว้างขวางและมีประสิทธิผลไว้สำหรับมาตรการที่กำหนด

การบังคับใช้อนุสัญญาภายใต้เขตอำนาจของมลรัฐหรือภายใต้อาณาเขตอื่นในทำนองเดียวกันซึ่งไม่ได้มีหน้าที่ตามรัฐธรรมนูญของสหพันธรัฐที่ต้องจัดให้มีมาตรการทางนิติบัญญัติที่เกี่ยวข้องนั้น ให้รัฐบาลของสหพันธรัฐแจ้งให้หน่วยงานที่มีอำนาจหน้าที่เกี่ยวข้องของมลรัฐนั้นๆได้ทราบถึงบทบัญญัติดังกล่าวข้างต้น และสนับสนุนตามที่เห็นสมควรเพื่อให้หน่วยงานที่มีอำนาจหน้าที่เหล่านั้นได้ดำเนินการตามที่เหมาะสมเพื่อให้มีผลใช้บังคับ (Article 41)

5. การสงวนสิทธิสามารถทำได้ในเวลาที่มีการลงนามเป็นภาคีหรือยื่นเอกสารหลักฐานของการให้สัตยาบัน การยอมรับ การเห็นชอบหรือการภาคยานุวัติ ประเทศนั้นอาจแสดงเจตจำนงโดยยื่นหนังสือแจ้งไปยังเลขาธิการสภายุโรปว่าประเทศนั้นในประเด็นที่กำหนดไว้ การสงวนสิทธิอื่นนอกเหนือจากที่อนุสัญญานี้กำหนดจะกระทำไม่ได้ (Article 42)

6. สถานะและการเพิกถอนการสงวนสิทธิ ประเทศภาคีที่ได้ทำการสงวนสิทธินั้นอาจเพิกถอนการสงวนสิทธิดังกล่าวทั้งหมดหรือบางส่วนโดยแจ้งต่อเลขาธิการสภายุโรป การเพิกถอนดังกล่าวให้มีผลตั้งแต่วันที่เลขาธิการสภายุโรปได้รับแจ้ง หากในการแจ้งดังกล่าวระบุโดยเฉพาะถึงวันที่ซึ่งประสงค์จะให้การเพิกถอนมีผลนั้นและเป็นวันหลังจากวันที่เลขาธิการสภายุโรปได้รับแจ้งดังกล่าวนั้นและก็ให้การเพิกถอนดังกล่าวมีผลตั้งแต่วันที่ในการแจ้งดังที่ระบุไว้โดยเฉพาะให้มีผลนั้น

ประเทศภาคีที่ได้ทำการสงวนสิทธิสามารถเพิกถอนการสงวนสิทธิดังกล่าวทั้งหมดหรือบางส่วนโดยเร็วที่สุดเมื่อตามพฤติการณ์ปรากฏว่าไม่จำเป็นต้องสงวนสิทธิต่อไป เลขาธิการสภายุโรปอาจสอบถามเป็นระยะๆ กับประเทศภาคีที่ได้ทำการสงวนสิทธิถึงโอกาสความเป็นไปได้ที่จะเพิกถอนคำสงวนสิทธิข้อใดข้อหนึ่งหรือหลายข้อนั้น (Article 43)

7. การแก้ไขเพิ่มเติม อนุสัญญาได้กำหนดหลักการทั่วไปเกี่ยวกับการแก้ไขเพิ่มเติมอนุสัญญา ไว้ว่า อนุสัญญานั้นอาจแก้ไขได้หากประเทศภาคีประเทศใดประเทศหนึ่งเสนอให้มีการแก้ไขเพิ่มเติม โดยเสนอไปยังเลขาธิการสภายุโรปเพื่อให้เลขาธิการสภายุโรปแจ้งไปยังประเทศสมาชิกของสภายุโรป และประเทศที่ไม่ใช่สมาชิกของสภายุโรปแต่ได้มีส่วนร่วมในการจัดทำรายละเอียดของอนุสัญญาฉบับนี้ ตลอดจนประเทศอื่นๆ ที่ภาคยานุวัติหรือได้รับการเชื้อเชิญให้ภาคยานุวัติ

การเสนอเรื่องแก้ไขเพิ่มเติมโดยประเทศภาคีนั้น อนุสัญญาได้กำหนดให้มีการแจ้งไปยังคณะกรรมาธิการของสภายุโรปว่าด้วยปัญหาอาชญากรรม ซึ่งจะทำการส่งต่อไปให้คณะมนตรี (Committee of Ministers) พร้อมเสนอความเห็นที่มีต่อการแก้ไขเพิ่มเติมดังกล่าว คณะมนตรีจึงจะทำการพิจารณาถึงข้อเสนอให้มีการแก้ไขเพิ่มเติมและความเห็นดังกล่าว และหลังจากที่ได้มีการพิจารณาและปรึกษาหารือกับประเทศภาคีที่ไม่ใช่สมาชิกของสภายุโรปแล้ว คณะมนตรีอาจรับรองให้มีการแก้ไขเพิ่มเติมอนุสัญญาฉบับนี้ เนื้อความของการแก้ไขเพิ่มเติมที่มีการรับรองโดยคณะมนตรีต้องส่งต่อไปยังประเทศภาคีเพื่อให้การยอมรับ

การแก้ไขเพิ่มเติมที่มีการรับรองแล้วให้มีผลใช้บังคับตั้งแต่ครบกำหนดสามสิบวันนับตั้งแต่ประเทศภาคีทั้งหมดได้แจ้งการยอมรับการแก้ไขเพิ่มเติมดังกล่าวต่อเลขาธิการสภายุโรปแล้ว (Article 44)

8. การปรึกษาหารือกันของประเทศภาคี อนุสัญญานี้ได้กำหนดให้ประเทศภาคีปรึกษาหารือกันเป็นระยะๆตามสมควรเกี่ยวกับการใช้บังคับและการปฏิบัติอย่างมีประสิทธิภาพ รวมถึงการชี้แจงปัญหาที่เกี่ยวข้อง ตลอดจนผลกระทบของการแสดงเจตจำนงหรือการสงวนสิทธิที่ให้ไว้ภายใต้อนุสัญญาฉบับนี้ การแลกเปลี่ยนข้อมูลเกี่ยวกับการพัฒนาทางกฎหมาย นโยบายและเทคโนโลยีที่สำคัญซึ่งเกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์และการรวบรวมพยานหลักฐานในรูปของอิเล็กทรอนิกส์ การพิจารณาถึงการเสริมหรือการแก้ไขเพิ่มเติมในสิ่งที่เป็นไปได้ ซึ่งการหารือดังกล่าวต้องแจ้งคณะกรรมาธิการของสภายุโรปว่าด้วยปัญหาอาชญากรรมเป็นระยะๆ เกี่ยวกับผลการปรึกษาหารือกันดังกล่าว

ในกรณีที่สมควรคณะกรรมธิการของสภายุโรป พึงสนับสนุนการปรึกษาหารือกัน และพึงจัดให้มีมาตรการที่จำเป็นเพื่อช่วยเหลือประเทศภาคีในความพยายามที่จะเสริมหรือแก้ไขเพิ่มเติมอนุสัญญาฉบับนี้ ในเวลาสามปีหลังจากอนุสัญญาฉบับนี้มีผลใช้บังคับให้คณะกรรมาธิการของสภายุโรปว่าด้วยปัญหาอาชญากรรมโดยร่วมมือกับประเทศภาคีจัดให้มีการทบทวนบทบัญญัติทั้งหมดของอนุสัญญาฉบับนี้ และหากมีความจำเป็นอาจแนะนำเกี่ยวกับการแก้ไขเพิ่มเติมที่เหมาะสมนั้น

นอกจากส่วนที่รับภาระโดยสภายุโรปแล้ว ค่าใช้จ่ายที่เกิดขึ้นในการจัดการปรึกษาหารือกันให้อยู่ในความรับผิดชอบของประเทศภาคีตามที่จะพิจารณาตกลงกัน ประเทศภาคีพึงได้รับความช่วยเหลือจากเลขาธิการสภายุโรปในการจัดการตามหน้าที่ดังกล่าว (Article 46)

9. การแจ้งความ เลขาธิการสภายุโรปมีหน้าที่แจ้งไปยังประเทศสมาชิกของสภายุโรปและประเทศที่ไม่ใช่สมาชิกของสภายุโรปแต่ได้มีส่วนร่วมในการจัดทำรายละเอียดของอนุสัญญาฉบับนี้ตลอดจนประเทศที่ภาคยานุวัติหรือได้รับการเชื้อเชิญให้ภาคยานุวัติในอนุสัญญาฉบับนี้ ในเรื่องการลงนามใดๆ การยื่นเอกสารหลักฐานของการให้สัตยาบัน การยอมรับ การเห็นชอบหรือการภาคยานุวัติในอนุสัญญาฉบับนี้และวันที่มีผลใช้บังคับของอนุสัญญา

การแสดงเจตจำนงใดหรือการสงวนสิทธิ การดำเนินการอื่นใด การแจ้งความหรือการติดต่อสื่อสารที่เกี่ยวข้องกับอนุสัญญาฉบับนี้ ให้ผู้ที่ได้รับมอบหมายโดยชอบลงนามเพื่อเป็นพยาน (Article 48)

จะเห็นได้ว่าอนุสัญญาดังกล่าวนี้ไม่ได้มีการกำหนดบทลงโทษสำหรับประเทศภาคีซึ่งแตกต่างจากอนุสัญญาระหว่างประเทศฉบับอื่นๆที่มีการกำหนดมาตรการการลงโทษ เช่น กฎบัตรสหประชาชาติที่ได้กำหนดบทลงโทษสำหรับประเทศภาคีสมาชิกที่ไม่ปฏิบัติตามพันธกรณีในสถานการณ์ที่ละเมิดต่อสันติภาพและความมั่นคงระหว่างประเทศ โดยใช้มาตรการร่วมกันในการลงโทษรัฐสมาชิกในรูปแบบของการแทรกแซงโดยไม่มีการใช้กำลัง ไม่ใช้อาวุธ มาตรการเหล่านี้อาจรวมถึงการตัดความสัมพันธ์ทางเศรษฐกิจ การคมนาคมทางรถไฟ ทางทะเล ทางอากาศ ทางไปรษณีย์ ทางโทรเลข ทางวิทยุ และวิถีทางคมนาคมอย่างอื่นโดยสิ้นเชิงหรือแต่บางส่วน รวมถึงการตัดสัมพันธ์ทางการทูตและทางการเงิน ทั้งนี้ การใช้มาตรการลงโทษอาจใช้ในกรณีที่ไม่ได้มีการละเมิดกฎหมายระหว่างประเทศก็ได้ ถ้าหากว่าเป็นการจำเป็นเพื่อรักษาไว้ซึ่งสันติภาพและความมั่นคงของประเทศ ซึ่งการใช้มาตรการต่างๆเหล่านี้ต้องกระทำการอย่างเหมาะสมเพื่อแก้ไขปรับปรุงความสัมพันธ์ระหว่างประเทศหรือการละเมิดสิทธิมนุษยชน

จากการที่ศึกษาบทบัญญัติอนุสัญญาที่ผ่านมานั้น ผู้เขียนจึงสรุปสาระสำคัญและความเห็นเกี่ยวกับมาตรการต่างๆ ของอนุสัญญา ดังนี้

1. การให้ประเทศภาคีกำหนดการกระทำความผิดอาชญากรรมทางคอมพิวเตอร์ทั้ง 9 ฐาน เป็นความผิดทางอาญาตามกฎหมายภายในประเทศ และมีการกำหนดโทษให้ได้สัดส่วนเหมาะสมกับการกระทำความผิดและความเสียหายที่เกิดขึ้น ผู้เขียนเห็นว่ามาตรการในข้อนี้ถือเป็นสิ่งสำคัญของการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ซึ่งประเทศภาคีจะต้องดำเนินการโดยเร่งด่วน ถึงแม้ประเทศภาคีนั้นจะแสดงเจตนารมณ์เพียงแค่การลงนามในอนุสัญญา แต่อย่างไรก็ตามพันธกรณีที่เกิดขึ้นกับประเทศภาคีเหล่านั้นคือการกระทำที่ไม่เป็นอุปสรรคต่อการปฏิบัติตามวัตถุประสงค์ของอนุสัญญาให้สำเร็จและมีประสิทธิผล ทั้งนี้เนื่องจากว่า หากกฎหมายภายในประเทศภาคีใดไม่ได้บัญญัติให้อาชญากรรมทางคอมพิวเตอร์เป็นความผิดทางอาญาแล้ว ก็ไม่อาจลงโทษผู้กระทำความผิดได้

นอกจากนี้หากประเทศภาคีได้บัญญัติให้การกระทำความผิดอาชญากรรมทางคอมพิวเตอร์เป็นกฎหมายภายในประเทศที่มีทิศทางสอดคล้องกันแล้วจะส่งผลให้การดำเนินคดีกับผู้กระทำความผิดเป็นไปได้อย่างรวดเร็วและมีประสิทธิภาพ และสามารถแก้ไขข้อขัดข้องเกี่ยวกับหลักเกณฑ์ของมาตรการความร่วมมือระหว่างประเทศ เช่น กรณีที่การกระทำความผิดดังกล่าวมีส่วนเกี่ยวข้องกับเขตอำนาจศาลหลายประเทศ การให้ความร่วมมือระหว่างประเทศ การส่งผู้ร้ายข้ามแดน และการช่วยเหลือซึ่งกันและกันนั้น ประเทศโดยส่วนใหญ่ต่างทำความตกลงระหว่างประเทศในรูปแบบของความตกลงทวิภาคีซึ่งมีหลักเกณฑ์โดยทั่วไปที่ก่อให้เกิดข้อขัดข้องไม่สามารถนำตัวผู้กระทำความผิดมาลงโทษได้ ไม่ว่าจะเป็นการกำหนดฐานความผิด การกำหนดบทลงโทษแตกต่าง เป็นต้น

ในส่วนของการกำหนดบทลงโทษแก่ผู้กระทำความผิดแม้ว่าจะมิใช่บทบังคับให้ประเทศภาคีต้อกำหนดโทษสถานใดแก่ผู้ระทำความผิด ดังนั้นจึงอยู่ในดุลพินิจของแต่ละประเทศภาคีที่จะกำหนดกรอบหรือระดับการลงโทษให้มีความเหมาะสมกับสภาพของการกระทำความผิด ความรุนแรงของการกระทำความผิด ความเสียหายที่เกิดขึ้นจากการกระทำความผิด รวมถึงแรงจูงใจในการกระทำความผิด ซึ่งในการที่ประเทศภาคีจะกำหนดโทษผู้เขียนเห็นว่าข้อพิจารณาที่สำคัญคือจะต้องคำนึงถึงหลักสิทธิมนุษยชนด้วย กล่าวคือ จะต้องได้สัดส่วนที่เหมาะสมเพื่อให้มีผลในการยังยั้งการกระทำความผิด เช่น โทษจำคุก โทษปรับ หรือการควบคุมให้ผู้กระทำความผิดอยู่ในความดูแลของเจ้าหน้าที่รัฐ และไม่สามารถออกไปกระทำความผิดได้ และยังสามารถให้ความรู้ความเข้าใจที่ถูกต้องต่อผู้กระทำความผิด ซึ่งส่วนใหญ่เป็นผู้มีความรู้ความสามารถ การ

สร้างความเข้าใจดังกล่าวอาจถือได้ว่าเป็นการสร้างทัศนคติที่ถูกต้องและไม่กระทำความผิดดังที่เคยทำมาแล้ว ทั้งนี้ ประเทศภาคีไม่ควรกำหนดบทลงโทษโดยวิธีการประหารชีวิต เพราะถือว่าเป็นการกระทำที่รุนแรงไม่คำนึงถึงหลักสิทธิมนุษยชน และอาจส่งผลให้เกิดปัญหาในการส่งผู้ร้ายข้ามแดนได้

2. การกำหนดให้ประเทศภาคีต้องมีมาตรการในการสืบสวนสอบสวนเพื่อให้สามารถนำตัวผู้กระทำความผิดเข้าสู่กระบวนการยุติธรรมและลงโทษได้ การนำตัวผู้กระทำความผิดมาลงโทษ จะต้องมีการกำหนดขั้นตอน และวิธีปฏิบัติที่แน่นอน รวดเร็วและมีประสิทธิภาพเท่าทันกับการกระทำความผิดในรูปแบบนี้ ซึ่งการให้ประเทศภาคีต้องมีวิธีการสืบสวนสอบสวนเพิ่มเติมจากวิธีการเดิม ไม่ว่าจะเป็น การเข้าเก็บรักษาข้อมูลคอมพิวเตอร์หรือการออกคำสั่งให้หน่วยงานใดหน่วยงานหนึ่งที่ทำหน้าที่เก็บรักษาข้อมูลคอมพิวเตอร์ส่งข้อมูลดังกล่าวให้หน่วยงานที่มีหน้าที่สืบสวนสอบสวน การค้นและยึดข้อมูลทางคอมพิวเตอร์ การรวบรวมเนื้อหาของข้อมูลจราจรทางคอมพิวเตอร์ หรือแม้กระทั่งการดักรับข้อมูลที่เป็นเนื้อหา ถึงแม้จะดูเหมือนว่ามาตรการดังกล่าวอาจส่งผลให้เกิดการละเมิดสิทธิส่วนบุคคลแต่การกำหนดมาตรการอนุสัญญาได้บัญญัติให้ประเทศภาคีต้องคำนึงถึงหลักการคุ้มครองสิทธิส่วนบุคคลและเสรีภาพขั้นพื้นฐานไว้แล้ว

ดังนั้น มาตรการดังกล่าวที่ประเทศภาคีกำหนดขึ้นจะต้องสร้างความเชื่อมั่นแก่เจ้าของข้อมูลคอมพิวเตอร์ดังกล่าวว่าจะได้รับความเป็นธรรมที่เหมาะสมกับคุ้มครองสิทธิส่วนบุคคลและเสรีภาพขั้นพื้นฐานดังกล่าวด้วย ทั้งนี้ นอกเหนือจากการเรียกร้องให้ประเทศภาคีดำเนินการร่วมกันในการนำตัวผู้กระทำความผิดมาลงโทษแล้ว ยังมีการเน้นย้ำถึงการนำตัวผู้มีส่วนร่วมและผู้สนับสนุนการกระทำความผิดเข้าสู่กระบวนการยุติธรรมอีกด้วย ซึ่งแสดงให้เห็นอย่างเด่นชัดว่าอนุสัญญาให้ความสำคัญกับการนำตัวผู้กระทำความผิดมาลงโทษอย่างมาก โดยการกำหนดให้บุคคลผู้มีส่วนเกี่ยวข้อง ไม่ว่าจะเป็นนิติบุคคลหรือผู้มีส่วนร่วมในการกระทำความผิดทุกขั้นตอนต้องถูกดำเนินคดี โดยไม่ว่าความผิดดังกล่าวจะเป็นความผิดสำเร็จหรือไม่ก็ตาม

3. การให้ประเทศภาคีกำหนดมาตรการความร่วมมือระหว่างประเทศ ซึ่งผู้เขียนเห็นว่าเป็นประเด็นที่มีความสำคัญมากที่สุด เพราะจะเป็นมาตรการที่เน้นในทางปฏิบัติและช่วยให้สามารถป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ได้เป็นอย่างดี เนื่องจากอาชญากรรมที่มีการแพร่ขยายอย่างรวดเร็วและสามารถกระทำความผิดได้ทั่วทุกมุมโลกทำให้ยากต่อการจับกุม จึงอาจถือได้ว่าอาชญากรรมทางคอมพิวเตอร์ก็อาจถือเป็นปัญหาระหว่างประเทศที่ประเทศภาคีต่างควรตระหนักถึงและให้ความสำคัญ ทั้งนี้ เพราะความเสียหายที่เกิดขึ้นหากเป็นความเสียหายที่ร้ายแรงกระทบต่อสาธารณูปโภคขั้นพื้นฐาน หรือข้อมูลขององค์กรที่มีความสำคัญ

ระดับชาติ ความเสียหายที่เกิดขึ้นจึงยากที่จะประเมินค่าได้ ในการดำเนินการเกี่ยวกับปัญหาดังกล่าวจึงต้องอาศัยความร่วมมือระหว่างประเทศในการกำหนดกรอบการดำเนินการให้ประเทศภาคีนำไปปฏิบัติ และจำเป็นอย่างยิ่งที่ประเทศภาคีแต่ละประเทศจะต้องจัดให้มีมาตรการภายในที่ดีมีความรวดเร็ว เหมาะสม และมีประสิทธิภาพที่เพียงพอต่อการจัดการกับอาชญากรรมทางคอมพิวเตอร์ได้ รวมถึง การกำหนดให้มีองค์กรหรือหน่วยงานที่มีความรู้ความสามารถเพื่อทำหน้าที่เป็นศูนย์กลางในการประสานงาน การแลกเปลี่ยนข้อมูลข่าวสาร รวมถึงการติดต่อสื่อสารในการให้คามร่วมมือระหว่างกัน ไม่ว่าจะเป็นการส่งผู้ร้ายข้ามแดน การช่วยเหลือซึ่งกันและกันจะช่วยให้ความร่วมมือดังกล่าวเกิดเป็นรูปธรรมมากยิ่งขึ้นและสามารถดำเนินคดีกับผู้กระทำความผิดได้

ในการดำเนินการนำตัวผู้กระทำความผิดมาลงโทษ เป็นปัญหาที่มีความสำคัญเนื่องจากการกระทำความผิดในรูปแบบนี้มีเทคโนโลยีที่ทันสมัยเข้ามาเกี่ยวข้อง ทำให้ยากต่อการจับกุมและนำตัวผู้กระทำความผิดมาลงโทษ หากไม่ได้รับความร่วมมือระหว่างประเทศที่เกี่ยวข้อง ซึ่งในประเด็นนี้ผู้เขียนเห็นว่าเป็นข้อจำกัดอย่างหนึ่งของอนุสัญญาที่สามารถใช้บังคับได้เฉพาะประเทศเท่านั้น อนุสัญญาได้เน้นย้ำถึงความสำคัญดังกล่าวโดยบัญญัติให้มีวิธีดำเนินการเกี่ยวกับการส่งตัวผู้กระทำความผิดมาลงโทษในฐานะผู้ร้ายข้ามแดนให้ประเทศภาคีสามารถปฏิบัติต่อกันได้รวดเร็วขึ้น โดยมีการผ่อนคลายหลักเรื่องความผิดอาญาของทั้งสองประเทศ ซึ่งทำให้สามารถดำเนินการได้อย่างมีประสิทธิภาพมากขึ้น

4. การกำหนดให้มีการจัดตั้งองค์กรที่มีเครือข่ายตลอด 24 ชั่วโมง และตลอด 7 วัน เพื่ออำนวยความสะดวกให้แก่การดำเนินการตามมาตรการต่างๆ ที่กำหนดขึ้นได้อย่างรวดเร็วเพื่อให้สามารถช่วยเหลือได้ทันท่วงทีไม่ว่าจะเป็นการรวบรวมพยานหลักฐานที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ การสืบหาข้อมูลผู้ต้องสงสัย การให้ข้อมูลทางกฎหมาย รวมถึงการให้คำปรึกษาด้วย โดยองค์กรดังกล่าวจะต้องมีบุคลากรที่มีความรู้และมีจำนวนเพียงพอสำหรับการปฏิบัติงานซึ่งการแลกเปลี่ยนข้อมูล การติดต่อสื่อสารระหว่างกันดังกล่าว ถือเป็นมาตรการให้ความร่วมมือที่มีความจำเป็นอย่างมาก และเป็นประเด็นที่สำคัญอย่างยิ่งที่ประเทศสมาชิกควรให้ความสำคัญรวมถึงทำให้เกิดเป็นรูปธรรมมากที่สุด เนื่องจากว่าการแลกเปลี่ยนข้อมูลข่าวสารระหว่างกัน จะทำให้ประเทศภาคีแต่ละประเทศทราบถึงวิวัฒนาการของการก่อการร้ายว่าได้ดำเนินไปในทิศทางใดเพื่อให้ประเทศภาคีอื่นๆ สามารถเตรียมการป้องกันทั้งในทางนโยบาย กฎหมาย และทางเทคนิคและทำให้สามารถรับมือกับรูปแบบใหม่ๆ ในการกระทำความผิดที่เกิดขึ้นได้

จากข้อสรุปดังกล่าวสามารถทำให้เห็นได้ว่า อนุสัญญาดังกล่าวนี้มีความสำคัญเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ในระดับสากล หรือที่มีลักษณะข้ามประเทศ โดยประเทศภาคีสามารถอาศัยความร่วมมือระหว่างกันเกี่ยวกับมาตรการต่างๆที่กำหนดไว้ในอนุสัญญาเพื่อช่วยให้สามารถป้องกันและปราบปรามอาชญากรรมรูปแบบใหม่นี้ได้มีประสิทธิภาพมากขึ้น

ทั้งนี้ จากมาตรการของอนุสัญญาที่มีการกำหนดให้มีองค์กรหรือหน่วยงานที่มีความรู้ความสามารถเพื่อทำหน้าที่เป็นศูนย์กลางในการประสานงาน การแลกเปลี่ยนข้อมูลข่าวสาร รวมถึงการติดต่อสื่อสารในการให้ความร่วมมือระหว่างกัน ไม่ว่าจะเป็นการส่งผู้ร้ายข้ามแดน การช่วยเหลือซึ่งกันและกัน รวมถึงการจัดตั้งองค์กรที่มีเครือข่ายตลอด 24 ชั่วโมง และตลอด 7 วัน เพื่ออำนวยความสะดวกให้แก่การดำเนินการตามมาตรการต่างๆ นั้น เพื่อให้เห็นภาพได้ชัดเจนยิ่งขึ้นว่าประเทศภาคีแต่ละประเทศทั้งที่มีการลงนามและให้สัตยาบัน และลงนามแต่มิได้มีการให้สัตยาบันมีการปฏิบัติตามพันธกรณีอนุสัญญาเกี่ยวกับการจัดตั้งองค์กรที่ทำหน้าที่ดังกล่าวหรือไม่ ตามตารางดังต่อไปนี้

ตารางที่ 1 รายชื่อประเทศภาคีและหน่วยงานที่มีอำนาจหน้าที่ตามอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001[55]

กลุ่มประเทศสมาชิกสภายุโรป (Member States of the Council of Europe)

ประเทศ	ลงนาม	ให้สัตยาบัน	มีผลบังคับใช้	R.	D.	A.	T.	C.	O.	หน่วยงานกลางให้ความช่วยเหลือซึ่งกันและกัน (Article 27)[56]	หน่วยงานที่รับผิดชอบการส่งผู้ร้ายข้ามแดน (Article 24)[57]	องค์กร 24/7 (Article 35)[58]
แอลแบเนีย	23/11/2001	20/6/2002	1/7/2004	-	-	X	-	-	-	Ministry of Justice, Bulevardi Zog. I., Tirana	Ministry of Justice, Bulevardi Zog. I., Tirana National Central Office of Interpol, Bulevardi Deshmoret e	Police of State Ministry of Interior Bulevardi Deshmoret e Kombit Tirana Albania

[55] Council of Europe,Chart of signatures and ratifications[Online]. 2009. Available from: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG[2009, December 5]

[56] Alexander Seger. Resources : Competent Authorities and Points of Contact for International Cooperation[Online]. Council of Europe. Available from : http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Internationalcooperation/Res_internatcoop_authorities_en.asp[2010, January 11]

[57] Ibid.,

[58] Ibid.,

ประเทศ	ลงนาม	ให้สัตยาบัน	มีผลบังคับใช้	R.	D.	A.	T.	C.	O.	หน่วยงานกลางให้ความช่วยเหลือซึ่งกันและกัน (Article 27)	หน่วยงานที่รับผิดชอบการส่งผู้ร้ายข้ามแดน (Article 24)	องค์กร 24/7 (Article 35)
(ต่อ) แอลแบเนีย											Kombit, Tirana	
อัลดอร์รา	-	-	-	-	-	-	-	-	-	-	-	-
อาร์เมเนีย	23/11/2001	12/10/2006	1/2/2007	-	-	X	-	-	-	Main Department on Combat Against Organized Crime of the Police of the Republic of Armenia	Main Department on Combat Against Organized Crime of the Police of the Republic of Armenia	Main Department on Combat Against Organized Crime of the Police of the Republic of Armenia
ออสเตรีย	23/11/2001	-	-	-	-	-	-	-	-	-	-	-
อาเซอร์ไบจาน	30/6/2008	-	-	X	X	X	X	-	-	Ministry of National Security	Ministry of Justice	Ministry of National Security
เบลเยี่ยม	23/11/2001	-	-	-	-	-	-	-	-	-	-	-

ประเทศ	ลงนาม	ให้สัตยาบัน	มีผลบังคับใช้	R.	D.	A.	T.	C.	O.	หน่วยงานกลางให้ความช่วยเหลือซึ่งกันและกัน (Article 27)	หน่วยงานที่รับผิดชอบการส่งผู้ร้ายข้ามแดน (Article 24)	องค์กร 24/7 (Article 35)
บอสเนียและเฮอร์เซ-โกวินา	9/2/2005	19/5/2006	1/9/2006	-	-	X	-	-	-	State Investigation and Protection Agency of Bosnia and Herzegovina. Director of the Sarajevo Regional Office	State Investigation and Protection Agency of Bosnia and Herzegovina. Director of the Sarajevo Regional Office	State Investigation and Protection Agency of Bosnia and Herzegovina. Director of the Sarajevo Regional Office
บัลแกเรีย	23/11/2001	7/4/2005	1/8/2005	X	X	X	-	-	-	Ministry of Justice (trial stage), Supreme Cassation Prosecutor's Office (pre-trial stage)	Ministry of Justice (extradition), Supreme Cassation Prosecutor's Office (provisional arrests)	National Service for Combating Organized Crime under the Ministry of Interior

ประเทศ	ลงนาม	ให้สัตยาบัน	มีผลบังคับใช้	R.	D.	A.	T.	C.	O.	หน่วยงานกลางให้ความช่วยเหลือซึ่งกันและกัน (Article 27)	หน่วยงานที่รับผิดชอบการส่งผู้ร้ายข้ามแดน (Article 24)	องค์กร 24/7 (Article 35)
โครเอเชีย	23/11/2001	17/10/2002	1/7/2004	-	-	X	-	-	-	Ministry of Justice, Dezmanova 6, 10 000 Zagreb	Ministry of Justice, Dezmanova 6, 10 000 Zagreb	Ministry of Interior, Police - Directorate for crime police, Ilica 335, 10 000 Zagreb
ไซปรัส	23/11/2001	19/1/2005	1/5/2005	-	-	X	-	-	-	Ministry of Justice and Public Order Athalassas Av. 125 1461 NICOSIA	Ministry of Justice and Public Order Athalassas Av. 125 1461 NICOSIA	Ministry of Justice and Public Order Athalassas Av. 125 1461 NICOSIA
สาธารณรัฐ-เช็ก	9/2/2005	-	-	-	-	-	-	-	-	-	-	-
เดนมาร์ก	22/4/2003	21/6/2005	1/10/2005	X		X	X			Ministry of Justice, Slotsholmsgade	Ministry of Justice,	Danish National Police, Police

ประเทศ	ลงนาม	ให้สัตยาบัน	มีผลบังคับใช้	R.	D.	A.	T.	C.	O.	หน่วยงานกลางให้ความช่วยเหลือซึ่งกันและกัน (Article 27)	หน่วยงานที่รับผิดชอบการส่งผู้ร้ายข้ามแดน (Article 24)	องค์กร 24/7 (Article 35)
(ต่อ) เดนมาร์ก										10, DK-1216 Copenhagen K, Denmark	Slotsholmsgade 10, DK-1216 Copenhagen K, Denmark	Department, Polititorvet 14, DK-1780 Copenhagen V, Denmark
เอสโตเนีย	23/11/2001	12/5/2003	1/7/2004	-	-	X	-	-	-	Ministry of Justice	Ministry of Justice	Estonian Central Criminal Police
ฟินแลนด์	23/11/2001	24/5/2007	1/9/2007	X	X	X	-	-	-	Ministry of Justice, Eteläesplanadi 10, FIN-00130 Helsinki	For requests for extradition, the Ministry of Justice, Eteläesplanadi 10, FIN-00130 Helsinki For requests for provisional arrest,	National Bureau of Investigation, Criminal Intelligence Division / Communications Centre

ประเทศ	ลงนาม	ให้สัตยาบัน	มีผลบังคับใช้	R.	D.	A.	T.	C.	O.	หน่วยงานกลางให้ความช่วยเหลือซึ่งกันและกัน (Article 27)	หน่วยงานที่รับผิดชอบการส่งผู้ร้ายข้ามแดน (Article 24)	องค์กร 24/7 (Article 35)
(ต่อ) ฟินแลนด์											the National Bureau of Investigation, Jokiniemenkuja 4, FIN-01370 Vantaa	
ฝรั่งเศส	23/11/2001	10/1/2006	1/5/2006	X	X	X	-	-	-	From French judicial authorities directed to foreign judicial authorities transmitted through the Ministry of Justice (Ministère de la Justice, 13, Place Vendôme, 75042	Ministry for Foreign Affairs for extradition (Ministère des Affaires étrangères, 37, Quai d'Orsay, 75700 Paris 07 SP); The territorially competent State	Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication" (11, Rue des Saussaies, 75800 Paris)

ประเทศ	ลงนาม	ให้สัตยาบัน	มีผลบังคับใช้	R.	D.	A.	T.	C.	O.	หน่วยงานกลางให้ความช่วยเหลือซึ่งกันและกัน (Article 27)	หน่วยงานที่รับผิดชอบการส่งผู้ร้ายข้ามแดน (Article 24)	องค์กร 24/7 (Article 35)
(ต่อ) ฝรั่งเศส										Paris Cedex 01) From foreign judicial authorities directed to French judicial authorities are transmitted through diplomatic channels (Ministère des Affaires étrangères, 37, Quai d'Orsay, 75700 Paris 07 SP)	Prosecutor for requests for provisional arrest	
จอร์เจีย	1/4/2008	-	-	-	-	-	-	-	-	-	-	-

ประเทศ	ลงนาม	ให้สัตยาบัน	มีผลบังคับใช้	R.	D.	A.	T.	C.	O.	หน่วยงานกลางให้ความช่วยเหลือซึ่งกันและกัน (Article 27)	หน่วยงานที่รับผิดชอบการส่งผู้ร้ายข้ามแดน (Article 24)	องค์กร 24/7 (Article 35)
เยอรมัน	23/11/2001	9/3/2009	1/7/2009	X	X	X				Ministry of Foreign Affairs (address: Auswärtiges Amt, Werderscher Markt 1, 10117 Berlin).	Ministry of Foreign Affairs (address: Auswärtiges Amt, Werderscher Markt 1, 10117 Berlin).	National High Tech Crime Unit at the Federal Criminal Police Office 65193 Wiesbaden
กรีซ	23/11/2001	-	-	-	-	-	-	-	-	-	-	-
ฮังการี	23/11/2001	4/12/2003	1/7/2004	X	X	X	-	-	-	Before starting the criminal procedure: the Hungarian National Police International Implementing Co-	Ministry of Justice for extradition or provisional arrest. The National Central Bureau of Interpol for provisional arrest.	Hungarian National Police International Implementing Co-operation Centre

ประเทศ	ลงนาม	ให้สัตยาบัน	มีผลบังคับใช้	R.	D.	A.	T.	C.	O.	หน่วยงานกลางให้ความช่วยเหลือซึ่งกันและกัน (Article 27)	หน่วยงานที่รับผิดชอบการส่งผู้ร้ายข้ามแดน (Article 24)	องค์กร 24/7 (Article 35)
(ต่อ) ฮังการี											operation Centre Budapest, Teve u. 4-6 1139 – Hungary After starting the criminal procedure: the General Prosecutor's Office of the Republic of Hungary Budapest, Markó u. 4-6 1055 - Hungary	

ประเทศ	ลงนาม	ให้สัตยาบัน	มีผลบังคับใช้	R.	D.	A.	T.	C.	O.	หน่วยงานกลางให้ความช่วยเหลือซึ่งกันและกัน (Article 27)	หน่วยงานที่รับผิดชอบการส่งผู้ร้ายข้ามแดน (Article 24)	องค์กร 24/7 (Article 35)
ไอซ์แลนด์	30/11/2001	29/1/2007	1/5/2007	X	-	X	-	-	-	Ministry of Justice, Skuggasundi, 150 Reykjavík, Iceland	Ministry of Justice, Skuggasundi, 150 Reykjavík, Iceland	National Commissioner of the Icelandic Police (Ríkislögreglustjórinn), Skúlagata 21, 101 Reykjavík, Iceland
ไอร์แลนด์	28/2/2002	-	-	-	-	-	-	-	-	-	-	-
อิตาลี	23/11/2001	5/6/2008	1/10/2008	-	-	X	-	-	-	Ministry of Justice Department for Affairs of Justice Directorate General of Criminal Justice Office II	Ministry of Justice Department for Affairs of Justice Directorate General of Criminal Justice Office II	District Attorney Roma

ประเทศ	ลงนาม	ให้สัตยาบัน	มีผลบังคับใช้	R.	D.	A.	T.	C.	O.	หน่วยงานกลางให้ความช่วยเหลือซึ่งกันและกัน (Article 27)	หน่วยงานที่รับผิดชอบการส่งผู้ร้ายข้ามแดน (Article 24)	องค์กร 24/7 (Article 35)
(ต่อ) อิตาลี										(International Judicial Cooperation) Viale Arenula 70 I - 00186 ROMA	(International Judicial Cooperation) Viale Arenula 70 I - 00186 ROMA	
ลัตเวีย	5/5/2004	14/2/2007	1/6/2007	X	-	X	-	-	-	Ministry of Justice Brivibas Blvd. 36, Riga LV-1536, Latvia	Prosecutor General Office Kalpaka Blvd. 6, Riga LV-1801, Latvia	International Cooperation Department of Central Criminal Police Department of State Police Brivibas Str. 61, Riga LV-1010, Latvia

ประเทศ	ลงนาม	ให้สัตยาบัน	มีผลบังคับใช้	R.	D.	A.	T.	C.	O.	หน่วยงานกลางให้ความช่วยเหลือซึ่งกันและกัน (Article 27)	หน่วยงานที่รับผิดชอบการส่งผู้ร้ายข้ามแดน (Article 24)	องค์กร 24/7 (Article 35)
ลิกเตน-สไตน์	17/11/2008		-	-	-	-	-	-	-	-	-	-
ลิทัวเนีย	23/6/2003	18/3/2004	1/7/2004	X	X	X				Ministry of Justice and the General Prosecutor's Office of the Republic of Lithuania	Ministry of Justice and the General Prosecutor's Office of the Republic of Lithuania	Police Department under the Ministry of the Interior of the Republic of Lithuania
ลักแซม-เบิร์ก	28/1/2003	-	-	-	-	-	-	-	-	-	-	-
มอลตา	17/1/2002	-	-	-	-	-	-	-	-	-	-	-

ประเทศ	ลงนาม	ให้สัตยาบัน	มีผลบังคับใช้	R.	D.	A.	T.	C.	O.	หน่วยงานกลางให้ความช่วยเหลือซึ่งกันและกัน (Article 27)	หน่วยงานที่รับผิดชอบการส่งผู้ร้ายข้ามแดน (Article 24)	องค์กร 24/7 (Article 35)
มอลโดวา	23/11/2001	12/5/2009	1/9/2009	-	X	X	X	-	-	Office of the Prosecutor General in the phase of penal prosecution: 26, Banulescu - Bodoni str., MD-2012 Chisinau, Republic of Moldova. Ministry of Justice in the judiciary phase or the execution of	Office of the Prosecutor General in the phase of penal prosecution: 26, Banulescu - Bodoni str., MD-2012 Chisinau, Republic of Moldova. Ministry of Justice in the judiciary phase or the execution of	Direction of Prevention and Combating of Cybernetic, Information and Transnational Offences of the Ministry of Internal Affairs: 14, Bucuriei str., MD-2004 Chisinau, Republic of Moldova.

ประเทศ	ลงนาม	ให้สัตยาบัน	มีผลบังคับใช้	R.	D.	A.	T.	C.	O.	หน่วยงานกลางให้ความช่วยเหลือซึ่งกันและกัน (Article 27)	หน่วยงานที่รับผิดชอบการส่งผู้ร้ายข้ามแดน (Article 24)	องค์กร 24/7 (Article 35)
(ต่อ) มอลโดวา										punishment: 82, 31 August 1989 str., MD-2012 Chisinau, Republic of Moldova.	punishment: 82, 31 August 1989 str., MD-2012 Chisinau, Republic of Moldova.	
โมนาโก(55)	-	-	-	-	-	-	-	-	-	-	-	-
มอนเต-นิโกร	7/4/2005	-	-	-	-	-	-	-	-	-	-	-
เนเธอร์-แลนด์	23/11/2001	16/11/2006	1/3/2007	-	-	X	X	-	-	Landelijk Parket van het openbaar ministerie (National office of the public prosecution	The Ministry of Justice Office of International Legal Assistance in Criminal	Landelijk Parket van het openbaar ministerie (National office of the public prosecution

ประเทศ	ลงนาม	ให้สัตยาบัน	มีผลบังคับใช้	R	D.	A.	T.	C.	O.	หน่วยงานกลางให้ความช่วยเหลือซึ่งกันและกัน (Article 27)	หน่วยงานที่รับผิดชอบการส่งผู้ร้ายข้ามแดน (Article 24)	องค์กร 24/7 (Article 35)
(ต่อ) เนเธอร์-แลนด์										service) Postbus 395 3000 AJ ROTTERDAM	Matters PO BOX 20301 2500 EH THE HAGUE	service) Postbus 395 3000 AJ ROTTERDAM
นอร์เวย์	23/11/2001	30/6/2006	1/10/2006	X	X	X	-	-	-	The National Criminal Investigation Service (KRIPOS)	Royal Ministry of Justice and the Police, P.O. Box 8005, N-0030 OSLO	the National Criminal Investigation Service (KRIPOS). The High Tech Crime Division
โปแลนด์	23/11/2001	-	-	-	-	-	-	-	-	-	-	-
โปรตุเกส	23/11/2001	-	-	-	-	-	-	-	-	-	-	-
โรมาเนีย	23/11/2001	12/5/2004	1/9/2004	-	-	X	-	-	-	The Prosecutor's Office to the High Court of Cassation	Ministry of Justice (address: Str. Apollodor nr. 17,	Service of Combating Cybercrime within

ประเทศ	ลงนาม	ให้สัตยาบัน	มีผลบังคับใช้	R	D.	A.	T.	C.	O.	หน่วยงานกลางให้ความช่วยเหลือซึ่งกันและกัน (Article 27)	หน่วยงานที่รับผิดชอบการส่งผู้ร้ายข้ามแดน (Article 24)	องค์กร 24/7 (Article 35)
(ต่อ) โรมาเนีย										and Justice for pre-trial investigations (address: Blvd. Libertatii nr. 12-14, sector 5, Bucuresti) The Ministry of Justice for the requests during the trial or execution of punishment	sector 5, Bucuresti)	the Section for Combating Organised Crime and Drugs Trafficking to the High Court of Cassation and Justice (address: Blvd. Libertatii nr. 12-14, sector 5, Bucuresti).
รัสเซีย	-	-	-	-	-	-	-	-	-	-	-	-

ประเทศ	ลงนาม	ให้สัตยาบัน	มีผลบังคับใช้	R.	D.	A.	T.	C.	O.	หน่วยงานกลางให้ความช่วยเหลือซึ่งกันและกัน (Article 27)	หน่วยงานที่รับผิดชอบการส่งผู้ร้ายข้ามแดน (Article 24)	องค์กร 24/7 (Article 35)
ซาน-มาริโน (55)	-	-	-	-	-	-	-	-	-	-	-	-
เซอร์เบีย	7/4/2005	14/4/2009	1/8/2009	-	-	X	-	-	-	District Attorney for High-Tech Crime of the Republic of Serbia Savska 17A 11000 Beograd Ministry of Interior of the Republic of Serbia Directorate of Crime Police Department for the fight against organized crime	District Attorney for High-Tech Crime of the Republic of Serbia Savska 17A 11000 Beograd Ministry of Interior of the Republic of Serbia Directorate of Crime Police Department for	District Attorney for High-Tech Crime of the Republic of Serbia Savska 17A 11000 Beograd T Ministry of Interior of the Republic of Serbia Directorate of Crime Police Department for the fight against organized crime

ประเทศ	ลงนาม	ให้สัตยาบัน	มีผลบังคับใช้	R.	D.	A.	T.	C.	O.	หน่วยงานกลางให้ความช่วยเหลือซึ่งกันและกัน (Article 27)	หน่วยงานที่รับผิดชอบการส่งผู้ร้ายข้ามแดน (Article 24)	องค์กร 24/7 (Article 35)
(ต่อ) เซอร์เบีย										Bulevar Mihajla Pupina 2 11070 Novi Beograd	the fight against organized crime Bulevar Mihajla Pupina 2 11070 Novi Beograd	Bulevar Mihajla Pupina 2 11070 Novi Beograd
สโลวาเกีย	4/2/2005	8/1/2008	1/5/2008	X	X	X	-	-	-	Ministry of Justice of the Slovak Republic (Zupné námestie 13, 81311 Bratislava) and the General Prosecutor's Office (Stúrova 2, 81285 Bratislava)	Ministry of Justice of the Slovak Republic (Zupné námestie 13, 81311 Bratislava) for extradition Competent prosecutor of the Regional Prosecutor's	Presidium of the Police Forces, International Police Cooperation Office, National Central Bureau of Interpol (Vajnorská 25, 81272 Bratislava)

ประเทศ	ลงนาม	ให้สัตยาบัน	มีผลบังคับใช้	R.	D.	A.	T.	C.	O.	หน่วยงานกลางให้ความช่วยเหลือซึ่งกันและกัน (Article 27)	หน่วยงานที่รับผิดชอบการส่งผู้ร้ายข้ามแดน (Article 24)	องค์กร 24/7 (Article 35)
(ต่อ) สโลวาเกีย											Office and the Ministry of Justice for receiving requests for provisional arrests Ministry of Justice of the Slovak Republic and the court competent for issuing an international arrest warrant	

ประเทศ	ลงนาม	ให้สัตยาบัน	มีผลบังคับใช้	R.	D.	A.	T.	C.	O.	หน่วยงานกลางให้ความช่วยเหลือซึ่งกันและกัน (Article 27)	หน่วยงานที่รับผิดชอบการส่งผู้ร้ายข้ามแดน (Article 24)	องค์กร 24/7 (Article 35)
สโลวีเนีย	24/7/2002	8/9/2004	1/1/2005	-	-	X	-	-	-	Ministry of Justice Zupanciceva 3 SI - 1000 Ljubljana	Ministry of Foreign Affairs for extradition: Presernova 25 SI - 1000 Ljubljana Ministry of the Interior, Criminal Investigation Police Directorate, International Police Cooperation Section for	Ministry of the Interior Criminal Investigation Police Directorate International Police Cooperation Section

ประเทศ	ลงนาม	ให้สัตยาบัน	มีผลบังคับใช้	R	D.	A.	T.	C.	O.	หน่วยงานกลางให้ความช่วยเหลือซึ่งกันและกัน (Article 27)	หน่วยงานที่รับผิดชอบการส่งผู้ร้ายข้ามแดน (Article 24)	องค์กร 24/7 (Article 35)
(ต่อ) สโลวีเนีย											requests for provisional arrests: Ministry of the Interior Criminal Investigation Police Directorate International Police Cooperation Section	
สเปน	23/11/2001 r	-	-	-	-	-	-	-	-	-	-	-
สวีเดน	23/11/2001	-	-	-	-	-	-	-	-	-	-	-

ประเทศ	ลงนาม	ให้สัตยาบัน	มีผลบังคับใช้	R.	D.	A.	T.	C.	O.	หน่วยงานกลางให้ความช่วยเหลือซึ่งกันและกัน (Article 27)	หน่วยงานที่รับผิดชอบการส่งผู้ร้ายข้ามแดน (Article 24)	องค์กร 24/7 (Article 35)
สวิตเซอร์-แลนด์	23/11/2001	-	-	-	-	-	-	-	-	-	-	-
มาซิโดเนีย	23/11/2001	15/9/2004	1/1/2005	-	-	X	-	-	-	Ministry of Justice	Ministry of Justice	Deputy Public Prosecutor Department for Fight against Crime and Corruption Office of Public Prosecutor ul. Krste Misirkov bb 1000 SKOPJE
ตุรกี	-	-	-	-	-	-	-	-	-	-	-	-

ประเทศ	ลงนาม	ให้สัตยาบัน	มีผลบังคับใช้	R.	D.	A.	T.	C.	O.	หน่วยงานกลางให้ความช่วยเหลือซึ่งกันและกัน (Article 27)	หน่วยงานที่รับผิดชอบการส่งผู้ร้ายข้ามแดน (Article 24)	องค์กร 24/7 (Article 35)
ยูเครน	23/11/2001	10/3/2006	1/7/2006	X	-	X	-	-	-	Ministry of Justice of Ukraine (concerning courts' commission) and the General Prosecutor's Office of Ukraine (concerning commissions of bodies of prejudicial inquiry)	Ministry of Justice of Ukraine (concerning court's inquiries) and the General Prosecutor's Office of Ukraine (concerning inquiries of bodies of prejudicial inquiry)	-
สหราช-อาณาจักร	23/11/2001											

กลุ่มประเทศที่ไม่ได้เป็นสมาชิกสภายุโรป (Non-member States of the Council of Europe)

ประเทศ	ลงนาม	ให้สัตยาบัน	มีผลบังคับใช้	R.	D.	A.	T.	C	O	หน่วยงานกลางให้ความช่วยเหลือซึ่งกันและกัน (Article 27)	หน่วยงานที่รับผิดชอบการส่งผู้ร้ายข้ามแดน (Article 24)	องค์กร 24/7 (Article 35)
แคนาดา	23/11/2001	-	-	-	-	-	-	-	-	-	-	-
ชิลี	-	-	-	-	-	-	-	-	-	-	-	-
คอสตาริกา	-	-	-	-	-	-	-	-	-	-	-	-
สาธารณรัฐโดมินิกัน	-	-	-	-	-	-	-	-	-	-	-	-
ญี่ปุ่น	23/11/2001	-	-	-	-	-	-	-	-	-	-	-
เม็กซิโก	-	-	-	-	-	-	-	-	-	-	-	-

ประเทศ	ลงนาม	ให้สัตยาบัน	มีผลบังคับใช้	R.	D.	A.	T.	C	O	หน่วยงานกลางให้ความช่วยเหลือซึ่งกันและกัน (Article 27)	หน่วยงานที่รับผิดชอบการส่งผู้ร้ายข้ามแดน (Article 24)	องค์กร 24/7 (Article 35)
ฟิลิปปินส์	-	-	-	-	-	-	-	-	-	-	-	-
แอฟฟริกา-ใต้	23/11/2001	-	-	-	-	-	-	-	-	-	-	-
สหรัฐ-อเมริกา	23/11/2001	29/9/2006	1/1/2007	X	X	X	-	-	-	Office of International Affairs, United States Department of Justice, Criminal Division, Washington, D.C., 20530	-	-

จำนวนประเทศที่ลงนามแต่ยังไม่ได้มีการให้สัตยาบัน	20
จำนวนประเทศที่ลงนามและมีการให้สัตยาบัน/ภาคยานุวัติ	26

หมายเหตุ : สถานะ ณ วันที่ 5 ธันวาคม 2552

55 = วันที่มีการลงนามโดยบอสเนียและเฮอร์เซโกวีนา

R = ข้อสงวน (Reservations)

D = ปฏิญญา (Declarations)

A = องค์กร (Authorities)

T = การบังคับใช้บทบัญญัติสำหรับสหพันธรัฐ (Territorial Application)

C = การบัญญัติในส่วนที่เกี่ยวกับการติดต่อสื่อสาร (Communication)

O = การคัดค้าน (Objection)