สิทธิที่จะไม่ให้การเป็นปฏิปักษ์ต่อตนเองกับการแสวงหาพยานหลักฐานดิจิทัลในชั้นสอบสวนของประเทศไทย
The Right Against Self-Incrimination and Acquisition of Digital Evidence in the Investigatory Phase in Thailand

ภาวิณี คุ้นสงคราม
Phawinee Kunsongklam
คณะนิติศาสตร์และรัฐศาสตร์ วิทยาลัยนอร์ทเทิร์น
Faculty of Law and Political Science, Northren College
Email: Phawinee.mungming@gmail.com

รับบทความ (Received): 8 ม.ค. 2569
ปรับแก้ไข (Revised): 6 มี.ค. 2569
ตอบรับบทความ (Accepted): 10 มี.ค. 2569

บทคัดย่อ

การวิจัยนี้ มีวัตถุประสงค์เพื่อวิเคราะห์ปัญหาทางกฎหมายและการปฏิบัติที่ส่งผลกระทบต่อสิทธิที่จะไม่ให้การเป็นปฏิปักษ์ต่อตนเองของผู้ต้องหา (Right Against Self-Incrimination) อันเนื่องมาจากการแสวงหาพยานหลักฐานดิจิทัลที่เพิ่มขึ้นอย่างรวดเร็วในคดีอาญา โดยเฉพาะอย่างยิ่งในชั้นพนักงานสอบสวน การวิจัยใช้วิธีดำเนินการวิจัยเชิงคุณภาพ (Qualitative Research) ด้วยการวิจัยเอกสาร (Documentary Research) เพื่อวิเคราะห์หลักกฎหมายรัฐธรรมนูญ และแนวคำพิพากษาที่เกี่ยวข้อง รวมถึงการสัมภาษณ์เชิงลึก (In-depth Interview) ผู้เชี่ยวชาญด้านกฎหมายและเทคโนโลยี ผลการวิจัยเบื้องต้นพบว่า การเข้าถึงข้อมูล

ดิจิทัลที่ถูกเข้ารหัส (Encrypted Data) หรือข้อมูลในระบบคลาวด์ (Cloud-based Data) โดยปราศจากความยินยอม อาจเป็นการละเมิดสิทธิของผู้ต้องหาโดยปริยาย เนื่องจากเป็นการบังคับให้ต้องเปิดเผยข้อมูลที่เป็นความลับส่วนบุคคล งานวิจัยนี้จึงมุ่งเสนอแนวทางปฏิรูปกฎหมายและกำหนดแนวทางการปฏิบัติงานของพนักงานสอบสวนให้ชัดเจน เพื่อสร้างความสมดุลระหว่างการคุ้มครองสิทธิของผู้ต้องหาตามหลักนิติธรรมกับการเพิ่มประสิทธิภาพในการสอบสวนคดีอาชญากรรมทางเทคโนโลยี

คำสำคัญ: สิทธิที่จะไม่ให้การเป็นปฏิปักษ์ต่อตนเอง, พยานหลักฐานดิจิทัล, การสอบสวนคดีอาญา

Abstract

This research aims to analyze legal and practical issues impacting the Right Against Self-Incrimination of the accused due to the rapid increase in the search for digital evidence in criminal cases, specifically during the investigatory phase. The study employs a qualitative methodology, combining documentary research, analyzing relevant laws, the Constitution, and judicial precedents with In-depth Interviews of legal and technology experts. Preliminary findings indicate that accessing encrypted or cloud-based data without consent may constitute an implicit violation of the accused's rights, as it compels the disclosure of private information. This research proposes legal reforms and clear operational guidelines for investigators to balance the protection of the accused's rights under the Rule of Law principle with enhancing the efficiency of investigating technology-related crimes.

Keywords: Right Against Self-Incrimination, Digital Evidence, Criminal Investigations

บทนำ

ในยุคดิจิทัล การดำเนินคดีอาญาของประเทศไทยได้เผชิญปัญหาทางกฎหมายที่สำคัญจากการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศและการสื่อสาร ข้อมูลอิเล็กทรอนิกส์ได้กลายเป็นพยานหลักฐานสำคัญในเกือบทุกประเภทคดี ไม่ว่าจะเป็นข้อมูลจากโทรศัพท์มือถือ บัญชีสื่อสังคมออนไลน์ กล้องวงจรปิด หรือระบบฐานข้อมูลคลาวด์ พยานหลักฐานเหล่านี้มีศักยภาพในการพิสูจน์ความผิดหรือความบริสุทธิ์ของบุคคลได้อย่างแม่นยำ แต่ในขณะเดียวกัน การเข้าถึงหรือรวบรวมข้อมูลดังกล่าว โดยเจ้าพนักงานก็อาจกระทบต่อสิทธิขั้นพื้นฐานของบุคคล โดยเฉพาะสิทธิที่จะไม่ให้การเป็นปฏิปักษ์ต่อตนเอง ซึ่งเป็นหลักการสำคัญในกระบวนการยุติธรรมอาญาที่อยู่ในระดับสากล

หลักสิทธินี้ได้รับการรับรองทั้งในกฎหมายระหว่างประเทศและภายในประเทศ เช่น มาตรา 14 วรรค 3 (g) แห่งกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (ICCPR) และรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 มาตรา 29 วรรคสอง ที่บัญญัติว่า ผู้ถูกกล่าวหาหรือจำเลยย่อมมีสิทธิที่จะไม่ให้การเป็นปฏิปักษ์ต่อตนเอง หลักการดังกล่าวมีเป้าหมายเพื่อป้องกันการบังคับให้บุคคลต้องเปิดเผยข้อมูลหรือพยานหลักฐานที่อาจใช้กล่าวหาตนเอง ซึ่งเป็นหัวใจของการคุ้มครองสิทธิมนุษยชนในกระบวนการยุติธรรม

อย่างไรก็ดี การประยุกต์ใช้หลักสิทธินี้ในทางปฏิบัติ โดยเฉพาะในบริบทของพยานหลักฐานดิจิทัลยังมีความซับซ้อนและคลุมเครือ เช่น กรณีพนักงานสอบสวนขอให้ผู้ต้องหามอบรหัสผ่านโทรศัพท์มือถือหรือรหัสผ่านบัญชีสื่อออนไลน์ เพื่อเข้าถึงข้อมูลที่เกี่ยวข้องกับคดี หากผู้ต้องหาปฏิเสธ อาจได้รับการพิจารณาว่าผู้ต้องหาไม่ให้ความร่วมมือในการสอบสวน แต่หากยินยอมก็อาจถูกใช้ข้อมูลนั้นเป็นพยานหลักฐานกล่าวหาในภายหลัง ปัญหานี้ก่อให้เกิดคำถามสำคัญว่า การบังคับหรือร้องขอให้ผู้ต้องหาเปิดเผยข้อมูลดิจิทัลดังกล่าวเป็นการละเมิดสิทธิที่จะไม่ให้การเป็นปฏิปักษ์ต่อตนเองหรือไม่ และรัฐควรมีแนวทางใดในการถ่วงดุลระหว่างสิทธิและเสรีภาพของบุคคลกับประสิทธิภาพของกระบวนการยุติธรรม

ในต่างประเทศ เช่น สหรัฐอเมริกาและสหภาพยุโรป ได้มีการพัฒนาแนวคำพิพากษาเกี่ยวกับการใช้สิทธิไม่ให้การเป็นปฏิปักษ์ต่อตนเองในกรณีที่เกี่ยวข้องกับข้อมูลดิจิทัลอย่างต่อเนื่อง เช่น คำพิพากษาศาลสูงสหรัฐฯ คดี *Riley v. California* (2014) ที่วางหลักว่า การตรวจค้นโทรศัพท์มือถือของผู้ต้องหาต้องได้รับหมายศาล และคดี *United States v. Hubbell* (2000) ซึ่งศาลวินิจฉัยว่า การบังคับให้เปิดเผยรหัสผ่านอาจถือเป็นการละเมิดสิทธิดังกล่าว หลักการเหล่านี้สะท้อนถึงแนวโน้มของโลกที่ให้ความสำคัญกับการตีความสิทธิในเชิงคุ้มครองบุคคลมากขึ้น

สำหรับประเทศไทย แม้จะมีการตราพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และมีการแก้ไขเพิ่มเติมกฎหมายเพื่อรองรับการตรวจสอบและรวบรวมหลักฐานทางดิจิทัล แต่ยังไม่มีแนวทางชัดเจนในส่วนขอบเขตหน้าที่และอำนาจของเจ้าพนักงานในการขอความร่วมมือจากผู้ต้องหาว่าควรอยู่ในกรอบใด จึงจะไม่ละเมิดสิทธิตามกฎหมายรัฐธรรมนูญ การศึกษาในครั้งนี้ จึงมีความจำเป็นเพื่อแสดงให้เห็นถึงปัญหาช่องว่างทางกฎหมาย แนวทางปฏิบัติที่เหมาะสม และข้อเสนอเพื่อพัฒนากระบวนการยุติธรรมให้สอดคล้องกับหลักสิทธิมนุษยชนสากล

ด้วยเหตุนี้ การวิจัยในประเด็นดังกล่าว จึงมีความจำเป็นอย่างยิ่งในการศึกษาถึงขอบเขตการใช้สิทธิที่จะไม่ให้การเป็นปฏิปักษ์ต่อตนเองของผู้ต้องหาในบริบทของพยานหลักฐานดิจิทัล เพื่อกำหนดแนวทางในการใช้และการตีความกฎหมาย รวมทั้งแนวทางการปฏิบัติที่ชัดเจน อันจะนำไปสู่การสร้างความสมดุลระหว่างการคุ้มครองสิทธิของผู้ต้องหาและการรักษาประสิทธิภาพในการอำนวยความยุติธรรมทางอาญาของรัฐ

วัตถุประสงค์การวิจัย

1. เพื่อวิเคราะห์หลักการคุ้มครอง สิทธิที่จะไม่ให้การเป็นปฏิปักษ์ต่อตนเองของผู้ต้องหาตามกฎหมายรัฐธรรมนูญและกฎหมายวิธีพิจารณาความอาญาของประเทศไทย

2. เพื่อศึกษาและวิเคราะห์ปัญหาทางกฎหมายและปัญหาในทางปฏิบัติของการแสวงหาพยานหลักฐานดิจิทัลในชั้นพนักงานสอบสวนที่อาจส่งผลกระทบต่อสิทธิที่จะไม่ให้การเป็นปฏิปักษ์ต่อตนเองของผู้ต้องหา

3. เพื่อเสนอแนวทางการปฏิรูปกฎหมาย และกำหนดแนวทางการปฏิบัติงานที่ชัดเจนแก่พนักงานสอบสวน และเพื่อสร้างความสมดุลระหว่างการคุ้มครองสิทธิของผู้ต้องหากับการเพิ่มประสิทธิภาพในการสอบสวนคดีอาชญากรรมทางเทคโนโลยี

การทบทวนวรรณกรรม

การทบทวนวรรณกรรมในงานวิจัยนี้ แบ่งออกเป็น 3 ประเด็นหลัก เพื่อสร้างกรอบแนวคิดในการวิเคราะห์ความขัดแย้งระหว่างสิทธิทางอาญากับอำนาจในการแสวงหาพยานหลักฐานดิจิทัล

หลักการของสิทธิที่จะไม่ให้การเป็นปฏิปักษ์ต่อตนเอง (Right Against Self-Incrimination)

สิทธิที่จะไม่ให้การเป็นปฏิปักษ์ต่อตนเองเป็นหลักการพื้นฐานที่ได้รับการรับรองตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 และประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 134/4 (สำนักงานกิจการยุติธรรม, 2565) โดยมีแก่นสาระสำคัญคือ การคุ้มครองผู้ต้องหาหรือจำเลยมิให้ถูกบังคับหรือบีบคั้นให้ต้องเปิดเผยข้อมูลหรือให้การใด ๆ ที่จะนำไปสู่การพิสูจน์ความผิดของตนเองได้ (ธรรมศาสตร์, 2562)

ขอบเขตตามกฎหมายไทยในชั้นสอบสวน เจ้าพนักงานต้องแจ้งสิทธิให้ผู้ต้องหาทราบว่ามีสิทธิให้การหรือไม่ให้การก็ได้ หากผู้ต้องหาให้การโดยไม่สมัครใจ เช่น ถูกบังคับ ขู่เข็ญ ทรมาน คำให้การนั้นจะไม่อาจรับฟังเป็นพยานหลักฐานได้ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226 (วรวุฒิ สุระ, 2558)

คำถามหลักในยุคดิจิทัล วรรณกรรมส่วนใหญ่จะเริ่มตั้งคำถามว่า สิทธิดังกล่าวครอบคลุมถึงพยานหลักฐานทางกายภาพ (Physical Evidence) หรือไม่ โดยเฉพาะข้อมูลดิจิทัล (Digital Data) ที่ต้องใช้ความรู้และค้นหาความลับส่วนบุคคล เช่น

รหัสผ่าน หรือข้อมูลทางชีวมิติ (Biometric Data) ในการปลดล็อก (พีระ สังข์สิงห์, 2563)

อำนาจในการแสวงหาพยานหลักฐานดิจิทัลตามกฎหมายไทย การแสวงหาพยานหลักฐานในชั้นสอบสวนของไทยดำเนินการภายใต้กฎหมายหลายฉบับ โดยมีเครื่องมือสำคัญในการเข้าถึงข้อมูลดิจิทัล ซึ่งได้แก่

ประมวลกฎหมายวิธีพิจารณาความอาญา ซึ่งกำหนดอำนาจในการค้นและยึดสิ่งของต่าง ๆ แต่ไม่ได้ระบุวิธีการค้นและยึดข้อมูลดิจิทัลที่ถูกเข้ารหัสไว้อย่างชัดเจน

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กำหนดให้อำนาจแก่พนักงานเจ้าหน้าที่ในการเข้าถึงข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ และสามารถยึดหรืออายัดอุปกรณ์ได้ โดยต้องมีหมายค้นหรือคำสั่งของศาล (กิตติพงษ์ ละออ, 2562)

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act: PDPA) แม้จะเน้นการคุ้มครองข้อมูลส่วนบุคคลในกิจกรรมทั่วไป แต่ก็กำหนดให้หน่วยงานรัฐต้องปฏิบัติตามหลักความจำเป็นและความได้สัดส่วนในการประมวลผลข้อมูล ซึ่งเป็นหลักที่ต้องนำมาพิจารณาควบคู่กับการสอบสวนด้วย (สถาบันเพื่อการยุติธรรมแห่งประเทศไทย, 2561)

1. สิทธิของปวงชนชาวไทยตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 สิทธิที่จะไม่ให้การปรักปรำตนเองหรือไม่ถูกบังคับให้สารภาพ

1.1 สิทธิที่จะไม่ให้การปรักปรำตนเองหรือไม่ถูกบังคับให้สารภาพมีความหมาย 3 ประการ คือ

1.1.1 เจ้าหน้าที่ของรัฐต้องไม่นำพยานหลักฐานที่ได้จากการถูกบังคับ ถูกข่มขู่ หรือโดยไม่สมัครใจ มาใช้เป็นหลักฐานในการลงโทษผู้ต้องหาหรือจำเลย

1.1.2 การถูกบังคับให้รวมถึงสถานการณ์ที่ผู้ต้องหาอาจถูกลงโทษหากไม่ให้การตามความจริงหรือถูกลงโทษหากไม่ยอมให้การใด

1.1.3 เมื่อพนักงานสอบสวนตั้งข้อหาและบุคคลตกเป็นผู้ต้องหา โดยผู้ต้องหามีสิทธิที่จะได้รับการแจ้งถึงสิทธิที่จะนิ่งและไม่ให้การปรักปรำตนเอง อย่างไรก็ดี สิทธิที่จะไม่ให้การปรักปรำตนเองมีข้อยกเว้นบางประการ เช่น

(1) สิทธิดังกล่าวเป็นสิทธิที่จะไม่ถูกบังคับต้องให้การใด ไม่ได้ขยายไปถึงพยานวัตถุ ดังนั้น แม้วิธีการได้พยานหลักฐานจะเป็นการฝืนใจผู้ถูกดำเนินคดี เช่น เอกสารที่ได้จากหมายค้นของศาล ลมหายใจ เลือด ปัสสาวะ หรือเนื้อเยื่อจากการตรวจ DNA พยานที่เป็นวัตถุดังกล่าวก็สามารถรับฟังในชั้นศาลได้

(2) การพิจารณาว่าการสอบปากคำผู้ต้องหาใดเป็นการบังคับให้ผู้ต้องหาให้การหรือไม่ ให้ศาลพิจารณาจากข้อเท็จจริงเป็นกรณีไป โดยคำนึงถึงปัจจัยอื่นประกอบด้วย เช่น ลักษณะและระดับแห่งการบังคับว่ารุนแรงเพียงใด การมีอยู่ของหลักประกันสิทธิระหว่างการพิจารณาว่ามีอยู่หรือไม่

(3) การที่ผู้ต้องหาไม่ให้การใด ไม่ใช่จะไม่มีผลในทางคดี ซึ่งหมายความว่า ศาลไม่อาจลงโทษจำเลยเพียงอาศัยเหตุผลเดียวว่า จำเลยไม่ยอมให้การใด แต่การที่จำเลยไม่ให้การใดเลยอาจนำไปสู่ข้อสงสัยหรือข้อพิรุธ เพื่อนำมาประกอบกับการชั่งน้ำหนักพยานหลักฐานอื่นในการลงโทษจำเลยได้

1.2 สิทธิตามกฎหมายรัฐธรรมนูญดังกล่าวจะถูกทำให้เป็นจริงขึ้นมาได้นอกเหนือจากการทำให้เจ้าหน้าที่ของรัฐตระหนักถึงสิทธิของประชาชนแล้ว องค์กรตุลาการก็มีบทบาทสำคัญในการทำให้สิทธิตามกฎหมายรัฐธรรมนูญเป็นจริง

2. พยานหลักฐานดิจิทัลและปัญหาทางกฎหมาย

พยานหลักฐานดิจิทัล (Digital Evidence) หมายถึง ข้อมูลในรูปแบบอิเล็กทรอนิกส์ที่สามารถใช้พิสูจน์ข้อเท็จจริงในคดีได้ เช่น ไฟล์ภาพ เสียง ข้อความการสื่อสารทางอีเมล หรือข้อมูลจากโซเชียลมีเดีย (Goodison, Davis, & Jackson, 2015) การใช้พยานหลักฐานดิจิทัลในคดีอาญาได้เพิ่มขึ้นอย่างต่อเนื่อง แต่ปัญหาที่สำคัญคือ การเข้าถึงข้อมูลส่วนบุคคลโดยไม่ละเมิดสิทธิของผู้ต้องหา เช่น การเข้าถึงโทรศัพท์มือถือหรือคอมพิวเตอร์ของผู้ต้องหาโดยไม่ได้รับความยินยอม

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาตรา 11 วางหลักว่า

ห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในกระบวนการพิจารณาตามกฎหมายทั้งในคดีแพ่ง คดีอาญา หรือคดีอื่นใด เพียงเพราะเหตุว่าเป็นข้อมูลอิเล็กทรอนิกส์

ในการชั่งน้ำหนักพยานหลักฐานว่า ข้อมูลอิเล็กทรอนิกส์จะเชื่อถือได้หรือไม่เพียงใดนั้น ให้พิเคราะห์ถึงความน่าเชื่อถือของลักษณะหรือวิธีการที่ใช้สร้าง เก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์ลักษณะหรือวิธีการเก็บรักษา ความครบถ้วน และไม่มีการเปลี่ยนแปลงของข้อความลักษณะ หรือวิธีการที่ใช้ในการระบุหรือแสดงตัวผู้ส่งข้อมูล รวมทั้งพฤติการณ์ที่เกี่ยวข้องทั้งปวง ให้นำความในวรรคหนึ่งมาใช้บังคับกับสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์ด้วย

จากประเด็นข้อกฎหมายดังกล่าว สามารถอธิบายได้ว่า ข้อมูลอิเล็กทรอนิกส์ ซึ่งหมายความรวมถึง ข้อมูลการติดต่อสื่อสารหรือสนทนาผ่าน E-mail, LINE Application, Facebook Messenger หรือการพูดคุยโต้ตอบกันผ่านทาง Comments ในกระทู้ต่าง ๆ หรือใน Facebook Website หรือเว็บไซต์อื่น ๆ ย่อมสามารถใช้อ้างอิงเป็นพยานหลักฐานในการพิจารณาคดีได้ทั้งคดีแพ่งและคดีอาญา

วิธีการนำสืบข้อมูลอิเล็กทรอนิกส์ดังกล่าวเป็นพยานหลักฐานนั้น มิได้จำเป็นว่าจะต้องนำเครื่องคอมพิวเตอร์ไปทำการประมวลผลข้อมูล เพื่อแสดงข้อมูลอิเล็กทรอนิกส์ให้ศาลพิจารณา หรือต้องทำการคัดลอกข้อมูลอิเล็กทรอนิกส์ใส่ซีดี ส่งไปให้ศาลแต่อย่างใด เพราะตามวรรคสามแห่งพระราชบัญญัติดังกล่าว วางหลักว่า สิ่งพิมพ์ออก หรือ Printout ของข้อมูลอิเล็กทรอนิกส์นั้นสามารถนำมาใช้อ้างอิงเป็นพยานหลักฐานในการพิจารณาได้ เช่นเดียวกับตัวข้อมูลอิเล็กทรอนิกส์ ดังนั้นทางปฏิบัติในการนำสืบข้อมูลอิเล็กทรอนิกส์นั้น ผู้นำสืบย่อมสามารถทำการพิมพ์ข้อมูลทางอิเล็กทรอนิกส์นั้นใส่กระดาษ แล้วนำเอากระดาษที่พิมพ์ข้อมูลอิเล็กทรอนิกส์นั้นไปนำสืบพยานในชั้นศาลได้

ส่วนวิธีการนำสืบข้อมูลอิเล็กทรอนิกส์ดังกล่าวให้มีน้ำหนักที่ศาลจะรับฟังได้นั้น ฝ่ายที่นำสืบควรจะต้องถามค้านและนำสืบให้ศาลเห็นถึงความน่าเชื่อถือของพยานหลักฐานเหล่านั้นตามที่กำหนดไว้ในวรรคสามของมาตราดังกล่าวด้วย กล่าวคือ

ผู้นำสืบควรจะนำสืบให้เห็นว่า ข้อมูลอิเล็กทรอนิกส์นั้นมีวิธีการสร้างหรือการเกิดขึ้นที่น่าเชื่อถือ ไม่อาจถูกปลอมแปลงได้ มีวิธีการเก็บรักษาข้อมูลที่ถูกต้องครบถ้วน ไม่อาจถูกเปลี่ยนแปลงได้ภายหลังจากเกิดขึ้นมาแล้ว และสามารถระบุตัวผู้ส่งข้อความนั้นได้อย่างแน่นอน รวมทั้งพฤติการณ์อื่น ๆ ที่จะทำข้อมูลอิเล็กทรอนิกส์นั้นมีความน่าเชื่อถือ

ตัวอย่างเช่น ในการนำสืบถึงข้อมูลทางอิเล็กทรอนิกส์ที่เป็นการตอบโต้กันผ่าน E-mail LINE หรือ Facebook Messenger ซึ่งพิจารณาแล้วเห็นว่า ผู้นำสืบควรต้องนำสืบและถามค้านพยานตามแนวทางเบื้องต้น ดังนี้

1. ถามค้านพยานฝ่ายตรงข้ามหรือนำสืบพยานฝ่ายตนในประเด็นว่า ผู้ส่งข้อมูลที่ปรากฏในสื่ออิเล็กทรอนิกส์ต่าง ๆ คือบุคคลที่ฝ่ายตนกล่าวอ้างว่าเป็นผู้ส่งจริง ตัวอย่างเช่น หากอ้างว่าจำเลยเป็นผู้ส่งข้อความมาหาโจทก์ทาง E-mail, LINE Application หรือ Facebook Messenger ผู้นำสืบต้องถามค้านจำเลย พยานจำเลย หรือนำสืบพยานโจทก์ที่รู้เห็นเกี่ยวข้องให้ได้ว่า จำเลยเป็นผู้ใช้ E-mail, LINE Application หรือ Facebook Messenger จริง และเป็นผู้ส่งข้อความนั้นในวันเกิดเหตุจริง โดยการนำสืบให้ศาลเห็นว่าจำเลยนั้นเป็นผู้ใช้และส่งข้อมูลทางอิเล็กทรอนิกส์ดังกล่าว อาจจะนำสืบโดยการหมายเรียกข้อมูลผู้สมัครใช้ E-mail, LINE Application หรือ Facebook Messenger ดังกล่าวมาจากผู้ให้บริการระบบข้อมูล (E-mail, LINE, Facebook) เพื่อแสดงให้เห็นว่าผู้ส่งข้อมูลนั้นคือ จำเลยซึ่งเป็นผู้สมัครใช้บริการจากเจ้าของระบบข้อมูล หรือนำสืบถึงผู้ที่รู้จักจำเลย และเคยเห็นจำเลยใช้ E-mail, LINE Application หรือ Facebook Messenger ดังกล่าว หรือการนำสืบถึงพฤติการณ์อื่น ๆ ที่เกี่ยวข้อง เช่น ข้อมูลหรือรูปถ่ายที่ปรากฏใน E-mail, LINE Application หรือ Facebook Messenger นั้น เป็นข้อมูลส่วนตัวของจำเลยบุคคลอื่นไม่สามารถนำเข้าข้อมูลดังกล่าวได้

2. ถามค้านและนำสืบให้ศาลเห็นว่า ข้อมูลต่าง ๆ ที่ปรากฏในสื่ออิเล็กทรอนิกส์นั้น ฝ่ายผู้อ้างไม่สามารถทำขึ้นเองได้โดยลำพัง หากปราศจากการสนทนาโต้ตอบกันจริง และผู้อ้างไม่สามารถแก้ไขเปลี่ยนแปลงข้อมูลที่ปรากฏนั้นได้เอง เช่น หากอ้างหลักฐานการสนทนาโต้ตอบผ่าน E-mail, LINE Application หรือ Facebook Messenger มาเป็นพยานต่อศาล ฝ่ายผู้อ้างก็ต้องถามค้านให้เห็นว่า ข้อมูลการสนทนาที่ปรากฏขึ้นนั้น จะไม่อาจเกิดมีขึ้นได้ หากไม่มีการสนทนาโต้ตอบกันจริง หรือ

เมื่อมีการสนทนาโต้ตอบกันแล้ว ฝ่ายผู้อ้างหรือบุคคลอื่นจะไม่สามารถทำการแก้ไขหรือเปลี่ยนแปลงข้อความดังกล่าวได้ โดยการนำสืบอาจใช้วิธีการถามค้านพยานฝ่ายตรงข้ามให้ยอมรับข้อเท็จจริงดังกล่าว หรือการหมายเรียกผู้ให้บริการระบบ หรือผู้เชี่ยวชาญ ซึ่งมีความชำนาญในเรื่องที่เกี่ยวกับ E-mail, LINE Application หรือ Facebook Messenger มาเบิกความยืนยันถึงข้อเท็จจริงว่า ข้อมูลดังกล่าวไม่อาจจะเกิดขึ้นได้หากไม่มีการสนทนาโต้ตอบกันจริง และเมื่อมีการสนทนาโต้ตอบกันแล้ว ไม่ว่าผู้ใดก็ไม่จะสามารถเปลี่ยนแปลงแก้ไขข้อมูลได้

3. ถามค้านและนำสืบให้เห็นว่า ข้อมูลที่พิมพ์ หรือ Printout ออกมานั้นถูกต้องกับข้อมูลที่ปรากฏอยู่ในสื่ออิเล็กทรอนิกส์จริง โดยการนำสืบประเด็นนี้ เบื้องต้นผู้อ้างจะต้องเบิกความยืนยันก่อนว่า ข้อมูลที่พิมพ์ ออกมานั้นถูกต้องกับข้อมูลที่ปรากฏในสื่ออิเล็กทรอนิกส์ โดยอธิบายถึงกระบวนการในการ Printout นอกจากนี้ ต้องถามค้านให้ฝ่ายตรงข้ามยอมรับ หากฝ่ายตรงข้ามไม่ยอมรับ ฝ่ายผู้อ้างก็ควรจะเตรียมตัวที่จะแสดงข้อมูลทางอิเล็กทรอนิกส์ดังกล่าวเปรียบเทียบกับข้อมูลที่พิมพ์ออกมาได้ทันที

กล่าวโดยสรุปแล้ว หลักฐานการติดต่อสนทนาทางสื่ออิเล็กทรอนิกส์โดยเฉพาะโปรแกรมในการสื่อสารยอดนิยมที่มักใช้กันประจำ E-mail, LINE Application หรือ Facebook Messenger นั้น สามารถใช้อ้างอ้างเป็นพยานหลักฐานในชั้นศาลได้ โดยการนำสืบ สามารถนำสิ่งพิมพ์ออก ของข้อมูลเหล่านั้นมาแสดงเป็นพยานหลักฐานต่อศาลได้ แต่ในการนำสืบนั้น ไม่ควรจะนำสืบลอยๆ แต่ควรจะต้องสืบพฤติการณ์ประกอบต่าง ๆ ที่แสดงให้เห็นว่าข้อมูลทางอิเล็กทรอนิกส์ดังกล่าวมีความน่าเชื่อ จึงจะมีน้ำหนักให้ศาลรับฟังได้ ซึ่งนับวันความจำเป็นในการอ้างอิงข้อมูลอิเล็กทรอนิกส์เหล่านี้มาเป็นพยานหลักฐานก็ยิ่งมีมากขึ้น ในคดีความหลายคดีข้อมูลทางอิเล็กทรอนิกส์เหล่านี้อาจมีผลต่อการแพ้หรือชนะคดีได้ ดังนั้น ทนายความหรือผู้ที่เกี่ยวข้อง จะต้องศึกษาหลักเกณฑ์ต่าง ๆ เกี่ยวกับการอ้างอิงและนำสืบพยานหลักฐานที่เป็นข้อมูลทางอิเล็กทรอนิกส์เหล่านี้

ความขัดแย้งของหลักการในต่างประเทศ

ในต่างประเทศ โดยเฉพาะในระบบกฎหมายจารีตประเพณี (Common Law System) มีการถกเถียงอย่างกว้างขวางว่า การบังคับให้ผู้ต้องหาเปิดเผยรหัสผ่าน

เพื่อเข้าถึงข้อมูลดิจิทัลเป็นการละเมิดสิทธิที่จะไม่ให้การเป็นปฏิปักษ์ต่อตนเองหรือไม่ (ชาติ ชัยเดชสุริยะ, 2549)

แนวคิดแบ่งแยก มีแนวโน้มแบ่งพยานหลักฐานออกเป็นพยานหลักฐานเชิงคำให้การ (Testimonial Evidence) และพยานหลักฐานเชิงวัตถุหรือกายภาพ (Non-Testimonial Evidence) หากข้อมูลดิจิทัลถูกจัดเป็นพยานหลักฐานเชิงวัตถุ เช่น ลายนิ้วมือ เสียง การบังคับให้ปลดล็อกจะไม่ถือเป็นการละเมิดสิทธิ แต่หากรหัสผ่านถูกจัดเป็นข้อมูลเชิงคำให้การที่ต้องอาศัยความรู้หรือความคิดส่วนตัวในการเปิดเผย การบังคับอาจถือเป็นการละเมิดสิทธิ

สมมุติฐานการวิจัย

สมมุติฐานการวิจัย การใช้อำนาจของพนักงานสอบสวนในการเข้าถึงพยานหลักฐานดิจิทัลที่ต้องอาศัยการเปิดเผยความรู้ภายในของผู้ต้องหา มีแนวโน้มก่อให้เกิดการกระทบสิทธิที่จะไม่ให้การเป็นปฏิปักษ์ต่อตนเองในระดับสูงกว่าการตรวจยึดพยานวัตถุทั่วไป

อีกทั้ง หากการใช้อำนาจดังกล่าวมิได้อยู่ภายใต้หลักความจำเป็นและได้สัดส่วน หรือขาดการควบคุมโดยศาลอย่างเข้มงวด การกระทบสิทธิย่อมมีลักษณะไม่ชอบด้วยรัฐธรรมนูญ ในทางกลับกัน หากมีหมายศาลเฉพาะเจาะจงและจำกัดขอบเขตอย่างเหมาะสม ระดับการกระทบสิทธิจะลดลงและสามารถถือได้ว่าเป็นการจำกัดสิทธิที่ชอบด้วยกฎหมาย

ดังนั้น สมมุติฐานหลักของงานวิจัยนี้คือ ระดับความเข้มข้นของการใช้อำนาจแสวงหาพยานหลักฐานดิจิทัล มีความสัมพันธ์โดยตรงกับระดับการกระทบสิทธิไม่ให้การเป็นปฏิปักษ์ต่อตนเอง และความชอบด้วยรัฐธรรมนูญของกระบวนการสอบสวน

กรอบแนวคิดการวิจัย

การวิจัยเรื่อง “สิทธิที่จะไม่ให้การเป็นปฏิปักษ์ต่อตนเองกับการแสวงหาพยานหลักฐานดิจิทัลในชั้นสอบสวนของประเทศไทย” ตั้งอยู่บนฐานแนวคิดสำคัญ 3 กลุ่ม ได้แก่ 1) แนวคิดสิทธิในกระบวนการยุติธรรมทางอาญา (Due Process of Law) 2) ทฤษฎีสิทธิที่จะไม่ให้การเป็นปฏิปักษ์ต่อตนเอง (Right Against Self-Incrimination) และ 3) แนวคิดเกี่ยวกับพยานหลักฐานดิจิทัลและหลักความได้สัดส่วน (Principle of Proportionality) ในการใช้อำนาจรัฐ

งานวิจัยตั้งอยู่บนหลัก “กระบวนการยุติธรรมที่เป็นธรรม” ซึ่งถือว่า รัฐต้องใช้อำนาจสอบสวนภายใต้กรอบรัฐธรรมนูญและหลักนิติธรรม โดยเคารพศักดิ์ศรีความเป็นมนุษย์และเสรีภาพของบุคคล แนวคิดนี้สัมพันธ์โดยตรงกับบทบัญญัติรัฐธรรมนูญ พ.ศ. 2560 มาตรา 29 และกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (ICCPR) ที่รับรองสิทธิของผู้ต้องหาในการไม่ถูกบังคับให้ปรักปรำตนเอง หลักการดังกล่าวมีรากฐานจากระบบกฎหมายจารีตประเพณี (Common Law) ซึ่งพัฒนาผ่านแนวคำพิพากษาในต่างประเทศ

งานวิจัยอาศัยทฤษฎีว่าด้วย “ลักษณะเชิงคำให้การ (Testimonial Character)” ของข้อมูล ซึ่งพิจารณาว่า การเปิดเผยข้อมูลบางประเภท เช่น รหัสผ่าน การถอดรหัส หรือการยืนยันตัวตนทางชีวมิติ เป็นการแสดงออกถึงความรู้หรือเจตจำนงภายในของบุคคลหรือไม่ หากการกระทำนั้นสะท้อนกระบวนการทางความคิด (Contents of the Mind) ก็อาจอยู่ในขอบเขตความคุ้มครองของสิทธิไม่ให้การเป็นปฏิปักษ์ต่อตนเอง งานศึกษาของต่างประเทศ เช่น Hubbell (2000) และแนวคำวินิจฉัยของศาลสิทธิมนุษยชนยุโรป สะท้อนแนวโน้มการตีความขยายขอบเขตสิทธิดังกล่าวให้ครอบคลุมข้อมูลดิจิทัลที่มีลักษณะเชิงคำให้การ

งานวิจัยเชื่อมโยงกับแนวคิดเรื่อง “พยานหลักฐานดิจิทัล (Digital Evidence Theory)” ซึ่งมองว่า ข้อมูลอิเล็กทรอนิกส์มีคุณลักษณะเฉพาะ ได้แก่ ความสามารถในการทำซ้ำ การเข้ารหัส การจัดเก็บในระบบคลาวด์ และการพึ่งพาเทคโนโลยีในการเข้าถึง คุณลักษณะดังกล่าวทำให้การแสวงหาพยานหลักฐานต้องอาศัยความร่วมมือจากผู้ครอบครองข้อมูลมากกว่าพยานวัตถุทั่วไป ส่งผลให้เกิดจุดตัดระหว่าง “อำนาจรัฐใน

การสืบสวน” กับ “สิทธิส่วนบุคคล” งานวิจัยจึงนำหลักความจำเป็นและได้สัดส่วน (Necessity and Proportionality) ตามแนวคิดกฎหมายมหาชนและกฎหมายสิทธิมนุษยชนมาเป็นกรอบประเมินความชอบด้วยกฎหมายของการใช้อำนาจสอบสวน

ดังนั้น ความสัมพันธ์ของตัวแปรสามารถอธิบายได้ว่า เมื่อรัฐใช้อำนาจเข้าถึงข้อมูลดิจิทัลในระดับที่ต้องอาศัยการเปิดเผยความรู้ภายในของผู้ต้องหา (เช่น การบังคับให้เปิดเผยรหัสผ่าน) ย่อมเพิ่มความเสี่ยงต่อการกระทบสิทธิไม่ให้การเป็นปฏิปักษ์ต่อตนเอง ในทางกลับกัน หากการเข้าถึงข้อมูลเป็นเพียงการตรวจยึดพยานวัตถุภายใต้หมายศาลและเป็นไปตามหลักความได้สัดส่วน การกระทบสิทธิก็จะลดลง

ขอบเขตการวิจัย

การวิจัยนี้กำหนดขอบเขตการศึกษา ดังนี้

1. ขอบเขตด้านเนื้อหา

ศึกษาหลักสิทธิที่จะไม่ให้การเป็นปฏิปักษ์ต่อตนเองตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ประมวลกฎหมายวิธีพิจารณาความอาญา พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และกฎหมายที่เกี่ยวข้องกับพยานหลักฐานดิจิทัล

2. ขอบเขตด้านกระบวนการ

จำกัดการศึกษาเฉพาะการแสวงหาพยานหลักฐานดิจิทัลในชั้นสอบสวนของพนักงานสอบสวน ซึ่งจะไม่ครอบคลุมถึงชั้นพิจารณาคดีหรือการบังคับคดี

3. ขอบเขตด้านการเปรียบเทียบกฎหมาย

ศึกษาแนวคิดและแนวคำพิพากษาของต่างประเทศเฉพาะในส่วนที่เกี่ยวข้องกับสิทธิไม่ให้การเป็นปฏิปักษ์ต่อตนเองและข้อมูลดิจิทัล เพื่อนำมาใช้เป็นกรอบวิเคราะห์เชิงเปรียบเทียบ

วิธีดำเนินการวิจัย

การวิจัยนี้ใช้วิธีดำเนินการวิจัยเชิงคุณภาพ (Qualitative Research) เป็นหลัก โดยมีขั้นตอนดังต่อไปนี้

1. การวิจัยเอกสาร (Documentary Research)

วิเคราะห์บทบัญญัติของรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ประมวลกฎหมายวิธีพิจารณาความอาญา พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และกฎหมายอื่นที่เกี่ยวข้องกับการคุ้มครองสิทธิผู้ต้องหาและการสอบสวนคดีเทคโนโลยี

พิเคราะห์แนวคำพิพากษาศาลฎีกาและศาลรัฐธรรมนูญที่วางบรรทัดฐานเกี่ยวกับขอบเขตของสิทธิที่จะไม่ให้การเป็นปฏิปักษ์ต่อตนเอง รวมถึงแนวทางการรับฟังพยานหลักฐานดิจิทัล เปรียบเทียบหลักการและแนวทางปฏิบัติของต่างประเทศ เช่น สหรัฐอเมริกา และสหราชอาณาจักรในประเด็นการบังคับให้เปิดเผยรหัสผ่านข้อมูลดิจิทัล

2. การสัมภาษณ์เชิงลึก (In-depth Interview)

สัมภาษณ์ผู้เชี่ยวชาญ (Experts) ที่เกี่ยวข้องกับกระบวนการยุติธรรม เช่น ผู้พิพากษา พนักงานอัยการ พนักงานสอบสวนคดีอาชญากรรมทางเทคโนโลยี ทนายความผู้เชี่ยวชาญด้านคดีอาญา และนักวิชาการด้านนิติศาสตร์ เพื่อรวบรวมข้อมูลเชิงลึกเกี่ยวกับปัญหาในทางปฏิบัติ และข้อจำกัดในการใช้และการตีความกฎหมายที่นำไปสู่ความขัดแย้งกับสิทธิผู้ต้องหา

กลุ่มผู้ให้ข้อมูลสำคัญ (Key Informants) จำนวน 10 คน คัดเลือกโดยใช้วิธีการเลือกแบบเจาะจง (Purposive Sampling) จากบุคคลที่มีความรู้ ความเชี่ยวชาญและมีประสบการณ์เกี่ยวข้องกับกระบวนการยุติธรรมทางอาญาและเทคโนโลยีสารสนเทศ ประกอบด้วย

1) ผู้พิพากษาที่มีประสบการณ์พิจารณาคดีอาญาหรือคดีเทคโนโลยี จำนวน 2 คน

2) พนักงานอัยการที่รับผิดชอบคดีอาญาหรือคดีอาชญากรรมทางเทคโนโลยี จำนวน 2 คน

3) พนักงานสอบสวนคดีอาชญากรรมทางเทคโนโลยี จำนวน 2 คน

4) ทนายความผู้เชี่ยวชาญด้านคดีอาญาและพยานหลักฐานดิจิทัล จำนวน 2 คน

5) นักวิชาการด้านนิติศาสตร์หรือกฎหมายเทคโนโลยีสารสนเทศ จำนวน 2 คน

การสัมภาษณ์ใช้รูปแบบกึ่งโครงสร้าง (Semi-Structured Interview) โดยใช้แบบสัมภาษณ์เป็นแนวคำถามหลัก เพื่อเปิดโอกาสให้ผู้ให้ข้อมูลสามารถแสดงความคิดเห็นและอธิบายประสบการณ์เชิงลึกเกี่ยวกับปัญหาในทางปฏิบัติ อันจะนำไปสู่การวิเคราะห์และสังเคราะห์ข้อเสนอเชิงกฎหมายต่อไป

3. การวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูล ใช้วิธีการวิเคราะห์เนื้อหา (Content Analysis) และการสังเคราะห์ (Synthesis) เพื่อประมวลผลหลักการทางกฎหมายที่ได้จากการวิจัยเอกสารและข้อค้นพบในทางปฏิบัติที่ได้จากการสัมภาษณ์ เพื่อนำไปสู่การสรุปผลและข้อเสนอแนะเชิงปฏิรูปกฎหมาย

ผลการศึกษา

ผลการศึกษาพบว่า สิทธิที่จะไม่ให้การเป็นปฏิปักษ์ต่อตนเองในระบบกฎหมายไทยได้รับการบัญญัติไว้ในระดับกฎหมายรัฐธรรมนูญและกฎหมายแม่บทในวิธีพิจารณาความอาญา แต่ในทางปฏิบัติยังคงมีความคลุมเครือ โดยเฉพาะในขั้นตอนการสอบสวนคดีอาญาที่เกี่ยวข้องกับพยานหลักฐานดิจิทัล สาระสำคัญของผลการศึกษาสามารถสรุปได้ ดังนี้

1. ขอบเขตของสิทธิตามรัฐธรรมนูญและกฎหมายไทยยังไม่ชัดเจนในทางปฏิบัติ

แม้มาตรา 29 วรรคสอง ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 และมาตรา 134/4 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา จะกำหนดสิทธิของผู้ต้องหาที่จะไม่ให้การเป็นปฏิปักษ์ต่อตนเอง แต่ยังไม่มีแนวทางหรือระเบียบปฏิบัติที่ชัดเจนสำหรับเจ้าพนักงานที่เกี่ยวข้องในการใช้และการตีความสิทธินี้ในกรณีที่เกี่ยวข้องกับข้อมูลดิจิทัล เช่น การร้องขอรหัสผ่านโทรศัพท์ หรือบัญชีสื่อสังคมออนไลน์ของผู้ต้องหา

2. พนักงานสอบสวนยังขาดหลักเกณฑ์การใช้ดุลพินิจที่ชัดเจนในการรวบรวมพยานหลักฐานดิจิทัล

ในหลายกรณี การเข้าถึงข้อมูลดิจิทัลของผู้ต้องหาอาศัยการตีความอำนาจตามกฎหมายทั่วไป ซึ่งอาจนำไปสู่การละเมิดสิทธิส่วนบุคคล เช่น การตรวจค้นโทรศัพท์โดยไม่ได้รับอนุญาตหรือหมายค้นที่ออกโดยไม่เฉพาะเจาะจง

3. แนวทางกฎหมายต่างประเทศเน้นคุ้มครองสิทธิของบุคคลมากกว่า

ศาลสูงแห่งสหรัฐอเมริกา และศาลสิทธิมนุษยชนยุโรป ได้ตีความสิทธิไม่ให้การเป็นปฏิปักษ์ต่อตนเองอย่างกว้าง โดยถือว่าการบังคับให้เปิดเผยรหัสผ่านหรือข้อมูลส่วนตัวในอุปกรณ์ดิจิทัลเป็นการละเมิดสิทธิ เว้นแต่จะมีคำสั่งศาลที่ระบุเหตุผลเฉพาะเจาะจงและมีความจำเป็นอย่างยิ่ง (*Riley v. California*, 573 U.S. 373 (2014); European Court of Human Rights, 2019)

4. สังคมไทยยังขาดความตระหนักถึงสิทธิขั้นพื้นฐานในกระบวนการสอบสวน จากการสัมภาษณ์ผู้เชี่ยวชาญด้านกฎหมายอาญา พบว่า ประชาชนส่วนใหญ่ไม่ทราบว่าตนมีสิทธิที่จะปฏิเสธการให้รหัสผ่านหรือข้อมูลดิจิทัลแก่เจ้าพนักงาน และมักเกรงกลัวต่ออำนาจรัฐ ส่งผลให้สิทธิในการปกป้องตนเองถูกละเลย

อภิปรายผลการวิจัย

การแสวงหาพยานหลักฐานดิจิทัลในชั้นสอบสวนเป็นความจำเป็นของกระบวนการยุติธรรมยุคใหม่ แต่ต้องอยู่ภายใต้หลักการคุ้มครองสิทธิของบุคคลตามรัฐธรรมนูญและกติการะหว่างประเทศ การบังคับให้ผู้ต้องหาเปิดเผยรหัสผ่านหรือข้อมูลส่วนบุคคลถือเป็นการให้การโดยปริยาย ซึ่งเข้าข่ายเป็นการละเมิดสิทธิไม่ให้การเป็นปฏิปักษ์ต่อตนเอง เพราะข้อมูลดังกล่าวอาจใช้เป็นพยานหลักฐานปรักปรำผู้ให้การได้

เมื่อเปรียบเทียบกับแนวทางของกฎหมายต่างประเทศจะพบว่า หลักสิทธิดังกล่าวได้รับการตีความอย่างเข้มงวด เช่น ในคดี *United States v. Hubbell* (2000) ศาลสูงแห่งสหรัฐอเมริกาเห็นว่า การบังคับให้ผู้ต้องหาส่งมอบเอกสารหรือรหัสผ่านเพื่อเปิดเผยข้อมูลที่อาจใช้กล่าวหาตนเอง ถือเป็นการละเมิดสิทธิตามการแก้ไขรัฐธรรมนูญ ครั้งที่ 5 เว้นแต่ผู้ต้องหาจะยินยอมโดยสมัครใจ นอกจากนี้ ในสหภาพยุโรป ศาลสิทธิมนุษยชนยุโรปได้วางหลักว่า การบังคับให้เปิดเผยข้อมูลส่วนบุคคลที่มีลักษณะสาระสำคัญทางความคิด (Testimonial Evidence) ย่อมละเมิดสิทธิดังกล่าวเช่นกัน (European Court of Human Rights, 2019)

ในประเทศไทย แม้เจ้าพนักงานจะมีอำนาจตรวจค้นและยึดพยานหลักฐานดิจิทัลตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แต่การร้องขอให้ผู้ต้องหามีส่วนร่วมในการเปิดเผยข้อมูล เช่น การพิมพ์รหัสผ่าน การสแกนใบหน้า หรือการปลดล็อกอุปกรณ์ต่าง ๆ ต้องถูกตีความอย่างเคร่งครัด เพราะเป็นการกระทำที่กระทบต่อเสรีภาพในร่างกายและข้อมูลส่วนบุคคลโดยตรง

การคุ้มครองสิทธิไม่ให้การเป็นปฏิปักษ์ต่อตนเองจึงควรได้รับการขยายขอบเขตให้ครอบคลุมข้อมูลดิจิทัลที่สะท้อนเจตจำนงของบุคคล ไม่ใช่เพียงพิจารณาแต่คำให้การหรือคำรับสารภาพ ซึ่งจะสอดคล้องกับหลักสิทธิมนุษยชนและหลักความยุติธรรมในยุคดิจิทัล (Mason, 2020; McGregor, 2021)

สรุปผลการวิจัย

ผลการวิจัยสรุปได้ว่า แม้กฎหมายไทยจะรับรองสิทธิที่จะไม่ให้การเป็นปฏิปักษ์ต่อตนเองไว้อย่างชัดเจนในระดับกฎหมายรัฐธรรมนูญ ซึ่งเป็นกฎหมายสูงสุดภายในประเทศ แต่ในทางปฏิบัติยังขาดหลักเกณฑ์ที่ชัดเจนในการใช้บังคับในกรณีที่เกี่ยวข้องกับพยานหลักฐานดิจิทัล โดยเฉพาะกรณีการร้องขอหรือบังคับ ให้ผู้ต้องหาเปิดเผยรหัสผ่านหรือข้อมูลส่วนบุคคลในอุปกรณ์อิเล็กทรอนิกส์ ซึ่งมีลักษณะเป็นการให้การโดยปริยาย และอาจเข้าข่ายละเมิดสิทธิดังกล่าว หากไม่มีการควบคุมโดยคำสั่งศาลและหลักความจำเป็นอย่างเคร่งครัด

สิทธิที่จะไม่ให้การเป็นปฏิปักษ์ต่อตนเองกับการแสวงหาพยานหลักฐานดิจิทัลในชั้นสอบสวนของประเทศไทยมีวัตถุประสงค์เพื่อศึกษาวิเคราะห์ขอบเขตและการบังคับใช้สิทธิที่จะไม่ให้การเป็นปฏิปักษ์ต่อตนเองของผู้ต้องหาในบริบทของการแสวงหาพยานหลักฐานดิจิทัล ซึ่งมีบทบาทเพิ่มขึ้นอย่างมากในกระบวนการยุติธรรมอาญายุคนี้ การวิจัยใช้ระเบียบวิธีวิจัยเชิงคุณภาพ โดยการศึกษาวิเคราะห์เอกสารทางกฎหมาย แนวคำพิพากษา และการสัมภาษณ์เชิงลึกผู้เชี่ยวชาญด้านกฎหมายและเทคโนโลยีจะช่วยให้ค้นพบแนวทางในการแก้ไขและปรับปรุงกฎหมายให้มีประสิทธิภาพยิ่งขึ้น

ผลการศึกษาพบว่า แม้กฎหมายไทยจะรับรองสิทธิที่จะไม่ให้การเป็นปฏิปักษ์ต่อตนเองไว้อย่างชัดเจน โดยปรากฏในกฎหมายรัฐธรรมนูญและกฎหมายแม่บทในวิธีพิจารณาความอาญาก็ตาม แต่การใช้บังคับกฎหมายดังกล่าวในทางปฏิบัติโดยเฉพาะในชั้นสอบสวนที่เกี่ยวข้องกับพยานหลักฐานดิจิทัล ยังขาดความชัดเจนในด้านขอบเขตและแนวทางการปฏิบัติ ส่งผลให้เกิดความเสี่ยงต่อการละเมิดสิทธิของผู้ต้องหา โดยเฉพาะกรณีการร้องขอหรือบังคับให้เปิดเผยรหัสผ่าน ข้อมูลที่ถูกเข้ารหัสหรือข้อมูลส่วนบุคคลในอุปกรณ์อิเล็กทรอนิกส์ ซึ่งมีลักษณะเป็นการให้การโดยปริยายและอาจเข้าข่ายเป็นการปรักปรำตนเอง

การศึกษาวิจัยนี้ ยังชี้ให้เห็นว่า ระบบกฎหมายไทยยังไม่มีการแยกแยะอย่างชัดเจนระหว่างการยึดอุปกรณ์อิเล็กทรอนิกส์กับการบังคับให้ผู้ต้องหามีส่วนร่วมในการเปิดเผยข้อมูลภายในอุปกรณ์ดังกล่าว ซึ่งแตกต่างจากแนวทางของต่างประเทศที่ให้

ความสำคัญกับการคุ้มครองสิทธิส่วนบุคคล และกำหนดเงื่อนไขการเข้าถึงข้อมูลดิจิทัลอย่างเข้มงวด ภายใต้การควบคุมของศาลและหลักความจำเป็น และหลักความได้สัดส่วน

โดยสรุป งานวิจัยนี้เสนอว่า สิทธิที่จะไม่ให้การเป็นปฏิปักษ์ต่อตนเองควรมีการใช้และการตีความอย่างก้าวหน้าและสอดคล้องกับบริบทของสังคมดิจิทัล เพื่อให้ครอบคลุมถึงข้อมูลดิจิทัลที่สะท้อนเจตจำนง ความรู้ หรือกระบวนการทางความคิดของบุคคล อันจะนำไปสู่การสร้างสมดุลระหว่างการคุ้มครองสิทธิขั้นพื้นฐานของผู้ต้องหาและการรักษาประสิทธิภาพของกระบวนการยุติธรรมอาญา ตลอดจนเสริมสร้างความชอบธรรมและความน่าเชื่อถือของระบบยุติธรรมไทยในระยะยาว

ข้อเสนอแนะการวิจัย

1. ข้อเสนอแนะเชิงนโยบาย

ควรมีการปรับปรุงกฎหมายโดยการแก้ไขเพิ่มเติมกฎหมายแม่บทที่เกี่ยวกับวิธีพิจารณาความอาญา โดยกำหนดหลักเกณฑ์การเข้าถึงพยานหลักฐานดิจิทัลให้ชัดเจน และบัญญัติบทกฎหมายในกรณีการบังคับให้ผู้ต้องหาเปิดเผยรหัสผ่านหรือข้อมูลส่วนบุคคลต้องได้รับคำสั่งศาลที่เฉพาะเจาะจง และอยู่ภายใต้หลักความจำเป็นและหลักความได้สัดส่วน

2. ข้อเสนอแนะเชิงปฏิบัติ

ควรจัดทำคู่มือหรือแนวปฏิบัติสำหรับพนักงานสอบสวนเกี่ยวกับการแสวงหาพยานหลักฐานดิจิทัล พร้อมทั้งให้ความรู้แก่พนักงานเจ้าหน้าที่ที่เกี่ยวข้องเพื่อให้ตระหนักถึงสิทธิของผู้ต้องหา และเพื่อลดการละเมิดสิทธิและเสรีภาพของบุคคล ซึ่งจะช่วยเพิ่มความน่าเชื่อถือของพยานหลักฐานที่ได้มาเพื่อใช้การพิจารณาคดี

3. ข้อเสนอแนะสำหรับการวิจัยครั้งต่อไป

ควรศึกษาประเด็นการใช้เทคโนโลยีชีวมิติ (Biometric Technology) เช่น การสแกนใบหน้า หรือลายนิ้วมือเพื่อใช้ในการปลดล็อกอุปกรณ์ดิจิทัล เพื่อป้องกันการกระทำของเจ้าหน้าที่ที่เข้าข่ายเป็นการละเมิดสิทธิไม่ให้การเป็นปฏิปักษ์ต่อตนเองของผู้ต้องหา

องค์ความรู้ใหม่และการนำไปใช้

1. องค์ความรู้ที่ค้นพบจากการวิจัย

บทความนี้เสนอองค์ความรู้ใหม่โดยนำเสนอให้เห็นว่า ข้อมูลดิจิทัลที่ต้องอาศัยความรู้หรือเจตจำนงของบุคคลในการเข้าถึง ควรได้รับการพิจารณาว่าเป็นพยานหลักฐานเชิงคำให้การ (Testimonial Evidence) ไม่ใช่เพียงพยานวัตถุทั่วไป ซึ่งเป็นการขยายกรอบการคุ้มครองสิทธิไม่ให้การเป็นปฏิปักษ์ต่อตนเองให้สอดคล้องกับบริบทเทคโนโลยีสมัยใหม่

2. การนำผลการวิจัยไปใช้ประโยชน์

1) ใช้เป็นแนวทางในการตีความกฎหมายของศาลและเจ้าพนักงาน

2) สามารถนำไปปรับใช้ประกอบการฝึกอบรมบุคลากรในกระบวนการยุติธรรม

3) เป็นฐานข้อมูลเชิงวิชาการสำหรับการปรับปรุงกฎหมายด้านอาชญากรรมทางเทคโนโลยี

4) ส่งเสริมการคุ้มครองสิทธิมนุษยชนและความเป็นธรรมในกระบวนการยุติธรรมอาญา

เอกสารอ้างอิง

กิตติพงษ์ ละออ. (2562). *แนวทางการพัฒนาระบบสอบสวนคดีอาญาของประเทศไทย.* [วิทยานิพนธ์นิติศาสตรมหาบัณฑิต]. มหาวิทยาลัยรามคำแหง.

ชาติ ชัยเดชสุริยะ. (2549). *มาตรการทางกฎหมายในการคุ้มครองสิทธิมนุษยชนในกระบวนการยุติธรรมทางอาญา.* เดือนตุลา.

ธรรมศาสตร์, คณะนิติศาสตร์. (2562). *ความรู้ทางกฎหมายหลากหลายและเข้าใจง่าย ชุดที่ 68: สิทธิในการไม่ให้การเป็นปฏิปักษ์ต่อตนเองในระบบกฎหมายอาญาไทย.* [Infographic].

พีระ สังข์สิงห์. (2563). ความเหลื่อมล้ำในการเข้าถึงกระบวนการยุติธรรมทางอาญาของประชาชน. *วารสารรามคำแหงฉบับนิติศาสตร์, 9*(2), 159-180.

วรวุฒิ สุระ. (2558). *ปัญหาและแนวทางแก้ไขการสอบสวนที่ไม่ถูกต้อง ไม่รวดเร็ว และไม่เป็นธรรม* [สารนิพนธ์นิติศาสตรมหาบัณฑิต]. มหาวิทยาลัยสุโขทัยธรรมาธิราช.

ศาลรัฐธรรมนูญ. (2565). *คำวินิจฉัยที่ 24/2565.* กระทรวงยุติธรรม.

สถาบันเพื่อการยุติธรรมแห่งประเทศไทย (TIJ). (2561). *รายงานการศึกษาระดับโลกว่าด้วยการเข้าถึงความยุติธรรม.* สถาบันเพื่อความยุติธรรมแห่งประเทศไทย (องค์การมหาชน).

สำนักงานกิจการยุติธรรม. (2565). *สิทธิของผู้ต้องหาหรือผู้ถูกจับ.* กระทรวงยุติธรรม.

สำนักงานกิจการยุติธรรม. (2565). *สิทธิของผู้ต้องหาหรือผู้ถูกจับ.* กระทรวงยุติธรรม.

Ashworth, A., & Redmayne, M. (2010). *The criminal process* (4th ed.). Oxford University Press.

European Court of Human Rights. (2006). *Case of Jalloh v. Germany,* App no. 54810/00. Council of Europe.

European Court of Human Rights. (2016). *Case of Ibrahim and Others v. the United Kingdom,* App nos. 50541/08 et al. Council of Europe.

Goodison, S. E., Davis, R. C., & Jackson, B. A. (2015). *Digital evidence and the U.S. criminal justice system: Identifying technology and other needs to more effectively acquire and utilize digital evidence*. RAND Corporation.

Kerr, O. S. (2018). *Computer crime law* (4th ed.). West Academic Publishing.

Mason, S. (2021). *Electronic evidence* (4th ed.). Institute of Advanced Legal Studies, University of London.

McGregor, L. (2021). The privilege against self-incrimination and modern digital evidence. *International Journal of Evidence & Proof, 25*(1), 1–23.