แนวทางเพิ่มประสิทธิภาพการดำเนินคดี
อาชญากรรมคอมพิวเตอร์

โดย

นายณัฐพงษ์ พุฒแก้ว
อัยการพิเศษฝ่าย
สำนักงานอัยการสูงสุด

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตรการป้องกันราชอาณาจักรรุ่นที่61
ประจำปีการศึกษา พุทธศักราช2561 – 2562

หนังสือรับรอง

วิทยาลัยป้องกันราชอาณาจักร สถาบันวิชาการป้องกันประเทศ ได้อนุมัติให้เอกสารวิจัยส่วนบุคคล เรื่อง “แนวทางเพิ่มประสิทธิภาพการดำเนินคดีอาชญากรรมคอมพิวเตอร์” ลักษณะวิชาการเมือง ของนายณัฐพงษ์ พุฒแก้ว เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรการป้องกันราชอาณาจักร รุ่นที่61ประจำปีการศึกษาพุทธศักราช2561 - 2562

พลโท

(ขจรฤทธิ์ นิลกำแหง)

ผู้อำนวยการวิทยาลัยป้องกันราชอาณาจักร

สถาบันวิชาการป้องกันประเทศ

บทคัดย่อ

เรื่อง แนวทางเพิ่มประสิทธิภาพการดำเนินคดีอาชญากรรมคอมพิวเตอร์

ลักษณะวิชา การเมือง

ผู้วิจัย นายณัฐพงษ์ พุฒแก้ว **หลักสูตร**วปอ.**รุ่นที่** 61

การวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาสภาพปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ที่พบในชั้นการสืบสวนสอบสวน รวบรวมพยานหลักฐาน จนถึงขั้นตอนการนำเสนอพยานหลักฐานในชั้นพิจารณาของศาลเพื่อวิเคราะห์ปัจจัยที่ก่อให้เกิดสภาพปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในปัจจุบันและเพื่อเสนอแนะแนวทางเพิ่มประสิทธิภาพการดำเนินคดีอาชญากรรมคอมพิวเตอร์โดยมีขอบเขตการวิจัยมุ่งเน้นมุ่งเน้นศึกษาปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในส่วนของการใช้เทคโนโลยีระบบคอมพิวเตอร์ในการกระทำความผิดที่สำคัญ โดยการรวบรวมข้อมูลปฐมภูมิจากวิธีการสัมภาษณ์ข้อมูลเชิงลึกผู้ทรงคุณวุฒิด้านการสืบสวนสอบสวน การตรวจพิสูจน์ทางนิติคอมพิวเตอร์และการดำเนินคดีอาชญากรรมคอมพิวเตอร์ พิจารณาประกอบกับข้อมูลทุติยภูมิจากการทบทวนวรรณกรรมที่เกี่ยวข้อง ผลการวิจัยพบว่าสภาพปัญหาสำคัญในการดำเนินคดีอาชญากรรมคอมพิวเตอร์มาจากปัจจัยสำคัญ ได้แก่ ปัจจัยด้านบุคลากรที่มีจำนวนไม่เพียงพอและขาดความรู้ด้านเทคนิคคอมพิวเตอร์ ปัจจัยด้านนิติคอมพิวเตอร์ที่มีประเด็นความกังวลด้านความน่าเชื่อถือของพยานหลักฐานที่มาจากการตรวจพิสูจน์โดยซอฟท์แวร์ที่ดาวน์โหลดแหล่งข้อมูลเปิด ปัจจัยด้านการประสานความร่วมมือระหว่างพนักงานสอบสวนและผู้ตรวจพิสูจน์หลักฐานในเรื่องขอบเขตการตรวจพิสูจน์ และการไม่ได้รับความร่วมมือจากผู้ประกอบการภาคเอกชน และปัจจัยด้านกฎหมาย ซึ่งพบว่าเจ้าพนักงานผู้ปฏิบัติงานมีความกังวลเกี่ยวกับอำนาจในการรวบรวมพยานหลักฐานดิจิทัลจากการความก้าวหน้าทางเทคโนโลยีของอุปกรณ์ดิจิทัล

ดังนั้นผู้วิจัยจึงมีข้อเสนอแนะว่า ในระดับนโยบาย รัฐควรจัดทำการศึกษา วิเคราะห์ และจัดทำข้อเสนอแนะเกี่ยวกับการเลือกใช้ซอฟท์แวร์จากแหล่งข้อมูลเปิดเพื่อช่วยเหลืองานด้านการตรวจพิสูจน์นิติคอมพิวเตอร์ รวมทั้งพิจารณานำแนวทางบทบัญญัติตาม“Computer Misuse Act (Chapter 50A) และ Criminal Procedure Code(Chapter 68) ของสาธารณรัฐสิงคโปร์มาเป็นแนวทางในการปรับปรุงกฎหมายวิธีพิจารณาความอาญาของไทย เพื่อแก้ไขปัญหาความชอบด้วยกฎหมายในการใช้อำนาจบางประการของเจ้าพนักงานในการรวบรวมพยานหลักฐานดิจิทัล ในระดับปฏิบัติการ สำนักงานตำรวจแห่งชาติและสำนักงานอัยการสูงสุด ควรนำแนวทางการสร้างหลักสูตรบนสื่ออิเล็กทรอนิกส์ (E-Learning) ตามแนวทางที่ INTERPOL – IGCI ของสาธารณรัฐสิงคโปร์ดำเนินการอยู่มาปรับใช้ นอกจากนี้ หน่วยงานผู้ปฏิบัติงานด้านอาชญากรรมคอมพิวเตอร์ควรร่วมกันกำหนดตัวอย่างแนวทางการกำหนดประเด็นและรูปแบบการร้องขอให้มีการตรวจพิสูจน์พยานหลักฐานทางดิจิทัลให้เหมาะสมกับประเภทของฐานความผิดในคดี และสร้างกลไกส่งเสริมให้ผู้ประกอบการภาคเอกชนเต็มใจให้ความร่วมมือเมื่อมีการร้องขอข้อมูลจากเจ้าพนักงานของรัฐ

Abstract

Title Guidelines for Increasing Efficiency in Cybercrime Prosecution
Field Politics
Name Mr. NattapongPutkaew**Course** NDC **Class** 61

This research is aimed at studying the problems and obstacles in prosecuting cybercrimes found in the investigation stage, evidence gathering stage and the stage of presenting evidence in the Court's trial; analyzing the factors that cause problems and obstacles in the prosecution of cybercrimes, and giving suggestions to improve the effectiveness of cybercrime prosecution. The scope of the research focuses on the problems encountered in the prosecution of cybercrimes, emphasizing on the use of computer system technology for committing crimes, by methods of collecting primary data from in-depth interview with investigators, computer forensics examiners and public prosecutors; and secondary data from literature reviews. It is found that the main problems in cybercrime prosecution are caused by several factors, such as insufficient number of expert officials and lack of computer technical knowledge, the concerns of evidence that comes from the examination carried out by software downloaded from open sources, coordination between investigators and forensics examiners in the scope of examination and the lack of cooperation from private entrepreneurs. Moreover, competent officials tend to be worried about the power to collect digital evidence as to the technological advancement of digital devices.

The researcher, therefore, has recommended that the State should consider on producing recommendation guidelines on the selection of software from open sources to assist in the investigation of computer forensics, and consider amendments of Thai Criminal Procedure Code to be in line with the Computer Misuse Act (Chapter 50A) and Criminal Procedure Code (Chapter 68) of the Republic of Singapore in order to resolve the legality ambiguity of certain powers of officials to collect digital evidence. At the operational level, the Royal Thai Police and the Office of the Attorney General should adopt the E-Learning curriculum of the

INTERPOL-IGCI of the Republic of Singapore. Moreover, the law enforcement on cybercrime should work together for making guidelines for determining issues and forms for requesting the examination of digital evidence which are appropriate with each related offence, and initiate mechanisms to encourage private entrepreneurs to be willing to give good cooperation to officials.

คำนำ

ประเทศไทยใช้ระบบการดำเนินคดีอาญาที่ผสมผสานระบบกล่าวหา (Inquisitorial System) และระบบไต่สวน (Accusatorial System) ในระบบการพิจารณาคดีและการสืบพยานโดยคู่ความในคดีทั้งสองฝ่ายมีหน้าที่แสวงหาพยานหลักฐานมาต่อสู้หักล้างกัน บุคคลซึ่งถูกกล่าวหาว่ามีความผิดอาญามีสิทธิที่จะได้รับการสันนิษฐานไว้ก่อนว่าบริสุทธิ์ตามหลักการสันนิษฐานว่าเป็นผู้บริสุทธิ์ (Presumption of Innocence)โดยโจทก์ผู้ฟ้องคดีมีหน้าที่ต้องพิสูจน์ตามมาตรฐาน “การพิสูจน์พ้นข้อสงสัยตามสมควร” หรือ “Proof Beyond Reasonable Doubt”ให้ศาลเชื่อได้ว่าจำเลยเป็นผู้กระทำผิด หากมีเหตุอันควรสงสัยอย่างใดอย่างหนึ่งว่าจำเลยอาจจะไม่ใช่คนร้ายที่กระทำผิด ศาลจะยกประโยชน์แห่งความสงสัยนั้นให้แก่จำเลยตามนัยประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 227 สำหรับคดีอาชญากรรมคอมพิวเตอร์ซึ่งจัดเป็นคดีอาญาประเภทหนึ่งนั้นรัฐได้ประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 (แก้ไขเพิ่มเติมพ.ศ.2560) เป็นกฎหมายหลักที่ใช้บังคับกับการกระทำความผิดที่เกี่ยวข้องกับคอมพิวเตอร์อย่างไรก็ดี หลักเกณฑ์ว่าด้วยเรื่องการรับฟังพยานหลักฐานในคดีอาชญากรรมคอมพิวเตอร์ รวมถึงอำนาจบางประการของพนักงานสอบสวน ยังคงเป็นไปตามประมวลกฎหมายวิธีพิจารณาความอาญาซึ่งมีการประกาศใช้มาแล้วเป็นเวลาหลายสิบปี เมื่อเทคโนโลยีในโลกไซเบอร์มีพัฒนาการที่ไม่หยุดนิ่ง และอาชญากรรมคอมพิวเตอร์ที่พบในปัจจุบันมีความซับซ้อนมากกว่าในอดีต จึงเป็นความท้าทายของผู้มีส่วนเกี่ยวข้องในกระบวนการยุติธรรมทางอาญาที่จะรวบรวม จัดการ และนำเสนอพยานหลักฐานดิจิทัลในการดำเนินคดีอาชญากรรมคอมพิวเตอร์กับผู้กระทำความผิดเพื่อพิสูจน์ความผิดของผู้ถูกกล่าวหา เพราะหัวใจหลักของการดำเนินคดีอาญานั้น อยู่ที่ความเพียงพอและความสมบูรณ์ของพยานหลักฐานที่ใช้กล่าวหาผู้กระทำความผิด

การวิจัยนี้จึงมุ่งศึกษาสภาพปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ที่พบในชั้นการสืบสวนสอบสวน รวบรวมพยานหลักฐาน จนถึงขั้นตอนการนำเสนอพยานหลักฐานในชั้นพิจารณาของศาลรวมทั้งวิเคราะห์ปัจจัยที่ก่อให้เกิดสภาพปัญหาและอุปสรรคดังกล่าว เพื่อเสนอแนะแนวทางเพิ่มประสิทธิภาพการดำเนินคดีอาชญากรรมคอมพิวเตอร์ อันจะก่อให้เกิดประสิทธิภาพในการดำเนินคดีอาชญากรรมคอมพิวเตอร์เพื่อตอบโต้อาชญากรรมทางไซเบอร์รูปแบบใหม่ๆทั้งในปัจจุบันและในอนาคต

(นายณัฐพงษ์ พุฒแก้ว)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร

หลักสูตรวปอ. รุ่นที่61
ผู้วิจัย

กิตติกรรมประกาศ

เอกสารวิจัยเรื่อง แนวทางเพิ่มประสิทธิภาพการดำเนินคดีอาชญากรรมคอมพิวเตอร์นี้สำเร็จลุล่วงได้ด้วยความกรุณาและความช่วยเหลืออย่างสูงยิ่งจาก พล.ท. ณรงค์ฤทธิ์ หอมอ่อน และ พ.อ. ถนาน ขำวิเศษ อาจารย์ที่ปรึกษาหลักที่ได้กรุณาให้คำปรึกษา แนวทาง และคำแนะนำในการแก้ไขข้อบกพร่องต่างๆของเนื้อหาทุกขั้นตอนของการวิจัย และขอขอบคุณ พ.อ.หญิงจิราพร ชั้นประดับที่ปรึกษาร่วม ที่ได้กรุณาตรวจรูปแบบการพิมพ์เอกสารวิจัย เพื่อให้เอกสารวิจัยนี้มีความครบถ้วนสมบูรณ์ยิ่งขึ้น ผู้วิจัยซาบซึ้งและขอขอบพระคุณเป็นอย่างสูง

ขอขอบคุณ ร.ต.อ.หญิง กชกร เพิงระนัย, ร.ต.อ.หญิง วันทนีย์ ตุลยเสวี, ร.ต.อ. ปฏิภาณ ยืนทนต์, ร.ต.อ. เผ่าภูมิ สมหมาย, ร.ต.อ. ปัญจะ ผลโต, พ.ต.ท. ชานนท์ คำนวณศักดิ์, พ.ต.ท. ดรัณ จาดเจริญ, พ.ต.ท. นิติ อินทลักษณ์, พ.ต.ท. เผ่าภูมิ สมหมาย, พ.ต.ท. อัศว์ณุต แสงทองดี, ท่านอัยการปกรณ์ ธรรมโรจน์และท่านอัยการเบญจพร วัชระวุฒิชัย ผู้ทรงคุณวุฒิด้านการสืบสวนสอบสวน การตรวจพิสูจน์ทางนิติคอมพิวเตอร์ และการดำเนินคดีอาชญากรรมคอมพิวเตอร์ที่ให้ความร่วมมืออย่างดียิ่งในการแบ่งปันข้อมูลที่เป็นประโยชน์อย่างยิ่งเกี่ยวกับปัญหา อุปสรรค และข้อเสนอแนะเกี่ยวกับการปฏิบัติงานสืบสวนสอบสวน การตรวจพิสูจน์ทางนิติคอมพิวเตอร์ และการดำเนินคดีอาชญากรรมคอมพิวเตอร์ผ่านการตอบแบบสอบถามการสัมภาษณ์เชิงลึก (In-depth Interview)

ท้ายที่สุดนี้ ขอขอบคุณสำนักงานอัยการสูงสุดที่ได้มอบโอกาสอันมีค่ายิ่งให้ผู้วิจัยได้มีโอกาสเข้าศึกษาในหลักสูตร วปอ. สถาบันชั้นนำของชาติทางการศึกษาเชิงสหวิทยาการด้านยุทธศาสตร์และความมั่นคง และได้จัดทำเอกสารวิจัยฉบับนี้ ซึ่งผู้วิจัยเชื่อว่าจะเป็นประโยชน์ในการนำไปใช้เป็นแนวทางในการประสิทธิภาพการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในประเทศไทยต่อไป

(นายณัฐพงษ์ พุฒแก้ว)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร วปอ. รุ่นที่61
ผู้วิจัย

สารบัญ

สารบัญ (ต่อ)

หน้า

สารบัญแผนภาพ

หน้า

แผนภาพที่

บทที่ 1
บทนำ

ความเป็นมาและความสำคัญของปัญหา

เป็นเวลามากกว่า 60 ปีที่ประเทศไทยประกาศใช้ประมวลกฎหมายอาญาเป็นกฎหมายสารบัญญัติหลักที่กำหนดให้การกระทำบางอย่างเป็นความผิดทางอาญา และประกาศใช้ประมวลกฎหมายวิธีพิจารณาความอาญา เป็นกฎหมายวิธีสบัญญัติที่กำหนดหลักเกณฑ์วิธีการในการสืบสวนสอบสวน รวบรวมพยานหลักฐาน จัดการให้ได้ตัวผู้กระทำความผิด การสืบพยาน และการพิจารณาคดีในชั้นศาล อย่างไรก็ดีเมื่อพัฒนาการของการกระทำความผิดอาญามีรูปแบบลักษณะที่แตกต่างไปจากความผิดอาญาทั่วไปตามประมวลกฎหมายอาญา รัฐจึงมีความจำเป็นในการประกาศใช้บทบัญญัติกฎหมายเฉพาะเพื่อใช้บังคับกับกรณีอย่างเหมาะสมและเพื่อให้สอดคล้องกับบริบทของสังคมโลกในส่วนของการกระทำความผิดซึ่งใช้เทคโนโลยีคอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด และการกระทำความผิดต่อตัวระบบคอมพิวเตอร์ รัฐได้ประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 โดยในระยะแรกบทบัญญัติดังกล่าวมีต้นแบบมาจากอนุสัญญาบูดาเปสต์ว่าด้วยเรื่องอาชญากรรมทางไซเบอร์ หรือThe Budapest Convention on Cybercrime โดยอนุสัญญาดังกล่าวเป็นเพียงต้นแบบกฎหมายเพื่อให้นานาประเทศได้นำไปปรับใช้ในการบัญญัติกฎหมายภายในประเทศของตน แม้ว่าพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 จะมีผลใช้บังคับ แต่ขณะเวลาดังกล่าวคนไทยจำนวนไม่น้อยยังไม่รู้จักกับสื่อสังคมออนไลน์อย่างเช่น “LINE” “Facebook” “Instagram” “WeChat” “BeeTalk”หรือระบบการชำระเงินหรือธุรกรรมทางการเงินทางอิเล็กทรอนิกส์ อย่าง “Promptpay” “TrueMoney” หรือ“PayPal” ต่อมา รัฐได้ประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ.2560 เพื่อปรับปรุงเนื้อหาสาระของกฎหมายให้เหมาะสมกับสภาพการณ์ในปัจจุบันมากยิ่งขึ้น อย่างไรก็ดี เมื่อคนไทยรู้จักและคุ้นเคยกับธุรกรรมในโลกไซเบอร์เหล่านั้นแล้ว เทคโนโลยีในโลกไซเบอร์ก็ยังคงไม่หยุดนิ่ง เช่นเดียวกับเหล่าอาชญากรที่อาศัยช่องว่างทางเทคโนโลยีและอิสระเสรีในโลกไซเบอร์ปกปิดตัวตนและการกระทำความผิดของตนผ่านนวัตกรรม

ใหม่ๆ ดังเช่นการใช้สกุลเงินถอดรหัส (Cryptocurrency) ในระบบบล็อกเชน (Blockchain) จัดการกับผลประโยชน์ที่ได้จากอาชญากรรมรวมไปถึงการฟอกเงิน ดังนั้นจึงมีความจำเป็นอย่างยิ่งยวดที่เจ้าหน้าที่บังคับใช้กฎหมายในกระบวนการยุติธรรมทางอาญาต้องเร่งสร้างความเข้าใจถึงรูปแบบของระบบปฏิบัติการของเทคโนโลยีรูปแบบใหม่เหล่านี้ เนื่องจากหัวใจหลักของมาตรฐานการพิสูจน์

ความผิดของจำเลยในคดีอาญาตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 227 ที่บัญญัติว่า “ให้ศาลใช้ดุลพินิจวินิจฉัยชั่งน้ำหนักพยานหลักฐานทั้งปวง อย่าพิพากษาลงโทษจนกว่าจะแน่ใจว่ามีการกระทำผิดจริงและจำเลยเป็นผู้กระทำความผิดนั้น เมื่อมีความสงสัยตามสมควรว่าจำเลยได้กระทำผิดหรือไม่ ให้ยกประโยชน์แห่งความสงสัยนั้นให้จำเลย” จึงเป็นความท้าทายของผู้มีส่วนเกี่ยวข้องในกระบวนการยุติธรรมทางอาญาที่จะรวบรวม จัดการ และนำเสนอพยานหลักฐานดิจิทัลในการดำเนินคดีอาชญากรรมคอมพิวเตอร์กับผู้กระทำความผิดเพื่อพิสูจน์ความผิดของผู้ถูกกล่าวหา

อย่างไรก็ดีเนื่องจากในคดีอาชญากรรมคอมพิวเตอร์พยานหลักฐานดิจิทัลถือเป็นพยานหลักฐานที่มีความสำคัญอย่างมาก แต่ด้วยเหตุที่พยานหลักฐานดิจิทัลมีลักษณะอ่อนไหวเสี่ยงต่อการถูกเปลี่ยนแปลงหรือสูญหายได้ง่าย รวมทั้งการเข้าถึงพยานหลักฐานดิจิทัลดังกล่าวซึ่งอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์อาจกระทบต่อสิทธิส่วนบุคคลที่ได้รับความคุ้มครองตามรัฐธรรมนูญ ซึ่งในปัจจุบันประเทศไทยยังไม่มีการบัญญัติกฎหมายวิธีพิจารณาความในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ไว้เป็นการเฉพาะ จึงมีความจำเป็นต้องศึกษาวิเคราะห์สภาพปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ตั้งแต่ชั้นของการสืบสวนสอบสวน รวบรวมพยานหลักฐาน จนถึงขั้นตอนการนำเสนอพยานหลักฐานในชั้นศาล แล้วเสนอแนะแนวทางในการแก้ไขปัญหาอย่างบูรณาการ โดยผลการศึกษานี้จะเป็นข้อมูลเพื่อนำไปสู่การปรับเปลี่ยนกระบวนทัศน์ในการบริหารจัดการคดีอาชญากรรมคอมพิวเตอร์ของหน่วยงานในกระบวนการยุติธรรมทางอาญา ได้แก่ เจ้าพนักงานตำรวจ ผู้ตรวจพิสูจน์พยานหลักฐาน พนักงานอัยการ รวมถึงข้อเสนอแนะในการแก้ไขเพิ่มเติมบทบัญญัติกฎหมายที่เกี่ยวข้อง อันจะก่อให้เกิดประสิทธิภาพในการดำเนินคดีอาชญากรรมคอมพิวเตอร์เพื่อตอบโต้อาชญากรรมทางไซเบอร์รูปแบบใหม่ๆทั้งในปัจจุบันและในอนาคต

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาสภาพปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ที่พบในชั้นการสืบสวนสอบสวน รวบรวมพยานหลักฐาน จนถึงขั้นตอนการนำเสนอพยานหลักฐานในชั้นพิจารณาของศาล

2. เพื่อวิเคราะห์ปัจจัยที่ก่อให้เกิดสภาพปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในปัจจุบัน

3. เพื่อเสนอแนะแนวทางเพิ่มประสิทธิภาพการดำเนินคดีอาชญากรรมคอมพิวเตอร์

ขอบเขตของการวิจัย

1. ขอบเขตด้านเนื้อหา มุ่งเน้นศึกษาปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในส่วนของการใช้เทคโนโลยีระบบคอมพิวเตอร์ในการกระทำความผิดที่สำคัญ อาทิเช่น การกระทำความผิดค้ามนุษย์ และการกระทำความผิดอาชญากรรมทางเศรษฐกิจและการเงินโดยใช้ระบบคอมพิวเตอร์และอุปกรณ์อิเล็กทรอนิกส์เป็นเครื่องมือในการกระทำความผิด ไม่รวมถึงการกระทำความผิดในลักษณะการโจมตีระบบคอมพิวเตอร์ซึ่งเป็นเรื่องของความมั่นคงปลอดภัยทางไซเบอร์

2. ขอบเขตด้านประชากร มุ่งเน้นศึกษาแนวคิดของผู้ทรงคุณวุฒิโดยใช้วิธีการสัมภาษณ์เชิงลึกผู้ทรงคุณวุฒิด้านการสืบสวนสอบสวน การตรวจพิสูจน์ทางนิติคอมพิวเตอร์ และการดำเนินคดีอาชญากรรมคอมพิวเตอร์ รวม 12 คน

วิธีดำเนินการวิจัย

การวิจัยนี้เป็นการวิจัยเชิงคุณภาพ โดยมีการดำเนินการดังนี้

1. การรวบรวมข้อมูล

1.1 ข้อมูลทุติยภูมิ (Secondary Data) เป็นการศึกษา แนวคิด ทฤษฎี บทบัญญัติกฎหมาย รวมถึงเอกสารและงานวิจัยที่เกี่ยวข้องที่มีเนื้อหาเกี่ยวกับทฤษฎีอาชญาวิทยาทฤษฎีการรับฟังพยานหลักฐานในคดีอาญาลักษณะและรูปแบบของอาชญากรรมคอมพิวเตอร์กฎหมายที่สำคัญในการดำเนินคดีอาชญากรรมคอมพิวเตอร์และหลักกฎหมายเกี่ยวกับพยานหลักฐานในคดีอาญา

1.2 ข้อมูลปฐมภูมิ (Primary Data)ดำเนินการศึกษาและเก็บรวบรวมข้อมูลภาคสนาม โดยใช้วิธีการสัมภาษณ์และแลกเปลี่ยนเรียนรู้กับกลุ่มผู้ให้ข้อมูลสำคัญที่ได้กำหนดเอาไว้ในหัวข้อขอบเขตของการวิจัย ข้อ 1 เพื่อสำรวจความคิดเห็นและข้อเสนอแนะจากเจ้าพนักงานผู้ทรงคุณวุฒิด้านการสืบสวนสอบสวน การตรวจพิสูจน์ทางนิติคอมพิวเตอร์ และการดำเนินคดีอาชญากรรมคอมพิวเตอร์ โดยใช้วิธีการสัมภาษณ์ข้อมูลเชิงลึก (In-depth Interview) จากกลุ่มตัวอย่างทั้งในกรุงเทพมหานคร และต่างจังหวัด

2. การวิเคราะห์ข้อมูล

ดำเนินการโดยการนำเอาข้อมูลที่ได้จากการศึกษาลักษณะและรูปแบบของอาชญากรรมคอมพิวเตอร์ในปัจจุบัน ทฤษฎี แนวคิดและหลักกฎหมายเกี่ยวกับการรับฟังพยานหลักฐานในคดีอาญาและการดำเนินคดีอาชญากรรมคอมพิวเตอร์มาพิจารณาร่วมกับข้อมูลผลการสัมภาษณ์เชิงลึกเจ้าพนักงานตำรวจ ผู้ตรวจพิสูจน์หลักฐาน และพนักงานอัยการ ผู้ทรงคุณวุฒิ (ข้อมูลปฐมภูมิ) โดยใช้วิธีการประสมประสานข้อมูลเข้าด้วยกัน แล้วนำข้อมูลที่ได้จากการวิเคราะห์ดังที่ได้กล่าวมาทั้งหมดมาใช้วิเคราะห์ปัจจัยที่ทำให้เกิดสภาพปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ เพื่อเสนอแนะแนวทางเพิ่มประสิทธิภาพในการดำเนินคดีอาชญากรรม

คอมพิวเตอร์ โดยนำหลักการ ทฤษฎีและแนวคิด มารองรับข้อสรุปจากการศึกษาวิจัยอย่างเป็นเหตุเป็นผลและนำไปปฏิบัติได้จริง

ประโยชน์ที่ได้รับจากการวิจัย

1. ทำให้ทราบสภาพปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ที่พบในชั้นการสืบสวนสอบสวน รวบรวมพยานหลักฐาน จนถึงขั้นตอนการนำเสนอพยานหลักฐานในชั้นพิจารณาของศาล

2. ทำให้ทราบปัจจัยที่ก่อให้เกิดสภาพปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในปัจจุบัน

3. ทำให้ได้แนวทางเพิ่มประสิทธิภาพการดำเนินคดีอาชญากรรมคอมพิวเตอร์

คำจำกัดความ

ไซเบอร์	หมายถึง	สิ่งที่เกี่ยวข้องกับระบบเครือข่ายและสังคมเครือข่ายสากลทั่วโลก เช่น ระบบอินเทอร์เน็ต โดยเป็นคำที่ลดรูปมาจากคำว่า ไซเบอร์เนติกส์ (Cybernetics)
ธุรกรรมอิเล็กทรอนิกส์	หมายถึง	ธุรกรรมที่กระทำขึ้นโดยใช้วิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือแต่บางส่วน การทำธุรกรรมผ่านสื่อเล็กทรอนิกส์ ได้แก่ ระบบเครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต และระบบโทรศัพท์เคลื่อนที่ ครอบคลุมการทำธุรกรรมตั้งแต่การชำระเงินทางอิเล็กทรอนิกส์ การซื้อขายสินค้าและบริการทางอิเล็กทรอนิกส์ เป็นต้น
พยานหลักฐานดิจิทัล	หมายถึง	พยานหลักฐานจากอุปกรณ์ดิจิทัลหรือข้อมูลและข้อมูลจราจรที่เกี่ยวข้อง
พาณิชย์ทางอิเล็กทรอนิกส์	หมายถึง	การประกอบธุรกิจ ดังต่อไปนี้ 1. การเสนอซื้อหรือขายสินค้าหรือบริการ โดยวิธีใช้สื่ออิเล็กทรอนิกส์ผ่านระบบเครือข่ายอินเทอร์เน็ต 2. การให้บริการอินเทอร์เน็ต 3. การให้เช่าพื้นที่ของเครื่องคอมพิวเตอร์ผ่านแม่ข่าย

		4. การบริการเป็นตลาดกลางในการซื้อขายสินค้าหรือบริการ โดยวิธีใช้สื่ออิเล็กทรอนิกส์ผ่านระบบเครือข่ายอินเทอร์เน็ต 5. การทำธุรกรรมโดยวิธีใช้สื่ออิเล็กทรอนิกส์อื่น ตามที่กรมพัฒนาธุรกิจการค้าประกาศกำหนด
ระบบคอมพิวเตอร์	หมายถึง	อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
สังคมออนไลน์	หมายถึง	สังคมออนไลน์ที่มีผู้ใช้เป็นผู้สื่อสาร หรือเขียนเล่าเนื้อหาเรื่องราว ประสบการณ์ บทความ รูปภาพ และวีดีโอที่ผู้ใช้เขียนขึ้นเอง ทำขึ้นเอง หรือพบเจอจากสื่ออื่นๆ แล้วนำมาแบ่งปันให้กับผู้อื่นที่อยู่ในเครือข่ายของตนผ่านทางเว็บไซต์ เครือข่ายสังคม (social network) ที่ให้บริการบนอินเทอร์เน็ต
อาชญากรรมคอมพิวเตอร์	หมายถึง	อาชญากรรมซึ่งมีลักษณะของการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ แต่ในงานวิจัยนี้มุ่งหมายให้หมายถึงการกระทำความผิดอาญาที่ใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด

บทที่ 2
แนวคิดและทฤษฎีการดำเนินคดีอาชญากรรมคอมพิวเตอร์

ประเทศไทยได้ประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 (แก้ไขเพิ่มเติม พ.ศ.2560) อันเป็นกฎหมายสารบัญญัติ เพื่อกำหนดให้การกระทำบางส่วนต่อระบบคอมพิวเตอร์หรือการใช้คอมพิวเตอร์เป็นเครื่องมือในการก่ออาชญากรรมอย่างอื่นเป็นความผิดที่มีโทษทางอาญาซึ่งพระราชบัญญัติฉบับดังกล่าวเป็นที่รู้จักกันในฐานะที่เป็นกฎหมายหลักในการจัดการกับอาชญากรรมคอมพิวเตอร์ (Cybercrime)แต่ทว่าเมื่อหัวใจหลักของการดำเนินคดีจนไปสู่การลงโทษผู้กระทำผิดอยู่ที่การพิสูจน์ความผิดของผู้ถูกกล่าวหา ดังนั้นตัวแปรสำคัญของประสิทธิภาพในการดำเนินคดีอาชญากรรมคอมพิวเตอร์จึงอยู่ที่การรวบรวมพยานหลักฐานในคดี คุณภาพของพยานหลักฐาน เทคนิคการนำเสนอพยานหลักฐานในชั้นศาลให้ได้ตามมาตรฐานการรับฟังพยานหลักฐานเพื่อลงโทษผู้ถูกกล่าวหา

การวิจัยนี้จึงมีวัตถุประสงค์เพื่อศึกษาสภาพปัญหาและอุปสรรคในการดำเนินคดีอาญาที่พบในชั้นสืบสวนสอบสวน รวบรวมพยานหลักฐาน รวมถึงขั้นตอนการนำเสนอพยานหลักฐานในชั้นศาลเพื่อทำการวิเคราะห์หาแนวทางเพิ่มประสิทธิภาพการดำเนินคดีอาชญากรรมคอมพิวเตอร์ โดยในบทที่ 2 นี้ผู้วิจัยได้ทบทวนวรรณกรรมที่เกี่ยวข้องครอบคลุมเนื้อหาเกี่ยวกับแนวคิด ทฤษฎี และหลักกฎหมายที่เกี่ยวข้องกับรูปแบบของอาชญากรรมคอมพิวเตอร์ที่พบเจอในปัจจุบัน การดำเนินคดีอาชญากรรมคอมพิวเตอร์ และหลักการรับฟังพยานหลักฐานของศาลไทย เพื่อเป็นข้อมูลพื้นฐานสำหรับการศึกษาวิจัยในบทต่อๆไป โดยมีลำดับการศึกษาดังนี้

1. แนวคิดและทฤษฎีอาชญาวิทยา
2. แนวคิดและทฤษฎีการรับฟังพยานหลักฐานในคดีอาญา
3. ลักษณะและรูปแบบของอาชญากรรมคอมพิวเตอร์
4. อำนาจหน้าที่ของเจ้าพนักงานในกระบวนการยุติธรรมทางอาญา
5. กฎหมายที่สำคัญในการดำเนินคดีอาชญากรรมคอมพิวเตอร์
6. หลักกฎหมายเกี่ยวกับพยานหลักฐานในคดีอาญา
7. วรรณกรรมและผลงานวิจัยที่เกี่ยวข้อง
8. กรอบแนวคิดของการวิจัย
9. สรุป

แนวคิดและทฤษฎีอาชญาวิทยา

1. ระบบการดำเนินคดีอาญา

การดำเนินคดีอาญาโดยใช้พยานหลักฐานพิสูจน์ความจริง ในเชิงทฤษฎีแบ่งออกเป็น 2 ระบบ (ดวงใจ สิงหนาท, 2555 : 4-5 ; ประมูล สุวรรณศร, 2526 : 2 ; ภัทรศักดิ์ วรรณแสง, ออนไลน์, 2562) คือ

1.1 ระบบไต่สวนหรือ Inquisitorial System หมายถึงระบบการดำเนินคดีอาญาแบบการค้นหาข้อเท็จจริงจากการนำสืบพยานหลักฐาน โดยในระบบนี้เปิดโอกาสให้คู่ความเสนอพยานหลักฐานทุกชนิดมาสู่ศาลได้โดยไม่มีบทตัดพยานที่เคร่งครัดทำให้ศาลมีความสามารถใช้ดุลพินิจได้อย่างกว้างขวางและมีอำนาจค้นหาข้อเท็จจริงด้วยตนเองได้ เพื่อให้ได้ข้อเท็จจริงครบถ้วนมากที่สุด ส่วนการดำเนินคดีในศาล ผู้พิพากษาจะเป็นผู้ดำเนินการซักถามพยาน ประเทศที่ใช้ระบบไต่สวนมักอยู่ในภาคพื้นยุโรป ได้แก่ ประเทศฝรั่งเศส ประเทศเยอรมัน ประเทศสวิตเซอร์แลนด์ เป็นต้น

1.2 ระบบกล่าวหาหรือAccusatorial System หมายถึงระบบการดำเนินคดีอาญาแบบค้นหาข้อเท็จจริงซึ่งคู่ความมีหน้าที่นำเสนอพยานหลักฐานต่อศาลเช่นเดียวกันกับระบบไต่สวน แต่ผู้พิพากษาจะวางตัวเป็นกลางโดยเคร่งครัด ปล่อยให้คู่ความแต่ละฝ่ายมีหน้าที่แสวงหาพยานหลักฐานและนำสืบพยานหลักฐานตามข้อกล่าวอ้างเอง โดยมีกฎหมายลักษณะพยานหลักฐาน กำหนดว่าข้อเท็จจริงใดบ้างที่ศาลพึงรับฟังหรือไม่อาจรับฟัง รวมทั้งกำหนดวิธีการในการนำสืบพยานหลักฐานไว้ด้วย ประเทศที่ใช้ระบบกล่าวหานี้ได้แก่ ประเทศอังกฤษ สหรัฐอเมริกา แคนาดา ออสเตรเลีย นิวซีแลนด์ มาเลเซีย สิงคโปร์ เป็นต้น

สำหรับประเทศไทยนำระบบกล่าวหาและระบบไต่สวนมาใช้ในระบบการพิจารณาคดีและการสืบพยานอย่างผสมผสานกัน กล่าวคือ เป็นหน้าที่ของคู่ความทั้งสองฝ่ายต่างต้องแสวงหาพยานหลักฐานมาต่อสู้หักล้างกันเองส่วนศาลจะวางตนเป็นกลางโดยพิจารณาและพิพากษาคดีจากพยานหลักฐานที่ทั้งโจทก์และจำเลยนำสืบมา อันเป็นลักษณะของระบบกล่าวหา แต่ก็นำกฎเกณฑ์การห้ามรับฟังพยานหลักฐานบางประเภทมาบังคับใช้เพื่อทำให้พยานหลักฐานที่มีน้ำหนักรับฟังในการลงโทษผู้ถูกกล่าวหาเป็นพยานหลักฐานที่น่าเชื่อถือ อันเป็นลักษณะของระบบไต่สวน

2. ข้อสันนิษฐานการเป็นผู้บริสุทธิ์ (Presumption of Innocence)

ในบทความของวศิน แดงประดับ (ออนไลน์, 2562) ได้กล่าวถึงคำกล่าวที่ว่า “มันดีกว่าที่จะปล่อยให้คนผิดสิบคนลอยนวลเมื่อเทียบกับการลงโทษคนบริสุทธิ์หนึ่งคน” คำกล่าวนี้มักถูก

หยิบยกขึ้นวิพากษ์บ่อยครั้งเมื่อต้องเผชิญกับความรู้สึกไม่แน่ใจว่าผู้ถูกกล่าวหาว่ากระทำความผิดนั้นเป็นคนร้ายที่แท้จริงหรือเป็นเพียงแพะที่ไม่สามารถพิสูจน์ความบริสุทธิ์ของตนในกระบวนการยุติธรรมทางอาญาได้ดังนั้นเพื่อให้แน่ใจอย่างที่สุดว่าศาลจะไม่ตัดสินลงโทษผู้บริสุทธิ์ผิดพลาดไป บุคคลผู้ถูกกล่าวหาว่ากระทำความผิดอาญาจึงสมควรได้รับการสันนิษฐานว่าเป็นผู้บริสุทธิ์จนกว่าความผิดนั้นจะถูกพิสูจน์โดยผู้ที่กล่าวหา

ในปัจจุบัน หลักข้อสันนิษฐานการเป็นผู้บริสุทธิ์ (Presumption of Innocence)ได้รับการรับรองไว้ในกฎหมายระหว่างประเทศ UniversalDeclaration of HumanRights (หรือ UDHR) Article 11(1) บัญญัติว่า

Everyone charged with a penal offence has the right to be presumed innocent until proved guilty according to law in a public trial at which he has had all the guarantees necessary for his defence.

แปลเป็นไทยได้ว่า

บุคคลซึ่งถูกกล่าวหาว่ามีความผิดอาญามีสิทธิที่จะได้รับการสันนิษฐานไว้ก่อนว่าบริสุทธิ์ จนกว่าจะมีการพิสูจน์ว่ามีความผิดตามกฎหมายโดยกระบวนพิจารณาที่เปิดเผย และผู้นั้นได้รับหลักประกันทั้งหลายที่จำเป็นในการต่อสู้คดี

หลักการสันนิษฐานการเป็นผู้บริสุทธิ์จัดเป็นสิทธิมนุษยชนขั้นพื้นฐานสำหรับผู้ถูกกล่าวหาในคดีอาญาหรือจำเลยในคดีอาญา สำหรับประเทศไทย มองหลักการสันนิษฐานการเป็นผู้บริสุทธิ์(Presumption of Innocence)ว่าเป็นหลักเสรีภาพที่แฝงอยู่ในกระบวนการยุติธรรมทางอาญาซึ่งไม่ได้จำกัดอยู่เพียงกระบวนการพิจารณาในศาลเท่านั้น แต่ขยายออกไปถึงกระบวนการยุติธรรมทางอาญาทั้งระบบ อันรวมถึงกระบวนการสืบสวนสอบสวนของเจ้าหน้าที่ตำรวจด้วย อาทิเช่น **รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560** (ออนไลน์, 2562) **มาตรา 29** บัญญัติว่า

บุคคลไม่ต้องรับโทษอาญา เว้นแต่ได้กระทำการอันกฎหมายที่ใช้อยู่ในเวลาที่กระทำนั้นบัญญัติเป็นความผิดและกำหนดโทษไว้ และโทษที่จะลงแก่บุคคลนั้นจะหนักกว่าโทษที่บัญญัติไว้ในกฎหมายที่ใช้อยู่ในเวลาที่กระทำความผิดมิได้

ในคดีอาญา ให้สันนิษฐานไว้ก่อนว่าผู้ต้องหาหรือจำเลยไม่มีความผิด และก่อนมีคำพิพากษาอันถึงที่สุดแสดงว่าบุคคลใดได้กระทำความผิด จะปฏิบัติต่อบุคคลนั้นเสมือนเป็นผู้กระทำความผิดมิได้

การควบคุมหรือคุมขังผู้ต้องหาหรือจำเลยให้กระทำได้เพียงเท่าที่จำเป็น เพื่อป้องกันมิให้มีการหลบหนี

ในคดีอาญา จะบังคับให้บุคคลให้การเป็นปฏิปักษ์ต่อตนเองมิได้

คำขอประกันผู้ต้องหาหรือจำเลยในคดีอาญาต้องได้รับการพิจารณาและจะเรียกหลักประกันจนเกินควรแก่กรณีมิได้ การไม่ให้ประกันต้องเป็นไปตามที่กฎหมายบัญญัติและ**ประมวลกฎหมายวิธีพิจารณาความอาญา** (ออนไลน์, 2562)**มาตรา 227** บัญญัติว่า

ให้ศาลใช้ดุลพินิจวินิจฉัยชั่งน้ำหนักพยานหลักฐานทั้งปวง อย่าพิพากษาลงโทษจนกว่าจะแน่ใจว่ามีการกระทำผิดจริงและจำเลยเป็นผู้กระทำความผิดนั้น

เมื่อมีความสงสัยตามสมควรว่าจำเลยได้กระทำผิดหรือไม่ ให้ยกประโยชน์แห่งความสงสัยนั้นให้จำเลย

โดยศาลรัฐธรรมนูญได้เคยมีการวินิจฉัยคดีกล่าวถึงหลักข้อสันนิษฐานว่าเป็นผู้บริสุทธิ์ (Presumption of Innocence)ไว้ใน**คำวินิจฉัยศาลรัฐธรรมนูญที่ 11/2554** (ราชกิจจานุเบกษา, 2545 : 108) ซึ่งได้อธิบายถึงหลักการสันนิษฐานการเป็นผู้บริสุทธิ์ว่ารัฐธรรมนูญ มาตรา 33 เป็นบทบัญญัติที่รับรองหลักการขั้นพื้นฐานของกฎหมายอาญาของนานาประเทศ มีเจตนารมณ์เพื่อรับรองและคุ้มครองสิทธิและเสรีภาพขั้นพื้นฐานของบุคคลซึ่งตกเป็นผู้ต้องหาหรือจำเลยในคดีอาญาทั่วไป ซึ่งมีหลักการว่า ในคดีอาญาโจทก์มีภาระต้องนำสืบการกระทำของผู้ต้องหาหรือจำเลยให้ครบทุกองค์ประกอบแห่งความผิดตามที่กฎหมายบัญญัติไว้ โดยผู้ต้องหาหรือจำเลยไม่จำเป็นต้องนำหลักฐานมาพิสูจน์ความบริสุทธิ์ของตน และตราบใดยังไม่มีคำพิพากษาอันถึงที่สุดแสดงว่าได้กระทำความผิด บุคคลนั้นจะได้รับความคุ้มครองตลอดไป เจ้าหน้าที่ของรัฐจะปฏิบัติต่อผู้ต้องหาหรือจำเลยเสมือนเป็นผู้กระทำความผิดมิได้

แนวคิดและทฤษฎีการรับฟังพยานหลักฐานในคดีอาญา

1. ข้อสันนิษฐานตามกฎหมายในคดีอาญา

ในกรณีทั่วไปหากคู่ความประสงค์ให้ศาลรับฟังข้อเท็จจริงไปในทางใดภาระพิสูจน์ย่อมตกแก่คู่ความฝ่ายนั้นในการนำสืบพยานหลักฐานให้ศาลเชื่อว่าข้อเท็จจริงนั้นเป็นความจริง เว้นแต่จะเป็นข้อเท็จจริงที่ไม่ต้องพิสูจน์ เช่น ข้อเท็จจริงซึ่งรู้กันอยู่ทั่วไปโดยเฉพาะในคดีอาญาโจทก์มีหน้าที่นำสืบพยานหลักฐานเพื่อพิสูจน์ว่าจำเลยเป็นผู้กระทำความผิด อย่างไรก็ดี การสืบพยานให้ได้มาตรฐานการพิสูจน์พอที่ศาลจะลงโทษผู้กระทำผิดในกรณีที่ข้อเท็จจริงอยู่ในความรับรู้ของจำเลยฝ่ายเดียวเป็นไปได้ยากมาก ดังนั้นเพื่อความเป็นธรรมแห่งคดีจึงมีการสร้างหลักกฎหมายเรื่อง “ข้อสันนิษฐาน” ขึ้นมาเพื่อช่วยบรรเทาภาระการพิสูจน์ดังกล่าว โดยโจทก์ในคดีอาญาไม่จำต้องแสดงพยานหลักฐานเพื่อชี้ให้เห็นว่ามีข้อเท็จจริงอย่างหนึ่งอย่างใดซึ่งยากแก่การนำสืบโดยตรง เพียงแต่พิสูจน์ให้เห็นว่ามีข้อเท็จจริงอย่างหนึ่งอย่างใด (Basic Fact)เพื่อโน้มน้าวให้ศาลเชื่อว่ามีข้อเท็จจริงที่ประสงค์จะพิสูจน์ (Presumed Fact) เกิดขึ้นแล้ว (วศิน แดงประดับ, ออนไลน์, 2562) ข้อสันนิษฐานแบ่งออกเป็น 2 ประเภท คือ

1.1 ข้อสันนิษฐานตามความเป็นจริง ซึ่งเกิดจากการใช้ดุลพินิจประกอบตรรกะของศาล เช่น ในความผิดฐานรับของโจรนั้น การจะพิสูจน์ให้ศาลเชื่อว่าจำเลยมีเจตนารับของโจรนั้น โจทก์อาจนำสืบพยานหลักฐานให้ศาลเห็นว่าราคาทรัพย์ตามท้องตลาดสูงกว่าราคาที่จำเลยรับซื้ออย่างผิดปกติและน่าเชื่อว่าจำเลยรู้ว่าเป็นทรัพย์ที่รับโอนได้มาจากการกระทำความผิด

1.2 ข้อสันนิษฐานตามกฎหมาย เป็นกรณีที่กฎหมายได้บัญญัติชัดเจนว่าเมื่อมีข้อเท็จจริงอย่างหนึ่งอย่างใดเกิดขึ้นแล้ว ให้สันนิษฐานว่ามีข้อเท็จจริงอีกอย่างหนึ่งเกิดขึ้นด้วย โดยข้อสันนิษฐานตามกฎหมายนี้มีทั้งที่เป็นข้อสันนิษฐานที่หักล้างได้ กับข้อสันนิษฐานเด็ดขาดขึ้นอยู่กับเจตนารมณ์ของกฎหมายเรื่องนั้นๆ

2. หลักมาตรฐานการพิสูจน์ (Standard of Proof)

ระบบการดำเนินคดีอาญาของไทยใช้ระบบกล่าวหาซึ่งฝ่ายโจทก์มีหน้าที่สืบนำเสนอพยานหลักฐานต่อศาลเพื่อให้ศาลรับฟังได้ว่าจำเลยเป็นผู้กระทำผิดกฎหมายตามข้อกล่าวหา ในการนำเสนอพยานหลักฐานในชั้นศาลนั้น ประเด็นสำคัญประการแรกที่ต้องทำความเข้าใจคือ มาตรฐานการพิสูจน์ที่โจทก์ต้องใช้ในการดำเนินคดีอาชญากรรมคอมพิวเตอร์นั้นอยู่ในระดับใดซึ่งมาตรฐานการพิสูจน์นี้จะเป็นภาพรวมภาระหน้าที่ของโจทก์ที่จะต้องดำเนินการในชั้นพิจารณา เพื่อนำไปสู่ขั้นตอนการใช้ดุลพินิจของศาลในการวินิจฉัยปัญหาข้อเท็จจริงและวิเคราะห์ชั่งน้ำหนักพยานหลักฐานในแต่ละคดีได้อย่างมีหลักมีเกณฑ์

มาตรฐานการพิสูจน์ในคดีแต่ละประเภทและแต่ละชั้นในกระบวนพิจารณานั้นแตกต่างกัน (จรัญภักดีธนากุล, 2561 : 296-302 ; วศิน แดงประดับ, ออนไลน์, 2562) ในภาพรวมสามารถแบ่งได้เป็น

1. มาตรฐานการพิสูจน์ในคดีอาญา (Proof Beyond Reasonable Doubt)

2. มาตรฐานการพิสูจน์ในคดีแพ่ง (Proof on the Balance of Probabilityหรือ on the Balance of Preponderance) ซึ่งเป็นมาตรฐานที่ต่ำกว่าการพิสูจน์คดีอาญา มาตรฐานการพิสูจน์ในระดับนี้ยังไม่มีการบัญญัติให้ชัดเจนในกฎหมายไทย แต่ปรากฏในทางตำราและบรรทัดฐานคำพิพากษาฎีกา เมื่อศาลชั่งน้ำหนักพยานหลักฐานแล้วเห็นว่าพยานหลักฐานของโจทก์มีน้ำหนักน่าเชื่อถือมากกว่าพยานหลักฐานของจำเลย ก็จะพิพากษาให้โจทก์เป็นฝ่ายชนะคดี

3. มาตรฐานการพิสูจน์ให้เห็นโดยพยานหลักฐานที่ชัดเจนและมีความน่าเชื่อถือ (Proof by Clear and Convincing Evidence) เป็นมาตรฐานที่อยู่กึ่งกลางสูงกว่ามาตรฐานการพิสูจน์ในคดีแพ่งทั่วไป แต่ไม่สูงถึงมาตรฐานการพิสูจน์ในคดีอาญา สำหรับประเทศไทยพบในประมวลกฎหมายวิธีพิจารณาความแพ่ง มาตรา 254 ในกรณีที่โจทก์ในคดีแพ่งร้องขอใช้วิธีการชั่วคราวก่อนที่ศาลจะมีคำพิพากษา

4. มาตรฐานการพิสูจน์ให้เห็นมูลความแห่งคดี (Proof of Prima Facie Case or Probable Cause) เป็นมาตรฐานการพิสูจน์ในระดับที่ต่ำที่สุดในทางกฎหมายพยานหลักฐาน คือ ไม่จำเป็นต้องแสดงให้เห็นถึงความโน้มเอียงว่าจะเป็นเช่นนั้นจริงๆ เพียงแค่ชี้ให้เห็นเหตุที่น่าเชื่อถือได้ก็เพียงพอแล้ว ปรากฏอยู่ในบทบัญญัติในชั้นไต่สวนมูลฟ้องคดีอาญาในคดีที่ราษฎรเป็นโจทก์ฟ้องคดีอาญา และกรณีมาตรฐานในการอนุมัติออกหมายค้น หมายจับ หมายขังของศาล

กล่าวโดยละเอียดเกี่ยวกับ **มาตรฐานในการพิสูจน์คดีอาญา (Proof Beyond Reasonable Doubt)**ซึ่งปรากฏอยู่ในประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 227 ที่กล่าวมาข้างต้น ถือได้ว่าเป็นมาตรฐานที่สูงที่สุดในระบบกฎหมายปัจจุบัน สอดคล้องกับหลักข้อสันนิษฐานว่าบุคคลทุกคนเป็นผู้บริสุทธิ์ (Presumption of Innocence) กล่าวคือ โจทก์มีหน้าที่ต้องพิสูจน์ให้ศาลเห็นได้โดยปราศจากเหตุอันควรสงสัยว่าจำเลยเป็นผู้กระทำผิดรายนี้ ถ้ามีเหตุอันควรสงสัยอย่างใดอย่างหนึ่งว่าจำเลยอาจจะไม่ใช่คนร้ายที่กระทำผิด ให้ยกประโยชน์แห่งความสงสัยนั้นให้แก่จำเลย หมายถึง ให้ศาลพิพากษายกฟ้องไป

มาตรฐานที่เรียกว่า Proof Beyond Reasonable Doubt แปลเป็นไทยได้ว่า มาตรฐาน “การพิสูจน์พ้นข้อสงสัยตามสมควร” ในกฎหมายต่างประเทศมีการวางบรรทัดฐานชัดเจนว่ามาตรฐานนี้ไม่ใช่ Proof Beyond any Doubt หรือ “การพิสูจน์พ้นทุกข้อสงสัย”เพราะการพิสูจน์พ้นทุกข้อสงสัยไม่อาจทำได้ในความเป็นจริง เหตุที่มาตรฐานการพิสูจน์เพื่อเอาผิดแก่จำเลยในคดีอาญาสูงกว่ามาตรฐานการพิสูจน์ในคดีแพ่งเป็นเพราะความเสียหายอันเกิดจากความผิดพลาดของคำพิพากษาในคดีอาญาอาจเกิดกับชีวิต เสรีภาพ หรือชื่อเสียงของบุคคล รวมไปถึงหน้าที่การงานของจำเลย (โดยเฉพาะจำเลยที่เป็นข้าราชการ) ซึ่งร้ายแรงยิ่งกว่าที่เกิดในคดีแพ่ง ด้วยเหตุนี้เพื่อเป็นการลดความเสี่ยงในการรับฟังพยานหลักฐานในคดีอาญาที่ผิดพลาดให้เกิดขึ้นน้อยที่สุดจึงมีความจำเป็นต้องใช้มาตรฐานการพิสูจน์พ้นข้อสงสัยตามสมควร (Proof Beyond Reasonable Doubt) นั่นเอง

อย่างไรก็ดี (David Hamer2007 : 147 อ้างถึงใน วศิน แดงประดับ, ออนไลน์, 2562)มีมุมมองว่า การให้ความคุ้มครองแก่ผู้ถูกกล่าวหาหรือจำเลยตามหลัก Presumption of Innocence และหลัก Proof Beyond Reasonable Doubt โดยไม่มีข้อยกเว้นใดๆนั้น เป็นเสมือนเหรียญสองด้านดาบสองคม เพราะบุคคลอื่นในสังคมซึ่งถือเป็นผู้บริสุทธิ์เช่นเดียวกันอาจไม่ได้รับการปกป้องจากผู้ไม่บริสุทธิ์ซึ่งได้รับการปกป้องจากกฎหมาย โดยสังคมเองย่อมได้รับความเสียหายจากการปล่อยคนผิดสิบคนให้กลับมาอยู่ในสังคมเช่นเดียวกัน แม้ว่าการกำหนดมาตรฐานการพิสูจน์ในคดีอาญาในระดับที่สูงสามารถลดความเสี่ยงที่จะเกิดคำพิพากษาลงโทษโดยผิดพลาด แต่ก็เพิ่มโอกาสที่จะเกิดคำพิพากษายกฟ้องที่ผิดพลาดได้เช่นเดียวกัน ในมุมมองของ David Hamerคำพิพากษายกฟ้อง (Acquittal) ที่ผิดพลาด มีผลเสียมากกว่าคำพิพากษาลงโทษ (Conviction) ที่ผิดพลาด คำพิพากษายกฟ้องไม่ก่อให้เกิด

ผลในทางห้ามปราม ในขณะที่คำพิพากษาลงโทษ แม้ในกรณีที่ผิดพลาดก็ยังก่อให้เกิดผลในทางห้ามปรามที่เป็นประโยชน์ต่อสังคมโดยรวม

ลักษณะและรูปแบบของอาชญากรรมคอมพิวเตอร์

อาชญากรรมคอมพิวเตอร์ที่พบมากในปัจจุบันสามารถจำแนกกลุ่มลักษณะของความผิดได้ดังนี้

1. กลุ่มความผิดที่คอมพิวเตอร์เป็นวัตถุหรือเป้าหมายที่ถูกกระทำ (Computer as Targets)

หมายถึง การกระทำความผิดเกี่ยวกับคอมพิวเตอร์โดยตรง ซึ่งผู้กระทำมีเจตนาที่จะกระทำต่อระบบคอมพิวเตอร์ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์โดยตรง มุ่งก่อให้เกิดความเสียหายแก่ผู้เป็นเจ้าของ ผู้ให้บริการ ผู้ใช้บริการ หรือประชาชนทั่วไป โดยมีบทบัญญัติกำหนดลักษณะของฐานความผิดไว้ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550(ที่แก้ไขเพิ่มเติม) ตัวอย่างเช่น ความผิดฐานเข้าถึงระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะโดยมิชอบ (Illegal access หรือ Hacking) ความผิดฐานดักรับข้อมูลคอมพิวเตอร์โดยมิชอบ (Illegal Interception หรือ Sniffing)ความผิดฐานเปลี่ยนแปลงหน้าเว็บไซต์โดยใช้การเข้าถึงโดยมิชอบ (Web Defacement)ความผิดฐานรบกวนหรือขัดขวางระบบคอมพิวเตอร์ (System Inference) หรือทำให้ระบบไม่สามารถทำงานได้ตามปกติ (Denial of Service) เป็นต้น

รูปแบบที่น่าสนใจของอาชญากรรมลักษณะนี้ ได้แก่

1.1 การแฮก (Hacking)

หมายถึงการเจาะระบบหรือการบุกรุกทางคอมพิวเตอร์ (Computer Trespass) ซึ่งพระราชบัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 (แก้ไขเพิ่มเติม พ.ศ.2560) มาตรา 5 ได้กำหนดว่าการเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน จัดเป็นการกระทำความผิดฐานเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ ทั้งนี้ การกระทำที่จะเป็นความผิดมาตราดังกล่าวจะต้องเป็นการเจาะเข้าไปในระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน เช่น การเจาะผ่านระบบ “ไฟร์วอลล์ (Firewall)” ซึ่งเป็นระบบป้องกันการเข้าถึงหรือรักษาความปลอดภัยของระบบเครือข่าย (Network) ด้วย (สราวุธปิติยาศักดิ์, 2661 : 58-59)

ตัวอย่างคดีแรกๆที่โด่งดังและทำให้คนไทยรู้จักกับคำว่า “แฮก” คือ คดีแฮกระบบเติมเงินของทรูมูฟ(สราวุธปิติยาศักดิ์, 2661 : 58-59 ;ศาลฎีกามีคำพิพากษา จำคุกแฮกเกอร์

ฐานแก้ไขวงเงิน ระบบเติมเงินทรูมูฟ, ออนไลน์, 2562) กล่าวคือ เมื่อเดือนสิงหาคม พ.ศ.2548(ก่อนที่พระราชบัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จะประกาศใช้) มีแฮกเกอร์ 3 คน ซึ่งเคยเป็นพนักงานของบริษัท ทรูคอร์ปอเรชั่น จำกัด (มหาชน) ใช้คอมพิวเตอร์โน้ตบุ๊กจากที่พักของตนโจรกรรมข้อมูลรหัสผู้ใช้และรหัสผ่านทางคอมพิวเตอร์ แล้วเข้าระบบฐานข้อมูลของบริษัท ทีเอ ออเรนจ์ จำกัด ซึ่งเป็นชื่อเดิมของบริษัท ทรูคอร์ปอเรชั่น จำกัด (มหาชน) เพื่อเข้าไปแก้ไขวงเงินการใช้โทรศัพท์เคลื่อนที่แบบเติมเงินให้มีมูลค่าสูงขึ้นกว่าเดิม และนำไปขายลูกค้าด้วยวิธีการตั้งจุดรับเติมเงินต่างๆตามห้างสรรพสินค้าและแหล่งชุมชน ตัวอย่างเช่น บัตรเติมเงินที่มีราคาโทรออกหนึ่งร้อยบาท แฮกเกอร์จะใส่ข้อมูลให้กลายเป็นหนึ่งหมื่นหรือหนึ่งแสนบาท เพื่อนำไปขายต่อด้วยวิธีการตั้งโต๊ะให้บริการขายซิมการ์ดแถมโปรโมชั่น สร้างความเสียหายให้แก่บริษัท ทรูคอร์ปอเรชั่น จำกัด (มหาชน) มากกว่า 105,000,000 บาทและจากนั้นต่อมาเมื่อเดือนพฤษภาคม 2550 แฮกเกอร์ในกลุ่มดังกล่าวได้ทำการเจาะฐานข้อมูลของเอไอเอส โจรกรรมข้อมูลรหัสผู้ใช้และรหัสผ่านทางคอมพิวเตอร์เพื่อแก้ไขวงเงินบัตรเติมเงินโทรศัพท์มือถือให้กับลูกค้าผ่านทางอินเทอร์เน็ต โดยใช้วิธีจ่ายเงินผ่านบัญชีธนาคารในชื่อของบุคคลอื่นสร้างความเสียหายแก่เอไอเอสนับร้อยล้านบาท

กรณีการแฮกระบบเติมเงินของทรูมูฟข้างต้นเห็นได้ชัดเจนว่าผู้กระทำผิดมุ่งหมายจะแสวงหาประโยชน์อันมิชอบจากมูลค่าบัตรเติมเงิน โดยมีบริษัทผู้ให้บริการเป็นผู้เสียหายสามารถคำนวณมูลค่าความเสียหายได้แน่นอน แต่เมื่อเวลาผ่านไปกว่าสิบปี รูปแบบการแฮกข้อมูลคอมพิวเตอร์พัฒนาความซับซ้อนมากขึ้นกว่าแต่เดิม เป้าหมายของผู้กระทำความผิดอาจไม่ชัดแจ้งทำให้ความเสียหายหรือผลกระทบที่เกิดขึ้นอาจเกินกว่าที่จะคาดหมายได้แน่นอน ตัวอย่างกรณีที่สร้างความตื่นตระหนกและความกังวลใจแก่ผู้ใช้สื่อสังคมออนไลน์อันดับหนึ่งของโลกอย่างเฟซบุ๊ก (Facebook)เกิดขึ้นดังถ้อยแถลงของบริษัท Facebook เมื่อวันที่ 28 กันยายน 2561 (ยังไม่ชัดใครแฮกFacebook กระทบผู้ใช้ 50 ล้านคนทั่วโลก, ออนไลน์, 2562)ที่ระบุว่าแฮกเกอร์ได้เข้าถึงบัญชีผู้ใช้Facebookกว่า 50,000,000 บัญชีโดยใช้ประโยชน์จากจุดอ่อนบนระบบเครือข่ายการโจมตีครั้งใหญ่ดังกล่าวมีผลโดยตรงต่อความมั่นใจของผู้ถือหุ้น ส่งให้หุ้นของบริษัท Facebook ตกลงประมาณ 3%โดยนายมาร์ก ซักเกอร์เบิร์ก ซึ่งเป็นผู้บริหารระดับสูง (CEO) ของบริษัทFacebook ได้ชี้แจงต่อสื่อมวลชนในวันเดียวกันว่า ในขณะเวลาดังกล่าวยังไม่ทราบว่ามีการใช้บัญชีเหล่านั้นในทางที่ผิดหรือไม่แต่ทางFacebook จะติดตามปัญหาที่เกิดขึ้นอย่างต่อเนื่องและจะปรับปรุงทันทีที่ Facebook พบเบาะแสอื่นมากขึ้น โดยสิ่งที่ Facebook ทราบในขณะดังกล่าว คือ นักแฮก (Hacker)ได้เจาะระบบของFacebook ผ่านฟีเจอร์ชื่อ“View as”ที่มีช่องโหวให้นักแฮกเข้าถึงบัญชีได้เหมือนเจ้าของบัญชีนั้น โดย View as เป็นคุณสมบัติที่ช่วยให้เจ้าของเพจสามารถเห็นหน้าเพจFacebook ได้เหมือนผู้ใช้ทั่วไป ผลจากการแฮกนี้ทำให้นักแฮกสามารถสวมรอยโพสต์หรือดูข้อมูลส่วนตัวในบัญชีนั้นได้โดยที่เจ้าของบัญชีไม่รู้ตัวซึ่งจะเห็นได้ว่าผลกระทบหรือความเสียหายในช่วงเวลาก่อนที่ทาง Facebook จะเข้าควบคุมสถานการณ์ไว้ได้นั้น ข้อมูลส่วนบุคคลหรือ

ความลับของผู้ใช้บริการ Facebook ที่ได้รั่วไหลไปจะถูกนำไปใช้แสวงหาประโยชน์ในทางมิชอบอย่างไร และยังไม่เป็นที่แน่ชัดว่าแท้จริงแล้วในช่วงเวลาที่เกิดการแฮกข้อมูลผ่านฟีเจอร์ชื่อ“View as”นั้น มีผู้ใช้บริการ Facebook จำนวนเท่าใดที่ได้รับผลกระทบจากการแฮกครั้งนี้

1.2 ดีดอส (DDOS)

หมายถึงรูปแบบการบุกรุกหรือโจมตีระบบคอมพิวเตอร์จนทำให้ไม่สามารถใช้งานได้ตามปกติ สราวุธปิติยาศักดิ์ (2661 : 51-52) ได้ยกตัวอย่างคดีสำคัญที่เกิดขึ้นกับหน่วยงานในวงการยุติธรรมเมื่อไม่นานมานี้ว่า เมื่อวันที่ 13 มกราคม 2559 หน้าเว็บไซต์สำนักงานศาลยุติธรรมถูกแฮกเกอร์โจมตีด้วยวิธี Distributed Denial of Service หรือ DDOS จนไม่สามารถใช้งานได้ตั้งแต่เวลา 22.00 ของวันที่ 12 มกราคม 2559 โดยพบว่า หน้าเว็บเพจหน้าแรกของสำนักงานศาลยุติธรรมกลายเป็นพื้นสีดำ และมีรูปคล้ายหน้ากากสีขาวพร้อมข้อความภาษาอังกฤษ “Blink Hacker Group” และ “Failed Law We Want Justice ! # Boycott Thailand” จากการสืบค้นพบว่า “Blink Hacker Group” เชื่อมโยงกลุ่มที่ใช้ชื่อ “Anonymous Myanmar Hacker”จากการตรวจสอบหาการบุกรุกและช่องโหว่ระบบเครือข่าย ขณะที่การตรวจสอบรายละเอียดไอพีแอดเดรส (IP Address)พบว่ามีประมาณ 10 ไอพีแอดเดรสของผู้ที่เข้ามาบุกรุกระบบโครงข่ายหน้าเว็บไซต์อยู่ในต่างประเทศ

1.3 สแปม (Spam)(สราวุธปิติยาศักดิ์, 2661 : 106-107)

เนื่องจากปัจจุบันอินเทอร์เน็ตมิได้ถูกจำกัดการใช้งานอยู่เพียงการติดต่อสื่อสารระหว่างบุคคลเท่านั้น แต่อินเทอร์เน็ตยังถูกนำไปใช้เป็นช่องทางสำคัญในการโฆษณาและจำหน่ายสินค้าและบริการเพื่อให้ผู้บริโภคสามารถเข้าเยี่ยมชมเว็บไซต์ของผู้ประกอบกิจการค้าขายผ่านเครือข่ายอินเทอร์เน็ตได้จากทุกสถานที่ ทำให้เกิดธุรกรรมทางการค้าแบบใหม่ที่เรียกว่า “พาณิชย์อิเล็กทรอนิกส์” หรือ Electronic Commerceผ่านการส่งจดหมายอิเล็กทรอนิกส์ (อีเมล หรือ E-mail) ไปยังผู้บริโภคโดยตรงเป็นสื่อทางการตลาดที่สะดวก อย่างไรก็ตามโอกาสทางธุรกิจของผู้ประกอบการอาจนำมาซึ่งปัญหาของการรบกวนและหลอกลวงผู้บริโภค หากการส่งอีเมลนั้นมีลักษณะเป็นการส่งจำนวนมหาศาลก่อให้เกิดความคับคั่งของระบบเครือข่ายอินเทอร์เน็ต ส่งผลให้ระบบคอมพิวเตร์เกิดความล่าช้าหรือล่มได้ พฤติกรรมการส่งจดหมายอีเมลแบบนี้ เรียกว่า “สแปมมิ่ง” (Spamming)(Spam Mail)ภัยร้ายใกล้ตัวคุณ, ออนไลน์, 2562)โดยสแปมเมล (Spam Mail) เป็นอีเมลที่มีลักษณะเหมือนๆกันและมีการส่งต่อตัวเองไปบนอินเทอร์เน็ตเป็นจำนวนมากโดยมักจะเป็นอีเมลเกี่ยวกับธุรกิจ โฆษณา หรือเป็นพวกสื่อลามกต่างๆซึ่งมีรูปแบบที่ไม่แน่นอน แต่จะมีรูปแบบที่ออกแนวเชิญชวนจนน่าสงสัยเพื่อดึงดูดให้ผู้ได้รับสแปมเมลเปิดอ่านอีเมลนั้น เช่น มีถ้อยคำชื่อเรื่องของเมลว่า “วิธีที่จะทำให้คุณรวยเร็ว” หรือมีข้อความเชิญชวนให้ดูภาพโป๊หรืออ่านเรื่องเซ็กซ์ เป็นต้นสแปมเมลมีอยู่ 2 แบบ แบบแรกเป็นสแปมเมลที่ส่งเข้าไปตามกระดานข่าวเว็บบอร์ดโดยจะโพสต์ข้อความซ้ำๆกันและจะกระจายไปยังกระดานข่าวต่างๆซึ่งข้อความอาจจะไม่เกี่ยวข้องกับหัวข้อในกระดาน

ข่าวนั้นเลยภายในจะมีข้อความเชื้อเชิญโดยอาจจะมีลิงก์ให้ผู้พบเห็นกดเพื่อเข้าไปชมหรืออาจหลอกให้ผู้พบเห็นทำการสมัครสมาชิก (สแปมเมลรูปแบบนี้มีความใกล้เคียงกับการฟิชชิ่งซึ่งจะกล่าวถึงในภายหลัง)และสแปมเมลแบบที่สอง คือ ส่งอีเมลไปยังผู้รับโดยตรงโดยผู้รับนั้นอาจจะไม่เคยรู้จักผู้ส่งมาก่อนว่าเป็นใคร มาจากไหนโดยผู้ที่รับจ้างส่งสแปม (สแปมเมอร์) จะทำการค้นหาอีเมลจากแหล่งต่างๆ ไม่ว่าจะเป็นกระดานข่าวที่ผู้พบเห็นเคยไปทำการโพสต์อีเมลไว้หรือค้นหาตามเว็บแอดเดรส รวมทั้งการที่ผู้พบเห็นนั้นเคยไปสมัครสมาชิกอะไรก็ตามพวกสแปมเมอร์จะเอาอีเมลเหล่านั้นมาแล้วส่งสแปมมายังอีเมลของผู้นั้นสแปมเมอร์เหล่านี้จะได้เงินจากการที่คนเปิดอีเมลที่สแปมเมอร์นั้นส่งไปแล้วเข้าไปใช้บริการภายใน ซึ่งภายในก็จะมีทั้งโฆษณา การเชิญชวนต่างๆความอันตรายต่อผู้ใช้อาจจะดูเหมือนไม่มากมาย แต่เมื่อคิดถึงในแง่ธุรกิจถ้าพนักงานภายในองค์กรทุกคนต้องเสียเวลาลบอีเมลขยะจำพวกนี้ทุกวันย่อมกระทบต่องานและอาจส่งผลให้การส่งข้อมูลคอมพิวเตอร์ขององค์กรมีปัญหาล่าช้า ทำให้ธุรกิจหรือองค์กรได้รับความเสียหาย

2. กลุ่มความผิดที่คอมพิวเตอร์ถูกใช้เป็นเครื่องมือเพื่อประกอบอาชญากรรมอย่างอื่น (Computer as Tools)

หมายถึง การกระทำความผิดที่ผู้กระทำมีเจตนาที่จะกระทำความผิดฐานอื่นแต่ได้นำเอาคอมพิวเตอร์มาใช้เป็นเครื่องมือในการกระทำความผิด การกระทำลักษณะนี้ นอกจากเป็นการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 (ที่แก้ไขเพิ่มเติม) แล้ว หากเข้าองค์ประกอบความผิดตามประมวลกฎหมายอาญาหรือกฎหมายอื่นก็ถือเป็นความผิดตามประมวลกฎหมายอาญาหรือกฎหมายอื่นด้วย เช่น การส่งภาพลามกอนาจารของผู้เสียหายไปยังบุคคลอื่นเพื่อต้องการให้ผู้เสียหายได้รับความอับอาย หากเป็นการกระทำที่ประสงค์ต่อทรัพย์ด้วย ก็ถือเป็นความผิดฐานกรรโชกทรัพย์ตามประมวลกฎหมายอาญาด้วย ส่วนกรณีการปลอมแปลงเกี่ยวกับข้อมูลคอมพิวเตอร์โดยมิชอบ (Computer-Related Forgery)ซึ่งหากเป็นการกระทำโดยประสงค์ต่อทรัพย์ ก็อาจเป็นความผิดฐานฉ้อโกงหรือฉ้อโกงประชาชน ตามประมวลกฎหมายอาญาด้วย ปัจจุบันมีการใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิดฐานฉ้อโกง (Computer-related Fraud)ในหลากหลายรูปแบบ เช่น กรณีที่คนร้ายโฆษณาขายสินค้าหลอกลวงทางเว็บไซต์ โดยไม่มีเจตนาจะขายและหรือส่งมอบสินค้าดังกล่าว หรือกรณีที่คนร้ายสั่งซื้อสินค้าทางอินเทอร์เน็ตโดยหลอกลวงใช้ข้อมูลอันเป็นเท็จในการซื้อสินค้า นอกจากนี้ ยังมีกรณีของการนำเข้าข้อมูลสู่ระบบคอมพิวเตอร์ในการกระทำความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรตามประมวลกฎหมายอาญา และการใช้คอมพิวเตอร์เป็นเครื่องมือในการทำซ้ำ ดัดแปลง เผยแพร่ต่อสาธารณชนซึ่งงานอันมีลิขสิทธิ์ของผู้อื่นอันเป็นความผิดเกี่ยวกับการละเมิดลิขสิทธิ์ เป็นต้น

รูปแบบที่น่าสนใจของอาชญากรรมลักษณะนี้ได้แก่

2.1 ฟิชชิ่ง (Phishing)(ระวังภัย ฟิชชิ่งเมล, ออนไลน์, 2562 ; TB-CERT ศูนย์เตือนภัยไซเบอร์ธนาคารไทย เตือนเมลฟิชชิ่ง ระบุการเก็บตัวอย่างทำได้ยาก หากใครเจอช่วยกันส่งให้ธนาคาร, ออนไลน์, 2562)

ฟิชชิ่งเป็นเทคนิคการหลอกลวงทางอินเทอร์เน็ตประเภทหนึ่งในรูปแบบของการปลอมแปลงอีเมลหรือข้อความที่สร้างขึ้นเพื่อหลอกให้เหยื่อเปิดเผยข้อมูลทางด้านการเงินหรือข้อมูลส่วนตัวต่างๆ เช่น ชื่อบัญชีผู้ใช้ รหัสผ่าน หมายเลขบัตรเครดิต และหมายเลขบัตรประจำตัวประชาชน เป็นต้น คนร้ายจะส่งอีเมลหลอกลวงโดยใช้ชื่อหน่วยงานหรือบุคคลที่เป็นผู้ส่งและเนื้อความที่น่าเชื่อถือ โดยคนร้ายอาจกำหนดชื่อผู้ส่งให้มีลักษณะตรงหรือคล้ายคลึงกับบริษัทที่มีชื่อเสียงหรือสถาบันการเงินเพื่อให้ผู้รับอีเมลเชื่อถือในเบื้องต้นว่าเป็นอีเมลที่ส่งมากจากบุคคลที่น่าเชื่อถือ โดยอีเมลนั้นจะประกอบไปด้วยข้อความในลักษณะแจ้งเตือนและเร่งให้ดำเนินการหากไม่ต้องการให้เกิดผลเสีย อาทิเช่น ข้อความว่าเหยื่อกำลังทำธุรกรรมโอนเงินออกจากบัญชีหากมิได้ดำเนินการดังกล่าวเหยื่อต้องรีบทำการยกเลิกธุรกรรม หรือทางระบบของผู้ประกอบการพบว่าเหยื่อมีการจองซื้อสินค้าหรือบริการที่มีราคาสูง หากเหยื่อไม่ประสงค์จะจองซื้อสินค้าหรือบริการ จะต้องรีบดำเนินการเพื่อยกเลิกรายการฉะนั้นจะถูกตัดจ่ายเงินจากบัตรเครดิตเพื่อเป็นค่าสินค้าและบริการ เมื่อเหยื่อหลงเชื่อก็จะดำเนินการตามความต้องการของคนร้าย เช่น กดลิ้งก์ที่คนร้ายระบุไว้ให้เข้าเว็บไซต์เพื่อการกรอกข้อมูลส่วนตัว รหัสผ่าน หรือตอบกลับอีเมลด้วยข้อมูลส่วนตัว ซึ่งหน้าเว็บไซต์ที่คนร้ายจัดทำขึ้นนี้จะบันทึกข้อมูลส่วนบุคคลที่เหยื่อได้กรอกบนเว็บไซต์ จากนั้นคนร้ายจะนำข้อมูลของเหยื่อที่ได้ไปใช้แสวงหาประโยชน์ในทางมิชอบอย่างอื่น

ทั้งนี้ในช่วงไตรมาสที่สามของปี พ.ศ.2561 ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร (TB-CERT)ได้สังเกตว่ามีปริมาณฟิชชิ่งที่เพิ่มสูงขึ้น โดยพบว่ามีการสร้างฟิชชิ่งเว็บไซต์ โดยใช้โดเมน (Domain) ของประเทศในแอฟริกา .ga (Gabonese Republic) .ml (Replublic of Mali) ประเทศอาณาเขตของประเทศนิวซีแลนด์ .tk (Tokelau Territory of New Zealand) เนื่องจากเป็นประเทศที่มีการใช้งานอินเทอร์เน็ตน้อยและสามารถจดทะเบียนโดเมนได้ง่าย จากนั้นจึงไปสร้างฟิชชิ่งเว็บไซต์ในอีกประเทศและส่งฟิชชิ่งเมลอ้างว่าเป็นอีเมลจากธนาคาร โดยเมื่อวันที่ 24 มกราคม 2562 ที่ผ่านมา TB-CERT ได้ออกประกาศเตือนประชาชนทั่วไปถึงการโจมตีแบบฟิชชิ่ง (Phishing) ที่มีเพิ่มมากขึ้น และขอให้เหยื่อแจ้งเตือนเมื่อได้รับอีเมลลักษณะนี้ด้วยการส่งตัวอย่างฟิชชิ่งที่เกิดขึ้นให้ธนาคารทราบเพื่อรีบดำเนินการแก้ไขโดยเร็วต่อไป

2.2 สแกมเมอร์ (Scammer)

สแกมเมอร์เป็นรูปแบบอาชญากรรมคอมพิวเตอร์ที่พบว่าเจ้าพนักงานได้ทำการขยายผลจับกุมจำนวนมากในช่วง 2-3 ปีที่ผ่านมา สแกมเมอร์หมายถึง การหลอกลวงทางอินเทอร์เน็ต โดยมีรูปแบบการหลอกลวงมากมายเพื่อหลอกเอาผลประโยชน์จากเหยื่อที่หลงเชื่อ เช่น หลอกให้ร่วม

ทำธุรกิจหรือลงทุนเพื่อประโยชน์ตอบแทนสูงหลอกว่าเหยื่อเป็นผู้โชคดีถูกรางวัล หลอกให้เหยื่อช่วยเหลือแล้วจะตอบแทนด้วยเงินจำนวนมากทั้งนี้ วิธีที่เหล่ามิจฉาชีพนิยมและมีผู้ตกเป็นเหยื่อมากที่สุด คือวิธีที่เรียกว่า “การแสร้งรัก” หรือ Romance Scam ซึ่งเป็นการใช้เรื่องของความรักมาเป็นเครื่องมือหลอกลวง โดยผู้เสียหายมีทั้งชายและหญิงไทยที่เชื่อคำหว่านล้อมและคำพูดที่สวยหรูของเหล่าสแกมเมอร์ที่มักมีการใช้รูปโปรไฟล์ของหญิงหรือชายชาวต่างชาติหน้าตาดี มีการงานและฐานะร่ำรวย แจ้งว่าประสงค์ที่จะคบหาและสร้างครอบครัวกับเหยื่อ สร้างความเชื่อมั่นให้เหยื่อหลงเชื่อเพื่อหวังเอาผลประโยชน์หรือทรพย์สินจากเหยื่อในยุคแรกๆ เหยื่อจะเป็นกลุ่มที่สามารถสื่อสารภาษาอังกฤษได้มีหน้าที่การงานดี อย่างหมอ พยาบาล ข้าราชการชั้นสูงๆต่อมาเริ่มเป็นกลุ่มนักศึกษาโดยใช้อุบายว่าจะส่งของขวัญไปให้เหยื่อแต่ในปัจจุบันเหยื่อจะเริ่มเป็นกลุ่มของแม่ค้าออนไลน์และผู้สูงอายุซึ่งแม่ค้าออนไลน์มักตั้งค่าโปรไฟล์เป็นสาธารณะง่ายต่อการเข้าถึงและจะรับแอดทุกคนเป็นปกติส่วนผู้สูงอายุคือกลุ่มที่มีเงินเก็บและมักไม่ได้ติดตามข่าวสาร ทำให้หลงเชื่อกลอุบายของสแกมเมอร์ได้ง่ายการหลอกลวงก็จะใช้การสร้างสถานการณ์ให้ทุกอย่างเหมือนเป็นเรื่องจริง แล้วแจ้งว่าจะส่งสิ่งของมีมูลค่าสูงหรือสัมภาระส่วนตัวมาเพื่อใช้ชีวิตร่วมกับเหยื่อ แต่ขอให้เหยื่อช่วยรับสิ่งของให้ก่อนโดยเหยื่อต้องช่วยเสียภาษีอากรหรือค่าธรรมเนียมในการนำเข้าสินค้าเหล่านั้นก่อนและในระยะช่วงปีที่ผ่านมาพบรูปแบบของสแกมเมอร์ ในลักษณะของ Scam Blackmail โดยที่สแกมเมอร์จะวีดีโอคอลเข้าไปหาเหยื่อแต่จอจะมืดสนิทจากนั้นจะนำวิดีโอของเหยื่อตัดต่อเข้ากับวีดีโอลามกอนาจารภายหลังจะขู่ให้เหยื่อโอนเงินให้มิฉะนั้นจะส่งคลิปวีดีโอประจานให้เพื่อนของเหยื่อ ในกรณีนี้เหยื่อมีทั้งผู้หญิงและผู้ชาย (แฉเหลี่ยม!! แก๊งแชตรักลวงโลก ภัยสาวไทยนิยมผัวฝรั่ง, ออนไลน์, 2562)

ในการแก้ไขการแพร่ระบาดของสแกมเมอร์ รัฐบาลได้มอบหมายให้สำนักงานตำรวจแห่งชาติดำเนินการปราบปรามกลุ่มองค์กรอาชญากรรมที่กระทำความผิดและส่งผลกระทบต่อความเป็นอยู่ของประชาชน ซึ่งเกี่ยวข้องกับเทคโนโลยีสารสนเทศเพื่อให้การปราบปรามอาชญากรรมดังกล่าวเกิดความรวดเร็วและมีประสิทธิภาพโดยสำนักงานตำรวจแห่งชาติจึงได้จัดตั้งศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ (ศปอส.ตร.)จากการสืบสวนติดตามกลุ่มคนร้ายทั้งชาวไทยและชาวต่างชาติของ ศปอส.ตร.เพื่อรับผิดชอบกับที่ใช้เทคโนโลยีสารสนเทศนำไปสู่การดำเนินคดีกับคนร้ายหลายราย (ทลายเครือข่าย Romance Scam” ผู้ต้องหา 17 ราย 8 เครือข่าย ผู้เสียหาย 48 ราย ความเสียหายมากกว่า 5,961,740 บาท, ออนไลน์, 2562)

2.3 การแสวงหาประโยชน์ทางเพศกับเด็กบนโลกออนไลน์ (Online Child Sexual Exploitation)

การแสวงหาประโยชน์ทางเพศกับเด็กบนโลกออนไลน์ เป็นอาชญากรรมรูปแบบใหม่ที่เริ่มมีความรุนแรงและมีแนวโน้มที่จะเกิดมากขึ้นเนื่องจากการใช้สื่อสังคมออนไลน์ของเด็กไทยในปัจจุบันยังขาดความระมัดระวังที่ดีพอ ทำให้อาชญากรอาศัยโลกไซเบอร์เป็นช่องทางละเมิด

และแสวงหาประโยชน์ต่อเด็กได้ง่ายขึ้น และมักพบว่าผู้กระทำความผิดมีทั้งคนไทยและคนต่างชาติโดย จากรายงานของ Internet Watch Foundation (ซับซ้อน ซ่อนเงื่อน ‘สื่อลามกเด็ก’ อาชญากรรมใต้ดิน ‘ยุคไซเบอร์’, ออนไลน์, 2562) พบว่า ในทุกๆ 7 นาทีในการใช้งานบนโลกออนไลน์ทั่วโลก จะพบภาพเด็กถูกทารุณกรรมทางเพศ ซึ่งในจำนวนดังกล่าวเป็นเด็กอายุ 11-15 ปี คิดเป็นจำนวนร้อยละ 43 อายุน้อยกว่า10 ปี คิดเป็นจำนวนร้อยละ 55 และที่น่าตกใจยิ่งไปกว่านั้น เป็นเด็กทารกจนถึง 2 ขวบ คิดเป็นจำนวนร้อยละ 2 พฤติกรรมการเข้าถึงตัวเด็กมีหลายรูปแบบทั้งจากการพูดคุยผ่านสื่อสังคมออนไลน์ อย่างเฟซบุ๊กแมสเซ็นเจอร์(Facebook Messenger) โดยในกรณีที่เป็นชาวต่างชาติพูดคุยกับเด็กไทย จะมีการใช้โปรแกรมแปลภาษาของกูเกิ้ล คือ Google Translate แปลระหว่างภาษาต่างประเทศและภาษาไทยคุยกัน

ตัวอย่างกรณีที่เพิ่งเกิดขึ้นเมื่อไม่นานมานี้ เมื่อวันที่ 17 กุมภาพันธ์ 2562 อธิบดีกรมสอบสวนคดีพิเศษ (ดีเอสไอ)ได้แถลงผลงานการปฏิบัติการตามที่ได้รับแจ้งเบาะแสจากมูลนิธิ Operation Underground Railroad (O.U.R.) เกี่ยวกับผู้ต้องสงสัยว่าครอบครองและเผยแพร่สื่อลามกอนาจารเด็กซึ่งอยู่ในพื้นที่จังหวัดตราด ซึ่งดีเอสไอสืบสวนและรวบรวมพยานหลักฐานเป็นเวลา 6 เดือนจนสามารถระบุผู้กระทำความผิดมีพฤติการณ์โฆษณาทางเฟซบุ๊กชักชวนให้จ่ายเงินสมัครเป็นสมาชิกกลุ่มไลน์แบบปิดซึ่งผู้กระทำผิดเป็นผู้ดูแลแอดมินโดยมีการแชร์ภาพลามกอนาจารเด็กระหว่างสมาชิกกลุ่มดังกล่าว ซึ่งต่อมาเมื่อวันที่ 15 กุมภาพันธ์ 2562 เจ้าพนักงานดีเอสไอในฐานะพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 (ที่แก้ไขเพิ่มเติม) ได้สนธิกำลังกับศูนย์พิทักษ์เด็ก สตรีครอบครัวและป้องกันปราบปรามการค้ามนุษย์ตำรวจภูธรภาค 2 กองบังคับการสืบสวนสอบสวนตำรวจภูธรภาค 2 และสถาบันนิติวิทยาศาสตร์เข้าจับกุมผู้ต้องหาและได้ทำการตรวจค้นบ้านพักของผู้ต้องหา พบอุปกรณ์อิเล็กทรอนิกส์หลายรายการเช่น คอมพิวเตอร์ตั้งโต๊ะ 1 เครื่อง คอมพิวเตอร์โน้ตบุ๊ก 1 เครื่องและพบไฟล์ภาพและคลิปลามกอนาจารเด็กในคอมพิวเตอร์ดังกล่าว มากกว่า 5,000 ไฟล์(ดีเอสไอบุกรวบแอดมินกลุ่มแชร์ภาพลามกเด็ก, ออนไลน์, 2562)

3. กลุ่มที่มีการใช้คอมพิวเตอร์เป็นเครื่องมือจัดการผลประโยชน์ที่ได้จากอาชญากรรม

นอกจากอาชญากรรมคอมพิวเตอร์สองกลุ่มข้างต้นแล้ว ในปัจจุบันมิจฉาชีพยังได้ใช้ประโยชน์จากความซับซ้อนของระบบคอมพิวเตอร์และนวัตกรรมใหม่ในโลกดิจิทัล เช่น สกุลเงินดิจิทัล หรือ Cryptocurrency เป็นเครื่องมือในการปิดบังเส้นทางการเงินของคนร้ายจากการถูกตรวจสอบ รวมถึงกระทำความผิดฐานฟอกเงินเพื่อช่วยเหลือในการฟอกผลประโยชน์สกปรกที่ได้จากอาชญากรรมให้เป็นทรัพย์สินที่สะอาดและหมุนเวียนต่อไปในระบบเศรษฐกิจ

คำว่า “Cryptocurrency”หากแปลเป็นไทยตรงตัว หมายความถึง“สกุลเงินที่ถูกเข้ารหัส” โดยในปัจจุบันมีสกุลเงินดิจิทัลที่ถูกสร้างขึ้นในโลกกว่า 2,500 สกุลเงิน โดย 10 สกุลเงินดิจิทัลที่มีมูลค่าสูงสุดตามลำดับ ณ เดือนตุลาคม พ.ศ.2561 ได้แก่ Bitcoin, Ethereum, Ripple, Bitcoin cash, EOS, Stellar, Litecoin, Tether, CardanoและMonero (10 อันดับสกุลเงินดิจิทัลที่มีมูลค่าสูงสุด, ออนไลน์, 2562)คำว่า “เข้ารหัส” มิได้เป็นเพียงรหัสผ่านทั่วไป หากแต่เป็นการเข้ารหัสด้วยการเปลี่ยนข้อมูลต่างๆ ให้อยู่ในรูปที่สามารถมองเห็นได้เพียงแค่รหัสที่อ่านไม่ออกเช่น หากนำข้อความคำว่า “สวัสดี” เข้าไปรหัส(Encrypt)ไว้สิ่งที่เห็นได้จะมีลักษณะเป็นดังนี้

“6E795F1D3F0BA8EB3A9372CF2A20ACDD90A3F59E5A33583E7E7D19C18B416BB”

และในทางกลับกัน เมื่อนำเอาชุดตัวเลขดังกล่าวไปถอดรหัส (Decrypt) ก็จะได้กลับมาเป็นคำว่า “สวัสดี” (Cryptocurrencyคืออะไร และคุณควรที่จะลงทุนกับมันหรือไม่, ออนไลน์, 2561)

เนื่องจากการทำความเข้าใจเกี่ยวกับสกุลเงินดิจิทัลในทางเทคนิคคอมพิวเตอร์เป็นเรื่องไม่ง่ายเพราะต้องอาศัยความรู้ความเข้าใจด้านคณิตศาสตร์และเทคโนโลยีคอมพิวเตอร์เป็นอย่างดี จากการทบทวนวรรณกรรมผู้วิจัยพบว่า ทพพล น้อยปัญญา (2561 : 11-13) ได้อธิบายถึงที่มาและการทำงานของบิทคอยน์ (Bitcoin)ซึ่งเป็นสกุลเงินดิจิทัลที่โด่งดังและมีมูลค่ามากสุดในปัจจุบันด้วยภาษาที่เข้าใจง่าย ว่า บิทคอยน์ (Bitcoin) เป็นเงินตราดิจิทัลสกุลหนึ่ง ที่ไม่มีรัฐบาลหรือธนาคารกลางของประเทศใดเป็นผู้ออกเหมือนอย่างเงินตราทั่วไปBitcoin คิดค้นขึ้นมาโดยบุคคลผู้ใช้นามแฝงว่า “Satoshi Nakamoto”ที่ยังไม่มีใครทราบว่าบุคคลดังกล่าวแท้จริงคือใคร เริ่มแรกSatoshi Nakamoto ไม่ได้มุ่งหมายจะสร้างเงินดิจิทัลขึ้นมาโดยตรง แต่ต้องการสร้างระบบการเงินที่เรียกว่าPeer-to-Peer Electronic Cash System ที่เป็นระบบการเงินใหม่ ที่ไม่มีรัฐบาลประเทศใดเป็นผู้ออก เป็นระบบการเงินระหว่างผู้ใช้ด้วยกัน (Peer-to-peer)ไม่มีคนกลางโดย Bitcoinถูกสร้างขึ้นด้วยโปรแกรมใหม่ทางคอมพิวเตอร์เรียกว่า “บล็อกเชน” (Blockchain) Bitcoin จะเกิดขึ้นได้ก็ด้วยการไป “ขุด” (Mining)ในเหมือง (หมายถึงพื้นที่ในระบบไซเบอร์)Bitcoin ถูกสร้างให้มีทั้งหมด 21 ล้านเหรียญ ถ้าขุดขึ้นมาหมดเมื่อไหร่ก็จะไม่มีการสร้างใหม่ ในตัวโปรแกรมที่สร้าง Bitcoin จะมี “อัลกอริทึม” (Algorithm) ที่จะเป็นเหมือนสูตรหรือสมการทางคอมพิวเตอร์ที่จะเปลี่ยนแปลงสูตรหรือสมการนั้นไปเรื่อยๆ ผู้ขุดจะต้องให้คำตอบเป็นสูตรหรือสมการนั้นให้ตรงกัน ถ้าตอบได้ตรงกับคำถามก็จะได้ Bitcoin เป็นรางวัล แต่การไปตอบคำถามนั้นไม่ใช่ว่าตอบถูกต้องอย่างเดียว ยังต้องมีปัจจัยอื่นคือตรงกับเวลาและโอกาสที่โปรแกรมจะตั้งคำถามมาด้วย ไม่ใช่ว่ารู้คำตอบแล้วก็จะได้เหรียญBitcoin ทุกวันนี้มีเหมืองดิจิทัลที่ทำการขุดอยู่ทั่วโลก มีคอมพิวเตอร์ขนาดใหญ่โตมโหฬารทำหน้าที่ในการขุด บางแห่งก็ใหญ่ขนาดเป็นสนามฟุตบอล คือถ้าเครื่องใหญ่กว่ามีกำลังมากกว่าก็มีโอกาสในการขุดเจอมากกว่า เหมือนกับเหมือง

แร่ธรรมดาทั่วไป เหมืองไหนที่มีคนงานมากกว่าโอกาสที่จะได้แร่ที่ขุดก็มีมากกว่า เมื่อ Bitcoin ไม่มีรูปร่าง ใครที่มี Bitcoin ก็จะต้องมีกระเป๋าเงินดิจิทัลที่เรียกว่า “วอลเลท” (Wallet) เอาไว้ใส่ และดูยอดเงินคงเหลือ

ทพพล น้อยปัญญา (2561 : 19 และ 43-46) ให้ข้อสังเกตไว้ว่า เทคโนโลยีBlockchainมีลักษณะสำคัญที่คือ

1. เมื่อมีรายการใหม่เกิดขึ้น จะมีการรับรองความถูกต้องของรายการนั้นโดยผู้ที่อยู่ในเครือข่ายนั้นเองเรียกว่า “มายเนอร์” (Miner) Miner ตรวจสอบวิธีการทางคอมพิวเตอร์แล้วเห็นว่าถูกต้องเป็นจริง รายการนั้นก็จะถูกบันทึกลงเป็นบล็อกใหม่ของเครือข่าย Blockchain นั้น ทั้งนี้ Miner ไม่ได้มีอยู่คนเดียว แต่เป็นใครก็ได้ที่อยู่ในเครือข่ายเดียวกัน Blockchain จึงไม่ได้มีเจ้าของและไม่อยู่ในความครอบครองของคนใดคนหนึ่งเลย

2. เมื่อทำรายการแล้วจะไปแก้ไขเปลี่ยนแปลงไม่ได้ ไม่ว่าจะโดยใครก็ตาม เพราะเหตุที่เป็น Blockchain รายการนั้นจะถูกบันทึกไว้ในทุกบล็อกที่อยู่ในเครือข่ายโดยอัตโนมัติ ผู้ที่เป็นเจ้าของบล็อกทุกบล็อกก็จะเห็นพร้อมกันหมด

3. ระบบนี้Blockchainมีความปลอดภัยมาก เพราะในระบบของ Blockchain ทุกคนแม้แต่ตัวเจ้าของบัญชีก็ไม่สามารถเข้าไปแก้ไขเปลี่ยนแปลงข้อมูลที่บันทึกลงแล้วได้ กล่าวคือ ข้อมูลที่ถูกบันทึกไว้แล้วด้วยการเข้ารหัสทางคอมพิวเตอร์ที่เรียกว่า “Cryptography” ใน Blockchain จะแก้ไขไม่ได้หรือแม้แต่กระทั่งยกเลิกบล็อกนั้นหรือทำให้หายไปเลยก็ไม่ได้ ข้อมูลที่อยู่ใน Blockchain จึงถูกต้องและเป็นจริงเสมอ

4. กระบวนการของ Blockchain ที่เกิดขึ้นทั้งหมดไม่มีผู้ควบคุม ไม่ต้องมีใครมาอนุญาต เพราะระบบ Blockchain เป็นระบบที่แต่ละคนทำรายการเอง และจะถูกบันทึกไว้ในทุกบล็อก จึงไม่ต้องมีรัฐบาลหรือบุคคลที่สามมาให้การรับรองรายการดังกล่าวอีก ด้วยเหตุนี้จึงมีการเรียกเทคโนโลยี Blockchain ว่า “Distributed Ledger Technology” แปลความหมายว่า Blockchain เป็นระบบบัญชีแยกประเภท (Ledger)เป็นบล็อกและกระจายตัว (Distributed) ออกไป ไม่มีการรวมศูนย์กลาง (Decentralized)ใครทำอะไรใน Blockchain ก็จะถูกบันทึกไว้หมดโดยทุกบล็อก ไม่ต้องมีคนกลางอย่างนายทะเบียนมารับรองหรือควบคุม เพราะระบบของ Blockchain จะทำให้เกิดความเชื่อถือได้ด้วยตัวเอง เพราะทุกบล็อกบันทึกรายการที่ทำไว้หมด

หนึ่งในเจตนารมณ์ของ Satoshi Nakamotoผู้ที่คิดค้นBitcoinคือการรักษาความเป็นส่วนตัวของผู้ที่ทำธุรกรรมผ่านระบบ ด้วยการอาศัยการเข้ารหัส จึงเป็นเหตุที่ทำให้เงินดิจิทัลในรูปแบบของBitcoinถูกเรียกในอีกชื่อหนึ่งว่า สกุลเงินเข้ารหัส (Cryptocurrency)แต่เพราะเหตุใดผู้ที่บุกเบิกบิทคอยน์จำเป็นต้องอำพรางข้อมูลธุรกรรมนั้นยังมีการตีความแตกต่างกันไปตัวอย่างการใช้ Bitcoin เพื่อปกปิดข้อมูลธุรกรรมผิดกฎหมายนั้น คือ ตลาดซื้อขายสินค้าและบริการผิด

กฎหมายเป็นการซื้อขายยาเสพติด ที่รู้จักกันในชื่อ ซิลค์โรด (Silk Road) จัดตั้งขึ้นเมื่อประมาณปี ค.ศ.2011(ตรงกับปี พ.ศ.2554) เพื่อเป็นตลาดค้าขายทั้งยาเสพติด อาวุธสงคราม เอกสารปลอม และสิ่งผิดกฎหมายอีกมากมาย โดยการเข้าถึงตลาดดังกล่าวมิได้อยู่บนเว็บไซต์ทั่วไปที่ทุกคนบนโลกอินเทอร์เน็ตสามารถเข้าถึงได้ แต่จะอยู่ในเว็บไซต์เฉพาะที่เรียกว่า “Deep Web”ซึ่งการเข้าถึงจะต้องกระทำผ่านซอฟแวร์เฉพาะบางอย่าง เช่น ซอฟท์แวร์ที่มีชื่อว่า “TOR” โดยการซื้อขายสิ่งของผิดกฎหมายผ่าน Silk Road นั้นกำหนดให้ชำระผ่านBitcoinเท่านั้นเพื่ออำพรางข้อมูลธุรกรรมที่ผิดกฎหมาย ทำให้เจ้าพนักงานของรัฐติดตามตัวคนร้ายได้ยากขึ้น(ปปง.แก้ ก.ม.เงินดิจิทัล‘บิทคอยน์’ คุมเข้มผู้ให้บริการ ปิดทางมิจฉาชีพ, ออนไลน์, 2562; ฟอกเงินผ่าน'บิทคอยน์'ปลอดภัยจริงหรือ, ออนไลน์, 2562 ; The History of Silk Road : A Tale of Drugs, Extortion &Bitcoin, ออนไลน์, 2562)

อำนาจหน้าที่ของเจ้าพนักงานในกระบวนการยุติธรรมทางอาญา

ทุกหน่วยงานซึ่งเป็นองคาพยพในกระบวนการยุติธรรมทางอาญาล้วนมีบทบาทสำคัญในการก่อให้เกิดประสิทธิภาพการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ทั้งนี้ เจ้าพนักงานในกระบวนการยุติธรรมที่มีบทบาทสำคัญในส่วนของการดำเนินคดีกับผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์ประกอบด้วย

1. เจ้าพนักงานสืบสวน

ตามประมวลกฎหมายวิธีพิจารณาความอาญา บัญญัติความหมายของการสืบสวนและการสอบสวนแยกต่างหากจากกัน มาตรา 2 (10) และ (11) บัญญัติว่า

(10) “การสืบสวน” หมายความถึงการแสวงหาข้อเท็จจริงและหลักฐานซึ่งพนักงานฝ่ายปกครองหรือตำรวจได้ปฏิบัติไปตามอำนาจและหน้าที่ เพื่อรักษาความสงบเรียบร้อยของประชาชน และเพื่อที่จะทราบรายละเอียดแห่งความผิด

(11) “การสอบสวน” หมายความถึงการรวบรวมพยานหลักฐานและการดำเนินการทั้งหลายอื่นตามบทบัญญัติแห่งประมวลกฎหมายนี้ ซึ่งพนักงานสอบสวนได้ทำไปเกี่ยวกับความผิดที่กล่าวหา เพื่อที่จะทราบข้อเท็จจริงหรือพิสูจน์ความผิดและเพื่อจะเอาตัวผู้กระทำผิดมาฟ้องลงโทษ

เจ้าพนักงานสืบสวนมีบทบาทสำคัญการรวบรวมข้อมูลเบื้องต้นเพื่อที่จะทราบรายละเอียดแห่งความผิด รวมถึงรูปแบบและพฤติกรรมที่คนร้ายใช้ในการกระทำความผิด โดยเฉพาะในคดีที่ต้องมีการวางแผนเพื่อล่อจับผู้กระทำความผิด ในปัจจุบันรายงานสืบสวนถือว่ามีความสำคัญในการสร้างความชอบด้วยกฎหมายของพยานหลักฐานในกรณีของการล่อจับ (Undercover) เพื่อชี้ให้เห็นว่าคนร้ายมีเจตนาในการกระทำผิดและมีพฤติการณ์เกี่ยวข้องกับการกระทำความผิดอยู่ก่อนแล้วอย่างไรและไม่ใช่การล่อให้กระทำความผิด (Entrapment) แต่ในทางกฎหมายเจ้าพนักงานสืบสวนยังมีอำนาจในการรวบรวมพยานหลักฐานไม่กว้างขวางเท่ากับพนักงานสอบสวนทั้งนี้ เป็นเพราะ

ในขั้นตอนของการสืบสวนเป็นไปเพียงเพื่อทราบรายละเอียดแห่งความผิด แต่ยังไม่ถึงขั้นตอนการพิสูจน์ความผิดเพื่อจะเอาตัวผู้กระทำผิดมาฟ้องลงโทษ อันเป็นอำนาจหน้าที่ของพนักงานสอบสวน ในคดีความผิดที่มีการใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด เช่นการแสวงหาประโยชน์ทางเพศกับเด็กบนโลกออนไลน์ เจ้าพนักงานสืบสวนถือได้ว่าเป็นเจ้าพนักงานกลุ่มแรกที่มีบทบาทในการแสวงหารายละเอียดแห่งความผิดเบื้องต้น เช่น ลักษณะกลุ่มเป้าหมายของเหยื่อ รูปแบบการกระทำความผิด และการเข้าถึงกลุ่มคนร้ายที่กระทำความผิด ซึ่งต้องอาศัยเทคนิควิธีการเพื่อการแฝงตัวบนโลกไซเบอร์ในการหาข้อมูลการกระทำความผิด

2. พนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 (ที่แก้ไขเพิ่มเติม)

หมายถึงผู้ซึ่งรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 (ที่แก้ไขเพิ่มเติม) โดยพนักงานเจ้าหน้าที่จะมีอำนาจตามมาตรา 18 ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 (ที่แก้ไขเพิ่มเติม) หรือในกรณีที่มีการร้องขอจากพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญาให้ทำการสืบสวนและสอบสวนในบรรดาความผิดอาญาต่อกฎหมายอื่นซึ่งได้ใช้ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์เป็นองค์ประกอบหรือเป็นส่วนหนึ่งในการกระทำความผิดหรือมีข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับการกระทำความผิดอาญาตามกฎหมายอื่นเพื่อประโยชน์ในการสืบสวนและสอบสวนของพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา โดยพนักงานเจ้าหน้าที่มีอำนาจหน้าที่เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิดดังนี้

1. มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดมาเพื่อให้ถ้อยคำส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

2. เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง

3. สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา 26 หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่หรือให้เก็บข้อมูลดังกล่าวไว้ก่อน

4. ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิด ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

5. สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

6. ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

7. ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

8. ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิด

3. พนักงานสอบสวน

คดีอาชญากรรมคอมพิวเตอร์มีลักษณะที่แตกต่างจากคดีอาญาทั่วไป เนื่องจากมีความสลับซับซ้อนในการกระทำความผิด ผู้กระทำความผิดเป็นผู้มีความรู้ความเชี่ยวชาญในการใช้คอมพิวเตอร์หรือระบบอิเล็กทรอนิกส์ต่างๆ แต่กลับนำไปใช้ในการกระทำผิดเพื่อให้เกิดความเสียหายแก่บุคคลอื่น ดังนั้นในการสืบสวนสอบสวน ติดตามจับกุมผู้กระทำความผิด รวมทั้งการค้นหาพยานหลักฐานต่างๆ จำเป็นต้องกระทำโดยผู้ที่มีความรู้ความเชี่ยวชาญในเรื่องคอมพิวเตอร์และระบบอิเล็กทรอนิกส์ด้วยเช่นกัน นอกจากนั้น การกระทำความผิดที่เกี่ยวข้องกับคอมพิวเตอร์ส่วนมากเกิดขึ้นในหลายท้องที่ต่อเนื่องเกี่ยวพันกัน รวมถึงการกระทำความผิดที่เกิดนอกราชอาณาจักรไทยที่จำเป็นต้องใช้ความร่วมมือระหว่างประเทศทางอาญา หรือในกรณีที่เป็นการกระทำความผิดที่เข้าลักษณะเป็นคดีพิเศษซึ่งพนักงานอัยการต้องคำนึงถึงความชอบด้วยกฎหมายของการสอบสวนเป็นพิเศษจากคดีอาญาอื่นๆ

พนักงานสอบสวนถือว่าเป็นเจ้าหน้าที่ในกระบวนการยุติธรรมที่มีความสำคัญอย่างมากในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ เนื่องจากการรวบรวมพยานหลักฐานที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ หรือพยานหลักฐานที่ถูกจัดเก็บในอุปกรณ์ดิจิทัลต่างๆ มีความเสี่ยงต่อการสูญหายของข้อมูลหรือการปนเปื้อนของข้อมูลจนทำให้พยานหลักฐานดิจิทัลขาดความน่าเชื่อถือ อีกทั้งวัตถุพยานในคดีอาชญากรรมคอมพิวเตอร์ เช่น เครื่องคอมพิวเตอร์ มีความแตกต่างจากวัตถุพยานในคดีอาญาประเภทอื่น เนื่องจากร่องรอยในการกระทำความผิดที่เกิดกับวัตถุพยานมิได้อยู่ในลักษณะ

เปิดเผยชัดแจ้งอย่างเช่น คราบเลือด หรือลายนิ้วมือ เหมือนกับวัตถุพยานในคดีอาญาทั่วไป แต่ร่องรอยการกระทำความผิดที่เกิดกับวัตถุพยานในคดีอาชญากรรมคอมพิวเตอร์ฝังอยู่ในส่วนประกอบของคอมพิวเตอร์ที่ต้องอาศัยผู้มีความรู้ความเข้าใจทางด้านดิจิทัลและนิติคอมพิวเตอร์เพื่อเชื่อมโยงข้อมูลสำคัญในอุปกรณ์คอมพิวเตอร์ซึ่งอาจประกอบด้วยข้อมูลในปริมาณจำนวนมากมาย มหาศาลแล้วชี้ให้เห็นถึงถึงรูปแบบการกระทำความผิดและระบุตัวผู้กระทำผิด ดังนั้น พนักงานสอบสวนจึงต้องมีความรู้พื้นฐานในการจัดการกับพยานหลักฐานดิจิทัล เพื่อประโยชน์ในการรวบรวมพยานหลักฐานให้ได้ครบถ้วนในระยะเวลารวดเร็วก่อนที่ข้อมูลนั้นจะถูกทำให้สูญหายหรือเสียหายอีก ทั้งเพื่ออุดช่องโหว่ข้อต่อสู้ในเรื่องของความน่าเชื่อถือของพยานหลักฐานดิจิทัลของฝ่ายจำเลยในชั้นพิจารณา

4. ผู้ตรวจพิสูจน์หลักฐาน

ในส่วนของคดีอาชญากรรมคอมพิวเตอร์ซึ่งต้องมีการตรวจพิสูจน์พยานหลักฐานดิจิทัลที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ เจ้าพนักงานผู้ตรวจพิสูจน์ใช้วิธีการทาง “นิติคอมพิวเตอร์” เพื่อพิสูจน์เชื่อมโยงพยานหลักฐานที่พบในอุปกรณ์ดิจิทัลกับผู้ถูกกล่าวหาว่ากระทำความผิดโดยในคดีอาชญากรรมคอมพิวเตอร์ ผู้ตรวจพิสูจน์หลักฐานถือได้ว่ามีความสำคัญอย่างมาก โดยเฉพาะอย่างยิ่งคดีซึ่งจำเลยเป็นผู้มีความรู้ด้านคอมพิวเตอร์และก่ออาชญากรรมที่มีความยุ่งยากซับซ้อน หากพยานหลักฐานดิจิทัลในสำนวนการสอบสวนไม่หนักแน่นมั่นคงเพียงพอ หรือยังมีข้อโต้แย้งด้านมาตรฐานการจัดการกับพยานหลักฐานดิจิทัล ก็อาจส่งผลกระทบทำให้พยานหลักฐานดิจิทัลนั้นมีน้ำหนักให้รับฟังได้น้อย หรือไม่น่าเชื่อถือ ส่งผลกระทบต่อรูปคดีได้ (สุนีย์ สกาวรัตน์, 2559 : 67-69)

5. พนักงานอัยการ

การดำเนินคดีอาชญากรรมคอมพิวเตอร์จัดเป็นการดำเนินคดีอาญาประเภทหนึ่ง ซึ่งเริ่มต้นเมื่อพนักงานอัยการได้รับสำนวนการสอบสวนคดีอาญาพร้อมความเห็นทางคดีจากพนักงานสอบสวน จากนั้น พนักงานอัยการจะพิจารณาพยานหลักฐานในสำนวนการสอบสวนและมีคำสั่งทางคดีโดยการปฏิบัติหน้าที่ของพนักงานอัยการดังกล่าวมีระเบียบสำนักงานอัยการสูงสุด ว่าด้วยการดำเนินคดีอาญาของพนักงานอัยการ พ.ศ.2547 (ที่แก้ไขเพิ่มเติม) หมวดที่ 3 บัญญัติให้แนวทางไว้ กล่าวคือ พนักงานอัยการต้องพิจารณาข้อเท็จจริงและพยานหลักฐานในสำนวนซึ่งพิสูจน์ความผิดหรือความบริสุทธิ์ของผู้ต้องหา แนวทางการดำเนินคดีจากพยานหลักฐานและข้อกฎหมายว่าจะทำให้ศาลลงโทษผู้ต้องหาได้หรือไม่ ทั้งนี้ ตามข้อ 69 ของระเบียบดังกล่าว ได้บัญญัติให้พนักงานอัยการพิจารณาพยานหลักฐานในคดีให้ได้ความแน่ชัดว่าผู้ต้องหาได้กระทำความผิดหรือไม่ก่อนจะมีความเห็นและคำสั่ง หากยังไม่แน่ชัดก็ให้สั่งให้พนักงานสอบสวนทำการสอบสวนเพิ่มเติมหรือสั่งให้ส่งพยานมาเพื่อซักถามตามรูปคดีก็ได้ จากนั้น เมื่อพนักงานอัยการเห็นว่าข้อเท็จจริงในคดีสิ้นกระแสความและคดีมีพยานหลักฐานเพียงพอในการทำความเห็นและคำสั่งแล้ว โดยทั่วไปพนักงานอัยการจะมีคำสั่งทางคดีอย่างหนึ่งอย่างใดใน 3 ลักษณะ ได้แก่ คำสั่งฟ้อง คำสั่งไม่ฟ้อง และคำสั่งยุติคดีกรณีสิทธิฟ้องคดีอาญาระงับ (สำนักงานอัยการสูงสุด, 2555:38-42)

นอกจากอำนาจในการสั่งคดีแล้ว ในกรณีที่มีคำสั่งฟ้องผู้ต้องหา พนักงานอัยการมีบทบาทหลักในชั้นพิจารณาคดี โดยจะต้องเชื่อมโยงพยานหลักฐานที่มีในสำนวนการสอบสวนทั้งหมดแล้วนำเสนอต่อศาลอย่างเป็นเหตุเป็นผลเพื่อโน้มน้าวให้ศาลรับฟังพยานหลักฐานที่ฝ่ายโจทก์นำเสนอ โดยในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ พนักงานอัยการจะต้องมีความรู้ความเข้าใจในพยานหลักฐานที่อยู่ในรูปข้อมูลอิเล็กทรอนิกส์หรือพยานหลักฐานดิจิทัลในระดับที่ดี เพื่อประโยชน์ในการนำเสนอพยานหลักฐานให้ศาลเข้าใจ และเพื่อซักถามติงในกรณีที่ทนายจำเลยถามค้านพยานหลักฐานในคดีด้วยข้อเท็จจริงเกี่ยวกับการทำงานของคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ ซึ่งหากพนักงานอัยการขาดความเข้าใจในระบบการทำงานของอุปกรณ์ ระบบ หรือข้อมูลคอมพิวเตอร์แล้วอาจส่งผลให้เสียเปรียบในทางคดีได้

6. ศาล

ในคดีอาญาซึ่งจำเลยปฏิเสธว่าไม่ได้กระทำความผิดตามฟ้อง หรือคดีซึ่งจำเลยให้การรับสารภาพว่ากระทำความผิดแต่คดีดังกล่าวมีอัตราโทษจำคุกขั้นต่ำตั้งแต่ 5 ปีขึ้นไป โจทก์มีหน้าที่ในการสืบพยานเพื่อให้ศาลรับฟังว่าจำเลยเป็นผู้กระทำความผิดตามบทกฎหมายที่มีการกล่าวหาจริง โดยศาลมีอำนาจในการพิจารณาพยานหลักฐานที่มีการนำสืบในชั้นพิจารณาคดี แล้ววินิจฉัยชั่งน้ำหนักพยานหลักฐานว่าเพียงพอที่จะรับฟังโดยปราศจากข้อสงสัยอันสมควรว่ามีการกระทำความผิดตามฟ้องและจำเลยคือผู้กระทำความผิดหรือไม่ แล้วมีคำสั่งหรือคำพิพากษาต่อไป โดยศาลต้องใช้ความระมัดระวังในการรับฟังพยานหลักฐานและชั่งน้ำหนักของพยานหลักฐานทั้งของฝ่ายโจทก์และของฝ่ายจำเลย ให้เป็นไปโดยชอบด้วยกฎหมายว่าด้วยพยานหลักฐานดังจะได้กล่าวในหลักกฎหมายเกี่ยวกับพยานหลักฐานในคดีอาญาต่อไป

กฎหมายที่สำคัญในการดำเนินคดีอาชญากรรมคอมพิวเตอร์

บทบัญญัติกฎหมายสำคัญเกี่ยวข้องกับการดำเนินคดีอาชญากรรมคอมพิวเตอร์ที่มีความเกี่ยวข้องกับงานวิจัยนี้ ได้แก่

1. ประมวลกฎหมายอาญา(ออนไลน์, 2562)บัญญัติฐานความผิดอาญาซึ่งมีการกระทำผ่านคอมพิวเตอร์ คือ

1.1 ความผิดเกี่ยวกับการฉ้อโกงและฉ้อโกงประชาชนมาตรา 341-343

1.2 ความผิดเกี่ยวกับการปลอมเอกสารมาตรา 264-268

1.3 ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์มาตรา 269/1-269/7

1.4 ความผิดเกี่ยวกับสื่อลามกอนาจารเด็กมาตรา 287-287/2

2. ประมวลกฎหมายวิธีพิจารณาความอาญา(ออนไลน์, 2562)บัญญัติวิธีสบัญญัติในขั้นตอนการสืบสวนสอบสวน (มาตรา 17-21 มาตรา 130-140) การพิจารณาคดีสั่งฟ้องหรือสั่งไม่ฟ้อง (มาตรา 141-147) พยานหลักฐาน (มาตรา 226-244/1) การพิจารณาคดีในศาล(มาตรา 172-181)

3. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550(ที่แก้ไขเพิ่มเติม)(ออนไลน์, 2562)แบ่งบัญญัติออกเป็น 2 หมวด หมวดที่ 1 เกี่ยวกับความผิดเกี่ยวกับคอมพิวเตอร์ ได้แก่ การเข้าถึงโดยมิชอบ (มาตรา 5-7) การดักรับข้อมูลคอมพิวเตอร์โดยมิชอบและการรบกวนข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ (มาตรา 8-10) การใช้อุปกรณ์การเข้าถึงโดยมิชอบ (มาตรา 13)การหลอกลวงบนอินเทอร์เน็ต (มาตรา 14) และหมวดที่ 2 เกี่ยวกับอำนาจของพนักงานเจ้าหน้าที่ตามกฎหมายเช่น คำสั่งให้เก็บรักษาข้อมูลคอมพิวเตอร์ คำสั่งให้ส่งข้อมูลคอมพิวเตอร์ที่จัดเก็บไว้โดยบุคคลที่สาม อำนาจการตรวจค้นและยึดข้อมูลคอมพิวเตอร์ (มาตรา 18-19)อำนาจเก็บรวบรวมข้อมูลจราจรทางคอมพิวเตอร์แบบเรียลไทม์และดักรับข้อมูลเนื้อหา (มาตรา 26)เป็นต้น

4. พระราชบัญญัติป้องกันและปราบปรามการค้ามนุษย์ พ.ศ.2551 (ที่แก้ไขเพิ่มเติม)(ออนไลน์, 2562)บัญญัติการกระทำที่เข้าข่ายเป็นความผิดฐานค้ามนุษย์ (มาตรา 6-10) อำนาจหน้าที่ของพนักงานเจ้าหน้าที่ตามกฎหมาย(มาตรา 27-32)โดยการปฏิบัติหน้าที่ตามพระราชบัญญัติดังกล่าว ให้ถือว่าพนักงานเจ้าหน้าที่เป็นเจ้าพนักงานตามประมวลกฎหมายอาญาด้วย

5. พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ.2547(ที่แก้ไขเพิ่มเติม) (ออนไลน์, 2562)บัญญัติคดีพิเศษที่จะต้องดำเนินการสืบสวนและสอบสวนตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ.2547 (ที่แก้ไขเพิ่มเติม)(มาตรา 21) อำนาจของพนักงานสอบสวนคดีพิเศษ (มาตรา 24-25 และมาตรา 27)

6. พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556(ออนไลน์, 2562)บัญญัติเกี่ยวกับการกระทำที่เข้าข่ายเป็นความผิดการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ (มาตรา 5-9)อำนาจของพนักงานสอบสวนและพนักงานเจ้าหน้าที่ตามกฎหมาย (มาตรา 14)อำนาจปฏิบัติการอำพราง หรือ Undercover (มาตรา 19)อำนาจเคลื่อนย้ายภายใต้การควบคุม หรือ Control Delivery (มาตรา 20)อำนาจสะกดรอย หรือ Surveillance (มาตรา 21)

หลักกฎหมายเกี่ยวกับพยานหลักฐานในคดีอาญา

1. ประเภทของพยานหลักฐาน

ประเภทของพยานหลักฐานในคดีอาญานั้น บัญญัติอยู่ในประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226 (ออนไลน์, 2562) ว่า

พยานวัตถุ พยานเอกสาร หรือพยานบุคคลซึ่งน่าจะพิสูจน์ได้ว่าจำเลยมีผิดหรือบริสุทธิ์ ให้อ้างเป็นพยานหลักฐานได้ แต่ต้องเป็นพยานชนิดที่มิได้เกิดขึ้นจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวงหรือโดยมิชอบประการอื่น และให้สืบตามบทบัญญัติแห่งประมวลกฎหมายนี้หรือกฎหมายอื่นอันว่าด้วยการสืบพยาน

ตามหลักกฎหมายลักษณะพยานของไทย พยานหลักฐานแบ่งออกเป็น 4 ประเภท (สราวุธปิติยาศักดิ์, 2561 : 310-311)

1.1 พยานบุคคล หมายถึง ถ้อยคำของบุคคลที่มาเบิกความต่อหน้าศาล ซึ่งจะเป็นคำเบิกความด้วยวาจาหรือลายลักษณ์อักษรของบุคคลนั้นโดยตรง ผ่านล่าม หรือกิริยาอาการที่แสดงความหมายได้

1.2 พยานเอกสารหมายถึง ข้อความที่บันทึกไว้ไม่ว่าจะด้วยวิธีใด เช่น การเขียน พิมพ์ แกะสลัก ไม่ว่าจะบันทึกในวัสดุใด เช่น กระดาษ ผ้า โลหะ เป็นต้น และไม่ว่าจะเป็นตัวอักษร ตัวเลข เครื่องหมาย สัญลักษณ์ใดๆ ที่สามารถสื่อหรือแสดงความหมายของสิ่งที่บันทึกไว้ให้ศาลเข้าใจได้

1.3 พยานวัตถุ หมายถึง วัตถุใดๆ ที่เสนอต่อศาลเพื่อให้ได้ข้อเท็จจริงอันเป็นประโยชน์ต่อการพิจารณาคดี เช่น มีด ท่อนไม้ เป็นต้น

1.4 พยานผู้เชี่ยวชาญ หมายถึง บุคคลที่ศาลแต่งตั้งโดยศาลเห็นสมควรหรือโดยที่คู่ความร้องขอให้ทำหน้าที่แสดงความคิดเห็นในเรื่องใดเรื่องหนึ่งซึ่งบุคคลนั้นมีความเชี่ยวชาญ

ส่วนคำว่า “พยานหลักฐานดิจิทัล” นั้น ยังไม่มีการบัญญัติเป็นพยานหลักฐานประเภทใดในประมวลกฎหมายวิธีพิจารณาความอาญา เนื่องจากกฎหมายลักษณะพยานของไทยถูกบัญญัติขึ้นในขณะที่ยังไม่รู้จักข้อมูลอิเล็กทรอนิกส์ จึงเกิดข้อสงสัยขึ้นว่า ข้อมูลอิเล็กทรอนิกส์จัดเป็นพยานหลักฐานประเภทใด และคู่ความสามารถนำเสนอข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานต่อศาลได้หรือไม่

ในเวลาต่อมา พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 มาตรา 4 (ออนไลน์, 2562) ได้บัญญัตินิยามความหมายของคำว่า “ข้อมูลอิเล็กทรอนิกส์” ว่าหมายถึง “ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร”ซึ่ง สราวุธปิติยาศักดิ์ (2561 : 302-307) อธิบายว่า ในทางเทคนิคข้อมูลอิเล็กทรอนิกส์สามารถแบ่งได้เป็น 3 ประเภท คือ

1. ข้อมูลอิเล็กทรอนิกส์ที่มนุษย์สร้างขึ้น แล้วบันทึกจัดเก็บไว้ในระบบคอมพิวเตอร์ เช่น ข้อความอิเล็กทรอนิกส์ที่เก็บบันทึกไว้ในแฟ้มจดหมายอิเล็กทรอนิกส์ ข้อความอิเล็กทรอนิกส์ในเว็บไซต์ซึ่งอาจอยู่ในรูปของข้อความ (Texts)รูปภาพ (Graphics) หรือเสียง (Audio)

2. ข้อมูลอิเล็กทรอนิกส์ที่ระบบคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์สร้างขึ้นแล้วได้ถูกบันทึกจัดเก็บไว้โดยอัตโนมัติ เช่น ข้อมูลอิเล็กทรอนิกส์ที่บันทึกในแฟ้มประวัติ (History Files) หรือข้อมูลอิเล็กทรอนิกส์ที่บันทึกในแฟ้มลงบันทึกเข้าออก (Log File) หลังจากที่ผู้ใช้ทำการค้นหารายการแฟ้มข้อมูล (Browse) ผ่านเครือข่ายอินเทอร์เน็ต

3. ข้อมูลอิเล็กทรอนิกส์ผสม ได้แก่ ข้อมูลอิเล็กทรอนิกส์ที่ประกอบไปด้วยข้อมูลข้อมูลอิเล็กทรอนิกส์ที่มนุษย์เป็นผู้สร้างขึ้นและข้อมูลอิเล็กทรอนิกส์ที่ระบบคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์สร้างขึ้น เช่น ข้อมูลอิเล็กทรอนิกส์ที่เป็นแผนภูมิ (Chart)ซึ่งเป็นผลลัพธ์ที่ได้จากการที่มนุษย์ได้สร้างข้อมูลอิเล็กทรอนิกส์ที่เป็นข้อมูลดิบ (Data) ป้อนเข้าไปยังเครื่องคอมพิวเตอร์ให้ระบบคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์นั้นทำการประมวลออกมาเป็นข้อมูลอิเล็กทรอนิกส์ที่เรียกว่า “สารสนเทศ (Information)”ข้อมูลอิเล็กทรอนิกส์ที่ใช้เป็นพยานหลักฐานสามารถพบใน 2 ระบบใหญ่ๆ คือ

1. ข้อมูลอิเล็กทรอนิกส์ในระบบคอมพิวเตอร์โดยในคดีอาญาอาจพบข้อมูลอิเล็กทรอนิกส์ในเครื่องคอมพิวเตอร์และอุปกรณ์ของผู้กระทำความผิดหรือของเหยื่อ รวมถึงเครื่องคอมพิวเตอร์และอุปกรณ์ระหว่างทาง โดยส่วนของเครื่องคอมพิวเตอร์ที่สามารถพบข้อมูลอิเล็กทรอนิกส์เพื่อใช้เป็นพยานหลักฐานนั้น ได้แก่ หน่วยความจำเข้าถึงได้โดยการสุ่ม หรือ “แรม” (Ram) และจานบันทึกแบบแข็ง หรือ “ฮาร์ดดิสก์” (Hard Disk)

2. ข้อมูลอิเล็กทรอนิกส์ในระบบเครือข่ายคอมพิวเตอร์โดยระบบเครือข่ายคอมพิวเตอร์ หรือ “Computer Network”หมายถึง ระบบการสื่อสารระหว่างคอมพิวเตอร์จำนวนตั้งแต่สองเครื่องขึ้นไปที่เชื่อมโยงเป็นเครือข่ายเพื่อสะดวกต่อการใช้ข้อมูลและติดต่อสื่อสารแลกเปลี่ยนข้อมูลระหว่างกัน ระบบเครือข่ายคอมพิวเตอร์อาจแบ่งได้เป็น 2 ประเภทใหญ่ คือ ระบบเครือข่ายอินเทอร์เน็ต (Internet) ที่เชื่อมต่อระหว่างเครือข่ายหลายๆเครือข่ายเข้าด้วยกันผู้ใช้งานอินเทอร์เน็ตจึงสามารถสืบค้นข้อมูลและข่าวสารต่างๆได้ทั่วโลก ตลอดจนสามารถติดต่อสื่อสารถึงระหว่างกันได้ในหลายทาง เช่น อีเมล กระดานสนทนา เว็บไซต์ เป็นต้น และระบบเครือข่ายอินทราเน็ต (Intranet) ซึ่งเป็นระบบเครือข่ายคอมพิวเตอร์ภายในองค์การสำหรับผู้ใช้ที่เป็นสมาชิกขององค์การเท่านั้น โดยมีเซิร์ฟเวอร์ (Server) หรือเครื่องคอมพิวเตอร์แม่ข่ายขององค์การทำหน้าที่จัดเก็บและให้บริการแฟ้มข้อมูลและทรัพยากรอื่นๆกับคอมพิวเตอร์เครื่องลูกข่ายอื่นๆ ในระบบอินทราเน็ต ผู้ใช้งานอินทราเน็ตสามารถมีเว็บไซต์และอีเมลของตนได้เช่นเดียวกับการใช้งานอินเทอร์เน็ต ตลอดจนสามารถเข้าถึงข้อมูลต่างๆ นอกจากนี้ ระบบเครือข่ายอินทราเน็ตมักมีการเชื่อมต่อกับระบบเครือข่ายอินเทอร์เน็ต โดยจะมีการติดตั้งไฟร์วอลล์ (Firewall) หรือด่านกันบุกรุก ซึ่งได้แก่อุปกรณ์หรือโปรแกรมสำหรับควบคุมการผ่านเข้าออกของข้อมูล ทำให้ผู้ดูแลด้านความปลอดภัยด้านสารสนเทศขององค์การสามารถควบคุมและตรวจสอบการเข้าถึงระบบเครือข่ายอินเทอร์เน็ตขององค์การ เช่น การควบคุมการเข้าเว็บไซต์ลามกหรือการตรวจสอบผู้บุกรุกระบบเครือข่ายอินทราเน็ต เป็นต้น

เมื่อพิเคราะห์ในเชิงพยานหลักฐาน พบว่า ข้อมูลอิเล็กทรอนิกส์มีลักษณะพิเศษที่แตกต่างกับข้อมูลที่อยู่ในรูปของกระดาษ (สราวุธปิติยาศักดิ์, 2561 : 309-310) กล่าวคือ ข้อมูลอิเล็กทรอนิกส์มักถูกบันทึกจัดเก็บไว้ในอุปกรณ์อิเล็กทรอนิกส์ เช่น ในฮาร์ดดิสก์ของ

เครื่องคอมพิวเตอร์ และสามารถทำซ้ำไปยังอุปกรณ์บันทึกข้อมูลอื่นๆ เช่น แผ่นดีวีดี แผ่นซีดี และยูเอสบีแฟลชไดร์ฟ ซึ่งอาจทำซ้ำได้นับร้อยครั้งโดยดูเหมือนข้อมูลต้นฉบับทุกประการและไม่ทำให้คุณภาพของข้อมูลนั้นลดลงแต่อย่างใด ทำให้การตรวจหาต้นฉบับด้วยตาเปล่าจึงไม่อาจกระทำได้ นอกจากนี้ ข้อมูลอิเล็กทรอนิกส์ที่ถูกลบทางเทคนิคยังคงบันทึกอยู่ในสื่อบันทึกนั้นต่อไปจนกว่าจะมีข้อมูลอิเล็กทรอนิกส์ใหม่มาบันทึกทับลงบนที่ที่บันทึกเดิมนั้น ด้วยเหตุนี้ถึงแม้ว่าข้อมูลอิเล็กทรอนิกส์จะถูกลบแล้วก็ยังสามารถกู้คืน (Recover) กลับมาได้โดยโปรแกรมคอมพิวเตอร์ในการกู้ข้อมูล ในส่วนแฟ้มข้อมูลของข้อมูลอิเล็กทรอนิกส์จะมีส่วนที่เรียกว่า “เมตาเดตา หรือเมตาดาตา (Meta Data)” ซึ่งเป็นข้อมูลที่ถูกซ่อนไว้ (Hidden Data)เป็นส่วนประกอบ เมตาเดตานี้เป็นข้อมูลที่ถูกสร้างขึ้นอัตโนมัติโดยเครื่องคอมพิวเตอร์ ตัวอย่างเช่น ข้อมูลอิเล็กทรอนิกส์ที่เป็นรูปภาพจะประกอบด้วยเมตาเดตา คือ ขนาดของภาพ (Image Size) ความละเอียดของสี (Colour Depth) ความละเอียดของภาพ (Image Resolution) วันเดือนปีและเวลาที่บันทึกภาพ รุ่นของกล้องที่ใช้บันทึกและอื่นๆ ส่วนข้อมูลอิเล็กทรอนิกส์ที่เป็นอักษร (Text) มักประกอบด้วยเมตาเดตา คือ ขนาดของเอกสาร ตัวเจ้าของหรือผู้สร้างเอกสาร วันเดือนปีและเวลาที่สร้างเอกสาร ตลอดจนแหล่งกำเนิดของข้อมูลนั้น เช่น ระบบคอมพิวเตอร์มักสร้างเมตาเดตาเหล่านี้ขึ้นโดยอัตโนมัติในอีเมล เช่น ชื่อผู้ส่งและที่อยู่อีเมลของผู้ส่งจดหมาย วันเดือนปีและเวลาที่ส่งอีเมล ตัวผู้รับและที่อยู่อีเมลของผู้รับสำเนาคู่ฉบับของอีเมล

สำหรับหลักเกณฑ์การรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานนั้น พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 มาตรา 11 (ออนไลน์, 2562) ได้บัญญัติว่า

ห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในกระบวนการพิจารณาตามกฎหมายทั้งในคดีแพ่ง คดีอาญา หรือคดีอื่นใด เพียงเพราะเหตุว่าเป็นข้อมูลอิเล็กทรอนิกส์

ในการชั่งน้ำหนักพยานหลักฐานว่าข้อมูลอิเล็กทรอนิกส์จะเชื่อถือได้หรือไม่เพียงใดนั้น ให้พิเคราะห์ถึงความน่าเชื่อถือของลักษณะหรือวิธีการที่ใช้สร้าง เก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์ ลักษณะหรือวิธีการเก็บรักษา ความครบถ้วน และไม่มีการเปลี่ยนแปลงของข้อความ ลักษณะ หรือวิธีการที่ใช้ในการระบุหรือแสดงตัวผู้ส่งข้อมูล รวมทั้งพฤติการณ์ที่เกี่ยวข้องทั้งปวง

ให้นำความในวรรคหนึ่งมาใช้บังคับกับสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์ด้วย

ในประเด็นว่าข้อมูลอิเล็กทรอนิกส์จัดเป็นพยานวัตถุหรือพยานเอกสารตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226 ขึ้นอยู่กับว่า หากข้อมูลอิเล็กทรอนิกส์ถูกบันทึกอยู่ในฮาร์ดดิสก์หรือสื่อบันทึกอื่นใด เช่น แผ่นซีดี แผ่นดีวีดี ซึ่งไม่สามารถรับรู้ได้ด้วยการเห็นหรือโดยประสาทตา แต่ต้องใช้เครื่องคอมพิวเตอร์ในการอ่าน ถ้ามีการอ้างฮาร์ดดิสก์หรือสื่อบันทึกดังกล่าวเป็นพยาน จะไม่ถือว่าเป็นพยานเอกสารแต่ถือเป็นพยานวัตถุ แต่หากข้อมูลอิเล็กทรอนิกส์ดังกล่าวถูกนำมาพิมพ์ออก (Print Out) แล้วนำผลลัพธ์ที่ได้นำมาเสนอต่อศาล พยานหลักฐานทางคอมพิวเตอร์นั้น

อาจรับฟังได้ในฐานะที่เป็นพยานเอกสาร ซึ่งในแนวทางการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานของศาลนั้นจะต้องปรากฏว่าระบบการบันทึก การสร้าง การเก็บรักษา และการเรียกข้อมูล หรือการใช้งานของคอมพิวเตอร์นั้นเป็นปกติเช่นที่เคยทำมา ไม่มีสิ่งผิดเพี้ยนหรือบิดเบือน ก็น่าเชื่อว่าเป็นข้อมูลที่ถูกต้องได้ (สอดคล้องกับแนวคำพิพากษาฎีกาที่ 7264/2542) แตกต่างจากในคดีแพ่งซึ่งปัจจุบันมีบทบัญญัติกฎหมายรองรับวิธีการนำสืบและรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์โดยเฉพาะ เช่น ข้อกำหนดคดีทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ พ.ศ.2540 ข้อ 33-36 ข้อกำหนดคดีภาษีอากร พ.ศ.2544 ข้อ 30-33 ข้อกำหนดคดีล้มละลาย พ.ศ.2549 ข้อ 20-23 (สราวุธปิติยาศักดิ์, 2561: 311-313)

2. การรับฟังพยานหลักฐาน(จรัญภักดีธนากุล, 2561 :303-447)

การรับฟังพยานหลักฐานเป็นคนละอย่างกับการชั่งน้ำหนักพยานหลักฐาน กล่าวคือ การชั่งน้ำหนักพยานหลักฐานนั้นเป็นเรื่องของการใช้ดุลพินิจโดยแท้ หากมีการโต้แย้งในเรื่องของการชั่งน้ำหนักพยานหลักฐานถือว่าเป็นปัญหาข้อเท็จจริง ส่วนเรื่องการรับฟังพยานหลักฐานนั้นโดยหลักวิชาถือว่าเป็นปัญหาที่ผสมกันอยู่ระหว่างข้อเท็จจริงและข้อกฎหมาย โดยพยานหลักฐานทุกชนิดที่สามารถบ่งชี้ถึงข้อเท็จจริงที่พิพาทกันในคดีได้ ย่อมรับฟังเป็นพยานหลักฐานในคดีได้ แต่หลักดังกล่าวมีข้อยกเว้นในกรณีที่มีกฎหมายบัญญัติหรือวางหลักเกณฑ์ห้ามมิให้รับฟังพยานหลักฐานชนิดใดหรือประเภทใดไว้ พยานหลักฐานชนิดนั้นหรือประเภทนั้นก็จะเข้าลักษณะเป็นพยานหลักฐานที่นำมาใช้เป็นพยานหลักฐานในคดีไม่ได้ กฎหมายที่บัญญัติห้ามไม่ให้รับฟังพยานหลักฐานในระบบกฎหมายของไทยมีหลายกรณี รวมเรียกชื่อกฎหมายเหล่านั้นว่า “บทตัดพยานหลักฐาน” หรือที่ตรงกับของต่างประเทศที่เรียกว่า “Exclusionary Rules”โดยจรัญภักดีธนากุล (2561 : 306-312) ให้ข้อสังเกตว่าการกำหนดบทตัดพยานหลักฐานของแต่ละประเทศมักมองเปรียบเทียบระหว่างคุณค่าในเชิงพิสูจน์ (Probative Value) ของพยานหลักฐานชนิดนั้นว่ามีสูงหรือต่ำอย่างไร เปรียบเทียบกับผลกระทบทางด้านอคติ (Prejudicial Effect) ที่จะทำให้การวินิจฉัยข้อเท็จจริงคลาดเคลื่อนไปว่ามีมากน้อยเพียงใด โดยหลักทั่วไปถ้าไม่มีกฎหมายตัดหรือห้ามรับฟัง พยานหลักฐานทุกชนิดย่อมรับฟังได้

บทตัดพยานหลักฐานในส่วนของพยานหลักฐานในคดีอาญาที่สำคัญ ได้แก่ (จรัญภักดีธนากุล, 2561 : 321-377)

2.1 บทตัดพยานหลักฐานที่เกิดขึ้นโดยมิชอบ

กฎหมายไทยมีบทบัญญัติเรื่องบทตัดพยานหลักฐานที่เกิดขึ้นโดยมิชอบอยู่ในประมวลกฎหมายวิธีพิจารณาความอาญา (ออนไลน์, 2562) ไว้ 4 กรณีได้แก่

2.1.1 มาตรา 226 บัญญัติว่า

พยานวัตถุ พยานเอกสาร หรือพยานบุคคลซึ่งน่าจะพิสูจน์ได้ว่าจำเลยมีความผิดหรือบริสุทธิ์ ให้อ้างเป็นพยานหลักฐานได้ แต่ต้องเป็นพยานชนิดที่มิได้เกิดขึ้นจากการ

จูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวงหรือโดยมิชอบประการอื่น และให้สืบตามบทบัญญัติแห่งประมวลกฎหมายนี้หรือกฎหมายอื่นอันว่าด้วยการสืบพยานหมายความว่า พยานหลักฐานใดก็ตาม ถึงแม้จะมีคุณสมบัติสามารถพิสูจน์ความผิดหรือบริสุทธิ์ของจำเลยได้ แต่ถ้าเป็นพยานหลักฐานที่เกิดจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบประการอื่นแล้ว ก็ย่อมต้องห้ามรับฟังเป็นพยานหลักฐาน

2.1.2 มาตรา 84 วรรคสี่บัญญัติว่า

ถ้อยคำใดๆ ที่ผู้ถูกจับให้ไว้ต่อเจ้าพนักงานผู้จับ หรือพนักงานฝ่ายปกครองหรือตำรวจในชั้นจับกุมหรือรับมอบตัวผู้ถูกจับ ถ้าถ้อยคำนั้นเป็นคำรับสารภาพของผู้ถูกจับว่าตนได้กระทำความผิดห้ามมิให้รับฟังเป็นพยานหลักฐาน แต่ถ้าเป็นถ้อยคำอื่น จะรับฟังเป็นพยานหลักฐานในการพิสูจน์ความผิดของผู้ถูกจับได้ต่อเมื่อได้มีการแจ้งสิทธิตามวรรคหนึ่ง หรือตามมาตรา 83 วรรคสอง แก่ผู้ถูกจับแล้วแต่กรณี

หมายความว่า คำให้การรับสารภาพของผู้ต้องหาในชั้นจับกุมแม้จะให้การโดยสมัครใจแต่กฎหมายห้ามไม่ให้เอามาใช้เป็นพยานหลักฐานพิสูจน์ความผิดของผู้ต้องหา แต่หากเป็น “ถ้อยคำอื่น” ยังอาจรับฟังเป็นพยานหลักฐานพิสูจน์ความผิดในชั้นพิจารณาได้ โดยมีเงื่อนไขว่าพนักงานเจ้าหน้าที่ผู้จับหรือผู้รับมอบตัวผู้ถูกจับไว้นั้นจะต้องแจ้งสิทธิต่างๆตามกฎหมายให้ผู้ถูกจับได้ทราบก่อนที่ผู้นั้นจะให้ถ้อยคำ จึงจะนำมาใช้เป็นพยานหลักฐานยันผู้นั้นได้ ตัวอย่างของ “ถ้อยคำอื่น” ที่ไม่ใช่การรับสารภาพในชั้นจับกุม หมายถึงข้อความหรือเรื่องราวอื่นๆ นอกเหนือจากคำว่า “รับสารภาพ” ซึ่งอาจจะเป็นคำซัดทอดของผู้ร่วมกระทำความผิดอื่นๆ หรือข้อมูลอันเป็นรายละเอียดของการกระทำความผิดในกรณีที่เป็นคำให้การภาคเสธยอมรับข้อเท็จจริงที่เกี่ยวเนื่องในการกระทำความผิดคดีนั้นบางข้อ แต่ยกข้อโต้เถียงปฏิเสธในข้อเท็จจริงบางข้อ

2.1.3 มาตรา 134/4 วรรคท้ายโดยมาตรา 134/4 บัญญัติว่า

ในการถามคำให้การผู้ต้องหาให้พนักงานสอบสวนแจ้งให้ผู้ต้องหาทราบก่อนว่า

(1) ผู้ต้องหามีสิทธิที่จะให้การหรือไม่ก็ได้ ถ้าผู้ต้องหาให้การถ้อยคำที่ผู้ต้องหาให้การนั้นอาจใช้เป็นพยานหลักฐานในการพิจารณาคดีได้

(2) ผู้ต้องหามีสิทธิให้ทนายความหรือผู้ซึ่งตนไว้วางใจเข้าฟังการสอบปากคำตนได้เมื่อผู้ต้องหาเต็มใจให้การอย่างใดก็ให้จดคำให้การไว้ ถ้าผู้ต้องหาไม่เต็มใจให้การเลยก็ให้บันทึกไว้ถ้อยคำใด ๆ ที่ผู้ต้องหาให้ไว้ต่อพนักงานสอบสวนก่อนมีการแจ้งสิทธิตามวรรคหนึ่ง หรือก่อนที่จะดำเนินการตามมาตรา 134/1 มาตรา 134/2 และมาตรา 134/3 จะรับฟังเป็นพยานหลักฐานในการพิสูจน์ความผิดของผู้นั้นไม่ได้

เมื่อพนักงานสอบสวนแจ้งข้อกล่าวหาแก่ผู้ต้องหาแล้ว ก่อนที่จะสอบปากคำผู้ต้องหา พนักงานสอบสวนต้องปฏิบัติตามมาตรา 134/1 มาตรา 134/2 มาตรา 134/3 และมาตรา 134/4 วรรคหนึ่ง ให้ครบถ้วนก่อน มิฉะนั้นแล้วคำให้การของผู้ต้องหาเป็นพยานหลักฐานที่ได้มาโดยมิชอบด้วยกฎหมายตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226

2.1.4 มาตรา 226/1บัญญัติว่า

ในกรณีที่ความปรากฏแก่ศาลว่า พยานหลักฐานใดเป็นพยานหลักฐานที่เกิดขึ้นโดยชอบแต่ได้มาเนื่องจากการกระทำโดยมิชอบ หรือเป็นพยานหลักฐานที่ได้มาโดยอาศัยข้อมูลที่เกิดขึ้นหรือได้มาโดยมิชอบ ห้ามมิให้ศาลรับฟังพยานหลักฐานนั้น เว้นแต่การรับฟังพยานหลักฐานนั้นจะเป็นประโยชน์ต่อการอำนวยความยุติธรรมมากกว่าผลเสียอันเกิดจากผลกระทบต่อมาตรฐานของระบบงานยุติธรรมทางอาญาหรือสิทธิเสรีภาพพื้นฐานของประชาชน

ในการใช้ดุลพินิจรับฟังพยานหลักฐานตามวรรคหนึ่ง ให้ศาลพิจารณาถึงพฤติการณ์ทั้งปวงแห่งคดี โดยต้องคำนึงถึงปัจจัยต่างๆ ดังต่อไปนี้ด้วย

(1) คุณค่าในเชิงพิสูจน์ ความสำคัญ และความน่าเชื่อถือของพยานหลักฐานนั้น

(2) พฤติการณ์และความร้ายแรงของความผิดในคดี

(3) ลักษณะและความเสียหายที่เกิดจากการกระทำโดยมิชอบ

(4) ผู้ที่กระทำการโดยมิชอบอันเป็นเหตุให้ได้พยานหลักฐานมานั้นได้รับการลงโทษหรือไม่เพียงใด

พยานหลักฐานที่ได้มาเนื่องจาก “การกระทำที่มิชอบ” ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226 และมาตรา 226/1อาจเป็นการกระทำของเจ้าหน้าที่ของรัฐหรือเป็นการกระทำของบุคคลที่มิใช่เจ้าหน้าที่ของรัฐก็ได้ ในเรื่องนี้ศาลฎีกาเคยวินิจฉัยไว้ใน **คำพิพากษาศาลฎีกาที่ 2414/2551** (ศูนย์เทคโนโลยีสารสนเทศ และการสื่อสาร ศาลฎีกา, ออนไลน์, 2562) ว่า การที่จำเลยไปที่บ้านของ ว. พร้อมกับทนายความและเจ้าพนักงานตำรวจอีกคนหนึ่งเพื่อพูดคุยเกี่ยวกับเรื่องการเบิกเงินของ บ. และการใช้กระแสไฟฟ้าจากโรงงานจำเลย โดยเจ้าพนักงานตำรวจผู้นั้นได้แอบบันทึกเหตุการณ์ทั้งภาพและเสียงไว้ด้วยพฤติการณ์ในการบันทึกเหตุการณ์ดังกล่าวเป็นการลักลอบกระทำก่อนวันที่จำเลยอ้างตนเองเข้าเบิกความเป็นพยานเพียง 1 วัน เพราะต้องการจะได้ข้อมูลที่แอบบันทึกไว้ เนื่องจากจำเลยฉีกเอกสารหลักฐานที่ว่าจ้าง บ. ก่อสร้างโรงงานทิ้งไปแล้วจึงพยายามหาหลักฐานใหม่ ดังนั้น ข้อมูลดังกล่าวจึงเป็นพยานหลักฐานที่จำเลยทำขึ้นใหม่ด้วยการทำเป็นดีกับ ว. แล้วลักลอบบันทึกเหตุการณ์นั้นไว้ ถือได้ว่า เป็นพยานหลักฐานที่เกิดขึ้นจากการหลอกลวงและด้วยวิธีการที่มิชอบ ต้องห้ามมิให้อ้างเป็นพยานหลักฐานตาม พระราชบัญญัติจัดตั้งศาล

ทรัพย์สินทางปัญญาและการค้าระหว่างประเทศและวิธีพิจารณาคดีทรัพย์สินทางปัญญาและการค้าระหว่างประเทศฯ มาตรา 26 ประกอบประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226

ส่วนในประเด็นเกี่ยวกับพยานหลักฐานที่เจ้าหน้าที่ได้มาจากการค้นโดยมิชอบตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 93 พยานหลักฐานที่เจ้าหน้าที่ได้มาโดยการค้นที่มิชอบนั้น เคยมีคำพิพากษาศาลฎีกาตัดสินว่ารับฟังเป็นพยานหลักฐานได้ไม่ต้องห้ามรับฟังตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226 (คำพิพากษาศาลฎีกาที่ 837/2483, ออนไลน์, 2562; คำพิพากษาศาลฎีกาที่ 6475/2547, ออนไลน์, 2562)

ทั้งนี้มีบางกรณีซึ่งก้ำกึ่งระหว่างเป็นพยานหลักฐานที่เกิดขึ้นโดยมิชอบ ซึ่งต้องห้ามรับฟังโดยเด็ดขาดตามมาตรา 226 หรือเป็นพยานหลักฐานที่กิดขึ้นโดยชอบแต่ได้มาโดยมิชอบ อันต้องห้ามรับฟังแบบไม่เด็ดขาด มีข้อยกเว้นตามมาตรา 226/1 คือ กรณีของ **การล่อซื้อล่อขาย** (จรัญภักดีธนากุล, 2561 : 338-342)

ในเรื่องการล่อซื้อล่อขายสิ่งผิดกฎหมาย ไม่ว่าจะเป็นในเรื่องยาเสพติด การค้าประเวณี หรือการละเมิดทรัพย์สินทางปัญญานั้น แม้ไม่มีกฎหมายบัญญัติไว้ชัดเจน แต่ศาลฎีกาได้วางแนวบรรทัดฐานไว้ค่อนข้างชัดเจนเป็นระบบ โดยให้แยกเป็นสองกรณีว่าเป็นการล่อให้ผู้บริสุทธิ์กระทำผิด (Entrapment) หรือการล่อซื้อนั้นเป็นการไปล่อเพื่อจับกุมคนร้ายมาดำเนินคดี (Undercover Operation)ถ้าการล่อซื้อนั้นเป็นการไปล่อหรือก่อให้ผู้บริสุทธิ์กระทำผิดย่อมเป็นการกระทำที่ไม่ชอบด้วยกฎหมาย เป็นการใช้ให้ผู้อื่นกระทำผิด ผู้ที่ไปล่อซื้อนั้นกลายเป็นผู้ใช้ให้ผู้อื่นกระทำผิด ตัวอย่างเช่น **คำพิพากษาศาลฎีกาที่ 2429/2551**ข้อเท็จจริงโดยย่อของคดีนี้คือ สิบตำรวจตรี ส. ขอซื้อยาลดความอ้วนซึ่งมีส่วนผสมของเฟนเตอมีนจากจำเลย จำเลยบอกว่าไม่มีและที่ร้านของจำเลยไม่ได้ขายลดความอ้วนดังกล่าวสิบตำรวจตรี ส. จึงบอกว่าคนรักต้องการใช้ยาลดความอ้วน จำเลยจึงบอกว่าจำเลยมียาลดความอ้วนอยู่ 1 ชุด ที่จำเลยซื้อมาไว้รับประทานเอง สิบตำรวจตรี ส.ขอซื้อยาลดความอ้วนชุดนั้นจำเลยจึงขายให้และเมื่อมีการตรวจค้นร้านขายยาของจำเลยก็ไม่พบสิ่งของผิดกฎหมายอื่นแต่อย่างใด เมื่อจำเลยไม่มีเฟนเตอมีนของกลางไว้เพื่อขายดังที่โจทก์ฟ้อง และรับฟังไม่ได้ว่าที่ร้านขายยาของจำเลยเคยมีการขายเฟนเตอมีนมาก่อน ดังนั้น การที่จำเลยขายเฟนเตอมีนของกลางให้แก่สิบตำรวจตรี ส. จึงเกิดจากการถูกล่อให้กระทำความผิด โดยจำเลยไม่มีเจตนาจะกระทำความผิดในการขายเฟนเตอมีนมาก่อน ศาลจึงวินิจฉัยว่าพยานหลักฐานของโจทก์ดังกล่าวจึงเป็นพยานที่เกิดขึ้นโดยมิชอบโจทก์ไม่สามารถอ้างเป็นพยานหลักฐานได้ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226

การล่อซื้อล่อขายจะเป็นการแสวงหาพยานหลักฐานโดยชอบต่อเมื่อผู้กระทำความผิดนั้นได้กระทำความผิดนั้นอยู่ก่อนแล้ว แต่ถ้าผู้กระทำความผิดไม่ได้เป็นผู้ที่กระทำความผิดนั้นอยู่ก่อน แต่เจ้าพนักงานก่อให้เกิดการกระทำผิดนั้นขึ้นเองโดยชักจูงให้ผู้นั้นกระทำ

ความผิด หากเป็นคดีความผิดอันยอมความได้และผู้เสียหายมีส่วนในการกระทำดังกล่าว ศาลถือว่าผู้เสียหายนั้นไม่ใช่ผู้เสียหายโดยนิตินัย ไม่มีอำนาจร้องทุกข์หรือฟ้องคดีได้ แต่ถ้าเป็นคดีความผิดต่อแผ่นดินที่เจ้าพนักงานเป็นผู้กระทำก็ถือว่าเป็นพยานหลักฐานที่เกิดจากการกระทำที่มิชอบของเจ้าพนักงาน ศาลไม่รับฟัง เช่น ตำรวจลงประกาศผ่านสื่อสังคมออนไลน์ว่าต้องการซื้อภาพเปลือยเด็กในราคาแพง จนมีผู้ไปแสวงหาภาพนั้นมาขายให้ ทั้งที่แต่เดิมไม่เคยมีภาพหรือพฤติการณ์ขายภาพเหล่านั้นมาก่อน (ภัทรศักดิ์ วรรณแสง, ออนไลน์, 2562) ตัวอย่างเช่น **คำพิพากษาศาลฎีกาที่ 4301/2543** วินิจฉัยว่า เมื่อมีการละเมิดลิขสิทธิ์ของโจทก์ โจทก์ย่อมมีสิทธิดำเนินคดีแก่ผู้ละเมิดลิขสิทธิ์ของโจทก์ได้ทั้งทางแพ่งและทางอาญาซึ่งมีวิธีพิจารณาคดีและการรับฟังพยานหลักฐานที่แตกต่างกัน เมื่อโจทก์เลือกดำเนินคดีอาญาจึงต้องนำประมวลกฎหมายวิธีพิจารณาความอาญา มาใช้บังคับโดยอนุโลมดังนี้ ในการที่ศาลจะลงโทษจำเลยตามคำฟ้องนั้น นอกจากโจทก์จะต้องนำสืบพยานหลักฐานเพื่อพิสูจน์ให้ศาลเห็นโดยปราศจากข้อสงสัยว่าจำเลยได้กระทำความผิดตามคำฟ้องแล้ว ยังต้องได้ความว่าโจทก์เป็นผู้เสียหายที่มีอำนาจฟ้องคดีอาญาได้ด้วย จำเลยที่ 1 ไม่มีเครื่องคอมพิวเตอร์ที่มีการทำซ้ำบันทึกโปรแกรมคอมพิวเตอร์ลงในแผ่นบันทึกข้อมูลถาวรของเครื่องก่อนที่ ส. ซึ่งรับจ้างทำงานให้โจทก์จะไปล่อซื้อ แต่จะมีการประกอบเครื่องคอมพิวเตอร์แล้วมีการทำซ้ำโปรแกรมคอมพิวเตอร์ในเครื่องคอมพิวเตอร์หลังจากที่ ส. ตกลงซื้อกับจำเลยที่ 3 แล้ว จำเลยที่ 3 ต้องการแถมโปรแกรมคอมพิวเตอร์ให้แก่ ส. ตามที่ได้ตกลงกันในวันที่ ส. ไปล่อซื้อ พนักงานของจำเลยที่ 1อาจนำแผ่นบันทึกข้อมูลถาวรเครื่องต้นแบบเข้ามาใช้เป็นต้นแบบบันทึกถ่ายโปรแกรมคอมพิวเตอร์ลงไปในแผ่นบันทึกข้อมูลถาวรของเครื่องคอมพิวเตอร์เครื่องที่ ส. ล่อซื้อในช่วงเวลาหลังจากที่จำเลยที่ 1 ประกอบเครื่องคอมพิวเตอร์ที่โรงงานเสร็จและส่งไปที่สำนักงานจำเลยที่ 1 เพื่อรอส่งมอบแก่ลูกค้าที่สั่งซื้อตามเวลาที่นัดไว้ การทำซ้ำบันทึกโปรแกรมคอมพิวเตอร์ของโจทก์ลงในแผ่นบันทึกข้อมูลถาวรของเครื่องคอมพิวเตอร์ที่ ส. ล่อซื้อนั้นเป็นการทำซ้ำอันเป็นการละเมิดลิขสิทธิ์ของโจทก์หลังจากวันที่ ส. ไปล่อซื้อแล้วเพื่อมอบโปรแกรมคอมพิวเตอร์ที่ทำซ้ำให้แก่ ส. มิใช่ทำซ้ำโดยผู้กระทำมีเจตนากระทำผิดอยู่แล้วก่อนการล่อซื้อ น่าเชื่อว่าการกระทำผิดดังกล่าวเกิดขึ้นเนื่องจากการล่อซื้อของ ส. ซึ่งได้รับจ้างให้ล่อซื้อจากโจทก์เท่ากับโจทก์เป็นผู้ก่อให้ผู้อื่นกระทำผิดโจทก์ย่อมไม่อยู่ในฐานะเป็นผู้เสียหายโดยนิตินัยที่มีอำนาจฟ้องคดีนี้ได้ (ต่อมามี คำพิพากษาศาลฎีกาที่ 4085/2545, ออนไลน์, 2562 วางหลักการทำนองเดียวกัน)

ในทางตรงกันข้ามถ้าข้อเท็จจริงปรากฏว่าผู้ต้องหาหรือจำเลยนั้นมีเจตนาจะกระทำความผิดเรื่องนั้นอยู่ก่อนแล้ว หรือได้มีพฤติการณ์ที่กระทำความผิดเรื่องนั้นอยู่ก่อนแล้ว แต่เจ้าหน้าที่รวมทั้งผู้เสียหายมีความจำเป็นต้องใช้วิธีการล่อซื้อเพื่อแสวงหาพยานหลักฐานในการจับกุมผู้ต้องหามาดำเนินคดี (Undercover Operation) การล่อซื้อในคดีนี้ถือว่าเป็นการกระทำที่ชอบด้วยกฎหมาย พยานหลักฐานที่ได้มาจากการล่อซื้อจึงเป็นพยานหลักฐานที่รับฟังได้ ไม่ต้องห้ามตามมาตรา 226 หรือมาตรา 226/1 (คณิต วัลยะเพ็ชร์, ออนไลน์, 2562) ตัวอย่างเช่น **คำพิพากษาศาลฎีกาที่ 6523/2545** (ออนไลน์, 2562) ซึ่งวินิจฉัยว่า บริษัทจำเลยที่ 1 มีโปรแกรมคอมพิวเตอร์ที่ทำซ้ำโดยละเมิดลิขสิทธิ์ของโจทก์และพร้อมที่จะคัดลอกหรือทำซ้ำติดตั้งลงในฮาร์ดดิสก์ของเครื่องคอมพิวเตอร์และส่งมอบให้ในวันที่ ฟ.ไปสุ่มซื้อได้ทันทีแม้การกระทำของฟ. จะเป็นการแสวงหา

พยานหลักฐานเพื่อดำเนินคดีแก่ผู้ที่ละเมิดลิขสิทธิ์ของโจทก์ แต่ก็ไม่เป็นการชักจูงใจหรือก่อให้ฝ่ายจำเลยกระทำความผิดคดีนี้ขึ้นมา เพราะจำเลยมีเจตนากระทำการอันละเมิดลิขสิทธิ์ของโจทก์อยู่ก่อนแล้ว ในทำนองเดียวกับ **คำพิพากษาศาลฎีกาที่ 81/2551**(ออนไลน์, 2562) ซึ่งวินิจฉัยว่า การใช้สายลับล่อซื้อเมทแอมเฟตามีนเป็นเพียงการกระทำเท่าที่จำเป็นและสมควรในการแสวงหาพยานหลักฐานในการกระทำความผิดของจำเลยตามอำนาจในประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 2 (10) ชอบที่เจ้าพนักงานตำรวจจะกระทำได้เพื่อให้ได้โอกาสจับกุมจำเลยพร้อมด้วยพยานหลักฐาน อันเป็นเพียงวิธีการพิสูจน์ความผิดของจำเลย ไม่เป็นการแสวงหาพยานหลักฐานโดยมิชอบ และ**คำพิพากษาศาลฎีกาที่ 10632/2554**(ออนไลน์, 2562) ที่วินิจฉัยว่า การใช้เจ้าพนักงานตำรวจไปล่อซื้อบริการค้าประเวณีเป็นเพียงการกระทำเท่าที่จำเป็นและสมควรในการแสวงหาหลักฐานในการกระทำความผิดของจำเลยตามอำนาจในประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 2 (10) ชอบที่เจ้าพนักงานตำรวจจะกระทำได้เพื่อให้ได้โอกาสจับกุมจำเลยพร้อมด้วยพยานหลักฐาน ดังนั้นการใช้เจ้าพนักงานตำรวจไปล่อซื้อบริการค้าประเวณีจากจำเลยจึงเป็นเพียงวิธีพิสูจน์ความผิดของจำเลย ไม่เป็นการแสวงหาหลักฐานโดยมิชอบ และแม้เจ้าพนักงานตำรวจจะให้ค่าจ้างแก่สายลับผู้ไปทำการล่อซื้อ ก็ยังคงเป็นการล่อซื้อโดยชอบ มิใช่พยานที่เกิดจากการจูงใจหรือมีคำมั่นสัญญาโดยไม่ชอบ เพราะผู้ที่รับจ้างไปล่อซื้อสิ่งผิดกฎหมายมิได้มีเจตนากระทำความผิดจึงไม่ต้องรับโทษทางอาญา คงถือว่าเป็นเครื่องมือ (Innocent Agent) ในการล่อซื้อที่ชอบด้วยกฎหมายของเจ้าหน้าที่เท่านั้น ดังนั้น เมื่อมาเบิกความเป็นพยานในคดีจึงมิใช่พยานซัดทอด (คำพิพากษาฎีกาที่ 2205/2554 (ป), ออนไลน์, 2562)

2.2 บทตัดพยานบอกเล่า

ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226/3 (ออนไลน์, 2562) บัญญัติว่า

ข้อความซึ่งเป็นการบอกเล่าที่พยานบุคคลใดนำมาเบิกความต่อศาลหรือที่บันทึกไว้ในเอกสารหรือวัตถุอื่นใดซึ่งอ้างเป็นพยานหลักฐานต่อศาล หากนำเสนอเพื่อพิสูจน์ความจริงแห่งข้อความนั้น ให้ถือเป็นพยานบอกเล่า

ห้ามมิให้ศาลรับฟังพยานบอกเล่า เว้นแต่

(1) ตามสภาพ ลักษณะ แหล่งที่มา และข้อเท็จจริงแวดล้อมของพยานบอกเล่านั้นน่าเชื่อว่าจะพิสูจน์ความจริงได้ หรือ

(2) มีเหตุจำเป็น เนื่องจากไม่สามารถนำบุคคลซึ่งเป็นผู้ที่ได้เห็น ได้ยิน หรือทราบข้อความเกี่ยวในเรื่องที่จะให้การเป็นพยานนั้นด้วยตนเองโดยตรงมาเป็นพยานได้ และมีเหตุผลสมควรเพื่อประโยชน์แห่งความยุติธรรมที่จะรับฟังพยานบอกเล่านั้น

ในกรณีที่ศาลเห็นว่าไม่ควรรับไว้ซึ่งพยานบอกเล่าใด และคู่ความฝ่ายที่เกี่ยวข้องร้องคัดค้านก่อนที่ศาลจะดำเนินคดีต่อไป ให้ศาลจดรายงานระบุนาม หรือชนิดและลักษณะของพยานบอกเล่า เหตุผลที่ไม่ยอมรับ และข้อคัดค้านของคู่ความฝ่ายที่เกี่ยวข้องไว้ ส่วนเหตุผลที่คู่ความฝ่ายคัดค้านยกขึ้นอ้างนั้น ให้ศาลใช้ดุลพินิจจดลงไว้ในรายงานหรือกำหนดให้คู่ความฝ่ายนั้นยื่นคำแถลงต่อศาลเพื่อรวมไว้ในสำนวน

คำว่า “**พยานบอกเล่า**” หมายถึงคำกล่าว (Statement) ของประจักษ์พยานที่ได้กระทำไว้นอกศาลและนำมาใช้เป็นพยานหลักฐานในศาล โดยไม่ได้นำตัวประจักษ์พยานผู้กล่าวข้อความนั้นมาเบิกความโดยตรงต่อศาล พยานบอกเล่านั้นไม่จำเป็นต้องเป็นพยานบุคคลเสมอไป แม้พยานเอกสารหรือพยานวัตถุก็สามารถเป็นพยานบอกเล่าได้ ถ้านำสืบเข้ามาเพื่อแสดงให้เห็นถึงข้อความหรือเรื่องราวที่คนที่รู้เรื่องนั้นโดยตรงไม่ได้มาเบิกความต่อศาล

ในกรณีที่พยานไม่ได้ถึงแก่ความตายแต่ไม่ยอมไปเบิกความที่ศาล ทำให้ต้องนำสืบคำให้การพยานชั้นสอบสวนแทน มีปัญหาว่าจะรับฟังได้หรือไม่นั้น **คำพิพากษาฎีกาที่ 2205/2554** (ออนไลน์, 2562) วินิจฉัยไว้ว่า ผู้เสียหายทั้งสองซึ่งเป็นประจักษ์พยานไม่มาเบิกความเป็นพยานโจทก์เพื่อยืนยันการกระทำความผิดของจำเลยคงมีแต่คำให้การในชั้นสอบสวนของผู้เสียหายที่ 1 และที่ 2 โดยผู้เสียหายที่ 1 ไม่ประสงค์จะเอาผิดต่อผู้ที่เกี่ยวข้องในกระบวนการค้ามนุษย์ เนื่องจากกังวลเรื่องความปลอดภัยของตนและครอบครัว โดยไม่ปรากฏว่า จำเลยมีอิทธิพลใดที่ทำให้ฝ่ายผู้เสียหายที่ 1 ต้องเกรงกลัวฝ่ายจำเลยจนถึงกับไม่กล้ามาเบิกความต่อศาลเอาผิดต่อจำเลยที่กระทำต่อตน การที่ผู้เสียหายทั้งสองไม่มาเบิกความต่อศาลทั้งที่ยังมีตัวตนอยู่ การรับฟังคำให้การชั้นสอบสวนของผู้เสียหายทั้งสองย่อมทำให้จำเลยเสียเปรียบ อย่างน้อยก็ไม่มีโอกาสซักค้านผู้เสียหายทั้งสองเพื่อกระจายข้อเท็จจริงให้เห็นว่าข้อเท็จจริงเป็นอย่างไร กรณีไม่ใช่เหตุจำเป็นเนื่องจากไม่สามารถนำบุคคลซึ่งเป็นผู้ได้เห็นได้ยิน หรือทราบข้อความเกี่ยวในเรื่องที่จะให้การเป็นพยานนั้นด้วยตนเองโดยตรงมาเป็นพยานได้ และไม่มีเหตุสมควรเพื่อประโยชน์แห่งความยุติธรรมที่จะรับฟังพยานบอกเล่านั้น จึงไม่เข้าข้อยกเว้นให้รับฟังตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226/3 วรรคสอง (2)

สำหรับกรณีของพยานเอกสาร แม้จะถือว่าเป็นพยานบอกเล่า ก็ไม่ต้องห้ามรับฟังเป็นพยานหลักฐาน เพราะตามประมวลกฎหมายวิธีพิจารณาความแพ่ง มาตรา 95 กำหนดห้ามมิให้รับฟังพยานบอกเล่าที่เป็นพยานบุคคลเท่านั้น จึงไม่รวมถึงพยานเอกสาร (สราวุธปิติยาศักดิ์, 2561 : 319-320)

3. การชั่งน้ำหนักพยานหลักฐาน

ในคดีอาญาโจทก์มีหน้าที่นำสืบให้เห็นโดยปราศจากเหตุอันควรสงสัย (Beyond Reasonable Doubt) เมื่อมีข้อสงสัยตามสมควรว่าจำเลยได้กระทำผิดหรือไม่ ศาลต้องยกประโยชน์แห่งความสงสัยนั้นให้จำเลย การชั่งน้ำหนักพยานหลักฐานของศาลนั้นเกิดขึ้นเมื่อพยานหลักฐานของ

โจทก์ที่ได้ในสืบในชั้นศาลมีน้ำหนักมั่นคงได้มาตรฐานการพิสูจน์แล้ว จากนั้นศาลต้องวิเคราะห์พยานหลักฐานของฝ่ายจำเลยอีกชั้นหนึ่งว่ามีน้ำหนักหักล้างพยานหลักฐานของฝ่ายโจทก์หรือไม่ ถ้าพยานหลักฐานของจำเลยไม่มีน้ำหนักหักล้างพยานโจทก์ได้ ศาลก็จะฟังข้อเท็จจริงว่าจำเลยกระทำผิดตามที่โจทก์ฟ้อง แต่หากพยานหลักฐานของจำเลยมีน้ำหนักดีจนก่อให้เกิดความสงสัยตามสมควร ศาลก็จะวินิจฉัยว่าพยานหลักฐานของจำเลยมีน้ำหนักหักล้างพยานหลักฐานของโจทก์ ยกประโยชน์แห่งความสงสัยให้แก่จำเลย และพิพากษายกฟ้อง

น้ำหนักของพยานหลักฐานในคดีอาญามีแตกต่างกันไป (จรัญภักดีธนากุล, 2561 :620-631) โดยพยานหลักฐานบางประเภทมีคุณค่าในเชิงพิสูจน์น้อย อาทิเช่น พยานบอกเล่า พยานซัดทอด พยานที่มีส่วนได้เสียกับคู่ความฝ่ายใดฝ่ายหนึ่ง พยานหลักฐานที่ได้มาโดยวิธีการที่ไม่ชอบ หรือพยานหลักฐานที่คู่ความฝ่ายใดฝ่ายหนึ่งยังไม่มีโอกาสที่จะตรวจสอบหรือหักล้างตามสมควร จะเป็นพยานหลักฐานเหล่านี้ถ้ามิได้ถูกตัดออกไปตามบทกฎหมายที่กล่าวมาข้างต้นก็จะเป็นพยานหลักฐานที่รับฟังได้ ศาลก็จะต้องนำมาพิจารณาชั่งน้ำหนักเพื่อใช้วินิจฉัยปัญหาข้อเท็จจริงในคดีนั้นด้วยความรอบคอบ เพราะโดยลักษณะของพยานชนิดดังกล่าวมีโอกาสที่จะผิดพลาดคลาดเคลื่อนจากความจริงได้มาก ด้วยเหตุนี้ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 227/1 (ออนไลน์, 2562) ที่บัญญัติเพิ่มขึ้นใหม่ในปี พ.ศ.2551 จึงได้นำหลักปฏิบัติในการชั่งน้ำหนักพยานหลักฐานประเภทนี้มาบัญญัติไว้ในทำนองเดียวกับแนวบรรทัดฐานศาลฎีกาที่มีมาแต่เดิมว่า

ในการวินิจฉัยชั่งน้ำหนักพยานบอกเล่า พยานซัดทอด พยานที่จำเลยไม่มีโอกาสถามค้าน หรือพยานหลักฐานที่มีข้อบกพร่องประการอื่นอันอาจกระทบถึงความน่าเชื่อถือของพยานหลักฐานนั้น ศาลจะต้องกระทำด้วยความระมัดระวัง และไม่ควรเชื่อพยานหลักฐานนั้นโดยลำพังเพื่อลงโทษจำเลย เว้นแต่จะมีเหตุผลอันหนักแน่น มีพฤติการณ์พิเศษแห่งคดี หรือมีพยานหลักฐานประกอบอื่นมาสนับสนุน

พยานหลักฐานประกอบตามวรรคหนึ่ง หมายถึง พยานหลักฐานอื่นที่รับฟังได้ และมีแหล่งที่มาเป็นอิสระต่างหากจากพยานหลักฐานที่ต้องการพยานหลักฐานประกอบนั้น ทั้งจะต้องมีคุณค่าเชิงพิสูจน์ที่สามารถสนับสนุนให้พยานหลักฐานอื่นที่ไปประกอบมีความน่าเชื่อถือมากขึ้นด้วย

วรรณกรรมและผลงานวิจัยที่เกี่ยวข้อง

จากการทบทวนตำรา งานเขียน วิทยานิพนธ์ และงานวิจัย ผ่านการสืบค้นฐานข้อมูลอิเล็กทรอนิกส์ทางวิชาการ ในเบื้องต้นพบวรรณกรรมและงานวิจัยที่เกี่ยวข้องกับการดำเนินคดี

อาชญากรรมคอมพิวเตอร์ (Cybercrime หรือ Computer Crime) พบว่ามีผลงานวิจัยที่สำคัญและแนวความคิดของผู้ทรงคุณวุฒิที่เกี่ยวข้องกับงานวิจัยนี้ ได้แก่

เฉลิมชนม์ แน่นหนา และคณะ (2555) ซึ่งทำการวิจัยในหลักสูตรการป้องกันราชอาณาจักร วปอ. รุ่นที่ 55 เรื่อง “อาชญากรรมบนสื่อออนไลน์ (CyberCrime)” เน้นวิเคราะห์แนวทางการป้องกันและแก้ปัญหาอาชญากรรมออนไลน์ โดยมีพื้นฐานความคิดว่าทุกคนต้องตระหนักถึงความสำคัญและภัยที่มาควบคู่กับสื่อออนไลน์ให้มากขึ้น และต้องมีการป้องกันภัยคุกคามออนไลน์อย่างรู้เท่าทัน โดยทำการศึกษาอาชญากรรมบนสื่อออนไลน์ในบริบทของการให้การประสานความร่วมมือกันทั้งภาครัฐและภาคเอกชน เพื่อชี้แนะแนวทางในการป้องกันและแก้ไขปัญหาอาชญากรรมบนสื่อออนไลน์อย่างเป็นระบบ โดยเฉลิมชนม์ แน่นหนา และคณะ (2555 : 90-91) ได้เสนอแนะแนวทางในการป้องกันและปราบปรามอาชญากรรมบนสื่อออนไลน์อย่างเป็นระบบ ดังนี้

1. การแก้กฎหมายต้องมีความชัดเจนระหว่างการกระทำความผิดอาญาตามประมวลกฎหมายอาญาหรือกฎหมายอื่นที่มีโทษทางอาญาโดยผ่านช่องทางคอมพิวเตอร์หรือสื่อออนไลน์กับการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 รวมทั้งเสนอให้มีการจัดตั้งศาลชำนัญการพิเศษและบัญญัติกฎหมายลักษณะพยาน และวิธีพิจารณาคดีอาชญากรรมคอมพิวเตอร์และอาชญากรรมออนไลน์บัญญัติขึ้นโดยเฉพาะเพื่อให้สอดคล้องกับสภาพปัญหาที่เกิดขึ้น

2. การนำนโยบายไปสู่การปฏิบัติไม่ควรมองปัญหาแบบแยกส่วนในลักษณะต่างคนต่างทำการดำเนินงานต้องมีเอกภาพในการดำเนินการ และให้มีหน่วยงานหลักในการรวมหรือบูรณาการแผนรวม เพื่อเดินไปสู่เป้าหมายและทิศทางเดียวกัน ซึ่งคดีที่เกี่ยวกับความผิดทางคอมพิวเตอร์บนสื่อออนไลน์ ส่วนใหญ่เป็นคดีที่ต้องอาศัยความรู้ความชำนาญและมีลักษณะคดีที่เกิดขึ้นในหลายท้องที่ทั้งในและนอกราชอาณาจักร อีกทั้ง ในแต่ละหน่วยงานที่ทำหน้าที่ป้องกันและปราบปรามก็ยังขาดแคลนบุคลากรที่มีความรู้ความเชี่ยวชาญอยู่เป็นจำนวนมาก จึงเห็นควรให้มีการยุบรวมหน่วยงานในการป้องกันและปราบปรามอาชญากรรมบนสื่อออนไลน์ โดยให้มีกฎหมายพิเศษระบุอำนาจหน้าที่เจ้าหน้าที่ผู้ปฏิบัติให้มีความคล่องตัวและสะดวกรวดเร็วทันต่ออาชญากรรมต่างๆที่ก่อตัวอย่างรวดเร็วผ่านสื่อออนไลน์ ในอีกด้านหนึ่งก็ต้องจัดให้มีระบบตรวจสอบและถ่วงดุลอำนาจที่มีความน่าเชื่อถือมิให้เป็นข้อกังขาได้ว่าเจ้าหน้าที่ปฏิบัติหน้าที่โดยมิชอบด้วย

3. จัดสรรอำนาจหน้าที่ งบประมาณ และวางกรอบแนวทางการประสานงานระหว่างหน่วยงานที่ทำหน้าที่ป้องกันและปราบปรามอาชญากรรมบนสื่อออนไลน์โดยตรง กับหน่วยงานที่มีหน้าที่ให้การสนับสนุนให้ชัดเจน โดยเฉพาะการจัดวางแผนอัตรากำลังเจ้าหน้าที่มีความรู้ความชำนาญให้เพียงพอต่อความต้องการ ซึ่งในเบื้องต้นอาจใช้การประสานความร่วมมือระหว่างหน่วยงานภาครัฐ

และภาคเอกชน เช่น การแต่งตั้งเจ้าหน้าที่หรือพนักงานของหน่วยงานภาครัฐหรือเอกชนที่มีความรู้ความเชี่ยวชาญในลักษณะงานที่มีประโยชน์ต่อการสืบสวนสอบสวนคดีเป็นผู้ช่วยพนักงานสอบสวน

4. จัดทำคู่มือปฏิบัติงานและหลักนิยมสำหรับผู้ทำหน้าที่ปราบปรามอาชญากรรมบนสื่อออนไลน์ รวมทั้งศึกษารวบรวมสถิติคดีความที่เกิดขึ้นเพื่อนำมาปรับปรุงพัฒนาคู่มือปฏิบัติให้ทันต่อความเปลี่ยนแปลงและความซับซ้อนของการก่ออาชญากรรมบนสื่อสื่อออนไลน์

เฉลิมชนม์ แน่นหนา และคณะ (2555 : 88)ได้ตั้งข้อสังเกตว่า ปัจจุบัน แม้ว่าหน่วยงานภาครัฐได้มีการบูรณาการความร่วมมือกับหน่วยงานต่างๆทั้งในและต่างประเทศเพื่อสืบสวนสอบสวนพิสูจน์หลักฐานและปราบปรามผู้กระทำความผิดอาชญากรรมคอมพิวเตอร์ก็ตาม แต่การใช้กลยุทธ์ต่างๆ ในการจัดการกับอาชญากรรมคอมพิวเตอร์ยังคงเป็นไปโดยขาดเอกภาพ อีกทั้งหน่วยงานภาครัฐมีข้อจำกัดด้านอัตรากำลังคน บุคลากรที่มีความรู้ความชำนาญด้านคอมพิวเตอร์ และงบประมาณประกอบกับยังมีข้อจำกัดทางกฎหมาย หลักเกณฑ์และวิธีการปฏิบัติทางราชการต่างๆ ที่ไม่เอื้ออำนวยต่อการปรับเปลี่ยนกลยุทธ์หรือยุทธวิธีต่างๆให้ทันต่ออาชญากรรมคอมพิวเตอร์

ศุทธดา วัฒนวิเชียร (2554) ได้ทำการศึกษาหลักการรับฟังพยานหลักฐานที่อยู่ในรูปของข้อมูลสื่ออิเล็กทรอนิกส์ทั้งในคดีแพ่งและคดีอาญา เนื่องจากตามประมวลกฎหมายวิธีพิจารณาความแพ่ง และประมวลกฎหมายวิธีพิจารณาความอาญายังมิได้มีการกำหนดวิธีการหรือขั้นตอนการรับรองความถูกต้องของกระบวนการได้มาซึ่งข้อมูลอิเล็กทรอนิกส์ กระบวนการวิเคราะห์ความน่าเชื่อถือของข้อมูลอิเล็กทรอนิกส์ รวมทั้งสถานะของข้อมูลอิเล็กทรอนิกส์มาชัดเจน อันมีผลต่อการรับฟังและชั่งน้ำหนักพยานหลักฐานในชั้นศาล โดยศุทธดา วัฒนวิเชียร (2554 : 26-27) ได้เสนอแนะแนวทางในการแก้ไขปัญหาดังกล่าวไว้ดังนี้

1. ควรกำหนดให้ชัดเจนว่าข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานประเภทใดหรือเป็นพยานหลักฐานอีกประเภทหนึ่งแยกต่างหาก เพราะการจัดประเภทพยานหลักฐานย่อมส่งผลโดยตรงต่อวิธีการนำสืบและการรับฟังพยานหลักฐาน แต่ข้อมูลอิเล็กทรอนิกส์มีลักษณะพิเศษแตกต่างจากพยานเอกสารและพยานวัตถุทั่วไป ดังนั้น ในการอ้าง การนำเสนอ และการนำสืบจึงต้องมีวิธีการพิเศษโดยเฉพาะ ซึ่งอาจจัดทำในรูปแบบของข้อกำหนดของประธานศาลฎีกาสำหรับพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ในทำนองเดียวกับข้อกำหนดคดีทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ พ.ศ.2540

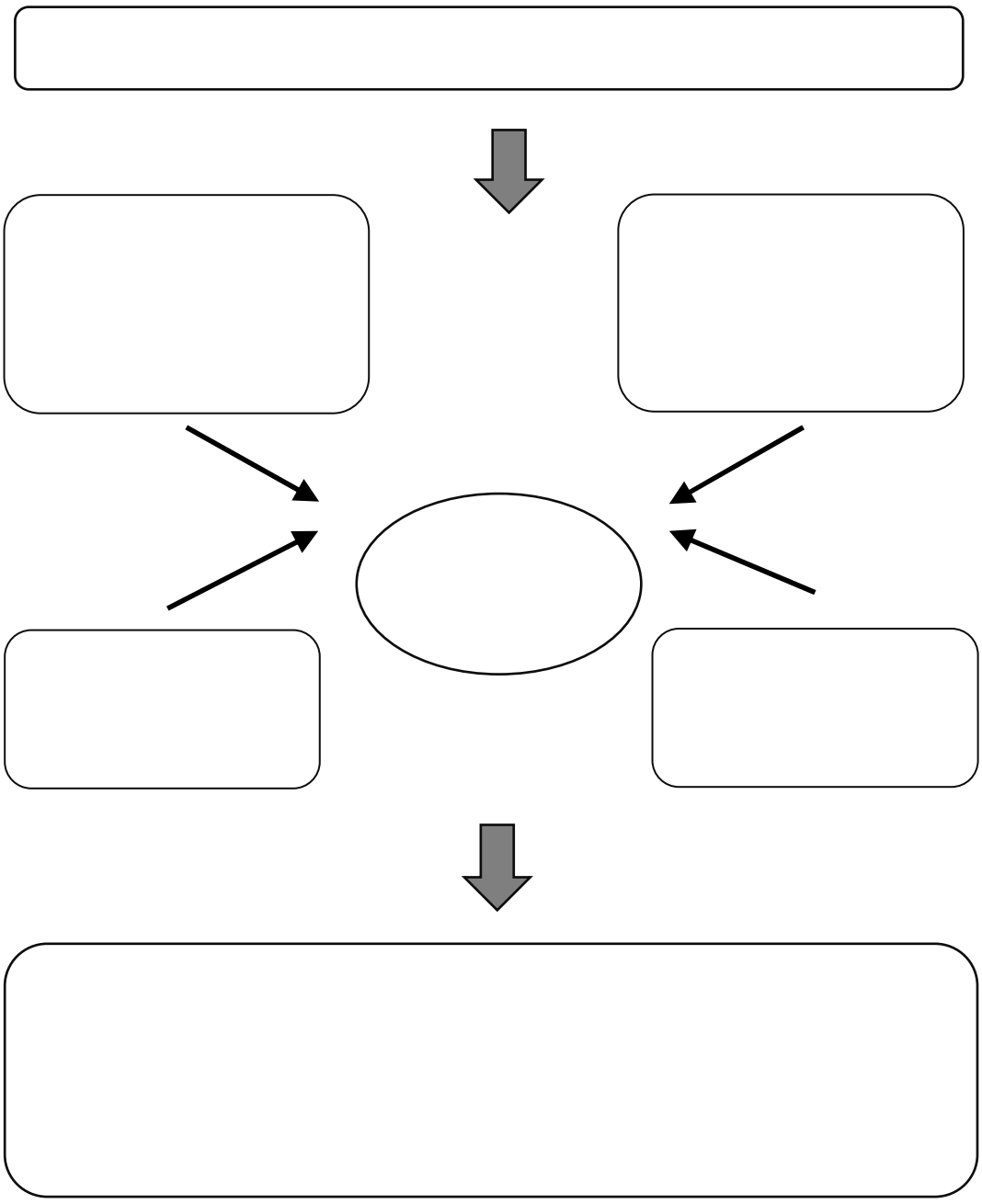
2. ไม่ควรนำบทตัดพยาน คือ หลักการรับฟังพยานบอกเล่ามาใช้กับการรับฟังพยานหลักฐานในรูปข้อมูลอิเล็กทรอนิกส์เนื่องจากลักษณะพิเศษของข้อมูลอิเล็กทรอนิกส์ที่มีการทำสำเนาได้โดยง่ายและสำเนาก็จะมีความถูกต้องตรงกับต้นฉบับจนแยกไม่ออก แต่ควรให้ความสำคัญกับวิธีการรับรองความถูกต้องของข้อมูลอิเล็กทรอนิกส์ และบางกรณีข้อมูลอิเล็กทรอนิกส์จะเป็นพยานบอกเล่าแต่ก็มีความน่าเชื่อถือหากสามารถทำให้เห็นถึงความถูกต้องแท้จริง การสื่อสาร รับ ส่ง

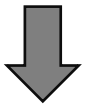
บันทึกต่อๆมาทำได้โดยง่ายและถูกต้องตรงกันต่างจากพยานบอกเล่าอย่างอื่น แต่ควรให้ศาลเป็นผู้ใช้ดุลพินิจชั่งน้ำหนักพยานหลักฐานแทน

3. ควรมีวิธีการรับรองความถูกต้องของข้อมูลอิเล็กทรอนิกส์ที่หลากหลาย เช่น การรับรองความถูกต้องโดยคู่ความฝ่ายที่อ้าง การตกลงรับกันของคู่ความที่เกี่ยวข้อง การรับรองความถูกต้องโดยใช้คำให้การพยานและการถามค้านของคู่ความ หรือการรับรองความถูกต้องโดยการตรวจสอบของศาล เป็นต้น

4. ควรยกเลิกหลักเกณฑ์การห้ามสืบพยานบุคคลเปลี่ยนแปลงแก้ไขพยานเอกสาร โดยหากมีข้อผิดพลาดที่สื่ออิเล็กทรอนิกส์บันทึกไม่ตรง คู่ความย่อมมีสิทธินำพยานบุคคลเปลี่ยนแปลงแก้ไขได้

กรอบแนวคิดของการวิจัย





สรุป

ท่ามกลางจำนวนผู้เข้าถึงโลกไซเบอร์ที่มีเพิ่มมากขึ้นทุกปี พฤติกรรมในการใช้งานระบบคอมพิวเตอร์ซึ่งมีทั้งการพาณิชย์อิเล็กทรอนิกส์ การจัดการธุรกรรมทางการเงิน และการเผยแพร่ข้อมูลในสื่อสังคมออนไลน์ ตกเป็นเป้าหมายในการก่ออาชญากรรมโดยมิจฉาชีพบนโลกไซเบอร์เพื่อแสวงหาประโยชน์อันมิชอบในหลายลักษณะ การดำเนินคดีอาชญากรรมคอมพิวเตอร์มีความเกี่ยวพันกับพยานหลักฐานดิจิทัล ซึ่งมีลักษณะที่แตกต่างจากพยานหลักฐานทั่วไป จึงเป็นความท้าทายอย่างยิ่งของเจ้าพนักงานในกระบวนการยุติธรรมในการจัดการกับพยานหลักฐานดิจิทัลเหล่านั้น เพื่อให้เป็นพยานหลักฐานที่รับฟังได้ตามกฎหมาย และมีน้ำหนักพิสูจน์ความผิดของผู้ถูกกล่าวหาในคดีอาชญากรรมคอมพิวเตอร์ให้ได้มาตรฐาน “ปราศจากข้อสงสัยตามสมควร” เพื่อที่ศาลจะลงโทษจำเลยได้

ข้อมูลที่ได้จากการทบทวนวรรณกรรมในบทนี้เป็นข้อมูลพื้นฐานสำคัญเกี่ยวกับแนวคิดทฤษฎีเกี่ยวกับอาชญาวิทยาและการรับฟังพยานหลักฐานของไทย ลักษณะและรูปแบบของอาชญากรรมคอมพิวเตอร์ที่พบมากในปัจจุบัน บทบาทหน้าที่ของเจ้าพนักงานที่เกี่ยวข้องกับการดำเนินคดีอาญา รวมถึงหลักกฎหมายที่สำคัญเกี่ยวกับการดำเนินคดีอาชญากรรมคอมพิวเตอร์เพื่อสร้างความเข้าใจพื้นฐานประกอบกับผลที่ได้จากการสัมภาษณ์เชิงลึกเจ้าพนักงานตำรวจในงานสืบสวนและงานสอบสวน ผู้ตรวจพิสูจน์หลักฐาน และพนักงานอัยการผู้ทรงคุณวุฒิ เพื่อการสะท้อนสภาพการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในปัจจุบันของเจ้าพนักงานแต่ละฝ่ายในกระบวนการยุติธรรมทางอาญาและสภาพปัญหาที่พบในการดำเนินคดีอาญากรรมคอมพิวเตอร์ ต่อไปในบทที่ 3 และเพื่อการวิเคราะห์ปัจจัยด้านต่างๆที่ส่งผลกระทบกับประสิทธิภาพในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในปัจจุบัน ในบทที่ 4

อันจะเป็นเหตุผลสนับสนุนในการเสนอแนะแนวทางเพิ่มประสิทธิภาพในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในบทที่ 5 ต่อไป

บทที่3
การดำเนินคดีอาชญากรรมคอมพิวเตอร์

คดีอาชญากรรมคอมพิวเตอร์จัดเป็นคดีอาญาประเภทหนึ่งซึ่งบุคคลผู้ถูกกล่าวว่ากระทำความผิดตามกฎหมายย่อมได้รับความคุ้มครองตามหลักสิทธิมนุษยชนขั้นพื้นฐานในอันจะถูกสันนิษฐานไว้ก่อนว่าเป็นผู้บริสุทธิ์ตามหลัก Presumption of Innocence จนกว่าผู้กล่าวหาจะพิสูจน์ให้ได้ตามมาตรฐานการพิสูจน์ในคดีอาญาในระดับปราศจากข้อสงสัยอันสมควร (Beyond Reasonable doubt) ดังนั้น ข้อขัดข้องในการปฏิบัติงานของเจ้าพนักงานในกระบวนการยุติธรรมที่ต้องเผชิญอาจส่งผลกระทบต่อความสมบูรณ์เพียงพอของพยานหลักฐานในคดีจึงเป็นตัวแปรสำคัญที่อาจทำให้การดำเนินคดีอาชญากรรมคอมพิวเตอร์ไม่มีประสิทธิภาพเท่าที่ควร และในบางกรณีอาจนำไปสู่ผลการวินิจฉัยของศาลที่ยกฟ้องคดีอีกด้วย

การศึกษาในบทที่ 3 จึงมีความมุ่งหมายเพื่อตอบวัตถุประสงค์การวิจัยข้อที่ 1เพื่อศึกษาสภาพปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ที่พบในชั้นการสืบสวนสอบสวน รวบรวมพยานหลักฐาน จนถึงขั้นตอนการนำเสนอพยานหลักฐานในชั้นพิจารณาของศาล ซึ่งข้อมูลที่ได้ในบทนี้จะเป็นพื้นฐานสำคัญในการศึกษาวิเคราะห์ในบทต่อไปโดยมีลำดับการศึกษาดังนี้

1. การสืบสวนสอบสวนคดีอาชญากรรมคอมพิวเตอร์
2. การตรวจพิสูจน์พยานหลักฐานในคดีอาชญากรรมคอมพิวเตอร์
3. การนำเสนอพยานหลักฐานในคดีอาชญากรรมคอมพิวเตอร์
4. ตัวอย่างการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในปัจจุบัน
5. สรุป

การสืบสวนสอบสวนคดีอาชญากรรมคอมพิวเตอร์

งานสืบสวนและงานสอบสวนถือได้ว่าเป็นการปฏิบัติงานด้านกระบวนการยุติธรรมทางอาญาในคดีอาชญากรรมคอมพิวเตอร์ในขั้นตอนแรกๆ เพื่อรวมรวมพยานหลักฐานเกี่ยวกับการกระทำความผิดว่าเกิดขึ้นได้อย่างไร รวมถึงสืบสวนหาตัวผู้กระทำความผิดด้วยการแสวงหาพยานหลักฐานเพื่อเชื่อมโยงและยืนยันตัวผู้กระทำผิด ตลอดจนอธิบายถึงรูปแบบของการกระทำความผิดที่คนร้ายใช้เพื่อนำไปสู่การแจ้งข้อกล่าวหาและดำเนินคดีต่อไปทั้งนี้ หน่วยงานที่มีอำนาจสืบสวนสอบสวนหลักได้แก่

1. เจ้าพนักงานสืบสวนสอบสวนสังกัดสำนักงานตำรวจแห่งชาติ

ตามโครงสร้างองค์กรของสำนักงานตำรวจแห่งชาติในปัจจุบันนอกจากเจ้าพนักงานสืบสวนสอบสวนที่ประจำอยู่ ณ สถานีตำรวจนครบาลและสถานีตำรวจภูธรทั่วประเทศซึ่งมีอำนาจหน้าที่รับผิดชอบคดีอาญาทั่วไปรวมถึงคดีอาชญากรรมคอมพิวเตอร์แล้ว ในส่วนของกองบัญชาการตำรวจสอบสวนกลางมีหน่วยงานภายใต้สังกัดที่รับผิดชอบคดีบางประเภทเกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ ดังนี้

1.1 กองบังคับการปราบปรามการการค้ามนุษย์ (บก.ปคม.)

1.2 กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ (บก.ปอศ.)

1.3 กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับการคุ้มครองผู้บริโภค (บก.ปคบ.)

1.4 กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี(บก.ปอท.)

นอกจากนี้สำนักงานตำราจแห่งชาติยังได้มีการแต่งตั้งคณะทำงานปราบปรามการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ต ที่รู้จักกันในชื่อของ “TICAC” เป็นหน่วยงานที่มีอำนาจหน้าที่สืบสวนสอบสวน ตรวจค้น จับกุมตามประมวลกฎหมายวิธีพิจารณาความอาญา พระราชบัญญัติป้องกันและปราบปรามการค้ามนุษย์ พ.ศ.2551 (ที่แก้ไขเพิ่มเติม) พระราชบัญญัติคุ้มครองเด็ก พ.ศ.2546 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 (ที่แก้ไขเพิ่มเติม) พระราชบัญญัติคนเข้าเมือง พ.ศ.2522 และมีหน้าที่ในการเป็นจุดประสานงานระหว่างประเทศด้านการละเมิดทางเพศต่อเด็กสำหรับเจ้าหน้าที่ตำรวจประสานงานของต่างประเทศประจำประเทศไทยและหน่วยงานด้านการละเมิดทางเพศต่อเด็กและต่างประเทศทั้งภาครัฐและภาคเอกชน โดยปัจจุบัน TICAC ถือได้ว่าเป็นหน่วยงานที่มีบทบาทสำคัญมากในการสืบสวนสอบสวนการกระทำความผิดการค้ามนุษย์เด็กหรือสื่อลามกอนาจารเด็กออนไลน์

นอกจากนี้สำนักงานตำรวจแห่งชาติยังได้จัดตั้งศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ (ศปอส.ตร.) หรือที่รู้จักในชื่อ “TACTICS” ให้เป็นหน่วยงานที่รวบรวมข้าราชการตำรวจ ที่มีความรู้ความชำนาญมาปฏิบัติงานเพื่อแก้ไขปัญหาอาชญากรรมเทคโนโลยีสารสนเทศและการกระทำความผิดทางอาญา ตามนโยบายสำนักงานตำรวจแห่งชาติ ซึ่งปัจจุบันมีผลงานในการปราบปรามอาชญากรรมคอมพิวเตอร์ที่แพร่ระบาดในสังคมไทย เช่น คดีRomance scam และคดีCall center (“ทลายเครือข่าย Romance Scam” ผู้ต้องหา 17 ราย 8 เครือข่าย ผู้เสียหาย 48 ราย ความเสียหายมากกว่า 5,961,740 บาท”, ออนไลน์, 2562)

2. เจ้าพนักงานสืบสวนสอบสวนสังกัดกรมสอบสวนคดีพิเศษ

พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ.2547 (ที่แก้ไขเพิ่มเติม) กำหนดให้ในการปฏิบัติหน้าที่เกี่ยวกับคดีพิเศษ ให้พนักงานสอบสวนคดีพิเศษมีอำนาจสืบสวนและสอบสวนคดีพิเศษและเป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่หรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา โดยคดีพิเศษจำนวนมากมักปรากฏว่ามีการใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด

เพื่อสะท้อนถึงสภาพปัญหาและอุปสรรคในการปฏิบัติงานคดีอาชญากรรมคอมพิวเตอร์ในชั้นสืบสวนสอบสวน ผู้วิจัยจึงได้ทำการสัมภาษณ์เชิงลึกเจ้าพนักงานตำรวจของสำนักงานตำรวจแห่งชาติและเจ้าพนักงานของกรมสอบสวนคดีพิเศษหลายท่านเกี่ยวกับลักษณะการปฏิบัติงานโดยทั่วไปและตัวอย่างสภาพปัญหาที่พบ แยกตามขั้นตอนการทำงานดังนี้

2.1 ขั้นตอนการสืบสวน

จากการสัมภาษณ์เชิงลึก (ปฏิภาณ ยืนทนต์, สัมภาษณ์, 2562 ; เผ่าภูมิ สมหมาย, สัมภาษณ์, 2562;เรวัติ บุญตันหล้า, สัมภาษณ์, 2562) พบว่า โดยทั่วในการปฏิบัติงานสืบสวนคดีอาชญากรรมคอมพิวเตอร์เพื่อสืบสวนหาตัวผู้กระทำผิดที่ใช้คอมพิวเตอร์ในกระบวนการกระทำผิด หาข้อมูลสนับสนุน เชื่อมโยง หรือยืนยันผู้กระทำผิด ผู้เกี่ยวข้อง และเหยื่อในระบบคอมพิวเตอร์ การสืบสวนแต่ละคดีเจ้าพนักงานสืบสวนจะมีการทำรายงานการสืบสวนและส่งมอบให้กับพนักงานสอบสวนทุกเรื่อง โดยเจ้าพนักงานสืบสวนบางรายมีฐานะเป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 (ที่แก้ไขเพิ่มเติม) ด้วย แต่สำหรับรายที่ไม่ได้เป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (ที่แก้ไขเพิ่มเติม) มักจะไม่เคยมีประสบการณ์ในการประสานงานร้องขอให้พนักงานเจ้าหน้าที่ตามกฎหมายดังกล่าวช่วยเหลือในชั้นของการสืบสวนคดีแต่อย่างใด เช่นเดียวกับที่เจ้าพนักงานสืบสวนบางรายได้มีการประสานงานกับผู้ตรวจพิสูจน์พยานหลักฐานทางดิจิทัลเพื่อให้ข้อมูลเกี่ยวกับพฤติการณ์ทางคดีและขอความร่วมมืออย่างไม่เป็นทางการในการตรวจพิสูจน์พยานหลักฐานทางดิจิทัล ในขณะที่เจ้าพนักงานสืบสวนบางรายปฏิบัติงานสืบสวนโดยมิได้มีการประสานงานกับบุคลากรด้านการพิสูจน์พยานหลักฐานทางดิจิทัลหรือแม้แต่กับพนักงานสอบสวน เนื่องจากมิได้มีหลักเกณฑ์ในการประสานงานที่ชัดเจน จึงขึ้นกับรูปแบบการทำงานของเจ้าพนักงานสืบสวนแต่ละคนและลักษณะของการกระทำความผิดแต่ละคดี

ในเรื่องของแนวทางในการปฏิบัติงานสืบสวนคดีอาชญากรรมคอมพิวเตอร์ ร้อยตำรวจเอกปฏิภาณ ยืนทนต์ จาก ศปอส.ตร.(สัมภาษณ์, 2562) ได้ให้ข้อมูลว่า แนวทางการปฏิบัติงานสืบสวนของเจ้าหน้าที่สืบสวนในพื้นที่ส่วนกลางและส่วนภูมิภาคมีความแตกต่างกัน

เนื่องจากเจ้าพนักงานในส่วนภูมิภาคยังไม่ค่อยมีความรู้ความเข้าใจในเรื่องอาชญากรรมคอมพิวเตอร์มากนัก และมักได้รับการพัฒนาความรู้เกี่ยวกับการปฏิบัติงานไม่ทั่วถึง

สำหรับสภาพปัญหาที่พบในการดำเนินการสืบสวนคดีอาชญากรรมคอมพิวเตอร์ พันตำรวจโทเผ่าภูมิ สมหมาย รอง ผกก.๔ บก.ปคม(สัมภาษณ์, 2562) และร้อยตำรวจเอกเรวัติ บุญตันหล้า รองสารวัตร กองกำกับการวิเคราะห์ข่าวและเครื่องมือพิเศษ กองบังคับการสืบสวนสอบสวนตำรวจภูธรภาค 5 (สัมภาษณ์, 2562) มีความเห็นสอดคล้องกันว่า ผู้ให้บริการภาคเอกชน เช่น ผู้ให้บริการสัญญาณโทรศัพท์ ผู้ให้บริการอินเทอร์เน็ต หรือธนาคารพาณิชย์ต่างๆ มักปฏิเสธการให้ข้อมูลหรือให้ข้อมูลตามที่ร้องขอล่าช้าจนทำให้ไม่ทันต่อสถานการณ์บ่อยครั้ง นอกจากนี้ในส่วนของเจ้าหน้าที่สืบสวนซึ่งมิได้มีฐานะเป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 (ที่แก้ไขเพิ่มเติม) จะพบอุปสรรคมาก เนื่องจากไม่มีอำนาจเรียกให้ผู้ให้บริการภาคเอกชนจัดส่งข้อมูลคอมพิวเตอร์หรือข้อมูลจราจรทางคอมพิวเตอร์โดยตรง ทำให้ต้องอาศัยการขอข้อมูลอย่างไม่เป็นทางการผ่านความสัมพันธ์ส่วนบุคคลระหว่างผู้ปฏิบัติงาน ซึ่งปัญหาการไม่ได้รับความร่วมมือเท่าที่ควรจากผู้ให้บริการพบได้กับผู้ให้บริการที่มีสถานประกอบการทั้งในประเทศไทยและในต่างประเทศ

นอกจากนี้ ยังพบข้อขัดข้องในขั้นตอนของการขออนุมัติหมายค้นจากศาล รวมถึงระยะเวลาในการตรวจค้นที่ได้รับการอนุมัติมีไม่เพียงพอในการดำเนินงานหลายคดี เนื่องจากในบางคดีต้องมีการจัดเก็บพยานหลักฐานดิจิทัลที่ค้นพบในสถานที่ตามหมายค้นซึ่งต้องใช้อุปกรณ์พิเศษและหากข้อมูลคอมพิวเตอร์มีจำนวนมากวิธีการจัดเก็บพยานหลักฐานที่ได้มาตรฐานเป็นที่ยอมรับย่อมมักใช้ระยะเวลาที่ค่อนข้างมาก โดยในการขออนุมัติหมายค้นดุลพินิจของศาลแต่ละแห่งซึ่งมีความแตกต่างกันอยู่บ้างขึ้นอยู่กับความเข้าใจในอาชญากรรมคอมพิวเตอร์ของผู้พิพากษาแต่ละท่าน (เผ่าภูมิ สมหมาย, สัมภาษณ์, 2562)

อุปสรรคต่อประสิทธิภาพในการดำเนินงานสืบสวนอาชญากรรมคอมพิวเตอร์ที่สำคัญอีกประการหนึ่ง ได้แก่ การขาดแคลนบุคลากรที่มีความรู้ความสามารถเฉพาะทางด้านดิจิทัล โดยบุคลากรในงานสืบสวนซึ่งเป็นคนรุ่นเก่าที่ยังขาดการพัฒนาเพิ่มพูนความรู้ให้ทันต่อการเปลี่ยนแปลงไปของเทคโนโลยีสมัยใหม่

2.2 ขั้นตอนการสอบสวน

จากการสัมภาษณ์เชิงลึก พันตำรวจโทดรัณ จาดเจริญเจ้าหน้าที่คดีพิเศษ กองคดีเทคโนโลยีและสารสนเทศ กรมสอบสวนคดีพิเศษ ซึ่งเคยปฏิบัติงานกองบังคับการสนับสนุนทางเทคโนโลยี (สัมภาษณ์, 2562) ได้ชี้ให้เห็นถึงประสบการณ์จากการที่ทำหน้าที่เป็นวิทยากรในหลักสูตรการสืบสวนสอบสวนอาชญากรรมทางคอมพิวเตอร์ ให้แก่พนักงานสอบสวนของสำนักงานตำรวจแห่งชาติและเจ้าพนักงานของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมมาอย่างต่อเนื่องหลายปี พบว่า

พนักงานสอบสวนในพื้นที่ส่วนกลางและส่วนภูมิภาค มีแนวทางในการสืบสวนสอบสวนที่แตกต่างกัน อันเนื่องจากหลายสาเหตุ เช่น ความรู้ความเข้าใจเกี่ยวกับการสืบสวนสอบสวนรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์การได้รับการสนับสนุนจากผู้เชี่ยวชาญด้านต่างๆ ความสามารถและความพร้อมด้านเครื่องมือเครื่องใช้ในการจัดเก็บพยานหลักฐานทางอิเล็กทรอนิกส์อย่างเหมาะสมถูกต้องตามหลักวิชาการเพื่อให้เกิดความน่าเชื่อถือในกระบวนการพิจารณาคดี ซึ่งส่วนใหญ่แล้วพนักงานสอบสวนในส่วนกลางจะมีความเข้าใจในการดำเนินคดีอาชญากรรมคอมพิวเตอร์มากกว่าพนักงานสอบสวนที่อยู่ในส่วนภูมิภาค

ในการประสานงานเพื่อการสอบสวน (ดรัณ จาดเจริญ, สัมภาษณ์, 2562 ;ปัญจะ ผลโต, สัมภาษณ์, 2562) พนักงานสอบสวนมีความจำเป็นต้องประสานขอความร่วมมือจากบุคลากรหลากหลายกลุ่มทั้งภาครัฐและภาคเอกชน อาทิเช่น ผู้ให้บริการในการเชื่อมต่ออินเทอร์เน็ต ผู้ให้บริการในการจัดเก็บข้อมูลบนระบบอินเทอร์เน็ต กลุ่มประกอบธุรกิจบนอินเทอร์เน็ต ผู้ให้บริการเกี่ยวกับธุรกรรมทางการเงิน เช่นธนาคารพาณิชย์และกลุ่มธุรกิจให้บริการเงินอิเล็กทรอนิกส์เจ้าหน้าที่ทางเทคนิคในเทคโนโลยีเฉพาะด้าน เช่น เทคโนโลยีเกี่ยวกับ Voice Over Internet Protocol (VOIP)หรือเทคโนโลยีที่เกี่ยวกับ Video Streaming เพื่อขอข้อมูลการใช้บริการอินเทอร์เน็ต ข้อมูลการจดทะเบียนการใช้งานของบุคคลที่อาจเกี่ยวข้องกับการกระทำความผิดข้อมูลเกี่ยวกับการทำงานของระบบคอมพิวเตอร์ที่เกี่ยวข้องกับการทำความผิดรวมถึงข้อมูลการทำธุรกรรมที่เกี่ยวข้อง เช่น ขั้นตอนการสมัครใช้งานบริการและรูปแบบการยืนยันตัวบุคคล นอกจากนี้ในบางครั้งพนักงานสอบสวนมีความจำเป็นต้องขอความรู้เกี่ยวกับเทคโนโลยีที่มีลักษณะเฉพาะจากผู้ให้บริการเพื่อใช้ในการวิเคราะห์รูปแบบการกระทำความผิด และหาแนวทางในการรวบรวมพยานหลักฐาน

สภาพปัญหาปัจจุบันที่พบในชั้นการรวบรวมพยานหลักฐานและการจัดเก็บพยานหลักฐานมาจากการเปลี่ยนแปลงของเทคโนโลยีที่ส่งผลต่อการจัดเก็บหลักฐาน เช่น กรณีคนร้ายใช้เทคโนโลยีเกี่ยวกับการเข้ารหัสป้องกันข้อมูล (Data Encryption) เพื่อป้องกันการเข้าถึงข้อมูล หรือเทคโนโลยีที่ทำให้พยานหลักฐานสามารถเก็บอยู่ที่ใดก็ได้ เช่น ในระบบคลาวด์ (Cloud) โดยการเปลี่ยนแปลงทางเทคโนโลยีดังกล่าวข้างต้นอาจนำไปสู่ข้อโต้แย้งทางกฎหมายเกี่ยวกับอำนาจในการรวบรวมหลักฐานของเจ้าพนักงานสืบสวน ผู้ตรวจพิสูจน์หลักฐาน และพนักงานสอบสวน เช่น ปัญหาการเข้าถึงระบบจัดเก็บข้อมูลที่อยู่นอกเหนือจากอุปกรณ์ที่ตรวจยึดได้ เช่น ข้อมูลในระบบ Cloud หรือ Social Media ของผู้ต้องหา ว่าพนักงานเจ้าหน้าที่จะมีอำนาจไปรวบรวมมาหรือไม่ (ดรัณ จาดเจริญ, สัมภาษณ์, 2562)

การรวบรวมพยานหลักฐานทางดิจิทัลจากผู้ครอบครองข้อมูลคอมพิวเตอร์ที่อยู่ในต่างประเทศ ในทางปฏิบัติพบข้อจำกัดเกี่ยวกับการใช้อำนาจของพนักงานสอบสวนเพื่อให้ได้ข้อมูลพยานหลักฐานเกี่ยวกับการใช้งานอินเทอร์เน็ตหรือข้อมูลเกี่ยวกับการลงทะเบียนการใช้งาน

ซึ่งหากพนักงานสอบสวนจะดำเนินการผ่านทางช่องทางอย่างเป็นทางการตามพระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ.2535 (ที่แก้ไขเพิ่มเติม) หรือ MLAT ผ่านต้นสังกัด คือ สำนักงานตำรวจแห่งชาติร้องขอไปยังอัยการสูงสุดในฐานะผู้ประสานงานกลางตามพระราชบัญญัติดังกล่าวเพื่อดำเนินการร้องขอไปยังผู้ประสานงานกลางของประเทศปลายทางในกรณีที่มีสนธิสัญญาให้ความช่วยเหลือระหว่างกัน แต่หากไม่มีสนธิสัญญาให้ความช่วยเหลือระหว่างกันขั้นตอนก็จะต้องกระทำผ่านพิธีการปฏิบัติทางการทูต โดยร้องขอผ่านกระทรวงการต่างประเทศ อาศัยหลักประติบัติต่างตอบแทนระหว่างประเทศซึ่งมักพบว่าต้องใช้ระยะเวลาดำเนินการนานหลายเดือนหรือหลายปี ทำให้ไม่ทันกำหนดระยะเวลาตามกฎหมายในการควบคุมผู้ต้องหาระหว่างสอบสวน ซึ่งหากปล่อยผู้ต้องหาไปอาจยากต่อการติดตามตัวมาดำเนินคดีก่อให้เกิดความเสียหายได้ นอกจากนี้ในท้ายที่สุดมีหลายกรณีที่หน่วยงานผู้บังคับใช้กฎหมายในต่างประเทศตอบปฏิเสธในการให้ความร่วมมือตามที่ไทยร้องขอโดยอ้างข้อจำกัดตามกฎหมายภายในของประเทศดังกล่าว ทำให้การรวบรวมพยานหลักฐานผ่านช่องทางความร่วมมือที่เป็นทางการนี้ไม่ค่อยเป็นที่นิยมมากนักในคดีอาญาทั่วไป(เบญจพร วัชระวุฒิชัย, สัมภาษณ์ 2562)

นอกจากนี้ พบมีปัญหาในประเด็นอำนาจสอบสวนความผิดซึ่งมีโทษตามกฎหมายไทยได้กระทำลงนอกราชอาณาจักรไทย ซึ่งประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 20 บัญญัติให้อัยการสูงสุดหรือผู้รักษาการแทนเป็นพนักงานสอบสวนผู้รับผิดชอบหรือจะมอบหมายหน้าที่นั้น ให้พนักงานอัยการหรือพนักงานสอบสวนคนใดเป็นผู้รับผิดชอบทำการสอบสวนแทน ซึ่งในขั้นตอนการสอบสวน พนักงานสอบสวนท้องที่ที่รับคำร้องทุกข์และเริ่มต้นดำเนินการสอบสวนมักพบปัญหาในข้อกฎหมายว่าการกระทำความผิดมีลักษณะที่เป็นความผิดซึ่งมีโทษตามกฎหมายไทยได้กระทำลงนอกราชอาณาจักรไทยหรือไม่ เนื่องจากการกระทำความผิดเกี่ยวกับระบบคอมพิวเตอร์สามารถลงมือกระทำการนำเข้าข้อมูลจากประเทศหนึ่ง แล้วไปเกิดผลหรือเกิดการกระทำความผิดในขั้นตอนต่อเนื่องในอีกประเทศหนึ่งได้ ดังนั้นพนักงานสอบสวนมักเผชิญกับปัญหาในการอธิบายถึงขั้นตอนและรูปแบบที่คนร้ายใช้ในการกระทำความผิดเพื่อวิเคราะห์ว่ามีการกระทำส่วนหนึ่งส่วนใดเกิดขึ้นนอกราชอาณาจักรไทย ซึ่งต้องส่งสำนวนคดีดังกล่าวไปยังอัยการสูงสุดเพื่อมอบหมายพนักงานสอบสวนผู้รับผิดชอบ (ดรัณ จาดเจริญ, สัมภาษณ์, 2562) เนื่องจากการสอบสวนที่มิได้กระทำลงโดยพนักงานสอบสวนที่มีอำนาจหน้าที่ตามกฎหมายย่อมเป็นการสอบสวนที่มิชอบ และพนักงานอัยการไม่มีอำนาจฟ้อง หากดำเนินคดีไปศาลต้องยกฟ้องทำให้เกิดความเสียหายต่อคดีได้

การตรวจพิสูจน์พยานหลักฐานในคดีอาชญากรรมคอมพิวเตอร์

งานตรวจพิสูจน์หลักฐานถือเป็นงานสนับสนุนในการดำเนินคดีอาญาที่มีความสำคัญอย่างยิ่งยวดในการพิสูจน์การกระทำความผิดของผู้ถูกกล่าวหา ในการดำเนินคดีอาญา คำให้การของ

พยานบุคคลผู้พบเห็นเกี่ยวข้องกับเหตุแห่งคดีอาจไม่เพียงพอในการพิสูจน์การกระทำความผิดของผู้ถูกกล่าวหา จึงมีความจำเป็นต้องอาศัยพยานเอกสารและพยานวัตถุเพื่อประโยชน์ในการเชื่อมโยงมูลเหตุแห่งคดีและสร้างน้ำหนักยืนยันว่าผู้ต้องหาหรือจำเลยในคดีคือคนร้ายผู้ลงมือกระทำความผิด

กองพิสูจน์หลักฐานกลาง สำนักงานตำรวจแห่งชาติ ถือเป็นหน่วยงานหลักที่มีพันธกิจในการพิสูจน์หลักฐานและการตรวจสถานที่เกิดเหตุ โดยงานตรวจพิสูจน์หลักฐานของกองพิสูจน์หลักฐานกลางประกอบไปด้วยกลุ่มงานต่างๆ ตามลักษณะเฉพาะที่ต้องอาศัยความรู้ความเชี่ยวชาญเฉพาะทางในการดำเนินงาน ได้แก่ กลุ่มงานตรวจสอบสถานที่เกิดเหตุ กลุ่มงานตรวจเอกสาร กลุ่มงานตรวจอาวุธปืนและเครื่องกระสุน กลุ่มงานตรวจยาเสพติด กลุ่มงานตรวจลายนิ้วมือแฝง กลุ่มงานตรวจชีววิทยาและดีเอ็นเอ กลุ่มงานตรวจทางเคมี ฟิสิกส์ และกลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์(งานตรวจพิสูจน์, ออนไลน์, 2562)

สำหรับงานตรวจพิสูจน์หลักฐานทางนิติคอมพิวเตอร์ (Digital Forensics Examination) มิได้มีเพียงกลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ กองพิสูจน์หลักฐานกลาง สำนักงานตำรวจแห่งชาติที่ปฏิบัติงานตรวจพิสูจน์หลักฐานทางนิติคอมพิวเตอร์เท่านั้น แต่ตามโครงสร้างหน่วยงานภายในสำนักงานตำรวจแห่งชาติยังมีเจ้าพนักงานที่ปฏิบัติงานเกี่ยวข้องกับการช่วยเหลือสนับสนุนในการตรวจพิสูจน์พยานหลักฐานดิจิทัล ได้แก่ กองบังคับการสนับสนุนทางเทคโนโลยี สำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร (บก.สสท.) ซึ่งมีกลุ่มงานตรวจสอบและวิเคราะห์การกระทำผิดทางเทคโนโลยีรวมถึงคณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ ซึ่งให้ความช่วยเหลือในการตรวจพิสูจน์ทางนิติคอมพิวเตอร์ อีกด้วย

ภารกิจของผู้ตรวจพิสูจน์หลักฐานอาจเริ่มต้นขึ้นตั้งแต่ชั้นของการสืบสวนด้วยการร่วมปฏิบัติงานกับเจ้าพนักงานสืบสวนเข้าตรวจสถานที่เกิดเหตุพร้อมจัดเก็บพยานหลักฐานที่เกี่ยวข้องต่อเนื่องไปจนถึงขั้นตอนการรับคำร้องขอจากพนักงานสอบสวนให้ทำการตรวจสอบพยานหลักฐานซึ่งยึดไว้เป็นของกลางในคดีอาญา โดยพยานหลักฐานแต่ละชิ้นอาจต้องการการพิสูจน์หลากหลายแนวทาง เช่น การปฏิบัติต่อของกลางซึ่งเป็นเครื่องคอมพิวเตอร์ นอกจากการตรวจพิสูจน์ทางนิติคอมพิวเตอร์แล้ว ยังอาจพบร่องรอยพยานหลักฐานอื่นอันเป็นประโยชน์ต่อคดีบนอุปกรณ์ของกลาง อันได้แก่ ลายนิ้วมือแฝง หรือสารคัดหลั่ง อย่างเหงื่อหรือคราบเลือด ซึ่งจำต้องได้รับการเก็บมาเป็นพยานหลักฐานและตรวจพิสูจน์ต่อไป

เพื่อสะท้อนให้เห็นถึงสภาพปัญหาและอุปสรรคในการปฏิบัติงานตรวจพิสูจน์ด้านอาชญากรรมคอมพิวเตอร์ ผู้วิจัยจึงได้ทำการสัมภาษณ์เชิงลึกเจ้าพนักงานผู้ตรวจพิสูจน์พยานหลักฐานจากกลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ กองพิสูจน์หลักฐานกลาง ผู้ตรวจพิสูจน์พยานหลักฐานจากกองบังคับการสนับสนุนทางเทคโนโลยี(บก.สสท.)และผู้ตรวจพิสูจน์พยานหลักฐาน

ของกลุ่มงานคณาจารย์ คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจเกี่ยวกับลักษณะการปฏิบัติงานโดยทั่วไป รวมถึงตัวอย่างสภาพปัญหาที่พบ ซึ่งได้รับทราบข้อมูลดังนี้

งานตรวจพิสูจน์และวิเคราะห์พยานหลักฐานดิจิทัลครอบคลุมการตรวจวัตถุพยานในคดีมีทั้งอุปกรณ์คอมพิวเตอร์อุปกรณ์สมาร์ทโฟน และอุปกรณ์อิเล็กทรอนิกส์อย่างอื่น เช่น กล้องวงจรปิด โดยแนวทางการปฏิบัติงานที่ผู้ตรวจพิสูจน์หลักฐานใช้ในการดำเนินงานมาจากคู่มือการตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ ของสำนักงานพิสูจน์หลักฐานตำรวจ และข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐาน version 1.0 จัดทำโดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. นอกจากนี้ พันตำรวจโท อัศว์ณุต แสงทองดี (สัมภาษณ์, 2562) ซึ่งเป็นอาจารย์ประจำ คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ ยังได้นำหลักเกณฑ์ตาม “The Standard Operating Procedures for FBI’s Regional Computer Forensics Laboratory Toward Digital Evidence and Computer Forensic”อันเป็นมาตรฐานของประเทศสหรัฐอเมริกา มาใช้ในงานตรวจพิสูจน์ และในการบรรยายให้ความรู้กับนักเรียนโรงเรียนนายร้อยตำรวจด้วย โดยผู้ตรวจพิสูจน์หลักฐานในแต่ละคดีมีความจำเป็นต้องประสานงานกับหน่วยงานผู้ตรวจพิสูจน์หลักฐานอื่นสำหรับงานตรวจพิสูจน์ที่เกี่ยวข้องเพื่อความครบถ้วนในการจัดทำรายงานผลการตรวจพิสูจน์

จากการสัมภาษณ์เชิงลึกพบข้อมูลว่า การปฏิบัติงานของผู้ตรวจพิสูจน์พยานหลักฐานทางนิติคอมพิวเตอร์จากต่างหน่วยงานมีลักษณะในการปฏิบัติงานที่แตกต่างกันอยู่บ้าง โดยผู้ตรวจพยานหลักฐานจากกองพิสูจน์หลักฐานกลางส่วนใหญ่มีแนวทางการปฏิบัติงานตรวจพิสูจน์และระบุให้ความเห็นเฉพาะประเด็นที่มีการร้องขอให้ดำเนินการเท่านั้น แต่ผู้ตรวจพยานหลักฐานดิจิทัลจากหน่วยงานอื่นจะมีการระบุข้อตรวจพบอย่างอื่นด้วยแม้จะไม่มีการร้องขอให้ดำเนินการโดยตรง เช่น ระบุข้อมูลเพื่อการขยายผลการสืบสวน และผลการวิเคราะห์ข้อมูลโทรศัพท์เคลื่อนที่ในชั้นสืบสวนไว้ในรายงานผลการตรวจพิสูจน์ ในขณะที่ผู้ตรวจพิสูจน์บางท่านให้ความสำคัญและคำนึงถึงประเด็นการนำผลการตรวจพิสูจน์ไปใช้ในชั้นการสรุปสำนวนของพนักงานสอบสวน และชั้นการดำเนินคดีของพนักงานอัยการ รวมถึงให้ความสำคัญและคำนึงถึงข้อโต้แย้งผลการตรวจพิสูจน์ในชั้นการพิจารณาคดี แต่ผู้ตรวจพิสูจน์บางท่านยังไม่ได้ให้ความสำคัญในการคำนึงถึงการนำรายงานผลการตรวจพิสูจน์ไปใช้ในกระบวนการทางคดีต่อไป

โดยทั่วไปแล้วผู้ตรวจพิสูจน์หลักฐานมีมาตรฐานการตรวจพิสูจน์ที่ใกล้เคียงกันไม่ว่าจะเป็นผู้ตรวจพิสูจน์หลักฐานที่อยู่ในส่วนกลางหรือส่วนภูมิภาค เนื่องจากผู้ตรวจพิสูจน์หลักฐานซึ่งจะเป็นผู้ออกรายงานการตรวจพิสูจน์ในนามของตนเองได้จะต้องเข้ารับการฝึกอบรมหลักสูตรพื้นฐานที่กำหนดโดยสำนักงานพิสูจน์หลักฐานตำรวจ และจะต้องผ่านการสอบเพื่อเลื่อนระดับเป็นผู้ชำนาญการก่อน (วันทนีย์ ตุลยเสวี, สัมภาษณ์, 2562) เพียงแต่สำนวนภาษาของข้อตรวจพบและ

ความเห็นที่ระบุในรายงานผลการตรวจพิสูจน์อาจมีความแตกต่างกันอยู่บ้างสำหรับผู้ตรวจพิสูจน์แต่ละคน ทั้งนี้ ชานนท์ คำนวณศักดิ์ (สัมภาษณ์, 2562) และ อัศว์ณุต แสงทองดี (สัมภาษณ์, 2562) มีความเห็นว่า ความละเอียดครบถ้วนของรายงานการตรวจพิสูจน์ที่จัดทำในส่วนกลางและในส่วนภูมิภาคนั้นอาจมีข้อแตกต่างอยู่บ้างด้วยเหตุเกี่ยวกับความพร้อมด้านเครื่องมือ อุปกรณ์ ซอฟท์แวร์สำหรับการตรวจพิสูจน์ที่ส่วนกลางมีความพร้อมมากกว่าส่วนภูมิภาค

ปัญหาขั้นต้นที่ผู้ตรวจพิสูจน์พยานหลักฐานในคดีอาชญากรรมคอมพิวเตอร์ต้องเผชิญเริ่มต้นขึ้นตั้งแต่ได้รับคำร้องขอให้ตรวจพิสูจน์พยานหลักฐานในคดี โดยผู้ตรวจพิสูจน์เกือบทุกรายล้วนให้ข้อมูลที่สอดคล้องกันว่า ขอบเขตการร้องขอจากพนักงานสอบสวนขาดความชัดเจนทำให้ไม่สามารถดำเนินการตรวจพิสูจน์ได้ทันที โดยปัญหาที่พบสามารถสรุปได้ดังนี้ (กชกร เพิงระนัย, สัมภาษณ์, 2562 ; ชานนท์ คำนวนศักดิ์, สัมภาษณ์, 2562 ; นิติ อินทลักษณ์, สัมภาษณ์, 2562 ; วันทนีย์ ตุลยเสวี, สัมภาษณ์, 2562 ; อัศว์ณุต แสงทองดี, สัมภาษณ์, 2562)

1. พนักงานสอบสวนมักมีหนังสือร้องขอให้ทำการตรวจพิสูจน์ของกลางในคดีโดยระบุวัตถุประสงค์ที่ต้องการตรวจพิสูจน์ด้วยถ้อยคำที่กว้างขวาง ไม่ชัดเจน หรือเป็นคำถามปลายเปิดเช่น “ขอให้ตรวจสอบหาพยานหลักฐานที่เกี่ยวข้อง” “ขอข้อมูลที่เป็นประโยชน์ต่อคดี”หรือการตั้งคำถามในการตรวจพิสูจน์ที่เกี่ยวข้องกับประเด็นข้อกฎหมาย เช่น “ขอให้ตรวจค้นว่ามีบัญชีสื่อสังคมออนไลน์ บัญชีธนาคาร ภาพถ่าย วีดีโอ แฟ้มข้อมูลที่ผิดกฎหมายหรือได้มาโดยผิดกฎหมาย” “ขอข้อมูลที่เป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ”ผู้ตรวจพิสูจน์อาจไม่สามารถวินิจฉัยข้อกฎหมายเองได้

2. พนักงานสอบสวนตั้งคำถามที่ต้องการให้มีการตรวจพิสูจน์ในลักษณะที่อยู่นอกขอบเขตที่วัตถุพยานจะสามารถระบุได้ เช่น การคาดการหรือคาดหมายถึงสภาพของวัตถุพยานหรือระบบการทำงานของวัตถุพยานที่มิได้ปรากฏในความเป็นจริง

3. พนักงานสอบสวนจัดส่งวัตถุพยานทุกชิ้นที่ยึดเป็นของกลางไปตรวจพิสูจน์ซึ่งมักมีปริมาณจำนวนมาก โดยมิได้ทำการคัดกรองส่งเฉพาะพยานหลักฐานที่เห็นว่าจำเป็นและมีประโยชน์ต่อรูปคดีจริงๆ ทำให้เกิดความล่าช้าในการปฏิบัติงานของผู้ตรวจพิสูจน์หลักฐาน ในเรื่องนี้ วันทนีย์ ตุลยเสวี (สัมภาษณ์, 2562) ได้กล่าวถึงประสบการณ์ที่เคยพบว่า ในคดีที่ได้รับความสนใจบางคดีพนักงานสอบสวนส่งของกลางจำนวนกว่า 300 รายการไปตรวจพิสูจน์ ซึ่งทางกองพิสูจน์หลักฐานกลางได้ขอให้พนักงานสอบสวนเลือกของกลางที่สำคัญและคิดว่าน่าจะใช้พิสูจน์ความผิดของผู้ถูกกล่าวหาได้จริงๆ ในชั้นแรกยังไม่สามารถหาข้อสรุปได้ จนกระทั่งต้องมีการจัดประชุมเจ้าหน้าที่ที่เกี่ยวข้องกับคดีจำนวนมากเพื่อหาข้อสรุปว่าจะเลือกตรวจสอบพยานหลักฐานชิ้นใดบ้าง และจะกำหนดวัตถุประสงค์ในการตรวจพิสูจน์อย่างไร ทำให้ใช้ระยะเวลานานพอสมควรจึงจะได้ข้อสรุป ส่งผลกระทบในเรื่องความล่าช้าของการตรวจพิสูจน์ในคดีดังกล่าวและการตรวจพิสูจน์ในคดีอื่นซึ่งอยู่

ในความรับผิดชอบของกองพิสูจน์หลักฐานกลางด้วย ในเรื่องนี้ เบญจพร วัชระวุฒิชัย (สัมภาษณ์, 2562) เคยได้รับการบอกเล่าปัญหาจากผู้เข้ารับฟังการบรรยายความรู้ด้านอาชญากรรมคอมพิวเตอร์ ซึ่งเป็นผู้ปฏิบัติงานด้านนิติคอมพิวเตอร์ว่า ในบางคดีซึ่งคนร้ายใช้อินเทอร์เน็ตคาเฟ่เป็นสถานที่ลงมือกระทำความผิด มีคอมพิวเตอร์ที่ให้บริการจำนวนมาก เมื่อพนักงานสอบสวนทำการยึดอุปกรณ์คอมพิวเตอร์ทั้งหมดมาเป็นของกลางในคดีและส่งตรวจพิสูจน์ หากผู้ตรวจพิสูจน์สุ่มตรวจคอมพิวเตอร์บางเครื่องแล้วพบข้อมูลยืนยันว่าน่าจะเป็นเครื่องคอมพิวเตอร์ที่ถูกใช้เป็นเครื่องมือในการกระทำความผิดและอาจเชื่อมโยงไปถึงตัวผู้ใช้งานได้แล้ว ผู้ตรวจพิสูจน์ยังมีความจำเป็นต้องทำการตรวจพิสูจน์เครื่องคอมพิวเตอร์ที่เหลืออีกหรือไม่ หรือในคดีที่มีผู้เสียหายอยู่ในท้องที่หลายแห่งทั่วประเทศ เมื่อผู้เสียหายในท้องที่หนึ่งแจ้งความดำเนินคดี และผู้ตรวจพิสูจน์ได้ตรวจพิสูจน์ของกลางในคดีพร้อมจัดทำความเห็นแล้ว ต่อมาหากมีผู้เสียหายรายอื่นแจ้งความดำเนินคดีกับผู้ต้องหาในมูลคดีเดียวกันในท้องที่อื่น มีปัญหาในเชิงกฎหมายว่า พนักงานสอบสวนในท้องที่คดีหลังต้องขอรับของกลางไปให้ผู้ตรวจพิสูจน์ในท้องที่ของตนทำการตรวจพิสูจน์ซ้ำอีกครั้งหรือไม่ หรือสามารถนำผลการตรวจพิสูจน์บนของกลางชิ้นเดียวกันในประเด็นเดียวกันจากคดีหนึ่งไปใช้ในคดีหนึ่งได้โดยตรง

4. พนักงานสอบสวนระบุรายละเอียดในหนังสือร้องขอให้ตรวจพิสูจน์หลักฐานไม่ครบถ้วนเพียงพอ โดยหลายกรณีมิได้มีการระบุข้อกล่าวหาและพฤติการณ์สังเขปของคดีไว้ในหนังสือขอให้ดำเนินการ รวมทั้งไม่ระบุชื่อและหมายเลขโทรศัพท์ติดต่อของพนักงานสอบสวนผู้รับผิดชอบในกรณีที่ผู้ตรวจพิสูจน์มีข้อสงสัยซักถามอีกด้วย

ปัญหาในเบื้องต้นเหล่านี้ทำให้ผู้ตรวจพิสูจน์หลักฐานยังไม่สามารถลงมือตรวจพิสูจน์พยานหลักฐานได้ในทันทีและจำเป็นต้องติดต่อกลับไปยังพนักงานสอบสวนผู้รับผิดชอบในคดีดังกล่าวเพื่อสอบถามพฤติการณ์รูปคดีโดยย่อ และประเด็นที่คิดว่าผลตรวจมีความสำคัญในการพิสูจน์ข้อกล่าวหาในคดี นอกจากนี้ยังทำให้ผู้ตรวจพิสูจน์หลักฐานต้องมีการประสานงานกับพนักงานสอบสวนเพื่อคัดกรองลดทอนขอบเขตของการตรวจพิสูจน์ เนื่องจากปัจจุบันเครื่องคอมพิวเตอร์และอุปกรณ์ดิจิทัลสามารถบันทึกข้อมูลคอมพิวเตอร์และข้อมูลอิเล็กทรอนิกส์อย่างอื่นจำนวนมากมายมหาศาล การตรวจสอบวิเคราะห์ที่ไม่มีการกำหนดขอบเขตและจำกัดพื้นที่ในการตรวจสอบที่ชัดเจนย่อมส่งผลกระทบต่อระยะเวลาที่ต้องใช้ในการตรวจพิสูจน์ การจัดหาเครื่องมือการตรวจพิสูจน์ที่เพียงพอต่องาน การกำหนดแนวทางการตรวจที่พิสูจน์ที่สอดคล้องกับการดำเนินคดี และการจัดทำรายงานผลการตรวจพิสูจน์ อีกทั้งในบางกรณียังพบปัญหาด้วยว่า เมื่อผู้ตรวจพิสูจน์ติดต่อสอบถามรายละเอียดแห่งคดีไปยังพนักงานสอบสวน พนักงานสอบสวนเองก็ไม่ทราบรายละเอียดแห่งคดีมากนักเนื่องจากมิได้เป็นผู้จับกุมคนร้ายเอง ทำให้ต้องประสานงานติดตามให้เจ้าพนักงานสืบสวนจับกุมซึ่งรู้รายละเอียดแห่งคดีในเชิงลึกเข้าให้ข้อมูลกับผู้ตรวจพิสูจน์ ทำให้การทำงานตรวจพิสูจน์ยิ่งล่าช้าออกไป (วันทนีย์ ตุลยเสวี, สัมภาษณ์, 2562)

ในด้านของเครื่องมืออุปกรณ์และซอฟท์แวร์ที่ใช้ในการตรวจพิสูจน์พยานหลักฐานถือได้ว่าเป็นอีกปัญหาที่มีความสำคัญมาก โดยเทคโนโลยีของโลกไซเบอร์และอุปกรณ์ดิจิทัลที่เปลี่ยนแปลงไปอย่างรวดเร็ว ซึ่งต้องอาศัยเครื่องมือในการตรวจพิสูจน์และซอฟท์แวร์ที่ใช้ในการตรวจพิสูจน์ที่มีมูลค่าราคาสูง โดยเฉพาะอย่างยิ่งซอฟท์แวร์ที่ใช้สำหรับการตรวจพิสูจน์ต้องนำเข้าจากต่างประเทศเป็นส่วนใหญ่ทำให้มีราคาแพงเนื่องจากมีลิขสิทธิ์และต้องมีการอัพเกรดให้เป็นปัจจุบันอยู่เป็นระยะ รวมทั้งต้องเสียค่าใช้จ่ายในการต่ออายุการได้รับอนุญาตให้ใช้งานซึ่งงบประมาณของหน่วยงานรัฐที่เกี่ยวข้องมีไม่เพียงพอ และถึงแม้ว่าจะมีซอฟท์แวร์ฟรีให้ดาวน์โหลดจากแหล่งข้อมูลเปิด (Open source) จำนวนมาก แต่ซอฟท์แวร์ฟรีดังกล่าวมักมีข้อจำกัดการใช้งาน เช่น กำหนดระยะเวลาสั้นเพื่อทดลองใช้งานเท่านั้น หรือความสามารถในการใช้งานตรวจพิสูจน์ที่ยังไม่ครบถ้วนสมบูรณ์อย่างซอฟท์แวร์ที่ต้องเสียค่าใช้จ่าย และในบางครั้งก็ยังสุ่มเสี่ยงต่อการเป็นซอฟแวร์ที่ละเมิดลิขสิทธิ์ผิดกฎหมายด้วย (กชกร เพิงระนัย, สัมภาษณ์, 2562 ; ชานนท์ คำนวนศักดิ์, สัมภาษณ์, 2562 ;วันทนีย์ ตุลยเสวี, สัมภาษณ์, 2562 ; อัศว์ณุต แสงทองดี, สัมภาษณ์, 2562) ซึ่งประเด็นนี้ เบญจพร วัชระวุฒิชัย (สัมภาษณ์, 2562) มีความเห็นเพิ่มเติมด้วยว่า การนำซอฟท์แวร์ฟรีให้ดาวน์โหลดจากแหล่งข้อมูลเปิดมาใช้งานในการตรวจพิสูจน์หลักฐานเพื่อแก้ไขปัญหาการขาดแคลนอุปกรณ์ในการตรวจพิสูจน์อาจเป็นการแก้ไขปัญหาอย่างเร่งด่วนในระยะสั้น แต่ในอนาคตอาจต้องเผชิญกับปัญหาข้อต่อสู้ในเรื่องมาตรฐานของผลการตรวจพิสูจน์ที่ได้รับจากซอฟท์แวร์บนแหล่งข้อมูลเปิด (Open source) ว่ามีความน่าเชื่อถือมากน้อยเพียงใด และผลที่ได้รับมีความเป็นไปได้ของความคลาดเคลื่อนมากน้อยแค่ไหน ซึ่งหากมีช่วงโหว่ในทางเทคนิคที่มีนัยสำคัญ อาจกลายเป็นข้อต่อสู้ที่ทางฝ่ายจำเลยอาจนำมาใช้หักล้างความน่าเชื่อถือในการรับฟังพยานหลักฐานของศาลได้

สำหรับกรณีของผู้ตรวจพิสูจน์ที่มีลักษณะการทำงานตรวจคัดกรองและเก็บวัตถุพยานในที่เกิดเหตุ (Onsize Seizure and Data Collection)ซึ่งผู้ตรวจพิสูจน์ร่วมปฏิบัติงานกับเจ้าหน้าที่อื่นในการปฏิบัติการตามหมายค้น ณ สถานที่ที่วัตถุพยานตั้งอยู่ ผู้ตรวจพิสูจน์ที่มีลักษณะงานประเภทนี้จะพบปัญหาว่าเครื่องมือและอุปกรณ์ที่ต้องใช้ในการเก็บข้อมูลตรวจพิสูจน์บริเวณหน้างานนั้นไม่เพียงพอ รวมทั้งขาดแคลนเครื่องมืออุปกรณ์ที่มีประสิทธิภาพสูงในการเข้าถึงข้อมูลคอมพิวเตอร์ในวัตถุพยาน นอกจากนี้ด้วยพัฒนาการปกป้องการเข้าถึงข้อมูลภายในอุปกรณ์ดิจิทัลสมัยใหม่โดยเฉพาะสมาร์ทโฟน ซึ่งถูกตั้งค่ารหัสผ่านไว้มักเกิดปัญหาไม่สามารถเข้าถึงข้อมูลได้โดยพลการ (กชกร เพิงระนัย, สัมภาษณ์, 2562 ;อัศว์ณุต แสงทองดี, สัมภาษณ์, 2562)ผู้ตรวจพิสูจน์ หรือแม้แต่เจ้าพนักงานสืบสวนมักเกิดความกังวลในเรื่องของวิธีการที่ใช้เพื่อให้เข้าถึงข้อมูลได้ เช่นการทำฟิชชิ่ง (Phishing)เพื่อให้คนร้ายหลงเปิดเผยชื่อผู้ใช้ (Log in) และรหัสผ่าน (Password) ของตน ว่าจะถือเป็นการได้มาซึ่งพยานหลักฐานโดยมิชอบด้วยกฎหมายหรือไม่ นอกจากนี้การเปลี่ยนแปลงทางเทคโนโลยีส่งผลต่อความสามารถในการจัดเก็บหลักฐาน เช่น เทคโนโลยีเกี่ยวกับการเข้ารหัสป้องกันข้อมูล (Data

encryption) เพื่อป้องกันการเข้าถึงข้อมูล ทำให้ไม่สามารถเข้าถึงข้อมูลดังกล่าวได้ หรือเทคโนโลยีที่ทำให้พยานหลักฐานสามารถเก็บอยู่ที่ใดก็ได้ เช่น ในระบบคลาวด์ (Cloud) ทำให้ผู้ตรวจพิสูจน์รวมทั้งเจ้าพนักงานอื่นที่เกี่ยวข้องกับการเข้าถึงข้อมูลในระบบ Cloud ไม่แน่ใจถึงขอบเขตอำนาจที่ได้รับตามหมายค้นซึ่งมักมีขอบเขตการเข้าถึงข้อมูลคอมพิวเตอร์ที่อยู่ในอุปกรณ์ดิจิทัลที่ตรวจค้นหรือตรวจยึดโดยเฉพาะในกรณีที่มีเหตุเร่งด่วนจำเป็นต้องเข้าถึงข้อมูลดังกล่าวแล้วผู้ต้องสงสัยไม่ให้ความร่วมมือในการเข้าถึงข้อมูล (เบญจพร วัชระวุฒิชัย, สัมภาษณ์, 2562)

ในขั้นตอนต่อมาคือ ขั้นตอนการออกรายงานผลการตรวจพิสูจน์ จากการสัมภาษณ์เชิงลึกพบว่าผู้ตอบแบบสัมภาษณ์ทุกรายพบสภาพปัญหาในการจัดทำรายงานผลการตรวจพิสูจน์ โดยสภาพข้อขัดข้องส่วนใหญ่สืบเนื่องมาจากปัญหาที่พบในชั้นการร้องขอให้มีการตรวจพิสูจน์ของพนักงานสอบสวนดังที่กล่าวมาข้างต้น โดยปัญหาที่พบระหว่างการจัดทำรายงานผลการตรวจพิสูจน์มีดังนี้ (กชกร เพิงระนัย, สัมภาษณ์, 2562 ; ชานนท์ คำนวนศักดิ์, สัมภาษณ์, 2562 ; นิติ อินทลักษณ์, สัมภาษณ์, 2562 ; วันทนีย์ ตุลยเสวี, สัมภาษณ์, 2562 ; อัศว์ณุต แสงทองดี, สัมภาษณ์, 2562)

1. ในกรณีที่พนักงานสอบสวนมิได้ระบุประเด็นจุดประสงค์ที่ต้องการให้มีการตรวจพิสูจน์ที่ชัดแจ้ง ทำให้ผู้ตรวจพิสูจน์ใช้เวลาในการทำรายงานข้อมูลที่ตรวจพบเป็นเวลานานมาก ทั้งที่ข้อตรวจพบบางอย่างอาจไม่มีความจำเป็นต่อรูปคดีมากนัก ในขณะที่ประเด็นสำคัญแห่งคดีอาจมิได้มีการเน้นย้ำไว้ในผลการตรวจ

2. เนื่องจากการตรวจพิสูจน์อาชญากรรมทางคอมพิวเตอร์ มีคำศัพท์ภาษาอังกฤษที่เกี่ยวข้องจำนวนมาก ซึ่งผู้ตรวจพิสูจน์ต้องใช้ระบุด้วยทับศัพท์ดังกล่าวเนื่องจากเป็นคำศัพท์สามัญที่ใช้ในระดับสากล บางครั้งทำให้พนักงานสอบสวนหรือผู้ใช้ประโยชน์ในรายงานเกิดความไม่เข้าใจและแปลความหมายไม่ถูกต้อง นอกจากนี้คำศัพท์หรือรูปประโยคที่ปรากฏในรายงานผลการตรวจพิสูจน์ผู้ตรวจพิสูจน์ต้องเลือกใช้คำศัพท์หรือรูปประโยคที่เป็นทางการและถูกต้องตามพจนานุกรมคอมพิวเตอร์ จึงทำให้บางคำศัพท์หรือบางรูปประโยคอาจสื่อความหมายที่ไม่เหมือนกับคำศัพท์หรือรูปประโยคที่บุคคลทั่วไปเข้าใจกัน

สภาพปัญหาที่พบกับการทำงานของผู้ตรวจพิสูจน์หลักฐานในคดีอาชญากรรมคอมพิวเตอร์ที่สำคัญประการสุดท้ายซึ่งไม่แตกต่างจากปัญหาที่หน่วยงานผู้บังคับใช้กฎหมายอื่นกำลังเผชิญ คือ การขาดแคลนกำลังผู้ตรวจพิสูจน์ด้านนิติคอมพิวเตอร์ ซึ่งปัจจุบันผู้ชำนาญการตรวจพิสูจน์ด้านดิจิทัลยังมีจำนวนน้อย ไม่เพียงพอต่อปริมาณคดี ส่งผลให้ผู้ตรวจพิสูจน์แต่ละท่านมีงานตรวจพิสูจน์ในความรับผิดชอบจำนวนมากแม้ในประเทศไทยจะมีผู้จบการศึกษาในสาขาด้านการจัดการคอมพิวเตอร์ หรือวิทยาการคอมพิวเตอร์ในแต่ละปีไม่น้อย แต่บัณฑิตดังกล่าวก็อาจไม่สามารถเป็นผู้เชี่ยวชาญด้านการตรวจพิสูจน์ทางนิติคอมพิวเตอร์ได้ทุกคน โดยอาจารย์ปริญญา หอมอเนก ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยทางไซเบอร์ (ออนไลน์, 2562) เคยอธิบายถึงคุณสมบัติของผู้ที่จะ

เป็นผู้ตรวจพิสูจน์พยานหลักฐานด้วยวิธีที่เรียกว่า “นิติคอมพิวเตอร์” (Computer Forensics) ว่าจำเป็นต้องเป็นผู้มีความสามารถใช้ความรู้ทางด้านการรักษาความปลอดภัยของข้อมูลและระบบสารสนเทศ(Information Security)และเจาะลึกในการพิสูจน์หลักฐานทางคอมพิวเตอร์ หรือนิติคอมพิวเตอร์ซึ่งหมายถึง การแสวงหาเก็บรักษาวิเคราะห์และการนำเสนอพยานหลักฐานที่เกี่ยวกับคอมพิวเตอร์ กล่าวอีกนัยหนึ่งก็คือการใช้กระบวนการที่จะระบุบ่งชี้เก็บรักษาและ กู้คืนบรรดาข้อมูลแบบดิจิทัลที่มีความสำคัญต่อการสืบสวน โดยศาสตร์เรื่องนิติคอมพิวเตอร์นับเป็นความรู้ขั้นสูงทางด้าน Information Security การรวบรวมและเก็บพยานหลักฐานที่อยู่ในรูปของข้อมูลดิจิทัลจำเป็นต้องกระทำโดยผู้ที่มีความเชี่ยวชาญทางด้านนิติคอมพิวเตอร์โดยเฉพาะ มิฉะนั้นข้อมูลที่มีค่าอาจสูญหายไปด้วยความรู้เท่าไม่ถึงการณ์

การนำเสนอพยานหลักฐานในคดีอาชญากรรมคอมพิวเตอร์

ในคดีอาญาทั่วไปรวมทั้งคดีอาชญากรรมคอมพิวเตอร์ เมื่อพนักงานสอบสวนผู้รับผิดชอบมีความเห็นว่าการสอบสวนแล้วเสร็จ พนักงานสอบสวนผู้รับผิดชอบจะทำความเห็นว่าควรสั่งฟ้องหรือควรสั่งไม่ฟ้องผู้ต้องหาในคดี แล้วส่งไปยังพนักงานอัยการพร้อมกับสำนวนการสอบสวน ตามประมวลกฎหมายวิธีพิจารณาความอาญามาตรา 141 เมื่อพนักงานอัยการได้รับสำนวนการสอบสวนคดีอาญาไว้พิจารณา พนักงานอัยการจะดำเนินการตรวจพิจารณาสำนวนและมีคำสั่งในทางคดีตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 143 โดยการปฏิบัติหน้าที่ดังกล่าวของพนักงานอัยการ มีระเบียบสำนักงานอัยการสูงสุดว่าด้วยการดำเนินคดีอาญาของพนักงานอัยการ พ.ศ. 2547 (ที่แก้ไขเพิ่มเติม) หมวดที่ 3 บัญญัติให้แนวทางไว้ว่า พนักงานอัยการต้องพิจารณาข้อเท็จจริงและพยานหลักฐานในสำนวนซึ่งพิสูจน์ความผิดหรือความบริสุทธิ์ของผู้ต้องหา รวมถึงแนวทางการดำเนินคดีจากพยานหลักฐาน และข้อกฎหมายว่าจะทำให้ศาลลงโทษผู้ต้องหาได้หรือไม่ ทั้งนี้ ตามข้อ 69 ของระเบียบดังกล่าว ได้บัญญัติให้พนักงานอัยการพิจารณาพยานหลักฐานในคดีให้ได้ความแน่ชัดว่าผู้ต้องหาได้กระทำความผิดหรือไม่ก่อนจะมีความเห็นและคำสั่ง หากยังไม่แน่ชัดก็ให้สั่งให้พนักงานสอบสวนทำการสอบสวนเพิ่มเติมหรือสั่งให้ส่งพยานมาเพื่อซักถามตามรูปคดีก็ได้ จากนั้น เมื่อพนักงานอัยการเห็นว่าข้อเท็จจริงในคดีสิ้นกระแสความและคดีมีพยานหลักฐานเพียงพอในการทำความเห็นและคำสั่งแล้วพนักงานอัยการจะมีคำสั่งทางคดี ซึ่งหากพนักงานอัยการมีคำสั่งฟ้องผู้ต้องหาในคดีอาญา พนักงานอัยการมีอำนาจหน้าที่เป็นโจทก์ฟ้องผู้ต้องหาเป็นจำเลยในคดีอาญาและต้องเป็นผู้ดำเนินกระบวนพิจารณาเป็นโจทก์ในศาลชั้นต้น ศาลอุทธรณ์ และศาลฎีกา จนกว่าคดีนั้นจะถึงที่สุดตามกฎหมาย

ในกรณีที่พนักงานอัยการเป็นโจทก์ยื่นฟ้องผู้ต้องหาเป็นจำเลยต่อศาล และศาลมีคำสั่งประทับรับฟ้องไว้พิจารณาแล้ว คดีจะเข้าสู่กระบวนการพิจารณาในศาล โดยบุคลากรที่มีบทบาทในกระบวนการพิจารณาคดีอาชญากรรมคอมพิวเตอร์ ได้แก่

1. พนักงานอัยการ

เนื่องจากบุคคลทุกคนย่อมได้รับการสันนิษฐานว่าเป็นผู้บริสุทธิ์ อันเป็นสิทธิมนุษยชนขั้นพื้นฐานที่ได้รับการรับรองไว้ในกฎหมายของนานาประเทศรวมถึงรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 มาตรา 29 ตามหลักเรื่อง Presumption of Innocence พนักงานอัยการซึ่งอยู่ในฐานะทนายแผ่นดินฝ่ายโจทก์จึงย่อมมีภาระหน้าที่ในการนำสืบพิสูจน์การกระทำความผิดของจำเลย โดยพนักงานอัยการต้องนำพยานหลักฐานซึ่งประกอบไปด้วยพยานบุคคล พยานเอกสาร พยานวัตถุ รวมทั้งพยานผู้เชี่ยวชาญ ที่พนักงานสอบสวนรวบรวมได้เข้าสืบในชั้นศาลให้เป็นไปตามมาตรฐานในการพิสูจน์คดีอาญาในระดับที่พ้นข้อสงสัยตามสมควร หรือ “Proof Beyond Reasonable Doubt”ดังที่ได้กล่าวไว้ในบทที่ 2 โดยในกระบวนการสืบพยานในชั้นศาลหากทนายความฝ่ายจำเลยถามค้านพยานบุคคลฝ่ายโจทก์ พนักงานอัยการมีหน้าที่ต้องถามติงพยานบุคคลตามรูปคดี นอกจากนี้พนักงานอัยการโจทก์มีหน้าที่ซักค้านพยานหลักฐานที่ทนายความฝ่ายจำเลยนำเสนอเข้าสู่กระบวนพิจารณาเพื่อแสดงข้อเท็จจริงให้ปรากฏว่าพยานหลักฐานที่ฝ่ายจำเลยนำเสนอนั้นขาดความน่าเชื่อถือหรือรับฟังไม่ได้ในทางกฎหมายหรือไม่อย่างไร

ในคดีที่จำเลยให้การรับสารภาพตามฟ้องและฐานความผิดตามฟ้องมีอัตราโทษจำคุกขั้นต่ำไม่ถึงห้าปี ศาลสามารถพิพากษาคดีไปได้โดยไม่จำเป็นต้องสืบพยานหลักฐาน แต่หากฐานความผิดซึ่งฟ้องจำเลยมีอัตราโทษจำคุกขั้นต่ำตั้งแต่ห้าปีขึ้นไปหรือโทษสถานหนักกว่านั้น พนักงานอัยการโจทก์มีหน้าที่ต้องนำสืบพยานหลักฐานโจทก์ประกอบคำรับสารภาพของจำเลย ให้ศาลเชื่อได้ว่าจำเลยกระทำความผิดจริง ตามนัยมาตรา 176 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา (ประมวลกฎหมายวิธีพิจารณาความอาญา (ฉบับ Update ล่าสุด), ออนไลน์, 2562) ส่วนในคดีที่จำเลยปฏิเสธฟ้องโจทก์ว่ามิได้กระทำความผิดตามฟ้อง พนักงานอัยการโจทก์มีหน้าที่นำสืบพยานหลักฐานเพื่อพิสูจน์การกระทำความผิดของจำเลย

2. ทนายความฝ่ายจำเลย

ในการต่อสู้คดีของจำเลยในคดีอาชญากรรมคอมพิวเตอร์จะมีทนายความเป็นผู้ช่วยเหลือในการดำเนินคดีและสืบพยานในคดีที่มีอัตราโทษประหารชีวิตหรือในคดีที่จำเลยมีอายุไม่เกินสิบแปดปีในวันที่ถูกฟ้องต่อศาล ก่อนเริ่มพิจารณาศาลจะถามจำเลยว่ามีทนายความหรือไม่ ถ้าไม่มีก็ให้ศาลตั้งทนายความให้ ส่วนในคดีที่มีอัตราโทษจำคุก ก่อนเริ่มพิจารณาศาลจะถามจำเลยว่ามีทนายความหรือไม่ ถ้าไม่มีและจำเลยต้องการทนายความ ศาลจะแต่งตั้งทนายความเพื่อให้ความช่วยเหลือ ทั้งนี้เป็นไปตามมาตรา 173 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา ส่วนในกรณีที่จำเลยมีความประสงค์ที่จะจัดหาทนายความซึ่งมีความเชี่ยวชาญเฉพาะคดีเข้าว่าความต่อสู้คดี

ก็สามารถกระทำได้เช่นเดียวกัน โดยแนวทางในการสู้คดีของฝ่ายจำเลยในคดีอาชญากรรมคอมพิวเตอร์มักเป็นลักษณะการต่อสู้ว่ามิได้เป็นผู้กระทำความผิดตามฟ้อง เช่น ต่อสู้คดีในเรื่องถิ่นที่อยู่ในวันเกิดเหตุ หรือต่อสู้เพื่อทำลายความน่าเชื่อถือของพยานหลักฐานฝ่ายโจทก์ ในขณะที่หากคดีดังกล่าวมีผู้กระทำความผิดตั้งแต่สองคนขึ้นไป ฝ่ายจำเลยอาจต่อสู้คดีแบบภาคเสธโดยยอมรับว่ามีความเกี่ยวข้องกับการกระทำความผิดอยู่บ้างแต่เป็นเพียงการให้ความสะดวกกับผู้กระทำความผิดรายอื่นมิใช่ผู้กระทำความผิดหลักในคดี เช่น ต่อสู้ว่าเป็นเพียงผู้สนับสนุนในการกระทำความผิดไม่ใช่ตัวการร่วมในการกระทำความผิด เนื่องจากความรับผิดทางอาญาของผู้สนับสนุนมีอัตราโทษเพียงสองในสามของโทษที่กำหนดสำหรับความผิดฐานนั้นๆ (ตามมาตรา 86 แห่งประมวลกฎหมายอาญา) และหากความผิดที่เกิดขึ้นอยู่ในขั้นของการพยายาม (ความผิดยังไม่สำเร็จ) ผู้สนับสนุนไม่ต้องรับโทษตามกฎหมาย (ตามมาตรา 88 แห่งประมวลกฎหมายอาญา) ซึ่งแนวทางการต่อสู้แบบหลังมักพบในคดีความผิดเกี่ยวกับการฉ้อโกงออนไลน์ในกรณีจำเลยคือเจ้าของบัญชีเงินฝากซึ่งถูกใช้รองรับเงินที่คนร้ายหลอกลวงได้ไปจากผู้เสียหาย(เบญจพร วัชระวุฒิชัย, ออนไลน์, 2562)

3. ศาล

เมื่อพนักงานอัยการโจทก์ และทนายความจำเลย ได้นำเสนอพยานหลักฐานที่เกี่ยวข้องกับคดีเข้าสู่การพิจารณาจนกระทั่งคดีเสร็จการพิจารณาแล้ว ผู้พิพากษาในคดีจะพิจารณาว่าพยานหลักฐานใดที่สามารถรับฟังได้บ้างโดยพิจารณาถึงบทตัดพยานและข้อต้องห้ามรับฟังพยานหลักฐานบางชนิด เช่น พยานหลักฐานที่เกิดขึ้นโดยมิชอบ ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226 หรือบทตัดพยานบอกเล่าตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226/3 รวมไปถึงพยานหลักฐานบางประเภทเช่นพยานหลักฐานที่เกิดขึ้นโดยชอบแต่ได้มาเนื่องจากการกระทำโดยมิชอบ หรือเป็นพยานหลักฐานที่ได้มาโดยอาศัยข้อมูลที่เกิดขึ้นหรือได้มาโดยมิชอบ ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226/1 ซึ่งศาลต้องใช้ความระมัดระวังในการรับฟัง จากนั้นศาลจะทำการชั่งน้ำหนักพยานหลักฐานซึ่งสามารถรับฟังได้ในคดีทั้งหมดว่าพยานโจทก์นั้นมีความน่าเชื่อถือหนักแน่นมั่นคง รับฟังโดยปราศจากเหตุสงสัยตามสมควรว่าจำเลยเป็นผู้กระทำความผิดตามฟ้องจริงหรือไม่ หากคดียังมีความสงสัยตามสมควรว่าจำเลยได้กระทำผิดหรือไม่ศาลจะยกประโยชน์แห่งความสงสัยนั้นให้จำเลย และพิพากษายกฟ้อง ตามนัยประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 227

ในส่วนของสภาพปัญหาในการนำเสนอพยานหลักฐานในคดีอาชญากรรมคอมพิวเตอร์ ผู้วิจัยได้ทำการสัมภาษณ์เชิงลึกพนักงานอัยการซึ่งมีประสบการณ์ดำเนินคดีอาชญากรรมคอมพิวเตอร์ รวมถึงเจ้าพนักงานสืบสวน พนักงานสอบสวน และผู้ตรวจพิสูจน์ทางนิติคอมพิวเตอร์ ซึ่งเคยมีประสบการณ์เข้าเบิกความเป็นพยานในชั้นศาล พบสภาพปัญหาเกิดขึ้นทั้งในขั้นตอนของการพิจารณาก่อนฟ้องของพนักงานอัยการ และในชั้นดำเนินคดีในศาล ดังนี้

3.1สภาพปัญหาที่พบในชั้นก่อนฟ้อง

พนักงานอัยการซึ่งรับผิดชอบงานคดีอาชญากรรมคอมพิวเตอร์ (เบญจพร วัชระวุฒิชัย, สัมภาษณ์, 2562 ; ปกรณ์ ธรรมโรจน์, สัมภาษณ์, 2562) พบว่าสำนวนการสอบสวนที่พนักงานสอบสวนส่งไปยังพนักงานอัยการเพื่อมีคำสั่งนั้น มักมีการรวบรวมพยานหลักฐานเกี่ยวกับ

การกระทำความผิดทางคอมพิวเตอร์ไม่ครบถ้วน เช่น กรณีการฉ้อโกงหลอกลวงจำหน่ายสินค้าผ่านทางระบบอินเทอร์เน็ต ในขณะที่ผู้เสียหายเข้าแจ้งความร้องทุกข์ ผู้เสียหายมิได้ทำการบันทึกหน้าเว็บเพจที่มีการประกาศจำหน่ายสินค้าเอาไว้ โดยพนักงานสอบสวนบางรายมิได้แจ้งแนะนำให้ผู้เสียหายรีบดำเนินการ และในส่วนของการตรวจสอบข้อมูลทางบัญชีของคนร้ายที่ได้ไปซึ่งเงินของผู้เสียหาย พนักงานสอบสวนมักมีหมายเรียกให้ธนาคารพาณิชย์ผู้ให้บริการทางบัญชีที่พบการกระทำความผิดจัดส่งรายการเดินบัญชีเงินฝากที่เกี่ยวข้องกับการกระทำความผิด แต่มักมิได้เรียกให้จัดส่งภาพถ่ายที่บันทึกได้จากกล้องวงจรปิดว่าผู้ใดเป็นผู้กดถอนเงินออกจากบัญชีไป ซึ่งในประเด็นนี้พบในชั้นศาลว่าจำเลยมักต่อสู้ว่าเป็นเพียงผู้เปิดบัญชีและส่งมอบบัญชีธนาคารพร้อมบัตรเอทีเอ็มให้แก่บุคคลอื่นซึ่งน่าจะเป็นคนร้ายที่นำไปใช้หลอกลวงผู้เสียหาย นอกจากนี้ในกรณีที่ปรากฏข้อเท็จจริงในคดีเกี่ยวพันกับเบอร์โทรศัพท์ของคนร้ายที่กระทำความผิด พนักงานสอบสวนบางรายก็มิได้สอบถามข้อมูลการเปิดใช้บริการและข้อมูลการโทร (Call Logs) มาประกอบคดีในเวลาอันสมควรตั้งแต่ทราบเหตุ ซึ่งกว่าสำนวนการสอบสวนจะส่งไปยังพนักงานอัยการเพื่อพิจารณาและพนักงานอัยการมีคำสั่งให้ทำการสอบสวนรวบรวมพยานหลักฐานเพิ่มเติมมักเป็นระยะเวลาล่วงเลยมาก คนร้ายสามารถลบหรือแก้ไขข้อความสนทนาหรือหน้าเว็บเพจที่มีการประกาศจำหน่ายสินค้า รวมทั้งธนาคารพาณิชย์หรือผู้ให้บริการสัญญาณโทรศัพท์ก็ไม่อาจจัดส่งพยานหลักฐานที่เกี่ยวข้องได้ เนื่องจากโดยปกติข้อมูลผู้ให้บริการจะจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ รวมถึงข้อมูลส่วนบุคคลต่างๆของลูกค้าผู้ใช้บริการเป็นเวลาไม่เกิน 90 วันเท่านั้นโดยปัญหานี้ ปกรณ์ ธรรมโรจน์ (สัมภาษณ์, 2562) มีความเห็นว่าเป็นเพราะพนักงานสอบสวนซึ่งมิใช่พนักงานสอบสวนของกลุ่มงานหรือสายงานที่รับผิดชอบคดีอาชญากรรมคอมพิวเตอร์โดยตรงขาดที่ปรึกษาในการดำเนินคดีทำให้การดำเนินคดีไม่ได้ข้อเท็จจริงในสาระสำคัญบางประการ ทำให้ขาดแนวทางปฏิบัติที่สมควรดำเนินการตั้งแต่โอกาสแรกที่พนักงานสอบสวนเริ่มต้นทำการสอบสวนคดี

ปัญหาอีกประการหนึ่งที่มักพบคือ แม้สำนวนการสอบสวนจะปรากฏพยานหลักฐานที่เกี่ยวข้อง แต่พนักงานสอบสวนยังขาดการสังเคราะห์และวิเคราะห์เชื่อมโยงเหตุผลของพยานหลักฐานนั้นทำให้บางครั้งคุณค่าในการใช้ประโยชน์จากพยานหลักฐานยังไม่บริบูรณ์ ซึ่งในชั้นพนักงานอัยการ หากพนักงานอัยการไม่มีความชำนาญด้านพยานหลักฐานดิจิทัล รวมไปถึงความรู้ในศาสตร์ที่เกี่ยวข้อง เช่น ความเข้าใจในเรื่องการทำธุรกรรมทางการเงินและรายการเดินบัญชี ก็ย่อมทำให้ขาดโอกาสที่จะนำเสนอข้อเท็จจริงบางประเด็นที่เป็นประโยชน์ต่อรูปคดี โดยในประเด็นนี้ เบญจพร วัชระวุฒิชัย (สัมภาษณ์, 2562) ชี้ให้เห็นตัวอย่างคดีซึ่งแม้จะไม่มีพยานหลักฐานทางดิจิทัล หรือการตรวจพิสูจน์ทางนิติคอมพิวเตอร์ในคดีฉ้อโกงออนไลน์ พนักงานอัยการสามารถหาร่องรอยการกระทำความผิดของผู้ต้องหาได้จากรูปแบบการทำธุรกรรมทางการเงิน เช่น ข้อมูลระบบการแจ้งเตือนการทำธุรกรรมผ่านการส่งข้อความสั้น (SMS) ไปยังโทรศัพท์เคลื่อนที่ของคนร้าย การทำธุรกรรมเพิ่มวงเงินเบิกถอนผ่านตู้เอทีเอ็มหรือการปิดบัญชีซึ่งเจ้าของบัญชีต้องเป็นผู้ดำเนินการเองหรือต้องมีการแสดงข้อมูลส่วนตัวอย่างอื่นที่ไม่ปรากฏอยู่บนบัตรเอทีเอเอ็มซึ่งผู้ต้องหาอ้างว่ามอบให้ผู้อื่นไป

เพื่อยืนยันว่าเจ้าของบัญชีเป็นผู้มีส่วนเกี่ยวข้องร่วมกระทำความผิดมิใช่เป็นเพียงแค่ผู้รับจ้างเปิดบัญชีเท่านั้น หรือข้อสังเกตเกี่ยวกับห้วงเวลาทำรายการและของรูปแบบรายการเดินบัญชีเพื่อบ่งบอกความแตกต่างระหว่างบัญชีที่ใช้ในการกระทำความผิดซึ่งเปิดโดยคนร้ายเอง กับบัญชีซึ่งมีผู้รับจ้างเปิด รวมถึงสถานที่ตั้งของตู้กดเงินสดที่คนร้ายใช้ทำรายการว่ามีความเชื่อมโยงกับพฤติการณ์อย่างอื่นในคดี เช่น บริเวณที่มีการใช้โทรศัพท์ติดต่อหลอกลวงผู้เสียหายในช่วงเวลาเกิดเหตุ (Cell Site)รวมไปถึงถิ่นที่อยู่ของผู้ต้องหา ซึ่งหากพนักงานอัยการซึ่งไม่คุ้นเคยกับเทคนิคสืบสวนร่องรอยทางการเงินดังกล่าวข้างต้น ย่อมพบปัญหาในการโน้มน้าวใจให้ศาลรับฟังพยานหลักฐานแวดล้อมดังกล่าวมาประกอบให้รับฟังหนักแน่นมั่นคงเพียงพอที่จะลงโทษจำเลย หรือแม้กระทั่งพนักงานอัยการบางรายยังไม่ทราบแนวทางที่สามารถมีคำสั่งให้พนักงานสอบสวนทำการสอบสวนรวบรวมพยานหลักฐานเพิ่มเติม

3.2 สภาพปัญหาที่พบในชั้นหลังฟ้อง (ชั้นพิจารณาในศาล)

ดรัณ จาดเจริญ (สัมภาษณ์, 2562) ได้แบ่งปันประสบการณ์สำคัญจากที่เคยเบิกความในฐานะผู้สืบสวน และผู้ตรวจพิสูจน์พยานหลักฐานทางอิเล็กทรอนิกส์ของสำนักงานตำรวจแห่งชาติ พบปัญหาและข้อขัดข้องเกี่ยวในส่วนต่างๆ เช่น การอธิบายความรู้พื้นฐานเกี่ยวกับการทำงานของระบบคอมพิวเตอร์ของบุคคลที่เข้าร่วมในการพิจารณาคดีซึ่งต้องใช้เวลาและยากต่อการทำความเข้าใจของพนักงานอัยการ ทนายความ และศาล ซึ่งศึกษาเฉพาะด้านกฎหมายแต่ไม่มีความรู้ด้านนิติคอมพิวเตอร์โดยเฉพาะอย่างยิ่ง ในการเบิกความถึงขั้นตอนกระบวนการของการตรวจพิสูจน์และทำรายงานการตรวจพิสูจน์ทางนิติคอมพิวเตอร์ในปัจจุบันผู้เบิกความจะพบอุปสรรคว่าในการนำเสนอข้อมูลทางเทคนิคผ่านถ้อยคำภายในระยะเวลาพิจารณาอันมีจำกัดเพื่อให้ศาลบันทึกถ้อยคำในรูปของเอกสารเป็นสิ่งที่ยากมากอีกทั้งการเบิกความถึงข้อสันนิษฐานซึ่งกระบวนการพิสูจน์ข้อเท็จจริงทำได้ยาก ตัวอย่างเช่น ในการกระทำความผิดต่อเว็บไซต์ของสถาบันการเงินลักลอบนำเงินของบุคคลออกไปจากธนาคารผ่านทางระบบธนาคารอิเล็กทรอนิกส์ เป็นภาระของพนักงานสอบสวนที่จะต้องอธิบายวิธีการเทคนิคที่คนร้ายได้ใช้ในการกระทำความผิด ซึ่งในหลายครั้งพบว่าเป็นเทคโนโลยีทางคอมพิวเตอร์ที่มีความสลับซับซ้อน ยากต่อการพิสูจน์และอธิบาย แม้แต่ในกลุ่มผู้เชี่ยวชาญด้านคอมพิวเตอร์เอง เช่นกรณีมีการสันนิษฐานว่าคนร้ายได้ใช้เทคนิคที่เรียกว่า Man in the Browser ในการดักรับรหัสผ่านของผู้เสียหายก่อนนำไปใช้ในการกระทำความผิด หรือ การอธิบายถึงรูปแบบการทำงานของอุปกรณ์ที่ใช้ในการถอดรหัสสัญญาณที่ส่งผ่านเคเบิ้ลทีวี เพื่อนำไปใช้ในการละเมิดลิขสิทธิ์ให้สามารถดูภาพยนตร์ผ่านทางเครือข่ายอินเทอร์เน็ตได้ เป็นต้นการนำเสนอความรู้เพื่อให้เกิดความเข้าใจในเรื่องดังกล่าว ซึ่งปกติก็นับว่าเป็นเรื่องที่เข้าใจได้ยาก และมักจะถูกจำกัดด้วยการให้บอกเล่าในเวลาอันสั้นในลักษณะของการสรุปโดยย่อ หรือใช้เพียงพยานเอกสารประกอบการอธิบาย ทำให้เจ้าหน้าที่หรือผู้เชี่ยวชาญไม่สามารถอธิบายหลักการต่างๆให้พนักงานอัยการ ทนายความ และศาลเกิดความเข้าใจถูกต้องตรงกัน

ความท้าทายสำคัญในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในชั้นศาลอีกประการหนึ่ง คือ ศิลปะในการอธิบายเรื่องทางเทคนิคที่ซับซ้อนให้ง่ายต่อการทำความเข้าใจของทุกฝ่ายในกระบวนพิจารณา โดยเบญจพร วัชระวุฒิชัย (สัมภาษณ์, 2562) ได้กล่าวถึงประสบการณ์ในการสืบพยานคดีอาชญากรรมคอมพิวเตอร์ว่า เมื่อศาลมีหน้าที่ต้องชั่งน้ำหนักพยานหลักฐานในทางคดีว่าโจทก์ได้นำสืบพิสูจน์หลักฐานให้ปราศจากข้อสงสัยอันสมควรว่าจำเลยเป็นผู้กระทำความผิดตามฟ้อง

ดังนั้นพนักงานอัยการโจทก์จึงมีหน้าที่ต้องเรียงร้อยความเชื่อมโยงของพยานหลักฐานในทางคดี จัดลำดับก่อนหลังของมูลเหตุในคดีและขั้นตอนการสืบสวนสอบสวน อีกทั้งควบคุมการเบิกความของพยานบุคคลซึ่งมักประกอบไปด้วยผู้เสียหาย เจ้าพนักงานสืบสวน ผู้ตรวจพิสูจน์หลักฐาน เจ้าหน้าที่ของบริษัทผู้ให้บริการอินเทอร์เน็ต เจ้าหน้าที่ของสถาบันการเงินที่เกี่ยวข้องกับบัญชีที่ใช้ในการกระทำความผิดของคนร้าย พนักงานสอบสวน ซึ่งต่างมีระดับความรู้ความเข้าใจและทักษะในการเบิกความที่แตกต่างกัน ให้เกิดความสอดคล้องต้องกัน น่าเชื่อถือ และไม่ถูกโจมตีโดยคำถามค้านของทนายจำเลยจนกระทบต่อรูปคดี นอกจากนี้ในบางครั้งถ้อยคำที่พยานใช้ตามหลักวิชาชีพโดยเฉพาะคำศัพท์ทางเทคนิค พนักงานอัยการควรจะช่วยเรียบเรียงถ้อยคำให้สอดคล้องกับถ้อยคำในทางกฎหมาย โดยเฉพาะถ้อยคำเฉพาะที่ปรากฏอยู่ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 (ที่แก้ไขเพิ่มเติม) เพื่อช่วยให้ผู้พิพากษาในคดีเข้าใจข้อเท็จจริงที่พยานเบิกความได้ง่ายขึ้น ทั้งยังเป็นการสะดวกในการที่จะหยิบยกถ้อยคำในคำเบิกความพยานดังกล่าวไปใช้ในการวินิจฉัยพิพากษาคดีอีกด้วย อย่างไรก็ดี พนักงานอัยการแต่ละท่านมีภาระความรับผิดชอบในคดีที่หลากหลายแตกต่างกัน ซึ่งหากได้รับมอบหมายให้ดำเนินคดีอาชญากรรมคอมพิวเตอร์อยู่บ่อยครั้ง พนักงานอัยการผู้นั้นย่อมมีความคุ้นเคยต่อเทคนิคการนำเสนอพยานหลักฐานและการดำเนินคดีอาชญากรรมคอมพิวเตอร์ แต่หากพนักงานอัยการท่านนั้นรับผิดชอบงานคดีด้านอื่นเป็นหลักก็อาจเกิดข้อขัดข้องบางประการในการนำเสนอพยานหลักฐานในชั้นศาล

นอกจากนี้เบญจพร วัชระวุฒิชัย (สัมภาษณ์, 2562) ได้ให้ข้อสังเกตว่า ในการนำสืบพยานหลักฐานดิจิทัลและการตรวจพิสูจน์ทางนิติคอมพิวเตอร์ในชั้นศาล มีความแตกต่างจากการนำสืบพยานหลักฐานอย่างอื่น อันได้แก่ การนำสืบการตรวจพิสูจน์ดีเอ็นเอ การนำสืบการตรวจพิสูจน์ตัวอย่างลายมือบนเอกสาร หรือการนำสืบบาดแผลในคดีอาญาทั่วไป ซึ่งลักษณะการถามค้านของทนายความจำเลยมักไม่ค่อยต่อสู้ในเรื่องมาตรฐานการตรวจพิสูจน์มากนัก และหากมีการโต้แย้งพนักงานอัยการย่อมใช้การถามติงตามรูปคดีได้ไม่ยาก แตกต่างจากการนำสืบพยานหลักฐานดิจิทัลและการตรวจพิสูจน์ทางนิติคอมพิวเตอร์ ซึ่งโดยสภาพของพยานที่อยู่ในรูปของอิเล็กทรอนิกส์ที่อาจถูกปนเปื้อน เปลี่ยนแปลง ทำให้เสียหายได้อย่างง่ายดาย ทั้งการทำสำเนาข้อมูลอิเล็กทรอนิกส์ผ่านอุปกรณ์ดิจิทัลสามารถกระทำต่อข้อมูลในปริมาณมากและไม่จำกัดจำนวนครั้ง เทคนิคในการปลอมแปลงและเลียนแบบร่องรอยมีความเป็นไปได้และมักต้องใช้วิธีการที่ซับซ้อนโดยมาตรฐานในการตรวจสอบอาจมีความบริบูรณ์ไม่เหมือนกันเมื่อกระทำผ่านเครื่องมือ อุปกรณ์ และซอฟท์แวร์ที่แตกต่างกัน อีกทั้งเมื่อเทคโนโลยีในโลกไซเบอร์พัฒนาอย่างไม่หยุดยั้ง เครื่องมือและอุปกรณ์ในการตรวจพิสูจน์เหล่านี้ย่อมต้องมีพลวัตรตามไปด้วยต่างจากการตรวจพิสูจน์แบบอื่นในคดีอาญาซึ่งอุปกรณ์ที่เครื่องมือที่ใช้ในการตรวจสอบมิได้มีการเปลี่ยนแปลงไปจากอดีตมากนักดังนั้นในคดีที่ฝ่ายจำเลยเป็นผู้มีความรู้ความเข้าใจด้านดิจิทัลเป็นอย่างดี ย่อมสามารถหาช่องโหว่ในการทำลายความน่าเชื่อถือของพยานฝ่ายโจทก์ได้ ซึ่งอาจทำให้พนักงานอัยการที่ว่าความในคดีดังกล่าวพบข้อขัดข้องในการถามติงพยานเพื่อให้น้ำหนักของคำเบิกความพยานเกี่ยวกับผลการตรวจพิสูจน์กลับมาน่าเชื่อถือได้ หรืออาจพบอุปสรรคในการซักค้านพยานผู้เชี่ยวชาญที่ฝ่ายจำเลยเพิ่งอ้างนำมาเบิกความในชั้นศาลได้หากพนักงานอัยการผู้นั้นไม่มีความรู้ความเข้าใจในด้านนิติคอมพิวเตอร์ที่ดีพอ

ตัวอย่างการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในปัจจุบัน

ตัวอย่างการดำเนินคดีอาชญากรรมคอมพิวเตอร์ที่ผู้วิจัยเห็นว่าแสดงถึงรูปแบบการดำเนินงานของบุคลากรในกระบวนการยุติธรรมทั้งระบบครบถ้วน และมีนัยสำคัญต่อการนำไปใช้วิเคราะห์สภาพปัญหาที่เกิดขึ้นในการดำเนินคดีเพื่อที่จะใช้กำหนดแนวทางในการแก้ไขปัญหาและเพิ่มประสิทธิภาพในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในอนาคต ดังที่จะได้ทำการศึกษาต่อไปในบทที่ 4 ต่อไป มีดังนี้

1. คดีปลอมอีเมลแก้ไขข้อมูลเพื่อลักเงิน(เรวัติ บุญตันหล้า, สัมภาษณ์, 2562)

เมื่อประมาณปลายเดือนกันยายน 2558 มีลูกค้าชื่อ นาย R (ชื่อสมมติ) ชาวสเปน ได้ส่งอีเมล (alphaxxx@hotmsil.com) (ชื่อสมมติ) ไปสั่งสินค้าจำพวกเครื่องเงินจากบริษัท A (ชื่อสมมุติ) ที่อีเมลของบริษัท A (psilver@xxxinfo.com) จากนั้นทางบริษัทจึงได้ตกลงรับคำสั่งซื้อและได้เริ่มผลิตสินค้า ต่อมาทางลูกค้าได้ส่งอีเมลมาสั่งสินค้าเพิ่มเติม รวมสินค้าที่สั่งจำนวน 2 ครั้ง เป็นเงินจำนวน 566,659 บาท หลังจากนั้นประมาณ 1 เดือน ลูกค้าได้ส่งอีเมลแจ้งบริษัทว่าให้ส่งสินค้าให้กับตนก่อนสำหรับสินค้าบางส่วนที่ผลิตเสร็จแล้ว เพื่อตนจะได้นำสินค้าไปออกงานแสดงสินค้า หลังจากนั้นทางบริษัทจึงได้ส่งสินค้าไปยังร้าน ค. (ชื่อสมมติ) เพื่อให้เป็นผู้จัดส่งสินค้าต่อไปยังลูกค้าที่ประเทศสเปน หลังจากลูกค้าได้รับสินค้าแล้ว ต่อมาเมื่อวันที่ 30 พฤศจิกายน 2558 ลูกค้าได้ส่งอีเมลแจ้งบริษัทว่าจะโอนเงินให้ทางบริษัทในวันรุ่งขึ้น หรือไม่เกินวันที่ 2 ธันวาคม 2558 หลังจากนั้นวันที่ 9 ธันวาคม 2558 ทางบริษัทได้ส่งอีเมลไปสอบถามลูกค้าว่าได้โอนเงินชำระค่าสินค้าให้กับทางบริษัทแล้วหรือไม่เนื่องจากตรวจสอบแล้วยังไม่มียอดโอนเงินเข้าไปยังบัญชีของทางบริษัท จากนั้นเมื่อวันที่ 17 ธันวาคม 2558 ทางลูกค้าได้ส่งข้อมูลการโอนเงินแสดงแก่ทางบริษัท ซึ่งจากการตรวจสอบปรากฏว่าหมายเลขบัญชีปลายทางที่รับโอนเงินไม่ใช่บัญชีของบริษัท A แต่เป็นบัญชีของผู้ต้องหา บริษัท A จึงแจ้งลูกค้าไปว่าบัญชีที่ลูกค้าโอนไปนั้นไม่ใช่บัญชีของทางบริษัท ซึ่งลูกค้าได้แจ้งทางบริษัทว่า เมื่อประมาณวันที่ 30 พฤศจิกายน 2558 ได้มีอีเมลแจ้งไปยังลูกค้าเพื่อขอเปลี่ยนแปลงบัญชีในการรับชำระค่าสินค้าเป็นบัญชีของผู้ต้องหา ซึ่งอีเมลของคนร้ายใช้ชื่อว่า psilver@xxxinfor.com (เพิ่มอักษร “r”) ซึ่งเป็นอีเมลที่คนร้ายสร้างขึ้นมาให้คล้ายคลึงกับอีเมลที่แท้จริงของบริษัท Aเพื่อใช้หลอกลวงลูกค้าของบริษัท A ทำให้บริษัท A ได้รับความเสียหายเป็นราคาค่าสินค้า จำนวน 566,659 บาท โดยบริษัท A เชื่อว่าคนร้ายสามารถเจาะเข้าไปยังอีเมลของทางบริษัทได้ ทำให้ทราบข้อมูลการติดต่อระหว่างบริษัท A กับลูกค้า ซึ่งนอกจากค่าเสียหายในเชิงตัวเงินแล้ว บริษัท A ยังได้รับความเสียหายจากการขาดความน่าเชื่อถือจากการถูกจารกรรมข้อมูล ซึ่งลูกค้าที่ทราบเรื่องอาจไม่ไว้วางใจสั่งซื้อสินค้ากับทางบริษัท A

คดีนี้ พนักงานสอบสวนพบข้อขัดข้องในการแสวงหาข้อมูลว่าผู้ใดเป็นผู้เปิดใช้อีเมลที่มีการทำปลอมเลียนแบบขึ้นเนื่องจากข้อจำกัดว่าผู้ให้บริการอีเมลมีสถานประกอบการอยู่ในต่างประเทศ โดยคดีจึงมีการดำเนินการกับผู้เป็นเจ้าของบัญชีปลายทางที่รับโอนเงินค้าสินค้าเท่านั้น

2. คดีแฮกข้อมูลบัญชีธนาคารเพื่อลักเงิน(คำพิพากษาศาลอาญาธนบุรี คดีหมายเลขดำที่ 2957/2560 คดีหมายเลขแดงที่ 1519/2561, อัดสำเนา, 2561 : 1-9)

ข้อเท็จจริงโดยย่อของคดีนี้ เมื่อประมาณต้นเดือนมีนาคม 2559 คนร้ายได้แสวงหาจนได้มาซึ่ง User ID (ชื่อผู้ใช้) และ Password (รหัสผ่าน) สำหรับการใช้บริการ Internet Banking (ธนาคารบนอินเทอร์เน็ต) ของผู้เสียหายที่ 1 ซึ่งเป็นมารดา และของผู้เสียหายที่ 2 ซึ่งเป็นบุตรชายของผู้เสียหายที่ 1 ซึ่งต่างเป็นเจ้าของบัญชีเงินฝากธนาคารกรุงไทย จำกัด (มหาชน) อันถือได้ว่าเป็นการเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีการป้องกันการเข้าถึงโดยเฉพาะ (User ID และ Password ดังกล่าว) และมาตรการนั้นมิได้มีไว้สำหรับตน โดยการเข้าใช้งานในระบบ Internet Banking ลูกค้าต้องเข้าสู่ระบบอินเทอร์เน็ตผ่านเว็บไซต์ของธนาคารกรุงไทย จำกัด (มหาชน) จากนั้นใส่ User ID และ Password เพื่อเข้าสู่หน้าจอหลัก ในกรณีที่ยังไม่เคยมีการเพิ่มบัญชีปลายทางไว้จะต้องทำการเพิ่มบัญชีปลายทาง โดยกรอกหมายเลขบัญชีปลายทางที่ต้องการเพิ่ม จากนั้นระบบจะส่งรหัส TOP ทีโอพี (ทีโอพี) หรือ PIN (พิน) ซึ่งเป็นตัวเลข 6 หลักมายังเจ้าของบัญชีผ่านทางโทรศัพท์มือถือที่ลูกค้าได้ลงทะเบียนไว้กับธนาคาร เมื่อได้รับรหัส TOP แล้ว เจ้าของบัญชีจะต้องป้อนรหัส TOP ผ่านโทรศัพท์มือถือ หรือลงในเว็บไซต์ของธนาคารกรุงไทย จำกัด (มหาชน) เพื่อยืนยันการทำรายการภายในระยะเวลาที่กำหนดแล้วระบบจะโอนเงินไปยังบัญชีปลายทางโดยอัตโนมัติ แต่สำหรับกรณีผู้เสียหายทั้งสอง ก่อนเกิดเหตุเคยมีการโอนเงินระหว่างบัญชีเงินฝากของผู้เสียหายที่ 1 กับบัญชีเงินฝากของผู้เสียหายที่ 2 และระหว่างบัญชีเงินฝากของผู้เสียหายที่ 2 (ซึ่งมีมากกว่า 1 บัญชี) ดังนั้นถ้ามีการโอนเงินระหว่างบัญชีดังกล่าวอีก ธนาคารจะไม่ส่งรหัส TOP หรือ PIN ให้อีก ซึ่งคนร้ายได้ใช้ User ID และ Password ของผู้เสียหายที่ 1 เข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์บนระบบ Internet Banking แล้วนำเข้าด้วยการจัดส่งข้อมูลคอมพิวเตอร์อันเป็นเท็จเข้าสู่เว็บไซต์ของธนาคารกรุงไทย จำกัด (มหาชน) ทางอินเทอร์เน็ต ว่าผู้เสียหายที่ 1 มีความประสงค์จะโอนเงินจำนวน 100,000 บาท ไปเข้าบัญชีของผู้เสียหายที่ 2 ซึ่งความจริงแล้ว ผู้เสียหายที่ 1 ไม่ประสงค์โอนเงินดังกล่าว โดยคนร้ายได้ใช้ IP Address 171.6.224.3 ของจำเลย แล้วคนร้ายยังได้นำ User ID และ Password ของผู้เสียหายที่ 2 เข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์บนระบบ Internet Banking แล้วนำเข้าด้วยการจัดส่งข้อมูลคอมพิวเตอร์อันเป็นเท็จเข้าสู่เว็บไซต์ของธนาคารกรุงไทย จำกัด (มหาชน) ทางอินเทอร์เน็ต ว่าผู้เสียหายที่ 2 มีความประสงค์จะโอนเงิน จำนวน 50,000.10 บาท และ 49,995.10 บาท ไปเข้าบัญชีธนาคารของ นาง ก. ซึ่งเป็นบัญชีของห้างหุ้นส่วนจำกัดเว็บ

เพย์ซึ่งจำหน่ายบัตรเติมเงิน (ใช้แทนเงินสดในการชำระค่าซื้อสินค้าและบริการต่างๆ) โดยคนร้ายได้ใช้ IP Address 171.6.224.3 ของจำเลย

ในการสืบพยานฝ่ายโจทก์ นอกจากผู้เสียหายที่ 1 และผู้เสียหายที่ 2 ซึ่งมาเบิกความเป็นพยานเกี่ยวกับรูปคดีแล้ว พนักงานอัยการโจทก์ยังนำพนักงานฝ่ายกฎหมายของบริษัททริปเปิลทีอินเทอร์เน็ต จำกัด เป็นพยานเบิกความว่า เมื่อตรวจสอบข้อมูลจราจรคอมพิวเตอร์แล้วพบว่าช่วงวันเวลาเกิดเหตุ หมายเลข IP Address 171.6.224.3 ที่มีการสั่งโอนเงินมีจำเลยเป็นสมาชิกสมัครใช้บริการไว้ และยังได้ความจากกรรมการผู้จัดการห้างหุ้นส่วนจำกัดเว็บเพย์ เข้าเบิกความเป็นพยานว่าในวันเกิดเหตุได้มีรายการโอนเงินจำนวน 2 รายการ จากบัญชีของผู้เสียหายที่ 2 เข้าสู่บัญชีเงินฝากของ นาง ก. (ชื่อสมมติ) ซึ่งเป็นมารดาของตน โดยก่อนเกิดเหตุคดีนี้ ผู้เสียหายที่ 2 เป็นลูกค้าและสมาชิกของห้างหุ้นส่วนจำกัดเว็บเพย์ ดังนั้นพยานจึงดำเนินการเก็บข้อมูล IP Address ในช่วงเกิดเหตุ (IP Address 171.6.224.3) ส่งมอบให้กับพนักงานสอบสวนคดีนี้ นอกจากนี้พนักงานอัยการโจทก์ยังนำผู้อำนวยการฝ่ายอาวุโส ผู้บริหารฝ่าย ฝ่ายสนับสนุนช่องทางอิเล็กทรอนิกส์ของธนาคารกรุงไทย จำกัด(มหาชน) ซึ่งมีหน้าที่อำนวยการแก้ไขปัญหาเกี่ยวกับการใช้ระบบอิเล็กทรอนิกส์ต่างๆ ของระบบเอทีเอ็ม หรือระบบอินเทอร์เน็ตแบงค์กิ้ง เข้าเบิกความ โดยพยานยืนยันว่าในวันเวลาเกิดเหตุตรวจสอบการโอนเงินผ่านระบบ Internet Banking พบว่ามีผู้ใช้ IP Address 171.6.224.3 เป็นผู้ทำรายการโอนเงิน และสุดท้ายโจทก์มีพนักงานสอบสวนคดีนี้ เข้าเบิกความว่า เชื่อมโยงผลการสอบสวนจนพบว่า IP Address ที่คนร้ายใช้ในการกระทำความผิดคดีนี้มีจำเลยเป็นผู้สมัครใช้บริการอินเทอร์เน็ตไว้

จำเลยให้การปฏิเสธ สู้คดีทำนองว่า ในช่วงวันเวลาเกิดเหตุจำเลยไม่ได้ใช้เครื่องคอมพิวเตอร์หรืออินเทอร์เน็ตบ้านของจำเลยเพราะจำเลยไม่ได้อยู่บ้าน โดยจำเลยได้นำคณบดี คณะวิทยาการและเทคโนโลยีสารสนเทศ สถาบันการศึกษาแห่งหนึ่ง ซึ่งจบการศึกษาระดับปริญญาเอก คณะวิศวกรรมศาสตร์สาขา วิศกรรมอิเล็กทรอนิกส์ การไฟฟ้าและการสื่อสารเข้าเบิกความเป็นพยานสนับสนุนยืนยันว่า IP Address ที่ปรากฏแม้มีจำเลยเป็นเจ้าของจริง แต่ไม่สามารถบ่งบอกหรือยืนยันได้ว่าจำเลยเป็นผู้ใช้ อีกทั้งผู้อื่นก็สามารถเข้ามาใช้ได้หากรู้รหัสผ่าน IP Address สามารถเปลี่ยนแปลงกันได้ และไม่สามารถยืนยันได้ 100 เปอร์เซ็นต์ว่าผู้นั้นเป็นผู้ใช้จริง ตามปกติ User ID และ Password ของผู้ใช้เครื่องคอมพิวเตอร์หรือโทรศัพท์นั้นสามารถใช้วิธีการฟิชชิ่ง (Phishing)เพื่อให้ได้มาซึ่ง User ID และ Password ของผู้อื่นได้โดยใช้วิธีการสุ่ม

ศาลชั้นต้นพิเคราะห์แล้วเห็นว่า พนักงานสอบสวนไม่ได้ยึดเครื่องคอมพิวเตอร์ของจำเลยมาตรวจสอบการใช้งาน ดังนั้น ลำพังเพียง IP Address ที่ปรากฏชื่อจำเลยเป็นเจ้าของเพียงอย่างเดียว จึงมีน้ำหนักน้อยในการพิสูจน์ความผิดของจำเลย พยานหลักฐานที่โจทก์นำสืบยังมีข้อสงสัยตามสมควรว่าจำเลยกระทำความผิดตามฟ้องหรือไม่ ศาลให้ยกประโยชน์แห่งความสงสัยนั้นให้จำเลยตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 227 วรรคสอง

ในเรื่องนี้ เบญจพร วัชระวุฒิชัย (สัมภาษณ์, 2562) เห็นว่า คดีได้สะท้อนว่าพยานหลักฐานดิจิทัลมีความอ่อนไหวในเรื่องของความน่าเชื่อถือ โดยเฉพาะอย่างยิ่ง เมื่อข้อโต้แย้งของฝ่ายจำเลยเพิ่งถูกหยิบเข้าสู่การพิจารณาในชั้นศาล ซึ่งปัจจุบันศาลมิได้มีผู้เชี่ยวชาญด้านนิติคอมพิวเตอร์เป็นที่ปรึกษาเพื่อช่วยเหลือให้ความเห็นถึงความน่าเชื่อถือและโอกาสคลาดเคลื่อนของข้อเท็จจริงที่ฝ่ายจำเลย (หรือแม้แต่ฝ่ายโจทก์) ที่ได้นำสืบ โดยในกระบวนการพิจารณาคดีในศาลผลการตรวจพิสูจน์ซึ่งฝ่ายโจทก์ใช้อ้างอิงเป็นพยานหลักฐานมักจะจัดทำในรูปของเอกสาร โดยคู่ความอีกฝ่ายสามารถขอตรวจพยานหลักฐานเพื่อเตรียมคดีก่อนการสืบพยานได้ แต่ในส่วนของพยานจำเลย (ตามคดีดังกล่าวข้างต้น) หากใช้วิธีการนำพยานบุคคลซึ่งมีความเชี่ยวชาญเข้าเบิกความโดยมิได้แถลงประเด็นต่อสู้ไว้และมิได้จัดทำพยานเอกสารจัดส่งต่อศาลเพื่อให้ฝ่ายโจทก์ตรวจพยานหลักฐานก่อนสืบพยาน ย่อมมีลักษณะเป็นการจู่โจมทางพยานหลักฐานและเอาเปรียบทางคดี ซึ่งเป็นการยากที่พนักงานอัยการจะสามารถถามค้านเชิงวิชาการนิติคอมพิวเตอร์ได้ด้วยตนเองในขณะพิจารณาคดีทั้งที่ฝ่ายจำเลยควรต้องเป็นผู้มีหน้าที่ในการนำสืบพิสูจน์ให้รับฟังได้ว่าจำเลยถูกแอบอ้างใช้ IP Address โดยการถูกทำฟิชชิ่งว่าเกิดขึ้นเมื่อใดอย่างไรข้อต่อสู้ไม่ควรเป็นเพียงการคาดเดาความเป็นไปได้ ซึ่งหากจำเลยทราบประเด็นต่อสู้ดังกล่าวตั้งแต่ต้น และเมื่ออุปกรณ์คอมพิวเตอร์อยู่ในความครอบครองของจำเลยเอง หากจำเลยประสงค์จะต่อสู้ด้วยข้ออ้างที่ว่าจำเลยถูกทำฟิชชิ่งโดยบุคคลอื่นแล้วบุคคลอื่นได้ไปซึ่ง IP Address ของจำเลยแล้วไปใช้กระทำความผิดคดีนี้ อันเป็นข้อกล่าวอ้างใหม่ จำเลยควรมีหน้าที่ต้องนำสืบให้เห็นถึงความเป็นไปได้ของข้อกล่าวอ้างดังกล่าวด้วย และนอกจากพยานหลักฐานดิจิทัลแล้ว การดำเนินคดีอาชญากรรมคอมพิวเตอร์ควรให้ความสำคัญกับร่องรอยการกระทำความผิดอื่น เช่น เส้นทางการเงินที่คนร้ายได้ไปซึ่งเงินของผู้เสียหายโดยเฉพาะการใช้บัตรเติมเงินสดไปซื้อสินค้าหรือบริการด้วย

สรุป

การศึกษาในบทที่ 3 มีความมุ่งหมายเพื่อตอบวัตถุประสงค์การวิจัยข้อที่ 1 เพื่อศึกษาสภาพปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ที่พบในชั้นการสืบสวนสอบสวน รวบรวมพยานหลักฐาน จนถึงขั้นตอนการนำเสนอพยานหลักฐานในชั้นพิจารณาของศาลจากการทบทวนวรรณกรรมและบทบัญญัติกฎหมายเกี่ยวกับการรับฟังพยานหลักฐานในคดีอาญา ลักษณะและรูปแบบของอาชญากรรมคอมพิวเตอร์ที่พบมากในปัจจุบัน อำนาจหน้าที่ของเจ้าพนักงานในกระบวนการยุติธรรม และหลักกฎหมายที่สำคัญว่าด้วยเรื่องพยานหลักฐานในคดีอาญาที่กล่าวไว้ในบทที่ 2 ประสมประสานข้อมูลที่ได้จากการสัมภาษณ์เชิงลึกเจ้าพนักงานผู้ทรงคุณวุฒิด้านการสืบสวนสอบสวน การตรวจพิสูจน์ทางนิติคอมพิวเตอร์ และการดำเนินคดีอาชญากรรมคอมพิวเตอร์จากหน่วยงานภาครัฐหลากหลายแห่ง เช่น สำนักงานอัยการสูงสุด สำนักงานตำรวจแห่งชาติ และกรมสอบสวนคดีพิเศษ สะท้อนถึงอุปสรรคปัญหาหลายประการในการปฏิบัติงานภายใต้กรอบอำนาจหน้าที่ของตน ซึ่งครอบคลุมหน่วยงานในกระบวนการยุติธรรมทางอาญาที่เกี่ยวข้องในการดำเนินคดี

อาชญากรรมคอมพิวเตอร์อย่างครบวงจร พร้อมทั้งแบ่งปันประสบการณ์การดำเนินคดีตั้งแต่ชั้นของการสืบสวน เก็บรวบรวมพยานหลักฐาน พิสูจน์พยานหลักฐาน สรุปสำนวนการสอบสวน ไปจนถึงขั้นตอนการเบิกความและการพิจารณาคดีในชั้นศาล ผลการศึกษาที่ตอบวัตถุประสงค์การวิจัยข้อที่ 1 สรุปได้ดังนี้

ปัญหาที่พบในส่วนของการปฏิบัติหน้าที่เฉพาะบุคคล พบว่าสภาพปัญหาในเรื่องความรู้ความเข้าใจของผู้ปฏิบัติงานสืบสวนสอบสวน และพนักงานอัยการ ซึ่งขาดการอบรมความรู้ด้านเทคโนโลยีสมัยใหม่และองค์ความรู้ด้านนิติคอมพิวเตอร์เบื้องต้น ในส่วนของผู้ตรวจพิสูจน์หลักฐานซึ่งเป็นผู้มีความรู้ด้านนิติคอมพิวเตอร์แต่ยังขาดงบประมาณเพื่อจัดหาเครื่องมืออุปกรณ์ที่ใช้ตรวจสอบอุปกรณ์ดิจิทัลที่สมัยให้เพียงพอต่อปริมาณงานอีกทั้งซอฟท์แวร์ที่ใช้ในการปฏิบัติงานมักมีราคาสูงและต้องนำเข้าจากต่างประเทศ รวมถึงจำนวนผู้ตรวจพิสูจน์นิติคอมพิวเตอร์ของหน่วยงานภาครัฐที่มีไม่เพียงพอต่อปริมาณงานอาชญากรรมคอมพิวเตอร์ในปัจจุบัน ทำให้การตรวจพิสูจน์เกิดความล่าช้า ในด้านการอธิบายพยานหลักฐานดิจิทัลในรูปของการรายงานผลการตรวจพิสูจน์หรือการเบิกความในชั้นศาลพบอุปสรรคในเรื่องของคำศัพท์ทางคอมพิวเตอร์ซึ่งบุคลากรในกระบวนการยุติธรรมยังขาดความคุ้นเคย และประการสำคัญคือความกังวลของเจ้าพนักงานในความไม่ชัดเจนเกี่ยวกับอำนาจในการรวบรวมพยานหลักฐานดิจิทัลอันเนื่องมาจากพัฒนาการของเทคโนโลยีสมัยใหม่ที่ข้อมูลคอมพิวเตอร์ของบุคคลมิได้จัดเก็บอยู่ในตัวอุปกรณ์ดิจิทัลเพียงอย่างเดียว เช่น การเก็บข้อมูลในระบบคลาวด์ หรือการใช้วิธีการฟิชชิ่งเพื่อให้ได้มาซึ่งรหัสผ่านระบบคอมพิวเตอร์ของคนร้ายซึ่งอาจนำไปสู่ข้อโต้แย้งเกี่ยวกับการรับฟังพยานหลักฐานในอนาคต

ปัญหาที่พบในส่วนของการปฏิบัติหน้าที่สัมพันธ์กับบุคลากรอื่น พบว่า ในส่วนของพนักงานสอบสวนและผู้ตรวจพิสูจน์พยานหลักฐานขาดการประสานงานที่เหมาะสมในการกำหนดประเด็นการแสวงหาพยานหลักฐานดิจิทัล โดยการประสานงานด้วยเอกสารหนังสือเพียงอย่างเดียวก่อให้เกิดความไม่ชัดเจนเกี่ยวกับวัตถุประสงค์ของการตรวจสอบเนื่องจากพนักงานสอบสวนมักคุ้นเคยในเรื่องทางนิติศาสตร์แต่ยังขาดความเข้าใจถึงคุณค่าของพยานหลักฐานดิจิทัลแต่ละชิ้นจึงพบข้อขัดข้องในการกำหนดประเด็นตรวจสอบไปยังผู้ตรวจพิสูจน์ นอกจากนี้ เจ้าพนักงานยังพบข้อขัดข้องจากการไม่ได้รับความร่วมมือจากผู้ให้บริการอินเทอร์เน็ต ผู้ให้บริการเว็บไซต์ และผู้ให้บริการด้านการเงินการธนาคาร หรือได้รับผลการดำเนินการตามที่ร้องขอในเวลาที่ล่าช้าเกินสมควร

ทั้งนี้ปัญหาและอุปสรรคที่กล่าวไว้ข้างต้นจะถูกนำไปวิเคราะห์เพื่อหาแนวทางแก้ไขและแนวทางเพิ่มประสิทธิภาพในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในบทที่ 4 ต่อไป

บทที่ 4
วิเคราะห์ปัจจัยที่ก่อให้เกิดสภาพปัญหาและอุปสรรค ในการดำเนินคดีอาชญากรรมคอมพิวเตอร์

บุคลากรในกระบวนการยุติธรรมทางอาญาได้แก่ เจ้าพนักงานสืบสวนพนักงานสอบสวน ผู้ตรวจพิสูจน์หลักฐาน และพนักงานอัยการ ต่างประสบปัญหาและอุปสรรคในการปฏิบัติหน้าที่เกี่ยวกับการดำเนินคดีอาชญากรรมคอมพิวเตอร์ทั้งที่คล้ายคลึงกันและแตกต่างกันดังที่ได้กล่าวมาแล้วในบทที่ 3 โดยปัญหาและอุปสรรคที่หลากหลายต่างเชื่อมโยงนำไปสู่ข้อขัดข้องที่ทำให้การดำเนินคดีอาชญากรรมคอมพิวเตอร์ยังไม่มีประสิทธิภาพเท่าที่ควร การศึกษาในบทที่ 4มีความมุ่งหมายเพื่อตอบวัตถุประสงค์การวิจัยข้อที่ 2เพื่อวิเคราะห์ปัจจัยที่ก่อให้เกิดสภาพปัญหาและอุปสรรคในการเนินคดีอาชญากรรมคอมพิวเตอร์ในปัจจุบันและเพื่อตอบวัตถุประสงค์การวิจัยข้อที่ 3เพื่อเสนอแนะแนวทางเพิ่มประสิทธิภาพการดำเนินคดีอาชญากรรมคอมพิวเตอร์โดยมีลำดับการศึกษาดังนี้

1. ปัจจัยด้านบุคลากรที่เกี่ยวข้อง
2. ปัจจัยด้านนิติคอมพิวเตอร์
3. ปัจจัยด้านความร่วมมือระหว่างผู้ปฏิบัติงาน
4. ปัจจัยด้านบทบัญญัติกฎหมาย
5. แนวทางการพัฒนาประสิทธิภาพการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในต่างประเทศที่น่าสนใจ
6. แนวทางเพิ่มประสิทธิภาพการดำเนินคดีอาชญากรรมคอมพิวเตอร์
7. สรุป

ปัจจัยด้านบุคลากรที่เกี่ยวข้อง

จากการสัมภาษณ์เชิงลึกเจ้าพนักงานทุกกลุ่มงานที่เกี่ยวข้องกับการดำเนินคดีอาชญากรรมคอมพิวเตอร์พบสภาพปัญหาหลัก คือ ผู้ปฏิบัติงานที่มีความรู้ความเข้าใจด้านนิติคอมพิวเตอร์ยังมีไม่เพียงพอกับปริมาณงานอาชญากรรมคอมพิวเตอร์ในปัจจุบัน(นิติ อินทลักษณ์, สัมภาษณ์, 2562 ; เบญจพร วัชระวุฒิชัย, สัมภาษณ์, 2562 ; ปกรณ์ ธรรมโรจน์, สัมภาษณ์, 2562 ; ปฏิภาณ ยืนทนต์, สัมภาษณ์, 2562 ; ปัญจะ ผลโต, สัมภาษณ์, 2562 ; เผ่าภูมิ สมหมาย, สัมภาษณ์, 2562 ; วันทนีย์ ตุลยเสวี, สัมภาษณ์, 2562 ; อัศว์ณุต แสงทองดี, สัมภาษณ์, 2562) สาเหตุของสภาพปัญหาสามารถจัดแบ่งได้เป็น 2 ประการ คือ

1. สาเหตุจากจำนวนผู้ปฏิบัติงานไม่เพียงพอ

เจ้าพนักงานผู้ตรวจพิสูจน์พยานหลักฐานทางคอมพิวเตอร์เห็นว่าปัญหาเรื่องของจำนวนผู้ตรวจพิสูจน์ทางนิติคอมพิวเตอร์ที่มีไม่เพียงพอเป็นปัญหาหลักที่ต้องเผชิญอยู่ในปัจจุบัน (กชกรเพิงระนัย, สัมภาษณ์, 2562 ; นิติ อินทลักษณ์, สัมภาษณ์, 2562 ; วันทนีย์ ตุลยเสวี, สัมภาษณ์, 2562 ; อัศว์ณุต แสงทองดี, สัมภาษณ์, 2562)ข้อมูลที่น่าสนใจจากพันตำรวจโทอัศว์ณุต แสงทองดี (สัมภาษณ์, 2562) พบว่า ในปัจจุบันนักวิทยาศาสตร์ที่ผ่านงานตามกำหนดระยะเวลาที่กองพิสูจน์หลักฐาน สำนักงานตำรวจแห่งชาติกำหนดเท่านั้นที่จะสามารถลงชื่อเป็นผู้จัดทำรายงานการตรวจพิสูจน์อย่างเป็นทางการในนามของกองพิสูจน์หลักฐาน ดังนั้นผลตรวจพิสูจน์หลักฐานทางนิติคอมพิวเตอร์จากผู้ตรวจพิสูจน์ชั้นปฏิบัติงานส่วนใหญ่จะถูกส่งต่อไปยังผู้ตรวจพิสูจน์หลักฐานที่มีคุณสมบัติครบถ้วนเพื่อจัดทำรายงานผลการตรวจพิสูจน์ ซึ่งทั่วประเทศมีผู้ตรวจพิสูจน์หลักฐานที่สามารถเป็นผู้จัดทำรายงานผลการตรวจพิสูจน์เพียงหลักสิบคนเท่านั้น ทำให้ปริมาณงานของผู้ตรวจพิสูจน์ที่มีคุณสมบัติสามารถเป็นผู้จัดทำรายงานผลการตรวจพิสูจน์มีค่อนข้างมาก อีกทั้งยังถูกจำกัดด้วยกรอบระยะเวลาการดำเนินงานและเครื่องมืออุปกรณ์ที่มีอยู่อย่างจำกัด ทำให้ผู้ตรวจพิสูจน์แต่ละคนต้องรีบเร่งดำเนินการทั้งที่การตรวจพิสูจน์ทางนิติคอมพิวเตอร์ต้องใช้ความละเอียดรอบคอบเพื่อให้ได้ข้อตรวจพบที่เป็นประโยชน์ต่อรูปคดีมากที่สุด หากมีภาระงานไม่สัมพันธ์กับกรอบระยะเวลาการตรวจพิสูจน์อาจส่งผลให้กรอบการตรวจพิสูจน์ถูกจำกัดเฉพาะประเด็นที่มีการร้องขอให้ตรวจโดยพนักงานสอบสวน แต่ไม่มีเวลาพอที่จะตรวจขยายผลเพื่อหาร่องรอยพยานหลักฐานอย่างอื่นเพิ่มเติม

2. สาเหตุจากการที่ผู้ปฏิบัติงานมีความรู้ไม่เพียงพอ

เจ้าพนักงานแต่ละส่วนงานมีหน้าที่ความรับผิดชอบในงานที่แตกต่างกัน เมื่อได้พิเคราะห์เกี่ยวกับอำนาจหน้าที่ของเจ้าพนักงานกลุ่มต่างๆในกระบวนการยุติธรรมทางอาญาตามที่ได้ทบทวนในบทที่ 2 แล้ว ผู้วิจัยเห็นว่าสามารถจำแนกความรู้ที่เจ้าพนักงานกลุ่มต่างๆในกระบวนการยุติธรรมทางอาญาต้องการสำหรับการปฏิบัติงานออกเป็น 2 ระดับ ดังนี้

2.1ความรู้ระดับหลัก

ได้แก่ ความรู้ความเข้าใจพื้นฐานเฉพาะทางที่จำเป็นต่อการปฏิบัติงานเฉพาะกลุ่มโดยตรง หากขาดความรู้ความเข้าใจในส่วนนี้ จะส่งผลกระทบต่อการปฏิบัติหน้าที่โดยตรง ซึ่งความรู้ในระดับนี้มีความแตกต่างกันออกไปตามบทบาทหน้าที่ของแต่ละกลุ่มตามที่ได้ศึกษามาในบทที่ 2 กล่าวคือ กลุ่มของผู้ตรวจพิสูจน์หลักฐานซึ่งเป็นผู้ปฏิบัติงานในกรอบของพยานหลักฐานดิจิทัลย่อมจะต้องมีความรู้ความชำนาญในแนวทางของ“นิติคอมพิวเตอร์” (Computer Forensics) โดยสามารถใช้ความรู้ทางด้านการรักษาความปลอดภัยของข้อมูลและระบบสารสนเทศ (Information Security)และเจาะลึกในการพิสูจน์หลักฐานทางคอมพิวเตอร์ หรือนิติคอมพิวเตอร์ซึ่งหมายถึง การแสวงหาการเก็บรักษาการวิเคราะห์และการนำเสนอพยานหลักฐานที่เกี่ยวกับคอมพิวเตอร์(ปริญญา หอมอเนก, ออนไลน์,

2562) ศาสตร์เรื่องนิติคอมพิวเตอร์นับเป็นความรู้ขั้นสูงทางด้าน Information Security โดยการรวบรวมและเก็บพยานหลักฐานที่อยู่ในรูปของข้อมูลดิจิทัลจำเป็นต้องกระทำโดยผู้ที่มีความเชี่ยวชาญทางด้านนิติคอมพิวเตอร์โดยเฉพาะ มิฉะนั้นข้อมูลที่มีค่าอาจสูญหายไปด้วยความรู้เท่าไม่ถึงการณ์ซึ่งความรู้ในส่วนนี้ยังคงมีความเปลี่ยนแปลงไปตามเทคโนโลยีที่มีการพัฒนาอย่างต่อเนื่องไม่หยุดนิ่ง

ในขณะที่ความรู้ระดับหลักที่กลุ่มเจ้าหน้าที่สืบสวนและพนักงานสอบสวนมีความต้องการได้แก่ความรู้ทางกฎหมายเกี่ยวกับอำนาจของเจ้าพนักงานในการรวบรวมพยานหลักฐานเพื่อให้พยานหลักฐานที่รวบรวมมาในสำนวนการสอบสวนนั้นเป็นพยานหลักฐานที่เกิดขึ้นและได้มาโดยชอบด้วยกฎหมาย อันจะทำให้พยานหลักฐานชิ้นนั้นเป็นพยานหลักฐานที่ศาลสามารถรับฟังได้ตามกฎหมายรวมไปถึงความรู้เกี่ยวกับเทคโนโลยีด้านคอมพิวเตอร์ การสื่อสารและการเงินสมัยใหม่เพื่อให้สามารถรวบรวมพยานหลักฐานที่สามารถเชื่อมโยงตัวบุคคลผู้กระทำความผิดอาชญากรรมคอมพิวเตอร์ เนื่องจากพยานหลักฐานดิจิทัลนั้นมีความอ่อนไหว เปลี่ยนแปลง และอาจมีข้อโต้แย้งในเชิงเทคนิคในการยืนยันตัวบุคคล ดังที่ปรากฏในตัวอย่างคดีปลอมอีเมลแก้ไขข้อมูลเพื่อลักเงิน และคดีแฮกข้อมูลบัญชีธนาคารเพื่อลักเงินที่ได้กล่าวไว้ในบทที่ 3 ซึ่งสะท้อนให้เห็นว่า คดีอาชญากรรมคอมพิวเตอร์นั้นไม่อาจอาศัยเพียงพยานหลักฐานทางดิจิทัล หรือพยานหลักฐานทางอิเล็กทรอนิกส์ในการพิสูจน์ความผิดของผู้ถูกกล่าวหาเพียงอย่างเดียว แต่พยานหลักฐานแวดล้อมอย่างอื่น เช่น เส้นทางการเงิน การทำธุรกรรมทางการเงิน ข้อมูลการเชื่อมต่อการสื่อสารทางโทรศัพท์ หรือแม้แต่ข้อมูลแวดล้อมเชิงพฤติกรรมของผู้ถูกกล่าวหา ล้วนเป็นพยานแวดล้อมที่สำคัญที่ควรให้ความสำคัญไม่ยิ่งหย่อนไปกว่าพยานหลักฐานทางดิจิทัล

ในส่วนของพนักงานอัยการ องค์ความรู้ระดับหลักจะค่อนข้างคล้ายคลึงกับกลุ่มเจ้าหน้าที่สืบสวนและพนักงานสอบสวน โดยพนักงานอัยการควรได้รับการอบรมความรู้เกี่ยวกับระบบการทำงานโดยรวมของอุปกรณ์คอมพิวเตอร์ และอุปกรณ์ดิจิทัลอื่นๆ เช่น โทรศัพท์เคลื่อนที่หรือกล้องวงจรปิด เช่นกัน เพื่อให้เกิดความเข้าใจภาพรวมของพยานหลักฐานดิจิทัลที่สามารถดำเนินการรวบรวม คุณค่าเชิงพิสูจน์ รวมถึงจุดอ่อนที่อาจถูกหยิบยกเป็นข้อต่อสู้ในชั้นพิจารณา เพื่อที่พนักงานอัยการจะได้สามารถประเมินน้ำหนักของพยานหลักฐานในสำนวนการสอบสวนว่ามีเพียงพอที่จะฟ้องคดีหรือไม่ และหากพนักงานอัยการเห็นว่าพยานหลักฐานจากการสอบสวนยังไม่เพียงพอที่จะพิสูจน์การกระทำความผิดของผู้ถูกกล่าวหา ก็จะต้องมีคำสั่งให้พนักงานสอบสวนทำการสอบสวนเพิ่มเติม โดยพนักงานอัยการต้องเป็นผู้กำหนดประเด็นการสอบสวนเพิ่มเติม ดังนั้น พนักงานอัยการจึงต้องมีความรู้ความเข้าใจเกี่ยวกับสภาพของพยานหลักฐานทางดิจิทัลรวมถึงข้อมูลเกี่ยวกับพยานแวดล้อมดีพอสมควร นอกจากนั้นแล้ว พนักงานอัยการซึ่งมีหน้าที่ต้องนำเสนอพยานหลักฐานในชั้นพิจารณาต้องมีความรู้ความเข้าใจเกี่ยวกับกฎหมายพยานหลักฐานของไทยเป็นอย่างดีว่าพยานหลักฐานแต่ละชิ้นจัดเป็นพยานหลักฐานประเภทใด ต้องใช้วิธีการในการนำสืบอย่างไร พยานแต่

ละชิ้นนั้นเกิดและได้มาโดยชอบหรือไม่ พยานหลักฐานใดมีน้ำหนักรับฟังได้มากหรือน้อย และพยานหลักฐานชิ้นใดที่เป็นพยานหลักฐานชิ้นหลักในคดี และจะต้องมีพยานแวดล้อมสนับสนุนมากน้อยเพียงใด เพื่อให้ศาลรับฟังโดยปราศจากเหตุสงสัยตามสมควร (Proof Beyond Reasonable Doubt) ว่าจำเลยเป็นผู้กระทำความผิดตามข้อหาที่ฟ้องจริง

2.2ความรู้ระดับรอง

นอกจากความรู้ระดับหลักที่เกี่ยวข้องกับการปฏิบัติหน้าที่เฉพาะหน่วยงานของตนแล้ว เจ้าพนักงานในกระบวนการยุติธรรมทางอาญามีความจำเป็นต้องเข้าใจถึงบทบาท และอำนาจหน้าที่ของเจ้าพนักงานอื่นๆในกระบวนการยุติธรรมทางอาญาเช่นกัน เนื่องจากในการดำเนินคดีอาชญากรรมคอมพิวเตอร์แต่ละคดีนั้น เริ่มต้นจากเจ้าพนักงานสืบสวนที่ต้องแสวงหาข้อมูลเบื้องต้นเพื่อให้ทราบว่ามีการกระทำความผิดใดเกิดขึ้น มีพฤติการณ์เบื้องต้นอย่างไร และมีผู้ใดเป็นผู้ต้องสงสัยว่าเป็นผู้กระทำความผิด ส่งต่อผลการดำเนินการของตนซึ่งอาจอยู่ในรูปของรายงานสืบสวน บันทึกการสืบสวน ภาพถ่ายประกอบคดี ข้อมูลที่ได้รับจากหน่วยงานภายนอก ให้กับพนักงานสอบสวนเพื่อดำเนินการสอบสวนเชิงลึก สอบคำให้การพยานบุคคลที่เกี่ยวข้อง ส่งของกลางที่ยึดได้ไปให้ผู้ตรวจพิสูจน์พยานหลักฐานทำการตรวจพิสูจน์มีความเห็น รวมถึงขอความร่วมมือไปยังผู้ให้บริการโทรศัพท์เคลื่อนที่ ผู้ให้บริการอินเทอร์เน็ต รวมถึงสถาบันการเงิน เพื่อขอข้อมูลการให้บริการที่เกี่ยวข้องกับคดี แล้วนำผลการสอบสวนที่ได้รับมาพิจารณาสรุปสำนวนว่าจากพยานหลักฐานที่รวบรวมได้นั้นสามารถเชื่อมโยงพิสูจน์การกระทำความผิดของผู้ต้องหาได้หรือไม่อย่างไร แล้วมีความเห็นว่าควรสั่งฟ้องหรือควรสั่งไม่ฟ้องผู้ต้องหาตามฐานความผิดที่ได้แจ้งข้อหาแก่ผู้ต้องหาในชั้นสอบสวน ด้านของผู้ตรวจพิสูจน์หลักฐาน มีหน้าที่ต้องแสวงหาร่องรอยหลักฐานจากของกลางที่ได้รับไว้ตรวจ และลงความเห็นตามประเด็นที่พนักงานสอบสวนกำหนดขอความร่วมมือมา จากนั้นพนักงานสอบสวนจะส่งสำนวนการสอบสวนพร้อมความเห็นไปให้พนักงานอัยการพิจารณาว่าคดีมีพยานหลักฐานพอฟ้องหรือไม่ โดยพนักงานอัยการเปรียบเสมือนนักวิ่งผลัดไม้สุดท้ายที่ต้องวิเคราะห์ข้อเท็จจริงที่ได้จากการสอบสวน รวมทั้งพิเคราะห์พยานหลักฐานในคดี ข้อกฎหมายที่เกี่ยวกับองค์ประกอบความผิดที่มีการกล่าวหา ข้อกฎหมายเกี่ยวกับอำนาจการสอบสวน และข้อกฎหมายที่เกี่ยวข้องกับพยานหลักฐาน จากนั้นเมื่อเห็นว่าคดีมีพยานหลักฐานพอฟ้องแล้ว พนักงานอัยการจะดำเนินการยื่นฟ้องผู้ต้องหาเป็นจำเลยต่อศาล ภายหลังจากนั้น พนักงานอัยการก็มีหน้าที่ในการดำเนินคดีในชั้นศาลเพื่อนำเสนอพยานหลักฐานในคดีเข้าสู่กระบวนการพิจารณาจนคดีถึงที่สุดด้วย

ดังนั้น ประสิทธิภาพในการดำเนินคดีอาชญากรรมคอมพิวเตอร์แต่ละเรื่องขึ้นอยู่กับประสิทธิภาพในการปฏิบัติงานของเจ้าพนักงานทุกๆหน่วยงานในกระบวนการยุติธรรมทางอาญาเปรียบเสมือนเป็นห่วงโซ่การดำเนินการซึ่งต้องอาศัยความร่วมมือและความเข้าใจในภาพรวมของการดำเนินคดีเพื่อที่งานในส่วนของตนจะถูกส่งต่อหรือนำไปใช้โดยหน่วยงานในกระบวนการยุติธรรมแห่ง

อื่นได้อย่างมีประสิทธิภาพ ดังนั้น นอกจากความรู้ระดับหลักแล้ว เจ้าพนักงานผู้ปฏิบัติงานยังต้องมีความรู้ระดับรอง อันได้แก่ ความเข้าใจในบทบาทของหน่วยงานยุติธรรมอื่นที่หน่วยงานของตนต้องมีการประสานงาน และความเข้าใจว่างานในส่วนที่ตนเองเป็นผู้ดำเนินการนั้น มีคุณค่าอย่างไร และจะถูกนำไปใช้ในกระบวนการดำเนินคดีได้อย่างไร ซึ่งจากการสัมภาษณ์เชิงลึกพบว่า การปฏิบัติงานระหว่างผู้ตรวจพิสูจน์พยานหลักฐานกับพนักงานสอบสวน พบปัญหาในเชิงของการประสานงานอย่างมาก (กชกร เพิงระนัย, สัมภาษณ์, 2562; ชานนท์ คำนวนศักดิ์, สัมภาษณ์, 2562; นิติ อินทลักษณ์, สัมภาษณ์, 2562; วันทนีย์ ตุลยเสวี, สัมภาษณ์, 2562)กล่าวคือ เมื่อพนักงานสอบสวนส่งของกลางคดีอาญาได้แก่ อุปกรณ์คอมพิวเตอร์ โทรศัพท์เคลื่อนที่ หรือกล้องวงจรปิด ไปให้ผู้ตรวจพิสูจน์พยานหลักฐานเพื่อทำการแสวงหาร่องรอยพยานหลักฐานจากของกลาง พนักงานสอบสวนส่วนใหญ่มีความรู้ความเข้าใจเกี่ยวกับระบบคอมพิวเตอร์ที่ค่อนข้างน้อย และไม่เข้าใจขอบเขตงานที่ผู้ตรวจพิสูจน์สามารถลงความเห็นในรายงานการตรวจพิสูจน์ ซึ่งผู้ตรวจพิสูจน์โดยมากมักจะลงความเห็นเฉพาะข้อตรวจพบซึ่งเป็นข้อเท็จจริงเท่านั้น ดังนั้นในกรณีที่พนักงานสอบสวนระบุวัตถุประสงค์ที่ต้องการให้ตรวจพิสูจน์ด้วยข้อความปลายเปิดหรือคำถามอย่างกว้างๆ เป็นเหตุให้ผู้ตรวจพยานหลักฐานพบปัญหาความไม่ชัดเจนของขอบเขตการดำเนินงานดังที่ได้กล่าวไว้ในบทที่ 3 ในทางกลับกัน จากการสัมภาษณ์เชิงลึกพบว่าผู้ตรวจพิสูจน์พยานหลักฐานมีความรู้ความเข้าใจเกี่ยวกับกฎหมายพยานหลักฐานและกระบวนการพิจารณาในคดีในศาลค่อนข้างน้อย ทำให้ผลการตรวจพิสูจน์ที่กล่าวถึงเฉพาะข้อตรวจพบซึ่งเป็นข้อเท็จจริง โดยมิได้อธิบายขยายความเพิ่มเติมถึงโอกาสในการเกิดความคลาดเคลื่อนของข้อตรวจพบ (เช่น หมายเลขไอพีแอดเดรส) ที่จะใช้เป็นข้อมูลหลักในการพิสูจน์การกระทำความผิดของจำเลยนอกจากนี้ หากผู้ตรวจพิสูจน์เองไม่ได้รับทราบพฤติการณ์เบื้องต้นแห่งคดีก็จะขาดความเข้าใจในวัตถุประสงค์แห่งการตรวจพิสูจน์และทำให้ในบางครั้งขาดโอกาสที่จะแสวงหาพยานแวดล้อมที่เกี่ยวข้องที่อาจปรากฏอยู่ในตัวของกลาง เช่น ร่องรอยว่าอุปกรณ์คอมพิวเตอร์ดังกล่าวเคยมีการใช้เข้าเยี่ยมชมเว็บไซต์ใดมากเป็นพิเศษในช่วงเวลาก่อนเกิดเหตุ ซึ่งจะสะท้อนพฤติกรรมและความสนใจของผู้ใช้งานรวมไปถึงโปรแกรมหรือแอพพลิเคชั่นเฉพาะบางอย่างซึ่งมักพบว่าถูกนำไปใช้ในการกระทำความผิดที่ผู้เป็นเจ้าของดาวน์โหลดเพื่อใช้งานเพื่อเป็นข้อมูลประกอบให้เห็นพฤติกรรมของผู้เป็นเจ้าของอุปกรณ์อิเล็กทรอนิกส์ของกลางที่อาจรับฟังประกอบทำให้พยานหลักฐานในส่วนอื่นมีความน่าเชื่อถือรับฟังได้อย่างหนักแน่นมั่นคง (เบญจพร วัชระวุฒิชัย, สัมภาษณ์, 2562)

นอกจากนี้ การขาดองค์ความรู้ระดับรองนี้สะท้อนได้จากปัญหาเกี่ยวกับการใช้คำศัพท์หรือรูปประโยคภาษาอังกฤษที่เกี่ยวข้องที่ปรากฏในรายงานผลการตรวจพิสูจน์ซึ่งคำศัพท์หรือรูปประโยคผู้ตรวจพิสูจน์เลือกใช้ในงานซึ่งเป็นคำศัพท์ที่เป็นที่คุ้นเคยกันในวงการนิติคอมพิวเตอร์หรือปรากฏอยู่ในพจนานุกรมคอมพิวเตอร์ แต่อาจไม่สอดคล้องกับความหมายที่บุคคลทั่วไปเข้าใจกันและไม่สะท้อนกับคำซึ่งเป็นองค์ประกอบของกฎหมายที่เป็นทางการ ทำให้เกิดปัญหา

ความเข้าใจในการอ่านรายงานการตรวจพิสูจน์และการนำข้อมูลที่ปรากฏไปใช้นำเสนอในชั้นพิจารณาคดี (ดรัณ จาดเจริญ, สัมภาษณ์, 2562 ; เบญจพร วัชระวุฒิชัย, สัมภาษณ์, 2562 ; วันทนีย์ ตุลยเสวี, สัมภาษณ์, 2562)ดังนั้น หากพนักงานสอบสวนและพนักงานอัยการขาดความเข้าใจลักษณะความหมายของถ้อยคำที่ใช้ในผลการตรวจพิสูจน์อาจส่งผลให้พนักงานสอบสวนและพนักงานอัยการไม่ทราบประเด็นที่ควรต้องมีการสอบสวนเพิ่มเติมขยายความจากผลการตรวจพิสูจน์นั้น และยังอาจส่งผลให้เกิดความคลาดเคลื่อนในการอ้างอิงในชั้นพิจารณาและสุ่มเสี่ยงต่อการโต้แย้งของฝ่ายจำเลยได้

ปัจจัยด้านนิติคอมพิวเตอร์

จากการสัมภาษณ์เชิงลึกผู้ตรวจพิสูจน์หลักฐานพบสภาพปัญหาหลากหลายประการในการปฏิบัติงานด้านการตรวจพิสูจน์พยานหลักฐานดิจิทัลประเภทต่างๆ เช่น อุปกรณ์คอมพิวเตอร์ โทรศัพท์สมาร์ทโฟน กล้องบันทึกภาพวงจรปิด ดังที่กล่าวไว้ในบทที่ 3 สามารถจัดแบ่งสาเหตุของปัญหาได้ 2 ประการ คือ

1. ความไม่เพียงพอของเครื่องมืออุปกรณ์ และซอฟท์แวร์ที่ใช้ในการตรวจพิสูจน์

ผู้ตรวจพิสูจน์ที่ให้สัมภาษณ์เชิงลึกทุกราย (กชกร เพิงระนัย, สัมภาษณ์, 2562 ; ชานนท์ คำนวนศักดิ์, สัมภาษณ์, 2562) มีความเห็นในทำนองเดียวกันว่า ในปัจจุบันเครื่องมือและซอฟท์แวร์ที่ใช้ในการตรวจพิสูจน์พยานหลักฐานดิจิทัลที่มีข้อมูลมาตรฐานสากลรองรับนั้นส่วนใหญ่จะต้องนำเข้าจากต่างประเทศ เป็นผลิตภัณฑ์ของบริษัทที่มีชื่อเสียงในต่างประเทศซึ่งมักมีประเด็นเรื่องทรัพย์สินทางปัญญา (ลิขสิทธิ์) โดยต้องเสียค่าใช้จ่ายเพื่อให้ได้รับอนุญาตในการใช้ซอฟท์แวร์ภายในระยะเวลาที่ผู้ผลิตกำหนดเท่านั้น (Commercial Software) ซึ่งซอฟท์แวร์ที่ผู้ตรวจพิสูจน์ต้องใช้ในงานตรวจพิสูจน์มิใช่ผลิตภัณฑ์ที่ทำการจัดซื้อแล้วจะสามารถใช้งานได้อย่างสมบูรณ์ชั่วระยะเวลานานตลอดไปอย่างเช่นครุภัณฑ์ทั่วไป แต่ซอฟท์แวร์เหล่านี้ต้องการการอัพเดทให้เป็นเวอร์ชั่นปัจจุบันที่มีการปรับปรุงเพื่อให้สอดคล้องกับเทคโนโลยีของอุปกรณ์ดิจิทัล ซึ่งการอัพเดทซอฟท์แวร์หรือการต่ออายุลิขสิทธิ์ใช้งานย่อมเกิดค่าใช้จ่ายที่เกี่ยวข้องด้วย โดยเครื่องมือในการตรวจพิสูจน์และซอฟท์แวร์ที่ใช้ในการตรวจพิสูจน์พยานหลักฐานดิจิทัลมีความจำเป็นอย่างยิ่งยวดต่องานตรวจพิสูจน์หลักฐานทางนิติคอมพิวเตอร์ในคดีอาชญากรรมคอมพิวเตอร์ที่มีความซับซ้อนทางเทคนิค ทั้งกลุ่มความผิดที่คอมพิวเตอร์เป็นวัตถุหรือเป้าหมายที่ถูกกระทำ เช่น การแฮก ดีดอส และสแปม กลุ่มของความผิดที่คอมพิวเตอร์ถูกใช้เป็นเครื่องมือประกอบอาชญากรรมอย่างอื่นและกลุ่มที่มีการใช้คอมพิวเตอร์เป็นเครื่องมือจัดการผลประโยชน์ที่ได้จากอาชญากรรมอื่น จึงเป็นความท้าทายในเชิง

งบประมาณในการจัดหาและบริหารการใช้เครื่องมืออุปกรณ์และซอฟท์แวร์สำหรับงานตรวจพิสูจน์หลักฐานทางดิจิทัลเหล่านี้ในอนาคต

2. การเลือกใช้ซอฟท์แวร์เพื่อการตรวจพิสูจน์โดยผู้ตรวจพิสูจน์ที่แตกต่างกัน

สืบเนื่องมาจากปัจจัยความไม่เพียงพอของเครื่องมืออุปกรณ์และซอฟแวร์สำหรับงานตรวจพิสูจน์หลักฐานทางดิจิทัล โดยเฉพาะซอฟท์แวร์ซึ่งมีค่าลิขสิทธิ์ในการใช้ที่มักมีกำหนดระยะเวลาการอนุญาตให้ใช้งานเพียงระยะเวลาสั้นๆเช่น 2 ปี จึงนำไปสู่การแก้ไขปัญหาเฉพาะหน้าด้วยการดาวน์โหลดซอฟท์แวร์ฟรีที่ไม่มีค่าใช้จ่าย (Free Software)จากแหล่งข้อมูลเปิดมาใช้ประกอบการตรวจพิสูจน์ ในเรื่องนี้ ชานนท์ คำนวณศักดิ์ (สัมภาษณ์, 2562) ได้อธิบายเพิ่มเติมว่า ซอฟท์แวร์ที่ผู้ตรวจพิสูจน์ดาวน์โหลดมาจากแหล่งข้อมูลเปิดซึ่งไม่มีค่าใช้จ่ายนั้น มีทั้งที่เป็นซอฟท์แวร์ที่ใช้ทำการตรวจพิสูจน์ในงานทดแทนซอฟท์แวร์ที่มีค่าลิขสิทธิ์โดยตรง และซอฟท์แวร์ที่นำมาใช้ประกอบเสริมซอฟท์แวร์ที่มีค่าลิขสิทธิ์เพื่อความง่ายในการใช้งานบางระดับ ซึ่งความแตกต่างกันระหว่างซอฟท์แวร์ที่มีค่าลิขสิทธิ์ที่ต้องมีการจัดซื้อและซอฟท์แวร์ฟรี คือ ซอฟท์แวร์ที่มีค่าลิขสิทธิ์ที่มีการจัดซื้อมาจากต่างประเทศ อาทิเช่น สหรัฐอเมริกา อิสราเอล หรือแคนาดา จะมีข้อมูลของผู้ประดิษฐ์และผู้พัฒนาที่ชัดเจน มีมาตรฐานที่องค์กรสากลรับรอง จึงทำให้มีความน่าเชื่อถือมากกว่าซอฟท์แวร์ฟรีที่ปรากฏอยู่บนแหล่งข้อมูลเปิดซึ่งมีอยู่หลากหลาย สำหรับการที่ผู้ตรวจพิสูจน์แต่ละคนจะเลือกใช้ซอฟท์แวร์ฟรีตัวใดขึ้นอยู่กับดุลพินิจของผู้ตรวจพิสูจน์เอง เพราะปัจจุบันยังไม่มีการทดสอบจนได้ข้อมูลที่ตกผลึกว่าซอฟท์แวร์ที่ปรากฏบนแหล่งข้อมูลเปิดแต่ละตัว มีความเหมาะสม มีจุดเด่น จุดด้อย ข้อควรระวังหรือค่าความคลาดเคลื่อนของการประมวลผลที่อาจมีการพบเจอ เพื่อเป็นฐานข้อมูลกลางประกอบการเลือกใช้ซอฟท์แวร์ของผู้ตรวจพิสูจน์โดยรวม จากการทบทวนวรรณกรรมที่เกี่ยวข้อง ผู้วิจัยพบว่าปัจจุบันมีเพียงเอกสารชื่อ“ข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์หลักฐาน Version 1.0” เผยแพร่โดย สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (ออนไลน์, 2560) ที่เป็นแนวทางสำหรับผู้ตรวจพิสูจน์ โดยเอกสารดังกล่าวเสนอแนะหลักการปฏิบัติงานเกี่ยวกับพยานหลักฐานดิจิทัลการปฏิบัติงานในสถานที่เกิดเหตุและการปฏิบัติงานในห้องปฏิบัติการที่มีความสอดคล้องกับมาตรฐานสากลแต่ทว่าเอกสารดังกล่าวมิได้พูดถึงข้อแนะนำในเกี่ยวกับการใช้ซอฟท์แวร์ที่ปรากฏบนแหล่งข้อมูลเปิดเพื่องานตรวจพิสูจน์พยานหลักฐานเพื่อให้เกิดความน่าเชื่อถือและหลีกเลี่ยงข้อโต้แย้งเมื่อมีการนำผลการตรวจพิสูจน์ไปใช้อ้างอิงในการดำเนินคดี โดยอัศว์ณุต แสงทองดี ซึ่งเคยจัดฝึกอบรมความรู้เทคนิคการตรวจพิสูจน์พยานหลักฐานดิจิทัลแก่ผู้ตรวจพิสูจน์ทั้งในส่วนกลาง และส่วนภูมิภาค พบว่า จากประสบการณ์การทำงานที่ผ่านมา การปฏิบัติงานตรวจพิสูจน์หลักฐานของผู้ตรวจพิสูจน์ที่ปฏิบัติงานพื้นที่ส่วนกลางและในส่วนภูมิภาคมีแนวทางมาตรฐานการทำงานในห้องปฏิบัติการที่เหมือนกันแต่แตกต่างกันที่เครื่องมืออุปกรณ์ และซอฟท์แวร์สำหรับการตรวจพิสูจน์ (สัมภาษณ์, 2562) ซึ่งผู้วิจัยเห็นว่า ในเรื่องนี้มีความละเอียดอ่อนและอาจถูกหยิบยก

โต้แย้งได้ในชั้นพิจารณา โดยผู้ตรวจพิสูจน์อาจต้องเผชิญคำถามเกี่ยวกับความน่าเชื่อถือของอุปกรณ์การปฏิบัติงาน เนื่องจากตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 243 ความน่าเชื่อถือของพยานผู้เชี่ยวชาญด้านการตรวจพิสูจน์พยานหลักฐานดิจิทัล นอกจากเรื่องความรู้ความเชี่ยวชาญในการประมวลผลการตรวจพิสูจน์แล้ว ความน่าเชื่อถือของความเห็นยังอยู่ที่ความน่าเชื่อถือของเครื่องมืออุปกรณ์ที่ใช้ในการตรวจพิสูจน์ รวมถึงขั้นตอนการตรวจพิสูจน์ที่ต้องมีความเป็นมาตรฐาน หากมีข้อโต้แย้งที่มีนัยสำคัญ ย่อมนำไปสู่ผลกระทบต่อน้ำหนักของพยานหลักฐานที่ศาลจะรับฟังได้

ปัจจัยด้านความร่วมมือระหว่างผู้ปฏิบัติงาน

จากการสัมภาษณ์เชิงลึกเจ้าพนักงานในกระบวนการยุติธรรมทางอาญาพบสภาพปัญหาด้านความร่วมมือประสานงานระหว่างเจ้าพนักงานของรัฐด้วยกัน และการไม่ได้รับความร่วมมือจากภาคเอกชนเท่าที่ควรโดยสามารถจัดแบ่งกลุ่มปัญหาด้านการประสานความร่วมมือในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ได้เป็น 2 กลุ่ม คือ

1. ปัญหาการประสานงานระหว่างหน่วยงานของรัฐ

จากการสัมภาษณ์เชิงลึกกลุ่มผู้ตรวจพิสูจน์หลักฐาน (กชกร เพิงระนัย, สัมภาษณ์, 2562 ; ชานนท์ คำนวนศักดิ์, สัมภาษณ์, 2562 ; นิติ อินทลักษณ์, สัมภาษณ์, 2562 ; วันทนีย์ ตุลยเสวี, สัมภาษณ์, 2562) พบว่า ในชั้นที่พนักงานสอบสวนจัดส่งของกลาง (อุปกรณ์ดิจิทัล) พร้อมประเด็นการตรวจพิสูจน์ไปให้กับผู้ตรวจพิสูจน์หลักฐาน พบปัญหาในเรื่องการกำหนดวัตถุประสงค์ของการตรวจพิสูจน์ด้วยถ้อยคำที่กว้างขวาง ไม่ชัดเจน เป็นคำถามปลายเปิด หรือการตั้งคำถามขอให้จัดทำความเห็นในเชิงประเด็นกฎหมาย รวมถึงบางกรณีพนักงานสอบสวนบางคนระบุเพียงข้อหาที่มีการดำเนินคดีกับผู้ต้องหาและพฤติการณ์โดยย่อ มิได้อธิบายถึงพฤติการณ์แห่งคดีให้เพียงพอที่จะทำให้ผู้ตรวจพิสูจน์เข้าใจความเชื่อมโยงของวัตถุประสงค์ที่ต้องการตรวจพิสูจน์ ผู้ตรวจพิสูจน์หลักฐานบางท่านแก้ไขข้อขัดข้องโดยติดต่อสอบถามรายละเอียดแห่งคดีไปยังพนักงานสอบสวน (วันทนีย์ ตุลยเสวี, สัมภาษณ์, 2562)ในขณะที่บางท่านก็จะทำการตรวจพิสูจน์ตามความเข้าใจของผู้ตรวจพิสูจน์เองส่งผลกระทบต่อระยะเวลาที่ต้องใช้ในการตรวจพิสูจน์ และการจัดหาเครื่องมือการตรวจพิสูจน์เพิ่มเติมให้เพียงพอต่องาน

ในเรื่องนี้ เจ้าพนักงานสืบสวนและพนักงานสอบสวน (ดรัณ จาดเจริญ, สัมภาษณ์, 2562 ; ปัญจะผลโต, สัมภาษณ์, 2562; เผ่าภูมิ สมหมาย, สัมภาษณ์, 2562) ได้สะท้อนมุมมองว่าโดยภาพรวมเจ้าพนักงานสืบสวนและพนักงานสอบสวนยังมีความรู้ความเข้าใจเกี่ยวกับพยานหลักฐานดิจิทัลค่อนข้างน้อย โดยเฉพาะเจ้าพนักงานผู้ปฏิบัติงานในส่วนภูมิภาคซึ่งมีคดีประเภทอื่นจำนวนมากที่อยู่ในความรับผิดชอบ มีโอกาสได้รับการฝึกฝนอบรมความรู้ด้านเทคโนโลยีทางคอมพิวเตอร์น้อยกว่าเจ้าพนักงานที่ปฏิบัติงานในส่วนกลางและโดยสภาพข้อจำกัดเรื่องของกำหนดเวลาในการควบคุมตัว

ของผู้ต้องหา (ระยะเวลาฝากขังผู้ต้องหา) พนักงานสอบสวนมีหน้าที่ต้องดำเนินการสอบสวนในประเด็นต่างๆในคดีมากมาย เช่น การประสานขอข้อมูลด้านการเงิน ข้อมูลการใช้บริการโทรศัพท์ การสอบคำให้การพยานบุคคลมาประกอบคดี และการตรวจสอบประวัติการกระทำความผิดของผู้ต้องหา จึงทำให้พนักงานสอบสวนมักมอบภาระหน้าที่ในการจัดการของกลางซึ่งเป็นอุปกรณ์ดิจิทัลให้กับผู้ตรวจพิสูจน์หลักฐานโดยคาดหวังว่าผู้ตรวจพิสูจน์หลักฐานจะช่วยเหลือในการหาพยานหลักฐานที่เกี่ยวข้องเอง โดยที่ผ่านมา การปฏิบัติงานของเจ้าพนักงานสืบสวน พนักงานสอบสวนและผู้ตรวจพิสูจน์หลักฐานยังมีการดำเนินงานที่มีการประสานความเข้าใจในงานระหว่างกันค่อนข้างน้อย และมักใช้ช่องทางการประสานงานอย่างเป็นทางการผ่านหนังสือราชการเป็นหลัก

นอกจากนี้ ปกรณ์ ธรรมโรจน์ (สัมภาษณ์, 2562) เห็นว่า พนักงานสอบสวนที่รับผิดชอบงานคดีอาชญากรรมคอมพิวเตอร์ยังขาดที่ปรึกษาในการดำเนินคดี ทำให้การดำเนินคดีไม่ได้ข้อเท็จจริงในสาระสำคัญบางประการ ซึ่งหากมีผู้เชี่ยวชาญเป็นที่ปรึกษาในการดำเนินคดี คดีจะมีความสมบูรณ์ทั้งข้อเท็จจริงและพยานหลักฐานมากยิ่งขึ้น

2. ปัญหาการให้ความร่วมมือของภาคเอกชนต่อการปฏิบัติหน้าที่ของเจ้าพนักงานของรัฐ

ดังที่กล่าวมาแล้วในบทที่ 3 แม้ว่าพยานหลักฐานดิจิทัลที่พบอยู่ในของกลางจะมีความสำคัญอย่างมากในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ แต่เนื่องจากลักษณะของพยานหลักฐานดิจิทัลมีความเป็นไปได้ในการถูกเปลี่ยนแปลง ปนเปื้อน แก้ไข หรือปลอมแปลงได้ง่าย นำไปสู่ข้อโต้แย้งต่อสู้ในทางคดีได้ คดีจึงจำต้องอาศัยพยานหลักฐานอย่างอื่นเพื่อเชื่อมโยงพิสูจน์พฤติการณ์แห่งคดี และเพื่อที่จะระบุตัวผู้กระทำความผิดด้วย เจ้าพนักงานสืบสวนและพนักงานสอบสวนเป็นเจ้าพนักงานกลุ่มหลักที่ต้องทำการร้องขอความร่วมมือในการรับข้อมูลทางด้านการทำธุรกรรมทางการเงิน เช่น ข้อมูลผู้เปิดบัญชีเงินฝาก ข้อมูลการเปิดใช้บริการทางการเงิน (บัตรเอทีเอ็ม บัตรเดบิต บัตรเครดิต ข้อความสั้นแจ้งเตือน (SMSAlert) บริการธนาคารบนอินเทอร์เน็ต (Internet Banking)หรือบริการธนาคารบนโทรศัพท์เคลื่อนที่ (Mobile Banking)) เพื่อค้นหารูปแบบและเส้นทางการได้รับผลประโยชน์จากอาชญากรรมคอมพิวเตอร์ เนื่องจากส่วนใหญ่คดีอาชญากรรมคอมพิวเตอร์มีความมุ่งหวังในเรื่องทรัพย์สินจากผู้เสียหาย รวมไปถึงข้อมูลการจราจรทางคอมพิวเตอร์ ข้อมูลพื้นที่การใช้โทรศัพท์เคลื่อนที่ (Cell Sites)ของคนร้าย ซึ่งจากการสัมภาษณ์เชิงลึก (ดรัณ จาดเจริญ ; เผ่าภูมิ สมหมาย) พบข้อมูลสภาพปัญหาของเจ้าพนักงานสืบสวนและพนักงานสอบสวนในการประสานขอรับข้อมูลที่เป็นประโยชน์แก่คดีจากผู้ให้บริการภาคเอกชน เช่น ผู้ให้บริการสัญญาณโทรศัพท์ ผู้ให้บริการอินเทอร์เน็ต หรือธนาคารพาณิชย์ต่างๆ ซึ่งภาคเอกชนมักปฏิเสธการให้ข้อมูลหรือให้ข้อมูลตามที่ร้องขอล่าช้าจนทำให้ไม่ทันต่อสถานการณ์บ่อยครั้ง

ในส่วนของกฎหมายแม้ว่าตาม**พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 (ที่แก้ไขเพิ่มเติม)**จะได้บัญญัติความรับผิดของผู้ให้บริการที่ไม่ให้ความร่วมมือกับทางเจ้าพนักงานผู้ทำการสืบสวนสอบสวนคดีอาชญากรรมคอมพิวเตอร์ไว้ อาทิเช่น **มาตรา 26** บัญญัติว่า

ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินสองปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง

ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใด ให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท

หรือกรณีที่เจ้าพนักงานตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 (ที่แก้ไขเพิ่มเติม)สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่ หรือสั่งให้ดำเนินการอย่างอื่นตามกฎหมายแล้วไม่ปฏิบัติตามคำสั่ง **มาตรา 27** บัญญัติว่า

ผู้ใดไม่ปฏิบัติตามคำสั่งของศาลหรือพนักงานเจ้าหน้าที่ที่สั่งตามมาตรา 18 หรือมาตรา 20 หรือไม่ปฏิบัติตามคำสั่งของศาลตามมาตรา 21 ต้องระวางโทษปรับไม่เกินสองแสนบาท และปรับเป็นรายวันอีกไม่เกินวันละห้าพันบาทจนกว่าจะปฏิบัติให้ถูกต้อง

ผู้วิจัยเห็นว่าแม้กฎหมายจะกำหนดความรับผิดไว้ชัดเจนก็ตาม แต่สาเหตุที่ผู้ให้บริการภาคเอกชนไม่ค่อยให้ความร่วมมือเท่าที่ควรแก่ทางภาครัฐอาจเนื่องมาจากความกังวลเกี่ยวกับการเปิดเผยข้อมูลส่วนบุคคลของลูกค้าผู้รับบริการ และไม่มั่นใจว่าการนำข้อมูลของผู้รับบริการไปใช้งานจะถูกจำกัดแต่เพียงเพื่อประโยชน์ในการดำเนินคดีนั้นเท่านั้น นอกจากนี้ผู้วิจัยเห็นว่า ประเด็นที่เบญจพร วัชระวุฒิชัย (สัมภาษณ์, 2562) ชี้ให้เห็นถึงปัญหาเชิงต้นทุนในการดำเนินการซึ่งภาคเอกชนเป็นผู้รับผิดชอบก็เป็นประเด็นสำคัญ เนื่องจากมักพบว่า ในการดำเนินคดีอาญาเกือบทุกประเภท (ไม่จำกัดเพียงคดีอาชญากรรมคอมพิวเตอร์) ที่คนร้ายได้ไปซึ่งทรัพย์สินของผู้เสียหาย พนักงานสอบสวนจะมีการร้องขอสำเนาเอกสารคำขอเปิดบัญชี และรายงานเดินบัญชีเงินฝากของผู้เสียหายและผู้ต้องหาทางผู้ประกอบการธนาคารพาณิชย์ซึ่งต้องจัดส่งสำเนาเอกสารเหล่านี้ยังไม่สามารถเรียกเก็บเอาค่าใช้จ่ายจากทางภาครัฐได้ หลายครั้งพบว่าแต่ละคดีต้องมีการจัดทำเอกสารหลายสิบหรือหลายร้อยแผ่นโดยยังไม่สามารถจัดส่งเอกสารในรูปแผ่นซีดีทดแทนได้ นอกจากนี้ ในส่วนของค่าใช้จ่ายในการเก็บ

ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ ผู้ประกอบการมีต้นทุนในด้านอุปกรณ์และพื้นที่สำรองในการจัดเก็บข้อมูลเหล่านั้นเพื่อปฏิบัติตามที่กฎหมายกำหนดอีกด้วย

ปัจจัยด้านบทบัญญัติกฎหมาย

แม้ว่าจากการสัมภาษณ์เชิงลึก เจ้าพนักงานในกระบวนการยุติธรรมที่เกี่ยวข้องกับการดำเนินคดีอาชญากรรมคอมพิวเตอร์ส่วนใหญ่ เห็นว่าบทบัญญัติกฎหมายในปัจจุบันยังคงเพียงพอในการปฏิบัติงาน แต่ยังคงมีข้อกังวลบางประการเกี่ยวกับการปรับใช้บทบัญญัติกฎหมายในการปฏิบัติงานของตน โดยสาเหตุของปัญหามาจากการขาดบทสันนิษฐานตามกฎหมายว่าด้วยพยานหลักฐาน และการขาดหลักเกณฑ์เฉพาะเพื่อการสอบสวน การรวบรวม และการรับฟังพยานหลักฐานที่อยู่ในรูปพยานหลักฐานดิจิทัล(หรือพยานหลักฐานทางอิเล็กทรอนิกส์) กล่าวคือ ผู้ตรวจพิสูจน์หรือแม้แต่เจ้าพนักงานสืบสวน (ชานนท์ คำนวนศักดิ์, สัมภาษณ์, 2562 ; ดรัณ จาดเจริญ, สัมภาษณ์, 2562 ; เบญจพร วัชระวุฒิชัย, สัมภาษณ์, 2562 ; ปกรณ์ ธรรมโรจน์, สัมภาษณ์, 2562 ; อัศว์ณุต แสงทองดี, สัมภาษณ์, 256) มักเกิดความกังวลในเรื่องของวิธีการที่เจ้าพนักงานใช้เพื่อให้เข้าถึงข้อมูลได้ เนื่องจากเทคโนโลยีเกี่ยวกับการเข้ารหัสป้องกันข้อมูล (Data Encryption) เพื่อป้องกันการเข้าถึงข้อมูล ทำให้ไม่สามารถเข้าถึงข้อมูลดังกล่าวได้ ดังนั้นแม้ว่าเจ้าพนักงานตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 (ที่แก้ไขเพิ่มเติม) หรือพนักงานสอบสวนยึดอุปกรณ์ดิจิทัล เช่น เครื่องคอมพิวเตอร์ หรือโทรศัพท์สมาร์ทโฟนของผู้ต้องสงสัยมาเป็นของกลางในคดีแล้ว แต่หากผู้ต้องสงสัยตั้งค่ารหัสผ่านอุปกรณ์ดิจิทัลหรือเข้ารหัสไฟล์ข้อมูลภายในอุปกรณ์เหล่านั้นและไม่ยินยอมเปิดเผยรหัสผ่านที่ใช้ในการปลดล็อคอุปกรณ์หรือถอดรหัสไฟล์ข้อมูล โดยเฉพาะในกรณีที่อุปกรณ์ดิจิทัลสมัยใหม่ที่ถูกพัฒนาระบบป้องกันความเป็นส่วนตัวสูงมากจนทำให้ไม่อาจใช้เครื่องมือหรือซอฟท์แวร์ใดๆเข้าตรวจสอบหาร่องรอยพยานหลักฐานที่อยู่ภายในอุปกรณ์ดิจิทัลของกลางได้ ย่อมทำให้ของกลางในคดีชิ้นนั้นแทบจะไม่เป็นประโยชน์ต่อการดำเนินคดีเลย หรือหากเจ้าพนักงานใช้วิธีการเช่นการทำฟิชชิ่ง (Phishing)เพื่อลวงให้คนร้ายหลงเปิดเผยชื่อผู้ใช้ (Log In) และรหัสผ่าน (Password) ของตน หรือกรณีที่แม้ผู้ต้องหาให้ความยินยอมในการเปิดเผยรหัสผ่าน (Password) ซึ่งเป็นมาตรการป้องกันการเข้าถึงโดยเฉพาะสำหรับอุปกรณ์ดิจิทัลที่ถูกยึดเป็นของกลางแล้วก็ตาม แต่เจ้าพนักงานก็มีความจำเป็นที่จะต้องเปลี่ยนแปลงรหัสผ่าน (Password) ซึ่งเป็นมาตรการป้องกันการเข้าถึงโดยเฉพาะสำหรับอุปกรณ์ดิจิทัลหรือการใช้งานโปรแกรมบางอย่าง เช่น อีเมลเฟซบุ๊กไลน์ หรือสื่อสังคมออนไลน์อย่างอื่นที่อาจมีข้อมูลการกระทำความผิดปรากฏอยู่โดยการตั้งค่ารหัสผ่านเพื่อป้องกันมิให้ตัวผู้ต้องหาซึ่งได้รับการปล่อยตัวระหว่างการสอบสวนหรือบุคคลภายนอกที่ล่วงรู้รหัสผ่านเช่นว่านั้น สามารถเข้าถึง ครอบครอง สั่งการข้อมูลคอมพิวเตอร์ที่อยู่ในอุปกรณ์ดิจิทัลเพื่อทำลายหรือเปลี่ยนแปลงสภาพของข้อมูลคอมพิวเตอร์ที่อาจใช้เป็นพยานหลักฐานใน

คดีจากพื้นที่ในระยะทางไกลได้ แต่การดำเนินการเช่นว่านั้นก่อให้เกิดความกังวลต่อผู้ปฏิบัติงานอย่างมากว่าจะถือเป็นวิธีการได้มาซึ่งพยานหลักฐานโดยมิชอบด้วยกฎหมายหรือไม่ อันอาจส่งผลต่อน้ำหนักการใช้เป็นพยานหลักฐานในคดีหรือแม้แต่อาจจะก่อให้เกิดความรับผิดกับเจ้าพนักงานผู้ปฏิบัติการดังกล่าวเป็นการส่วนตัวอีกด้วย เนื่องจากตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 (ที่แก้ไขเพิ่มเติม) ได้บัญญัติเกี่ยวกับความผิดอาญาในการดักรับ เข้าถึง เปลี่ยนแปลง รหัสผ่าน (Password) ซึ่งเป็นมาตรการป้องกันการเข้าถึงโดยเฉพาะของผู้อื่นไว้ดังนี้

มาตรา 5 ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 7 ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 8ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 9 ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา 10 ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

ผู้วิจัยเห็นว่าสภาพปัญหาดังกล่าวมีที่มาจากการขาดบทสันนิษฐานทางกฎหมายสำหรับกรณีพยานหลักฐานดิจิทัล กล่าวคือ ในกรณีทั่วไปเมื่อเป็นพยานหลักฐานที่มีลักษณะจำเพาะว่าจะเข้าถึงได้ต่อเมื่อผู้เป็นเจ้าของจะต้องให้ความร่วมมือและยินยอมส่งวัตถุพยานหรือยินยอมให้กระทำการใดเพื่อให้ได้ไปซึ่งข้อมูลพยานหลักฐานเท่านั้น อาทิเช่น พยานหลักฐานทางนิติวิทยาศาสตร์ในการตรวจพิสูจน์ส่วนประกอบร่างกายบุคคล มีบทบัญญัติกฎหมายกำหนดหลักเกณฑ์ไว้เป็นพิเศษ ตาม**ประมวลกฎหมายวิธีพิจารณาความอาญา** (“ประมวลกฎหมายวิธีพิจารณาความอาญา (ฉบับ Update ล่าสุด)”, 2562)**มาตรา 131/1** ซึ่งบัญญัติว่า

ในกรณีที่จำเป็นต้องใช้พยานหลักฐานทางวิทยาศาสตร์ เพื่อพิสูจน์ข้อเท็จจริงตามมาตรา 131 ให้พนักงานสอบสวนมีอำนาจให้ทำการตรวจพิสูจน์บุคคล วัตถุ หรือเอกสารใดๆ โดยวิธีการทางวิทยาศาสตร์ได้

ในกรณีความผิดอาญาที่มีอัตราโทษจำคุกอย่างสูงเกินสามปี หากการตรวจพิสูจน์ตามวรรคหนึ่ง จำเป็นต้องตรวจเก็บตัวอย่างเลือด เนื้อเยื่อ ผิวหนัง เส้นผมหรือขน น้ำลาย ปัสสาวะ อุจจาระ สารคัดหลั่ง สารพันธุกรรมหรือส่วนประกอบของร่างกายจากผู้ต้องหา ผู้เสียหายหรือบุคคลที่เกี่ยวข้อง ให้พนักงานสอบสวนผู้รับผิดชอบมีอำนาจให้แพทย์หรือผู้เชี่ยวชาญดำเนินการตรวจดังกล่าวได้ แต่ต้องกระทำเพียงเท่าที่จำเป็นและสมควรโดยใช้วิธีการที่ก่อให้เกิดความเจ็บปวดน้อยที่สุดเท่าที่จะกระทำได้ ทั้งจะต้องไม่เป็นอันตรายต่อร่างกายหรืออนามัยของบุคคลนั้น และผู้ต้องหา ผู้เสียหาย หรือบุคคลที่เกี่ยวข้องต้องให้ความยินยอม หากผู้ต้องหาหรือผู้เสียหายไม่ยินยอมโดยไม่มีเหตุอันสมควรหรือผู้ต้องหาหรือผู้เสียหายกระทำการป้องปัดขัดขวางมิให้บุคคลที่เกี่ยวข้องให้ความยินยอมโดยไม่มีเหตุอันสมควร ให้สันนิษฐานไว้เบื้องต้นว่าข้อเท็จจริงเป็นไปตามผลการตรวจพิสูจน์ที่หากได้ตรวจพิสูจน์แล้วจะเป็นผลเสียต่อผู้ต้องหาหรือผู้เสียหายนั้น แล้วแต่กรณี

ค่าใช้จ่ายในการตรวจพิสูจน์ตามมาตรานี้ ให้สั่งจ่ายจากงบประมาณตามระเบียบที่สำนักงานตำรวจแห่งชาติ กระทรวงมหาดไทย กระทรวงยุติธรรม หรือสำนักงานอัยการสูงสุด แล้วแต่กรณี กำหนดโดยได้รับความเห็นชอบจากกระทรวงการคลัง

ในวรรคสองตอนท้ายซึ่งบัญญัติว่า “หากผู้ต้องหาหรือผู้เสียหายไม่ยินยอมโดยไม่มีเหตุอันสมควรหรือผู้ต้องหาหรือผู้เสียหายกระทำการป้องปัดขัดขวางมิให้บุคคลที่เกี่ยวข้องให้ความยินยอมโดยไม่มีเหตุอันสมควร ให้สันนิษฐานไว้เบื้องต้นว่าข้อเท็จจริงเป็นไปตามผลการตรวจพิสูจน์ที่หากได้ตรวจพิสูจน์แล้วจะเป็นผลเสียต่อผู้ต้องหาหรือผู้เสียหายนั้น แล้วแต่กรณี” ถือเป็นข้อยกเว้นหลักของระบบการดำเนินคดีอาญาในระบบกล่าวหา (Accusatorial System)ซึ่งคู่ความที่ต้องการกล่าวอ้างข้อเท็จจริงใดย่อมต้องมีหน้าที่นำสืบ และยังเป็นข้อยกเว้นของหลักข้อสันนิษฐานการเป็นผู้บริสุทธิ์ (Presumption of Innocence) ดังที่ได้กล่าวมาในบทที่ 2 ซึ่งเป็นหลักการใดการดำเนินคดีอาญาในกรณีทั่วไป ทั้งนี้มาตรา 131/1 มีเหตุผลในการประกาศใช้เพื่อให้ทันสมัยและสอดคล้องกับสภาวการณ์ทางเศรษฐกิจ สังคม และการพัฒนาด้านเทคโนโลยีของประเทศในปัจจุบันดังนั้น ในกรณีคดีที่มีการกล่าวหาความผิดอาญาที่มีอัตราโทษจำคุกอย่างสูงเกินสามปี ซึ่งเจ้าพนักงานของรัฐได้ขอตรวจพิสูจน์ทางนิติวิทยาศาสตร์ที่ต้องเก็บตัวอย่างเลือด เนื้อเยื่อ ผิวหนัง เส้นผมหรือขน น้ำลาย ปัสสาวะ อุจจาระ สารคัดหลั่ง สารพันธุกรรมหรือส่วนประกอบของร่างกายจากผู้ต้องหา ผู้เสียหายหรือบุคคลที่เกี่ยวข้อง โดยมีวัตถุประสงค์เพื่อยืนยันข้อเท็จจริงเกี่ยวกับการกระทำความผิดหรือความบริสุทธิ์ของบุคคลใดแล้ว บุคคลที่เกี่ยวข้องไม่ให้ความยินยอมโดยปราศจากเหตุอันสมควรแล้วกฎหมายกำหนดข้อสันนิษฐานว่าข้อเท็จจริงเป็นไปในแนวทางที่เป็นผลเสียต่อผู้ต้องหาหรือผู้เสียหายนั้นหากมีการตรวจพิสูจน์จริง โดยผลักภาระให้เป็นของผู้ต้องหาหรือผู้เสียหายที่ต้องเสียหายจากข้อ

สันนิษฐานตามกฎหมายที่ในการนำสืบพิสูจน์หักล้างข้อสันนิษฐานว่าข้อเท็จจริงมิได้เป็นไปในทางผลร้ายนั้นเอง

อย่างไรก็ดี แม้ว่าการตรวจพิสูจน์ทางนิติคอมพิวเตอร์ถือได้ว่าเป็นการตรวจพิสูจน์วัตถุหรือเอกสารใดๆ โดยวิธีการทางวิทยาศาสตร์ตามมาตรา 131/1 วรรคหนึ่งก็ตาม แต่มาตรา 131/1 วรรคสอง มิได้บัญญัติให้ครอบคลุมถึงการที่ผู้ต้องหาหรือผู้เสียหายไม่ให้ความยินยอมโดยปราศจากเหตุอันสมควรในกรณีที่เจ้าพนักงานขอเข้าถึงข้อมูลภายในอุปกรณ์ดิจิทัลซึ่งผู้ต้องหาหรือผู้เสียหายนั้นได้ตั้งค่ารหัสผ่าน (Password)หรือมาตรการป้องกันการเข้าถึงโดยเฉพาะอย่างอื่นไว้เพื่อทำการตรวจพิสูจน์ทางนิติคอมพิวเตอร์

นอกจากนี้ ผู้วิจัยเห็นว่าจากข้อจำกัดที่บทบัญญัติประมวลกฎหมายวิธีพิจารณาความอาญาในปัจจุบัน ซึ่งยังมิได้มีการบัญญัติหลักเกณฑ์เฉพาะในการสอบสวน การรวบรวม และการรับฟังพยานหลักฐานที่อยู่ในรูปพยานหลักฐานดิจิทัล หรือพยานหลักฐานทางอิเล็กทรอนิกส์ไว้ อาจก่อให้เกิดอุปสรรคในการปฏิบัติงานกับเจ้าพนักงานที่เกี่ยวข้องในอนาคต ทั้งยังก่อให้เกิดข้อกังวลในการใช้อำนาจตามกฎหมายในการรวบรวมพยานหลักฐานในคดีอาชญากรรมคอมพิวเตอร์ด้วย

แนวทางการพัฒนาประสิทธิภาพการดำเนินคดีอาชญากรรมคอมพิวเตอร์ของต่างประเทศที่น่าสนใจ

เมื่อกล่าวถึงประเทศเพื่อนบ้านซึ่งมีแนวนโยบายการเตรียมความพร้อมด้านอาชญากรรมคอมพิวเตอร์หรืออาชญากรรมทางไซเบอร์ (Cybercrime) อย่างเป็นระบบ ผู้วิจัยเห็นว่าสาธารณรัฐสิงคโปร์เป็นหนึ่งในประเทศแม่แบบของการพัฒนาความรู้ของบุคลากรและระบบกฎหมายด้านอาชญากรรมคอมพิวเตอร์

จากสภาพปัญหาในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ของประเทศไทยดังที่ได้กล่าวมา และจากข้อมูลที่ เบญจพร วัชระวุฒิชัย (สัมภาษณ์, 2562) อัยการจังหวัดประจำสำนักงานอัยการสูงสุด สำนักงานอัยการพิเศษฝ่ายคดีเศรษฐกิจและทรัพยากร 7 ซึ่งเป็นผู้แทนสำนักงานอัยการสูงสุดเข้าร่วมการประชุมด้านอาชญากรรมทางไซเบอร์ ณ สาธารณรัฐสิงคโปร์ ในปี 2559 และ 2561 บอกเล่าประสบการณ์ในการประชุมระดับภูมิภาคอาเซียนและการร่วมฝึกอบรมภาคปฏิบัติกับอัยการสหรัฐอเมริกาและตำรวจสากล (INTERPOL) พบว่าสาธารณรัฐสิงคโปร์มีแนวทางในการพัฒนาประสิทธิภาพในการปราบปรามอาชญากรรมคอมพิวเตอร์ที่น่าสนใจ และสามารถนำมาวิเคราะห์ปรับใช้เป็นแนวทางในการเพิ่มประสิทธิภาพด้านการดำเนินคดีอาชญากรรมคอมพิวเตอร์ของไทยได้ 2 แนวทางดังนี้

1. **แนวทางการพัฒนาความรู้ด้านอาชญากรรมคอมพิวเตอร์**(เบญจพร วัชระวุฒิชัย, สัมภาษณ์, 2562)

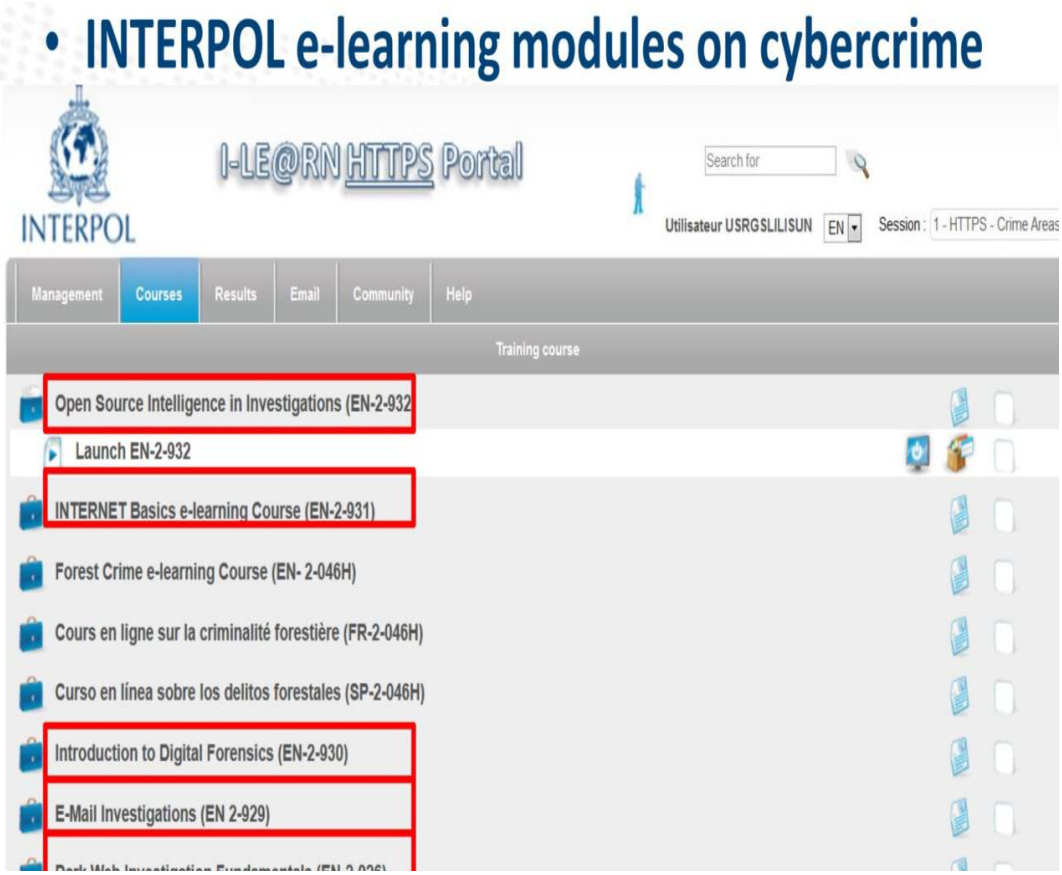
ด้วยเหตุที่เทคโนโลยีด้านเทคนิคคอมพิวเตอร์ และนิติคอมพิวเตอร์ เป็นองค์ความรู้ที่ค่อนข้างใหม่ และมีพัฒนาการต่อเนื่องไปตามเทคโนโลยีที่ก้าวหน้าไม่หยุดยั้งของอุปกรณ์ดิจิทัล

การจัดฝึกอบรมความรู้ด้วยวิธีแบบดั้งเดิม ในลักษณะที่มีวิทยากรบรรยายสดให้แก่ผู้เข้ารับการอบรม ณ สถานที่ใดสถานที่หนึ่ง อาจไม่ตอบสนองและไม่ทันต่อการแก้ปัญหาการขาดองค์ความรู้ในการดำเนินคดีอาชญากรรมคอมพิวเตอร์เนื่องจากการจัดอบรมรูปแบบดังกล่าวต้องมีการจัดทำโครงการเพื่อขออนุมัติงบประมาณด้านสถานที่ วิทยากร อุปกรณ์และเอกสารที่ในการฝึกอบรม ค่าอาหาร และค่าใช้จ่ายอื่นๆ ซึ่งต้องการทั้งเวลาในการเตรียมการและงบประมาณ อีกทั้งผู้ที่มีโอกาสรับการฝึกอบรมมีจำนวนจำกัดตามงบประมาณที่ได้รับ ผู้เข้าอบรมบางส่วนไม่ใช่ผู้ปฏิบัติงานด้านคดีอาชญากรรมคอมพิวเตอร์โดยตรง จึงอาจมิใช่แนวทางการแก้ปัญหาการขาดองค์ความรู้ด้านอาชญากรรมคอมพิวเตอร์ที่เหมาะสมและเพียงพอต่อความต้องการ

องค์การตำรวจอาชญากรรมระหว่างประเทศ(International Criminal Police Organization) หรือตำรวจสากล (INTERPOL)ซึ่งเป็นหน่วยงานประสานงานตำรวจระดับสากลมีสมาชิก194 ประเทศ มีสำนักงานสาขาที่ใช้ชื่อว่า “The INTERPOL Global Complex for Innovation” (หรือ “IGCI”) ตั้งอยู่ ณ สาธารณรัฐสิงคโปร์ เพื่อเป็นหน่วยงานที่พัฒนางานวิจัยอำนวยเครื่องมือความรู้ และการจัดฝึกอบรมที่สร้างสรรค์ เพื่อการรับมือกับอาชญากรรมในศตวรรษที่ 21 โดยIGCI ได้นำรูปแบบการจัดฝึกอบรมให้ความรู้แก่เจ้าพนักงานของรัฐผู้ปฏิบัติงานด้านอาชญากรรมคอมพิวเตอร์ ทั้งเจ้าพนักงานสืบสวน พนักงานสอบสวน ผู้ตรวจพิสูจน์นิติคอมพิวเตอร์ และพนักงานอัยการ ในรูปของการฝึกภาคปฏิบัติ (Workshop)จากกรณีคดีตัวอย่างและสถานการณ์จำลองบนเครื่องมือคอมพิวเตอร์และอุปกรณ์การตรวจพิสูจน์จริง ผู้เข้ารับการฝึกอบรมคือ บุคลากรภาครัฐด้านอาชญากรรมคอมพิวเตอร์ของประเทศสมาชิกซึ่งได้รับการคัดเลือกจากหน่วยงานต้นสังกัดเข้ารับการฝึกอบรม สำหรับเจ้าพนักงานซึ่งมีความสนใจเรียนรู้ด้านอาชญากรรมทางไซเบอร์แต่ไม่สามารถเข้าร่วมการฝึกอบรมอย่างเป็นทางการได้ ก็สามารถเข้าศึกษาเรียนรู้ผ่านช่องทางหลักสูตรบนสื่ออิเล็กทรอนิกส์ (E-learning) ในหัวข้อเกี่ยวกับอาชญากรรมทางไซเบอร์ที่น่าสนใจต่างๆ บนเว็บไซต์ของ INTERPOL ได้ ทั้งนี้ หลักสูตรบนสื่ออิเล็กทรอนิกส์ (E-learning) ส่วนใหญ่จะจำกัดการเข้าถึงโดยผู้เข้าใช้งานต้องเป็นบุคลากรของหน่วยงานผู้ใช้บังคับกฎหมายซึ่งร้องขอให้ผู้แทนสำนักงานกลางแห่งชาติของ INTERPOL ในประเทศสมาชิก (หรือ NCB)ดำเนินการแจ้งชื่อ ตำแหน่ง หน่วยงานต้นสังกัด และอีเมล ไปยังIGCI เพื่อขอรหัสผ่านในการลงทะเบียนเข้าศึกษาสำหรับ NCB ของประเทศไทย คือ กองการต่างประเทศ สำนักงานตำรวจแห่งชาติ

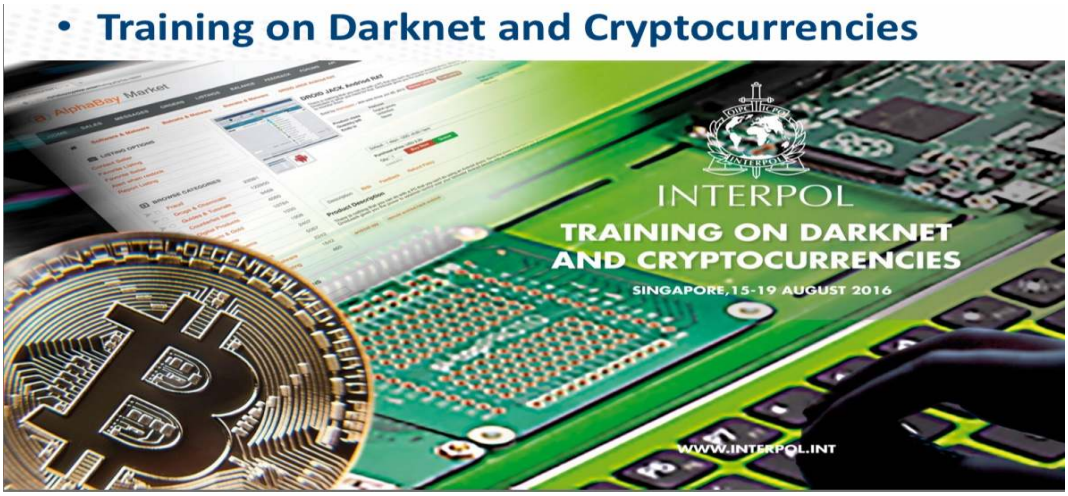
หลักสูตรบนสื่ออิเล็กทรอนิกส์ หรือหลักสูตรออนไลน์ (E-learning) ด้านการดำเนินคดีอาชญากรรมคอมพิวเตอร์ของ INTERPOL มีตัวอย่างดังนี้

แผนภาพที่ 4-1 ตัวอย่างหลักสูตรออนไลน์ด้านอาชญากรรมคอมพิวเตอร์ของ INTERPOL



ที่มา : เอกสารประกอบการบรรยายเรื่อง INTERPOL Capacity Building and Training Activities (Lily Sun, ออนไลน์, 2562)อ้างถึงใน เบญจพร วัชระวุฒิชัย, สัมภาษณ์, 2562.

แผนภาพที่ 4-2 หลักสูตรฝึกอบรมเกี่ยวกับเว็บไซต์อำพราง(Darknetหรือ Deep Web)และสกุลเงินถอดรหัส (Cryptocurrencies)ของ INTERPOL



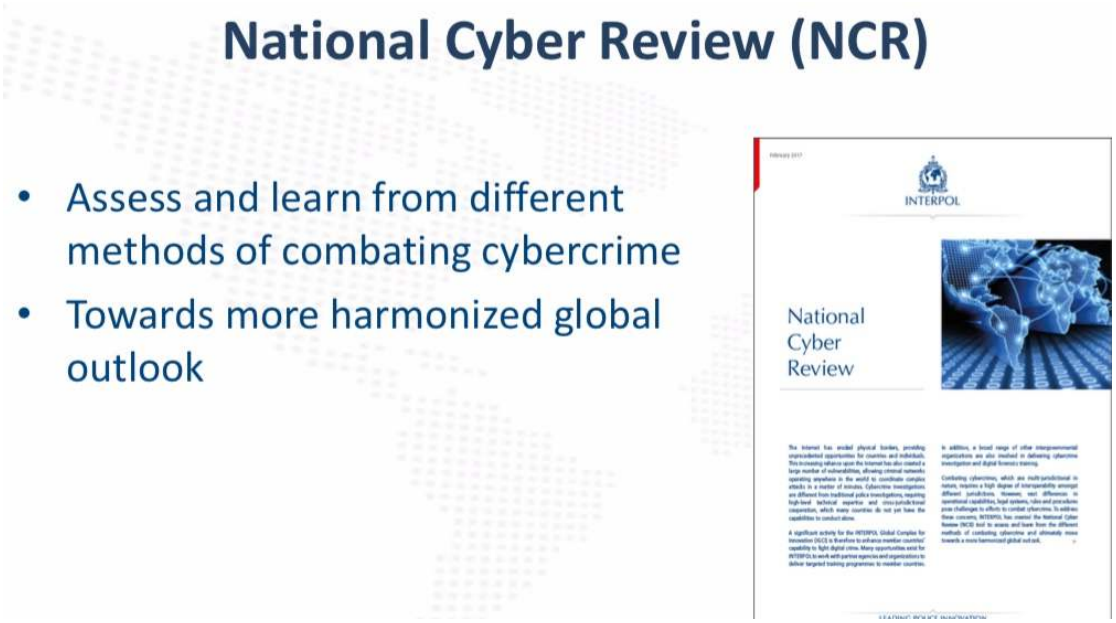
ที่มา : เอกสารประกอบการบรรยายเรื่อง INTERPOL Capacity Building and Training Activities (Lily Sun, ออนไลน์, 2562)อ้างถึงในเบญจพร วัชระวุฒิชัย, สัมภาษณ์, 2562.

จากแผนภาพที่ 4-1 และ 4-2 แสดงตัวอย่างหลักสูตรที่น่าสนใจ เช่น หลักสูตรการสืบสวนบนแหล่งข้อมูลเปิด (Open Source Intelligence in Investigations) หลักสูตรอินเทอร์เน็ตขั้นพื้นฐาน (INTERNET Basics E-Learning Course) หลักสูตรความรู้เบื้องต้นสำหรับการตรวจพิสูจน์ทางดิจิทัล (Introduction to Digital Forensics) การสืบสวนเกี่ยวกับอีเมล (E-Mail Investigations) ความรู้พื้นฐานทางสำหรับสืบสวนเว็บไซต์อำพราง (DarkWebInvestigation Fundamentals) และสกุลเงินเข้ารหัส (Cryptocurrencies) ซึ่งหลักสูตรเหล่านี้ใช้ภาษาอังกฤษเป็นภาษาหลักในการศึกษา

แผนภาพที่ 4-3 แนวทางการประเมินผลข้อมูลด้านอาชญากรรมคอมพิวเตอร์ของ INTERPOL

ที่มา :เอกสารประกอบการบรรยายเรื่อง INTERPOL Capacity Building and Training Activities (Lily Sun, ออนไลน์, 2562)อ้างถึงในเบญจพร วัชระวุฒิชัย, สัมภาษณ์, 2562.

แผนภาพที่ 4-4 เอกสารการรวบรวมข้อมูลด้านอาชญากรรมคอมพิวเตอร์ของ INTERPOL



ที่มา : เอกสารประกอบการบรรยายเรื่อง INTERPOL Capacity Building and Training Activities (Lily Sun, ออนไลน์, 2562) อ้างถึงในเบญจพร วัชระวุฒิชัย, สัมภาษณ์, 2562.

ตามแผนภาพที่ 4-3 แสดงถึงข้อมูลเป้าประสงค์ที่ INTERPOL มีการเก็บรวบรวมข้อมูลด้านอาชญากรรมคอมพิวเตอร์ของประเทศต้นแบบซึ่งINTERPOL เห็นว่าน่าสนใจโดยจะทำการประเมินแบบครอบคลุม (Comprehensive Assessment)เกี่ยวกับความสามารถในการป้องกัน ตรวจจับ และการสืบสวนอาชญากรรมทางไซเบอร์ โดยพิจารณาจากประสิทธิภาพในการบังคับใช้กฎหมาย และบทบัญญัติกฎหมายที่มี จากนั้นจะจัดทำบทวิจารณ์ในรูปรายงานข้อเสนอแนะสำหรับการส่งเสริมขอบข่ายด้านเทคนิค กฎหมาย การปฏิบัติการ และโครงสร้างองค์กร เพื่อการจัดการกับอาชญากรรมเกี่ยวกับคอมพิวเตอร์จากนั้นทำการเผยแพร่ในรูปของสื่อเอกสารที่ชื่อ “National Cyber Review”(หรือ NCR) ตามแผนภาพที่ 4-4

2. แนวทางเกี่ยวกับอำนาจของเจ้าพนักงานในคดีอาชญากรรมคอมพิวเตอร์(เบญจพร วัชระวุฒิชัย, สัมภาษณ์, 2562)

ในด้านบทบัญญัติกฎหมาย สาธารณรัฐสิงคโปร์มี**Computer Misuse Act (Chapter 50 A)**เป็นกฎหมายหลักที่กำหนดบรรดาฐานความผิดซึ่งกระทำต่อระบบคอมพิวเตอร์หรือใช้คอมพิวเตอร์ในการกระทำความผิด แต่ไม่ได้บัญญัติให้มีเจ้าพนักงานพิเศษเพื่อใช้อำนาจพิเศษตามกฎหมายฉบับดังกล่าวเช่นเดียวกับที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 (ที่แก้ไขเพิ่มเติม)ของไทย ซึ่งกำหนดให้มี “พนักงานเจ้าหน้าที่” ตามพระราชบัญญัติดังกล่าวให้มีอำนาจดำเนินการสืบสวนสอบสวนความผิดตามพระราชบัญญัติดังกล่าว ตามมาตรา 18 และ มาตรา 19

แต่ตาม **มาตรา 14** แห่ง**Computer Misuse Act (Chapter 50 A)** มีการบัญญัติอำนาจสืบสวนสอบสวนของเจ้าหน้าที่ตำรวจและเจ้าพนักงานตามกฎหมายไว้ว่า พระราชบัญญัติดังกล่าวไม่เป็นการกระทบกับอำนาจตามที่กฎหมายบัญญัติให้ไว้แก่เจ้าพนักงานตำรวจ หรือเจ้าพนักงานซึ่งมีอำนาจตาม **มาตรา 39** แห่ง **Criminal Procedure Code 2010**หรือเจ้าพนักงานผู้บังคับใช้กฎหมายตามกฎหมายอื่น ในการปฏิบัติงานสืบสวนสอบสวนโดยชอบด้วยกฎหมาย (“Computer Misuse Act (Chapter 50A)”, ออนไลน์, 2562) ซึ่งCriminal Procedure Code(ออนไลน์, 2562) ได้บัญญัติอำนาจที่น่าสนใจบางประการของเจ้าพนักงานสืบสวนสอบสวนในการเข้าถึงข้อมูลคอมพิวเตอร์ไว้ใน **มาตรา 39**อาทิเช่น เจ้าพนักงานตำรวจหรือผู้ซึ่งได้รับมอบอำนาจในการสืบสวนสอบสวนความผิดซึ่งทำการจับกุมได้ (An Arrestable Offence) มีอำนาจทุกเมื่อในการ

1. เข้าถึง ตรวจสอบ และตรวจเช็คการปฏิบัติการ (Operation)ที่อยู่ภายในหรือจากในสาธารณรัฐสิงคโปร์ ของคอมพิวเตอร์ (ไม่ว่าอยู่ภายในสาธารณรัฐสิงคโปร์ หรือสถานที่อื่นใด) ซึ่งเจ้าพนักงานมีเหตุอันควรสงสัยว่าได้ถูกใช้ในการเชื่อมต่อหรือการจัดเก็บซึ่งพยานหลักฐานอันเกี่ยวโยงกับฐานความผิดที่มีการจับกุม

2. ใช้คอมพิวเตอร์หรือกระทำด้วยวิธีการอื่นเพื่อมีการใช้คอมพิวเตอร์ดังกล่าวที่อยู่ภายในหรือจากในสาธารณรัฐสิงคโปร์เพื่อค้นหาข้อมูลซึ่งถูกจัดเก็บอยู่ภายใน หรือซึ่งสามารถได้มาด้วยคอมพิวเตอร์นั้น และจัดทำสำเนาซึ่งข้อมูลดังกล่าว

3. ป้องกันมิให้บุคคลอื่นเข้าถึง หรือใช้ซึ่งคอมพิวเตอร์นั้น (รวมไปถึงการเปลี่ยนแปลงรหัสผู้ใช้ รหัสผ่าน หรือข้อมูลยืนยันตัวบุคคลอื่นใดซึ่งจำเป็นต่อการเข้าถึงคอมพิวเตอร์นั้น)

4. สั่งให้บุคคลใดหยุดการเข้าถึง หยุดการใช้ ไม่อาจเข้าถึง หรือไม่อาจใช้ซึ่งคอมพิวเตอร์นั้น

5. สั่งให้บุคคลซึ่งมีเหตุอันควรสงสัยได้ว่าได้ใช้คอมพิวเตอร์นั้นในการเชื่อมต่อสำหรับการกระทำความผิด หรือบุคคลที่มีเหตุอันควรเชื่อได้ว่ารู้หรือสามารถเข้าถึงรหัสผู้ใช้ รหัสผ่าน หรือข้อมูลยืนยันตัวบุคคลอื่นใดซึ่งจำเป็นต่อการเข้าถึงคอมพิวเตอร์นั้น เพื่อให้ความช่วยเหลือในการเข้าถึง (รวมถึงความช่วยเหลือผ่านการจัดหาให้ซึ่งรหัสผู้ใช้ รหัสผ่าน หรือข้อมูลยืนยันตัวบุคคลอื่นใดซึ่งจำเป็นต่อการเข้าถึงคอมพิวเตอร์นั้น) หรือให้ความช่วยเหลือในการป้องกันบุคคลใดบุคคลหนึ่ง (นอกจากเจ้าพนักงานตำรวจหรือผู้ซึ่งได้รับมอบอำนาจ) มิให้เข้าถึง หรือใช้คอมพิวเตอร์ รวมถึงช่วยเหลือในการเปลี่ยนแปลงรหัสผู้ใช้ รหัสผ่าน หรือข้อมูลยืนยันตัวบุคคลอื่นใดซึ่งจำเป็นต่อการเข้าถึงคอมพิวเตอร์นั้น

มาตรา 39 (2B)แห่ง Criminal Procedure Codeของสาธารณรัฐสิงคโปร์ มีการแก้ไขเพิ่มเติมเมื่อปี พ.ศ.2561 ได้ขยายอำนาจของเจ้าพนักงานตำรวจหรือผู้ซึ่งได้รับมอบอำนาจไปในกรณีที่ทราบว่าคอมพิวเตอร์ดังกล่าวตั้งอยู่นอกสาธารณรัฐสิงคโปร์หรือไม่ทราบว่าคอมพิวเตอร์ดังกล่าวจะ

ตั้งอยู่ภายในหรือนอกสาธารณรัฐสิงคโปร์ก็ตาม เจ้าพนักงานตำรวจหรือผู้ซึ่งได้รับมอบอำนาจตามกฎหมายอาจใช้อำนาจดังกล่าวมาข้างต้นเพื่อจัดการคอมพิวเตอร์หรือข้อมูลซึ่งจัดเก็บภายในหรือสามารถได้มาโดยคอมพิวเตอร์นั้น หากเจ้าของเครื่องคอมพิวเตอร์นั้นยินยอมในการใช้อำนาจดังกล่าวหรือปรากฏเหตุอย่างหนึ่งอย่างใดตามที่กฎหมายกำหนดระหว่างการเข้าถึงคอมพิวเตอร์ผ่านการใช้อำนาจสืบสวนสอบสวนตามบทบัญญัติของกฎหมาย

ในเรื่องของข้อมูลซึ่งถูกเข้ารหัสเพื่อป้องกันการเข้าถึง **Criminal Procedure Code มาตรา40** ได้บัญญัติอำนาจในการเข้าถึงข้อมูลการถอดรหัส (Power to Access DecryptyionInformation)ไว้โดยละเอียด โดยให้กำหนดให้พนักงานอัยการมีอำนาจออกคำสั่งให้เจ้าพนักงานตำรวจหรือผู้ซึ่งได้รับมอบอำนาจใช้อำนาจตามมาตรา 39 เพื่อประโยชน์ในการสืบสวนสอบสวนความผิดที่สามารถจับกุมได้ ในการเข้าถึงข้อมูล รหัส (Code) หรือเทคโนโลยีซึ่งสามารถแปลงหรือถอดรหัสข้อมูลให้อยู่ในรูปซึ่งสามารถอ่านได้ และอยู่ในรูปแบบที่สามารถเข้าใจได้หรือข้อความอักษร (Retransforming ot Unscrambling Encrypted Data into Readable and Comprehensible Format or Text) รวมถึงให้เจ้าพนักงานตำรวจหรือผู้ซึ่งได้รับมอบอำนาจเรียกให้บุคคลใดซึ่งมีเหตุควรสงสัยว่าใช้คอมพิวเตอร์ในการเชื่อมต่อกับการกระทำความผิดหรือในทำนองเช่นว่านั้น หรือเป็นผู้มีหน้าที่ดูแลหรือเป็นผู้เกี่ยวข้องกับการดำเนินงานของคอมพิวเตอร์นั้นให้ความช่วยเหลือทางเทคนิคหรือความช่วยเหลืออย่างอื่นตามสมควรเพื่อดำเนินการดังกล่าว รวมไปถึงมีอำนาจเรียกให้บุคคลใดซึ่งมีเหตุอันควรสงสัยได้ว่าครอบครองข้อมูลการถอดรหัส (Decryption Information)อนุญาตให้เจ้าพนักงานตำรวจหรือผู้ซึ่งได้รับมอบอำนาจเข้าถึงข้อมูลการถอดรหัสนั้นเท่าที่จำเป็นต่อการถอดรหัสข้อมูลใดๆที่ต้องการเพื่อประโยชน์ในการสืบสวนสอบสวน (สำหรับต้นฉบับบทบัญญัติ Computer Misuse Act และ Criminal Procedure Code ในส่วนที่เกี่ยวข้อง โปรดดูเพิ่มเติมในภาคผนวก ก)

แนวทางเพิ่มประสิทธิภาพการดำเนินคดีอาชญากรรมคอมพิวเตอร์

เมื่อระบบยุติธรรมของไทยเป็นแบบกล่าวหาเป็นหลักผู้กล่าวหา (โจทก์) มีหน้าที่ในการนำเสนอพยานหลักฐานต่อศาลด้วยการค้นหาความจริงผ่านการสอบสวนรวบรวมพยานหลักฐานที่เกี่ยวข้อง ซึ่งต้องเป็นพยานหลักฐานที่ต้องเกิดขึ้นโดยชอบด้วยกฎหมายและได้มาโดยชอบด้วยกฎหมาย เพื่อพิสูจน์ให้ศาลรับฟังมีน้ำหนักพ้นข้อสงสัยอันสมควร (Beyond Reasonable Doubt) น่าเชื่อได้ว่าจำเลยเป็นผู้กระทำความผิดตามที่โจทก์กล่าวหาจริง มิฉะนั้นศาลจำต้องยกประโยชน์แห่งความสงสัยให้แก่จำเลยตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา227 วรรคสอง ตามหลัก Presumption of Innocence ดังที่ได้กล่าวมาในบทที่ 2 ประสิทธิภาพในการดำเนินคดีอาญาซึ่งรวมถึงคดีอาชญากรรมคอมพิวเตอร์จึงขึ้นอยู่กับปัจจัยความเพียงพอและความน่าเชื่อถือของพยานหลักฐานในคดี โดยผู้บังคับใช้กฎหมายที่เกี่ยวข้องกับการจัดการพยานหลักฐานเพื่อนำเข้าสู่การพิจารณาคดีในศาลอันได้แก่ เจ้าพนักงานสืบสวน พนักงานสอบสวน ผู้ตรวจพิสูจน์หลักฐาน และพนักงานอัยการ ต่างมีบทบาทสำคัญในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ซึ่งจากการสัมภาษณ์เชิงลึกสภาพปัญหาในการปฏิบัติงานของบุคลากรผู้เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ดังที่ได้กล่าวอ้างอิงไว้ในบทที่ 3

และนำมาวิเคราะห์ปัจจัยการเกิดของสภาพปัญหาในตอนต้นของบทนี้ พิจารณาประกอบกับแนวทางพัฒนาประสิทธิภาพในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ที่น่าสนใจของประเทศสิงคโปร์ ผู้วิจัยเห็นว่า มีแนวทางในการเพิ่มประสิทธิภาพในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ของประเทศไทยดังนี้

1. แนวทางด้านบุคลากร

สำนักงานตำรวจแห่งชาติและสำนักงานอัยการสูงสุดสุดเป็นหน่วยงานในกระบวนการยุติธรรมทางอาญาที่มีอำนาจหน้าที่โดยตรงเกี่ยวข้องกับการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ควรกำหนดยุทธศาสตร์ด้านบริหารงานบุคคลเพื่อแก้ไขปัญหาการขาดแคลนกำลังเจ้าพนักงานซึ่งมีความรู้ ความถนัดในงานสืบสวน งานสอบสวน งานตรวจพิสูจน์ทางนิติคอมพิวเตอร์ และงานนำสืบพยานหลักฐานคดีอาชญากรรมคอมพิวเตอร์ ซึ่งปัญหาด้านการขาดแคลนกำลังเจ้าพนักงานผู้ปฏิบัติงานนี้ไม่อาจแก้ไขได้ด้วยการบรรจุปริมาณเจ้าหน้าที่เพิ่มขึ้นเพียงอย่างเดียว แต่เกี่ยวพันโดยตรงกับพัฒนาบุคคลากรที่ปฏิบัติงานในปัจจุบันให้เกิดความรู้ความเข้าใจในพยานหลักฐานที่เกี่ยวข้องกับการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ทั้งพยานหลักฐานที่อยู่ในรูปดิจิทัล และพยานหลักฐานแวดล้อมอย่างอื่น เช่น พยานหลักฐานเกี่ยวกับธุรกรรมทางการเงิน เป็นต้น ซึ่งเมื่อพิจารณาแนวโน้มปริมาณงานคดีอาชญากรรมคอมพิวเตอร์ที่สูงขึ้นไปตามปริมาณการเข้าใช้งานระบบคอมพิวเตอร์ การพัฒนาความรู้ของผู้ปฏิบัติงานรูปแบบดั้งเดิมด้วยในรูปการจัดฝึกอบรมความรู้ในหรือนอกสถานที่แม้ยังคงมีความจำเป็น แต่อาจไม่เพียงพอต่อความต้องการของผู้ปฏิบัติงานเนื่องจากโอกาสได้รับการอบรมขึ้นอยู่กับความเพียงพอของงบประมาณ อีกทั้งบุคลากรบางส่วนแม้ว่าปัจจุบันจะยังไม่ได้รับผิดชอบงานคดีอาชญากรรมคอมพิวเตอร์โดยตรงแต่มีความสนใจด้านคดีอาชญากรรมคอมพิวเตอร์และมีแนวโน้มที่อาจเปลี่ยนแปลงสายงานในอนาคตมีจำนวนไม่น้อย ดังนั้นจึงควรจัดให้มีช่องทางการอบรมความรู้บนแหล่งข้อมูลเปิดที่น่าเชื่อถือ โดยหลักสูตรบนสื่ออิเล็กทรอนิกส์ (E-learning) ของ INTERPOL ครอบคลุมหัวข้อที่หลากหลายทั้งงานสืบสวน สอบสวน การตรวจพิสูจน์ทางดิจิทัล และการดำเนินคดีกับผู้กระทำความผิดอาชญากรรมทางไซเบอร์ อันเป็นความรู้ทั้งในระดับหลัก คือ ความรู้เฉพาะงานแต่ละงาน และความรู้ระดับรอง คือ ความรู้ในภาพรวมของงานต่างสาขาที่เกี่ยวข้อง ซึ่งหน่วยงานรัฐของไทยสามารถเข้าใช้งานบนเว็บไซต์ของ INTERPOL ได้ผ่านช่องทางการร้องขอผ่านกองการต่างประเทศ สำนักงานตำรวจแห่งชาติซึ่งมีฐานะเป็นสำนักงานกลางแห่งชาติของ INTERPOL (NCB)ทั้งนี้ แม้ว่าหลักสูตรออนไลน์ดังกล่าวจะนำเสนอเป็นภาษาอังกฤษ แต่หน่วยงานของรัฐที่เกี่ยวข้องสามารถให้บุคลากรของตนที่มีความเชี่ยวชาญด้านภาษานำหลักสูตรดังกล่าวมาปรับปรุงเป็นภาษาไทยประกอบเพื่อความเข้าใจต่อไป ซึ่งผู้วิจัยเห็นว่าโรงเรียนนายร้อยตำรวจเป็นหน่วยงานที่เหมาะสมในการรวบรวมแหล่งความรู้จาก INTERPOL กระจายสู่นักเรียนนายร้อย

ตำรวจรุ่นใหม่ๆรวมไปถึงเจ้าพนักงานตำรวจ และเจ้าพนักงานในหน่วยงานยุติธรรมอื่นที่เกี่ยวข้องได้เป็นอย่างดี

2. แนวทางด้านอุปกรณ์เครื่องมือสำหรับงานนิติคอมพิวเตอร์

ในการแก้ไขอุปสรรคด้านการขาดแคลนอุปกรณ์เครื่องมือ และซอฟท์แวร์ที่ใช้ในการตรวจพิสูจน์พยานหลักฐานทางดิจิทัล หน่วยงานที่เกี่ยวข้องควรมีการวิเคราะห์แผนการปฏิบัติงานด้านการตรวจพิสูจน์ว่ามีความจำเป็นต้องใช้อุปกรณ์เครื่องมือ และซอฟท์แวร์ที่ต้องจัดซื้ออย่างไร ซึ่งในทางปฏิบัติเนื่องจากอุปกรณ์เครื่องมือ และซอฟท์แวร์ที่จัดซื้อจากต่างประเทศมีราคาแพง และยังมีค่าใช้จ่ายในการได้รับอนุญาตสิทธิในการใช้ตามกำหนดระยะเวลาของผู้ผลิต จึงเป็นไปไม่ได้ที่จะสามารถจัดซื้ออุปกรณ์เครื่องมือ และซอฟท์แวร์ใช้ในการตรวจพิสูจน์พยานหลักฐานทางดิจิทัลในทุกพื้นที่ของการปฏิบัติงาน แต่ควรต้องมีการวางแผนจัดซื้อด้วยการรวบรวมสถิติปริมาณงานประกอบกับความซับซ้อนของงาน โดยหากงานส่วนใดที่สามารถใช้ซอฟท์แวร์จากแหล่งข้อมูลเปิดมาช่วยเหลือในการปฏิบัติงานได้ ก็สมควรนำมาใช้ทดแทนอย่างเป็นทางการ (ซึ่งปัจจุบันมีการใช้งานอย่างแพร่หลายเป็นการทั่วไปโดยผู้ตรวจพิสูจน์ทางนิติคอมพิวเตอร์แล้ว) อย่างไรก็ดี รัฐควรมีการจัดทำการศึกษา วิเคราะห์ และจัดทำข้อเสนอแนะเกี่ยวกับการเลือกใช้ซอฟท์แวร์จากแหล่งข้อมูลเปิดเพื่อช่วยเหลือในงานด้านการตรวจพิสูจน์นิติคอมพิวเตอร์ รวมไปถึงหลักเกณฑ์ที่ผู้ตรวจพิสูจน์พึงปฏิบัติเมื่อใช้ซอฟท์แวร์ดังกล่าว จัดทำโดยหน่วยงานภาครัฐซึ่งมีความน่าเชื่อถือ เช่น กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม หรือสำนักงานตำรวจแห่งชาติ (กองพิสูจน์หลักฐานกลาง) ในลักษณะเช่นเดียวกับการจัดทำเอกสาร “ข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์หลักฐาน Version 1.0” เผยแพร่โดย สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (ออนไลน์, 2560)

3. แนวทางด้านการประสานความร่วมมือของผู้เกี่ยวข้อง

การประสานงานระหว่างเจ้าพนักงานสืบสวน พนักงานสอบสวน และผู้ตรวจพิสูจน์ทางนิติคอมพิวเตอร์ แม้ว่าจะเป็นเจ้าพนักงานสังกัดสำนักงานตำรวจแห่งชาติเช่นเดียวกัน แต่ยังขาดการประสานงานที่เหมาะสมอันเนื่องมาจากระดับความรู้ความเข้าใจด้านพยานหลักฐานดิจิทัลที่แตกต่างกัน ในส่วนนี้ผู้วิจัยเห็นสอดคล้องกับแนวทางที่เฉลิมชนม์ แน่นหนา และคณะ (2555 : 90-91) ที่ได้เสนอให้มีการวางกรอบแนวทางการประสานงานระหว่างหน่วยงานที่ทำหน้าที่ป้องกันและปราบปรามอาชญากรรมบนสื่อออนไลน์ (ในที่นี้หมายถึงเจ้าพนักงานสืบสวนและพนักงานสอบสวน) กับหน่วยงานที่ทำหน้าที่ให้การสนับสนุน (ในที่นี้หมายถึงผู้ตรวจพิสูจน์หลักฐาน) ให้ชัดเจน โดยผู้วิจัยเห็นเพิ่มเติมว่า แนวทางที่จะทำให้การประสานงานระหว่างเจ้าพนักงานสืบสวน พนักงานสอบสวน และผู้ตรวจพิสูจน์ มีประสิทธิภาพมากขึ้น คือ การร่วมกันกำหนดตัวอย่างแนวทางการกำหนดประเด็นและรูปแบบการร้องขอให้มีการตรวจพิสูจน์พยานหลักฐานทางดิจิทัลของพนักงานสอบสวนที่ควรจะเป็นให้

เหมาะสมกับประเภทของฐานความผิดในคดี เพื่อให้การปฏิบัติงานของผู้ตรวจพิสูจน์มีกรอบการดำเนินการที่ไม่กว้างเกินความจำเป็น เข้าใจในวัตถุประสงค์การตรวจพิสูจน์ ประหยัดเวลาและทรัพยากรทั้งบุคลากรและเครื่องมือที่ใช้ในการดำเนินการ นอกจากนี้ ควรมีการกำหนดอภิธานศัพท์ที่สำคัญด้านเทคนิคนิติคอมพิวเตอร์ที่ทำให้ผู้ปฏิบัติงานในแต่ละหน่วยงานมีความเข้าใจที่ถูกต้องสอดคล้องกัน โดยคำนึงถึงมุมมองด้านกฎหมายในการหยิบยกไปใช้ในการดำเนินคดีตามฐานความผิดที่กำหนดไว้ในกฎหมายด้วยอีกทั้ง รัฐควรส่งเสริมให้ภาคเอกชนตระหนักรู้ถึงความสำคัญต่อการให้ความร่วมมือกับเจ้าพนักงานในคดีอาชญากรรมคอมพิวเตอร์ และสร้างมาตรการในการช่วยเหลือภาระค่าใช้จ่ายที่เกิดขึ้นจากการให้ความช่วยเหลือตามคำร้องขอของเจ้าพนักงานตามความเหมาะสม เพื่อให้ภาคเอกชนให้ความช่วยเหลือในปฏิบัติหน้าที่ของเจ้าพนักงานอย่างเต็มกำลังและด้วยความเต็มใจ

4. แนวทางด้านกฎหมาย

ผู้วิจัยเห็นว่า แม้ปัจจุบันจะมีกฎหมายหลายฉบับที่เกี่ยวข้องกับการกำหนดความผิดซึ่งมีการใช้คอมพิวเตอร์เป็นเครื่องมือ หรือการกระทำความผิดต่อตัวระบบคอมพิวเตอร์ก็ตาม แต่ลักษณะที่กฎหมายต่างฉบับกล่าวถึงอำนาจหน้าที่ในการดำเนินคดีเฉพาะประเภท และเฉพาะเจ้าพนักงานพิเศษที่แต่งตั้งตามกฎหมายนั้นๆ จึงอาจเกิดความไม่ชัดเจนบางประการในกรณีที่ความผิดที่เกิดขึ้นมีความเกี่ยวพันกับกฎหมายหลายฉบับ รวมถึงบทบัญญัติในกฎหมายปัจจุบันยังไม่ครอบคลุมถึงวิธีการในการแสวงหาพยานหลักฐานด้วยเทคโนโลยีใหม่บนอุปกรณ์ดิจิทัล ซึ่งผู้วิจัยมีความเห็นต่อยอดจากความเห็นของ เฉลิมชนม์ แน่นหนา และคณะ (2555 : 90-91) ที่เสนอให้การแก้ไขกฎหมายต้องมีความชัดเจนระหว่างการกระทำความผิดอาญาตามประมวลกฎหมายอาญาหรือกฎหมายอื่นที่มีโทษทางอาญาที่ได้กระทำผ่านคอมพิวเตอร์ กับการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 กล่าวคือ ผู้วิจัยเห็นว่า ปัจจุบันในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในศาลยุติธรรม (ไม่รวมศาลชำนัญพิเศษ หรือแผนกคดีพิเศษอื่น) ใช้หลักเกณฑ์การสอบสวนและการพิจารณาคดีตามประมวลกฎหมายวิธีพิจารณาความอาญาซึ่งประกาศใช้มาเป็นระยะเวลาอันยาวนานเป็นหลัก และยังไม่มีบทบัญญัติว่าด้วยอำนาจของเจ้าพนักงานสืบสวนและพนักงานสอบสวนในการรวบรวมพยานหลักฐานดิจิทัล และหลักเกณฑ์การรับฟังพยานหลักฐานดิจิทัลโดยตรง ผู้วิจัยเห็นสมควรนำแนวทางบทบัญญัติตาม“Computer Misuse Act (Chapter 50A) และ Criminal Procedure Code(Chapter 68) ของสาธารณรัฐสิงคโปร์มาเป็นแนวทางในการปรับปรุงกฎหมายวิธีพิจารณาความอาญาของไทย เพื่อแก้ไขปัญหาความคลุมเครือในการใช้อำนาจบางประการของเจ้าพนักงาน เช่น การใช้วิธีทางเทคนิคบางประการเพื่อแสวงหารหัสผ่านที่เจ้าของอุปกรณ์กำหนดใช้เพื่อป้องกันการเข้าถึงข้อมูลคอมพิวเตอร์ รวมถึงการเปลี่ยนแปลงมาตรการป้องกันการเข้าถึงโดยเฉพาะสำหรับอุปกรณ์ดิจิทัลหรือการใช้งานโปรแกรมบางอย่างเพื่อป้องกันและหยุดยั้งไม่ให้ผู้หนึ่งผู้ใดเข้าถึงข้อมูลเพื่อทำลายหรือเปลี่ยนแปลงพยานหลักฐานด้วยเทคนิคการควบคุมระยะทางไกลได้ และผู้วิจัยเห็นสอดคล้องกับศุทธดา วัฒนวิเชียร (2554 : 27) ที่ว่าในส่วนของการแก้ไข

บทบัญญัติเกี่ยวกับพยานหลักฐานดิจิทัลนั้นควรผ่อนปรนไม่นำหลักการรับฟังพยานบอกเล่ามาใช้กับการรับฟังพยานหลักฐานในรูปข้อมูลอิเล็กทรอนิกส์อย่างเคร่งครัดเนื่องจากลักษณะพิเศษของข้อมูลอิเล็กทรอนิกส์ที่มีการทำสำเนาได้โดยง่ายและสำเนาก็จะมีความถูกต้องตรงกับต้นฉบับจนแยกไม่ออก โดยควรให้ความสำคัญกับวิธีการรับรองความถูกต้องของข้อมูลอิเล็กทรอนิกส์เป็นสำคัญ

อนึ่งผู้วิจัยมีความเห็นต่างจาก เฉลิมชนม์ แน่นหนา และคณะ (2555 : 90-91) ในส่วนที่เสนอให้มีการจัดตั้งศาลชำนัญพิเศษเพื่อพิจารณาคดีอาชญากรรมคอมพิวเตอร์ เนื่องจากผู้วิจัยเห็นว่าปัจจุบันคอมพิวเตอร์ รวมถึงอุปกรณ์ดิจิทัลเช่นโทรศัพท์สมาร์ทโฟน ถูกนำไปใช้ก่ออาชญากรรมหรือจัดเก็บพยานหลักฐานการกระทำความผิดหลากหลายประเภท หากมีการจัดตั้งศาลชำนัญพิเศษโดยเฉพาะอาจมีข้อถกเถียงเรื่องอำนาจศาลในกรณีที่เกี่ยวพันกับกฎหมายที่พิจารณาโดยศาลชำนัญพิเศษเฉพาะอื่น เช่น ศาลอาญาแผนกคดีค้ามนุษย์ หรือ ศาลทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ เป็นต้น แต่ผู้วิจัยเห็นว่า บุคลากรของสำนักงานศาลยุติธรรมมีความจำเป็นต้องพัฒนาความรู้ความเข้าใจด้านดิจิทัล เช่นเดียวกับเจ้าพนักงานในหน่วยงานยุติธรรมอื่นเพื่อสร้างความพร้อมรองรับปริมาณงานคดีอาญาที่มีคอมพิวเตอร์เข้าไปเกี่ยวข้อง โดยอาจมีการแต่งตั้งผู้เชี่ยวชาญด้านนิติคอมพิวเตอร์ประจำศาลเพื่อเป็นที่ปรึกษาแก่ผู้พิพากษาที่พิจารณาคดีในคดีซึ่งมีความซับซ้อนยุ่งยากเป็นกรณีพิเศษ

สรุป

การศึกษาในบทที่ 4 เพื่อตอบวัตถุประสงค์การวิจัยข้อที่ 2 เพื่อวิเคราะห์ปัจจัยที่ก่อให้เกิดสภาพปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในปัจจุบันและเพื่อตอบวัตถุประสงค์การวิจัยข้อที่ 3 เพื่อเสนอแนะแนวทางเพิ่มประสิทธิภาพการดำเนินคดีอาชญากรรมคอมพิวเตอร์

ผลการศึกษาที่ตอบวัตถุประสงค์การวิจัยข้อที่ 2 สรุปได้ว่า จากการสัมภาษณ์เชิงลึกเจ้าพนักงานผู้ทรงคุณวุฒิด้านการสืบสวนสอบสวน การตรวจพิสูจน์ทางนิติคอมพิวเตอร์ และการดำเนินคดีอาชญากรรมคอมพิวเตอร์ และการทบทวนวรรณกรรมที่เกี่ยวข้อง พบปัจจัยก่อให้เกิดสภาพปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในปัจจุบันที่สำคัญประการแรก คือ ปัจจัยด้านบุคลากร ซึ่งกลุ่มผู้ตรวจพิสูจน์มีสาเหตุของปัญหาจากจำนวนผู้ปฏิบัติงานด้านนิติคอมพิวเตอร์ที่สามารถจัดทำรายงานการตรวจพิสูจน์ไม่เพียงพอ ส่วนกลุ่มเจ้าพนักงานสืบสวน พนักงานสอบสวน และพนักงานอัยการ พบว่ามีปัญหาจากการขาดความรู้ด้านเทคนิคคอมพิวเตอร์และนิติคอมพิวเตอร์ในการปฏิบัติงาน ปัจจัยประการที่สองคือ ในส่วนของกลุ่มผู้ตรวจพิสูจน์หลักฐานพบปัจจัยปัญหาด้านนิติคอมพิวเตอร์จากความขาดแคลนเครื่องมืออุปกรณ์และซอฟท์แวร์ที่ใช้ในงานตรวจพิสูจน์นิติคอมพิวเตอร์ที่ต้องจัดซื้อจากต่างประเทศ และผู้ตรวจพิสูจน์หลักฐานมักเลือกใช้ซอฟท์แวร์ที่ใช้ในการตรวจพิสูจน์บางรายการมีเผยแพร่ให้ดาวน์โหลดใช้โดยไม่มีค่าใช้จ่ายจากแหล่งข้อมูล

เปิดมาเสริมควบคู่ไปกับซอฟท์แวร์ที่มีลิขสิทธ์หรือแม้แต่ใช้ทดแทน โดยที่ยังไม่มีการตกผลึกเชิงวิชาการถึงความเหมาะสมและความน่าเชื่อถือของซอฟท์แวร์ดังกล่าว รวมถึงแนวทางปฏิบัติที่ดีเมื่อผู้ตรวจพิสูจน์ต้องใช้นำซอฟท์แวร์ฟรีเหล่านั้นมาใช้ในการตรวจพิสูจน์พยานหลักฐานในคดี โดยปัจจัยสองประการแรกที่กล่าวมานี้เกี่ยวพันกับประเด็นด้านงบประมาณของภาครัฐเพื่อการแก้ปัญหา ปัจจัยประการที่สามคือ เรื่องความร่วมมือระหว่างเจ้าพนักงานในหน่วยงานยุติธรรมทางอาญาด้วยกันในเรื่องการประสานงานระหว่างเจ้าพนักงานสืบสวนหรือพนักงานสอบสวน กับผู้ตรวจพิสูจน์ และความร่วมมือที่เจ้าพนักงานแสวงหาจากผู้ประกอบการภาคเอกชน และปัจจัยที่ก่อให้เกิดสภาพปัญหาประการสุดท้าย ซึ่งเป็นปัจจัยที่กระทบต่อความเชื่อมั่นและการใช้อำนาจของผู้ปฏิบัติงานด้านอาชญากรรมคอมพิวเตอร์ คือ ปัจจัยด้านกฎหมาย ซึ่งพบว่าตามประมวลกฎหมายวิธีพิจารณาความอาญา หรือกฎหมายพิเศษอื่นที่เกี่ยวกับการดำเนินคดีอาญาบัญญัติหลักเกณฑ์ด้านการสอบสวน การรวบรวม และการรับฟังพยานหลักฐานดิจิทัลไม่ครอบคลุมประเด็นความก้าวหน้าทางเทคโนโลยีของอุปกรณ์ดิจิทัลที่มุ่งปิดกั้นและสร้างความเป็นส่วนตัวของผู้เป็นเจ้าของข้อมูลคอมพิวเตอร์ซึ่งใช้เป็นพยานหลักฐาน

สำหรับผลการศึกษาที่ตอบวัตถุประสงค์การวิจัยข้อที่ 3 นั้น พบว่าแนวทางการเพิ่มประสิทธิภาพในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ซึ่งจะเป็นการบรรเทาหรือแก้ไขปัญหาที่พบระหว่างการปฏิบัติงานของเจ้าพนักงานที่เกี่ยวข้อง ประกอบไปด้วย แนวทางด้านบุคลากร ซึ่งสำนักงานตำรวจแห่งชาติและสำนักงานอัยการสูงสุด ควรกำหนดยุทธศาสตร์การบริหารงานบุคคลทั้งในเรื่องอัตรากำลัง และการพัฒนาความรู้ความสามารถในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ที่เหมาะสม โดยสมควรนำแนวทางการสร้างหลักสูตรบนสื่ออิเล็กทรอนิกส์ (E-Learning) ตามแนวทางที่ INTERPOL – IGCI ของสาธารณรัฐสิงคโปร์ดำเนินการอยู่มาปรับใช้ รวมถึงดำเนินการเพื่อส่งเสริมให้เจ้าพนักงานของรัฐผู้ปฏิบัติงานด้านอาชญากรรมคอมพิวเตอร์สามารถเข้าศึกษาเรียนรู้หลักสูตรดังกล่าวของ INTERPOL – IGCI ตามหลักเกณฑ์เงื่อนไขที่กำหนด เพื่อขยายฐานการเรียนรู้และข้ามพ้นสภาพการขาดแคลนงบประมาณในการจัดฝึกอบรม แนวทางด้านอุปกรณ์เครื่องมือสำหรับงานนิติคอมพิวเตอร์ โดยการวางแผนจัดซื้ออุปกรณ์เครื่องมือและซอฟท์แวร์ ด้วยการรวบรวมสถิติปริมาณงานประกอบกับความซับซ้อนของงาน หากงานส่วนใดที่สามารถใช้ซอฟท์แวร์จากแหล่งข้อมูลเปิดมาช่วยเหลือในการปฏิบัติงานได้ ก็สมควรนำมาใช้ทดแทนอย่างเป็นทางการ โดยรัฐควรมีการจัดทำการศึกษา วิเคราะห์ และจัดทำข้อเสนอแนะเกี่ยวกับการเลือกใช้ซอฟท์แวร์จากแหล่งข้อมูลเปิดเพื่อช่วยเหลือในงานด้านการตรวจพิสูจน์นิติคอมพิวเตอร์ รวมไปถึงหลักเกณฑ์ที่ผู้ตรวจพิสูจน์พึงปฏิบัติเมื่อใช้ซอฟท์แวร์ดังกล่าว แนวทางด้านการประสานความร่วมมือของผู้เกี่ยวข้องคือ การร่วมกันกำหนดตัวอย่างแนวทางการกำหนดประเด็นและรูปแบบการร้องขอให้มีการตรวจพิสูจน์พยานหลักฐานทางดิจิทัลของพนักงานสอบสวนที่ควรจะเป็นให้เหมาะสมกับประเภทของฐานความผิดในคดี และการ

สร้างกลไกส่งเสริมให้ผู้ประกอบการภาคเอกชนเต็มใจให้ความร่วมมือเมื่อมีการร้องขอข้อมูลจากเจ้าพนักงานของรัฐ และแนวทางด้านกฎหมาย ซึ่งเห็นสมควรนำแนวทางบทบัญญัติตาม“Computer Misuse Act (Chapter 50A) และCriminal Procedure Code(Chapter 68) ของสาธารณรัฐสิงคโปร์มาเป็นแนวทางในการปรับปรุงกฎหมายวิธีพิจารณาความอาญาของไทย เพื่อแก้ไขปัญหาความชอบด้วยกฎหมายในการใช้อำนาจบางประการของเจ้าพนักงานในการรวบรวมพยานหลักฐานดิจิทัล และหลักเกณฑ์การรับฟังพยานหลักฐานดิจิทัล เพื่อให้สอดคล้องกับเทคโนโลยีด้านคอมพิวเตอร์ที่พัฒนาอย่างต่อเนื่องไม่หยุดยั้ง

บทที่ 5
สรุปและข้อเสนอแนะ

การศึกษาวิจัยเรื่องแนวทางเพิ่มประสิทธิภาพการดำเนินคดีอาชญากรรมคอมพิวเตอร์ เป็นการวิจัยเชิงคุณภาพ ผู้วิจัยได้กำหนดวัตถุประสงค์การวิจัยไว้ 3 ข้อ ประกอบด้วย

วัตถุประสงค์การวิจัยข้อที่ 1เพื่อศึกษาสภาพปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ที่พบในชั้นการสืบสวนสอบสวน รวบรวมพยานหลักฐาน จนถึงขั้นตอนการนำเสนอพยานหลักฐานในชั้นพิจารณาของศาล

วัตถุประสงค์การวิจัยข้อที่ 2 เพื่อวิเคราะห์ปัจจัยที่ก่อให้เกิดสภาพปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในปัจจุบัน

วัตถุประสงค์การวิจัยข้อที่ 3เพื่อเสนอแนะแนวทางเพิ่มประสิทธิภาพการดำเนินคดีอาชญากรรมคอมพิวเตอร์

ในการดำเนินการวิจัย ผู้วิจัยใช้การรวบรวมข้อมูลทั้งข้อมูลทุติยภูมิจากหลากหลายแหล่งข้อมูลที่เกี่ยวข้อง และรวบรวมข้อมูลปฐมภูมิจากการสัมภาษณ์เชิงลึกผู้ทรงคุณวุฒิด้านการสืบสวนสอบสวน การตรวจพิสูจน์ทางนิติคอมพิวเตอร์ และการดำเนินคดีอาชญากรรมคอมพิวเตอร์ รวมจำนวน 12 ท่าน เพื่อให้ข้อมูลที่ได้มีความเที่ยงตรงและน่าเชื่อถือ ส่วนการวิเคราะห์ข้อมูลนั้น ผู้วิจัยใช้การวิเคราะห์เนื้อหาเป็นหลัก โดยเมื่อนำข้อมูลที่รวบรวมได้มาจัดระเบียบแล้วนำมาวิเคราะห์สังเคราะห์ ประกอบกับแนวความคิด ทฤษฎีที่เกี่ยวข้อง จนกระทั่งได้แนวทางในการเพิ่มประสิทธิภาพการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ซึ่งในบทที่ 5 นี้ จะนำเสนอ 2 ประเด็น คือ สรุปผลการวิจัยและข้อเสนอแนะเพิ่มเติม จากผลการวิจัยดังนี้

สรุป

ตอบวัตถุประสงค์การวิจัยข้อที่ 1มีรายละเอียดผลการศึกษาโดยสรุปดังนี้

ระบบการดำเนินคดีอาญาของประเทศไทยเป็นระบบที่ผสมผสานระบบกล่าวหา (Inquisitorial System) และระบบไต่สวน (Accusatorial System) มาใช้ในระบบการพิจารณาคดีและการสืบพยาน คู่ความทั้งสองฝ่ายมีหน้าที่แสวงหาพยานหลักฐานมาต่อสู้หักล้างกัน ส่วนศาลจะวางตนเป็นกลางโดยพิจารณาและพิพากษาคดีจากพยานหลักฐานที่ทั้งโจทก์และจำเลยนำสืบมา โดยมีการนำกฎเกณฑ์การห้ามรับฟังพยานหลักฐานบางประเภทมาบังคับใช้เพื่อทำให้พยานหลักฐานที่จะมีน้ำหนักรับฟังในการลงโทษผู้ถูกกล่าวหาเป็นพยานหลักฐานที่น่าเชื่อถือ โดยบุคคลซึ่งถูกกล่าวหาว่ามี

ความผิดอาญามีสิทธิที่จะได้รับการสันนิษฐานไว้ก่อนว่าบริสุทธิ์ตามหลักการสันนิษฐานว่าเป็นผู้บริสุทธิ์ (Presumption of Innocence)ซึ่งเป็นหลักการพื้นฐานที่ได้รับการรับรองตามรัฐธรรมนูญ

แห่งราชอาณาจักรไทย พุทธศักราช 2560 (ออนไลน์, 2562) มาตรา 29 และประมวลกฎหมายวิธีพิจารณาความอาญา (ออนไลน์, 2562) มาตรา 227

คดีอาชญากรรมคอมพิวเตอร์จัดเป็นคดีอาญาประเภทหนึ่งที่ผู้กล่าวหามีหน้าที่นำสืบพยานหลักฐานพิสูจน์ความผิดของผู้ถูกกล่าวหาซึ่งมาตรฐานการพิสูจน์ในคดีอาญา คือ มาตรฐาน “การพิสูจน์พ้นข้อสงสัยตามสมควร” หรือ Proof Beyond Reasonable Doubt โดยโจทก์ผู้ฟ้องคดีมีหน้าที่ต้องพิสูจน์ให้ศาลเห็นได้โดยปราศจากเหตุอันควรสงสัยว่าจำเลยเป็นผู้กระทำผิด ถ้ามีเหตุอันควรสงสัยอย่างใดอย่างหนึ่งว่าจำเลยอาจจะไม่ใช่คนร้ายที่กระทำผิด ให้ยกประโยชน์แห่งความสงสัยนั้นให้แก่จำเลย มาตรฐานการพิสูจน์นี้ปรากฏอยู่ในประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 227 ดังนั้นประสิทธิภาพในการดำเนินคดีกับผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์จนนำไปสู่การได้รับการลงโทษในกระบวนการยุติธรรม จึงขึ้นอยู่กับประสิทธิภาพในการแสวงหาและการรวบรวมพยานหลักฐานที่มีคุณค่าในเชิงพิสูจน์ ไม่ต้องห้ามรับฟังเป็นพยานหลักฐาน รวมถึงการนำเสนอพยานหลักฐานดังกล่าวสามารถร้อยเรียงเชื่อมโยงข้อเท็จจริงได้น่าเชื่อถือจนพ้นข้อสงสัยตามสมควร ซึ่งเจ้าพนักงานในกระบวนการยุติธรรมที่มีบทบาทสำคัญในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ได้แก่ เจ้าพนักงานสืบสวน พนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 (ที่แก้ไขเพิ่มเติม) พนักงานสอบสวน ผู้ตรวจพิสูจน์หลักฐาน พนักงานอัยการ และศาล

จากข้อมูลที่ได้จากการสัมภาษณ์เชิงลึกผู้ทรงคุณวุฒิด้านการสืบสวน การสอบสวน การตรวจพิสูจน์ทางนิติคอมพิวเตอร์ และการดำเนินคดีอาชญากรรมคอมพิวเตอร์ สามารถจำแนกสภาพปัญหาที่เกิดขึ้นในกระบวนการดำเนินคดีอาชญากรรมคอมพิวเตอร์ได้ดังนี้

1. สภาพปัญหาในส่วนของการปฏิบัติหน้าที่เฉพาะบุคคล

1.1 สภาพปัญหาด้านความรู้ความเข้าใจในเทคโนโลยีสมัยใหม่ ซึ่งพบว่าผู้ปฏิบัติงานด้านการสืบสวนสอบสวนและพนักงานอัยการ ยังขาดโอกาสได้รับการฝึกอบรมความรู้ด้านเทคโนโลยีสมัยใหม่และองค์ความรู้ด้านนิติคอมพิวเตอร์เบื้องต้นในการปฏิบัติงาน อันเนื่องมาจากข้อจำกัดด้านงบประมาณนอกจากนี้ ในด้านการอธิบายเกี่ยวกับพยานหลักฐานดิจิทัลในรูปของการรายงานผลการตรวจพิสูจน์หรือการเบิกความในชั้นศาลพบอุปสรรคในเรื่องของคำศัพท์ทางคอมพิวเตอร์ซึ่งบุคลากรในกระบวนการยุติธรรมยังขาดความคุ้นเคย

1.2 สภาพปัญหาด้านเครื่องมืออุปกรณ์ในการทำงาน ซึ่งพบว่า สภาพปัญหาผู้ตรวจพิสูจน์หลักฐานพบนั้นมิใช่เรื่องของการขาดความรู้ความเข้าใจเกี่ยวกับเทคโนโลยีทางคอมพิวเตอร์อย่างบุคลากรกลุ่มอื่น เพราะผู้ตรวจพิสูจน์หลักฐานมีความรู้ด้านนิติคอมพิวเตอร์ในระดับที่ดีอยู่แล้ว แต่ปัญหาที่ผู้ตรวจพิสูจน์พบนั้น เป็นเรื่องของการขาดแคลนงบประมาณเพื่อจัดหาเครื่องมืออุปกรณ์ที่ใช้ตรวจสอบอุปกรณ์ดิจิทัลที่สมัยให้เพียงพอต่อปริมาณงานที่มีแนวโน้มเพิ่มมากขึ้นในปัจจุบัน เนื่องจากซอฟท์แวร์ที่ใช้ในการปฏิบัติงานมักมีราคาสูงและต้องนำเข้าจากต่างประเทศ

1.3 สภาพปัญหาด้านกำลังคน ซึ่งพบว่า จำนวนผู้ตรวจพิสูจน์นิติคอมพิวเตอร์ของหน่วยงานภาครัฐยังไม่เพียงพอต่อปริมาณงานอาชญากรรมคอมพิวเตอร์ในปัจจุบัน ทำให้การตรวจพิสูจน์พยานหลักฐานดิจิทัลเกิดความล่าช้า ซึ่งอาจนำไปสู่การเกิดผลกระทบต่อความสมบูรณ์ของพยานหลักฐานดิจิทัลซึ่งเสี่ยงต่อการสูญหาย เสียหาย หรือปนเปื้อน

1.4 สภาพปัญหาด้านความชัดเจนเกี่ยวกับกฎหมายในการปฏิบัติงาน ซึ่งพบว่าเจ้าพนักงานมีความกังวลเกี่ยวกับอำนาจตามกฎหมายในการรวบรวมพยานหลักฐานดิจิทัลอันเนื่องมาจากสภาพของพัฒนาการด้านเทคโนโลยีสมัยใหม่ที่ข้อมูลคอมพิวเตอร์ของบุคคลมิได้จัดเก็บอยู่ในตัวอุปกรณ์ดิจิทัลเพียงอย่างเดียว เช่น การเก็บข้อมูลในระบบคลาวด์ หรือการใช้วิธีการฟิชชิ่งเพื่อให้ได้มาซึ่งรหัสผ่านระบบคอมพิวเตอร์ของคนร้ายโดยเจ้าหน้าที่ผู้ปฏิบัติงานมีความกังวลว่าอาจนำไปสู่ข้อโต้แย้งเรื่องการได้มาซึ่งพยานหลักฐานโดยมิชอบ หรือพยานหลักฐานที่ได้มาเป็นพยานหลักฐานที่เกิดขึ้นโดยมิชอบ ซึ่งจะส่งผลทำให้พยานหลักฐานที่ได้มานั้นไม่สามารถรับฟังได้ตามกฎหมาย หรือแม้จะรับฟังได้ตามกฎหมาย แต่มีน้ำหนักน่าเชื่อถือน้อย

2. **สภาพปัญหาในส่วนของการปฏิบัติหน้าที่สัมพันธ์กับบุคลากรกลุ่มอื่น**

2.1 ในส่วนของพนักงานสอบสวนและผู้ตรวจพิสูจน์พยานหลักฐาน พบปัญหาการขาดการประสานงานที่เหมาะสมในการกำหนดประเด็นการแสวงหาพยานหลักฐานดิจิทัล โดยการประสานงานด้วยเอกสารหนังสือเพียงอย่างเดียวก่อให้เกิดความไม่ชัดเจนเกี่ยวกับวัตถุประสงค์ของการตรวจสอบเนื่องจากพนักงานสอบสวนมักคุ้นเคยในเรื่องทางนิติศาสตร์แต่ยังขาดความเข้าใจถึงคุณค่าของพยานหลักฐานดิจิทัลแต่ละชิ้นจึงพบข้อขัดข้องในการกำหนดประเด็นตรวจสอบไปยังผู้ตรวจพิสูจน์

2.2 เจ้าพนักงานผู้ปฏิบัติงานสืบสวนและงานสอบสวนพบปัญหาการได้รับความร่วมมือจากผู้ให้บริการอินเทอร์เน็ต ผู้ให้บริการเว็บไซต์ และผู้ให้บริการด้านการเงินการธนาคารในการส่งมอบข้อมูลคอมพิวเตอร์หรือพยานหลักฐานที่เกี่ยวข้องซึ่งอยู่ในความครอบครองของผู้ให้บริการดังกล่าว หรือได้รับผลการดำเนินการตามที่มีการร้องขอในเวลาที่ล่าช้าเกินสมควร

ตอบวัตถุประสงค์การวิจัยข้อที่ 2รายละเอียดผลการศึกษาโดยสรุปดังนี้

ผู้วิจัยได้นำข้อมูลเกี่ยวกับสภาพปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ที่ได้จากการสัมภาษณ์เชิงลึกเจ้าพนักงานผู้ทรงคุณวุฒิดังกล่าวข้างต้นมาจัดระเบียบแล้วนำมาวิเคราะห์ สังเคราะห์ ประกอบกับแนวความคิด ทฤษฎีที่เกี่ยวข้อง สามารถจำแนกปัจจัยที่ก่อให้เกิดสภาพปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ได้ดังนี้

1. ปัจจัยด้านบุคลากร ทั้งปัจจัยในเรื่องของจำนวนผู้ปฏิบัติงานในกลุ่มผู้ตรวจพิสูจน์ที่มีจำนวนผู้ปฏิบัติงานด้านนิติคอมพิวเตอร์ที่สามารถจัดทำรายงานการตรวจพิสูจน์ไม่เพียงพอและปัจจัยในเรื่ององค์ความรู้ ซึ่งผู้ปฏิบัติงานในกลุ่มเจ้าพนักงานสืบสวน พนักงานสอบสวน และ

พนักงานอัยการ ยังขาดความรู้ด้านเทคนิคคอมพิวเตอร์และนิติคอมพิวเตอร์ในระดับที่เพียงพอต่อการปฏิบัติงาน

2. ปัจจัยด้านนิติคอมพิวเตอร์ ซึ่งครอบคลุมเรื่องของความไม่เพียงพอในการจัดหาอุปกรณ์และซอฟท์แวร์เพื่อการตรวจพิสูจน์ และในเรื่องของความน่าเชื่อถือของพยานหลักฐานดิจิทัลที่ได้จากการแก้ไขปัญหาเฉพาะหน้าด้วยการนำซอฟท์แวร์ที่มีเผยแพร่ให้ดาวน์โหลดใช้โดยไม่มีค่าใช้จ่ายจากแหล่งข้อมูลเปิดมาเสริมควบคู่ไปกับซอฟท์แวร์ที่มีลิขสิทธิ์หรือแม้แต่ใช้ทดแทนในบางกรณี

3. ปัจจัยด้านการประสานความร่วมมือ ได้แก่ ปัจจัยด้านความร่วมมือระหว่างเจ้าพนักงานในหน่วยงานยุติธรรมทางอาญาด้วยกัน ในเรื่องการประสานงานระหว่างเจ้าพนักงานสืบสวนหรือพนักงานสอบสวนกับผู้ตรวจพิสูจน์ และความร่วมมือที่เจ้าพนักงานแสวงหาจากผู้ประกอบการภาคเอกชน

4. ปัจจัยด้านกฎหมายซึ่งส่งผลกระทบต่อความเชื่อมั่นและการใช้อำนาจของผู้ปฏิบัติงานด้านอาชญากรรมคอมพิวเตอร์ จากการที่ประมวลกฎหมายวิธีพิจารณาความอาญาหรือกฎหมายพิเศษอื่นที่เกี่ยวกับการดำเนินคดีอาญาบัญญัติหลักเกณฑ์ด้านการสอบสวน การรวบรวมและการรับฟังพยานหลักฐานดิจิทัลไม่ครอบคลุมประเด็นความก้าวหน้าทางเทคโนโลยีของอุปกรณ์ดิจิทัลที่มุ่งปิดกั้นและสร้างความเป็นส่วนตัวของผู้เป็นเจ้าของข้อมูลคอมพิวเตอร์ซึ่งใช้เป็นพยานหลักฐาน

ตอบวัตถุประสงค์การวิจัยข้อที่ 3รายละเอียดผลการศึกษาโดยสรุปดังนี้

แนวทางการเพิ่มประสิทธิภาพในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ซึ่งจะเป็นการบรรเทาหรือแก้ไขปัญหาที่พบระหว่างการปฏิบัติงานของเจ้าพนักงานที่เกี่ยวข้อง ประกอบด้วย

1. แนวทางด้านบุคลากร

แนวทางในการแก้ไขปัญหาจำนวนเจ้าหน้าที่ผู้มีความรู้ความเชี่ยวชาญด้านเทคโนโลยีคอมพิวเตอร์และนิติคอมพิวเตอร์ ด้วยการเพิ่มจำนวนบุคลากรที่มีความรู้ความสามารถเข้าไปในระบบงานภาครัฐ อาจมิใช่แนวทางการแก้ไขปัญหาที่ดีที่สุด เนื่องจากรัฐต้องจัดเตรียมความพร้อมด้านงบประมาณให้เพียงพอต่อการเพิ่มจำนวนเจ้าหน้าที่ของรัฐ ซึ่งอาจกระทำได้ไม่ง่ายนัก เนื่องจากรัฐเองมีความจำเป็นต้องจัดสรรเงินงบประมาณเพื่อการพัฒนาประเทศด้านอื่นๆ ด้วย

ปัจจุบันรูปแบบของอาชญากรรมคอมพิวเตอร์มีหลากหลาย มีทั้งกลุ่มความผิดที่คอมพิวเตอร์เป็นวัตถุหรือเป้าหมายที่ถูกกระทำ เช่น การแฮก ดีดอส สแปม กลุ่มความผิดที่คอมพิวเตอร์ถูกใช้เป็นเครื่องมือเพื่อประกอบอาชญากรรมอย่างอื่น เช่น ฟิชชิ่งสแกมเมอร์หรือการแสวงหาประโยชน์ทางเพศกับเด็กบนโลกออนไลน์ และกลุ่มที่มีการใช้คอมพิวเตอร์เป็นเครื่องมือจัดการกับผลประโยชน์ที่ได้จากอาชญากรรม เช่น การใช้สกุลเงินเข้ารหัส หรือ Cryptocurrency

ในการจัดการกับทรัพย์สินที่ได้มาจากการประกอบอาชญากรรมเพื่อปกปิดตัวของผู้ทำธุรกรรมที่แท้จริง ซึ่งรูปแบบและลักษณะของอาชญากรรมคอมพิวเตอร์ดังที่กล่าวมาข้างต้นนี้ มีแนวโน้มของจำนวนและความซับซ้อนเพิ่มมากขึ้นตามความก้าวหน้าของเทคโนโลยีด้านคอมพิวเตอร์ ดังนั้น แนวทางการเพิ่มประสิทธิภาพด้านบุคลากรผู้มีความรู้ความเชี่ยวชาญในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ที่มีความเป็นไปได้มากที่สุดในขณะที่รัฐยังไม่พร้อมทางด้านงบประมาณในการจัดจ้างบุคลากร และระบบการศึกษายังไม่สามารถผลิตบุคลากรที่มีความรู้ความเชี่ยวชาญด้านนิติคอมพิวเตอร์ได้ทันต่อความต้องการของสังคม คือ แนวทางการพัฒนาความรู้ด้านอาชญากรรมคอมพิวเตอร์ ด้วยการพัฒนาขีดความสามารถของเจ้าหน้าที่ในกระบวนการยุติธรรมซึ่งปฏิบัติหน้าที่เกี่ยวกับการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในปัจจุบัน ให้มีความรู้ความเชี่ยวชาญในการปฏิบัติงานในระดับที่เพียงพอต่อการปฏิบัติงานในความรับผิดชอบของตนและเข้าใจรูปแบบการทำงานของเจ้าพนักงานต่างหน่วยงานให้เกิดการบูรณาการด้านองค์ความรู้มากที่สุด ซึ่งเป็นแนวทางที่ INTERPOL – IGCI ของสาธารณรัฐสิงคโปร์เร่งพัฒนาและดำเนินการอยู่

2. แนวทางด้านอุปกรณ์เครื่องมือสำหรับงานนิติคอมพิวเตอร์

การเลือกใช้ซอฟท์แวร์จากแหล่งข้อมูลเปิดเพื่อช่วยเหลือในงานด้านการตรวจพิสูจน์นิติคอมพิวเตอร์เป็นทางปฏิบัติทั่วไปที่ผู้ตรวจพิสูจน์หลักฐานทางนิติคอมพิวเตอร์ในต่างประเทศนิยมใช้กัน โดยภาครัฐของแต่ละประเทศมีหน้าที่ในการสร้างกลไกในการสร้างความน่าเชื่อถือในพยานหลักฐานที่ได้จากการตรวจพิสูจน์โดยเครื่องมือที่พบในแหล่งข้อมูลเปิด โดยต้องมีการคำนึงถึงหลักการรับฟังพยานหลักฐานตามกฎหมายภายในของแต่ละประเทศ เพื่อหลีกเลี่ยงข้อโต้แย้งเกี่ยวกับความน่าเชื่อถือจากความเห็นของผู้เชี่ยวชาญ หรือพยานหลักฐานที่ได้จากการตรวจพิสูจน์โดยซอฟท์แวร์จากแหล่งข้อมูลเปิด อันจะเป็นแนวทางในการเพิ่มประสิทธิภาพในการดำเนินคดีอาชญากรรมคอมพิวเตอร์

3. แนวทางด้านการประสานความร่วมมือของผู้เกี่ยวข้อง

ในการดำเนินคดีอาญาเพื่อพิสูจน์การกระทำความผิดของผู้ถูกกล่าวหา ต้องอาศัยการปฏิบัติหน้าที่ของเจ้าพนักงานในหลายหน่วยงาน ตั้งแต่ชั้นการสืบสวน การสอบสวนรวบรวมพยานหลักฐาน การตรวจพิสูจน์พยานหลักฐาน และการดำเนินการสืบพยานในชั้นศาล เพื่อแก้ไขปัญหาความไม่เข้าใจในการขอความร่วมมือระหว่างเจ้าพนักงานสังกัดหน่วยงานที่แตกต่างกันเป็นเรื่องที่สำคัญ โดยจะส่งผลเป็นการลดระยะเวลาในการปฏิบัติงานและเพิ่มประสิทธิภาพในการทำงานมากขึ้น และโดยที่การดำเนินคดีอาชญากรรมคอมพิวเตอร์แต่ละคดีต้องอาศัยข้อมูลเกี่ยวกับการใช้บริการอินเทอร์เน็ตข้อมูลการใช้บริการโทรศัพท์ รวมถึงข้อมูลการทำธุรกรรมทางการเงินผ่านช่องทางอิเล็กทรอนิกส์ ซึ่งข้อมูลเหล่านี้อยู่ในความครอบครองของเอกชนผู้ให้บริการ ดังนั้น

แนวทางในการประสานความร่วมมือระหว่างเจ้าพนักงานของรัฐและภาคเอกชน ถือเป็นเรื่องที่สำคัญอย่างมาก

4. แนวทางด้านกฎหมาย

มาตรการในทางกฎหมายถือเป็นเครื่องมือสำคัญในการสร้างความชัดเจนและความชอบธรรมในการปฏิบัติหน้าที่ของเจ้าพนักงานในคดีอาชญากรรมคอมพิวเตอร์ ซึ่งเป็นปัจจัยสำคัญที่จะสร้างความเชื่อมั่นในการปฏิบัติงานของเจ้าพนักงานสืบสวนสอบสวนซึ่งมีบทบาทหลักในการรวบรวมพยานหลักฐานและข้อเท็จจริงในทางคดีเพื่อนำตัวผู้กระทำผิดมาลงโทษ อันเป็นวิถีทางในการเยียวยาความเสียหายให้แก่ผู้เสียหายและสังคม และในอีกทางหนึ่งเพื่อเป็นการคุ้มครองสิทธิของประชาชนผู้ที่อาจได้รับผลกระทบจากการปฏิบัติงานของเจ้าหน้าที่ในระดับที่เหมาะสม

ข้อเสนอแนะ

1. ข้อเสนอแนะเชิงนโยบาย

1.1 หน่วยงานด้านตรวจพิสูจน์หลักฐานควรวางแผนจัดซื้ออุปกรณ์เครื่องมือและซอฟท์แวร์ ด้วยการรวบรวมสถิติปริมาณงานประกอบกับความซับซ้อนของงาน หากงานส่วนใดที่สามารถใช้ซอฟท์แวร์จากแหล่งข้อมูลเปิดมาช่วยเหลือในการปฏิบัติงานได้ ก็สมควรนำมาใช้ทดแทนอย่างเป็นทางการ โดยรัฐควรมีการจัดทำการศึกษา วิเคราะห์ และจัดทำข้อเสนอแนะเกี่ยวกับการเลือกใช้ซอฟท์แวร์จากแหล่งข้อมูลเปิดเพื่อช่วยเหลือในงานด้านการตรวจพิสูจน์นิติคอมพิวเตอร์ รวมไปถึงการกำหนดหลักเกณฑ์หรือข้อปฏิบัติที่เหมาะสมที่ผู้ตรวจพิสูจน์พึงปฏิบัติก่อนการใช้ซอฟท์แวร์จากแหล่งข้อมูลเปิดดังกล่าว

1.2 รัฐควรพิจารณานำแนวทางบทบัญญัติตาม“Computer Misuse Act (Chapter 50A) และ Criminal Procedure Code(Chapter 68) ของสาธารณรัฐสิงคโปร์มาเป็นแนวทางในการปรับปรุงกฎหมายวิธีพิจารณาความอาญาของไทย เพื่อแก้ไขปัญหาความชอบด้วยกฎหมายในการใช้อำนาจบางประการของเจ้าพนักงานในการรวบรวมพยานหลักฐานดิจิทัล และหลักเกณฑ์การรับฟังพยานหลักฐานดิจิทัล เพื่อให้สอดคล้องกับเทคโนโลยีด้านคอมพิวเตอร์ที่พัฒนาอย่างต่อเนื่องไม่หยุดยั้ง

2. ข้อเสนอแนะระดับปฏิบัติการ

2.1 สำนักงานตำรวจแห่งชาติและสำนักงานอัยการสูงสุด ควรกำหนดยุทธศาสตร์การบริหารงานบุคคลทั้งในเรื่องอัตรากำลัง และการพัฒนาความรู้ความสามารถในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ที่เหมาะสม โดยสมควรนำแนวทางการสร้างหลักสูตรบนสื่ออิเล็กทรอนิกส์ (E-Learning) ตามแนวทางที่ INTERPOL – IGCI ของสาธารณรัฐสิงคโปร์ดำเนินการอยู่มาปรับใช้ รวมถึง

ดำเนินการเพื่อส่งเสริมให้เจ้าพนักงานของรัฐผู้ปฏิบัติงานด้านอาชญากรรมคอมพิวเตอร์สามารถเข้าศึกษาเรียนรู้หลักสูตรดังกล่าวของ INTERPOL – IGCI ตามหลักเกณฑ์เงื่อนไขที่กำหนด เพื่อขยายฐานการเรียนรู้และข้ามพ้นสภาพการขาดแคลนงบประมาณในการจัดฝึกอบรมและสร้างการพัฒนาความรู้อย่างยั่งยืน

2.2 หน่วยงานผู้ปฏิบัติงานด้านอาชญากรรมคอมพิวเตอร์ ควรร่วมกันกำหนดตัวอย่างแนวทางการกำหนดประเด็นและรูปแบบการร้องขอให้มีการตรวจพิสูจน์พยานหลักฐานทางดิจิทัลของพนักงานสอบสวนที่ควรจะเป็นให้เหมาะสมกับประเภทของฐานความผิดในคดีและการสร้างกลไกส่งเสริมให้ผู้ประกอบการภาคเอกชนเต็มใจให้ความร่วมมือเมื่อมีการร้องขอข้อมูลจากเจ้าพนักงานของรัฐ

3. ข้อเสนอแนะเพื่อการวิจัยครั้งต่อไป

ผลการวิจัยนี้ สามารถนำไปทำการวิจัยต่อยอดได้ใน 2 ประเด็นหลัก คือ

3.1 ประเด็นแนวทางการประสานความร่วมมือของผู้เกี่ยวข้อง

ผู้วิจัยเห็นสอดคล้องกับแนวทางที่เฉลิมชนม์ แน่นหนา และคณะ (2555 : 90-91) ที่ได้เสนอให้มีการวางกรอบแนวทางการประสานงานระหว่างหน่วยงานที่ทำหน้าที่ป้องกันและปราบปรามอาชญากรรมบนสื่อออนไลน์ (ในที่นี้หมายถึงเจ้าพนักงานสืบสวนและพนักงานสอบสวน) กับหน่วยงานที่ทำหน้าที่ให้การสนับสนุน (ในที่นี้หมายถึงผู้ตรวจพิสูจน์หลักฐาน) ให้ชัดเจน โดยผู้วิจัยเห็นเพิ่มเติมว่า แนวทางที่จะทำให้การประสานงานระหว่างเจ้าพนักงานสืบสวน พนักงานสอบสวนและผู้ตรวจพิสูจน์ มีประสิทธิภาพมากขึ้น คือ การร่วมกันกำหนดตัวอย่างแนวทางการกำหนดประเด็นและรูปแบบการร้องขอให้มีการตรวจพิสูจน์พยานหลักฐานทางดิจิทัลของพนักงานสอบสวนที่ควรจะเป็นให้เหมาะสมกับประเภทของฐานความผิดในคดี เพื่อให้การปฏิบัติงานของผู้ตรวจพิสูจน์มีกรอบการดำเนินการที่ไม่กว้างเกินความจำเป็น เข้าใจในวัตถุประสงค์การตรวจพิสูจน์ ประหยัดเวลาและทรัพยากรทั้งบุคลากรและเครื่องมือที่ใช้ในการดำเนินการ ซึ่งในเรื่องนี้จำเป็นต้องมีการต่อยอดทำการศึกษาถึงแนวทางความร่วมมือที่เหมาะสม โดยควรศึกษาแนวทางที่มีการดำเนินการในต่างประเทศซึ่งผู้วิจัยเห็นว่าควรเป็นประเทศที่มีลักษณะโครงสร้างของหน่วยงานและอำนาจหน้าที่ของบุคลากรในกระบวนการยุติธรรมทางอาญาที่คล้ายคลึงกับประเทศไทยมากที่สุด เพื่อให้ได้ผลการศึกษาที่จะสามารถนำมาปรับใช้ได้ในระบบยุติธรรมของประเทศไทย

3.2 ประเด็นแนวทางการพัฒนากฎหมาย

แม้ปัจจุบันจะมีกฎหมายหลายฉบับเกี่ยวข้องกับการกำหนดความผิดซึ่งมีการใช้คอมพิวเตอร์เป็นเครื่องมือ หรือการกระทำความผิดต่อตัวระบบคอมพิวเตอร์ก็ตาม แต่ลักษณะที่กฎหมายต่างฉบับได้บัญญัติถึงอำนาจหน้าที่ในการดำเนินคดีเฉพาะประเภท และกำหนดให้มีเจ้าพนักงานที่แต่งตั้งเพื่อปฏิบัติตามกฎหมายนั้นๆเป็นการเฉพาะ ก่อให้เกิดความไม่ชัดเจนบางประการในกรณีที่ความผิดที่เกิดขึ้นมีความเกี่ยวพันกับกฎหมายหลายฉบับ รวมถึงบทบัญญัติ

ในกฎหมายปัจจุบันยังไม่ครอบคลุมถึงวิธีการในการแสวงหาพยานหลักฐานด้วยเทคโนโลยีใหม่บนอุปกรณ์ดิจิทัล ซึ่งผู้วิจัยมีความเห็นต่อยอดจากความเห็นของ เฉลิมชนม์ แน่นหนา และคณะ (2555 : 90-91) ที่เสนอให้การแก้ไขกฎหมายต้องมีความชัดเจนระหว่างการกระทำความผิดอาญาตามประมวลกฎหมายอาญาหรือกฎหมายอื่นที่มีโทษทางอาญาที่ได้กระทำผ่านคอมพิวเตอร์ กับการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 กล่าวคือ ผู้วิจัยเห็นว่า ปัจจุบันในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในศาลยุติธรรม (ไม่รวมศาลชำนัญพิเศษ หรือแผนกคดีพิเศษอื่น) ใช้หลักเกณฑ์การสอบสวนและการพิจารณาคดีตามประมวลกฎหมายวิธีพิจารณาความอาญาซึ่งประกาศใช้มาเป็นระยะเวลาอันยาวนานเป็นหลัก และยังไม่มีบทบัญญัติว่าด้วยอำนาจของเจ้าพนักงานสืบสวนและพนักงานสอบสวนในการรวบรวมพยานหลักฐานดิจิทัล และหลักเกณฑ์การรับฟังพยานหลักฐานดิจิทัลโดยตรง ผู้วิจัยเห็นสมควรนำแนวทางบทบัญญัติตาม“Computer Misuse Act (Chapter 50A) และ Criminal Procedure Code(Chapter 68) ของสาธารณรัฐสิงคโปร์มาเป็นแนวทางในการปรับปรุงกฎหมายวิธีพิจารณาความอาญาของไทย เพื่อแก้ไขปัญหาความคลุมเครือในการใช้อำนาจบางประการของเจ้าพนักงาน เช่น การใช้วิธีทางเทคนิคบางประการเพื่อแสวงหารหัสผ่านที่เจ้าของอุปกรณ์กำหนดใช้เพื่อป้องกันการเข้าถึงข้อมูลคอมพิวเตอร์ รวมถึงการเปลี่ยนแปลงมาตรการป้องกันการเข้าถึงโดยเฉพาะสำหรับอุปกรณ์ดิจิทัลหรือการใช้งานโปรแกรมบางอย่างเพื่อป้องกันและหยุดยั้งไม่ให้ผู้หนึ่งผู้ใดเข้าถึงข้อมูลเพื่อทำลายหรือเปลี่ยนแปลงพยานหลักฐานด้วยเทคนิคการควบคุมระยะทางไกลได้ ซึ่งในเรื่องนี้จำเป็นต้องมีการต่อยอดทำการศึกษาวิจัยถึงความซ้ำซ้อนในเรื่องอำนาจของเจ้าพนักงานผู้ปฏิบัติงานเกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ตามประมวลกฎหมายวิธีพิจารณาความอาญา ซึ่งเป็นเสมือนบทกฎหมายสบัญญัติหลักที่ครอบคลุมการดำเนินคดีอาญาโดยทั่วไป และบรรดากฎหมายซึ่งกำหนดอำนาจของเจ้าพนักงานตามกฎหมายแต่ละฉบับไว้เป็นการเฉพาะ อาทิเช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 (ที่แก้ไขเพิ่มเติม) พระราชบัญญัติป้องกันและปราบปรามการค้ามนุษย์ พ.ศ.2551 (ที่แก้ไขเพิ่มเติม) พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ.2547 (ที่แก้ไขเพิ่มเติม) และพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ.2556 เพื่อแก้ไขปัญหาความซ้ำซ้อนและไม่ชัดเจนในกรณีที่คดีอาชญากรรมคอมพิวเตอร์มีความเกี่ยวพันกับกฎหมายหลายฉบับ จากนั้นควรต้องมีการศึกษาถึงช่องว่างของกฎหมายจากการที่มีบทบัญญัติไม่ครอบคลุมประเด็นข้อกังวลใจในการใช้อำนาจของเจ้าพนักงานในการแสวงหาพยานหลักฐานเพื่อพิสูจน์การกระทำความผิดของผู้ถูกกล่าวหา เพื่อเป็นการป้องกันการโต้แย้งเกี่ยวกับอำนาจของเจ้าพนักงานในการได้มาซึ่งพยานหลักฐานในคดี

ผู้วิจัยเชื่อว่าแนวทางการเพิ่มประสิทธิภาพการดำเนินคดีอาชญากรรมคอมพิวเตอร์ดังที่กล่าวมาในงานวิจัยนี้ จะสามารถแก้ไขหรือบรรเทาปัญหาที่เจ้าพนักงานทุกภาคส่วนในกระบวนการ

ยุติธรรมที่เกี่ยวข้องกับงานด้านการสืบสวนสอบสวน การตรวจพิสูจน์ทางนิติคอมพิวเตอร์ และการดำเนินคดีอาชญากรรมคอมพิวเตอร์ พบในการปฏิบัติงานในลักษณะการบูรณาการแนวทางการแก้ไขปัญหาอย่างเป็นระบบและอย่างยั่งยืน และสร้างบรรยากาศความร่วมมือในการปฏิบัติงานระหว่างเจ้าพนักงานในกระบวนการยุติธรรมด้วยกัน อันจะก่อให้เกิดประสิทธิภาพในการดำเนินคดีอาชญากรรมคอมพิวเตอร์เพื่อตอบโต้อาชญากรรมคอมพิวเตอร์รูปแบบใหม่ๆทั้งในปัจจุบันและในอนาคต

บรรณานุกรม

ภาษาไทย

หนังสือ

จรัญ ภักดีธนากุล. กฎหมายลักษณะพยานหลักฐาน. กรุงเทพฯ : สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา, 2561.

ทพพล น้อยปัญญา. กฎหมายเรื่อง BitcoinBlockchain ICO and etc. กรุงเทพฯ : วิญญูชน, 2561.

ประมูล สุวรรณศร. คำธิบายกฎหมายลักษณะพยานหลักฐาน. กรุงเทพฯ : นิติบรรณการ, 2526.

วีระพงษ์ บุญโญภาส และสุพัตรา แผนวิชิต. อาชญากรรมทางเศรษฐกิจ (Economic Crime). กรุงเทพฯ : นิติธรรม, 2557.

สราวุธ ปิติยาศักดิ์. คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ (ฉบับที่ 2) พ.ศ.2560 พร้อมด้วยประกาศกระทรวงที่เกี่ยวข้อง. กรุงเทพฯ : นิติธรรม, 2561.

สุนีย์ สกาวรัตน์. การตรวจพิสูจน์หลักฐานดิจิทัลสำหรับผู้ประกอบวิชาชีพกฎหมาย. กรุงเทพฯ : มูลนิธิเพื่ออินเตอร์เน็ตและวัฒนธรรมพลเมือง, 2559.

สุเนติ คงเทพ. กฎหมายเกี่ยวกับคอมพิวเตอร์. กรุงเทพฯ : บริษัท มังกุ๊ด ดิจิตอลเพรส จำกัด, 2561.

วิทยานิพนธ์ รายงานวิจัย เอกสารวิจัย

จันทิมา โรจนสโรช. “พยานหลักฐานที่ได้มาโดยมิชอบ : ศึกษาเปรียบเทียบระหว่างคำพิพากษาศาลฎีกาก่อนบัญญัติมาตรา 226/1 กับผลของมาตรา 226/1”. วิทยานิพนธ์หลักสูตรนิติศาสตรมหาบัณฑิต,คณะนิติศาสตร์ปรีดี พนมยงค์,มหาวิทยาลัยธุรกิจบัณฑิต, 2557.

เฉลิมชนม์ แน่นหนา และคณะ. “อาชญากรรมบนสื่อออนไลน์”. เอกสารวิจัย, หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ 55, หลักสูตรการป้องกันราชอาณาจักรภาครัฐร่วมเอกชน รุ่นที่ 25, วิทยาลัยป้องกันราชอาณาจักร, 2555.

ชลลดา จินตเสถียร. “ข้อยกเว้นการห้ามรับฟังพยานหลักฐานที่ได้มาโดยมิชอบตามมาตรา 226/1 ประมวลกฎหมายวิธีพิจารณาความอาญา”. วิทยานิพนธ์หลักสูตรนิติศาสตรมหาบัณฑิต, คณะนิติศาสตร์, มหาวิทยาลัยธรรมศาสตร์, 2553.

ดวงใจ สิงหนาท. “การรับฟังพยานหลักฐานที่ได้มาเนื่องจากการกระทำโดยมิชอบ”. ผลงานส่วนบุคคล, การอบรมหลักสูตรผู้พิพากษาผู้บริหารในศาลชั้นต้น รุ่นที่ 10, สถาบันพัฒนาข้าราชการตุลาการศาลยุติธรรม, 2555.

นัทธ์ ธเนศวาณิชย์. “การรับฟังและวิธีการนำสืบพยานหลักฐานอิเล็กทรอนิกส์ในคดีอาญา: ศึกษาตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550”. วิทยานิพนธ์หลักสูตรนิติศาสตรมหาบัณฑิต, คณะนิติศาสตร์, มหาวิทยาลัยธรรมศาสตร์, 2555.

วิจัย, กอง. “การวิจัยเพื่อพัฒนากระบวนการสืบสวนและสอบสวนของเจ้าหน้าที่ตำรวจในการรับมือกับอาชญากรรมคอมพิวเตอร์”. เอกสารวิจัย, สำนักงานยุทธศาสตร์ตำรวจ สำนักงานตำรวจแห่งชาติ, 2559.

ศุทธดา วัฒนวิเชียร. “การรับฟังและชั่งน้ำหนักพยานหลักฐานในรูปข้อมูลอิเล็กทรอนิกส์”. ผลงานส่วนบุคคล, การอบรมหลักสูตรผู้พิพากษาผู้บริหารในศาลชั้นต้น รุ่นที่ 9, สถาบันพัฒนาข้าราชการตุลาการศาลยุติธรรม, 2554.

สมบัติ ดาวแจ้ง. “ข้อสันนิษฐานความรับผิดในกฎหมายอาญา”. วิทยานิพนธ์หลักสูตรนิติศาสตรมหาบัณฑิต, คณะนิติศาสตร์, มหาวิทยาลัยธรรมศาสตร์, 2543.

อรวรรณ เดชโชติวุฒิ. “การกระทำความผิดผ่านทางอินเตอร์เน็ต : ศึกษากรณีการเผยแพร่ภาพและสื่อลามกอนาจารโดยผ่านโปรแกรมแคมฟรอก (Camfrog)”. สารนิพนธ์หลักสูตรนิติศาสตรมหาบัณฑิต, คณะนิติศาสตร์, มหาวิทยาลัยกรุงเทพ, 2550.

สัมภาษณ์

กชกร เพิงระนัย, ร้อยตำรวจเอกหญิง,อาจารย์ (สบ1) กลุ่มคณาจารย์ คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ. สัมภาษณ์. มีนาคม 2562.

ชานนท์ คำนวนศักดิ์, พันตำรวจโท, กลุ่มงานตรวจสอบและวิเคราะห์ กองบังคับการสนับสนุนทางเทคโนโลยี. สัมภาษณ์.มีนาคม 2562.

ดรัณ จาดเจริญ, พันตำรวจโท,เจ้าหน้าที่คดีพิเศษ ชำนาญการพิเศษ กรมสอบสวนคดีพิเศษ สัมภาษณ์. มีนาคม2562.

นิติ อินทลักษณ์, พันตำรวจโท,นักวิทยาศาสตร์ (สบ.3) กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ กองพิสูจน์หลักฐานกลาง. สัมภาษณ์. มีนาคม2562.

เบญจพร วัชระวุฒิชัย, อัยการจังหวัดประจำสำนักงานอัยการสูงสุด สำนักงานคดีเศรษฐกิจและทรัพยากร. สัมภาษณ์.มีนาคม2562.

ปกรณ์ ธรรมโรจน์, อัยการจังหวัดประจำสำนักงานอัยการสูงสุด สำนักงานคดีอาญา. สัมภาษณ์. มีนาคม2562.

ปฏิภาณ ยืนทนต์, ร้อยตำรวจเอก,รองสารวัตร (สอบสวน) สถานีตำรวจนครบาลชนะสงคราม. สัมภาษณ์.มีนาคม 2562.

ปัญจะ ผลโต, ร้อยตำรวจเอก,รองสารวัตร (สอบสวน) สถานีตำรวจนครบาลหนองค้างพลู. สัมภาษณ์. มีนาคม2562.

เผ่าภูมิ สมหมาย, พันตำรวจโท,รองผู้กำกับการ 4 กองบังคับการปราบปรามการค้ามนุษย์.สัมภาษณ์. มีนาคม2562.

เรวัติ บุญตันหล้า, ร้อยตำรวจเอก,รองสารวัตร กองกำกับการวิเคราะห์ข่าวและเครื่องมือพิเศษ กองบังคับการสืบสวนสอบสวนตำรวจภูธรภาค 5. สัมภาษณ์.มีนาคม2562.

วันทนีย์ ตุลยเสวี, ร้อยตำรวจเอก,นักวิทยาศาสตร์ (สบ.1) กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ กองพิสูจน์หลักฐานกลาง. สัมภาษณ์. มีนาคม2562.

อัศว์ณุต แสงทองดี, พันตำรวจโท,อาจารย์ (สบ2) กลุ่มคณาจารย์ คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ. สัมภาษณ์. มีนาคม2562.

กฎหมาย

“พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550”, ราชกิจจานุเบกษา. เล่มที่ 124 (ตอนที่ 27 ก), 18 มิถุนายน 2550, หน้า 4–13.

“พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560”, ราชกิจจานุเบกษา. เล่มที่ 134 (ตอนที่ 10 ก), 24 มกราคม 2560, หน้า 24–35.

“พระราชบัญญัติองค์กรอัยการและพนักงานอัยการ พ.ศ. 2553”, ราชกิจจานุเบกษา. เล่มที่ 127 (ตอนที่ 75 ก), 7 ธันวาคม 2553, หน้า 38–50.

เอกสารไม่ตีพิมพ์

คำพิพากษาศาลอาญาธนบุรี คดีหมายเลขดำที่ 2957/2560 คดีหมายเลขแดงที่ 1519/2561, อัดสำเนา, 2561.

ป้องกันราชอาณาจักร, วิทยาลัย. “เอกสาร วปอ. หมายเลข 006 คู่มือการเขียนเอกสารวิจัย”. 2561.

อัยการสูงสุด, สำนักงาน. “คู่มือการดำเนินคดีอาญาของพนักงานอัยการ”. 2555.

อัยการสูงสุด, สำนักงาน. “คู่มือพนักงานอัยการสำหรับการสอบสวนและการดำเนินคดีความผิดเกี่ยวกับคอมพิวเตอร์”. 2554.

อนุชาติ คงมาลัย. “คู่มือพนักงานอัยการว่าด้วยการค้นและยึดคอมพิวเตอร์และการได้มาซึ่งพยานหลักฐานทางอิเล็กทรอนิกส์ในการสอบสวนคดีอาญา”. (ออนไลน์). เข้าถึงได้จาก :http://www.ago.go.th/articles/comcrime_061051_1.pdf, 2551.

ฐานข้อมูลอิเล็กทรอนิกส์

คณิต วัลยะเพ็ชร์. “หลักนิติธรรม – การได้รับการพิจารณาคดีที่เป็นธรรม : การพัฒนาหลักกฎหมายการรับฟังพยานหลักฐานของไทยในคดีอาญา” . (ออนไลน์). เข้าถึงได้จาก : http://elibrary.constitutionalcourt.or.th/document/documents/documents/Individual_Study_5.pdf, 2562.

“ความน่าเชื่อถือของพยานหลักฐานอิเล็กทรอนิกส์ที่ได้จากโทรศัพท์เคลื่อนที่ประเภทสมาร์ทโฟน”. (ออนไลน์). เข้าถึงได้จาก : http://www.policecyber.com/journal/j5/J506.pdf, 2562.

“คำวินิจฉัยศาลรัฐธรรมนูญที่ 11/2544”. (ออนไลน์). เข้าถึงได้จาก : http://www.kodmhai.com/vinit/2544/11.html, 2562.

“งานตรวจพิสูจน์”. (ออนไลน์). เข้าถึงได้จาก : http://www.science.police.go.th/main/index.php, 2562.

“แฉเหลี่ยม!! แก๊งแชตรักลวงโลก ภัยสาวไทยนิยมผัวฝรั่ง”. (ออนไลน์). เข้าถึงได้จาก : https://www.thairath.co.th/content/1311031, 2562.

“ชวนดู วิธีใช้หลักฐานอิเล็กทรอนิกส์หาตัวผู้กระทำผิดออนไลน์ กฎหมายปัจจุบันให้อำนาจไว้พอแล้ว”. (ออนไลน์). เข้าถึงได้จาก : https://freedom.ilaw.or.th, 2562.

“ซับซ้อน ซ่อนเงื่อน ‘สื่อลามกเด็ก’ อาชญากรรมใต้ดิน ‘ยุคไซเบอร์’”. (ออนไลน์). เข้าถึงได้จาก : https://www.matichon.co.th/lifestyle/news_1236480, 2561.

“ดีเอสไอบุกรวบแอดมินกลุ่มแชร์ภาพลามกเด็ก”. (ออนไลน์). เข้าถึงได้จาก :https://mgronline.com/crime/detail/9620000016689, 2562.

“ทลายเครือข่าย Romance Scam” ผู้ต้องหา 17 ราย 8 เครือข่าย ผู้เสียหาย 48 ราย ความเสียหายมากกว่า 5,961,740 บาท”. (ออนไลน์). เข้าถึงได้จาก : https://touristpolice.go.th/2018/09/15/romancescam/, 2562.

“ปปง.แก้ ก.ม.เงินดิจิทัล‘บิตคอยน์’ คุมเข้มผู้ให้บริการ ปิดทางมิจฉาชีพ”. (ออนไลน์). เข้าถึงได้จาก : https://www.thairath.co.th/content/1191080, 2561.

“ประมวลกฎหมายวิธีพิจารณาความอาญา (ฉบับ Update ล่าสุด)”. (ออนไลน์). เข้าถึงได้จาก : http://app-thca.krisdika.go.th/Naturesig/CheckSig?whichLaw=law4&folderName=%bb05&lawPath=%bb05-20-9999-update, 2562.

“ประมวลกฎหมายอาญา (ฉบับ Update ล่าสุด)”. (ออนไลน์). เข้าถึงได้จาก : http://app-thca.krisdika. go.th/Naturesig/CheckSig?whichLaw=law4&folderName=%bb06&lawPath=%bb06-20-9999-update, 2562.

ปริญญา หอมอเนก, “กฎหมายอาชญากรรมคอมพิวเตอร์ และ การพิสูจน์หลักฐานด้วยวิธีการ “นิติคอมพิวเตอร์” (Thailand Computer Crime Law and Computer Forensics)”. (ออนไลน์). เข้าถึงได้จาก : https://www.acisonline.net/?p=1417&lang=th, 2562.

“พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 แก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2551 (ฉบับ Update ล่าสุด)”. (ออนไลน์). เข้าถึงได้จาก : http://app-thca.krisdika.go.th/Naturesig/CheckSig?whichLaw=law2&folderName=%a1114&lawPath=%a1114-20-9999-update, 2562.

“พระราชบัญญัติป้องกันและปราบปรามการค้ามนุษย์ พ.ศ. 2551 (ฉบับ Update ล่าสุด)”.(ออนไลน์). เข้าถึงได้จาก : http://app-thca.krisdika.go.th/Naturesig/CheckSig?whichLaw=law2&folderName=%bb47&lawPath=%bb47-20-9999-update, 2562.

“พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556”. (ออนไลน์). เข้าถึงได้จาก : http://app-thca.krisdika.go.th/Naturesig/CheckSig?whichLaw=law2&folderName=%bb52&lawPath=%bb52-20-2556-a0001, 2562.

“พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 แก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 (ฉบับ Update ล่าสุด)”. (ออนไลน์). เข้าถึงได้จาก : http://app-thca.krisdika.go.th/Naturesig/CheckSig?whichLaw=law2&folderName=%c771&lawPath=%c771-20-9999-update, 2562.

“พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 (ฉบับ Update ล่าสุด)”. (ออนไลน์). เข้าถึงได้จาก : http://app-thca.krisdika.go.th/Naturesig/CheckSig?whichLaw=law2&folderName=%c763&lawPath=%c763-20-9999-update, 2562.

“ฟอกเงินผ่าน'บิทคอยน์'ปลอดภัยจริงหรือ”. (ออนไลน์). เข้าถึงได้จาก : http://www.bangkokbiznews.com /blog/detail/643776, 2561.

“รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.2560”. (ออนไลน์). เข้าถึงได้จาก : http://app- thca.krisdika.go.th/ Naturesig/CheckSig?whichLaw=law1&folderName=%c306&lawPath=%c306 -10-2560-a0003, 2562.

“ระวังภัย ฟิชชิ่งเมล”. (ออนไลน์). เข้าถึงได้จาก : https://www.moneyandbanking.co.th/new/ 23814/13/index.php, 2562.

“ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .....”. (ออนไลน์). เข้าถึงได้จาก : https://ictlawcenter.etda.or.th/de_laws/detail/de-laws-data-privacy-act, 2562.

“ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .....”. (ออนไลน์). เข้าถึงได้จาก : https://ictlawcenter.etda.or.th/de_laws/detail/de-laws-cyber-security-protection-act, 2562.

“รู้ลึกรู้จริงรอบรู้ทุกแง่มุมกับ “ภัยคุกคาม””. (ออนไลน์). เข้าถึงได้จาก : http://www.ictc.ago.go.th/download53/new_it%281%29.pdf, 2562.

“ยังไม่ชัดใครแฮกFacebook กระทบผู้ใช้ 50 ล้านคนทั่วโลก”. (ออนไลน์). เข้าถึงได้จาก : https://mgronline.com/cyberbiz/detail/9610000097420, 2562.

วศิน แดงประดับ. “การสันนิษฐานว่าบุคคลทุกคนเป็นผู้บริสุทธิ์ : หลักการและข้อยกเว้นบางประการ”. (ออนไลน์). เข้าถึงได้จาก : http://web.krisdika.go.th/pdfPage.jsp?type=act&actCode=229, 2562.

“ศาลฎีกามีคำพิพากษา จำคุกแฮกเกอร์ ฐานแก้ไขวงเงิน ระบบเติมเงินทรูมูฟ”. (ออนไลน์). เข้าถึงได้จาก : http://www3.truecorp.co.th/investor/entry/1301, 2562.

ศูนย์เทคโนโลยีสารสนเทศ และการสื่อสาร ศาลฎีกา. “คำพิพากษาฎีกาที่ 10632/2554”. (ออนไลน์). เข้าถึงได้จาก : http://deka.supremecourt.or.th/search, 2562.

ศูนย์เทคโนโลยีสารสนเทศ และการสื่อสาร ศาลฎีกา. “คำพิพากษาฎีกาที่ 2205/2554 (ป)”. (ออนไลน์). เข้าถึงได้จาก : http://deka.supremecourt.or.th/search, 2562.

ศูนย์เทคโนโลยีสารสนเทศ และการสื่อสาร ศาลฎีกา. “คำพิพากษาฎีกาที่ 2281/2555”. (ออนไลน์). เข้าถึงได้จาก : http://deka.supremecourt.or.th/search, 2562.

ศูนย์เทคโนโลยีสารสนเทศ และการสื่อสาร ศาลฎีกา. “คำพิพากษาฎีกาที่ 2414/2551”. (ออนไลน์). เข้าถึงได้จาก : http://deka.supremecourt.or.th/search, 2562.

ศูนย์เทคโนโลยีสารสนเทศ และการสื่อสาร ศาลฎีกา. “คำพิพากษาฎีกาที่ 2429/2551”. (ออนไลน์). เข้าถึงได้จาก : http://deka.supremecourt.or.th/search, 2562.

ศูนย์เทคโนโลยีสารสนเทศ และการสื่อสาร ศาลฎีกา. “คำพิพากษาฎีกาที่ 3118/2559”. (ออนไลน์). เข้าถึงได้จาก : http://deka.supremecourt.or.th/search, 2562.

ศูนย์เทคโนโลยีสารสนเทศ และการสื่อสาร ศาลฎีกา. “คำพิพากษาฎีกาที่ 4085/2545”. (ออนไลน์). เข้าถึงได้จาก : http://deka.supremecourt.or.th/search, 2562.

ศูนย์เทคโนโลยีสารสนเทศ และการสื่อสาร ศาลฎีกา. “คำพิพากษาฎีกาที่ 4301/2543”. (ออนไลน์). เข้าถึงได้จาก : http://deka.supremecourt.or.th/search, 2562.

ศูนย์เทคโนโลยีสารสนเทศ และการสื่อสาร ศาลฎีกา. “คำพิพากษาฎีกาที่ 6475/2547”. (ออนไลน์). เข้าถึงได้จาก : http://deka.supremecourt.or.th/search, 2562.

ศูนย์เทคโนโลยีสารสนเทศ และการสื่อสาร ศาลฎีกา. “คำพิพากษาฎีกาที่ 6523/2545”. (ออนไลน์). เข้าถึงได้จาก : http://deka.supremecourt.or.th/search, 2562.

ศูนย์เทคโนโลยีสารสนเทศ และการสื่อสาร ศาลฎีกา. “คำพิพากษาฎีกาที่ 7013/2556”. (ออนไลน์). เข้าถึงได้จาก : http://deka.supremecourt.or.th/search, 2562.

ศูนย์เทคโนโลยีสารสนเทศ และการสื่อสาร ศาลฎีกา. “คำพิพากษาฎีกาที่ 81/2551”. (ออนไลน์). เข้าถึงได้จาก : http://deka.supremecourt.or.th/search, 2562.

ศูนย์เทคโนโลยีสารสนเทศ และการสื่อสาร ศาลฎีกา. “คำพิพากษาฎีกาที่ 837/2483”. (ออนไลน์). เข้าถึงได้จาก : http://deka.supremecourt.or.th/search, 2562.

“หลักอาชญาวิทยากับกระบวนการยุติธรรม”. (ออนไลน์). เข้าถึงได้จาก : http://www.oja.go.th/TH/wp-content/uploads/2017/11/13-11-60%20A.pdf, 2562.

“Cryptocurrencyคืออะไร และคุณควรที่จะลงทุนกับมันหรือไม่”. (ออนไลน์). เข้าถึงได้จาก : https://siamblockchain.com/2018/03/11/cryptocurrency-%E0%B8%84%E0-%B8%B7%E0%B8%AD-%E0%B8%AD%E0%B8%B0%E0%B9%84%E0%B8%A3/, 2561.

“Spam Mail ภัยร้ายใกล้ตัวคุณ”. (ออนไลน์). เข้าถึงได้จาก : http://oknation.nationtv.tv/blog/Rosejoker/2008/01/22/entry-21, 2562.

“TB-CERT ศูนย์เตือนภัยไซเบอร์ธนาคารไทย เตือนเมลฟิชชิ่ง ระบุการเก็บตัวอย่างทำได้ยาก หากใครเจอช่วยกันส่งให้ธนาคาร”. (ออนไลน์). เข้าถึงได้จาก :https://www.blognone.com/node/107725, 2562.

ภาษาต่างประเทศ

"Cybersecurity Act 2018". (ออนไลน์). เข้าถึงได้จาก : "UniversalDeclaration of Human Rights". (ออนไลน์). เข้าถึงได้จาก : https://sso.agc.gov.sg/Acts-Supp/9-2018/, 2562.

"Singapore cybersecurity – new amendments introduce four key changes". (ออนไลน์). เข้าถึงได้จาก : https://www.nortonrosefulbright.com/en/knowledge/publications/a027c3a8/singapore-cybersecurity---new-amendments-introduce-four-key-changes, 2560.

"UniversalDeclaration of Human Rights". (ออนไลน์). เข้าถึงได้จาก : http://www.un.org/en/universal-declaration-human-rights/, 2562.

ภาคผนวก

ผนวก ก

Computer Misuse Act (Chapter 50 A) และ Criminal Procedure Code (Chapter 68) ของสาธารณรัฐสิงคโปร์ (เฉพาะส่วนที่เกี่ยวข้องกับอำนาจเจ้าพนักงาน)

COMPUTER MISUSE ACT

(CHAPTER 50A)

(Original Enactment: Act 19 of 1993)

REVISED EDITION 2007

(31st July 2007)

.....

.....

PART III

MISCELLANEOUS AND GENERAL

.....

.....

Saving for investigations by police and law enforcement officers

14. Nothing in this Act shall prohibit a police officer, an authorised person within the meaning of section 39 of the Criminal Procedure Code 2010 or any other duly authorised law enforcement officer from lawfully conducting investigations pursuant to the powers conferred on him under any written law.

[21/98; 42/2005]
[15/2010 wef 02/01/2011]

CRIMINAL PROCEDURE CODE

(CHAPTER 68)

(Original Enactment: Act 15 of 2010)

REVISED EDITION 2012

(31st August 2012)

.....

.....

PART IV

INFORMATION TO POLICE AND POWERS OF INVESTIGATION

Division 1 — Duties of police officer on receiving information about offences

.....

.....

Power to access computer

39.—(1) A police officer or an authorised person investigating an arrestable offence may, at any time —

(*a*) access, inspect and check the operation in or from Singapore of a computer (whether in Singapore or elsewhere) that the police officer or authorised person has reasonable cause to suspect is or has been used in connection with, or contains or contained evidence relating to, the arrestable offence;

(*b*) use any such computer in or from Singapore, or cause any such computer to be used in or from Singapore —

(i) to search any data contained in or available to such computer; and

(ii) to make a copy of any such data;

(*c*) prevent any other person from gaining access to, or using, any such computer (including by changing any username, password or other authentication information required to gain access to the computer); or

(*d*) order any person —

(i) to stop accessing or using or to not access or use any such computer; or

(ii) to access or use any such computer only under such conditions as the police officer or authorised person may specify.

[Act 19 of 2018 wef 17/09/2018]

(2) The police officer or authorised person may also order any of the following persons to provide any assistance mentioned in subsection (2A):

(*a*) any person whom the police officer or authorised person reasonably suspects of using, or of having used, the computer in connection with the arrestable offence;

(*b*) any person having charge of, or otherwise concerned with the operation of, the computer;

(*c*) any person whom the police officer or authorised person reasonably believes has knowledge of or access to any username, password or other authentication information required to gain access to the computer.

[Act 19 of 2018 wef 17/09/2018]

(2A) For the purposes of subsection (2), the types of assistance are as follows:

(*a*) assistance to gain access to the computer (including assistance through the provision of any username, password or other authentication information required to gain access to the computer);

(*b*) assistance to prevent a person (other than the police officer or authorised person) from gaining access to, or using, the computer, including assistance in changing any username, password or other authentication information required to gain access to the computer.

[Act 19 of 2018 wef 17/09/2018]

(2B) Without limiting subsection (1), where the police officer or authorised person knows that the computer mentioned in that subsection is located outside Singapore, or does not know whether that computer is located in or outside Singapore, the police officer or authorised person —

(*a*) may exercise the powers under subsection (1) in relation to that computer, or any data contained in or available to that computer, if —

(i) the owner of that computer consents to the exercise of those powers; or

(ii) the police officer or authorised person obtains access to that computer through the exercise of any power of investigation under any written law, such as in any of the following circumstances:

(A) the access is obtained with the assistance mentioned in subsection (2A)(*a*) provided under subsection (2) by a person having charge of, or otherwise concerned with the operation of, that computer;

(B) the access is obtained through an active connection with, or through any username,

password or other authentication information stored in, another computer, which has been seized under section 35 and accessed under subsection (1);

(C) the access is obtained through any username, password or other authentication information contained in any document seized under section 35;

(D) the access is obtained through any username, password or other authentication information provided in any statement made by any person examined under section 22; and

(*b*) may exercise the powers under subsection (1)(*b*) in relation to any data contained in or available to that computer, if the owner of that data consents to the exercise of those powers.

[Act 19 of 2018 wef 17/09/2018]

(3) Any person who obstructs the lawful exercise by a police officer or an authorised person of any power under subsection (1)(*a*), (*b*) or (*c*), or who fails to comply with any order of the police officer or authorised person under subsection (1)(*d*) or (2), shall be guilty of an offence and shall be liable on conviction —

(*a*) in any case where the person is a body corporate, a limited liability partnership, a partnership or an unincorporated association — to a fine not exceeding $10,000; or

(*b*) in any other case — to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 6 months or to both.

[Act 19 of 2018 wef 17/09/2018]

(4) An offence under subsection (3) shall be an arrestable offence.

(5) A person who had acted in good faith under subsection (1) or in compliance with a requirement under subsection (1)(*d*) or (2) shall not be liable in any criminal or civil proceedings for any loss or damage resulting from the act.

[Act 19 of 2018 wef 17/09/2018]

(6) In this section and section 40 —

"authorised person" means —

(*a*) a forensic specialist appointed under section 65A of the Police Force Act (Cap. 235), or any other person, who is authorised in writing by the Commissioner of Police for the purposes of this section or section 40 or both; or

(*b*) any officer of a prescribed law enforcement agency who is authorised in writing, by the head of that law enforcement agency, for the purposes of this section or section 40 or both;

"prescribed law enforcement agency" means a law enforcement agency prescribed, by order in the *Gazette*, by the Minister charged with the responsibility for that law enforcement agency.

[Act 19 of 2018 wef 17/09/2018]

Power to access decryption information

40.—(1) For the purposes of investigating an arrestable offence, the Public Prosecutor may by order authorise a police officer or an authorised person to exercise, in addition to the powers under section 39, all or any of the powers under this section.

(2) The police officer or authorised person referred to in subsection (1) shall be entitled to —

(*a*) access any information, code or technology which has the capability of retransforming or unscrambling encrypted data into readable and comprehensible format or text for the purposes of investigating the arrestable offence;

(*b*) require —

(i) any person whom he reasonably suspects of using a computer in connection with an arrestable offence or of having used it in this way; or

(ii) any person having charge of, or otherwise concerned with the operation of, such computer,

to provide him with such reasonable technical and other assistance as he may require for the purposes of paragraph (*a*); and

(*c*) require any person whom he reasonably suspects to be in possession of any decryption information to grant him access to such decryption information as may be necessary to decrypt any data required for the purposes of investigating the arrestable offence.

(3) Any person who obstructs the lawful exercise by a police officer or an

authorised person of the powers under subsection (2)(*a*) or who fails to comply with any requirement of the police officer or authorised person under subsection (2)(*b*) or (*c*) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both.

(4) Where a person is convicted of an offence under subsection (3) and it is shown that the encrypted data contains evidence relevant to the planning, preparation or commission of a specified serious offence, he shall, in lieu of the punishment prescribed under subsection (3) —

(*a*) be liable to be punished with the same punishment prescribed for that specified serious offence, except that the punishment imposed shall not exceed a fine of $50,000 or imprisonment for a term not exceeding 10 years or both; or

(*b*) be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 10 years or to both where the specified serious offence is punishable on conviction with death or imprisonment for life.

(5) For the purposes of subsection (4) but subject to subsection (6), "specified serious offence" means an offence under any of the following written laws:

(*a*) any written law which provides for any offence involving the causing of death or bodily harm;

(*b*) any written law relating to actions or the threat of actions prejudicial to national security;

(*c*) any written law relating to radiological or biological weapons;

(*d*) the Arms and Explosives Act (Cap. 13);

(*e*) the Chemical Weapons (Prohibition) Act (Cap. 37B);

(*f*) the Corrosive and Explosive Substances and Offensive Weapons Act (Cap. 65);

(*g*) the Hijacking of Aircraft and Protection of Aircraft and International Airports Act (Cap. 124);

(*h*) the Kidnapping Act (Cap. 151);

(*i*) the Maritime Offences Act (Cap. 170B);

(*j*) the Official Secrets Act (Cap. 213);

(*k*) the Infrastructure Protection Act 2017;

[Act 41 of 2017 wef 18/12/2018]

(*l*) the Statutory Bodies and Government Companies (Protection of Secrecy) Act (Cap. 319);

(*m*) the Strategic Goods (Control) Act (Cap. 300);

(*n*) the Terrorism (Suppression of Financing) Act (Cap. 325);

(*o*) the United Nations (Anti-Terrorism Measures) Regulations (Cap. 339, Rg 1); and

(*p*) such other written law as the Minister may, by order published in the *Gazette*, specify.

(6) No offence shall be a specified serious offence for the purposes of subsection (4) unless the maximum punishment prescribed for that offence, whether for a first or subsequent conviction, is —

(*a*) imprisonment for a term of 5 years or more;

(*b*) imprisonment for life; or

(*c*) death.

(7) In proceedings against any person for an offence under this section, if it is shown that that person was in possession of any decryption information at any time before the time of the request for access to such information, that person shall be presumed for the purposes of those proceedings to have continued to be in possession of that decryption information at all subsequent times, unless it is shown that the decryption information —

(*a*) was not in his possession at the time the request was made; and

(*b*) continued not to be in his possession after the request was made.

(8) A person who had acted in good faith or in compliance with a requirement under subsection (2) shall not be liable in any criminal or civil proceedings for any loss or damage resulting from the act.

(9) In this section —

"data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer;

"decryption information" means information, code or technology or part thereof that enables or facilitates the retransformation or unscrambling of encrypted data from its unreadable and incomprehensible format to its plain text version;

"encrypted data" means data which has been transformed or scrambled

from its plain text version to an unreadable or incomprehensible format, regardless of the technique utilised for such transformation or scrambling and irrespective of the medium in which such data occurs or can be found for the purposes of protecting the content of such data;

"plain text version" means the original data before it has been transformed or scrambled to an unreadable or incomprehensible format.

ผนวก ข

แบบสอบถามการสัมภาษณ์เชิงลึก (In-depth Interview)

แบบสอบถามการสัมภาษณ์เชิงลึก (In-depth Interview)

เรื่อง แนวทางเพิ่มประสิทธิภาพการดำเนินคดีอาชญากรรมคอมพิวเตอร์

คำชี้แจง

1. แบบสอบถามนี้เป็นแบบสอบถาม**ผู้ทรงคุณวุฒิด้านการสืบสวนอาชญากรรมคอมพิวเตอร์ ด้านการสอบสวนอาชญากรรมคอมพิวเตอร์ ด้านการตรวจพิสูจน์ทางนิติคอมพิวเตอร์ และด้านการดำเนินคดีอาชญากรรมคอมพิวเตอร์** มีวัตถุประสงค์เพื่อนำข้อมูลที่ได้ไปใช้ประโยชน์ในการทำวิจัยทางวิชาการของ นายณัฐพงษ์ พุฒแก้ว อัยการผู้เชี่ยวชาญพิเศษสำนักงานอัยการสูงสุด ผู้วิจัย ซึ่งเป็นส่วนหนึ่งของหลักสูตรการป้องกันราชอาณาจักร (วปอ.)

2. วัตถุประสงค์ของการวิจัย เพื่อทราบสภาพปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ที่พบในชั้นสืบสวนสอบสวน รวบรวมพยานหลักฐาน ตลอดถึงขั้นตอนการนำเสนอพยานหลักฐานในชั้นศาล เพื่อวิเคราะห์ปัจจัยที่ก่อให้เกิดสภาพปัญหาและอุปสรรคดังกล่าว ซึ่งจะนำไปสู่ข้อเสนอแนะแนวทางเพิ่มประสิทธิภาพในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ต่อไป

3. ในแบบสอบถามนี้

“อาชญากรรมคอมพิวเตอร์” มุ่งเน้นการกระทำความผิดอาญาที่ใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด อันเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 (ที่แก้ไขเพิ่มเติม)

“สภาพปัญหาหรืออุปสรรค” ที่พบในการดำเนินงาน/ดำเนินคดี ที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ หมายถึง ข้อติดขัดที่ส่งผลกระทบต่อประสิทธิภาพในการดำเนินงาน/ดำเนินคดี <u>รวมไปถึงกรณีที่ผู้ปฏิบัติงานไม่แน่ใจถึงอำนาจตามกฎหมายในการดำเนินงานของตนด้วย</u>

“กลุ่ม” ของผู้ตอบแบบสอบถามนี้ หมายถึงเจ้าหน้าที่ในกระบวนการยุติธรรมทางอาญาที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ 4 กลุ่ม ได้แก่

1. กลุ่มเจ้าหน้าที่สืบสวน
2. กลุ่มพนักงานสอบสวน
3. กลุ่มผู้ตรวจพิสูจน์หลักฐาน
4. กลุ่มพนักงานอัยการ

1. แบบสอบถามชุดนี้ แบ่งออกเป็น3 ตอน คือ

ตอนที่ 1 ข้อมูลทั่วไป

ตอนที่ 2 ความคิดเห็นเกี่ยวกับการดำเนินคดีอาชญากรรมคอมพิวเตอร์

ตอนที่ 3 ตัวอย่างการดำเนินงานเกี่ยวกับอาชญากรรมคอมพิวเตอร์

ขอความกรุณาโปรดตอบแบบสอบถามในส่วนที่ท่านเกี่ยวข้อง และขอขอบพระคุณอย่างสูงที่ให้ความร่วมมือตอบแบบสอบถาม มา ณ โอกาสนี้

ตอนที่ 1 ข้อมูลทั่วไป

1. ชื่อผู้ตอบแบบสอบถาม

.....

2. ตำแหน่ง

.....

3. ที่ทำงานปัจจุบัน

.....

4. ระยะเวลาการปฏิบัติงานเกี่ยวกับอาชญากรรมคอมพิวเตอร์โดยรวมของท่าน ..... ปี

5. ลักษณะหน้าที่และความรับผิดชอบของท่านที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ จัดอยู่ใน**กลุ่ม**ใด **(การระบุกลุ่มในข้อนี้ เพื่อประโยชน์ในการตอบแบบสอบถามส่วนที่ 2)**

☐เจ้าหน้าที่สืบสวน ☐ พนักงานสอบสวน ☐ ผู้ตรวจพิสูจน์หลักฐาน ☐พนักงานอัยการ

6. งานเกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ในความรับผิดชอบของท่าน มีลักษณะงานและกรอบของงานเป็นอย่างไร

.....

.....

.....

7. ท่านมีความรู้ความเข้าใจเกี่ยวกับการทำงานของระบบคอมพิวเตอร์และอุปกรณ์ดิจิทัลในระดับใด

☐ มาก☐ ค่อนข้างมาก ☐ ปานกลาง☐ ค่อนข้างน้อย☐ น้อย

.....

8. ท่านมีความรู้ความเข้าใจเกี่ยวกับการทำธุรกรรมทางการเงินออนไลน์ การชำระราคาผ่านช่องทางออนไลน์ และสกุลเงินดิจิทัล ในระดับใด

□ มาก□ ค่อนข้างมาก □ ปานกลาง□ ค่อนข้างน้อย□ น้อย

.....

9. ในการทำงานด้านอาชญากรรมคอมพิวเตอร์ของท่าน ต้องมีการประสานงานกับบุคลากรข้ามกลุ่มหรือไม่

□ ไม่ต้องมีการประสานงาน

□ ต้องมีการประสานงาน (โปรดตอบคำถามในข้อ 9.1 – 9.3)

□ เป็นดุลพินิจว่าจะประสานงานหรือไม่ก็ได้ (โปรดตอบคำถามในข้อ 9.1 – 9.3)

9.1 ท่านมีการประสานงานกับเจ้าหน้าที่กลุ่มใดบ้าง

.....

.....

9.2 ลักษณะการประสานงานเป็นแบบ

□ เป็นทางการ□ ไม่เป็นทางการ□ทั้งที่เป็นและไม่เป็นทางการ

9.3 วัตถุประสงค์ในการประสานงานมีอย่างไรบ้าง

.....

.....

.....

.....

.....

ตอนที่ 2 ความคิดเห็นเกี่ยวกับการดำเนินคดีอาชญากรรมคอมพิวเตอร์

(ตอบเฉพาะคำถามที่เกี่ยวของกับกลุ่มงานของท่าน)

กลุ่มเจ้าหน้าที่สืบสวน

1.อำนาจในการการปฏิบัติงานด้านอาชญากรรมคอมพิวเตอร์ของท่านเป็นไปตามกฎหมายและระเบียบใดบ้าง

.....

.....

.....

2.ในการปฏิบัติงานสืบสวนแต่ละเรื่อง ท่านได้มีการทำรายงานการสืบสวนและส่งมอบให้กับพนักงานสอบสวนหรือไม่อย่างไร

☐ มีการทำรายงานการสืบสวนและส่งมอบให้กับพนักงานสอบสวนทุกเรื่อง

☐ มีการทำรายงานการสืบสวนและส่งมอบให้กับพนักงานสอบสวนเป็นส่วนใหญ่

☐ มีการทำรายงานการสืบสวนและส่งมอบให้กับพนักงานสอบสวนเป็นส่วนน้อย

3.ในการปฏิบัติงานสืบสวนของท่าน ท่านเห็นว่ากฎหมายตามข้อ 1. ให้อำนาจในการปฏิบัติงานเพียงพอหรือไม่อย่างไร

☐ เพียงพอต่อการปฏิบัติงาน

☐ ไม่เพียงพอต่อการปฏิบัติงาน (โปรดระบุ ประเด็นที่ท่านเห็นว่าไม่เพียงพอ หรือประเด็นที่เห็นว่ามีข้อเคลือบคลุมหรือข้อกังวลเกี่ยวกับอำนาจของเจ้าหน้าที่สืบสวน)

.....

.....

.....

.....

4.ท่านเป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 (ที่แก้ไขเพิ่มเติม) หรือไม่

☐ เป็น (ให้ข้ามคำถามข้อ 5. ไป) ☐ ไม่เป็น

5.ในการปฏิบัติงานท่าน ท่านเคยขอให้พนักงานสอบสวนร้องขอให้พนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 (ที่แก้ไขเพิ่มเติม) ใช้อำนาจตามมาตรา 18 ของพระราชบัญญัติดังกล่าวหรือไม่

☐ เคย ☐ ไม่เคย เพราะ.....

.....

6.จากประสบการณ์ที่ผ่านมา ท่านเห็นว่าการปฏิบัติงานสืบสวนคดีอาชญากรรมคอมพิวเตอร์ของเจ้าหน้าที่สืบสวนในพื้นที่ส่วนกลางและส่วนภูมิภาค มีแนวทางที่ใกล้เคียงกันหรือแตกต่างกันอย่างไร

.....

.....

.....

7.ท่านเห็นว่ามีปัจจัยอะไรบ้างที่เป็นอุปสรรคต่อประสิทธิภาพในการดำเนินงานด้านอาชญากรรมคอมพิวเตอร์ของท่าน

.....

.....

.....

8.ท่านมีความรู้ความเข้าใจเกี่ยวกับกฎหมายพยานหลักฐานโดยเฉพาะในประเด็นเรื่องความชอบด้วยกฎหมายของพยานหลักฐาน การได้มาซึ่งพยานหลักฐาน คุณค่าและน้ำหนักของพยานหลักฐาน ในระดับใด

☐ มาก☐ ค่อนข้างมาก ☐ ปานกลาง☐ ค่อนข้างน้อย☐ น้อย

.....

9.ท่านเคยไปเบิกความเป็นพยานในชั้นศาลหรือไม่ หากเคยเบิกความเป็นพยานในศาล ท่านพบปัญหาหรือข้อขัดข้องในการเบิกความหรือไม่ อย่างไร

.....

.....

.....

10.ภายหลังการปฏิบัติงานสืบสวนของท่านแล้วเสร็จ ท่านได้ติดตามผลการดำเนินคดีกับผู้ต้องหา เพื่อนำไปวิเคราะห์ความสำเร็จหรือข้อบกพร่องในการปฏิบติงานของท่านหรือไม่

☐ ติดตาม ☐ ไม่ได้ติดตาม

.....

กลุ่มผู้ตรวจพิสูจน์หลักฐาน

1.การปฏิบัติงานตรวจพิสูจน์หลักฐานทางดิจิทัลของท่าน มีบทบัญญัติกฎหมาย มาตรฐาน ข้อแนะนำ คู่มือ หรือแนวปฏิบัติใดเกี่ยวข้องบ้าง (ทั้งที่กำหนดในประเทศไทย และที่เป็นมาตรฐานสากล)

.....

.....

.....

.....

2.มาตรฐาน ข้อเสนอแนะ หรือแนวทางในการจัดเก็บ ดูแลรักษา และจัดการพยานหลักฐานทางดิจิทัล ที่ท่านใช้ปฏิบัติงานท่านเห็นว่า

☐ ครบถ้วนสำหรับการทำงาน

☐ ยังไม่ครบถ้วน

(โปรดระบุ ประเด็นที่ยังไม่ครบถ้วน.....

.....)

3.เมื่อได้รับมอบหมายให้ทำการตรวจพิสูจน์พยานหลักฐานในคดีอาชญากรรมคอมพิวเตอร์ ท่านพบปัญหาความไม่ชัดเจนในการกำหนดขอบเขตของการตรวจพิสูจน์ที่จะต้องดำเนินการ รวมถึงความประสงค์ของผู้ร้องขอให้ดำเนินการหรือไม่ อย่างไร

☐ ไม่พบ

☐ พบ (<u>โปรดระบุ</u> ประเด็นสภาพปัญหา)

.....

.....

4.ท่านพบปัญหาหรือข้อขัดข้องในการทำความเห็นในรายงานการตรวจพิสูจน์หรือไม่ อย่างไร

☐ ไม่พบ

☐ พบ (<u>โปรดระบุ</u> ปัญหาหรือขัดข้อง)

.....

.....

.....

.....

5.ในการจัดทำรายงานการตรวจพิสูจน์ของท่าน (ตอบได้มากกว่า 1 ข้อ)

☐ ตรวจพิสูจน์และระบุให้ความเห็นเฉพาะที่มีการร้องขอให้ดำเนินการ

☐ ระบุข้อตรวจพบอื่นด้วย แม้จะมิได้มีการร้องขอให้ดำเนินการ
(เช่น.....)

☐ ให้ความสำคัญและคำนึงถึงประเด็นการนำผลการตรวจพิสูจน์ไปใช้ในชั้นการสรุปสำนวนของพนักงานสอบสวน และชั้นการดำเนินคดีในศาลของพนักงานอัยการ

☐ ให้ความสำคัญและคำนึงถึงข้อโต้แย้งผลการตรวจพิสูจน์ในชั้นการพิจารณาคดี

6.จากประสบการณ์ที่ผ่านมา ท่านเห็นว่าการปฏิบัติงานตรวจพิสูจน์หลักฐานของผู้ตรวจพิสูจน์ที่ปฏิบัติงานในพื้นที่ส่วนกลางและส่วนภูมิภาค มีแนวทางที่ใกล้เคียงกันหรือแตกต่างกันอย่างไร

.....

.....

.....

7.ท่านเห็นว่ามีปัจจัยอะไรบ้างที่เป็นอุปสรรคต่อประสิทธิภาพในการดำเนินงานด้านอาชญากรรมคอมพิวเตอร์ของท่าน

.....

.....

.....

8.ท่านมีความรู้ความเข้าใจเกี่ยวกับกฎหมายพยานหลักฐานโดยเฉพาะในประเด็นเรื่องความชอบด้วยกฎหมายของพยานหลักฐาน การได้มาซึ่งพยานหลักฐาน คุณค่าและน้ำหนักของพยานหลักฐาน ในระดับใด

☐ มาก☐ ค่อนข้างมาก ☐ ปานกลาง☐ ค่อนข้างน้อย☐ น้อย

.....

9.ท่านเคยไปเบิกความเป็นพยานในชั้นศาลหรือไม่ หากเคยเบิกความเป็นพยานในศาล ท่านพบปัญหาหรือข้อขัดข้องในการเบิกความหรือไม่ อย่างไร

.....

.....

.....

10.ภายหลังการปฏิบัติงานของท่านแล้วเสร็จ ท่านได้ติดตามผลการดำเนินคดีกับผู้ต้องหา เพื่อนำไปวิเคราะห์ความสำเร็จหรือข้อบกพร่องในการปฏิบติงานของท่านหรือไม่

☐ ติดตาม ☐ ไม่ได้ติดตาม

.....

กลุ่มพนักงานสอบสวน

1.อำนาจในการการปฏิบัติงานด้านอาชญากรรมคอมพิวเตอร์ของท่านเป็นไปตามกฎหมาย ระเบียบ แนวทางปฏิบัติ และคู่มือดำเนินงาน ใดบ้าง

.....

.....

.....

2.ในการปฏิบัติงานสอบสวนของท่าน ท่านเห็นว่ากฎหมาย ระเบียบ แนวทางปฏิบัติ คู่มือดำเนินงาน ให้อำนาจในการปฏิบัติงานเพียงพอหรือไม่ อย่างไร

☐ เพียงพอต่อการปฏิบัติงาน

☐ ไม่เพียงพอต่อการปฏิบัติงาน (<u>โปรดระบุ</u> ประเด็นที่ท่านเห็นว่าไม่เพียงพอ หรือประเด็นที่เห็นว่ามีข้อเคลือบคลุมหรือข้อกังวลเกี่ยวกับอำนาจการสอบสวน)

.....

.....

.....

.....

3.ท่านเป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 (ที่แก้ไขเพิ่มเติม) หรือไม่

☐ เป็น (ให้ข้ามคำถามข้อ 4. ไป) ☐ ไม่เป็น

4.ในการปฏิบัติงานท่านเคยขอให้พนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 (ที่แก้ไขเพิ่มเติม) ใช้อำนาจตามมาตรา 18 ของพระราชบัญญัติดังกล่าวหรือไม่

☐ เคย ☐ ไม่เคย เพราะ.....

.....

5.จากประสบการณ์ของท่าน ท่านเห็นว่าการปฏิบัติงานด้านการสอบสวนคดีอาชญากรรมคอมพิวเตอร์ของพนักงานสอบสวนในพื้นที่ส่วนกลางและส่วนภูมิภาค มีแนวทางที่ใกล้เคียงกันหรือแตกต่างกันอย่างไร

.....

.....

.....

6.ท่านเห็นว่ามีปัจจัยอะไรบ้างที่เป็นอุปสรรคต่อประสิทธิภาพในการดำเนินงานด้านอาชญากรรมคอมพิวเตอร์ของท่าน

.....

.....

.....

7.ท่านมีความรู้ความเข้าใจเกี่ยวกับกฎหมายพยานหลักฐานโดยเฉพาะในประเด็นเรื่องความชอบด้วยกฎหมายของพยานหลักฐาน การได้มาซึ่งพยานหลักฐาน คุณค่าและน้ำหนักของพยานหลักฐาน ในระดับใด

☐ มาก☐ ค่อนข้างมาก ☐ ปานกลาง☐ ค่อนข้างน้อย☐ น้อย

.....

8.ท่านเคยไปเบิกความเป็นพยานในชั้นศาลหรือไม่ หากเคยเบิกความเป็นพยานในศาล ท่านพบปัญหาหรือข้อขัดข้องในการเบิกความหรือไม่ อย่างไร

.....

.....

.....

9.ภายหลังการปฏิบัติงานสอบสวนของท่านแล้วเสร็จ ท่านได้ติดตามผลการดำเนินคดีกับผู้ต้องหา เพื่อนำไปวิเคราะห์ความสำเร็จหรือข้อบกพร่องในการปฏิบัติงานของท่านหรือไม่

☐ ติดตาม ☐ ไม่ได้ติดตาม

กลุ่มพนักงานอัยการ

1.ในภาพรวมของสำนวนการสอบสวนคดีอาชญากรรมคอมพิวเตอร์ที่ท่านได้รับไว้เพื่อมีความเห็นและคำสั่ง มีพยานหลักฐานเพียงพอในการทำความเห็นคำสั่งได้ในทันทีหรือไม่

☐ เพียงพอ ☐ ไม่เพียงพอ โดยมักต้องสอบสวนเพิ่มเติมในประเด็นเกี่ยวกับ

.....

.....

2.ท่านเห็นว่ามาตรฐานการสั่งคดีด้านอาชญากรรมคอมพิวเตอร์ของพนักงานอัยการซึ่งปฏิบัติงานต่างสำนักงานจากท่านมีแนวทางที่ใกล้เคียงกัน หรือแตกต่างกันอย่างไร

.....

.....

.....

3.ในงานคดีอาชญากรรมคอมพิวเตอร์ที่ท่านเคยรับผิดชอบ พบประเด็นข้อต่อสู้ในชั้นพิจารณาเกี่ยวกับ (ตอบมากกว่า 1 ข้อ)

☐ การร้องทุกข์ไม่ชอบด้วยกฎหมาย ☐ การจับกุม หรือการค้นไม่ชอบด้วยกฎหมาย

☐ การสอบสวนไม่ชอบด้วยกฎหมาย ☐ พยานหลักฐานได้มาโดยไม่ชอบด้วยกฎหมาย

☐ พยานหลักฐานถูกเปลี่ยนแปลง แก้ไข หรือทำให้เสียหาย จนไม่น่าเชื่อถือ

☐ พยานหลักฐานไม่เพียงพอที่จะบ่งชี้ว่าจำเลย คือ ผู้กระทำความผิด

☐ อื่นๆ โปรดระบุ .....

.....

4.ท่านเคยพบปัญหาในการนำเสนอพยานหลักฐานแต่ละประเภท (พยานบุคคล พยานผู้เชี่ยวชาญ พยานเอกสาร และพยานวัตถุ) ในชั้นศาลหรือไม่ อย่างไร

.....

.....

.....

.....

5.ในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ท่านเห็นว่า นอกจากพยานหลักฐานทางดิจิทัล คดีต้องมีพยานหลักฐานในส่วนใดเพิ่มเติมในการพิสูจน์การกระทำความผิดของจำเลย

.....

.....

.....

.....

6.ท่านเห็นว่ามีปัจจัยอะไรที่เป็นอุปสรรคต่อประสิทธิภาพในการดำเนินงานด้านอาชญากรรมคอมพิวเตอร์บ้าง

.....

.....

.....

ตอนที่ 3 ตัวอย่างการดำเนินงานเกี่ยวกับอาชญากรรมคอมพิวเตอร์

1.ขอให้ท่านยกตัวอย่างกรณีศึกษาที่แสดงถึงสภาพปัญหาหรืออุปสรรคที่พบในการปฏิบัติงาน/ดำเนินคดี ที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ ในความรับผิดชอบของท่าน

(ตอบได้มากกว่า 1 งาน/คดี)

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

2.จากกรณีศึกษาตามข้อ 1. ท่านเห็นว่าสภาพปัญหาและอุปสรรคที่พบคืออะไร และท่านมีข้อเสนอแนะในการจัดการกับปัญหาและอุปสรรคดังกล่าวอย่างไร

.....

.....

.....

.....

.....

.....

.....

.....

.....

3.ท่านมีข้อเสนอแนะสำหรับการเพิ่มประสิทธิภาพในการดำเนินงานเกี่ยวกับอาชญากรรมคอมพิวเตอร์อย่างไรบ้าง(เช่น ข้อเสนอแนะด้านบุคลากร ด้านอุปกรณ์ที่ใช้ดำเนินงาน ด้านเทคโนโลยีความรู้ ด้านนโยบายและงบประมาณ ด้านกฎหมาย ด้านการประสานงานระหว่างหน่วยงาน เป็นต้น)

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

ลงชื่อ ..... ผู้ตอบแบบสอบถาม

วันที่ตอบแบบสอบถาม .....

ประวัติย่อผู้วิจัย

ชื่อ นายณัฐพงษ์ พุฒแก้ว

วัน เดือน ปี เกิด 21 ธันวาคม 2507

การศึกษา นิติศาสตร์บัณฑิตมหาวิทยาลัยรามคำแหง (เกียรตินิยมอันดับสอง)
เนติบัณฑิตไทย สมัยที่ 41 (สอบได้ลำดับที่ 1)
รัฐประศาสนศาสตร์มหาบัณฑิต (นิด้า)

ประวัติการทำงานโดยย่อ

อัยการจังหวัดคดีเยาวชนและครอบครัวจังหวัดระนอง
อัยการจังหวัดคดีเยาวชนและครอบครัวจังหวัดภูเก็ต
อัยการจังหวัดตรัง
อัยการผู้เชี่ยวชาญ สำนักงานคดีอัยการสูงสุด
อัยการผู้เชี่ยวชาญพิเศษ สำนักงานอัยการพิเศษฝ่ายคดีแพ่ง ภาค 8
อัยการผู้เชี่ยวชาญพิเศษ สำนักงานอัยการพิเศษฝ่ายสถาบันกฎหมายอาญา

ตำแหน่งปัจจุบัน อัยการพิเศษฝ่าย

สรุปย่อ

ลักษณะวิชาการเมือง

เรื่อง แนวทางเพิ่มประสิทธิภาพการดำเนินคดีอาชญากรรมคอมพิวเตอร์

ผู้วิจัยนายณัฐพงษ์ พุฒแก้ว **หลักสูตร** วปอ. **รุ่นที่**61

ตำแหน่ง อัยการพิเศษฝ่ายสำนักงานอัยการสูงสุด

ความเป็นมาและความสำคัญของปัญหา

เป็นเวลามากกว่า 60 ปีที่ประเทศไทยประกาศใช้ประมวลกฎหมายอาญาเป็นกฎหมายสารบัญญัติหลักที่กำหนดให้การกระทำบางอย่างเป็นความผิดทางอาญา และประกาศใช้ประมวลกฎหมายวิธีพิจารณาความอาญาเป็นกฎหมายวิธีสบัญญัติที่กำหนดหลักเกณฑ์วิธีการในการสืบสวนสอบสวน รวบรวมพยานหลักฐาน จัดการให้ได้ตัวผู้กระทำความผิด การสืบพยาน และการพิจารณาคดีในชั้นศาล อย่างไรก็ดีเมื่อพัฒนาการของการกระทำความผิดอาชญากรรมคอมพิวเตอร์มีรูปแบบลักษณะที่แตกต่างไปจากความผิดอาญาทั่วไปตามประมวลกฎหมายอาญา รัฐจึงมีความจำเป็นในการประกาศใช้บทบัญญัติกฎหมายเฉพาะเพื่อใช้บังคับกับกรณีอย่างเหมาะสมและเพื่อให้สอดคล้องกับบริบทของสังคมโลก ในส่วนของการกระทำความผิดซึ่งใช้เทคโนโลยีคอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด และการกระทำความผิดต่อตัวระบบคอมพิวเตอร์ รัฐได้ประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 โดยในระยะแรกบทบัญญัติดังกล่าวมีต้นแบบมาจากอนุสัญญาบูดาเปสต์ว่าด้วยเรื่องอาชญากรรมทางไซเบอร์ หรือThe Budapest Convention on Cybercrime โดยอนุสัญญาดังกล่าวเป็นเพียงต้นแบบกฎหมายเพื่อให้นานาประเทศได้นำไปปรับใช้ในการบัญญัติกฎหมายภายในประเทศของตน แม้ว่าพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 จะมีผลใช้บังคับ แต่ขณะเวลาดังกล่าวคนไทยจำนวนไม่น้อยยังไม่รู้จักกับสื่อสังคมออนไลน์อย่างเช่น “LINE” “Facebook”“Instagram” “WeChat” “BeeTalk” หรือระบบการชำระเงินหรือธุรกรรมทางการเงินทางอิเล็กทรอนิกส์ อย่าง “Promptpay” “TrueMoney” หรือ“PayPal” ต่อมา รัฐได้ประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ.2560 เพื่อปรับปรุงเนื้อหาสาระของกฎหมายให้เหมาะสมกับสภาพการณ์ในปัจจุบันมากยิ่งขึ้น อย่างไรก็ดี เมื่อคนไทยรู้จักและคุ้นเคยกับธุรกรรมในโลกไซเบอร์เหล่านั้นแล้ว เทคโนโลยีในโลกไซเบอร์ก็ยังคงไม่หยุดนิ่ง เช่นเดียวกับเหล่าอาชญากรที่อาศัยช่องว่างทางเทคโนโลยีและอิสระเสรีในโลกไซเบอร์ปกปิดตัวตนและการกระทำความผิดของตนผ่านนวัตกรรมใหม่ๆ ดังเช่นการใช้สกุลเงินถอดรหัส (Cryptocurrency) ในระบบบล็อกเชน (Blockchain) จัดการกับผลประโยชน์ที่ได้

จากอาชญากรรมรวมไปถึงการฟอกเงิน ดังนั้นจึงมีความจำเป็นอย่างยิ่งยวดที่เจ้าหน้าที่บังคับใช้กฎหมายในกระบวนการยุติธรรมทางอาญาต้องเร่งสร้างความเข้าใจถึงรูปแบบของระบบปฏิบัติการของเทคโนโลยีรูปแบบใหม่เหล่านี้ เนื่องจากหัวใจหลักของมาตรฐานการพิสูจน์ความผิดของจำเลยในคดีอาญาตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 227 ที่บัญญัติว่า “ให้ศาลใช้ดุลพินิจวินิจฉัยชั่งน้ำหนักพยานหลักฐานทั้งปวง อย่าพิพากษาลงโทษจนกว่าจะแน่ใจว่ามีการกระทำผิดจริงและจำเลยเป็นผู้กระทำความผิดนั้น เมื่อมีความสงสัยตามสมควรว่าจำเลยได้กระทำผิดหรือไม่ให้ยกประโยชน์แห่งความสงสัยนั้นให้จำเลย” จึงเป็นความท้าทายของผู้มีส่วนเกี่ยวข้องในกระบวนการยุติธรรมทางอาญาที่จะรวบรวม จัดการ และนำเสนอพยานหลักฐานดิจิทัลในการดำเนินคดีอาชญากรรมคอมพิวเตอร์กับผู้กระทำความผิดเพื่อพิสูจน์ความผิดของผู้ถูกกล่าวหา

อย่างไรก็ดีเนื่องจากในคดีอาชญากรรมคอมพิวเตอร์พยานหลักฐานดิจิทัลถือเป็นพยานหลักฐานที่มีความสำคัญอย่างมาก แต่ด้วยเหตุที่พยานหลักฐานดิจิทัลมีลักษณะอ่อนไหว เสี่ยงต่อการถูกเปลี่ยนแปลงหรือสูญหายได้ง่าย รวมทั้งการเข้าถึงพยานหลักฐานดิจิทัลดังกล่าวซึ่งอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์อาจกระทบต่อสิทธิส่วนบุคคลที่ได้รับความคุ้มครองตามรัฐธรรมนูญ ซึ่งในปัจจุบันประเทศไทยยังไม่มีการบัญญัติกฎหมายวิธีพิจารณาความในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ไว้เป็นการเฉพาะ จึงมีความจำเป็นต้องศึกษาวิเคราะห์สภาพปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ตั้งแต่ชั้นของการสืบสวนสอบสวน รวบรวมพยานหลักฐาน จนถึงขั้นตอนการนำเสนอพยานหลักฐานในชั้นศาล แล้วเสนอแนะแนวทางในการแก้ไขปัญหาอย่างบูรณาการ โดยผลการศึกษานี้จะเป็นข้อมูลเพื่อนำไปสู่การปรับเปลี่ยนกระบวนทัศน์ในการบริหารจัดการคดีอาชญากรรมคอมพิวเตอร์ของหน่วยงานในกระบวนการยุติธรรมทางอาญา ได้แก่ เจ้าพนักงานตำรวจ ผู้ตรวจพิสูจน์พยานหลักฐาน พนักงานอัยการ รวมถึงข้อเสนอแนะในการแก้ไขเพิ่มเติมบทบัญญัติกฎหมายที่เกี่ยวข้อง อันจะก่อให้เกิดประสิทธิภาพในการดำเนินคดีอาชญากรรมคอมพิวเตอร์เพื่อตอบโต้อาชญากรรมทางไซเบอร์รูปแบบใหม่ๆทั้งในปัจจุบันและในอนาคต

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาสภาพปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ที่พบในชั้นการสืบสวนสอบสวน รวบรวมพยานหลักฐาน จนถึงขั้นตอนการนำเสนอพยานหลักฐานในชั้นพิจารณาของศาล
2. เพื่อวิเคราะห์ปัจจัยที่ก่อให้เกิดสภาพปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในปัจจุบัน
3. เพื่อเสนอแนะแนวทางเพิ่มประสิทธิภาพการดำเนินคดีอาชญากรรมคอมพิวเตอร์

ขอบเขตของการวิจัย

1. ขอบเขตด้านเนื้อหา มุ่งเน้นศึกษาปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในส่วนของการใช้เทคโนโลยีระบบคอมพิวเตอร์ในการกระทำความผิดที่สำคัญ อาทิเช่น การกระทำความผิดอาชญากรรมทางเศรษฐกิจและการเงินโดยใช้ระบบคอมพิวเตอร์และอุปกรณ์อิเล็กทรอนิกส์เป็นเครื่องมือในการกระทำความผิด แต่ไม่รวมถึงการกระทำความผิดในลักษณะการโจมตีระบบคอมพิวเตอร์ซึ่งเป็นเรื่องของความมั่นคงปลอดภัยทางไซเบอร์

2. ขอบเขตด้านประชากร มุ่งเน้นศึกษาแนวคิดของผู้ทรงคุณวุฒิโดยใช้วิธีการสัมภาษณ์เชิงลึกผู้ทรงคุณวุฒิด้านการสืบสวนสอบสวน การตรวจพิสูจน์ทางนิติคอมพิวเตอร์ และการดำเนินคดีอาชญากรรมคอมพิวเตอร์ รวม 12 คน

วิธีดำเนินการวิจัย

การวิจัยนี้เป็นการวิจัยเชิงคุณภาพ โดยมีการดำเนินการดังนี้

1. การรวบรวมข้อมูล

1.1 ข้อมูลทุติยภูมิ (Secondary Data) เป็นการศึกษา แนวคิด ทฤษฎี บทบัญญัติกฎหมาย รวมถึงเอกสารและงานวิจัยที่เกี่ยวข้องที่มีเนื้อหาเกี่ยวกับทฤษฎีอาชญาวิทยาทฤษฎีการรับฟังพยานหลักฐานในคดีอาญาลักษณะและรูปแบบของอาชญากรรมคอมพิวเตอร์กฎหมายที่สำคัญในการดำเนินคดีอาชญากรรมคอมพิวเตอร์และหลักกฎหมายเกี่ยวกับพยานหลักฐานในคดีอาญา

1.2 ข้อมูลปฐมภูมิ (Primary Data)ดำเนินการศึกษาและเก็บรวบรวมข้อมูลภาคสนามโดยใช้วิธีการสัมภาษณ์และแลกเปลี่ยนเรียนรู้กับกลุ่มผู้ให้ข้อมูลสำคัญที่ได้กำหนดเอาไว้ในหัวข้อขอบเขตของการวิจัย ข้อ 2 เพื่อสำรวจความคิดเห็นและข้อเสนอแนะจากเจ้าพนักงานผู้ทรงคุณวุฒิด้านการสืบสวนสอบสวน การตรวจพิสูจน์ทางนิติคอมพิวเตอร์ และการดำเนินคดีอาชญากรรมคอมพิวเตอร์ โดยใช้วิธีการสัมภาษณ์ข้อมูลเชิงลึก (In-depth Interview) จากกลุ่มตัวอย่างทั้งในกรุงเทพมหานคร และต่างจังหวัด

2. การวิเคราะห์ข้อมูล

ดำเนินการโดยการนำเอาข้อมูลที่ได้จากการศึกษาลักษณะและรูปแบบของอาชญากรรมคอมพิวเตอร์ในปัจจุบัน ทฤษฎี แนวคิดและหลักกฎหมายเกี่ยวกับการรับฟังพยานหลักฐานในคดีอาญาและการดำเนินคดีอาชญากรรมคอมพิวเตอร์มาพิจารณาร่วมกับข้อมูลผลการสัมภาษณ์เชิงลึกเจ้าพนักงานตำรวจ ผู้ตรวจพิสูจน์หลักฐาน และพนักงานอัยการ ผู้ทรงคุณวุฒิ (ข้อมูลปฐมภูมิ) โดยใช้วิธีการประสมประสานข้อมูลเข้าด้วยกัน แล้วนำข้อมูลที่ได้จากการวิเคราะห์ดังที่ได้กล่าวมาทั้งหมดมาใช้วิเคราะห์ปัจจัยที่ทำให้เกิดสภาพปัญหาและอุปสรรคในการดำเนินคดี

อาชญากรรมคอมพิวเตอร์ เพื่อเสนอแนะแนวทางเพิ่มประสิทธิภาพในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ โดยนำหลักการ ทฤษฎีและแนวคิด มารองรับข้อสรุปจากการศึกษาวิจัยอย่างเป็นเหตุเป็นผลและนำไปปฏิบัติได้จริง

ผลการวิจัย

การศึกษาครั้งนี้ผลการวิจัยสามารถตอบวัตถุประสงค์ของการวิจัยทั้ง 3 ข้อ โดยผู้วิจัยใช้การรวบรวมข้อมูลทั้งข้อมูลทุติยภูมิจากหลากหลายแหล่งข้อมูลที่เกี่ยวข้อง และรวบรวมข้อมูลปฐมภูมิจากการสัมภาษณ์เชิงลึกผู้ทรงคุณวุฒิด้านการสืบสวนสอบสวน การตรวจพิสูจน์ทางนิติคอมพิวเตอร์ และการดำเนินคดีอาชญากรรมคอมพิวเตอร์ รวมจำนวน 12 ท่าน เพื่อให้ข้อมูลที่ได้มีความเที่ยงตรงและน่าเชื่อถือ ส่วนการวิเคราะห์ข้อมูลนั้น ผู้วิจัยใช้การวิเคราะห์เนื้อหาเป็นหลัก โดยเมื่อนำข้อมูลที่รวบรวมได้มาจัดระเบียบแล้วนำมาวิเคราะห์ สังเคราะห์ ประกอบกับแนวความคิดทฤษฎีที่เกี่ยวข้อง จนกระทั่งได้แนวทางในการเพิ่มประสิทธิภาพการดำเนินคดีอาชญากรรมคอมพิวเตอร์โดยมีรายละเอียดผลการศึกษาวิจัยที่ตอบวัตถุประสงค์ทั้ง 3 ประการ สรุปได้ดังนี้

1. ผลการวิจัยตอบวัตถุประสงค์การวิจัยข้อที่ 1เพื่อศึกษาสภาพปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ที่พบในชั้นการสืบสวนสอบสวน รวบรวมพยานหลักฐาน จนถึงขั้นตอนการนำเสนอพยานหลักฐานในชั้นพิจารณาของศาล มีรายละเอียดสรุปได้ดังนี้

ระบบการดำเนินคดีอาญาของประเทศไทยเป็นระบบที่ผสมผสานระบบกล่าวหา (Inquisitorial System) และระบบไต่สวน (Accusatorial System) มาใช้ในระบบการพิจารณาคดีและการสืบพยาน คู่ความทั้งสองฝ่ายมีหน้าที่แสวงหาพยานหลักฐานมาต่อสู้หักล้างกัน ส่วนศาลจะวางตนเป็นกลางโดยพิจารณาและพิพากษาคดีจากพยานหลักฐานที่ทั้งโจทก์และจำเลยนำสืบมา โดยมีการนำกฎเกณฑ์การห้ามรับฟังพยานหลักฐานบางประเภทมาบังคับใช้เพื่อทำให้พยานหลักฐานที่จะมีน้ำหนักรับฟังในการลงโทษผู้ถูกกล่าวหาเป็นพยานหลักฐานที่น่าเชื่อถือโดยบุคคลซึ่งถูกกล่าวหาว่ามีความผิดอาญามีสิทธิที่จะได้รับการสันนิษฐานไว้ก่อนว่าบริสุทธิ์ตามหลักการสันนิษฐานว่าเป็นผู้บริสุทธิ์ (Presumption of Innocence)ซึ่งเป็นหลักการพื้นฐานที่ได้รับการรับรองตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 (ออนไลน์, 2562) มาตรา 29 และประมวลกฎหมายวิธีพิจารณาความอาญา (ออนไลน์, 2562) มาตรา 227

คดีอาชญากรรมคอมพิวเตอร์จัดเป็นคดีอาญาประเภทหนึ่งที่ผู้กล่าวหามีหน้าที่นำสืบพยานหลักฐานพิสูจน์ความผิดของผู้ถูกกล่าวหาซึ่งมาตรฐานการพิสูจน์ในคดีอาญา คือ มาตรฐาน “การพิสูจน์พ้นข้อสงสัยตามสมควร” หรือ Proof Beyond Reasonable Doubt โดยโจทก์ผู้ฟ้องคดีมีหน้าที่ต้องพิสูจน์ให้ศาลเห็นได้โดยปราศจากเหตุอันควรสงสัยว่าจำเลยเป็นผู้กระทำผิด ถ้ามี

เหตุอันควรสงสัยอย่างใดอย่างหนึ่งว่าจำเลยอาจจะไม่ใช่คนร้ายที่กระทำผิด ให้ยกประโยชน์แห่งความสงสัยนั้นให้แก่จำเลย มาตรฐานการพิสูจน์นี้ปรากฏอยู่ในประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 227ดังนั้นประสิทธิภาพในการดำเนินคดีกับผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์จนนำไปสู่การได้รับการลงโทษในกระบวนการยุติธรรม จึงขึ้นอยู่กับประสิทธิภาพในการแสวงหาและการรวบรวมพยานหลักฐานที่มีคุณค่าในเชิงพิสูจน์ ไม่ต้องห้ามรับฟังเป็นพยานหลักฐาน รวมถึงการนำเสนอพยานหลักฐานดังกล่าวสามารถร้อยเรียงเชื่อมโยงข้อเท็จจริงได้น่าเชื่อถือจนพ้นข้อสงสัยตามสมควร ซึ่งเจ้าพนักงานในกระบวนการยุติธรรมที่มีบทบาทสำคัญในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ได้แก่ เจ้าพนักงานสืบสวน พนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 (ที่แก้ไขเพิ่มเติม) พนักงานสอบสวน ผู้ตรวจพิสูจน์หลักฐาน พนักงานอัยการ และศาล

จากข้อมูลที่ได้จากการสัมภาษณ์เชิงลึกผู้ทรงคุณวุฒิด้านการสืบสวน การสอบสวน การตรวจพิสูจน์ทางนิติคอมพิวเตอร์ และการดำเนินคดีอาชญากรรมคอมพิวเตอร์ สามารถจำแนกสภาพปัญหาที่เกิดขึ้นในกระบวนการดำเนินคดีอาชญากรรมคอมพิวเตอร์ได้ดังนี้

1.1 สภาพปัญหาในส่วนของการปฏิบัติหน้าที่เฉพาะบุคคล

1.1.1 สภาพปัญหาด้านความรู้ความเข้าใจในเทคโนโลยีสมัยใหม่ ซึ่งพบว่า ผู้ปฏิบัติงานด้านการสืบสวนสอบสวน และพนักงานอัยการ ยังขาดโอกาสได้รับการฝึกอบรมความรู้ด้านเทคโนโลยีสมัยใหม่และองค์ความรู้ด้านนิติคอมพิวเตอร์เบื้องต้นในการปฏิบัติงาน อันเนื่องมาจากข้อจำกัดด้านงบประมาณ นอกจากนี้ ในด้านการอธิบายเกี่ยวกับพยานหลักฐานดิจิทัลในรูปของการรายงานผลการตรวจพิสูจน์หรือการเบิกความในชั้นศาล พบอุปสรรคในเรื่องของคำศัพท์ทางคอมพิวเตอร์ซึ่งบุคลากรในกระบวนการยุติธรรมยังขาดความคุ้นเคย

1.1.2 สภาพปัญหาด้านเครื่องมืออุปกรณ์ในการทำงาน ซึ่งพบว่า สภาพปัญหาผู้ตรวจพิสูจน์หลักฐานพบนั้นมิใช่เรื่องของการขาดความรู้ความเข้าใจเกี่ยวกับเทคโนโลยีทางคอมพิวเตอร์อย่างบุคลากรกลุ่มอื่น เพราะผู้ตรวจพิสูจน์หลักฐานมีความรู้ด้านนิติคอมพิวเตอร์ในระดับที่ดีอยู่แล้ว แต่ปัญหาที่ผู้ตรวจพิสูจน์พบนั้น เป็นเรื่องของการขาดแคลนงบประมาณเพื่อจัดหาเครื่องมืออุปกรณ์ที่ใช้ตรวจสอบอุปกรณ์ดิจิทัลที่สมัยให้เพียงพอต่อปริมาณงานที่มีแนวโน้มเพิ่มมากขึ้นในปัจจุบัน เนื่องจากซอฟท์แวร์ที่ใช้ในการปฏิบัติงานมักมีราคาสูงและต้องนำเข้าจากต่างประเทศ

1.1.3 สภาพปัญหาด้านกำลังคน ซึ่งพบว่า จำนวนผู้ตรวจพิสูจน์นิติคอมพิวเตอร์ของหน่วยงานภาครัฐยังไม่เพียงพอต่อปริมาณงานอาชญากรรมคอมพิวเตอร์ในปัจจุบัน ทำให้การตรวจพิสูจน์พยานหลักฐานดิจิทัลเกิดความล่าช้า ซึ่งอาจนำไปสู่การเกิดผลกระทบต่อความสมบูรณ์ของพยานหลักฐานดิจิทัลซึ่งเสี่ยงต่อการสูญหาย เสียหาย หรือปนเปื้อน

1.1.4 สภาพปัญหาด้านความชัดเจนเกี่ยวกับกฎหมายในการปฏิบัติงาน ซึ่งพบว่าเจ้าพนักงานมีความกังวลเกี่ยวกับอำนาจตามกฎหมายในการรวบรวมพยานหลักฐานดิจิทัล อันเนื่องมาจากสภาพของพัฒนาการด้านเทคโนโลยีสมัยใหม่ที่ข้อมูลคอมพิวเตอร์ของบุคคลมิได้จัดเก็บอยู่ในตัวอุปกรณ์ดิจิทัลเพียงอย่างเดียว เช่น การเก็บข้อมูลในระบบคลาวด์ หรือการใช้วิธีการฟิชชิ่งเพื่อให้ได้มาซึ่งรหัสผ่านระบบคอมพิวเตอร์ของคนร้าย โดยเจ้าหน้าที่ผู้ปฏิบัติงานมีความกังวลว่าอาจนำไปสู่ข้อโต้แย้งเรื่องการได้มาซึ่งพยานหลักฐานโดยมิชอบ หรือพยานหลักฐานที่ได้มาเป็นพยานหลักฐานที่เกิดขึ้นโดยมิชอบ ซึ่งจะส่งผลทำให้พยานหลักฐานที่ได้มานั้นไม่สามารถรับฟังได้ตามกฎหมาย หรือแม้จะรับฟังได้ตามกฎหมาย แต่มีน้ำหนักน่าเชื่อถือน้อย

1.2 สภาพปัญหาในส่วนของของการปฏิบัติหน้าที่สัมพันธ์กับบุคลากรกลุ่มอื่น

1.2.1 ในส่วนของพนักงานสอบสวนและผู้ตรวจพิสูจน์พยานหลักฐาน พบปัญหาการขาดการประสานงานที่เหมาะสมในการกำหนดประเด็นการแสวงหาพยานหลักฐานดิจิทัล โดยการประสานงานด้วยเอกสารหนังสือเพียงอย่างเดียวก่อให้เกิดความไม่ชัดเจนเกี่ยวกับวัตถุประสงค์ของการตรวจสอบเนื่องจากพนักงานสอบสวนมักคุ้นเคยในเรื่องทางนิติศาสตร์แต่ยังขาดความเข้าใจถึงคุณค่าของพยานหลักฐานดิจิทัลแต่ละชิ้นจึงพบข้อขัดข้องในการกำหนดประเด็นตรวจสอบไปยังผู้ตรวจพิสูจน์

1.2.2 เจ้าพนักงานผู้ปฏิบัติงานสืบสวนและงานสอบสวนพบปัญหาการได้รับความร่วมมือจากผู้ให้บริการอินเทอร์เน็ต ผู้ให้บริการเว็บไซต์ และผู้ให้บริการด้านการเงินการธนาคารในการส่งมอบข้อมูลคอมพิวเตอร์หรือพยานหลักฐานที่เกี่ยวข้องซึ่งอยู่ในความครอบครองของผู้ให้บริการดังกล่าว หรือได้รับผลการดำเนินการตามที่มีการร้องขอในเวลาที่ล่าช้าเกินสมควร

2. ผลการวิจัยตอบวัตถุประสงค์การวิจัยข้อที่ 2เพื่อวิเคราะห์ปัจจัยที่ก่อให้เกิดสภาพปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในปัจจุบัน โดยผู้วิจัยได้นำข้อมูลเกี่ยวกับสภาพปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ที่ได้จากการสัมภาษณ์เชิงลึกเจ้าพนักงานผู้ทรงคุณวุฒิดังกล่าวข้างต้นมาจัดระเบียบแล้วนำมาวิเคราะห์ สังเคราะห์ ประกอบกับแนวความคิด ทฤษฎีที่เกี่ยวข้อง สามารถจำแนกปัจจัยที่ก่อให้เกิดสภาพปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ สรุปได้ดังนี้

2.1 ปัจจัยด้านบุคลากร ทั้งปัจจัยในเรื่องของจำนวนผู้ปฏิบัติงานในกลุ่มผู้ตรวจพิสูจน์ที่มีจำนวนผู้ปฏิบัติงานด้านนิติคอมพิวเตอร์ที่สามารถจัดทำรายงานการตรวจพิสูจน์ไม่เพียงพอ และปัจจัยในเรื่ององค์ความรู้ ซึ่งผู้ปฏิบัติงานในกลุ่มเจ้าพนักงานสืบสวน พนักงานสอบสวน และพนักงานอัยการ ยังขาดความรู้ด้านเทคนิคคอมพิวเตอร์และนิติคอมพิวเตอร์ในระดับที่เพียงพอต่อการปฏิบัติงาน

2.2 ปัจจัยด้านนิติคอมพิวเตอร์ ซึ่งครอบคลุมเรื่องของความไม่เพียงพอในการจัดหาอุปกรณ์และซอฟแวร์เพื่อการตรวจพิสูจน์ และในเรื่องของความน่าเชื่อถือของพยานหลักฐานดิจิทัลที่ได้จากการแก้ไขปัญหาเฉพาะหน้าด้วยการนำซอฟท์แวร์ที่มีเผยแพร่ให้ดาวโหลดใช้โดยไม่มีค่าใช้จ่ายจากแหล่งข้อมูลเปิดมาเสริมควบคู่ไปกับซอฟท์แวร์ที่มีลิขสิทธ์หรือแม้แต่ใช้ทดแทนในบางกรณี

2.3 ปัจจัยด้านการประสานความร่วมมือ ได้แก่ ปัจจัยด้านความร่วมมือระหว่างเจ้าพนักงานในหน่วยงานยุติธรรมทางอาญาด้วยกัน ในเรื่องการประสานงานระหว่างเจ้าพนักงานสืบสวนหรือพนักงานสอบสวนกับผู้ตรวจพิสูจน์ และความร่วมมือที่เจ้าพนักงานแสวงหาจากผู้ประกอบการภาคเอกชน

2.4 ปัจจัยด้านกฎหมาย ซึ่งส่งผลกระทบต่อความเชื่อมั่นและการใช้อำนาจของผู้ปฏิบัติงานด้านอาชญากรรมคอมพิวเตอร์ จากการที่ประมวลกฎหมายวิธีพิจารณาความอาญา หรือกฎหมายพิเศษอื่นที่เกี่ยวกับการดำเนินคดีอาญาบัญญัติหลักเกณฑ์ด้านการสอบสวน การรวบรวมและการรับฟังพยานหลักฐานดิจิทัลไม่ครอบคลุมประเด็นความก้าวหน้าทางเทคโนโลยีของอุปกรณ์ดิจิทัลที่มุ่งปิดกั้นและสร้างความเป็นส่วนตัวของผู้เป็นเจ้าของข้อมูลคอมพิวเตอร์ซึ่งใช้เป็นพยานหลักฐาน

3. ผลการวิจัยตอบวัตถุประสงค์การวิจัยข้อที่ 3เพื่อเสนอแนะแนวทางเพิ่มประสิทธิภาพการดำเนินคดีอาชญากรรมคอมพิวเตอร์ พบว่าการเพิ่มประสิทธิภาพในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ซึ่งจะเป็นการบรรเทาหรือแก้ไขปัญหาที่พบระหว่างการปฏิบัติงานของเจ้าพนักงานที่เกี่ยวข้อง ต้องประกอบด้วยแนวทางดังนี้

3.1 แนวทางด้านบุคลากร

แนวทางในการแก้ไขปัญหาจำนวนเจ้าหน้าที่ผู้มีความรู้ความเชี่ยวชาญด้านเทคโนโลยีคอมพิวเตอร์และนิติคอมพิวเตอร์ ด้วยการเพิ่มจำนวนบุคลากรที่มีความรู้ความสามารถเข้าไปในระบบงานภาครัฐ อาจมิใช่แนวทางการแก้ไขปัญหาที่ดีที่สุด เนื่องจากรัฐต้องจัดเตรียมความพร้อมด้านงบประมาณให้เพียงพอต่อการเพิ่มจำนวนเจ้าหน้าที่ของรัฐ ซึ่งอาจกระทำได้ไม่ง่ายนัก เนื่องจากรัฐเองมีความจำเป็นต้องจัดสรรเงินงบประมาณเพื่อการพัฒนาประเทศด้านอื่นๆ ด้วย

ปัจจุบันรูปแบบของอาชญากรรมคอมพิวเตอร์มีหลากหลาย มีทั้งกลุ่มความผิดที่คอมพิวเตอร์เป็นวัตถุหรือเป้าหมายที่ถูกกระทำ เช่น การแฮก ดีดอส สแปม กลุ่มความผิดที่คอมพิวเตอร์ถูกใช้เป็นเครื่องมือเพื่อประกอบอาชญากรรมอย่างอื่น เช่น ฟิชชิ่งสแกมเมอร์ หรือการแสวงหาประโยชน์ทางเพศกับเด็กบนโลกออนไลน์ และกลุ่มที่มีการใช้คอมพิวเตอร์เป็นเครื่องมือจัดการกับผลประโยชน์ที่ได้จากอาชญากรรม เช่น การใช้สกุลเงินเข้ารหัส หรือ Cryptocurrency ในการจัดการกับทรัพย์สินที่ได้มาจากการประกอบอาชญากรรมเพื่อปกปิดตัวของผู้ทำธุรกรรมที่แท้จริง ซึ่งรูปแบบและลักษณะของอาชญากรรมคอมพิวเตอร์ดังที่กล่าวมาข้างต้นนี้ มีแนวโน้มของจำนวนและความซับซ้อนเพิ่มมาก

ขึ้นตามความก้าวหน้าของเทคโนโลยีด้านคอมพิวเตอร์ ดังนั้น แนวทางการเพิ่มประสิทธิภาพด้านบุคลากรผู้มีความรู้ความเชี่ยวชาญในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ที่มีความเป็นไปได้มากที่สุดในขณะที่รัฐยังไม่พร้อมทางด้านงบประมาณในการจัดจ้างบุคลากร และระบบการศึกษายังไม่สามารถผลิตบุคลากรที่มีความรู้ความเชี่ยวชาญด้านนิติคอมพิวเตอร์ได้ทันต่อความต้องการของสังคม คือ แนวทางการพัฒนาความรู้ด้านอาชญากรรมคอมพิวเตอร์ ด้วยการพัฒนาขีดความสามารถของเจ้าหน้าที่ในกระบวนการยุติธรรมซึ่งปฏิบัติหน้าที่เกี่ยวกับการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในปัจจุบัน ให้มีความรู้ความเชี่ยวชาญในการปฏิบัติงานในระดับที่เพียงพอต่อการปฏิบัติงานในความรับผิดชอบของตนและเข้าใจรูปแบบการทำงานของเจ้าพนักงานต่างหน่วยงานให้เกิดการบูรณาการด้านองค์ความรู้มากที่สุด ซึ่งเป็นแนวทางที่ INTERPOL – IGCI ของสาธารณรัฐสิงคโปร์เร่งพัฒนาและดำเนินการอยู่

3.2 แนวทางด้านอุปกรณ์เครื่องมือสำหรับงานนิติคอมพิวเตอร์

การเลือกใช้ซอฟท์แวร์จากแหล่งข้อมูลเปิดเพื่อช่วยเหลือในงานด้านการตรวจพิสูจน์นิติคอมพิวเตอร์เป็นทางปฏิบัติทั่วไปที่ผู้ตรวจพิสูจน์หลักฐานทางนิติคอมพิวเตอร์ในต่างประเทศนิยมใช้กัน โดยภาครัฐของแต่ละประเทศมีหน้าที่ในการสร้างกลไกในการสร้างความน่าเชื่อถือในพยานหลักฐานที่ได้จากการตรวจพิสูจน์โดยเครื่องมือที่พบในแหล่งข้อมูลเปิด โดยต้องมีการคำนึงถึงหลักการรับฟังพยานหลักฐานตามกฎหมายภายในของแต่ละประเทศ เพื่อหลีกเลี่ยงข้อโต้แย้งเกี่ยวกับความน่าเชื่อถือจากความเห็นของผู้เชี่ยวชาญ หรือพยานหลักฐานที่ได้จากการตรวจพิสูจน์โดยซอฟท์แวร์จากแหล่งข้อมูลเปิด อันจะเป็นแนวทางในการเพิ่มประสิทธิภาพในการดำเนินคดีอาชญากรรมคอมพิวเตอร์

3.3 แนวทางด้านการประสานความร่วมมือของผู้เกี่ยวข้อง

ในการดำเนินคดีอาญาเพื่อพิสูจน์การกระทำความผิดของผู้ถูกกล่าวหา ต้องอาศัยการปฏิบัติหน้าที่ของเจ้าพนักงานในหลายหน่วยงาน ตั้งแต่ชั้นการสืบสวน การสอบสวนรวบรวมพยานหลักฐาน การตรวจพิสูจน์พยานหลักฐาน และการดำเนินการสืบพยานในชั้นศาล เพื่อแก้ไขปัญหาความไม่เข้าใจในการขอความร่วมมือระหว่างเจ้าพนักงานสังกัดหน่วยงานที่แตกต่างกันเป็นเรื่องที่สำคัญ โดยจะส่งผลเป็นการลดระยะเวลาในการปฏิบัติงานและเพิ่มประสิทธิภาพในการทำงานมากขึ้น และโดยที่การดำเนินคดีอาชญากรรมคอมพิวเตอร์แต่ละคดีต้องอาศัยข้อมูลเกี่ยวกับการใช้บริการอินเทอร์เน็ตข้อมูลการใช้บริการโทรศัพท์ รวมถึงข้อมูลการทำธุรกรรมทางการเงินผ่านช่องทางอิเล็กทรอนิกส์ ซึ่งข้อมูลเหล่านี้อยู่ในความครอบครองของเอกชนผู้ให้บริการ ดังนั้น แนวทางในการประสานความร่วมมือระหว่างเจ้าพนักงานของรัฐและภาคเอกชน ถือเป็นเรื่องที่สำคัญอย่างมาก

3.4 แนวทางด้านกฎหมาย

มาตรการในทางกฎหมายถือเป็นเครื่องมือสำคัญในการสร้างความชัดเจนและความชอบธรรมในการปฏิบัติหน้าที่ของเจ้าพนักงานในคดีอาชญากรรมคอมพิวเตอร์ ซึ่งเป็นปัจจัยสำคัญที่จะสร้างความเชื่อมั่นในการปฏิบัติงานของเจ้าพนักงานสืบสวนสอบสวนซึ่งมีบทบาทหลักในการรวบรวมพยานหลักฐานและข้อเท็จจริงในทางคดีเพื่อนำตัวผู้กระทำผิดมาลงโทษ อันเป็นวิถีทางในการเยียวยาความเสียหายให้แก่ผู้เสียหายและสังคม และในอีกทางหนึ่งเพื่อเป็นการคุ้มครองสิทธิของประชาชนผู้ที่อาจได้รับผลกระทบจากการปฏิบัติงานของเจ้าหน้าที่ในระดับที่เหมาะสม

ข้อเสนอแนะ

ผู้วิจัยเห็นว่า แนวทางเพิ่มประสิทธิภาพการดำเนินคดีอาชญากรรมคอมพิวเตอร์มีดังนี้

1. ข้อเสนอแนะเชิงนโยบาย

1.1 หน่วยงานด้านตรวจพิสูจน์หลักฐานควรวางแผนจัดซื้ออุปกรณ์เครื่องมือและซอฟท์แวร์ ด้วยการรวบรวมสถิติปริมาณงานประกอบกับความซับซ้อนของงาน หากงานส่วนใดที่สามารถใช้ซอฟท์แวร์จากแหล่งข้อมูลเปิดมาช่วยเหลือในการปฏิบัติงานได้ ก็สมควรนำมาใช้ทดแทนอย่างเป็นทางการ โดยรัฐควรมีการจัดทำการศึกษา วิเคราะห์ และจัดทำข้อเสนอแนะเกี่ยวกับการเลือกใช้ซอฟท์แวร์จากแหล่งข้อมูลเปิดเพื่อช่วยเหลือในงานด้านการตรวจพิสูจน์นิติคอมพิวเตอร์ รวมไปถึงการกำหนดหลักเกณฑ์หรือข้อปฏิบัติที่เหมาะสมที่ผู้ตรวจพิสูจน์พึงปฏิบัติก่อนการใช้ซอฟท์แวร์จากแหล่งข้อมูลเปิดดังกล่าว

1.2 รัฐควรพิจารณานำแนวทางบทบัญญัติตาม“Computer Misuse Act (Chapter 50A) และCriminal Procedure Code(Chapter 68) ของสาธารณรัฐสิงคโปร์มาเป็นแนวทางในการปรับปรุงกฎหมายวิธีพิจารณาความอาญาของไทย เพื่อแก้ไขปัญหาความชอบด้วยกฎหมายในการใช้อำนาจบางประการของเจ้าพนักงานในการรวบรวมพยานหลักฐานดิจิทัล และหลักเกณฑ์การรับฟังพยานหลักฐานดิจิทัล เพื่อให้สอดคล้องกับเทคโนโลยีด้านคอมพิวเตอร์ที่พัฒนาอย่างต่อเนื่องไม่หยุดยั้ง

2. ข้อเสนอแนะระดับปฏิบัติการ

2.1 สำนักงานตำรวจแห่งชาติและสำนักงานอัยการสูงสุด ควรกำหนดยุทธศาสตร์การบริหารงานบุคคลทั้งในเรื่องอัตรากำลัง และการพัฒนาความรู้ความสามารถในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ที่เหมาะสม โดยสมควรนำแนวทางการสร้างหลักสูตรบนสื่ออิเล็กทรอนิกส์ (E-Learning) ตามแนวทางที่ INTERPOL – IGCI ของสาธารณรัฐสิงคโปร์ดำเนินการอยู่มาปรับใช้ รวมถึงดำเนินการเพื่อส่งเสริมให้เจ้าพนักงานของรัฐผู้ปฏิบัติงานด้านอาชญากรรมคอมพิวเตอร์สามารถเข้าศึกษาเรียนรู้หลักสูตรดังกล่าวของ INTERPOL – IGCI ตามหลักเกณฑ์เงื่อนไขที่กำหนด

เพื่อขยายฐานการเรียนรู้และข้ามพ้นสภาพการขาดแคลนงบประมาณในการจัดฝึกอบรม และสร้างการพัฒนาความรู้อย่างยั่งยืน

2.2 หน่วยงานผู้ปฏิบัติงานด้านอาชญากรรมคอมพิวเตอร์ ควรร่วมกันกำหนดตัวอย่างแนวทางการกำหนดประเด็นและรูปแบบการร้องขอให้มีการตรวจพิสูจน์พยานหลักฐานทางดิจิทัลของพนักงานสอบสวนที่ควรจะเป็นให้เหมาะสมกับประเภทของฐานความผิดในคดี และการสร้างกลไกส่งเสริมให้ผู้ประกอบการภาคเอกชนเต็มใจให้ความร่วมมือเมื่อมีการร้องขอข้อมูลจากเจ้าพนักงานของรัฐ

3. ข้อเสนอแนะเพื่อการวิจัยครั้งต่อไป

ผลการวิจัยนี้ สามารถนำไปทำการวิจัยต่อยอดได้ใน 2 ประเด็นหลัก คือ

3.1 ประเด็นแนวทางการประสานความร่วมมือของผู้เกี่ยวข้อง

ผู้วิจัยเห็นสอดคล้องกับแนวทางที่เฉลิมชนม์ แน่นหนา และคณะ (2555 : 90-91) ที่ได้เสนอให้มีการวางกรอบแนวทางการประสานงานระหว่างหน่วยงานที่ทำหน้าที่ป้องกันและปราบปรามอาชญากรรมบนสื่อออนไลน์ (ในที่นี้หมายถึงเจ้าพนักงานสืบสวนและพนักงานสอบสวน) กับหน่วยงานที่ทำหน้าที่ให้การสนับสนุน (ในที่นี้หมายถึงผู้ตรวจพิสูจน์หลักฐาน) ให้ชัดเจน โดยผู้วิจัยเห็นเพิ่มเติมว่า แนวทางที่จะทำให้การประสานงานระหว่างเจ้าพนักงานสืบสวน พนักงานสอบสวน และผู้ตรวจพิสูจน์ มีประสิทธิภาพมากขึ้น คือ การร่วมกันกำหนดตัวอย่างแนวทางการกำหนดประเด็นและรูปแบบการร้องขอให้มีการตรวจพิสูจน์พยานหลักฐานทางดิจิทัลของพนักงานสอบสวนที่ควรจะเป็นให้เหมาะสมกับประเภทของฐานความผิดในคดี เพื่อให้การปฏิบัติงานของผู้ตรวจพิสูจน์มีกรอบการดำเนินการที่ไม่กว้างเกินความจำเป็น เข้าใจในวัตถุประสงค์การตรวจพิสูจน์ ประหยัดเวลาและทรัพยากรทั้งบุคลากรและเครื่องมือที่ใช้ในการดำเนินการ ซึ่งในเรื่องนี้จำเป็นต้องมีการต่อยอดทำการศึกษาถึงแนวทางความร่วมมือที่เหมาะสม โดยควรศึกษาแนวทางที่มีการดำเนินการในต่างประเทศซึ่งผู้วิจัยเห็นว่าควรเป็นประเทศที่มีลักษณะโครงสร้างของหน่วยงานและอำนาจหน้าที่ของบุคลากรในกระบวนการยุติธรรมทางอาญาที่คล้ายคลึงกับประเทศไทยมากที่สุด เพื่อให้ได้ผลการศึกษาที่จะสามารถนำมาปรับใช้ได้ในระบบยุติธรรมของประเทศไทย

3.2 ประเด็นแนวทางการพัฒนากฎหมาย

แม้ปัจจุบันจะมีกฎหมายหลายฉบับเกี่ยวข้องกับการกำหนดความผิดซึ่งมีการใช้คอมพิวเตอร์เป็นเครื่องมือ หรือการกระทำความผิดต่อตัวระบบคอมพิวเตอร์ก็ตาม แต่ลักษณะที่กฎหมายต่างฉบับได้บัญญัติถึงอำนาจหน้าที่ในการดำเนินคดีเฉพาะประเภท และกำหนดให้มีเจ้าพนักงานที่แต่งตั้ง

เพื่อปฏิบัติตามกฎหมายนั้นๆเป็นการเฉพาะ ก่อให้เกิดความไม่ชัดเจนบางประการในกรณีที่ความผิดที่เกิดขึ้นมีความเกี่ยวพันกับกฎหมายหลายฉบับ รวมถึงบทบัญญัติในกฎหมายปัจจุบันยังไม่ครอบคลุมถึงวิธีการในการแสวงหาพยานหลักฐานด้วยเทคโนโลยีใหม่บนอุปกรณ์ดิจิทัล ซึ่งผู้วิจัยมีความเห็นต่อยอดจากความเห็นของ เฉลิมชนม์ แน่นหนา และคณะ (2555 : 90-91) ที่เสนอให้การแก้ไขกฎหมายต้องมีความชัดเจนระหว่างการกระทำความผิดอาญาตามประมวลกฎหมายอาญาหรือกฎหมายอื่นที่มีโทษทางอาญาที่ได้กระทำผ่านคอมพิวเตอร์ กับการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 กล่าวคือ ผู้วิจัยเห็นว่า ปัจจุบันในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในศาลยุติธรรม (ไม่รวมศาลชำนัญพิเศษ หรือแผนกคดีพิเศษอื่น) ใช้หลักเกณฑ์การสอบสวนและการพิจารณาคดีตามประมวลกฎหมายวิธีพิจารณาความอาญาซึ่งประกาศใช้มาเป็นระยะเวลาอันยาวนานเป็นหลัก และยังไม่มีบทบัญญัติว่าด้วยอำนาจของเจ้าพนักงานสืบสวนและพนักงานสอบสวนในการรวบรวมพยานหลักฐานดิจิทัล และหลักเกณฑ์การรับฟังพยานหลักฐานดิจิทัลโดยตรง ผู้วิจัยเห็นสมควรนำแนวทางบทบัญญัติตาม“Computer Misuse Act (Chapter 50A) และCriminal Procedure Code(Chapter 68) ของสาธารณรัฐสิงคโปร์มาเป็นแนวทางในการปรับปรุงกฎหมายวิธีพิจารณาความอาญาของไทย เพื่อแก้ไขปัญหาความคลุมเครือในการใช้อำนาจบางประการของเจ้าพนักงาน เช่น การใช้วิธีทางเทคนิคบางประการเพื่อแสวงหารหัสผ่านที่เจ้าของอุปกรณ์กำหนดใช้เพื่อป้องกันการเข้าถึงข้อมูลคอมพิวเตอร์ รวมถึงการเปลี่ยนแปลงมาตรการป้องกันการเข้าถึงโดยเฉพาะสำหรับอุปกรณ์ดิจิทัลหรือการใช้งานโปรแกรมบางอย่างเพื่อป้องกันและหยุดยั้งไม่ให้ผู้หนึ่งผู้ใดเข้าถึงข้อมูลเพื่อทำลายหรือเปลี่ยนแปลงพยานหลักฐานด้วยเทคนิคการควบคุมระยะทางไกลได้ ซึ่งในเรื่องนี้จำเป็นต้องมีการต่อยอดทำการศึกษาวิจัยถึงความซ้ำซ้อนในเรื่องอำนาจของเจ้าพนักงานผู้ปฏิบัติงานเกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ตามประมวลกฎหมายวิธีพิจารณาความอาญาซึ่งเป็นเสมือนบทกฎหมายสบัญญัติหลักที่ครอบคลุมการดำเนินคดีอาญาโดยทั่วไป และบรรดากฎหมายซึ่งกำหนดอำนาจของเจ้าพนักงานตามกฎหมายแต่ละฉบับไว้เป็นการเฉพาะ อาทิเช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 (ที่แก้ไขเพิ่มเติม) พระราชบัญญัติป้องกันและปราบปรามการค้ามนุษย์ พ.ศ. 2551 (ที่แก้ไขเพิ่มเติม) พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ.2547 (ที่แก้ไขเพิ่มเติม) และพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 เพื่อแก้ไขปัญหาความซ้ำซ้อนและไม่ชัดเจนในกรณีที่คดีอาชญากรรมคอมพิวเตอร์มีความเกี่ยวพันกับกฎหมายหลายฉบับ จากนั้นควรต้องมีการศึกษาถึงช่องว่างของกฎหมายจากการที่มีบทบัญญัติไม่ครอบคลุมประเด็นข้อกังวลใจในการใช้อำนาจของเจ้าพนักงานในการแสวงหาพยานหลักฐานเพื่อพิสูจน์การกระทำความผิดของผู้ถูกกล่าวหา เพื่อเป็นการป้องกันการโต้แย้งเกี่ยวกับอำนาจของเจ้าพนักงานในการได้มาซึ่งพยานหลักฐานในคดี

ผู้วิจัยเชื่อว่า แนวทางการเพิ่มประสิทธิภาพการดำเนินคดีอาชญากรรมคอมพิวเตอร์ดังที่กล่าวมาในงานวิจัยนี้ จะสามารถแก้ไขหรือบรรเทาปัญหาที่เจ้าพนักงานทุกภาคส่วนในกระบวนการยุติธรรมที่เกี่ยวข้องกับงานด้านการสืบสวนสอบสวน การตรวจพิสูจน์ทางนิติคอมพิวเตอร์ และการดำเนินคดีอาชญากรรมคอมพิวเตอร์ พบในการปฏิบัติงาน ในลักษณะการบูรณาการแนวทางการแก้ไขปัญหาอย่างเป็นระบบและอย่างยั่งยืน และสร้างบรรยากาศความร่วมมือในการปฏิบัติงานระหว่างเจ้าพนักงานในกระบวนการยุติธรรมด้วยกัน อันจะก่อให้เกิดประสิทธิภาพในการดำเนินคดีอาชญากรรมคอมพิวเตอร์เพื่อตอบโต้อาชญากรรมคอมพิวเตอร์รูปแบบใหม่ๆทั้งในปัจจุบันและในอนาคต