2021

กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล: การวิเคราะห์เพื่อพัฒนาเชิงนโยบาย

กานต์ ศรีสุวรรณ
คณะรัฐศาสตร์

กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล: การวิเคราะห์เพื่อพัฒนาเชิงนโยบาย

นายกานต์ ศรีสุวรรณ

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาศิลปศาสตรดุษฎีบัณฑิต
สาขาวิชาอาชญาวิทยาและงานยุติธรรม ภาควิชาสังคมวิทยาและมานุษยวิทยา
คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2564

DIGITAL FORENSICS EVIDENCE PROVING PROCESS: AN ANALYTIC APPROACH TO POLICY DEVELOPMENT

Mr. Karnt Srisuwan

A Dissertation Submitted in Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy in Criminology and Criminal Justice
Department of Sociology and Anthropology
FACULTY OF POLITICAL SCIENCE
Chulalongkorn University
Academic Year 2021

หัวข้อวิทยานิพนธ์	กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล: การวิเคราะห์เพื่อพัฒนาเชิงนโยบาย
โดย	นายกานต์ ศรีสุวรรณ
สาขาวิชา	อาชญาวิทยาและงานยุติธรรม
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	รองศาสตราจารย์ ดร.สุมนทิพย์ จิตสว่าง

คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาศิลปศาสตรดุษฎีบัณฑิต

..... คณบดีคณะรัฐศาสตร์
(รองศาสตราจารย์ ดร.เอก ตั้งทรัพย์วัฒนา)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(ศ.พล.ต.ต.ดร.หญิงพัชรา สินลอยมา)

..... อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(รองศาสตราจารย์ ดร.สุมนทิพย์ จิตสว่าง)

..... กรรมการ
(รองศาสตราจารย์ ดร.จุฑารัตน์ เอื้ออำนวย)

..... กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.ฐิติยา เพชรมุนี)

..... กรรมการภายนอกมหาวิทยาลัย
(พ.อ.ดร.เศรษฐพงศ์ มะลิสุวรรณ)

กานต์ ศรีสุวรรณ : กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล: การวิเคราะห์เพื่อพัฒนาเชิงนโยบาย. (DIGITAL FORENSICS EVIDENCE PROVING PROCESS: AN ANALYTIC APPROACH TO POLICY DEVELOPMENT) อ.ที่ปรึกษาหลัก : รศ. ดร. สุมนทิพย์ จิตสว่าง

การวิจัยนี้ มีวัตถุประสงค์ในการนำเสนอขั้นตอนของกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลในประเทศไทย กฎหมายที่เกี่ยวข้อง ตลอดจนปัญหาและอุปสรรค เพื่อนำไปสู่ข้อเสนอเชิงนโยบายในการปรับปรุงกฎหมายและพัฒนากระบวนการตรวจพิสูจน์พยานหลักฐาน โดยเนื้อหาเกี่ยวกับลักษณะเฉพาะของพยานหลักฐานดิจิทัล กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล ประเด็นปัญหาและอุปสรรคจากผู้ที่เกี่ยวข้อง ข้อเสนอเชิงนโยบายและเชิงปฏิบัติ โดยใช้วิธีการวิจัยเชิงคุณภาพจากเอกสาร การลงพื้นที่สัมภาษณ์เชิงลึกและกรณีศึกษา จากการศึกษาพบว่า กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลในประเทศไทย 4 ขั้นตอน มีปัญหาและอุปสรรค คือ 1) การรวบรวมพยานหลักฐาน มีปัญหาในการรวบรวมพยานหลักฐานให้สมบูรณ์ขณะเกิดเหตุโดยไม่ถูกเปลี่ยนแปลงแก้ไข 2) การเก็บรักษาพยานหลักฐาน ไม่เป็นไปตามมาตรฐานการจัดเก็บ และการจัดการพยานหลักฐานดิจิทัล 3) การวิเคราะห์พยานหลักฐานดิจิทัล บุคลากรบางส่วนขาดความเชี่ยวชาญที่จำเป็นเฉพาะด้าน 4) การนำเสนอผลพิสูจน์พยานหลักฐานดิจิทัล มีการโต้แย้ง หรือขาดน้ำหนักในการรับฟังในชั้นพิจารณาคดี ข้อเสนอแนะจากการศึกษาครั้งนี้ คือ ควรมีการปรับปรุงพัฒนากระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลในประเทศไทยให้มีมาตรฐานการปฏิบัติที่ชัดเจนในทั้ง 4 ขั้นตอนให้สอดคล้องกับมาตรฐานสากล บุคลากรควรได้รับการอบรมเพิ่มเติมในประเด็นความเชี่ยวชาญเฉพาะด้าน เพื่อช่วยลดปัญหาและอุปสรรคในการปฏิบัติงาน มีการแก้ไขกฎหมายที่เกี่ยวข้อง รวมถึงสนับสนุนให้มีการจัดตั้งสภาวิชาชีพนิติวิทยาศาสตร์ และจัดตั้งหน่วยงานเฉพาะที่ทำหน้าที่ในการกำกับดูแล โดยเริ่มต้นจากการส่งเสริมบทบาทของศูนย์ดิจิทัลฟอเรนสิกส์ที่มีอยู่เดิม เพื่อให้การป้องกันปราบปรามอาชญากรรมคอมพิวเตอร์ในประเทศไทยมีประสิทธิภาพมากขึ้น

สาขาวิชา อาชญาวิทยาและงานยุติธรรม ลายมือชื่อนิสิต .....

ปีการศึกษา 2564 ลายมือชื่อ อ.ที่ปรึกษาหลัก .....

5881352324 : MAJOR CRIMINOLOGY AND CRIMINAL JUSTICE
KEYWORD: Digital Evidence, Digital Forensics, Cybercrime, Proposed Policy
Karnt Srisuwan : DIGITAL FORENSICS EVIDENCE PROVING PROCESS: AN ANALYTIC APPROACH TO POLICY DEVELOPMENT. Advisor: Assoc. Prof. SUMONTHIP CHITSAWANG, Ph.D.

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 documents, case studies and in-depth interviews with scholars who involve in digital forensics. This research found that the process to acquire digital evidence in Thailand still remains unclear even there is a digital forensic management standard for digital forensics, provided by the Digital Forensics Center under the Electronic Transactions Development Agency (ETDA). There should be the policy development that makes the digital forensic process meet the standards demanded to comprehensible standards of practice. 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 revision or guarantees that create standards for forensics, that lead to bringing justice to every parties in the criminal justice process.

Field of Study: Criminology and Criminal Justice Student's Signature .....
Academic Year: 2021 Advisor's Signature .....

กิตติกรรมประกาศ

ดุษฎีนิพนธ์นี้สำเร็จลุล่วงด้วยดี เนื่องด้วยได้รับคำชี้แนะที่เป็นประโยชน์จากหลายฝ่ายที่ช่วยเติมเต็มความสมบูรณ์ให้งานวิจัย กราบขอบพระคุณอาจารย์ที่ปรึกษา รองศาสตราจารย์ ดร. สุมนทิพย์ จิตสว่าง ที่เมตตา สละเวลา คอยผลักดันช่วยเหลือจนสำเร็จ ศาสตราจารย์ พลตำรวจตรีหญิง ดร.พัชรา สินลอยมา, รองศาสตราจารย์ ดร.จุฑารัตน์ เอื้ออำนวย, ผู้ช่วยศาสตราจารย์ ดร. ฐิติยา เพชรมุนี และพันเอก ดร.เศรษฐพงค์ มะลิสุวรรณ กรรมการสอบ ที่ได้กรุณา ตรวจแก้ไข แนะนำ กราบขอบพระคุณคณาจารย์ จุฬาลงกรณ์มหาวิทยาลัย และอาจารย์ผู้ทรงคุณวุฒิทุกท่าน สำหรับองค์ความรู้และข้อมูลที่เป็นประโยชน์ยิ่งต่องานวิจัย รวมถึงเจ้าหน้าที่ภาควิชาสังคมวิทยาและมานุษยวิทยา คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ที่ได้คอยดูแล ช่วยเหลือ ประสานงาน

กราบขอบพระคุณ คุณพ่อคุณแม่ และขอบคุณภรรยา ลูกสาว ที่คอยเป็นกำลังใจ ผลักดัน สนับสนุน ให้ความรัก ความห่วงใยให้ผู้วิจัยมีความพยายามมุ่งมั่น ขอบคุณเพื่อน ป.เอก อาชญาฯ รุ่น 1 รวมถึงน้องๆ ป.โท อาชญาฯ รุ่น 1 ที่ได้ร่วมเรียนกันมา รวมถึงทุกๆ คนที่คอยช่วยเหลือด้านเอกสารมาโดยตลอด ขอบคุณผู้ให้ข้อมูลสำคัญทุกท่าน สำหรับการถ่ายทอดข้อมูล ประสบการณ์ให้กับผู้วิจัย

การวิจัยนี้ ได้รับการสนับสนุนทุนการศึกษาจากทุนการศึกษาหลักสูตรดุษฎีบัณฑิต “100 ปี จุฬาลงกรณ์มหาวิทยาลัย” (The 100th Anniversary Chulalongkorn University Fund for Doctoral Scholarship) และทุน 90 ปี จุฬาลงกรณ์มหาวิทยาลัย กองทุนรัชดาภิเษกสมโภช [The 90th Anniversary of Chulalongkorn University Fund (Ratchadaphiseksomphot Endowment Fund)]

หากผลการศึกษานี้มีข้อมูลบกพร่องประการใด ผู้วิจัยขอน้อมรับไว้แต่เพียงผู้เดียว และหวังว่าจะมีโอกาสได้ต่อยอด แก้ไขให้สมบูรณ์ยิ่งขึ้นในโอกาสต่อไป สุดท้ายนี้ผู้วิจัยหวังเป็นอย่างยิ่งว่า งานวิจัยนี้จะมีประโยชน์ในการผลักดันให้เกิดการพัฒนาเชิงนโยบาย สำหรับกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลในประเทศไทยต่อไป

กานต์ ศรีสุวรรณ

กานต์ ศรีสุวรรณ

สารบัญ

หน้า

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญของปัญหา

สำหรับโลกยุคปัจจุบัน เครือข่ายอินเทอร์เน็ต และสังคมดิจิทัล เข้ามามีบทบาทและส่งผลต่อการเปลี่ยนแปลงในรูปแบบและวัฒนธรรมการดำรงชีวิตของคนมากขึ้น เครือข่ายสังคม (Social network) หรือชุมชนออนไลน์ต่างๆ เข้ามาเป็นส่วนหนึ่งของการใช้ชีวิต ควบคู่ไปกับการเติบโตของตลาดอุปกรณ์พกพาอัจฉริยะ (Smart portable devices) ที่เป็นมากกว่าแค่อุปกรณ์สื่อสาร ความก้าวหน้าทางเทคโนโลยี การพลิกผันทางดิจิทัล[1] (Digital disruption) ซึ่ง เศรษฐพงค์ มะลิสุวรรณ (2560) ได้ชี้ให้เห็นว่า จากความก้าวหน้าทางเทคโนโลยีอย่างก้าวกระโดด ทำให้โลกของเรามีการผลิตข้อมูลปริมาณมหาศาลในทุกวินาที และการพลิกผันช่างใกล้ตัวเราเพียงแต่เรามองข้ามเท่านั้น โดยเฉพาะการเข้ามาของ Internet of things (IoT), Cloud, Big data และ Crypto currency ส่งผลให้ชีวิตประจำวันของผู้คนสะดวกสบายและง่ายขึ้น แต่นอกจากประโยชน์อันมหาศาลที่ผู้คนได้รับจากการเปลี่ยนแปลงนี้ ก็นำมาซึ่งอาชญากรรมอีกรูปแบบ ที่อาจคุกคามชีวิต ทรัพย์สินเงินทอง รวมถึงส่งผลกระทบด้านอื่นๆ อย่างมากมายเช่นกัน ในประเทศไทย สถิติจำนวนผู้ใช้งานอินเทอร์เน็ตเพิ่มมากขึ้นแบบก้าวกระโดด จากเกือบ 7 ล้านคน ในปี 2547 เป็น 53.3 ล้านคนในปี 2563[2] อาชญากรรม ไซเบอร์ในประเทศไทยมีแนวโน้มเพิ่มสูงขึ้นอย่างรวดเร็ว เมื่อมองย้อนกลับไปดูในช่วง 10 ปีที่ผ่านมา หรือเทียบ 3 ปีย้อนหลัง จะเห็นแนวโน้มชัดเจนว่า แต่เดิมอาชญากรรมคอมพิวเตอร์ที่คนทั่วไปรู้จักจากเพียงฉากในภาพยนตร์ มีอาชญากรนั่งอยู่ในห้องมืดๆแคบๆ เรื่องต่างๆ ยังคงห่างไกลตัว เริ่มต้นจากการเจาะระบบคอมพิวเตอร์เฉพาะ เช่น ระบบของสำนักงานสอบสวนกลางของประเทศสหรัฐอเมริกา (Federal Bureau of Investigation: FBI) หรืออาคารที่ทำการกระทรวงกลาโหมของประเทศสหรัฐอเมริกา; อาคารเพนตากอน ก็คืบคลานเข้ามาใกล้ตัว เข้ามาในชีวิตประจำวันของเรามากขึ้น อุปกรณ์มือถือที่เชื่อมต่อกับเครือข่ายอินเทอร์เน็ตได้มีราคาถูกลง ใช้กันอย่างแพร่หลาย เครือข่ายอินเทอร์เน็ตมีความเร็วสูงขึ้น เป้าหมายของการก่ออาชญากรรมไซเบอร์เดิมมีเป้าหมายและจุดประสงค์เฉพาะ เน้นการทดสอบ ทดลอง หรือก่อกวนเป็นจุดๆ มีผู้ก่อเหตุคนเดียวหรือกลุ่มย่อยๆ เนื่องจากสมัยก่อนการติดต่อสื่อสารกันทำได้ยาก ต้องอาศัยช่องทางเฉพาะ ในปัจจุบันมีลักษณะเป็นกลุ่มขนาดใหญ่มากขึ้นคล้ายกับองค์กรอาชญากรรม เป้าหมายและวัตถุประสงค์

---

[1] “The Year of Disruption”, tct.or.th, สืบค้นเมื่อ 12 เม.ย.61, http://tct.or.th/images/article/special_article/25610110/198410_Disruption.pdf.

[2] “สรุปผลที่สำคัญ สำรวจการมีการใช้เทคโนโลยีสารสนเทศและการสื่อสารในครัวเรือน พ.ศ. 2563 สำนักงานสถิติแห่งชาติ”, www.nso.go.th, สืบค้นเมื่อ 9 ก.ย.64, http://www.nso.go.th/sites/2014/DocLib13/ด้านICT/เทคโนโลยีในครัวเรือน/2563/Pocketbook63.pdf.

เปลี่ยนไป การขู่เรียกเงินจากทั้งรายบุคคล และหน่วยงาน (Ransomeware)[3] มีการเติบโตอย่างชัดเจนในปี พ.ศ. 2558-2563 เมื่อเทียบกับปีก่อนๆ และหลายตัว ยังไม่สามารถแก้ไขได้ มุ่งเน้นที่สถาบันการเงินมากขึ้น เน้นทำลายระบบมากกว่าการก่อกวน และมีการสร้างความหวาดกลัวในวงกว้างคล้ายกับองค์กรก่อการร้ายผ่านทางเครือข่ายสังคมที่ยากต่อการควบคุม มีเทคนิคใหม่ๆมากขึ้นในการเจาะทำลายระบบ ซึ่งยากต่อการป้องกันด้วยอุปกรณ์เดี่ยวๆแต่เดิม เช่น ใช้เพียงแค่ไฟร์วอลล์ (Firewall) สมัยก่อนความเสียหายเกิดขึ้นในวงแคบ แม้จะร้ายแรงแต่สามารถควบคุมจัดการได้ ติดตามจับกุมผู้กระทำผิดได้ง่าย เนื่องจากการกระทำผิดมักเชื่อมต่อมาจากจุดๆ เดียว มีเป้าหมายเดียว ในขณะที่ปัจจุบัน การจับกุมกระทำยากขึ้น เนื่องจากประสิทธิภาพของอุปกรณ์พกพาและความเร็วเครือข่าย ความเสียหายเกิดขึ้นพร้อมกันหลายจุด และผู้ก่อเหตุร่วมมือกัน "ข้ามชาติ" เป็นขบวนการ จากข้อมูลสถิติเกี่ยวกับอาชญากรรมคอมพิวเตอร์[4] ในปี พ.ศ. 2563 พบว่า มีผู้ตกเป็นเหยื่ออาชญากรรมคอมพิวเตอร์มากกว่า 556 ล้านคนต่อปี โดยคิดเป็น 1.5 ล้านคนต่อวัน 1,080 คนต่อนาทีและ 18 คนต่อวินาที โดยสามารถขโมยเงินได้มากถึงประมาณ 3,500,000,000,000 บาทต่อปี หรือสามารถขโมยเงินจากเหยื่อได้เฉลี่ย 6,300 บาทต่อคนต่อปี มูลเหตุจูงใจที่ทำให้ก่ออาชญากรรมอันดับหนึ่ง 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 การหลอกถามข้อมูลตัวต่อตัวทางโทรศัพท์ผ่านอีเมล และสุดท้ายคือการนำข้อมูลของลูกค้ามาเปิดเผย นอกจากนี้อาชญากรรมพื้นฐาน (Traditional street crimes) เอง ก็เกิดขึ้นในชุมชนออนไลน์ หรือเกี่ยวเนื่องกับสังคมดิจิทัลมากขึ้น

สำหรับประเทศไทย หลังจากที่มีการประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 หรือที่มักเรียกกันว่า พระราชบัญญัติคอมพิวเตอร์ ก็ได้มีการรวบรวมสถิติการดำเนินคดีตามพระราชบัญญัตินี้ เพื่อเก็บเป็นสถิติ โดยตัวอย่างข้อมูลจากศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย หรือไทยเซิร์ต ในปี พ.ศ. 2550–2563 พบว่า เว็บไซต์หน่วยงานด้านการศึกษามีไวรัสมากกว่าเว็บไซต์หน่วยงานอื่น คิดเป็นร้อยละ 48 และในปี พ.ศ. 2563 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 โดยสามารถจำแนกคดีได้ตามขั้นของ

[3] “ภัยไซเบอร์ในปี 2021 ทิศทางจะเป็นอย่างไร”, www.cyfence.com, สืบค้นเมื่อ 11 ส.ค. 64, https://www.cyfence.com/article/next-it-security-trend-2021/

[4] “Top 12 Cyber Crime Facts and Statistics”, www.blue-pencil.ca, สืบค้นเมื่อ 8 ก.ย. 64, https://www.blue-pencil.ca/top-12-cyber-crime-facts-and-statistics/

กระบวนการพิจารณาคดีและผลของคดี คือ คดีที่อยู่ในชั้นพนักงานสอบสวนหรือเจ้าหน้าที่ตำรวจ 74 คดี คดีที่พนักงานอัยการสั่งฟ้อง 43 คดี คดีที่พนักงานอัยการสั่งไม่ฟ้อง 1 คดี คดีที่มีการไกล่เกลี่ยยอมความ ถอนฟ้อง 10 คดี คดีที่ศาลพิพากษายกฟ้องโจทก์ 2 คดี คดีที่ศาลพิพากษาว่าจำเลยมีความผิด 37 คดี คดีที่ศาลพิพากษาแล้วแต่ไม่สามารถเข้าถึงผลการพิจารณาคดีได้ 14 คดี คดีที่พนักงานสอบสวนตั้งข้อหาตามพระราชบัญญัติคอมพิวเตอร์ แต่พนักงานอัยการไม่ได้สั่งฟ้องตามข้อหาดังกล่าวหรือศาลไม่ได้พิพากษาว่าเป็นความผิดตามพระราชบัญญัติคอมพิวเตอร์ 4 คดี

ประชาชนทั่วไป รวมถึงหน่วยงานภาครัฐ ภาคเอกชน แม้มีความคุ้นเคยกับการใช้งานเครือข่ายอินเทอร์เน็ต แต่ยังขาดความรู้ความเข้าใจในปัญหาและการป้องกันอาชญากรรมไซเบอร์ เมื่อมีการออกพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติฉบับที่ 2 ในปี พ.ศ. 2560 และกฎหมายอื่นๆ ที่เกี่ยวข้อง ซึ่งมีบทลงโทษสำหรับผู้กระทำผิด แต่สถิติการเกิดคดีก็ยังคงสูงอย่างต่อเนื่อง มีกรณีการเจาะระบบคอมพิวเตอร์เพิ่มมากขึ้นเรื่อยๆ ดังนั้น จึงควรมีการพิจารณาถึงปัญหา สาเหตุ แนวทางป้องกันแก้ไข ทั้งทางด้านกฎหมายและด้านอื่นๆ เพื่อให้ความเสียหายที่เกิดจากอาชญากรรมคอมพิวเตอร์ลดน้อยลง สำหรับในส่วนตำรวจเองได้มีการจัดตั้งกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) แต่ก็ยังมีปัญหาในส่วนเจ้าหน้าผู้ปฏิบัติงานขาดทักษะ ความรู้ด้านเทคนิคคอมพิวเตอร์ ประสบความยากลำบากในการแกะรอยผู้บุกรุกเข้าสู่ระบบ ปัญหาในการชี้และรวบรวมพยานหลักฐาน และข้อจำกัดด้านกฎหมายต่างๆ ตลอดจนขาดสถิติและความรู้เกี่ยวกับรูปแบบและลักษณะอาชญากรรมคอมพิวเตอร์ในประเทศไทย บวกกับการเปลี่ยนแปลงอย่างรวดเร็วของเทคโนโลยีคอมพิวเตอร์ มาตรการการกำกับดูแลต่างๆ ที่ใช้ก็ยังไม่ครอบคลุม ไม่สามารถบังคับใช้ได้อย่างมีประสิทธิภาพ มีประเด็นใหม่ๆ เกิดขึ้นในสังคม เกิดความสงสัย ข้อโต้แย้งมากมายว่าผู้ที่เกี่ยวข้องในกระบวนการยุติธรรม เช่น ตำรวจใช้บรรทัดฐานใดก่อนจะพิจารณารับเป็นคดี การดำเนินการตามขั้นตอนต่างๆ ในการจับกุม ตลอดจนการใช้พยานหลักฐานดิจิทัล (Digital evidences) และการตรวจพิสูจน์พยานหลักฐานดิจิทัล (Digital forensics) มีกระบวนการอย่างไร ทำให้ทราบถึงความจำเป็นที่จะต้องตระหนัก และมีความเข้าใจในปัญหาอาชญากรรมคอมพิวเตอร์ สาเหตุของอาชญากรรมคอมพิวเตอร์ในบริบทของทฤษฎีอาชญาวิทยาและทฤษฎีทางสังคม สิทธิ หน้าที่ เสรีภาพ กฎหมายที่เกี่ยวข้อง ตลอดจนต้องมีการกำหนดนโยบายทางอาญา มีขั้นตอนการจับกุม และกรอบการตรวจพิสูจน์พยานหลักฐานดิจิทัลที่ชัดเจนเพื่อที่จะได้มีเกณฑ์ที่ใช้ และการดำเนินการในทิศทางเดียวกัน ขจัดความเคลือบแคลงสงสัยในประเด็นทางสังคม และนำไปสู่ข้อเสนอแนะเชิงนโยบายและปฏิบัติ ตลอดจนข้อเสนอในการปรับปรุงกฎหมายและการบังคับใช้ เพื่อยกระดับกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลและกระบวนการยุติธรรมทางอาญาที่เกี่ยวข้องกับการกระทำความผิดทางคอมพิวเตอร์ในประเทศไทย เพื่อให้สามารถพัฒนาการป้องกันปราบปรามอาชญากรรมคอมพิวเตอร์ในประเทศไทย และนำไปสู่การแก้ไขปัญหาอย่างมีประสิทธิภาพและสอดคล้องกับมาตรฐานสากล

1.2 คำถามการวิจัย

1.2.1 กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลในประเทศไทยมีกระบวนการอย่างไร และมีกฎหมายใดที่เกี่ยวข้อง

1.2.2 ปัญหาและอุปสรรคของกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลในประเทศไทยในปัจจุบันมีอะไรบ้าง ทั้งในส่วนของกฎหมาย การบังคับใช้ และกระบวนการ ประเด็นใดที่ควรให้ความสำคัญ

1.2.3 ข้อเสนอแนะเชิงนโยบายในการปรับปรุงกฎหมาย และขั้นตอนการปฏิบัติ เพื่อให้กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลในประเทศไทยมีประสิทธิภาพมากขึ้นมีอะไรบ้าง

1.3 วัตถุประสงค์การวิจัย

1.3.1 เพื่อศึกษาขั้นตอนของกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลในประเทศไทย และกฎหมายที่เกี่ยวข้อง

1.3.2 เพื่อศึกษาวิเคราะห์ ปัญหาและอุปสรรคของกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลในประเทศไทย ในส่วนของกฎหมาย มุมมองของผู้เกี่ยวข้องในกระบวนการยุติธรรม ภาคประชาชน และกรณีศึกษา

1.3.3 เพื่อจัดทำข้อเสนอแนะเชิงนโยบาย ข้อแนะนำสำหรับแต่ละขั้นของกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล ข้อเสนอในการปรับปรุงกฎหมายและการบังคับใช้ เพื่อให้กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลในประเทศไทยสอดคล้องกับมาตรฐานสากล และการป้องกันปราบปรามอาชญากรรมคอมพิวเตอร์ในประเทศไทยมีประสิทธิภาพมากขึ้น

1.4 ขอบเขตการวิจัย

1.4.1 ขอบเขตด้านเนื้อหา

การศึกษานี้จะศึกษาเกี่ยวกับ ขั้นตอนของกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลในประเทศไทย กฎหมายที่เกี่ยวข้อง ปัญหาและอุปสรรค ข้อแนะนำสำหรับแต่ละขั้นตอนของกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล ข้อเสนอในการปรับปรุงกฎหมายและการบังคับใช้ เพื่อให้กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลในประเทศไทยสอดคล้องกับมาตรฐานสากล และการป้องกันปราบปรามอาชญากรรมคอมพิวเตอร์มีประสิทธิภาพมากขึ้น

ข้อมูลปฐมภูมิ (Primary data) เป็นข้อมูลที่ผู้วิจัยรวบรวมจากแหล่งของข้อมูลโดยตรง โดยได้มาจากการเก็บรวบรวมข้อมูลจากผู้ให้ข้อมูลสำคัญ ผู้วิจัยเก็บข้อมูลโดยวิธีการสัมภาษณ์ โดย ใช้วิธีการสัมภาษณ์เชิงลึกแบบกึ่งโครงสร้าง (Semi-structured in-depth interview) สอบถามผู้ให้ข้อมูลสำคัญในประเด็นต่างๆ ของกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล ตามหัวข้อการวิจัย

ข้อมูลทุติยภูมิ (Secondary data) เป็นข้อมูลที่ไม่ได้มาจากแหล่งข้อมูลโดยตรง ผู้วิจัยศึกษาค้นคว้าเก็บรวบรวมจากข้อมูลที่มีผู้อื่นรวบรวมไว้แล้ว เป็นการศึกษาจากเอกสารทางวิชาการ บทความ วารสาร หนังสือ สิ่งพิมพ์ กรณีศึกษา รายงานการวิจัย วิทยานิพนธ์ และดุษฎีนิพนธ์ต่างๆ รวมถึงสืบค้นจากสื่ออิเล็กทรอนิกส์ อินเทอร์เน็ต ในส่วนของข้อมูลเกี่ยวกับแนวคิดทฤษฎีและงานวิจัยที่เกี่ยวข้อง

1.4.2 ขอบเขตของผู้ให้ข้อมูลสำคัญ

ในการศึกษาวิจัยครั้งนี้ กลุ่มตัวอย่าง (Sample) ที่ใช้ในการวิจัยครั้งนี้ ผู้วิจัยเลือกการสุ่มตัวอย่างแบบเจาะจง (Purposive sampling) เป็นการเลือกตัวอย่างโดยกำหนดคุณลักษณะของประชากรที่ต้องการศึกษา เป็นการเก็บข้อมูลจากผู้ให้ข้อมูลสำคัญ (Key informants) จำนวน 31 คน โดยมีเกณฑ์การเลือก คือ ผู้ที่มีส่วนได้ส่วนเสีย และมีความเกี่ยวข้องกับกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล ในบริบทต่างๆ ที่

มีประสบการณ์ ความเชี่ยวชาญอย่างน้อย 3 ปี เป็นผู้มีส่วนร่วมในการวิจัย เกณฑ์การคัดเข้า และเกณฑ์การคัดออก

ผู้ให้ข้อมูลสำคัญ ได้แก่

1) บุคลากรภาครัฐ เจ้าหน้าที่ตำรวจที่มีประสบการณ์ทางด้านอาชญากรรมคอมพิวเตอร์ ในส่วนของกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล จำนวน 6 คน
2) อัยการที่มีความรู้ความชำนาญในคดีอาชญากรรมคอมพิวเตอร์ จำนวน 6 คน
3) ผู้พิพากษาที่มีความเชี่ยวชาญในคดีอาชญากรรมคอมพิวเตอร์ จำนวน 6 คน
4) บุคลากรภาคเอกชน ผู้เชี่ยวชาญ ที่มีทักษะด้านการสืบสวนสอบสวนอาชญากรรมคอมพิวเตอร์ จำนวน 6 คน
5) นักวิชาการ ผู้มีส่วนได้ส่วนเสีย ที่มีประสบการณ์ หรือได้รับผลกระทบจาก อาชญากรรมคอมพิวเตอร์ในประเทศไทย จำนวน 7 คน

1.5 คำจำกัดความในการวิจัย

พยานหลักฐานดิจิทัล หมายถึง รูปแบบของข้อมูลอิเล็กทรอนิกส์ ที่ถูกจัดเก็บไว้ที่ใดที่หนึ่ง ซึ่งสามารถเข้าถึงได้โดยบางวิธี และกู้คืนได้โดยผู้ตรวจพิสูจน์พยานหลักฐาน และประมวลผลในแง่ของความเชื่อมโยงกับการดำเนินคดีทางแพ่งหรือทางอาญา

กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล หมายถึง การประยุกต์ใช้เทคโนโลยีคอมพิวเตอร์กับปัญหาทางกฎหมายในกรณีที่พยานหลักฐานประกอบด้วยสิ่งที่สร้างขึ้นโดยมนุษย์และสิ่งที่สร้างขึ้นโดยเทคโนโลยีอันเป็นผลมาจากการมีปฏิสัมพันธ์กับมนุษย์ ประกอบด้วยการรวบรวม เก็บรักษา วิเคราะห์ และนำเสนอพยานหลักฐานดิจิทัล

อาชญากรรมคอมพิวเตอร์ หมายถึง อาชญากรรมใดๆ ที่เกี่ยวข้องกับคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์ เป็นการกระทำผิดทางอาญาในระบบคอมพิวเตอร์ หรือใช้คอมพิวเตอร์เพื่อกระทำผิดทางอาญา

อาชญากรรมไซเบอร์ หมายถึง อาชญากรรมคอมพิวเตอร์ ที่มีองค์ประกอบสำคัญอย่างหนึ่งคือเครือข่ายอินเทอร์เน็ต

การป้องกันปราบปรามอาชญากรรม หมายถึง การใช้มาตรการและวิธีการต่างๆ ที่จะไม่ให้เกิดอาชญากรรมขึ้น โดยอาจจำแนกได้คือ การกำจัดต้นเหตุการณ์ ขจัดความปรารถนาที่จะกระทำผิด และขจัดช่วงโอกาสที่จะกระทำผิด

กระบวนการยุติธรรมทางอาญา หมายถึง กระบวนการสำหรับดำเนินคดีอาญา กล่าวคือเมื่อมีการกระทำผิดทางอาญาแล้ว การนำตัวผู้ประทำผิดมาลงโทษจะต้องกระทำอย่างไร บทบัญญัติที่กำหนดวิธีดำเนินคดีอาญา มีอยู่ในประมวลกฎหมายวิธีพิจารณาความอาญา

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1.6.1 เพื่อทราบขั้นตอนของกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลในประเทศไทย และกฎหมายที่เกี่ยวข้อง

1.6.2 เพื่อทราบปัญหาและอุปสรรคของกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลในประเทศไทยในส่วนของกฎหมาย มุมมองของผู้เกี่ยวข้อง ภาคประชาชน และกรณีศึกษา

1.6.3 จัดทำข้อเสนอแนะเชิงนโยบาย ข้อแนะนำสำหรับแต่ละขั้นของกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล ข้อเสนอในการปรับปรุงกฎหมายและการบังคับใช้ เพื่อให้กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลในประเทศไทยสอดคล้องกับมาตรฐานสากล และการป้องกันปราบปรามอาชญากรรมคอมพิวเตอร์ในประเทศไทยมีประสิทธิภาพมากขึ้น

บทที่ 2
แนวคิด ทฤษฎี และเอกสารงานวิจัยที่เกี่ยวข้อง

งานวิจัยเรื่องกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล: การวิเคราะห์เพื่อพัฒนาเชิงนโยบาย ผู้วิจัยได้ทำการศึกษาแนวคิด ทฤษฎี และวรรณกรรมต่างๆ รวมทั้งได้ทบทวนเอกสารงานวิจัยที่เกี่ยวข้อง เพื่อเป็นแนวทางในการวิจัย และกำหนดกรอบแนวคิดที่จะใช้ในการศึกษา ผู้วิจัยได้ศึกษาตามลำดับ ดังนี้

2.1 แนวคิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์
2.2 แนวคิด ทฤษฎีทางอาชญาวิทยาและสังคมวิทยา
2.3 แนวคิด ทฤษฎีเกี่ยวกับกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล
2.4 กฎหมายที่เกี่ยวข้องกับกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล
2.5 งานวิจัยที่เกี่ยวข้อง
2.6 กรอบแนวคิดในการวิจัย

2.1 แนวคิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์

2.1.1 ความหมายของอาชญากรรมและอาชญากรรมคอมพิวเตอร์

อาชญากรรม[5] ได้มีผู้ให้คำนิยามไว้หลากหลาย ทั้งความหมายอย่างกว้าง ซึ่งหมายถึง พฤติกรรมที่มีการกระทำผิด โดยผู้กระทำผิดมีเจตนาในการกระทำดังกล่าว เป็นการกระทำผิดที่มีลักษณะร้ายแรง มีความรุนแรงและเป็นอันตรายต่อสังคม ก่อให้เกิดผลกระทบจำนวนมหาศาลต่อสังคม อันเป็นการกระทำที่มีการละเมิดต่อกฎหมายบ้านเมือง ผู้กระทำผิดจะต้องได้รับโทษทั้งที่ไม่เป็นทางการจากสมาชิกในสังคม อาทิ การตำหนิติเตียน การไม่คบหาสมาคมด้วย และได้รับโทษที่เป็นทางการจากข้อกำหนดของกฎหมายบ้านเมือง โดยผู้กระทำผิดจะต้องถูกลงโทษโดยผ่านกระบวนการยุติธรรมเป็นสำคัญ หรือความหมายอย่างแคบ อาชญากรรม คือ การกระทำที่เป็นความผิดที่ละเมิดต่อกฎหมายที่มีโทษทางอาญา

ประเภทของอาชญากรรมซึ่งเป็นความผิดทางอาญา แบ่งได้หลายประเภท ตามลักษณะการแบ่ง หากแบ่งตามลักษณะความชั่วร้ายแล้ว จะสามารถแบ่งประเภทของความผิดได้เป็น 2 ประเภท คือ

1) ความผิดที่มีความชั่วร้ายในตัวเอง (mala in se) เช่น ปล้น ฆ่า ข่มขืน ทำร้ายร่างกาย ลักทรัพย์
2) ความผิดที่ไม่มีหรือมีความชั่วร้ายน้อย (mala prohibita) เป็นสิ่งที่กฎหมายบัญญัติให้มีความผิด เช่น กฎจราจร หรือความผิดตามพระราชบัญญัติการพนัน

สำหรับนิยามของอาชญากรรมคอมพิวเตอร์ ได้มีผู้ให้คำนิยามไว้ดังนี้

---

[5] “ความหมายของอาชญากรรม”, secnia.go.th, สืบค้นเมื่อ 26 ธ.ค. 60, https://www.secnia.go.th/2016/01/13/ความหมายของอาชญากรรม/

อาชญากรรมคอมพิวเตอร์[6] คือ

1) การกระทำการใดๆ เกี่ยวกับการใช้คอมพิวเตอร์ อันทำให้เหยื่อได้รับความเสียหาย และผู้กระทำได้รับผลประโยชน์ตอบแทน
2) การกระทำผิดกฎหมายใดๆ โดยใช้เทคโนโลยีคอมพิวเตอร์เป็นเครื่องมือ และในการสืบสวนสอบสวนของเจ้าหน้าที่เพื่อนำผู้กระทำผิดมาดำเนินคดีต้องใช้ความรู้ทางเทคโนโลยีเช่นเดียวกัน

ในการประชุมสหประชาชาติครั้งที่ 10 ว่าด้วยการป้องกันอาชญากรรม และการปฏิบัติต่อผู้กระทำผิด ซึ่งจัดขึ้นที่กรุงเวียนนา เมื่อวันที่ 10 - 17 เมษายน พ.ศ. 2543 ได้มีการจำแนกประเภทของอาชญากรรมทางคอมพิวเตอร์ โดยแบ่งเป็น 5 ประเภท คือ การเข้าถึงโดยไม่ได้รับอนุญาต, การสร้างความเสียหายแก่ข้อมูลหรือโปรแกรมคอมพิวเตอร์, การก่อกวนการทำงานของระบบคอมพิวเตอร์หรือเครือข่าย, การยับยั้งข้อมูลที่ส่งถึงจากและภายในระบบหรือเครือข่ายโดยไม่ได้รับอนุญาต และการจารกรรมข้อมูลบนคอมพิวเตอร์

โครงการอาชญากรรมทางคอมพิวเตอร์และการโจรกรรมทรัพย์สินทางปัญญา (Cyber crime and intellectual property theft) พยายามที่จะเก็บรวบรวม เผยแพร่ข้อมูลและค้นคว้าเกี่ยวกับอาชญากรรมคอมพิวเตอร์ 9 ประเภท ซึ่งส่งผลกระทบโดยตรงต่อประชาชน คือ

1) การเงิน – อาชญากรรมที่ขัดขวางความสามารถขององค์กรธุรกิจในการทำธุรกรรมพาณิชย์อิเล็กทรอนิกส์
2) การละเมิดลิขสิทธิ์ – การคัดลอกผลงานที่มีลิขสิทธิ์ ในปัจจุบันคอมพิวเตอร์ส่วนบุคคลและอินเทอร์เน็ตถูกใช้เป็นสื่อในการก่ออาชญากรรมพื้นฐาน โดยการโจรกรรมทางออนไลน์หมายรวมถึง การละเมิดลิขสิทธิ์ ใดๆ ที่เกี่ยวข้องกับการใช้อินเทอร์เน็ตเพื่อจำหน่ายหรือเผยแพร่ผลงานสร้างสรรค์ที่ได้รับการคุ้มครองลิขสิทธิ์
3) การเจาะระบบ – การให้ได้มาซึ่งสิทธิในการเข้าถึงระบบคอมพิวเตอร์หรือเครือข่ายโดยไม่ได้รับอนุญาต และในบางกรณีอาจหมายถึงการใช้สิทธิการเข้าถึงนี้โดยไม่ได้รับอนุญาต นอกจากนี้การเจาะระบบยังอาจรองรับอาชญากรรมทางคอมพิวเตอร์ในรูปแบบอื่นๆ (เช่น การปลอมแปลง การก่อการร้าย ฯลฯ)
4) การก่อการร้ายทางคอมพิวเตอร์ – ผลสืบเนื่องจากการเจาะระบบ โดยมีจุดมุ่งหมายเพื่อสร้างความหวาดกลัวเช่นเดียวกับการก่อการร้ายทั่วไป โดยการกระทำที่เข้าข่ายการก่อการร้ายทางอิเล็กทรอนิกส์ (e-terrorism) จะเกี่ยวข้องกับการเจาะระบบคอมพิวเตอร์เพื่อก่อเหตุรุนแรงต่อบุคคลหรือทรัพย์สิน หรืออย่างน้อยก็มีจุดมุ่งหมายเพื่อสร้างความหวาดกลัว
5) ภาพอนาจารทางออนไลน์ – ตามข้อกำหนด 18 USC 2252 และ 18 USC 2252A การประมวลผลหรือการเผยแพร่ภาพอนาจารเด็กถือเป็นการกระทำที่ผิดกฎหมาย และตามข้อกำหนด 47 USC 223 การเผยแพร่ภาพลามกอนาจารในรูปแบบใดๆ แก่เยาวชนถือ

---

[6] “ความหมาย และอาชญากรคอมพิวเตอร์”, gotoknow.org, สืบค้นเมื่อ 26 ธ.ค. 60, https://www.gotoknow.org/posts/372559

เป็นการกระทำที่ขัดต่อกฎหมาย อินเทอร์เน็ตเป็นเพียงช่องทางใหม่สำหรับอาชญากรรมพื้นฐาน และประเด็นเรื่องวิธีที่เหมาะสมที่สุดในการควบคุมช่องทางการสื่อสารที่ครอบคลุมทั่วโลกและเข้าถึงทุกกลุ่มอายุนี้ ก่อให้เกิดการถกเถียงและการโต้แย้งอย่างกว้างขวาง

6) ภายในโรงเรียน – ถึงแม้ว่าอินเทอร์เน็ตจะเป็นแหล่งทรัพยากรสำหรับการศึกษาและสันทนาการ แต่เยาวชนจำเป็นต้องได้รับทราบเกี่ยวกับวิธีการใช้งานเครื่องมือนี้อย่างปลอดภัยและมีความรับผิดชอบ โดยเป้าหมายหลักของโครงการคือ กระตุ้นให้เด็กได้เรียนรู้เกี่ยวกับข้อกำหนดทางกฎหมาย สิทธิของตนเอง และวิธีที่เหมาะสมในการป้องกันการใช้อินเทอร์เน็ตในทางที่ผิด
7) การหลอกค้าขาย ลงทุนผ่านทางเครือข่ายคอมพิวเตอร์ เช่น การประกาศโฆษณา การชักชวนให้เข้าร่วมลงทุนแต่ไม่ได้มีกิจการเหล่านั้นจริง
8) การแทรกแซงข้อมูลโดยมิชอบโดยการนำเอาข้อมูลเหล่านั้นมาเป็นประโยชน์ต่อตน เช่น การเจาะระบบอินเทอร์เน็ตเข้าไปแอบล้วงความลับทางการค้า การดักฟังข้อมูล เพื่อนำมาเป็นประโยชน์กับกิจการของตนเอง
9) การใช้เทคโนโลยีคอมพิวเตอร์ดัดแปลงข้อมูล โดยการใช้เครือข่ายคอมพิวเตอร์ในการเปลี่ยนแปลงหรือดัดแปลงข้อมูลบัญชีธนาคาร หรือการโอนเงินจากบัญชีเข้าไปอีกบัญชีหนึ่ง โดยที่ไม่ได้มีการเปลี่ยนถ่ายทรัพย์สินกันจริง

นอกเหนือจากนิยามในเชิงเทคนิคแล้ว พิชญ์ พงษ์สวัสดิ์[7] (2560) กล่าวว่า โดยภาพรวมเมื่อพิจารณากฎหมายในประเทศไทย จะพบว่าองค์ประกอบของอาชญากรรมต่อคอมพิวเตอร์เป็นเรื่องที่กว้างขวางครอบคลุมอย่างมากและเกี่ยวพันกับรายละเอียดที่ว่าด้วยประเด็นทางสังคมว่า อะไรบ้างที่ถือเป็นการกระทำความผิดต่อคอมพิวเตอร์ ซึ่งเป็นส่วนหนึ่งของการกระทำผิดต่อบุคคล สังคม และประเทศชาติ และมีนิยามการกระทำความผิดไว้แค่ไหน อย่างไร รวมถึงมีการถกเถียงต่างๆ ในเรื่องของกระบวนการพิจารณาคดี ไม่เพียงแต่ว่า ผิด-ไม่ผิด และขอบเขตอำนาจของคนที่จะเข้าไปตัดสินความผิด มีการพิจารณาอาชญากรรมคอมพิวเตอร์เป็น 3 ระดับ คือ อาชญากรรมที่มีเป้าหมายไปที่ตัวเทคโนโลยี เช่น การเจาะระบบ อาชญากรรมที่มีเป้าหมายไปที่ตัวข้อมูล และการก่อการร้ายไซเบอร์และสงครามไซเบอร์ รวมถึงมีบริบททางสังคมต่างๆ มาเกี่ยวข้อง ไม่ว่าจะเป็นการเข้าถึงระบบโดยไม่ได้รับอนุญาตในลักษณะของปัจเจกชน หรือการกระทำโดยมีจุดมุ่งหมายทางการเมือง และตั้งประเด็นว่า แค่ไหนถึงจะเรียกว่าเป็นความผิด ถ้าเทียบกับการชุมนุมประท้วงที่ได้รับการรับรองทางกฎหมาย

กล่าวโดยสรุป อาชญากรรมคอมพิวเตอร์จึงหมายถึง อาชญากรรมใดๆ ที่เกี่ยวข้องกับคอมพิวเตอร์ เทคโนโลยีคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์ เป็นการกระทำผิดทางอาญาในระบบคอมพิวเตอร์ หรือใช้คอมพิวเตอร์เพื่อกระทำผิดทางอาญา เช่น เปลี่ยนแปลง ทำลาย หรือขโมยข้อมูลต่างๆ โดยไม่ได้รับอนุญาต สำหรับอาชญากรรมในเครือข่ายคอมพิวเตอร์ เช่น

อินเทอร์เน็ต อาจเรียกได้อีกอย่างว่า อาชญากรรมไซเบอร์ (Cybercrime) โดยอาชญากรรมคอมพิวเตอร์สามารถเป็นทั้งอาชญากรรมที่มีทั้งความผิดหรือความชั่วร้ายในตัวเอง เช่น การขโมยข้อมูล หรืออาชญากรรมที่ไม่มีความชั่วร้ายในตัวเอง เป็นสิ่งที่กฎหมายบัญญัติให้มีความผิด และยังมีอาชญากรรมพื้นฐานต่างๆ ที่เกี่ยวเนื่องกับคอมพิวเตอร์ แต่ไม่ถือเป็นอาชญากรรมคอมพิวเตอร์โดยตรงอีกเช่นกัน

2.1.2 ความเป็นมาของอาชญากรรมคอมพิวเตอร์[8]

จากอดีตเรื่อยมาจนถึงยุคของ “อาชญากรรมในเครือข่ายคอมพิวเตอร์” (Cybercrime) หรือ “อาชญากรรมอินเทอร์เน็ต” (Internet crime) ในปัจจุบัน

1) การกระทำความผิดต่อ “สิทธิความเป็นส่วนตัว และข้อมูลส่วนบุคคล” แม้ที่สุดแล้วจนถึงปัจจุบัน จะยังไม่มีใครสามารถให้คำนิยาม คำว่า “อาชญากรรมคอมพิวเตอร์” ที่ชัดเจน ครอบคลุม และเป็นเอกภาพจนเป็นที่ยอมรับกันในระหว่างประเทศได้ แต่หากกล่าวถึงความหมายโดยทั่วๆ ไปที่ทำให้คนในสังคมเริ่มเข้าใจและตระหนักถึงความเสียหายที่เกิดขึ้นจากอาชญากรรมประเภทนี้แล้ว ความหมายโดยนัยดังกล่าว เริ่มขึ้นเมื่อไม่กี่สิบปีที่ผ่านมานี้เอง ในช่วงระยะเวลาที่ข้อมูลชีวิตของมนุษย์จำนวนหนึ่งถูกควบคุม หรือตกอยู่ภายใต้การทำงานของเทคโนโลยีคอมพิวเตอร์ ทศวรรษที่ 60 (ช่วงปี ค.ศ. 1960-1969) นับเป็นช่วงเวลาแรกๆ ที่เริ่มมีความพยายามในการชี้ให้เห็นถึงภยันตรายจากการกระทำความผิดทางคอมพิวเตอร์ ทั้งนี้ด้วยในสมัยนั้นหลายประเทศในแถบตะวันตกใช้คอมพิวเตอร์เป็นอุปกรณ์ในการเก็บบันทึก ถ่ายทอด และเชื่อมโยงฐานข้อมูลส่วนบุคคลของประชาชนในรัฐเข้าด้วยกัน และด้วยเหตุที่มีการนำข้อมูลต่างๆ เหล่านี้ไปรวบรวมไว้ภายใต้การจัดการของรัฐนี้เอง นักวิชาการจำนวนหนึ่งจึงเริ่มอภิปรายถกเถียงถึงประเด็นปัญหาที่ประชาชนอาจถูกตรวจสอบ เฝ้ามอง หรือควบคุมจากรัฐได้ โดยข้อถกเถียงทั้งหลาย ได้รับอิทธิพลมาจากหนังสือของ จอร์จ ออร์เวลล์ (George Orwell) ชื่อ “1984” อันเป็นหนังสือด้านการเมือง การปกครอง แต่มีเนื้อหาส่วนหนึ่งที่ออร์เวลล์กล่าวถึงพัฒนาการทางเทคโนโลยีข้อมูลข่าวสาร พร้อมๆ กับชี้ให้เห็นว่าแม้ในช่วงเวลาเริ่มต้นกระบวนทัศน์ (Paradigm) ของมนุษย์ที่มีต่อคอมพิวเตอร์ คือ อุปกรณ์ หรือเครื่องมือทรงพลังที่มีประโยชน์ต่อระบบการจัดการข้อมูลอย่างสูง ที่จะทำให้การทำงานต่างๆ ของมนุษย์สะดวกและรวดเร็วขึ้น แต่ในอนาคตการใช้เทคโนโลยีและเครื่องมือชนิดนี้ โดยเฉพาะอย่างยิ่งโดยรัฐจะเริ่มล้ำเส้นและเกินขอบเขตความเป็นส่วนตัวของประชาชน หรือจะถูกใช้เป็นเครื่องมือในการควบคุมตรวจสอบพฤติกรรมพลเมืองโดยผู้ปกครองรัฐมากขึ้นเรื่อยๆ และด้วยเหตุที่ในยุคสมัยนั้น คุณประโยชน์หลักๆ ของเครื่องคอมพิวเตอร์ยังจำกัดอยู่เพียงแค่การเก็บบันทึก ประมวลผล หรือเชื่อมต่อข้อมูลต่างๆ ของประชาชนในประเทศเท่านั้น ความเข้าใจที่มีต่อการกระทำความผิดโดยมีคอมพิวเตอร์เข้าไปเกี่ยวข้อง

---

[7] “อาชญากรรมคอมพิวเตอร์ แฮกเกอร์ แฮกติวิสต์?”, matichon.co.th, สืบค้นเมื่อ 26 ธ.ค. 60, https://www.matichon.co.th/news-monitor/news_413499

[8] “รายงาน การวิจัยเพื่อพัฒนากระบวนการสืบสวนและสอบสวนของเจ้าหน้าที่ตำรวจในการรับมือกับอาชญากรรมคอมพิวเตอร์”, research.police.go.th, สืบค้นเมื่อ 26 ธ.ค. 60, http://research.police.go.th/index.php/datacenter/research/2558/-2559-1/342---67/file

ในยุคสมัยแรกๆ จึงยังไม่ได้มีความหมายทำนองเดียวกับ “อาชญากรรมคอมพิวเตอร์” ที่เราเข้าใจกันในปัจจุบัน แต่หมายถึง การกระทำความผิดใดๆ ที่เป็นอันตรายต่อข้อมูลข่าวสาร และระดับความลับหรือความเป็นส่วนตัวที่มนุษย์แต่ละคนอาจไม่ได้ต้องการเปิดเผยให้ผู้อื่นได้รับรู้ ดังนั้น สิ่งสำคัญที่คนเริ่มให้ความสนใจและเรียกร้องให้รัฐต้องให้ความคุ้มครองเป็นพิเศษ ก็คือ “ข้อมูลส่วนบุคคล” และข้อมูลข่าวสารที่มีความสำคัญที่รัฐควรต้องให้ความคุ้มครองอย่างมาก ก็คือความลับในทางวิชาชีพต่างๆ โดยเฉพาะอย่างยิ่ง ข้อมูลทางการแพทย์ ความลับทางราชการ ข้อมูลทางการเงินการธนาคาร หรือข้อมูลทางด้านคดีความ เป็นต้น แต่เพราะในช่วงระยะหลังๆ จากการเก็บสถิติการกระทำความผิดที่เกิดขึ้นในหลายๆ ประเทศพบว่าการกระทำความผิดต่อ “ข้อมูลข่าวสาร” ที่ได้รับความคุ้มครองตามกฎหมาย อันมีผลกระทบต่อประโยชน์ของปัจเจกชนมีจำนวนไม่มากนัก เราจึงมักไม่ค่อยได้ยินว่า “ข้อมูลส่วนบุคคล” เป็นเป้าหมายสำคัญที่รัฐต้องเฝ้าระวังป้องกันเป็นพิเศษจากการกระทำความผิดทางคอมพิวเตอร์ อย่างไรก็ตาม คดีการกระทำความผิดต่อข้อมูลข่าวสารที่เกิดขึ้นมักมีระดับของภยันตรายที่แตกต่างกันไป ขึ้นอยู่กับว่าข้อมูลที่ถูกละเมิดนั้นเป็นของใครหรือหน่วยงานใด เช่น การจารกรรมข้อมูลข่าวสารที่เกี่ยวกับระบบความปลอดภัยของรัฐอันตรายที่เกิดขึ้นอาจกว้างกว่าการขโมยข้อมูลส่วนบุคคลบางอย่าง เพื่อผู้กระทำความผิดจะนำไปใช้ในการข่มขู่ หรือรีดไถจากเจ้าของข้อมูล

2) อาชญากรรมเศรษฐกิจ แม้ในปัจจุบันอาชญากรรมคอมพิวเตอร์ที่เกิดขึ้นในหลายๆ กรณีเป็นความผิดในกลุ่มอื่นที่มีผลกระทบต่อชีวิต ระบบรักษาความปลอดภัย หรือเป็นอันตรายต่อสังคมซึ่งอาจไม่ได้เกี่ยวพันกับปัญหาในทางเศรษฐกิจเลยก็ตาม แต่ในยุคสมัยหนึ่ง “อาชญากรรม” หรือ “การกระทำความผิด” อันมีคอมพิวเตอร์เข้าไปเกี่ยวข้องนี้ ได้เคยถูกขึ้นบัญชีให้อยู่ในกลุ่มของ “อาชญากรรมทางเศรษฐกิจ“ หรือที่รู้จักกันในนาม “White collar crimes” อาชญากรรมคอปกขาว ที่ผู้กระทำความผิดเป็นกลุ่มคนทำงานที่แต่งตัวดี หรือมีความรู้ความสามารถเท่านั้น ความหมายของ อาชญากรรมทางเศรษฐกิจค่อนข้างกว้าง ครอบคลุมความผิดหลายอย่าง เป็นการกระทำที่สร้างความเสียหายทั้งแก่เศรษฐกิจของปัจเจกชน และประเทศชาติสังคมส่วนรวม มีลักษณะของการทำลายความเชื่อถือ ความมั่นคงทางเศรษฐกิจ ตัวอย่างอาชญากรรมเศรษฐกิจ เช่น ความผิดเกี่ยวกับการปลอมแปลงเงินตรา, การปั่นหุ้น, ความผิดเกี่ยวกับภาษีอากร, เกี่ยวกับธุรกิจต่างๆ , สถาบันการเงิน เกี่ยวกับการค้า หรือธุรกิจเงินกู้นอกระบบ เป็นต้น ทศวรรษที่ 70 (ช่วงปี ค.ศ. 1970-1979) การอภิปรายเพื่อแก้ไขปัญหาการกระทำความผิดทางคอมพิวเตอร์ ไม่ได้จำกัดขอบเขตให้อยู่ที่ประเด็นการกระทำความผิดต่อข้อมูลข่าวสารส่วนบุคคลอีกต่อไป แต่รัฐเริ่มหันมาให้ความสนใจในประเด็นปัญหา “อาชญากรรมทางเศรษฐกิจ” มากขึ้น (ซึ่งจนถึงปัจจุบันประเด็นดังกล่าว ก็ยังคงเป็นปัญหาข้อหลักๆ ของอาชญากรรมคอมพิวเตอร์อยู่) ทั้งนี้ ก็เนื่องมาจากรัฐพบว่า สถิติการกระทำความผิดทางคอมพิวเตอร์ที่เกิดขึ้น และส่งผลกระทบต่อเศรษฐกิจโดยรวมของประเทศ โดยเฉพาะอย่างยิ่งในกลุ่มธุรกิจการเงิน เพิ่มจำนวนสูงขึ้นจนน่าวิตก หลังจากปี ค.ศ. 1969 ที่เทคโนโลยีอินเทอร์เน็ตเกิดขึ้นครั้งแรก และได้รับการพัฒนาเรื่อยมา จนอินเทอร์เน็ตกลายเป็นส่วนสำคัญในการทำงานในหน่วยงานของรัฐ รวมทั้งผู้ประกอบธุรกิจรายใหญ่ๆ ของประเทศ ในขณะที่เทคโนโลยีชนิดนี้สร้างความสะดวก และความเป็นอิสระในการแลกเปลี่ยนข้อมูลข่าวสารระหว่างผู้ประกอบธุรกิจทั้งหลาย โดยไม่จำเป็นต้องเดินทางไปพบกันโดยตรง แต่ในอีกด้านหนึ่งก็กลายเป็นประโยชน์สำหรับผู้กระทำความผิดที่ต้องการ

จารกรรม หรือลักลอบทำซ้ำข้อมูลเหล่านั้นไปใช้ประโยชน์ทางธุรกิจของตน หรือสร้างความเสียหายทางด้านการเงินต่อธุรกิจของผู้อื่น จากที่สมัยเดิม “อาชญากรรมเศรษฐกิจ” ไม่ได้มีเครื่องมือพิเศษเพื่อเพิ่มศักยภาพในการกระทำความผิด และมักเป็นเพียงแค่การปลอมแปลง หรือการกระทำต่อเอกสารบัญชี การเงินการธนาคาร และเอกสารอื่นๆ เท่านั้น อาชญากรรมเศรษฐกิจรูปแบบใหม่ที่มีเทคโนโลยีคอมพิวเตอร์ และเครือข่ายอินเทอร์เน็ตเข้ามาเกี่ยวข้องสามารถขยายขอบเขตไปสู่การสร้างความเสียหายต่อเศรษฐกิจในด้านอื่นๆ ด้วยก็เริ่มปรากฏตัวในยุคนี้เอง มีการจำแนกอาชญากรรมคอมพิวเตอร์ ออกเป็นสองกลุ่มใหญ่ คือ กลุ่มความผิดที่ผู้กระทำอาศัยคอมพิวเตอร์เป็น “เครื่องมือ” และ กลุ่มความผิดที่ระบบคอมพิวเตอร์ และข้อมูลที่อยู่ในคอมพิวเตอร์เป็น “เป้าหมาย” ของผู้กระทำความผิด ความผิดสำคัญๆ ที่เกิดขึ้นบ่อยครั้งและได้รับความสนใจจากนักกฎหมาย และนักวิชาการด้านอื่นๆ ด้วย ได้แก่ การเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ (Computer manipulation), การก่อวินาศกรรมคอมพิวเตอร์ (Computer sabotage) หรือการกรรโชก รีดไถทางคอมพิวเตอร์, การเข้าไปในระบบคอมพิวเตอร์โดยปราศจากอำนาจ หรือการเจาะระบบ (Hacking) และการละเมิดลิขสิทธิ์ซอฟต์แวร์ รวมทั้งการลักลอบขโมยผลิตภัณฑ์ที่มีลิขสิทธิ์ต่าง ๆ เช่น เพลง หรือภาพยนตร์

2.1) การกระทำความผิดด้วยการหลอกลวง โดยอาศัยวิธีการเปลี่ยนแปลงข้อมูลคอมพิวเตอร์แม้ในสมัยนั้น (ช่วงทศวรรษที่ 70) การกระทำความผิดแบบนี้จะหมายถึงเฉพาะที่กระทำต่อระบบคอมพิวเตอร์ หรือข้อมูลที่อยู่ในคอมพิวเตอร์ตัวหลักเท่านั้น แต่เนื่องจากในสมัยต่อๆ มา (ช่วงทศวรรษที่ 80) จนถึงปัจจุบันระบบคอมพิวเตอร์ได้รับการพัฒนาเพื่อใช้งานร่วมกับเครื่องมืออื่นๆ ที่มีความหลากหลายมากขึ้น ดังนั้น ประเภทของความผิดที่เกิดจากการกระทำในรูปแบบนี้จึงถูกจำแนกเพิ่มขึ้นด้วย

- การเปลี่ยนแปลงข้อมูลคอมพิวเตอร์แบบดั้งเดิม เป้าหมายหลักๆ ของผู้กระทำความผิดยังคงอยู่ที่บัญชีด้านการเงินการธนาคารของบริษัท และผู้ประกอบธุรกิจต่างๆ อาทิ การกระทำความผิดด้วยการเปลี่ยนแปลง หรือบิดเบือนข้อมูลการชำระเงิน การเปลี่ยนแปลงรายรับ-รายจ่ายของบริษัท, การเปลี่ยนแปลงงบดุลบัญชีบริษัท, การเปลี่ยนแปลงรายการ หรือ สถานภาพการเงินของธนาคาร รวมทั้งการเปลี่ยนแปลงระบบ “บัญชีเงินสะสม” ของบริษัทต่าง ๆ ก็เกิดขึ้นเป็นจำนวนมาก ในระยะหลังๆ คดีใหญ่ๆ ที่เคยเกิดขึ้นมาแล้ว ก็เช่น คดีในประเทศเยอรมนี ปี ค.ศ. 1974 โปรแกรมเมอร์ของบริษัทแห่งหนึ่งได้ทำการตกแต่งบัญชีและบิดเบือนรายรับของบริษัท ยักยอกเงินไปได้กว่า 193,000 ดอยช์มาร์ค และในปีเดียวกัน ธนาคาร Herstatt ประเทศเยอรมนี ถูกเปลี่ยนแปลงข้อมูลด้านงบดุลบัญชี จนต้องสูญเสียเงินไปกว่า 1 ล้านดอยช์มาร์ค หรืออย่างคดีที่เกิดขึ้นเมื่อปี ค.ศ. 1994 โดยกลุ่มผู้กระทำความผิดชาวรัสเซียร่วมกันเปลี่ยนแปลงบัญชีของโบสถ์แห่งหนึ่งจนได้รับโอนเงินจากธนาคารประเทศสหรัฐอเมริกาจำนวนกว่า 10 ล้านเหรียญดอลลาร์สหรัฐ เป็นต้น
- ในช่วงกลางของทศวรรษที่ 80 การเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ในลักษณะของการกระทำความผิดต่อเครื่องเบิกเงินอัตโนมัติหรือตู้เอทีเอ็ม รวมทั้งบัตรชำระเงินหรือบัตรเครดิตประเภทต่างๆ เริ่มเกิดขึ้นและขยายตัว แม้โดยปกติแล้ว การกระทำความผิดที่เกี่ยวกับบัตรจ่ายเงินเหล่านี้ในแต่ละครั้งจะสร้างความเสียหายต่อเหยื่อไม่มากนัก เพราะ

ผู้กระทำความผิดมักได้เงินไปเพียงเล็กน้อย แต่จากสถิติการกระทำความผิดพบว่า การเปลี่ยนแปลงข้อมูลคอมพิวเตอร์รูปแบบนี้เกิดขึ้นบ่อยกว่าการเปลี่ยนแปลงข้อมูลคอมพิวเตอร์แบบดั้งเดิมหลายเท่าตัว จึงนับเป็นความผิดสำคัญที่รัฐต้องให้ความสนใจมากพอๆกัน วิธีการกระทำความผิดที่ผ่านมา มีตั้งแต่ การขโมยบัตรชำระเงินจากเหยื่อแล้วใช้เทคนิคในการสุ่มหมายเลขเพื่อเบิกเงิน, ขโมยบัตรมาเปลี่ยนแปลงรหัสโดยใช้คอมพิวเตอร์ก่อนแล้วจึงนำไปเบิกเงินจากเครื่องเอทีเอ็ม ไปจนถึงการติดตั้งเครื่องมือดักรหัสลับไว้ที่ตู้เบิกเงิน หรือใช้เครื่องดักฟังระยะไกลเพื่อบันทึกรหัสลับของผู้เสียหาย

- ปลายทศวรรษที่ 80 ขอบเขตการกระทำความผิดการเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ ก็พัฒนากว้างขวางยิ่งขึ้นอีก ธุรกิจบริการรูปแบบอื่นๆ ไม่เฉพาะการเงินการธนาคารเริ่มตกเป็นเป้าหมายของผู้กระทำความผิด โดยเฉพาะอย่างยิ่งการกระทำความผิดเกี่ยวกับบริการโทรศัพท์ผ่านเครือข่ายอินเทอร์เน็ต แม้ในอดีตที่ผ่านมา (ช่วงทศวรรษที่ 60) การลักลอบใช้บริการโทรศัพท์จะเกิดขึ้นมาก่อนแล้ว แต่ผู้กระทำความผิดส่วนใหญ่มักกระทำไปเพียงเพื่อประหยัดค่าโทรศัพท์กับเครื่องโทรศัพท์ส่วนบุคคล หรือโทรศัพท์ในระบบธรรมดาเท่านั้น เทคนิคที่นิยมในสมัยนั้น เรียกว่าวิธี “Blue boxing” มีเครื่องมือที่เรียกว่า “Blue box” ใช้ในการตัดและควบคุมช่องส่งสัญญาณเสียงเพื่อจะได้แทรกเข้าไปใช้บริการได้โดยไม่เสียเงิน หมายเลขโทรศัพท์ที่มักถูกโจมตี มักเป็นหมายเลขโทรศัพท์ที่ให้บริการฟรี เพื่อติดต่อหน่วยงานประชาสัมพันธ์ของบริษัทต่างๆ อย่างไรก็ตามด้วยวิธีการดังกล่าว ยังสามารถใช้ได้เฉพาะกับบริการโทรศัพท์ภายในประเทศเท่านั้น แต่นับจากที่นักเจาะระบบโทรศัพท์ ได้คิดค้นวิธีการลักลอบใช้โทรศัพท์ในระบบต่างๆ ทั้งจากบริษัท รวมทั้งระบบโทรศัพท์ทางไกลข้ามประเทศ แล้วนำวิธีการนั้นมาเผยแพร่ การกระทำความผิดรูปแบบนี้ก็ขยายตัวอย่างรวดเร็ว จนในช่วงทศวรรษที่ 90 เป็นต้นมา ธุรกิจการให้บริการโทรศัพท์ ก็กลายเป็นเป้าหมายใหญ่ของบรรดาผู้กระทำความผิด โดยเฉพาะอย่างยิ่ง บริษัทผู้ให้บริการโทรศัพท์ที่มีการวางระบบรักษาความปลอดภัยหรือเฝ้าระวังการลักลอบใช้บริการไม่ดีพอ ปัจจุบันการกระทำความผิดในกลุ่มนี้ ผู้กระทำความผิดอาจใช้วิธีเปลี่ยนแปลง ยักย้ายรายการหรือบัญชีการใช้โทรศัพท์ของตนให้กลายเป็นของผู้ใช้บริการโทรศัพท์ทางอินเทอร์เน็ตคนอื่น วิธีเจาะระบบคอมพิวเตอร์ของผู้ให้บริการจดหมายเสียงที่มีระบบการป้องกันไม่แน่นหนาพอ เพื่อแอบใช้บริการหรือใช้วิธีดักรับ หรือหลอกลวง บริษัทผู้ให้บริการเพื่อขอรหัสการ์ดโทรศัพท์ของผู้ใช้บริการรายอื่น เป็นต้น

2.2) การก่อวินาศกรรมอินเทอร์เน็ต และการข่มขู่ทางอินเทอร์เน็ต

- กล่าวได้ว่า การก่อวินาศกรรมคอมพิวเตอร์ จนถึงปัจจุบันก็ยังจัดอยู่ในกลุ่มการกระทำความผิดที่เกิดขึ้นแพร่แหลาย เช่นเดียวกับการเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ อย่างไรก็ตามจากสถิติการกระทำความผิดพบว่า ความผิดส่วนใหญ่ที่เกิดขึ้น มักเป็นการกระทำต่อคอมพิวเตอร์ส่วนบุคคล ด้วยวิธีปล่อยโปรแกรมไวรัส หรือวอร์ม ทำลายระบบ หรือ

ข้อมูลคอมพิวเตอร์เท่านั้น ส่วนการก่อวินาศกรรมที่สร้างความเสียหายกับบริษัทใหญ่ๆ มีจำนวนไม่มากนัก การกระทำความผิดในลักษณะนี้ เริ่มขยายตัวมากขึ้นภายหลังจากระบบเครือข่ายคอมพิวเตอร์ได้รับการพัฒนา ทั้งนี้เพราะผู้กระทำความผิด เขียนโปรแกรมทำลายแค่เพียงครั้งเดียว แต่สามารถส่งต่อ เผยแพร่ สร้างความเสียหายให้เหยื่อได้จำนวนมาก ไวรัสที่มีเป้าหมายในการทำลายล้าง หรือเพื่อก่อวินาศกรรมตัวแรกถูกสร้างขึ้นในราวปี ค.ศ. 1986 ในชื่อ “Brain” โดยไวรัสนี้มีผลต่อ Boot sector ของคอมพิวเตอร์ อย่างไรก็ตาม โปรแกรมไวรัสจำนวนมากและหลากหลายชนิดถูกเขียนขึ้นก่อนหน้าไวรัส “Brain” แล้ว เพียงแต่ยังไม่ได้ถูกนำมาใช้เพื่อเป้าหมายในการโจมตี หรือก่อวินาศกรรมโดยเฉพาะ โดยไวรัสตัวแรกถูกเปิดเผยในงานวิจัยปริญญาเอกของเฟรด โคเฮน (Fred cohen) ตั้งแต่ปี ค.ศ. 1983 สำหรับโปรแกรมวอร์ม ที่เป็นที่รู้จักอย่างกว้างขวางเกิดขึ้นราวปี ค.ศ. 1988 ในชื่อ “The Morris worm” โดยหลังมีการเผยแพร่เพียงไม่กี่วัน สามารถทำลายระบบคอมพิวเตอร์ไปกว่า 6,000 เครื่อง นอกจากโปรแกรมไวรัส และวอร์มแล้ว ปัจจุบันโปรแกรมทำลายอื่นๆ ยังได้รับการพัฒนาออกมาอีกจำนวนมาก อาทิ โทรจัน, Logic bomb หรือ Time bomb เป็นต้น

- การก่อวินาศกรรมคอมพิวเตอร์ นับเป็นการกระทำความผิดที่มีผลกระทบต่อระบบเศรษฐกิจโดยรวมอย่างมาก ทั้งนี้เพราะในยุคสมัยดังกล่าว เทคโนโลยีคอมพิวเตอร์และระบบการสื่อสารผ่านเครือข่ายเริ่มเป็นส่วนสำคัญ ทั้งต่อการประกอบธุรกิจโดยทั่วไปและชีวิตประจำวันของคนในสังคม นอกจากนี้การก่อวินาศกรรมคอมพิวเตอร์ยังนำมาซึ่งความผิดอีกรูปแบบหนึ่งด้วย คือ การข่มขู่ทางอินเทอร์เน็ต เป็นภยันตรายอีกรูปแบบหนึ่ง ที่เกิดขึ้นในช่วงเวลาเดียวกัน ในลักษณะของการข่มขู่ กรรโชก หรือรีดไถเงิน ผู้เสียหายจะถูกข่มขู่ผ่านทางจดหมายอิเล็กทรอนิกส์ หรือเอกสารลับ ให้ต้องยินยอมกระทำการอย่างหนึ่งอย่างใด มิเช่นนั้นระบบคอมพิวเตอร์ส่วนบุคคลจะถูกทำลาย หรือเกิดความเสียหายจนใช้ประโยชน์ไม่ได้ หรือบางกรณี ผู้กระทำผิดจะใช้วิธีเขียนโปรแกรมเข้ารหัสเครื่องคอมพิวเตอร์ของเหยื่อ เพื่อไม่ให้เหยื่อเข้าไปใช้งานได้ จากนั้นจึงข่มขู่ให้เหยื่อจ่ายเงินเพื่อแลกกับการถอดรหัสดังกล่าว เป็นต้น

2.3) การเข้าไปในระบบคอมพิวเตอร์โดยปราศจากอำนาจ หรือ การเจาะระบบ

- สำหรับนิยาม หรือลักษณะของการกระทำความผิดด้วยการเจาะระบบคอมพิวเตอร์หรือการเข้าถึงโดยปราศจากอำนาจ ในช่วงระยะเวลาเริ่มต้นนั้น อาจกล่าวได้ว่าความผิดรูปแบบนี้ในระยะแรกๆ ผู้กระทำส่วนใหญ่ไม่ได้มีเป้าหมายในการกระทำความผิดอย่างอื่น อาทิ เปลี่ยนแปลงข้อมูลเพื่อหลอกลวง ทำลายระบบ หรือจารกรรมข้อมูล ผู้กระทำต้องการเพียงทดลอง หรือทดสอบความสามารถในการฝ่าระบบรักษาความปลอดภัยของผู้อื่นเท่านั้น โดยการเจาะระบบคอมพิวเตอร์นี้ คาดว่าเกิดขึ้นครั้งแรกในราวปี ค.ศ. 1980 โดย เควิน มิตนิค (Kevin mitnick) ซึ่งทำการเจาะเข้าไปในระบบคอมพิวเตอร์ของบริษัท US leasing ความผิดลักษณะนี้เกิดขึ้นบ่อยครั้งทั้งจากนักเจาะระบบมืออาชีพ และแบบสมัครเล่น ความเสียหายจึงอาจแตกต่างกันไป และแม้คดีส่วนใหญ่ที่

เกิดขึ้นจะเป็นกรณีที่สร้างความเสียหายต่อระบบรักษาความปลอดภัยของบริษัท หรือหน่วยงานที่ถูกเจาะระบบเท่านั้น แต่ในหลายคดี ก็สร้างความเสียหายอื่นๆ ตามมาด้วย เมื่อปรากฏว่าผู้เจาะระบบนั้น นำเทคนิควิธีการที่ตนใช้ไปเผยแพร่ต่อยังบุคคลอื่นซึ่งอาจนำไปใช้ในการกระทำความผิดอื่น ๆ ต่อไปอีก

- ดังกล่าวมาแล้วว่า เมื่อเทคโนโลยีด้านนี้ยังได้รับการพัฒนาอย่างต่อเนื่อง รูปแบบการกระทำความผิดก็ย่อมมีการพัฒนาและขยายตัวไปด้วย การเจาะระบบก็เช่นเดียวกัน ปัจจุบันไม่เฉพาะแต่ระบบคอมพิวเตอร์เท่านั้นที่เป็นเป้าหมายของการกระทำความผิด ระบบให้บริการอื่นๆ โดยเฉพาะอย่างยิ่งบริการโทรศัพท์ทางอินเทอร์เน็ต โทรศัพท์ทางไกล บริการจดหมายเสียง ได้กลายเป็นเป้าหมายใหญ่ของนักเจาะระบบ และการเข้าถึงต่างๆ ดังกล่าว ไม่ใช่เป็นเพียงแค่การทำลายระบบป้องกัน หรือระบบรักษาความปลอดภัยอย่างเดียวแบบเดิมๆ แต่ผู้กระทำยังมีเป้าหมาย เพื่อลักลอบใช้บริการเหล่านั้นโดยไม่ต้องเสียเงินอีกด้วย ดังนั้น จากที่แต่เดิมความผิดในฐานความผิดนี้อาจไม่ได้เป็นภัยต่อเศรษฐกิจมากนัก แต่ในปัจจุบันการกระทำดังกล่าว สร้างความเสียหายอย่างกว้างขวางไม่แพ้ความผิดในรูปแบบอื่นๆ เลย

2.4) การจารกรรมทางคอมพิวเตอร์

- แม้จากสถิติการกระทำความผิด การกระทำรูปแบบนี้ไม่ได้เกิดขึ้นบ่อยนักเช่นกัน แต่ถ้าเทียบกับการ “จารกรรมข้อมูลทางเศรษฐกิจ” ด้วยวิธีดั้งเดิมแล้ว จะพบว่าอันตรายและความเสียหายที่เกิดจากการจารกรรมทางคอมพิวเตอร์ มีสูงกว่าอาชญากรรมเศรษฐกิจแบบเดิมๆ หลายเท่าตัว ทั้งนี้เนื่องจากระบบคอมพิวเตอร์ได้กลายเป็นอุปกรณ์หลักในการเก็บบันทึกข้อมูล ดั้งนั้น ทั้งปริมาณและความหลากหลายของข้อมูลจึงมีมหาศาล ประกอบกับความทันสมัยในเรื่องเทคนิควิธีการ ทำให้ผู้กระทำความผิดสามารถค้นหาและทำซ้ำข้อมูลเหล่านั้นได้อย่างรวดเร็วและง่าย โดยไม่จำเป็นต้องมีการเข้าถึงทางกายภาพ วิธีการจารกรรมข้อมูลที่ใช้ จะมีทั้งกรณีเจาะระบบเพื่อเข้าถึงฐานข้อมูลในคอมพิวเตอร์ก่อนแล้วจึงค้นหาเพื่อทำซ้ำ และการใช้เครื่องมือพิเศษเพื่อดักรับข้อมูลในระหว่างการติดต่อสื่อสาร ข้อมูลส่วนใหญ่ที่ตกเป็นเป้าหมายของผู้กระทำในรูปแบบนี้ ได้แก่ โปรแกรมคอมพิวเตอร์, ข้อมูลการศึกษาวิจัย, ความลับทางการทหาร, ข้อมูลการประกอบธุรกิจประเภทบัญชีการเงิน รวมทั้งข้อมูลเกี่ยวกับลูกค้า โดยในระยะหลังที่ผ่านมา การกระทำความผิดรูปแบบนี้ มักเกิดขึ้นกับข้อมูลทางธุรกิจเป็นส่วนใหญ่ ซึ่งคู่กรณีมักเป็นบริษัทคู่แข่งกัน
- เช่นเดียวกับความผิดในรูปแบบอื่นๆ การจารกรรมทางคอมพิวเตอร์ รวมทั้งการใช้เครื่องมือดักรับข้อมูลข่าวสาร ได้ถูกพัฒนาวิธีการและขยายขอบเขตเป้าหมายของการกระทำความผิดไปพร้อมๆ กับวิวัฒนาการทางเทคโนโลยีด้านนี้ เช่น การดักรหัสลับสำหรับใช้บริการต่างๆ ของผู้ใช้อินเทอร์เน็ตรายอื่น เป็นต้น นอกจากนี้ยังปรากฏด้วยว่าหน่วยงานรัฐได้นำวิธีการดังกล่าวมาใช้ร่วมกับการสืบสวนการกระทำความผิด หรือในราชการลับต่างๆ เช่น ดักฟังการสนทนาทางโทรศัพท์ของผู้ต้องสงสัย ทั้งโทรศัพท์ที่

เชื่อมต่อด้วยระบบธรรมดา และด้วยระบบสัญญาณผ่านดาวเทียม จนเกิดข้อถกเถียงโต้แย้งกันว่า การกระทำของรัฐเหล่านั้น หลายครั้งเกินความจำเป็นจนกลายเป็นการล่วงล้ำสิทธิของพลเมืองมากเกินไป โดยเฉพาะอย่างยิ่งในประเทศสหรัฐอเมริกา จากการเปิดเผยรายงานในปี ค.ศ. 1991 พบว่า หน่วยงานรัฐ ดักฟังการสนทนาทางโทรศัพท์ไปกว่า 2,000 ครั้ง ในขณะที่มีการจับตาและควบคุมการสนทนาทางโทรศัพท์ไปกว่า 54,000 ครั้ง

2.5) การขโมย ลักลอกทำซ้ำ หรือใช้ซอฟต์แวร์ หรือผลิตภัณฑ์อื่นๆ โดยไม่ได้รับอนุญาต

- การกระทำความผิดในฐานความผิดนี้ ในระยะแรกมักมีเป้าหมายอยู่ที่ “ซอฟต์แวร์เฉพาะทาง” (Individual software) เป็นส่วนใหญ่ เนื่องจากในระยะนั้นยังมีหน่วยงานจำนวนไม่มากที่สามารถลงทุนกับเครื่องคอมพิวเตอร์และโปรแกรมใช้งานได้ โปรแกรมใช้งานพื้นฐานอื่นๆ ยังไม่ค่อยได้รับการพัฒนา โปรแกรมส่วนใหญ่ที่ผลิตออกมาจึงเป็นโปรแกรมที่ถูกเขียนขึ้นตามความต้องการของผู้ว่าจ้างเป็นรายๆ ไปโดยไม่มีจำหน่ายในตลาดปกติ คดี “Inkasso-programm” เป็นคดีแรกที่ได้รับการตัดสินจากศาลประเทศเยอรมนี ให้ผู้ลักลอบทำซ้ำต้องรับผิดในฐานละเมิดลิขสิทธิ์โปรแกรมคอมพิวเตอร์ อย่างไรก็ตาม ภายหลังที่ความต้องการในการใช้คอมพิวเตอร์โดยบุคคลทั่วไปเพิ่มมากขึ้น เป้าหมายของการกระทำความผิดลักษณะนี้จึงเปลี่ยนไปที่ “โปรแกรมการใช้งานพื้นฐาน” (Standard software) แทน โดยเฉพาะอย่างยิ่งโปรแกรมสำหรับใช้งานด้านต่างๆ ในเครื่องคอมพิวเตอร์ส่วนบุคคล ทั้งนี้เพราะโปรแกรมใช้งานดังกล่าว ในช่วงต้นๆ ของการพัฒนา เกือบทั้งสิ้นเป็นโปรแกรมมีลิขสิทธิ์ที่จำหน่ายในราคาสูง ผู้ใช้ส่วนหนึ่งที่มีความสามารถทางคอมพิวเตอร์ แต่ไม่ต้องการเสียเงินจำนวนมาก จึงพยายามหาวิธีในการลักลอบทำซ้ำมาใช้แทน การกระทำความผิดรูปแบบนี้ ส่งผลกระทบต่อบริษัทผู้ผลิตซอฟต์แวร์จำนวนมาก ในปัจจุบันนอกจากการลักลอบทำซ้ำเพื่อใช้ประโยชน์ส่วนบุคคลแล้ว ยังมีการนำมาวางจำหน่ายในราคาต่ำกว่าซอฟต์แวร์ของจริงด้วย ดังที่รู้จักกันในชื่อของ “ซอฟต์แวร์เถื่อน” หรือ “ซอฟต์แวร์ผิดกฎหมาย” เคยมีรายงานว่าตลาดด้านนี้ในประเทศสหรัฐอเมริกา มีซอฟต์แวร์เถื่อนขายอยู่ราว 40%, ประเทศเยอรมัน 76%, ประเทศญี่ปุ่น 81% และประเทศไทยมีถึง 98% ดังนั้นความเสียหายที่เกิดขึ้นกับบริษัทผู้ผลิตโปรแกรมเหล่านี้จึงมีค่อนข้างสูง และมีแนวโน้มสูงขึ้นอีกในอนาคต นอกจากนั้น ในช่วงไม่กี่ปีนี้ยังมีการพัฒนาเปลี่ยนแปลงรูปแบบของการกระทำความผิดจากเดิมไปอีก จากที่ในช่วงหนึ่ง (กลางทศวรรษที่ 80) ธุรกิจขายซอฟต์แวร์เถื่อนลดลงอย่างมาก อันเป็นผลจากการไล่ติดตามจับกุมผู้ขายอย่างจริงจัง แต่ต่อมากลุ่มผู้กระทำความผิดได้พัฒนารูปแบบวิธีการขายไป อาทิ มีการเสนอขายผ่านทางเว็บไซต์ หรืออีเมล ทั้งตัวซอฟต์แวร์เถื่อนเอง และเครื่องมือในการทำซ้ำ, พ่อค้าหรือผู้ขายสามารถทำซ้ำได้ด้วยตนเอง เพราะมีเครื่องมือที่ทันสมัย รวมทั้งมีบ่อยครั้งที่ผู้จำหน่ายฮาร์ดแวร์นำซอฟต์แวร์เถื่อนเหล่านั้นมาขายพร้อมกัน หรือให้ฟรีกับลูกค้าด้วย อย่างไรก็ตามมีการคาดไว้เช่นกันว่า หลังจากที่ซอฟต์แวร์ฟรี หรือ ซอฟต์แวร์ Open source ต่างๆ เริ่ม

ได้รับการพัฒนามากขึ้น และได้รับความนิยมเพิ่มขึ้น ที่สุดแล้วการกระทำความผิดที่มีเป้าหมายอยู่ที่ “โปรแกรมการใช้งานคอมพิวเตอร์” จะลดจำนวนลงไปได้เอง

- “มูลค่า” ที่เพิ่มสูงขึ้นของข้อมูลทั้งหลายในยุคข้อมูลข่าวสาร เป็นสาเหตุหนึ่งที่จูงใจให้เกิดการพัฒนาวิธีการกระทำความผิด และขยายขอบเขตเป้าหมายของการกระทำออกไปมากยิ่งขึ้น เพราะในระยะต่อมานอกจากการลักลอบใช้ “โปรแกรมคอมพิวเตอร์” โดยไม่ได้รับอนุญาตจะมีเพิ่มมากขึ้นแล้ว ข้อมูลประเภทอื่น ๆ อาทิ ข้อมูลทางธุรกิจ ข้อมูลลูกค้า เพลง ภาพยนตร์ เกมคอมพิวเตอร์ ฯลฯ ก็ถูกลักลอบทำซ้ำเพื่อนำมาจำหน่ายต่อด้วยเช่นกัน โดยแหล่งที่มาหรือฐานข้อมูลที่ถูกลักลอบดาวน์โหลดโดยไม่ได้รับอนุญาตดังกล่าว มีทั้งแหล่งข้อมูลประเภทออนไลน์และฐานข้อมูลออฟไลน์ด้วย โดยสรุปนับตั้งแต่ทศวรรษที่ 70 เป็นต้นมา จะเห็นได้ว่าเมื่อกล่าวถึง “อาชญากรรมคอมพิวเตอร์” ในสมัยที่อยู่ในนิยามของคำว่า “อาชญากรรมทางเศรษฐกิจ” แล้ว สิ่งสำคัญที่กฎหมายประสงค์จะคุ้มครองเป็นพิเศษ ได้ขยายจาก “ข้อมูลส่วนบุคคลและสิทธิความเป็นส่วนตัว” ไปสู่ “เศรษฐกิจโดยรวม” ของประเทศ ทั้งนี้ เนื่องมาจากในยุคสมัยดังกล่าว ระบบคอมพิวเตอร์และเทคโนโลยีสารสนเทศ เริ่มมีความสำคัญและถูกนำไปใช้ในการประกอบกิจการหรือทำธุรกิจต่างๆ มากขึ้น ไม่เฉพาะข้อมูลส่วนบุคคลของ

  ปัจเจกชน หรือประชาชนพลเมืองของรัฐเท่านั้นที่ถูกบันทึก หรือผูกติดอยู่กับเทคโนโลยี แต่ข้อมูลหลากหลายประเภท โดยเฉพาะข้อมูลทางด้านการเงินการบัญชี ลูกค้า ผลิตภัณฑ์ดิจิตอล โปรแกรม เกม เพลง ภาพยนตร์ ฯลฯ ล้วนแล้วแต่มีคอมพิวเตอร์เป็นเครื่องมือสำคัญในการเก็บบันทึกและประมวลผล และด้วยสถานการณ์ดังกล่าวนี้เอง เมื่อผนวกกับความก้าวหน้าและศักยภาพในการเชื่อมโยงข้อมูลเข้ากับเทคโนโลยีเครือข่ายคอมพิวเตอร์ และการขยายตัวอย่างรวดเร็วของอินเทอร์เน็ต เครื่องมือต่างๆ ในการกระทำความผิดได้รับการพัฒนามากขึ้น วิธีการและเป้าหมายแห่งการกระทำความผิดจึงเปลี่ยนแปลงไป และสามารถสร้างความเสียหายในวงกว้างได้ในช่วงระยะเวลาเพียงไม่กี่ปี

3) การเผยแพร่เนื้อหาข้อมูลที่ไม่ชอบด้วยกฎหมาย กับ อาชญากรรมไซเบอร์ นับจากทศวรรษที่ 90 เรื่อยมาจนถึงปัจจุบัน การกระทำความผิดที่อยู่ในความหมายของคำว่า “อาชญากรรมคอมพิวเตอร์” ไม่ได้จำกัดอยู่แต่เฉพาะการละเมิดข้อมูลส่วนบุคคล โดยนัยของการกระทำความผิดที่มีคอมพิวเตอร์เข้ามาเกี่ยวข้องในระยะแรกๆ หรือเฉพาะการละเมิดทรัพย์สินที่ก่อให้เกิดความเสียหายต่อเศรษฐกิจ โดยนัยแห่ง “อาชญากรรมทางเศรษฐกิจ” เท่านั้น แต่ยังรวมความไปถึงการกระทำความผิดต่อสิ่งที่กฎหมายประสงค์จะคุ้มครองในด้านอื่นๆ ผ่านบริการต่างๆ บนอินเทอร์เน็ตด้วย ความผิดสำคัญที่เริ่มปรากฏขึ้นในยุคหลังการแพร่หลายของอินเทอร์เน็ตเรื่อยมาจนถึงปัจจุบัน ได้แก่ การเผยแพร่ข้อมูลที่ไม่ชอบด้วยกฎหมาย ในแง่มุมต่าง ๆ อาทิ ภาพลามกอนาจารเด็ก, การพนัน, การจำหน่ายอาวุธ หรือ เผยแพร่ข้อมูลที่มีเนื้อหาแอบแฝงแนวคิดก้าวร้าว รุนแรง หรือแนวคิดในการดูหมิ่นสถาบัน ดูหมิ่นชนชาติ การเลือกปฏิบัติ รวมทั้งการหมิ่นประมาทผ่านสื่อบริการต่างๆ บน

เครือข่ายอินเตอร์เน็ต โดยเฉพาะอย่างยิ่งในเครือข่ายสังคม เว็บไซต์ กระดานข่าว จดหมายอิเล็กทรอนิกส์ และห้องสนทนาออนไลน์ เป็นต้น และเพื่อเจาะจงให้ชัดเจนลงไป “อาชญากรรมอินเทอร์เน็ต“ หรือ “อาชญากรรมไซเบอร์” จึงเป็นถ้อยคำที่ถูกคิดขึ้นเพื่ออธิบายการกระทำความผิดในรูปแบบดังกล่าว จากการสำรวจพบว่า เว็บไซต์ที่มีเนื้อหาเกี่ยวกับการดูหมิ่นชนชาติหรือแนวทางนีโอนาซี เกิดขึ้นจำนวนมากในประเทศสหรัฐอเมริกา เช่นเดียวกันในประเทศเยอรมนี แม้เว็บไซต์ที่มีเนื้อหาลักษณะดังกล่าวจะถูกปิดไปจำนวนมาก แต่ก็ยังคงมีการลักลอบเผยแพร่แนวคิดในการต่อต้านแรงงานต่างชาติ ลัทธิซ้ายจัด ขวาจัด ฯลฯ หรือส่งต่อกันทางอีเมลเป็นจำนวนไม่น้อย เท่ากับว่าปัจจุบัน “อาชญากรรมไซเบอร์” ซึ่งเป็นส่วนหนึ่งของ “อาชญากรรมคอมพิวเตอร์” ได้เริ่มขยายขอบเขตและสามารถสร้างความเสียหายต่อประโยชน์สาธารณะหรือส่งผลกระทบต่อ ค่านิยม แนวคิดสังคม รวมทั้งพัฒนาการของเด็ก และเยาวชนด้วย

4) การกระทำความผิดอื่นๆ นอกจากความผิดรูปแบบใหม่ต่างๆ ดังกล่าวมาแล้ว การกระทำความผิดในฐานความผิดดั้งเดิม แต่มีคอมพิวเตอร์เข้าไปเกี่ยวข้องก็เริ่มมีจำนวนมากขึ้น จากสถิติพบว่าการเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ หลายคดีผู้กระทำมิได้มุ่งหมายเพื่อผลประโยชน์ในทางทรัพย์สินหรือสร้างความเสียหายด้านเศรษฐกิจเท่านั้น แต่มีเป้าหมายในการทำร้าย หรือละเมิด ชีวิต ร่างกายของเหยื่อผู้เสียหาย อาทิ การเปลี่ยนแปลงข้อมูลการรักษา หรือแก้ไขรายการให้ยาผู้ป่วยในฐานข้อมูลของโรงพยาบาล, การทำลายระบบรักษาความปลอดภัย หรือข้อมูลการบินของอากาศยาน เป็นต้น อีกทั้งในปัจจุบัน เทคโนโลยีคอมพิวเตอร์ยังถูกนำมาใช้เพื่อสร้างเสริมประสิทธิภาพการทำงาน หรือเพื่อความสะดวกในการติดต่อสื่อสารระหว่างอาชญากรในองค์กรอาชญากรรม และในขบวนการผู้ก่อการร้ายอีกด้วย

2.1.3 ลักษณะของอาชญากรรมคอมพิวเตอร์/อินเทอร์เน็ต

ลักษณะของอาชญากรรมคอมพิวเตอร์/อินเทอร์เน็ตนี้ เป็นการแบ่งโดยดูจาก “บทบาท” ของเครื่องคอมพิวเตอร์ที่เข้าไปเกี่ยวกันกับความผิดที่เกิดขึ้นเป็นหลัก โดยแบ่งออกได้เป็น 3 ลักษณะใหญ่ๆ ด้วยกัน คือ

1) คอมพิวเตอร์ในฐานะที่มีส่วนเกี่ยวข้องกับการกระทำความผิด (Computers as incidental to crime) การกระทำความผิดในลักษณะนี้ “บทบาท” ของคอมพิวเตอร์จะไม่มีความสำคัญมากนัก กล่าวคือ คอมพิวเตอร์ไม่ใช่สาระสำคัญในกระทำความผิด แม้ผู้กระทำความผิดไม่มีคอมพิวเตอร์ ความผิดที่ได้กระทำเหล่านั้นก็สามารถสำเร็จลงได้ ดังนั้น คอมพิวเตอร์จึงเป็นอุปกรณ์เสริมที่ช่วยอำนวยความสะดวกให้กับการกระทำผิดในรูปแบบเดิมๆ เท่านั้น เช่น ใช้คอมพิวเตอร์เก็บข้อมูลเกี่ยวกับการค้ายาเสพติด ใช้คอมพิวเตอร์ในการติดต่อสื่อสารในองค์กรอาชญากรรมหรือใช้คอมพิวเตอร์ในการเก็บสะสมภาพลามกเด็ก เป็นต้น
2) คอมพิวเตอร์ในฐานะที่เป็นเครื่องมือที่ใช้ในการกระทำความผิด (Computers as a tool in the commission of a crime) คอมพิวเตอร์เข้ามามีบทบาทหรือมีส่วนสำคัญที่จะทำให้กระทำความผิดสำเร็จลงได้ ความผิดในกลุ่มนี้ส่วนใหญ่มักเป็นเรื่องของอาชญากรรม

อินเทอร์เน็ต ยกตัวอย่างเช่น การเผยแพร่ภาพลามกอนาจาร หรือข้อความที่มีเนื้อหาเป็นภัยต่อสังคม หรือความมั่นคงทางเครือข่าย การพนันบนเครือข่าย การหมิ่นประมาทผู้อื่นโดยการโฆษณา โดยอาศัยเครือข่ายอินเทอร์เน็ต การละเมิดทรัพย์สินทางปัญญาด้วยการดาวน์โหลดหรือทำซ้ำผลงานอันมีลิขสิทธิ์ต่างๆ การลักลอบหรือขโมยใช้บริการสารสนเทศ การฟอกเงินทางอินเทอร์เน็ต หรือการโอนเงินที่ได้มาจากกระทำความผิดผ่านทางอินเทอร์เน็ต เพื่อให้เกิดความยากลำบากต่อการหาต้นตอของเงินเหล่านั้น การฉ้อโกงผ่านเครือข่ายอินเทอร์เน็ต เป็นต้น

3) คอมพิวเตอร์ในฐานะที่เป็นเป้าหมายหรือวัตถุแห่งการกระทำความผิด (Computers as a target of the crime) อาชญากรรมในลักษณะนี้ถือเป็นความผิดประเภทที่มีปัญหาทางด้านกฎหมายมากที่สุดในปัจจุบัน เนื่องจากมีรูปแบบการกระทำความผิดแบบใหม่ทั้งหมด ไม่ว่าจะเป็นวิธีการหรือวัตถุที่ถูกกระทำต่อ จนไม่อาจตีความกฎหมายเดิมที่มีอยู่ให้ควบคุมได้ และจำเป็นต้องมีการบัญญัติกฎหมายใหม่ขึ้น เพื่อกำหนดฐานความผิดใหม่ เนื่องจากผู้กระทำความผิดมีเป้าหมายที่ระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์เป็นสำคัญ ทั้งนี้อาจจะมีการเข้าถึง ทำลายเปลี่ยนแปลง หรือกระทำด้วยประการใดๆ เพื่อให้ระบบและข้อมูลดังกล่าวได้รับความเสียหาย เปลี่ยนแปลงไปจากเดิม โดยอาจได้รับประโยชน์จากการกระทำดังกล่าวด้วยหรือไม่ก็ตาม

2.2 แนวคิด ทฤษฎีทางอาชญาวิทยาและสังคมวิทยา

2.2.1 ทฤษฎีการเปลี่ยนผ่านเชิงพื้นที่ (Space transitional theory) [9]

ชัยชันการ์ (Jaishankar) นักอาชญาวิทยา ได้เสนอทฤษฎีที่นำมาใช้ ในการอธิบายแนวโน้มในการเกิดอาชญากรรมคอมพิวเตอร์ คือ “ทฤษฎีการเปลี่ยนผ่านเชิงพื้นที่” เพื่อใช้ในการอธิบายพฤติกรรมของบุคคลที่ใช้อินเทอร์เน็ตในการกระทำความผิด

ทฤษฎีการเปลี่ยนผ่านเชิงพื้นที่ในทางอาชญากรรมคอมพิวเตอร์ มีข้อสันนิษฐานเบื้องต้นว่าบุคคลอาจประพฤติตนในอินเทอร์เน็ตแตกต่างจากพื้นที่ทางกายภาพ ซึ่งความประพฤติบางอย่างนั้นอาจนำไปสู่การกระทำผิดทางคอมพิวเตอร์ และใช้ในการอธิบายรูปแบบการกระทำความผิดของอาชญากรคอมพิวเตอร์ด้วย

ทฤษฎีการเปลี่ยนผ่านเชิงพื้นที่ประกอบด้วยสมมุติฐาน 7 ประการคือ

1) บุคคลที่เก็บกดพฤติกรรมที่จะกระทำความผิดเอาไว้ในพื้นที่ทางกายภาพ ไม่ว่าจะด้วยเหตุผลทางจิตวิทยา ด้วยสถานะ หรือตำแหน่ง มีความโน้มเอียงในการที่จะกระทำความผิดในอินเทอร์เน็ต

[9] “รายงาน การวิจัยเพื่อพัฒนากระบวนการสืบสวนและสอบสวนของเจ้าหน้าที่ตำรวจในการรับมือกับอาชญากรรมคอมพิวเตอร์”, research.police.go.th, สืบค้นเมื่อ 26 ธ.ค. 60, http://research.police.go.th/index.php/datacenter/research/2558/-2559-1/342---67/file

2) การระบุสถานะบุคคลที่ยืดหยุ่น การกลมกลืนไปกับบุคคลอื่น ๆ โดยไม่แสดงตัวอย่างชัดเจน และการขาดปัจจัยในการตรวจสอบปราบปรามในอินเทอร์เน็ตเปิดโอกาสให้ผู้กระทำความผิดมีทางเลือกที่จะกระทำความผิดในทางคอมพิวเตอร์
3) การกระทำความผิดในทางคอมพิวเตอร์มีแนวโน้มที่จะถูกส่งต่อไปยังพื้นที่ทางกายภาพและการกระทำความผิดในพื้นที่ทางกายภาพก็มีแนวโน้มที่จะถูกส่งต่อมายังอินเทอร์เน็ตด้วยเช่นกัน
4) ความเสี่ยงภัยในการกระทำความผิดในอินเทอร์เน็ตจะเกิดขึ้นบางช่วงเวลา (Intermittent venture) และธรรมชาติของอินเทอร์เน็ตซึ่งมีการเปลี่ยนแปลงอยู่ตลอดเวลานั้นทำให้มีโอกาสที่จะหลบหนีได้ง่าย
5) บุคคลที่ไม่รู้จักกันมีแนวโน้มจะรวมตัวกัน และร่วมมือกันกระทำความผิดทางอินเทอร์เน็ต และกลุ่มคนที่มีการรวมตัวกันกระทำความผิดในพื้นที่ทางกายภาพอยู่เดิมแล้ว มีแนวโน้มจะกระทำความผิดร่วมกันในอินเทอร์เน็ตด้วย
6) บุคคลที่อยู่ในสังคมปิดมีแนวโน้มในการกระทำความผิดบนอินเทอร์เน็ตมากกว่าบุคคลที่มาจากสังคมที่เปิดกว้าง
7) บรรทัดฐานของสังคมและค่านิยมในพื้นที่ทางกายภาพและอินเทอร์เน็ตที่ขัดแย้งกันอาจนำไปสู่การกระทำความผิดทางคอมพิวเตอร์ได้

จากทฤษฎีดังกล่าว จะสามารถนำมาอธิบายพฤติกรรมการเข้าไปเกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ได้ เช่นในกรณีบุคคลที่ไม่สามารถแสดงพฤติกรรมบางอย่างทางพื้นที่กายภาพ แต่กลับแสดงพฤติกรรมการกระทำความผิดในระบบคอมพิวเตอร์ ไม่ว่าจะเป็นการเจาะระบบ หรือ แม้แต่การว่าร้าย ด่าทอ หมิ่นประมาททางเครือข่ายสังคม ซึ่งอาจจะด้วยข้อจำกัดที่จำเป็นต้องระบุตัวตนอย่างชัดเจนในสังคม เมื่อเปลี่ยนผ่านมาสู่พื้นที่ออนไลน์ในอินเทอร์เน็ต ซึ่งระบุตัวตนได้ยาก เช่น มีการใช้นามแฝง จึงตัดสินใจกระทำความผิด เป็นต้น

2.2.2 **ทฤษฎีความกดดันทางสังคม** (Strain theory) [10]

ทฤษฎีความกดดันทางสังคมของเมอร์ตัน (Merton) มีสมมติฐานว่า ธรรมชาติของมนุษย์เป็นผู้ปฏิบัติตามกฎระเบียบหรือบรรทัดฐานของสังคม ทฤษฎีดังกล่าวจึงอธิบายเกี่ยวกับการที่โครงสร้างทางสังคมได้กระตุ้นหรือเร่งเร้าให้บุคคลมีพฤติกรรมเบี่ยงเบนไปจากบรรทัดฐานของสังคม เมอร์ตันเชื่อว่า พฤติกรรมเบี่ยงเบนหรืออาชญากรรมเป็นปรากฏการณ์ปกติที่บุคคลตอบโต้หรือปรับตัวต่อความกดดันทางสังคมที่เกิดขึ้น นอกจากนี้วัฒนธรรมของสังคมจะเป็นตัวกำหนดจุดมุ่งหมายหรือความต้องการของคนในสังคมที่บุคคลควรไขว่คว้าหรือหามาให้ได้ ซึ่งจุดมุ่งหมายของแต่ละสังคมก็จะแตกต่างกันไปตามวัฒนธรรม

---

[10] พ.ต.อ.ดร.พรชัย ขันตี, ทฤษฎีอาชญาวิทยา : หลักการ งานวิจัย และนโยบายประยุกต์ (กรุงเทพมหานคร: ส.เจริญการพิมพ์, 2558). หน้า 184.

นั่นคือ ระบบโครงสร้าง วิถีชีวิต หรือระบบเศรษฐกิจของสังคมจะสร้างหรือพัฒนาความกดดันให้แก่คนในสังคม เนื่องจากได้สร้างค่านิยมทางวัตถุกับคนในสังคม ทำให้บุคคลบางกลุ่มไม่สามารถบรรลุวัตถุประสงค์ได้ จึงตอบโต้กับความกดดัน ด้วยการมีพฤติกรรมเบี่ยงเบนหรือพฤติกรรมอาชญากรรม

ในส่วนของทฤษฎีนี้ สามารถนำมาอธิบายเพิ่มเติมเกี่ยวกับสาเหตุของการเกิดอาชญากรรมไซเบอร์ได้ กล่าวคือ เมื่อบุคคลหรือกลุ่มบุคคลบางกลุ่ม ไม่สามารถบรรลุเป้าหมายได้ ทั้งในโลกแห่งความเป็นจริง หรือ สังคมออนไลน์ จึงมีการโต้ตอบกับความกดดัน ด้วยพฤติกรรมการก่ออาชญากรรม สมาชิกในสังคมออนไลน์ ก็มีการกำหนดเป้าหมายหรือค่านิยมทางสังคมเช่นเดียวกันกับในสังคมทางกายภาพ และต่างก็ต้องมีการปรับเปลี่ยนตนเอง เพื่อให้บรรลุถึงเป้าหมายหรือค่านิยมนั้น การที่ผู้ใช้แต่ละคนต่างนำเสนอเฉพาะด้านดีๆ ของตนผ่านทางพื้นที่เสมือนดังกล่าว ในอีกด้านหนึ่งก็คือการสร้างเป้าหมายหรือค่านิยมบนสังคมเช่นกัน โดยเป้าหมายทางสังคมจะถูกกำหนดอย่างไม่เป็นทางการหรือโดยไม่ตั้งใจ เช่น การลงภาพการรับประทานอาหาร การใช้ชีวิต การเดินทางท่องเที่ยวทั้งในและต่างประเทศ เป็นการกำหนดค่านิยมว่า หากใครมีรูปแบบการใช้ชีวิตดังกล่าว ก็จะได้รับการยอมรับว่าบรรลุเป้าหมายหรือเป็นผู้ประสบความสำเร็จในสังคมออนไลน์

จากเป้าหมายหรือการสร้างค่านิยมทางสังคมดังกล่าว เมื่อนำมาพิจารณาโดยอาศัยทฤษฎีของเมอร์ตันจะเห็นได้ว่า สมาชิกที่อยู่ในสังคมออนไลน์เอง ก็ย่อมสามารถถูกแบ่งออกได้ตามทฤษฎีนี้เช่นเดียวกัน โดยอาจมีบางกลุ่มที่ยอมรับในเป้าหมายหรือค่านิยมนั้น รวมทั้งยึดในวิธีการที่เป็นที่ยอมรับของสังคมเพื่อบรรลุสู่เป้าหมายหรือค่านิยมดังกล่าว แต่ขณะเดียวกันกับที่สมาชิกอีกหลายคนของสังคมที่ไม่อาจจะไปสู่เป้าหมายได้ด้วยวิธีการนั้น ก็แสวงหาวิธีการอื่นที่อาจไม่เป็นที่ยอมรับของสังคม ประกอบกับลักษณะของเครือข่ายทางสังคมออนไลน์บางอย่าง เอื้อต่อพฤติกรรมเบี่ยงเบนได้ง่าย เช่น การไม่อาจระบุได้แน่ชัดว่าสิ่งที่แต่ละคนส่งข้อความลงไปนั้นมีความจริงแท้มากน้อยเพียงใด บางคนจึงอาจเลือกวิธีการนำรูปอาหาร สถานที่ต่างๆ รวมถึงเสื้อผ้าเครื่องแต่งกายตามเว็บไซต์ แล้วนำมาลงแสดงในหน้ากระดานส่วนตัว เสมือนว่ารับประทานอาหารนั้น ได้ไปสถานที่นั้น หรือได้แต่งกายเช่นนั้น เพียงเพื่อให้ได้รับการยอมรับหรือมีตัวตนบนพื้นที่ทางสังคม แม้ว่าสิ่งที่ลงแสดงนั้นจะเป็นข้อมูลหลอกลวงที่สร้างขึ้นมาเองก็ตาม หรืออาจนำไปสู่พฤติกรรมอาชญากรรมที่มีความร้ายแรงมากขึ้น โดยเฉพาะสมาชิกของสังคมในกลุ่ม Innovation ซึ่งตามทฤษฎีของเมอร์ตัน จัดว่าเป็นกลุ่มที่ยอมรับในเป้าหมายทางค่านิยมของสังคมออนไลน์ โดยเชื่อว่าคนที่ประสบความสำเร็จในชีวิตจะต้องมีความร่ำรวย ได้รับการยอมรับจากสังคม มีรูปแบบการใช้ชีวิตที่หรูหรา แต่เนื่องจากสมาชิกในกลุ่มดังกล่าวเลือกที่จะปฏิเสธการปฏิบัติตามแนวทางที่สังคมยอมรับ ดังนั้นบุคคลในกลุ่มจึงมีแนวโน้มที่จะ

ใช้ช่องทางบนพื้นที่เสมือนในการกระทำความผิดลักษณะต่างๆ ซึ่งใช้เทคโนโลยีคอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด ได้แก่ การหลอกลวงบนพื้นที่ไซเบอร์ (Cyber fraud) การคุกคามบนพื้นที่ไซเบอร์ (Cyber harassment) การปลอมตัวเป็นบุคคลอื่นบนพื้นที่ไซเบอร์ (Cyber impersonating) หรือแม้แต่การเจาะระบบคอมพิวเตอร์ (Hacking) เพื่อเปลี่ยนแปลงแก้ไขข้อมูลทางคอมพิวเตอร์

นอกจากนี้ เป้าหมายหรือค่านิยมทางสังคมออนไลน์ ยังมีข้อแตกต่างที่สำคัญจากสังคมทางกายภาพอีกประการหนึ่งคือ ลักษณะของเนื้อหาที่มีการเผยแพร่ผ่านทางสังคมออนไลน์มีลักษณะเป็นกระแสสังคมที่เรียกว่ามาเร็วไปเร็ว ดังนั้น เป้าหมายหรือค่านิยมทางสังคมออนไลน์บางอย่างจะคงอยู่เฉพาะช่วงเวลาสั้นๆ และเมื่อผ่านไปช่วงระยะเวลาหนึ่ง เป้าหมายนั้นก็อาจเกิดการเปลี่ยนแปลงหรือเรียกว่าตกยุค ดังนั้นด้วยลักษณะของการเปลี่ยนแปลงอย่างรวดเร็วของค่านิยม จะก่อให้เกิดปัญหาการปรับตัวในทุกกลุ่มสมาชิก โดยเฉพาะอย่างยิ่งในกลุ่ม Conformity ซึ่งเป็นกลุ่มที่มีแนวโน้มการก่ออาชญากรรมต่ำที่สุดในสังคมทางกายภาพ เนื่องจากเป็นกลุ่มที่มีลักษณะในการยอมรับค่านิยมของสังคมและปฏิบัติตามวิถีทางของสังคมในการบรรลุเป้าหมาย แต่เมื่อเกิดความเปลี่ยนแปลงทางเป้าหมายอย่างรวดเร็วเช่นลักษณะของค่านิยมบนสังคมออนไลน์ ก็อาจส่งผลให้บุคคลในกลุ่มดังกล่าวไม่สามารถปฏิบัติตามวิถีทางที่ควรจะเป็นได้ และอาจเปลี่ยนตัวเองให้ก่ออาชญากรรม เนื่องจากไม่สามารถไปสู่เป้าหมายของสังคมที่มีความหลากหลายและมีความเปลี่ยนแปลงอย่างรวดเร็วได้ นอกจากนี้ในการเปลี่ยนแปลงของเป้าหมายดังกล่าว หากว่าเร็วเกินไปจนทำให้สมาชิกในสังคมออนไลน์ปรับตัวไม่ทัน ก็อาจเกิดปัญหาในเรื่องของความหดหู่ทางอารมณ์ อันนำไปสู่การฆ่าตัวตายอีกด้วย

2.2.3 **ทฤษฎีวัฒนธรรมรอง (Subcultural theory)**

2.2.3.1 ทฤษฎีวัฒนธรรมรองของอัลเบิรต์ โคเฮน (Albert K. Cohen) [11]

ทฤษฎีวัฒนธรรมรองของโคเฮน ให้ความสำคัญกับค่านิยมทางสังคมและชีวิตความเป็นอยู่ของบุคคล ซึ่งแต่ละชนชั้นในสังคมจะมีค่านิยมและความเป็นอยู่ที่แตกต่างกันไป โคเฮนได้นำสมมติฐานของทฤษฎีความกดดันทางสังคมที่ว่าการมีความกดดันเกิดขึ้นกับบางกลุ่มของสังคม ทำให้พวกเขาโต้ตอบโดยการเป็นอาชญากร โดยโคเฮนได้เสนอว่า การกระทำผิดกฎหมายในลักษณะเป็นกลุ่มโดยไม่กระทำผิดคนเดียว พฤติกรรมดังกล่าวมีลักษณะของการกระทำที่ไม่มีจุดมุ่งหมาย แต่มีพฤติกรรมโหดร้ายและเป็นการแสดงออกถึงการต่อต้านสังคม ซึ่งลักษณะของพฤติกรรมนี้จะแตกต่าง

[11] เรื่องเดียวหน้า, หน้า 198-200.

จากอาชญากรรมทั่วไป โคเฮนเชื่อว่าการกระทำผิดเหล่านี้เป็นการโต้ตอบต่อวัฒนธรรมของสังคมที่ยกย่องและยอมรับในบรรทัดฐานของสังคม โดยมีลักษณะที่ตรงกันข้ามกับบรรทัดฐานและค่านิยมของสังคม อันเป็นเหตุให้เกิดพฤติกรรมอาชญากรรมที่มีลักษณะส่อไปในทางเจตนาร้าย

ทฤษฎีของโคเฮนแสดงถึงว่าโครงสร้างทางสังคมเป็นรากฐานของพฤติกรรมเบี่ยงเบนหรืออาชญากรรม โดยเป็นตัวกีดกันไม่ให้ชนชั้นล่างของสังคมได้รับการยอมรับหรือมีสถานภาพในสังคม เกิดการถูกถอดถอนสถานภาพและนำไปสู่การผิดหวังในเรื่องสถานภาพ และเกิดการโต้ตอบปรากฏการณ์ทางสังคม โดยการรวมตัวกันและสร้างวัฒนธรรมขึ้นมาใหม่ อันมีลักษณะตรงกันข้ามกับวัฒนธรรมหลักของสังคม

2.2.3.2 ทฤษฎีวัฒนธรรมรองของโควาร์ดและโฮลิน (Cloward & Ohlin) [12]

โควาร์ดและโฮลิน นำเสนอทฤษฎีวัฒนธรรมรอง โดยมีสมมุติฐานว่าการที่บุคคลจะกระทำผิดกฎหมายนั้น นอกจากเกิดจากการที่ช่องทางที่ถูกกฎหมายถูกปิดกั้นแล้ว บุคคลนั้นจะต้องอยู่ในสถานะที่สามารถเรียนรู้ถึงวิธีการกระทำผิด ที่จะส่งผลให้เกิดการเรียนรู้และฝึกฝนทักษะ ตลอดจนความชำนาญของการกระทำผิดกฎหมาย แสดงให้เห็นว่าช่องทางที่ผิดกฎหมายก็สามารถถูกปิดกั้นได้เช่นเดียวกันกับช่องทางที่ถูกกฎหมาย โควาร์ดและโฮลินแบ่งแยกรูปแบบการกระทำผิดหรือวัฒนธรรมรองออกเป็น 3 รูปแบบ คือ วัฒนธรรมรองอาชญากรรม (Criminal subculture) วัฒนธรรมรองขัดแย้ง (Conflict subculture) และวัฒนธรรมรองหลบหนี (Retreatist subculture) โดยวัฒนธรรมรองอาชญากรรม เป็นวัฒนธรรมของกลุ่มที่รวมตัวกันประกอบอาชญากรรมต่างๆ โดยมีวัตถุประสงค์เพื่อบรรลุจุดมุ่งหมายของสังคม คือการมีสถานภาพทางเศรษฐกิจและสังคม มีการเรียนรู้รูปแบบอาชญากรรมและรับการถ่ายทอดวัฒนธรรมการกระทำผิดกฎหมาย

สำหรับวัฒนธรรมรองขัดแย้งนั้น จะแสดงออกโดยการต่อสู้ระหว่างกลุ่ม สถานภาพหรือชื่อเสียงจะได้มาจากการเป็นบุคคลที่แข็งแรง ก้าวร้าว ความที่ไม่สามารถพัฒนาความรู้ความสามารถในการหาเงินทั้งทางสุจริตและทุจริต จึงหันไปรวมกลุ่มและทำสิ่งที่ทำให้ได้รับการยอมรับ คือ ความรุนแรงและความกล้าหาญในการต่อสู้ระหว่างกลุ่ม และวัฒนธรรมรองรูปแบบสุดท้าย คือ วัฒนธรรมรองหลบหนี เป็นพฤติกรรมอาชญากรรมของกลุ่มที่ไม่ยอมรับหรือไม่ยึดถือจุดมุ่งหมายของสังคมที่ต้องการสร้างสถานภาพจากความมั่นคงทางเศรษฐกิจ จึงหลบหนีออกจากสังคม หรือปลีกตัวไปสร้างวัฒนธรรมใหม่ของตนเอง

ดังที่กล่าวแล้ว ในสังคมปัจจุบัน นอกจากสังคมปกติแบบดั้งเดิม ปัจจุบันจากความก้าวหน้าทางเทคโนโลยี และเครือข่ายอินเทอร์เน็ต ทำให้เกิดสังคมอีกรูปแบบหนึ่ง ควบคู่ไปกับสังคมแบบ

---

[12] เรื่องเดียวหน้า, หน้า 201-202.

ดั้งเดิม ก็คือสังคมในเครือข่ายคอมพิวเตอร์ หรือสังคมออนไลน์ ซึ่งทฤษฎีนี้ ก็ยังสามารถนำมาประยุกต์ใช้ในการอธิบายเกี่ยวกับอาชญากรรมคอมพิวเตอร์ที่เกิดขึ้นได้

2.2.4 ทฤษฎีการลงโทษ (Punishment theory)

การลงโทษผู้กระทำความผิดนั้นเป็นการกระทำเพื่อเหตุผลทางจิตวิทยาเป็นหลัก ไม่ว่าจะเป็นการขัดเกลาพฤติกรรม หรือส่งเสริมพฤติกรรมต่างๆ แล้วแต่กรณี โดยทั่วไปจะเป็นการนำกระบวนการหนึ่งๆ มาใช้กับบุคคลที่ได้รับการลงโทษ เพื่อส่งเสริมพฤติกรรมที่ดีและลดทอนพฤติกรรมที่ไม่ดีให้น้อยลงหรือหมดไป แต่ก็มีผลที่ต้องคำนึงถึงหลายประการ เช่น การที่พ่อแม่ใช้การดุด่ากับลูกที่กระทำพฤติกรรมไม่เหมาะสม อาจสร้างความเข้าใจผิดแก่ตัวลูกทำให้ลูกขาดความมั่นใจในการใช้ชีวิต ซึ่งในความเป็นจริงควรจะว่ากล่าวแต่พอเหมาะ และสอนให้เข้าใจว่าพฤติกรรมของลูกไม่ถูกต้องอย่างไร เพื่อเป็นการปรับพฤตินิสัยของเด็กอย่างยั่งยืน มากกว่าการทำให้เขาเกรงกลัวชั่วขณะแล้วก็กลับไปทำพฤติกรรมนั้นๆ อีกในอนาคต

นอกจากนี้ยังมีตัวอย่างของครูในโรงเรียนกับนักเรียน เช่น หากครูตั้งคำถามในชั้นเรียนแล้วนักเรียนตอบได้ก็ควรชื่นชมนักเรียนในชั้นเรียน แต่หากนักเรียนตอบไม่ถูกก็ไม่ควรว่ากล่าวต่อหน้าชั้นเรียน แต่ควรเป็นการอธิบายเสริมว่าคำตอบนั้นๆ ไม่ถูกตรงไหน อย่างไร แล้วส่งเสริมให้นักเรียนมีแรงบันดาลใจในการเรียนรู้ต่อไป เป็นต้น

<u>รูปแบบของการลงโทษผู้กระทำผิด</u>

การลงโทษเชิงบวก

การลงโทษเชิงบวก คือ การลงโทษที่เน้นการปรับพฤตินิสัยให้ดีขึ้นโดยไม่ใช้ความรุนแรงต่อร่างกายและจิตใจ ซึ่งแนวคิดนี้เป็นแนวคิดทัณฑวิทยาสมัยใหม่ ที่เล็งเห็นว่าการลงโทษทางลบที่รุนแรงนั้นมิได้แก้ไขพฤติกรรมของผู้กระทำผิดได้อย่างยั่งยืน ปัจจุบันเราอาจพบเห็นการลงโทษเชิงบวกได้หลายรูปแบบในหลากหลายประเทศ โดยรูปแบบที่น่าสนใจและได้รับความนิยม อาทิ การตักเตือนแล้วแนะนำแนวทางแก้ไขกับผู้กระทำผิด การให้คำปรึกษา และการให้ทำกิจกรรมที่เป็นประโยชน์ต่อร่างกาย (เช่น การออกกำลังกาย) โดยเรียกโดยรวมว่าเป็นการเสริมแรงทางบวกเพื่อไม่ให้กระทำผิดซ้ำ

การลงโทษเชิงลบ

การลงโทษเชิงลบ คือ การลงโทษที่เน้นความรุนแรงต่อร่างกายและจิตใจ ซึ่งเป็นแนวคิดทางทัณฑวิทยาแบบเก่า มีแนวคิดว่าการลงโทษที่รุนแรงจะทำให้ผู้กระทำผิดหวาดกลัวและหลาบจำจนไม่กล้าทำผิดอีก เช่น การโบยตี การคุมขังโดยลดทอนความเป็นมนุษย์ (เช่น ขังเดี่ยว คุกมืด) และการประหารชีวิต ซึ่งเป็นการทั้งข่มขู่ยับยั้งให้ผู้กระทำความผิดหวาดกลัว และตัดออกจากสังคมเพื่อลดโอกาสการกระทำผิดนั่นเอง

<u>แรงจูงใจและประสิทธิผลของการลงโทษ</u>

ความเร่งด่วน

การลงโทษทั้งเชิงบวกและเชิงลบนั้นต้องกระทำอย่างรวดเร็วฉับไว เพื่อลดพฤตินิสัยที่ไม่ดี หากทำได้อย่างรวดเร็วฉับไว จะเป็นการแก้ไขพฤตินิสัยนั้นได้อย่างมีประสิทธิภาพ

ความเข้มข้น และความหนักเบาของการลงโทษ

การลงโทษนั้นต้องมีความเข้มข้น และขนาดที่เหมาะสมกับความผิด ไม่สามารถนำการลงโทษแบบหนึ่งใช้กับความผิดทุกรูปแบบได้ เนื่องจากความคิดพื้นฐานของการกระทำผิดของแต่ละกรณีนั้นต่างกัน จึงต้องใช้วิธีการแก้ไขที่แตกต่างกันด้วย

แผนงานการลงโทษ

การลงโทษทั้งในเชิงบวกและเชิงลบจำเป็นต้องมีการวางแผนงานที่ชัดเจน มิใช่ลงโทษไปเรื่อยๆ ตามแต่ผู้ลงโทษจะพอใจ ซึ่งจะไม่ใช่การลงโทษ หากแต่จะเป็นการทรมานผู้กระทำผิด และไม่สามารถแก้ไขผู้กระทำผิดให้ดีขึ้นได้

การเสริมแรง

การเสริมแรงมีอยู่ 2 ลักษณะ คือการเสริมแรงทางบวก อาจเป็นการชมเชย ให้รางวัลเล็กๆ น้อยๆ และการเสริมแรงทางลบ อาจเป็นการตำหนิ การงดให้สวัสดิการต่างๆ ซึ่งมีวิธีใช้ที่แตกต่างกันตามความเหมาะสม ในกรณีของการลงโทษนั้นสามารถนำเอาแนวคิดการเสริมแรงนั้นมาปรับใช้โดยการเสริมแรงทางบวกหากผู้กระทำความผิดประพฤติตนดีขึ้น หรือนำการเสริมแรงทางลบมาปรับใช้หากผู้กระทำความผิดประพฤติตนไม่ถูก

ผลกระทบของการลงโทษ

ผลกระทบในที่นี้มิได้หมายถึงผลกระทบที่ไม่ดีแต่เพียงอย่างเดียว แต่หมายความรวมถึงผลกระทบในทางดีด้วย ซึ่งอาจเป็นการที่บุคคลอาจมีพฤติกรรมแย่ลงหากลงโทษไม่เหมาะสมกับความผิด หรือการมีพฤติกรรมที่ดีขึ้นหากได้รับการลงโทษที่เหมาะสม

การฟื้นฟูหลังการลงโทษ

การฟื้นฟูนับเป็นกระบวนการสำคัญที่สุดของการลงโทษ เพราะเป็นปัจจัยสำคัญที่จะทำให้กลับตัวเป็นคนดีของสังคม อาจเป็นในรูปแบบของการให้ทำกิจกรรมกับครอบครัว การฝึกอาชีพ การผ่อนคลาย เช่น ฟังธรรมะ เป็นต้น ซึ่งในประเทศไทยเป็นหน้าที่ของกรมราชทัณฑ์เป็นหลัก

ไม่ว่าจะเป็นพื้นที่ทางกายภาพ หรือในสังคมออนไลน์ ทั้งสองพื้นที่ก็ถือว่าเป็นพื้นที่ทางสังคมเช่นเดียวกัน ดังนั้นแนวคิด ทฤษฎีที่อธิบายเกี่ยวกับสังคมบนพื้นที่ทางกายภาพ ก็ย่อมนำมาศึกษาสังคมออนไลน์ได้เช่นกัน การนำทฤษฎีการลงโทษมากล่าวถึงในบริบทของความเกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์คือ การนำการลงโทษที่เหมาะสม ทั้งเชิงบวกและเชิงลบมาปรับใช้ จะสามารถช่วยในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์อย่างมีประสิทธิภาพได้

2.3 แนวคิด ทฤษฎีเกี่ยวกับกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล

2.3.1 นิติวิทยาศาสตร์ และการตรวจพิสูจน์พยานหลักฐาน[13]

จากเอกสารประกอบการบรรยาย หัวข้อ การแก้ไขปัญหาอาชญากรรมด้วยนิติวิทยาศาสตร์ โดย พัชรา สินลอยมา (2560) นิติวิทยาศาสตร์ (Forensic science) คือ “การนำความรู้ทางวิทยาศาสตร์ทุกสาขามาประยุกต์ใช้ เพื่อพิสูจน์ข้อเท็จจริงในคดีความเพื่อผลในการบังคับใช้กฎหมายและการลงโทษ”

2.3.1.1 ความสำคัญของนิติวิทยาศาสตร์

การอำนวยความยุติธรรม (Enhancement of justice) ถือเป็นภารกิจสำคัญพื้นฐานของรัฐ ซึ่งรัฐจะต้องดำเนินการอำนวยความยุติธรรมโดยการจัดการบริหารองค์การในกระบวนการยุติธรรมให้เป็นที่พึงพอใจของประชาชนและเป็นสากลตามหลักนิติธรรม (The Rule of law)

ทั้งนี้ จุดมุ่งหมายหลักในการอำนวยความยุติธรรม คือ การให้ประชาชนที่เข้าสู่กระบวนการยุติธรรมได้รับความสะดวก รวดเร็ว ประหยัด และเป็นธรรม ซึ่งปัจจัยที่จะทำให้บรรลุจุดมุ่งหมายดังกล่าวประกอบด้วย กฎหมาย ระบบการพิจารณาคดี ระเบียบปฏิบัติ ตลอดจนการปฏิบัติงานของหน่วยงานและบุคคลที่เกี่ยวข้องเช่น ตำรวจ พนักงานสอบสวน พนักงานอัยการ ทนายความ พยาน เจ้าหน้าที่ของศาล และผู้พิพากษา

ระบบการพิจารณาคดีและสืบพยานของไทย ศาลจะต้องวางตัวเป็นกลางในคดีอาญา ซึ่งเริ่มคดีโดยโจทก์เป็นผู้กล่าวหา และโจทก์ต้องนำพยานหลักฐานมาพิสูจน์ความผิดของจำเลย ซึ่งจำเลยในคดีอาญา ได้รับการสันนิษฐานว่าเป็นผู้บริสุทธิ์ จนกว่าจะพิสูจน์ให้ศาลเห็นเป็นที่สิ้นสงสัยว่าจำเลยเป็นผู้กระทำความผิด

เมื่อโจทก์นำสืบได้ว่าจำเลยเป็นผู้กระทำผิดแล้ว จำเลยจึงมีหน้าที่นำสืบพยานหลักฐานหักล้างพยานหลักฐานของโจทก์ และเป็นหน้าที่ของคู่ความแต่ละฝ่ายจะต้องเสนอพยานหลักฐานของตน ซึ่งศาลจะพิจารณาโดยพยานหลักฐานที่คู่ความเสนอต่อศาลเท่านั้น โดยปกติศาลจะไม่เข้าไปสอดแทรกถามพยานโดยไม่จำเป็น จะไม่เรียกพยานมาสืบเอง ในคดีอาญาศาลจะช่วยถามพยานให้จำเลย แต่ศาลจะไม่ช่วยซักถามพยานโจทก์ โดยถือหลักว่าเป็นหน้าที่ของโจทก์ที่จะพิสูจน์ความผิดของจำเลย ศาลจะไม่ช่วยถามพยานโจทก์ให้จำเลยได้รับโทษ ถ้าโจทก์ถามพยานหลักฐานไม่สิ้นสงสัยตามสมควร ศาลก็จะยกฟ้อง และศาลถือเคร่งครัดว่าถ้าฟ้องโจทก์เคลือบคลุมหรือข้อเท็จจริงที่โจทก์นำสืบแตกต่างไปจากคำฟ้องแล้ว ศาลจะยกฟ้องเสมอโดยไม่คำนึงถึงความเป็นจริงว่าจำเลยได้กระทำความผิดหรือไม่ ในปัจจุบันนี้ ได้เกิดปัญหาทางด้านอาชญากรรมขึ้นมากมาย ซึ่งการที่จะเอาตัวผู้กระทำผิดที่แท้จริงมาลงโทษตามกระบวนการยุติธรรมนั้นเป็นเรื่องที่สำคัญอย่างยิ่ง โดยเฉพาะจะต้องมีการรวบรวมพยานหลักฐานมายืนยันให้สามารถพิสูจน์ความผิดได้อย่างชัดเจน ดังนั้นในประเทศที่พัฒนาแล้ว อาทิเช่น ประเทศญี่ปุ่น ยุโรปและสหรัฐอเมริกา จึงมีการนำเอาความรู้ทางด้านวิทยาศาสตร์และเทคโนโลยีต่างๆ มาพัฒนาใช้ในการตรวจพิสูจน์หลักฐานต่างๆให้ได้ผลที่ถูกต้องแท้จริงตามหลักวิทยาศาสตร์ ซึ่งได้ผลอย่างดียิ่งในการสืบสวนติดตามหาคนร้ายต่างๆ โดยเฉพาะประเทศญี่ปุ่น เมื่อเกิดคดีฆาตกรรมเกิดขึ้น

---

[13] “การแก้ไขปัญหาอาชญากรรมด้วยนิติวิทยาศาสตร์”, www.oja.go.th, สืบค้นเมื่อ 14 ก.พ. 61, http://www.oja.go.th/th/wp-content/uploads/course/26-1-60.doc

สามารถจับกุมคนร้ายได้ถึง 90% โดยการใช้เครื่องมือวิทยาศาสตร์และเทคโนโลยีที่ค้นคว้าวิจัยและผลิตขึ้นอย่างทันสมัย ผสานกับหลักนิติวิทยาศาสตร์นี้ให้บรรลุผลได้เป็นอย่างมาก

จากประโยชน์ดังกล่าวข้างต้น จึงมีการนำนิติวิทยาศาสตร์มาใช้ในขอบเขตโดยทั่วไปดังนี้

1) การตรวจสถานที่เกิดเหตุ และการถ่ายรูป (Crime scene investigation and forensic)
2) การตรวจลายนิ้วมือ ฝ่ามือ ฝ่าเท้า (Fingerprint, palm print, footprint)
3) การตรวจเอกสาร (Document) เช่น ตรวจลายเซ็น ลายมือเขียน
4) การตรวจอาวุธปืน และกระสุนปืนของกลาง (Forensic ballistics)
5) การตรวจทางเคมี (Forensic chemistry) เช่น ตรวจวิเคราะห์องค์ประกอบทางเคมีของสารต่าง ๆ
6) การตรวจทางฟิสิกส์ (Forensic physics) เช่น ตรวจร่องรอยการเฉี่ยวชนของรถ
7) การตรวจทางชีววิทยา (Biological trace evidence) เช่น ตรวจเส้นผม เลือด อสุจิ
8) การตรวจทางนิติเวช (Forensic medicine) ได้แก่ งานนิติพยาธิ งานนิติวิทยา งานชีวเคมี งานพิสูจน์บุคคล งานภาพการแพทย์

ทั้งนี้ โดยทั่วไปการพิจารณาประเภทของพยานวัตถุและจุดประสงค์ในการตรวจพิสูจน์สามารถแยกวิธีการออกได้ดังนี้

1) การตรวจโดยวิธีทางเคมี และชีววิทยา (Chemical and biological analysis)
2) การตรวจโดยการใช้วิธีทางกายภาพ (Physical experiments)
3) การตรวจโดยใช้เครื่องมือทางวิทยาศาสตร์ (Instrumental analysis)

2.3.1.2 สถานที่เกิดเหตุและพยานหลักฐานทางชีววิทยา

เมื่อมีการกระทำที่กฎหมายบัญญัติว่าเป็นความผิดเกิดขึ้น สถานที่เกิดเหตุถือเป็นสถานที่แรกของกระบวนการต่างๆ และเป็นจุดเริ่มต้นของการดำเนินการทั้งหลายเพื่อให้ได้มาซึ่งพยานหลักฐานที่สามารถนำมาพิสูจน์ถึงการกระทำผิดและตัวผู้กระทำผิด เหตุในคดีอาญาร้ายแรงเมื่อเกิดเหตุดังกล่าวขึ้นแล้วผู้มีหน้าที่รับผิดชอบทุกแขนง เช่น พนักงานสอบสวน เจ้าหน้าที่ตรวจสถานที่เกิดเหตุ ผู้ชำนาญการตรวจพิสูจน์จะต้องให้ความสนใจ โดยเฉพาะอย่างยิ่งการตรวจเก็บรวบรวมพยานหลักฐานเพื่อตรวจพิสูจน์ทางวิทยาศาสตร์ และนำผลที่ได้มาประมวลเหตุการณ์ให้ได้ข้อสรุปที่แท้จริงของรายละเอียดแห่งคดี ผลการตรวจวัตถุพยานดังกล่าวจึงเป็นข้อมูลที่สามารถนำมาใช้สนับสนุนการสืบสวนสอบสวน และใช้เป็นพยานหลักฐานต่อศาลในการปฏิบัติงานของเจ้าหน้าที่ที่เกี่ยวข้องภายหลังเกิดเหตุ ด้วยเหตุนี้จึงไม่ใช่เพียงแต่พนักงานสอบสวนหรือเจ้าหน้าที่ตรวจสถานที่เกิดเหตุเท่านั้นที่ต้องเรียนรู้และรอบรู้การตรวจสถานที่เกิดเหตุ แม้แต่อัยการ ผู้พิพากษา และผู้ตรวจพิสูจน์หรือผู้ชำนาญการที่ตรวจพิสูจน์ของกลางต่างๆ ทางวิทยาศาสตร์ก็ควรศึกษาและรอบรู้ไว้ เพราะมีโอกาสเสมอที่ผู้ชำนาญการจะต้องเข้าร่วมตรวจเก็บวัตถุพยานในสถานที่เกิดเหตุ รวมถึงการให้คำแนะนำการเก็บรักษาพยานหลักฐานที่ถูกต้องตามหลักวิชาการ เพื่อประโยชน์สูงสุดในการนำมาใช้ตรวจพิสูจน์ทางวิทยาศาสตร์

2.3.1.3 หลักฐานทางนิติวิทยาศาสตร์กับกระบวนการพิจารณาคดีอาญา

กระบวนการยุติธรรมของประเทศไทยมีการปรับเปลี่ยนจากการเน้นความสำคัญของประจักษ์พยานมาสู่ระบบพิสูจน์การกระทำความผิดโดยการรับฟังพยานหลักฐานทางด้านวิทยาศาสตร์ มีการนำหลักนิติวิทยาศาสตร์มาใช้ควบคู่กับกระบวนการยุติธรรม ซึ่งเป็นมาตรการในการป้องกัน และปราบปรามการก่ออาชญากรรมทางหนึ่ง ซึ่งใช้หลักนิติวิทยาศาสตร์ 2 ประเภท

(1) นิติวิทยาศาสตร์ที่เป็นวิทยาศาสตร์ธรรมชาติ เช่น วิชาพิสูจน์หลักฐาน รวมถึงการตรวจสถานที่เกิดเหตุและเก็บรวบรวมวัตถุพยานในสถานที่เกิดเหตุ

(2) นิติวิทยาศาสตร์ที่เป็นวิทยาศาสตร์ประยุกต์โดยการนำความรู้ทางวิทยาศาสตร์ในสาขาต่างๆ มาประยุกต์ใช้ให้เป็นประโยชน์ต่อกระบวนการยุติธรรม โดยขณะเดียวกันนิติวิทยาศาสตร์ได้ถูกนำมาใช้ประโยชน์ในงานสืบสวนสอบสวน เช่น การตรวจสถานที่เกิดเหตุและการถ่ายรูป การตรวจลายนิ้วมือ ฝ่ามือ ฝ่าเท้า การตรวจเอกสาร การตรวจทางฟิสิกส์ เช่น ตรวจร่องรอยการเฉี่ยวชนรถ การตรวจทางนิติเวช เช่น งานนิติพยาธิ งานนิติวิทยา งานชีวเคมีและการตรวจทางชีววิทยา เช่น ตรวจเส้นผม เลือด อสุจิ และตรวจรหัสพันธุกรรม (DNA)

การพิจารณาคดีอาญาในกระบวนการยุติธรรมของประเทศไทย มีข้อที่ต้องวินิจฉัยชี้ขาดอยู่สองประการ ได้แก่ ข้อกฎหมายและข้อเท็จจริง หลักในการวินิจฉัยจะต้องพิจารณาค้นคว้าหาข้อเท็จจริงหรือความสัตย์จริงในคดีว่าเป็นอย่างไร แล้วจึงยกข้อกฎหมายขึ้นปรับวินิจฉัยว่าจำเลยควรจะได้รับโทษหรือควรจะได้รับการปล่อยตัวไป ตามกฎหมายลักษณะพยานข้อเท็จจริงที่ศาลจะรับรู้ได้เองจำกัดอยู่เพียงข้อเท็จจริงที่เป็นไปตามธรรมดาธรรมชาติ ซึ่งบุคคลธรรมดาจะพึงรู้ได้เอง ส่วนข้อเท็จจริงอย่างอื่นที่อยู่นอกเหนือไปจากความรู้ของบุคคลธรรมดาศาลรับรู้เองไม่ได้ ฉะนั้นฝ่ายผู้กล่าวหาจะต้องพิสูจน์ให้ประจักษ์แก่ศาล ว่าผู้ต้องหาได้กระทำการที่อ้างว่าเป็นความผิดนั้นจริงโดยพยานหลักฐานที่เกี่ยวกับข้อเท็จจริงในคดี (Relevant evidence) หมายความถึง พยานที่มีแนวโน้มที่จะทำให้ความมีอยู่ของข้อเท็จจริงใด โดยผลจากการวินิจฉัยมีความเป็นไปได้มากกว่าหรือน้อยกว่าการไม่มีพยานหลักฐาน กล่าวอีกนัยหนึ่ง คือ พยานหลักฐานที่เกี่ยวกับข้อเท็จจริงในคดีเกี่ยวข้องกับพยานหลักฐานทางวิทยาศาสตร์ในสาขาต่างๆ ที่มีคุณค่าในการพิสูจน์ความจริงที่เกิดขึ้น สามารถยืนยันข้อเท็จจริงได้ ซึ่งสิ่งต่างๆ ที่จะนำ ไปใช้เป็นพยานหลักฐานในคดีจำต้องมีคุณค่าในตัวเอง

พยานหลักฐานทางนิติวิทยาศาสตร์ เป็นพยานหลักฐานที่เกิดขึ้นด้วยการวิเคราะห์ หรือวิจัย ซึ่งในทางกฎหมาย ถือว่า พยานหลักฐานเหล่านี้เป็นพยานหลักฐานอย่างหนึ่งที่จะนำเข้าสู่กระบวนการพิจารณาหรือจะนำเข้าสู่ความรู้ของศาลเพื่อให้ศาลวินิจฉัยว่าจำเลยมีความผิดหรือไม่ โดยกำหนดวิธีการนำสืบไว้ คือ หากคู่ความประสงค์จะอ้างหลักฐานทางนิติวิทยาศาสตร์เข้าสู่สำนวนเพื่อนำสืบข้อเท็จจริง ให้นำสืบโดยผู้เชี่ยวชาญซึ่งได้ทำการตรวจ ได้วิเคราะห์หรือได้วิจัยสังเกตเหตุการณ์หรือสิ่งของต่างๆที่เกี่ยวข้องกับในคดีนั้นมาแล้ว ฉะนั้น จึงกล่าวได้ว่าพยานหลักฐานทางวิทยาศาสตร์นี้ก็คือพยานความเห็นของผู้เชี่ยวชาญตามกฎหมายนั่นเอง ที่ผ่านมามีการนำหลักฐานทางนิติวิทยาศาสตร์มาช่วยคลี่คลายคดีต่างๆ ที่มีความสำคัญ และมีความยุ่งยากสลับซับซ้อนทั้งที่เกิดขึ้นทั้งในประเทศและต่างประเทศมาแล้วหลายคดี ในประเทศสหรัฐอเมริกาคดีที่มีการนำหลักฐานทางนิติวิทยาศาสตร์มาช่วยในการคลี่คลายคดี ได้แก่ คดีลอบสังหารประธานาธิบดีเคนนาดี้ พฤศจิกายน ค.ศ.

1963, คดีโอ เจ ซิมป์สัน ฆาตกรรมภรรยาและเพื่อน มิถุนายน ค.ศ.1994 และคดีฆาตกรรมไร้ศพ เหตุเกิดที่รัฐฟลอริดา เป็นต้น สำหรับในประเทศอังกฤษ คดีสำคัญที่มีการนำหลักฐานทางนิติวิทยาศาสตร์มาช่วยในการคลี่คลายคดี คือ คดีฆาตกรรมอำพรางที่ฟาร์มวิดเดนฮิลล์ หมู่บ้านฮอตัน ในปี ค.ศ.1984

ในประเทศไทยคดีที่สำคัญ และมีความสลับซับซ้อน ซึ่งคลี่คลายลงได้โดยอาศัยหลักฐานทางนิติวิทยาศาสตร์ ได้แก่ คดีฆาตกรรม น.ส.ดอริส ฟอน ฮาเฟน นางแบบสาวชาวเดนมาร์ก เมื่อ 24 มกราคม พ.ศ. 2511, คดีฆาตกรรมนางศยามล พ.ศ. 2536, คดีฆาตกรรมนายแสงชัย สุนทรวัฒน์ พ.ศ. 2539, คดีฆาตกรรม น.ส.เจนจิรา พลอยองุ่นศรี นักศึกษาแพทย์ปี 5 พ.ศ. 2541 และคดีล่าสุดที่ได้รับความสนใจจากประชาชน คือ คดีฆาตกรรมแพทย์หญิงผัสพร บุญเกษมสันติ โดยศาลฎีกาพิพากษาประหารชีวิตนายแพทย์วิสุทธิ์ บุญเกษมสันติ (สามี) คดีนี้ถึงแม้ว่าจะไม่พบศพของผู้เสียชีวิต แต่ผลการพิสูจน์รหัสพันธุกรรม ประกอบกับพยานแวดล้อมต่างๆ จึง เชื่อได้ว่า แพทย์หญิงผัสพรฯ เสียชีวิตแล้ว

โดยสรุปแล้ว ถือได้ว่านิติวิทยาศาสตร์เป็นการประยุกต์ใช้ความรู้ทางวิชาการทางด้านต่างๆ ผนวกเข้ากับการบังคับใช้ทางกฎหมาย เพื่อเป็นประโยชน์ต่อกระบวนการยุติธรรม ให้สามารถอำนวยความยุติธรรมให้กับผู้เสียหาย และผู้ต้องหาได้เป็นอย่างดี ซึ่งจำเป็นอย่างยิ่งที่ประเทศไทยจะต้องส่งเสริมให้มีการพัฒนาทางด้านการตรวจวิเคราะห์ต่างๆ ดังกล่าวข้างต้น รวมถึงการนำเอานิติวิทยาศาสตร์นี้มาส่งเสริมกระบวนการยุติธรรมของประเทศไทยให้ทัดเทียมกับอารยประเทศ ซึ่งจะส่งผลอย่างดียิ่งต่อประชาชนคนไทยในท้ายที่สุด

<u>ประโยชน์ของพยานหลักฐานทางนิติวิทยาศาสตร์กับการแก้ไขปัญหาอาชญากรรม</u>

1) เป็นเครื่องช่วยชี้ว่ามีการก่ออาชญากรรมแน่นอน เช่น ผู้เสียหายแจ้งว่าถูกข่มขืน และตรวจพบว่าผู้เสียหายมีเสื้อผ้าฉีกขาด มีแผลตามร่างกาย
2) เป็นเครื่องช่วยชี้ว่าผู้ต้องสงสัยได้อยู่ในที่เกิดเหตุ เช่น ตรวจได้ขนแมวที่ขากางเกงของผู้ต้องสงสัย ที่ผู้ต้องสงสัยอธิบายที่มาไม่ได้ และบ้านที่ผู้เสียหายถูกข่มขืนเลี้ยงแมว
3) เป็นเครื่องช่วยชี้ว่าบุคคลนั้นเกี่ยวข้องกับอาชญากรรมที่เกิดขึ้น เช่น พบลายพิมพ์นิ้วมือผู้ต้องสงสัยในด้านในของถุงมือที่ถอดทิ้งไว้ในบ้านที่ถูกโจรกรรม
4) เป็นเครื่องช่วยกันผู้บริสุทธิ์ออกไป เช่น เด็กหญิง 2 คนพี่น้องกล่าวหาว่า ผู้ต้องสงสัยวางยาแล้วทำมิดีมิร้าย แต่การตรวจทั้งเลือดและปัสสาวะของเด็กแล้วไม่พบสารใด
5) เป็นเครื่องยืนยันคำให้การของผู้เสียหาย เช่น ผู้เสียหายอ้างว่าถูกผู้ต้องสงสัยแทงมือ ผู้เสียหายจึงเอามือที่เลือดออกป้ายไปบนแขนเสื้อของผู้ต้องสงสัย จากการตรวจพบว่าคราบเลือดบนแขนเสื้อของผู้ต้องสงสัยเป็นเลือดของผู้เสียหายจริง
6) ผู้ต้องสงสัยที่ถูกยันด้วยพยานทางฟิสิกส์อาจจะสารภาพ เช่น คดีเจนจิรา เมื่อพิสูจน์ได้ว่าผู้ตายเสียชีวิตเพราะถูกยิง ในขณะที่ผู้ต้องหาให้การกับตำรวจก่อนหน้านี้ว่า ฆ่าโดยการบีบคอ ผู้ต้องหาจึงสารภาพ
7) มีค่ามากกว่าประจักษ์พยานเพราะเคยมีการทดลองแล้วพบว่า ประจักษ์พยานอาจให้การคลาดเคลื่อนไปได้ เมื่อเวลาผ่านไปเป็นเดือนหรือเป็นปี พยานหลักฐานทางนิติวิทยาศาสตร์ได้รับความเชื่อถือจากศาลมากขึ้นเรื่อยๆ
8) การไม่พบพยานทางนิติวิทยาศาสตร์ช่วยยืนยันว่าไม่มีอาชญากรรม เช่น แจ้งว่าถูกลักทรัพย์ แต่ตรวจแล้วไม่มีร่องรอยงัดและทรัพย์ที่ว่าหายยังอยู่

2.3.1.4 การพิสูจน์หลักฐานและสาขาต่างๆ ของนิติวิทยาศาสตร์

2.3.1.4.1 วิชาพิสูจน์หลักฐาน

นิติวิทยาศาสตร์ คือ “คือการนำวิทยาศาสตร์ทุกสาขามาประยุกต์ใช้เพื่อประโยชน์แห่งกฎหมาย” ประโยชน์แห่งกฎหมายที่กล่าวถึงนี้ได้แก่ ประโยชน์ทางนิติบัญญัติในเรื่องการออกกฎหมาย และประโยชน์ของการบังคับใช้กฎหมายในการลงโทษ (Enforcement)

คำว่า Criminalities เป็นศัพท์ที่ไม่แพร่หลายมากนักในประเทศไทย จะมีผู้คุ้นเคยและใช้อยู่ก็ในเฉพาะแวดวงจำกัด ตรงข้ามกันกับ Forensic science นิติวิทยาศาสตร์ ซึ่งจะดูแพร่หลาย และเป็นที่คุ้นเคยมากในหลายวงการ เช่น ตำรวจ ทนายความ อัยการและศาล เป็นต้น ตามคำอธิบายของสมาคมนักพิสูจน์หลักฐานแห่งรัฐแคลิฟอร์เนีย (California association of criminalizes) ซึ่งได้ให้ไว้เมื่อ วันที่ 25 พฤษภาคม พ.ศ. 2506 มีว่า “Criminalities is that profession and scientific discipline to the recognition, identification and evaluation of physical evidence by application of the natural sciences to law-science matter”

หากถอดความหมายของคำว่า Criminalities นี้ออกมาอย่างคร่าวๆ จะได้ว่าเป็นกฎเกณฑ์ทั้งทางวิชาชีพและทางวิทยาศาสตร์ ซึ่งมุ่งในการให้การรับรอง การชี้เฉพาะ การจำแนกและการตีความหมายของพยานวัตถุโดยนำวิทยาศาสตร์ธรรมชาติมาประยุกต์ใช้ในกรณีที่เกี่ยวข้องระหว่างกฎหมายกับวิทยาศาสตร์

คำจำกัดความนี้หากจะขยายให้ชัดเจนอาจกล่าวได้ว่าเป็นศาสตร์แขนงหนึ่งซึ่งอาศัยกฎเกณฑ์ทฤษฎีต่างๆ ของวิทยาศาสตร์หลายสาขาเช่น เคมี ฟิสิกส์ ชีววิทยา มารวมกันภายใต้กำหนดกฎเกณฑ์แห่งกฎหมาย เพื่อบรรลุจุดประสงค์สำคัญคือ การพิสูจน์การกระทำผิด หรือความบริสุทธิ์ของผู้ถูกกล่าวหา

คุณสมบัติที่ทำให้วิชาพิสูจน์หลักฐานเป็นที่ยอมรับว่าเป็นวิชาการอิสระสาขาหนึ่งเช่นเดียวกับสาขาวิชาอื่นๆ ก็คือ มีสายใยซึ่งเชื่อมโยงกับหลักเกณฑ์ทฤษฎีต่างๆ เข้าด้วยกันเป็นกลุ่มก้อน หลักทฤษฎีที่ว่านี้มีหัวใจสำคัญอยู่ที่

1) การจำแนก (Individualization) เป็นการแสดงเห็นความแตกต่าง การจัดวัตถุ จัดประเภท เช่น กรณีรถหายแจ้งความกับตำรวจ เมื่อตำรวจพบรถ ผู้เสียหายต้องสอบถามก่อนว่า เป็นรถชนิดอะไร สีไหน ยี่ห้ออะไร นั้นคือการจำแนกก่อนที่จะมาถึงขั้นตอนชี้เฉพาะ
2) การชี้เฉพาะ (Identification) ทางด้านวิชาปรัชญาได้ให้คำอธิบายของ Identity ไว้ว่าคือ ความหายาก หรือสิ่งที่มีเพียงหนึ่งเท่านั้น ไม่สามารถนำสิ่งอื่นมาทดแทนได้ ฉะนั้นของสองสิ่งก็จะไม่เป็น identical กันได้นอกจากตัวของมันเอง และวิชาพิสูจน์หลักฐานได้เข้ามามีบทบาทก็เพราะความหมายนี้ การชี้เฉพาะ ก็เป็นกรรมวิธีที่จะจัดให้สิ่งของที่มีตัวตนสิ่งหนึ่ง ให้ไปรวมอยู่ในประเภทหรือจำพวกที่ได้กำหนดขอบเขตหรือคุณลักษณะตายตัวเอาไว้ เช่น Fingerprint identification ได้แก่การตรวจสอบลายนิ้วมือต้องสงสัยว่าจะเกิดจากลายนิ้วมือของบุคคลที่ต้องสงสัยหรือไม่ โดยอาศัยหลักกำหนดตายตัวไว้แล้วในเรื่องจำนวน และชนิดของลักษณะสำคัญพิเศษต่างๆ ของลายเส้นนิ้วมือ เป็นต้น การชี้เฉพาะต้องอาศัยคุณลักษณะ 2 ประการ
    2.1) คุณลักษณะโดยทั่วไป (Class characteristics) คือ ลักษณะที่ปรากฏเหมือนกันโดยทั่วไปตามปกติ เช่น เมื่อคนร้ายลงมือก่ออาชญากรรมในสถานที่ใด ย่อมมีการทิ้ง

ร่องรอยและพยานหลักฐานไว้ในสถานที่นั้นเสมอเป็นกฎตายตัว ไม่มีการก่ออาชญากรรมใดที่คนร้ายจะทำลายหลักฐานได้อย่างหมดจดแนบเนียน เพราะคนเราแต่ละคนมีลักษณะรูปแบบความเคยชินแต่ละคนแตกต่างกัน สิ่งที่คนร้ายอาจจะทิ้งไว้ได้แก่ รอยรองเท้าเปื้อนเลือดที่ปรากฏ เป็นรอยพื้นของรองเท้า ยี่ห้อใด รุ่นใด ผลิตปี พ.ศ.ใด ก็จะมีลักษณะรอยพื้นเป็นลวดลายเหมือนกันทั้งหมด (ขอแบบลายพื้นได้จากบริษัทผู้ผลิต ; ควรนำมาเก็บรวบรวมไว้เป็นระบบเพื่อใช้ในการเปรียบเทียบ)

2.2) คุณลักษณะเฉพาะ (Individual characteristics) คือ ลักษณะที่ปรากฏแตกต่างออกไปจากปกติ เช่น รอยพื้นรองเท้าเปื้อนเลือดที่ปรากฏ มีรอยสึกจากการใส่ใช้งานที่ส้นรองเท้า จะมีลักษณะแตกต่างกันไป แต่ละคู่จะไม่เหมือนกัน

นักพิสูจน์หลักฐานนั้นมีภาระหน้าที่ที่จะต้องศึกษาพยานหลักฐาน ไม่ว่าจะเป็นลายพิมพ์นิ้วมือ ลายพิมพ์นิ้วมือแฝง หรือลูกกระสุนปืนก็ตาม เพื่อที่จะหา Class และ Individual characteristics ออกมา เพื่อเป็นเครื่องพิสูจน์การ Identity ระหว่างพยานวัตถุที่ได้จากสถานที่เกิดเหตุกับวัตถุตัวอย่างที่ทราบแหล่งที่มาแล้ว Class characteristics เป็นรากฐานของการ Identification ส่วน Individual characteristics เป็นสิ่งที่ใช้บอก Identity ตัวอย่างแสดงที่มาของ Class และ Individual characteristics

ประเภทของพยานหลักฐาน	**Characteristics**	
	Class	**Individual**
ของเหลวไม่มีสี	แอลกอฮอลล์	เอธิลแอลกอฮอลล์
วัตถุผงสีขาว	แอลคาลอยด์	เฮโรอีน
สิ่งที่สงสัยว่าเป็นคราบอสุจิ	เมื่อลูบดูแล้วแข็งกระด้างทดสอบแล้วให้ผลบวกกับเอซิดฟอสฟาเตส	ตัวสเปอร์มที่ยังมีชีวิตและสมบูรณ์
ลูกกระสุนปืน	ขนาด, จำนวนร่องเกลียว สันเกลียวและเวียนซ้าย ขวา	ร่องรอยลายเส้นภายในร่องเกลียว
รอยรองเท้า	ลักษณะของพื้น และส้นรองเท้าตลอดจนรุ่น หรือแบบหรือบริษัทผู้ผลิต	ลักษณะการสึกหรอ หรือร่องรอยเสียหายจากการใช้งาน

ตารางที่ 1 ประเภทพยานหลักฐานโดย พัชรา สินลอยมา (2560)

2.3.1.5 การรวบรวมพยานหลักฐาน

การรวบรวมพยานหลักฐานในชั้นสอบสวน เป็นการดำเนินการโดยตรงของพนักงานสอบสวน ซึ่งการรวบรวมพยานหลักฐานของพนักงานสอบสวนมิใช่เพียงเพื่อจะรู้ตัวผู้กระทำผิดและพิสูจน์ให้เห็นความผิดเท่านั้น แต่รวมถึงพยานหลักฐานที่อาจพิสูจน์ถึงความบริสุทธิ์ของผู้ต้องหาได้ด้วย ดังนั้น ความหมายและพยานหลักฐานในคดีอาญา การรวบรวมพยานหลักฐาน รวมทั้งการรับฟังพยานหลักฐานปรากฏรายละเอียด ดังนี้

2.3.1.5.1 ความหมายและพยานหลักฐานในคดีอาญา

พยานหลักฐาน หมายความถึง สิ่งที่สามารถพิสูจน์และสนับสนุนข้อเท็จจริงที่คู่ความแต่ละฝ่ายกล่าวอ้างมาในการดำเนินคดี ซึ่งคู่ความแต่ละฝ่ายจึงมีความจำเป็นที่จะต้องนำพยานหลักฐานมาแสดงพิสูจน์ยืนยันข้อเท็จจริงตามที่ตนกล่าวอ้าง เมื่อการสอบสวนคือการรวบรวมพยานหลักฐานให้อยู่ในรูปแบบของสำนวนการสอบสวน ดังนั้น พยานหลักฐานในสำนวนการสอบสวน จะต้องถูกรวบรวมอย่างมีประสิทธิภาพและประสิทธิผล

พยานหลักฐานในคดีอาญาประกอบด้วย

1) พยานบุคคล หมายความถึง ถ้อยคำของบุคคลที่มาให้การต่อหน้าพนักงานหรือศาล รวมทั้งอากัปกิริยาอาการของคนใบ้ ที่สามารถแสดงออกซึ่งแทนความหมายของถ้อยคำพูด
2) พยานเอกสาร หมายความถึง ข้อความใดๆ ที่สื่อถึงความหมายใดที่เจ้าพนักงานหรือศาลสามารถอ่านหรือตรวจดูได้จากหนังสือ ลายลักษณ์อักษร หรือเครื่องหมาย รูปรอยใดๆ โดยประการที่ว่าเครื่องหมาย รูปรอยนั้นสามารถใช้แทนลายลักษณ์อักษรได้
3) พยานวัตถุ หมายความถึง สิ่งของใดๆที่คู่ความอ้างเป็นพยานหลักฐานในคดี ด้วยความประสงค์ที่จะให้เจ้าพนักงานหรือศาลตรวจดูรูปร่างลักษณะของสิ่งของ หรือวัตถุนั้นเพื่อประโยชน์แก่คดีของตน
4) พยานผู้ชำนาญการพิเศษ หมายความถึง บุคคลผู้มีอาชีพหรือมิใช่ก็ตาม มีความรู้ความชำนาญพิเศษในการใดๆ ซึ่งความเห็นของเขานั้นมีประโยชน์ในการวินิจฉัยคดีได้

2.3.1.5.2 การรวบรวมพยานหลักฐาน

การรวบรวมพยานหลักฐานเป็นหน้าที่ของพนักงานสอบสวนหรือตำรวจ การพิจารณาพยานหลักฐานที่ได้จากการสอบสวนตกเป็นหน้าที่ของพนักงานอัยการ ส่วนศาลยุติธรรมโดยผู้พิพากษาชั่งน้ำหนักพยานหลักฐานของคู่ความที่ได้จากการสอบสวน จึงปฏิเสธไม่ได้ว่า การรวบรวมพยานหลักฐานเป็นสิ่งที่ค่อนข้างยากลำบากที่สุด ซึ่งเป็นหน้าที่ของพนักงานสอบสวนหรือผู้เกี่ยวข้องในการสืบสวนสอบสวน เมื่อกล่าวถึงการสืบสวนหมายความถึงการแสวงหาข้อเท็จจริงและหลักฐานซึ่งพนักงานฝ่ายปกครองหรือตำรวจได้ปฏิบัติไปตามอำนาจหน้าที่ เพื่อรักษาความสงบเรียบร้อยของประชาชน และเพื่อที่จะทราบรายละเอียดแห่งความผิด ดังนั้น ผู้มีอำนาจสืบสวนคือพนักงานฝ่ายปกครองหรือตำรวจ ส่วนการสอบสวน หมายความถึง การรวบรวมพยานหลักฐานและการดำเนินการทั้งหลายอื่นตามบทบัญญัติแห่งประมวลกฎหมายนี้ ซึ่งพนักงานสอบสวนได้ทำไปเกี่ยวกับความผิดที่กล่าวหา เพื่อที่จะทราบข้อเท็จจริงหรือพิสูจน์ความผิดเพื่อจะเอาตัวผู้กระทำผิด มาฟ้องลงโทษ ซึ่ง

เป็นหน้าที่ของพนักงานสอบสวน คือ เจ้าพนักงาน ซึ่งกฎหมายให้มีอำนาจและหน้าที่ทำการสอบสวน ดังนั้น พนักงานสอบสวนจึงเป็นผู้ทำการรวบรวมพยานหลักฐาน ทั้งพยานบุคคล พยานวัตถุ และพยานเอกสาร

กระบวนการสืบสวนและสอบสวน ถึงแม้จะมีความแตกต่างในวัตถุประสงค์และวิธีการก็ตามแต่ต้องควบคู่กันไป ซึ่งการสืบสวนมีทั้งเป็นการดำเนินการก่อนการกระทำความผิดทางอาญาเพื่อรักษาความสงบเรียบร้อย อันเป็นมาตรการเชิงรุกเพื่อตัดวงจรการเกิดของคดีอาญา และเป็นการดำเนินการหลังมีการกระทำความผิดทางอาญาเกิดขึ้นอันเป็นมาตรการเชิงรับ โดยมุ่งเน้นเพื่อแสวงหาข้อเท็จจริงและหลักฐาน และทราบรายละเอียดแห่งการกระทำความผิดที่กล่าวหา ถูกนำมาประกอบเข้ากับการสอบสวนที่พนักงานสอบสวนเป็นผู้ใช้อำนาจตามกฎหมายในการรวบรวมข้อเท็จจริงและหลักฐานที่ได้ เพื่อพิสูจน์ความผิดตามข้อกล่าวหาและเอาตัวผู้กระทำผิด มาฟ้องลงโทษ

การรวบรวมพยานหลักฐานของพนักงานสอบสวน อาจกระทำได้โดยใช้วิธีการ หรือกระบวนการตามหลักทั่วไปว่าด้วยการสอบสวน คือ

1) พยานบุคคล ใช้วิธีบันทึกถ้อยคำของบุคคลนั้น โดยพนักงานสอบสวนรวมเข้าไว้ในสำนวน เช่น คำให้การของผู้กล่าวหา ผู้ต้องหา พยาน เป็นต้น
2) พยานเอกสาร คือ เอกสารต่าง ๆ ที่เป็นประโยชน์ในการสอบสวน เช่น บันทึกการตรวจบาดแผลของแพทย์ บันทึกการตรวจพิสูจน์ของกลางของผู้ชำนาญการพิเศษให้รวมเข้าไปในสำนวน ถ้าสิ่งใดไม่สามารถรวมเข้าสำนวนการสอบสวน ก็ให้ถ่ายภาพรวมเข้าสำนวนได้
3) พยานวัตถุ ได้แก่ วัตถุของกลางที่จะพิสูจน์ความผิด หรือทราบข้อเท็จจริงนำมารวมในสำนวนการสอบสวนไม่ได้ก็ให้ทำบัญชีติดไว้ในสำนวน เช่น มีด ไม้ อาวุธปืน เป็นต้น
4) การดำเนินงานอันจำเป็นของพนักงานสอบสวนเพื่อให้ได้มาซึ่งพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญา ได้แก่ การออกหมายเรียกพยาน การจับกุมผู้กระทำผิด การตรวจค้น การตรวจตัวผู้เสียหาย การตรวจค้นตัวผู้ต้องหา การตรวจสิ่งของ การตรวจสถานที่เกิดเหตุ ถ่ายรูป การจัดทำแผนที่สังเขป วาดภาพ พิมพ์ลายนิ้วมือ พิมพ์ลายเท้า เหล่านี้เป็นต้น ย่อมถือเป็นการสอบสวนรวบรวมพยานหลักฐานทั้งสิ้น เช่น การออกหมายเรียกพยานบุคคลมาบันทึกถ้อยคำ ออกหมายเรียกให้ส่งพยานเอกสารประกอบสำนวนการสอบสวนคดีอาญา หรือขอหมายค้นเพื่อพบหรือยึดพยานวัตถุหรือของกลางประกอบคดี เป็นต้น

การที่จะทำให้การรวบรวมพยานหลักฐานของพนักงานสอบสวนเกิดประสิทธิภาพและประสิทธิผล นั้น ประการแรก คือ ความละเอียดรอบคอบของพนักงานสอบสวนในการรวบรวมพยานหลักฐาน ประการต่อมา ได้แก่ ตัวพยานหลักฐานที่มีอยู่ในสำนวนการสอบสวน ประการที่สาม คือ ความสามารถนำพยานไปเบิกความต่อศาล ทั้งสามประการดังกล่าวจะต้องอยู่บนพื้นฐานของความชอบด้วยกฎหมาย ซึ่งถือว่าเป็นหลักของการสอบสวน ที่จะต้องปฏิบัติตามวิธีการของบทบัญญัติกฎหมายอย่างเคร่งครัด การกระทำที่ขัดต่อหลักกฎหมายย่อมทำให้พยานหลักฐานซึ่งได้มาโดยมิชอบศาลจะไม่รับฟัง หรือกล่าวอีกนัยหนึ่ง เป็นไปตามบทบัญญัติของประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226 “พยานวัตถุ พยานเอกสาร หรือพยานบุคคล (ผู้ชำนาญการพิเศษ) ซึ่งน่าจะพิสูจน์

ได้ว่าจำเลยมีความผิดหรือบริสุทธิ์ ให้อ้างเป็นพยานหลักฐานได้ แต่ต้องเป็นพยานชนิดที่มิได้เกิดขึ้นจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบประการอื่น และให้สืบตามบทบัญญัติแห่งประมวลกฎหมายนี้ หรือกฎหมายอื่น ๆ ด้วยการสืบพยาน”

คดีอาญา การรวบรวมพยานหลักฐานเป็นหน้าที่ของพนักงานสอบสวน ที่จะต้องรวบรวมพยานหลักฐานให้เป็นไปตามประมวลกฎหมายวิธีพิจารณาความอาญา คือ

1) การรวบรวมพยานหลักฐานจะชอบด้วยกฎหมาย ก็ต่อเมื่อการนั้นได้กระทำโดยพนักงานสอบสวน และพนักงานสอบสวนจะต้องมีเขตอำนาจที่จะสอบสวนรวบรวมพยานหลักฐานคดีนั้น ๆ ได้ การรวบรวมพยานหลักฐานใดที่ไม่ได้เป็นไปตามนัยดังกล่าวย่อมเป็นการไม่ชอบ และอาจถือไม่ได้ว่ามีการสอบสวนรวบรวมพยานหลักฐานแล้ว

2) การสอบสวนรวบรวมพยานหลักฐานถือเป็นเงื่อนไขสำคัญในการ ยื่นฟ้องคดีของพนักงานอัยการ ถ้ายังไม่มีการสอบสวนของพนักงานสอบสวนก็ยังฟ้องคดีอาญาไม่ได้ การสอบสวนรวบรวมพยานหลักฐานจึงถือเป็นหัวใจของการดำเนินคดีอาญา ฉะนั้นการสอบสวนรวบรวมพยานหลักฐานจึงต้องทำด้วยความบริสุทธิ์ยุติธรรม สอดคล้องกับหลักกฎหมายที่บัญญัติและจะต้องมีประสิทธิภาพในการจัดการกับผู้กระทำผิด เพื่อส่งผลต่อการควบคุมอาชญากรรมในกระบวนการยุติธรรม

3) การสอบสวนรวบรวมพยานหลักฐานเป็นการให้อำนาจแก่พนักงานสอบสวนในการปฏิบัติหน้าที่ตามบทบัญญัติของกฎหมายที่กระทบต่อสิทธิเสรีภาพของบุคคลโดยตรงหลายประการ อาทิ อำนาจในการตรวจตัวผู้ต้องหา การค้นพบสิ่งของที่มีไว้เป็นความผิด การจับ การควบคุม เป็นต้น

<u>พยานวัตถุ (Physical evidence)</u>

คำนิยามของ “พยานหลักฐาน” หมายถึง สิ่งใดที่สามารถจับต้องได้ตามกฎหมาย และเป็นสิ่งที่สามารถนำเสนอในชั้นศาลเพื่อพิสูจน์ถึงข้อเท็จจริงในคดีได้ ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226 “พยานหลักฐาน” หมายถึง พยานหลักฐาน เอกสารหรือพยานบุคคล ตลอดจนหลักฐานอื่นๆ ซึ่งอาจเป็นเครื่องพิสูจน์การกระทำผิดได้ ตัวอย่างเช่น

- บุคคลผู้ใดได้รู้เห็นพฤติกรมในการกระทำผิดของคนร้าย ถือเป็นพยานบุคคล
- เอกสารต่างๆ ที่ได้กระทำขึ้นโดยชอบ หรือมิชอบด้วยกฎหมายก็ดีและกระทำขึ้นโดยผู้ร้ายหรือบุคคลหนึ่งบุคคลใดก็ตาม คือเป็นพยานเอกสาร
- วัตถุต่างๆ ที่คนร้ายใช้เป็นเครื่องมือในการกระทำผิด ซึ่งตรวจพบในสถานที่เกิดเหตุ คือเป็นพยานวัตถุ

โอกาสที่คนจะประกอบความผิดโดยไม่ทิ้งร่องรอยพยานหลักฐานไว้นั้น เป็นไปได้ยากมาก ในกรณีปกติพยานหลักฐานที่จะช่วยในการนำคนผิดไปฟ้องลงโทษได้นั้นจะเป็นพยานบุคคลเสียเป็นส่วนใหญ่ นั่นก็คืออาชญากรถูกชี้ตัวโดยผู้เสียหาย พยานผู้รู้เห็นเหตุการณ์หรือจากคำรับสารภาพของตัวผู้กระทำผิดเอง ดังนั้นจะเห็นว่า แนวทางการสืบสวนของเจ้าหน้าที่ตำรวจ จะมุ่งหาพยานบุคคลก่อนเป็นอันดับแรก เพราะเป็นสิ่งที่หาได้โดยง่ายและความรู้ความสามารถของพนักงานสอบสวนในอันที่จะเค้นเอาความจริงหรือเจรจาหว่านล้อมให้พยานทบทวนเหตุการณ์ที่พบเห็นมาเป็นสิ่งที่พนักงานสอบสวนได้รับการถ่ายทอด ฝึกฝนและปลูกฝังติดต่อกันมาหลายยุคหลายสมัยแล้ว แต่มีหลายครั้งที่ไม่สามารถหาพยานบุคคลมาใช้ได้ อย่างเช่นกรณีคนร้ายฆ่าเจ้าทุกข์จนถึงแก่ความตาย และในคดีกระทำความผิดต่อทรัพย์ที่เกิดขึ้นตอนค่ำคืนปราศจากผู้รู้เห็น เป็นต้น พยานที่

พนักงานสอบสวนจะหาได้กรณีนี้ ก็มีเพียงแต่พยานวัตถุเท่านั้น ซึ่งในปัจจุบันนี้สำนักงานตำรวจแห่งชาติ ได้ให้ความสำคัญกับพยานวัตถุมากขึ้น เนื่องจากเทคโนโลยีทางวิทยาศาสตร์ที่เจริญก้าวหน้าขึ้น อุปกรณ์เครื่องมือวิทยาศาสตร์ต่างๆ มีขีดความสามารถในการตรวจพิสูจน์สูง ไม่ว่าจะเป็นเครื่อง Scanning electron microscope (SEM) ที่สามารถตรวจวิเคราะห์พยานวัตถุในเชิงกายภาพได้ถึงระดับโมเลกุล หรือเทคนิค Polymerase chain reaction (PCR) ที่สามารถวิเคราะห์รหัสพันธุกรรมได้จากพยานวัตถุประเภทที่มาจากร่างกายมนุษย์ ถึงแม้พยานวัตถุนั้นจะมีปริมาณเล็กน้อยเท่าหัวเข็มหมุดก็ตาม นอกจากนั้นพยานวัตถุยังเป็นสิ่งที่มีความเป็นรูปธรรมสามารถพิสูจน์ให้เห็นจึงถือเป็นพยานหลักฐานที่รับการยอมรับในชั้นศาลมากที่สุด

เมื่อกล่าวถึงพยานวัตถุ เราไม่สามารถให้คำจำกัดความง่ายๆ สั้นๆ แต่ได้ใจความถูกต้องที่สุดได้ เพราะเกือบทุกสิ่งทุกอย่างหากอยู่ในสภาวะที่เหมาะสม ก็สามารถกลายสภาพเป็นพยานวัตถุได้ ทั้งนั้น ไม่ว่าจะอยู่ในสถานะของแข็ง ของเหลว หรือก๊าซก็ตาม สิ่งใดที่สามารถใช้พิสูจน์ได้ว่ามีการกระทำผิดเกิดขึ้น ใช้บอกได้ว่าใครเป็นผู้กระทำผิด และสามารถเชื่อมโยงผู้กระทำผิด เข้ากับอาชญากรรมได้ก็ถือได้ว่าสิ่งนั้นเป็นพยานวัตถุ บุคคลใดก็ตามที่กระทำความผิดจะหนีไม่พ้นที่ต้องมีกิริยาอย่างใดอย่างหนึ่งไม่ว่าจะเป็นกิริยาชนิดรุนแรงหรือแบบนุ่มนวลก็ตาม เมื่อมีกิริยาเกิดขึ้นก็เป็นไปได้ที่เขาผู้นั้นจะต้องทิ้งบางสิ่งบางอย่างไว้ในสถานที่ที่กระทำผิด หรือนำบางสิ่งบางอย่างจากสถานที่เกิดเหตุติดตัวไปด้วย และสิ่งที่จะยกเป็นตัวอย่างได้ดีที่สุดในกรณีนี้คือรอยลายนิ้วมือเพียงแต่คนร้ายสัมผัสเข้ากับวัตถุสักชิ้นหนึ่งเท่านั้นก็อาจเกิดเป็นพยานวัตถุที่สำคัญบนวัตถุนั้นแล้ว รอยของเครื่องมือจะสามารถใช้มัดตัวผู้กระทำผิด หากพบอุปกรณ์สิ่งที่ใช้ทำให้เกิดร่องรอยนั้นที่ตัวหรือในความครอบครองของผู้ต้องหาหรือผู้ต้องสงสัย

ในกรณีของอาวุธปืน ถ้าถูกพบในความครอบครองของผู้ต้องหา สามารถใช้ผูกมัดตัวเจ้าของปืนกับคดีฆาตกรรมที่เขากระทำลงไปแล้วได้ ถ้าหากว่าร่องรอยที่ปรากฏบนลูกกระสุนปืนที่ผู้ชำนาญยิงทดลองจากปืนของเขา มีลักษณะเหมือนกับร่องรอยที่ลูกกระสุนปืนที่ผ่ามาจากศพผู้ตาย วัตถุสิ่งของบางอย่างที่ผู้กระทำผิดอาจนึกไม่ถึงได้เกิดการแลกเปลี่ยนกันขึ้นระหว่างที่เกิดเหตุกับตัวของผู้กระทำผิด ตัวอย่างเช่น เศษชิ้นส่วนของแก้ว หรือกระจกที่แตกเป็นชิ้นเล็กชิ้นน้อย ขณะคนร้ายทุบประตูหน้าต่างเข้าไปกระทำการโจรกรรม หากพบเศษกระจกฝังอยู่ในบริเวณเสื้อผ้าเครื่องแต่งกายของคนร้าย สามารถนำมาเปรียบเทียบกับชิ้นส่วนที่ยังเหลืออยู่ในสถานที่เกิดเหตุได้ เศษชิ้นสี หรือเส้นผม หรือคราบเลือด น้ำลาย อสุจิ ฯลฯ สามารถนำมาใช้ได้ได้โดยกรรมวิธีเดียวกันนี้

การใช้พยานวัตถุในการสืบสวนสอบสวน จะต้องระลึกอยู่เสมอว่า พยานวัตถุไม่สามารถพิสูจน์เอกลักษณ์ในตัวของมันเองได้อย่างเด็ดขาดแน่นอน แต่ส่วนใหญ่จะให้ความมั่นใจภายในขอบเขตของความเป็นได้พอสมควรเท่านั้น แม้แต่ลายนิ้วมือซึ่งเชื่อกันว่าจะใช้พิสูจน์เอกลักษณ์ของบุคคลได้นั้น แท้ที่จริงแล้วยังต้องอาศัยหลักที่ว่าโอกาสที่คนสองคนจะมีลักษณะของลายเส้นนิ้วมือตรงกันทั้งหมดนั้นจะมีเปอร์เซ็นต์น้อยมาก เช่น ถ้าตรงกัน 1 จุดบนลายนิ้วมือจะเป็นไปได้ในอัตราส่วน 1:20 หากจะให้พบตรงกัน 2 จุดก็จะกลายเป็น 1:20 x 20 หรือ 1:400 และถ้าตรวจพบว่าลายนิ้วมือ 2 ลายมือจุดลักษณะสำคัญตรงกันตั้งแต่ 8-12 จุดแล้ว โอกาสที่จะพบคนสองคนมีลายนิ้วมือตรงกันเช่นนั้น จะกลายเป็น 1:15,000,000,000 ซึ่งมากกว่าจำนวนประชากรโลกหลายเท่า

และจากรายงานขององค์การตำรวจทั่วโลกยังไม่เคยปรากฏว่าพบบุคคลคู่ใดที่มีลายนิ้วมือตรงกันขนาดนั้นเลย ทุกประเทศจึงใช้ 8-12 จุด เป็นเกณฑ์ในการพิสูจน์ลายนิ้วมือ

ประเภทของพยานหลักฐาน

พยานหลักฐาน แบ่งเป็น 3 ประเภท ได้แก่

1) พยานหลักฐานโดยตรง (Direct evidence) พยานประเภทนี้ ได้แก่ พยานบุคคลหรือประจักษ์พยานที่รู้เห็นเหตุการณ์ที่เกิดขึ้นด้วยตนเอง โดยอาจรับรู้ด้วยประสาทตา หู จมูก สัมผัสหรือลิ้นรส มิใช่ได้ยินได้ฟังมาจากผู้อื่นอีกทอดหนึ่ง
2) พยานแวดล้อมกรณี (Circumstantial evidence) หรือพยานหลักฐานทางอ้อม เป็นพยานหลักฐานที่ไม่สามารถพิสูจน์ข้อเท็จจริงได้โดยตรง แต่สามารถนำมาปะติดปะต่อให้เกิดความคิด ลำดับหรือเชื่อมโยงเหตุการณ์ได้ เพื่อบอกถึงข้อเท็จจริงบางอย่างหรือหลายอย่าง ซึ่งนำมาใช้คลี่คลายปัญหาในคดีได้
3) พยานหลักฐานที่แท้จริง (Real evidence) ได้แก่ พยานวัตถุที่มีความชัดแจ้งในตัวเอง เป็นพยานหลักฐานที่มีความสำคัญที่สุดและสามารถนำไปใช้เพื่อยืนยันการกระทำผิดในคดีนั้นๆ ได้โดยตรงหรือนำไปเชื่อมโยงเกี่ยวพันกับคดีได้ เช่น คราบเลือด คราบอสุจิ เส้นผม เส้นขน รอยลายนิ้วมือ เส้นใยผ้าและอาวุธอื่นๆ ฯลฯ

อาจกล่าวได้ว่าพยานหลักฐาน หมายถึง สิ่งใดๆ ที่สามารถใช้พิสูจน์ได้ว่ามีการกระทำผิดเกิดขึ้น ใช้บอกได้ว่าใครเป็นผู้กระทำความผิด และสามารถเชื่อมโยงผู้กระทำความผิดเข้ากับอาชญากรรมที่เกิดขึ้นได้ พยานหลักฐานจึงประกอบด้วย พยานบุคคล พยานเอกสาร และพยานวัตถุ ดังที่บัญญัติไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226 “พยานวัตถุ พยานเอกสาร และพยานบุคคลซึ่งน่าจะพิสูจน์ได้ว่าจำเลย มีความผิดหรือบริสุทธิ์ ให้อาจเป็นพยานหลักฐานได้ แต่ต้องเป็นพยานชนิดที่มิได้เกิดขึ้นจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวงหรือโดยมิชอบประการอื่น และให้สืบตามบทบัญญัติแห่งประมวล กฎมายนี้หรือกฎมายอื่นว่าด้วยกรสืบพยาน”

ในทางทฤษฎี “สถานที่เกิดเหตุ” เริ่มต้น ณ จุดที่ผู้กระทำความผิดเริ่มกระทำไปจนถึงบริเวณที่ผู้กระทำความผิดหลบหนีไป รวมทั้งบริเวณที่มีวัตถุพยานต่างๆอยู่ด้วย แต่ในทางปฏิบัติเป็นการยากที่จะระบุลงไปได้ชัดๆ ว่าขอบเขตของสถานที่เกิดเหตุนั้นอยู่ตรงไหน ดังนั้น สถานที่เกิดเหตุจึงประกอบไปด้วยสถานที่ต่างๆที่เกี่ยวข้องกับเหตุการณ์นั้นรวมๆกัน ได้แก่ บริเวณที่พบศพ บริเวณที่ศพถูกเคลื่อนย้าย บริเวณที่พบวัตถุพยาน และรวมถึงบริเวณที่เกี่ยวข้องเนื่องด้วย เช่น บริเวณที่ผู้กระทำความผิดเข้ามาหาผู้ตาย บริเวณที่ผู้กระทำความผิดหลบหนีไป และบริเวณที่พักของผู้กระทำความผิดด้วย เป็นต้น

แต่ปกติแล้ว เรามักจะเริ่มจากบริเวณที่เหตุเกิดหรือบริเวณที่พบศพก่อน ถือเป็น Primary crime scene แล้วจึงขยายวงกว้างออกไป ในทางปฏิบัติพนักงานสอบสวนจะเป็นผู้รับผิดชอบในการกำหนดและตรวจสถานที่เกิดเหตุ ผู้เชี่ยวชาญการตรวจพิสูจน์ทางชีววิทยาจะเข้าไปมีบทบาทก็ต่อเมื่อพนักงานสอบสวนได้ร้องขอให้เข้าไปร่วมหรือช่วยทำการตรวจเก็บพยานหลักฐานทางชีววิทยาต่างๆ หรืออาจขอความเห็นว่าบริเวณนั้นเป็นสถานที่เกิดเหตุหรือเกี่ยวข้องกับเหตุที่เกิดขึ้นนั้นหรือไม่อย่างไร เพื่อนำความเห็นของผู้ชำนาญการพิสูจน์ไปใช้ในแนวทางการสืบสวนสอบสวน เพราะสถานที่เกิดเหตุโดยสภาพแล้วก็คือพยานวัตถุชนิดหนึ่งนั่นเอง

ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 16 มาตรา 17 มาตรา 18 และมาตรา 132 กำหนดให้พนักงานสอบสวนมีอำนาจสอบสวน และมีหน้าที่ในการรวบรวมพยานหลักฐาน กับการดำเนินการทั้งหลายอื่น ซึ่งหมายความรวมถึง การจดบันทึก ถ่ายภาพ ทำแผนที่สถานที่เกิดเหตุและการกระทำอื่นๆ เพื่อให้ได้ตัวผู้กระทำความผิดมาฟ้องลงโทษทางอาญา

แต่อย่างไรก็ตาม ผู้ชำนาญการตรวจพิสูจน์วัตถุพยานแขนงต่างๆ หรือผู้ชำนาญการ เฉพาะทางที่จะต้องเข้าไปมีส่วนร่วมในการตรวจสถานที่เกิดเหตุ ก็ควรรอบรู้ถึงข้อกฎหมาย ระเบียบ ข้อกำหนดและบทบาทการมีส่วนร่วมของตน โดยเฉพาะควรรับทราบรายละเอียดเกี่ยวกับสถานที่เกิดเหตุและพฤติกรรมการกระทำผิดที่ปรากฏในเบื้องต้น เพื่อเป็นข้อมูลในการพิจารณาเกี่ยวกับรายละเอียดต่างๆ ของวัตถุพยานรวมถึงการพิจารณาความสัมพันธ์เชื่อมโยงกับเหตุการณ์ได้อย่างเหมาะสมตามสภาพความเป็นจริง ซึ่งจะช่วยให้การปฏิบัติหน้าที่เป็นไปอย่างรวดเร็ว ถูกต้อง เหมาะสม และมีประสิทธิภาพยิ่งขึ้น และเป็นที่พึ่งของพนักงานสืบสวนสอบสวนได้ในสภาวการณ์ที่เร่งรีบในการพิสูจน์ทราบถึงการกระทำความผิด รวมถึงการหาตัวหรือยืนยัน ตัวผู้กระทำผิด

<u>ชนิดของพยานวัตถุ</u>

พยานวัตถุ แบ่งตามลักษณะการเก็บออกได้เป็น 2 ชนิด

1) พยานวัตถุที่เคลื่อนย้ายไม่ได้ (Fixed of immovable evidence) เป็นพยานวัตถุที่มีขนาดใหญ่, น้ำหนักมาก หรือถ้าเคลื่อนย้ายอาจทำให้คุณสมบัติบางอย่างเปลี่ยนไป เช่น ผนัง, เตาผิง, รอยประทับยางรถยนต์ เป็นต้น พยานวัตถุชนิดนี้จะใช้วิธีเกิดรักษาโดยการถ่ายภาพ วาดรูปเหมือนตามมาตราส่วนของจริง หล่อปูนพลาสเตอร์ เป็นต้น
2) พยานวัตถุที่เคลื่อนย้ายได้ (Movable evidence) เป็นวัตถุพยานที่มีขนาดเล็ก มีน้ำหนักเบา สามารถเคลื่อนย้ายได้โดยไม่ทำให้คุณสมบัติเปลี่ยนไป เช่น กระป๋อง เก้าอี้ ของเหลว ชิ้นส่วนพรม เป็นต้น

ก่อนที่จะทำความเข้าใจถึงบทบาทและประโยชนที่แท้จริงของพยานหลักฐานแต่ละประเภท ควรเข้าใจเกี่ยวกับศัพท์และกฎเกณฑ์ที่ว่าด้วยพยานวัตถุให้ถ่องแท้เสียก่อน เพื่อจะได้นำพยานหลักฐานที่ได้มาในระหว่างการสืบสวนสอบสวนไปใช้ให้เป็นประโยชน์ให้ได้มากที่สุด ซึ่งสิ่งเหล่านี้ได้แก่กฎแห่งพยานหลักฐาน (Law of evidence) ประกอบด้วยกฎหมายที่เกี่ยวข้องกับการสืบสวนสอบสวน มีหัวใจสำคัญอยู่ 2 ประเด็นด้วยกันคือความเป็นสาระสำคัญ (Materiality) และการยอมรับฟัง (Admissibility) ยกตัวอย่างเช่น นายแดงถูกกล่าวหาว่า ฆ่าคนตายโดยใช้มีดแทง พยานยืนยันว่าเห็นนายแดงซื้อมีดมาจากร้าน พร้อมทั้งบอกคนขายว่าจะเข้าไปแทงคน และมีผู้เห็นนายแดงเดินมุ่งหน้าไปยังสถานที่เกิดเหตุ อย่างนี้ถือว่าพยานหลักฐานนั้นเป็นสาระสำคัญและการยอมรับฟังได้ (Material admissible) ในทางตรงกันข้าม สมมติว่านายดำ ถูกกล่าวหาว่าฆ่าคนตายโดยใช้อาวุธปืนยิง อาวุธปืนย่อมนำมาเป็นพยานวัตถุได้ เพราะเป็นสาระสำคัญ แต่จะนำหลักฐานที่ว่านายดำเป็นนักแม่นธนูมีความสามารถสูงมากมาประกอบการฟ้องคดี ปกติแล้วยอมทำไม่ได้เพราะหลักฐานนี้ไม่เกี่ยวกับสาระสำคัญของเรื่องนี้ แต่ถ้าหากปัญหาของคดีนี้ อยู่ที่ความแม่นยำทางธนูของคนร้ายก็ย่อมนำพยานหลักฐานดังกล่าวมาใช้ได้เหมือนกัน

การที่พยานหลักฐานจะเป็นที่ยอมรับใช้ในชั้นศาลได้ จะต้องปฏิบัติตามกฎเกณฑ์พื้นฐาน 4 ประการ การหลีกเลี่ยงหรือปฏิบัติเบี่ยงเบนไปจากกฎเกณฑ์พื้นฐาน 4 ประการ นี้จะเป็นจุดอ่อนให้ทนายสามารถโต้แย้งในชั้นศาลทำให้คุณค่าของพยานหลักฐานสูญเสียไป

กฎข้อที่ 1 “ป้องกันรักษาสถานที่เกิดเหตุ”

ป้องกันรักษาสถานที่เกิดเหตุ เริ่มต้นตั้งแต่เมื่อเจ้าหน้าที่ตำรวจคนแรก (เจ้าหน้าที่ดับเพลิงหรือเจ้าหน้าที่ตำรวจในท้องที่) ไปถึงสถานที่เกิดเหตุจนกระทั่งเจ้าหน้าที่ผู้ชำนาญ(แพทย์, เจ้าหน้าที่กองพิสูจน์หลักฐาน) ทำการตรวจสถานที่เกิดเหตุเสร็จสิ้น

กฎข้อที่ 2 “เก็บพยานหลักฐานอย่างถูกต้องตามกฎหมาย”

หมายถึง บุคคลที่ทำการเก็บพยานหลักฐานนั้น จะต้องเป็นบุคคลที่กฎหมายให้อำนาจไว้ในการเข้าและเก็บพยานวัตถุต่างๆ ในสถานที่เกิดเหตุได้ตัวอย่างเช่น พนักงานสอบสวน, เป็นเจ้าหน้าที่กองพิสูจน์หลักฐานหรือเจ้าหน้าที่วิทยาการตำรวจ เป็นต้น

กฎข้อที่ 3 “กระทำการค้นหาพยานหลักฐานอย่างเหมาะสม”

ผู้ตรวจสถานที่เกิดเหตุจะต้องไม่มองข้ามหรือละเลยพยานวัตถุทุกชิ้น ถ้าสงสัยว่าสิ่งนั้นจะเป็นพยานวัตถุหรือไม่ให้ทำการเก็บไว้ก่อน พร้อมทั้งระบุรายละเอียดของพยานวัตถุตำแหน่งที่พบและบรรจุในหีบห่อรักษาไว้อย่างเหมาะสม

กฎข้อที่ 4 “มีห่วงโซ่การครอบครองพยานหลักฐานโดยตลอด”

หมายถึงว่าพยานนั้นต้องอยู่ในการคุ้มครองดูแลของบุคคลหรือหน่วยงาน ตั้งแต่เริ่มเก็บจนกระทั่งแสดงในชั้นศาลโดยไม่ขาดช่วงการครอบครองเลย ถ้ามีการเปลี่ยนแปลงการครอบครอง เช่น ส่งของกลางไปตรวจพิสูจน์ยังห้องปฏิบัติการ จะต้องมีหลักฐานแสดงการรับส่งของกลางนั้นโดยตลอด

เมื่อใดมีการนำพยานหลักฐานไปแสดงในชั้นศาลจะต้องมีการตรวจสอบดังนี้

1) พยานหลักฐานนั้นเป็นอันเดียวกันกับที่พบในสถานที่เกิดเหตุหรือไม่
2) สิ่งที่เป็นสาระสำคัญของพยานหลักฐานนั้นจะต้องไม่เปลี่ยนแปลง และมีสภาพเหมือนกับตอนที่เก็บจากสถานที่เกิดเหตุ

โดยทั่วไปแล้วขั้นตอนการตรวจสอบพยานหลักฐานในชั้นศาล สามารถกระทำได้โดยง่าย โดยบุคคลที่เป็นผู้พบพยานหลักฐานนั้นในสถานที่เกิดเหตุ แต่ในบางกรณีที่มีบุคคลหรือหน่วยงานครอบครองพยานหลักฐานมากกว่าหนึ่ง เช่น เมื่อนำพยานวัตถุส่งตรวจพิสูจน์ยังห้องปฏิบัติการ ศาลจะต้องให้แสดงลูกโซ่แห่งการครอบครองวัตถุพยาน ซึ่งประกอบไปด้วย

1) การจัดการ (Taking) กระทำโดยบุคคลผู้เก็บพยานวัตถุเพื่อจำแนกพยานวัตถุในสถานที่เกิดเหตุโดยการทำตำหนิ ระบุวัน เดือน ปี เวลาที่เก็บ พร้อมทั้งรายละเอียดต่าง ๆ ของพยานวัตถุนั้นจากสถานที่เกิดเหตุจริง
2) การเก็บ (Keeping) พิสูจน์ให้เห็นว่าการเก็บและครอบครองพยานวัตถุได้กระทำอย่างเหมาะสม เพื่อไม่ให้เกิดการปนเปื้อนหรือผิดพลาดขึ้น วิธีการที่ดีที่สุด คือแสดงให้เห็นว่าพยานวัตถุนั้นได้ถูกเก็บอย่างถูกต้องตามหลักวิชาการ มีการแยกเก็บและจำกัดให้เกี่ยวข้องได้เฉพาะผู้ที่จำเป็นเท่านั้น

3) การขนส่ง (Transporting) การขนส่งวัตถุพยานทุกครั้ง จะต้องมีความรัดกุมและแสดงให้เห็นว่า ไม่เกิดการสับสนกับของกลางหรือพยานวัตถุอื่นๆ รวมถึงแสดงให้เห็นถึงว่า พยานวัตถุนั้นได้ถูกบรรจุ หีบห่อ ปิดผนึก และติดฉลากได้อย่างเหมาะสม
4) การส่งมอบ (Delivering) เป็นการตรวจพิสูจน์ว่า ของกลางได้ส่งมอบให้แก่ผู้รับ (เจ้าหน้าที่ผู้ชำนาญในห้องปฏิบัติการ แพทย์ หรือหน่วยงานอื่น) อย่างถูกต้องและเหมาะสม โดยมีหลักฐาน แสดงวัน เดือน ปี เวลา ที่รับของกลาง รายละเอียดของของกลาง และให้ผู้รับลงลายมือชื่อ พร้อมทั้ง วัน เวลา ไว้ในสำเนาหนังสือนำส่ง

สรุปได้ว่าพยานหลักฐานทางนิติวิทยาศาสตร์เป็นพยานหลักฐานที่มีน้ำหนักและมีความสำคัญแต่ไม่อาจปฏิเสธได้เช่นกันว่าเป็นพยานหลักฐานที่เปิดโอกาสให้มีการตั้งข้อสงสัยได้ ผู้พิพากษาที่ทำหน้าที่ในศาล ต้องทำหน้าที่ในการชั่งน้ำหนักพยานหลักฐานทางวิทยาศาสตร์โดยพิจารณาจากความเกี่ยวข้องกับประเด็นข้อพิพาทและความน่าเชื่อถือของพยานหลักฐานทางวิทยาศาสตร์นั้น ในบางกรณีการนำเสนอพยานหลักฐานทางวิทยาศาสตร์ พนักงานอัยการและจำเลยจะมีการนำสืบพยานผู้เชี่ยวชาญ ซึ่งผู้พิพากษาต้องพิจารณาว่าคดีมีความยุ่งยากซับซ้อนมากน้อยเพียงใด สมควรหรือไม่ที่ศาลจะตั้งพยานผู้เชี่ยวชาญที่เป็นกลางของตนเอง อีกทั้งผู้เชี่ยวชาญนี้รอบรู้จริงหรือไม่ แต่อย่างไรก็ดีคดีที่มีความยุ่งยากและเกี่ยวข้องกับวิทยาศาสตร์ พยานหลักฐานวิทยาศาสตร์เหล่านี้ เป็นเพียงพยานหลักฐานประเภทหนึ่งของพยานหลักฐานทั้งหมดเท่านั้น ซึ่งผู้พิพากษาสามารถตั้งคำถามหรือข้อสงสัยในความน่าเชื่อถือได้ อีกทั้งน้ำหนักความน่าเชื่อถือของพยานหลักฐานทางนิติวิทยาศาสตร์อันสำคัญขึ้นอยู่กับ (1) เครื่องมือและวิธีการ (2) การตัดสินใจ และ (3) การตีความหมาย เป็นสำคัญ

2.3.2 การตรวจพิสูจน์พยานหลักฐานดิจิทัล[14]

การตรวจพิสูจน์พยานหลักฐานดิจิทัล ในประทศไทยยังคงเป็นเรื่องใหม่ แต่แนวโน้มและความสำคัญกำลังเพิ่มมากขึ้น ปัจจุบันจะพบว่า มีบริษัทที่โฆษณาการให้บริการด้านการตรวจพิสูจน์พยานหลักฐานดิจิทัลมากขึ้น มีคอร์สฝึกอบรม และเว็บบล็อกที่ให้ความรู้จากทั้งในประเทศและจากต่างประเทศ แต่หลายคน ก็ยังไม่ทราบความหมายที่แท้จริงของคำว่า Digital forensics หรือ การตรวจพิสูจน์พยานหลักฐานดิจิทัล ซึ่งเราสามารถทำความเข้าใจง่ายๆ ได้ว่า คือการรวบรวมข้อมูลหลักฐาน การพิสูจน์หลักฐานทางคอมพิวเตอร์และอุปกรณ์ทางอิเล็กทรอนิกส์ ซึ่งสามารถนำมาใช้เป็นหลักฐานได้ ในทางการตรวจพิสูจน์พยานหลักฐานดิจิทัล หลักฐานที่ได้จะไม่มีการเปลี่ยนแปลง ซึ่งถ้ามีความจำเป็นที่จะต้องมีการเปลี่ยนแปลงก็จะต้องมีการเปลี่ยนแปลงน้อยที่สุด โดยจะต้องมีการบันทึกกระบวนการได้มาของหลักฐานอย่างเที่ยงตรง

การตรวจพิสูจน์พยานหลักฐานดิจิทัล ไม่เพียงแต่เป็นการสืบสวนข้อมูลทางอิเล็กทรอนิกส์ แต่ยังเป็นการระบุข้อมูลที่เกี่ยวข้องกับการสืบสวนค้นหาหลักฐานเพื่อนำเสนอประกอบการดำเนินคดี ดังนั้นจึงมีความจำเป็นที่คนทั่วไปจะต้องทำความเข้าใจว่า ข้อมูลเหล่านี้ ไม่ได้หมายถึงเฉพาะข้อมูลในคอมพิวเตอร์ แต่ยังรวมไปถึงอุปกรณ์ที่สามารถจัดเก็บข้อมูลทางอิเล็กทรอนิคส์ เช่น โทรศัพท์มือถือ

---

[14] “การตรวจพิสูจน์พยานหลักฐานทางดิจิทัลหรือคอมพิวเตอร์”, www.orionforensics.com, สืบค้นเมื่อ 14 ก.พ. 61, http://www.orionforensics.com/w_th_page/digital-forensics_th.php

กล้องถ่ายรูป อุปกรณ์รับสัญญาณดาวเทียม (GPS) อุปกรณ์จัดเก็บข้อมูล USB เครื่องเล่นเกม หรือแม้แต่เตาอบไฟฟ้า ซึ่งหลายคนอาจคาดไม่ถึง

เพื่อพิจารณาการสื่อสารข้อมูลในปัจจุบันจะพบว่า เป็นการสื่อสารข้อมูลในรูปของข้อมูลอิเล็กทรอนิกส์ จึงเห็นได้ว่า ทำไมการตรวจพิสูจน์พยานหลักฐานดิจิทัล จึงเป็นเครื่องมือที่สำคัญต่อธุรกิจในปัจจุบัน จากการสำรวจ Global economic crime survey 2011 พบว่า อาชญากรรมคอมพิวเตอร์เป็นหนึ่งในอาชญกรรมทางเศรษฐกิจที่มีความสำคัญและมีการรายงานว่า 1 ใน 10 ของการทุจริตที่เกิดขึ้นในองค์กรซึ่งมีความสูญเสียกว่า 5 ล้านดอลล่าสหรัฐ ซึ่งความเสียหายทางชื่อเสียงคือสิ่งที่ผู้คนหวั่นกลัวที่สุดคิดเป็น 40% ของผู้ตอบแบบสอบถาม และมากกว่า 56% ตอบว่าการทุจริตที่ร้ายแรงที่สุดคือ “ภายในองค์กร” การสำรวจยังแสดงให้เห็นว่า 60% ของผู้ตอบแบบสอบถาม ตอบว่าองค์กรไม่ได้มีกฎข้อห้ามในการใช้เครือข่ายสังคม สุดท้าย 34% ของผู้ตอบแบบสอบถามมีประสบการณ์อาชญกรรมทางเศรษฐกิจในช่วง 12 เดือนที่ผ่านมา ซึ่งเพิ่มขึ้นจากเดือนจากปี 2009 กว่า 30% นอกจากนี้ 2 ใน 5 ของผู้ตอบแบบสอบ กล่าวว่า ไม่เคยได้รับการอบรมใดๆเกี่ยวกับ ความปลอดภัยด้านอาชญกรรมคอมพิวเตอร์

เป็นสิ่งที่น่าแปลกใจ เมื่อพิจารณาว่าโลกของเราก้าวไปอย่างรวดเร็ว องค์กรต่างๆ ต้องพึ่งพาเทคโนโลยีมากขึ้นและการแข่งขันทางด้านเทคโนโลยีที่สูงมากขึ้นตามไปด้วย องค์กรส่วนใหญ่ย่อมคาดหวังที่จะนำเสนอข้อมูลเพื่อดึงดูดลูกค้าผ่านทางเว็บไซต์ และทำให้ลูกค้าสามารถตอบสนองได้อย่างรวดเร็วผ่านผ่านทางการสนทนาออนไลน์ และยังสามารถสั่งซื้อสินค้าได้อย่างปลอดภัยผ่านทางการบริการออนไลน์ของเว็บ จึงเห็นได้ว่าเทคโนโลยีได้กลายมาเป็นส่วนหนึ่งในชีวิตของผู้คนสมัยนี้ ซึ่งคนทั่วไปสามารถเข้าถึงอีเมลล์ส่วนตัวเพื่อให้สามารถติดต่อกับบุคคลอื่นแม้ในช่วงเวลาทำงาน

สิ่งต่างๆ ที่กล่าวมามีผลกระทบต่อองค์กรอย่างไร? องค์กรจะต้องเผชิญกับเหตุการณ์ที่เกี่ยวข้องกับระบบความปลอดภัยขององค์กรและบางองค์กรไม่ได้เตรียมการล่วงหน้าสำหรับการปกป้องข้อมูลขององค์กรที่เป็นความลับอย่างมีประสิทธิภาพ องค์กรทราบดีว่าพวกเขาต้องมีระบบป้องกันข้อมูลรั่วไหลภายในองค์กร เช่น การมีไฟร์วอลล์, ติดตั้งตัวปรับปรุงข้อมูลล่าสุดของโปรแกรมป้องกันไวรัส อย่างไรก็ตามหลายองค์กรไม่สามารถใช้นโยบายควบคุมการใช้คอมพิวเตอร์ เช่น การนำอุปกรณ์ USB มาใช้ในองค์กร ซึ่งพนักงานอาจจะทำสำเนาข้อมูลของบริษัทออกไปได้ ถึงแม้องค์กรจะมีนโยบายการปิดอีเมลล์และป้องกันการเข้าถึงข้อมูลองค์กรเมื่อพนักงานคนนั้นลาออก แต่ก็ไม่สามารถป้องกันข้อมูลบริษัทรั่วไหลไปได้

ทุกองค์กรในทุกอุตสาหกรรมทั้งในประเทศไทยและต่างประเทศ ต่างก็มีนโยบายในการเข้าถึงข้อมูลที่เป็นความลับขององค์กรและข้อมูลของลูกค้า เพื่อที่จะปกป้องการขโมยข้อมูลออกจากองค์กร แต่การรั่วไหลของข้อมูลยังคงเป็นหนึ่งในปัญหาที่ใหญ่ที่สุดที่องค์กรต้องเผชิญในโลกเทคโนโลยีทุกวันนี้ ถ้าภาคธุรกิจในประเทศไทยปราถนาที่จะแข่งขันในระดับโลก องค์กรเหล่านี้ควรจะต้องมีความสามารถในการรับมือหรือจัดการกับอาชญกรรมคอมพิวเตอร์ได้ การรักษาข้อมูล กลายเป็นปัญหาใหญ่สำหรับองค์กรที่ไม่มีการวางแผนการจัดการกับอาชญกรรมคอมพิวเตอร์ ซึ่งอาจทำให้พลาดการทำสัญญาทางการค้ากับบริษัทขนาดใหญ่ได้ ดังที่มีผู้กล่าวไว้ว่า “การคาดการณ์ในอนาคตจะผิดพลาด เมื่อมันได้มาถึงตัวอย่างไม่คาดคิด”

ตัวอย่างของอาชญากรรมคอมพิวเตอร์ ได้แก่การฉ้อโกงผ่านทางคอมพิวเตอร์ การฝ่าฝืนนโยบายความปลอดภัยข้อมูลคอมพิวเตอร์ขององค์กร การจารกรรมข้อมูล การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การละเมิดสิทธิส่วนบุคคล และการดาวน์โหลดข้อมูลที่ผิดกฎหมาย

เมื่อมีเหตุการณ์ไม่ปกติเกิดขึ้นกับองค์กร จึงมีความจำเป็นต้องมีการประเมินความเสี่ยงที่อาจจะเกิดขึ้นกับองค์กร ไม่ว่าจะเป็นในด้านจริยธรรม, การเงิน และกฎหมาย เมื่อมีการสืบสวนภายในองค์กรและพบว่าอาจทำให้เกิดความเสียหายอย่างร้ายแรง อาจจะมีความจำเป็นต้องใช้การสืบสวนและดำเนินงานจากหน่วยงานภายนอกองค์กรที่น่าเชื่อถือและสามารถรักษาความลับขององค์กรได้

จากที่กล่าวมาข้างต้น จะเห็นได้ว่าการตรวจพิสูจน์พยานหลักฐานดิจิทัลในประเทศไทยถือเป็นเรื่องใหม่ และผู้ที่เกี่ยวข้องยังมีประสบการณ์ไม่มากพอ จึงมีความจำเป็นที่หน่วยงานด้านกฎหมายทั้งภาครัฐและเอกชนต้องให้ความสนใจเรียนรู้และหาประสบการณ์เพิ่มเติมเพราะพยานหลักฐานดิจิทัลอาจจะเป็นหลักฐานสำคัญที่ไม่ควรมองข้าม

ยังมีผู้คนจำนวนมากเข้าใจผิดเกี่ยวกับการตรวจพิสูจน์พยานหลักฐานดิจิทัล เช่น เกี่ยวข้องกับการสืบสวนคดีอาชญากรรมเท่านั้น หรือหลักฐานดิจิทัลมีความยุ่งยากซับซ้อน ซึ่งแท้จริงแล้วการตรวจพิสูจน์พยานหลักฐานดิจิทัลเกี่ยวข้องกับหลายๆ ส่วนไม่ว่าจะเป็น การสืบสวนคดีอาชญากรรม, การฟ้องร้องในคดีแพ่งหรือการฟ้องร้องเรื่องส่วนตัว ถ้าเกี่ยวข้องกับคอมพิวเตอร์, การสื่อสารผ่านอุปกรณ์อิเล็กทรอนิกส์หรือเอกสารอิเล็กทรอนิกส์แล้ว ก็ล้วนแต่มีความจำเป็นต้องใช้กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล เช่น การกู้ข้อมูลที่ถูกลบและไฟล์การใช้งานชั่วคราวที่เกิดขึ้นจากกระบวนการทำงานของคอมพิวเตอร์ ซึ่งข้อมูลที่พิสูจน์ได้นี้ ผู้ใช้งานจะไม่สามารถโต้แย้งได้เนื่องจากเป็นข้อมูลที่เกิดขึ้นจริง เช่น ข้อมูลการกระทำผิดของพนักงาน

ปัจจุบันนักกฎหมายในเมืองไทยบางส่วนยังคิดว่าการใช้พยานหลักฐานดิจิทัลมีความยุ่งยากซับซ้อนและคิดว่าไม่ได้รับอนุญาต ซึ่งเป็นความเข้าใจที่ยังไม่ตรงนัก เนื่องจากมีหลายกรณีที่มีความจำเป็นต้องใช้พยานหลักฐานดิจิทัล เช่น รูปภาพ, อีเมลล์, เอกสารอิเล็กทรอนิกส์ และประวัติการใช้งานอินเทอร์เน็ต ซึ่งหลักฐานเหล่านี้สามารถนำมาอธิบายในรูปแบบที่คนทั่วไปเข้าใจได้ง่าย

การจัดการกับพยานหลักฐานดิจิทัลมีสองสิ่งทีสำคัญคือ ความสมบูรณ์ของพยานหลักฐานและความถูกต้องของหลักฐาน โดยเป็นไปตามพระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2554 ซึ่งถือเป็นจุดเริ่มต้นงานด้านตรวจพิสูจน์พยานหลักฐานดิจิทัลในประเทศไทย

อาชญากรรมคอมพิวเตอร์ถูกระบุว่า เป็นหนึ่งในสี่อาชญากรรมที่สำคัญทางเศรษฐกิจและปัจจุบันมีแนวโน้มเพิ่มมากขึ้น ธุรกิจจำนวนมากไม่ได้ตระหนักว่าอาชญากรรมคอมพิวเตอร์จะส่งผลร้ายแรงต่อธุรกิจทั้งทางด้านการเงินและภาพพจน์ขององค์กรจนกระทั่งสายเกินไป ในปัจจุบันคนส่วนใหญ่ทำธุรกรรมและติดต่อสื่อสารในรูปแบบของอิเล็กทรอนิกส์ เพื่อที่เกิดจะประโยชน์สูงสุด องค์กรต่างๆ ควรมีการดำเนินการเพื่อลดความเสี่ยงที่อาจจะเกิดขึ้นเพื่อป้องกันการตกเป็นเหยื่อของอาชญากรรมคอมพิวเตอร์ จะเห็นได้ว่าการตรวจพิสูจน์พยานหลักฐานดิจิทัลเป็นเครื่องมือที่มีประสิทธิภาพที่บริษัทควรจะนำไปเป็นนโยบายพื้นฐานในการป้องกันอาชญกรรมคอมพิวเตอร์

การรับฟังพยานหลักฐานดิจิทัลของศาลไทย การเปลี่ยนแปลงทางสังคมเข้าสู่ยุคเทคโนโลยีสารสนเทศ จากเดิมที่เราสื่อสารโดยการพึ่งพาเพียงภาษาและตัวหนังสือเป็นหลัก มาเป็นการสื่อสาร

ด้วยภาษาอิเล็กทรอนิกส์ซึ่งมีประสิทธิภาพมากขึ้นในการประมวลผล ปัจจุบันจึงมีการกำหนดให้สื่ออิเล็กทรอนิกส์ใช้เป็นพยานหลักฐานได้ในการพิจารณาคดี นอกจากพยานวัตถุ พยานเอกสาร หรือพยานบุคคล และพยานนิติวิทยาศาสตร์ ซึ่งน่าจะพิสูจน์ได้ว่าจำเลยมีผิดหรือบริสุทธิ์ ให้อ้างเป็นพยานหลักฐานได้แล้ว ในส่วนการจัดประเภทพยานหลักฐานนั้น ข้อมูลอิเล็กทรอนิกส์แม้จะมีลักษณะเป็นพยานเอกสารและพยานวัตถุ แต่ก็มีลักษณะพิเศษแตกต่างจากพยานเอกสารและพยานวัตถุทั่วไป ในการนำสืบจึงต้องมีวิธีการพิเศษโดยเฉพาะการยอมรับให้ข้อมูลอิเล็กทรอนิกส์เป็นพยานอีกประเภทหนึ่งจึงมีความเหมาะสมมากกว่า เมื่อจัดข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานอีกประเภทหนึ่งแล้ว ข้อที่ต้องพิจารณาต่อมาก็คือ จะต้องมีวิธีการนำสืบและหลักในการรับฟังอย่างไร และจะนำบทตัดพยานได้แก่ หลักการรับฟังพยานหลักฐานที่ดีที่สุด และหลักการรับฟังพยานบอกเล่า มาใช้ด้วยหรือไม่ กรณีของวิธีการนำสืบนั้น ควรกำหนดให้ผู้กล่าวอ้างต้องดำเนินการเหมือนกันกับพยานหลักฐานประเภทอื่น คือ ต้องยื่นบัญชีระบุพยานที่เกี่ยวข้อง มีลายเซ็นต์ผู้ที่เกี่ยวข้อง เช่น คนรับเครื่อง คนอนุญาต วันและเวลา มีการส่งสำเนาพยานหลักฐานที่จะอ้างอิงให้แก่คู่ความอีกฝ่าย

การรับฟังพยานหลักฐานอิเล็กทรอนิกส์มีหลักกฎหมายสำคัญ 3 ประการ ในการพิจารณาพยานหลักฐานอิเล็กทรอนิกส์นั้นว่าสามารถยืนยันความแท้จริง (Authentication) ได้อย่างเหมาะสมหรือไม่

ความแท้จริงของพยานหลักฐานอิเล็กทรอนิกส์ประกอบด้วย

1) เนื้อหานั้นไม่ได้ถูกเปลี่ยนแปลง
2) ข้อมูลนั้นเป็นไปตามเจตนาที่แท้จริงของผู้สร้างเอกสารนั้น ทั้งนี้ไม่ว่าผู้สร้างเอกสารจะเป็นมนุษย์ หรือคอมพิวเตอร์
3) ข้อมูลพิเศษ เช่น วันเดือนปีที่ถูกสร้างนั้นถูกต้อง

ในปัจจุบันศาลไทยได้ให้การยอมรับและรับฟังพยานหลักฐานอิเล็กทรอนิกส์ เช่น ในคำพิพากษาศาลฎีกาที่ 7264/2542 ซึ่งวางหลักว่า พยานหลักฐานทางคอมพิวเตอร์สามารถรับฟังได้ ซึ่งอาจรับฟังได้ในฐานะที่เป็นพยานเอกสารในกรณีที่มีการพิมพ์ แล้วนำผลลัพธ์ที่ได้มานำเสนอ ซึ่งในแนวทางการรับฟังพยานหลักฐานชนิดนี้ของศาลนั้น จะต้องปรากฏว่าระบบการบันทึก การสร้าง การเก็บรักษา และการเรียกข้อมูล หรือการใช้งานของคอมพิวเตอร์นั้นเป็นปกติเช่นที่เคยทำมา ไม่มีสิ่งที่ผิดเพี้ยนหรือบิดเบือน ก็น่าเชื่อถือว่าเป็นข้อมูลที่ถูกต้องได้ ดังนั้น ปัญหาในการรับฟังพยานหลักฐานของศาลนั้น จึงอาจกล่าวได้ว่ามิใช่สิ่งที่เป็นอุปสรรคต่อการดำเนินคดีหรือการค้นหาความจริงแล้ว

การใช้พยานเอกสารข้อมูลทางอิเล็กทรอนิกส์นั้นสามารถอ้างอิงเป็นพยานหลักฐานต่อศาล ได้ศาลจะไม่ปฏิเสธการรับฟังข้อมูลนั้นเพราะเหตุว่าเป็นข้อมูลทางอิเล็กทรอนิกส์ แต่ข้อมูลดังกล่าวจะมีความน่าเชื่อถือรับฟังในเนื้อหาสาระได้หรือไม่นั้น เป็นดุลยพินิจของศาลซึ่งเป็นผู้รับฟังข้อมูลในการชั่งน้ำหนักพยานเอง โดยใช้หลักเกณฑ์ความน่าเชื่อถือตามที่กำหนดไว้ในมาตรา 10 วรรคสอง (พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544) เป็นเกณฑ์ในการพิจารณา จึงจำเป็นต้องมีการอบรมและให้ความรู้ทางด้านความปลอดภัยของข้อมูล การปรับเปลี่ยนทัศนคติค่านิยมเดิมๆ ความเคยชินในระบบพยานหลักฐานของไทย ตามบทบัญญัติของประมวลกฎหมายวิธีพิจารณาความแพ่ง ซึ่งนำไปใช้ในวิธีพิจารณาความอาญาด้วยนั้น จะเป็นระบบของพยานบุคคล พยานเอกสาร พยานวัตถุ และพยานผู้เชี่ยวชาญหรือผู้ชำนาญการพิเศษ ซึ่งมิได้ออกแบบไว้สำหรับ

พยานหลักฐานทางคอมพิวเตอร์หรืออิเล็กทรอนิกส์ จึงควรปรับเปลี่ยนเพราะเนื่องจากเป็นเรื่องจำเป็นสำหรับพนักงานสอบสวนตลอดจนผู้ที่เกี่ยวข้องในกระบวนการยุติธรรมจนถึงขั้นศาล ซึ่งสอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่ได้บังคับใช้แล้วในประเทศไทย เพื่อรับมือกับอาชญากรรมคอมพิวเตอร์ที่นับวันจะเพิ่มมากขึ้น และรูปแบบคดีก็ทวีความซับซ้อนมากขึ้น ความรู้ ความเข้าใจด้านการตรวจพิสูจน์พยานหลักฐานดิจิทัลจะทำให้ผู้ที่เกี่ยวข้องในกระบวนการยุติธรรมสามารถนำกฎหมายมาบังคับใช้ได้อย่างมีประสิทธิภาพสูงสุด

การทำความเข้าใจทั้งในส่วนของทฤษฎีทางอาชญาวิทยา สังคมวิทยาที่เกี่ยวข้อง และการพิสูจน์พยานหลักฐาน จะทำให้สามารถเชื่อมโยงกับกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลเพื่อทำความเข้าใจในส่วนของกระบวนการ ตลอดจนปัญหาและอุปสรรคที่เกิดขึ้นได้

2.4 กฎหมายที่เกี่ยวข้องกับกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล

เพื่อให้ผลการตรวจพิสูจน์พยานหลักฐานดิจิทัล ได้รับการยอมรับและรับฟังได้ในชั้นศาล ต้องมีการพิจารณาถึงกฎหมายที่เกี่ยวข้องต่างๆ ดังนี้

2.4.1 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ฉบับที่ 4 พ.ศ. 2562

โดยมีมาตราที่เกี่ยวข้องที่ยกมา คือ

หมวด 1 ธุรกรรมทางอิเล็กทรอนิกส์

มาตรา 7 ห้ามมิให้ปฏิเสธความมีผลผูกพันและการบังคับใช้ทางกฎหมายของข้อความใดเพียงเพราะเหตุที่ข้อความนั้นอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

มาตรา 8 ภายใต้บังคับบทบัญญัติแห่งมาตรา 9 ในกรณีที่กฎหมายกำหนดให้การใดต้องทำเป็นหนังสือ มีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดง ถ้าได้มีการจัดทำข้อความขึ้นเป็นข้อมูลอิเล็กทรอนิกส์ที่สามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง ให้ถือว่าข้อความนั้นได้ทำเป็นหนังสือ มีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดงแล้ว

มาตรา 9 ในกรณีที่บุคคลพึงลงลายมือชื่อในหนังสือ ให้ถือว่าข้อมูลอิเล็กทรอนิกส์นั้นมีการลงลายมือชื่อแล้ว ถ้า

(1) ใช้วิธีการที่สามารถระบุตัวเจ้าของลายมือชื่อ และสามารถแสดงได้ว่าเจ้าของลายมือชื่อรับรองข้อความในข้อมูลอิเล็กทรอนิกส์นั้นว่าเป็นของตน

(2) วิธีการดังกล่าวเป็นวิธีการที่เชื่อถือได้โดยเหมาะสมกับวัตถุประสงค์ของการสร้าง หรือส่งข้อมูลอิเล็กทรอนิกส์ โดยคำนึงถึงพฤติการณ์แวดล้อมหรือข้อตกลงของคู่กรณี

มาตรา 10 ในกรณีที่กฎหมายกำหนดให้นำเสนอหรือเก็บรักษาข้อความใดในสภาพที่เป็นมาแต่เดิมอย่างเอกสารต้นฉบับ ถ้าได้นำเสนอหรือเก็บรักษาในรูปข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์ดังต่อไปนี้ ให้ถือว่าได้มีการนำเสนอหรือเก็บรักษาเป็นเอกสารต้นฉบับตามกฎหมายแล้ว

(1) ข้อมูลอิเล็กทรอนิกส์ได้ใช้วิธีการที่เชื่อถือได้ในการรักษาความถูกต้อง ของข้อความตั้งแต่การสร้างข้อความเสร็จสมบูรณ์ และ

(2) สามารถแสดงข้อความนั้นในภายหลังได้ความถูกต้องของข้อความตาม

(3) ให้พิจารณาถึงความครบถ้วนและไม่มีการเปลี่ยนแปลงใดของข้อความ เว้นแต่การรับรอง หรือบันทึกเพิ่มเติม หรือการเปลี่ยนแปลงใด ๆ ที่อาจจะเกิดขึ้นได้ตามปกติในการติดต่อสื่อสาร การเก็บรักษา หรือการแสดงข้อความซึ่งไม่มีผลต่อความถูกต้องของข้อความนั้นในการวินิจฉัยความน่าเชื่อถือของวิธีการรักษาความถูกต้องของข้อความตาม ให้พิเคราะห์ถึงพฤติการณ์ที่เกี่ยวข้องทั้งปวง รวมทั้งวัตถุประสงค์ของการสร้างข้อความนั้น

มาตรา 11 ห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐาน ในกระบวนการพิจารณาตามกฎหมายเพียงเพราะเหตุว่าเป็นข้อมูลอิเล็กทรอนิกส์ ในการชั่งน้ำหนักพยานหลักฐานว่าข้อมูลอิเล็กทรอนิกส์จะเชื่อถือได้หรือไม่เพียงใดนั้น ให้พิเคราะห์ถึงความน่าเชื่อถือของลักษณะหรือวิธีการที่ใช้สร้าง เก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์ ลักษณะหรือวิธีการรักษา ความครบถ้วนและไม่มีการเปลี่ยนแปลงของ ข้อความ ลักษณะหรือวิธีการที่ใช้ในการระบุหรือแสดงตัวผู้ส่งข้อมูล รวมทั้งพฤติการณ์ที่เกี่ยวข้องทั้งปวง

มาตรา 12 ภายใต้บังคับบทบัญญัติ มาตรา 10 ในกรณีที่กฎหมายกำหนดให้เก็บรักษาเอกสารหรือข้อความใด ถ้าได้เก็บรักษาในรูปข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์ดังต่อไปนี้ ให้ถือว่าได้มีการเก็บรักษาเอกสารหรือข้อความตามที่กฎหมายต้องการแล้ว

(1) ข้อมูลอิเล็กทรอนิกส์นั้นสามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง

(2) ได้เก็บรักษาข้อมูลอิเล็กทรอนิกส์นั้นให้อยู่ในรูปแบบที่เป็นอยู่ในขณะที่สร้าง ส่ง หรือได้รับข้อมูลอิเล็กทรอนิกส์นั้น หรืออยู่ในรูปแบบที่สามารถแสดงข้อความที่สร้าง ส่ง หรือได้รับให้ปรากฏอย่างถูกต้องได้ และ

(3) ได้เก็บรักษาข้อความส่วนที่ระบุถึงแหล่งกำเนิด ต้นทาง และปลายทางของข้อมูลอิเล็กทรอนิกส์ตลอดจนวันและเวลาที่ส่งหรือได้รับข้อความดังกล่าว ถ้ามี

มาตรา 25 ธุรกรรมทางอิเล็กทรอนิกส์ใดที่ได้กระทำตามวิธีการแบบปลอดภัยที่กำหนดในพระราชกฤษฎีกา ให้สันนิษฐานว่าเป็นวิธีการที่เชื่อถือได้

จะเห็นได้ว่า พยานหลักฐานดิจิทัล มีกฎหมายรองรับ และสามารถรับฟังได้ในชั้นศาล หากมีมาตรฐานที่สามารถพิสูจน์ได้ถึงการรักษาความถูกต้องตลอดสาย สิ่งสำคัญที่จะทำให้การตรวจพิสูจน์พยานหลักฐานดิจิทัล ได้รับการยอมรับในชั้นศาล โดยไม่ถูกโต้แย้ง คือ ต้องสามารถยืนยันได้ว่าหลักฐานที่นำมาตรวจสอบ เป็นหลักฐานเดียวกับที่เก็บมาจากสถานที่เกิดเหตุจริง (Authentication) และไม่มีการเปลี่ยนแปลงข้อมูลใดๆ ไปจากเดิม (Integrity) ซึ่งในการจะยืนยันคุณสมบัติทั้งสองข้อนี้ได้นั้น ต้องอาศัยหลักการสำคัญของการตรวจพิสูจน์พยานหลักฐานดิจิทัลคือ Chain of custody และ Hash value

2.4.2 ประมวลกฎหมายวิธีพิจารณาความอาญา

มาตราที่เกี่ยวข้อง คือ

มาตรา 226 เป็นบททั่วไปของหลักเรื่องพยานหลักฐานในคดีอาญา ได้บัญญัติถึงพยานหลักฐานที่ใช้อ้างเพื่อพิสูจน์ว่าจำเลยมีผิดหรือบริสุทธิ์ แบ่งเป็น 3 ประเภท ได้แก่ พยานบุคคล พยานเอกสาร และพยานวัตถุ

1) พยานบุคคล หมายถึง บุคคลที่รู้เห็นเหตุการณ์หรือข้อเท็จจริงในคดี หากบุคคล ดังกล่าวพบเห็นเหตุการณ์ ในขณะเกิดการกระทำความผิด จะเรียกว่า “ประจักษ์พยาน” ซึ่งถือว่าเป็นพยานโดยตรงในคดี แต่หากพยานบุคคลนั้นมิได้พบเห็นเหตุการณ์ในขณะเกิดการกระทำความผิดอัน เป็นข้อเท็จจริงที่คู่ความในคดีมุ่งประสงค์จะพิสูจน์ความมีอยู่ แต่ได้รู้เห็นข้อเท็จจริงอย่างอื่นซึ่งต้องอาศัยการอนุมานข้อเท็จจริงหรือรับฟังร่วมกับพยานอย่างอื่น จะเรียกว่า “พยานแวดล้อม” นอกจากนี้ บุคคลยังสามารถเป็นพยานบุคคล แม้มิได้ประสบพบเห็นเหตุการณ์การกระทำความผิด
2) พยานเอกสาร หมายถึง ข้อมูลความหมายที่ถูกสื่อด้วยกระดาษหรือวัตถุอื่นใดที่ทำให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข ผัง หรือแผนแบบอย่างอื่น ไม่ว่าจะโดยวิธีพิมพ์ ถ่ายภาพ หรือวิธีอื่นอันเป็นหลักฐานแห่งความหมายนั้น
3) พยานวัตถุ หมายถึง วัตถุสิ่งของ รวมถึงสัตว์ สิ่งมีชีวิต ที่ใช้อ้างอิงเพื่อให้ศาลตรวจดู อย่างไรก็ดีพยานเอกสาร และพยานวัตถุในบางกรณีก็มีความยากในการจำแนก

กล่าวคือ การอ้างเอกสารเป็นพยานในคดี ไม่ได้หมายความว่าเอกสารดังกล่าวจะเป็นพยานเอกสารในทุกกรณี เช่น หากเป็นการอ้างข้อความบางตอนในเอกสาร เพื่อพิสูจน์ข้อเท็จจริงตามข้อความนั้น จะถือว่าเป็นการอ้างเอกสารในฐานะที่เป็นพยานเอกสาร แต่หากอ้างลายมือชื่อในเอกสารเพื่อพิสูจน์ว่าเป็นลายมือชื่อที่จำเลยทำปลอมขึ้นในความผิดฐานปลอมเอกสาร หรืออ้างเอกสารทั้งเล่มเพื่อพิสูจน์ว่ามีการทำซ้ำซึ่งงานอันมีลิขสิทธิ์ จะถือว่าเป็นการอ้างเอกสารในฐานะที่เป็นพยานวัตถุ กล่าวอีกนัยหนึ่ง จะต้องพิจารณาโดยดูที่วัตถุประสงค์ในการใช้อ้างเอกสารเพื่อเป็นพยาน หากเป็นการอ้างเพื่อให้ศาลดูข้อความในเอกสารก็จัดเป็นพยานเอกสาร แต่หากเป็นการอ้างเพื่อให้ศาลดูรูปลักษณะของเอกสาร ก็จัดเป็นพยานวัตถุ

เหตุที่กฎหมายได้กำหนดประเภทของพยานหลักฐานดังกล่าวไว้ เพื่อให้สอดคล้องกับหลักการรับฟังพยานหลักฐานแต่ละประเภท โดยในส่วนของข้อมูลที่บันทึกอยู่ในระบบคอมพิวเตอร์ อาจจัดเป็นพยานเอกสารหรือพยานวัตถุตามแต่วัตถุประสงค์ในการใช้อ้างในคดี หากมีวัตถุประสงค์มุ่งยืนยันความถูกต้องแท้จริงของเนื้อความด้วยการนำข้อมูลอิเล็กทรอนิกส์ที่บันทึกไว้ในระบบคอมพิวเตอร์ประมวลผลผ่านชุดคำสั่งและอุปกรณ์ต่างๆ โดยทำออกมาในรูปของสิ่งพิมพ์ ในรูปของเอกสาร และมีเนื้อหาตรงกันกับที่แสดงอยู่ ก็จะจัดเป็นพยานเอกสาร แต่หากการใช้อ้างข้อมูลที่บันทึกอยู่ในระบบคอมพิวเตอร์ เพื่อมุ่งยืนยันความมีอยู่ของข้อมูล อิเล็กทรอนิกส์ ด้วยการนำระบบคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ที่บันทึกข้อมูลไว้มานำสืบ ด้วยการแสดงออกในรูปแบบที่เข้าใจได้ และทำให้เห็นว่าเป็นข้อมูลที่ระบบคอมพิวเตอร์แสดงออกมา เป็นข้อมูลถูกต้องแท้จริง ไม่มีการแก้ไข หรือทำลายให้เกิดความเสียหาย ก็จะจัดเป็นพยานวัตถุ

โดยทั่วไปแล้ว พนักงานสอบสวนมีอำนาจรวบรวมพยานหลักฐานตามประมวลกฎหมาย วิธีพิจารณาความอาญา อันเป็นบทกฎหมายทั่วไป แต่บทกฎหมายดังกล่าวมิได้บัญญัติเกี่ยวกับการรวบรวมพยานหลักฐานที่เป็นอุปกรณ์ดิจิทัลหรือข้อมูลคอมพิวเตอร์ไว้โดยตรง ซึ่งคดีอาญาบางประเภทความผิด มีกฎหมายบัญญัติเอาไว้โดยเฉพาะในเรื่องของอำนาจของพนักงานสอบสวนหรือเจ้าพนักงานผู้มีอำนาจรวบรวมพยานหลักฐาน และหลักเกณฑ์วิธีการในการรวบรวมและจัดเก็บ

พยานหลักฐาน พนักงานสอบสวนหรือเจ้าพนักงานเหล่านั้นก็จะต้องปฏิบัติให้เป็นไปตามบทบัญญัติกฎหมายเฉพาะดังกล่าวนั้นด้วย เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

2.4.3 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560

มาตราที่เกี่ยวข้อง คือ

มาตรา 18 ภายใต้บังคับมาตรา 19 เพื่อประโยชน์ในการสืบสวนและสอบสวน ในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ หรือในกรณีที่มีการร้องขอ ตามวรรคสองให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด และหาตัวผู้กระทำความผิด

1) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิด มาเพื่อให้ถ้อยคำส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูลหรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้
2) เรียกข้อมูลการจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง
3) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา 26 หรือที่อยู่ในความครอบครอง หรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่หรือให้เก็บข้อมูลดังกล่าวไว้ก่อน
4) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลการจราจรทางคอมพิวเตอร์จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิด ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่
5) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่
6) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลการจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดหรือเพื่อสืบสวนหาตัวผู้กระทำความผิด และสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ ข้อมูลการจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้
7) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว
8) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะ เพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิด

เพื่อประโยชน์ในการสืบสวนและสอบสวนของพนักงานสอบสวน ตามประมวลกฎหมายวิธีพิจารณาความอาญา ในความผิดอาญาต่อกฎหมายอื่นซึ่งได้ใช้ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์เป็นองค์ประกอบหรือเป็นส่วนหนึ่งในการกระทำความผิดหรือมีข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับการกระทำความผิดอาญาตามกฎหมายอื่น พนักงานสอบสวนอาจร้องขอให้พนักงานเจ้าหน้าที่ตามวรรคหนึ่งดำเนินการตามวรรคหนึ่งก็ได้ หรือหากปรากฏข้อเท็จจริงดังกล่าวต่อพนักงานเจ้าหน้าที่เนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่รีบรวบรวมข้อเท็จจริงและหลักฐานแล้ว แจ้งไปยังเจ้าหน้าที่ที่เกี่ยวข้องเพื่อดำเนินการต่อไป

ให้ผู้ได้รับการร้องขอจากพนักงานเจ้าหน้าที่ตามวรรคหนึ่ง (1) (2) และ (3) ดำเนินการตามคำร้องขอโดยไม่ชักช้า แต่ต้องไม่เกินเจ็ดวันนับแต่วันที่ได้รับคำร้องขอ หรือภายในระยะเวลาที่พนักงานเจ้าหน้าที่กำหนดซึ่งต้องไม่น้อยกว่าเจ็ดวันและไม่เกินสิบห้าวัน เว้นแต่ในกรณีที่มีเหตุสมควร ต้องได้รับอนุญาตจากพนักงานเจ้าหน้าที่ ทั้งนี้ รัฐมนตรีอาจประกาศในราชกิจจานุเบกษา กำหนดระยะเวลาที่ต้องดำเนินการที่เหมาะสมกับประเภทของผู้ให้บริการก็ได้

มาตรา 19 การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา 18 (4) (5) (6) (7) และ (8) ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำ หรือกำลังจะกระทำการอย่างหนึ่งอย่างใดอันเป็นความผิด เหตุที่ต้องใช้อำนาจลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิดเท่าที่สามารถจะระบุได้ ประกอบคำร้องด้วย ในการพิจารณาคำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็ว

เมื่อศาลมีคำสั่งอนุญาตแล้ว ก่อนดำเนินการตามคำสั่งของศาล ให้พนักงานเจ้าหน้าที่ส่งสำเนาบันทึกเหตุอันควรเชื่อที่ทำให้ต้องใช้อำนาจตามมาตรา 18 (4) (5) (6) (7) และ (8) มอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐาน แต่ถ้าไม่มีเจ้าของหรือ ผู้ครอบครองเครื่องคอมพิวเตอร์อยู่ ณ ที่นั้น ให้พนักงานเจ้าหน้าที่ส่งมอบสำเนาบันทึกนั้นให้แก่เจ้าของหรือผู้ครอบครองดังกล่าวในทันทีที่กระทำได้

ให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าในการดำเนินการตามมาตรา 18 (4) (5) (6) (7) และ (8) ส่งสำเนาบันทึกรายละเอียดการดำเนินการ และเหตุผลแห่งการดำเนินการให้ศาลที่มี เขตอำนาจภายในสี่สิบแปดชั่วโมงนับแต่เวลาลงมือดำเนินการ เพื่อเป็นหลักฐาน

การทำสำเนาข้อมูลคอมพิวเตอร์ตามมาตรา 18 (4) ให้กระทำได้เฉพาะเมื่อมีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิด และต้องไม่เป็นอุปสรรคในการดำเนินกิจการของเจ้าของหรือ ผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นเกินความจำเป็น

การยึดหรืออายัดตามมาตรา 18 (8) นอกจากจะต้องส่งมอบสำเนาหนังสือแสดง การยึดหรืออายัดมอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐานแล้ว พนักงานเจ้าหน้าที่จะสั่งยึดหรืออายัดไว้เกินสามสิบวันมิได้ ในกรณีจำเป็นที่ต้องยึดหรืออายัดไว้นานกว่านั้น ให้ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอขยายเวลายึดหรืออายัดได้ แต่ศาลจะอนุญาตให้ขยายเวลาครั้งเดียวหรือหลายครั้งรวมกันได้อีกไม่เกินหกสิบวัน เมื่อหมดความจำเป็นที่จะยึดหรือ อายัด หรือครบกำหนดเวลาดังกล่าวแล้ว พนักงานเจ้าหน้าที่ต้องส่งคืนระบบคอมพิวเตอร์ที่ยึดหรือถอนการอายัดโดยพลัน

หนังสือแสดงการยึดหรืออายัดตามวรรคห้าให้เป็นไปตามที่กำหนดในกฎกระทรวง

มาตรา 25 ข้อมูล ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ที่ พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้หรือที่พนักงานสอบสวนได้มาตามมาตรา 18 วรรคสอง ให้อ้างและรับฟังเป็นพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญาหรือกฎหมายอื่นอันว่าด้วยการสืบพยานได้ แต่ต้องเป็นชนิดที่มิได้เกิดขึ้นจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบประการอื่น

2.4.4 พระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ.2535

มาตราที่เกี่ยวข้อง คือ

ส่วนที่ 2 การสอบสวนและการสืบพยานหลักฐาน

มาตรา 15 ในกรณีที่ได้รับคำร้องขอความช่วยเหลือจากต่างประเทศ ให้สอบปากคำพยานหรือรวบรวมพยานหลักฐานที่อยู่ในประเทศไทยในชั้นสอบสวน ให้เจ้าหน้าที่ผู้มีอำนาจแจ้งให้พนักงานสอบสวนดำเนินการตามคำร้องขอนั้น ให้พนักงานสอบสวนมีอำนาจสอบปากคำพยานหรือรวบรวมพยานหลักฐานตามคำร้องขอในวรรคหนึ่ง ในกรณีที่จำเป็นให้มีอำนาจค้นและยึดเอกสารหรือวัตถุใด ๆ ทั้งนี้ ตามหลักเกณฑ์วิธีการและเงื่อนไขที่บัญญัติไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา เมื่อพนักงานสอบสวนดำเนินการสอบปากคำพยานหรือรวบรวมพยานหลักฐานเสร็จแล้ว ให้แจ้งผลการดำเนินการหรือส่งมอบพยานหลักฐานที่รวบรวมได้ให้แก่เจ้าหน้าที่ผู้มีอำนาจดำเนินการต่อไป

มาตรา 16 ถ้าสนธิสัญญาระหว่างประเทศผู้ร้องขอกับประเทศไทยว่าด้วยความร่วมมือระหว่างประเทศในเรื่องทางอาญา กำหนดให้ต้องมีการรับรองความถูกต้องแท้จริงแห่งเอกสารอย่างใดอย่างหนึ่ง ให้เจ้าหน้าที่ผู้มีอำนาจมีอำนาจสั่งให้บุคคลผู้มีหน้าที่เก็บรักษาเอกสารรับรองความถูกต้องแท้จริงของเอกสารนั้นตามแบบและวิธีการที่กำหนดไว้ในสนธิสัญญาดังกล่าวหรือตามที่ผู้ประสานงานกลางกำหนด

มาตรา 17 ในกรณีที่ได้รับคำร้องขอความช่วยเหลือจากต่างประเทศให้สืบพยานหลักฐานในศาลไทย ให้เจ้าหน้าที่ผู้มีอำนาจแจ้งให้พนักงานอัยการดำเนินการตามคำร้องขอนั้น ให้พนักงานอัยการมีอำนาจยื่นคำร้องต่อศาลที่บุคคลซึ่งจะเป็นพยานหรือบุคคลซึ่งครอบครองหรือดูแลรักษาพยานเอกสารหรือพยานวัตถุมีภูมิลำเนาหรือมีที่อยู่ในเขตศาลให้สืบพยานหลักฐานดังกล่าว และให้ศาลมีอำนาจดำเนินกระบวนพิจารณาสืบพยานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญา เมื่อศาลดำเนินการสืบพยานหลักฐานเสร็จแล้ว ให้พนักงานอัยการยื่นคำร้องต่อศาล ขอรับบันทึกคำเบิกความของพยานรวมทั้งพยานหลักฐานอื่นในสำนวนไปส่งให้เจ้าหน้าที่ผู้มีอำนาจเพื่อดำเนินการต่อไป

2.5 งานวิจัยที่เกี่ยวข้อง

สุรพันธ์ มั่นคงดี (2541) ปัญหาและอุปสรรคด้านงานสืบสวนสอบสวนที่สำคัญประการหนึ่งได้แก่ ปัญหาด้านการบังคับใช้กฎหมาย ซึ่งผลการวิจัยเรื่อง พยานหลักฐานในคดีอาชญากรรมคอมพิวเตอร์ พบว่าในการสืบสวนสอบสวนคดีอาชญากรรมคอมพิวเตอร์ประสบปัญหาสำคัญ คือ ความสามารถทางเทคนิคของผู้สืบสวน ความจำเป็นในการเพิ่มทักษะการเรียนรู้ของเจ้าหน้าที่ตำรวจ

ความยากลำบากในการแกะรอยผู้บุรุกเข้าสู่ระบบ ปัญหาในการชี้และรวบรวมพยานหลักฐาน การขาดสถิติและความรู้เกี่ยวกับรูปแบบและลักษณะอาชญากรรมคอมพิวเตอร์ ความยากลำบากในการติดตามวิวัฒนาการทางคอมพิวเตอร์ที่เปลี่ยนแปลงไปอย่างรวดเร็ว ข้อจำกัดในการปรับใช้กฎหมายลักษณะพยานกับอาชญากรรมคอมพิวเตอร์

เลิศชาย สุธรรมพร (2541) ผลการวิจัยเรื่องอาชญากรรมคอมพิวเตอร์: ศึกษาเฉพาะกรณีความปลอดภัยของข้อมูล พบว่าปัจจุบันยังไม่มีกฎหมายเฉพาะที่จะนำมาปรับใช้เพื่อลงโทษผู้กระทำความผิดเกี่ยวกับข้อมูลในคอมพิวเตอร์ได้ อย่างไรก็ตามเมื่อมีการกระทำความผิดเกี่ยวกับข้อมูลในคอมพิวเตอร์เกิดขึ้น หน่วยงานที่บังคับใช้กฎหมายพยายามที่จะปรับการกระทำความผิดดังกล่าวให้เข้ากับฐานความผิดตามประมวลกฎหมายอาญาหรือความผิดตามพระราชบัญญัติที่มีลักษณะใกล้เคียงกัน จึงส่งผลให้เกิดปัญหาการตีความ เช่น กรณีตีความว่าข้อมูลมิใช่ทรัพย์ จึงไม่อาจลงโทษผู้กระทำความผิดฐานลักทรัพย์ตามประมวลกฎหมายอาญา มาตรา 334 หรือฐานทำให้เสียทรัพย์ตามประมวลกฎหมายอาญา มาตรา 358 ได้ ประเทศสหรัฐอเมริกาได้บัญญัติกฎหมายอาญาพิเศษเฉพาะ หรือที่เรียกว่ากฎหมายอาชญากรรมคอมพิวเตอร์มาบังคับใช้กับการกระทำความผิดเกี่ยวกับข้อมูลในคอมพิวเตอร์ โดยกฎหมายฉบับนี้ประกอบด้วยฐานความผิดที่เป็นสาระสำคัญ สามฐานความผิด คือ ความผิดฐานเข้าถึงโดยปราศจากอำนาจ ความผิดฐานแก้ไขเปลี่ยนแปลง และความผิดฐานทำให้เสียหายหรือทำลาย ส่วนประเทศอังกฤษได้บัญญัติกฎหมายอาชญากรรมคอมพิวเตอร์มาบังคับใช้เช่นกัน โดยกำหนดความผิดออกเป็นสามฐาน คือ ความผิดฐานเข้าถึงโดยปราศจากอำนาจ ความผิดฐานเข้าถึงโดยปราศจากอำนาจ โดยมีเจตนาที่จะกระทำหรือเพื่อความสะดวกในการกระทำความผิดอื่นๆ และความผิดฐานเปลี่ยนแปลงแก้ไขโดยปราศจากอำนาจ ปัจจุบันประเทศไทยได้นำเอาเทคโนโลยีสารสนเทศมาใช้ในเกือบทุกกิจกรรมเพื่อพัฒนาประเทศ แต่ขณะเดียวกันก็ต้องคำนึงถึงการใช้เทคโนโลยีสารสนเทศกระทำความผิดควบคู่กันไปด้วย เมื่อกฎหมายที่มีอยู่ไม่สามารถบังคับใช้ได้อย่างครอบคลุมและมีประสิทธิภาพ จึงควรมีการบัญญัติกฎหมายเฉพาะมาบังคับใช้ เพื่อจะได้ขจัดปัญหาและอุปสรรคดังกล่าว

สินเลิศ สุขุม (2543) ทำการศึกษาวิจัยเรื่อง ปัจจัยที่มีผลต่อประสิทธิภาพในการป้องกันปราบปรามอาชญากรรมคอมพิวเตอร์ของเจ้าหน้าที่ตำรวจกองบังคับการสืบสวนสอบสวนคดีเศรษฐกิจ โดยการวิจัยมีวัตถุประสงค์เพื่อศึกษาปัจจัยที่มีผลต่อประสิทธิภาพในการป้องกัน ปราบปรามอาชญากรรมคอมพิวเตอร์ของเจ้าหน้าที่ตำรวจกองบังคับการสืบสวนสอบสวนคดี เศรษฐกิจ โดยเก็บรวบรวมข้อมูลและประเมินผลจากแบบสอบถามจำนวน 100 ชุด และจากการสัมภาษณ์เจ้าหน้าที่ตำรวจในกองบังคับการสืบสวนสอบสวนคดีเศรษฐกิจของการปฏิบัติงาน จำนวน 10 คน แล้วนำมาวิเคราะห์ร้อยละ หาค่าเฉลี่ยส่วนเบี่ยงเบนมาตรฐาน และการทดสอบ ค่า Chi-Square ซึ่งการทดสอบพความแตกต่างอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ผลการวิจัยพบว่า ปัจจัยที่มีผลต่อประสิทธิภาพในการป้องกันปราบปรามอาชญากรรมคอมพิวเตอร์ของเจ้าหน้าที่ ตำรวจกองบังคับการสืบสวนสอบสวนคดีเศรษฐกิจ ได้แก่ ปัจจัยในด้านระยะเวลาในการทำงาน เกี่ยวข้องกับคอมพิวเตอร์ และความสามารถเกี่ยวกับการใช้คอมพิวเตอร์

นัยนรัตน์ งานแสง (2547) ได้ทำการศึกษาวิจัยเรื่อง อาชญากรรมคอมพิวเตอร์: ศึกษาเฉพาะกรณีปัจจัยที่มีผลต่อการเกิดปัญหาอาชญากรรมบนอินเทอร์เน็ต มีจุดมุ่งหมายเพื่อศึกษาสภาพปัญหาอาชญากรรมบนอินเทอร์เน็ตในปัจจุบัน ตลอดจนความเสียหายที่เกิดขึ้น รวมทั้งประเภทและรูปแบบ

ของอาชญากรรมบนอินเทอร์เน็ตในประเทศไทย เพื่อแสวงหาแนวทางแก้ไขและจัดการปัญหา โดยเป็นการศึกษาเชิงพรรณนาจากแนวคิดและทฤษฎีต่างๆ และงานวิจัยที่เกี่ยวข้องมาใช้เป็นกรอบการวิเคราะห์ข้อมูลที่ได้รับ จากแบบสอบถามและการสัมภาษณ์บุคลากรผู้เชี่ยวชาญที่เกี่ยวข้อง ผลการศึกษาพบว่า ปัญหาอาชญากรรมคอมพิวเตอร์ในประเทศไทยมีแนวโน้มเพิ่มขึ้น เนื่องจากการขยายตัวของอินเทอร์เน็ตในประเทศไทยเพิ่มขึ้นอย่างรวดเร็ว ในขณะที่ผู้ใช้อินเทอร์เน็ตในสังคมไทยยังขาดความรู้และความเข้าใจและการปลูกฝังด้านจริยธรรมและวัฒนธรรม รวมถึงการใช้งานเทคโนโลยีในเชิงสร้างสรรค์ ทำให้เกิดปัญหาการนำเทคโนโลยีไปใช้ไปทางที่ผิด ส่วนบุคลากรที่มีความรู้ความสามารถด้านการรักษาความปลอดภัยคอมพิวเตอร์และเครือข่ายของประเทศไทยยังมีจำนวนจำกัด รวมทั้งภาครัฐไม่มีนโยบายและองค์กรเกี่ยวกับการป้องกันปราบปราม อาชญากรรมคอมพิวเตอร์โดยตรง ประกอบกับปัญหาทางด้านกฎหมาย ซึ่งปัจจุบัน(ในปีที่ทำการวิจัย) ยังไม่มีกฎหมายอาชญากรรมคอมพิวเตอร์ออกมาบังคับใช้ ทำให้เกิดปัญหาในการดำเนินคดีกับผู้กระทำผิด

พกรณ์ รักษาชาติ (2552) อาชญากรรมอิเล็กทรอนิกส์: กรณีศึกษา อาชญากรรมบนเครือข่ายอินเทอร์เน็ต การวิจัยนี้เป็นการศึกษาเชิงสำรวจโดยมีวัตถุประสงค์เพื่อศึกษาถึงสาเหตุและปัจจัยต่างๆที่นำไปสู่การก่ออาชญากรรมอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ประเภท รูปแบบ และผลกระทบจากอาชญากรรมอิเล็กทรอนิกส์บนเครืออินเทอร์เน็ต ความรู้ความเข้าใจต่อการป้องกันตนเองจากอาชญากรรมอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต และแนวทางในการแก้ไข การป้องกันและการจัดการกับปัญหาอาชญากรรมอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ตของข้าราชการ และเจ้าหน้าที่สังกัดกรุงเทพมหานคร ผลการศึกษา พบว่า

1) ข้าราชการ และเจ้าหน้าที่สังกัดกรุงเทพมหานคร ส่วนใหญ่เพศชาย มีอายุ 40 ปี ขึ้นไป โสด จบการศึกษาระดับปริญญาตรี มีรายได้เฉลี่ย 10,000 – 15,000 บาท ต่อเดือน และเคยได้รับการอบรมความรู้เกี่ยวกับคอมพิวเตอร์หรืออินเทอร์เน็ต มากกว่า 3 ครั้ง
2) ข้าราชการ และเจ้าหน้าที่สังกัดกรุงเทพมหานคร ส่วนใหญ่ใช้เครื่อง PC ในการเชื่อมต่ออินเทอร์เน็ต โดยใช้อุปกรณ์ Modem ใช้บริการอินเทอร์เน็ตทุกวันๆ วันละไม่เกิน 3 ชั่วโมง ใช้บริการอินเทอร์เน็ตจากที่ทำงานเพื่อค้นหาข้อมูลจากเว็บไซต์ www.google.com ใช้อุปกรณ์อิเล็กทรอนิกส์ร่วมกับผู้อื่น แต่ไม่เคยใช้บัญชีอินเทอร์เน็ตร่วมกับผู้อื่น และมีการดาวน์โหลดซอฟท์แวร์จากอินเทอร์เน็ตบางครั้งบางคราว มีการติดตั้งโปรแกรมป้องกันไวรัส และ ทำการปรับปรุงโปรแกรมป้องกันไวรัสทุกครั้งที่มีการแจ้ง และปัญหาที่สร้างความเสียหายต่อผู้ใช้งานอินเทอร์เน็ต คือ ปัญหาไวรัสคอมพิวเตอร์ ทั้งยังพบว่าส่วนใหญ่ไม่มีการสร้างตารางเวลาในการบันทึกข้อมูล และการตรวจสอบพื้นที่ว่างภายในเครื่องแม่ข่าย นานๆ ครั้งจะมีหน่วยงานในการจัดการ และบำรุงรักษาเครื่องแม่ข่าย ส่วนใหญ่มีระบบรักษาความปลอดภัยของข้อมูลอิเล็กทรอนิกส์ แต่ไม่มีการแจ้งข่าวสารหรืออบรมเกี่ยวกับการป้องกันตนจากอาชญากรรมคอมพิวเตอร์ขององค์กร
3) ข้าราชการ และเจ้าหน้าที่สังกัดกรุงเทพมหานคร มีความรู้ความเข้าใจในการป้องกันการก่ออาชญากรรมทางอิเล็กทรอนิกส์ด้านกฎหมาย และด้านรูปแบบ หรือวิธีการก่ออาชญากรรมอิเล็กทรอนิกส์

4) ระดับความคิดเห็นต่อปัญหาอาชญากรรมอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ตของข้าราชการ และเจ้าหน้าที่สังกัดกรุงเทพมหานคร ในภาพรวมอยู่ในระดับมากโดยเฉพาะแนวโน้มความรุนแรงและผลกระทบของอาชญากรรมบนเครือข่ายอินเทอร์เน็ต

5) ปัจจัยที่มีผลต่อการก่ออาชญากรรมทางอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต มาจากการเปิดรับและตอบกลับอีเมล์จากผู้ไม่รู้จัก คลิกลิงค์บนหน้าต่าง หรือมีการป๊อบอัพขึ้น การใช้บริการธนาคารผ่านร้าน อินเทอร์เน็ต การส่งข้อมูลส่วนตัวหรือข้อมูลทางการเงินให้กับบุคคลอื่นที่ไม่รู้จัก การไม่สำรองข้อมูล และโปรแกรมคอมพิวเตอร์

Guofu Ma และคณะ (2554) ศึกษาวิจัยเรื่องรูปแบบพื้นฐาน วงแหวนหลักฐานและห่วงโซ่หลักฐานของงานการตรวจพิสูจน์พยานหลักฐานทางดิจิทัล พบว่า การพัฒนาเทคโนโลยีที่เกี่ยวข้องกับการพิจารณาคดีทางด้านการตรวจพิสูจน์พยานหลักฐานทางดิจิทัล ส่วนใหญ่เป็นงานทางด้านวิทยาศาสตร์ และงานด้านคอมพิวเตอร์ และยังไม่สามารถเชื่อมโยงกับการพิจารณาคดีตามกฎหมายได้มากนัก ส่วนใหญ่จะศึกษาเฉพาะด้านเทคนิคของพยานหลักฐานดิจิทัลเท่านั้น ในการศึกษาจึงศึกษาคุณลักษณะทั่วไปของพยานหลักฐาน วัตถุประสงค์ ความเกี่ยวข้อง และความถูกต้องของกฎหมายเพื่อบรรทัดฐานในการสร้างแบบจำลอง ของการตรวจพิสูจน์พยานหลักฐานทางดิจิทัลบนพื้นฐานของวงแหวนและห่วงโซ่ของหลักฐาน

จุลศักดิ์ แก้วกาญจน์ (2558) นักวิจัยโครงการศึกษาเผยแพร่ความรู้ด้านนิติวิทยาศาสตร์คอมพิวเตอร์กล่าวถึงในงานวิจัย ว่า มาตรฐานเป็นเรื่องสำคัญ เพราะพยานหลักฐานดิจิทัลมีอยู่ทุกแห่ง จะจัดการอย่างไรให้น่าเชื่อถือ โดยในกระบวนการยุติธรรม การเก็บรวบรวมรักษาและพิสูจน์พยานหลักฐานดังกล่าวมีอยู่ด้วยกัน 4 ขั้นตอน ได้แก่

1) เก็บรวบรวม ซึ่งต้องทำอย่างถูกวิธีเพื่อไม่ให้มีการเปลี่ยนแปลงในพยานหลักฐานดิจิทัล

2) เก็บรักษา ซึ่งสื่อแต่ละชนิดก็มีวิธีในการเก็บรักษาต่างกัน

3) การเอาหลักฐานมาตรวจวิเคราะห์ และ

4) การนำเสนอพยานหลักฐานในชั้นศาล

จุลศักดิ์กล่าวถึงปัญหาในประเทศไทยว่า ตอนนี้ประเทศไทยยังไม่มีการกำหนดมาตรฐานการเก็บรวบรวมและพิสูจน์พยานหลักฐานดิจิทัล ทั้งในเรื่องหน่วยงานกลาง ไม่มีเครื่องมือในการตรวจพิสูจน์เพียงพอครบทุกสื่อดิจิทัล ทั้งยังไม่มีการวางมาตรฐานกลาง ขณะที่ต่างประเทศมีหน่วยงานที่ทำหน้าที่กำหนดมาตรฐานการเก็บรวบรวมและพิสูจน์พยานหลักฐานดิจิทัล ยกตัวอย่างเช่น หากเป็นมือถือสมาร์ทโฟนยี่ห้อ iPhone รุ่น 4 ก็มีกำหนดว่าต้องใช้เครื่องมือประเภทใด ยี่ห้ออะไรในการตรวจและต้องมีวิธีการตรวจอย่างไร

Andrew Smith (2560) ผู้อำนวยการพิสูจน์พยานหลักฐานดิจิทัลของ Orion Investigations กล่าวถึงทักษะที่จำเป็นสำหรับนักตรวจพิสูจน์พยานหลักฐานดิจิทัล ไว้ในบทความ Required Skills for Digital forensics investigator ว่าต้องประกอบด้วย

1) Self-motivation/Desire to learn ผู้เชี่ยวชาญตรวจพิสูจน์พยานหลักฐานดิจิทัล ไม่ได้ทำงานเพียงแค่ในเวลาทำงานปกติ ผู้เชี่ยวชาญตรวจพิสูจน์พยานหลักฐานดิจิทัลที่ดีจะต้องใช้เวลา

นอกเหนือเวลาทำงานสืบค้นหาเทคนิคใหม่ๆ เพื่อพัฒนาทักษะให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยี รวมถึงข้อมูลที่มีจำนวนมากขึ้นในปัจจุบัน

2) Investigator's mindset ทักษะข้อนี้อาจจะเป็นทักษะที่ยากที่สุดในการสอนผู้เชี่ยวชาญคนใหม่ ผู้เชี่ยวชาญจะต้องไม่กลัวที่จะถามคำถามและตั้งใจที่จะหาคำตอบเหล่านั้น เมื่อเริ่มการตรวจสอบ ผู้เชี่ยวชาญอาจไม่ทราบว่าควรเริ่มตรงไหน ผู้เชี่ยวชาญต้องสามารถทำงานเป็นทีมได้ แต่ก็เป็นอิสระด้วย ผู้เชี่ยวชาญจะต้องสามารถตัดสินใจได้ว่าข้อมูลส่วนใดที่เกี่ยวข้องกับการสืบสวนสอบสวน และเมื่อไหร่ควรหยุดสืบค้นหาข้อมูลหลักฐาน

3) Communication skills ทักษะการสื่อสารที่ดี ผู้เชี่ยวชาญจำเป็นต้องมีทักษะในการใช้หลักฐานที่อาจซับซ้อนและนำเสนอในรูปแบบที่เข้าใจได้ง่ายสำหรับบุคคลทั่วไปที่ไม่มีความรู้พื้นฐานเรื่อง IT หรือเทคนิคต่างๆ ทักษะการนำเสนอรายงานหรือพยานหลักฐานดิจิทัลที่พบ มีความสำคัญเป็นอย่างมาก ในฐานะบทบาทของผู้เชี่ยวชาญมักจะเกี่ยวข้องกับการนำเสนอหลักฐานในศาลและเป็นพยานผู้เชี่ยวชาญ ซึ่งส่งผลให้ผู้เชี่ยวชาญต้องเตรียมตัวให้พร้อมและสามารถตอบคำถามได้อย่างชัดเจน รัดกุมขณะที่อยู่ภายใต้แรงกดดัน

4) Technical skills นิติวิทยาศาสตร์เป็นสาขาวิชาทางเทคนิคและผู้เชี่ยวชาญควรมีพื้นฐานด้านเทคนิค เมื่อต้องการหาผู้เชี่ยวชาญตรวจพิสูจน์พยานหลักฐานดิจิทัล บุคคลนั้นควรมีทักษะด้านเทคนิคทั่วไปมากมาย และทักษะในส่วนเทคนิคพิเศษทางคอมพิวเตอร์ เช่น ผู้เชี่ยวชาญอาจมีความสนใจเป็นพิเศษในการตรวจสอบระบบปฏิบัติการ Apple ระบบปฏิบัติการ Microsoft การตรวจสอบเครือข่าย (Network forensics) หรือการวิเคราะห์มัลแวร์ (Malware analysis)

พิชศาล พันธุ์วัฒนา (2562) ศึกษาวิจัยเรื่อง ความน่าเชื่อถือในการนำเอกสารอิเล็กทรอนิกส์มาใช้เป็นพยานหลักฐานในชั้นศาล โดยนำเสนอ 8 ประเด็น ที่เป็นพื้นฐานและมีความสำคัญ ประกอบด้วย (1) ความหมายของเอกสาร อิเล็กทรอนิกส์ ธุรกรรมทางอิเล็กทรอนิกส์ และข้อมูลอิเล็กทรอนิกส์ (2) โครงสร้างเอกสารอิเล็กทรอนิกส์ (3) การนำเอกสารอิเล็กทรอนิกส์มาใช้เป็นพยานหลักฐาน (4) การรับฟังพยานหลักฐานที่ดีที่สุดกับเอกสารอิเล็กทรอนิกส์ (5) การพิสูจน์ความถูกต้องแท้จริงของพยานเอกสารอิเล็กทรอนิกส์ (6) การชั่งน้ำหนักพยานหลักฐานของเอกสารอิเล็กทรอนิกส์ (7) กฎหมายแม่แบบว่าด้วยพยานหลักฐานทางอิเล็กทรอนิกส์ และ (8) หลักเกณฑ์มาตรฐานทางด้านเทคโนโลยีของข้อมูลอิเล็กทรอนิกส์ ซึ่งการสร้างความน่าเชื่อถือของเอกสารอิเล็กทรอนิกส์ที่นำมาใช้เป็นพยานหลักฐานในชั้นศาลจำต้องให้ความสำคัญต่อขั้นตอนการจัดทำข้อมูลที่ได้ปฏิบัติตามหลักเกณฑ์มาตรฐานสากล และผ่านการพิจารณาเพื่อรับรองความถูกต้อง จากหน่วยงานที่มีอำนาจตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549 มาตรา 3 เพื่อแสดงให้เห็นว่าเอกสารอิเล็กทรอนิกส์ที่ใช้เป็นพยานหลักฐานมีความถูกต้องแท้จริง ส่วนการที่ศาลจะเชื่อถือเอกสารอิเล็กทรอนิกส์ที่นำมาใช้เป็นพยานหลักฐานมากน้อยเพียงใดขึ้นอยู่กับดุลยพินิจของศาลที่พิจารณาผ่านการชั่งน้ำหนักพยานหลักฐานนั้น

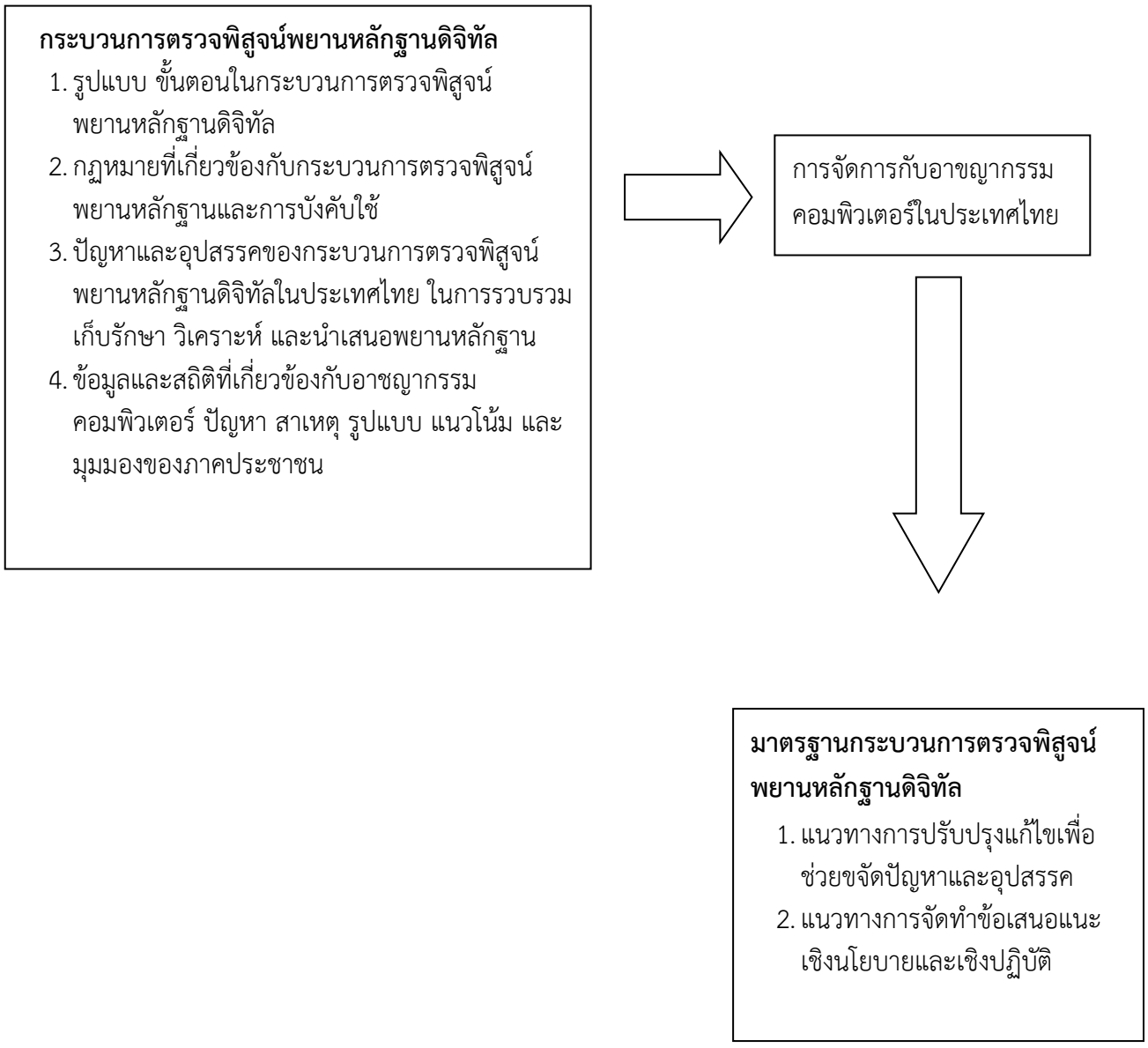
Martin Novak (2563) ศึกษาวิจัย เกี่ยวกับ พยานหลักฐานดิจิทัล ในคดีอาชญากรรมในชั้นศาลอุทธรณ์ของประเทศสหรัฐอเมริกา โดยนำเสนอประเด็น และยกกรณีศึกษาในมลรัฐต่างๆ เพื่อสรุปการรับฟังพยานหลักฐานดิจิทัลในชั้นศาล ว่า ศาลนำหลักเกณฑ์แห่งพยานหลักฐานในเรื่องกฎ

แห่งการรับฟังพยานบอกเล่า การรับฟังพยานหลักฐานที่ดีที่สุด ความถูกต้องแท้จริงของพยานหลักฐาน มาปรับใช้กับพยานหลักฐานดิจิทัลด้วย กล่าวคือ การนำพยานหลักฐานดิจิทัลมาใช้ในการพิสูจน์ข้อเท็จจริงได้นั้น จะต้องคำนึงถึง 2 ประเด็น ประเด็นแรก จะต้องแสดงให้เห็นถึงความแท้จริงของพยานหลักฐาน ว่า เพียงพอที่จะสนับสนุนข้อกล่าวอ้างของฝ่ายที่มีหน้าที่นำสืบได้ตามที่กล่าวอ้าง และประเด็นที่สอง ถ้าพยานหลักฐานดิจิทัลเป็นบันทึกที่เก็บไว้ในคอมพิวเตอร์ที่มีข้อความที่มนุษย์สร้างขึ้นอยู่ด้วย จะต้องแสดงให้เห็นว่า ข้อความนั้นไม่อยู่ในหลักเกณฑ์การห้ามรับฟังพยานบอกเล่า รวมถึง หลักเกณฑ์การรับฟังพยานหลักฐานที่ดีที่สุด ซึ่งกำหนดว่าในการพิสูจน์เนื้อหาของข้อเขียน บันทึก หรือภาพจะต้องใช้ ต้นฉบับ ของข้อเขียน บันทึก หรือภาพนั้น และประเด็นเรื่องความถูกต้องแท้จริงของพยานหลักฐานดิจิทัล อาจนำมาสู่ประเด็นโต้แย้งโดยคู่ความของฝ่ายตรงข้ามได้

กล่าวโดยสรุป แต่เดิมในช่วงแรกประเทศไทยยังไม่มีกฎหมายเฉพาะเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ จึงเป็นที่มาของการออกพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ แต่อย่างไรก็ตาม จากความก้าวหน้าทางเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว ทำให้ประสบปัญหาทั้งทางด้านเทคนิค สำหรับการสืบสวน สอบสวน และตรวจพิสูจน์พยานหลักฐานดิจิทัล ซึ่งต้องการความรู้ความชำนาญและผู้เชี่ยวชาญเฉพาะด้าน รวมไปถึงปัญหาด้านกฎหมาย; ในปัจจุบันอาชญากรรมคอมพิวเตอร์มีแนวโน้มสูงขึ้น แต่การให้ความรู้เกี่ยวกับคอมพิวเตอร์และอินเทอร์เน็ต ทำให้สามารถป้องกันตนเองจากอาชญากรรมคอมพิวเตอร์ได้ในเบื้องต้น ควบคู่ไปกับการใช้มาตรการทางกฎหมายของรัฐ และการสร้างมาตรฐานของการตรวจพิสูจน์พยานหลักฐานดิจิทัล ตลอดจนการให้ความสำคัญกับการอบรมบุคลากร หรือใช้ทีมผู้เชี่ยวชาญที่มีทักษะเฉพาะด้าน จะสามารถรับมือกับการเปลี่ยนแปลงทางเทคโนโลยี และการเพิ่มขึ้นของอาชญากรรมคอมพิวเตอร์ได้

2.6 กรอบแนวคิดในการวิจัย

จากแนวคิด ทฤษฎี และเอกสารงานวิจัยที่เกี่ยวข้อง นำมากำหนดกรอบแนวคิดในการวิจัยได้ ดังนี้


กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล
1. รูปแบบ ขั้นตอนในกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล
2. กฎหมายที่เกี่ยวข้องกับกระบวนการตรวจพิสูจน์พยานหลักฐานและการบังคับใช้
3. ปัญหาและอุปสรรคของกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลในประเทศไทย ในการรวบรวม เก็บรักษา วิเคราะห์ และนำเสนอพยานหลักฐาน
4. ข้อมูลและสถิติที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ ปัญหา สาเหตุ รูปแบบ แนวโน้ม และมุมมองของภาคประชาชน
การจัดการกับอาชญากรรมคอมพิวเตอร์ในประเทศไทย
มาตรฐานกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล
1. แนวทางการปรับปรุงแก้ไขเพื่อช่วยขจัดปัญหาและอุปสรรค
2. แนวทางการจัดทำข้อเสนอแนะเชิงนโยบายและเชิงปฏิบัติ

บทที่ 3
วิธีดำเนินการวิจัย

การศึกษาเรื่อง กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล: การวิเคราะห์เพื่อพัฒนาเชิงนโยบาย เป็นการวิจัยเชิงคุณภาพ (Qualitative research) โดยมีวิธีดำเนินการวิจัยดังนี้

3.1 วิธีการวิจัย
3.2 กลุ่มตัวอย่าง
3.3 วิธีการเก็บรวบรวมข้อมูล
3.4 วิธีการสร้างเครื่องมือในการวิจัย
3.5 โครงร่างแบบสัมภาษณ์
3.6 การวิเคราะห์ข้อมูล
3.7 จริยธรรมของการวิจัยในคน

3.1 วิธีการวิจัย

ในการศึกษาวิจัยครั้งนี้ มีวิธีการวิจัยดังนี้

1) การศึกษาค้นคว้าจากเอกสาร (Documentary study) เป็นการศึกษาค้นคว้าและรวบรวมข้อมูลจากเอกสารทางวิชาการ บทความ วารสาร หนังสือ สิ่งพิมพ์ รายงานการวิจัย วิทยานิพนธ์ และดุษฎีนิพนธ์ต่างๆ รวมถึงสืบค้นจากสื่ออิเล็กทรอนิกส์ อินเทอร์เน็ต ในส่วนของข้อมูลเกี่ยวกับแนวคิด ทฤษฎีและเอกสารงานวิจัยที่เกี่ยวข้องเพื่อนำมาใช้เป็นกรอบแนวคิดในการวิจัย

2) การศึกษาภาคสนาม (Field study) ผู้วิจัยเก็บรวบรวมข้อมูลด้วยการลงพื้นที่เพื่อสัมภาษณ์ผู้ให้ข้อมูลสำคัญด้วยการสัมภาษณ์เชิงลึกแบบกึ่งโครงสร้าง (Semi-structured in-depth interview) โดยสัมภาษณ์เป็นรายบุคคล ใช้คำถามตามแบบสัมภาษณ์ และจดบันทึกข้อมูลรวมถึงบันทึกเสียงของผู้ให้สัมภาษณ์ โดยมีแบบสัมภาษณ์เป็นเครื่องมือในการเก็บรวบรวมข้อมูล

3) การศึกษาแบบกรณีศึกษา (Case study) ผู้วิจัยเลือกสถานการณ์ เหตุการณ์ที่เกิดขึ้นจริงที่มีคุณสมบัติเฉพาะตัว เพื่อศึกษาค้นคว้าเชิงลึก เป็นการศึกษาปัญหาเพื่อให้ได้คำตอบที่ครอบคลุม ในเรื่องที่มาของปัญหา ผลกระทบทางตรง และทางอ้อมที่เกิดขึ้น นำไปสู่การวิเคราะห์ แนวทางพัฒนาและแก้ไขต่อไป

3.2 ผู้ให้ข้อมูลสำคัญ

ในการศึกษาวิจัยครั้งนี้ กลุ่มตัวอย่าง (Sample) ที่ใช้ในการวิจัยครั้งนี้ ผู้วิจัยเลือกการสุ่มตัวอย่างแบบเจาะจง (Purposive sampling) เป็นการเลือกตัวอย่างโดยกำหนดคุณลักษณะของประชากรที่ต้องการศึกษา เป็นการเก็บข้อมูลจากผู้ให้ข้อมูลสำคัญ (Key informants) จำนวน 31 คน โดยมีเกณฑ์การเลือก คือ ผู้ที่มีส่วนได้ส่วนเสีย และมีความเกี่ยวข้องกับกระบวนการตรวจพิสูจน์

พยานหลักฐานดิจิทัล ในบริบทต่างๆ ที่มีประสบการณ์ ความเชี่ยวชาญอย่างน้อย 3 ปี เป็นผู้มีส่วนร่วมในการวิจัย เกณฑ์การคัดเข้า และเกณฑ์การคัดออก

ผู้ให้ข้อมูลสำคัญ ได้แก่

1) บุคลากรภาครัฐ เจ้าหน้าที่ตำรวจที่มีประสบการณ์ทางด้านอาชญากรรม คอมพิวเตอร์ ในส่วนของกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล จำนวน 6 คน
2) อัยการที่มีความรู้ความชำนาญในคดีอาชญากรรมคอมพิวเตอร์ จำนวน 6 คน
3) ผู้พิพากษาที่มีความเชี่ยวชาญในคดีอาชญากรรมคอมพิวเตอร์ จำนวน 6 คน
4) บุคลากรภาคเอกชน ผู้เชี่ยวชาญ ที่มีทักษะด้านการสืบสวนสอบสวนอาชญากรรมคอมพิวเตอร์ จำนวน 6 คน
5) นักวิชาการ ผู้มีส่วนได้ส่วนเสีย ที่มีประสบการณ์ หรือได้รับผลกระทบจาก อาชญากรรมคอมพิวเตอร์ในประเทศไทย จำนวน 7 คน

3.3 วิธีการเก็บรวบรวมข้อมูล

ในการวิจัยครั้งนี้ใช้วิธีการเก็บรวบรวมข้อมูล ดังนี้

ข้อมูลปฐมภูมิ (Primary data)

เป็นข้อมูลที่ผู้วิจัยรวบรวมจากแหล่งข้อมูลโดยตรง โดยได้มาจากการเก็บรวบรวมข้อมูลภาคสนามจากการสัมภาษณ์ ผู้วิจัยเก็บข้อมูลโดยการสัมภาษณ์ตามวัตถุประสงค์ของการวิจัย ใช้วิธีการสัมภาษณ์เชิงลึกแบบกึ่งโครงสร้าง (Semi-structured in-depth interview) ผู้วิจัยใช้คำถามปลายเปิดตามแบบสัมภาษณ์ ดำเนินไปเสมือนการสนทนา เริ่มต้นทำการสัมภาษณ์ตามคำถามที่กำหนดไว้ และผู้วิจัยใช้การจดบันทึกข้อมูลและบันทึกเสียงผู้ให้สัมภาษณ์

ข้อมูลทุติยภูมิ (Secondary data)

เป็นข้อมูลที่ไม่ได้มาจากแหล่งข้อมูลโดยตรง ผู้วิจัยได้มาจากข้อมูลที่มีผู้อื่นรวบรวมไว้แล้ว เช่น จากเอกสารทางวิชาการ กรณีศึกษา สถิติ หรือข้อมูลของแต่ละหน่วยงาน

วิธีการเก็บรวบรวมข้อมูลจากเอกสาร เป็นวิธีการศึกษาค้นคว้าเก็บรวบรวมข้อมูลทั่วไป โดยการรวบรวมจากเอกสารซึ่งเป็นข้อมูลที่มีการบันทึกไว้แล้วโดยผู้อื่น ได้แก่

1) หนังสือทั่วไป ได้แก่ ตำรา คู่มือ เอกสารประกอบการบรรยาย รวมถึงเอกสารทางวิชาการ บทความ วารสาร สิ่งพิมพ์ เป็นต้น
2) หนังสืออ้างอิง ได้แก่ สารานุกรม พจนานุกรม เป็นต้น
3) งานวิจัย วิทยานิพนธ์ ดุษฎีนิพนธ์ เป็นงานที่ผู้ศึกษาได้ทำการศึกษาค้นคว้าในเรื่องนั้นๆ อย่างละเอียด
4) กรณีศึกษา เป็นสถานการณ์ เหตุการณ์ที่เกิดขึ้นจริง ที่เลือกมาเพื่อศึกษาค้นคว้าเชิงลึก
5) เอกสารของทางราชการ เป็นเอกสารที่ส่วนราชการจัดทำขึ้นเพื่อประโยชน์ในการปฏิบัติ เช่น นโยบาย กฎระเบียบ พระราชบัญญัติ คู่มือปฏิบัติงาน ประกาศ คำสั่ง เป็นต้น

3.4 วิธีการสร้างเครื่องมือในการวิจัย

การสร้างเครื่องมือในการวิจัยได้จากการทบทวนแนวคิด ทฤษฎี และเอกสารงานวิจัยที่เกี่ยวข้องทั้งในประเทศไทยและต่างประเทศ โดยใช้แบบสัมภาษณ์เป็นเครื่องมือในการวิจัยเพื่อศึกษาข้อมูลจากกลุ่มตัวอย่างในเชิงคุณภาพ เมื่อสร้างเครื่องมือในการวิจัยแล้ว ต้องมีการตรวจสอบคุณภาพของเครื่องมือด้วยการตรวจสอบด้านเนื้อหาของแบบสัมภาษณ์ โดยให้อาจารย์ที่ปรึกษาการวิจัยและผู้เชี่ยวชาญที่มีความรู้ความชำนาญด้านการตรวจพิสูจน์พยานหลักฐานดิจิทัลและอาชญากรรมคอมพิวเตอร์ จำนวน 3 คน เป็นผู้ตรวจสอบความถูกต้องของเนื้อหาแบบสัมภาษณ์ เพื่อให้มีประเด็นการสัมภาษณ์ที่ชัดเจน ไม่คลุมเครือ และเมื่อผ่านการพิจารณาอนุมัติจากคณะกรรมการจริยธรรมเรียบร้อยแล้ว จึงจะทำการสัมภาษณ์กับผู้ให้ข้อมูลสำคัญ

เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูลในการวิจัยครั้งนี้ คือ แบบสัมภาษณ์ ผู้วิจัยใช้แบบสัมภาษณ์ และวิธีการสัมภาษณ์เชิงลึกแบบกึ่งโครงสร้าง (Semi-structured in-depth interview) ลักษณะการสัมภาษณ์ เป็นการสัมภาษณ์ตามแบบสัมภาษณ์ที่มีคำถามปลายเปิด มีความยืดหยุ่น ดำเนินไปเสมือนเป็นการสนทนาในชีวิตประจำวัน จะสัมภาษณ์ผู้ใดก็ใช้คำถามเดียวกัน การสัมภาษณ์จะสัมภาษณ์เป็นรายบุคคล ก่อนการเก็บรวบรวมข้อมูล ผู้วิจัยได้กำหนดนัดหมายวันสัมภาษณ์โดยแจ้งผู้ให้สัมภาษณ์ทราบก่อนล่วงหน้าในการสัมภาษณ์ ผู้สัมภาษณ์จะใช้การจดบันทึกและการบันทึกเสียง โดยก่อนสัมภาษณ์จะขออนุญาตผู้ให้สัมภาษณ์ในการบันทึกการสนทนาก่อนทุกครั้ง

3.5 โครงร่างแบบสัมภาษณ์

คำถามวิจัยเชิงคุณภาพสำหรับผู้ให้ข้อมูลสำคัญ

<u>ส่วนที่ 1</u>: ข้อมูลทั่วไป ชื่อ สกุล ประวัติส่วนตัว อายุงาน และประวัติการทำงานอย่างย่อในส่วนที่เกี่ยวข้องกับการตรวจพิสูจน์พยานหลักฐานดิจิทัล และอาชญากรรมคอมพิวเตอร์ของผู้ให้สัมภาษณ์

- ชื่อ
- เพศ
- อายุ
- ตำแหน่งและอายุงาน
- ประสบการณ์ทำงาน

<u>ส่วนที่ 2</u>: คำถามปลายเปิด คำถามทั่วไป เกี่ยวกับ การตรวจพิสูจน์พยานหลักฐานดิจิทัล และสถานการณ์อาชญากรรมคอมพิวเตอร์ ในประเทศไทย

- ท่านมีขั้นตอนการตรวจพิสูจน์พยานหลักฐานดิจิทัล และ/หรือ การดำเนินคดีอาชญากรรมคอมพิวเตอร์อย่างไร ขั้นตอนการรับแจ้งเรื่อง ลักษณะการกระทำผิดที่พบ รายละเอียดการทำงานและการประสานหน่วยงานอื่นๆ

- พื้นที่ หรืออำนาจหน้าที่ความรับผิดชอบของท่าน มีอาชญากรรมคอมพิวเตอร์หรือความเกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์มากน้อยเพียงใด อย่างไร ประสบการณ์การบังคับใช้กฎหมาย
- แนวโน้มปัญหาอาชญากรรมคอมพิวเตอร์ ลักษณะคดี รายละเอียด ความถี่ เป็นอย่างไร

ส่วนที่ 3: คำถามปลายเปิด เกี่ยวกับ ปัญหาและอุปสรรคของการทำงาน การตรวจพิสูจน์พยานหลักฐานดิจิทัล และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

- ปัญหา และอุปสรรคที่พบ ทั้งในด้านกฎหมาย เทคโนโลยี วิธีการ ความรู้ความเชี่ยวชาญที่จำเป็นในการปฏิบัติงานและอื่นๆ ของการตรวจพิสูจน์พยานหลักฐานดิจิทัลและคดีอาชญากรรมคอมพิวเตอร์ มีอะไรบ้าง
- การตีความแต่ละมาตรา และการใช้อำนาจภายใต้ พระราชบัญญัติคอมพิวเตอร์ พ.ศ. 2560 ชัดเจนหรือไม่ มีปัญหา และอุปสรรคหรือไม่ อย่างไร
- มุมมองของภาคประชาขน ทัศนคติเกี่ยวกับการตรวจพิสูจน์พยานหลักฐานดิจิทัล อาชญากรรมคอมพิวเตอร์ และประเด็นสิทธิ เสรีภาพ ประเด็นประมวลกฎหมายอาญา มาตรา 112 รวมถึงประเด็นทางสังคมอื่นๆ เป็นอย่างไร มีอะไรบ้าง

ส่วนที่ 4: คำถามปลายเปิด เกี่ยวกับความคิดเห็นและข้อเสนอแนะ ต่อมาตรฐานการตรวจพิสูจน์พยานหลักฐานดิจิทัลในประเทศไทย และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

- ความคิดเห็นต่อกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลในปัจจุบัน มาตรฐาน ข้อกำหนด กฎหมายอื่น และอื่นๆ ที่เกี่ยวข้อง การปรับปรุง พัฒนา
- ความคิดเห็นด้านความเหมาะสมของ พระราชบัญญัติคอมพิวเตอร์ พ.ศ. 2560 กับบริบทของสังคมไทย ความก้าวหน้าทางเทคโนโลยี และการพลิกผันทางดิจิทัล
- ข้อเสนอแนะ เพื่อแก้ไข ปรับปรุง พระราชบัญญัติคอมพิวเตอร์ พ.ศ. 2560 ทั้งด้านกฎหมายและด้านการบังคับใช้

3.6 การวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลในการศึกษาครั้งนี้ เป็นการวิเคราะห์ข้อมูลเชิงคุณภาพ ผู้วิจัยมีขั้นตอนในการวิเคราะห์ ดังนี้

1) ผู้วิจัยจะนำข้อมูลที่ได้จากการสัมภาษณ์มาแยกประเด็นตามแต่ละประเด็น
2) นำข้อมูลที่ได้จากการสัมภาษณ์มาแยกประเด็นคำถาม แล้วนำมาเปรียบเทียบความเหมือน หรือความแตกต่างของผู้ให้สัมภาษณ์แต่ละคน ก่อนจะนำข้อมูลนั้นไปวิเคราะห์
3) นำข้อมูลที่ได้จากการสัมภาษณ์มาแยกประเด็นคำถาม แล้วนำมาเปรียบเทียบกับข้อมูลเอกสารที่เกี่ยวข้องกัน เช่น ทฤษฎีทางด้านอาชญาวิทยา สังคมวิทยา และสังเคราะห์เนื้อหา ก่อนจะนำข้อมูลนั้นไปวิเคราะห์

4) นำข้อมูลที่ได้จากการเปรียบเทียบมาทำการวิเคราะห์ข้อมูลร่วมกัน โดยใช้วิธีการสร้างข้อสรุปจากการศึกษารูปแบบหรือข้อมูล จากนั้นจึงใช้วิธีการวิเคราะห์โดยการวิเคราะห์เนื้อหา (Content analysis) เพื่อสรุปผลการวิจัย โดยใช้การนำเสนอผลการวิจัยในรูปแบบ บทความวิจัย และแบบบรรยาย

สำหรับเทคนิคการวิเคราะห์ข้อมูลมี 2 ส่วน คือ ส่วนที่หนึ่ง คือการวิเคราะห์ข้อมูลแบบสร้างข้อสรุปในการวิจัยเชิงคุณภาพ ซึ่งส่วนใหญ่ข้อมูลที่นำมาวิเคราะห์ จะเป็นข้อมูลเชิงพรรณา (Descriptive) ที่ได้จากการสังเกต สัมภาษณ์ แล้วจดบันทึกไว้ ส่วนที่สอง คือการวิเคราะห์เนื้อหา (Content analysis) ซึ่งเป็นการวิเคราะห์ข้อมูลเชิงพรรณาเช่นกัน

การวิจัยเชิงคุณภาพมีความยืดหยุ่นสูง เพื่อให้ผลการวิจัยมีความน่าเชื่อถือ และเกิดความไว้วางใจในคุณภาพของงานวิจัยเชิงคุณภาพ ในการวิจัยนี้ ผู้วิจัยจึงต้องใช้วิธีในการตรวจสอบความถูกต้องของข้อมูลก่อนนำไปวิเคราะห์ โดยใช้การตรวจสอบแบบสามเส้าเชิงคุณภาพ (Triangulation) คือ

1) การตรวจสอบสามเส้าด้านข้อมูล (Data triangulation) เพื่อพิสูจน์ว่าข้อมูลที่ผู้วิจัยได้มานั้นถูกต้องหรือไม่ โดยตรวจสอบแหล่งของข้อมูล แหล่งเวลา แหล่งสถานที่ และแหล่งบุคคล
2) การตรวจสอบสามเส้าด้านวิธีรวบรวมข้อมูล (Methodological triangulation) โดยการใช้วิธีเก็บรวบรวมข้อมูลต่างๆ กันเพื่อรวบรวมข้อมูลเรื่องเดียวกัน เช่น ใช้วิธีการสังเกตควบคู่กับการซักถาม และศึกษาข้อมูลจากแหล่งเอกสารประกอบด้วย

3.7 จริยธรรมของการวิจัยในคน

ดำเนินการขอจริยธรรมการวิจัยในคนจากคณะกรรมการ โดยได้หมายเลข 232/2561

ผู้วิจัยคำนึงถึงและให้ความสำคัญกับจริยธรรมของการวิจัยในคน ซึ่งเป็นหลักที่ให้ความเคารพในตัวบุคคล (Respect for person) ให้ประโยชน์และไม่ก่อให้เกิดอันตรายกับผู้ถูกวิจัย (Beneficence) รวมถึงมีความเที่ยงธรรม (Fairness) และความเท่าเทียม (Equity) โดยในการศึกษาเรื่อง กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล: การวิเคราะห์เพื่อพัฒนาเชิงนโยบาย นี้ อาจเกิดกรณีที่สร้างความลำบากใจต่อผู้ถูกวิจัย ผู้วิจัยจึงคำนึงถึงประเด็นต่างๆ ในการวิจัย ดังนี้

1) การเก็บข้อมูล ผู้วิจัยจะแจ้งวัตถุประสงค์ของการวิจัยอย่างชัดเจน ครบถ้วน เพื่อให้ผู้ถูกวิจัยได้รับข้อมูลที่เพียงพอและเป็นอิสระในการตัดสินใจ (Free and informed consent) ในการให้ความยินยอม และมีการเคารพในศักดิ์ศรีของกลุ่มเปราะบางและอ่อนแอ เช่น ผู้ต้องขัง เพื่อไม่ให้ถูกนำข้อมูลไปใช้ในทางที่ผิด รวมถึงมีการรักษาความลับของผู้ถูกวิจัย จะไม่มีการระบุชื่อของผู้ถูกวิจัยโดยไม่ได้รับความยินยอม
2) การเก็บข้อมูล ผู้วิจัยจะคำนึงถึงหลักการชั่งน้ำหนักของความเสี่ยง และคุณประโยชน์ (Balancing risks and benefits) โดยประโยชน์ที่จะได้จากการวิจัย ต้องมากกว่าความเสี่ยงที่จะเกิดขึ้น และความเสี่ยงต้องเป็นที่ยอมรับได้โดยผู้ถูกวิจัย และได้รับความเห็นชอบจากคณะกรรมการจริยธรรม มีการลดอันตรายให้น้อยที่สุด (Minimizing harm) และสร้างคุณประโยชน์สูงสุด (Maximizing benefit)

3) การเก็บข้อมูล ผู้วิจัยจะใช้กระบวนการที่มีทั้งความเที่ยงธรรม และความเท่าเทียม ผู้ถูกวิจัยควรได้ประโยชน์จากการวิจัย โดยไม่มีการทอดทิ้งหรือแบ่งแยกบุคคลที่อาจได้ประโยชน์จากการวิจัย

การดำเนินการต่อผู้มีส่วนร่วมในการวิจัย ผู้วิจัยสัมภาษณ์ผู้ให้ข้อมูลสำคัญ โดยการสัมภาษณ์เชิงลึกและการสนทนากลุ่ม เป็นการสัมภาษณ์ปากเปล่า และเอกสาร การสัมภาษณ์จะมีการสัมภาษณ์ 1 ครั้ง ใช้เวลาประมาณ 1 ชั่วโมง ตามสถานที่ซึ่งมีการนัดหมายกับผู้มีส่วนร่วมในการวิจัย ในประเด็นตามหัวข้อ โดยหากข้อมูลไม่สมบูรณ์ จะมีการนัดสัมภาษณ์เพิ่มเติมอีก 1 ครั้ง ใช้เวลาประมาณ 30 นาที มีการให้ข้อมูลที่มา วัตถุประสงค์ในการวิจัยเป็นเอกสารชี้แจง และการอธิบาย การเปิดเผยข้อมูลส่วนตัว ได้รับการยินยอมโดยสมัครใจ มีการบันทึกความคิดเห็น โดยได้รับการยินยอม และเมื่อสิ้นสุดการวิจัยแล้ว การบันทึกความคิดเห็น และเสียงสัมภาษณ์จะถูกทำลาย ลบทิ้ง ไม่มีการเก็บรักษาไว้ ผู้ให้ข้อมูลสำคัญมีสิทธิถอนตัวออกจากการวิจัยเมื่อใดก็ได้ โดยไม่ต้องแจ้งเหตุผล โดยการถอนตัวนั้นจะไม่มีผลกระทบใดๆ ต่อการผู้ให้ข้อมูลสำคัญ ความเสี่ยงในการเข้าร่วมการวิจัยอยู่ในระดับน้อยมาก มีความไม่สะดวกเพียงการสละเวลา นัดหมายเพื่อสัมภาษณ์ และข้อมูลที่ให้สัมภาษณ์ ผู้วิจัยจะเก็บเป็นความลับ โดยจะนำเสนอข้อมูลการวิจัยเป็นภาพรวม ไม่มีข้อมูลใดที่จะเป็นการระบุตัวของผู้ให้ข้อมูลสำคัญ

บทที่ 4
ผลการศึกษาและการอภิปรายผล

การศึกษาวิจัยเรื่อง กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล: การวิเคราะห์เพื่อพัฒนาเชิงนโยบาย มีวัตถุประสงค์ในการวิจัยเพื่อศึกษากระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลในประเทศไทย จากชั้นสอบสวน ถึงชั้นพิจารณาคดี และกฎหมายที่เกี่ยวข้อง ตลอดจนปัญหาและอุปสรรคของการดำเนินงานในกระบวนการตรวจพิสูจน์พยานหลักฐานของหน่วยงานที่เกี่ยวข้อง เพื่อนำไปสู่การจัดทำข้อเสนอแนะเชิงนโยบายและแนวทางปฏิบัติในการตัดสินใจนโยบาย และข้อเสนอในการปรับปรุงกฎหมายและการบังคับใช้ ให้แก่หน่วยงานในกระบวนการยุติธรรมและหน่วยงานที่เกี่ยวข้อง การนำเสนอผลการศึกษาวิจัยดังกล่าวนี้ ได้จากการวิเคราะห์และสังเคราะห์ข้อมูลโดยอาศัยข้อมูลเชิงคุณภาพจากการสัมภาษณ์เชิงลึกผู้ให้ข้อมูลสำคัญ (Key informants) และนำมาวิเคราะห์เนื้อหา ทั้งในส่วนของบุคลากรภาครัฐที่เกี่ยวข้องในกระบวนการยุติธรรมและภาคประชาชน ซึ่งผู้วิจัยได้แยกผู้ให้ข้อมูลสำคัญออกเป็น 2 กลุ่ม ได้แก่

กลุ่มที่ 1 บุคลากรภาครัฐที่เกี่ยวข้อง อาทิ เจ้าหน้าที่ตำรวจ อัยการ ผู้พิพากษา จำนวน 18 คน
กลุ่มที่ 2 ภาคเอกชน (ประชาชน) นักวิชาการ ที่มีทักษะด้านกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล ผู้ได้รับผลกระทบจากอาชญากรรมคอมพิวเตอร์ จำนวน 13 คน

ในการเก็บข้อมูล ผู้วิจัยเก็บข้อมูลเชิงลึกโดยครอบคลุมสาระสำคัญในส่วนของ ปัญหา สาเหตุ และกรณีศึกษาต่างๆ เพื่อนำมาใช้ในการวิเคราะห์ (Analysis) และสังเคราะห์ข้อมูล (Synthesize) โดยแบ่งข้อมูลออกเป็น 3 ส่วน ดังนี้

ส่วนที่ 1 กระบวนการหรือวิธีการในการตรวจพิสูจน์พยานหลักฐานดิจิทัลในประเทศไทย และกฎหมายที่เกี่ยวข้อง
ส่วนที่ 2 ปัญหาและอุปสรรคที่เกิดขึ้นในการดำเนินงานของกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล
ส่วนที่ 3 แนวทางการแก้ไขปัญหา และปรับปรุงการดำเนินงาน รวมถึงการปรับปรุงกฎหมายและการบังคับใช้

ซึ่งสามารถอธิบายโดยแยกออกเป็น 3 ส่วนได้ดังนี้

4.1 กระบวนการในการตรวจพิสูจน์พยานหลักฐานดิจิทัล 4 ขั้นตอน และกฎหมายที่เกี่ยวข้อง

ในคดีที่มีการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี พยานหลักฐานหลายกรณีจะอยู่ในลักษณะของพยานหลักฐานดิจิทัล ซึ่งการรวบรวม จัดเก็บ หรือตรวจพิสูจน์หลักฐานจะต้องดำเนินการโดยผู้ที่มีความเชี่ยวชาญเฉพาะ และพยานหลักฐานดิจิทัลมีความสำคัญอย่างมากใน

กระบวนการพิจารณาคดีความผิดที่เกี่ยวกับอาชญากรรมทางเทคโนโลยี โดยต้องมีกระบวนการที่ชัดเจนในการตรวจพิสูจน์พยานหลักฐานดิจิทัล

กระบวนการในการตรวจพิสูจน์พยานหลักฐานดิจิทัล

หลักการพื้นฐานในการตรวจพิสูจน์พยานหลักฐานดิจิทัล ประกอบไปด้วย

1) <u>การรวบรวมพยานหลักฐานดิจิทัล</u>

สิ่งสำคัญที่สุด คือ ความสมบูรณ์ของพยานหลักฐาน และการรวบรวมพยานหลักฐานทั้งหมดให้เป็นไปอย่างสมบูรณ์ขณะเกิดเหตุโดยไม่ถูกเปลี่ยนแปลงแก้ไขใดๆ โดยทั่วไปแล้ว พนักงานสอบสวนมีอำนาจรวบรวมพยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 132 อันเป็นบทกฎหมายทั่วไป แต่บทกฎหมายดังกล่าวไม่ได้บัญญัติเกี่ยวกับการรวบรวมพยานหลักฐานที่เป็นอุปกรณ์ดิจิทัลหรือข้อมูลคอมพิวเตอร์ไว้โดยตรง อย่างไรก็ดี คดีอาญาบางประเภทความผิด มีกฎหมายบัญญัติเอาไว้โดยเฉพาะเจาะจงในเรื่องของอำนาจของพนักงานสอบสวนหรือเจ้าพนักงานผู้มีอำนาจรวบรวมพยานหลักฐานและหลักเกณฑ์วิธีการในการรวบรวมและจัดเก็บพยานหลักฐาน พนักงานสอบสวนหรือเจ้าพนักงานเหล่านั้นก็จะต้องปฏิบัติให้เป็นไปตามบทบัญญัติกฎหมายเฉพาะดังกล่าวนั้นด้วย ดังเช่นที่กำหนดไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ มาตรา 18, 26 ได้ให้อำนาจในการเรียกผู้ถูกกล่าวหามาให้ถ้อยคำ เรียกข้อมูลการจราจรทางคอมพิวเตอร์ สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บ ทำสำเนา หรือส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าว รวมถึงตรวจสอบการเข้าถึง และถอดรหัสลับของข้อมูลคอมพิวเตอร์ หรือสั่งให้บุคคลที่เกี่ยวข้อง ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว รวมทั้งยึดหรืออายัดระบบคอมพิวเตอร์เฉพาะเท่าที่จำเป็น การรวบรวมพยานหลักฐานดิจิทัล จะมีหน่วยงานเฉพาะเข้ามาทำหน้าที่เก็บรวบรวมพยานหลักฐาน เช่น กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) และสถาบันนิติวิทยาศาสตร์ ซึ่งมีเจ้าหน้าที่ที่มีความรู้ความเชี่ยวชาญทางด้านคอมพิวเตอร์และเทคโนโลยีโดยเฉพาะ และเป็นเจ้าหน้าที่ที่ได้รับการแต่งตั้งตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (แก้ไขเพิ่มเติม พ.ศ. 2560) มีอำนาจในการติดตามและรวบรวมพยานหลักฐานดิจิทัล เพื่อนำไปใช้เป็นหลักฐานในชั้นกระบวนพิจารณาของศาล

2) <u>การเก็บรักษาพยานหลักฐานดิจิทัล</u>

การเก็บรักษาจะต้องเก็บรักษาไว้ในสภาพที่รับฟังได้ในชั้นศาล เป็นไปตามกระบวนการสร้างห่วงโซ่คุ้มครองพยานหลักฐานในหลักสากล ต้องมีมาตรฐานการเก็บรักษาพยานหลักฐานดิจิทัลที่เป็นที่ยอมรับของทุกฝ่ายมีบันทึกขั้นตอนการคุ้มครองพยานหลักฐานและวิธีการเก็บรักษา เพื่อให้มั่นใจได้ว่าเป็นข้อมูลที่ไม่ได้ถูกแก้ไขเปลี่ยนแปลงนับจากที่ได้รับมาจากที่เกิดเหตุ มาตรฐานในการจัดเก็บและจัดการพยานหลักฐานดิจิทัลของเจ้าพนักงานที่เกี่ยวข้อง อาจทำให้เกิดประเด็นข้อโต้แย้งในการรับฟังพยานหลักฐานได้ เนื่องจากพยานหลักฐานดิจิทัลในรูปของข้อมูลคอมพิวเตอร์หรือข้อมูลอิเล็กทรอนิกส์ มีความเสี่ยงต่อการถูกเปลี่ยนแปลงแก้ไข สูญหาย เสียหาย โดยง่าย โดยเฉพาะอย่างยิ่งเมื่อต้องมีการส่งผ่านข้อมูลคอมพิวเตอร์หรือข้อมูลอิเล็กทรอนิกส์ระหว่างเจ้าพนักงานที่เกี่ยวข้องหลายทอด ในส่วนนี้ปัจจุบันสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. ได้

เผยแพร่เอกสาร “ข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐาน” เพื่อเป็นแนวทางเบื้องต้นให้กับเจ้าหน้าที่ที่เกี่ยวข้องกับการจัดเก็บ รวบรวม และตรวจพิสูจน์พยานหลักฐานดิจิทัล ให้ปฏิบัติงานในสถานที่เกิดเหตุและในห้องปฏิบัติการให้สอดคล้องกับมาตรฐานสากล โดยสพธอ. เน้นในเรื่องการให้ความสำคัญต่อการบันทึกแบบฟอร์มที่เรียกว่า “Chain of Custody” หรือห่วงโซ่คุ้มครองพยานหลักฐาน คือ กระบวนการระบุสายความรับผิดชอบการเก็บรักษาพยานหลักฐาน เริ่มตั้งแต่เมื่อพยานหลักฐานถูกเก็บรวบรวม เพื่อสร้างความต่อเนื่องของการครอบครองพยานหลักฐาน โดยข้อมูลที่เจ้าหน้าที่ผู้ปฏิบัติงานในแต่ละสายงาน จำเป็นต้องระบุ รวมถึงข้อมูลติดต่อและลงลายมือชื่อของผู้ส่งมอบพยานหลักฐาน, เหตุผลในการับ-ส่งมอบพยานหลักฐาน, วิธีการส่งมอบพยานหลักฐาน เช่น ส่งมอบโดยเจ้าหน้าที่ที่เกี่ยวข้องหรือส่งมอบโดยพนักงานส่งของ และสถานที่จัดเก็บพยานหลักฐาน เป็นต้น นอกจากนี้ International Organization on Computer Evidence หรือ IOCE ซึ่งเป็นหน่วยงานสากลที่ดูแลเกี่ยวกับการปฏิบัติต่อพยานหลักฐานดิจิทัล ได้กำหนดหลักการสำคัญ ในการเข้าค้นและยึดอุปกรณ์อิเล็กทรอนิกส์ไว้ 6 ประการ คือ

1. เมื่อใดก็ตามที่ต้องดำเนินการกับพยานหลักฐานดิจิทัล จะต้องมีการดำเนินการตามหลักปฏิบัติทั่วไปทางนิติคอมพิวเตอร์ และต้องดำเนินการตามขั้นตอนของนิติคอมพิวเตอร์
2. ในขณะปฏิบัติการเก็บยึดพยานหลักฐานดิจิทัล การดำเนินการทุกอย่างจะต้องไม่ก่อให้เกิดการเปลี่ยนแปลงต่อพยานหลักฐานนั้น
3. หากมีความจำเป็นที่จะต้องเข้าถึงข้อมูลในพยานหลักฐานต้นฉบับ เจ้าหน้าที่ผู้ปฏิบัติจะต้องได้รับการอบรมมาเพื่อดำเนินการเป็นการเฉพาะ
4. จะต้องมีการจดบันทึกรายละเอียดทุกขั้นตอน ทุกการกระทำที่เกี่ยวข้องกับการเก็บยึด การเข้าถึงข้อมูล การเคลื่อนย้าย และต้องมีการเก็บรักษาบันทึกนั้นไว้ และสามารถนำมาแสดงได้เมื่อถูกร้องขอ
5. จะต้องมีบุคคลผู้รับผิดชอบที่ชัดเจนในทุกกระบวนการที่เกิดขึ้นในขณะที่พยานหลักฐานดิจิทัลอยู่ในความดูแลของบุคคลนั้น
6. หน่วยงานและเจ้าหน้าที่ที่ดำเนินการเก็บยึด เข้าถึงข้อมูล บันทึกข้อมูล โอนถ่ายเคลื่อนย้ายพยานหลักฐานดิจิทัล จะต้องรับผิดชอบในการปฏิบัติงานให้สอดคล้องกับหลักการข้างต้น

3) <u>การวิเคราะห์พยานหลักฐานดิจิทัล</u>

พยานหลักฐานแต่ละประเภทของคดีจะมีความแตกต่างกัน วิธีวิเคราะห์จึงแตกต่างกัน มีการใช้เครื่องมือที่แตกต่างกัน ทักษะเจ้าหน้าที่แตกต่างกัน การฝึกอบรมเจ้าหน้าที่พิสูจน์หลักฐานจึงมีความสำคัญ การวิเคราะห์พยานหลักฐานดิจิทัล จึงต้องใช้ผู้เชี่ยวชาญด้านพยานหลักฐานดิจิทัลมาวิเคราะห์ โดยปกติแล้ว จะมีการใช้โปรแกรมคอมพิวเตอร์เฉพาะทาง ไม่ว่าจะเป็นโปรแกรมที่พัฒนาขึ้นโดยเฉพาะ หรือมีผู้พัฒนาสำหรับใช้วิเคราะห์พยานหลักฐานดิจิทัล เช่น โปรแกรมที่ใช้สำหรับตรวจสอบคอมพิวเตอร์และโทรศัพท์มือถือ สำหรับวิเคราะห์พยานหลักฐานดิจิทัลที่นิยมใช้ คือ Encase และ FTK

จะเป็นโปรแกรมที่พัฒนาและขายให้กับหน่วยงานที่ทำหน้าที่พิสูจน์หลักฐานทางดิจิทัล โดยเฉพาะ สามารถใช้กู้ข้อมูลที่ถูกลบ ซ่อน ไม่ว่าจะโดยผู้ใช้ หรือโดยระบบ สามารถค้นหาข้อมูลที่ถูกเปลี่ยนแปลง แก้ไข เข้ารหัส และอื่นๆ โดยทั่วไปแล้ว การวิเคราะห์พยานหลักฐานดิจิทัล จะมีการวิเคราะห์ต่างๆ ดังนี้

- Computer forensics เช่น บัญชีผู้ใช้ รอยประทับเวลา รูปภาพ อีเมลที่บันทึกอยู่ในฮาร์ดไดฟ์คอมพิวเตอร์ รวมทั้งบันทึกจากหน่วยความจำ
- Cell Phone forensics เช่น บันทึกที่สร้างขึ้นโดยผู้ให้บริการโทรศัพท์มือถืออย่างข้อมูลการเรียกเก็บเงิน การบันทึกการใช้บริการ ไม่ว่าหมายเลขที่โทรออก โทรเข้า ระยะเวลาการโทร วันเวลาการโทร สถานีเครือข่ายที่โทรศัพท์เครื่องนั้นใช้งาน รายชื่อในโทรศัพท์ ข้อความ รูปภาพ อีเมล ฯลฯ
- GPS Forensics เช่น ตำแหน่งที่ไปเมื่อเร็วๆ นี้ สถานที่ที่ชอบ หยุดที่สถานที่ใดบ้างนานเท่าใด ฯลฯ
- Social Media Forensics เช่น ข้อมูลเกี่ยวกับกิจกรรมออนไลน์ของกลุ่มเพื่อน การสื่อสาร กระทั่งแนวคิดของบุคคลผู้ต้องสงสัย
- Digital Video and Photo Forensics คือ การตรวจสอบรวมทั้งวิเคราะห์ภาพถ่าย
- Digital Camera Forensics เช่น ภาพถ่าย ข้อมูลเกี่ยวกับภาพ metadata รุ่นของกล้อง วันเวลาบันทึกภาพ
- Game Console forensics เช่น metadata ข้อมูลผู้เล่น บัญชีออนไลน์

4) <u>การนำเสนอผลพิสูจน์พยานหลักฐานดิจิทัล</u>

การนำเสนอผลการตรวจพิสูจน์พยานหลักฐานดิจิทัล เป็นรายงานบันทึกคำให้การผู้เชี่ยวชาญอธิบายวิธีการตรวจสอบ เครื่องมือที่ใช้ตรวจสอบ ตรวจสอบสิ่งใดบ้าง วิธีเก็บพยานหลักฐาน สิ่งที่ค้นพบและวิธีการยืนยันความแท้จริงของพยานหลักฐานดิจิทัล พยานหลักฐานดิจิทัลซึ่งพนักงานสอบสวนได้รวบรวมเพื่อพิสูจน์ว่าผู้ต้องหากระทำความผิดตามข้อกล่าวหา จะถูกนำเสนอต่อศาลระหว่างกระบวนการพิจารณาสืบพยาน โดยศาลมีอำนาจใช้ดุลพินิจรับฟังและชั่งน้ำหนักของพยานหลักฐานดิจิทัลตามที่กฎหมายกำหนด ปัจจุบันยังไม่มีบทบัญญัติเกี่ยวกับการรับฟังพยานหลักฐานดิจิทัลในคดีอาญาเป็นการเฉพาะเจาะจง การรับฟังพยานหลักฐานดิจิทัลจึงต้องเป็นไปตามหลักการรับฟังพยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาความอาญาอันเป็นบทกฎหมายทั่วไป ซึ่งมาตรา 226 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา บัญญัติไว้ว่า “พยานวัตถุ พยานเอกสาร หรือพยานบุคคลซึ่งน่าจะพิสูจน์ได้ว่าจำเลยมีผิดหรือบริสุทธิ์ ให้อ้างเป็นพยานหลักฐานได้ แต่ต้องเป็นพยานชนิดที่ไม่ได้เกิดขึ้นจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวงหรือโดยมิชอบประการอื่น และให้สืบตามบทบัญญัติแห่งประมวลกฎหมายนี้ หรือกฎหมายอื่นอันว่าด้วยการสืบพยาน” โดยคำว่า “...ที่ไม่ได้เกิดขึ้น...โดยมิชอบประการอื่น” จึงหมายถึงว่า กรณีที่มีกฎหมายเฉพาะอื่นที่ใช้บังคับหรือบัญญัติหลักเกณฑ์ และวิธีการในการได้มาซึ่งพยานหลักฐานดิจิทัลไว้ การรวบรวมพยานหลักฐานนั้นจะต้องต้องปฏิบัติให้ถูกต้องตามหลักเกณฑ์และวิธีการดังกล่าวนอกเหนือไปจากหลักเกณฑ์ทั่วไปตามประมวลกฎหมายวิธีพิจารณาความอาญาด้วย ไม่เช่นนั้นจะถือ

ว่าเป็นการได้พยานหลักฐานดิจิทัลมาโดยมิชอบ ศาลมีอำนาจไม่รับฟังได้ ดังนั้น การจัดเก็บรวบรวมพยานพยานหลักฐานดิจิทัลให้ชอบด้วยกฎหมายที่ใช้บังคับในแต่ละประเภทคดีจึงเป็นเรื่องที่สำคัญมาก เนื่องจากแม้ว่าในชั้นสอบสวน เจ้าพนักงานได้รวบรวมพยานหลักฐานที่เห็นว่าเพียงพอต่อการระบุตัวผู้กระทำความผิดและพิสูจน์ความผิดที่บุคคลนั้นกระทำแล้ว หากกระบวนการจัดเก็บพยานหลักฐานมีข้อโต้แย้งในเรื่องการได้มาซึ่งพยานหลักฐานดิจิทัลว่าเป็นไปโดยชอบด้วยกฎหมายหรือไม่ จะมีประเด็นในเรื่องของคุณค่าในการพิสูจน์ความผิดของพยานหลักฐานนั้น หรือไม่อาจรับฟังในชั้นพิจารณาหรือทำให้พยานหลักฐานนั้นมีน้ำ หนักในการรับฟังได้น้อย

4.1.1 ประเภทของพยานหลักฐานดิจิทัล

พยานหลักฐานดิจิทัล แบ่งออกเป็น 3 ประเภท ดังนี้

1) พยานหลักฐานที่มนุษย์สร้างขึ้น (Human Generated Evidence) คือ ข้อมูลหรือเนื้อหาที่เกิดจากมนุษย์จัดทำขึ้นหรือพิมพ์เข้าไปในระบบคอมพิวเตอร์ เช่น เนื้อหาการถามตอบในกระดานข่าวออนไลน์ บทสนทนาออนไลน์ เสียงอิเล็กทรอนิกส์ เป็นต้น
2) พยานหลักฐานที่คอมพิวเตอร์สร้างขึ้น (Computer Generated Evidence) คือ เมื่อมนุษย์สร้างเนื้อหา หรือข้อมูลขึ้น คอมพิวเตอร์จะบันทึกและสร้างข้อมูลขึ้นมาหนึ่งชุด เช่น ไฟล์ข้อมูลชั่วคราว (Temp File) ไฟล์บันทึกการทำงาน (Log File) ไฟล์ประวัติการทำงาน (History File) เป็นต้น
3) พยานหลักฐานที่มนุษย์และคอมพิวเตอร์ร่วมกันสร้างขึ้น (Hybrid Human and Computer Generated Evidence) เป็นข้อมูลที่ประกอบด้วยทั้งสองส่วนข้างต้น เช่น จดหมายอิเล็กทรอนิกส์ที่ส่งออก จะประกอบด้วยทั้งเนื้อหาที่ถูกพิมพ์เข้าไป และข้อมูลในส่วนของที่อยู่ต้นทาง การเข้ารหัสข้อความ ซึ่งถูกคอมพิวเตอร์สร้างขึ้น, ตารางหรือไฟล์ที่เป็นผลลัพธ์จากการป้อนข้อมูล และคอมพิวเตอร์คำนวณ เป็นต้น

4.1.2 หลักการพื้นฐานของการตรวจพิสูจน์พยานหลักฐานดิจิทัล

เริ่มต้นจากการตรวจพิสูจน์พยานหลักฐานทางคอมพิวเตอร์ในราวปี ค.ศ. 1980 โดยสำนักงานสืบสวนกลางของสหรัฐอเมริกา หรือ FBI และได้มีการพัฒนามาตรฐานการตรวจพิสูจน์พยานหลักฐานดิจิทัลต่อเนื่องมาโดยตลอด จนได้รับการรับรองให้ใช้ในหน่วยงานอื่นๆ ในสหรัฐอเมริกาและหลากหลายประเทศทั่วโลก ในปัจจุบันประเทศไทยไม่ได้มีการบัญญัติกฎหมายที่กำหนดมาตรฐานในการตรวจพิสูจน์พยานหลักฐานดิจิทัลไว้โดยเฉพาะ มีเพียง “ข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐานดิจิทัล” เพื่อเป็นแนวทางในการปฏิบัติงานของเจ้าหน้าที่ และมีการฝึกอบรมเจ้าหน้าที่ที่เกี่ยวข้อง เพื่อนำมาปรับใช้ในการตรวจพิสูจน์พยานหลักฐานดิจิทัลเท่านั้น

ในการตรวจพิสูจน์พยานหลักฐานดิจิทัลมีปัจจัยสำคัญหลายอย่างที่ควรต้องคำนึงถึง และระมัดระวังเพื่อไม่ให้เกิดความผิดพลาด โดยเฉพาะอย่างยิ่งการเลือกเครื่องมือที่เหมาะสมกับงาน การ

ทำความเข้าใจถึงวิธีการใช้เครื่องมือที่ถูกต้อง รวมถึงการจัดการอุปกรณ์ดิจิทัลในการตรวจพิสูจน์พยานหลักฐาน โดยมีมาตรฐานสากล ที่เป็นแนวปฏิบัติในการตรวจพิสูจน์พยานหลักฐาน เช่น ACPO Good Practice Guide for Digital Evidence; ISO/IEC 27037 Information technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence และ SWGDE Best Practices for Computer Forensics V3-1 และยังรวมถึงมาตรฐานการจัดการอุปกรณ์ดิจิทัลในการตรวจพิสูจน์พยานหลักฐานในการปฏิบัติงานทั้งใน สถานที่เกิดเหตุและในห้องปฏิบัติการ ตลอดจนการจัดการข้อมูลคอมพิวเตอร์ สื่อบันทึกข้อมูลดิจิทัล และเครื่องมือสื่อสารอื่นๆ ด้วย

หลักการปฏิบัติงานเกี่ยวกับพยานหลักฐานดิจิทัล ที่สอดคล้องกับมาตรฐานสากล มีหลักการที่สำคัญดังนี้

(1) ดำเนินการโดยผู้ที่ผ่านการฝึกอบรมทางเทคนิคด้านการตรวจพิสูจน์พยานหลักฐานดิจิทัล
(2) รักษาสภาพพยานหลักฐานไม่ให้ถูกเปลี่ยนแปลง หรือถูกเปลี่ยนแปลงน้อยที่สุด โดยผู้ปฏิบัติงานต้องสามารถอธิบาย และบันทึกเป็นลายลักษณ์อักษรแสดงถึงขั้นตอนการคุ้มครองพยานหลักฐานโดยละเอียด
(3) การคุ้มครองพยานหลักฐาน ต้องบันทึกข้อมูลในแบบฟอร์ม โดยมีรายละเอียด ได้แก่ ข้อมูลการติดต่อและลายมือชื่อของผู้ส่งมอบพยานหลักฐาน ข้อมูลการติดต่อและลายมือชื่อของผู้รับมอบพยานหลักฐาน วัน เวลาในการรับ-ส่งพยานหลักฐาน รายละเอียดในการรับ-ส่งพยานหลักฐาน วิธีการส่งมอบพยานหลักฐาน เช่น ส่งมอบโดยเจ้าหน้าที่ หรือส่งมอบโดยพนักงานส่งของ และสถานที่จัดเก็บพยานหลักฐานดิจิทัล เป็นต้น
(4) มีการบันทึกขั้นตอนการปฏิบัติงาน การเก็บรวบรวมและการวิเคราะห์พยานหลักฐานโดยละเอียด เพื่อให้ผู้ตรวจพิสูจน์อื่นสามารถเข้าใจได้ และหากทำซ้ำด้วยวิธีการเดิมและเครื่องมือที่มีลักษณะเดียวกัน จะต้องได้ผลลัพธ์เหมือนกัน
(5) บุคคลที่สามารถเข้าถึงพยานหลักฐาน ต้องเป็นผู้ที่ได้รับมอบหมาย หรือมีหน้าที่รับผิดชอบโดยตรงเท่านั้น และผู้ปฏิบัติงานต้องตระหนักถึงการดำเนินงานตามกฎหมายเกี่ยวข้องกับพยานหลักฐาน
(6) เครื่องมือและอุปกรณ์ต้องเป็นไปตามมาตรฐาน ตามหลักการตรวจพิสูจน์พยานหลักฐาน เช่น อยู่ในสภาพพร้อมใช้งานและเหมาะสมกับการตรวจพิสูจน์พยานหลักฐานแต่ละประเภท มีมาตรการในการป้องกันการเปลี่ยนแปลง และปนเปื้อนของพยานหลักฐาน ได้รับการตรวจสอบความถูกต้องแม่นยำของเครื่องมือก่อนใช้งานสม่ำเสมอ รวมถึงมีคู่มือการใช้งานหรือเอกสารอธิบายการใช้งานเพื่อใช้อ้างอิง

หลักการในการตรวจพิสูจน์พยานหลักฐานดิจิทัล หรือ ห่วงโซ่การคุ้มครองพยานหลักฐาน ได้แก่

(1) การระบุรูปพรรณ (Identification) คือ การระบุประเภทและที่ตั้งของพยานหลักฐานดิจิทัล เพื่อใช้ในการออกหมายเรียกหรือหมายค้น โดยคำที่ใช้ในการระบุรูปพรรณจะต้องมีความชัดเจน เฉพาะเจาะจงและใช้คำศัพท์ที่ถูกต้อง

(2) การเก็บรวบรวม (Collection) หรือ กระบวนการสร้างห่วงโซ่การคุ้มครองพยานหลักฐาน ถือเป็นขั้นตอนที่มีความสำคัญมาก เนื่องจากเป็นการสัมผัสพยานหลักฐานครั้งแรก หากไม่ทำตามขั้นตอนหรือวิธีการที่ถูกต้อง เหมาะสม จะส่งผลทำให้พยานหลักฐานถูกทำลายหรือเปลี่ยนแปลงได้ ในการเก็บรวบรวมนั้นจะต้องมีการถ่ายภาพพยานหลักฐานในสถานที่เกิดเหตุก่อนการรวบรวมพยานหลักฐาน มีการจดบันทึกรายละเอียดอย่างครบถ้วน เช่น ยี่ห้อ รุ่น หมายเลขเครื่อง และรายละเอียดอื่น ๆ

(3) การบรรจุและการเคลื่อนย้าย (Transport) ควรจัดเก็บพยานหลักฐานทุกชิ้นในบรรจุภัณฑ์ ปิดผนึกให้เรียบร้อย ติดหมายเลขกำกับพยานหลักฐานทุกชิ้นในบรรจุภัณฑ์ เพื่อป้องกันไม่ให้พยานหลักฐานถูกเปลี่ยนแปลงหรือเสียหายในระหว่างขนส่ง

(4) การสำเนาข้อมูล (Acquisition) เป็นการทำให้พยานหลักฐานต้นฉบับได้รับการป้องกันจากการเปลี่ยนแปลง ต้องทำโดยผู้ที่ผ่านการฝึกอบรมมาเท่านั้น เนื่องจากเป็นขั้นตอนที่อาจเกิดความผิดพลาดได้ง่าย จะต้องมีการใช้อุปกรณ์ป้องกันการเขียนทับข้อมูลบนอุปกรณ์เก็บข้อมูลต้นฉบับ

(5) การตรวจสอบ (Verification) การที่พยานหลักฐานจะเป็นที่ยอมรับในชั้นศาลได้นั้น จะต้องมีวิธีการตรวจสอบว่าพยานหลักฐานดิจิทัลที่นำเสนอตรงกับต้นฉบับที่เก็บรวบรวมมา เพื่อตรวจสอบทั้งต้นฉบับและสำเนาในระหว่างขั้นตอนการทำสำเนาข้อมูล

(6) การวิเคราะห์ (Analysis) ผู้ปฏิบัติงานต้องผ่านการฝึกอบรมและมีความเชี่ยวชาญในขอบข่ายที่จะตรวจพิสูจน์ โดยไม่ควรวิเคราะห์จากพยานหลักฐานต้นฉบับโดยตรง ให้ทำการวิเคราะห์จากสำเนาพยานหลักฐานที่ทำไว้แล้วข้างต้น

(7) การรายงานผลการตรวจพิสูจน์พยานหลักฐาน (Presentation) คือการนำเสนอผลการตรวจพิสูจน์เป็นลายลักษณ์อักษรหรือรายงานผลตรวจพิสูจน์พยานหลักฐานด้วยวาจา และทำบันทึกคำให้การของผู้เชี่ยวชาญ สำหรับใช้อ้างอิงในชั้นศาลโดยมีรายละเอียดของเครื่องมือที่ใช้ในการตรวจสอบ วิธีการที่ใช้ยืนยันความถูกต้องของข้อมูลกระบวนการและอุปกรณ์ที่ใช้ในการกู้ข้อมูลและทำสำเนาข้อมูล และรายงานแสดงผลการตรวจสอบเป็นต้น

หลักการตรวจพิสูจน์พยานหลักฐานดิจิทัลดังกล่าว มีความสำคัญอย่างมาก เพราะพยานหลักฐานทางดิจิทัลนั้นมีความอ่อนไหวมาก การปฏิบัติตามขั้นตอนที่ถูกต้องเป็นสิ่งสำคัญในการพิสูจน์ความถูกต้องแท้จริง(Authentication) ของพยานหลักฐานดิจิทัล

อย่างไรก็ตาม ในการตรวจพิสูจน์พยานหลักฐานดิจิทัลก็มีข้อจำกัดหลายประการ เช่น ยังต้องกระทำโดยผู้เชี่ยวชาญด้านการตรวจพิสูจน์พยานหลักฐานดิจิทัลเท่านั้น เนื่องจากการจัดการกับพยานหลักฐานจะต้องอาศัยความรู้ความเชี่ยวชาญ ในการจัดการกับข้อมูลที่ได้ และการทำงานที่เกี่ยวข้องในการรวบรวมและวิเคราะห์พยานหลักฐานนั้น ผู้เชี่ยวชาญจะต้องคำนึงถึงห่วงโซ่ของการคุ้มครองพยานหลักฐานเป็นสำคัญ

4.1.3 หลักการชั่งน้ำหนักพยาน และการรับฟังพยานหลักฐานดิจิทัล

จากการที่พยานหลักฐานดิจิทัลมีลักษณะเฉพาะ แม้จะไม่เป็นข้อที่จะไม่ถูกรับฟังในชั้นศาล เพียงเพราะเป็นพยานหลักฐานดิจิทัล แต่ศาลจะใช้ดุลยพินิจ โดยอาศัยหลักการดังนี้

1) <u>หลักการชั่งน้ำหนักพยานหลักฐานทั่วไป</u>

การชั่งน้ำหนักพยานหลักฐาน หมายถึง การที่ศาลจะนำพยานหลักฐานที่คู่ความนำสืบและเห็นว่าสามารถนำมารับฟังเป็นพยานหลักฐานได้ในชั้นศาล มาวินิจฉัยปัญหา ข้อเท็จจริงในประเด็นที่พิพาทกันให้เป็นที่ยุติโดยอาศัยพยานหลักฐาน

ในคดีอาญา อำนาจในการวินิจฉัยน้ำหนักของพยานหลักฐาน ศาลสามารถใช้ดุลยพินิจ ชั่งน้ำหนักพยานทั้งหมด และจะไม่พิพากษาลงโทษจำเลยจนกว่าจะแน่ใจได้ว่ามีการกระทำความผิดจริง และจำเลยเป็นผู้กระทำความผิดนั้น โจทก์จะต้องพิสูจน์ให้ศาลเห็นโดยปราศจากเหตุอันควรสงสัย ว่าจำเลยเป็นผู้กระทำความผิด ถ้ามีเหตุอันควรสงสัยอย่างใดอย่างหนึ่ง ว่าจำเลยไม่ใช่ผู้ที่กระทำความผิด ให้ยกประโยชน์แห่งความ สงสัยนั้นแก่จำเลย การวินิจฉัยชี้ขาดข้อเท็จจริงแห่งคดีของศาล จะใช้ดุลพินิจชั่งน้ำหนักพยานหลักฐานทั้งหมดในสำนวนว่าควรรับฟังได้หรือไม่ เพียงไร และไม่มีกฎหมายบทใดบัญญัติห้ามมิให้ศาลรับฟังคำให้การชั้นสอบสวนของพยานเป็นข้อประกอบการพิจารณาของศาล ส่วนจะรับฟังได้หรือไม่ เพียงใดนั้นแล้วแต่เหตุผลของแต่ละเรื่องไป

2) <u>หลักการชั่งน้ำหนักพยานหลักฐานดิจิทัล</u>

การรับฟังพยานหลักฐานดิจิทัลในคดีอาญามีหลักเกณฑ์ 3 ประการที่ศาลใช้ในการพิจารณาว่าสามารถยืนยันความถูกต้องแท้จริง (Authentication) ได้อย่างเหมาะสมหรือไม่ ซึ่งพยานหลักฐานดิจิทัลที่ศาลจะรับฟังและพิจารณาประกอบด้วย

1. เนื้อหาของเอกสารไม่ถูกเปลี่ยนแปลง
2. ข้อมูลในเอกสารเป็นไปตามเจตนาแท้จริงของผู้สร้างเอกสารนั้น ไม่ว่าผู้สร้างเอกสารจะเป็นมนุษย์ หรือคอมพิวเตอร์
3. ข้อมูลพิเศษในเอกสาร อันได้แก่ วัน เดือน ปีที่ถูกสร้าง ถูกต้อง หลักในการพิจารณาว่าพยานหลักฐานดิจิทัลมีความน่าเชื่อถือ สามารถรับฟังในชั้นศาลได้หรือไม่นั้น เป็นดุลยพินิจของศาลในการชั่งน้ำหนักพยานหลักฐาน โดยพิจารณาถึงความน่าเชื่อถือตามที่กำหนดไว้ในพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาตรา 11 วรรคสอง แก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ.2551 มาตรา 619 ซึ่งให้พิจารณาความน่าเชื่อถือจากลักษณะหรือ วิธีการที่ใช้สร้าง เก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์ ลักษณะหรือวิธีการเก็บรักษา ความ ครบถ้วน และไม่มีการเปลี่ยนแปลงของข้อความ ลักษณะหรือวิธีการที่ใช้ในการระบุหรือแสดงตัวผู้ส่งข้อมูล รวมทั้งพฤติการณ์ที่เกี่ยวข้องทั้งหมด

อย่างไรก็ตาม การชั่งน้ำหนัก และการรับฟังพยานหลักฐานดิจิทัลยังมีข้อจำกัด เนื่องจากพยานหลักฐานดิจิทัลง่ายต่อการถูกแก้ไขเปลี่ยนแปลง ส่วนใหญ่เป็นพยานหลักฐานที่เกิดจากการกระทำของมนุษย์ และเป็นการกระทำโดยฝ่ายใดฝ่ายหนึ่ง เป็นการแก้ไข เปลี่ยนแปลงหรือสร้างพยานหลักฐานดิจิทัลเท็จขึ้น ทำให้พยานผู้เชี่ยวชาญด้านการตรวจพิสูจน์พยานหลักฐานดิจิทัลจึงมี

ความสำคัญในการอธิบายให้ศาลเข้าใจลักษณะเฉพาะและวิธีการเข้าถึง การรวบรวมพยานหลักฐานว่าถูกต้องตามหลักการตรวจพิสูจน์พยานหลักฐานดิจิทัลหรือไม่ ประกอบกับผู้พิพากษาจะต้องมีความรู้พื้นฐานในการตรวจพิสูจน์พยานหลักฐานดิจิทัล สามารถพิจารณาถึงลักษณะการสืบสวนหาความเชื่อมโยงของข้อมูล การเก็บรักษา การตรวจสอบ และ การนำเสนอพยานหลักฐานประกอบกับพยานแวดล้อมอื่นๆ ในคดีด้วย กฎหมายที่เกี่ยวกับพยานหลักฐานดิจิทัล ก็ควรต้องมีบทบัญญัติไว้โดยเฉพาะ โดยกำหนดวิธีการ และกระบวนการการตรวจพิสูจน์พยานหลักฐานดิจิทัลและหลักการชั่งน้ำหนัก รับฟังพยานหลักฐานดิจิทัล เนื่องจากพยานหลักฐานดิจิทัลแตกต่างจากพยานหลักฐานทั่วไป

การตรวจพิสูจน์พยานหลักฐานดิจิทัล หากมีกระบวนการเก็บรวบรวมพยานหลักฐานที่ไม่เป็นไปตามรูปแบบมาตรฐานสากล จะส่งผลให้พยานหลักฐานดิจิทัลได้รับความเสียหาย สูญหาย หรือถูกปนเปื้อน รวมถึงการถูกแก้ไขเปลี่ยนแปลง และถ้ากระบวนการการตรวจพิสูจน์พยานหลักฐานดิจิทัลที่ไม่เป็นไปตามมาตรฐานเกิดขึ้นเรื่อยๆ ก็จะทำให้การตรวจพิสูจน์พยานหลักฐานดิจิทัลกลายเป็นการเก็บรวบรวมพยานหลักฐานตามหลักข้อยกเว้นที่ไม่เป็นไปตามรูปแบบ และข้อจำกัดในการตรวจพิสูจน์พยานหลักฐานดิจิทัลอีกประการหนึ่ง คือ ข้อจำกัดในบทบัญญัติทางกฎหมายในการรวบรวมพยานหลักฐานจากผู้ให้บริการอินเทอร์เน็ต ในคดีอาญาที่เกี่ยวข้องกับพยานหลักฐานดิจิทัลตามที่บัญญัติไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (แก้ไข เพิ่มเติม พ.ศ. 2560) กำหนดให้ผู้ให้บริการอินเทอร์เน็ตเก็บข้อมูลการจราจรทางคอมพิวเตอร์ไว้อย่างน้อย 90 วัน นับตั้งแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ ตามหลักเกณฑ์การเก็บรักษาข้อมูลการจราจรทางคอมพิวเตอร์ของผู้ให้บริการ ซึ่งข้อจำกัดดังกล่าว จะส่งผลกระทบโดยตรงกับฝ่ายที่ถูกกล่าวหา และไม่ใช่เจ้าหน้าที่รัฐที่มีอำนาจหน้าที่เกี่ยวกับพยานหลักฐานดิจิทัล ซึ่งผู้ให้ข้อมูลสำคัญกลุ่มที่ 1 ได้ให้ความเห็นไว้ว่า

> *“ประกาศ กสทช. เรื่องการเก็บข้อมูลการสัญจรทางคอมพิวเตอร์ของผู้ให้บริการ ซึ่งกำหนดให้ผู้ให้บริการเก็บข้อมูลไว้ 90 วัน แล้วจึงจะสามารถทำลายได้นั้น ส่งผลคือ ถ้าฝ่ายผู้ต้องหาหรือจำเลยจะเป็นฝ่ายใช้ข้อมูลนี้จะขอข้อมูลไม่ทัน เพราะจำเลยที่ถูกจับกุมและฝากขัง จะมีโอกาสที่จะพบทนายที่ศาลแต่งตั้งให้ครั้งแรกหลังจากครบฝากขังไปแล้ว กรณีนี้คือจำเลยไม่มีฐานะพอจะจ้างทนายเองและ ไม่มีระยะเวลาเพียงพอที่จะข้อมูลจากผู้ให้บริการ”*

4.1.4 กฎหมายที่เกี่ยวข้องกับกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล

กฎหมายได้บัญญัติถึงพยานหลักฐานที่สามารถใช้อ้างเพื่อพิสูจน์ ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226 อันเป็นบททั่วไปของหลักเรื่องพยานหลักฐานในคดีอาญา แบ่งเป็น 3 ประเภท ได้แก่ พยานบุคคล พยานเอกสาร และพยานวัตถุ

1) พยานบุคคล หมายถึง บุคคลที่รู้เห็นเหตุการณ์หรือข้อเท็จจริงในคดี หากบุคคล ดังกล่าวพบเห็นเหตุการณ์ ในขณะเกิดการกระทำความผิด จะเรียกว่า “ประจักษ์พยาน” ซึ่งถือว่าเป็นพยานโดยตรงในคดี แต่หากพยานบุคคลนั้นมิได้พบเห็นเหตุการณ์ในขณะเกิดการกระทำความผิดอัน เป็นข้อเท็จจริงที่คู่ความในคดีมุ่งประสงค์จะพิสูจน์ความมีอยู่ แต่ได้รู้เห็นข้อเท็จจริงอย่างอื่นซึ่งต้องอาศัยการอนุมานข้อเท็จจริงหรือรับฟังร่วมกับพยานอย่างอื่น จะ

เรียกว่า “พยานแวดล้อม” นอกจากนี้ บุคคลยังสามารถเป็นพยานบุคคล แม้มิได้ประสบพบเห็นเหตุการณ์การกระทำความผิด

2) พยานเอกสาร หมายถึง ข้อมูลความหมายที่ถูกสื่อด้วยกระดาษหรือวัตถุอื่นใดที่ทำให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข ผัง หรือแผนแบบอย่างอื่น ไม่ว่าจะโดยวิธีพิมพ์ ถ่ายภาพ หรือวิธีอื่นอันเป็นหลักฐานแห่งความหมายนั้น
3) พยานวัตถุ หมายถึง วัตถุสิ่งของ รวมถึงสัตว์ สิ่งมีชีวิต ที่ใช้อ้างอิงเพื่อให้ศาลตรวจดู อย่างไรก็ดีพยานเอกสาร และพยานวัตถุในบางกรณีก็มีความยากในการจำแนก

กล่าวคือ การอ้างเอกสารเป็นพยานในคดี ไม่ได้หมายความว่าเอกสารดังกล่าวจะเป็นพยานเอกสารในทุกกรณี เช่น หากเป็นการอ้างข้อความบางตอนในเอกสาร เพื่อพิสูจน์ข้อเท็จจริงตามข้อความนั้น จะถือว่าเป็นการอ้างเอกสารในฐานะที่เป็นพยานเอกสาร แต่หากอ้างลายมือชื่อในเอกสารเพื่อพิสูจน์ว่าเป็นลายมือชื่อที่จำเลยทำปลอมขึ้นในความผิดฐานปลอมเอกสาร หรืออ้างเอกสารทั้งเล่มเพื่อพิสูจน์ว่ามีการทำซ้ำซึ่งงานอันมีลิขสิทธิ์ จะถือว่าเป็นการอ้างเอกสารในฐานะที่เป็นพยานวัตถุ กล่าวอีกนัยหนึ่ง จะต้องพิจารณาโดยดูที่วัตถุประสงค์ในการใช้อ้างเอกสารเพื่อเป็นพยาน หากเป็นการอ้างเพื่อให้ศาลดูข้อความในเอกสารก็จัดเป็นพยานเอกสาร แต่หากเป็นการอ้างเพื่อให้ศาลดูรูปลักษณะของเอกสาร ก็จัดเป็นพยานวัตถุ

เหตุที่กฎหมายได้กำหนดประเภทของพยานหลักฐานดังกล่าวไว้ เพื่อให้สอดคล้องกับหลักการรับฟังพยานหลักฐานแต่ละประเภท โดยในส่วนของข้อมูลที่บันทึกอยู่ในระบบคอมพิวเตอร์ อาจจัดเป็นพยานเอกสารหรือพยานวัตถุตามแต่วัตถุประสงค์ในการใช้อ้างในคดี หากมีวัตถุประสงค์มุ่งยืนยันความถูกต้องแท้จริงของเนื้อความด้วยการนำข้อมูลอิเล็กทรอนิกส์ที่บันทึกไว้ในระบบคอมพิวเตอร์ประมวลผลผ่านชุดคำสั่งและอุปกรณ์ต่างๆ โดยทำออกมาในรูปของสิ่งพิมพ์ ในรูปของเอกสาร และมีเนื้อหาตรงกันกับที่แสดงอยู่ ก็จะจัดเป็นพยานเอกสาร แต่หากการใช้อ้างข้อมูลที่บันทึกอยู่ในระบบคอมพิวเตอร์ เพื่อมุ่งยืนยันความมีอยู่ของข้อมูล อิเล็กทรอนิกส์ ด้วยการนำระบบคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ที่บันทึกข้อมูลไว้มานำสืบ ด้วยการแสดงออกในรูปแบบที่เข้าใจได้ และทำให้เห็นว่าเป็นข้อมูลที่ระบบคอมพิวเตอร์แสดงออกมา เป็นข้อมูลถูกต้องแท้จริง ไม่มีการแก้ไข หรือทำลายให้เกิดความเสียหาย ก็จะจัดเป็นพยานวัตถุ

เพื่อให้ผลการตรวจพิสูจน์พยานหลักฐานดิจิทัล ได้รับการยอมรับและรับฟังได้ในชั้นศาล ต้องมีการพิจารณาถึงกฎหมายที่เกี่ยวข้องดังนี้

4.1.4.1 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ฉบับที่ 4 พ.ศ. 2562

ตามมาตรา 7 ที่ห้ามมิให้ปฏิเสธความมีผลผูกพันและการบังคับใช้ทางกฎหมายของข้อความใด เพียงเพราะเหตุที่ข้อความนั้นอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ มาตรา 10 ในกรณีที่กฎหมายกำหนดให้นำเสนอหรือเก็บรักษาข้อความใดในสภาพที่เป็นมาแต่เดิมอย่างเอกสารต้นฉบับ ถ้าได้นำเสนอหรือเก็บรักษาในรูปข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์ดังต่อไปนี้ ให้ถือว่าได้มีการนำเสนอหรือเก็บรักษาเป็นเอกสารต้นฉบับตามกฎหมายแล้ว มาตรา 11 ห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐาน ในกระบวนการพิจารณาตามกฎหมายเพียงเพราะเหตุว่าเป็นข้อมูล

อิเล็กทรอนิกส์ ในการชั่งน้ำหนักพยานหลักฐานว่าข้อมูลอิเล็กทรอนิกส์จะเชื่อถือได้หรือไม่เพียงใดนั้น ให้พิเคราะห์ถึงความน่าเชื่อถือของลักษณะหรือวิธีการที่ใช้สร้าง เก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์ ลักษณะหรือวิธีการรักษา ความครบถ้วน และไม่มีการเปลี่ยนแปลงของ ข้อความ ลักษณะหรือวิธีการที่ใช้ในการระบุหรือแสดงตัวผู้ส่งข้อมูล รวมทั้งพฤติการณ์ที่เกี่ยวข้องทั้งปวง และ มาตรา 25 ธุรกรรมทางอิเล็กทรอนิกส์ใดที่ได้กระทำตามวิธีการแบบปลอดภัยที่กำหนดในพระราชกฤษฎีกา ให้สันนิษฐานว่าเป็นวิธีการที่เชื่อถือได้ จะเห็นได้ว่า พยานหลักฐานดิจิทัล มีกฎหมายรองรับ สามารถรับฟังได้ในชั้นศาล หากมีมาตรฐานที่สามารถพิสูจน์ได้ถึงการรักษาความถูกต้อง สิ่งสำคัญที่จะทำให้การตรวจพิสูจน์พยานหลักฐานดิจิทัล ได้รับการยอมรับในชั้นศาล โดยไม่ถูกโต้แย้ง คือ ต้องสามารถยืนยันได้ว่าหลักฐานที่นำมาตรวจสอบ เป็นหลักฐานเดียวกับที่เก็บมาจากสถานที่เกิดเหตุจริง (Authentication) และไม่มีการเปลี่ยนแปลงข้อมูลใดๆ ไปจากเดิม (Integrity) ซึ่งในการจะยืนยันคุณสมบัติทั้งสองข้อนี้ได้นั้น ต้องอาศัยหลักการสำคัญของการตรวจพิสูจน์พยานหลักฐานดิจิทัล คือ Chain of custody และ Hash value

4.1.4.2 ประมวลกฎหมายวิธีพิจารณาความอาญา

มาตรา 226 เป็นบททั่วไปของหลักเรื่องพยานหลักฐานในคดีอาญา ได้บัญญัติถึงพยานหลักฐานที่ใช้อ้างเพื่อพิสูจน์ว่าจำเลยมีผิดหรือบริสุทธิ์ แบ่งเป็น 3 ประเภท ได้แก่ พยานบุคคล พยานเอกสาร และพยานวัตถุ ดังนั้น การอ้างเอกสารเป็นพยานในคดี ไม่ได้หมายความว่าเอกสารดังกล่าวจะเป็นพยานเอกสารในทุกกรณี เช่น หากเป็นการอ้างข้อความบางตอนในเอกสาร เพื่อพิสูจน์ข้อเท็จจริงตามข้อความนั้น จะถือว่าเป็นการอ้างเอกสารในฐานะที่เป็นพยานเอกสาร แต่หากอ้างลายมือชื่อในเอกสารเพื่อพิสูจน์ว่าเป็นลายมือชื่อที่จำเลยทำปลอมขึ้นในความผิดฐานปลอมเอกสาร หรืออ้างเอกสารทั้งเล่มเพื่อพิสูจน์ว่ามีการทำซ้ำซึ่งงานอันมีลิขสิทธิ์ จะถือว่าเป็นการอ้างเอกสารในฐานะที่เป็นพยานวัตถุ กล่าวอีกนัยหนึ่ง จะต้องพิจารณาโดยดูที่วัตถุประสงค์ในการใช้อ้างเอกสารเพื่อเป็นพยาน หากเป็นการอ้างเพื่อให้ศาลดูข้อความในเอกสารก็จัดเป็นพยานเอกสาร แต่หากเป็นการอ้างเพื่อให้ศาลดูรูปลักษณะของเอกสาร ก็จัดเป็นพยานวัตถุ

เหตุที่กฎหมายได้กำหนดประเภทของพยานหลักฐานดังกล่าวไว้ เพื่อให้สอดคล้องกับหลักการรับฟังพยานหลักฐานแต่ละประเภท โดยในส่วนของข้อมูลที่บันทึกอยู่ในระบบคอมพิวเตอร์ อาจจัดเป็นพยานเอกสารหรือพยานวัตถุตามแต่วัตถุประสงค์ในการใช้อ้างในคดี หากมีวัตถุประสงค์มุ่งยืนยันความถูกต้องแท้จริงของเนื้อความด้วยการนำข้อมูลอิเล็กทรอนิกส์ที่บันทึกไว้ในระบบคอมพิวเตอร์ประมวลผลผ่านชุดคำสั่งและอุปกรณ์ต่างๆ โดยทำออกมาในรูปของสิ่งพิมพ์ ในรูปของเอกสาร และมีเนื้อหาตรงกันกับที่แสดงอยู่ ก็จะจัดเป็นพยานเอกสาร แต่หากการใช้อ้างข้อมูลที่บันทึกอยู่ในระบบคอมพิวเตอร์ เพื่อมุ่งยืนยันความมีอยู่ของข้อมูล อิเล็กทรอนิกส์ ด้วยการนำระบบคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ที่บันทึกข้อมูลไว้มานำสืบ ด้วยการแสดงออกในรูปแบบที่เข้าใจได้ และทำให้เห็นว่าเป็นข้อมูลที่ระบบคอมพิวเตอร์แสดงออกมา เป็นข้อมูลถูกต้องแท้จริง ไม่มีการแก้ไข หรือทำลายให้เกิดความเสียหาย ก็จะจัดเป็นพยานวัตถุ พนักงานสอบสวนมีอำนาจรวบรวมพยานหลักฐานตามประมวลกฎหมาย วิธีพิจารณาความอาญา มาตรา 132 อันเป็นบทกฎหมายทั่วไป แต่บทกฎหมายดังกล่าวมิได้บัญญัติเกี่ยวกับการรวบรวมพยานหลักฐานที่เป็นอุปกรณ์ดิจิทัลหรือ

ข้อมูลคอมพิวเตอร์ไว้โดยตรง ซึ่งคดีอาญาบางประเภทความผิด มีกฎหมายบัญญัติเอาไว้โดยเฉพาะในเรื่องของอำนาจของพนักงานสอบสวนหรือเจ้าพนักงานผู้มีอำนาจรวบรวมพยานหลักฐาน และหลักเกณฑ์วิธีการในการรวบรวมและจัดเก็บพยานหลักฐาน พนักงานสอบสวนหรือเจ้าพนักงานเหล่านั้นก็จะต้องปฏิบัติให้เป็นไปตามบทบัญญัติกฎหมายเฉพาะดังกล่าวนั้นด้วย เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

4.1.4.3 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560

มีส่วนที่เกี่ยวข้องกับกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล คือ มาตรา 18 ภายใต้บังคับมาตรา 19 เพื่อประโยชน์ในการสืบสวนและสอบสวน ในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ หรือในกรณีที่มีการร้องขอ ตามวรรคสองให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่ง อย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด และหาตัวผู้กระทำความผิด

1) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิด มาเพื่อให้ถ้อยคำส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูลหรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้
2) เรียกข้อมูลการจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง
3) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา 26 หรือที่อยู่ในความครอบครอง หรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่หรือให้เก็บข้อมูลดังกล่าวไว้ก่อน
4) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลการจราจรทางคอมพิวเตอร์จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิด ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่
5) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่
6) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลการจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดหรือเพื่อสืบสวนหาตัวผู้กระทำความผิด และสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ ข้อมูลการจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

7) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

8) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะ เพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิด

เพื่อประโยชน์ในการสืบสวนและสอบสวนของพนักงานสอบสวน ตามประมวลกฎหมายวิธีพิจารณาความอาญา ในความผิดอาญาต่อกฎหมายอื่นซึ่งได้ใช้ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์เป็นองค์ประกอบหรือเป็นส่วนหนึ่งในการกระทำความผิดหรือมีข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับการกระทำความผิดอาญาตามกฎหมายอื่น พนักงานสอบสวนอาจร้องขอให้พนักงานเจ้าหน้าที่ตามวรรคหนึ่งดำเนินการตามวรรคหนึ่งก็ได้ หรือหากปรากฏข้อเท็จจริงดังกล่าวต่อพนักงานเจ้าหน้าที่เนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่รีบรวบรวมข้อเท็จจริงและหลักฐานแล้ว แจ้งไปยังเจ้าหน้าที่ที่เกี่ยวข้องเพื่อดำเนินการต่อไป

ให้ผู้ได้รับการร้องขอจากพนักงานเจ้าหน้าที่ตามวรรคหนึ่ง (1) (2) และ (3) ดำเนินการตามคำร้องขอโดยไม่ชักช้า แต่ต้องไม่เกินเจ็ดวันนับแต่วันที่ได้รับคำร้องขอ หรือภายในระยะเวลาที่พนักงานเจ้าหน้าที่กำหนดซึ่งต้องไม่น้อยกว่าเจ็ดวันและไม่เกินสิบห้าวัน เว้นแต่ในกรณีที่มีเหตุสมควร ต้องได้รับอนุญาตจากพนักงานเจ้าหน้าที่ ทั้งนี้ รัฐมนตรีอาจประกาศในราชกิจจานุเบกษา กำหนดระยะเวลาที่ต้องดำเนินการที่เหมาะสมกับประเภทของผู้ให้บริการก็ได้

มาตรา 19 การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา 18 (4) (5) (6) (7) และ (8) ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำ หรือกำลังจะกระทำการอย่างหนึ่งอย่างใดอันเป็นความผิด เหตุที่ต้องใช้อำนาจลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิดเท่าที่สามารถจะระบุได้ ประกอบคำร้องด้วย ในการพิจารณาคำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็ว

เมื่อศาลมีคำสั่งอนุญาตแล้ว ก่อนดำเนินการตามคำสั่งของศาล ให้พนักงานเจ้าหน้าที่ส่งสำเนาบันทึกเหตุอันควรเชื่อที่ทำให้ต้องใช้อำนาจตามมาตรา 18 (4) (5) (6) (7) และ (8) มอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐาน แต่ถ้าไม่มีเจ้าของหรือ ผู้ครอบครองเครื่องคอมพิวเตอร์อยู่ ณ ที่นั้น ให้พนักงานเจ้าหน้าที่ส่งมอบสำเนาบันทึกนั้นให้แก่เจ้าของหรือผู้ครอบครองดังกล่าวในทันทีที่กระทำได้

ให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าในการดำเนินการตามมาตรา 18 (4) (5) (6) (7) และ (8) ส่งสำเนาบันทึกรายละเอียดการดำเนินการ และเหตุผลแห่งการดำเนินการให้ศาลที่มี เขตอำนาจภายในสี่สิบแปดชั่วโมงนับแต่เวลาลงมือดำเนินการ เพื่อเป็นหลักฐาน

การทำสำเนาข้อมูลคอมพิวเตอร์ตามมาตรา 18 (4) ให้กระทำได้เฉพาะเมื่อมีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิด และต้องไม่เป็นอุปสรรคในการดำเนินกิจการของเจ้าของหรือ ผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นเกินความจำเป็น

การยึดหรืออายัดตามมาตรา 18 (8) นอกจากจะต้องส่งมอบสำเนาหนังสือแสดง การยึดหรืออายัดมอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐานแล้ว พนักงานเจ้าหน้าที่จะสั่งยึดหรืออายัดไว้เกินสามสิบวันมิได้ ในกรณีจำเป็นที่ต้องยึดหรืออายัดไว้นานกว่านั้น ให้ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอขยายเวลายึดหรืออายัดได้ แต่ศาลจะอนุญาตให้ขยายเวลาครั้งเดียวหรือหลายครั้งรวมกันได้อีกไม่เกินหกสิบวัน เมื่อหมดความจำเป็นที่จะยึดหรือ อายัด หรือครบกำหนดเวลาดังกล่าวแล้ว พนักงานเจ้าหน้าที่ต้องส่งคืนระบบคอมพิวเตอร์ที่ยึดหรือถอนการอายัดโดยพลัน

หนังสือแสดงการยึดหรืออายัดตามวรรคห้าให้เป็นไปตามที่กำหนดในกฎกระทรวง

มาตรา 25 ข้อมูล ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ที่ พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้หรือที่พนักงานสอบสวนได้มาตามมาตรา 18 วรรคสอง ให้อ้างและรับฟังเป็นพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญาหรือกฎหมายอื่นอันว่าด้วยการสืบพยานได้ แต่ต้องเป็นชนิดที่มิได้เกิดขึ้นจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบประการอื่น

4.2 ปัญหาและอุปสรรคกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลในประเทศไทย

จากการเก็บข้อมูลในเขตกรุงเทพมหานครและปริมณฑล และการวิจัยเอกสาร ผู้วิจัยพบว่ากระบวนการตรวจพิสูจน์หลักฐานดิจิทัลในประเทศไทย มีประเด็นที่เป็นข้อสงสัยทางสังคม ที่น่าสนใจตามดังต่อไปนี้

4.2.1 ปัญหาและอุปสรรคในการรวบรวมพยานหลักฐานดิจิทัล

ผู้ให้ข้อมูลสำคัญกลุ่มที่ 2 มีข้อสงสัยว่า

“พยานหลักฐานอิเล็กทรอนิกส์น่าจะเป็นสิ่งที่เปลี่ยนแปลงง่าย “ในฐานะผมเป็นประชาชนธรรมดา ท่านเอาคอมพิวเตอร์ไป เราจะรู้ได้อย่างไร ว่าท่านจะไม่เอาข้อมูลอื่นใส่เข้าไปเพื่อที่จะเอาผิดเรา””

ในประเด็นนี้ ผู้ให้ข้อมูลสำคัญกลุ่มที่ 1 ได้อธิบายไว้ดังนี้

“การเปลี่ยนแปลงพยานหลักฐานอิเล็กทรอนิกส์ดังกล่าวไม่ได้กระทำได้ง่าย เหมือนกับ “การยัดยาบ้า” เนื่องจากในคอมพิวเตอร์นั้น เมื่อมีการเปลี่ยนแปลงเกิดขึ้น ความเปลี่ยนแปลงนั้นจะถูกบันทึกไว้ในคุณลักษณะเฉพาะของไฟล์ เช่น ข้อมูลในไฟล์ใหม่ที่ใส่เข้ามานี้ถูกนำเข้ามาเมื่อใด ซึ่งเป็นสิ่งที่สามารถพิสูจน์ได้ ส่วนฮาร์ดดิสก์ การพิสูจน์ความน่าเชื่อถือของฮาร์ดดิสก์ที่เจ้าหน้าที่พิสูจน์หลักฐานได้โคลนมา คือการเทียบค่า แฮช ว่าฮาร์ดดิสก์ที่โคลนมามีค่า แฮช ตรงกับค่าในฮาร์ดดิสก์ต้นฉบับของจำเลยหรือไม่ อย่างไรก็ตาม พยานหลักฐานอิเล็กทรอนิกส์เป็นเพียงส่วนประกอบหนึ่งเท่านั้น ในการระบุตัวผู้กระทำผิด อาจต้องใช้พยานหลักฐานอื่นมาประกอบด้วย” และ

“การใช้พยานหลักฐานอิเล็กทรอนิกส์จะต้องมีมาตรฐาน อย่างแรกคือ ต้องไม่มีการเปลี่ยนแปลงในพยานหลักฐาน ตั้งแต่ขั้นตอนการเก็บจนกระทั่งถึงศาล เจ้าหน้าที่ที่เกี่ยวข้อง

ต้องผ่านการอบรมมาโดยเฉพาะ รวมทั้งการปฏิบัติหน้าที่และการดำเนินการทั้งหมด จะต้องได้รับการจดบันทึกไว้ในเอกสารเพื่อให้ตรวจสอบย้อนกลับได้ด้วย”

ผู้ให้ข้อมูลสำคัญกลุ่มที่ 1 ให้รายละเอียดไว้ว่า

“ในกรณีของการดักรับข้อมูล ตามพระราชบัญญัติคอมพิวเตอร์ฯ การใช้มาตรา 18 (5)-(8) ของพระราชบัญญัติคอมพิวเตอร์ เพื่อเข้าถึงข้อมูลต้องขออำนาจศาลทั้งสิ้น ซึ่งส่วนใหญ่ข้อมูลที่ขอศาลดักฟัง คือข้อมูลที่ไม่สามารถหาได้โดยวิธีการตามปกติ และเมื่อศาลอนุญาตแล้ว เจ้าหน้าที่ต้องส่งเอกสารชี้แจงต่อศาลอย่างละเอียดถึงวิธีการเข้าถึงข้อมูลต่างๆ และรายละเอียดต่างๆ รวมทั้งต้องทำรายงานต่อศาลด้วย ตนเองคิดว่าในกรณีนี้ ไม่ค่อยน่าเป็นห่วงเท่าใดนัก”

“เจ้าหน้าที่จะไม่ดักฟังข้อมูลทั้งระบบ เพราะข้อมูลมีจำนวนมาก ระบบไม่สามารถรองรับได้อยู่แล้ว แต่จะจำกัดไปเฉพาะบางจุด และในการดักฟังจะไม่ไปรบกวนระบบ เพราะจะไม่ได้ใช้เทคนิค “man in the middle”(เทคนิคการเข้ามาแทรกเป็นตัวกลางดักการรับ ส่งข้อมูลระหว่างผู้ใช้กับเครือข่าย หรือผู้รับ: ผู้วิจัย)”

“ในการขอและการอนุญาตของศาลจะอนุญาตเป็นรายกรณี และหากกรณีนั้นมีหลายจุดที่ต้องดักฟัง ศาลจะให้เข้าไปเพียงจุดเดียวก่อน และต้องรายงานผลการดักฟังด้วย หากต้องการดักฟังที่จุดใหม่จะต้องยื่นขอต่อศาลอีกครั้งหนึ่ง ซึ่งเป็นเช่นเดียวกับกรณีการให้ศาลพิจารณาปิดกั้นเว็บไซต์”

ผู้ให้ข้อมูลสำคัญกลุ่มที่ 1 ได้ให้รายละเอียดว่า

“สำหรับเฟซบุ๊ก เวลาที่เราใช้ จะมีร่องรอยการใช้งานปรากฏอยู่ในเครื่องของเรา ซึ่งเจ้าหน้าที่สามารถตรวจสอบพบได้ แต่หากเมื่อผลตรวจสอบออกมาแล้วผู้ถูกกล่าวหาไม่เห็นด้วยกับผล ก็มีสิทธิเรียกร้อง ขอให้มีการตรวจพิสูจน์ซ้ำ หรือขอให้หน่วยงานอื่นที่เป็นหน่วยงานกลางพิสูจน์ได้”

และ

“นอกจากการใช้กฎหมายแล้ว มาตรการทางเทคโนโลยี ก็เป็นอีกหนทางหนึ่งที่สามารถช่วยสร้างความเสมอภาคในการต่อสู้คดีได้ โดยมาตรการทางเทคโนโลยีสามารถช่วยสร้างพยานหลักฐานยืนยันตัวเรา ว่าเราเคยอยู่ที่ตรงนี้ ในเวลานี้ และเป็นหลักฐานที่ตัวเราสามารถอ้างอิง บริหารจัดการได้ และสามารถนำมาใช้เป็นหลักฐานยืนยันความบริสุทธิ์ของตัวเราเองเวลาที่มีคดีเกิดขึ้น นอกจากนี้ในอนาคต เมื่อเทคโนโลยีพัฒนาไปมากขึ้น ผู้ใช้ก็จะช่วยเหลือตัวเองได้มากขึ้นและไม่ต้องพึ่งพาภาครัฐหรือผู้ให้บริการแต่เพียงอย่างเดียว”

4.2.2 ปัญหาและอุปสรรคในขั้นตอนการจัดเก็บพยานหลักฐานดิจิทัล

ผู้ให้ข้อมูลสำคัญกลุ่มที่ 2 ได้ตั้งข้อสงสัยในประเด็นของ ขั้นตอนการจัดการกับพยานหลักฐานดิจิทัล ไว้ดังนี้

“สมมติว่า ผมเป็นผู้ต้องสงสัยและโดนยึดมือถือของผมไป มือถือผมจะไปอยู่ที่ไหน ที่ใครบ้าง จนกระทั่งถึงศาล”

โดยมีคำอธิบายเพิ่มเติม จากผู้ให้ข้อมูลสำคัญกลุ่มที่ 1 คือ

“สำหรับการยึดมือถือ สิ่งแรกที่ต้องทำคือ ตัดการติดต่อสื่อสาร เช่น ตั้งค่าให้เป็นโหมดการบิน และต้องให้เจ้าของเครื่องเซ็นรับทราบ สำหรับขั้นตอนการตรวจพิสูจน์ ผู้ตรวจพิสูจน์ซึ่งจะไม่ใช่คนเดียวกับเจ้าหน้าที่ตำรวจที่ยึดมือถือมา จะตรวจพิสูจน์ตามที่ถูกร้องขอมาว่าต้องการให้ค้นหาอะไร เช่น หากต้องการหาข้อความหมิ่นประมาท ก็จะหาแค่ส่วนนั้น ผลตรวจจะออกมาเป็นรายงาน เพื่อส่งให้ตำรวจดำเนินการต่อ เมื่อถึงขั้นตอนดังกล่าว หากเจ้าของมือถืออยากได้เครื่องคืนก็สามารถยื่นคำร้องได้ และเจ้าหน้าที่จะเป็นผู้พิจารณาว่าสมควรคืนเครื่องให้หรือไม่ ซึ่งหากคืนเครื่อง เครื่องนั้นจะอยู่ในสภาพสมบูรณ์ สามารถนำไปใช้งานได้ต่อตามปกติ สำหรับข้อมูลจากการตรวจ ก็จะไหลไปสู่ชั้นสอบสวน อัยการ และศาล ซึ่งในเบื้องต้น ผู้ตรวจหลักฐานคือเจ้าหน้าที่ตำรวจ แต่หากผลการตรวจออกมาแล้วจำเลยเห็นว่าไม่เป็นธรรม ก็อาจขอให้หน่วยงานอื่นตรวจเพิ่มเติมได้ แต่ในบางกรณี เช่น ในกรณีที่รัฐเป็นโจทก์ ก็อาจไม่เหมาะสมที่จะให้เจ้าหน้าที่ตำรวจเป็นผู้ตรวจ ศาลก็อาจให้เอกชนเป็นผู้ตรวจได้”

“หากผลตรวจทั้ง 2 ครั้งออกมาไม่ตรงกัน มีข้อสงสัย ก็อาจมีการขอให้หน่วยงานที่ 3 เข้ามาเป็นผู้ตรวจ เช่นเดียวกับการตรวจศพ และในขั้นตอนการตรวจพิสูจน์หลักฐานทางอิเล็กทรอนิกส์ เช่น คอมพิวเตอร์ หากเจ้าหน้าที่ต้องการตรวจหาหลักฐานที่เกี่ยวข้องกับความผิดหนึ่งๆ แต่ไปพบไฟล์ที่เป็นความผิดอย่างอื่นด้วย จะสามารถเอาผิดกับเจ้าของคอมพิวเตอร์ในฐานความผิดอย่างอื่นด้วยได้ไหม คำตอบก็คือ สามารถทำได้ โดยอาศัยข้อยกเว้นตามพระราชบัญญัติประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226/1”

4.2.3 ปัญหาและอุปสรรคในการวิเคราะห์พยานหลักฐานดิจิทัล

ผู้ให้ข้อมูลสำคัญกลุ่มที่ 1 ยกตัวอย่างว่า

“ในบางคดีที่มีเรื่องอีเมลมาเกี่ยวข้องกับการกระทำผิด เจ้าหน้าที่สอบปากคำผู้ต้องหาอย่างเดียวโดยไม่พิมพ์อีเมลออกมา หรือบางคดีพิมพ์อีเมลออกมาประกอบ ทว่าไม่พิมพ์ header ของอีเมลออกมาด้วย หรือในบางคดี เจ้าหน้าที่ให้ผู้เสียหายเก็บพยานหลักฐานอิเล็กทรอนิกส์มาเอง ซึ่งปัญหาก็คือผู้เสียหายแต่ละคนก็มีองค์ความรู้ไม่เท่ากัน พยานหลักฐานที่ได้มาจึงมีความหลากหลายและมีความน่าเชื่อถือแตกต่างกัน ทำให้ในฐานะอัยการ บางครั้งก็ไม่มั่นใจในความบริสุทธิ์ของพยานหลักฐานเหล่านั้น”

ผู้ให้ข้อมูลสำคัญกลุ่มที่ 1 เสริมเพิ่มเติมว่า

> “ปัญหาหลักคือเจ้าหน้าที่ตำรวจไม่มีความรู้เกี่ยวกับการจัดการพยานหลักฐานอิเล็กทรอนิกส์ ไม่ได้มีความตั้งใจจะทำให้พยานหลักฐานปนเปื้อน ที่ผ่านมาเคยมีการแปลคู่มือปฏิบัติงานจากต่างประเทศให้กับเจ้าหน้าที่ตำรวจ แต่พบว่าหลายครั้งเจ้าหน้าที่ไม่ทำตามคู่มือดังกล่าว เพราะเจ้าหน้าที่เห็นว่าวิธีปฏิบัติยุ่งยากเกินไป การทำแนวทางในการปฏิบัติงานให้เจ้าหน้าที่ตำรวจ โดยไม่จำเป็นต้องลงรายละเอียดมากเกินไปนัก จะช่วยให้เจ้าหน้าที่จัดการกับพยานหลักฐานอิเล็กทรอนิกส์ได้ดีขึ้น”

> *“รื่องการขาดแคลนบุคลากรและค่าตอบแทนบุคคลากรที่ไม่ดึงดูดเป็นสาเหตุสำคัญหนึ่ง นอกไปจากปัญหาเรื่องการขาดแคลนงบประมาณ”*

> *“ทุกวันนี้เจ้าพนักงานประสบปัญหาเรื่องการจัดซื้อ ตามทฤษฎีแล้วการตรวจพยานหลักฐานอิเล็กทรอนิกส์ในคอมพิวเตอร์จำเป็นต้องมีการทำสำเนาข้อมูลทั้งหมด แต่ทุกวันนี้ไม่สามารถทำสำเนาได้หมด เนื่องจากพื้นที่เก็บข้อมูลไม่เพียงพอ บางครั้งเจ้าหน้าที่ตำรวจบอกจำเลยว่าหากไม่มีฮาร์ดดิสก์มาให้ เจ้าหน้าที่ก็ไม่ทำสำเนาข้อมูลให้ เพราะไม่มีงบสำหรับซื้อฮาร์ดดิสก์เป็นต้น”*

ผู้ให้ข้อมูลสำคัญกลุ่มที่ 2 เพิ่มเติมว่า

> *“ปัญหาที่ประสบจากการเป็นผู้ดูแลห้องตรวจพิสูจน์พยานหลักฐานอิเล็กทรอนิกส์ที่ผ่านมาพบว่าเจ้าหน้าที่ตำรวจที่นำพยานหลักฐานอิเล็กทรอนิกส์มาให้ตรวจขาดความรู้ในเรื่องนี้ และมักไม่ทราบชัดเจนว่าสิ่งที่ต้องการให้ห้องตรวจตรวจพิสูจน์คืออะไร”*

4.2.4 ปัญหาและอุปสรรคในการนำเสนอพยานหลักฐานดิจิทัลสู่ชั้นศาล

ผู้ให้ข้อมูลสำคัญกลุ่มที่ 1 อธิบายว่า

> *“เจ้าหน้าที่ตำรวจในฐานะผู้รวบรวมพยานหลักฐาน จะรวบรวมพยานหลักฐานเป็นสำนวนเพื่อส่งให้อัยการ และอาจมีการสอบปากคำผู้ตรวจพิสูจน์พยานหลักฐานอิเล็กทรอนิกส์ ผู้ตรวจพิสูจน์อาจต้องขึ้นเป็นพยานในชั้นศาล ในฐานะพยานผู้เชี่ยวชาญ รวมถึงจะต้องเป็นผู้อธิบายให้ศาลฟังว่าข้อมูลการตรวจพิสูจน์ได้มาอย่างไร ข้อมูลแต่ละจุดมีหมายความว่าอะไร”*
> และ

> *“เจ้าหน้าที่ตำรวจจะรายงานไปตามข้อเท็จจริงที่พบ เช่น พบไฟล์อะไร อยู่ที่ไหน สร้างหรือมีการแก้ไขวันไหน ไฟล์มีขนาดเท่าใด ตามมาด้วยการตีความและวิเคราะห์ของเจ้าหน้าที่โดย*

อยู่บนข้อเท็จจริงดังกล่าว และนำเสนอเป็นรายงานให้ศาล แต่มักพบปัญหาว่า ศาลอ่านรายงานไม่เข้าใจ ในการนำข้อมูลต่อศาล จึงมักอธิบายให้ศาลฟังโดยใช้แผนภูมิรูปภาพประกอบด้วย”

ผู้ให้ข้อมูลสำคัญกลุ่มที่ 2 กล่าวเกี่ยวกับประเด็นในส่วนที่เกี่ยวข้องกับคดีในชั้นศาลว่า

“ในการบังคับใช้พระราชบัญญัติคอมพิวเตอร์ฯ เมื่อพิจารณาการดำเนินคดีที่เป็นธรรม คือ การที่คู่คดีทั้งสองฝ่ายมีเครื่องมือในการสู้คดีเท่าเทียมกันนั้น เบื้องต้นพบว่า คดีที่เกี่ยวกับพระราชบัญญัติคอมพิวเตอร์ฯ จำนวนมาก จำเลยและทนายจำเลยไม่มีเครื่องมือที่เพียงพอในการหักล้างพยานหลักฐานฝ่ายรัฐ การทำให้ผู้มีส่วนเกี่ยวข้อง รวมถึงทนายจำเลย ทราบถึงวิธีการแสวงหาและตรวจสอบความชอบด้วยกฎหมายของพยานหลักฐานทางอิเล็กทรอนิกส์ จึงเป็นอีกเครื่องมือหนึ่งที่จะช่วยให้การดำเนินคดีเป็นไปตามหลักการดำเนินคดีที่เป็นธรรมมากขึ้น”

และผู้ให้ข้อมูลสำคัญกลุ่มที่ 2 ยังได้ให้ความเห็นเพิ่มเติมไว้ ดังนี้

““เรื่องการพิสูจน์พยานหลักฐานอิเล็กทรอนิกส์ ประชาชนทั่วไปยังขาดความรู้ความเข้าใจ ในกรณีที่เกิดเหตุการณ์ขึ้น เช่น มีผู้แอบอ้างใช้เฟซบุ๊กของตนเองไปกระทำการผิดตามพระราชบัญญัติคอมพิวเตอร์ฯ มีคำถามว่า ภาระหน้าที่ในการพิสูจน์ควรจะตกเป็นของใคร ซึ่งปกติแล้ว กฎหมายจะยึดหลักว่า หากใครกล่าวอ้างข้อเท็จจริงอันใด ผู้นั้นต้องเป็นผู้พิสูจน์ ในกรณีข้างต้น การที่ผู้ถูกกล่าวหาจะกล่าวอ้างข้อเท็จจริงว่า ตนไม่ได้เป็นผู้โพสต์แต่มีผู้อื่นเข้าไปในเฟซบุ๊กของตนเองแล้วโพสต์ข้อความ ตามหลัก เจ้าของเฟซบุ๊กจะต้องเป็นผู้พิสูจน์เองว่ามีคนลักลอบเข้าไปในเฟซบุ๊กของตนด้วยวิธีการใด

“คำถามก็คือ ในแง่การสร้างความเสมอภาคในการพิสูจน์พยานหลักฐานอิเล็กทรอนิกส์ หลักการที่ว่า หากใครกล่าวอ้างข้อเท็จจริงอันใด ผู้นั้นต้องเป็นผู้พิสูจน์ ใช้ในกรณีพยานหลักฐานอิเล็กทรอนิกส์ได้มากน้อยแค่ไหน และควรมีข้อยกเว้นอย่างไร

“สมมติว่าดิฉันเป็นเจ้าของบัญชีเฟซบุ๊ก เราจะไม่สามารถเข้าไปดูในระบบ หรือเข้าไปพิสูจน์ในระบบ เราเป็นชาวบ้านธรรมดา เราไม่สามารถใช้กระบวนการนี้ เพื่อมาช่วยในการต่อสู้ของเรา กฎหมายจะมีอะไรที่จะสร้างข้อต่อรองให้กับชาวบ้านธรรมดาในการต่อสู้ในเรื่องพยานหลักฐานอิเล็กทรอนิกส์ได้มากน้อยแค่ไหน””

รวมถึงได้เสนอเพิ่มเติมว่า

“จะเป็นไปได้หรือไม่ ที่ในกรณีของพยานหลักฐานอิเล็กทรอนิกส์ การพิสูจน์ความบริสุทธิ์จะใช้กลับทิศทางกับในกรณีพยานหลักฐานทั่วไป โดยในกรณีพยานหลักฐานอิเล็กทรอนิกส์เพียงแต่เราแสดงให้เห็นตามสมควรว่า มีความผิดปกติในระบบ เช่น เคยมี ข้อความขึ้นเตือน

ว่า เคยมีผู้ล็อกอินเข้าใช้บัญชีเฟซบุ๊กเราจากที่อื่น และเกิดการกระทำความผิดพ.ร.บ.ฯ ผ่านบัญชีของเรา เพียงเท่านี้ และภาระในการพิสูจน์ที่เหลือควรจะตกเป็นของฝ่ายรัฐ ที่จะต้องเป็นผู้พิสูจน์ว่าในระบบไม่มีความผิดปกติเกิดขึ้น และผู้กระทำผิดเป็นเราจริง”

4.2.5 ปัญหาและอุปสรรคในแง่มุมของกฎหมาย

ผู้ให้ข้อมูลสำคัญกลุ่มที่ 2 ตั้งข้อสังเกตว่า

“ทั้งๆ ที่จุดประสงค์แท้จริงของการมีกฎหมายฉบับนี้ ก็คือเพื่อปกป้องข้อมูลของบุคคลในระบบดิจิทัลเป็นสำคัญ หรือเน้นการคุ้มครองระบบ แต่ทำไมกลับมีการฟ้องคดีในส่วนความผิดต่อระบบค่อนข้างน้อย ขณะที่มีการฟ้องคดีเกี่ยวกับเนื้อหาค่อนข้างสูง”

ซึ่งผู้ให้ข้อมูลสำคัญกลุ่มที่ 1 มีความเห็นว่า

“เป็นเพราะกฎหมายใช้คำว่า เป็นความผิด “เกี่ยวกับคอมพิวเตอร์” จึงทำให้ความผิดที่เกี่ยวข้องกับคอมพิวเตอร์ทั้งหมดไม่ว่าจะมากหรือน้อย รวมไปถึงสมาร์ทโฟนและข้อมูลที่อยู่ในระบบทุกอย่างล้วนเกี่ยวข้องหมด ฐานความผิดของพระราชบัญญัตินี้จึงกว้าง แทบจะพูดได้ว่า ทุกคดีเกี่ยวพันกับคอมพิวเตอร์หมด รวมถึงคดีอย่างคดีฆาตกรรมด้วย “เพราะสิ่งแรกที่ต้องตรวจสอบเมื่อมีเหตุฆาตกรรมเกิดขึ้น คืออุปกรณ์มือถือและโน้ตบุ๊ก””

4.2.6 กรณีศึกษาเพิ่มเติม

1) คดี “อากง เอสเอ็มเอส”

คดี “อากง เอสเอ็มเอส” เป็นคดีที่นายอำพล ตั้งนพกุล หรือ “อากง”ถูกกล่าวหาว่าส่งข้อความเอสเอ็มเอสมีเนื้อหาดูหมิ่นแสดงความอาฆาตมาดร้ายต่อสถาบัน พระมหากษัตริย์รวม 4 ข้อความ ผ่านทางโทรศัพท์มือถือ ซึ่งศาลได้ตัดสินว่านายอำพลผิดจริงและให้ลงโทษจำคุก 20 ปี โดยคำพิพากษาของศาลในคดีค่อนข้างชัดเจนว่า มือถือเครื่องดังกล่าวเป็นมือถือที่ใช้ส่งข้อความ ซึ่งสามารถพิสูจน์ได้จากการใช้นิติวิทยาศาสตร์ แต่คดีนี้มีความน่าสงสัยในเรื่องความเชื่อมโยงระหว่างผู้กระทำการกับอุปกรณ์ดังกล่าว เช่น มีพยานหลักฐานในศาลหรือไม่ ว่าอากงเป็นคนพิมพ์ข้อความเอสเอ็มเอส ซึ่งแม้ในคดีดังกล่าวไม่มีประจักษ์พยานอยู่ด้วย แต่ในคำพิพากษาของศาลฉบับเต็มจะเห็นว่า ศาลได้พิจารณาและชั่งน้ำหนักพยานหลักฐานอิเล็กทรอนิกส์อย่างรอบด้านแล้ว และคำตัดสินดังกล่าวเป็นดุลยพินิจของศาลหลังจากที่ได้ชั่งน้ำหนักพยานหลักฐานทั้งหมด

คดีนี้ถือเป็นคดีแรกๆ และเป็นคดีที่มีประชาชนให้ความสนใจเป็นอย่างมาก ทางฝ่ายของอากง

ได้โต้แย้งด้วยพยานหลักฐานดิจิทัลว่า องกงใช้โทรศัพท์มือถือดังกล่าวติดต่อก้บลูกสาว และหมายเลขโทรศัพท์ทั้ง 2 หมายเลข มีการใช้งานในพื้นที่ใกล้เคียงกัน ซึ่งตรงกับเอกสารข้อมูลจาก Cell site และเลขที่ระบุตำแหน่งพื้นที่ อีกทั้งทนายฝ่ายอากง ยังมีประเด็นข้อต่อสู้ในเรื่องหมายเลขประจำเครื่องโทรศัพท์ หรือ IMEI ที่จะต้องมีจำนวณ 15 หลักจึงจะสามารถระบุได้ว่าเป็นโทรศัพท์มือถือเครื่องใด และการแก้ไขเปลี่ยนแปลงหมายเลขประจำเครื่องโทรศัพท์ สามารถกระทำได้โดยง่าย และประเด็นข้อต่อสู้อีกประการหนึ่ง คือ เรื่องข้อจำกัดของการเข้าถึงข้อมูลหลักฐานดิจิทัลภายในระยะเวลาที่กฎหมายกำหนด ที่ให้ผู้ให้บริการต้องเก็บข้อมูลการจราจรทางคอมพิวเตอร์ไว้ 90 วัน นับตั้งแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ตามหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ แต่ทางฝ่ายทนายของอากงไม่สามารถเข้าถึงข้อมูลหลักฐานการใช้โทรศัพท์ของอากงได้ เนื่องจากเกินระยะเวลาที่กฎหมายกำหนด ซึ่งทนายของอากงได้ตั้งข้อสังเกตว่า

> *“ข้อสังเกตในคดีนี้ไม่พบบันทึกถึงวิธีการตรวจพิสูจน์พยานหลักฐานดิจิทัล โทรศัพท์เคลื่อนที่โดยเจ้าพนักงานในคดีว่าได้มาตรฐานตามหลักนิติวิทยาศาสตร์ ที่เกี่ยวกับคอมพิวเตอร์หรือไม่ อีกทั้งในคดีนี้ ทนายจำเลยไม่ได้รับการติดต่อตั้งแต่จำเลยถูกควบคุมตัว ดังนั้น หลังจากที่ทนายจำเลยเข้าให้การช่วยเหลือแก่จำเลย ระยะเวลาดังกล่าวก็ได้ล่วงเลยเกินกว่า 90 วันแล้ว ซึ่งพอเกิน 90 วันแล้ว ข้อมูลก็ถูกทำลายทิ้ง เราจึงไม่สามารถขอข้อมูลจากผู้ให้บริการโทรศัพท์เคลื่อนที่ได้ ทางบริษัทมีสำเนาเอกสารการใช้ข้อมูลโทรศัพท์อยู่ชุดเดียว ซึ่งได้ให้เจ้าหน้าที่ตำรวจไปแล้ว พยานหลักฐานชุดเดียวที่เรามีคือ พยานหลักฐานจากโจทก์ในวันนัดตรวจพยานหลักฐาน และในคดีนี้ไม่มีพยานผู้เชี่ยวชาญคนใดมาเบิกความต่อศาล เพื่อหักล้างพยานหลักฐานที่โจทก์กล่าวอ้าง เนื่องจากเป็นคดีอ่อนไหว และทำให้เกิดความหวาดกลัวในการออกมาเคลื่อนไหวทางคดี”*

ในการชั่งน้ำหนักและรับฟังพยานหลักฐานของศาล ศาลอาญาได้พิจารณาคดีและพิพากษาให้อำพลถูกลงโทษจำคุกเป็นเวลา 20 ปี โดยให้เหตุผลในคำพิพากษาว่า

> *“แม้โจทก์จะไม่สามารถนำสืบพยานให้เห็นได้อย่างชัดแจ้งว่าจำเลยเป็นผู้ส่งข้อความตามฟ้อง เพราะเป็นการยากที่โจทก์จะสามารถนำสืบได้ด้วยประจักษ์พยาน เนื่องจากจำเลยซึ่งเป็นผู้กระทำความผิดย่อมต้องปกปิดการกระทำของตนมิให้บุคคลอื่นได้ล่วงรู้ จึงจำเป็นต้องอาศัยเหตุผล จากประจักษ์พยานแวดล้อมที่โจทก์นำสืบ ได้แก่ ข้อมูลการใช้โทรศัพท์ที่ระบุตำแหน่งว่าข้อความถูกส่งมาจากเสาสัญญาณใกล้บ้านจำเลย รวมทั้งหมายเลขอีมี่ที่ตรงกับโทรศัพท์เครื่องที่จำเลยยอมรับว่าเป็นผู้ใช้งาน ศาลเห็นว่าพยานแวดล้อมมีน้ำหนักพอรับฟังได้ว่าจำเลยกระทำความผิดจริง”*

คดีของอากงทำให้เห็นถึงความสำคัญและข้อจำกัดของการเก็บรวบรวมพยานหลักฐานดิจิทัล มาตรฐานการตรวจพิสูจน์พยานหลักฐานดิจิทัล รวมถึงข้อจำกัดด้านกฎหมายที่กำหนด ระยะเวลาเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการเกี่ยวกับคอมพิวเตอร์ การสื่อสาร ไว้เพียง 90 วันเท่านั้น ทำ ให้การเข้าถึงข้อมูลที่จะนำมาเป็นพยานหลักฐานในคดีถูกจำกัดลง ซึ่ง อาจจะเกิดความไม่เป็นธรรมต่อฝ่ายที่ถูกกล่าวหาได้

ผู้ให้ข้อมูลสำคัญกลุ่มที่ 2 ตั้งประเด็นสงสัยว่า

“ในเมื่อมีความไม่ชัดเจนดังกล่าว ประกอบกับพฤติการณ์แวดล้อมที่ว่า จำเลยเป็นชายแก่ ที่ไม่เคยส่งเอสเอ็มเอส หรือไม่เคยใช้โซเชียลมีเดียเป็นประจำ อยู่มาวันหนึ่งได้ส่งข้อความเอสเอ็มเอส 4 ข้อความออกไป จุดนี้มีข้อที่น่าสงสัย นี่คือคดีอาญา ซึ่งเมื่อไหร่ก็ตามที่มีความสงสัย ต้องยกประโยชน์แห่งความสงสัยให้ผู้ถูกกล่าวหา ถ้าดูพฤติการณ์แวดล้อมของบุคคลคนนี้ มันมีข้อสงสัย ศาลได้พิจารณาหรือไม่ ซึ่งอ่านแล้วไม่พบประเด็นนี้ในคำวินิจฉัยของศาล ซึ่งหาความเชื่อมโยงไม่ได้ ว่ามือถือเป็นมือถือเครื่องที่ใช้กระทำความผิด และคนที่กระทำความผิดไม่ชัดเจน ในสำนวนทั้งหมดไม่สามารถยืนยันได้ว่า จะไม่มีทางเป็นคนอื่นได้เลย ประเด็นจึงกลับไปสู่หลักว่า เมื่อมีความสงสัย ต้องยกประโยชน์ให้กับคนที่ถูกสงสัย เผอิญศาลไม่สงสัยใช่ไหม หรือมีอะไรที่ไม่ปรากฏในสำนวน ตรงนี้เป็นจุดที่อ่อนที่สุดในคำพิพากษานี้ หากยึดตามคำพิพากษาข้างต้นของศาล เราก็อาจโดนคดีแบบอากงได้ หากเราเผลอวางมือถือทิ้งไว้ และมือถือของเราก็ไม่ใส่รหัสเข้าไว้ด้วย”

และ

“ต่อไปถ้าเราจะเอาโทษเจ้าของมือถือหรือเจ้าของคอมพิวเตอร์ กฎหมายต้องเขียนให้ชัด ว่าเป็นความรับผิดชอบของเจ้าของอุปกรณ์ที่จะต้องไใส่รหัส หรือทำอะไรให้คนอื่นไม่สามารถเข้าถึงคอมพิวเตอร์ของเราได้ แต่วันนี้ กฎหมายยังไม่ได้เขียนแบบนี้ การมีข้อสงสัยแบบนี้โดยหลักแล้ว ศาลต้องไม่ลงโทษ”

2) คดีของสุรภักดิ์ อดีตโปรแกรมเมอร์ถูกกล่าวหาว่าเป็นเจ้าของอีเมล dorkao@hotmail.com และใช้อีเมลดังกล่าวสร้างบัญชีผู้ใช้เฟซบุ๊กชื่อว่า “เราจะครองแผ่นดินฯ...” เผยแพร่ข้อความเข้าข่ายหมิ่นประมาท ดูหมิ่น หรือแสดงความอาฆาตมาดร้ายสถาบันพระมหากษัตริย์ฯ จำนวน 5 ข้อความ ในคดีนี้มีการนำพยานหลักฐานดิจิทัล ได้แก่ เครื่องคอมพิวเตอร์ โน้ตบุ๊ก คอมพิวเตอร์ตั้งโต๊ะ แอร์การ์ด ซิมการ์ดทรูมูฟ ซิมวันทูคอล ซีดี โมเด็มเราเตอร์ และแผงวงจรไฟฟ้ามาเป็นพยานหลักฐานประกอบการพิจารณาคดีของศาล ในคดีนี้ฝ่ายโจทก์ให้พยานผู้เชี่ยวชาญจากหน่วยงานของรัฐเบิกความ ให้ความเห็นประกอบเอกสารภาพถ่ายจากหน้าจอข้อความที่พิมพ์ในเฟซบุ๊ก จำนวน 5 ข้อความ และเอกสารจากบริษัทไมโครซอฟต์ ซึ่งกล่าวอ้างว่า แสดงความเชื่อมโยงระหว่างเลขหมายประจำเครื่องคอมพิวเตอร์ของสุรภักดิ์กับบัญชีผู้ใช้อีเมล รวมทั้งบันทึกวันเวลาการลงทะเบียนใช้งานอีเมล เอกสารรายงานการตรวจพิสูจน์คอมพิวเตอร์ และเอกสารที่อ้างว่าแสดงข้อมูลการใช้งานอีเมลและเฟซบุ๊ก ที่บันทึกอยู่ในแฟ้มเก็บบันทึกชั่วคราวในเครื่องคอมพิวเตอร์ของสุรภักดิ์

คดีนี้มีประเด็นพิพาทสำคัญที่ต้องวินิจฉัย คือ

1) คอมพิวเตอร์ของกลางมีการใช้งานระบบอินเทอร์เน็ต หรือไม่

2) คอมพิวเตอร์มีการใช้อีเมล dorkao@hotmail.com หรือไม่

3) สามารถระบุความเป็นเจ้าของบัญชีเฟซบุ๊ก ชื่อว่า “เราจะครองแผ่นดินฯ...” ได้หรือไม่

4) คอมพิวเตอร์ดังกล่าว มีประวัติการเข้าใช้บัญชีเฟซบุ๊กดังกล่าวหรือไม่ และสามารถตรวจสอบหาข้อความที่หมิ่นสถาบันหลายรายการ ตามวันเวลาที่พนักงานสอบสวนระบุได้หรือไม่

โดยฝ่ายสุรภักดิ์ไม่ได้ต่อสู้ในประเด็นที่เป็นเนื้อหาของข้อความที่ปรากฏบนเฟซบุ๊ก แต่ได้ต่อสู้ว่าไม่ใช่เจ้าของ หรือผู้ใช้อีเมลและเฟซบุ๊กตามข้อกล่าวหาของโจทก์ จึงทำให้มีประเด็นที่ต้องพิสูจน์คือความเชื่อมโยงระหว่างข้อความหมิ่นฯ กับเครื่องคอมพิวเตอร์ของสุรภักดิ์ ผลปรากฏว่าหน่วยงานที่พิสูจน์พยานหลักฐานดิจิทัลได้ระบุว่า ไม่พบถ้อยคำหมิ่นประมาทพระมหากษัตริย์ฯ ตามฟ้องจากการตรวจพิสูจน์เครื่องคอมพิวเตอร์ของกลางแต่อย่างใด แม้ว่าข้อความที่โพสไปแล้วนั้นจะถูกส่งไปที่เซิร์ฟเวอร์ของเฟซบุ๊ก อาจทำให้ไม่หลงเหลือข้อความที่อยู่ในคอมพิวเตอร์ของสุรภักดิ์ก็ตาม และนอกจากนี้เอกสารที่เจ้าพนักงานได้ข้อมูลจากเอกสารบันทึกประวัติการใช้อีเมลจากบริษัทไมโครซอฟต์ปรากฏว่าได้มีการล็อกอินเข้าใช้งานอีเมลดังกล่าวอยู่หลายครั้ง ซึ่งเป็นเวลาวันที่สุรภักดิ์ถูกจับและควบคุมตัวแล้ว โดยสุรภักดิ์ไม่ได้รับอนุญาตให้ใช้อุปกรณ์สื่อสารใดๆ แสดงให้เห็นว่าสุรภักดิ์ไม่ได้เป็นผู้ใช้งานอีเมลในช่วงเวลานั้น ส่งผลทำให้เกิดความสงสัยว่าใครเป็นเจ้าของ หรือผู้ใช้อีเมลดังกล่าว และถึงแม้ว่าจำเลยเป็นเจ้าของหรือผู้ใช้ก็ตาม แต่เมื่อมีบุคคลอื่นใช้อีเมลนี้ก็ย่อมมีข้อสงสัยว่าสุรภักดิ์เป็นผู้กระทำความผิดจริงหรือไม่

ในคดีนี้ยังพบว่า วิธีการตรวจพิสูจน์พยานหลักฐานดิจิทัลโดยเจ้าพนักงานในคดี ไม่ได้มาตรฐานในการตรวจพิสูจน์พยานหลักฐานดิจิทัล ทำให้พยานหลักฐานขาดความน่าเชื่อถือ ตามเอกสารประกอบรายงานการตรวจพิสูจน์ที่แสดงประวัติการใช้อุปกรณ์ เพื่อเชื่อมต่อระบบเครือข่ายที่โจทก์ใช้อ้างว่ามีข้อมูลต่างๆ ที่พิสูจน์ความผิดของจำเลยบันทึกอยู่ในเครื่องคอมพิวเตอร์ของกลาง มีวันเวลาการบันทึกปรากฏอยู่ด้วย และวันเวลาเหล่านั้นได้แสดงให้เห็นว่า เครื่องคอมพิวเตอร์ของกลางซึ่งเป็นของสุรภักดิ์ถูกเปิดใช้งานอีกหลายครั้งหลังจากที่จำเลยถูกจับและควบคุมตัว เรื่องนี้สอดคล้องกับล็อกไฟล์ ที่แสดงถึงการใช้งานอีเมล จึงแสดงให้เห็นว่าพนักงานตรวจพิสูจน์พยานหลักฐานดิจิทัลใช้วิธีเปิดเครื่องคอมพิวเตอร์ของจำเลยโดยตรง ไม่ใช่ตรวจสอบจากสำเนาของข้อมูลคอมพิวเตอร์ ซึ่งวิธีการดังกล่าวไม่ชอบด้วยหลักการการตรวจพิสูจน์พยานหลักฐานดิจิทัล ที่โดยปกติแล้ว เจ้าหน้าที่ที่ต้องพิสูจน์ ต้องเก็บรักษาเครื่องต้นฉบับให้อยู่ในสภาพเดิม และทำสำเนาเครื่องและข้อมูลอย่างน้อยหนึ่งชุด เพราะการเปิดเครื่องคอมพิวเตอร์ของกลางโดยตรงอาจส่งผลกระทบต่อข้อมูลที่บันทึกอยู่ภายในเครื่อง และคดีนี้ศาลก็ไม่สามารถตรวจสอบหรือเปรียบเทียบภายหลังได้ว่าข้อมูลหรือพยานหลักฐานที่โจทก์กล่าวอ้างว่าอยู่ในเครื่องของกลางถูกสร้างขึ้นภายหลังหรือว่ามีอยู่ในเครื่องคอมพิวเตอร์มาก่อน เนื่องจากเจ้าพนักงานไม่ได้เก็บรักษาเครื่องจริงให้อยู่ในสภาพเดิม อีกทั้งยังไม่ปรากฏข้อเท็จจริงว่าเจ้าพนักงานใช้มาตรการที่เหมาะสม เพื่อรักษาความปลอดภัยและความถูกต้องของข้อมูลในเครื่องคอมพิวเตอร์ของกลาง ซึ่งลักษณะและวิธีการตรวจพิสูจน์ที่ไม่เป็นไปตามมาตรฐานนี้ ส่งผลกระทบและลดทอนความน่าเชื่อถือของพยานหลักฐานดิจิทัลของฝ่ายโจทก์ลง

การนำเสนอพยานหลักฐานดิจิทัลในคดีนี้ ยังมีข้อมูลที่ไม่สอดคล้องกับความเป็นจริงในทางเทคนิคคอมพิวเตอร์ เห็นได้จากข้อมูลประวัติการเข้าใช้งานอีเมล dorkao@hotmail.com ที่มีบันทึกอยู่ในแฟ้มเก็บข้อมูลชั่วคราวในเครื่องคอมพิวเตอร์ของสุรภักดิ์มีจำนวนเพียงหนึ่งไฟล์เท่านั้น คือ ไฟล์

ที่แสดงข้อมูลการใช้งานอีเมลตามฟ้อง ซึ่งโดยปกติแล้ว หากเว็บไซต์ที่เรียกใช้งานไม่มีนโยบายห้ามการแคช เครื่องคอมพิวเตอร์ก็จะแคชเว็บไซต์เหล่านั้นทั้งหมดเก็บไว้โดยอัตโนมัติ จึงเป็นไปไม่ได้ที่เครื่องคอมพิวเตอร์เครื่องหนึ่งจะเก็บบันทึกไฟล์การใช้เว็บไซต์ใดเว็บไซต์หนึ่งไว้เพียงแค่ไฟล์เดียวตามที่โจทก์กล่าวอ้าง เป็นไปไม่ได้เลยที่การกู้ข้อมูลที่ถูกลบทิ้ง ผู้กู้จะพบไฟล์เพียงไฟล์เดียวในแฟ้มเก็บบันทึกข้อมูลชั่วคราวที่เก็บบันทึกการใช้งานอินเทอร์เน็ต เนื่องจากหลักการทำงานของแฟ้มเก็บบันทึกข้อมูลการใช้งานชั่วคราว หรือการแคช จะเก็บบันทึกข้อมูลการใช้งานเว็บไซต์ต่างๆ ไว้ในเครื่องคอมพิวเตอร์ของผู้ใช้ เพื่อนำกลับมาแสดงผลใหม่ได้อย่างรวดเร็วเมื่อผู้ใช้เรียกเว็บไซต์นั้นดูอีกครั้ง และการที่ไฟล์ข้อมูลถูกลบภายในเวลาสามวินาที ก็ขัดกับหลักการทำงานและวัตถุประสงค์ของการแคชเว็บไซต์เพื่อจะเรียกกลับมาแสดงผลใหม่ในเวลาอันรวดเร็ว จึงเป็นไปไม่ได้เลยที่เครื่องคอมพิวเตอร์จะบันทึกและลบไฟล์ดังกล่าวทิ้ง ไฟล์ที่โจทก์อ้างว่าพบในเครื่องคอมพิวเตอร์ของจำเลยจึงอาจถูกสร้างขึ้นใหม่เพื่อมุ่งจะดำเนินคดีกับจำเลย รวมถึงมีข้อสงสัยว่าไฟล์หลักฐานที่โจทก์อ้างนั้นไม่ใช่ข้อมูลที่ถูกต้องแท้จริง และถูกสร้างขึ้นใหม่เพื่อใช้กล่าวหาสุรภักดิ์ ซึ่งขัดกับพยานหลักฐานที่ฝ่ายโจทก์อ้างว่าพบร่องรอยการใช้เฟซบุ๊กบันทึกอยู่ในเครื่องคอมพิวเตอร์ของกลาง

ในการชั่งน้ำหนักและรับฟังพยานหลักฐานของศาล คดีนี้ศาลฎีกามีคำพิพากษายกฟ้อง โดยให้เหตุผลในคำพิพากษาว่า

> *“เนื่องจากไม่ปรากฏประวัติการใช้งานอีเมลและเฟซบุ๊กตามฟ้องจากเครื่องคอมพิวเตอร์ของจำเลย รวมถึงรหัสต้นฉบับที่พบในคอมพิวเตอร์ของกลางไม่อาจเกิดขึ้นในพื้นที่จัดเก็บข้อมูลปกติ แต่เกิดจากการทำขึ้นแล้วนำไปวางในเครื่องคอมพิวเตอร์ของกลาง นอกจากนี้คอมพิวเตอร์ของกลางยังถูกเปิดหลังจากจำเลยถูกควบคุมตัว ทำให้ข้อมูลที่ได้จากการตรวจพิสูจน์พยานหลักฐานดิจิทัลมีข้อบกพร่องและไม่น่าเชื่อถือว่าจำเลยกระทำความผิดตามฟ้องจริงหรือไม่ ต้องยกประโยชน์แห่งความสงสัยให้จำเลยตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 227 วรรคสอง”*

ในกระบวนการยุติธรรมทางอาญาที่เกี่ยวข้องกับพยานหลักฐานดิจิทัล หากมีการโต้แย้งถึงความถูกต้องของพยานหลักฐานดิจิทัล ในกรณีทั่วไปคู่ความฝ่ายที่กล่าวอ้าง จะต้องนำพยานบุคคลที่ตรวจยึด และเก็บรักษาพยานหลักฐานดังกล่าวมาเบิกความต่อศาล ส่วนในกรณีที่พยานหลักฐานมีความซับซ้อน คู่ความฝ่ายที่กล่าวอ้างอาจจำเป็นต้องนำพยานผู้เชี่ยวชาญมาเบิกความต่อศาล ซึ่งความเห็นของผู้เชี่ยวชาญจะมีประโยชน์ต่อการวินิจฉัยคดี

จากกรณีศึกษาดังกล่าว ทำให้เห็นถึงความสำคัญของพยานหลักฐานดิจิทัล การรับฟังพยานหลักฐานดิจิทัล และการต่อสู้คดีโดยใช้พยานหลักฐานดิจิทัล ซึ่งทั้งฝ่ายโจทก์และจำเลยได้ใช้พยานหลักฐานดิจิทัลในการต่อสู้คดี โดยประเด็นการต่อสู้คดีมีลักษณะร่วมกัน คือ การพิสูจน์ตัวตนจากพยานหลักฐานดิจิทัลที่ฝ่ายโจทก์กล่าวอ้าง และความสำคัญของพยานผู้เชี่ยวชาญในการต่อสู้คดี โดยเฉพาะในคดีสุรภักดิ์ที่จำเลยเป็นผู้เชี่ยวชาญทางด้านคอมพิวเตอร์อยู่แล้ว จึงมีประเด็นต่อสู้เพิ่มเติมที่แตกต่างออกไป คือหลักการในการตรวจพิสูจน์พยานหลักฐานดิจิทัลของฝ่ายโจทก์ และการที่อุปกรณ์คอมพิวเตอร์ของจำเลยถูกเปิดใช้งานในระหว่างที่จำเลยถูกคุมขัง การสู้คดีในลักษณะนี้มีความ

ซับซ้อน ฝ่ายที่โต้แย้งจะต้องทำการพิสูจน์และอธิบายเรื่องทางเทคนิคให้ศาลเข้าใจ เนื่องจากภาระการพิสูจน์ถูกผลักมาอยู่ที่ผู้กล่าวอ้างหรือโต้แย้ง ตามหลักผู้ใดกล่าวอ้างผู้นั้นมีหน้าที่นำสืบ

คดีอาญาที่เกี่ยวข้องกับการตรวจพิสูจน์พยานหลักฐานดิจิทัล ที่รัฐเป็นโจทก์ฟ้องคดี ฝ่ายโจทก์มักจะมีทรัพยากรเครื่องมือทางด้านเทคโนโลยีในการแสวงหาและได้มาซึ่งพยานหลักฐานดิจิทัล และยังมีพยานผู้เชี่ยวชาญที่มีความรู้ความสามารถในการอธิบายถึงพยานหลักฐานมาสนับสนุนความน่าเชื่อถือของน้ำหนักพยานหลักฐาน ซึ่งตรงกันข้ามกับฝ่ายจำเลยที่มีข้อจำกัดในการแสวงหาพยานผู้เชี่ยวชาญเพื่อมาอธิบายและโต้แย้งข้อกล่าวอ้างที่เกี่ยวกับพยานหลักฐานดิจิทัลของฝ่ายโจทก์ ว่ามีความถูกต้องแท้จริงหรือไม่ รวมถึงข้อจำกัดในการเข้าถึงพยานหลักฐานดิจิทัล และฝ่ายจำเลยยังต้องใช้ทรัพยากรส่วนบุคคลในแสวงหาพยานผู้เชี่ยวชาญมาเบิกความเป็นพยานให้ อีกทั้งยังไม่มีหน่วยงานของรัฐหรือองค์กรเอกชนใดที่เข้ามามีส่วนเกี่ยวข้องในการช่วยเหลือในด้านการตรวจพิสูจน์พยานหลักฐานดิจิทัล และสนับสนุนผู้เชี่ยวชาญด้านการตรวจพิสูจน์พยานหลักฐานดิจิทัล จะเห็นได้จากการที่ผู้ให้ข้อมูลสำคัญกลุ่มที่ 2 ให้ความเห็นว่า

> *“ทนายความหรือตัวจำเลยเองต้องมีเส้นสาย ที่ผ่านมาเราใช้ทรัพยากรส่วนบุคคล ไม่มีหน่วยงานใดเข้ามาให้การช่วยเหลือ ไม่แน่ใจว่าอันนี้จะเป็นข้อเสนอได้หรือไม่ว่าศาลควรจะมีพยานผู้เชี่ยวชาญให้เลือก เหมือนกับถ้าเป็นหมอ ศาลก็จะมี รายชื่อพยานผู้เชี่ยวชาญอยู่ ที่พร้อมจะมาเบิกความตามหลักวิชาการ”*

สอดคล้องกับข้อมูลจากการผู้ให้ข้อมูลสำคัญกลุ่มที่ 1 ที่ได้สะท้อนปัญหาและมุมมองของการออกประกาศหรือระเบียบเกี่ยวกับการคัดกรองพยานผู้เชี่ยวชาญไว้ว่า

> *“ศาลได้มีทะเบียนพยานผู้เชี่ยวชาญของศาลอยู่ แต่ในส่วนของการตรวจพิสูจน์พยานหลักฐานดิจิทัล ยังไม่มีการขึ้นทะเบียน ส่วนใหญ่จะขอความร่วมมือจากเจ้าหน้าที่ตำรวจ เจ้าหน้าที่นิติวิทยาศาสตร์ เจ้าหน้าที่จากหน่วยงานของรัฐ เข้ามาช่วยเหลือในส่วนของหลักเกณฑ์จากพยานผู้เชี่ยวชาญ ซึ่งประเทศไทยก็ไม่ได้ตั้งหลักเกณฑ์ว่าต้องจบการศึกษาอะไรมา หากมีความชำนาญในเรื่องของการตรวจพิสูจน์พยานหลักฐานดิจิทัล แต่ไม่ได้มีใบรับรองการฝึกอบรม ศาลก็รับฟังได้ ว่าเขามีความชำนาญเกี่ยวกับการตรวจพิสูจน์พยานหลักฐานดิจิทัล เพราะมันไม่ได้เป็นสาขาวิชาชีพเฉพาะ”*

4.2.7 ปัญหาและอุปสรรคในประเด็นอื่นๆ

4.2.7.1 สถานะของพยานหลักฐานดิจิทัล

ประเด็นข้อโต้แย้งเกี่ยวกับการรับฟังพยานหลักฐานดิจิทัลที่สำคัญประการหนึ่ง คือ มาตรฐานในการจัดเก็บและจัดการพยานหลักฐานดิจิทัลของเจ้าพนักงานที่เกี่ยวข้อง เนื่องจากพยานหลักฐานดิจิทัลในรูปของข้อมูลคอมพิวเตอร์หรือข้อมูลอิเล็กทรอนิกส์ มีความเสี่ยงต่อการถูกเปลี่ยนแปลงแก้ไข สูญหาย เสียหาย ง่าย โดยเฉพาะเมื่อจำต้องมีการส่งผ่านข้อมูลคอมพิวเตอร์หรือข้อมูลอิเล็กทรอนิกส์ระหว่างเจ้าพนักงานที่เกี่ยวข้องโดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. เสนอแนวทางเบื้องต้นใน “ข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจ

พิสูจน์พยานหลักฐาน” เพื่อเป็นแนวทางให้กับเจ้าหน้าที่ที่เกี่ยวข้องกับการจัดเก็บ รวบรวม และตรวจพิสูจน์พยานหลักฐานดิจิทัล ให้ปฏิบัติงานในสถานที่เกิดเหตุ และในห้องปฏิบัติการให้สอดคล้องกับมาตรฐานสากล โดยได้เน้นย้ำในเรื่องการให้ความสำคัญต่อการบันทึกแบบฟอร์ม กระบวนการระบุสายความรับผิดชอบการเก็บรักษาพยานหลักฐาน เริ่มตั้งแต่เมื่อพยานหลักฐานชิ้นนั้นถูกเก็บรวบรวม เพื่อสร้างความต่อเนื่องของการครอบครองพยานหลักฐาน โดยข้อมูลที่เจ้าพนักงานผู้ปฏิบัติงานในแต่ละสายงานจำเป็นต้องระบุ ประกอบด้วย ข้อมูลการติดต่อและลายมือชื่อของผู้ส่งมอบพยานหลักฐาน เหตุผลในการรับ-ส่งพยานหลักฐาน วิธีการส่งมอบพยานหลักฐาน เช่น ส่งมอบโดยเจ้าหน้าที่ที่เกี่ยวข้องหรือส่งมอบโดยพนักงานส่งของ และสถานที่จัดเก็บพยานหลักฐาน เป็นต้น

นอกจากนี้ International Organization on Computer Evidence หรือ IOCE ซึ่งเป็นหน่วยงานสากลที่ดูแลเกี่ยวกับการปฏิบัติต่อพยานหลักฐานคอมพิวเตอร์ ได้กำหนดหลักการสำคัญในการเข้าค้นและยึดอุปกรณ์อิเล็กทรอนิกส์ไว้ 6 ประการ คือ

1) เมื่อใดก็ตามที่ต้องดำเนินการกับพยานหลักฐานดิจิทัล จะต้องมีการดำเนินการตามหลักปฏิบัติทั่วไปทางนิติวิทยาศาสตร์คอมพิวเตอร์ และต้องดำเนินการตามขั้นตอนของนิติวิทยาศาสตร์คอมพิวเตอร์
2) ในขณะปฏิบัติการเก็บยึดพยานหลักฐานดิจิทัล การดำเนินการทุกอย่างจะต้องไม่ก่อให้เกิดการเปลี่ยนแปลงต่อพยานหลักฐานนั้น
3) หากมีความจำเป็นที่จะต้องเข้าถึงข้อมูลในพยานหลักฐานต้นฉบับ บุคคลผู้ปฏิบัติจะต้องได้ผ่านการอบรมมาเพื่อดำเนินการนั้นเป็นการเฉพาะ
4) จะต้องมีการจดบันทึกทุกขั้นตอน ทุกการกระทำที่เกี่ยวข้องกับการเก็บยึด การเข้าถึงข้อมูล การเคลื่อนย้ายอย่างละเอียด และต้องมีการเก็บบันทึกนั้นไว้เป็นอย่างดี และสามารถนำมาแสดงให้ดูได้ทุกเมื่อเมื่อถูกร้องขอ
5) จะต้องมีบุคคลผู้รับผิดชอบที่ชัดเจนต่อทุกการกระทำที่เกิดขึ้น ในขณะที่พยานหลักฐานดิจิทัลนั้นอยู่ในความดูแลของบุคคลนั้น
6) หน่วยงานและเจ้าหน้าที่ที่ดำเนินการเก็บยึด เข้าถึงข้อมูลบันทึกข้อมูล โอนถ่ายเคลื่อนย้ายพยานหลักฐานดิจิทัล จะต้องรับผิดชอบในการปฏิบัติการให้สอดคล้องกับหลักการทั้ง 6 ข้อ นี้

สภาพเศรษฐกิจและสังคมของโลกยุคปัจจุบันได้เปลี่ยนแปลงไปจากอดีต อุปกรณ์ดิจิทัล เช่น โทรศัพท์มือถือ คอมพิวเตอร์ และอุปกรณ์อื่นที่เชื่อมต่อกับอินเทอร์เน็ตกลายเป็นปัจจัยพื้นฐานในการดำรงชีวิตของประชาชน ในการดำเนินคดีกับผู้กระทำความผิดในความผิดหลากหลายประเภท จึงมีอุปกรณ์ดิจิทัลรวมถึงข้อมูลที่บันทึกอยู่ในอุปกรณ์ดังกล่าวเป็นพยานหลักฐานที่มีความสำคัญในการพิสูจน์ความผิดในคดีอาญาไม่น้อยไปกว่าพยานหลักฐานประเภทอื่น อย่างไรก็ตามด้วยลักษณะของพยานหลักฐานดิจิทัลทั้งในรูปของพยานเอกสารและพยานวัตถุมีความเสี่ยงต่อการเสียหายหรือสูญหายโดยง่าย หลักเกณฑ์และวิธีการในการจัดเก็บ และตรวจพิสูจน์พยานหลักฐานดิจิทัลจึงต้องมีความชัดเจน รัดกุมและรอบคอบ เพื่อลดข้อโต้แย้งในการรับฟังพยานหลักฐานในคดี หลักการสำคัญที่เจ้า

พนักงานซึ่งมีอำนาจสืบสวนสอบสวนรวบรวมพยานหลักฐานดิจิทัล และผู้ปฏิบัติงานด้านการตรวจพิสูจน์พยานหลักฐานดิจิทัลพึงต้องระมัดระวัง คือ การได้มาซึ่งพยานหลักฐานดิจิทัลต้องปฏิบัติให้ถูกต้องตามประมวลกฎหมายวิธีพิจารณาความอาญา และบทกฎหมายเฉพาะอื่นซึ่งระบุขั้นตอนปฏิบัติในการได้มาซึ่งพยานหลักฐานดิจิทัล โดยเฉพาะอย่างยิ่ง ข้อมูลคอมพิวเตอร์ ซึ่งมาตรฐานในการจัดเก็บพยานหลักฐานดิจิทัลต้องเป็นไปตามมาตรฐานสากลในการเข้าค้นและยึดอุปกรณ์อิเล็กทรอนิกส์ ซึ่งเป็นมาตรการพื้นฐานที่จะทำให้พยานหลักฐานที่รวบรวมได้นั้นมีความน่าเชื่อถือและชอบด้วยกฎหมายเพียงพอที่ศาลจะรับฟัง และให้น้ำหนักกับพยานหลักฐานดิจิทัลในการลงโทษผู้กระทำความผิด

4.2.7.2 การอภิปรายผลการศึกษากระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล

1) กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล

หลักการพื้นฐานในการตรวจพิสูจน์พยานหลักฐานดิจิทัล ประกอบไปด้วย

1.1) <u>การรวบรวมพยานหลักฐานดิจิทัล</u>

สิ่งสำคัญที่สุด คือ ความสมบูรณ์ของพยานหลักฐาน และการรวบรวมพยานหลักฐานทั้งหมดให้เป็นไปอย่างสมบูรณ์ขณะเกิดเหตุโดยไม่ถูกเปลี่ยนแปลงแก้ไขใดๆ โดยทั่วไปแล้ว พนักงานสอบสวนมีอำนาจรวบรวมพยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 132 อันเป็นบทกฎหมายทั่วไป แต่บทกฎหมายดังกล่าวไม่ได้บัญญัติเกี่ยวกับการรวบรวมพยานหลักฐานที่เป็นอุปกรณ์ดิจิทัลหรือข้อมูลคอมพิวเตอร์ไว้โดยตรง อย่างไรก็ดี คดีอาญาบางประเภทความผิด มีกฎหมายบัญญัติเอาไว้โดยเฉพาะเจาะจงในเรื่องของอำนาจของพนักงานสอบสวนหรือเจ้าพนักงานผู้มีอำนาจรวบรวมพยานหลักฐานและหลักเกณฑ์วิธีการในการรวบรวมและจัดเก็บพยานหลักฐาน พนักงานสอบสวนหรือเจ้าพนักงานเหล่านั้นก็จะต้องปฏิบัติให้เป็นไปตามบทบัญญัติกฎหมายเฉพาะดังกล่าวนั้นด้วย

1.2) <u>การเก็บรักษาพยานหลักฐานดิจิทัล</u>

การเก็บรักษาจะต้องเก็บรักษาไว้ในสภาพที่รับฟังได้ในชั้นศาล เป็นไปตามกระบวนการสร้างห่วงโซ่คุ้มครองพยานหลักฐานในหลักสากลต้องมีมาตรฐานการเก็บรักษาพยานหลักฐานดิจิทัลที่เป็นที่ยอมรับของทุกฝ่ายมีบันทึกขั้นตอนการคุ้มครองพยานหลักฐานและวิธีการเก็บรักษา เพื่อให้มั่นใจได้ว่าเป็นข้อมูลที่ไม่ได้ถูกแก้ไขเปลี่ยนแปลงนับจากที่ได้รับมาจากที่เกิดเหตุ มาตรฐานในการจัดเก็บและจัดการพยานหลักฐานดิจิทัลของเจ้าพนักงานที่เกี่ยวข้อง อาจทำให้เกิดประเด็นข้อโต้แย้งในการรับฟังพยานหลักฐานได้ เนื่องจากพยานหลักฐานดิจิทัลในรูปของข้อมูลคอมพิวเตอร์หรือข้อมูลอิเล็กทรอนิกส์ มีความเสี่ยงต่อการถูกเปลี่ยนแปลงแก้ไข สูญหาย เสียหาย โดยง่าย โดยเฉพาะอย่างยิ่งเมื่อต้องมีการส่งผ่านข้อมูลคอมพิวเตอร์หรือข้อมูลอิเล็กทรอนิกส์ระหว่างเจ้าพนักงานที่เกี่ยวข้องหลายทอด ในส่วนนี้ปัจจุบันสำนักงานพัฒนาธุรกรรมทาง

อิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. ได้เผยแพร่เอกสาร “ข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐาน” เพื่อเป็นแนวทางเบื้องต้นให้กับเจ้าหน้าที่ที่เกี่ยวข้องกับการจัดเก็บ รวบรวม และตรวจพิสูจน์พยานหลักฐานดิจิทัล ให้ปฏิบัติงานในสถานที่เกิดเหตุและในห้องปฏิบัติการให้สอดคล้องกับมาตรฐานสากล โดยสพธอ. เน้นในเรื่องการให้ความสำคัญต่อการบันทึกแบบฟอร์มที่เรียกว่า “Chain of Custody” หรือห่วงโซ่คุ้มครองพยานหลักฐาน คือ กระบวนการระบุสายความรับผิดชอบการเก็บรักษาพยานหลักฐาน เริ่มตั้งแต่เมื่อพยานหลักฐานถูกเก็บรวบรวม เพื่อสร้างความต่อเนื่องของการครอบครองพยานหลักฐาน โดยข้อมูลที่เจ้าหน้าที่ผู้ปฏิบัติงานในแต่ละสายงาน จำเป็นต้องระบุ รวมถึงข้อมูลติดต่อและลงลายมือชื่อของผู้ส่งมอบพยานหลักฐาน, เหตุผลในการับ-ส่งมอบพยานหลักฐาน, วิธีการส่งมอบพยานหลักฐาน เช่น ส่งมอบโดยเจ้าหน้าที่ที่เกี่ยวข้องหรือส่งมอบโดยพนักงานส่งของ และสถานที่จัดเก็บพยานหลักฐาน เป็นต้น นอกจากนี้ International Organization on Computer Evidence หรือ IOCE ซึ่งเป็นหน่วยงานสากลที่ดูแลเกี่ยวกับการปฏิบัติต่อพยานหลักฐานดิจิทัล ได้กำหนดหลักการสำคัญ ในการเข้าค้นและยึดอุปกรณ์ อิเล็กทรอนิกส์ไว้ 6 ประการ คือ

1) เมื่อใดก็ตามที่ต้องดำเนินการกับพยานหลักฐานดิจิทัล จะต้องมีการดำเนินการตามหลักปฏิบัติทั่วไปทางนิติคอมพิวเตอร์ และต้องดำเนินการตามขั้นตอนของนิติคอมพิวเตอร์
2) ในขณะปฏิบัติการเก็บยึดพยานหลักฐานดิจิทัล การดำเนินการทุกอย่างจะต้องไม่ก่อให้เกิดการเปลี่ยนแปลงต่อพยานหลักฐานนั้น
3) หากมีความจำเป็นที่จะต้องเข้าถึงข้อมูลในพยานหลักฐานต้นฉบับ เจ้าหน้าที่ผู้ปฏิบัติจะต้องได้รับการอบรมมาเพื่อดำเนินการเป็นการเฉพาะ
4) จะต้องมีการจดบันทึกรายละเอียดทุกขั้นตอน ทุกการกระทำที่เกี่ยวข้องกับการเก็บยึด การเข้าถึงข้อมูล การเคลื่อนย้าย และต้องมีการเก็บรักษาบันทึกนั้นไว้ และสามารถนำมาแสดงได้เมื่อถูกร้องขอ
5) จะต้องมีบุคคลผู้รับผิดชอบที่ชัดเจนในทุกกระบวนการที่เกิดขึ้นในขณะที่พยานหลักฐานดิจิทัลอยู่ในความดูแลของบุคคลนั้น
6) หน่วยงานและเจ้าหน้าที่ที่ดำเนินการเก็บยึด เข้าถึงข้อมูล บันทึกข้อมูล โอนถ่ายเคลื่อนย้ายพยานหลักฐานดิจิทัล จะต้องรับผิดชอบในการปฏิบัติงานให้สอดคล้องกับหลักการข้างต้น

1.3) <u>การวิเคราะห์พยานหลักฐานดิจิทัล</u>

พยานหลักฐานแต่ละประเภทของคดีจะมีความแตกต่างกัน วิธีวิเคราะห์จึงแตกต่างกัน มีการใช้เครื่องมือที่แตกต่างกัน ทักษะเจ้าหน้าที่แตกต่างกัน การฝึกอบรมเจ้าหน้าที่พิสูจน์หลักฐานจึงมีความสำคัญ การวิเคราะห์พยานหลักฐานดิจิทัล จึงต้องใช้ผู้เชี่ยวชาญด้านพยานหลักฐานดิจิทัลมาวิเคราะห์ โดยปกติแล้ว จะมีการใช้โปรแกรมคอมพิวเตอร์เฉพาะ

ทาง ไม่ว่าจะเป็นโปรแกรมที่พัฒนาขึ้นโดยเฉพาะ หรือมีผู้พัฒนาสำหรับใช้วิเคราะห์พยานหลักฐานดิจิทัล เช่น โปรแกรมที่ใช้สำหรับตรวจสอบคอมพิวเตอร์และโทรศัพท์มือถือ สำหรับวิเคราะห์พยานหลักฐานดิจิทัลที่นิยมใช้ คือ Encase และ FTK จะเป็นโปรแกรมที่พัฒนาและขายให้กับหน่วยงานที่ทำหน้าที่พิสูจน์หลักฐานทางดิจิทัล โดยเฉพาะ สามารถใช้กู้ข้อมูลที่ถูกลบ ซ่อน ไม่ว่าจะโดยผู้ใช้ หรือโดยระบบ สามารถค้นหาข้อมูลที่ถูกเปลี่ยนแปลง แก้ไข เข้ารหัส และอื่นๆ โดยทั่วไปแล้ว การวิเคราะห์พยานหลักฐานดิจิทัล จะมีการวิเคราะห์ต่างๆ ดังนี้

- Computer forensics เช่น บัญชีผู้ใช้ รอยประทับเวลา รูปภาพ อีเมลที่บันทึกอยู่ในฮาร์ดไดฟ์คอมพิวเตอร์ รวมทั้งบันทึกจากหน่วยความจำ
- Cell Phone forensics เช่น บันทึกที่สร้างขึ้นโดยผู้ให้บริการโทรศัพท์มือถืออย่างข้อมูลการเรียกเก็บเงิน การบันทึกการใช้บริการ ไม่ว่าหมายเลขที่โทรออก โทรเข้า ระยะเวลาการโทร วันเวลาการโทร สถานีเครือข่ายที่โทรศัพท์เครื่องนั้นใช้งาน รายชื่อในโทรศัพท์ ข้อความ รูปภาพ อีเมล ฯลฯ
- GPS Forensics เช่น ตำแหน่งที่ไปเมื่อเร็วๆ นี้ สถานที่ที่ชอบ หยุดที่สถานที่ใดบ้าง นานเท่าใด ฯลฯ
- Social Media Forensics เช่น ข้อมูลเกี่ยวกับกิจกรรมออนไลน์ของกลุ่มเพื่อน การสื่อสาร กระทั่งแนวคิดของบุคคลผู้ต้องสงสัย
- Digital Video and Photo Forensics คือ การตรวจสอบรวมทั้งวิเคราะห์ภาพถ่าย
- Digital Camera Forensics เช่น ภาพถ่าย ข้อมูลเกี่ยวกับภาพ metadata รุ่นของกล้อง วันเวลาบันทึกภาพ
- Game Console forensics เช่น metadata ข้อมูลผู้เล่น บัญชีออนไลน์

1.4) <u>การนำเสนอผลพิสูจน์พยานหลักฐานดิจิทัล</u> การนำเสนอผลการตรวจพิสูจน์พยานหลักฐานดิจิทัล เป็นรายงานบันทึกคำให้การผู้เชี่ยวชาญ อธิบายวิธีการตรวจสอบ เครื่องมือที่ใช้ตรวจสอบ ตรวจสอบสิ่งใดบ้าง วิธีเก็บพยานหลักฐาน สิ่งที่ค้นพบ และวิธีการยืนยันความแท้จริงของพยานหลักฐานดิจิทัล พยานหลักฐานดิจิทัลซึ่งพนักงานสอบสวนได้รวบรวมเพื่อพิสูจน์ว่าผู้ต้องหากระทำความผิดตามข้อกล่าวหา จะถูกเสนอต่อศาลระหว่างกระบวนการพิจารณาสืบพยาน โดยศาลมีอำนาจใช้ดุลพินิจรับฟังและชั่งน้ำหนักของพยานหลักฐานดิจิทัลตามที่กฎหมายกำหนด ปัจจุบันยังไม่มีบทบัญญัติเกี่ยวกับการรับฟังพยานหลักฐานดิจิทัลในคดีอาญาเป็นการเฉพาะเจาะจง การรับฟังพยานหลักฐานดิจิทัลจึงต้องเป็นไปตามหลักการรับฟังพยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาความอาญาอันเป็นบทกฎหมายทั่วไป ซึ่งมาตรา 226 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา บัญญัติไว้ว่า “พยานวัตถุ พยานเอกสาร หรือพยานบุคคลซึ่งน่าจะพิสูจน์ได้ว่าจำเลยมีผิดหรือบริสุทธิ์ ให้อ้างเป็นพยานหลักฐานได้ แต่ต้องเป็นพยานชนิดที่ไม่ได้เกิดขึ้นจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวงหรือโดยมิ

ชอบประการอื่น และให้สืบตามบทบัญญัติแห่งประมวลกฎหมายนี้ หรือกฎหมายอื่นอันว่าด้วยการสืบพยาน” โดยคำว่า “...ที่ไม่ได้เกิดขึ้น...โดยมิชอบประการอื่น” จึงหมายถึงว่า กรณีที่มีกฎหมายเฉพาะอื่นที่ใช้บังคับหรือบัญญัติหลักเกณฑ์ และวิธีการในการได้มาซึ่งพยานหลักฐานดิจิทัลไว้ การรวบรวมพยานหลักฐานนั้นจะต้องต้องปฏิบัติให้ถูกต้องตามหลักเกณฑ์และวิธีการดังกล่าวนอกเหนือไปจากหลักเกณฑ์ทั่วไปตามประมวลกฎหมายวิธีพิจารณาความอาญาด้วย ไม่เช่นนั้นจะถือว่าเป็นการได้พยานหลักฐานดิจิทัลมาโดยมิชอบ ศาลมีอำนาจไม่รับฟังได้ ดังนั้น การจัดเก็บรวบรวมพยานพยานหลักฐานดิจิทัลให้ชอบด้วยกฎหมายที่ใช้บังคับในแต่ละประเภทคดีจึงเป็นเรื่องที่สำคัญมาก เนื่องจากแม้ว่าในชั้นสอบสวน เจ้าพนักงานได้รวบรวมพยานหลักฐานที่เห็นว่าเพียงพอต่อการระบุตัวผู้กระทำความผิดและพิสูจน์ความผิดที่บุคคลนั้นกระทำแล้ว หากกระบวนการจัดเก็บพยานหลักฐานมีข้อโต้แย้งในเรื่องการได้มาซึ่งพยานหลักฐานดิจิทัลว่าเป็นไปโดยชอบด้วยกฎหมายหรือไม่ จะมีประเด็นในเรื่องของคุณค่าในการพิสูจน์ความผิดของพยานหลักฐานนั้น หรือไม่อาจรับฟังในชั้นพิจารณา หรือทำให้พยานหลักฐานนั้นมีน้ำ หนักในการรับฟังได้น้อย

2) ปัญหาและอุปสรรคของกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล

ในขณะนี้ประเทศไทยยังไม่มีการกำหนดมาตรฐานการเก็บรวบรวมและพิสูจน์พยานหลักฐานดิจิทัล ทั้งในเรื่องหน่วยงานกลาง ไม่มีเครื่องมือในการตรวจพิสูจน์เพียงพอครบทุกสื่อดิจิทัล ทั้งยังไม่มีการวางมาตรฐานกลาง ขณะที่ต่างประเทศมีหน่วยงานที่ทำหน้าที่กำหนดมาตรฐานการเก็บรวบรวมและพิสูจน์พยานหลักฐานดิจิทัล

พยานหลักฐานดิจิทัลมีลักษณะเฉพาะ คือ สามารถเปลี่ยนแปลงแก้ไขได้ และอีกลักษณะเฉพาะของอุปกรณ์ดิจิทัล โดยเฉพาะคอมพิวเตอร์หรืออุปกรณ์เก็บข้อมูลก็คือ เมื่อสามารถเข้าถึงข้อมูลได้แล้วก็สามารถ เห็นได้หมดว่าในคอมพิวเตอร์หรืออุปกรณ์เครื่องนั้นเก็บข้อมูลอะไรไว้บ้าง โดยอาจมีการเข้ารหัสไว้ ซึ่งนำมาสู่คำถามที่ว่า หากเจ้าหน้าที่มีหมายค้นการกระทำผิดหนึ่ง และเมื่อเข้าถึงเครื่องคอมพิวเตอร์ของบุคคลแล้วพบความผิดอื่น เจ้าหน้าที่สามารถแจ้งข้อหาอื่นด้วยได้หรือไม่ ซึ่งยังเป็นสิ่งที่ต้องมีการตีความ ว่าจัดว่าเป็นความผิดซึ่งหน้า ที่ใน ป. วิอาญาเปิดช่องไว้ให้ศาลใช้ดุลพินิจได้ว่า แม้ว่าพยานหลักฐานจะได้มาโดยมิชอบ แต่หากพยานหลักฐานนั้นเป็นประโยชน์ต่อการอำนวยความยุติธรรมก็สามารถนำมาใช้ได้ หรือเป็นการเปิดช่องให้เจ้าหน้าที่อ้างความผิดอย่างหนึ่งเพื่อเข้าค้นทุกอย่างในคอมพิวเตอร์ส่วนบุคคลได้

จากสถานการณ์ในปัจจุบัน เมื่อมีคดีความซึ่งมีพยานหลักฐานดิจิทัลเข้ามาเกี่ยวข้อง โจทก์และจำเลยมักมีอำนาจในการต่อสู้คดีไม่เท่าเทียมกัน เพราะคดีดังกล่าวส่วนใหญ่โจทก์คือรัฐ ซึ่งมีเครื่องมือและทรัพยากรของรัฐในขณะที่จำเลยส่วนใหญ่ไม่มีทั้งผู้เชี่ยวชาญและความรู้ทางเทคนิคที่จะมาใช้ต่อสู้คดี จึงเป็นเหตุที่ควรให้มีการเรียนรู้เรื่องเทคนิคของพยานหลักฐานดิจิทัลด้วย โดยที่ผ่านมาพบว่าศาลมักไม่ค่อยได้นำสืบตัวพยานหลักฐานดิจิทัลที่นำมาใช้กล่าวอ้าง ว่ามีข้อบกพร่องอย่างไรผ่านการเก็บรักษาและพิสูจน์พยานหลักฐานอย่างถูกต้องหรือไม่ แต่มักจะให้น้ำหนักกับคำอธิบายหรือการตีความพยานหลักฐานของฝ่ายเจ้าหน้าที่รัฐ และแม้ว่าจะมีการค้านและพยายามชี้ให้เห็นจุดอ่อน

ของพยานหลักฐานดิจิทัลที่ฝ่ายโจทก์นำมาใช้กล่าวอ้าง บางครั้งก็ประสบปัญหาว่าศาลไม่รับฟังคำค้าน

นอกจากนี้ หลายคดีที่เกี่ยวข้องกับ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 แม้จะมีจุดอ่อนในพยานหลักฐานดิจิทัลที่ฝ่ายรัฐนำมาใช้อ้าง แต่ในทางปฏิบัติแล้วบ่อยครั้งพบว่าผู้ถูกกล่าวหาเลือกที่จะไม่สู้คดี แต่เลือกที่จะสารภาพแทนแม้ว่าจะไม่ได้กระทำผิดจริง โดยมีคำบอกเล่าจาก กลุ่มที่ 2 ของผู้สัมภาษณ์อธิบายว่า เมื่อสู้คดีไป ก็ไม่แน่ว่าจะต้องถูกตัดสินจำคุกเป็นระยะเวลานานเท่าใด อีกทั้ง ไม่ทราบว่าจะมีโอกาสในการชนะคดีหรือไม่ ในขณะที่หากเลือกการรับสารภาพ จะทราบแน่ชัดว่า ต้องโทษจำคุกกี่ปี มีสิทธิได้รับการลดหย่อน โดยได้รับโทษกึ่งหนึ่ง และยังมีสิทธิได้รับการอภัยโทษ

พยานหลักฐานทางอิเล็กทรอนิกส์เป็นข้อมูลอิเล็กทรอนิกส์ที่มีลักษณะเฉพาะ คือ สามารถเปลี่ยนแปลงแก้ไขได้ง่าย เจ้าหน้าที่ที่เกี่ยวข้องต้องตามให้ทันความพยายามกลบเกลื่อนร่องรอยของผู้กระทำความผิด และสำหรับความก้าวหน้าของเทคโนโลยี เช่น ความจุของอุปกรณ์เก็บข้อมูลที่มีความจุมากขึ้น รวมถึงความซับซ้อนในการเข้ารหัส ทำให้ต้องใช้เวลาในการตรวจพิสูจน์มากขึ้น ในขณะที่ต้องทำงานแข่งกับเวลา นอกจากนั้น การที่ประเทศไทยยังต้องพึ่งพาเทคโนโลยีจากต่างประเทศเป็นหลัก ทำให้ขาดผู้เชี่ยวชาญที่มีความรู้ในเชิงลึก และขาดการประสานงานระหว่างภาครัฐกับภาคเอกชน ที่จะทำให้การสืบสวน เป็นไปอย่างมีประสิทธิภาพและรวดเร็ว ทำให้ผู้กระทำความผิดอาศัยช่องว่างของการไม่ประสานงานกันระหว่างหน่วยงานกระทำความผิดเพิ่มมากขึ้น

ในการเก็บรวบรวมและตรวจพิสูจน์พยานหลักฐานนั้น ปัญหาที่พบส่วนหนึ่ง ไม่ใช่การใช้เครื่องมือ แต่อยู่ที่ “กระบวนการ” บ่อยครั้งที่หลักฐานถูกเปลี่ยนแปลงมาก่อนที่จะถึงผู้ตรวจพิสูจน์ การสื่อสารเพื่อให้เกิดความเข้าใจที่ตรงกันระหว่างผู้เก็บรวบรวมหลักฐาน เจ้าหน้าที่ผู้ทำคดี และผู้ตรวจพิสูจน์จึงมีความสำคัญ รวมทั้งการสร้างความรู้และการตระหนักรู้ให้ผู้เกี่ยวข้อง ปฏิบัติงานโดยไม่ให้หลักฐานถูกเปลี่ยนแปลงโดยไม่ทราบหรือไม่ได้ตั้งใจ

หลักการรักษาสภาพหลักฐานและไม่เปลี่ยนแปลงหลักฐาน เจ้าหน้าที่ที่ตรวจพิสูจน์จะต้องสามารถอธิบายสิ่งที่ทำและผลกระทบ รวมทั้งมีการจดบันทึกทุกอย่างอย่างครบถ้วน ซึ่งประเทศไทยก็ดำเนินการตาม Statement of Purpose หรือ SOP ซึ่งเป็นมาตรฐานที่จะกำหนดว่า พยานหลักฐานทางอิเล็กทรอนิกส์คืออะไร และอธิบายแนวทางวิธีการเก็บหลักฐาน การขนส่ง การเขียนรายงาน ฯลฯ ซึ่งหน่วยงานที่เกี่ยวข้อง ไม่เพียงแต่ตำรวจ อัยการ ศาล ต้องพัฒนาร่วมกัน เพื่อให้ เป็นที่ยอมรับของทุกฝ่ายและสามารถใช้ได้จริง เพราะการจัดการกับอาชญากรรมคอมพิวเตอร์ต้องมีการบูรณาการการทำงานร่วมกันเป็นทีม

ศาสตร์ทางด้านอาชญาวิทยาก็เป็นสิ่งสำคัญ การเข้าใจความคิดของอาชญากรเป็นอีกส่วนที่ช่วยให้เข้าใจมุมมองและค้นหาสาเหตุ แรงจูงใจในการกระทำทำความผิด รวมถึงเรื่องการรักษาความปลอดภัยในระบบคอมพิวเตอร์ และการส่งเสริมองค์ความรู้ด้านการตรวจพิสูจน์หลักฐานซึ่งยังไม่เพียงพอในขณะนี้ ควบคู่ไปกับแนวคิดด้านการสืบสวนสอบสวน จากประสบการณของผู้เชี่ยวชาญในกระบวนการยุติธรรม ทั้งไทยและต่างประเทศ ซึ่งในส่วนพนักงานเจ้าหน้าที่ของรัฐเองก็ต้องปรับตัวให้ทันกับเทคโนโลยีในการเพิ่มพูนความรู้และการทำงาน การจัดการกับหลักฐาน ฝ่ายบังคับใช้

กฎหมายกับฝ่ายเทคนิคต้องประสานงานและเข้าใจกันมีการแชร์ข้อมูลให้กัน เพื่อเป็นฐานข้อมูลที่เป็นประโยชน์ในการจัดการกับอาชญากรรมทางออนไลน์รวมทั้งพยานหลักฐานทางอิเล็กทรอนิกส์

สิ่งสำคัญอีกอย่าง ก็คือ การสร้างความตระหนักในการป้องกันข้อมูลของตนเอง และเรียนรู้วิธีการแจ้งเหตุเมื่อเกิดภัยคุกคามต่างๆ อย่างมีประสิทธิภาพ

4.3 แนวทางการแก้ไขปัญหา และปรับปรุงการดำเนินงาน รวมถึงการปรับปรุงกฎหมายและการบังคับใช้

4.3.1 แนวทางการแก้ไขปัญหา และปรับปรุงการดำเนินงาน

องค์ความรู้เรื่องการจัดการกับพยานหลักฐานอิเล็กทรอนิกส์ ยังเป็นเรื่องใหม่สำหรับประเทศไทย ต่างจากความรู้เรื่องการจัดการพยานหลักฐานแบบเดิมมีอยู่แล้ว และปัจจุบันกฎหมายหลายฉบับของประเทศไทยก็ได้ให้อำนาจเจ้าหน้าที่ของรัฐในการเข้าถึงพยานหลักฐานเหล่าแต่ปัญหาคือ ประเทศไทยยังไม่มีมาตรฐานชัดเจนว่า เมื่อเข้าถึงแล้วจะมีการดูแลรักษาความบริสุทธิ์ของพยานหลักฐานอย่างไร ในการกระทำความผิดที่เกี่ยวข้องกับพยานหลักฐานอิเล็กทรอนิกส์ ผู้กระทำผิดสามารถกระทำที่ใดก็ได้ ทำให้เกิดความยุ่งยากในการสืบว่าผู้กระทำผิดกระทำผิด ณ ที่ใด และการหาความเชื่อมโยงระหว่างผู้กระทำความผิดกับอุปกรณ์ที่ใช้กระทำความผิดยังทำได้ยาก พยานหลักฐานอิเล็กทรอนิกส์จึงมีลักษณะเหมือน “จิ๊กซอว์” คือ กระจายหลายที่ และการเข้ารหัสข้อมูล ยังเป็นอีกหนึ่งอุปสรรคที่ทำให้การเข้าถึงข้อมูลพยานหลักฐานอิเล็กทรอนิกส์ของเจ้าหน้าที่ยุ่งยากขึ้น หรือแม้ว่าสามารถเข้าถึงข้อมูลได้ แต่ก็ประสบปัญหาการขาดผู้เชี่ยวชาญในการวิเคราะห์ข้อมูลและเชื่อมโยงข้อมูลที่มีเข้ากับตัวผู้กระทำผิด ทำให้ให้บางครั้งไม่มั่นใจในความบริสุทธิ์ของพยานหลักฐานเหล่านั้น ปัญหาหลักของเจ้าหน้าที่ตำรวจ คือ ไม่มีความรู้เกี่ยวกับการจัดการพยานหลักฐานอิเล็กทรอนิกส์ แม้ไม่ได้มีความตั้งใจจะทำให้พยานหลักฐานปนเปื้อน ดังนั้น การทำแนวทางในการปฏิบัติงานให้เจ้าหน้าที่ตำรวจ ที่เข้าใจง่าย ชัดเจน เป็นขั้นตอนไม่จำเป็นต้องลงรายละเอียดมากนัก จะช่วยให้เจ้าหน้าสามารถจัดการกับพยานหลักฐานอิเล็กทรอนิกส์ได้ดีขึ้น การขาดแคลนบุคลากรและค่าตอบแทนบุคคลากรที่ไม่ดึงดูดก็เป็นอีกสาเหตุหนึ่ง นอกไปจากปัญหาเรื่องการขาดแคลนงบประมาณ เจ้าหน้าที่เทคนิคที่ทำงานในห้องตรวจพิสูจน์พยานหลักฐานอิเล็กทรอนิกส์ หลายครั้งเขียนรายงานผลการตรวจพิสูจน์พยานหลักฐานอิเล็กทรอนิกส์ไม่ชัดเจน เนื้อหาในรายงานตอบไม่ตรงประเด็นคำถามของเจ้าหน้าที่ผู้ที่นำพยานหลักฐานมาให้ตรวจ

นอกจากมาตรฐานในการจัดเก็บ และตรวจวิเคราะห์พยานหลักฐานอิเล็กทรอนิกส์ในคอมพิวเตอร์แล้ว ยังมีเทคนิคเฉพาะในการจัดการกับพยานหลักฐานอิเล็กทรอนิกส์ที่อยู่ในโทรศัพท์มือถือ และบนระบบเครือข่าย ซึ่งประเทศไทยควรต้องมีการจัดทำมาตรฐานเหล่านี้ด้วย ในต่างประเทศได้มีการพัฒนามาตรฐานการตรวจพิสูจน์พยานหลักฐานอิเล็กทรอนิกส์ให้ครอบคลุมมาก เช่น มีการสร้างมาตรฐานการตรวจพิสูจน์พยานหลักฐานดิจิทัลและมัลติมีเดีย โดยดูว่ามีการเปลี่ยนแปลงแก้ไขพยานหลักฐานอิเล็กทรอนิกส์ที่อยู่ในรูปไฟล์เสียง หรือวิดีโอ หรือไม่ และยังมีการจัดทำแนวปฏิบัติในการตั้งคำถามเพื่อให้ได้คำตอบที่เป็นประโยชน์ต่อรูปคดี เช่น หากเกิดเหตุการณ์ที่หลักฐานมีการปนเปื้อนขึ้น เจ้าหน้าที่ควรจะตั้งคำถามอะไร นอกจากนี้ ในต่างประเทศยังมีแนวปฏิบัติในส่วนของเอกสาร เช่น การเขียนคำร้องขอหมายค้นและหมายยึดจากศาลด้วย เนื่องจากประสบ

ปัญหาว่า เมื่อได้หมายค้นจากศาล เจ้าหน้าที่ไม่สามารถระบุได้ชัดเจนว่าต้องการค้นหาอะไรในคอมพิวเตอร์ของผู้ต้องสงสัย เนื่องจากลักษณะเฉพาะของคอมพิวเตอร์ที่ทำให้ยากจะระบุเฉพาะเจาะจงไปได้ว่าต้องการค้นอะไร ซึ่งประเทศไทยเอง ก็ควรมีการพัฒนามาตรฐานในส่วนนี้ รวมถึงมีการแก้ไขกฎหมายที่เกี่ยวข้อง เช่น ประมวลกฎหมายวิธีพิจารณาความอาญา, ประมวลกฎหมายวิธีพิจารณาความแพ่ง

จากปัจจุบันที่ผู้ใช้อินเทอร์เน็ตเริ่มใช้บริการเก็บข้อมูลไว้บนคลาวด์ (Cloud) มากขึ้น ซึ่งข้อมูลส่วนใหญ่จะถูกนำไปเก็บไว้ในเครื่องคอมพิวเตอร์แม่ข่ายในต่างประเทศ ส่งผลต่อประเด็นขอบเขตอำนาจศาล โดยปัญหาเรื่องขอบเขตอำนาจศาลเป็นอุปสรรคหนึ่งของเจ้าหน้าที่รัฐ ในการเข้าถึงพยานหลักฐานและผู้กระทำผิด เนื่องจากกฎหมายของไทยบังคับใช้ได้เพียงในประเทศไทยเท่านั้น ไม่สามารถบังคับใช้กับประเทศอื่น ปัจจุบันช่องทางเดียวที่เป็นทางการในการประสานความร่วมมือกับต่างประเทศคือ พ.ร.บ.ความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ.2535 อย่างไรก็ตาม พ.ร.บ.ดังกล่าวไม่ตอบโจทย์การทำงานจริง เพราะมีความล่าช้า และกระบวนการยังเป็นแบบงานเอกสาร กินเวลานาน ไม่ทันกับความรวดเร็วในการทำลายพยานหลักฐานดิจิทัล ส่วนอีกช่องทางหนึ่งที่เจ้าหน้าที่ของไทยใช้ในการประสานงานกับต่างประเทศ คือ องค์การตำรวจอาชญากรรมระหว่างประเทศ หรือ INTERPOL แต่ก็ยังไม่ใช่ช่องทางที่เป็นทางการ ประเทศไทยจำเป็นต้องพัฒนาช่องทางการประสานงานกับต่างประเทศในเรื่องพยานหลักฐานอิเล็กทรอนิกส์ให้ทันสมัย

ในส่วนของพยานหลักฐานอิเล็กทรอนิกส์ที่อยู่ในสังคมออนไลน์ หรือระบบเครือข่าย สามารถมองแยกว่ามีอยู่ 3 ส่วนด้วยกัน คือ

1) ผู้ให้บริการเนื้อหา เช่น เฟซบุ๊ก กูเกิล ซึ่งเจ้าหน้าที่ไทยไม่สามารถดำเนินการได้อย่างสะดวกนัก เพราะผู้ให้บริการเนื้อหาเหล่านี้อยู่ในต่างประเทศ ถึงแม้จะมีสำนักงานในประเทศไทย
2) ผู้ให้บริการเชื่อมต่ออินเทอร์เน็ต ซึ่งมีความสำคัญมาก เนื่องจากเป็นผู้เชื่อมต่อระหว่างผู้กระทำความผิดกับเนื้อหาที่ผิดกฎหมาย
3) อุปกรณ์ของผู้กระทำความผิดเอง เช่น คอมพิวเตอร์ โทรศัพท์มือถือที่ใช้ในการกระทำความผิด

ข้อเสนอแนะและมาตรฐานต่างๆ ขณะนี้ เน้นไปที่การจัดการกับพยานหลักฐานอิเล็กทรอนิกส์ที่อยู่ในความครอบครองของผู้กระทำผิด แต่หากมีมาตรฐานการจัดการ กับพยานหลักฐานอิเล็กทรอนิกส์ที่เกี่ยวกับระบบเครือข่าย ก็จะช่วยในการสืบสวน เพราะบางครั้งไม่จำเป็นต้องขอความร่วมมือไปยังผู้ให้บริการเนื้อหาที่อยู่ต่างประเทศ ซึ่งบางครั้งก็ไม่ให้ความร่วมมือ แต่จะสามารถเก็บบันทึกข้อมูลการจราจรทางอินเทอร์เน็ตจากผู้ให้บริการเชื่อมต่ออินเทอร์เน็ตได้

พยานหลักฐานอิเล็กทรอนิกส์ ควรเป็นส่วนหนึ่งในแผนแม่บทของนโยบายเศรษฐกิจดิจิทัลของรัฐบาล เพราะพยานหลักฐานอิเล็กทรอนิกส์เป็นส่วนหนึ่งของเศรษฐกิจดิจิทัลอย่างแยกกันไม่ออก ถึงแม้จะมีกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์ มีกฎหมายคุ้มครองข้อมูลส่วนบุคคล แต่หากการเก็บข้อมูลพยานหลักฐานอิเล็กทรอนิกส์ยังไม่มีมาตรฐาน กระบวนการตรวจพิสูจน์พยานหลักฐานอิเล็กทรอนิกส์ยังไม่มีมาตรฐานที่ชัดเจน รัดกุม สิ่งเหล่านี้จะเป็นอุปสรรคต่อความเชื่อมั่น และการเติบโตของเศรษฐกิจดิจิทัล ซึ่งเป็นแนวโน้มหลักของโลกยุคปัจจุบัน

นอกจากเรื่องมาตรฐานการจัดการกับพยานหลักฐานอิเล็กทรอนิกส์ของเจ้าหน้าที่รัฐแล้ว ก็ควรมีกระบวนการและเครื่องมือให้ภาคเอกชน ในการเข้าถึงพยานหลักฐานอิเล็กทรอนิกส์อย่างเท่าเทียมกันด้วย จึงจะอำนวยความยุติธรรมให้เป็นไปอย่างทัดเทียม ไม่เป็น 2 มาตรฐาน หรือเปิดโอกาสให้เจ้าหน้าที่ของรัฐใช้เป็นช่องทาง เป็นข้องได้เปรียบในคดี

การพัฒนากระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล แต่เดิมส่วนใหญ่เป็นงานด้านวิทยาศาสตร์และคอมพิวเตอร์ ไม่สามารถเชื่อมโยงกับการพิจารณาคดีตามกฎหมายได้มากนัก ศึกษาเฉพาะด้านเทคนิค ดังนั้นการจัดการกับปัญหาอาชญากรรมจะเป็นไปอย่างมีประสิทธิภาพ จะต้องมีการทำงานร่วมกันเป็นทีม เป็นการบูรณาการร่วมกันขอทุกภาคส่วน เพื่อให้เป็นมาตรฐานเดียวกัน มาตรฐานส่วนนี้จึงเป็นเรื่องสำคัญ ที่จะทำให้การจัดการพยานหลักฐานดิจิทัลซึ่งมีอยู่ทุกแห่ง มีความน่าเชื่อถือ รับฟังได้ในชั้นพิจารณาคดี

4.3.2 การปรับปรุงกฎหมายและการบังคับใช้

4.3.2.1 ข้อเสนอแนะในการปรับปรุงกฎหมาย

1) มีการศึกษาและทบทวนกฎหมายที่เกี่ยวข้องเพื่อให้เหมาะสมกับบริบทของอาชญากรรมคอมพิวเตอร์ในสถานการณ์ปัจจุบัน ทั้งในส่วนของพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ และในส่วนของพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ เพื่อให้ขอบเขตของกระบวนการตรวจพิสูจน์หลักฐานทางดิจิทัล มีความชัดเจน ครอบคลุม และ การกระทำความผิดทางคอมพิวเตอร์ มุ่งเน้นในส่วนของระบบมากกว่าเนื้อหา กล่าวคือ

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

ตามร่างที่เสนอ เพื่อปรับปรุงหลักเกณฑ์เกี่ยวกับการดำเนินการทางธุรกรรมทางอิเล็กทรอนิกส์ให้มีมาตรฐานสากล เช่น การเพิ่มบทนิยามคำว่า “ระบบแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์” เพื่อให้สอดคล้องกับอนุสัญญาสหประชาชาติว่าด้วยการใช้การติดต่อสื่อสารทางอิเล็กทรอนิกส์ในสัญญาระหว่างประเทศ (United Nations Convention on the Use of Electronic Communications in International Contracts), เพิ่มเติมเกี่ยวกับผลทางกฎหมายในการลงลายมือชื่ออิเล็กทรอนิกส์ ในกรณีที่ไม่มีการลงลายมือชื่อ หากได้ดำเนินการตามที่กำหนดไว้ก็ถือว่าได้มีการลงลายมือชื่อ, แก้ไขวิธีการตรวจสอบว่าข้อมูลอิเล็กทรอนิกส์เป็นของผู้ส่งข้อมูล โดยให้ผู้รับข้อมูลตรวจสอบตามวิธีการที่ผู้ส่งข้อมูลได้ตกลงหรือผูกพันตนไว้ว่าเป็นข้อมูลอิเล็กทรอนิกส์, กำหนดให้บุคคลธรรมดามีสิทธิที่จะถอนการแสดงเจตนาในกรณีที่มีการลงข้อมูลโดยผิดพลาดและส่งผ่านระบบแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์อัตโนมัติของผู้อื่นซึ่งไม่มีช่องทางให้แก้ไขข้อผิดพลาด, กำหนดให้ศาลหรือองค์กรตามรัฐธรรมนูญมีดุลพินิจที่จะนำหลักเกณฑ์ในเรื่องใดของพระราชกฤษฎีกาที่กำหนดหลักเกณฑ์และวิธีการเกี่ยวกับการจัดทำข้อมูลอิเล็กทรอนิกส์ของหน่วยงานของรัฐมาใช้แก่การดำเนินกระบวนพิจารณาพิพากษาคดีของศาลหรือในการวินิจฉัยชี้ขาดข้อพิพาทก็ได้

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ควรมีการแก้ไขพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ใน มาตรา 14, 16 และ 20 โดย

มาตรา 14 จากเดิมที่กำหนดฐานความผิดเกี่ยวกับการนำเข้า เผยแพร่หรือส่งต่อข้อมูลที่บิดเบือน ปลอม หรือเป็นเท็จ หรือข้อมูลที่กระทบความมั่นคง หรือข้อมูลลามก ให้เหลือเพียงฐานความผิดเดียวคือ "ฐานความผิดกรณีหลอกลวงผู้อื่นด้วยการนำเข้า เผยแพร่ และส่งต่อข้อมูลปลอม" หรือเรียกว่า ความผิดฐานปลอมข้อมูลคอมพิวเตอร์ และกำหนดให้ฐานความผิดดังกล่าวเป็นความผิดอันยอมความได้

มาตรา 16 เพิ่มเติมกรณีที่กำหนดให้ศาลอาจสามารถสั่งให้ทำลายข้อมูลหรือให้โฆษณาหรือเผยแพร่คำพิพากษาทั้งหมดหรือแต่บางส่วน หรือให้ดำเนินการอื่นตามที่ศาลเห็นสมควร ซึ่งเดิมกำหนดให้ศาลมีอำนาจสั่งได้เฉพาะคดีที่เป็นความผิดตามมาตรา 14 กรณีความผิดฐานหลอกลวงผู้อื่นด้วยการนำเข้า เผยแพร่และส่งต่อข้อมูลโดยทุจริต และมาตรา 16 กรณีความผิดฐานนำข้อมูลภาพของผู้อื่นที่สร้างขึ้น ตัดต่อ เติม ดัดแปลงเข้าสู่ระบบคอมพิวเตอร์ โดยประการที่น่าจะเสียชื่อเสียง ถูกดูหมิ่นถูกเกลียดชัง หรืออับอาย โดยตัดความว่า "มาตรา 14 หรือมาตรา 16 ซึ่งมี" ออก เพื่อให้ศาลสามารถสั่งให้จำเลยดำเนินการดังกล่าวได้ในทุกฐานความผิดตามที่ศาลพิพากษาว่าจำเลยมีความผิดอันเป็นไปตามที่ศาลเห็นสมควร

มาตรา 20 แก้ไขเพิ่มเติมเกี่ยวกับอำนาจหน้าที่ของเจ้าหน้าที่ในการยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจ เพื่อขอให้ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ จากเดิมที่กำหนดให้พนักงานเจ้าหน้าที่ต้องดำเนินกระบวนการดังกล่าวโดยได้รับความเห็นชอบจากรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และกำหนดให้รัฐมนตรีสามารถแต่งตั้งคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์เพื่อดำเนินการสำหรับกรณีที่ข้อมูลคอมพิวเตอร์ที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชนมีการทำให้แพร่หลาย โดยแก้ไขเพิ่มเติมให้การยื่นคำร้องต่อศาลดำเนินการโดยเจ้าหน้าที่ซึ่งมีอำนาจหน้าที่ทำการสอบสวนในการกระทำความผิดตามกฎหมาย หรือให้พนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญาซึ่งได้ร้องขอให้พนักงานเจ้าหน้าที่ตามกฎหมายนี้เป็นผู้ดำเนินการ โดยไม่ต้องมีคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์ที่แต่งตั้งโดยรัฐมนตรีเกี่ยวข้อง

2) กำหนดหน่วยงานกลางของรัฐที่รับผิดชอบดูแลและปรับปรุงมาตรฐานกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลให้เหมาะกับเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว เริ่ม

จากการส่งเสริมบทบาทของ ศูนย์ดิจิทัลฟอเรนสิกส์ (Digital Forensics Center) ที่มีอยู่เดิม ซึ่งอยู่ภายใต้การกำกับดูแลของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) หรือ ETDA กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และยกระดับเป็นหน่วยงานที่มีขอบเขตอำนาจที่ชัดเจนในการกำหนดมาตรฐาน

3) มีการกำหนดแนวทางในการประเมินผล เพื่อให้ทราบถึงปัญหาและอุปสรรคที่เกิดขึ้นของกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลจากการปฏิบัติงานจริงของภาคส่วนต่างๆ และนำผลที่ได้มาเป็นแนวทางสำหรับการจัดทำแผนแม่บท และใช้ในการศึกษาและทบทวนกฎหมายที่เกี่ยวข้อง
4) สร้างเครือข่ายการบูรณาการความร่วมมือกับหน่วยงานทั้งภาครัฐ ภาคเอกชน ภาคประชาชน และความร่วมมือระหว่างประเทศในด้านอาชญากรรมคอมพิวเตอร์ รวมถึงกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล เพื่อนำกรณีศึกษาต่างๆ มาเป็นตัวอย่างสำหรับพัฒนากระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลในประเทศไทย

4.3.2.2 ข้อเสนอแนะในการบังคับใช้

ข้อเสนอแนะในส่วนการกระบวนการตรวจพิสูจน์พยานหลักฐาน มีดังนี้

1) <u>การรวบรวมพยานหลักฐานดิจิทัล</u>

เนื่องจากสิ่งสำคัญที่สุด คือ ความสมบูรณ์ของพยานหลักฐาน และการรวบรวมพยานหลักฐานทั้งหมดให้เป็นไปอย่างสมบูรณ์ขณะเกิดเหตุโดยไม่ถูกเปลี่ยนแปลงแก้ไขใดๆ พนักงานสอบสวน ผู้มีหน้าที่ในการรวบรวมพยานหลักฐานดิจิทัล จะต้องดำเนินการโดยปฏิบัติตาม ประมวลกฎหมายวิธีพิจารณาความอาญา ซึ่งเป็นกฎหมายทั่วไป รวมถึงอำนาจหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งมีกฎหมายบัญญัติไว้โดยเฉพาะเจาะจงในเรื่องของอำนาจของพนักงานสอบสวนและหลักเกณฑ์วิธีการในการรวบรวมและจัดเก็บพยานหลักฐานด้วย

2) <u>การเก็บรักษาพยานหลักฐานดิจิทัล</u>

การเก็บรักษาจะต้องเก็บรักษาไว้ในสภาพที่รับฟังได้ในชั้นศาล เป็นไปตามกระบวนการสร้างห่วงโซ่คุ้มครองพยานหลักฐานในหลักสากลต้องมีมาตรฐานการเก็บรักษาพยานหลักฐานดิจิทัลที่เป็นที่ยอมรับของทุกฝ่ายมีบันทึกขั้นตอนการคุ้มครองพยานหลักฐานและวิธีการเก็บรักษา เพื่อให้มั่นใจได้ว่าเป็นข้อมูลที่ไม่ได้ถูกแก้ไขเปลี่ยนแปลงนับจากที่ได้รับมาจากที่เกิดเหตุ ในปัจจุบันสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. ได้เผยแพร่เอกสาร “ข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐาน” เพื่อเป็นแนวทางเบื้องต้นให้กับเจ้าหน้าที่ที่เกี่ยวข้องกับการจัดเก็บ รวบรวม และตรวจพิสูจน์พยานหลักฐานดิจิทัล ให้ปฏิบัติงานในสถานที่เกิดเหตุและในห้องปฏิบัติการให้สอดคล้องกับมาตรฐานสากล โดยสพธอ. เน้นในเรื่องการให้ความสำคัญต่อการบันทึกแบบฟอร์มที่เรียกว่า “Chain of Custody” หรือห่วงโซ่คุ้มครองพยานหลักฐาน คือ กระบวนการระบุสายความรับผิดชอบการเก็บรักษาพยานหลักฐาน เริ่มตั้งแต่เมื่อพยานหลักฐานถูก

เก็บรวบรวม เพื่อสร้างความต่อเนื่องของการครอบครองพยานหลักฐาน โดยข้อมูลที่เจ้าหน้าที่ผู้ปฏิบัติงานในแต่ละสายงาน จำเป็นต้องระบุ รวมถึงข้อมูลติดต่อและลงลายมือชื่อของผู้ส่งมอบพยานหลักฐาน, เหตุผลในการรับ-ส่งมอบพยานหลักฐาน, วิธีการส่งมอบพยานหลักฐาน เช่น ส่งมอบโดยเจ้าหน้าที่ที่เกี่ยวข้องหรือส่งมอบโดยพนักงานส่งของ และสถานที่จัดเก็บพยานหลักฐาน เป็นต้น นอกจากนี้ International Organization on Computer Evidence หรือ IOCE ซึ่งเป็นหน่วยงานสากลที่ดูแลเกี่ยวกับการปฏิบัติต่อพยานหลักฐานดิจิทัล ได้กำหนดหลักการสำคัญ ในการเข้าค้นและยึดอุปกรณ์ อิเล็กทรอนิกส์ไว้ 6 ประการ คือ

- เมื่อใดก็ตามที่ต้องดำเนินการกับพยานหลักฐานดิจิทัล จะต้องมีการดำเนินการตามหลักปฏิบัติทั่วไปทางนิติคอมพิวเตอร์ และต้องดำเนินการตามขั้นตอนของนิติคอมพิวเตอร์
- ในขณะปฏิบัติการเก็บยึดพยานหลักฐานดิจิทัล การดำเนินการทุกอย่างจะต้องไม่ก่อให้เกิดการเปลี่ยนแปลงต่อพยานหลักฐานนั้น
- หากมีความจำเป็นที่จะต้องเข้าถึงข้อมูลในพยานหลักฐานต้นฉบับ เจ้าหน้าที่ผู้ปฏิบัติจะต้องได้รับการอบรมมาเพื่อดำเนินการเป็นการเฉพาะ
- จะต้องมีการจดบันทึกรายละเอียดทุกขั้นตอน ทุกการกระทำที่เกี่ยวข้องกับการเก็บยึด การเข้าถึงข้อมูล การเคลื่อนย้าย และต้องมีการเก็บรักษาบันทึกนั้นไว้ และสามารถนำมาแสดงได้เมื่อถูกร้องขอ
- จะต้องมีบุคคลผู้รับผิดชอบที่ชัดเจนในทุกกระบวนการที่เกิดขึ้นในขณะที่พยานหลักฐานดิจิทัลอยู่ในความดูแลของบุคคลนั้น
- หน่วยงานและเจ้าหน้าที่ที่ดำเนินการเก็บยึด เข้าถึงข้อมูล บันทึกข้อมูล โอนถ่ายเคลื่อนย้ายพยานหลักฐานดิจิทัล จะต้องรับผิดชอบในการปฏิบัติงานให้สอดคล้องกับหลักการข้างต้น

3) <u>การวิเคราะห์พยานหลักฐานดิจิทัล</u>

พยานหลักฐานแต่ละประเภทของคดีจะมีความแตกต่างกัน วิธีวิเคราะห์จึงแตกต่างกัน มีการใช้เครื่องมือที่แตกต่างกัน ทักษะเจ้าหน้าที่แตกต่างกัน การฝึกอบรมเจ้าหน้าที่พิสูจน์หลักฐานจึงมีความสำคัญ การวิเคราะห์พยานหลักฐานดิจิทัล จึงต้องใช้ผู้เชี่ยวชาญด้านพยานหลักฐานดิจิทัลมาวิเคราะห์ โดยปกติแล้ว จะมีการใช้โปรแกรมคอมพิวเตอร์เฉพาะทาง ไม่ว่าจะเป็นโปรแกรมที่พัฒนาขึ้นโดยเฉพาะ หรือมีผู้พัฒนาสำหรับใช้วิเคราะห์พยานหลักฐานดิจิทัล เช่น โปรแกรมที่ใช้สำหรับตรวจสอบคอมพิวเตอร์และโทรศัพท์มือถือ สำหรับวิเคราะห์พยานหลักฐานดิจิทัลที่นิยมใช้ คือ Encase และ FTK จะเป็นโปรแกรมที่พัฒนาและขายให้กับหน่วยงานที่ทำหน้าที่พิสูจน์หลักฐานทางดิจิทัล โดยเฉพาะ สามารถใช้กู้ข้อมูลที่ถูกลบ ซ่อน ไม่ว่าจะโดยผู้ใช้ หรือโดยระบบ สามารถค้นหาข้อมูลที่ถูกเปลี่ยนแปลง แก้ไข เข้ารหัส และอื่นๆ โดยทั่วไปแล้ว การวิเคราะห์พยานหลักฐานดิจิทัล จะมีการวิเคราะห์ต่างๆ ดังนี้

- Computer forensics เช่น บัญชีผู้ใช้ รอยประทับเวลา รูปภาพ อีเมลที่บันทึกอยู่ในฮาร์ดไดฟ์คอมพิวเตอร์ รวมทั้งบันทึกจากหน่วยความจำ
- Cell Phone forensics เช่น บันทึกที่สร้างขึ้นโดยผู้ให้บริการโทรศัพท์มือถืออย่างข้อมูลการเรียกเก็บเงิน การบันทึกการใช้บริการ ไม่ว่าหมายเลขที่โทรออก โทรเข้า ระยะเวลาการโทร วันเวลาการโทร สถานีเครือข่ายที่โทรศัพท์เครื่องนั้นใช้งาน รายชื่อในโทรศัพท์ ข้อความ รูปภาพ อีเมล ฯลฯ
- GPS Forensics เช่น ตำแหน่งที่ไปเมื่อเร็วๆ นี้ สถานที่ที่ชอบ หยุดที่สถานที่ใดบ้าง นานเท่าใด ฯลฯ
- Social Media Forensics เช่น ข้อมูลเกี่ยวกับกิจกรรมออนไลน์ของกลุ่มเพื่อน การสื่อสาร กระทั่งแนวคิดของบุคคลผู้ต้องสงสัย
- Digital Video and Photo Forensics คือ การตรวจสอบรวมทั้งวิเคราะห์ภาพถ่าย
- Digital Camera Forensics เช่น ภาพถ่าย ข้อมูลเกี่ยวกับภาพ metadata รุ่นของกล้อง วันเวลาบันทึกภาพ
- Game Console forensics เช่น metadata ข้อมูลผู้เล่น บัญชีออนไลน์

4) <u>การนำเสนอผลพิสูจน์พยานหลักฐานดิจิทัล</u>

การนำเสนอผลการตรวจพิสูจน์พยานหลักฐานดิจิทัล เป็นรายงานบันทึกคำให้การผู้เชี่ยวชาญ อธิบายวิธีการตรวจสอบ เครื่องมือที่ใช้ตรวจสอบ ตรวจสอบสิ่งใดบ้าง วิธีเก็บพยานหลักฐาน สิ่งที่ค้นพบ และวิธีการยืนยันความแท้จริงของพยานหลักฐานดิจิทัล พยานหลักฐานดิจิทัลซึ่งพนักงานสอบสวนได้รวบรวมเพื่อพิสูจน์ว่าผู้ต้องหากระทำความผิดตามข้อกล่าวหา จะถูกนำเสนอต่อศาลระหว่างกระบวนการพิจารณาสืบพยาน โดยศาลมีอำนาจใช้ดุลพินิจรับฟังและชั่งน้ำหนักของพยานหลักฐานดิจิทัลตามที่กฎหมายกำหนด การรับฟังพยานหลักฐานดิจิทัลจึงต้องเป็นไปตามหลักการรับฟังพยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาความอาญาอันเป็นบทกฎหมายทั่วไป ซึ่งมาตรา 226 บัญญัติไว้ว่า “พยานวัตถุ พยานเอกสาร หรือพยานบุคคลซึ่งน่าจะพิสูจน์ได้ว่าจำเลยมีผิดหรือบริสุทธิ์ ให้อ้างเป็นพยานหลักฐานได้ แต่ต้องเป็นพยานชนิดที่ไม่ได้เกิดขึ้นจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวงหรือโดยมิชอบประการอื่น และให้สืบตามบทบัญญัติแห่งประมวลกฎหมายนี้ หรือกฎหมายอื่น จึงหมายถึงว่า กรณีที่มีกฎหมายเฉพาะอื่นที่ใช้บังคับหรือบัญญัติหลักเกณฑ์ และวิธีการในการได้มาซึ่งพยานหลักฐานดิจิทัลไว้ การรวบรวมพยานหลักฐานนั้นจะต้องต้องปฏิบัติให้ถูกต้องตามหลักเกณฑ์และวิธีการดังกล่าวนอกเหนือไปจากหลักเกณฑ์ทั่วไปตามประมวลกฎหมายวิธีพิจารณาความอาญาด้วย ไม่เช่นนั้นจะถือว่าเป็นการได้พยานหลักฐานดิจิทัลมาโดยมิชอบ ศาลมีอำนาจไม่รับฟังได้ ดังนั้นทุกขั้นตอนข้างต้นของกระบวนกาตรวจพิสูจน์หลักฐานต่างมีความสำคัญ ที่จะต้องปฏิบัติให้เป็นไปตามมาตรฐาน ให้ชอบด้วยกฎหมาย

ที่ใช้บังคับในแต่ละประเภทคดี จะไม่มีประเด็นในเรื่องของคุณค่าในการพิสูจน์ความผิดของพยานหลักฐานนั้น ทำให้ไม่อาจรับฟังในชั้นพิจารณาหรือทำให้พยานหลักฐานนั้นมีน้ำหนักในการรับฟังได้น้อย

5) บุคลากรภาครัฐที่เกี่ยวข้องกับกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล จะต้องมีการเรียนรู้พัฒนาตนเอง เพื่อเรียนรู้เทคนิคใหม่ๆ ให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยี และปริมาณข้อมูลที่มีจำนวนมากขึ้น เพื่อให้การรวบรวมพยานหลักฐาน และการเก็บรักษา เป็นไปอย่างถูกวิธี และหน่วยงานต้นสังกัด ควรจัดให้มีการฝึกอบรมเพื่อเพิ่มความรู้ความชำนาญด้านกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลอย่างสม่ำเสมอ เพื่อให้บุคลากรสามารถพัฒนา และเรียนรู้เทคนิคใหม่ๆ เพิ่มเติม โดยควรจัดทำเครือข่ายความร่วมมือทางวิชาการ และผลักดันให้มีการจัดตั้งสภาวิชาชีพนิติวิทยาศาสตร์ เพื่อให้มีสามารถมีการจัดการอบรมอย่างเร่งด่วน สม่ำเสมอ ในหัวข้อใหม่ๆ เช่น ในหัวข้อของการตรวจพิสูจน์พยานหลักฐานในสกุลเงินดิจิทัล (Cryptocurrency Forensics), เทคโนโลยีการเข้ารหัสต่างๆ, การตรวจพิสูจน์หลักฐานในส่วนที่เกี่ยวข้องกับ Cloud และโนโลกเสมือน (Virtual World) เป็นต้น
6) มีการจัดการสนับสนุน ทั้งในส่วนของบุคลากรอื่นๆ ที่ปฏิบัติงานร่วมกัน และด้านอุปกรณ์ทางเทคโนโลยีที่ใช้ในการสืบสวน และตรวจพิสูจน์หลักฐานอย่างพอเพียง เพื่อให้สามารถทำงานร่วมกันเป็นทีมได้ แต่ก็มีความเป็นอิสระในการปฏิบัติงาน
7) มีการจัดทำแผนปฏิบัติงานเป็นขั้นตอน ที่ชัดเจน เป็นระบบ เพื่อกำหนดแนวทางในการทำงานอย่างมีประสิทธิภาพ ลดปัญหาที่จะส่งผลกระทบต่อพยานหลักฐานดิจิทัล
8) เพิ่มความร่วมมือ กับนักวิชาการ ภาคเอกชน ผู้เชี่ยวชาญด้านกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล ตลอดจนทำความเข้าใจกับภาคประชาชน ถึงแนวทางการปฏิบัติงานในขั้นตอนต่างๆ เพื่อสร้างความมั่นใจ และคลายปมปัญหา ตลอดจนข้อสงสัยอันจะนำไปสู่อุปสรรคในการปฏิบัติงาน
9) นำเทคโนโลยีใหม่ๆ ไม่ว่าจะเป็นฐานข้อมูลของระบบผู้เชี่ยวชาญ การใช้ปัญญาประดิษฐ์มาช่วยเสริมการทำงานของบุคลากร เพื่อเตรียมรับ กับการเพิ่มขึ้นอย่างรวดเร็วของอาชญากรรมคอมพิวเตอร์ที่เกิดขึ้น ลดภาระของบุคลากร และเพิ่มประสิทธิภาพประสิทธิผล ในการปฏิบัติงาน
10) มีการประชาสัมพันธ์ขั้นตอน และห้วงเวลาในการทำงานในขั้นตอนต่างๆ ของผู้ปฏิบัติงาน กับภาคประชาชน ตลอดจนสื่อต่างๆ อย่างสม่ำเสมอ เพื่อให้ไม่เกิดความเข้าใจผิด หรือ หลงเชื่อตามข่าวลือต่างๆ อันจะนำไปสู่ปัญหาและอุปสรรคในการปฏิบัติงาน ตลอดจนเกิดการไม่ร่วมมือ จากภาคประชาชน อันเนื่องมาจากได้รับข้อมูลที่ไม่ถูกต้องตามความเป็นจริง

การตรวจพิสูจน์พยานหลักฐานดิจิทัล ทุกฝ่ายที่เกี่ยวข้องควรมีความรู้และความเข้าใจถึงหลักการตรวจพิสูจน์พยานหลักฐานดิจิทัล ตั้งแต่กระบวนการรวบรวมพยานหลักฐาน การเก็บรักษาพยานหลักฐาน การวิเคราะห์และการนำเสนอที่ต้องกระทำโดยผู้เชี่ยวชาญ และเป็นไปตามมาตรฐานสากล มิเช่นนั้นอาจส่งผลให้พยานหลักฐานดิจิทัลขาดความน่าเชื่อถือ และไม่สามารถรับฟัง

เป็นพยานหลักฐานในชั้นศาลได้ ปัจจุบันแม้ไม่มีกฎหมายเฉพาะ เกี่ยวกับการตรวจพิสูจน์พยานหลักฐานดิจิทัล แต่ก็มีการจัดทำมาตรฐานการจัดการอุปกรณ์ดิจิทัล ในงานตรวจพิสูจน์พยานหลักฐานดิจิทัล โดยศูนย์ดิจิทัลฟอเรนสิกส์ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) เพื่อเป็นแนวทางการตรวจพิสูจน์พยานหลักฐานดิจิทัลที่มีมาตรฐานการปฏิบัติการที่ชัดเจน

ในการต่อสู้คดีที่มีพยานหลักฐานดิจิทัลเข้ามาเกี่ยวข้อง หลายกรณีพบว่า การดำเนินคดีเป็นการสร้างภาระให้ผู้ถูกกล่าวหาในการต่อสู้คดี ดังนั้น แนวทางในการสร้างความเท่าเทียมในการใช้พยานหลักฐานดิจิทัล อย่างหนึ่งคือในทุกขั้นตอนของกระบวนการยุติธรรม ในการตรวจพิสูจน์พยานหลักฐานดิจิทัล โดยเฉพาะอย่างยิ่งขั้นตอนการสืบสวน การรวบรวมพยานหลักฐานดิจิทัล รวมถึงการรับฟังพยานหลักฐานดิจิทัล ควรมีแนวทางมาตรฐานและขั้นตอนการปฏิบัติที่ชัดเจน สอดคล้องกับมาตรฐานสากล และเปิดโอกาสให้หน่วยงานอื่นๆ ที่มีศักยภาพและความน่าเชื่อถือเข้ามาร่วมในการตรวจพิสูจน์พยานหลักฐานดิจิทัล มีกฎหมายหรือหลักประกันที่เป็นมาตรฐานในการตรวจพิสูจน์พยานหลักฐาน ซึ่งจะนำไปสู่การสร้างความเป็นธรรมให้กับทุกฝ่ายในกระบวนการยุติธรรมทางอาญา

บทที่ 5
สรุปผลการศึกษาและข้อเสนอแนะ

การตรวจพิสูจน์พยานหลักฐานดิจิทัลในประทศไทยยังคงเป็นเรื่องใหม่ เมื่อเทียบกับการตรวจพิสูจน์พยานหลักฐานทางนิติวิทยาศาสตร์ แต่แนวโน้มและความสำคัญกำลังเพิ่มมากขึ้นเรื่อยๆ โดยเฉพาะในโลกยุคปัจจุบัน ที่เครือข่ายอินเทอร์เน็ตและสังคมดิจิทัล เข้ามามีบทบาทในวัฒนธรรมการดำรงชีวิตของคนไทยมากขึ้น เครือข่ายสังคม และชุมชนออนไลน์ต่างๆ เข้ามาเป็นส่วนหนึ่งในการใช้ชีวิต ควบคู่ไปกับการเติบโตของตลาดอุปกรณ์พกพาอัจฉริยะ ที่เป็นมากกว่าแค่อุปกรณ์สื่อสาร และความก้าวหน้าทางเทคโนโลยี รวมถึงการพลิกผันทางดิจิทัล ที่สร้างปริมาณข้อมูลจำนวนมหาศาลในทุกวินาทีส่งผลให้อาชญากรรมคอมพิวเตอร์ในประเทศไทยมีแนวโน้มเพิ่มสูงขึ้นอย่างรวดเร็วแบบก้าวกระโดด เมื่อมองย้อนกลับไปดูในช่วงหลายปีที่ผ่านมา ประชาชนทั่วไป แม้มีความคุ้นเคยกับการใช้งานเครือข่ายอินเทอร์เน็ต แต่ยังขาดความรู้ความเข้าใจในปัญหาและการป้องกันอาชญากรรมคอมพิวเตอร์ เมื่อมีการออกกฎหมายที่เกี่ยวข้องกับการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งมีบทลงโทษสำหรับผู้กระทำผิด แต่สถิติการเกิดคดีก็ยังคงสูงอย่างต่อเนื่อง มีประเด็นใหม่ๆเกิดขึ้นในสังคม เกิดความสงสัย ข้อโต้แย้งมากมายว่าผู้ที่เกี่ยวข้องในกระบวนการยุติธรรม ใช้บรรทัดฐานใดก่อนจะพิจารณารับเป็นคดี การดำเนินการตามขั้นตอนต่างๆ ในการจับกุม ตลอดจนการใช้พยานหลักฐานและการตรวจพิสูจน์พยานหลักฐาน มีกระบวนการอย่างไร มีความเที่ยงธรรม และชอบธรรมหรือไม่

5.1 สรุปผลการศึกษาวิจัย

กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล มีบทบาทสำคัญอย่างมากจากสังคมดิจิทัลที่เติบโตขึ้น และแนวโน้มการเพิ่มขึ้นของอาชญากรรมคอมพิวเตอร์ ตลอดจนประเด็นความเคลือบแคลงทางสังคมต่างๆ ในกฎหมายที่เกี่ยวข้องกับการกระทำผิดเกี่ยวกับคอมพิวเตอร์ งานวิจัยชิ้นนี้จัดทำขึ้นเพื่อศึกษาวิเคราะห์เสนอแนะเชิงนโยบายสำหรับกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล โดยมีวัตถุประสงค์ ดังนี้

1) เพื่อศึกษากระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลในประเทศไทย จากชั้นสอบสวนถึงชั้นพิจารณาคดี และกฎหมายที่เกี่ยวข้อง
2) เพื่อศึกษาวิเคราะห์ ปัจจัยที่เกี่ยวข้องกับปัญหาและอุปสรรคของกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลในประเทศไทย
3) เพื่อศึกษาวิเคราะห์ เสนอแนะเชิงนโยบายและข้อเสนอในการปรับปรุงกฎหมายและการบังคับใช้ เพื่อยกระดับกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลและกระบวนการยุติธรรมทางอาญาที่เกี่ยวข้อง

โดยใช้กระบวนการวิจัยเชิงคุณภาพ (Qualitative research) เป็นระเบียบวิธีวิจัย (Methodology) ในการศึกษานี้ใช้การสัมภาษณ์แบบเจาะลึก (in-depth interview) มีการออกแบบคำถามที่สามารถนำไปใช้สัมภาษณ์แบบกึ่งโครงสร้าง ซึ่งเป็นลักษณะของการสัมภาษณ์โดยใช้คำถามปลายเปิด มีความยืดหยุ่นและเปิดกว้างให้ผู้ถูกสัมภาษณ์ ผู้วิจัยกำหนดประชากรกลุ่มเป้าหมาย คือ บุคลากรภาครัฐในกระบวนการยุติธรรม รวมถึงภาคเอกชน ตลอดจนนักวิชาการที่เกี่ยวข้องกับ

กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล เพื่อให้ทราบถึงกระบวนการที่เกี่ยวข้อง ตลอดจนปัญหาและอุปสรรคเพื่อนำไปสู่การวิเคราะห์เพื่อจัดทำข้อเสนอแนะเชิงนโยบายและปฏิบัติ โดยดำเนินการคัดเลือกกลุ่มตัวอย่างทำโดยวิธีการสุ่มแบบเจาะจง (Purposive sampling) เนื่องจากมีข้อจำกัดเรื่องของระยะเวลาการศึกษาวิจัย จึงใช้วิธีการเก็บข้อมูลจากผู้ให้ข้อมูลสำคัญ (Key Informants) กลุ่มตัวอย่างที่ใช้ในการศึกษาครั้งนี้ ได้แก่ บุคลากรภาครัฐ เจ้าหน้าที่ตำรวจที่มีประสบการณ์ทางด้านอาชญากรรมคอมพิวเตอร์ ในส่วนของกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล อัยการ ผู้พิพากษา ที่มีความเชี่ยวชาญในคดีอาชญากรรมคอมพิวเตอร์ ภาคเอกชน นักวิชาการที่มีทักษะด้านกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล และภาคประชาชนที่ได้รับผลกระทบจากอาชญากรรมคอมพิวเตอร์ รวม 31 คน

จากการวิจัยพบว่า

5.1.1 กระบวนการในการตรวจพิสูจน์พยานหลักฐานดิจิทัลประกอบด้วย 4 ขั้นตอนคือ

1) <u>การรวบรวมพยานหลักฐานดิจิทัล</u>

สิ่งสำคัญที่สุดในส่วนนี้ คือ ความสมบูรณ์ของพยานหลักฐาน และการรวบรวมพยานหลักฐานทั้งหมดให้เป็นไปอย่างสมบูรณ์ขณะเกิดเหตุโดยไม่ถูกเปลี่ยนแปลงแก้ไขใดๆ โดยมีอำนาจรวบรวมพยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 132 อันเป็นบทกฎหมายทั่วไป และมีกฎหมายบัญญัติเอาไว้โดยเฉพาะในเรื่องของอำนาจของพนักงานสอบสวนหรือเจ้าพนักงานผู้มีอำนาจรวบรวมพยานหลักฐาน และหลักเกณฑ์วิธีการในการรวบรวมและจัดเก็บพยานหลักฐาน พนักงานสอบสวนหรือเจ้าพนักงานเหล่านั้นก็จะต้องปฏิบัติให้เป็นไปตามบทบัญญัติกฎหมายเฉพาะดังกล่าวนั้นด้วย เช่น ที่กำหนดไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ มาตรา 18, 26 ได้ให้อำนาจในการเรียกผู้ถูกกล่าวหามาให้ถ้อยคำ เรียกข้อมูลการจราจรทางคอมพิวเตอร์ สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บทำสำเนา หรือส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าว รวมถึงตรวจสอบการเข้าถึง และถอดรหัสลับของข้อมูลคอมพิวเตอร์ หรือสั่งให้บุคคลที่เกี่ยวข้อง ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว รวมทั้งยึดหรืออายัดระบบคอมพิวเตอร์เฉพาะเท่าที่จำเป็น การรวบรวมพยานหลักฐานดิจิทัล จะมีหน่วยงานเฉพาะเข้ามาทำหน้าที่เก็บรวบรวมพยานหลักฐาน เช่น กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) และสถาบันนิติวิทยาศาสตร์ ซึ่งมีเจ้าหน้าที่ที่มีความรู้ความเชี่ยวชาญทางด้านคอมพิวเตอร์และเทคโนโลยีโดยเฉพาะ และเป็นเจ้าหน้าที่ที่ได้รับการแต่งตั้งตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (แก้ไขเพิ่มเติม พ.ศ. 2560) มีอำนาจในการติดตามและรวบรวมพยานหลักฐานดิจิทัล เพื่อนำไปใช้เป็นหลักฐานในชั้นกระบวนพิจารณาของศาล

2) <u>การเก็บรักษาพยานหลักฐานดิจิทัล</u>

การเก็บรักษาจะต้องเก็บรักษาไว้ในสภาพที่รับฟังได้ในชั้นศาล เป็นไปตามกระบวนการสร้างห่วงโซ่คุ้มครองพยานหลักฐานในหลักสากล ต้องมีมาตรฐานการเก็บรักษาพยานหลักฐานดิจิทัลที่เป็นที่ยอมรับของทุกฝ่ายมีบันทึกขั้นตอนการคุ้มครองพยานหลักฐานและวิธีการเก็บรักษา เพื่อให้มั่นใจได้ว่าเป็นข้อมูลที่ไม่ได้ถูกแก้ไขเปลี่ยนแปลงนับจากที่ได้รับมาจากที่เกิดเหตุ มาตรฐานในการจัดเก็บและจัดการพยานหลักฐานดิจิทัลของเจ้าพนักงานที่เกี่ยวข้อง อาจทำให้เกิดประเด็นข้อโต้แย้งในการรับฟังพยานหลักฐานได้ เนื่องจากพยานหลักฐานดิจิทัลในรูปของข้อมูลคอมพิวเตอร์หรือข้อมูลอิเล็กทรอนิกส์ มีความเสี่ยงต่อการถูกเปลี่ยนแปลงแก้ไข สูญหาย เสียหายโดยง่าย โดยเฉพาะอย่างยิ่งเมื่อต้องมีการส่งผ่านข้อมูลคอมพิวเตอร์หรือข้อมูลอิเล็กทรอนิกส์ระหว่างเจ้าพนักงานที่เกี่ยวข้องหลายทอด ในส่วนนี้ปัจจุบันสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. ได้เผยแพร่เอกสาร “ข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐาน” เพื่อเป็นแนวทางเบื้องต้นให้กับเจ้าหน้าที่ที่เกี่ยวข้องกับการจัดเก็บ รวบรวม และตรวจพิสูจน์พยานหลักฐานดิจิทัล ให้ปฏิบัติงานในสถานที่เกิดเหตุและในห้องปฏิบัติการให้สอดคล้องกับมาตรฐานสากล โดยสพธอ. เน้นในเรื่องการให้ความสำคัญต่อการบันทึกแบบฟอร์มที่เรียกว่า “Chain of Custody” หรือห่วงโซ่คุ้มครองพยานหลักฐาน คือ กระบวนการระบุสายความรับผิดชอบการเก็บรักษาพยานหลักฐาน เริ่มตั้งแต่เมื่อพยานหลักฐานถูกเก็บรวบรวม เพื่อสร้างความต่อเนื่องของการครอบครองพยานหลักฐาน โดยข้อมูลที่เจ้าหน้าที่ผู้ปฏิบัติงานในแต่ละสายงาน จำเป็นต้องระบุรวมถึงข้อมูลติดต่อและลงลายมือชื่อของผู้ส่งมอบพยานหลักฐาน, เหตุผลในการับ-ส่งมอบพยานหลักฐาน, วิธีการส่งมอบพยานหลักฐาน เช่น ส่งมอบโดยเจ้าหน้าที่ที่เกี่ยวข้องหรือส่งมอบโดยพนักงานส่งของ และสถานที่จัดเก็บพยานหลักฐาน เป็นต้น นอกจากนี้ International Organization on Computer Evidence หรือ IOCE ซึ่งเป็นหน่วยงานสากลที่ดูแลเกี่ยวกับการปฏิบัติต่อพยานหลักฐานดิจิทัล ได้กำหนดหลักการสำคัญ ในการเข้าค้นและยึดอุปกรณ์ อิเล็กทรอนิกส์ไว้ 6 ประการ คือ

- เมื่อใดก็ตามที่ต้องดำเนินการกับพยานหลักฐานดิจิทัล จะต้องมีการดำเนินการตามหลักปฏิบัติทั่วไปทางนิติคอมพิวเตอร์ และต้องดำเนินการตามขั้นตอนของนิติคอมพิวเตอร์
- ในขณะปฏิบัติการเก็บยึดพยานหลักฐานดิจิทัล การดำเนินการทุกอย่างจะต้องไม่ก่อให้เกิดการเปลี่ยนแปลงต่อพยานหลักฐานนั้น
- หากมีความจำเป็นที่จะต้องเข้าถึงข้อมูลในพยานหลักฐานต้นฉบับ เจ้าหน้าที่ผู้ปฏิบัติจะต้องได้รับการอบรมมาเพื่อดำเนินการเป็นการเฉพาะ
- จะต้องมีการจดบันทึกรายละเอียดทุกขั้นตอน ทุกการกระทำที่เกี่ยวข้องกับการเก็บยึด การเข้าถึงข้อมูล การเคลื่อนย้าย และต้องมีการเก็บรักษาบันทึกนั้นไว้ และสามารถนำมาแสดงได้เมื่อถูกร้องขอ

- จะต้องมีบุคคลผู้รับผิดชอบที่ชัดเจนในทุกกระบวนการที่เกิดขึ้นในขณะที่พยานหลักฐานดิจิทัลอยู่ในความดูแลของบุคคลนั้น
- หน่วยงานและเจ้าหน้าที่ที่ดำเนินการเก็บยึด เข้าถึงข้อมูล บันทึกข้อมูล โอนถ่าย เคลื่อนย้ายพยานหลักฐานดิจิทัล จะต้องรับผิดชอบในการปฏิบัติงานให้สอดคล้องกับหลักการข้างต้น

3) <u>การวิเคราะห์พยานหลักฐานดิจิทัล</u>

พยานหลักฐานแต่ละประเภทของคดีจะมีความแตกต่างกัน วิธีวิเคราะห์จึงแตกต่างกัน มีการใช้เครื่องมือที่แตกต่างกัน ทักษะเจ้าหน้าที่แตกต่างกัน การฝึกอบรมเจ้าหน้าที่พิสูจน์หลักฐานจึงมีความสำคัญ การวิเคราะห์พยานหลักฐานดิจิทัล จึงต้องใช้ผู้เชี่ยวชาญด้านพยานหลักฐานดิจิทัลมาวิเคราะห์ โดยปกติแล้ว จะมีการใช้โปรแกรมคอมพิวเตอร์เฉพาะทาง ไม่ว่าจะเป็นโปรแกรมที่พัฒนาขึ้นโดยเฉพาะ หรือมีผู้พัฒนาสำหรับใช้วิเคราะห์พยานหลักฐานดิจิทัล เช่น โปรแกรมที่ใช้สำหรับตรวจสอบคอมพิวเตอร์และโทรศัพท์มือถือ สำหรับวิเคราะห์พยานหลักฐานดิจิทัลที่นิยมใช้ คือ Encase และ FTK จะเป็นโปรแกรมที่พัฒนาและขายให้กับหน่วยงานที่ทำหน้าที่พิสูจน์หลักฐานทางดิจิทัลโดยเฉพาะ สามารถใช้กู้ข้อมูลที่ถูกลบ ซ่อน ไม่ว่าจะโดยผู้ใช้ หรือโดยระบบ สามารถค้นหาข้อมูลที่ถูกเปลี่ยนแปลง แก้ไข เข้ารหัส และอื่นๆ โดยทั่วไปแล้ว การวิเคราะห์พยานหลักฐานดิจิทัล จะมีการวิเคราะห์ต่างๆ ในหลายรูปแบบ เช่น บัญชีผู้ใช้ รอยประทับเวลา รูปภาพ อีเมลที่บันทึกอยู่ในฮาร์ดไดรฟ์คอมพิวเตอร์ รวมทั้งบันทึกจากหน่วยความจำ บันทึกที่สร้างขึ้นโดยผู้ให้บริการโทรศัพท์มือถือข้อมูลการเรียกเก็บเงิน การบันทึกการใช้บริการ ไม่ว่าหมายเลขที่โทรออก โทรเข้า ระยะเวลาการโทร วันเวลาการโทร สถานีเครือข่ายที่โทรศัพท์เครื่องนั้นใช้งาน รายชื่อในโทรศัพท์ ข้อความ รูปภาพ อีเมล ฯลฯ ตำแหน่งที่ไปเมื่อเร็วๆ นี้ สถานที่ที่ชอบ หยุดที่สถานที่ใดบ้าง นานเท่าใด ข้อมูลเกี่ยวกับกิจกรรมออนไลน์ของกลุ่มเพื่อน การสื่อสาร กระทั่งแนวคิดของบุคคลผู้ต้องสงสัย การตรวจสอบรวมทั้งวิเคราะห์ภาพถ่าย รุ่นของกล้อง วันเวลาบันทึกภาพ ข้อมูลผู้เล่น บัญชีออนไลน์

4) <u>การนำเสนอผลพิสูจน์พยานหลักฐานดิจิทัล</u>

การนำเสนอผลการตรวจพิสูจน์พยานหลักฐานดิจิทัล เป็นรายงานบันทึกคำให้การผู้เชี่ยวชาญ อธิบายวิธีการตรวจสอบ เครื่องมือที่ใช้ตรวจสอบ ตรวจสอบสิ่งใดบ้าง วิธีเก็บพยานหลักฐาน สิ่งที่ค้นพบ และวิธีการยืนยันความแท้จริงของพยานหลักฐานดิจิทัล พยานหลักฐานดิจิทัลซึ่งพนักงานสอบสวนได้รวบรวม เพื่อพิสูจน์ว่าผู้ต้องหากระทำความผิดตามข้อกล่าวหา จะถูกนำเสนอต่อศาลระหว่างกระบวนการพิจารณาสืบพยาน โดยศาลมีอำนาจใช้ดุลพินิจรับฟังและชั่งน้ำหนักของพยานหลักฐานดิจิทัลตามที่กฎหมายกำหนด ปัจจุบันยังไม่มีบทบัญญัติเกี่ยวกับการรับฟังพยานหลักฐานดิจิทัลในคดีอาญาเป็นการเฉพาะเจาะจง การรับฟังพยานหลักฐานดิจิทัลจึงต้องเป็นไปตาม

> หลักการรับฟังพยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาความอาญาอันเป็นบทกฎหมายทั่วไป ซึ่งมาตรา 226 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา บัญญัติไว้ว่า “พยานวัตถุ พยานเอกสาร หรือพยานบุคคลซึ่งน่าจะพิสูจน์ได้ว่าจำเลยมีผิดหรือบริสุทธิ์ ให้อ้างเป็นพยานหลักฐานได้ แต่ต้องเป็นพยานชนิดที่ไม่ได้เกิดขึ้นจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวงหรือโดยมิชอบประการอื่น และให้สืบตามบทบัญญัติแห่งประมวลกฎหมายนี้ หรือกฎหมายอื่นอันว่าด้วยการสืบพยาน ไม่เช่นนั้นจะถือว่าเป็นการได้พยานหลักฐานดิจิทัลมาโดยมิชอบ ศาลมีอำนาจไม่รับฟังได้ ดังนั้นทุกขั้นตอนของกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลจึงเป็นเรื่องที่สำคัญมาก เนื่องจากแม้ว่าในชั้นสอบสวน เจ้าพนักงานได้รวบรวมพยานหลักฐานที่เห็นว่าเพียงพอต่อการระบุตัวผู้กระทำความผิดและพิสูจน์ความผิดที่บุคคลนั้นกระทำแล้ว หากกระบวนการอื่นมีข้อโต้แย้งว่าเป็นไปโดยชอบด้วยกฎหมายหรือไม่ จะมีประเด็นในเรื่องของคุณค่าในการพิสูจน์ความผิดของพยานหลักฐานนั้น หรือไม่อาจรับฟังในชั้นพิจารณาหรือทำให้พยานหลักฐานนั้นมีน้ำ หนักในการรับฟังได้น้อย

ในการตรวจพิสูจน์พยานหลักฐานดิจิทัล มีปัจจัยสำคัญหลายอย่างที่ควรต้องคำนึงถึง และระมัดระวังเพื่อไม่ให้เกิดความผิดพลาด โดยเฉพาะอย่างยิ่งการเลือกเครื่องมือที่เหมาะสมกับงาน การทำความเข้าใจถึงวิธีการใช้เครื่องมือที่ถูกต้อง รวมถึงการจัดการอุปกรณ์ดิจิทัลในการตรวจพิสูจน์พยานหลักฐาน โดยมีมาตรฐานสากล ที่เป็นแนวปฏิบัติในการตรวจพิสูจน์พยานหลักฐาน เช่น ACPO Good Practice Guide for Digital Evidence; ISO/IEC 27037 Information technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence และ SWGDE Best Practices for Computer Forensics V3-1 และยังรวมถึงมาตรฐานการจัดการอุปกรณ์ดิจิทัลในการตรวจพิสูจน์พยานหลักฐานในการปฏิบัติงานทั้งใน สถานที่เกิดเหตุและในห้องปฏิบัติการ ตลอดจนการจัดการข้อมูลคอมพิวเตอร์ สื่อบันทึกข้อมูลดิจิทัล และเครื่องมือสื่อสารอื่นๆ ด้วย

หลักการปฏิบัติงานเกี่ยวกับพยานหลักฐานดิจิทัล ที่สอดคล้องกับมาตรฐานสากล มีหลักการที่สำคัญดังนี้

(1) ดำเนินการโดยผู้ที่ผ่านการฝึกอบรมทางเทคนิคด้านการตรวจพิสูจน์พยานหลักฐานดิจิทัล
(2) รักษาสภาพพยานหลักฐานไม่ให้ถูกเปลี่ยนแปลง หรือถูกเปลี่ยนแปลงน้อยที่สุด โดยผู้ปฏิบัติงานต้องสามารถอธิบาย และบันทึกเป็นลายลักษณ์อักษรแสดงถึงขั้นตอนการคุ้มครองพยานหลักฐานโดยละเอียด
(3) การคุ้มครองพยานหลักฐาน ต้องบันทึกข้อมูลในแบบฟอร์ม โดยมีรายละเอียด ได้แก่ ข้อมูลการติดต่อและลายมือชื่อของผู้ส่งมอบพยานหลักฐาน ข้อมูลการติดต่อและลายมือชื่อของผู้รับมอบพยานหลักฐาน วัน เวลาในการรับ-ส่งพยานหลักฐาน รายละเอียดในการรับ-ส่งพยานหลักฐาน วิธีการส่งมอบพยานหลักฐาน เช่น ส่งมอบโดยเจ้าหน้าที่ หรือส่งมอบโดยพนักงานส่งของ และสถานที่จัดเก็บพยานหลักฐานดิจิทัล เป็นต้น

(4) มีการบันทึกขั้นตอนการปฏิบัติงาน การเก็บรวบรวมและการวิเคราะห์พยานหลักฐานโดยละเอียด เพื่อให้ผู้ตรวจพิสูจน์อื่นสามารถเข้าใจได้ และหากทำซ้ำด้วยวิธีการเดิมและเครื่องมือที่มีลักษณะเดียวกัน จะต้องได้ผลลัพธ์เหมือนกัน

(5) บุคคลที่สามารถเข้าถึงพยานหลักฐาน ต้องเป็นผู้ที่ได้รับมอบหมาย หรือมีหน้าที่รับผิดชอบโดยตรงเท่านั้น และผู้ปฏิบัติงานต้องตระหนักถึงการดำเนินงานตามกฎหมายเกี่ยวข้องกับพยานหลักฐาน

(6) เครื่องมือและอุปกรณ์ต้องเป็นไปตามมาตรฐาน ตามหลักการตรวจพิสูจน์พยานหลักฐาน เช่น อยู่ในสภาพพร้อมใช้งานและเหมาะสมกับการตรวจพิสูจน์พยานหลักฐานแต่ละประเภท มีมาตรการในการป้องกันการเปลี่ยนแปลง และปนเปื้อนของพยานหลักฐาน ได้รับการตรวจสอบความถูกต้องแม่นยำของเครื่องมือก่อนใช้งานสม่ำเสมอ รวมถึงมีคู่มือการใช้งานหรือเอกสารอธิบายการใช้งานเพื่อใช้อ้างอิง

หลักการตรวจพิสูจน์พยานหลักฐานดิจิทัลดังกล่าว มีความสำคัญอย่างมาก เพราะพยานหลักฐานทางดิจิทัลนั้นมีความอ่อนไหวมาก การปฏิบัติตามขั้นตอนที่ถูกต้องเป็นสิ่งสำคัญในการพิสูจน์ความถูกต้องแท้จริง(Authentication) ของพยานหลักฐานดิจิทัล

อย่างไรก็ตาม ในการตรวจพิสูจน์พยานหลักฐานดิจิทัลก็มีข้อจำกัดหลายประการ เช่น ยังต้องกระทำโดยผู้เชี่ยวชาญด้านการตรวจพิสูจน์พยานหลักฐานดิจิทัลเท่านั้น เนื่องจากการจัดการกับพยานหลักฐานจะต้องอาศัยความรู้ความเชี่ยวชาญ ในการจัดการกับข้อมูลที่ได้ และการทำงานที่เกี่ยวข้องในการรวบรวมและวิเคราะห์พยานหลักฐานนั้น ผู้เชี่ยวชาญจะต้องคำนึงถึงห่วงโซ่ของการคุ้มครองพยานหลักฐานเป็นสำคัญ

หลักการชั่งน้ำหนักพยาน และการรับฟังพยานหลักฐานดิจิทัล

จากการที่พยานหลักฐานดิจิทัลมีลักษณะเฉพาะ แม้จะไม่เป็นข้อที่จะไม่ถูกรับฟังในชั้นศาลเพียงเพราะเป็นพยานหลักฐานดิจิทัล แต่ศาลจะใช้ดุลยพินิจ โดยอาศัยหลักการดังนี้

1) <u>หลักการชั่งน้ำหนักพยานหลักฐานทั่วไป</u>

การชั่งน้ำหนักพยานหลักฐาน หมายถึง การที่ศาลจะนำพยานหลักฐานที่คู่ความนำสืบและเห็นว่าสามารถนำมารับฟังเป็นพยานหลักฐานได้ในชั้นศาล มาวินิจฉัยปัญหา ข้อเท็จจริงในประเด็นที่พิพาทกันให้เป็นที่ยุติโดยอาศัยพยานหลักฐาน

ในคดีอาญา อำนาจในการวินิจฉัยน้ำหนักของพยานหลักฐาน ศาลสามารถใช้ดุลยพินิจ ชั่งน้ำหนักพยานทั้งหมด และจะไม่พิพากษาลงโทษจำเลยจนกว่าจะแน่ใจได้ว่ามีการกระทำความผิดจริงและจำเลยเป็นผู้กระทำความผิดนั้น โจทก์จะต้องพิสูจน์ให้ศาลเห็นโดยปราศจากเหตุอันควรสงสัย ว่าจำเลยเป็นผู้กระทำความผิด ถ้ามีเหตุอันควรสงสัยอย่างใดอย่างหนึ่ง ว่าจำเลยไม่ใช่ผู้ที่กระทำความผิดให้ยกประโยชน์แห่งความ สงสัยนั้นแก่จำเลย การวินิจฉัยชี้ขาดข้อเท็จจริงแห่งคดีของศาล จะใช้ดุลพินิจชั่งน้ำหนักพยานหลักฐานทั้งหมดในสำนวนว่าควรรับฟังได้หรือไม่ เพียงไร และไม่มีกฎหมายบทใดบัญญัติห้ามมิให้ศาลรับฟังคำให้การชั้นสอบสวนของพยานเป็นข้อประกอบการพิจารณาของศาล ส่วนจะรับฟังได้หรือไม่ เพียงใดนั้นแล้วแต่เหตุผลของแต่ละเรื่องไป

2) <u>หลักการชั่งน้ำหนักพยานหลักฐานดิจิทัล</u>

การรับฟังพยานหลักฐานดิจิทัลในคดีอาญามีหลักเกณฑ์ 3 ประการที่ศาลใช้ในการพิจารณาว่าสามารถยืนยันความถูกต้องแท้จริง (Authentication) ได้อย่างเหมาะสมหรือไม่ ซึ่งพยานหลักฐานดิจิทัลที่ศาลจะรับฟังและพิจารณาประกอบด้วย

1. เนื้อหาของเอกสารไม่ถูกเปลี่ยนแปลง
2. ข้อมูลในเอกสารเป็นไปตามเจตนาแท้จริงของผู้สร้างเอกสารนั้น ไม่ว่าผู้สร้างเอกสารจะเป็นมนุษย์ หรือคอมพิวเตอร์
3. ข้อมูลพิเศษในเอกสาร อันได้แก่ วัน เดือน ปีที่ถูกสร้าง ถูกต้อง หลักในการพิจารณาว่าพยานหลักฐานดิจิทัลมีความน่าเชื่อถือ สามารถรับฟังในชั้นศาลได้หรือไม่นั้น เป็นดุลยพินิจของศาลในการชั่งน้ำหนักพยานหลักฐาน โดยพิจารณาถึงความน่าเชื่อถือตามที่กำหนดไว้ในพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาตรา 11 วรรคสอง แก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ.2551 มาตรา 619 ซึ่งให้พิจารณาความน่าเชื่อถือจากลักษณะหรือ วิธีการที่ใช้สร้าง เก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์ ลักษณะหรือวิธีการเก็บรักษา ความ ครบถ้วน และไม่มีการเปลี่ยนแปลงของข้อความ ลักษณะหรือวิธีการที่ใช้ในการระบุหรือแสดงตัวผู้ส่งข้อมูล รวมทั้งพฤติการณ์ที่เกี่ยวข้องทั้งหมด

อย่างไรก็ตาม การชั่งน้ำหนัก และการรับฟังพยานหลักฐานดิจิทัลยังมีข้อจำกัด เนื่องจากพยานหลักฐานดิจิทัลง่ายต่อการถูกแก้ไขเปลี่ยนแปลง ส่วนใหญ่เป็นพยานหลักฐานที่เกิดจากการกระทำของมนุษย์ และเป็นการกระทำโดยฝ่ายใดฝ่ายหนึ่ง เป็นการแก้ไข เปลี่ยนแปลงหรือสร้างพยานหลักฐานดิจิทัลเท็จขึ้น ทำให้พยานผู้เชี่ยวชาญด้านการตรวจพิสูจน์พยานหลักฐานดิจิทัลจึงมีความสำคัญในการอธิบายให้ศาลเข้าใจลักษณะเฉพาะและวิธีการเข้าถึง การรวบรวมพยานหลักฐานว่าถูกต้องตามหลักการตรวจพิสูจน์พยานหลักฐานดิจิทัลหรือไม่ ประกอบกับผู้พิพากษาจะต้องมีความรู้พื้นฐานในการตรวจพิสูจน์พยานหลักฐานดิจิทัล สามารถพิจารณาถึงลักษณะการสืบสวนหาความเชื่อมโยงของข้อมูล การเก็บรักษา การตรวจสอบ และ การนำเสนอพยานหลักฐานประกอบกับพยานแวดล้อมอื่นๆ ในคดีด้วย กฎหมายที่เกี่ยวกับพยานหลักฐานดิจิทัล ก็ควรต้องมีบทบัญญัติไว้โดยเฉพาะ โดยกำหนดวิธีการ และกระบวนการการตรวจพิสูจน์พยานหลักฐานดิจิทัลและหลักการชั่งน้ำหนัก รับฟังพยานหลักฐานดิจิทัล เนื่องจากพยานหลักฐานดิจิทัลแตกต่างจากพยานหลักฐานทั่วไป

การตรวจพิสูจน์พยานหลักฐานดิจิทัล หากมีกระบวนการเก็บรวบรวมพยานหลักฐานที่ไม่เป็นไปตามรูปแบบมาตรฐานสากล จะส่งผลให้พยานหลักฐานดิจิทัลได้รับความเสียหาย สูญหาย หรือถูกปนเปื้อน รวมถึงการถูกแก้ไขเปลี่ยนแปลง และถ้ากระบวนการการตรวจพิสูจน์พยานหลักฐานดิจิทัลที่ไม่เป็นไปตามมาตรฐานเกิดขึ้นเรื่อยๆ ก็จะทำให้การตรวจพิสูจน์พยานหลักฐานดิจิทัลกลายเป็นการเก็บรวบรวมพยานหลักฐานตามหลักข้อยกเว้นที่ไม่เป็นไปตามรูปแบบ

5.1.2 กฎหมายที่เกี่ยวข้องกับกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล

5.1.2.1 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ฉบับที่ 4 พ.ศ. 2562

มีมาตราที่เกี่ยวข้อง คือ มาตรา 7 ที่ห้ามมิให้ปฏิเสธความมีผลผูกพันและการบังคับใช้ทางกฎหมายของข้อความใด เพียงเพราะเหตุที่ข้อความนั้นอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ มาตรา 10 ในกรณีที่กฎหมายกำหนดให้นำเสนอหรือเก็บรักษาข้อความใดในสภาพที่เป็นมาแต่เดิมอย่างเอกสารต้นฉบับ ถ้าได้นำเสนอหรือเก็บรักษาในรูปข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์ดังต่อไปนี้ ให้ถือว่าได้มีการนำเสนอหรือเก็บรักษาเป็นเอกสารต้นฉบับตามกฎหมายแล้ว มาตรา 11 ห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐาน ในกระบวนการพิจารณาตามกฎหมายเพียงเพราะเหตุว่าเป็นข้อมูลอิเล็กทรอนิกส์ ในการชั่งน้ำหนักพยานหลักฐานว่าข้อมูลอิเล็กทรอนิกส์จะเชื่อถือได้หรือไม่เพียงใดนั้น ให้พิเคราะห์ถึงความน่าเชื่อถือของลักษณะหรือวิธีการที่ใช้สร้าง เก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์ ลักษณะหรือวิธีการรักษา ความครบถ้วน และไม่มีการเปลี่ยนแปลงของ ข้อความ ลักษณะหรือวิธีการที่ใช้ในการระบุหรือแสดงตัวผู้ส่งข้อมูล รวมทั้งพฤติการณ์ที่เกี่ยวข้องทั้งปวง และ มาตรา 25 ธุรกรรมทางอิเล็กทรอนิกส์ใดที่ได้กระทำตามวิธีการแบบปลอดภัยที่กำหนดในพระราชกฤษฎีกา ให้สันนิษฐานว่าเป็นวิธีการที่เชื่อถือได้ จะเห็นได้ว่า พยานหลักฐานดิจิทัล มีกฎหมายรองรับ สามารถรับฟังได้ในชั้นศาล หากมีมาตรฐานที่สามารถพิสูจน์ได้ถึงการรักษาความถูกต้อง สิ่งสำคัญที่จะทำให้การตรวจพิสูจน์พยานหลักฐานดิจิทัล ได้รับการยอมรับในชั้นศาล โดยไม่ถูกโต้แย้ง คือ ต้องสามารถยืนยันได้ว่าหลักฐานที่นำมาตรวจสอบ เป็นหลักฐานเดียวกับที่เก็บมาจากสถานที่เกิดเหตุจริง (Authentication) และไม่มีการเปลี่ยนแปลงข้อมูลใดๆ ไปจากเดิม (Integrity)

5.1.2.2 ประมวลกฎหมายวิธีพิจารณาความอาญา

มาตรา 226 เป็นบททั่วไปของหลักเรื่องพยานหลักฐานในคดีอาญา ได้บัญญัติถึงพยานหลักฐานที่ใช้อ้างเพื่อพิสูจน์ว่าจำเลยมีผิดหรือบริสุทธิ์ แบ่งเป็น 3 ประเภท ได้แก่ พยานบุคคล พยานเอกสาร และพยานวัตถุ ดังนั้น การอ้างเอกสารเป็นพยานในคดี ไม่ได้หมายความว่าเอกสารดังกล่าวจะเป็นพยานเอกสารในทุกกรณี เช่น หากเป็นการอ้างข้อความบางตอนในเอกสาร เพื่อพิสูจน์ข้อเท็จจริงตามข้อความนั้น จะถือว่าเป็นการอ้างเอกสารในฐานะที่เป็นพยานเอกสาร แต่หากอ้างลายมือชื่อในเอกสารเพื่อพิสูจน์ว่าเป็นลายมือชื่อที่จำเลยทำปลอมขึ้นในความผิดฐานปลอมเอกสาร หรืออ้างเอกสารทั้งเล่มเพื่อพิสูจน์ว่ามีการทำซ้ำซึ่งงานอันมีลิขสิทธิ์ จะถือว่าเป็นการอ้างเอกสารในฐานะที่เป็นพยานวัตถุ กล่าวอีกนัยหนึ่ง จะต้องพิจารณาโดยดูที่วัตถุประสงค์ในการใช้อ้างเอกสารเพื่อเป็นพยาน หากเป็นการอ้างเพื่อให้ศาลดูข้อความในเอกสารก็จัดเป็นพยานเอกสาร แต่หากเป็นการอ้างเพื่อให้ศาลดูรูปลักษณะของเอกสาร ก็จัดเป็นพยานวัตถุ กฎหมายได้กำหนดประเภทของพยานหลักฐานดังกล่าวไว้ เพื่อให้สอดคล้องกับหลักการรับฟังพยานหลักฐานแต่ละประเภท โดยในส่วนของข้อมูลที่บันทึกอยู่ในระบบคอมพิวเตอร์ อาจจัดเป็นพยานเอกสารหรือพยานวัตถุตามแต่วัตถุประสงค์ในการใช้อ้างในคดี

5.1.2.3 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560

มีส่วนที่เกี่ยวข้องกับกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล คือ มาตรา 18 ภายใต้บังคับมาตรา 19 ได้กำหนดอำนาจของพนักงานเจ้าหน้าที่ไว้เพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด และหาตัวผู้กระทำความผิด โดยพนักงานเจ้าหน้าที่สามารถยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำ หรือกำลังจะกระทำการอย่างหนึ่งอย่างใดอันเป็นความผิด เหตุที่ต้องใช้อำนาจลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิดเท่าที่สามารถจะระบุได้ ประกอบคำร้องด้วย ในการพิจารณาคำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็ว เมื่อศาลมีคำสั่งอนุญาตแล้ว ก่อนดำเนินการตามคำสั่งของศาลให้พนักงานเจ้าหน้าที่ส่งสำเนาบันทึกเหตุอันควรเชื่อที่ทำให้ต้องใช้อำนาจ มอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐาน แต่ถ้าไม่มีเจ้าของหรือ ผู้ครอบครองเครื่องคอมพิวเตอร์อยู่ ณ ที่นั้น ให้พนักงานเจ้าหน้าที่ส่งมอบสำเนาบันทึกนั้นให้แก่เจ้าของหรือผู้ครอบครองดังกล่าวในทันทีที่กระทำได้ และให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าในการดำเนินการ ส่งสำเนาบันทึกรายละเอียดการดำเนินการ และเหตุผลแห่งการดำเนินการให้ศาลที่มี เขตอำนาจภายในสี่สิบแปดชั่วโมงนับแต่เวลาลงมือดำเนินการ เพื่อเป็นหลักฐาน การทำสำเนาข้อมูลคอมพิวเตอร์ให้กระทำได้เฉพาะเมื่อมีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิด และต้องไม่เป็นอุปสรรคในการดำเนินกิจการของเจ้าของหรือ ผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นเกินความจำเป็น การยึดหรืออายัด นอกจากจะต้องส่งมอบสำเนาหนังสือแสดงการยึดหรืออายัดมอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐานแล้ว พนักงานเจ้าหน้าที่จะสั่งยึดหรืออายัดไว้เกินสามสิบวันมิได้ ในกรณีจำเป็นที่ต้องยึดหรืออายัดไว้นานกว่านั้น ให้ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอขยายเวลายึดหรืออายัดได้ แต่ศาลจะอนุญาตให้ขยายเวลาครั้งเดียวหรือหลายครั้งรวมกันได้อีกไม่เกินหกสิบวัน เมื่อหมดความจำเป็นที่จะยึดหรือ อายัด หรือครบกำหนดเวลาดังกล่าวแล้ว พนักงานเจ้าหน้าที่ต้องส่งคืนระบบคอมพิวเตอร์ที่ยึดหรือถอนการอายัด

5.1.3 ปัญหาและอุปสรรคของการตรวจพิสูจน์พยานหลักฐานดิจิทัลในประเทศไทย

มีประเด็นปัญหาดังนี้

1. หลายภาคส่วน ยังมีความเข้าใจเกี่ยวกับการตรวจพิสูจน์พยานหลักฐานดิจิทัลว่าเกี่ยวข้องกับการสืบสวนคดีอาชญากรรมเท่านั้น หรือพยานหลักฐานดิจิทัลมีความยุ่งยากซับซ้อน ซึ่งแท้จริงแล้วการตรวจพิสูจน์พยานหลักฐานดิจิทัลเกี่ยวข้องกับหลายส่วนไม่ว่าจะเป็นการสืบสวนคดีอาชญากรรม, การฟ้องร้องในคดีแพ่ง หรือการฟ้องร้องเรื่องส่วนตัว ถ้าเกี่ยวข้องกับคอมพิวเตอร์ การสื่อสารผ่านอุปกรณ์อิเล็กทรอนิกส์หรือเอกสารอิเล็กทรอนิกส์ ก็มีความจำเป็นต้องใช้กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล เช่น การกู้ข้อมูลที่ถูกลบและไฟล์การใช้งานชั่วคราวที่เกิดขึ้นจากกระบวนการทำงานของคอมพิวเตอร์ ซึ่งข้อมูลที่พิสูจน์ได้ ผู้ใช้งานจะไม่สามารถโต้แย้งได้เนื่องจากเป็นข้อมูลที่เกิดขึ้นจริง
2. ปัจจุบันผู้เกี่ยวข้องในกระบวนการยุติธรรมบางส่วนยังเข้าใจว่าการใช้พยานหลักฐานดิจิทัลมีความยุ่งยากซับซ้อนและคิดว่าไม่สามารถนำมาอ้างอิง ซึ่งเป็นความเข้าใจที่ไม่ตรงนัก เนื่องจากหลายกรณีมีความจำเป็นที่จะต้องใช้พยานหลักฐานดิจิทัล เช่น ไฟล์รูปภาพ อีเมลล์ เอกสาร

อิเล็กทรอนิกส์ และประวัติการใช้งานเครือข่ายอินเทอร์เน็ต ซึ่งหลักฐานเหล่านี้สามารถนำมาอธิบายในชั้นพิจารณาคดี ในรูปแบบที่เข้าใจได้ง่าย

3. การจัดการกับพยานหลักฐานดิจิทัลมีสิ่งทีสำคัญ คือ

    1) ความสมบูรณ์ของพยานหลักฐาน และ

    2) ความถูกต้องของหลักฐาน โดยเป็นไปตามพระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2554 ซึ่งถือเป็นจุดเริ่มต้นของงานด้านตรวจพิสูจน์พยานหลักฐานดิจิทัลในประเทศไทย

4. ในส่วนการรับฟังพยานหลักฐานดิจิทัลของศาลไทย ปัจจุบันมีการกำหนดให้สื่ออิเล็กทรอนิกส์สามารถใช้เป็นพยานหลักฐานในการพิจารณาคดีได้ นอกเหนือจากพยานวัตถุ พยานเอกสาร พยานบุคคล และพยานนิติวิทยาศาสตร์ สามารถใช้เป็นข้อพิสูจน์ว่าจำเลยมีความผิดหรือบริสุทธิ์ โดยมีข้อที่ต้องพิจารณาคือ มีวิธีการนำสืบและหลักในการรับฟังพยานอย่างไร จะนำบทตัดพยาน คือ หลักการรับฟังพยานหลักฐานที่ดีที่สุด และหลักการรับฟังพยานบอกเล่า มาใช้ด้วยหรือไม่ รวมถึงกำหนดให้ผู้กล่าวอ้างดำเนินการเหมือนกันกับพยานหลักฐานประเภทอื่น คือ ยื่นบัญชีระบุพยาน มีลายเซ็นต์ผู้ที่เกี่ยวข้อง เช่น คนรับเครื่อง คนอนุญาต วันและเวลา มีการส่งสำเนาพยานหลักฐานที่จะอ้างอิงให้แก่คู่ความอีกฝ่าย การตรวจพิสูจน์พยานหลักฐานดิจิทัล ไม่เพียงแต่เป็นการสืบสวนข้อมูลทางอิเล็กทรอนิกส์ แต่ยังเป็นการระบุข้อมูลที่เกี่ยวข้องกับการสืบสวนและค้นหาหลักฐานเพื่อประกอบการดำเนินคดี จึงจำเป็นจะต้องทำความเข้าใจว่า ข้อมูลนี้ไม่ได้หมายถึงเฉพาะข้อมูลในคอมพิวเตอร์ แต่รวมถึงอุปกรณ์ที่สามารถจัดเก็บข้อมูลทางอิเล็กทรอนิคส์ เช่น โทรศัพท์มือถือ กล้องถ่ายรูป อุปกรณ์รับสัญญาณดาวเทียม อุปกรณ์จัดเก็บข้อมูลพกพา เครื่องเล่นเกม และแม้แต่อุปกรณ์อิเล็กทรอนิกส์ในชีวิตประจำวันอื่นๆ ซึ่งในปัจจุบันพบว่า เป็นการสื่อสารข้อมูลในรูปของข้อมูลอิเล็กทรอนิกส์ค่อนข้างมาก การตรวจพิสูจน์พยานหลักฐานดิจิทัลจึงเป็นเครื่องมือที่สำคัญ

    การรับฟังพยานหลักฐานอิเล็กทรอนิกส์มีหลักกฎหมายสำคัญ 3 ประการ ในการพิจารณาพยานหลักฐานนั้นว่าสามารถยืนยันความแท้จริงได้อย่างเหมาะสมหรือไม่

    <u>ความแท้จริงของพยานหลักฐานอิเล็กทรอนิกส์ประกอบด้วย</u>

    1) เนื้อหานั้นไม่ได้ถูกเปลี่ยนแปลง
    2) ข้อมูลนั้นเป็นไปตามเจตนาที่แท้จริงของผู้สร้างเอกสารนั้น ทั้งนี้ไม่ว่าผู้สร้างเอกสารจะเป็นมนุษย์ หรือคอมพิวเตอร์
    3) ข้อมูลพิเศษ เช่น วันเดือนปี ที่ถูกสร้างนั้นถูกต้อง

ในปัจจุบันศาลไทยได้ยอมรับและรับฟังพยานหลักฐานอิเล็กทรอนิกส์ เช่น ในคำพิพากษาศาลฎีกาที่ 7264/2542 วางหลักไว้ว่า พยานหลักฐานทางคอมพิวเตอร์สามารถรับฟังได้ ซึ่งอาจรับฟังในฐานะที่เป็นพยานเอกสาร ในกรณีที่มีการพิมพ์แล้วนำผลที่ได้มานำเสนอ ซึ่งแนวทางการรับฟังพยานหลักฐานของศาล จะต้องปรากฏว่าระบบการบันทึก การสร้าง การเก็บรักษา การเรียกข้อมูลหรือการใช้งานของคอมพิวเตอร์เป็นปกติตามที่เคยเป็น ไม่มีสิ่งที่ผิดปกติ หรือบิดเบือน จึงจะถือว่าเป็นข้อมูลที่ถูกต้อง ดังนั้น ปัญหาในการรับฟังพยานหลักฐานของศาล จึงไม่เป็นอุปสรรคต่อการดำเนินคดีหรือการค้นหาความจริงทางคดี

การใช้พยานเอกสารที่เป็นข้อมูลทางอิเล็กทรอนิกส์ สามารถนำมาอ้างอิงเป็นหลักฐานต่อศาลได้ ศาลจะไม่ปฏิเสธการรับฟังข้อมูล เพราะเหตุว่าเป็นข้อมูลทางอิเล็กทรอนิกส์ แต่ข้อมูลดังกล่าวจะมีความน่าเชื่อถือ รับฟังในเนื้อหาสาระได้หรือไม่ เป็นดุลยพินิจของศาลซึ่งเป็นผู้รับฟังข้อมูลในการชั่งน้ำหนักพยานเอง โดยใช้หลักเกณฑ์ความน่าเชื่อถือตามที่กำหนดไว้ในมาตรา 10 วรรคสอง ของพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2554 เป็นเกณฑ์ในการพิจารณา จึงจำเป็นต้องมีการอบรมและให้ความรู้ทางด้านความปลอดภัยของข้อมูล การปรับเปลี่ยนทัศนคติ ค่านิยม และความเคยชินในระบบพยานหลักฐานของไทย จากบทบัญญัติของประมวลกฎหมายวิธีพิจารณาความแพ่ง ซึ่งนำไปใช้ในวิธีพิจารณาความอาญาด้วยนั้น ไม่ว่าจะเป็นระบบพยานบุคคล พยานเอกสาร พยานวัตถุ และพยานผู้เชี่ยวชาญหรือผู้ชำนาญการพิเศษ ซึ่งแต่เดิมไม่ได้ออกแบบไว้สำหรับพยานหลักฐานทางคอมพิวเตอร์หรืออิเล็กทรอนิกส์ จึงควรมีการปรับเปลี่ยน เนื่องจากเป็นเรื่องจำเป็นสำหรับพนักงานสอบสวนตลอดจนผู้ที่เกี่ยวข้องในกระบวนการยุติธรรมจนถึงชั้นศาล ที่จะรับมือกับอาชญากรรมคอมพิวเตอร์ที่เพิ่มมากขึ้น และรูปแบบที่มีความซับซ้อนมากขึ้น ความรู้ ความเข้าใจด้านการตรวจพิสูจน์พยานหลักฐานดิจิทัล จะทำให้ผู้ที่เกี่ยวข้องในกระบวนการยุติธรรมสามารถนำกฎหมายมาบังคับใช้ได้อย่างมีประสิทธิภาพสูงสุด

5.2 ข้อเสนอแนะ

การพัฒนากระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล แต่เดิมส่วนใหญ่เป็นงานด้านวิทยาศาสตร์และคอมพิวเตอร์ ไม่สามารถเชื่อมโยงกับการพิจารณาคดีตามกฎหมายได้มากนัก จะศึกษาเฉพาะด้านเทคนิคของพยานหลักฐานดิจิทัลเท่านั้น ในการเก็บรวบรวมและตรวจพิสูจน์พยานหลักฐานดิจิทัล ปัญหาที่พบไม่ใช่การใช้เทคโนโลยี หรือเครื่องมือ แต่อยู่ที่กระบวนการ หลายครั้งหลักฐานถูกเปลี่ยนแปลงก่อนที่จะถึงผู้ตรวจพิสูจน์ การสื่อสารให้เกิดความเข้าใจที่ตรงกันระหว่างผู้เก็บรวบรวมหลักฐาน คนทำคดีและผู้ตรวจพิสูจน์จึงมีความสำคัญ รวมทั้งการสร้างความรู้และความเข้าใจ เพื่อไม่ให้หลักฐานถูกเปลี่ยนแปลงโดยไม่ทราบหรือไม่ตั้งใจ ในกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล ควรจะมีการสร้างมาตรฐานโดยยึดหลักการรักษาสภาพหลักฐานและไม่เปลี่ยนแปลงหลักฐาน มีการกำหนดว่าอะไรคือพยานหลักฐานดิจิทัล แนวทางวิธีการเก็บหลักฐาน การขนส่ง การเขียนรายงาน และอื่นๆ ซึ่งหน่วยงานในกระบวนการยุติธรรมที่เกี่ยวข้องต้องมาพัฒนาร่วมกัน นอกเหนือไปจากมาตรฐานการจัดการอุปกรณ์ดิจิทัลในการตรวจพิสูจน์พยานหลักฐานดิจัลที่ศูนย์ดิจิทัลฟอเรนสิกส์ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ได้จัดทำขึ้น เพื่อให้เป็นที่ยอมรับของทุกฝ่ายและสามารถใช้งานได้จริงไม่ใช่เป็นเพียงหลักการหรือทฤษฎี การจัดการกับปัญหาอาชญากรรมจะเป็นไปอย่างมีประสิทธิภาพต้องมีการทำงานร่วมกันเป็นทีม มาตรฐานส่วนนี้เป็นเรื่องสำคัญ เพราะพยานหลักฐานดิจิทัลมีอยู่ทุกแห่ง การจะจัดการอย่างไรให้น่าเชื่อถือ รับฟังได้ในชั้นพิจารณาคดี จึงเป็นเรื่องที่ต้องให้ความสำคัญ จากการศึกษาผู้วิจัยมีข้อเสนอแนะ ดังต่อไปนี้

5.2.1 ข้อเสนอแนะเชิงนโยบาย

1) ควรมีการศึกษาและทบทวนกฎหมายที่เกี่ยวข้องเพื่อให้เหมาะสมกับบริบทของอาชญากรรมคอมพิวเตอร์ในสถานการณ์ปัจจุบัน ทั้งในส่วนของพระราชบัญญัติว่า

ด้วยธุรกรรมทางอิเล็กทรอนิกส์ และในส่วนของพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ เพื่อให้ขอบเขตของกระบวนการตรวจพิสูจน์หลักฐานทางดิจิทัล มีความชัดเจน ครอบคลุม และ การกระทำความผิดทางคอมพิวเตอร์ มุ่งเน้นในส่วนของระบบ มากกว่าเนื้อหา กล่าวคือ

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

ตามร่างที่เสนอ เพื่อปรับปรุงหลักเกณฑ์เกี่ยวกับการดำเนินการทางธุรกรรมทางอิเล็กทรอนิกส์ให้มีมาตรฐานสากล เช่น การเพิ่มบทนิยามคำว่า “ระบบแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์” เพื่อให้สอดคล้องกับอนุสัญญาสหประชาชาติว่าด้วยการใช้การติดต่อสื่อสารทางอิเล็กทรอนิกส์ในสัญญาระหว่างประเทศ (United Nations Convention on the Use of Electronic Communications in International Contracts), เพิ่มเติมเกี่ยวกับผลทางกฎหมายในการลงลายมือชื่ออิเล็กทรอนิกส์ ในกรณีที่ไม่มีการลงลายมือชื่อ หากได้ดำเนินการตามที่กำหนดไว้ก็ถือว่าได้มีการลงลายมือชื่อ, แก้ไขวิธีการตรวจสอบว่าข้อมูลอิเล็กทรอนิกส์เป็นของผู้ส่งข้อมูล โดยให้ผู้รับข้อมูลตรวจสอบตามวิธีการที่ผู้ส่งข้อมูลได้ตกลงหรือผูกพันตนไว้ว่าเป็นข้อมูลอิเล็กทรอนิกส์, กำหนดให้บุคคลธรรมดามีสิทธิที่จะถอนการแสดงเจตนาในกรณีที่มีการลงข้อมูลโดยผิดพลาดและส่งผ่านระบบแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์อัตโนมัติของผู้อื่นซึ่งไม่มีช่องทางให้แก้ไขข้อผิดพลาด, กำหนดให้ศาลหรือองค์กรตามรัฐธรรมนูญมีดุลพินิจที่จะนำหลักเกณฑ์ในเรื่องใดของพระราชกฤษฎีกาที่กำหนดหลักเกณฑ์และวิธีการเกี่ยวกับการจัดทำข้อมูลอิเล็กทรอนิกส์ของหน่วยงานของรัฐมาใช้แก่การดำเนินกระบวนพิจารณาพิพากษาคดีของศาลหรือในการวินิจฉัยชี้ขาดข้อพิพาทก็ได้

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ควรมีการแก้ไขพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในมาตรา 14, 16 และ 20 โดย

มาตรา 14 จากเดิมที่กำหนดฐานความผิดเกี่ยวกับการนำเข้า เผยแพร่หรือส่งต่อข้อมูลที่บิดเบือน ปลอม หรือเป็นเท็จ หรือข้อมูลที่กระทบความมั่นคง หรือข้อมูลลามก ให้เหลือเพียงฐานความผิดเดียวคือ "ฐานความผิดกรณีหลอกลวงผู้อื่นด้วยการนำเข้า เผยแพร่ และส่งต่อข้อมูลปลอม" หรือเรียกว่า ความผิดฐานปลอมข้อมูลคอมพิวเตอร์ และกำหนดให้ฐานความผิดดังกล่าวเป็นความผิดอันยอมความได้

มาตรา 16 เพิ่มเติมกรณีที่กำหนดให้ศาลอาจสามารถสั่งให้ทำลายข้อมูลหรือให้โฆษณาหรือเผยแพร่คำพิพากษาทั้งหมดหรือแต่บางส่วน หรือให้ดำเนินการ

อื่นตามที่ศาลเห็นสมควร ซึ่งเดิมกำหนดให้ศาลมีอำนาจสั่งได้เฉพาะคดีที่เป็นความผิดตามมาตรา 14 กรณีความผิดฐานหลอกลวงผู้อื่นด้วยการนำเข้า เผยแพร่และส่งต่อข้อมูลโดยทุจริต และมาตรา 16 กรณีความผิดฐานนำข้อมูลภาพของผู้อื่นที่สร้างขึ้น ตัดต่อ เติม ดัดแปลงเข้าสู่ระบบคอมพิวเตอร์ โดยประการที่น่าจะเสียชื่อเสียง ถูกดูหมิ่นถูกเกลียดชัง หรืออับอาย โดยตัดความว่า "มาตรา 14 หรือมาตรา 16 ซึ่งมี" ออก เพื่อให้ศาลสามารถสั่งให้จำเลยดำเนินการดังกล่าวได้ในทุกฐานความผิดตามที่ศาลพิพากษาว่าจำเลยมีความผิดอันเป็นไปตามที่ศาลเห็นสมควร

มาตรา 20 แก้ไขเพิ่มเติมเกี่ยวกับอำนาจหน้าที่ของเจ้าหน้าที่ในการยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจ เพื่อขอให้ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ จากเดิมที่กำหนดให้พนักงานเจ้าหน้าที่ต้องดำเนินกระบวนการดังกล่าวโดยได้รับความเห็นชอบจากรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และกำหนดให้รัฐมนตรีสามารถแต่งตั้งคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์เพื่อดำเนินการสำหรับกรณีที่ข้อมูลคอมพิวเตอร์ที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชนมีการทำให้แพร่หลาย โดยแก้ไขเพิ่มเติมให้การยื่นคำร้องต่อศาลดำเนินการโดยเจ้าหน้าที่ซึ่งมีอำนาจหน้าที่ทำการสอบสวนในการกระทำความผิดตามกฎหมาย หรือให้พนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญาซึ่งได้ร้องขอให้พนักงานเจ้าหน้าที่ตามกฎหมายนี้เป็นผู้ดำเนินการ โดยไม่ต้องมีคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์ที่แต่งตั้งโดยรัฐมนตรีเกี่ยวข้อง

2) กำหนดหน่วยงานกลางของรัฐที่รับผิดชอบดูแลและปรับปรุงมาตรฐานกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลให้เหมาะกับเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว โดยเบื้องต้น สามารถเริ่มจากการส่งเสริมบทบาทของ ศูนย์ดิจิทัลฟอเรนสิกส์ (Digital Forensics Center) ที่มีอยู่เดิม ซึ่งอยู่ภายใต้การกำกับดูแลของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) หรือ ETDA กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และยกระดับเป็นหน่วยงานที่มีขอบเขตอำนาจที่ชัดเจนในการกำหนดมาตรฐาน
3) มีการกำหนดแนวทางในการประเมินผล เพื่อให้ทราบถึงปัญหาและอุปสรรคที่เกิดขึ้นของกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลจากการปฏิบัติงานจริงของภาคส่วนต่างๆ และนำผลที่ได้มาเป็นแนวทางสำหรับการจัดทำแผนแม่บท และใช้ในการศึกษาและทบทวนกฎหมายที่เกี่ยวข้อง
4) สร้างเครือข่ายการบูรณาการความร่วมมือกับหน่วยงานทั้งภาครัฐ ภาคเอกชน ภาคประชาชน และความร่วมมือระหว่างประเทศในด้านอาชญากรรมคอมพิวเตอร์ รวมถึงกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล เพื่อนำกรณีศึกษาต่างๆ มา

เป็นตัวอย่างสำหรับพัฒนากระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลในประเทศไทย

5.2.2 ข้อเสนอแนะเชิงปฏิบัติ

ในส่วนของกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล มีข้อเสนอแนะดังนี้

1) <u>การรวบรวมพยานหลักฐานดิจิทัล</u>

สิ่งสำคัญที่สุด คือ ความสมบูรณ์ของพยานหลักฐาน และการรวบรวมพยานหลักฐานทั้งหมดให้เป็นไปอย่างสมบูรณ์ขณะเกิดเหตุโดยไม่ถูกเปลี่ยนแปลงแก้ไขใดๆ พนักงานสอบสวนต้องเคร่งครัดกับการใช้อำนาจรวบรวมพยานหลักฐานให้เป็นไปตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 132 และกฎหมายที่บัญญัติเอาไว้โดยเฉพาะเจาะจงในเรื่องของอำนาจของพนักงานสอบสวนหรือเจ้าพนักงานผู้มีอำนาจรวบรวมพยานหลักฐานและหลักเกณฑ์วิธีการในการรวบรวมและจัดเก็บพยานหลักฐาน เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

2) <u>การเก็บรักษาพยานหลักฐานดิจิทัล</u>

การเก็บรักษาจะต้องเก็บรักษาไว้ในสภาพที่รับฟังได้ในชั้นศาล เป็นไปตามกระบวนการสร้างห่วงโซ่คุ้มครองพยานหลักฐานในหลักสากลต้องมีมาตรฐานการเก็บรักษาพยานหลักฐานดิจิทัลที่เป็นที่ยอมรับของทุกฝ่ายมีบันทึกขั้นตอนการคุ้มครองพยานหลักฐานและวิธีการเก็บรักษา เพื่อให้มั่นใจได้ว่าเป็นข้อมูลที่ไม่ได้ถูกแก้ไขเปลี่ยนแปลงนับจากที่ได้รับมาจากที่เกิดเหตุ โดยมาตรฐานในการจัดเก็บและจัดการพยานหลักฐานดิจิทัลของเจ้าพนักงานที่เกี่ยวข้อง อาจทำให้เกิดประเด็นข้อโต้แย้งในการรับฟังพยานหลักฐานได้ เนื่องจากพยานหลักฐานดิจิทัลในรูปของข้อมูลคอมพิวเตอร์หรือข้อมูลอิเล็กทรอนิกส์ มีความเสี่ยงต่อการถูกเปลี่ยนแปลงแก้ไข สูญหาย เสียหาย โดยง่าย โดยเฉพาะอย่างยิ่งเมื่อต้องมีการส่งผ่านข้อมูลคอมพิวเตอร์หรือข้อมูลอิเล็กทรอนิกส์ระหว่างเจ้าพนักงานที่เกี่ยวข้องหลายทอด โดยในปัจจุบัน มีข้อเสนอแนะจาก สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. ได้เผยแพร่เอกสาร “ข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐาน” เพื่อเป็นแนวทางเบื้องต้นให้กับเจ้าหน้าที่ที่เกี่ยวข้องกับการจัดเก็บ รวบรวม และตรวจพิสูจน์พยานหลักฐานดิจิทัล ให้ปฏิบัติงานในสถานที่เกิดเหตุและในห้องปฏิบัติการให้สอดคล้องกับมาตรฐานสากล โดยสพธอ. เน้นในเรื่องการให้ความสำคัญต่อการบันทึกแบบฟอร์มที่เรียกว่า “Chain of Custody” หรือห่วงโซ่คุ้มครองพยานหลักฐาน

3) <u>การวิเคราะห์พยานหลักฐานดิจิทัล</u>

พยานหลักฐานแต่ละประเภทของคดีจะมีความแตกต่างกัน วิธีวิเคราะห์จึงแตกต่างกัน มีการใช้เครื่องมือที่แตกต่างกัน ทักษะเจ้าหน้าที่แตกต่างกัน การฝึกอบรมเจ้าหน้าที่พิสูจน์หลักฐานจึงมีความสำคัญ การวิเคราะห์พยานหลักฐานดิจิทัล จึงต้องใช้ผู้เชี่ยวชาญด้าน

พยานหลักฐานดิจิทัลมาวิเคราะห์ และต้องจัดหาอุปกรณ์ ทั้งฮาร์ดแวร์และซอฟต์แวร์ที่เหมาะสมมาใช้ โดยมีงบประมาณสนับสนุนที่เพียงพอ มีการปรับปรุงให้เป็นปัจจุบัน ทันกับเทคโนโลยี โดยทั่วไปจะมีการใช้โปรแกรมคอมพิวเตอร์เฉพาะทาง ไม่ว่าจะเป็นโปรแกรมที่พัฒนาขึ้นโดยเฉพาะ หรือมีผู้พัฒนาสำหรับใช้วิเคราะห์พยานหลักฐานดิจิทัล เช่น โปรแกรมที่ใช้สำหรับตรวจสอบคอมพิวเตอร์และโทรศัพท์มือถือ สำหรับวิเคราะห์พยานหลักฐานดิจิทัลที่นิยมใช้ คือ Encase และ FTK จะเป็นโปรแกรมที่พัฒนาและขายให้กับหน่วยงานที่ทำหน้าที่พิสูจน์หลักฐานทางดิจิทัลโดยเฉพาะ สามารถใช้กู้ข้อมูลที่ถูกลบ ซ่อน ไม่ว่าจะโดยผู้ใช้ หรือโดยระบบ สามารถค้นหาข้อมูลที่ถูกเปลี่ยนแปลง แก้ไข เข้ารหัส และอื่นๆ

4) <u>การนำเสนอผลพิสูจน์พยานหลักฐานดิจิทัล</u> การนำเสนอผลการตรวจพิสูจน์พยานหลักฐานดิจิทัล เป็นรายงานบันทึกคำให้การผู้เชี่ยวชาญ อธิบายวิธีการตรวจสอบ เครื่องมือที่ใช้ตรวจสอบ ตรวจสอบสิ่งใดบ้าง วิธีเก็บพยานหลักฐาน สิ่งที่ค้นพบ และวิธีการยืนยันความแท้จริงของพยานหลักฐานดิจิทัล พยานหลักฐานดิจิทัลซึ่งพนักงานสอบสวนได้รวบรวมเพื่อพิสูจน์ว่าผู้ต้องหากระทำความผิดตามข้อกล่าวหา จะถูกนำเสนอต่อศาลระหว่างกระบวนการพิจารณาสืบพยาน โดยศาลมีอำนาจใช้ดุลพินิจรับฟังและชั่งน้ำหนักของพยานหลักฐานดิจิทัลตามที่กฎหมายกำหนด ปัจจุบันยังไม่มีบทบัญญัติเกี่ยวกับการรับฟังพยานหลักฐานดิจิทัลในคดีอาญาเป็นการเฉพาะเจาะจง การรับฟังพยานหลักฐานดิจิทัลจึงต้องเป็นไปตามหลักการรับฟังพยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาความอาญาอันเป็นบทกฎหมายทั่วไป ซึ่งบัญญัติไว้ว่า พยานวัตถุ พยานเอกสาร หรือพยานบุคคลซึ่งน่าจะพิสูจน์ได้ว่าจำเลยมีผิดหรือบริสุทธิ์ ให้อ้างเป็นพยานหลักฐานได้ แต่ต้องเป็นพยานชนิดที่ไม่ได้เกิดขึ้นจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวงหรือโดยมิชอบประการอื่น และให้สืบตามบทบัญญัติแห่งประมวลกฎหมายนี้ หรือกฎหมายอื่นอันว่าด้วยการสืบพยาน ดังนั้น ทุกขั้นตอนของการตรวจพิสูจน์พยานหลักฐานดิจิทัลจะต้องต้องปฏิบัติให้ถูกต้องตามหลักเกณฑ์และวิธีการดังกล่าว ไม่เช่นนั้นจะถือว่าเป็นการได้พยานหลักฐานดิจิทัลมาโดยมิชอบ ศาลมีอำนาจไม่รับฟังได้

5) บุคลากรภาครัฐที่เกี่ยวข้องกับกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล จะต้องมีการเรียนรู้พัฒนาตนเอง เพื่อเรียนรู้เทคนิคใหม่ๆ ให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยี และปริมาณข้อมูลที่มีจำนวนมากขึ้น เพื่อให้การรวบรวมพยานหลักฐาน และการเก็บรักษา เป็นไปอย่างถูกวิธี และหน่วยงานต้นสังกัด ควรจัดให้มีการฝึกอบรมเพื่อเพิ่มความรู้ความชำนาญด้านกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลอย่างสม่ำเสมอ เพื่อให้บุคลากรสามารถพัฒนา และเรียนรู้เทคนิคใหม่ๆ เพิ่มเติม โดยควรจัดทำเครือข่ายความร่วมมือทางวิชาการ และผลักดันให้มีการจัดตั้งสภาวิชาชีพนิติวิทยาศาสตร์ เพื่อให้มีสามารถมีการจัดการอบรมอย่างเร่งด่วน สม่ำเสมอ ในหัวข้อใหม่ๆ เช่น ในหัวข้อของการตรวจพิสูจน์พยานหลักฐานในสกุลเงินดิจิทัล (Cryptocurrency

Forensics), เทคโนโลยีการเข้ารหัสต่างๆ, การตรวจพิสูจน์หลักฐานในส่วนที่เกี่ยวข้องกับ Cloud และโนโลกเสมือน (Virtual World) เป็นต้น

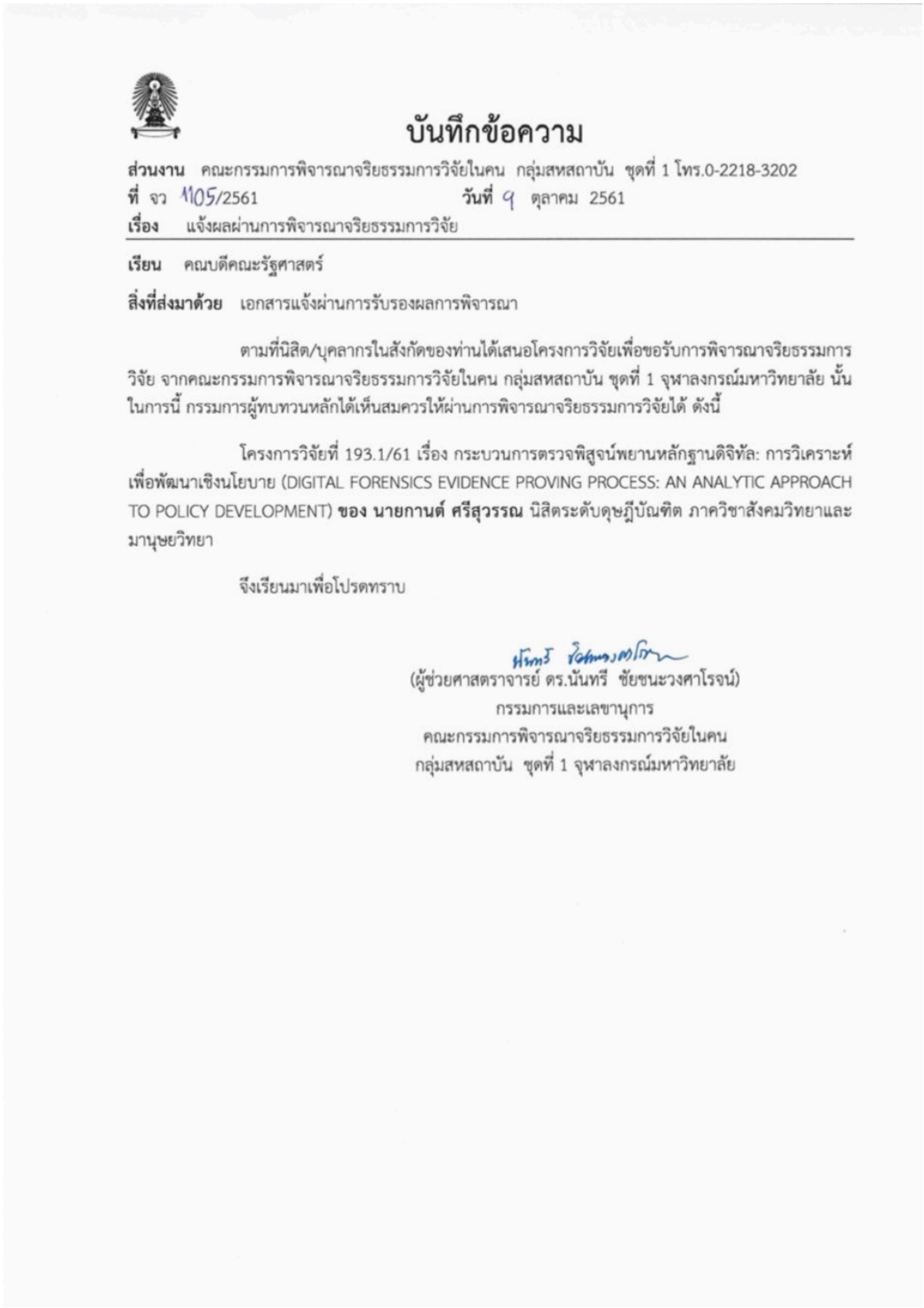
6) มีการจัดการสนับสนุน ทั้งในส่วนของบุคลากรอื่นๆ ที่ปฏิบัติงานร่วมกัน และด้านอุปกรณ์ทางเทคโนโลยีที่ใช้ในการสืบสวน และตรวจพิสูจน์หลักฐานอย่างพอเพียง เพื่อให้สามารถทำงานร่วมกันเป็นทีมได้ แต่ก็มีความเป็นอิสระในการปฏิบัติงาน
7) มีการจัดทำแผนปฏิบัติงานเป็นขั้นตอน ที่ชัดเจน เป็นระบบ เพื่อกำหนดแนวทางในการทำงานอย่างมีประสิทธิภาพ ลดปัญหาที่จะส่งผลกระทบต่อพยานหลักฐานดิจิทัล
8) เพิ่มความร่วมมือ กับนักวิชาการ ภาคเอกชน ผู้เชี่ยวชาญด้านกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล ตลอดจนทำความเข้าใจกับภาคประชาชน ถึงแนวทางการปฏิบัติงานในขั้นตอนต่างๆ เพื่อสร้างความมั่นใจ และคลายปมปัญหา ตลอดจนข้อสงสัยอันจจะนำไปสู่อุปสรรคในการปฏิบัติงาน
9) นำเทคโนโลยีใหม่ๆ ไม่ว่าจะเป็นฐานข้อมูลของระบบผู้เชี่ยวชาญ การใช้ปัญญาประดิษฐ์มาช่วยเสริมการทำงานของบุคลากร เพื่อเตรียมรับ กับการเพิ่มขึ้นอย่างรวดเร็วของอาชญากรรมคอมพิวเตอร์ที่เกิดขึ้น ลดภาระของบุคลากร และเพิ่มประสิทธิภาพประสิทธิผล ในการปฏิบัติงาน
10) มีการประชาสัมพันธ์ขั้นตอน และห้วงเวลาในการทำงานในขั้นตอนต่างๆ ของผู้ปฏิบ้ติงาน กับภาคประชาชน ตลอดจนสื่อต่างๆ อย่างสม่ำเสมอ เพื่อให้ไม่เกิดความเข้าใจผิด หรือ หลงเชื่อตามข่าวลือต่างๆ อ้นจะนำไปสู่ปัญหาและอุปสรรคในการปฏิบัติงาน ตลอดจนเกิดการไม่ร่วมมือ จากภาคประชาชน อันเนื่องมาจากได้รับข้อมูลที่ไม่ถูกต้องตามความเป็นจริง

5.2.3 ข้อเสนอแนะสำหรับการศึกษาต่อไป

1) ควรศึกษาเพิ่มเติมในส่วนของอาชญากรรมคอมพิวเตอร์รูปแบบใหม่ๆ ที่อาศัยเทคโนโลยีที่มีความซับซ้อนมากขึ้น เพื่อสร้างและพัฒนาองค์ความรู้ด้านกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล ให้เท่าทันกับอาชญากรรมที่เกิดขึ้น
2) ควรศึกษาเพิ่มเติมในส่วนของการนำแนวคิด ทฤษฎีทางด้านอาชญาวิทยา และด้านสังคมมาเพื่อเรียนรู้ถึงปัญหา สาเหตุ และแนวทางแก้ไขอาชญากรรมคอมพิวเตอร์ เพื่อจะได้พัฒนาแนวทางการป้องกัน และรู้เท่าทันอาชญากร
3) ควรศึกษาเพิ่มเติมในส่วนของการรักษาความปลอดภัยทางด้านคอมพิวเตอร์ ทั้งเชิงเทคนิค และบริบททางสังคม เพื่อสร้างความตระหนักรู้ร่วมกันของทุกภาคส่วน ในการป้องกันตนเอง และลดความเสียหาย ตลอดจนลดอัตราการเกิดอาชญากรรมคอมพิวเตอร์

ภาคผนวก

ภาคผนวก ก หนังสือแสดงความยินยอมเข้าร่วมวิจัย



บันทึกข้อความ

ส่วนงาน คณะกรรมการพิจารณาจริยธรรมการวิจัยในคน กลุ่มสหสถาบัน ชุดที่ 1 โทร.0-2218-3202
ที่ จว 1105/2561 **วันที่** 9 ตุลาคม 2561
เรื่อง แจ้งผลผ่านการพิจารณาจริยธรรมการวิจัย

เรียน คณบดีคณะรัฐศาสตร์

สิ่งที่ส่งมาด้วย เอกสารแจ้งผ่านการรับรองผลการพิจารณา

ตามที่นิสิต/บุคลากรในสังกัดของท่านได้เสนอโครงการวิจัยเพื่อขอรับการพิจารณาจริยธรรมการวิจัย จากคณะกรรมการพิจารณาจริยธรรมการวิจัยในคน กลุ่มสหสถาบัน ชุดที่ 1 จุฬาลงกรณ์มหาวิทยาลัย นั้น ในการนี้ กรรมการผู้ทบทวนหลักได้เห็นสมควรให้ผ่านการพิจารณาจริยธรรมการวิจัยได้ ดังนี้

โครงการวิจัยที่ 193.1/61 เรื่อง กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล: การวิเคราะห์เพื่อพัฒนาเชิงนโยบาย (DIGITAL FORENSICS EVIDENCE PROVING PROCESS: AN ANALYTIC APPROACH TO POLICY DEVELOPMENT) **ของ นายกานต์ ศรีสุวรรณ** นิสิตระดับดุษฎีบัณฑิต ภาควิชาสังคมวิทยาและมานุษยวิทยา

จึงเรียนมาเพื่อโปรดทราบ

(ผู้ช่วยศาสตราจารย์ ดร.นันทรี ชัยชนะวงศาโรจน์)
กรรมการและเลขานุการ
คณะกรรมการพิจารณาจริยธรรมการวิจัยในคน
กลุ่มสหสถาบัน ชุดที่ 1 จุฬาลงกรณ์มหาวิทยาลัย

AF 04-07

ข้อมูลสำหรับผู้มีส่วนร่วมในการวิจัย

ชื่อโครงการวิจัย...กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล: การวิเคราะห์เพื่อพัฒนาเชิงนโยบาย....

ชื่อผู้วิจัย...นายกานต์ ศรีสุวรรณ.....ตำแหน่ง...นิสิตปริญญาเอก.....

สถานที่ติดต่อผู้วิจัย (ที่บ้าน) ...959/3 ถนนอิสรภาพ แขวงหิรัญรูจี เขตธนบุรี กทม. 10600.....

โทรศัพท์ที่บ้าน ...028902120.....โทรศัพท์มือถือ ...0816956666.....

E-mail : ∴karnt@karnt.com.....

1. ขอเรียนเชิญท่านเข้าร่วมในการวิจัยก่อนที่ท่านจะตัดสินใจเข้าร่วมในการวิจัย มีความจำเป็นที่ท่านควรทำความเข้าใจว่างานวิจัยนี้ทำเพราะเหตุใด และเกี่ยวข้องกับอะไร กรุณาใช้เวลาในการอ่านข้อมูลต่อไปนี้อย่างละเอียดรอบคอบ และสอบถามข้อมูลเพิ่มเติมหรือข้อมูลที่ไม่ชัดเจนได้ตลอดเวลา

2. โครงการนี้เกี่ยวข้องกับการวิจัยเรื่อง กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล และอาชญากรรมคอมพิวเตอร์

3. รายละเอียดของผู้มีส่วนร่วมในการวิจัย

- ผู้มีส่วนร่วมในการวิจัยคือผู้เกี่ยวข้องกับกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล ผู้มีความรู้ความชำนาญหรือมีสาขาอาชีพที่มีข้อมูลเกี่ยวกับอาชญากรรมคอมพิวเตอร์ หรือมีส่วนเกี่ยวข้องในกระบวนการยุติธรรมที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ *โดยใช้หลักเกณฑ์ประสบการณ์ ความเชี่ยวชาญอย่างน้อย 3 ปีนี้* ในการคัดเลือกผู้มีส่วนร่วมในการวิจัย เกณฑ์การคัดเข้าและเกณฑ์การคัดออก
- จำนวนทั้งหมด 20 ท่าน
- ผู้มีส่วนร่วมในการวิจัยได้จากการสุ่มตัวอย่างแบบเจาะจง
- การแบ่งกลุ่มผู้มีส่วนร่วมในการวิจัยมีแบ่งตามประเภทความชำนาญและอาชีพ เป็น 5 กลุ่ม กลุ่มละ 4 ท่าน

4. กระบวนการการวิจัยต่อผู้มีส่วนร่วมในการวิจัย ดำเนินการโดยผู้วิจัยตามรายชื่อข้างต้น จากการสัมภาษณ์เชิงลึกและการสนทนากลุ่ม *การสัมภาษณ์จะมีการสัมภาษณ์ 1 ครั้ง ใช้เวลาประมาณ 1 ชั่วโมง ตามสถานที่ซึ่งมีการนัดหมายกับผู้มีส่วนร่วมในการวิจัย ในประเด็นตามหัวข้อการวิจัย โดยหากข้อมูลไม่สมบูรณ์จะมีการกลับมาสัมภาษณ์เพิ่มเติมอีก 1 ครั้ง ใช้เวลาประมาณ 30 นาที*

การวิจัยนี้กลุ่มประชากรหรือผู้มีส่วนร่วมในการวิจัยมีการเปิดเผยข้อมูลส่วนตัวโดยได้รับการยินยอม มีการบันทึกความเห็น โดยได้รับการยินยอม *และเมื่อสิ้นสุดการวิจัยแล้ว การบันทึกความเห็นและเทปเสียงสัมภาษณ์จะถูกทำลาย ไม่มีการเก็บรักษาไว้*

5. กระบวนการให้ข้อมูลแก่กลุ่มประชากรหรือผู้มีส่วนร่วมในการวิจัย กระทำโดยผู้วิจัย ด้วยการให้ข้อมูลปากเปล่า และเอกสาร

6. **ประโยชน์**ในการเข้าร่วมวิจัย เพื่อจัดทำข้อเสนอแนะเชิงนโยบาย ข้อเสนอในการปรับปรุงกฎหมายและการบังคับใช้ ปรับปรุงมาตรฐานของกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลในประเทศไทยและกระบวนการยุติธรรมทางอาญาที่เกี่ยวข้องกับการกระทำความผิดทางคอมพิวเตอร์ในประเทศไทย เพื่อนำไปสู่การเพิ่มประสิทธิภาพในการป้องกันปราบปรามอาชญากรรมคอมพิวเตอร์ในประเทศไทย ให้สอดคล้องกับมาตรฐานสากล

V.2.4/2558

7. การเข้าร่วมในการวิจัยของท่านเป็นโดย**สมัครใจ** และสามารถ**ปฏิเสธ**ที่จะเข้าร่วมหรือถอนตัวจากการวิจัยได้ทุกขณะ โดยไม่ต้องให้เหตุผลและไม่สูญเสียประโยชน์ที่พึงได้รับ *การถอนตัวหรือปฏิเสธการเข้าร่วมจะไม่มีผลใดๆ ต่อองค์กร หรือการทำงานของท่าน ความเสี่ยงของการเข้าร่วมงานวิจัยอยู่ในระดับน้อยมาก มีความไม่สะดวกเพียงการสละเวลา เพื่อการสัมภาษณ์*

8. หากท่านมีข้อสงสัยให้สอบถามเพิ่มเติมได้โดยสามารถติดต่อผู้วิจัยได้ตลอดเวลา และหากผู้วิจัยมีข้อมูลเพิ่มเติมที่เป็นประโยชน์หรือโทษเกี่ยวกับการวิจัย ผู้วิจัยจะแจ้งให้ท่านทราบอย่างรวดเร็ว**เพื่อให้ผู้มีส่วนร่วมในการวิจัยทบทวนว่ายังสมัครใจจะอยู่ในงานวิจัยต่อไปหรือไม่**

9. ข้อมูลที่เกี่ยวข้องกับท่านจะเก็บเป็น**ความลับ** หากมีการเสนอผลการวิจัยจะเสนอเป็นภาพรวม ข้อมูลใดที่สามารถระบุถึงตัวท่านได้จะไม่ปรากฏในรายงาน

10. การวิจัยนี้ ไม่มีการจ่ายค่าพาหนะ หรือของที่ระลึก

11. "หากท่านไม่ได้รับการปฏิบัติตามข้อมูลดังกล่าวสามารถร้องเรียนได้ที่ คณะกรรมการพิจารณาจริยธรรมการวิจัยในคน กลุ่มสหสถาบัน ชุดที่ 1 จุฬาลงกรณ์มหาวิทยาลัย 254 อาคารจามจุรี 1 ชั้น 2 ถนนพญาไท เขตปทุมวัน กรุงเทพฯ 10330 โทรศัพท์/โทรสาร 0-2218-3202 E-mail: eccu@chula.ac.th"

ลงชื่อ.....
(ผศ. ดร. คมนีย์ จิตสว่าง)
อาจารย์ที่ปรึกษาวิทยานิพนธ์

เลขที่โครงการวิจัย 193.1/61
รับที่รับรอง - 5 ต.ค. 2561
วันหมดอายุ - 4 ต.ค. 2562

AF05-07

หนังสือแสดงความยินยอมเข้าร่วมการวิจัย

ทำที่.....

วันที่.....เดือน.....พ.ศ. .....

เลขที่ .....

ข้าพเจ้า ซึ่งได้ลงนามท้ายหนังสือนี้ ขอแสดงความยินยอมเข้าร่วมโครงการวิจัย

ชื่อโครงการวิจัย ...กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล: การวิเคราะห์เพื่อพัฒนาเชิงนโยบาย.....

ชื่อผู้วิจัย ....นายกานต์ ศรีสุวรรณ.....

ที่อยู่ที่ติดต่อ ...959/3 ถนนอิสรภาพ แขวงหิรัญรูจี เขตธนบุรี กรุงเทพมหานคร 10600.....โทรศัพท์ ...0816956666.....

ข้าพเจ้า **ได้รับทราบ**รายละเอียดเกี่ยวกับที่มาและวัตถุประสงค์ในการทำวิจัย รายละเอียดขั้นตอนต่างๆ ที่จะต้องปฏิบัติหรือได้รับการปฏิบัติ ความเสี่ยง/อันตราย และประโยชน์ซึ่งจะเกิดขึ้นจากการวิจัยเรื่องนี้ โดยได้อ่านรายละเอียดในเอกสารชี้แจงผู้เข้าร่วมการวิจัยโดยตลอด และ**ได้รับคำอธิบาย**จากผู้วิจัย **จนเข้าใจเป็นอย่างดี**แล้ว

ข้าพเจ้า**จึงสมัครใจ**เข้าร่วมในโครงการวิจัยนี้ ตามที่ระบุไว้ในเอกสารชี้แจงผู้เข้าร่วมการวิจัย โดยข้าพเจ้ายินยอม ให้ข้อมูลประกอบการวิจัยดังกล่าว *โดยการสัมภาษณ์ หรือสนทนากลุ่ม* เป็นระยะเวลาประมาณ 1 ชม. จำนวน 1 ครั้ง *ตามสถานที่ที่ได้มีการนัดหมายกับผู้วิจัยในประเด็นตามหัวข้อการวิจัย โดยหากข้อมูลไม่สมบูรณ์จะมีการกลับมาสัมภาษณ์เพิ่มเติมอีก 1 ครั้ง ใช้เวลาประมาณ 30 นาที* และทราบว่า เมื่อเสร็จสิ้นการวิจัยแล้ว *การบันทึกความเห็นและเทปเสียงสัมภาษณ์จะถูกทำลาย ไม่มีการเก็บไว้*

ข้าพเจ้ามีสิทธิ**ถอนตัว**ออกจากการวิจัยเมื่อใดก็ได้ตามความประสงค์ **โดยไม่ต้องแจ้งเหตุผล** ซึ่งการถอนตัวออกจากการวิจัยนั้น จะไม่มีผลกระทบในทางใดๆ ต่อข้าพเจ้า *การทำงานหรือองค์กรทั้งสิ้น ความเสี่ยงของการเข้าร่วมงานวิจัยอยู่ในระดับน้อยมาก มีความไม่สะดวกเพียงการสละเวลา เพื่อการสัมภาษณ์*

ข้าพเจ้าได้รับคำรับรองว่า ผู้วิจัยจะปฏิบัติต่อข้าพเจ้าตามข้อมูลที่ระบุไว้ในเอกสารชี้แจงผู้เข้าร่วมการวิจัย และข้อมูลใดๆ ที่เกี่ยวข้องกับข้าพเจ้า ผู้วิจัยจะ**เก็บรักษาเป็นความลับ** โดยจะนำเสนอข้อมูลการวิจัยเป็นภาพรวมเท่านั้น ไม่มีข้อมูลใดในการรายงานที่จะนำไปสู่การระบุตัวข้าพเจ้า

หากข้าพเจ้าไม่ได้รับการปฏิบัติตรงตามที่ได้ระบุไว้ในเอกสารชี้แจงผู้เข้าร่วมการวิจัย ข้าพเจ้าสามารถร้องเรียนได้ที่คณะกรรมการพิจารณาจริยธรรมการวิจัยในคน กลุ่มสหสถาบัน ชุดที่ 1 จุฬาลงกรณ์มหาวิทยาลัย 254 อาคารจามจุรี 1 ชั้น 2 ถนนพญาไท เขตปทุมวัน กรุงเทพฯ 10330 โทรศัพท์/โทรสาร 0-2218-3202

E-mail: eccu@chula.ac.th

ข้าพเจ้าได้ลงลายมือชื่อไว้เป็นสำคัญต่อหน้าอาจารย์ที่ปรึกษาวิทยานิพนธ์ ทั้งนี้ข้าพเจ้าได้รับสำเนาเอกสารชี้แจงผู้เข้าร่วมการวิจัย และสำเนาหนังสือแสดงความยินยอมไว้แล้ว

ลงชื่อ.....
(.....)
ผู้วิจัยหลัก

ลงชื่อ.....
(.....)
ผู้มีส่วนร่วมในการวิจัย

ลงชื่อ.....
(.....)
อาจารย์ที่ปรึกษาวิทยานิพนธ์

เลขที่โครงการวิจัย 193.1/61
วันที่รับรอง - 5 ต.ค. 2561
วันหมดอายุ - 4 ต.ค. 2562

V.2.4/2558

ภาคผนวก ข ใบรับรองโครงการวิจัย

AF 01-12

คณะกรรมการพิจารณาจริยธรรมการวิจัยในคน กลุ่มสหสถาบัน ชุดที่ 1 จุฬาลงกรณ์มหาวิทยาลัย
254 อาคารจามจุรี 1 ชั้น 2 ถนนพญาไท เขตปทุมวัน กรุงเทพฯ 10330
โทรศัพท์/โทรสาร: 0-2218-3202 E-mail: eccu@chula.ac.th

COA No. 232/2561

ใบรับรองโครงการวิจัย

โครงการวิจัยที่ 193.1/61 : กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล: การวิเคราะห์เพื่อพัฒนาเชิงนโยบาย

ผู้วิจัยหลัก : นายกานต์ ศรีสุวรรณ

หน่วยงาน : คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

คณะกรรมการพิจารณาจริยธรรมการวิจัยในคน กลุ่มสหสถาบัน ชุดที่ 1 จุฬาลงกรณ์มหาวิทยาลัย ได้พิจารณา โดยใช้หลัก ของ The International Conference on Harmonization – Good Clinical Practice (ICH-GCP) อนุมัติให้ดำเนินการศึกษาวิจัยเรื่องดังกล่าวได้

ลงนาม.....
(รองศาสตราจารย์ นายแพทย์ปรีดา ทัศนประดิษฐ)
ประธาน

ลงนาม.....
(ผู้ช่วยศาสตราจารย์ ดร.นันทรี ชัยชนะวงศาโรจน์)
กรรมการและเลขานุการ

วันที่รับรอง : 5 ตุลาคม 2561 **วันหมดอายุ** : 4 ตุลาคม 2562

เอกสารที่คณะกรรมการรับรอง

1) โครงการวิจัย
2) ข้อมูลสำหรับกลุ่มประชากรหรือผู้มีส่วนร่วมในการวิจัยและใบยินยอมของกลุ่มประชากรหรือผู้มีส่วนร่วมในการวิจัย
3) ผู้วิจัย

เอกสารรับรองโครงการวิจัยที่ 193.1/61
วันที่รับรอง - 5 ต.ค. 2561
วันหมดอายุ - 4 ต.ค. 2562

เงื่อนไข

1. *ข้าพเจ้ารับทราบว่าเป็นการผิดจริยธรรม หากดำเนินการเก็บข้อมูลการวิจัยก่อนได้รับการอนุมัติจากคณะกรรมการพิจารณาจริยธรรมการวิจัยฯ*
2. *หากใบรับรองโครงการวิจัยหมดอายุ การดำเนินการวิจัยต้องยุติ เมื่อต้องการต่ออายุต้องขออนุมัติใหม่ล่วงหน้าไม่ต่ำกว่า 1 เดือน พร้อมส่งรายงานความก้าวหน้าการวิจัย*
3. *ต้องดำเนินการวิจัยตามที่ระบุไว้ในโครงการวิจัยอย่างเคร่งครัด*
4. *ใช้เอกสารข้อมูลสำหรับกลุ่มประชากรหรือผู้มีส่วนร่วมในการวิจัย ใบยินยอมของกลุ่มประชากรหรือผู้มีส่วนร่วมในการวิจัย และเอกสารเชิญเข้าร่วมวิจัย (ถ้ามี) **เฉพาะที่ประทับตราคณะกรรมการเท่านั้น***
5. *หากเกิดเหตุการณ์ไม่พึงประสงค์ร้ายแรงในสถานที่เก็บข้อมูลที่ขออนุมัติจากคณะกรรมการ ต้องรายงานคณะกรรมการภายใน 5 วันทำการ*
6. *หากมีการเปลี่ยนแปลงการดำเนินการวิจัย ให้ส่งคณะกรรมการพิจารณารับรองก่อนดำเนินการ*
7. *โครงการวิจัยไม่เกิน 1 ปี ส่งแบบรายงานสิ้นสุดโครงการวิจัย (AF 03-12) และบทคัดย่อผลการวิจัยภายใน 30 วัน เมื่อโครงการวิจัยเสร็จสิ้น สำหรับโครงการวิจัยที่เป็นวิทยานิพนธ์ให้ส่งบทคัดย่อผลการวิจัย ภายใน 30 วัน เมื่อโครงการวิจัยเสร็จสิ้น*

AF 02-12

The Research Ethics Review Committee for Research Involving Human Research Participants, Health Sciences Group, Chulalongkorn University
Jamjuree 1 Building, 2nd Floor, Phyathai Rd., Patumwan district, Bangkok 10330, Thailand,
Tel/Fax: 0-2218-3202 E-mail: eccu@chula.ac.th

COA No. 232/2018

Certificate of Approval

Study Title No. 193.1/61 : DIGITAL FORENSICS EVIDENCE PROVING PROCESS: AN ANALYTIC APPROACH TO POLICY DEVELOPMENT

Principal Investigator : MR. KARNT SRISUWAN

Place of Proposed Study/Institution : Faculty of Political Science, Chulalongkorn University

The Research Ethics Review Committee for Research Involving Human Research Participants, Health Sciences Group, Chulalongkorn University, Thailand, has approved constituted in accordance with the International Conference on Harmonization – Good Clinical Practice (ICH-GCP).

Signature: ..... Signature: .....

(Associate Professor Prida Tasanapradit, M.D.) (Assistant Professor Nuntaree Chaichanawongsaroj, Ph.D.)

Chairman Secretary

Date of Approval : 5 October 2018 Approval Expire date : 4 October 2019

Protocol No. 193.1/61
Date of Approval -5 OCT 2018
Approval Expire Date -4 OCT 2019

The approval documents including

1) Research proposal
2) Patient/Participant Information Sheet and Informed Consent Form
3) Researcher

The approved investigator must comply with the following conditions:

1. *The research/project activities must end on the approval expired date of the Research Ethics Review Committee for Research Involving Human Research Participants, Health Sciences Group, Chulalongkorn University (RECCU). In case the research/project is unable to complete within that date, the project extension can be applied one month prior to the RECCU approval expired date.*
2. *Strictly conduct the research/project activities as written in the proposal.*
3. *Using only the documents that bearing the RECCU's seal of approval with the subjects/volunteers (including subject information sheet, consent form, invitation letter for project/research participation (if available).*
4. *Report to the RECCU for any serious adverse events within 5 working days*
5. *Report to the RECCU for any change of the research/project activities prior to conduct the activities.*
6. *Final report (AF 03-12) and abstract is required for a one year (or less) research/project and report within 30 days after the completion of the research/project. For thesis, abstract is required and report within 30 days after the completion of the research/project.*
7. *Annual progress report is needed for a two- year (or more) research/project and submit the progress report before the expire date of certificate. After the completion of the research/project processes as No. 6.*

ภาคผนวก ค
แบบสัมภาษณ์ความคิดเห็น และแบบบันทึกการสัมภาษณ์
เรื่อง กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล: การวิเคราะห์เพื่อพัฒนาเชิงนโยบาย

คำถามวิจัยเชิงคุณภาพสำหรับผู้ให้ข้อมูลสำคัญ

ส่วนที่ 1: ข้อมูลทั่วไป ชื่อ สกุล ประวัติส่วนตัว อายุงาน และประวัติการทำงานอย่างย่อในส่วนที่เกี่ยวข้องกับการตรวจพิสูจน์พยานหลักฐานดิจิทัล และอาชญากรรมคอมพิวเตอร์ของผู้ให้สัมภาษณ์

- ชื่อ
- เพศ
- อายุ
- ตำแหน่งและอายุงาน
- ประสบการณ์ทำงาน

ส่วนที่ 2: คำถามปลายเปิด คำถามทั่วไป เกี่ยวกับ การตรวจพิสูจน์พยานหลักฐานดิจิทัล และสถานการณ์อาชญากรรมคอมพิวเตอร์ ในประเทศไทย

- ท่านมีขั้นตอนการตรวจพิสูจน์พยานหลักฐานดิจิทัล และ/หรือ การดำเนินคดีอาชญากรรมคอมพิวเตอร์อย่างไร ขั้นตอนการรับแจ้งเรื่อง ลักษณะการกระทำผิดที่พบ รายละเอียดการทำงานและการประสานหน่วยงานอื่นๆ
- พื้นที่ หรืออำนาจหน้าที่ความรับผิดชอบของท่าน มีอาชญากรรมคอมพิวเตอร์หรือความเกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์มากน้อยเพียงใด อย่างไร ประสบการณ์การบังคับใช้กฎหมาย
- แนวโน้มปัญหาอาชญากรรมคอมพิวเตอร์ ลักษณะคดี รายละเอียด ความถี่ เป็นอย่างไร

ส่วนที่ 3: คำถามปลายเปิด เกี่ยวกับ ปัญหาและอุปสรรคของการทำงาน การตรวจพิสูจน์พยานหลักฐานดิจิทัล และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

- ปัญหา และอุปสรรคที่พบ ทั้งในด้านกฎหมาย เทคโนโลยี วิธีการ ความรู้ความเชี่ยวชาญที่จำเป็นในการปฏิบัติงานและอื่นๆ ของการตรวจพิสูจน์พยานหลักฐานดิจิทัลและคดีอาชญากรรมคอมพิวเตอร์ มีอะไรบ้าง
- การตีความแต่ละมาตรา และการใช้อำนาจภายใต้ พระราชบัญญัติคอมพิวเตอร์ พ.ศ. 2560 ชัดเจนหรือไม่ มีปัญหา และอุปสรรคหรือไม่ อย่างไร
- มุมมองของภาคประชาขน ทัศนคติเกี่ยวกับการตรวจพิสูจน์พยานหลักฐานดิจิทัล อาชญากรรมคอมพิวเตอร์ และประเด็นสิทธิ เสรีภาพ ประเด็นประมวลกฎหมายอาญา มาตรา 112 รวมถึงประเด็นทางสังคมอื่นๆ เป็นอย่างไร มีอะไรบ้าง

<u>ส่วนที่ 4</u>: คำถามปลายเปิด เกี่ยวกับความคิดเห็นและข้อเสนอแนะ ต่อมาตรฐานการตรวจพิสูจน์พยานหลักฐานดิจิทัลในประเทศไทย และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

- ความคิดเห็นต่อกระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัลในปัจจุบัน มาตรฐาน ข้อกำหนด กฎหมายอื่น และอื่นๆ ที่เกี่ยวข้อง การปรับปรุง พัฒนา
- ความคิดเห็นด้านความเหมาะสมของ พระราชบัญญัติคอมพิวเตอร์ พ.ศ. 2560 กับบริบทของสังคมไทย ความก้าวหน้าทางเทคโนโลยี และการพลิกผันทางดิจิทัล
- ข้อเสนอแนะ เพื่อแก้ไข ปรับปรุง พระราชบัญญัติคอมพิวเตอร์ พ.ศ. 2560 ทั้งด้านกฎหมายและด้านการบังคับใช้

ประวัติผู้เขียน

ชื่อ-สกุล	กานต์ ศรีสุวรรณ
วัน เดือน ปี เกิด	15 ธันวาคม 2518
สถานที่เกิด	กรุงเทพมหานคร
วุฒิการศึกษา	มัธยมศึกษาตอนปลาย โรงเรียนสวนกุหลาบวิทยาลัย ปริญญาตรี วิทยาศาสตร์บัณฑิต สาขาวิทยาการคอมพิวเตอร์ วิทยาลัยนานาชาติ มหาวิทยาลัยมหิดล ปริญญาโท บริหารธุรกิจมหาบัณฑิต มหาวิทยาลัยรามคำแหง ปริญญาโท รัฐประศาสนศาสตรมหาบัณฑิต มหาวิทยาลัยรามคำแหง 2558-2564: ปริญญาเอก ศิลปศาสตรดุษฎีบัณฑิต สาขาอาชญาวิทยาและงานยุติธรรม จุฬาลงกรณ์มหาวิทยาลัย
ที่อยู่ปัจจุบัน	959/3 ถนนอิสรภาพ แขวงหิรัญรูจี เขตธนบุรี กรุงเทพมหานคร 10600
ผลงานตีพิมพ์	- บทความเรื่อง “ขั้นตอนการจับกุมดำเนินคดีอาชญากรรมคอมพิวเตอร์ กรณีศึกษาการหมิ่นประมาททางโซเชียลมีเดีย” - บทความเรื่อง “กระบวนการตรวจพิสูจน์พยานหลักฐานดิจิทัล: การวิเคราะห์เพื่อพัฒนาเชิงนโยบาย”
รางวัลที่ได้รับ	- ทุนการศึกษาหลักสูตรดุษฎีบัณฑิต “100 ปี จุฬาลงกรณ์มหาวิทยาลัย” (The 100th Anniversary Chulalongkorn University Fund for Doctoral Scholarship) - ทุน 90 ปี จุฬาลงกรณ์มหาวิทยาลัย กองทุนรัชดาภิเษกสมโภช [The 90th Anniversary of Chulalongkorn University Fund (Ratchadaphiseksomphot Endowment Fund)]

บรรณานุกรม

กรรณิกา ภัทรวิศิษฏ์สัณธ์. “Digital Forensics 101 (ตอนที่ 1).” สืบค้นเมื่อ 22 สิงหาคม 2560 http://www.thaicert.or.th/papers/general/2013/pa2013ge012.html

การตรวจพิสูจน์พยานหลักฐานทางดิจิทัลหรือคอมพิวเตอร์”, www.orionforensics.com, สืบค้นเมื่อ 14 ก.พ. 2561, http://www.orionforensics.com/w_th_page/digital-forensics_th.php

การป้องกันอาชญากรรมเชิงรุก โดย ทฤษฎีสามเหลี่ยมอาชญากรรม”, blogspot.com, สืบค้นเมื่อ 14 ก.พ. 2561, http://phoklangpolice.blogspot.com/2016/10/blog-post.html

โกวิท หนูโยม. “การรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในคดีแพ่ง.” วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2551

เข็มชัย ชุติวงศ์. (2551). กฎหมายลักษณะพยาน (พิมพ์ครั้งที่ 8). กรุงเทพฯ: นิติบรรณการ.

คณิต ณ นคร, กฎหมายอาญาภาคความผิด (พิมพ์ครั้งที่ 6), 2539. กรุงเทพมหานคร: สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์

ความหมาย และอาชญากรคอมพิวเตอร์, gotoknow.org, สืบค้นเมื่อ 26 ธ.ค. 2560, https://www.gotoknow.org/posts/372559

ความหมายของอาชญากรรม, secnia.go.th, สืบค้นเมื่อ 26 ธ.ค. 2560, https://www.secnia.go.th/2016/01/13/ความหมายของอาชญากรรม/

จรัญ ภักดีธนากุล. (2555). กฎหมายลักษณะพยานหลักฐาน (พิมพ์ครั้งที่ 6). กรุงเทพฯ: สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิต.

จุลศักดิ์ แก้วกาญจน์, โครงการศึกษาเผยแพร่ความรู้ด้านนิติวิทยาศาสตร์คอมพิวเตอร์, thainetizen.org, สืบค้นเมื่อ 25 ธ.ค. 2560, https://thainetizen.org/2015/03/csdig-digital-forensics/

เจษฎา คารินทร์. “ปัญหาทางกฎหมายเกี่ยวกับการรับฟังพยานหลักฐานทางอิเล็กทรอนิกส์ในคดีอาญา.” วารสาร มหาจุฬานาครทรรศ์ 6, ฉ.9 (2562): 4549-4550.

ชัยวัฒน์ วงศ์วัฒนศานต์, ทวีศักดิ์ กออนันตกูล และ สุรางคณา แก้วจานงค์. (2545). คำอธิบายพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544. กรุงเทพมหานคร:

ธีระวัฒน์ พุฒิบูรณวัฒน์. “แนวทางการปรับปรุงยุทธศาสตร์สำนักงานอัยการสูงสุดด้านการอำนวยความยุติธรรมทางอาญาเพื่อตอบโต้อาชญากรรมคอมพิวเตอร์ในยุคประเทศไทย 4.0”.

นัยนรัตน์ งามแสง,ร.ต.ท.. (2547).อาชญากรรมคอมพิวเตอร์ : ศึกษาเฉพาะกรณีปัจจัยที่มีผลต่อการเกิดปัญหาอาชญากรรมบนอินเตอร์เน็ต, วิทยานิพนธ์ศิลปศาสตรมหาบัณฑิต (การบริหารงานยุติธรรม), มหาวิทยาลัยธรรมศาสตร์.

น้ำแท้ มีบุญสล้าง, กระบวนการยุติธรรมทางอาญาเปรียบเทียบ. 2554. กรุงเทพมหานคร: สูตรไพศาล

ประมูล สุวรรณศร. (2526). คำอธิบายกฎหมายลักษณะพยานหลักฐาน. กรุงเทพมหานคร: สำนักพิมพ์นิติบรรณการ.

ปิติกุล จิระมงคลพาณิชย์. (2548). คำอธิบายกฎหมายลักษณะพยาน:ว่าด้วยพยานเอกสาร. กรุงเทพมหานคร: สำนักพิมพ์วิญญูชน.

แผนแม่บทเทคโนโลยีสารสนเทศกระบวนการยุติธรรม พ.ศ.2559-2562 เรื่องนโยบายทิศทางและกฎหมายที่เกี่ยวข้องกับการพัฒนาเทคโนโลยีสารสนเทศ.

พ.ต.อ.ดร.พรชัย ขันตี, ทฤษฎีอาชญาวิทยา : หลักการ งานวิจัย และนโยบายประยุกต์ (กรุงเทพมหานคร: ส.เจริญการพิมพ์, 2558). หน้า 86, 184, 198-200, 201-202.

พกรณ์ รักษาชาติ, อาชญากรรมอิเล็กทรอนิกส์ : กรณีศึกษาอาชญากรรมบนเครือข่ายอินเทอร์เน็ต, grad.kbu.ac.th, สืบค้นเมื่อ 10 กรกฎาคม 2561, http://grad.kbu.ac.th/pdf/sar_data52/d3-52.pdf

พรเพชร วิชิตชลชัย. (2546). ข้อบังคับว่าด้วยพยานหลักฐานของศาลสหรัฐอเมริกา พร้อมคำแปล. กรุงเทพมหานคร: ผู้แต่ง.

พรเพชร วิชิตชลลัย. คำอธิบายกฎหมายลักษณะพยาน. พิมพ์ครั้งที่ 4. กรุงเทพฯ: สำนักอบรมศึกษากฎหมายแห่ง เนติบัณฑิตยสภา, 2555.

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560, ราชกิจจานุเบกษา. เล่มที่ 134 (ตอนที่ 10 ก), 24 มกราคม 2560, หน้า 24-35.

พิชญ์ พงษ์สวัสดิ์. “อาชญากรรมคอมพิวเตอร์ แฮกเกอร์ แฮกติวิสต์?”, matichon.co.th, สืบค้นเมื่อ 26 ธ.ค. 2560, https://www.matichon.co.th/news-monitor/news_413499

พิชศาล พันธุ์วัฒนา. (2562). ความน่าเชื่อถือในการนำเอกสารอิเล็กทรอนิกส์มาใช้เป็นพยานหลักฐาน. วารสารวิชาการอาชญาวิทยาและนิติวิทยาศาสตร์ โรงเรียนายร้อยตำรวจ. 5(1), 146.

พินัย ณ นคร. “กฎหมายว่าด้วยพาณิชย์อิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์.” เล่มที่ 56. บทบัณฑิตย์. (2543) : 1-42.

ไพจิตร สวัสดิสาร. (2557). การใช้คอมพิวเตอร์ทางกฎหมายและกฎหมายที่เกี่ยวกับคอมพิวเตอร์. กรุงเทพมหานคร: บริษัท ชวนพิมพ์ 50 จำกัด

พัชรา สินลอยมา. “การแก้ไขปัญหาอาชญากรรมด้วยนิติวิทยาศาสตร์”, www.oja.go.th, สืบค้นเมื่อ 14 ก.พ. 2561, http://www.oja.go.th/th/wp-content/uploads/course/26-1-60.doc

ภัยไซเบอร์ในปี 2021 ทิศทางจะเป็นอย่างไร, www.cyfence.com, สืบค้นเมื่อ 11 ส.ค. 2564, https://www.cyfence.com/article/next-it-security-trend-2021/

มานิตย์ จุมปา. (2554). คำอธิบายกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์. กรุงเทพมหานคร: บริษัท สำนักพิมพ์วิญญูชน จำกัด.

รายงาน การวิจัยเพื่อพัฒนากระบวนการสืบสวนและสอบสวนของเจ้าหน้าที่ตำรวจในการรับมือกับอาชญากรรมคอมพิวเตอร์”, research.police.go.th, สืบค้นเมื่อ 26 ธ.ค. 2560, http://research.police.go.th/index.php/datacenter/research/2558/-2559-1/342---67/file

เลิศชาย สุธรรมพร, (2541). อาชญากรรมคอมพิวเตอร์: ศึกษาเฉพาะกรณีความปลอดภัยของข้อมูล, กรุงเทพมหานคร: สำนักพิมพ์จุฬาลงกรณ์มหาวิทยาลัย

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

วัลลิกา อุ่นศรี. “ปัญหาการรวบรวมและพิสูจน์พยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ในคดีอาญา.” วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2544

ศูนย์ดิจิทัลฟอเรนสิกส์. ข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐานดิจิทัล. กรุงเทพฯ: สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2559.

เศรษฐพงค์ มะลิสุวรรณ. The Year of Disruption, tct.or.th, สืบค้นเมื่อ 12 เม.ย. 2561, http://tct.or.th/images/article/special_article/25610110/198410_Disruption.pdf.

สรุปผลที่สำคัญ สำรวจการมีการใช้เทคโนโลยีสารสนเทศและการสื่อสารในครัวเรือน พ.ศ. 2563 สำนักงานสถิติแห่งชาติ, www.nso.go.th, สืบค้นเมื่อ 9 ก.ย. 2564, http://www.nso.go.th/sites/2014/DocLib13/ด้านICT/เทคโนโลยีในครัวเรือน/2563/Pocketbook63.pdf.

สำนักงานตำรวจแห่งชาติ. (2553). เรื่องกระบวนการเก็บรวบรวมและรักษาความน่าเชื่อถือของพยานหลักฐานทางอิเล็กทรอนิกส์. กรุงเทพมหานคร: โรงพิมพ์ตำรวจ สำนักงานตำรวจแห่งชาติ

สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ.

สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์, แนวทางการจัดทำกฎหมายอาชญากรรมทางคอมพิวเตอร์, 2546 กรุงเทพมหานคร: ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

นเลิศ สุขุม. (2543). ปัจจัยที่มีผลต่อประสิทธิภาพในการป้องกันปราบปรามอาชญากรรมคอมพิวเตอร์ของเจ้าหน้าที่ตำรวจกองบังคับการสืบสวนสอบสวนคดีเศรษฐกิจ. ปริญญาสังคมวิทยามหาบัณฑิต จุฬาลงกรณ์มหาวิทยาลัย

สุมนทิพย์ จิตสว่างและคณะ, รายงานการวิจัยเรื่องบทบาทขององค์กรปกครองส่วนท้องถิ่นในการป้องกันปัญหาอาชญากรรม, (กรุงเทพฯ:คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2560). หน้า 24.

สุรพันธ์ มั่นคงดี. (2541). พยานหลักฐานในคดีอาชญากรรมคอมพิวเตอร์, กรุงเทพมหานคร: สำนักพิมพ์จุฬาลงกรณ์มหาวิทยาลัย

อาชญากรรมบนสะพานลอยในกรุงเทพมหานคร”, digi.library.tu.ac.th, สืบค้นเมื่อ 14 ก.พ. 2561, http://digi.library.tu.ac.th/thesis/sw/2258/09CHAPTER_2.pdf

เอกสารวิจัย, หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ 59, วิทยาลัยป้องกันราชอาณาจักร, 2560.

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

Andrew Smith. (2560). Required Skills for Digital Forensics Investigators, from http://www.orionforensics.com/2020/06/20/required-skills-for-digital-forensics-investigators-orion-forensics/

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

Council of Europe, Explanatory Note to Convention on Cybercrime [Online]. [20 มิถุนายน 2559]

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

Federal Bureau of Investigation. “Digital Evidence : Standards and Principles”.

Guofu Ma, Zixian Wang, Likun Zou, Qian Zhang a*. (2011). Computer Forensics Model Based on Evidence Ring and Evidence Chain. The Central Institute for Correctional Police.

J. Robert Lilly and others. Criminological Theory 6th Edition. page 4.

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.

Martin Novak. (2020). Digital Evidence in Criminal Cases Before The U.S. Courts of Appeal:Trends and IssuesForConsideration.RetrievedOctober5, 2020, from https:// com.mons.erau.edu/cgi/viewcontent.cgi?article=1609&context=jdfsl.

(Online). Available : https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm#Proposed, 2018.

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)

Top 12 Cyber Crime Facts and Statistics, www.blue-pencil.ca, สืบค้นเมื่อ 8 ก.ย. 2564, https://www.blue-pencil.ca/top-12-cyber-crime-facts-and-statistics/

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