Received: 2021 – 05 – 02
Revised: 2021 – 06 – 04
Accepted: 2021 – 06– 09

กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล: การวิเคราะห์เพื่อพัฒนาเชิงนโยบาย

Digital Forensics Evidence Proving Process: An Analytic Approach to Policy Development

กานต์ ศรีสุวรรณ*สุมนทิพย์ จิตสว่าง*
Karnt Srisuwan*Sumonthip Jitsawang*
หลักสูตรศิลปศาสตรดุษฎีบัณฑิต สาขาวิชาอาชญาวิทยาและงานยุติธรรม จุฬาลงกรณ์มหาวิทยาลัย
Philosophy in Criminal Justice, Chulalongkorn University
E-mail: karnt@karnt.com

บทคัดย่อ

บทความนี้มีวัตถุประสงค์ในการนำเสนอกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลเพื่อนำไปสู่ข้อเสนอเชิงนโยบาย โดยเนื้อหาเกี่ยวกับลักษณะเฉพาะของพยานหลักฐานดิจิทัล กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล การรับฟังพยานหลักฐานอิเล็กทรอนิกส์หลักการในการพิสูจน์พยานหลักฐานดิจิทัลและข้อเสนอเชิงนโยบาย โดยใช้วิธีการศึกษาจากเอกสาร ตำรา งานวิจัยและการลงพื้นที่สัมภาษณ์เชิงลึกจากนักวิชาการ ผู้มีส่วนเกี่ยวข้องกับการตรวจพิสูจน์พยานหลักฐานดิจิทัลเนื่องจากโลกยุคปัจจุบันเป็นโลกของเทคโนโลยีสารสนเทศ และการสื่อสารไร้พรมแดนด้วยการเชื่อมโยงโลกเข้าด้วยกันของอินเทอร์เน็ต เทคโนโลยีสารสนเทศเข้ามามีบทบาทต่อการดำเนินชีวิตประจำวันเป็นอย่างมากจนเรียกได้ว่า เป็นส่วนหนึ่งของการดำรงชีวิต จากการศึกษาพบว่า ปัจจุบันแม้มีการจัดทำมาตรฐานการจัดการอุปกรณ์ดิจิทัลในการตรวจพิสูจน์พยานหลักฐานดิจัลโดยศูนย์ดิจิทัลฟอเรนสิกส์ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ทำ ให้กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลมีมาตรฐานการปฏิบัติที่ชัดเจนมากขึ้นแต่ก็ยังต้องมีการปรับปรุงพัฒนาให้ครอบคลุมครบถ้วนตามบริบทของสังคมปัจจุบัน ข้อเสนอแนะจากการศึกษาในครั้งนี้ คือ ทุกกระบวนการของกระบวนการยุติธรรมทางอาญา ต้องมีการบูรณาการในการจัดการพยานหลักฐานดิจิทัล โดยเฉพาะในขั้นตอนการสืบสวน สอบสวน การรวมรวมพยานหลักฐาน และการรับฟังพยานหลักฐานดิจิทัล ต้องมีมาตรฐานทางการปฏิบัติที่ชัดเจนและสอดคล้องกับมาตรฐานสากล เปิดโอกาสให้หน่วยงานอื่นที่มีศักยภาพ และมาตรฐานเป็นที่ยอมรับเข้ามาร่วมในการตรวจพิสูจน์พยานหลักฐาน และควรมีกฎหมายหรือหลักประกันที่เป็นมาตรฐานในการตรวจพิสูจน์พยานหลักฐานดิจิทัล เพื่อ อำนวยความเป็นธรรมให้กับทุกฝ่ายในกระบวนการยุติธรรม

คำสำคัญ: พยานหลักฐานดิจิทัล, การตรวจพิสูจน์พยานหลักฐานดิจิทัล, อาชญากรรมคอมพิวเตอร์, ข้อเสนอเชิงนโยบาย

Abstract

The objective of this study is to present digital forensics evidence proving process and policy development which included special characteristics of digital evidence, digital forensics process, principles of digital forensics as well as policy development by applying a variety of different sources, from the most recent articles, books, research papers, and in-depth interviews with scholars who involve in digital forensics. Nowadays is a world of information technology and borderless communication. Internet is connecting the world together. Information technology therefore plays a very important role in daily life and be a part of life. This research found that nowadays there is a digital forensic management standard for digital forensics, provided by the Digital Forensics Center under the Electronic Transactions Development Agency (ETDA), that makes the digital forensic process meet the standards demanded to comprehensible standards of practice. However, the process to acquire digital evidence still remains unclear. This research suggests that in every step of criminal procedure for digital forensic management, particularly, investigation process, inquiry process, gathering of digital evidence, and the digital evidential hearing should have clear standards of conduct and practice to meet international standards and should give an opportunity of participation to other potential agencies in digital evidence forensics. Furthermore, there should be laws or guarantees that create standards for forensics, that lead to bringing justice to every party in the criminal justice process.

Keywords: Digital Evidence, Digital Forensics, Cybercrime, Proposed Policy

บทนำ

สำหรับโลกยุคปัจจุบันเครือข่ายอินเทอร์เน็ตและสังคมดิจิทัลเข้ามามีบทบาทและส่งผลต่อการเปลี่ยนแปลงในรูปแบบและวัฒนธรรมการดำรงชีวิตของคนมากขึ้น เครือข่ายสังคม (Social network) หรือชุมชนออนไลน์ต่างๆ เข้ามาเป็นส่วนหนึ่งของการใช้ชีวิต ควบคู่ไปกับการเติบโตของตลาดอุปกรณ์พกพาอัจฉริยะ (Smart portable devices) ที่เป็นมากกว่าแค่อุปกรณ์สื่อสาร ความก้าวหน้าทางเทคโนโลยี การพลิกผันทางดิจิทัล (Digital disruption) ทำให้โลกของเรามีการผลิตข้อมูลปริมาณมหาศาลในทุกวินาที ส่งผลให้ชีวิตประจำวันของผู้คนสะดวกสบายและง่ายขึ้น แต่นอกจากประโยชน์อันมหาศาลที่ผู้คนได้รับจากการเปลี่ยนแปลงนี้ ก็นำมาซึ่งอาชญากรรมอีกรูปแบบที่อาจคุกคามชีวิต ทรัพย์สินเงินทอง รวมถึงส่งผลกระทบด้านอื่นๆอย่างมากมายเช่นกัน ในประเทศไทยสถิติจำนวนผู้ใช้งานอินเทอร์เน็ตเพิ่มมากขึ้นแบบก้าวกระโดด อาชญากรรมคอมพิวเตอร์ในประเทศไทยมีแนวโน้มเพิ่มสูงขึ้นอย่างรวดเร็ว เมื่อมองย้อนกลับไปดูในช่วง 10 ปีที่ผ่านมา หรือเทียบ 3 ปีย้อนหลัง จะเห็นแนวโน้มชัดเจนว่า แต่เดิมอาชญากรรมคอมพิวเตอร์ที่คนทั่วไปรู้จักจากเพียงฉากในภาพยนตร์ก็คืบคลานเข้ามาใกล้ตัว เข้ามาในชีวิตประจำวันของเรามากขึ้น อุปกรณ์มือถือที่เชื่อมต่อกับเครือข่ายอินเทอร์เน็ตได้มีราคาถูกลง ใช้กันอย่างแพร่หลาย เครือข่ายอินเทอร์เน็ตมีความเร็วสูงขึ้น เป้าหมายของการก่ออาชญากรรมคอมพิวเตอร์ เดิมมีเป้าหมาย และจุดประสงค์เฉพาะ เน้นการทดสอบ ทดลอง หรือก่อกวนเป็นจุดๆ มีผู้ก่อเหตุคนเดียวหรือกลุ่มย่อยๆ เนื่องจากสมัยก่อนการติดต่อสื่อสารกันทำได้ยาก ต้องอาศัยช่องทางเฉพาะ ในปัจจุบันมีลักษณะเป็นกลุ่มขนาดใหญ่มากขึ้นคล้ายกับองค์กรอาชญากรรม เป้าหมายและวัตถุประสงค์เปลี่ยนไป มีการขู่ เรียกเงินจากทั้งรายบุคคล และหน่วยงาน (Ransomeware มีการเติบโตอย่างเห็นชัดเจนในปี พ.ศ. 2560-2562 เมื่อเทียบกับปี

ก่อนๆ และหลายตัว ยังไม่สามารถแก้ไขได้) มุ่งเน้นที่สถาบันการเงินมากขึ้น เน้นทำลายระบบมากกว่าการก่อกวน และมีการสร้างความหวาดกลัวในวงกว้างคล้ายกับองค์กรก่อการร้ายผ่านทางเครือข่ายสังคมที่ยากต่อการควบคุม มีเทคนิคใหม่ๆมากขึ้นในการเจาะ ทำลายระบบ ซึ่งยากต่อการป้องกันด้วยอุปกรณ์เดี่ยวๆแต่เดิม ในสมัยก่อนความเสียหายเกิดขึ้นในวงแคบ แม้จะร้ายแรงแต่สามารถควบคุมจัดการได้ ติดตามจับกุมผู้กระทำผิดได้ง่าย เนื่องจากการกระทำผิดมักเชื่อมต่อมาจากจุดๆ เดียว มีเป้าหมายเดียว ในขณะที่ปัจจุบันการจับกุมกระทำยากขึ้น เนื่องจากประสิทธิภาพของอุปกรณ์พกพาและความเร็วเครือข่าย ความเสียหายเกิดขึ้นพร้อมกันหลายจุด และผู้ก่อเหตุร่วมมือกัน "ข้ามชาติ" เป็นขบวนการ จากข้อมูลสถิติเกี่ยวกับอาชญากรรมคอมพิวเตอร์ในปี พ.ศ.2555 พบว่ามีผู้ตกเป็นเหยื่ออาชญากรรมคอมพิวเตอร์มากกว่า 556 ล้านคนต่อปี โดยคิดเป็น 1.5 ล้านคนต่อวัน 1,080 คนต่อนาทีและ 18 คนต่อวินาที โดยสามารถขโมยเงินได้มากถึงประมาณ 3,500,000,000,000 บาทต่อปี หรือสามารถขโมยเงินจากเหยื่อได้เฉลี่ย 6,300 บาทต่อคนต่อปี มูลเหตุจูงใจที่ทำให้ก่ออาชญากรรม อันดับหนึ่ง ร้อยละ 94 คือ เหตุผลทางด้านการเงิน, อันดับสอง ร้อยละ 3 คือ ความไม่เห็นด้วยหรือการประท้วงต่อต้าน, อันดับสาม ร้อยละ 2 เพราะความสนุกสนานความอยากรู้อยากเห็น ความภาคภูมิใจ และอันดับสุดท้าย ร้อยละ 1 ความโกรธแค้นส่วนตัว นอกจากนี้ ยังสำรวจพบว่าอาชญากรรมคอมพิวเตอร์สามารถเข้าถึงคอมพิวเตอร์ผ่านการเจาะระบบ (Hacking) มากที่สุดเป็นอันดับหนึ่ง อันดับสองคือ มัลแวร์ (Malware) ตามด้วยการโจรกรรมข้อมูลโดยตรงโดยการลักลอบทำสำเนาข้อมูลในบัตรเครดิต บัตรเอทีเอ็ม หรือทำบัตรปลอม การหลอกถามข้อมูลตัวต่อตัวทางโทรศัพท์ ผ่านอีเมล และสุดท้ายคือการนำข้อมูลของลูกค้ามาเปิดเผย นอกจากนี้อาชญากรรมพื้นฐาน (Traditional street crimes) เอง ก็เกิดขึ้นในชุมชนออนไลน์ หรือเกี่ยวเนื่องกับสังคมดิจิทัลมากขึ้น

สำหรับประเทศไทย หลังจากที่มีการประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 หรือที่มักเรียกกันว่า พระราชบัญญัติคอมพิวเตอร์ ก็ได้มีการรวบรวมสถิติการดำเนินคดีตามพระราชบัญญัตินี้ เพื่อเก็บเป็นสถิติ โดยตัวอย่างข้อมูลจากศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย หรือไทยเซิร์ต ในปี พ.ศ. 2550–2554 พบว่าเว็บไซต์หน่วยงานด้านการศึกษามีไวรัสมากกว่าเว็บไซต์หน่วยงานอื่น คิดเป็นร้อยละ 48 และในปี พ.ศ. 2555 ประเทศไทยมีสถิติการหลอกลวงต้มตุ๋นทางอินเทอร์เน็ตมากที่สุดในจำนวนภัยคุกคาม คิดเป็นร้อยละ 67 ในส่วนของการดำเนินคดี จากการรวบรวมข้อมูลตั้งแต่เดือนกรกฎาคม พ.ศ. 2550 จนถึงเดือนกรกฎาคม พ.ศ. 2553 พบว่ามีคดีที่เข้าข่ายผิดกฎหมายตามพระราชบัญญัตินี้ทั้งสิ้น 185 คดี โดยแบ่งเป็น พ.ศ. 2550 จำนวน 9 คดี พ.ศ. 2551 จำนวน 28 คดี พ.ศ. 2552 จำนวน 72 คดี และใน พ.ศ. 2553 จำนวน 73 คดี โดยสามารถจำแนกคดีได้ตามขั้นของกระบวนการพิจารณาคดีและผลของคดี คือ คดีที่อยู่ในชั้นพนักงานสอบสวนหรือเจ้าหน้าที่ตำรวจ 74 คดี คดีที่พนักงานอัยการสั่งฟ้อง 43 คดี คดีที่พนักงานอัยการสั่งไม่ฟ้อง 1 คดี คดีที่มีการไกล่เกลี่ย ยอมความ ถอนฟ้อง 10 คดี คดีที่ศาลพิพากษายกฟ้องโจทก์ 2 คดี คดีที่ศาลพิพากษาว่าจำเลยมีความผิด 37 คดี คดีที่ศาลพิพากษาแล้วแต่ไม่สามารถเข้าถึงผลการพิจารณาคดีได้ 14 คดี คดีที่พนักงานสอบสวนตั้งข้อหาตามพระราชบัญญัติคอมพิวเตอร์ แต่พนักงานอัยการไม่ได้สั่งฟ้องตามข้อหาดังกล่าว หรือศาลไม่ได้พิพากษาว่าเป็นความผิดตามพระราชบัญญัติคอมพิวเตอร์ 4 คดี

ประชาชนทั่วไป รวมถึงหน่วยงานภาครัฐ ภาคเอกชน แม้มีความคุ้นเคยกับการใช้งานเครือข่ายอินเทอร์เน็ต แต่ยังขาดความรู้ความเข้าใจในปัญหาและการป้องกันอาชญากรรมคอมพิวเตอร์ เมื่อมีการออกพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติฉบับที่ 2 ในปี พ.ศ. 2560 และกฎหมายอื่นๆ ที่เกี่ยวข้อง ซึ่งมีบทลงโทษสำหรับผู้กระทำผิด แต่สถิติการเกิดคดีก็ยังคงสูงอย่างต่อเนื่อง ดังนั้นจึงควรมีการพิจารณาถึงปัญหา สาเหตุ แนวทางป้องกันแก้ไข ทั้งทางด้านกฎหมายและด้านอื่นๆ เพื่อให้ความเสียหายที่เกิดจากอาชญากรรมคอมพิวเตอร์ลดน้อยลง สำหรับในส่วนตำรวจเองได้มีการจัดตั้งกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บอท.) แต่ก็ยังมีปัญหาในส่วนเจ้าหน้าผู้ปฏิบัติงานขาดทักษะ ความรู้ด้านเทคนิคคอมพิวเตอร์ ประสบความยากลำบากในการแกะรอยผู้บุกรุกเข้าสู่ระบบ

ปัญหาในการชี้และรวบรวมพยานหลักฐาน และข้อจำกัดด้านกฎหมายต่างๆ ตลอดจนขาดสถิติ และความรู้เกี่ยวกับรูปแบบและลักษณะอาชญากรรมคอมพิวเตอร์ในประเทศไทย บวกกับการเปลี่ยนแปลงอย่างรวดเร็วของเทคโนโลยีคอมพิวเตอร์ มาตรการการกำกับดูแลต่างๆที่ใช้ก็ยังไม่ครอบคลุม ไม่สามารถบังคับใช้ได้อย่างมีประสิทธิภาพ มีประเด็นใหม่ๆเกิดขึ้นในสังคม เกิดความสงสัย ข้อโต้แย้งมากมายว่าผู้ที่เกี่ยวข้องในกระบวนการยุติธรรม เช่น ตำรวจใช้บรรทัดฐานใดก่อนจะพิจารณารับเป็นคดี การดำเนินการตามขั้นตอนต่างๆในการจับกุม ตลอดจนการใช้พยานหลักฐานดิจิทัล (Digital evidences) และการตรวจพิสูจน์พยานหลักฐานดิจิทัล (Digital forensics) มีกระบวนการอย่างไร ทำให้ทราบถึงความจำเป็นที่จะต้องตระหนักและมีความเข้าใจในปัญหาอาชญากรรมคอมพิวเตอร์ สาเหตุของอาชญากรรมคอมพิวเตอร์ในบริบทของทฤษฎีอาชญาวิทยาและทฤษฎีทางสังคม สิทธิ หน้าที่ เสรีภาพ กฎหมายที่เกี่ยวข้อง ตลอดจนต้องมีการกำหนดนโยบายทางอาญา มีขั้นตอนการจับกุมและกรอบการตรวจพิสูจน์พยานหลักฐานดิจิทัลที่ชัดเจน เพื่อที่จะได้มีเกณฑ์ที่ใช้และการดำเนินการในทิศทางเดียวกัน ขจัดความเคลือบแคลงสงสัยในประเด็นทางสังคมเหล่านี้ และนำไปสู่ข้อเสนอเชิงนโยบายและปฏิบัติ ตลอดจนข้อเสนอในการปรับปรุงกฎหมายและการบังคับใช้ เพื่อยกระดับกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล และกระบวนการยุติธรรมทางอาญาที่เกี่ยวข้องกับการกระทำความผิดทางคอมพิวเตอร์ในประเทศไทย เพื่อให้สามารถพัฒนาการป้องกันปราบปรามอาชญากรรมคอมพิวเตอร์ในประเทศไทย และนำไปสู่การแก้ไขปัญหาอาชญากรรมคอมพิวเตอร์ในประเทศไทยอย่างมีประสิทธิภาพและสอดคล้องกับมาตรฐานสากล

กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล (Digital Forensics Evidence Proving Process)

การตรวจพิสูจน์พยานหลักฐานดิจิทัลในประทศไทยยังคงเป็นเรื่องใหม่ แต่แนวโน้มและความสำคัญกำลังเพิ่มมากขึ้น ความหมายที่แท้จริงของ Digital forensics หรือ การตรวจพิสูจน์พยานหลักฐานดิจิทัล สามารถทำความเข้าใจง่ายๆ คือ การรวบรวมข้อมูลหลักฐาน การพิสูจน์หลักฐานทางคอมพิวเตอร์และอุปกรณ์ทางอิเล็กทรอนิกส์ ซึ่งสามารถนำมาใช้เป็นหลักฐานได้ ในทางการตรวจพิสูจน์พยานหลักฐานดิจิทัล หลักฐานที่ได้จะไม่มีการเปลี่ยนแปลง หรือถ้ามีความจำเป็นที่จะต้องมีการเปลี่ยนแปลงก็จะต้องมีการเปลี่ยนแปลงน้อยที่สุด โดยจะต้องมีการบันทึกกระบวนการได้มาของหลักฐานอย่างเที่ยงตรง

การตรวจพิสูจน์พยานหลักฐานดิจิทัล ไม่เพียงแต่เป็นการสืบสวนข้อมูลทางอิเล็กทรอนิกส์ แต่ยังเป็นการระบุข้อมูลที่เกี่ยวข้องกับการสืบสวนค้นหาหลักฐานเพื่อนำเสนอประกอบการดำเนินคดี ดังนั้น จึงมีความจำเป็นที่คนทั่วไปจะต้องทำความเข้าใจว่า ข้อมูลเหล่านี้ไม่ได้หมายถึงเฉพาะข้อมูลในคอมพิวเตอร์ แต่ยังรวมไปถึงอุปกรณ์ที่สามารถจัดเก็บข้อมูลทางอิเล็กทรอนิคส์ เช่น โทรศัพท์มือถือ กล้องถ่ายรูป อุปกรณ์รับสัญญาณดาวเทียม (GPS) อุปกรณ์จัดเก็บข้อมูล USB เครื่องเล่นเกม และแม้แต่อุปกรณ์อิเล็กทรอนิกส์ในชีวิตประจำวันทั่วไปอื่นๆ เมื่อพิจารณาการสื่อสารข้อมูลในปัจจุบันจะพบว่า เป็นการสื่อสารข้อมูลในรูปของข้อมูลอิเล็กทรอนิกส์ค่อนข้างมาก จึงเห็นได้ว่า ทำไมการตรวจพิสูจน์พยานหลักฐานดิจิทัล จึงเป็นเครื่องมือที่สำคัญในปัจจุบัน จากการสำรวจพบว่าอาชญากรรมคอมพิวเตอร์เป็นหนึ่งในอาชญกรรมทางเศรษฐกิจที่มีความสำคัญและมีการรายงานว่าสร้างความเสียหายที่มีมูลค่ามหาศาล โลกของเทคโนโลยีก้าวไปอย่างรวดเร็ว องค์กรต่างๆ ต้องพึ่งพาเทคโนโลยีและการแข่งขันทางด้านเทคโนโลยีที่สูงมากขึ้นตามไปด้วย เทคโนโลยีได้กลายมาเป็นส่วนหนึ่งในชีวิตของผู้คนในปัจจุบัน องค์กรในทุกอุตสาหกรรมทั้งในประเทศและต่างประเทศต่างก็มีนโยบายในการเข้าถึงข้อมูลที่เป็นความลับขององค์กรและข้อมูลของลูกค้า เพื่อที่จะปกป้องการขโมยข้อมูลออกจากองค์กร แต่การรั่วไหลของข้อมูลยังคงเป็นหนึ่งในปัญหาใหญ่ที่องค์กรต้องเผชิญในโลกเทคโนโลยีทุกวันนี้ การรักษาข้อมูลกลายเป็นปัญหาสำหรับองค์กรที่ไม่มีการวางแผนการจัดการกับอาชญากรรมคอมพิวเตอร์ ตัวอย่างของอาชญากรรมคอมพิวเตอร์ ได้แก่การฉ้อโกงผ่าน

ทางคอมพิวเตอร์ การฝ่าฝืนนโยบายความปลอดภัยข้อมูลคอมพิวเตอร์ขององค์กร การจารกรรมข้อมูล การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การละเมิดสิทธิส่วนบุคคล และการดาวน์โหลดข้อมูลที่ผิดกฎหมาย เป็นต้น

จากที่กล่าวมา จะเห็นได้ว่าการตรวจพิสูจน์พยานหลักฐานดิจิทัลในประเทศไทยถือเป็นเรื่องใหม่ ที่เข้ามามีบทบาท ผู้ที่เกี่ยวข้องยังมีประสบการณ์ไม่มาก จึงมีความจำเป็นที่หน่วยงานด้านกฎหมายทั้งภาครัฐและเอกชนต้องให้ความสนใจเรียนรู้และหาประสบการณ์เพิ่มเติม เพราะพยานหลักฐานดิจิทัลจะเป็นหลักฐานสำคัญที่ไม่อาจมองข้าม

คนจำนวนมากยังมีความเข้าใจผิดเกี่ยวกับการตรวจพิสูจน์พยานหลักฐานดิจิทัลว่าเกี่ยวข้องกับการสืบสวนคดีอาชญากรรมเท่านั้น หรือพยานหลักฐานดิจิทัลมีความยุ่งยากซับซ้อน โดยแท้จริงแล้วการตรวจพิสูจน์พยานหลักฐานดิจิทัลเกี่ยวข้องกับหลายส่วนไม่ว่าจะเป็นการสืบสวนคดีอาชญากรรม, การฟ้องร้องในคดีแพ่งหรือการฟ้องร้องเรื่องส่วนตัว ถ้าเกี่ยวข้องกับคอมพิวเตอร์, การสื่อสารผ่านอุปกรณ์อิเล็กทรอนิกส์หรือเอกสารอิเล็กทรอนิกส์แล้ว ก็มีความจำเป็นต้องใช้กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล เช่น การกู้ข้อมูลที่ถูกลบและไฟล์การใช้งานชั่วคราวที่เกิดขึ้นจากกระบวนการทำงานของคอมพิวเตอร์ ซึ่งข้อมูลที่พิสูจน์ได้นี้ ผู้ใช้งานจะไม่สามารถโต้แย้งได้เนื่องจากเป็นข้อมูลที่เกิดขึ้นจริง เช่น ข้อมูลการกระทำความผิดของพนักงาน

ปัจจุบันนักกฎหมายในประเทศไทยบางส่วนยังคิดว่าการใช้พยานหลักฐานดิจิทัลมีความยุ่งยากซับซ้อนและคิดว่าไม่ได้รับอนุญาตให้นำมาอ้างอิง ซึ่งเป็นความเข้าใจที่ไม่ตรงนัก เนื่องจากหลายกรณีมีความจำเป็นที่จะต้องใช้พยานหลักฐานดิจิทัล เช่น รูปภาพ, อีเมลล์, เอกสารอิเล็กทรอนิกส์ และประวัติการใช้งานอินเทอร์เน็ต ซึ่งหลักฐานเหล่านี้สามารถนำมาอธิบายในชั้นพิจารณาคดี ในรูปแบบที่คนทั่วไปเข้าใจได้ง่าย

การจัดการกับพยานหลักฐานดิจิทัลมีสองสิ่งทีสำคัญคือ ความสมบูรณ์ของพยานหลักฐานและความถูกต้องของหลักฐาน โดยเป็นไปตามพระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2554 ซึ่งถือเป็นจุดเริ่มต้นของงานด้านตรวจพิสูจน์พยานหลักฐานดิจิทัลในประเทศไทย

ในส่วนการรับฟังพยานหลักฐานดิจิทัลของศาลไทย จากเดิมที่การสื่อสารอาศัยเพียงภาษาและตัวหนังสือเป็นหลัก มาเป็นการสื่อสารด้วยภาษาอิเล็กทรอนิกส์ซึ่งมีประสิทธิภาพมากขึ้นในการประมวลผล ปัจจุบันจึงมีการกำหนดให้สื่ออิเล็กทรอนิกส์สามารถใช้เป็นพยานหลักฐานได้ในการพิจารณาคดีได้ นอกเหนือจากพยานวัตถุ พยานเอกสาร พยานบุคคล และพยานนิติวิทยาศาสตร์ เพื่อให้สามารถพิสูจน์ว่าจำเลยมีผิดหรือบริสุทธิ์ ในส่วนการจัดประเภทพยานหลักฐานนั้น ข้อมูลอิเล็กทรอนิกส์แม้จะมีลักษณะเป็นพยานเอกสารและพยานวัตถุ แต่ก็มีลักษณะพิเศษแตกต่างจากพยานเอกสารและพยานวัตถุทั่วไป ในการนำสืบจึงต้องมีวิธีการพิเศษ การยอมรับให้ข้อมูลอิเล็กทรอนิกส์เป็นพยานอีกประเภทหนึ่งจึงมีความเหมาะสมกว่า เมื่อจัดให้ข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานอีกประเภทหนึ่งแล้ว ข้อที่ต้องพิจารณาต่อมาก็คือ จะมีวิธีการนำสืบและหลักในการรับฟังอย่างไร และจะนำบทตัดพยาน ได้แก่ หลักการรับฟังพยานหลักฐานที่ดีที่สุด และหลักการรับฟังพยานบอกเล่า มาใช้ด้วยหรือไม่กรณีของวิธีการนำสืบนั้น รวมถึงควรกำหนดให้ผู้กล่าวอ้างต้องดำเนินการเหมือนกันกับพยานหลักฐานประเภทอื่น คือ ต้องยื่นบัญชีระบุพยานที่เกี่ยวข้อง มีลายเซ็นต์ผู้ที่เกี่ยวข้อง เช่น คนรับเครื่อง คนอนุญาต วันและเวลา มีการส่งสำเนาพยานหลักฐานที่จะอ้างอิงให้แก่คู่ความอีกฝ่าย

การรับฟังพยานหลักฐานอิเล็กทรอนิกส์มีหลักกฎหมายสำคัญ 3 ประการ ในการพิจารณาพยานหลักฐานอิเล็กทรอนิกส์นั้นว่าสามารถยืนยันความแท้จริง (Authentication) ได้อย่างเหมาะสมหรือไม่

<u>ความแท้จริงของพยานหลักฐานอิเล็กทรอนิกส์ประกอบด้วย</u>

1. เนื้อหานั้นไม่ได้ถูกเปลี่ยนแปลง
2. ข้อมูลนั้นเป็นไปตามเจตนาที่แท้จริงของผู้สร้างเอกสารนั้น ทั้งนี้ไม่ว่าผู้สร้างเอกสารจะเป็นมนุษย์ หรือคอมพิวเตอร์

3. ข้อมูลพิเศษ เช่น วันเดือนปี ที่ถูกสร้างนั้นถูกต้อง

ในปัจจุบันศาลไทยได้ให้การยอมรับและรับฟังพยานหลักฐานอิเล็กทรอนิกส์ เช่น ในคำพิพากษาศาลฎีกาที่ 7264/2542 ซึ่งวางหลักไว้ว่าพยานหลักฐานทางคอมพิวเตอร์สามารถรับฟังได้ ซึ่งอาจรับฟังได้ในฐานะที่เป็นพยานเอกสาร ในกรณีที่มีการพิมพ์แล้วนำผลลัพธ์ที่ได้มานำเสนอ ซึ่งในแนวทางการรับฟังพยานหลักฐานชนิดนี้ของศาลนั้น จะต้องปรากฏว่าระบบการบันทึก การสร้าง การเก็บรักษา การเรียกข้อมูล หรือการใช้งานของคอมพิวเตอร์นั้นเป็นปกติเช่นที่เคยทำมา ไม่มีสิ่งที่ผิดเพี้ยนหรือบิดเบือน ก็จะน่าเชื่อถือว่าเป็นข้อมูลที่ถูกต้องได้ ดังนั้น ปัญหาในการรับฟังพยานหลักฐานของศาล จึงมิใช่สิ่งที่เป็นอุปสรรคต่อการดำเนินคดีหรือการค้นหาความจริงทางคดี

การใช้พยานเอกสารที่เป็นข้อมูลทางอิเล็กทรอนิกส์นั้น สามารถอ้างอิงเป็นพยานหลักฐานต่อศาลได้ ศาลจะไม่ปฏิเสธการรับฟังข้อมูลนั้นเพราะเหตุว่าเป็นข้อมูลทางอิเล็กทรอนิกส์ แต่ข้อมูลดังกล่าวจะมีความน่าเชื่อถือรับฟังในเนื้อหาสาระได้หรือไม่นั้น เป็นดุลยพินิจของศาลซึ่งเป็นผู้รับฟังข้อมูลในการชั่งน้ำหนักพยานเอง โดยใช้หลักเกณฑ์ความน่าเชื่อถือตามที่กำหนดไว้ในมาตรา 10 วรรคสอง (พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544) เป็นเกณฑ์ในการพิจารณา จึงจำเป็นต้องมีการอบรมและให้ความรู้ทางด้านความปลอดภัยของข้อมูล การปรับเปลี่ยนทัศนคติ ค่านิยมเดิมๆ ความเคยชินในระบบพยานหลักฐานของไทย ตามบทบัญญัติของประมวลกฎหมายวิธีพิจารณาความแพ่ง ซึ่งนำไปใช้ในวิธีพิจารณาความอาญาด้วยนั้น จะเป็นระบบของพยานบุคคล พยานเอกสาร พยานวัตถุ และพยานผู้เชี่ยวชาญหรือผู้ชำนาญการพิเศษ ซึ่งมิได้ออกแบบไว้สำหรับพยานหลักฐานทางคอมพิวเตอร์หรืออิเล็กทรอนิกส์ จึงควรมีการปรับเปลี่ยนเนื่องจากเป็นเรื่องจำเป็นสำหรับพนักงานสอบสวนตลอดจนผู้ที่เกี่ยวข้องในกระบวนการยุติธรรมจนถึงขั้นศาล ที่จะรับมือกับอาชญากรรมคอมพิวเตอร์ที่นับวันจะเพิ่มมากขึ้น และรูปแบบคดีก็ทวีความซับซ้อนมากขึ้น ความรู้ ความเข้าใจด้านการตรวจพิสูจน์พยานหลักฐานดิจิทัล จะทำให้ผู้ที่เกี่ยวข้องในกระบวนการยุติธรรมสามารถนำกฎหมายมาบังคับใช้ได้อย่างมีประสิทธิภาพสูงสุด

หลักการพื้นฐานในการตรวจพิสูจน์พยานหลักฐานดิจิทัล

หลักการพื้นฐานในการตรวจพิสูจน์พยานหลักฐานดิจิทัล ประกอบไปด้วย

- <u>การรวบรวมพยานหลักฐานดิจิทัล (Acquisition)</u>
  สิ่งสำคัญที่สุดคือความสมบูรณ์ของพยานหลักฐาน และการรวบรวมพยานหลักฐานทั้งหมดให้เป็นไปอย่างสมบูรณ์ขณะเกิดเหตุโดยไม่ถูกเปลี่ยนแปลงแก้ไขใดๆ
- <u>การเก็บรักษาพยานหลักฐานดิจิทัล (Preservation)</u>
  การเก็บรักษาจะต้องเก็บรักษาไว้ในสภาพที่รับฟังได้ในชั้นศาล เป็นไปตามกระบวนการสร้างห่วงโซ่คุ้มครองพยานหลักฐาน (Chain of Custody) ในหลักสากล จะมีมาตรฐานการเก็บรักษาพยานหลักฐานดิจิทัลที่เป็นที่ยอมรับของทุกฝ่าย มีบันทึกขั้นตอนการคุ้มครองพยานหลักฐาน และวิธีการเก็บรักษา เพื่อให้มั่นใจได้ว่าเป็นข้อมูลที่ไม่ได้ถูกแก้ไขเปลี่ยนแปลงนับจากที่ได้รับมาจากที่เกิดเหตุ
- <u>การวิเคราะห์พยานหลักฐานดิจิทัล (Analysis)</u>
  พยานหลักฐานแต่ละประเภทของคดีจะมีความแตกต่างกัน วิธีวิเคราะห์จึงแตกต่างกัน มีการใช้เครื่องมือที่แตกต่างกัน ทักษะเจ้าหน้าที่แตกต่างกัน การฝึกอบรมเจ้าหน้าที่พิสูจน์หลักฐานจึงมีความสำคัญ การวิเคราะห์พยานหลักฐานดิจิทัล จึงต้องใช้ผู้เชี่ยวชาญด้านพยานหลักฐานดิจิทัลมาวิเคราะห์

- <u>การนำเสนอผลพิสูจน์พยานหลักฐานดิจิทัล (Presentation)</u> การนำเสนอผลการตรวจพิสูจน์พยานหลักฐานดิจิทัล เป็นรายงานบันทึกคำให้การผู้เชี่ยวชาญ อธิบายวิธีการตรวจสอบ เครื่องมือที่ใช้ตรวจสอบ ตรวจสอบสิ่งใด วิธีเก็บพยานหลักฐาน สิ่งที่ค้นพบ และวิธีการยืนยันความแท้จริงของพยานหลักฐานดิจิทัล

ข้อเสนอเชิงนโยบายในการพัฒนากระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล

การพัฒนากระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล แต่เดิมส่วนใหญ่เป็นงานด้านวิทยาศาสตร์และคอมพิวเตอร์ ยังไม่สามารถเชื่อมโยงกับการพิจารณาคดีตามกฎหมายได้มากนัก จะศึกษาเฉพาะด้านเทคนิคของพยานหลักฐานดิจิทัลเท่านั้น ในการเก็บรวบรวมและตรวจพิสูจน์พยานหลักฐานดิจิทัล ปัญหาที่พบไม่ใช่การใช้เทคโนโลยี หรือเครื่องมือ แต่อยู่ที่กระบวนการ หลายครั้งหลักฐานถูกเปลี่ยนแปลงก่อนที่จะถึงผู้ตรวจพิสูจน์ การสื่อสารให้เกิดความเข้าใจที่ตรงกันระหว่างผู้เก็บรวบรวมหลักฐาน คนทำคดีและผู้ตรวจพิสูจน์จึงมีความสำคัญ รวมทั้งการสร้างความรู้และความเข้าใจ เพื่อไม่ให้หลักฐานถูกเปลี่ยนแปลงโดยไม่ทราบหรือไม่ตั้งใจ ในกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล ควรจะมีการสร้างมาตรฐานโดยยึดหลักการรักษาสภาพหลักฐานและไม่เปลี่ยนแปลงหลักฐาน มีการกำหนดว่าอะไรคือพยานหลักฐานดิจิทัล แนวทางวิธีการเก็บหลักฐาน การขนส่ง การเขียนรายงาน และอื่นๆ ซึ่งหน่วยงานในกระบวนการยุติธรรมที่เกี่ยวข้องต้องมาพัฒนาร่วมกัน นอกเหนือไปจากมาตรฐานการจัดการอุปกรณ์ดิจิทัล ในการตรวจพิสูจน์พยานหลักฐานดิจัล ที่ศูนย์ดิจิทัลฟอเรนสิกส์ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ได้จัดทำขึ้น เพื่อให้เป็นที่ยอมรับของทุกฝ่ายและสามารถใช้งานได้จริงไม่ใช่เป็นเพียงหลักการหรือทฤษฎี การจัดการกับปัญหาอาชญากรรมจะเป็นไปอย่างมีประสิทธิภาพต้องมีการทำงานร่วมกันเป็นทีม มาตรฐานส่วนนี้เป็นเรื่องสำคัญ เพราะพยานหลักฐานดิจิทัลมีอยู่ทุกแห่ง การจะจัดการอย่างไรให้น่าเชื่อถือ รับฟังได้ในชั้นพิจารณาคดี จึงเป็นเรื่องที่ต้องให้ความสำคัญ

โดยในกระบวนการยุติธรรม การเก็บรวบรวมและพิสูจน์พยานหลักฐานมีอยู่ด้วยกัน 4 ขั้นตอน คือ

1. การรวบรวมพยานหลักฐาน ต้องทำอย่างถูกวิธีเพื่อไม่ให้มีการเปลี่ยนแปลงในพยานหลักฐานดิจิทัล
2. การเก็บรักษา สื่อดิจิทัลแต่ละประเภทมีวิธีในการเก็บรักษาที่แตกต่างกัน
3. การวิเคราะห์
4. การนำเสนอผลพิสูจน์ในชั้นศาล

ประเทศไทยยังไม่มีการกำหนดมาตรฐานในการเก็บรวบรวม และพิสูจน์พยานหลักฐานดิจิทัลที่ชัดเจนครบถ้วน ไม่มีเครื่องมือในการตรวจพิสูจน์เพียงพอครบทุกสื่อดิจิทัล และยังไม่มีการวางมาตรฐานกลาง ขณะที่ต่างประเทศมีหน่วยงานที่ทำหน้าที่กำหนดมาตรฐาน การเก็บรวบรวม และพิสูจน์พยานหลักฐานดิจิทัล รวมถึงผู้เชี่ยวชาญ

เจ้าหน้าที่ที่จะตรวจพิสูจน์พยานหลักฐานดิจิทัล จะต้องมีทักษะที่จำเป็น คือ

1. ทักษะในการเรียนรู้พัฒนาตนเอง เพื่อเรียนรู้เทคนิคใหม่ๆ ให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีและปริมาณข้อมูลที่มีจำนวนมากขึ้น
2. ทักษะด้านการสืบสวน ผู้เชี่ยวชาญต้องสามารถทำงานเป็นทีมได้ แต่ก็ต้องมีความเป็นอิสระ ผู้เชี่ยวชาญจะต้องสามารถตัดสินใจได้ว่า ข้อมูลใดที่เกี่ยวข้องกับการสืบสวนสอบสวน และเมื่อใดควรหยุดสืบค้นหาข้อมูลหลักฐานเนื่องจากพยานหลักฐานสำคัญมีเพียงพอ
3. ทักษะการสื่อสารที่ดี ผู้เชี่ยวชาญจำเป็นต้องมีทักษะในการสื่อสารที่จะนำหลักฐานที่อาจซับซ้อน มานำเสนอในรูปแบบที่เข้าใจได้ง่ายสำหรับบุคคลทั่วไป ทักษะส่วนนี้มีความสำคัญเป็นอย่างมาก บทบาท

ของผู้เชี่ยวชาญมักจะเกี่ยวข้องกับการนำเสนอหลักฐานในศาล และเป็นพยานผู้เชี่ยวชาญ ผู้เชี่ยวชาญต้องเตรียมตัวให้พร้อมและสามารถตอบคำถามได้อย่างชัดเจน ครบถ้วนขณะที่อยู่ภายใต้แรงกดดัน

4. ทักษะความรู้ความชำนาญด้านเทคนิค นิติวิทยาศาสตร์เป็นสาขาวิชาทางเทคนิค และผู้เชี่ยวชาญควรมีพื้นฐานด้านเทคนิคทั่วไป และทักษะในส่วนเทคนิคพิเศษทางคอมพิวเตอร์

บทสรุป

ในช่วงแรกประเทศไทยยังไม่มีกฎหมายเฉพาะเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ จึงเป็นที่มาของการออกพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ แต่อย่างไรก็ตาม จากความก้าวหน้าทางเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว ทำให้ประสบปัญหาทางด้านเทคนิค สำหรับการสืบสวน สอบสวน และตรวจพิสูจน์พยานหลักฐานดิจิทัล ซึ่งต้องอาศัยความรู้ความชำนาญและผู้เชี่ยวชาญเฉพาะด้าน รวมไปถึงปัญหาด้านการตีความกฎหมาย; ในปัจจุบันอาชญากรรมคอมพิวเตอร์มีแนวโน้มสูงขึ้นมาก การให้ความรู้เกี่ยวกับคอมพิวเตอร์และอินเทอร์เน็ต จะทำให้สามารถป้องกันตนเองจากอาชญากรรมคอมพิวเตอร์ได้ในเบื้องต้น ศาสตร์ด้านอาชญาวิทยาก็มีความสำคัญ เพื่อช่วยให้เข้าใจในมุมมองของผู้กระทำผิด ควบคู่ไปกับการใช้มาตรการทางกฎหมายที่มีอยู่ของรัฐ และการสร้างมาตรฐานของการตรวจพิสูจน์พยานหลักฐานดิจิทัลเพิ่มเติมเพื่อให้มีความถูกต้อง น่าเชื่อถือ ชัดเจน ครบถ้วน เป็นที่ยอมรับในชั้นศาล ตลอดจนการให้ความสำคัญกับการฝึกอบรมพัฒนาบุคลากรให้มีความรู้ หรือ ใช้ทีมผู้เชี่ยวชาญที่มีทักษะที่จำเป็นเฉพาะด้าน เป็นการบูรณาการร่วมกันของทุกฝ่าย ทั้งฝ่ายบังคับใช้กฎหมายและฝ่ายเทคนิค จะทำให้สามารถรับมือกับการเปลี่ยนแปลงทางเทคโนโลยี และการเพิ่มขึ้นของอาชญากรรมคอมพิวเตอร์ เพื่อนำไปสู่การสร้างความเป็นธรรมให้กับทุกฝ่ายในกระบวนการยุติธรรม

บรรณานุกรม

Adam, C. (2016). **Forensic Evidence in Court: Evaluation and Scientific Opinion.** John Wiley & Sons.

Beckett, J. (2010). **Forensic Computing: A Deterministic Model for Validation and Verification through an Ontological Examination of Forensic Functions and Processes (PhD, University of South Australia).** Retrieved from Personal communication from author, September 2011

Christensen, A. M., Crowder, C. M., Ousley, S. D., & Houck, M. M. (2014). **Error and its Meaning in Forensic Science.** Journal of Forensic Sciences, 59(1), 123–126. https://doi.org/10.1111/1556-4029.12275 de Waal et al., 2008, A. de Waal, J. Venter, E. Barnard. Applying topic modeling to forensic data IFIP International Conference on Digital Forensics, Springer (2008), pp. 115-126

Kohn, M., Eloff, J., & Olivier, M. (2006). **Framework for a digital forensic investigation.** Paper presented at the Information Security South Africa Conference 2006 from Insight to Foresight, Sandton, South Africa. Presented on 5-7 July.

Mann, P. (2004). **Cybersecurity: the CTOSE project.** Computer Law & Security Review, 20(2), 125-126.

Pollitt et al., 2008, **Mark Pollitt, Kara Nance, Brian Hay, Ronald C. Dodge, Phili p Craiger, Paul Burke, Chris Marberry, Bryan Brubaker.** Virtualization and digital forensics: a research and education agenda, J Digit Forensic Pract, 1556-7281, 2 (2) (2008), pp. 62-73

Richard and Roussev, (2006). **Golden G. Richard III, Vassil Roussev.** Next-generation digital forensics Commun ACM, 0001-0782, 49 (2) (2006), pp. 76-80

Saltzer and Frans Kaashoek, (2009). **Jerome H. Saltzer, M. Frans Kaashoek.** Principles of computer system design: an introduction, Morgan Kaufmann (2009)

Turnbull et al., (2009). **Benjamin Turnbull, Robert Taylor, Barry Blundell.** The anatomy of electronic evidence â quantitative analysis of police e-crime data, International conference on availability, reliability and security, (ARES '09) (March 16–19 2009), pp. 143-149