



ISSN: 2774-0390 (Online)

วารสารวิทยาการจัดการ มหาวิทยาลัยราชภัฏสกลนคร
Journal of Management Science, Sakon Nakhon Rajabhat University
Homepage: <https://so08.tci-thaijo.org/index.php/JMSSNRU>
e-mail: jmssnru@gmail.com



ปัญหาทางกฎหมายเกี่ยวกับการค้นเครื่องคอมพิวเตอร์เพื่อให้ได้มาซึ่ง พยานหลักฐานในคดีอาญาของประเทศไทย

Legal issues concerning computer searches for obtaining evidence in criminal cases in Thailand

ธนัทเทพ เตียรประสิทธิ์^{1*}

Tanatthep Tianprasit^{1*}

¹ คณะนิติศาสตร์ สถาบันบัณฑิตพัฒนบริหารศาสตร์

¹ Graduate School of Law, National Institute of Development Administration (NIDA)

*Corresponding author's e-mail: tanattheptianprasit@gmail.com^{1*}

Received: January 12, 2026

Revised: January 29, 2026

Accepted: March 15, 2026

บทคัดย่อ

ในปัจจุบัน เทคโนโลยีและนวัตกรรมมีความเจริญก้าวหน้าอย่างรวดเร็ว อุปกรณ์อิเล็กทรอนิกส์ เช่น คอมพิวเตอร์ โทรศัพท์มือถือ และอุปกรณ์ที่สามารถเชื่อมต่ออินเทอร์เน็ตได้ ได้เข้ามามีบทบาทสำคัญต่อการดำเนินชีวิตประจำวันของประชาชน ทั้งในด้านการติดต่อสื่อสารและการทำธุรกรรมต่าง ๆ ไม่ว่าจะเป็นการซื้อขายสินค้าและบริการ การชำระเงิน หรือธุรกรรมทางการเงินรูปแบบอื่น ความสะดวกและรวดเร็วของเทคโนโลยีดังกล่าว ส่งผลให้มีการนำอุปกรณ์อิเล็กทรอนิกส์ไปใช้เป็นเครื่องมือในการกระทำความผิดทางอาญา หรือใช้เป็นแหล่งจัดเก็บข้อมูลที่เกี่ยวข้องกับการกระทำความผิดเพิ่มมากขึ้น อำนาจของรัฐในการค้นและเข้าถึงข้อมูลที่อยู่ในอุปกรณ์อิเล็กทรอนิกส์ของบุคคลในประเทศไทยได้ถูกกำหนดไว้ในกฎหมายหลายฉบับ โดยกฎหมายที่มีบทบาทสำคัญคือ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 อย่างไรก็ตาม แม้กฎหมายดังกล่าวจะมีบทบัญญัติเกี่ยวกับการค้นเครื่องคอมพิวเตอร์เพื่อให้ได้มาซึ่งพยานหลักฐานในคดีอาญาแล้ว แต่ยังปรากฏปัญหาทางกฎหมายบางประการ ได้แก่ ปัญหาเกี่ยวกับสิทธิที่จะไม่ให้การปรักปรำตนเองกรณีการบังคับให้ผู้ต้องหาถอดรหัสลับ และปัญหาเกี่ยวกับความชอบด้วยกฎหมายของพยานหลักฐานในความผิดอื่นที่ได้มาโดยไม่มีคำสั่งอนุญาตจากศาล บทความนี้มีวัตถุประสงค์เพื่อศึกษาและวิเคราะห์ปัญหาทางกฎหมายดังกล่าว โดยเปรียบเทียบกับกฎหมายต่างประเทศ เพื่อเสนอแนะแนวทางในการปรับปรุงกฎหมายไทยให้สามารถคุ้มครองสิทธิส่วนบุคคลควบคู่กับการควบคุมอาชญากรรมได้อย่างเหมาะสมและมีประสิทธิภาพ โดยบทความนี้เสนอให้มีการเพิ่มบัญญัติให้ชัดเจนใน

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เพื่อเป็นการแก้ไขปัญหาในการได้มาซึ่งพยานหลักฐานจากการค้นเครื่องคอมพิวเตอร์ของประเทศไทย

คำสำคัญ: การค้นเครื่องคอมพิวเตอร์, พยานหลักฐานในคดีอาญา, สิทธิส่วนบุคคล

Abstract

At present, technology and innovation are advancing rapidly. Electronic devices – such as computers, smartphones, and other internet-connected devices – play a significant role in people's daily lives, both in communication and various transactions. These include the purchase and sale of goods and services, payment, and other forms of financial transactions. The convenience and speed afforded by such technologies have led to an increasing use of electronic devices as instruments for the commission of criminal offenses, as well as repositories for data related to such offenses. In Thailand, state authority to search and access data stored in individuals' electronic devices is prescribed under several statutes, most notably the computer-related Crime Act B.E. 2550 (2007). Notwithstanding the existence of statutory provisions governing the search of computer systems for the purpose of obtaining evidence in criminal proceedings, certain legal issues remain. These include concerns relating to the right against self-incrimination in cases where suspects are compelled to disclose passwords or encryption keys, as well as questions regarding the admissibility and legality of evidence pertaining to other offenses obtained without prior judicial authorization. This article aims to examine and analyze the aforementioned legal issues through a comparative study with relevant foreign laws, with a view to proposing recommendations for the reform of Thai law to effectively balance the protection of individual privacy rights with appropriate and efficient crime control. The objective is to ensure that personal rights are adequately protected while maintaining effective and proportionate mechanisms for crime control. In particular, this article proposes that clearer and more explicit provisions be incorporated into the computer-related Crime Act B.E. 2550 (2007) in order to address the challenges associated with obtaining evidence from computer searches in Thailand.

Keywords: computer search, criminal evidence, individual rights

บทนำ

ในปัจจุบันเทคโนโลยีและนวัตกรรมมีความเจริญก้าวหน้าอย่างรวดเร็ว อุปกรณ์อิเล็กทรอนิกส์ เช่น คอมพิวเตอร์ โทรศัพท์มือถือ หรืออุปกรณ์อื่นที่เชื่อมต่ออินเทอร์เน็ต ได้เข้ามามีบทบาทสำคัญในชีวิตประจำวันของประชาชน ทั้งในด้านการสื่อสาร การทำธุรกรรมทางการเงิน ตลอดจนการซื้อขายสินค้าและบริการผ่านระบบอิเล็กทรอนิกส์ อย่างไรก็ตาม ผลที่ตามมาของความสะดวกและความรวดเร็วของเทคโนโลยีดังกล่าวคือ การที่อุปกรณ์อิเล็กทรอนิกส์อาจถูกนำมาใช้เป็นเครื่องมือในการกระทำความผิด หรือใช้เป็นแหล่งจัดเก็บข้อมูลที่เกี่ยวข้องกับการกระทำความผิดได้ รายงานของเว็ลด์อีโคโนมิกฟอรัม (World Economic Forum) ระบุว่า ในปี ค.ศ. 2023 อาชญากรรมไซเบอร์ได้สร้างความเสียหายต่อเศรษฐกิจโลกเป็นมูลค่าประมาณ 8.4 ล้านล้านดอลลาร์สหรัฐ (Charlton, 2024) ซึ่งสะท้อนให้เห็นถึงความสำคัญของการพัฒนากลไกทางกฎหมายเพื่อรองรับการจัดการกับอาชญากรรมในโลกดิจิทัล เมื่ออุปกรณ์อิเล็กทรอนิกส์มีความเกี่ยวข้องกับการกระทำความผิดไม่ว่าในทางใดทางหนึ่ง ข้อมูลที่ถูกจัดเก็บอยู่

ภายในอุปกรณ์ดังกล่าว เช่น ข้อความสนทนา ไฟล์เสียง หรือข้อมูลดิจิทัลอื่นที่เกี่ยวข้องกับการกระทำความผิด จึงอาจมีความสำคัญในฐานะพยานหลักฐานในการพิสูจน์ความบริสุทธิ์หรือความผิดของผู้ถูกกล่าวหาไม่ยิ่งหย่อนไปกว่าพยานหลักฐานในรูปแบบดั้งเดิม เช่น พยานบุคคล พยานเอกสาร หรือพยานวัตถุ

อย่างไรก็ตาม แม้ว่ามาตรา 11 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และมาตรา 25 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จะบัญญัติให้ข้อมูลอิเล็กทรอนิกส์สามารถรับฟังเป็นพยานหลักฐานได้ทั้งในคดีแพ่ง คดีอาญา หรือคดีอื่นใด (พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544, 2544; พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550, 2550) แต่ประมวลกฎหมายวิธีพิจารณาความอาญาซึ่งเป็นกฎหมายหลักเกี่ยวกับวิธีการนำพยานหลักฐานเข้าสู่การพิจารณาในชั้นศาล กลับมิได้บัญญัติเกี่ยวกับพยานหลักฐานอิเล็กทรอนิกส์ไว้โดยเฉพาะ

ด้วยเหตุนี้ จึงก่อให้เกิดประเด็นทางกฎหมายเกี่ยวกับการค้นอุปกรณ์อิเล็กทรอนิกส์ ซึ่งยังไม่สับทบัญญัติเฉพาะรองรับในประมวลกฎหมายวิธีพิจารณาความอาญา อันอาจนำไปสู่ข้อสงสัยว่าพยานหลักฐานที่ได้จากการค้นอุปกรณ์ดังกล่าวจะสามารถรับฟังได้ตามมาตรา 226 แห่งประมวลกฎหมายวิธีพิจารณาความอาญาหรือไม่ ซึ่งประเด็นดังกล่าวจะได้กล่าวถึงต่อไปในบทความนี้

แนวคิดและบทบัญญัติเกี่ยวกับการแสวงหาพยานหลักฐานในคดีอาญาในประเทศไทย

ในการดำเนินคดีอาญาของประเทศไทย ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 131 ได้กำหนดให้พนักงานสอบสวนมีหน้าที่รวบรวมพยานหลักฐานทุกชนิดเท่าที่สามารถกระทำได้ ไม่ว่าจะเป็นพยานหลักฐานที่เป็นผลดีหรือผลร้ายแก่ผู้ต้องหา (ประมวลกฎหมายวิธีพิจารณาความอาญา พ.ศ. 2477, ม.ป.ป.) โดยคำพิพากษาศาลฎีกาที่ 4440/2562 ได้วางหลักเพิ่มเติมว่าพนักงานสอบสวนมีดุลพินิจในการเลือกเก็บพยานหลักฐานที่จำเป็นต่อความแจ่ม กระฉ่างของคดี การแสวงหาพยานหลักฐานดังกล่าวมีวัตถุประสงค์เพื่อให้ทราบข้อเท็จจริงและพฤติการณ์ต่าง ๆ อันเกี่ยวกับความผิดที่ถูกลกล่าวหา อันจะนำไปสู่การพิสูจน์ความผิดหรือความบริสุทธิ์ของผู้ต้องหา เมื่อพิจารณาบทบัญญัติดังกล่าวประกอบกับมาตรา 11 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และมาตรา 25 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งบัญญัติให้ข้อมูลอิเล็กทรอนิกส์สามารถรับฟังเป็นพยานหลักฐานได้ทั้งในคดีแพ่ง คดีอาญา หรือคดีอื่นใด (พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544, 2544; พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550, 2550) ซึ่งบัญญัติให้ข้อมูลอิเล็กทรอนิกส์สามารถรับฟังเป็นพยานหลักฐานได้ทั้งในคดีแพ่ง คดีอาญา หรือคดีอื่นใด จึงอาจกล่าวได้ว่า พนักงานสอบสวนมีหน้าที่รวบรวมข้อมูลอิเล็กทรอนิกส์ที่ได้จากอุปกรณ์อิเล็กทรอนิกส์ เช่น คอมพิวเตอร์ หรือโทรศัพท์มือถือ เพื่อนำมาใช้เป็นพยานหลักฐานในการดำเนินคดี ทั้งนี้ การนำข้อมูลดังกล่าวมาใช้เป็นพยานหลักฐานสอดคล้องกับหลักพยานหลักฐานที่ดีที่สุด (best evidence rule) ซึ่งเป็นหลักการที่กำหนดให้ศาลรับฟังพยานหลักฐานที่มีความใกล้เคียงกับข้อเท็จจริงมากที่สุด เพื่อให้การพิสูจน์ข้อเท็จจริงเป็นไปอย่างถูกต้องและน่าเชื่อถือ (Cornell Law School, 2024) ดังนั้น หากข้อมูลที่ได้จากอุปกรณ์อิเล็กทรอนิกส์สามารถพิสูจน์ได้ว่าได้มาโดยชอบด้วยกฎหมายและมีความถูกต้องเชื่อถือได้ ข้อมูลดังกล่าวย่อมสามารถใช้เป็นพยานหลักฐานสำคัญในการดำเนินคดีกับผู้ต้องหาได้ไม่ต่างจากพยานหลักฐานประเภทอื่น

นอกจากนี้ ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 131/1 ยังให้อำนาจพนักงานสอบสวนในการตรวจพิสูจน์บุคคล วัตถุ หรือเอกสารใด ๆ โดยวิธีการทางวิทยาศาสตร์ ซึ่งรวมถึงการตรวจเครื่องคอมพิวเตอร์หรือข้อมูลในระบบคอมพิวเตอร์ด้วย (ณรงค์ ใจหาญ, 2565) อย่างไรก็ตาม เพื่อให้พนักงานสอบสวนสามารถรวบรวม

พยานหลักฐานได้อย่างครบถ้วน ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 132 จึงให้อำนาจพนักงานสอบสวนในการตรวจตัวบุคคล ตรวจสอบสิ่งของหรือสถานที่ ค้นเพื่อพบสิ่งของ หมายถึงบุคคล ซึ่งครอบครองสิ่งของ ตลอดจนยึดไว้ซึ่งสิ่งของที่ค้นพบหรือส่งมา ทั้งนี้เป็นไปตามเงื่อนไขที่กฎหมายกำหนด อย่างไรก็ตาม การค้นและตรวจหาพยานหลักฐานจากอุปกรณ์อิเล็กทรอนิกส์มีลักษณะซับซ้อนกว่าพยานหลักฐานประเภทอื่น เนื่องจากการเข้าถึงข้อมูลที่จัดเก็บอยู่ภายในอุปกรณ์ดังกล่าวมักต้องอาศัยรหัสผ่านหรือมาตรการป้องกันการเข้าถึง หากไม่ได้รับความยินยอมหรือไม่ทราบรหัสผ่านจากเจ้าของหรือผู้ครอบครอง ย่อมไม่อาจเข้าถึงข้อมูลดังกล่าวได้

ดังนั้น หากพนักงานสอบสวนประสงค์จะเข้าถึงข้อมูลภายในอุปกรณ์อิเล็กทรอนิกส์ จึงจำเป็นต้องดำเนินการถอดรหัสผ่านหรือมาตรการป้องกันการเข้าถึงข้อมูลเสียก่อน อย่างไรก็ตาม ประมวลกฎหมายวิธีพิจารณาความอาญา ยังมิได้บัญญัติให้อำนาจพนักงานสอบสวนในการดำเนินการดังกล่าวไว้โดยชัดแจ้ง แม้ในกรณีที่ได้มีการขออนุญาตค้นและยึดอุปกรณ์อิเล็กทรอนิกส์โดยชอบแล้วก็ตาม อำนาจตามหมายค้นก็ไม่ครอบคลุมถึงการถอดรหัสเพื่อเข้าถึงข้อมูลภายในอุปกรณ์นั้น (ณรงค์ ใจหาญ, 2565) หากพนักงานสอบสวนดำเนินการดังกล่าวโดยไม่มีอำนาจตามกฎหมาย พยานหลักฐานที่ได้ อาจถือเป็นพยานหลักฐานที่ได้มาโดยมิชอบ ซึ่งศาลอาจไม่รับฟังตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226/1 นอกจากนี้ พนักงานสอบสวนอาจมีความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 5 ฐานเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ ซึ่งมีโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกิน 10,000 บาท หรือทั้งจำทั้งปรับ

กฎหมายที่เกี่ยวข้องกับการเข้าถึงข้อมูลในอุปกรณ์อิเล็กทรอนิกส์

1. แนวคิดพื้นฐานในการคุ้มครองสิทธิของบุคคล

สิทธิในความเป็นอยู่ส่วนตัว (right to privacy) เป็นหนึ่งในสิทธิมนุษยชนพื้นฐานที่ได้รับการรับรองไว้ในรัฐธรรมนูญแห่งราชอาณาจักรไทย ฉบับปัจจุบัน โดยรัฐธรรมนูญได้บัญญัติรับรองการคุ้มครองข้อมูลส่วนบุคคลของบุคคล และห้ามมิให้นำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใด เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมายที่ตราขึ้นเพียงพอที่จำเป็นเพื่อประโยชน์สาธารณะ ตามมาตรา 32 (รัฐธรรมนูญแห่งราชอาณาจักรไทย, 2560) นอกจากนี้ สิทธิและเสรีภาพในการติดต่อสื่อสาร (right to communication) ยังเป็นสิทธิมนุษยชนพื้นฐานอีกประการหนึ่งที่ได้รับการรับรองไว้ในรัฐธรรมนูญ โดยรัฐธรรมนูญได้ห้ามมิให้มีการตรวจ การกัก หรือการเปิดเผยข้อมูลที่บุคคลสื่อสารถึงกันไม่ว่าในทางใด รวมทั้งการกระทำด้วยประการใด ๆ เพื่อให้ล่วงรู้หรือได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกัน เว้นแต่จะมีคำสั่งหรือหมายของศาล หรือมีเหตุอย่างอื่นตามที่กฎหมายบัญญัติ ตามมาตรา 36 (รัฐธรรมนูญแห่งราชอาณาจักรไทย, 2560) จากบทบัญญัติดังกล่าวจะเห็นได้ว่า อุปกรณ์อิเล็กทรอนิกส์ เช่น คอมพิวเตอร์ หรือโทรศัพท์มือถือ มีความเกี่ยวข้องอย่างใกล้ชิดกับสิทธิขั้นพื้นฐานของบุคคลในปัจจุบัน เนื่องจากอุปกรณ์เหล่านี้ถูกออกแบบให้สามารถใช้เป็นทั้งเครื่องมือในการจัดเก็บข้อมูลส่วนบุคคล และเป็นช่องทางในการติดต่อสื่อสารกับบุคคลอื่น (สาวตรี สุขศรี, 2563) ส่งผลให้อุปกรณ์อิเล็กทรอนิกส์กลายเป็นพื้นที่ที่รวบรวมข้อมูลส่วนบุคคลจำนวนมากของผู้ใช้งาน

ดังนั้น การที่รัฐจะเข้าถึงข้อมูลที่จัดเก็บอยู่ภายในอุปกรณ์อิเล็กทรอนิกส์ของบุคคลจึงอาจกระทบต่อสิทธิในความเป็นอยู่ส่วนตัวและเสรีภาพในการติดต่อสื่อสารของบุคคลได้ อย่างไรก็ตาม สิทธิดังกล่าวตามรัฐธรรมนูญมิใช่สิทธิเด็ดขาด (absolute right) หากแต่เป็นสิทธิที่มีเงื่อนไข (qualified right) ซึ่งอาจถูกจำกัดได้ภายใต้เงื่อนไขที่กฎหมายกำหนด เพื่อประโยชน์สาธารณะ เช่น ความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ หรือการป้องกันและปราบปรามอาชญากรรม (Australian Human Rights Commission, 2018) ด้วยเหตุนี้ รัฐจึงอาจเข้าถึงข้อมูลในอุปกรณ์

อิเล็กทรอนิกส์ของประชาชนได้ภายใต้กรอบที่กฎหมายกำหนด ทั้งนี้เพื่อให้เกิดความสมดุลระหว่างการคุ้มครองสิทธิและเสรีภาพของบุคคลตามหลักกระบวนการยุติธรรม (due process) กับความจำเป็นในการควบคุมอาชญากรรม (crime control)

2. นิยามพยานหลักฐานอิเล็กทรอนิกส์ในประเทศไทย

ปัจจุบัน กฎหมายหลักที่เกี่ยวข้องกับพยานหลักฐานในคดีอาญาของประเทศไทย ได้แก่ ประมวลกฎหมายวิธีพิจารณาความอาญา ยังมีได้บัญญัตินิยามของ “พยานหลักฐานอิเล็กทรอนิกส์” ไว้โดยเฉพาะ โดยมาตรา 226 ได้กำหนดประเภทของพยานหลักฐานไว้เพียงสามประเภท ได้แก่ พยานวัตถุ พยานเอกสาร และพยานบุคคล (ประมวลกฎหมายวิธีพิจารณาความอาญา พ.ศ. 2477, ม.ป.ป.) ดังนั้น ในทางปฏิบัติ พยานหลักฐานอิเล็กทรอนิกส์จึงต้องเข้าสู่กระบวนการพิจารณาในชั้นศาลในฐานะของพยานประเภทอื่น เช่น พยานเอกสาร หรือพยานวัตถุ ทั้งนี้ขึ้นอยู่กับลักษณะของข้อมูลหรือสื่อบันทึกข้อมูลนั้น ๆ เมื่อพิจารณาเทียบเคียงกับแนวคำพิพากษาศาลฎีกาที่ 7155/2539 ซึ่งวินิจฉัยเกี่ยวกับสถานะของพยานหลักฐานที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์แล้ว อาจกล่าวได้ว่าสถานะของพยานหลักฐานอิเล็กทรอนิกส์ในระบบกฎหมายไทยมีแนวโน้มที่จะถูกจัดให้เป็นพยานวัตถุ เนื่องจากข้อมูลดังกล่าวมักปรากฏอยู่ในสื่อบันทึกข้อมูลหรืออุปกรณ์ทางอิเล็กทรอนิกส์ที่สามารถตรวจสอบหรือพิสูจน์ได้โดยตรง

อย่างไรก็ตาม ในทางวิชาการ พยานหลักฐานอิเล็กทรอนิกส์มักถูกพิจารณาในฐานะพยานหลักฐานรูปแบบใหม่ที่มีลักษณะเฉพาะแตกต่างจากพยานหลักฐานแบบดั้งเดิม เนื่องจากข้อมูลดังกล่าวอยู่ในรูปแบบดิจิทัลและอาจถูกแก้ไข เปลี่ยนแปลง หรือทำซ้ำได้โดยง่าย

3. กรอบกฎหมายของประเทศไทย

ในปัจจุบัน อำนาจของรัฐในการเข้าถึงข้อมูลในอุปกรณ์อิเล็กทรอนิกส์ของบุคคลในประเทศไทยได้ถูกบัญญัติไว้ในกฎหมายหลายฉบับ เช่น พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547, 2547; และพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 (พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547; พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542, 2542) อย่างไรก็ตาม กฎหมายที่มีบทบาทสำคัญในเรื่องการเข้าถึงข้อมูลคอมพิวเตอร์โดยตรงคือ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัตินี้ได้กำหนดอำนาจของ “พนักงานเจ้าหน้าที่” ไว้ในมาตรา 18 โดยให้อำนาจในการดำเนินการเพื่อประโยชน์ในการสืบสวนและสอบสวนความผิดเกี่ยวกับคอมพิวเตอร์ เช่น การเรียกบุคคลที่เกี่ยวข้องมาให้ถ้อยคำ การเรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการ การส่งให้ส่งมอบข้อมูลคอมพิวเตอร์ การเข้าถึงระบบคอมพิวเตอร์ ตลอดจนการถอดรหัสข้อมูลคอมพิวเตอร์ และการยึดหรืออายัดระบบคอมพิวเตอร์เพื่อใช้เป็นพยานหลักฐานเกี่ยวกับการกระทำความผิด ตามมาตรา 18 (พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์, 2550) ทั้งนี้ ผู้ที่จะใช้อำนาจดังกล่าวได้ต้องเป็น “พนักงานเจ้าหน้าที่” ตามพระราชบัญญัตินี้ ซึ่งหมายถึงบุคคลที่รัฐมนตรีแต่งตั้งให้ปฏิบัติหน้าที่ตามพระราชบัญญัติ โดยกฎหมายได้กำหนดคุณสมบัติของพนักงานเจ้าหน้าที่ไว้ค่อนข้างเข้มงวด ทั้งในด้านวุฒิการศึกษา ความรู้ทางเทคโนโลยีสารสนเทศ และประสบการณ์ในการปฏิบัติงานที่เกี่ยวข้องกับการสืบสวนสอบสวนหรือการตรวจพิสูจน์พยานหลักฐานทางคอมพิวเตอร์ (ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550, 2550)

นอกจากนี้ เพื่อเป็นการคุ้มครองสิทธิและเสรีภาพของประชาชน พระราชบัญญัตินี้ยังได้กำหนดกลไกการตรวจสอบถ่วงดุลไว้ในมาตรา 19 โดยกำหนดให้การใช้อำนาจบางประการของพนักงานเจ้าหน้าที่ เช่น การทำสำเนาข้อมูลคอมพิวเตอร์ การเข้าถึงระบบคอมพิวเตอร์ การถอดรหัสข้อมูล หรือการยึดและอายัดระบบคอมพิวเตอร์ ต้องได้รับอนุญาตจากศาลก่อนดำเนินการ ทั้งนี้ คำร้องต่อศาลต้องแสดงเหตุอันควรเชื่อได้ว่ามีการกระทำความผิด

รวมทั้งต้องระบุนรายละเอียดเกี่ยวกับการใช้อำนาจดังกล่าวเพื่อให้ศาลพิจารณานุญาตโดยเร็ว ตามมาตรา 19 (พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550, 2550) บทบัญญัติดังกล่าวสะท้อนให้เห็นถึงความพยายามของกฎหมายไทยในการสร้างความสมดุลระหว่างการให้อำนาจแก่รัฐในการสืบสวนสอบสวนอาชญากรรมทางคอมพิวเตอร์ กับการคุ้มครองสิทธิและเสรีภาพของประชาชนตามหลักกระบวนการยุติธรรม

ปัญหาบางประการเกี่ยวกับการค้นเครื่องคอมพิวเตอร์เพื่อให้ได้มาซึ่งพยานหลักฐานในคดีอาญาของประเทศไทย

จากการพิจารณาบทบัญญัติของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จะเห็นได้ว่ากฎหมายดังกล่าวได้กำหนดกลไกในการเข้าถึงข้อมูลคอมพิวเตอร์เพื่อใช้เป็นพยานหลักฐานในการสืบสวนและสอบสวนคดีอาญา โดยมุ่งสร้างความสมดุลระหว่างการคุ้มครองสิทธิและเสรีภาพของบุคคลกับความจำเป็นในการป้องกันและปราบปรามอาชญากรรม (พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550, 2550)

อย่างไรก็ตาม เมื่อพิจารณาการนำบทบัญญัตินี้มาใช้รวมกับการดำเนินคดีอาญาตามประมวลกฎหมายวิธีพิจารณาความอาญา (ประมวลกฎหมายวิธีพิจารณาความอาญา พ.ศ. 2477, ม.ป.ป.) โดยเฉพาะในกรณีที่มีความผิดตามกฎหมายอื่นมีการใช้ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์เป็นองค์ประกอบของการกระทำความผิด หรือมีข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับการกระทำความผิดนั้น อาจก่อให้เกิดปัญหาทางกฎหมายบางประการเกี่ยวกับการเข้าถึงข้อมูลในอุปกรณ์อิเล็กทรอนิกส์ของบุคคล ปัญหาดังกล่าวสามารถพิจารณาได้ในประเด็นสำคัญต่อไปนี้

1. ปัญหาเรื่องสิทธิที่จะไม่ให้การปรักปรำตนเอง (right against self-incrimination)

สิทธิที่จะไม่ให้การปรักปรำตนเอง หรือสิทธิที่จะไม่ถูกบังคับให้สารภาพ เป็นสิทธิมนุษยชนสากล และเป็นส่วนหนึ่งของสิทธิที่ได้รับการดำเนินคดีอย่างเป็นธรรม (right to a fair trial) สำหรับประเทศไทย สิทธิดังกล่าวได้รับการรับรองไว้ในรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 มาตรา 29 วรรคสี่ ซึ่งบัญญัติว่า “ในคดีอาญาจะบังคับให้บุคคลให้การเป็นปฏิปักษ์ต่อตนเองมิได้” เหตุที่รัฐต้องให้ความคุ้มครองสิทธินี้แก่ประชาชน เนื่องจากในการดำเนินคดีอาญา รัฐมีหน้าที่พิสูจน์ความผิดของผู้ต้องหาหรือจำเลย ดังนั้น เพื่อให้เป็นไปตามหลักนิติธรรม รัฐจึงไม่อาจนำพยานหลักฐานที่ได้รับจากผู้ถูกดำเนินคดีโดยไม่สมัครใจ เช่น จากการถูกบังคับหรือถูกข่มขู่ มาใช้เป็นหลักฐานในการลงโทษ (ปกป้อง ศรีสนิท, 2564) ในประเด็นนี้ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 18 (7) ซึ่งบัญญัติให้ในกรณีที่ศาลมีคำสั่งอนุญาต พนักงานเจ้าหน้าที่ที่สามารถถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว อาจก่อให้เกิดข้อพิจารณาว่า หากพนักงานเจ้าหน้าที่สั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับทำการถอดรหัสลับ และเมื่อเจ้าหน้าที่เข้าถึงข้อมูลภายในเครื่องคอมพิวเตอร์แล้วพบข้อมูลที่สามารถนำมาใช้เป็นพยานหลักฐานในการลงโทษบุคคลดังกล่าวได้ การกระทำตามมาตรานี้จะเป็นการละเมิดต่อสิทธิที่จะไม่ให้การปรักปรำตนเองหรือไม่ (พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550, 2550)

ทั้งนี้ หากบุคคลดังกล่าวไม่ปฏิบัติตามคำสั่งให้ถอดรหัสลับ มาตรา 27 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้กำหนดโทษสำหรับผู้ที่ไม่ปฏิบัติตามคำสั่งของศาลหรือพนักงานเจ้าหน้าที่ที่สั่งตามมาตรา 18 โดยต้องระวางโทษปรับไม่เกินสองแสนบาท และปรับเป็นรายวันอีกไม่เกินวันละ

ห้าพันบาทจนกว่าจะปฏิบัติให้ถูกต้อง (พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550, 2550) จึงอาจเกิดข้อสงสัยว่าการใช้มาตรการดังกล่าวเป็นการทำให้เจ้าหน้าที่ของรัฐได้มาซึ่งพยานหลักฐานจากการบังคับหรือโดยไม่สมัครใจ และนำมาใช้เป็นหลักฐานในการลงโทษผู้ต้องหาหรือจำเลยหรือไม่

2. ปัญหาเรื่องความชอบด้วยกฎหมายของพยานหลักฐานในความผิดอื่นที่ได้มาโดยไม่ได้มีคำสั่งอนุญาตของศาล

นอกจากประเด็นปัญหาเกี่ยวกับสิทธิที่จะไม่ให้การปรักปรำตนเองแล้ว ปัญหาเรื่องความชอบด้วยกฎหมายของพยานหลักฐานในความผิดอื่นที่ได้มาโดยไม่ได้มีคำสั่งอนุญาตของศาลก็เป็นอีกประเด็นหนึ่งของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่ควรได้รับการพิจารณา มาตรา 19 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กำหนดให้ศาลที่มีเขตอำนาจเป็นผู้อนุญาตการใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา 18 (4) (5) (6) (7) และ (8) โดยพนักงานเจ้าหน้าที่ต้องยื่นคำร้องต่อศาล พร้อมระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำความผิดหรือกำลังจะกระทำความผิด เหตุผลความจำเป็นในการใช้อำนาจ ลักษณะของการกระทำความผิด รวมถึงรายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและตัวผู้กระทำความผิดเท่าที่สามารถระบุได้ ทั้งนี้ ศาลต้องพิจารณาคำร้องดังกล่าวโดยเร็ว (พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550, 2550)

อย่างไรก็ตาม อาจเกิดปัญหาในกรณีที่ศาลได้อนุญาตให้พนักงานเจ้าหน้าที่ใช้อำนาจตามมาตรา 18 (6) ซึ่งให้อำนาจในการตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดหรือเพื่อสืบสวนหาตัวผู้กระทำความผิด (พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550, 2550) ในความผิดฐานหนึ่ง เช่น ความผิดฐานฆ่าผู้อื่นโดยไตร่ตรองไว้ก่อนตามประมวลกฎหมายอาญา มาตรา 289 (4) (ประมวลกฎหมายอาญา, ม.ป.ป.) แต่ในระหว่างการดำเนินการแสวงหาพยานหลักฐานในคดีดังกล่าว พนักงานเจ้าหน้าที่กลับพบพยานหลักฐานที่สามารถนำไปสู่การลงโทษบุคคลนั้นในความผิดฐานอื่น เช่น ความผิดฐานวางเพลิงโดยมีเหตุฉกรรจ์ตามประมวลกฎหมายอาญา มาตรา 218 (ประมวลกฎหมายอาญา, ม.ป.ป.) กรณีดังกล่าวจึงก่อให้เกิดข้อพิจารณาว่า พยานหลักฐานที่พบเพิ่มเติมซึ่งเกี่ยวข้องกับความผิดอื่นที่มีได้ระบุไว้ในคำร้องขออนุญาตต่อศาลตั้งแต่ต้นนั้น จะสามารถนำมาใช้เป็นพยานหลักฐานที่ชอบด้วยกฎหมายในการดำเนินคดีอาญาได้หรือไม่

บทวิเคราะห์ประเด็นปัญหาบางประการเกี่ยวกับการค้นเครื่องคอมพิวเตอร์เพื่อให้ได้มาซึ่งพยานหลักฐานในคดีอาญาของประเทศไทย

จากข้อมูลดังกล่าวมาข้างต้นจะเห็นได้ว่า แม้ว่าพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งถือเป็นกฎหมายหลักของประเทศไทยที่ให้อำนาจพนักงานเจ้าหน้าที่ในการแสวงหาพยานหลักฐานในคดีอาญาจากอุปกรณ์อิเล็กทรอนิกส์ จะได้กำหนดหลักเกณฑ์เกี่ยวกับการใช้อำนาจของเจ้าหน้าที่ไว้ค่อนข้างรัดกุมเพื่อให้กระทบต่อสิทธิเสรีภาพของประชาชนให้น้อยที่สุดก็ตาม (พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550, 2550) แต่ในทางปฏิบัติก็ยังคงปรากฏประเด็นปัญหาบางประการ ดังที่ได้กล่าวไว้ในหัวข้อก่อนหน้านี้ ทั้งนี้ ประเด็นปัญหาดังกล่าวมิได้เกิดขึ้นเฉพาะในระบบกฎหมายของประเทศไทยเท่านั้น หากแต่เป็นปัญหาที่ปรากฏในหลายประเทศเช่นเดียวกัน โดยเฉพาะในประเทศที่มีการพัฒนากฎหมายเกี่ยวกับพยานหลักฐานอิเล็กทรอนิกส์และการค้นข้อมูลคอมพิวเตอร์มาอย่างต่อเนื่อง ดังนั้น การศึกษาเปรียบเทียบกฎหมายและแนวทางการแก้ไขปัญหของประเทศต่าง ๆ จึงอาจเป็นแนวทางหนึ่งที่จะช่วยให้ประเทศไทยสามารถพิจารณาและ

พัฒนาแนวทางที่เหมาะสมในการจัดการกับปัญหาดังกล่าวได้

1. บทวิเคราะห์ปัญหาเรื่องสิทธิที่จะไม่ให้เกิดการปรักปรำตนเอง

ประเด็นปัญหาเกี่ยวกับสิทธิที่จะไม่ให้เกิดการปรักปรำตนเองในกรณีของการบังคับให้บุคคลถอดรหัสข้อมูลคอมพิวเตอร์นั้น ในระดับสากลยังไม่มีข้อยุติที่เป็นเอกฉันท์ โดยประเทศต่าง ๆ มีแนวทางในการกำหนดกฎหมายที่แตกต่างกัน ทั้งนี้ อาจแบ่งแนวทางของประเทศต่าง ๆ ออกได้เป็นสองกลุ่มใหญ่

กลุ่มแรก คือกลุ่มประเทศที่กำหนดกฎหมายให้อำนาจอรัฐในการบังคับให้บุคคลให้ความช่วยเหลือในการถอดรหัสลับของข้อมูลคอมพิวเตอร์อย่างกว้างขวาง โดยอาจครอบคลุมทั้งเจ้าของข้อมูล บุคคลที่สาม และผู้ต้องหาหรือจำเลย ทั้งยังมีการกำหนดโทษในกรณีที่บุคคลไม่ปฏิบัติตามคำสั่งของเจ้าหน้าที่ ตัวอย่างเช่น ประเทศออสเตรเลียซึ่งมีพระราชบัญญัติอาชญากรรมทางไซเบอร์ พ.ศ. 2544 (Cybercrime Act (Cth), 2001) มาตรา 12 และมาตรา 28 ที่ให้อำนาจเจ้าหน้าที่ตำรวจซึ่งได้รับคำสั่งอนุญาตจากศาล สามารถกำหนดให้ “บุคคลที่ระบุเจาะจง” (a specified person) ต้องให้ข้อมูลหรือความช่วยเหลือใด ๆ ที่สมเหตุสมผลและจำเป็นเพื่อให้เจ้าหน้าที่สามารถเข้าถึงข้อมูลคอมพิวเตอร์ที่สามารถใช้เป็นพยานหลักฐานได้ ซึ่งรวมถึงการถอดรหัสลับแบบบังคับ โดยผู้ที่ฝ่าฝืนคำสั่งดังกล่าวอาจมีโทษจำคุกไม่เกิน 6 เดือน (Cybercrime Act (Cth), 2001)

อีกกลุ่มหนึ่ง คือกลุ่มประเทศที่กำหนดกฎหมายให้อำนาจอรัฐในการบังคับให้บุคคลให้ความช่วยเหลือในการถอดรหัสลับในขอบเขตที่จำกัดมากกว่า โดยไม่ครอบคลุมถึงผู้ต้องหาหรือจำเลย ตัวอย่างเช่น ประเทศเบลเยียมซึ่งมีกฎหมายว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ. 2543 (Loi du 28 novembre 2000 relative à la criminalité informatique, 2000) มาตรา 9 อนุญาตให้ศาลสามารถสั่งให้เจ้าหน้าที่ตรวจค้นระบบคอมพิวเตอร์ และให้ผู้ให้บริการโทรคมนาคมให้ความช่วยเหลือแก่หน่วยงานบังคับใช้กฎหมาย รวมถึงการถอดรหัสลับข้อมูลได้ โดยข้อมูลเกี่ยวกับการให้ความช่วยเหลือดังกล่าวจะต้องถูกเก็บรักษาเป็นความลับ อย่างไรก็ตาม การสั่งให้กระทำการดังกล่าวไม่อาจใช้บังคับกับผู้ต้องสงสัยหรือสมาชิกในครอบครัวของบุคคลดังกล่าวได้ ทั้งนี้ ผู้ที่ไม่ปฏิบัติตามคำสั่งอาจต้องระวางโทษจำคุกตั้งแต่ 6 เดือนถึง 1 ปี และ/หรือปรับตั้งแต่ 130 ถึง 100,000 ยูโร (Loi du 28 novembre 2000 relative à la criminalité informatique, 2000)

จากตัวอย่างข้างต้นจะเห็นได้ว่า ประเทศไทยมีแนวโน้มที่จะอยู่ในกลุ่มประเทศที่ให้อำนาจเจ้าหน้าที่ของรัฐซึ่งได้รับคำสั่งอนุญาตจากศาล สามารถใช้อำนาจในการแสวงหาพยานหลักฐานจากระบบคอมพิวเตอร์ได้ในขอบเขตที่ค่อนข้างกว้าง อย่างไรก็ตาม โทษในกรณีที่บุคคลไม่ปฏิบัติตามคำสั่งของพนักงานเจ้าหน้าที่ตามกฎหมายไทยกำหนดไว้เพียงโทษปรับเท่านั้น ตามมาตรา 27 (พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550, 2550) ซึ่งมีความรุนแรงน้อยกว่ากฎหมายของบางประเทศ เช่น ออสเตรเลีย สถานการณ์ดังกล่าวสะท้อนให้เห็นว่าแม้กฎหมายไทยจะให้อำนาจแก่เจ้าหน้าที่ในการแสวงหาพยานหลักฐานจากระบบคอมพิวเตอร์ค่อนข้างกว้าง แต่ในขณะเดียวกันก็ยังคงพยายามรักษาสสมดุลระหว่างประสิทธิภาพในการปราบปรามอาชญากรรมกับการคุ้มครองสิทธิของบุคคลอยู่ในระดับหนึ่ง

อย่างไรก็ตาม การกำหนดให้บุคคลต้องให้ความร่วมมือในการถอดรหัสลับของข้อมูลคอมพิวเตอร์ยังคงก่อให้เกิดข้อถกเถียงสำคัญว่า การกระทำดังกล่าวควรถูกมองว่าเป็นการบังคับให้บุคคลให้การเป็นปฏิปักษ์ต่อตนเองหรือไม่ ซึ่งเป็นประเด็นที่จำเป็นต้องพิจารณาอย่างรอบคอบในบริบทของการคุ้มครองสิทธิในกระบวนการยุติธรรมทางอาญา

2. บทวิเคราะห์ปัญหาเรื่องความชอบด้วยกฎหมายของพยานหลักฐานในความผิดอื่นที่ได้มาโดยไม่ได้รับคำสั่งอนุญาตของศาล

ปัญหาเรื่องความชอบด้วยกฎหมายของพยานหลักฐานในความผิดอื่นที่ไม่ได้มีคำสั่งอนุญาตของศาล เป็นอีกประเด็นหนึ่งที่ไม่ควรถูกมองข้าม เนื่องจากหลักกฎหมายเกี่ยวกับพยานหลักฐานในคดีอาญากำหนดให้พยานหลักฐานที่จะนำมาใช้ในการพิจารณาคดีต้องเป็นพยานหลักฐานที่ได้มาโดยชอบด้วยกฎหมายจึงจะสามารถรับฟังได้

สำหรับประเทศไทย หลักการดังกล่าวปรากฏอยู่ในประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226 ซึ่งบัญญัติว่า “พยานวัตถุ พยานเอกสาร หรือพยานบุคคลซึ่งน่าจะพิสูจน์ได้ว่าจำเลยมีผิดหรือบริสุทธิ์ ให้อ้างเป็นพยานหลักฐานได้ แต่ต้องเป็นพยานชนิดที่มีได้เกิดขึ้นจากการจงใจ มีคำมั่นสัญญา ชูเชิญ หลอกลวง หรือโดยมิชอบประการอื่น และให้สืบตามบทบัญญัติแห่งประมวลกฎหมายนี้หรือกฎหมายอื่นอันว่าด้วยการสืบพยาน” (ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226) ในทางทฤษฎี หลักการดังกล่าวมักถูกอธิบายผ่านหลักสากลที่เรียกว่า “ผลของต้นไม้พิษ” (fruit of the poisonous tree doctrine) ซึ่งมีวัตถุประสงค์เพื่อป้องกันไม่ให้มีการใช้พยานหลักฐานที่ได้มาโดยมิชอบด้วยกฎหมายในการดำเนินคดีอาญา อย่างไรก็ตาม นักกฎหมายไทยได้อธิบายหลักการตามมาตรา 226 โดยแยกพิจารณาออกเป็นสองประเด็น คือ “การเกิดขึ้นของพยานหลักฐาน” และ “วิธีการได้มาซึ่งพยานหลักฐาน” (สุรศักดิ์ ลิขสิทธิ์วัฒนกุล, 2563) กล่าวโดยสรุป หากพยานหลักฐานเกิดขึ้นโดยมิชอบ เช่น กรณีที่มีการข่มขู่ผู้ต้องหาให้รับสารภาพ พยานหลักฐานดังกล่าวย่อมไม่อาจรับฟังได้ แต่หากพยานหลักฐานนั้นเกิดขึ้นโดยชอบ แม้ว่าวิธีการได้มาจะไม่ชอบด้วยกฎหมาย ศาลก็อาจรับฟังพยานหลักฐานนั้นได้ (สุรศักดิ์ ลิขสิทธิ์วัฒนกุล, 2563)

แนวคิดดังกล่าวได้รับการรับรองไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226/1 ซึ่งเปิดโอกาสให้ศาลใช้ดุลพินิจในการรับฟังพยานหลักฐานที่เกิดขึ้นโดยชอบ แต่ได้มาเนื่องจากการกระทำโดยมิชอบ หรือได้มาโดยอาศัยข้อมูลที่เกิดขึ้นหรือได้มาโดยมิชอบ ทั้งนี้ ศาลต้องพิจารณาถึงพฤติการณ์แห่งคดีโดยคำนึงถึงปัจจัยต่าง ๆ เช่น คุณค่าในเชิงพิสูจน์ของพยานหลักฐาน ความร้ายแรงของความผิด และผลกระทบต่อสิทธิเสรีภาพของบุคคล เป็นต้น (ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226/1) ดังนั้น ในกรณีที่พนักงานเจ้าหน้าที่เข้าถึงข้อมูลในเครื่องคอมพิวเตอร์โดยอาศัยคำสั่งศาลเพื่อสืบสวนความผิดฐานหนึ่ง แต่กลับพบพยานหลักฐานที่เกี่ยวข้องกับความผิดอื่นซึ่งมิได้ระบุไว้ในคำร้องขออนุญาตต่อศาลตั้งแต่นั้น พยานหลักฐานดังกล่าวอาจถือว่าเป็นพยานหลักฐานที่มีอยู่โดยชอบ เพียงแต่วิธีการได้มานั้นอาจไม่สอดคล้องกับขอบเขตของคำสั่งศาล ดังนั้น ศาลจึงอาจใช้ดุลพินิจรับฟังพยานหลักฐานดังกล่าวได้ตามข้อยกเว้นในมาตรา 226/1 หากเห็นว่าการรับฟังพยานหลักฐานนั้นเป็นประโยชน์ต่อการอำนวยความยุติธรรมมากกว่าผลเสียที่อาจเกิดขึ้นต่อมาตรฐานของกระบวนการยุติธรรมทางอาญาหรือสิทธิเสรีภาพของประชาชน (ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226/1)

อย่างไรก็ตาม แนวทางดังกล่าวอาจก่อให้เกิดข้อวิพากษ์วิจารณ์ได้ว่าเป็นการใช้ข้อยกเว้นแทนหลัก กล่าวคือ แม้กฎหมายจะมีวัตถุประสงค์เพื่อคุ้มครองสิทธิของบุคคล แต่ในทางปฏิบัติกลับเปิดช่องให้พยานหลักฐานที่ได้มาโดยวิธีการที่ไม่ชอบด้วยกฎหมายสามารถถูกนำมาใช้ในการดำเนินคดีอาญาได้ ในประเด็นนี้ ศาลฎีกาแห่งสาธารณรัฐเกาหลีได้มีคำพิพากษาว่าหลักเกณฑ์ไว้ว่า หากหน่วยงานบังคับใช้กฎหมายกำลังค้นหาข้อมูลอิเล็กทรอนิกส์โดยชอบด้วยกฎหมายตามคำสั่งศาล และพบข้อมูลที่เกี่ยวข้องกับความผิดอื่นซึ่งแตกต่างหากจากความผิดที่ได้รับอนุญาตไว้ หน่วยงานบังคับใช้กฎหมายจะต้องยุติการค้นหาข้อมูลในส่วนดังกล่าวก่อน และต้องยื่นคำร้องขออนุญาตต่อศาลแยกต่างหาก จึงจะสามารถดำเนินการยึดหรือค้นหาข้อมูลดังกล่าวต่อไปได้โดยชอบด้วยกฎหมาย (Supreme Court of Korea, 2015) แนวทางดังกล่าวไม่เพียงแต่ช่วยคุ้มครองสิทธิของบุคคลเท่านั้น แต่ยังทำให้การได้มาซึ่งพยานหลักฐานของเจ้าหน้าที่รัฐเป็นไปโดยชอบด้วยกฎหมาย และสามารถนำมาใช้ในการดำเนินคดีได้โดยไม่ต้องอาศัยข้อยกเว้นตามมาตรา 226/1 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา (ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226/1) ดังนั้น แนวทางของศาลฎีกาเกาหลีจึงอาจถือเป็นอีกแนวทางหนึ่งที่ประเทศไทยสามารถนำมาพิจารณาเพื่อพัฒนาหลักเกณฑ์ในการแสวงหาพยานหลักฐานจากข้อมูลอิเล็กทรอนิกส์ให้มีความสมดุลระหว่าง

ประสิทธิภาพในการบังคับใช้กฎหมายและการคุ้มครองสิทธิเสรีภาพของประชาชน ประเด็นดังกล่าวจึงสะท้อนให้เห็นว่ากฎหมายไทยยังขาดหลักเกณฑ์ที่ชัดเจนเกี่ยวกับการจัดการพยานหลักฐานที่พบโดยบังเอิญจากการค้นข้อมูลคอมพิวเตอร์ ซึ่งควรได้รับการพิจารณาเพื่อกำหนดแนวทางที่ชัดเจนต่อไป

จากการศึกษากฎหมายไทยและการเปรียบเทียบกับกฎหมายต่างประเทศข้างต้น จะเห็นได้ว่าปัญหาการค้นเครื่องคอมพิวเตอร์เพื่อให้ได้มาซึ่งพยานหลักฐานในคดีอาญามีความเกี่ยวข้องโดยตรงกับการสร้างดุลยภาพระหว่างการคุ้มครองสิทธิขั้นพื้นฐานของบุคคลกับความจำเป็นของรัฐในการปราบปรามอาชญากรรมในยุคดิจิทัล ดังนั้นการกำหนดกลไกทางกฎหมายที่ชัดเจนเกี่ยวกับอำนาจในการเข้าถึงข้อมูลและการถอดรหัสลับจึงมีความสำคัญอย่างยิ่งต่อความชอบด้วยกฎหมายของพยานหลักฐานอิเล็กทรอนิกส์ในกระบวนการยุติธรรมทางอาญา

ข้อเสนอแนะ

จากการวิเคราะห์เปรียบเทียบกฎหมายต่างประเทศเกี่ยวกับการค้นและเข้าถึงข้อมูลในเครื่องคอมพิวเตอร์ในคดีอาญา บทความนี้จึงเสนอแนวทางในการสร้างดุลยภาพระหว่างการคุ้มครองสิทธิขั้นพื้นฐานของประชาชน ดังต่อไปนี้

ประการแรก บทความเสนอกรอบแนวคิดในการคุ้มครองสิทธิที่จะไม่ให้เกิดการปรักปรำตนเอง โดยเสนอให้จำกัดการบังคับให้ความร่วมมือในการถอดรหัสหรือเข้าถึงข้อมูลเฉพาะบุคคลที่มีผู้ต้องสงสัยหรือสมาชิกในครอบครัวของผู้ต้องสงสัย พร้อมทั้งกำหนดบทบาทของศาลและโทษทางอาญาที่ได้สัดส่วน เพื่อให้สอดคล้องกับ principle of equality of arms และหลักการพิจารณาคดีที่เป็นธรรม

ประการที่สอง บทความเสนอแนวทางเกี่ยวกับความชอบด้วยกฎหมายของพยานหลักฐานในความผิดอื่นที่ตรวจพบระหว่างการค้นข้อมูลอิเล็กทรอนิกส์ โดยเสนอให้รับรองความชอบด้วยกฎหมายของพยานหลักฐานดังกล่าวภายใต้การอนุญาตเดิมของศาล พร้อมกำหนดหน้าที่แจ้งศาลภายหลังโดยเร็ว เพื่อสร้างความชัดเจนทางกฎหมายควบคู่กับการกำกับตรวจสอบโดยศาล และการคุ้มครองสิทธิของประชาชนอย่างเหมาะสมในบริบทของประเทศไทย

องค์ความรู้ใหม่

บทความนี้เสนอองค์ความรู้ใหม่ในด้านกฎหมายวิธีพิจารณาความอาญาเกี่ยวกับการค้นเครื่องคอมพิวเตอร์เพื่อให้ได้มาซึ่งพยานหลักฐานในคดีอาญา โดยมีประเด็นสำคัญดังต่อไปนี้

ประการแรก บทความเสนอกรอบการวิเคราะห์การค้นข้อมูลอิเล็กทรอนิกส์โดยแยกออกเป็น 2 ระดับ ได้แก่ 1) การเข้าถึงอุปกรณ์คอมพิวเตอร์ และ 2) การเข้าถึงข้อมูลภายในอุปกรณ์ ซึ่งเป็นขั้นตอนที่มีผลกระทบต่อสิทธิของบุคคลแตกต่างกัน การจำแนกดังกล่าวช่วยให้เห็นความแตกต่างระหว่างการค้นทรัพย์สินทางกายภาพกับการเข้าถึงข้อมูลอิเล็กทรอนิกส์ และช่วยอธิบายช่องว่างของการบังคับใช้กฎหมายที่ยังไม่มีบัญญัติรองรับอย่างชัดเจน

ประการที่สอง บทความได้วิเคราะห์หลักสิทธิที่จะไม่ให้เกิดการปรักปรำตนเองในบริบทของข้อมูลอิเล็กทรอนิกส์ โดยแยกความแตกต่างระหว่างการให้ถ้อยคำรับสารภาพกับการให้ความร่วมมือในการเปิดเผยข้อมูลทางเทคนิค เช่น รหัสผ่านหรือการถอดรหัสข้อมูล ซึ่งเป็นประเด็นที่กฎหมายไทยยังไม่มีแนวทางวินิจฉัยที่ชัดเจน การวิเคราะห์ดังกล่าวช่วยขยายความเข้าใจเกี่ยวกับขอบเขตของสิทธิในกระบวนการยุติธรรมให้ครอบคลุมบริบทเทคโนโลยีสารสนเทศมากยิ่งขึ้น

ประการที่สาม บทความได้เชื่อมโยงหลักความชอบด้วยกฎหมายของพยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 226 และ 226/1 กับกรณีการค้นพบความผิดอื่นในระหว่างการตรวจสอบข้อมูล

อิเล็กทรอนิกส์ โดยชี้ให้เห็นความจำเป็นในการกำหนดขอบเขตการใช้ข้อมูลที่ได้มาให้สอดคล้องกับหลักความได้สัดส่วนและการคุ้มครองสิทธิของบุคคล

องค์ความรู้ที่ได้จากการศึกษานี้ช่วยให้เกิดความเข้าใจเชิงระบบเกี่ยวกับการใช้อำนาจของรัฐในการค้นและเข้าถึงข้อมูลอิเล็กทรอนิกส์ อันเป็นพื้นฐานสำคัญสำหรับการพัฒนากฎหมายและแนวทางปฏิบัติด้านพยานหลักฐานอิเล็กทรอนิกส์ในประเทศไทยต่อไป

บทสรุป

จากการศึกษาข้างต้นจะเห็นได้ว่า ปัจจุบันพยานหลักฐานในรูปแบบอิเล็กทรอนิกส์มีบทบาทสำคัญในการพิสูจน์ข้อเท็จจริงทั้งในกระบวนการยุติธรรมทางแพ่งและทางอาญา สำหรับประเทศไทย กฎหมายสำคัญที่เกี่ยวข้องกับการแสวงหาและการใช้พยานหลักฐานประเภทดังกล่าวคือ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งเปิดโอกาสให้นำข้อมูลคอมพิวเตอร์มาใช้เป็นพยานหลักฐานในกระบวนการพิจารณาคดีได้ อย่างไรก็ตาม การค้นและเข้าถึงข้อมูลในอุปกรณ์อิเล็กทรอนิกส์มีลักษณะแตกต่างจากการค้น ยึด หรืออายัดพยานวัตถุหรือพยานเอกสารทั่วไป เนื่องจากข้อมูลอิเล็กทรอนิกส์จำเป็นต้องผ่านกระบวนการตรวจสอบและดึงข้อมูลจากอุปกรณ์ที่ใช้เก็บข้อมูลก่อนจึงจะสามารถนำมาใช้เป็นพยานหลักฐานได้ อีกทั้งการเข้าถึงข้อมูลดังกล่าวยังต้องอาศัยบุคลากรที่มีความรู้ความเชี่ยวชาญเฉพาะด้านและผ่านการอบรมตามที่กฎหมายกำหนด จากการวิเคราะห์กฎหมายที่เกี่ยวข้อง บทความนี้พบประเด็นปัญหาทางกฎหมายที่สำคัญสองประการ

ประการแรก คือปัญหาเกี่ยวกับการบังคับให้บุคคลถอดรหัสลับของข้อมูลคอมพิวเตอร์ตามมาตรา 18 (7) แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งให้อำนาจเจ้าหน้าที่ขอให้ศาลมีคำสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ทำการถอดรหัสลับหรือให้ความร่วมมือแก่เจ้าหน้าที่ ทั้งนี้ หากบุคคลดังกล่าวไม่ปฏิบัติตามคำสั่งศาล อาจต้องรับโทษปรับตามมาตรา 27 ของกฎหมายฉบับเดียวกัน ประเด็นดังกล่าวจึงก่อให้เกิดข้อพิจารณาว่า การบังคับให้บุคคลเปิดเผยหรือถอดรหัสลับข้อมูลของตนอาจเป็นการละเมิดต่อสิทธิที่จะไม่ให้การปรักปรำตนเอง (right against self-incrimination) หรือไม่ เมื่อพิจารณาเปรียบเทียบกับกฎหมายของต่างประเทศ พบว่าประเทศต่าง ๆ มีแนวทางกำหนดกฎหมายแตกต่างกันออกเป็นสองแนวทางหลักได้แก่ แนวทางที่ให้อำนาจเจ้าหน้าที่สามารถบังคับให้บุคคลทุกฝ่ายให้ความช่วยเหลือแก่เจ้าหน้าที่ และแนวทางที่จำกัดการบังคับดังกล่าวเฉพาะบุคคลที่มีผู้ต้องสงสัยหรือบุคคลในครอบครัวของผู้ต้องสงสัย โดยเมื่อพิจารณาประกอบกับหลักสิทธิที่จะไม่ให้การปรักปรำตนเองและหลักความเสมอภาคของอาวุธ (equality of arms) ซึ่งเป็นหลักสำคัญของการพิจารณาคดีที่เป็นธรรม (fair trial) บทความนี้จึงเสนอว่าประเทศไทยควรปรับปรุงกฎหมายโดยนำแนวทางของประเทศเบลเยียมมาใช้ กล่าวคือ ให้ศาลสามารถสั่งให้บุคคลใดก็ตาม ยกเว้นผู้ต้องสงสัยหรือบุคคลในครอบครัวของผู้ต้องสงสัย ต้องให้ความช่วยเหลือแก่เจ้าหน้าที่ในการถอดรหัสลับของข้อมูลคอมพิวเตอร์ โดยข้อมูลที่เกี่ยวข้องกับการให้ความช่วยเหลือดังกล่าวต้องถูกเก็บรักษาเป็นความลับ และควรกำหนดบทลงโทษทั้งจำคุกและปรับในกรณีที่มิปฏิบัติตามคำสั่งศาล เพื่อให้เกิดความสมดุลระหว่างการบังคับใช้กฎหมายและการคุ้มครองสิทธิเสรีภาพของประชาชนมากยิ่งขึ้น

ประการที่สอง คือปัญหาเกี่ยวกับความชอบด้วยกฎหมายของพยานหลักฐานในความผิดอื่นที่พบเพิ่มเติมจากการค้นข้อมูลคอมพิวเตอร์ ซึ่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มิได้กำหนดหลักเกณฑ์เกี่ยวกับประเด็นดังกล่าวไว้อย่างชัดเจน อันอาจก่อให้เกิดปัญหาในการรับฟังพยานหลักฐานในคดีอาญา เมื่อพิจารณาเปรียบเทียบกับแนวทางของสาธารณรัฐเกาหลีซึ่งกำหนดให้เจ้าหน้าที่ต้องยื่นคำร้องขอ

อนุญาตต่อศาลทุกครั้งที่พบพยานหลักฐานที่เกี่ยวข้องกับความผิดอื่นเพิ่มเติม บทความนี้เห็นว่าแนวทางดังกล่าวอาจทำให้กระบวนการสืบสวนสอบสวนเกิดความล่าช้าและอาจส่งผลกระทบต่อประสิทธิภาพของกระบวนการยุติธรรมทางอาญา

ดังนั้น บทความนี้จึงเสนอให้มีการบัญญัติกฎหมายเพิ่มเติมเพื่อกำหนดหลักเกณฑ์ในกรณีดังกล่าวให้ชัดเจน โดยกำหนดว่า เมื่อเจ้าหน้าที่ได้รับอนุญาตจากศาลให้เข้าถึงข้อมูลคอมพิวเตอร์ในคดีหนึ่งโดยชอบด้วยกฎหมายแล้ว หากต่อมาพบพยานหลักฐานที่เกี่ยวข้องกับการกระทำความผิดในคดีอื่นเพิ่มเติม ให้ถือว่าพยานหลักฐานดังกล่าวสามารถนำมาใช้เป็นพยานหลักฐานได้เช่นเดียวกับพยานหลักฐานในคดีเดิม แต่เจ้าหน้าที่จะต้องแจ้งเหตุดังกล่าวต่อศาลที่อนุญาตให้ดำเนินการค้นโดยเร็วที่สุด การกำหนดหลักเกณฑ์ดังกล่าวจะช่วยสร้างความชัดเจนทางกฎหมาย ทำให้เจ้าหน้าที่สามารถปฏิบัติหน้าที่ได้อย่างมั่นใจมากขึ้น ขณะเดียวกันก็ช่วยลดข้อโต้แย้งเกี่ยวกับการละเมิดสิทธิเสรีภาพของประชาชน และส่งเสริมให้เกิดความสมดุลระหว่างประสิทธิภาพในการบังคับใช้กฎหมายกับการคุ้มครองสิทธิมนุษยชนในกระบวนการยุติธรรมทางอาญา

เอกสารอ้างอิง

- ณรงค์ ใจหาญ. (2565). เอกสารประกอบการอบรมหลักสูตรการสืบสวนสอบสวนและการรับฟังพยานหลักฐานอิเล็กทรอนิกส์ รุ่นที่ 3. สถาบันเพื่อการยุติธรรมแห่งประเทศไทย.
- ปกป้อง ศรีสนธิ. (2564). สิทธิของปวงชนชาวไทยตามรัฐธรรมนูญ: สิทธิที่จะไม่ให้การปรักปรำตนเองหรือไม่ถูกบังคับให้สารภาพ. The 101.World. <https://www.the101.world/right-to-remain-silent/>.
- ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550. (2550, 23 สิงหาคม). ราชกิจจานุเบกษา. เล่ม 124 ตอนพิเศษ 102ง. หน้า 9.
- ประมวลกฎหมายวิธีพิจารณาความอาญา พ.ศ. 2477. (ม.ป.ป.). ประเทศไทย.
- ประมวลกฎหมายอาญา. (ม.ป.ป.). ประเทศไทย
- พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547. (2547, 19 มกราคม). ราชกิจจานุเบกษา. เล่ม 121 ตอนที่ 8 ก. หน้า 1-6.
- พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542. (2542, 21 เมษายน). ราชกิจจานุเบกษา. เล่ม 116 ตอนที่ 29 ก. หน้า 1-39.
- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550. (2550, 18 มิถุนายน). ราชกิจจานุเบกษา. เล่ม 124 ตอนที่ 27 ก. หน้า 4-13.
- พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544. (2544, 4 ธันวาคม). ราชกิจจานุเบกษา. เล่ม 118 ตอนที่ 112 ก. หน้า 1-20.
- รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560. (2560, 6 เมษายน). ราชกิจจานุเบกษา. เล่ม 134 ตอนที่ 40 ก. หน้า 1-90.
- สาวตรี สุขศรี. (2563). กฎหมายว่าด้วยอาญากรรมคอมพิวเตอร์และอาญากรรมไซเบอร์ (พิมพ์ครั้งที่ 2). มหาวิทยาลัยธรรมศาสตร์.
- สุรศักดิ์ ลิขสิทธิ์วัฒนกุล. (2563). ประมวลกฎหมายวิธีพิจารณาความอาญา ฉบับอ้างอิง (พิมพ์ครั้งที่ 20). วิญญูชน.

- Australian Human Rights Commission. (2018). *Annual report 2017–2018*. Australian Human Rights Commission.
https://humanrights.gov.au/resource-hub/human-rights/annual-report-2017-2018?utm_source=copilot.com.
- Charlton, E. (2024). 2023 was a big year for cybercrime—here’s how we can make our systems safer. *World Economic Forum*. <https://www.weforum.org/agenda/2024/01/cybersecurity-cybercrime-system-safety/>.
- Cybercrime Act 2001 (Cth). (2001, December 21). Federal Register of Legislation.
<https://www.legislation.gov.au/C2004A00937>.
- Cornell Law School. (2024). *Best evidence rule*. Legal Information Institute.
https://www.law.cornell.edu/wex/best_evidence_rule.
- Loi du 28 novembre 2000 relative à la criminalité informatique. (2000, 28 Novembre). Moniteur belge, 2000–11–28/34.
https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2000112834&table_name=loi.
- Supreme Court of Korea. (2015). Supreme Court en banc decision 2011Mo1839 (Decided July 23, 2015).