กระบวนการเข้าถึงพยานหลักฐานทางดิจิทัลสำหรับเจ้าหน้าที่สืบสวนเชิงคดี

A Process of Digital Evidence Accessibility for Forensic Investigation Officers

จิระพัชร์ ทวงศ์เฉลียว
คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ

Jirapat Tawongshaliao
Faculty of Forensic Sciences, Royal Police Cadet Academy

Received: July 7, 2023 | Revised: January 14, 2024 | Accepted: January 17, 2024

บทความวิจัย (Research Article)

บทคัดย่อ

บทความนี้ศึกษาถึงแนวทางการแก้ไขปัญหาการเข้าถึงพยานหลักฐานทางดิจิทัลและอำนาจหน้าที่ของเจ้าหน้าที่ในการปฏิบัติงาน ซึ่งประกอบด้วย (1) ความหมายของข้อมูลอิเล็กทรอนิกส์ (2) การเข้าถึงข้อมูลหลักฐานทางอิเล็กทรอนิกส์ (3) หลักการให้ความยินยอมตามกฎหมาย ซึ่งการเข้าถึงข้อมูลหลักฐานทางดิจิทัลสำหรับเจ้าหน้าที่ผู้ปฏิบัติงานทางนิติวิทยาศาสตร์ในประเทศไทยมีปัจจัยและข้อจำกัดทางกฎหมายหลายด้าน การศึกษานี้จึงมีวัตถุประสงค์เพื่อศึกษาแนวทางการป้องกันในปัญหาและอุปสรรคของการเข้าถึงพยานหลักฐานทางอิเล็กทรอนิกส์ เพื่อจะได้เป็นแนวทางในการนำมาแก้ไขปรับปรุงข้อกฎหมายในการปฏิบัติงานของเจ้าหน้าที่ให้มีความเหมาะสม สอดคล้องกับตำแหน่งหน้าที่ ทั้งนี้ผู้ให้ข้อมูลหลักได้ให้สัมภาษณ์ทั้งหมด คือ เจ้าหน้าที่จากหน่วยงานทางนิติวิทยาศาสตร์ที่เกี่ยวข้องกับการบังคับใช้กฎหมายในประเทศไทย จำนวน 3 หน่วยงาน หน่วยงานละ 4 ราย ได้แก่ กรมสอบสวนคดีพิศษ สำนักงานพิสูจน์หลักฐานตำรวจ สำนักงานตำรวจแห่งชาติ และกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) ที่เป็นผู้มีความรู้ความสามารถและมีประสบการณ์การทำงานในด้านพิสูจน์หลักฐานทางอิเล็กทรอนิกส์ไม่ต่ำกว่า 3 - 5 ปี โดยส่วนใหญ่ให้ความสำคัญกับปัญหาทางด้านข้อกฎหมาย เทคโนโลยี งบประมาณและบุคลากร ทั้งนี้ยังมีข้อเสนอแนะในการปรับแก้ข้อกฎหมาย จัดสรรงบประมาณ จัดการฝึกอบรมให้กับเจ้าหน้าที่ทุกระดับ

คำสำคัญ: การเข้าถึงข้อมูลหลักฐานทางอิเล็กทรอนิกส์, หน่วยงานทางนิติวิทยาศาสตร์

Abstract

In accessing digital evidence, forensic scientists were met with restrictions in the need to have an authorization or consent from the owner of the evidence and their limited power due to the enforcement of law. Thus, the purposes of this study were to study the

problems in accessing digital evidence for forensic scientists in Thailand and to study methods to prevent problems that may occurred in accessing digital evidence. In this study, our samples were officials from 3 state agencies related to law enforcement in Thailand namely, Department of Special Investigation, Royal Thai Police's Office of Police Forensic Science, and Technology Crime Suppression Division. Thailand's Computer-related Crime Act B.E. 2550 and its amendments, The Criminal Procedure Code and interview form were used as instruments for this study. The result showed that the problems in accessing digital evidence stemmed mostly from legal problems, technology used, budget allocated and personnel. Regarding the preventative methods, it was suggested that the law regarding computer-related crime itself should be amended, the budget should be appropriately allocated and lastly, personnel of all levels should be suitably trained.

Keywords: Electronic Evidence Access**,** forensic science agency

บทนำ

ในปัจจุบันข้อมูลเอกสารที่อยู่ในรูปแบบกระดาษได้มีการเปลี่ยนรูปแบบของข้อมูลมาอยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์มากยิ่งขึ้น เพื่อให้มีการเข้าถึงของข้อมูลได้อย่างง่าย สะดวก รวดเร็ว และสามารถตรวจสอบได้ ไม่ว่าจะเปลี่ยนข้อมูลเอกสารกระดาษโดยใช้วิธีการกรอกข้อมูล สแกนเอกสารเป็นไฟล์อิเล็กทรอนิกส์ หรือแปลงไฟล์เอกสาร รูปภาพหรือไมโครซอฟออฟฟิส (Microsoft office) เป็นไฟล์ข้อมูลอิเล็กทรอนิกส์ ซึ่งประมวลผลและจัดเก็บไว้ในระบบคอมพิวเตอร์ หรือถูกส่งผ่านระบบเครือข่ายไปยังคอมพิวเตอร์เครื่องอื่น และการนำระบบคลาวด์ (Cloud) เข้ามาใช้และมีบทบาทในภาคธุรกิจมากยิ่งขึ้น เพื่อช่วยลดข้อจำกัดของการทำงานแบบเดิม ๆ ที่ต้องทำงานในสำนักงานเท่านั้น ให้สามารถทำงานจากที่ใดเมื่อไหร่ก็ได้ เมื่อมีการนำระบบคลาวด์ (Cloud) เข้ามาใช้ มาตรการในการป้องกันข้อมูลส่วนบุคคลการละเมิดลิขสิทธิ์ย่อมตามมาด้วย ส่งผลทำให้การเข้าถึงข้อมูลอิเล็กทรอนิกส์ในระบบคลาวด์ (Cloud) ต้องได้รับความยินยอมจากเจ้าของผู้ใช้บริการระบบคลาวด์ (Cloud)

การเข้าถึงข้อมูลอิเล็กทรอนิกส์ในรูปแบบต่าง ๆ สามารถเข้าผ่านด้วยการถอดรหัสการตั้งค่าความปลอดภัยของชุดข้อมูล ซึ่งการที่จะเข้าถึงข้อมูลได้นั้น จำเป็นต้องทราบรหัสความปลอดภัยจากผู้ดูแลและได้รับความยินยอมจากผู้เป็นเจ้าของรหัสความปลอดภัย หากแต่มีความจำเป็นที่จะต้องเข้าถึงข้อมูลอิเล็กทรอนิกส์อันอาจควรเชื่อได้ว่าเป็นข้อมูลที่เกิดจากการกระทำความผิด ให้พนักงานเจ้าหน้าที่ผู้ซึ่งได้รับแต่งตั้งจากรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 (กฤษฎีกา.2560) หรือพนักงานสอบสวนตามประมวลกฎหมาย

วิธีพิจารณาความอาญา ยื่นคำร้องขอต่อศาลเพื่อดำเนินการเข้าถึงข้อมูลคอมพิวเตอร์ ทำการถอดรหัส หรือตรวจสอบระบบคอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการเก็บข้อมูลคอมพิวเตอร์นั้น ๆ

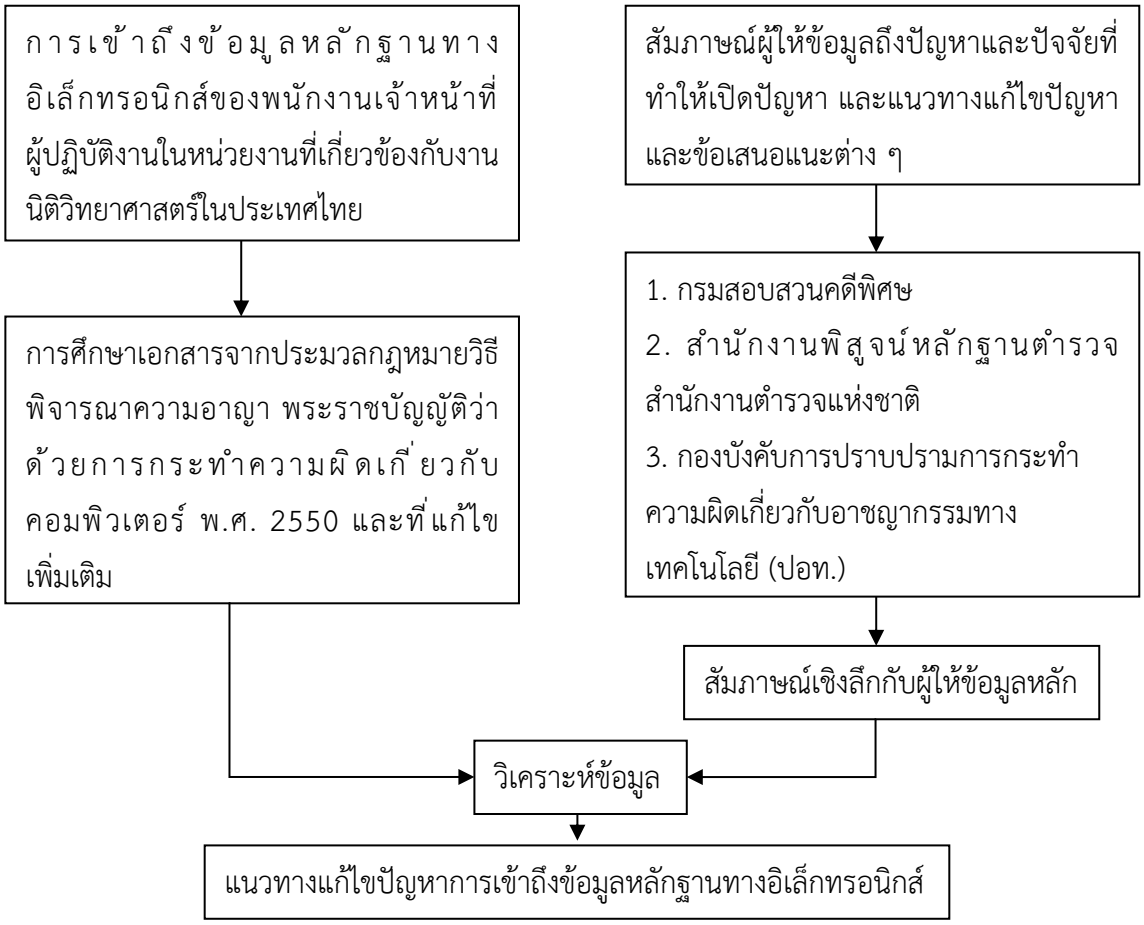
ซึ่งปัจจุบันคนไทยใช้สื่อสังคมออนไลน์ หรือ โซเชียลมีเดีย (social media) กันเป็นจำนวนมากขึ้น ทั้งการนำมาใช้เพื่อการทำงาน ติดตามข่าวสาร การซื้อขายของออนไลน์ ธุรกรรมทางการเงิน การประชุม การเรียน โดยใช้ผ่านแพลตฟอร์มสื่อสังคมออนไลน์ต่าง ๆ เช่น เฟสบุ๊ก (Facebook) ทวิตเตอร์ (Twitter) อินสตราแกรม (Instagram) แมสเซนเจอร์ (Messenger) ไลน์ (LINE) ซูม (Zoom) โดยมีการนำเข้าและส่งออกของข้อมูลอิเล็กทรอนิกส์หรือใช้ข้อมูลอิเล็กทรอนิกส์ผ่านอุปกรณ์อิเล็กทรอนิกส์ ซึ่งการกระทำเหล่านี้อาจทำให้เกิดการกระทำความผิดอันเป็นการเข้าข่ายความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ประมวลกฎหมายวิธีพิจารณาความอาญา และกฎหมายอื่น ๆ ที่เกี่ยวข้อง หรือเป็นช่องทางให้อาชญากรใช้ข้อมูลอิเล็กทรอนิกส์แสวงหาผลประโยชน์และก่ออาชญากรรมได้ นำไปสู่คดีอาชญากรรมทางคอมพิวเตอร์หรืออาชญากรรมทั่วไป ทำให้มีการเกี่ยวพันกับอุปกรณ์หรือเครื่องมืออิเล็กทรอนิกส์ ซึ่งพนักงานเจ้าหน้าที่ที่มีอำนาจหน้าที่เป็นการเฉพาะเข้ามาทำการรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์ ติดตามร่องรอยของข้อมูลจราจรทางคอมพิวเตอร์ในการตามหาผู้กระทำความผิด ดังนั้นในการปฏิบัติหน้าที่ของพนักงานเจ้าหน้าที่ควรมีการดำเนินการตามขั้นตอน และการคุ้มครองห่วงโซ่พยานหลักฐาน (Chain of custody) เพื่อป้องกันไม่ให้เกิดการปนเปื้อนของพยานหลักฐานทางอิเล็กทรอนิกส์หรือไปทำลายพยานหลักฐานทางอิเล็กทรอนิกส์ได้ และพนักงานเจ้าหน้าที่ผู้ปฏิบัติงานต้องมีความรู้ความเชี่ยวชาญ และประสบการณ์การทำงานทางด้านคอมพิวเตอร์และเทคโนโลยีเป็นอย่างมาก

งานวิจัยเรื่องนี้เป็นการศึกษาปัญหาการเข้าถึงพยานหลักฐานทางอิเล็กทรอนิกส์ของพนักงานเจ้าหน้าที่ผู้ปฏิบัติงาน ด้วยวิธีการศึกษาเอกสารจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม ประมวลกฎหมายวิธีพิจารณาความอาญา และการสัมภาษณ์เชิงลึกถึงปัญหาและปัจจัยที่ส่งผลต่อการเข้าถึงพยานหลักฐานทางอิเล็กทรอนิกส์กับผู้ให้ข้อมูลหลักจากหน่วยงานที่เกี่ยวข้องกับการบังคับใช้กฎหมายในประเทศไทย จำนวน 3 หน่วยงาน ได้แก่ 1) กรมสอบสวนคดีพิศษ 2) สำนักงานพิสูจน์หลักฐานตำรวจ สำนักงานตำรวจแห่งชาติ 3) กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.)

วัตถุประสงค์

1. เพื่อศึกษากระบวนการทางกฎหมายที่เกี่ยวข้องกับการเข้าถึงข้อมูลหลักฐานทางอิเล็กทรอนิกส์
2. เพื่อศึกษากระบวนการการเข้าถึงข้อมูลหลักฐานทางอิเล็กทรอนิกส์ของหน่วยงานที่เกี่ยวข้องกับการบังคับใช้กฎหมายในประเทศไทย
3. เพื่อกำหนดแนวทางแก้ไขปัญหาการเข้าถึงข้อมูลหลักฐานทางอิเล็กทรอนิกส์ของหน่วยงานที่เกี่ยวข้องกับการบังคับใช้กฎหมายในประเทศไทย

กรอบแนวคิดการวิจัย



ภาพที่ 1 ความสัมพันธ์ของแนวทางการเข้าถึงข้อมูลหลักฐานทางอิเล็กทรอนิกส์ของพนักงานเจ้าหน้าที่ผู้ปฏิบัติงานในหน่วยงานที่เกี่ยวข้องกับงานนิติวิทยาศาสตร์ในประเทศไทย

ทบทวนวรรณกรรม

งานวิจัยเรื่อง กระบวนการเข้าถึงข้อมูลหลักฐานทางอิเล็กทรอนิกส์ของพนักงานเจ้าหน้าที่ผู้ปฏิบัติงานในหน่วยงานที่เกี่ยวข้องกับงานนิติวิทยาศาสตร์ในประเทศไทย ผู้วิจัยได้ทำการศึกษาวรรณกรรม แนวคิด ทฤษฎีและงานวิจัยที่เกี่ยวข้องกับแนวทางการเข้าถึงข้อมูลหลักฐานทางอิเล็กทรอนิกส์ โดยประกอบด้วย

1. แนวคิดเกี่ยวกับข้อมูลอิเล็กทรอนิกส์

1.1 ความหมายของข้อมูลอิเล็กทรอนิกส์

ข้อมูลอิเล็กทรอนิกส์ หมายความถึง ข้อมูลอิเล็กทรอนิกส์เป็นข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ และหมายความรวมถึงข้อมูลหรือบันทึกที่สร้างขึ้นโดยคอมพิวเตอร์ แม้จะไม่ได้ใช้เป็นสื่อในการติดต่อสื่อสารกับบุคคลอื่นก็ตาม

1.2 ประเภทของข้อมูลอิเล็กทรอนิกส์

ประเภทแรก ข้อมูลอิเล็กทรอนิกส์ที่สร้างโดยมนุษย์

ประเภทที่สอง ข้อมูลอิเล็กทรอนิกส์ที่สร้างโดยอัตโนมัติ

ประเภทที่สาม ข้อมูลอิเล็กทรอนิกส์ที่สร้างโดยมนุษย์และโดยอัตโนมัติประกอบกัน

1.3 การเก็บรวบรวมข้อมูลทางอิเล็กทรอนิกส์

กระบวนการเก็บข้อมูลที่เรียกว่า Digital Forensics หรือ การพิสูจน์หลักฐานจากทางดิจิทัล เพื่อป้องกันการปนเปื้อนของพยานหลักฐานด้วย ซึ่งการเก็บพยานหลักฐานดิจิทัลมีอยู่ 3 กระบวนการ ดังนี้

กระบวนการที่หนึ่ง การรวบรวมวัตถุพยานจากผู้เสียหาย การรวบรวมวัตถุพยานอยู่ที่ต้นทาง คือ ผู้เสียหาย โดยผู้เสียหายจะเป็นคนรวบรวมวัตถุพยาน อย่างเช่น แชทที่มีการพูดคุยกัน รูปภาพที่ส่งมาบัญชีผู้ใช้ (Account) ปลอมที่ผู้เสียหายโดนหลอก ซึ่งไม่ว่าจะเป็นการรวบรวมเองของผู้เสียหายหรือจะเป็นการนำเครื่องคอมพิวเตอร์หรือเครื่องโทรศัพท์ดังกล่าวมาให้เจ้าหน้าที่เป็นคนรวบรวมตรวจสอบก็ได้ ในส่วนนี้จะเป็นการเริ่มต้นของกระบวนการหาตัวผู้กระทำความผิด กรณีที่บัญชีผู้ใช้ (Account) ของผู้กระทำความผิดยังไม่ถูกปิดหรือถูกบล็อคไป ก็ยังสามารถที่จะติดต่อพูดคุยกันต่อไปได้ แต่บางกรณีที่ผู้เสียหายไม่สามารถติดต่อกับผู้กระทำความผิดได้แล้วนั้น ก็จะเป็นการยากที่จะติดตามตัวผู้กระทำความผิด

กระบวนการที่สอง การรวบรวมพยานหลักฐานจากผู้ให้บริการอินเทอร์เน็ต ในระหว่างการพูดคุยกันผ่านแพลตฟอร์ม เช่น เฟสบุ๊ก (Facebook) เจ้าของแพลตฟอร์มหรือผู้ให้บริการอินเทอร์เน็ตต้องทำการเก็บล็อคไฟล์ (log file) หรือข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) เอาไว้ ตามที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ซึ่งข้อมูลจราจรทางคอมพิวเตอร์ที่จะได้จากผู้ให้บริการอินเทอร์เน็ตนั้นจะแสดงรายละเอียดของไอพี (IP Address) ว่ามีไอพีใดบ้างที่ติดต่อสื่อสารกันอยู่ในขณะนั้น มีเวลาเริ่มต้นและสิ้นสุดอย่างไร หรือแสดงเบอร์โทรศัพท์ที่ใช้ในการติดต่อสื่อสาร โดยมาตรา 26 ของตามที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 บัญญัติไว้ว่า ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินสองปีเป็นกรณีพิเศษ เฉพาะรายและเฉพาะคราวก็ได้ ดังนั้น หากทางผู้ให้บริการอินเทอร์เน็ตให้ความร่วมมือในการดำเนินการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เอาไว้ เจ้าหน้าที่ก็จะสามารถตรวจสอบได้ถึงต้นตอหรือสามารถระบุได้ถึงที่อยู่ของผู้กระทำความผิดได้

กระบวนการที่สาม การรวบรวมพยานหลักฐานจากผู้กระทำความผิด มักเป็นวัตถุพยานปลายทาง กล่าวคือ เป็นข้อมูลของผู้กระทำผิด ไม่ว่าจะเป็นโทรศัพท์มือถือ เครื่องคอมพิวเตอร์ รูปภาพ หรือไฟล์ข้อมูลชนิดอื่นที่ใช้ในการแอบอ้าง หรือปลอมผ่านบัญชีผู้ใช้ (Account) บนอินเทอร์เน็ต ซึ่งในขั้นตอนนี้ขึ้นอยู่กับว่าเจ้าหน้าที่จะสามารถจับกุมและยึดอุปกรณ์ในการกระทำความผิดได้หรือไม่ ด้วยเหตุที่ตัวผู้กระทำความผิดส่วนมากมักเป็นคนต่างชาติ และมีการเดินทางไปมาหลายพื้นที่ ไม่มีที่อยู่เป็นหลักเป็นแหล่ง หรือมีการหลอกลวงให้บุคคลอื่นเป็นผู้กระทำความผิดแทนตนเอง ทำให้การจับกุมตัวผู้กระทำผิด

เป็นสิ่งที่ทำได้ยาก นอกเสียจากว่าบุคคลนั้นจะอยู่ในประเทศไทยในระยะเวลาหนึ่ง และเป็นผู้ที่ลงมือกระทำความผิดเอง โดยไม่ได้ใช้ให้บุคคลอื่นเป็นผู้กระทำแทน จึงจะมีโอกาสในการจับตัวได้ค่อนข้างสูง ในกระบวนการนี้ เมื่อจับตัวผู้กระทำผิดพร้อมทั้งอุปกรณ์หรือเครื่องมือที่ใช้ในการกระทำความผิดได้แล้วนั้น เจ้าหน้าที่พิสูจน์หลักฐานจะต้องทำการตรวจสอบว่าเป็นผู้กระทำผิดที่จับตัวมานั้นเป็นผู้กระทำความผิดที่แท้จริงหรือไม่ ซึ่งในขั้นตอนนี้จะเป็นการตรวจสอบที่ต้องใช้เทคนิค และความรู้ความเชี่ยวชาญด้านคอมพิวเตอร์เป็นอย่างมาก

2. แนวคิดทฤษฎีการเข้าถึงข้อมูลหลักฐานทางอิเล็กทรอนิกส์

2.1 ความหมายของพยานหลักฐานดิจิทัล

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (2559) ให้ความหมายของพยานหลักฐานดิจิทัล ไว้ว่า ข้อมูลที่ได้เก็บรักษาบนสื่อบันทึกข้อมูลหรืออยู่ระหว่างการส่ง รับ ด้วย วิธีการทางอิเล็กทรอนิกส์ ซึ่งสามารถถูกใช้อ้างอิงเป็นพยานหลักฐาน

2.2 รูปแบบการรวบรวมหลักฐานคอมพิวเตอร์

กรณีหลักฐานเป็นคอมพิวเตอร์ ควรตรวจสอบสถานะของคอมพิวเตอร์ว่าปิด เปิด หรืออยู่ในโหมด Standby สภาพและรายการอุปกรณ์ภายนอกที่เชื่อมต่อกับคอมพิวเตอร์ และตรวจสอบในช่อง CD, DVD, Floppy, Card reader และพอร์ตเชื่อมต่อ USBว่า มีสื่อบันทึกข้อมูลตกค้างหลงเหลืออยู่หรือไม่ หากมีให้จดบันทึกไว้เป็นหลักฐานอีกชิ้นหนึ่ง โดยระบุว่าพบในคอมพิวเตอร์เครื่องใด

กรณีคอมพิวเตอร์เปิดทำงานอยู่ให้ดำเนินการถ่ายภาพรายละเอียดหน้าจอแสดงผลของโปรแกรมที่เปิดอยู่ทุกหน้า และทุกแท็บ หากพบข้อมูลแสดงวันเวลาของเครื่องปรากฏที่หน้าจอแสดงผล ให้ถ่ายภาพวัน เวลาให้เห็นชัดเจนเทียบกับนาฬิกาเทียบเวลา ถ้าหน้าจอแสดงผลถูกล็อคและต้องใช้รหัสผ่านในการเข้าสู่ระบบปฏิบัติการ ให้สอบถาม รหัสผ่านจากเจ้าของเครื่องเพื่อปลดล็อคเครื่อง หากไม่ทราบรหัสผ่านที่ถูกต้องให้ปิดเครื่องด้วยวิธีการถอดปลั๊กไฟฟ้าที่ต่ออยู่ที่ตัวเครื่องคอมพิวเตอร์พีซีออก (ไม่ใช่ถอดจากแหล่งจ่าย ไฟฟ้า) กรณีสามารถปิดคอมพิวเตอร์ได้ ให้ดำเนินการด้วยวิธีการสำหรับคอมพิวเตอร์พีซี คือ ถอดปลั๊กไฟฟ้าที่ต่ออยู่ที่ตัวเครื่องคอมพิวเตอร์พีซีออก (ไม่ใช่ถอดจากแหล่งจ่าย ไฟฟ้า) วิธีการสำหรับเซิร์ฟเวอร์ ในกรณีเซิร์ฟเวอร์ดังกล่าวเป็นเครื่องให้บริการที่มีระบบฐานข้อมูล ควรปิดโปรแกรมฐานข้อมูลตามขั้นตอนที่กำหนดไว้ในคู่มือการใช้งานก่อนปิดเครื่อง ถอดปลั๊กไฟฟ้าที่ต่ออยู่ที่ตัวเครื่องเซิร์ฟเวอร์ออก และข้อมูลที่สามารถใช้เป็นพยานหลักฐานดิจิทัลบันทึกไว้ในเทปสำรองข้อมูล จึงควรพิจารณาจัดเก็บเทปสำรองข้อมูลและเครื่องอ่านเทปที่เกี่ยวข้อง วิธีการสำหรับแล็ปท็อป คือ ถอดปลั๊กไฟฟ้าที่ต่ออยู่ที่ตัวแล็ปท็อปออก ถอดแบตเตอรี่ออกหรือหากไม่สามารถถอดแบตเตอรี่ออกได้ ให้กดปุ่มเปิดเครื่องค้างไว้จนกว่าเครื่องจะดับ

กรณีหลักฐานคอมพิวเตอร์ปิดอยู่ให้ดำเนินการถอดสายที่เชื่อมต่อกับเครือข่ายและอุปกรณ์ต่อพ่วงทั้งหมด และควรบันทึกการเชื่อมต่อสายต่าง ๆ ข้างต้นไว้ด้วย หากจำเป็นต้องทำสำเนาหลักฐานดิจิทัล

ในสถานที่เกิดเหตุ ให้ดำเนินการทำสำเนาข้อมูลในหลักฐานด้วยกระบวนการที่น่าเชื่อถือและสามารถตรวจสอบได้ จัดเก็บคอมพิวเตอร์ และสายไฟฟ้าลงบรรจุภัณฑ์ กรณีที่เป็นเซิร์ฟเวอร์ ให้รวบรวมข้อมูลเกี่ยวกับ RAID โดยพิจารณาจัดเก็บเทปสำรองข้อมูลและเครื่องอ่านเทปที่เกี่ยวข้อง

2.3 รูปแบบการรวบรวมหลักฐานเครื่องมือสื่อสารเคลื่อนที่

กรณีหลักฐานเป็นเครื่องมือสื่อสารเคลื่อนที่ ให้สอบถามรหัสผ่านเพื่อปลดล็อคเครื่องและซิมการ์ดและจดบันทึกโดยให้ระบุด้วยว่าเป็น PIN หรือ Pattern lock

กรณีที่หลักฐานเปิดใช้งานอยู่ และสามารถเข้าใช้งานได้ ควรดำเนินการตรวจสอบรายละเอียดเกี่ยวกับหลักฐาน โดยบันทึกภาพหลักฐานและเนื้อหาที่ปรากฏบนหน้าจอแสดงผลและจดบันทึกข้อมูลโดยละเอียด ตรวจสอบข้อมูลเฉพาะของหลักฐาน เช่น IMEI รุ่น ผู้ให้บริการ เป็นต้น เปิดการใช้งานโหมดเครื่องบิน (Airplane mode) เพื่อตัดการรับสัญญาณ ปิดการใช้งานสัญญาณไร้สาย (Wi-Fi) เพื่อตัดการสื่อสารผ่านระบบเน็ตเวิร์ก ปิดการใช้งานสัญญาณบลูทูธ (Bluetooth) ปิดการใช้รหัสผ่าน เพื่อให้สามารถเข้าถึงเครื่องได้ภายหลัง ปิดการล็อคหน้าจอแสดงผล (Disable screen lock) และดำเนินการบรรจุและเคลื่อนย้ายหลักฐาน

กรณีที่ไม่สามารถเข้าใช้งานหลักฐานได้ เช่น ติดล็อครหัสผ่าน ให้บันทึกภาพหลักฐานและเนื้อหาที่ปรากฏบนหน้าจอแสดงผล และจดบันทึกโดยละเอียด หลังจากนั้นจึงดำเนินการบรรจุและเคลื่อนย้ายหลักฐาน

2.4 รูปแบบการรวบรวมหลักฐานสื่อบันทึกข้อมูล

กรณีหลักฐานเป็นสื่อบันทึกข้อมูล สื่อบันทึกข้อมูลในที่นี้หมายความรวมถึง สื่อบันทึกข้อมูลดิจิทัล ได้แก่ ฮาร์ดดิสก์แบบเชื่อมต่อภายนอก USB Flash drive, SD card, CD, DVD และ Blu-ray Disc ให้จัดเก็บลงในบรรจุภัณฑ์ ในกรณีจำเป็นต้องทำสำเนาหลักฐานดิจิทัลในสถานที่เกิดเหตุ ให้ดำเนินการทำสำเนาข้อมูลในหลักฐานด้วยกระบวนการที่น่าเชื่อถือและสามารถตรวจสอบได้ หากพบข้อผิดพลาดระหว่างการสำเนาข้อมูลให้จดบันทึกรายละเอียดไว้ ให้ยืนยันความครบถ้วนสมบูรณ์ของข้อมูลที่สำเนาได้ด้วยการคำนวณและเปรียบเทียบค่า แฮช ของต้นฉบับและสำเนา เช่น MD5 SHA1 SHA256 เป็นต้น โดยดำเนินการอย่างน้อยสองรูปแบบ หากพบสื่อบันทึกข้อมูลอยู่ในน้ำ ให้จัดเก็บหลักฐานในสภาพที่มีน้ำในแหล่งที่พบหลักฐานอยู่ และนำกลับไปตรวจวิเคราะห์ในห้องปฏิบัติการโดยเร็ว

2.5 ประเภทการสำเนาข้อมูลจากคอมพิวเตอร์และสื่อบันทึกข้อมูล

ประเภทที่หนึ่ง Physical เป็นการสำเนาข้อมูลทั้งหมดในหลักฐานแบบบิตต่อบิต (bit-by-bit) ใช้ Write blocker เพื่อป้องกันการเปลี่ยนแปลงข้อมูลต้นฉบับ โดย Imaging (Disk-to-file) ให้สำเนาฮาร์ดดิสก์ทั้งลูกเก็บในรูปแบบไฟล์ หรือ Cloning (Disk-to-disk) ให้สำเนาฮาร์ดดิสก์ทั้งลูกลงในฮาร์ดดิสก์อีกลูกหนึ่ง

ประเภทที่สอง Logical เป็นการสำเนาข้อมูลเฉพาะส่วนจากหลักฐาน เช่น พาร์ทิชัน, ไดเร็กทอรี หรือ ไฟล์บางไฟล์ เป็นต้น โดยใช้ Write blocker เพื่อป้องกันการเปลี่ยนแปลงข้อมูลต้นฉบับ หากทำได้ โดยอาจเลือกใช้ในกรณีพบ RAID หรือกรณีที่คาดว่าฮาร์ดดิสก์หลักฐานถูกเข้ารหัสลับไว้

ประเภทที่สาม Volatile data อย่างน้อยให้สำเนาข้อมูลจากหน่วยความจำหลัก (RAM) ของคอมพิวเตอร์ที่กำลังเปิดใช้งานอยู่ (Live) โดยรันซอฟต์แวร์สำหรับจัดเก็บ Volatile data จากสื่อบันทึกข้อมูล (เช่น USB flash drive) ที่เชื่อถือได้

2.6 ห่วงโซ่การครอบครองพยานหลักฐาน (Chain of custody)

ห่วงโซ่การครอบครองพยานหลักฐาน หมายถึง ข้อมูลที่ระบุรายละเอียดของพยานหลักฐานและการส่งต่อพยานหลักฐานโดยเจ้าหน้าที่ที่รับผิดชอบ ซึ่งจะต้องมีการบันทึกไว้เริ่มตั้งแต่เมื่อพยานหลักฐานชิ้นนั้นถูกเก็บมาจากที่เกิดเหตุมาอยู่ในความครอบครองของเจ้าหน้าที่ที่เกี่ยวข้อง จนถึงเมื่อสิ้นสุดคดี ไว้ในแบบฟอร์มการครอบครองซึ่งจะเป็นประโยชน์หากผู้ที่เกี่ยวข้องต้องไปให้การในศาล โดยจะต้องสามารถยืนยันได้ว่าในระหว่างการครอบครองพยานหลักฐานชิ้นนั้นได้ถูกจัดเก็บไว้ที่ไหน ได้ถูกนำไปทำอะไรบ้าง มีปัจจัยที่จะทำให้พยานหลักฐานเปลี่ยนแปลงหรือไม่ ได้ส่งต่อให้กับบุคคลอื่นหรือไม่ เมื่อวัน/เวลาใด ดังนั้น ห่วงโซ่การครอบครองพยานหลักฐาน คือ เอกสารแสดงลำดับการเกิดเหตุการณ์หรือเอกสารแสดงทุกขั้นตอน ตั้งแต่การยึด การดูแลรักษา การควบคุม การวิเคราะห์ และการจัดเก็บหลักฐานทางอิเล็กทรอนิกส์ โดยสามารถแบ่งออกเป็น 4 ส่วน ได้แก่

ส่วนที่หนึ่งการจัดการ (Taking) เป็นกระทำโดยผู้เก็บวัตถุพยาน จำแนกวัตถุพยานโดยการทำตำหนิ ระบุวันเดือนปีที่เก็บ และรายละเอียดต่างๆ

ส่วนที่สองการเก็บ (Keeping) เป็นพิสูจน์ให้เห็นว่าการเก็บและครอบครองวัตถุพยานได้กระทำอย่างเหมาะสม ถูกต้องตามหลักวิชาการ

ส่วนที่สามการขนส่ง (Transporting) ต้องรัดกุม แสดงให้เห็นว่าไม่เกิดการสับสนกับวัตถุพยานอื่น มีการลงทะเบียนถ้าเป็นการส่งทางไปรษณีย์

ส่วนที่สี่การส่งมอบ (Delivering) เป็นการพิสูจน์ว่าของกลางได้ส่งมอบให้กับผู้รับอย่างถูกต้องและเหมาะสม มีหลักฐานแสดงวันเดือนปีที่รับของกลาง และมีรายชื่อผู้รับผิดชอบทุกครั้ง

3. แนวคิดหลักให้ความยินยอม

3.1 ความหมายของการให้ความยินยอม

การจงใจปล่อยให้เหตุการณ์อย่างใดอย่างหนึ่ง เกิดขึ้นโดยไม่ขัดขวางทั้งที่สามารถขัดขวางได้ซึ่งจะต้องเป็นการแสดงความประสงค์ที่จะให้เกิดเหตุการณ์ เช่นนั้นขึ้น โดยแสดงออกด้วยการกระทำอย่างหนึ่งโดยตนเองหรือโดยให้ผู้อื่นกระทำแทนตน อันเป็นการ แสดงความประสงค์ต่อผู้กระทำเหตุการณ์นั้นให้เข้าใจว่าตนอนุญาตให้ทำ ยกเว้นแต่ในกรณีพิเศษอย่างยิ่งเท่านั้นที่การนิ่งไม่ขัดขวาง อาจถือได้ว่าเป็นความ

ยินยอม เพราะเป็นที่เข้าใจกันโดยปกติทั่วไปว่าการนิ่ง เช่นนั้นเป็นการยินยอม และการแสดงออกซึ่งความประสงค์อันถือได้ว่าเป็นความยินยอมนั้นอาจแสดงออก โดยชัดแจ้งหรือโดยปริยายก็ได้

การที่ผู้เสียหายยินยอมโดยสมัครใจต่อการกระทำ ประทุษร้าย หรือผู้เสียหายสมัครใจเข้าสู่อันตรายเอง ไม่ว่าจะยินยอมให้กระทำต่อร่างกายทรัพย์สินหรือ สิทธิของตน และเป็นการยินยอมของผู้สามารถให้ความยินยอม ทำให้การกระทำไม่เป็นละเมิด อันที่จริง ความยินยอมของผู้เสียหายมิใช่เป็นสิทธิของผู้กระทำ แต่เป็นข้อแก้ตัวของผู้กระทำ ทำให้ผู้กระทำไม่ต้อง รับผิดเพื่อละเมิด

3.2 ลักษณะการให้ความยินยอม

ผู้ให้ความยินยอมซึ่งเป็นผู้ได้รับความเสียหายต้องเป็นผู้มีความสามารถในการให้ความยินยอม คือ เข้าใจหยั่งรู้ถึงการกระทำนั้น และรู้คุณค่าของการกระทำว่าดีหรือไม่ เข้าใจถึงธรรมชาติของ การกระทำและผลที่อาจเกิดขึ้นจากการกระทำนั้นได้และต้องรู้ถึงคุณค่าของการกระทำนั้นจากประสบการณ์ของตนเอง ซึ่งจะต้องเป็นผู้ใหญ่พอสมควร

วิธีการให้ความยินยอม กฎหมายมิได้กำหนดแบบไว้จึงอาจให้โดยแจ้งชัดหรือโดยปริยาย และการนิ่งถือว่าเป็นการให้ความยินยอมได้ถ้าตามพฤติการณ์ทำให้บุคคลทั่วไปเข้าใจว่าเป็นการให้ความ ยินยอม

ผลของความยินยอม เมื่อการให้ความยินยอมได้กระทำโดยผู้ให้ความยินยอมที่ถูกต้องตามกฎหมาย และใช้วิธีการให้ความยินยอมตลอดจนเงื่อนไขความสมบูรณ์ของความยินยอมถูกต้องครบถ้วนตามหลักความยินยอมที่ได้กล่าวในตอนต้นแล้ว ย่อมทำให้ผลของความยินยอมเป็นไปโดยสมบูรณ์ ซึ่งผู้กระทำสามารถอ้างหลักความยินยอมไม่เป็นละเมิดได้

ข้อยกเว้นหลักความยินยอมไม่เป็นละเมิด อาจมีในกรณีที่เกิดการประทุษกรรมโดยไม่ได้รับความยินยอม แต่ผู้กระทำไม่ต้องรับผิด ได้แก่ กรณีมีเหตุฉุกเฉินเกิดขึ้นอย่างแท้จริงและแจ้งชัด จำเป็นต้องกระทำก่อนได้รับความยินยอม เช่น การจับคนที่จะฆ่าตัวตายด้วยการกระโดดจากที่สูง โดยมัดมือมัดเท้าขังไว้ในห้อง ในกรณีเช่นนั้นวิญญูชนย่อมให้ความยินยอมเช่นมีคนโยนระเบิดเข้ามาและระเบิดกำลังจะระเบิดจึงผลักผู้ซึ่งอยู่ด้านข้างให้ล้มเพื่อหลบแรงระเบิด และการผลักทำให้ผู้นั้นได้รับบาดเจ็บ ไม่ต้องรับผิด ผู้กระทำไม่รู้หรือไม่มีเหตุควรรู้ว่าผู้ถูกกระทำจะไม่ให้ความยินยอมถ้ามีโอกาสถามบุคคล นั้น เช่น แพทย์นำคนเจ็บซึ่งสลบจากอุบัติเหตุเข้าทำการผ่าตัดเพื่อช่วยชีวิต

4. งานวิจัยที่เกี่ยวข้อง

4.1 Nath Thanesavanich (2012) ได้ทำการศึกษาแนวทางในการรับฟังพยานหลักฐานทางอิเล็กทรอนิกส์ที่ได้รับการรับรองความถูกต้องก่อนนำคดีเข้าสู่ศาลและการนำสืบพยานหลักฐานอิเล็กทรอนิกส์ในคดีอาญา โดยทำการศึกษาเปรียบเทียบระหว่างกฎหมายประเทศไทยกับกฎหมายต่างประเทศ

4.2 Pannat Khankhet (2016) ได้ทำการศึกษาเกี่ยวกับอำนาจหน้าที่ของพนักงานสอบสวนในการรวบรวมพยานหลักฐานในชั้นพนักงานสอบสวนของประเทศไทยนำมาเปรียบเทียบกับอำนาจหน้าที่ของ

พนักงานสอบสวนในต่างประเทศที่ใช้ เพื่อนำเสนอแนวทางในการปรับปรุงแก้ไขปัญหาเกี่ยวกับอำนาจหน้าที่ของเจ้าพนักงานสอบสวนคดีทั่วไปของประเทศไทยให้มีอำานาจหน้าที่ตามกฎหมาย เพื่อให้สามารถรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ได้อย่างมีประสิทธิภาพ แต่ในขณะเดียวกันก็อยู่ภายใต้กรอบของกฎหมายที่บัญญัติชัดเจนและเหมาะสมกับประเทศไทย

4.3 Electronic Transactions Development Agency (2016) ทำการศึกษาแนวทางสำหรับการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์ พยานหลักฐานที่มีความสอดคล้องกับมาตรฐานสากล สำหรับการปฏิบัติงานในสถานที่เกิดเหตุและในห้องปฏิบัติการ ซึ่งครอบคลุมการจัดการคอมพิวเตอร์ สื่อบันทึกข้อมูลดิจิทัลแบบภายใน สื่อบันทึกข้อมูลดิจิทัลแบบภายนอก ข้อมูลคอมพิวเตอร์ และเครื่องมือสื่อสารเคลื่อนที่

4.4 Wichayada Amphonkitwiwat (2018) ได้ทำการศึกษาวัตถุประสงค์ การถกเถียงและผลกระทบที่เกิดขึ้นจากการบังคับใช้ของกฎหมาย นับตั้งแต่ขั้นตอนของการจัดทำร่าง พ.ร.บ. ว่าด้วยอาชญากรรมคอมพิวเตอร์ขึ้นเป็นครั้งแรกจนกระทั่งเปลี่ยนมาเป็น พ.ร.บ. ว่า ด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ทั้งในประเด็นด้านเนื้อหาของกฎหมาย บทลงโทษ และขอบเขตการบังคับใช้ของกฎหมายว่ามีลักษณะอย่างไร เพื่อชี้ให้เห็นถึงความแตกต่างของกฎหมายดังกล่าวนี้ว่าได้มีความเปลี่ยนแปลงไปอย่างสำคัญ

4.5 Kunnida Phatinawin (2015) ได้ทำการศึกษาเกี่ยวกับปัญหาการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ในคดีอาญาตามประมวลกฎหมายวิธีพิจารณาความอาญา ตลอดจนศึกษาแนวคิด หลักการและบทบัญญัติกฎหมายของต่างประเทศที่เกี่ยวข้องกับปัญหาดังกล่าว ได้แก่ สหรัฐอเมริกา ประเทศอังกฤษและเครือรัฐออสเตรเลีย เพื่อนำมาวิเคราะห์และเสนอแนวทางในการปรับปรุงแก้ไขกฎหมายเกี่ยวกับการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ในประเทศไทย

4.6 Natthanan Jaisue (2021) ได้ทำการศึกษาเกี่ยวกับกรณีพยานหลักฐานที่ถูกบันทึกไว้ในโทรศัพท์เคลื่อนที่ และคอมพิวเตอร์ เพื่อเสนอปัญหาและแนวทางการแก้ไขปัญหาระบบ กฎหมายลักษณะพยานหลักฐานของประเทศไทยเกี่ยวกับพยานหลักฐานดิจิทัลที่ถูกบันทึกไว้ในโทรศัพท์เคลื่อนที่และคอมพิวเตอร์

4.7 Cecelia Horan and Hossein Saiedian (2021) ได้ทำการศึกษาเทคโนโลยีในการสืบสวนอาชญากรรมทางไซเบอร์ การกำหนดเครื่องมือที่จะนำมาใช้ในการตรวจสอบข้อมูล และวิธีการทำงานของเครื่องมือให้มีประสิทธิภาพ เพื่อนำมาเปรียบเทียบว่าเครื่องมือใดต้องนำมาใช้สืบสวนกับหลักฐานประเภทใด และวิธีการใด ให้มีประสิทธิภาพมากที่สุด

ระเบียบวิธีวิจัย

1) ประชากรและกลุ่มตัวอย่าง

การวิจัยนี้เป็นการศึกษาปัญหาการเข้าถึงข้อมูลหลักฐานทางอิเล็กทรอนิกส์ของพนักงานเจ้าหน้าที่ผู้ปฏิบัติงานในหน่วยงานที่เกี่ยวข้องกับงานนิติวิทยาศาสตร์ในประเทศไทย โดยเป็นการวิจัยเชิงคุณภาพ (Qualitative Research) ซึ่งใช้วิธีการศึกษาเอกสารจากประมวลกฎหมายวิธีพิจารณาความอาญา พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม และการสัมภาษณ์เชิงลึก (In-Depth Interview) กับผู้ให้ข้อมูลหลัก ได้แก่ เจ้าหน้าที่ของหน่วยงานที่เกี่ยวข้องกับการบังคับใช้กฎหมายในประเทศไทย จำนวน 3 หน่วยงาน ประกอบด้วย กรมสอบสวนคดีพิศษ สำนักงานพิสูจน์หลักฐานตำรวจ สำนักงานตำรวจแห่งชาติ และกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.)

2) การเก็บรวบรวมข้อมูล

1. การรวบรวมข้อมูลเชิงคุณภาพด้วยวิธีการศึกษาเอกสารประมวลกฎหมายวีพิจารณาความอาญา พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม และศึกษาวิทยานิพนธ์ที่เกี่ยวข้องกับพยานหลักฐานทางอิเล็กทรอนิกส์ในประเทศไทย

2. การรวบรวมข้อมูลเชิงคุณภาพด้วยแบบสัมภาษณ์ โดยมีรูปแบบเป็นการสัมภาษณ์เชิงลึก (In-depth Interview) คือ การพูดคุย สัมภาษณ์ ซักถามเพื่อให้ได้คำตอบ

3) เครื่องมือการวิจัย

การวิจัยนี้ใช้แนวทางการวิจัยเชิงคุณภาพ โดยแบ่งวิธีการศึกษาออกเป็น 2 ส่วน คือ การศึกษาเอกสารและการสัมภาษณ์เชิงลึก โดยมีรายละเอียดดังนี้

1. ศึกษาพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม ประมวลกฎหมายวิธีพิจารณาความอาญา เพื่อรวบรวมข้อมูลที่เกี่ยวกับอำนาจของพนักงานเจ้าหน้าที่ในการเข้าถึงข้อมูลหลักฐานทางอิเล็กทรอนิกส์

2. แบบสอบถาม (Questionnaire) ใช้สอบถามกับเจ้าหน้าที่ของหน่วยงานที่เกี่ยวข้องกับการบังคับใช้กฎหมายในประเทศไทย จำนวน 3 หน่วยงาน ประกอบด้วย กรมสอบสวนคดีพิศษ สำนักงานพิสูจน์หลักฐานตำรวจ สำนักงานตำรวจแห่งชาติ และกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.)

4) การวิเคราะห์ข้อมูล

ผู้วิจัยทำการศึกษากฎหมายการเข้าถึงข้อมูลหลักฐานทางอิเล็กทรอนิกส์ของพนักงานเจ้าหน้าที่ผู้ปฏิบัติงานในหน่วยงานที่เกี่ยวข้องกับงานนิติวิทยาศาสตร์ในประเทศไทย ได้แก่ ประมวลกฎหมายวิธีพิจารณาความอาญา พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม ซึ่งเน้นศึกษาเกี่ยวกับขั้นตอนการเข้าถึงเข้าถึงข้อมูลหลักฐานทางอิเล็กทรอนิกส์ โดยมีสาระสำคัญดังนี้

รัฐธรรมนูญแห่งราชอาณาจักรไทย มาตรา 25 กำหนดไว้ว่า สิทธิและเสรีภาพของปวงชนชาวไทยนอกจากที่บัญญัติคุ้มครองไว้เป็นการเฉพาะในรัฐธรรมนูญแล้ว การใดที่มิได้ห้ามหรือจำกัดไว้ในรัฐธรรมนูญ

หรือในกฎหมายอื่น บุคคลย่อมมีสิทธิและเสรีภาพที่จะทำการนั้นได้และได้รับความคุ้มครองตามรัฐธรรมนูญ ตราบเท่าที่การใช้สิทธิหรือเสรีภาพเช่นว่านั้นไม่กระทบกระเทือนหรือเป็นอันตรายต่อความมั่นคงของรัฐ ความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน และไม่ละเมิดสิทธิหรือเสรีภาพของบุคคลอื่น ดังนั้น สิทธิและเสรีภาพของบุคคลย่อมได้รับการคุ้มครองโดยกฎหมาย ตลอดจนทรัพย์สินของบุคคลนั้น ๆ ที่มีสิทธิครอบครองหรือกรรมสิทธิ์ในตัวทรัพย์สินนั้นด้วย ผู้ใดจะกระทำการละเมิดสิทธิและเสรีภาพของบุคคลอื่นไม่ได้

ประมวลกฎหมายวิธีพิจารณาความอาญา ได้กำหนดอำนาจหน้าที่ของพนักงานสอบสวนในการรวบรวมพยานหลักฐาน ตามมาตรา 131 บัญญัติไว้ว่า ให้พนักงานสอบสวนรวบรวมหลักฐานทุกชนิด เท่าที่สามารถจะทำได้ เพื่อประสงค์จะทราบข้อเท็จจริงและพฤติการณ์ต่าง ๆ อันเกี่ยวกับความผิดที่ถูกกล่าวหา เพื่อจะรู้ตัวผู้กระทำผิดและพิสูจน์ให้เห็นความผิดหรือความบริสุทธิ์ของผู้ต้องหา ซึ่งเป็นช่องว่างทางกฎหมายให้พนักงานสอบสวนในการใช้ดุลพินิจที่จะรวบรวมพยานหลักฐานหรือไม่รวบรวมพยานหลักฐานก็ได้ เนื่องจากกฎหมายกำหนดไว้ว่า “เท่าที่สามารถจะทำได้” จึงไม่ได้เป็นการบังคับให้พนักงานสอบสวนจะต้องดำเนินการทำเสมอไป แต่เป็นการใช้ดุลพินิจในการที่จะรวบรวมหรือไม่รวบรวมพยานหลักฐานเพื่อให้ทราบข้อเท็จจริงและพฤติการณ์แห่งคดีเท่านั้น ตราบเท่าที่จะกระทำได้ และมาตรา 131/1 วรรคแรก ยังได้บัญญัติเกี่ยวกับพยานหลักฐานทางวิทยาศาสตร์เอาไว้ด้วยว่า ในกรณีที่จำเป็นต้องใช้พยานหลักฐานทางวิทยาศาสตร์ เพื่อพิสูจน์ข้อเท็จจริงตามมาตรา 131 ให้พนักงานสอบสวนมีอำนาจให้ทำการตรวจพิสูจน์บุคคล วัตถุ หรือเอกสารใด ๆ โดยวิธีการทางวิทยาศาสตร์ได้ ก็เป็นการกำหนดข้อกฎหมายไว้อย่างกว้างให้พนักงานสอบสวนทำการตรวจพยานหลักฐานทางวิทยาศาสตร์ได้ แต่ไม่ได้มีการกำหนดขั้นตอน รูปแบบ หรือวิธีการไว้เป็นการเฉพาะ ทำให้มีการตรากฎหมายออกมาหลายฉบับ ตามแต่ละหน่วยงานก็มีการตรากฎหมาย ระเบียบ ข้อบังคับ เพื่อใช้ในการรวบรวมพยานหลักฐาน ตรวจพิสูจน์ของหน่วยงานตนเองไว้เป็นการเฉพาะ แต่ละฉบับกำหนดวิธีการได้มา อำนาจหน้าที่ที่แตกต่างกัน ส่งผลให้เจ้าหน้าที่ผู้ปฏิบัติงานจริงมีความสับสนว่าตนเองต้องใช้อำนาจตามกฎหมายฉบับใด ดังนั้น การบัญญัติอำนาจหน้าที่ของพนักงานสอบสวนในการรวบรวมพยานหลักฐานตามมาตรา 131 แห่งประมวลวิธีพิจารณาความอาญา นั้นกว้างจนเกินไป อีกทั้งยังให้เป็นดุลพินิจของพนักงานสอบสวนอีกด้วยว่าจะกระทำหรือไม่กระทำ ตราบเท่าที่สามารถจะทำได้

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม ในแนวทางนี้ได้แบ่งการปฏิบัติงานออกเป็น 2 ส่วนดังนี้

ส่วนที่หนึ่ง อำนาจหน้าที่ตามมาตรา 18 ของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ได้กำหนดให้การสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิด พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

(1) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดมาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(2) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง

(3) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา 26 หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่หรือให้เก็บข้อมูลดังกล่าวไว้ก่อน

(4) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิด ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

(5) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

(6) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

(7) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับ

(8) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิด

ส่วนวรรคสอง เป็นการบัญญัติข้อกฎหมายที่ตัดอำนาจของพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ว่าหากมีการกระทำความผิดอันเกิดจากการใช้ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์เป็นองค์ประกอบหรือเป็นส่วนหนึ่งในการกระทำความผิดหรือมีข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับการกระทำความผิดอาญาตามกฎหมายอื่นนั้น ให้พนักงานสอบสวนมีคำร้องขอให้พนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ดำเนินการตามมาตรา 18 (1) – (8) หากแต่บางครั้งพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญาอาจเป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้ในคราวเดียวกัน เนื่องจากการที่จะได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่ได้นั้น ต้องเป็นผู้ที่ได้รับการเข้าฝึกอบรมซึ่งจัดการฝึกอบรมโดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และได้รับการแต่งตั้งจากรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม จึงจะสามารถเป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้

ส่วนที่สอง อำนาจหน้าที่ตามมาตรา 19 ได้กำหนดเอาไว้ว่า การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา 18 (4) - (8) ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้

พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำการอย่างหนึ่งอย่างใดอันเป็นความผิด เหตุที่ต้องใช้อำนาจ ลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิด เท่าที่สามารถจะระบุได้ ประกอบคำร้องด้วย ในการพิจารณาคำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็ว ดังนั้น หากการที่พนักงานเจ้าหน้าที่จะใช้อำนาจตามมาตรา 18 (4) – (8) อันเกี่ยวกับการการตรวจสอบ ทำสำเนาข้อมูล ถอดรหัส หรือกระทำการใด ๆ เกี่ยวกับระบบคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ จำเป็นต้องยื่นคำร้องต่อศาลที่มีเขตอำนาจ กล่าวคือ อุปกรณ์อิเล็กทรอนิกส์หรือระบบคอมพิวเตอร์ที่ต้องสงสัยว่าได้มีการกระทำความผิดตั้งอยู่ในพื้นที่ใด ก็ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่อุปกรณ์หรือคอมพิวเตอร์นั้นตั้งอยู่ อันเป็นเขตพื้นที่ของการกระทำความผิดและเขตอำนาจของศาลที่มีอำนาจพิจารณาออกคำสั่งตามคำร้อง นั้น

หลักการให้ความยินยอม ความยินยอมของผู้เสียหายในคดีอาญา คือ หลักความยินยอมอันบริสุทธิ์ของผู้เสียหายเป็นเหตุยกเว้นความผิดอาญามีหลักเกณฑ์ 3 หลักเกณฑ์ดังนี้

(1) ความยินยอมนั้นต้องมีอยู่อย่างน้อยในขณะกระทำการอันกฎหมายบัญญัติเป็นความผิด

(2) ความยินยอมนั้นต้องเป็นความยินยอมอันบริสุทธิ์

(3) ความยินยอมนั้นต้องไม่ขัดต่อความความสงบเรียบร้อยหรือศีลธรรมอันดี

คำพิพากษาศาลฎีกาที่ 1403/2508 ได้วินิจฉัยวางบรรทัดฐานเอาไว้ว่า การยอมความในความผิดอันยอมความได้ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 35 วรรคสอง และ 39 (2) นั้น เป็นการกระทำภายหลังที่ความผิดได้เกิดขึ้นแล้ว มิใช่การที่จะกระทำกันไว้ล่วงหน้าก่อนการกระทำผิดข้อตกลงล่วงหน้าก่อนมีการกระทำผิดจะถือเป็นการยอมความตามบทกฎหมายดังกล่าวแล้วไม่ได้ และบุคคลจะตกลงกันไว้ก่อนว่าจะไม่ฟ้องคดีอาญา ถ้าหากจะมีการกระทำผิดเกิดขึ้นต่อไปข้างหน้านั้น ข้อตกลงนั้นก็หามีผลก่อให้เกิดหนี้ที่จะผูกพันคู่กรณีให้จำต้องงดเว้นไม่ฟ้องคดีอาญาเช่นว่านั้นแต่ประการใดไม่ เพราะอำนาจฟ้องคดีอาญาจะมีอยู่หรือไม่ นั้น มิได้อยู่ภายใต้บังคับของกฎหมายลักษณะหนี้ในทางแพ่ง หากอยู่ภายใต้บังคับของกฎหมายว่าด้วยวิธีพิจารณาความอาญาอีกส่วนหนึ่ง แต่อย่างไรก็ดี ข้อตกลงว่าจะไม่ฟ้องคดีอาญานั้น อาจถือเป็นความยินยอมให้กระทำการที่ตามปกติต้องด้วยบทบัญญัติว่าเป็นความผิดได้มีหลักกฎหมายทั่วไปเป็นเหตุยกเว้นความผิดอาญาอยู่ตามฎีกาที่ 616/2482 และ 787/2483 ว่า ความยินยอมอันบริสุทธิ์ของผู้เสียหายให้ผู้ใดกระทำการที่กฎหมายบัญญัติว่าเป็นความผิดนั้นถ้าความยินยอมนั้นไม่ขัดต่อความสำนึกในศีลธรรมอันดีและมีอยู่จนถึงขณะกระทำการอันกฎหมายบัญญัติว่าเป็นความผิดนั้นแล้วความยินยอมนั้นย่อมเป็นข้อยกเว้นมิให้การกระทำนั้นเป็นความผิดขึ้นได้

ผู้ให้การยินยอมจะต้องมีความสามารถในการให้ความยินยอม กล่าวคือ บุคคลผู้ให้ความยินยอมจะต้องมีสภาพความเป็นบุคคลตามมาตรา 15 แห่งประมวลกฎหมายแพ่งและพาณิชย์ คือ สภาพบุคคลย่อมเริ่มแต่เมื่อคลอดแล้วอยู่รอดเป็นทารกและสิ้นสุดลงเมื่อตาย ทารกในครรภ์มารดาก็สามารถมีสิทธิต่าง ๆ ได้ หากว่าภายหลังคลอดแล้วอยู่รอดเป็นทารก และการให้ความยินยอมผู้ให้ความยินยอมต้องสามารถ

รับรู้และเข้าใจได้ว่ากระทำการสิ่งใด ดังนั้น การให้ความยินยอมจึงเป็นสิทธิ์เฉพาะตัวของบุคคลใดบุคคลหนึ่งที่กฎหมายได้รับรองไว้ ยินยอมให้บุคคลอื่นเข้ามากระทำการในสิทธิ์ของตนเอง

5) การนำระบบคลาวด์มาใช้สนับสนุนการเข้าถึงพยานหลักฐาน

เทคโนโลยีคลาวด์ เป็นตัวกลางในการจัดเก็บข้อมูลขนาดใหญ่บนอินเทอร์เน็ตผ่านไปยัง cloud-based servers ที่ผู้ใช้งานสามารถเข้าถึงข้อมูลตนเองได้ ผ่านอุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ ได้ในทุกที่ทุกเวลา และเทคโนโลยีคลาวด์คอมพิวติ้ง (Cloud Computing) ซึ่งเป็นแนวคิดของการใช้เทคโนโลยีที่ดึงสมรรถนะจากคอมพิวเตอร์หลาย ๆ ตัวจากสถานที่ต่างกัน นำมาประมวลผลในลักษณะคล้ายกลุ่มเมฆ ซึ่งมีเซิร์ฟเวอร์จำนวนมหาศาลตั้งอยู่ในที่เดียวกัน และถูกส่งขึ้นไปเก็บในส่วนกลาง กลุ่มเมฆจะต่อเชื่อมเข้าหากันด้วยเครือข่ายเป็นระบบกริด (Grid) โดยทำการจำลองกลุ่ม CPU ขึ้นมาเพื่อให้ผู้ใช้ได้ใช้งานตามต้องการ CPU จะถูกบริหารจัดการโดยซอฟต์แวร์ที่สามารถปรับเปลี่ยนรูปแบบตัวเองให้เหมาะกับสภาพการใช้งาน ผู้ใช้จำนวนมากจึงได้รับความรวดเร็วในการใช้งานหรือเกิดความคล่องตัว โดยที่ระบบคลาวด์คอมพิวติ้ง (Cloud Computing) มีรูปแบบหลัก ๆ ด้วยกัน 3 แบบ ได้แก่

1) Software as a Service (SaaS) เป็นการที่ผู้ให้บริการระบบซอฟต์แวร์เป็นผู้ดูแลและบริหารจัดการประมวลผลในรูปแบบของการใช้งานซอฟต์แวร์ผ่านเว็บบราวเซอร์จากที่ใดก็ได้ผ่านอุปกรณ์อิเล็กทรอนิกส์ ซึ่งบริการ Software as a Service (SaaS) ที่ใกล้ตัวเรามากที่สุด ได้แก่ Google Apps, Dropbox และ Slack แอปพลิเคชันเหล่านี้ได้รับการจัดการโดยผู้ให้บริการคลาวด์ทั้งหมด

2) Platform as a Service (PaaS) เป็นบริการแพลตฟอร์มบนคลาวด์ ที่มี framework หรือเครื่องมือเพื่อช่วยให้นักพัฒนาสามารถพัฒนาซอฟต์แวร์หรือแอปพลิเคชันต่าง ๆ ได้อย่างสะดวก รวดเร็วและปรับเปลี่ยนได้ตามต้องการตามความเหมาะสม ตัวอย่าง PaaS เช่น Google App Engine (GAE) และ Heroku เป็นต้น

3) Infrastructure as a Service (IaaS) เป็นบริการโครงสร้างพื้นฐานระบบไอทีสำหรับองค์กร โดยให้บริการเกี่ยวกับ Virtual Machine (VMs) ที่ประกอบไปด้วย CPU, memory, storage และ networking โดยที่ลูกค้าสามารถกำหนดขนาดความจุให้เหมาะสมกับความต้องการได้เอง ตัวอย่าง IaaS เช่น Microsoft Azure, AWS EC2, Google Compute Engine (GCE) เป็นต้น

การพิสูจน์หลักฐานทางอิเล็กทรอนิกส์บนคลาวด์ เป็นการนำเอาหลักการทางวิทยาศาสตร์ การปฏิบัติทางเทคโนโลยี และวิธีการสกัดและตรวจสอบเพื่อสร้างเหตุการณ์ในระบบคลาวด์ผ่านการระบุตัวตน การเก็บและรักษา การตรวจสอบ และการจัดทำรายงานพยานหลักฐานทางอิเล็กทรอนิกส์ โดยขั้นตอนในการเก็บรวบรวมและรักษาพยานหลักฐานทางอิเล็กทรอนิกส์ แบ่งได้ 3 ขั้นตอน ได้แก่

1) การรวบรวมพยานหลักฐานจากผู้เสียหายซึ่งเป็นวัตถุพยานต้นทางในกระบวนการหาตัวผู้กระทำผิด

2) การรวบรวมพยานหลักฐานจากผู้ให้บริการอินเทอร์เน็ต ตามที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2558 และที่แก้ไขเพิ่มเติม มาตรา 26 บัญญัติไว้ว่า ผู้ให้บริการ

ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินสองปีเป็นกรณีพิเศษ เฉพาะรายและเฉพาะคราวก็ได้

3) การรวบรวมพยานหลักฐานจากผู้กระทำผิด ซึ่งเป็นวัตถุพยานปลายทางที่เป็นข้อมูลของผู้กระทำผิด

ผลการวิจัย

ผู้วิจัยได้ทำการสัมภาษณ์ผู้ให้ข้อมูลหลักของแต่ละหน่วยงาน หน่วยงานละ 4 คน โดยใช้แบบสัมภาษณ์เชิงลึกที่ผู้วิจัยเป็นผู้จัดทำขึ้น (ภาคผนวก ก) โดยคำถามแบ่งออกเป็น 4 ส่วน ซึ่งผลการสัมภาษณ์ผู้วิจัยได้ทำการสรุปข้อมูลจากการสัมภาษณ์ผู้ให้ข้อมูลหลักของแต่ละหน่วยงานและได้วิเคราะห์ข้อมูลการสัมภาษณ์ผู้ให้ข้อมูลหลักเกี่ยวกับปัญหาการเข้าถึงข้อมูลหลักฐานทางอิเล็กทรอนิกส์ของพนักงานเจ้าหน้าที่ผู้ปฏิบัติงานในหน่วยงานที่เกี่ยวข้องกับงานนิติวิทยาศาสตร์ในประเทศไทย โดยมีรายละเอียดดังนี้

1. ประวัติส่วนบุคคลและประวัติการทำงานอย่างย่อของผู้ถูกสัมภาษณ์

จากการสัมภาษณ์ผู้ให้ข้อมูลหลักของหน่วยงานที่เกี่ยวข้องกับงานนิติวิทยาศาสตร์ในประเทศไทย จำนวน 3 หน่วยงาน หน่วยงานละ 4 คน รวมเป็น 12 คน และต้องเป็นผู้มีความรู้ความสามารถและมีประสบการณ์การทำงานในด้านพิสูจน์หลักฐานทางอิเล็กทรอนิกส์ไม่ต่ำกว่า 5 ปี พบว่าผู้ให้ข้อมูลหลักเป็นเพศชายจำนวน 9 คน และเพศหญิงจำนวน 3 คน มีช่วงอายุระหว่างไม่เกิน 30 - 60 ปี โดยผู้ให้ข้อมูลส่วนใหญ่มีประสบการณ์การทำงานในด้านพิสูจน์หลักฐานทางอิเล็กทรอนิกส์อย่างน้อย 3 - 5 ปี ขึ้นไป โดยมีข้อมูลการสัมภาษณ์ผู้ให้ข้อมูลหลักดังตารางที่ 1

ตารางที่ 1 ข้อมูลการสัมภาษณ์ผู้ให้ข้อมูลหลักของหน่วยงานที่เกี่ยวข้องกับงานนิติวิทยาศาสตร์ในประเทศไทยถึงประวัติส่วนตัวและประวัติการทำงานอย่างย่อของผู้ถูกสัมภาษณ์

ลำดับ	หน่วยงาน	ประวัติส่วนบุคคลและประวัติการทำงานอย่างย่อของผู้ถูกสัมภาษณ์
1.	สำนักงานพิสูจน์หลักฐานตำรวจ สำนักงานตำรวจแห่งชาติ	ผู้ให้ข้อมูล จำนวน 4 ราย ช่วงอายุระหว่าง 31 – 50 ปี แบ่งออกเป็นเพศชาย 2 ราย เพศหญิง 2 ราย ผู้ให้ข้อมูลจำนวน 3 ราย มีประสบการณ์การทำงานในด้านพิสูจน์หลักฐานทางอิเล็กทรอนิกส์อย่างน้อย 4 ปี ขึ้นไป ซึ่งมีผู้ให้ข้อมูล จำนวน 1 ราย มีประสบการณ์การทำงานในด้านพิสูจน์หลักฐานทางอิเล็กทรอนิกส์อย่างน้อย 12 ปี ขึ้นไป
2.	กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.)	ผู้ให้ข้อมูล จำนวน 4 ราย ช่วงอายุต่ำกว่า 30 – 50 ปี เป็นเพศชาย จำนวน 4 ราย ผู้ให้ข้อมูลจำนวน 3 ราย มีประสบการณ์การทำงานในด้านพิสูจน์หลักฐานทางอิเล็กทรอนิกส์อย่างน้อย 5 – 10 ปี ขึ้นไป ซึ่งมีผู้ให้ข้อมูล

ลำดับ	หน่วยงาน	ประวัติส่วนบุคคลและประวัติการทำงานอย่างย่อของผู้ถูกสัมภาษณ์
		จำนวน 1 ราย มีประสบการณ์การทำงานในด้านพิสูจน์หลักฐานทางอิเล็กทรอนิกส์อย่างน้อย 2 ปี ขึ้นไป
3.	กรมสอบสวนคดีพิเศษ (DSI)	ผู้ให้ข้อมูล จำนวน 4 ราย ช่วงอายุต่ำกว่า 30 – 50 ปี แบ่งออกเป็นเพศชาย จำนวน 3 ราย เพศหญิง จำนวน 1 ราย ช่วงอายุต่ำกว่า 30 – 50 ปี ผู้ให้ข้อมูลจำนวน 3 ราย มีประสบการณ์การทำงานในด้านพิสูจน์หลักฐานทางอิเล็กทรอนิกส์อย่างน้อย 10 - 15 ปี ขึ้นไป ซึ่งมีผู้ให้ข้อมูลจำนวน 1 ราย มีประสบการณ์การทำงานในด้านพิสูจน์หลักฐานทางอิเล็กทรอนิกส์อย่างน้อย 4 ปี ขึ้นไป
	รวมทั้งสิ้น	**12 ราย**

2. ข้อมูลสภาพปัญหาในการเข้าถึงข้อมูลหลักฐานทางอิเล็กทรอนิกส์ ในส่วนนี้จะแบ่งออกเป็น 2 ข้อย่อย โดยสรุปข้อมูลจากการสัมภาษณ์ผู้ให้ข้อมูลหลักดังนี้

2.1 ผู้เชี่ยวชาญมีปัญหาเกี่ยวกับการเข้าถึงข้อมูลหลักฐานทางอิเล็กทรอนิกส์หรือไม่ มากน้อยเพียงใด และเป็นปัญหาในเรื่องใดตามลำดับของปัญหา

จากการสัมภาษณ์ผู้ให้ข้อมูลหลักที่ทำหน้าที่เกี่ยวข้องกับการตรวจพิสูจน์หลักฐานทางดิจิทัล พบว่าผู้ให้ข้อมูลหลักพบเจอปัญหาที่เกี่ยวข้องกับการเข้าถึงข้อมูลหลักฐานทางอิเล็กทรอนิกส์ ดังนี้

1) ผู้ให้ข้อมูลหลักส่วนใหญ่มีความคิดเห็นที่สอดคล้องกันว่า หลักสิทธิเสรีภาพตามกฎหมายรัฐธรรมนูญมาตรา 25 อันได้รับการคุ้มครอง ผู้ใดจะละเมิดสิทธิและเสรีภาพของตนเองนั้นไม่ได้ การให้ความยินยอมของผู้ต้องหาหรือผู้กระทำความผิดในการเข้าถึงข้อมูลหลักฐานทางอิเล็กทรอนิกส์ก็เช่นเดียวกัน ทำให้เกิดปัญหาต่อเจ้าหน้าที่ผู้ปฏิบัติงานตรวจ กล่าวคือ เมื่อมีการยึดอุปกรณ์ที่ใช้ในการกระทำความผิด เช่น โทรศัพท์มือถือมีการเข้ารหัส แม้จะตรวจยึดมาได้พนักงานเจ้าหน้าที่ก็ไม่สามารถเข้าดูข้อมูลได้เนื่องจากอุปกรณ์ได้มีการเข้ารหัสเอาไว้

2) ผู้ให้ข้อมูลหลักบางส่วนพบเจอปัญหาการเข้าถึงข้อมูลที่มีการจัดเก็บอยู่ในรูปแบบของระบบคลาวด์ (Cloud) การเข้าถึงข้อมูลหลักฐานทางอิเล็กทรอนิกส์จึงต้องดำเนินการประสานไปยังผู้ให้บริการ (service provider) เพื่อขอให้อนุญาตให้พนักงานเจ้าหน้าที่สามารถเข้าถึงข้อมูลดังกล่าวได้ ซึ่งหากเป็นกรณีที่มีการจัดเก็บในระบบคลาวด์ (Cloud) ของแอปเปิล (Apple) ที่มีระบบรักษาความปลอดภัย หรือระบบของ Samsung ที่มีการสร้างระบบรักษาความปลอดภัยที่เรียกว่า Samsung nock สิ่งเหล่านี้ถือว่าเป็นความเป็นส่วนตัว (privacy) ที่ผู้ให้บริการต้องรักษาความลับของลูกค้า ส่งผลให้การดำเนินการตรวจสอบของพนักงานเจ้าหน้าที่ไม่สามารถเข้าถึงข้อมูลได้ แม้จะมีการร้องขอไปยังเจ้าของผู้ให้บริการก็ตาม เช่นเดียวกับกรณีที่มีการตรวจสอบแอคเคาท์ (Account) บนแพลตฟอร์ม (Platfotm) สื่อโซเชียล

มีเดีย (social media) เมื่อพนักงานเจ้าหน้าที่มีการร้องขอไปยังผู้ให้บริการในประเทศไทยว่าจะดำเนินการตรวจสอบแอคเคาท์เหล่านั้น ผู้ให้บริการกลับทำการแบนหรือลบแอคเคาท์ดังกล่าวนั้นทิ้งออกจากระบบ ทำให้ไม่สามารถดำเนินการตรวจสอบเข้าถึงข้อมูลได้เลย เพราะไม่มีแอคเคาท์ที่อยู่ในระบบที่สามารถเปิดเข้ามาตรวจสอบข้อมูลภายในได้

3) ผู้ให้ข้อมูลหลักบางส่วนเป็นเพียงเจ้าหน้าที่ผู้สนับสนุนการดำเนินงานของพนักงานสอบสวน พนักงานเจ้าหน้าที่พบเจอปัญหาในด้านระยะเวลาของการปฏิบัติงานที่มีความเร่งรีบไม่สอดคล้องกับปริมาณงานที่จำเป็นต้องตรวจสอบ ประกอบกับอุปกรณ์ที่จะต้องใช้ในการสำเนาข้อมูลก่อนนำมาตรวจสอบไม่เพียงพอ

4) ผู้ให้ข้อมูลหลักส่วนใหญ่เป็นนักวิทยาศาสตร์ซึ่งไม่ได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ แต่อาศัยอำนาจของพนักงานสอบสวนตามประมวลวิธีพิจารณาความอาญาในการปฏิบัติงาน ส่งผลให้วัตถุพยานที่พนักงานสอบสวนส่งมาให้ทำการตรวจสอบอาจมีปัญหาในด้านการรวบรวมพยานหลักฐานที่ไม่ถูกต้อง เช่น การตรวจยึดโทรศัพท์มือถือที่มีการเข้ารหัส ไม่ดำเนินการขอความยินยอมจากเจ้าของโทรศัพท์มือถือให้ส่งรหัสการเข้าถึงมาด้วย ทำให้นักวิทยาศาสตร์ไม่สามารถเข้าตรวจสอบได้ หรือจัดเก็บวัตถุพยานไม่เป็นไปตามห่วงโซ่การครอบครองพยานหลักฐาน (Chain of custody)

5) ผู้ให้ข้อมูลหลักส่วนใหญ่มีความคิดเห็นที่สอดคล้องกันว่า มีปัญหาการขาดแคลนบุคลากรด้านนิติวิทยาศาสตร์ ที่มีความรู้ความสามารถในการปฏิบัติงานด้านตรวจพิสูจน์หลักฐานดิจิทัล

2.2 ปัจจัยที่มีอิทธิพลที่ทำให้ท่านประสบปัญหาเกี่ยวกับการเข้าถึงข้อมูลหลักฐานทางอิเล็กทรอนิกส์ มีอะไรบ้างและมีอิทธิพลอย่างไร

จากการสัมภาษณ์ผู้ให้ข้อมูลหลักพบว่าปัจจัยหลักที่ทำให้เกิดปัญหาเกี่ยวกับการเข้าถึงข้อมูลหลักฐานทางอิเล็กทรอนิกส์ มีอยู่ 5 ปัจจัย ได้แก่

1) ปัจจัยด้านกฎหมาย ผู้ให้ข้อมูลหลักส่วนใหญ่มีความคิดเห็นที่สอดคล้องกันว่า พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม ให้อำนาจพนักงานเจ้าหน้าที่กระทำการเข้าถึงข้อมูลหลักฐานทางอิเล็กทรอนิกส์ที่มีการเข้ารหัสได้หากผู้กระทำความผิดให้ความยินยอม ซึ่งการให้ความยินยอมเข้าถึงรหัสของอุปกรณ์เป็นสิทธิ์เฉพาะตัวไม่สามารถบังคับได้ เมื่ออุปกรณ์ที่การเข้ารหัสเอาไว้และไม่ได้รับความยินยอม แม้จะได้มาโดยชอบด้วยกฎหมายแต่ก็ไม่สามารถเข้าถึงข้อมูลหลักฐานทางอิเล็กทรอนิกส์ได้ เพราะมีการเข้ารหัสเอาไว้ ซึ่งตามมาตรา 18 (7) บัญญัติไว้ว่า ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว ฉะนั้น จึงไม่อาจทำการตรวจสอบได้หากเจ้าของหรือผู้เกี่ยวข้องกับรหัสลับไม่ให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับ

2) ปัจจัยด้านเทคโนโลยี ผู้ให้ข้อมูลหลักส่วนใหญ่มีความคิดเห็นที่สอดคล้องกันว่า เทคโนโลยีมีการอัพเดทเวอร์ชัน (update version) อยู่ตลอดเวลา ส่งผลให้พนักงานเจ้าหน้าที่ผู้ปฏิบัติงานไม่สามารถตรวจสอบหรือเข้าถึงข้อมูลได้ เนื่องจากอุปกรณ์ที่ใช้ในการตรวจสอบมีเวอร์ชัน (version) ที่ล่าช้ากว่า การดำเนินการอัพเดท (update) อุปกรณ์ที่ใช้ในการตรวจสอบต้องผ่านการอนุมัติจากต้นสังกัดเพื่อดำเนินการจัดซื้อจัดจ้างหรือต่อใบอนุญาต (license)

3) ปัจจัยด้านอำนาจหน้าที่ ผู้ให้ข้อมูลหลักส่วนใหญ่ไม่ใช้พนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งการที่จะได้รับการแต่งตั้งให้เป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้นั้น ต้องผ่านการฝึกอบรมของทางกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และได้รับแต่งตั้งจากรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม จึงจะได้รับบัตรพนักงานเจ้าหน้าที่ ส่งผลให้เวลาปฏิบัติงานจริงผู้ทำหน้าที่ตรวจสอบและเข้าถึงข้อมูลหลักฐานทางอิเล็กทรอนิกส์ไม่ใช่พนักงานเจ้าหน้าที่ที่ได้รับแต่งตั้ง ทำให้มีความกังวลใจหากต้องไปเป็นพยานในชั้นศาลและศาลถามว่าใช้อำนาจอะไรในการเข้าถึงพยานหลักฐาน

4) ปัจจัยด้านระยะเวลา ผู้ให้ข้อมูลหลักบางส่วนพบเจอปัญหาด้านระยะเวลาที่ใช้ในการตรวจสอบและเข้าถึงข้อมูล เนื่องจากอุปกรณ์ที่ได้รับมาต้องสำเนาข้อมูลเป็นจำนวนมากและมีกรอบระยะเวลาของการปฏิบัติงานที่สั้น ส่งผลให้ต้องดำเนินการเร่งรีบซึ่งไม่สอดคล้องกับอุปกรณ์ที่มีให้ใช้อย่างไม่เพียงพอ

5) ปัจจัยด้านงบประมาณและบุคลากร ผู้ให้ข้อมูลหลักส่วนใหญ่มีความคิดเห็นที่สอดคล้องกันว่า ปัจจัยด้านงบประมาณในการจัดสรรอุปกรณ์ที่นำมาใช้ตรวจสอบมีอย่างจำกัด ไม่เพียงพอต่อการจัดเก็บข้อมูลที่มีจำนวนมาก และบุคลากรที่มีคุณสมบัติที่ตรงกับการปฏิบัติงานด้านนิติวิทยาศาสตร์ทางคอมพิวเตอร์มีจำนวนไม่เพียงพอ บางครั้งประสบปัญหาต้องยืมเจ้าหน้าที่ที่มีความรู้ความสามารถใกล้เคียงกับการปฏิบัติงานด้านคอมพิวเตอร์มาช่วยเหลือซึ่งทำให้มีปัญหาว่าอาจไม่มีความรู้ความเข้าใจในรูปแบบและโครงสร้างของข้อมูล ส่งผลให้การตรวจสอบและเข้าถึงไม่มีประสิทธิภาพอย่างเพียงพอ

3. แนวทางการป้องกันการเกิดปัญหาเกี่ยวกับการเข้าถึงข้อมูลหลักฐานทางอิเล็กทรอนิกส์

จากการสัมภาษณ์ผู้ให้ข้อมูลหลักพบว่าผู้ให้ข้อมูลหลักส่วนใหญ่มีแนวทางแก้ไขที่คล้ายคลึงกันดังนี้

1) จัดหลักสูตรให้ความรู้แก่เจ้าหน้าที่ตำรวจที่ประจำสถานีตำรวจทุกพื้นที่ทุกระดับ ให้มีความรู้เบื้องต้นเกี่ยวกับการตรวจเก็บพยานหลักฐานทางอิเล็กทรอนิกส์อย่างถูกต้อง ตลอดจนทั้งสร้างความรู้ความเข้าใจแก่ผู้บริหารทุกหน่วยงานเกี่ยวกับพยานหลักฐานทางอิเล็กทรอนิกส์ว่ามีความแตกต่างกับพยานหลักฐานทั่วไป

2) จัดอบรมให้แก่เจ้าหน้าที่ผู้ปฏิบัติงานด้านนิติวิทยาศาสตร์อย่างสม่ำเสมอและเป็นประจำ เพื่อให้เกิดการเรียนรู้และพัฒนางานอยู่ตลอดเวลา

3) จัดสรรงบประมาณให้มีอุปกรณ์ในการปฏิบัติงานอย่างเพียงพอ อัพเดทอุปกรณ์ให้มีความทันสมัยเป็นปัจจุบัน และจัดหาบุคลากรที่มีคุณสมบัติให้ตรงกับการปฏิบัติงาน

4) ผลักดันให้เกิดการสร้างห้องปฏิบัติการที่มีมาตรฐานได้รับการรองรับ ISO เพื่อยกระดับการปฏิบัติงานให้มีมาตรฐานมากยิ่งขึ้น

4. ข้อเสนอแนะที่เกี่ยวกับการเข้าถึงข้อมูลหลักฐานทางอิเล็กทรอนิกส์

ในส่วนของข้อเสนอแนะนั้นผู้ให้ข้อมูลหลักส่วนใหญ่มีความคิดเห็นที่คล้ายคลึงกัน และสามารถสรุปข้อเสนอแนะอื่น ๆ ได้ดังนี้

1) เสนอให้มีการจัดอบรมเจ้าหน้าที่ผู้ปฏิบัติงานอย่างสม่ำเสมอและเป็นประจำ ตลอดจนเปิดหลักสูตรการเรียนการสอนหรือสัมมนาวิชาการให้พนักงานสอบสวนหรือเจ้าหน้าที่ตำรวจทุกระดับทั่วประเทศให้ได้รับความรู้เกี่ยวกับการตรวจยึดพยานหลักฐานทางอิเล็กทรอนิกส์ การจัดเก็บและรวบรวมพยานหลักฐานตามแบบห่วงโซ่การครอบครองพยานหลักฐาน (Chain of custody) เพื่อที่จะทำให้เจ้าหน้าที่พิสูจน์หลักฐานทางนิติวิทยาศาสตร์ สามารถดำเนินการตรวจพิสูจน์หลักฐานได้อย่างถูกต้อง รวดเร็ว และไม่เกิดการปนเปื้อน อีกทั้ง สร้างความเข้าใจให้กับผู้บริหารระดับสูงในการเข้าใจเรื่องพยานหลักฐานทางอิเล็กทรอนิกส์แตกต่างจากพยานหลักฐานทั่วไป เพื่อป้องกันการดำเนินการที่อาจทำให้พยานหลักฐานเกิดความเสียหาย

2) จัดหางบประมาณในการจัดซื้ออุปกรณ์ให้มีความเพียงพอต่อการตรวจสอบพยานหลักฐาน เนื่องจากพยานหลักฐานทางอิเล็กทรอนิกส์มีข้อมูลเป็นจำนวนมากและใช้ระยะเวลานานในการสำเนาข้อมูล แต่อุปกรณ์มีจำนวนจำกัดไม่เพียงพอต่อปริมาณงานที่มีจำนวนมาก

สรุปและอภิปรายผล

1. สรุปผลการศึกษาเอกสาร

1) ประมวลกฎหมายวิธีพิจารณาความอาญา ผลการศึกษาพบว่าพนักงานสอบสวนมีอำนาจที่จะดำเนินการรวบรวมพยานหลักฐานได้เท่าที่สามารถจะทำได้ โดยให้เป็นดุลพินิจของแต่ละบุคคลในการตัดสินใจว่าจะดำเนินการรวบรวมพยานหลักฐานข้อเท็จจริงและพฤติการณ์แห่งคดีเท่าใดก็ได้ อีกทั้งการบัญญัติเกี่ยวกับพยานหลักฐานทางวิทยาศาสตร์เอาไว้ว่า ในกรณีที่จำเป็นต้องใช้พยานหลักฐานทางวิทยาศาสตร์ เพื่อพิสูจน์ข้อเท็จจริงตามมาตรา 131 ให้พนักงานสอบสวนมีอำนาจให้ทำการตรวจพิสูจน์บุคคล วัตถุ หรือเอกสารใด ๆ โดยวิธีการทางวิทยาศาสตร์ได้ ก็เป็นการกำหนดข้อกฎหมายไว้อย่างกว้างให้พนักงานสอบสวนทำการตรวจพยานหลักฐานทางวิทยาศาสตร์ได้ แต่ไม่ได้มีการกำหนดขั้นตอนรูปแบบ หรือวิธีการไว้เป็นการเฉพาะ ส่งผลให้หน่วยงานต่าง ๆ ที่มีหน้าที่ตรวจรวบรวมพยานหลักฐานจำเป็นที่จะต้องตรากฎหมาย ระเบียบ ข้อบังคับ ขึ้นมาเพื่อใช้ในการรวบรวมพยานหลักฐานและตรวจพิสูจน์ของหน่วยงานตนเองไว้เป็นการเฉพาะ แต่ละฉบับกำหนดวิธีการได้มา อำนาจหน้าที่ที่แตกต่างกัน

ส่งผลให้เจ้าหน้าที่ผู้ปฏิบัติงานจริงมีความสับสนว่าตนเองต้องใช้อำนาจตามกฎหมายฉบับใด ดังนั้น การบัญญัติอำนาจหน้าที่ของพนักงานสอบสวนในการรวบรวมพยานหลักฐานตามมาตรา 131 และมาตรา 131/1 แห่งประมวลวิธีพิจารณาความอาญา นั้นกว้างจนเกินไป อีกทั้งยังให้เป็นดุลพินิจของพนักงานสอบสวนอีกด้วยว่าจะกระทำหรือไม่กระทำ ตราบเท่าที่สามารถจะทำได้

2) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม ผลการศึกษาพบว่าเจ้าหน้าที่ผู้ปฏิบัติงานทางด้านตรวจพิสูจน์พยานหลักฐานทางอิเล็กทรอนิกส์ไม่ได้เป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ทั้งหมด เนื่องจากตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม มาตรา 3 กำหนดไว้ว่า พนักงานเจ้าหน้าที่ต้องเป็นผู้ซึ่งรัฐมนตรีแต่งตั้ง จึงจะสามารถปฏิบัติการตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม ได้ โดยผู้ที่จะได้รับการแต่งตั้งได้นั้นต้องเข้าหลักเกณฑ์และมีคุณสมบัติตามประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร อันประกอบด้วย 1) มีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์ 2) สำเร็จการศึกษาไม่น้อยกว่าระดับปริญญาตรีทางวิศวกรรมศาสตร์ วิทยาศาสตร์วิทยาการคอมพิวเตอร์ เทคโนโลยีสารสนเทศ สถิติศาสตร์ นิติศาสตร์ รัฐศาสตร์ หรือรัฐประศาสนศาสตร์ 3) ผ่านการอบรมทางด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (Information security) สืบสวน สอบสวน และการพิสูจน์หลักฐานทางคอมพิวเตอร์ (computer forensics) และ 4) มีคุณสมบัติอื่นอย่างใดอย่างหนึ่ง ซึ่งผู้ให้ข้อมูลที่ผู้วิจัยได้ทำการสัมภาษณ์มีข้อกังวลใจในส่วนของการได้รับแต่งตั้งเป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เนื่องจากมาตรา 19 เป็นการใช้อำนาจของพนักงานเจ้าหน้าที่ที่จะยื่นคำร้องต่อศาลเพื่อขอให้ศาลมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง โดยที่พนักงานเจ้าหน้าที่ที่จะสามารถดำเนินการตามมาตรา 18 (4) – (8) ได้นั้น ต้องเป็นผู้ซึ่งรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษกิจและสังคมเป็นผู้แต่งตั้ง อีกทั้ง การที่จะแต่งตั้งให้เป็นพนักงานเจ้าหน้าที่ก็ไม่มีกำหนดการและแนวทางในการเข้าร่วมการอบรมอย่างชัดเจน

ตามมาตรา 18 (7) ที่ให้อำนาจพนักงานเจ้าหน้าที่ในการถอดรหัสลับของข้อมูลหรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูล ทำการถอดรหัสลับหรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว พนักงานเจ้าหน้าที่ย่อมสามารถใช้เทคโนโลยีต่าง ๆ ในการถอดรหัสลับของข้อมูลที่ได้รับมา หากแต่อุปกรณ์ที่พนักงานเจ้าหน้าที่ได้รับมีการล็อคหรือเข้ารหัสเอาไว้ และขณะรวบรวมพยานหลักฐานผู้ต้องสงสัยหรือถูกกล่าวไม่ได้ให้ความยินยอมในการให้รหัสเพื่อทำการปลดล็อคอุปกรณ์เอาไว้ พนักงานเจ้าหน้าที่ย่อมไม่สามารถกระทำการใด ๆ กับอุปกรณ์เหล่านั้นได้ เพราะเป็นสิทธิ์เฉพาะตัวของบุคคลตามรัฐธรรมนูญที่ได้รับรองเอาไว้ แม้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม จะให้อำนาจพนักงานเจ้าหน้าที่ในการถอดรหัสลับของข้อมูลก็ตาม ผู้ต้องสงสัยหรือถูกกล่าวย่อมมีสิทธิ์ที่จะปฏิเสธการให้ยินยอมได้

3) ระบบคลาวด์ (Cloud) ผลการศึกษาพบว่า ระบบคลาวด์ มีรูปแบบหลัก ๆ ด้วยกัน 3 แบบ ได้แก่ Software as a Service (SaaS), Platform as a Service (PaaS) และ Infrastructure as a Service (IaaS) โดยที่แต่ละแบบมีโครงสร้างและลักษณะของ log file ที่แตกต่างกัน การพิสูจน์พยานหลักฐานทางอิเล็กทรอนิกส์บนคลาวด์ต้องใช้ผู้เชี่ยวชาญด้านการเก็บรวบรวมและพิสูจน์พยานหลักฐานที่มีความรู้ความเข้าใจเกี่ยวกับโครงสร้างและวิธีการทำงานของระบบคลาว์ นำเอาหลักการทางวิทยาศาสตร์ การปฏิบัติทางเทคโนโลยี และวิธีการสกัดและตรวจสอบเพื่อสร้างเหตุการณ์ในระบบคลาวด์ผ่านการระบุตัวตน การเก็บและรักษา การตรวจสอบ และการจัดทำรายงานพยานหลักฐานดิจิทัล นำมาเป็นเครื่องมือในการตรวจสอบและปรับใช้กระบวนการและเครื่องมือของพยานหลักฐานตามลักษณะและสภาพแวดล้อมในบริบทที่แตกต่างกัน

2. สรุปผลการศึกษาเชิงคุณภาพ

จากการสัมภาษณ์เชิงลึกกับผู้ให้ข้อมูล ได้แก่ เจ้าหน้าที่ผู้ปฏิบัติงานของกรมสอบสวนคดีพิเศษ เจ้าหน้าที่ผู้ปฏิบัติงานของสำนักงานพิสูจน์หลักฐานตำรวจ สำนักงานตำรวจแห่งชาติ และเจ้าหน้าที่ผู้ปฏิบัติงานของกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) จำนวน 12 ราย สามารถสรุปผลการศึกษาโดยจำแนกตามวัตถุประสงค์การศึกษา ดังนี้

2.1 ปัจจัยที่ส่งผลเกิดปัญหาเกี่ยวกับการเข้าถึงข้อมูลหลักฐานทางอิเล็กทรอนิกส์

1) ด้านข้อกฎหมาย สิทธิและเสรีภาพของบุคคลได้รับการคุ้มครองโดยรัฐธรรมนูญตลอดจนทรัพย์สินของบุคคลนั้น ๆ ที่มีสิทธิครอบครองหรือกรรมสิทธิ์ในตัวทรัพย์สินนั้นด้วย แม้วัตถุพยานที่พนักงานเจ้าหน้าที่ตรวจยึดมาโดยชอบด้วยกฎหมาย แต่วัตถุพยานหรืออุปกรณ์มีการเข้ารหัสความปลอดภัยส่วนบุคคลเอาไว้ หากปราศจากการได้รับความยินยอมของเจ้าของวัตถุพยานหรืออุปกรณ์ในการให้รหัสความปลอดภัยส่วนบุคคล พนักงานเจ้าหน้าที่ก็ไม่สามารถดำเนินการตรวจสอบกับอุปกรณ์หรือวัตถุพยานเหล่านั้นได้ แม้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม จะให้อำนาจพนักงานเจ้าหน้าที่ในการถอดรหัสลับของข้อมูลก็ตาม ทำให้พนักงานเจ้าหน้าที่จะต้องดำเนินการขอความยินยอมในการให้ผู้ต้องสงสัยหรือผู้ถูกกล่าวหาให้รหัสความปลอดภัยส่วนบุคคลทุกครั้ง บางครั้งหากเป็นกรณีที่พนักงานสอบสวนเป็นผู้ตรวจยึดและรวบรวมพยานหลักฐานมาแล้วไม่ได้ขอรหัสความปลอดภัยส่วนบุคคลมาด้วยตั้งแต่ขณะตรวจยึดหรือรวบรวมพยานหลักฐาน พนักงานเจ้าหน้าที่ผู้ตรวจสอบต้องทำความเห็นส่งกลับคืนพนักงานสอบสวนว่าไม่สามารถทำการตรวจสอบวัตถุพยานหรืออุปกรณ์ได้ เนื่องจากติดรหัสความปลอดภัยส่วนบุคคล ให้พนักงานสอบสวนร้องขอให้ผู้ต้องสงสัยหรือผู้ถูกกล่าวหาให้รหัสความปลอดภัยส่วนบุคคลและนำส่งกลับมาให้พนักงานเจ้าหน้าที่ตรวจสอบใหม่อีกครั้ง

2) ด้านเครื่องมือและบุคลากร จากการสัมภาษณ์เจ้าหน้าที่หน่วยงานของภาครัฐทั้ง 3 หน่วยงาน พบว่า เจ้าหน้าที่ส่วนใหญ่ไม่ใช่พนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม เป็นเพียงนักวิทยาศาสตร์เป็นผู้ปฏิบัติงานในด้าน

การตรวจสอบ พิสูจน์พยานหลักฐานในห้องปฏิบัติการเท่านั้น เนื่องจากในประเทศไทยมีการกำหนดอำนาจหน้าที่ของแต่ละตำแหน่งเอาไว้แยกต่างหากอย่างชัดเจน พนักงานสอบสวนหรือเจ้าหน้าที่ตำรวจเป็นผู้สืบสวนสอบสวนและรวบรวมพยานหลักฐาน และนำส่งให้นักวิทยาศาสตร์ซึ่งสังกัดในหน่วยงานของตนเองเป็นผู้ตรวจสอบ มักพบว่าพนักงานสอบสวนหรือเจ้าหน้าที่ตำรวจดำเนินการรวบรวมพยานหลักฐานไม่ถูกต้องหรือไม่ครบถ้วน ขาดองค์ความรู้เกี่ยวกับการการรวบรวมพยานหลักฐานทางดิจิทัล ซึ่งการดำเนินการไม่เหมือนกับการรวบรวมพยานหลักฐานทางอาญาทั่วไป อีกทั้ง การทำสำเนาข้อมูลหลักฐานทางดิจิทัลมีจำนวนมากและต้องใช้ระยะเวลาที่นาน แต่อุปกรณ์ที่ใช้ในการทำสำเนาข้อมูลไม่เพียงพอต่อความต้องการกับปริมาณของงานที่ต้องทำการตรวจสอบ และระยะเวลาที่ต้องเร่งรีบของพนักงานสอบสวนในการทราบผลการตรวจสอบ

2.2 แนวทางการป้องกัน

1) สร้างหลักสูตรการเรียนรู้ออนไลน์หรือ e – learning เพื่อเสริมสร้างความรู้ความเข้าใจให้พนักงานสอบสวนหรือเจ้าหน้าที่ตำรวจให้สามารถเข้ามาเรียนรู้วิธีการดำเนินการรวบรวมพยานหลักฐานทางดิจิทัลและห่วงโซ่การครอบครองพยานหลักฐาน (Chain of custody) อย่างถูกต้อง และให้มีการทดสอบความรู้ที่ได้จากการเรียนภายหลังจากการเรียนรู้ และเสนอแนะให้หน่วยงานของรัฐทุกภาคส่วนให้ความร่วมมือในการแลกเปลี่ยนข้อมูลการดำเนินงาน เพื่อสร้างความร่วมมือระหว่างหน่วยงานและเจ้าหน้าที่ทั้งในประเทศไทยและต่างประเทศ เพื่อให้รู้เท่าทันอาชญกรรมคอมพิวเตอร์และอาชญากรรมเทคโนโลยีอย่างมีประสิทธิภาพมากยิ่งขึ้น

2) ภาครัฐเห็นควรส่งเสริมและผลักดันให้หน่วยงานของรัฐมีห้องปฏิบัติการที่เป็นสากลตามมาตรฐาน ISO เพื่อพร้อมรับมือกับอาชญากรรมไซเบอร์ในปัจจุบันให้ทันท่วงทีและอาชญากรรมในรูปแบบใหม่ที่จะเกิดขึ้นในอนาคต เพื่อรองรับกับการตรวจสอบข้อมูลที่มีขนาดมหาศาลในการสนับสนุนอุปกรณ์ให้มีความพร้อมและเพียงพอต่อความต้องการตามปริมาณงานที่จะมีเพิ่มมากขึ้นในอนาคต

ข้อเสนอแนะ

1) ควรมีการศึกษาวิจัยเพื่อศึกษาแนวทางขั้นตอนการดำเนินการพิจารณาและรวบรวมพยานหลักฐานเกี่ยวกับการกระทำความผิดโดยใช้เทคโนโลยีระบบคลาวด์

2) ควรศึกษาวิจัยเกี่ยวกับแนวทางการปฏิบัติงานเกี่ยวกับปัญหาการรวบรวมพยานหลักฐานดิจิทัลเกี่ยวกับการกระทำความผิดในต่างประเทศ

เอกสารอ้างอิง

Kallachai Rattanasakawong. (1980). Studies in criminal law. Master of Laws Thesis, Thammasat University.

Natthanan Jaisue. (2021). Legal measures regarding listening to digital evidence. Sripatum University Chonburi Campus

Triphol Ketsuriya. (2015). Consent of minors in criminal law: a study of specific cases of body tattooing and genital mutilation. Master of Laws Thesis, Dhurakij Pundit University.

Nath Thanesavanich. (2012). Listening and methods for taking electronic evidence in criminal cases: Study according to the Computer Crimes Act of 2007. Master of Laws thesis. Criminal Law Department, Thammasat University.

Nanthawadee Kanchan. (2019). Problems in suppressing cybercrime under international law. Master's Thesis Department of Criminal Law Faculty of Law Thammasat University.

Criminal Procedure Code. (2008, 30 January). Royal Gazette. Volume 125 (Issue 28). Page 4

Pannat Khankhet. (2016). Legal problems regarding the collection of electronic evidence in the investigation court. Master of Laws Thesis, National Institute of Development Administration.

Computer Crime Act (No. 2) B.E. 2017. (2017, 24 January). Royal Gazette. Volume 134, Chapter 10, Pages 24-35.

Pichaisak Haryangkun, Narisara Daengpai. Principle of consent. https://www.stou.ac.th/Schools/Slw/upload/Ex%2040701-3.pdf

Wichayada Amphonkitwiwat. (2018). Computer Act: Computer Law or Security Protection Law. At the 1st National Jurisprudence Conference, topic: Thai Legal System: Reform/Transition/Restoration, 8 June 2018. Chiang Mai University, Chiang Mai.

Wiramon Daoduang. (2021). Problems in gathering evidence to prosecute cyber crimes. Master's Thesis Criminal Law Department, Thammasat University.

Wallika Oonsri. (2001). Problems in collecting and verifying electronic evidence in criminal cases. Master of Laws Thesis, Thammasat University.

Yadfon Chusaeng. (2016). Principles for listening to evidence that was created or obtained illegally: A comparative study of the status of evidence obtained by private individuals and in the case of acquisition by a government official. 39 – 40

Digital Forensics Center Electronic Transactions Development Agency (Public Organization) Working group to draft standards for digital evidence verification practices. (2016). Suggestions for standards for managing digital devices in evidence verification work.

ประวัติผู้เขียน

คำนำหน้า ชื่อ-สกุล	**นายจิระพัชร์ ทวงศ์เฉลียว**
ตำแหน่ง/สถานะ	นักศึกษาปริญญาโท
ที่อยู่หน่วยงาน/สังกัด	457 หมู่ที่ 8 ตำบลขมิ้น อำเภอเมืองสกลนคร จังหวัดสกลนคร
ไปรษณีย์อิเล็กทรอนิกส์	Jirapat.wongz@outlook.com