ปัญหาและอุปสรรคในการรวบรวมพยานหลักฐานทางดิจิทัลของคดีอาชญากรรมทางคอมพิวเตอร์ในชั้นพนักงานสอบสวน

Issues and Limitations in Digital Evidence Collection in Cybercrime Investigations by Law Enforcement Officers

เศวรัตน์ ปุริสาย*
หลักสูตรนิติวิทยาศาสตร์
E-mail: purisai_s@silpakorn.edu
อรทัย เขียวพุ่ม
ภาควิชาฟิสิกส์ คณะวิทยาศาสตร์ มหาวิทยาลัยศิลปากร
ศิริรัตน์ ชูสกุลเกรียง
ภาควิชาเคมี คณะวิทยาศาสตร์ มหาวิทยาลัยศิลปากร

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาถึงปัญหาและอุปสรรคในการรวบรวมพยานหลักฐานทางดิจิทัลของคดีอาชญากรรมทางคอมพิวเตอร์ในชั้นพนักงานสอบสวนของประเทศไทย โดยวิจัยนี้เป็นการวิจัยเชิงคุณภาพ ใช้การวิเคราะห์เอกสาร งานวิจัย ข้อมูลจากหน่วยงานที่เกี่ยวข้อง และสัมภาษณ์เชิงลึกในกลุ่มตัวอย่างเจ้าหน้าที่ตำรวจผู้รับผิดชอบคดีอาชญากรรมทางคอมพิวเตอร์โดยตรง จำนวน 14 คน โดยใช้การสัมภาษณ์แบบกึ่งโครงสร้าง ผลการศึกษาพบว่าสามารถจำแนกปัญหาและอุปสรรคหลักได้เป็น 4 ประการ ได้แก่ ปัญหาการขอข้อมูลระหว่างหน่วยงานที่เกี่ยวข้องในกระบวนการยุติธรรม และหน่วยงานที่มีความเกี่ยวข้องกับพยานหลักฐานในคดีอย่างมีประสิทธิภาพ ปัญหาการขอข้อมูลจากต่างประเทศ ปัญหาในการใช้อำนาจตามบทบัญญัติกฎหมาย เนื่องจากกฎหมายมีความล้าสมัยไม่สอดรับกับอาชญกรรมทางเทคโนโลยีรูปแบบใหม่ และปัญหาข้อจำกัดทางทรัพยากรบุคคล ควรมีการฝึกอบรมข้าราชการตำรวจเพื่อให้เท่าทันเทคโนโลยีที่เปลี่ยนแปลงไป การขาดอุปกรณ์ และทุนทรัพย์ และการจัดการบังคับใช้กฎหมาย แม้ว่าจะมีกฎหมายที่เกี่ยวข้องในการให้อำนาจพนักงานสอบสวน แต่ยังไม่สามารถป้องกันปราบปรามอาชญากรรมทางคอมพิวเตอร์ได้อย่างมีประสิทธิภาพ ผลการศึกษาในครั้งนี้สามารถนำไปวิเคราะห์และนำเสนอแนวทางแก้ไขปรับปรุงเพื่อประสิทธิผล ในการรวบรวมพยานหลักฐานและบังคับใช้กฎหมายให้เหมาะสมเพื่อประโยชน์ทางนิติวิทยาศาสตร์ได้

คำสำคัญ: พยานหลักฐานทางดิจิทัล, อาชญากรรมทางคอมพิวเตอร์, ข้อมูลจราจรทางคอมพิวเตอร์

Abstract

This study aims to explore the challenges and obstacles in the collection of digital evidence in cybercrime cases during the investigative stage by law enforcement officers in Thailand. Employing a qualitative research methodology, the study involves document

analysis, review of related research and data from relevant agencies, and in-depth interviews with a purposive sample of 14 police officers directly responsible for cybercrime investigations. Semi-structured interviews were utilized to gather detailed insights. The findings identify four primary challenges: (1) ineffective coordination and data-sharing among agencies within the justice system and with entities that hold relevant digital evidence; (2) difficulties in obtaining information from foreign sources; (3) limitations in the application of legal authority due to outdated legislation that does not align with modern technological crimes; and (4) constraints in human resources, including inadequate training, lack of proper equipment, insufficient funding, and weak law enforcement mechanisms. Despite existing legal frameworks that empower investigators, they remain insufficient for effectively combating cybercrime. The study's results offer a foundation for developing practical recommendations to enhance the efficiency of digital evidence collection and law enforcement, contributing to improvements in digital forensics and the overall administration of justice.

Keywords: Digital Evidence, Cybercrime, Computer Traffic Data

บทนำ

ปัจจุบันถือเป็นยุคดิจิทัลที่เทคโนโลยีมีการพัฒนาอย่างก้าวกระโดด แม้ว่าเทคโนโลยีจะถูกนำมาใช้ประโยชน์อย่างแพร่หลาย แต่หากถูกนำไปใช้ในทางที่ไม่เหมาะสม ก็อาจก่อให้เกิดความเสียหายอย่างร้ายแรงได้เช่นกัน อีกทั้งอาชญากรได้ปรับเปลี่ยนวิธีการก่ออาชญากรรมจากอาชญากรรมทั่วไป (Street Crime) มาสู่อาชญากรรมทางคอมพิวเตอร์ หรืออาชญากรรมไซเบอร์ (Cyber Crime) ซึ่งมีความซับซ้อนและยากต่อการติดตามมากขึ้น โดยในการก่ออาชญากรรมประเภทนี้ ดังนั้น เจ้าหน้าที่ตำรวจจึงจำเป็นต้องพัฒนาความรู้และทักษะให้ทันกับรูปแบบอาชญากรรมที่เปลี่ยนแปลงอยู่ตลอดเวลา รวมถึงต้องมีความเชี่ยวชาญในการแสวงหาและรวบรวมพยานหลักฐานทางดิจิทัล ซึ่งสามารถนำไปใช้ในการพิสูจน์ข้อเท็จจริงหรือการกระทำความผิดในกระบวนการยุติธรรมทางอาญาได้อย่างมีประสิทธิภาพ โดยอาจกล่าวได้ว่าตำรวจเป็นต้นธารแห่งกระบวนการยุติธรรม ซึ่งมีพนักงานสอบสวนเป็นผู้ทำหน้าที่รวบรวมพยานหลักฐานจากที่เกิดเหตุ รวมถึงพยานหลักฐานทุกชนิดเท่าที่จะสามารถหาได้ โดยงานของแต่ละฝ่าย ไม่ว่าจะเป็นฝ่ายสืบสวนหรือฝ่ายสอบสวน จะต้องดำเนินไปอย่างสอดคล้องกัน เพื่อให้เกิดความยุติธรรมอย่างแท้จริง จากข้อมูลของรัฐบาลไทย (https://www.thaigov.go.th/news/contents/details/90002, 2567) ระบุว่า ตั้งแต่วันที่ 1 มีนาคม 2565 – 31 ตุลาคม 2567 มีผลการแจ้งความออนไลน์ผ่าน https://www.thaipoliceonline.com รวมทั้งสิ้น 708,141 เรื่อง คิดเป็นมูลค่าความเสียหายรวมกว่า 74,893,134,395 บาท เฉลี่ยความเสียหายวันละประมาณ 77 ล้านบาท โดยมีผลการอายัดบัญชีจำนวน 544,183 บัญชี มียอดขออายัดกว่า 43,040,600,310 บาท และสามารถอายัดได้จริงจำนวน 8,243,782,268 บาท จากสถิติดังกล่าว จะเห็นได้ว่าคดีอาชญากรรมทางคอมพิวเตอร์มีมูลค่าความเสียหายในระดับสูง อีกทั้งยังมีความซับซ้อนในรูปแบบของคดี เจ้าหน้าที่ตำรวจผู้รับผิดชอบจึงจำเป็นต้องมีความเข้าใจทางเทคโนโลยีในระดับหนึ่ง เนื่องจากพยานหลักฐาน

ที่เกี่ยวข้องกับคอมพิวเตอร์นั้นมีลักษณะเฉพาะ กล่าวคือ สามารถเปลี่ยนแปลงได้ง่าย อาจถูกทำลายและยากต่อการสืบค้นหรือจัดเก็บอย่างถูกต้อง

จากการทบทวนวรรณกรรมและรายงานวิจัยพบว่า พยานหลักฐานดิจิทัลสามารถจำแนกได้เป็น 3 ประเภท ได้แก่ 1. พยานหลักฐานที่มนุษย์สร้างขึ้น (Human Generated Evidence) 2. พยานหลักฐานที่คอมพิวเตอร์สร้างขึ้น (Computer Generated Evidence) และ 3. พยานหลักฐานที่มนุษย์และคอมพิวเตอร์ร่วมกันสร้าง (Hybrid Evidence) โดยบทบัญญัติทางกฎหมายที่ให้อำนาจหน่วยงานที่เกี่ยวข้อง ได้แก่ ประมวลกฎหมายวิธีพิจารณาความอาญา พุทธศักราช 2477,พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560, พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 และพระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา (ฉบับที่ 2) พ.ศ. 2559

อย่างไรก็ตาม กฎหมายที่มีอยู่ในปัจจุบันอาจยังไม่สามารถป้องกันหรือปราบปรามอาชญากรรมทางคอมพิวเตอร์ได้อย่างมีประสิทธิภาพ เนื่องจากยังมีข้อจำกัดและอุปสรรคในการบังคับใช้ โดยเฉพาะในขั้นตอนการรวบรวมพยานหลักฐานของพนักงานสอบสวน ทั้งนี้ แม้ประเทศไทยยังไม่มีบทบัญญัติเฉพาะเกี่ยวกับการจัดเก็บพยานหลักฐานดิจิทัลอย่างเป็นทางการ แต่ศูนย์ดิจิทัลฟอเรนสิกส์ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ได้จัดทำเอกสารข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐาน เพื่อเป็นแนวทางสำหรับเจ้าหน้าที่ในการปฏิบัติงานในสถานที่เกิดเหตุให้สอดคล้องกับมาตรฐานสากล โดยสามารถดำเนินการตามสถานการณ์และอำนาจหน้าที่ที่กฎหมายกำหนด

จากที่กล่าวมาข้างต้น แม้จะมีกฎหมายและความพยายามจากหลายภาคส่วน แต่การเปลี่ยนแปลงของเทคโนโลยีที่รวดเร็ว ส่งผลให้คดีอาชญากรรมทางคอมพิวเตอร์มีแนวโน้มเพิ่มสูงขึ้น การศึกษาปัญหาและอุปสรรคในการรวบรวมพยานหลักฐานทางนิติดิจิทัลในคดีอาชญากรรมทางคอมพิวเตอร์ในชั้นพนักงานสอบสวนจึงเป็นสิ่งจำเป็น โดยมุ่งเน้นการสัมภาษณ์เจ้าหน้าที่ตำรวจผู้รับผิดชอบคดีอาชญากรรมทางคอมพิวเตอร์โดยตรง และเปรียบเทียบกับแนวทางของประเทศที่ประสบความสำเร็จในการรับมือกับอาชญากรรมทางคอมพิวเตอร์ เช่น ประเทศสิงคโปร์ เพื่อให้ได้ข้อเสนอเชิงนโยบายที่เป็นรูปธรรม และสามารถนำไปสู่การปรับปรุงกลไก ในการรวบรวมพยานหลักฐานและการบังคับใช้กฎหมายได้อย่างมีประสิทธิภาพและเหมาะสมกับบริบทของประเทศไทย

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาปัญหาในการรวบรวมพยานหลักฐานทางดิจิทัลในคดีอาชญากรรมทางคอมพิวเตอร์ในชั้นพนักงานสอบสวนของประเทศไทย
2. เพื่อศึกษากฎหมายที่เกี่ยวข้อง และวิเคราะห์เปรียบเทียบปัญหาในการรวบรวมพยานหลักฐานทางคอมพิวเตอร์ในคดีอาชญากรรมของประเทศไทยและประเทศสิงคโปร์

ขอบเขตการวิจัย

1. ขอบเขตด้านเนื้อหา เพื่อศึกษาสภาพปัญหาและอุปสรรคในการรวบรวมพยานหลักฐานทางดิจิทัล โดยผู้วิจัยนำงานวิจัยที่เกี่ยวข้องมาวิเคราะห์หลักกฎหมายที่เกี่ยวข้อง พร้อมศึกษาหลักกฎหมายเกี่ยวกับการค้นและการยึดพยานหลักฐานทางดิจิทัลของประเทศไทยและประเทศสิงคโปร์

2. ขอบเขตด้านผู้ให้ข้อมูลคนสำคัญ การวิจัยครั้งนี้ใช้กระบวนวิธีการวิจัยเชิงคุณภาพ (Qualitative Research) โดยการสัมภาษณ์เชิงลึก (In-depth Interview)

วิธีดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) โดยผู้วิจัยดำเนินการศึกษาในลักษณะของการวิจัยเอกสาร (Documentary Research) และการสัมภาษณ์เชิงลึก (In-depth Interview) เพื่อให้ได้ข้อมูลที่ครอบคลุมและลึกซึ้งในประเด็นที่เกี่ยวข้องกับการรวบรวมพยานหลักฐานทางดิจิทัลในคดี อาชญากรรมทางคอมพิวเตอร์

ในส่วนของการวิจัยเอกสาร ผู้วิจัยได้ทำการรวบรวม วิเคราะห์ และสังเคราะห์ข้อมูลจากแหล่งต่าง ๆ รวมถึงเอกสารทางกฎหมายของประเทศไทย เปรียบเทียบกับเอกสารทางกฎหมายของประเทศสิงคโปร์ เพื่อศึกษาข้อเปรียบเทียบเชิงกฎหมายในประเด็นที่เกี่ยวข้อง สำหรับการเก็บข้อมูลภาคสนาม ผู้วิจัยใช้วิธีการสัมภาษณ์แบบเจาะจง (Purposive Sampling) โดยกำหนดกลุ่มผู้ให้ข้อมูลเป็นเจ้าหน้าที่ตำรวจผู้ที่มีความรู้และประสบการณ์ตรงกับหัวข้อการวิจัย รวมทั้งสิ้นจำนวน 14 คน

การเก็บรวบรวมข้อมูล

การเก็บรวบรวมข้อมูลในการวิจัยครั้งนี้ประกอบด้วยขั้นตอนสำคัญ ได้แก่ การจัดทำโครงร่างแนวคำถามสำหรับการสัมภาษณ์แบบเจาะลึก (In-depth Interview) โดยมีการกำหนดประเด็นคำถามที่ชัดเจน การสัมภาษณ์ดำเนินการในลักษณะกึ่งโครงสร้าง (Semi-structured Interview) ซึ่งเปิดโอกาสให้ผู้ให้ข้อมูลสามารถสะท้อนมุมมองและประสบการณ์ที่เกี่ยวข้องได้อย่างเต็มที่ การจดบันทึกข้อมูลประกอบด้วยการบันทึกรายละเอียดของการสัมภาษณ์ทุกครั้ง โดยได้รับความยินยอมจากกลุ่มตัวอย่างในการบันทึกเสียง ทั้งนี้ ข้อมูลเสียงที่บันทึกไว้จะถูกจัดเก็บในสถานที่ปลอดภัย และจำกัดการเข้าถึงเฉพาะผู้วิจัยเท่านั้น

การวิเคราะห์ข้อมูล

ในการวิเคราะห์ข้อมูล ผู้วิจัยเริ่มต้นจากการศึกษาทบทวนวรรณกรรม แนวคิด ทฤษฎี และผลงานวิจัยที่เกี่ยวข้องทั้งในและต่างประเทศ รวมถึงบทบัญญัติกฎหมายที่เกี่ยวข้องของประเทศสิงคโปร์ จากนั้นจึงนำข้อมูลเชิงคุณภาพที่ได้จากการสัมภาษณ์เชิงลึกมาวิเคราะห์โดยใช้วิธีการวิเคราะห์เนื้อหา (Content Analysis) และสามารถนำไปสู่ข้อเสนอเชิงนโยบายหรือแนวทางปรับปรุงได้อย่างมีประสิทธิภาพ

ผลการวิจัย

จากการศึกษาพบว่า สำนักงานตำรวจแห่งชาติได้พัฒนาระบบ “การแจ้งความออนไลน์” เพื่ออำนวยความสะดวกแก่ประชาชนในการแจ้งเหตุหรือร้องเรียนต่าง ๆ โดยประชาชนสามารถติดตามขั้นตอนได้ด้วย

ตนเอง มีศูนย์บริหารการรับแจ้งความออนไลน์จะทำหน้าที่เป็นตัวกลางประสานงานไปยังสถานีตำรวจที่รับผิดชอบ พร้อมกับประสานการอายัดบัญชีกับธนาคารในทันที ทั้งยังมีการลงนามบันทึกข้อตกลงความร่วมมือ (MOU) ระหว่างสำนักงานตำรวจแห่งชาติ สมาคมสถาบันการเงินที่เกี่ยวข้อง เพื่อเสริมสร้างประสิทธิภาพในกระบวนการดำเนินคดี อย่างไรก็ตาม ยังคงพบปัญหาและความท้าทายในการรวบรวมพยานหลักฐานทางดิจิทัล ซึ่งสามารถแบ่งออกเป็น 4 ประเด็นหลัก โดยผู้วิจัยขอยกตัวอย่างที่สำคัญ ดังนี้

1. ปัญหาในการขอข้อมูลภายในประเทศ พบว่าการติดต่อขอข้อมูลเป็นไปได้ยาก โดยพนักงานสอบสวนใช้อำนาจตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 52, 131, 132(3)(4) และ 133 ในการออกหมายเรียกเพื่อขอข้อมูลจากธนาคารต่างๆ เช่น รายการเดินบัญชี ผ่านระบบออนไลน์ banking.ccib.go.th เป็นต้น อย่างไรก็ตาม พนักงานสอบสวนยังต้องทำหนังสือถึงธนาคารสาขาโดยตรง เพื่อขอข้อมูลแบบกระดาษเพื่อมาใช้ในการประกอบสำนวนคดี เป็นขั้นตอนที่ซ้ำซ้อน ซึ่งการสัมภาษณ์เจ้าหน้าที่ตำรวจกลุ่มตัวอย่างได้กล่าวไว้อย่างน่าสนใจว่า

“ในกรณีการสืบสวนเส้นทางการเงิน การขอข้อมูลไปยังธนาคารแต่ละแห่ง ต้องส่งเป็นหนังสือหมายเรียกไปยังสาขาธนาคาร หรือ สำนักงานใหญ่ โดยส่วนใหญ่ธนาคารสาขาที่คนร้ายเปิดบัญชี กระจายทั่วประเทศไทย และส่วนใหญ่ช้ามาก ส่วนของหนังสือส่งทางระบบประสานงานธนาคาร (banking.ccib.go.th) พอได้รับเอกสารจากระบบ เราก็ปริ๊นออกมาประกอบสำนวนแต่พนักงานอัยการไม่ให้เจ้าหน้าที่ตำรวจใช้เอกสารที่ทำบันทึกตามข้อตกลงไว้ สุดท้ายพนักงานสอบสวนต้องทำหมายเรียกต่างหากไปยังธนาคารสาขาเพื่อขอรายการเดินบัญชีแบบกระดาษมาประกอบสำนวน”

เมื่อเปรียบเทียบกับประเทศสิงคโปร์ การดำเนินคดีกับผู้กระทำความผิดทางคอมพิวเตอร์สำหรับประเทศสิงค์โปร์ถูกบัญญัติไว้ตาม Computer Misuse Act (CMA) เจ้าหน้าที่สามารถร้องขอข้อมูลดิจิทัลได้โดยไม่ต้องมีหมายศาลในบางกรณีเร่งด่วน และมีระบบเชื่อมต่อแบบ Real-time กับผู้ให้บริการ เช่น ผู้ให้บริการอินเทอร์เน็ต (Internet service provider: ISP) และผู้ให้บริการคลาวด์ในประเทศ

2. ปัญหาในการขอข้อมูลจากต่างประเทศ เป็นที่ประจักษ์ว่าการเข้าถึงข้อมูลจากแพลตฟอร์มระดับโลก เช่น Google และ Line เป็นไปได้ยาก เนื่องจากมีข้อจำกัดด้านกฎหมายและนโยบายความเป็นส่วนตัว อีกทั้งต้องอาศัยความร่วมมือระหว่างประเทศ ซึ่งใช้เวลานาน และส่งผลให้การติดตามตัวผู้กระทำผิดล่าช้า ในประเด็นนี้ เจ้าหน้าตำรวจในกลุ่มตัวอย่างได้กล่าวไว้สอดคล้องกับปัญหา

“ปัญหาจากการขอข้อมูลการจราจรทางคอมพิวเตอร์ พบเกือบทุกเคส การขอข้อมูลการลงทะเบียนบัญชีผู้ใช้งาน หรือ พวก log file มันแบ่งย่อยออกไปอีกหลายอย่าง เช่น อยู่นอกเขตไทย มีทั้งแบบไม่ให้ความร่วมมือเลย ให้ความร่วมมือแต่ต้องผ่าน MLAT อย่าง Line หรือมีช่องทางร้องขอข้อมูลที่ทำไว้แล้วไม่ต้องทำ MLAT แต่ยังไม่เปิดให้เจ้าหน้าที่ต่างชาติเข้าถึงได้ เช่น Google LERS พอขอไม่ได้ ก็พิสูจน์ว่าใครเป็นคนใช้งานไม่ได้”

ในขณะที่ประเทศสิงคโปร์เป็นพันธมิตรกับสหรัฐอเมริกา ทำให้สามารถขอข้อมูลจากบริษัทเทคโนโลยีได้สะดวก นอกจากนี้ ยังมีการจัดตั้งศูนย์กลางการจัดการอาชญากรรมไซเบอร์ (Cybercrime Command Center) ซึ่งประสานงานโดยตรงกับ องค์การตำรวจอาชญากรรมระหว่างประเทศ INTERPOL ซึ่งมีสำนักงานใหญ่ด้านเทคโนโลยีสารสนเทศตั้งอยู่ที่ประเทศสิงคโปร์

3. ปัญหาในการใช้อำนาจตามบทบัญญัติกฎหมาย แม้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 จะให้อำนาจพนักงานสอบสวนในการยื่นคำร้องต่อศาลเพื่อขอหมายค้นและเข้าถึงอุปกรณ์คอมพิวเตอร์ แต่ในทางปฏิบัติยังพบอุปสรรคหลายประการ เช่น ต้องได้รับอนุญาตจากเจ้าของอุปกรณ์ก่อน หรือจำเป็นต้องขอรหัสผ่าน ซึ่งหากผู้ต้องหาไม่ให้ความร่วมมือ ก็มีเพียงโทษปรับ ซึ่งอาจไม่เพียงพอในการบังคับใช้กฎหมาย และในส่วนของประเทศสิงค์โปร์นั้น เจ้าหน้าที่รัฐมีอำนาจเข้าถึงข้อมูลคอมพิวเตอร์ได้ในบางกรณีโดยไม่ต้องผ่านศาลเลย โดยมีเจ้าหน้าที่ตำรวจแสดงทัศนคติในประเด็นนี้ไว้ว่า

“ในมุมมองของการรักษาสิทธิของผู้เป็นเจ้าของเครื่องเป็นสิ่งที่ดี แต่พอขอหมายเข้าถึงจากศาลแล้ว ผู้ต้องหาหรือผู้ถูกกล่าวหาไม่ปฏิบัติตามหมายของศาล มีโทษปรับแค่เป็นวัน พนักงานสอบสวนไม่ได้มีอำนาจที่เข้าถึงอุปกรณ์ โดยทันที ซึ่งในมุมมองของพนักงานสอบสวนคิดว่าพยานหลักฐานมันถูกลบง่ายอยู่แล้ว ช่วงเวลาที่เจ้าของเครื่องปฏิเสธไม่ให้เข้าอุปกรณ์ เขาอาจให้คนอื่นเข้าไปลบให้ก็ได้”

4. ข้อจำกัดด้านทรัพยากร โดยเจ้าหน้าที่ผู้ปฏิบัติงานด้านนิติวิทยาศาสตร์ดิจิทัล (Digital Forensics) ยังมีจำนวนจำกัด และขาดแคลนการฝึกอบรมอย่างต่อเนื่อง ขณะเดียวกันก็มีข้อจำกัดด้านงบประมาณและเครื่องมือ เช่น ซอฟต์แวร์ เทคโนโลยีแยกประเภทข้อมูลดิจิทัลที่บันทึกธุรกรรมอย่างปลอดภัย Blockchain Analysis ที่ใช้ติดตามเส้นทางของคริปโตเคอร์เรนซี (เช่น TRM Labs) มีค่าใช้จ่ายสูง ทำให้ไม่สามารถนำมาใช้ติดตามอาชญากรรมในโลกดิจิทัลได้อย่างเต็มประสิทธิภาพ โดยเจ้าหน้าที่ตำรวจได้กล่าวไว้อย่างสอดคล้องว่า

“ในบางคดี เช่น การวิเคราะห์บล็อกเชน หรือ คริปโต ถ้าต้องการความรวดเร็วกับการวิเคราะห์ต้องอาศัยซอฟต์แวร์ของบริษัทเอกชนที่มีค่าใช้จ่ายสูง ก่อนหน้านี้ เคยมีเคสที่ใช้งานเว็บไซต์ฟรี ข้อมูลมันเยอะมาก กว่าจะเอามาวิเคราะห์อีกใช้เวลานานในการสืบสวนไปถึงคนร้าย และความรู้เฉพาะทางที่มีของบุคลากรไม่เพียงพอด้วย”

เมื่อเปรียบเทียบกับประเทศสิงค์โปร์ แม้กฎหมายอาจจะไม่ทันตามเทคโนโลยีที่เปลี่ยนไป แต่มีการพัฒนาการอบรมอยู่เสมอ โดยมีโครงการฝึกอบรมระดับชาติ (SG Cyber Talent) เพื่อส่งเสริมบริษัทเอกชนในสิงคโปร์เพิ่มขีดความสามารถด้านการป้องกันความมั่นคงปลอดภัยไซเบอร์ โดยรัฐบาลมุ่งหวังเห็นการยกระดับความมั่นคงปลอดภัยไซเบอร์โดยรวมของสิงคโปร์

สรุปและอภิปรายผลการวิจัย

จากการศึกษา พบว่า แนวโน้มของอาชญากรรมทางคอมพิวเตอร์มีการเพิ่มขึ้นอย่างต่อเนื่อง ซึ่งเป็นผลมาจากการพัฒนาอย่างรวดเร็วของวิทยาศาสตร์และเทคโนโลยี ส่งผลให้เกิดช่องโหว่ที่อาชญากรสามารถใช้ประโยชน์ในการก่ออาชญากรรม และก่อให้เกิดความเสียหายแก่สังคม เศรษฐกิจ และประชาชนทั่วไป แม้ว่าประเทศไทยจะมีกฎหมายหลายฉบับที่เกี่ยวข้องกับการควบคุมอาชญากรรมทางคอมพิวเตอร์ตามที่กล่าวไปข้างต้น แต่ในการบังคับใช้กฎหมายเหล่านี้ยังพบ ข้อจำกัดที่สำคัญในทางปฏิบัติ ได้แก่ ความล่าช้าในการประสานงานระหว่างหน่วยงานที่เกี่ยวข้อง, อุปสรรคในการเข้าถึงข้อมูลจากผู้ให้บริการทั้งในและต่างประเทศ ขาดกลไกที่มีประสิทธิภาพในการรวบรวมพยานหลักฐานดิจิทัล,ปัญหาเรื่องการเข้าถึงข้อมูลข้ามพรมแดนในคดีที่เกี่ยวข้องกับแพลตฟอร์มระดับโลก,การขาดแคลนทรัพยากร เช่น บุคลากรผู้เชี่ยวชาญเฉพาะด้าน และเทคโนโลยีที่ทันสมัย

เมื่อเปรียบเทียบกับประเทศสิงคโปร์ ซึ่งมีกรอบกฎหมายที่เอื้อต่อการทำงานของเจ้าหน้าที่สอบสวน เช่น การดำเนินคดีกับผู้กระทำความผิดทางคอมพิวเตอร์สำหรับประเทศสิงค์โปร์ถูกบัญญัติไว้ตาม Computer Misuse Act (CMA) และประมวลกฎหมายวิธีพิจารณาความอาญา Criminal Procedure Code (CPC) อีกทั้งยังมีระบบการประสานงานแบบทันที Real-time กับผู้ให้บริการในประเทศ รวมถึงการมีความร่วมมือระหว่างประเทศที่เข้มแข็ง

ในส่วนของแนวทางแก้ไขปรับปรุงจากภาพรวมข้างต้น สะท้อนให้เห็นว่า แม้ประเทศไทยจะมีความพยายามในการพัฒนากฎหมาย กระบวนการบังคับใช้ แต่ยังคงเผชิญกับข้อจำกัดทั้งเชิงระบบ บุคลากร กฎหมาย และความร่วมมือระหว่างประเทศ ดังนั้น จึงสามารถสรุปได้ว่า แนวทางในการปรับปรุงควรเป็นไปในลักษณะบูรณาการระหว่างหน่วยงานที่เกี่ยวข้อง โดยให้ความสำคัญกับการพัฒนาและปรับปรุงกฎหมายให้สอดรับกับเทคโนโลยี, การสร้างกลไกความร่วมมือกับบริษัทเทคโนโลยีระดับโลกผ่านการลงนามบันทึกข้อตกลง (MOU), การพัฒนาและเพิ่มจำนวนบุคลากรที่มีความเชี่ยวชาญเฉพาะทาง,การจัดสรรงบประมาณสำหรับเทคโนโลยีและเครื่องมือที่ทันสมัย, การเสริมสร้างความร่วมมือกับองค์กรระหว่างประเทศเพื่อเพิ่มศักยภาพในการรับมือกับอาชญากรรมข้ามพรมแดน เป็นสิ่งที่ควรมีการปรับปรุงแก้ไข

ข้อเสนอแนะ

จากผลการศึกษาและการวิเคราะห์เชิงลึกเกี่ยวกับปัญหาและอุปสรรคในการรวบรวมพยานหลักฐานทางดิจิทัล ผู้วิจัยเห็นว่า การแก้ไขปัญหาดังกล่าวควรดำเนินการอย่างเป็นระบบทั้งในระดับนโยบายและระดับเชิงปฏิบัติ เพื่อเพิ่มประสิทธิภาพในการรวบรวมพยานหลักฐานและการบังคับใช้กฎหมายให้เหมาะสมกับบริบทของอาชญากรรมทางคอมพิวเตอร์ในยุคปัจจุบัน

ข้อเสนอแนะเชิงนโยบาย

1. ปรับปรุงและพัฒนากฎหมายให้สอดรับกับภัยคุกคามรูปแบบใหม่: เช่น เทคนิคการปลอมแปลงข้อมูลด้วยปัญญาประดิษฐ์ (AI) โดยใช้เทคโนโลยีการเรียนรู้ เชิงลึก (deepfake) ในการปลอมใบหน้า เสียง หรือแสดงตนเป็นเจ้าหน้าที่รัฐเพื่อล่อลวงผู้เสียหาย

2. พัฒนานโยบายการขอข้อมูลระหว่างหน่วยงานในกระบวนการยุติธรรม: ควรมีการจัดทำบันทึกข้อตกลง (MOU) ระหว่างสำนักงานตำรวจแห่งชาติ สำนักงานอัยการสูงสุด ศาล และผู้ให้บริการด้านเทคโนโลยี เพื่อกำหนดกระบวนการขอข้อมูลดิจิทัลอย่างชัดเจน เสนอให้มีร่างกฎหมายหัวข้อ “การแลกเปลี่ยนข้อมูลดิจิทัลเพื่อการสอบสวนและดำเนินคดี” ที่กำหนดขั้นตอน ระยะเวลา และแนวทางปฏิบัติร่วมกัน

3. พัฒนาและเสริมสร้างความร่วมมือระหว่างประเทศ: ส่งเสริมการจัดทำความร่วมมือหรือบันทึกข้อตกลงกับประเทศที่มีเทคโนโลยีสูงหรือมีบริษัทแพลตฟอร์มที่ได้รับความนิยมในไทย เช่น สหรัฐอเมริกา ญี่ปุ่น รวมถึงจัดตั้งทีมประสานงานกลางของไทยสำหรับการขอข้อมูลอย่างเร่งด่วนจากต่างประเทศ

ข้อเสนอแนะเชิงปฏิบัติ

1. ส่งเสริมบทบาทของภาคเอกชนโดยเฉพาะธนาคารและบริษัทเทคโนโลยี: ควรมีการพัฒนาแพลตฟอร์มกลางที่สามารถร้องขอ–ติดตาม–ส่งมอบข้อมูลแบบทันที

2. การฝึกอบรมเจ้าหน้าที่ตำรวจให้ทันต่อเทคโนโลยีที่เปลี่ยนแปลง: สนับสนุนการอบรมอย่างต่อเนื่องในหัวข้อ เช่น นิติวิทยาศาสตร์ดิจิทัล (Digital Forensics), เทคโนโลยีแยกประเภทข้อมูลดิจิทัลที่บันทึกธุรกรรมอย่างปลอดภัย Blockchain Analysis เป็นต้น

3. การบังคับใช้กฎหมายอย่างมีประสิทธิภาพ จำเป็นต้องบูรณาการการพัฒนาด้านกฎหมายเทคโนโลยี และทักษะของบุคลากรให้สามารถใช้งานได้จริงในทางปฏิบัติ

ข้อเสนอแนะสำหรับการศึกษาครั้งต่อไป

1. ควรมีการศึกษาปัญหาและอุปสรรคเพิ่มเติม โดยเฉพาะในมิติที่เกี่ยวกับผู้เสียหาย พยาน และผู้ต้องหา เพื่อให้เข้าใจภาพรวมของปัญหาอย่างรอบด้าน

2. ศึกษามุมมองของผู้บริหารระดับสูงในหน่วยงานยุติธรรม เช่น ศาล อัยการ หรือผู้บัญชาการตำรวจเกี่ยวกับการแก้ไขปัญหาในการรวบรวมพยานหลักฐานทางดิจิทัล

3. ศึกษาแนวทางการบังคับใช้กฎหมายที่สอดคล้องกับเทคโนโลยีที่เปลี่ยนแปลงตลอดเวลา เพื่อรองรับความซับซ้อนของอาชญากรรมไซเบอร์

4. ศึกษาผลกระทบและการบังคับใช้ พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2568 ซึ่งมีผลบังคับใช้ตั้งแต่วันที่ 13 เมษายน 2568 โดยเฉพาะประเด็นเกี่ยวกับนิยามของ “สินทรัพย์ดิจิทัล” ที่เกี่ยวข้องกับการก่ออาชญากรรม

เอกสารอ้างอิง

กุลนิดา ผาตินาวิน. (2564). *ปัญหาทางกฎหมายเกี่ยวกับการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ในคดีอาญา*. วิทยานิพนธ์นิติศาสตรมหาบัณฑิต กลุ่มวิชากฎหมายอาญาและกระบวนการยุติธรรมทางอาญา. คณะนิติศาสตร์ มหาวิทยาลัยศรีปทุม.

อนุกลู จันธิมา. (2566). *ปัญหาในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ ในคดีอาชญากรรมไซเบอร์*. วิทยานิพนธ์นิติศาสตร์มหาบัณฑิต กลุ่มวิชากฎหมายอาญาและกระบวนการยุติธรรมทางอาญา. คณะนิติศาสตร์ มหาวิทยาลัยศรีปทุม.

Cyber Security Agency of Singapore. (n. d.) *Overview of legislations on cybersecurity, personal data, protection, and computer misuse.* https://www.csa.gov.sg/docs/default-source/csa/documents/publications/legislation-e-book/

Singapore Police Force. (n.d.). SPF | Collaboration with other Agencies. Retrieved December 8,2024, from https://www.police.gov.sg/Advisories/Crime/Cybercrime/Collaboration-with-other-Agencies