การตรวจพิสูจน์พยานหลักฐานดิจิทัลกับคดีเกี่ยวกับความมั่นคง
Digital forensics and Crimes Against National Security

วรินทรา ศรีวิชัย
คณะนิติศาสตร์ มหาวิทยาลัยเชียงใหม่ 239 ถนนห้วยแก้ว ตำบลสุเทพ อำเภอเมือง จังหวัดเชียงใหม่ 50200

Warintra Seevichai
Faculty of Law, Chiang Mai University, 239 Huay Kaew Road, Muang District, Chiang Mai, Thailand, 50200

E-mail : warintraseevichai@gmail.com
Received: October 11, 2019; Revised: May 1, 2020; Accepted: May 8, 2020

บทคัดย่อ

บทความชิ้นนี้มีจุดประสงค์เพื่อศึกษาสภาพปัญหาและข้อจำกัดของการตรวจพิสูจน์พยานหลักฐานดิจิทัลในกระบวนการยุติธรรมทางอาญาในคดีความผิดเกี่ยวกับความมั่นคง และอธิบายเกี่ยวกับลักษณะเฉพาะของพยานหลักฐานดิจิทัล ตลอดจนแนวทางการรับฟังพยานหลักฐานดิจิทัลในคดีอาญา โดยใช้วิธีการศึกษาจากเอกสาร ตำรา งานวิจัยและการลงพื้นที่สัมภาษณ์เชิงลึกจากนักวิชาการ ผู้ที่มีส่วนเกี่ยวข้องกับการตรวจพิสูจน์พยานหลักฐานดิจิทัล จากการศึกษาพบว่า ปัจจุบันมีการจัดทำมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐานดิจิทัล โดยศูนย์ดิจิทัลฟอเรนสิกส์ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ทำให้กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลมีมาตรฐานการปฏิบัติการที่ชัดเจน แต่อำนาจหน้าที่ในการปฏิบัติการตรวจพยานหลักฐานดิจิทัลรวมศูนย์อยู่ที่หน่วยงานภาครัฐ

ในคดีอาญาที่เกี่ยวข้องกับพยานหลักฐานดิจิทัล โดยเฉพาะในคดีความมั่นคงที่รัฐเป็นผู้ฟ้องคดี พบว่ามีประเด็นความไม่เป็นธรรมเกิดขึ้นกับผู้ถูกกล่าวหา เช่น ข้อจำกัดในการเข้าถึงและการรวบรวมพยานหลักฐานดิจิทัล และประเด็นสิทธิของผู้ถูกกล่าวหาในคดีความมั่นคง ตลอดจนการรับฟังและการชั่งน้ำหนักพยานหลักฐานดิจิทัลของศาล เป็นต้น

ข้อเสนอแนะจากการศึกษาในครั้งนี้ กล่าวคือ ในทุกขั้นตอนของกระบวนการยุติธรรมทางอาญาในการจัดการพยานหลักฐานดิจิทัล โดยเฉพาะอย่างยิ่งในขั้นตอนการสืบสวน สอบสวน การรวบรวมพยานหลักฐานดิจิทัล ตลอดจนการรับฟังพยานหลักฐานดิจิทัล ควรมีแนวทาง มาตรฐานการปฏิบัติที่ชัดเจนและสอดคล้องกับมาตรฐานสากล ตลอดจนการเปิดโอกาสให้หน่วยงานอื่นที่มีศักยภาพและมาตรฐานเข้ามาร่วมทำงานในการตรวจพิสูจน์พยานหลักฐานดิจิทัล อีกทั้งควรมีกฎหมายหรือหลักประกันที่เป็นมาตรฐานในการตรวจพิสูจน์พยานหลักฐาน ซึ่งนำไปสู่การสร้างความเป็นธรรมให้กับทุกฝ่ายในกระบวนการยุติธรรมทางอาญา

คำสำคัญ: พยานหลักฐานดิจิทัล, การรวบรวมพยานหลักฐานดิจิทัล, กระบวนการยุติธรรมทางอาญา, ความผิดเกี่ยวกับความมั่นคง

Abstract

This article aims to study problems and limitations of digital forensics in criminal procedure of crimes against national security and elucidates the special characteristics of digital evidence as well as rules regarding the admissibility of evidence in a criminal trial 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. 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 power to acquire digital evidence remains centred in government agencies.

In criminal cases, that relate to digital evidence, especially, crimes against national security, which state is the plaintiff, demonstrate injustice performed on defendants, for example, the limitation to access and gather digital evidence and rights of defendants in crimes against national security, including the hearing and the preponderance of digital evidence. This research suggests that in every step of criminal procedure for digital forensic management, particularly, investigation process,

the 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 forensics, Acquisition of digital forensics, Criminal Procedure, Crimes against National Security.

1. บทนำ

ปัจจุบันประเทศไทยมีการใช้งานอินเทอร์เน็ตต่อวันสูงมากเป็นอันดับ 3 ของโลก โดยมีการใช้งานอินเทอร์เน็ตมากกว่า 9 ชั่วโมงต่อวัน[1] และข้อมูลสถิติจากกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) ยังพบว่าอาชญากรรมทางเทคโนโลยีมีแนวโน้มที่จะเพิ่มสูงขึ้น เห็นได้จากจำนวนคดีความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีในปี 2561 มีจำนวน 2,718 คดี และจำนวนคดีที่เพิ่มขึ้นในปี 2562 (ม.ค. – ส.ค. 62) มี 2,870 คดี[2] การกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีในแต่ละคดีนั้น มีทั้งคดีอาชญากรรมคอมพิวเตอร์ คดีอาชญากรรมอินเทอร์เน็ต และคดีอาชญากรรมทั่วไป ซึ่งมีความเกี่ยวพันกับอุปกรณ์หรือเครื่องมืออิเล็กทรอนิกส์[3] นอกจากนั้นคดีอาชญากรรมทางเทคโนโลยียังแบ่งลักษณะคดีออกเป็น คดีที่รู้ตัวผู้กระทำความผิดชัดเจน คดีที่ปรากฏพยานหลักฐานที่สามารถนำไปสู่ตัวผู้กระทำความผิดได้ และคดีที่ไม่รู้ตัวผู้กระทำความผิดเลย[4]

---

[1] We are social, “Digital 2019”, We are social, accessed April 12 2020 https://wearesocial.com/global-digital-report-2019.

[2] ไอซีที, “8 เดือนคดีไซเบอร์แซงปี61 ปอท. เฟ้นหาไวต์แฮกเกอร์,” ประชาชาติธุรกิจ, 13 กันยายน 2562. สืบค้นเมื่อวันที่ 12 เมษายน 2563, https://www.prachachat.net/ict/news-370708.

[3] ประชาไท, “หลักฐานดิจิทัล#1: ความเข้าใจพื้นฐาน ผู้ใช้อินเทอร์เน็ตต้องรู้!,” ประชาไท, สืบค้นเมื่อวันที่ 12 เมษายน 2563 https://prachatai.com/journal/2015/10/61879.

[4] ประชาไท, “การรวบรวมพยานหลักฐานในคดีอาชญากรรมคอมพิวเตอร์,” ประชาไท, สืบค้นเมื่อวันที่ 12 เมษายน 2563 https://prachatai.com/journal/2019/12/85402#_ftn14.

ในคดีที่มีการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี พยานหลักฐานบนโลกออนไลน์ และพยานหลักฐานหลายๆ ชิ้นที่เกี่ยวข้องกับการกระทำความผิด จะอยู่ในลักษณะของพยานหลักฐานดิจิทัล ซึ่งการรวบรวม จัดเก็บหรือการตรวจพิสูจน์พยานหลักฐานจะต้องดำเนินการโดยผู้ที่มีความรู้ความเชี่ยวชาญโดยเฉพาะ และพยานหลักฐานดิจิทัลมีความสำคัญอย่างมากในกระบวนการพิจารณาคดีความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี โดยเฉพาะคดีความผิดเกี่ยวกับความมั่นคง ซึ่งเห็นได้จากการเก็บข้อมูลคดีความมั่นคงที่เกิดขึ้นบนโลกออนไลน์ของศูนย์ข้อมูลกฎหมายและคดีเสรีภาพโดยโครงการอินเทอร์เน็ตเพื่อกฎหมายประชาชน (iLaw) พบว่าตั้งแต่ปี 2557 เป็นต้นมา มีผู้ถูกกล่าวหาและถูกดำเนินคดี ตามมาตรา 112 และ มาตรา 116 ประมวลกฎหมายอาญา จำนวน 216 คดี[5] ด้วยลักษณะความผิดที่หลากหลาย เช่น การโพสต์ข้อความบนเฟซบุ๊ก การส่งต่อหรือแชร์เนื้อหาในโลกออนไลน์ เป็นต้น

ดังนั้น การรวบรวมพยานหลักฐานดิจิทัล กรณีความผิดเกี่ยวกับความมั่นคงจะมีหน่วยงานที่มีอำนาจหน้าที่เฉพาะเข้ามาทำหน้าที่เก็บรวบรวมพยานหลักฐาน ได้แก่ กรมสอบสวนคดีพิเศษ (DSI) กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และสถาบันนิติวิทยาศาสตร์ ซึ่งเป็นเจ้าหน้าที่ที่มีความรู้ความเชี่ยวชาญทางด้านคอมพิวเตอร์และเทคโนโลยีเป็นอย่างมาก และยังเป็นเจ้าหน้าที่ที่ได้รับการแต่งตั้งตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (แก้ไขเพิ่มเติม) 2560 อีกด้วย ทำให้มีอำนาจในการติดตามและรวบรวมพยานหลักฐานดิจิทัล เพราะกระบวนการตรวจพิสูจน์พยานหลักฐานทางดิจิทัลสามารถนำไปใช้เป็นพยานหลักฐานในชั้นกระบวนพิจารณาของศาล ทำให้การรวบรวมพยานหลักฐานจึงต้องมีการปฏิบัติตามขั้นตอน และต้องคุ้มครองพยานหลักฐานไว้อย่างดีที่สุด (Chain of custody) เพื่อป้องกันการปนเปื้อนของพยานหลักฐานนั้นๆ แต่อย่างไรก็ตามการตรวจพิสูจน์พยานหลักฐานดิจิทัลในปัจจุบันทำให้เกิดปัญหาตามมาหลายประการ เช่น การเข้าถึงพยานหลักฐานดิจิทัลที่ส่งผลให้ผู้ถูกกล่าวหามีภาระในการพิสูจน์เพิ่มมากขึ้น และการดำเนินกระบวนการยุติธรรมทางอาญาโดยการตรวจพิสูจน์พยานหลักฐานดิจิทัลของภาครัฐยังไม่สอดคล้องกับมาตรฐานสากล ตลอดจนยังไม่มีหลักประกันที่เพียงพอในการคุ้มครองและให้ความเป็นธรรมแก่ผู้ถูกกล่าวหาในคดีความผิดเกี่ยวกับความมั่นคง

[5] ไอลอว์, “สถิติศูนย์ข้อมูลกฎหมายและคดีเสรีภาพ,” ไอลอว์, สืบค้นเมื่อวันที่ 12 เมษายน 2563 https://freedom.ilaw.or.th/case?page=7&Offense=9%2B10&d_ from=&d_to=&k=&p=.

2. พยานหลักฐานดิจิทัล หลักการในการตรวจพิสูจน์และการชั่งน้ำหนักพยานหลักฐานดิจิทัลในกระบวนการยุติธรรมทางอาญา

2.1. ความหมายของคำว่า “พยานหลักฐานดิจิทัล”

การนิยามความหมายของคำว่า “พยานหลักฐานดิจิทัล” ไม่ปรากฏในพจนานุกรมฉบับราชบัณฑิตยสถาน แต่ปรากฏเพียงคำว่า “ดิจิทัล” หมายถึง เชิงเลข[6]

การนิยามความหมายในทางกฎหมาย ในข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐานดิจิทัลของศูนย์ดิจิทัลฟอเรนสิกส์ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ได้ให้ความหมายของคำว่า “พยานหลักฐานดิจิทัล” หมายถึง ข้อมูลที่ได้เก็บรักษาบนสื่อบันทึกข้อมูลหรืออยู่ระหว่างการส่งรับด้วยวิธีการทางอิเล็กทรอนิกส์ ซึ่งสามารถถูกใช้อ้างอิงเป็นพยานหลักฐาน[7] กล่าวโดยสรุป พยานหลักฐานดิจิทัลเป็นข้อมูลที่อยู่ในอุปกรณ์คอมพิวเตอร์และอิเล็กทรอนิกส์ เช่น ไฟล์ที่อยู่ในคอมพิวเตอร์, อุปกรณ์อิเล็กทรอนิกส์, โทรศัพท์มือถือ รวมถึงหลักฐานที่ถูกสร้างจากระบบคอมพิวเตอร์ ซึ่งข้อมูลเหล่านี้สามารถนำไปใช้อ้างอิงเป็นพยานหลักฐานในการพิจารณาคดีของศาลได้

2.2. ประเภทของพยานหลักฐานดิจิทัล

พยานหลักฐานดิจิทัล แบ่งออกเป็น 3 ประเภท[8] ดังนี้

1. พยานหลักฐานที่มนุษย์สร้างขึ้น (Human Generated) คือ เนื้อหาหรือข้อมูลที่มนุษย์จัดทำขึ้นหรือพิมพ์เข้าไปในระบบคอมพิวเตอร์ เช่น บทสนทนา (chat) และ เสียงอิเล็กทรอนิกส์ (voicemail) เป็นต้น

2. พยานหลักฐานที่คอมพิวเตอร์สร้างขึ้น (Computer Generated Evidence) คือ เมื่อมนุษย์สร้างเนื้อหาหรือข้อมูลขึ้นมา คอมพิวเตอร์จะทำการบันทึกและสร้างข้อมูลขึ้นมาหนึ่งชุด เช่น ข้อมูลจากโปรแกรมคอมพิวเตอร์ ได้แก่ แฟ้มประวัติอินเทอร์เน็ต (Internet history files)

---

[6] สำนักงานราชบัณฑิตยสภา, “ศัพท์บัญญัติสำนักงานราชบัณฑิตยสภา,” สำนักงานราชบัณฑิตยสภา, สืบค้นเมื่อวันที่ 12 เมษายน 2563 http://www.royin.go.th/coined_word/.

[7] ศูนย์ดิจิทัลฟอเรนสิกส์, ข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐานดิจิทัล, (กรุงเทพฯ: สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2559),: 1.

[8] สำนักการต่างประเทศ, “รายงานของคณะข้าราชการตุลาการหลักสูตร กฎหมายอาชญากรรมคอมพิวเตอร์และกฎหมายเกี่ยวกับพยานหลักฐานดิจิตอล,” สำนักการต่างประเทศ, สืบค้นเมื่อวันที่ 12 เมษายน 2563 https://oia.coj.go.th/th/content/ category/detail/id/8/cid/9041/iid/154331.

แฟ้มอินเทอร์เน็ตชั่วคราว (Cache file) และข้อมูลการใช้บริการ ได้แก่ แฟ้มบันทึกการเข้าออกและตารางแสดงสถานะ (Log file) เป็นต้น

3. พยานหลักฐานที่มนุษย์และคอมพิวเตอร์ร่วมกันสร้างขึ้น (Hybrid computer and human generated Evidence) หรือเรียกว่า “Metadata” ซึ่งพยานหลักฐานประเภทนี้จะมีโปรแกรมที่ถูกเขียนขึ้นมา มีความสามารถคิด วิเคราะห์ วางแผน และตัดสินใจได้ หรือที่เรียกว่า “AI” (artificial intelligence) เช่น การปักหมุดสถานที่ออนไลน์ (check in) หรือ จดหมายอิเล็กทรอนิกส์ (e-mail) เป็นต้น

2.3. หลักการพื้นฐานของการตรวจพิสูจน์พยานหลักฐานดิจิทัล

จุดเริ่มต้นมาจากการตรวจพิสูจน์พยานหลักฐานคอมพิวเตอร์ในกลางปี ค.ศ. 1980 ด้วยโครงการสื่อบันทึกแม่เหล็ก (Magnetic Media Program) ที่ก่อตั้งโดยสำนักงานสืบสวนกลางของสหรัฐอเมริกา (Federal Bureau of Investigation) หรือ FBI[9] ซึ่งได้มีการพัฒนามาตรฐานการตรวจพิสูจน์พยานหลักฐานดิจิทัลตลอดมา จนกระทั่งได้รับการรับรองให้ใช้ในหน่วยงานอื่นๆ ทั่วทั้งสหรัฐอเมริกาและต่างประเทศทั่วโลก ซึ่งปัจจุบันประเทศไทยไม่ได้บัญญัติกฎหมายที่กำหนดมาตรฐานในการตรวจพิสูจน์พยานหลักฐานไว้โดยเฉพาะ ปรากฏเพียง “ข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐานดิจิทัล” เพื่อเป็นแนวทางในการปฏิบัติงานของเจ้าหน้าที่ และมีการฝึกอบรมเจ้าหน้าที่ที่เกี่ยวข้อง ณ ต่างประเทศ เพื่อศึกษามาตรฐานดังกล่าวและนำมาปรับใช้ในการตรวจพิสูจน์พยานหลักฐานดิจิทัลเท่านั้น

ในการตรวจพิสูจน์พยานหลักฐานดิจิทัล มีปัจจัยสำคัญหลายอย่างที่ควรต้องคำนึงและคอยระมัดระวังเพื่อไม่ให้เกิดความผิดพลาด โดยเฉพาะอย่างยิ่งการเลือกเครื่องมือที่เหมาะสมกับงาน การทำความเข้าใจถึงวิธีการใช้เครื่องมือที่ถูกต้อง รวมถึงการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐาน ซึ่งมีแนวทางมาตรฐานสากลที่เป็นแนวปฏิบัติในการตรวจพิสูจน์พยานหลักฐาน เช่น ACPO Good Practice Guide for Digital Evidence (Edition: March 2012); ISO/IEC 27037 Information technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence, First edition

[9] แลร์รี อี แดนเนียล และลาร์ส อี แดนเนียล, การตรวจพิสูจน์พยานหลักฐานดิจิทัลสำหรับผู้ประกอบวิชาชีพกฎหมาย, แปลโดยสุนีย์ สกาวรัตน์, (กรุงเทพฯ: มูลนิธิเพื่ออินเทอร์เน็ตและวัฒนธรรมพลเมือง, 2559), 72-73.

2012-10-15 และ SWGDE Best Practices for Computer Forensics V3-1[10] ทั้งนี้ยังรวมถึงมาตรฐานการจัดการอุปกรณ์ดิจิทัลในการตรวจพิสูจน์พยานหลักฐานในการปฏิบัติงาน ทั้งในสถานที่เกิดเหตุและในห้องปฏิบัติการ ตลอดจนการจัดการข้อมูลคอมพิวเตอร์ สื่อบันทึกข้อมูลดิจิทัลแบบภายใน สื่อบันทึกข้อมูลดิจิทัล และเครื่องมือสื่อสารเคลื่อนที่อีกด้วย

หลักการปฏิบัติงานเกี่ยวกับพยานหลักฐานดิจิทัลที่สอดคล้องกับหลักการมาตรฐานสากลมีหลักการที่สำคัญดังต่อไปนี้[11]

(1) ควรดำเนินการโดยผู้ที่เคยผ่านการฝึกอบรมทางเทคนิคด้านการตรวจพิสูจน์พยานหลักฐานดิจิทัล

(2) ควรรักษาสภาพพยานหลักฐานไม่ให้ถูกเปลี่ยนแปลง หรือถูกเปลี่ยนแปลงน้อยที่สุด โดยผู้ปฏิบัติงานต้องสามารถอธิบายและบันทึกเป็นลายลักษณ์อักษรแสดงขั้นตอนการคุ้มครองพยานหลักฐานไว้โดยละเอียด

(3) การคุ้มครองพยานหลักฐาน (Chain of Custody) ต้องบันทึกข้อมูลในแบบฟอร์มมีรายละเอียด ได้แก่ ข้อมูลติดต่อและลายมือชื่อของผู้ส่งมอบพยานหลักฐาน, ข้อมูลติดต่อ และลายมือชื่อของผู้รับมอบพยานหลักฐาน, วันที่และเวลาในการรับ-ส่งมอบพยานหลักฐาน, เหตุผลในการรับ-ส่งมอบพยานหลักฐาน, วิธีการส่งมอบพยานหลักฐาน เช่น ส่งมอบโดยเจ้าหน้าที่ที่เกี่ยวข้องหรือส่งมอบโดยพนักงานส่งของ และสถานที่จัดเก็บพยานหลักฐาน เป็นต้น

(4) มีการบันทึกขั้นตอนการปฏิบัติงาน การเก็บรวบรวมและการวิเคราะห์พยานหลักฐานโดยละเอียด เพื่อให้ผู้ตรวจพิสูจน์รายอื่นที่มีความเชี่ยวชาญในสาขาเดียวกันสามารถเข้าใจได้ และหากทำซ้ำด้วยวิธีการเดิม และเครื่องมือที่มีลักษณะเดียวกันจะต้องได้ผลลัพธ์เหมือนกัน

(5) บุคคลที่เข้าถึงพยานหลักฐานต้องเป็นผู้ที่ได้รับมอบหมายหรือมีหน้าที่รับผิดชอบโดยตรง

(6) ผู้ปฏิบัติงานพึงตระหนักถึงหน้าที่และความรับผิดชอบในการปฏิบัติงาน รวมถึงการดำเนินการตามกฎหมายเกี่ยวกับพยานหลักฐาน

(7) เครื่องมือและอุปกรณ์ที่มีมาตรฐานตามหลักการตรวจพิสูจน์พยานหลักฐาน เช่น มี

---

[10] ศูนย์ดิจิทัลฟอเรนสิกส์, ข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐานดิจิทัล(กรุงเทพฯ: สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2559), 1.

[11] เรื่องเดียวกัน, 2-3.

สภาพพร้อมใช้งานและเหมาะสมกับกระบวนการตรวจพิสูจน์พยานหลักฐานแต่ละประเภท มีมาตรการในการป้องกันการเปลี่ยนแปลงและปนเปื้อนของพยานหลักฐาน และได้รับการตรวจสอบความถูกต้องแม่นยำ (Validation) ของเครื่องมือก่อนใช้งานอย่างสม่ำเสมอ รวมทั้งมีคู่มือการใช้งานหรือเอกสารคำอธิบายเพื่อใช้ประกอบการอ้างอิง

หลักการในการตรวจพิสูจน์พยานหลักฐานดิจิทัล[12] หรือ ห่วงโซ่การคุ้มครองพยานหลักฐาน (Chain of custody) ได้แก่

(1) การระบุรูปพรรณ (Identification) คือขั้นตอนแรกที่จะต้องระบุประเภทและตำแหน่งที่ตั้งของพยานหลักฐานดิจิทัลเพื่อใช้ในการขอหมายเรียกหรือหมายค้น โดยถ้อยคำที่ใช้ระบุรูปพรรณนั้นจะต้องมีความเฉพาะเจาะจงและใช้ศัพท์ที่ถูกต้อง

(2) การเก็บรวบรวม (Collection) หรือเรียกว่ากระบวนการสร้างห่วงโซ่การคุ้มครองพยานหลักฐาน (Chain of Custody) ถือเป็นขั้นตอนที่มีความสำคัญอย่างมาก เนื่องจากเป็นการสัมผัสพยานหลักฐานเป็นครั้งแรก หากไม่ทำตามขั้นตอนหรือวิธีการที่เหมาะสมอาจส่งผลทำให้พยานหลักฐานนั้นถูกทำลายหรือเปลี่ยนแปลงได้ ในการเก็บรวบรวมนั้นจะต้องมีการถ่ายภาพพยานหลักฐานในสถานที่เกิดเหตุก่อนการรวบรวมพยานหลักฐาน จากนั้นจดบันทึกรายละเอียด เช่นหมายเลขเครื่อง ชื่อยี่ห้อ ชื่อรุ่นและรายละเอียดอื่น ๆ

(3) การบรรจุและการเคลื่อนย้าย (Transport) ควรจัดเก็บพยานหลักฐานทุกชั้นลงในบรรจุภัณฑ์ ใช้เทปปิดผนึกพยานหลักฐานให้เรียบร้อย และติดป้ายหมายเลขกำกับพยานหลักฐานทุกชิ้นลงบนบรรจุภัณฑ์ เพื่อป้องกันมิให้พยานหลักฐานนั้นถูกเปลี่ยนแปลงหรือเกิดความเสียหายในระหว่างการขนส่ง

(4) การทำสำเนาข้อมูล (Acquisition) การทำให้พยานหลักฐานต้นฉบับได้รับการป้องกันจากการเปลี่ยนแปลงต้องกระทำโดยผู้ที่ผ่านการฝึกอบรมมาแล้วเท่านั้น เนื่องจากเป็นขั้นตอนที่อาจเกิดความผิดพลาดได้โดยง่าย โดยจะต้องใช้อุปกรณ์ป้องกันการเขียนทับข้อมูล (write-blocking) บนอุปกรณ์จัดเก็บข้อมูลต้นฉบับ กระบวนการเรียงลำดับวิธีการทำงานโดยใชหลักทางคณิตศาสตร์ (algorithm) ที่คำนวณตัวเลขจากเนื้อหาของพยานหลักฐาน แสดงให้เห็นถึงฮาร์ด

[12] เรื่องเดียวกัน, 68-100.

ไดรฟ์และกระบวนการตั้งค่าแฮชของไฟล์ที่ใช้ในการคำนวณค่าการตรวจสอบแฮช หรือที่เรียกว่าการสร้าง “ค่าแฮช” (hash Value)[13]

(5) การตรวจสอบ (Verification) การที่พยานหลักฐานจะเป็นที่ยอมรับในชั้นศาลนั้นจะต้องมีวิธีการตรวจสอบว่าพยานหลักฐานที่นำเสนอตรงกับต้นฉบับที่เก็บรวบรวมมาหรือไม่ เพื่อตรวจสอบต้นฉบับและสำเนาในระหว่างขั้นตอนการทำสำเนาข้อมูล หากค่าแฮชไม่ตรงกันก็สามารถโต้แย้งถึงความถูกต้องแท้จริงของพยานหลักฐานในชั้นศาลได้

(6) การวิเคราะห์ (Analysis) ผู้ปฏิบัติงานต้องผ่านการฝึกอบรมและมีความเชี่ยวชาญในขอบข่ายที่ตรวจพิสูจน์ โดยห้ามวิเคราะห์พยานหลักฐานต้นฉบับโดยตรง ให้ทำการวิเคราะห์จากสำเนาพยานหลักฐานที่ได้กระทำไว้แล้วข้างต้นเท่านั้น

(7) การรายงานผลการตรวจพิสูจน์พยานหลักฐาน (Presentation) คือการนำเสนอผลการตรวจพิสูจน์เป็นลายลักษณ์อักษรหรือรายงานการตรวจพิสูจน์พยานหลักฐาน และจัดทำบันทึกคำให้การของผู้เชี่ยวชาญสำหรับใช้ในชั้นศาล เช่น เครื่องมือที่ใช้ในการตรวจสอบ วิธีการที่ใช้ในการยืนยันความถูกต้องของข้อมูล กระบวนการและอุปกรณ์ที่ใช้ในการกู้คืนข้อมูลและการทำสำเนาข้อมูล และรายงานแสดงผลการตรวจสอบ เป็นต้น

หลักการตรวจพิสูจน์พยานหลักฐานดิจิทัลที่กล่าวมาข้างต้น มีความสำคัญอย่างมาก เพราะหลักฐานทางดิจิทัลนั้นมีความอ่อนไหว การปฏิบัติตามขั้นตอนที่ถูกต้องถือเป็นสิ่งสำคัญในการพิสูจน์ความถูกต้องแท้จริงของพยานหลักฐานดิจิทัล (Authentication)

อย่างไรก็ตาม ในการตรวจพิสูจน์พยานหลักฐานดิจิทัลยังมีข้อจำกัดบางประการ กล่าวคือ การตรวจพิสูจน์พยานหลักฐานดิจิทัลต้องกระทำโดย “ผู้เชี่ยวชาญด้านการตรวจพิสูจน์พยานหลักฐานดิจิทัล” เท่านั้น เนื่องจากการจัดการกับพยานหลักฐานดังกล่าวจะต้องอาศัยความรู้ความเชี่ยวชาญ และระยะเวลาในการจัดการกับข้อมูลที่ได้จากคอมพิวเตอร์หรือโทรศัพท์มือถือ โดยการทำงานที่เกี่ยวข้องกับการรวบรวมและการวิเคราะห์พยานหลักฐานดิจิทัลนั้น ผู้เชี่ยวชาญต้องคำนึงถึงห่วงโซ่ของการคุ้มครองพยานหลักฐาน (Chain of custody) เป็นสำคัญ[14]

---

[13] ค่าแฮช (hash Value) หมายถึง ค่าเฉพาะที่ได้จากการคำนวณเนื้อหาของข้อมูลด้วยฟังก์ชันทางคณิตศาสตร์ เป็นเสมือนลายนิ้วมือของข้อมูล ช่วยให้ไฟล์หรือฮาร์ดไดรฟ์นั้นถูกระบุโดยลักษณะเฉพาะตามที่ปรากฏอยู่ในเวลาที่ถูกสร้าง ใช้ยืนยันความถูกต้องครบถ้วนของข้อมูล โดยค่านี้มักเป็นเลขฐาน 16 มีความยาวแน่นอนขึ้นอยู่กับฟังก์ชันที่ใช้ ได้แก่ Message Digest 5 (MD5) และ Secure Hash Algorithm 1 (SHA1).

[14] ประชาไท, “หลักฐานดิจิทัล#1: ความเข้าใจพื้นฐาน ผู้ใช้อินเทอร์เน็ตต้องรู้!”, ประชาไท, สืบค้นเมื่อวันที่ 20

2.4. หลักการชั่งน้ำหนัก/การรับฟังพยานหลักฐานดิจิทัล

หลักการชั่งน้ำหนักพยานหลักฐานทั่วไป

การชั่งน้ำหนักพยานหลักฐาน หมายถึง การที่ศาลนำพยานหลักฐานทุกประเภทที่คู่ความนำสืบและเห็นว่าสามารถรับฟังเป็นพยานหลักฐานได้ในชั้นศาล จึงเป็นการวินิจฉัยปัญหาข้อเท็จจริงในประเด็นที่พิพาทกันให้เป็นที่ยุติโดยอาศัยพยานหลักฐาน[15]

ในคดีอาญาหลักการชั่งน้ำหนักพยานหลักฐาน อำนาจในการวินิจฉัยน้ำหนักของพยานหลักฐาน ให้ศาลใช้ดุลยพินิจชั่งน้ำหนักพยานหลักฐานทั้งปวง และจะไม่พิพากษาลงโทษจำเลยจนกว่าจะแน่ใจว่า มีการกระทำความผิดจริงและจำเลยเป็นผู้กระทำความผิดนั้น โจทก์จะต้องพิสูจน์ให้ศาลเห็นได้โดยปราศจากเหตุอันควรสงสัยว่าจำเลยเป็นผู้กระทำความผิด ถ้ามีเหตุอันควรสงสัยอย่างใดอย่างหนึ่งว่าจำเลยไม่ใช่คนร้ายที่กระทำความผิด ให้ยกประโยชน์แห่งความสงสัยนั้นให้แก่จำเลย[16] เห็นได้จากการวินิจฉัยชี้ขาดข้อเท็จจริงแห่งคดีของศาลฎีกา โดยศาลจะต้องใช้ดุลพินิจชั่งน้ำหนักพยานหลักฐานทั้งปวงในสำนวนว่าควรรับฟังได้เพียงไรหรือไม่นั้น มิใช่ว่าพยานเบิกความอย่างไรแล้ว ศาลจะต้องรับฟังข้อเท็จจริงตามคำเบิกความของพยานเสมอไป และไม่มีกฎหมายบทใดบัญญัติห้ามมิให้ศาลรับฟังคำให้การชั้นสอบสวนของพยานเป็นข้อประกอบการพิจารณาของศาล ส่วนจะรับฟังได้เพียงใดหรือไม่นั้น แล้วแต่เหตุผลของแต่ละเรื่องไป[17]

หลักการชั่งน้ำหนักพยานหลักฐานดิจิทัล

การรับฟังพยานหลักฐานดิจิทัลในคดีอาญา มีหลักเกณฑ์ 3 ประการที่ศาลใช้ในการพิจารณาพยานหลักฐานดิจิทัลที่สามารถยืนยันความถูกต้องแท้จริง (Authentication) ได้อย่างเหมาะสมหรือไม่ และความสำคัญการพิสูจน์พยานหลักฐานดิจิทัลที่ช่วยในการพิจารณาคดี และการรับฟัง ซึ่งพยานหลักฐานดิจิทัลที่ศาลจะรับฟังและพิจารณาประกอบด้วย[18]

เมษายน 2563 https://prachatai.com/journal/2015/10/61879.

[15] พรเพชร วิชิตชลลัย, คำอธิบายกฎหมายลักษณะพยาน, พิมพ์ครั้งที่ 4, (กรุงเทพฯ: สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา, 2555),: 385.

[16] พระราชบัญญัติให้ใช้ประมวลกฎหมายวิธีพิจารณาความอาญา 2477, มาตรา 227, ราชกิจจานุเบกษา ฉบับกฤษฎีกา เล่มที่ 52 (10 มิถุนายน 2478): 76.

[17] คำพิพากษาศาลฎีกาที่ 1123 (ศาลฎีกา 2526).

[18] เจษฎา คำรินทร์, “ปัญหาทางกฎหมายเกี่ยวกับการรับฟังพยานหลักฐานทางอิเล็กทรอนิกส์ในคดีอาญา,”

1. เนื้อหาของเอกสารไม่ได้ถูกเปลี่ยนแปลง

2. ข้อมูลในเอกสารเป็นไปตามเจตนาที่แท้จริงของผู้สร้างเอกสารนั้น ทั้งนี้ไม่ว่าผู้สร้างเอกสารจะเป็นมนุษย์ หรือคอมพิวเตอร์

3. ข้อมูลพิเศษในเอกสาร อันได้แก่ วันเดือนปีที่ถูกสร้าง นั้นถูกต้อง

หลักในการพิจารณาว่าพยานหลักฐานดิจิทัลมีความน่าเชื่อถือ สามารถรับฟังในชั้นศาลได้หรือไม่นั้น เป็นดุลยพินิจของศาลซึ่งเป็นผู้รับฟังข้อมูลในการชั่งน้ำหนักพยานหลักฐาน โดยพิจารณาถึงความน่าเชื่อถือตามที่กำหนดไว้ในพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาตรา 11 วรรคสอง แก้ไขเพิ่มเติมโดย พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ.2551 มาตรา 6[19] ซึ่งให้พิจารณาความน่าเชื่อถือจากลักษณะหรือวิธีการที่ใช้สร้าง เก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์ ลักษณะหรือวิธีการเก็บรักษา ความครบถ้วน และไม่มีการเปลี่ยนแปลงของข้อความ ลักษณะ หรือวิธีการที่ใช้ในการระบุหรือแสดงตัวผู้ส่งข้อมูล รวมทั้งพฤติการณ์ที่เกี่ยวข้องทั้งหมด

อย่างไรก็ตาม การชั่งน้ำหนัก/การรับฟังพยานหลักฐานดิจิทัลยังมีข้อจำกัด เนื่องจากพยานหลักฐานดิจิทัลโดยสภาพง่ายต่อการถูกแก้ไขเปลี่ยนแปลง ส่วนใหญ่เป็นพยานหลักฐานที่เกิดขึ้นจากการกระทำของมนุษย์และเป็นการกระทำของฝ่ายใดฝ่ายหนึ่ง ซึ่งเป็นการแก้ไขเปลี่ยนแปลงหรือสร้างพยานหลักฐานดิจิทัลเท็จขึ้นมา ทำให้พยานผู้เชี่ยวชาญด้านการตรวจพิสูจน์พยานหลักฐานดิจิทัลจึงมีความสำคัญในการอธิบายให้ศาลเข้าใจลักษณะเฉพาะและวิธีการเข้าถึง การรวบรวมพยานหลักฐานดิจิทัลว่าถูกต้องตามหลักการตรวจพิสูจน์พยานหลักฐานดิจิทัลหรือไม่ ประกอบกับผู้พิพากษาก็ต้องมีความรู้พื้นฐานในการตรวจพิสูจน์พยานหลักฐานดิจิทัล พิจารณาถึงลักษณะการสืบสวนหาความเชื่อมโยงของข้อมูล การตรวจยึด การเก็บรักษา การตรวจสอบ และการนำเสนอพยานหลักฐานประกอบกับพยานแวดล้อมอื่นๆ ในคดีด้วย อีกทั้งกฎหมายเกี่ยวกับพยานหลักฐานดิจิทัลควรต้องมีบทบัญญัติไว้โดยเฉพาะ ซึ่งกำหนดวิธีการกระบวนการ การตรวจพยานหลักฐานดิจิทัลและหลักการชั่งน้ำหนัก/รับฟังพยานหลักฐานดิจิทัล เนื่องจากโดยสภาพของพยานหลักฐานดิจิทัลแตกต่างจากพยานหลักฐานทั่วไป

วารสารมหาจุฬานาครทรรศ์ 6, ฉ.9 (2562): 4549-4550.

[19] พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ 2544, มาตรา 11 วรรคสอง, ราชกิจจานุเบกษา ฉบับกฤษฎีกา เล่มที่ 118 ตอนที่ 112 ก (4 ธันวาคม 2544): 6.

3. พยานหลักฐานดิจิทัลกับคดีความมั่นคง

การตรวจพิสูจน์พยานหลักฐานดิจิทัลในความผิดเกี่ยวกับความมั่นคง หากมีกระบวนการเก็บรวบรวมพยานหลักฐานที่ไม่เป็นไปตามรูปแบบมาตรฐานสากล อาจจะส่งผลให้พยานหลักฐานดิจิทัลได้รับความเสียหาย สูญหาย หรือถูกปนเปื้อน รวมถึงการถูกแก้ไขเปลี่ยนแปลง และถ้ากระบวนการการตรวจพิสูจน์พยานหลักฐานดิจิทัลที่ไม่เป็นไปตามมาตรฐานสากลถูกทำซ้ำๆ และเกิดขึ้นเรื่อยๆ ก็อาจจะทำให้การตรวจพิสูจน์พยานหลักฐานดิจิทัลกลายเป็นการเก็บรวบรวมพยานหลักฐานตามหลักข้อยกเว้นที่ไม่เป็นไปตามรูปแบบหรือมาตรฐานสากลได้[20] และข้อจำกัดการตรวจพิสูจน์พยานหลักฐานดิจิทัลในคดีความมั่นคงอีกประการหนึ่งคือ ข้อจำกัดในบทบัญญัติทางกฎหมายในการรวบรวมพยานหลักฐานจากผู้ให้บริการอินเทอร์เน็ตในคดีอาญาที่เกี่ยวข้องกับพยานหลักฐานดิจิทัล ตามที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (แก้ไขเพิ่มเติม) พ.ศ. 2560 ที่กำหนดให้ผู้ให้บริการอินเทอร์เน็ต (Internet Service Providers : ISP) เก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้ 90 วัน นับตั้งแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์[21] ตามหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ[22] โดยผู้ให้บริการอินเทอร์เน็ตต้องทำการเก็บ log file หรือข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) เอาไว้ ซึ่งข้อจำกัดดังกล่าวจะส่งผลกระทบโดยตรงกับฝ่ายที่ถูกกล่าวหาและไม่ใช่เจ้าหน้าที่รัฐที่มีอำนาจหน้าที่เกี่ยวกับพยานหลักฐานดิจิทัล ซึ่งผู้พิพากษาหัวหน้าศาลอาญาให้ความเห็นเกี่ยวกับข้อจำกัดเรื่องระยะเวลาการเก็บข้อมูลของผู้ให้บริการว่า

> *“ประกาศ กสทช. เรื่องการเก็บข้อมูลการสัญจรทางคอมพิวเตอร์ของผู้ให้บริการ ซึ่งกำหนดให้ผู้ให้บริการเก็บข้อมูลไว้ 90 วัน แล้วจึงจะสามารถทำลายได้นั้น ส่งผลคือ ถ้าฝ่ายผู้ต้องหาหรือจำเลยจะเป็นฝ่ายใช้ข้อมูลนี้จะขอข้อมูลไม่ทัน เพราะจำเลยที่ถูกจับกุมและฝากขัง จะมีโอกาสที่จะพบทนายที่ศาลแต่งตั้งให้ครั้ง*

---

[20] ปิยบุตร แสงกนกกุล, “สภาวะยกเว้นในความคิดของ Giorgio Agamben,” วารสารฟ้าเดียวกัน 8, ฉ.1 (2553): 84-91.

[21] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ 2550, มาตรา 26, ราชกิจจานุเบกษา ฉบับกฤษฎีกา เล่มที่ 124 ตอนที่ 27 ก (18 มิถุนายน 2550): 11-12.

[22] ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ 2550, ข้อ 8, ราชกิจจานุเบกษา ฉบับกฤษฎีกา เล่มที่ 124 ตอนพิเศษ 102 ง (23 สิงหาคม 2550): 7-8.

แรกหลังจากครบฝากขังไปแล้ว กรณีนี้คือจำเลยไม่มีฐานะพอจะจ้างทนายเองและมีระยะเวลาเพียงพอที่จะข้อมูลจากผู้ให้บริการ"[23]

กรณีตัวอย่าง การใช้พยานหลักฐานดิจิทัลกับคดีเกี่ยวกับความมั่นคง

จากฐานข้อมูลคดีของศูนย์ข้อมูลกฎหมายและคดีเสรีภาพ ตั้งแต่ปี 2557 เป็นต้นมา พบว่ามีผู้ถูกกล่าวหาและถูกดำเนินคดีตามมาตรา 112 และ มาตรา 116 ประมวลกฎหมายอาญา จำนวน 216 คดี[24] ซึ่งคดีความผิดเกี่ยวกับความมั่นคงมักจะนำพยานหลักฐานดิจิทัลมาเป็นหลักฐานสำคัญประกอบการพิจารณาของศาล ดังนั้น ผู้เขียนจึงนำคดีเกี่ยวกับความมั่นคงที่อยู่ในความสนใจของสังคมและประชาชนทั่วไปจำนวน 2 คดี คือ คดีอำพล (คดีอากง SMS) และ คดีสุรภักดิ์ (คดีเฟซบุ๊ก: เราจะครองฯ) กรณีสองคดีดังกล่าวจะกรณีตัวอย่างของการใช้พยานหลักฐานดิจิทัลในคดีเกี่ยวกับความมั่นคง และข้อจำกัดในการใช้พยานหลักฐานดิจิทัล

(1) คดีอำพล (คดีอากง SMS) ถือเป็นคดีแรกๆ และเป็นคดีที่มีประชาชนให้ความสนใจอย่างมาก ในช่วงปี 2553-2554 อำพลถูกกล่าวหาว่าใช้โทรศัพท์มือถือส่งข้อความ (SMS – Short Messages) ที่เป็นการดูหมิ่นสถาบันพระมหากษัตริย์และให้ร้ายสมเด็จพระบรมราชินีนาถ ไปยังโทรศัพท์ของสมเกียรติ ครองวัฒนสุข เลขานุการของอดีตนายกอภิสิทธิ์ เวชชาชีวะ จำนวน 4 ข้อความ[25] ซึ่งในคดีนี้มีการนำพยานหลักฐานดิจิทัล ได้แก่ เครื่องคอมพิวเตอร์โน้ตบุ๊ค โทรศัพท์เคลื่อนที่จำนวน 3 เครื่อง พร้อมซิมการ์ดและระบบอุปกรณ์สายเสียงมาเป็นพยานหลักฐานประกอบการพิจารณาคดีของศาล ทำให้ประเด็นสำคัญในคดีนี้คือ การพิสูจน์ตัวตนจากพยานหลักฐานดิจิทัลที่ฝ่ายโจทก์กล่าวอ้างในการนำสืบพยานว่า "หมายเลขโทรศัพท์ที่ใช้ส่งข้อความ" จากผู้รับข้อความ ปรากฏในเอกสารข้อมูลการใช้โทรศัพท์ (CDR -Call Detail Record) จากผู้ให้บริการว่าเป็นหมายเลขโทรศัพท์ที่ใช้และส่งข้อความอย่างต่อเนื่อง แต่มีการหยุดใช้งานโดย

[23] สัมภาษณ์ผู้พิพากษาหัวหน้าศาลประจำสำนักงานอธิบดีผู้พิพากษาภาค 5 , สัมภาษณ์โดย วรินทรา ศรีวิชัย, สำนักงานศาลยุติธรรม ศาลอาญา, 16 มกราคม 2562.

[24] ไอลอว์, "สถิติศูนย์ข้อมูลกฎหมายและคดีเสรีภาพ," ไอลอว์, สืบค้นเมื่อวันที่ 12 เมษายน 2563 https://freedom.ilaw.or.th/case?page=7&Offense=9%2B10&d_ from=&d_to=&k=&p=.

[25] ไอลอว์, "ฐานข้อมูลคดีอำพล : อากงเอสเอ็มเอส," ไอลอว์, สืบค้นเมื่อวันที่ 12 เมษายน 2562 https://freedom.ilaw.or.th/th/case/21.

การถอดซิมการ์ด อีกทั้งยังพบว่าหมายเลขประจำเครื่องโทรศัพท์ (IMEI)[26] ถูกใช้งานกับหมายเลขโทรศัพท์อื่นในเครือข่ายทรูมูฟ (TURE) ที่ถูกลงทะเบียนโดยลูกเขยของอำพล

ทางฝ่ายของอำพลได้โต้แย้งด้วยพยานหลักฐานดิจิทัลเช่นกันว่า อำพลได้ใช้โทรศัพท์เคลื่อนที่ดังกล่าวติดต่อลูกสาวและหมายเลขโทรศัพท์ทั้ง 2 หมายเลขนั้น มีการใช้งานในพื้นที่ใกล้เคียงกัน ซึ่งตรงกับเอกสารข้อมูลจาก Cell Site และเลข CI 23672 ที่ระบุตำแหน่งพื้นที่คือ พื้นที่ซอยวัดด่านสำโรง อีกทั้งทนายฝ่ายอำพลยังมีประเด็นข้อต่อสู้ในเรื่องหมายเลขประจำเครื่องโทรศัพท์ (IMEI) จะต้องมีจำนวณ 15 หลักจึงจะสามารถระบุได้ว่าเป็นโทรศัพท์เคลื่อนที่เครื่องใด และการแก้ไข เปลี่ยนแปลงหมายเลขประจำเครื่องโทรศัพท์ (IMEI) สามารถทำได้โดยง่าย และประเด็นข้อต่อสู้อีกประการหนึ่งคือ เรื่องข้อจำกัดของการเข้าถึงข้อมูลหลักฐานดิจิทัลภายใต้ระยะเวลากฎหมายกำหนดให้ให้ผู้ให้บริการต้องเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้ 90 วัน นับตั้งแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ตามหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ[27] แต่ทางฝ่ายทนายของอำพลไม่สามารถเข้าถึงข้อมูลหลักฐานการใช้โทรศัพท์ของอำพลได้เนื่องจากเกินระยะเวลาที่กฎหมายกำหนดให้ผู้ให้บริการต้องเก็บรักษาข้อมูลไว้ ซึ่งทนายของอำพลได้ตั้งข้อสังเกตว่า

> *“ข้อสังเกตในคดีนี้ไม่พบบันทึกถึงวิธีการตรวจพิสูจน์พยานหลักฐานดิจิทัลโทรศัพท์เคลื่อนที่โดยเจ้าพนักงานในคดี ว่าได้มาตรฐานตามหลักนิติวิทยาศาสตร์ที่เกี่ยวกับคอมพิวเตอร์ (Computer Forensic) หรือไม่ อีกทั้งคดีนี้ทนายจำเลยไม่ได้รับการติดต่อตั้งแต่จำเลยถูกควบคุมตัว ดังนั้น หลังจากที่ทนายจำเลยเข้าให้การช่วยเหลือแก่จำเลยระยะเวลาดังกล่าวก็ได้ล่วงเลยกว่า 90 วันแล้ว ซึ่งพอเกิน 90 วันแล้ว ก็ทำลายทิ้ง เราจึงไม่สามารถขอข้อมูลจากผู้ให้บริการโทรศัพท์เคลื่อนที่ได้ แล้วทางบริษัทมีสำเนาเอกสารการใช้ข้อมูลโทรศัพท์อยู่ชุด*

---

[26] หมายเลขประจำเครื่องโทรศัพท์ IMEI: International Mobile Equipment ID คือ เลขหมายเฉพาะของโทรศัพท์เคลื่อนที่แต่ละครั้ง จำนวน 15 หลัก โดยจะไม่มีการซ้ำกัน โดยหกหลักแรก หมายถึงรหัสประเทศ สองหลักถัดมาหมายถึงบริษัทผู้ผลิตโทรศัพท์ หกหลักถัดไป หมายถึงลำดับของเครื่องยี่ห้อนั้น และเลขหมาย หลักที่สิบห้า เป็นค่าฟรี คือไม่มีความหมาย ดังนั้นหมายเลขประจำเครื่องโทรศัพท์ (IMEI) 14 หลักแรกเท่านั้นที่ใช้เป็นมาตรฐานในการระบุเอกลักษณ์โทรศัพท์เคลื่อนที่นั้น

[27] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) 2560, มาตรา 17, ราชกิจจานุเบกษา ฉบับกฤษฎีกา เล่มที่ 134 ตอนที่ 10 ก (24 มกราคม 2560): 33.

> *เดียวซึ่งได้ให้เจ้าพนักงานตำรวจไปแล้ว พยานหลักฐานชุดเดียวที่เรามีก็คือพยานหลักฐานจากทางโจทก์ ในวันนัดตรวจพยานหลักฐาน และคดีนี้ไม่มีพยานผู้เชี่ยวชาญคนใดมาเบิกความต่อศาล เพื่อหักล้างพยานหลักฐานที่โจทก์กล่าวอ้าง เนื่องจากเป็นคดีอ่อนไหว และทำให้เกิดความหวาดกลัวในการออกมาเคลื่อนไหวทางคดี"*[28]

ในการชั่งน้ำหนักและรับฟังพยานหลักฐานของศาล ศาลอาญาได้พิจารณาคดีและพิพากษาให้อำพลถูกลงโทษจำคุกเป็นเวลา 20 ปี โดยให้เหตุผลในคำพิพากษาว่า

> *"แม้โจทก์จะไม่สามารถนำสืบพยานให้เห็นได้อย่างชัดแจ้งว่าจำเลยเป็นผู้ส่งข้อความตามฟ้อง ก็เพราะเป็นการยากที่โจทก์จะสามารถนำสืบได้ด้วยประจักษ์พยาน เนื่องจากจำเลยซึ่งเป็นผู้กระทำความผิดย่อมต้องปกปิดการกระทำของตน มิให้บุคคลอื่นได้ล่วงรู้ จึงจำเป็นต้องอาศัยเหตุผล ประจักษ์พยานแวดล้อม ที่โจทก์นำสืบ ได้แก่ ข้อมูลการใช้โทรศัพท์ที่ระบุตำแหน่งว่าข้อความถูกส่งมาจากเสาสัญญาณใกล้บ้านจำเลย รวมทั้งหมายเลขอีมี่ที่ตรงกับโทรศัพท์เครื่องที่จำเลยยอมรับว่าเป็นผู้ใช้งาน ศาลเห็นว่าพยานแวดล้อมมีน้ำหนักพอรับฟังได้ว่าจำเลยกระทำความผิดจริง"*[29]

คดีของอำพลทำให้เห็นถึงความสำคัญและข้อจำกัดของการเก็บรวบรวมพยานหลักฐานดิจิทัล และมาตรฐานการตรวจพิสูจน์พยานหลักฐานดิจิทัล รวมถึงข้อจำกัดด้านกฎหมายที่กำหนดระยะเวลาเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการเกี่ยวกับคอมพิวเตอร์/การสื่อสารไว้เพียง 90 วันเท่านั้น ทำให้การเข้าถึงข้อมูลที่จะนำมาเป็นพยานหลักฐานในคดีถูกจำกัดลง ซึ่งอาจจะทำให้เกิดความไม่เป็นธรรมต่อฝ่ายที่ถูกกล่าวหาได้

(2) คดีของสุรภักดิ์ (คดีเฟซบุ๊ก: เราจะครองฯ) อดีตโปรแกรมเมอร์ถูกกล่าวหาว่าน่าจะเป็นเจ้าของอีเมล dorkao@hotmail.com และใช้อีเมลดังกล่าวสร้างบัญชีผู้ใช้ในเฟซบุ๊กชื่อว่า "เราจะครองแผ่นดินฯ..." ขึ้นใช้งานและเผยแพร่ข้อความเข้าข่ายหมิ่นประมาท ดูหมิ่น หรือแสดงความอาฆาตมาดร้ายพระมหากษัตริย์ฯ จำนวน 5 ข้อความในบัญชีผู้ใช้เฟซบุ๊ก "เราจะครอง

---

[28] สัมภาษณ์ทนายความอาสาและทนายความเครือข่ายของศูนย์ทนายความเพื่อสิทธิมนุษยชน, สัมภาษณ์โดย วริน ทรา ศรีวิชัย, ศูนย์ทนายความเพื่อสิทธิมนุษยชน, 17 มกราคม 2562.

[29] นายอำพล กับ พนักงานอัยการ สำนักงานอัยการสูงสุด, คำพิพากษาศาลอาญาที่ 4726 (ศาลอาญา 2554).

แผ่นดินฯ...” ทางอินเทอร์เน็ต[30] ซึ่งในคดีนี้มีการนำพยานหลักฐานดิจิทัล ได้แก่ เครื่องคอมพิวเตอร์โน้ตบุ๊ก คอมพิวเตอร์ตั้งโต๊ะ แอร์การ์ด ซิมการ์ดทรูมูฟ ซิมวันทูคอล ซีดี โมเด็มเราเตอร์ และแผงวงจรไฟฟ้ามาเป็นพยานหลักฐานประกอบการพิจารณาคดีของศาล ในคดีนี้ฝ่ายโจทก์ได้ให้พยานผู้เชี่ยวชาญจากหน่วยงานของรัฐมาเบิกความให้ความเห็นประกอบเอกสารภาพถ่ายหน้าจอข้อความที่พิมพ์ในเฟซบุ๊กจำนวน 5 ข้อความ และเอกสารจากบริษัทไมโครซอฟต์ซึ่งอ้างว่าแสดงให้เห็นความเชื่อมโยงระหว่างเลขหมายประจำเครื่องคอมพิวเตอร์ (IP Address) ของสุรภักดิ์กับบัญชีผู้ใช้อีเมล dorkao@hotmail.com รวมทั้งบันทึกวันเวลาการลงทะเบียนใช้งานอีเมลนั้น (Log file) เอกสารรายงานการตรวจพิสูจน์คอมพิวเตอร์ และเอกสารที่อ้างว่าแสดงข้อมูลการใช้งานอีเมลและเพจเฟซบุ๊กที่บันทึกอยู่ในแฟ้มเก็บบันทึกชั่วคราว (Temporary Internet File) ในเครื่องคอมพิวเตอร์ของสุรภักดิ์

คดีนี้มีประเด็นพิพาทที่สำคัญคือ 1) คอมพิวเตอร์ของกลางมีการใช้งานระบบอินเทอร์เน็ตหรือไม่ 2) คอมพิวเตอร์มีการใช้อีเมล dorkao@hotmail.com หรือไม่ 3) สามารถระบุความเป็นเจ้าของบัญชีเฟซบุ๊ก ชื่อว่า “เราจะครองแผ่นดินฯ...” ได้หรือไม่ และ 4) คอมพิวเตอร์ดังกล่าว มีประวัติการเข้าใช้บัญชีเฟซบุ๊ก ดังกล่าวหรือไม่ และสามารถตรวจสอบหาข้อความที่หมิ่นสถาบันฯ หลายรายการ ตามวันเวลาที่พนักงานสอบสวนระบุได้หรือไม่

อย่างไรก็ตาม ฝ่ายสุรภักดิ์ไม่ได้ต่อสู้ในประเด็นที่เป็นเนื้อหาของข้อความที่ปรากฏบนเฟซบุ๊ก เพราะเห็นว่าเป็นข้อความที่เข้าข่ายความผิดตามมาตรา 112 จริง แต่สุรภักดิ์ได้ต่อสู้ว่าไม่ใช่เจ้าของหรือผู้ใช้อีเมลและเฟซบุ๊กตามข้อกล่าวหาของโจทก์ จึงทำให้มีประเด็นที่ต้องพิสูจน์คือความเชื่อมโยงระหว่างข้อความหมิ่นฯกับเครื่องคอมพิวเตอร์ของสุรศักดิ์ ผลปรากฏว่า หน่วยงานที่พิสูจน์พยานหลักฐานได้ระบุว่า ไม่พบถ้อยคำหมิ่นประมาทพระมหากษัตริย์ฯ ตามฟ้องจากการตรวจพิสูจน์เครื่องคอมพิวเตอร์ของกลางแต่อย่างใด แม้ว่าข้อความที่โพสไปแล้วนั้นจะถูกส่งไปที่เซิร์ฟเวอร์ของเฟซบุ๊ก อาจทำให้ไม่หลงเหลือข้อความที่อยู่ในคอมพิวเตอร์ก็ตาม และนอกจากนี้เอกสารที่เจ้าพนักงานได้ข้อมูลจากเอกสารบันทึกประวัติการใช้อีเมล dorkao@hotmail.com จากบริษัทไมโครซอฟต์นั้น ปรากฏว่าได้มีการล็อคอินเข้าใช้งานอีเมลดังกล่าวอยู่หลายครั้ง ซึ่งเป็นเวลาวันที่สุรศักดิ์ถูกจับและควบคุมตัวแล้ว โดยสุรศักดิ์ไม่ได้รับอนุญาตให้ใช้อุปกรณ์สื่อสารใดๆ

[30] ไอลอว์, “ฐานข้อมูลคดีสุรภักดิ์,” ไอลอว์, สืบค้นเมื่อวันที่ 12 เมษายน 2563 https://freedom.ilaw.or.th/th/case/176.

แสดงให้เห็นว่าสุรศักดิ์ไม่ได้เป็นผู้ใช้งานอีเมลในช่วงเวลานั้น ส่งผลทำให้เกิดความสงสัยว่าใครเป็นเจ้าของหรือผู้ใช้อีเมลดังกล่าวและถึงแม้ว่าจำเลยเป็นเจ้าของหรือผู้ใช้ก็ตาม แต่เมื่อมีบุคคลอื่นใช้อีเมลนี้ก็ย่อมมีข้อสงสัยว่าสุรศักดิ์เป็นผู้กระทำความผิดจริงหรือไม่

ในคดีนี้ยังพบว่า วิธีการตรวจพิสูจน์พยานหลักฐานดิจิทัลโดยเจ้าพนักงานในคดี ไม่ได้มาตรฐานการตรวจพิสูจน์พยานหลักฐานดิจิทัล (Digital Forensic) ทำให้พยานหลักฐานขาดความน่าเชื่อถือ ตามเอกสารประกอบรายงานการตรวจพิสูจน์ที่แสดงประวัติการใช้อุปกรณ์เพื่อเชื่อมต่อระบบเครือข่ายที่โจทก์ใช้อ้างว่า มีข้อมูลต่างๆ ที่พิสูจน์ความผิดของจำเลยได้บันทึกอยู่ในเครื่องคอมพิวเตอร์ของกลาง มีวันเวลาการบันทึกปรากฏอยู่ด้วย และวันเวลาเหล่านั้นได้แสดงให้เห็นว่าเครื่องคอมพิวเตอร์ของกลางซึ่งเป็นของสุรศักดิ์ถูกเปิดใช้งานอีกหลายครั้งหลักจากที่จำเลยถูกจับและควบคุมตัว เรื่องนี้สอดคล้องกับล็อกไฟล์ (Log file) ที่แสดงถึงการใช้งานอีเมล จึงแสดงให้เห็นว่า พนักงานสอบสวนพิสูจน์พยานหลักฐานดิจิทัลโดยใช้วิธีเปิดเครื่องคอมพิวเตอร์ของจำเลยโดยตรง ไม่ใช่สำเนาคอมพิวเตอร์ ซึ่งวิธีการดังกล่าวไม่ชอบด้วยหลักการการตรวจพิสูจน์พยานหลักฐานดิจิทัลที่โดยปกติแล้ว เมื่อยึดเครื่องคอมพิวเตอร์ของกลาง เจ้าพนักงานต้องเก็บรักษาเครื่องจริงให้อยู่ในสภาพเดิม และทำสำเนาเครื่องอย่างน้อยหนึ่งชุด รวมทั้งสร้างค่าแฮช (Hash) เพื่อตรวจสอบต้นฉบับและสำเนา ซึ่งเป็นการย่อยข้อมูลให้เป็นตัวเลขหรือตัวอักษรสั้นๆ ซึ่งแม้ข้อมูลจะถูกเปลี่ยนแปลงไปเพียงนิดเดียว แต่ค่าแฮชนั้นจะเปลี่ยนไปชนิดที่ไม่มีความคล้ายกับของเดิมเลย เราจึงใช้ค่าแฮชเพื่อบ่งบอกความแตกต่างของข้อมูลที่เปลี่ยนแปลงไปได้ เพราะการเปิดเครื่องคอมพิวเตอร์ของกลางโดยตรงอาจส่งผลกระทบต่อข้อมูลที่บันทึกอยู่ภายในเครื่อง และคดีนี้ศาลก็ไม่สามารถตรวจสอบหรือเปรียบเทียบภายหลังได้ว่า ข้อมูลหรือพยานหลักฐานที่โจทก์กล่าวอ้างว่าอยู่ในเครื่องของกลางถูกสร้างขึ้นภายหลังหรือว่ามีอยู่ในเครื่องคอมพิวเตอร์มาก่อน เนื่องจากเจ้าพนักงานไม่ได้เก็บรักษาเครื่องจริง และไม่ได้สร้างค่าแฮชเปรียบเทียบ อีกทั้งยังไม่ปรากฏข้อเท็จจริงใดๆ ว่าเจ้าพนักงานใช้มาตรการที่เหมาะสม เพื่อรักษาความปลอดภัยและความถูกต้องของข้อมูลในเครื่องคอมพิวเตอร์ของกลาง ซึ่งลักษณะและวิธีการตรวจพิสูจน์เช่นนี้ ย่อมส่งผลกระทบหรือลดทอนความน่าเชื่อถือของพยานหลักฐานดิจิทัลของฝ่ายโจทก์ลง[31]

การนำเสนอพยานหลักฐานดิจิทัลในคดีนี้ ยังมีข้อมูลที่ไม่สอดคล้องกับความเป็นจริงในทางเทคนิคคอมพิวเตอร์ เห็นได้จากข้อมูลประวัติการเข้าใช้งานอีเมล dorkao@hotmail.com

[31] นลินี ฐิตะวรรณ, โลกใหม่ ใครกำกับ?, (กรุงเทพฯ: มูลนิธิเพื่ออินเทอร์เน็ตและวัฒนธรรมพลเมือง ,2557),: 66.

ที่มีบันทึกอยู่ในแฟ้มเก็บบันทึกชั่วคราวในเครื่องคอมพิวเตอร์ของสุรศักดิ์จำนวนหนึ่งไฟล์เท่านั้น คือไฟล์ที่แสดงข้อมูลการใช้งานอีเมลตามฟ้อง ซึ่งพยานผู้เชี่ยวชาญของสุรศักดิ์ให้ความเห็นว่า

“โดยปกติแล้ว หากเว็บไซต์ที่เรียกใช้งานไม่มีนโยบายห้ามแคช เครื่องคอมพิวเตอร์ก็จะแคชเว็บไซต์เหล่านั้นทั้งหมดเก็บไว้โดยอัตโนมัติ จึงเป็นไปไม่ได้ที่เครื่องคอมพิวเตอร์เครื่องหนึ่งจะเก็บบันทึกไฟล์การใช้เว็บไซต์ใดเว็บไซต์หนึ่งไว้เพียงแค่ไฟล์เดียวตามที่โจทก์กล่าวอ้าง แทบเป็นไปไม่ได้เลยที่การกู้ข้อมูลที่ถูกลบทิ้งแล้ว ผู้กู้จะพบไฟล์เพียงไฟล์เดียวเท่านั้นในแฟ้มเก็บบันทึกชั่วคราวที่เก็บบันทึกการใช้งานอินเทอร์เน็ต เนื่องจากหลักการทำงานของแฟ้มเก็บบันทึกชั่วคราวหรือการแคช (Cache) คือการเก็บบันทึกข้อมูลการใช้งานเว็บไซต์ต่างๆ ไว้ในเครื่องคอมพิวเตอร์ของผู้ใช้ชั่วคราว เพื่อรอเวลานำกลับมาแสดงผลใหม่ได้อย่างรวดเร็วเมื่อผู้ใช้เรียกเว็บไซต์นั้นดูอีกครั้ง และการที่ไฟล์ข้อมูลถูกลบภายในเวลาสามวินาทีเท่านั้น ซึ่งหลักการทำงานและวัตถุประสงค์ของการแคชเว็บไซต์เพื่อเรียกกลับมาแสดงผลใหม่ได้ในเวลาอันรวดเร็ว ย่อมเป็นไปไม่ได้เลยที่เครื่องคอมพิวเตอร์จะบันทึกและลบไฟล์ดังกล่าวทิ้งเองภายในสามวินาที ดังนั้น ไฟล์ที่โจทก์อ้างว่าพบในเครื่องคอมพิวเตอร์ของจำเลยอาจถูกสร้างขึ้นใหม่ เพื่อมุ่งจะดำเนินคดีกับจำเลย”[32]

นอกจากนั้น พยานผู้เชี่ยวชาญของสุรภักดิ์ ได้แสดงให้ศาลเห็นว่า เฟซบุ๊กไม่สามารถเกิดแคชไฟล์ได้ เพราะ นโยบายของเฟซบุ๊กต้องการปกป้องความเป็นส่วนตัวของผู้ใช้ และ ในทางเทคนิคเซิร์ฟเวอร์ของเฟซบุ๊กจะใช้การติดต่อแบบเอชทีทีพี (http) ซึ่งก็จะแยกเป็นเฮดเดอร์กับบอดี้ การที่โจทก์จะพบไฟล์แคชที่แสดงการล็อกอินใช้งานเฟซบุ๊กจากเครื่องคอมพิวเตอร์ของสุรศักดิ์นั้นจึงเป็นไปไม่ได้ ทำให้มีข้อสงสัยว่าไฟล์หลักฐานที่โจทก์อ้างนั้นไม่ใช่ข้อมูลที่ถูกต้องแท้จริง และถูกสร้างขึ้นใหม่เพื่อใช้กล่าวหาสุรศักดิ์ ซึ่งขัดกับพยานหลักฐานที่ฝ่ายโจทก์อ้างว่าพบร่องรอยการใช้เฟซบุ๊กบันทึกอยู่ในเครื่องคอมพิวเตอร์ของกลาง

ในการพิจารณาคดีในชั้นศาล ทนายความของสุรภักดิ์ ยังได้ขอให้พยานผู้เชี่ยวชาญโจทก์ให้ความเห็นต่อศาลว่า เครื่องคอมพิวเตอร์ของจำเลยเก็บบันทึกแคชหรือข้อมูลการใช้งานเฟซบุ๊กไว้ในพื้นที่บันทึกชั่วคราวได้หรือไม่ ปรากฏว่าพยานผู้เชี่ยวชาญฝ่ายโจทก์ยืนยันว่าเก็บบันทึกได้ แต่ปรากฏว่าพยานผู้เชี่ยวชาญของสุรภักดิ์ สาธิตด้วยคอมพิวเตอร์แสดงให้ศาลเห็นว่าเฟซบุ๊กไม่

[32] เรื่องเดียวกัน, 66-67.

อนุญาตให้เครื่องคอมพิวเตอร์ของผู้ใช้เก็บบันทึกไฟล์ ทำให้ความน่าเชื่อถือของพยานผู้เชี่ยวชาญฝ่ายโจทก์ลดลง เพราะไม่ได้มีความเชี่ยวชาญในเรื่องความเชี่ยวชาญทางเทคนิคอย่างแท้จริง[33]

ในการชั่งน้ำหนักและรับฟังพยานหลักฐานของศาล คดีนี้ศาลฎีกามีคำพิพากษา ยกฟ้อง โดยให้เหตุผลในคำพิพากษาว่า

> *"เนื่องจากไม่ปรากฏประวัติการใช้อีเมลและเฟซบุ๊กตามฟ้องจากเครื่องคอมพิวเตอร์ของจำเลย รวมถึงรหัสต้นฉบับที่พบในคอมพิวเตอร์ของกลาง ไม่อาจเกิดขึ้นในพื้นที่จัดเก็บข้อมูลปกติ แต่เกิดจากการทำขึ้นแล้วนำไปวางในเครื่องคอมพิวเตอร์ของกลาง นอกจากนี้คอมพิวเตอร์ของกลางยังถูกเปิดหลังจำเลยถูกควบคุมตัว ทำให้ข้อมูลที่ได้จากการตรวจพิสูจน์พยานหลักฐานดิจิทัลมีข้อบกพร่องและไม่น่าเชื่อถือว่าจำเลยกระทำความผิดตามฟ้องจริงหรือไม่ ต้องยกประโยชน์แห่งความสงสัยให้จำเลยตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 227 วรรคสอง"*[34]

จากการวิเคราะห์พบว่า คดีนี้ผู้พิพากษาอนุญาตให้จำเลยนำคอมพิวเตอร์มาสืบประกอบการสืบพยานในศาลได้ และมีประโยชน์ต่อรูปคดีอย่างมากในการที่จะแสดงให้ศาลเห็นถึงข้อบกพร่องในการนำเสนอพยานหลักฐานของพยานผู้เชี่ยวชาญฝ่ายโจทก์ อีกทั้งยังแสดงให้เห็นว่าพยานผู้เชี่ยวชาญฝ่ายโจทก์ขาดความรู้ความเชี่ยวชาญทางเทคนิค จึงส่งผลให้รายงานผลการตรวจพิสูจน์พยานหลักฐานดิจิทัลของฝ่ายโจทก์ขาดความน่าเชื่อถือ

ในกระบวนการยุติธรรมทางอาญาที่เกี่ยวข้องกับพยานหลักฐานดิจิทัล หากมีการโต้แย้งถึงความถูกต้องของพยานหลักฐานดิจิทัล ในกรณีทั่วไปคู่ความฝ่ายที่กล่าวอ้างจะต้องนำพยานบุคคลที่ตรวจยึด และเก็บรักษาพยานหลักฐานดังกล่าวมาเบิกความต่อศาล ส่วนในกรณีที่พยานหลักฐานมีความซับซ้อนคู่ความฝ่ายที่กล่าวอ้างอาจจำเป็นต้องนำพยานผู้เชี่ยวชาญ (Expert Witness) มาเบิกความต่อศาล ซึ่งความเห็นของผู้เชี่ยวชาญจะมีประโยชน์ต่อการวินิจฉัยคดี

จากคดีตัวอย่าง คดีอำพล (คดีอากง SMS) และ คดีสุรภักดิ์ (คดีเฟซบุ๊ก: เราจะครองฯ) ทำให้เห็นถึงความสำคัญของคุณค่าของพยานหลักฐานดิจิทัล การรับฟังพยานหลักฐานดิจิทัล และการต่อสู้คดีโดยใช้พยานหลักฐานดิจิทัล ซึ่งทั้งฝ่ายโจทก์และฝ่ายจำเลยได้ใช้พยานหลักฐานดิจิทัล

---

[33] เรื่องเดียวกัน หน้า ,67-68.

[34] สุรภักดิ์ กับ พนักงานอัยการ สำนักงานอัยการสูงสุด, คำพิพากษาศาลอาญาที่ 4008 (ศาลอาญา2555).

ในการต่อสู้คดี โดยคดีอำพลและคดีสุรภักดิ์ได้มีประเด็นการต่อสู้คดีที่มีลักษณะร่วมกัน คือ การพิสูจน์ตัวตนจากพยานหลักฐานดิจิทัลที่ฝ่ายโจทก์กล่าวอ้าง และความสำคัญของพยานผู้เชี่ยวชาญในการต่อสู้คดี โดยเฉพาะในคดีสุรภักดิ์ที่เจ้าตัวเป็นผู้เชี่ยวชาญทางคอมพิวเตอร์อยู่แล้ว จึงมีประเด็นต่อสู้เพิ่มเติมที่แตกต่างออกไป คือ หลักการในการตรวจพิสูจน์พยานหลักฐานดิจิทัลของฝ่ายโจทก์ กรณีการจัดเก็บอุปกรณ์ คอมพิวเตอร์ของจำเลยถูกเปิดใช้งานในระหว่างที่จำเลยถูกคุมขัง การสู้คดีในลักษณะนี้มีความซับซ้อนอย่างมาก ฝ่ายที่โต้แย้งต่อสู้จะต้องทำการพิสูจน์และอธิบายเรื่องทางเทคนิคให้ศาลเข้าใจ เนื่องจากภาระการพิสูจน์ถูกผลักมาอยู่ที่ผู้กล่าวอ้าง/โต้แย้งตามหลักผู้ใดกล่าวอ้างผู้นั้นมีหน้าที่นำสืบ

คดีเกี่ยวกับความมั่นคงหรือคดีอาญาที่เกี่ยวข้องกับการตรวจพิสูจน์พยานหลักฐานดิจิทัลที่รัฐ (พนักงานอัยการ) เป็นโจทก์ฟ้องคดี ฝ่ายโจทก์มักจะมีทรัพยากร เครื่องมือทางด้านเทคโนโลยีในการแสวงหาและได้มาซึ่งพยานหลักฐานดิจิทัล อีกทั้งยังมีพยานผู้เชี่ยวชาญที่ผ่านการอบรม มีความรู้ความสามารถในการอธิบายถึงตัวพยานหลักฐานดิจิทัลมาสนับสนุนความน่าเชื่อถือของน้ำหนักพยานหลักฐานฝ่ายตน ซึ่งตรงข้ามกับฝ่ายจำเลยที่มีข้อจำกัดในการแสวงหาพยานผู้เชี่ยวชาญเพื่อมาอธิบายและโต้แย้งข้อกล่าวอ้างที่เกี่ยวกับพยานหลักฐานดิจิทัลของฝ่ายโจทก์ว่ามีความถูกต้องแท้จริงหรือไม่ รวมถึงข้อจำกัดในการเข้าถึงพยานหลักฐานดิจิทัล อย่างไรก็ตาม ฝ่ายจำเลยยังต้องใช้ทรัพยากรส่วนบุคคลในแสวงหาพยานผู้เชี่ยวชาญมาเบิกความเป็นพยานให้ฝ่ายจำเลยเอง อีกทั้งยังไม่มีหน่วยงานของรัฐหรือองค์กรอื่นใดที่เข้ามาส่วนเกี่ยวข้อง/บทบาทในการช่วยเหลือในด้านการตรวจพิสูจน์พยานหลักฐานดิจิทัล และการสนับสนุนผู้เชี่ยวชาญด้านการตรวจพิสูจน์พยานหลักฐานดิจิทัล จะเห็นได้จากการสัมภาษณ์ทนายความ[35] ที่ได้ให้ความเห็นว่า

> *“ทนายความหรือตัวจำเลยต้องมีเส้นสาย ที่ผ่านมาเราใช้ทรัพยากรส่วนบุคคล ไม่มีหน่วยงานใดเข้ามาช่วยเหลือ ไม่แน่ใจว่า อันนี้เป็นข้อเสนอได้หรือไม่ว่า ศาลควรจะมีพยานผู้เชี่ยวชาญให้เลือกเหมือนกับถ้าเป็นหมอ ศาลก็จะมี Listพยานผู้เชี่ยวชาญอยู่ ที่พร้อมจะมาเบิกความตามหลักวิชาการ”*

[35] สัมภาษณ์ทนายความอาสาและทนายความเครือข่ายของศูนย์ทนายความเพื่อสิทธิมนุษยชน, สัมภาษณ์โดย วรินทรา ศรีวิชัย, คณะนิติศาสตร์ มหาวิทยาลัยเชียงใหม่, 24 ธันวาคม 2561.

สอดคล้องกับข้อมูลจากการสัมภาษณ์ผู้พิพากษา[36] ได้สะท้อนปัญหาและมุมมองของการออกประกาศหรือระเบียบเกี่ยวกับการคัดกรองพยานผู้เชี่ยวชาญไว้ว่า

> *“ศาลได้มีทะเบียนผู้เชี่ยวชาญของศาลอยู่ แต่ในส่วนของการตรวจพิสูจน์พยานหลักฐานดิจิทัลนั้น ยังไม่มีการขึ้นทะเบียน ส่วนใหญ่จะขอความร่วมมือจากเจ้าหน้าที่ตำรวจ เจ้าหน้าที่นิติวิทยาศาสตร์ เจ้าหน้าที่จากหน่วยงานของรัฐ เข้ามาช่วยเหลือ ในส่วนของหลักเกณฑ์ของพยานผู้เชี่ยวชาญนั้น ประเทศไทยก็ไม่ได้ตั้งหลักเกณฑ์ว่าต้องจบการศึกษาอะไรมา หากมีความชำนาญในเรื่องของการตรวจพิสูจน์พยานหลักฐานดิจิทัลแต่ไม่ได้มีใบรับรองการฝึกอบรม ศาลก็รับฟังได้ว่าเขามีความชำนาญเกี่ยวกับการตรวจพิสูจน์พยานหลักฐานดิจิทัลแล้ว เพราะมันไม่ได้เป็นสาขาวิชาชีพเฉพาะ”*

ทั้งนี้ ผู้เขียนเห็นว่าผู้เชี่ยวชาญด้านการตรวจพิสูจน์พยานหลักฐานดิจิทัลมีความสำคัญอย่างมากในทุกขั้นตอนที่เกี่ยวข้องกับพยานหลักฐานดิจิทัล ตั้งแต่การรวบรวมพยานหลักฐาน การเก็บรักษาพยานหลักฐาน การวิเคราะห์พยานหลักฐาน และการนำเสนอผลการตรวจพิสูจน์พยานหลักฐาน หากฝ่ายโจทก์และฝ่ายจำเลยต้องเผชิญกับพยานหลักฐานดิจิทัลเป็นครั้งแรก โดยขาดความรู้เกี่ยวกับวิธีการดำเนินคดีที่มีพยานหลักฐานดิจิทัลเข้ามาเกี่ยวข้อง จะส่งผลต่อกระบวนการพิจารณาคดี ดังนั้น ผู้เชี่ยวชาญด้านการตรวจพิสูจน์พยานหลักฐานดิจิทัลจึงมีหน้าที่ในการนำเสนอและอธิบายให้ทุกฝ่ายเห็นข้อเท็จจริง กระบวนการตรวจพิสูจน์หลักฐาน รวมถึงความถูกต้องของข้อมูลดิจิทัล อย่างไรก็ตาม การรวมศูนย์อำนาจหน้าที่การตรวจพิสูจน์พยานหลักฐานดิจิทัลยังคงจำกัดอยู่ที่หน่วยงานภาครัฐ ซึ่งยังไม่มีการสร้างความร่วมมือกับหน่วยงานภาคส่วนอื่นๆ หรือภาคเอกชนที่จะเข้ามามีส่วนร่วมในการตรวจพิสูจน์พยานหลักฐานดิจิทัล โดยเฉพาะในคดีเกี่ยวกับความมั่นคงที่หน่วยงานรัฐเป็นผู้ฟ้องคดี อีกทั้งการมีหน่วยงานอื่นเข้ามามีส่วนร่วมในการตรวจพิสูจน์พยานหลักฐานดิจิทัลจะเป็นการสร้างหลักประกัน และการตรวจสอบความน่าเชื่อถือของพยานหลักฐานดิจิทัลนั้นๆ

---

[36] สัมภาษณ์ผู้พิพากษาศาลชั้นต้นประจำสำนักประธานศาลฎีกา, สัมภาษณ์โดย วรินทรา ศรีวิชัย, สำนักงานศาลยุติธรรม ศาลอาญา, 16 มกราคม 2562.

บทสรุป

การตรวจพิสูจน์พยานหลักฐานดิจิทัล ทุกฝ่ายที่เกี่ยวข้องควรมีความรู้และความเข้าใจถึงหลักการตรวจพิสูจน์พยานหลักฐานดิจิทัล ตั้งแต่กระบวนการรวบรวมพยานหลักฐาน การเก็บพยานหลักฐาน การวิเคราะห์พยานหลักฐาน และการนำเสนอพยานหลักฐานที่ต้องกระทำโดยผู้เชี่ยวชาญและเป็นไปตามมาตรฐานสากล มิเช่นนั้นอาจส่งผลให้พยานหลักฐานดิจิทัลขาดความน่าเชื่อถือและไม่สามารถรับฟังเป็นพยานหลักฐานในชั้นศาลได้ ปัจจุบันแม้จะไม่มีกฎหมายเฉพาะเกี่ยวกับการตรวจพิสูจน์พยานหลักฐานดิจิทัล แต่ก็มีการจัดทำมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐานดิจิทัล โดยศูนย์ดิจิทัลฟอเรนสิกส์ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) เพื่อเป็นแนวทางการตรวจพิสูจน์พยานหลักฐานดิจิทัลที่ทีมาตรฐานการปฏิบัติการที่ชัดเจน

ในการต่อสู้คดีที่มีพยานหลักฐานดิจิทัลเข้ามาเกี่ยวข้อง โดยเฉพาะคดีเกี่ยวกับความมั่นคง พบว่า การดำเนินคดีเป็นการสร้างภาระให้แก่ผู้ถูกกล่าวหาในการต่อสู้คดี เช่น ความรู้ความเข้าใจพยานหลักฐานดิจิทัล ทุนทรัพย์ในแสวงหาพยานผู้เชี่ยวชาญในการต่อสู้คดี และ ข้อจำกัดในการเข้าถึงข้อมูลจากจากผู้ให้บริการ/หน่วยงานของรัฐ เป็นต้น

แนวทางในการสร้างหลักประกันและความเท่าเทียมในการเข้าถึงและใช้พยานหลักฐานดิจิทัล กล่าวคือ ในทุกขั้นตอนของการดำเนินกระบวนการยุติธรรมทางอาญาในการจัดการตรวจพิสูจน์พยานหลักฐานดิจิทัล โดยเฉพาะอย่างยิ่งในขั้นตอนการสืบสวน สอบสวน การรวบรวมพยานหลักฐานดิจิทัล ตลอดจนการรับฟังพยานหลักฐานดิจิทัล ควรมีแนวทางมาตรฐาน ขั้นตอนการปฏิบัติที่ชัดเจนและสอดคล้องกับมาตรฐานสากล ตลอดจนการเปิดโอกาสให้หน่วยงานอื่นที่มีศักยภาพและความน่าเชื่อถือเข้ามาร่วมทำงานในการตรวจพิสูจน์พยานหลักฐานดิจิทัล อีกทั้งควรมีกฎหมายหรือหลักประกันที่เป็นมาตรฐานในการตรวจพิสูจน์พยานหลักฐาน ซึ่งนำไปสู่การสร้างความเป็นธรรมให้กับทุกฝ่ายในกระบวนการยุติธรรมทางอาญา

References

We are social. “Digital 2019.” We are social. accessed April 12 2020 https://wearesocial .com/global-digital-report-2019.

เจษฎา คำรินทร์. “ปัญหาทางกฎหมายเกี่ยวกับการรับฟังพยานหลักฐานทางอิเล็กทรอนิกส์ในคดีอาญา.” วารสารมหาจุฬานาครทรรศ์ 6, ฉ.9 (2562): 4549-4550.

แลร์รี อี แดนเนียล และลาร์ส อี แดนเนียล. *การตรวจพิสูจน์พยานหลักฐานดิจิทัลสำหรับผู้ประกอบวิชาชีพกฎหมาย*.แปลโดย สุนีย์ สกาวรัตน์. กรุงเทพฯ: มูลนิธิเพื่ออินเทอร์เน็ตและวัฒนธรรมพลเมือง, 2559.

ไอซีที. “8 เดือนคดีไซเบอร์แซงปี61 ปอท. เฟ้นหาไวต์แฮกเกอร์.” ประชาชาติธุรกิจ. 13 กันยายน 2562. สืบค้นเมื่อวันที่ 12 เมษายน 2563. https://www.prachachat.net/ict/news-370708.

ไอลอว์. “ฐานข้อมูลคดีสุรภักดิ์.” ไอลอว์. สืบค้นเมื่อวันที่ 12 เมษายน 2563 https://freedom.ilaw.or.th/th/case/176.

ไอลอว์. “ฐานข้อมูลคดีอำพล : อากงเอสเอ็มเอส.” ไอลอว์. สืบค้นเมื่อวันที่ 12 เมษายน 2562 https://freedom.ilaw.or.th/th/case/21.

ไอลอว์. “สถิติศูนย์ข้อมูลกฎหมายและคดีเสรีภาพ.” ไอลอว์. สืบค้นเมื่อวันที่ 12 เมษายน 2563 https://freedom.ilaw.or.th/case?page=7 &Offense=9 % 2 B1 0 &d_ from=&d_to =&k=&p=.

นลินี ฐิตะวรรณ. *โลกใหม่ ใครกำกับ?*. กรุงเทพฯ: มูลนิธิเพื่ออินเทอร์เน็ตและวัฒนธรรมพลเมือง, 2557.

ประชาไท. “การรวบรวมพยานหลักฐานในคดีอาชญากรรมคอมพิวเตอร์.” ประชาไท. สืบค้นเมื่อวันที่ 12 เมษายน 2563 https://prachatai.com/journal/2019/12/85402#_ftn14.

ประชาไท. “หลักฐานดิจิทัล#1: ความเข้าใจพื้นฐาน ผู้ใช้อินเทอร์เน็ตต้องรู้!.” ประชาไท. สืบค้นเมื่อวันที่ 12 เมษายน 2563 https://prachatai.com/journal/2015/10/61879.

ประชาไท. “หลักฐานดิจิทัล#1: ความเข้าใจพื้นฐาน ผู้ใช้อินเทอร์เน็ตต้องรู้!.” ประชาไท. สืบค้นเมื่อวันที่ 20 เมษายน 2563 https://prachatai.com/journal/2015/10/61879.

ปิยบุตร แสงกนกกุล. “สภาวะยกเว้นในความคิดของ Giorgio Agamben.” *วารสารฟ้าเดียวกัน* 8, ฉ.1 (2553): 84-91.

พรเพชร วิชิตชลลัย. *คำอธิบายกฎหมายลักษณะพยาน.* พิมพ์ครั้งที่ 4. กรุงเทพฯ: สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา, 2555.

ศูนย์ดิจิทัลฟอเรนสิกส์. *ข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐานดิจิทัล.* กรุงเทพฯ: สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2559.

ศูนย์ดิจิทัลฟอเรนสิกส์. *ข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐานดิจิทัล.*กรุงเทพฯ: สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2559.

สำนักการต่างประเทศ. “รายงานของคณะข้าราชการตุลาการหลักสูตร กฎหมายอาชญากรรมคอมพิวเตอร์และกฎหมายเกี่ยวกับพยานหลักฐานดิจิตอล.” สำนักการต่างประเทศ. สืบค้นเมื่อวันที่ 12 เมษายน 2563 https://oia.coj.go.th/th/content/category/detail/id/8/cid/9041/iid/154331.

สำนักงานราชบัณฑิตยสภา. “ศัพท์บัญญัติสำนักงานราชบัณฑิตยสภา.” สำนักงานราชบัณฑิตยสภา. สืบค้นเมื่อวันที่ 12 เมษายน 2563 http://www.royin.go.th/coined_word/.