รายงานวิจัยฉบับสมบูรณ์

โครงการวิจัยเรื่อง
ต้นแบบกฎหมายเพื่อป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตน

โดย

ผู้ช่วยศาสตราจารย์ ดร. สุพัตรา แผนวิชิต

รองศาสตราจารย์ คณาธิป ทองรวีวงศ์

มหาวิทยาลัยสุโขทัยธรรมาธิราช

ได้รับทุนวิจัยจากกองทุนวิทยาศาสตร์ วิจัยและนวัตกรรม ประจำปี 2565

สำนักงานคณะกรรมการส่งเสริมวิทยาศาสตร์ วิจัยและนวัตกรรม (สกสว.)

มีนาคม 2566

ชื่อเรื่อง ต้นแบบกฎหมายเพื่อป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตน

ชื่อผู้วิจัย ผู้ช่วยศาสตราจารย์ ดร. สุพัตรา แผนวิชิต หัวหน้าโครงการ
รองศาสตราจารย์ คณาธิป ทองรวีวงศ์ นักวิจัยร่วม

ปีที่แล้วเสร็จ 2566

บทคัดย่อ

การศึกษาวิจัยครั้งนี้มีวัตถุประสงค์เพื่อ 1) ศึกษารูปแบบของอาชญากรรมแบบไร้ตัวตนที่กระทำโดยองค์กรอาชญากรรมข้ามชาติในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ ตลอดจนความเสี่ยงจากภัยคุกคามจากอาชญากรรมประเภทดังกล่าว 2) ศึกษากฎหมายที่กำหนดความผิดเกี่ยวกับอาชญากรรมแบบไร้ตัวตนที่กระทำโดยองค์กรอาชญากรรมข้ามชาติในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์โดยศึกษาเปรียบเทียบกฎหมายต่างประเทศ และศึกษากฎหมายที่เกี่ยวข้องกับการบังคับใช้กฎหมายของประเทศไทย ทั้งด้านการสืบสวนสอบสวน การรวบรวมพยานหลักฐาน การดำเนินคดี การดำเนินมาตรการตามกฎหมายฟอกเงิน และความร่วมมือระหว่างประเทศ 3) ศึกษาถึงปัญหาและอุปสรรคในการบังคับใช้กฎหมายและการป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตนที่กระทำโดยองค์กรอาชญากรรมข้ามชาติในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ 4) ศึกษาและจัดทำต้นแบบกฎหมาย (Model Law) ของประเทศไทย ในรูปแบบของการจัดทำกฎหมายต้นแบบเพื่อป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ และ 5) เสนอแนะมาตรการความร่วมมือระหว่างประเทศเพื่อป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตนที่กระทำโดยองค์กรอาชญากรรมข้ามชาติในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์

ระเบียบวิธีการวิจัย ประกอบด้วย การวิจัยเอกสาร (Documentary research) การประชุมกลุ่มย่อย (Focus Group) และการจัดสัมมนาเพื่อรับฟังความคิดเห็นจากหน่วยงานที่เกี่ยวข้องและผู้มีส่วนได้เสีย

ผลการศึกษาพบว่า มีปัญหาการบังคับใช้กฎหมายกับอาชญากรรมแบบไร้ตัวตนหลายประการคือ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ยังไม่ครอบคลุมถึงความผิดในส่วนขั้นตอนการกระทำอันเป็นการปกปิดตัวตน มีข้อจำกัดของการบังคับใช้กฎหมายเกี่ยวกับมาตรการด้านการสืบสวนสอบสวน รวบรวมพยานหลักฐาน การดำเนินการกับทรัพย์สินที่เกี่ยวกับการกระทำความผิด และมาตรการความร่วมมือระหว่างประเทศ ผู้วิจัยจึงเสนอแนะแนวทางการจัดทำต้นแบบกฎหมายเพื่อป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ โดยมีสาระสำคัญเกี่ยวกับการกำหนดฐานความผิดของอาชญากรรมแบบไร้ตัวตน การกำหนดมาตรการสืบสวนสอบสวน การดำเนินการกับทรัพย์สินที่เกี่ยวกับการกระทำความผิด มาตรการด้านพยานหลักฐาน และมาตรการความร่วมมือระหว่างประเทศ

คำสำคัญ ต้นแบบกฎหมาย อาชญากรรมแบบไร้ตันตน ความผิดเกี่ยวกับคอมพิวเตอร์

Title: Model Law for Prevention and Suppression of Criminal Anonymity

Researcher: Asst. Prof. Dr. Supatra Phanwichit Project Manager
Assoc. Prof. Kanathip Thongraweewong Co-Researcher

Year of Completion: 2023

Abstract

The objectives of this research are: 1) to study patterns of criminal anonymity devised by trans-national organized crimes in commission of offenses, which breaches computer systems or data, as well as risks of potential threats posed by the said category of crimes; 2) to study laws, which prescribe against offenses relating to criminal anonymity devised by trans-national organized crimes in commission of offenses breaching computer systems or data, by conducting comparative study of foreign laws and Thai laws relating to law enforcement, in terms of both detecting and investigating into the crimes, gathering the evidence, prosecuting the offenders, applying measures under anti-money laundering laws and coordinating international cooperation; 3) to study problems with and obstacles to enforcement of the laws and prevention and suppression of the criminal anonymity devised by trans-national organized crimes in commission of offenses, which breach computer systems or data; 4) to study and draft a model law for Thailand in a form of legislating the model law for prevention and suppression of the criminal anonymity, which breaches computer systems or data; and 5) to recommend measures of international cooperation for prevention and suppression of the criminal anonymity devised by trans-national organized crimes in commission of offenses, which breach computer systems or data.

The research methodology consists of documentary research, focus group, and seminar for hearing opinions from competent agencies and stakeholders.

The study results show that there are many problems with enforcement of the laws against the criminal anonymity. That is to say - Computer-related Crime Act, B.E. 2550 (2007), does not cover offenses on parts, which are committed by the criminal anonymity. There are restrictions on enforcement of the law, in relation to detection, investigation, evidence gathering, procedures for offense-related properties, and measures of international cooperation. Therefore, the researchers recommend an approach to drafting the model law for prevention and suppression of the criminal anonymity in the offenses, which breach computer systems or data, whereas the essential matter is to prescribe against offenses in forms of the criminal anonymity, stipulate detection and investigation measures, procedures for offense-related properties, measures for evidence and witnesses, and measures of international cooperation.

Keyword: Model Law; Criminal Anonymity; Computer-Related Offense

สารบัญ

บทที่ 5

บทที่ 1
บทนำ

1.1 หลักการและเหตุผล

ปัจจุบันโลกเข้าสู่ยุคสังคมดิจิทัลอย่างแท้จริงประกอบกับนโยบายรัฐบาลได้เร่งผลักดันให้มีนำเทคโนโลยีดิจิทัลมาใช้เป็นเครื่องมือสำคัญในการขับเคลื่อนการพัฒนาเศรษฐกิจและสังคมของประเทศไปสู่ความมั่นคง มั่งคั่ง ยั่งยืนและให้ความสำคัญต่อการพัฒนาวิจัยและการใช้ประโยชน์จากนวัตกรรม ทั้งนี้ตามแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมของไทย มุ่งเน้นการมีกฎหมาย กฎเกณฑ์และมาตรฐานที่มีประสิทธิภาพ ทันสมัย สอดคล้องกับหลักการสากล รองรับการทำธุรกรรมทางอิเล็กทรอนิกส์และพาณิชย์อิเล็กทรอนิกส์ เพื่ออำนวยความสะดวก ลดอุปสรรคและเพิ่มประสิทธิภาพในการทำธุรกรรมออนไลน์ รวมทั้งสร้างความเชื่อมั่นและคุ้มครองสิทธิ์แก่ผู้ใช้บริการแต่ด้วยนวัตกรรมใหม่ที่พัฒนาอย่างรวดเร็ว และ Disrupt โครงสร้างสังคมและธุรกิจแบบเดิม ๆ ส่งผลให้เกิดรูปแบบของอาชญากรรมในยุคดิจิทัลที่เปลี่ยนแปลงไปจากอาชญากรรมในรูปแบบเดิมอย่างสิ้นเชิง ทั้งรูปแบบวิธีการกระทำความผิด ความซับซ้อนของการกระทำความผิด การใช้เทคโนโลยีเป็นช่องทางในการกระทำความผิดและมีลักษณะเป็นอาชญากรรมข้ามชาติ กลายเป็นอาชญากรรมในรูปแบบไร้ตัวตน หรือ Anonymous Crime ซึ่งหมายถึงอาชญากรรมที่ไม่สามารถระบุตัวตนของผู้ประทำความผิดได้ รูปแบบของอาชญากรรมไร้ตัวตนที่ปรากฏในปัจจุบันและเป็นความท้าทายของหน่วยงานบังคับใช้กฎหมายและหน่วยงานในกระบวนการยุติธรรม ทำให้มีความยากในการบังคับใช้กฎหมายบนโลกออนไลน์ที่ไร้พรมแดน ทั้งในด้านการติดตามการกระทำความผิด การสืบสวนสอบสวน การรวบรวมหลักฐาน รวมทั้งการพิสูจน์พยานหลักฐานทางอิเล็กทรอนิกส์ รูปแบบอาชญากรรมในรูปแบบไร้ตัวตน อาทิ การก่ออาชญากรรมไซเบอร์ การโจรกรรมข้อมูล การยักยอกเงินจากระบบออนไลน์ การปล่อยมัลแวร์เพื่อขู่เงินเรียกค่าไถ่ การใช้เงินดิจิทัลซื้อขายสินค้าผิดกฎหมาย การฟอกเงินผ่านการโอนเงินอิเล็กทรอนิกส์หรือเงินดิจิทัล เป็นต้น

กฎหมายที่ใช้บังคับในปัจจุบัน ได้แก่ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม ที่บังคับใช้กับรูปแบบอาชญากรรมที่เข้าข่ายเป็นตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พบว่า โครงสร้างของความผิดออกเป็น 2 ลักษณะคือ ความผิดในลักษณะที่ 1 คือความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ (Computer as a target) ซึ่งจะเป็นผลกระทบที่เกิดกับทรัพย์สินเป็นหลัก ได้แก่ ความผิดฐานเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันตาม

มาตรา 5 ความผิดฐานเปิดเผยมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นโดยมิชอบตามมาตรา 6 ความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์ตามมาตรา 7 ความผิดฐานดักรับข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบตามมาตรา 8 ความผิดฐานทำให้เสียหาย เปลี่ยนแปลงข้อมูลคอมพิวเตอร์โดยมิชอบตามมาตรา 9 ความผิดฐานกระทำเพื่อให้การทำงานของระบบคอมพิวเตอร์ไม่สามารถทำงานตามปกติได้ตามมาตรา 10 ความผิดฐานส่งข้อมูลคอมพิวเตอร์รบกวนการใช้ระบบคอมพิวเตอร์ตามมาตรา 11 ความผิดฐานจำหน่ายชุดคำสั่งที่จัดทำขึ้นเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา 13 และลักษณะที่ 2 คือ ความผิดที่ใช้ระบบหรือข้อมูลหรืออุปกรณ์คอมพิวเตอร์เป็นช่องทางหรือเป็นเครื่องมือ (Computer as a tool) ได้แก่ ความผิดฐานใช้คอมพิวเตอร์กระทำความผิดอื่นตามมาตรา 14 และความผิดฐานนำเข้าสู่ระบบคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่นถูกเกลียดชัง หรือได้รับความอับอายตามมาตรา 16

อย่างไรก็ตาม ในการบังคับใช้กฎหมายกับการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ดังกล่าว ยังมีปัญหาและอุปสรรคหลายประการ สืบเนื่องจากลักษณะของอาชญากรรมในยุคดิจิทัลกระทำผ่านเทคโนโลยีในรูปแบบที่ทันสมัยและพัฒนาไปอย่างรวดเร็ว ทำให้เกิดรูปแบบอาชญากรรมที่เรียกว่า “อาชญากรรมแบบไร้ตัวตน” ทำให้ยากต่อการสืบสวนและเชื่อมโยงไปสู่ตัวผู้กระทำความผิด อาชญากรรมลักษณะนี้จึงเป็นสิ่งที่ภาครัฐต้องเฝ้าระวัง เพราะประเทศกำลังมุ่งไปสู่ยุคดิจิทัลย่อมจะมีโอกาสเผชิญกับอาชญากรรมแบบไร้ตัวตนที่สูงขึ้น จึงเป็นความท้าทายในการบังคับใช้กฎหมายเพื่อรับมือกับป้องกันปัญหาอาชญากรรม ไม่ว่าจะเป็นการแก้ไขปัญหาโดยใช้มาตรการสืบสวนสอบสวนและเทคนิคพิเศษ การใช้เทคโนโลยีในการติดตามร่องรอยการกระทำความผิด การดำเนินคดีกับผู้บงการขององค์กรอาชญากรรม การใช้มาตรการด้านพยานหลักฐานที่มีประสิทธิภาพเพื่อพิสูจน์การกระทำความผิด มาตรการตรวจสอบพยานหลักฐานทางอิเล็กทรอนิกส์ และในปัจจุบันประเทศไทยยังไม่มีกฎหมายเฉพาะที่ใช้บังคับเพื่อป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตนทั้งระบบ ดังนั้น จึงจำเป็นต้องศึกษาและวิเคราะห์เพื่อนำไปสู่การจัดทำกฎหมายต้นแบบในการป้องกันและปราบปรามอาชญากรรมไร้ตัวตนในยุคดิจิทัล โดยกฎหมายจะต้องมีรูปแบบที่ทันต่อการเปลี่ยนแปลงด้านนวัตกรรมทางเทคโนโลยี สามารถการรับมืออาชญากรรมแบบไร้ตัวตนที่สามารถกระทำได้ทุกที่ทุกเวลาและมีพลวัตร และต้นแบบกฎหมายดังกล่าวจะต้องแก้ไขบังคับใช้กฎหมายกับอาชญากรรมแบบไร้ตัวตนได้ โดยในการศึกษาวิจัยในครั้งนี้ ผู้วิจัยจะมุ่งศึกษาเฉพาะการกระทำความผิดขององค์กรอาชญากรรมข้ามชาติในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ (Computer as a target) อันเป็น

อาชญากรรมคอมพิวเตอร์หรืออาชญากรรมไซเบอร์ที่กำหนดไว้ตามกฎหมายระหว่างประเทศและกฎหมายต่างประเทศ เช่น สหรัฐอเมริกา กับสหภาพยุโรป มีวัตถุประสงค์เพื่อเสนอแนะต้นแบบกฎหมายในการป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตน ทั้งการกำหนดนิยามและรูปแบบการกระทำความผิด มาตรการทางกฎหมายในการสืบสวนสอบสวน ติดตามร่องรอยการกระทำความผิด และการบังคับใช้ในกรณีการกระทำความผิดของอาชญากรรมแบบไร้ตัวตนที่มีลักษณะเป็นองค์กรอาชญากรรมข้ามชาติ

ดังนั้น เพื่อป้องกันหรือรับมือกับภัยคุกคามจากอาชญากรรมแบบไร้ตัวตน จึงจำเป็นต้องทำการศึกษาวิจัยเพื่อพัฒนาต้นแบบกฎหมายเพื่อป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตน โดยวิเคราะห์จากแนวโน้มรูปแบบความผิดและกฎหมายที่เกี่ยวข้อง รวมถึงศึกษาปัญหาการบังคับใช้กฎหมายกับอาชญากรรมแบบไร้ตัวตนทั้งในด้านการสืบสวน สอบสวน การดำเนินคดี การใช้มาตรการพิเศษและการลงโทษผู้กระทำความผิด โดยศึกษากับแนวทางการบังคับใช้กฎหมายของต่างประเทศและแนวปฏิบัติสากล เพื่อวิเคราะห์และเสนอแนะต้นแบบกฎหมายในการป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตนของประเทศไทย เพื่อประโยชน์ในป้องกันอาชญากรรมที่อาจก่อให้เกิดความเสี่ยงต่อการให้บริการ การใช้บริการหรือการใช้ประโยชน์จากเครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม จนเกิดความเสียหายต่อประชาชนและกระทบต่อความมั่นคงทางเศรษฐกิจและสังคมของประเทศ สอดคล้องกับเป้าหมายและยุทธศาสตร์ในการพัฒนาและปรับปรุงกฎหมาย กฎระเบียบ มาตรการ เพื่อสร้างความเชื่อมั่นในการทำธุรกรรมอิเล็กทรอนิกส์และเพื่อความมั่นคงปลอดภัยทางไซเบอร์ ส่งผลต่อการคุ้มครองความปลอดภัยในทรัพย์สินของประชาชนและอำนวยความยุติธรรมให้แก่ประชาชน สอดคล้องกับยุคเศรษฐกิจและสังคมดิจิทัล

2. วัตถุประสงค์

1) เพื่อศึกษารูปแบบของอาชญากรรมแบบไร้ตัวตนที่กระทำโดยองค์กรอาชญากรรมข้ามชาติในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ ตลอดจนความเสี่ยงจากภัยคุกคามจากอาชญากรรมประเภทดังกล่าว
2) เพื่อศึกษากฎหมายที่กำหนดความผิดเกี่ยวกับอาชญากรรมแบบไร้ตัวตนที่กระทำโดยองค์กรอาชญากรรมข้ามชาติในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์โดยศึกษาเปรียบเทียบกฎหมายต่างประเทศ และศึกษากฎหมายที่เกี่ยวข้องกับการบังคับใช้กฎหมายของประเทศไทย ทั้งด้านการสืบสวนสอบสวน การรวบรวมพยานหลักฐาน การดำเนินคดี การดำเนินมาตรการตามกฎหมายฟอกเงิน และความร่วมมือระหว่างประเทศ

3) เพื่อศึกษาถึงปัญหาและอุปสรรคในการบังคับใช้กฎหมายและการป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตนที่กระทำโดยองค์กรอาชญากรรมข้ามชาติในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์
4) เพื่อศึกษาและจัดทำต้นแบบกฎหมาย (Model Law) ของประเทศไทย ในรูปแบบของการจัดทำกฎหมายต้นแบบเพื่อป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์
5) เพื่อเสนอแนะมาตรการความร่วมมือระหว่างประเทศเพื่อป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตนที่กระทำโดยองค์กรอาชญากรรมข้ามชาติในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์

3. สมมติฐานงานวิจัย

ลักษณะของอาชญากรรมในยุคดิจิทัลที่กระทำผ่านเทคโนโลยีในรูปแบบที่ทันสมัยและพัฒนาไปอย่างรวดเร็ว ทำให้เกิดอาชญากรรมรูปแบบใหม่ที่ยากต่อการสืบสวนและเชื่อมโยงไปสู่ตัวผู้กระทำความผิด เรียกว่า “อาชญากรรมแบบไร้ตัวตน” ที่มีแนวโน้มการกระทำความผิดที่สูงขึ้นและมีปัญหาในการบังคับใช้กฎหมายหลายประการทั้งปัญหาการสืบสวน สอบสวน การดำเนินคดี การพิจารณาคดีและมาตรการลงโทษ จึงจำเป็นต้องศึกษาและวิเคราะห์แนวโน้ม รูปแบบของอาชญากรรมแบบไร้ตัวตนที่เกิดขึ้นในยุคดิจิทัล โดยศึกษาเฉพาะการกระทำความผิดขององค์กรอาชญากรรมข้ามชาติในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์และเปรียบเทียบกับแนวทางการบังคับใช้กฎหมายของต่างประเทศ เพื่อจัดทำต้นแบบกฎหมายในการป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ของประเทศไทย เพื่อให้ประเทศไทยมีมาตรการประสิทธิภาพ สอดคล้องตามหลักสากลและทันต่อการเปลี่ยนแปลงทางเทคโนโลยีและรูปแบบอาชญากรรมทางเทคโนโลยี เป็นการพัฒนาระบบการบริหารจัดการด้านกระบวนการยุติธรรมของภาครัฐ ส่งผลต่อการคุ้มครองความปลอดภัยในทรัพย์สินของประชาชนและอำนวยความยุติธรรมให้แก่ประชาชน สอดคล้องกับยุคเศรษฐกิจและสังคมดิจิทัล

4. กรอบการวิจัย

5. นิยามสำคัญ

“อาชญากรรมแบบไร้ตัวตน” หมายความถึง รูปแบบหนึ่งของอาชญากรรมคอมพิวเตอร์ที่อาศัยประโยชน์จากสภาพแวดล้อมทางไซเบอร์ในการกระทำความผิด มีการกระทำความผิดทางระบบคอมพิวเตอร์ที่ใช้วิธีการปกปิดตัวตน โดยมีการนำข้อมูลบุคคลอื่นมาใช้ระบุตัว หรือการใช้วิธีการต่าง ๆ ในการปกปิดตัวตนของผู้กระทำความผิดและเป็นความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์

6. วิธีการดำเนินงาน

การวิจัยเชิงคุณภาพ ประกอบด้วย

1) การวิจัยเอกสาร (Documentary Research)

การดำเนินการวิจัยโดยการวิจัยเอกสาร เป็นการรวบรวมข้อมูลที่เกี่ยวข้องกับงานวิจัยจากเอกสารที่เกี่ยวข้อง ทั้งจากแหล่งข้อมูลปฐมภูมิ (Primary Sources) ประกอบด้วย ตัวบทกฎหมาย กฎกระทรวง ระเบียบและคำสั่ง ข้อบังคับของกระทรวง ทบวง กรม หรือหน่วยงานราชการต่างๆ รวมถึงคำพิพากษาต่างๆ และจากแหล่งข้อมูลทุติยภูมิ (Secondary Sources) ประกอบด้วย ตำรากฎหมาย รายงานการวิจัย ตำรา บทความในวารสาร เอกสารการสัมมนา และข้อมูลจากอินเตอร์เน็ตในรูปแบบของเว็บไซต์ เอกสารที่เกี่ยวข้องนี้มีทั้งเอกสาร

ไทยและต่างประเทศ ซึ่งส่วนหนึ่งของการวิจัยเอกสารนี้จะปรากฏอยู่ในบทที่ 2 การทบทวนวรรณกรรมและเป็นข้อมูลที่ใช้ในการวิเคราะห์ร่วมกับข้อมูลจากการจัดประชุมกลุ่มย่อยและการสัมมนารับฟังความเห็น

2) การประชุมกลุ่มย่อย (Focus Group)

ผู้วิจัยจะดำเนินการจัดประชุมกลุ่มย่อย เพื่อระดมความคิดเห็นเกี่ยวกับแนวทางป้องกันและปราบปรามการกระทำความผิดในรูปแบบอาชญากรรมไร้ตัวตนและแนวทางการกำหนดต้นแบบต้นแบบเกี่ยวกับอาชญากรรมไร้ตัวตน โดยจะดำเนินการส่งประเด็นการประชุมให้ผู้เข้าประชุมทราบล่วงหน้า เพื่อให้ได้มาซึ่งข้อมูลที่จะใช้ในการวิเคราะห์ร่วมกับวิธีการวิจัยวิธีอื่น รายละเอียดดังนี้

2.1) ประชากร

ประชากรที่เข้าร่วมประชุมกลุ่มย่อย กำหนดให้เป็นผู้ทรงคุณวุฒิที่มีความเชี่ยวชาญในหน่วยงานบังคับใช้กฎหมายกับอาชญากรรมแบบไร้ตัวตน จำนวน 30 คน จากหน่วยงานดังต่อไป

1. สำนักงานตำรวจแห่งชาติ
2. ผู้บังคับการกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี
3. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
4. กรมสอบสวนคดีพิเศษ
5. สำนักงานคดีพิเศษ สำนักงานอัยการสูงสุด
6. สำนักงานศาลยุติธรรม
7. สำนักงานป้องกันและปราบปรามการฟอกเงิน
8. สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ
9. กรมคุ้มครองสิทธิและเสรีภาพ กระทรวงยุติธรรม
10. กรมราชทัณฑ์
11. กรมบังคับคดี
12. ผู้ทรงคุณวุฒิด้านกฎหมายอาญา
13. สำนักงานคณะกรรมการคุ้มครองผู้บริโภค
14. ผู้ทรงคุณวุฒิด้านกฎหมายอาชญากรรมทางเทคโนโลยี
15. ผู้ทรงคุณวุฒิด้านเทคโนโลยีสารสนเทศ

2.2) เครื่องมือในการเก็บรวบรวมข้อมูล

เครื่องมือในการเก็บรวบรวมข้อมูล ได้แก่ ประเด็นการประชุม ประกอบด้วยคำถามดังนี้

1. ความเห็นเกี่ยวกับแนวโน้ม รูปแบบของอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์
2. ความเห็นเกี่ยวกับความเสี่ยงจากภัยคุกคามจากอาชญากรรมแบบไร้ตัวตนและผลกระทบต่อประชาชนและสังคมและต่อระบบเศรษฐกิจและความมั่นคงของประเทศ
3. ความเห็นเกี่ยวกับบทบาทหน้าที่ของหน่วยงานที่เกี่ยวข้องและการบูรณาการความร่วมมือในการป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตน
4. ความเห็นเกี่ยวกับปัญหาและอุปสรรคในการบังคับใช้กฎหมายและการป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตน เกี่ยวข้องกับฐานความผิดเกี่ยวกับอาชญากรรมแบบไร้ตัวตน การบังคับใช้กฎหมาย การดำเนินคดี การบังคับกับทรัพย์สินและการลงโทษผู้กระทำความผิด
5. ความเห็นเกี่ยวกับร่างต้นแบบกฎหมาย (Model Law) เพื่อป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ของประเทศไทย
6. ความเห็นเกี่ยวกับมาตรการความร่วมมือระหว่างหน่วยงานทั้งภายในประเทศและต่างประเทศที่จำเป็นต่อการป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตน
7. ข้อเสนอแนะและมาตรการอื่นในการป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์

3) การจัดสัมมนารับฟังความคิดเห็น (Hearing)

ดำเนินการจัดสัมมนารับฟังความคิดเห็น (Hearing) เพื่อนำเสนอผลการวิจัยและร่างต้นแบบกฎหมาย (Model Law) เพื่อป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตนของประเทศ และรับฟังความคิดเห็นจากหน่วยงานที่เกี่ยวข้องและผู้มีส่วนได้เสีย จำนวนไม่ต่ำกว่า 50 คน

3.1) ประชากร

กลุ่มเป้าหมายของผู้เข้าร่วมสัมมนา ได้แก่ ผู้แทนหน่วยงานที่เกี่ยวข้องกับการบังคับใช้กฎหมายและผู้มีส่วนได้เสีย ได้แก่ สำนักงานตำรวจแห่งชาติ ผู้บังคับการกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กระทรวงยุติธรรม กรม

สอบสวนคดีพิเศษ กรมราชทัณฑ์ สำนักงานอัยการสูงสุด สำนักงานป้องกันและปราบปรามการฟอกเงิน สำนักงานศาลยุติธรรม กรมบังคับคดี สำนักงานคณะกรรมการคุ้มครองผู้บริโภค ธนาคารแห่งประเทศไทย สภาทนายความ สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ กรมคุ้มครองสิทธิและเสรีภาพ กระทรวงยุติธรรม นักวิชาการหรือผู้ทรงคุณวุฒิด้านกฎหมาย ด้านเทคโนโลยีสารสนเทศและประชาชนผู้มีส่วนได้เสีย และนำผลการรับฟังความคิดเห็นมาพิจารณาประกอบเพื่อแก้ไขปรับปรุงร่างกฎหมายและรายงานการวิจัยฉบับสมบูรณ์ให้มีความสมบูรณ์มากยิ่งขึ้น

3.2) เครื่องมือในการวิจัย

การจัดสัมมนารับฟังความคิดเห็น (Hearing) เครื่องมือการวิจัย ได้แก่ แบบแสดงความเห็นเกี่ยวกับร่างกฎหมายต้นแบบและข้อเสนอแนะ (ระบุประเด็นตามร่างกฎหมายและข้อเสนอแนะของงานวิจัย

7. ประโยชน์ที่คาดว่าจะได้รับ

7.1) ด้านนโยบาย

งานวิจัยนี้มีเป้าหมายในการเสนอต้นแบบกฎหมายในการป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ โดยการจัดทำเป็นข้อเสนอแนะทางวิชาการเพื่อให้รัฐบาลและหน่วยงานที่เกี่ยวข้องสามารถนำผลการศึกษาวิจัยไปใช้ประโยชน์อย่างเป็นรูปธรรม โดยการผลักดันร่างกฎหมายดังกล่าวเข้าสู่กระบวนการตรากฎหมายต่อไป โดยหน่วยงานที่สามารถนำผลงานไปใช้ประโยชน์ในด้านนโยบาย ได้แก่

1) คณะรัฐมนตรี สำนักงานตำรวจแห่งชาติ กระทรวงยุติธรรมและกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สามารถจะนำผลงานวิจัยไปใช้ในเป็นแนวทางในการแก้ไขปรับปรุงกฎหมายและแผนยุทธศาสตร์และตัวชี้วัดในหน่วยงาน

2) กรมสอบสวนคดีพิเศษ สำนักงานอัยการสูงสุดและสำนักงานศาลยุติธรรม สามารถนำผลงานวิจัยไปใช้ในส่วนที่เป็นร่างกฎหมายต้นแบบไปใช้ในการป้องกันและปราบปรามการกระทำความผิดที่เป็นอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์

7.2) ด้านสาธารณะ

ผลการศึกษาวิจัยจะได้รับการเผยแพร่ไปสู่สาธารณะ โดยเฉพาะกลุ่มผู้เกี่ยวข้องและผู้มีส่วนได้เสียผ่านการสัมมนารับฟังความคิดเห็นและรายงานการศึกษาวิจัยจะได้รับการเผยแพร่ต่อหน่วยงานที่เกี่ยวข้องและผู้ที่

สนใจทั่วไป ผ่านการจัดทำบทความเผยแพร่งานวิจัยลงในวารสารที่เป็นที่ยอมรับในวงวิชาการ เพื่อเป็นองค์ความรู้ทางวิชาการ ผู้สนใจ และประชาชนทั่วไป

7.3) ด้านพาณิชย์

ต้นแบบกฎหมายในการปราบปรามอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ ที่เป็นผลจากการวิจัยจะส่งผลด้านเศรษฐกิจที่สำคัญคือ ลดความสูญเสียมูลค่าทางเศรษฐกิจจากการกระทำความผิดทางเทคโนโลยี เนื่องจากกฎหมายสร้างมาตรการที่มุ่งเน้นการดำเนินการกับตัวผู้กระทำความผิดและเน้นการลงโทษทางด้านทรัพย์สินของผู้กระทำความผิด เพื่อชดใช้และเยียวยาผู้เสียหาย ทำให้รัฐใช้งบประมาณน้อยลงในการช่วยเหลือและเยียวยาเหยื่อหรือผู้เสียหาย

7.4) ด้านชุมชนและพื้นที่

ต้นแบบกฎหมายในการปราบปรามอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ที่เป็นผลจากการวิจัย จะส่งผลในระดับพื้นที่คือ ประชาชนทุกพื้นที่ของประเทศไทยจะมีหลักประกันในสวัสดิภาพและความเป็นอยู่ของตน เนื่องจากรัฐมีมาตรการเฝ้าระวัง มาตรการป้องกันและปราบปรามอาชญากรรมในยุคดิจิทัลที่ทันต่อสถานการณ์และมีประสิทธิภาพ จะทำให้อาชญากรรมลดน้อยลง ลดปัญหาภัยคุกคามทางเทคโนโลยีที่เกิดต่อประชาชน ส่งผลให้เกิดความสงบสุข ความเป็นระเบียบเรียบร้อยและความปลอดภัยของสังคมและประชาชนตามมา

7.5) ด้านวิชาการ

ประโยชน์ทางด้านวิชาการคือ เป็นองค์ความรู้เพื่อให้หน่วยงานที่เกี่ยวข้องนำไปใช้ประโยชน์เพื่อเป็นแนวทางในการตรากฎหมาย ซึ่งจะส่งผลโดยตรงต่อประสิทธิภาพในการบังคับใช้กฎหมาย และหน่วยงานรัฐและบุคคลทั่วไปสามารถนำไปใช้ประโยชน์หรืออ้างอิงทางวิชาการได้

บทที่ 2

แนวคิด ทฤษฎี และรูปแบบอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์

1. แนวคิดทฤษฎีเกี่ยวกับอาชญากรรมความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์

แนวคิดทฤษฎี “ความมั่นคงปลอดภัยของข้อมูลสารสนเทศ” (Information security) วางหลักเกณฑ์เกี่ยวกับปัจจัยหรือองค์ประกอบในการบ่งชี้ความปลอดภัยของระบบ หรือ เครือข่าย หรือข้อมูลคอมพิวเตอร์[1] โดยทั่วไปปัจจัยบ่งชี้ที่สำคัญมีสามประการหรือที่เรียกย่อว่า “CIA” ได้แก่

- “Confidentiality” หรือ “C” หมายถึง หมายถึง ระบบหรือข้อมูลไม่ถูกเข้าถึงโดยผู้ที่ไม่มีสิทธิ[2]

- “Integrity” หรือ “I” คือ บูรณภาพ ซึ่งมีความหมายว่าข้อมูลจะถูกเปลี่ยนแปลงได้เฉพาะกรณีที่กระทำโดยมีอำนาจ[3] คุณลักษณะความบูรณภาพนี้ มีความสัมพันธ์กับคุณลักษณะอื่น เช่น ความถูกต้อง (Correctness) ความสม่ำเสมอ (Consistency) ความสมบูรณ์ (Completeness) และ ความเชื่อถือได้ (Reliability) ของระบบและข้อมูล[4]

- “Availability” หรือ “A” คือความพร้อมใช้งาน หมายถึง ระบบอยู่ในสภาพพร้อมที่จะทำงานเมื่อผู้มีสิทธิประสงค์จะใช้งาน[5]

ในระดับของกฎหมายและข้อตกลงระหว่างประเทศ ก็ปรากฏถึงการนำแนวคิดนี้มาใช้ในการกำหนดลักษณะของอาชญากรรมคอมพิวเตอร์ เช่น ข้อมติ 55/63 ที่รับรองโดยสมัชชาใหญ่สหประชาชาติ[6] เน้นย้ำว่า

---

[1] Yulia Cherdantseva and Jeremy Hilton, “Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals,” in Organizational, Legal, and Technological Dimensions of Information System Administrator, eds. Fernando Almeida and Irene M. Portela (IGI Global Publishing, 2013).

[2] Urs E. Gattiker, The Information Security Dictionary (Kluwer Academic Publisher, 2004), p. 59.

[3] National Research Council, Computers at Risk (Washington, DC: National Academy Press, 1991), p. 54.

[4] Kathleen Frawley, Dale W. Miller, and Cynthia Miller, “State of Security Features for Medical Information,” in Information Technology for the Practicing Physician, ed. Joan M. Kiel (Springer, 2001), p. 251.

[5] Kathleen Frawley, Dale W. Miller, and Cynthia Miller, “State of Security Features for Medical Information,” in Information Technology for the Practicing Physician, ed. Joan M. Kiel (Springer, 2001), p. 251.

[6] United Nations General Assembly, Combating the Criminal Misuse of Information Technologies (Resolution 55/63) [Online]. 2000. Available from: http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf [21 November 2018]

ระบบกฎหมายควรคุ้มครองความลับ บูรณภาพและความพร้อมใช้ของข้อมูลและระบบคอมพิวเตอร์ จากการแก้ไขเปลี่ยนแปลงโดยไม่มีสิทธิ สำหรับสิ่งที่ก่อให้เกิดความเสี่ยงหรือผลกระทบต่อความปลอดภัยหรือ “ CIA” ดังกล่าวก็คือ “ภัยคุกคาม” (Threat) ซึ่งในที่นี้ก็คือการกระทำของอาชญากรรมคอมพิวเตอร์

เนื่องจากอาชญากรรมแบบไร้ตัวตนมีหลายรูปแบบและใช้วิธีการที่แตกต่างกัน ในการพิจารณาผลกระทบของอาชญากรรมต่อความปลอดภัยทางคอมพิวเตอร์จึงต้องแยกวิเคราะห์เป็นกรณีไป เช่น องค์กรอาชญากรรมใช้วิธีการแฮกข้อมูลเพื่อโจรกรรม หรือการได้มาซึ่งข้อมูลคอมพิวเตอร์โดยมิชอบ จัดเป็นอาชญากรรมที่กระทบต่อความลับของข้อมูล หรือการใช้มัลแวร์ (Malware) เช่น ไวรัส เกิดความเสียหายแก้ไข เปลี่ยนแปลงข้อมูลคอมพิวเตอร์ จัดเป็นอาชญากรรมที่กระทบต่อบูรณภาพของข้อมูล อาชญากรรมไร้ตัวตนที่ทำการโจมตีให้ระบบเกิดการปฏิเสธการใช้งาน (DOS) ส่งผลกระทบต่อความพร้อมใช้งาน ทั้งนี้ในแง่ของกฎหมายผู้วิจัยจะได้นำกรอบแนวคิดด้านความปลอดภัย (CIA) มาใช้วิเคราะห์การปรับใช้ฐานความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์กับกรณีอาชญากรรมไร้ตัวตน

2. แนวคิดทฤษฎีเกี่ยวกับความสัมพันธ์ระหว่างอาชญากรรมกับคอมพิวเตอร์

เมื่อพิจารณาสภาพการทำธุรกรรมและการดำรงชีวิตปัจจุบันจะพบว่ามีการกระทำต่างๆ เกิดขึ้นผ่านระบบคอมพิวเตอร์และกฎหมายกำหนดให้การกระทำหลายอย่างเป็นความผิด โดยแต่ละประเทศอาจกำหนดความผิดสำหรับการกระทำผ่านระบบคอมพิวเตอร์แตกต่างกันไป ในประเด็นนี้ นอกจากการใช้กรอบแนวคิดเกี่ยวกับความปลอดภัยทางคอมพิวเตอร์ดังกล่าวมาแล้ว ยังมีนักวิชาการหลายท่าน[7] เสนอเกณฑ์เพื่อวิเคราะห์จำแนกความสัมพันธ์ระหว่างอาชญากรรมกับคอมพิวเตอร์ ซึ่งรวมถึงระบบ เครือข่าย ข้อมูลคอมพิวเตอร์ ออกเป็นสองกลุ่มคือ

(1) อาชญากรรมซึ่งกระทำการโดยมุ่งเป้าไปที่คอมพิวเตอร์หรือมีคอมพิวเตอร์เป็นเป้าหมาย (Computer is the target) อาชญากรรมกลุ่มนี้ ส่งผลกระทบต่อความมั่นคงปลอดภัยทางคอมพิวเตอร์ หรือกระทบต่อคุณลักษณะเช่น “CIA” ดังที่ได้ทบทวนแนวคิดทฤษฎีไปแล้ว เช่น การแก้ไขเปลี่ยนแปลงข้อมูล การทำลายข้อมูลโดยมัลแวร์ ฯลฯ

---

[7] David L. Carter, “Computer Crime Categories: How Techno-Criminals Operate,” FBI Law Enforcement Bulletin 64,7 (1995): 21-26. ; Russell G. Smith, Peter N. Grabosky, and Gregor F. Urbas, Cyber Criminals on Trial (UK: Cambridge University Press, 2004) ; Susan Brenner, Cybercrime: Criminal Threats from Cyberspace (Santa Barbara, California: Praeger, 2010).

(2) อาชญากรรมที่ใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด (Computer is the instrumentality of the crime) หรือใช้คอมพิวเตอร์เป็นเครื่องมืออำนวยความสะดวกหรือใช้สนับสนุนการกระทำผิด แต่ไม่ได้มีเป้าหมายที่คอมพิวเตอร์ โดยเฉพาะอย่างยิ่ง อาชญากรรมเกี่ยวกับเนื้อหา (Content-related offenses) เช่น เนื้อหาลามกอนาจาร เนื้อหาที่เกี่ยวกับพฤติกรรมความรุนแรง (Violent behavior)[8] จะเห็นได้ว่า การโพสต์แชร์เนื้อหาผิดกฎหมาย มีเป้าหมายที่การรับรู้ข้อมูลข่าวสารของบุคคล แต่ไม่ใช่มีเป้าหมายที่ความปลอดภัยของระบบ เครือข่าย หรือข้อมูลคอมพิวเตอร์

เมื่อนำแนวคิดทฤษฎีดังกล่าวมาพิจารณาอาชญากรรมแบบไร้ตัวตนจะพบว่า ในภาพรวมแล้วอาชญากรรมแบบไร้ตัวตนอาจเกี่ยวข้องกับความผิดได้ทั้งสองกลุ่ม หากปรากฏว่าการประกอบอาชญากรรมนั้นมีการใช้วิธีการเพื่อปกปิดร่องรอยหรือการระบุตัวของผู้กระทำ ดังเช่นตัวอย่างต่อไปนี้

- แฮกเกอร์ส่งไวรัสไปทำลายข้อมูลในคอมพิวเตอร์ขององค์กรเป้าหมายและใช้วิธีการทางเทคนิคปกปิดร่องรอยการกระทำ กรณีนี้เป็นการกระทำที่มุ่งเป้าไปที่ข้อมูลคอมพิวเตอร์และส่งผลกระทบต่อความปลอดภัยทางคอมพิวเตอร์หรือกระทบต่อคุณสมบัติ “CIA”

- การโพสต์แชร์เนื้อหาผิดกฎหมายโดยใช้วิธีการปกปิดตัวตนเพื่อไม่ให้ถูกจับกุม กรณีนี้แม้เป็นการกระทำที่เกี่ยวข้องกับคอมพิวเตอร์หรือใช้ช่องทางคอมพิวเตอร์ในการกระทำผิด แต่ไม่ใช่การกระทำที่มุ่งเป้าไปที่ระบบหรือข้อมูลคอพิวเตอร์และส่งผลกระทบต่อความปลอดภัยทางคอมพิวเตอร์ กล่าวคือไม่กระทบต่อคุณสมบัติ “CIA”

สำหรับงานวิจัยนี้มีขอบเขตศึกษาเฉพาะอาชญากรรมแบบไร้ตัวตนที่ส่งผลกระทบต่อความปลอดภัยของคอมพิวเตอร์ จึงเป็นกรณีอาชญากรรมประเภทที่หนึ่งซึ่งมีคอมพิวเตอร์เป็นเป้าหมาย

อย่างไรก็ตามเนื่องจากอาชญากรรมแบบไร้ตัวตนมีการกระทำสองส่วนคือ ส่วนของการกระทำหลักอันเป็นวัตถุประสงค์และส่วนของการกระทำเพื่อปกปิดร่องรอยหรือตัวตนของผู้ก่อเหตุซึ่งการกระทำในส่วนปกปิดตัวตน ในบางวิธีการอาจจัดอยู่ในกลุ่มการกระทำทางเนื้อหาหรือกระทำที่ใช้คอมพิวเตอร์เป็นเครื่องมือโดยไม่ได้กระทบต่อความปลอดภัยของระบบหรือข้อมูลคอมพิวเตอร์ เช่น อาชญากรสร้างบัญชีสื่อออนไลน์โดยใช้ข้อมูลระบุตัวของบุคคลอื่น จากนั้นใช้บัญชีดังกล่าวไปทำการหลอกลวงทรัพย์สิน จะเห็นได้ว่า ในส่วนของการกระทำปกปิด

[8] David Wall, “The Internet as a Conduit for Criminals,” in Information Technology and the Criminal Justice System, ed. April Pattavina (Thousand Oaks, CA: Sage, 2005), pp. 83-84.

ตัวตนคือในขั้นตอนการสร้างบัญชีเป็นการนำข้อมูลปลอมหรือเท็จเข้าสู่ระบบ ซึ่งเกี่ยวข้องกับเนื้อหาข้อมูล (Content) โดยมุ่งเป้าที่การหลอกลวงบุคคลมิใช่การโจมตีระบบหรือข้อมูลคอมพิวเตอร์

3. นิยามหรือความหมายของอาชญากรรมแบบไร้ตัวตน

จากการทบทวนวรรณกรรมและแนวคิดทฤษฎี ยังไม่พบการกำหนดนิยามของอาชญากรรมไร้ตัวตนหรืออาชญากรรมนิรนามที่กระทำทางคอมพิวเตอร์หรือไซเบอร์ (Anonymous Cybercrime) ไว้เป็นการเฉพาะ แต่มีวรรณกรรมที่กล่าวถึงองค์ประกอบหรือลักษณะสำคัญของอาชญากรรมแบบไร้ตัวตน ซึ่งผู้วิจัยนำมาวิเคราะห์และจำแนกเป็นแนวทางต่างๆ ในการอธิบายความหมายของอาชญากรรมไร้ตัวตนดังนี้

3.1 แนวทางการพิจารณาอาชญากรรมแบบไร้ตัวตนในแง่การบังคับใช้กฎหมายหรือการสืบสวนสอบสวน

วรรณกรรมหลายชิ้นชี้ให้เห็นว่าการกระทำผิดในพื้นที่ไซเบอร์เป็นปัญหาสำคัญเนื่องจากลักษณะความนิรนามสร้างอุปสรรคต่อการบังคับใช้กฎหมาย[9]งานวิชาการบางเรื่องชี้ให้เห็นว่า ปัญหาสำคัญของการกระทำโดยปกปิดตัวตนคือประเด็นด้านการสืบสวนสอบสวน[10]

จากการพิจารณาแนวทางนี้สามารถอธิบายได้ว่า *อาชญากรรมไร้ตัวตนเป็นการกระทำความผิดทางระบบคอมพิวเตอร์ที่ใช้วิธีการปกปิดตัวตนซึ่งเป็นอุปสรรคต่อการสืบสวนสอบสวน*

3.2 แนวทางการพิจารณาอาชญากรรมแบบไร้ตัวตนในแง่สภาพแวดล้อม

แนวทางนี้อธิบายอาชญากรรมไร้ตัวตนในกรอบของสภาพแวดล้อมอันเป็นสาเหตุหลักของอาชญากรรมประเภทนี้ โดยวรรณกรรมหลายเรื่อง อธิบายลักษณะของโลกไซเบอร์ว่าเป็นสภาพแวดล้อมนิรนาม (Anonymous nature of cyberspace) ซึ่งอาจถูกนำไปใช้ประกอบอาชญากรรมได้หลายรูปแบบ[11] สำหรับสภาพแวดล้อมที่สำคัญประการหนึ่งในการประกอบอาชญากรรมแบบไร้ตัวตนคือ เครือข่ายการสื่อสาร (Network)

---

[9] Zheng, R., Qin, Y., Huang, Z., & Chen, H. (2003, June). Authorship analysis in cybercrime investigation. In International conference on intelligence and security informatics (pp. 59-73). Springer, Berlin, Heidelberg.

[10] Nirkhi, S. M., Dharaskar, R. V., & Thakre, V. M. (2012, June). Analysis of online messages for identity tracing in cybercrime investigation. In Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec) (pp. 300-305). IEEE.

[11] Iqbal, F., Binsalleeh, H., Fung, B. C., & Debbabi, M. (2013). A unified data mining solution for authorship analysis in anonymous textual communications. Information Sciences, 231, 98-112.

โดยเฉพาะในการใช้เครือข่ายการสื่อสารบางชนิด ทำให้การส่งข้อมูลและการสื่อสารมีลักษณะของความนิรนามโดยสภาพ เช่น เครือข่าย Tor[12] นักวิชาการหลายท่านชี้ให้เห็นว่า การใช้งานเทคโนโลยีสารสนเทศที่มีคุณลักษณะนิรนาม เช่น เครือข่ายการสื่อสารแบบนิรนามนั้น ไม่จัดเป็นปัญหาโดยตัวเอง แต่ปัญหาเกิดจากอาชญากรรมไซเบอร์ที่ใช้คุณลักษณะนิรนามของการสื่อสารผ่านเครือข่าวดังกล่าวโดยมิชอบ (Abuse) [13]

จากการพิจารณาแนวทางนี้สามารถอธิบายได้ว่า *อาชญากรรมไร้ตัวตนอาศัยสภาพแวดล้อมทางไซเบอร์อันมีลักษณะนิรนามโดยสภาพ และใช้เทคโนโลยีหรือวิธีการสื่อสารที่ไม่ระบุตัวโดยมิชอบ เพื่อการก่ออาชญากรรม*

3.3 แนวทางการอธิบายอาชญากรรมไร้ตัวตน ในฐานะของอาชญากรรมประเภท “การโจรกรรมข้อมูลเอกลักษณ์” (Identify theft)

แม้ว่าในทางวิชาการยังไม่มีนิยามเฉพาะสำหรับ อาชญากรรมไร้ตัวตน (Anonymous crime) และยังไม่ปรากฏฐานความผิดเฉพาะสำหรับอาชญากรรมไร้ตัวตนในกฎหมายต่างประเทศ แต่มีวรรณกรรมหลายเรื่องที่ศึกษาเกี่ยวกับอาชญากรรมประเภทการโจรกรรมข้อมูลเอกลักษณ์หรืออัตลักษณ์ (Identity theft) รวมทั้งมีกฎหมายต่างประเทศบางประเทศระบุฐานความผิดสำหรับการโจรกรรมข้อมูลอัตลักษณ์ไว้โดยเฉพาะ ซึ่งโดยทั่วไปในทางวิชาการมีการให้ความหมายว่า การประกอบอาชญากรรมโดยใช้ข้อมูลระบุตัวตนของเหยื่อไปใช้เพื่อปกปิดตัวตนของตนในการกระทำผิดต่างๆ ทางออนไลน์[14] ในระดับองค์การระหว่างประเทศมีการระบุความหมายไว้ เช่น องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (Organization for Economic Co-operation and Development หรือ OECD) ให้ความหมายของอาชญากรรมประเภทโจรกรรมข้อมูลอัตลักษณ์ว่า “กิจกรรม

---

[12] Lin, Z., Tong, L., Zhijie, M., & Zhen, L. (2017, October). Research on cyber crime threats and countermeasures about tor anonymous network based on meek confusion plug-in. In 2017 International Conference on Robots & Intelligent System (ICRIS) (pp. 246-249). IEEE.

[13] Fu, X., Ling, Z., Yu, W., & Luo, J. (2010, June). Cyber Crime Scene Investigations (C²SI) through Cloud Computing. In 2010 IEEE 30th International Conference on Distributed Computing Systems Workshops (pp. 26-31). IEEE.

[14] Neil Mitchison, Marc Wilikens, Lothar Breitenbach, Robin Urry, and Portesi, Identity Theft – A Discussion Paper (Italy: European Commission, Directorate-General, Joint Research Centre, 2004).

เกี่ยวกับการได้มาและใช้ข้อมูลส่วนบุคคลของบุคคลธรรมดาโดยปราศจากอำนาจ ด้วยเจตนาที่จะประกอบอาชญากรรมอื่น”[15]

จากลักษณะของการโจรกรรมข้อมูลเอกลักษณ์จะพบลักษณะหรือองค์ประกอบสำคัญคือ การกระทำผิดหรืออาชญากรรมที่แยกเป็นสองส่วนได้แก่ ส่วนการกระทำกับข้อมูลระบุตัวผู้อื่น และ ส่วนการกระทำผิดที่เป็นเป้าหมาย ซึ่งกรอบแนวคิดนี้จะนำไปวิเคราะห์จำแนกรูปแบบของอาชญากรรมแบบไร้ตัวตนในหัวข้อ 9.1

อย่างไรก็ตาม อาชญากรรมแบบไร้ตัวตนมีความหมายกว้างกว่าการโจรกรรมข้อมูลอัตลักษณ์ เนื่องจากการปกปิดตัวตนอาจใช้วิธีการอื่นนอกเหนือจากการใช้หรืออ้างข้อมูลระบุตัวของผู้อื่นก็ได้ ดังจะกล่าวต่อไปในหัวข้อเกี่ยวกับวิธีการ

3.4 แนวทางการพิจารณาอาชญากรรมแบบไร้ตัวตนในแง่อุปสงค์และอุปทานของตลาดมืด

งานวิชาการหลายเรื่อง อธิบายอาชญากรรมแบบไร้ตัวตน ภายใต้กรอบทฤษฎีใหม่ที่มีการเสนอขึ้น เช่น แนวคิดเกี่ยวกับการทำตลาดของอาชญากรรมไซเบอร์ (Commoditization of cybercrime)[16] กล่าวคือ ในสภาพแวดล้อมของตลาดมืดทางไซเบอร์ (Underground market) อาชญากรรมไซเบอร์เป็นสินค้าชนิดหนึ่งอันเป็นอุปทานหรือผู้ให้บริการ (Vendor)[17] โดยผู้ประสงค์ใช้บริการหรือฝ่ายอุปสงค์เป็นผู้ติดต่อเลือกบริการในสภาวะตลาดแบบนี้จะเกิดขึ้นและดำรงอยู่ได้ด้วยปัจจัยสำคัญคือความไร้ตัวตนหรือนิรนามของทั้งฝ่ายอุปสงค์และอุปทาน งานวิชาการบางเรื่องแบ่งช่วงระยะเวลาของตลาดอาชญากรรมไซเบอร์ที่อยู่ในสภาพแวดล้อมนิรนามหรือไร้ตัวตนเป็นสามช่วงโดยอาศัยปัจจัยหลักคือ การใช้จ่ายเงินอิเล็กทรอนิกส์ กล่าวคือ ช่วงเริ่มต้น ช่วงคงตัว (Stable) ซึ่งเริ่ม

---

[15] Organization for Economic Co-operation and Development (OECD), OECD Policy Guidance on Online Identity Theft [Online]. 2008. Available from: http://www.oecd.org/dataoecd/49/39/40879136.pdf [21 November 2018]

[16] Van Wegberg, R., Tajalizadehkhoob, S., Soska, K., Akyazi, U., Ganan, C. H., Klievink, B., ... & Van Eeten, M. (2018). Plug and prey? measuring the commoditization of cybercrime via online anonymous markets. In 27th USENIX security symposium (USENIX security 18) (pp. 1009-1026).

[17] Van Wegberg, R., Miedema, F., Akyazi, U., Noroozian, A., Klievink, B., & van Eeten, M. (2020, April). Go see a specialist? predicting cybercrime sales on online anonymous markets from vendor and product characteristics. In Proceedings of The Web Conference 2020 (pp. 816-826).

มีแนวโน้มคงที่ และช่วงหลังการระบาดของโรคติดต่อโควิด 19 ซึ่งมีการขยายตัวของการใช้จ่ายทางอิเล็กทรอนิกส์ ส่งผลให้อุปสงค์ของอาชญากรรมไซเบอร์แบบไร้ตัวตนสูงขึ้นอีก [18]

จากการพิจารณาแนวทางนี้สามารถอธิบายได้ว่า *อาชญากรรมไร้ตัวตนเป็นส่วนหนึ่งของระบบตลาดในฐานะเป็นบริการหนึ่งซึ่งมีอุปสงค์เปลี่ยนแปลงไปตามการขยายตัวของการทำธุรกรรมออนไลน์* อย่างไรก็ตาม ตลาดและบริการลักษณะนี้ไม่มีกฎหมายรองรับ

จะเห็นได้ว่า ในปัจจุบันยังไม่มีการนิยามความหมายอันเป็นที่ยอมรับทั่วไปหรือความหมายอันเป็นมาตรฐานเดียวกันของอาชญากรรมไร้ตัวตน (Anonymous crime) แต่จากวรรณกรรมที่อธิบายอาชญากรรมไร้ตัวตนในมุมมองต่างๆ สรุปได้ว่า *“อาชญากรรมไร้ตัวตนเป็นรูปแบบหนึ่งของอาชญากรรมคอมพิวเตอร์ ที่อาศัยประโยชน์จากสภาพแวดล้อมทางไซเบอร์โดยใช้ข้อมูลระบุตัวบุคคลอื่นโดยมิชอบหรือใช้วิธีการอื่นใดเพื่อปกปิดตัวตนหรือเพื่อไม่ให้ถูกระบุตัวตนในการก่ออาชญากรรมใดๆ ที่กระทบต่อความปลอดภัยทางคอมพิวเตอร์”*

4. อาชญากรรมคอมพิวเตอร์กับอาชญากรรมแบบไร้ตัวตน

แม้ว่ามีงานวิชาการที่กล่าวถึงอาชญากรรมแบบไร้ตัวตนในมุมมองต่างๆ ดังกล่าวมาแล้ว แต่ยังไม่มีนิยามเฉพาะของอาชญากรรมไร้ตัวตน อย่างไรก็ตาม อาชญากรรมแบบไร้ตัวตนเป็นการกระทำทางคอมพิวเตอร์ จึงวิเคราะห์เทียบเคียงกับความหมายของอาชญากรรมไซเบอร์หรืออาชญากรรมคอมพิวเตอร์ ซึ่งพบว่านิยามทางวิชาการของอาชญากรรมคอมพิวเตอร์ (Computer crime) หรืออาชญากรรมไซเบอร์ (Cybercrime) ก็มีความหลากหลาย ภายใต้กรอบและแนวทางพิจารณาที่แตกต่างกันไป โดยยังไม่มีนิยามแน่นอนชัดเจนอันใดอันหนึ่งเป็นที่ยอมรับทั่วไป[19] หากพิจารณาในระดับระหว่างประเทศ พบว่า ข้อมติ 45/121 และคู่มือการป้องกันและควบคุมอาชญากรรมเกี่ยวกับคอมพิวเตอร์ของสหประชาชาติ (UN Manual on the Prevention and Control of Computer-Related Crime)[20] ก็ชี้ให้เห็นว่า ยังไม่มีนิยามของอาชญากรรมคอมพิวเตอร์อันเป็นที่ยอมรับอย่างเป็นสากล ตัวอย่างความหมายหรือนิยามของอาชญากรรมคอมพิวเตอร์ในทางวิชาการ เช่น

---

[18] Vu, A. V., Hughes, J., Pete, I., Collier, B., Chua, Y. T., Shumailov, I., & Hutchings, A. (2020, October). Turning up the dial: the evolution of a cybercrime market through set-up, stable, and covid-19 eras. In Proceedings of the ACM Internet Measurement Conference (pp. 551-566).

[19] คณาธิป ทองรวีวงศ์ , ความผิดเกี่ยวกับคอมพิวเตอร์ เล่ม 1 : ความผิดต่อความปลอดภัยของระบบและข้อมูลคอมพิวเตอร์ , กรุงเทพ: สำนักพิมพ์นิติธรรม , พิมพ์ครั้งที่ 2 , 2565.

[20] United Nations, United Nations Manual on the Prevention and Control of Computer-Related Crime: International review of criminal policy (New York: United Nations, 1994), p. 7.

- การประกอบอาชญากรรมที่เกี่ยวข้องกับโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศ ซึ่งรวมถึงการเข้าถึงโดยปราศจากอำนาจ การกระทำอันส่งผลกระทบต่อข้อมูล เช่น ทำลาย ลบ แก้ไข การกระทำอันส่งผลกระทบ รบกวน หรือแทรกแซงการทำงานของระบบคอมพิวเตอร์ [21]

- การกระทำโดยใช้อุปกรณ์อิเล็กทรอนิกส์ซึ่งสามารถประมวลผลได้โดยอัตโนมัติ อันเป็นการฝ่าฝืนกฎหมาย[22]

- การกระทำโดยใช้คอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์เป็นวิธีการหลัก ในการกระทำความผิดกฎหมาย”[23]

- การใช้คอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์เป็นเครื่องมือ หรือตกเป็นเป้าหมายของการประกอบอาชญากรรม”[24]

- การประกอบอาชญากรรมในพื้นที่เสมือน (Virtual space)[25]

- ข้อมติเกี่ยวกับการต่อต้านอาชญากรรมทางเทคโนโลยีสารสนเทศของสหประชาชาติ (Resolution 55/63)[26] ไม่ได้นิยามอาชญากรรมคอมพิวเตอร์ แต่เรียกว่า “อาชญากรรมเกี่ยวกับการใช้เทคโนโลยีสารสนเทศโดยมิชอบ”

แม้ว่านิยามความหมายข้างต้นมีความแตกต่างหลากหลายและการกำหนดความผิดสำหรับอาชญากรรมคอมพิวเตอร์มีฐานความผิดแตกต่างกันไปในแต่ละประเทศ แต่มีปัจจัยหรือองค์ประกอบร่วม ซึ่งทำให้สามารถสรุป

---

[21] Paul Taylor, Hackers: Crime in the Digital Sublime (Routledge, 1999), p. 200.

[22] Anthony Reyes, Kevin O'Shea, Jim Steele, Jon R. Hansen, Benjamin R. Jean, and Thomas Ralph, Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement and Prosecutors (Elsevier, 2007), p. 33.

[23] Nir Kshetri, “Positive Externality, Increasing Returns, and the Rise in Cybercrimes,” Communications of the ACM 52,12 (2009):141-144.

[24] David L. Carter, “Computer Crime Categories: How Techno-Criminals Operate,” FBI Law Enforcement Bulletin 64,7 (1995): 21-26.

[25] Azeez Nureni Ayofe and Osunade Oluwaseyifunmitan, “Approach To Solving Cybercrime And Cybersecurity,” International Journal of Computer Science and Information Security 3,1 (2009): 1-11.

[26] United Nations General Assembly, Combating the Criminal Misuse of Information Technologies (Resolution 55/63) [Online]. 2000. Available from: http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf [21 November 2018]

ได้ว่า อาชญากรรมคอมพิวเตอร์เป็นการกระทำที่เกิดขึ้นในสภาพแวดล้อมทางไซเบอร์หรือเครือข่ายคอมพิวเตอร์ อันเป็นการกระทำโดยปราศจากอำนาจและกฎหมายกำหนดเป็นความผิด

เมื่อนำความหมายและลักษณะทั่วไปของอาชญากรรมไร้ตัวตนมาเปรียบเทียบกับความหมายของอาชญากรรมคอมพิวเตอร์ จะเห็นได้ว่า อาชญากรรมไร้ตัวตนจัดเป็นส่วนหนึ่งของอาชญากรรมไซเบอร์หรืออาชญากรรมคอมพิวเตอร์ โดยมีองค์ประกอบหรือลักษณะพิเศษเพิ่มเติมขึ้นมาคือ การนำข้อมูลบุคคลอื่นมาใช้ระบุตัวหรือการใช้วิธีการต่างๆ ในการปกปิดตัวตนของผู้กระทำหรือกล่าวอีกนัยหนึ่งคือ อาชญากรรมคอมพิวเตอร์มีขอบเขตความหมายกว้างกว่าและครอบคลุมอาชญากรรมไม่ว่าจะใช้วิธีการปกปิดตัวตนหรือไม่ก็ตาม

นอกจากนี้ จากการพิจารณาลักษณะทั่วไปของอาชญากรรมไร้ตัวตน โดยเฉพาะในกรณีที่ใช้วิธีการนำข้อมูลระบุตัวผู้อื่นมาใช้ปกปิดตัวตน จะพบว่ามีความเกี่ยวข้องกับการกระทำสองส่วนคือการโจรกรรมข้อมูลบุคคลอื่นซึ่งอาจเป็นความผิดในตัวเอง และการประกอบอาชญากรรมอื่นใดโดยอาศัยข้อมูลระบุตัวผู้อื่นหากใช้กรอบความหมายของอาชญากรรมคอมพิวเตอร์มาวิเคราะห์จะพบว่า การกระทำทั้งสองส่วนอาจมีลักษณะเป็นอาชญากรรมคอมพิวเตอร์ได้ เช่น การเข้าถึงบัญชีการใช้งานจดหมายอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบและใช้งานบัญชีดังกล่าวในการส่งมัลแวร์เพื่อโจมตีบุคคลอื่นอีกคนหนึ่ง จะเห็นได้ว่าการกระทำทั้งสองส่วนจัดเป็นอาชญากรรมคอมพิวเตอร์ได้

5. อาชญากรรมแบบไร้ตัวตนกับอาชญากรรมที่กระทำทางกายภาพ

การใช้วิธีการปกปิดตัวตนที่ใช้เทคนิควิธีการทางคอมพิวเตอร์ต่างๆ ของอาชญากรดังกล่าวมาแล้ว เช่น การเข้ารหัสการสื่อสาร การนำข้อมูลบุคคลอื่นมาใช้กระทำผิด ฯลฯ ไม่จำกัดว่าจะต้องเป็นกรณีที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ ทั้งนี้เพราะอาชญากรที่เกี่ยวข้องกับฐานความผิดอื่นที่กระทำทางกายภาพก็มีการนำเทคนิควิธีการต่างๆ เพื่อปกปิดตัวตนหรือทำให้ไร้ตัวตนมาใช้เพื่อหลบเลี่ยงจากการสืบสวนสอบสวนได้ด้วยเช่นกัน เช่น องค์กรอาชญากรรมค้ามนุษย์ทำการสื่อสารวางแผนกันทางระบบคอมพิวเตอร์โดยใช้วิธีการปกปิดตัวตน ดังนั้น เมื่อนำกรอบแนวคิดเกี่ยวกับความมั่นคงปลอดภัยทางคอมพิวเตอร์มาพิจารณาประกอบกับลักษณะของอาชญากรรมไร้ตัวตนที่จำแนกเป็นกระทำสองส่วนคือ การกระทำเพื่อปกปิดตัวตนและการกระทำอาชญากรรมอื่นที่เป็นวัตถุประสงค์หลัก จะสามารถจำแนกความสัมพันธ์ระหว่างอาชญากรรมและวิธีการปกปิดตัวตนได้ 2 รูปแบบ คือ

1. การกระทำอันเป็นหลักของอาชญากรรมส่งผลต่อความปลอดภัยทางคอมพิวเตอร์และใช้วิธีการปกปิดตัวตนที่ส่งผลกระทบต่อความปลอดภัยทางคอมพิวเตอร์

ตัวอย่าง อาชญากรรมโจรกรรมข้อมูลคอมพิวเตอร์ ซึ่งใช้วิธีการเข้ารหัสข้อมูลการสื่อสารและข้อมูลที่เกี่ยวข้องเพื่อไม่ให้สามารถระบุตัวผู้กระทำได้

ตัวอย่าง อาชญากรรมเข้าถึงและควบคุมบัญชีสื่อสังคมออนไลน์ของเหยื่อและใช้บัญชีดังกล่าวกระจายมัลแวร์ต่อไป จะเห็นได้ว่า วิธีการปกปิดตัวตนคือการโจรกรรมข้อมูลบุคคลอื่นซึ่งส่งผลกระทบต่อความปลอดภัยในแง่ความลับหรือการเข้าถึงโดยปราศจากอำนาจและการกระทำหลักคือการแพร่มัลแวร์ซึ่งกระทบต่อความปลอดภัย เนื่องจากเป็นการแก้ไขข้อมูลผู้อื่น

2. การกระทำอันเป็นหลักของอาชญากรรมไม่ส่งผลต่อความปลอดภัยทางคอมพิวเตอร์ แต่ใช้วิธีการปกปิดตัวตนที่ส่งผลกระทบต่อความปลอดภัยทางคอมพิวเตอร์

ตัวอย่าง[27] องค์กรอาชญากรรมยาเสพติด ในสหรัฐอเมริกา (Drug cartel) มีการนำวิธีการปกปิดตัวตนมาใช้หลายรูปแบบ เช่น การเข้ารหัสอุปกรณ์และข้อมูลการสื่อสาร (Communication encryption) เพื่อปกปิดเนื้อหาข้อมูล หมายเลขโทรศัพท์ อุปกรณ์ที่ใช้สื่อสาร การเข้ารหัสการสื่อสารทางวีดีโอคอลเพื่อปกปิดข้อมูลระบุตัวผู้สื่อสาร

ตัวอย่าง[28] อาชญากรทำการซื้อขายสื่อลามกเด็กออนไลน์ โดยใช้วิธีเข้ารหัสไดรฟ์เพื่อป้องกันการสืบสวนสอบสวนของเจ้าหน้าที่

จากตัวอย่างจะเห็นได้ว่า การกระทำหลักของอาชญากรรมคือการกระทำผิดกฎหมายยาเสพติดและกฎหมายสื่อลามกเด็ก ซึ่งไม่ใช่อาชญากรรมที่กระทบต่อความปลอดภัยของระบบและข้อมูลคอมพิวเตอร์ แต่มีการนำวิธีการทางคอมพิวเตอร์ เช่น การเข้ารหัสข้อมูล (Encryption) มาใช้เพื่อปกปิดตัวตน

สำหรับการศึกษาวิจัยนี้จะศึกษาเฉพาะในส่วนของอาชญากรรมแบบไร้ตัวตนที่การกระทำหลักหรือเป้าหมายหลักของอาชญากรรมส่งผลกระทบต่อความปลอดภัยทางคอมพิวเตอร์

---

[27] Grabosky, P. N. and Smith, R. G. (1998) Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities, Transaction Publishers.

[28] David Kravets, Feds Crack Encrypted Drives, Arrest Child Porn Suspect, Weird, 14 August 2013, https://www.wired.com/2013/08/feds-crack-encrypted-drives/

6. แนวคิดทฤษฎีวิเคราะห์คุณลักษณะของตัวอาชญากรที่กระทำผิดแบบไร้ตัวตน

เนื่องจากความผิดเกี่ยวกับคอมพิวเตอร์ตามกฎหมายของประเทศต่างๆ มีความหลากหลายและอาชญากรผู้กระทำความผิดแต่ละฐานจะมีคุณลักษณะที่แตกต่างกัน ในภาพรวมมีงานวิชาการที่จำแนกอาชญากรตามคุณสมบัติด้านทักษะหรือความสามารถไว้หลายประเภทโดยมีชื่อเรียกแตกต่างกัน แต่สามารถจำแนกเป็น 2 กลุ่ม คือ

1. กลุ่มอาชญากรมือใหม่ที่มีทักษะจำกัด ซึ่งนักวิชาการเรียกชื่อแตกต่างกันไป เช่น เด็กใหม่ (Newbie หรือ Tool kit)[29] ผู้อยากรู้ที่มีความสามารถทางเทคนิคต่ำ (The merely curious with low technical competence)[30] มือใหม่ (Novices)[31] ผู้มุ่งหวัง (Wannabe lamer)[32] อาชญากรกลุ่มนี้นอกจากไม่มีทักษะในการใช้วิธีการทางเทคนิคเพื่อปกปิดหรือปลอมตัว ยังอาจไม่สามารถกระทำความผิดทางคอมพิวเตอร์ในกลุ่มที่กระทบต่อความปลอดภัยของระบบหรือข้อมูลคอมพิวเตอร์ โดยทั่วไปอาชญากรที่มีทักษะในกลุ่มนี้อาจทำความผิดเกี่ยวกับคอมพิวเตอร์ในฐานที่เกี่ยวกับเนื้อหา (Content) เช่น การโพสต์แชร์ข้อมูลผิดกฎหมายของประเทศนั้นๆ

2. กลุ่มอาชญากรที่มีทักษะในการใช้อุปกรณ์เครื่องมือ ชุดคำสั่ง ในการกระทำที่ส่งผลกระทบต่อความมั่นคงปลอดภัยทางคอมพิวเตอร์ โดยนักวิชาการเรียกชื่อแตกต่างกันไป เช่น ผู้กระทำมืออาชีพ (Professional hacker)[33] แฮกเกอร์ผู้มีความสามารถทางเทคนิคสูง (The determined hacker with high technical competence)[34] ไซเบอร์พังค์ (Cyber-punks Coders)[35] อาชญากรที่มีทักษะในกลุ่มนี้ สามารถใช้วิธีการทางเทคนิคในการทำให้เกิดความเป็นนิรนามเพื่อปกปิดตัวตนในการกระทำ

---

[29] Marc Rogers, Psychology of Hackers: Steps Toward a New Taxonomy (1999), cited in John Van Beveren, "A Conceptual Model of Hacker Development and Motivations," Journal of E-Business 1,2 (December 2001).

[30] Ed Tiley, Personal Computer Security (California: IDG Books Worldwide, Inc., 1996), p. 49.

[31] Carol Meyers, Sara Powers, and Daniel Faissol, Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches (Lawrence Livermore National Laboratory, 2009).

[32] Raoul Chiesa, Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking, 1st ed. (Auerbach Publications, 2008), pp. 52-56.

[33] Marc Rogers, Psychology of Hackers: Steps Toward a New Taxonomy (1999), cited in John Van Beveren, "A Conceptual Model of Hacker Development and Motivations," Journal of E-Business 1,2 (December 2001).

[34] Ed Tiley, Personal Computer Security (California: IDG Books Worldwide, Inc., 1996), p. 49.

[35] Carol Meyers, Sara Powers, and Daniel Faissol, Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches (Lawrence Livermore National Laboratory, 2009).

จากกรอบแนวคิดดังกล่าวจะพบว่า อาชญากรรมแบบไร้ตัวตนที่กระทำการต่อระบบหรือข้อมูลคอมพิวเตอร์ มักอยู่ในกลุ่มที่ 2 เนื่องจากการโจมตีระบบหรือข้อมูลจำต้องอาศัยทักษะทางด้านเทคโนโลยีสารสนเทศ เช่น การเขียนและใช้ชุดคำสั่งต่าง ๆ กรอบแนวคิดทฤษฎีนี้มีนัยสำคัญทางวิชาการในการจำแนกประเภทผู้กระทำความผิดแบบไร้ตัวตน แต่ไม่ได้มีนัยสำคัญในการกำหนดองค์ประกอบความผิดของกฎหมาย เนื่องจากกฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ของต่างประเทศไม่ได้กำหนดองค์ประกอบเกี่ยวกับทักษะของผู้กระทำ เช่น อนุสัญญาอาชญากรรมไซเบอร์ฯ ไม่ได้กำหนดองค์ประกอบความผิดโดยอาศัยปัจจัยความสามารถหรือทักษะของผู้กระทำ อย่างไรก็ตาม กรอบแนวคิดทฤษฎีนี้นำไปสู่การวิเคราะห์ตัวแบบกฎหมายสำหรับอาชญากรรมไร้ตัวตนซึ่งไม่จำต้องกำหนดองค์ประกอบเกี่ยวกับทักษะทางเทคนิคของผู้กระทำ

7. แนวคิดทฤษฎีเกี่ยวกับการวิเคราะห์ความสัมพันธ์ของอาชญากรที่กระทำการแบบนิรนามกับเหยื่อ

เนื่องจากอาชญากรผู้กระทำความผิดโดยใช้วิธีปกปิดตัวตนหรือนิรนาม อาจมีความสัมพันธ์กับเหยื่อหรือเป้าหมายของการโจมตีที่แตกต่างกัน โดยจำแนกได้ 2 กลุ่มคือ

- อาชญากรรมนิรนามที่มีความสัมพันธ์ทางนิติกรรมหรือสัญญาชนิดใดชนิดหนึ่งกับเหยื่อ เช่น อาชญากรเป็นบุคคลากรในองค์กรของเหยื่อ (Insider) เช่น ลูกจ้าง ผู้ดูแลระบบ[36] โดยการกระทำที่ส่งผลกระทบต่อความปลอดภัยทางคอมพิวเตอร์ที่เกิดขึ้นนั้นอาจทำไปเพื่อแสวงประโยชน์หรืออาจเกิดจากแรงจูงใจส่วนตัว เช่น การโจมตีระบบเพราะปัญหาด้านความสัมพันธ์กับนายจ้าง โดยลักษณะของความสัมพันธ์แล้ว อาชญากรกลุ่มนี้จึงมักใช้วิธีการเพื่อปกปิดตัวตนหรือทำให้เกิดความนิรนามเพื่อไม่ให้บ่งระบุตัวผู้กระทำได้

- อาชญากรรมนิรนามที่ไม่มีความสัมพันธ์ทางนิติกรรมหรือสัญญาชนิดใดชนิดหนึ่งกับเหยื่อ กล่าวคือเป็นบุคคลภายนอก (Outsider)[37] เช่น แฮกเกอร์ทั่วไปที่ไม่มีความเกี่ยวข้องกับองค์กร

สำหรับในส่วนของอาชญากรรมนิรนามที่ดำเนินการในรูปแบบองค์กรอาชญากรรมนั้น อาจจัดอยู่ในประเภทที่ไม่มีความสัมพันธ์กับเหยื่อ เนื่องจากโดยทั่วไปเป็นบุคคลภายนอก อย่างไรก็ตาม งานวิชาการบางชิ้นจัดอาชญากรรมนิรนามที่เกิดจากองค์กรอาชญากรรมแยกเป็นอีกประเภทหนึ่ง เช่น สำนักงานสอบสวนกลางของ

---

[36] Eileen Kowalski, Dawn Cappelli, and Andrew Moore, Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector Pittsburgh (Pittsburgh: Carnegie Mellon, Software Engineering Institute, 2008).

[37] Deborah Russell and G.T. Gangemi, Computer Security Basics (California: O'Reilly & Associates Inc., 1991), pp. 14-15.

สหรัฐอเมริกา (Federal Bureau of Investigation หรือ FBI) จัดกลุ่มอาชญากรรมคอมพิวเตอร์ประเภทที่สอง (Classification 2)[38] ว่ามี 3 ประเภทคือ การกระทำของลูกจ้างหรือคนภายใน การกระทำของบุคคลภายนอก การกระทำขององค์กรอาชญากรรม

จะเห็นได้ว่า กรอบแนวคิดทฤษฎีในการวิเคราะห์อาชญากรนิรนามตามลักษณะความสัมพันธ์กับเหยื่อนั้น ไม่ได้พิจารณาจากแรงจูงใจหรือวัตถุประสงค์ แต่มุ่งเน้นที่ความสัมพันธ์ระหว่างเหยื่อกับอาชญากร ซึ่งมีความสำคัญในแง่โอกาสในการก่ออาชญากรรม แต่ไม่ได้มีนัยสำคัญในการกำหนดองค์ประกอบความผิดของกฎหมาย เช่น อนุสัญญาอาชญากรรมไซเบอร์ไม่ได้กำหนดองค์ประกอบความผิดโดยอาศัยปัจจัยความสัมพันธ์ระหว่างอาชญากรไซเบอร์กับเหยื่อ กรอบแนวคิดทฤษฎีนี้นำไปสู่การวิเคราะห์ตัวแบบกฎหมายสำหรับอาชญากรรมไร้ตัวตนซึ่งไม่จำต้องกำหนดองค์ประกอบเกี่ยวกับความสัมพันธ์ระหว่างผู้กระทำและเหยื่อ

8. แนวคิดทฤษฎีเกี่ยวกับการวิเคราะห์มูลเหตุจูงใจหรือวัตถุประสงค์ในการประกอบอาชญากรรมของอาชญากรแบบไร้ตัวตน

อาชญากรรมทางคอมพิวเตอร์ที่ใช้วิธีการปกปิดตัวตน อาจมีวัตถุประสงค์หรือมูลเหตุชักจูงใจในการกระทำที่แตกต่างกัน[39] เช่น เพื่อแสวงประโยชน์โดยมิชอบ เพื่อความอยากรู้อยากเห็นหรือความท้าทาย เพื่อวัตถุประสงค์ทางการเมืองหรือทางธุรกิจ ฯลฯ หัวข้อนี้จึงศึกษาแนวคิดทฤษฎีเพื่อนำไปสู่การวิเคราะห์จัดทำกฎหมายต้นแบบอาชญากรรมนิรนามในส่วนของเจตนาพิเศษหรือมูลเหตุชักจูงใจ ซึ่งจำแนกได้เป็น 5 กลุ่มคือ

1. อาชญากรรมแบบไร้ตัวตนที่มีมูลเหตุจูงใจเกี่ยวกับการทดสอบหรือปรับปรุงระบบ กล่าวคือ กระทำการโดยส่งผลกระทบต่อระบบหรือข้อมูลคอมพิวเตอร์แต่ไม่มีวัตถุประสงค์ในการแสวงประโยชน์ทางทรัพย์สินหรือประโยชน์ทางธุรกิจ โดยในทางวิชาการมีการใช้คำเรียกว่า *“Hacker” และ “Cracker”* ในความหมายว่า ผู้เจาะระบบหรือกระทบต่อความปลอดภัยทางคอมพิวเตอร์ด้วยแรงจูงทางเทคนิคในการปรับปรุง

[38] Hossein Bidgoli, The Internet Encyclopedia (John Wiley & Sons, 2004), p. 327.

[39] Steven M. Furnell, “The Problem of Categorising Cybercrime and Cybercriminals,” Paper presented at the 2nd Australian Information Warfare and Security Conference, Perth, Australia, 2001.

พัฒนาระบบ เช่น เพื่อหาจุดอ่อน[40] การแจ้งเตือนให้ผู้ดูและหรือเจ้าของระบบทราบถึงช่องโหว่หรือปัญหาของระบบ[41] งานวิชาการหลายเรื่องเรียกผู้กระทำในกลุ่มนี้ว่า “White hat”[42]

2. อาชญากรรมแบบไร้ตัวตนที่มีมูลเหตุจูงใจเพื่อการทำอันตรายต่อระบบหรือข้อมูลคอมพิวเตอร์ โดยบางท่านเรียกว่า “Cracker”[43] สำหรับวัตถุประสงค์ของการทำอันตรายต่อระบบหรือข้อมูลนั้นอาจจำแนกย่อยได้อีกหลายประการ เช่น แสวงประโยชน์ทางทรัพย์สิน หรืออาจเป็นการตอบสนองความท้าทายโดยไม่ได้แสวงประโยชน์ หรือ อาจเป็นการกระทำเป็นกลุ่มหรือองค์กรอาชญากรรมก็ได้ งานวิชาการหลายเรื่องเรียกอาชญากรรมกลุ่มนี้ว่า *“Black hat”* [44] สำหรับอาชญากรรมแบบไร้ตัวตนที่กระทำในลักษณะองค์กรอาชญากรรมนั้น โดยทั่วไปจัดอยู่ในกลุ่มประเภทที่สอง

3. อาชญากรรมแบบไร้ตัวตนที่มีมูลเหตุจูงใจแบบผสมระหว่างการแสวงประโยชน์และการปรับปรุงพัฒนาระบบ เช่น การทดสอบหาจุดอ่อนในระบบป้องกันความปลอดภัยขององค์กรและเมื่อพบแล้วจะแจ้งให้ผู้ดูแลระบบทราบเพื่อเรียกค่าตอบแทนทางทรัพย์สิน ในทางวิชาการมีการเรียกชื่อกลุ่มนี้ว่า “Grey Hat” ในแง่ของการกระทำเชิงการรวมกลุ่มหรือองค์กร โดยทั่วไปผู้กระทำการกลุ่มนี้ไม่สังกัดองค์กรแต่กระทำโดยอิสระ[45]

4.อาชญากรรมแบบไร้ตัวตนที่มีมูลเหตุจูงใจทางสังคม มีการศึกษาในต่างประเทศพบว่า กิจกรรมหรือการกระทำทางอินเทอร์เน็ตโดยใช้วิธีการเพื่อปกปิดตัวตนหรือนิรนาม (Anonymous activities) อาจถูกนำมาใช้เพื่อตอบโต้แก้แค้นระหว่างฝ่ายที่มีข้อพิพาทหรือนำมาใช้เพื่อลงโทษกันเองทางสื่อออนไลน์โดยไม่ใช้กระบวนการทางกฎหมาย (Internet vigilantism) [46]

---

[40] Michael T. Simpson, Hands on ethical hacking and network defense (Thomson Course Technology, 2006), pp. 25-27.

[41] Gráinne Kirwan and Andrew Power, Cybercrime: The Psychology of Online Offenders (Cambridge University Press, 2013), p. 54.

[42] Marcus K. Rogers, “A Two-dimensional Circumplex approach to the Development of a Hacker Taxonomy,” Digital Investigation 3,2 (2006): 97-102.

[43] Michael T. Simpson, Hands on ethical hacking and network defense (Thomson Course Technology, 2006), pp. 25-27.

[44] Gráinne Kirwan and Andrew Power, Cybercrime: The Psychology of Online Offenders (Cambridge University Press, 2013), p. 54.

[45] Carol Meyers, Sara Powers, and Daniel Faissol, Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches (Lawrence Livermore National Laboratory, 2009).

[46] O'Malley, G. (2013). Hacktivism: cyber activism or cyber crime. Trinity CL Rev., 16, 137.

5. อาชญากรรมแบบไร้ตัวตนที่มีวัตถุประสงค์ทางการเมือง หรือการก่อการร้ายไซเบอร์ (Cyber-terrorist) ซึ่งอาจมีทั้งกรณีที่แสดงหรือเปิดเผยตัวตนให้ปรากฏจากผลของการกระทำเพื่อผลทางการเมืองหรือการเรียกร้อง แต่ในบางกรณีอาจมีการใช้วิธีการปกปิดตัวตน ซึ่งเมื่อพิจารณาจากลักษณะหรือองค์ประกอบภายนอกอาจมีความคล้ายคลึงกับอาชญากรรมไซเบอร์แบบไร้ตัวตนที่กระทำการให้เกิดผลกระทบในวงกว้าง เช่น การโจมตีระบบจ่ายพลังงาน แต่มีความแตกต่างกันที่มูลเหตุจูงใจ จึงจำแนกเป็นอีกประเภทหนึ่ง นอกจากนี้ ยังมีกรณีอาชญากรรมคอมพิวเตอร์โดยผู้กระทำที่เป็นรัฐ (State actors) กล่าวคือ รัฐอาจใช้วิธีการทางเทคโนโลยีเพื่อทำสงครามระหว่างกัน (Cyberwar) หรือ อาจเรียกว่าสงครามข้อมูลสารสนเทศ (Infowar)[47] ซึ่งกรณีนี้จะอยู่ภายใต้กรอบแนวคิดกฎหมายที่แตกต่างออกไปโดยอยู่ในกลุ่มกฎหมายระหว่างประเทศว่าด้วยสงครามไซเบอร์ (Cyber warfare) ซึ่งไม่อยู่ในขอบเขตการวิจัยนี้

จะเห็นได้ว่า กรอบแนวคิดทฤษฎีในการวิเคราะห์อาชญากรนิรนามตามมูลเหตุจูงใจนั้นมีนัยสำคัญในการกำหนดองค์ประกอบความผิดของกฎหมาย โดยกฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ของหลายประเทศกำหนดองค์ประกอบเกี่ยวกับเจตนาพิเศษหรือมูลเหตุจูงใจ สำหรับบางฐานความผิด เช่น อนุสัญญาอาชญากรรมไซเบอร์กำหนดองค์ประกอบความผิดฐานเข้าถึงโดยมิชอบ (Illegal access, Article 2) โดยเปิดโอกาสให้ประเทศภาคีไปกำหนดกฎหมายภายใน โดยคำนึงถึงองค์ประกอบ “เจตนาได้มาซึ่งข้อมูลคอมพิวเตอร์หรือด้วยเจตนาไม่สุจริตอื่น” สำหรับกฎหมายความผิดเกี่ยวกับคอมพิวเตอร์สหรัฐอเมริกาบางฐานมีการระบุองค์ประกอบการเข้าถึงเพื่อแสวงประโยชน์ในทรัพย์สิน (18 U.S.C., Section 1030 (a)(4) อย่างไรก็ตาม กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ของต่างประเทศไม่ได้กำหนดองค์ประกอบที่ยกเว้นความผิดสำหรับการกระทำต่อระบบหรือข้อมูลโดยมีมูลเหตุจูงใจเพื่อการทดสอบระบบดังเช่นพฤติกรรมแบบ “Hacker”

9. รูปแบบของอาชญากรรมแบบไร้ตัวตน

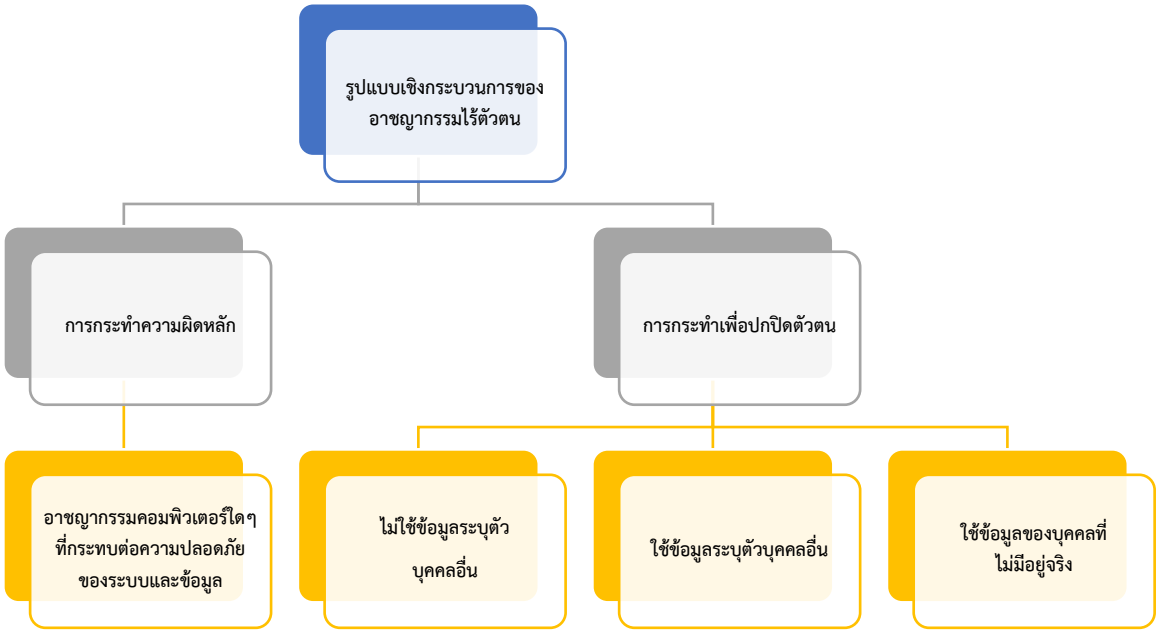
เนื่องจากอาชญากรรมแบบไร้ตัวตนไม่มีนิยามที่ชัดเจนและเป็นที่ยอมรับอย่างเป็นสากล อีกทั้งเมื่อศึกษากฎหมายต่างประเทศพบว่า ไม่ได้ระบุนิยามหรือแยกนิยามโดยเฉพาะออกจากอาชญากรรมคอมพิวเตอร์ งานวิจัยนี้จึงใช้วิธีศึกษาแนวคิดทฤษฎีที่เกี่ยวข้องเพื่อนำมาวิเคราะห์จำแนกรูปแบบหรือลักษณะสำคัญ

[47] Nir Kshetri, “Pattern of global cyber war and crime: A conceptual framework,” Journal of International Management 11,4 (2005): 541-562.

อาชญากรรมประเภทนี้ โดยจำแนกพิจารณารูปแบบในมิติต่างๆ เพื่อนำไปสู่การสังเคราะห์องค์ประกอบของการกระทำออกมาเป็นข้อเสนอในการจัดทำตัวแบบกฎหมายต่อไป

9.1 รูปแบบเชิงกระบวนการของอาชญากรรมแบบไร้ตัวตน

อาชญากรรมคอมพิวเตอร์แบบไร้ตัวตนไม่มีนิยามเฉพาะ โดยมีความหลากหลายในเชิงพฤติกรรม มูลเหตุจูงใจ ลักษณะวิธีการกระทำ นอกจากนั้น ยังอาจประกอบด้วยการกระทำหลายอย่างซึ่งกระทำต่อเนื่องหรือแยกจากกัน จากแนวคิดทฤษฎีเกี่ยวกับความผิดที่กระทบต่อความปลอดภัยของระบบและข้อมูลคอมพิวเตอร์ และการอธิบายความหมายและลักษณะของอาชญากรรมไร้ตัวตน ฯลฯ ดังกล่าวข้างต้น จะนำมาสู่การวิเคราะห์รูปแบบเชิงกระบวนการหรือขั้นตอน (Process, steps) ของอาชญากรรมไร้ตัวตน ซึ่งพบว่าประกอบด้วยกระทำสองส่วน สรุปภาพรวมตามแผนภาพต่อไปนี้และศึกษาวิเคราะห์รายละเอียดในลำดับถัดไป



ภาพรวมรูปแบบเชิงกระบวนการของอาชญากรรมแบบไร้ตัวตน

9.1.1 การกระทำความผิดหลัก

การใช้วิธีการปกปิดตัวตนหรือทำให้เกิดลักษณะนิรนาม ไม่ใช่วัตถุประสงค์หลักหรือเป้าหมายสุดท้าย (Target) ของอาชญากรรมแบบไร้ตัวตน แต่เป็นวิธีการ (Mean) เพื่อมุ่งไปสู่การกระทำอันเป็นหลัก งานวิชาการชี้ให้เห็นว่า อาชญากรรมแบบไร้ตัวตนเกิดจากสภาพแวดล้อม (Nature) ของการสื่อสารข้อมูลทาง

อินเทอร์เน็ตที่มีลักษณะนิรนามโดยสภาพ (Anonymous nature) จึงอาจถูกนำไปใช้ประกอบอาชญากรรมได้หลายรูปแบบ เช่น มัลแวร์ การส่งสแปม[48] ดังนั้น จากการพิจารณาอาชญากรรมคอมพิวเตอร์โดยใช้กรอบแนวคิดด้านความมั่นคงปลอดภัยทางคอมพิวเตอร์ สามารถจำแนกอาชญากรรมอันเป็นเป้าหมายหรือการกระทำหลักได้ 3 กลุ่มคือ

1. อาชญากรรมคอมพิวเตอร์ที่ส่งผลกระทบต่อความปลอดภัยของระบบหรือข้อมูล กล่าวคือ อาชญากรรมที่มีคอมพิวเตอร์เป็นเป้าหมาย (Computer as target) เช่น

การโจมตีในลักษณะของการเข้าถึงระบบที่มีมาตรการป้องกันด้วยวิธีการต่างๆ เช่น การเดารหัสผ่าน (Password guessing attack)

บอทเน็ต (Botnets) เช่น การส่งคำสั่งเพื่อควบคุมเครื่องหรืออุปกรณ์ของเหยื่อให้กระทำการตามคำสั่ง

การโจมตีระบบคอมพิวเตอร์ให้เกิดการปฏิเสธบริการ (Denial-of-Service หรือ DOS)

กาใช้มัลแวร์ (Malicious software) ชนิดต่างๆ

การใช้มัลแวร์เรียกค่าไถ่ (Ransomware)

สแปม (Spam) เช่น การส่งข้อมูลคอมพิวเตอร์ปริมาณมากทำให้เกิดการรบกวนระบบหรือใช้การส่งข้อมูลเป็นพาหะของการแพร่มัลแวร์

2. อาชญากรรมคอมพิวเตอร์ที่โดยหลักแล้วไม่ส่งผลกระทบต่อความปลอดภัยของระบบหรือข้อมูล แต่มีเป้าหมายที่การหลอกลวงบุคคล เช่น การฉ้อโกงทางคอมพิวเตอร์ (Computer fraud) อย่างไรก็ตาม อาชญากรรมประเภทนี้บางกรณีอาจใช้วิธีการที่กระทบต่อความปลอดภัยทางคอมพิวเตอร์ได้ เช่น การใช้ชุดคำสั่งเพื่อหลอกลวงการทำงานของระบบ

3. อาชญากรรมคอมพิวเตอร์ที่ไม่ส่งผลกระทบต่อความปลอดภัยของระบบหรือข้อมูล เช่น การโพสต์แชร์เนื้อหาผิดกฎหมาย (Content crime)

แม้ว่าตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ของไทยจะครอบคลุมอาชญากรรมทั้ง 3 รูปแบบ และอาชญากรรมไร้ตัวตนก็อาจมีเป้าหมายหรือการกระทำผิดหลักที่เกี่ยวข้องกับความผิดทั้ง 3 กลุ่มข้างต้น แต่ขอบเขตการศึกษาการกระทำหลักของอาชญากรรมไร้ตัวตนในการวิจัย

[48] Iqbal, F., Binsalleeh, H., Fung, B. C., & Debbabi, M. (2013). A unified data mining solution for authorship analysis in anonymous textual communications. Information Sciences, 231, 98-112.

นี้ จำกัดเฉพาะอาชญากรรมไร้ตัวตนที่มีเป้าหมายหลักเป็นการกระทำกลุ่มที่ 1 และกลุ่มที่ 2 ซึ่งส่งผลกระทบต่อความปลอดภัยทางคอมพิวเตอร์ (Computer as target)

9.1.2 การกระทำเพื่อให้มีลักษณะไร้ตัวตนหรือการปกปิดตัวตน

ตำราอาชญากรรมไซเบอร์[49] ชี้ให้เห็นคุณลักษณะสำคัญของอาชญากรรมไซเบอร์คือความนิรนาม (Anonymity) กล่าวคือ การใช้เทคโนโลยีดิจิทัลหรือเทคโนโลยีสารสนเทศในการปกปิดตัวตนของอาชญากรด้วยเทคนิคต่างๆ เพื่อวัตถุประสงค์สำคัญคือการหลบเลี่ยงจากการบังคับใช้กฎหมายหรือการสืบสวนสอบสวน สำหรับการกระทำเพื่อปกปิดตัวตน อาจเป็นการกระทำต่างวาระกับการกระทำหลัก รวมทั้งอาจเข้าองค์ประกอบความผิดคนละฐานกับความผิดหลักอันเป็นเป้าหมายของอาชญากรรมชนิดนี้ก็ได้ โดยวิธีการปกปิดตัวตนมีความหลากหลายซึ่งงานวิจัยนี้จำแนกเป็นสองรูปแบบคือ

9.1.2.1 รูปแบบการใช้เทคโนโลยีเพื่อปกปิดตัวตนด้วยเทคนิคต่างๆ ซึ่งไม่ได้อาศัยข้อมูลระบุตัวผู้อื่น

อาชญากรรมคอมพิวเตอร์ที่ใช้เทคโนโลยีปกปิดตัวตนโดยไม่ได้อาศัยข้อมูลระบุตัวของผู้อื่น อาจใช้เทคนิควิธีการหลายอย่าง ซึ่งเมื่อพิจารณาเชิงกระบวนการหรือขั้นตอนการกระทำ จะพบว่าการใช้วิธีปกปิดตัวตนในรูปแบบนี้ อาจจัดเป็นขั้นตอนภายหลังจากการกระทำความผิดส่วนหลักซึ่งเป็นเป้าหมายของการกระทำแล้ว โดยอาจเป็นอีกกรรมหนึ่งแยกจากการกระทำความผิดหลัก เช่น อาชญากรเข้าถึงระบบคอมพิวเตอร์ขององค์กรหนึ่งเพื่อโจรกรรมข้อมูล จากนั้นจึงใช้วิธีการทางเทคนิคเพื่อปกปิดร่องรอยทางคอมพิวเตอร์ที่เกิดจากการเข้าถึงนั้น จะเห็นได้ว่า ในส่วนการกระทำเพื่อให้เกิดความนิรนามเป็นการกระทำในขั้นตอนที่สองหลังจากการกระทำหลักคือการเข้าถึงโดยมิชอบแล้ว สำหรับรูปแบบหรือวิธีการของการปกปิดตัวตน เช่น

- การใช้วิธีการเข้ารหัส (Encryption) การสื่อสารแบบเรียลไทม์ช่องทางต่างๆ ของอาชญากร เพื่อไม่ให้เจ้าหน้าที่บังคับใช้กฎหมายสามารถเข้าถึงได้แม้ว่าจะมีหมายศาลก็ตาม ดังตัวอย่างต่อไปนี้

ตัวอย่าง ผู้อำนวยการหน่วยสืบสวนกลางสหรัฐ (FBI) ให้ข้อมูลแก่คณะกรรมาธิการในวุฒิสภาถึงกรณี FBI ได้รับคำร้องจากเจ้าหน้าที่ที่เกี่ยวข้องกับการบังคับใช้กฎหมายในการให้ความช่วยเหลือเพื่อดำเนินการตามหมายศาลที่สั่งให้เข้าถึงและถอดรหัส (Decryption) ข้อมูลการสื่อสารของผู้ต้องหา แต่เนื่องจากการสื่อสารตามคำขอได้เข้ารหัสไว้จึงไม่สามารถดำเนินการได้ [50]

---

[49] Jonathan Clough, Principle of Cybercrime, 2nd ed. (Cambridge University Press, 2015), pp. 6-8.

[50] US Congress (1997a) Statement of Louis J. Freeh, Director FBI, before the Senate

ตัวอย่าง การใช้อีเมล์ที่เข้ารหัสและการบริการโอนเงินที่ปกปิดตัวตน ตัวอย่างเช่น อาชญากรทำการเจาะระบบคอมพิวเตอร์ของมหาวิทยาลัยแห่งหนึ่ง และนำข้อมูลเลขบัตรเครดิตกว่า 100,000 ข้อมูลมาขายออนไลน์ โดยในการติดต่อซื้อขายใช้วิธีการติดต่อผ่านอีเมล์ที่เข้ารหัสเพื่อไม่ให้ระบุตัวตนผู้ซื้อและขาย รวมทั้งใช้บริการโอนเงินแบบไม่ระบุตัว (Anonymous wire transfer) [51]

- การใช้โปรแกรมหรือซอฟท์แวร์สำเร็จรูปในการปกปิดตัวตน หรือ ลบร่องรอย (Trace) ที่เกิดจากการสื่อสารหรือการกระทำทางอินเทอร์เน็ต[52]

ตัวอย่าง อาชญากรใช้โปรแกรม PGP (Pretty Good Privacy) ซึ่งหาดาวน์โหลดได้ทั่วไปทางอินเทอร์เน็ตใ มาใช้ในการเข้ารหัสข้อมูลสื่อลามกเด็กเพื่อไม่ให้เจ้าหน้าที่สามารถตรวจสอบได้ [53]

การใช้วิธีเข้ารหัสข้อมูลหลายชั้น (เช่น Defense Encryption Standard) ส่งผลกระทบต่อทรัพยากรทั้งในแง่ต้นทุนและเวลา กล่าวคือ แม้เจ้าหน้าที่จะใช้วีการทางเทคนิคในการค้นหากุญแจเพื่อถอดรหัส (Decryption) แต่ก็ใช้งบประมาณมากและใช้เวลานับเดือน[54]

หากพิจารณาในภาพรวมของอาชญากรรมคอมพิวเตอร์จะพบว่า วิธีการเข้ารหัสที่อาชญากรรมคอมพิวเตอร์นำมาใช้นั้นอาจแยกได้เป็นสองกรณีคือ การเข้ารหัสที่ใช้เพื่อปกปิดตัวตนในการกระทำผิด เช่น การเข้ารหัสการสื่อสารหรือการทำธุรกรรมเพื่อไม่ให้ระบุตัวผู้เกี่ยวข้องได้ ซึ่งอาจใช้ได้หลายช่องทาง เช่น เข้ารหัสการสื่อสารทางจดหมายอิเล็กทรอนิกส์ เข้ารหัสการสื่อสารแบบเรียลไทม์ ฯลฯ และการเข้ารหัสเพื่อใช้ปกปิดหลักฐานสำหรับการกระทำผิด เช่น การเข้ารหัสอุปกรณ์จัดเก็บข้อมูลที่มีหลักฐานการกระทำผิด[55]

Committee on Commerce, Science, and Transportation, regarding the Impact
of Encryption on Law Enforcement and Public Safety, March 19

[51] Power, R. (1997) 'CSI Special Report: Salgado Case Reveals Darkside of Electronic Commerce,' Computer Security Alert, No. 174, September.

[52] Jonathan Clough, Principle of Cybercrime, 2nd ed. (Cambridge University Press, 2015), pp. 6-8.

[53] Monique Ferraro, Eoghan Casey, BS, MA, Eoghan Casey, Michael McGrath, Investigating child exploitation and pornography: the Internet, the law and forensic science, Elsevier Academic Press, 2005, p.153.

[54] Littman, J. (1997) The Watchman: The Twisted Life and Crimes of Serial Hacker
Kevin Poulson, Little, Brown and Co.

[55] Dorothy E. Denning & William E. Baugh Jr (1999) HIDING CRIMES IN CYBERSPACE, Information, Communication & Society, 2:3, 251-276, DOI: 10.1080/136911899359583

9.1.2.2 รูปแบบการใช้ข้อมูลระบุตัวผู้อื่นเพื่อปกปิดตัวตนในการก่ออาชญากรรม

อาชญากรรมคอมพิวเตอร์อาจใช้เทคโนโลยีที่หลากหลายในการปกปิดตัวตนโดยอาศัยข้อมูลระบุตัวของผู้อื่น ซึ่งการกระทำต่อข้อมูลระบุตัวผู้อื่นนั้น อาจจัดเป็นขั้นตอนก่อนการกระทำความผิดส่วนหลัก ซึ่งเป็นเป้าหมายของการกระทำ เช่น อาชญากรเข้าถึงระบบคอมพิวเตอร์ขององค์กรหนึ่งเพื่อโจรกรรมข้อมูลระบุตัวตนของบุคคลและนำข้อมูลเหล่านั้นมาใช้แสดงตนเป็นผู้กระทำความผิดหลักเพื่อปกปิดการกระทำของตน จะเห็นได้ว่า ในส่วนการกระทำเพื่อให้เกิดความนิรนามเป็นการกระทำในขั้นตอนก่อนการกระทำหลัก ตัวอย่างรูปแบบหรือวิธีการของการปกปิดตัวตนโดยการใช้ข้อมูลระบุตัวผู้อื่น เช่น การเข้าถึงบัญชีใช้งานของเหยื่อและเปลี่ยนรหัสจากนั้นควบคุมบัญชีดังกล่าวเพื่อไปใช้ประกอบอาชญากรรม การนำข้อมูลระบุตัวของผู้อื่นมาใช้เพื่อสมัครบริการสื่อสารออนไลน์ต่างๆ เพื่อทำการโจมตีระบบคอมพิวเตอร์ของเป้าหมายในการกระทำความผิดหลัก การใช้อีเมล์ของผู้อื่นในการกระทำความผิด[56]

แม้ว่าโดยทั่วไป การกระทำในส่วนของการปกปิดตัวตนจะเกิดขึ้นก่อนการกระทำความผิดหลัก แต่จากการศึกษาวรรณกรรมแนวคิดทฤษฎีแล้วพบว่า การใช้ข้อมูลระบุตัวผู้อื่นมาปกปิดการกระทำเรียกชื่อว่า “การโจรกรรมข้อมูลเอกลักษณ์หรืออัตลักษณ์ (Identity theft) ดังกล่าวในหัวข้อ 3. ซึ่งอาจเกิดขึ้นได้โดยไม่จำกัดสภาพแวดล้อมและเทคโนโลยี โดยในบางกรณีอาจไม่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ เช่น การโจรกรรมข้อมูลสำเนาบัตรประชาชนไปใช้ทำธุรกรรมทางเอกสาร[57] แม้ว่าบางกรณีเกี่ยวข้องกับการกระทำความผิดทางคอมพิวเตอร์ แต่อาจไม่ใช่การกระทำต่อระบบหรือข้อมูล เช่น การนำข้อมูลระบุตัวบุคคลอื่นไปสมัครใช้สื่อออนไลน์และโพสต์เนื้อหาผิดกฎหมาย แต่ในงานวิจัยนี้จะศึกษาเฉพาะการโจรกรรมข้อมูลเอกลักษณ์ในฐานะที่เป็นวิธีการหนึ่งของอาชญากรรมคอมพิวเตอร์แบบไร้ตัวตนที่ส่งผลกระทบต่อความปลอดภัยของระบบและข้อมูลคอมพิวเตอร์ ซึ่งในทางวิชาการมีการจำแนกรูปแบบเชิงกระบวนการหรือขั้นตอนไว้แตกต่างกัน เช่น

---

[56] Nirkhi, S. M., Dharaskar, R. V., & Thakre, V. M. (2012, June). Analysis of online messages for identity tracing in cybercrime investigation. In Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec) (pp. 300-305). IEEE.

[57] คณาธิป ทองรวีวงศ์ , มาตรการทางกฎหมายอาญาในการป้องกันและปราบปรามการโจรกรรมข้อมูลเชิงเอกลักษณ์ , วารสารวิชาการเซาธ์อีสท์บางกอก 1, 1 (ม.ค.-มิ.ย. 2558) 56-75

การจำแนกรูปแบบการกระทำเป็น 3 ขั้นตอน คือ [58]

1) ขั้นตอนการค้นหา (Discovery stage) ซึ่งประกอบด้วยพฤติกรรมหลักสองอย่าง คือ

(ก) อาชญากรได้มาซึ่งข้อมูล (Gain information) โดยใช้วิธีการต่างๆ เช่น การเข้าถึงคอมพิวเตอร์เพื่อค้นข้อมูล

(ข) อาชญากรตรวจสอบข้อมูล (Verify information) เพื่อให้แน่ใจว่าเป็นข้อมูลระบุตัวตนของเหยื่อ เช่น การส่งข้อความหรืออีเมล์ไปทดสอบ.

2) ขั้นตอนการดำเนินการ (Action) หมายถึง การนำข้อมูลระบุตัวของเหยื่อที่ได้มาไปเตรียมสำหรับการลงมือกระทำเพื่อแสวงประโยชน์ในขั้นต่อไป เช่น การนำข้อมูลระบุตัวผู้อื่นไปเปิดบัญชี สมัครบัตรเครดิต การนำข้อมูลไปสมัครใช้งานการซื้อขายออนไลน์

3) ขั้นตอนการลงมือ (Trial) ในขั้นตอนนี้อาชญากรจะลงมือกระทำการเพื่อให้ได้มาซึ่งทรัพย์สินหรือประโยชน์ เช่น การใช้บัตรเครดิตที่เปิดขึ้นในนามของเหยื่อไปซื้อสินค้าหรือบริการ การใช้ข้อมูลเอกลักษณ์ของเหยื่อไปหลอกลวงผู้อื่นเพื่อให้ได้มาซึ่งทรัพย์สิน เป็นต้น

งานวิชาการบางชิ้นเสนอกรอบกระบวนการพิจารณาการโจรกรรมข้อมูลอัตลักษณ์ 2 ขั้นตอน คือ [59]

1) ขั้นตอนการได้มาซึ่งข้อมูลระบุตัวโดยมิชอบ (Unauthorized collection of information) กล่าวคือ ใช้วิธีการใดๆ ในการได้มาซึ่งข้อมูลเอกลักษณ์ของผู้อื่นโดยไม่มีสิทธิ

2) ขั้นตอนการนำข้อมูลระบุตัวผู้อื่นไปใช้ในทางมิชอบ (Fraudulent use) เช่นนำไปใช้ทำธุรกรรมต่างๆ หรือหลอกลวงผู้อื่นเพื่อให้ได้มาซึ่งประโยชน์ในทางใดๆ

อย่างไรก็ตาม การจำแนกรูปแบบบางเกณฑ์ กำหนดขั้นตอนเพิ่มเติมหลังจากการประกอบอาชญากรรม เช่น รายงานวิจัยของสถาบันการยุติธรรมแห่งชาติของสหรัฐ (National Institute of Justice หรือ NIJ)[60] ชี้ให้เห็นว่า หลังจากขั้นตอนที่อาชญากรรมนำข้อมูลระบุตัวผู้อื่นไปใช้ปกปิดตัวตนแล้ว ยังมี

---

[58] W. Steve Albrecht, Chad O. Albrecht, Conan C Albrecht, and Mark F. Zimbelman, Fraud Examination (SouthWestern Cengage Learning, 2011), pp. 533-534.

[59] Nazura Abdul Manap, Anita Abdul Rahim, and Hossein Taji, “Cyberspace Identity theft: The Conceptual Framework,” Mediteranean Jouranl of Social Science 6,4 (August 2015): 600.

[60] Graeme R. Newman and Megan M. McNally, “Identity Theft : A Research Review,” Final Report to the National Institute of Justice (2005): 5-6.

ขั้นตอนที่สามของกระบวนการคือ การค้นพบอาชญากรรม (Discovery of the theft) กล่าวคือ การตรวจสอบพบข้อเท็จจริงว่าเจ้าของข้อมูลที่อ้างอิงหรือถูกนำข้อมูลไปใช้นั้นไม่เกี่ยวข้องกับการกระทำผิด แต่ขั้นตอนนี้อาจใช้เวลานานหรืออาจไม่ปรากฏหรือตรวจสอบพบเลยก็ได้

จากวรรณกรรมต่างๆ เมื่อนำมาพิจารณาประกอบกับรูปแบบของอาชญากรรมไร้ตัวตนที่ประกอบด้วย การกระทำหลักและการกระทำเพื่อปกปิดตัวตน ดังกล่าวมาแล้วนั้น ผู้วิจัยจึงสรุปรูปแบบเชิงกระบวนการของอาชญากรรมไร้ตัวตนในกรณีที่ใช้ข้อมูลระบุตัวผู้อื่นมาปกปิดตัวตน เป็นการกระทำ 3 ขั้นตอนคือ

1 ขั้นตอนการได้มาซึ่งข้อมูลระบุตัวตนของผู้อื่น

การกระทำในขั้นตอนนี้อาจใช้วิธีการที่หลากหลายและบางวิธีการจะเข้าองค์ประกอบความผิดได้ในตัวเอง โดยเป็นความผิดสำเร็จในขั้นตอนนี้ เช่น

- การเจาะระบบและโจรกรรมข้อมูลระบุตัวที่อยู่ในระบบของผู้อื่น เช่น ข้อมูลลูกค้าหรือผู้ใช้บริการของภาคธุรกิจต่างๆ

- การใช้วิธีการฟิชชิ่ง (Phishing) เช่นสร้างหน้าเว็บไซต์หลอกลวงเป็นผู้ขายสินค้าหรือบริการต่างๆ เพื่อให้คนกรอกข้อมูลระบุตัวตน[61]

- การซื้อขายข้อมูลส่วนบุคคล[62] ซึ่งอาจเกิดขึ้นในตลาดมืดออนไลน์

2. ขั้นตอนการกระทำต่อข้อมูลระบุตัวของผู้อื่น ก่อนการกระทำความผิดหลัก

การกระทำในขั้นตอนนี้ยังไม่ใช่เป้าหมายหลักหรือวัตถุประสงค์สุดท้าย แต่เป็นการกระทำที่มีวัตถุประสงค์เพื่อปกปิดตัวตน เช่น การนำข้อมูลระบุตัวบุคคลอื่นที่ได้มาไปใช้สมัครหรือลงทะเบียนใช้บริการการสื่อสาร บัญชีธนาคาร บริการสื่อสังคมออนไลน์ เพื่อที่จะนำไปใช้กระทำความผิดหลักต่อไป การกระทำในขั้นตอนนี้อาจไม่มีกฎหมายกำหนดไว้เป็นความผิด หรือในบางกรณีอาจเข้าองค์ประกอบความผิดได้ในตัวเองแม้ยังไม่มีการกระทำในขั้นต่อไป เช่น การโจรกรรมข้อมูลภาพจำลองใบหน้าของผู้อื่นมาเพื่อใช้ในการเปิดบัญชีธนาคารออนไลน์ อาจเข้าข่ายการนำข้อมูลปลอมหรือเท็จเข้าสู่ระบบตามมาตรา 14 แห่งพระราชบัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

---

[61] Marco Gercke, Internet-related Identity Theft, Project on Cybercrime (Council of Europe, 2007), p. 19-20.; Ruth Halperin, “Identity as an Emerging Field of Study,” Datenschutz und Datensicherheit - DuD 30,9 (2006): 533–537.

[62] Mohammed Chawki and Mohamed S. Abdel Wahab, ibid., p. 17.

3. ขั้นตอนการกระทำหลัก

การกระทำในขั้นตอนนี้เป็นวัตถุประสงค์หลักหรือเป้าหมายสุดท้าย (Target) ของอาชญากรรมแบบไร้ตัวตน กล่าวคือ หลังจากการได้มาและกระทำการกับข้อมูลระบุตัวของผู้อื่นแล้ว อาชญากรจะกระทำการอันเป็นเป้าหมายโดยใช้ข้อมูลดังกล่าวในฐานะการแสดงหรือยืนยันตัวตนให้เข้าใจว่าร่องรอยหรือการกระทำที่เกิดขึ้นเป็นการกระทำของเจ้าของข้อมูลการกระทำหลักอาจจำแนกเป็นหลายรูปแบบดังกล่าวมาแล้ว เช่น การใช้มัลแวร์ การโจรกรรมข้อมูล การใช้มัลแวร์เรียกค่าไถ่ การโจมตีให้ระบบขัดข้องไม่สามารถใช้งานได้ ฯลฯ และอาจเป็นการกระทำที่มุ่งประโยชน์ทางทรัพย์สิน เช่น การฉ้อโกงการลงทุน การกระทำผิดเกี่ยวกับบัตรเครดิต[63]

นอกจากการใช้ข้อมูลระบุตัวบุคคลอื่นเพื่อปกปิดตัวตนของอาชญากรแล้ว ในบางกรณีอาจมีการใช้ข้อมูลของนิติบุคคล เช่น การสร้างข้อมูลเว็บไซต์ปลอมเป็นขององค์กรที่เป็นบริษัทหรือสมาคมแห่งหนึ่งเพื่อหลอกลวงให้เหยื่อหลงเชื่อกรอกข้อมูลหรือทำธุรกรรม ดังนี้เป็นการปกปิดตัวตนโดยอาศัยข้อมูลนิติบุคคลในแง่กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ การจำแนกระหว่างการปกปิดตัวตนด้วยข้อมูลของบุคคลธรรมดาหรือนิติบุคคลไม่มีนัยที่แตกต่างกันเชิงองค์ประกอบ แต่การจำแนกดังกล่าวอาจมีนัยสำคัญตามกฎหมายอื่น เช่น กฎหมายคุ้มครองข้อมูลส่วนบุคคล กำหนดหลักการครอบคลุมเฉพาะการกระทำต่อข้อมูลของบุคคลธรรมดาโดยไม่มีขอบเขตถึงข้อมูลนิติบุคคล

ผู้วิจัยมีข้อพิจารณาเพิ่มเติมว่า การจำแนกรูปแบบอาชญากรรมไร้ตัวตนเป็นการกระทำสองส่วนคือการกระทำหลักและการกระทำเพื่อปกปิดตัวตนนั้น อาจมีบางกรณีที่เป็นการกระทำอันเดียวซึ่งมุ่งเป้าหมายสุดท้ายและเป็นทั้งวิธีการปกปิดตัวตนด้วย เช่น การสร้างข้อมูลเว็บไซต์ปลอมเพื่อ หลอกลวงให้เหยื่อหลงเชื่อกรอกข้อมูลหรือทำธุรกรรม จะเห็นได้ว่า การกระทำหลักคือการปลอมตัวนั้นมีเป้าหมายคือการแสวงประโยชน์จากข้อมูลเหยื่อและการกระทำหลักนั้นก็มีลักษณะของการปกปิดตัวตนไปด้วยในตัว

9.1.2.3 รูปแบบการใช้ข้อมูลระบุตัวที่ไม่มีตัวตนจริงเพื่อปกปิดตัวตนในการก่ออาชญากรรม

การกระทำเพื่อปกปิดตัวตนโดยใช้ข้อมูลบุคคลอื่นในกรณีนี้แตกต่างจากรูปแบบที่สองซึ่งเป็นการโจรกรรมข้อมูลของเหยื่อที่มีตัวตนและไม่มีส่วนเกี่ยวข้องกับอาชญากรรมมาใช้ (Stolen identity)

---

[63] Federal Trade Commission, Consumer Fraud and Identity Theft Complain Data : January – December 2005 (Federal Trade Commission, 2006). p. 3.

เนื่องจากในกรณีนี้อาชญากรใช้ข้อมูลระบุตัวของบุคคลที่ไม่มีอยู่จริง[64] หรือการสร้างตัวตนขึ้นมาใหม่ (Constructed identity) ดังนั้น หากจำแนกพิจารณารูปแบบเชิงกระบวนการหรือขั้นตอนของการกระทำนี้จะแบ่งได้ 2 ขั้นตอนคือ

1 ขั้นตอนการสร้างข้อมูลระบุตัวตน

การกระทำในขั้นตอนนี้อาจใช้วิธีการหรือเทคนิคที่หลากหลาย เช่น การใช้โปรแกรมสร้างภาพ การสร้างข้อมูลแวดล้อมหรือข้อมูลเพื่อเป็นโปรไฟล์ของตัวตนเสมือนในแง่ฐานความผิด การกระทำนี้อาจไม่เข้าข่ายความผิดเกี่ยวกับคอมพิวเตอร์เนื่องจากไม่ได้มีการเข้าถึงข้อมูลของบุคคลอื่น อย่างไรก็ตาม การสร้างตัวตนเสมือนในบางกรณีอาจเข้าข่ายความผิด เช่น การลงทะเบียนหรือสมัครใช้งานบริการสื่อสารโดยใช้ข้อมูลบุคคลที่ไม่มีจริงอาจเข้าองค์ประกอบการนำข้อมูลปลอมหรือเท็จเข้าสู่ระบบ

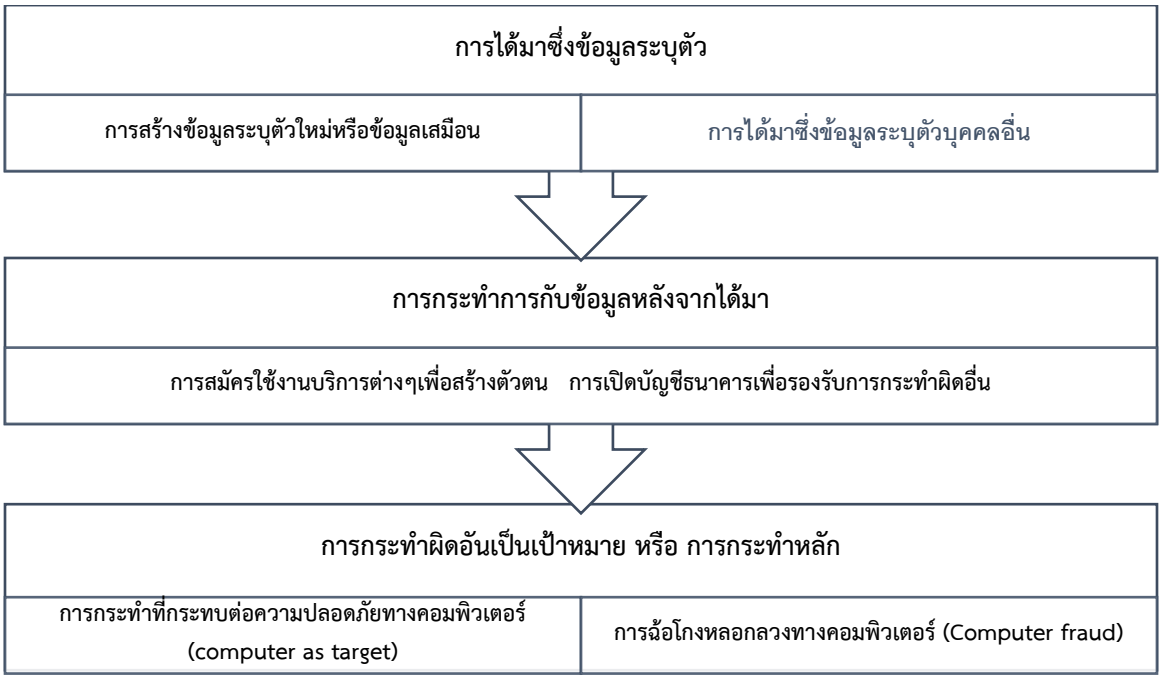
2. ขั้นตอนการกระทำหลัก

การกระทำในขั้นตอนนี้เป็นวัตถุประสงค์หลักหรือเป้าหมายสุดท้าย (Target) ซึ่งอาจเป็นความผิดต่างๆที่กระทบต่อความปลอดภัยทางคอมพิวเตอร์ อันเป็นรูปแบบเดียวกับการใช้ข้อมูลระบุตัวผู้อื่นเพื่อปกปิดตัวตนในการก่ออาชญากรรมดังกล่าวในหัวข้อก่อนหน้า

จากการวิเคราะห์รูปแบบของอาชญากรรมไร้ตัวตนข้างต้น จะพบว่า รูปแบบที่สำคัญและส่งผลกระทบต่อหลายฝ่ายคือ การใช้ข้อมูลระบุตัวบุคคลอื่นเพื่อปกปิดการกระทำของตน ซึ่งสรุปขั้นตอนการกระทำได้ดังนี้

---

[64] Zingerle, A. (2014). Remain Anonymous, Create Characters and Backup Stories: Online Tools Used in Internet Crime Narratives. In: Mitchell, A., Fernández-Vara, C., Thue, D. (eds) Interactive Storytelling. ICIDS 2014. Lecture Notes in Computer Science, vol 8832. Springer, Cham.



ภาพการจำแนกรูปแบบของการกระทำในส่วนปกปิดตัวตนของอาชญากรรมแบบไร้ตัวตน

จะเห็นได้ว่า งานวิชาการไม่ได้จำแนกอาชญากรรมแบบไร้ตัวตนว่ามีรูปแบบเฉพาะหรือพิเศษอันแตกต่างหรือจัดเป็นประเภทอาชญากรรมใหม่นอกเหนือจากอาชญากรรมไซเบอร์ แต่การประกอบอาชญากรรมไซเบอร์รูปแบบต่างๆนั้น สามารถกระทำโดยมีลักษณะของความนิรนามหรือไร้ตัวตนได้ทั้งสิ้น เมื่อนำรูปแบบเชิงกระบวนการหรือขั้นตอนการประกอบอาชญากรรมไร้ตัวตนดังกล่าวแล้วมาพิจารณา จึงกล่าวได้ว่า ในส่วนการกระทำหลักของอาชญากรรมแบบไร้ตัวตน สามารถอธิบายรูปแบบวิธีการได้ในกลุ่มของวิธีการเช่นเดียวกับอาชญากรรมไซเบอร์ทั่วไป เช่น การเข้าถึงโดยมิชอบ การโจมตีรบกวนขัดขวางการทำงานของระบบ การทำลายหรือแก้ไขข้อมูล ฯลฯ แต่จะมีการกระทำในส่วนที่สองเพิ่มเติมขึ้นมาคือ*การใช้วิธีการเพื่อปกปิดตัวตนหรือทำให้การกระทำส่วนแรกไม่สามารถระบุร่องรอยหรือติดตามตัวผู้กระทำได้*

9.2 รูปแบบในแง่ช่องทางหรือแพลตฟอร์มของการประกอบอาชญากรรมแบบไร้ตัวตน

หากพิจารณาในแง่ช่องทาง (Channel) หรือแพลตฟอร์ม (Platform) ที่เกิดการประกอบอาชญากรรม จะพบว่าอาชญากรรมไซเบอร์แบบไร้ตัวตน อาศัยช่องทางที่หลากหลาย เช่น

- การใช้ช่องทางอีเมล์ที่ไม่ระบุตัวผู้ใช้งาน (Anonymous email) [65]

- การใช้ช่องทางการสื่อสารแบบเรียลไทม์ โปรแกรมการสนทนา [66]

- การใช้ช่องทางการชำระเงินอิเล็กทรอนิกส์แบบนิรนาม ในกรณีผู้ให้บริการด้านการชำระเงินอิเล็กทรอนิกส์ซึ่งออกแบบระบบเพื่อให้การชำระเงินไม่ต้องใช้ข้อมูลที่ระบุตัวทั้งผู้รับและผู้จ่ายเงิน ซึ่งอยู่ในลักษณะนิรนาม ระบบนี้มีประโยชน์ในแง่ของการรักษาความปลอดภัยและความเป็นส่วนตัวของคู่กรณีในธุรกรรม แต่อาจถูกนำไปใช้โดยมิชอบ (Abuse) เนื่องจากมีความเปราะบางต่ออาชญากรรม [67]

สื่อสังคมออนไลน์หรือโซเชียลมีเดีย (Social media platform) อาชญากรไร้ตัวตนใช้สื่อสังคมออนไลน์เป็นช่องทางสำคัญในการประกอบอาชญากรรมรูปแบบต่างๆ ได้อย่างกว้างขวาง เช่น สร้างตัวตนในสื่อออนไลน์ด้วยข้อมูลของบุคคลอื่นและใช้สื่อออนไลน์นั้นทำการวางแผนหลอกลวงเหยื่อ (Scam) การฉ้อโกง (Fraud) โดยในหลายกรณีเป็นการกระทำเชิงองค์กรอาชญากรรมที่มีการวางแผนอย่างเป็นระบบและมีขอบเขตทำการข้ามพรมแดน (global scale) [68]

จะเห็นได้ว่า กรณีที่ช่องทางหรือแพลตฟอร์มบางอย่างออกแบบไว้เพื่อให้ผู้ใช้งานสามารถสื่อสารหรือทำธุรกรรมโดยไม่ระบุตัวหรือมีความเป็นนิรนาม เช่น แพลตฟอร์มการชำระเงินโดยไม่ระบุตัวตน หรือสื่อสังคมออนไลน์ที่สามารถเปิดบัญชีใช้งานโดยไม่ต้องระบุตัวตน ในแง่หนึ่งจะมีประโยชน์สำหรับการปกป้องความเป็นส่วนตัวของผู้ใช้งาน แต่ในอีกแง่หนึ่งอาจถูกอาชญากรรมนำคุณลักษณะนี้ไปใช้โดยมิชอบเพื่อประกอบอาชญากรรมแบบไร้ตัวตน

---

[65] Nirkhi, S. M., Dharaskar, R. V., & Thakre, V. M. (2012, June). Analysis of online messages for identity tracing in cybercrime investigation. In Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec) (pp. 300-305). IEEE.

[66] Dorothy E. Denning & William E. Baugh Jr (1999) HIDING CRIMES IN CYBERSPACE, Information, Communication & Society, 2:3, 251-27

[67] Sander, T., Ta-Shma, A. (1999). On Anonymous Electronic Cash and Crime. In: Information Security. ISW 1999. Lecture Notes in Computer Science, vol 1729. Springer, Berlin, Heidelberg.

[68] Zingerle, A. (2014). Remain Anonymous, Create Characters and Backup Stories: Online Tools Used in Internet Crime Narratives. In: Mitchell, A., Fernández-Vara, C., Thue, D. (eds) Interactive Storytelling. ICIDS 2014. Lecture Notes in Computer Science, vol 8832. Springer, Cham. https://doi.org/10.1007/978-3-319-12337-0_8

9.3 รูปแบบของความถี่ (Frequency) ในการกระทำผิดแบบไร้ตัวตน

ในทางวิชาการมีการนำเกณฑ์ด้านความถี่ของการโจมตีทางไซเบอร์มาวิเคราะห์อาชญากรรม ซึ่งจะทำให้สามารถจำแนกรูปแบบของอาชญากรรมไร้ตัวตนเป็นสองกลุ่มคือ[69]

- การโจมตีหรือก่อเหตุครั้งเดียว (Single event) หรืออาชญากรรมไม่ต่อเนื่องซึ่งเป็นการก่อเหตุที่เกิดขึ้นครั้งเดียวโดยเจาะจง (Specific attack) กล่าวคือ ไม่มีลักษณะการกระทำต่อเนื่อง แม้ว่าจะมีผลเสียหายที่ยังคงอยู่อันกระทบต่อระบบหรือข้อมูลของเหยื่อ แต่อาชญากรได้ยุติหรือเสร็จสิ้นการโจมตีแล้ว เช่น การแฮกคอมพิวเตอร์ของเหยื่อและนำไปใช้ส่งคำสั่งปล่อยมัลแวร์โจมตีระบบคอมพิวเตอร์ขององค์กรหนึ่งเพียงครั้งเดียวซึ่งทำให้ข้อมูลบางส่วนเสียหาย แม้ว่าความเสียหายของข้อมูลนั้นยังคงเกิดต่อเนื่องหรือระบบขององค์กรที่ถูกโจมตียังไม่สามารถใช้งานได้ปกติอีกระยะหนึ่ง หรือเหยื่อในความผิดในระดับการปกปิดตัวตนยังคงไม่สามารถเข้าถึงคอมพิวเตอร์ของตนได้ แต่ก็จัดว่าเป็นการโจมตีครั้งเดียว

- การโจมตีหรือก่อเหตุเป็นชุด (Series of event) ซึ่งอาจเป็นการโจมตีหลายครั้งแยกกัน (Separate event) หรือการโจมตีในลักษณะต่อเนื่องหรือซ้ำๆ (Continuous or repeated attack) เช่น การโจรกรรมข้อมูลภาคธุรกิจอย่างต่อเนื่อง การส่งมัลแวร์ที่มีลักษณะการทำงานดักรับข้อมูลในคอมพิวเตอร์ของเหยื่อโดยไม่รู้ตัวอย่างต่อเนื่องทุกวัน

9.4 รูปแบบของเครื่องมือที่ใช้กระทำผิดแบบไร้ตัวตน

อาชญากรรมแบบไร้ตัวตนใช้วิธีการทางเทคนิค เช่น ชุดคำสั่ง โปรแกรม รวมทั้งอุปกรณ์ฮาร์แวร์ต่างๆ ในการกระทำผิด ซึ่งอาจมีรายละเอียดทางเทคนิคที่หลากหลาย แต่ในงานวิจัยนี้จะพิจารณาในแง่ของกฎหมายและรูปแบบอาชญากรรมซึ่งในทางวิชาการมีการจำแนกรูปแบบเครื่องมือเป็นสองกลุ่มคือ [70]

(1) *อาชญากรรมซึ่งใช้เครื่องมือเฉพาะ กล่าวคือ* มีการใช้ซอฟท์แวร์หรือโปรแกรมที่จัดทำขึ้นเฉพาะสำหรับอาชญากรรม (Crime-ware) [71] ซึ่งอาจออกแบบให้เหมาะสมกับวิธีการทางเทคนิคและสอดคล้องกับเป้าหมาย เช่น การเขียนชุดคำสั่งโดยเฉพาะเพื่อการโจมตีระบบขององค์กรเป้าหมาย

---

[69] H. Thomas Milhorn, Cybercrime: How to Avoid Becoming a Victim (Universal Publishers, 2007), p. 2.

[70] Sarah Gordon and Richard Ford, "On the Definition and Classification of Cybercrime," Journal in Computer Virology 2,1 (2006): 13-20.

[71] Norton, What is cybercrime? [Online]. (n.d.). Available from: https://us.norton.com/cybercrime-definition [21 November 2018]

(2) อาชญากรรมซึ่งไม่ได้ใช้เครื่องมือเฉพาะ ความผิดกลุ่มนี้อาจไม่ได้ใช้ซอฟท์แวร์หรือชุดคำสั่งที่สร้างขึ้นโดยเฉพาะสำหรับประกอบอาชญากรรม (Crime- ware) โดยอาจใช้เครื่องมือที่ใช้สำหรับการปฏิบัติงานอื่นในการประกอบอาชญากรรม เช่น การใช้โปรแกรมสนทนาเป็นเครื่องมือส่งลิงค์ที่มีไวรัส หรือการใช้อีเมล์ในการส่งมัลแวร์

9.5 รูปแบบเหยื่อของอาชญากรรมแบบไร้ตัวตน

จากการนำแนวคิดทฤษฎีเกี่ยวกับเหยื่อ (Victim) ในแง่อาชญาวิทยามาพิจารณาอาชญากรรมแบบไร้ตัวตน จะพบว่าจำแนกรูปแบบของเหยื่อของอาชญากรรมเป็นสองประเภท คือ

(1) อาชญากรรมแบบไร้ตัวตนที่มีเหยื่อ เช่น การเข้าถึงโดยมิชอบซึ่งข้อมูลหรือระบบของหน่วยงานหรือบุคคล การทำลายหรือแก้ไขข้อมูลของบริษัท การฉ้อโกงทางคอมพิวเตอร์ การโจมตีระบบขององค์กรหรือหน่วยงานให้ไม่สามารถใช้การได้และเนื่องจากอาชญากรรมแบบไร้ตัวตนมีรูปแบบในแง่กระบวนการที่จำแนกได้สองระดับคือ ระดับความผิดหลักและระดับของความผิดอันเป็นวิธีการปกปิดตัวตน จึงจำแนกเหยื่อได้สองกลุ่มคือ

1) เหยื่อของอาชญากรรมไร้ตัวตนในระดับความผิดหลัก ซึ่งเป็นเป้าหมายหรือวัตถุประสงค์หลักของการประกอบอาชญากรรม เช่น การแฮกข้อมูลสำคัญทางการค้าขององค์กร หรือการส่งมัลแวร์ทำลายข้อมูลขององค์กรที่เป็นเหยื่อ

2) เหยื่อของอาชญากรรมไร้ตัวตนในระดับความผิดอันเป็นวิธีการปกปิดตัวตน ซึ่งไม่ใช่เป้าหมายหลักหรือวัตถุประสงค์สุดท้ายของการประกอบอาชญากรรม เช่น เหยื่อที่ถูกโจรกรรมข้อมูลระบุตัวตน เช่น ชื่อ บัญชีการใช้งานสื่อออนไลน์ บัญชีจดหมายอิเล็กทรอนิกส์ ซึ่งอาชญากรรมนำไปใช้ในฐานะวิธีการทำให้ตนเองอยู่ในภาวะไร้ตัวตนเพื่อการประกอบอาชญากรรมในระดับหลัก เช่น การแฮกบัญชีจดหมายอิเล็กทรอนิกส์ของเหยื่อมาใช้ในการส่งมัลแวร์ไปทำลายข้อมูลขององค์กรเป้าหมาย

(2) อาชญาแบบไร้ตัวตนที่ปราศจากเหยื่อ (Victimless crime) คือ พฤติกรรมที่กฎหมายกำหนดเป็นความผิด แต่ไม่กระทบหรือไม่ละเมิดสิทธิของบุคคล[72] เช่น การนำเข้าสู่ระบบหรือเผยแพร่ส่งต่อข้อมูลเนื้อหาที่กระทบต่อความมั่นคงของรัฐ อย่างไรก็ตาม ในส่วนอาชญากรรมไร้ตัวตนที่กระทบต่อความปลอดภัยของระบบและข้อมูลคอมพิวเตอร์นั้น โดยทั่วไปแล้วจะเป็นอาชญากรรมที่มีเหยื่อ ไม่ว่าจะเป็นกรณีของบุคคลธรรมดาหรือนิติบุคคลก็ตาม สำหรับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่ไม่มีเหยื่อและไม่กระทบต่อความปลอดภัยทาง

[72] Vera Bergelson, “Victimless Crimes,” in The International Encyclopedia of Ethics (Wiley Online Library, 2013).

คอมพิวเตอร์นั้น อาจใช้วิธีการปกปิดหรือนิรนามได้เช่นกัน เช่น การโจรกรรมอุปกรณ์คอมพิวเตอร์ของเหยื่อไปใช้เพื่อโพสต์ข้อมูลเนื้อหาผิดกฎหมาย แต่ไม่อยู่ในขอบเขตการศึกษานี้

9.6 ความเสี่ยงและผลกระทบของอาชญากรรมแบบไร้ตัวตน

อาชญากรรมคอมพิวเตอร์แบบไร้ตัวตนนำไปสู่ความเสี่ยงและผลกระทบในหลายมิติดังจะแยกพิจารณาต่อไปนี้

9.6.1 ผลกระทบต่อความปลอดภัยของระบบและข้อมูลคอมพิวเตอร์

โดยหลักแล้วอาชญากรรมแบบไร้ตัวตนส่งผลกระทบต่อความปลอดภัยของระบบและข้อมูลคอมพิวเตอร์ดังที่อธิบายในส่วนแนวคิดทฤษฎีด้านความมั่นคงทางคอมพิวเตอร์ อย่างไรก็ตาม สามารถขยายความอธิบายผลกระทบต่อความปลอดภัยทางคอมพิวเตอร์ของการประกอบอาชญากรรมแบบไร้ตัวตน ได้สองกรณีตามลักษณะการโจมตี (Type of attack) ดังนี้[73]

(1) *การโจมตีแบบไม่กระทบต่อการทำงานของระบบ (Passive attack) หมายถึง* การโจมตีหรือการคุกคามที่เกิดขึ้นต่อระบบเครือข่ายโดยไม่ส่งผลกระทบต่อการทำงานตามปกติของเครือข่าย ระบบคอมพิวเตอร์ โดยอาชญากรมุ่งใช้ประโยชน์จากข้อมูลในระบบ เช่น การดักรับข้อมูล (Interception) การสอดส่องหรือสอดแนม[74]

ตัวอย่าง องค์กรอาชญากรรมใช้วิธีการส่งชุดคำสั่งเพื่อดักรับข้อมูลการทำธุรกรรมของหน่วยงานต่างๆ ที่ส่งผ่านเครือข่ายคอมพิวเตอร์ ดังนี้ แม้ว่าผู้เกี่ยวข้องและผู้ใช้งานยังคงสามารถใช้งานระบบและข้อมูลได้ตามปกติ รวมทั้งอาจไม่ทราบถึงการโจมตีโดยการดักรับข้อมูลนี้ แต่ก็จัดว่าส่งผลกระทบต่อความปลอดภัยทางคอมพิวเตอร์แล้ว

(2) *การโจมตีแบบส่งผลกระทบต่อการทำงานของระบบ (Active attack) หมายถึงการใช้วิธีการ* ซึ่งส่งผลกระทบต่อระบบหรือข้อมูลในลักษณะของการแก้ไขเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ หรือส่งผลกระทบต่อการทำงานตามปกติของระบบหรือเครือข่ายคอมพิวเตอร์

---

[73] Joe Wright and Jim Harmening, “Security Management Systems,” in Computer and Information Security Handbook, ed. John R. Vacca (Morgan Kaufmann Publishers, Elsevier Inc., 2009), p. 257.

[74] William Stallings, Network Security Essentials: Applications and Standards, 4th ed. (US: Prentice Hall, 2011), pp. 9-10.

ตัวอย่าง การใช้มัลแวร์ซึ่งส่งผลให้เกิดการทำลายหรือแก้ไขข้อมูลคอมพิวเตอร์ การโจมตีแบบ DOS ส่งผลกระทบต่อการทำงานตามปกติของระบบคอมพิวเตอร์

ดังนั้นจึงสรุปได้ว่า แม้โดยหลักแล้วอาชญากรรมคอมพิวเตอร์แบบไร้ตัวตนจัดเป็นภัยคุกคามความปลอดภัยทางคอมพิวเตอร์ตามกรอบแนวคิดทฤษฎีเกี่ยวกับปัจจัยด้านความปลอดภัย เช่น “CIA” แต่ยังอาจจำแนกผลกระทบต่อความปลอดภัยทางคอมพิวเตอร์ออกเป็นสองกรณีย่อยดังกล่าวข้างต้น

9.6.2 ผลกระทบต่อทรัพย์สิน

อาชญากรรมแบบไร้ตัวตนซึ่งแบ่งเป็นหลายประเภทและวิธีการนั้น อาจส่งผลกระทบในมิติที่แตกต่างกัน ในส่วนผลกระทบต่อทรัพย์สินของเหยื่อในระดับบุคคล เช่น [75] องค์กรอาชญากรรมที่โจรกรรมทรัพย์สินทางอิเล็กทรอนิกส์ องค์กรอาชญากรรมที่ทำการฉ้อโกงประชาชนในวงกว้าง

9.6.3 ผลกระทบทางเศรษฐกิจ

นอกจากความเสียหายต่อทรัพย์สินของบุคคลที่ตกเป็นเหยื่ออันเป็นการพิจารณาในระดับบุคคลหรือเอกชนแล้ว อาชญากรรมแบบไร้ตัวตนยังสามารถส่งผลกระทบต่อทรัพย์สินในระดับมหภาคหรือเศรษฐกิจด้วย เช่น ผลกระทบต่อผลิตภัณฑ์มวลรวมประชาชาติ (Gross National Product หรือ GNP)[76]

9.6.4 ผลกระทบระดับมหภาคในหลายมิติ

อาชญากรรมไซเบอร์แบบไร้ตัวตน บางกรณีโดยเฉพาะอย่างยิ่งกรณีที่กระทำต่อเป้าหมายคอมพิวเตอร์หรือข้อมูลขององค์กรที่มีลักษณะเป็นโครงสร้างพื้นฐาน การให้บริการสาธารณะ หน่วยงานรัฐ บริษัทขนาดใหญ่ ฯลฯ อาจส่งผลกระทบอย่างกว้างระดับมหภาค ในหลายมิติ เช่น เศรษฐกิจ ความปลอดภัยของประชาชน คุณภาพและการดำรงชีวิตประจำวันของประชาชน เช่น

ตัวอย่าง กลุ่มแฮกเกอร์ที่ไม่สามารถระบุตัวตนทำการโจมตีระบบโครงสร้างพื้นฐานด้านพลังงาน ในเดือนพฤษภาคม ค.ศ. 2021 บริษัท “Colonial Pipeline” ผู้ดำเนินการท่อส่งน้ำมันในสหรัฐอเมริกา ปิดระบบ

---

[75] Lynne D. Roberts, “Cyber Victimization,” in Handbook of Research on Technoethics, ed. Rocci Luppicini (IGI Global, 2009), pp. 577-579.

[76] Robin T. Naylor, “Wages of Crime: Black Markets,” in Illegal Finance, and the Underworld Economy (Cornell University Press, 2004), pp. 126-128.

คอมพิวเตอร์ที่ควบคุมการส่งน้ำมันหลังจากถูกกลุ่มแฮกเกอร์ที่ไม่ทราบตัวตนทำการเจาะระบบ โจรกรรมข้อมูล ซึ่งการปิดระบบดังกล่าวส่งผลกระทบในวงกว้างทั้งผู้บริโภคทั่วไปและผู้ประกอบการที่ต้องใช้น้ำมัน[77]

9.6.5 ผลกระทบเชิงความเสียหายในแง่อื่นของบุคคล

นอกจากความเสียหายต่อทรัพย์สินและความปลอดภัยของระบบหรือข้อมูลคอมพิวเตอร์แล้ว งานวิชาการได้จำแนกผลกระทบของอาชญากรรมคอมพิวเตอร์ว่า ยังอาจส่งผลกระทบเกี่ยวกับบุคคล (Cyber-crimes against person) ในแง่อื่นเช่น ผลกระทบต่อชื่อเสียง หรือจิตใจ [78] นอกจากนี้ยังอาจส่งผลกระทบต่อความปลอดภัยทางกายภาพหรือสุขภาพของบุคคลด้วย โดยเฉพาะอย่างยิ่งอาชญากรรมแบบไร้ตัวตนที่โจมตีระบบคอมพิวเตอร์ที่เกี่ยวข้องกับการดูแลสุขภาพ เช่น

ตัวอย่าง หน่วยงานรักษาความมั่นคงปลอดภัยไซเบอร์ของสหรัฐอเมริกา (CISA) แจ้งเตือนมัลแวร์หลายชนิดที่ตรวจพบว่าแฮกเกอร์นำมาใช้เรียกค่าไถ่โรงพยาบาล เช่น “TrickBot” “BazarLoader”[79] การโจมตีแบบเรียกค่าไถ่ดังกล่าวในหลายกรณีไม่สามารถระบุตัวตนของอาชญากรได้ จะเห็นได้ว่า การโจมตีระบบคอมพิวเตอร์ของโรงพยาบาลอาจกระทบต่อการดูและรักษาผู้ป่วยซึ่งเป็นผลกระทบในแง่สุขภาพและความปลอดภัยของบุคคล

10. แนวคิดและทฤษฎีที่เกี่ยวข้องกับการบังคับใช้กฎหมาย

10.1 แนวคิดความร่วมมือระหว่างประเทศและแนวคิดความช่วยเหลือระหว่างประเทศในทางอาญา

ความช่วยเหลือระหว่างประเทศในทางอาญา หมายถึง ความร่วมมือในการดำเนินการช่วยเหลือในด้านต่างๆ ในการดำเนินคดีอาญา ตั้งแต่การสืบสวน สอบสวน การสืบพยานบุคคลและการสอบปากคำบุคคล การจัดหาเอกสาร บันทึก และพยานหลักฐาน การปฏิบัติตามคำร้องในการค้น การยึด การสืบหาตัวบุคคล การให้ความช่วยเหลือเกี่ยวกับการดำเนินการริบทรัพย์สิน ตลอดจนถึงการบังคับโทษตามคำพิพากษา หรือมีความหมาย

---

[77] Bloomberg News. Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom. Bloomberg News [Online], 13 May 2021 Available from: https://www.bloomberg.com/news/articles/2021-05-13/

[78] Lynne D. Roberts, “Cyber Victimization,” in Handbook of Research on Technoethics, ed. Rocci Luppicini (IGI Global, 2009), pp. 577-579.

[79] Cybersecurity and Infrastructure Security Agency, Alert (AA20-302A): Ransomware Activity Targeting the Healthcare and Public Health Sector (20 November 2020)

ครอบคลุมกว้างขวางเกี่ยวกับการดำเนินคดีอาญา ไม่ว่าจะเป็นการส่งผู้ร้ายข้ามแดน (Extradition) การโอนตัวนักโทษ (Transfer of Sentenced Persons) และการให้ความช่วยเหลือซึ่งกันและกันในเรื่องทางอาญา (Mutual Assistance in Criminal Matters)

แนวคิดความร่วมมือระหว่างประเทศ (International Cooperation) มีพื้นฐานอยู่บนหลักความสัมพันธ์ระหว่างประเทศที่มองว่าเวทีระหว่างประเทศไม่มีรัฐใดที่มีอำนาจอธิปไตยอันสมบูรณ์ หากแต่ต้องเอื้ออาทรช่วยเหลือซึ่งกันและกันเพื่อลดความขัดแย้ง และแบ่งปันผลประโยชน์ร่วมกันจึงจะทำให้แต่ละประเทศดำรงอยู่ได้อย่างสงบสุข[80] โดยแนวคิดนี้ถือได้ว่าเป็นแนวคิดตามสำนักเสรีนิยมสมัยใหม่ (Neo liberalism) ซึ่งมีรายละเอียดดังต่อไปนี้

- การขยายตัวของความสัมพันธ์ระหว่างประเทศสามารถทำได้โดยการขยายความร่วมมือระหว่างประเทศ ทั้งการขยายเครือข่ายความสัมพันธ์ระหว่างรัฐ และตัวแสดงที่ไม่ใช่รัฐ[81]
- การจัดตั้งสถาบันระหว่างประเทศช่วยให้รัฐสามารถแก้ไขปัญหาต่างๆ โดยสันติ
- สันติภาพและความร่วมมือเกิดขึ้นภายใต้เครือข่าย ความเชื่อมโยง และความสัมพันธ์ในหลากหลายรูปแบบ

สำนักเสรีนิยมสมัยใหม่นี้ได้รับการพัฒนาให้สอดคล้องกับการปรากฏและการแพร่กระจายของสภาวะโลกาภิวัตน์ โดยมีนักคิดคนสำคัญ คือ โรเบิร์ต โคเฮน (Robert Keohane) และโจเซฟ ไนย์ (Joseph Nye) ได้เสนอแนวคิดว่า ในโลกที่เต็มไปด้วยการพึ่งพาอย่างสลับซับซ้อนของตัวแสดงต่างๆ (Complex Interdependence) การสร้างกรอบความร่วมมือที่หลากหลายจัดเป็นองค์ประกอบสำคัญในการจัดระเบียบโลก การบูรณาการระหว่างประเทศ กฎหมายระหว่างประเทศ เพื่อให้สอดคล้องกับกระบวนการโลกาภิวัตน์ โดยเน้นการมองโครงสร้างระหว่างประเทศในบริบทของความร่วมมือและความสัมพันธ์ในหลากหลายมิติ มากกว่ามองแค่การจัดสรรอำนาจระหว่างกลุ่มประเทศต่างๆ[82]

---

[80] ชิตพล กาญจนกิจ, ความท้าทายของรัฐอาเซียนในการต่อต้านอาชญากรรมข้ามชาติ, วารสารสังคมศาสตร์ ปีที่ 46 ฉบับที่ 1 (2559), หน้า 61, http://www.library.polsci.chula.ac.th/journal.

[81] ตัวแสดงที่ไม่ใช่รัฐ ยกตัวอย่างเช่น องค์การระหว่างรัฐ (The Inter-Governmental Organizations: IGOs) เช่น องค์กรสหประชาชาติ (The United Nations: UN), บรรษัทข้ามชาติ (Multinational Corporations: MNCs), องค์กรพัฒนาเอกชน (The Non-Governmental Organizations: NGOs) เป็นต้น

[82] จุฑาทิพ คล้ายทับทิม, หลักความสัมพันธ์ระหว่างประเทศ, พิมพ์ครั้งที่ 4 (กรุงเทพมหานคร: สำนักพิมพ์มหาวิทยาลัยเกษตรศาสตร์, 2559), หน้า 46-47.

ทั้งนี้ รูปแบบของแนวคิดความร่วมมือระหว่างประเทศที่เห็นเป็นรูปธรรมปรากฏตามความร่วมมือระหว่างประเทศทั้งในระดับทวิภาคีและพหุภาคีที่เกี่ยวข้องกับองค์กรอาชญากรรมข้ามชาติ ยกตัวอย่างเช่น สหภาพยุโรป (European Union: EU) ซึ่งถือว่าเป็นตัวอย่างความร่วมมือในปราบปรามองค์กรอาชญากรรมข้ามชาติเป็นภูมิภาคแรก และมีประสิทธิภาพอย่างมาก กล่าวคือ สหภาพยุโรปได้ตั้ง ตำรวจสากลยุโรป (Europol) ขึ้นเมื่อเดือนตุลาคม ค.ศ. 1998 โดยมีวัตถุประสงค์ที่สำคัญคือ เพื่อเพิ่มประสิทธิภาพ และความร่วมมือของเจ้าหน้าที่รัฐในประเทศภาคีต่างๆ ในการป้องกัน และปราบปรามการก่อการร้าย การค้ายาเสพติด และอาชญากรรมข้ามชาติร้ายแรงในรูปแบบอื่นที่มีลักษณะเป็นองค์กรอาชญากรรมข้ามชาติอันมีลักษณะความเกี่ยวพันกับประเทศอื่นตั้งแต่ 2 ประเทศขึ้นไป โดยหน้าที่หลักของตำรวจสากลยุโรปมีดังนี้[83]

1) การอำนวยความสะดวก ทำให้กระบวนการดำเนินการมีความรวดเร็วมากขึ้น โดยดำเนินการให้มีการแลกเปลี่ยนข้อมูลผ่านช่องทางการติดต่อโดยตรงกับเจ้าหน้าที่ผู้บังคับใช้กฎหมายที่เกี่ยวข้องหรือหน่วยงานของรัฐที่เกี่ยวข้องของประเทศที่รับคำร้องขอ
2) รับ ตรวจสอบ และวิเคราะห์ข้อมูลที่ได้รับจากหน่วยงานต่างๆ รวมถึงการทำรายงานประจำปีเกี่ยวกับองค์กรอาชญากรรมข้ามชาติ โดยข้อมูลที่นำมาทำรายงานประจำปีเป็นข้อมูลที่ได้มาจากเจ้าหน้าที่ของรัฐที่เป็นตัวแทนจากประเทศภาคีต่างๆ นอกจากนั้น ในรายงานประจำปีที่พิเศษคือจะประกอบด้วยข้อแนะนำแก่รัฐภาคีอันได้มาจากการวิเคราะห์ข้อมูล
3) รายงานต่อเจ้าหน้าที่รัฐของประเทศภาคีต่างๆ ให้ทราบถึงข้อมูลที่จะเชื่อมโยง ระบุถึงฐานความผิดทางอาญาต่างๆ
4) ให้การช่วยเหลือเจ้าหน้าที่รัฐของประเทศภาคีต่างๆ ในการสืบสวน สอบสวนคดี โดยการส่งข้อมูลที่เกี่ยวข้องกับคดีไปยังหน่วยงานต่างๆ ของประเทศภาคีแต่ละประเทศ
5) รับข้อมูลจากระบบคอมพิวเตอร์เพื่อนำข้อมูลที่เกี่ยวข้องมาเก็บรวบรวมไว้ ซึ่งข้อมูลในที่นี้หมายถึง ข้อมูลเกี่ยวกับผู้ต้องสงสัยที่อาจเป็นอาชญากรข้ามชาติเป็นรายบุคคล และข้อมูลที่เป็นประโยชน์เกี่ยวข้องกับการสืบสวนคดี
6) ให้คำปรึกษา การวิจัยผ่านการฝึกฝนแก่เจ้าหน้าที่ขององค์กรรัฐของประเทศภาคีต่าง ๆ ไม่ว่าจะเป็นการใช้เครื่องมือ หรืออุปกรณ์ที่ใช้ในการสืบสวน สอบสวน เทคนิคที่ใช้ในการตรวจพิสูจน์

---

[83] Matti Joutsen, International Cooperation against Transnational Organized Crime: The Practical Experience of the European Union, p. 396-397, Retrived 16 April 2019, https://www.unafei.or.jp/publications/pdf/RS_No59/No59_29VE_Joutsen3.pdf.

หลักฐานของเจ้าหน้าที่ตำรวจ ตลอดจนอบรมเกี่ยวกับขั้นตอนหรือกระบวนการในการดำเนินการสืบสวน สอบสวนของเจ้าหน้าที่ตำรวจเกี่ยวกับคดีองค์กรอาชญากรรมข้ามชาติ อีกทั้ง อบรมถึงกลยุทธที่มีประสิทธิภาพเกี่ยวกับการนำทรัพยากรที่มีอยู่ในประเทศของตนมาใช้ในการดำเนินงานได้อย่างมีประสิทธิภาพ

10.2 แนวคิดเกี่ยวกับองค์กรอาชญากรรมข้ามชาติตามอนุสัญญาสหประชาชาติว่าด้วยการต่อต้านองค์กรอาชญากรรมที่จัดตั้งในลักษณะองค์กร ค.ศ. 2000

ตามอนุสัญญาสหประชาชาติว่าด้วยการต่อต้านองค์กรอาชญากรรมข้ามชาติที่จัดตั้งในลักษณะองค์กร ค.ศ. 2000 ข้อ 2 และ 3 ได้กำหนดนิยามที่เกี่ยวข้องกับองค์กรอาชญากรรมข้ามชาติไว้ดังต่อไปนี้

องค์กรอาชญากรรม หมายถึง กลุ่มที่มีการจัดโครงสร้างของบุคคลสามคนหรือมากกว่า ที่ดำรงอยู่เป็นระยะเวลาหนึ่ง และที่มีการประสานการดำเนินงานระหว่างกันโดยมีเป้าหมายในการกระทำอาชญากรรมร้ายแรงหนึ่งอย่างหรือมากกว่า หรือในการกระทำความผิดตามที่กำหนดไว้ในอนุสัญญานี้ เพื่อให้ได้มาซึ่งผลประโยชน์ทางการเงินหรือผลประโยชน์ทางวัตถุอย่างอื่นไม่ว่าโดยทางตรงหรือทางอ้อม

กลุ่มที่มีการจัดโครงสร้าง หมายถึง กลุ่มที่ไม่ได้จัดตั้งขึ้นโดยความบังเอิญเพื่อกระทำความผิดโดยทันใด และไม่จำเป็นต้องมีการกำหนดบทบาทของสมาชิกอย่างเป็นทางการ ไม่จำเป็นต้องมีความต่อเนื่องของการเป็นสมาชิกหรือมีโครงสร้างที่พัฒนาแล้ว

อาชญากรรมร้ายแรง หมายถึง การกระทำที่เป็นความผิด ซึ่งสามารถลงโทษโดยการทำให้สูญเสียเสรีภาพขั้นสูงสุดเป็นเวลาอย่างน้อย 4 ปี หรือโดยโทษที่รุนแรงกว่าได้

ส่วนลักษณะข้ามชาติได้มีการให้คำนิยามไว้ในอนุสัญญาฯ ข้อ 3 (2) กล่าวคือ “.....ความผิดมีลักษณะข้ามชาติ หาก

(a) ความผิดกระทำในรัฐมากกว่าหนึ่งรัฐ

(b) ความผิดกระทำในรัฐหนึ่ง แต่มีส่วนที่สำคัญของการเตรียมการ การวางแผน การสั่งการ หรือการควบคุมเกิดขึ้นในอีกรัฐหนึ่ง

(c) ความผิดกระทำในรัฐหนึ่ง แต่เกี่ยวข้องกับองค์กรอาชญากรรมซึ่งเกี่ยวข้องกับกิจกรรมที่เป็นความผิดอาญาในรัฐมากกว่าหนึ่งรัฐ หรือ

(d) ความผิดกระทำในรัฐหนึ่งแต่มีผลกระทบอย่างสำคัญในอีกรัฐหนึ่ง”

ดังนั้น คำว่า “องค์กรอาชญากรรมข้ามชาติ” จึงหมายความถึง กลุ่มของบุคคลตั้งแต่ 3 คนขึ้นไป ที่ไม่ได้จัดตั้งขึ้นโดยความบังเอิญเพื่อกระทำความผิดโดยทันใด และไม่จำเป็นต้องมีการกำหนดบทบาทของสมาชิกอย่างเป็นทางการ ไม่จำเป็นต้องมีความต่อเนื่องของการเป็นสมาชิกหรือมีโครงสร้างที่พัฒนาแล้ว แต่ต้องดำรงอยู่เป็นระยะเวลาหนึ่ง และมีการประสานดำเนินงานระหว่างกัน อันมีเป้าหมายในการกระทำความผิดซึ่งสามารถลงโทษโดยการทำให้สูญเสียเสรีภาพขั้นสูงสุดเป็นเวลาอย่างน้อย 4 ปีหรือโทษที่รุนแรงกว่านั้นอย่างหนึ่งหรือมากกว่า เพื่อให้ได้มาซึ่งผลประโยชน์ทางการเงินหรือผลประโยชน์ทางวัตถุอย่างอื่นไม่ว่าโดยทางตรงหรือทางอ้อม โดยความผิดที่กระทำนั้นได้กระทำในรัฐมากกว่าหนึ่งรัฐ หรือกระทำในรัฐหนึ่ง แต่มีส่วนสำคัญของการเตรียมการ การวางแผน การสั่งการ หรือการควบคุมเกิดขึ้นในอีกรัฐหนึ่ง หรือมีผลกระทบอย่างสำคัญในอีกรัฐหนึ่ง หรือกระทำในรัฐหนึ่งแต่เกี่ยวข้องกับองค์กรอาชญากรรมซึ่งเกี่ยวข้องกับกิจกรรมที่เป็นความผิดอาญาในรัฐมากกว่าหนึ่งรัฐ

โดยองค์การสหประชาชาติได้แบ่งประเภทความผิดของอาชญากรรมข้ามชาติออกเป็น 19 ประเภท ดังนี้[84]

1) การฟอกเงิน
2) การก่อการร้าย
3) การโจรกรรมศิลปวัตถุและทรัพย์สินทางวัฒนธรรม
4) การละเมิดทรัพย์สินทางปัญญา
5) การค้าอาวุธ
6) การจี้บังคับอากาศยาน
7) โจรสลัดในทะเล
8) โจรสลัดบนบก
9) การจับตัวประกัน
10) อาชญากรรมคอมพิวเตอร์

[84] United Nations, Results of the Fourth United Nations Survey of Crime Trends and Operations of Criminal Justice Systems - Interim report prepared by the Secretariat - Addendum, In Ninth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 29 April – 8 May 1995, Cairo Egypt, p. 7, อ้างในชญานิศ ทรัพย์มา, มาตรการทางกฎหมายในการป้องกันและปราบปรามอาชญากรรมข้ามชาติทางด้านสิ่งแวดล้อม: กรณีศึกษาการลักลอบค้าสารทำลายชั้นโอโซน. สารานิพนธ์นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ สถาบันบัณฑิตพัฒนบริหารศาสตร์, กรุงเทพฯ, 2556, หน้า 28.

11) อาชญากรรมสิ่งแวดล้อม

12) การค้ามนุษย์

13) การค้าชิ้นส่วนอวัยวะของมนุษย์

14) การค้ายาเสพติดให้โทษ

15) การฉ้อโกงธนาคาร

16) การแทรกซึมองค์กรธุรกิจ

17) การทุจริตและติดสินบนต่อเจ้าหน้าที่รัฐ

18) การทุจริตและติดสินเจ้าหน้าที่พรรคและผู้แทนจากการเลือกตั้ง

19) ความผิดที่กระทำโดยองค์กรอาชญากรรม

10.3 แนวคิดการใช้เทคนิคการสืบสวนพิเศษตามอนุสัญญาสหประชาชาติเพื่อต่อต้านอาชญากรรมข้ามชาติที่จัดตั้งในลักษณะองค์กร ค.ศ. 2000

เมื่อวันที่ 13 ธันวาคม 2543 ประเทศไทยได้ลงนามเป็นภาคีในอนุสัญญาสหประชาชาติว่าด้วยการต่อต้านอาชญากรรมข้ามชาติที่จัดตั้งในลักษณะองค์กร (United Nations Convention against Transnational Organized Crime) ซึ่งมีผลให้ประเทศไทยต้องแก้ไขกฎหมายที่มีอยู่รวมทั้งตรากฎหมายใหม่เพื่อให้มีมาตรการที่ทันสมัยและเหมาะสมกับการต่อต้านและปราบปรามองค์กรอาชญากรรม ซึ่งในอนุสัญญาฯ ยังได้กำหนดจุดประสงค์ไว้คือ “เพื่อสนับสนุนความร่วมมือในการป้องกันและปราบปรามองค์กรอาชญากรรมข้ามชาติให้มีประสิทธิภาพมากยิ่งขึ้น”

ต่อมาเมื่อวันที่ 17 ตุลาคม 2556 ประเทศไทยได้ยื่นสัตยาบันสารอนุสัญญาสหประชาชาติเพื่อต่อต้านอาชญากรรมที่จัดตั้งในลักษณะองค์กร และพิธีสารเพื่อป้องกันปราบปรามและลงโทษการค้ามนุษย์โดยเฉพาะสตรีและเด็ก ทำให้การเข้าเป็นภาคีอนุสัญญาฯ ของประเทศไทยจะมีผลอย่างสมบูรณ์ ซึ่งจะช่วยให้ประเทศไทยสามารถร่วมมือกับประเทศภาคีอนุสัญญาฯ ซึ่งมีจำนวน 173 ประเทศ ได้มีประสิทธิภาพมากยิ่งขึ้นในการป้องกันและต่อต้านอาชญากรรมข้ามชาติที่จัดตั้งในลักษณะองค์กร

ในอนุสัญญาฯ ได้กำหนดถึงแนวทางของเทคนิคการสืบสวนพิเศษที่จะนำมาใช้ปราบปรามองค์กรอาชญากรรมไว้เป็นหลักเกณฑ์ในข้อ 20 โดยได้ยกตัวอย่างเทคนิคการสืบสวนพิเศษ เช่น การส่งมอบภายใต้การควบคุม (Controlled Delivery) การปฏิบัติการอำพราง (Undercover Operation) การสะกดรอยติดตามและการดักฟังข้อมูลทางอิเล็กทรอนิกส์ (Electronic and other form of surveillance) เป็นต้น และได้กำหนดให้

ประเทศสมาชิกนำเทคนิคการสืบสวนพิเศษดังกล่าวข้างต้นไปปรับใช้ตามกรอบที่กฎหมายภายในของแต่ละประเทศกำหนด เพื่อประโยชน์ในการปราบปรามองค์กรอาชญากรรม

ในข้อ 20 ของอนุสัญญาฯ ได้กำหนดหลักเกณฑ์การนำเทคนิคสืบสวนสอบสวนพิเศษไปปรับใช้กับกฎหมายภายในไว้ สรุปได้ดังนี้

(1) เป็นการกระทำภายใต้หลักการพื้นฐานของระบบกฎหมายภายใน ซึ่งรัฐภาคีต้องใช้มาตรการที่จำเป็นและเหมาะสมเกี่ยวกับการจัดส่งภายใต้การควบคุม หรือการใช้เทคนิคการสืบสวนสอบสวนพิเศษอย่างอื่น เช่น การเฝ้าติดตามโดยใช้เครื่องมืออิเล็กทรอนิกส์หรือการเฝ้าติดตามในรูปแบบอื่นๆ และการปฏิบัติการลับ (การอำพราง) ภายใต้เงื่อนไขที่กำหนดไว้ในกฎหมายภายในของรัฐภาคีโดยเจ้าหน้าที่ผู้มีอำนาจของรัฐภายในดินแดน

(2) รัฐภาคีจะได้รับการส่งเสริมให้ทำความตกลงหรือข้อตกลงทวิภาคีหรือพหุภาคีที่เหมาะสมเพื่อใช้เทคนิคการสืบสวนสอบสวนพิเศษในระดับระหว่างประเทศตามความตกลงหรือข้อตกลงนั้นสอดคล้องกับหลักการความเท่าเทียมกันของอธิปไตยแห่งรัฐและต้องมีการดำเนินการอย่างเคร่งครัดตามข้อกำหนดของความตกลงหรือข้อตกลงนั้น

(3) ในกรณีที่ไม่มีความตกลงหรือการจัดการตามข้อ 1.2 การใช้เทคนิคการสืบสวนสอบสวนพิเศษในระดับระหว่างประเทศจะกระทำเป็นรายกรณีไป และอาจนำข้อตกลงและความเข้าใจระหว่างกันในเรื่องทางการเงินมาพิจารณาด้วย โดยคำนึงถึงเขตอำนาจของรัฐภาคีที่เกี่ยวข้อง

(4) การจัดส่งภายใต้การควบคุมในระดับระหว่างประเทศอาจให้รวมถึงวิธีการ เช่น การสกัดและอนุญาตให้สิ่งของยังคงสภาพเดิมหรือมีการเคลื่อนย้ายหรือสับเปลี่ยนทั้งหมดหรือบางส่วนด้วยความยินยอมของรัฐภาคีที่เกี่ยวข้อง

นอกจากนี้ตามข้อ 20 ของอนุสัญญาฯ ยังได้กำหนดตัวอย่าง เทคนิคการสืบสวนสอบสวนพิเศษไว้หลายประการ

ประการแรก คือ การจัดส่งภายใต้การควบคุม (Controlled Delivery) ซึ่งหมายถึง วิธีการอนุญาตให้ของผิดกฎหมายหรือต้องสงสัยผ่านออกไปจากผ่านหรือเข้าไปสู่เขตแดนของรัฐหนึ่งหรือมากกว่ารัฐหนึ่งโดยการรับรู้และอยู่ภายใต้การกำกับดูแลของเจ้าหน้าที่ผู้มีอำนาจ เพื่อการสืบสวนสอบสวนความผิดและเพื่อการระบุตัวบุคคลที่เกี่ยวข้องในการกระทำความผิดนั้นที่มีการใช้อย่างมาก คือการส่งยาเสพติดทำให้สามารถดำเนินการได้กับบุคคลในองค์กรได้ทุกระดับ นอกจากนั้นนำมาใช้กับการค้าอาวุธหรือยานพาหนะที่ถูกขโมย และประโยชน์

ในการรวบรวมพยานหลักฐานระหว่างการสืบสวนโดยได้รับอนุญาตตามที่กฎหมายบัญญัติ แต่ต้องดำเนินการอย่างโปร่งใส เทคโนโลยี ความเท่าเทียมกันและความร่วมมือระหว่างประเทศ

ประการที่สอง คือ การปฏิบัติการลับ (Undercover Operation) โดยการใช้เจ้าหน้าที่ปฏิบัติการลับที่มีประสบการณ์สืบสวนโดยการอำพรางสถานะ เพื่อให้ได้รับข้อสารสนเทศและการรวบรวมพยานหลักฐานเกี่ยวกับองค์กรอาชญากรรมที่มีความสัมพันธ์กันโดยการแทรกซึม และมีการควบคุมการปฏิบัติการในช่วงระยะเวลาที่กำหนดไว้ แต่เป็นวิธีการที่อันตรายและเลือกใช้เป็นวิธีการสุดท้ายของการสืบสวนซึ่งต้องกระทำด้วยความระมัดระวัง โดยวิธีการร้องขอและได้รับอนุญาตจากผู้มีอำนาจของหน่วยงานปฏิบัติการหรือพนักงานอัยการหรือศาล

ประการที่สาม คือ การเฝ้าติดตามโดยใช้เครื่องมืออิเล็กทรอนิกส์ (Electronic Surveillance) เช่น การดักฟังโทรศัพท์ การดักการติดต่อสื่อสาร กระทำได้โดยชอบภายใต้กฎหมายให้อำนาจไว้โดยการยื่นคำร้องขอภายใต้เงื่อนไขของกฎหมายที่กำหนดเพื่อคุ้มครองสิทธิเสรีภาพของประชาชนทั่วไป โดยได้รับอนุญาตจากผู้มีอำนาจ เช่น ผู้พิพากษา พนักงาน อัยการ รัฐมนตรี เป็นต้น และไม่มีการแทรกแซงในเรื่องส่วนตัว ซึ่งพยานหลักฐานที่ได้จากวิธีการนี้มีความเชื่อถือได้และเป็นประโยชน์ต่อเจ้าหน้าที่ในการได้รับข้อมูลสารสนเทศและข่าวสารจากการกระทำผิดกฎหมายทำให้เกิดความชัดเจน เช่น การลักลอบค้ายาเสพติด การฟอกเงิน การค้าประเวณี การพนัน การลักพาตัวเพื่อเรียกค่าไถ่ เป็นต้น

ดังนั้น จากการที่ประเทศไทยลงนามเป็นภาคีในอนุสัญญาสหประชาชาติเพื่อต่อต้านอาชญากรรมข้ามชาติที่จัดตั้งในลักษณะองค์กร จึงจำต้องปฏิบัติตามพันธกรณีของอนุสัญญาฯ เพื่อให้การปฏิบัติตามอนุสัญญาฯ เป็นไปอย่างได้ผล จึงมีแนวคิดที่จะนำเทคนิคการสืบสวนพิเศษต่าง ๆ นี้ บัญญัติไว้ในกฎหมายภายในเพื่อให้มีผลรองรับตามกฎหมายต่อไป

บทที่ 3
กฎหมายที่กำหนดความผิดเกี่ยวกับอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ของประเทศไทยและต่างประเทศ

1. กฎหมายที่กำหนดความผิดเกี่ยวกับอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ของประเทศไทย

เนื่องจากในประเทศไทยยังไม่มีกฎหมายเฉพาะที่กำหนดฐานความผิดเกี่ยวกับอาชญากรรมไร้ตัวตน (Anonymous computer crime) แต่มีกฎหมายที่เกี่ยวข้องหลายฉบับซึ่งจะชี้ให้เห็นดังต่อไปนี้

1.1 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม

พระราชบัญญัตินี้เป็นกฎหมายที่เกี่ยวข้องโดยตรงกับอาชญากรรมคอมพิวเตอร์ แต่ไม่มีฐานความผิดหรือหลักการที่ระบุถึง“อาชญากรรมคอมพิวเตอร์แบบไร้ตัวตนหรือนิรนาม” (Anonymous computer crime) ไว้โดยเฉพาะ อย่างไรก็ตาม ฐานความผิดต่างๆ ที่มีอยู่มีขอบเขตและองค์ประกอบที่เกี่ยวข้องกับอาชญากรรมแบบไร้ตัวตน ในหัวข้อนี้จะวิเคราะห์การปรับใช้ฐานความผิดต่างๆ ตามพระราชบัญญัตินี้กับอาชญากรรมแบบไร้ตัวตน โดยอาศัยกรอบแนวคิดทฤษฎีที่ได้ศึกษาในบทที่ 1 คือ แนวคิดเกี่ยวกับความปลอดภัยของระบบหรือข้อมูลคอมพิวเตอร์ (Computer security) และแนวคิดเกี่ยวกับการจำแนกกระบวนการหรือขั้นตอนของอาชญากรรมแบบไร้ตัวตน ออกเป็นการกระทำสองส่วนคือ การกระทำหลักและการกระทำในส่วนปกปิดตัวตน จึงพบว่า ฐานความผิดที่เกี่ยวข้องหรือส่งผลกระทบต่อความปลอดภัยทางคอมพิวเตอร์คือมาตรา 5 ถึงมาตรา 11 อาจปรับใช้กับอาชญากรรมแบบไร้ตัวตนโดยจะวิเคราะห์การปรับใช้เป็นรายฐานแยกระหว่างการกระทำหลักและการกระทำในส่วนปกปิดตัวตน ดังต่อไปนี้

(1) ฐานความผิดการเข้าถึงระบบโดยมิชอบ (มาตรา 5)

ฐานนี้สามารถปรับใช้กับการกระทำหลักของอาชญากรรมแบบไร้ตัวตน เนื่องจากเป้าหมายหลักของอาชญากรรมประเภทนี้คือการกระทำต่อระบบและข้อมูลจึงต้องมีการเข้าถึงระบบที่มีมาตรการป้องกันซึ่งจะเป็นความผิดมาตรา 5

ฐานนี้สามารถปรับใช้กับการกระทำในส่วนปกปิดตัวตนของอาชญากรรมแบบไร้ตัวตน โดยเฉพาะในกรณีที่อาชญากรใช้วิธีการเข้าถึงอุปกรณ์หรือระบบของผู้อื่นเพื่อใช้ปกปิดตัวตนของตนเอง เช่น การเข้าถึงบัญชี

ใช้งานหรือจดหมายอิเล็กทรอนิกส์ของผู้อื่นและนำไปใช้ในการเข้าถึงระบบคอมพิวเตอร์อันเป็นเป้าหมายของการโจรกรรม

สรุปได้ว่า การกระทำของอาชญากรรมแบบไร้ตัวตนทั้งในส่วนของการกระทำหลักและการกระทำอันเป็นการปกปิดตัวตนสามารถเกี่ยวข้องกับองค์ประกอบความผิดมาตรา 5

(2) ฐานความผิดการเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ (มาตรา 7)

ฐานนี้สามารถปรับใช้กับการกระทำหลักของอาชญากรรมแบบไร้ตัวตน เนื่องจากเป้าหมายหลักของอาชญากรรมประเภทนี้คือการกระทำต่อระบบและข้อมูล ดังนั้น โดยทั่วไปจึงมีลักษณะการกระทำที่เข้าองค์ประกอบของการเข้าถึงข้อมูลคอมพิวเตอร์ของผู้อื่นที่มีมาตรการป้องกัน เช่น การโจรกรรมข้อมูลทางการเงิน การโจรกรรมข้อมูลการค้า

ฐานนี้สามารถปรับใช้กับการกระทำในส่วนปกปิดตัวตนของอาชญากรรมแบบไร้ตัวตน โดยเฉพาะในกรณีที่อาชญากรใช้วิธีการโจรกรรรมข้อมูลระบุตัวของผู้อื่นเพื่อใช้ปกปิดการกระทำของตน เช่น การแฮกเข้าระบบอีเมล์ของเหยื่อและนำไปใช้ส่งมัลแวร์เพื่อโจมตีระบบของผู้อื่น การเข้าถึงข้อมูลส่วนบุคคลของลูกค้าที่เปิดบัญชีธนาคารและนำบัญชีดังกล่าวไปใช้กระทำผิดทางระบบคอมพิวเตอร์เพื่อให้เข้าใจว่าเป็นการกระทำของเจ้าของบัญชี

(3) ฐานความผิดเปิดเผยมาตรการป้องกันการเข้าถึง (มาตรา 6)

ฐานนี้สามารถปรับใช้กับการกระทำหลักของอาชญากรรมแบบไร้ตัวตน ในกรณีที่การกระทำอันเป็นเป้าหมายหลักมีพฤติกรรมเกี่ยวเนื่องกับการที่บุคคลภายในของเหยื่อทำการเปิดเผยมาตรการป้องกัน เช่น ผู้ดูแลระบบขององค์กรบอกรหัสผ่านให้กับองค์กรอาชญากรรมที่นำไปใช้ในการโจรกรรมข้อมูล ดังนี้ผู้ดูแลระบบจะมีความผิดมาตรา 6

ในส่วนของการกระทำอันเป็นการปกปิดตัวตนนั้น มักเป็นวิธีการทางเทคนิคเพื่อปกปิดร่องรอยซึ่งอาจเป็นความผิดมาตราอื่น เช่น การแก้ไขข้อมูล การเข้าถึงข้อมูลระบุตัวของบุคคลอื่น ดังนั้น โดยทั่วไปแล้วการที่ผู้ดูแลระบบหรือผู้มีหน้าที่เกี่ยวกับมาตรการป้องกันบอกมาตรการป้องกันการเข้าถึงหรือรหัสผ่านให้แก่อาชญากรจะไม่เกี่ยวข้องกับการกระทำเพื่อปกปิดตัวตนในส่วนนี้ แต่ก็อาจเกิดกรณีที่การเปิดเผยมาตรการป้องกันเป็นส่วนหนึ่งของการกระทำเพื่อปกปิดตัวตน เช่น องค์กรอาชญากรรมตกลงกับผู้ดูแลระบบของบริษัทเพื่อให้บอกรหัสผ่านสำหรับเข้าถึงข้อมูลลูกค้า เพื่อนำข้อมูลระบุตัวลูกค้ามาใช้ปกปิดการกระทำผิดของตน ดังนี้ในส่วนของการบอกรหัสผ่านจะเป็นความผิดมาตรา 6

(4) ฐานความผิดดักรับข้อมูลคอมพิวเตอร์ (มาตรา 8)

ฐานนี้สามารถปรับใช้กับการกระทำหลักของอาชญากรรมแบบไร้ตัวตน ในกรณีเป้าหมายหลักคือการโจรกรรมข้อมูลคอมพิวเตอร์ระหว่างการส่ง เช่น การติดตั้งมัลแวร์เพื่อดักรับข้อมูลการใช้จ่ายอิเล็กทรอนิกส์ในเว็บไซต์เป้าหมาย ซึ่งเข้าองค์ประกอบมาตรา 8

ฐานนี้สามารถปรับใช้กับการกระทำในส่วนปกปิดตัวตนของอาชญากรรมแบบไร้ตัวตน ในกรณีที่อาชญากรใช้วิธีการดักรับข้อมูลระบุตัวของผู้อื่นเพื่อนำไปใช้ปกปิดการกระทำของตน เช่น การใช้โปรแกรมดักรับข้อมูลส่วนบุคคลของผู้สมัครใช้บัญชีออนไลน์ขณะกรอกข้อมูลและนำไปใช้แสดงตนในการกระทำความผิดหลักอันเป็นเป้าหมาย

(5) ฐานความผิดแก้ไขเปลี่ยนแปลงข้อมูล (มาตรา 9)

ฐานนี้สามารถปรับใช้กับการกระทำหลักของอาชญากรรมแบบไร้ตัวตน ในกรณีเป้าหมายหลักคือการทำลายหรือแก้ไขเปลี่ยนแปลงข้อมูลเป้าหมาย เช่น การส่งมัลแวร์ไปยังระบบคอมพิวเตอร์เป้าหมายโดยทำให้ข้อมูลเสียหาย องค์กรอาชญากรรมที่ใช้มัลแวร์เรียกค่าไถ่ (Ransomware) ที่ส่งผลให้เกิดการแก้ไขเปลี่ยนแปลงข้อมูลของเหยื่อ

ฐานนี้สามารถปรับใช้กับการกระทำในส่วนปกปิดตัวตน ของอาชญากรรมแบบไร้ตัวตน ในกรณีที่อาชญากรใช้วิธีการปกปิดตัวตนที่ส่งผลให้เกิดการแก้ไขเปลี่ยนแปลงข้อมูล เช่น การปกปิดข้อมูลร่องรอยการสื่อสารที่อาจระบุตัวตนได้โดยวิธีการเข้ารหัส (Encryption) ที่ส่งผลกระทบต่อการแก้ไขเปลี่ยนแปลงข้อมูล

(6) ฐานความผิดขัดขวางการทำงานของระบบ (มาตรา 10)

ฐานนี้สามารถปรับใช้กับการกระทำหลักของอาชญากรรมแบบไร้ตัวตน ในกรณีเป้าหมายหลักคือการทำให้ระบบหรือเครือข่ายเกิดการระงับหรือขัดข้อง เช่น การโจมตีแบบทำให้ระบบปฏิเสธบริการ (DDOS attack)

ฐานนี้สามารถปรับใช้กับการกระทำในส่วนปกปิดตัวตนของอาชญากรรมแบบไร้ตัวตน ในกรณีที่อาชญากรใช้วิธีการปกปิดตัวตนที่ส่งผลให้เกิดการแก้ไขเปลี่ยนแปลงข้อมูล เช่น การปกปิดข้อมูลร่องรอยการสื่อสารที่อาจระบุตัวตนได้โดยวิธีการเข้ารหัส (Encryption) ที่ส่งผลกระทบต่อการแก้ไขเปลี่ยนแปลงข้อมูล

(7) ฐานความผิดสแปม (มาตรา 11)

สำหรับความผิดมาตรา 11 วรรคหนึ่ง ซึ่งมีองค์ประกอบคือการส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์อันกระทบต่อการทำงานของระบบ เป็นความผิดต่อระบบหรือข้อมูลคอมพิวเตอร์ โดยฐาน

นี้สามารถปรับใช้กับการกระทำหลักของอาชญากรรมแบบไร้ตัวตน ในกรณีที่ใช้วิธีการโจมตีเป้าหมายด้วยการส่งข้อมูลหรือจดหมายอิเล็กทรอนิกส์ เช่น การส่งเมล์จำนวนมากที่มีไฟล์มัลแวร์ติดไปด้วยเพื่อโจมตีเหยื่อ

ฐานนี้สามารถปรับใช้กับการกระทำในส่วนปกปิดตัวตนของอาชญากรรมแบบไร้ตัวตน เช่น การส่งเมล์จำนวนมากไปโจมตีเหยื่อโดยใช้วิธีการทางเทคนิคเพื่อปกปิดแหล่งที่มาของการส่งซึ่งจะเข้าองค์ประกอบมาตรา 11 นอกจากนี้ หากปรากฏว่ามีการใช้วิธีเข้าถึงบัญชีการใช้งานของผู้อื่นเพื่อใช้ในการส่งเมล์ก็จะเป็นความผิดฐานเข้าถึงระบบโดยมิชอบตามมาตรา 5 ด้วย

(8) ฐานความผิดฉ้อโกงทางคอมพิวเตอร์

ความผิดเกี่ยวกับการฉ้อโกงทางคอมพิวเตอร์ (Computer fraud) ตามมาตรา 14 (1) มีองค์ประกอบที่กว้างแบ่งเป็นการกระทำได้สองกลุ่มคือ กลุ่มการกระทำที่ไม่ส่งผลกระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ กล่าวคือการใช้ข้อมูลเท็จเพื่อหลอกลวงเป้าหมายคือการรับรู้ของบุคคลและกลุ่มการกระทำที่ใช้วิธีการทางเทคนิคเพื่อหลอกลวงการทำงานอัตโนมัติของระบบจัดเป็นการกระทำที่กระทบต่อความปลอดภัยทางคอมพิวเตอร์ [85] เมื่อพิจารณาอาชญากรรมแบบไร้ตัวตนจะพบว่า

ฐานนี้สามารถปรับใช้กับการกระทำหลักของอาชญากรรมแบบไร้ตัวตน ในกรณีเป้าหมายหลักคือการกระทำผิดในลักษณะฉ้อโกงทางคอมพิวเตอร์ เช่น องค์กรอาชญากรรมที่ส่งข้อมูลเท็จในแง่มุมต่างๆเพื่อหลอกลวงทรัพย์สินของเหยื่อ (Scam) และในกรณีที่ความผิดหลักคือการฉ้อโกงทางคอมพิวเตอร์โดยใช้ข้อมูลเท็จการที่อาชญากรใช้วิธีปกปิดตัวตนหรือปลอมตัวเป็นบุคคลอื่นเพื่อการหลอกลวงก็เข้าข่ายความผิดมาตรา 14 (1) เนื่องจากเป็นการนำข้อมูลปลอมหรือเท็จเข้าสู่ระบบได้เช่นเดียวกัน ฐานนี้จึงครอบคลุมทั้งการกระทำความผิดหลักและการกระทำเพื่อปกปิดตัวตน นอกจากนี้ ในส่วนของการกระทำเพื่อปกปิดตัวตนยังอาจเข้าข่ายความผิดอื่นแล้วแต่รูปแบบของการกระทำ เช่น การเข้าถึงข้อมูลระบุตัวตนของบุคคลโดยมิชอบและนำมาใช้หลอกลวงทรัพย์สินบุคคลอื่น เป็นความผิดมาตรา 7 ด้วย

จากการนำฐานความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาวิเคราะห์กับอาชญากรรมแบบไร้ตัวตนพบว่า แม้พระราชบัญญัตินี้ไม่กำหนดฐานความผิดเฉพาะแต่เมื่อนำพฤติกรรมและรูปแบบของอาชญากรรมไร้ตัวตนที่จำแนกเป็นการกระทำสองส่วนมาพิจารณาตามองค์ประกอบความผิดเกี่ยวกับความปลอดภัยของระบบคอมพิวเตอร์มาตรา 5 - 11 และมาตรา 14 (1) ในส่วนที่

---

[85] คณาธิป ทองรวีวงศ์ . กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ เล่ม 2 : ภาคการฉ้อโกงทางคอมพิวเตอร์ สแปม และความผิดอื่น , กรุงเทพ:สำนักพิมพ์นิติธรรม, , (2564)

เกี่ยวกับการปลอมแปลงข้อมูลนั้น พบว่า สามารถปรับใช้กับอาชญากรรมแบบไร้ตัวตนที่มีรูปแบบหลากหลายทั้งสองส่วนของการกระทำ สำหรับมาตรา 14 (1) ในส่วนที่ไม่เกี่ยวข้องกับผลกระทบต่อระบบหรือข้อมูลคอมพิวเตอร์นั้น ก็อาจปรับใช้ได้กับอาชญากรรมแบบไร้ตัวตนสำหรับกรณีที่ปกปิดตัวตนโดยลักษณะของการนำข้อมูลเท็จเข้าสู่ระบบ จากการวิเคราะห์การปรับใช้ฐานความผิดรายมาตราข้างต้นสามารถสรุปเป็นตารางดังต่อไปนี้

ฐานความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์	**คุณลักษณะของความมั่นคงปลอดภัยทางคอมพิวเตอร์**			**อาชญากรรมคอมพิวเตอร์แบบไร้ตัวตน**	
	ความลับ (Confidentiality)	**บูรณภาพ (Integrity)**	**ความพร้อมใช้ (Availability)**	**การกระทำหลักอันเป็นเป้าหมาย**	**การกระทำในส่วนปกปิดตัวตน**
การเข้าถึงระบบโดยมิชอบ (มาตรา 5)	✓			✓	✓
การเปิดเผยมาตรการป้องกันการเข้าถึงระบบ (มาตรา 6)	✓			✓	✓
การเข้าถึงข้อมูลโดยมิชอบ (มาตรา 7)	✓			✓	✓
การดักรับข้อมูล (Interception / Eavesdrop) (มาตรา 8)	✓			✓	✓
การแก้ไขเปลี่ยนแปลงข้อมูล (มาตรา 9)		✓		✓	✓
การขัดขวางการทำงานของระบบหรือการแทรกแซงระบบ (System interference) เช่น DOS (มาตรา 10)			✓	✓	✓
สแปม (Spam) (มาตรา 11 วรรคแรก)			✓	✓	✓
มาตรา 12 (เหตุเพิ่มโทษกรณีความผิดมาตรา 5-11 ที่กระทำต่อข้อมูลหรือระบบคอมพิวเตอร์บางลักษณะ)	✓	✓	✓	✓	✓
การฉ้อโกงทางคอมพิวเตอร์ตามมาตรา 14 (1))	ขึ้นอยู่กับวิธีการกระทำ	ขึ้นอยู่กับวิธีการกระทำ	ขึ้นอยู่กับวิธีการกระทำ	✓	✓

ตารางจำแนกฐานความผิดตามกฎหมายไทยที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์แบบไร้ตัวตน (ประยุกต์จากตารางจำแนกฐานความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ภายใต้กรอบแนวคิดความมั่นคงปลอดภัยทางสารสนเทศ , คณาธิป ทองรวีวงศ์ ความผิดเกี่ยวกับคอมพิวเตอร์ เล่ม1 : ความผิดต่อความปลอดภัยของระบบและข้อมูลคอมพิวเตอร์ , กรุงเทพ: สำนักพิมพ์นิติธรรม , พิมพ์ครั้งที่ 2 , 2565)

2. กฎหมายระหว่างประเทศที่กำหนดความผิดเกี่ยวกับอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์

หัวข้อนี้จะศึกษากฎหมายระหว่างประเทศในรูปของอนุสัญญาหรือสนธิสัญญาพหุพาคีระหว่างรัฐที่กำหนดองค์ประกอบกฎหมายต้นแบบ (Model law) ที่เกี่ยวข้องกับอาชญากรรมไซเบอร์หรืออาชญากรรมคอมพิวเตอร์ เพื่อศึกษาว่ามีฐานความผิดต้นแบบโดยเฉพาะสำหรับอาชญากรรมแบบไร้ตัวตนหรือไม่ อย่างไร

2.1 อนุสัญญาว่าด้วยอาชญากรรมไซเบอร์สหภาพยุโรป (Convention on Cybercrime)

อนุสัญญาอาชญากรรมไซเบอร์ (The Convention on Cybercrime of the Council of Europe) เป็นสนธิสัญญาระหว่างประเทศฉบับแรกที่กำหนดหลักการเกี่ยวกับอาชญากรรมคอมพิวเตอร์ โดยกำหนดองค์ประกอบของฐานความผิดต่างๆ เพื่อเป็นกฎหมายต้นแบบ (Model offence) สำหรับใช้เป็นแนวทางให้ประเทศต่างๆ นำไปบัญญัติฐานความผิดตามกฎหมายภายใน ซึ่งฐานความผิดต้นแบบดังกล่าวแบ่งออกเป็น 4 หมวดหลัก ดังนี้

หมวดที่ 1 ความผิดเกี่ยวกับความปลอดภัยของระบบและข้อมูลสารสนเทศ (Offences against confidentiality, integrity and availability of computer data and system) ประกอบด้วยฐานความผิดต้นแบบดังนี้

- ความผิดฐานเข้าถึงโดยมิชอบ (Illegal access, Article 2) ซึ่งมีองค์ประกอบความผิดต้นแบบว่า “การกระทำโดยเจตนา เข้าถึงระบบคอมพิวเตอร์ทั้งหมดหรือบางส่วนโดยไม่มีสิทธิ” แม้ว่าความผิดต้นแบบนี้จะไม่ได้กำหนดองค์ประกอบเจตนาพิเศษแต่ก็เปิดทางให้ประเทศสมาชิกกำหนดองค์ประกอบนี้ในรายละเอียด กล่าวคือ “ประเทศสมาชิกอาจกำหนดองค์ประกอบสำหรับการกระทำด้วยเจตนาได้มาซึ่งข้อมูลคอมพิวเตอร์หรือด้วยเจตนาไม่สุจริตอื่น”

- ความผิดฐานดักรับข้อมูลคอมพิวเตอร์โดยมิชอบ (Illegal Interception, Article 3) ซึ่งมีองค์ประกอบความผิดต้นแบบว่า “...การกระทำโดยเจตนาและไม่มีสิทธิ ใช้วิธีการทางเทคนิคใดๆ ในการดักรับข้อมูลคอมพิวเตอร์ที่ส่งไปยังหรือส่งจากระบบคอมพิวเตอร์ ที่มิใช่การส่งต่อสาธารณะ”

- ความผิดฐานกระทำต่อข้อมูลโดยมิชอบ (Data interference, Article 4) ซึ่งมีองค์ประกอบความผิดต้นแบบว่า “...การกระทำโดยเจตนา ทำให้เสียหาย ลบ ทำลาย แก้ไข ข้อมูลคอมพิวเตอร์โดยไม่มีสิทธิ”

- ความผิดฐานกระทำต่อระบบคอมพิวเตอร์โดยมิชอบ (System interference, Article 5) ซึ่งมีองค์ประกอบความผิดต้นแบบว่า “... การกระทำโดยเจตนาและไม่มีสิทธิ ขัดขวางการทำงานของระบบคอมพิวเตอร์อย่างร้ายแรง โดยการ นำเข้า ส่ง ทำให้เสียหาย ลบ ทำลาย แก้ไข ข้อมูลคอมพิวเตอร์”

- ความผิดฐานการใช้อุปกรณ์โดยมิชอบ (Misuse of device, Article 6) ซึ่งมีองค์ประกอบความผิดต้นแบบว่า “...การกระทำโดยเจตนาและไม่มีสิทธิ ผลิต ขาย จัดให้มีเพื่อการใช้ นำเข้า เผยแพร่ การครอบครอง หรือทำให้มีขึ้นด้วยประการใด ซึ่งเครื่องมือ โปรแกรมคอมพิวเตอร์ ที่สร้างขึ้นเพื่อกระทำความผิดเกี่ยวกับคอมพิวเตอร์ตามที่ระบุในอนุสัญญานี้”

หมวดที่ 2 ความผิดเกี่ยวกับคอมพิวเตอร์ (Computer-related offences)

ความผิดต้นแบบในหมวดนี้ แบ่งเป็น 2 ฐานความผิดคือ

- การฉ้อโกงหลอกลวงทางคอมพิวเตอร์ (Computer-related fraud, Article 8) ซึ่งมีองค์ประกอบความผิดต้นแบบว่า “...การกระทำโดยเจตนาและไม่มีสิทธิ ก่อให้เกิดความเสียหายแก่ทรัพย์สินผู้อื่นโดยนำข้อมูลคอมพิวเตอร์เข้าสู่ระบบ แก้ไขลบ หรือทำการแทรกแซงการทำงานของระบบคอมพิวเตอร์ ด้วยเจตนาหลอกลวงหรือไม่สุจริต เพื่อให้ได้มาซึ่งผลประโยชน์ทางเศรษฐกิจสำหรับตนหรือผู้อื่นโดยไม่มีสิทธิ”

- การปลอมแปลงทางคอมพิวเตอร์(Computer-related forgery, Article 7) ซึ่งมีองค์ประกอบความผิดต้นแบบว่า “.....การกระทำโดยเจตนา และ โดยไม่มีสิทธิ นำเข้าสู่ระบบ แก้ไข ลบ ข้อมูลคอมพิวเตอร์ อันส่งผลกระทบต่อความถูกต้องแท้จริงของข้อมูลคอมพิวเตอร์ด้วยเจตนาเพื่อให้กระทำการกับข้อมูลดังกล่าวเสมือนกับข้อมูลนั้นเป็นข้อมูลที่ถูกต้องแท้จริง..”

หมวดที่ 3 ความผิดเกี่ยวกับเนื้อหา (Content-related offences)

อนุสัญญานี้กำหนดว่าประเทศสมาชิกควรกำหนดความผิดอาญาสำหรับเนื้อหาที่เป็นสื่อลามกเด็ก (Child pornography , Article 9)

หมวดที่ 4 ความผิดเกี่ยวกับการละเมิดลิขสิทธิ์และสิทธิที่เกี่ยวเนื่อง (Infringement of copyright and related rights) (Article 10)

2.2 บทวิเคราะห์

จากการศึกษาหลักและองค์ประกอบความผิดต้นแบบตามอนุสัญญาว่าด้วยอาชญากรรมไซเบอร์สหภาพยุโรปกับอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ มีข้อวิเคราะห์ดังนี้

- อนุสัญญานี้ไม่จำกัดเฉพาะประเทศสมาชิกสหภาพยุโรป โดยมีประเทศนอกกลุ่มยุโรปให้สัตยาบันด้วย เช่น สหรัฐอเมริกา แคนาดา ออสเตรเลีย ญี่ปุ่น เป็นต้น สำหรับประเทศไทยไม่ได้ให้สัตยาบันและไม่มีพันธกรณีผูกพันตามกฎหมายระหว่างประเทศสำหรับอนุสัญญานี้ อย่างไรก็ตาม เมื่อพิจารณาฐานความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พบว่าหลายฐานสะท้อนถึงองค์ประกอบจากอนุสัญญาดังกล่าว

- จากกรอบแนวคิดทฤษฎีเกี่ยวกับความปลอดภัยทางคอมพิวเตอร์ดังกล่าวในบทที่ 1 เมื่อนำมาพิจารณาฐานความผิดต้นแบบจะพบว่า ฐานความผิดหมวดที่ 1 จัดเป็นความผิดต้นแบบที่มีองค์ประกอบสำหรับอาชญากรรมที่ส่งผลกระทบต่อความปลอดภัยของระบบหรือข้อมูลคอมพิวเตอร์ แต่ในส่วนความผิดต้นแบบหมวดที่ 3 และ 4 เป็นความผิดในกลุ่มเนื้อหา (Content) ซึ่งไม่กระทบต่อการทำงานของระบบและข้อมูลคอมพิวเตอร์ไม่อยู่ในขอบเขตการวิจัยนี้ จึงไม่กล่าวถึงรายละเอียดขององค์ประกอบต้นแบบสำหรับความผิดต้นแบบหมวดที่ 2 โดยหลักแล้วเป็นการกระทำทางคอมพิวเตอร์และอาจส่งผลกระทบในแง่อื่น เช่น ทรัพย์สิน ซึ่งไม่ได้ส่งผลกระทบต่อความปลอดภัยของระบบหรือข้อมูลคอมพิวเตอร์ เช่น การเผยแพร่เนื้อหาข้อมูลหลอกลวงทรัพย์สิน (Scam) แต่ในบางกรณีการฉ้อโกงหลอกลวงมุ่งเป้าหมายไปที่การตอบสนองของระบบหรือโปรแกรมจึงจัดเป็นการกระทำต่อระบบหรือข้อมูลคอมพิวเตอร์ได้

- อนุสัญญาอาชญากรรมไซเบอร์นับเป็นกฎหมายระหว่างประเทศฉบับหลักที่เกี่ยวกับการวางแนวทางกฎหมายต้นแบบสำหรับอาชญากรรมไซเบอร์โดยเฉพาะ แต่พบว่าไม่มีฐานความผิดหรือหลักการที่ระบุถึง “อาชญากรรมคอมพิวเตอร์แบบไร้ตัวตนหรือนิรนาม” (Anonymous computer crime) ไว้โดยเฉพาะ อย่างไรก็ตาม องค์ประกอบความผิดต้นแบบที่ระบุในอนุสัญญาฯมีความเกี่ยวข้องกับอาชญากรรมไร้ตัวตน ทั้งในส่วนของการกระทำหลักและการกระทำในส่วนปกปิดตัวตน โดยเฉพาะอย่างยิ่งความผิดต้นแบบในหมวดที่ 1 ซึ่งแยกวิเคราะห์การปรับใช้ได้ดังนี้

(1) ความผิดฐานเข้าถึงโดยมิชอบ (Illegal access, Article 2)

ฐานนี้กว้างกว่ากฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ของไทย เนื่องจากครอบคลุมรวมทั้งการเข้าถึงระบบ (System) และเข้าถึงข้อมูล (Data) หรือเทียบเคียงได้ว่าครอบคลุมมาตรา 5 และ 7 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งสามารถปรับใช้กับการกระทำหลักของอาชญากรรมแบบไร้ตัวตน ในกรณีเป้าหมายหลักคือการเข้าถึง (Access) ระบบหรือข้อมูลคอมพิวเตอร์ เช่น องค์กรอาชญากรรมที่ใช้วิธีการเจาะระบบหรือแฮกเข้าสู่ระบบหรือข้อมูลของเหยื่อต่างๆ

ฐานนี้สามารถปรับใช้กับการกระทำในส่วนปกปิดตัวตนของอาชญากรรมแบบไร้ตัวตน ในกรณีที่อาชญากรใช้วิธีการปกปิดตัวตนที่มีลักษณะของการเข้าถึงระบบหรือข้อมูล เช่น องค์กรอาชญากรทำการเข้าถึงข้อมูลระบุตัวลูกค้าขององค์กรหนึ่งและนำข้อมูลดังกล่าวไปใช้แสดงตนเพื่อทำธุรกรรมต่างๆทางอิเล็กทรอนิกส์

(2) ความผิดฐานดักรับข้อมูลคอมพิวเตอร์โดยมิชอบ (Illegal Interception, Article 3)

ฐานนี้เทียบเคียงได้กับมาตรา 8 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และสามารถปรับใช้กับการกระทำหลักของอาชญากรรมแบบไร้ตัวตน ในกรณีเป้าหมายหลักคือการดักรับข้อมูลคอมพิวเตอร์ระหว่างการส่ง เช่น การติดตั้งมัลแวร์เพื่อดักรับข้อมูลการใช้จ่ายอิเล็กทรอนิกส์ในเว็บไซต์เป้าหมาย นอกจากนั้น ตัวแบบความผิดฐานนี้สามารถปรับใช้กับการกระทำในส่วนปกปิดตัวตนของอาชญากรรมแบบไร้ตัวตน ในกรณีที่อาชญากรใช้วิธีการดักรับข้อมูลระบุตัวของผู้อื่นเพื่อนำไปใช้ปกปิดการกระทำของตน

(3) ความผิดฐานกระทำต่อข้อมูลโดยมิชอบ (Data interference, Article 4)

ฐานนี้เทียบได้กับมาตรา 8 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 สามารถปรับใช้กับการกระทำหลักของอาชญากรรมแบบไร้ตัวตน ในกรณีเป้าหมายหลักคือการทำลายหรือแก้ไขเปลี่ยนแปลงข้อมูลเป้าหมาย เช่น องค์กรอาชญากรรมที่ใช้วิธีแพร่ไวรัสทางจดหมายอิเล็กทรอนิกส์ทำให้ข้อมูลของผู้อื่นเสียหายในวงกว้าง ฐานนี้สามารถปรับใช้กับการกระทำในส่วนปกปิดตัวตนของอาชญากรรมแบบไร้ตัวตน ในกรณีที่อาชญากรใช้วิธีการปกปิดตัวตนที่ส่งผลให้เกิดการแก้ไขเปลี่ยนแปลงข้อมูล เช่น การแก้ไขเปลี่ยนแปลงรหัสผ่านบัญชีจดหมายอิเล็กทรอนิกส์ของเหยื่อและเข้าควบคุมบัญชีนั้นเพื่อนำมาใช้ส่งไวรัส

(4) ความผิดฐานกระทำต่อระบบคอมพิวเตอร์โดยมิชอบ (System interference, Article 5)

ฐานนี้เทียบได้กับมาตรา 10 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 สามารถปรับใช้กับการกระทำหลักของอาชญากรรมแบบไร้ตัวตน ในกรณีเป้าหมายหลักคือการทำให้ระบบหรือเครือข่ายขัดข้องหรือไม่สามารถทำงานตามปกติ เช่น องค์กรอาชญากรรมที่ใช้วิธีโจมตีแบบบอทเน็ต (Botnet) โดยควบคุมคอมพิวเตอร์ของผู้อื่นและสั่งการให้ส่งข้อมูลปริมาณมากไปยังระบบเป้าหมายทำให้ขัดข้องไม่สามารถให้บริการ ฐานนี้สามารถปรับใช้กับการกระทำในส่วนปกปิดตัวตนของอาชญากรรมแบบไร้ตัวตน ในกรณีที่อาชญากรใช้วิธีการปกปิดตัวตนที่ส่งผลให้เกิดการระงับหรือขัดข้องของระบบ

(5) ความผิดฐานการใช้อุปกรณ์โดยมิชอบ (Misuse of device , Article 6)

ฐานนี้ไม่ใช่การโจมตีระบบหรือข้อมูลโดยตรง แต่เป็นความผิดสำหรับผู้ผลิตหรือจำหน่ายอุปกรณ์ที่ใช้ในการกระทำผิด เช่น ผู้เขียนโปรแกรมหรือชุดคำสั่งเพื่อใช้โจมตีระบบ ซึ่งอาจส่งผลกระทบต่อความปลอดภัยทางคอมพิวเตอร์โดยหลายแง่มุม ทั้งผลกระทบต่อความลับ ความพร้อมใช้ ฯลฯ ขึ้นอยู่การทำงานของอุปกรณ์หรือเครื่องมือนั้นเป็นกรณีไป เนื่องจากฐานความผิดนี้กำหนดไว้กว้างรวมถึงอุปกรณ์ที่อาจนำไปใช้กระทำความผิดฐานต่างๆ ได้อย่างกว้าง แม้ว่าความผิดต้นแบบนี้ไม่ใช่ฐานความผิดเฉพาะ สำหรับอาชญากรรมแบบไร้ตัวตนและไม่ใช่ฐานความผิดสำหรับพฤติกรรมการโจมตีระบบของอาชญากรรมไร้ตัวตนโดยตรง แต่อาจนำมาปรับใช้ได้กับการกระทำที่เกี่ยวข้อง เช่น ผู้ขายซอฟท์แวร์ที่ออกแบบเพื่อปกปิดร่องรอยหรือลบร่องรอยการเข้าถึงระบบของอาชญากร เป็นต้น

(6) ความผิดต้นแบบเกี่ยวกับการปลอมแปลงและการฉ้อโกงทางคอมพิวเตอร์

- การฉ้อโกงหลอกลวงทางคอมพิวเตอร์ (Computer-related fraud, Article 8) ซึ่งแตกต่างจากความผิดตามมาตรา 14 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เนื่องจากตัวแบบของอนุสัญญาไม่ได้กำหนดองค์ประกอบเกี่ยวกับความเท็จของข้อมูล แต่องค์ประกอบมุ่งเน้นที่การแก้ไขเปลี่ยนแปลงหรือแทรกแซงการทำงานของระบบ เพื่อแสวงประโยชน์โดยมิชอบ กล่าวคือ เป็นการฉ้อโกงที่มุ่งหมายไปยังการประมวลผลของระบบหรือโปรแกรมจึงเกี่ยวข้องกับผลกระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ ฐานนี้สามารถปรับใช้กับการกระทำหลักของอาชญากรรมแบบไร้ตัวตน ในกรณีที่ลักษณะหรือวิธีการกระทำเป็นการใช้ชุดคำสั่งหรือโปรแกรมเพื่อให้ระบบประมวลผลไปตามความต้องการชองอาชญากร อย่างไรก็ตาม เนื่องจากองค์ประกอบฐานนี้กำหนดสำหรับการแก้ไขหรือแทรกแซงการทำงานของระบบเพื่อแสวงประโยชน์ จึงเป็นความผิดเป้าหมายหรือการกระทำหลักมากกว่าการกระทำอันเป็นการปกปิดตัวตน ดังนั้นในส่วนของการกระทำเพื่อปกปิดตัวตนอาจต้องพิจารณาฐานความผิดอื่นตามข้อเท็จจริง เช่น องค์กรอาชญากรรมส่งชุดคำสั่งเพื่อแก้ไขเปลี่ยนแปลงระบบการคำนวณและจ่ายเงิน ในส่วนการกระทำหลักนี้อยู่ภายใต้องค์ประกอบกฎหมายต้นแบบมาตรา 8 ทั้งนี้องค์กรดังกล่าวใช้วิธีการเข้าถึงระบบคอมพิวเตอร์ของเหยื่อจำนวนหนึ่งเพื่อให้ส่งชุดคำสั่งดังกล่าว ทำให้ร่องรอยหลักฐานปรากฏว่า การส่งชุดคำสั่งนั้นมาจากคอมพิวเตอร์ของเหยื่อ การกระทำในส่วนนี้เป็นการปกปิดตัวตนแต่ต้องพิจารณาองค์ประกอบความผิดอื่น เช่น การเข้าถึงโดยมิชอบ อย่างไรก็ตาม เนื่องจากมาตรา 8 ของความผิดต้นแบบมีองค์ประกอบที่กว้าง ส่งผลให้การกระทำในส่วนปกปิดตัวตนอาจเข้าข่ายฐานความผิดนี้ เช่น การแก้ไขเปลี่ยนแปลงข้อมูลที่บ่งชี้ร่องรอยการกระทำของตนโดยมุ่งหมายปกปิดการกระทำ อาจเข้าองค์ประกอบความผิดนี้ได้

- การปลอมแปลงทางคอมพิวเตอร์ (Computer-related forgery, Article 7) ซึ่งมีองค์ประกอบสำคัญคือการกระทำต่อข้อมูลซึ่งส่งผลต่อความถูกต้องแท้จริง จึงสามารถปรับใช้กับการกระทำหลักของอาชญากรรมแบบไร้ตัวตน ในกรณีลักษณะหรือวิธีการกระทำคือการสร้างข้อมูลที่ไม่ถูกต้องหรือข้อมูลปลอม รวมทั้งอาจปรับใช้กับการกระทำในส่วนของการปกปิดตัวตน ในกรณีที่มีการใช้ข้อมูลปลอม เช่น องค์กรอาชญากรรมส่งชุดคำสั่งเพื่อแก้ไขข้อมูลเอกสารการทำธุรกรรมให้เชื่อว่าเอกสารนั้นทำโดยองค์กรหนึ่ง จะเห็นได้ว่าการกระทำนี้มีทั้งส่วนการกระทำที่เป็นเป้าหมายหลักและเป็นการปกปิดตัวตนไปด้วย ซึ่งอยู่ภายใต้ขอบเขตองค์ประกอบความผิดต้นแบบฐานนี้

จากการวิเคราะห์องค์ประกอบความผิดต้นแบบของอนุสัญญษฯ ดังกล่าวข้างต้นสามารถสรุปเป็นตารางดังต่อไปนี้

องค์ประกอบความผิดต้นแบบของอนุสัญญาอาชญากรรมไซเบอร์ของสหภาพยุโรป	**คุณลักษณะของความมั่นคงปลอดภัยทางคอมพิวเตอร์**			**อาชญากรรมคอมพิวเตอร์แบบไร้ตัวตน**	
	ความลับ (Confidentiality)	**บูรณภาพ (Integrity)**	**ความพร้อมใช้ (Availability)**	**การกระทำหลักอันเป็นเป้าหมาย**	**การกระทำในส่วนปกปิดตัวตน**
- ความผิดฐานเข้าถึงโดยมิชอบ (Illegal access, Article 2)	✓			✓	✓
- ความผิดฐานดักรับข้อมูลคอมพิวเตอร์โดยมิชอบ (Illegal Interception, Article 3)	✓			✓	✓
ความผิดฐานกระทำต่อข้อมูลโดยมิชอบ (Data interference, Article 4)		✓		✓	✓
ความผิดฐานกระทำต่อระบบคอมพิวเตอร์โดยมิชอบ (System interference, Article 5)			✓	✓	✓
-ความผิดฐานการใช้อุปกรณ์โดยมิชอบ (Misuse of device , Article 6)	✓	✓	✓	✓	✓
-การฉ้อโกงหลอกลวงทางคอมพิวเตอร์ (Computer-related fraud, Article 8)		✓		✓	✓

องค์ประกอบความผิดต้นแบบของอนุสัญญาอาชญากรรมไซเบอร์ของสหภาพยุโรป	คุณลักษณะของความมั่นคงปลอดภัยทางคอมพิวเตอร์			อาชญากรรมคอมพิวเตอร์แบบไร้ตัวตน	
	ความลับ (Confidentiality)	บูรณภาพ (Integrity)	ความพร้อมใช้ (Availability)	การกระทำหลักอันเป็นเป้าหมาย	การกระทำในส่วนปกปิดตัวตน
การปลอมแปลงทางคอมพิวเตอร์ (Computer-related forgery, Article 7)		✓		✓	✓

ตารางจำแนกฐานความผิดตามอนุสัญญาอาชญากรรมไซเบอร์ของยุโรปเกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์แบบไร้ตัวตน (ประยุกต์จาก ตารางจำแนกฐานความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ภายใต้กรอบแนวคิดความมั่นคงปลอดภัยทางสารสนเทศ , คณาธิป ทองรวีวงศ์ ความผิดเกี่ยวกับคอมพิวเตอร์ เล่ม1 : ความผิดต่อความปลอดภัยของระบบและข้อมูลคอมพิวเตอร์ , กรุงเทพ: สำนักพิมพ์นิติธรรม , พิมพ์ครั้งที่ 2 , 2565)

3. กฎหมายต่างประเทศที่กำหนดความผิดเกี่ยวกับอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์

หัวข้อนี้จะศึกษากฎหมายต่างประเทศที่เกี่ยวข้องกับอาชญากรรมแบบไร้ตัวตน

3.1 กฎหมายสหรัฐอเมริกา

กฎหมายสหรัฐอเมริกาที่เกี่ยวข้องกับอาชญากรรมแบบไร้ตัวตน จำแนกได้สองกลุ่มคือ กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์และกฎหมายเกี่ยวกับการโจรกรรมข้อมูลซึ่งจะเกี่ยวข้องกับการกระทำในส่วนปกปิดตัวตนของอาชญากรรมประเภทนี้

3.1.1 กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์

สหรัฐอเมริกามีกฎหมายเฉพาะในระดับรัฐบาลกลางที่กำหนดฐานความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์คือ รัฐบัญญัติว่าด้วยการกระทำโดยมิชอบและการฉ้อโกงทางคอมพิวเตอร์ (The Computer Fraud and Abuse Act หรือ “CFAA”) ซึ่งประกอบด้วยฐานความผิด ดังต่อไปนี้

1) ความผิดฐานโจรกรรมข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับความมั่นคงของรัฐ มีองค์ประกอบความผิดคือ “เข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจและได้มาซึ่งข้อมูลที่อาจถูกนำไปใช้ในทางเสียหายต่อรัฐหรืออาจถูกนำไปใช้ประโยชน์โดยรัฐบาลต่างชาติ”[86]

2) ความผิดฐานโจรกรรมข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับการเงิน มีองค์ประกอบความผิดคือ “เข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจและได้มาซึ่งข้อมูลเกี่ยวกับสถาบันการเงิน หรือข้อมูลการเงินของผู้บริโภค หรือข้อมูลจากหน่วยงานของรัฐ[87]

3) ความผิดเกี่ยวกับการเข้าถึงโดยมิชอบซึ่งคอมพิวเตอร์ของหน่วยงานรัฐ มีองค์ประกอบความผิดคือ *“เข้าถึงซึ่งคอมพิวเตอร์ทของหน่วยงานรัฐบาลซึ่งไม่ได้เปิดให้ใช้ต่อสาธารณะ[88]*

4) ความผิดฐานฉ้อโกงหลอกลวงทางคอมพิวเตอร์ มีองค์ประกอบความผิดคือ “เข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจ ทำการฉ้อโกงและได้มาซึ่งสิ่งใดอันมีคุณค่า”[89]

5) ความผิดฐานทำให้เสียหายต่อคอมพิวเตอร์ มีองค์ประกอบความผิดคือ “กระทำโดยปราศจากอำนาจ โดยการใช้โปรแกรม ข้อมูล คำสั่ง ทำให้เกิดความเสียหายต่อคอมพิวเตอร์”[90]

6) ความผิดเกี่ยวกับรหัสผ่าน มีองค์ประกอบความผิดคือ “หลอกลวงเกี่ยวกับการได้มาซึ่งรหัสผ่านหรือข้อมูลอื่นที่คล้ายคลึงกันซึ่งอาจนำไปสู่การเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจ”[91]

7) ความผิดฐานกรรโชกทรัพย์ทางระบบคอมพิวเตอร์ มีองค์ประกอบความผิดคือ “ผู้ใด*โดยเจตนาเพื่อกรรโชกทรัพย์สินจากผู้อื่น กระทำการข่มขู่ว่าจะกระทำความเสียหายต่อคอมพิวเตอร์”*[92]

ความผิดตามกฎหมาย CFAA มีขอบเขตครอบคลุมเฉพาะการกระทำต่อเป้าหมายคือ “คอมพิวเตอร์ที่ได้รับการคุ้มครอง” (Protected computer) ซึ่งหมายถึง[93] “คอมพิวเตอร์ของหน่วยงานรัฐหรือคอมพิวเตอร์ที่ถูกใช้หรือส่งผลกระทบต่อการสื่อสารระหว่างรัฐหรือการค้าระหว่างประเทศ ...” ทั้งนี้เนื่องจาก

---

[86] 18 U.S.C., Section 1030(a)(1)

[87] 18 U.S.C., Section 1030(a)(2) ข้อสังเกต ความผิดฐานแรกและฐานที่สองเกี่ยวข้องกับการ “โจรกรรมข้อมูลคอมพิวเตอร์” เช่นเดียวกัน แต่ข้อมูลที่อยู่ในขอบเขตของฐานความผิดเป็นคนละประเภท

[88] 18 U.S.C., Section 1030(a)(3)

[89] 18 U.S.C., Section 1030(a)(4)

[90] 18 U.S.C., Section 1030(a)(5)

[91] 18 U.S.C., Section 1030(a)(6)

[92] 18 U.S.C., Section 1030(a)(7) ความผิดฐานนี้จะกล่าวถึงในบทว่าด้วยการกรรโชกทรัพย์ไซเบอร์

[93] 18 U.S.C., Section 1030(e)(2)

กฎหมาย CFAA เป็นกฎหมายระดับรัฐบาลกลาง โดยในแต่ละมลรัฐจะมีกฎหมายความผิดเกี่ยวกับคอมพิวเตอร์อันเป็นกฎหมายระดับรัฐอีก อย่างไรก็ตาม สำหรับการกระทำความผิดผ่านเครือข่ายอินเทอร์เน็ตโดยทั่วไปมีลักษณะการกระทำที่ไม่มีเขตแดนจึงส่งผลต่อการสื่อสารระหว่างรัฐได้และจัดอยู่ในขอบเขต “คอมพิวเตอร์ที่ได้รับการคุ้มครอง” ตามกฎหมายนี้

จากหลักกฎหมายและองค์ประกอบความผิดตามกฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ของสหรัฐอเมริกา พบว่า ไม่ได้กำหนดความผิดเฉพาะสำหรับอาชญากรรมแบบไร้ตัวตน อย่างไรก็ตาม ฐานความผิดเกี่ยวกับการกระทำต่อระบบหรือข้อมูลคอมพิวเตอร์ อาจนำมาปรับใช้กับอาชญากรรมไร้ตัวตนได้ ทั้งในส่วนการกระทำหลักและการกระทำอันเป็นการปกปิดตัวตน ขึ้นอยู่กับลักษณะและวิธีการกระทำ อย่างไรก็ตาม หากพิจารณาในส่วนการกระทำปกปิดตัวตนที่ใช้วิธีการนำข้อมูลระบุตัวบุคคลอื่นมาใช้ปกปิดการกระทำ จะพบว่าสหรัฐอเมริกามีกฎหมายเฉพาะดังจะกล่าวต่อไป

3.1.2 กฎหมายเกี่ยวกับการโจรกรรมข้อมูล

ในปี ค.ศ. 1998 มีการบัญญัติกฎหมายในระดับรัฐบาลกลาง (Federal law) เรียกว่า “The Identity Theft and Assumption Deterrence Act” (ITADA) ซึ่งแก้ไขประมวลกฎหมายสหรัฐโดยเพิ่มเติมฐานความผิดการโจรกรรมข้อมูลระบุตัวตนหรือข้อมูล[94] ต่อมาในปี ค.ศ. 2004 ได้มีการตรากฎหมายเฉพาะเรียกว่า “The Identity Theft Penalty Enhancement Act[95] โดยเพิ่มเติมโทษสำหรับการโจรกรรมข้อมูลชนิดร้ายแรง (Aggregated identity theft) ฐานความผิดนี้ครอบคลุมการกระทำหลายประการ เช่น

- ผู้ใดทำขึ้น ซึ่งคุณลักษณะยืนยันตัวตน หรือเอกสารระบุตัวตนปลอม (False identification document)

- ผู้ใดส่งหรือโอน คุณลักษณะยืนยันตัวตน หรือเอกสารระบุตัวตนปลอม

- ผู้ใดครอบครอง (Possess) เอกสารระบุตัวตน หรือคุณลักษณะยืนยันตัวตน หรือเอกสารระบุตัวตนปลอมตั้งแต่ 5 ฉบับ ด้วยเจตนาจะใช้หรือโอนโดยมิชอบด้วยกฎหมาย

- ผู้ใดทำหรือผลิต โอน หรือครอบครอง อุปกรณ์สำหรับใช้ในการผลิตเอกสารระบุตัวตนหรือคุณลักษณะยืนยันตัวตน ด้วยเจตนาที่จะใช้เพื่อผลิตเอกสารระบุตัวตนปลอม

---

[94] Title 18 United States Code, Section 1028 (Fraud and related activity in connection with identification documents, authentication features, and information)

[95] Title 18 United States Code, Section 1028 A

ฐานความผิดดังกล่าวมีองค์ประกอบที่สำคัญคือ การกระทำเกี่ยวกับข้อมูลระบุตัวหรือข้อมูลของบุคคล โดยเฉพาะกรณีของ “เอกสารระบุตัวตน” (Identification document) ซึ่งหมายถึง “เอกสารซึ่งทำขึ้นหรือออกโดยอำนาจของรัฐบาลกลาง มลรัฐ รัฐบาลต่างประเทศ หรือองค์กรระหว่างประเทศ ซึ่งนำมาใช้ระบุตัวบุคคล”

นอกจากเอกสารระบุตัวตนปลอม เช่น บัตรประจำตัวที่ออกโดยหน่วยงานรัฐแล้ว การทำขึ้นหรือโอนหรือใช้ข้อมูลระบุตัวตนยังรวมถึงคุณลักษณะหรือ “วิธีการระบุตัวตน” (Means of identification) ซึ่งหมายถึง ชื่อหรือตัวเลขใดๆ ที่อาจนำมาใช้โดยลำพังหรือร่วมกับข้อมูลอื่นเพื่อระบุตัวบุคคล รวมถึง ชื่อ เลขหมายประกันสังคม วันเกิด เลขใบขับขี่ หมายเลขหนังสือเดินทาง เลขหมายประจำตัวผู้เสียภาษี ข้อมูลชีวภาพ (Biometric data) เช่น ลายพิมพ์นิ้วมือ เสียง ม่านตา หรือคุณลักษณะเฉพาะทางชีวภาพอื่น ข้อมูลระบุตัวตนเกี่ยวกับการใช้งานอุปกรณ์อิเล็กทรอนิกส์ กฎหมายนี้มีโทษอาญาจำคุกมีหลายระดับตั้งแต่ จำคุกไม่เกิน 15 ปี ไม่เกิน 3 ปี ไม่เกิน 20 ปี และไม่เกิน 25 ปี ขึ้นอยู่กับลักษณะการโจรกรรมข้อมูลอัตลักษณ์ เช่น การโจรกรรมข้อมูลอัตลักษณ์ซึ่งกระทำอันเป็นการให้ความสะดวกแก่การก่อการร้ายระหว่างประเทศจะมีโทษจำคุกไม่เกิน 25 ปี

ดังนั้น ฐานความผิดตามกฎหมายนี้จึงครอบคลุมการกระทำหลักคือ ทำขึ้น ครอบครอง ใช้ ข้อมูลระบุตัวปลอมหรือข้อมูลของบุคคลอื่น

จากหลักกฎหมายและองค์ประกอบความผิดตามกฎหมาย ITADA ของสหรัฐอเมริกา พบว่าจัดเป็นฐานความผิดเฉพาะสำหรับอาชญากรรมแบบไร้ตัวตน ในส่วนการกระทำเพื่อปกปิดตัวตน โดยเป็นความผิดเฉพาะและเป็นความผิดสำเร็จในตัวเองซึ่งไม่จำต้องเชื่อมโยงกับการกระทำความผิดหลักหรือจุดประสงค์สุดท้ายของผู้ก่ออาชญากรรม กล่าวคือ ไม่ว่าอาชญากรมุ่งประสงค์จะทำหรือสร้างข้อมูลระบุตัวตนปลอมเพื่อนำไปใช้กระทำความผิดอื่นฐานใดก็เป็นความผิดตามกฎหมาย ITADA ได้ นอกจากนี้ การโจรกรรมข้อมูลตามกฎหมายนี้ไม่จำกัดเฉพาะการกระทำทางคอมพิวเตอร์ กล่าวคือ รวมถึงการทำหรือใช้เอกสารระบุตัวตนปลอมด้วย

เมื่อนำกรอบแนวคิดในการวิเคราะห์อาชญากรรมไร้ตัวตนในเชิงกระบวนการหรือขั้นตอนดังกล่าวในบทที่ 1 มาวิเคราะห์ฐานความผิดตามกฎหมาย ITADA พบว่า กฎหมายนี้ครอบคลุมการกระทำหลายขั้นตอนดังนี้

1) ขั้นตอนการได้มาซึ่งข้อมูล กฎหมายกำหนดความผิดสำหรับการทำขึ้นหรือผลิต (Produce) เอกสารระบุตัวตนปลอม ซึ่งรวมถึงการนำข้อมูลบุคคลอื่นมาใช้สร้างข้อมูลระบุตัวตนปลอม โดยอาจเป็นการกระทำทางออนไลน์ เช่น การใช้ข้อมูลบุคคลอื่นสร้างเอกสารระบุตัวตนขึ้นมาและจากนั้นนำไปใช้ประกอบอาชญากรรมต่างๆ

2) ขั้นตอนการกระทำต่อข้อมูลที่ได้มาก่อนนำไปใช้ กฎหมายกำหนดความผิดสำหรับ การโอน ซึ่งรวมถึงการขายหรือจำหน่ายข้อมูลระบุตัวตนปลอมที่ทำขึ้น จึงจัดเป็นการกระทำต่อข้อมูลก่อนนำไปใช้ประกอบอาชญากรรมอันเป็นการกระทำหลักหรือเป้าหมายสุดท้ายของอาชญากรรมแบบไร้ตัวตน

3) ขั้นตอนการใช้ข้อมูลเพื่อกระทำผิด กฎหมายกำหนดความผิดสำหรับการ “ใช้” (use) ซึ่งครอบคลุมการนำข้อมูลไปใช้ประกอบอาชญากรรมอื่นซึ่งกฎหมายกำหนดความผิดไว้ ซึ่งต้องพิจารณากฎหมายอื่นนอกจาก ITADA โดยไม่จำกัดเฉพาะการกระทำทางคอมพิวเตอร์ ดังนั้น จึงแบ่งได้สองกลุ่มคือ

(ก) การใช้ข้อมูลเพื่อประกอบอาชญากรรมเกี่ยวกับคอมพิวเตอร์ กล่าวคือ ฐานความผิดตามกฎหมายเกี่ยวกับคอมพิวเตอร์ เช่น CFAA ดังกล่าวมาแล้ว

(ข) การใช้ข้อมูลเพื่อประกอบอาชญากรรมอื่น เช่น การใช้เพื่อก่อการร้ายทางกายภาพ ซึ่งในส่วนนี้ไม่จัดเป็นอาชญากรรมแบบไร้ตัวตนทางไซเบอร์ในการวิจัยนี้

อย่างไรก็ตาม แม้ฐานความผิดนี้มีขอบเขตครอบคลุมพฤติกรรมของอาชญากรรมแบบไร้ตัวตนที่ใช้วิธีการปกปิดตัวตนโดยอาศัยข้อมูลระบุตัวบุคคลอื่นในการกระทำส่วนปกปิดตัวตนแยกเป็นหลายขั้นตอน แต่ไม่ครอบคลุมพฤติกรรมบางอย่างในขั้นตอนการได้มาซึ่งข้อมูล เช่น การ “เข้าถึง” ระบบคอมพิวเตอร์เพื่อให้ได้มาซึ่งข้อมูลระบุตัวตนของผู้อื่น ซึ่งพฤติกรรมนี้ต้องกลับไปพิจารณาฐานความผิดตามกฎหมายเกี่ยวกับคอมพิวเตอร์ (CFAA)

3.2 กฎหมายสหราชอาณาจักร

กฎหมายสหราชอาณาจักรที่เกี่ยวข้องกับอาชญากรรมแบบไร้ตัวตน จำแนกได้สองกลุ่มคือ กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์และกฎหมายเกี่ยวกับการโจรกรรมข้อมูลซึ่งจะเกี่ยวข้องกับการกระทำในส่วนปกปิดตัวตน

3.2.1 กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์

สหราชอาณาจักรมีกฎหมายเฉพาะสำหรับอาชญากรรมคอมพิวเตอร์คือ พระราชบัญญัติการใช้คอมพิวเตอร์โดยมิชอบ (Computer Misuse Act หรือ “CMA”) ประกอบด้วยความผิดหลัก 3 ฐานดังนี้

1. การเข้าถึงโดยปราศจากอำนาจ (Unauthorized Access to computer material, section1)

องค์ประกอบความผิดคือ “ทำให้คอมพิวเตอร์ปฏิบัติการใดๆ ด้วยเจตนาเข้าถึงโปรแกรมหรือข้อมูลใดๆ ที่เก็บอยู่ในคอมพิวเตอร์ การเข้าถึงดังกล่าวต้องเป็นไปโดยปราศจากอำนาจและในขณะที่กระทำการนั้นผู้กระทำรู้ถึงการกระทำดังกล่าว”

2. การเข้าถึงโดยปราศจากอำนาจด้วยเจตนากระทำความผิดอื่น (Unauthorized access with intent to commit or facilitate of further offences ,Section 2)

องค์ประกอบความผิดคือ “กระทำการเข้าถึงโดยปราศจากอำนาจด้วยเจตนาที่จะกระทำความผิดอื่นซึ่งกฎหมายกำหนดโทษไว้

3. การทำให้เสียหายซึ่งข้อมูลคอมพิวเตอร์ (Unauthorized acts with intent to impair, section 3)

องค์ประกอบความผิดคือ มีเจตนากระทำการทำให้เสียหายซึ่งการปฏิบัติการของคอมพิวเตอร์ป้องกันหรือขัดขวางการเข้าถึงโปรแกรมหรือข้อมูลใดที่เก็บไว้ในคอมพิวเตอร์

3.2.2 กฎหมายเกี่ยวกับการโจรกรรมข้อมูล

สหราชอาณาจักรไม่ได้กำหนดความผิดสำหรับการโจรกรรมข้อมูลอัตลักษณ์ (Identity theft) โดยเฉพาะ แต่มีกฎหมายหลายฉบับที่อาจนำมาปรับใช้ เช่น[96]

- พระราชบัญญัติบัตรประจำตัวบุคคล (The identity card Act of 2006) ซึ่งกำหนดความผิดสำหรับการครอบครองเอกสารปลอมแสดงข้อมูลอัตลักษณ์ของผู้อื่น โดยรู้ว่าเป็นของปลอม หรือได้มาโดยมิชอบด้วยเจตนาจะใช้เอกสารดังกล่าวเพื่อลงทะเบียนข้อเท็จจริงที่เกี่ยวกับตน หรืออนุญาตให้บุคคลอื่นใช้เพื่อตรวจสอบข้อเท็จจริงเกี่ยวกับตนเองหรือผู้อื่น จากคำนิยาม “เอกสารข้อมูล” (Identity document) ไม่จำกัดเฉพาะ บัตรประจำตัว แต่รวมถึงเอกสารอื่น เช่น เอกสารการเข้าเมือง หนังสือเดินทาง ใบอนุญาตขับขี่

- พระราชบัญญัติการฉ้อโกง (The Fraud Act of 2006) กำหนดความผิดสำหรับการฉ้อโกง (Fraud) 3 รูปแบบคือ การฉ้อโกงโดยการแสดงความเท็จ การบกพร่องต่อหน้าที่เปิดเผยข้อมูลและการฉ้อโกงโดยการใช้อำนาจหน้าที่โดยมิชอบ

---

[96] คณาธิป ทองรวีวงศ์, “ปัญหาทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลการโจรกรรมเอกลักษณ์,” รายงานสืบเนื่อง การประชุมวิชาการระดับชาติ SMARTS ครั้งที่ 5 (กรุงเทพมหานคร, มหาวิทยาลัยศรีนครินทรวิโรฒ, 2558).

เมื่อนำกรอบแนวคิดในการวิเคราะห์อาชญากรรมไร้ตัวตนในเชิงกระบวนการหรือขั้นตอนดังกล่าวในบทที่ 1 มาวิเคราะห์ฐานความผิดตามกฎหมายสหราชอาณาจักรทั้งสองกลุ่ม พบว่าครอบคลุมการกระทำหลายขั้นตอน ดังนี้

1) **ขั้นตอนการได้มาซึ่งข้อมูล** เกี่ยวข้องกับความผิดฐานเข้าถึงโดยปราศจากอำนาจตามพระราชบัญญัติความผิดเกี่ยวกับคอมพิวเตอร์ หากข้อมูลนั้นเป็นเอกสารแสดงข้อมูลก็จะมีความผิดตามพระราชบัญญัติบัตรประจำตัวบุคคล

2) **ขั้นตอนการกระทำต่อข้อมูลที่ได้มาก่อนนำไปใช้** สามารถปรับใช้กฎหมายเกี่ยวกับบัตรประจำตัวบุคคลในกรณี “ครอบครอง” ด้วยเจตนาใช้เพื่อกระทำความผิด

3) **ขั้นตอนการนำข้อมูลไปใช้** เกี่ยวข้องกับความผิดฐานฉ้อโกงตามกฎหมายเฉพาะ

จากแนวทางของสหราชอาณาจักรจึงพบว่า พระราชบัญญัติความผิดเกี่ยวกับคอมพิวเตอร์ (Computer Misuse Act, 1990) ไม่ได้กำหนดความผิดฐานโจรกรรมข้อมูลไว้โดยเฉพาะ แต่มีฐานความผิดตามกฎหมายหลายฉบับที่นำมาปรับใช้ตามข้อเท็จจริงและลักษณะของการกระทำ

3.3 กฎหมายสิงคโปร์

สิงค์โปร์มีกฎหมายเฉพาะสำหรับอาชญากรรมคอมพิวเตอร์ เรียกว่า กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์โดยมิชอบและความมั่นคงปลอดภัยทางไซเบอร์ ค.ศ. 1993 และที่แก้ไขเพิ่มเติมปี 2017 (Computer Misuse and Cybersecurity Act หรือ CMCA) :ซึ่งมีฐานความผิดดังนี้

(1) การเข้าถึงข้อมูลคอมพิวเตอร์ (Unauthorized access to computer material) โดยมีองค์ประกอบความผิดที่สำคัญคือ ผู้ใดเข้าถึงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยปราศจากอำนาจ

(2) การเข้าถึงด้วยเจตนากระทำความผิดอื่น (Access with intent to commit or facilitate commission of offence) โดยมีองค์ประกอบความผิดที่สำคัญคือ ผู้ใดเข้าถึงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยปราศจากอำนาจด้วยเจตนากระทำการหรือสนับสนุนให้เกิดการกระทำความผิดตามกฎหมาย

(3) การแก้ไขข้อมูลคอมพิวเตอร์ (Unauthorized modification of computer material) โดยมีองค์ประกอบความผิดที่สำคัญคือ ผู้ใดกระทำการด้วยวิธีการใดในการแก้ไขเปลี่ยนแปลงหรือทำลายข้อมูลคอมพิวเตอร์ของผู้อื่นโดยปราศจากอำนาจ

(4) การใช้หรือดักรับบริการคอมพิวเตอร์ (Unauthorized use or interception of computer service) โดยมีองค์ประกอบความผิดที่สำคัญคือ ผู้ใดกระทำการโดยไม่มีสิทธิในการใช้หรือดักรับบริการ

คอมพิวเตอร์ของผู้อื่น ฐานความผิดนี้ไม่ได้มุ่งเน้นที่การดักรับเนื้อหาข้อมูลแต่เป็นฐานความผิดสำหรับพฤติกรรมการใช้บริการโดยไม่มีสิทธิ เช่น การใช้เครือข่ายไวไฟโดยไม่ได้สมัครใช้บริการ

(5) การขัดขวางการใช้คอมพิวเตอร์ (Unauthorized obstruction of use of computer) โดยมีองค์ประกอบความผิดที่สำคัญคือ ผู้ใดกระทำการด้วยวิธีการใดอันเป็นการรบกวน ขัดขวาง การทำงานของระบบคอมพิวเตอร์ของผู้อื่นโดยไม่มีสิทธิ

(6) การเปิดเผยรหัสสำหรับการเข้าถึง (Unauthorized disclosure of access code) โดยมีองค์ประกอบความผิดที่สำคัญคือ ผู้ใดกระทำการโดยไม่มีสิทธิในการเปิดเผยรหัส หรือมาตรการใดๆที่มีไว้เพื่อป้องกันการเข้าถึงระบบหรือข้อมูลคอมพิวเตอร์

(7) การได้มา เก็บรักษาไว้ จัดหาให้ ส่งต่อ หรือทำให้ปรากฏซึ่งข้อมูลส่วนบุคคลของผู้อื่นซึ่งผู้กระทำรู้หรือมีเหตุอันควรเชื่อว่ามีการได้มาซึ่งข้อมูลดังกล่าวจากการกระทำอันเป็นความผิดตามกฎหมายนี้ (Section 8A Supplying, etc., personal information obtained in contravention of certain provisions)

3.4 บทวิเคราะห์

จากหลักกฎหมายและองค์ประกอบความผิดตามกฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ของสิงคโปร์ ผู้วิจัยมีข้อวิเคราะห์ดังนี้

กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ของสิงคโปร์ไม่ได้กำหนดความผิดเฉพาะสำหรับอาชญากรรมแบบไร้ตัวตน แต่มีการกำหนดฐานความผิดเกี่ยวกับคอมพิวเตอร์ที่กระทบต่อความปลอดภัยของระบบหรือข้อมูลคล้ายคลึงกับอนุสัญญาอาชญากรรมไซเบอร์ กฎหมายสหรัฐอเมริกาและกฎหมายไทย เช่น การเข้าถึงโดยมิชอบ การทำลายหรือแก้ไขข้อมูลคอมพิวเตอร์ การรบกวนขัดขวางการทำงานของคอมพิวเตอร์ ซึ่งฐานความผิดเกี่ยวกับการกระทำต่อระบบหรือข้อมูลคอมพิวเตอร์เหล่านี้ อาจนำมาปรับใช้กับอาชญากรรมไร้ตัวตนได้ ทั้งในส่วนการกระทำหลักและการกระทำอันเป็นการปกปิดตัวตน ขึ้นอยู่กับลักษณะและวิธีการกระทำ

หากพิจารณาในส่วนการกระทำปกปิดตัวตนที่ใช้วิธีการนำข้อมูลระบุตัวบุคคลอื่นมาใช้ปกปิดการกระทำจะพบว่า สิงค์โปร์กำหนดฐานความผิดเฉพาะสำหรับการโจรกรรมข้อมูล (Section 8A ซึ่งแก้ไขเพิ่มเติมในปี ค.ศ. 2017) ซึ่งเมื่อเปรียบเทียบกับกฎหมายประเทศอื่นที่ศึกษาก่อนหน้าพบว่า

- การกำหนดความผิดฐานนี้แตกต่างจากอนุสัญญาอาชญากรรมไซเบอร์ เนื่องจากไม่ได้กำหนดความผิดฐานการได้มาซึ่งข้อมูลระบุตัวบุคคลอันเกิดจากการกระทำผิดเกี่ยวกับคอมพิวเตอร์ไว้โดยเฉพาะ แม้ว่าฐานความผิดหลักของกฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ของสิงค์โปร์จะสามารถนำมาปรับใช้กับการ

ได้มาซึ่งข้อมูลระบุตัว แต่ก็ไม่ได้กำหนดความผิดสำหรับการกระทำบางประการ เช่น การครอบครองหรือเก็บรักษาไว้ซึ่งข้อมูลระบุตัวผู้อื่น

- การกำหนดความผิดฐานนี้แตกต่างจากกฎหมายสหรัฐอเมริกา เนื่องจากความผิดตามกฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ (CFAA) ไม่ได้กำหนดความผิดฐานได้มาหรือเก็บไว้ซึ่งข้อมูลระบุตัวบุคคลอันได้มาจากการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หากเปรียบเทียบกับกฎหมาย ITADA ก็พบว่า ความผิดตามมาตรา 8A ของกฎหมายสิงคโปร์มีขอบเขตจำกัดหรือแคบกว่า เพราะไม่ได้กำหนดความผิดสำหรับการได้มาซึ่งข้อมูลระบุตัวบุคคลหรือการสร้างขึ้นในกรณีทั่วไป แต่กำหนดความผิดเฉพาะการได้มาซึ่งข้อมูลระบุตัวอันสืบเนื่องหรือเชื่อมโยงกับการกระทำผิดเกี่ยวกับคอมพิวเตอร์ฐานอื่นในกฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ ตัวอย่างเช่น อาชญากรกระทำความผิดฐานเข้าถึงข้อมูลโดยมิชอบ ซึ่งเป็นความผิดเกี่ยวกับคอมพิวเตอร์ฐานหนึ่ง และการกระทำนี้ส่งผลให้ได้มาซึ่งข้อมูลระบุตัวบุคคลหรือนำข้อมูลระบุตัวที่ได้จากการเข้าถึงโดยมิชอบมาเก็บรักษาไว้ ก็จะเข้าองค์ประกอบความผิดมาตรา 8A อีกฐานหนึ่ง อย่างไรก็ตามความผิดมาตรา 8A ไม่ได้มีขอบเขตกว้างครอบคลุมถึงการสร้างหรือทำปลอมขึ้นซึ่งข้อมูลระบุตัวบุคคลหรือได้มาโดยไม่เกี่ยวข้องกับความผิดเกี่ยวกับคอมพิวเตอร์ที่ระบุไว้ในกฎหมายความผิดเกี่ยวกับคอมพิวเตอร์

เมื่อนำกรอบแนวคิดในการวิเคราะห์อาชญากรรมไร้ตัวตนในเชิงกระบวนการหรือขั้นตอนดังกล่าวในบทที่ 1 มาวิเคราะห์ฐานความผิดในส่วนที่เกี่ยวกับการกระทำอันเป็นการปกปิดตัวตนหรือการโจรกรรมข้อมูลตามมาตรา 8A ของกฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ของสิงคโปร์ พบว่า กฎหมายนี้ครอบคลุมการกระทำหลายขั้นตอน ดังนี้

1) ขั้นตอนการได้มาซึ่งข้อมูล ไม่อยู่ในฐานความผิดนี้ แต่เกี่ยวข้องกับความผิดฐานอื่นในกฎหมายฉบับเดียวกัน เช่น การเข้าถึงโดยมิชอบ การดักรับบริการคอมพิวเตอร์ จากนั้นในส่วนของการได้มาซึ่งข้อมูลระบุตัวจากการกระทำความผิดดังกล่าวรวมถึงการเก็บรักษาไว้จึงเป็นความผิดมาตรา 8A

2) ขั้นตอนการกระทำต่อข้อมูลที่ได้มาก่อนนำไปใช้ อยู่ภายใต้มาตรา 8A ซึ่งกำหนดความผิดสำหรับการ โอน ขาย ส่งต่อ ข้อมูลที่ได้จากการกระทำผิดกฎหมายนี้

3) ขั้นตอนการใช้ข้อมูลเพื่อกระทำผิด กฎหมายนี้ไม่ได้กำหนดความผิดโดยตรงสำหรับการ “ใช้” หรือนำข้อมูลระบุตัวบุคคลอื่นไปใช้ในการกระทำความผิดหลักอันเป็นเป้าหมาย แต่มาตรา 8A กำหนดความผิดสำหรับการจัดหา ทำให้ปรากฏ ส่งต่อ ข้อมูลที่ได้จากการกระทำผิดกฎหมายนี้ หรือเป็นการซื้อขายข้อมูลระบุตัว ซึ่งเป็นความผิดสำเร็จได้ตั้งแต่การส่งต่อหรือซื้อขายโดยยังไม่จำต้องถึงขั้นนำข้อมูลไปปกปิดตัวตนเพื่อกระทำความผิดอื่นใด

ตารางสรุปเปรียบเทียบกฎหมายที่เกี่ยวข้องกับอาชญากรรมไร้ตัวตน โดยจำแนกตามกระบวนการกระทำ

รูปแบบของอาชญากรรมไร้ตัวตน	กฎหมายสหรัฐอเมริกา	กฎหมายสหราชอาณาจักร	กฎหมายสิงค์โปร์	กฎหมายไทย
การกระทำความผิดหลักหรือเป้าหมายของอาชญากรรมไร้ตัวตน	กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ (CFAA)	กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ (CMA)	กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ CMCA	พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
การกระทำในการปกปิดตัวตนที่ไม่ได้ใช้ข้อมูลระบุตัวบุคคลอื่น	.กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ (CFAA)	กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ (CMA)	กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ CMCA	พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
การกระทำในการปกปิดตัวโดยอาศัยข้อมูลระบุตัวหรือข้อมูลผู้อื่น	-กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ไม่ได้กำหนดความผิดเฉพาะ - มีกฎหมาย เฉพาะสำหรับการโจรกรรมข้อมูล (ITADA)	กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ (CMA) ไม่ได้กำหนดความผิดเฉพาะ - ไม่มีกฎหมายเฉพาะสำหรับการโจรกรรมข้อมูล	กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ (CMA) มีฐานความผิดเกี่ยวกับการโจรกรรมข้อมูล	พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไม่ได้กำหนดความผิดเฉพาะ - ไม่มีกฎหมายเฉพาะสำหรับการโจรกรรมข้อมูล
การนำข้อมูลอัตลักษณ์ไปใช้โดยมิชอบ	กำหนดความผิดสำหรับการใช้ (use) โดยมีเจตนากระทำความผิดกฎหมาย	กำหนดความผิดสำหรับการ “ใช้” โดยมิชอบ ซึ่งไม่จำกัดว่าจะต้องเป็นการใช้เพื่อแสวงประโยชน์ทางทรัพย์สินเท่านั้น	มาตรา 8 การฉ้อโกงทางคอมพิวเตอร์ (Computer related fraud)	มาตรา 14 (1) การนำข้อมูลปลอม เท็จ บิดเบือนเข้าสู่ระบบคอมพิวเตอร์โดยหลอกลวงหรือโดยทุจริต

4. กฎหมายที่เกี่ยวข้องกับการบังคับใช้กฎหมายเพื่อป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตนของประเทศไทย

4.1 พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556

สืบเนื่องจากลักษณะองค์กรอาชญากรรมข้ามชาติเป็นความผิดที่ส่งผลกระทบต่อความสงบเรียบร้อยและความมั่นคงของประเทศและกฎหมายที่ใช้บังคับอยู่ยังไม่สามารถใช้บังคับเพื่อดำเนินคดีและดำเนินการกับผู้บงการขององค์กรอาชญากรรมได้อย่างมีประสิทธิภาพ ประกอบกับประเทศไทยได้ลงนามในอนุสัญญาสหประชาชาติเพื่อต่อต้านอาชญากรรมข้ามชาติที่จัดตั้งในลักษณะองค์กร ค.ศ.2000 (United Nations Convention against Transnational Organized Crime 2000) เมื่อวันที่ 13 ธันวาคม พ.ศ. 2543 จึงจำเป็นต้องตรากฎหมายใหม่เพื่ออนุวัติการตามอนุสัญญาฯ โดยคณะรัฐมนตรีได้มีมติเมื่อวันที่ 26 กันยายน พ.ศ. 2543 อนุมัติให้สำนักงานอัยการสูงสุดเป็นหน่วยงานหลักในการตรวจสอบพันธกรณีตามอนุสัญญาเพื่อยกร่างกฎหมายขึ้นใหม่เพื่อรองรับพันธกรณีต่างๆ ของไทยตามอนุสัญญาฯ ต่อมาจึงได้มีการตราพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 ประกาศในพระราชกิจจานุเบกษา เล่ม 130 ตอน 55ก วันที่ 26 มิถุนายน พ.ศ. 2556 มีผลใช้บังคับเมื่อพ้นกำหนดเก้าสิบวันนับจากวันประกาศในพระราชกิจจานุเบกษา โดยเป็นกฎหมายที่กำหนดมาตรการในการปราบปรามอาชญากรรมทางเศรษฐกิจที่มีลักษณะเป็นองค์กรอาชญากรรม ซึ่งหมายถึงคณะบุคคลตั้งแต่สามคนขึ้นไปที่รวมตัวกันช่วงระยะเวลาหนึ่งและร่วมกันกระทำการใด โดยมีวัตถุประสงค์เพื่อกระทำความผิดร้ายแรงและเพื่อได้มาซึ่งผลประโยชน์ทางการเงิน ทรัพย์สิน หรือผลประโยชน์ทางวัตถุอย่างอื่นไม่ว่าโดยทางตรงหรือทางอ้อม (บทนิยามในมาตรา 3) กฎหมายตราขึ้นเนื่องจากปัจจุบันประเทศไทยมีปัญหาเกี่ยวกับการประกอบอาชญากรรมที่มีลักษณะเป็นองค์กรอาชญากรรมข้ามชาติซึ่งส่งผลกระทบต่อความสงบเรียบร้อยและความมั่นคงของประเทศเป็นอย่างมากและยังไม่มีกฎหมายสารบัญญัติใดที่จะใช้ในการป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติได้เนื่องจากกฎหมายสารบัญญัติส่วนใหญ่จะใช้บังคับกับการกระทำความผิดอาญาที่กระทำโดยปัจเจกบุคคลหรือบุคคลตั้งแต่สองคนขึ้นไปที่สมคบกันเท่านั้น กฎหมายสารบัญญัติดังกล่าวจึงไม่สามารถนำมาใช้บังคับกับการกระทำความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติหรือการกระทำความผิดอาญาที่มีลักษณะที่มีการเชื่อมโยงกันเป็นเครือข่ายหรือขบวนการได้ นอกจากนี้กฎหมายวิธีสบัญญัติที่ใช้บังคับอยู่ได้กำหนดหลักเกณฑ์และวิธีการเกี่ยวกับการดำเนินคดีอาญากับผู้กระทำความผิดอาญาโดยทั่วไปเมื่อนำมาใช้บังคับกับการกระทำความผิดฐานมีส่วนร่วมในองค์อาชญากรรมข้ามชาติแล้วก็ไม่สามารถใช้บังคับได้อย่างมีประสิทธิภาพและประสิทธิผลเนื่องจากไม่มีบทบัญญัติที่ให้อำนาจเจ้าพนักงานที่จะใช้มาตรการ

พิเศษในการสืบสวนสอบสวนรวบรวมพยานหลักฐานรวมทั้งการแสวงหาความร่วมมือระหว่างประเทศในการสืบสวนและดำเนินคดีกับผู้กระทำความผิดและองค์กรอาชญากรรมข้ามชาติได้ ประกอบกับประเทศไทยได้ลงนามในอนุสัญญาสหประชาชาติเพื่อต่อต้านอาชญากรรมข้ามชาติที่จัดตั้งในลักษณะองค์กร จึงสมควรกำหนดลักษณะความผิดให้ครอบคลุมการกระทำดังกล่าว รวมทั้งกำหนดวิธีการสืบสวน สอบสวนการกระทำความผิดดังกล่าวนั้นด้วย รวมทั้งกำหนดบทกำหนดโทษที่เหมาะสมแก่การกระทำความผิดเพื่อให้การป้องกันและปราบปรามการมีส่วนร่วมในองค์อาชญากรรมข้ามชาติเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล

สำหรับเนื้อหาของบทบัญญัติแห่งพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 มี 32 มาตรา โดยแบ่งเนื้อหาออกเป็น 4 หมวด ดังนี้

หมวด 1 บททั่วไป (มาตรา 5 – มาตรา 9)

หมวด 2 การสืบสวนสอบสวนคดีความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ (มาตรา 10 – มาตรา 22)

หมวด 3 ความร่วมมือที่เป็นประโยชน์ต่อการดำเนินคดี(มาตรา 23 – มาตรา 24)

หมวด 4 บทกำหนดโทษ (มาตรา 25 – มาตรา 32)[97]

โดยสาระสำคัญของกฎหมายมีดังนี้

1) กำหนดนิยามสำคัญไว้ดังนี้

“องค์กรอาชญากรรม” ให้หมายความว่า “คณะบุคคลตั้งแต่สามคนขึ้นไปที่รวมตัวกันช่วงระยะเวลาหนึ่งและร่วมกันกระทำการใด โดยมีวัตถุประสงค์เพื่อกระทำความผิดร้ายแรงและเพื่อได้มาซึ่งผลประโยชน์ทางการเงิน ทรัพย์สิน หรือผลประโยชน์ทางวัตถุอย่างอื่นไม่ว่าโดยทางตรงหรือทางอ้อม” และกำหนดนิยามของคำว่า

“ความผิดร้ายแรง” ให้หมายความว่า “ความผิดอาญาที่กฎหมายกำหนดโทษจำคุกขั้นสูงตั้งแต่สี่ปีขึ้นไปหรือโทษสถานที่หนักกว่านั้น”

“องค์กรอาชญากรรมข้ามชาติ” ให้หมายความว่า “องค์กรอาชญากรรมที่มีการกระทำความผิดซึ่งมีลักษณะอย่างหนึ่งอย่างใด ดังต่อไปนี้

(1) ความผิดที่กระทำในเขตแดนของรัฐมากกว่าหนึ่งรัฐ

(2) ความผิดที่กระทำในรัฐหนึ่ง แต่การตระเตรียม การวางแผน การสั่งการ การสนับสนุน หรือการควบคุมการกระทำความผิดได้กระทำในอีกรัฐหนึ่ง

---

[97] วีระพงษ์ บุญโญภาส และสุพัตรา แผนวิชิต , รายงานวิจัยฉบับสมบูรณ์เรื่องการติดตามเส้นทางการเงินของขบวนการค้าผู้หญิงและเด็กในอนุภูมิภาคลุ่มแม่น้ำโขง , สถาบันเพื่อการยุติธรรมแห่งประเทศไทย (TIJ) , 2558, หน้า 45 – 46.

(3) ความผิดที่กระทำในรัฐหนึ่ง แต่เกี่ยวข้องกับองค์กรอาชญากรรมที่มีการกระทำความผิดมากกว่าหนึ่งรัฐ

(4) ความผิดที่กระทำในรัฐหนึ่ง แต่ผลของการกระทำที่สำคัญเกิดขึ้นในอีกรัฐหนึ่ง”

ดังนั้น คำว่า “องค์กรอาชญากรรมข้ามชาติ” จึงหมายความถึง การกระทำของคณะบุคคลตั้งแต่สามคนขึ้นไปที่รวมตัวกันช่วงระยะเวลาหนึ่งและร่วมกันกระทำการใด โดยมีวัตถุประสงค์เพื่อกระทำความผิดอาญาที่กฎหมายกำหนดโทษจำคุกขั้นสูงตั้งแต่ 4 ปีขึ้นไป เพื่อให้ได้มาซึ่งผลประโยชน์ทางการเงินหรือผลประโยชน์ทางวัตถุอย่างอื่นไม่ว่าโดยทางตรงหรือทางอ้อม โดยความผิดที่กระทำนั้นได้กระทำในรัฐมากกว่าหนึ่งรัฐ หรือกระทำในรัฐหนึ่ง แต่มีส่วนสำคัญของการเตรียมการ การวางแผน การสั่งการ หรือการควบคุมเกิดขึ้นในอีกรัฐหนึ่ง หรือมีผลกระทบอย่างสำคัญในอีกรัฐหนึ่ง หรือกระทำในรัฐหนึ่งแต่เกี่ยวข้องกับองค์กรอาชญากรรมซึ่งเกี่ยวข้องกับกิจกรรมที่เป็นความผิดอาญาในรัฐมากกว่าหนึ่งรัฐ

2) กำหนดองค์ประกอบความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติไว้ในมาตรา 5 ดังนี้

1) ผู้ใด

2) กระทำการอย่างหนึ่งอย่างใดดังต่อไปนี้

(1) เป็นสมาชิกหรือเป็นเครือข่ายดำเนินงานขององค์กรอาชญากรรมข้ามชาติ

(2) สมคบกันตั้งแต่สองคนขึ้นไปเพื่อกระทำความผิดร้ายแรงอันเกี่ยวข้องกับองค์กรอาชญากรรมข้ามชาติ

(3) มีส่วนร่วมกระทำการใด ๆ ไม่ว่าโดยทางตรงหรือทางอ้อมในกิจกรรมหรือการดำเนินการขององค์กรอาชญากรรมข้ามชาติ โดยรู้ถึงวัตถุประสงค์และการดำเนินกิจกรรมหรือโดยรู้ถึงเจตนาที่จะกระทำความผิดร้ายแรงขององค์กรอาชญากรรมข้ามชาติดังกล่าว

(4) จัดการ สั่งการ ช่วยเหลือ ยุยง อำนวยความสะดวก หรือให้คำปรึกษาในการกระทำความผิดร้ายแรงขององค์กรอาชญากรรมข้ามชาติโดยรู้ถึงวัตถุประสงค์และการดำเนินกิจกรรม หรือโดยรู้ถึงเจตนาที่จะกระทำความผิดร้ายแรงขององค์กรอาชญากรรมข้ามชาติดังกล่าว

3) ผู้นั้นกระทำความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ

โดยผู้กระทำความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ ต้องระวางโทษจำคุกตั้งแต่สี่ปีถึงสิบห้าปี หรือปรับตั้งแต่แปดหมื่นบาทถึงสามแสนบาท หรือทั้งจำทั้งปรับตามที่บัญญัติไว้ในมาตรา 25

3) กำหนดมาตรการบังคับใช้กฎหมายกับองค์กรอาชญากรรมข้ามชาติหลายมาตรการเพื่อให้การบังคับใช้กฎหมายเป็นไปอย่างมีประสิทธิและสามารถนำผู้กระทำความผิดและผู้บงการมาลงโทษได้ ได้แก่

(1) การได้มาและการเข้าถึงข้อมูล ตามมาตรา 17 ที่กำหนดให้ในกรณีที่มีเหตุอันควรเชื่อว่าเอกสารหรือข้อมูลข่าวสารซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีใด ถูกใช้หรืออาจถูกใช้ เพื่อให้ได้รับประโยชน์จากการกระทำความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พนักงานสอบสวนซึ่งได้รับอนุมัติจากอัยการสูงสุด ผู้บัญชาการตำรวจแห่งชาติ หรือผู้ซึ่งได้รับมอบหมาย แล้วแต่กรณี อาจยื่นคำขอฝ่ายเดียวต่ออธิบดีผู้พิพากษาศาลอาญาเพื่อมีคำสั่งอนุญาตให้ได้มาซึ่งเอกสารหรือข้อมูลข่าวสารดังกล่าวก็ได้

(2) การปฏิบัติการอำพราง ซึ่งหมายความว่า การดำเนินการทั้งหลายเพื่อปิดบังสถานะหรือวัตถุประสงค์ของการดำเนินการโดยลวงผู้อื่นให้เข้าใจไปในทางอื่น หรือเพื่อมิให้รู้ความจริงเกี่ยวกับการปฏิบัติหน้าที่ของเจ้าพนักงาน โดยมาตรา 19 ประกอบกับข้อบังคับของอัยการสูงสุดว่าด้วยการปฏิบัติการอำพรางตามพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 มาตรา 19 พ.ศ. 2556 กฎหมายกำหนดให้ในกรณีจำเป็นและเพื่อประโยชน์ในการสืบสวนสอบสวนเกี่ยวกับความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ ให้อัยการสูงสุด ผู้บัญชาการตำรวจแห่งชาติ หรือผู้ซึ่งได้รับมอบหมาย มอบหมายให้บุคคลใดจัดทำเอกสารหรือหลักฐานใดขึ้นหรือปฏิบัติการอำพราง โดยให้ถือว่าการจัดทำเอกสารหรือหลักฐานใดหรือการปฏิบัติการอำพรางตามวรรคหนึ่ง ให้ถือว่าเป็นการกระทำโดยชอบด้วยกฎหมาย

(3) การเคลื่อนย้ายภายใต้การควบคุม ซึ่งหมายความว่า วิธีการอนุญาตให้ของผิดกฎหมายหรือต้องสงสัยผ่านออกไปจาก ผ่าน หรือเข้าไปสู่เขตแดนของรัฐหนึ่งหรือมากกว่ารัฐหนึ่ง โดยการรับรู้และอยู่ภายใต้การติดตามดูแลของเจ้าหน้าที่ผู้มีอำนาจ เพื่อการสืบสวนสอบสวนความผิดและเพื่อระบุตัวบุคคลที่เกี่ยวข้องในการกระทำความผิดนั้น โดยมาตรา 20 ประกอบกับข้อบังคับของอัยการสูงสุดว่าด้วยการเคลื่อนย้ายภายใต้การควบคุมตามพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 มาตรา 20 พ.ศ. 2557กำหนดให้ในกรณีจำเป็นและเพื่อประโยชน์ในการสืบสวนสอบสวนความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ ให้พนักงานสอบสวนหรือพนักงานเจ้าหน้าที่ผู้ได้รับอนุญาตเป็นหนังสือจากอัยการสูงสุด ผู้บัญชาการตำรวจแห่งชาติ หรือผู้ซึ่งได้รับมอบหมาย แล้วแต่กรณีมีอำนาจให้มีการเคลื่อนย้ายภายใต้การควบคุม โดยการกระทำและพยานหลักฐานที่ได้มาจากการกระทำของพนักงานสอบสวนหรือพนักงานเจ้าหน้าที่ตามมาตรานี้ ให้รับฟังเป็นพยานหลักฐานได้

(4) การสะกดรอย ตามมาตรา 21 ประกอบกับข้อบังคับของอัยการสูงสุดว่าด้วยการสะกดรอยผู้ต้องสงสัยตามพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 มาตรา 21 พ.ศ. 2556 กำหนดให้พนักงานสอบสวนหรือพนักงานเจ้าหน้าที่อาจใช้เครื่องมือสื่อสารโทรคมนาคม เครื่องมืออิเล็กทรอนิกส์ หรือด้วยวิธีการอื่นใด เฉพาะในการสะกดรอยผู้ต้องสงสัยว่ากระทำความผิดหรือจะกระทำความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ เพื่อสืบสวน จับกุม แสวงหาและรวบรวมพยานหลักฐาน

(5) มาตรการด้านความร่วมมือในการให้ข้อมูลที่เป็นประโยชน์แก่คดีจากผู้กระทำความผิด เนื่องจากความผิดเกี่ยวกับองค์กรอาชญากรรมข้ามชาติเป็นอาชญากรรมพิเศษที่พยานหลักฐานส่วนใหญ่จะไม่ปรากฏและอยู่ในความครอบครองของผู้กระทำความผิด จึงจำเป็นต้องได้ข้อมูลหรือพยานหลักฐานจากตัวผู้กระทำความผิดเอง โดยมาตรการดังกล่าวบัญญัติไว้ในหมวด 3 ในมาตรา 23 และมาตรา 24 กล่าวคือ ในระหว่างการสอบสวนคดีความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ หากผู้ต้องหาให้ข้อมูลเองโดยสมัครใจต่อพนักงานสอบสวน หรือพนักงานอัยการ ซึ่งเป็นข้อมูลที่สำคัญและเป็นประโยชน์อย่างยิ่งในการสืบสวนสอบสวนเกี่ยวกับกิจกรรมและการกระทำความผิดขององค์กรอาชญากรรมข้ามชาติ สามารถใช้เป็นพยานหลักฐานในการดำเนินคดีต่อหัวหน้าหรือผู้มีบทบาทสำคัญในองค์กรอาชญากรรมข้ามชาติ ให้พนักงานสอบสวนบันทึกข้อมูลดังกล่าวไว้ในสำนวนการสอบสวนแล้วเสนอสำนวนการสอบสวนต่ออัยการสูงสุด ถ้าอัยการสูงสุดเห็นว่าข้อมูลที่ได้รับจากผู้ต้องหาเป็นข้อมูลที่สำคัญและเป็นประโยชน์อย่างยิ่ง ให้อัยการสูงสุดมีอำนาจใช้ดุลพินิจออกคำสั่งไม่ฟ้องผู้ต้องหานั้นทุกข้อหาหรือบางข้อหาก็ได้

หากการให้ข้อมูลที่สำคัญและเป็นประโยชน์อย่างยิ่ง เกิดขึ้นหลังจากที่มีการฟ้องคดีแล้ว โดยได้กระทำในระหว่างการพิจารณาคดีของศาล ให้อัยการสูงสุดมีอำนาจออกคำสั่งถอนฟ้อง ถอนอุทธรณ์ ถอนฎีกา หรือไม่อุทธรณ์ ไม่ฎีกา ในความผิดนั้นทั้งหมดหรือบางส่วนแล้วแต่กรณี

ถ้าศาลเห็นว่าผู้กระทำความผิดผู้ใดได้ให้ข้อมูลที่สำคัญและเป็นประโยชน์อย่างยิ่งในการปราบปรามการกระทำความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติต่อพนักงานฝ่ายปกครองหรือตำรวจ พนักงานสอบสวน หรือพนักงานอัยการ ศาลจะลงโทษผู้นั้นน้อยกว่าอัตราโทษขั้นต่ำที่กำหนดไว้สำหรับความผิดตามพระราชบัญญัตินี้ก็ได้

การนำมาตรการต่าง ๆ ที่มีประสิทธิภาพตามพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 มาบังคับใช้กับอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ จะต้องปรากฏว่าเป็นอาชญากรรมแบบไร้ตัวตนนั้นเป็นความผิดที่มีลักษณะเป็นองค์กรอาชญากรรมข้ามชาติตามนิยามและองค์ประกอบความผิดของกฎหมายด้วย กล่าวคือ ต้องเป็นความผิดที่การ

กระทำโดยบุคคลตั้งแต่ 3 คนขึ้นไปและเป็นความผิดอาญาที่กฎหมายกำหนดโทษจำคุกขั้นสูงตั้งแต่ 4 ปีขึ้นไป โดยมีวัตถุประสงค์เพื่อให้ได้มาซึ่งผลประโยชน์ทางการเงินหรือผลประโยชน์ทางวัตถุอย่างอื่นไม่ว่าโดยทางตรงหรือทางอ้อม โดยความผิดที่กระทำนั้นได้กระทำในรัฐมากกว่าหนึ่งรัฐ หรือกระทำในรัฐหนึ่ง แต่มีส่วนสำคัญของการเตรียมการ การวางแผน การสั่งการ หรือการควบคุมเกิดขึ้นในอีกรัฐหนึ่ง หรือมีผลกระทบอย่างสำคัญในอีกรัฐหนึ่ง หรือกระทำในรัฐหนึ่งแต่เกี่ยวข้องกับองค์กรอาชญากรรมซึ่งเกี่ยวข้องกับกิจกรรมที่เป็นความผิดอาญาในรัฐมากกว่าหนึ่งรัฐ จึงจำเป็นต้องแยกพิจารณาตามลักษณะของอาชญากรรมแบบไร้ตัวตนเป็นกรณี ๆ ไป

4.2 พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 และที่แก้ไขเพิ่มเติม

สืบเนื่องจากปัญหาอาชญากรรมในสังคมได้ทวีความรุนแรงและมีความสลับซับซ้อนมากยิ่งขึ้น ส่วนหนึ่งเนื่องมาจากการพัฒนาในด้านเทคโนโลยี การสื่อสาร การคมนาคม ทำให้มีการเปลี่ยนแปลงรูปแบบและวิธีการกระทำความผิดที่มีความซับซ้อนและยากต่อการดำเนินคดี ทั้งนี้ เนื่องจากอาชญากรมักเป็นผู้ความรู้และได้นำความรู้ความเชี่ยวชาญของตนไปใช้ในการกระทำความผิด เพื่อแสวงหาประโยชน์และปกปิดซ่อนเร้นทำลายพยานหลักฐาน เพื่อให้รอดพ้นจากการกระทำความผิด ดังนั้น หากไม่มีการปรับปรุงระบบการสอบสวนให้ทันสมัยแล้วเป็นการยากที่จะนำเอาตัวผู้กระทำความผิดมาลงโทษได้[98] โดยเฉพาะปัญหาในการปราบปรามอาชญากรรมพิเศษที่กระทำในลักษณะเป็นองค์กรอาชญากรรม หรือองค์กรอาชญากรรมข้ามชาตินั้น ซึ่งเป็นการรวมกลุ่มของอาชญากรที่มีการบริหารองค์กรอย่างเป็นระบบ มีลำดับขั้นในการบังคับบัญชา ผู้นำองค์กรอาชญากรรมมักเป็นผู้ทรงอิทธิพลซึ่งมีเครือข่ายหรือมีปฏิสัมพันธ์กับผู้มีอิทธิพลในแวดวงต่างๆ อาทิ วงการเมือง วงราชการหรือวงการธุรกิจ โดยขั้นตอนสำคัญในการดำเนินคดีกับผู้กระทำความผิดที่เป็นองค์กรอาชญากรรม ได้แก่ การแสวงหาพยานหลักฐานเพื่อพิสูจน์ความผิดให้ได้ ซึ่งในทางปฏิบัติการเสาะแสวงหาพยานหลักฐานในคดีความผิดเกี่ยวกับองค์กรอาชญากรรมกระทำได้ยากยิ่ง ด้วยเหตุผลที่กล่าวมาข้างต้น ซึ่งการนำมาตรการสืบสวนสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญายังไม่เพียงพอและยังไม่เท่าทันกับพัฒนาการของผู้กระทำความผิดที่เป็นองค์กรอาชญากรรม

ด้วยเหตุผลดังกล่าว ประเทศไทยได้ตราพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 จัดตั้งกรมสอบสวนคดีพิเศษ (Department of Special Investigation: DSI) ขึ้น ให้เป็นหน่วยงานในสังกัดกระทรวง

[98] ไพฑูรย์ ขัมภรัตน์, “กรมสอบสวนคดีพิเศษกับการแก้ไขความบกพร่องของพยานหลักฐานในคดีอาญา” , มติชน , 24 กรกฎาคม 2545 .

ยุติธรรมจัดตั้งขึ้นตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 โดยพระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม พ.ศ. 2545 ได้กำหนดให้กรมสอบสวนคดีพิเศษมีอำนาจหน้าที่ในการป้องกันและปราบปรามอาชญากรรมที่มีลักษณะเป็นคดีพิเศษ โดยเฉพาะอย่างยิ่งในคดีที่มีความยุ่งยากสลับซับซ้อน โดยหน่วยงานสอบสวนคดีพิเศษจะเป็นหน่วยงานบังคับใช้กฎหมายที่มีความเป็นอิสระบุคลากรที่เป็นพนักงานสอบสวนจะเป็นผู้ที่มีคุณสมบัติเช่นเดียวกับพนักงานอัยการหรือผู้พิพากษามีความเชี่ยวชาญในคดีพิเศษต่าง ๆ อันจะทำให้ประสิทธิภาพในการสอบสวนดีมากยิ่งขึ้น โดยให้มีภารกิจคือ การป้องกัน ปราบปรามและควบคุมอาชญากรรมที่มีผลกระทบร้ายแรงต่อเศรษฐกิจ สังคม ความมั่นคง และความสัมพันธ์ระหว่างประเทศ โดยมีวัตถุประสงค์หลักของการสอบสวนอยู่ที่การแสวงหาพยานหลักฐาน โดยเฉพาะในกรณีที่คดีอาชญากรรมพิเศษนั้น จะไม่มีประจักษ์พยาน วิธีและมาตรการสอบสวนตามกฎหมายวิธีพิจารณาความอาญาไม่สามารถแสวงหาพยานหลักฐานได้อย่างเพียงพอและมีประสิทธิภาพ จึงทำให้ไม่สามารถนำตัวผู้กระทำความผิดในคดีที่สำคัญมาลงโทษได้ การมีมาตรการพิเศษในการรวบรวมพยานหลักฐานจึงเป็นสิ่งที่จำเป็น

เจตนารมณ์สำคัญในการกำหนดให้มีงานสอบสวนคดีพิเศษขึ้นโดยให้กรมสอบสวนคดีพิเศษมีอำนาจหน้าที่และความรับผิดชอบในการดำเนินการก็เพื่อแก้ไขความบกพร่องในกระบวนการยุติธรรมให้มีประสิทธิภาพมากขึ้น ทั้งนี้ เนื่องจากการสืบสวนสอบสวนคดีอาชญากรรมทั่วไปเป็นหัวใจสำคัญของการอำนวยความยุติธรรมแก่ประชาชน แต่ปรากฏว่าระบบการสอบสวนในปัจจุบันไม่สามารถแก้ไขปัญหาความบกพร่องของพยานหลักฐานในคดีบางประเภทได้ รวมทั้งระบบการสอบสวนตามที่บัญญัติไว้ในประมวลกฎหมายวิธีพิจารณาความอาญาได้ใช้บังคับมาตั้งแต่ปี พ.ศ. 2477 โดยยังมิได้มีการปรับปรุงแก้ไข ทั้งที่สังคมและปัญหาอาชญากรรมได้มีการเปลี่ยนแปลงพัฒนาไปในแบบต่าง ๆ อีกมากมาย อีกทั้งเรื่องความรอบรู้คดีอาชญากรรมนั้น พนักงานสอบสวนซึ่งเป็นเจ้าหน้าที่ตำรวจเพียงฝ่ายเดียวไม่สามารถรอบรู้ได้ทุกเรื่อง โดยเฉพาะเมื่อต้องดำเนินการกับอาชญากรรมที่ผู้กระทำผิดอาศัยความรู้ความเชี่ยวชาญเฉพาะด้านเกี่ยวกับเทคนิควิชาชีพต่างๆ การค้นหาความจริงจึงต้องอาศัยผู้มีความรู้ ความชำนาญพิเศษเข้ามาร่วมทำการสอบสวน[99]

[99] สุพัตรา แผนวิชิต , โครงการศึกษาวิเคราะห์และกำหนดแนวทางแก้ไขเพิ่มเติมมาตรการพิเศษตามกฎหมายว่าด้วยการสอบสวนคดีพิเศษ , กรุงเทพมหานคร : มหาวิทยาลัยสุโขทัยธรรมาธิราช , 2564 , หน้า 23-24.

กลไกการบังคับใช้มาตรการพิเศษ[100]

มาตรการพิเศษตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 รวมถึงกฎหมายอื่นที่เกี่ยวข้องกับการสอบสวนคดีพิเศษ เป็นมาตรการที่ได้บัญญัติไว้เป็นอำนาจพิเศษสำหรับพนักงานสอบสวนคดีพิเศษนอกเหนือไปจากประมวลกฎหมายวิธีพิจารณาความอาญา ซึ่งเป็นมาตรการที่มีประสิทธิภาพสูงในการสืบสวนสอบสวนคดีพิเศษที่กฎหมายบัญญัติให้พนักงานสอบสวนคดีพิเศษมีอำนาจในการดำเนินการสืบสวนสอบสวนคดีพิเศษที่มีลักษณะ (ก) คดีความผิดทางอาญาที่มีความซับซ้อน จำเป็นต้องใช้วิธีการสืบสวนสอบสวนและรวบรวมพยานหลักฐานเป็นพิเศษ (ข) คดีความผิดทางอาญาที่มีหรืออาจมีผลกระทบอย่างรุนแรงต่อความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน ความมั่นคงของประเทศ ความสัมพันธ์ระหว่างประเทศหรือระบบเศรษฐกิจหรือการคลังของประเทศ (ค) คดีความผิดทางอาญาที่มีลักษณะเป็นการกระทำความผิดข้ามชาติที่สำคัญหรือเป็นการกระทำขององค์กรอาชญากรรม (ง) คดีความผิดทางอาญาที่มีผู้ทรงอิทธิพลที่สำคัญเป็นตัวการ ผู้ใช้หรือผู้สนับสนุน (จ) คดีความผิดทางอาญาที่มีพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ซึ่งมิใช่พนักงานสอบสวนคดีพิเศษหรือเจ้าหน้าที่คดีพิเศษเป็นผู้ต้องสงสัยเมื่อมีหลักฐานตามสมควรว่าน่าจะได้กระทำความผิดอาญาหรือเป็นผู้ถูกกล่าวหาหรือผู้ต้องหา ให้ได้อย่างมีประสิทธิภาพประสิทธิผล อย่างไรก็ตามในขณะเดียวกันมาตรการพิเศษดังกล่าวก็เป็นมาตรการที่กระทบสิทธิและเสรีภาพของประชาชนค่อนข้างสูง ดังนั้น กฎหมายจึงต้องกำหนดกลไกและหลักเกณฑ์ในการบังคับใช้มาตรการพิเศษที่เหมาะสมเอาไว้[101] ดังนี้

1) คดีพิเศษที่จะสามารถดำเนินการสืบสวนและสอบสวนโดยใช้วิธีการสืบสวนสอบสวนตามพระราชบัญญัติฯ ได้นั้น จะต้องเป็นคดีความผิดทางอาญาตามที่กฎหมายกำหนดเอาไว้เท่านั้น[102]

2) ในกรณีที่ผู้กระทำความผิดอันเป็นคดีพิเศษตามพระราชบัญญัติฯ นี้เป็นเจ้าหน้าที่ของรัฐซึ่งมิได้เป็นบุคคลตามมาตรา 66 แห่งพระราชบัญญัติประกอบรัฐธรรมนูญว่าด้วยการป้องกันและปราบปรามการทุจริต พ.ศ. 2542 และอยู่ในอำนาจหน้าที่ของคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ กฎหมาย

---

[100] สุพัตรา แผนวิชิต , โครงการศึกษาวิเคราะห์และกำหนดแนวทางแก้ไขเพิ่มเติมมาตรการพิเศษตามกฎหมายว่าด้วยการสอบสวนคดีพิเศษ , กรุงเทพมหานคร : มหาวิทยาลัยสุโขทัยธรรมาธิราช , 2564 , หน้า 45-49.

[101] ญาดา รัตนอารักขา และศุภชัย คำคุ้ม, คำอธิบายกฎหมายว่าด้วยการสอบสวนคดีพิเศษและกรมสอบสวนคดีพิเศษ (DSI), กรุงเทพมหานคร: กรุงสยามพับลิชชิ่ง, 2556 , หน้า 99 อ้างถึงใน สุพัตรา แผนวิชิต , โครงการศึกษาวิเคราะห์และกำหนดแนวทางแก้ไขเพิ่มเติมมาตรการพิเศษตามกฎหมายว่าด้วยการสอบสวนคดีพิเศษ , กรุงเทพมหานคร : มหาวิทยาลัยสุโขทัยธรรมาธิราช , 2564 , หน้า 45.

[102] พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 21 ประกอบกฎกระทรวงว่าด้วยการกำหนดคดีพิเศษเพิ่มเติมตามกฎหมายว่าด้วยการสอบสวนคดีพิเศษ พ.ศ. 2547

กำหนดให้พนักงานสอบสวนคดีพิเศษส่งเรื่องไปยังคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติดำเนินการ ทั้งนี้ ต้องเป็นไปตามเงื่อนไขและหลักเกณฑ์ตามที่กฎหมายกำหนด[103]

3) เพื่อประโยชน์ในการประสานการปฏิบัติงานป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคดีพิเศษ กฎหมายให้อำนาจให้มีการปฏิบัติหน้าที่ในคดีพิเศษระหว่างหน่วยงานของรัฐ[104]และให้มีอำนาจในการขอความช่วยเหลือหน่วยงานของรัฐหรือเจ้าหน้าที่ของรัฐได้ ทั้งนี้ ต้องเป็นไปตามเงื่อนไขและหลักเกณฑ์ตามที่กฎหมายกำหนด[105]

4) กรมสอบสวนคดีพิเศษมีอำนาจในการใช้มาตรการพิเศษโดยการเข้าไปค้นในเคหสถานหรือสถานที่ใด ๆ ได้โดยไม่ต้องมีหมายค้นหรือคำสั่งของศาลและสามารถจับได้โดยไม่มีหมายจับหรือคำสั่งของศาล รวมทั้งมีอำนาจในการค้นตัวบุคคลหรือยานพาหนะได้ด้วยหากมีเหตุอันสมควรที่จะต้องมีการค้นในกรณีดังกล่าว ทั้งนี้ ต้องเป็นไปตามเงื่อนไขและหลักเกณฑ์ตามที่กฎหมายกำหนด[106]

5) กรมสอบสวนคดีพิเศษมีอำนาจในการใช้มาตรการพิเศษโดยการขอข้อมูลเอกสารหลักฐานใด ๆ ดังเช่น มีหนังสือสอบถามหรือเรียกบุคคลใด ๆ มาเพื่อให้ถ้อยคำ หรือให้ส่งบัญชีเอกสาร หรือหลักฐานใด ๆ มาเพื่อตรวจสอบ หรือเพื่อประกอบการพิจารณาได้ ทั้งนี้ ต้องเป็นไปตามเงื่อนไขและหลักเกณฑ์ตามที่กฎหมายกำหนด[107]

6) กรมสอบสวนคดีพิเศษมีอำนาจในการใช้มาตรการพิเศษโดยการยึดหรืออายัดทรัพย์สินที่ค้นพบหรือที่ส่งมาได้ ทั้งนี้ ต้องเป็นไปตามเงื่อนไขและหลักเกณฑ์ตามที่กฎหมายกำหนด[108] นอกจากนี้กรมสอบสวนคดีพิเศษยังมีอำนาจเก็บรักษาของกลางหรือมอบหมายให้ผู้อื่นเป็นผู้เก็บรักษาด้วย แต่ในกรณีที่ของกลาง

---

[103] พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 21/1

[104] พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 22 ประกอบข้อบังคับ กคพ. ว่าด้วยการปฏิบัติหน้าที่ในคดีพิเศษระหว่างหน่วยงานของรัฐที่เกี่ยวข้อง พ.ศ. 2547

[105] พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 22/1

[106] พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 24 (1) (2) ประกอบประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 98 และประกอบข้อบังคับ กคพ. ว่าด้วยการปฏิบัติหน้าที่ของพนักงานสอบสวนคดีพิเศษตามมาตรา 24 แห่งพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547

[107] พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 24 (3) (4) ประกอบข้อบังคับ กคพ. ว่าด้วยการปฏิบัติหน้าที่ของพนักงานสอบสวนคดีพิเศษตามมาตรา 24 แห่งพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547

[108] พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 24 (5) ประกอบข้อบังคับ กคพ. ว่าด้วยการปฏิบัติหน้าที่ของพนักงานสอบสวนคดีพิเศษตามมาตรา 24 แห่งพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547

นั้นไม่เหมาะสมที่จะเก็บรักษา หรือเก็บรักษาไว้จะเป็นภาระแก่ทางราชการ ให้อธิบดีกรมสอบสวนคดีพิเศษมีอำนาจสั่งให้นำของกลางนั้น ออกขายทอดตลาดหรือนำไปใช้ประโยชน์ของทางราชการ โดยอาจหักค่าใช้จ่ายได้ ทั้งนี้ เป็นไปตามเงื่อนไขและหลักเกณฑ์ตามที่กฎหมายกำหนด[109]

7) กรมสอบสวนคดีพิเศษมีอำนาจในการใช้มาตรการพิเศษในการแสวงหาพยานหลักฐานเพื่อให้ได้มาซึ่งข้อมูลเอกสารพยานหลักฐานใด ๆ ดังเช่น การใช้วิธีการดักฟังทางโทรศัพท์ โทรสาร หรือสื่อเทคโนโลยีสารสนเทศอื่นใด เป็นต้นได้ ทั้งนี้ ต้องเป็นไปตามเงื่อนไขและหลักเกณฑ์ตามที่กฎหมายกำหนด[110]

8) กรมสอบสวนคดีพิเศษมีอำนาจในการใช้มาตรการพิเศษในการแสวงหาพยานหลักฐานโดยการจัดทำเอกสารหลักฐานในการเข้าไปแฝงตัวในองค์กรหรือกลุ่มบุคคลใด หรือกล่าวอีกนัยหนึ่งคือกรมสอบสวนคดีพิเศษมีอำนาจในการใช้ปฏิบัติการอำพรางโดยการใช้สายลับเพื่อเข้าไปหาข้อมูลได้ ซึ่งผู้เป็นสายลับนี้อาจจะใช้วิธีการเปลี่ยนแปลงนามของตนเองโดยจัดทำเอกสารหลักฐานในการสร้างตัวตนขึ้นมาใหม่เพื่อแฝงตัวเข้าไปหาข้อมูลในองค์กรอื่นก็ได้ แต่ทั้งนี้ต้องเป็นไปตามเงื่อนไขและหลักเกณฑ์ตามที่กฎหมายกำหนด[111]

9) ในกรณีที่การสืบสวนและสอบสวนคดีพิเศษคดีใดมีเหตุจำเป็นต้องใช้ความรู้ความเชี่ยวชาญเฉพาะด้านเป็นพิเศษ กฎหมายให้อำนาจอธิบดีกรมสอบสวนคดีพิเศษมีอำนาจในการแต่งตั้งบุคคลซึ่งมีความรู้ความเชี่ยวชาญในด้านนั้นเป็นที่ปรึกษาคดีพิเศษได้ ทั้งนี้ ต้องเป็นไปตามเงื่อนไขและหลักเกณฑ์ตามที่กฎหมายกำหนด[112]

10) ในบางครั้งการใช้มาตรการสอบสวนคดีพิเศษนั้น อาจต้องมีค่าใช้เพื่อดำเนินการตามมาตรการดังกล่าว กฎหมายจึงกำหนดให้กรมสอบสวนคดีพิเศษมีอำนาจในการเบิกค่าใช้จ่ายสำหรับการสืบสวนสอบสวนได้ ทั้งนี้ ต้องเป็นไปตามเงื่อนไขและหลักเกณฑ์ตามที่กฎหมายกำหนด[113]

---

[109] พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 28 ประกอบระเบียบกระทรวงยุติธรรมว่าด้วยการนำของกลางออกขายทอดตลาดหรือนำไปใช้ประโยชน์ของทางราชการ พ.ศ. 2547

[110] พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 25, 26

[111] พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 27 ประกอบข้อบังคับกรมสอบสวนคดีพิเศษว่าด้วยการจัดทำเอกสารหลักฐาน และการแฝงตัว พ.ศ. 2555

[112] พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 30

[113] พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 31 ประกอบระเบียบกระทรวงยุติธรรมว่าด้วยค่าใช้จ่ายสำหรับการสืบสวนและสอบสวนคดีพิเศษและวิธีการเบิกจ่ายเงินทดรองจ่ายตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 พ.ศ. 2548

11) กรมสอบสวนคดีพิเศษมีอำนาจในการขอให้พนักงานอัยการร่วมสอบสวนในคดีพิเศษได้ ทั้งนี้ ต้องเป็นไปตามเงื่อนไขและหลักเกณฑ์ตามที่กฎหมายกำหนด[114]

12) ในกรณีที่มีความจำเป็นเพื่อประโยชน์ในการสืบสวนและสอบสวนคดีพิเศษเรื่องใดเรื่องหนึ่งโดยเฉพาะ นายกรัฐมนตรีอาจมีคำสั่งให้หน่วยงานอื่นมาปฏิบัติหน้าที่ในกรมสอบสวนคดีพิเศษนั้นได้ ทั้งนี้ ต้องเป็นไปตามเงื่อนไขและหลักเกณฑ์ตามที่กฎหมายกำหนด[115]

13) ในกรณีที่พนักงานอัยการหรือพนักงานอัยการทหารแล้วแต่กรณี มีคำสั่งไม่ฟ้องคดีซึ่งได้สอบสวนโดยพนักงานสอบสวนคดีพิเศษ กฎหมายจึงได้กำหนดให้ในการทำความเห็นแย้งตามมาตรา 145 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา[116] หรือกฎหมายเกี่ยวกับวิธีพิจารณาความอาญาอื่นเป็นอำนาจหน้าที่ของอธิบดีกรมสอบสวนคดีพิเศษหรือผู้ดำรงตำแหน่งอื่นตามที่กำหนดในกฎกระทรวง[117]

การบังคับใช้พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 กับอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ จะต้องพิจารณาบนเงื่อนไขการเข้าสู่คดีพิเศษตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 คือจะต้องพิจารณาตามหลักของมาตรา 21 (1) เป็นหลักกล่าวคือ เป็นความผิดตามบัญชีท้ายพระราชบัญญัติที่มีลักษณะ (ก) คดีความผิดทางอาญาที่มีความซับซ้อนจำเป็นต้องใช้วิธีการสืบสวนสอบสวนและรวบรวมพยานหลักฐานเป็นพิเศษ (ข) คดีความผิดทางอาญาที่มีหรืออาจมี

---

[114] พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 32 ประกอบข้อบังคับ กคพ. ว่าด้วยหลักเกณฑ์และวิธีการเกี่ยวกับการสอบสวนร่วมกัน หรือการปฏิบัติหน้าที่ร่วมกันในคดีพิเศษระหว่างพนักงานสอบสวนคดีพิเศษกับพนักงานอัยการหรืออัยการทหาร พ.ศ. 2547

[115] พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 33

[116] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 145 บัญญัติว่า *“ในกรณีที่มีคำสั่งไม่ฟ้อง และคำสั่งนั้นไม่ใช่ของอธิบดีกรมอัยการ ถ้าในนครหลวงกรุงเทพธนบุรี ให้รีบส่งสำนวนการสอบสวนพร้อมกับคำสั่งไปเสนออธิบดีกรมตำรวจ รองอธิบดีกรมตำรวจ หรือผู้ช่วยอธิบดีกรมตำรวจ ถ้าในจังหวัดอื่นให้รีบส่งสำนวนการสอบสวนพร้อมกับคำสั่งไปเสนอผู้ว่าราชการจังหวัด แต่ทั้งนี้ มิได้ตัดอำนาจพนักงานอัยการที่จะจัดการอย่างใดแก่ผู้ต้องหาดังบัญญัติไว้ในมาตรา 143*

ในกรณีที่อธิบดีกรมตำรวจ รองอธิบดีกรมตำรวจหรือผู้ช่วยอธิบดีกรมตำรวจในนครหลวงกรุงเทพธนบุรี หรือผู้ว่าราชการจังหวัดในจังหวัดอื่นแย้งคำสั่งของพนักงานอัยการ ให้ส่งสำนวนพร้อมกับความเห็นที่แย้งกันไปยังอธิบดีกรมอัยการเพื่อชี้ขาด แต่ถ้าคดีจะขาดอายุความหรือมีเหตุอย่างอื่นอันจำเป็นจะต้องรีบฟ้อง ก็ให้ฟ้องคดีนั้นตามความเห็นของอธิบดีกรมตำรวจ รองอธิบดีกรมตำรวจ ผู้ช่วยอธิบดีกรมตำรวจ หรือผู้ว่าราชการจังหวัดไปก่อน

บทบัญญัติในมาตรานี้ ให้นำมาบังคับในการที่พนักงานอัยการจะอุทธรณ์ ฎีกา หรือถอนฟ้อง ถอนอุทธรณ์และถอนฎีกาโดยอนุโลม”

[117] พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 34

ผลกระทบอย่างรุนแรงต่อความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน ความมั่นคงของประเทศ ความสัมพันธ์ระหว่างประเทศหรือระบบเศรษฐกิจหรือการคลังของประเทศ (ค) คดีความผิดทางอาญาที่มีลักษณะเป็นการกระทำความผิดข้ามชาติที่สำคัญหรือเป็นการกระทำขององค์กรอาชญากรรม (ง) คดีความผิดทางอาญาที่มีผู้ทรงอิทธิพลที่สำคัญเป็นตัวการ ผู้ใช้หรือผู้สนับสนุน (จ) คดีความผิดทางอาญาที่มีพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ซึ่งมิใช่พนักงานสอบสวนคดีพิเศษหรือเจ้าหน้าที่คดีพิเศษเป็นผู้ต้องสงสัยเมื่อมีหลักฐานตามสมควรว่าน่าจะได้กระทำความผิดอาญาหรือเป็นผู้ถูกกล่าวหาหรือผู้ต้องหา ซึ่งตามประกาศ กคพ. (ฉบับที่ 8) พ.ศ. 2565 เรื่อง กำหนดรายละเอียดของลักษณะของการกระทำความผิดที่เป็นคดีพิเศษ ตามมาตรา 21 วรรคหนึ่ง (1) แห่งพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 ที่ระบุว่าคดีความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ คดีความผิดที่มีบทกำหนดโทษตามมาตรา 5 มาตรา 6 มาตรา 7 มาตรา 8 มาตรา 9 มาตรา 10 มาตรา 11 มาตรา 12 มาตรา 14 และมาตรา 17 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ. 2550 และที่แก้ไขเพิ่มเติม ที่มีลักษณะหนึ่งลักษณะใด ดังนี้ (1) มีผลกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ ด้านความมั่นคง และบริการภาครัฐที่สำคัญ ด้านการเงิน ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ด้านการขนส่งและโลจิสติกส์ ด้านพลังงานและสาธารณูปโภค ด้านสาธารณสุข หรือด้านกระบวนการยุติธรรม (2) มีผลกระทบต่อความมั่นคงของประเทศ (3) มีผลกระทบต่อความสงบเรียบร้อยของสังคมหรือศีลธรรมอันดีของประชาชนอย่างร้ายแรง (4) มีผลกระทบต่อระบบเศรษฐกิจ การเงิน การคลังของประเทศ จะเห็นได้ว่า แม้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ. 2550 และที่แก้ไขเพิ่มเติม จะเป็นความผิดตามบัญชีท้ายก็ตาม แต่ก็จะมีข้อจำกัดในกรณีบางฐานความผิดที่ไม่ปรากฏตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ จึงเป็นช่องว่างของการบังคับใช้กฎหมาย

4.3 พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 และที่แก้ไขเพิ่มเติม

พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 ซึ่งเป็นกฎหมายหลักของประเทศไทยในการกำหนดมาตรการ กลไกและกระบวนการบังคับใช้กฎหมาย ให้สามารถดำเนินการป้องกันและปราบปรามการฟอกเงินได้อย่างมีประสิทธิภาพ ตราขึ้นโดยมีวัตถุประสงค์เพื่อเพื่อเป็นการตัดวงจรการประกอบอาชญากรรมที่ผู้กระทำความผิดบางประเภทได้นำเงินหรือทรัพย์สินที่เกี่ยวกับการกระทำความผิดมากระทำการในรูปแบบต่าง ๆ อันเป็นการฟอกเงิน เพื่อนำเงินหรือทรัพย์สินนั้นไปใช้เป็นประโยชน์ในการกระทำความผิดต่อไปได้อีก โดยได้บัญญัติหลักการที่สำคัญคือ การกำหนดความผิดอาญาฐานฟอกเงินที่มีบทกำหนดโทษจำคุกตั้งแต่หนึ่งปีถึงสิบปี หรือปรับตั้งแต่สองหมื่นบาทถึงสองแสนบาท หรือทั้งจำทั้งปรับ และการนำมาตรการร้องขอให้ทรัพย์สินที่เกี่ยวกับ

การกระทำความผิดตกเป็นของแผ่นดินมาดำเนินควบคู่กับการริบทรัพย์สินทางอาญา มาตรการดังกล่าวเป็นกระบวนการพิจารณาคดีโดยกระทำต่อตัวทรัพย์สินโดยตรงและไม่ต้องคำนึงถึงความผิดของเจ้าของทรัพย์สิน ซึ่งผลของการดำเนินการย่อมกระทบต่อกรรมสิทธิ์ในทรัพย์สินของผู้กระทำความผิดหรืออาจกระทบถึงทรัพย์สินของบุคคลอื่น เนื่องจากกฎหมายมุ่งประสงค์จะดำเนินการกับทรัพย์สินที่มีความเกี่ยวข้องสัมพันธ์กับการกระทำความผิดและถือว่าทรัพย์สินดังกล่าวเป็นสิ่งที่พึงริบเสมอ

โดยพระราชบัญญัติฯ นี้มีเนื้อหาสาระประกอบด้วย หมวด 1 บททั่วไป หมวด 2 การรายงานและการแสดงตน หมวด 3 คณะกรรมการป้องกันและปราบปรามการฟอกเงิน หมวด 4 คณะกรรมการธุรกรรม หมวด 5 สำนักงานป้องกันและปราบปรามการฟอกเงิน หมวด 6 การดำเนินการเกี่ยวกับทรัพย์สิน หมวด 6/1 กองทุนป้องกันและปราบปรามการฟอกเงิน และ หมวด 7 บทกำหนดโทษ กฎหมายฉบับนี้ใช้บังคับเมื่อ 19 สิงหาคม พ.ศ. 2542 ปัจจุบันมีแก้ไขเพิ่มเติมจำนวนทั้งสิ้น 6 ครั้ง ได้แก่ พระราชกำหนดแก้ไขเพิ่มเติมพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 พ.ศ. 2546 พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน (ฉบับที่ 2) พ.ศ. 2551 พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน (ฉบับที่ 3) พ.ศ. 2552 พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน (ฉบับที่ 4) พ.ศ. 2556 พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน (ฉบับที่ 5) พ.ศ. 2558 และพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน (ฉบับที่ 6) พ.ศ. 2565

พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มาตรา 5 กำหนดความผิดอาญาฐานฟอกเงินในกรณีการกระทำที่เป็นการโอน รับโอน หรือเปลี่ยนสภาพทรัพย์สินที่เกี่ยวกับการกระทำความผิดเพื่อซุกซ่อนหรือปกปิดแหล่งที่มาของทรัพย์สินนั้น หรือเพื่อช่วยเหลือผู้อื่นไม่ว่าก่อน ขณะหรือหลังการกระทำความผิด มิให้ต้องรับโทษหรือรับโทษน้อยลงในความผิดมูลฐาน หรือ กระทำด้วยประการใด ๆ เพื่อปกปิดหรืออำพรางลักษณะที่แท้จริงการได้มาแหล่งที่ตั้ง การจำหน่าย การโอน การได้สิทธิใด ๆ ซึ่งทรัพย์สินที่เกี่ยวกับการกระทำความผิด รวมถึงการได้มา ครอบครอง หรือใช้ทรัพย์สิน โดยรู้ในขณะที่ได้มา ครอบครอง หรือใช้ทรัพย์สินนั้นว่าเป็นทรัพย์สินที่เกี่ยวกับการกระทำความผิด โดยผู้กระทำความผิดฐานฟอกเงินมีโทษตามมาตรา 60 คือต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงสิบปี หรือปรับตั้งแต่สองหมื่นบาทถึงสองแสนบาท หรือทั้งจำทั้งปรับ[118]

[118] สุพัตรา แผนวิชิต (2562) หน่วยที่ 12 เรื่อง การฟอกเงิน ในเอกสารประกอบการสอนชุดวิชา 41719 กฎหมายกระบวนการยุติธรรมเกี่ยวกับการควบคุมและปราบปรามอาชญากรรมในประเทศและข้ามชาติที่สำคัญ, นนทบุรี : สาขาวิชานิติศาสตร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช , 12-24-12-25.

พระราชบัญญัติฯฉบับนี้ ได้ขยายหลักเกณฑ์มาตรการทางทรัพย์สินให้มีขอบเขตกว้างขวางขึ้นกว่าหลักเกณฑ์ตามกฎหมายอาญาที่มีอยู่เดิม โดยให้กระทำกับทรัพย์สินที่เกี่ยวกับการกระทำความผิดมูลฐานตามที่บัญญัติไว้ในกฎหมายได้ทั้งหมด โดยไม่คำนึงว่าทรัพย์สินดังกล่าวจะมีการจำหน่าย จ่าย โอน หรือเปลี่ยนแปลงสภาพไปแล้วกี่ครั้ง หรือตกเป็นกรรมสิทธิ์ของบุคคลอื่นแล้วก็ตาม ซึ่งมาตรการทางทรัพย์สินตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงินพ.ศ. 2542 นั้น มีลักษณะพิเศษแตกต่างจากการริบทรัพย์สินตามประมวลกฎหมายอาญา โดยการนำเอามาตรการการริบทรัพย์สินทางแพ่ง ซึ่งเป็นมาตรการพิเศษที่บัญญัติไว้ในกฎหมายนี้ไปเสริมกับมาตรการลงโทษผู้กระทำความผิดที่จะต้องถูกดำเนินการริบทรัพย์สินในทางอาญาตามกฎหมายอื่นๆ ได้ จึงเป็นการเพิ่มประสิทธิภาพในการบังคับกับทรัพย์สินที่เกี่ยวกับการกระทำผิดนั้นได้ แม้จะไม่มีผู้ถูกลงโทษในคดีอาญาก็ตาม

ดังนั้น เมื่อนำเอามาตรการร้องขอให้ทรัพย์สินที่เกี่ยวกับการกระทำความผิดตกเป็นของแผ่นดินของกฎหมายป้องกันและปราบปรามการฟอกเงินมาดำเนินควบคู่กับการริบทรัพย์สินทางอาญา จะเป็นการเสริมสร้างให้มาตรการดำเนินการกับทรัพย์สินมีประสิทธิภาพยิ่งขึ้น เพราะในส่วนของมาตรการริบทรัพย์สินทางแพ่งนั้น เป็นกระบวนการพิจารณาคดีต่อตัวทรัพย์สินโดยตรงและผลของการดำเนินการย่อมกระทบต่อกรรมสิทธิ์ในทรัพย์สินของผู้กระทำความผิดหรืออาจกระทบถึงทรัพย์สินของบุคคลอื่น เนื่องจากกฎหมายมุ่งประสงค์จะดำเนินการกับทรัพย์สินที่มีความเกี่ยวพันกับการกระทำความผิดและถือว่าทรัพย์สินดังกล่าวเป็นสิ่งที่พึงริบเสมอ ในส่วนของการดำเนินคดีนั้นสามารถกระทำได้โดยการฟ้องตัวทรัพย์สินโดยตรงและไม่ต้องคำนึงถึงความผิดของเจ้าของทรัพย์สิน อย่างไรก็ตาม คำพิพากษาตามกระบวนการดังกล่าวนี้มีผลต่อกรรมสิทธิ์ในทรัพย์สินเท่านั้นและไม่สามารถลงโทษผู้กระทำความผิดหรือผู้ใดได้ แตกต่างไปจากการริบทรัพย์สินทางอาญา ซึ่งเป็นกระบวนการที่มุ่งดำเนินคดีต่อตัวบุคคล อันเป็นการมุ่งประสงค์ไปในเชิงลงโทษผู้กระทำความผิดเป็นสำคัญ โดยการดำเนินคดีจะต้องพิจารณาว่าบุคคลผู้ถูกกล่าวหาได้กระทำความผิดตามที่ถูกฟ้องหรือไม่ เมื่ออัยการพิสูจน์ให้ศาลเห็นจนปราศจากข้อสงสัยว่าบุคคลผู้ตกเป็นผู้ต้องหาหรือจำเลยได้กระทำความผิดจริงตามฟ้อง ศาลจึงจะสามารถริบทรัพย์สินดังกล่าวของผู้กระทำความผิดได้

สำหรับทรัพย์สินที่เกี่ยวกับการกระทำความผิดที่สามารถริบได้ตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 ได้แก่ เงินหรือทรัพย์สินที่ได้มาจากการกระทำซึ่งเป็นความผิดมูลฐานหรือความผิดฐานฟอกเงินหรือจากการสนับสนุนหรือช่วยเหลือการกระทำซึ่งเป็นความผิดมูลฐาน หรือความผิดฐานฟอกเงิน และเงินหรือทรัพย์สินที่ได้มาจากการจำหน่าย จ่าย โอนด้วยประการใด ๆ ซึ่งเงินหรือทรัพย์สินที่ได้มาจากการกระทำหรือสนับสนุนการกระทำซึ่งเป็นความผิดมูลฐานหรือความผิดฐานฟอกเงิน และดอกผลของเงินหรือทรัพย์สินดังกล่าว

ทั้งนี้ ไม่ว่าทรัพย์สินนั้นจะมีการจำหน่าย จ่าย โอน หรือเปลี่ยนสภาพไปกี่ครั้งและไม่ว่าจะอยู่ในความครอบครองของบุคคลใด โอนไปเป็นของบุคคลใด หรือปรากฏหลักฐานทางทะเบียนว่าเป็นของบุคคลใดก็ตาม[119]

การกระทำความผิดฐานฟอกเงินนั้นนอกจากเป็นการกระทำในลักษณะที่บัญญัติไว้ในมาตรา 5 แล้วจะต้องเป็นความผิดที่กระทำต่อเงินหรือทรัพย์สินที่ได้มาจากการกระทำความผิดเพียงบางประเภทเท่านั้น ซึ่งเรียกว่า “ความผิดมูลฐาน” หรือ ความผิดอาญาที่เป็นมูลเหตุ เป็นที่มา หรือเป็นฐานก่อให้เกิด หรือให้ได้มาซึ่งเงินหรือทรัพย์สินจากการกระทำความผิด ความผิดมูลฐานจึงเปรียบเสมือนสะพานเชื่อมโยงไปสู่การที่จะเป็นความผิดฐานฟอกเงิน ทั้งนี้ กฎหมายฟอกเงินของแต่ละประเทศจะมีขอบเขตบังคับใช้เพียงใดขึ้นอยู่กับการกำหนดความผิดมูลฐานของประเทศนั้น ความผิดมูลฐานจึงเป็นสิ่งที่มีความสำคัญในเบื้องต้นที่จะต้องพิจารณาว่า หากมีการกระทำความผิดตามความผิดมูลฐานแล้วได้เงินหรือทรัพย์สินนั้นมา หรือได้เงินหรือทรัพย์สินมาจากการจำหน่าย จ่าย โอน หรือทรัพย์สินที่ได้มาจากการกระทำความผิดมูลฐาน และได้กระทำเข้าลักษณะที่กฎหมายฟอกเงินกำหนดไว้ย่อมมีความผิดฐานฟอกเงิน

ปัจจุบันประเทศไทยมีการกำหนดความผิดมูลฐานไว้ทั้งสิ้น 28 ความผิดมูลฐาน กล่าวคือ (1) ความผิดเกี่ยวกับยาเสพติด (2) ความผิดเกี่ยวกับการค้ามนุษย์และความผิดเกี่ยวกับการค้าหญิงค้าเด็ก (3) ความผิดเกี่ยวกับการฉ้อโกงประชาชน (4) ความผิดเกี่ยวกับการยักยอกหรือฉ้อโกงหรือประทุษร้ายต่อทรัพย์หรือกระทำโดยทุจริตตามกฎหมายว่าด้วยธุรกิจสถาบันการเงินหรือกฎหมายว่าด้วยหลักทรัพย์และตลาดหลักทรัพย์ (5) ความผิดต่อตำแหน่งหน้าที่ราชการ หรือความผิดต่อตำแหน่งหน้าที่ในกระบวนการยุติธรรม (6) ความผิดเกี่ยวกับกรรโชก รีดเอาทรัพย์โดยอ้างอำนาจอั้งยี่ ซ่องโจร (7) ความผิดเกี่ยวกับการลักลอบหนีภาษีศุลกากร (8) ความผิดเกี่ยวกับการก่อการร้าย (9) ความผิดเกี่ยวกับการพนัน (10) ความผิดเกี่ยวกับการเป็นสมาชิกอั้งยี่หรือการมีส่วนร่วมในองค์กรอาชญากรรม (11) ความผิดเกี่ยวกับการรับของโจร (12) ความผิดเกี่ยวกับการปลอมหรือการแปลงเงินตรา (13) ความผิดเกี่ยวกับการละเมิดทรัพย์สินทางปัญญา (14) ความผิดเกี่ยวกับการปลอมเอกสารสิทธิ (15) ความผิดเกี่ยวกับทรัพยากรธรรมชาติหรือสิ่งแวดล้อม (16) ความผิดเกี่ยวกับการประทุษร้ายต่อชีวิตหรือร่างกายจนเป็นเหตุให้เกิดอันตรายสาหัส (17) ความผิดเกี่ยวกับการหน่วงเหนี่ยวหรือกักขัง (18) ความผิดเกี่ยวกับการลักทรัพย์ กรรโชก รีดเอาทรัพย์ ชิงทรัพย์ ปล้นทรัพย์ ฉ้อโกงหรือยักยอกอันมีลักษณะเป็นปกติธุระ (19) ความผิดเกี่ยวกับการกระทำอันเป็นโจรสลัด (20) ความผิดเกี่ยวกับการกระทำอันไม่เป็นธรรมเกี่ยวกับการซื้อขายหลักทรัพย์

---

[119] สุพัตรา แผนวิชิต , “กฎหมายวิธีพิจารณาคดีอาชญากรรมทางเศรษฐกิจและการเงินต้นแบบ”, วิทยานิพนธ์หลักสูตรนิติศาสตรดุษฎีบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยศรีปทุม , 2559, หน้า 110-111.

(21) ความผิดเกี่ยวกับอาวุธหรือเครื่องมืออุปกรณ์ของอาวุธที่ใช้หรืออาจนำไปใช้การสงคราม (22) ความผิดเกี่ยวกับการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ (23) ความผิดฐานสนับสนุนทางการเงินแก่การก่อการร้าย (24) ความผิดฐานสนับสนุนทางการเงินแก่การแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง (25) ความผิดเกี่ยวกับการเลือกตั้งสมาชิกสภาผู้แทนราษฎร (26) ความผิดเกี่ยวกับการได้มาซึ่งสมาชิกวุฒิสภา (27) ความผิดเกี่ยวกับการเลือกตั้งสมาชิกสภาท้องถิ่นหรือผู้บริหารท้องถิ่น และ (28) ความผิดเกี่ยวกับการบังคับใช้แรงงานหรือบริการที่เป็นเหตุให้ผู้ถูกกระทำได้รับอันตรายสาหัสหรือถึงแก่ความตายตามกฎหมายว่าด้วยการป้องกันและปราบปรามการค้ามนุษย์ โดยให้ความผิดมูลฐานดังกล่าว ให้หมายความรวมถึงการกระทำความผิดอาญานอกราชอาณาจักรซึ่งหากการกระทำความผิดนั้นได้กระทำลงในราชอาณาจักรจะเป็นความผิดมูลฐานด้วย บรรดาทรัพย์สินที่ได้มาจากการกระทำความผิดทั้ง 28 ความผิดมูลฐานย่อมจะต้องถูกดำเนินการตามกฎหมายฟอกเงินทั้งสิ้น

อย่างไรก็ตาม จะเห็นได้ว่าความผิดมูลฐานทั้ง 28 มูลฐานยังไม่ครอบคลุมถึงความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งเป็นรูปแบบของอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ในการกระทำความผิดหลักและไม่รวมถึงอาชญากรรมแบบไร้ตัวตนในรูปแบบความผิดตามพฤติกรรมของกระบวนการกระทำความผิดที่ไม่มีบัญญัติเป็นฐานความผิดตามกฎหมายไทย เว้นแต่การกระทำความผิดในรูปแบบอาชญากรรมแบบไร้ตัวตนที่อาจมีส่วนหนึ่งส่วนใดที่ครบองค์ประกอบความผิดตามความผิดมูลฐานทั้ง 28 มูลฐาน จึงจะสามารถนำกฎหมายฟอกเงินและมาตรการร้องขอให้ทรัพย์สินตกเป็นของแผ่นดินมาบังคับใช้ได้

4.4 พระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. 2535 และที่แก้ไขเพิ่มเติม

ในการปราบปรามการอาชญากรรมแบบไร้ตัวตนที่มีลักษณะเป็นอาชญากรรมข้ามชาติ จำเป็นต้องอาศัยความร่วมมือระหว่างประเทศในการสืบสวนสอบสวน รวบรวมพยานหลักฐานและการดำเนินคดี ตลอดจนการดำเนินการเกี่ยวกับทรัพย์สินของผู้กระทำความผิด โดยดำเนินการผ่านสำนักงานอัยการสูงสุดในฐานะผู้ประสานงานกลางภายใต้หลักเกณฑ์ของพระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. 2535 และที่แก้ไขเพิ่มเติม พระราชบัญญัตินี้ตราขึ้นเนื่องจากการประกอบอาชญากรรมมีการกระทำร่วมกันเป็นเครือข่ายในดินแดนของหลายประเทศ และกระบวนการยุติธรรมทางอาญาของแต่ละประเทศโดยลำพังไม่อาจป้องกันและปราบปรามได้อย่างเด็ดขาด การป้องกันและปราบปรามอาชญากรรมดังกล่าวจำต้องอาศัยความร่วมมือระหว่างประเทศ จึงตราขึ้นเพื่อกำหนดมาตรการให้ความช่วยเหลือและรับความช่วยเหลือระหว่างประเทศในเรื่องทางอาญา และได้มีการแก้ไขเพิ่มเติม (ฉบับที่ 2) ในพ.ศ. 2559 โดยแก้ไขเพิ่มเติมการให้ความร่วมมือ

ระหว่างประเทศ ในเรื่องทางอาญาในหลายส่วน เช่น กรณีกำหนดให้ผู้ประสานงานกลางมีอำนาจส่งคำร้องขอความช่วยเหลือจากต่างประเทศให้แก่เจ้าพนักงานหรือพนักงานเจ้าหน้าที่ตามกฎหมายอื่น เพื่อดำเนินการในส่วนที่เกี่ยวกับคำร้องขอนั้นด้วย ซึ่งจะส่งผลทำให้เกิดความคล่องตัวยิ่งขึ้น และการกำหนดให้ผู้ประสานงานกลางอาจจะส่งข้อมูลเกี่ยวกับการกระทำความผิด หรือทรัพย์สินใดไปให้ต่างประเทศ เพื่อประโยชน์ในการสืบสวน สอบสวน การฟ้องคดี หรือการพิจารณาคดีแม้ประเทศนั้นยังมิได้ร้องขอความช่วยเหลือตามพระราชบัญญัติฉบับนี้ก็ได้ ซึ่งจะเป็นประโยชน์ในการให้ความร่วมมือระหว่างประเทศในการต่อต้านการกระทำความผิดสากล โดยเฉพาะการกระทำความผิดฐานทุจริตและอาชญากรรมข้ามชาติ เป็นต้น

พระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา (ฉบับที่ 2) พ.ศ. 2559 มีเหตุผลในการประกาศใช้คือ โดยที่อัยการสูงสุดในฐานะผู้ประสานงานกลางตามกฎหมายว่าด้วยความร่วมมือระหว่างประเทศในเรื่องทางอาญาเป็นผู้มีบทบาทและอำนาจหน้าที่ที่สำคัญตามกฎหมายดังกล่าว สมควรกำหนดเพิ่มให้อัยการสูงสุดเป็นผู้รักษาการตามกฎหมายนี้ในส่วนที่เกี่ยวข้องกับอำนาจหน้าที่ของตน และบทบัญญัติบางประการในกฎหมายว่าด้วยความร่วมมือระหว่างประเทศในเรื่องทางอาญายังไม่สอดคล้องกับการให้ความร่วมมือระหว่างประเทศในเรื่องทางอาญาในปัจจุบัน กล่าวคือ ผู้ประสานงานกลางไม่สามารถส่งคำร้องขอความช่วยเหลือจากต่างประเทศไปให้เจ้าพนักงานหรือพนักงานเจ้าหน้าที่ตามกฎหมายอื่นเพื่อดำเนินการในส่วนที่เกี่ยวข้องกับคำร้องขอได้และผู้ประสานงานกลางไม่มีอำนาจส่งข้อมูลเกี่ยวกับการกระทำความผิดหรือทรัพย์สินใดไปให้ต่างประเทศเพื่อประโยชน์ในการสืบสวน สอบสวน การฟ้องคดี หรือการพิจารณาคดีในศาล หากประเทศนั้นยังมิได้ร้องขอ อันทำให้การให้ความร่วมมือเป็นไปอย่างจำกัด กระบวนการค้นหรือยึดทรัพย์สินเพื่อประโยชน์ในการรวบรวมพยานหลักฐานและเพื่อประโยชน์ชั้นที่สุดในการริบทรัพย์สินที่เป็นอยู่ในปัจจุบันไม่สามารถป้องกันการยักย้ายถ่ายเททรัพย์สินที่ได้มาจากการกระทำความผิดได้ นอกจากนี้การบัญญัติให้มีการเจรจาตกลงเพื่อให้มีการรับรองว่าจะไม่มีการประหารชีวิตถือเป็นกลไกในการร้องขอความช่วยเหลือในความผิดอันเป็นมูลเหตุแห่งการร้องขอความช่วยเหลือนั้นต้องระวางโทษถึงประหารชีวิตตามกฎหมายไทย แต่ไม่ถึงโทษประหารชีวิตตามกฎหมายของประเทศผู้รับคำร้องขอ อีกทั้งการโอนบุคคลซึ่งถูกคุมขังยังไม่ครอบคลุมถึงการโอนบุคคลซึ่งถูกคุมขัง เพื่อช่วยเหลือในการดำเนินคดีในชั้นเจ้าพนักงาน การริบหรือยึดทรัพย์สินยังไม่ครอบคลุมถึงการบังคับชำระเงินแทนการริบทรัพย์สินตามคำพิพากษาหรือคำสั่งของศาลต่างประเทศ จึงสมควรแก้ไขเพิ่มเติมบทบัญญัติดังกล่าวเพื่อให้การให้ความร่วมมือระหว่างประเทศในเรื่องทางอาญามีประสิทธิภาพมากยิ่งขึ้น

พระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา (ฉบับที่ 2) พ.ศ. 2559 มีเนื้อหาที่แก้ไขเพิ่มเติมสรุปสาระสำคัญดังนี้[120]

1. กำหนดให้อัยการสูงสุดร่วมรักษาการตามพระราชบัญญัตินี้และให้มีอำนาจออกระเบียบหรือประกาศเพื่อปฏิบัติการตามพระราชบัญญัตินี้ทั้งนี้ในส่วนที่เกี่ยวข้องกับอำนาจของอัยการสูงสุด (มาตรา 5)

2. กำหนดให้เจ้าหน้าที่ผู้มีอำนาจดำเนินการตามคำร้องขอความช่วยเหลือจากต่างประเทศ โดยกรณีคำร้องขอให้สอบปากคำพยานหรือจัดหาให้ซึ่งเอกสารหรือทรัพย์สินอันเป็นพยานหลักฐานซึ่งเป็นการดำเนินการนอกศาล คำร้องขอให้จัดส่งเอกสาร คำร้องขอให้ค้น คำร้องขอให้สืบหาบุคคล และคำร้องขอให้อายัดหรือยึดเอกสารหรือทรัพย์สินเพื่อประโยชน์ ในการรวบรวมพยานหลักฐาน ให้ผู้ประสานงานกลางส่งผู้บัญชาการตำรวจแห่งชาติหรืออธิบดี กรมสอบสวนคดีพิเศษเพื่อดำเนินการต่อไป ส่วนคำร้องขอให้เริ่มกระบวนการคดีทางอาญา ให้ผู้ประสานงานกลางส่งพนักงานอัยการเพื่อดำเนินการต่อไป นอกจากนี้ได้กำหนดให้ผู้ประสานงานกลางมีอำนาจส่งคำร้องขอความช่วยเหลือจากต่างประเทศให้แก่เจ้าพนักงานหรือพนักงานเจ้าหน้าที่ตามกฎหมายอื่น เพื่อดำเนินการในส่วนที่เกี่ยวกับคำร้องขอนั้นด้วย (มาตรา 12)

3. กำหนดให้ผู้ประสานงานกลางอาจจะส่งข้อมูลเกี่ยวกับการกระทำความผิด หรือทรัพย์สินใดไปให้ต่างประเทศเพื่อประโยชน์ในการสืบสวนสอบสวน การฟ้องคดี หรือการพิจารณาคดีแม้ประเทศนั้นยังมิได้ร้องขอความช่วยเหลือตามพระราชบัญญัตินี้ก็ได้ หากผู้ประสานงานกลางเห็นว่าการส่งข้อมูลดังกล่าวเป็นกรณีที่จำเป็นและมีเหตุผลอันสมควร ทั้งนี้การส่งข้อมูลดังกล่าวต้องไม่กระทบกระเทือนต่อการสืบสวนสอบสวน การฟ้องคดีหรือการพิจารณาคดีในประเทศไทย (มาตรา 14/1)

4. กำหนดให้ศาลส่งบันทึกคำเบิกความของพยาน รวมทั้งพยานหลักฐานอื่นในสำนวนไปยังพนักงานอัยการผู้ยื่นคำร้องเพื่อส่งให้เจ้าหน้าที่ผู้มีอำนาจดำเนินการต่อไป โดยพนักงานอัยการไม่ต้องยื่นคำร้องขอรับบันทึกคำเบิกความของพยาน รวมทั้งพยานหลักฐานอื่นต่อศาลอีก (มาตรา 17 วรรคสาม)

5. แก้ไขเพิ่มเติมส่วนที่ 5 ในกรณีที่ได้รับคำร้องขอความช่วยเหลือจากต่างประเทศให้ค้น อายัด ยึด และส่งมอบสิ่งของเพื่อประโยชน์ในการรวบรวมพยานหลักฐาน ถ้ามีเหตุที่จะออกหมายค้น หรือคำสั่งอายัดหรือยึด

---

[120] สภานิติบัญญัติแห่งชาติ , สรุปสาระสำคัญของ*แก้ไข*เพิ่มเติม*พระราชบัญญัติความร่วมมือ*ระหว่างประเทศในเรื่องทางอาญา. พ.ศ. ... , http://www.senate.go.th/document/manual/499.pdf. อ้างถึงใน วีระพงษ์ บุญโญภาสและคณะ , โครงการจ้างที่ปรึกษาเพื่อทำการศึกษาวิจัยการนำหลักการแบ่งเฉลี่ยทรัพย์สิน (Asset Sharing) มาใช้ในคดียาเสพติดของประเทศไทย , สำนักงาน ป.ป.ส. : กรุงเทพมหานคร , 2559, 186-189.

สิ่งของได้ตามกฎหมาย ให้เจ้าหน้าที่ผู้มีอำนาจดำเนินการขอให้ศาลออกหมายค้น หรือคำสั่งอายัดหรือยึดสิ่งของนั้นได้ (มาตรา 23)

ให้นำบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญามาใช้บังคับกับการออกหมายค้นหรือคำสั่งอายัดหรือยึด และการค้น อายัด หรือยึดตามความในส่วนนี้ด้วยโดยอนุโลมและให้ดำเนินการได้แม้ว่าการกระทำความผิดอันเป็นเหตุให้มีการค้น อายัด หรือยึดจะมิได้เกิดขึ้นในราชอาณาจักรก็ตาม (มาตรา 24)

เจ้าหน้าที่ผู้มีอำนาจซึ่งทำการค้น และอายัดหรือยึดสิ่งของตามคำร้องขอความช่วยเหลือจะต้องทำหนังสือรับรองการเก็บรักษารูปพรรณ ลักษณะและความบริบูรณ์แห่งสภาพของสิ่งของนั้น และส่งมอบสิ่งของที่ค้น และอายัดหรือยึดได้พร้อมหนังสือรับรองนั้นให้แก่ผู้ประสานงานกลางเพื่อดำเนินการต่อไป (มาตรา 25)

6. กำหนดให้การโอนบุคคลที่ถูกคุมขังให้ครอบคลุมถึงการโอนบุคคลที่ถูกคุมขัง เพื่อช่วยเหลือในการดำเนินคดีทั้งในชั้นเจ้าพนักงานและชั้นศาล (มาตรา 26 มาตรา 27 และมาตรา 28)

7. เพิ่มมาตรการให้ความช่วยเหลือ ในกรณีที่ได้รับคำร้องขอความช่วยเหลือ จากต่างประเทศให้บุคคลซึ่งถูกควบคุมโดยประเทศผู้ร้องขอหรือประเทศที่สามเดินทางผ่านประเทศไทย เพื่อประโยชน์ในการดำเนินคดีชั้นเจ้าพนักงานหรือชั้นศาลในประเทศผู้ร้องขอ โดยหากผู้ประสานงานกลางเห็นว่าเป็นกรณีที่อาจให้ความช่วยเหลือได้ให้แจ้งเจ้าหน้าที่ผู้มีอำนาจเพื่ออำนวยความสะดวกในการเดินทางผ่าน ในการนี้บุคคลนั้นต้องเดินทางผ่านประเทศไทย ภายในระยะเวลาที่ผู้ประสานงานกลางกำหนด หากพ้นกำหนดเวลาดังกล่าวแล้วบุคคลนั้นยังมิได้ เดินทางต่อไปยังประเทศผู้ร้องขอหรือประเทศที่สาม ให้ผู้ประสานงานกลางมีอำนาจสั่งให้บุคคลนั้น เดินทางกลับไปยังประเทศที่บุคคลนั้นออกเดินทางมาในตอนแรก และในระหว่างเดินทางผ่านประเทศไทย ให้ประเทศผู้ร้องขอรับผิดชอบการควบคุมตัวบุคคลนั้น เว้นแต่ประเทศผู้ร้องขอและผู้ประสานงานกลางตกลงกันเป็นอย่างอื่น (มาตรา 29/1)

8. แก้ไขเพิ่มเติมชื่อส่วนที่ 9 แก้ไขเพิ่มเติมเกี่ยวกับการให้เจ้าหน้าที่ผู้มีอำนาจยื่นคำขอต่อศาลในกรณีที่ได้รับคำร้องขอความช่วยเหลือจากต่างประเทศให้อายัดหรือยึดทรัพย์สินตามคำสั่งก่อนมีคำพิพากษาของศาลต่างประเทศ หรือให้ริบทรัพย์สิน หรือบังคับบุคคลใด ให้ชำระเงินแทนการริบทรัพย์สินตามคำพิพากษาหรือคำสั่งที่ยังไม่ถึงที่สุดของศาลต่างประเทศเกี่ยวกับอำนาจศาลในการพิจารณาคำร้องดังกล่าว สิทธิของเจ้าของที่แท้จริงของทรัพย์สินที่ศาลมีคำสั่งอายัดหรือยึด หรือบุคคลซึ่งถูกอายัดหรือยึดทรัพย์สิน ในการยื่นคำขอเพื่อให้ศาลยกเลิกคำสั่งนั้น แก้ไขเพิ่มเติมเกี่ยวกับการให้เจ้าหน้าที่ผู้มีอำนาจยื่นคำขอต่อศาลในกรณี ที่ได้รับคำร้องขอความช่วยเหลือจากต่างประเทศให้ริบทรัพย์สินหรือบังคับบุคคลใดให้ชำระเงิน แทนการริบทรัพย์สินตามคำพิพากษาหรือคำสั่งถึงที่สุดของศาลต่างประเทศ รวมถึงการกำหนดให้ อำนาจศาลในการหมายเรียกเจ้าหน้าที่ผู้มีอำนาจและ

บุคคลที่เกี่ยวข้อง และอำนาจในการริบทรัพย์สินหรือให้บุคคลนั้นชำระเงินแทนการริบทรัพย์สิน แก้ไขเพิ่มเติมเกี่ยวกับการให้อำนาจศาล ในการอายัด ยึด หรือริบทรัพย์สินและการบังคับชำระเงินแทนการริบทรัพย์สินที่กำหนดไว้ในคำพิพากษาหรือคำสั่งของศาลต่างประเทศตามส่วนนี้ได้แม้ว่าการกระทำความผิดอันเป็นเหตุให้ศาลจะมีคำสั่งเช่นว่านั้นจะมิได้เกิดขึ้นในราชอาณาจักร และให้ศาลพิพากษาริบทรัพย์สินหรือบังคับชำระเงินแทนการริบทรัพย์สินได้แม้ว่าผู้กระทำความผิดถึงแก่ความตายไปแล้ว แก้ไขเพิ่มเติมเกี่ยวกับการให้นำบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญาและประมวลกฎหมายอาญาว่าด้วยการริบทรัพย์สินมาใช้บังคับโดยอนุโลม แก้ไขเพิ่มเติมเกี่ยวกับการให้การริบทรัพย์สิน และเงินตกเป็นของแผ่นดิน รวมทั้งให้อำนาจศาลในการพิพากษาให้ทำให้ทรัพย์สินนั้นใช้ไม่ได้ หรือทำลายทรัพย์สินนั้น แก้ไขเพิ่มเติมเกี่ยวกับหลักเกณฑ์การปฏิบัติกรณีที่ต้องคืนทรัพย์สินที่ริบหรือเงินที่ศาลมีคำพิพากษาให้ชำระแทนการริบทรัพย์ให้แก่ประเทศผู้ร้องขอและกำหนดเกี่ยวกับการคืนทรัพย์สินหรือเงินส่วนที่เหลือให้แก่ประเทศผู้ร้องขอ เมื่อได้หักค่าใช้จ่ายในประเทศไทยได้ใช้ไปในการดำเนินการต่างๆ และค่าใช้จ่ายอันจำเป็นแล้ว รวมทั้งกำหนดเกี่ยวกับดอกผลของทรัพย์สิน หรือเงินดังกล่าว (มาตรา 33 มาตรา 34 และมาตรา 35)

9. กำหนดให้ในกรณีที่ประเทศไทยร้องขอความช่วยเหลือในความผิดอันเป็นมูลเหตุแห่งการร้องขอความช่วยเหลือนั้นต้องระวางโทษถึงประหารชีวิตตามกฎหมายไทยแต่ไม่ถึงโทษประหารชีวิตตามกฎหมายของประเทศผู้รับคำร้องขอ และรัฐบาลจำเป็นต้องให้คำรับรองว่าจะไม่มีการประหารชีวิตก็ให้มีการเจรจาตกลงเพื่อให้มีการรับรองดังกล่าวได้ ในกรณีนี้หากศาลพิพากษาลงโทษประหารชีวิตให้รัฐบาลดำเนินการตามบทบัญญัติแห่งกฎหมายเพื่อให้มีการบังคับตามคำพิพากษาโดยวิธีจำคุกตลอดชีวิตแทนการประหารชีวิต ทั้งนี้ ห้ามมิให้บุคคลนั้นได้รับการลดหย่อนผ่อนโทษไม่ว่าด้วยเหตุใดๆ เว้นแต่เป็นการพระราชทานอภัยโทษ (มาตรา 36/1)

10. กำหนดให้การรับฟังพยานหลักฐานที่ได้มาจากต่างประเทศ ให้นำบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญามาใช้บังคับโดยอนุโลม (มาตรา 41)

4.5 พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 เป็นกฎหมายที่ตราเป็นการเร่งด่วนเพื่อปราบปรามอาชญากรรมทางเทคโนโลยีในรูปแบบของแก๊งคอลเซ็นเตอร์หรือการฉ้อโกงประชาชน โดยมีหลักการและเหตุผลคือ สืบเนื่องจากปัจจุบันนมีการใช้วิธีการทางเทคโนโลยีหลอกลวงประชาชนทั่วไปผ่านอุปกรณ์เทคโนโลยีต่าง ๆ จนทำให้ประชาชนสูญเสียทรัพย์สินเป็นจำนวนมาก และผู้หลอกลวงได้โอนทรัพย์สินที่ได้จากการกระทำความผิดดังกล่าวนั้นผ่านบัญชีเงินฝาก บัตรอิเล็กทรอนิกส์ หรือบัญชีเงินอิเล็กทรอนิกส์

ของบุคคลอื่นต่อไปเป็นทอด ๆ อย่างรวดเร็ว เพื่อปกปิดหรืออำพรางการกระทำความผิด ซึ่งแต่ละวันประชาชนผู้สุจริตถูกหลอกลวงจำนวนมากและมีมูลค่าความเสียหายสูงมากและการหลอกลวงดังกล่าว ซึ่งเป็นการกระทำความผิดได้เพิ่มมากขึ้น ส่งผลกระทบต่อประชาชนในวงกว้างและเป็นอันตรายร้ายแรง ต่อระบบเศรษฐกิจของประเทศ เป็นกรณีฉุกเฉินที่มีความจำเป็นรีบด่วนอันมิอาจจะหลีกเลี่ยงได้ เพื่อประโยชน์ในอันที่จะต้องมีมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีดังกล่าว เพื่อรักษาความปลอดภัยของประเทศ ความปลอดภัยสาธารณะ และความมั่นคงในทางเศรษฐกิจของประเทศ

สาระสำคัญของกฎหมาย

1) กำหนดนิยามความหมายของ “อาชญากรรมทางเทคโนโลยี” ให้หมายความว่า การกระทำหรือพยายามกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เพื่อฉ้อโกง กรรโชก หรือรีดเอาทรัพย์ บุคคลหนึ่งบุคคลใด หรือโดยประการที่น่าจะทำให้บุคคลอื่นเสียหาย หรือกระทำความผิดฐานฉ้อโกง กรรโชก หรือรีดเอาทรัพย์ โดยใช้ระบบคอมพิวเตอร์เป็นเครื่องมือ

2) กำหนดมาตรการเปิดเผยและแลกเปลี่ยนข้อมูลระหว่างกัน ในกรณีที่มีเหตุอันควรสงสัยว่ามีหรืออาจมีการกระทำความผิดอาชญากรรมทางเทคโนโลยี โดยให้สถาบันการเงินและผู้ประกอบธุรกิจมีหน้าที่เปิดเผยหรือแลกเปลี่ยนข้อมูลเกี่ยวกับบัญชีและธุรกรรมของลูกค้าที่เกี่ยวข้องในระหว่างสถาบันการเงินและผู้ประกอบธุรกิจนั้นผ่านระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูลที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ สำนักงานป้องกันและปราบปรามการฟอกเงินและธนาคารแห่งประเทศไทยเห็นชอบร่วมกัน (มาตรา 4)

3) มาตรการสั่งให้ผู้ให้บริการเปิดเผยและส่งข้อมูล ในกรณีที่มีเหตุอันควรสงสัยว่ามีการกระทำความผิดอาชญากรรมทางเทคโนโลยีและมีความจำเป็นต้องทราบข้อมูลการลงทะเบียนผู้ใช้งานหรือข้อมูลจราจรทางคอมพิวเตอร์ ให้สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ หรือสำนักงานป้องกันและปราบปรามการฟอกเงิน แล้วแต่กรณีมีอำนาจสั่งให้ผู้ให้บริการเครือข่ายโทรศัพท์ ผู้ให้บริการโทรคมนาคมอื่น หรือผู้ให้บริการอื่นที่เกี่ยวข้องกับการกระทำดังกล่าว เปิดเผยข้อมูลที่เกี่ยวข้องเท่าที่จำเป็นและเมื่อได้รับคำสั่งแล้ว ให้ผู้ให้บริการเครือข่ายโทรศัพท์ ผู้ให้บริการโทรคมนาคมอื่น หรือผู้ให้บริการอื่นที่เกี่ยวข้องกับการกระทำนั้น มีหน้าที่ส่งข้อมูลดังกล่าวให้แก่ผู้สั่งภายในระยะเวลาที่ผู้สั่งกำหนด (มาตรา 5)

4) มาตรการระงับการทำธุรกรรม ในกรณีที่สถาบันการเงินหรือผู้ประกอบธุรกิจพบเหตุอันควรสงสัยเองหรือได้รับข้อมูลจากระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน ว่าบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ใดถูกใช้หรืออาจถูกใช้ทำธุรกรรมที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี หรือการกระทำ

ความผิดมูลฐานหรือความผิดฐานฟอกเงินตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน ให้สถาบันการเงินหรือผู้ประกอบธุรกิจมีหน้าที่ระงับการทำธุรกรรมและแจ้งสถาบันการเงิน หรือผู้ประกอบธุรกิจที่รับโอนถัดไป พร้อมทั้งนำข้อมูลเข้าสู่ระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูล เพื่อให้สถาบันการเงินและผู้ประกอบธุรกิจผู้รับโอนทุกทอดทราบ และระงับการทำธุรกรรมดังกล่าวไว้ทันทีเป็นการชั่วคราวไม่เกินเจ็ดวันนับแต่วันที่พบเหตุอันควรสงสัย หรือได้รับแจ้ง แล้วแต่กรณี เพื่อตรวจสอบความถูกต้องแท้จริงและแจ้งให้เจ้าพนักงานผู้มีอำนาจดำเนินคดีอาญาหรือเลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงินดำเนินการตรวจสอบในกรณีที่สถาบันการเงินหรือผู้ประกอบธุรกิจได้รับแจ้งเหตุตามวรรคหนึ่งจากเจ้าพนักงาน ผู้มีอำนาจดำเนินคดีอาญาหรือเลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงินให้สถาบันการเงินหรือผู้ประกอบธุรกิจมีหน้าที่ระงับการทำธุรกรรม พร้อมทั้งนำข้อมูลเข้าสู่ระบบหรือกระบวนการเปิดเผย (มาตรา 6)

5) มาตรการระงับการทำธุรกรรมในกรณีที่ได้รับแจ้งจากผู้เสียหาย ในกรณีที่สถาบันการเงินหรือผู้ประกอบธุรกิจได้รับแจ้งจากผู้เสียหาย ซึ่งเป็นผู้ถือบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ว่า ได้มีการทำธุรกรรมโดยบัญชีเงินฝากหรือ บัญชีเงินอิเล็กทรอนิกส์ดังกล่าวและเข้าข่ายเกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี ให้สถาบันการเงิน หรือผู้ประกอบธุรกิจดังกล่าวมีหน้าที่ระงับการทำธุรกรรมนั้นไว้ชั่วคราว พร้อมทั้งนำข้อมูลเข้าสู่ระบบ หรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูล เพื่อให้สถาบันการเงินและผู้ประกอบธุรกิจ ผู้รับโอนทุกทอดทราบและระงับการทำธุรกรรมดังกล่าวไว้ทันที และแจ้งให้ผู้เสียหายไปร้องทุกข์ต่อพนักงานสอบสวนภายในเจ็ดสิบสองชั่วโมง เมื่อมีการร้องทุกข์แล้ว ให้พนักงานสอบสวนแจ้งให้สถาบันการเงินหรือผู้ประกอบธุรกิจที่ได้รับการทำธุรกรรมไว้ทราบ และให้พนักงานสอบสวนพิจารณาดำเนินการเกี่ยวกับบัญชีเงินฝากและบัญชีเงินอิเล็กทรอนิกส์ดังกล่าวภายในเจ็ดวันนับแต่วันที่ได้รับแจ้งความร้องทุกข์ หากไม่มีคำสั่งให้ระงับการทำธุรกรรมไว้ต่อไปภายในเวลาดังกล่าว ให้สถาบันการเงินหรือผู้ประกอบธุรกิจยกเลิกการระงับการทำธุรกรรมนั้น

6) การกำนดโทษของผู้ที่เกี่ยวข้องกับการกระทำความผิดอาชญากรรมทางเทคโนโลยีและความผิดอาญาอื่น ได้แก่

- ความผิดฐานเปิดหรือยินยอมให้บุคคลอื่นใช้บัญชีเงินฝาก บัตรอิเล็กทรอนิกส์ หรือบัญชีเงินอิเล็กทรอนิกส์ของตน โดยมิได้มีเจตนาใช้เพื่อตนหรือเพื่อกิจการที่ตนเกี่ยวข้อง หรือยินยอมให้บุคคลอื่นใช้หรือยืมใช้เลขหมายโทรศัพท์สำหรับบริการโทรศัพท์เคลื่อนที่ของตน ทั้งนี้ โดยประการที่รู้หรือควรรู้ว่าจะนำไปใช้ในการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี หรือความผิดทางอาญาอื่นใด ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินสามแสนบาท หรือทั้งจำทั้งปรับ (มาตรา 9)

- ความผิดฐานเป็นธุระจัดหา โฆษณา หรือไขข่าวโดยประการใด ๆ เพื่อให้มีการซื้อ ขาย ให้เช่า หรือให้ยืม บัญชีเงินฝาก บัตรอิเล็กทรอนิกส์ หรือบัญชีเงินอิเล็กทรอนิกส์ เพื่อใช้ในการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีหรือความผิดทางอาญาอื่นใด ต้องระวางโทษจำคุก ตั้งแต่สองปีถึงห้าปี หรือปรับตั้งแต่สองแสนบาทถึงห้าแสนบาท หรือทั้งจำทั้งปรับ (มาตรา 10)

- ความผิดฐานเป็นธุระจัดหา โฆษณา หรือไขข่าวโดยประการใด ๆ เพื่อให้มีการซื้อ หรือขายเลขหมายโทรศัพท์สำหรับบริการโทรศัพท์เคลื่อนที่ ซึ่งลงทะเบียนผู้ใช้บริการในนามของบุคคลหนึ่งบุคคลใดแล้ว แต่ไม่สามารถระบุตัวผู้ใช้บริการได้ ต้องระวางโทษจำคุกตั้งแต่สองปีถึงห้าปี หรือปรับตั้งแต่สองแสนบาทถึงห้าแสนบาท หรือทั้งจำทั้งปรับ (มาตรา 11)

การบังคับใช้พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 กับอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ มีข้อจำกัดด้านขอบเขตการบังคับใช้กฎหมาย เนื่องจากนิยามคำว่า “อาชญากรรมทางเทคโนโลยี” ตามกฎหมายจำกัดเฉพาะการกระทำหรือพยายามกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เพื่อฉ้อโกง กรรโชก หรือรีดเอาทรัพย์ บุคคลหนึ่งบุคคลใด หรือโดยประการที่น่าจะทำให้บุคคลอื่นเสียหาย หรือกระทำความผิดฐานฉ้อโกง กรรโชก หรือรีดเอาทรัพย์ โดยใช้ระบบคอมพิวเตอร์เป็นเครื่องมือ ไม่รวมถึงการกระทำความผิดต่อระบบหรือข้อมูลคอมพิวเตอร์ ดังนั้น มาตรการทางกฎหมายที่จำกัดเฉพาะอาชญากรรมทางเทคโนโลยี ไม่รวมถึงความผิดอาญาอื่น จึงไม่สามารถนำมาใช้บังคับกับการกระทำความผิดในรูปแบบอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ได้ เว้นแต่มีการกระทำที่คาบเกี่ยวกันและเข้าองค์ประกอบนิยามของอาชญากรรมทางเทคโนโลยีและต้องมีเจตนาพิเศษตามกฎหมายด้วย นอกจากนั้น ยังไม่สามารถใช้บังคับกับความผิดที่ไม่ได้มีระบุเป็นฐานความผิดไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

บทที่ 4
การจัดทำต้นแบบกฎหมาย (Model Law) เพื่อป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตน

1. สรุปผลจากการเก็บรวบรวมข้อมูล

จากการประชุมกลุ่มย่อย (Focus Group) เพื่อระดมความคิดเห็นเกี่ยวกับแนวทางป้องกันและปราบปรามการกระทำความผิดในรูปแบบอาชญากรรมไร้ตัวตนและแนวทางการกำหนดต้นแบบต้นแบบเกี่ยวกับอาชญากรรมไร้ตัวตน เมื่อวันอังคารที่ 28 มิถุนายน 2565 เวลา 10.00 – 12.00 น. สรุปความเห็นจากผู้เข้าร่วมประชุมได้ดังนี้

ประเด็นภารกิจหรืออำนาจหน้าที่ของหน่วยงานในการบังคับใช้การบังคับใช้กฎหมายเพื่อป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตน

ความเห็นจากที่ประชุม

บริษัทที่ปรึกษา - มีการดำเนินการเฝ้าระวังเกี่ยวกับการละเมิดลิขสิทธิ์ในสื่อออนไลน์ ซึ่งตอนนี้เทคโนโลยีทำให้การละเมิดลิขสิทธิในลักษณะการกระจาย content ทำได้ง่ายขึ้น ส่วนอาชญากรรมในลักษณะ anonymous มักพบในรูปแบบของแฮกเกอร์ในการเข้าถึงข้อมูลและต้นทางมีการปล่อยมัลแวร์ ซึ่งเคยเกิดเคสที่มาต้นทางมาจากมหาวิทยาลัยในไทย ซึ่งตอนเกิดเหตุได้มีการประสานไปยังฝ่าย IT ของมหาวิทยาลัยเพื่อสืบหาผู้กระทำความผิดและแจ้งทาง ปอศ. ในการติดตามดำเนินคดีกับผู้กระทำความผิดและติดตามเส้นทางการเงิน ซึ่งในปัจจุบันพบบัญชีม้าในการกระทำความผิด และใช้ Wallet ทรูมันนี่ และคริปโตเคอเรนซี่เป็นเครื่องมือในการกระทำความผิด ทำให้ยากต่อการสืบสวนสอบสวน

ผู้แทนสำนักงานอัยการสูงสุด - ภารกิจของสำนักงานอัยการสูงสุดเกี่ยวข้องกับการอำนวยความยุติธรรม คือการสอบสวนคดีอาญาบางกรณี การสั่งคดี การดำเนินคดีในชั้นศาล การดำเนินการเกี่ยวกับความร่วมมือระหว่างประเทศในเรื่องทางอาญา โดยมีกฎหมายที่เกี่ยวข้องหลายฉบับ

การสอบสวนคดีอาญา พนักงานอัยการจะเกี่ยวข้องกับการสอบสวนคดีความผิดซึ่งมีโทษตามกฎหมายไทยที่ได้กระทำลงนอกราชอาณาจักรไทยและการสอบสวนคดีพิเศษ ซึ่งการสอบสวนคดีพิเศษ มีทั้งกรณีที่เป็นบทบังคับและกรณีที่เป็นดุลพินิจ (หมายถึง เป็นดุลพินิจของคณะกรรมการคดีพิเศษ)

การดำเนินการเกี่ยวกับความร่วมมือระหว่างประเทศในเรื่องทางอาญาตามพระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. 2535 อัยการสูงสุดหรือผู้ซึ่งอัยการสูงสุดมอบหมายจะทำหน้าที่

เป็นผู้ประสานงานกลาง เพื่อดำเนินการให้เป็นไปตามขั้นตอนของกฎหมาย ซึ่งความช่วยเหลือตามกฎหมายดังกล่าว ได้แก่ การสืบสวน การสอบสวน การรวบรวมพยานหลักฐาน เป็นต้น

นอกจากนี้ สำนักงานอัยการสูงสุดมีสถาบันวิจัยเพื่อการพัฒนาการสอบสวนและการดำเนินคดี ซึ่งทำงานด้านวิจัยเกี่ยวกับการสอบสวนและการดำเนินคดี เพื่อนำมาใช้ประโยชน์ในการพัฒนาการสอบสวนและการดำเนินคดี

ประเด็นแนวโน้ม รูปแบบของอาชญากรรมแบบไร้ตัวตนและความเสี่ยงจากภัยคุกคามจากอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์

ความเห็นจากที่ประชุม

ผู้แทนสำนักงานอัยการสูงสุด - พิจารณาจากวัตถุประสงค์ของงานวิจัยแล้วเห็นว่า ควรใช้ชื่อว่า “อาชญากรรมที่ผู้กระทำความผิดไม่เปิดเผยตัวตน” หรือ “การก่ออาชญากรรมโดยผู้กระทำความผิดที่ไม่เปิดเผยตัวตน” หรือ “อาชญากรรมที่ไม่เปิดเผยตัวตนของผู้กระทำความผิด” แทนคำว่า “อาชญากรรมแบบไร้ตัวตน” เพราะน่าจะสอดคล้องกับนิยามของคำว่า “อาชญากรรมแบบไร้ตัวตน” มากกว่า

ผู้แทนสำนักงานอัยการสูงสุด - เนื่องจากเทคโนโลยีออกแบบให้มนุษย์ได้รับความสะดวกสบาย การใช้เทคโนโลยีเพื่อกระทำความผิดจึงกระทำได้ง่ายและถูกดำเนินคดียาก ดังนั้น แนวโน้มของการก่ออาชญากรรมแบบไร้ตัวตนจึงมีสถานการณ์ที่รุนแรงขึ้น

บริษัทที่ปรึกษา – รูปแบบของการกระทำความผิดส่วนใหญ่ที่พบคือการใช้การปล่อยมัลแวร์เข้ามาทำลายระบบโดยมีวิธีการปล่อยมัลแวร์ที่หลากหลายรูปแบบ หรือกรณีความผิดเกี่ยวกับ ransomware รวมทั้งการใช้เงินดิจิทัลในการกระทำความผิด

ผู้แทนสถาบันการศึกษา – สาเหตุที่อาชญากรรมที่ไร้ตัวตน หรือปกปิดตัวตนมีการกระทำความผิดมากขึ้นในปัจจุบัน สืบเนื่องมาจากการมีเสรีภาพทางอินเทอร์เน็ตที่ค่อนข้างมาก รัฐจึงจำเป็นต้องเข้ามาจำกัดเสรีภาพของบุคคลและการที่รัฐเข้ามาจำกัดเสรีภาพดังกล่าวก็อาจส่งผลให้มีการเจาะเข้ามาในระบบเพื่อเป็นการแก้แค้นได้ เช่น การแฮกเข้ามาในระบบของหน่วยงานและการเอาข้อมูลสำคัญต่าง ๆ มาเผยแพร่ หรือการที่หันไปนิยมการใช้เงินดิจิทัลมากขึ้นเนื่องจากไม่มีตัวกลางไม่มีการควบคุมจากรัฐ ส่งผลให้อาชญากรรมไร้ตัวตนมีแนวโน้มที่สูงขึ้น โดยเป้าหมายหลักจะเป็นหน่วยงานภาครัฐ เช่น กระทรวงกลาโหม หน่วยงานด้านกระบวนการยุติธรรม หน่วยงานที่ดูแลข้อมูลส่วนบุคคล

ผู้แทนสำนักงานศาลยุติธรรม - กฎหมายที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ปัจจุบันมีกฎหมายที่เกี่ยวข้องไม่กี่ฉบับ แต่รูปแบบการกระทำความผิดค่อนข้างมีความก้าวหน้า ทำให้กฎหมายที่มีอยู่ไม่สามารถปราบปรามความผิดได้อย่างมีประสิทธิภาพ รูปแบบอาชญากรรมไร้ตัวตนที่มีเข้ามาสู่กระบวนการพิจารณาคดีของศาล ส่วนใหญ่เป็นเรื่องการเข้าถึงข้อมูลโดยปราศจากอำนาจ หรือการฉ้อโกงต่าง ๆ ที่เกี่ยวข้องกับคอมพิวเตอร์และปัญหาสำคัญมาจากการที่กฎหมายไม่มีบทนิยามหรือบทลงโทษที่จริงจัง ทำให้การบังคับใช้กฎหมายไม่มีประสิทธิภาพ ไม่สามารถปราบปรามผู้กระทำความผิด ส่งผลทำให้ผู้เสียหายไม่อยากเข้ามาดำเนินคดีและการรวบรวมพยานหลักฐานในชั้นตำรวจอาจติดขัดในเรื่องทักษะและอุปกรณ์เครื่องมือในการตรวจสอบติดตามการกระทำความผิด

ผู้แทนสถาบันการศึกษา – อาชญากรรมไร้ตัวตนในปัจจุบันมีทั้งกรณีแบบไร้ตัวตน และในกรณีการเข้ารหัส จึงอยากให้นิยามให้ชัดเจนว่า “ไร้ตัวตน” ให้มีความหมายถึงอาชญากรรมที่กระทำโดยวิธีการเข้ารหัส หรือ encryption ด้วยหรือไม่ เพราะอาจกระทบกับผู้ใช้อินเทอร์เน็ตทั่วไปที่ไม่ได้เกี่ยวกับการกระทำความผิด

การใช้บราวเซอร์ TOR หรือ Dark Net จะทำให้การติดตามตัวตนผู้กระทำความผิดทำได้ยากมาก

ผู้แทน บก. ปอศ. - เห็นว่าในอนาคตจะมีอาชญากรรมไร้ตัวตนเกิดขึ้นมาก ดังนั้น การกำหนดนิยามเป็นเรื่องสำคัญ ต้องมีความชัดเจนว่าหมายถึงความผิดรูปแบบใดบ้าง ส่วนใหญ่รูปแบบอาชญากรรมไร้ตัวตนจะเป็นกระทำความผิดที่กระทบต่อความมั่นคงปลอดภัยของระบบ หรือ CIA แต่คดีที่อยู่ในอำนาจของ บก. ปอศ. ปัจจุบันส่วนใหญ่เป็นคดีความผิดอินเทอร์เน็ตที่เกี่ยวข้องกับการกระทำต่อเนื้อหา

ประเด็นการบังคับใช้กฎหมายและการป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตนเกี่ยวข้องกับฐานความผิดเกี่ยวกับอาชญากรรมแบบไร้ตัวตน การบังคับใช้กฎหมาย การดำเนินคดี การบังคับกับทรัพย์สินและการลงโทษผู้กระทำความผิด

ความเห็นจากที่ประชุม

ผู้แทน บก. ปอศ.

1) การบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีปัญหาเรื่องการรวบรวมพยานหลักฐานเพื่อพิสูจน์ว่าใครเป็นผู้กระทำความผิดอย่างมาก และเป็นปัญหาที่ค่อนข้างยุ่งยากต่อหน่วยงานต่าง ๆ ในกระบวนการยุติธรรมและยังมีปัญหาการบังคับใช้พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 ในส่วนการใช้มาตรการต่างๆ ในการสืบสวนสอบสวน

2) การติดตามทรัพย์สินผู้กระทำความผิดทำได้ยาก เพราะเมื่อมีการโอนเงินจากบัญชีม้าออกไป ก็จะมีการนำเงินที่ได้จากการกระทำความผิดไปซื้อสกุลเงินดิจิทัล ซึ่งโดยระบบของคริปโตเป็นระบบ Peer - 2- Peer และไม่สามาระระบุตัวตนได้

ผู้แทนสำนักงานอัยการสูงสุด

1) ควรมีมาตรการลงโทษผู้ใช้ให้บุคคลอื่นหาผู้รับจ้างเปิดบัญชีธนาคาร ผู้จัดหาผู้รับจ้างเปิดบัญชีธนาคาร และผู้รับจ้างเปิดบัญชีธนาคาร เพราะอาชญากรรมที่ผู้กระทำความผิดไม่เปิดเผยตัวตนจะเกี่ยวข้องกับการเปิดบัญชีแทน จึงควรมีกฎหมายที่ระบุชัดแบบประมวลกฎหมายยาเสพติด มาตรา 129 ที่ว่า ผู้ใดยอมให้ผู้อื่นใช้ชื่อ เอกสาร หลักฐานของตน ในการเปิด จด หรือลงทะเบียนทำธุรกรรมทางการเงิน ซื้อสินค้าหรือบริการอื่นใด ยอมให้ใช้บัญชีธนาคาร บัตรอิเล็กทรอนิกส์ ซิมการ์ดโทรศัพท์ หรือยอมให้ผู้อื่นใช้สิ่งเช่นว่านั้น ซึ่งตนได้เปิด จด หรือลงทะเบียนไว้แล้ว โดยรู้หรือควรรู้ว่าจะเป็นประโยชน์ต่อการกระทำความผิดร้ายแรงเกี่ยวกับยาเสพติด ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ จึงควรพิจารณาประเด็นนี้และกำหนดเป็นบทลงโทษไว้ในกฎหมายเพื่อป้องกันการใช้บัญชีม้า
2) การบังคับใช้กฎหมาย การป้องกันการกระทำความผิด การดำเนินคดี การรวบรวมพยานหลักฐานเป็นไปได้โดยยาก พยานหลักฐานอาจไม่เพียงพอดำเนินคดี หรือไม่สามารถตรวจสอบพยานหลักฐานบางอย่างได้
3) การบังคับกับทรัพย์สินและการลงโทษผู้กระทำความผิดเป็นไปได้ยาก
4) กระบวนการตรวจสอบข้อมูลของผู้ให้บริการและข้อมูลจราจรคอมพิวเตอร์ยังไม่มีประสิทธิภาพ ดังนั้นควรมีการออกแบบเรื่องกระบวนการจัดเก็บข้อมูลส่วนบุคคลให้รู้ว่าผู้ใช้งานเป็นบุคคลใด และควรมีการออกแบบการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ที่สามารถตรวจสอบได้และสามารถระบุตัวตนหรือยืนยันตัวตนผู้ใช้งานได้ จึงควรจัดให้มีการประสานงานไปยังหน่วยงานที่เกี่ยวข้องเพื่อให้ทราบถึงอุปสรรคในการดำเนินการ

ผู้แทน บก. ปอท. – บก. ปอท. เป็นหน่วยงานหลักในการบังคับใช้กฎหมายคอมพิวเตอร์ แต่ช่วงหลังลดบทบาทลงไปบ้างเนื่องจากมีหน่วยงานศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศของสำนักงานตำรวจแห่งชาติเข้ามาแทน บก. ปอท. จึงเป็นหน่วยงานสนับสนุนการบังคับใช้กฎหมาย ปัญหาการบังคับใช้กฎหมายส่วนหนึ่งเกิดจากความรู้ความเชี่ยวชาญของเจ้าหน้าที่ตำรวจที่ตามไปทันอาชญากรไซเบอร์ ซึ่งพัฒนาของอาชญากรก้าวล้ำไปกว่าบุคลากรภาครัฐมาก

ผู้แทนสำนักงาน ปปง. – ในกระบวนการฟอกเงินพบปัญหาการฟอกเงินผ่าน cryptocurrency ที่ทำให้ไม่สามารถติดตามตัวได้ แม้ว่าปัจจุบันจะมีกฎหมายว่าด้วยการประกอบธุรกิจสินทรัพย์ดิจิทัลก็สามารถบังคับได้เพียงตัวกลางที่เข้าสู่ระบบตามกฎหมายเท่านั้น แต่กรณีที่เป็นปัญหาคือการโอนจากตัวกลางไปสู่บัญชีส่วนตัว ก็ไม่สามารถรู้ได้ว่าเป็นบัญชีของใคร และยังไม่มีมาตรการบังคับให้เจ้าของบอก private key ของคริปโตให้แก่เจ้าหน้าที่รัฐได้

ประเด็นบทบาทหน้าที่ของหน่วยงานที่เกี่ยวข้องและการบูรณาการความร่วมมือในการป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตน

ความเห็นจากที่ประชุม

ผู้แทน บก. ปอศ. - มีความจำเป็นที่ต้องบูรณาการความร่วมมือระหว่างหน่วยงาน เพราะหน่วยงานใดหน่วยงานหนึ่งไม่สามารถดำเนินการได้อย่างสัมฤทธิผล เช่น แม้ว่า บก. ปอศ. จะมีอำนาจในการดำเนินคดีละเมิดลิขสิทธิ์ แต่ก็ไม่มีเครื่องมือในการตรวจสอบการกระทำความผิด ต้องอาศัยความร่วมมือจาก บก. ปอท. กรมทรัพย์สินทางปัญญา ในการตรวจสอบ

ผู้แทนสำนักงานอัยการสูงสุด

1) อยากเห็นการพัฒนาการประสานงานระหว่างหน่วยงาน จึงเห็นว่ามีความจำเป็นต้องตั้งศูนย์ประสานงานที่เกี่ยวกับเรื่องนี้โดยตรง เป็นศูนย์ประสานงานกลางที่เก็บรวบรวมข้อมูลและเป็นศูนย์ประสานงานระหว่างหน่วยงานที่เกี่ยวข้องทั้งหมด
2) ควรแก้ไขกฎหมายให้อำนาจพนักงานอัยการใช้ดุลพินิจเข้าร่วมสอบสวนได้หรือมีอำนาจสอบสวนคดีประเภทต่าง ๆ ซึ่งจะช่วยให้การดำเนินงานในชั้นเจ้าพนักงานตำรวจมีประสิทธิภาพมากยิ่งขึ้น
3) จะต้องพิจารณาว่า องค์กรอัยการมีความจำเป็นต้องตั้งหน่วยงานที่มีอำนาจหน้าที่รับผิดชอบพิจารณาเรื่องนี้โดยตรงหรือไม่
4) เนื่องจากเจ้าหน้าที่ที่เกี่ยวข้องยังมีปัญหาติดขัดเกี่ยวกับการดำเนินคดี กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมควรเข้ามามีบทบาทในการสนับสนุนการดำเนินคดี แม้ว่าจะไม่ใช่หน่วยงานที่บังคับใช้กฎหมายโดยตรง เช่น มีแนวทางบังคับให้ผู้ประกอบการให้ความร่วมมือเก็บรวบรวมข้อมูลจราจรคอมพิวเตอร์และข้อมูลของผู้ใช้บริการ เป็นต้น

ประเด็นสาระสำคัญของร่างต้นแบบกฎหมาย (Model Law) เพื่อป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ของประเทศไทย

ความเห็นจากที่ประชุม

ผู้แทนสำนักงานศาลยุติธรรม - ควรเพิ่มเนื้อหาของร่างเกี่ยวกับเรื่องการระงับความเสียหายหรือการเยียวยาผู้เสียหายจากอาชญากรรมไร้ตัวตน เนื่องจากการความเสียหายจากการอาชญากรรมเหล่านี้อาจมีความแตกต่างจากอาชญากรรมแบบดั้งเดิม เช่น ความเสียหายเป็นวงกว้างมากกว่าเพราะเป็นการกระทำผ่านระบบอินเตอร์เน็ต นอกจากมาตรการป้องกันและปราบปราม จึงควรกำหนดมาตรการในการบรรเทาความเสียหาย

ผู้แทนสำนักงานอัยการสูงสุด

1) เป็นแนวคิดที่ดีหากจะมีการปรับปรุงกฎหมาย แต่ถ้าจะออกเป็นกฎหมายฉบับใหม่ จะต้องพิจารณาว่ามีความจำเป็นหรือไม่ หรือถ้าจะแก้ไขเพิ่มเติมกฎหมายที่มีอยู่ จะต้องพิจารณาว่าการแก้ไขเพิ่มเติมจะครอบคลุมกฎหมายทุกฉบับหรือไม่
2) ควรปลูกฝังประชาชนเรื่องคุณธรรมและจริยธรรมด้วย เพราะกฎหมายอย่างเดียวคงไม่เพียงพอ

ผู้แทนสถาบันการศึกษา

1) ให้ความสำคัญกับการกำหนดนิยามในกฎหมาย เพราะจะเชื่อมโยงไปสู่การกำหนดความผิดและการบังคับใช้กฎหมาย
2) การกำหนดความผิด ขอให้พิจารณาเป็น 2 ประเด็น คือ การกำหนดให้การใช้เทคโนโลยีปกปิดตัวตนกับองค์ประกอบของความผิดตามกฎหมาย และลักษณะของการให้อำนาจเจ้าหน้าที่ให้สามารถดำเนินการต่าง ๆ ได้ เช่น การใช้เทคโนโลยีในการถอดรหัส
3) การกำหนดกฎหมายไม่ควรก่อให้เกิดการละเมิดสิทธิส่วนบุคคลมากเกินไป
4) กฎหมายจะเน้นด้านการปราบปรามการกระทำความผิด ส่วนตัวมองว่า การปราบปรามความผิดกระทำได้ยาก เพราะไม่สามารถระบุตัวตนได้ จึงอยากให้เสริมในร่างกฎหมายในเรื่องของการป้องกันการกระทำความผิดด้วย แม้ว่าการป้องกันจะเป็นนโยบายเชิงรับก็ตาม แต่ก็ควรดำเนินการเท่าที่สามารถกระทำได้เพื่อป้องกันอาชญากรรมคอมพิวเตอร์ที่เกิดขึ้นในปัจจุบัน เช่น การป้องกันที่เริ่มจากตัวผู้ใช้อินเตอร์เน็ตเอง มิให้ตนเองตกเป็นเหยื่อ หรือการใช้เทคโนโลยีในการควบคุมอาชญากรรม เพราะอาชญากรรมที่เกิดบนโลกทางกายภาพ ก็เหมาะกับการใช้กฎหมายทางกายภาพในการป้องกันและปราบปราม ส่วนอาชญากรรมไซเบอร์ก็ควรใช้วิธีการทางไซเบอร์เข้ามาป้องกัน เช่น กรณีการป้องกันการถูกโจมตีระบบหรือการป้องกันการเข้าถึงระบบ สิ่งที่ดำเนินการได้นอกจากการป้องกัน

ระบบ การติดตามเส้นทางการเงิน อีกอย่างที่สามารถดำเนินการได้คือ การสร้างเทคโนโลยีเข้ามาเพื่อป้องกันการกระทำความผิด (Technological Protection Measure)

ผู้แทนสำนักงาน ปปง. – ควรมีกระบวนการในการรู้จักตัวตนของผู้ใช้บริการคอมพิวเตอร์ เทียบเคียงกับรูปแบบของการรายงานธุรกรรมของผู้มีหน้าที่รายงานตามกฎหมายฟอกเงิน ซึ่งก็จะให้ผู้มีหน้าที่รายงานมีหน้าที่ในการจัดให้ลูกค้าแสดงตน จึงเห็นว่าร่างกฎหมายควรมีข้อกำหนดลักษณะแบบนี้ เพื่อการระบุตัวตนของผู้ใช้บริการ

ประเด็นมาตรการความร่วมมือระหว่างหน่วยงานทั้งภายในประเทศและต่างประเทศที่จำเป็นต่อการป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตน

ความเห็นจากที่ประชุม

ผู้แทนสำนักงาน ปปง. – สำนักงาน ปปง. จะมีการประสานเพื่อแลกเปลี่ยนข้อมูลระหว่าง Egmont group กับสำนักงาน ปปง. ในฐานะหน่วยข่าวกรองทางการเงิน

ผู้แทนสำนักงานอัยการสูงสุด

1) ควรมีการประสานงานและให้ความร่วมมือระหว่างหน่วยงานและควรมีการจัดตั้งศูนย์ประสานงานกลาง
2) อาจพบปัญหาว่าต่างประเทศไม่ได้ให้ความร่วมมือกับไทย ดังนั้น ควรใช้ช่องทางหลักในการประสานงานตามปกติ แต่สิ่งที่ควรเพิ่มเติมคือ ควรให้เจ้าหน้าที่ของรัฐของประเทศไทยสร้างความสัมพันธ์ส่วนตัวกับเจ้าหน้าที่ของรัฐต่างประเทศ เนื่องจากการสร้างความสัมพันธ์ส่วนตัวจะเป็นตัวช่วยสนับสนุนการทำงานของเจ้าหน้าที่ให้มีประสิทธิภาพมากขึ้น

ประเด็นข้อเสนอแนะและมาตรการอื่นในการป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์

ความเห็นจากที่ประชุม

ผู้แทน บก. ปอศ. - ควรแก้ไขมาตรการป้องกันปราบปรามอาชญากรรมไร้ตัวโดยกำหนดให้เป็นส่วนหนึ่งของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไม่ควรตราเป็นกฎหมายฉบับใหม่ โดยการแก้ไขควรกำหนดนิยามคำว่า “อาชญากรรมไร้ตัวตน” ให้ชัดเจน กำหนดมาตรการทางกฎหมายที่เป็นเครื่องมือปราบปรามการกระทำความผิดเช่นเดียวกับกฎหมายว่าด้วยการสอบสวนคดีพิเศษ หรือกฎหมายป้องกันการมีส่วนร่วมในองค์กรอาชญากรรม จะเป็นการใช้กฎหมายที่มีอยู่ให้เป็นประโยชน์มากขึ้น โดยไม่จำเป็นต้องตราเป็นร่างกฎหมายใหม่

ผู้แทนสำนักงานอัยการสูงสุด

1) เนื่องจากการบังคับใช้กฎหมายกับผู้ที่รู้เห็นการกระทำความผิดจะบังคับได้ยาก จึงควรมีมาตรการบังคับอย่างอื่นนอกเหนือไปจากการบังคับโทษทางอาญา โดยอาจแก้ไขเพิ่มเติมกฎหมาย โดยใช้มาตรการบังคับอย่างอื่น เช่น การงดให้สัมปทานกับค่ายโทรศัพท์ในบางกรณี เป็นต้น หรือใช้มาตรการจูงใจให้ผู้ที่เกี่ยวข้องให้ความร่วมมือกับส่วนราชการและหน่วยงานที่เกี่ยวข้อง เช่น การลดหย่อนภาษีให้กับผู้ที่ให้ความร่วมมือกับส่วนราชการและหน่วยงานที่เกี่ยวข้อง เป็นต้น ซึ่งข้อมูลที่ผู้ประกอบการสามารถให้ได้ คือ ข้อมูลจราจรคอมพิวเตอร์และข้อมูลส่วนบุคคลของผู้ใช้บริการ

2) ควรมีการทบทวนกฎหมายที่เกี่ยวข้องกับมาตรการแฝงตัวหรืออำพรางตัว เพื่อแก้ไขกฎหมายให้ชัดเจนและลดปัญหาในการทำงานของเจ้าหน้าที่ที่จะเข้าไปดำเนินการแฝงตัวหรืออำพรางตัว

3) กฎหมายคุ้มครองข้อมูลส่วนบุคคลอาจทำให้มีปัญหาในการทำงาน เจ้าหน้าที่อาจทำงานยากขึ้น

4) ควรปรับปรุงกฎหมายให้เจ้าหน้าที่ที่เกี่ยวข้องสามารถใช้วิธีการแฝงตัวเพื่อเข้าถึงระบบคอมพิวเตอร์ได้โดยชอบกฎหมาย ภายใต้เงื่อนไขที่เหมาะสม เพื่อประโยชน์ในการสืบสวน

5) ประเด็นปัญหาเกี่ยวกับผู้ใช้บริการโทรศัพท์เคลื่อนที่ไม่ได้เป็นคนลงทะเบียนเอง แต่มีร้านรับลงทะเบียนแทน ซึ่งถ้ามีการนำหมายเลขเหล่านี้ไปใช้กระทำความผิดจะเป็นอุปสรรคในการดำเนินคดีอย่างยิ่ง จึงควรมีมาตรการป้องกันไม่ให้ผู้ที่ไม่ได้ใช้หมายเลขโทรศัพท์เคลื่อนที่ใด ๆ เป็นผู้จดทะเบียนใช้บริการหมายเลขโทรศัพท์เคลื่อนที่นั้น ๆ

6) ประเด็นเรื่องบัญชีม้า ควรแก้ไขกฎหมายเพื่อป้องกันการเปิดบัญชีม้าตามที่กล่าวในประเด็นที่ 3

7) มาตรการส่งมอบภายใต้การควบคุม (CD) เป็นไปได้ยากที่จะนำมาใช้กับกรณีนี้ เนื่องจากมาตรการดังกล่าวเป็นมาตรการควบคุมทางกายภาพ ดังนั้น จึงควรนำหลักการของมาตรการส่งมอบภายใต้การควบคุม (CD) มาประยุกต์ใช้กับกรณีนี้ โดยอาจเป็นเรื่องการควบคุมเส้นทางการใช้งานหรือความเคลื่อนไหวของอาชญากร หรือการสะกดรอยอาชญากร ซึ่งต้องพิจารณาว่าจะมีเทคโนโลยีอะไรมาช่วยในกรณีนี้

8) ควรพัฒนาบุคลากรที่เกี่ยวข้อง ไม่ว่าจะเป็นเจ้าพนักงานตำรวจ พนักงานอัยการ หรือเจ้าหน้าที่อื่นที่เกี่ยวข้อง และควรเปิดรับผู้ที่มีความรู้ความเชี่ยวชาญด้านคอมพิวเตอร์/ด้านเทคโนโลยีเข้ามาทำงานในกระบวนการยุติธรรมให้มากขึ้น เพราะประเด็นบุคลากรนับว่ามีความสำคัญมาก

ผู้แทนภาคธุรกิจ - เห็นด้วยกับมาตรา Know Your Business Customer

ผู้แทนสำนักงาน ปปง. - ของสำนักงาน ปปง. มีการเสนอร่างกฎหมายเกี่ยวกับการปราบปรามบัญชีม้าเช่นเดียวกับประมวลกฎหมายยาเสพติด

2. ปัญหาและอุปสรรคในการบังคับใช้กฎหมายและการป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์

2.1 ปัญหาการบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม กับอาชญากรรมไร้ตัวตนที่มีลักษณะการกระทำหลายขั้นตอน

อาชญากรรมไร้ตัวตนจัดเป็นอาชญากรรมไซเบอร์ซึ่งมีลักษณะการกระทำเชิงกระบวนการและประกอบด้วยการกระทำหลายขั้นตอน ดังจะเห็นได้จากการศึกษาภาพรวมในแง่รูปแบบเชิงกระบวนการของอาชญากรรมไร้ตัวตนดังกล่าวในบทที่ 2 ซึ่งพบว่า อาชญากรรมไซเบอร์แบบไร้ตัวตนที่กระทำต่อระบบหรือข้อมูลคอมพิวเตอร์ สามารถจำแนกการกระทำเป็น 2 ขั้นตอนคือ 1. ขั้นตอนการกระทำความผิดหลัก 2. ขั้นตอนการกระทำอันเป็นการปกปิดตัวตน ซึ่งจำแนกเป็น 2 กลุ่มพฤติกรรมย่อย คือ 2.1 การปกปิดตัวตนโดยไม่ใช้ข้อมูลระบุตัวผู้อื่น และ 2.2 การปกปิดตัวตนโดยใช้ข้อมูลส่วนบุคคลของผู้อื่น ซึ่งจำแนกเป็น 3 ขั้นตอนการกระทำย่อย ได้แก่ การได้มาซึ่งข้อมูลระบุตัวผู้อื่น การกระทำต่อข้อมูลก่อนนำไปใช้และการนำข้อมูลระบุตัวผู้อื่นไปใช้ปกปิดการกระทำผิด ดังนั้น การวิเคราะห์ปัญหาการบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กับอาชญากรรมไร้ตัวตนจึงต้องแยกพิจารณาตามการกระทำแต่ละขั้นตอนซึ่งอาจแตกต่างกันในรายละเอียด ดังนี้

2.1.1 การบังคับใช้ฐานความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กับการกระทำความผิดหลักของอาชญากรรมไร้ตัวตน

จากกรอบแนวคิดด้านความมั่นคงปลอดภัยทางคอมพิวเตอร์ ประกอบกับต้นแบบฐานความผิดตามอนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรป สามารถจำแนกอาชญากรรมอันเป็นเป้าหมายหรือการกระทำหลัก ได้ 3 กลุ่มคือ

1. อาชญากรรมคอมพิวเตอร์ที่ส่งผลกระทบต่อความปลอดภัยของระบบหรือข้อมูล กล่าวคือ อาชญากรรมที่มีคอมพิวเตอร์เป็นเป้าหมาย (Computer as target) ซึ่งฐานความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และอนุสัญญาอาชญากรรมไซเบอร์ของยุโรปกำหนดองค์ประกอบที่สามารถนำมาบังคับใช้ได้ ดังนี้

- การโจมตีในลักษณะของการเข้าถึงระบบที่มีมาตรการป้องกันด้วยวิธีการต่างๆ เช่น การเดารหัสผ่าน (Password guessing attack) อยู่ภายใต้องค์ประกอบการเข้าถึงระบบโดยมิชอบตามมาตรา 5 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

- บอทเน็ต (Botnets) เช่น การส่งคำสั่งเพื่อควบคุมเครื่องหรืออุปกรณ์ของเหยื่อให้กระทำการตามคำสั่งอยู่ภายใต้มาตรา 5 มาตรา 7 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

- การโจมตีระบบคอมพิวเตอร์ให้เกิดการปฏิเสธบริการ (Denial-of-Service หรือ DOS) อยู่ภายใต้มาตรา 10 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

- การใช้มัลแวร์ (Malicious software) ชนิดต่างๆ ซึ่งจะส่งผลกระทบต่อข้อมูลคอมพิวเตอร์ในแง่ความเสียหาย การแก้ไขเปลี่ยนแปลง อยู่ภายใต้มาตรา 9 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

- สแปม (Spam) เช่น การส่งข้อมูลคอมพิวเตอร์ปริมาณมากทำให้เกิดการรบกวนระบบหรือใช้การส่งข้อมูลเป็นพาหะของการแพร่มัลแวร์ อยู่ภายใต้มาตรา 11 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

2. อาชญากรรมคอมพิวเตอร์ที่โดยหลักแล้วไม่ส่งผลกระทบต่อความปลอดภัยของระบบหรือข้อมูล แต่มีเป้าหมายที่การหลอกลวงบุคคล เช่น การฉ้อโกงทางคอมพิวเตอร์ (Computer fraud) อยู่ภายใต้มาตรา 14 (1) แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 บางกรณีอาจใช้วิธีการที่กระทบต่อความปลอดภัยทางคอมพิวเตอร์ เช่น การใช้ชุดคำสั่งเพื่อหลอกลวงการทำงานของระบบ สำหรับการหลอกลวงที่ตัวบุคคลก็อาจใช้วิธีการที่ส่งผลกระทบต่อความปลอดภัยของระบบได้ขึ้นอยู่กับวิธีการและข้อเท็จจริง เช่น อาชญากรรมเข้าถึงบัญชีการใช้งานสื่อออนไลน์ของเหยื่อและควบคุมการเข้าถึงโดยเปลี่ยนรหัสผ่านเดิม และใช้บัญชีดังกล่าวไปกระทำการหลอกลวงฉ้อโกงเหยื่อรายอื่น กรณีนี้เป็นอาชญากรรมไร้ตัวตนประเภทฉ้อโกงหลอกลวงทางคอมพิวเตอร์ อยู่ภายใต้มาตรา 14 (1) แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

3. อาชญากรรมคอมพิวเตอร์ที่ไม่ส่งผลกระทบต่อความปลอดภัยของระบบหรือข้อมูล เช่น การโพสต์แชร์เนื้อหาผิดกฎหมาย (Content crime) ซึ่งเกี่ยวข้องกับมาตรา 14 (2)-(4) แต่ไม่อยู่ในขอบเขตของอนุสัญญาอาชญากรรมไซเบอร์ที่มีขอบเขตเฉพาะในส่วนเนื้อหาผิดกฎหมายที่เป็นสื่อลามกเด็ก

สรุปผลการศึกษาพบว่า พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยเฉพาะฐานความผิดต่อระบบหรือข้อมูลมาตรา 5-11 มีขอบเขตในแง่องค์ประกอบฐานความผิดที่ครอบคลุมและสามารถนำไปบังคับใช้กับการกระทำหลักหรือการกระทำอันเป็นเป้าหมายของอาชญากรรมไร้ตัวตนทั้งสามกลุ่ม และเป็นฐานความผิดที่มีหลักการสอดคล้องกับกรอบแนวทางระหว่างประเทศเช่นอนุสัญญาอาชญากรรมไซเบอร์ของสหภาพยุโรป

2.1.2 การบังคับใช้ฐานความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กับการกระทำเพื่อให้มีลักษณะไร้ตัวตนหรือการปกปิดตัวตน

ขั้นตอนที่สำคัญอันเป็นลักษณะเฉพาะของอาชญากรไร้ตัวตนอันแตกต่างจากอาชญากรรมไซเบอร์ประเภทอื่นคือ การกระทำเพื่อให้มีลักษณะความนิรนาม (Anonymity) โดยใช้วิธีการต่างๆ ซึ่งจะวิเคราะห์การปรับใช้ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ตามลักษณะวิธีการปกปิดตัวตน 2 รูปแบบดังนี้

(1) การบังคับใช้ฐานความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กับการปกปิดตัวตนโดยไม่ใช้ข้อมูลระบุตัวผู้อื่น

อาชญากรรมคอมพิวเตอร์ที่ใช้เทคโนโลยีปกปิดตัวตนโดยไม่ได้อาศัยข้อมูลระบุตัวของผู้อื่นอาจใช้เทคนิควิธีการหลายอย่าง ซึ่งจำแนกเป็นสองวิธีการหลักคือ การเข้ารหัสและการใช้โปรแกรมลบร่องรอยการกระทำ

(1) การใช้วิธีการเข้ารหัส (Encryption) อาจแยกได้เป็นสองกรณีคือ

กรณีที่หนึ่ง การเข้ารหัสที่ใช้เพื่อปกปิดตัวตนในการกระทำผิด เช่น การเข้ารหัสการสื่อสารหรือการทำธุรกรรมเพื่อไม่ให้ระบุตัวผู้เกี่ยวข้องได้ การเข้ารหัสโปรแกรมการสื่อสารแบบเรียลไทม์ระหว่างกลุ่มตัวการผู้ร่วมกระทำการ เพื่อไม่ให้เจ้าหน้าที่บังคับใช้กฎหมายสามารถเข้าถึงหรือตรวจสอบ

กรณีที่สอง การเข้ารหัสเพื่อใช้ปกปิดหลักฐานสำหรับการกระทำผิด เช่น การเข้ารหัสอุปกรณ์จัดเก็บข้อมูลที่มีหลักฐานการกระทำผิด[121]

---

[121] Dorothy E. Denning & William E. Baugh Jr (1999) HIDING CRIMES IN CYBERSPACE, Information, Communication & Society, 2:3, 251-276, DOI: 10.1080/136911899359583

วิเคราะห์การบังคับใช้ฐานความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กับการเข้ารหัสทั้งสองกรณีพบว่า ไม่เข้าข่ายองค์ประกอบความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 หากเป็นการกระทำต่อระบบหรือข้อมูลของตนเอง ทั้งนี้เพราะองค์ประกอบหลายฐานตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กำหนดว่าเป้าหมายการกระทำที่กฎหมายคุ้มครองต้องเป็น “ของผู้อื่น” เช่น การเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นโดยมิชอบตามมาตรา 5 การเข้าถึงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบตามมาตรา 7 แม้ว่าการเข้าหรัสอาจพิจารณาว่าเป็นการแก้ไขเปลี่ยนแปลงข้อมูลหรือชุดคำสั่งตามมาตรา 9 แต่ก็มีองค์ประกอบว่าต้องเป็นข้อมูลคอมพิวเตอร์ของผู้อื่น นอกจากนี้ การเข้ารหัสของอาชญากรมีมูลเหตุจูงใจเพื่อปกปิดการกระทำ อย่างไรก็ตาม องค์ประกอบความผิดที่อาจเกี่ยวข้องกับพฤติกรรมการเข้ารหัส เช่น มาตรา 5 มาตรา 7 และ มาตรา 9 ไม่ได้กำหนดมูลเหตุชักจูงใจ ดังนั้น การเข้ารหัสข้อมูลเพื่อปกปิดการกระทำจึงไม่เข้าข่ายฐานความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

(2) การใช้โปรแกรมหรือซอฟท์แวร์สำเร็จรูปในการปกปิดตัวตน หรือ ลบร่องรอย (Trace) ที่เกิดจากการสื่อสารหรือการกระทำทางอินเทอร์เน็ต[122]

วิเคราะห์การบังคับใช้ฐานความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กับการใช้โปรแกรมปกปิดหรือลบร่องรอยการกระทำพบว่า มีฐานความผิดที่เกี่ยวข้องคือการแก้ไขเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ของผู้อื่นตามมาตรา 9 ซึ่งอาจนำมาบังคับใช้หากข้อเท็จจริงปรากฏว่าอาชญากรทำการปกปิดตัวตนโดยใช้โปรแกรมแก้ไขเปลี่ยนแปลงหรือลบข้อมูลคอมพิวเตอร์ของบุคคลอื่น นอกจากนี้ หากการลบข้อมูลนั้นมีพฤติกรรมการเข้าถึงระบบโดยมิชอบมาก่อนก็อาจเข้าข่ายความผิดการเข้าถึงระบบโดยมิชอบตามมาตรา 5 ด้วย เช่น การเข้าถึงระบบของผู้ให้บริการโปรแกรมสนทนาเพื่อลบร่องรอยการล็อคอินเข้าใช้งานและร่องรอยข้อความสนทนา พฤติกรรมนี้เป็นการเข้าถึงระบบและทำการแก้ไขข้อมูลของผู้อื่นจึงเข้าองค์ประกอบมาตรา 5 และมาตรา 9

สรุปผลการศึกษาพบว่า พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยเฉพาะฐานความผิดต่อระบบหรือข้อมูลมาตรา 5 ถึงมาตรา 11 มีขอบเขตในแง่องค์ประกอบฐานความผิดที่มีข้อจำกัดในแง่การบังคับใช้กับการกระทำในขั้นตอนการปกปิดตัวตนของอาชญากรไร้ตัวตนในกรณีที่ใช้วิธีการเข้ารหัสข้อมูลหรืออุปกรณ์ของตนเอง แม้ว่าจะเป็นการกระทำที่เป็นอุปสรรคต่อการบังคับใช้กฎหมาย

[122] Jonathan Clough, Principle of Cybercrime, 2nd ed. (Cambridge University Press, 2015), pp. 6-8.

แต่โดยทั่วไปไม่เข้าองค์ประกอบความผิดตามพระราชบัญญัติฯ อย่างไรก็ตาม ฐานความผิดเกี่ยวกับการกระทำต่อระบบหรือข้อมูลตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 สามารถนำมาบังคับใช้กับการกระทำในขั้นตอนการปกปิดตัวตนของอาชญากรไร้ตัวตนในกรณีที่ใช้โปรแกรมลบร่องรอยการกระทำของตนซึ่งเป็นข้อมูลคอมพิวเตอร์ในระบบของบุคคลอื่น

(2) การบังคับใช้ฐานความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กับการปกปิดตัวตนโดยใช้ข้อมูลระบุตัวผู้อื่น

อาชญากรรมไร้ตัวตนซึ่งใช้วิธีการปกปิดตัวตนโดยอาศัยข้อมูลระบุตัวตนผู้อื่นอาจเรียกว่า “การโจรกรรมข้อมูลเอกลักษณ์หรืออัตลักษณ์ (Identity theft) ซึ่งในทางวิชาการจำแนกรูปแบบและขั้นตอนการกระทำได้หลายแนวทาง สำหรับในงานวิจัยนี้จำแนกการกระทำเป็น 3 ขั้นตอน โดยหัวข้อนี้จะนำฐานความผิดพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาวิเคราะห์การบังคับใช้กับการกระทำแต่ละขั้นตอน ดังนี้

1 ขั้นตอนการได้มาซึ่งข้อมูลระบุตัวตนของผู้อื่น

การกระทำในขั้นตอนนี้อาจใช้วิธีการที่หลากหลาย เมื่อนำกรอบแนวคิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์ที่กระทบต่อความปลอดภัยต่อระบบหรือข้อมูลมาวิเคราะห์ จะแยกพิจารณาได้สองกรณีคือ

- การได้มาโดยมีการเข้าถึงโดยมิชอบซึ่งระบบที่มีมาตรการป้องกัน (Unauthorized access) เพื่อให้ได้มาซึ่งข้อมูลระบุตัวเหยื่อ ซึ่งเป็นการกระทำที่กระทบต่อความปลอดภัยทางคอมพิวเตอร์ การกระทำเช่นนี้สามารถบังคับใช้ฐานความผิด มาตรา 5 และมาตรา 7

- การได้มาโดยไม่มีการเข้าถึงโดยมิชอบซึ่งระบบที่มีมาตรการป้องกัน เช่น การสืบค้นข้อมูลที่ปรากฏทั่วไปจากแหล่งออนไลน์ การกระทำเช่นนี้ไม่สามารถบังคับใช้ฐานความผิดมาตรา 5 มาตรา 7 เพราะไม่มีองค์ประกอบการกระทำ “เข้าถึง” ระบบหรือข้อมูลที่มีมาตรการป้องกัน

จะเห็นได้ว่า ฐานความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่เกี่ยวข้องกับการกระทำต่อระบบและข้อมูล มีองค์ประกอบสำคัญคือ “มาตรการป้องกันการเข้าถึง” ดังนั้น การนำฐานความผิดไปบังคับใช้กับอาชญากรรมไร้ตัวตนในขั้นตอนการได้มาซึ่งข้อมูลเหยื่อเพื่อนำมาปกปิดการกระทำนั้น จึงขึ้นอยู่กับว่าเป้าหมายหรือฐานข้อมูลมีมาตรการป้องกันการเข้าถึงหรือไม่ หากเป็นการเข้าถึงข้อมูลที่ไม่มีมาตรการป้องกันก็ไม่สามารถนำฐานความผิดนี้ไปบังคับใช้ได้

สำหรับกรณีที่อาชญากรใช้วิธีการได้มาซึ่งข้อมูลระบุตัวเหยื่อโดยไม่มีลักษณะการเข้าถึง (Access) แต่ใช้วิธีการหลอกลวงให้เหยื่อส่งข้อมูล จะไม่เกี่ยวข้องกับฐานความผิดมาตรา 5 - 7 แต่อาจเข้าข่ายความผิดฐานนำข้อมูลปลอมเท็จเข้าสู่ระบบตามมาตรา 14 (1) ซึ่งขึ้นอยู่กับวิธีการหลอกลวง เช่น การอ้างข้อเท็จจริงอันเป็นเท็จเพื่อให้เหยื่อส่งข้อมูลของตน

จากการวิเคราะห์การบังคับใช้ฐานความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กับการกระทำในขั้นตอนนี้พบว่า จึงพบว่าแม้กฎหมายนี้จะไม่ได้กำหนดฐานความผิดเฉพาะเกี่ยวกับการอาชญากรรมไร้ตัวตน แต่ฐานความผิดที่มีอยู่อาจนำมาปรับใช้กับอาชญากรรมประเภทนี้ในพฤติกรรมที่มีการเข้าถึงระบบหรือข้อมูลของผู้อื่นเพื่อที่จะได้มาซึ่งข้อมูล โดยการกระทำเช่นนี้อาจเกี่ยวข้องกับหลายฐานความผิดขึ้นอยู่กับวิธีการกระทำและองค์ประกอบของกฎหมายด้วย ลักษณะการบังคับใช้ฐานความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เช่นนี้สามารถเปรียบเทียบกับกฎหมายสหรัฐอเมริกา ซึ่งแม้ว่ากฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ระดับรัฐบาลกลางไม่ได้กำหนดความผิดเฉพาะสำหรับอาชญากรรมไร้ตัวตน แต่หากอาชญากรรมดังกล่าวทำการเข้าถึงข้อมูลหรือโจรกรรมข้อมูลเหยื่อเพื่อนำไปปกปิดตัวตน จะสามารถนำฐานความผิดเกี่ยวกับการเข้าถึงโดยปราศจากอำนาจมาใช้บังคับได้[123] เปรียบเทียบกับสหภาพยุโรป อนุสัญญาอาชญากรรมไซเบอร์ไม่ได้กำหนดความผิดเฉพาะเกี่ยวกับอาชญากรรมไร้ตัวตน แต่ในส่วนของพฤติกรรมการเข้าถึงข้อมูลบุคคลอื่นเพื่อนำมาใช้ปกปิดตัวตนนั้นจะเกี่ยวข้องกับฐานความผิดว่าด้วยการเข้าถึงระบบหรือข้อมูลโดยมิชอบคล้ายคลึงกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จึงเห็นได้ว่า พฤติกรรมของอาชญากรรมไร้ตัวตนในขั้นตอนการเข้าถึงข้อมูลนั้น ฐานความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 สามารถนำมาปรับใช้ได้แม้ว่าไม่มีฐานความผิดเฉพาะสำหรับอาชญากรรมไร้ตัวตนก็ตาม

2. ขั้นตอนการกระทำต่อข้อมูลระบุตัวของผู้อื่น

การกระทำในขั้นตอนนี้ยังไม่ใช่เป้าหมายหลักหรือวัตถุประสงค์สุดท้าย และยังไม่ใช่การนำข้อมูลไปใช้ปกปิดร่องรอยหรือการกระทำ แต่เป็นการกระทำหลังจากได้มาซึ่งข้อมูลระบุตัวของเหยื่อเพื่อเตรียมการก่อนการใช้ปกปิดตัวตนในขั้นตอนต่อไป โดยการกระทำในขั้นตอนนี้มีวิธีการหลากหลาย เช่น การนำข้อมูลระบุตัว

[123] คณาธิป ทองรวีวงศ์ (2566). มาตรการทางกฎหมายเกี่ยวกับการโจรกรรมข้อมูลส่วนบุคคลทางระบบคอมพิวเตอร์ : ศึกษาเปรียบเทียบกฎหมายไทยกับกฎหมายสหรัฐอเมริกา, รายงานสืบเนื่อง การประชุมวิชาการระดับชาติการวิจัยประยุกต์ “มิติใหม่ของโลกภายหลังจากการแพร่ระบาดของเชื้อไวรัส โคโรนา 2019 : ความท้าทายและโอกาส" ครั้งที่ 5” มหาวิทยาลัยนอร์ทกรุงเทพ.

บุคคลอื่นที่ได้มาไปใช้สมัครหรือลงทะเบียนใช้บริการการสื่อสาร บัญชีการใช้งานสื่อสังคมออนไลน์ เปิดบัญชีธนาคาร โดยการกระทำขั้นตอนนี้อาจมีลักษณะของการ “ครอบครอง ประมวลผล ดัดแปลงแก้ไข การส่งต่อ โอน เผยแพร่ จำหน่าย”

วิเคราะห์การบังคับใช้ฐานความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กับการกระทำในขั้นตอนนี้พบว่ามีฐานความผิดที่เกี่ยวข้องหลายฐานขึ้นอยู่กับวิธีการกระทำ เช่น

- การแก้ไขเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ของผู้อื่นตามมาตรา 9 ซึ่งอาจนำมาบังคับใช้หากข้อเท็จจริงปรากฏว่าอาชญากรทำการเตรียมข้อมูลโดยมีลักษณะของการแก้ไขเปลี่ยนแปลง

- การนำข้อมูลปลอมหรือเท็จเข้าสู่ระบบ ตามมาตรา 14 (1) ซึ่งอาจนำมาบังคับใช้หากข้อเท็จจริงปรากฏว่าอาชญากรนำข้อมูลระบุตัวบุคคลอื่นเข้าสู่ระบบสมัครการใช้งานต่างๆ แพลตฟอร์มการสื่อสาร การเปิดบัญชีการใช้บริการออนไลน์ต่างๆ โดยอ้างว่าเป็นการกระทำของเจ้าของข้อมูลนั้นซึ่งจะเป็นการนำข้อมูลปลอมหรือเท็จเข้าสู่ระบบ

อย่างไรก็ตาม เนื่องจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไม่ได้กำหนดความผิดอย่างเป็นระบบสำหรับพฤติกรรมการปกปิดตัวตนของอาชญากรรมไร้ตัวตน จึงอาจไม่สามารถบังคับใช้กับพฤติกรรมบางประการที่ไม่เข้าองค์ประกอบฐานความผิดที่มีอยู่ เช่น

- การซื้อขายแลกเปลี่ยนข้อมูลระบุตัวของเหยื่อที่ได้มาเพื่อให้เครือข่ายอาชญากรนำไปใช้ปกปิดตัวตน

- การโอนหรือส่งต่อข้อมูลระบุตัวของเหยื่อไปยังแหล่งอื่น หรือบุคคลอื่นที่จะนำไปใช้กระทำผิด

- การครอบครองหรือสร้างฐานข้อมูลที่เก็บรวบรวมข้อมูลระบุตัวของเหยื่อที่ได้มา

กรณีเช่นนี้ ฐานความผิดมาตรา 5 - 11 ไม่ได้กำหนดความผิดฐานซื้อขายแลกเปลี่ยนข้อมูลระบุตัวของผู้อื่น หรือฐานการครอบครองข้อมูลระบุตัว สำหรับฐานที่เกี่ยวข้องมีข้อจำกัด เช่น

- มาตรา 13 กำหนดความผิดที่มีองค์ประกอบในส่วนการกระทำคือ “จำหน่ายหรือเผยแพร่” แต่ก็จำกัดเฉพาะ การจำหน่ายหรือเผยแพร่ชุดคำสั่ง (Code) ไม่รวมถึงการจำหน่ายข้อมูลระบุตัวบุคคลของเหยื่อ และการจำหน่ายชุดคำสั่งตามมาตรา 13 จะต้องเป็นชุดคำสั่งที่นำไปใช้แป็นเครื่องมือกระทำผิดมาตรา 5 - 11 ด้วย จึงไม่สามารถนำมาบังคับใช้กับอาชญากรไร้ตัวตนในขั้นตอนการซื้อขายแลกเปลี่ยนหรือจำหน่ายข้อมูลระบุตัวของเหยื่อเพื่อนำมาใช้ปกปิดตัวตนและร่องรอยการประกอบอาชญากรรม

- มาตรา 16/2 กำหนดความผิดมีองค์ประกอบการกระทำคือ “ครอบครอง”[124] แต่ต้องเชื่อมโยงกับข้อมูลที่เป็นความผิดมาตรา 16/1 ที่จำเลยมีความผิดฐานนำข้อมูลเข้าสู่ระบบและศาลสั่งให้ลบหรือทำลาย เช่น เนื้อหาข้อมูลข่าวปลอม เนื้อหากระทบความมั่นคง เนื้อหาลามกอนาจาร จึงไม่สามารถนำมาบังคับใช้กับการครอบครองข้อมูลระบุตัวผู้อื่นซึ่งเป็นข้อมูลจริงก่อนที่จะนำไปใช้กระทำผิดหรือใช้เพื่อปกปิดตัวตนของอาชญากรต่อไป

ดังนั้น จะเห็นได้ว่า ฐานความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีข้อจำกัดในด้านองค์ประกอบการกระทำ เนื่องจากไม่ได้ร่างขึ้นเฉพาะสำหรับพฤติกรรมของอาชญากรรมไร้ตัวตนในขั้นตอนการนำข้อมูลระบุตัวผู้อื่นมากระทำการต่างๆ ก่อนนำไปใช้ปกปิดตัวตน เช่น ครอบครอง สร้างฐานข้อมูล แลกเปลี่ยน ฯลฯ เปรียบเทียบกับกฎหมายต่างประเทศพบว่า บางประเทศมีฐานความผิดที่อาจนำมาปรับใช้กับขั้นตอนการกระทำต่อข้อมูลส่วนบุคคล ซึ่งฐานความผิดดังกล่าวอาจไม่บัญญัติไว้ในกฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ โดยอาจตราเป็นกฎหมายเฉพาะ เช่น สหรัฐอเมริกามีกฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ (CFAA) แต่ไม่ได้กำหนดความผิดเกี่ยวกับการโจรกรรมข้อมูลส่วนบุคคลเพื่อนำไปใช้ปกปิดตัวตนของผู้กระทำหรือเพื่อวัตถุประสงค์อื่นใด[125] ซึ่งเป็นแนวทางคล้ายกฎหมายไทย แต่สหรัฐอเมริกามีกฎหมายการโจรกรรมข้อมูลส่วนบุคคลของสหรัฐอเมริกา (ITADA) กำหนดความผิดที่มีองค์ประกอบการกระทำ “โอน (Transfer) ครอบครอง (Possession) ซึ่งข้อมูลของผู้อื่นที่ได้มาจากการโจรกรรม ส่งผลให้สามารถปรับใช้กฎหมายกับขั้นตอนที่อาชญากรดำเนินการบางประการกับข้อมูลส่วนบุคคลดังกล่าว ก่อนนำไปใช้กระทำผิดอื่น[126] เช่น การซื้อขายข้อมูล การครอบครองหรือเก็บรักษาข้อมูลดังกล่าวไว้

3. ขั้นตอนการนำข้อมูลระบุตัวผู้อื่นไปใช้ปกปิดตัวตนของอาชญากร

การกระทำในขั้นตอนนี้อาจเกิดขึ้นร่วมกับการกระทำหลักอันเป็นวัตถุประสงค์หลักหรือเป้าหมายสุดท้าย (Target) ของอาชญากรรมแบบไร้ตัวตน เช่น การโจมตีระบบคอมพิวเตอร์ การทำลายข้อมูลของเป้าหมาย

---

[124] มาตรา 16/2 “ผู้ใดรู้ว่าข้อมูลคอมพิวเตอร์ในความครอบครองของตนเป็นข้อมูลที่ศาลสั่งให้ทำลายตามมาตรา 16/1 ผู้นั้นต้องทำลายข้อมูลดังกล่าว หากฝ่าฝืนต้องระวางโทษกึ่งหนึ่งของโทษที่บัญญัติไว้ในมาตรา 14 หรือมาตรา 16 แล้วแต่กรณี”

[125] DiSanto, P. F. (2015). Blurred lines of identity crimes: Intersection of the first amendment and federal identity fraud. Columbia Law Review., 115, p.941.

[126] คณาธิป ทองรวีวงศ์, มาตรการทางกฎหมายเกี่ยวกับการโจรกรรมข้อมูลส่วนบุคคลทางระบบคอมพิวเตอร์ : ศึกษาเปรียบเทียบกฎหมายไทยกับกฎหมายสหรัฐอเมริกา, รายงานสืบเนื่องการประชุมวิชาการระดับชาติการวิจัยประยุกต์ มิติใหม่ของโลกภายหลังจากการแพร่ระบาดของเชื้อไวรัส โคโรนา 2019 : ความท้าทายและโอกาส" ครั้งที่ 5”มหาวิทยาลัยนอร์ทกรุงเทพ 2566

การใช้มัลแวร์ การโจรกรรมข้อมูล การใช้มัลแวร์เรียกค่าไถ่ การโจมตีให้ระบบขัดข้องไม่สามารถใช้งานได้ รวมถึงการประกอบอาชญากรรมที่เกี่ยวข้องกับการได้มาซึ่งทรัพย์สิน เช่น การฉ้อโกงการลงทุน การกระทำผิดเกี่ยวกับบัตรเครดิต[127] ฯลฯ โดยในการประกอบอาชญากรรมดังกล่าวจะมีการใช้ข้อมูลระบุตัวของเหยื่อที่ได้จากการกระทำในขั้นตอนที่หนึ่งและขั้นตอนที่สอง เพื่อดำเนินการต่างๆ ให้เกิดความนิรนาม (Anonymity) หรือการปกปิดตัวตน ในการวิเคราะห์การบังคับใช้ฐานความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กับการกระทำในขั้นตอนนี้พบว่า ไม่มีฐานความผิดโดยเฉพาะที่กำหนดความผิดสำหรับการ “ใช้” ข้อมูลระบุตัวผู้อื่นโดยมิชอบ เมื่อพิจารณาฐานความผิดที่มีอยู่ประกอบกับพฤติกรรมการกระทำของอาชญากรแบบไร้ตัวตนจะสามารถแยกการปรับใช้กฎหมายตามผลกระทบต่อความปลอดภัยของระบบหรือข้อมูลดังนี้

- *การใช้ข้อมูลระบุตัวบุคคลอื่นในการประกอบอาชญากรรมที่กระทบต่อความปลอดภัยของระบบหรือข้อมูล โดยอาจมีลักษณะของการหลอกลวงบุคคลให้เข้าใจผิดหรือไม่ก็ได้* เช่น การใช้บัญชีสื่อสังคมออนไลน์ของบุคคลอื่นหรือบัญชีการใช้งานจดหมายอิเล็กทรอนิกส์ของผู้อื่นที่อาชญากรเข้าควบคุมตามขั้นตอนที่ 1 มาใช้ส่งไวรัสทำลายข้อมูลในระบบของเหยื่อ โดยผู้รับข้อความหรือจดหมายเข้าใจว่าส่งมาจากบัญชีของบุคคลที่ถูกนำข้อมูลระบุตัวมาใช้ ในส่วนของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กรณีเช่นนี้สามารถบังคับใช้ฐานความผิดแก้ไข ทำลาย ข้อมูลคอมพิวเตอร์ตามมาตรา 9

- *การใช้ข้อมูลระบุตัวบุคคลอื่นในการประกอบอาชญากรรมที่มีลักษณะหลอกลวงเหยื่อให้เข้าใจผิด โดยไม่ได้ส่งผลกระทบต่อความปลอดภัยทางคอมพิวเตอร์หรือไม่ใช่อาชญากรรมไซเบอร์โดยแท้ โดยเฉพาะการฉ้อโกงทางคอมพิวเตอร์* เช่น การใช้บัญชีสื่อสังคมออนไลน์ของบุคคลอื่นที่อาชญากรเข้าควบคุมตามขั้นตอนที่ 1 มาใช้หลอกลวงฉ้อโกงบุคคลอื่น ในส่วนของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แม้ว่าไม่ได้กำหนดความผิดฐาน “ใช้” ข้อมูลระบุตัวผู้อื่นโดยมิชอบ แต่เป็นการนำข้อมูลปลอมหรือเท็จเข้าสู่ระบบตามมาตรา 14 (1) หากเป็นการกระทำเพื่อประโยชน์ทางทรัพย์สินจะเข้าองค์ประกอบ “โดยทุจริต”

อย่างไรก็ตาม ปัญหาที่สำคัญประการหนึ่งของพฤติกรรมขั้นตอนนำข้อมูลไปใช้คือ การนำข้อมูลระบุตัวผู้อื่นไปทำให้ปรากฏ หรือแสดง หรือประกอบกับการสร้างร่องรอยทางอิเล็กทรอนิกส์ เพื่อปกปิดตัวตนของอาชญากร ทำให้เจ้าหน้าที่บังคับใช้กฎหมายทำการสืบสวนสอบสวนกับบุคคลเจ้าของข้อมูลที่เป็นเหยื่อ โดยอาชญากรรมหลักของอาชญากรที่ใช้วิธีการปกปิดตัวตนนั้นอาจเป็นการกระทำต่อความปลอดภัยของระบบ

---

[127] Federal Trade Commission, Consumer Fraud and Identity Theft Complain Data : January – December 2005 (Federal Trade Commission, 2006). p. 3.

หรือ การฉ้อโกงหลอกลวงบุคคลก็ได้ อย่างไรก็ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไม่ได้กำหนดฐานความผิดสำหรับการนำข้อมูลส่วนบุคคลผู้อื่นไปแสดงระบุตัวตนประกอบการกระทำความผิดต่างๆ เพื่อปกปิดตัวตนและทำให้เกิดความเข้าใจผิดว่าการกระทำความผิดนั้นเกิดจากเจ้าของข้อมูล จากเปรียบเทียบกับกฎหมายสหรัฐอเมริกาพบว่า กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ (CFAA) ไม่ได้กำหนดความผิดเกี่ยวกับการนำข้อมูลส่วนบุคคลของผู้อื่นไปใช้โดยมิชอบ แต่กฎหมายการโจรกรรมข้อมูลระบุตัว (ITADA) กำหนดความผิดสำหรับการ โอนหรือใช้ ซึ่งข้อมูลส่วนบุคคลของบุคคลอื่นโดยมีเจตนากระทำความผิดหรือสนับสนุนการกระทำความผิดซึ่งความผิดที่มุ่งกระทำนี้ไม่จำกัดเฉพาะการหลอกลวงหรือฉ้อโกงเท่านั้น[128] เนื่องจากคำว่า “โอน” (Transfer) หมายถึงการทำให้ข้อมูลส่วนบุคคลปรากฏหรือนำไปใช้ในที่อยู่ข้อมูลออนไลน์ใดๆ (Online location) ที่ปรากฏต่อบุคคลอื่น (18 U.S. Code § 1028 (10)) จึงรวมถึงการนำข้อมูลส่วนบุคคลของผู้อื่นไปใช้แสดงระบุตัวตนเพื่อให้เจ้าหน้าที่บังคับใช้กฎหมายเข้าใจว่าเป็นการกระทำของเจ้าของข้อมูล เพื่อปกปิดตัวตนของผู้กระทำแท้จริง ส่งผลให้เจ้าของข้อมูลตกเป็นผู้ต้องหาและได้รับผลกระทบต่อเสรีภาพ[129] ดังนั้น จึงเห็นได้ว่าแม้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีฐานความผิดที่สามารถปรับใช้ได้กับการปกปิดตัวตนของอาชญากร แต่ยังมีข้อจำกัดในการนำไปบังคับใช้กับอาชญากรรมไร้ตัวตนในขั้นตอนการนำข้อมูลผู้อื่นไปปิดบังหรือปกปิดการกระทำของตน

2.1.3 การบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กับอาชญากรรมไร้ตัวตนที่ในส่วนการกระทำหลักมีขั้นตอนเฉพาะ

รูปแบบอาชญากรรมไร้ตัวตนที่จำแนกเป็นขั้นตอนต่างๆ ดังวิเคราะห์ในหัวข้อ 2.1.1 และ 2.1.2 เป็นรูปแบบทั่วไปซึ่งปรับใช้ได้กับอาชญากรรมไร้ตัวตนลักษณะต่างๆ แม้ว่าอาชญากรรมไซเบอร์บางประเภทอาจมีขั้นตอนการกระทำหลักของตนเองเป็นการเฉพาะ แต่ในส่วนขั้นตอนการปกปิดตัวตนที่อาชญากรรมไซเบอร์แต่ประเภทนั้นนำมาใช้ ก็ยังสามารถประยุกต์กรอบขั้นตอนพฤติกรรมจากหัวข้อ 2.1.2 ได้ โดยในที่นี้จะยกตัวอย่าง

---

[128] Wyre, M., Lacey, D., & Allan, K. (2020). The identity theft response system. Trends and Issues in Crime and Criminal Justice, (592), pp.1-18.

[129] คณาธิป ทองรวีวงศ์, มาตรการทางกฎหมายเกี่ยวกับการโจรกรรมข้อมูลส่วนบุคคลทางระบบคอมพิวเตอร์ : ศึกษาเปรียบเทียบกฎหมายไทยกับกฎหมายสหรัฐอเมริกา, รายงานสืบเนื่องการประชุมวิชาการระดับชาติการวิจัยประยุกต์ มิติใหม่ของโลกภายหลังจากการแพร่ระบาดของเชื้อไวรัส โคโรนา 2019 : ความท้าทายและโอกาส" ครั้งที่ 5”มหาวิทยาลัยนอร์ทกรุงเทพ, 2566.

อาชญากรรมไซเบอร์ประเภทการฉ้อโกงหลอกลวง (Scam) ในกรณีการหลอกลวงเกี่ยวกับความสัมพันธ์เชิงความรัก (Romance scam) สามารถจำแนกขั้นตอนการกระทำเป็น 3 ขั้น ได้แก่[130]

(1) ขั้นตอนการแสวงหาเหยื่อ กล่าวคือ การสืบค้นข้อมูลหรือแสวงหาเหยื่อจากสื่อออนไลน์ เช่น เว็บไซต์จัดหาคู่หรือสื่อสังคมออนไลน์ (Social media) ในขั้นตอนนี้อาจยังไม่เป็นความผิดตามกฎหมายหากเป็นการค้นหาข้อมูลที่บุคคลทั่วไปเข้าถึงได้

(2) ขั้นตอนการสร้างความสัมพันธ์ กล่าวคือ อาชญากรติดต่อสร้างความรู้จัก ลักษณะพฤติกรรมของการกระทำในขั้นตอนนี้จะเป็นการยากที่จะจำแนกความแตกต่างจากการติดต่อสร้างความสัมพันธ์ระหว่างบุคคลในสังคมออนไลน์ จึงยังไม่เข้าองค์ประกอบความผิดเว้นแต่ปรากฏข้อเท็จจริงว่าในการสื่อสารข้อมูลในขั้นตอนนี้มีลักษณะข้อมูลอันเป็นเท็จตามมาตรา 14 (1)

(3) ขั้นตอนการแสวงประโยชน์ทางทรัพย์สิน โดยอาชญากรอาจเริ่มจากสิ่งเล็กน้อย เช่น ขอสิ่งของ ของขวัญ เพื่อเป็นการทดสอบเหยื่อ จากนั้นจะขอเงินจำนวนที่มากขึ้นโดยอ้างเหตุจำเป็นต่างๆ ขั้นตอนนี้แม้เป็นการนำข้อมูลเท็จเข้าสู่ระบบ แต่หากข้อเท็จจริงปรากฏว่าเป็นการสื่อสารหลอกลวงเฉพาะเหยื่อโดยเจาะจงตัว จะไม่เป็นความผิดมาตรา 14 (4) เพราะไม่มีพฤติการณ์ที่ประชาชนทั่วไปน่าจะเกิดความเสียหาย

จะเห็นได้ว่า ในส่วนของการบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กับการกระทำความผิดหลักในที่นี้คือการฉ้อโกงหลอกลวงด้านความรัก ฐานความผิดที่มีอยู่อาจนำมาบังคับใช้กับอาชญากรรมประเภทนี้เฉพาะในบางขั้นตอนของพฤติกรรม อีกทั้งยังอาจไม่สามารถบังคับใช้ได้กับทุกกรณีเนื่องจากขึ้นอยู่กับสภาพข้อเท็จจริงของการกระทำ อย่างไรก็ตาม อาชญากรรมประเภทนี้หากใช้วิธีการปกปิดตัวตน จะยังคงสามารถประยุกต์ใช้การวิเคราะห์ขั้นตอนการกระทำตามข้อ 2.1.2 โดยจำแนกขั้นตอนการปกปิดตัวตนเป็นขั้นตอนย่อย ซึ่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 อาจนำมาปรับใช้ได้อย่างจำกัดเฉพาะพฤติกรรมบางขั้นตอน ทั้งนี้ขึ้นอยู่กับข้อเท็จจริงและรายละเอียดของการกระทำเป็นกรณีไป

---

[130] คณาธิป ทองรวีวงศ์ และ ชลธิชา สมสอาด, การปรับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แก้ไขเพิ่มเติม พ.ศ. 2560 กับการหลอกลวงเกี่ยวกับความสัมพันธ์เชิงความรักที่กระทำทางระบบคอมพิวเตอร์: วารสารรัชต์ภาคย์ (สาขามนุษยศาสตร์และสังคมศาสตร์) ,ปีที่ 15 ฉบับที่ 39 มีนาคม – เมษายน 2564 , หน้า 230-239.

2.1.4 บทวิเคราะห์

สรุปผลการวิเคราะห์การบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กับอาชญากรรมไร้ตัวตน โดยจำแนกวิเคราะห์ตามขั้นตอนพฤติกรรม 2 ขั้นตอนหลักพบว่า

1. ในส่วนขั้นตอนการกระทำความผิดหลัก ฐานความผิดที่มีอยู่ปัจจุบันสามารถมีขอบเขตบังคับใช้ครอบคลุมขั้นตอนการกระทำความผิดหลักหรือความผิดที่เป็นเป้าหมายของอาชญากรรมไร้ตัวตน เช่น การส่งมัลแวร์ การโจรกรรมข้อมูล การแทรกแซงระบบ การทำให้เสียหายซึ่งข้อมูล ฯลฯ

2. ในส่วนขั้นตอนการกระทำอันเป็นการปกปิดตัวตน จำแนกเป็น 2 กลุ่มพฤติกรรมย่อย คือ

การปกปิดตัวตนโดยไม่ใช้ข้อมูลระบุตัวผู้อื่น พบว่าฐานความผิดที่มีอยู่ไม่ได้กำหนดหลักการเฉพาะสำหรับพฤติกรรมเหล่านี้และสามารถนำมาบังคับใช้กับการกระทำอันเป็นการปกปิดตัวตนได้อย่างจำกัดเฉพาะในกรณีที่วิธีการหรือลักษณะการกระทำเข้าองค์ประกอบของบางฐาน

การกระทำอันเป็นการปกปิดตัวตนโดยใช้ข้อมูลส่วนบุคคลของผู้อื่น จำแนกเป็น 3 ขั้นตอนการกระทำย่อยพบว่า ฐานความผิดที่มีอยู่ไม่ได้กำหนดหลักการเฉพาะสำหรับพฤติกรรมเหล่านี้ และสามารถนำมาบังคับใช้กับการกระทำอันเป็นการปกปิดตัวตนได้อย่างจำกัดเฉพาะในกรณีที่วิธีการหรือลักษณะการกระทำเข้าองค์ประกอบของบางฐาน เช่น ขั้นตอนการได้มาซึ่งข้อมูลอาจบังคับใช้ฐานความผิดเข้าถึงโดยมิชอบ ขั้นตอนการกระทำต่อข้อมูลก่อนนำไปใช้ อาจบังคับใช้ความผิดฐานแก้ไขเปลี่ยนแปลงข้อมูล แต่ไม่มีฐานความผิดการแลกเปลี่ยน การซื้อขาย การโอนข้อมูล ฯลฯ ขั้นตอนการนำข้อมูลไปใช้ อาจมีข้อจำกัดการบังคับใช้กับวิธีการนำข้อมูลระบุตัวผู้อื่นไปประกอบหรือสร้างร่องรอยทางระบบออนไลน์เพื่อปกปิดตัวตน ดังสรุปตามแผนภาพต่อไปนี้

2.2 ปัญหาการบังคับใช้กฎหมายด้านการสืบสวนสอบสวน

สืบเนื่องด้วยสภาพแวดล้อมดิจิทัลและความก้าวหน้าทางเทคโนโลยี ทำให้ผู้กระทำความผิดสามารถใช้วิธีปกปิดตัวตนในการกระทำความผิดได้หลากหลายรูปแบบและนำเทคโนโลยีมาใช้เป็นเครื่องมือในการกระทำความผิดและอาจมีการกระทำในลักษณะองค์กรอาชญากรรมและอาชญากรรมข้ามชาติ ทำให้พบปัญหาเรื่องการรวบรวมพยานหลักฐานเพื่อพิสูจน์ว่าใครเป็นผู้กระทำความผิดอย่างมาก ส่งผลให้การดำเนินคดีเป็นไปได้โดยยาก พยานหลักฐานอาจไม่เพียงพอดำเนินคดี หรือไม่สามารถตรวจสอบพยานหลักฐานบางอย่างได้ ดังนั้นในการสืบสวนสอบสวนความผิดประเภทนี้จำเป็นต้องใช้มาตรการพิเศษหรือเทคนิคในการสืบสวนสวนพิเศษซึ่งเป็นมาตรการที่บัญญัติเป็นพิเศษนอกเหนือไปจากที่บัญญัติไว้ในประมวลกฎหมายวิธีพิจารณาความอาญาอัน

เป็นมาตรการทั่วไปในคดีอาญา ทั้งนี้ เพื่อให้เป็นไปตามหลักการของอนุสัญญาสหประชาชาติเพื่อต่อต้านอาชญากรรมข้ามชาติที่จัดตั้งในลักษณะองค์กร ค.ศ. 2000 ซึ่งตามอนุสัญญาฯ อาชญากรรมคอมพิวเตอร์ถือเป็นประเภทของความผิดร้ายแรง โดยรูปแบบของการบัญญัติกฎหมายเพื่อกำหนดเทคนิคการสืบสวนสอบสวนพิเศษของประเทศไทย จะมีทั้งการกำหนดเป็นกฎหมายเฉพาะ ซึ่งได้แก่ พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 หรือการกำหนดเทคนิคการสืบสวนสอบสวนพิเศษไว้ในกฎหมายที่กำหนดฐานความผิดในแต่ละประเภทความผิด เช่น ประมวลกฎหมายยาเสพติด พระราชบัญญัติป้องกันและปราบปรามการค้ามนุษย์ พ.ศ. 2551 พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรม พ.ศ. 2556 เป็นต้น กล่าวได้ว่า ปัจจุบันประเทศไทยมีกฎหมายเกี่ยวกับสืบสวนสอบสวนด้วยวิธีพิเศษที่บังคับใช้กับอาชญากรรมแบบไร้ตัวตนที่กระทำต่อระบบหรือข้อมูลคอมพิวเตอร์ ได้แก่

1) พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 เป็นกฎหมายที่มุ่งปราบปรามการกระทำความผิดที่มีลักษณะเป็นอาชญากรรมพิเศษ อันเป็นความผิดที่ยากในการแสวงหาและรวบรวมพยานหลักฐาน โดยมุ่งเน้นต่อการนำตัวผู้กระทำความผิดมาลงโทษ โดยกฎหมายดังกล่าวกำหนดมาตรการพิเศษไว้ 2 มาตรการ ได้แก่ มาตรการเข้าถึงข้อมูล (มาตรการดักฟัง) และมาตรการแฝงตัวและการจัดทำเอกสารหลักฐานที่ใช้ในการแฝงตัว ซึ่งสามารถนำมาตรการดังกล่าวมาใช้บังคับกับความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้โดยมีเงื่อนไขบางประการ เนื่องจากถือเป็นคดีพิเศษตามมาตรา 21 (1) เป็นความผิดตามบัญชีท้ายของพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 ประกอบกับประกาศ กคพ. (ฉบับที่ 8) พ.ศ. 2565 เรื่อง กำหนดรายละเอียดของลักษณะของการกระทำความผิดที่เป็นคดีพิเศษ ตามมาตรา 21 วรรคหนึ่ง (1) แห่งพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 ที่ระบุว่าคดีพิเศษหมายถึง คดีความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ คดีความผิดที่มีบทกำหนดโทษตามมาตรา 5 มาตรา 6 มาตรา 7 มาตรา 8 มาตรา 9 มาตรา 10 มาตรา 11 มาตรา 12 มาตรา 14 และมาตรา 17 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ. 2550 และที่แก้ไขเพิ่มเติม โดยจะต้องเป็นความผิดที่มีลักษณะหนึ่งลักษณะใดดังนี้ (1) มีผลกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ ด้านความมั่นคง และบริการภาครัฐที่สำคัญ ด้านการเงิน ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ด้านการขนส่งและโลจิสติกส์ ด้านพลังงานและสาธารณูปโภค ด้านสาธารณสุข หรือด้านกระบวนการยุติธรรม (2) มีผลกระทบต่อความมั่นคงของประเทศ (3) มีผลกระทบต่อความสงบเรียบร้อยของสังคมหรือศีลธรรมอันดีของประชาชนอย่างร้ายแรง (4) มีผลกระทบต่อระบบเศรษฐกิจ การเงินการคลังของประเทศ

2) พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 มุ่งบังคับใช้กับคดีความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ โดยเป็นกฎหมายที่กำหนดมาตรการในการปราบปรามอาชญากรรมทางเศรษฐกิจที่มีลักษณะเป็นองค์กรอาชญากรรม ซึ่งหมายถึง คณะบุคคลตั้งแต่สามคนขึ้นไปที่รวมตัวกันช่วงระยะเวลาหนึ่งและร่วมกันกระทำการใด โดยมีวัตถุประสงค์เพื่อกระทำความผิดร้ายแรงและเพื่อได้มาซึ่งผลประโยชน์ทางการเงิน ทรัพย์สิน หรือผลประโยชน์ทางวัตถุอย่างอื่นไม่ว่าโดยทางตรงหรือทางอ้อม (บทนิยามในมาตรา 3) และกำหนดมาตรการสืบสวนสอบสวนพิเศษไว้ ได้แก่ 1) มาตรการเข้าถึงข้อมูล (มาตรการดักฟัง) 2) มาตรการสะกดรอยโดยใช้เครื่องมืออิเล็กทรอนิกส์ 3) มาตรการปฏิบัติการอำพรางและ 4) มาตรการจัดส่งภายใต้การควบคุม

3) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ให้อำนาจพนักงานเจ้าหน้าที่ในการตรวจสอบและเข้าถึงข้อมูลตามมาตรา 18 (6) ซึ่งบัญญัติให้อำนาจพนักงานเจ้าหน้าที่ในการตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้ แต่มีข้อจำกัดว่าจะใช้บังคับได้เฉพาะฐานความผิดที่ระบุไว้ในกฎหมายเท่านั้น

4) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีการให้อำนาจในลักษณะเป็นมาตรการเชิงป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ตามที่กำหนดไว้ในมาตรา 66 อาทิ มาตรการเข้าตรวจสอบสถานที่ หากมีเหตุอันควรเชื่อได้ว่ามีคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ มาตรการเข้าถึงข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทำสำเนาหรือสกัดคัดกรองข้อมูลสารสนเทศ หรือโปรแกรมคอมพิวเตอร์ ซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้อง หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ เป็นต้น แต่มาตรการดังกล่าวยังมีข้อจำกัดเฉพาะอาชญากรรมแบบไร้ตัวตนที่กระทำต่อระบบหรือข้อมูลคอมพิวเตอร์ที่ถึงขนาดเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรงเท่านั้น ซึ่งหมายถึง ภัยคุกคามที่มีลักษณะการเพิ่มขึ้นอย่างมีนัยสำคัญของการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ โดยมุ่งหมายเพื่อโจมตีโครงสร้างพื้นฐานสำคัญของประเทศ และการโจมตีดังกล่าวมีผลทำให้ระบบคอมพิวเตอร์ หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศ ความมั่นคงของรัฐ ความสัมพันธ์ระหว่างประเทศ การป้องกันประเทศ เศรษฐกิจ การสาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชนเสียหายจนไม่สามารถทำงานหรือให้บริการได้ ไม่รวมถึงภัยคุกคามทั่วไป

จากการศึกษาปัญหาการบังคับใช้มาตรการพิเศษกับอาชญากรรมแบบไร้ตัวตนที่กระทำต่อระบบหรือข้อมูลคอมพิวเตอร์พบว่า

1) แม้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ. 2550 และที่แก้ไขเพิ่มเติม จะเป็นความผิดตามบัญชีท้ายพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 ก็ตาม แต่มีข้อจำกัดกล่าวคือ ไม่มีฐานความผิดเฉพาะสำหรับอาชญากรรมไร้ตัวตนที่กระทำต่อระบบหรือข้อมูลคอมพิวเตอร์ ในกรณี 1) การได้มาซึ่งรหัสผ่านหรือมาตรการป้องกันของบุคคลอื่น 2) กระทำการใดๆ โดยทุจริต ในการใช้ ลายมือชื่ออิเล็กทรอนิกส์ รหัสผ่านหรือ สิ่งบ่งชี้หรือระบุตัวบุคคลใดๆ ของบุคคลอื่น 3) การเข้าถึงโดยมิชอบซึ่งข้อมูลระบุตัวของบุคคลอื่น โดยมีเจตนาทำลาย แก้ไข ทำซ้ำ หรือ แลกเปลี่ยน และ 4) การฉ้อโกงทางคอมพิวเตอร์ที่อาชญากรนำข้อมูลดิจิทัลที่ระบุตัวบุคคลอื่นมาให้บุคคลอื่นเข้าใจผิดหรือปกปิดตัวตน จึงทำให้เป็นช่องว่างที่ไม่สามารถใช้มาตรการสืบสวนสอบสวนที่บัญญัติไว้ในพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 กับความผิดประเภทดังกล่าวได้

2) มาตรการพิเศษตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 ยังไม่เพียงพอต่อการปราบปรามอาชญากรรมแบบไร้ตัวตนที่กระทำต่อระบบหรือข้อมูลคอมพิวเตอร์ เนื่องด้วยในกฎหมายกำหนดไว้เพียง 2 มาตรการ ได้แก่ มาตรการเข้าถึงข้อมูล (มาตรการดักฟัง) และมาตรการแฝงตัวและการจัดทำเอกสารหลักฐานที่ใช้ในการแฝงตัว ยังไม่ครบถ้วนตามมาตรฐานขั้นต่ำที่กำหนดไว้ในอนุสัญญาสหประชาชาติเพื่อต่อต้านอาชญากรรมข้ามชาติที่จัดตั้งในลักษณะองค์กร ค.ศ. 2000 อีกทั้งบทบัญญัติของมาตรการดังกล่าวยังมีปัญหาการตีความและบังคับใช้กฎหมายคือ บทบัญญัติตามมาตรา 27 ขาดนิยามความหมายของคำว่าแฝงตัว ทำให้เกิดปัญหาการใช้และการตีความ เพราะเป็นกฎหมายที่เป็นการล่วงละเมิดสิทธิและเสรีภาพ ซึ่งแม้กฎหมายจะให้อำนาจทำได้แต่จำเป็นต้องกำหนดรายละเอียดให้ชัดเจนและตีความอย่างเคร่งครัด การบัญญัติกฎหมายที่กว้างเกินไปอาจทำให้ขาดการตรวจสอบความชอบด้วยกฎหมายและเปิดโอกาสให้เจ้าหน้าที่รัฐและผู้เกี่ยวข้องใช้เป็นช่องทางในการแสวงหาประโยชน์โดยไม่ชอบ และในทางปฏิบัติมีปัญหาเกี่ยวกับการจัดทำเอกสารหลักฐานในการแฝงตัวอย่างมากภายใต้ข้อบังคับกรมสอบสวนคดีพิเศษ ว่าด้วยการจัดทำเอกสาร หลักฐานและการแฝงตัว พ.ศ. 2555 และฉบับที่ 2 พ.ศ. 2559 เนื่องจากหน่วยงานที่ได้รับการร้องขอจากกรมสอบสวนคดีพิเศษอาจอ้างกฎหมายภายในหน่วยงานซึ่งเป็นกฎหมายระดับพระราชบัญญัติเช่นเดียวกัน หรือมีข้อขัดข้องในการตีความกฎหมาย ทำให้ปฏิเสธไม่ให้ความร่วมมือ เพราะแต่ละหน่วยงานย่อมมีกฎหมายภายในของตนที่ไม่เปิดช่องให้สามารถกระทำการจัดทำเอกสารหลักฐานบางประเภทได้ เช่น เรื่องการทำบัตรประชาชนของกรมการปกครองจะมีข้อจำกัดอำนาจตาม

พระราชบัญญัติบัตรประจำตัวประชาชน พ.ศ. 2526 หรือการเปิดบัญชีธนาคารจะมีข้อจำกัดตามประกาศของธนาคารแห่งประเทศไทยประกอบกับพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 เป็นต้น ทำให้กฎหมายขาดสภาพบังคับ ซึ่งจากการรับฟังความเห็น ผู้แทนหน่วยงานบังคับใช้กฎหมายเห็นว่า ควรมีการทบทวนกฎหมายที่เกี่ยวข้องกับมาตรการแฝงตัวหรืออำพรางตัว เพื่อแก้ไขกฎหมายให้ชัดเจนและลดปัญหาในการทำงานของเจ้าหน้าที่ที่จะเข้าไปดำเนินการแฝงตัวหรืออำพรางตัว และควรปรับปรุงกฎหมายให้เจ้าหน้าที่ที่เกี่ยวข้องสามารถใช้วิธีการแฝงตัวเพื่อเข้าถึงระบบคอมพิวเตอร์ได้โดยชอบกฎหมาย ภายใต้เงื่อนไขที่เหมาะสม เพื่อประโยชน์ในการสืบสวน และเห็นควรนำหลักการของมาตรการส่งมอบภายใต้การควบคุม (CD) ซึ่งเป็นมาตรการพิเศษที่ไม่มีอยู่ในพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาประยุกต์ใช้กับอาชญากรรมประเภทนี้ โดยอาจเป็นเรื่องการควบคุมเส้นทางการใช้งานหรือความเคลื่อนไหวของอาชญากร หรือการสะกดรอยอาชญากร

3) การบังคับใช้พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 จะต้องปรากฏว่าเป็นอาชญากรรมแบบไร้ตัวตนนั้นเป็นความผิดที่มีลักษณะเป็นองค์กรอาชญากรรมข้ามชาติตามนิยามและองค์ประกอบความผิดของกฎหมายด้วย กล่าวคือ ต้องเป็นความผิดที่การกระทำโดยบุคคลตั้งแต่ 3 คนขึ้นไปและเป็นความผิดอาญาที่กฎหมายกำหนดโทษจำคุกขั้นสูงตั้งแต่ 4 ปีขึ้นไป โดยมีวัตถุประสงค์เพื่อให้ได้มาซึ่งผลประโยชน์ทางการเงินหรือผลประโยชน์ทางวัตถุอย่างอื่นไม่ว่าโดยทางตรงหรือทางอ้อม โดยความผิดที่กระทำนั้นได้กระทำในรัฐมากกว่าหนึ่งรัฐ หรือกระทำในรัฐหนึ่ง แต่มีส่วนสำคัญของการเตรียมการ การวางแผน การสั่งการ หรือการควบคุมเกิดขึ้นในอีกรัฐหนึ่ง หรือมีผลกระทบอย่างสำคัญในอีกรัฐหนึ่ง หรือกระทำในรัฐหนึ่งแต่เกี่ยวข้องกับองค์กรอาชญากรรมซึ่งเกี่ยวข้องกับกิจกรรมที่เป็นความผิดอาญาในรัฐมากกว่าหนึ่งรัฐ จึงไม่ครอบคลุมทุกฐานความผิดสำหรับอาชญากรรมไร้ตัวตนที่กระทำต่อระบบหรือข้อมูลคอมพิวเตอร์ และตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เนื่องจากจะเข้าองค์ประกอบความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติตามมาตรา 5 ได้จะต้องเป็น “ความผิดร้ายแรง” ด้วย กล่าวคือความผิดอาญาที่กฎหมายกำหนดโทษจำคุกขั้นสูงตั้งแต่สี่ปีขึ้นไปหรือโทษสถานที่หนักกว่านั้น ซึ่งความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 5 มาตรา 6 มาตรา 7 มาตรา 8 มาตรา 11 ไม่เข้าข่ายเป็นความผิดร้ายแรง และแม้จะเป็นความผิดร้ายแรงก็จะต้องเป็นความผิดที่กระทำในลักษณะองค์กรอาชญากรรมคือกระทำโดยบุคคลตั้งแต่สามคนขึ้นไปที่รวมตัวกันช่วงระยะเวลาหนึ่งและร่วมกันกระทำการใด โดยมีวัตถุประสงค์เพื่อกระทำความผิดร้ายแรงและเพื่อได้มาซึ่งผลประโยชน์ทางการเงินทรัพย์สิน หรือผลประโยชน์ทางวัตถุอย่างอื่นไม่ว่าโดยทางตรงหรือทางอ้อม ซึ่งอาชญากรรมไร้ตัวตนในบางครั้งอาจ

กระทำเพียงคนเดียว และอาจกระทำโดยไม่ได้มุ่งหวังให้ได้มาซึ่งผลประโยชน์ทางการเงิน ทรัพย์สินหรืออื่นใด เป็นเพียงการก่อความคุกคามเท่านั้น จึงไม่มีลักษณะเป็นองค์กรอาชญากรรมที่จะสามารถนำมาตรการพิเศษที่มีอยู่ตามพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 มาใช้บังคับได้

2.3 ปัญหาการรวบรวมพยานหลักฐานดิจิทัล

จากการศึกษาพบปัญหาการรวบรวมพยานหลักฐานดังนี้

1) ปัญหาระยะเวลาการเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ของผู้ให้บริการที่มีหน้าที่ต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 26 ประกอบกับประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564 ที่กำหนดให้ผู้ให้บริการอินเทอร์เน็ต (Internet Service Providers) ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แยกเป็น (1) กรณีทั่วไป ให้ผู้ให้บริการเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวัน นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ (2) กรณีจำเป็นเมื่อมีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ หรือเพื่อประโยชน์ในการรวบรวมข้อเท็จจริงและหลักฐานเกี่ยวกับการกระทำความผิดที่เกี่ยวข้องกับความมั่นคงแห่งราชอาณาจักร การก่อการร้าย องค์กรอาชญากรรมข้ามชาติ หรือความสงบเรียบร้อยของประชาชน ซึ่งได้ใช้ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์เป็นองค์ประกอบ หรือเป็นส่วนหนึ่งในการกระทำความผิด หรือมีข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับการกระทำความผิด ไม่ว่าข้อเท็จจริงในเหตุแห่งความจำเป็นดังกล่าวปรากฏต่อพนักงานเจ้าหน้าที่นั้นเอง หรือเมื่อได้รับการร้องขอจากเจ้าหน้าที่ผู้รับผิดชอบในการสืบสวนหรือสอบสวน ก่อนครบกำหนดเวลาตาม (1) ให้พนักงานเจ้าหน้าที่มีคำสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ของผู้ใช้บริการเป็นกรณีพิเศษเฉพาะรายต่อไปอีกคราวละไม่เกินหกเดือนต่อเนื่องกัน แต่ต้องไม่เกินสองปี โดยข้อมูลจราจรทางคอมพิวเตอร์ หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น ทั้งนี้ เป็นไปเพื่อประโยชน์ในการสืบสวนสอบสวนของพนักงานเจ้าหน้าที่เมื่อมีการกระทำความผิดเกิดขึ้น เพราะข้อมูลจราจรทางคอมพิวเตอร์นับเป็นพยานหลักฐานสำคัญในการดำเนินคดีอันเป็นประโยชน์อย่างยิ่งต่อการสืบสวน สอบสวน เพื่อนำตัวผู้กระทำความผิดมาลงโทษ จึงกำหนดให้ผู้ให้บริการมีหน้าที่ในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ดังกล่าว แต่อย่างไรก็ดี ระยะเวลาใน

การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ที่กำหนดไว้เพียง 90 วันนั้น ไม่เพียงพอต่อการสืบสวนสอบสวนหาตัวผู้กระทำความผิด

2) อาชญากรรมแบบไร้ตัวตนมีลักษณะและผลกระทบที่ไม่จำกัดพรมแดน การประกอบอาชญากรรมกรณีใดกรณีหนึ่งอาจส่งผลเกี่ยวเนื่องกับหลายประเทศ ทั้งตัวผู้ต้องหาและผู้ได้รับผลกระทบ รวมทั้งพยานหลักฐานและข้อมูลที่เกี่ยวข้องอาจกระจายอยู่ในเขตแดนหลายประเทศ ในทางปฏิบัติจึงพบปัญหาการขอข้อมูลจราจรคอมพิวเตอร์ที่อยู่ในต่างประเทศและการประสานความร่วมมือในการสืบสวน สอบสวน รวบรวมพยานหลักฐาน ที่จะต้องดำเนินการตามพระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. 2535 และที่แก้ไขเพิ่มเติม ซึ่งการประสานขอความร่วมมือในการขอความช่วยเหลือในเรื่องเกี่ยวกับการดำเนินการสืบสวน สอบสวน ฟ้องคดี ริบทรัพย์สิน และการดำเนินการอื่น ๆ ที่เกี่ยวเนื่องกับคดีอาญาเป็นอำนาจของอัยการสูงสุดหรือผู้ซึ่งอัยการสูงสุดมอบหมายในฐานะเป็นผู้ประสานงานกลางตามมาตรา 6 โดยมีหน้าที่รับคำร้องขอความช่วยเหลือจากหน่วยงานของรัฐบาลไทยและส่งให้ประเทศผู้รับคำร้องขอตามมาตรา 7 ทำให้เกิดกระบวนการขั้นตอนการประสานงานที่ต้องใช้ระยะเวลา ส่งผลให้การดำเนินคดีและการรวบรวมพยานหลักฐานประเภทนี้กระทำได้ล่าช้า

3) การขาดกฎหมายพยานดิจิทัลเป็นการเฉพาะ แม้ว่าปัจจุบันกฎหมายที่เกี่ยวข้องกับการรับฟังพยานดิจิทัลปรากฏตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาตรา 11 ที่บัญญัติห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์ รวมถึงสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในกระบวนการพิจารณาตามกฎหมายทั้งในคดีแพ่ง คดีอาญา หรือคดีอื่นใด เพียงเพราะเหตุว่าเป็นข้อมูลอิเล็กทรอนิกส์ และในการชั่งน้ำหนักพยานหลักฐานว่าข้อมูลอิเล็กทรอนิกส์จะเชื่อถือได้หรือไม่เพียงใดนั้นให้พิเคราะห์ถึงความน่าเชื่อถือของลักษณะหรือวิธีการที่ใช้สร้าง เก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์ ลักษณะหรือวิธีการเก็บรักษา ความครบถ้วน และไม่มีการเปลี่ยนแปลงของข้อความลักษณะ หรือวิธีการที่ใช้ในการระบุหรือแสดงตัวผู้ส่งข้อมูล รวมทั้งพฤติการณ์ที่เกี่ยวข้องทั้งปวง และตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 25 ก็ได้บัญญัติให้ ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้ให้อ้างและรับฟังเป็นพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญาหรือกฎหมายอื่นอันว่าด้วยการสืบพยานได้ แต่ต้องเป็นชนิดที่มิได้เกิดขึ้นจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบประการอื่น แต่อย่างไรก็ดี การที่กฎหมายกำหนดให้ข้อมูลอิเล็กทรอนิกส์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์สามารถอ้างและรับฟังได้นั้น ไม่ได้มีผลต่อการกำหนดให้พยานดิจิทัลเป็นพยานหลักฐานอีกประเภทหนึ่ง เป็นเพียงพยานเอกสารหรือพยานวัตถุท่านั้น

เนื่องจากไม่มีกฎหมายบัญญัติเรื่องการรับฟังและชั่งน้ำหนักพยานดิจิทัลไว้เป็นการเฉพาะ แม้ในปัจจุบันศาลไทยให้การยอมรับและรับฟังพยานหลักฐานดิจิทัล แต่การพิสูจน์ อ้างอิง หรือการนำสืบก็ยังมีความท้าทายอย่างมากและในหลายครั้งเกิดเป็นข้อโต้แย้งเมื่อมีการอ้างอิง ตัวอย่างปัญหาที่พบเมื่อมีการอ้างอิง พยานหลักฐานดิจิทัล เช่น การอ้างข้อมูลคอมพิวเตอร์ซึ่งเป็นสิ่งไม่มีรูปร่างและไม่สามารถจับต้องได้โดยตรงทั้งยังสามารถถูกเปลี่ยนแปลงได้โดยง่ายมาเป็นพยานหลักฐานนั้น จะเชื่อได้อย่างไรว่าข้อมูลที่ได้มานั้นมีความครบถ้วน สมบูรณ์และมีความน่าเชื่อถือ ข้อโต้แย้งเรื่องข้อมูลพยานหลักฐานที่อยู่ในรูปดิจิทัลอาจถูกเปลี่ยนแปลงในระหว่างกระบวนการรวบรวมพยานหลักฐาน หรือข้อโต้แย้งเรื่องความน่าเชื่อถือของผลการวิเคราะห์และตรวจพิสูจน์ พยานหลักฐานดิจิทัล เป็นต้น[131]

4) ปัญหาอื่น ๆ อาทิ ปัญหาเรื่องงบประมาณในการตรวจพิสูจน์พยานหลักฐานดิจิทัลตามกฎหมาย ปัญหาพนักงานเจ้าหน้าที่และพนักงานสอบสวนขาดความรู้ในการจัดเก็บพยานหลักฐานดิจิทัล

2.4 ปัญหาการดำเนินการกับทรัพย์สินและการตรวจสอบเส้นทางการเงิน

โดยสภาพของอาชญากรรมไร้ตัวตนนอกจากจะยากต่อการติดตามตัวผู้กระทำความผิดมาลงโทษแล้ว การติดตามทรัพย์สินหรือการตรวจสอบเส้นทางการเงินของผู้กระทำความผิดก็เป็นไปได้ยาก สืบเนื่องจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไม่ได้มีการกำหนดหมวดว่าด้วยการดำเนินการกับทรัพย์สินไว้เป็นการเฉพาะ และไม่ได้เป็นความผิดมูลฐานตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงินจึงไม่สามารถนำมาตรการร้องขอให้ทรัพย์สินตกเป็นของแผ่นดินตามกฎหมายฟอกเงินซึ่งเป็นมาตรการที่มีประสิทธิภาพ เนื่องเป็นกระบวนการพิจารณาคดีต่อตัวทรัพย์สินโดยตรง โดยไม่ต้องคำนึงถึงความผิดของเจ้าของทรัพย์สินมาใช้บังคับกับทรัพย์สินที่เกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้ ดังนั้น การดำเนินการกับทรัพย์สินจึงต้องดำเนินการตามประมวลกฎหมายอาญา มาตรา 32 และมาตรา 33 ที่กำหนดให้ริบสำหรับทรัพย์ที่มีไว้เป็นความผิด ใช้ในการกระทำความผิด หรือไม่เพื่อใช้ในการกระทำความผิด หรือได้มาจากการกระทำความผิด ซึ่งจะสามารถริบได้ทั้งหมด เว้นแต่จะเข้ายกเว้นเนื่องจากเป็นทรัพย์ของบุคคลภายนอกที่ไม่ได้รู้เห็นในการกระทำผิดนั้นด้วย ซึ่งเป็นแนวคิดการริบทรัพย์ทางอาญาที่ต้องยึดโยงกับความผิดอาญาที่เป็นที่มาของทรัพย์สินที่ได้จากการกระทำความผิด จึงมีแนวคิดในการกำหนดให้ความผิดตามพระราชบัญญัติว่าด้วยการกระทำ

[131] โปรดดู สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) , ข้อเสนอแนะมาตรฐาน การจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐาน , Feedback-Device-Management-standard-in-digital-forensic-evidence.pdf (etda.or.th)

ความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นความผิดมูลฐานตามกฎหมายฟอกเงิน เพื่อเปิดช่องให้สำนักงานป้องกันและปราบปรามการฟอกเงินสามารถดำเนินการกับทรัพย์สินที่เกี่ยวกับการกระทำความผิดในความผิดประเภทนี้ได้ โดยเป็นการนำหลักการของมาตรการริบทรัพย์ทางแพ่ง หรือ กระบวนการฟ้องร้องเพื่อริบทรัพย์ทางแพ่งต่อตัวทรัพย์สิน หรือ Civil Forfeiture ที่ไม่ผูกติดกับคดีอาญามาใช้ โดยอาศัยเหตุและหลักฐานอันควรเชื่อได้ว่าเป็นทรัพย์สินที่เกี่ยวกับการกระทำความผิด มาตรการดำเนินการกับทรัพย์สินตามกฎหมายฟอกเงินจะทำให้สามารถดำเนินการตัดวงจรของเครือข่ายองค์กรอาชญากรรมได้

2.5 ปัญหาขอบเขตการบังคับใช้พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 ที่ยังไม่ครอบคลุมความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 มีผลใช้บังคับเมื่อวันที่ 17 มีนาคม 2566 เป็นกฎหมายที่มุ่งปราบปรามการกระทำความผิดอาชญากรรมทางเทคโนโลยี โดยการกำหนดมาตรการที่สำคัญ อาทิ

- มาตรการในการเปิดเผยหรือแลกเปลี่ยนข้อมูลระหว่างหน่วยงานรัฐและเอกชน กล่าวคือ ให้สถาบันการเงินและผู้ประกอบธุรกิจมีหน้าที่เปิดเผยหรือแลกเปลี่ยนข้อมูลเกี่ยวกับบัญชีและธุรกรรมของลูกค้าที่เกี่ยวข้องในระหว่าง สถาบันการเงินและผู้ประกอบธุรกิจนั้นผ่านระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูล ที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ สำนักงานป้องกันและปราบปรามการฟอกเงินและธนาคารแห่งประเทศไทย เห็นชอบร่วมกัน (มาตรา 4)

- มาตรการในการสั่งให้ผู้ให้บริการเครือข่ายโทรศัพท์ ผู้ให้บริการโทรคมนาคมอื่น หรือผู้ให้บริการอื่น ที่เกี่ยวข้องกับการกระทำความผิดเปิดเผยข้อมูลที่เกี่ยวข้องเท่าที่จำเป็นและมีหน้าที่ส่งข้อมูลดังกล่าว (มาตรา 5)

- มาตรการในการระงับการทำธุรกรรม ในกรณีที่สถาบันการเงินหรือผู้ประกอบธุรกิจพบเหตุอันควรสงสัยเองหรือได้รับข้อมูลจากระบบหรือกระบวนการเปิดเผยหรือแลกเปลี่ยนข้อมูลว่าบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ใดถูกใช้หรืออาจถูกใช้ทำธุรกรรมที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี หรือการกระทำความผิดมูลฐานหรือความผิดฐานฟอกเงินตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน (มาตรา 6)

- มาตรการระงับการทำธุรกรรมชั่วคราวในกรณีที่สถาบันการเงินหรือผู้ประกอบธุรกิจได้รับแจ้งจากผู้เสียหาย ซึ่งเป็นผู้ถือบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ว่า ได้มีการทำธุรกรรมโดยบัญชีเงินฝากหรือ บัญชีเงินอิเล็กทรอนิกส์ดังกล่าวและเข้าข่ายเกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี (มาตรา 7)

- มาตรการในการปราบปรามบัญชีม้า โดยกำหนดความผิดกรณีผู้ใดเปิดหรือยินยอมให้บุคคลอื่นใช้บัญชีเงินฝาก บัตรอิเล็กทรอนิกส์ หรือบัญชีเงินอิเล็กทรอนิกส์ของตน โดยมิได้มีเจตนาใช้เพื่อตนหรือเพื่อกิจการที่ตนเกี่ยวข้อง หรือยินยอมให้บุคคลอื่นใช้หรือยืมใช้เลขหมายโทรศัพท์สำหรับบริการโทรศัพท์เคลื่อนที่ของตน ทั้งนี้ โดยประการที่รู้หรือควรรู้ว่าจะนำไปใช้ในการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีหรือความผิดทางอาญาอื่นใด กำหนดระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินสามแสนบาท หรือทั้งจำทั้งปรับ (มาตรา 9)

- มาตรการกำหนดโทษในกรณีผู้ใดเป็นธุระจัดหา โฆษณา หรือไขข่าวโดยประการใด ๆ เพื่อให้มีการซื้อ ขาย ให้เช่า หรือให้ยืม บัญชีเงินฝาก บัตรอิเล็กทรอนิกส์ หรือบัญชีเงินอิเล็กทรอนิกส์ เพื่อใช้ในการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีหรือความผิดทางอาญาอื่นใด ต้องระวางโทษจำคุก ตั้งแต่สองปีถึงห้าปี หรือปรับตั้งแต่สองแสนบาทถึงห้าแสนบาท หรือทั้งจำทั้งปรับ (มาตรา 10)

- มาตรการกำหนดโทษในกรณีผู้ใดเป็นธุระจัดหา โฆษณา หรือไขข่าวโดยประการใด ๆ เพื่อให้มีการซื้อ หรือขายเลขหมายโทรศัพท์สำหรับบริการโทรศัพท์เคลื่อนที่ ซึ่งลงทะเบียนผู้ใช้บริการในนามของบุคคลหนึ่งบุคคลใดแล้ว แต่ไม่สามารถระบุตัวผู้ใช้บริการได้ โดยกำหนดระวางโทษจำคุกตั้งแต่สองปีถึงห้าปี หรือปรับตั้งแต่สองแสนบาทถึงห้าแสนบาท หรือทั้งจำทั้งปรับ (มาตรา 11)

ทั้งนี้ ขอบเขตในการบังคับใช้กฎหมายดังกล่าว ได้กำหนดนิยามคำว่า “อาชญากรรมทางเทคโนโลยี” ให้หมายความว่า การกระทำหรือพยายามกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เพื่อฉ้อโกง กรรโชก หรือรีดเอาทรัพย์ บุคคลหนึ่งบุคคลใด หรือโดยประการที่น่าจะทำให้บุคคลอื่นเสียหาย หรือกระทำความผิดฐานฉ้อโกง กรรโชก หรือรีดเอาทรัพย์ โดยใช้ระบบคอมพิวเตอร์เป็นเครื่องมือ ไม่รวมถึงการกระทำความผิดต่อระบบหรือข้อมูลคอมพิวเตอร์ ดังนั้น มาตรการบังคับใช้กฎหมายที่จำกัดเฉพาะอาชญากรรมทางเทคโนโลยี ไม่รวมถึงความผิดอาญาอื่น จึงไม่สามารถนำมาใช้บังคับกับการกระทำความผิดในรูปแบบอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ได้ เว้นแต่มีการกระทำที่คาบเกี่ยวกันและเข้าองค์ประกอบนิยามของอาชญากรรมทางเทคโนโลยีและต้องมีเจตนาพิเศษตามกฎหมายด้วย เพราะจากนิยาม จะเห็นว่าองค์ประกอบสำคัญของอาชญากรรมทางเทคโนโลยีตามพระราชกำหนด จะต้องมีเจตนาพิเศษตามกฎหมายอาญา กล่าวคือ ต้องมีมูลเหตุในการกระทำความผิด โดยจะต้องเป็นไปเพื่อฉ้อโกง กรรโชก หรือรีดเอาทรัพย์ บุคคลหนึ่งบุคคลใด หรือโดยประการที่น่าจะทำให้บุคคลอื่นเสียหาย ดังนั้น การวินิจฉัยความผิดทางอาญาของบุคคลผู้กระทำนั้นจะต้องพิจารณาถึงองค์ประกอบของเจตนาธรรมดาและเจตนาพิเศษให้ครบถ้วน หากขาดส่วนใดส่วนหนึ่งไปแล้วย่อมไม่ครบองค์ประกอบความผิดของกฎหมายและไม่อาจถือได้ว่า

ผู้กระทำมีเจตนาเป็นความผิดตามกฎหมายได้ ดังนั้น จึงทำให้ความผิดอาชญากรรมแบบไร้ตัวตนตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ ที่ที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ตามมาตรา 5 ถึงมาตรา 11 กล่าวคือ ฐานความผิดการเข้าถึงระบบโดยมิชอบ (มาตรา 5) ฐานความผิดการเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ (มาตรา 7) ฐานความผิดเปิดเผยมาตรการป้องกันการเข้าถึง (มาตรา 6) ฐานความผิดดักรับข้อมูลคอมพิวเตอร์ (มาตรา 8) ฐานความผิดแก้ไขเปลี่ยนแปลงข้อมูล (มาตรา 9) ฐานความผิดขัดขวางการทำงานของระบบ (มาตรา 10) ฐานความผิดสแปม (มาตรา 11) ที่ไม่ได้มีเจตนาพิเศษกระทำไปเพื่อการฉ้อโกง กรรโชก หรือรีดเอาทรัพย์ ไม่เข้าตามนิยามความหมายดังกล่าว จึงไม่อยู่ขอบเขตการบังคับใช้ของพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 เป็นช่องว่างที่ไม่สามารถนำมาตรการบางเรื่องมาใช้บังคับได้ ได้แก่ มาตรการในการเปิดเผยหรือแลกเปลี่ยนข้อมูลระหว่างหน่วยงานรัฐและเอกชนตามมาตรา 4 มาตรการในการสั่งให้ผู้ให้บริการเครือข่ายโทรศัพท์ ผู้ให้บริการโทรคมนาคมอื่น หรือผู้ให้บริการอื่นที่เกี่ยวข้องกับการกระทำความผิดเปิดเผยข้อมูลที่เกี่ยวข้องเท่าที่จำเป็นและมีหน้าที่ส่งข้อมูล ตามมาตรา 5 มาตรการในการระงับการทำธุรกรรมตามในกรณีที่สถาบันการเงินหรือผู้ประกอบธุรกิจพบเหตุอันควรสงสัยเองตามมาตรา 6 และมาตรการระงับการทำธุรกรรมชั่วคราวในกรณีที่สถาบันการเงินหรือผู้ประกอบธุรกิจได้รับแจ้งจากผู้เสียหาย ตามมาตรา 7 คงใช้ได้เฉพาะมาตรการในการปราบปรามบัญชีม้าตามมาตรา 9 และกำหนดโทษสำหรับผู้ที่เป็นธุระจัดหา โฆษณา หรือไขข่าวโดยประการใด ๆ เพื่อให้มีการซื้อ ขาย ให้เช่า หรือให้ยืม บัญชีเงินฝาก บัตรอิเล็กทรอนิกส์ หรือบัญชีเงินอิเล็กทรอนิกส์ ตามมาตรา 10 ที่กำหนดบังคับใช้กับกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีหรือความผิดทางอาญาอื่นใดด้วย และมาตรการกำหนดโทษในกรณีผู้ใดเป็นธุระจัดหา โฆษณา หรือไขข่าวโดยประการใด ๆ เพื่อให้มีการซื้อ หรือขายเลขหมายโทรศัพท์สำหรับบริการโทรศัพท์เคลื่อนที่ ซึ่งลงทะเบียนผู้ใช้บริการในนามของบุคคลหนึ่งบุคคลใดแล้ว แต่ไม่สามารถระบุตัวผู้ใช้บริการได้ตามมาตรา 11 ซึ่งกำหนดโทษเมื่อครบองค์ประกอบความผิดโดยไม่ได้จำกัดการบังคับใช้เฉพาะความผิดอาชญากรรมทางเทคโนโลยี

3. การกำหนดฐานความผิดของกฎหมายต้นแบบเพื่อป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์

จากกรอบแนวคิดทฤษฎีและแนวทางการร่างกฎหมายต้นแบบเกี่ยวกับอาชญากรรมไซเบอร์ในระดับระหว่างประเทศปัจจุบัน ได้แก่ แนวทางกฎหมายต้นแบบของสหประชาชาติและแนวทางกฎหมายต้นแบบของสหภาพยุโรปพบว่า ยังไม่มีการกำหนดนิยามของอาชญากรรมไร้ตัวตนในลักษณะนิยามความหมายกลาง

อันครอบคลุมพฤติกรรมเป็นการทั่วไปอย่างเป็นสากลของอาชญากรรมประเภทนี้ เนื่องจากลักษณะการกระทำมีความหลากหลาย ดังนั้น แนวทางที่เหมาะสมในการพัฒนากฎหมายต้นแบบจึงเป็นการร่างตัวแบบฐานความผิด (Model offence) ที่ครอบคลุมพฤติกรรมเชิงกระบวนการของอาชญากรรมไร้ตัวตน ซึ่งแบ่งเป็นสองแนวทางหลัก คือ การกำหนดความผิดต้นแบบสำหรับอาชญากรรมที่ใช้วิธีปกปิดตัวตน และการกำหนดฐานความผิดต้นแบบสำหรับอาชญากรรมไร้ตัวตนที่มีลักษณะการฉ้อโกง ซึ่งผู้วิจัยจะนำกรอบแนวทางระหว่างประเทศที่เกี่ยวข้องมาศึกษาและเปรียบเทียบกับกฎหมายไทย

3.1 ฐานความผิดเฉพาะสำหรับอาชญากรรมซึ่งใช้วิธีปกปิดตัวตน

ฐานความผิดเฉพาะสำหรับอาชญากรรมซึ่งใช้วิธีการปกปิดตัวตนตามร่างของสนธิสัญญาสหประชาชาติมีประเทศสมาชิกเสนอรายละเอียดและองค์ประกอบความผิดต้นแบบสำหรับฐานนี้แตกต่างกันเป็น 3 แนวทาง ซึ่งจะนำมาวิเคราะห์เปรียบเทียบกับอนุสัญญาอาชญากรรมไซเบอร์ของยุโรปและกฎหมายไทยดังนี้

รูปแบบฐานความผิดต้นแบบแนวทางที่ 1 (Proposal 1)

ร่างความผิดต้นแบบฐาน “ได้มาซึ่งรหัสผ่านหรือมาตรการป้องกันของบุคคลอื่น” (Illegal obtaining or receiving of passwords) มีองค์ประกอบร่างฐานความผิดว่า ประเทศสมาชิกจะดำเนินการที่จำเป็นเพื่อกำหนดฐานความผิดอาญาตามกฎหมายภายในสำหรับการกระทำ*โดยเจตนาด้วยประการใดๆ ในการได้มาหรือได้รับซึ่งรหัสผ่านหรือมาตรการป้องกันการเข้าถึงใดๆ ของระบบคอมพิวเตอร์ของผู้อื่น*” ร่างมาตรานี้เสนอโดยบราซิลและสิงค์โปร์ [132]

- ร่างต้นแบบฐานความผิดนี้ เมื่อพิจารณาตามแนวคิดรูปแบบเชิงกระบวนการของอาชญากรรมแบบไร้ตัวตนจะพบว่า เป็นการกำหนดความผิดสำหรับขั้นตอนการกระทำเพื่อปกปิดตัวตน โดยองค์ประกอบครอบคลุมการกระทำใดๆ เพื่อได้มาหรือได้รับ (Obtain or receive) ซึ่งรหัสผ่านของผู้อื่น ซึ่งเมื่อได้มาแล้วอาจนำไปใช้ประกอบอาชญากรรมต่อระบบหรือความปลอดภัยทางคอมพิวเตอร์ประเภทใดก็ได้ โดยร่างความผิดต้นแบบมุ่งประสงค์ควบคุมพฤติกรรมนี้โดยกำหนดเป็นฐานความผิดเฉพาะและสามารถเข้าองค์ประกอบเป็นความผิดสำเร็จในตัวเอง แม้ยังไม่ปรากฏว่ามีการใช้รหัสผ่านนั้นเข้าถึงคอมพิวเตอร์หรืออุปกรณ์เพื่อนำไปกระทำความผิดหลักใดก็ตาม

---

[132] Ad Hoc Committee to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, Compilation of Draft provisions submitted by Member States on criminalization, p.15 23 May, 2022

- เมื่อวิเคราะห์เปรียบเทียบกับอนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรปพบว่า ไม่ได้กำหนดฐานความผิดนี้ไว้โดยเฉพาะ แต่มีฐานความผิดการเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นโดยมิชอบ (มาตรา 5) ซึ่งกำหนดความผิดสำหรับการกระทำในการเข้าถึงระบบของผู้อื่น ในแง่หนึ่งพิจารณาได้ว่า มีขอบเขตกว้างสามารถครอบคลุมการเข้าถึงระบบของผู้อื่นไม่ว่าด้วยวิธีใด ๆ จึงรวมการเข้าถึงระบบของผู้อื่นโดยวิธีการใช้รหัสผ่านหรือข้อมูลผู้อื่น แต่ในอีกแง่หนึ่งพิจารณาได้ว่า มาตรา 5 ไม่ได้กำหนดความผิดเฉพาะสำหรับการได้มาซึ่งรหัสผ่านของผู้อื่น โดยเป็นความผิดสำเร็จในตัวเองแม้ว่ายังไม่ได้ใช้รหัสผ่านหรือข้อมูลนั้นเพื่อเข้าถึงระบบใดๆ

- วิเคราะห์เปรียบเทียบกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 5 พบว่า กำหนดความผิดคล้ายคลึงกับมาตรา 5 อนุสัญญาอาชญากรรมไซเบอร์ของยุโรป แต่มีการกำหนด มาตรา 6 ที่มีองค์ประกอบความผิดสำหรับการล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นและนำไปเปิดเผยโดยมิชอบ อย่างไรก็ตาม มาตรา 6 มีข้อจำกัด ในแง่ขององค์ประกอบการกระทำที่จะต้องมีการ “เปิดเผย” ไม่มีองค์ประกอบเกี่ยวกับการ “ได้มาหรือได้รับ” (Obtain or receive) จึงไม่สามารถปรับใช้ครอบคลุมถึงการกระทำเฉพาะการได้มาซึ่งรหัสผ่านของผู้อื่น

รูปแบบฐานความผิดต้นแบบแนวทางที่ 2 (Proposal 2)

ร่างความผิดต้นแบบฐานการปลอมตัวเป็นบุคคลอื่น (Impersonation) มีองค์ประกอบร่างฐานความผิดว่า ประเทศสมาชิกจะดำเนินการที่จำเป็นเพื่อกำหนดฐานความผิดอาญาตามกฎหมายภายในสำหรับการกระทำ *โดยทุจริต กระทำการใดๆ ในการใช้ลายมือชื่ออิเล็กทรอนิกส์ รหัสผ่าน หรือสิ่งบ่งชี้หรือระบุตัวบุคคลใด ๆ ของบุคคลอื่น”* ร่างมาตรานี้เสนอโดยอินเดีย[133]

- ร่างต้นแบบฐานความผิดนี้ เมื่อพิจารณาตามแนวคิดรูปแบบเชิงกระบวนการของอาชญากรรมแบบไร้ตัวตนจะพบว่า เป็นการกำหนดความผิดสำหรับขั้นตอนที่คาบเกี่ยวหรือทับซ้อนระหว่างการกระทำเพื่อปกปิดตัวตน และการกระทำความผิดหลัก สำหรับในส่วนของการกระทำความผิดหลักนั้นหากปรากฏว่ามีส่วนของวิธีการที่อาชญากรใช้ข้อมูลระบุตัวบุคคอื่นในการกระทำก็จะเข้าองค์ประกอบนี้ ซึ่งเป็นฐานความผิดเฉพาะแยกต่างหากจากฐานความผิดหลักอื่น นอกจากนี้ ฐานความผิดดังกล่าวอาจเป็นความผิดสำเร็จในตัวเอง แม้ว่าการกระทำหลักหรือการกระทำอันเป็นเป้าหมายไม่เข้าองค์ประกอบความผิดอาญาเกี่ยวกับอาชญากรรมไซเบอร์ฐานใด

[133] Ad Hoc Committee to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, Compilation of Draft provisions submitted by Member States on criminalization, p.15 23 May, 2022

โดยเฉพาะ เนื่องจากการกระทำครบองค์ประกอบเมื่อใช้ลายมือชื่ออิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ แม้ว่าจะไม่ได้ใช้ในการฉ้อโกงทางคอมพิวเตอร์หรืออาชญากรรมไซเบอร์ฐานอื่นก็ตาม

- ร่างต้นแบบฐานความผิดนี้ เมื่อวิเคราะห์เปรียบเทียบกับอนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรปพบว่า ไม่ได้กำหนดฐานความผิดนี้ไว้โดยเฉพาะ การใช้ลายมือชื่ออิเล็กทรอนิกส์หรือสิ่งบ่งชี้ระบุตัวบุคคลใด ๆ ของบุคคลอื่นจะเข้าข่ายฐานความผิดต้นแบบตามอนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรปเมื่อมีการนำข้อมูลดังกล่าวไปกระทำความผิดหลักซึ่งอาจเป็นฐานความผิดใดต่อระบบหรือข้อมูลคอมพิวเตอร์ เช่น การเข้าถึงโดยมิชอบ จึงไม่มีฐานความผิดสำหรับอาชญากรรมไร้ตัวตนในขั้นตอนการกระทำเพื่อปกปิดตัวตนโดยวิธีการใช้ลายมือชื่ออิเล็กทรอนิกส์ดังเช่นต้นแบบความผิดของสหประชาชาติ

- วิเคราะห์เปรียบเทียบกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 การกระทำในขอบเขตร่างต้นแบบฐานนี้ อาจเข้าข่ายความผิดบางมาตราของพระราชบัญญัตินี้ แต่ขึ้นอยู่กับข้อเท็จจริงเป็นกรณีไป เช่น การฉ้อโกงทางคอมพิวเตอร์โดยการนำข้อมูลเท็จเข้าสู่ระบบหากปรากฏว่ามีการใช้ลายมือชื่ออิเล็กทรอนิกส์ของผู้อื่นก็เป็นการนำข้อมูลปลอมหรือเท็จเข้าสู่ระบบ อย่างไรก็ตาม เนื่องจากพระราชบัญญัตินี้ไม่มีฐานความผิดดังเช่นร่างต้นแบบโดยเฉพาะ จึงทำให้ไม่มีฐานความผิดที่ปรับใช้ได้อย่างครอบคลุมสำหรับอาชญากรรมไร้ตัวตนในขั้นตอนการปกปิดตัวตนและขั้นตอนการกระทำหลักที่มีพฤติกรรมไม่เข้าองค์ประกอบของฐานความผิดที่มีอยู่[134] เช่น อาชญากรใช้ลายเซ็นอิเล็กทรอนิกส์ของบุคคลอื่นโดยไม่ได้รับอนุญาต แต่การกระทำนั้นยังไม่เข้าองค์ประกอบมาตรา 14 (1) เนื่องจากไม่มีลักษณะน่าจะทำให้ประชาชนทั่วไปเสียหาย รวมทั้งพฤติกรรมยังไม่เข้าองค์ประกอบฐานความผิดอื่นในมาตรา 5-10 เป็นต้น

รูปแบบฐานความผิดต้นแบบแนวทางที่ 3 (Proposal 3)

ร่างต้นแบบความผิดฐาน “การเข้าถึงข้อมูลระบุตัวบุคคลอื่นโดยมิชอบ” (Unauthorized access to personal data) มีองค์ประกอบร่างฐานความผิดว่า ประเทศสมาชิกจะดำเนินการที่จำเป็นเพื่อกำหนดฐานความผิดอาญาตามกฎหมายภายในสำหรับการกระทำ <u>การเข้าถึงโดยมิชอบซึ่งข้อมูลระบุตัวของบุคคลอื่น</u>

---

[134] คณาธิป ทองรวีวงศ์ 2566 *การปรับปรุงพัฒนาพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ตามแนวทางองค์การสหประชาชาติ ในกรณีความผิดฐานโจรกรรมข้อมูลส่วนบุคคล* , รายงานสืบเนื่อง การประชุมวิชาการระดับชาติ "การจัดการเทคโนโลยีและนวัตกรรม" (The National Conference on Technology and Innovation Management , NCTIM 2023)

<u>โดยมีเจตนาทำลาย แก้ไข ทำซ้ำ หรือ แลกเปลี่ยน</u>” ร่างมาตรานี้เสนอโดยรัสเซีย เบลารุส จีน นิคารากัว บุรุนดี ทาจิกิสถาน[135]

- ร่างต้นแบบฐานความผิดนี้ เมื่อพิจารณาตามแนวคิดรูปแบบเชิงกระบวนการของอาชญากรรมแบบไร้ตัวตนจะพบว่า เป็นการกำหนดความผิดสำหรับขั้นตอนที่การกระทำเพื่อปกปิดตัวตน ซึ่งอาชญากรเข้าถึงข้อมูลระบุตัวของเหยื่อและอาจทำการแก้ไขหรือแลกเปลี่ยนกับข้อมูลอื่นจากนั้นนำไปใช้สร้างร่องรอยการประกอบอาชญากรรมใดๆ ซึ่งเป็นการกระทำความผิดหลักทั้งนี้เพื่อให้เจ้าหน้าที่บังคับใช้กฎหมายเข้าใจว่าเป็นการกระทำของเหยื่อ ฐานความผิดดังกล่าวอาจเป็นความผิดสำเร็จในตัวเอง แม้ว่าการกระทำหลักหรือการกระทำอันเป็นเป้าหมายไม่เข้าองค์ประกอบความผิดอาญาเกี่ยวกับอาชญากรรมไซเบอร์ฐานใดโดยเฉพาะ เนื่องจากการกระทำครบองค์ประกอบเมื่อมีการเข้าถึงและแก้ไขเปลี่ยนแปลงข้อมูลระบุตัวผู้อื่น แม้ว่าจะไม่ได้ใช้ในการฉ้อโกงทางคอมพิวเตอร์หรืออาชญากรรมไซเบอร์ฐานอื่นก็ตาม

- ร่างต้นแบบฐานความผิดนี้ เมื่อวิเคราะห์เปรียบเทียบกับอนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรป พบว่า ไม่ได้กำหนดฐานความผิดนี้ไว้โดยเฉพาะอย่างไรก็ตาม เมื่ออาชญากรรมนำข้อมูลระบุตัวบุคคลอื่นที่ได้มาจากการเข้าถึงโดยอาจนำมาแก้ไขเปลี่ยนแปลงและนำไปใช้ประกอบการกระทำผิดต่อระบบหรือข้อมูลคอมพิวเตอร์จึงเข้าข่ายต้นแบบฐานความผิดที่อนุสัญญานี้กำหนดไว้ เช่น การเข้าถึงข้อมูลระบุตัวของเหยื่อจากอุปกรณ์คอมพิวเตอร์และแก้ไขรหัสผ่านเพื่อมิให้เหยื่อสามารถใช้อุปกรณ์ จากนั้นอาชญากรควบคุมอุปกรณ์และใช้อุปกรณ์นั้นไปกระทำความผิดต่อระบบหรือข้อมูลเพื่อปกปิดการกระทำของตนและให้เข้าใจว่าเหยื่อเป็นผู้กระทำ จะเห็นได้ว่าฐานความผิดตามอนุสัญญาอาชญากรรมไซเบอร์มีข้อจำกัดเฉพาะการกระทำหลังจากใช้ข้อมูลระบุตัวเหยื่อแล้ว แต่ร่างฐานความผิดของสหประชาชาติสามารถครอบคลุมไปถึงขั้นตอนการกระทำตั้งแต่การได้มาและแก้ไขเปลี่ยนแปลงข้อมูลระบุตัวเหยื่อโดยยังไม่ปรากฏว่านำข้อมูลนั้นไปปกปิดตัวตนเพื่อประกอบอาชญากรรมฐานใด

นอกจากนี้ อนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรปมีฐานความผิดใกล้เคียงคือ ฐานกระทำต่อข้อมูลโดยมิชอบ (Data interference, Article 4) ซึ่งมีองค์ประกอบความผิดต้นแบบว่า “...การกระทำโดยเจตนาทำให้เสียหาย ลบ ทำลาย แก้ไข ข้อมูลคอมพิวเตอร์โดยไม่มีสิทธิ” อย่างไรก็ตามฐานนี้แตกต่างจากร่างต้นแบบของ

---

[135] Ad Hoc Committee to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, Compilation of Draft provisions submitted by Member States on criminalization, p.16 23 May, 2022

สหประชาชาติเนื่องจากเป็นการกระทำต่อข้อมูลทั่วไปไม่ใช่ข้อมูลระบุตัวบุคคล จึงไม่ใช่ฐานความผิดที่มีเจตนารมณ์หรือขอบเขตสำหรับการควบคุมอาชญากรรมไร้ตัวตนตั้งแต่ขั้นตอนการกระทำเพื่อปกปิดตัวตน

- วิเคราะห์เปรียบเทียบกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไม่ได้กำหนดฐานความผิดที่ตรงตามองค์ประกอบของร่างสนธิสัญญาสหประชาชาติว่าด้วยอาชญากรรมเทคโนโลยีอย่างไรก็ตาม การกระทำในขอบเขตร่างต้นแบบฐานนี้ อาจเข้าข่ายความผิดบางมาตราของพระราชบัญญัตินี้ ขึ้นอยู่กับข้อเท็จจริงเป็นกรณีไป เช่น การเข้าถึงและแก้ไขข้อมูลระบุตัวของเหยื่อเป็นการแก้ไขเปลี่ยนแปลงข้อมูลคอมพิวเตอร์โดยมิชอบตามมาตรา 9[136] อย่างไรก็ตาม ฐานความผิดดังกล่าวไม่ได้มีวัตถุประสงค์เพื่อกำหนดความผิดอย่างเป็นกระบวนการตามขั้นตอนของอาชญากรรมไร้ตัวตนเพราะเป็นการกำหนดความผิดสำหรับการแก้ไขเปลี่ยนแปลงข้อมูล คอมพิวเตอร์ทั่วไปเช่นเดียวกับร่างฐานความผิดของอนุสัญญาอาชญากรรมไซเบอร์ของสหภาพยุโรป

สรุป เมื่อพิจารณาจากกรอบสนธิสัญญาระหว่างประเทศที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ปัจจุบันพบว่า สนธิสัญญาและร่างสนธิสัญญาที่สำคัญสองฉบับ ไม่ได้ใช้แนวทางการกำหนดนิยามทั่วไปที่ครอบคลุมอาชญากรรมไร้ตัวตน แต่ใช้วิธีการกำหนดความผิดต้นแบบที่มีองค์ประกอบครอบคลุมพฤติกรรมของอาชญากรรมไร้ตัวตน โดยหัวข้อนี้วิเคราะห์ความผิดต้นแบบสำหรับอาชญากรรมซึ่งใช้วิธีปกปิดตัวตน 3 แนวทางย่อยตามร่างอนุสัญญาของสหประชาชาติ คือ 1. ฐานความผิดเข้าถึงรหัสผ่านของผู้อื่น 2. ฐานความผิดใช้ลายมือชื่ออิเล็กทรอนิกส์ของผู้อื่น และ 3. ฐานความผิดเข้าถึงและแก้ไขข้อมูลระบุตัวของผู้อื่น โดยเมื่อนำองค์ประกอบต้นแบบความผิดทั้ง 3 แนวทางมาวิเคราะห์เปรียบเทียบกับอนุสัญญาอาชญากรรมไซเบอร์ของยุโรปและพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พบว่า ยังไม่มีฐานความผิดเหล่านี้โดยเฉพาะ ซึ่งสรุปการวิเคราะห์เปรียบเทียบองค์ประกอบดังตารางต่อไปนี้

---

[136] คณาธิป ทองรวีวงศ์, 2566, การปรับปรุงพัฒนาพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ตามแนวทางองค์การสหประชาชาติ ในกรณีความผิดฐานโจรกรรมข้อมูลส่วนบุคคล , รายงานสืบเนื่อง การประชุมวิชาการระดับชาติ "การจัดการเทคโนโลยีและนวัตกรรม" (The National Conference on Technology and Innovation Management , NCTIM 2023)

ฐานความผิดเฉพาะสำหรับอาชญากรรมซึ่งใช้วิธีปกปิดตัวตนตามร่างสนสิสัญญาสหประชาชาติ (Draft of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes)	เปรียบเทียบกับต้นแบบความผิดตามอนุสัญญาอาชญากรรมไซเบอร์ สหภาพยุโรป the Council of Europe Convention on Cybercrime (The Budapest Convention)	เปรียบเทียบกับฐานความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
รูปแบบฐานความผิดต้นแบบแนวทางที่ 1 (Proposal 1) “เข้าถึงรหัสผ่านหรือมาตรการป้องกันของบุคคลอื่น”	ไม่ได้กำหนดความผิดฐานนี้โดยเฉพาะ มีฐานที่ใกล้เคียงเช่นการเข้าถึงโดยมิชอบ	ไม่ได้กำหนดความผิดฐานนี้โดยเฉพาะ มีฐานที่ใกล้เคียงตามมาตรา 6 แต่จำกัดเฉพาะการเปิดแผยรหัสผ่าน องค์ประกอบไม่ครอบคลุมการกระทำ “ได้มาหรือได้รับ” (Obtain or receive) รหัสผ่านของผู้อื่น
รูปแบบฐานความผิดต้นแบบแนวทางที่ 2 (Proposal 2) กระทำการใดๆ โดยทุจริต ในการใช้ลายมือชื่ออิเล็กทรอนิกส์ รหัสผ่านหรือสิ่งบ่งชี้หรือระบุตัวบุคคลใดๆ ของบุคคลอื่น	ไม่ได้กำหนดความผิดฐานนี้โดยเฉพาะ	ไม่ได้กำหนดความผิดฐานนี้โดยเฉพาะ
รูปแบบฐานความผิดต้นแบบแนวทางที่ 3 (Proposal 3) การเข้าถึงโดยมิชอบซึ่งข้อมูลระบุตัวของบุคคลอื่น โดยมีเจตนาทำลาย แก้ไข ทำซ้ำ หรือ แลกเปลี่ยน	ไม่ได้กำหนดความผิดฐานนี้โดยเฉพาะ มีความผิดฐานใกล้เคียงคือการแก้ไขข้อมูลคอมพิวเตอร์ตามมาตรา 4	ไม่ได้กำหนดความผิดฐานนี้โดยเฉพาะ มีความผิดฐานใกล้เคียงคือการแก้ไขข้อมูลคอมพิวเตอร์ตามมาตรา 9

3.2 ฐานความผิดเฉพาะสำหรับการฉ้อโกงทางคอมพิวเตอร์

แม้ว่าอาชญากรรมไซเบอร์อาจใช้วิธีการกระทำแบบไร้ตัวตนเพื่อปกปิดการกระทำในการประกอบอาชญากรรมตามฐานความผิดต่างๆ ได้อย่างกว้างขวาง โดยรวมถึงการฉ้อโกงทางคอมพิวเตอร์ (Computer fraud) แต่จากลักษณะพฤติกรรมและวัตถุประสงค์อันเป็นเป้าหมายของอาชญากรรมไร้ตัวตนโดยทั่วไปคือการมุ่งแสวงประโยชน์จากทรัพยากรของผู้อื่นโดยการหลอกลวง รวมทั้งใช้วิธีการปกปิดตัวตนหรือใช้ข้อมูลระบุตัวคนอื่นประกอบการกระทำ ดังนั้น ในการร่างสนธิสัญญาอาชญากรรมไซเบอร์ของสหประชาชาติมี

ข้อเสนอจากบางประเทศให้กำหนดฐานความผิดต้นแบบเฉพาะสำหรับอาชญากรรมไร้ตัวตนในกรณีของการฉ้อโกงทางคอมพิวเตอร์ โดยร่างข้อเสนอต้นแบบความผิดมีดังนี้

“การใช้ข้อมูลดิจิทัลที่ระบุตัวบุคคลอื่นหรือใช้ข้อมูลใด ๆ หลายอย่างประกอบกันที่สามารถบ่งระบุตัวบุคคลอื่น ในการกระทำการให้บุคคลอื่นเข้าใจผิด เพื่อให้ได้มาซึ่งประโยชน์ (Gain)” ร่างต้นแบบนี้เสนอโดยบุรุนดี [137]

- ร่างต้นแบบฐานความผิดนี้ เมื่อวิเคราะห์เปรียบเทียบกับอนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรป พบว่าคล้ายคลึงกับ *หมวดที่ 2 ความผิดเกี่ยวกับคอมพิวเตอร์ (Computer-related offences)* ซึ่งกำหนดฐานความผิดสำหรับการฉ้อโกงหลอกลวงทางคอมพิวเตอร์ (Computer-related fraud, Article 8) และมีองค์ประกอบความผิดต้นแบบว่า “...การกระทำโดยเจตนาและไม่มีสิทธิ ก่อให้เกิดความเสียหายแก่ทรัพย์สินผู้อื่นโดยนำข้อมูลคอมพิวเตอร์เข้าสู่ระบบ แก้ไขลบ หรือทำการแทรกแซงการทำงานของระบบคอมพิวเตอร์ ด้วยเจตนาหลอกลวงหรือไม่สุจริต เพื่อให้ได้มาซึ่งผลประโยชน์ทางเศรษฐกิจสำหรับตนหรือผู้อื่นโดยไม่มีสิทธิ” อย่างไรก็ตามมีความแตกต่างกับร่างต้นแบบของสหประชาชาติ ดังนี้

- การฉ้อโกงทางคอมพิวเตอร์ตามอนุสัญญายุโรป มีองค์ประกอบการกระทำที่ไม่ได้มุ่งเน้นการหลอกลวงบุคคล ทั้งนี้เนื่องจากการฉ้อโกงทางคอมพิวเตอร์ซึ่งจัดอยู่ในกลุ่มอาชญากรรมที่กระทบต่อความมั่นคงปลอดภัยทางคอมพิวเตอร์ ไม่ได้ใช้วิธีการหลอกลวงที่มีเป้าหมายที่ความเข้าใจของมนุษย์ จึงไม่มีองค์ประกอบการทำให้เข้าใจผิด (Mistake) ของบุคคล เพราะการฉ้อโกงที่กระทำต่อระบบจะมุ่งหมายให้ระบบอัตโนมัติตอบสนองไปตามที่อาชญากรต้องการ[138] อย่างไรก็ตาม ความผิดต้นแบบตามร่างของสหประชาชาติมุ่งเน้นที่การปกปิดตัวตน จึงมีองค์ประกอบ “...การใช้ข้อมูลระบุตัวผู้อื่นเพื่อให้เข้าใจผิด” เพื่อปรับใช้กับการฉ้อโกงทางคอมพิวเตอร์โดยมุ่งหลอกลวงมนุษย์ซึ่งจะมีการนำข้อมูลระบุตัวของผู้อื่นเพื่อปกปิดร่องรอยและเพื่อให้เจ้าหน้าที่บังคับใช้กฎหมายเข้าใจว่าเป็นกากระทำของผู้อื่นที่เป็นเหยื่อนั้น

---

[137] Ad Hoc Committee to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, Compilation of Draft provisions submitted by Member States on criminalization, 23 May, 2022, pp33-34

[138] คณาธิป ทองรวีวงศ์ . กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ เล่ม 2 : ภาคการฉ้อโกงทางคอมพิวเตอร์ สแปม และความผิดอื่น, กรุงเทพ:สำนักพิมพ์นิติธรรม. (2564)

- วิเคราะห์เปรียบเทียบกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไม่ได้กำหนดฐานความผิดที่ตรงตามองค์ประกอบของร่างสนธิสัญญาสหประชาชาติว่าด้วยอาชญากรรมเทคโนโลยีโดยมีความผิดเฉพาะฐานฉ้อโกงทางคอมพิวเตอร์ตามมาตรา 14 (1) อย่างไรก็ตามฐานความผิดนี้แตกต่างจากอนุสัญญาอาชญากรรม ไซเบอร์ เนื่องจากกำหนดองค์ประกอบหลักคือ “นำข้อมูลปลอมหรือเท็จหรือบิดเบือนเข้าสู่ระบบ..” และมีองค์ประกอบพฤติการณ์ประกอบการกระทำ “โดยทุจริตหรือโดยหลอกลวง” จึงสะท้อนถึงการควบคุมอาชญากรประเภทฉ้อโกงทางคอมพิวเตอร์ที่ใช้เนื้อหา (Content) หลอกลวงบุคคล อย่างไรก็ตาม เมื่อเปรียบเทียบกับร่างต้นแบบของสหประชาชาติพบว่า มีองค์ประกอบที่สะท้อนถึงการหลอกลวงบุคคลให้เข้าใจผิดเช่นกัน แต่มีข้อแตกต่างคือ มาตรา 14 (1) ไม่ได้กำหนดเฉพาะถึงการหลอกลวงโดยการใช้ข้อมูลระบุตัวบุคคลอื่น กล่าวคือ มาตรานี้มุ่งเน้นความผิดจากเนื้อหา (Content) ที่ทำให้บุคคลเข้าใจผิด เช่น เนื้อหาการลงทุนหรือการทำธุรกิจซึ่งไม่มีอยู่จริง ทั้งนี้ไม่ว่าผู้หลอกลวงจะอาศัยข้อมูลตัวตนของบุคคลอื่นมาประกอบการหลอกลวงหรือไม่ก็ตาม ในขณะที่ร่างต้นแบบของสหประชาชาติมีองค์ประกอบที่ไม่ได้มุ่งเน้นการหลอกลวงให้เข้าใจผิดในเนื้อหา (Content) หรือเรื่องราวการหลอกลวง แต่กำหนดองค์ประกอบความผิดสำหรับการหลอกลวงให้เข้าใจผิดโดยใช้ข้อมูลบุคคลอื่นซึ่งเป็นการปกปิดการกระทำเพื่อให้อาชญากรที่ทำการฉ้อโกงนั้นมีลักษณะไร้ตัวตนนั่นเอง ทั้งนี้ไม่ว่าเนื้อหาจะเป็นการหลอกลวงในเรื่องราวใดก็อยู่ภายใต้ฐานความผิดต้นแบบนี้ เช่น การหลอกลวงให้ลงทุน การหลอกลวงเชิงความสัมพันธ์ การหลอกลวงการทำงานหรือการประกอบธุรกิจออนไลน์ ฯลฯ

สรุป เมื่อพิจารณาจากกรอบสนธิสัญญาระหว่างประเทศที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ปัจจุบันพบว่า สนธิสัญญาและร่างสนธิสัญญาที่สำคัญสองฉบับ ไม่ได้ใช้แนวทางการกำหนดนิยามทั่วไปที่ครอบคลุมอาชญากรรมไร้ตัวตน แต่ใช้วิธีการกำหนดความผิดต้นแบบที่มีองค์ประกอบครอบคลุมพฤติกรรมของอาชญากรรมไร้ตัวตน ซึ่งประกอบด้วยความผิดต้นแบบหลายฐาน โดยหัวข้อนี้วิเคราะห์*ความผิดต้นแบบสำหรับอาชญากรรมไร้ตัวตนในกรณีที่ทำการฉ้อโกงทางคอมพิวเตอร์* โดยพบว่า ร่างอนุสัญญาสหประชาชาติระบุถึงความผิดต้นแบบฐานนี้ไว้ ในขณะที่ผลการเปรียบเทียบกับอนุสัญญาอาชญากรรมไซเบอร์ยุโรปพบว่า ต้นแบบความผิดฐานฉ้อโกงทางคอมพิวเตอร์ไม่ได้มุ่งเน้นการฉ้อโกงที่อาชญากรใช้วิธีปกปิดตัวตนโดยอาศัยข้อมูลระบุตัวเหยื่อ สำหรับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 นั้น มีฐานความผิดฉ้อโกงทางคอมพิวเตอร์ที่แตกต่างจากอนุสัญญาอาชญากรรมไซเบอร์ยุโรป เนื่องจากมุ่งเน้นที่เนื้อหาการหลอกลวงอันเป็นเท็จ (Content) แต่ไม่ได้ระบุองค์ประกอบสำหรับการฉ้อโกงโดยวิธีนำข้อมูลระบุตัวบุคคลอื่นมาปกปิดร่องรอยหรือการกระทำของอาชญากร ซึ่งสรุปการวิเคราะห์เปรียบเทียบองค์ประกอบดังตารางต่อไปนี้

ฐานความผิดเฉพาะสำหรับอาชญากรรมซึ่งใช้วิธีปกปิดตัวตนตามร่างสนสิสัญญาสหประชาชาติ	เปรียบเทียบกับต้นแบบความผิดตามอนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรป	เปรียบเทียบกับฐานความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
มีฐานความผิดเฉพาะสำหรับอาชญากรรมไร้ตัวตนในกรณีของการฉ้อโกงทางคอมพิวเตอร์ ที่อาชญากรนำข้อมูลดิจิทัลที่ระบุตัวบุคคลอื่นมาให้บุคคลอื่นเข้าใจผิดหรือปกปิดตัวตน	มีฐานความผิดเฉพาะสำหรับฉ้อโกงทางคอมพิวเตอร์ แต่มีข้อจำกัดคือ - องค์ประกอบมุ่งเน้นที่การหลอกลวงการทำงานของระบบ - ไม่มีองค์ประกอบที่เจาะจงสำหรับการใช้ข้อมูลบุคคลอื่นมาปกปิดการกระทำการหลอกลวง	มีฐานความผิดเฉพาะสำหรับฉ้อโกงทางคอมพิวเตอร์ แต่มีข้อจำกัดคือ - องค์ประกอบมุ่งเน้นเนื้อหาการหลอกลวง (content) มิได้กำหนดองค์ประกอบเจาะจงถึงการใช้ข้อมูลระบุตัวผู้อื่นมาประกอบการหลอกลวงเพื่อปกปิดตัวตนของอาชญากร

จากการวิเคราะห์ประเด็นที่ 2 พบว่า

- ตามแนวทางของต่างประเทศและกฎหมายระหว่างประเทศ ไม่ได้ใช้วิธีการกำหนดนิยามสากลหรือความหมายกลางของอาชญากรรมไร้ตัวตน เพราะการกระทำดังกล่าวมีลักษณะเชิงกระบวนการหลายขั้นตอน อีกทั้งอาจเกี่ยวข้องกับอาชญากรรมไซเบอร์ชนิดใดก็ได้ เนื่องจากอาจนำวิธีการปกปิดตัวตนมาประกอบหรือปกปิดการกระทำได้ แนวทางที่เหมาะสมของการพัฒนากฎหมายต้นแบบคือ การกำหนดฐานความผิดที่มีองค์ประกอบครอบคลุมการกระทำของอาชญากรรมไร้ตัวตน ซึ่งความผิดเกี่ยวกับคอมพิวเตอร์ตามกฎหมายภายในเดิมของประเทศต่างๆ อาจยังไม่ครอบคลุม

- ในการกำหนดความผิดต้นแบบ (Model offence) สำหรับอาชญากรรมไร้ตัวตนตามแนวทางระหว่างประเทศพบว่ามีข้อเสนอและร่างฐานความผิดหลายแนวทาง โดยแต่ละแนวทางมีลักษณะร่วมกันที่สำคัญคือ มุ่งเน้นการกำหนดความผิดสำหรับพฤติกรรมการปกปิดตัวตน ทั้งนี้เพราะการกระทำความผิดหลักของอาชญากรรมไร้ตัวตนมักอยู่ภายใต้องค์ประกอบฐานความผิดตามกฎหมายเกี่ยวกับความผิดคอมพิวเตอร์ของประเทศต่าง ๆ แล้ว

- ในการนำความผิดต้นแบบ (Model offence) สำหรับอาชญากรรมไร้ตัวตนมาประยุกต์ใช้พัฒนาและปรับปรุงฐานความผิดในประเทศไทยนั้น จากการศึกษาแนวทางระหว่างประเทศ ประกอบกับการวิเคราะห์จำแนกขั้นตอนกระบวนการของอาชญากรรมไร้ตัวตนพบว่า กฎหมายที่เกี่ยวข้องของไทยสามารถครอบคลุมการกระทำหลักของอาชญากรรมไร้ตัวตนซึ่งอาจเข้าข่ายความผิดต่าง ๆ เช่น การเข้าถึงข้อมูลหรือระบบ การส่งมัลแวร์ การทำลายข้อมูล แต่ยังมีปัญหาขอบเขตฐานความผิดสำหรับการกระทำในส่วนปกปิดตัวตนที่ไม่ได้มี

องค์ประกอบเฉพาะเจาะจงสำหรับอาชญากรรมประเภทนี้ ดังนั้น ตัวแบบฐานความผิดแนวทางต่างๆ ที่ศึกษาในหัวข้อนี้จึงสามารถนำมาเป็นข้อเสนอแนะปรับปรุงพัฒนาฐานความผิดดังกล่าวของไทยได้ต่อไป

4. มาตรการความร่วมมือระหว่างประเทศที่จำเป็นต่อการป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตนที่กระทำโดยองค์กรอาชญากรรมข้ามชาติในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์

อาชญากรรมไร้ตัวตนมีลักษณะและผลกระทบที่ไม่จำกัดพรมแดน อีกทั้งในการประกอบอาชญากรรมกรณีใดกรณีหนึ่ง อาจส่งผลเกี่ยวเนื่องกับหลายประเทศ ผู้ต้องสงสัยและผู้ได้รับผลกระทบ รวมทั้งพยานหลักฐานและข้อมูลที่เกี่ยวข้องอาจกระจายอยู่ในเขตแดนหลายประเทศเช่นกัน ดังนั้น ความร่วมมือระหว่างสองประเทศหรือทวิภาคีในการป้องกันปราบปรามอาชญากรรมประเภทนี้จึงยังไม่เพียงพอและยากที่จะตอบสนองต่อลักษณะการสืบสวนสอบสวนอาชญากรรมลักษณะนี้ เป็นเหตุให้ความร่วมมือที่สำคัญจะอยู่ในกรอบกฎหมายระหว่างประเทศ ในการวิเคราะห์หัวข้อนี้จึงเริ่มจากมาตรการความร่วมมือในระดับระหว่างประเทศที่เกี่ยวข้องโดยตรงกับอาชญากรรมไร้ตัวตนและอาชญากรรมไซเบอร์ตามกรอบของสหประชาชาติและสหภาพยุโรป จากนั้นจะวิเคราะห์เปรียบเทียบกับความร่วมมือในทางอาญาระหว่างประเทศ (MLAT) ซึ่งไม่ได้มีหลักการเฉพาะสำหรับอาชญากรรมไซเบอร์และอาชญากรรมไร้ตัวตน สำหรับประเทศไทยไม่ได้เข้าร่วมเป็นภาคีในกรอบกฎหมายระหว่างประเทศที่เกี่ยวข้องกับอาชญากรรมไร้ตัวตนและอาชญากรรมไซเบอร์ทั้งในส่วนของยุโรปและสหประชาชาติ จึงจะศึกษาเปรียบเทียบหลักการร่วมมือระดับระหว่างประเทศในทางอาญของอาเซียนซึ่งประเทศไทยมีพันธกรณี จากนั้นจะชี้ให้เห็นตัวอย่างความร่วมมือระหว่างประเทศตามแนวทางกฎหมายต่างประเทศ เช่น กฎหมายสหรัฐอเมริกา เป็นต้น

4.1 รูปแบบความร่วมมือระหว่างประเทศในการป้องกันและปราบปรามอาชญากรรมไร้ตัวตน

จากการศึกษาพบว่ากรอบความตกลงระหว่างประเทศที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ในปัจจุบันมีสองฉบับคือ

1. อนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรป หรืออนุสัญญาบูดาเปสท์ (the Council of Europe Convention on Cybercrime or The Budapest Convention)

2. ร่างสนธิสัญญาสหประชาชาติว่าด้วยอาชญากรรมเทคโนโลยี (Draft of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes) โดยในเดือนธันวาคม 2019 ที่ประชุมสมัชชาใหญ่ได้รับรองมติว่าด้วย “การต่อต้านการ

ใช้เทคโนโลยีสารสนเทศเพื่อประกอบอาชญากรรม” และจัดตั้งคณะทำงานเฉพาะกิจ (Ad Hoc Committee) เพื่อดำเนินการเกี่ยวกับการจัดทำกรอบความร่วมมือและร่างสนธิสัญญาระดับระหว่างประเทศต่อไป ซึ่งกำหนดแผนดำเนินการในระยะ 3 ปี การประชุมครั้งแรกได้เริ่มขึ้นในเดือนมีนาคม 2022[139] โดยร่างสนธิสัญญานี้ประกอบด้วยหลายหมวด สำหรับหมวดที่เกี่ยวกับต้นแบบฐานความผิด (Model offence) ได้นำมาวิเคราะห์แยกเป็นประเด็นต่างหากแล้ว สำหรับในหัวข้อนี้จะกล่าวถึงร่างสนธิสัญญาในหมวด 4 ว่าด้วย “ความร่วมมือระหว่างประเทศ” (International cooperation)

แม้ว่าร่างกฎหมายและกฎหมายระหว่างประเทศทั้งสองฉบับ จะไม่ได้ระบุถึงความร่วมมือในกรณีอาชญากรรมไร้ตัวตนโดยเฉพาะ แต่เนื่องจากอาชญากรรมไร้ตัวตนที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์มีลักษณะเป็นรูปแบบพฤติกรรมเชิงกระบวนการหลายขั้นตอนและเกี่ยวข้องกับความผิดหลายฐานดังได้วิเคราะห์มาแล้ว ซึ่งความผิดเหล่านั้นจัดอยู่ในขอบเขตของอาชญากรรมไซเบอร์หรืออาชญากรรมเทคโนโลยีตามกฎหมายระหว่างประเทศดังกล่าว ด้วยเหตุนี้ กรอบแนวทางด้านความร่วมมือตามระหว่างประเทศทั้งสองฉบับ จึงมีขอบเขตครอบคลุมอาชญากรรมไร้ตัวตนด้วย โดยในการวิเคราะห์ในหัวข้อนี้จะไม่แยกศึกษาแต่ละความตกลง แต่ใช้วิธีจำแนกประเด็นทางกฎหมายและตามลักษณะของแต่ละมาตรการของความร่วมมือ โดยในส่วนของแต่ละมาตรการจะนำตัวแบบหลักการของความร่วมมือทั้งสองฉบับมาวิเคราะห์เปรียบเทียบ ดังนี้

4.1.1 หลักการเกี่ยวกับพันธกรณีทั่วไปของความร่วมมือป้องกันปราบปรามอาชญากรรมแบบไร้ตัวตนระหว่างประเทศ

ร่างมาตรา 56 ของสนธิสัญญาสหประชาชาติว่าด้วยอาชญากรรมเทคโนโลยีกำหนดหลักการเกี่ยวกับความร่วมมือระหว่างประเทศทั่วไปในการป้องกันและปราบปรามอาชญากรรมเทคโนโลยี (General principles of international cooperation) มีหลักการสำคัญว่า

ประเทศสมาชิกจะดำเนินการให้ความร่วมมือระหว่างกันในขอบเขตสูงสุดที่เป็นไปได้ (fullest extent possible) ภายใต้กรอบสนสิสัญญานี้ตลอดจนกฎหมายระหว่างประเทศอื่น รวมทั้งหลักต่างตอบแทน ในการดำเนินมาตรการป้องกันปราบปรามอาชญากรรรมอิเล็กทรอนิกส์ ในเรื่องของการป้องกัน สืบสวนสอบสวน การบังคับใช้กฎหมาย การรวบรวม แลกเปลี่ยน พยานหลักฐาน การดำเนินคดีกับอาชญากรรม...”

---

[139] United Nations, A UN treaty on cybercrime en route, https://unric.org/en/a-un-treaty-on-cybercrime-en-route/ , 4/05/2022.

อนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรป กำหนดหลักการทั่วไปเกี่ยวกับความร่วมมือระหว่างประเทศ ในมาตรา 23 ที่มีหลักการว่า

“ประเทศสมาชิกจะดำเนินการด้านความร่วมมือในขอบเขตสูงสุดที่เป็นไปได้ (Fullest extent possible) ภายใต้สนธิสัญญานี้และกฎหมายระหว่างประเทศที่เกี่ยวข้อง รวมทั้งหลักการต่างตอบแทน เพื่อดำเนินมาตรการต่างๆ รวมทั้งลดอุปสรรคของความร่วมมือ โดยเฉพาะในการแลกเปลี่ยนข้อมูลและหลักฐานระหว่างประเทศอย่างราบรื่นและรวดเร็ว (Smooth and rapid flow of information and evidence)”

ข้อวิเคราะห์

จากร่างของสหประชาชาติและอนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรป พบว่าร่างมาตรา 56 และมาตรา 23 มีหลักการที่คล้ายคลึงกันในการกำหนดพันธกรณีให้ประทศสมาชิกต้องจัดให้มีมาตรการร่วมมือด้านต่างๆ ในการป้องกันและปราบปรามอาชญากรรมอิเล็กทรอนิกส์ โดยหลักการทั้งสองฉบับกำหนดให้มีพันธกรณีทั่วไปอย่างกว้าง ๆ ซึ่งจะมีการกำหนดพันธกรณีย่อยเป็นรายละเอียดมาตรการแต่ละด้านที่จะวิเคราะห์ต่อไป

ในแง่ของข้อจำกัด ร่างมาตรา 56 และ มาตรา 23 มีขอบเขตจำกัดสองด้านคือ

<u>ด้านขอบเขตอาชญากรรมที่จะดำเนินมาตรการร่วมมือ</u> มีข้อจำกัดเฉพาะการดำเนินมาตรการร่วมมือที่เกี่ยวข้องกับอาชญากรรมอิเล็กทรอนิกส์ ตามฐานความผิดที่กำหนดในร่างสนธิสัญญาและอนุสัญญาฯ อย่างไรก็ตาม ในส่วนของร่างสนธิสัญญาสหประชาชาติยังไม่เป็นที่สุด โดยมีความเห็นจากผู้แทนประเทศที่เข้าร่วมการร่างเป็นสองฝ่าย ฝ่ายหนึ่งเห็นว่า อาชญากรรมในขอบเขตความร่วมมือจำกัดเฉพาะฐานความผิดที่ระบุในสนธิสัญญานี้ แต่อีกฝ่ายเห็นว่ามาตรการความร่วมมือนี้ควรเป็นไปอย่างกว้างเพื่อป้องกันและปราบปรามอาชญากรรมไซเบอร์ใด ๆ แม้ว่าไม่ระบุในสนธิสัญญานี้ ในแง่สิทธิมนุษยชน ความร่วมมือตามสนธิสัญญานี้ประกอบด้วยมาตรการอันหลากหลาย ซึ่งบางมาตรการกระทบต่อสิทธิมนุษยชน เช่น การเข้าถึงข้อมูลคอมพิวเตอร์ดังจะกล่าวต่อไป ดังนั้น การขยายขอบเขตความร่วมมือไปครอบคลุมอาชญากรรมที่ไม่ระบุเจาะจงอาจทำให้ประเทศสมาชิกบางแห่งใช้มาตรการนี้โดยมิชอบ (Abuse) ซึ่งอาจส่งผลต่อการสื่อสารของสื่อมวลชน ข้อมูลส่วนบุคคลของผู้ใช้บริการ การสื่อสารที่เป็นความผิดอื่นนอกเหนือจากความผิดต่อความมั่นคงของระบบหรือข้อมูลคอมพิวเตอร์[140] ซึ่งประเด็นด้านขอบเขตตามร่างสนธิสัญญานี้แตกต่างจากอนุสัญญาไซเบอร์สหภาพยุโรปซึ่ง

[140] คณาธิป ทองรวีวงศ์, การคุ้มครองสิทธิมนุษยชนจากมาตรการความร่วมมือระหว่างประเทศเพื่อการป้องกันแปราบปรามอาชญากรรมไซเบอร์ : ศึกษากรณีมาตรการเข้าถึงข้อมูลส่วนบุคคลในกรอบการเจราจาสนธิสัญญาของสหประชาชาติ, รายงานสืบเนื่อง การประชุมหาดใหญ่วิชาการระดับชาติ และนานาชาติ ครั้งที่ 14 มหาวิทยาลัยหาดใหญ่

จำกัดเฉพาะฐานความผิดที่ระบุในอนุสัญญาเท่านั้น อย่างไรก็ตาม ในส่วนอาชญากรรมแบบไร้ตัวตนนั้น แม้ว่าความตกลงระหว่างประเทศทั้งสองฉบับจะไม่ได้กำหนดฐานความผิดโดยเรียกชื่อดังกล่าวไว้เฉพาะ แต่ก็มีฐานความผิดหลายฐานที่เกี่ยวข้องดังได้วิเคราะห์มาแล้ว เช่น การโจรกรรมข้อมูล การเข้าถึงโดยมิชอบ จึงกล่าวได้ว่า กรอบความร่วมมือระหว่างประเทศทั้งสองฉบับสามารถมีขอบเขตครอบคลุมอาชญากรรมไร้ตัวตนที่กระทำต่อระบบหรือข้อมูลได้

<u>ด้านข้อจำกัดของความตกลงในการร่วมมือระหว่างประเทศ</u> แม้หลักความร่วมมือทั่วไปแสดงถึงพันธกรณีในการร่วมมือหลายด้าน แต่ความร่วมมือต้องอยู่ภายใต้กฎหมายระหว่างประเทศอื่นรวมทั้งประเทศสมาชิกอาจดำเนินมาตรการร่วมมือตามหลักต่างตอบแทน (Reciprocity) โดยประเทศสมาชิกอาจทำความตกลงทวิภาคีระหว่างกันในการดำเนินความร่วมมือแต่ละด้าน ซึ่งจะเกิดขึ้นต่อเมื่อทั้งสองฝ่ายดำเนินการต่างตอบแทนในเรื่องนั้น เช่น การส่งผู้ร้ายข้ามแดน

4.1.2 หลักการเกี่ยวกับความร่วมมือในการส่งผู้ร้ายข้ามแดน (Extradition)

ร่างมาตรา 58 ของสนธิสัญญาสหประชาชาติว่าด้วยอาชญากรรมเทคโนโลยีกำหนดหลักการความร่วมมือในการส่งผู้ร้ายข้ามแดน (Extradition) มีหลักการสำคัญว่า

ประเทศสมาชิกจะดำเนินการให้ความผิดที่ระบุในสนธิสัญญานี้เป็นความผิดที่ส่งผู้ร้ายข้ามแดนได้ภายใต้กฎหมายภายในประเทศของตนและจะดำเนินการร่วมมือในการส่งผู้กระทำความผิดแก่ประเทศสมาชิกที่ร้องขอ ในกรณีที่ความผิดนั้นเป็นความผิดตามกฎหมายภายในที่มีโทษทางอาญาขั้นต่ำไม่น้อยกว่าหนึ่งปีทั้งของประเทศที่ร้องขอและประเทศที่บุคคลนั้นอยู่ในดินแดน

ในกรณีที่ความผิดที่ร้องขอให้ส่งผู้ร้ายข้ามแดนมีอัตราโทษขั้นต่ำแตกต่างกัน ความร่วมมือย่อมอยู่ภายใต้การเจรจาหรือสนธิสัญญาระหว่างกัน รวมทั้งหลักต่างตอบแทนของประเทศสมาชิก

อนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรป มาตรา 24 มีหลักการว่า

ความผิดที่ระบุในอนุสัญญานี้ เป็นความผิดที่ประเทศสมาชิกมีพันธกรณีในการส่งผู้ร้ายข้ามแดน ทั้งนี้ความผิดดังกล่าวต้องมีโทษอาญาขั้นต่ำอย่างน้อยหนึ่งปี

ในกรณีที่ความผิดที่ร้องขอให้ส่งผู้ร้ายข้ามแดนมีอัตราโทษขั้นต่ำแตกต่างกัน ความร่วมมือในการส่งผู้ร้ายข้ามแดนจะอยู่ภายใต้อนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรปว่าด้วยการส่งผู้ร้ายข้ามแดน (European convention on extradition) รวมทั้งเป็นไปตามหลักต่างตอบแทนของประเทศที่ร้องขอและที่รับคำร้องขอ ทั้งนี้

ประเทศสมาชิกมีพันธกรณีในการนำเอาฐานความผิดที่ระบุในอนุสัญญานี้ไปกำหนดเป็นความผิดที่ส่งผู้ร้ายข้ามแดนตามสนธิสัญญาทวิภาคีระหว่างกัน

ข้อวิเคราะห์

จากร่างของสหประชาชาติและอนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรปพบว่า ร่างมาตรา 58 และ มาตรา 24 มีหลักการที่คล้ายคลึงกันในการกำหนดพันธกรณีให้ประทศสมาชิกต้องดำเนินการส่งผู้ร้ายข้ามแดน โดยมีข้อจำกัดที่คล้ายคลึงกันคือ

1. อาชญากรรมทางอิเล็กทรอนิกส์ที่อยู่ภายใต้ขอบเขตการส่งผู้ร้ายข้ามแดน ต้องเป็นฐานความผิดที่ระบุในร่างสนธิสัญญา/ อนุสัญญาฯ

2. ความผิดที่ส่งผู้ร้ายข้ามแดนต้องมีโทษอาญาตามกฎหมายภายในของทั้งสองประเทศอย่างน้อยจำคุก 1 ปี

อย่างไรก็ตาม การส่งผู้ร้ายข้ามแดนที่มีอัตราโทษแตกต่างกันตามกฎหมายภายในอาจทำได้ตามหลักต่างตอบแทนและความตกลงระหว่างประเทศแบบทวิภาคีของผู้ร้องขอและผู้รับคำร้องขอ อย่างไรก็ตาม เนื่องจากประเทศสมาชิกสหภาพยุโรปมีความผูกพันตามสนธิสัญญาว่าด้วยการส่งผู้ร้ายข้ามแดน ความร่วมมือด้านนี้จึงขึ้นอยู่กับหลักการของสนธิสัญญาดังกล่าวด้วย อย่างไรก็ตาม หลักความร่วมมือทั้งสองฉบับมีความคล้ายคลึงกันในแง่ที่เปิดโอกาสให้ประเทศที่ร้องขอและรับการร้องขอ ใช้หลักต่างตอบแทนในความร่วมมือด้านนี้

4.1.3 หลักการเกี่ยวกับความร่วมมือในการส่งตัวนักโทษ (Transfer of sentenced persons)

ร่างมาตรา 59 ของสนธิสัญญาสหประชาชาติวางหลักว่า ประเทศสมาชิกอาจพิจารณาทำความตกลงระหว่างกันในรูปแบบสนธิสัญญาทวิภาคีหรือพหุภาคี เกี่ยวกับการโอนตัวหรือส่งตัวนักโทษในความผิดที่ระบุในสนธิสัญญานี้ระหว่างกัน

อนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรปไม่ได้กำหนดความร่วมมือในด้านการโอนตัวหรือส่งตัวนักโทษในความผิดอาชญากรรมไซเบอร์ไปรับโทษในประเทศสมาชิกอื่น

4.1.4 หลักการพื้นฐานของมาตรการสนับสนุนร่วมกัน (General principles and procedures relating to mutual legal assistance)

ร่างมาตรา 61 ของสนธิสัญญาสหประชาชาติวางหลักว่า

ประเทศสมาชิกตกลงจะดำเนินมาตรการสนับสนุนร่วมกัน (Mutual assistance) เพื่อป้องกันปราบปรามอาชญากรรมอิเล็กทรอนิกส์ ในด้านต่างๆ เช่น

การรวบรวมพยานหลักฐาน หรือเอกสารจากบุคคลที่เกี่ยวข้อง

การดำเนินการค้น ยึด อายัดทรัพย์สิน

การค้น การเข้าถึง ข้อมูลคอมพิวเตอร์ที่จัดเก็บอยู่ในระบบคอมพิวเตอร์ซึ่งตั้งอยู่ในเขตแดนประเทศสมาชิก

การเก็บรวบรวมข้อมูลจราจรคอมพิวเตอร์แบบตามเวลาจริง (Real time traffic data)

การเก็บรวบรวมหรือการบันทึกข้อมูลเนื้อหาการสื่อสาร (Content data) ที่ส่งผ่านระบบคอมพิวเตอร์

การตรวจสอบ วิเคราะห์ พยานหลักฐานทางอิเล็กทรอนิกส์ เว็บไซต์

การดำเนินการร่วมมือ แลกเปลี่ยนข้อมูลและการวิเคราะห์หรือประเมินของผู้เชี่ยวชาญ

การติดตามด้านทรัพย์สิน หรือเครื่องมือของอาชญากรรม

การกู้คืนซึ่งข้อมูลคอมพิวเตอร์

ความร่วมมือเรื่องอื่นใดที่เกี่ยวข้องกับอาชญากรรมที่ระบุในสนธิสัญญานี้

ความร่วมมือดังกล่าวข้างต้น มีเงื่อนไขและรายละเอียดตามบทมาตราที่เกี่ยวข้องของสนธิสัญญานี้

อนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรป มาตรา 25 มีหลักการว่า

ประเทศสมาชิกมีพันธกรณีในการดำเนินมาตรการสนับสนุนร่วมกัน (Mutual assistance) เพื่อวัตถุประสงค์ในการสืบสวนสอบสวน บังคับใช้กฎหมาย สำหรับความผิดที่ระบุในอนุสัญญานี้ที่เกี่ยวข้องกับระบบหรือข้อมูลคอมพิวเตอร์ รวมทั้งการเก็บรวบรวมพยานหลักฐานอิเล็กทรอนิกส์สำหรับการบังคับใช้กฎหมายกับผู้กระทำผิด

ประเทศสมาชิกจะดำเนินการเพื่อให้กฎหมายภายในประเทศของตนมีหลักการที่สอดคล้องและสนับสนุนกับการดำเนินมาตรการสนับสนุนร่วมกันดังที่ระบุในมาตรา 27-35

ข้อวิเคราะห์

จากร่างของสหประชาชาติและอนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรปพบว่า ร่างมาตรา 61 และมาตรา 25 มีหลักการพื้นฐานที่คล้ายคลึงกันในการกำหนดพันธกรณีให้ประทศสมาชิกจัดให้มีมาตรการสนับสนุนร่วมกัน (Mutual assistance) ในการป้องกันและปราบปรามอาชญากรรมอิเล็กทรอนิกส์ โดยจะมีการกำหนดหลักการเกี่ยวกับมาตรการย่อยหรือมาตรการเฉพาะด้านที่จะวิเคราะห์ต่อไป ทั้งนี้ อนุสัญญาอาชญากรรม

ไซเบอร์สหภาพยุโรประบุเจาะจงว่ามาตรการย่อยหรือมาตรการเฉพาะด้านมุ่งเน้นถึงการดำเนินการเพื่อรวบรวมหรือได้มาซึ่งพยานหลักฐานเกี่ยวกับการประกอบอาชญากรรมเปรียบเทียบกับร่างของสหประชาชาติกำหนดหลักพื้นฐานที่มีขอบเขตกว้าง แต่เมื่อพิจารณาจากหัวข้อของมาตรการย่อยจะเห็นได้ว่ายังคงเป็นความร่วมมือที่เกี่ยวกับการสืบสวนสอบสวนและรวบรวมพยานหลักฐานนั่นเอง อย่างไรก็ตาม หลักความร่วมมือนี้เป็นกรอบพื้นฐานหรือหัวข้อความร่วมมือ ซึ่งจะมีการกำหนดรายละเอียดของมาตรการความร่วมมือแต่ละด้าน ดังจะแยกวิเคราะห์ต่อไป

4.1.5 ความร่วมมือในการสืบสวนสอบสวนโดยใช้เทคโนโลยีการประชุมทางไกล (Conducting interrogations using video or telephone conferencing systems)

ร่างมาตรา 62 ของสนธิสัญญาสหประชาชาติกำหนดหลักการเกี่ยวกับความร่วมมือในการสืบสวนสอบสวนโดยใช้เทคโนโลยีการประชุมทางไกล มีหลักสำคัญว่า

ประเทศสมาชิกจะให้ความร่วมมือโดยทำความตกลงระหว่างกันในการให้ความช่วยเหลือหรือสนับสนุนการสืบสวนสอบสวนความผิดตามสนธิสัญญานี้โดยใช้เทคโนโลยีการประชุมทางไกล เช่น การใช้ระบบการประชุมทางอิเล็กทรอนิกส์ ในกรณีที่มีการสืบสวน สอบถาม บุคคลที่เกี่ยวข้อง รวมถึงพยานและผู้เชี่ยวชาญที่อยู่ในเขตแดนของประเทศสมาชิกด้วยกัน

เปรียบเทียบกับอนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรป ไม่ได้กำหนดหลักความร่วมมือในประเด็นนี้

4.1.6 ความร่วมมือในการจัดให้มีฐานข้อมูลกลาง (Electronic database on mutual legal assistance requests)

ร่างมาตรา 63 ของสนธิสัญญาสหประชาชาติว่าด้วยอาชญากรรมเทคโนโลยีมีหลักสำคัญว่า

ประเทศสมาชิกจะพิจารณาดำเนินการให้มีการแลกเปลี่ยนและเก็บรักษาฐานข้อมูลอิเล็กทรอนิกส์ที่เกี่ยวข้องกับสถิติในการขอความร่วมมือในเรื่องต่างๆ ตามสนธิสัญญานี้ เพื่อวัตถุประสงค์ในการศึกษา ปรับปรุง ทบทวนความมีประสิทธิภาพของมาตรการความร่วมมือระหว่างกัน

ข้อวิเคราะห์

เปรียบเทียบกับอนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรป ไม่ได้กำหนดหลักความร่วมมือในประเด็นนี้ อย่างไรก็ตามความร่วมมือในการจัดให้มีและรักษาไว้ซึ่งฐานข้อมูลกลางตามแนวทางสหประชาชาติ มิใช่ฐานข้อมูลเกี่ยวกับอาชญากรรมไซเบอร์ แต่เป็นฐานข้อมูลเก็บรวบรวมสถิติ การดำเนินการด้านความร่วมมือ เช่น

จำนวนการร้องขอระหว่างประเทศสมาชิก เพื่อวัตถุประสงค์ในการวิจัยพัฒนาการปรับปรุงการดำเนินการด้านความร่วมมือระหว่างกัน มิใช่เพื่อศึกษาวิจัยการกระทำของอาชญากรและไม่เกี่ยวข้องกับฐานข้อมูลรายละเอียดผู้เสียหาย

4.1.7 ความร่วมมือในการขอให้เก็บรักษาข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับการกระทำผิด (Mutual legal assistance in the expedited preservation of stored computer data)

ร่างมาตรา 68 ของสนธิสัญญาสหประชาชาติว่าด้วยอาชญากรรมเทคโนโลยีมีหลักว่า

ประเทศสมาชิกอาจร้องขอให้ประเทศสมาชิกดำเนินการออกคำสั่งหรือดำเนินการตามกฎหมายภายในของประเทศผู้รับคำร้อง เพื่อให้มีการเก็บรักษาไว้ซึ่งข้อมูลคอมพิวเตอร์ในระบบหรืออุปกรณ์ที่ตั้งอยู่ในเขตอำนาจของประเทศผู้รับคำร้องขอ

คำร้องตามมาตรานี้ ต้องระบุฐานความผิดอันเป็นเหตุแห่งการร้องขอ ระบุความเชื่อมโยงของข้อมูลคอมพิวเตอร์ที่ร้องขอกับฐานความผิดอันเป็นเหตุแห่งการร้องขอ

อนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรป มาตรา 29 มีหลักการว่า

ประเทศสมาชิกอาจร้องขอให้ประเทศสมาชิกมีคำสั่งหรือดำเนินการใดๆ เพื่อให้เกิดการเก็บรักษาไว้ซึ่งข้อมูลคอมพิวเตอร์ที่อยู่ในระบบหรืออุปกรณ์ของประเทศผู้รับคำขอ โดยคำขอดังกล่าวอย่างน้อยควรระบุ ความผิดอันเป็นเหตุแห่งการร้องขอ รายละเอียดของข้อมูลที่ร้องขอให้เก็บรักษา ความจำเป็นหรือความเร่งด่วนของการร้องขอ

ข้อวิเคราะห์

ร่างมาตรา 68 และมาตรา 29 ต่างมีหลักการความร่วมมือตามมาตรการนี้เช่นเดียวกัน ทั้งนี้ความร่วมมือตามมาตรการนี้ ยังไม่ใช่การขอให้ส่งหรือเปิดเผยข้อมูล แต่เป็นขั้นตอนการขอให้เก็บรักษา (Preservation) ในทางวิชาการอาจเรียกขั้นตอนนี้ว่า มาตรการชั่วคราวในการสืบสวนสอบสวนอาชญากรรมคอมพิวเตอร์ (Provisional measures)[141] เนื่องจากการร้องขอให้ประเทศอื่นดำเนินการเก็บรักษาคือการระงับไว้ซึ่งการแก้ไขเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ที่สามารถใช้เป็นหลักฐานการดำเนินคดีอาชญากรรมอิเล็กทรอนิกส์ เพราะมิฉะนั้นอาจเกิดการแก้ไขเปลี่ยนแปลงพยานหลักฐาน โดยยังไม่มีความร่วมมือในลักษณะของการส่งหรือ

[141] Chat Le Nguyen, Wilfred Golman. Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries, Computer Law & Security Review, Volume 40, 2021.

เปิดเผยข้อมูลนั้น อย่างไรก็ตาม ความร่วมมือตามมาตรการนี้อาจเป็นขั้นตอนแรกของกระบวนการขอความร่วมมือ เพราะประเทศผู้ร้องขออาจมีการขอความร่วมมือในขั้นตอนไป โดยการขอให้ส่งหรือโอนข้อมูลคอมพิวเตอร์

การร่วมมือตามมาตรการนี้ อาจไม่สามารถดำเนินการโดยรัฐซึ่งเป็นคู่ภาคีสนธิสัญญา เพราะข้อมูลคอมพิวเตอร์อาจอยู่ในความครอบครองของผู้ให้บริการ (Service provider) ซึ่งเป็นภาคเอกชนของประเทศนั้น ด้วยเหตุนี้ ร่างมาตรา 68 และมาตรา 29 ของอนุสัญญาฯ จึงกำหนดถ้อยคำ “ขอให้ประเทศสมาชิก “มีคำสั่ง” (Oder) หมายถึง ประเทศสมาชิกขอให้ประเทศสมาชิกผู้รับคำขอให้ความร่วมมือโดยออกคำสั่งไปยังเอกชนผู้ให้บริการในประเทศผู้รับคำขอ ซึ่งอาจต้องขอให้ศาลเป็นผู้ออกคำสั่ง ทั้งนี้จะขึ้นอยู่กับกฎหมายภายในของประเทศผู้รับคำขอ แต่หลักการตามความตกลงระหว่างประเทศนี้ จะส่งผลให้รัฐสมาชิกต้องดำเนินการให้กฎหมายภายในสอดคล้องกับพันธกรณีระหว่างประเทศเรื่องความร่วมมือ ซึ่งอาจทำให้ประเทศสมาชิกต้องแก้ไขกฎหมายเพื่อให้สามารถสั่งผู้ให้บริการในเรื่องดังกล่าวได้

4.1.8 ความร่วมมือในการเข้าถึงข้อมูลคอมพิวเตอร์ที่เก็บรักษาไว้ (Mutual legal assistance in accessing stored computer data)

ร่างมาตรา 70 ของสนธิสัญญาสหประชาชาติว่าด้วยอาชญากรรมเทคโนโลยีมีหลักว่า

ประเทศสมาชิกอาจร้องขอให้ประเทศสมาชิก ทำการค้น (Search) หรือเข้าถึง (Access) หรือยึด (Seize) หรือการกระทำอื่นในลักษณะเดียวกัน และเปิดเผย (Disclose) ข้อมูลคอมพิวเตอร์ที่เก็บไว้ในระบบหรืออุปกรณ์คอมพิวเตอร์ในเขตอำนาจประเทศสมาชิกนั้น การดำเนินการนี้รวมถึงการกระทำต่อข้อมูลคอมพิวเตอร์ที่มีคำขอให้ดำเนินการร่วมมือในการเก็บรักษาไว้ตามมาตรา 68

คำขอตามมาตรานี้ อย่างน้อยต้องระบุเหตุอันควรเชื่อว่าข้อมูลนั้นเกี่ยวข้องกับการกระทำผิดอันเป็นเหตุแห่งการร้องขอ เหตุอันควรเชื่อว่าข้อมูลนั้นมีความเสี่ยงต่อการถูกทำลายหรือแก้ไข

มาตรา 31 อนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรป มีหลักว่า

ประเทศสมาชิกอาจร้องขอให้ประเทศสมาชิก ทำการค้น (Search) หรือ เข้าถึง (Access) หรือยึด (Seize) หรือการกระทำอื่นในลักษณะเดียวกัน และ เปิดเผย (Disclose) ข้อมูลคอมพิวเตอร์ที่เก็บไว้ในระบบหรืออุปกรณ์คอมพิวเตอร์ในเขตอำนาจประเทศสมาชิกนั้น การดำเนินการนี้รวมถึงการกระทำต่อข้อมูลคอมพิวเตอร์ที่มีคำขอให้ดำเนินการร่วมมือในการเก็บรักษาไว้ตามมาตรา 29

คำขอตามมาตรานี้ อย่างน้อยต้องระบุเหตุอันควรเชื่อว่าข้อมูลนั้นเกี่ยวข้องกับการกระทำผิดอันเป็นเหตุแห่งการร้องขอ เหตุอันควรเชื่อว่าข้อมูลนั้นมีความเสี่ยงต่อการถูกทำลายหรือแก้ไข

ข้อวิเคราะห์

ร่างมาตรา 70 และมาตรา 31 ต่างมีหลักการความร่วมมือในด้านการเข้าถึงข้อมูลเช่นเดียวกัน โดยเป็นความร่วมมือขั้นตอนต่อเนื่องจากความร่วมมือในการขอเก็บรักษา (Preservation) ดังที่กล่าวมาแล้ว อย่างไรก็ตาม ความตกลงระหว่างประเทศทั้งสองฉบับไม่ได้กำหนดให้มาตรการขอให้เก็บรักษาและมาตรการเข้าถึงข้อมูลต้องเป็นเงื่อนไขก่อนหรือหลังซึ่งกันและกัน กล่าวคือ ประเทศสมาชิกอาจขอความร่วมมือให้เก็บรักษาโดยไม่มีการขอให้เข้าถึง หรืออาจขอให้เข้าถึงโดยไม่ต้องขอให้เก็บรักษาก็ได้ หรืออาจยื่นคำขอความร่วมมือทั้งสองมาตรการพร้อมกันก็ได้

4.1.9 ความร่วมมือในการร้อขอให้เปิดเผยข้อมูลการจราจรคอมพิวเตอร์ (Mutual legal assistance in the disclosure of traffic data)

ร่างมาตรา 69 ของสนธิสัญญาสหประชาชาติว่าด้วยอาชญากรรมเทคโนโลยีมีหลักว่า

ในกรณีที่ประเทศสมาชิกมีคำขอให้ประเทศสมาชิกเก็บรักษาข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับการสืบสวนสอบสวนความผิดตามสนธิสัญญานี้และประเทศสมาชิกผู้รับคำขอเห็นว่า ข้อมูลคอมพิวเตอร์ตามคำขอมีความเกี่ยวข้องกับผู้ให้บริการที่ตั้งอยู่ในประเทศสมาชิกอื่น ประเทศสมาชิกผู้รับคำขอจะทำการเปิดเผยข้อมูลจราจรคอมพิวเตอร์ ให้แก่ประเทศผู้ร้องขอ เพื่อบ่งระบุรายละเอียดของผู้ให้บริการที่เกี่ยวข้องกับการสื่อสารข้อมูลนั้น อย่างไรก็ตาม ประเทศสมาชิกที่รับคำขอมีสิทธิปฏิเสธหากพิจารณาแล้วเห็นว่าความผิดที่เกี่ยวข้องกับการร้องขอข้อมูลนั้นเป็นความผิดทางการเมือง หรือการดำเนินการตามคำขอจะกระทบต่อความมั่นคงหรือประโยชน์สาธารณะของประเทศผู้รับคำขอ

อนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรป มาตรา 30 มีหลักการว่า

ในกรณีที่ประเทศสมาชิกมีคำขอให้ประเทศสมาชิกเก็บรักษาข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับการสืบสวนสอบสวนความผิดตามสนธิสัญญานี้และประเทศสมาชิกผู้รับคำขอเห็นว่า ข้อมูลคอมพิวเตอร์ตามคำขอมีความเกี่ยวข้องกับผู้ให้บริการที่ตั้งอยู่ในประเทศสมาชิกอื่น ประเทศสมาชิกผู้รับคำขอจะทำการเปิดเผยข้อมูลจราจรคอมพิวเตอร์ ให้แก่ประเทศผู้ร้องขอ แต่ประเทศสมาชิกที่รับคำขออาจปฏิเสธความร่วมมือนี้ หากพิจารณาแล้วเห็นว่าความผิดที่เกี่ยวข้องกับการร้องขอข้อมูลนั้นเป็นความผิดทางการเมือง หรือการดำเนินการตามคำขอจะกระทบต่อความมั่นคงหรือประโยชน์สาธารณะของประเทศผู้รับคำขอ

ข้อวิเคราะห์

ร่างมาตรา 69 และ มาตรา 30 มีหลักการเช่นเดียวกัน โดยเป็นความร่วมมือที่อาจเชื่อมโยงและเกี่ยวข้องกับความร่วมมือในการขอเก็บรักษา (Preservation) หรือความร่วมมือในการเข้าถึงข้อมูล (Access) ที่กล่าวมาข้างต้น ทั้งนี้เนื่องจากข้อมูลที่ขอให้เก็บรักษาหรือขอเข้าถึง อาจอยู่ในที่ตั้งหรือเซิร์ฟเวอร์ในประเทศสมาชิกอื่นนอกเหนือจากประเทศผู้ขอและประเทศผู้รับคำขอ นอกจากนี้ ยังอาจเกี่ยวข้องกับผู้ให้บริการ (Service provider) ที่ตั้งอยู่ในประเทศสมาชิกมากกว่าหนึ่งประเทศ ดังนั้น ความร่วมมือด้านนี้คือ เป็นการให้สิทธิประเทศผู้รับคำร้องขอ ดำเนินการเปิดเผยข้อมูลจราจรคอมพิวเตอร์ที่สามารถบ่งชี้รายละเอียดของข้อมูลที่ร้องขอ รวมถึงการให้ข้อมูลจราจรคอมพิวเตอร์ที่สามารถบ่งชี้ผู้ให้บริการที่เก็บรักษาหรือทราบร่องรอยการสื่อสารข้อมูลนั้น ซึ่งอาจเป็นผู้ให้บริการหลายรายและตั้งอยู่ในหลายประเทศ จะเห็นได้ว่า ความร่วมมือข้อนี้ไม่ได้เป็นการขอให้เปิดเผยหรือเข้าถึงเนื้อหาข้อมูลโดยตรง แต่เป็นการส่งข้อมูลการจราจรคอมพิวเตอร์ที่แสดงถึงร่อยรอยข้อมูลและนำไปสู่การบ่งทราบผู้ให้บริการข้อมูลนั้น ซึ่งประเทศผู้ร้องขออาจต้องดำเนินการอื่นต่อไป เช่น การขอความร่วมมือจากประเทศที่สามซึ่งพบว่า ผู้ให้บริการนั้นมีสำนักงานหรือที่ทำการตั้งอยู่ เพื่อให้ประเทศที่สามเข้าถึงหรือสั่งให้เก็บรักษาข้อมูลอีกขั้นตอนหนึ่ง ความร่วมมือด้านนี้มีความสำคัญสำหรับอาชญากรรมไร้ตัวตนที่ไม่มีข้อจำกัดด้านพรมแดนและอาจมีร่องรอยที่เกี่ยวข้องกับระบบของผู้ให้บริการในหลายประเทศ

การขอความร่วมมือในด้านนี้ ส่งผลกระทบต่อผู้ประกอบการเอกชน และยังส่งผลต่อสิทธิของผู้ใช้บริการด้วย ร่างสนธิสัญญาและอนุสัญญาฯ จึงกำหนดข้อยกเว้นประโยชน์สาธารณะ ความมั่นคง และกรณีความผิดทางการเมือง ซึ่งเป็นการให้ดุลพินิจของประเทศผู้รับคำขอ ที่แม้จะให้สัตยาบันหรือมีความผูกพันตามสนธิสัญญาในการให้ความร่วมมือข้อนี้ แต่ยังคงสามารถมีเหตุปฏิเสธโดยไม่ถือว่าเป็นการกระทำที่ฝ่าฝืนพันธกรณีดังกล่าว

สำหรับในส่วนของความผิดทางการเมืองนั้น เป็นเรื่องสำคัญที่อนุสัญญาอาชญากรรมไซเบอร์ยุโรปเน้นย้ำถึงการคุ้มครองสิทธิมนุษยชน และกำหนดเป็นข้อยกเว้นไว้เช่นเดียวกับร่างของสหประชาชาติ แม้ว่าการขอความร่วมมือจะเกี่ยวโยงกับฐานความผิดที่ระบุในอนุสัญญา ซึ่งทั้งสหภาพยุโรปและสหประชาชาติไม่ได้กำหนดความผิดเกี่ยวกับเนื้อหาอยู่แล้ว แต่ในทางปฏิบัติประเทศสมาชิกอาจขอความร่วมมือเข้าถึงข้อมูลหรือขอให้เปิดเผยรายละเอียดผู้ให้บริการ โดยอ้างว่าเพื่อสืบสวนสอบสวนความผิดต่อระบบหรือข้อมูลซึ่งอยู่ในฐานความผิดตามอนุสัญญา ทั้งที่ความจริงเป็นการสืบสวนสอบสวนความผิดทางการเมือง กรณีเช่นนี้ อนุสัญญาและร่างสนธิสัญญาให้สิทธิประเทศสมาชิกที่รับคำขอใช้ดุลพินิจปฏิเสธคำขอได้โดยไม่ถือว่าฝ่าฝืนพันธกรณีระหว่างประเทศในด้านความร่วมมือนี้

4.1.10 การเข้าถึงหรือได้มาซึ่งข้อมูลคอมพิวเตอร์ที่จัดเก็บในประเทศสมาชิกอื่น (Cross-border access to stored computer data)

ร่างมาตรา 72 ของสนธิสัญญาสหประชาชาติว่าด้วยอาชญากรรมเทคโนโลยีมีหลักว่า ประเทศสมาชิกมีสิทธิ

- เข้าถึงข้อมูลคอมพิวเตอร์ที่เก็บไว้ในระบบคอมพิวเตอร์ใด ๆ ซึ่งเปิดเผยหรือเข้าถึงได้โดยสาธารณะ โดยไม่ต้องดำเนินการร้องขอต่อประเทศสมาชิกอื่น

- เข้าถึงข้อมูลคอมพิวเตอร์ผ่านระบบการสื่อสารใด ๆ ที่จัดเก็บไว้อุปกรณ์ที่ตั้งอยู่ในประเทศสมาชิกอื่น ซึ่งจะทำได้ต่อเมื่อได้รับความยินยอมจากผู้มีสิทธิตามกฎหมายของระบบคอมพิวเตอร์นั้น

ส่วนอนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรป ไม่ได้กำหนดหลักความร่วมมือในด้านนี้

ข้อวิเคราะห์

(1) การป้องกันปราบปรามอาชญากรรมไร้ตัวตนจำเป็นต้องมีการสืบสวนสอบสวนพยานหลักฐาน แต่อาจมีปัญหาเนื่องจากข้อมูลเก็บไว้ในฐานข้อมูลในประเทศอื่น นำไปสู่กรอบความตกลงในการให้สิทธิประเทศสมาชิกที่ทำการสืบสวนสอบสวน ดำเนินการเข้าถึงข้อมูลที่เก็บไว้ในประเทศอื่น ซึ่งแยกเป็นสองกรณีคือ

กรณีที่หนึ่ง การเข้าถึงข้อมูลที่ปรากฏทั่วไปจากการสืบค้นทางอินเทอร์เน็ต แต่โดยเทคนิคแล้วข้อมูลเหล่านั้นอาจจัดเก็บในเซิร์ฟเวอร์หรืออุปกรณ์ที่ตั้งอยู่ในขอบเขตประเทศสมาชิกอื่น ดังนั้น ร่างสนธิสัญญาสหประชาชาติจึงกำหนดให้เกิดความชัดเจนว่า หากเป็นการสืบค้นหรือได้มาซึ่งข้อมูลจากแหล่งสาธารณะ (Open data) ก็สามารถเข้าถึงหรือสืบค้นได้โดยไม่ต้องขออนุญาตจากประเทศสมาชิกอื่นแม้ปรากฏว่าข้อมูลนั้นมีการจัดเก็บในระบบหรืออุปกรณ์ที่ตั้งอยู่ในประเทศสมาชิกใดก็ตาม

กรณีที่สอง การเข้าถึงข้อมูลที่เก็บไว้ในระบบหรืออุปกรณ์ที่ตั้งอยู่ในประเทศสมาชิกอื่น โดยอุปกรณ์ดังกล่าวอาจเป็นของภาคเอกชน ในกรณีนี้ ร่างสนธิสัญญาสหประชาชาติว่าด้วยอาชญากรรมเทคโนโลยีกำหนดให้ต้องมีการขอความยินยอมจากผู้มีสิทธิตามกฎหมาย ซึ่งอาจเป็นผู้ให้บริการหรือผู้ประกอบการในประเทศนั้น อย่างไรก็ตาม ประเทศที่ต้องการเข้าถึงข้อมูลอาจขอความร่วมมือจากประเทศปลายทางผ่านศูนย์ประสานงานที่เปิดตลอดเวลา เพื่อให้ประสานงานการขอความยินยอมจากผู้มีสิทธิ

(2) จากการที่หลักความร่วมมือนี้เป็นการให้สิทธิประเทศผู้ร้องเข้าถึงข้อมูลเพื่อการสืบสวนสอบสวนโดยข้อมูลนั้นอยู่ในประเทศสมาชิกอื่น อันอาจเป็นการดำเนินการเข้าถึงโดยตรง หรือการติดต่อเพื่อขอ

เข้าถึงจากผู้ให้บริการที่อยู่ในอีกประเทศหนึ่ง ส่งผลกระทบต่อสิทธิมนุษยชนในหลายแง่มุม[142] เช่น การให้ประเทศสมาชิกหนึ่งทำการติดต่อกับผู้ให้บริการในอีกประเทศเพื่อขอเข้าถึงข้อมูลการกระทำที่เป็นความผิดในประเทศผู้ร้องขอแต่อาจไม่เป็นความผิดประเทศที่ผู้ให้บริการนั้นตั้งอยู่ หากเปรียบเทียบกับอนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรปพบว่าไม่ได้กำหนดหลักการนี้ ด้วยเหตุผลที่วิเคราะห์ได้หลายประการ เช่น ประเทศกลุ่มสหภาพยุโรปมีความผูกพันตามสนธิสัญญาสิทธิมนุษยชนยุโรปที่เน้นความสำคัญของสิทธิพื้นฐาน (Fundamental right) โดยมีกฎหมายระดับสหภาพยุโรปที่เกี่ยวข้องกับการคุ้มครองสิทธิหลายฉบับ นอกจากกฎหมายคุ้มครองข้อมูลส่วนบุคคล (GDPR) แล้วยังมีกฎหมายสหภาพยุโรปว่าด้วยการคุ้มครองบุคคลธรรมดาจากการประมวลผลข้อมูลส่วนบุคคลโดยเจ้าหน้าที่บังคับใช้กฎหมาย (Directive (EU) 2016/680) แม้ว่ากฎหมายดังกล่าวมีข้อยกเว้นเกี่ยวกับการเข้าถึงข้อมูลเพื่อบังคับใช้กฎหมาย แต่ก็มีข้อจำกัดหลายประการ เช่น ความผิดอันเป็นเหตุแห่งการเข้าถึงข้อมูลต้องเป็นความผิดร้ายแรง (Serious crime) ซึ่งแตกต่างกันไปในหลายประเทศ รวมทั้งมาตรการบังคับใช้กฎหมายด้วยการเข้าถึงข้อมูลต้องมีมาตรการปกป้องสิทธิ (Safeguard) อีกทั้งต้องชั่งน้ำหนักความจำเป็นตามหลักความได้สัดส่วน อย่างไรก็ตาม เมื่อพิจารณาร่างของสหประชาชาติพบว่า แม้มีข้อจำกัดในการเข้าถึงข้อมูลในกรณีที่เก็บรักษาไว้ในระบบของผู้มีสิทธิโดยจะต้องขอความยินยอมก่อน แต่การเปิดโอกาสให้หน่วยงานบังคับใช้กฎหมายของประเทศอื่น อาศัยกลไกความร่วมมือตามสนธิสัญญาเพื่อเข้าถึงข้อมูลในประเทศอื่น รวมทั้งการติดต่อกับผู้ให้บริการในประเทศปลายทางโดยตรง นับว่าเป็นประเด็นที่มีความเสี่ยงต่อสิทธิเสรีภาพต่อประชาชนในประเทศปลายทางที่อาจมีกฎหมายกำหนดความผิดแตกต่างกับประเทศที่ดำเนินการเข้าถึงข้อมูล หากเปรียบเทียบกับการเข้าถึงข้อมูลตามกลไกความร่วมมือตามร่างมาตราอื่นและกลไกความร่วมมือในกรอบสหภาพยุโรปจะพบว่าไม่ได้ให้ประเทศผู้ร้องขอทำการเข้าถึงโดยตรงข้ามพรมแดน (Cross border access) แต่เป็นการขอให้ประเทศปลายทางดำเนินการเข้าถึงและส่งข้อมูลให้อีกทอดหนึ่ง มาตรการนี้จึงอาจพิจารณาว่าไม่สอดคล้องกับหลักความได้สัดส่วน เมื่อเปรียบเทียบกับอนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรปพบว่า ไม่ได้กำหนดหลักความร่วมมือนี้

(3) ในแง่ของประสิทธิภาพของความร่วมมือ ในทางวิชาการมีประเด็นว่า เนื่องจากสภาพปัจจุบันมีประเด็นว่าข้อมูลต่างๆ ที่อาจเกี่ยวข้องและใช้เป็นหลักฐานของการกระทำผิดโดยอาชญากรรมไซเบอร์ อาจไม่ได้

[142] คณาธิป ทองรวีวงศ์, การคุ้มครองสิทธิมนุษยชนจากมาตรการความร่วมมือระหว่างประเทศเพื่อการป้องกันแปราบปรามอาชญากรรมไซเบอร์ : ศึกษากรณีมาตรการเข้าถึงข้อมูลส่วนบุคคลในกรอบการเจราจาสนธิสัญญาของสหประชาชาติ, รายงานสืบเนื่อง การประชุมหาดใหญ่วิชาการระดับชาติ และนานาชาติ ครั้งที่ 14 มหาวิทยาลัยหาดใหญ่

จัดเก็บในเซิร์ฟเวอร์ที่ตั้งอยู่ในประเทศใดประเทศหนึ่ง แต่จัดเก็บไว้ในระบบคลาวด์ (Cloud storage) [143] ซึ่งความร่วมมือตามหลักการดังกล่าวไม่ได้ระบุชัดเจนถึงการเข้าถึงข้อมูลที่เก็บไว้ในระบบคลาวด์ แต่อาจปรับใช้จากหลักการข้างต้น กล่าวคือพิจารณาว่าข้อมูลในระบบคลาวด์นั้นมีลักษณะเข้าถึงได้โดยสาธารณะหรือไม่ หากเป็นข้อมูลที่เปิดเผยต่อสาธารณะอยู่แล้วก็สามารถเข้าถึงได้แม้จะเก็บไว้ในระบบคลาวด์หรือระบบอื่นใดก็ตาม

4.1.11 ความช่วยเหลือร่วมกันในการเก็บรวบรวมข้อมูลจราจรคอมพิวเตอร์แบบเรียลไทม์ (Mutual legal assistance in the real-time collection of traffic)

ร่างมาตรา 73 ของสนธิสัญญาสหประชาชาติว่าด้วยอาชญากรรมเทคโนโลยีมีหลักว่า

ประเทศสมาชิกจะให้ความร่วมมือในการเก็บรวบรวมข้อมูลจราจรคอมพิวเตอร์แบบเรียลไทม์ที่เกี่ยวข้องกับการสื่อสารที่ระบุเจาะจง ซึ่งส่งข้อมูลการสื่อสารผ่านเขตแดนประเทศสมาชิก ทั้งนี้ ภายใต้ข้อจำกัดและเงื่อนไขของกฎหมายภายใน ประเทศสมาชิกจะให้ความร่วมมือตามมาตรานี้เมื่ออาชญากรรมที่เป็นเหตุแห่งการสืบสวนสอบสวนนั้นเป็นความผิดตามกฎหมายภายในของประเทศที่รับการร้องขอ

ในการยื่นคำขอประเทศผู้ร้องขอความร่วมมืออย่างน้อยต้องระบุและให้รายละเอียด สรุปข้อเท็จจริงและอาชญากรรมอันเป็นเหตุให้ร้องขอ ระบุข้อมูลคอมพิวเตอร์และการสื่อสารที่เจาะจงสำหรับข้อมูลการจราจรคอมพิวเตอร์ ความจำเป็นและความเชื่อมโยงระหว่างข้อมูลจราจรคอมพิวเตอร์กับความผิดอันเป็นเหตุให้ร้องขอ ช่วงระยะเวลาในการเก็บรวบรวมข้อมูลจราจรคอมพิวเตอร์

ส่วนอนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรป มาตรา 33 กำหนดว่า

ประเทศสมาชิกจะดำเนินการร่วมมือในการช่วยเหลือระหว่างกันเพื่อให้ประเทศสมาชิกได้มาซึ่งข้อมูลจราจรคอมพิวเตอร์เพื่อการสืบสวนสอบสวนอาชญากรรมทางคอมพิวเตอร์ที่ระบุในอนุสัญญานี้ อย่างไรก็ตาม ความร่วมมือระหว่างกันในมาตรานี้จำกัดเฉพาะการสืบสวนสอบสวนการกระทำที่เป็นความผิดตามกฎหมายภายในของประเทศผู้ขอและผู้รับคำขอ

ข้อวิเคราะห์

ร่างมาตรา 73 คล้ายคลึงกับร่างมาตรา 69 ของสหประชาชาติ และมาตรา 30 ของอนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรป ในแง่ที่เกี่ยวข้องกับการร่วมมือด้านข้อมูลจราจรคอมพิวเตอร์ (Traffic data)

[143] Mulligan, S. P. (2018). Cross-border data sharing under the CLOUD Act. Washington: Congressional Research Service.

แต่ข้อแตกต่างคือร่างมาตรา 69 และ มาตรา 30 เป็นการขอข้อมูลจราจรคอมพิวเตอร์เพื่อบ่งระบุผู้ให้บริการที่เกี่ยวข้องกับการสื่อสารนั้น ซึ่งเมื่อผู้รับคำขอได้ข้อมูลแล้วก็ยังต้องดำเนินการติดต่อกับผู้ให้บริการต่อไป หากประสงค์จะเข้าถึงหรือได้ข้อมูลเกี่ยวกับการสื่อสารนั้น และไม่ใช่การเข้าถึงข้อมูลจราจรคอมพิวเตอร์ตามเวลาจริงหรือเรียลไทม์ แต่ร่างมาตรา 73 ของสหประชาชาติและมาตรา 33 ของสหภาพยุโรปกำหนดความร่วมมือในการขอเก็บรวบรวมข้อมูลการจราจรคอมพิวเตอร์แบบเรียลไทม์ที่เกี่ยวข้องกับการสื่อสารที่สงสัยหรือที่เกี่ยวข้องกับอาชญากรรม โดยตัวแบบความร่วมมือทั้งสองฉบับมีข้อจำกัดสองประการคือ

ประการที่หนึ่ง อาชญากรรมที่เป็นเหตุแห่งการสืบสวนสอบสวนนั้นเป็นความผิดตามกฎหมายภายในของทั้งสองประเทศ กล่าวคือประเทศที่มีคำขอและประเทศที่รับการร้องขอ สำหรับอาชญากรรมไร้ตัวตนที่เกี่ยวข้องกับระบบหรือข้อมูลคอมพิวเตอร์ อยู่ในขอบเขตความผิดตามกรอบระหว่างประเทศทั้งสองฉบับ

ประการที่สอง การร้องขอข้อมูลจราจรคอมพิวเตอร์ มีขอบเขตที่เกี่ยวข้องกับการสื่อสารข้อมูลเจาะจง มิใช่เป็นการดักรับหรือเก็บรวบรวมข้อมูลการสื่อสารของบุคคลใดบุคคลหนึ่งทั้งหมดหรือทุกเรื่อง

นอกจากนี้มีข้อพิจารณาว่า ร่างของสหประชาชาติกำหนดรายละเอียดที่ประเทศผู้ร้องขอต้องระบุในคำขอ เช่น ระบุข้อมูลคอมพิวเตอร์และการสื่อสารที่เจาะจงสำหรับข้อมูลการจราจรคอมพิวเตอร์ ความจำเป็นและความเชื่อมโยงระหว่างข้อมูลจราจรคอมพิวเตอร์กับความผิดอันเป็นเหตุให้ร้องขอ ช่วงระยะเวลาในการเก็บรวบรวมข้อมูลจราจรคอมพิวเตอร์ แต่อนุสัญญายุโรปมาตรา 33 ไม่ได้ระบุรายละเอียดคำขอ แต่ทั้งนี้ขึ้นอยู่กับประเทศสมาชิกที่จะกำหนดรายละเอียดได้

4.1.12 ความช่วยเหลือร่วมกันในการดักรับข้อมูลเนื้อหาการสื่อสารทางคอมพิวเตอร์ (Mutual legal assistance in the interception of content data)

ร่างมาตรา 74 ของสนธิสัญญาสหประชาชาติว่าด้วยอาชญากรรมเทคโนโลยีมีหลักว่า

ประเทศสมาชิกจะดำเนินการช่วยเหลือร่วมกันในการเก็บรวบรวมและบันทึกข้อมูลการสื่อสารทางคอมพิวเตอร์จากการสื่อสารโดยเจาะจงที่ส่งผ่านระบบคอมพิวเตอร์ ภายใต้เงื่อนไขและข้อจำกัดของกฎหมายภายในประเทศ

อนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรป มาตรา 34 กำหนดว่า

ประเทศสมาชิกจะดำเนินมาตรการร่วมมือสนับสนุนระหว่างกันในการเก็บรวบรวมและบันทึกข้อมูลเนื้อหาการสื่อสารที่ระบุเจาะจง ซึ่งส่งผ่านระบบคอมพิวเตอร์ ทั้งนี้ภายใต้ขอบเขตอนุสัญญา สนธิสัญญาอื่นที่เกี่ยวข้อง และกฎหมายภายในของประเทศผู้ร้องขอและผู้รับคำขอ

ข้อวิเคราะห์

ร่างมาตรา 77 และมาตรา 34 ของอนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรป มีหลักการคล้ายคลึงกันในแง่ที่เกี่ยวข้องกับการร่วมมือด้านการเข้าถึงเนื้อหาข้อมูลการสื่อสาร (Content data) โดยมีลักษณะเป็นการดักรับ (Interception) จึงส่งผลกระทบต่อสิทธิมนุษยชน แต่ในอีกแง่หนึ่งอาจพิจารณาได้ว่า หลักความร่วมมือนี้มีการวางข้อจำกัดเพื่อความสมดุลระหว่างสิทธิมนุษยชนกับการสืบสวนสอบสวน กล่าวคือ การเก็บรวบรวมข้อมูลการสื่อสารมีขอบเขตเนื้อหาที่เจาะจง ไม่ครอบคลุมถึงเนื้อหาการสื่อสารทั้งหมดหรือในเรื่องอื่นของบุคคลที่ไม่เกี่ยวข้องกับเรื่องอาชญากรรมที่สืบสวน อย่างไรก็ตาม อนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรปมีข้อจำกัดมากกว่าเนื่องจากระบุว่าการร่วมมือจะขึ้นอยู่กับข้อจำกัดตามสนธิสัญญาอื่นโดยเฉพาะอย่างยิ่งสนธิสัญญาสิทธิมนุษยชนยุโรป แต่ในขณะที่ร่างของสหประชาชาติกำหนดเงื่อนไขให้ขึ้นอยู่กับกฎหมายภายในประเทศที่รับคำร้องขอ

4.1.13 การจัดตั้งศูนย์ประสานงานความร่วมมือที่ทำการตลอด 24 ชั่วโมง

ร่างมาตรา 67 ของสนธิสัญญาสหประชาชาติว่าด้วยอาชญากรรมเทคโนโลยีมีหลักว่า

ประเทศสมาชิกจะดำเนินการจัดให้มีศูนย์ประสานงานความร่วมมือตามสนธิสัญญานี้ โดยสามารถทำการได้ 27 ชั่วโมงต่อวัน และตลอด 7 วันต่อสัปดาห์ ศูนย์ดังกล่าวจะทำการรับคำร้องขอต่างๆ ตามพันธกรณีในสนธิสัญญานี้ รวมถึงการดำเนินการตามคำร้อง เช่น การเก็บรักษาข้อมูล การรวบรวมพยานหลักฐาน

อนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรป มาตรา 35 มีหลักการว่า

ประเทศสมาชิกจะดำเนินการจัดให้มีศูนย์ประสานงานความร่วมมือตามสนธิสัญญานี้ โดยสามารถทำการได้ 27 ชั่วโมงต่อวันและตลอด 7 วันต่อสัปดาห์ เพื่อดำเนินการเกี่ยวกับความร่วมมือ เช่น การรับคำร้องขอต่างๆ การดำเนินการตามคำร้อง เช่น การเก็บรักษาข้อมูล การรวบรวมพยานหลักฐาน

ข้อวิเคราะห์

ร่างมาตรา 67 และมาตรา 35 มีหลักการเช่นเดียวกัน แนวคิดการจัดตั้งศูนย์ประสานงานความร่วมมือระหว่างประเทศที่สามารถทำงานตลอดเวลา 24 ชั่วโมง และทุกวันตลอดสัปดาห์ (24/7 point of contact) นั้นเป็นต้นแบบที่เกิดจากการประชุม G8 ซึ่งมีการจัดตั้งคณะทำงานเฉพาะกลุ่มย่อยเกี่ยวกับอาชญากรรมเทคโนโลยี (High tech crime sub group) ซึ่งเริ่มจัดทำเครือข่ายนี้ ตั้งแต่ ปี ค.ศ. 1997[144] ต้นแบบความร่วมมือ

[144] Kierkegaard, S. M. (2007). EU tackles cybercrime. In Cyber warfare and cyber terrorism , IGI Global. pp. 431-438.

ลักษณะดังกล่าวปรากฏในอนุสัญญาอาชญากรรมไซเบอร์ยุโรป และต่อมาปรากฏในร่างสนธิสัญญาสหประชาชาติด้วย การจัดตั้งศูนย์ดังกล่าวมีความสำคัญเนื่องจาก (1) อาชญากรรมไร้ตัวตนที่กระทำทางไซเบอร์ สามารถเกิดขึ้นได้ตลอดเวลา ศูนย์ประสานงานที่เปิดเฉพาะเวลาทำการจึงไม่สามารถตอบสนองการแก้ปัญหาได้ (2) อาชญากรรมไซเบอร์เกิดขึ้นโดยไม่จำกัดเขตแดนและส่งผลในหลายประเทศที่เขตเวลาต่างกัน ในการจัดตั้งศูนย์ประสานงานความร่วมมือจึงต้องสามารถตอบสนองต่อลักษณะความแตกต่างด้านเวลาได้ ด้วยเหตุนี้ แนวคิดการจัดตั้งศูนย์ประสานงานที่ทำงาน 24 ชั่วโมง จึงมีความสำคัญและปรากฏในความตกลงระหว่างประเทศทั้งสองฉบับ

สรุป การวิเคราะห์ในหัวข้อนี้แสดงให้เห็นถึงกรอบแนวทางระหว่างประเทศเกี่ยวกับการดำเนินมาตรการความร่วมมือด้านต่าง ๆ ในการป้องกันปราบปรามอาชญากรรมไซเบอร์หรืออาชญากรรมเทคโนโลยี ซึ่งครอบคลุมถึงอาชญากรรมที่ใช้วิธีการปกปิดตัวตนในการกระทำผิดด้วย สำหรับประเทศไทยไม่ได้เป็นภาคีสมาชิกอนุสัญญาอาชญากรรมไซเบอร์ยุโรป สำหรับการร่างสนธิสัญญาของสหประชาชาติก็ไม่ปรากฏว่ามีผู้แทนอยู่ในส่วนของคณะทำงานเฉพาะกิจและไม่ปรากฏข้อเสนอหรือความเห็นในการร่างดังกล่าว อย่างไรก็ตาม แม้กรอบกฎหมายระหว่างประเทศทั้งสองฉบับไม่มีผลผูกพันตามกฎหมายระหว่างประเทศกับไทย แต่สามารถนำต้นแบบมาตรการด้านความร่วมมือระหว่างประเทศมาปรับใช้กับประเทศไทยในสองกรณีคือ

- การปรับปรุงตัวบทกฎหมายภายในให้มีหลักการรองรับความร่วมมือระหว่างประเทศ สำหรับกรณีที่ประเทศไทยจะเข้าร่วมเป็นภาคีสนธิสัญญาของสหประชาชาติเมื่อร่างเสร็จ หรือเพื่อรองรับการเข้าร่วมอนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรป
- การนำมาตราต้นแบบดังกล่าวมาใช้เป็นแนวทางการเจรจาทำความตกลงทวิภาคีกับประเทศอื่นเป็นรายประเทศ

ตารางสรุปการเปรียบเทียบรูปแบบความร่วมมือระหว่างประเทศ
ในการป้องกันปราบปรามอาชญากรรมไร้ตัวตน

รูปแบบและมาตรการความร่วมมือระหว่างประเทศในการป้องกันและปราบปรามอาชญากรรมไร้ตัวตน	**ร่างสนธิสัญญาของสหประชาชาติว่าด้วยอาชญากรรมเทคโนโลยี (Draft of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes)**	**อนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรป the Council of Europe Convention on Cybercrime (The Budapest Convention)**
พันธกรณีทั่วไปเกี่ยวกับความร่วมมือ	ร่างมาตรา 56 ร่วมมือในทุกด้านที่เกี่ยวข้องกับการป้องกันปราบปรามอาชญากรรมอิเล็กทรอนิกส์	มาตรา 23 ร่วมมือในทุกด้านที่เกี่ยวข้องกับการป้องกันปราบปรามอาชญากรรมอิเล็กทรอนิกส์
ความร่วมมือในการส่งผู้ร้ายข้ามแดน (Extradition)	ร่างมาตรา 58 - ฐานความผิดเฉพาะที่กำหนดในร่างสนธิสัญญา - มีความผิดจำคุกขั้นต่ำหนึ่งปี - ขึ้นอยู่กับการเจรจาและหลักต่างตอบแทน	มาตรา 24 - ฐานความผิดเฉพาะที่กำหนดในร่างสนธิสัญญา - มีความผิดจำคุกขั้นต่ำหนึ่งปี - ขึ้นอยู่กับการเจรจาและหลักต่างตอบแทน -เป็นไปตามสนธิสัญญาส่งผู้ร้ายข้ามแดนยุโรป
ความร่วมมือในการส่งตัวนักโทษ (Transfer of sentenced persons)	ร่างมาตรา 59 กำหนดให้เป็นไปตามความตกลงระหว่างประเทศสมาชิก	ไม่ได้กำหนดหลักการนี้
หลักการพื้นฐานของมาตรการสนับสนุนร่วมกัน (General principles and procedures relating to mutual legal assistance)	ร่างมาตรา 61 ระบุหลักพื้นฐานการสนับสนุนร่วมกัน โดยมีการกำหนดมาตรการย่อย	มาตรา 25 ระบุหลักพื้นฐานการสนับสนุนร่วมกัน โดยมีการกำหนดมาตรการย่อย
ความร่วมมือในการสืบสวนสอบสวนโดยใช้เทคโนโลยีการประชุมทางไกล (Conducting interrogations using video	ร่างมาตรา 62 การกำหนดให้ประเทศสมาชิก ร่วมมือในการสืบสวนสอบสวน ผู้เกี่ยวข้องกับความผิด โดยใช้ระบบประชุมสอบถามทางไกล	ไม่ได้กำหนดหลักการนี้

รูปแบบและมาตรการความร่วมมือระหว่างประเทศในการป้องกันและปราบปรามอาชญากรรมไร้ตัวตน	ร่างสนธิสัญญาของสหประชาชาติว่าด้วยอาชญากรรมเทคโนโลยี (Draft of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes)	อนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรป the Council of Europe Convention on Cybercrime (The Budapest Convention)
or telephone conferencing systems)		
ความร่วมมือในการจัดให้มีฐานข้อมูลกลาง (Electronic database on mutual legal assistance requests)	ร่างมาตรา 63 กำหนดให้จัดทำฐานข้อมูลอิเล็กทรอนิกส์เกี่ยวกับการดำเนินการขอความร่วมมือระหว่างประเทศสมาชิก	ไม่ได้กำหนดหลักการนี้
ความร่วมมือในการเก็บรักษาข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับการกระทำผิด (Mutual legal assistance in the expedited preservation of stored computer data)	ร่างมาตรา 68 - ความร่วมมือในการร้องขอให้ประเทศสมาชิกออกคำสั่งหรือดำเนินการเก็บรักษาข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับความผิดไว้ - ประเทศผู้รับคำขออาจมีพันธกรณีในการสั่งผู้ให้บริการในประเทศของตนเพื่อเก็บรักษาข้อมูล	มาตรา 29 - ความร่วมมือในการร้องขอให้ประเทศสมาชิกออกคำสั่งหรือดำเนินการเก็บรักษาข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับความผิดไว้ - ประเทศผู้รับคำขออาจมีพันธกรณีในการสั่งผู้ให้บริการในประเทศของตนเพื่อเก็บรักษาข้อมูล
ความร่วมมือในการเข้าถึงข้อมูลคอมพิวเตอร์ที่เก็บรักษาไว้ (Mutual legal assistance in accessing stored computer data)	ร่างมาตรา 70 - ขอความร่วมมือในการเข้าถึงหรือเปิดเผยข้อมูลคอมพิวเตอร์ ที่เก็บรักษาไว้ในประเทศผู้รับคำร้องขอ - อาจเป็นข้อมูลที่ต่อเนื่องจากมาตรการความร่วมมือตามร่างมาตรา 68	มาตรา 31 - ขอความร่วมมือในการเข้าถึงหรือเปิดเผยข้อมูลคอมพิวเตอร์ ที่เก็บรักษาไว้ในประเทศผู้รับคำร้องขอ - อาจเป็นข้อมูลที่ต่อเนื่องจากมาตรการความร่วมมือตามมาตรา 29
ความร่วมมือในการร้อขอให้เปิดเผยข้อมูลการจราจรคอมพิวเตอร์ (Mutual legal assistance in the disclosure of traffic data)	ร่างมาตรา 69 - ประเทศที่รับคำขอให้เก็บรักษาหรือเข้าถึงข้อมูลเปิดเผยข้อมูลจราจรคอมพิวเตอร์ที่บ่งชี้ผู้ให้บริการซึ่งตั้งอยู่ในประเทศสมาชิกอื่น	มาตรา 30 - ประเทศที่รับคำขอให้เก็บรักษาหรือเข้าถึงข้อมูล เปิดเผยข้อมูลจราจรคอมพิวเตอร์ที่บ่งชี้ผู้ให้บริการซึ่งตั้งอยู่ในประเทศสมาชิกอื่น

รูปแบบและมาตรการความร่วมมือระหว่างประเทศในการป้องกันและปราบปรามอาชญากรรมไร้ตัวตน	ร่างสนธิสัญญาของสหประชาชาติว่าด้วยอาชญากรรมเทคโนโลยี (Draft of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes)	อนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรป the Council of Europe Convention on Cybercrime (The Budapest Convention)
	- ข้อยกเว้น ประโยชน์สาธารณะ ความมั่นคง และกรณีความผิดทางการเมือง	- ข้อยกเว้น ประโยชน์สาธารณะ ความมั่นคง และกรณีความผิดทางการเมือง
การเข้าถึงหรือได้มาซึ่งข้อมูลคอมพิวเตอร์ที่จัดเก็บในประเทศสมาชิกอื่นและที่เข้าถึงได้โดยสาธารณะ (Cross-border access to stored computer data)	ร่างมาตรา 72 - การให้สิทธิเข้าถึงข้อมูลที่เปิดเผยต่อสาธารณะ (Open data, publicly available) - การวางหลักขออนุญาตในกรณีข้อมูลเก็บในระบบคอมพิวเตอร์ของบุคคลที่มีสิทธิ	ไม่ได้กำหนดหลักการและความร่วมมือด้านนี้
การเก็บรวบรวมข้อมูลจราจรคอมพิวเตอร์แบบเรียลไทม์ (Mutual legal assistance in the real-time collection of traffic)	ร่างมาตรา 73 - การเข้าถึงข้อมูลจราจรคอมพิวเตอร์แบบตามเวลาจริงหรือเรียลไทม์ - ข้อจำกัดเฉพาะเพื่อการสืบสวนสอบสวนการกระทำที่เป็นความผิดตามกฎหมายภายในประเทศผู้รับคำร้อง	มาตรา 33 - การเข้าถึงข้อมูลจราจรคอมพิวเตอร์แบบตามเวลาจริงหรือเรียลไทม์ - ข้อจำกัดเฉพาะเพื่อการสืบสวนสอบสวนการกระทำที่เป็นความผิดตามกฎหมายภายในประเทศผู้รับคำร้อง
ความช่วยเหลือร่วมกันในการดักรับข้อมูลเนื้อหาการสื่อสารทางคอมพิวเตอร์ (Mutual legal assistance in the interception of content data)	ร่างมาตรา 74 - ความร่วมมือในการเก็บรวบรวมและบันทึกข้อมูลการสื่อสารทางคอมพิวเตอร์จากการสื่อสารโดยเจาะจง - ภายใต้เงื่อนไขและข้อจำกัดของกฎหมายภายในประเทศ	มาตรา 34 - ความร่วมมือในการเก็บรวบรวมและบันทึกข้อมูลการสื่อสารทางคอมพิวเตอร์จากการสื่อสารโดยเจาะจง - ภายใต้เงื่อนไขและข้อจำกัดของกฎหมายภายในประเทศ สนธิสัญญาสหภาพยุโรป
ศูนย์ประสานงานความร่วมมือที่เปิดทำการตลอดเวลา (24/7 point of contact)	ร่างมาตรา 67 ประเทศสมาชิกจัดให้มีศูนย์ประสานงานเพื่อความร่วมมือได้ตลอดเวลา 24/7	มาตรา 35 ประเทศสมาชิกจัดให้มีศูนย์ประสานงานเพื่อความร่วมมือได้ตลอดเวลา 24/7

4.2 วิเคราะห์เปรียบเทียบกับความร่วมมือระหว่างประเทศในเรื่องทางอาญา (MLAT)

มาตรการด้านความร่วมมือระหว่างประเทศในหัวข้อ 4.1 แม้ว่าไม่ได้ระบุเจาะจงถึงอาชญากรรมไร้ตัวตน แต่จากขอบเขตที่มุ่งเน้นการสืบสวนสอบสวนอาชญากรรมไซเบอร์หรืออิเล็กทรอนิกส์ ก็ครอบคลุมถึงอาชญากรรมไร้ตัวตนด้วย อย่างไรก็ตาม นอกจากความร่วมมือเจาะจงดังกล่าวแล้ว ในระดับระหว่างประเทศและระดับความตกลงทวิภาคี พบว่ามีสนธิสัญญาความร่วมมือทางอาญาในการดำเนินมาตรการช่วยเหลือระหว่างประเทศ (mutual legal assistance treaty (MLAT) ซึ่งจะนำมาวิเคราะห์เปรียบเทียบกับกรณีของอาชญากรรมไร้ตัวตนดังนี้

4.2.1 สนธิสัญญาสหภาพยุโรปว่าด้วยความร่วมมือในทางอาญา (The European Convention on Mutual Assistance in Criminal Matters)

สนธิสัญญาฉบับนี้กำหนดกรอบความร่วมมือในการให้ความช่วยเหลือทางกฎหมายร่วมกันระหว่างประเทศสมาชิก ซึ่งมีพันธกรณีจะให้ความร่วมมืออย่างโดยกำหนดมาตรการในระดับกว้างที่สุดที่เป็นไปได้ (Widest measure) เพื่อการสืบสวนสอบสวน ดำเนินคดีกับอาชญากรรม โดยมีเงื่อนไขสำคัญคือ ประเทศผู้ร้องขอ (Requesting state) และประเทศผู้รับการร้องขอ (Requested state) ต้องมีความตกลงร่วมกัน ด้วยการส่งคำร้องขอและพิจารณาคำร้อง ตามหลักต่างตอบแทนและตามความตกลงระกว่างกัน สนธิสัญญานี้เปิดให้ประเทศนอกสหภาพยุโรปให้สัตยาบันด้วย ซึ่งมีประเทศนอกสหภาพยุโรปที่เข้าร่วมเช่น รัสเซีย อิสราเอล เกาหลีใต้ สำหรับไทยไม่ได้ให้สัตยาบันสนธิสัญญานี้

ข้อวิเคราะห์

ข้อจำกัดของสนธิสัญญานี้คือ ไม่ได้กำหนดหลักการความร่วมมือที่เจาะจงสำหรับอาชญากรรมไร้ตัวตนหรืออาชญากรรมที่กระทำทางระบบคอมพิวเตอร์ บทบัญญัติเกี่ยวกับมาตรการร่วมมือไม่ได้บ่งระบุถึงความร่วมมือในการเข้าถึงข้อมูลในระบบคอมพิวเตอร์หรือเก็บรวบรวมข้อมูลการสื่อสารทางคอมพิวเตอร์ นอกจากนี้ข้อจำกัดที่สำคัญคือการกำหนดหลักการกว้าง โดยให้ประเทศภาคีตกลงร่วมก้นในการ่วมมือเป็นรายกรณีด้วยกระบวนการส่งคำร้องขอและพิจารณาคำร้องขอ

4.2.2 สนธิสัญญาความร่วมมือในการดำเนินกระบวนการทางอาญาของอาเซียน (Treaty on Mutual Legal Assistance in Criminal Matters (MLAT)

สนธิสัญญานี้เป็นความตกลงของประเทศสมาชิกอาเซียน โดยไทยได้เข้าร่วมลงนามในปี ค.ศ. 2006

ขอบเขตความร่วมมือระบุในมาตรา 1 ซึ่งมีหลักสำคัญว่า ประเทศสมาชิกจะดำเนินการให้ความร่วมมือในมาตรการช่วยเหลือกันทางด้านคดีอาญาอย่างกว้างเท่าที่เป็นไปได้ภายใต้กฎหมายภายในประเทศ ซึ่งรวมถึงความร่วมมือด้านสืบสวนสอบสวน การฟ้องร้องดำเนินคดี และการดำเนินการบังคับตามคำพิพากษา

มาตรการความช่วยเหลือซึ่งแบ่งเป็นด้านต่างๆ ได้ระบุไว้ในมาตรา 2 เช่น การเก็บรวบรวมพยานหลักฐานหรือเอกสารจากบุคคล การจัดการเพื่อให้บุคคลเป็นพยาน การบังคับใช้หมายค้นหรือยึด การตรวจสอบวัตถุและสถานที่ การจัดให้ซึ่งเอกสารต้นฉบับหรือสำเนา บันทึกและหลักฐาน การบ่งระบุและติดตามทรัพย์สินที่ได้มจากการกระทำผิด การยึดอายัดทรัพย์ที่ได้มาจากการกระทำผิด การสืบสวนและบ่งระบุตัวพยานและผู้ต้องสงสัย

การดำเนินการช่วยเหลือดังกล่าวอยู่ภายใต้เงื่อนไขของการตกลงระหว่างกันภายใต้กรอบสนธิสัญญานี้และภายใต้กฎหมายภายในของประเทศที่รับคำร้องขอ

ข้อวิเคราะห์

สนธิสัญญานี้มีขอบเขตกว้าง ไม่จำกัดประเภทของอาชญากรรมที่เป็นเหตุแห่งการร้องขอความร่วมมือ แต่มีข้อจำกัดคือ ไม่ได้กำหนดหลักการความร่วมมือที่เจาะจงสำหรับอาชญากรรมไร้ตัวตนหรืออาชญากรรมที่กระทำทางระบบคอมพิวเตอร์ ในส่วนรายละเอียดความร่วมมือ แม้ว่ามีบทบัญญัติความร่วมมือในแง่ของพยานหลักฐาน แต่ตัวบทยังคงสะท้อนถึงการส่งเอกสารทางกายภาพ การสอบถามหรือส่งตัวบุคคล ฯลฯ ไม่ได้บ่งระบุถึงมาตรการที่มีลักษณะเจาะจงทางเทคโนโลยี เช่น การเข้าถึงข้อมูลในระบบคอมพิวเตอร์หรือเก็บรวบรวมข้อมูลการสื่อสารทางคอมพิวเตอร์

4.3 วิเคราะห์เปรียบเทียบกับความร่วมมือระหว่างประเทศทางอาญาตามกฎหมายภายในประเทศ

จากการศึกษาในหัวข้อ 4.1 และ 4.2 แสดงให้เห็นถึงมาตรการความร่วมมือในระดับความตกลงระหว่างประเทศ อย่างไรก็ตาม การดำเนินความร่วมมือระหว่างประเทศอาจต้องพิจารณาเชื่อมโยงกับกฎหมายภายในอันเป็นพื้นฐานรองรับการร่วมมือระหว่างประเทศ โดยจะยกตัวอย่างกฎหมายสหรัฐอเมริกา

ความร่วมมือระหว่างประเทศเกี่ยวกับอาชญากรรมไซเบอร์และพยานหลักฐานอิเล็กทรอนิกส์ของสหรัฐอเมริกา เกี่ยวข้องกับกฎหมายภายในระดับรัฐบาลกลางคือ กฎหมายว่าด้วยการใช้ข้อมูลจากต่างประเทศโดยชอบด้วยกฎหมาย (The Clarifying Lawful Overseas Use of Data Act หรือในที่นี้จะใช้คำย่อว่า CLOUD Act)

กฎหมายนี้ให้อำนาจเจ้าหน้าที่บังคับใช้กฎหมายของรัฐบาลกลาง ร้องขอให้ผู้ให้บริการข้อมูลอิเล็กทรอนิกส์ ส่งมอบหรือให้เจ้าหน้าที่เข้าถึงข้อมูลอิเล็กทรอนิกส์ที่จัดเก็บไว้ ไม่ว่าจะเก็บไว้ในเซิร์ฟเวอร์ที่ตั้งอยู่ในสหรัฐอเมริกาหรือตั้งอยู่นอกสหรัฐอเมริกา โดยกฎหมายนี้กำหนดหน้าที่ให้ผู้ให้บริการที่จัดเก็บข้อมูลต้องส่งมอบหรือให้เจ้าหน้าที่เข้าถึงข้อมูลผู้ใช้บริการที่เก็บไว้ในเซิร์ฟเวอร์ในความควบคุมของตน อย่างไรก็ตาม กฎหมายกำหนดเหตุในการโต้แย้งคำสั่งกรณีที่การให้เข้าถึงข้อมูลจะกระทบสิทธิของบุคคลในประเทศที่เซิร์ฟเวอร์ตั้งอยู่

กฎหมายนี้ให้อำนาจรัฐบาลสหรัฐอเมริกา ดำเนินการทำความตกลงกับประเทศอื่นในลักษณะสนธิสัญญาหรือความตกลงทวิภาคีเพื่อให้ประเทศนั้นให้ความร่วมมือกับสหรัฐอเมริกาในการเข้าถึงและได้มาซึ่งข้อมูล ในปัจจุบันสหรัฐอาศัยกฎหมายภายในดังกล่าวเป็นพื้นฐานของการเจราจาและได้ทำความตกลงร่วมกับสหราชอาณาจักร อย่างไรก็ตาม ในส่วนของประเทศไทยยังไม่มีความตกลงทวิภาคีกับสหรัฐอเมริกาบนพื้นฐานจากกฎหมาย CLOUD Act

ข้อวิเคราะห์ กฎหมาย CLOUD Act แยกพิจารณาได้สองส่วนคือ

1. ส่วนของหลักการที่กำหนดหน้าที่ผู้ให้บริการ ทั้งนี้เพราะ CLOUD Act เป็นกฎหมายภายในที่ไม่ได้วางหลักการร่วมมือหรือขอความช่วยเหลือระหว่างประเทศโดยตรง เพราะกฎหมายนี้เกิดขึ้นจากเหตุผลและความจำเป็นในการสืบสวนสอบสวนและบังคับใช้กฎหมายสหรัฐอเมริกา[145] เนื่องจากข้อมูลอันเป็นพยานหลักฐานของอาชญากรรมไซเบอร์ปัจจุบันอาจอยู่ในเซิร์ฟเวอร์ที่ตั้งอยู่ในหลายประเทศ นอกเขตแดนสหรัฐอเมริกา รวมทั้งระบบคลาวด์ที่ข้อมูลมีลักษณะกระจายและไม่รวมศูนย์ ดังนั้น หลักการสำคัญของกฎหมายนี้คือให้อำนาจเจ้าหน้าที่ร้องขอข้อมูลจากผู้ให้บริการเอกชนในสหรัฐอเมริก โดยมีขอบเขตการสั่งให้ได้มาหรือเข้าถึงข้อมูลของผู้ให้บริการนั้นที่จัดเก็บในต่างประเทศ จะเห็นได้ว่า แม้กฎหมายนี้เป็นกฎหมายภายใน ไม่สามารถบังคับใช้กับพยานหลักฐานที่จัดเก็บในเขตแดนต่างประเทศโดยสั่งการบุคคลหรือนิติบุคคลในต่างประเทศ แต่มีลักษณะการสั่งหรือบังคับผู้ให้บริการสหรัฐอเมริกาให้ส่งมอบหรือให้เจ้าหน้าที่เข้าถึงข้อมูลที่รวมถึงข้อมูลจัดเก็บในต่างประเทศ การดำเนินการตามหลักการในส่วนนี้ไม่จัดเป็นความร่วมมือหรือความช่วยเหลือระหว่างประเทศ นอกจากนั้น

[145] Schwartz, P. M. (2018). Legal access to the global cloud. Columbia Law Review, 118(6), 1681-1762.

หลักการส่วนนี้จัดเป็นมาตรการที่ให้เจ้าหน้าที่สหรัฐเข้าถึงข้อมูลเพื่อการสอบสวนอาชญากรรมอันเป็นความผิดตามกฎหมายสหรัฐ ไม่เกี่ยวข้องกับการที่ประเทศอื่นขอให้สหรัฐส่งข้อมูลในสหรัฐให้กับประเทศผู้ร้องขอ

2. ส่วนของความร่วมมือระหว่างประเทศ กฎหมาย CLOUD Act ไม่ได้ให้สิทธิแก่รัฐบาลต่างประเทศในการยื่นคำร้องขอให้สหรัฐยอมให้เข้าถึงข้อมูลที่จัดเก็บในสหรัฐหรือให้ทางสหรัฐส่งข้อมูลให้ตามคำขอ แต่กฎหมายนี้ให้รัฐบาลสหรัฐสามารถมีอำนาจเจรจาทำความตกลงทวิภาคีกับรัฐบาลต่างประเทศ เพื่อให้เกิดความร่วมมือในการขอเข้าถึงหรือขอให้ผู้ให้บริการสหรัฐอเมริกาส่งข้อมูลคอมพิวเตอร์เพื่อการสืบสวนสอบสวนอาชญากรรมได้ตามหลักความช่วยเหลือร่วมกัน ซึ่งกฎหมายนี้ไม่ได้กำหนดรายละเอียดของมาตรการแต่ละด้านดังเช่นกรอบความตกลงระหว่างประเทศในหัวข้อ 4.1 ดังนั้น ความร่วมมือระหว่างประเทศจึงขึ้นอยู่กับการเจราจาโดยอาจเป็นความร่วมมือในลักษณะ MLAT หรืออาจใช้กรอบของความร่วมมืออาชญากรรมไซเบอร์ของร่างสหประชาชาติ

ตารางสรุปการเปรียบเทียบความร่วมมือระหว่างประเทศในการป้องกันปราบปรามอาชญากรรมไซเบอร์และความร่วมมือระหว่างประเทศในเรื่องทางอาญา (MLAT)

จากการศึกษาในหัวข้อ 4.1 และ 4.2 จะเห็นได้ว่า หลักการความร่วมมือระหว่างประเทศตามร่างสนธิสัญญาสหประชาชาติและตามอนุสัญญาอาชญากรรมไซเบอร์ยุโรป กำหนดหลักการความร่วมมือที่เกี่ยวกับอาชญากรรมไซเบอร์หรืออาชญากรรมเทคโนโลยีไว้เป็นการเฉพาะซึ่งรวมไปถึงอาชญากรรมไร้ตัวตนที่กระทำทางคอมพิวเตอร์ จึงแตกต่างกับความร่วมมือระหว่างประเทศในเรื่องทางอาญา (MLAT) ซึ่งแม้ว่ามีการระบุถึงความร่วมมือในการรวบรวมพยานหลักฐาน โดยมีการระบุเกี่ยวกับการขอให้ส่งเอกสาร แต่ไม่ได้ระบุมาตรการที่เจาะจงในบริบทของอาชญากรรมเทคโนโลยีดังเช่นสนธิสัญญาความร่วมมือป้องกันและปราบปรามอาชญากรรมไซเบอร์ทั้ง 2 ฉบับดังกล่าวมาแล้ว เช่น ไม่มีการกำหนดหลักการเกี่ยวกับการ “เข้าถึง” ข้อมูลคอมพิวเตอร์ ไม่ได้ระบุถึงมาตาการความร่วมมือทางเทคโนโลยี การจัดตั้งศูนย์ประสานงานที่อาศัยเทคโนโลยีในการติดต่อสื่อสารตลอดเวลา ทั้งนี้ผู้วิจัยได้สรุปการวิเคราะห์ หลักความร่วมมือระหว่างประเทศในกรณีอาชญากรรมไซเบอร์ของสหประชาชาติและสหภาพยุโรป โดยนำไปเปรียบเทียบกับความร่วมมือระหว่างประเทศในเรื่องทางอาญา (MLAT) ตามประเด็นหรือมาตรการร่วมมือย่อยแต่ละด้าน ดังตารางต่อไปนี้

รูปแบบและมาตรการความร่วมมือระหว่างประเทศในการป้องกันและปราบปรามอาชญากรรมไร้ตัวตน	ความร่วมมือตามกฎหมายระหว่างประเทศที่เกี่ยวกับอาชญากรรมไซเบอร์หรืออาชญากรรมเทคโนโลยี	ความร่วมมือระหว่างประเทศในเรื่องทางอาญา (MLAT)
ความร่วมมือในการสืบสวนสอบสวนโดยใช้เทคโนโลยีการประชุมทางไกล (Conducting interrogations using video or telephone conferencing systems)	- ร่างมาตรา 62 สนธิสัญญาสหประชาชาติ - อนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรป ไม่ได้กำหนด	สนธิสัญญายุโรป / อาเซียน ไม่ได้กำหนดหลักการนี้ - มีหลักการใกล้เคียงคือมาตรการร่วมมือในการสอบถามพยาน แต่ไม่ได้ระบุถึงการสอบสวนหรือสอบถามทางอิเล็กทรอนิกส์
ความร่วมมือในการจัดให้มีฐานข้อมูลกลาง (Electronic database on mutual legal assistance requests)	ร่างมาตรา 63 สนธิสัญญาสหประชาชาติกำหนดให้จัดทำฐานข้อมูลอิเล็กทรอนิกส์เกี่ยวกับการดำเนินการขอความร่วมมือระหว่างประเทศสมาชิก	สนธิสัญญายุโรป / อาเซียน ไม่ได้กำหนดหลักการนี้
ความร่วมมือในการเก็บรักษาข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับการกระทำผิด (Mutual legal assistance in the expedited preservation of stored computer data)	ร่างมาตรา 68 สนธิสัญญาสหประชาชาติ อนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรปมาตรา 29 - ความร่วมมือในการร้องขอให้ประเทศสมาชิกออกคำสั่งหรือดำเนินการเก็บรักษาข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับความผิดไว้ (Preservation)	สนธิสัญญายุโรป / อาเซียน ไม่ได้กำหนดหลักการนี้ - มีหลักการใกล้เคียงคือการร่วมมือเก็บรวบรวมหลักฐาน ซึ่งไม่เจาะจงถึงการรักษาข้อมูลคอมพิวเตอร์ไว้ก่อนหรือป้องกันมิให้มีการแก้ไขข้อมูล
ความร่วมมือในการเข้าถึงข้อมูลคอมพิวเตอร์ที่เก็บรักษาไว้ (Mutual legal assistance in accessing stored computer data)	ร่างมาตรา 70 สนธิสัญญาสหประชาชาติ อนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรปมาตรา 31	สนธิสัญญายุโรป / อาเซียน ไม่ได้กำหนดหลักการนี้ - มีหลักการใกล้เคียงคือการร่วมมือเก็บรวบรวมหลักฐาน ซึ่งไม่เจาะจงถึงการเข้าถึง (Access) ข้อมูลคอมพิวเตอร์
ความร่วมมือในการร้อขอให้เปิดเผยข้อมูลการจราจรคอมพิวเตอร์ (Mutual legal assistance in the disclosure of traffic data)	ร่างมาตรา 69 สนธิสัญญาสหประชาชาติ อนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรปมาตรา 30	สนธิสัญญายุโรป / อาเซียน ไม่ได้กำหนดหลักการนี้ - ไม่ได้ระบุความร่วมมือในการสั่งผู้ให้บริการเอกชนในประเทศผู้รับคำร้องขอ

รูปแบบและมาตรการความร่วมมือระหว่างประเทศในการป้องกันและปราบปรามอาชญากรรมไร้ตัวตน	ความร่วมมือตามกฎหมายระหว่างประเทศที่เกี่ยวกับอาชญากรรมไซเบอร์หรืออาชญากรรมเทคโนโลยี	ความร่วมมือระหว่างประเทศในเรื่องทางอาญา (MLAT)
การเข้าถึงหรือได้มาซึ่งข้อมูลคอมพิวเตอร์ที่จัดเก็บในประเทศสมาชิกอื่นและที่เข้าถึงได้โดยสาธารณะ (Cross-border access to stored computer data)	ร่างมาตรา 72 สนธิสัญญาสหประชาชาติอนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรปไม่ได้กำหนดหลักการนี้	สนธิสัญญายุโรป / อาเซียน ไม่ได้กำหนดหลักการนี้ - มีหลักการใกล้เคียงคือการร่วมมือเก็บรวบรวมหลักฐาน ซึ่งไม่เจาะจงถึงการเข้าถึง (Access) ข้อมูลคอมพิวเตอร์
การเก็บรวบรวมข้อมูลจราจรคอมพิวเตอร์แบบเรียลไทม์ (Mutual legal assistance in the real-time collection of traffic)	ร่างมาตรา 73 สนธิสัญญาสหประชาชาติอนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรปมาตรา 33	สนธิสัญญายุโรป / อาเซียน ไม่ได้กำหนดหลักการนี้ - มีหลักการใกล้เคียงคือการร่วมมือเก็บรวบรวมหลักฐาน ซึ่งไม่เจาะจงถึงข้อมูลจราจรคอมพิวเตอร์ (Traffic data)
ความช่วยเหลือร่วมกันในการดักรับข้อมูลเนื้อหาการสื่อสารทางคอมพิวเตอร์ (Mutual legal assistance in the interception of content data)	ร่างมาตรา 74 สนธิสัญญาสหประชาชาติอนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรปมาตรา 34	สนธิสัญญายุโรป / อาเซียน ไม่ได้กำหนดหลักการนี้ - มีหลักการใกล้เคียงคือการร่วมมือเก็บรวบรวมหลักฐาน ซึ่งไม่เจาะจงถึงการดักรับข้อมูลคอมพิวเตอร์ (Interception)
ศูนย์ประสานงานความร่วมมือที่เปิดทำการตลอดเวลา (24/7 point of contact)	ร่างมาตรา 67 สนธิสัญญาสหประชาชาติอนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรปมาตรา 35	สนธิสัญญายุโรป / อาเซียน ไม่ได้กำหนดหลักการนี้

สรุปบทวิเคราะห์

จากการวิเคราะห์มาตรการความร่วมมือในระดับระหว่างประเทศพบว่า ไม่มีสนธิสัญญาหรือร่างสนธิสัญญาที่ระบุถึงความร่วมมือในกรณีอาชญากรรมไร้ตัวตนโดยเฉพาะ แต่กรอบแนวทางระหว่างประเทศที่ใกล้เคียงและครอบคลุมถึงอาชญากรรมไร้ตัวตนคือ กรอบแนวทางความร่วมมือป้องกันและปราบปรามอาชญากรรมไซเบอร์ตามกรอบของสหภาพยุโรปและสหประชาชาติ โดยผลการวิเคราะห์เปรียบเทียบชี้ให้เห็นประเด็นหรือมาตรการย่อยที่เจาะจงถึงสภาพและลักษณะของอาชญากรรมไซเบอร์โดยเฉพาะอย่างยิ่งความร่วมมือด้านการสืบสวนสอบสวนและรวบรวมพยานหลักฐานทางดิจิทัลหรืออิเล็กทรอนิกส์ เมื่อเปรียบเทียบกับความ

ร่วมมือในทางอาญาระหว่างประเทศ (MLAT) ซึ่งเป็นหลักการและแนวปฏิบัติของความตกลงระดับทวิภาคีที่พบในหลายประเทศ จะพบว่า MLAT แม้จะมีหลักความร่วมมือเกี่ยวกับการสืบสวนสอบสวนและได้มาซึ่งพยานหลักฐาน แต่ไม่ได้มีหลักการเฉพาะสำหรับความร่วมมือด้านต่างๆเพื่อป้องกันและปราบปรามอาชญากรรมไซเบอร์และอาชญากรรมไร้ตัวตน

สำหรับประเทศไทยไม่ได้เข้าร่วมเป็นภาคีในกรอบกฎหมายระหว่างประเทศที่เกี่ยวข้องกับอาชญากรรมไร้ตัวตนและอาชญากรรมไซเบอร์ กล่าวคือ ในส่วนของอนุสัญญาอาชญากรรมไซเบอร์ของสหภาพยุโรปนั้น ไทยไม่ได้เป็นภาคีและไม่ได้ให้สัตยาบัน สำหรับร่างสนธิสัญญาสหประชาชาติว่าด้วยอาชญากรรมเทคโนโลยี ในส่วนของประเทศไทยไม่ปรากฏการเป็นผู้แทนหรือคณะทำงาน (Ad hoc committee) ในการร่างสนธิสัญญานี้ จึงกล่าวได้ว่าในทางกฎหมายระหว่างประเทศไทยไม่มีพันธกรณีความร่วมมือตามสนธิสัญญาดังกล่าว เมื่อเปรียบเทียบกับกฎหมายระหว่างประเทศที่ไทยมีความผูกพัน จะพบว่า ในอาเซียนมีหลักการร่วมมือระดับระหว่างประเทศในทางอาญา แต่มีข้อจำกัดเพราะไม่ใช่ความร่วมมือโดยตรงเกี่ยวกับอาชญากรรมไร้ตัวตนและอาชญากรรมไซเบอร์

บทที่ 5
บทสรุปและข้อเสนอแนะ

1. บทสรุป

โครงการศึกษาวิจัยเรื่อง ต้นแบบกฎหมายเพื่อป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตน มีวัตถุประสงค์เพื่อ 1) ศึกษารูปแบบของอาชญากรรมแบบไร้ตัวตนที่กระทำโดยองค์กรอาชญากรรมข้ามชาติในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ ตลอดจนความเสี่ยงจากภัยคุกคามจากอาชญากรรมประเภทดังกล่าว 2) ศึกษากฎหมายที่กำหนดความผิดเกี่ยวกับอาชญากรรมแบบไร้ตัวตนที่กระทำโดยองค์กรอาชญากรรมข้ามชาติในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์โดยศึกษาเปรียบเทียบกฎหมายต่างประเทศ และศึกษากฎหมายที่เกี่ยวข้องกับการบังคับใช้กฎหมายของประเทศไทย ทั้งด้านการสืบสวนสอบสวน การรวบรวมพยานหลักฐาน การดำเนินคดี การดำเนินมาตรการตามกฎหมายฟอกเงิน และความร่วมมือระหว่างประเทศ 3) ศึกษาปัญหาและอุปสรรคในการบังคับใช้กฎหมายและการป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตนที่กระทำโดยองค์กรอาชญากรรมข้ามชาติในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ 4) ศึกษาและจัดทำต้นแบบกฎหมาย (Model Law) ของประเทศไทย ในรูปแบบของการจัดทำกฎหมายต้นแบบเพื่อป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ และ 5) เสนอแนะมาตรการความร่วมมือระหว่างประเทศเพื่อป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตนที่กระทำโดยองค์กรอาชญากรรมข้ามชาติในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์

ผลการศึกษาเป็นไปตามวัตถุประสงค์ของการวิจัย สรุปได้ดังนี้

<u>วัตถุประสงค์ประการแรก</u> ศึกษารูปแบบของอาชญากรรมแบบไร้ตัวตนที่กระทำโดยองค์กรอาชญากรรมข้ามชาติในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ ตลอดจนความเสี่ยงจากภัยคุกคามจากอาชญากรรมประเภทดังกล่าว พบว่า อาชญากรรมคอมพิวเตอร์แบบไร้ตัวตนประกอบด้วยกระทำสองส่วน คือ 1) การกระทำความผิดหลัก ได้แก่ อาชญากรรมคอมพิวเตอร์ที่ส่งผลกระทบต่อความปลอดภัยของระบบหรือข้อมูล กล่าวคือ อาชญากรรมที่มีคอมพิวเตอร์เป็นเป้าหมาย (Computer as target) และอาชญากรรมคอมพิวเตอร์ที่โดยหลักแล้วไม่ส่งผลกระทบต่อความปลอดภัยของระบบหรือข้อมูล แต่มีเป้าหมายที่การหลอกลวงบุคคล เช่น การฉ้อโกงทางคอมพิวเตอร์ (Computer fraud) และ 2) การกระทำเพื่อให้มีลักษณะไร้ตัวตนหรือการปกปิดตัวตน ที่มี

คุณลักษณะสำคัญของคือ ความนิรนาม (Anonymity) มีการใช้เทคโนโลยีดิจิทัลหรือเทคโนโลยีสารสนเทศในการปกปิดตัวตนของอาชญากรด้วยเทคนิคต่างๆ เพื่อวัตถุประสงค์สำคัญคือการหลบเลี่ยงจากการบังคับใช้กฎหมายหรือการสืบสวนสอบสวน สำหรับการกระทำเพื่อปกปิดตัวตน อาจเป็นการกระทำต่างวาระกับการกระทำหลัก รวมทั้งอาจเข้าองค์ประกอบความผิดคนละฐานกับความผิดหลักอันเป็นเป้าหมายของอาชญากรรมชนิดนี้ก็ได้ โดยวิธีการปกปิดตัวตนจำแนกเป็นสองรูปแบบคือ รูปแบบการใช้เทคโนโลยีเพื่อปกปิดตัวตนด้วยเทคนิคต่างๆ ซึ่งไม่ได้อาศัยข้อมูลระบุตัวผู้อื่น และรูปแบบการใช้ข้อมูลระบุตัวผู้อื่นเพื่อปกปิดตัวตนในการก่ออาชญากรรม ซึ่งในส่วนการกระทำหลักของอาชญากรรมแบบไร้ตัวตน สามารถอธิบายรูปแบบวิธีการได้ในกลุ่มของวิธีการเช่นเดียวกับอาชญากรรมไซเบอร์หรืออาชญากรรมคอมพิวเตอร์ทั่วไป เช่น การเข้าถึงโดยมิชอบ การโจมตีรบกวนขัดขวางการทำงานของระบบ การทำลายหรือแก้ไขข้อมูล ฯลฯ แต่จะมีการกระทำในส่วนที่สองเพิ่มเติมขึ้นมาคือการใช้วิธีการเพื่อปกปิดตัวตนหรือทำให้การกระทำส่วนแรกไม่สามารถระบุร่องรอยหรือติดตามตัวผู้กระทำได้ จากลักษณะดังกล่าว ผู้วิจัยจึงได้กำหนดขอบเขตคำว่า “อาชญากรรมแบบไร้ตัวตน” ให้หมายความถึง รูปแบบหนึ่งของอาชญากรรมคอมพิวเตอร์ที่อาศัยประโยชน์จากสภาพแวดล้อมทางไซเบอร์ในการกระทำความผิด มีการกระทำความผิดทางระบบคอมพิวเตอร์ที่ใช้วิธีการปกปิดตัวตน โดยมีการนำข้อมูลบุคคลอื่นมาใช้ระบุตัว หรือการใช้วิธีการต่าง ๆ ในการปกปิดตัวตนของผู้กระทำความผิดและเป็นความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์

<u>วัตถุประสงค์ประการที่สอง</u> ศึกษากฎหมายที่กำหนดความผิดเกี่ยวกับอาชญากรรมแบบไร้ตัวตนที่กระทำโดยองค์กรอาชญากรรมข้ามชาติในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์โดยศึกษาเปรียบเทียบกฎหมายต่างประเทศ และศึกษากฎหมายที่เกี่ยวข้องกับการบังคับใช้กฎหมายของประเทศไทย ทั้งด้านการสืบสวนสอบสวน การรวบรวมพยานหลักฐาน การดำเนินคดี การดำเนินมาตรการตามกฎหมายฟอกเงิน และความร่วมมือระหว่างประเทศ พบว่า

อนุสัญญาว่าด้วยอาชญากรรมไซเบอร์สหภาพยุโรป (Convention on Cybercrime) นับเป็นกฎหมายระหว่างประเทศฉบับหลักที่เกี่ยวกับการวางแนวทางกฎหมายต้นแบบสำหรับอาชญากรรมไซเบอร์โดยเฉพาะ แต่พบว่าไม่มีฐานความผิดหรือหลักการที่ระบุถึง “อาชญากรรมคอมพิวเตอร์แบบไร้ตัวตนหรือนิรนาม” (Anonymous computer crime) ไว้โดยเฉพาะ อย่างไรก็ตาม องค์ประกอบความผิดต้นแบบที่ระบุในอนุสัญญาฯ มีความเกี่ยวข้องกับอาชญากรรมไร้ตัวตน ทั้งในส่วนของการกระทำหลักและการกระทำในส่วนปกปิดตัวตน ได้แก่ ความผิดฐานเข้าถึงโดยมิชอบ (Illegal access, Article 2) สามารถปรับใช้กับการกระทำในส่วนปกปิดตัวตนของอาชญากรรมแบบไร้ตัวตน ในกรณีที่อาชญากรใช้วิธีการปกปิดตัวตนที่มีลักษณะของการเข้าถึงระบบหรือข้อมูล

เช่น องค์กรอาชญากรทำการเข้าถึงข้อมูลระบุตัวลูกค้าขององค์กรหนึ่งและนำข้อมูลดังกล่าวไปใช้แสดงตนเพื่อทำธุรกรรมต่างๆทางอิเล็กทรอนิกส์ ความผิดฐานดักรับข้อมูลคอมพิวเตอร์โดยมิชอบ (Illegal Interception, Article 3) สามารถปรับใช้กับการกระทำในส่วนปกปิดตัวตนของอาชญากรรมแบบไร้ตัวตน ในกรณีที่อาชญากรใช้วิธีการดักรับข้อมูลระบุตัวของผู้อื่นเพื่อนำไปใช้ปกปิดการกระทำของตน ความผิดฐานกระทำต่อข้อมูลโดยมิชอบ (Data interference, Article 4) สามารถปรับใช้กับการกระทำในส่วนปกปิดตัวตนของอาชญากรรมแบบไร้ตัวตน ในกรณีที่อาชญากรใช้วิธีการปกปิดตัวตนที่ส่งผลให้เกิดการแก้ไขเปลี่ยนแปลงข้อมูล เช่น การแก้ไขเปลี่ยนแปลงรหัสผ่านบัญชีจดหมายอิเล็กทรอนิกส์ของเหยื่อและเข้าควบคุมบัญชีนั้นเพื่อนำมาใช้ส่งไวรัส ความผิดฐานกระทำต่อระบบคอมพิวเตอร์โดยมิชอบ (System interference, Article 5) สามารถปรับใช้กับการกระทำในส่วนปกปิดตัวตนของอาชญากรรมแบบไร้ตัวตน ในกรณีที่อาชญากรใช้วิธีการปกปิดตัวตนที่ส่งผลให้เกิดการระงับหรือขัดข้องของระบบ ความผิดฐานการใช้อุปกรณ์โดยมิชอบ (Misuse of device , Article 6) ซึ่งอาจนำมาปรับใช้ได้กับการกระทำที่เกี่ยวข้อง เช่น ผู้ขายซอฟท์แวร์ที่ออกแบบเพื่อปกปิดร่องรอยหรือลบร่องรอยการเข้าถึงระบบของอาชญากร เป็นต้น ความผิดต้นแบบเกี่ยวกับการปลอมแปลงทางคอมพิวเตอร์ (Computer-related forgery, Article 7) สามารถปรับใช้กับการกระทำหลักของอาชญากรรมแบบไร้ตัวตน ในกรณีลักษณะหรือวิธีการกระทำคือการสร้างข้อมูลที่ไม่ถูกต้องหรือข้อมูลปลอม รวมทั้งอาจปรับใช้กับการกระทำในส่วนของการปกปิดตัวตนในกรณีที่มีการใช้ข้อมูลปลอม และความผิดต้นแบบเกี่ยวกับการฉ้อโกงหลอกลวงทางคอมพิวเตอร์ (Computer-related fraud, Article 8) สามารถปรับใช้กับการกระทำหลักของอาชญากรรมแบบไร้ตัวตน ในกรณีที่ลักษณะหรือวิธีการกระทำเป็นการใช้ชุดคำสั่งหรือโปรแกรมเพื่อให้ระบบประมวลผลไปตามความต้องการของอาชญากรและเนื่องจากมาตรา 8 ของความผิดต้นแบบมีองค์ประกอบที่กว้าง ส่งผลให้การกระทำในส่วนปกปิดตัวตนอาจเข้าข่ายฐานความผิดนี้ อย่างไรก็ตาม อนุสัญญานี้ไม่จำกัดเฉพาะประเทศสมาชิกสหภาพยุโรป โดยมีประเทศนอกกลุ่มยุโรปให้สัตยาบันด้วย เช่น สหรัฐอเมริกา แคนาดา ออสเตรเลีย ญี่ปุ่น เป็นต้น สำหรับประเทศไทยไม่ได้ให้สัตยาบันและไม่มีพันธกรณีผูกพันตามกฎหมายระหว่างประเทศสำหรับอนุสัญญานี้ อย่างไรก็ตาม เมื่อพิจารณาฐานความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พบว่าหลายฐานความผิดสะท้อนถึงองค์ประกอบจากอนุสัญญาฯดังกล่าว

การบังคับใช้กฎหมายภายในพบว่า พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม เป็นกฎหมายที่เกี่ยวข้องโดยตรงกับอาชญากรรมคอมพิวเตอร์ ไม่มีฐานความผิดหรือหลักการที่ระบุถึง “อาชญากรรมคอมพิวเตอร์แบบไร้ตัวตนหรือนิรนาม” (Anonymous computer crime) ไว้โดยเฉพาะ แต่เมื่อนำพฤติกรรมและรูปแบบของอาชญากรรมไร้ตัวตนที่จำแนกเป็นการกระทำสองส่วนมาพิจารณาตามองค์ประกอบความผิดเกี่ยวกับความปลอดภัยของระบบคอมพิวเตอร์มาตรา 5 - 11

และมาตรา 14 (1) ในส่วนที่เกี่ยวกับการปลอมแปลงข้อมูลนั้น พบว่า สามารถปรับใช้กับอาชญากรรมแบบไร้ตัวตนที่มีรูปแบบหลากหลายทั้งสองส่วนของการกระทำ สำหรับมาตรา 14 (1) ในส่วนที่ไม่เกี่ยวข้องกับผลกระทบต่อระบบหรือข้อมูลคอมพิวเตอร์นั้น ก็อาจปรับใช้ได้กับอาชญากรรมแบบไร้ตัวตนสำหรับกรณีที่ปกปิดตัวตนโดยลักษณะของการนำข้อมูลเท็จเข้าสู่ระบบ

ในส่วนกฎหมายอื่นที่เกี่ยวข้องพบว่า มีข้อจำกัดในการนำมาบังคับใช้กับอาชญากรรมแบบไร้ตัวตน ในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์หลายประการดังนี้

- พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 จะต้องปรากฏข้อเท็จจริงว่าเป็นอาชญากรรมแบบไร้ตัวตนนั้น เป็นความผิดที่มีลักษณะเป็นองค์กรอาชญากรรมข้ามชาติตามนิยามและองค์ประกอบความผิดของกฎหมายด้วย จึงจำเป็นต้องแยกพิจารณาตามลักษณะของอาชญากรรมแบบไร้ตัวตนเป็นกรณี ๆ ไป

- พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 จะต้องพิจารณาบนเงื่อนไขการเข้าสู่คดีพิเศษตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 จะต้องพิจารณาตามหลักของมาตรา 21 (1) เป็นหลัก ซึ่งแม้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ. 2550 และที่แก้ไขเพิ่มเติม จะเป็นความผิดตามบัญชีท้ายก็ตาม แต่ก็จะมีข้อจำกัดในกรณีบางฐานความผิดที่ไม่ปรากฏตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

- พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 และที่แก้ไขเพิ่มเติม ไม่อาจนำมาบังคับใช้ได้กับความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งเป็นรูปแบบของอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ในการกระทำความผิดหลัก เพราะไม่ใช่ความผิดมูลฐานตามกฎหมายฟอกเงิน รวมถึงอาชญากรรมแบบไร้ตัวตนในรูปแบบความผิดตามพฤติกรรมของกระบวนการกระทำความผิดที่ไม่มีบัญญัติเป็นฐานความผิดตามกฎหมายไทย เว้นแต่การกระทำความผิดในรูปแบบอาชญากรรมแบบไร้ตัวตนที่อาจมีส่วนหนึ่งส่วนใดที่ครบองค์ประกอบความผิดตามความผิดมูลฐานทั้ง 28 มูลฐาน

- พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 ยังมีข้อจำกัดในการบังคับใช้กฎหมาย เนื่องจาก “อาชญากรรมทางเทคโนโลยี” จำกัดเฉพาะการกระทำหรือพยายามกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เพื่อฉ้อโกง กรรโชก หรือรีดเอาทรัพย์ บุคคลหนึ่งบุคคลใด หรือโดยประการที่น่าจะทำให้บุคคลอื่นเสียหาย หรือกระทำความผิดฐานฉ้อโกง กรรโชก หรือรีดเอาทรัพย์ โดยใช้ระบบคอมพิวเตอร์เป็นเครื่องมือ ไม่รวมถึงการกระทำความผิดต่อระบบหรือข้อมูลคอมพิวเตอร์ จึงทำให้มาตรการบังคับใช้กฎหมายที่จำกัดเฉพาะอาชญากรรมทางเทคโนโลยี ไม่รวมถึง

ความผิดอาญาอื่น ไม่สามารถนำมาใช้บังคับกับการกระทำความผิดในรูปแบบอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ เว้นแต่มีการกระทำที่คาบเกี่ยวกันและเข้าองค์ประกอบนิยามของอาชญากรรมทางเทคโนโลยีและต้องมีเจตนาพิเศษตามกฎหมายด้วย และไม่สามารถใช้บังคับได้กับความผิดที่ไม่ได้มีระบุไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

<u>วัตถุประสงค์ประการที่สาม</u> ศึกษาปัญหาและอุปสรรคในการบังคับใช้กฎหมายและการป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตนที่กระทำโดยองค์กรอาชญากรรมข้ามชาติในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ พบว่า

- การบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กับอาชญากรรมไร้ตัวตน โดยจำแนกวิเคราะห์ตามขั้นตอนพฤติกรรม 2 ขั้นตอนหลักพบว่า ในส่วนขั้นตอนการกระทำความผิดหลัก ฐานความผิดที่มีอยู่ปัจจุบันมีขอบเขตบังคับใช้ครอบคลุมขั้นตอนการกระทำความผิดหลักหรือความผิดที่เป็นเป้าหมายของอาชญากรรมไร้ตัวตน เช่น การส่งมัลแวร์ การโจรกรรมข้อมูล การแทรกแซงระบบการทำให้เสียหายซึ่งข้อมูล ฯลฯ ในส่วนขั้นตอนการกระทำอันเป็นการปกปิดตัวตน จำแนกเป็น 2 กลุ่มพฤติกรรมย่อย คือ การปกปิดตัวตนโดยไม่ใช้ข้อมูลระบุตัวผู้อื่น พบว่าฐานความผิดที่มีอยู่ไม่ได้กำหนดหลักการเฉพาะสำหรับพฤติกรรมเหล่านี้และสามารถนำมาบังคับใช้กับการกระทำอันเป็นการปกปิดตัวตนได้อย่างจำกัดเฉพาะในกรณีที่วิธีการหรือลักษณะการกระทำเข้าองค์ประกอบของบางฐาน และการกระทำอันเป็นการปกปิดตัวตนโดยใช้ข้อมูลส่วนบุคคลของผู้อื่นจำแนกเป็น 3 ขั้นตอนการกระทำย่อยพบว่า ฐานความผิดที่มีอยู่ไม่ได้กำหนดหลักการเฉพาะสำหรับพฤติกรรมเหล่านี้ และสามารถนำมาบังคับใช้กับการกระทำอันเป็นการปกปิดตัวตนได้อย่างจำกัดเฉพาะในกรณีที่วิธีการหรือลักษณะการกระทำเข้าองค์ประกอบของบางฐาน เช่น ขั้นตอนการได้มาซึ่งข้อมูล อาจบังคับใช้ฐานความผิดเข้าถึงโดยมิชอบ ขั้นตอนการกระทำต่อข้อมูลก่อนนำไปใช้ อาจบังคับใช้ความผิดฐานแก้ไขเปลี่ยนแปลงข้อมูล แต่ไม่มีฐานความผิดการแลกเปลี่ยน การซื้อขาย การโอนข้อมูล ฯลฯ ขั้นตอนการนำข้อมูลไปใช้อาจมีข้อจำกัดการบังคับใช้กับวิธีการนำข้อมูลระบุตัวผู้อื่นไปประกอบหรือสร้างร่องรอยทางระบบออนไลน์เพื่อปกปิดตัวตน

- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไม่มีฐานความผิดเฉพาะสำหรับอาชญากรรมไร้ตัวตนที่กระทำต่อระบบหรือข้อมูลคอมพิวเตอร์ ในกรณี 1) การได้มาซึ่งรหัสผ่านหรือมาตรการป้องกันของบุคคลอื่น 2) กระทำการใดๆ โดยทุจริต ในการใช้ ลายมือชื่ออิเล็กทรอนิกส์ รหัสผ่านหรือ สิ่งบ่งชี้หรือระบุตัวบุคคลใดๆ ของบุคคลอื่น 3) การเข้าถึงโดยมิชอบซึ่งข้อมูลระบุตัวของบุคคลอื่น โดยมี

เจตนาทำลาย แก้ไข ทำซ้ำ หรือ แลกเปลี่ยน และ 4) การฉ้อโกงทางคอมพิวเตอร์ที่อาชญากรนำข้อมูลดิจิทัลที่ระบุตัวบุคคลอื่นมาให้บุคคลอื่นเข้าใจผิดหรือปกปิดตัวตน จึงทำให้เป็นช่องว่างที่ไม่สามารถใช้มาตรการสืบสวนสอบสวนที่บัญญัติไว้ในพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 กับความผิดประเภทดังกล่าวได้

- มาตรการพิเศษตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 ยังไม่เพียงพอต่อการปราบปรามอาชญากรรมแบบไร้ตัวตนที่กระทำต่อระบบหรือข้อมูลคอมพิวเตอร์ เนื่องด้วยในกฎหมายกำหนดไว้เพียง 2 มาตรการ ได้แก่ มาตรการเข้าถึงข้อมูล (มาตรการดักฟัง) และมาตรการแฝงตัวและการจัดทำเอกสารหลักฐานที่ใช้ในการแฝงตัว ยังไม่ครบถ้วนตามมาตรฐานขั้นต่ำที่กำหนดไว้ในอนุสัญญาสหประชาชาติเพื่อต่อต้านอาชญากรรมข้ามชาติที่จัดตั้งในลักษณะองค์กร ค.ศ. 2000 อีกทั้งบทบัญญัติของมาตรการดังกล่าวยังมีปัญหาการตีความและบังคับใช้กฎหมายและโดยหลักเป็นมาตรการทางกายภาพ

- การบังคับใช้พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 จะต้องปรากฏว่าเป็นอาชญากรรมแบบไร้ตัวตนนั้นเป็นความผิดที่มีลักษณะเป็นองค์กรอาชญากรรมข้ามชาติตามนิยามและองค์ประกอบความผิดของกฎหมาย จะต้องเป็น “ความผิดร้ายแรง” ด้วย กล่าวคือ ความผิดอาญาที่กฎหมายกำหนดโทษจำคุกขั้นสูงตั้งแต่สี่ปีขึ้นไปหรือโทษสถานที่หนักกว่านั้น จึงไม่ครอบคลุมทุกฐานความผิดสำหรับอาชญากรรมไร้ตัวตนที่กระทำต่อระบบหรือข้อมูลคอมพิวเตอร์

- ปัญหาเรื่องระยะเวลาการเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ของผู้ให้บริการที่มีหน้าที่ต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 26 ประกอบกับประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564 ที่ไม่เพียงพอต่อการสืบสวนสอบสวนหาตัวผู้กระทำความผิด

- ปัญหาการขอข้อมูลจราจรคอมพิวเตอร์ที่อยู่ในต่างประเทศและการประสานความร่วมมือในการสืบสวน สอบสวน รวบรวมพยานหลักฐาน ที่จะต้องดำเนินการตามพระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. 2535 และที่แก้ไขเพิ่มเติม ซึ่งกระบวนการดังกล่าวมีขั้นตอนการประสานงานที่ต้องใช้ระยะเวลา ส่งผลให้การดำเนินคดีและการรวบรวมพยานหลักฐานทำได้ล่าช้า

- ปัญหาการดำเนินการกับทรัพย์สิน เนื่องจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไม่ได้กำหนดหมวดว่าด้วยการดำเนินการกับทรัพย์สินไว้เป็นการเฉพาะ และไม่ได้เป็นความผิดมูลฐานตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน จึงไม่สามารถนำมาตรการร้องขอให้ทรัพย์สินตกเป็นของแผ่นดินตามกฎหมายฟอกเงินซึ่งเป็นมาตรการที่มีประสิทธิภาพ เนื่องเป็นกระบวนการ

พิจารณาคดีต่อตัวทรัพย์สินโดยตรง โดยไม่ต้องคำนึงถึงความผิดของเจ้าของทรัพย์สินมาใช้บังคับกับทรัพย์สินที่เกี่ยวกับการกระทำความผิดได้

- ปัญหาขอบเขตการบังคับใช้พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 ที่ยังไม่ครอบคลุมความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ ทำให้ไม่สามารถนำมาตรการบังคับใช้กฎหมายที่จำกัดเฉพาะอาชญากรรมทางเทคโนโลยี ไม่รวมถึงความผิดอาญาอื่นมาใช้บังคับกับการกระทำความผิดในรูปแบบอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ได้ เว้นแต่มีการกระทำที่คาบเกี่ยวกันและเข้าองค์ประกอบนิยามของอาชญากรรมทางเทคโนโลยี

<u>วัตถุประสงค์ประการที่สี่</u> ศึกษาและจัดทำต้นแบบกฎหมาย (Model Law) ของประเทศไทย ในรูปแบบของการจัดทำกฎหมายต้นแบบเพื่อป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ พบว่า ตามแนวทางของต่างประเทศและกฎหมายระหว่างประเทศไม่ได้ใช้วิธีการกำหนดนิยามสากลหรือความหมายกลางของอาชญากรรมไร้ตัวตน เพราะการกระทำดังกล่าวมีลักษณะเชิงกระบวนการหลายขั้นตอน อีกทั้งอาจเกี่ยวข้องกับอาชญากรรมไซเบอร์ชนิดใดก็ได้ เนื่องจากอาจนำวิธีการปกปิดตัวตนมาประกอบหรือปกปิดการกระทำได้ แนวทางที่เหมาะสมของการพัฒนากฎหมายต้นแบบคือ การกำหนดฐานความผิดที่มีองค์ประกอบครอบคลุมการกระทำของอาชญากรรมไร้ตัวตน ซึ่งความผิดเกี่ยวกับคอมพิวเตอร์ตามกฎหมายภายในเดิมของประเทศต่างๆ อาจยังไม่ครอบคลุม โดยมีลักษณะที่สำคัญคือ มุ่งเน้นการกำหนดความผิดสำหรับพฤติกรรมการปกปิดตัวตน และนอกจากการกำหนดฐานความผิดต้นแบบแล้ว รวมถึงการกำหนดมาตรการบังคับใช้กฎหมายที่จำเป็นต่อการป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตนด้วย อาทิ มาตรการด้านการสืบสวนสอบสวนและรวบรวมพยานหลักฐาน มาตรการการดำเนินการกับทรัพย์สิน เพื่อให้ประเทศไทยมีกฎหมายมีมาตรการประสิทธิภาพ สอดคล้องตามหลักสากล ทันต่อการเปลี่ยนแปลงทางเทคโนโลยีและรูปแบบอาชญากรรมทางเทคโนโลยี รายละเอียดปรากฏตามข้อเสนอแนะ

<u>วัตถุประสงค์ประการสุดท้าย</u> เสนอแนะมาตรการความร่วมมือระหว่างประเทศเพื่อป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตนที่กระทำโดยองค์กรอาชญากรรมข้ามชาติในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ พบว่า ไม่มีสนธิสัญญาหรือร่างสนธิสัญญาที่ระบุถึงความร่วมมือในกรณีอาชญากรรมไร้ตัวตนโดยเฉพาะ แต่กรอบแนวทางระหว่างประเทศที่ใกล้เคียงและครอบคลุมถึงอาชญากรรมไร้ตัวตนคือ กรอบแนวทางความร่วมมือป้องกันและปราบปรามอาชญากรรมไซเบอร์ตามกรอบของอนุสัญญาอาชญากรรมไซเบอร์สหภาพยุโรป หรืออนุสัญญาบูดาเปสท์ (the Council of Europe Convention on Cybercrime or The Budapest

Convention) และร่างสนธิสัญญาสหประชาชาติว่าด้วยอาชญากรรมเทคโนโลยี (Draft of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes) โดยผลการวิเคราะห์เปรียบเทียบชี้ให้เห็นประเด็นหรือมาตรการย่อยที่เจาะจงถึงสภาพและลักษณะของอาชญากรรมไซเบอร์โดยเฉพาะอย่างยิ่งความร่วมมือด้านการสืบสวนสอบสวนและรวบรวมพยานหลักฐานทางดิจิทัลหรืออิเล็กทรอนิกส์ สำหรับประเทศไทยไม่ได้เข้าร่วมเป็นภาคีในกรอบกฎหมายระหว่างประเทศที่เกี่ยวข้องกับอาชญากรรมไร้ตัวตนและอาชญากรรมไซเบอร์ กล่าวคือ ในส่วนของอนุสัญญาอาชญากรรมไซเบอร์ของสหภาพยุโรปนั้น ไทยไม่ได้เป็นภาคีและไม่ได้ให้สัตยาบัน สำหรับร่างสนธิสัญญาสหประชาชาติว่าด้วยอาชญากรรมเทคโนโลยี ในส่วนของประเทศไทยไม่ปรากฏการเป็นผู้แทนหรือคณะทำงาน (Ad hoc committee) ในการร่างสนธิสัญญานี้ จึงกล่าวได้ว่าในทางกฎหมายระหว่างประเทศไทยไม่มีพันธกรณีความร่วมมือตามสนธิสัญญาดังกล่าว เมื่อเปรียบเทียบกับความร่วมมือในทางอาญาระหว่างประเทศ (MLAT) ซึ่งเป็นหลักการและแนวปฏิบัติของความตกลงระดับทวิภาคีที่พบในหลายประเทศ จะพบว่า MLAT แม้จะมีหลักความร่วมมือเกี่ยวกับการสืบสวนสอบสวนและได้มาซึ่งพยานหลักฐาน แต่ไม่ได้มีหลักการเฉพาะสำหรับความร่วมมือด้านต่าง ๆ เพื่อป้องกันและปราบปรามอาชญากรรมไซเบอร์และอาชญากรรมไร้ตัวตน

2. ข้อเสนอแนะ

จากผลการศึกษาวิจัย ผู้วิจัยมีข้อเสนอแนะเกี่ยวกับการจัดทำต้นแบบกฎหมายเพื่อป้องกันและปราบปรามอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ โดยมีสาระสำคัญเกี่ยวกับการกำหนดฐานความผิดของอาชญากรรมแบบไร้ตัวตน การกำหนดมาตรการสืบสวนสอบสวน การดำเนินการกับทรัพย์สินที่เกี่ยวกับการกระทำความผิด มาตรการด้านพยานหลักฐาน และมาตรการความร่วมมือระหว่างประเทศ ดังนี้

2.1 การกำหนดฐานความผิด

จากการศึกษาแนวทางระหว่างประเทศ ประกอบกับการวิเคราะห์จำแนกขั้นตอนกระบวนการของอาชญากรรมไร้ตัวตนพบว่า พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 สามารถครอบคลุมการกระทำหลักของอาชญากรรมไร้ตัวตนซึ่งอาจเข้าข่ายความผิดต่าง ๆ เช่น การเข้าถึงข้อมูลหรือระบบ การส่งมัลแวร์ การทำลายข้อมูล แต่ยังมีปัญหาขอบเขตฐานความผิดสำหรับการกระทำในส่วนปกปิด

ตัวตนที่ไม่ได้มีองค์ประกอบเฉพาะเจาะจงสำหรับอาชญากรรมประเภทนี้ ดังนั้น แนวทางที่เหมาะสมของการพัฒนากฎหมายต้นแบบคือการกำหนดฐานความผิดที่มีองค์ประกอบครอบคลุมการกระทำของอาชญากรรม แบบไร้ตัวตน ซึ่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 อาจยังไม่ครอบคลุม โดยมุ่งเน้นการกำหนดฐานความผิดสำหรับพฤติกรรมการปกปิดตัวตน

เสนอแนะให้แก้ไขเพิ่มเติมพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กำหนดฐานความผิดเฉพาะสำหรับอาชญากรรมซึ่งใช้วิธีปกปิดตัวตน และฐานความผิดเฉพาะสำหรับการฉ้อโกงทางคอมพิวเตอร์โดยการใช้ข้อมูลดิจิทัลที่ระบุตัวบุคคลอื่น ดังนี้

1) ฐานความผิดการได้มาซึ่งรหัสผ่านหรือมาตรการป้องกันของบุคคลอื่น (Illegal obtaining or receiving of passwords) สำหรับการกระทำโดยเจตนาด้วยประการใดๆ ในการได้มาหรือได้รับซึ่งรหัสผ่านหรือมาตรการป้องกันการเข้าถึงใดๆ ของระบบคอมพิวเตอร์ของผู้อื่น

โดยเสนอร่างต้นแบบกฎหมายดังนี้

“ผู้ใดกระทำด้วยประการใดเพื่อให้ได้มาหรือได้รับซึ่งรหัสผ่านหรือมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ของผู้อื่น ต้องระวางโทษ ...”

เป็นการกำหนดความผิดสำหรับขั้นตอนการกระทำเพื่อปกปิดตัวตน โดยองค์ประกอบครอบคลุมการกระทำใดๆ เพื่อได้มาหรือได้รับ (Obtain or receive) ซึ่งรหัสผ่านหรือมาตรการป้องกันการเข้าถึง ซึ่งอาจเป็นข้อมูลระบุตัวใดๆ ของผู้อื่น ซึ่งเมื่อได้มาแล้วอาจนำไปใช้ประกอบอาชญากรรมต่อระบบหรือความปลอดภัยทางคอมพิวเตอร์ประเภทใดก็ได้ โดยมุ่งประสงค์ควบคุมพฤติกรรมนี้โดยกำหนดเป็นฐานความผิดเฉพาะและสามารถเข้าองค์ประกอบเป็นความผิดสำเร็จในตัวเอง แม้ยังไม่ปรากฏว่ามีการใช้รหัสผ่านนั้นเข้าถึงคอมพิวเตอร์หรืออุปกรณ์เพื่อนำไปกระทำความผิดหลักใดก็ตาม

2) ฐานความผิดการปลอมตัวเป็นบุคคลอื่น (Impersonation) สำหรับการกระทำ โดยทุจริตกระทำการใดๆ ในการใช้ลายมือชื่ออิเล็กทรอนิกส์ รหัสผ่าน หรือสิ่งบ่งชี้หรือระบุตัวบุคคลใด ๆ ของบุคคลอื่น

โดยเสนอร่างต้นแบบกฎหมายดังนี้

“ผู้ใดกระทำด้วยประการใดเพื่อให้ได้มาหรือได้รับซึ่งลายมือชื่ออิเล็กทรอนิกส์ รหัสผ่าน หรือมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ของผู้อื่น ต้องระวางโทษ ...”

เป็นการกำหนดความผิดสำหรับขั้นตอนที่คาบเกี่ยวหรือทับซ้อนระหว่างการกระทำเพื่อปกปิดตัวตน และการกระทำความผิดหลัก สำหรับในส่วนของการกระทำความผิดหลักนั้นหากปรากฏว่ามีส่วนของวิธีการ

ที่อาชญากรใช้ข้อมูลระบุตัวบุคคลอื่นในการกระทำก็จะเข้าองค์ประกอบนี้ ซึ่งเป็นฐานความผิดเฉพาะแยกต่างหากจากฐานความผิดหลักอื่น นอกจากนี้ ฐานความผิดดังกล่าวอาจเป็นความผิดสำเร็จในตัวเอง แม้ว่าการกระทำหลักหรือการกระทำอันเป็นเป้าหมายไม่เข้าองค์ประกอบความผิดอาญาเกี่ยวกับอาชญากรรมไซเบอร์ฐานใดโดยเฉพาะ เนื่องจากการกระทำครบองค์ประกอบเมื่อใช้ลายมือชื่ออิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ แม้ว่าจะไม่ได้ใช้ในการฉ้อโกงทางคอมพิวเตอร์หรืออาชญากรรมไซเบอร์ฐานอื่นก็ตาม

3) ฐานความผิดการเข้าถึงข้อมูลระบุตัวบุคคลอื่นโดยมิชอบ (Unauthorized access to personal data) สำหรับการกระทำการเข้าถึงโดยมิชอบซึ่งข้อมูลระบุตัวของบุคคลอื่น โดยมีเจตนาทำลาย แก้ไข ทำซ้ำ หรือ แลกเปลี่ยน

โดยเสนอร่างต้นแบบกฎหมายดังนี้

“ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลส่วนบุคคลของผู้อื่น โดยมีเจตนาทำให้เสียหาย ทำลาย ทำซ้ำแก้ไข แลกเปลี่ยน เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ต้องระวางโทษ ...”

เป็นการกำหนดความผิดสำหรับขั้นตอนที่การกระทำเพื่อปกปิดตัวตน ซึ่งอาชญากรเข้าถึงข้อมูลระบุตัวของเหยื่อและอาจทำการแก้ไขหรือแลกเปลี่ยนกับข้อมูลอื่นจากนั้นนำไปใช้สร้างร่องรอยการประกอบอาชญากรรมใดๆ ซึ่งเป็นการกระทำความผิดหลักทั้งนี้เพื่อให้เจ้าหน้าที่บังคับใช้กฎหมายเข้าใจว่าเป็นการกระทำของเหยื่อ ฐานความผิดดังกล่าวอาจเป็นความผิดสำเร็จในตัวเอง แม้ว่าการกระทำหลักหรือการกระทำอันเป็นเป้าหมายไม่เข้าองค์ประกอบความผิดอาญาเกี่ยวกับอาชญากรรมไซเบอร์ฐานใดโดยเฉพาะ เนื่องจากการกระทำครบองค์ประกอบเมื่อมีการเข้าถึงและแก้ไขเปลี่ยนแปลงข้อมูลระบุตัวผู้อื่น แม้ว่าจะไม่ได้ใช้ในการฉ้อโกงทางคอมพิวเตอร์หรืออาชญากรรมไซเบอร์ฐานอื่นก็ตาม

4) ฐานความผิดเฉพาะสำหรับการฉ้อโกงทางคอมพิวเตอร์ โดยการใช้ข้อมูลดิจิทัลที่ระบุตัวบุคคลอื่นหรือใช้ข้อมูลใด ๆ หลายอย่างประกอบกันที่สามารถบ่งระบุตัวบุคคลอื่น ในการกระทำการให้บุคคลอื่นเข้าใจผิด เพื่อให้ได้มาซึ่งประโยชน์ (Gain)

โดยเสนอร่างต้นแบบกฎหมายดังนี้

“ผู้ใดโดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลส่วนบุคคลของผู้อื่นโดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน ต้องระวางโทษ ...”

เป็นการกำหนดฐานความผิดที่ไม่ได้มุ่งเน้นการหลอกลวงให้เข้าใจผิดในเนื้อหา (Content) หรือเรื่องราวการหลอกลวง แต่กำหนดองค์ประกอบความผิดสำหรับการหลอกลวงให้เข้าใจผิดโดยใช้ข้อมูลบุคคลอื่นซึ่ง

เป็นการปกปิดการกระทำเพื่อให้อาชญากรที่ทำการฉ้อโกงนั้นมีลักษณะไร้ตัวตน ทั้งนี้ไม่ว่าเนื้อหาจะเป็นการหลอกลวงในเรื่องราวใดก็อยู่ภายใต้ฐานความผิดนี้ เช่น การหลอกลวงให้ลงทุน การหลอกลวงเชิงความสัมพันธ์ การหลอกลวงการทำงานหรือการประกอบธุรกิจออนไลน์ ฯลฯ เป็นการขยายฐานความผิดเพิ่มเติมจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่มีข้อจำกัดคือองค์ประกอบมุ่งเน้นเนื้อหาการหลอกลวง (content) มิได้กำหนดองค์ประกอบเจาะจงถึงการใช้ข้อมูลระบุตัวผู้อื่นมาประกอบการหลอกลวงเพื่อปกปิดตัวตนของอาชญากร

2.2 มาตรการสืบสวนสอบสวน

เห็นควรกำหนดมาตรการสืบสวนสอบสวนเพิ่มเติม ดังนี้

1) มาตรการสั่งให้ผู้ให้บริการส่งมอบข้อมูลจราจรคอมพิวเตอร์ที่จัดเก็บไว้ในต่างประเทศ

เป็นมาตรการเพื่อความจำเป็นในการสืบสวนสอบสวน เนื่องจากข้อมูลอันเป็นพยานหลักฐานของอาชญากรรมแบบไร้ตัวตนปัจจุบันอาจอยู่ในเซิร์ฟเวอร์ที่ตั้งอยู่ในหลายประเทศ รวมทั้งระบบคลาวด์ที่ข้อมูลมีลักษณะกระจายและไม่รวมศูนย์ ดังนั้น จึงควรบัญญัติให้อำนาจพนักงานเจ้าหน้าที่ร้องขอข้อมูลจากผู้ให้บริการเอกชน โดยขยายขอบเขตให้ชัดเจนไปถึงข้อมูลของผู้ให้บริการที่จัดเก็บในต่างประเทศด้วย เป็นหลักการที่กำหนดหน้าที่ผู้ให้บริการ

เสนอให้แก้ไขเพิ่มเติมพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 18 (3) ดังนี้

มาตรา 18 ภายใต้บังคับมาตรา 19 เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ หรือในกรณีที่มีการร้องขอตามวรรคสองให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด ...

(3) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา 26 หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการ *<u>รวมถึงข้อมูลที่จัดเก็บในต่างประเทศ</u>* ให้แก่พนักงานเจ้าหน้าที่หรือให้เก็บข้อมูลดังกล่าวไว้ก่อน”

2) มาตรการสะกดรอยโดยใช้เครื่องมืออิเล็กทรอนิกส์ (Electronic Surveillance)

มาตรการสะกดรอยโดยใช้เครื่องมืออิเล็กทรอนิกส์ (Electronic Surveillance) เป็นมาตรการเพื่อประโยชน์ในการสืบสวน สอบสวนและรวบรวมพยานหลักฐานในคดี ดำเนินการโดยใช้เครื่องมือทั้งทางกายภาพและอุปกรณ์อิเล็กทรอนิกส์ เพื่อสะกดรอย ติดตามการกระทำความผิด ซึ่งเป็นวิธีการที่จำเป็นสำหรับการสืบสวนเพื่อให้ได้มาซึ่งพยานหลักฐานในคดีที่กลุ่มผู้กระทำความผิดที่มีบุคลากรที่เชี่ยวชาญในเรื่องการเฝ้าระวังเป็นอย่างสูง ตัวอย่าง มาตรการสะกดรอยโดยใช้เครื่องมืออิเล็กทรอนิกส์ อาทิ การเฝ้าตรวจตราทางเสียงหรือการดักฟัง (Audio Surveillance) การเฝ้าตรวจตราทางภาพ (Visual Surveillance) การใช้เครื่องมือเฝ้าติดตาม (Tracking Surveillance) การเฝ้าตรวจตราทางข้อมูล (Data Surveillance) โดยใช้คอมพิวเตอร์/อินเตอร์เน็ต (Computer/Internet)

เสนอให้เพิ่มเติมมาตรการดังกล่าวไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กำหนดให้

“พนักงานเจ้าหน้าที่อาจใช้เครื่องมือสื่อสารโทรคมนาคม เครื่องมืออิเล็กทรอนิกส์ หรือด้วยวิธีการอื่นใดเฉพาะในการสะกดรอยผู้ต้องสงสัยว่ากระทำความผิดหรือจะกระทำความผิด เพื่อสืบสวน จับกุม แสวงหาและรวบรวมพยานหลักฐาน ดำเนินคดีและเพื่อประโยชน์ในการขยายผลการจับกุมผู้อยู่เบื้องหลังการกระทำความผิด ทั้งนี้ ตามหลักเกณฑ์ วิธีการและเงื่อนไขที่กำหนดในกฎกระทรวง”

มาตรการดังกล่าวมีหลักการเช่นเดียวกับพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 มาตรา 21 ที่ให้อำนาจพนักงานสอบสวนหรือพนักงานเจ้าหน้าที่อาจใช้เครื่องมือสื่อสารโทรคมนาคม เครื่องมืออิเล็กทรอนิกส์ หรือด้วยวิธีการอื่นใด เฉพาะในการสะกดรอยผู้ต้องสงสัยว่ากระทำความผิดหรือจะกระทำความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ เพื่อสืบสวน จับกุม แสวงหาและรวบรวมพยานหลักฐาน

3) มาตรการอำพราง (Undercover)

มาตรการอำพราง (Undercover Operation)[146] เป็นปฏิบัติการลับที่เป็นเครื่องมือสืบสวนพิเศษเป็นการแทรกซึมเข้าไปในเครือข่ายองค์กรอาชญากรรม หรือการดำเนินการทั้งหลายเพื่อปิดบังสถานะหรือ

[146] the United Nations Office on Drugs and Crime (UNODC) , Undercover operations , Organized Crime Module 8 Key Issues: Special Investigative Techniques - Undercover Operations (unodc.org)

วัตถุประสงค์ของการดำเนินการโดยลวงผู้อื่นให้เข้าใจไปในทางอื่น หรือเพื่อมิให้รู้ความจริงเกี่ยวกับการสืบสวนหรือการสอบสวน และมีการควบคุมการปฏิบัติการในช่วงระยะเวลาที่กำหนดไว้ โดยการนำมาตรการอำพรางมาใช้กับในการปราบปรามอาชญากรรมแบบไร้ตัวตน จำเป็นต้องเปิดช่องของกฎหมายในการใช้การอำพรางด้วยวิธีทางอิเล็กทรอนิกส์มากกว่าการวิธีทางกายภาพตามที่ปรากฏในกฎหมายอื่น ไม่ว่าจะเป็นพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 หรือพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556

เสนอให้เพิ่มเติมมาตรการดังกล่าวไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กำหนดให้

“ในกรณีจำเป็นและเพื่อประโยชน์ในการดำเนินการตามพระราชบัญญัตินี้ พนักงานเจ้าหน้าที่ผู้ได้รับอนุญาตเป็นหนังสือจากรัฐมนตรีหรือผู้ซึ่งได้รับมอบหมาย มีอำนาจให้บุคคลใดจัดทำเอกสารหรือหลักฐานใดขึ้น หรือปฏิบัติการอำพราง เพื่อประโยชน์ในการสืบสวนสอบสวน การรวบรวมพยานหลักฐานและการขยายผลการจับกุมผู้กระทำความผิด ทั้งนี้ ให้เป็นไปตามหลักเกณฑ์ วิธีการและเงื่อนไขที่กำหนดในกฎกระทรวง

การปฏิบัติการอำพราง หมายความว่า การดำเนินการทั้งหลายเพื่อปิดบังสถานะหรือวัตถุประสงค์ของการดำเนินการโดยลวงผู้อื่นให้เข้าใจไปในทางอื่น หรือเพื่อมิให้รู้ความจริงเกี่ยวกับการปฏิบัติหน้าที่ของพนักงานเจ้าหน้าที่ รวมถึงการดำเนินการใด ๆ ด้วยวิธีทางอิเล็กทรอนิกส์ด้วย

การจัดทำเอกสารหรือหลักฐานใด หรือการปฏิบัติการอำพรางตามวรรคหนึ่ง ให้ถือว่าเป็นการกระทำโดยชอบด้วยกฎหมาย”

4) มาตรการเข้าถึงข้อมูลทางการเงิน

มาตรการการเข้าถึงข้อมูลทางการเงิน เป็นมาตรการที่มีประโยชน์ต่อการติดตามและวิเคราะห์เส้นทางการเงิน โดยกำหนดให้พนักงานเจ้าหน้าที่มีอำนาจในการขอข้อมูลทางบัญชีหรือการทำธุรกรรมของสถาบันการเงินได้ เพื่อประสิทธิภาพในการพิสูจน์เส้นทางการเงินที่เกี่ยวข้องกับการกระทำความผิด

เสนอให้เพิ่มเติมมาตรการดังกล่าวไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กำหนดให้

“ในการดำเนินการสืบสวนสอบสวนตามพระราชบัญญัตินี้ หากมีพยานหลักฐานตามสมควรว่าบัญชีลูกค้าของสถาบันการเงิน หรือข้อมูลทางการเงินใด ถูกใช้ อาจถูกใช้ มีความเกี่ยวพันเชื่อมโยงกับการกระทำ

ความผิด หรือเป็นประโยชน์ต่อการวิเคราะห์เพื่อติดตามร่องรอยทางการเงิน ให้พนักงานเจ้าหน้าที่มีคำขอเป็นหนังสือไปยังสำนักงานป้องกันและปราบปรามการฟอกเงินเพื่อขอข้อมูลดังกล่าว”

2.3 การดำเนินการกับทรัพย์สินที่เกี่ยวกับการกระทำความผิด

เสนอแนะให้แก้ไขเพิ่มเติมมาตรา 3 แห่งพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 กำหนดให้ความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์เป็นความผิดมูลฐานตามกฎหมายฟอกเงิน ซึ่งเป็นข้อเสนอแนะที่เชื่อมโยงมาจากการข้อเสนอแนะให้เพิ่มฐานความผิดเกี่ยวกับอาชญากรรมแบบไร้ตัวตนตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ประกอบกับแนวคำวินิจฉัยศาลรัฐธรรมนูญ ที่ 8/2564 ที่ว่าในการกำหนดให้ความผิดมูลฐานตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน รัฐควรบัญญัติให้เป็น “ความผิดมูลฐาน” ไว้ในพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มาตรา 3 อันเป็นกฎหมายหลักสำหรับการดำเนินการเกี่ยวกับการป้องกันและปราบปรามการฟอกเงินซึ่งเป็นมาตรการทางกฎหมายที่มีความพิเศษโดยเฉพาะ โดยมีพนักงานเจ้าหน้าที่ที่มีความเชี่ยวชาญเฉพาะ มีกระบวนการขั้นตอนในการตรวจสอบถ่วงดุลการใช้อำนาจแต่ละฝ่าย เพื่อให้การบังคับใช้กฎหมายมีความชัดเจน เป็นระบบ ไม่ซ้ำซ้อน อันเป็นหลักการพื้นฐานในการตรากฎหมายและหลักความจำเป็นในการตรากฎหมายขึ้นใช้บังคับ โดยกำหนดลักษณะของความผิดมูลฐานเฉพาะรูปแบบของอาชญากรรมแบบไร้ตัวตนในความผิดที่กระทบต่อระบบหรือข้อมูลคอมพิวเตอร์ในการกระทำความผิดหลักและอาชญากรรมแบบไร้ตัวตนในรูปแบบความผิดตามพฤติกรรมของกระบวนการกระทำความผิดเพื่อปกปิดตัวตนที่กระทำไปเพื่อให้ได้ประโยชน์ซึ่งทรัพย์สิน ซึ่งเป็นหลักการสำคัญในการกำหนดความผิดมูลฐานของประเทศไทย เพื่อให้สำนักงานป้องกันและปราบปรามการฟอกเงินสามารถดำเนินการกับทรัพย์สินที่เกี่ยวกับการกระทำความผิดในความผิดประเภทนี้ได้ โดยนำหลักการของมาตรการริบทรัพย์ทางแพ่งหรือ กระบวนการฟ้องร้องเพื่อริบทรัพย์ทางแพ่งต่อตัวทรัพย์สินที่ไม่ผูกติดกับคดีอาญามาใช้ โดยอาศัยเหตุและหลักฐานอันควรเชื่อได้ว่าเป็นทรัพย์สินที่เกี่ยวกับการกระทำความผิด เพื่อให้สามารถดำเนินการตัดวงจรของอาชญากรรมดังกล่าวได้ รวมทั้งการใช้มาตรการทางอาญาในการดำเนินคดีกับผู้กระทำความผิดในข้อหาฟอกเงิน

2.4 มาตรการด้านพยานหลักฐาน

เสนอแนะให้มีการผลักดันกฎหมายพยานหลักฐานดิจิทัลเป็นกฎหมายกลางที่อาจทำได้ในรูปแบบการกำหนดเป็นพระราชบัญญัติเฉพาะ หรือการแก้ไขเพิ่มเติมกฎหมายวิธีพิจารณาความอาญา เนื่องจากกฎหมายพยานหลักฐานดิจิทัลเป็นกฎหมายวิธีสบัญญัติที่ใช้กับคดีทุกประเภท จึงไม่สามารถกำหนดเรื่องดังกล่าวไว้ใน

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้ ทั้งนี้ กฎหมายพยานหลักฐานดิจิทัลควรกำหนดรายละเอียดเกี่ยวกับประเภทของพยานหลักฐานดิจิทัล หลักเกณฑ์ในการแบ่งประเภทพยานหลักฐานดิจิทัล หลักการนำสืบและการรับฟังพยานหลักฐานดิจิทัล หลักการชั่งน้ำหนักพยานหลักฐานดิจิทัล รวมทั้งกระบวนการตรวจพิสูจน์และรับรองพยานหลักฐานดิจิทัล เนื่องจากพยานหลักฐานดิจิทัลมีลักษณะเฉพาะคือสามารถถูกเปลี่ยนแปลงแก้ไขได้ง่ายและการแก้ไขนั้นอาจไม่เหลือร่องรอยให้ตรวจสอบในภายหลัง จึงจำเป็นต้องมีกระบวนการตรวจพิสูจน์และรับรองน้ำหนักหรือความน่าเชื่อถือของพยานหลักฐาน เพื่อให้พยานหลักฐานดิจิทัลคงไว้ซึ่งความน่าเชื่อถือและสามารถรับฟังได้

2.5 ความร่วมมือระหว่างประเทศ

เสนอแนะให้นำกรอบแนวทางระหว่างประเทศตามร่างสนธิสัญญาสหประชาชาติว่าด้วยอาชญากรรมเทคโนโลยี (Draft of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes) และอนุสัญญาอาชญากรรมไซเบอร์ (The Convention on Cybercrime of the Council of Europe) มาใช้เป็นแนวทางในการดำเนินการเชิงนโยบายหลายมิติ อาทิ

- การปรับปรุงพัฒนาและประยุกต์ใช้หลักความร่วมมือทางอาญาตามกรอบระหว่างประเทศ ในการเจรจาสนธิสัญญาความร่วมมือสืบสวนสอบสวนอาชญากรรมไร้ตัวตนทางคอมพิวเตอร์ ในระดับทวิภาคีกับประเทศต่างๆ (Bilateral treaty)

- การปรับปรุงพัฒนาและและร่างกฎหมายไทยให้สอดคล้องและรองรับกับความร่วมมือตามกฎหมายระหว่างประเทศดังกล่าวหากไทยจะเข้าร่วมเป็นภาคีหรือให้สัตยาบันต่อไป

- การปรับปรุงพัฒนาและร่างกฎหมายเกี่ยวกับอาชญากรรมไร้ตัวตน ซึ่งแบ่งเป็นหลายหมวด เช่น หมวดฐานความผิด (Model offence) สำหรับ หมวดความร่วมมือระหว่างประเทศ เสนอแนะให้นำมีการนำแนวทางรูปแบบของกฎหมายสหรัฐอเมริกา (CLOUD Act) มาใช้เป็นต้นแบบในการร่างกฎหมายภายในให้รัฐดำเนินการเจรจาทำสัญญาทวิภาคีกับประเทศอื่นเพื่อกำหนดความร่วมมือป้องกันปราบปรามอาชญากรรมไร้ตัวตน โดยในส่วนเนื้อหารายละเอียดมาตรการความร่วมมือนั้นเสนอให้นำหลักการและกรอบความร่วมมือระหว่างประเทศของสหประชาชาติมาเป็นตัวแบบในการเจรจาความร่วมมือแต่ละกรณี

บรรณานุกรม

ภาษาไทย

ไพฑูรย์ ขัมภรัตน์ . “กรมสอบสวนคดีพิเศษกับการแก้ไขความบกพร่องของพยานหลักฐานในคดีอาญา”. มติชน . 24 กรกฎาคม 2545 .

คณาธิป ทองรวีวงศ์ . มาตรการทางกฎหมายเกี่ยวกับการโจรกรรมข้อมูลส่วนบุคคลทางระบบคอมพิวเตอร์ : ศึกษาเปรียบเทียบกฎหมายไทยกับกฎหมายสหรัฐอเมริกา, รายงานสืบเนื่อง การประชุมวิชาการระดับชาติการวิจัยประยุกต์ “มิติใหม่ของโลกภายหลังจากการแพร่ระบาดของเชื้อไวรัส โคโรนา 2019 : ความท้าทายและโอกาส" ครั้งที่ 5” มหาวิทยาลัยนอร์ทกรุงเทพ, 2566.

คณาธิป ทองรวีวงศ์ . มาตรการทางกฎหมายอาญาในการป้องกันและปราบปรามการโจรกรรมข้อมูลเชิงเอกลักษณ์ . วารสารวิชาการเซาธ์อีสท์บางกอก . 1, 1 ม.ค.-มิ.ย. 2558 : 56-75.

คณาธิป ทองรวีวงศ์. ความผิดเกี่ยวกับคอมพิวเตอร์ เล่ม 1 : ความผิดต่อความปลอดภัยของระบบและข้อมูลคอมพิวเตอร์ . กรุงเทพ : สำนักพิมพ์นิติธรรม . พิมพ์ครั้งที่ 2 , 2565.

คณาธิป ทองรวีวงศ์ . กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ เล่ม 2 : ภาคการฉ้อโกงทางคอมพิวเตอร์ สแปมและความผิดอื่น . กรุงเทพ : สำนักพิมพ์นิติธรรม, 2564.

คณาธิป ทองรวีวงศ์และชลธิชา สมสอาด . การปรับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แก้ไขเพิ่มเติม พ.ศ. 2560 กับการหลอกลวงเกี่ยวกับความสัมพันธ์เชิงความรักที่กระทำทางระบบคอมพิวเตอร์ . วารสารรัชต์ภาคย์ (สาขามนุษยศาสตร์และสังคมศาสตร์) ,ปีที่ 15 ฉบับที่ 39 มีนาคม – เมษายน 2564 , หน้า 230-239.

คณาธิป ทองรวีวงศ์. “ปัญหาทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลการโจรกรรมเอกลักษณ์”. รายงานสืบเนื่อง การประชุมวิชาการระดับชาติ SMARTS ครั้งที่ 5 . กรุงเทพมหานคร : มหาวิทยาลัยศรีนครินทรวิโรฒ, 2558.

คณาธิป ทองรวีวงศ์ . การคุ้มครองสิทธิมนุษยชนจากมาตรการความร่วมมือระหว่างประเทศเพื่อการป้องกันแปราบปรามอาชญากรรมไซเบอร์ : ศึกษากรณีมาตรการเข้าถึงข้อมูลส่วนบุคคลในกรอบการเจราจาสนธิสัญญาของสหประชาชาติ . รายงานสืบเนื่อง การประชุมหาดใหญ่วิชาการระดับชาติและนานาชาติ ครั้งที่ 14 มหาวิทยาลัยหาดใหญ่

คณาธิป ทองรวีวงศ์ . การปรับปรุงพัฒนาพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ตามแนวทางองค์การสหประชาชาติ ในกรณีความผิดฐานโจรกรรมข้อมูลส่วนบุคคล , รายงานสืบเนื่อง การประชุมวิชาการระดับชาติ "การจัดการเทคโนโลยีและนวัตกรรม" (The National Conference on Technology and Innovation Management , NCTIM 2023) , 2566.

จุฑาทิพ คล้ายทับทิม . หลักความสัมพันธ์ระหว่างประเทศ . พิมพ์ครั้งที่ 4 . กรุงเทพมหานคร: สำนักพิมพ์มหาวิทยาลัยเกษตรศาสตร์, 2559.

ชญานิศ ทรัพย์มา . มาตรการทางกฎหมายในการป้องกันและปราบปรามอาชญากรรมข้ามชาติทางด้านสิ่งแวดล้อม: กรณีศึกษาการลักลอบค้าสารทำลายชั้นโอโซน. สารานิพนธ์นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ สถาบันบัณฑิตพัฒนบริหารศาสตร์, กรุงเทพฯ, 2556.

ชิตพล กาญจนกิจ . ความท้าทายของรัฐอาเซียนในการต่อต้านอาชญากรรมข้ามชาติ. วารสารสังคมศาสตร์ ปีที่ 46 ฉบับที่ 1 . 2559 . http://www.library.polsci.chula.ac.th/journal.

ญาดา รัตนอารักขาและศุภชัย คำคุ้ม . คำอธิบายกฎหมายว่าด้วยการสอบสวนคดีพิเศษและกรมสอบสวนคดีพิเศษ (DSI) . กรุงเทพมหานคร : กรุงสยาม พับลิชชิ่ง, 2556.

วีระพงษ์ บุญโญภาส และสุพัตรา แผนวิชิต . รายงานวิจัยฉบับสมบูรณ์เรื่องการติดตามเส้นทางการเงินของขบวนการค้าผู้หญิงและเด็กในอนุภูมิภาคลุ่มแม่น้ำโขง . สถาบันเพื่อการยุติธรรมแห่งประเทศไทย (TIJ) , 2558.

สภานิติบัญญัติแห่งชาติ . สรุปสาระสำคัญของ*แก้ไข*เพิ่มเติม*พระราชบัญญัติความร่วมมือ*ระหว่างประเทศในเรื่องทางอาญา. พ.ศ. ... , http://www.senate.go.th/document/manual/499.pdf.

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) . ข้อเสนอแนะมาตรฐาน การจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐาน. Feedback-Device-Management-standard-in-digital-forensic-evidence.pdf (etda.or.th)

สุพัตรา แผนวิชิต . หน่วยที่ 12 เรื่อง การฟอกเงิน ในเอกสารประกอบการสอนชุดวิชา 41719 กฎหมายกระบวนการยุติธรรมเกี่ยวกับการควบคุมและปราบปรามอาชญากรรมในประเทศและข้ามชาติที่สำคัญ , นนทบุรี : สาขาวิชานิติศาสตร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2562.

สุพัตรา แผนวิชิต . “กฎหมายวิธีพิจารณาคดีอาชญากรรมทางเศรษฐกิจและการเงินต้นแบบ”. วิทยานิพนธ์หลักสูตรนิติศาสตรดุษฎีบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยศรีปทุม , 2559.

สุพัตรา แผนวิชิต . โครงการศึกษาวิเคราะห์และกำหนดแนวทางแก้ไขเพิ่มเติมมาตรการพิเศษตามกฎหมายว่าด้วยการสอบสวนคดีพิเศษ . กรุงเทพมหานคร : มหาวิทยาลัยสุโขทัยธรรมาธิราช , 2564.

สุพัตรา แผนวิชิต . โครงการศึกษาและพัฒนากฎหมายว่าด้วยการสอบสวนคดีพิเศษ . กรุงเทพมหานคร : กรมสอบสวนคดีพิเศษ , 2565.

ภาษาอังกฤษ

Anthony Reyes, Kevin O'Shea, Jim Steele, Jon R. Hansen, Benjamin R. Jean, and Thomas Ralph, Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement and Prosecutors . Elsevier, 2007.

Azeez Nureni Ayofe and Osunade Oluwaseyifunmitan . “Approach To Solving Cybercrime And Cybersecurity,” International Journal of Computer Science and Information Security 3,1 (2009) : 1-11.

Bloomberg News. Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom. Bloomberg News [Online], 13 May 2021 Available from: https://www.bloomberg.com/news/articles/2021-05-13/

Carol Meyers, Sara Powers, and Daniel Faissol, Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches . Lawrence Livermore National Laboratory, 2009.

Chat Le Nguyen, Wilfred Golman. Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries . Computer Law & Security Review . Volume 40, 2021.

Cybersecurity and Infrastructure Security Agency, Alert (AA20-302A) : Ransomware Activity Targeting the Healthcare and Public Health Sector (20 November 2020)

David Kravets, Feds Crack Encrypted Drives, Arrest Child Porn Suspect, Weird, 14 August 2013, https://www.wired.com/2013/08/feds-crack-encrypted-drives/

David L. Carter. “Computer Crime Categories: How Techno-Criminals Operate,” FBI Law Enforcement Bulletin 64,7 (1995) : 21-26.

David Wall . “The Internet as a Conduit for Criminals” . in Information Technology and the Criminal Justice System, ed. April Pattavina .Thousand Oaks, CA: Sage, 2005.

Deborah Russell and G.T. Gangemi . Computer Security Basics . California: O'Reilly & Associates Inc., 1991.

DiSanto, P. F. Blurred lines of identity crimes: Intersection of the first amendment and federal identity fraud. Columbia Law Review., 115, 2015.

Dorothy E. Denning & William E. Baugh Jr . HIDING CRIMES IN CYBERSPACE . Information, Communication & Society, 2:3, 251-276, 1995, DOI: 10.1080/136911899359583

Ed Tiley. Personal Computer Security . California: IDG Books Worldwide, Inc., 1996 .

Eileen Kowalski, Dawn Cappelli, and Andrew Moore. Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector Pittsburgh . Pittsburgh: Carnegie Mellon. Software Engineering Institute, 2008 .

Federal Trade Commission. Consumer Fraud and Identity Theft Complain Data : January – December 2005. (Federal Trade Commission, 2006.

Fu, X., Ling, Z., Yu, W., & Luo, J. (2010, June) . Cyber Crime Scene Investigations (C²SI) through Cloud Computing. In 2010 IEEE 30th International Conference on Distributed Computing Systems Workshops (pp. 26-31). IEEE.

Grabosky, P. N. and Smith, R. G. . Crime in the Digital Age : Controlling Telecommunications and Cyberspace Illegalities, Transaction Publishers, 1998.

Graeme R. Newman and Megan M. McNally. "Identity Theft : A Research Review," Final Report to the National Institute of Justice (2005) : 5-6.

Gráinne Kirwan and Andrew Power. Cybercrime: The Psychology of Online Offenders . Cambridge University Press, 2013 .

H. Thomas Milhorn, Cybercrime: How to Avoid Becoming a Victim . Universal Publishers, 2007.

Hossein Bidgoli . The Internet Encyclopedia . John Wiley & Sons, 2004.

Iqbal, F., Binsalleeh, H., Fung, B. C., & Debbabi, M. A unified data mining solution for authorship analysis in anonymous textual communications. Information Sciences, 231, 2013.

Joe Wright and Jim Harmening. "Security Management Systems" in Computer and Information Security Handbook, ed. John R. Vacca . Morgan Kaufmann Publishers, Elsevier Inc., 2009.

Jonathan Clough. Principle of Cybercrime . 2nd ed. Cambridge University Press, 2015.

Kathleen Frawley, Dale W. Miller, and Cynthia Miller . “State of Security Features for Medical Information”. in Information Technology for the Practicing Physician, ed. Joan M. Kiel . Springer, 2001.

Kierkegaard, S. M. . EU tackles cybercrime. In Cyber warfare and cyber terrorism , IGI Global. 2007.

Lin, Z., Tong, L., Zhijie, M., & Zhen, L. (2017, October). Research on cyber crime threats and countermeasures about tor anonymous network based on meek confusion plug-in. In 2017 International Conference on Robots & Intelligent System (ICRIS) (pp. 246-249). IEEE.

Littman, J. . The Watchman : The Twisted Life and Crimes of Serial Hacker Kevin Poulson, Little, Brown and Co.,1997.

Lynne D. Roberts . “Cyber Victimization” in Handbook of Research on Technoethics, ed. Rocci Luppicini . IGI Global, 2009.

Marc Rogers . Psychology of Hackers: Steps Toward a New Taxonomy , 1999. cited in John Van Beveren, “A Conceptual Model of Hacker Development and Motivations,” Journal of E-Business 1,2 (December 2001)

Marco Gercke . Internet-related Identity Theft, Project on Cybercrime (Council of Europe, 2007), p. 19-20.; Ruth Halperin, “Identity as an Emerging Field of Study,” Datenschutz und Datensicherheit - DuD 30,9 (2006): 533–537.

Marcus K. Rogers. “A Two-dimensional Circumplex approach to the Development of a Hacker Taxonomy.” . Digital Investigation 3,2 (2006): 97-102.

Matti Joutsen. International Cooperation against Transnational Organized Crime: The Practical Experience of the European Union, p. 396-397. Retrived 16 April 2019, https://www.unafei.or.jp/publications/pdf/RS_No59/No59_29VE_Joutsen3.pdf.

Michael T. Simpson. Hands on ethical hacking and network defense .Thomson Course Technology, 2006.

Monique Ferraro, Eoghan Casey, BS, MA, Eoghan Casey, Michael McGrath. Investigating child exploitation and pornography: the Internet. the law and forensic science, Elsevier Academic Press, 2005.

Mulligan, S. P. Cross-border data sharing under the CLOUD Act. Washington : Congressional Research Service, 2018.

National Research Council. Computers at Risk . Washington, DC: National Academy Press, 1991.

Nazura Abdul Manap, Anita Abdul Rahim, and Hossein Taji, "Cyberspace Identity theft: The Conceptual Framework." Mediteranean Jouranl of Social Science 6,4 (August 2015): 600.

Neil Mitchison, Marc Wilikens, Lothar Breitenbach, Robin Urry, and Portesi . Identity Theft – A Discussion Paper . Italy: European Commission, Directorate-General, Joint Research Centre, 2004.

Nir Kshetri . "Pattern of global cyber war and crime: A conceptual framework ." Journal of International Management 11,4 (2005): 541-562.

Nirkhi, S. M., Dharaskar, R. V., & Thakre, V. M. (2012, June). Analysis of online messages for identity tracing in cybercrime investigation. In Proceedings Title : 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec) (pp. 300-305). IEEE.

Norton, What is cybercrime? [Online]. (n.d.). Available from: https://us.norton.com/cybercrime-definition [21 November 2018]

O'Malley, G. (2013). Hacktivism: cyber activism or cyber crime. Trinity CL Rev., 16, 137.

Organization for Economic Co-operation and Development (OECD), OECD Policy Guidance on Online Identity Theft [Online]. 2008. Available from: http://www.oecd.org/dataoecd/49/39/40879136.pdf [21 November 2018]

Paul Taylor, Hackers: Crime in the Digital Sublime (Routledge, 1999), p. 200.

Power, R. (1997) 'CSI Special Report: Salgado Case Reveals Darkside of Electronic Commerce,' Computer Security Alert, No. 174, September.

Raoul Chiesa . Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking. 1st ed. . Auerbach Publications, 2008.

Robin T. Naylor . “Wages of Crime: Black Markets.” in Illegal Finance, and the Underworld Economy . Cornell University Press, 2004.

Russell G. Smith, Peter N. Grabosky, and Gregor F. Urbas. Cyber Criminals on Trial . UK: Cambridge University Press, 2004.

Sander, T., Ta-Shma, A. (1999). On Anonymous Electronic Cash and Crime. In: Information Security. ISW 1999. Lecture Notes in Computer Science, vol 1729. Springer, Berlin, Heidelberg.

Sarah Gordon and Richard Ford, “On the Definition and Classification of Cybercrime,” Journal in Computer Virology 2,1 (2006): 13-20.

Schwartz, P. M. (2018). Legal access to the global cloud. Columbia Law Review, 118 (6), 1681-1762.

Steven M. Furnell . “The Problem of Categorising Cybercrime and Cybercriminals,” Paper presented at the 2nd Australian Information Warfare and Security Conference, Perth, Australia, 2001.

Susan Brenner. Cybercrime: Criminal Threats from Cyberspace . Santa Barbara, California: Praeger, 2010.

the United Nations Office on Drugs and Crime (UNODC) , Undercover operations , Organized Crime Module 8 Key Issues: Special Investigative Techniques - Undercover Operations (unodc.org)

United Nations General Assembly, Combating the Criminal Misuse of Information Technologies (Resolution 55/63) [Online]. 2000. Available from: http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf [21 November 2018]

United Nations, A UN treaty on cybercrime en route, https://unric.org/en/a-un-treaty-on-cybercrime-en-route/ , 4/05/2022.

United Nations, Results of the Fourth United Nations Survey of Crime Trends and Operations of Criminal Justice Systems - Interim report prepared by the Secretariat - Addendum, In Ninth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 29 April – 8 May 1995.

United Nations/ United Nations Manual on the Prevention and Control of Computer-Related Crime: International review of criminal policy . New York: United Nations, 1994.

Urs E. Gattiker. The Information Security Dictionary . Kluwer Academic Publisher, 2004.

US Congress (1997a) Statement of Louis J. Freeh, Director FBI, before the Senate Committee on Commerce, Science, and Transportation, regarding the Impact of Encryption on Law Enforcement and Public Safety, March 19

Van Wegberg, R., Miedema, F., Akyazi, U., Noroozian, A., Klievink, B., & van Eeten, M. (2020, April). Go see a specialist? predicting cybercrime sales on online anonymous markets from vendor and product characteristics. In Proceedings of The Web Conference 2020 (pp. 816-826).

Vera Bergelson. "Victimless Crimes." in The International Encyclopedia of Ethics . Wiley Online Library, 2013.

Vu, A. V., Hughes, J., Pete, I., Collier, B., Chua, Y. T., Shumailov, I., & Hutchings, A. (2020, October). Turning up the dial: the evolution of a cybercrime market through set-up, stable, and covid-19 eras. In Proceedings of the ACM Internet Measurement Conference (pp. 551-566).

W. Steve Albrecht, Chad O. Albrecht, Conan C Albrecht, and Mark F. Zimbelman, Fraud Examination . SouthWestern Cengage Learning, 2011.

William Stallings. Network Security Essentials: Applications and Standards, 4th ed. . US: Prentice Hall, 2011.

Wyre, M., Lacey, D., & Allan, K. The identity theft response system. Trends and Issues in Crime and Criminal Justice. (592).2020, pp.1-18.

Yulia Cherdantseva and Jeremy Hilton, "Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals," in Organizational, Legal, and Technological Dimensions of Information System Administrator . eds. Fernando Almeida and Irene M. Portela . IGI Global Publishing, 2013.

Zheng, R., Qin, Y., Huang, Z., & Chen, H. (2003, June). Authorship analysis in cybercrime investigation. In International conference on intelligence and security informatics (pp. 59-73). Springer, Berlin, Heidelberg.

Zingerle, A. (2014). Remain Anonymous, Create Characters and Backup Stories: Online Tools Used in Internet Crime Narratives. In: Mitchell, A., Fernández-Vara, C., Thue, D. (eds) Interactive Storytelling. ICIDS 2014. Lecture Notes in Computer Science, vol 8832. Springer, Cham.