บทความวิชาการ

กรอบแนวคิดการตรวจพิสูจน์หลักฐานดิจิทัลในกระบวนการยุติธรรมทางอาญา*

A CONCEPTUAL FRAMEWORK ON DIGITAL IN CRIMINAL JUSTICE SYSTEM

ศลทร คงหวาน

Sonthon Khongwan

หลักสูตรปรัชญาดุษฎีบัณฑิต สาขาวิชานิติวิทยาศาสตร์และงานยุติธรรม คณะวิทยาศาสตร์ มหาวิทยาลัยศิลปากร

Ph.D. Candidate in Forensic Science and Criminal Justice, Graduate School, Silpakorn University, Thailand

ศุภชัย ศุภลักษณ์นารี

Supachai Supraluknaree

คณะวิทยาศาสตร์ มหาวิทยาลัยศิลปากร

Faculty of Science, Silpakorn University Nakhon Pathom, Thailand

Corresponding author: Sonthonkhongwan@yahoo.com

บทคัดย่อ

การตรวจพิสูจน์หลักฐานดิจิทัลกลายเป็นองค์ประกอบสำคัญในระบบยุติธรรมทางอาญา ซึ่งสะท้อนถึงผลกระทบอันเกี่ยวพันทางเทคโนโลยีสารสนเทศต่ออาชญากรรมและกระบวนการสืบสวนในปัจจุบัน ลักษณะของหลักฐานดิจิทัลมีความแตกต่างจากหลักฐานรูปแบบดั้งเดิม ซึ่งสะท้อนถึงลักษณะเฉพาะ ความท้าทาย และผลกระทบต่อระบบยุติธรรมทางอาญา การทำความเข้าใจลักษณะเฉพาะเหล่านี้ถือเป็นสิ่งสำคัญในการจัดการหลักฐานดิจิทัลอย่างมีประสิทธิภาพ ในการรักษาความสมบูรณ์และรับรองความน่าเชื่อถือในบริบททางกฎหมาย

บทความนี้นำเสนอกรอบแนวคิดสำหรับการทำความเข้าใจการตรวจพิสูจน์หลักฐานดิจิทัลในกระบวนการทางกฎหมาย โดยมีจุดมุ่งหมายเพื่อนำเสนอข้อมูลที่ครอบคลุมเกี่ยวกับวิธีการ ความท้าทาย และผลกระทบที่เกี่ยวข้องกับการตรวจพิสูจน์หลักฐานดิจิทัลในบริบททางกฎหมาย โดยมุ่งเน้นไปที่การรวบรวม การเก็บรักษา การวิเคราะห์และการนำเสนอหลักฐานดิจิทัลอย่างเป็นระบบ ซึ่งทำให้เห็นว่าการยอมรับหลักฐานดิจิทัลในกระบวนการทางกฎหมายนั้นอาจเต็มไปด้วยความท้าทายที่เกิดจากลักษณะเฉพาะตัว ความซับซ้อนทางเทคโนโลยี และผลกระทบทางกฎหมาย การแก้ไขปัญหาเหล่านี้ต้องอาศัยแนวทางปฏิบัติทางนิติวิทยาศาสตร์ที่เข้มงวด มาตรฐานการตรวจพิสูจน์ที่มีความเป็นสากล และความร่วมมือจากสหวิทยาการ เพื่อสนับสนุนผลลัพธ์ที่เกิดจากการตรวจพิสูจน์หลักฐานทางดิจิทัลอย่างมีประสิทธิภาพ

คำสำคัญ: การตรวจพิสูจน์หลักฐานดิจิทัล, พยานดิจิทัล, กระบวนการยุติธรรมทางอาญา

* Received 15 August 2024; Revised 29 August 2024; Accepted 30 August 2024

Abstract

Digital forensics has emerged as a critical component of the criminal justice system, underscoring the profound impact of technology on modern crime and investigative processes. The nature of digital evidence is distinct from traditional forms of evidence, characterized by its unique attributes, challenges, and implications for the criminal justice system. Understanding these aspects is essential for effectively handling digital evidence, preserving its integrity, and ensuring its reliability in legal contexts.

This article presents a conceptual framework for understanding the role of digital forensics in legal processes, aiming to provide a comprehensive overview of the methodologies, challenges, and implications associated with digital evidence. It focuses on the systematic identification, collection, preservation, analysis, and presentation of digital evidence. Significant challenges accompany the acceptance of digital evidence in legal proceedings, stemming from its unique nature, technological complexity, and legal implications. Addressing these challenges requires a combination of robust forensic practices, international standards, ongoing education, and interdisciplinary collaboration to support the effective outcomes of digital forensics.

Keywords: Digital Forensics, Digital Evidence, Criminal Justice System

บทนำ

ความก้าวหน้าทางเทคโนโลยีสารสนเทศเข้ามามีบทบาทและมีส่วนสำคัญในการดำเนินชีวิตประจำวันของมนุษย์มากขึ้นไม่ว่าจะใช้เป็นการติดต่อสื่อสารระหว่างบุคคล การทำธุรกรรมต่าง ๆ ของมนุษย์ จึงไม่สามารถปฏิเสธหรือหลีกเลี่ยงที่จะไม่มีส่วนเกี่ยวข้องกับเทคโนโลยีสารสนเทศได้เลย ชี้ให้เห็นข้อเท็จจริงประการหนึ่งว่า ในโลกแห่งการเชื่อมต่อกันดังปัจจุบันนี้ แทบเป็นไปไม่ได้เลยที่มนุษย์จะสามารถอยู่ “นอกเครือข่าย” (Off the Net) อย่างสมบูรณ์เพื่อที่กิจกรรมต่าง ๆ ของมนุษย์จะไม่ได้สร้างบันทึกอิเล็กทรอนิกส์บางรูปแบบขึ้น (แลร์รี อี. แดเนียล, ลาร์ส อี. แดเนียล, 2559) การใช้ชีวิตที่มีอินเทอร์เน็ตเข้ามามีส่วนเกี่ยวข้องในชีวิตประจำวันหรือการเข้าถึงอุปกรณ์ที่ใช้เข้าถึงอินเทอร์เน็ตได้ง่ายขึ้น สิ่งเหล่านี้ล้วนส่งผลให้ประชาชนเข้าถึงอินเทอร์เน็ตได้มากยิ่งขึ้น ผู้ใช้อินเทอร์เน็ตส่วนใหญ่ยอมรับว่ามีการใช้อินเทอร์เน็ตจนเป็นส่วนหนึ่งในชีวิตแล้ว (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2565) อย่างไรก็ตามการใช้งานผ่านอินเทอร์เน็ตในบางกรณีอาจก่อให้เกิดความเสียหายต่อบุคคลอื่นได้ มีคดีความตามมาเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์เพิ่มมากขึ้นด้วยเช่นเดียวกัน (สาวตรี สุขศรี และคณะ, 2555) ผลของการกระทำผิดทางคอมพิวเตอร์ย่อมส่งผลกระทบหรือก่อให้เกิดความเสียหายในวงกว้างและรวดเร็ว ซึ่งอาจส่งผลกระทบทั้งด้านเศรษฐกิจ สังคม รวมถึงด้านความมั่นคงปลอดภัยของประเทศชาติด้วย จึงทำให้เห็นถึงความสำคัญของข้อมูลต่าง ๆ ที่ถูกสร้างและบันทึกด้วยรูปแบบอิเล็กทรอนิกส์ซึ่งจะกลายเป็นข้อมูลดิจิทัลที่มีความสำคัญในการที่จะนำไปใช้ทั้งเพื่อปัจเจกชนและเพื่อสาธารณะชน ซึ่งการนำข้อมูลทางดิจิทัลไปใช้นั้นอาจจะ

อยู่ในส่วนที่เกี่ยวข้องกับผลประโยชน์ทางแพ่งเพื่อยืนยันถึงสิทธิหรือหน้าที่ระหว่างบุคคลหรือผลประโยชน์ทางอาญาเพื่อการยืนยันข้อเท็จจริงที่เกิดขึ้น ซึ่งมีความเกี่ยวพันกับการกระทำความผิดทางอาญาได้

การกระทำความผิดทางอาญาผ่านเครือข่ายทางอินเทอร์เน็ต สิ่งที่สำคัญที่จะนำมาพิสูจน์การกระทำคือ “พยานหลักฐานดิจิทัล” (Digital Evidence) ซึ่งเป็นรูปแบบทางข้อมูลอิเล็กทรอนิกส์อย่างหนึ่ง พยานหลักฐานดิจิทัลถูกแสดงให้ปรากฏในรูปแบบข้อมูลทางอิเล็กทรอนิกส์ ซึ่งต้องมีการปฏิบัติในกระบวนการนำเสนอหลักฐานดิจิทัลที่แตกต่างจากหลักฐานทางกายภาพอื่น ๆ ไม่ว่าในแง่ของการได้มาหรือการอธิบายหลักฐานดิจิทัล โดยข้อมูลจะถูกจัดเก็บไว้ที่ใดที่หนึ่งซึ่งสามารถเข้าถึงได้โดยบางวิธี อีกทั้งต้องสามารถกู้คืนได้โดยผู้ตรวจพิสูจน์พยานหลักฐานหนึ่งในความท้าทายของพยานหลักฐานดิจิทัลคือ ข้อมูลถูกเก็บไว้ที่ใด การเข้าถึงที่จัดเก็บ การเข้าถึงและการประมวลผลพยานหลักฐานดิจิทัลนั้นในแง่ของการเชื่อมโยงกับการดำเนินคดีอาญาเป็นอย่างไร (แลร์รี อี. แดเนียล, ลาร์ส อี. แดเนียล, 2559) ทั้งนี้ สิ่งที่มีความสำคัญที่สุดเมื่อมีการดำเนินคดีอาญาในชั้นศาลคือ ความน่าเชื่อถือของพยานหลักฐานดิจิทัล (Reliability of Digital Evidence) ซึ่งถือว่ามีความสำคัญอย่างยิ่ง ความท้าทายในการพิสูจน์ความถูกต้องและความน่าเชื่อถือของหลักฐานดิจิทัลมาจากข้อเท็จจริงที่ว่า หลักฐานชนิดนั้นบางครั้งก็ไม่เป็นเช่นนั้น ความแปรปรวนของซอฟต์แวร์ทางนิติวิทยาศาสตร์ ข้อผิดพลาดในการประมวลผลภาพ (Image Processing) และความรู้ความเข้าใจและอคติที่แตกต่างของผู้ตรวจสอบ มีผลต่อความผิดพลาด ความน่าเชื่อถือความถูกต้องและความสมบูรณ์ของพยานหลักฐานดิจิทัล ทั้งนี้ ความไม่น่าเชื่อถือโดยส่วนใหญ่เนื่องจากความสมบูรณ์ของข้อมูลดิจิทัลที่ไม่สามารถยืนยันและพิสูจน์ได้ (Gary C. Kessler, 2010) (Nina Sunde a, and Itiel E. Dror, 2019) หรือการไม่สามารถตรวจสอบข้อบกพร่องของซอฟต์แวร์ได้เนื่องจากที่ไม่สามารถเข้าถึงรหัสต้นฉบับ (Source Code) อันเป็นผลมาจากกฎหมายความลับทางการค้า พยานหลักฐานดิจิทัลจึงถูกท้าทายความน่าเชื่อถือ (Van Buskirk, E., and Liu, V. T. , 2006) ดังนั้น การพิจารณาถึงความถูกต้องแท้จริงของข้อมูล ระบบที่ทำงานการเก็บบันทึกหรือข้อมูลอิเล็กทรอนิกส์นั้น ว่ามีความน่าเชื่อมากน้อยเพียงใด เพื่อการพิจารณาให้เป็นที่ยุติและพิพากษาคดีจึงเป็นสิ่งสำคัญ (นัทธ์ ธเนศวาณิชย์, 2555) จากที่กล่าวมาข้างต้นนี้จึงเห็นได้ว่า การรวบรวมข้อมูลทางอิเล็กทรอนิกส์อันจะนำไปใช้เป็นพยานดิจิทัลนั้น มีรายละเอียดและขั้นตอนที่เกี่ยวข้องในการรวบรวม จัดเก็บและการวิเคราะห์มากกว่าพยานหลักฐานทางกายภาพอื่น ๆ เช่น พยานเอกสาร พยานวัตถุ หรือพยานบุคคล จึงจำเป็นที่ผู้ที่เกี่ยวข้องในนำเสนอพยานดิจิทัลต่อศาลหรือนำพยานหลักฐานดิจิทัลเข้ามามีส่วนเกี่ยวข้องไว้ในสำนวนคดีจะต้องมีความรู้ ความเข้าใจเกี่ยวกับหลักการที่สำคัญ ๆ ของกระบวนการเกี่ยวกับการได้มา เพื่อให้การนำเสนอพยานหลักฐานดิจิทัลนั้นมีคุณค่าเพียงพอที่จะสามารถยืนยันข้อเท็จจริงใดข้อเท็จจริงหนึ่งให้มีความน่าเชื่อถือ เพื่อให้การนำเสนอพยานหลักฐานดิจิทัลนั้นมีประโยชน์สูงสุดเมื่อเข้าสู่กระบวนการพิจารณาพิพากษาคดีในชั้นศาล

บทความนี้จึงมีวัตถุประสงค์เพื่อศึกษาทบทวนวรรณกรรมที่เกี่ยวข้องกับการตรวจพิสูจน์หลักฐานทางดิจิทัล รวมถึงองค์ความรู้ของพยานหลักฐานดิจิทัล เพื่อนำมาสรุปเป็นแนวทางในการตรวจพิสูจน์พยานหลักฐานดิจิทัล สำหรับใช้เป็นกรอบแนวคิดพื้นฐานในการตรวจสอบหรือประเมินความน่าเชื่อถือของกระบวนตรวจพิสูจน์หลักฐานทางดิจิทัลที่มีประสิทธิภาพ และเป็นประโยชน์สำหรับการประยุกต์ใช้ดุลพินิจวิเคราะห์ความน่าเชื่อถือพยานหลักฐานดิจิทัลของบุคลากรในกระบวนการยุติธรรมทางอาญา

พรมแดนแห่งอาชญากรรมทางเทคโนโลยี

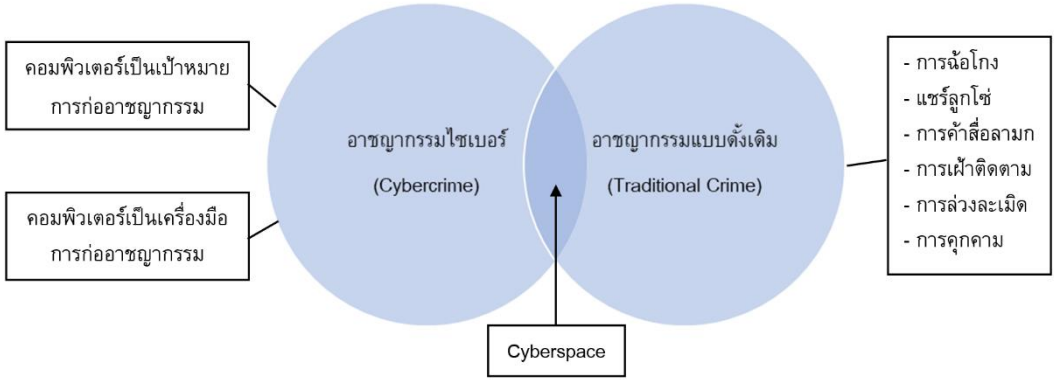
การกระทำความผิดที่มีความเกี่ยวข้องกับคอมพิวเตอร์ในช่วงแรก ๆ มักจะมีการใช้คำว่า “อาชญากรรมคอมพิวเตอร์” หรือ “Computer Crime” โดยคำว่าอาชญากรรมคอมพิวเตอร์ปรากฏครั้งแรกในปี ค.ศ. 1976 ในหนังสือของดอนน่า ปาร์คเกอร์ (Donna Parker) เรื่อง “Crime in Computer” และปรากฏครั้งแรกใน Florida Computer Crimes Act 1978 ซึ่งเป็นกฎหมายที่เกี่ยวข้องกับการห้ามมิให้ลบหรือปรับเปลี่ยนข้อมูลในระบบคอมพิวเตอร์ (Damshenas, M., Dehghantanha, A., and Mahmoud, R., 2014) จนถึงปลายปี ค.ศ. 1990 คำศัพท์เริ่มเปลี่ยนไปเนื่องจากการใช้เทคโนโลยีและการเข้าถึงอินเทอร์เน็ตในสังคมที่เปลี่ยนแปลงไป การพัฒนาระบบปฏิบัติการ Windows 95 ทำให้ผู้ใช้คอมพิวเตอร์มีความสะดวกมากขึ้น เช่นเดียวกับความสะดวกในการเข้าถึงการเชื่อมต่ออินเทอร์เน็ต แพลตฟอร์มธุรกิจถูกย้ายไปที่สภาพแวดล้อมออนไลน์เพื่อให้บริการโดยตรงกับผู้ใช้คอมพิวเตอร์ เมื่อรูปแบบการใช้เทคโนโลยีเปลี่ยนแปลงไปนักวิจัยเช่น David Wall เริ่มใช้คำว่า "อาชญากรรมไซเบอร์" (Cybercrime) เพื่ออ้างถึงอาชญากรรมที่ดำเนินการทางออนไลน์ (Thomas J. Holt and Adam M. Bossler, 2016) โดยมีจุดเริ่มต้นอย่างเป็นทางการของ รายงานวิจัยชุมชนทางวิชาการเกี่ยวกับการสืบสวนทางนิติวิทยาศาสตร์แบบดิจิทัลเกิดขึ้นในปี ค.ศ. 2002 ในบทความของ V. Corey และคณะ (Damshenas, M., Dehghantanha, A., and Mahmoud, R., 2014) เรื่อง “การวิเคราะห์ความผิดปกติของระบบเครือข่าย” (Network Forensics Analysis) ซึ่งทำการศึกษาเครื่องมือที่ใช้ในการวิเคราะห์ความผิดปกติของระบบเครือข่าย (Network Forensic Analysis Tool (NFAT)) และเน้นประโยชน์ในเรื่องของการจับประเด็นการวิเคราะห์ การดักจับการจราจรข้อมูล และประเด็นความปลอดภัยของระบบ

อาชญากรได้สร้างโอกาสในการก่ออาชญากรรมและการใช้เทคโนโลยีในทางที่ผิดอย่างหาที่เปรียบไม่ได้ และการประยุกต์ใช้เทคโนโลยีใหม่ๆ เพื่อสร้างอาชญากรรมรูปแบบใหม่ที่ไม่เคยมีมาก่อน ซึ่งอาจใช้เทคโนโลยีเป็นสื่อกลางในการสื่อสารหรือกลไกในการกำหนดเป้าหมายหรือเป็นเครื่องช่วยอำนวยความสะดวกในการก่ออาชญากรรม ซึ่งไม่สามารถทำได้ในโลกแห่งความเป็นจริง (Thomas J. Holt, Adam M. Bossler, Kathryn C. Seigfried-Spellar, 2017) อาชญากรรมทางเทคโนโลยีจึงยังคงมีข้อถกเถียงว่า มีความแตกต่างจากอาชญากรรมแบบดั้งเดิมอย่างไร โดย Grabosky, P. N. (2001) ให้ความเห็นว่าอาชญากรไซเบอร์อาจถูกมองว่าเป็น “เหล้าเก่าในขวดใหม่” อาชญากรรมในโลกเสมือนจริง (Virtual Criminality) โดยพื้นฐานแล้วเหมือนกับอาชญากรรมในทางโลกที่เราคุ้นเคย โดยใช้เทคโนโลยีเพื่ออำนวยความสะดวกในการดำเนินการตามแรงจูงใจ อย่างไรก็ตามการกระทำผิดแบบใหม่ (True Cybercrime) ซึ่งถือเป็นการกระทำความผิดทางเทคโนโลยีสารสนเทศโดยแท้ เพราะเป็นผลที่เกิดขึ้นจากระบบเทคโนโลยีสารสนเทศ (products of IT) และเป็นสิ่งที่เกิดขึ้นในโลกเสมือนออนไลน์โดยไม่คำนึงถึงบริบทสภาพแวดล้อมทางกายภาพและเวลาท้องถิ่น เช่น สแปม (spam) การก่อกวนระบบไม่ให้ใช้งานได้ (denial of service) สงครามข้อมูลข่าวสาร (information warfare) การดูดทรัพยากรคอมพิวเตอร์ (parasitic computing) การละเมิดทรัพย์สินทางปัญญา การหลอกลวงในการประมูลออนไลน์ (online auction scams) การหลอกเอาข้อมูลส่วนบุคคล (phishing) การร่วมประเวณีออนไลน์ (cyber-sex) นายหน้าค้าประเวณีออนไลน์ (cyber-pimping) การล่อลวงเด็กออนไลน์ (online grooming) เครือข่ายแลกเปลี่ยนข้อมูลการทำระเบิดและยาเสพติด การสร้างความเกลียดชังอย่าเจาะจง (targeted hate speech) ก็ล้วนมีลักษณะที่เป็นประเด็นทาง

เทคโนโลยีสารสนเทศโดยแท้เช่นเดียวกัน ซึ่งถ้าหากตัดอินเทอร์เน็ตออกไป กิจกรรมเหล่านี้ก็จะไม่สามารถเกิดขึ้นได้ (พัฒนาพร โกวพัฒนกิจ และคณะ, 2560) อย่างไรก็ตามหลักการพื้นฐานทางอาชญาวิทยาสามารถอธิบายแนวโน้มของการตกเป็นเหยื่ออาชญากรรมไซเบอร์และอาชญากรรมแบบดั้งเดิมหรืออาชญากรรมพื้นฐาน (Street Crime) ที่ไม่มีความแตกต่างกัน ด้วยปัจจัยสามประการคือ 1) แรงจูงใจ 2) โอกาส และ 3) ไม่มีผู้พิทักษ์ที่มีความสามารถ (Grabosky, P. N., 2001)

สาวตรี สุขศรี (2563) เห็นว่าอาชญากรรมไซเบอร์หรืออาชญากรรมอินเทอร์เน็ต คือ อาชญากรรมคอมพิวเตอร์รูปแบบหนึ่ง โดยอาชญากรอาศัยความสามารถและคุณสมบัติการทำงานที่ไร้พรมแดนของอินเทอร์เน็ตในการกระทำต่อระบบสารสนเทศ หรือข้อมูลคอมพิวเตอร์ ทำให้รูปแบบการกระทำถูกพัฒนาและเปลี่ยนแปลงไป ใช้เวลาน้อยกว่าในการสร้างความเสียหาย ทั้งขยายผลแห่งความเสียหายได้กว้างขวาง นอกจากนี้ยังอาจหมายรวมถึงความผิดที่ถูกกระทำลงในพื้นที่ที่เกิดขึ้นใหม่โดยการเชื่อมโยงเครือข่ายคอมพิวเตอร์ (Computer Network) หรือที่เรียกว่า “Cyberspace” การใช้คำว่าอาชญากรรมคอมพิวเตอร์จึงเป็นเรื่องที่อ้างถึงการใช้คอมพิวเตอร์ในทางที่ผิด ความแตกต่างทางเทคนิคในบทบาทของเทคโนโลยีเกี่ยวกับการกระทำความผิดโดยเฉพาะอาชญากรรมไซเบอร์หมายถึงอาชญากรรมซึ่งผู้กระทำความผิดใช้ความรู้พิเศษของไซเบอร์สเปซในขณะที่อาชญากรรมคอมพิวเตอร์เกิดขึ้นเพราะผู้กระทำความผิดใช้ความรู้พิเศษเกี่ยวกับเทคโนโลยีทางคอมพิวเตอร์

นิยามอาชญากรรมไซเบอร์ จึงเป็นเรื่องเกี่ยวกับอาชญากรรมซึ่งผู้กระทำความผิดได้กระทำบนเครือข่ายคอมพิวเตอร์ อาชญากรรมทางไซเบอร์และอาชญากรรมแบบดั้งเดิมยังคงมีพรมแดนที่เป็นจุดเกาะเกี่ยวกัน



ภาพที่ 1 แสดงความเกี่ยวพันระหว่างอาชญากรรมแบบดั้งเดิมกับอาชญากรรมไซเบอร์ในพื้นที่ Cyberspace

ความสัมพันธ์ตาม *ภาพที่ 1* แสดงให้เห็นว่าทั้งอาชญากรรมไซเบอร์และอาชญากรรมแบบดั้งเดิมไม่ได้แยกออกจากกันอย่างสิ้นเชิง สอดคล้องกับ Grabosky, P. N. (2001) ซึ่งให้ความเห็นว่าอาชญากรรมไซเบอร์คือการกระทำผิดความผิดแบบดั้งเดิมที่อาชญากร (มนุษย์) ใช้เทคโนโลยีเป็นเครื่องอำนวยความสะดวกในการก่ออาชญากรรม อย่างไรก็ตามในอนาคตอันใกล้นี้กรณีความเสียหายที่เกิดจากปัญญาประดิษฐ์ (Artificial Intelligence: AI) (เหมือน สุขมาตย์, 2562) และ (ภูมินทร์ บุตรอินทร์, 2561) พรมแดนอาชญากรรมแบบดั้งเดิมกับอาชญากรรมไซเบอร์ที่มนุษย์มีส่วนเกี่ยวข้องต้องมีการเปลี่ยนแปลงไปในลักษณะที่ไม่มีส่วนเกาะเกี่ยวกัน

บริบทของพยานหลักฐานคอมพิวเตอร์และพยานหลักฐานดิจิทัล

ในอดีตข้อมูลทางเทคโนโลยีสารสนเทศ พยานหลักฐานคอมพิวเตอร์ (Computer Evidence) มักจะหมายถึงสิ่งที่พิมพ์ออกมา (print-out) จากคอมพิวเตอร์ การนำเสนอต่อศาลก็มักจะใช้รูปแบบเช่นนั้น การตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensics) จึงเป็นเรื่องเกี่ยวกับหลักฐานที่มาจากคอมพิวเตอร์ (John R. Vacca, 2008) ทั้งนี้ Mark Reith (2002) ให้คำจำกัดความการตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์ว่าเป็น “วิธีการทางเทคนิคและเครื่องมือที่ใช้ในการค้นหาหลักฐานในคอมพิวเตอร์” (Reith, M., Carr, C., and Gunsch, G., 2002) คำจำกัดความนี้แสดงให้เห็นว่าพยานหลักฐานทางคอมพิวเตอร์มาจากคอมพิวเตอร์มีได้หลายรูปแบบ เช่น ฮาร์ดไดรฟ์ (Hard drives) ระบบบันทึก (System logs) อุปกรณ์จัดเก็บข้อมูลแบบพกพา (ไดรฟ์ USB ไดรฟ์ภายนอก ฯลฯ) บันทึกเราเตอร์ (Router logs) อีเมล (E-mail) บันทึกห้องสนทนา (Chat-room logs) บันทึกจากอุปกรณ์รักษาความปลอดภัย เช่น ไฟร์วอลล์และระบบตรวจจับการบุกรุก ฐานข้อมูลและบันทึกฐานข้อมูล (Databases and database logs) (Easttom, C. and Taylor, J., 2011) การเข้าถึงข้อมูลจากแหล่งข้อมูลข้างต้นสามารถเข้าถึงได้ทางกายภาพจากแหล่งข้อมูลเมื่อยึดอุปกรณ์เหล่านั้นได้ อย่างไรก็ตามการเติบโตทางเทคโนโลยี แหล่งที่มาของข้อมูลที่เปลี่ยนแปลงไปจากเดิม ทำให้เกิดการตั้งคำถามเกี่ยวกับขอบเขตของพยานหลักฐานทางคอมพิวเตอร์ เนื่องจากข้อมูลประเภทใหม่ๆ ที่ดึงมาจากอุปกรณ์ดิจิทัลจำนวนมากไม่เหมาะกับแนวคิดทั่วไปของคอมพิวเตอร์ อันเป็นผลมาจากความเจริญก้าวหน้าทางด้านเทคโนโลยีคอมพิวเตอร์ และการสื่อสารผ่านเครือข่ายอินเทอร์เน็ตทำให้สรรพสิ่ง หรือวัตถุต่าง ๆ (Things) บนโลกสามารถปฏิสัมพันธ์ตอบโต้กับมนุษย์ได้ผ่านการเชื่อมต่อกับอุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ ซึ่งเป็นที่มาของคำว่า Internet Of Things (IoT) ที่นิยามโดย Kevin Ashton ในปี คศ. 2009 สำหรับภาษาไทยแปลคำว่า Internet Of Things ไว้หลากหลาย เช่น อินเทอร์เน็ตทุกสรรพสิ่ง (วิวัฒน์ มีสุวรรณ์, 2559) อินเทอร์เน็ตแห่งสรรพสิ่ง (ซามูเอล กรีนการ์ด, 2560)อย่างไรก็ตามรายงานฉบับแรกที่กล่าวถึง IoT คือ รายงานของสหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union: ITU) ในปี ค.ศ. 2005 โดยสังเกตว่า การสื่อสารหรือส่งข้อมูลระหว่างเครื่องจักรกับเครื่องจักร (Machine to Machine: M2M) และการสื่อสารระหว่างบุคคลกับคอมพิวเตอร์จะขยายไปสู่สิ่งของทุกสิ่งทุกอย่างในชีวิตประจำวัน (Qusay F. Hassan, Atta ur Rehman Khan, Sajjad A. Madani (Eds), 2018) เทคโนโลยี IoT จึงมีความหมายโดยกว้างคือ เทคโนโลยีการสื่อสารข้อมูลที่เชื่อมต่อ วัตถุอุปกรณ์ อิเล็กทรอนิกส์ และผู้คนเข้าเป็นโครงข่ายเดียวกัน (ถิรพิรุฬห์ ทองคำวิฑูรย์, 2559)

ปัจจุบันพยานหลักฐานดิจิทัล (Digital Evidence) ถูกนำมาใช้อธิบายข้อมูลทางเทคโนลียีสารสนเทศที่มาจากแหล่งข้อมูลต่าง ๆ ซึ่งเริ่มต้นด้วยรูปแบบของข้อมูลอิเล็กทรอนิกส์ ซึ่งอาจมาจากสิ่งที่สร้างขึ้นโดยมนุษย์และสร้างโดยเทคโนลียีอันเป็นผลมาจากการมีปฏิสัมพันธ์กับมนุษย์ (แลร์รี อี. แดเนียล, ลาร์ส อี. แดเนียล, 2559) โดยการตรวจพิสูจน์หลักฐานทางดิจิทัล (Digital Forensic) วิธีการใช้ทางวิทยาศาสตร์และได้รับการพิสูจน์แล้วเพื่อการเก็บรักษา เก็บ ข้อมูล การให้เหตุผล การระบุตัวตน การวิเคราะห์การตีความ การจัดทำเอกสารและ การนำเสนอหลักฐาน ดิจิทัลจากแหล่งดิจิทัลเพื่อจุดประสงค์ในการอำนวยความสะดวก หรือการสร้างใหม่ของเหตุการณ์ที่พบว่า เป็นความผิดทางอาญาหรือช่วยในการคาดการณ์การกระทำที่ไม่ได้รับอนุญาตที่แสดงให้เห็นว่าเป็น อุปสรรคต่อการดำเนินการตามที่ได้วางแผนไว้ (Vassil Roussev, 2016) ซึ่งมีความสัมพันธ์กับ การตรวจพิสูจน์หลักฐานบน

ระบบคลาวด์ (Cloud Forensics) การตรวจพิสูจน์หลักฐานโทรศัพท์มือถือ (Mobile Forensics) การตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensics) และ การตรวจพิสูจน์หลักฐานทางเครือข่าย (Network Forensics) (Raymond Lutui, 2016) ทั้งนี้เห็นได้ว่าการตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์เป็นสาขาหนึ่งของการตรวจพิสูจน์หลักฐานทางดิจิทัล

ทั้งนี้ หากพิจารณาถึงบริบทของหลักการปฏิบัติงานเห็นได้ว่าการตรวจพิสูจน์พยานหลักฐานทางคอมพิวเตอร์และพยานหลักฐานทางดิจิทัลมีรูปแบบขั้นตอนไม่แตกต่างกัน กล่าวคือขอบการตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์ คือการรวบรวม (Collection) การเก็บรักษา (Preservation) การวิเคราะห์ (Analysis) และการนำเสนอหลักฐาน (Presentation) ที่เกี่ยวข้องกับคอมพิวเตอร์ (John R. Vacca, 2008) แม้จะมีกระบวนการเหมือนกันแต่กลับพบว่าการใช้ผู้เชี่ยวชาญในการตรวจพิสูจน์หลักฐานมีความแตกต่างกัน

วิเคราะห์กรอบแนวคิดการตรวจพิสูจน์หลักฐานทางดิจิทัลในกระบวนการยุติธรรมทางอาญา

พยานหลักฐานดิจิทัลถูกแสดงให้ปรากฏในรูปแบบข้อมูลทางอิเล็กทรอนิกส์ โดยสองสถานะในรูปแบบ 0 และ 1 หรือที่เรียกว่า เลขฐานสอง (Binary Number) ซึ่งแตกต่างจากพยานหลักฐานประเภทอื่น ๆ ที่แสดงออกให้เห็นทางกายภาพ เช่น อาวุธที่ใช้ในการกระทำผิด หรือเอกสารหลักฐานการกู้ยืมเงิน เป็นต้น ทำให้การรับรู้ ความเข้าใจในธรรมชาติของพยานประเภทนี้มีความแตกต่างกันไป ในหัวข้อนี้มีจุดมุ่งหมายเพื่อให้ความเข้าใจที่ครอบคลุมเกี่ยวกับการรวบรวม การเก็บรักษา การวิเคราะห์ และการนำเสนอหลักฐานดิจิทัลวิธีการ โดยมีประเด็นที่เกี่ยวข้องดังนี้

1. การรวบรวมและเก็บรักษาหลักฐานดิจิทัล

การรวบรวมและเก็บรักษาหลักฐานดิจิทัลเป็นแง่มุมพื้นฐานของการตรวจพิสูจน์หลักฐานดิจิทัล ซึ่งมีบทบาทสำคัญในการรับรองความสมบูรณ์และความน่าเชื่อถือของหลักฐานที่ใช้ในกระบวนการทางกฎหมาย อย่างไรก็ตามเมื่อพิจารณาจากหลักฐานดิจิทัลที่มีอยู่ทั่วไป แต่มีคนเพียงไม่กี่คนที่สามารถค้นหาหลักฐานดิจิทัลได้ ด้วยเหตุนี้ข้อมูลดิจิทัลจึงมักถูกมองข้ามและรวบรวมไม่ถูกต้อง อีกทั้งลักษณะเฉพาะที่เป็นเอกลักษณ์ของหลักฐานดิจิทัล เป็นประเด็นสำคัญที่ทำให้เกิดความท้าทายของบุคคลากรในกระบวนการยุติธรรมในการรวบรวมและการเก็บรักษา ซึ่งต้องใช้เครื่องมือ เทคนิค และวิธีการเฉพาะทางเพื่อปกป้องความถูกต้องของหลักฐานดิจิทัลอย่างเหมาะสม เนื่องจากความผิดพลาดใดๆ ในขั้นตอนนี้อาจส่งผลต่อความสมบูรณ์ของหลักฐานและอาจเป็นผลร้ายทางคดีในการยอมรับพยานหลักฐานดิจิทัลในศาล สอดคล้องกับ พรรณทิพย์ เต็มเจริญ (2565) เห็นว่าการเก็บรวบรวมพยานหลักฐานดิจิทัล และการรักษาพยานหลักฐาน มีความสำคัญอย่างยิ่ง เจ้าหน้าที่ต้องรู้เท่าทันอาชญากรรมคอมพิวเตอร์และอาชญากรรมเทคโนโลยีและเพิ่มศักยภาพองค์ความรู้ และความเชี่ยวชาญในการนำเทคโนโลยีมาประยุกต์ใช้ให้เกิดประโยชน์สูงสุดเพื่อนำตัวผู้กระทำผิดทางเทคโนโลยีมาดำเนินคดี (พรรณทิพย์ เต็มเจริญ, 2565) นอกจากนี้จากการศึกษาของ ณัฐนันท์ ใจซื่อ (2564) ทำให้ทราบแง่มุมเกี่ยวกับการใชดุลพินิจในการรวบรวมพยานหลักฐานดิจิทัลว่า ในปัจจุบันการรวบรวมพยานหลักฐานดิจิทัลมักขึ้นอยู่กับดุลพินิจในการปฏิบัติงานของเจ้าพนักงานที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่งเจ้าพนักงานตำรวจที่ประจำอยู่ที่สถานีตำรวจแต่ละแห่งซึ่งอาจมี

ระดับความรู้ความเข้าใจในเทคโนโลยีต่างกัน ปัญหาความเชี่ยวชาญในการค้นหา การจัดเก็บ การส่งต่อ และการใช้ประโยชน์จากพยานหลักฐานดิจิทัลเป็นปัญหาสำคัญที่พบค่อนข้างมาก (ณัฐนันท์ ใจซื่อ, 2564)

การรวบรวมและเก็บรักษาหลักฐานดิจิทัลจึงต้องปฏิบัติตามมาตรฐานสากลซึ่งใช้เป็นกฎเกณฑ์หรือแนวทางปฏิบัติอย่างเคร่งครัดในการเก็บรวบรวมและวิธีการรวบรวม ในกรณีที่มีการละเมิดข้อบังคับหรือกฎเกณฑ์ทางวิทยาศาสตร์ หลักฐานดิจิทัลอาจไม่ได้รับการยอมรับในศาล ปัจจุบันมาตรฐานและแนวทางสำคัญที่ได้รับการยอมรับอย่างกว้างขวางสำหรับการรวบรวมและการเก็บรักษาหลักฐานดิจิทัลอย่างมีประสิทธิภาพ เช่น

1. ACPO Guidelines (Association of Chief Police Officers) ซึ่งส่วนใหญ่ใช้ในสหราชอาณาจักร เป็นกรอบการทำงานสำหรับการจัดการหลักฐานดิจิทัลในลักษณะที่รักษาความสมบูรณ์โดยมีหลักการที่สำคัญคือ ไม่ควรดำเนินการใดๆ เปลี่ยนแปลงข้อมูลที่เก็บไว้บนคอมพิวเตอร์หรือสื่อจัดเก็บข้อมูลที่อาจนำไปใช้ในศาล ทั้งนี้เมื่อเข้าถึงข้อมูลต้นฉบับ

2. NIST Guidelines (National Institute of Standards and Technology) โดย NIST เป็นหน่วยงานหนึ่งภายใต้กระทรวงพาณิชย์ ประเทศสหรัฐอเมริกา แนวทางนี้จัดทำขึ้นครอบคลุมสำหรับการตรวจพิสูจน์หลักฐานทางดิจิทัลและการรวบรวมหลักฐานในสหรัฐอเมริกา โดยเสนอมาตรฐานสำหรับเครื่องมือ วิธีการ และกระบวนการทางนิติวิทยาศาสตร์

3. ISO/IEC 27037:2012 มาตรฐานสากลนี้ให้แนวทางในการระบุ รวบรวม การได้มา และรักษาหลักฐานดิจิทัล

4. SWGDE Guidelines (Scientific Working Group on Digital Evidence) เอกสารนี้ให้คำแนะนำและแนวทางปฏิบัติที่ดีที่สุดสำหรับการจัดการหลักฐานดิจิทัล โดยมุ่งเน้นไปที่การรักษาความสมบูรณ์และความถูกต้องของหลักฐาน

5. ข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐานของ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) เป็นแนวทางการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐานสำหรับการปฏิบัติงานในสถานที่เกิดเหตุและในห้องปฏิบัติการซึ่งครอบคลุมการจัดการคอมพิวเตอร์ สื่อบันทึกข้อมูลดิจิทัลแบบภายใน สื่อบันทึกข้อมูลดิจิทัลแบบภายนอก ข้อมูลคอมพิวเตอร์และเครื่องมือสื่อสารเคลื่อนที่ ให้มีความเหมาะสมและสอดคล้องกับมาตรฐานสากล

การปฏิบัติตามมาตรฐานและแนวทางปฏิบัติเหล่านี้เป็นสิ่งสำคัญสำหรับการรวบรวมและเก็บรักษาหลักฐานดิจิทัลที่เชื่อถือได้ เมื่อปฏิบัติตามแนวทางเหล่านี้จะสามารถมั่นใจได้ว่าหลักฐานดิจิทัลยังคงมีความน่าเชื่อถือและเป็นที่ยอมรับได้ในศาล ซึ่งนำไปใช้สนับสนุนการแก้ปัญหาคดีความได้อย่างยุติธรรม

2. การวิเคราะห์และการตีความหลักฐานดิจิทัล

การวิเคราะห์และการตีความหลักฐานดิจิทัลมีบทบาทสำคัญในระบบยุติธรรมทางอาญา เป็นการให้ข้อมูลเชิงลึกที่สำคัญเกี่ยวกับหลักฐานดิจิทัล อย่างไรก็ตามเทคโนโลยีมีการพัฒนาอย่างต่อเนื่อง ความซับซ้อนและความหลากหลายของหลักฐานดิจิทัลก็มีมากขึ้นเช่นกัน ตั้งแต่อีเมล ข้อความไปจนถึงข้อมูลที่ซับซ้อนจากระบบคลาวด์ กระบวนการวิเคราะห์หลักฐานดิจิทัลไม่เพียงแต่การใช้เครื่องมือที่เหมาะสมกับประเภทของหลักฐานหรือทักษะทางเทคนิคขั้นสูงเท่านั้น แต่ยังต้องมีความเข้าใจอย่างลึกซึ้งเกี่ยวกับบริบททางกฎหมายที่จะนำเสนอ ความ

เข้าใจของผู้ตรวจหลักฐานทางดิจิทัลกับประเด็นทางกฎหมาย จึงเป็นสิ่งสำคัญที่ต้องดำเนินการควบคู่กันไป ตัวอย่างเช่น เมื่อพนักงานสอบสวนนำเทปบันทึกเสียงส่งตรวจพิสูจน์คดีหมิ่นประมาท ผู้ตรวจนอกจากจะต้องทำการวิเคราะห์ว่าเทปบันทึกเสียงดังกล่าวถูกสร้างขึ้นมาหรือไม่ มีการตัด ต่อ เติมเสียงในเทปบันทึกนั้นหรือไม่แล้ว ผู้ตรวจต้องเข้าใจด้วยว่าข้อความใดเป็นข้อความหมิ่นประมาท หรือ ภาพแบบใดเป็นภาพอนาจาร ดังนั้น หากผู้ตรวจไม่เข้าใจบริบทกฎหมายเกี่ยวกับเรื่องนั้น ๆ อาจทำให้การวิเคราะห์และการตีความหลักฐานทางดิจิทัลคลาดเคลื่อนได้

การจัดการปัญหาในประเด็นนี้เจ้าหน้าที่ตำรวจต้องอำนวยความสะดวกให้แก่ผู้ตรวจ คือ ต้องระบุขอบเขตของสิ่งที่พนักงานสอบสวนต้องการจากพยานหลักฐานที่ส่งตรวจ หากเป็นคดีหมิ่นประมาทต้องระบุให้ชัดว่า ข้อความแบบใดเข้าข่ายเป็นความผิดหมิ่นประมาท เพื่อให้ผู้ตรวจสามารถค้นหาข้อมูลเพื่อนำไปวิเคราะห์และตีความข้อมูลได้อย่างถูกต้อง

3. การนำเสนอหลักฐานดิจิทัล

กระบวนการนำเสนอการตรวจพิสูจน์หลักฐานดิจิทัลในระบบยุติธรรมทางอาญาเป็นขั้นตอนสำคัญซึ่งนำเสนอเทคนิคที่ซับซ้อนมาแปลข้อมูลเป็นหลักฐานที่ชัดเจนและเข้าใจได้ถึงที่มาและความน่าเชื่อถือของกระบวนการตรวจพิสูจน์หลักฐานดิจิทัลซึ่งสามารถนำไปใช้ในศาลได้อย่างมีประสิทธิภาพ เนื่องจากหลักฐานดิจิทัลมีอิทธิพลต่อการดำเนินคดีมากขึ้นในคดีที่เกี่ยวกับอาชญากรรมไซเบอร์ วิธีการนำเสนออาจส่งผลกระทบอย่างมากต่อผลลัพธ์ของคดี กระบวนการนี้ไม่เพียงแต่เกี่ยวข้องกับการถ่ายทอดรายละเอียดทางเทคนิคของการตรวจพิสูจน์หลักฐานดิจิทัลแต่ยังต้องทำให้เกิดความมั่นใจได้ว่าผู้พิพากษา อัยการ ทนายความ โจทก์ จำเลย ซึ่งบุคคลเหล่านี้อาจไม่มีพื้นฐานทางวิทยาศาสตร์สามารถเข้าใจได้ อย่างไรก็ตามปัญหาที่มักเกิดขึ้นในกระบวนการนี้คือ

1. ความซับซ้อนทางเทคนิค การตรวจพิสูจน์หลักฐานดิจิทัลมักเกี่ยวข้องกับข้อมูลทางเทคนิคขั้นสูงซึ่งอาจเป็นเรื่องยากสำหรับผู้พิพากษา อัยการ และคู่ความในคดีที่จะเข้าใจความซับซ้อนของหลักฐาน รวมถึงรายละเอียดเกี่ยวกับการเข้ารหัสข้อมูล (Data Encryption) ข้อมูลจราจรทางคอมพิวเตอร์ (Log File) และข้อมูลเมทาดาตา (Metadata) สามารถสร้างอุปสรรคต่อความเข้าใจได้ ผลกระทบที่ตามมาหากหลักฐานไม่ถูกนำเสนออย่างชัดเจน อาจถูกเข้าใจผิดหรือประเมินคุณค่าต่ำเกินไป อาจนำไปสู่ข้อสรุปหรือการตัดสินใจที่ไม่ถูกต้อง

2. การแปลศัพท์ทางเทคนิค ผู้เชี่ยวชาญด้านการตรวจพิสูจน์หลักฐานดิจิทัลต้องแปลคำศัพท์ทางเทคนิคที่ซับซ้อนเป็นคำศัพท์ทั่วไปที่วิญญูชนเข้าใจได้ ปัญหาที่เกิดขึ้นคือ คำศัพท์ทางคอมพิวเตอร์มักไม่มีคำศัพท์บัญญัติส่วนมากใช้ทับศัพท์ การสื่อสารที่ผิดพลาดอาจนำไปสู่การตีความหลักฐานที่ผิดพลาดได้

3. ความเชี่ยวชาญของพยานผู้เชี่ยวชาญ ความน่าเชื่อถือเกี่ยวกับความเชี่ยวชาญของผู้เชี่ยวชาญด้านการตรวจพิสูจน์หลักฐานดิจิทัลอาจเป็นประเด็นที่คู่ความฝ่ายใดฝ่ายหนึ่งตั้งคำถามถึงได้โดยเฉพาะอย่างยิ่งหากคู่กรณีที่ต้องได้รับผลร้ายจากพยานหลักฐานดิจิทัลนั้น ซึ่งอาจส่งผลกระทบความน่าเชื่อถือของผู้เชี่ยวชาญนำไปสู่การปฏิเสธหรือลดคุณค่าความน่าเชื่อถือของหลักฐานทางดิจิทัลได้

4. พลวัตของหลักฐานดิจิทัล ธรรมชาติของหลักฐานดิจิทัลบางอย่างมีลักษณะเป็นพลวัต (Dynamic) ซึ่งอาจมีการเปลี่ยนแปลงเมื่อเวลาผ่านไป เช่น ในกรณีของบันทึกที่มีการอัพเดตอย่างต่อเนื่องการนำเสนอหลักฐานดังกล่าวอย่างถูกต้องจำเป็นต้องมีการจัดการอย่างระมัดระวังเพื่อแสดงสถานะของข้อมูลดิจิทัลใน

ช่วงเวลาที่เกี่ยวข้องกับการกระทำผิด หากไม่สามารถนำเสนอเช่นนั้นได้อาจทำให้คุณค่าของหลักฐานดิจิทัลมีความน่าเชื่อถือลดลง

จากที่กล่าวมาข้างต้นเห็นได้ว่าการนำเสนอหลักฐานดิจิทัลในระบบยุติธรรมทางอาญาเต็มไปด้วยความท้าทายที่อาจส่งผลต่อประสิทธิผลและการยอมรับหลักฐานดิจิทัล การแก้ไขปัญหาเหล่านี้ไม่เพียงแต่ต้องการความเชี่ยวชาญด้านเทคนิคเท่านั้น แต่ยังรวมถึงความสามารถในการสื่อสารข้อมูลที่ซับซ้อนในลักษณะที่ชัดเจนเป็นกลางและถูกต้องตามกฎหมาย

บทสรุป/ข้อเสนอแนะ

กรอบแนวคิดการตรวจพิสูจน์หลักฐานดิจิทัลในกระบวนการยุติธรรมทางอาญาให้แนวทางที่มีโครงสร้างในการจัดการ วิเคราะห์ และนำเสนอหลักฐานดิจิทัลในบริบททางกฎหมาย กรอบแนวคิดนี้นำเสนอประเด็นความท้าทายที่เกิดจากหลักฐานดิจิทัล รวมถึงความซับซ้อนทางเทคนิค ความจำเป็นในการปฏิบัติหลักการทางวิทยาศาสตร์ที่เข้มงวด และความสำคัญของการปฏิบัติตามมาตรฐานสากล ซึ่งมีส่วนครอบคลุมทุกขั้นตอนของการตรวจพิสูจน์หลักฐานดิจิทัลตั้งแต่การระบุเบื้องต้นและการรวบรวมหลักฐาน ไปจนถึงการเก็บรักษา การวิเคราะห์ และการนำเสนอขั้นสุดท้ายในศาล ทั้งนี้องค์ประกอบสำคัญของกรอบการทำงาน ได้แก่ การรักษาความสมบูรณ์และความถูกต้องของหลักฐานดิจิทัลผ่านการใช้เครื่องมือและวิธีการทางนิติวิทยาศาสตร์ที่เหมาะสมและการแปลข้อมูลทางเทคนิคที่ซับซ้อนให้เป็นข้อมูลที่ชัดเจนและเข้าใจได้สำหรับบุคลากรในกระบวนการยุติธรรมทางอาญาไม่ว่าจะเป็นทนายความ ตำรวจ อัยการ หรือผู้พิพากษา เพื่อสนับสนุนผลลัพธ์ที่ยุติธรรมในการตัดสินคดี

อย่างไรก็ตามเพื่อให้การทำงานภายใต้กรอบแนวคิดเกี่ยวกับการตรวจพิสูจน์หลักฐานทางดิจิทัลมีประสิทธิภาพมากยิ่งขึ้น ผู้เขียนจึงมีข้อเสนอแนะดังต่อไปนี้

1. การตรวจพิสูจน์หลักฐานดิจิทัลควรตรวจสอบให้แน่ใจว่ากรอบการทำงานสอดคล้องกับข้อกำหนดทางกฎหมายสำหรับการยอมรับหลักฐานดิจิทัลในศาลหรือไม่ เช่น การขอออกหมายค้น ตำรวจควรระบุขอบเขตสิ่งที่ต้องการค้นไว้คร่าวๆ ที่เกี่ยวข้องกับการกระทำผิดลดปัญหาข้อโต้แย้งการค้นไม่ชอบด้วยกฎหมาย นอกจากนี้การทำความเข้าใจและการรวมมาตรฐานต่างๆ มาประยุกต์ใช้เช่น แนวทาง ACPO และมาตรฐาน ISO/IEC เป็นสิ่งสำคัญเพื่อทำให้แน่ใจว่า วิธีการทางนิติวิทยาศาสตร์ที่ใช้นั้นถูกต้องหลักการวิทยาศาสตร์และกฎหมาย

2. ความร่วมมือแบบสหวิทยาการ การตรวจพิสูจน์หลักฐานดิจิทัลมักต้องการความร่วมมือระหว่างผู้มีส่วนได้ส่วนเสียต่างๆ ซึ่งรวมถึงหน่วยงานบังคับใช้กฎหมาย ผู้เชี่ยวชาญด้านกฎหมาย ผู้เชี่ยวชาญด้านนิติวิทยาศาสตร์ และผู้เชี่ยวชาญด้านไอที ดังนั้น ควรสร้างความร่วมมือสำหรับการทำงานร่วมกันแบบสหวิทยาการเพื่อให้เกิดการถ่ายทอดประสบการณ์ ซึ่งอาจรวมถึงการฝึกอบรม คณะทำงานร่วม เป็นต้น

3. แนวทางการรายงานผลและการนำเสนอที่มีประสิทธิภาพ ควรกำหนดแนวทางการรายงานผลการตรวจพิสูจน์หลักฐานดิจิทัลในลักษณะที่วิญญูชนทั่วไปสามารถเข้าใจได้ ซึ่งอาจรวมถึงแนวทางในการแสดงภาพ การลดความซับซ้อนของศัพท์ทางเทคนิค และการนำเสนอหลักฐานในรูปแบบการบรรยายที่สอดคล้องกับบริบทโดยรวมของคดี เป็นต้น

เอกสารอ้างอิง

เหมือน สุขมาตย์. (2562). ความรับผิดทางอาญาของปัญญาประดิษฐ์. วารสารวิชาการ คณะนิติศาสตร์ มหาวิทยาลัยราชภัฏอุบลราชธานี, 7(2), 37-49.

แลร์รี อี. แดเนียล, ลาร์ส อี. แดเนียล. (2559). การตรวจพิสูจน์หลักฐานดิจิทัลสำหรับผู้ประกอบวิชาชีพกฎหมาย: เข้าใจพยานหลักฐานดิจิทัลจากขั้นตอนหมายถึงห้องพิจารณาคดี. แปลโดย สุนีย์ สกาวรัตน์. กรุงเทพมหานคร: มูลนิธิเพื่ออินเทอร์เน็ตและวัฒนธรรมเมือง.

ซามูเอล กรีนการ์ด. (2560). อินเทอร์เน็ตแห่งสรรพสิ่ง. แปลโดย ทีปกร วุฒิพิทยามงคล. กรุงเทพมหานคร: โอเพ่น เวิลด์ส พับลิชชิ่ง เฮาส์.

ณัฐนันท์ ใจซื่อ. (2564). มาตรการทางกฎหมายเกี่ยวกับการรับฟังพยานหลักฐานดิจิทัล. วารสารมหาวิทยาลัยราช ภัฏมหาสารคาม, 15(1), 109-121.

ถิรพิรุฬห์ ทองคำวิฑูรย์. (2559). เทคโนโลยี Internet of Things และข้อเสนอแนะในการบริหารคลื่นความถี่ใน ประเทศไทย. วารสารกิจการสื่อสารดิจิทัล, 1(1), 168-172.

นัทธ์ ธเนศวาณิชย์. (2555). การรับฟังและวิธีการนำสืบพยานหลักฐานอิเล็กทรอนิกส์ในคดีอาญา ศึกษาตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550. ใน วิทยานิพนธ์. กรุงเทพมหานคร: คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์.

พรรณทิพย์ เต็มเจริญ. (2565). แนวทางการพิจารณาและรวบรวม พยานหลักฐานเกี่ยวกับการกระทำความผิดโดย ใช้เทคโนโลยี: ระบบคลาวด์. วารสาร DSI, 14(1), 11-18.

พัฒนาพร โกวพัฒนกิจ และคณะ. (2560). แนวโน้มพฤติการณ์ในการกระทำความผิดทางอาญาที่เกี่ยวกับ เทคโนโลยีสารสนเทศ. ใน รายงานวิจัยเสนอ สถาบันวิจัยและพัฒนารพีพัฒนศักดิ์. กรุงเทพมหานคร: สำนักงานศาลยุติธรรม.

ภูมินทร์ บุตรอินทร์. (2561). กฎหมายกับปัญญาประดิษฐ์. วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 47(3), 491-511.

วิวัฒน์ มีสุวรรณ์. (2559). อินเทอร์เน็ตเพื่อสรรพสิ่ง (Internet of Things) กับการศึกษา. วารสารวิชาการ นวัตกรรมสื่อสารสังคม, 4(2), 83-92.

สาวตรี สุขศรี. (2563). กฎหมายว่าด้วยอาชญากรรมคอมพิวเตอร์และอาชญากรรมไซเบอร์. กรุงเทพมหานคร: โครงการตำราและเอกสารประกอบการสอน คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์.

สาวตรี สุขศรี และคณะ. (2555). อาชญากรรมคอมพิวเตอร์: ผลกระทบจากพระราชบัญญัติว่าด้วยการกระทำ ความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และนโยบายของรัฐกับสิทธิเสรีภาพในการแสดงความคิดเห็น. กรุงเทพมหานคร: โครงการอินเทอร์เน็ตเพื่อกฎหมายประชาชน.

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2565). การสำรวจพฤติกรรมผู้ใช้อินเทอร์เน็ตในประเทศไทย ปี 2565. เข้าถึงได้จาก กระทรวงดิจิทัล ETDA: https://www.etda.or.th/th/Useful-Resource/publications/iub2022.aspx

Damshenas, M., Dehghantanha, A., and Mahmoud, R. (2014). A Survey on Digital Forensics Trends. International Journal of Cyber-Security and Digital Forensics (IJCSDF), 3(4), 209-234.

Easttom, C. and Taylor, J. (2011). Computer Crime, Investigation, and the Law,. Massachusetts: Cengage Learning PTR.

Gary C. Kessler. (2010). Judges' Awareness, Understanding, and Application of Digital Evidence. In Ph.D. Diss. Florida: Nova Southeastern University.

Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? Social & Legal Studies, 10(2), 243–249.

John R. Vacca. (2008). Computer Forensics: Computer Crime Scene Investigation (2nd ed.). Boston: Charles River Media.

Nina Sunde a, and Itiel E. Dror. (2019). Cognitive and human factors in digital forensics: Problems, challenges, and the way forward. Digital Investigation, 29, 101-108.

Qusay F. Hassan, Atta ur Rehman Khan, Sajjad A. Madani (Eds). (2018). Internet of Things Challenges, Advances, and Applications. New York: CRC Press.

Raymond Lutui. (2016). A multidisciplinary digital forensic investigation process model. Business Horizons, 59(6), 593-604.

Reith, M., Carr, C., and Gunsch, G. (2002). An examination of digital forensic models. International Journal of Digital Evidence, 1(3). 1-12.

Thomas J. Holt and Adam M. Bossler. (2016). Cybercrime in Progress Theory and prevention of technology-enabled offenses. New York: Routledge.

Thomas J. Holt, Adam M. Bossler, Kathryn C. Seigfried-Spellar. (2017). Cybercrime and Digital Forensics: An Introduction. New York: Routledge.

Van Buskirk, E., and Liu, V. T. . (2006). Digital evidence: challenging the presumption of reliability. Journal of Digital Forensic Practice, 1(1), 19-26.

Vassil Roussev. (2016). Digital Forensic Science: Issues, Methods, and Challenges. San Antonio: Morgan & Claypool Publishers.