ปัญหาในการแสวงหาพยานหลักฐานในคดีอาชญากรรมทางอิเล็กทรอนิกส์

โดย
นายภัทรดิษย์ วรประดิษฐ์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต
สาขาวิชานิติวิทยาศาสตร์ แผน ก แบบ ก 2
สาขาวิชานิติวิทยาศาสตร์
มหาวิทยาลัยศิลปากร
ปีการศึกษา 2567

ปัญหาในการแสวงหาพยานหลักฐานในคดีอาชญากรรมทางอิเล็กทรอนิกส์

โดย
นายภัทรดิษย์ วรประดิษฐ์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต
สาขาวิชานิติวิทยาศาสตร์ แผน ก แบบ ก 2
สาขาวิชานิติวิทยาศาสตร์
มหาวิทยาลัยศิลปากร
ปีการศึกษา 2567

THE PROBLEMS IN OBTAINING EVIDENCE IN ELECTRONIC CRIME CASES

By

MR. Pattaradit WORAPRADITH

A Thesis Submitted in Partial Fulfillment of the Requirements

for Master of Science FORENSIC SCIENCE

Department of FORENSIC SCIENCE

Academic Year 2024

หัวข้อ	ปัญหาในการแสวงหาพยานหลักฐานในคดีอาชญากรรมทางอิเล็กทรอนิกส์
โดย	นายภัทรดิษย์ วรประดิษฐ์
สาขาวิชา	นิติวิทยาศาสตร์ แผน ก แบบ ก 2
อาจารย์ที่ปรึกษาหลัก	อาจารย์ ดร. อรทัย เขียวพุ่ม
อาจารย์ที่ปรึกษาร่วม	อาจารย์ ดร. ศิริรัตน์ ชูสกุลเกรียง

คณะวิทยาศาสตร์ มหาวิทยาลัยศิลปากร ได้รับพิจารณาอนุมัติให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต

.....คณบดีคณะวิทยาศาสตร์

(ผู้ช่วยศาสตราจารย์ ดร. กรกช ชั้นจิรกุล)

พิจารณาเห็นชอบโดย

.....ประธานกรรมการ

(อาจารย์ ดร. ศุภชัย ศุภลักษณ์นารี)

.....อาจารย์ที่ปรึกษาหลัก

(อาจารย์ ดร. อรทัย เขียวพุ่ม)

.....อาจารย์ที่ปรึกษาร่วม

(อาจารย์ ดร. ศิริรัตน์ ชูสกุลเกรียง)

.....ผู้ทรงคุณวุฒิภายนอก

(รองศาสตราจารย์ ดร. ยุภาพร สมีน้อย)

650720025 : นิติวิทยาศาสตร์ แผน ก แบบ ก 2
คำสำคัญ : การแสวงหาพยานหลักฐาน, อาชญากรรมทางอิเล็กทรอนิกส์

นาย ภัทรดิษย์ วรประดิษฐ์: ปัญหาในการแสวงหาพยานหลักฐานในคดีอาชญากรรมทางอิเล็กทรอนิกส์ อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก : อาจารย์ ดร. อรทัย เขียวพุ่ม

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อศึกษาปัญหาทางกฎหมายที่เกี่ยวข้องกับการแสวงหาหลักฐานทางอิเล็กทรอนิกส์ ซึ่งใช้เป็นพยานหลักฐานในคดีอาญา โดยเฉพาะในกระบวนการตรวจค้น การยึด และการนำเสนอพยานหลักฐานเพื่อดำเนินคดีกับผู้กระทำความผิดทางคอมพิวเตอร์และบนเครือข่ายอินเทอร์เน็ต การศึกษานี้มุ่งวิเคราะห์มาตรการทางกฎหมายของไทยที่เกี่ยวข้องกับขั้นตอนในการแสวงหาหลักฐานซึ่งเป็นข้อมูลอิเล็กทรอนิกส์ และศึกษาทฤษฎีที่เกี่ยวข้องกับการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ตามกฎหมายของไทย

การวิจัยเป็นการวิจัยเชิงคุณภาพ โดยมีผู้ให้ข้อมูลสำคัญจำนวน 9 คน ได้แก่ เจ้าหน้าที่ตำรวจ ผู้พิพากษา ทนายความ และพนักงานอัยการในพื้นที่จังหวัดสมุทรสาคร ซึ่งได้จากการเลือกแบบเจาะจง (Purposive Sampling) โดยมีเกณฑ์ในการคัดเลือกว่าต้องเป็นผู้ที่มีประสบการณ์เกี่ยวข้องกับการจัดการพยานหลักฐานในคดีอาญาไม่น้อยกว่า 5 ปี เครื่องมือที่ใช้ในการวิจัย ได้แก่ แบบสัมภาษณ์แบบมีโครงสร้าง และการวิเคราะห์ข้อมูลเชิงเนื้อหา (Content Analysis)

ผลการวิจัยพบว่า แม้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งแก้ไขเพิ่มเติม พ.ศ. 2560 และพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 จะให้อำนาจแก่เจ้าพนักงานอย่างกว้างขวาง ซึ่งช่วยในการควบคุมและปราบปรามอาชญากรรมทางเทคโนโลยี แต่ยังส่งผลกระทบต่อสิทธิและเสรีภาพของประชาชน นอกจากนี้ยังพบปัญหาในการบังคับใช้มาตรการในขั้นตอนการรวบรวมพยานหลักฐาน การเก็บรักษาและการยึดพยานหลักฐาน รวมถึงปัญหาการรับฟังพยานหลักฐานจากการใช้มาตรการที่ขาดความชัดเจนทางกฎหมาย และปัญหาในการนำเสนอพยานหลักฐานต่อศาล

โดยเฉพาะในประเทศไทย พบว่าเจ้าหน้าที่ที่เกี่ยวข้องยังขาดองค์ความรู้ที่จำเป็นในการใช้มาตรการทางกฎหมายเหล่านี้ให้ถูกต้องและสามารถนำไปสู่การรับฟังพยานหลักฐานอย่างถูกต้องตามกฎหมาย ซึ่งทำให้เกิดช่องว่างที่อาจถูกใช้เป็นช่องทางในการดำเนินการสอบสวนที่ไม่ชอบด้วยกฎหมาย ผลการศึกษานี้สามารถนำไปใช้เป็นแนวทางในการให้ความรู้เพิ่มเติมแก่เจ้าหน้าที่ที่

เกี่ยวข้อง อันจะส่งผลให้การรวบรวมพยานหลักฐานเพื่อนำไปสู่การดำเนินคดีมีประสิทธิภาพยิ่งขึ้น

650720025 : Major FORENSIC SCIENCE

Keyword : Evidence Collection Cybercrime

MR. Pattaradit WORAPRADITH : The problems in obtaining evidence in electronic crime cases Thesis advisor : Orathai Kheawpum, Ph.D.

This research aims to examine the legal challenges involved in the collection of electronic evidence for use in criminal proceedings, particularly in the processes of search, seizure, and presentation of evidence for the prosecution of offenders in computer-related and internet-based crimes. The study focuses on analyzing relevant Thai legal measures and procedures, as well as theoretical frameworks associated with the collection of electronic evidence under Thai law.

This is a qualitative study based on data collected from nine key informants, including police officers, judges, lawyers, and public prosecutors in Samut Sakhon Province. Participants were selected using purposive sampling, with the criterion that each informant must have at least five years of experience related to forensic evidence in criminal cases. Data were collected through structured interviews and analyzed using content analysis methods.

The findings reveal that although the Computer Crime Act B.E. 2550 (2007), as amended by B.E. 2560 (2017), and the Special Case Investigation Act B.E. 2547 (2004) grant broad investigative powers to authorities—which are beneficial in combating cybercrime such powers can also impact individual rights and freedoms. The study identifies several legal and procedural issues, including deficiencies in the processes of evidence seizure, preservation, and admissibility. The lack of clear legal guidelines further complicates the presentation of electronic evidence in court.

In particular, the research highlights that law enforcement officers in Thailand often lack the necessary knowledge and expertise to apply these legal measures appropriately, resulting in potential loopholes that could lead to unlawful investigative practices. The study's findings can be used to enhance the knowledge and skills of relevant personnel, thereby improving the effectiveness of evidence collection and the overall administration of justice in cybercrime cases.

มหาวิทยาลัยศิลปากร

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้ด้วยดี เนื่องจากความกรุณาและคำแนะนำจากอาจารย์ที่ปรึกษา และอาจารย์ผู้ทรงคุณวุฒิหลายท่าน ที่ได้ให้คำปรึกษาและตรวจสอบเครื่องมือวิจัยอย่างรอบคอบขอกราบขอบพระคุณ ดร.อรทัย เขียวพิมพ์ อาจารย์ที่ปรึกษา และดร.ศิริรัตน์ ชูสกุลเกรียง ที่กรุณาสอนและถ่ายทอดประสบการณ์ในการทำวิทยานิพนธ์ ให้คำแนะนำเป็นที่ปรึกษา ชี้แนะแนวทางและแก้ไขข้อผิดพลาดต่าง ๆ ตลอดการทำงาน และคอยเป็นกำลังใจในการสนับสนุนเสมอมาจนกระทั่งสามารถก้าวผ่านความกลัวและอุปสรรคต่าง ๆ ไปได้ด้วยดี

ขอกราบขอบพระคุณ ดร.ศุภชัย ศุภลักษณ์นารี ประธานกรรมการ และ ดร.ยุภาพร สมีน้อย กรรมการผู้ทรงคุณวุฒิ ที่ได้เสียสละเวลาอันมีค่าให้คำแนะนำ และช่วยเติมเต็มวิทยานิพนธ์ฉบับนี้ให้สมบูรณ์ยิ่งขึ้น

ขอขอบพระคุณครอบครัว ผู้ร่วมงาน และผู้มีพระคุณทุกท่านที่ไม่ได้กล่าวถึงชื่อ ที่ได้มีส่วนร่วมในวิทยานิพนธ์ครั้งนี้จนทำให้สำเร็จลุล่วงไปได้ด้วยดี

สุดท้ายนี้ หากวิทยานิพนธ์ฉบับนี้สามารถเป็นประโยชน์ในด้านใดต่อไปในอนาคต ผู้นำเสนอขอมอบความเคารพและขอบคุณแก่บุคคลทุกท่านที่ได้มีส่วนร่วมในกระบวนการวิจัยครั้งนี้

ภัทรดิษย์ วรประดิษฐ์

สารบัญ

หน้า

บทที่1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ผู้วิจัยเล็งเห็นว่า ปัจจุบันการพัฒนาเทคโนโลยีสารสนเทศมีความก้าวหน้าอย่างรวดเร็วและเข้ามามีบทบาทสำคัญในชีวิตประจำวันของประชาชนในสังคม ส่งผลให้เกิดการเปลี่ยนแปลงในรูปแบบการดำเนินชีวิตอย่างมีนัยสำคัญ โดยเฉพาะอย่างยิ่งในด้านการสื่อสาร เศรษฐกิจ อุตสาหกรรม และการบริการ เทคโนโลยีสารสนเทศได้ก่อให้เกิดระบบโทรคมนาคมที่ทันสมัย ทำให้ผู้คนสามารถติดต่อสื่อสารกันได้สะดวกมากยิ่งขึ้น อย่างไรก็ตาม การพัฒนาดังกล่าวย่อมมาพร้อมกับภัยคุกคามในรูปแบบใหม่ โดยเฉพาะอาชญากรรมที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์ซึ่งมีแนวโน้มเพิ่มมากขึ้นทั้งในด้านปริมาณ ความหลากหลาย และความซับซ้อน

ผู้วิจัยพบว่า อาชญากรรมทางเทคโนโลยีในปัจจุบันมีลักษณะที่เปลี่ยนแปลงตามการพัฒนาของเทคโนโลยี เช่น การโจรกรรมข้อมูลส่วนบุคคล การหลอกลวงผ่านสื่อสังคมออนไลน์ หรือการใช้ข้อมูลทางการเงินอย่างไม่ชอบด้วยกฎหมาย โดยมีวัตถุประสงค์เพื่อแสวงหาผลประโยชน์ทางทรัพย์สิน อาชญากรรมเหล่านี้มักเกี่ยวข้องกับการใช้คอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ ไม่ว่าจะเป็นโทรศัพท์มือถือ ฮาร์ดดิสก์ หรือสื่อจัดเก็บข้อมูลดิจิทัลอื่น ๆ ทั้งนี้ คอมพิวเตอร์อาจถูกใช้เป็นเครื่องมือในการกระทำความผิด หรือเกี่ยวข้องโดยตรงในฐานะที่เป็นแหล่งบันทึกข้อมูลการกระทำความผิด

ในประเทศไทย ผู้วิจัยเห็นว่าการดำเนินคดีอาญาที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์ยังประสบปัญหาในการสืบสวนสอบสวน เนื่องจากพยานหลักฐานทางอิเล็กทรอนิกส์มักตรวจจับได้ยาก อาจถูกซ่อนหรือปลอมแปลง และผู้กระทำผิดอาจใช้เทคนิคขั้นสูง เช่น การปลอมแปลง IP Address หรือใช้เซิร์ฟเวอร์ในต่างประเทศ ทำให้ยากต่อการติดตามตัวและรวบรวมหลักฐาน ด้วยเหตุนี้ แนวทางการตรวจสอบพยานหลักฐานอิเล็กทรอนิกส์จึงต้องอาศัยความรู้ทางด้านนิติวิทยาศาสตร์คอมพิวเตอร์ (Computer Forensics) เพื่อทำการตรวจสอบ วิเคราะห์ และเก็บรวบรวมข้อมูลที่เกี่ยวข้องอย่างเป็นระบบ โดยอาจตรวจสอบจากอุปกรณ์จัดเก็บข้อมูล เช่น ฮาร์ดดิสก์ CD/DVD หรืออุปกรณ์สำรองข้อมูลประเภทต่าง ๆ

ดังนั้น ผู้วิจัยจึงมีแนวคิดที่จะศึกษาเกี่ยวกับปัญหาทางกฎหมายที่เกี่ยวข้องกับกระบวนการสืบค้น ยึด และนำเสนอพยานหลักฐานอิเล็กทรอนิกส์ในคดีอาชญากรรมทางคอมพิวเตอร์ รวมถึงศึกษาข้อจำกัดในการปฏิบัติของเจ้าหน้าที่ผู้เกี่ยวข้อง ตลอดจนแนวทางการประยุกต์ใช้หลักวิชานิติวิทยาศาสตร์คอมพิวเตอร์เพื่อพัฒนาให้กระบวนการสืบสวนสอบสวนมีประสิทธิภาพ สอดคล้องกับหลักกฎหมาย และสามารถใช้ในกระบวนการพิจารณาคดีได้อย่างมีประสิทธิผล

1.2 วัตถุประสงค์ของการศึกษา

1.2.1 เพื่อศึกษาปัญหาทางกฎหมายในการแสวงหาหลักฐานทางอิเล็กทรอนิกส์ที่ใช้เป็นหลักฐานในคดี โดยพิจารณากระบวนการตรวจค้น กระบวนการยึด และการนำเสนอพยานหลักฐานเพื่อดำเนินคดีกับผู้กระทำความผิดทางคอมพิวเตอร์และบนเครือข่ายอินเทอร์เน็ต

1.2.2 เพื่อศึกษามาตรการทางกฎหมายของประเทศไทยที่เกี่ยวข้องกับวิธีการและขั้นตอนในการแสวงหาพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์

1.2.3 เพื่อศึกษาทฤษฎีที่เกี่ยวข้องกับการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ตามกฎหมายของประเทศไทย

1.3 คำถามการวิจัย

1.3.1ปัญหาทางกฎหมายและอุปสรรคที่เกิดขึ้นในกระบวนการแสวงหาพยานหลักฐานทางอิเล็กทรอนิกส์ในคดีอาชญากรรมทางคอมพิวเตอร์และบนเครือข่ายอินเทอร์เน็ตในปัจจุบันมีลักษณะอย่างไร

1.3.2กระบวนการและมาตรการในการป้องกัน รักษา และควบคุมพยานหลักฐานทางอิเล็กทรอนิกส์ในคดีอาชญากรรมทางคอมพิวเตอร์มีความเหมาะสมและเพียงพอต่อการนำไปใช้ในกระบวนการยุติธรรมหรือไม่ อย่างไร

1.3.3เทคนิค วิธีการ และขั้นตอนในการสืบสวนสอบสวนที่ใช้เพื่อระบุตัวผู้กระทำความผิดในคดีอาชญากรรมทางอิเล็กทรอนิกส์มีลักษณะอย่างไร และมีประสิทธิภาพเพียงพอต่อการดำเนินคดีตามกฎหมายหรือไม่

1.4 ขอบเขตของการวิจัย

การวิจัยครั้งนี่มีรายละเอียดการดำเนินการวิจัยดังนี้

1.4.1 ขอบเขตด้านเนื้อหา

การศึกษาครั้งนี้จะมุ่งเน้นการศึกษาการแสวงหาหลักฐานทางอิเล็กทรอนิกส์ที่ใช้เป็นหลักฐานทางคดี โดยพิจารณากระบวนการตรวจค้น กระบวนการยึด และการนำเสนอพยานหลักฐาน เพื่อดำเนินคดีกับผู้กระทำความผิดทางคอมพิวเตอร์และบนเครือข่ายอินเทอร์เน็ต โดยใช้งานแนวคิดการแสวงหาพยานหลักฐานในคดีอาชญากรรมทางอิเล็กทรอนิกส์ หลักกฎหมาย วิธีพิจารณาความอาญาที่เกี่ยวข้อง ซึ่งจะนำมาปรับใช้กับการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์

1.4.2 ขอบเขตด้านผู้ให้ข้อมูลสำคัญ

ในการวิจัยครั้งนี้ ผู้วิจัยได้กำหนดขอบเขตของผู้ให้ข้อมูลสำคัญโดยการสัมภาษณ์ผู้ที่มีความรู้ความสามารถ และมีความเชี่ยวชาญในด้านพยานหลักฐานในคดีอาชญากรรมทางอิเล็กทรอนิกส์และด้านกฎหมาย รวมถึงผู้ที่มีประสบการณ์ตรงในการดำเนินคดีอาชญากรรมทางคอมพิวเตอร์และการใช้มาตรการทางกฎหมายในการรวบรวมพยานหลักฐาน

การศึกษาครั้งนี้เป็นการวิจัยเชิงคุณภาพ เพื่อศึกษาปัญหาที่เกี่ยวข้องกับการแสวงหาพยานหลักฐานในคดีอาชญากรรมทางอิเล็กทรอนิกส์ โดยการสัมภาษณ์ผู้ปฏิบัติงานและผู้ที่มีความรู้ความสามารถ ได้แก่ ตำรวจ (หน่วยงานที่เกี่ยวข้องด้านพยานหลักฐานในคดีอาชญากรรม) ผู้พิพากษา ทนายความ และเจ้าหน้าที่ในสำนักงานอัยการ (ในพื้นที่จังหวัดสมุทรสาคร) จำนวน 9 คน

1.4.3 ขอบเขตด้านพื้นที่

ในการวิจัยครั้งนี้ ผู้วิจัยได้กำหนดขอบเขตของการศึกษาในหน่วยงานที่เกี่ยวข้องในพื้นที่จังหวัดสมุทรสาคร ซึ่งเป็นพื้นที่ที่มีความสำคัญในแง่ของการดำเนินคดีอาชญากรรมทางคอมพิวเตอร์และการรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์

1.4.4 ขอบเขตด้านระยะเวลา

ระยะเวลาในการเก็บรวบรวมข้อมูลในการวิจัยครั้งนี้อยู่ระหว่างเดือนตุลาคม พ.ศ. 2566 ถึงเดือนมีนาคม พ.ศ. 2567

1.5 นิยามศัพท์เฉพาะ

อิเล็กทรอนิกส์ หมายถึงการประยุกต์ใช้วิธีการทางอิเล็กตรอนหรือไฟฟ้าที่ใช้ในเครื่องมือและอุปกรณ์ต่าง ๆ ที่เกี่ยวข้องกับกระบวนการทางเทคโนโลยี เช่น การใช้แม่เหล็กไฟฟ้าในการถ่ายโอนข้อมูลหรือการใช้วิธีการทางคลื่นแม่เหล็กไฟฟ้าในการสื่อสาร การประยุกต์ใช้ในลักษณะนี้ช่วยให้เราสามารถสร้างเครื่องมือที่มีความซับซ้อนได้ รวมถึงการพัฒนาอุปกรณ์ต่าง ๆ ที่สามารถเก็บรักษาและประมวลผลข้อมูลได้อย่างมีประสิทธิภาพ

พยานหลักฐานดิจิทัล คือ ข้อมูลที่เก็บรักษาอยู่ในรูปแบบดิจิทัล ซึ่งสามารถใช้เป็นหลักฐานในการพิสูจน์ข้อเท็จจริงในคดีต่าง ๆ เช่น ข้อมูลจากคอมพิวเตอร์หรือโทรศัพท์มือถือที่สามารถถูกใช้ในการยืนยันเหตุการณ์หรือพฤติกรรมที่เกิดขึ้นในคดี โดยข้อมูลดิจิทัลนี้อาจเป็นสิ่งที่มนุษย์สร้างขึ้นหรือคอมพิวเตอร์เป็นผู้สร้างขึ้นเอง

ประเภทของพยานหลักฐานดิจิทัล สามารถแบ่งออกเป็น 3 ประเภทหลัก:

1.พยานหลักฐานที่มนุษย์สร้างขึ้น (Human Generated) ได้แก่ ข้อมูลที่มนุษย์เป็นผู้สร้างหรือเขียนขึ้นในระบบคอมพิวเตอร์ เช่น บทสนทนา (chat) หรือเสียงที่บันทึกในระบบอิเล็กทรอนิกส์

2.พยานหลักฐานที่คอมพิวเตอร์สร้างขึ้น (Computer Generated Evidence) คือ ข้อมูลที่เกิดจากกระบวนการคำนวณหรือการบันทึกของคอมพิวเตอร์ เช่น ประวัติการเข้าใช้งานเว็บไซต์ (internet history) หรือข้อมูลที่ถูกบันทึกโดยโปรแกรมคอมพิวเตอร์

3.พยานหลักฐานที่มนุษย์และคอมพิวเตอร์ร่วมกันสร้างขึ้น (Hybrid computer and human generated Evidence) หรือที่เรียกว่า Metadata ซึ่งเป็นข้อมูลที่เกิดจากการทำงานร่วมกันระหว่างมนุษย์และคอมพิวเตอร์ โดยอาจมีการบันทึกข้อมูลจากโปรแกรมที่สามารถวิเคราะห์ข้อมูลได้เอง เช่น การเช็กอินออนไลน์หรือข้อมูลจากอีเมล

อาชญากรรมทางอิเล็กทรอนิกส์ หมายถึงการกระทำผิดที่เกี่ยวข้องกับการใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด ซึ่งสามารถเกิดขึ้นได้ในโลกไซเบอร์ โดยการกระทำผิดเหล่านี้ไม่เพียงแต่ส่งผลกระทบต่อเหยื่อโดยตรง แต่ยังสร้างความเสียหายต่อเศรษฐกิจของประเทศในระดับที่ไม่สามารถมองข้ามได้

Computer Forensics คือ กระบวนการทางวิทยาศาสตร์ที่ใช้ในการตรวจสอบและพิสูจน์หลักฐานทางคอมพิวเตอร์ที่เกิดขึ้นในโลกไซเบอร์ โดยมุ่งเน้นที่การเก็บรวบรวมและรักษาหลักฐานที่สามารถนำไปใช้ในการสืบสวนสอบสวนหรือใช้เป็นหลักฐานในการดำเนินคดี นอกจากนี้ยังเกี่ยวข้องกับการเตรียมการรับมือกับเหตุการณ์ที่อาจเกิดขึ้นโดยไม่มีการเตรียมตัวล่วงหน้า เช่น การรับมือกับการโจมตีทางไซเบอร์หรือการเกิดเหตุการณ์ที่อาจทำลายหลักฐานสำคัญได้

1.6 ประโยชน์ที่คาดว่าจะได้รับจากการวิจัย

จากการศึกษาปัญหาเกี่ยวกับการกระทำความผิดทางอิเล็กทรอนิกส์ในปัจจุบัน ผู้วิจัยมีความมุ่งหมายที่จะศึกษารูปแบบและกระบวนการในการสืบสวนสอบสวนคดีอาชญากรรมทางอิเล็กทรอนิกส์ โดยเฉพาะในส่วนของการแสวงหาและรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ที่มีความสำคัญต่อกระบวนการยุติธรรม อันมีจุดมุ่งหมายดังต่อไปนี้

1.เพื่อศึกษาถึงปัญหาและอุปสรรคที่เกิดขึ้นในการแสวงหาและรวบรวมพยานหลักฐานในคดีอาชญากรรมทางอิเล็กทรอนิกส์ ซึ่งในทางปฏิบัติมีความซับซ้อน เนื่องจากลักษณะของข้อมูลอิเล็กทรอนิกส์มีความเปลี่ยนแปลงได้ง่าย ถูกลบหรือแก้ไขได้ในเวลาอันสั้น รวมทั้งมีข้อจำกัดในการเข้าถึงและการยอมรับในฐานะพยานหลักฐานในชั้นศาล

2.เพื่อวิเคราะห์กระบวนการและวิธีการที่ใช้ในการจัดเก็บและรักษาพยานหลักฐานอิเล็กทรอนิกส์ ตลอดจนศึกษาบทบัญญัติทางกฎหมายที่เกี่ยวข้อง ซึ่งจะนำไปสู่ความเข้าใจในกรอบของการปฏิบัติงานของเจ้าหน้าที่ผู้บังคับใช้กฎหมาย รวมถึงการประเมินความเหมาะสมและประสิทธิภาพของกระบวนการที่มีอยู่ในปัจจุบัน

3.เพื่อศึกษาแนวคิด ทฤษฎี และหลักการที่เกี่ยวข้องกับการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ตามกฎหมายของไทย โดยผู้วิจัยมุ่งหวังที่จะเชื่อมโยงหลักกฎหมายเข้ากับสภาพการณ์ในโลกดิจิทัลที่เปลี่ยนแปลงอย่างรวดเร็ว เพื่อพิจารณาว่าหลักการทางกฎหมายที่มีอยู่สามารถรองรับการกระทำผิดในรูปแบบใหม่ได้เพียงใด

4.เพื่อเสนอแนวทางในการสืบสวนและรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ที่มีประสิทธิภาพ ตลอดจนวิธีการสืบหาตัวผู้กระทำผิดในคดีอาชญากรรมทางอิเล็กทรอนิกส์ โดยพิจารณาจากทั้งมิติทางกฎหมายและมิติทางเทคโนโลยี เพื่อให้สามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างเหมาะสมและทันสมัย

บทที่ 2

วรรณกรรมที่เกี่ยวข้อง

ในบทนี้ ผู้วิจัยได้ศึกษาค้นคว้าแนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง เพื่อเป็นแนวทางในการศึกษาประเด็นที่เกี่ยวข้องกับงานวิจัยครั้งนี้ โดยมุ่งเน้นการวิเคราะห์ข้อมูล แนวทาง และวิธีการที่ปรากฏในงานวิจัยที่ผ่านมา เพื่อให้สามารถนำมาปรับใช้เป็นกรอบแนวคิดในการดำเนินการวิจัยอย่างเหมาะสม ทั้งนี้ ผู้วิจัยได้ศึกษาแนวคิดและทฤษฎีที่เกี่ยวข้องกับหัวข้อวิจัยจากบทความทางวิชาการ เพื่อรวบรวมข้อมูลและแนวคิดเพิ่มเติมอันเป็นประโยชน์ต่อการวิจัย รวมถึงได้ศึกษาเอกสารและวารสารทางวิชาการทั้งในประเทศและต่างประเทศ เพื่อติดตามองค์ความรู้และแนวโน้มล่าสุดที่เกี่ยวข้องกับประเด็นปัญหาที่ศึกษา

แนวคิดและทฤษฎีที่เกี่ยวข้อง

2.1 แนวคิดเกี่ยวกับพยานหลักฐาน

2.2 แนวคิดเกี่ยวกับพยานหลักฐานอิเล็กทรอนิกส์และการสืบหาพยานหลักฐานอิเล็กทรอนิกส์

2.3 แนวคิดเกี่ยวกับพยานหลักฐานดิจิทัลแยกออกจากพยานหลักฐานทั่วไป

2.4 แนวคิดเกี่ยวกับปัญหาการรับมือกับพยานหลักฐานอิเล็กทรอนิกส์

2.5 แนวคิดเกี่ยวกับเอกสารอิเล็กทรอนิกส์ ธุรกรรมทางอิเล็กทรอนิกส์ และข้อมูลอิเล็กทรอนิกส์ที่เกี่ยวกับการบันทึกภาพและเครื่องมืออิเล็กทรอนิกส์

2.6 ข้อมูลหลักกฎหมายวิธีพิจารณาความอาญา

2.7 งานวิจัยที่เกี่ยวข้อง

2.8 กรอบแนวคิดในการวิจัย

แนวคิดและทฤษฎีที่เกี่ยวข้อง

2.1 แนวคิดเกี่ยวกับพยานหลักฐาน

พยานหลักฐานถือเป็นองค์ประกอบสำคัญในการดำเนินกระบวนพิจารณาคดี ไม่ว่าจะเป็นคดีแพ่งหรือคดีอาญา โดยพยานหลักฐานหมายถึง สิ่งที่สามารถพิสูจน์ข้อเท็จจริงที่มีการกล่าวอ้างในการดำเนินคดีได้ ซึ่งอาจเป็นได้ทั้งบุคคล เอกสาร หรือวัตถุที่เกี่ยวข้องกับการกระทำความผิด

ในทางกฎหมาย พยานหลักฐาน หมายถึง สิ่งใด ๆ ที่สามารถจับต้องได้ตามกฎหมาย และสามารถนำเสนอในชั้นศาลเพื่อพิสูจน์ข้อเท็จจริงในคดีได้ โดยประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226 ได้บัญญัติไว้ว่า “พยานหลักฐาน ได้แก่ พยานวัตถุ พยานเอกสาร หรือพยานบุคคล ตลอดจนหลักฐานอื่น ๆ ซึ่งจะใช้เป็นเครื่องพิสูจน์การกระทำผิดได้” ตัวอย่างเช่น บุคคลที่ได้เห็นพฤติกรรมของผู้กระทำผิด ถือเป็นพยานบุคคล เอกสารที่จัดทำขึ้นโดยชอบด้วยกฎหมายหรือเกิดขึ้นจากการกระทำของผู้ใดผู้หนึ่ง ถือเป็นพยานเอกสาร และวัตถุที่ใช้ในการกระทำความผิดซึ่งตรวจพบในสถานที่เกิดเหตุ ถือเป็นพยานวัตถุ หรือวัตถุพยาน (สืบพงษ์ศิริ, 2546)

กล่าวโดยสรุป พยานหลักฐานจึงหมายถึงสิ่งใดก็ตามที่สามารถนำมาใช้เพื่อพิสูจน์ได้ว่า มีการกระทำความผิดเกิดขึ้นจริง ใช้ชี้บ่งได้ว่าใครคือผู้กระทำความผิด และสามารถเชื่อมโยงตัวผู้กระทำความผิดเข้ากับอาชญากรรมที่เกิดขึ้นได้ ทั้งนี้ พยานหลักฐานที่สำคัญตามกฎหมายไทยประกอบด้วย พยานบุคคล พยานเอกสาร และพยานวัตถุ ซึ่งมีบทบาทในการนำไปสู่ข้อเท็จจริงอันเป็นสาระสำคัญในการพิจารณาคดีของศาล

หลักเกณฑ์เกี่ยวกับกฎหมายลักษณะพยาน (ชุติวงศ์, 2552)ได้อธิบายถึงหลักเกณฑ์สำคัญในกฎหมายลักษณะพยาน ซึ่งเป็นองค์ประกอบหลักในกระบวนการพิจารณาคดีภายใต้ระบบกล่าวหา (Adversary System) โดยระบบดังกล่าวให้ความสำคัญกับกระบวนการนำสืบและการใช้พยานหลักฐานอย่างเคร่งครัด เพื่อให้ศาลสามารถวินิจฉัยข้อเท็จจริงได้อย่างถูกต้องและเป็นธรรม โดยหลักเกณฑ์เกี่ยวกับพยานในระบบกฎหมายนี้ มีอยู่ด้วยกัน 5 ประการสำคัญ ดังนี้

1.หลักเกณฑ์ว่าด้วยกรณีที่ต้องใช้หรือไม่ต้องใช้พยานหลักฐาน ในกระบวนการพิจารณาคดี ศาลต้องพิจารณาแยกแยะระหว่างปัญหาข้อกฎหมายและปัญหาข้อเท็จจริง หากเป็นปัญหาข้อกฎหมาย ศาลสามารถวินิจฉัยได้โดยไม่ต้องอาศัยพยานหลักฐาน แต่หากเป็นปัญหาข้อเท็จจริง ศาลจะต้องอาศัยพยานหลักฐานในการวินิจฉัยเพื่อให้ได้ข้อยุติ

2.หลักเกณฑ์ว่าด้วยภาระการพิสูจน์ เมื่อทราบแล้วว่าข้อเท็จจริงต้องใช้พยานหลักฐานเพื่อการพิสูจน์ ในระบบกล่าวหาถือเป็นหน้าที่ของฝ่ายคู่ความในการเสาะแสวงหาพยานหลักฐานเพื่อให้ศาลเชื่อและตัดสินให้ตนชนะคดี โดยฝ่ายใดกล่าวอ้างประเด็นใด ย่อมมีภาระในการพิสูจน์ประเด็นนั้น หรือที่เรียกว่า “ภาระการพิสูจน์” (Burden of Proof)

3.หลักเกณฑ์ว่าด้วยพยานหลักฐานใดที่รับฟังได้หรือรับฟังไม่ได้ ศาลสามารถรับฟังเฉพาะพยานหลักฐานที่ชอบด้วยกฎหมายเท่านั้น หากมีการนำพยานหลักฐานที่กฎหมายห้ามรับฟังมายื่นต่อศาล ศาลจะต้องตัดออก ไม่รับฟังในการวินิจฉัยข้อเท็จจริงในคดี ซึ่งขั้นตอนนี้เรียกว่า “บทตัดพยาน” (Exclusionary Rule) โดยหลักเกณฑ์นี้ได้รับอิทธิพลจากระบบกฎหมายคอมมอนลอว์ ซึ่งให้ประชาชนในฐานะคณะลูกขุนมีส่วนร่วมในการพิจารณาข้อเท็จจริง

4.หลักเกณฑ์ว่าด้วยวิธีการนำพยานหลักฐานเข้าสู่การพิจารณา ขั้นตอนนี้เกี่ยวข้องกับกระบวนการตามกฎหมายวิธีพิจารณาความ ที่ต้องดำเนินการให้ถูกต้อง เช่น การยื่นบัญชีระบุพยาน การแสดงสำเนาพยานเอกสาร การแจ้งให้คู่ความรับทราบ และการนำพยานเข้าสืบในศาล

5.หลักเกณฑ์ว่าด้วยการชั่งน้ำหนักพยานหลักฐาน เมื่อศาลรับฟังพยานหลักฐานเข้าสู่สำนวนแล้ว ขั้นตอนสุดท้ายคือการพิเคราะห์พยานหลักฐานว่าศาลจะให้ความเชื่อถือมากน้อยเพียงใด ซึ่งเรียกว่า “การชั่งน้ำหนักพยานหลักฐาน” (Weight of Evidence) การพิจารณาข้อเท็จจริงในขั้นตอนนี้ ศาลมีดุลพินิจอย่างเต็มที่ในการตัดสินว่าจะเชื่อหรือไม่เชื่อในพยานหลักฐานนั้น ๆ

จากหลักเกณฑ์ข้างต้น จะเห็นได้ว่าการที่ศาลจะออกหมายจับตามคำร้องขอของเจ้าหน้าที่รัฐนั้น เป็นเรื่องที่เกี่ยวข้องกับข้อเท็จจริงโดยตรง ดังนั้น เจ้าหน้าที่ผู้ร้องขอจึงมีหน้าที่ในการแสวงหาและรวบรวมพยานหลักฐานให้เพียงพอ เพื่อให้ศาลใช้ดุลพินิจพิจารณาออกหมายจับได้อย่างถูกต้องตามกฎหมาย ทั้งนี้ การแสวงหาพยานหลักฐานดังกล่าวจะต้องดำเนินการภายใต้หลักเกณฑ์ของกฎหมายลักษณะพยานอย่างเคร่งครัด

กฎแห่งพยานหลักฐาน

(สุขวัจน์, 2550)อธิบายว่าหัวใจสำคัญของกฎแห่งพยานหลักฐานมีอยู่ 2 ประการ ได้แก่ ความเป็นสาระสำคัญ (Materiality) และ การยอมรับฟังได้ (Admissibility) กล่าวคือ พยานหลักฐานหรือพยานวัตถุจะสามารถนำมาใช้เป็นหลักฐานในกระบวนการพิจารณาคดีได้ ก็ต่อเมื่อปฏิบัติให้ถูกต้องตามหลักเกณฑ์พื้นฐานของกฎหมายพยานทั้งสองประการดังกล่าว หากพยานหลักฐานใด

เบี่ยงเบนไปจากหลักเกณฑ์พื้นฐานทั้งสองประการนี้ ย่อมเป็นจุดอ่อนที่อาจถูกฝ่ายตรงข้ามยกขึ้นโต้แย้งต่อศาล ทำให้พยานหลักฐานนั้นสูญเสียคุณค่าในตัวและไม่สามารถนำไปใช้ประกอบการพิจารณาคดีได้ **(**Hobson, **1992)**

โดยหลักการแล้ว กฎแห่งพยานหลักฐานที่มีความสำคัญต่อการรวบรวมและนำเสนอพยานหลักฐานต่อศาลมี 4 ประการ ดังนี้

1.การป้องกันและรักษาสถานที่เกิดเหตุ ถือเป็นจุดเริ่มต้นที่สำคัญ โดยให้เริ่มตั้งแต่เจ้าหน้าที่คนแรกที่ไปถึงสถานที่เกิดเหตุจนกระทั่งผู้ชำนาญการได้ตรวจสอบสถานที่เกิดเหตุเสร็จสิ้น กระบวนการนี้มีเป้าหมายเพื่อป้องกันมิให้พยานหลักฐานในที่เกิดเหตุถูกทำลาย ปะปน หรือสูญหาย ซึ่งอาจส่งผลกระทบต่อความน่าเชื่อถือของพยานหลักฐานโดยตรง

2.การเก็บพยานหลักฐาน โดยชอบด้วยกฎหมาย การเก็บพยานหลักฐานจะต้องกระทำโดยบุคคลที่มีอำนาจตามกฎหมายเท่านั้น เช่น พนักงานสอบสวน เจ้าหน้าที่กองพิสูจน์หลักฐาน หรือเจ้าหน้าที่วิทยาการตำรวจ ซึ่งบุคคลเหล่านี้ต้องดำเนินการเก็บรวบรวมพยานหลักฐานในสถานที่เกิดเหตุโดยมีขั้นตอนและวิธีการที่เป็นไปตามหลักกฎหมายและหลักวิชาการ

3.การค้นหาและเก็บพยานหลักฐานอย่างเหมาะสม ผู้ตรวจสถานที่เกิดเหตุจะต้องมีความรอบคอบ ไม่ละเลยหรือมองข้ามวัตถุพยานแม้เพียงชิ้นเดียว หากมีข้อสงสัยว่าสิ่งใดอาจเป็นวัตถุพยาน ให้เก็บไว้ทั้งหมด พร้อมทั้งบันทึกรายละเอียดอย่างครบถ้วน รวมถึงการบรรจุหีบห่อและการรักษาวัตถุพยานให้อยู่ในสภาพที่ถูกต้อง ไม่เสียหายหรือปนเปื้อน เพื่อคงไว้ซึ่งคุณค่าและความเชื่อถือได้ของวัตถุพยานนั้น

4.การจัดทำหลักฐานแสดงลำดับการครอบครองพยานหลักฐาน วัตถุพยานจะต้องอยู่ภายใต้การควบคุมดูแลของบุคคลหรือหน่วยงานที่ชอบด้วยกฎหมายอย่างต่อเนื่องตั้งแต่เริ่มเก็บรวบรวมจนถึงขั้นตอนการนำเสนอในชั้นศาล โดยไม่ให้เกิดช่วงเวลาที่ไม่มีผู้รับผิดชอบต่อการครอบครอง หากมีการเปลี่ยนแปลงผู้ครอบครองวัตถุพยานในระหว่างทาง จะต้องมีหลักฐานแสดงการรับ-ส่งอย่างครบถ้วน โดยหลักฐานที่แสดงถึงความต่อเนื่องของการครอบครองนี้จะต้องระบุวัน เดือน ปี เวลา รายละเอียดของวัตถุพยาน และลายมือชื่อของผู้รับมอบไว้อย่างชัดเจน

ทั้งนี้ ในกรณีที่มีการเปลี่ยนแปลงช่วงการครอบครองวัตถุพยาน ศาลมีอำนาจเรียกพยานหลักฐานมาแสดงว่า

1.มีการดำเนินการเก็บและจำแนกวัตถุพยาน ณ สถานที่เกิดเหตุโดยถูกต้อง พร้อมระบุวันเวลา รายละเอียด และผู้ดำเนินการอย่างครบถ้วน

2.วัตถุพยานได้รับการเก็บรักษาโดยปราศจากการปนเปื้อนหรือความผิดพลาด และสามารถเข้าถึงได้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้องเท่านั้น

3.ระหว่างการขนส่งมีมาตรการป้องกันมิให้วัตถุพยานแต่ละชิ้นเกิดการปะปน และมีการบรรจุหีบห่อ พร้อมติดฉลากอย่างเหมาะสม

4.วัตถุพยานได้ถูกส่งมอบให้แก่เจ้าหน้าที่ผู้ชำนาญการหรือหน่วยงานที่เกี่ยวข้องอย่างถูกต้อง มีการลงลายมือชื่อผู้รับมอบพร้อมวันและเวลาในเอกสารรับส่ง

จากแนวปฏิบัติดังกล่าวจะเห็นได้ว่า กระบวนการจัดการกับพยานหลักฐานที่ดีและถูกต้องตามหลักการทางกฎหมาย ย่อมเป็นปัจจัยสำคัญที่ส่งผลต่อการพิจารณาคดี หากขั้นตอนใดบกพร่องอาจส่งผลให้พยานหลักฐานถูกตัดออกจากกระบวนการวินิจฉัยข้อเท็จจริงได้

พยานหลักฐานที่ดีที่สุด

ตามแนวคิดของ (คณิต, 2546)ได้กล่าวไว้เกี่ยวกับหลักการรับฟังพยานหลักฐาน ระบุว่าพยานหลักฐานทุกชนิดสามารถนำมารับฟังได้ หากมีคุณสมบัติเห็นถึงข้อเท็จจริงที่เป็นข้อพิพาทในคดี โดยทั่วไปแล้ว พยานหลักฐานจะถูกพิจารณาว่าสามารถรับฟังได้เว้นแต่จะมีข้อยกเว้นที่ระบุไว้ในกฎหมาย หากพยานหลักฐานใดไม่ตรงตามหลักเกณฑ์ดังกล่าว จะถูกจัดอยู่ในประเภทของพยานหลักฐานที่ไม่สามารถรับฟังได้ (Inadmissible evidence) ซึ่งในบรรดาพยานหลักฐานหลายประเภทที่สามารถนำมาสืบสวนได้ พยานหลักฐานที่ดีที่สุดเท่านั้นที่จะได้รับการยอมรับและนำมาพิจารณาในการตัดสินคดีได้ โดยสามารถอ้างถึงหลักการทางกฎหมายที่ระบุว่า "พยานหลักฐานที่ดีที่สุด" จะเป็นพยานที่มีความน่าเชื่อถือสูงสุดในการพิสูจน์ข้อเท็จจริงในคดีนั้น ๆ

พยานหลักฐานที่ดีที่สุด เป็นหลักการในการแบ่งประเภทของพยานหลักฐาน โดยการเปรียบเทียบระหว่างพยานหลักฐานหลายชนิดที่พิสูจน์ข้อเท็จจริงเดียวกัน ซึ่งเป็นแนวคิดที่มาจากหลักกฎหมายอังกฤษที่ระบุว่า คดีความจะต้องใช้พยานหลักฐานที่ดีที่สุดในการพิสูจน์ข้อเท็จจริง

ศาลจะไม่ยอมรับพยานบอกเล่า หากยังมีประจักษ์พยานที่สามารถพิสูจน์ข้อเท็จจริงได้ ศาลยังไม่ยอมรับสำเนาเอกสารหากต้นฉบับยังมีอยู่ และจะไม่รับฟังการสืบหาลายมือในเอกสารโดยผู้เชี่ยวชาญหากตัวผู้เขียนเอกสารยังมีชีวิตอยู่

อย่างไรก็ตาม ภายหลังการพิจารณาของนักกฎหมายพบว่า พยานหลักฐานบางประเภทสามารถรับฟังได้ โดยไม่จำเป็นต้องใช้พยานหลักฐานที่ดีที่สุดเสมอไป หากการไม่ได้นำพยานหลักฐานที่ดีที่สุดมาสืบค้น อาจกระทบต่อความน่าเชื่อถือของพยานหลักฐานในคดีนั้น ๆ ทั้งนี้ ในระบบกฎหมายของประเทศไทยก็มีบทบัญญัติหลายมาตราที่แสดงให้เห็นถึงการยอมรับหลักการพยานหลักฐานที่ดีที่สุด โดยมีข้อยกเว้นให้สามารถรับฟังสำเนาเอกสารได้ในบางกรณี ได้แก่

1.กรณีที่ทั้งสองฝ่ายตกลงกันให้สามารถนำสำเนาเอกสารมาสืบได้

2.กรณีที่ต้นฉบับเอกสารถูกทำลายหรือสูญหาย หรือไม่สามารถนำมาทำการสืบได้เนื่องจากเหตุสุดวิสัย

3.กรณีที่ศาลเห็นว่าเป็นกรณีจำเป็น และเพื่อประโยชน์แห่งความยุติธรรม ซึ่งจำเป็นต้องใช้สำเนาเอกสารนั้นในการสืบ

4.กรณีที่ต้นฉบับเอกสารอยู่ในความดูแลของทางราชการ และกรณีที่คู่ความฝ่ายหนึ่งอ้างว่าไม่สามารถนำต้นฉบับเอกสารมาสืบได้เนื่องจากมีข้อจำกัดบางประการ

ในการรับฟังพยานเอกสารในคดีอาญา ประมวลกฎหมายวิธีพิจารณาความอาญามาตรา 238 ได้บัญญัติว่า ศาลจะรับฟังได้เฉพาะต้นฉบับเอกสาร แต่หากไม่สามารถหาได้ ต้นฉบับจะถูกทดแทนด้วยสำเนาเอกสารที่ได้รับการยอมรับตามหลักเกณฑ์ที่กฎหมายกำหนด

สรุปได้ว่าการนำเสนอพยานหลักฐานที่ดีที่สุดในกระบวนการพิจารณาคดี คือต้องมีความใกล้ชิดกับเหตุการณ์ที่เกิดขึ้นมากที่สุด โดยหลักฐานต้นฉบับถือเป็นหลักฐานที่มีความสำคัญสูงสุดในการพิสูจน์ข้อเท็จจริง อย่างไรก็ตาม การนำเสนอพยานหลักฐานประเภทอื่นที่มีความเหมาะสมและสอดคล้องตามข้อกำหนดของกฎหมายก็สามารถทำได้

เมื่อพยานหลักฐานได้รับการนำเสนอตามหลักการทางกฎหมายที่ถูกต้องแล้ว จะส่งผลให้เกิดผลสำคัญ 2 ประการ คือ ความสามารถในการสืบสวนสอบสวนที่มีประสิทธิภาพ และ

ความสามารถในการใช้พยานหลักฐานดังกล่าวในการตัดสินข้อเท็จจริงในศาล การนำเสนอพยานหลักฐานที่ชอบธรรมและถูกต้องจะช่วยให้ศาลสามารถใช้ข้อมูลเหล่านั้นในการพิจารณาคดีอย่างมีความยุติธรรมและถูกต้องตามกฎหมาย

การจัดการเพื่อให้ได้มาซึ่งพยานหลักฐาน ในงานวิจัยของ (สุขาบูรณ์, 2560)ได้กล่าวถึงความสำคัญของพยานหลักฐานในกระบวนการยุติธรรมทางอาญา ซึ่งการพิสูจน์ความผิดหรือการหาความจริงในคดีอาญานั้นขึ้นอยู่กับการนำเสนอพยานหลักฐานที่มีความน่าเชื่อถือและมีคุณค่าในการแสดงข้อเท็จจริงอย่างถูกต้องและโปร่งใส กระบวนการยุติธรรมจึงจำเป็นต้องมีการรวบรวมพยานหลักฐานที่มีคุณภาพมาตั้งแต่ขั้นตอนแรกจนถึงขั้นตอนสุดท้าย เพื่อให้สามารถนำมาใช้ในการพิจารณาคดีอย่างมีประสิทธิภาพ และสามารถพิสูจน์ความผิดของผู้กระทำผิดได้อย่างยุติธรรม

กระบวนการที่มีประสิทธิภาพในการจัดการพยานหลักฐานในกระบวนการยุติธรรมควรมีลักษณะดังนี้:

1.ระบบที่เปิดโอกาสให้ทุกฝ่ายมีโอกาสเสนอพยานหลักฐาน: ตามหลักการของฟังความทุกฝ่าย (Auditors et Altera pars) ซึ่งหมายถึง การที่ทุกฝ่ายในคดีมีโอกาสเสนอและพิจารณาพยานหลักฐานอย่างเท่าเทียมกัน เพื่อให้กระบวนการยุติธรรมเป็นไปอย่างเป็นธรรมและโปร่งใส

2.การคัดกรองพยานหลักฐานที่มีคุณภาพ: กระบวนการรวบรวมพยานหลักฐานตั้งแต่ขั้นตอนการสอบสวนในชั้นตำรวจ ควรเป็นการทำงานที่มีความชำนาญและเป็นกลาง โดยไม่มีอคติหรือการแทรกแซง เพื่อให้พยานหลักฐานที่ได้มีความน่าเชื่อถือและสามารถใช้ในการพิสูจน์ข้อเท็จจริงได้อย่างถูกต้อง

3.การทดสอบและตรวจสอบพยานหลักฐาน: พยานหลักฐานที่ถูกนำเสนอให้ศาลต้องสามารถตรวจสอบได้ผ่านกระบวนการของการถามค้าน (Cross-Examination) ซึ่งจะทำให้สามารถพิสูจน์ความถูกต้องหรือความผิดพลาดของพยานหลักฐานนั้นๆ ได้ อีกทั้งยังต้องยอมให้ผู้เชี่ยวชาญทางนิติวิทยาศาสตร์สามารถพิสูจน์พยานหลักฐานและสามารถมีการคัดค้านได้จากทั้งฝ่ายโจทก์และจำเลย

จากหลักการดังกล่าว การรวบรวมและใช้พยานหลักฐานในกระบวนการยุติธรรมทางอาญาจะช่วยให้กระบวนการพิสูจน์ความผิดมีความชัดเจนและยุติธรรมมากยิ่งขึ้น โดยทุกฝ่ายจะได้รับการพิจารณาอย่างเท่าเทียมกัน และสามารถสืบสวนหาความจริงได้อย่างครบถ้วน

สรุปได้ว่าการรวบรวมพยานหลักฐานโดยพนักงานสอบสวนมีความสำคัญอย่างยิ่งในการทำให้กระบวนการยุติธรรมมีประสิทธิภาพและผลสำเร็จ การรวบรวมพยานหลักฐานที่มีความละเอียดรอบคอบและเป็นระบบจะทำให้การนำเสนอพยานหลักฐานในศาลมีความน่าเชื่อถือและมีความถูกต้อง ซึ่งจะช่วยให้กระบวนการพิสูจน์ความผิดหรือข้อเท็จจริงในคดีเป็นไปตามกฎหมาย

ประการแรกที่สำคัญคือ ความละเอียดรอบคอบในการรวบรวมพยานหลักฐานโดยพนักงานสอบสวน ซึ่งรวมถึงการเก็บรวบรวมพยานหลักฐานที่มีอยู่ในสถานที่เกิดเหตุหรือในกระบวนการสอบสวน นอกจากนี้ยังต้องพิจารณาความสามารถในการนำพยานหลักฐานเหล่านั้นไปใช้ในการเบิกความต่อศาลได้อย่างมีประสิทธิภาพ การทำเช่นนี้จะต้องปฏิบัติตามวิธีการที่กำหนดในบทบัญญัติกฎหมายอย่างเคร่งครัด เพื่อให้การสอบสวนมีความเป็นกลางและถูกต้องตามหลักการทางกฎหมาย

2.2 แนวคิดเกี่ยวกับพยานหลักฐานอิเล็กทรอนิกส์และการสืบหาพยานหลักฐานอิเล็กทรอนิกส์

2.2.1 ความหมายของพยานหลักฐานอิเล็กทรอนิกส์

ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 แก้ไขเพิ่มเติมโดย (พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์, 2544)พ.ศ. 2551 มาตรา 4 ได้กำหนดให้พยานหลักฐานอิเล็กทรอนิกส์หมายถึง สารสนเทศ (Information) หรือข้อมูล (Data) ที่อาจมีประโยชน์ต่อการสืบสวนสอบสวน ซึ่งสารสนเทศและข้อมูลเหล่านี้จะถูกจัดเก็บไว้ในอุปกรณ์อิเล็กทรอนิกส์ เช่น คอมพิวเตอร์ โทรศัพท์มือถือ หรืออุปกรณ์อิเล็กทรอนิกส์อื่น ๆ และสามารถส่งข้อมูลไปยังแหล่งข้อมูลอื่น ๆ ผ่านอุปกรณ์เหล่านี้

พยานหลักฐานอิเล็กทรอนิกส์จะเกิดขึ้นได้เมื่อมีการรวบรวมข้อมูลหรืออุปกรณ์อิเล็กทรอนิกส์ และมีการจัดเก็บเพื่อการตรวจสอบ เพื่อให้สามารถส่งข้อมูลไปยังประเทศอื่น ๆ ได้อย่างรวดเร็วและง่ายดายผ่านระบบเครือข่ายอิเล็กทรอนิกส์ นอกจากนี้ ข้อมูลอิเล็กทรอนิกส์ยังสามารถถูกแก้ไข เปลี่ยนแปลง ทำลาย หรือทำให้เสียหายได้ง่ายกว่าพยานหลักฐานประเภทอื่น ๆ เช่น พยานวัตถุที่สามารถมองเห็นหรือสัมผัสได้ด้วยมือ

โดยพยานหลักฐานอิเล็กทรอนิกส์ที่ถูกจัดเก็บในคอมพิวเตอร์หรือโทรศัพท์มือถือ จะถูกเรียกว่า "ข้อมูลอิเล็กทรอนิกส์" หรือ "ข้อมูลคอมพิวเตอร์" ซึ่งตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 แก้ไขเพิ่มเติม พ.ศ. 2551 มาตรา 4 ได้กำหนดความหมายของข้อมูล

อิเล็กทรอนิกส์เพื่อใช้เป็นพยานหลักฐานในกระบวนการยุติธรรมและการพิจารณาคดีต่าง ๆ ที่เกี่ยวข้องกับการกระทำผิดทางอิเล็กทรอนิกส์ รวมถึงการสืบสวนสอบสวนในคดีที่เกี่ยวข้องกับเทคโนโลยีและการกระทำผิดทางคอมพิวเตอร์

2.2.2 ประเภทของพยานหลักฐานอิเล็กทรอนิกส์

ตามที่(สำนักงานคณะกรรมการกฤษฎีกา, 2561)ได้พิจารณาและแบ่งประเภทข้อมูลอิเล็กทรอนิกส์ออกเป็น 3 ประเภทหลัก ได้แก่

1.ข้อมูลอิเล็กทรอนิกส์ที่เก็บไว้ในระบบคอมพิวเตอร์ ซึ่งถูกสร้างขึ้นโดยมนุษย์และประกอบด้วยข้อมูลที่มีลักษณะเป็นข้อความ รูปภาพ หรือข้อมูลอื่น ๆ ที่สามารถเข้าถึงและใช้งานได้ในระบบคอมพิวเตอร์ เช่น อีเมล แฟ้มบันทึกสารองและถาวร และเว็บไซต์

2.ข้อมูลอิเล็กทรอนิกส์ที่ถูกสร้างขึ้นโดยระบบคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ เช่น โปรแกรมคอมพิวเตอร์ แฟ้มข้อมูลชั่วคราว หรือแฟ้มประวัติของระบบ เป็นต้น

3.ระบบคอมพิวเตอร์ที่สร้างขึ้นโดยระบบคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ ทั้งสองประเภทนี้จะได้ผลลัพธ์ที่สามารถนำไปใช้ได้ในรูปแบบต่าง ๆ เช่น ข้อมูลอิเล็กทรอนิกส์ที่เป็นแผนภูมิ (Chart) ซึ่งได้จากการประมวลผลข้อมูลตัวเลขในโปรแกรมตารางการทำงานหรือคำนวณ (Spreadsheet Program)

อย่างไรก็ตาม กฎหมายไทยยังไม่มีการกำหนดประเภทของพยานหลักฐานอิเล็กทรอนิกส์และหลักเกณฑ์ในการรับรองความถูกต้องและแท้จริงของพยานหลักฐานอิเล็กทรอนิกส์อย่างชัดเจน ซึ่งจึงเป็นเหตุผลที่ควรมีการแก้ไขกฎหมายในส่วนนี้เพื่อให้การใช้งานพยานหลักฐานอิเล็กทรอนิกส์มีความชัดเจนและรองรับในกระบวนการพิจารณาคดี

ในขณะเดียวกัน พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2551 ได้ให้คำนิยามของคำต่าง ๆ ที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์ เช่น

“ข้อมูลอิเล็กทรอนิกส์” หมายถึง ข้อมูลที่ถูกสร้าง ส่ง รวบรวม หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ เช่น อีเมล โทรเลข โทรพิมพ์ หรือโทรสาร

“ข้อความ” หมายถึง เรื่องราวหรือข้อเท็จจริงที่สามารถแสดงออกในรูปแบบต่าง ๆ เช่น ตัวอักษร ตัวเลข เสียง ภาพ หรือรูปแบบอื่น ๆ ที่สามารถถ่ายทอดความหมายได้

“อิเล็กทรอนิกส์” หมายถึง การประยุกต์ใช้วิธีการทางอิเล็กทรอนิกส์ เช่น การใช้ไฟฟ้าคลื่นแม่เหล็กไฟฟ้าหรือวิธีอื่น ๆ ที่คล้ายกัน

“ข้อมูลคอมพิวเตอร์” หมายถึง ข้อมูล ข้อความ คำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์และสามารถประมวลผลได้

“ระบบคอมพิวเตอร์” หมายถึง ชุดอุปกรณ์คอมพิวเตอร์ที่เชื่อมต่อการทำงานร่วมกันและมีการกำหนดคำสั่งหรือวิธีการปฏิบัติงานให้สามารถประมวลผลข้อมูลโดยอัตโนมัติ

การที่กฎหมายไทยยังไม่มีกำหนดชัดเจนเกี่ยวกับพยานหลักฐานอิเล็กทรอนิกส์ ทำให้มีความจำเป็นที่ต้องมีการแก้ไขและพัฒนากฎหมายเพื่อรองรับความเป็นจริงในด้านการนำข้อมูลอิเล็กทรอนิกส์มาใช้ในกระบวนการยุติธรรมและกระบวนการพิจารณาคดีทางกฎหมายในอนาคต

2.2.3 ลักษณะของพยานหลักฐานอิเล็กทรอนิกส์

พยานหลักฐานอิเล็กทรอนิกส์หมายถึงข้อมูลคอมพิวเตอร์ที่ไม่ได้มีรูปแบบที่สามารถรับรู้ได้ด้วยตาเปล่าและไม่สามารถจัดเก็บได้ในรูปแบบที่เป็นมนุษย์เข้าใจได้โดยตรง ข้อมูลเหล่านี้ถูกเก็บในระบบเลขฐานสอง (Binary Number System) ซึ่งประกอบด้วยตัวเลขเพียงสองตัว คือ 0 และ 1 โดยข้อมูลในรูปแบบนี้จำเป็นต้องใช้เครื่องคอมพิวเตอร์หรือโทรศัพท์มือถือในการประมวลผลและแปลงข้อมูลดังกล่าวให้อยู่ในรูปแบบที่มนุษย์สามารถเข้าใจได้ เช่น ข้อความ รูปภาพ หรือรูปแบบอื่น ๆ ที่สามารถตีความได้ตามที่ต้องการ

สิ่งที่ทำให้พยานหลักฐานอิเล็กทรอนิกส์แตกต่างจากพยานหลักฐานประเภทอื่น ๆ คือความสามารถในการโยกย้ายข้อมูลได้อย่างง่ายดายและรวดเร็ว ซึ่งทำให้ข้อมูลอิเล็กทรอนิกส์สามารถถ่ายโอนไปยังอุปกรณ์อื่น ๆ หรือส่งไปยังที่เก็บข้อมูลอื่นได้สะดวก นอกจากนี้พยานหลักฐานอิเล็กทรอนิกส์ยังมีคุณสมบัติที่สามารถถูกแก้ไข เปลี่ยนแปลง หรือทำลายได้ง่ายโดยไม่ทิ้งร่องรอยที่สามารถสังเกตเห็นได้ด้วยตาเปล่า ซึ่งข้อจำกัดนี้เป็นสิ่งที่แตกต่างจากพยานหลักฐานประเภทอื่น ๆ เช่น พยานวัตถุที่สามารถมองเห็นและสัมผัสได้

ดังนั้น การตรวจสอบพยานหลักฐานอิเล็กทรอนิกส์ต้องอาศัยเครื่องมือและโปรแกรมเฉพาะที่สามารถช่วยในการตรวจสอบความสมบูรณ์และความถูกต้องของข้อมูล เพื่อให้แน่ใจว่าไม่มีการเปลี่ยนแปลงหรือการทำลายข้อมูลเกิดขึ้น โดยการใช้เทคนิคและเครื่องมือทางเทคโนโลยีที่เหมาะสมในการตรวจสอบความถูกต้องของข้อมูลอิเล็กทรอนิกส์จึงเป็นสิ่งที่จำเป็นในกระบวนการพิจารณาคดีทางกฎหมาย

ตารางที่ 2.1 พยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาอาญาแตกต่างไปจากพยานหลักฐานอิเล็กทรอนิกส์

พยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาความอาญา	**พยานหลักฐานอิเล็กทรอนิกส์**
1.ลักษณะรูปร่าง	
-เป็นวัตถุมีรูปร่างจับต้องได้ หรือเป็นเอกสารที่แสดงความหมายอย่างใดอย่างหนึ่ง	-เป็นคลื่นแม่เหล็กไฟฟ้าที่ไม่มีรูปร่าง จับต้องไม่ได้ มองไม่เห็นได้ด้วยตาเปล่าต้องอาศัยเครื่องคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์อย่างอื่น ๆ ในการประมวลผลให้สามารถมองเห็นและเข้าใจได้
2.การเคลื่อนย้ายเปลี่ยนทิศทาง	
-ต้องใช้แรงทางกายภาพของมนุษย์ในการเคลื่อนย้ายหลักฐาน	-เพียงสั่งเริ่มคำสั่งในการเคลื่อนย้ายข้อมูลในคอมพิวเตอร์
-การเคลื่อนย้ายหลักฐานข้ามประเทศต้องใช้ระยะเวลาและมีค่าดำเนินการ	-ใช้ระยะไม่นานและไม่สิ้นเปลืองค่าใช้จ่าย
3.การแก้ไขเปลี่ยนแปลง	
-ต้องใช้ระยะเวลาในการแก้ไขเปลี่ยนแปลง	-ใช้เวลาไม่นานในการเปลี่ยนแปลง
-มักจะมีร้องรอยการแก้ไขเปลี่ยนแปลง	-กลบเกลื่อนร่องรอยได้อย่างแนบเนียนต้อง

	อาศัยเครื่องมือในการตรวจสอบ

ที่มา : สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, (2566)

สรุปได้ว่า พยานหลักฐานอิเล็กทรอนิกส์ โดยเฉพาะที่เกี่ยวข้องกับการใช้คอมพิวเตอร์และอุปกรณ์อิเล็กทรอนิกส์ ได้ก่อให้เกิดการเปลี่ยนแปลงรูปแบบของการดำเนินการในกระบวนการยุติธรรม กล่าวคือ ข้อมูลหรือสารสนเทศที่อาจมีประโยชน์ต่อการสืบสวนสอบสวน จะถูกจัดเก็บไว้ในอุปกรณ์อิเล็กทรอนิกส์ และการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์นั้นจะเกิดขึ้นได้เมื่อมีการรวบรวมข้อมูลหรืออุปกรณ์อิเล็กทรอนิกส์ รวมถึงการจัดเก็บไว้เพื่อการตรวจพิสูจน์ผ่านระบบเครือข่าย ซึ่งเป็นลักษณะเฉพาะของพยานหลักฐานในยุคดิจิทัลที่แตกต่างจากพยานหลักฐานแบบดั้งเดิม

การสืบหาพยานหลักฐานอิเล็กทรอนิกส์

ในคดีอาชญากรรมทางคอมพิวเตอร์ การกระทำความผิดมักดำเนินการผ่านแพลตฟอร์มบนเครือข่ายอินเทอร์เน็ต เช่น สื่อสังคมออนไลน์ (Social Network) หรืออีเมล ซึ่งผู้กระทำผิดสามารถซ่อนตัวตนหรือใช้วิธีการทางเทคนิคต่าง ๆ เพื่อหลีกเลี่ยงการติดตามตัว กระบวนการสืบหาผู้กระทำความผิดในคดีอาชญากรรมทางคอมพิวเตอร์จึงมีความซับซ้อน และต้องอาศัยเครื่องมือทางเทคนิค เช่น การตรวจสอบหมายเลขไอพี (IP Address) หรือการตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) เพื่อระบุตำแหน่งหรือสถานที่ที่ใช้ในการกระทำความผิด รวมถึงเทคนิคที่ซับซ้อนขึ้น เช่น การตรวจสอบค่าการแฮช (Hash Value) ซึ่งเป็นหนึ่งในวิธีการทางนิติวิทยาศาสตร์ดิจิทัลที่ใช้ตรวจสอบความถูกต้องของข้อมูล

เมื่อเกิดเหตุความผิด ผู้เสียหายจำนวนมากมักใช้วิธีจับภาพหน้าจอ (Screenshot) จากคอมพิวเตอร์หรือโทรศัพท์ของตนเองมาเป็นหลักฐานในการแจ้งความร้องทุกข์ อย่างไรก็ตาม ภาพดังกล่าวมักไม่เพียงพอสำหรับการสืบหาตัวผู้กระทำความผิด เนื่องจากไม่สามารถยืนยันแหล่งที่มาหรือความถูกต้องของข้อมูลได้อย่างแน่นอน ดังนั้น จึงจำเป็นต้องนำรายละเอียดที่จัดเก็บไว้ในไฟล์บันทึก (Log File) มาใช้ประกอบการสืบสวน โดยเฉพาะการนำหมายเลขไอพีมาใช้เพื่อตรวจหาตัวผู้กระทำความผิด

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับแก้ไขเพิ่มเติม) พ.ศ. 2560 ได้กำหนดขั้นตอนและหลักเกณฑ์ในการเก็บพยานหลักฐานดิจิทัลไว้ โดย

บัญญัติให้เฉพาะเจ้าหน้าที่ที่ได้รับการแต่งตั้งโดยอาศัยอำนาจตามพระราชบัญญัติดังกล่าวเท่านั้นที่สามารถขอข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการอินเทอร์เน็ตที่เกี่ยวข้องได้[1] ทั้งนี้ ข้อมูลที่ได้รับจากผู้ให้บริการถือเป็นพยานหลักฐานดิจิทัลที่สำคัญในกระบวนการยุติธรรม

นอกจากนี้ การเก็บรักษาพยานหลักฐานอิเล็กทรอนิกส์จะต้องดำเนินการภายใต้กระบวนการที่เรียกว่า Digital Forensics หรือ การพิสูจน์หลักฐานทางดิจิทัล เพื่อป้องกันการปนเปื้อนหรือการดัดแปลงข้อมูล ซึ่งหากไม่มีการดำเนินการอย่างถูกต้องตามกระบวนการ อาจทำให้พยานหลักฐานดังกล่าวไม่สามารถนำมาใช้ในชั้นศาลได้

(จันทรมัสการ, 2563)ได้เสนอว่า การเก็บพยานหลักฐานดิจิทัลที่ถูกต้องตามหลักวิชาชีพมีอยู่ **3** ขั้นตอนสำคัญ ได้แก่ (1) การเก็บรวบรวม (Acquisition) (2) การวิเคราะห์ (Analysis) และ (3) การรายงานผล (Reporting) ซึ่งทั้งสามขั้นตอนนี้ต้องดำเนินการภายใต้หลักความปลอดภัยและความน่าเชื่อถือของข้อมูล เพื่อให้พยานหลักฐานดังกล่าวสามารถนำไปใช้ในการดำเนินคดีได้อย่างมีประสิทธิภาพ

1.การรวบรวมวัตถุพยานจากผู้เสียหาย

การรวบรวมวัตถุพยานทางอิเล็กทรอนิกส์ในคดีอาชญากรรมทางคอมพิวเตอร์ในเบื้องต้น มักเริ่มต้นจากการที่ผู้เสียหายเป็นผู้ดำเนินการรวบรวมพยานหลักฐานด้วยตนเอง วัตถุพยานเหล่านี้อาจอยู่ในรูปแบบของข้อความสนทนา (chat logs) ที่มีการติดต่อระหว่างผู้เสียหายกับผู้กระทำความผิด ภาพถ่ายหรือไฟล์สื่อที่มีการส่งผ่านช่องทางอิเล็กทรอนิกส์ ตลอดจนบัญชีผู้ใช้ปลอม (fake account) ซึ่งผู้เสียหายถูกใช้เป็นเครื่องมือในการหลอกลวง ไม่ว่าจะเป็นการรวบรวมข้อมูลดังกล่าวด้วยตนเอง หรือการนำอุปกรณ์อิเล็กทรอนิกส์ เช่น เครื่องคอมพิวเตอร์หรือโทรศัพท์เคลื่อนที่ มาให้พนักงานเจ้าหน้าที่ดำเนินการรวบรวมและตรวจสอบข้อมูล ก็ล้วนถือเป็นจุดเริ่มต้นของกระบวนการสืบสวนและติดตามตัวผู้กระทำความผิด

ในกรณีที่บัญชีผู้ใช้ของผู้กระทำความผิดยังคงสามารถใช้งานได้ และยังไม่ถูกระงับหรือปิดการใช้งาน ผู้เสียหายอาจสามารถดำเนินการติดต่อสื่อสารกับผู้กระทำความผิดต่อไปได้ ซึ่งเป็นประโยชน์ต่อกระบวนการสืบสวน อย่างไรก็ดี หากไม่สามารถติดต่อกับผู้กระทำความผิดได้อีก หรือบัญชีดังกล่าวถูกลบหรือระงับการใช้งานไปแล้ว จะส่งผลให้การติดตามตัวผู้กระทำ

ความผิดเป็นไปด้วยความยากลำบาก และอาจเป็นอุปสรรคสำคัญในกระบวนการสืบสวนสอบสวนและดำเนินคดี

2.การรวบรวมพยานหลักฐานจากผู้ให้บริการอินเทอร์เน็ต

ในการติดต่อสื่อสารผ่านแพลตฟอร์มต่าง ๆ เช่น Facebook หรือแอปพลิเคชันส่งข้อความออนไลน์ ข้อมูลที่เกิดขึ้นในระหว่างการสนทนาสามารถถือเป็นวัตถุพยานทางอิเล็กทรอนิกส์ที่มีความสำคัญยิ่งต่อการสืบสวนและดำเนินคดีทางกฎหมาย ทั้งนี้ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับแก้ไขเพิ่มเติม) พ.ศ. 2560 ได้กำหนดให้ผู้ให้บริการอินเทอร์เน็ต **(**Internet Service Providers: ISP) มีหน้าที่จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ **(**Traffic Data) เป็นระยะเวลาไม่น้อยกว่า 90 วัน เพื่อสนับสนุนการดำเนินงานของเจ้าหน้าที่รัฐในการติดตามตัวผู้กระทำความผิดเมื่อเกิดเหตุอาชญากรรมทางคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์ดังกล่าวประกอบด้วยรายละเอียดเกี่ยวกับหมายเลขไอพีแอดเดรส (IP Address) ซึ่งสามารถบ่งชี้ได้ว่ามีการติดต่อสื่อสารกันระหว่างหมายเลขไอพีใด ในช่วงเวลาใด เริ่มต้นและสิ้นสุดเมื่อใด รวมถึงเบอร์โทรศัพท์ที่ใช้ในการเชื่อมต่ออินเทอร์เน็ต โดยเจ้าหน้าที่สามารถอาศัยอำนาจตามกฎหมายขอข้อมูลจากผู้ให้บริการได้ เพื่อทำการตรวจสอบว่าหมายเลขไอพีหรือหมายเลขโทรศัพท์ดังกล่าวได้ลงทะเบียนไว้ในชื่อของบุคคลใด และมีที่อยู่ในการใช้งานอยู่ที่ใด ซึ่งเป็นข้อมูลพื้นฐานที่ช่วยนำไปสู่การติดตามตัวผู้กระทำความผิดได้ในลำดับต่อไป

อย่างไรก็ตาม กรณีที่เป็นการติดต่อผ่านบัญชีผู้ใช้ปลอม (Fake Account) โดยเฉพาะในลักษณะที่ผู้เสียหายไม่สามารถระบุตัวตนที่แท้จริงของอีกฝ่ายได้ อาจก่อให้เกิดอุปสรรคต่อการสืบสวนอย่างมาก เนื่องจากผู้เสียหายจะทราบเพียงชื่อบัญชีหรือรูปโปรไฟล์ที่ปรากฏ ซึ่งอาจไม่มีความเกี่ยวข้องกับผู้กระทำความผิดตัวจริงเลย อย่างไรก็ตาม หากผู้ให้บริการอินเทอร์เน็ตหรือแพลตฟอร์มให้ความร่วมมือในการตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์ เจ้าหน้าที่ก็ยังคงสามารถดำเนินการตรวจสอบย้อนกลับไปยังต้นทางของการเชื่อมต่อได้

การตรวจสอบและติดตามหมายเลขไอพีแอดเดรส (IP Address) เป็นกระบวนการที่ต้องอาศัยความรู้ความชำนาญทางด้านเทคโนโลยีสารสนเทศอย่างมาก เจ้าหน้าที่ผู้ดำเนินการต้องเป็นบุคคลที่ได้รับการแต่งตั้งตามที่กฎหมายกำหนดจึงจะมีอำนาจในการรวบรวม ตรวจสอบ และใช้ข้อมูลดังกล่าวเป็นพยานหลักฐานในกระบวนการยุติธรรม ทั้งนี้ ไอพีแอดเดรสประกอบด้วย

ตัวเลขสี่ชุด โดยมีเครื่องหมายจุด (.) คั่นระหว่างชุด ซึ่งสามารถใช้ระบุได้ว่าเครื่องคอมพิวเตอร์นั้นอยู่ในเครือข่ายใด เป็นเครื่องใดในเครือข่าย และมีตำแหน่งที่ตั้งอยู่ ณ ที่ใด

เมื่อเจ้าหน้าที่ได้รับข้อมูลไอพีแอดเดรสดังกล่าวแล้ว อาจดำเนินการตรวจสอบเพิ่มเติมผ่านเว็บไซต์หรือโปรแกรมที่สามารถระบุตำแหน่งทางภูมิศาสตร์ของไอพี หรือใช้ตรวจสอบความเชื่อมโยงของอุปกรณ์ที่เชื่อมต่อในขณะเกิดเหตุ ซึ่งข้อมูลเหล่านี้สามารถนำไปใช้ประกอบการสืบสวน และหากเก็บรวบรวมโดยถูกต้องตามขั้นตอนที่กฎหมายกำหนดแล้ว ก็สามารถนำมาใช้เป็นพยานหลักฐานในชั้นศาลได้ต่อไป ดังนั้น การรวบรวมและตรวจสอบหลักฐานดิจิทัลจึงต้องกระทำด้วยความระมัดระวัง และควรมีมาตรการปกป้องพยานหลักฐานไม่ให้เกิดการปนเปื้อนหรือการเปลี่ยนแปลงใด ๆ เพื่อให้สามารถใช้อ้างอิงทางกฎหมายได้อย่างมีประสิทธิภาพ

3.การรวบรวมพยานหลักฐานจากผู้กระทำความผิด

ในกรณีของการกระทำความผิดทางคอมพิวเตอร์ พยานหลักฐานที่สำคัญมักจะเป็นวัตถุพยานปลายทาง ซึ่งเป็นข้อมูลหรืออุปกรณ์ของผู้กระทำความผิด เช่น โทรศัพท์มือถือ เครื่องคอมพิวเตอร์ รูปภาพ หรือไฟล์ข้อมูลอื่น ๆ ที่ใช้ในการแอบอ้าง ปลอมแปลง หรือหลอกลวงผ่านบัญชีผู้ใช้งานบนเครือข่ายอินเทอร์เน็ต การดำเนินการเพื่อตรวจสอบและจับกุมผู้กระทำความผิดพร้อมกับอุปกรณ์ที่ใช้ในการกระทำความผิดจึงเป็นขั้นตอนที่สำคัญ โดยมีความท้าทายเนื่องจากผู้กระทำความผิดส่วนใหญ่เป็นบุคคลต่างชาติที่มักเดินทางไปมาหลายพื้นที่และไม่คงที่ในที่อยู่อาศัย อีกทั้งยังอาจใช้บุคคลอื่นในการกระทำความผิดแทนตนเอง ทำให้การสืบสวนและจับกุมยากลำบาก เว้นแต่ผู้กระทำผิดจะพำนักอยู่ในประเทศไทยและลงมือกระทำความผิดด้วยตนเอง การจับกุมตัวผู้กระทำผิดในกรณีนี้จึงมีความเป็นไปได้มากขึ้น

ในกรณีที่สามารถจับกุมผู้กระทำความผิดได้พร้อมกับอุปกรณ์ที่เกี่ยวข้อง การตรวจสอบเพื่อยืนยันตัวบุคคลว่าเป็นผู้กระทำความผิดตามที่กล่าวหาเป็นขั้นตอนที่สำคัญ โดยกระบวนการตรวจสอบนี้จำเป็นต้องใช้เทคนิคและความรู้เฉพาะทางด้านคอมพิวเตอร์อย่างมาก กระบวนการที่สำคัญในการพิสูจน์พยานหลักฐานดิจิทัลคือ การสร้างค่าแฮช (Hash Value) ซึ่งเป็นกระบวนการทางคณิตศาสตร์ในการคำนวณไฟล์หรือข้อมูลต่าง ๆ เช่น รูปภาพ เอกสาร หรือข้อมูลในฮาร์ดไดรฟ์ เพื่อให้ได้ชุดตัวเลขหรือตัวอักษรที่มีลักษณะเฉพาะตัว เปรียบเสมือน “ลายนิ้วมือดิจิทัล” ของไฟล์ดังกล่าว

กระบวนการนี้จะช่วยให้สามารถตรวจสอบและยืนยันได้ว่าไฟล์หรือข้อมูลนั้นไม่ได้ถูกดัดแปลงแก้ไขระหว่างทาง โดยจะใช้ค่าแฮชที่ได้จากกระบวนการนี้มาเปรียบเทียบกับพยานหลักฐานที่มีอยู่ หากค่าแฮชจากข้อมูลของผู้เสียหายและจากผู้กระทำความผิดตรงกัน หรือมีการจับคู่ค่าแฮช (Match) กัน ก็สามารถยืนยันได้ว่าไฟล์หรือข้อมูลนั้นเป็นของผู้กระทำความผิดตัวจริง

ในประเทศไทย เครื่องมือที่นิยมใช้ในการคำนวณค่าแฮชคือ Message Digest 5 (MD5) และ Secure Hash Algorithm 1 (SHA-1) โดยกระบวนการนี้จะไม่สนใจลักษณะของไฟล์ เช่น ชื่อไฟล์ ขนาดของไฟล์ หรือความยาวของไฟล์ แต่จะคำนวณจากลักษณะเฉพาะของเนื้อหาภายในไฟล์นั้น ๆ เพื่อให้ได้ค่าแฮชที่เป็นเอกลักษณ์เฉพาะตัวของไฟล์แต่ละชิ้น

การสร้างค่าแฮชจึงเป็นเครื่องมือที่สำคัญในการพิสูจน์ความถูกต้องของพยานหลักฐานดิจิทัล ซึ่งสามารถช่วยให้กระบวนการยุติธรรมไม่ถูกหลอกลวงหรือเข้าใจผิด โดยพยานหลักฐานดิจิทัลนั้นต้องได้รับการจัดการด้วยความระมัดระวัง เนื่องจากข้อมูลในรูปแบบดิจิทัลนั้นสามารถถูกดัดแปลงหรือสูญหายได้ง่าย การเก็บรวบรวม การเก็บรักษา และการตรวจวิเคราะห์ข้อมูลเหล่านี้จึงต้องมีมาตรการที่เข้มงวด หากดำเนินการไม่ถูกต้องอาจทำให้พยานหลักฐานเสียหายและหมดความน่าเชื่อถือได้ ซึ่งอาจส่งผลต่อกระบวนการพิจารณาคดีในชั้นศาล

ตามที่(ทรรศนกุลพันธ์, 2562)รวมถึงคมสัน สีหมื่นตรี (2560) ได้กล่าวไว้ว่าพยานหลักฐานดิจิทัลนั้นมีความเกี่ยวข้องโดยตรงและโดยอ้อมกับเทคโนโลยี และมีลักษณะที่ละเอียดอ่อน เปลี่ยนแปลงหรือสูญหายได้ง่าย ซึ่งหากไม่มีการจัดการที่ถูกต้องและระมัดระวัง อาจทำให้พยานหลักฐานนั้นหมดความน่าเชื่อถือและไม่สามารถนำมาใช้ในกระบวนการยุติธรรมได้

การรักษาความน่าเชื่อถือของพยานหลักฐาน

ในกระบวนการดำเนินคดีที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี การรักษาความน่าเชื่อถือของพยานหลักฐานดิจิทัลเป็นสิ่งสำคัญที่ไม่สามารถมองข้ามได้ เนื่องจากพยานหลักฐานเหล่านี้มักมีลักษณะที่สามารถถูกเปลี่ยนแปลงได้ง่าย เช่น ไฟล์ข้อมูล รูปภาพ หรือข้อความที่ถูกบันทึกผ่านอุปกรณ์อิเล็กทรอนิกส์ต่างๆ ดังนั้น การรักษาความน่าเชื่อถือของพยานหลักฐานจึงจำเป็นต้องพึ่งพาหลักการสำคัญ 3 ประการที่ได้รับการยอมรับในวงการกฎหมายและการตรวจสอบพยานหลักฐานดิจิทัลดังนี้

1. การยืนยันว่าเป็นพยานหลักฐานที่แท้จริง (Authentication of Evidence) การยืนยันว่าเป็นพยานหลักฐานที่แท้จริง หรือ Authentication เป็นกระบวนการที่สำคัญในการพิสูจน์ว่าพยานหลักฐานที่นำเสนอในกระบวนการพิจารณาคดีนั้นไม่ได้ถูกดัดแปลงหรือลบข้อมูลใดๆ ซึ่งการพิสูจน์ความแท้จริงของพยานหลักฐานนั้นมักทำโดยการเปรียบเทียบค่าแฮช (Hash Value) ของไฟล์หรือข้อมูลในช่วงเวลาที่เก็บรวบรวมกับค่าแฮชที่ได้จากข้อมูลที่นำเสนอในศาล การเปรียบเทียบค่าแฮชนี้จะทำให้มั่นใจได้ว่าพยานหลักฐานยังคงความสมบูรณ์และไม่ถูกดัดแปลงระหว่างการจัดเก็บหรือการส่งต่อข้อมูลไปยังหน่วยงานที่เกี่ยวข้อง

2. การรักษาห่วงโซ่ของพยานหลักฐาน (Chain of Custody) การรักษาห่วงโซ่ของพยานหลักฐานเป็นกระบวนการที่เกี่ยวข้องกับการติดตามและบันทึกการเคลื่อนย้ายพยานหลักฐานตลอดกระบวนการทางกฎหมาย ตั้งแต่การเก็บรวบรวมพยานหลักฐานไปจนถึงการนำเสนอในศาล การรักษาห่วงโซ่ของพยานหลักฐานช่วยให้สามารถพิสูจน์ได้ว่า ไม่มีการดัดแปลงหรือการเข้าถึงโดยมิชอบพยานหลักฐานในระหว่างขั้นตอนการเก็บรวบรวมและการส่งต่อ การบันทึกการเปลี่ยนมือและการเคลื่อนย้ายพยานหลักฐานถือเป็นหลักการที่สำคัญในการรักษาความน่าเชื่อถือ

3. การยืนยันความถูกต้องของพยานหลักฐาน (Evidence Validation) การยืนยันความถูกต้องของพยานหลักฐานหมายถึงการตรวจสอบความสมบูรณ์และความถูกต้องของข้อมูลที่ได้รับการรวบรวม ซึ่งสามารถทำได้โดยการตรวจสอบรูปแบบหรือเนื้อหาของข้อมูล เช่น การตรวจสอบไฟล์รูปภาพที่แสดงข้อมูลระยะเวลาและสถานที่ที่สามารถเชื่อมโยงกับเหตุการณ์ที่เกิดขึ้นในคดี หรือการใช้เครื่องมือทางเทคนิคในการตรวจสอบความถูกต้องของไฟล์ข้อมูล การยืนยันความถูกต้องนี้จะช่วยให้มั่นใจได้ว่าพยานหลักฐานที่ใช้ในการพิจารณาคดีนั้นมีความเหมาะสมและถูกต้องตามกระบวนการทางกฎหมาย

ความสำคัญของการรักษาความน่าเชื่อถือของพยานหลักฐาน หลักการทั้งสามข้างต้นเป็นสิ่งสำคัญที่ช่วยให้กระบวนการพิจารณาคดีในคดีอาชญากรรมทางเทคโนโลยีสามารถดำเนินไปอย่างยุติธรรม การรักษาความน่าเชื่อถือของพยานหลักฐานดิจิทัลไม่เพียงแต่ช่วยป้องกันการดัดแปลงพยานหลักฐาน แต่ยังช่วยให้การพิจารณาคดีเป็นไปด้วยความโปร่งใสและสามารถพิสูจน์ได้ว่าผู้กระทำความผิดเป็นบุคคลที่แท้จริง ตามหลักการของการพิสูจน์ทางกฎหมาย

การรักษาความน่าเชื่อถือของพยานหลักฐานเป็นขั้นตอนที่สำคัญที่สามารถส่งผลกระทบต่อผลการพิจารณาคดี โดยเฉพาะในกรณีที่เกี่ยวข้องกับอาชญากรรมที่มีการใช้เทคโนโลยีในการกระทำความผิด เช่น การใช้เครื่องคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ในการหลอกลวงหรือปลอมแปลงข้อมูล ซึ่งการรักษาความน่าเชื่อถือของพยานหลักฐานเหล่านี้เป็นสิ่งที่ต้องได้รับการควบคุมและปฏิบัติตามอย่างเคร่งครัด

กฎในการรักษาความน่าเชื่อถือของพยานหลักฐานอิเล็กทรอนิกส์

ในการรักษาความน่าเชื่อถือของพยานหลักฐานอิเล็กทรอนิกส์ในกระบวนการทางกฎหมาย มีความสำคัญอย่างยิ่งที่จะต้องมีการจัดการอย่างรัดกุมและตรงตามหลักเกณฑ์ที่กำหนดเพื่อให้สามารถนำเสนอหลักฐานเหล่านั้นได้อย่างมีประสิทธิภาพและมีความเชื่อถือได้ในชั้นศาล ดังนั้น กฎเกณฑ์ที่เกี่ยวข้องกับการรักษาความน่าเชื่อถือของพยานหลักฐานอิเล็กทรอนิกส์จึงมีบทบาทสำคัญในการประกันว่าข้อมูลที่ถูกนำมาใช้ในกระบวนการพิจารณาคดีมีความถูกต้องและไม่ถูกดัดแปลง

กฎข้อที่ 1: ต้องไม่กระทำให้เกิดการเปลี่ยนแปลงใด ๆ ในพยานหลักฐาน

ข้อกำหนดแรกนี้สะท้อนถึงความสำคัญของการปกป้องพยานหลักฐานจากการถูกดัดแปลงหรือแก้ไข เพราะการเปลี่ยนแปลงข้อมูลในพยานหลักฐานอาจทำให้ข้อมูลนั้นสูญเสียความน่าเชื่อถือและไม่สามารถนำมาใช้เป็นหลักฐานในกระบวนการทางกฎหมายได้ การปฏิบัติตามหลักการนี้จะช่วยรักษาความบริสุทธิ์ของข้อมูลและเพิ่มความเชื่อมั่นในความถูกต้องของการใช้พยานหลักฐานในคดี

กฎข้อที่ 2: กรณีที่มีความจำเป็นไม่สามารถหลีกเลี่ยงการเปลี่ยนแปลงของพยานหลักฐาน จะต้องสามารถอธิบายได้และพยายามให้เกิดการเปลี่ยนแปลงน้อยที่สุดเท่าที่จะเป็นไปได้

ในบางกรณีที่การเปลี่ยนแปลงพยานหลักฐานเป็นสิ่งจำเป็น เช่น การแปลงรูปแบบของข้อมูลเพื่อความสะดวกในการตรวจสอบ เราจำเป็นต้องมีการอธิบายถึงเหตุผลและกระบวนการเปลี่ยนแปลงอย่างชัดเจน นอกจากนี้ยังควรพยายามทำให้การเปลี่ยนแปลงนั้นมีผลกระทบน้อยที่สุดเพื่อรักษาความถูกต้องและความสมบูรณ์ของพยานหลักฐาน

กฎข้อที่ 3: บันทึกรายละเอียดทุกขั้นตอนที่กระทำกับพยานหลักฐานอิเล็กทรอนิกส์และหากใช้เครื่องมืออื่นที่ได้รับมาตรฐานเดียวกันจะต้องได้รับผลลัพธ์แบบเดียวกัน

การบันทึกรายละเอียดทุกขั้นตอนที่กระทำกับพยานหลักฐานเป็นสิ่งสำคัญ เนื่องจากจะช่วยให้สามารถตรวจสอบได้ในกรณีที่เกิดข้อสงสัยเกี่ยวกับกระบวนการการจัดการพยานหลักฐาน โดยการบันทึกข้อมูลเหล่านี้จะช่วยให้สามารถติดตามกระบวนการได้อย่างโปร่งใส นอกจากนี้ หากใช้เครื่องมือหรือซอฟต์แวร์ที่ได้รับมาตรฐาน เราควรมั่นใจว่าเครื่องมือเหล่านั้นจะให้ผลลัพธ์ที่เที่ยงตรงและสอดคล้องกันในทุกครั้งที่ใช้

กฎข้อที่ 4: ผู้ที่เป็นเจ้าของคดีต้องทำให้แน่ใจว่าได้ปฏิบัติถูกต้องตามกฎหมายและกฎในการรักษาความน่าเชื่อถือของพยานหลักฐาน

การปฏิบัติตามกฎหมายอย่างถูกต้องเป็นสิ่งสำคัญในการรักษาความน่าเชื่อถือของพยานหลักฐาน เจ้าหน้าที่ที่เกี่ยวข้องในกระบวนการตรวจสอบและเก็บรวบรวมพยานหลักฐานต้องมั่นใจว่าได้ปฏิบัติตามขั้นตอนและมาตรฐานที่กำหนด โดยการทำเช่นนี้จะช่วยป้องกันข้อผิดพลาดที่อาจเกิดขึ้นจากการปฏิบัติที่ไม่ถูกต้อง และทำให้พยานหลักฐานที่ได้รับการตรวจสอบมีความน่าเชื่อถือและสามารถนำมาใช้ในการพิจารณาคดีได้

โดยรวมแล้ว การรักษาความน่าเชื่อถือของพยานหลักฐานอิเล็กทรอนิกส์เป็นสิ่งที่ไม่อาจมองข้ามได้ในกระบวนการยุติธรรม โดยเฉพาะในคดีที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์หรืออาชญากรรมที่ใช้เทคโนโลยีเป็นเครื่องมือ การรักษามาตรฐานเหล่านี้จะช่วยให้สามารถรักษาความถูกต้องและความยุติธรรมในการพิจารณาคดีได้อย่างมีประสิทธิภาพ

หลักการทั่วไปในการรักษาความน่าเชื่อถือของพยานหลักฐานอิเล็กทรอนิกส์

ในการรักษาความน่าเชื่อถือของพยานหลักฐานอิเล็กทรอนิกส์ มีหลักการสำคัญที่ต้องปฏิบัติตามเพื่อให้การใช้พยานหลักฐานในกระบวนการพิจารณาคดีเป็นไปอย่างมีประสิทธิภาพและถูกต้อง โดยหลักการเหล่านี้มุ่งเน้นไปที่การรักษาความสมบูรณ์ของข้อมูล และการป้องกันการดัดแปลงหรือการเปลี่ยนแปลงพยานหลักฐานในกระบวนการทางกฎหมาย

1. การยืนยันว่าเป็นพยานหลักฐานที่แท้จริง

การยืนยันว่าเป็นพยานหลักฐานที่แท้จริงหมายถึงการตรวจสอบให้มั่นใจว่าพยานหลักฐานนั้นมีความถูกต้องและมีที่มาจากเหตุการณ์ที่เกิดขึ้นจริง หากไม่สามารถยืนยันได้ว่าพยานหลักฐานนั้นมาจากเหตุการณ์จริงหรือไม่ ก็จะไม่สามารถรับฟังเป็นพยานหลักฐานในชั้นศาลได้ การตรวจสอบแหล่งที่มาของข้อมูล จึงเป็นสิ่งสำคัญที่ต้องดำเนินการให้ถูกต้องและชัดเจน

2. การรักษาห่วงโซ่ของพยานหลักฐาน

การรักษาห่วงโซ่ของพยานหลักฐานหมายถึงการติดตามและบันทึกการเคลื่อนย้ายหรือการเปลี่ยนแปลงการครอบครองของพยานหลักฐานทุกขั้นตอน โดยเฉพาะในกรณีที่พยานหลักฐานถูกส่งต่อจากบุคคลหนึ่งไปยังบุคคลอื่น ต้องมีการบันทึกลงในใบรายการและลงลายมือชื่อของผู้รับและผู้ส่ง การทำเช่นนี้ช่วยให้สามารถตรวจสอบได้ว่า พยานหลักฐานในแต่ละขั้นตอนอยู่ภายใต้การควบคุมของใคร และสามารถย้อนกลับไปตรวจสอบได้ในทุกขั้นตอน

3. การยืนยันในความถูกต้องของพยานหลักฐาน

การยืนยันความถูกต้องของพยานหลักฐานในกรณีของอุปกรณ์อิเล็กทรอนิกส์ไม่ใช่เพียงแค่การตรวจสอบจากภายนอกเท่านั้น แต่ต้องตรวจสอบว่าเนื้อหาภายในอุปกรณ์ยังคงสภาพเดิม ไม่ถูกเปลี่ยนแปลงหรือแก้ไข การตรวจสอบอุปกรณ์ต้องทำอย่างระมัดระวัง เพื่อหลีกเลี่ยงการเปลี่ยนแปลงข้อมูลโดยไม่ตั้งใจ เช่น การเปิดดูไฟล์หรือการนำไฟล์ออกจากอุปกรณ์โดยไม่มีมาตรการในการปกป้องข้อมูลนั้น ซึ่งอาจทำให้ข้อมูลสูญเสียความน่าเชื่อถือได้

หลักการเหล่านี้มีความสำคัญในการรักษาความน่าเชื่อถือของพยานหลักฐานอิเล็กทรอนิกส์ และช่วยให้กระบวนการทางกฎหมายสามารถใช้ข้อมูลจากอุปกรณ์อิเล็กทรอนิกส์ในการพิจารณาคดีได้อย่างถูกต้องและเชื่อถือได้

2.3 แนวคิดเกี่ยวกับพยานหลักฐานดิจิทัลแยกออกจากพยานหลักฐานทั่วไป

พยานหลักฐานอิเล็กทรอนิกส์ในปัจจุบันมีบทบาทสำคัญในกระบวนการทางกฎหมาย โดยไม่ว่าจะเป็นในคดีอาชญากรรมทางคอมพิวเตอร์หรืออาชญากรรมทั่วไป พยานหลักฐานอิเล็กทรอนิกส์มักเกี่ยวข้องในทุกกรณี แม้แต่การกระทำผิดที่เกิดขึ้นก็อาจจะมีการสร้างหรือเก็บพยานหลักฐาน

อิเล็กทรอนิกส์โดยไม่รู้ตัว ดังนั้น การรักษาความน่าเชื่อถือของพยานหลักฐานอิเล็กทรอนิกส์จึงเป็นสิ่งสำคัญเพื่อให้สามารถนำไปใช้ในกระบวนการพิจารณาคดีได้อย่างถูกต้องและเป็นธรรม

การจัดการพยานหลักฐานอิเล็กทรอนิกส์นั้นยังคงเป็นเรื่องใหม่ในประเทศไทย ซึ่งแตกต่างจากการจัดการพยานหลักฐานแบบเดิมที่มีอยู่แล้ว ในปัจจุบันกฎหมายบางฉบับได้ให้เจ้าหน้าที่สามารถเข้าถึงพยานหลักฐานเหล่านี้ได้ แต่ยังคงมีปัญหาที่ประเทศไทยยังขาดมาตรฐานที่ชัดเจนในการจัดการและรักษาความบริสุทธิ์ของพยานหลักฐานอิเล็กทรอนิกส์ เมื่อพิจารณาถึงการกระทำผิดที่เกี่ยวข้องกับพยานหลักฐานอิเล็กทรอนิกส์, ผู้กระทำผิดอาจสามารถทำการดัดแปลงหรือเปลี่ยนแปลงข้อมูลในพยานหลักฐานเหล่านี้ได้ง่าย ซึ่งสร้างความยากลำบากในการหาความเชื่อมโยงระหว่างผู้กระทำผิดกับอุปกรณ์ที่ใช้กระทำความผิด

ในบางประเทศพยานหลักฐานอิเล็กทรอนิกส์จะถูกจัดอยู่ในกลุ่มของพยานเอกสาร ซึ่งหมายถึง ข้อความที่สามารถอ้างอิงเป็นพยานในศาลได้ โดยอาศัยการสื่อความหมายของข้อความในเอกสารนั้น การนำพยานเอกสารมาใช้ในการพิจารณาคดีจะต้องใช้ต้นฉบับและไม่สามารถใช้สำเนาแทนได้ ในขณะที่พยานวัตถุสามารถนำมาใช้ได้โดยไม่ต้องใช้ต้นฉบับเสมอไป ซึ่งแตกต่างจากพยานเอกสาร

กรณีของพยานหลักฐานอิเล็กทรอนิกส์ที่อยู่ในรูปของข้อมูลทางอิเล็กทรอนิกส์หรือข้อมูลในระบบคอมพิวเตอร์นั้นมีความท้าทายในการนำเสนอเป็นพยานในศาล เนื่องจากข้อมูลเหล่านี้ไม่ได้มีรูปร่างที่สามารถมองเห็นได้ด้วยตาเปล่า และการพิมพ์ออกมาเป็นกระดาษหรือข้อความก็ไม่สามารถพิสูจน์ได้ว่าข้อมูลนั้นถูกต้องหรือไม่จนกว่าจะมีการตรวจสอบจากอุปกรณ์ที่ใช้บันทึกข้อมูลนั้นๆ

อีกทั้งข้อมูลในระบบคอมพิวเตอร์ยังสามารถถูกดัดแปลงได้ง่าย ทำให้เกิดปัญหาว่าข้อมูลที่ถูกนำมาเป็นพยานนั้นอาจมีการเปลี่ยนแปลงไปโดยไม่ตั้งใจ หรือผู้ที่เกี่ยวข้องอาจทำการแก้ไขข้อมูลเพื่อให้เกิดความผิดปกติในกระบวนการตรวจสอบข้อมูล ซึ่งทำให้การใช้พยานหลักฐานเหล่านี้ในศาลต้องมีการตรวจสอบความถูกต้องอย่างเข้มงวด เพื่อให้มั่นใจว่าข้อมูลที่นำเสนอนั้นมีความน่าเชื่อถือและไม่ถูกเปลี่ยนแปลง

ทั้งนี้ พยานหลักฐานอิเล็กทรอนิกส์ในกระบวนการพิจารณาคดีจึงมีความท้าทายที่แตกต่างจากพยานหลักฐานประเภทอื่น ๆ ซึ่งจำเป็นต้องมีการพัฒนาและปรับปรุงกฎหมาย รวมถึงมาตรการใน

การจัดการและรักษาความปลอดภัยของพยานหลักฐานอิเล็กทรอนิกส์ เพื่อให้การพิจารณาคดีมีความเป็นธรรมและมีความถูกต้องมากยิ่งขึ้น

ขั้นตอนในการตรวจสอบพยานหลักฐานทางดิจิทัล

ในบทนี้กล่าวถึงกระบวนการตรวจพิสูจน์พยานหลักฐานทางดิจิทัล ซึ่งมีความสำคัญในการใช้พยานหลักฐานที่ได้จากระบบหรืออุปกรณ์ดิจิทัลมาใช้ในกระบวนการทางกฎหมาย กระบวนการนี้ไม่สามารถใช้วิธีเดียวกันกับพยานหลักฐานทางกายภาพทั่วไปได้ เนื่องจากการพิสูจน์ความผิดในคดีที่เกี่ยวข้องกับเทคโนโลยีดิจิทัลมีความซับซ้อนและต้องการความเชี่ยวชาญเฉพาะด้าน โดยในประเทศสหรัฐอเมริกา Federal Bureau of Investigation (FBI) ได้กำหนดขั้นตอนการตรวจพิสูจน์พยานหลักฐานทางดิจิทัลเป็น 7 ขั้นตอน ซึ่งประกอบไปด้วยการระบุพยานหลักฐาน การเก็บรักษาพยานหลักฐาน และการตัดสินใจเกี่ยวกับพยานหลักฐาน

ในขณะที่ National Institute of Standards and Technology (NIST) ได้นำเสนอขั้นตอนการตรวจพิสูจน์ที่แบ่งออกเป็น 4 ขั้นตอน ซึ่งได้แก่:

ขั้นตอนการรวบรวม: การระบุพยานหลักฐาน การติดฉลาก และการจัดทำรายงาน รวมถึงการดึงข้อมูลจากแหล่งข้อมูลทั้งหมด

ขั้นตอนการตรวจสอบ: การประมวลผลพยานหลักฐานทั้งหมดที่ได้มาโดยวิธีการทางเทคนิคเพื่อประเมินและเลือกพยานหลักฐานที่มีความน่าสนใจ

ขั้นตอนการวิเคราะห์: การวิเคราะห์พยานหลักฐานที่ได้คัดเลือกมาแล้วด้วยเครื่องมือและวิธีการทางเทคนิคที่มีความน่าเชื่อถือทางกฎหมาย

ขั้นตอนการรายงาน: การจัดทำรายงานผลการวิเคราะห์ ซึ่งต้องอธิบายถึงการดำเนินการในแต่ละขั้นตอนอย่างชัดเจน

สรุปได้ว่า แม้ว่าขั้นตอนเหล่านี้อาจแตกต่างกันไปในรายละเอียดตามองค์กร แต่ทุกขั้นตอนมีความสำคัญในการได้มาซึ่งพยานหลักฐานที่สามารถใช้ในการพิสูจน์ความผิดได้ โดยเฉพาะในกระบวนการที่ต้องใช้การตรวจสอบพยานหลักฐานทางดิจิทัลเพื่อหาพยานหลักฐานที่มีความสำคัญในการพิสูจน์ความผิด

2.4 แนวคิดเกี่ยวกับปัญหาการรับมือกับพยานหลักฐานอิเล็กทรอนิกส์

พยานหลักฐานอิเล็กทรอนิกส์มีลักษณะที่แตกต่างจากพยานหลักฐานในรูปแบบดั้งเดิม เนื่องจากข้อมูลมักถูกจัดเก็บแบบกระจายตามแหล่งต่าง ๆ ทั้งในประเทศและต่างประเทศ ซึ่งเป็นผลมาจากธรรมชาติของระบบดิจิทัลและเครือข่ายอินเทอร์เน็ต ตัวอย่างเช่น ในหลายกรณี พยานหลักฐานอาจถูกจัดเก็บอยู่ในเซิร์ฟเวอร์ของผู้ให้บริการที่ตั้งอยู่ต่างประเทศ ทำให้การเข้าถึงข้อมูลดังกล่าวต้องเผชิญกับข้อจำกัดด้านกฎหมายระหว่างประเทศ รวมถึงข้อจำกัดด้านเทคนิคและเวลา

อีกหนึ่งอุปสรรคสำคัญคือการเข้ารหัสข้อมูล (encryption) ซึ่งถูกออกแบบมาเพื่อรักษาความปลอดภัยของข้อมูล แต่ในขณะเดียวกันก็เป็นอุปสรรคในการเข้าถึงข้อมูลโดยเจ้าหน้าที่ผู้มีหน้าที่ตรวจสอบ โดยเฉพาะเมื่อไม่มีเครื่องมือหรือกุญแจถอดรหัสที่จำเป็น การเข้ารหัสจึงกลายเป็นสิ่งที่ขัดขวางกระบวนการพิสูจน์ความผิดอย่างมีนัยสำคัญ

แม้ว่าเจ้าหน้าที่จะสามารถเข้าถึงข้อมูลได้แล้วก็ตาม ปัญหาต่อมาที่มักพบคือการขาดความเชี่ยวชาญเฉพาะทางในการวิเคราะห์และเชื่อมโยงข้อมูลเข้ากับตัวผู้กระทำความผิด อาทิ การแปลผลข้อมูลเมตา (metadata) หรือการวิเคราะห์หัวอีเมล (email header) ซึ่งเป็นข้อมูลสำคัญในการพิสูจน์แหล่งที่มาของการกระทำผิด หากเจ้าหน้าที่ไม่มีความรู้เพียงพอ ก็อาจเกิดการจัดเก็บหรือใช้พยานหลักฐานอย่างไม่ถูกต้อง ส่งผลให้พยานหลักฐานขาดน้ำหนักหรือไม่สามารถใช้ได้ในกระบวนการพิจารณาคดี

นอกจากนี้ ยังพบว่ามีการปล่อยให้ผู้เสียหายเป็นผู้รวบรวมพยานหลักฐานด้วยตนเอง ซึ่งอาจนำไปสู่ปัญหาด้านความถูกต้องและความน่าเชื่อถือของข้อมูล เนื่องจากระดับความรู้และความเข้าใจของผู้เสียหายแต่ละรายย่อมแตกต่างกัน ส่งผลให้พยานหลักฐานที่ได้มีลักษณะไม่เป็นมาตรฐาน บางครั้งไม่สามารถตรวจสอบย้อนกลับได้ หรืออาจเกิดข้อสงสัยในความบริสุทธิ์ของข้อมูลดังกล่าว

จากปัญหาทั้งหมดนี้สะท้อนให้เห็นว่า การจัดการกับพยานหลักฐานอิเล็กทรอนิกส์จำเป็นต้องมีการวางระบบที่รัดกุม มีเจ้าหน้าที่ที่มีความรู้ความเชี่ยวชาญเฉพาะด้าน รวมถึงต้องมีการพัฒนากฎหมายและแนวปฏิบัติที่สอดคล้องกับเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว เพื่อให้

พยานหลักฐานอิเล็กทรอนิกส์สามารถนำมาใช้ได้อย่างมีประสิทธิภาพและเชื่อถือได้ในกระบวนการยุติธรรม

ปัญหาการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ในคดีอาญา

ในปัจจุบัน การรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ยังคงเป็นความท้าทายสำคัญในกระบวนการสอบสวนคดีอาญา โดยเฉพาะเมื่อพิจารณาจากลักษณะเฉพาะของพยานหลักฐานประเภทนี้ ซึ่งอยู่ในรูปแบบของข้อมูลหรือสารสนเทศที่สามารถถูกแก้ไข ลบ เปลี่ยนแปลง หรือทำลายได้อย่างรวดเร็ว ทั้งนี้ ปัญหาที่พบสามารถแบ่งออกได้เป็น 3 ประการหลัก ได้แก่

1.ปัญหาเกี่ยวกับขอบเขตอำนาจของพนักงานสอบสวน

ประมวลกฎหมายวิธีพิจารณาความอาญาให้อำนาจพนักงานสอบสวนในการใช้ดุลพินิจรวบรวมพยานหลักฐานทุกชนิดที่สามารถกระทำได้เพื่อพิสูจน์ข้อเท็จจริงและตัวผู้กระทำความผิด อย่างไรก็ตาม ลักษณะเฉพาะของพยานหลักฐานอิเล็กทรอนิกส์ที่อ่อนไหวและเสี่ยงต่อการถูกเปลี่ยนแปลงหรือลบทิ้ง ทำให้การใช้ดุลพินิจของพนักงานสอบสวนเพียงลำพังอาจไม่เพียงพอ อีกทั้งยังมีความกังวลเรื่องการละเมิดสิทธิส่วนบุคคลหากไม่มีบทบัญญัติที่ชัดเจนรองรับการใช้อำนาจดังกล่าว ดังนั้นการให้อำนาจในการรวบรวมพยานหลักฐานจึงควรอยู่ภายใต้กรอบกฎหมายที่ชัดเจนและตรวจสอบได้

2.ปัญหาเกี่ยวกับแนวทางและขั้นตอนในการเก็บรวบรวมพยานหลักฐาน

กระบวนการสอบสวนโดยพนักงานสอบสวนมีความสำคัญอย่างยิ่งในฐานะเป็นกลไกแรกของกระบวนการยุติธรรม การดำเนินการต่าง ๆ จำเป็นต้องยึดหลักความเป็นธรรม ความโปร่งใส และการเคารพสิทธิของประชาชน อย่างไรก็ดี ปัจจุบันยังไม่มีกฎหมายที่กำหนดแนวทางหรือขั้นตอนเฉพาะสำหรับการเก็บรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ ส่งผลให้การปฏิบัติงานอาศัยดุลยพินิจของเจ้าหน้าที่เป็นหลัก ซึ่งเสี่ยงต่อการขาดมาตรฐานและอาจกระทบต่อความสมบูรณ์ของพยานหลักฐานที่ต้องใช้ในการพิจารณาคดี หากมีการกำหนดแนวทางปฏิบัติที่ชัดเจนและเป็นมาตรฐาน จะสามารถช่วยให้การบังคับใช้กฎหมายเป็นไปอย่างมีประสิทธิภาพมากขึ้น

3.ปัญหาเกี่ยวกับข้อจำกัดในการขอหมายค้น

พยานหลักฐานอิเล็กทรอนิกส์สามารถถูกเปลี่ยนแปลงหรือลบทิ้งได้ในระยะเวลาอันสั้น แต่กระบวนการออกหมายค้นตามประมวลกฎหมายวิธีพิจารณาความอาญา โดยเฉพาะมาตรา 69 และ 96 ต้องอาศัยเวลาและขั้นตอนที่ซับซ้อน ทั้งยังมีข้อจำกัดในการระบุรายละเอียดของข้อมูลหรือสถานที่ค้นอย่างชัดเจน เนื่องจากข้อมูลอิเล็กทรอนิกส์ไม่มีรูปร่างหรือสภาพที่แน่นอน ส่งผลให้พนักงานสอบสวนไม่สามารถเข้าถึงพยานหลักฐานได้อย่างทันท่วงที อีกทั้งการกระจายตัวของหน่วยงานที่มีอำนาจในการออกหมายค้นยังทำให้เสียเวลาเพิ่มขึ้น จนอาจทำให้พยานหลักฐานถูกทำลายก่อนเจ้าหน้าที่จะสามารถเข้าตรวจค้นได้

แม้ว่าประเทศไทยจะมีพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และมีการแก้ไขเพิ่มเติมในปี พ.ศ. 2560 เพื่อให้สอดคล้องกับการเปลี่ยนแปลงของสังคมและเทคโนโลยี รวมถึงเพื่อเพิ่มประสิทธิภาพในการใช้มาตรการทางกฎหมายในการสืบสวนสอบสวนและคุ้มครองสิทธิเสรีภาพของประชาชน แต่ก็ยังคงมีความจำเป็นต้องปรับปรุงกลไกการปฏิบัติให้มีความชัดเจน สอดคล้อง และทันต่อสถานการณ์ โดยเฉพาะในส่วนที่เกี่ยวข้องกับการเก็บรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ในทางปฏิบัติ

ปัญหาเกี่ยวกับการให้อำนาจในการรวบรวมพยานหลักฐาน

มาตรการรวบรวมพยานหลักฐานที่อาจกระทบต่อสิทธิความเป็นส่วนตัวของประชาชน

หนึ่งในมาตรการสำคัญที่ใช้ในการรวบรวมพยานหลักฐานในคดีอาชญากรรมทางคอมพิวเตอร์ คือ การเรียกข้อมูลจากผู้ที่เกี่ยวข้องกับการกระทำความผิดหรือจากผู้ให้บริการระบบคอมพิวเตอร์ ซึ่งข้อมูลดังกล่าวประกอบด้วยข้อมูลที่ถูกจัดเก็บไว้ล่วงหน้า และข้อมูลที่ถูกดึงแบบเรียลไทม์ (Real-time data) โดยนิยามของ “ผู้ให้บริการ” ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ มีความครอบคลุมอย่างกว้างขวาง

ทั้งนี้ เมื่อพิจารณาประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564 พบว่า ผู้ให้บริการมิได้หมายถึงเฉพาะผู้ประกอบธุรกิจอินเทอร์เน็ตโดยตรงเท่านั้น แต่ยังรวมถึงผู้ประกอบกิจการอื่น ๆ ที่ใช้ระบบอินเทอร์เน็ตในการดำเนินงาน เช่น ผู้ให้บริการโทรคมนาคม ร้านอินเทอร์เน็ต ร้านเกมออนไลน์ แอปพลิเคชัน เช่น Telegram, Facebook, Line รวมถึงผู้ให้บริการคลังข้อมูลออนไลน์ (Cloud

Service), เว็บบอร์ด, เว็บเซิร์ฟเวอร์ ตลอดจนธุรกิจในด้านไลฟ์สไตล์ การศึกษา และอสังหาริมทรัพย์ เป็นต้น

กฎหมายกำหนดให้ผู้ให้บริการเหล่านี้ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ซึ่งเป็นข้อมูลทางเทคนิคที่แสดงถึงพฤติกรรมการใช้งาน โดยต้องเก็บรักษาอย่างน้อย 90 วัน นับแต่วันที่ข้อมูลเข้าสู่ระบบ และสามารถขยายระยะเวลาการเก็บได้สูงสุดถึง 2 ปี หากเจ้าพนักงานมีคำสั่งตามสมควร แม้จะมีเป้าหมายเพื่อให้เจ้าพนักงานสามารถรวบรวมข้อมูลเพื่อใช้เป็นพยานหลักฐานในการดำเนินคดี แต่ก็ส่งผลกระทบต่อสิทธิความเป็นส่วนตัวของผู้ใช้บริการ และยังเพิ่มภาระค่าใช้จ่ายแก่ผู้ให้บริการโดยเฉพาะรายย่อยที่ต้องลงทุนในอุปกรณ์จัดเก็บข้อมูล

ข้อมูลที่ผู้ให้บริการต้องเก็บและสามารถถูกเรียกตรวจสอบได้ ได้แก่ ข้อมูลที่สามารถระบุตัวตนของผู้ใช้บริการ และข้อมูลใด ๆ ที่อยู่ในครอบครองหรือควบคุมของผู้ให้บริการ ซึ่งตามกฎหมายไม่จำเป็นต้องได้รับอนุญาตจากศาล แม้ว่าข้อมูลเหล่านั้นจะจัดเป็นข้อมูลส่วนบุคคลที่เกี่ยวข้องกับสิทธิความเป็นส่วนตัวของผู้ใช้งาน โดยเฉพาะข้อมูลจราจรทางคอมพิวเตอร์ที่สามารถสะท้อนพฤติกรรมการใช้งาน เช่น การเข้าเว็บไซต์ หรือการใช้บัญชี Facebook ซึ่งอาจมีผลกระทบต่อภาพลักษณ์ของบุคคลในโลกแห่งความจริง

การที่กฎหมายให้อำนาจในการเรียกดูข้อมูลจากผู้ให้บริการเพื่อใช้เป็นพยานหลักฐานโดยไม่จำกัดเฉพาะผู้ต้องสงสัย แต่ครอบคลุมถึงบุคคลอื่นที่อาจไม่เกี่ยวข้องกับการกระทำความผิด อาจนำไปสู่การละเมิดสิทธิความเป็นส่วนตัวของประชาชนทั่วไปด้วย

มาตรการรวบรวมพยานหลักฐานที่กระทบต่อสิทธิในการสื่อสารของประชาชน

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ มิได้ให้อำนาจแก่เจ้าพนักงานในการดักจับข้อมูลการสื่อสารแบบเรียลไทม์ อย่างไรก็ตาม หากพิจารณาตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 25 พบว่า เจ้าพนักงานสามารถดักข้อมูลจากระบบคอมพิวเตอร์ อุปกรณ์สื่อสาร หรือสื่ออิเล็กทรอนิกส์ได้ เพื่อให้ได้ข้อมูล ณ เวลาปัจจุบัน หากเป็นความผิดตามมาตรา 5-12, 14 และ 17 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ ซึ่งเกี่ยวข้องกับโครงสร้างพื้นฐานของประเทศ หรือความมั่นคง เช่น ระบบการเงิน เทคโนโลยีสารสนเทศ โทรคมนาคม พลังงาน และบริการสาธารณะ

มาตรการดังกล่าวสามารถดำเนินการได้คราวละไม่เกิน 90 วัน โดยอาจกำหนดเงื่อนไขเพิ่มเติม และเมื่อดำเนินการแล้วเสร็จ ต้องรายงานผลต่ออธิบดีผู้พิพากษาศาลอาญา อย่างไรก็ตาม การให้อำนาจในการดักจับข้อมูลการสื่อสารเช่นนี้ มีลักษณะเปิดกว้างและไม่มีการจำกัดขอบเขตอย่างชัดเจน ซึ่งอาจครอบคลุมถึงเนื้อหาสื่อสารส่วนตัวของบุคคลทั่วไป เป็นการละเมิดสิทธิความเป็นส่วนตัวอย่างร้ายแรง แม้จะเป็นมาตรการที่ใช้เฉพาะกับคดีที่มีผลกระทบร้ายแรงต่อสาธารณะ แต่รัฐต้องมีความระมัดระวังในการใช้มาตรการดังกล่าว

ปัญหาทางกฎหมายในการรับฟังพยานหลักฐานทางอิเล็กทรอนิกส์

(สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2559)ชี้ว่า ประเทศไทยยังไม่มีบทบัญญัติว่าด้วยพยานหลักฐานที่ตราขึ้นเฉพาะเพื่อรองรับพยานหลักฐานทางอิเล็กทรอนิกส์โดยเฉพาะ การนำพยานดังกล่าวมาใช้ในชั้นศาลขึ้นอยู่กับการตีความว่าเข้าข่ายพยานบุคคล พยานเอกสาร หรือพยานวัตถุ เช่น การให้เจ้าหน้าที่พิสูจน์หลักฐานเบิกความ การอ้างผลรายงานตรวจสอบ หรือการนำอุปกรณ์คอมพิวเตอร์เข้าสืบ

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ มาตรา 25 ได้บัญญัติให้ข้อมูลคอมพิวเตอร์และข้อมูลจราจรทางคอมพิวเตอร์ที่ได้มาโดยชอบด้วยกฎหมาย สามารถอ้างและรับฟังเป็นพยานหลักฐานได้ หากมิได้เกิดจากการปลอมแปลง หลอกลวง หรือการกระทำโดยมิชอบ นอกจากนี้ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาตรา 11 ก็ให้แนวทางเช่นเดียวกัน โดยกำหนดว่า ความน่าเชื่อถือของพยานหลักฐานอิเล็กทรอนิกส์จะพิจารณาจากลักษณะและวิธีการสร้าง จัดเก็บ หรือสื่อสารข้อมูล วิธีการระบุผู้ส่งข้อมูล และสภาพแวดล้อมที่เกี่ยวข้องทั้งหมด

อย่างไรก็ตาม ในทางปฏิบัติ การพิสูจน์ความน่าเชื่อถือของพยานอิเล็กทรอนิกส์ยังไม่มีหลักเกณฑ์ที่ชัดเจน ซึ่งเป็นปัญหาในกระบวนการยุติธรรม โดยเฉพาะในคดีอาญาซึ่งมีภาระการพิสูจน์สูงสุด ศาลต้องเชื่อโดยปราศจากข้อสงสัยว่าจำเลยกระทำความผิดจริง การขาดมาตรฐานกลางในกระบวนการจัดเก็บ ตรวจสอบ และประเมินพยานหลักฐานทางอิเล็กทรอนิกส์ อาจทำให้ศาลไม่รับฟังพยานหลักฐานหรือไม่เชื่อถือ ส่งผลให้ไม่สามารถลงโทษผู้กระทำผิดได้

ดังนั้น การจัดทำหลักเกณฑ์ทางกฎหมายที่ชัดเจนเพื่อใช้เป็นแนวทางในการรวบรวมและประเมินพยานหลักฐานอิเล็กทรอนิกส์ จึงมีความจำเป็นอย่างยิ่งในยุคที่อาชญากรรมไซเบอร์มีบทบาทสำคัญในสังคมปัจจุบัน

ปัญหาเกี่ยวกับการให้อำนาจในการรวบรวมพยานหลักฐาน

มาตรการรวบรวมพยานหลักฐานที่อาจกระทบต่อสิทธิความเป็นส่วนตัวของประชาชน

หนึ่งในมาตรการสำคัญที่ใช้ในการรวบรวมพยานหลักฐานในคดีอาชญากรรมทางคอมพิวเตอร์ คือ การเรียกข้อมูลจากผู้ที่เกี่ยวข้องกับการกระทำความผิดหรือจากผู้ให้บริการระบบคอมพิวเตอร์ ซึ่งข้อมูลดังกล่าวประกอบด้วยข้อมูลที่ถูกจัดเก็บไว้ล่วงหน้า และข้อมูลที่ถูกดึงแบบเรียลไทม์ (Real-time data) โดยนิยามของ “ผู้ให้บริการ” ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ มีความครอบคลุมอย่างกว้างขวาง

ทั้งนี้ เมื่อพิจารณาประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564 พบว่า ผู้ให้บริการมิได้หมายถึงเฉพาะผู้ประกอบธุรกิจอินเทอร์เน็ตโดยตรงเท่านั้น แต่ยังรวมถึงผู้ประกอบกิจการอื่น ๆ ที่ใช้ระบบอินเทอร์เน็ตในการดำเนินงาน เช่น ผู้ให้บริการโทรคมนาคม ร้านอินเทอร์เน็ต ร้านเกมออนไลน์ แอปพลิเคชัน เช่น Telegram, Facebook, Line รวมถึงผู้ให้บริการคลังข้อมูลออนไลน์ (Cloud Service), เว็บบอร์ด, เว็บเซิร์ฟเวอร์ ตลอดจนธุรกิจในด้านไลฟ์สไตล์ การศึกษา และอสังหาริมทรัพย์ เป็นต้น

กฎหมายกำหนดให้ผู้ให้บริการเหล่านี้ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ซึ่งเป็นข้อมูลทางเทคนิคที่แสดงถึงพฤติกรรมการใช้งาน โดยต้องเก็บรักษาอย่างน้อย 90 วัน นับแต่วันที่ข้อมูลเข้าสู่ระบบ และสามารถขยายระยะเวลาการเก็บได้สูงสุดถึง 2 ปี หากเจ้าพนักงานมีคำสั่งตามสมควร แม้จะมีเป้าหมายเพื่อให้เจ้าพนักงานสามารถรวบรวมข้อมูลเพื่อใช้เป็นพยานหลักฐานในการดำเนินคดี แต่ก็ส่งผลกระทบต่อสิทธิความเป็นส่วนตัวของผู้ใช้บริการ และยังเพิ่มภาระค่าใช้จ่ายแก่ผู้ให้บริการโดยเฉพาะรายย่อยที่ต้องลงทุนในอุปกรณ์จัดเก็บข้อมูล

ข้อมูลที่ผู้ให้บริการต้องเก็บและสามารถถูกเรียกตรวจสอบได้ ได้แก่ ข้อมูลที่สามารถระบุตัวตนของผู้ใช้บริการ และข้อมูลใด ๆ ที่อยู่ในครอบครองหรือควบคุมของผู้ให้บริการ ซึ่งตามกฎหมายไม่จำเป็นต้องได้รับอนุญาตจากศาล แม้ว่าข้อมูลเหล่านั้นจะจัดเป็นข้อมูลส่วนบุคคลที่

เกี่ยวข้องกับสิทธิความเป็นส่วนตัวของผู้ใช้งาน โดยเฉพาะข้อมูลจราจรทางคอมพิวเตอร์ที่สามารถสะท้อนพฤติกรรมการใช้งาน เช่น การเข้าเว็บไซต์ หรือการใช้บัญชี Facebook ซึ่งอาจมีผลกระทบต่อภาพลักษณ์ของบุคคลในโลกแห่งความจริง

การที่กฎหมายให้อำนาจในการเรียกดูข้อมูลจากผู้ให้บริการเพื่อใช้เป็นพยานหลักฐานโดยไม่จำกัดเฉพาะผู้ต้องสงสัย แต่ครอบคลุมถึงบุคคลอื่นที่อาจไม่เกี่ยวข้องกับการกระทำความผิด อาจนำไปสู่การละเมิดสิทธิความเป็นส่วนตัวของประชาชนทั่วไปด้วย

มาตรการรวบรวมพยานหลักฐานที่กระทบต่อสิทธิในการสื่อสารของประชาชน

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ มิได้ให้อำนาจแก่เจ้าพนักงานในการดักจับข้อมูลการสื่อสารแบบเรียลไทม์ อย่างไรก็ตาม หากพิจารณาตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 25 พบว่า เจ้าพนักงานสามารถดักข้อมูลจากระบบคอมพิวเตอร์ อุปกรณ์สื่อสาร หรือสื่ออิเล็กทรอนิกส์ได้ เพื่อให้ได้ข้อมูล ณ เวลาปัจจุบัน หากเป็นความผิดตามมาตรา 5-12, 14 และ 17 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ ซึ่งเกี่ยวข้องกับโครงสร้างพื้นฐานของประเทศ หรือความมั่นคง เช่น ระบบการเงิน เทคโนโลยีสารสนเทศ โทรคมนาคม พลังงาน และบริการสาธารณะ

มาตรการดังกล่าวสามารถดำเนินการได้คราวละไม่เกิน 90 วัน โดยอาจกำหนดเงื่อนไขเพิ่มเติม และเมื่อดำเนินการแล้วเสร็จ ต้องรายงานผลต่อออธิบดีผู้พิพากษาศาลอาญา อย่างไรก็ตาม การให้อำนาจในการดักจับข้อมูลการสื่อสารเช่นนี้ มีลักษณะเปิดกว้างและไม่มีการจำกัดขอบเขตอย่างชัดเจน ซึ่งอาจครอบคลุมถึงเนื้อหาสื่อสารส่วนตัวของบุคคลทั่วไป เป็นการละเมิดสิทธิความเป็นส่วนตัวอย่างร้ายแรง แม้จะเป็นมาตรการที่ใช้เฉพาะกับคดีที่มีผลกระทบร้ายแรงต่อสาธารณะ แต่รัฐต้องมีความระมัดระวังในการใช้มาตรการดังกล่าว

ปัญหาทางกฎหมายในการรับฟังพยานหลักฐานทางอิเล็กทรอนิกส์

(สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2559)ชี้ว่า ประเทศไทยยังไม่มีบทบัญญัติว่าด้วยพยานหลักฐานที่ตราขึ้นเฉพาะเพื่อรองรับพยานหลักฐานทางอิเล็กทรอนิกส์โดยเฉพาะ การนำพยานดังกล่าวมาใช้ในชั้นศาลขึ้นอยู่กับการตีความว่าเข้าข่ายพยานบุคคล พยานเอกสาร หรือพยานวัตถุ เช่น การให้เจ้าหน้าที่พิสูจน์หลักฐานเบิกความ การอ้างผลรายงานตรวจสอบ หรือการนำอุปกรณ์คอมพิวเตอร์เข้าสืบ

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ มาตรา 25 ได้บัญญัติให้ข้อมูลคอมพิวเตอร์และข้อมูลจราจรทางคอมพิวเตอร์ที่ได้มาโดยชอบด้วยกฎหมาย สามารถอ้างและรับฟังเป็นพยานหลักฐานได้ หากมิได้เกิดจากการปลอมแปลง หลอกลวง หรือการกระทำโดยมิชอบ นอกจากนี้ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาตรา 11 ก็ให้แนวทางเช่นเดียวกัน โดยกำหนดว่า ความน่าเชื่อถือของพยานหลักฐานอิเล็กทรอนิกส์จะพิจารณาจากลักษณะและวิธีการสร้าง จัดเก็บ หรือสื่อสารข้อมูล วิธีการระบุผู้ส่งข้อมูล และสภาพแวดล้อมที่เกี่ยวข้องทั้งหมด

อย่างไรก็ตาม ในทางปฏิบัติ การพิสูจน์ความน่าเชื่อถือของพยานอิเล็กทรอนิกส์ยังไม่มีหลักเกณฑ์ที่ชัดเจน ซึ่งเป็นปัญหาในกระบวนการยุติธรรม โดยเฉพาะในคดีอาญาซึ่งมีภาระการพิสูจน์สูงสุด ศาลต้องเชื่อโดยปราศจากข้อสงสัยว่าจำเลยกระทำความผิดจริง การขาดมาตรฐานกลางในกระบวนการจัดเก็บ ตรวจสอบ และประเมินพยานหลักฐานทางอิเล็กทรอนิกส์ อาจทำให้ศาลไม่รับฟังพยานหลักฐานหรือไม่เชื่อถือ ส่งผลให้ไม่สามารถลงโทษผู้กระทำผิดได้

ดังนั้น การจัดทำหลักเกณฑ์ทางกฎหมายที่ชัดเจนเพื่อใช้เป็นแนวทางในการรวบรวมและประเมินพยานหลักฐานอิเล็กทรอนิกส์ จึงมีความจำเป็นอย่างยิ่งในยุคที่อาชญากรรมไซเบอร์มีบทบาทสำคัญในสังคมปัจจุบัน

2.5 แนวคิดเกี่ยวกับเอกสารอิเล็กทรอนิกส์ และข้อมูลอิเล็กทรอนิกส์ที่เกี่ยวกับสื่อบันทึกภาพและเครื่องมืออิเล็กทรอนิกส์

ในยุคที่เทคโนโลยีสารสนเทศเข้ามามีบทบาทอย่างมากในชีวิตประจำวัน การดำเนินกิจกรรมหลายอย่างไม่ว่าจะเป็นธุรกรรม การสื่อสาร หรือการจัดเก็บข้อมูล ต่างก็มีการเปลี่ยนผ่านจากระบบเอกสารกระดาษไปสู่ระบบดิจิทัลอย่างหลีกเลี่ยงไม่ได้ ส่งผลให้การตีความและใช้ประโยชน์จาก "เอกสาร" และ "ข้อมูล" ต้องมีการขยายขอบเขตความหมายให้ครอบคลุมถึงรูปแบบอิเล็กทรอนิกส์ด้วย

โดยทั่วไป “เอกสาร” หมายถึง สิ่งที่แสดงความหมายผ่านตัวอักษร ตัวเลข แผนผัง หรือภาพใด ๆ ที่ปรากฏอยู่บนวัตถุ เช่น กระดาษ หรือวัสดุอื่น ไม่ว่าจะจัดทำขึ้นด้วยวิธีการพิมพ์ การถ่ายภาพ หรือวิธีการอื่นก็ตาม จุดประสงค์คือเพื่อใช้เป็นหลักฐานหรือสื่อความหมายที่ชัดเจนตามกฎหมาย อย่างไรก็ตาม เมื่อเทคโนโลยีได้เข้ามาเปลี่ยนแปลงรูปแบบของข้อมูล การนิยามคำว่า

“อิเล็กทรอนิกส์” จึงถูกขยายออกไปให้ครอบคลุมถึงวิธีการที่ใช้พลังงานไฟฟ้า คลื่นแม่เหล็กไฟฟ้า รวมถึงการใช้วิธีการทางแสงหรือแม่เหล็ก และรวมไปถึงอุปกรณ์หรือระบบที่เกี่ยวข้องกับการประมวลผลทางอิเล็กทรอนิกส์

ภายใต้บริบทนี้ คำว่า “ข้อมูลอิเล็กทรอนิกส์” จึงหมายถึง ข้อความหรือข้อมูลที่ถูกสร้างขึ้น ส่งต่อ รับไว้ เก็บรักษา หรือประมวลผลผ่านระบบอิเล็กทรอนิกส์ ตัวอย่างเช่น การแลกเปลี่ยนข้อมูลผ่านระบบออนไลน์ อีเมล โทรเลข หรือโทรสาร ซึ่งล้วนแต่เป็นรูปแบบของข้อมูลที่สามารถนำมาใช้เป็นพยานหลักฐานได้ในทางกฎหมาย

การเข้าใจความหมายของเอกสารและข้อมูลในรูปแบบอิเล็กทรอนิกส์จึงเป็นรากฐานที่สำคัญในการศึกษาพยานหลักฐานยุคใหม่ โดยเฉพาะอย่างยิ่งในบริบทของคดีอาชญากรรมทางเทคโนโลยีที่ต้องพิจารณาทั้งรูปแบบของข้อมูล ช่องทางการได้มา และความน่าเชื่อถือของข้อมูลดังกล่าวอย่างรอบด้าน

เอกสารอิเล็กทรอนิกส์

การจัดเก็บเอกสารในรูปแบบอิเล็กทรอนิกส์ได้กลายเป็นแนวทางหลักของการบริหารข้อมูลในยุคดิจิทัล เอกสารอิเล็กทรอนิกส์ หรือ Electronic Document เป็นข้อมูลที่ถูกจัดเก็บในระบบอิเล็กทรอนิกส์ ไม่ว่าจะอยู่ในรูปแบบไฟล์ข้อความ รูปภาพ หรือรูปแบบที่สามารถประมวลผลได้โดยเครื่องคอมพิวเตอร์ โดยมีวัตถุประสงค์เพื่อใช้ทดแทนเอกสารกระดาษในงานธุรกรรมหรือกิจกรรมต่าง ๆ ทั้งภาครัฐและภาคเอกชน

การเปลี่ยนจากระบบเอกสารกระดาษไปสู่ระบบอิเล็กทรอนิกส์นั้น มีข้อดีหลายประการ โดยเฉพาะด้านการลดค่าใช้จ่าย ไม่ว่าจะเป็นค่าใช้จ่ายทางตรง เช่น กระดาษ หมึกพิมพ์ และการจัดเก็บเอกสาร รวมไปถึงค่าใช้จ่ายทางอ้อมอย่างเช่นเวลาในการค้นหาเอกสารหรือความเสี่ยงจากการสูญหายของข้อมูล นอกจากนี้ เอกสารอิเล็กทรอนิกส์ยังสามารถเพิ่มประสิทธิภาพในการเข้าถึงและแลกเปลี่ยนข้อมูลได้อย่างรวดเร็วและน่าเชื่อถือมากขึ้น

อีกหนึ่งจุดเด่นของเอกสารอิเล็กทรอนิกส์ คือ ความสามารถในการแนบไฟล์ในรูปแบบที่เครื่องคอมพิวเตอร์สามารถนำไปประมวลผลต่อได้ เช่น ไฟล์ XML ซึ่งเป็นภาษามาตรฐานในการจัดโครงสร้างข้อมูล ทำให้สามารถแลกเปลี่ยนข้อมูลระหว่างหน่วยงานหรือระบบต่าง ๆ ได้อย่างสะดวกโดยไม่ต้องพึ่งพาการป้อนข้อมูลด้วยมนุษย์โดยตรง

ด้วยคุณสมบัติดังกล่าว เอกสารอิเล็กทรอนิกส์จึงไม่ได้เป็นเพียงแค่รูปแบบใหม่ของการจัดเก็บข้อมูล แต่ยังเป็นเครื่องมือสำคัญที่ช่วยสนับสนุนการบริหารจัดการองค์กรให้มีความคล่องตัว โปร่งใส และทันสมัยมากยิ่งขึ้น

โครงสร้างเอกสารอิเล็กทรอนิกส์

เอกสารอิเล็กทรอนิกส์ (Electronic Documents) หมายถึง ข้อมูลที่ถูกสร้างขึ้นและจัดเก็บในรูปแบบดิจิทัลภายในระบบคอมพิวเตอร์ โดยไม่จำเป็นต้องมีรูปแบบทางกายภาพเหมือนเอกสารกระดาษที่ใช้กันทั่วไปในอดีต แนวทางนี้ช่วยให้เอกสารสามารถเข้าถึงและดำเนินการได้โดยไม่ต้องพิมพ์ออกมาเป็นกระดาษ การใช้เอกสารอิเล็กทรอนิกส์จึงเป็นการประหยัดทรัพยากรและเวลา ในขณะเดียวกันยังช่วยให้การจัดการเอกสารมีความคล่องตัวมากยิ่งขึ้น

ในปัจจุบัน แม้ว่าเอกสารอิเล็กทรอนิกส์จะมีความสะดวกในการจัดเก็บและแลกเปลี่ยนข้อมูล แต่ผู้ใช้งานจำนวนมากยังคงต้องพิมพ์เอกสารเหล่านั้นออกมาเป็นรูปแบบกระดาษเพื่อให้สามารถใช้ในกระบวนการต่าง ๆ ที่ต้องการรูปแบบทางกายภาพ อย่างไรก็ตาม การพัฒนาเทคโนโลยีด้านระบบเครือข่ายคอมพิวเตอร์ช่วยให้เอกสารอิเล็กทรอนิกส์สามารถส่งไปยังปลายทางได้ในทันที โดยไม่จำเป็นต้องแปลงเอกสารนั้นเป็นกระดาษก่อนที่จะดำเนินการ

นอกจากนี้ เทคโนโลยีการแสดงผลและการรักษาความปลอดภัยในเอกสารอิเล็กทรอนิกส์ยังช่วยให้ข้อความในเอกสารสามารถอ่านได้อย่างชัดเจนและปลอดภัย ผู้ใช้สามารถมั่นใจได้ว่าเอกสารที่ได้รับมีความถูกต้องครบถ้วนและสามารถตรวจสอบตัวตนได้ ผ่านกระบวนการตรวจสอบและรักษาความปลอดภัยที่ทันสมัย

จากการพัฒนาเทคโนโลยีดังกล่าว ส่งผลให้เอกสารอิเล็กทรอนิกส์ได้รับความนิยมและใช้แพร่หลายมากขึ้น ซึ่งมีผลต่อการดำเนินธุรกรรมในทุกระดับ ไม่ว่าจะเป็นธุรกรรมทางการเงิน การสื่อสาร หรือการจัดการข้อมูลของหน่วยงานต่าง ๆ ความสะดวกและประสิทธิภาพในการใช้เอกสารอิเล็กทรอนิกส์ทำให้แนวโน้มในอนาคตจะเห็นการลดลงของการใช้เอกสารกระดาษอย่างชัดเจน

ด้วยคุณสมบัติและประโยชน์ของเอกสารอิเล็กทรอนิกส์ที่มีทั้งความสะดวก รวดเร็ว และปลอดภัย จึงไม่น่าแปลกใจที่การใช้เอกสารอิเล็กทรอนิกส์จะเพิ่มขึ้นในอนาคต โดยคาดว่าในอีกไม่กี่ปีข้างหน้า ธุรกรรมที่เกี่ยวข้องกับเอกสารจะถูกดำเนินการในรูปแบบอิเล็กทรอนิกส์มากขึ้นเรื่อย ๆ

การใช้พยานหลักฐานในกระบวนการพิจารณาคดีของศาลนั้นสามารถแบ่งออกเป็นหลายประเภท ตามวัตถุประสงค์และเกณฑ์การจัดประเภทที่ใช้ โดย Merryman (1985) ได้แบ่งพยานหลักฐานออกเป็นประเภทต่าง ๆ ดังนี้

1.พยานบุคคล พยานเอกสาร และพยานวัตถุ

2.พยานชนิดหนึ่ง และพยานชนิดสอง

3.พยานโดยตรง และพยานแวดล้อม

4.พยานทราบเอง และพยานบอกเล่า

การแบ่งประเภทพยานหลักฐานเหล่านี้มีความสำคัญต่อการพิจารณาในกระบวนการยุติธรรม เนื่องจากสามารถช่วยให้การพิจารณาปัญหาทางกฎหมายชัดเจนยิ่งขึ้น โดยเฉพาะในกรณีที่เกี่ยวข้องกับเอกสารอิเล็กทรอนิกส์ ซึ่งการนำข้อมูลจากสื่ออิเล็กทรอนิกส์มาใช้เป็นพยานหลักฐานในศาลนั้นอาจมีข้อสงสัยเกี่ยวกับสถานะทางกฎหมายและการยอมรับข้อมูลดังกล่าว

ในปัจจุบัน ข้อมูลที่ได้จากสื่ออิเล็กทรอนิกส์ยังไม่มีกฎหมายที่ชัดเจนกำหนดว่าข้อมูลเหล่านี้สามารถนำมาใช้เป็นพยานหลักฐานในศาลได้อย่างไร และจะอยู่ในประเภทใด เนื่องจากในระบบกฎหมายของประเทศไทย การแบ่งประเภทพยานหลักฐานยังคงมีเพียง 4 ประเภท ได้แก่ พยานบุคคล พยานเอกสาร พยานวัตถุ และพยานผู้เชี่ยวชาญ ซึ่งการนำเอกสารอิเล็กทรอนิกส์มาใช้ในกระบวนการยุติธรรมนั้นยังต้องพิจารณาในแง่ของหลักเกณฑ์และการยอมรับตามกฎหมาย

ทั้งนี้ เพื่อให้สามารถดำเนินการต่าง ๆ ตามที่กฎหมายบัญญัติได้ในรูปแบบข้อมูลอิเล็กทรอนิกส์และมีผลผูกพันตามกฎหมาย จำเป็นต้องมีการกำหนดกฎหมายหรือข้อบังคับเพิ่มเติมที่ชัดเจนเกี่ยวกับการใช้เอกสารอิเล็กทรอนิกส์เป็นพยานหลักฐานในศาล เพื่อให้การพิจารณาคดีมีความโปร่งใสและเป็นธรรมในยุคที่ข้อมูลดิจิทัลมีบทบาทสำคัญในการดำเนินกระบวนการยุติธรรม

การพิสูจน์ความถูกต้องและแท้จริงของพยานเอกสารอิเล็กทรอนิกส์

การพิจารณาความน่าเชื่อถือของพยานเอกสารในกระบวนการยุติธรรมนั้น ถือเป็นขั้นตอนสำคัญในการตัดสินคดี โดยเฉพาะเมื่อพยานเอกสารนั้นเป็นเอกสารอิเล็กทรอนิกส์ ซึ่งมีข้อกังวลเรื่องความถูกต้องและความแท้จริงของข้อมูลที่ถูกนำเสนอในศาลตามมาตรา 126 ของประมวลกฎหมายวิธีพิจารณาความแพ่ง

การนำพยานเอกสารเข้าสู่กระบวนการพิจารณาคดีในศาลนั้น โดยทั่วไปจะต้องมีการสนับสนุนจากพยานบุคคล ซึ่งบุคคลนั้นต้องสามารถยืนยันถึงความถูกต้องและที่มาของเอกสารได้ หากฝ่ายใดฝ่ายหนึ่งคัดค้านความถูกต้องของเอกสารที่นำมาใช้ ศาลจะต้องสอบสวนพยานที่มีความรู้หรือเกี่ยวข้องกับเอกสารนั้น ๆ เพื่อพิสูจน์ความแท้จริงของข้อมูลและเอกสาร

ในกรณีของเอกสารอิเล็กทรอนิกส์ ผู้ที่สามารถเป็นพยานในการพิสูจน์ความถูกต้องของเอกสาร คือ เจ้าหน้าที่หรือบุคคลที่มีหน้าที่ดูแลรักษาข้อมูลหรือผู้ที่ใช้ข้อมูลนั้น ๆ ในการปฏิบัติงาน ซึ่งบุคคลเหล่านี้อาจไม่รู้หรือไม่เข้าใจระบบการทำงานของคอมพิวเตอร์ที่ใช้ในการจัดการข้อมูล โดยในบางกรณีจะเป็นการยากที่จะหาพยานบุคคลที่สามารถยืนยันถึงกระบวนการทั้งหมดที่นำไปสู่การสร้างเอกสารอิเล็กทรอนิกส์นั้น

ดังนั้น การพิจารณาความน่าเชื่อถือของเอกสารอิเล็กทรอนิกส์ในศาลจึงไม่สามารถอาศัยเพียงแค่การนำเอกสารออกจากระบบคอมพิวเตอร์มาใช้เป็นหลักฐานได้ แต่ต้องมีการพิสูจน์ถึงความถูกต้องของระบบคอมพิวเตอร์ที่ใช้ในการสร้างข้อมูลนั้น ๆ และต้องพิสูจน์ด้วยว่ามีมาตรการในการรักษาความปลอดภัยในการเข้าถึงข้อมูล เพื่อให้มั่นใจว่าไม่มีความผิดพลาดในการจัดการข้อมูลดังกล่าว

การนำเอกสารอิเล็กทรอนิกส์มาใช้ในกระบวนการยุติธรรมนั้น จึงต้องพิจารณาถึงทั้งความปลอดภัย ความถูกต้อง และการตรวจสอบระบบที่เกี่ยวข้อง เพื่อให้การพิจารณาคดีเป็นไปอย่างยุติธรรมและถูกต้องตามหลักกฎหมาย ซึ่งเป็นสิ่งสำคัญในการทำให้ข้อมูลดิจิทัลสามารถนำมาใช้เป็นหลักฐานที่มีความน่าเชื่อถือในกระบวนการยุติธรรมในอนาคต

การชั่งน้ำหนักพยานหลักฐานของเอกสารอิเล็กทรอนิกส์

การพิจารณาความน่าเชื่อถือของพยานหลักฐานเป็นกระบวนการสำคัญที่ใช้ในการตัดสินคดีในศาล โดยเฉพาะในคดีที่เกี่ยวข้องกับพยานหลักฐานอิเล็กทรอนิกส์ ซึ่งมีลักษณะเฉพาะที่แตกต่างจากพยานหลักฐานประเภทอื่น ๆ การประเมินความน่าเชื่อถือของพยานหลักฐานอิเล็กทรอนิกส์จึงเป็นเรื่องที่ท้าทาย เนื่องจากข้อมูลอิเล็กทรอนิกส์มีความเสี่ยงในการเปลี่ยนแปลงหรือถูกดัดแปลงได้ง่าย การที่ศาลจะรับฟังข้อมูลจากเอกสารอิเล็กทรอนิกส์ได้หรือไม่นั้น ขึ้นอยู่กับหลายปัจจัย เช่น วิธีการเก็บรวบรวมข้อมูล การประมวลผลข้อมูล และมาตรการป้องกันการดัดแปลงข้อมูล

ในการพิจารณาคดีแพ่ง ศาลจะต้องทำการเปรียบเทียบหลักฐานจากทั้งสองฝ่าย โดยพิจารณาเหตุผลและน้ำหนักของพยานหลักฐานที่แต่ละฝ่ายนำเสนอ ส่วนในคดีอาญา ศาลจะพิจารณาพยานหลักฐานของโจทก์ก่อน โดยมักจะพิจารณาในเชิงลึกถึงความน่าเชื่อถือและความถูกต้องของข้อมูล หากข้อมูลที่นำมาใช้เป็นเอกสารอิเล็กทรอนิกส์ ก็จะต้องมีการตรวจสอบว่าไม่มีการเปลี่ยนแปลงข้อมูลหลังจากที่ข้อมูลถูกจัดทำขึ้นมาแล้ว

การเปลี่ยนแปลงจากระบบการทำธุรกรรมแบบกระดาษไปสู่ระบบไร้กระดาษทำให้ข้อมูลอิเล็กทรอนิกส์มีบทบาทสำคัญในปัจจุบัน แม้ว่าในบางกรณีเอกสารอิเล็กทรอนิกส์จะได้รับการยอมรับในฐานะพยานหลักฐาน แต่ก็ยังคงมีความท้าทายในการตรวจสอบความน่าเชื่อถือของข้อมูลเหล่านั้น การที่ระบบกฎหมายในประเทศไทยยังไม่ได้กำหนดแนวทางที่ชัดเจนในการรับฟังพยานหลักฐานอิเล็กทรอนิกส์ ทำให้มีความไม่แน่นอนในกระบวนการพิจารณาคดี และอาจทำให้การพิจารณาคดีแต่ละคดีแตกต่างกันไป

การที่จะทำให้พยานหลักฐานอิเล็กทรอนิกส์ได้รับการยอมรับในกระบวนการยุติธรรมได้อย่างเหมาะสม จำเป็นต้องมีการปรับปรุงกฎหมายและแนวทางในการพิจารณาความน่าเชื่อถือของข้อมูลอิเล็กทรอนิกส์ โดยเฉพาะในประมวลกฎหมายวิธีพิจารณาความแพ่งและประมวลกฎหมายวิธีพิจารณาความอาญา ซึ่งควรจะมีบทบัญญัติเพิ่มเติมเกี่ยวกับการใช้ข้อมูลอิเล็กทรอนิกส์ในฐานะพยานหลักฐาน การพัฒนามาตรฐานในการเก็บข้อมูลและการป้องกันการดัดแปลงข้อมูลจะช่วยให้ข้อมูลเหล่านี้ได้รับการยอมรับในกระบวนการยุติธรรมได้มากขึ้น

การพัฒนาเทคโนโลยีและมาตรฐานที่ชัดเจนในการใช้ข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในศาล จะช่วยเพิ่มความโปร่งใสและความเป็นธรรมในกระบวนการยุติธรรม อีกทั้งยังช่วยให้การดำเนินการทางกฎหมายในยุคดิจิทัลสามารถทำได้อย่างมีประสิทธิภาพและเป็นที่ยอมรับในระดับสากล

หลักเกณฑ์มาตรฐานทางด้านเทคโนโลยีของข้อมูลอิเล็กทรอนิกส์

หลักเกณฑ์มาตรฐานทางด้านเทคโนโลยีในการจัดการข้อมูลอิเล็กทรอนิกส์เพื่อให้ข้อมูลสามารถนำมาใช้เป็นพยานหลักฐานในกระบวนการยุติธรรมได้อย่างมีประสิทธิภาพและเชื่อถือได้ จำเป็นต้องมีการกำหนดมาตรฐานที่สอดคล้องกับข้อกำหนดของสากล เพื่อให้ศาลสามารถมั่นใจใน

กระบวนการต่างๆ ที่เกี่ยวข้องกับการเก็บรวบรวมข้อมูล รวมถึงวิธีการตรวจสอบและยืนยันความถูกต้องของข้อมูลเหล่านั้น โดยหลักเกณฑ์ที่สำคัญมีดังนี้:

1.การรักษาความลับ (Confidentiality) การจัดการข้อมูลอิเล็กทรอนิกส์ต้องมีการรักษาความลับเพื่อป้องกันไม่ให้ข้อมูลถูกเปิดเผยหรือถูกเข้าถึงโดยบุคคลที่ไม่ได้รับอนุญาต มาตรการที่ใช้ในขั้นตอนนี้อาจรวมถึงการเข้ารหัสข้อมูลและการกำหนดระดับความลับของข้อมูล เพื่อให้มั่นใจได้ว่าข้อมูลที่ถูกเก็บไว้จะได้รับการปกป้องอย่างเต็มที่ และสามารถรักษาความปลอดภัยในทุกขั้นตอนของกระบวนการ.

2.การรักษาความครบถ้วนและความถูกต้อง (Integrity) ข้อมูลอิเล็กทรอนิกส์ต้องมีความถูกต้องและครบถ้วนในทุกๆ การนำเสนอและใช้งาน ในการตรวจสอบความสมบูรณ์และความถูกต้องของข้อมูล ควรมีการใช้เทคโนโลยีเช่น การเข้ารหัสลับ (Encryption) และการคำนวณข้อมูลผ่านอัลกอริธึม Hashing เพื่อให้สามารถตรวจสอบได้ว่าไม่มีการเปลี่ยนแปลงหรือการแทรกแซงข้อมูลในระหว่างกระบวนการต่างๆ.

3.การกำหนดสิทธิในการเข้าถึง (Access Control) การควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศเป็นอีกหนึ่งมาตรการสำคัญในการรักษาความปลอดภัยของข้อมูล โดยการกำหนดสิทธิการเข้าถึงระบบและการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอจะช่วยให้ข้อมูลได้รับการปกป้องจากการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต การระบุผู้ใช้งานและการยืนยันตัวตน (Authentication) ผ่านกระบวนการที่มีความปลอดภัย เช่น การใช้รหัสผ่านหรือเทคโนโลยีอื่นๆ เพื่อยืนยันสิทธิในการเข้าถึงข้อมูล.

4.การรักษาความมั่นคงปลอดภัย (Security) การรักษาความปลอดภัยทางกายภาพและทางเทคนิคของระบบที่ใช้จัดเก็บข้อมูลอิเล็กทรอนิกส์เป็นสิ่งสำคัญ เพื่อให้ข้อมูลได้รับการปกป้องจากภัยคุกคามต่างๆ ซึ่งอาจรวมถึงการใช้ระบบสำรองข้อมูล (Backup) และการควบคุมการเข้าถึงในระดับต่างๆ ของข้อมูล นอกจากนี้ยังต้องมีการควบคุมด้านการฝึกอบรมบุคลากรเพื่อให้การรักษาความปลอดภัยข้อมูลเป็นไปตามมาตรฐานที่กำหนด.

การกำหนดมาตรฐานเหล่านี้ไม่เพียงแต่จะช่วยในการจัดการข้อมูลอย่างมีประสิทธิภาพ แต่ยังเสริมสร้างความมั่นใจให้กับทุกฝ่ายที่เกี่ยวข้องในกระบวนการยุติธรรมว่า ข้อมูลที่ถูกนำมาใช้ในคดีนั้นมีความถูกต้องและมีความน่าเชื่อถือตามหลักเกณฑ์ที่ได้มาตรฐาน

2.6 ข้อมูลหลักกฎหมายวิธีพิจารณาความอาญา

ในระบบกฎหมายไทย การพิจารณาคดีในทางแพ่งได้มีการปรับตัวและพัฒนาเพื่อให้ทันสมัยและสอดคล้องกับการเปลี่ยนแปลงในด้านต่างๆ โดยเฉพาะการใช้เทคโนโลยีสารสนเทศในการนำพยานหลักฐานเข้าสู่กระบวนการพิจารณา โดยมีการแก้ไขและปรับปรุงประมวลกฎหมายวิธีพิจารณาความแพ่งเพื่อรองรับการใช้เทคโนโลยีอิเล็กทรอนิกส์ในการดำเนินคดีมากยิ่งขึ้น

การแก้ไขในประมวลกฎหมายวิธีพิจารณาความแพ่ง (ฉบับที่ 23) พ.ศ. 2550 ถือเป็นการเปลี่ยนแปลงสำคัญในทางกฎหมาย โดยเปิดโอกาสให้ศาลสามารถรับฟังพยานหลักฐานที่มีการบันทึกในรูปแบบอิเล็กทรอนิกส์หรือที่จัดเก็บในสื่อดิจิทัลต่างๆ ได้ ซึ่งไม่เพียงแต่ช่วยให้กระบวนการพิจารณาคดีมีความสะดวกมากขึ้น แต่ยังทำให้ศาลสามารถเข้าถึงข้อมูลที่ถูกบันทึกในรูปแบบดิจิทัลได้โดยง่ายและรวดเร็ว

นอกจากนี้ยังมีการแก้ไขประมวลกฎหมายวิธีพิจารณาความแพ่ง (ฉบับที่ 28) พ.ศ. 2558 ซึ่งเพิ่มเติมการรองรับการใช้เทคโนโลยีสารสนเทศในทุกขั้นตอนของกระบวนการพิจารณาคดี โดยการใช้ระบบดิจิทัลในการจัดเก็บข้อมูล การส่งเอกสาร และการติดต่อระหว่างศาลกับคู่ความ ซึ่งช่วยลดภาระและเพิ่มประสิทธิภาพในการดำเนินคดีให้เกิดความรวดเร็วและสะดวกมากขึ้น

การพัฒนาเหล่านี้ไม่เพียงแค่การตอบสนองต่อการเติบโตของเทคโนโลยีในยุคปัจจุบัน แต่ยังสะท้อนให้เห็นถึงความพยายามในการยกระดับกระบวนการยุติธรรมให้มีประสิทธิภาพและสามารถรองรับข้อมูลในรูปแบบดิจิทัลได้อย่างถูกต้องและน่าเชื่อถือ การใช้พยานหลักฐานอิเล็กทรอนิกส์ในศาลจึงไม่ใช่แค่การปรับตัวตามเทคโนโลยี แต่ยังเป็นการเสริมสร้างความโปร่งใสและความยุติธรรมในกระบวนการพิจารณาคดี ซึ่งช่วยเพิ่มความเชื่อมั่นให้กับประชาชนในระบบการยุติธรรมของประเทศ

การดำเนินกระบวนพิจารณาทางอิเล็กทรอนิกส์

การพิจารณาคดีทางอิเล็กทรอนิกส์ในระบบศาลไทยเป็นเรื่องที่เกี่ยวข้องกับการรับรองความถูกต้องและการใช้ข้อมูลอิเล็กทรอนิกส์ในการพิจารณาคดีและรับฟังพยานหลักฐาน โดยในปี พ.ศ. 2563 ได้มีข้อกำหนดของประธานศาลฎีกาเกี่ยวกับวิธีการพิจารณาคดีทางอิเล็กทรอนิกส์ ซึ่ง

กำหนดให้ศาลสามารถใช้เทคโนโลยีในการดำเนินกระบวนการพิจารณาคดี โดยไม่จำเป็นต้องใช้วิธีการดั้งเดิมที่ต้องปรากฏตัวในห้องพิจารณาคดี

1.การพิจารณาคดีทางอิเล็กทรอนิกส์ ศาลสามารถกำหนดให้มีการพิจารณาคดีทางอิเล็กทรอนิกส์ได้ โดยพิจารณาความสะดวกและประหยัดสำหรับผู้ที่ไม่สามารถเข้าถึงเทคโนโลยีได้ การใช้วิธีพิจารณาทางอิเล็กทรอนิกส์นี้สามารถใช้ได้กับคดีทุกประเภท รวมถึงคดีแพ่ง คดีผู้บริโภค และคดีอื่นๆ ที่กฎหมายกำหนดให้นำวิธีการนี้มาใช้

2.การจัดการเอกสารและพยานหลักฐาน ระบบการจัดการเอกสารและพยานหลักฐานผ่านระบบอิเล็กทรอนิกส์ (**e-**Filing) และบริการข้อมูลคดีศาล **(**CIOS) ช่วยให้การส่งเอกสารและพยานหลักฐานทำได้อย่างสะดวกและรวดเร็ว โดยเอกสารที่ส่งผ่านระบบจะได้รับการรับรองและเชื่อถือได้ตามกฎหมาย

3.พยานเอกสารและพยานวัตถุ เอกสารที่ส่งผ่านระบบอิเล็กทรอนิกส์จะได้รับการรับรองตามมาตรฐานที่กำหนด โดยสามารถใช้เอกสารและพยานวัตถุในรูปแบบอิเล็กทรอนิกส์เป็นหลักฐานในการพิจารณาคดีได้ หากศาลเห็นว่าเป็นข้อมูลที่เชื่อถือได้

4.การนั่งพิจารณาคดี ศาลอาจจัดให้มีการนั่งพิจารณาคดีและบันทึกคำให้การของพยานผ่านระบบอิเล็กทรอนิกส์ โดยไม่จำเป็นต้องมีการปรากฏตัวของผู้เกี่ยวข้องในศาล ซึ่งจะถือว่าเป็นการพิจารณาคดีที่เสมือนการดำเนินการในห้องพิจารณาคดีจริง

5.การรับฟังพยานหลักฐาน ศาลไม่สามารถปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานเพียงเพราะเป็นข้อมูลอิเล็กทรอนิกส์ และต้องรับฟังตามข้อกำหนดของกฎหมาย

6.การพิพากษา เมื่อศาลพิจารณาคดีเสร็จสิ้นแล้วสามารถออกคำพิพากษาหรือคำสั่งในรูปแบบอิเล็กทรอนิกส์ได้ ตามวิธีการที่กำหนดไว้

7.การสนับสนุนความน่าเชื่อถือของข้อมูลอิเล็กทรอนิกส์ กฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ (พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544) ได้กำหนดให้ข้อมูลอิเล็กทรอนิกส์สามารถรับรองสถานะทางกฎหมายและใช้เป็นหลักฐานได้ โดยหากข้อมูลอิเล็กทรอนิกส์ได้รับการรับรองความถูกต้องและความน่าเชื่อถือจากเจ้าของลายมือชื่อ ก็จะถือว่าเป็นข้อมูลที่ถูกต้องตามกฎหมาย

การพิจารณาคดีทางอิเล็กทรอนิกส์จึงเป็นการปรับใช้เทคโนโลยีในการทำให้กระบวนการยุติธรรมมีความรวดเร็วและมีประสิทธิภาพมากขึ้น โดยไม่ลดทอนความถูกต้องหรือความยุติธรรมในการพิจารณาคดี

ตารางที่ 2.1 วิเคราะห์กฎหมายเกี่ยวกับการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์

วิเคราะห์กฎหมายเกี่ยวกับการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ของประเทศไทย	
ปัญหาการออกหมายค้นโดยศาล	1.เห็นได้ว่าหมายค้นของศาลเป็นสิ่งสำคัญในการคุ้มครองสิทธิและเสรีภาพของประชาชน เพราะช่วยให้การใช้อำนาจของเจ้าพนักงานอยู่ภายใต้การตรวจสอบ ไม่ให้กระทำเกินความจำเป็น 2.การที่หมายค้นต้องระบุสถานที่ค้นอย่างชัดเจน กลับไม่สอดคล้องกับลักษณะของอาชญากรรมทางคอมพิวเตอร์ ซึ่งคนร้ายสามารถเข้าถึงและทำลายข้อมูลจากที่ใดก็ได้ในโลก โดยเฉพาะเมื่อมีการร่วมมือกันหลายคน ยิ่งทำให้สามารถปกปิดและลบหลักฐานได้ง่ายขึ้น 3.พยานหลักฐานในคดีลักษณะนี้มีความละเอียดอ่อนและสามารถถูกทำลายได้อย่างรวดเร็ว ทำให้ขั้นตอนการขอหมายค้นอาจเกิดความล่าช้า ดังนั้น จึงเห็นว่าควรมีมาตรการเพิ่มเติม เช่น การตรวจสอบการใช้อำนาจของเจ้าพนักงานโดยศาล เพื่อให้ยังสามารถคุ้มครองสิทธิของประชาชนได้อย่างมีประสิทธิภาพ

ตารางที่ 2.1 (ต่อ) วิเคราะห์กฎหมายเกี่ยวกับการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์

วิเคราะห์กฎหมายเกี่ยวกับการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ของประเทศไทย	
ปัญหาเกี่ยวกับการระบุรายละเอียดในหมายค้น	1.การระบุสิ่งของที่จะค้นในคดีอาชญากรรมทางคอมพิวเตอร์มีความซับซ้อนมากกว่าคดีทั่วไป เนื่องจากพยานหลักฐานมักอยู่ในรูปของข้อมูลในคอมพิวเตอร์หรือสื่ออิเล็กทรอนิกส์ซึ่งไม่สามารถจับต้องได้โดยตรง การยึดพยานหลักฐานจึงไม่สามารถทำได้เหมือนการยึดวัตถุทั่วไป แต่ต้องใช้วิธีทางเทคนิค เช่น การคัดลอกไฟล์ หรือการเก็บข้อมูลแบบอิมเมจของระบบ อย่างไรก็ตาม ในทางปฏิบัติยังมีข้อสงสัยว่าเจ้าหน้าที่สามารถยึดข้อมูลได้เฉพาะบางส่วนหรือทั้งระบบ และจะกระทบต่อสิทธิของเจ้าของระบบในระดับใด 2.การขอหมายค้นตามมาตรา 69 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา กำหนดให้ต้องระบุสถานที่ค้นและพยานหลักฐานที่จะค้นอย่างชัดเจน โดยต้องแสดงให้เห็นว่าหลักฐานนั้นเกี่ยวข้องกับความผิดจริง อย่างไรก็ตาม ในคดีที่เกี่ยวข้องกับระบบคอมพิวเตอร์ การระบุรายละเอียดเหล่านี้ให้ชัดเจนกลับเป็นเรื่องที่ทำได้ยาก เพราะข้อมูลอาจถูกจัดเก็บกระจายอยู่ในหลายสถานที่ และยังอาจมีการเข้ารหัสหรือซ่อนข้อมูลไว้โดยผู้กระทำผิด ทำให้การค้นและยึดพยานหลักฐานอิเล็กทรอนิกส์มีความท้าทายและซับซ้อนมากยิ่งขึ้น
ปัญหาการรับฟังพยานหลักฐานอิเล็กทรอนิกส์	1.ประเทศไทยมีหลักประกันโดยการบัญญัติรับรองไว้ในรัฐธรรมนูญในการให้ความคุ้มครองสิทธิและเสรีภาพเป็นหลัก รัฐจะใช้อำนาจล่วงละเมิดสิทธิเสรีภาพของประชาชนได้เป็นข้อยกเว้นในกรณีที่มีกฎหมายบัญญัติอำนาจ และ

	เจ้าหน้าที่ของรัฐต้องกระทำโดยชัดแจ้ง พร้อมมีกระบวนการควบคุมที่แน่ชัดและสามารถตรวจสอบได้ 2.การใช้อำนาจในการปราบปรามอาชญากรรมของเจ้าหน้าที่ของรัฐยังคงต้องคำนึงถึงหลักเกณฑ์และรัฐธรรมนูญในการให้ความคุ้มครองสิทธิและเสรีภาพเป็นหลัก รัฐจะใช้อำนาจล่วงละเมิดสิทธิเสรีภาพของประชาชนไม่ได้ ยกเว้นในกรณีที่มีกฎหมายบัญญัติอำนาจของเจ้าหน้าที่ของรัฐไว้โดยชัดแจ้ง และต้องมีกระบวนการควบคุมที่แน่นอน
วิเคราะห์กฎหมายเกี่ยวกับการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ในต่างประเทศ	

ปัญหาในการรับฟังพยานหลักฐานอิเล็กทรอนิกส์ของศาล	1.ตามมาตรา 69 (2) ที่ให้อำนาจเจ้าหน้าที่เข้าตรวจค้นและยึดสิ่งของที่เกี่ยวข้องกับความผิด เช่น ของที่ใช้ก่อเหตุ ของผิดกฎหมาย หรือของที่อาจใช้กระทำความผิดในอนาคต อย่างไรก็ตาม สำหรับพยานหลักฐานทางอิเล็กทรอนิกส์ที่อยู่ในความครอบครองของบุคคล ยังคงเป็นข้อถกเถียงว่าเจ้าหน้าที่สามารถเข้าถึงได้โดยไม่ต้องมีหมายค้นหรือไม่ เพราะข้อยกเว้นในกฎหมายนี้ยังไม่เคยถูกตีความอย่างชัดเจนโดยศาล 2.เมื่อเจ้าหน้าที่ดำเนินการยึดพยานหลักฐานทางอิเล็กทรอนิกส์ เช่น การถ่ายโอนข้อมูลลงแผ่นดิสก์ หรือการพิมพ์ข้อมูลออกมาเป็นกระดาษ ปัญหาสำคัญที่ตามมาคือความน่าเชื่อถือของพยานหลักฐานที่นำมาใช้ 2.1 จะทำอย่างไรให้มั่นใจได้ว่าสิ่งที่เจ้าหน้าที่นำมาเสนอในกระบวนการยุติธรรม เป็นข้อมูลเดียวกันกับที่ได้มาจากสถานที่เกิดเหตุจริง ๆ โดยไม่มีการเปลี่ยนแปลงหรือบิดเบือน 2.2 และจะทำอย่างไรให้มั่นใจได้ว่าข้อมูลที่ยึดมา มีความครบถ้วน สมบูรณ์ ไม่ตกหล่นหรือขาดรายละเอียดสำคัญ

ประเทศสหรัฐอเมริกา	1.ควรกำหนดมาตรฐานขั้นต่ำให้เจ้าหน้าที่ผู้บังคับใช้กฎหมาย เช่น เจ้าหน้าที่ตำรวจหรืออัยการ ต้องปฏิบัติตามขั้นตอนที่ชัดเจนและอยู่ภายใต้การตรวจสอบของศาล เพราะการค้นและยึดทรัพย์มีผลกระทบต่อสิทธิและเสรีภาพของประชาชน ดังนั้น หากไม่มีเหตุอันสมควร ก็ไม่ควรมีการค้นหรือยึดโดยพลการ 2.ในกรณีฉุกเฉิน หากมีความเสี่ยงที่พยานหลักฐานจะถูกทำลาย หน่วยงานบังคับใช้กฎหมายสามารถยึดอุปกรณ์ที่เก็บข้อมูลอิเล็กทรอนิกส์ได้ทันที และหากมีภัยเร่งด่วนที่อาจทำให้ข้อมูลสูญหาย ก็สามารถตรวจค้นได้โดยจำกัดขอบเขตเท่าที่จำเป็นเพื่อป้องกันการสูญเสียข้อมูลสำคัญ 3.หากเป็นการตรวจค้นเพื่อจับกุม การกระทำดังกล่าวอาจจำเป็นเพื่อความปลอดภัยของเจ้าหน้าที่ หรือเพื่อการรักษาพยานหลักฐาน ซึ่งรวมถึงการตรวจค้นอุปกรณ์อิเล็กทรอนิกส์ เช่น โทรศัพท์มือถือ ที่อยู่ในการครอบครองของผู้ต้องสงสัย 4.สำหรับการตรวจค้นทรัพย์สิน ข้อยกเว้นบางประการอาจมีขึ้นเพื่อวัตถุประสงค์ในการป้องกันความเสียหายหรือปกป้องพยานหลักฐาน อย่างไรก็ตาม ต้องอยู่ภายใต้ขอบเขตของเหตุผลอันสมควรและการกำกับดูแลอย่างรอบคอบ

สรุปได้ว่า ในสหรัฐอเมริกา การบังคับใช้กฎหมายและการยึดพยานหลักฐานทางอิเล็กทรอนิกส์เริ่มมีแนวโน้มผ่อนคลายจากหลัก "The Exclusionary Rule" ซึ่งเป็นหลักที่ศาลสูงของสหรัฐฯ ใช้ในการคุ้มครองสิทธิส่วนบุคคลของประชาชนตาม "The Fourth Amendment" โดยการห้ามไม่ให้เจ้าหน้าที่ละเมิดสิทธิของประชาชนโดยไม่มีเหตุผลและไม่จำเป็น และห้ามไม่ให้รับพยานหลักฐานที่ได้มาโดยวิธีที่ผิดกฎหมาย รวมถึงพยานหลักฐานที่ได้มาจากการกระทำที่ไม่ชอบด้วยกฎหมาย

อย่างไรก็ตาม ในปัจจุบัน การบังคับใช้กฎหมายเกี่ยวกับพยานหลักฐานทางอิเล็กทรอนิกส์เริ่มมีการผ่อนคลายมากขึ้น

โดยเฉพาะในกรณีที่เกี่ยวข้องกับข้อมูลดิจิทัล ซึ่งมีความท้าทายในการรวบรวมพยานหลักฐาน และในบางกรณีอาจมีการพิจารณาทบทวนหลักการนี้ตามสถานการณ์ต่าง ๆ ที่เกิดขึ้น

ตารางที่ 2.1 (ต่อ) วิเคราะห์กฎหมายเกี่ยวกับการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์

ประเทศอังกฤษ	1.มาตรา 60 ระบุว่าในการพิจารณาคดีทางกฎหมาย พยานหลักฐานที่เป็นข้อมูลที่ประมวลผลโดยคอมพิวเตอร์ หรือเอกสารที่ได้รับการประมวลผลโดยคอมพิวเตอร์จะไม่สามารถนำมาใช้เป็นพยานหลักฐานได้ ยกเว้นในกรณีที่: 1.1 ไม่มีเหตุผลที่เชื่อได้ว่าพยานเอกสารนั้นมีข้อผิดพลาดจากการใช้คอมพิวเตอร์ในการประมวลผล 1.2 ในกระบวนการพิมพ์เอกสารจากคอมพิวเตอร์ไม่มีความผิดพลาด และข้อมูลในเอกสารนั้นเป็นข้อมูลที่ถูกต้องแท้จริง

สรุปได้ว่า ในคดีอาญา พยานหลักฐานที่เป็นข้อมูลจากการประมวลผลของคอมพิวเตอร์สามารถนำมาพิจารณาได้หากไม่มีข้อผิดพลาดในกระบวนการทำงานของคอมพิวเตอร์ และข้อมูลนั้นมีความถูกต้องแท้จริง ไม่มีการแก้ไขหรือเปลี่ยนแปลงเนื้อหา อย่างไรก็ตาม ในคดีแพ่ง ต้องมีการรับรองความถูกต้องของพยานหลักฐานที่เป็นเอกสารหรือพยานวัตถุอย่างชัดเจน ซึ่งเป็นหลักการที่ยังคงใช้บังคับอยู่ตามกฎหมาย ในระบบกฎหมายคอมมอนลอว์ (Common Law) การรับรองความถูกต้องแท้จริงของพยานหลักฐานที่เกี่ยวข้องกับการประมวลผลโดยคอมพิวเตอร์นั้นจำเป็นต้องมีลายมือชื่อของบุคคลที่รับผิดชอบในกระบวนการทำงานของคอมพิวเตอร์นั้น เพื่อให้การรับฟังพยานหลักฐานนั้นเป็นที่ยอมรับได้ตามกฎหมาย

ตารางที่ 2.1 (ต่อ) วิเคราะห์กฎหมายเกี่ยวกับการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์

ประเทศสหพันธ์สาธารณรัฐเยอรมัน	1.การค้นตามกฎหมายของประเทศเยอรมนีตามมาตรา 107 จะต้องระบุรายละเอียดในหมายค้นอย่างชัดเจน โดยรวมถึงมูลเหตุที่ต้องทำการค้น บุคคลที่เกี่ยวข้อง และสิ่งของที่ต้องการค้น 2.ในการค้นและยึดพยานหลักฐานตามกฎหมายเยอรมนี วิธีการค้นต้องดำเนินการอย่างเคร่งครัดตามมาตรา 106 วรรคแรก ซึ่งระบุว่า "การค้นต้องกระทำต่อหน้าเจ้าของสถานที่ หากเจ้าของสถานที่ไม่อยู่จะต้องกระทำต่อหน้าผู้แทน ญาติ หรือเพื่อนบ้าน" เพื่อรับรองความน่าเชื่อถือและโปร่งใสของกระบวนการค้น 3.ประเทศเยอรมนีไม่มีบทบัญญัติพิเศษที่ลงโทษอาชญากรรมทางอิเล็กทรอนิกส์โดยตรงเหมือนกับในประเทศสหรัฐอเมริกา แต่ในกรณีที่มีบทลงโทษทางอาญา ภายใต้ประมวลกฎหมายอาญาเยอรมัน (German Criminal Code 1974) จะมีการตรวจค้นข้อมูลอิเล็กทรอนิกส์ที่อยู่ในความครอบครองของบุคคลในสถานที่ส่วนตัว เช่น ในเครื่องคอมพิวเตอร์พีซี (PC)

สรุปได้ว่า ปัจจุบันในประเทศเยอรมนี การรวบรวมพยานหลักฐานมีลักษณะคล้ายคลึงกับกฎหมายของประเทศไทย โดยพนักงานตำรวจจะดำเนินการภายใต้กรอบของกฎหมายที่ให้อำนาจไว้เท่านั้น สำหรับการรวบรวมพยานหลักฐานในคดีที่เกี่ยวข้องกับคอมพิวเตอร์ กฎหมายจะได้รับการพัฒนาและปรับปรุงให้สามารถรองรับกับการเปลี่ยนแปลงทางเทคโนโลยีได้ โดยศาลจะมีอำนาจในการใช้ดุลพินิจอย่างกว้างขวางในการพิจารณาพยานหลักฐานที่คู่ความเสนอ และดุลพินิจของศาลนี้ไม่

สามารถถูกโต้แย้งได้

2.7 งานวิจัยที่เกี่ยวข้อง

งานวิจัยในประเทศ

การศึกษาของ(วิศวจรรยา, 2565)ได้ศึกษาความตระหนักรู้และความเข้าใจในด้านนิติวิทยาศาสตร์ของทนายความไทย โดยผลการศึกษาพบว่าโดยรวมแล้ว ทนายความมีความรู้และความเข้าใจในด้านนิติวิทยาศาสตร์ในระดับปานกลาง การวิเคราะห์ข้อมูลพบว่าคะแนนความรู้และความเข้าใจนั้นแตกต่างกันตามอายุและประสบการณ์การทำงาน แต่ไม่พบความสัมพันธ์ที่ชัดเจนกับเพศ ระดับการศึกษา หรือสถานที่ทำงาน

จากการสัมภาษณ์ ทนายความหลายคนได้แสดงความต้องการที่จะได้รับการฝึกอบรมเพิ่มเติมในด้านนิติวิทยาศาสตร์ โดยเฉพาะในเรื่องของการใช้หลักฐานทางวิทยาศาสตร์ในกระบวนการยุติธรรม ทนายความมีมุมมองที่หลากหลายเกี่ยวกับแนวทางการใช้หลักฐานทางนิติวิทยาศาสตร์ในคดี และบางคนได้แสดงความต้องการที่จะได้รับความรู้เกี่ยวกับหลักฐานทางวิทยาศาสตร์ที่มีความน่าเชื่อถือมากขึ้น

ผลการศึกษายังแสดงให้เห็นว่า การฝึกอบรมในด้านนี้เป็นสิ่งที่ทนายความเห็นว่ามีความสำคัญ และอาจช่วยเสริมสร้างความเชื่อมั่นในการใช้หลักฐานทางวิทยาศาสตร์ในกระบวนการยุติธรรม โดยอาจนำไปสู่การวางแผนขยายโครงการฝึกอบรมในหลักสูตรที่เกี่ยวข้องกับพยานหลักฐานทางนิติวิทยาศาสตร์ในอนาคต.

การศึกษานี้ช่วยให้เห็นถึงความสำคัญของการฝึกอบรมในด้านนิติวิทยาศาสตร์เพื่อให้ทนายความสามารถใช้หลักฐานทางวิทยาศาสตร์ได้อย่างถูกต้องและมีประสิทธิภาพมากขึ้นในการทำงาน

การศึกษาของ(จันธิมา, 2566)ได้ศึกษาปัญหาในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ในคดีอาชญากรรมไซเบอร์ โดยพบว่ามีปัญหาหลัก ๆ ที่ส่งผลกระทบต่อการเก็บรวบรวมพยานหลักฐาน ได้แก่

1.ความยากในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ เนื่องจากพยานหลักฐานอิเล็กทรอนิกส์มักถูกทำลายหรือถูกลบได้อย่างรวดเร็ว ทำให้การเก็บรักษาพยานหลักฐานในรูปแบบดิจิทัลเป็นเรื่องยาก

2.ปัญหาการเข้าถึงข้อมูลที่ถูกจัดเก็บในอุปกรณ์ดิจิทัล เช่น คอมพิวเตอร์หรือโทรศัพท์มือถือที่สามารถควบคุมจากระยะไกลได้ ซึ่งอาจถูกทำลายหรือลบข้อมูลได้ ทำให้เจ้าหน้าที่ตำรวจไม่สามารถเก็บรวบรวมข้อมูลเพื่อขยายผลไปยังองค์กรอาชญากรรมไซเบอร์ได้

ถึงแม้ว่าจะมีการออกกฎหมายสำคัญหลายฉบับที่เกี่ยวข้องกับการปราบปรามอาชญากรรมไซเบอร์ เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และ พระราชกฤษฎีกามาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 แต่กฎหมายเหล่านี้ยังไม่สามารถแก้ไขปัญหาการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ในคดีอาชญากรรมไซเบอร์ได้อย่างมีประสิทธิภาพ

การศึกษานี้ชี้ให้เห็นถึงความท้าทายที่เจ้าหน้าที่ต้องเผชิญในการเก็บรวบรวมพยานหลักฐานในยุคดิจิทัล และยังแสดงให้เห็นว่าแม้กฎหมายจะมีการพัฒนา แต่ก็ยังต้องการการปรับปรุงหรือเพิ่มประสิทธิภาพในการจัดการกับปัญหาดังกล่าวเพื่อให้การรวบรวมพยานหลักฐานในคดีอาชญากรรมไซเบอร์มีประสิทธิภาพยิ่งขึ้น

การศึกษาของ(ทุมเสน, 2566)นำเสนอปัญหาและมาตรการในการสนับสนุนความน่าเชื่อถือของข้อมูลพยานหลักฐานอิเล็กทรอนิกส์ในกระบวนการยุติธรรม โดยมีการกล่าวถึงการใช้เทคโนโลยีสารสนเทศที่เพิ่มขึ้นในสังคม ซึ่งนำไปสู่การเปลี่ยนแปลงในวิธีการเก็บและจัดการข้อมูลจากเอกสารกระดาษเป็นเอกสารอิเล็กทรอนิกส์ การใช้ระบบเครือข่ายอิเล็กทรอนิกส์ในการรับส่งข้อมูล และการสร้างหรือจัดเก็บเอกสารในรูปแบบไฟล์ดิจิทัลทำให้เกิดความสำคัญในการรักษาความน่าเชื่อถือของพยานหลักฐานอิเล็กทรอนิกส์ เนื่องจากพยานหลักฐานอิเล็กทรอนิกส์นั้นแตกต่างจากพยานหลักฐานทั่วไป เนื่องจากมีความเปราะบางสูง สามารถถูกแก้ไขหรือเปลี่ยนแปลงได้ง่าย และไม่ทิ้งร่องรอย

ผลการศึกษายังพบว่ากฎหมายไทยยังมีช่องโหว่ในกระบวนการทางกฎหมายที่เกี่ยวข้องกับพยานหลักฐานอิเล็กทรอนิกส์ ซึ่งยังไม่สามารถปฏิบัติตามมาตรฐานสากลได้อย่างมีประสิทธิภาพ ทำให้เกิดความไม่มั่นใจในกระบวนการยุติธรรม ดังนั้นประเทศไทยควรมีการพัฒนามาตรการที่

สอดคล้องกับมาตรฐานสากลในการรับฟังพยานหลักฐานอิเล็กทรอนิกส์ในกระบวนการยุติธรรม รวมถึงการกำหนดหลักเกณฑ์ที่ชัดเจนในกระบวนการการรับรองความถูกต้องของพยานหลักฐานอิเล็กทรอนิกส์ในคดีอาญา

การศึกษาแนะนำให้มีการแก้ไขและเพิ่มเติม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 เพื่อสร้างมาตรฐานในการตรวจสอบและรับรองความน่าเชื่อถือของพยานหลักฐานอิเล็กทรอนิกส์ ซึ่งจะช่วยให้การดำเนินคดีมีความเป็นธรรม และให้การใช้ดุลยพินิจของผู้พิพากษามีความชัดเจนและเชื่อถือได้

นอกจากนี้ ยังแนะนำให้มีการอบรมผู้พิพากษาในเรื่องของระบบคอมพิวเตอร์และระบบอิเล็กทรอนิกส์ เพื่อให้สามารถพิจารณาคดีเกี่ยวกับพยานหลักฐานอิเล็กทรอนิกส์ได้อย่างมีประสิทธิภาพและเป็นธรรมมากขึ้น

การศึกษาของ(วรธัช, 2566)เกี่ยวกับปัญหาการดำเนินการกับทรัพย์สินตามกฎหมายฟอกเงินโดยใช้พยานหลักฐานทางดิจิทัล พบปัญหาหลักสองประการ ได้แก่

1.ปัญหาที่เกี่ยวข้องกับการดำเนินการกับทรัพย์สินตามกฎหมายฟอกเงินในทางปฏิบัติ ซึ่งหมายถึงความท้าทายในการนำกฎหมายมาใช้ในทางปฏิบัติในการตรวจสอบและตรวจจับการฟอกเงิน โดยเฉพาะในกรณีที่เกี่ยวข้องกับการใช้เทคโนโลยีดิจิทัลในการกระทำความผิด

2.ปัญหาการดำเนินการกับทรัพย์สินในการสอบสวนขยายผลและดำเนินการยึดทรัพย์สิน ซึ่งเป็นปัญหาในการติดตามและยึดทรัพย์สินที่ได้จากการฟอกเงิน โดยใช้ข้อมูลดิจิทัลเป็นหลักฐานในการดำเนินการตามกฎหมาย

ข้อเสนอแนะเพื่อแก้ไขปัญหาในด้านต่างๆ ได้แก่

1.การกำหนดนโยบายและยุทธศาสตร์ที่สอดคล้องกับการป้องกันและปราบปรามการฟอกเงินตามแนวทางของ สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) ซึ่งควรกำหนดทิศทางและแนวทางการดำเนินงานที่ชัดเจนและสอดคล้องกับมาตรฐานสากล

2.การเร่งปรับปรุงระเบียบและกฎหมายตามมาตรการทางการเงินของ FATF (Financial Action Task Force) เพื่อให้การดำเนินงานตามกฎหมายฟอกเงินมีความสอดคล้องกับมาตรฐานระดับสากลในการป้องกันการฟอกเงิน

3.การกำหนดนโยบายในการจัดทำข้อตกลงระหว่างหน่วยงานที่เกี่ยวข้อง เพื่อการรายงานข้อมูลและการจัดทำฐานข้อมูลกลางในการติดตามทรัพย์สินที่ได้จากการฟอกเงิน

4.การกำหนดมาตรฐานในการรับรองพยานหลักฐานทางดิจิทัล โดยใช้แนวทางกฎหมายจากต่างประเทศเพื่อให้พยานหลักฐานทางดิจิทัลสามารถใช้ได้อย่างมีประสิทธิภาพในกระบวนการยุติธรรม

การศึกษานี้เสนอให้มีการพัฒนาระบบและมาตรการที่เหมาะสมในการใช้พยานหลักฐานทางดิจิทัลในการดำเนินคดีฟอกเงิน รวมทั้งการปรับปรุงกฎหมายและระเบียบต่าง ๆ เพื่อให้สามารถต่อสู้กับอาชญากรรมฟอกเงินในยุคดิจิทัลได้อย่างมีประสิทธิภาพ

งานวิจัยต่างประเทศ

การศึกษาของ (Rakha, 2024)เกี่ยวกับ อาชญากรรมทางไซเบอร์และกฎหมาย นำเสนอความท้าทายในการตรวจสอบทางดิจิทัลในการสืบสวนคดีอาญา โดยชี้ให้เห็นถึงปัญหาหลักที่เกิดจาก การขาดมาตรฐานและข้อบังคับในการจัดการหลักฐานดิจิทัล ซึ่งทำให้ไม่สามารถนำหลักฐานเหล่านี้มาใช้ในการพิจารณาคดีของศาลได้อย่างมีประสิทธิภาพ

บทความนี้กล่าวถึงความท้าทายที่เกิดจากการเพิ่มขึ้นของอาชญากรรมทางไซเบอร์ และวิธีการที่ วิทยาศาสตร์ดิจิทัล หรือ ดิจิทัลฟอร์นิกส์ สามารถช่วยในการสืบสวนคดีอาญา โดยอธิบายถึงความสำคัญของการพัฒนากรอบกฎหมายและมาตรฐานการจัดการหลักฐานดิจิทัลที่เหมาะสม ซึ่งต้องมีความร่วมมือระหว่างภาคกฎหมายและเทคโนโลยีเพื่อให้สามารถรับมือกับอาชญากรรมไซเบอร์ได้อย่างมีประสิทธิภาพ

ผลการศึกษายังเน้นถึงความสำคัญของ การพัฒนาแนวทางและกระบวนการมาตรฐาน ในการรวบรวมและประมวลผลหลักฐานดิจิทัล ซึ่งเป็นสิ่งจำเป็นในการสืบสวนคดีอาญาในยุคดิจิทัล และการสร้าง กรอบกฎหมายที่แข็งแกร่ง เพื่อปรับใช้กับการต่อสู้กับอาชญากรรมทางไซเบอร์

ข้อเสนอแนะ จากการศึกษานี้คือการพัฒนากรอบกฎหมายที่สามารถเผชิญหน้ากับอาชญากรรมไซเบอร์ได้อย่างมีประสิทธิภาพ โดยการออกแบบนโยบายที่เหมาะสมและการสร้างมาตรฐานในการจัดการหลักฐานดิจิทัลในกระบวนการทางกฎหมาย ซึ่งจะช่วยให้สามารถใช้หลักฐานดิจิทัลในการพิจารณาคดีได้อย่างมีความน่าเชื่อถือและสามารถสนับสนุนการต่อสู้กับอาชญากรรมทางไซเบอร์ได้อย่างมีประสิทธิภาพ

การศึกษาของ (Miller, 2023)เรื่อง การสำรวจอัยการและผู้สืบสวนโดยใช้หลักฐานดิจิทัล เน้นถึงความสำคัญและความท้าทายในการใช้งานหลักฐานดิจิทัลในการสืบสวนและดำเนินคดีอาญา หลักฐานดิจิทัลมีความจำเป็นต่อการสืบสวนคดี แต่การใช้งานนั้นเต็มไปด้วยความท้าทายต่าง ๆ เช่น การเปลี่ยนแปลงอย่างรวดเร็วของเทคโนโลยี และการสื่อสารเกี่ยวกับการเปลี่ยนแปลงเหล่านี้ที่มักจะไม่สามารถส่งถึงผู้เกี่ยวข้องได้ทันเวลา นอกจากนี้ยังมีปัญหาด้านมุมมองทางสังคมและการเมืองที่อาจส่งผลต่อการรับฟังและการนำหลักฐานมาใช้ในการพิจารณาคดีอย่างเหมาะสม

การสำรวจนี้ได้ทำการสัมภาษณ์อัยการ 50 รายในสหรัฐอเมริกา โดยใช้ข้อมูลจากการสำรวจครั้งที่สองของผู้ตอบแบบสอบถาม 51 ราย ซึ่งมีการสำรวจทั้งปัญหาปัจจุบันและปัญหาในอนาคต ผลการศึกษาพบว่า ปัจจัยที่สำคัญที่ส่งผลต่อการใช้งานหลักฐานดิจิทัลในการสืบสวนและดำเนินคดีอาญา ได้แก่:

1.การฝึกอบรม: อัยการและผู้สืบสวนต้องได้รับการฝึกอบรมที่เหมาะสมในด้านหลักฐานดิจิทัลเพื่อให้สามารถใช้เทคโนโลยีในการสืบสวนได้อย่างมีประสิทธิภาพ

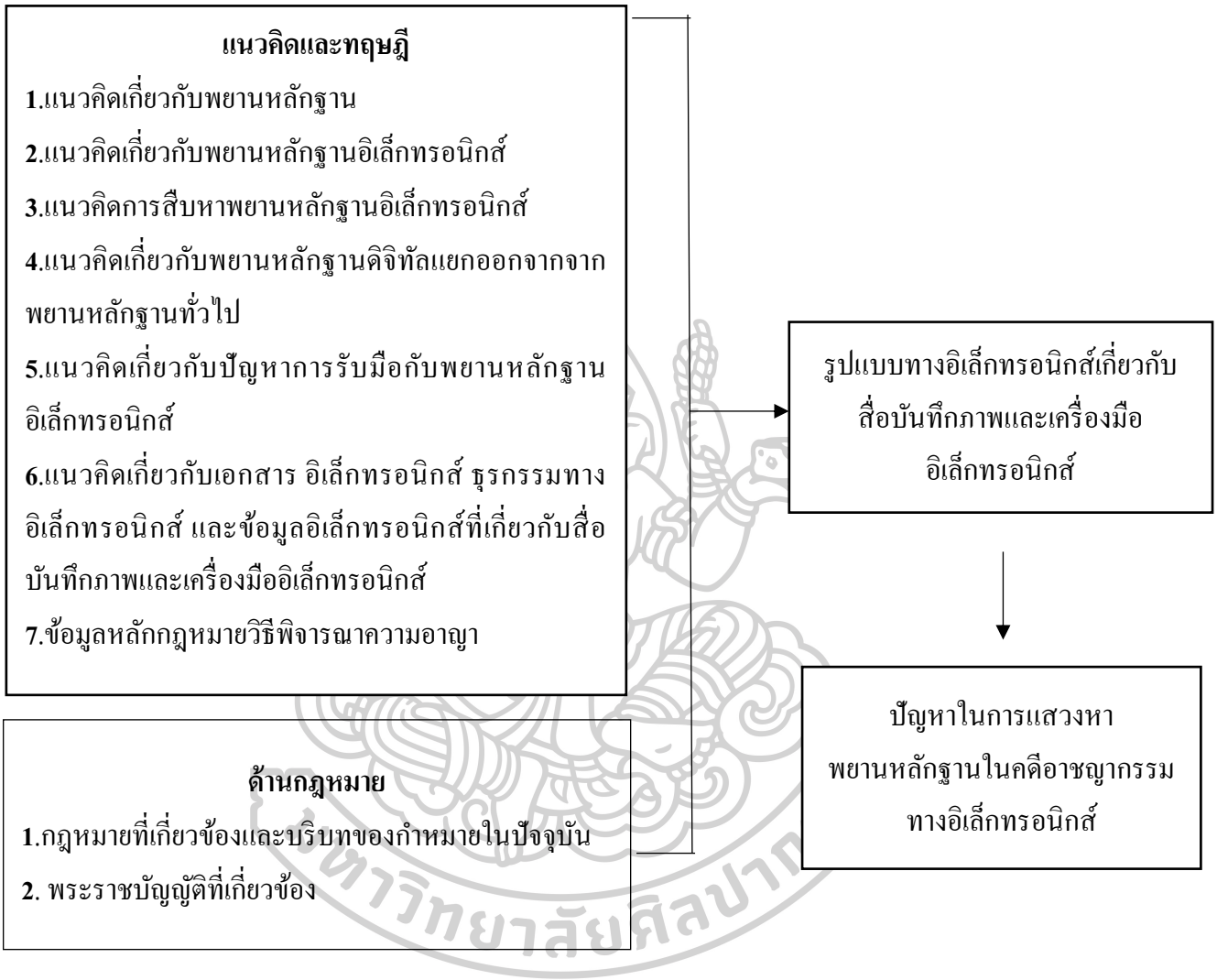
2.ความเชี่ยวชาญ: การมีความเชี่ยวชาญเฉพาะด้านหลักฐานดิจิทัลช่วยให้การสืบสวนและดำเนินคดีอาญามีความถูกต้องและชัดเจน

3.ความสัมพันธ์ระหว่างอัยการและผู้สืบสวน: ความสัมพันธ์ที่ดีและการประสานงานอย่างมีประสิทธิภาพระหว่างอัยการและผู้สืบสวนเป็นปัจจัยที่สำคัญในการใช้หลักฐานดิจิทัลในการดำเนินคดี

ผลการศึกษาเน้นถึงความจำเป็นในการพัฒนาการฝึกอบรมและความร่วมมือระหว่างภาคส่วนต่าง ๆ ในกระบวนการยุติธรรมทางอาญา เพื่อให้สามารถจัดการกับหลักฐานดิจิทัลได้อย่างมีประสิทธิภาพและปลอดภัยในการนำไปใช้ในศาล

2.8 กรอบแนวคิดในการวิจัย

กรอบแนวคิดจากการศึกษาเรื่อง ปัญหาในการแสวงหาพยานหลักฐานในคดีอาชญากรรมทางอิเล็กทรอนิกส์เกี่ยวกับสื่อบันทึกภาพและเครื่องมืออิเล็กทรอนิกส์ ที่ผู้วิจัยได้สรุปจากงานวิจัย เอกสาร และตำราที่เกี่ยวข้องทั้งในประเทศและต่างประเทศ มีดังนี้



ภาพที่2.1 กรอบแนวคิด

ที่มา: ผู้วิจัย

บทที่ 3

วิธีดำเนินการวิจัย

จากการศึกษาคดีอาชญากรรมทางคอมพิวเตอร์ในปัจจุบัน ผู้วิจัยเห็นว่ากระบวนการในการแสวงหาและจัดเก็บพยานหลักฐานทางอิเล็กทรอนิกส์ยังคงประสบปัญหาหลายด้าน โดยเฉพาะในแง่ของข้อจำกัดทางกฎหมายและการปฏิบัติของเจ้าหน้าที่ ซึ่งส่งผลต่อประสิทธิภาพในการดำเนินคดีและการนำตัวผู้กระทำผิดมาลงโทษ ดังนั้น ผู้วิจัยจึงตั้งวัตถุประสงค์ของงานวิจัยฉบับนี้ไว้ 3 ประการคือ

1.เพื่อศึกษาปัญหาทางกฎหมายที่เกี่ยวข้องกับการแสวงหาหลักฐานทางอิเล็กทรอนิกส์ ทั้งในกระบวนการตรวจค้น การยึด และการนำเสนอพยานหลักฐานต่อศาล ซึ่งเป็นขั้นตอนสำคัญในการดำเนินคดีกับผู้กระทำความผิดทางคอมพิวเตอร์และในระบบเครือข่ายอินเทอร์เน็ต

2.เพื่อศึกษามาตรการทางกฎหมายของไทยในขั้นตอนการสืบค้นและรวบรวมพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ โดยเฉพาะข้อมูลประเภทภาพและเครื่องมืออิเล็กทรอนิกส์ เช่น โทรศัพท์มือถือ คอมพิวเตอร์ หรืออุปกรณ์จัดเก็บข้อมูล

3.เพื่อศึกษาทฤษฎีและหลักกฎหมายที่เกี่ยวข้องกับการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ เพื่อให้เข้าใจแนวคิดพื้นฐานที่สนับสนุนการตีความและการใช้กฎหมายในทางปฏิบัติ

ในส่วนของแนวทางการวิจัย ผู้วิจัยเลือกใช้แนวทางการวิจัยเชิงคุณภาพ (Qualitative Research) เพราะมองว่าเป็นวิธีที่เหมาะสมในการทำความเข้าใจเชิงลึกเกี่ยวกับปัญหา ข้อจำกัด และบริบททางกฎหมายที่เกี่ยวข้อง โดยแบ่งกระบวนการออกเป็น 3 ขั้นตอน ได้แก่

ขั้นตอนที่1การศึกษาข้อมูลจากเอกสาร (Documentary Research) เพื่อวิเคราะห์กฎหมายที่เกี่ยวข้อง บทความวิชาการ และแนวปฏิบัติทั้งในและต่างประเทศ

ขั้นตอนที่2การวิจัยเชิงคุณภาพ (Qualitative Research) โดยการสัมภาษณ์ผู้ที่เกี่ยวข้อง เช่น เจ้าหน้าที่ตำรวจ ผู้เชี่ยวชาญด้านนิติวิทยาศาสตร์ดิจิทัล และนักกฎหมาย เพื่อให้ได้ข้อมูลที่สะท้อนประสบการณ์จริง

ขั้นตอนที่3การวิเคราะห์และนำเสนอปัญหา ที่พบจากการแสวงหาและรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ในคดีอาชญากรรมทางคอมพิวเตอร์ เพื่อเสนอแนวทางปรับปรุงหรือพัฒนากฎหมายให้เหมาะสมกับสถานการณ์ปัจจุบัน

3.1 ขั้นตอนที่ 1 การวิจัยเอกสาร (Documentary Research)

ในการดำเนินการวิจัยครั้งนี้ ผู้วิจัยได้ศึกษารวบรวมข้อมูลจากงานวิจัยที่เกี่ยวข้องและบทบัญญัติกฎหมายที่ว่าด้วยอาชญากรรมทางอิเล็กทรอนิกส์ ทั้งนี้เพื่อทำความเข้าใจบริบททางกฎหมายและแนวทางปฏิบัติที่มีอยู่ในปัจจุบัน รวมถึงการศึกษารูปแบบของพยานหลักฐานทางอิเล็กทรอนิกส์ในกรณีศึกษาที่เกี่ยวข้อง โดยเน้นการพิจารณาถึงปัญหาที่มักพบในการจัดเก็บและตรวจสอบพยานหลักฐานอิเล็กทรอนิกส์ โดยเฉพาะข้อมูลประเภทภาพและเครื่องมืออิเล็กทรอนิกส์ เช่น โทรศัพท์มือถือ คอมพิวเตอร์ กล้องวงจรปิด หรืออุปกรณ์จัดเก็บข้อมูลต่าง ๆ

ผู้วิจัยนำข้อมูลที่ได้จากเอกสารและกรณีศึกษาเหล่านี้มาวิเคราะห์ เพื่อทำความเข้าใจถึงช่องว่างของกฎหมายหรือข้อจำกัดในการปฏิบัติที่อาจส่งผลต่อกระบวนการยุติธรรม จากนั้นจึงสรุปผลการวิเคราะห์เพื่อนำไปใช้ในการพัฒนากระบวนการวิจัยในขั้นตอนถัดไป

3.2ขั้นตอนที่2การวิจัยเชิงคุณภาพ(Qualitative Research)

จากการดำเนินการวิจัยเชิงคุณภาพ ผู้วิจัยได้เก็บข้อมูลโดยใช้วิธีการสัมภาษณ์เชิงลึก **(**In-depth Interview) เพื่อให้ได้ข้อมูลเชิงลึกในมิติที่หลากหลายและสะท้อนประสบการณ์จากผู้ที่มีส่วนเกี่ยวข้องโดยตรงกับกระบวนการแสวงหาพยานหลักฐานทางอิเล็กทรอนิกส์ ผู้วิจัยได้คัดเลือกผู้ให้ข้อมูลสำคัญจำนวนทั้งสิ้น ๑ คน จากพื้นที่จังหวัดสมุทรสาคร โดยใช้วิธีการเลือกแบบเจาะจง **(**Purposive Sampling) ซึ่งเป็นการเลือกกลุ่มตัวอย่างที่ผู้วิจัยพิจารณาแล้วว่ามีคุณสมบัติเหมาะสม มีบทบาทและประสบการณ์ตรงที่เกี่ยวข้องกับการดำเนินคดีอาชญากรรมทางคอมพิวเตอร์ และการจัดการกับพยานหลักฐานที่เป็นข้อมูลภาพและเครื่องมืออิเล็กทรอนิกส์

กลุ่มผู้ให้ข้อมูลประกอบด้วย เจ้าหน้าที่ตำรวจ หน่วยงานที่เกี่ยวข้องกับการจัดการพยานหลักฐานในคดีอาชญากรรมทางอิเล็กทรอนิกส์ ผู้พิพากษา อัยการ และทนายความ โดยมีรายละเอียดเกณฑ์การคัดเลือก ดังนี้

1.เจ้าหน้าที่ตำรวจ จากหน่วยงานที่เกี่ยวข้องกับพยานหลักฐานในคดีอาชญากรรมทางอิเล็กทรอนิกส์ ต้องมีประสบการณ์ในการปฏิบัติงานไม่ต่ำกว่า 5 ปี

2.ผู้พิพากษาและอัยการ ต้องเคยพิจารณาคดีอาชญากรรมทางอิเล็กทรอนิกส์มาแล้วไม่ต่ำกว่า 7 ปี

3.ทนายความ ต้องมีประสบการณ์ในการว่าความคดีอาชญากรรมทางอิเล็กทรอนิกส์ไม่น้อยกว่า 7 ปี

การคัดเลือกผู้ให้ข้อมูลตามเกณฑ์ดังกล่าว มีเป้าหมายเพื่อให้ได้ข้อมูลที่ลึกซึ้ง มีความถูกต้อง และครอบคลุมมุมมองจากผู้มีประสบการณ์ตรงในการปฏิบัติงานเกี่ยวกับพยานหลักฐานอิเล็กทรอนิกส์โดยเฉพาะ

เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูล

ในการวิจัยครั้งนี้ ผู้วิจัยเลือกใช้เครื่องมือในการเก็บข้อมูลเป็นแบบสัมภาษณ์แบบมีโครงสร้าง (Structured Interview) ซึ่งผู้วิจัยได้จัดทำขึ้นจากการศึกษาทบทวนแนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง เพื่อให้สอดคล้องกับวัตถุประสงค์ของการวิจัย และสามารถนำไปสู่การเก็บข้อมูลเชิงลึกได้อย่างเป็นระบบ แบบสัมภาษณ์นี้แบ่งออกเป็น 4 ตอนหลัก ดังนี้

ตอนที่ 1: ลักษณะข้อมูลทั่วไปของผู้ให้ข้อมูลในการสัมภาษณ์ เช่น ตำแหน่ง หน่วยงาน ประสบการณ์ในการทำงานที่เกี่ยวข้องกับพยานหลักฐานอิเล็กทรอนิกส์

ตอนที่ 2: ข้อมูลเกี่ยวกับสภาพปัญหาและแนวทางการแก้ไขปัญหาทางกฎหมายในการแสวงหาหลักฐานทางอิเล็กทรอนิกส์ที่ใช้เป็นหลักฐานในกระบวนการพิจารณาคดี ทั้งในขั้นตอนการตรวจค้น การยึด และการนำเสนอพยานหลักฐานในคดีอาชญากรรมทางคอมพิวเตอร์และบนเครือข่ายอินเทอร์เน็ต

ตอนที่ 3: ข้อมูลเกี่ยวกับมาตรการทางกฎหมายของประเทศไทยที่เกี่ยวข้องกับการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ โดยเฉพาะข้อมูลที่เกี่ยวข้องกับภาพและเครื่องมืออิเล็กทรอนิกส์ รวมถึงขั้นตอนและวิธีการดำเนินการตามกฎหมาย

ตอนที่ 4: แนวทางในการแก้ไขปัญหาที่เกี่ยวข้องกับการแสวงหาพยานหลักฐานในคดีอาชญากรรมทางอิเล็กทรอนิกส์ ซึ่งเกี่ยวข้องกับข้อมูลภาพและเครื่องมืออิเล็กทรอนิกส์ โดยเน้นข้อเสนอแนะเชิงนโยบายและแนวทางปฏิบัติที่สามารถนำไปใช้ได้จริง

ผู้วิจัยได้ออกแบบเครื่องมือดังกล่าวโดยคำนึงถึงความชัดเจน ครอบคลุมประเด็นสำคัญ และสามารถนำไปสู่การวิเคราะห์ข้อมูลเชิงลึกที่เป็นประโยชน์ต่อข้อค้นพบของการวิจัย

การสร้างและตรวจสอบคุณภาพเครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูล

เครื่องมือที่ใช้ในการวิจัยในขั้นตอนนี้ คือ แบบสัมภาษณ์แบบมีโครงสร้าง (Structured Interview) ซึ่งผู้วิจัยเป็นผู้สร้างและพัฒนาขึ้นเอง โดยมีกระบวนการในการพัฒนาเครื่องมือดังต่อไปนี้

1.ผู้วิจัยได้ศึกษาทบทวนแนวคิด ทฤษฎี และผลงานวิจัยที่เกี่ยวข้องกับปัญหาในการแสวงหาพยานหลักฐานในคดีอาชญากรรมทางอิเล็กทรอนิกส์ โดยเฉพาะในประเด็นที่เกี่ยวข้องกับข้อมูลภาพและเครื่องมืออิเล็กทรอนิกส์ จากเอกสาร ตำรา วารสารวิชาการ และงานวิจัยต่าง ๆ เพื่อใช้เป็นพื้นฐานในการกำหนดเนื้อหาและกรอบแนวทางของแบบสัมภาษณ์

2.นำข้อมูลจากการศึกษาทบทวนมาประมวลผล เพื่อกำหนดโครงสร้างของแบบสัมภาษณ์ให้สอดคล้องกับขอบเขตของเนื้อหาและวัตถุประสงค์ของการวิจัย

3.สร้างแบบสัมภาษณ์ตามโครงสร้างและขอบเขตของเนื้อหาที่ได้กำหนดไว้ โดยให้ครอบคลุมประเด็นสำคัญตามวัตถุประสงค์ของการวิจัยทั้งในด้านปัญหา มาตรการทางกฎหมาย และแนวทางในการแก้ไข

4.นำแบบสัมภาษณ์ที่ผู้วิจัยสร้างขึ้น เสนอให้อาจารย์ที่ปรึกษาตรวจสอบความตรงเชิงเนื้อหา (Content Validity) ความเหมาะสมของภาษาที่ใช้ ความชัดเจน และความครบถ้วนของคำถาม เพื่อให้เครื่องมือมีความถูกต้องและเหมาะสมสำหรับการเก็บข้อมูล

5.ผู้วิจัยได้นำข้อเสนอแนะที่ได้รับจากอาจารย์ที่ปรึกษามาปรับปรุงแก้ไขแบบสัมภาษณ์ให้สมบูรณ์ยิ่งขึ้น โดยผลการตรวจสอบพบว่า แบบสัมภาษณ์มีความตรงเชิงเนื้อหา และมีความเหมาะสมครบถ้วนทุกข้อ ผู้วิจัยจึงนำแบบสัมภาษณ์ดังกล่าวไปใช้ในการเก็บรวบรวมข้อมูลจากผู้ให้ข้อมูลสำคัญ (Key Informants)

การเก็บรวบรวมข้อมูล

ผู้วิจัยดำเนินการเก็บรวบรวมข้อมูลตามขั้นตอน ดังนี้

1.ผู้วิจัยได้ติดต่อผู้ให้ข้อมูลสำคัญ (Key Informants) ด้วยตนเอง โดยในเบื้องต้นได้แนะนำตนเอง และแจ้งวัตถุประสงค์ของการสัมภาษณ์เชิงลึก (In-depth Interview) ให้แก่ผู้ให้ข้อมูลทราบอย่างชัดเจน เพื่อสร้างความเข้าใจและความร่วมมือในการให้ข้อมูลที่เกี่ยวข้องกับหัวข้อการวิจัย

2.ผู้วิจัยดำเนินการสัมภาษณ์ผู้ให้ข้อมูลสำคัญตามแบบสัมภาษณ์ที่ได้จัดทำขึ้น ซึ่งผ่านการตรวจสอบและปรับปรุงแก้ไขจากอาจารย์ที่ปรึกษาจนอยู่ในระดับที่มีความเหมาะสมและสามารถใช้งานได้จริง โดยระหว่างการสัมภาษณ์ ผู้วิจัยได้จดบันทึกข้อมูลที่ได้รับ พร้อมทั้งบันทึกเสียงการสัมภาษณ์อย่างเป็นระบบ จากนั้นจึงนำข้อมูลทั้งหมดมาจัดเรียบเรียงและสรุปประเด็นต่าง ๆ ให้สอดคล้องกับวัตถุประสงค์ของการวิจัย

การวิเคราะห์ข้อมูล

ในการดำเนินการวิจัยครั้งนี้ ผู้วิจัยได้ดำเนินการเก็บข้อมูลโดยการจดบันทึกประเด็นสำคัญจากการสัมภาษณ์ ซึ่งเป็นขั้นตอนแรกในการแปลข้อมูล หลังจากนั้น ผู้วิจัยได้ทำการวิเคราะห์ข้อมูลด้วยวิธีการที่เรียกว่า การวิเคราะห์เนื้อหา (Content analysis) โดยการอ่านและทำความเข้าใจข้อมูลที่ได้จากการสัมภาษณ์ และกำหนดประเด็นหลักเพื่อจัดหมวดหมู่เรื่องราวและตีความหมายเชื่อมโยงข้อมูลอย่างเป็นระบบ โดยตรวจสอบความหมายและความสมบูรณ์ของข้อมูลในแต่ละด้าน เพื่อให้แน่ใจว่าข้อมูลที่ได้มาเพียงพอและเหมาะสมสำหรับการวิเคราะห์ หากพบว่าข้อมูลยังไม่ชัดเจนหรือไม่ครบถ้วน จะทำการสัมภาษณ์เพิ่มเติมเพื่อให้ข้อมูลสมบูรณ์ยิ่งขึ้น ก่อนนำไปสู่การเรียบเรียงเนื้อหาต่อไป

นอกจากนี้ ผู้วิจัยยังใช้วิธีการ ตรวจสอบความถูกต้อง ด้วยการใช้ การตรวจสอบสามเส้าเพื่อเพิ่มความน่าเชื่อถือและความถูกต้องของข้อมูลที่ได้ โดยประกอบด้วยสองประเภทหลัก ได้แก่

1.การตรวจสอบสามเส้าด้านข้อมูล (Data Triangulation)

การตรวจสอบว่า ข้อมูลที่ได้มานั้นถูกต้องหรือไม่ โดยจะพิจารณาจากแหล่งข้อมูลต่าง ๆ ดังนี้:

แหล่งเวลา: ข้อมูลที่ได้จากช่วงเวลาต่าง ๆ จะต้องมีความสอดคล้องกัน

แหล่งสถานที่: ข้อมูลที่ได้จากสถานที่ต่าง ๆ ต้องไม่ขัดแย้งกัน

แหล่งบุคคล: ข้อมูลจากบุคคลต่าง ๆ ต้องมีความสอดคล้องกันเพื่อยืนยันความถูกต้อง

2.การตรวจสอบสามเส้าด้านวิธีรวบรวมข้อมูล (Methodological Triangulation)

การใช้วิธีการเก็บรวบรวมข้อมูลที่หลากหลาย เช่น การสัมภาษณ์ผู้อื่นร่วมกับการศึกษาจากแหล่งเอกสารต่าง ๆ เพื่อให้ข้อมูลที่ได้มีความหลากหลายและสามารถเปรียบเทียบได้ ทำให้ข้อมูลที่ได้มีความน่าเชื่อถือมากยิ่งขึ้น

3.3 ขั้นตอนที่ 3 นำเสนอปัญหาในการแสวงหาพยานหลักฐานในคดีอาชญากรรมทางอิเล็กทรอนิกส์

การรวบรวมและวิเคราะห์ปัญหาในการแสวงหาพยานหลักฐานในคดีอาชญากรรมทางอิเล็กทรอนิกส์ช่วยให้เห็นถึงข้อจำกัดในกระบวนการปัจจุบัน ซึ่งสามารถชี้ให้เห็นจุดที่ต้องปรับปรุงเพื่อเพิ่มประสิทธิภาพในการดำเนินคดี การนำเสนอข้อมูลให้หน่วยงานที่เกี่ยวข้องจะเป็นโอกาสในการปรับปรุงกระบวนการและมาตรการในการเก็บรวบรวมหลักฐานทางอิเล็กทรอนิกส์

บทที่4

ผลการวิเคราะห์ข้อมูล

ผู้วิจัยได้เลือกศึกษาปัญหาในการแสวงหาพยานหลักฐานในคดีอาชญากรรมทางอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการตรวจสอบบันทึกภาพและเครื่องมืออิเล็กทรอนิกส์ เนื่องจากเล็งเห็นว่าเป็นประเด็นที่มีความสำคัญและท้าทายต่อกระบวนการยุติธรรมในยุคดิจิทัล โดยในการศึกษาครั้งนี้ ผู้วิจัยใช้ระเบียบวิธีวิจัยเชิงคุณภาพ (Qualitative Research) เพื่อให้สามารถเข้าถึงข้อมูลเชิงลึกและเข้าใจปัญหาจากประสบการณ์จริงของผู้ที่เกี่ยวข้องอย่างรอบด้าน

ผู้วิจัยได้ดำเนินการเก็บข้อมูลด้วยการสัมภาษณ์เชิงลึก (In-depth Interview) กับผู้ให้ข้อมูลสำคัญ (Key Informants) จำนวน 9 คน ซึ่งเป็นผู้ที่มีบทบาทหน้าที่เฉพาะและมีประสบการณ์เกี่ยวข้องโดยตรงกับการแสวงหาพยานหลักฐานในคดีอาชญากรรมทางอิเล็กทรอนิกส์ การคัดเลือกผู้ให้ข้อมูลในครั้งนี้ ผู้วิจัยใช้วิธีการเลือกแบบเจาะจง (Purposive Sampling) โดยพิจารณาจากคุณสมบัติและความเกี่ยวข้องของผู้ให้สัมภาษณ์ เพื่อให้ได้ข้อมูลที่มีความหลากหลายและลึกซึ้งตามวัตถุประสงค์ของการวิจัย

ผลการวิเคราะห์ข้อมูลเชิงคุณภาพในครั้งนี้ ผู้วิจัยได้จัดแบ่งเนื้อหาออกเป็น 4 ตอนหลัก เพื่อสะท้อนให้เห็นถึงประเด็นสำคัญที่เกี่ยวข้องกับการแสวงหาพยานหลักฐานในคดีอาชญากรรมทางอิเล็กทรอนิกส์ ดังนี้

ตอนที่ 1 ลักษณะข้อมูลของผู้ให้ข้อมูลในการสัมภาษณ์

ผู้วิจัยนำเสนอข้อมูลพื้นฐานของผู้ให้สัมภาษณ์ ซึ่งเป็นผู้ที่มีบทบาทหน้าที่เกี่ยวข้องกับการแสวงหาพยานหลักฐานในคดีอาชญากรรมทางอิเล็กทรอนิกส์ ทั้งในด้านการบังคับใช้กฎหมาย การสืบสวนสอบสวน และการวิเคราะห์ข้อมูลอิเล็กทรอนิกส์ โดยมุ่งเน้นให้เห็นถึงความหลากหลายของประสบการณ์และมุมมองที่แตกต่างกัน เพื่อสร้างความเข้าใจต่อบริบทของข้อมูลที่ได้รับ

ตอนที่ 2 ข้อมูลเกี่ยวกับสภาพปัญหาและแนวทางการแก้ไขปัญหาในทางกฎหมาย

ในตอนนี้ ผู้วิจัยได้วิเคราะห์ข้อมูลที่เกี่ยวข้องกับสภาพปัญหาและข้อจำกัดทางกฎหมายที่เกิดขึ้นในกระบวนการแสวงหาพยานหลักฐานทางอิเล็กทรอนิกส์ ซึ่งมีความซับซ้อนจากลักษณะเฉพาะของข้อมูลและเทคโนโลยี โดยเฉพาะเมื่อพยานหลักฐานนั้นอยู่บนเครือข่าย

อินเทอร์เน็ตหรือถูกซ่อนอยู่ในระบบคอมพิวเตอร์ ซึ่งเป็นอุปสรรคต่อการดำเนินคดีกับผู้กระทำความผิด

ตอนที่ 3 ลักษณะของมาตรการทางกฎหมายในประเทศไทย

ผู้วิจัยได้วิเคราะห์ถึงมาตรการและกลไกทางกฎหมายที่มีอยู่ในประเทศไทยในการแสวงหาพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ทั้งในแง่ของขั้นตอนทางกฎหมาย วิธีการดำเนินการของเจ้าหน้าที่ผู้มีอำนาจ ตลอดจนข้อจำกัดที่เกี่ยวข้องกับการตรวจสอบบันทึกภาพ และการเข้าถึงเครื่องมืออิเล็กทรอนิกส์ ซึ่งสะท้อนถึงความจำเป็นในการปรับปรุงกระบวนการทางกฎหมายให้สอดคล้องกับสภาพแวดล้อมของอาชญากรรมทางไซเบอร์ที่เปลี่ยนแปลงอย่างรวดเร็ว

ตอนที่ 4 แนวทางการแก้ไขปัญหาในการแสวงหาพยานหลักฐาน

ในตอนสุดท้ายนี้ ผู้วิจัยได้นำเสนอข้อเสนอแนะและแนวทางในการปรับปรุงกระบวนการแสวงหาพยานหลักฐานในคดีอาชญากรรมทางอิเล็กทรอนิกส์ โดยเฉพาะกรณีที่เกี่ยวข้องกับบันทึกภาพและเครื่องมืออิเล็กทรอนิกส์ เพื่อให้กระบวนการเป็นไปอย่างมีประสิทธิภาพ ถูกต้องตามกฎหมาย และสามารถนำไปใช้ในการดำเนินคดีได้จริง

4.1 ผลการวิเคราะห์ข้อมูลเชิงคุณภาพ

จากการวิเคราะห์ข้อมูลเชิงคุณภาพโดยใช้วิธีการสัมภาษณ์เชิงลึกในหัวข้อ “ปัญหาในการแสวงหาพยานหลักฐานในคดีอาชญากรรมทางคอมพิวเตอร์เกี่ยวกับสื่อบันทึกภาพและเครื่องมืออิเล็กทรอนิกส์” ผู้วิจัยได้ดำเนินการสัมภาษณ์ผู้ให้ข้อมูลซึ่งเป็นผู้ที่เกี่ยวข้องกับกระบวนการยุติธรรม ได้แก่ เจ้าหน้าที่ตำรวจในหน่วยงานที่เกี่ยวข้องกับพยานหลักฐานในคดีอาชญากรรมทางอิเล็กทรอนิกส์ ทนายความ ผู้พิพากษา และอัยการ

ในการวิเคราะห์ข้อมูล ผู้วิจัยใช้เทคนิคการวิเคราะห์ข้อมูลเชิงคุณภาพแบบการจำแนกชนิดข้อมูล (Typological Analysis) โดยพิจารณาข้อมูลเชิงลึกที่ได้จากการสัมภาษณ์ตามวัตถุประสงค์ของการวิจัย หลังจากการจำแนกชนิดข้อมูลแล้ว ผู้วิจัยได้ทำการวิเคราะห์เพื่อหาความสม่ำเสมอของข้อมูล และสกัดหาคำสำคัญที่สามารถนำมาใช้ในการวิเคราะห์เนื้อหาอย่างเป็นระบบ

กลุ่มผู้ให้ข้อมูลสำคัญในการวิจัยครั้งนี้แบ่งออกเป็น 3 กลุ่ม ได้แก่

1.เจ้าหน้าที่ตำรวจ เป็นผู้ปฏิบัติงานในหน่วยงานที่เกี่ยวข้องกับพยานหลักฐานในคดีอาชญากรรมทางอิเล็กทรอนิกส์ไม่น้อยกว่า 5 ปี โดยให้ข้อมูลเกี่ยวกับสภาพปัญหาและแนวทางในการแก้ไขปัญหาด้านกฎหมายเกี่ยวกับการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ ซึ่งรวมถึงกระบวนการตรวจค้น การยึด และการนำเสนอพยานหลักฐาน เพื่อใช้ในการดำเนินคดีกับผู้กระทำผิดทางคอมพิวเตอร์และบนเครือข่ายอินเทอร์เน็ต

2.ผู้พิพากษาและอัยการมีประสบการณ์ในการพิจารณาคดีอาชญากรรมทางอิเล็กทรอนิกส์ไม่น้อยกว่า 7 ปี ให้ข้อมูลเกี่ยวกับลักษณะของมาตรการทางกฎหมายไทยที่เกี่ยวข้องกับการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ โดยเฉพาะกระบวนการและขั้นตอนในการรวบรวมพยานหลักฐานตลอดจนข้อมูลที่เกี่ยวข้องกับสื่อบันทึกภาพและเครื่องมืออิเล็กทรอนิกส์

3.ทนายความมีประสบการณ์ในการว่าความคดีอาชญากรรมทางอิเล็กทรอนิกส์ไม่น้อยกว่า 7 ปี ให้ข้อมูลเกี่ยวกับมาตรการทางกฎหมายที่ใช้ในการแสวงหาพยานหลักฐานอิเล็กทรอนิกส์ในกระบวนการยุติธรรม โดยเน้นทั้งในด้านขั้นตอนการดำเนินการและข้อมูลที่เกี่ยวข้องกับสื่อบันทึกภาพและเครื่องมืออิเล็กทรอนิกส์

การวิเคราะห์ข้อมูลจากการสัมภาษณ์เชิงลึกเจ้าหน้าที่ที่เกี่ยวข้องกับการตรวจสอบพยานหลักฐานทางอิเล็กทรอนิกส์

การวิจัยครั้งนี้ได้ดำเนินการเก็บข้อมูลจากการสัมภาษณ์เชิงลึกกลุ่มเจ้าหน้าที่ตำรวจที่มีหน้าที่รับผิดชอบเกี่ยวกับการตรวจสอบและวิเคราะห์พยานหลักฐานในคดีอาชญากรรมทางคอมพิวเตอร์ โดยผู้ให้ข้อมูลหลักคือเจ้าหน้าที่ในตำแหน่งนักวิชาการคอมพิวเตอร์ ประจำกลุ่มตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์ ศูนย์เทคโนโลยีสารสนเทศ ซึ่งเป็นหน่วยงานที่มีบทบาทสำคัญในการรวบรวม วิเคราะห์ และตรวจสอบพยานหลักฐานอิเล็กทรอนิกส์ เพื่อนำไปใช้ประกอบในกระบวนการสอบสวนและดำเนินคดีทางกฎหมาย

จากการสัมภาษณ์เชิงลึกกลุ่มเจ้าหน้าที่ตำรวจซึ่งเป็นผู้ปฏิบัติงานในหน่วยที่เกี่ยวข้องกับพยานหลักฐานในคดีอาชญากรรมทางอิเล็กทรอนิกส์ โดยผู้ให้ข้อมูลดำรงตำแหน่งนักวิชาการคอมพิวเตอร์ ประจำกลุ่มตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์ ศูนย์เทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ ผู้วิจัยได้สรุปประเด็นสำคัญจากการสัมภาษณ์เชิงลึก ดังนี้

ด้านกระบวนการตรวจค้น

จากการสัมภาษณ์และการศึกษาข้อมูลที่ได้จากเจ้าหน้าที่ที่เกี่ยวข้องกับการตรวจพิสูจน์พยานหลักฐานทางอิเล็กทรอนิกส์ ผู้วิจัยเห็นว่าการตรวจพิสูจน์พยานหลักฐานทางอิเล็กทรอนิกส์นั้นไม่เพียงแต่เป็นกระบวนการสืบสวนข้อมูลทางอิเล็กทรอนิกส์เท่านั้น แต่ยังเป็นการค้นหาและระบุข้อมูลที่เกี่ยวข้องกับการสืบสวน ซึ่งสามารถนำมาใช้เป็นหลักฐานในการดำเนินคดีได้อย่างมีประสิทธิภาพ ด้วยเหตุนี้ การตรวจพิสูจน์พยานหลักฐานทางอิเล็กทรอนิกส์จึงต้องการความเข้าใจที่ลึกซึ้งและครอบคลุมถึงอุปกรณ์ต่าง ๆ ที่สามารถเก็บข้อมูลได้ ไม่จำกัดเพียงแค่ข้อมูลในคอมพิวเตอร์ แต่ยังรวมไปถึงโทรศัพท์มือถือ กล้องถ่ายรูป อุปกรณ์จัดเก็บข้อมูล USB และแม้กระทั่งอุปกรณ์อิเล็กทรอนิกส์อื่น ๆ ในชีวิตประจำวันที่อาจเกี่ยวข้องกับการสื่อสารและการเก็บข้อมูลของผู้ต้องสงสัยหรือผู้มีส่วนเกี่ยวข้องในคดี โดยกระบวนการเหล่านี้เป็นสิ่งสำคัญในการพิจารณาการสื่อสารและการเชื่อมโยงข้อมูลจากแหล่งต่าง ๆ ซึ่งจะส่งผลต่อการตัดสินคดีในที่สุด

“ปัญหาในส่วนเจ้าหน้าที่ผู้ปฏิบัติงานขาดทักษะความรู้ด้านเทคนิคคอมพิวเตอร์ ประสบความลำบากในการแกะรอยผู้บุกรุกเข้าสู่ระบบ ปัญหาในการชี้และรวบรวมพยานหลักฐาน และข้อจำกัดด้านกฎหมาย รวมทั้งมาตรการการกำกับดูแลต่าง ๆ ที่ใช้ก็ยังไม่ครอบคลุม ไม่สามารถบังคับใช้ได้อย่างมีประสิทธิภาพ เช่น ตำรวจใช้บรรทัดฐานใดก่อนจะพิจารณารับเป็นคดี การดำเนินการตามขั้นตอนต่าง ๆ ในการจับกุม เป็นต้น” (ข้อมูลจากการสัมภาษณ์ ณ วันที่ 21 กันยายน 2567)

“เจ้าหน้าที่ผู้ปฏิบัติงานด้านการตรวจพิสูจน์พยานหลักฐานทางคอมพิวเตอร์ให้ความสำคัญกับการรักษาสภาพหลักฐานไม่ให้ถูกเปลี่ยนแปลงไปจากเดิม เนื่องจากข้อมูลการเก็บรวบรวมมีหลายขั้นตอน โดยปฏิบัติตามขั้นตอนตามคู่มือปฏิบัติงานที่มีความสอดคล้องกับมาตรฐานการดำเนินงาน” (ข้อมูลจากการสัมภาษณ์ ณ วันที่ 29 กันยายน 2567)

“ในการลงพื้นที่ตรวจค้นจะต้องเข้าถึงแหล่งข้อมูลในอุปกรณ์ต่าง ๆ เช่น โทรศัพท์และคอมพิวเตอร์ โดยจำเป็นต้องใช้รหัสผ่านเพื่อปลดล็อคและเข้าถึงข้อมูลที่อยู่ภายในอุปกรณ์ โดยจะต้องมีความเชี่ยวชาญในการดำเนินการ รวมทั้งมาตรฐานในเรื่องของการครอบครองพยานหลักฐาน เนื่องจากการปฏิบัติตามหลักเกณฑ์และแนวทางที่มีผลต่อความน่าเชื่อถือของผลการวิเคราะห์ข้อมูลของหลักฐาน” (ข้อมูลจากการสัมภาษณ์ ณ วันที่ 10 ตุลาคม 2567)

“เจ้าหน้าที่ที่มีหน้าที่ในการเก็บรวบรวมและวิเคราะห์พยานหลักฐานมีการกระบวนการตรวจค้น โดยการบันทึกขั้นตอนการปฏิบัติงาน การเก็บรวบรวม และการวิเคราะห์พยานหลักฐานอย่างละเอียดตามมาตรฐาน” (ข้อมูลจากการสัมภาษณ์ ณ วันที่ 10 ตุลาคม 2567)

“เจ้าหน้าที่ปฏิบัติการมีการลงพื้นที่เพื่อจัดเก็บพยานหลักฐาน โดยการวางแผน นักตรวจพิสูจน์จะทำการประสานงานกับพนักงานเจ้าหน้าที่ที่รับผิดชอบล่วงหน้าสำหรับการตรวจค้น นอกจากนี้ในกระบวนการตรวจค้นการเก็บรวบรวมวัตถุพยานในสถานที่เกิดเหตุ มีการจำกัดให้เฉพาะบุคคลที่เกี่ยวข้องเข้าไปในพื้นที่ เช่น เจ้าหน้าที่ตำรวจพิสูจน์หลักฐาน เพื่อให้มีการกั้นสถานที่เกิดเหตุตามมาตรฐานหรือแนวทางที่กำหนด เพื่อรักษาความปลอดภัยและความถูกต้องของข้อมูลที่เก็บรวบรวมในกระบวนการนั้น ซึ่งเป็นการปฏิบัติตามมาตรฐานและแนวทางที่ได้รับการกำหนดไว้” (ข้อมูลจากการสัมภาษณ์ ณ วันที่ 19 ตุลาคม 2567)

“ปัญหาการออกหมายค้นโดยศาล หมายค้นของศาลถือเป็นหลักประกันการคุ้มครองสิทธิและเสรีภาพของประชาชนที่ดีที่สุด เพราะกระบวนการยุติธรรมมุ่งเน้นตรวจสอบการใช้อำนาจของเจ้าพนักงานไม่ให้กระทำเกินกว่าความจำเป็น โดยคำนึงถึงศักดิ์ศรีความเป็นมนุษย์ตามบทบัญญัติแห่งรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550 มาตรา 4 โดยบัญญัติว่า ศักดิ์ศรีความเป็นมนุษย์ สิทธิและเสรีภาพของบุคคลย่อมได้รับการคุ้มครอง การค้นตัวบุคคลหรือกระทำใดอันกระทบต่อสิทธิและเสรีภาพตามวรรคหนึ่งจะกระทำมิได้ เว้นแต่มีเหตุตามที่กฎหมายบัญญัติ มาตรา 3269 วรรคสี่ รวมถึงการเข้าไปในเคหสถาน โดยปราศจากความยินยอมของผู้ครอบครอง หรือการตรวจค้นเคหสถานหรือที่รโหฐานจะกระทำมิได้ เว้นแต่มีคำสั่งหมายของศาล หรือมีเหตุอย่างอื่นตามที่กฎหมายบัญญัติ โดยกำหนดให้เฉพาะศาลเท่านั้นที่มีอำนาจออกหมายค้น มาตรา 3370 ในทางปฏิบัติทำให้พนักงานสอบสวนเข้าถึงพยานหลักฐานได้ล่าช้า ทำให้พยานหลักฐานถูกทำลายก่อนที่จะทำการค้น” (ข้อมูลจากการสัมภาษณ์ ณ วันที่ 2 พฤศจิกายน 2567)

“การดำเนินการขอหมายค้นจึงเกิดความล่าช้า การที่รัฐประสงค์จะให้ความคุ้มครองสิทธิส่วนบุคคล จึงสร้างหลักประกันสิทธิของประชาชนด้วยการกำหนดมาตรการตรวจสอบการใช้ดุลพินิจของเจ้าพนักงานโดยองค์กรศาล และในส่วนอำนาจในการออกหมายค้น กำหนดให้ศาลมีอำนาจแต่ผู้เดียว แม้แต่การค้นข้อมูลอิเล็กทรอนิกส์ที่ใช้อุปกรณ์เชื่อมต่อคอมพิวเตอร์เข้าไปค้นหาหลักฐานข้อมูลในเครื่องคอมพิวเตอร์ที่ต้องสงสัยโดยไม่มีการรุกล้ำเข้าไปในทรัพย์สินหรือสถานที่

ส่วนบุคคล ต้องใช้หมายค้นเช่นเดียวกัน เพราะถือว่าการล่วงล้ำเข้าไปในพื้นที่นั้นสงวนไว้เป็นสิทธิส่วนตัว” (ข้อมูลจากการสัมภาษณ์ ณ วันที่ 27 พฤศจิกายน 2567)

จากการสัมภาษณ์เจ้าหน้าที่ผู้ปฏิบัติงานในกระบวนการตรวจค้นพยานหลักฐานทางอิเล็กทรอนิกส์ ผมเห็นว่า การเริ่มต้นกระบวนการตรวจค้นนั้นเป็นสิ่งสำคัญที่ไม่ควรมองข้าม เจ้าหน้าที่จำเป็นต้องตรวจสอบข้อมูลจากแหล่งต่าง ๆ ที่เกี่ยวข้อง อาทิ คอมพิวเตอร์ โทรศัพท์มือถือ หรืออุปกรณ์จัดเก็บข้อมูลอื่น ๆ อย่างละเอียดและครอบคลุม เพราะข้อมูลจากอุปกรณ์หลายประเภทอาจมีความสำคัญในการดำเนินคดี

อีกประเด็นหนึ่งที่สำคัญคือ การรักษาสภาพของพยานหลักฐานทางอิเล็กทรอนิกส์ เจ้าหน้าที่ต้องดำเนินการตามขั้นตอนที่กำหนดไว้ในคู่มือการปฏิบัติงานเพื่อป้องกันไม่ให้ข้อมูลถูกเปลี่ยนแปลงหรือสูญหาย การรักษาความถูกต้องและสมบูรณ์ของข้อมูลจึงเป็นเรื่องที่ไม่สามารถละเลยได้ และไม่เพียงแค่การรักษาสภาพพยานหลักฐานเท่านั้น แต่ยังต้องสามารถเข้าถึงข้อมูลที่เก็บอยู่ในอุปกรณ์ต่าง ๆ ได้อย่างมีประสิทธิภาพ เช่น การปลดล็อกโทรศัพท์มือถือหรือคอมพิวเตอร์ ซึ่งจำเป็นต้องใช้ทักษะและเครื่องมือทางเทคนิคที่เหมาะสม

สุดท้าย เจ้าหน้าที่ต้องมีมาตรฐานในการครอบครองและการเก็บรักษาพยานหลักฐานอย่างเคร่งครัด เพื่อรับประกันว่า ข้อมูลที่เก็บรวบรวมมานั้นยังคงมีความน่าเชื่อถือและสามารถนำไปใช้เป็นหลักฐานในกระบวนการยุติธรรมได้

ด้านกระบวนการยึด

“การยึดโดยรวมของเจ้าหน้าที่มีการเก็บรักษาและยึดพยานหลักฐานที่อยู่ในสภาพจริงมากที่สุด เพื่อความน่าเชื่อถือของพยานหลักฐานในชั้นศาล ถ้าเกี่ยวเนื่องกับการยึดที่เป็นฮาร์ดแวร์ไม่มีปัญหาถ้าทำตามประมวลกฎหมาย” (ข้อมูลจากการสัมภาษณ์ ณ วันที่ 2 พฤศจิกายน 2567)

“แต่ในส่วนใหญ่ปัญหาที่เกิดขึ้นในการหาพยานหลักฐานคือ ความเสียหายจากข้อมูลที่ถูกทำลายโดยสภาพแวดล้อมทางธรรมชาติ ก็ยากที่จะตรวจยึดได้สมบูรณ์ของข้อมูลทั้งหมด” (ข้อมูลจากการสัมภาษณ์ ณ วันที่ 17 พฤศจิกายน 2567)

“การยึดหลักฐานจะมีการทำสำเนาไว้ 2 ฉบับ เพื่อทำการพิสูจน์ หากในกรณีที่ศาลสงสัยว่าข้อมูลที่นำมาเสนอจะไม่ใช่สิ่งเดียวกับที่ยึดมาจากที่เกิดเหตุก็สามารถนำอีกฉบับมาพิสูจน์ได้ กระบวนการประมวลผลจากหลักฐานในการยึดมีการประมวลผลทางคอมพิวเตอร์ว่าข้อมูลที่พิสูจน์

ในศาลมีความถูกต้องเหมือนกับสิ่งที่ยึดจากผู้ต้องสงสัย” (ข้อมูลจากการสัมภาษณ์ ณ วันที่ 17 พฤศจิกายน 2567)

“กระบวนการติดตามจากไอพี (IP Address) นี้เป็นสิ่งที่ต้องใช้เจ้าหน้าที่ที่มีความรู้ความเชี่ยวชาญทางด้านคอมพิวเตอร์เป็นอย่างมาก และยังต้องเป็นเจ้าหน้าที่ที่ได้รับการแต่งตั้งตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (แก้ไขเพิ่มเติม) 2560 ด้วยจึงจะมีอำนาจในการติดตามและรวบรวมพยานหลักฐาน เพราะกระบวนการเก็บรวบรวมและตรวจสอบหลักฐานทางดิจิทัลสามารถนำไปใช้เป็นพยานหลักฐานในชั้นศาลได้ การรวบรวมพยานหลักฐานจึงต้องมีการปฏิบัติตามขั้นตอน และต้องคุ้มครองพยานหลักฐานไว้อย่างดีที่สุด เพื่อป้องกันการปนเปื้อนของพยานหลักฐานนั้น” (ข้อมูลจากการสัมภาษณ์ ณ วันที่ 26 พฤศจิกายน 2567)

ด้านการนำเสนอพยานหลักฐาน

“พนักงานสอบสวนต้องคำนึงถึงกระบวนการค้นและยึดที่ชอบด้วยกฎหมาย เพื่อความน่าเชื่อถือ ต้องมีความรู้ความสามารถในด้านนี้โดยเฉพาะ โดยสถานะของข้อมูลอิเล็กทรอนิกส์ ถ้าจะเสนอพยานวัตถุต้องนำวัตถุไปให้ศาลตรวจสอบ” (ข้อมูลจากการสัมภาษณ์ ณ วันที่ 10 ธันวาคม 2567)

“ลักษณะในการนำเสนอพยานวัตถุในฐานะพยานเอกสาร ต้องวิเคราะห์เรื่องปัญหาต้นฉบับหรือสำเนา ส่วนใหญ่ต้นฉบับที่แท้จริงคือข้อมูลที่เก็บไว้ในฮาร์ดดิสก์ในรูปแบบสัญลักษณ์ตัวเลขในการนำเสนอในแบบ Printouts ที่เป็นสำเนา” (ข้อมูลจากการสัมภาษณ์ ณ วันที่ 19 ธันวาคม 2567)

“แต่ในกฎหมายไทยในคดีอาญาสามารถส่งสำเนาได้ แต่ถ้าในคดีเพ่งที่การนำเสนอพยานเอกสารต้องใช้ต้นฉบับเมื่อต้องนำเสนอในรูปสำเนา จึงต้องมีพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 บัญญัติรองรับในคดีเพ่งไว้ในมาตรา 11 ว่าห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในกระบวนการพิจารณาตามกฎหมายเพียงเพราะเหตุว่าเป็นข้อมูลอิเล็กทรอนิกส์ ในการชั่งน้ำหนักว่าข้อมูลอิเล็กทรอนิกส์จะเชื่อถือได้หรือไม่เพียงใดนั้นให้พิเคราะห์ถึงความน่าเชื่อถือของลักษณะหรือวิธีการที่ใช้สร้าง เก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์ ลักษณะหรือวิธีการเปลี่ยนแปลงของข้อความ ลักษณะหรือวิธีการที่ใช้ในการระบุ

หรือแสดงตัวผู้ส่งข้อมูล รวมทั้งพฤติกรรมที่เกี่ยวข้องทั้งปวง” (ข้อมูลจากการสัมภาษณ์ ณ วันที่ 26 พฤศจิกายน 2567)

“การนำเสนอพยานหลักฐานต้องอาศัยพยานชำนาญการพิเศษให้ความเห็นเกี่ยวกับการเก็บรักษาและกระบวนการประมวลผลของเครื่องคอมพิวเตอร์ เพื่อรับรองความถูกต้องและเป็นสิ่งเดียวที่สามารถตรวจค้นได้ เรียกว่า Integrity การนำเสนอเพื่อการรับรองผู้ที่ประมวลผล คือ Authentication” (ข้อมูลจากการสัมภาษณ์ ณ วันที่ 19 ธันวาคม 2567)

จากการวิเคราะห์ข้อมูลที่ได้รับ ผมคิดว่าในปัจจุบัน การที่กฎหมายวิธีพิจารณาความอาญาให้อำนาจพนักงานสอบสวนในการใช้ดุลพินิจเพื่อรวบรวมพยานหลักฐานทุกประเภท ถือเป็นสิ่งสำคัญในการดำเนินคดีให้สามารถตรวจสอบข้อเท็จจริงได้อย่างครบถ้วน แต่ในกรณีของพยานหลักฐานทางอิเล็กทรอนิกส์ที่อาจถูกแก้ไข ลบ หรือทำลายได้ง่ายนั้น สิ่งที่ทำให้พยานหลักฐานเหล่านี้มีความท้าทาย คือ ต้องการความเชี่ยวชาญและเทคโนโลยีที่เหมาะสมในการรักษาความสมบูรณ์ของข้อมูล

อย่างไรก็ตาม การให้พนักงานสอบสวนมีอำนาจในการรวบรวมหลักฐานอิเล็กทรอนิกส์นั้น ควรต้องมีกรอบกฎหมายที่ชัดเจนและมีมาตรฐานที่เหมาะสม เพราะหากไม่มีการกำหนดขอบเขตที่ชัดเจนในการใช้ดุลพินิจอาจนำไปสู่การละเมิดสิทธิส่วนบุคคล หรือการกระทำที่อาจขัดต่อความเป็นธรรม เช่น การรวบรวมพยานหลักฐานโดยไม่ได้รับอนุญาตจากศาล ซึ่งอาจทำให้กระบวนการยุติธรรมมีความไม่โปร่งใสและสร้างความไม่เชื่อมั่นในกระบวนการสอบสวน

จึงเห็นว่า การกำหนดข้อบังคับหรือเกณฑ์ที่ชัดเจนในการใช้ดุลพินิจของพนักงานสอบสวนในการรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์นั้น เป็นสิ่งที่สำคัญ เพื่อให้กระบวนการยุติธรรมดำเนินไปอย่างถูกต้องและเคารพสิทธิส่วนบุคคลของผู้ที่เกี่ยวข้องทุกฝ่าย

ขั้นตอนในการเก็บรวบรวมพยานหลักฐาน

จากความคิดเห็นที่เสนอเกี่ยวกับการควรกำหนดกฎกระทรวงเพิ่มเติมในประมวลกฎหมายวิธีพิจารณาความอาญาเพื่อการรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์นั้น ผมเห็นว่าเป็นข้อเสนอที่มีความสำคัญอย่างยิ่ง เนื่องจากปัจจุบันการใช้เทคโนโลยีในกระบวนการยุติธรรมกำลังมีบทบาทสำคัญมากขึ้น โดยเฉพาะในคดีที่เกี่ยวข้องกับพยานหลักฐานทางอิเล็กทรอนิกส์ เช่น ข้อมูล

ในคอมพิวเตอร์ หรืออุปกรณ์ดิจิทัลต่างๆ ที่อาจถูกแก้ไขหรือลบได้ง่ายหากไม่มีมาตรการที่ชัดเจนในการเก็บรวบรวมรักษาไว้

ข้อเสนอที่ให้เพิ่มมาตรา 131/2 ในประมวลกฎหมายวิธีพิจารณาความอาญา โดยให้มีการกำหนดเกณฑ์การรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ในกฎกระทรวงนั้น ควรประกอบด้วยการกำหนดวิธีการและขั้นตอนที่ชัดเจนในการเก็บรวบรวม เช่น การใช้เทคโนโลยีที่เหมาะสมในการเก็บรักษาข้อมูลโดยไม่ให้ข้อมูลสูญหายหรือถูกดัดแปลง และควรกำหนดบทบัญญัติที่คุ้มครองสิทธิของบุคคลที่เกี่ยวข้องในกระบวนการนี้ เพื่อป้องกันการละเมิดสิทธิส่วนบุคคล

โดยส่วนที่สำคัญในการดำเนินการเก็บรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ (Golden Rules) นั้น ควรกำหนดหลักการที่เป็นมาตรฐานที่สามารถตรวจสอบได้ เช่น การรักษาความสมบูรณ์ของข้อมูล การเข้าถึงข้อมูลควรเป็นไปตามขั้นตอนที่ได้รับการอนุญาตจากศาล หรือการบันทึกกระบวนการเก็บรวบรวมอย่างละเอียดเพื่อให้สามารถตรวจสอบได้ในภายหลัง ซึ่งจะทำให้กระบวนการยุติธรรมมีความโปร่งใสและเชื่อถือได้มากยิ่งขึ้น

ข้อสรุปการกำหนดกฎกระทรวงเกี่ยวกับวิธีการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์จะช่วยเสริมสร้างความชัดเจนและมาตรฐานในการปฏิบัติงานของพนักงานสอบสวน ทำให้สามารถปกป้องสิทธิของบุคคลได้ดีขึ้นและรักษาความน่าเชื่อถือในกระบวนการยุติธรรม

ในปัจจุบันการนำพยานหลักฐานประเภทภาพและเสียงที่ถูกบันทึกในอุปกรณ์อิเล็กทรอนิกส์มาใช้ในคดีอาญามีความแพร่หลายมากขึ้น และมีการยอมรับจากศาลมากขึ้นเรื่อยๆ แม้ว่าจะมีแนวทางในการบริหารจัดการพยานประเภทนี้ในแต่ละเขตพื้นที่หรือในแต่ละศาลที่แตกต่างกันออกไป ซึ่งการจัดการพยานประเภทนี้อาจส่งผลกระทบต่อกระบวนการยุติธรรม โดยเฉพาะในด้านความตรงตามระยะเวลาที่ศาลกำหนด รวมไปถึงความเป็นธรรมในการพิจารณาคดีที่อาจได้รับผลกระทบจากการตีความและการนำเสนอพยานหลักฐานที่ไม่ตรงตามหลักเกณฑ์ที่กฎหมายกำหนด

ปัญหาที่สำคัญอย่างหนึ่งที่พบคือการตีความพยานหลักฐานประเภทสื่อบันทึกภาพและเสียงในกระบวนการยุติธรรม เพราะจากการพิจารณาประมวลกฎหมายวิธีพิจารณาความแพ่งและประมวลกฎหมายวิธีพิจารณาความอาญา กลับพบว่าไม่มีการกำหนดคำนิยามหรือมาตรการที่ชัดเจนในการใช้พยานประเภทนี้ สิ่งที่สำคัญคือความหมายของภาพและเสียงที่ถูกบันทึกมาเป็น

พยานหลักฐาน ซึ่งต้องสามารถสะท้อนเหตุการณ์ที่เกิดขึ้นได้จริง ดังนั้นการนำสื่อบันทึกภาพและเสียงมาใช้จึงอาจเกิดปัญหาหากไม่ได้มีการกำหนดมาตรการการพิสูจน์ความถูกต้องของพยานหลักฐานนี้อย่างชัดเจน

อีกปัญหาหนึ่งคือการใช้สื่อบันทึกภาพและเสียงเป็นพยานบอกเลา ซึ่งตามกฎหมายไทยจะห้ามการยอมรับพยานบอกเลา ซึ่งทำให้เกิดปัญหาหากเหตุการณ์ที่ถูกบันทึกไว้ในสื่อเหล่านี้เป็นเพียงการรายงานเหตุการณ์ที่เกิดขึ้นโดยบุคคลอื่น และไม่ได้เป็นเหตุการณ์ที่สามารถพิสูจน์ได้จากบุคคลที่เกี่ยวข้องโดยตรง การที่สื่อบันทึกภาพและเสียงถูกมองว่าเป็นพยานบอกเลาจึงทำให้เกิดความยากลำบากในการยอมรับพยานประเภทนี้ในกระบวนการพิจารณาคดี

นอกจากนี้ ปัญหาการจัดทำคำแปลของสื่อบันทึกภาพและเสียงยังเป็นอุปสรรคสำคัญในการใช้พยานหลักฐานประเภทนี้ในคดีอาญา หากผู้เกี่ยวข้องไม่สามารถเข้าใจภาษาที่ปรากฏในสื่อเหล่านั้น กฎหมายกลับไม่ได้มีการกำหนดมาตรการที่ชัดเจนในการจัดทำคำแปล ซึ่งจะทำให้ผู้เสียหายหรือผู้ต้องหาต้องแบกรับภาระค่าใช้จ่ายในการจัดหาผู้แปลเอง โดยไม่สามารถคาดการณ์หรือวางแผนได้อย่างถูกต้อง

จากปัญหาดังกล่าว การปรับปรุงกฎหมายและแนวทางการใช้พยานหลักฐานประเภทสื่อบันทึกภาพและเสียงจึงมีความสำคัญอย่างยิ่ง เพื่อให้กระบวนการพิจารณาคดีมีความเป็นธรรมและมีประสิทธิภาพมากขึ้น ควรกำหนดมาตรการที่ชัดเจนในการนำเสนอและรับฟังพยานหลักฐานประเภทนี้ พร้อมทั้งมีการจัดเตรียมมาตรฐานการใช้พยานประเภทนี้ในกระบวนการยุติธรรม เพื่อให้การพิจารณาคดีสอดคล้องกับหลักการของความเป็นธรรมและความยุติธรรม

"ตามกฎหมายที่เกี่ยวข้อง คือ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ มาตรา 11 ซึ่งกำหนดหลักเกณฑ์ไว้ว่า"

ในส่วนนี้ได้อธิบายถึงการยอมรับข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในกระบวนการพิจารณาคดีตามกฎหมาย ทั้งในคดีแพ่งและคดีอาญา โดยเฉพาะในส่วนของข้อมูลที่ได้จากการสื่อสารผ่านอีเมล ไลน์ หรือเฟซบุ๊ก แมสเซนเจอร์ ซึ่งมีการอธิบายว่า การยอมรับข้อมูลอิเล็กทรอนิกส์เหล่านี้เป็นพยานหลักฐานนั้นไม่จำเป็นต้องนำเครื่องคอมพิวเตอร์ไปประมวลผลข้อมูลเพื่อแสดงต่อศาล แต่สามารถใช้การพิมพ์ออกมาเป็นเอกสารหรือ printout เพื่อเป็นพยานในศาลได้ตามข้อกำหนดในกฎหมาย

ในกระบวนการนำเสนอพยานหลักฐานจากข้อมูลอิเล็กทรอนิกส์นั้น การแสดงความน่าเชื่อถือของข้อมูลเหล่านี้เป็นสิ่งสำคัญ ศาลจะพิจารณาความถูกต้องของข้อมูลโดยดูจากวิธีการเก็บรักษา การไม่สามารถเปลี่ยนแปลงข้อมูลได้หลังจากถูกบันทึก และความสามารถในการระบุตัวผู้ส่งข้อมูล รวมไปถึงพฤติกรรมที่เกี่ยวข้องในการใช้งานข้อมูลนั้นๆ

การนำข้อมูลอิเล็กทรอนิกส์เหล่านี้มาใช้ในศาลต้องมีการสอบถามพยานในประเด็นต่างๆ เช่น การยืนยันตัวตนของผู้ส่งข้อมูล การป้องกันไม่ให้มีการปลอมแปลงข้อมูล และการไม่สามารถแก้ไขข้อมูลเหล่านั้นได้หลังจากการส่งแล้ว นอกจากนี้ยังมีการตรวจสอบว่า printout ที่นำมาใช้เป็นหลักฐานนั้นตรงกับข้อมูลในระบบอิเล็กทรอนิกส์หรือไม่

การใช้ข้อมูลจากสื่ออิเล็กทรอนิกส์เช่นนี้เป็นสิ่งที่มีความสำคัญมากในยุคปัจจุบัน เพราะมันสามารถใช้ในการตัดสินคดีได้อย่างมีประสิทธิภาพ โดยเฉพาะในคดีที่เกี่ยวข้องกับการสื่อสารทางดิจิทัล ซึ่งข้อมูลอิเล็กทรอนิกส์สามารถทำให้การตัดสินคดีมีความถูกต้องและยุติธรรมมากขึ้น โดยไม่จำเป็นต้องพึ่งพาพยานบุคคลเพียงอย่างเดียว

โดยสรุป การยอมรับข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในศาลนั้น เป็นการสร้างความมั่นใจในกระบวนการยุติธรรมให้มีความสมบูรณ์และเป็นไปตามหลักการของความยุติธรรมและความเชื่อถือได้ โดยการใช้ข้อมูลทางอิเล็กทรอนิกส์เพื่อช่วยในการพิสูจน์ความจริงในคดีต่างๆ

ตอนที่ 3 มาตรการในทางกฎหมายของไทยมีลักษณะอย่างไรในการแสวงหาพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ดังขั้นตอนต่อไปนี้

ในการทำวิจัยเกี่ยวกับพยานหลักฐานทางอิเล็กทรอนิกส์ในคดีอาชญากรรมทางคอมพิวเตอร์, ข้าพเจ้าได้ศึกษาและวิเคราะห์ปัญหาต่าง ๆ ที่เกี่ยวข้องกับการใช้เอกสารอิเล็กทรอนิกส์และการรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์ ซึ่งพบว่าแม้ว่าการใช้งานเอกสารอิเล็กทรอนิกส์จะสามารถทดแทนเอกสารกระดาษได้อย่างมีประสิทธิภาพ โดยไม่ต้องพึ่งพากระดาษในการรับส่งหรือจัดเก็บข้อมูล แต่อย่างไรก็ตาม ปัญหาหลักที่พบคือความไม่ชัดเจนในมาตรฐานและการยอมรับสถานะทางกฎหมายของเอกสารอิเล็กทรอนิกส์ ซึ่งส่งผลให้มีความยากลำบากในการนำเอกสารเหล่านี้มาใช้เป็นพยานหลักฐานในกระบวนการยุติธรรม

อีกประการที่ต้องพิจารณาคือ ปัญหาการรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์ โดยเฉพาะข้อมูลที่ถูกจัดเก็บในรูปแบบดิจิทัล ซึ่งมีลักษณะพิเศษ คือ ไม่สามารถมองเห็นได้ด้วยตา

เปล่า และสามารถถูกเปลี่ยนแปลงหรือแก้ไขได้อย่างง่ายดาย ทำให้การเก็บรักษาพยานหลักฐานทางอิเล็กทรอนิกส์ให้คงสภาพเดิมนั้นมีความยากลำบาก อีกทั้งการนำเสนอพยานหลักฐานเหล่านี้ในศาลยังมีความท้าทาย เนื่องจากต้องพิสูจน์ว่าเป็นข้อมูลที่ไม่ได้ถูกแก้ไขหรือเปลี่ยนแปลง ซึ่งเป็นการยืนยันความน่าเชื่อถือของข้อมูล

จากการศึกษากฎหมายที่เกี่ยวข้องในประเทศไทย เช่น พระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ข้าพเจ้าพบว่ากฎหมายเหล่านี้ยังมีช่องว่างในบางประเด็น เช่น การกำหนดมาตรฐานสำหรับการรองรับสถานะทางกฎหมายของเอกสารอิเล็กทรอนิกส์ และการรับฟังพยานหลักฐานทางอิเล็กทรอนิกส์ในกระบวนการพิจารณาคดี ซึ่งอาจทำให้เกิดความไม่ชัดเจนในการดำเนินคดี

นอกจากนี้ ยังพบว่าการฝึกอบรมและพัฒนาความรู้ของบุคลากรในสายงานที่เกี่ยวข้องกับการรวบรวมและตรวจสอบพยานหลักฐานทางอิเล็กทรอนิกส์ยังไม่เพียงพอ ส่งผลให้การดำเนินงานในส่วนนี้ยังไม่เต็มประสิทธิภาพ ข้าพเจ้าจึงเห็นว่า ควรมีการฝึกอบรมและจัดสัมมนาให้กับเจ้าหน้าที่ผู้เกี่ยวข้อง เพื่อให้มีความรู้ความเข้าใจในกฎหมายที่เกี่ยวข้อง และสามารถดำเนินการได้อย่างถูกต้องและมีประสิทธิภาพ

โดยสรุป ปัญหาหลักที่ต้องได้รับการพัฒนาในประเทศไทย คือ การปรับปรุงกฎหมายให้มีความชัดเจนและสามารถรองรับสถานการณ์ในปัจจุบันได้ รวมถึงการพัฒนาบุคลากรในภาครัฐและเอกชนในการดำเนินการกับพยานหลักฐานทางอิเล็กทรอนิกส์อย่างมีประสิทธิภาพ เพื่อให้กระบวนการยุติธรรมในคดีอาชญากรรมทางคอมพิวเตอร์สามารถดำเนินการได้อย่างมีความยุติธรรมและเป็นไปตามกฎหมาย

ขั้นตอนในการแสวงหาพยานหลักฐานทางอิเล็กทรอนิกส์

“ในการดำเนินคดีอาญาที่เกี่ยวข้องกับความผิดซึ่งมีลักษณะสร้างความเสียหายต่อสังคมอย่างรุนแรง หรือมีอัตราโทษจำคุกในระดับสูงนั้น โดยทั่วไปจะกำหนดให้มีการบันทึกภาพและเสียงระหว่างการสอบสวนผู้ต้องหาไว้ในสำนวนการสอบสวน ทั้งนี้เนื่องจากคดีในลักษณะดังกล่าวมักมีรายละเอียดเกี่ยวกับการกระทำความผิดที่ซับซ้อน และจำเป็นต้องมีการแสวงหาพยานหลักฐานในจำนวนมากเพื่อนำมาประกอบการพิสูจน์ข้อเท็จจริงของคดี การสอบสวนผู้กระทำความผิดจึงต้องดำเนินการอย่างละเอียด รอบคอบ และอยู่ภายใต้ขั้นตอนที่ถูกต้องตามกฎหมายอย่างเคร่งครัด

หากกระบวนการใดในขั้นตอนการสอบสวนมีลักษณะไม่ชอบด้วยกฎหมาย อาจส่งผลให้พยานหลักฐานที่ได้มาในส่วนนั้นไม่สามารถนำมาใช้ในการลงโทษผู้กระทำความผิดได้ ดังนั้น การบันทึกภาพและเสียงการสอบสวนจึงเป็นกลไกสำคัญในการป้องกันมิให้เกิดการสอบสวนโดยมิชอบ เป็นการคุ้มครองสิทธิของผู้ต้องหาและเสริมสร้างความน่าเชื่อถือให้กับกระบวนการยุติธรรมทางอาญา โดยถือเป็นส่วนหนึ่งของการส่งเสริมประสิทธิภาพและความโปร่งใสในการบังคับใช้กฎหมาย" (ข้อมูลจากการสัมภาษณ์ วันที่ 8 มกราคม 2568)

"การนำมาตรการบันทึกภาพและเสียงมาใช้กับคดีอาญาที่มีลักษณะเป็นคดีเล็กน้อย อาจก่อให้เกิดผลกระทบในทางลบต่อกระบวนการยุติธรรมทางอาญาอย่างมีนัยสำคัญ เนื่องจากคดีลักษณะดังกล่าวมักมีรายละเอียดของการกระทำความผิดที่ไม่สลับซับซ้อน อีกทั้งยังส่งผลกระทบต่อสังคมในวงจำกัด การกำหนดให้มีการบันทึกภาพและเสียงในทุกคดี รวมถึงคดีที่มีอัตราโทษต่ำอาจเป็นเหตุให้กระบวนการดำเนินคดีเกิดความล่าช้า อันเป็นอุปสรรคต่อการบริหารจัดการกระบวนการยุติธรรมโดยรวมนอกจากนี้ มาตรการดังกล่าวยังอาจก่อให้เกิดภาระเกินสมควรต่อเจ้าหน้าที่รัฐที่เกี่ยวข้อง โดยเฉพาะในด้านการจัดเตรียมสถานที่สอบสวน อุปกรณ์บันทึกภาพและเสียง ตลอดจนกำลังคนและทรัพยากรที่จำเป็นอื่น ๆ หากต้องจัดให้มีการบันทึกภาพและเสียงในทุกคดีโดยไม่คำนึงถึงลักษณะหรือความร้ายแรงของความผิด จะส่งผลให้เจ้าหน้าที่ต้องใช้ทรัพยากรและบุคลากรในระดับเดียวกันทั้งในคดีที่มีความซับซ้อนและคดีทั่วไป ซึ่งย่อมทำให้เกิดภาระงานที่ไม่สมดุล และส่งผลกระทบต่อประสิทธิภาพในการปฏิบัติงานของพนักงานสอบสวน" (ข้อมูลจากการสัมภาษณ์ วันที่ 11 มกราคม 2568)

"การดำเนินการตรวจค้นในคดีอาชญากรรมทางคอมพิวเตอร์มีลักษณะเฉพาะที่แตกต่างจากคดีอาญาทั่วไป เนื่องจากการรวบรวมพยานหลักฐานที่เป็นข้อมูลคอมพิวเตอร์จำเป็นต้องใช้วิธีการเฉพาะทางและเทคนิคพิเศษ โดยเฉพาะในขั้นตอนของการตรวจค้น พนักงานสอบสวนจำเป็นต้องเข้าใจลักษณะของอาชญากรรมทางคอมพิวเตอร์เสียก่อนว่าเกี่ยวข้องกับส่วนประกอบใด เช่น ฮาร์ดแวร์ ซอฟต์แวร์ หรือระบบการสื่อสารโทรคมนาคม ซึ่งแต่ละรูปแบบจะส่งผลต่อแนวทางในการสืบค้นและรวบรวมพยานหลักฐานที่แตกต่างกันดังนั้น การวางแผนในการตรวจค้นจะต้องคำนึงถึงโครงสร้างของระบบเครือข่ายที่เกี่ยวข้อง รวมถึงการจัดเตรียมเครื่องมือและบุคลากรที่มีความเชี่ยวชาญเฉพาะทาง เพื่อให้สามารถเข้าถึงข้อมูลอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการกระทำ

ความผิดได้อย่างถูกต้องและมีประสิทธิภาพสูงสุด” (ข้อมูลจากการสัมภาษณ์ วันที่ 19 มกราคม 2568)

หลักการพื้นฐานในการตรวจพิสูจน์พยานหลักฐานดิจิทัล

1.การรวบรวมพยานหลักฐานดิจิทัล

การรวบรวมพยานหลักฐานดิจิทัลหมายถึงกระบวนการจัดเก็บพยานหลักฐานที่เกี่ยวข้องกับเหตุการณ์ที่เกิดขึ้นในรูปแบบดิจิทัล โดยมุ่งเน้นที่การเก็บรักษาข้อมูลในสภาพที่สมบูรณ์ ไม่ถูกเปลี่ยนแปลง แก้ไข หรือกระทบกระเทือนใด ๆ ทั้งในระหว่างการเก็บรวบรวมและการส่งมอบไปยังหน่วยงานที่เกี่ยวข้อง เพื่อให้มั่นใจได้ว่าพยานหลักฐานที่ได้รับมานั้นสามารถใช้ในการดำเนินคดีได้อย่างถูกต้องและน่าเชื่อถือ

2.การเก็บรักษาพยานหลักฐานดิจิทัล

การเก็บรักษาพยานหลักฐานดิจิทัลต้องเป็นไปตามกระบวนการที่สามารถตรวจสอบย้อนกลับได้ หรือที่เรียกว่า “ห่วงโซ่การครอบครองพยานหลักฐาน (**Chain of Custody)”** ตามมาตรฐานสากล ซึ่งจะต้องมีการบันทึกขั้นตอนการจัดเก็บและควบคุมดูแลพยานหลักฐานไว้อย่างละเอียดถี่ถ้วน เพื่อให้มั่นใจได้ว่าพยานหลักฐานยังคงอยู่ในสภาพเดิมตั้งแต่ได้รับมาจากที่เกิดเหตุจนถึงกระบวนการนำเสนอในชั้นศาล ทั้งนี้ การเก็บรักษาต้องใช้วิธีที่สามารถป้องกันการเข้าถึง การแก้ไข หรือการทำลายข้อมูลโดยมิชอบ

3.การวิเคราะห์พยานหลักฐานดิจิทัล

การวิเคราะห์พยานหลักฐานดิจิทัลขึ้นอยู่กับประเภทของคดี ซึ่งแต่ละประเภทจะมีลักษณะเฉพาะและแนวทางการตรวจสอบที่แตกต่างกัน ทั้งในด้านเครื่องมือ เทคนิค และทักษะของเจ้าหน้าที่ผู้ดำเนินการ การฝึกอบรมและพัฒนาศักยภาพของเจ้าหน้าที่พิสูจน์หลักฐานจึงมีความสำคัญอย่างยิ่ง โดยเฉพาะการใช้ผู้เชี่ยวชาญเฉพาะด้านในการตรวจสอบและวิเคราะห์พยานหลักฐานดิจิทัลอย่างถูกต้อง แม่นยำ และเป็นไปตามหลักวิชาการ

4.การนำเสนอผลการพิสูจน์พยานหลักฐานดิจิทัล

ผลการพิสูจน์พยานหลักฐานดิจิทัลจะถูกจัดทำเป็นรายงานหรือบันทึกคำให้การของผู้เชี่ยวชาญ ซึ่งจะต้องมีการอธิบายรายละเอียดเกี่ยวกับขั้นตอนการตรวจสอบ เครื่องมือที่ใช้ สิ่งที่ตรวจสอบ วิธีการเก็บรักษาพยานหลักฐาน ข้อมูลที่ค้นพบ รวมถึงแนวทางในการยืนยันความแท้จริงของพยานหลักฐาน เพื่อให้ศาลสามารถเข้าใจ และใช้ประกอบการพิจารณาคดีได้อย่างมีประสิทธิภาพ

การค้นพยานหลักฐานอิเล็กทรอนิกส์เป็นมาตรการบังคับที่มีความสำคัญอย่างยิ่งในกระบวนการยุติธรรมทางอาญา โดยเฉพาะในคดีอาชญากรรมทางเทคโนโลยี ซึ่งพยานหลักฐานส่วนใหญ่มักอยู่ในรูปแบบของข้อมูลดิจิทัลที่ไม่สามารถเข้าถึงได้โดยทั่วไป หากไม่มีอำนาจตามกฎหมายรองรับ การค้นจึงถือเป็นเครื่องมือที่จำเป็นในการแสวงหาพยานหลักฐาน ทั้งนี้ หากไม่มีมาตรการดังกล่าว กระบวนการดำเนินคดีอาญาย่อมไม่อาจดำเนินไปได้อย่างมีประสิทธิภาพ

ตามแนวทางของกฎหมายไทย การค้นสามารถกระทำได้โดยเจ้าพนักงานของรัฐเท่านั้น ได้แก่ เจ้าพนักงานฝ่ายปกครอง ตำรวจ หรือพนักงานสอบสวน ซึ่งประชาชนทั่วไปไม่อาจดำเนินการค้นได้ในทุกกรณี การออกหมายค้นต้องเป็นไปตามเหตุที่กฎหมายกำหนดไว้ในมาตรา 69 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา

ผู้วิจัยเห็นว่า การค้นพยานหลักฐานอิเล็กทรอนิกส์ แม้จะเป็นการดำเนินการตามกฎหมาย แต่ก็ย่อมกระทบต่อสิทธิส่วนบุคคล เสรีภาพในเคหสถาน และสิทธิในชีวิตและร่างกายของบุคคล ดังนั้น การดำเนินการจึงต้องอยู่ภายใต้หลักความจำเป็น ความเหมาะสม และการกลั่นกรองของศาลอย่างเคร่งครัด

ในส่วนของข้อมูลอิเล็กทรอนิกส์ที่อาจถูกค้นพบ ผู้วิจัยพิจารณาว่าอาจแบ่งลักษณะการแสวงหาออกเป็น 2 แนวทางหลัก ได้แก่

1.การค้นหาในเครื่องคอมพิวเตอร์ส่วนบุคคลของบุคคลใดบุคคลหนึ่ง กรณีนี้เจ้าพนักงานของรัฐไม่สามารถเข้าถึงข้อมูลที่เก็บอยู่ในฮาร์ดดิสก์ของเครื่องคอมพิวเตอร์นั้นได้ หากไม่ได้เข้าไปในสถานที่ตั้งของเครื่องนั้น ซึ่งโดยทั่วไปมักเป็นเคหสถาน การดำเนินการจึงต้องมีหมายค้นและต้องปฏิบัติตามขั้นตอนของกฎหมายอย่างเคร่งครัด เนื่องจากเกี่ยวข้องกับการบุกรุกเคหสถานของประชาชน

2.การค้นหาข้อมูลจากระบบเครือข่าย เช่น ระบบ LAN ภายในองค์กร ระบบ WAN ของหน่วยงาน หรือระบบอินเทอร์เน็ต ข้อมูลที่ค้นหาในลักษณะนี้อาจถูกจัดเก็บไว้ในเซิร์ฟเวอร์หรืออุปกรณ์เครือข่าย ผู้วิจัยเห็นว่าการเข้าถึงข้อมูลดังกล่าวสามารถใช้เครื่องคอมพิวเตอร์อื่นเชื่อมต่อกับแม่ข่าย **(server)** เพื่อดึงข้อมูลออกมาตรวจสอบได้ ซึ่งการดำเนินการต้องพิจารณาถึงขอบเขตอำนาจและข้อจำกัดทางกฎหมาย เช่น ต้องได้รับอนุญาตจากศาลหากเป็นการเข้าถึงข้อมูลส่วนบุคคล

การกระทำความผิดที่เกิดจากอาชญากรรมทางอิเล็กทรอนิกส์ได้ก่อให้เกิดความท้าทายอย่างมากต่อระบบกฎหมายภายในของแต่ละประเทศทั่วโลก เนื่องจากพยานหลักฐานที่เกี่ยวข้องกับอาชญากรรมประเภทนี้มักอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ ซึ่งมีลักษณะแตกต่างจากพยานหลักฐานทั่วไปอย่างมีนัยสำคัญ

ความแตกต่างดังกล่าวส่งผลให้เกิดปัญหาในหลายด้าน ไม่ว่าจะเป็นขั้นตอนของการค้น การยึด สถานะของข้อมูลอิเล็กทรอนิกส์ในทางพยานหลักฐาน รวมถึงประเด็นเรื่องการรับฟังข้อมูลดังกล่าวเป็นพยานหลักฐานในชั้นศาล ซึ่งในปัจจุบันยังคงต้องอาศัยกรอบของกฎหมายวิธีพิจารณาความอาญาเป็นหลัก ทั้งที่กฎหมายดังกล่าวเดิมถูกออกแบบมาเพื่อใช้กับพยานหลักฐานในลักษณะดั้งเดิม เช่น พยานวัตถุ พยานบุคคล หรือพยานเอกสาร

แม้การกระทำความผิดทางอาญาจะเป็นการกระทำที่มีผลกระทบต่อสังคมโดยรวม แต่กระบวนการดำเนินคดีอาญาก็ย่อมมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลผู้ถูกกล่าวหาอย่างหลีกเลี่ยงไม่ได้ ดังนั้น จึงจำเป็นอย่างยิ่งที่กระบวนการในการแสวงหาความจริงและการดำเนินคดีจะต้องยึดหลักการตามกฎหมายวิธีพิจารณาความอาญา ซึ่งให้ความคุ้มครองสิทธิและเสรีภาพของบุคคลในฐานะที่เขาเป็นส่วนหนึ่งของสังคม

ผู้วิจัยจึงเห็นว่า การปรับปรุงกฎหมายให้สามารถรองรับลักษณะเฉพาะของพยานหลักฐานอิเล็กทรอนิกส์ได้อย่างชัดเจน เป็นสิ่งที่จำเป็นต่อการเพิ่มประสิทธิภาพของกระบวนการยุติธรรมทางอาญา และยังเป็นการคุ้มครองสิทธิขั้นพื้นฐานของประชาชนไม่ให้ถูกลิดรอนโดยไม่มีหลักประกันที่เหมาะสม

ประเทศไทยมีการคุ้มครองสิทธิและเสรีภาพของประชาชนตามที่ระบุไว้ในรัฐธรรมนูญ ซึ่งหมายความว่า รัฐไม่สามารถใช้อำนาจล่วงละเมิดสิทธิของประชาชนได้ ยกเว้นในกรณีที่มีกฎหมาย

อนุญาตให้ทำได้ และเมื่อมีการใช้อำนาจดังกล่าวจะต้องมีกระบวนการควบคุมที่ชัดเจน เพื่อให้สามารถตรวจสอบได้ว่าไม่ได้ละเมิดสิทธิของประชาชน

ในปัจจุบันมีอาชญากรรมใหม่ ๆ ที่ร้ายแรง เช่น อาชญากรรมทางไซเบอร์ ที่ต้องการวิธีการใหม่ในการหาพยานหลักฐาน การใช้อำนาจของเจ้าหน้าที่รัฐในการปราบปรามอาชญากรรมเหล่านี้ยังคงต้องคำนึงถึงสิทธิและเสรีภาพของประชาชนตามที่รัฐธรรมนูญกำหนด

การแสวงหาพยานหลักฐาน เช่น ข้อมูลจากคอมพิวเตอร์หรือเครือข่าย จะต้องมีการควบคุมอย่างโปร่งใส และต้องทำให้เกิดผลกระทบต่อสิทธิของบุคคลน้อยที่สุด เจ้าหน้าที่รัฐต้องทำตามขั้นตอนที่ชัดเจนและสามารถตรวจสอบได้เพื่อให้เกิดความเป็นธรรม

แม้การใช้อำนาจของรัฐจะจำเป็นในการปราบปรามอาชญากรรม แต่ก็ต้องทำในกรอบที่ไม่ละเมิดสิทธิของประชาชน โดยต้องให้ความสำคัญกับหลักการของรัฐธรรมนูญที่คุ้มครองสิทธิและเสรีภาพของบุคคล

พยานหลักฐานที่ศาลจะรับฟังได้ต้องได้มาโดยชอบด้วยกฎหมาย และสามารถพิสูจน์ความผิดหรือความบริสุทธิ์ของผู้ต้องหาได้ พยานหลักฐานอาจเป็นพยานวัตถุ เอกสาร หรือพยานบุคคล แต่ต้องไม่เกิดจากการกระทำที่ผิดกฎหมาย เช่น การใช้วิธีการที่ไม่ถูกต้องในการเก็บพยานหลักฐาน ตามมาตรา 226 ของประมวลกฎหมายวิธีพิจารณาความอาญา

ในกรณีของพยานหลักฐานที่เป็นอุปกรณ์อิเล็กทรอนิกส์ เช่น คอมพิวเตอร์ที่ใช้ในการกระทำผิด เจ้าหน้าที่จะต้องมีหมายค้นในการยึดพยานหลักฐานเหล่านี้ตามกฎหมาย โดยไม่สามารถทำได้โดยไม่มีหมายค้น ยกเว้นในกรณีที่มีเหตุอันสมควรตามมาตรา 69 (2) ซึ่งอนุญาตให้ค้นหาสิ่งของที่เชื่อว่าอาจใช้ในการกระทำความผิดได้

จากการวิเคราะห์พบว่า กฎหมายวิธีพิจารณาความอาญากำหนดให้เจ้าหน้าที่สามารถทำการค้นหาพยานหลักฐานได้เฉพาะในช่วงกลางวัน แต่บริการบนอินเทอร์เน็ตเปิดให้บริการตลอด 24 ชั่วโมง ซึ่งทำให้การกระทำความผิดสามารถเกิดขึ้นได้ตลอดเวลา เช่นเดียวกัน การค้นหาพยานหลักฐานอิเล็กทรอนิกส์ก็มีความซับซ้อน เพราะเจ้าหน้าที่ต้องรอจนกว่าจะถึงเวลาทำการ และยังจำกัดให้เฉพาะเจ้าหน้าที่ฝ่ายปกครองหรือตำรวจเท่านั้นที่มีอำนาจในการค้นหาพยานหลักฐาน แต่ไม่มีช่องทางให้ภาคเอกชนเข้ามาช่วยเหลือได้

ปัญหานี้ยังทำให้การค้นหาพยานหลักฐานทางอิเล็กทรอนิกส์มีความยุ่งยากขึ้น เนื่องจากเจ้าหน้าที่บางคนอาจขาดความรู้และความชำนาญในเรื่องคอมพิวเตอร์ และบางครั้งพนักงานที่ทำการค้นหาอาจกลายเป็นผู้ทำลายพยานหลักฐานโดยไม่ตั้งใจ

ประมวลกฎหมายวิธีพิจารณาความอาญากำหนดให้พนักงานสอบสวนมีอำนาจในการยึดสิ่งของที่พบในการค้นตามหมายค้น เช่น คอมพิวเตอร์ของบุคคล เมื่อพนักงานสอบสวนต้องการข้อมูลภายในคอมพิวเตอร์นั้น พวกเขาต้องดำเนินการอย่างระมัดระวังและคำนึงถึงกระบวนการที่ถูกต้อง เพื่อรักษาข้อมูลให้คงอยู่ในสภาพที่ไม่ได้รับการแก้ไขหรือทำลาย และต้องเก็บรักษาพยานหลักฐานที่เกี่ยวข้องไว้ในสภาพที่สมบูรณ์ที่สุด เพื่อให้การใช้พยานหลักฐานในคดีมีความน่าเชื่อถือและเป็นที่ยอมรับในชั้นศาล

ตอนที่ 4: แนวทางการแก้ไขปัญหาในการแสวงหาพยานหลักฐานในคดีอาชญากรรมทางอิเล็กทรอนิกส์

การแก้ปัญหาของกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลต้องคำนึงถึงหลายปัจจัย โดยเฉพาะการรักษาความถูกต้องและความสมบูรณ์ของข้อมูล ซึ่งปัญหาที่พบมักเกิดจากกระบวนการที่ข้อมูลถูกเปลี่ยนแปลงก่อนจะถึงมือผู้ตรวจพิสูจน์ ดังนั้น การสื่อสารที่เข้าใจตรงกันระหว่างผู้เก็บรวบรวมหลักฐาน ผู้ดำเนินคดี และผู้ตรวจพิสูจน์จึงเป็นเรื่องสำคัญเพื่อไม่ให้เกิดการเปลี่ยนแปลงข้อมูลโดยไม่ตั้งใจ

แนวทางการแก้ไขปัญหานี้ต้องมีการสร้างมาตรฐานที่ชัดเจน โดยคำนึงถึงหลักการรักษาสภาพหลักฐานดิจิทัล และไม่ให้ข้อมูลเกิดการเปลี่ยนแปลงระหว่างกระบวนการตรวจพิสูจน์ รวมถึงการกำหนดมาตรฐานต่างๆ เช่น วิธีการเก็บรวบรวม การส่งมอบ การเขียนรายงาน และอื่นๆ เพื่อให้กระบวนการตรวจพิสูจน์มีความน่าเชื่อถือและสามารถใช้งานได้จริง ไม่เพียงแต่เป็นหลักการหรือทฤษฎี

กระบวนการการจัดการพยานหลักฐานดิจิทัลที่มีประสิทธิภาพต้องผ่าน 4 ขั้นตอนหลัก คือ:

1.การรวบรวมพยานหลักฐาน: ต้องทำตามวิธีการที่ถูกต้อง เพื่อไม่ให้เกิดการเปลี่ยนแปลงในข้อมูล

2.การเก็บรักษา: มีวิธีการเก็บรักษาที่เหมาะสมตามประเภทของพยานหลักฐาน

3.การวิเคราะห์: ต้องมีการวิเคราะห์พยานหลักฐานอย่างละเอียดและมีมาตรฐาน

4.การนำเสนอผลพิสูจน์ในชั้นศาล: การนำเสนอผลการพิสูจน์ต้องมีความชัดเจนและสามารถยอมรับได้ในกระบวนการยุติธรรม

ประเทศไทยยังคงขาดมาตรฐานที่ชัดเจนในการเก็บรวบรวมและพิสูจน์พยานหลักฐานดิจิทัล ซึ่งส่งผลให้กระบวนการตรวจพิสูจน์พยานหลักฐานไม่สามารถเชื่อมโยงกับการพิจารณาคดีตามกฎหมายได้อย่างมีประสิทธิภาพ ในขณะที่หลายประเทศมีหน่วยงานที่รับผิดชอบในการกำหนดมาตรฐานการเก็บรวบรวมและพิสูจน์พยานหลักฐานดิจิทัลอย่างเป็นระบบ

การแก้ไขปัญหานี้จำเป็นต้องให้ความสำคัญกับการพัฒนาทักษะของผู้เชี่ยวชาญที่มีหน้าที่ตรวจพิสูจน์พยานหลักฐานดิจิทัล ซึ่งจะต้องมีทักษะสำคัญดังนี้

1.ทักษะในการเรียนรู้และพัฒนาตนเอง เพื่อให้ทันกับการเปลี่ยนแปลงของเทคโนโลยีและข้อมูลขนาดใหญ่

2.ทักษะด้านการสืบสวน โดยผู้เชี่ยวชาญต้องสามารถทำงานเป็นทีม และตัดสินใจได้ว่าเมื่อใดควรหยุดการสืบค้นข้อมูลหลักฐาน

3.ทักษะการสื่อสารที่ดี เพื่อให้นำเสนอหลักฐานที่อาจซับซ้อนได้อย่างเข้าใจง่าย ทั้งในศาลและกับบุคคลทั่วไป

4.ทักษะด้านเทคนิค ซึ่งรวมถึงความรู้ในด้านคอมพิวเตอร์และการใช้เทคโนโลยีในการสอบสวนคดีอาญา

ในส่วนของกระบวนการสอบสวน ควรมีการบันทึกภาพและเสียงตลอดกระบวนการสอบสวน ตั้งแต่เริ่มต้นจนจบ เพื่อสร้างกลไกในการควบคุมการใช้อำนาจของเจ้าหน้าที่ โดยเฉพาะการป้องกันการกระทำที่ไม่ชอบด้วยกฎหมาย นอกจากนี้ ควรมีการกำหนดบทบัญญัติใน ประมวลกฎหมายวิธีพิจารณาความอาญา เพื่อให้มีการบันทึกภาพและเสียงในคดีที่เหมาะสม พร้อมกำหนดข้อบังคับเกี่ยวกับการเก็บรักษาและการเปิดเผยบันทึกเหล่านี้อย่างชัดเจน เพื่อความโปร่งใสและประสิทธิภาพในกระบวนการยุติธรรมทางอาญา

บทที่ 5

สรุป อภิปรายผล และข้อเสนอแนะ

จากการศึกษาปัญหาในการแสวงหาพยานหลักฐานในคดีอาชญากรรมทางอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการสอบบันทึกภาพและเครื่องมืออิเล็กทรอนิกส์ ข้าพเจ้าได้ตั้งวัตถุประสงค์ของการวิจัยไว้ 3 ประการ ได้แก่

1.เพื่อศึกษาและทำความเข้าใจปัญหาของกฎหมายในการแสวงหาหลักฐานทางอิเล็กทรอนิกส์ที่ใช้เป็นหลักฐานในคดีอาชญากรรมทางคอมพิวเตอร์และในเครือข่ายอินเทอร์เน็ต ซึ่งครอบคลุมถึงกระบวนการตรวจค้น กระบวนการยึด และการนำเสนอพยานหลักฐานในกระบวนการยุติธรรม

2.เพื่อศึกษามาตรการในทางกฎหมายของไทยที่เกี่ยวข้องกับขั้นตอนการแสวงหาพยานหลักฐานทางอิเล็กทรอนิกส์ โดยเฉพาะข้อมูลที่เกี่ยวข้องกับบันทึกภาพและเครื่องมืออิเล็กทรอนิกส์

3.เพื่อศึกษาทฤษฎีที่เกี่ยวข้องกับการรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการสอบบันทึกภาพและเครื่องมืออิเล็กทรอนิกส์ตามกฎหมายของไทย

ในการวิจัยครั้งนี้ ข้าพเจ้าใช้การวิจัยเชิงคุณภาพ (Qualitative Research) โดยใช้วิธีการสัมภาษณ์เชิงลึก (In-depth Interview) เพื่อเก็บข้อมูลจากเจ้าหน้าที่ตำรวจ ผู้พิพากษา ทนายความและอัยการในพื้นที่จังหวัดสมุทรสาคร รวมจำนวนทั้งสิ้น 9 คน ข้าพเจ้าเลือกกลุ่มตัวอย่างตามหลักการเลือกแบบเจาะจง (Purposive Sampling) โดยเลือกบุคคลที่มีบทบาทหน้าที่เฉพาะและมีประสบการณ์ตรงในการแสวงหาพยานหลักฐานในคดีอาชญากรรมทางอิเล็กทรอนิกส์ที่เกี่ยวข้องกับการสอบบันทึกภาพและเครื่องมืออิเล็กทรอนิกส์

จากผลการศึกษา ข้าพเจ้าได้สรุปและอภิปรายผลการศึกษา พร้อมทั้งได้ข้อเสนอแนะที่เป็นประโยชน์ในการพัฒนาการแสวงหาพยานหลักฐานทางอิเล็กทรอนิกส์ในคดีอาชญากรรมทางคอมพิวเตอร์ และการปรับปรุงข้อกฎหมายเพื่อให้สามารถรองรับการใช้งานหลักฐานทางอิเล็กทรอนิกส์ได้อย่างมีประสิทธิภาพยิ่งขึ้นจากการศึกษา สามารถสรุปผล อภิปรายผล และเสนอแนะได้ดังนี้

5.1 สรุปผลการวิจัย

ในกระบวนการแสวงหาหลักฐานทางอิเล็กทรอนิกส์ที่เกี่ยวข้องกับคดีอาชญากรรมทางคอมพิวเตอร์ มีปัญหาหลายประการที่ส่งผลต่อประสิทธิภาพของการเก็บรวบรวมและการนำเสนอหลักฐานในศาล ซึ่งสามารถแบ่งเป็นปัญหาหลัก ๆ ได้ดังนี้:

1.กระบวนการตรวจค้น

การตรวจค้นในคดีอาชญากรรมไซเบอร์มักจะต้องใช้เทคโนโลยีเฉพาะเพื่อเข้าถึงข้อมูลที่เก็บอยู่ในอุปกรณ์ต่าง ๆ เช่น คอมพิวเตอร์ โทรศัพท์มือถือ หรือสื่อดิจิทัลอื่น ๆ ซึ่งมีความท้าทายในการรักษาสภาพของหลักฐานให้สมบูรณ์ โดยเฉพาะเมื่อข้อมูลถูกเก็บอยู่ในรูปแบบที่มีการป้องกัน เช่น การเข้ารหัสหรือรหัสผ่าน ที่ทำให้การเข้าถึงข้อมูลทำได้ยากขึ้น การรักษาความสมบูรณ์ของหลักฐานจึงเป็นสิ่งสำคัญอย่างยิ่ง เพราะหากข้อมูลถูกจัดการไม่ดี อาจทำให้หลักฐานสูญหายหรือมีการเปลี่ยนแปลงได้.

2.การยึดหลักฐาน

การยึดหลักฐานอิเล็กทรอนิกส์ในคดีไซเบอร์ต้องดำเนินการอย่างรอบคอบ เพื่อให้ข้อมูลที่ถูกยึดมามีความน่าเชื่อถือในศาล ซึ่งจะต้องมีการเก็บรวบรวมข้อมูลในสภาพที่ไม่ถูกทำลายหรือเปลี่ยนแปลง เช่น การทำสำเนาไว้หลายชุดเพื่อยืนยันความถูกต้องของข้อมูล และการดำเนินการตามขั้นตอนทางกฎหมายที่เกี่ยวข้อง การยึดข้อมูลที่เก็บอยู่ในฮาร์ดแวร์หรือเซิร์ฟเวอร์ที่สามารถควบคุมจากระยะไกลก็เป็นอุปสรรคใหญ่ เนื่องจากอาจเกิดการลบข้อมูลหรือเปลี่ยนแปลงได้หากไม่ได้รับการจัดการอย่างเหมาะสม.

3.การนำเสนอพยานหลักฐาน

การนำเสนอพยานหลักฐานในรูปแบบเอกสาร เช่น Printouts หรือสำเนาข้อมูลจากอุปกรณ์อิเล็กทรอนิกส์ มักจะมีข้อถกเถียงในเรื่องของความถูกต้องของต้นฉบับ โดยเฉพาะเมื่อหลักฐานเป็นข้อมูลดิจิทัลที่อาจถูกเปลี่ยนแปลงได้ง่าย ดังนั้น การยืนยันความถูกต้องของข้อมูลเหล่านี้จึงเป็นสิ่งจำเป็น ซึ่งในปัจจุบันกฎหมายไทยได้มีการรับรองพยานหลักฐานอิเล็กทรอนิกส์ในศาลตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 แต่ยังคงต้องมีการปรับปรุงกฎหมายและขั้นตอนการนำเสนอหลักฐานเพื่อให้มีความชัดเจนและทันสมัยมากยิ่งขึ้น.

นอกจากนี้ การเข้าถึงข้อมูลในอุปกรณ์ที่สามารถควบคุมจากระยะไกล เช่น โทรศัพท์มือถือหรือคอมพิวเตอร์ที่มีการเก็บข้อมูลในระบบคลาวด์ ยังคงเป็นอุปสรรคสำคัญในการรวบรวมพยานหลักฐาน เนื่องจากอาจมีการลบหรือทำลายข้อมูลได้ง่าย ซึ่งทำให้เจ้าหน้าที่ไม่สามารถเข้าถึงข้อมูลที่จำเป็นสำหรับการขยายผลไปยังองค์กรอาชญากรรมไซเบอร์ได้ แม้จะมีกฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และพระราชกฤษฎีกามาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 แต่กฎหมายเหล่านี้ยังไม่สามารถตอบโจทย์ปัญหาในการรวบรวมหลักฐานอิเล็กทรอนิกส์ในคดีอาชญากรรมไซเบอร์ได้อย่างมีประสิทธิภาพ.

ทั้งหมดนี้สะท้อนให้เห็นถึงความท้าทายในการจัดการหลักฐานอิเล็กทรอนิกส์ในคดีอาชญากรรมไซเบอร์ ซึ่งกฎหมายปัจจุบันยังไม่สามารถตอบสนองปัญหาดังกล่าวได้ครบถ้วน การพัฒนากฎหมายและมาตรการในการเก็บรักษาและนำเสนอพยานหลักฐานในรูปแบบดิจิทัลจึงเป็นสิ่งที่จำเป็นอย่างยิ่งในยุคดิจิทัลนี้

จากการศึกษาเกี่ยวกับมาตรการทางกฎหมายในการแสวงหาพยานหลักฐานที่เป็นข้อมูลดิจิทัล โดยเฉพาะในเรื่องของการสอบปากคำและการบันทึกภาพและเสียง พบว่า ในประเทศไทยยัง

ขาดกฎหมายที่ชัดเจนและระบบการจัดการพยานหลักฐานในรูปแบบดิจิทัล ซึ่งส่งผลต่อความน่าเชื่อถือและประสิทธิภาพในการพิสูจน์คดีอาญา โดยปัญหาหลักที่พบได้แก่

1.การขาดระบบการบันทึกภาพและเสียงในกระบวนการสอบสวน

การใช้เทคโนโลยีในการบันทึกภาพและเสียงในกระบวนการสอบสวนควรจะเป็นมาตรการที่ต้องมีการบังคับใช้ตลอดกระบวนการตั้งแต่ต้นจนจบ เพื่อป้องกันการใช้อำนาจของเจ้าหน้าที่ตำรวจไม่ชอบด้วยกฎหมาย และสร้างความโปร่งใสในการสอบสวน อีกทั้งยังช่วยป้องกันการกระทำที่ไม่เป็นธรรมจากฝ่ายเจ้าหน้าที่ หากการบันทึกภาพและเสียงเป็นมาตรการที่ชัดเจนในกฎหมายจะช่วยให้กระบวนการสอบสวนดำเนินไปอย่างถูกต้องตามหลักกฎหมายและมีความยุติธรรม.

2.การขาดกฎหมายเกี่ยวกับประเภทของพยานหลักฐานดิจิทัล

ขณะนี้ประเทศไทยยังไม่มีการกำหนดประเภทของพยานหลักฐานดิจิทัลอย่างชัดเจน ทำให้เกิดปัญหาความยุ่งยากในการตัดสินใจว่า ข้อมูลที่ได้จากโทรศัพท์มือถือ คอมพิวเตอร์ หรืออุปกรณ์อิเล็กทรอนิกส์อื่น ๆ ควรจะจัดประเภทเป็นพยานหลักฐานในคดีใด ซึ่งทำให้เกิดความไม่แน่ชัดและแตกต่างกันในการตีความข้อมูลจากพยานหลักฐานดิจิทัลในแต่ละคดี นอกจากนี้ยังมีปัญหาเกี่ยวกับการใช้กฎหมายหลายฉบับที่ไม่มีหลักเกณฑ์ในการจัดการและแยกประเภทพยานหลักฐานดิจิทัลอย่างเป็นระบบ

3.ข้อเสนอแนะในการแก้ไขปัญหากฎหมาย

การปรับปรุงและเพิ่มเติมกฎหมายที่เกี่ยวข้อง เช่น ประมวลกฎหมายวิธีพิจารณาความอาญาควรมีการกำหนดประเภทของพยานหลักฐานดิจิทัลอย่างชัดเจน เพื่อให้สามารถนำไปใช้ในกระบวนการพิจารณาคดีได้อย่างมีประสิทธิภาพ โดยควรกำหนดประเภทคดีที่ต้องมีการบันทึกภาพและเสียงตลอดกระบวนการสอบสวน รวมถึงการจัดทำระเบียบและมาตรการเกี่ยวกับการเก็บรักษาและการเปิดเผยข้อมูลเหล่านี้อย่างระมัดระวัง เพื่อลดความเสี่ยงจากการละเมิดสิทธิและเสรีภาพของผู้ต้องหา

การเปรียบเทียบระหว่างระบบกฎหมายของประเทศไทยและต่างประเทศทำให้เห็นว่าประเทศไทยยังขาดความชัดเจนในการจัดการพยานหลักฐานดิจิทัลและไม่ได้กำหนดหลักเกณฑ์ใน

การตรวจยึดพยานหลักฐานดิจิทัลไว้อย่างเหมาะสม ซึ่งอาจทำให้เกิดปัญหาในการแยกแยะและตีความพยานหลักฐานดิจิทัลในกระบวนการพิจารณาคดี

การปรับปรุงกฎหมายและระเบียบการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับการเก็บรักษาและนำเสนอพยานหลักฐานดิจิทัล จึงเป็นสิ่งที่จำเป็นต้องดำเนินการเพื่อให้กระบวนการยุติธรรมในคดีอาญามีความสมบูรณ์และเชื่อถือได้มากยิ่งขึ้น

5.2 อภิปรายผลการวิจัย

ปัญหาทางกฎหมายในการแสวงหาหลักฐานทางอิเล็กทรอนิกส์ที่ใช้ในกระบวนการยุติธรรม

จากการศึกษาพบว่า การแสวงหาหลักฐานทางอิเล็กทรอนิกส์เพื่อใช้ในการดำเนินคดีกับผู้กระทำความผิดทางคอมพิวเตอร์และบนเครือข่ายอินเทอร์เน็ตมีประเด็นปัญหาสำคัญ 3 ประการ ได้แก่

1.กระบวนการตรวจค้น

การตรวจค้นหลักฐานทางอิเล็กทรอนิกส์ต้องเริ่มตั้งแต่การค้นหาข้อมูลอย่างมีระบบ โดยให้ความสำคัญกับการรักษาสภาพของหลักฐานจากแหล่งต่าง ๆ ที่เจ้าหน้าที่พบเจอในขณะปฏิบัติหน้าที่ การดำเนินการควรเป็นไปตามขั้นตอนที่ระบุไว้ในคู่มือการปฏิบัติงาน รวมถึงการเข้าถึงข้อมูลและรหัสผ่านในอุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ เพื่อปลดล็อกและทำสำเนาข้อมูล เจ้าหน้าที่ต้องมีมาตรฐานในการครอบครองหลักฐานอย่างเหมาะสมเพื่อสร้างความน่าเชื่อถือในกระบวนการยุติธรรม

2.การยึดและการจัดเก็บพยานหลักฐาน

การยึดหลักฐานอิเล็กทรอนิกส์ควรอยู่ในสภาพที่ใกล้เคียงกับความเป็นจริงมากที่สุดเพื่อรักษาความน่าเชื่อถือเมื่อนำไปใช้ในชั้นศาล ในกรณีที่ยึดอุปกรณ์ฮาร์ดแวร์ ต้องมีการจัดทำสำเนาหลักฐานไว้ 2 ฉบับ เพื่อใช้ในการพิสูจน์ความถูกต้องในกรณีที่ศาลมีข้อสงสัยว่าหลักฐานที่นำเสนอไม่ตรงกับต้นฉบับที่ยึดมาจากที่เกิดเหตุ การประมวลผลหลักฐานที่ได้จากการยึดต้องมีความถูกต้องและสามารถพิสูจน์ได้ว่าเป็นข้อมูลเดียวกันกับที่ได้จากผู้ต้องสงสัย

3.การนำเสนอพยานหลักฐาน

การนำเสนอพยานวัตถุในฐานะพยานเอกสาร ต้องพิจารณาเรื่องต้นฉบับและสำเนา โดยทั่วไป ต้นฉบับของพยานอิเล็กทรอนิกส์คือข้อมูลที่เก็บอยู่ในฮาร์ดดิสก์ในรูปของสัญลักษณ์ตัวเลข และการนำเสนอในรูปแบบเอกสารมักเป็นสำเนา (printouts) ซึ่งอาจไม่ถือเป็นต้นฉบับในบางกรณี อย่างไรก็ตาม พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาตรา 11 ได้บัญญัติว่า "ห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในกระบวนการพิจารณาตามกฎหมายเพียงเพราะเหตุว่าเป็นข้อมูลอิเล็กทรอนิกส์" การพิจารณาความน่าเชื่อถือของพยานหลักฐานประเภทนี้ต้องพิจารณาลักษณะหรือวิธีการที่ใช้ในการสร้าง เก็บรักษา หรือสื่อสารข้อมูล ตลอดจนการเปลี่ยนแปลงข้อมูล และการระบุหรือแสดงตัวผู้ส่งข้อมูล

ผลการวิจัยของ (ดาวดวง **& Daoduang,** 2021)และ อนุกล จันธิมา (2566) สอดคล้องกัน โดยพบว่า การได้มาซึ่งพยานหลักฐานอิเล็กทรอนิกส์เป็นไปได้โดยยาก เนื่องจากข้อมูลมักถูกทำลายอย่างรวดเร็ว อีกทั้งยังประสบปัญหาในการเข้าถึงข้อมูลที่ถูกจัดเก็บไว้ในอุปกรณ์ที่สามารถควบคุมจากระยะไกล เช่น โทรศัพท์มือถือหรือคอมพิวเตอร์ ซึ่งส่งผลให้เจ้าหน้าที่ไม่สามารถขยายผลไปยังเครือข่ายองค์กรอาชญากรรมไซเบอร์ได้ แม้จะมีกฎหมายสำคัญที่เกี่ยวข้อง อาทิ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 แต่กฎหมายเหล่านี้ยังไม่สามารถแก้ไขปัญหาได้อย่างมีประสิทธิภาพ

นอกจากนี้ งานวิจัยของ (วงศ์ใหญ่, 2557)พบว่า ภาพและเสียงจากกล้องวงจรปิด (CCTV) สามารถใช้เป็นพยานหลักฐานที่มีคุณค่าในการพิสูจน์ข้อเท็จจริงในคดีอาญา แม้จะมีกฎหมายที่รองรับการใช้พยานหลักฐานประเภทนี้แล้ว แต่ก็ยังมีประเด็นที่ควรศึกษาเพิ่มเติม เช่น สถานะของพยานหลักฐานจากกล้องวงจรปิด ปัญหา และอุปสรรคในการนำสืบและรับฟังพยานดังกล่าว เพื่อเพิ่มความน่าเชื่อถือของพยานหลักฐาน การศึกษานี้มีวัตถุประสงค์เพื่อเสนอแนะการแก้ไขกฎหมายให้มีความชัดเจนทั้งในด้านวิธีการนำสืบพยานหลักฐาน การกำหนดหลักเกณฑ์ในการแต่งตั้งผู้เชี่ยวชาญ และบทบาทของหน่วยงานที่เกี่ยวข้อง เพื่อเพิ่มประสิทธิภาพในการพิสูจน์พยานหลักฐานจากกล้องวงจรปิดในอนาคต

ประเทศไทยยังขาดความชัดเจนในกระบวนการทางกฎหมายที่เกี่ยวข้องกับการแสวงหาและนำเสนอพยานหลักฐานอิเล็กทรอนิกส์ โดยเฉพาะอย่างยิ่งในกระบวนการสอบสวนคดีอาญา การนำเทคโนโลยีบันทึกภาพและเสียงมาใช้ในการสอบสวนผู้ต้องหาควรได้รับการกำหนดให้เป็น

มาตรฐานตามกฎหมาย โดยควรมีการบันทึกภาพและเสียงตลอดกระบวนการสอบสวนตั้งแต่เริ่มต้นจนสิ้นสุด และให้ผู้ต้องหามีสิทธิไว้วางใจทนายความหรือบุคคลที่ไว้วางใจเข้าร่วมในการสอบสวนทุกครั้ง เพื่อเป็นกลไกในการตรวจสอบการใช้อำนาจของพนักงานสอบสวน

ทั้งนี้ ควรมีการบัญญัติในประมวลกฎหมายวิธีพิจารณาความอาญาเพิ่มเติมให้ชัดเจนถึงประเภทของคดีที่จำเป็นต้องมีการบันทึกภาพและเสียง รวมถึงหลักเกณฑ์ ข้อยกเว้นในกรณีเร่งด่วน เพื่อป้องกันมิให้กระบวนการยุติธรรมต้องชะงัก นอกจากนี้ควรมีการกำหนดระเบียบว่าด้วยการจัดเก็บ รักษา และการเปิดเผยบันทึกภาพและเสียงดังกล่าวอย่างรัดกุม เพื่อให้การใช้เทคโนโลยีดังกล่าวสามารถตอบสนองต่อการแก้ไขปัญหาการสอบสวนที่มิชอบด้วยกฎหมายได้อย่างมีประสิทธิภาพ

ข้อเสนอแนวทางนี้สอดคล้องกับผลการวิจัยของ (ใจซื่อ, 2021)ซึ่งชี้ให้เห็นว่าระบบกฎหมายของประเทศไทยยังไม่ได้กำหนด “พยานหลักฐานดิจิทัล” ให้เป็นประเภทพยานหลักฐานแยกเฉพาะจากพยานหลักฐานประเภทอื่น ทำให้เกิดปัญหาในการตีความว่าพยานหลักฐานดิจิทัลนั้นอยู่ในประเภทใด และมีผลต่อการนำเสนอในแต่ละคดี นอกจากนี้ แม้จะมีบทบัญญัติเกี่ยวกับการตรวจยึดพยานหลักฐานดิจิทัลอยู่ในกฎหมายหลายฉบับ แต่ยังขาดหลักเกณฑ์ที่ชัดเจนเกี่ยวกับลักษณะของข้อมูลและการจำแนกประเภทพยานหลักฐาน

ปัญหานี้ยังขยายไปถึงพยานหลักฐานที่บันทึกไว้ในอุปกรณ์อิเล็กทรอนิกส์ เช่น โทรศัพท์มือถือและคอมพิวเตอร์ ที่ยังไม่มีหลักเกณฑ์ทางกฎหมายในการจำแนกประเภทของข้อมูล จึงเกิดความแตกต่างในการตีความและการนำเสนอพยานหลักฐานในคดีต่าง ๆ โดยอาศัยวัตถุประสงค์ของแต่ละฝ่าย อาจทำให้เกิดการคัดค้านในกระบวนการพิจารณาคดี และความไม่แน่นอนทางกฎหมาย

ดังนั้น จึงมีข้อเสนอแนะให้ปรับปรุงแก้ไขประมวลกฎหมายวิธีพิจารณาความอาญาให้มีความชัดเจนมากยิ่งขึ้นเกี่ยวกับประเภทพยานหลักฐานดิจิทัล การกำหนดหลักเกณฑ์ที่เหมาะสมในการจัดการและนำเสนอพยานหลักฐานดังกล่าว เพื่อประโยชน์ในการอำนวยความยุติธรรมอย่างมีประสิทธิภาพ

5.3 ข้อเสนอแนะการวิจัย

ข้อเสนอแนะเพื่อการนำผลการวิจัยไปใช้

1การบัญญัติในประมวลกฎหมายวิธีพิจารณาความอาญาในการรวบรวมพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ควรจะมีการบัญญัติไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา เพื่อให้กระบวนการรวบรวมพยานหลักฐานที่เป็นข้อมูลดิจิทัลมีความชัดเจนและมีประสิทธิภาพมากขึ้น โดยอาจจะมีข้อกำหนดเกี่ยวกับการใช้พยานหลักฐานดิจิทัลในคดีอาญาเฉพาะกรณี เช่น การจัดประเภทพยานหลักฐานดิจิทัลและข้อกำหนดการตรวจสอบในกรณีที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์ เพื่อป้องกันการใช้พยานหลักฐานที่ไม่ชอบด้วยกฎหมาย และควรให้อำนาจเจ้าหน้าที่ที่ปฏิบัติงานตามพระราชบัญญัติคอมพิวเตอร์ พ.ศ. 2550 มีอำนาจในการตรวจสอบและรวบรวมข้อมูลในกรณีที่มีเหตุสงสัยว่าจะมีการกระทำความผิด การมีหลักการพิเศษและแนวทางการปฏิบัติจะทำให้กระบวนการดำเนินคดีมีประสิทธิภาพมากยิ่งขึ้น

2.อำนาจในการตรวจสอบข้อมูลอิเล็กทรอนิกส์เนื่องจากอาชญากรรมทางอิเล็กทรอนิกส์สามารถลบหรือเปลี่ยนแปลงข้อมูลได้อย่างรวดเร็วและง่ายดาย การให้เจ้าหน้าที่ตำรวจหรือเจ้าหน้าที่สอบสวนมีอำนาจในการตรวจสอบข้อมูลคอมพิวเตอร์ตลอด 24 ชั่วโมงจึงเป็นสิ่งที่จำเป็นเพื่อให้สามารถรวบรวมพยานหลักฐานได้ทันท่วงทีและไม่ให้เกิดการเปลี่ยนแปลงข้อมูลได้ง่าย นอกจากนี้ ยังควรกำหนดกรอบเวลาในการรวบรวมข้อมูลอย่างชัดเจน เพื่อป้องกันไม่ให้พยานหลักฐานถูกทำลายหรือถูกลบไป ซึ่งจะทำให้กระบวนการพิจารณาคดีมีความโปร่งใสและยุติธรรมมากยิ่งขึ้น

3.การฝึกอบรมบุคลากรและการพัฒนากระบวนการเก็บรวบรวมพยานหลักฐานขั้นตอนการเก็บรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์มีความสำคัญอย่างยิ่ง เพราะข้อมูลดิจิทัลสามารถเปลี่ยนแปลงได้โดยไม่ตั้งใจหรือจากการกระทำผิดของบุคคลที่เกี่ยวข้อง การฝึกอบรมบุคลากรให้มีความรู้และความเข้าใจในวิธีการรวบรวมพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์จึงมีความสำคัญมาก โดยหน่วยงานภาครัฐต้องให้ความสำคัญในการพัฒนาทักษะและความสามารถของเจ้าหน้าที่ในการทำงานด้านนี้ รวมถึงการปรับปรุงและพัฒนาแนวทางการปฏิบัติให้สอดคล้องกับกฎหมายอาชญากรรมทางอิเล็กทรอนิกส์ เพื่อให้กระบวนการรวบรวมข้อมูลมีความรัดกุมและยุติธรรมมากยิ่งขึ้น

การพัฒนากฎหมายและกระบวนการทางกฎหมายให้สอดคล้องกับเทคโนโลยีที่เปลี่ยนแปลงไปเป็นสิ่งที่จำเป็นมาก เพื่อให้ประเทศไทยสามารถจัดการกับอาชญากรรมทางอิเล็กทรอนิกส์ได้อย่างมีประสิทธิภาพและยุติธรรม

รายการอ้างอิง

Hobson, C. B. (1992). *Fire investigation: a new concept*. CC Thomas.

Miller, C. M. (2023). A survey of prosecutors and investigators using digital evidence: A starting point. *Forensic Science International: Synergy*, *6*, 100296. https://doi.org/https://doi.org/10.1016/j.fsisyn.2022.100296

Rakha, N. A. (2024). Cybercrime and the law: Addressing the challenges of digital forensics in criminal investigations. *Mexican Law Review*, *16*(2), 2.

ใจซื่อ, ณ. (2021). มาตรการทางกฎหมายเกี่ยวกับการรับฟังพยานหลักฐานดิจิทัล. วารสารมหาวิทยาลัยราชภัฏมหาสารคาม, *15*(1), 109-121. **https://so05.tci-thaijo.org/index.php/rmuj/article/view/250839**

คณิต. (2546). ระบบไต่สวนตามกฎหมายว่าด้วยวิธีพิจารณาคดี ทุจริตและประพฤติมิชอบ. วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, *46*(2).

จันทรมัสการ, ป. ค. ส. (2563). การจัดการความรู้งานสืบสวนที่เป็น BestPractice ของสุดยอดนักสืบยุค. 4.0. วารสารศิลปะการจัดการ, *4*(2).

จันธิมา, อ. (2566). ปัญหาในการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ในคดีอาชญากรรมไซเบอร์ กลุ่มวิชากฎหมายอาญาและกระบวนการยุติธรรมทางอาญา, นิติศาสตร์ มหาวิทยาลัยศรีปทุม].

ชุติวงศ์, เ. (2552). กฎหมายลักษณะพยานหลักฐาน รวมคำบรรยายภาคสอง เล่ม 4 สมัยที่ 62 ปีการศึกษา 2552. กรุงเทพมหานคร : สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา.

ดาวดวง, ว. (2021). ปัญหาการรวบรวมพยานหลักฐานเพื่อดำเนินคดีอาชญากรรมไซเบอร์. มหาวิทยาลัยธรรมศาสตร์.

ทรรศนกุลพันธ์, ส. ส. ท. (2562). พิศวาสอาชญากรรมกับการบริหารอาชญากรรมหลอกลวงของรัฐสมัยใหม่ *CMU Journal of Law and Social Sciences*, *1*(13), 57-77.

ทุมเสน, ก. (2566). มาตรการสนับสนุนความน่าเชื่อถือข้อมูล พยานหลักฐานอิเล็กทรอนิกส์ในกระบวนการยุติธรรม วิทยานิพนธ์ หลักสูตรปริญญานิติศาสตร์มหาบัณฑิต, มหาวิทยาลัยพะเยา].

วงศ์ใหญ่, ต. (2557). แนวทางกฎหมายในการสร้างกลไก องค์กร และกระบวนการในการแสวงหาพยานหลักฐานใหม่ ตามพระราชบัญญัติการรื้อฟื้นคดีอาญา พ.ศ.2526 นิติศาสตรมหาบัณฑิต สาขาวิชากฎหมายอาญาและกระบวนการยุติธรรม มหาวิทยาลัยแม่ฟ้าหลวง].

วรธัช, ธ. (2566). บทวิเคราะห์ปัญหา และข้อเสนอแนะที่เกี่ยวข้อง กับการดำเนินการกับทรัพย์สินตามกฎหมายฟอกเงินโดยใช้พยานหลักฐานทางดิจิทัล. วารสารวิชาการอาชญาวิทยา และนิติวิทยาศาสตร์, *9*(1), 203-214.

วิศวจรรยา, ว. (2565). ความตระหนักรู้และความเข้าใจในพยานหลักฐานทางนิติวิทยาศาสตร์ของทนายความไทย. ปรัชญาดุษฎีบัณฑิต สาขาวิชานิติวิทยาศาสตร์และงานยุติธรรม มหาวิทยาลัยศิลปากร.

ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์.(2561). ข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์ พยานหลักฐาน.

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2559). ข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์ พยานหลักฐาน. ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์.

สืบพงษ์ศิริ, ส. (2546). ความรู้และความคิดเห็นของเจ้าหน้าที่บรรเทาสาธารณภัย มูลนิธิป่อเต็กตึ๊งต่อการป้องกัน รักษาวัตถุพยานในสถานที่เกิดเหตุ (วิทยานิพนธ์ปริญญามหาบัณฑิต วิชาอาชญาวิทยาและงานยุติธรรม) คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย.].

สุขวัจน์, ส. (2550). การพิสูจน์หลักฐาน โรงเรียนนายร้อยตำรวจ.

สุขาบูรณ์, ก. (2560). การรับฟังพยานหลักฐานทางนิติวิทยาศาสตร์กรณีรอยฝ่าเท้าที่ไม่ปรากฏรอยลายเส้น มหาวิทยาลัยสุโขทัยธรรมาธิราช].

ภาคผนวก ก

เครื่องมือที่ใช้ในการวิจัย

แบบสัมภาษณ์การวิจัย

เรื่อง ปัญหาในการแสวงหาพยานหลักฐานในคดีอาชญากรรมทางอิเล็กทรอนิกส์เกี่ยวกับสื่อบันทึกภาพและเครื่องมืออิเล็กทรอนิกส์

<u>คำชี้แจง</u>

1.แบบสัมภาษณ์ชุดนี้เป็นการเก็บข้อมูลประกอบการทำวิทยานิพนธ์ ของนักศึกษาหลักสูตร วิทยาศาสตร์มหาบัณฑิต สาขาวิชานิติวิทยาศาสตร์ มหาวิทยาลัยศิลปากร มีวัตถุประสงค์เพื่อศึกษาปัญหาของกฎหมายการในการแสวงหาหลักฐานทางอิเล็กทรอนิกส์ที่ใช้เป็นหลักฐานทางคดีโดยกระบวนการตรวจค้น กระบวนการยึด และนำเสนอพยานหลักฐานเพื่อดำเนินคดีกับผู้กระทำผิดทางคอมพิวเตอร์และบนเครือข่ายอินเตอร์เน็ต และเพื่อศึกษามาตรการในทางกฎหมายของไทยที่เกี่ยวกับวิธีการขั้นตอนในการแสวงหาพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์เกี่ยวกับสื่อบันทึกภาพและเครื่องมืออิเล็กทรอนิกส์

2. คำตอบของผู้ตอบแบบสัมภาษณ์ถือเป็นข้อมูลที่สำคัญอย่างยิ่งซึ่งผู้วิจัยรับรองว่าคำตอบของท่านจะไม่มีผลกระทบต่อการปฏิบัติงานของท่าน

3. หากท่านไม่ประสงค์ที่จะตอบคำถาม ท่านสามารถปฏิเสธไม่ตอบได้ตามความประสงค์ แต่ หากท่านพิจารณาแล้วยินดีจะตอบ ผู้วิจัยใคร่ขอความกรุณาท่านให้ข้อมูลตามความเป็นจริงให้ครบทุกข้อเพื่อผลประโยชน์ทางวิชาการ

4. แบบสัมภาษณ์ทุกฉบับผู้วิจัยจะปกปิดเป็นความลับโดยไม่มีการอ้างถึงตัวบุคคล

5. ผู้วิจัยขอขอบพระคุณผู้ตอบแบบสัมภาษณ์ทุกท่านที่ให้ความร่วมมือด้วยดีและเสียสละเวลาในครั้งนี้

ภัทรดิษย์ วรประดิษฐ์
นักศึกษาปริญญาโท หลักสูตรวิทยาศาสตร์มหาบัณฑิต
สาขาวิชานิติวิทยาศาสตร์ มหาวิทยาลัยศิลปากร

ตอนที่ 1 **ข้อมูลทั่วไปของผู้ให้สัมภาษณ์**

ชื่อ– นามสกุล……

ตำแหน่ง.....หน่วยงาน.....

อายุราชการ ..... ปีประสบการณ์ในการทำงานในตำแหน่งปัจจุบัน……ปี

วุฒิการศึกษา .....

เบอร์ติดต่อ .....E-mail …….....

ตอนที่ **2** สภาพปัญหาและแนวทางแก้ไขปัญหาของกฎหมายการในการแสวงหาหลักฐานทางอิเล็กทรอนิกส์ที่ใช้เป็นหลักฐานทางคดีเป็นอย่างไร เพื่อดำเนินคดีกับผู้กระทำผิดทางคอมพิวเตอร์และบนเครือข่ายอินเตอร์เน็ต ดังกระบวนการต่อไปนี้

2.1 ด้านกระบวนการตรวจค้น

สภาพปัญหา

……

……

แนวทางแก้ปัญหา

……

……

2.2 ด้านกระบวนการยึด

สภาพปัญหา

……

……

แนวทางแก้ปัญหา

……

……

2.3 ด้านการนำเสนอพยานหลักฐาน เพื่อดำเนินคดีกับผู้กระทำผิดทางคอมพิวเตอร์และบนเครือข่ายอินเตอร์เน็ต

สภาพปัญหา

……

……

แนวทางแก้ปัญหา

……

……

ตอนที่ **3** มาตรการในทางกฎหมายของไทยมีลักษณะอย่างไรเพื่อการแสวงหาพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์

3.1 วิธีการขั้นตอนในการแสวงหาพยานหลักฐาน

……

……

3.2 ด้านข้อมูลอิเล็กทรอนิกส์เกี่ยวกับสื่อบันทึกภาพและเครื่องมืออิเล็กทรอนิกส์

……

……

ตอนที่ **4** แนวทางการแก้ไขปัญหาในการแสวงหาพยานหลักฐานในคดีอาชญากรรมทางอิเล็กทรอนิกส์เกี่ยวกับสื่อบันทึกภาพและเครื่องมืออิเล็กทรอนิกส์ควรเป็นอย่างไร ด้วยวิธีการใด

……

……

ขอขอบคุณที่เสียสละในการให้ข้อมูลครั้งนี้

ประวัติผู้เขียน

ชื่อ-สกุล	ภัทรดิษย์ วรประดิษฐ์
วุฒิการศึกษา	จบการศึกษาจาก::มหาวิทยาลัยศิลปากร
	ระดับการศึกษา :ปริญญาตรี
	คณะ:วิทยาการจัดการ
	หลักสูตร : รัฐประศาสนศาสตร์
	ชื่อปริญญา: รัฐประศาสนศาสตรบัณฑิต