แนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา*

The guidelines for personal data protection in criminal investigation

รติมา สุระรัตน์ชัย
Ratima Suraratchai

นิสิตในหลักสูตรนิติศาสตรมหาบัณฑิต
คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ถนนพญาไท แขวงวังใหม่ เขตปทุมวัน กรุงเทพฯ 10330
LL.M Candidate
Faculty of Law, Chulalongkorn University, Phayathai Road, Pathumwan, Bangkok 10330
Corresponding author E-mail: rsuraratchai@gmail.com
(Received: November 14, 2022; Revised: December 18, 2022; Accepted: December 26, 2022)

บทคัดย่อ

การสืบสวนและสอบสวนคดีอาญาได้รับยกเว้นไม่ให้อยู่ภายใต้บังคับของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เว้นแต่ส่วนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ทำให้การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาต้องอาศัยมาตรการทางกฎหมายที่มีอยู่เดิม ซึ่งมีข้อจำกัดและมีมาตรฐานไม่เทียบเท่ากับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นเหตุให้ข้อมูลส่วนบุคคลไม่ได้รับการคุ้มครองจากการดำเนินงานในชั้นสืบสวนและสอบสวนคดีอาญาอย่างเหมาะสม และอาจส่งผลให้ประเทศไทยถูกพิจารณาได้ว่ามีระดับการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอตามมาตรฐานของสากล บทความนี้จึงมุ่งศึกษาวิเคราะห์แนวคิดและทฤษฎีที่เกี่ยวข้อง ตลอดจนแนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาตามกฎหมายระหว่างประเทศและกฎหมายต่างประเทศ ทั้งนี้ เพื่อกำหนดแนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาที่เหมาะสมและสอดคล้องกับบริบทของกระบวนการยุติธรรมทางอาญาไทยต่อไป

คำสำคัญ: การคุ้มครองข้อมูลส่วนบุคคล, สิทธิส่วนบุคคล, การสืบสวนและสอบสวนคดีอาญา

* บทความวิจัยนี้เป็นส่วนหนึ่งและเรียบเรียงจากวิทยานิพนธ์เรื่อง “แนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา” หลักสูตรนิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

Abstract

Criminal investigations are exempt from being subject to the Personal Data Protection Act B.E. 2562 (2019), except for the security of personal data. As a result, the protection of personal data in criminal investigations relies on existing legal measures. This is limited and has standards not comparable to the Personal Data Protection Act B.E. 2562 (2019). This may result in Thailand being considered to have inadequate personal data protection by international standards. This paper, therefore, focuses on the study, and analysis of relevant concepts and theories, as well as approaches to the protection of personal data in the criminal investigation of international law and foreign law. In this regard, to establish guidelines for the protection of personal data in criminal investigations that are appropriate and consistent with the context of the Thai criminal justice system.

Keywords: Personal data protection, Privacy right, Criminal investigation

1. ความเป็นมาและความสำคัญของปัญหา

ท่ามกลางกระแสความตื่นตัวจากการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หลายภาคส่วนในประเทศไทยกลับให้น้ำหนักไปที่การคุ้มครองข้อมูลของผู้บริโภคเป็นหลัก ทั้งที่ในความเป็นจริง ปัญหาการละเมิดข้อมูลส่วนบุคคลมีอยู่ด้วยกันสองประเด็นหลัก ได้แก่ การใช้ประโยชน์จากข้อมูลของกลุ่มธุรกิจประการหนึ่ง และการที่รัฐต้องการควบคุมประชาชนผ่านการสอดแนมข้อมูลอีกประการหนึ่ง[1] ซึ่งในประเด็นของการสอดแนมข้อมูลโดยรัฐ มีข้อสังเกตว่า การสืบสวนและสอบสวนคดีอาญาเป็นเหตุผลหนึ่งที่รัฐมักนำมาใช้เพื่อสร้างความชอบธรรมในการก้าวล่วงข้อมูลส่วนบุคคลของประชาชน[2] แต่การสืบสวนและสอบสวนคดีอาญาของประเทศไทยกลับได้รับยกเว้นมิให้อยู่ภายใต้บังคับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพียงแต่ต้องจัดการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐานเท่านั้น[3] เป็นเหตุให้การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาในประเทศไทยจำต้องอาศัยมาตรการทางกฎหมายที่มีอยู่เดิมเป็นหลัก คือ ประมวลกฎหมายวิธีพิจารณาความอาญาและกฎหมายอื่นที่เกี่ยวข้องกับวิธีพิจารณาความอาญา (ซึ่งต่อไป

---

[1] นคร เสรีรักษ์, “ความเป็นส่วนตัวภายใต้รัฐธรรมนูญฉบับใหม่ “ต้องจับตา” [ออนไลน์] แหล่งที่มา: https://ilaw.or.th/node/4255 [23 กันยายน 2564]

[2] สาวตรี สุขศรี, **กฎหมายว่าด้วยอาชญากรรมคอมพิวเตอร์และอาชญากรรมไซเบอร์,** (กรุงเทพฯ: โครงการตำราและเอกสารประกอบการสอน คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2563), หน้า 396-400.

[3] มาตรา 4 วรรคหนึ่ง (2) และ (5) ประกอบกับวรรคสาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

บทความฉบับนี้จะเรียกรวมว่า “กฎหมายวิธีพิจารณาความอาญา”) และหมวด 3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

เมื่อการสืบสวนและสอบสวนคดีอาญาในประเทศไทยยังคงต้องอาศัยมาตรการทางกฎหมายที่มีอยู่เดิม การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาจึงมีมาตรฐานที่ไม่เทียบเท่ากับการดำเนินการประเภทอื่น ที่ได้ยกระดับมาตรฐานไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งสภาพปัญหาดังกล่าวไม่เพียงส่งผลกระทบต่อความเป็นส่วนตัวในข้อมูลของประชาชนชาวไทย แต่ยังอาจมีผลกระทบต่อการแลกเปลี่ยนถ่ายโอนข้อมูลระหว่างประเทศอีกด้วย จึงมีความจำเป็นที่ประเทศไทยจะต้องกำหนดแนวทางในการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาให้สอดคล้องกับมาตรฐานสากลต่อไป

ทั้งนี้ การศึกษาแนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาในบทความนี้ประกอบด้วย 6 หัวข้อหลัก โดยเริ่มศึกษาตั้งแต่ (1) แนวคิดและทฤษฎีที่เกี่ยวข้อง ในหัวข้อที่ 3 (2) บทบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาของประเทศไทย ในหัวข้อที่ 4 จากนั้นจึงจะศึกษาเปรียบเทียบกับ (3) แนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาของสหภาพยุโรป ในหัวข้อที่ 5 และ (4) กรณีศึกษาแนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาของต่างประเทศ ในหัวข้อที่ 6 (5) เพื่อวิเคราะห์ความเหมาะสมของการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา ในหัวข้อที่ 7 ก่อนจะนำมาสู่ (6) ข้อเสนอแนะในหัวข้อที่ 8 ต่อไป

2. ระเบียบวิธีวิจัย

ระเบียบวิธีวิจัยจะประกอบด้วย วัตถุประสงค์การวิจัย (หัวข้อที่ 2.1) สมมติฐานการวิจัย (หัวข้อที่ 2.2) วิธีดำเนินงานวิจัย (หัวข้อที่ 2.3) รวมถึงขอบเขตการวิจัย (หัวข้อที่ 2.4) ดังนี้

2.1 วัตถุประสงค์การวิจัย

1.) เพื่อให้คนในสังคมไทยตระหนักถึงความจำเป็นของการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา ในฐานะหลักประกันสิทธิขั้นพื้นฐาน

2.) เพื่อวิเคราะห์แนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา โดยศึกษาเปรียบเทียบกับกฎหมายระหว่างประเทศและกฎหมายต่างประเทศ

3.) เพื่อเสนอแนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาที่เหมาะสมกับลักษณะของกระบวนการยุติธรรมทางอาญาในประเทศไทย

2.2 สมมติฐาน

แม้การสืบสวนและสอบสวนคดีอาญามีความจำเป็นต้องเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลจำนวนมาก แต่ประเทศไทยกลับไม่มีมาตรการทางกฎหมายที่เหมาะสมเพียงพอในการคุ้มครองข้อมูลส่วนบุคคลในกระบวนการดังกล่าว เป็นเหตุให้ความเป็นส่วนตัวของประชาชนถูกละเมิดเกินกว่าที่จำเป็น จึงสมควรกำหนดแนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาเป็นการเฉพาะ พร้อมกำหนดให้องค์กรอิสระมีบทบาทตรวจสอบกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคลในชั้นนี้เพิ่มเติม

2.3 วิธีดำเนินงานวิจัย

การศึกษาวิจัยนี้เป็นการศึกษาวิจัยทางเอกสาร (Documentary Research) โดยค้นคว้าและรวบรวมข้อมูลที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาจากแหล่งข้อมูลทั้งภายใน ประเทศไทยและต่างประเทศมาวิเคราะห์เปรียบเทียบเพื่อนำมาสู่ข้อเสนอแนะต่อไป

2.4 ขอบเขตการวิจัย

บทความฉบับนี้เป็นการวิจัยทางนิติศาสตร์ ซึ่งมุ่งศึกษาแนวทางในการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา โดยจำกัดขอบเขตการศึกษาเฉพาะมาตรการทางกฎหมายที่มีลักษณะเป็นหลักเกณฑ์กลางทั่วไป มิได้ทำการศึกษาในรูปแบบเป็นรายกิจกรรมหรือรายกรณีไป

3. แนวคิดและทฤษฎีที่เกี่ยวข้อง

การคุ้มครองข้อมูลส่วนบุคคลนั้นถือเป็นส่วนหนึ่งของการคุ้มครองความเป็นอยู่ส่วนตัวของบุคคล สิทธิในข้อมูลส่วนบุคคลจึงเป็นสิทธิมนุษยชนขั้นพื้นฐาน ทั้งยังเป็นสิทธิและเสรีภาพของพลเมืองที่ได้รับการรับรองในกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (International Covenant on Civil and Political Rights: “ICCPR”) ความว่า “บุคคลจะถูกแทรกแซงความเป็นส่วนตัว ครอบครัว เคหสถาน หรือการติดต่อสื่อสารโดยพลการหรือโดยไม่ชอบด้วยกฎหมายมิได้ และจะถูกลบหลู่เกียรติและชื่อเสียงโดยไม่ชอบด้วยกฎหมายมิได้ และบุคคลทุกคนย่อมมีสิทธิได้รับความคุ้มครองตามกฎหมายมิให้ถูกแทรกแซงหรือลบหลู่นั้น”[4]

แม้สิทธิในข้อมูลส่วนบุคคลจะได้รับการยอมรับเป็นการทั่วไปว่าเป็นสิทธิมนุษยชนขั้นพื้นฐาน แต่ก็ไม่ใช่สิทธิเด็ดขาด[5] สิทธิในข้อมูลส่วนบุคคลจึงอาจถูกจำกัดเพื่อให้ความคุ้มครองคุณค่าอื่นที่เหนือกว่า ซึ่งรวมถึงการจำกัดในชั้นสืบสวนและสอบสวนคดีอาญา เพราะเมื่อพิจารณาถึงความจำเป็นด้านประโยชน์

[4] Article 17 International Covenant on Civil and Political Rights

[5] คณาธิป ทองรวีวงศ์, **คำอธิบาย หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล**, พิมพ์ครั้งที่ 2 (กรุงเทพฯ: นิติธรรม, 2565), หน้า 16.

สาธารณะ การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลก็เป็นส่วนหนึ่งของการแสวงหาข้อเท็จจริงและพยานหลักฐาน

อย่างไรก็ตาม มิได้หมายความว่าพนักงานสืบสวนและสอบสวนจะสามารถเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลได้อย่างไร้ขอบเขต เพราะหลักการพื้นฐานของกระบวนการยุติธรรมอาญาคือการรักษาสมดุลระหว่างการป้องกันและปราบปรามอาชญากรรมกับหลักประกันสิทธิและเสรีภาพของประชาชน การใช้อำนาจสืบสวนและสอบสวนจึงต้องเลือกมาตรการที่เหมาะสม ซึ่งก่อให้เกิดผลกระทบที่น้อยที่สุด และประโยชน์สำคัญที่ได้จากการใช้อำนาจนั้นจะต้องมีน้ำหนักมากกว่าผลร้ายที่เกิดขึ้นจากการจำกัดสิทธิและเสรีภาพของประชาชนตาม “หลักความได้สัดส่วน” (Principle of Proportionality)[6]

ดังนั้น ความท้าทายของการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาจึงเป็นเรื่องของการรักษาสมดุลระหว่างประโยชน์สาธารณะกับสิทธิส่วนบุคคล ไม่ให้โน้มเอียงไปทางใดทางหนึ่งจนเกินไป โดยสำนักงานข้าหลวงใหญ่เพื่อสิทธิมนุษยชนแห่งสหประชาชาติ (OHCHR) ได้ให้ข้อเสนอแนะในรายงาน เรื่อง สิทธิความเป็นส่วนตัวในยุคดิจิทัลว่า รัฐต้องประกันระดับการคุ้มครองข้อมูลส่วนบุคคลตามมาตรฐานขั้นต่ำตามกติการะหว่างประเทศหรือแนวปฏิบัติระหว่างประเทศที่เกี่ยวข้อง[7] ซึ่งในประเทศไทย แนวปฏิบัติขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD Guidelines) และกฎหมายสหภาพยุโรป (EU Directives) จะอิทธิพลต่อการยกร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยเป็นอย่างมาก แม้จะไม่มีผลผูกพันทางกฎหมายก็ตาม เนื่องจากมาตรฐานระหว่างประเทศทั้งสองเรียกร้องให้รัฐอื่นที่ติดต่อสัมพันธ์กับรัฐสมาชิกจะต้องมีกฎเกณฑ์ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลไม่ต่ำกว่ามาตรฐานที่กำหนด[8]

อนึ่ง มีข้อสังเกตว่าในส่วนที่เกี่ยวข้องกับการสืบสวนและสอบสวนคดีอาญา OECD Guidelines และ EU Directives ต่างให้ข้อเสนอแนะว่ารัฐอาจกำหนดเป็นกฎเกณฑ์เฉพาะสำหรับการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาให้มีความยืดหยุ่นกว่าหลักเกณฑ์ทั่วไปได้[9] เพื่อป้องกันไม่ให้การคุ้มครองข้อมูลส่วนบุคคลลดประสิทธิภาพของรัฐในการป้องกันและปราบปรามอาชญากรรม

---

[6] บรรเจิด สิงคะเนติ, หลักความได้สัดส่วน (Principle of Proportionality) ในการตรวจสอบขอบเขตอำนาจรัฐ ตามมาตรา 23 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย (พุทธศักราช 2550), (กรุงเทพฯ: สำนักงานศาลรัฐธรรมนูญ, 2558), หน้า 17-20; ปรียาชาติ หาลำเจียก. การตรวจสอบและถ่วงดุล: ศึกษากรณีการสะกดรอยด้วยเครื่องมือสื่อสารโทรคมนาคมและเครื่องมืออิเล็กทรอนิกส์ตามพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 มาตรา 21. วิทยานิพนธ์ปริญญามหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2557; หน้า 28-29.

[7] United Nations Human Rights Council, “The Right to Privacy in the Digital Age (a/Hrc/39/29),”(2018)

[8] สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์, รายงานผลการดำเนินการ โครงการพัฒนามาตรการในการดำเนินการ การพิจารณาความเหมาะสม ความเป็นไปได้ เพื่อจัดทำแนวทาง ขั้นตอนและวิธีการในการเข้าร่วมหรือทำความตกลงตามกรอบว่าด้วยการคุ้มครองข้อมูลความเป็นส่วนตัวของ Apec (คณะกรรมการข้อมูลข่าวสารของราชการ,ธันวาคม 2557)

[9] “The OECD Privacy Framework 2013”, Paragraph 4: Exceptions to the Guidelines.; “Law Enforcement Directive.” (LED), Recital (11)

4. มาตรการทางกฎหมายและข้อจำกัดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาของประเทศไทย

สำหรับประเทศไทย ประเทศไทยเข้าเป็นภาคีอนุสัญญาสิทธิมนุษยชนตามกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมืองด้วยเช่นกัน ประเทศไทยจึงมีพันธกรณีในการคุ้มครองสิทธิในข้อมูลส่วนบุคคล ในฐานะที่เป็นส่วนหนึ่งของความเป็นอยู่ส่วนตัวตามกติการะหว่างประเทศดังกล่าว ซึ่งปัจจุบัน ประเทศไทยได้มีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นกฎหมายกลางว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลแต่พระราชบัญญัติดังกล่าวกลับมีผลบังคับใช้ในชั้นสืบสวนและสอบสวนคดีอาญาเพียงบางส่วนเท่านั้น จึงทำให้การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาต้องอาศัยมาตรการที่มีอยู่เดิมเป็นหลัก อันได้แก่ (1) กฎหมายวิธีพิจารณาความอาญา คือ ประมวลกฎหมายวิธีพิจารณาความอาญาและกฎหมายอื่นที่เกี่ยวข้องกับวิธีพิจารณาความอาญา และ (2) กฎหมายคุ้มครองข้อมูลส่วนบุคคล คือ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในส่วนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล สรุปเป็นภาพรวมได้ ดังนี้

หลักเกณฑ์ที่เกี่ยวข้อง	กฎหมายวิธีพิจารณาความอาญา	กฎหมายคุ้มครองข้อมูลส่วนบุคคล
ขอบเขตของข้อมูลส่วนบุคคล	ไม่มีนิยามคำว่าข้อมูลส่วนบุคคล เนื่องจากกฎหมายวิธีพิจารณาความอาญาของไทยมิได้มีเจตนารมณ์ในการคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะ แต่ถึงกระนั้น กฎหมายวิธีพิจารณาความอาญาก็เป็นกฎหมายว่าด้วยกฎเกณฑ์และวิธีการค้นหาความจริงเกี่ยวกับการกระทำผิด รวมถึงการนำตัวผู้กระทำผิดมาดำเนินคดีและลงโทษอาญา[10] กฎหมายวิธีพิจารณาความอาญาจึงเป็นกฎหมายที่ให้อำนาจเจ้าหน้าที่รัฐรุกล้ำสิทธิและเสรีภาพของบุคคล แต่ในอีกด้านหนึ่ง หลักเกณฑ์ต่าง ๆ ในกฎหมายวิธีพิจารณาความอาญาก็เป็นกฎเกณฑ์ที่ควบคุมอำนาจรัฐไม่ให้ก้าวล่วงสิทธิและเสรีภาพของบุคคลเกินกว่าขอบเขต[11] ซึ่งรวมไปถึงสิทธิ	มีนิยามแตกต่างกันตามกฎหมายแต่ละฉบับ กล่าวคือ (1) พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 นิยามคำว่า “ข้อมูลข่าวสารส่วนบุคคล” ว่าเป็นข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคลธรรมดา ไม่ว่าจะถึงแก่กรรมหรือไม่ก็ตาม แต่ต้องมีสัญชาติไทยหรือมีถิ่นที่อยู่ในประเทศไทย[12] (2) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นิยามคำว่า “ข้อมูลส่วนบุคคล” ให้หมายถึงข้อมูลที่ระบุถึงตัวบุคคลธรรมดาได้ แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม[13]

[10] ณรงค์ ใจหาญ, **หลักกฎหมายวิธีพิจารณาความอาญา เล่ม 1,** พิมพ์ครั้งที่ 14 (กรุงเทพฯ: วิญญูชน, 2565), หน้า 15-16.

[11] ธานิศ เกศวพิทักษ์, **คำอธิบาย ประมวลกฎหมายวิธีพิจารณาความอาญา เล่ม 1**, พิมพ์ครั้งที่ 16 (กรุงเทพฯ: สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา, 2564), หน้า 317-318.

[12] มาตรา 4 และมาตรา 21 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

[13] มาตรา 6 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

หลักเกณฑ์ที่เกี่ยวข้อง	กฎหมายวิธีพิจารณาความอาญา	กฎหมายคุ้มครองข้อมูลส่วนบุคคล
	ในความเป็นอยู่ส่วนตัวและข้อมูลส่วนบุคคล กฎหมายวิธีพิจารณาความอาญาจึงมีความเชื่อมโยงกับการคุ้มครองข้อมูลส่วนบุคคลในแง่นี้	
การเก็บรวบรวมข้อมูลส่วนบุคคล	มีบทบัญญัติกำหนดกรอบการใช้อำนาจสืบสวนและสอบสวนคดีอาญาสามรูปแบบใหญ่ ได้แก่ (1) เหตุแห่งการใช้อำนาจ โดยระบุสถานการณ์ที่เจ้าหน้าที่รัฐอาจเก็บรวบรวมข้อมูลส่วนบุคคลได้[14] (2) วิธีการใช้อำนาจ โดยระบุขั้นตอนการดำเนินงานรวมถึงข้อจำกัดการเก็บรวบรวมข้อมูลส่วนบุคคล[15] (3) ตรวจสอบถ่วงดุลโดยองค์กรอื่น โดยทั่วไปคือการให้ศาลตรวจสอบก่อนออกหมายหรือคำสั่ง ซึ่งในปัจจุบัน จะมีการค้นในที่รโหฐานและการค้นเอกสารซึ่งส่งทางไปรษณีย์และโทรเลข[16] ตลอดจนการได้มาซึ่งเอกสารหรือข้อมูลข่าวสารที่ส่งผ่านสิ่งติดต่อสื่อสาร[17] ที่อยู่ในบังคับจะต้องได้รับหมายหรือคำสั่งจากศาล	อยู่ภายใต้พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ซึ่งกำหนดให้หน่วยงานของรัฐมีหน้าที่[18] (1) จัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลเพียงเท่าที่เกี่ยวข้องและจำเป็น (2) พิมพ์รายการแสดงรายละเอียดของข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความครอบครองลงในราชกิจจานุเบกษา (3) พยายามเก็บข้อมูลข่าวสารโดยตรง (4) แจ้งรายละเอียดเกี่ยวกับการใช้ข้อมูล

[14] ตัวอย่างเช่น มาตรา 92 ประมวลกฎหมายวิธีพิจารณาความอาญา กำหนดให้การค้นในที่รโหฐานจะกระทำได้ต่อเมื่อมีหมายค้นหรือคำสั่งของศาล เว้นแต่พนักงานฝ่ายปกครองหรือตำรวจเป็นผู้ค้น เมื่อปรากฏเหตุยกเว้นอย่างหนึ่งอย่างใดตามกฎหมาย อาทิ เมื่อมีเสียงร้องให้ช่วยมากจากข้างในที่รโหฐาน หรือเมื่อปรากฏความผิดซึ่งหน้ากำลังกระทำลงในที่รโหฐาน หรือมาตรา 134 วรรคสอง ประมวลกฎหมายวิธีพิจารณาความอาญา กำหนดว่าการแจ้งข้อหาและการสอบสวนผู้ต้องหาจะกระทำได้ต่อเมื่อมีหลักฐานตามสมควรว่าผู้นั้นน่าจะได้กระทำผิดตามข้อกล่าวหา เป็นต้น

[15] ตัวอย่างเช่น ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 131/1 กำหนดว่าการตรวจพิสูจน์ทางวิทยาศาสตร์ ด้วยวิธีการเก็บตรวจส่วนประกอบของร่างกายให้กระทำเท่าที่จำเป็นและสมควร โดยใช้วิธีการที่ไม่เป็นอันตราย และก่อให้เกิดความเจ็บปวดน้อยที่สุดเท่าที่จะกระทำได้ หรือมาตรา 134 - 134/4 กำหนดว่าในการสอบสวนผู้ต้องหา ต้องแจ้งข้อหาประกอบกับข้อเท็จจริงเกี่ยวกับการกระทำผิด รวมถึงแจ้งสิทธิต่าง ๆ ให้ผู้ต้องหาทราบและดำเนินการให้เป็นไปตามสิทธิดังกล่าว ทั้งนี้ ห้ามมิให้ถามคำให้การในลักษณะที่เป็นการให้คำมั่นสัญญา ขู่เข็ญ หลอกลวง ทรมาน ใช้กำลังบังคับ หรือกระทำโดยมิชอบประการใด หรือมาตรา 133 ทวิ และมาตรา 134/2 มีการกำหนดวิธีการสอบสวนสำหรับผู้เสียหาย พยาน หรือผู้ต้องหาที่เป็นเด็กอายุไม่เกินสิบแปดปีเป็นการเฉพาะ เป็นต้น

[16] มาตรา 92 และมาตรา 105 ประมวลกฎหมายวิธีพิจารณาความอาญา

[17] อาทิ มาตรา 19 วรรคหนึ่ง พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กำหนดให้การใช้อำนาจตามมาตรา 18 (4) (5) (6) (7) (8) ของพนักงานเจ้าหน้าที่ต้องยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้ดำเนินการ

[18] มาตรา 23 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

หลักเกณฑ์ที่เกี่ยวข้อง	กฎหมายวิธีพิจารณาความอาญา	กฎหมายคุ้มครองข้อมูลส่วนบุคคล
การใช้และเปิดเผยข้อมูลส่วนบุคคล	มีกฎเกณฑ์เกี่ยวข้องโดยตรงไม่มากนัก โดยมักจะพบในพระราชบัญญัติเฉพาะ[19] หรือระเบียบภายใน[20] มากกว่าในประมวลกฎหมายวิธีพิจารณาความอาญาซึ่งเป็นบทบัญญัติหลัก	อยู่ภายใต้พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ซึ่งห้ามมิให้มีการเปิดเผยข้อมูลข่าวสารส่วนบุคคล เว้นแต่ได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลหรือเข้าข้อยกเว้นตามมาตรา 24 แห่งพระราชบัญญัตินี้[21] อาทิ (1) เปิดเผยในหน่วยงาน เพื่อใช้ตามอำนาจหน้าที่ (2) เป็นการใช้ข้อมูลตามปกติภายในวัตถุประสงค์ (3) เปิดเผยต่อเจ้าหน้าที่รัฐ เพื่อป้องกันการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย หรือเพื่อการสืบสวนสอบสวน หรือฟ้องคดี (4) เป็นการจำเป็นเพื่อป้องกันหรือระงับอันตรายต่อชีวิตหรือสุขภาพของบุคคล (5) เปิดเผยศาล และเจ้าหน้าที่รัฐหรือหน่วยงานของรัฐหรือบุคคลที่มีอำนาจตามกฎหมาย
การเก็บรักษาข้อมูลส่วนบุคคล	ทำนองเดียวกับการใช้และเปิดเผยข้อมูลส่วนบุคคล จะมีกฎเกณฑ์เกี่ยวข้องโดยตรงไม่มากนัก โดยจะพบในพระราชบัญญัติเฉพาะ[22] หรือระเบียบภายใน[23] มากกว่าในประมวลกฎหมายวิธีพิจารณาความอาญาซึ่งเป็นบทบัญญัติหลัก	อยู่ภายใต้พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ซึ่งกำหนดให้หน่วยงานของรัฐมีหน้าที่[24] (1) ตรวจสอบแก้ไขข้อมูลให้ถูกต้องเสมอ (2) จัดระบบรักษาความปลอดภัย (3) ยกเลิกระบบข้อมูล เมื่อหมดความจำเป็น

[19] อาทิ พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 กำหนดว่าการใช้ประโยชน์จากข้อมูลข่าวสารในสิ่งสื่อสารซึ่งได้มาในคดีพิเศษ จะต้องเป็นไปเพื่อการสืบสวนหรือใช้เป็นพยานหลักฐานเฉพาะในการดำเนินคดีพิเศษที่ได้รับอนุญาตตามคำสั่งศาลเท่านั้น (มาตรา 25) และกำหนดให้การเปิดเผยข้อมูลข่าวสารที่ได้มาโดยมิชอบมีความรับผิดทางอาญา (มาตรา 26 ประกอบกับมาตรา 39) เป็นต้น

[20] อาทิ คำสั่งสำนักงานตำรวจแห่งชาติ ที่ 465/2550 (แก้ไขเพิ่มเติม) ลงวันที่ 15 สิงหาคม พ.ศ. 2550 เรื่อง การปฏิบัติเกี่ยวกับการให้ข่าว การแถลงข่าว การให้สัมภาษณ์ การเผยแพร่ภาพต่อสื่อมวลชน และการจัดทำสื่อประชาสัมพันธ์

[21] มาตรา 24 (1), (2), (6), (7), และ (8) พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

[22] อาทิ มาตรา 17 พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 กำหนดให้รักษาเฉพาะข้อมูลข่าวสารเกี่ยวกับการกระทำความผิด ส่วนข้อมูลข่าวสารอื่นให้ทำลายตามข้อบังคับที่อัยการสูงสุดกำหนด

[23] อาทิ คำสั่งสำนักงานตำรวจแห่งชาติที่ 419/2556 ลงวันที่ 1 กรกฎาคม พ.ศ. 2556 เรื่อง การอำนวยความยุติธรรมในคดีอาญา การทำสำนวนสอบสวน และมาตรฐานการควบคุม ตรวจสอบ เร่งรัดการสอบสวนคดีอาญา

[24] มาตรา 23 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

หลักเกณฑ์ที่เกี่ยวข้อง	กฎหมายวิธีพิจารณาความอาญา	กฎหมายคุ้มครองข้อมูลส่วนบุคคล
		นอกจากนี้ การรักษาความมั่นคงปลอดภัยจะอยู่ในบังคับของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อีกส่วนหนึ่ง โดยจะมีหน้าที่[25] (1) จัดมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม และทบทวนมาตรการดังกล่าว (2) แจ้งเหตุการละเมิดข้อมูลส่วนบุคคล
สิทธิของเจ้าของข้อมูลส่วนบุคคล	ไม่มีบทบัญญัติรับรองสิทธิของเจ้าของข้อมูลโดยตรง จะมีเพียงการรับรองสิทธิในกระบวนการยุติธรรม อย่างไรก็ดี สิทธิในกระบวนการยุติธรรมก็อาจมีความเกี่ยวพันกับการคุ้มครองข้อมูลส่วนบุคคลได้ ในบางบริบท อาทิ สิทธิของจำเลยในการตรวจดูคัดสำเนา หรือถ่ายรูปสิ่งที่ยื่นเป็นพยานหลักฐาน[26] ซึ่งมีความคล้ายคลึงกับสิทธิในการเข้าถึงข้อมูลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล เนื่องจากเป็นการอนุญาตให้จำเลยสามารถเข้าถึงและรับสำเนาข้อมูลอันเกี่ยวตนในฐานะเจ้าของข้อมูลได้ เพียงแต่มีข้อสังเกตว่าเจตนารมณ์ของกฎหมายวิธีพิจารณาความอาญาจะมุ่งเน้นการประกันสิทธิในการต่อสู้คดีของจำเลยเป็นหลัก จึงมิได้มีเจตนารมณ์เช่นเดียวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล	ได้รับการรับรองสิทธิของเจ้าของข้อมูลข่าวสารส่วนบุคคลตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 อยู่สองประการ อันได้แก่[27] (1) สิทธิที่จะรู้ข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับตน (2) สิทธิแก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับตน ในส่วนที่ไม่ถูกต้อง
สภาพบังคับและบทกำหนดโทษ	ในแง่ของการพิจารณาคดี ข้อมูลข่าวสารที่ได้มาโดยไม่ชอบ ไม่อาจรับฟังเป็นพยานหลักฐานได้ เว้นแต่ศาลเลือกที่จะใช้ดุลพินิจรับฟัง[28] ส่วนในแง่ความรับผิดและบทกำหนดโทษ จะมีเพียงพระราชบัญญัติเฉพาะที่กำหนดความรับผิด	ในกรณีที่มีการฝ่าฝืนหมวด 3 ของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 จะไม่มีบทกำหนดความรับผิดไว้โดยเฉพาะ แต่จะใช้ระบบการตรวจสอบด้วยการอุทธรณ์ต่อคณะกรรมการ[29]

[25] มาตรา 37 (1) และ (4) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[26] มาตรา 7 ประมวลกฎหมายวิธีพิจารณาความอาญา

[27] มาตรา 25 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

[28] มาตรา 226/1 ประมวลกฎหมายวิธีพิจารณาความอาญา

[29] วิริยะ รามสมภพ, “ความสัมพันธ์เชิงวิเคราะห์ของร่างพระราชบัญญัติคุ้มครองข้อมูลข่าวสารส่วนบุคคล พ.ศ. ... กับพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540,”(สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ, 2562).

หลักเกณฑ์ที่เกี่ยวข้อง	กฎหมายวิธีพิจารณาความอาญา	กฎหมายคุ้มครองข้อมูลส่วนบุคคล
	สำหรับการเปิดเผยข้อมูลโดยไม่ชอบ ความรับผิดกรณีอื่น ๆ จึงต้องอาศัยบททั่วไปแทน เช่น ความผิดตามมาตรา 157 ประมวลกฎหมายอาญา ฐานเจ้าพนักงานปฏิบัติหรือละเว้นการปฏิบัติหน้าที่โดยมิชอบ ทั้งนี้ ในกรณีที่เกิดความเสียหาย ผู้เสียหายก็มีสิทธิที่จะนำคดีไปฟ้องร้องทางแพ่งเพื่อให้มีการเยียวยาความเสียหายต่อไป	แต่หากการฝ่าฝืนหน้าที่ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นอกเหนือจากการร้องเรียนต่อคณะกรรมการเพื่อให้คณะกรรมการมีคำสั่งให้ปฏิบัติหรือห้ามกระทำการที่ทำให้เจ้าของข้อมูลส่วนบุคคลเสียหาย ผู้ที่ฝ่าฝืนยังอาจมีความรับผิดทางแพ่งและทางปกครองได้อีกด้วย[30]

อย่างไรก็ดี จากการศึกษาพบว่ามาตรการทางกฎหมายที่มีอยู่มีข้อจำกัดบางประการ อันเป็นช่องว่างในการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา กล่าวคือ

4.1 ข้อจำกัดของกฎหมายวิธีพิจารณาความอาญา

ข้อจำกัดที่หนึ่ง กฎหมายวิธีพิจารณาความอาญาของไทยมีบทบัญญัติเปิดช่องให้เจ้าหน้าที่รัฐมีอำนาจในการเก็บรวบรวมข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนอย่างกว้างขวาง โดยมีข้อสังเกตดังนี้

(1) การค้นที่ผ่านกระบวนการตรวจสอบจากศาลในประมวลกฎหมายวิธีพิจารณาความอาญามีขอบเขตจำกัดเฉพาะการค้นภายในที่รโหฐาน และการค้นเอกสารซึ่งส่งทางไปรษณีย์และโทรเลข ทำให้การแสวงหาพยานหลักฐานในชั้นสืบสวนและสอบสวนคดีอาญาโดยส่วนใหญ่เป็นอำนาจดุลพินิจของพนักงานสืบสวนและสอบสวนเป็นหลัก อาทิ มาตรา 131 ประมวลกฎหมายวิธีพิจารณาความอาญาบัญญัติให้พนักงานสอบสวนรวบรวมหลักฐานทุกชนิดเท่าที่จะทำได้ โดยไม่มีข้อจำกัดอำนาจที่ชัดเจน[31]

(2) การได้มาซึ่งข้อมูลข่าวสารตามพระราชบัญญัติเฉพาะมีขอบเขตการใช้อำนาจอย่างกว้าง เนื่องจากบทบัญญัติขาดความเฉพาะเจาะจง คือไม่ระบุสถานการณ์หรือเหตุปัจจัยที่ชัดเจน แต่จะใช้ถ้อยคำกว้าง ๆ ว่าเพื่อให้ได้มาซึ่งข้อมูลข่าวสาร[32] อันเป็นการเปิดช่องให้เกิดการเข้าถึงข้อมูลส่วนบุคคลโดยไม่จำกัดวิธีการ โดยเฉพาะพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งไม่เพียงแต่ไม่มีการระบุมาตรการที่เฉพาะเจาะจง แต่ยังขยายขอบเขตไปถึงความผิดอื่นที่มีคอมพิวเตอร์

[30] มาตรา 73 และมาตรา 74 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[31] พิสิฏฐ์ สีกากี, “ปัญหาและอุปสรรคการใช้อำนาจดุลพินิจของพนักงานสอบสวนในการรวบรวมพยานหลักฐาน,” **วารสารมนุษยศาสตร์และสังคมศาสตร์ มหาวิทยาลัยราชภัฏสุรินทร์** 20, 1 (2018).

[32] โปรดดู มาตรา 25 พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 และ มาตรา 30 พระราชบัญญัติป้องกันและปราบปรามการค้ามนุษย์ พ.ศ. 2551

เกี่ยวข้อง[33] ทั้งที่การกระทำความผิดปัจจุบันมักเกี่ยวข้องกับคอมพิวเตอร์โดยสภาพ จึงเป็นการกำหนดที่กว้างขวางเกินไป[34]

(3) การขอข้อมูลข่าวสารจากภาคเอกชนในทางปฏิบัติ มักกระทำในรูปแบบหมายเรียกพยานเอกสารหรือหนังสือขอความร่วมมือ เพราะถือเป็นอำนาจสอบสวนทั่วไปตามมาตรา 132 (3) ประมวลกฎหมายวิธีพิจารณาความอาญา[35] ซึ่งไม่มีข้อจำกัดอำนาจ และไม่อยู่ในบังคับที่จะต้องผ่านกระบวนการตรวจสอบจากศาล

ข้อจำกัดที่สอง กฎหมายวิธีพิจารณาความอาญาของไทยไม่ได้ถูกออกแบบให้สอดคล้องกับธรรมชาติของความเป็นส่วนตัวในข้อมูลหรือแนวคิดว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล เนื่องจากกฎหมายวิธีพิจารณาความอาญาเป็นกฎหมายที่ว่าด้วยหลักเกณฑ์และวิธีการค้นหาความจริงเกี่ยวกับการกระทำผิด รวมถึงการนำตัวผู้กระทำผิดมาดำเนินคดีและลงโทษ[36] จึงมิได้มุ่งคุ้มครองเฉพาะข้อมูลส่วนบุคคล เป็นเหตุให้กฎหมายวิธีพิจารณาความอาญาไม่ได้มีการบัญญัติมาตรการที่จำเป็นในการคุ้มครองข้อมูลส่วนบุคคลได้อย่างเพียงพอ อันได้แก่

(1) กฎหมายวิธีพิจารณาความอาญาไม่มีกฎเกณฑ์ครอบคลุมรูปแบบการดำเนินการต่อข้อมูลครบถ้วนทุกลักษณะ เนื่องจากกฎหมายวิธีพิจารณาความอาญามุ่งเน้นการควบคุมการแสวงหาข้อเท็จจริงและรวบรวมพยานหลักฐาน ซึ่งหากพิจารณาในแง่พฤติกรรมต่อข้อมูล จะเป็นในขั้นตอนการเก็บรวบรวมเป็นสำคัญ ในขณะที่การใช้ เปิดเผย และเก็บรักษานั้นจะมีกฎเกณฑ์ที่เกี่ยวข้องโดยตรงไม่มากนัก

(2) กฎหมายวิธีพิจารณาความอาญามิได้มีบทบัญญัติรับรองสิทธิเจ้าของข้อมูลส่วนบุคคล

(3) กฎหมายวิธีพิจารณาความอาญาไม่มีสภาพบังคับและบทกำหนดโทษที่เหมาะสม เนื่องจากสภาพบังคับหลักของกฎหมายวิธีพิจารณาความอาญาเป็นเรื่องของการไม่รับฟังหรือไม่ให้น้ำหนักกับพยานหลักฐานที่ได้มาโดยไม่ชอบด้วยกฎหมาย แตกต่างจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่สภาพบังคับอาจอยู่ในรูปแบบการออกคำสั่งให้มีการปฏิบัติ แก้ไข หรือระงับการการดำเนินการใด ๆ เพื่อให้เป็นไปตามมาตรฐานขั้นต่ำที่กฎหมายกำหนด โดยไม่จำต้องรอให้มีความเสียหายเกิดขึ้น[37] อันเป็นมาตรการเชิงป้องกัน

---

[33] มาตรา 18 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

[34] อนุสิษฐ คุณากร และคณะ, **การคุ้มครองข้อมูลส่วนบุคคลกับสังคมไทย,** (กรุงเทพฯ: สถาบันนโยบายการศึกษา ภายใต้มูลนิธิส่งเสริมนโยบายการศึกษา, 2563), หน้า 51.

[35] เรื่องเสร็จที่ 343/2549 บันทึกสำนักงานคณะกรรมการกฤษฎีกา เรื่อง อำนาจของเจ้าพนักงานตำรวจในการปิดกั้นเว็บไซต์ที่ไม่เหมาะสมทางอินเตอร์เน็ต และของพนักงานสอบสวนตามมาตรา 132 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา.

[36] ณรงค์ ใจหาญ, **หลักกฎหมายวิธีพิจารณาความอาญา เล่ม 1**, หน้า 15-16.

[37] คณาธิป ทองรวีวงศ์, **คำอธิบาย หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล,** หน้า 522-525.

อีกทั้ง กฎหมายวิธีพิจารณาความอาญาไม่มีบทกำหนดความรับผิดและโทษเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลอย่างครอบคลุม โดยในปัจจุบัน จะมีเพียงโทษฐานเปิดเผยข้อมูลข่าวสารโดยไม่ชอบเท่านั้น แต่ไม่มีพระราชบัญญัติใดเลยที่กำหนดโทษฐานนำข้อมูลไปใช้ประโยชน์อื่น นอกเหนือจากการปฏิบัติหน้าที่[38] และหากพิจารณาด้านการเยียวยาความเสียหาย แม้ผู้เสียหายจะมีสิทธิเรียกร้องค่าเสียหายทางแพ่ง แต่ก็ต้องตกเป็นผู้มีภาระพิสูจน์ตามหลักทั่วไป[39] ที่ว่าฝ่ายใดกล่าวอ้าง ฝ่ายนั้นมีหน้าที่นำสืบ ภาระการพิสูจน์จึงตกแก่ผู้เสียหาย ซึ่งเป็นการยากที่ผู้เสียหายจะต่อสู้คดี

4.2 ข้อจำกัดของกฎหมายคุ้มครองข้อมูลส่วนบุคคล

โดยที่หมวด 3 ว่าด้วยข้อมูลข่าวสารส่วนบุคคล พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ได้รับการยกร่างขึ้นตั้งแต่ปี พ.ศ. 2540 และมีบทบัญญัติอยู่เพียง 5 มาตรา กฎเกณฑ์ในพระราชบัญญัติดังกล่าวจึงอาจมีข้อจำกัดในการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยมีข้อสังเกตดังนี้

(1) ขอบเขตข้อมูลข่าวสารส่วนบุคคลตามหมวด 3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 แตกต่างจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ทำให้การบังคับใช้กฎหมายกับหน่วยงานของรัฐที่อยู่ภายใต้กฎหมายทั้งสองฉบับมีความลักลั่น[40]

(2) โดยส่วนใหญ่ เกณฑ์การเก็บรวบรวม ใช้ เปิดเผย และเก็บรักษาข้อมูลข่าวสารส่วนบุคคลตามหมวด 3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 จะเป็นเพียงหลักการกว้าง ๆ จึงขาดรายละเอียดปฏิบัติที่ชัดเจน เมื่อเปรียบเทียบกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562[41]

(3) หมวด 3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มีการรับรองสิทธิเจ้าของข้อมูลข่าวสารส่วนบุคคลอยู่เพียงสองประการ ได้แก่ สิทธิที่จะรู้ข้อมูลอันเกี่ยวกับตนและสิทธิที่จะแก้ไขหรือลบข้อมูลที่ไม่ถูกต้อง นอกจากนี้ ในการปฏิเสธไม่ดำเนินการตามคำขอ ก็ไม่ได้มีการบัญญัติเหตุแห่งการปฏิเสธไว้ชัดเจน การปฏิเสธสิทธิจึงขึ้นอยู่กับดุลพินิจของหน่วยงานของรัฐเป็นรายกรณีไป

(4) แม้ว่าหมวด 3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 จะมีระบบอุทธรณ์ต่อคณะกรรมการ แต่คณะกรรมการดังกล่าวมีเพียงอำนาจในการเรียกบุคคลมาให้ถ้อยคำส่งวัตถุ เอกสาร

---

[38] มติชนออนไลน์, “เปิดร่างป.วิอาญา’ดักฟัง’ อัยการเทียบเนื้อหาพ.ร.บ. 7 ฉบับ ชี้ข้อมูลลักลั่น” [ออนไลน์] แหล่งที่มา: https://www.matichon.co.th/local/crime/news_552146 [20 กุมภาพันธ์ 2565]

[39] จันทจิรา เอี่ยมมยุรา, “การคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย”, **วารสารนิติศาสตร์มหาวิทยาลัยธรรมศาสตร์** 34, 4 (ธันวาคม 2547), หน้า 627-652.

[40] ตัวอย่างเช่น บุคคลที่ไม่มีสัญชาติไทยหรือไม่มีถิ่นที่อยู่ในประเทศไทยจะไม่ได้รับความคุ้มครองตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 แต่จะได้รับความคุ้มครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในขณะที่ผู้ถึงแก่กรรมจะไม่ได้รับความคุ้มครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แต่ได้รับความคุ้มครองตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 แทน

[41] บุญชู ณ ป้อมเพชร, **“คำอธิบายกฎหมายข้อมูลข่าวสารของราชการ”,** (PUB HTML5), หน้า 261-263.

หรือพยานหลักฐานประกอบการพิจารณา โดยที่ไม่มีอำนาจสืบสวนและสอบสวน (Investigation power) แต่อย่างใด[42] ประกอบกับพระราชบัญญัติดังกล่าวไม่มีบทกำหนดความรับผิดและโทษสำหรับการฝ่าฝืนบทบัญญัติในหมวด 3 การดำเนินการที่ผ่านมาจึงเป็นการฟ้องร้องทางแพ่งและอาญา[43] เป็นเหตุให้การบังคับใช้พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ในส่วนที่เกี่ยวข้องกับการคุ้มครองข้อมูลข่าวสารส่วนบุคคลไม่ประสบผลสำเร็จเท่าที่ควร

เมื่อการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยยังคงมีข้อจำกัด ในการเสนอแนะแนวทางแก้ไขปัญหา จึงสมควรศึกษาแนวทางตามกฎหมายระหว่างประเทศและกฎหมายต่างประเทศที่มีพัฒนาการด้านการคุ้มครองข้อมูลส่วนบุคคลก้าวหน้ากว่าประเทศไทย โดยในส่วนกฎหมายระหว่างประเทศ (หัวข้อที่ 5) จะเป็นการศึกษากฎหมายของสหภาพยุโรป ซึ่งเป็นต้นแบบในการร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ทั้งยังมีอิทธิพลต่อกฎหมายคุ้มครองข้อมูลส่วนบุคคลในหลายประเทศ และในส่วนกฎหมายต่างประเทศ (หัวข้อที่ 6)จะมีบทบัญญัติเป็นกรณีศึกษาอยู่สามประเทศ อันได้แก่ สหราชอาณาจักร สหรัฐอเมริกา และสาธารณรัฐเกาหลี (เกาหลีใต้) เพื่อให้เห็นถึงความหลากหลายของแนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาของแต่ละประเทศที่มีบริบทแตกต่างกันออกไป

5. แนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาของสหภาพยุโรป

หากพิเคราะห์ขอบเขตในทางเนื้อหาของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป กล่าวคือ GDPR (General Data Protection Regulation) จะพบว่ามีข้อยกเว้นไม่ให้นำข้อกำหนดนี้ไปบังคับใช้แก่การประมวลผลข้อมูลที่ดำเนินการโดยหน่วยงานที่มีอำนาจหน้าที่ เพื่อวัตถุประสงค์ในการป้องกัน สืบสวน ตรวจจับ ดำเนินคดี ลงโทษอาญา รวมถึงป้องกันความมั่นคงปลอดภัยของสาธารณะ[44] ด้วยเหตุนี้ การสืบสวนและสอบสวนคดีอาญาจึงไม่ตกอยู่ภายใต้ GDPR ในทำนองเดียวกันกับที่กฎหมายไทยกำหนด

อย่างไรก็ตาม การยกเว้นตาม GDPR นี้ไม่ใช่การยกเว้นโดยเด็ดขาด แต่เป็นการยกเว้นเพื่อให้กิจการที่เกี่ยวข้องกับการป้องกัน สืบสวน ตรวจจับ ดำเนินคดี ลงโทษอาญา และความมั่นคงปลอดภัยของสาธารณะอยู่ภายใต้มาตรการทางกฎหมายที่มีความเฉพาะเจาะจงมากยิ่งขึ้น ได้แก่ (1) เกณฑ์

---

[42] นคร เสรีรักษ์, ความเป็นส่วนตัว: ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย, พิมพ์ครั้งที่ 2 (แพร่: พี.เพรส, 2563), หน้า 254.

[43] เรื่องเดียวกัน

[44] Article 2 General Data Protection Regulation.” (GDPR)

ตรวจสอบความสอดคล้องกับหลักสิทธิมนุษยชน ซึ่งใช้ในการประเมินความชอบด้วยกฎหมายของบทบัญญัติที่มีผลกระทบต่อสิทธิส่วนบุคคล (หัวข้อที่ 5.1) และ Directive (EU) 2016/680 หรือ LED (Law Enforcement Directive) ซึ่งวางกฎระเบียบคุ้มครองข้อมูลส่วนบุคคลในการดำเนินการที่มีวัตถุประสงค์เพื่อบังคับใช้กฎหมายอาญา (Law enforcement) เป็นการเฉพาะ[45] (หัวข้อที่ 5.2) โดยมีสาระสำคัญดังนี้

5.1 เกณฑ์การตรวจสอบความสอดคล้องกับหลักสิทธิมนุษยชน

แม้ว่าอนุสัญญายุโรปว่าด้วยสิทธิมนุษยชน (European Convention on Human Rights: "ECHR") จะวางหลักไว้ว่าสิทธิความเป็นส่วนตัวของบุคคลนั้นอาจถูกจำกัดได้โดยกฎหมาย[46] แต่กฎหมายดังกล่าวก็จำต้องอยู่ภายใต้หลักสิทธิมนุษยชน ที่เรียกว่า "หลักเกณฑ์ปกป้องสิทธิ" (Safeguard principle) ซึ่งเป็นมาตรการหรือกลไกในการป้องกันมิให้เจ้าหน้าที่รัฐใช้อำนาจโดยอำเภอใจ ดังจะเห็นได้จากการที่ LED รับรองให้การคุ้มครองบุคคลธรรมดาที่เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลเป็นสิทธิขั้นพื้นฐานตามข้อ 8 (1) กฎบัตรว่าด้วยสิทธิขั้นพื้นฐานของสหภาพยุโรป (The Charter of Fundamental Rights of the European Union) และตามข้อ 16 (1) ของสนธิสัญญาว่าด้วยการทำหน้าที่ของสหภาพยุโรป (The Treaty on the Functioning of the European Union: "TFEU")[47] พร้อมกำหนดให้การจำกัดสิทธิใด ๆ ของเจ้าของข้อมูลจะต้องสอดคล้องกับหลักการในกฎบัตรว่าด้วยสิทธิขั้นพื้นฐานของสหภาพยุโรป และ ECHR ตามที่ศาลยุติธรรมหรือศาลสิทธิมนุษยชนตีความ[48] โดยมีตัวอย่างหลักเกณฑ์สำคัญ ๆ ดังนี้[49]

(ก.) หลักความเฉพาะเจาะจง กฎหมายควรมีขอบเขตที่ชัดเจนและไม่กว้างขวางจนเกินไป ทั้งในแง่ของเหตุแห่งการใช้อำนาจ มาตรการที่ใช้ กลุ่มเป้าหมาย และระยะเวลา หรืออีกนัยหนึ่งคือควรระบุเงื่อนไขและสถานการณ์ที่จะมีการใช้อำนาจอย่างชัดเจนเพียงพอให้ประชาชนคาดหมายได้ (Foreseeability)

(ข.) หลักการตรวจสอบถ่วงดุล กฎหมายควรอยู่ภายใต้การตรวจสอบขององค์กรอิสระที่แยกต่างหากจากองค์กรบังคับใช้กฎหมายนั้น เช่น การกำหนดให้มีการขอหมายศาลก่อนการเข้าถึงข้อมูล

(ค.) หลักความจำเป็นและได้สัดส่วน กฎหมายควรชั่งน้ำหนักระหว่างความจำเป็นกับประโยชน์สำคัญที่กฎหมายมุ่งคุ้มครองให้เป็นไปโดยได้สัดส่วนกัน

---

[45] Ibid., Recital (19)

[46] Article 8 The European Convention on Human Rights." (ECHR)

[47] Recital (1) Law Enforcement Directive

[48] Ibid., Recital (46)

[49] คณาธิป ทองรวีวงศ์, "การปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน,"(2560); คณาธิป ทองรวีวงศ์, "สิทธิในข้อมูลส่วนบุคคลที่ไม่ได้รับการคุ้มครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 : การเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามกฎหมายเกี่ยวกับความมั่นคงของรัฐ", **วารสารกฎหมายสิทธิมนุษยชน** 1, 1 (มกราคม - เมษายน 2563): 49-58; อนุสิษฐ คุณากร และคณะ, **การคุ้มครองข้อมูลส่วนบุคคลกับสังคมไทย**, หน้า 49-58.

ดังนั้น แม้สหภาพยุโรปจะมิได้ขัดขวางการมีกฎหมายให้อำนาจเจ้าพนักงานสืบสวนสอบสวนในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล แต่พลเมืองยุโรปก็มีสิทธินำคดีให้ศาลสิทธิมนุษยชนยุโรปพิจารณาว่ากฎหมายที่ให้อำนาจสืบสวนและสอบสวนคดีอาญาดังกล่าวขัดแย้งกับสิทธิในข้อมูลส่วนบุคคลตาม ECHR หรือไม่ ประการใด เกณฑ์การตรวจสอบความสอดคล้องกับหลักสิทธิมนุษยชนของสหภาพยุโรปจึงเป็นกลไกสำคัญที่ทำให้รัฐไม่อาจอ้างการรักษาความมั่นคงปลอดภัยหรือการรักษาความสงบเรียบร้อย เพื่อตรากฎหมายแทรกแซงข้อมูลส่วนบุคคลของประชาชนอย่างกว้างขวางได้[50]

นอกจากนี้ หลักเกณฑ์ดังกล่าวยังมีความเชื่อมโยงกับการประเมินระดับการคุ้มครองข้อมูลส่วนบุคคลของประเทศอื่น นอกเหนือจากรัฐสมาชิกสหภาพยุโรปอีกด้วย กล่าวคือ หากประเทศใดมีกฎหมายที่ให้อำนาจรัฐขัดแย้งกับหลักสิทธิมนุษยชน ประเทศที่สามนั้นก็อาจถูกพิจารณาได้ว่ามีระดับการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอ เพราะการประเมินระดับการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปเป็นการประเมินจากปัจจัยแวดล้อมทั้งหมดของการโอนข้อมูลส่วนบุคคล[51] ซึ่งศาลยุติธรรมแห่งยุโรป (European court of justice) ได้ตีความบนพื้นฐานของ ECHR เอาไว้ว่ากฎหมายดังกล่าวจะต้องผ่านการทดสอบระดับ “ความเทียบเท่าที่จำเป็น” (Essential equivalence) ซึ่งประกอบด้วย[52]

(1) การให้อำนาจรัฐแทรกแซงข้อมูลส่วนบุคคลจะต้องได้รับการบัญญัติในกฎหมายโดยชัดแจ้ง และกฎหมายดังกล่าวต้องมีการกำหนดขอบเขตการใช้อำนาจที่ชัดเจน

(2) การแทรกแซงข้อมูลส่วนบุคคลต้องกระทำเท่าที่จำเป็นในสังคมประชาธิปไตย เพื่อบรรลุวัตถุประสงค์ด้านประโยชน์สาธารณะเทียบเท่ากับที่รับรองใน ECHR และเพื่อควบคุมการใช้อำนาจกฎหมายซึ่งให้อำนาจรัฐแทรกแซงข้อมูลส่วนบุคคลจะต้องมีกฎเกณฑ์ที่ชัดเจน โดยระบุว่าการใช้อำนาจดังกล่าวจะกระทำได้ในสถานการณ์ใด ด้วยเงื่อนไขอย่างไร พร้อมมีมาตรการเชิงป้องกันรองรับให้เป็นตามหลักความได้สัดส่วน

(3) กฎหมายต้องมีผลผูกพันระบบกฎหมายภายใน และมีผลบังคับใช้ โดยไม่จำต้องรอให้ศาลวินิจฉัยถึงความไม่ชอบด้วยกฎหมาย อีกทั้ง ควรรับรองให้เจ้าของข้อมูลมีสิทธิที่จะเข้าถึง แก้ไข ลบข้อมูลเกี่ยวกับตน ตลอดจนมีสิทธิที่จะดำเนินคดีทางศาล

อนึ่ง แม้กฎหมายวิธีพิจารณาความอาญาจะมีความเกี่ยวพันโดยอ้อมกับการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาในฐานะที่เป็นกรอบการใช้อำนาจสืบสวนและสอบสวน

---

[50] เรื่องเดียวกัน

[51] คณาธิป ทองรวีวงศ์, “การปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน.”

[52] European Commission, “Commission Implementing Decision of 28.6.2021 Pursuant to Regulation (Eu) 2016/679 of the European Parliament and of the Council on the Adequate Protection of Personal Data by the United Kingdom.”

แต่โดยที่กฎหมายวิธีพิจารณาความอาญาไม่ใช่กฎหมายที่มีเจตนารมณ์เพื่อคุ้มครองข้อมูลส่วนบุคคลเป็นการเฉพาะ ดังนั้น กฎหมายวิธีพิจารณาความอาญาโดยทั่วไปจึงมีข้อจำกัดโดยสภาพในการให้ความคุ้มครองข้อมูลส่วนบุคคล เนื่องจากมิได้มีมาตรการที่ออกแบบมาให้สอดคล้องกับลักษณะธรรมชาติของข้อมูลส่วนบุคคลอย่างเพียงพอ จึงจำเป็นที่การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาต้องอาศัยการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลควบคู่ไปกับกฎหมายวิธีพิจารณาความอาญาเพิ่มเติม ซึ่งจะได้กล่าวในหัวข้อถัดไป

5.2 กฎหมายคุ้มครองข้อมูลส่วนบุคคล (LED)

ในการปฏิรูประบบกฎหมายคุ้มครองข้อมูลส่วนบุคคล สหภาพยุโรปได้ออกคำสั่ง LED ซึ่งวางกฎเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลสำหรับการบังคับใช้กฎหมาย (Law enforcement) ไว้เป็นการเฉพาะ บังคับใช้คู่ขนานกันไปกับ GDPR ที่เป็นกฎเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลทั่วไป โดย LED จะมีขอบเขตการบังคับใช้แก่การประมวลผลข้อมูลที่มีวัตถุประสงค์เพื่อการป้องกัน สืบสวน ตรวจสอบ ดำเนินคดี ลงโทษอาญา หรือรักษาความมั่นคงปลอดภัยสาธารณะ ซึ่งดำเนินการโดยหน่วยงานผู้มีอำนาจหน้าที่นั้น[53] อย่างไรก็ดี LED ไม่ได้ขยายขอบเขตการบังคับใช้ในเชิงพื้นที่ครอบคลุมไปถึงนอกสหภาพยุโรป เนื่องจากการสืบสวนและสอบสวนคดีอาญามีความสัมพันธ์กับอำนาจอธิปไตยของแต่ละรัฐโดยเฉพาะ

ทั้งนี้ โครงสร้างและเนื้อหาของ LED นั้นจะมีความคล้ายคลึงกับ GDPR เนื่องจากสหภาพยุโรปต้องการให้หลักเกณฑ์ของกฎหมายทั้งสองฉบับมีมาตรฐานที่สอดคล้องกันให้มากที่สุด และให้มีกฎเกณฑ์เฉพาะในกรณีที่มีความจำเป็น เพื่อให้สอดคล้องกับลักษณะของการบังคับใช้กฎหมายเท่านั้น โดยมีสาระสำคัญดังนี้

(ก.) ขอบเขตของข้อมูลส่วนบุคคลที่ได้รับความคุ้มครอง LED มุ่งคุ้มครองข้อมูลส่วนบุคคล (Personal data) หรือข้อมูลใด ๆ เกี่ยวกับบุคคล ที่ระบุหรือทำให้ระบุถึงบุคคลธรรมดาผู้เป็นเจ้าของข้อมูลได้ (Data subject) ไม่ว่าโดยตรงหรือโดยอ้อมก็ตาม[54] ซึ่งเป็นนิยามเดียวกับ GDPR

(ข.) หลักการประมวลผลข้อมูลส่วนบุคคล LED มุ่งเน้นการควบคุมกำกับ “การประมวลผล” หรือการดำเนินการใด ๆ ต่อข้อมูลส่วนบุคคล[55] โดยมีหลักการพื้นฐาน 7 ประการสำคัญ[56] ได้แก่

(1) *หลักความชอบด้วยกฎหมายและเป็นธรรม (Lawfulness and Fairness)* กำหนดให้การประมวลผลข้อมูลส่วนบุคคลต้องมีฐานทางกฎหมาย คือมีบทบัญญัติกฎหมายให้อำนาจและเป็น

---

[53] Article 2 (1) Law Enforcement Directive.” (LED)

[54] Ibid., Article 3 (1)

[55] Ibid., Article 3 (2)

[56] Ibid., Article 4 (1)

การดำเนินการที่จำเป็นในการบังคับใช้กฎหมายอาญา[57] อีกทั้ง หากข้อมูลส่วนบุคคลดังกล่าวเป็นข้อมูลอ่อนไหว การประมวลผลจะกระทำได้เฉพาะกรณีที่มีความจำเป็นอย่างยิ่ง โดยจัดให้มีการคุ้มครองสิทธิและเสรีภาพอย่างเหมาะสม[58]

(2) *หลักการจำกัดวัตถุประสงค์ (Purpose Limitation)* กำหนดให้การประมวลผลข้อมูลส่วนบุคคลต้องมีวัตถุประสงค์ที่ชัดแจ้งเฉพาะเจาะจง โดยห้ามมิให้ประมวลผลข้อมูลไม่สอดคล้องกับวัตถุประสงค์ที่กำหนดไว้[59] เว้นแต่การใช้ข้อมูลดังกล่าวมีอยู่ในความคาดการณ์ของกฎหมาย (Subsequent processing)[60]

(3) *หลักการใช้ข้อมูลให้น้อยที่สุด (Data Minimisation)* กำหนดให้การประมวลผลข้อมูลส่วนบุคคลต้องจำกัดให้น้อยที่สุดเท่าที่เพียงพอ จำเป็น และเกี่ยวข้องสัมพันธ์กับการกระทำความผิดที่สืบสวนและสอบสวน[61]

(4) *หลักความถูกต้องสมบูรณ์ (Accuracy)* กำหนดให้ข้อมูลส่วนบุคคลจะต้องถูกรักษาให้ถูกต้อง สมบูรณ์ เป็นปัจจุบัน โดยคำนึงถึงธรรมชาติและบริบทการบังคับใช้กฎหมาย เช่น ความถูกต้องของข้อมูลจากการสอบปากคำพยานอาจเป็นข้อเท็จจริงที่ว่าพยานระบุถึงข้อมูลดังกล่าวเท่านั้น[62] นอกจากนี้ LED ได้กำหนดหน้าที่พิเศษในการแยกแยะประเภทข้อมูลส่วนบุคคล (Categorization of Individuals) โดยให้แยกแยะเจ้าของข้อมูลว่าเป็นผู้ต้องหา ผู้เสียหาย พยาน หรือบุคคลอื่นใด และให้แยกแยะคุณภาพของข้อมูลระหว่างข้อเท็จจริงกับข้อคิดเห็น ซึ่งจะเป็นประโยชน์สำหรับการประเมินความน่าเชื่อถือในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานหรือระหว่างรัฐด้วยกัน[63]

(5) *หลักการจำกัดการเก็บรักษา (Storage Limitation)* กำหนดให้ข้อมูลส่วนบุคคลต้องถูกเก็บรักษาในรูปแบบที่ระบุตัวตนของเจ้าของข้อมูลได้ไม่นานเกินกว่าที่จำเป็นเพื่อบรรลุวัตถุประสงค์ในการบังคับใช้กฎหมายอาญา[64]

(6) *หลักความสมบูรณ์และเป็นความลับ (Integrity and Confidentiality)* กำหนดให้การประมวลผลข้อมูลส่วนบุคคลจะต้องมีมาตรการที่ประกันความมั่นคงปลอดภัย[65] และหากการ

---

[57] Ibid., Article 8

[58] Ibid., Article 10

[59] Ibid., Article 4 (1) (b) and Recital 29

[60] Council of Europe, “Practical Guide on the Use of Personal Data in the Police Sector.”

[61] Article (1) (c) Law Enforcement Directive.” (LED)

[62] Ibid., Article 4 (1) (d) and Recital (30)

[63] Ibid., Article 6-7 and Recital (31)

[64] Ibid., Article 4-5

[65] Ibid., Article 29

ประมวลผลข้อมูลมีแนวโน้มที่จะก่อให้เกิดความเสี่ยงสูงต่อสิทธิและเสรีภาพ อย่างการใช้เทคโนโลยีสมัยใหม่ที่ซับซ้อน ก็จะต้องมีการประเมินความเสี่ยงผลกระทบ (Data protection impact assessment: "DPIA") เพื่อจะจัดการกับความเสี่ยงนั้น โดยปรึกษาหารือกับหน่วยงานกำกับดูแลก่อนการประมวลผล (Prior consultation of the supervisory authority)[66] ในขณะที่เมื่อเกิดเหตุข้อมูลรั่วไหล ก็ให้แจ้งเหตุต่อหน่วยงานกำกับดูแลภายใน 72 วัน นับตั้งแต่ทราบเหตุ รวมถึงให้แจ้งต่อเจ้าของข้อมูล เมื่อการรั่วไหลของข้อมูลมีความเสี่ยงสูงที่จะกระทบต่อสิทธิและเสรีภาพ[67]

(7) *หลักความรับผิดชอบ (Accountability)* ผู้ควบคุมข้อมูลส่วนบุคคลมีความรับผิดชอบในการปฏิบัติตามหลักการข้างต้น โดยผู้ควบคุมข้อมูลส่วนบุคคล (Data controller) หมายถึงหน่วยงานผู้มีอำนาจรับผิดชอบ ซึ่งมีอำนาจตัดสินใจเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล โดยกำหนดวัตถุประสงค์และวิธีการประมวลผลข้อมูลนั้น[68]

อย่างไรก็ตาม มีข้อสังเกตว่า LED ไม่ได้บัญญัติรับรองถึงหลักความโปร่งใส (Transparency) ไว้อย่างชัดแจ้ง แตกต่างจาก GDPR เพราะด้วยธรรมชาติของการสืบสวนและสอบสวนคดีอาญา การดำเนินการในบางลักษณะก็จำต้องดำเนินการโดยลับ จึงยากที่จะมีความโปร่งใสอย่างสมบูรณ์[69]

(ค.) สิทธิของเจ้าของข้อมูลส่วนบุคคล นอกเหนือจากหลักการประมวลผลข้อมูลส่วนบุคคลโดยหลัก ผู้ควบคุมข้อมูลส่วนบุคคลย่อมมีหน้าที่ตอบสนองการใช้สิทธิของเจ้าของข้อมูล เว้นแต่การใช้สิทธินั้นไม่สมเหตุสมผล (Unfounded) ฟุ่มเฟือยเกินความจำเป็น (Excessive)[70] หรือมีเหตุในการปฏิเสธตามกฎหมาย โดย LED ได้บัญญัติรับรองสิทธิของเจ้าของข้อมูลส่วนบุคคลอยู่สามประการ อันได้แก่

(1) *สิทธิที่จะได้รับแจ้งข้อมูล (Right to be Informed)* โดยการแจ้งรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลให้เจ้าของข้อมูลทราบ จำแนกได้เป็นข้อมูลทั่วไปซึ่งเปิดเผยต่อสาธารณะและข้อมูลจำเพาะเพื่อประกอบการใช้สิทธิอื่น[71]

(2) *สิทธิที่จะเข้าถึงข้อมูล (Right to Access)* โดยยืนยันแก่บุคคลว่าข้อมูลส่วนบุคคลของบุคคลนั้น ๆ ถูกนำไปประมวลผลหรือไม่ และมีรายละเอียดอย่างไร[72]

---

[66] Ibid., Article 28-29

[67] Ibid., Article 30-31

[68] Ibid., Article 3 (8)

[69] Mark Leiser and Bart Custers, "The Law Enforcement Directive: Conceptual Challenges of Eu Directive 2016/680," in **European Data Protection Law Review** 5, 3 (October 2019).

[70] Article 12 (4) Law Enforcement Directive." (LED)

[71] Ibid., Article 13; Council of Europe, "Practical Guide on the Use of Personal Data in the Police Sector."

[72] Article 14 Law Enforcement Directive." (LED)

(3) *สิทธิที่จะแก้ไข ลบ หรือจำกัดการประมวลผล (Right to Rectification or Erasure of Personal Data and Restriction of Processing)* โดยแก้ไขข้อมูลส่วนบุคคลที่ไม่ถูกต้องสมบูรณ์และลบข้อมูลส่วนบุคคลที่ถูกประมวลผลโดยไม่ชอบด้วยกฎหมายหรือพ้นระยะเวลาเก็บรักษา แต่หากมีความจำเป็นที่จะต้องเก็บรักษาข้อมูลเพื่อเป็นหลักฐาน หรือเป็นกรณีไม่สามารถยืนยันความถูกต้องของข้อมูลส่วนบุคคล ก็ให้จำกัดการประมวลผลข้อมูลส่วนบุคคลแทนการลบได้[73]

อย่างไรก็ตาม การใช้สิทธิของเจ้าของข้อมูลจะต้องไม่กระทบการสืบสวนและสอบสวนคดีอาญาหน่วยงานผู้มีอำนาจหน้าที่จึงอาจปฏิเสธการใช้สิทธิของเจ้าของข้อมูล หากมีเหตุอย่างใดอย่างหนึ่งต่อไปนี้[74]

(1) เพื่อไม่ให้เป็นอุปสรรคต่อการป้องกัน สืบสวน ตรวจจับ ดำเนินคดีหรือลงโทษอาญา

(2) เพื่อรักษาความมั่นคงปลอดภัยของชาติหรือสาธารณะ

(3) เพื่อปกป้องสิทธิและเสรีภาพของบุคคลอื่นใด

โดยในการปฏิเสธ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งเหตุผลให้เจ้าของข้อมูลทราบ เว้นแต่การแจ้งนั้นจะเป็นอุปสรรคต่อการสืบสวนและสอบสวนคดีอาญา ผู้ควบคุมข้อมูลส่วนบุคคลอาจไม่ให้เหตุผลได้ (Neutral reply) แต่เจ้าของข้อมูลย่อมมีสิทธิที่จะร้องเรียนต่อหน่วยงานกำกับดูแล เพื่อให้ตรวจสอบความชอบด้วยกฎหมายของการประมวลผลข้อมูลส่วนบุคคล ซึ่งถือว่าเป็นการใช้สิทธิ “โดยอ้อม”[75]

(ง.) กลไกการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล

กลไกการบังคับใช้ LED ของสหภาพยุโรป จะอยู่ในรูปแบบหน่วยงานกำกับดูแลที่มีความเป็นอิสระ (Independent supervisory authorities)[76] ทำหน้าที่ควบคุมกำกับดูแลให้มีการปฏิบัติตาม LED ตั้งแต่ให้คำแนะนำ วินิจฉัยเรื่องร้องเรียน ตรวจสอบความชอบด้วยกฎหมายของการประมวลผลข้อมูล และในกรณีที่มีการฝ่าฝืน หน่วยงานดังกล่าวจะมีอำนาจออกคำเตือน สั่งแก้ไขปรับปรุง กระทั่งจำกัดหรือระงับการประมวลผล โดยหน่วยงานกำกับดูแลนี้จะจัดตั้งให้เป็นหน่วยงานเดียวกับหน่วยงานกำกับดูแลตาม GDPR ได้ เพียงแต่สำหรับการบังคับใช้กฎหมาย จะมีเงื่อนไขเพิ่มเติมว่าการควบคุมกำกับดูแลต้องไม่กระทบความเป็นอิสระของศาล[77]

---

[73] Ibid., Article 16

[74] Ibid., Article 13 (3), 15 and 16 (4)

[75] Ibid., Article 17; Emmanuel Salami, “The Impact of Directive (Eu) 2016/680 on the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties and on the Free Movement of Such Data on the Existing Privacy Regime,”(2017).

[76] Article 41-42 Law Enforcement Directive.”, (LED)

[77] Ibid., Article 45 (2) and 46-47

นอกจากนี้ LED ยังได้กำหนดเงื่อนไขการโอนข้อมูลไปยังต่างประเทศ[78] ได้แก่

(1) การโอนนั้นมีความจำเป็นเพื่อการป้องกัน สืบสวน ตรวจจับ ดำเนินคดี ลงโทษอาญา หรือรักษาความปลอดภัยสาธารณะ

(2) เป็นการโอนไปยังผู้ควบคุมข้อมูลส่วนบุคคลซึ่งมีวัตถุประสงค์ในการป้องกัน สืบสวน ตรวจจับ ดำเนินคดี ลงโทษทางอาญา หรือรักษาความปลอดภัยสาธารณะ

(3) ในกรณีที่ข้อมูลส่วนบุคคลได้รับมาจากรัฐสมาชิกอื่น ต้องได้รับอนุญาตล่วงหน้าตามที่กฎหมายของรัฐสมาชิกนั้นกำหนด เว้นแต่มีความจำเป็นเพื่อความมั่นคงหรือประโยชน์สาธารณะ และการอนุญาตล่วงหน้าไม่อาจกระทำได้ในเวลาที่เหมาะสม

(4) ประเทศปลายทางต้องมีระดับการคุ้มครองข้อมูลที่เพียงพออย่างหนึ่งอย่างใด ต่อไปนี้

- ได้รับวินิจฉัยถึงระดับการคุ้มครองข้อมูลที่เพียงพอ (Adequacy decision)[79]
- มีมาตรการป้องกันที่เหมาะสม (Appropriate safeguards)[80]
- เฉพาะในสถานการณ์พิเศษ (Derogations for specific situations)[81]

(5) ในกรณีที่มีการโอนข้อมูลส่วนบุคคลต่อ ต้องได้รับอนุญาตจากหน่วยงานซึ่งดำเนินการโอนเดิมหรือรัฐสมาชิกอื่นที่มีอำนาจ โดยให้คำนึงถึงปัจจัยที่เกี่ยวข้องทั้งหมด

สุดท้าย เพื่อประกันว่า LED จะมีผลบังคับใช้ได้จริงในทางปฏิบัติ การฝ่าฝืนหลักเกณฑ์ใน LED จึงต้องมีบทกำหนดความรับผิดและโทษทั้งสำหรับบุคคลธรรมดาและหน่วยงานที่เป็นนิติบุคคลอีกด้วย[82]

6. กรณีศึกษาแนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาของต่างประเทศ

จากการศึกษาแนวทางตามกฎหมายของสหราชอาณาจักร สหรัฐอเมริกา และสาธารณรัฐเกาหลี พบว่า การดำเนินงานในชั้นสืบสวนและสอบสวนคดีอาญาของทั้งสามประเทศอยู่ในบังคับที่จะต้องปฏิบัติตามกฎหมายวิธีพิจารณาความอาญาควบคู่กับกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยอาจสรุปได้โดยสังเขป ดังนี้

---

[78] Ibid., Article 35

[79] Ibid., Article 36

[80] Ibid., Article 37

[81] Ibid., Article 38

[82] Ibid., Article 57 and Recital (39)

6.1 กฎหมายวิธีพิจารณาความอาญาในต่างประเทศ

เพื่อเป็นไปตามหลักความได้สัดส่วน กฎหมายของประเทศต่าง ๆ ข้างต้นจึงมีการกำหนดกรอบการใช้อำนาจสืบสวนและสอบสวนคดีอาญาอยู่หลายประการ อาทิ

หลักเกณฑ์ที่เกี่ยวข้อง	สหราชอาณาจักร	สหรัฐอเมริกา	สาธารณรัฐเกาหลี
การค้นและยึดทั่วไป	จะต้องได้รับหมายหรือคำสั่งศาล[83]	ห้ามมิให้ค้นและยึดโดยปราศจากเหตุผลอันสมควร และห้ามมิให้ออกหมายโดยไม่มีเหตุอันควร[84]	จะต้องได้รับหมายหรือคำสั่งศาล แม้เป็นกรณีเร่งด่วน ก็จำต้องขอหมายหรือคำสั่งศาลย้อนหลัง[85]
การได้มาซึ่งข้อมูล	ผ่านกระบวนการ Double-lockหรือการตรวจสอบถ่วงดุลสองชั้น ทั้งจากหน่วยงานผู้มีอำนาจหน้าที่และศาล[86] โดยกำหนดขอบเขตการใช้อำนาจสืบสวนและสอบสวนที่ชัดเจน พร้อมบัญญัติ General privacy protection เพื่อคุ้มครองสิทธิบุคคล[87]	ได้รับคุ้มครองตาม The Fourth Amendment ด้วยหลักความคาดหมายความเป็นส่วนตัว[88] อันเป็นการเปิดโอกาสให้ศาลสามารถตีความเพื่อคุ้มครองสิทธิส่วนบุคคลได้ตามอย่างกว้างขวาง ตามแต่ละบริบทที่เกิดขึ้น นอกจากนี้ ในกฎหมายเฉพาะก็จะมีหลักเกณฑ์การขออนุญาตและเปิดโอกาสให้ผู้ได้รับผลกระทบโต้แย้งความถูกต้อง[89] อีกด้วย	จะต้องได้รับหมายหรือคำสั่งศาล โดยแบ่งข้อมูลเป็นสองระดับ ได้แก่ - ข้อมูลที่ยืนยันการติดต่อสื่อสาร - เนื้อความของการติดต่อสื่อสาร โดยบัญญัติหลักเกณฑ์การเข้าถึงเนื้อความการติดต่อสื่อสารให้มีความเคร่งครัดมากกว่า[90]

[83] มีข้อสังเกตว่า ระบบกฎหมายของสหราชอาณาจักร รายละเอียดของบทบัญญัติกฎหมายดังกล่าวอาจมีความแตกต่างกันไปตามแต่ละพื้นที่ เช่น บทบัญญัติเกี่ยวกับการค้นในอังกฤษและเวลส์จะเป็นไปตาม Article 4 Police and Criminal Evidence Act 1984 (“PACE 1984”) ในขณะที่ไอร์แลนด์เหนือจะเป็น Police and Criminal Evidence Order Article 10 (โปรดดู “Regulation (Eu) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/Ec (General Data Protection Regulation).”; UK Department for Digital Culture Media & Sport, “Explanatory Framework for Adequacy Discussion, Section F: Law Enforcement,”(2020).Section F: Law Enforcement,"(2020)

[84] “The Fourth Amendment.”

[85] Article 215 Criminal Procedure Act (CPA), Article 12 (3) Constitution of the Republic of Korea.

[86] Article 18-25 Investigatory Powers Act 2016

[87] Ibid., Article 2

[88] “Katz V. United States,” (1967).

[89] ปิติ เอี่ยมจำรูญลาภ, “กฎหมายเกี่ยวกับการกำหนดให้รัฐเข้าถึง หรือได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกัน : กรณีศึกษาประเทศสหรัฐอเมริกา,”(ธันวาคม 2561).

[90] Article 6 The Communication Privacy Protection Act

หลักเกณฑ์ที่เกี่ยวข้อง	สหราชอาณาจักร	สหรัฐอเมริกา	สาธารณรัฐเกาหลี
การขอข้อมูลจากเอกชน	ถือเป็นการค้นและยึดทั่วไป จึงต้องได้รับหมายหรือคำสั่งศาล[91]	ไม่ได้รับความคุ้มครอง เนื่องจาก “The third-party doctrine” วางหลักว่าบุคคลไม่อาจคาดหมายความเป็นส่วนตัวจากข้อมูลที่ให้บุคคลที่สามด้วยความสมัครใจ[92] อย่างไรก็ตาม ข้อมูลส่วนบุคคลที่อยู่ในครอบครองของเอกชนอาจได้รับความคุ้มครองตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลเฉพาะภาคส่วน[93] ในแง่นี้ การคุ้มครองดังกล่าวจึงเป็นเสมือนข้อยกเว้นของ The third-party doctrine[94]	เป็นการขอความร่วมมือบนพื้นฐานความสมัครใจ[95] โดยภาคเอกชนที่เปิดเผยข้อมูลจะมีหน้าที่ในการแจ้งข้อเท็จจริงให้เจ้าของข้อมูลทราบอีกด้วย[96]

6.2 กฎหมายคุ้มครองข้อมูลส่วนบุคคลในต่างประเทศ

จากการศึกษากฎหมายของสหราชอาณาจักร สหรัฐอเมริกา และสาธารณรัฐเกาหลี พบว่าไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศใดที่กำหนดบทยกเว้นให้การสืบสวนและสอบสวนคดีอาญาเป็นการทั่วไปในลักษณะเดียวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การสืบสวนและสอบสวนคดีอาญาของทั้งสามประเทศจึงยังคงอยู่ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยมีหลักเกณฑ์ที่เกี่ยวข้องต่อไปนี้

---

[91] European Commission, “Commission Implementing Decision of 28.6.2021 Pursuant to Regulation (Eu) 2016/679 of the European Parliament and of the Council on the Adequate Protection of Personal Data by the United Kingdom.”

[92] “Smith V. Maryland,” (1979).

[93] ยกตัวอย่างเช่น The Right to Financial Privacy Act of 1978 (RFPA) หรือ Health Insurance Portability and Accountability Act of 1996 (HIPAA) หรือ The Cable Communication Policy Act of 1984 (Cable Act) ฯลฯ

[94] Rebecca Lipman, “The Third Party Exception: Reshaping an Imperfect Doctrine for the Digital Age,” Harvard Law & Policy Review 8(2014); Erin Murphy, “The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions,” in **Michigan Law Review** 111, 4 (2013).

[95] Article 83 (3) The Telecommunications Business Act

[96] Article 2 Personal Information Protection Act

หลักเกณฑ์ที่เกี่ยวข้อง	สหราชอาณาจักร	สหรัฐอเมริกา	สาธารณรัฐเกาหลี
ขอบเขตของข้อมูลส่วนบุคคล	Personal data (ข้อมูลส่วนบุคคล) หมายถึงข้อมูลเกี่ยวกับบุคคล ซึ่งระบุหรือทำให้อาจระบุถึงบุคคลธรรมดาที่มีชีวิตอยู่ไม่ว่าโดยตรงหรือโดยอ้อม[97]	Record (บันทึกข้อมูล) คือชุดหรือกลุ่มของข้อมูลเกี่ยวกับบุคคลที่มีสัญชาติอเมริกันหรือมีถิ่นที่อยู่ในสหรัฐอเมริกา ซึ่งอยู่ในครอบครองของหน่วยงานรัฐระดับสหพันธรัฐ[98]	Personal Information (ข้อมูลส่วนบุคคล) หมายถึงข้อมูลเกี่ยวกับบุคคลที่มีชีวิตอยู่ ไม่ว่าระบุถึงตัวบุคคลโดยตรง หรือประกอบกับข้อมูลอื่นเพื่อระบุถึงบุคคลโดยให้รวมถึงข้อมูลแฝง[99]
เกณฑ์การคุ้มครองข้อมูลส่วนบุคคล	อยู่ภายใต้บังคับของ PART 3: Law Enforcement Processing The Data Protection Act 2018 (The UK DPA) ซึ่งเป็นกฎเกณฑ์เฉพาะสำหรับการบังคับใช้กฎหมายอาญา โดยมีสาระสำคัญเหมือน LED ของสหภาพยุโรป เว้นแต่มีการยอมรับให้ “ความยินยอม” เป็นฐานการประมวลผลข้อมูล[100]	มีกฎหมายเฉพาะเรื่องเฉพาะกรณีกระจัดกระจายอยู่จำนวนมาก แต่สำหรับการบังคับใช้กฎหมายของหน่วยงานระดับสหพันธรัฐ จะอยู่ภายใต้ The Privacy Act of 1974 ซึ่งไม่ได้มีหลักเกณฑ์เฉพาะสำหรับการสืบสวนและสอบสวนคดีอาญา มีเพียงข้อยกเว้นเป็นรายบทบัญญัติ โดยมักยกเว้นให้การสืบสวนและสอบสวนคดีอาญาสามารถเก็บรวบรวมและเปิดเผยบันทึกข้อมูลได้มากกว่ากรณีทั่วไป[101]	อยู่ภายใต้บังคับ The Personal Information Protection Act (South Korea’s PIPA) แต่ไม่ได้มีหลักเกณฑ์เฉพาะสำหรับการสืบสวนและสอบสวนคดีอาญา เพียงแต่กำหนดให้การประมวลผลข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาต้องมีกฎหมายเป็นฐานอำนาจ และกำหนดบทยกเว้นเป็นรายมาตราสำหรับการสืบสวนและสอบสวนคดีอาญาเป็นการเฉพาะ[102]

[97] Article 3 (2) Data Protection Act 2018

[98] “§ 552a. (the Privacy Act of 1974).”, (a)(4)

[99] Article 2 Personal Information Protection Act

[100] Article 35 (2) Data Protection Act 2018 European Commission, “Commission Implementing Decision of 28.6.2021 Pursuant to Directive (Eu) 2016/680 of the European Parliament and of the Council on the Adequate Protection of Personal Data by the United Kingdom.”

[101] Murphy, E., “The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions,” in **Michigan Law Review**

[102] ยกตัวอย่างเช่น การประมวลผลข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาของสาธารณรัฐเกาหลีได้รับยกเว้นไม่จำต้องจดทะเบียนแฟ้มข้อมูลส่วนบุคคล และไม่ต้องบันทึกฐานทางกฎหมาย เมื่อใช้ข้อมูลแตกต่างจากวัตถุประสงค์ดั้งเดิม และได้รับยกเว้นให้สามารถใช้กล้องตรวจจับภาพในพื้นที่สาธารณะได้ (โปรดดู “Personal Information Protection Act.”, Article 18, 25 (1) and 32 (2).)

หลักเกณฑ์ที่เกี่ยวข้อง	สหราชอาณาจักร	สหรัฐอเมริกา	สาธารณรัฐเกาหลี
สิทธิของเจ้าของข้อมูลส่วนบุคคล	แยกบัญญัติสิทธิเจ้าของข้อมูลในชั้นสืบสวนและสอบสวนคดีอาญาใน PART 3: Law Enforcement Processing โดยรับรองสิทธิน้อยกว่าการประมวลผลข้อมูลทั่วไป รวมถึงกำหนดกลไกในการใช้สิทธิทางอ้อมผ่านหน่วยงานกำกับดูแลเช่นเดียวกับ LED[103]	The Privacy Act of 1974 รับรองสิทธิของเจ้าของข้อมูลในการเข้าถึงและโต้แย้งความถูกต้องของบันทึกข้อมูล เช่นเดียวกับการดำเนินการทั่วไป อย่างไรก็ดี หน่วยงานบังคับใช้กฎหมายอาจใช้อำนาจกำหนดข้อยกเว้นการเข้าถึงบันทึกข้อมูลได้เพิ่มเติม[104] นอกจากนี้ พลเมืองสหรัฐอเมริกายังมีสิทธิที่จะโต้แย้งความชอบด้วยกฎหมายของการใช้อำนาจสืบสวนและสอบสวนคดีอาญาตาม The Fourth Amendment ซึ่งอาจรวมถึงการใช้สิทธิขอให้ระงับหรือทำลายข้อมูลส่วนบุคคลที่ได้มาโดยไม่ชอบอีกด้วย	รับรองสิทธิเจ้าของข้อมูลในชั้นสืบสวนและสอบสวนคดีอาญาเช่นเดียวกับการดำเนินงานทั่วไป แต่การใช้สิทธินั้นอาจถูกปฏิเสธได้หากการปฏิเสธเป็นไปตามกฎหมาย หรือการใช้สิทธิจะทำให้เสียหายแก่ชีวิต ร่างกาย ทรัพย์สิน หรือประโยชน์ของบุคคลอื่นใด[105]
กลไกการบังคับใช้	กำหนดความรับผิดทางอาญาและโทษปรับทางปกครองสำหรับการฝ่าฝืนหลักเกณฑ์[106] และบัญญัติ ข้อจำกัดการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศตามแนวทางของ LED โดยมี	กำหนดความรับผิดอาญาสำหรับการฝ่าฝืนหลักเกณฑ์[107] ในขณะที่การบังคับใช้กฎหมายจะไม่ได้อยู่ในรูปแบบองค์กรอิสระ แต่จะเป็นองค์กรต่าง ๆ ที่มีอำนาจหน้าที่ตามกฎหมายเฉพาะประกอบกับกลไกกำกับดูแลตนเอง[108]	กำหนดความรับผิดทางอาญาและโทษปรับทางปกครองสำหรับการฝ่าฝืนหลักเกณฑ์ พร้อมบัญญัติข้อกำหนดในการโอนข้อมูลไปยังต่างประเทศ โดยมีองค์กรอิสระคือ Personal Information Protection Commission (PIPC)

[103] Article 51 Data Protection Act 2018

[104] "§ 552a. (the Privacy Act of 1974).", (j)(2) and (k)(2)

[105] "Personal Information Protection Act.", Chapter V. guarantee of rights of data subjects.

[106] Article 170-173 Data Protection Act 2018

[107] "§ 552a. (the Privacy Act of 1974).", (i)

[108] นคร เสรีรักษ์, ความเป็นส่วนตัว: ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย, หน้า 164.

หลักเกณฑ์ที่เกี่ยวข้อง	สหราชอาณาจักร	สหรัฐอเมริกา	สาธารณรัฐเกาหลี
	Information Commissioner's Office (ICO) เป็นองค์กรอิสระทำหน้าที่ควบคุมและกำกับดูแลการประมวลผลข้อมูลส่วนบุคคลในทุกกิจการ[109]		ทำหน้าที่ควบคุมและกำกับดูแลการประมวลผลข้อมูลส่วนบุคคลในกิจการทุกประเภท[110]

7. บทวิเคราะห์ความเหมาะสมของการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา

เมื่อการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาในสหภาพยุโรปและต่างประเทศล้วนแล้วแต่บังคับใช้กฎหมายวิธีพิจารณาความอาญาควบคู่กับกฎหมายคุ้มครองข้อมูลส่วนบุคคล การวิเคราะห์ความเหมาะสมของแนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาของประเทศไทยจึงต้องทำการวิเคราะห์มาตรการทางกฎหมายเชิงควบคู่ แบ่งเป็นกฎหมายวิธีพิจารณาความอาญา (หัวข้อที่ 7.1) และกฎหมายคุ้มครองข้อมูลส่วนบุคคล (หัวข้อที่ 7.2) โดยนำแนวทางของสหภาพยุโรปมาเป็นเกณฑ์พื้นฐานในการประเมิน เนื่องจากแนวทางการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปเป็นมาตรฐานที่ได้รับการยอมรับจากนานาประเทศ และเป็นต้นแบบของการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยในปัจจุบัน

7.1 บทวิเคราะห์กฎหมายวิธีพิจารณาความอาญา

จากการศึกษาพบว่า แม้กฎหมายวิธีพิจารณาความอาญากับกฎหมายคุ้มครองข้อมูลส่วนบุคคลจะเป็นกฎหมายคนละฉบับ แต่กฎหมายวิธีพิจารณาความอาญาก็เป็นกฎหมายที่ให้อำนาจเจ้าหน้าที่รัฐเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา ซึ่งเป็นมาตรการที่กระทบต่อข้อมูลส่วนบุคคล กฎหมายวิธีพิจารณาความอาญาจึงมีความเชื่อมโยงกับระดับการคุ้มครองข้อมูลส่วนบุคคล เพราะหากกฎหมายวิธีพิจารณาความอาญาไม่มีกรอบจำกัดอำนาจที่เหมาะสม หลักประกันสิทธิในข้อมูลส่วนบุคคลของประชาชนก็ย่อมถูกลดทอนลงเมื่ออยู่ในชั้นสืบสวนและสอบสวน

[109] European Commission, "Commission Implementing Decision of 28.6.2021 Pursuant to Directive (Eu) 2016/680 of the European Parliament and of the Council on the Adequate Protection of Personal Data by the United Kingdom."

[110] European Commission, "Commission Implementing Decision of 17.12.2021 Pursuant to Regulation (Eu) 2016/679 of the European Parliament and of the Council on the Adequate Protection of Personal Data by the Republic of Korea under the Personal Information Protection Act."

คดีอาญา จึงมีความจำเป็นที่รัฐแต่ละรัฐจะต้องออกแบบให้กฎหมายวิธีพิจารณาความอาญารักษาสมดุลระหว่างการป้องปรามอาชญากรรมกับการคุ้มครองสิทธิความเป็นส่วนตัวของบุคคลให้มีความเหมาะสมและได้สัดส่วนกัน

อย่างไรก็ตาม เมื่อนำกฎหมายวิธีพิจารณาความอาญาของไทยมาประเมินกับหลักเกณฑ์ปกป้องสิทธิของสหภาพยุโรป กลับพบว่ากฎหมายวิธีพิจารณาความอาญาของไทยมีแนวโน้มที่จะถูกพิจารณาว่าไม่สอดคล้องกับหลักเกณฑ์ดังกล่าว โดยมีข้อควรพิเคราะห์สามประการคือ

(1) ขอบเขตการค้นในประมวลกฎหมายวิธีพิจารณาความอาญาที่ผ่านกระบวนการตรวจสอบจากศาลนั้นมีขอบเขตจำกัด จึงไม่สอดคล้องกับ “หลักการตรวจสอบถ่วงดุล” เพราะหากเป็นการใช้อำนาจลักษณะอื่น นอกเหนือจากการค้นในที่รโหฐานหรือการค้นเอกสารซึ่งส่งทางไปรษณีย์โทรเลข[111] ก็มีแนวโน้มที่เจ้าหน้าที่รัฐจะกล่าวอ้างว่าเป็นอำนาจสอบสวนทั่วไปเพื่อไม่ให้อยู่ภายใต้บังคับที่จะต้องได้รับอนุญาตจากศาล เช่น การค้นหาตำแหน่งจากเสาสัญญาณโทรศัพท์ บันทึกภาพด้วยโดรน หรือใช้เทคโนโลยีตรวจจับใบหน้า เป็นต้น

(2) บทบัญญัติให้อำนาจพนักงานเจ้าหน้าที่ได้มาซึ่งข้อมูลข่าวสารตามพระราชบัญญัติเฉพาะมักใช้ถ้อยคำอย่างกว้าง ๆ จึงไม่สอดคล้องกับ “หลักความเฉพาะเจาะจง” กล่าวคือ

- แม้โดยทั่วไป การได้มาซึ่งข้อมูลข่าวสารตามพระราชบัญญัติเฉพาะจะจำกัดขอบเขตประเภทความผิดเพื่อการสืบสวนและสอบสวนหรือบังคับใช้กฎหมายนั้น ๆ แต่พระราชบัญญัติบางฉบับ เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ก็ขยายขอบเขตไปถึงความผิดอื่นที่มีคอมพิวเตอร์เกี่ยวข้อง ทำให้ในปัจจุบัน ความผิดอาญาแทบทุกประเภทจึงอาจถูกพิจารณาได้ว่าอยู่ในขอบเขตความผิดตามพระราชบัญญัตินี้ได้ จึงไม่มีความเฉพาะเจาะจงในแง่เหตุแห่งการใช้อำนาจ[112]

- พระราชบัญญัติเฉพาะมักบัญญัติให้อำนาจด้วยถ้อยคำที่ว่า “เพื่อให้ได้มาซึ่งข้อมูลข่าวสาร” เท่านั้น โดยไม่ระบุมาตรการที่จะใช้อย่างชัดเจน จึงเป็นการเปิดโอกาสให้เจ้าหน้าที่รัฐใช้มาตรการตามอำเภอใจ โดยไม่จำกัดวิธีการ ซึ่งไม่มีความเฉพาะเจาะจงในแง่มาตรการที่ใช้[113]

---

[111] มาตรา 32 และมาตรา 105 ประมวลกฎหมายวิธีพิจารณาความอาญา

[112] คณาธิป ทองรวีวงศ์, “การปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน.”; คณาธิป ทองรวีวงศ์, “สิทธิในข้อมูลส่วนบุคคลที่ไม่ได้รับการคุ้มครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 : การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามกฎหมายเกี่ยวกับความมั่นคงของรัฐ”, **วารสารกฎหมายสิทธิมนุษยชน**.

[113] ตัวอย่างเช่น มาตรา 25 พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 และ มาตรา 30 พระราชบัญญัติป้องกันและปราบปรามการค้ามนุษย์ พ.ศ. 2551.

- การได้มาซึ่งข้อมูลข่าวสารของประเทศไทย ไม่ได้มีการกำหนดขอบเขตในแง่เป้าหมายที่ตัวบุคคล แต่จะเป็นการกำหนดขอบเขตที่ข้อมูลข่าวสาร ที่ถูกใช้เพื่อกระทำผิด ข้อมูลที่เจ้าหน้าที่รัฐอาจเข้าถึงจึงไม่ได้จำกัดเฉพาะข้อมูลของผู้ต้องสงสัยหรือผู้กระทำผิด[114] จึงไม่มีความเฉพาะเจาะจงในแง่เป้าหมาย

- ในบรรดาพระราชบัญญัติเฉพาะ พบว่าพระราชบัญญัติบางฉบับก็ไม่ได้มีการกำหนดขอบเขตของระยะเวลาในการใช้อำนาจที่ชัดเจน เช่น การตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จึงไม่มีความเฉพาะเจาะจงในแง่ระยะเวลา

นอกจากนี้ เมื่อพิจารณาเปรียบเทียบกับกฎหมายต่างประเทศจะพบว่าประเทศไทยไม่มีมาตรการเพื่อคุ้มครองสิทธิของบุคคลแต่อย่างใด จึงแตกต่างจากกฎหมายต่างประเทศที่ให้ความสำคัญกับการคุ้มครองสิทธิของผู้ได้รับผลกระทบจากการใช้มาตรการเหล่านี้

(3) การขอข้อมูลส่วนบุคคลจากภาคเอกชนในรูปแบบหมายเรียกพยานเอกสารหรือหนังสือขอความร่วมมือ ไม่สอดคล้องกับ “หลักความเฉพาะเจาะจง” และ “หลักการตรวจสอบถ่วงดุล” เพราะไม่ว่าการกระทำผิดประเภทใด ในสถานการณ์อย่างไร เจ้าหน้าที่รัฐก็อาจขอตรวจดูข้อมูลข่าวสารได้โดยที่ไม่มีข้อจำกัดอำนาจและไม่จำต้องได้รับคำสั่งหรือหมายจากศาล ในทำนองเดียวกันกับสหรัฐอเมริกา[115] ซึ่งบริบทแวดล้อมทางกฎหมายดังกล่าวเป็นปัจจัยหนึ่งที่ทำให้สหภาพยุโรปประเมินว่าสหรัฐอเมริกามีระดับการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอ เป็นเหตุให้การโอนข้อมูลระหว่างสหรัฐอเมริกาและสหภาพยุโรปไม่อาจกระทำได้โดยเสรี และต้องอาศัยการทำข้อตกลงระหว่างประเทศระดับทวิภาคี[116]

---

[114] คณาธิป ทองรวีวงศ์, “การปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน.”; คณาธิป ทองรวีวงศ์, “สิทธิในข้อมูลส่วนบุคคลที่ไม่ได้รับการคุ้มครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 : การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามกฎหมายเกี่ยวกับความมั่นคงของรัฐ”, **วารสารกฎหมายสิทธิมนุษยชน**.

[115] มีข้อสังเกตว่า แม้การขอข้อมูลข่าวสารจากภาคเอกชนในประเทศไทยและสหรัฐอเมริกาจะไม่ได้อยู่ในบังคับที่จะต้องมีคำสั่งหรือหมายจากศาลเช่นเดียวกัน แต่การเปิดเผยข้อมูลส่วนบุคคลโดยภาคเอกชนของทั้งสองประเทศก็มีพื้นฐานทางกฎหมายที่แตกต่างกันอยู่ โดยสำหรับประเทศไทย การเปิดเผยข้อมูลส่วนบุคคลของภาคเอกชนจะอยู่ภายใต้บังคับของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 คือจะเปิดเผยได้ต่อเมื่อมีฐานทางกฎหมาย ซึ่งในด้านที่เอกชนเปิดเผยข้อมูลส่วนบุคคลให้รัฐนั้นจะอาศัยฐานการปฏิบัติหน้าที่ตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 24 (6) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แตกต่างจากสหรัฐอเมริกาที่การไม่เปิดเผยข้อมูลส่วนบุคคลของภาคเอกชนจะอยู่บนพื้นฐานของกฎหมายคุ้มครองข้อมูลส่วนบุคคลเฉพาะเรื่องหรือสัญญามากกว่า

[116] “Commission Decision of 26 July 2000 Pursuant to Directive 95/46/Ec of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the Us Department of Commerce (Notified under Document Number C(2000) 2441),” (2000); คณาธิป ทองรวีวงศ์, “การปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน.”

สุดท้าย หากนำข้อวิเคราะห์ทั้งหมดมาพิจารณาร่วมกับ “หลักความจำเป็นและได้สัดส่วน” อาจสรุปได้ว่า แม้มีความจำเป็นที่กฎหมายวิธีพิจารณาความอาญาจะต้องให้อำนาจเจ้าหน้าที่รัฐเก็บรวบรวม ใช้และเปิดเผยข้อมูลส่วนบุคคลในการป้องปรามอาชญากรรม แต่เมื่อกฎหมายวิธีพิจารณาความอาญาของไทยไม่อาจควบคุมการใช้อำนาจสืบสวนและสอบสวนให้เป็นไปตามหลักเกณฑ์ปกป้องสิทธิ อันอาจส่งผลกระทบต่อสิทธิความเป็นส่วนตัวในข้อมูลจนไม่ได้สัดส่วน จึงมีความเสี่ยงที่ภาพรวมการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยจะได้รับการวินิจฉัยได้ว่ามีระดับที่ไม่เพียงพอตามมาตรฐานของสหภาพยุโรป

7.2 บทวิเคราะห์กฎหมายคุ้มครองข้อมูลส่วนบุคคล

จากการศึกษาพบว่า แม้การสืบสวนและสอบสวนคดีอาญาจะเป็นความชอบธรรมของรัฐประการหนึ่งที่จะจำกัดการคุ้มครองข้อมูลส่วนบุคคล แต่การกำหนดบทยกเว้นทั่วไปมิให้กฎหมายคุ้มครองข้อมูลส่วนบุคคลใช้บังคับแก่การสืบสวนและสอบสวนคดีอาญาโดยสิ้นเชิงนั้นอาจเป็นการยกเว้นที่กว้างขวางเกินกว่าความจำเป็น จากการศึกษากฎหมายระหว่างประเทศและกฎหมายต่างประเทศ พบว่ามีหลายประเทศที่ไม่ได้กำหนดให้การสืบสวนและสอบสวนคดีอาญาเป็นข้อยกเว้นของการคุ้มครองข้อมูลส่วนบุคคลโดยเด็ดขาด แต่จะกำหนดเป็นข้อยกเว้นรายมาตราหรือบัญญัติกฎเกณฑ์เฉพาะ เพื่อให้สอดคล้องกับบริบทการสืบสวนและสอบสวนคดีอาญา ทั้งนี้ เนื่องจากความเป็นส่วนตัวในข้อมูลเป็นหนึ่งในสิทธิมนุษยชนขั้นพื้นฐาน รัฐจึงมีพันธกรณีที่จะต้องคุ้มครองไม่ว่าจากการดำเนินงานประเภทใดประกอบกับสิทธิดังกล่าวมีลักษณะเฉพาะ แตกต่างไปจากสิทธิและเสรีภาพรูปแบบดั้งเดิม ทำให้กฎหมายทั่วไป รวมถึงกฎหมายวิธีพิจารณาความอาญา มีข้อจำกัดโดยสภาพในการคุ้มครองข้อมูลส่วนบุคคล จึงมีความจำเป็นที่การสืบสวนและสอบสวนคดีอาญาจะต้องอยู่ในบังคับของกฎหมายคุ้มครองข้อมูลส่วนบุคคล เพื่อให้การประกันสิทธิในข้อมูลส่วนบุคคลของประชาชนมีมาตรการที่เหมาะสมและสอดคล้องกับลักษณะของความเป็นส่วนตัวในข้อมูลมารองรับเช่นเดียวกับการดำเนินงานประเภทอื่น

ด้วยเหตุนี้ บทยกเว้นตามมาตรา 4 (2) และ (5) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งมีผลเป็นการยกเว้นการสืบสวนและสอบสวนคดีอาญาทั้งกิจการให้ไม่อยู่ภายใต้บังคับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เว้นแต่ในส่วนของการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล จึงมีขอบเขตที่กว้างขวางเกินกว่าความจำเป็นและไม่สอดคล้องกับหลักการสากล รวมถึงรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ซึ่งมาตรา 32 วางหลักให้การตรากฎหมายที่จำกัดสิทธิในข้อมูลส่วนบุคคลพึงกระทำเท่าที่จำเป็นเพื่อประโยชน์สาธารณะเท่านั้น โดยเฉพาะเมื่อพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นมีฐานะเป็นกฎหมายกลาง จึงควรมุ่งเน้นการคุ้มครองสิทธิมากกว่าจำกัดสิทธิเสียเอง เพราะหากมีความจำเป็น ก็อาจบัญญัติบทยกเว้นเป็นรายกรณี

ได้ตามความเหมาะสม จะเห็นได้จากมาตรา 4 วรรคสอง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เปิดช่องให้การยกเว้นมิให้นำพระราชบัญญัตินี้ไม่ว่าทั้งหมดหรือแต่บางส่วนมาใช้บังคับให้ตราเป็นพระราชกฤษฎีกาได้

ยิ่งไปกว่านั้น เมื่อพิจารณาประกอบกับข้อเท็จจริงที่ว่าหมวด 3 ตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ซึ่งบังคับใช้แก่การสืบสวนและสอบสวนคดีอาญาอยู่ในปัจจุบัน พบว่ายังคงมีข้อจำกัดจากการที่มีบทบัญญัติอยู่เพียง 5 มาตรา และได้รับยกร่างตั้งแต่ในปี พ.ศ. 2540 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 จึงมิใช่มาตรการที่มีความเหมาะสมอีกต่อไป มิฉะนั้น การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาของประเทศไทยก็จะมีมาตรฐานที่ไม่เทียบเท่าการดำเนินการประเภทอื่นที่ปัจจุบันอยู่ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

อย่างไรก็ดี การกำหนดให้การสืบสวนและสอบสวนคดีอาญาอยู่ภายใต้หลักการคุ้มครองข้อมูลส่วนบุคคล ก็จำเป็นที่จะต้องพิจารณาต่อไปว่า เกณฑ์การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญานั้นควรเป็นเช่นไร จึงจะรักษาสมดุลระหว่างการคุ้มครองสิทธิส่วนบุคคลกับการป้องกันและปราบปรามอาชญากรรมได้อย่างเหมาะสม โดยมีข้อควรพิจารณา 4 ประการดังนี้

(1) โดยทั่วไป “ขอบเขตข้อมูลส่วนบุคคล” ที่ได้รับความคุ้มครองในชั้นสืบสวนและสอบสวนคดีอาญาจะมีนิยามเช่นเดียวกับกิจการทั่วไป ไม่ได้มีกฎเกณฑ์เฉพาะแต่อย่างใด จึงเห็นว่าประเทศไทยสามารถนำนิยามของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาปรับใช้ได้ เนื่องจากบทนิยามในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สอดคล้องกับหลักการของสหภาพยุโรปมากกว่าพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ที่จำกัดการคุ้มครองเฉพาะผู้มีสัญชาติไทยหรือมีถิ่นที่อยู่ในประเทศไทย เพราะการจำกัดดังกล่าวอาจทำให้สหภาพยุโรปประเมินว่า ข้อมูลของพลเมืองยุโรปไม่ได้รับการคุ้มครองอย่างเพียงพอในบริบทของการโอนข้อมูล เช่นเดียวกับสหรัฐอเมริกา[117]

ทว่าสำหรับการขยายขอบเขตเชิงพื้นที่ หรือการคุ้มครองข้อมูลส่วนบุคคลซึ่งเจ้าของข้อมูลอยู่ในประเทศไทยจากการประมวลผลข้อมูลที่เกิดขึ้นนอกประเทศ[118] เห็นควรยกเว้นไม่ให้การสืบสวนและสอบสวนคดีอาญาอยู่ภายใต้บังคับของการขยายขอบเขตเชิงพื้นที่ดังกล่าว ตามแนวทางของ LED เพราะการสืบสวนและสอบสวนมีความเกี่ยวพันกับอำนาจอธิปไตยของแต่ละรัฐ จึงไม่ควรบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แก่การสืบสวนและสอบสวนคดีอาญานอกราชอาณาจักรได้

---

[117] European Parliament, “A Comparison between Us and Eu Data Protection Legislation for Law Enforcement,”(2015).

[118] มาตรา 5 วรรคสอง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

(2) จากการศึกษาพบว่า กฎหมายของสหภาพยุโรปและกฎหมายของต่างประเทศยอมรับให้นำ “เกณฑ์การคุ้มครองข้อมูลส่วนบุคคล” ตามมาตรฐานสากลมาใช้บังคับแก่การสืบสวนและสอบสวนคดีอาญาเกือบทั้งสิ้น โดยกำหนดข้อยกเว้นเฉพาะในบางประเด็น ได้แก่

- ฐานทางกฎหมาย กล่าวคือการสืบสวนและสอบสวนคดีอาญาได้รับยกเว้นให้สามารถเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลได้ โดยไม่จำต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หากมีกฎหมายให้อำนาจ เว้นแต่ในบางบริบท กฎหมายต่างประเทศก็ยอมรับให้ใช้ความยินยอมเป็นฐานทางกฎหมายในชั้นสืบสวนและสอบสวนคดีอาญาได้ ซึ่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะมีฐานทางกฎหมายที่เกี่ยวข้องคือ (1) ฐานการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ[119] และ (2) ฐานความยินยอม[120] แต่การอาศัยฐานความยินยอมนั้นจะต้องกระทำอย่างจำกัดและปฏิบัติตามเงื่อนไขการขอความยินยอมโดยเคร่งครัด เพื่อประกันความเป็นอิสระในการให้ความยินยอมของเจ้าของข้อมูลส่วนบุคคล[121]

- หลักการประมวลผลข้อมูลส่วนบุคคล เห็นว่ามีเพียงหลักความโปร่งใสเท่านั้นที่การสืบสวนและสอบสวนคดีอาญาไม่อาจอยู่ในบังคับได้โดยบริบูรณ์ เพราะหลักดังกล่าวเรียกร้องให้มีการเปิดเผยต่อเจ้าของข้อมูลว่า ข้อมูลส่วนบุคคลจะถูกประมวลผลอย่างไร ด้วยเหตุผลใด จึงขัดกับธรรมชาติของการสืบสวนและสอบสวนคดีอาญา ในแง่นี้ การมีข้อจำกัดอำนาจที่ชัดเจนจึงอาจมีความเหมาะสมกับบริบทของการสืบสวนและสอบสวนคดีอาญามากกว่า[122]

ด้วยเหตุนี้ จึงเห็นควรนำแนวทางของ LED มาปรับใช้กับประเทศไทย โดยให้การสืบสวนและสอบสวนคดีอาญายังคงอยู่ในบังคับที่จะต้องปฏิบัติหลักการประมวลผลข้อมูลอื่น ๆ เว้นแต่หลักความโปร่งใส ซึ่งจะมีผลกระทบต่อการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาในสองมิติ คือในด้านหนึ่ง จะส่งผลกระทบต่อการใช้สิทธิของเจ้าของข้อมูลในการควบคุมและตัดสินใจเกี่ยวกับข้อมูล เพราะเจ้าของข้อมูลไม่มีโอกาสทราบข้อเท็จจริงและรายละเอียดที่เกี่ยวข้องแต่แรกเริ่ม

---

[119] มาตรา 24 (4) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[120] มาตรา 19 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[121] มีข้อสังเกตว่า LED ของสหภาพยุโรปจะไม่ได้บัญญัติรับรองให้ความยินยอมเป็นฐานการประมวลผลข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา เนื่องจากเห็นว่าในชั้นสืบสวนและสอบสวนคดีอาญา เจ้าของข้อมูลอาจไม่ได้มีอิสระในการให้ความยินยอมอย่างแท้จริง เพราะมีความไม่เท่าเทียมอย่างชัดเจนเชิงอำนาจ (โปรดดู “General Data Protection Regulation.” (GDPR), Recital 43.”) ดังนั้น การนำฐานความยินยอมมาใช้ในชั้นสืบสวนและสอบสวนคดีอาญาจึงควรกระทำอย่างจำกัดอย่างยิ่ง โดยอาจพิจารณาแนวทางตามคำแนะนำของ ICO สหราชอาณาจักร (โปรดดู Information Commission’s Office (ICO), “Guide to Law Enforcement Processing” [Online] Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/) [14 December 2020]

[122] Leiser, M. and B. Custers, “The Law Enforcement Directive: Conceptual Challenges of Eu Directive 2016/680,” in **European Data Protection Law Review.**

และในอีกด้านหนึ่ง ก็มีความจำเป็นที่การสืบสวนและสอบสวนคดีอาญาต้องกำหนดมาตรการทดแทนเพื่อถ่วงดุลกับการยกเว้นการบังคับใช้หลักความโปร่งใสดังกล่าวตามแนวทางกฎหมายของต่างประเทศ เช่น การจัดเก็บบันทึก logs การกำหนดให้มีการประเมินความเสี่ยง หรือการตรวจถ่วงดุลการใช้อำนาจโดยองค์กรตุลาการ เป็นต้น

(3) แม้มีความจำเป็นที่ “สิทธิเจ้าของข้อมูลส่วนบุคคล” ในชั้นสืบสวนและสอบสวนคดีอาญาต้องถูกจำกัดกว่ากรณีปกติ แต่ในกฎหมายต่างประเทศจะมีการบัญญัติเหตุผลการปฏิเสธการใช้สิทธิอย่างชัดแจ้ง เพื่อไม่ให้การปฏิเสธคำขอกลายเป็นอำนาจดุลพินิจโดยลำพัง และในขณะเดียวกัน สหภาพยุโรปและสหราชอาณาจักรก็ได้กำหนดกลไกการใช้สิทธิโดยอ้อม โดยให้หน่วยงานกำกับดูแลตรวจสอบความชอบด้วยกฎหมายของการประมวลผลข้อมูล[123] แทนการใช้สิทธิโดยตรง ดังนั้น เมื่อพิจารณาถึงความเหมาะสม แนวทางตามกฎหมายของสหภาพยุโรปและสหราชอาณาจักรจึงอาจนำมาปรับใช้ได้เพื่อลดความเสี่ยงที่การใช้สิทธิของเจ้าของข้อมูลจะส่งผลกระทบต่อการสืบสวนและสอบสวนคดีอาญา

(4) สำหรับ “กลไกการบังคับใช้” พบว่าแต่ละประเทศไม่ได้กำหนดกลไกการบังคับใช้เฉพาะสำหรับการสืบสวนและสอบสวนคดีอาญา การบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในกระบวนการดังกล่าว จึงสามารถนำกลไกการบังคับใช้ที่มีอยู่ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาปรับใช้ได้ในทันที โดยไม่ต้องบัญญัติหลักเกณฑ์ขึ้นใหม่ ควบคู่ไปกับการตรวจสอบถ่วงดุลโดยองค์กรตุลาการ

8. ข้อเสนอแนะ

เมื่อได้พิจารณาถึงความจำเป็น แนวคิดและทฤษฎีที่เกี่ยวข้อง ตลอดจนกฎหมายระหว่างประเทศและกฎหมายต่างประเทศแล้ว ผู้เขียนจึงเห็นควรมีข้อเสนอแนะในการกำหนดแนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาสำหรับประเทศไทย ด้วยการใช้แนวทางของ LED เป็นสำคัญ ทั้งนี้ เนื่องจากกฎหมายของสหภาพยุโรปเป็นต้นแบบแนวทางการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย การนำมาปรับใช้กับระบบกฎหมายไทยจึงน่าจะมีความเหมาะสม เพราะเป็นพื้นฐานทางกฎหมายที่ประเทศไทยมีความคุ้นเคย ซึ่งจากการศึกษาพบว่า หลักการพื้นฐานประการสำคัญของ LED ในการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาคือการกำหนดให้ “การประมวลผลข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาจะกระทำได้แต่โดยมีกฎหมายบัญญัติให้อำนาจโดยชัดแจ้ง บนพื้นฐานของหลักความได้สัดส่วน” จึงเห็นสมควรให้ประเทศไทยกำหนดแนวทางเพื่อคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา โดยแบ่งเป็น 2 ส่วน ได้แก่ ข้อเสนอแนะเกี่ยวกับกฎหมายวิธีพิจารณาความอาญา และข้อเสนอแนะเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล ดังต่อไปนี้

[123] Article 51 Data Protection Act 2018. Article 17 General Data Protection Regulation

8.1 ข้อเสนอแนะเกี่ยวกับกฎหมายวิธีพิจารณาความอาญา

แม้หลักการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาจะอยู่บนพื้นฐานของ “การมีกฎหมายให้อำนาจโดยชัดแจ้ง” แต่ลำพังการมีอยู่ของกฎหมายวิธีพิจารณาความอาญา ซึ่งเป็นบทบัญญัติหลักที่ให้อำนาจเจ้าหน้าที่รัฐเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาของไทย ก็มิได้เป็นหลักประกันที่เพียงพอว่าการใช้อำนาจสืบสวนและสอบสวนจะเป็นไปด้วยความเหมาะสม จึงมีความจำเป็นที่ประเทศไทยจะต้องพิจารณาแก้ไขปรับปรุงกฎหมายวิธีพิจารณาความอาญาของไทยให้มีความสอดคล้องกับหลักสิทธิมนุษยชน โดยอาจใช้เกณฑ์ปกป้องสิทธิของสหภาพยุโรปมาเป็นแนวทาง เพื่อลดผลกระทบที่อาจเกิดขึ้นกับข้อมูลส่วนบุคคลจากการใช้มาตรการบังคับ ในชั้นสืบสวนและสอบสวนคดีอาญา เนื่องจากเกณฑ์การปกป้องสิทธิ อันประกอบด้วย (1) หลักความเฉพาะเจาะจง (2) หลักการตรวจสอบถ่วงดุล และ (3) หลักความจำเป็นและได้สัดส่วน เป็นหลักการพื้นฐานที่ปรากฏในกติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทาง การเมืองที่ประเทศไทยเป็นภาคี จึงเห็นควรให้ประเทศไทยแก้ไขปรับปรุงกฎหมายวิธีพิจารณาความอาญาให้มีความสอดคล้องกับหลักเกณฑ์การปกป้องสิทธิดังกล่าว โดยมีข้อเสนอแนะ 3 ประการดังนี้

(1) เห็นควรให้ประเทศไทยให้พิจารณาทบทวนว่าการแสวงหาพยานหลักฐานรูปแบบใดควรจัดให้อยู่ในขอบเขตการค้นที่ต้องผ่านกระบวนการตรวจสอบถ่วงดุลจากศาล โดยเฉพาะการแสวงหาพยานหลักฐานที่เกี่ยวข้องกับการใช้เทคโนโลยีสมัยใหม่ เพื่อให้สอดคล้องกับบริบททางสังคมที่เปลี่ยนแปลงไป

(2) เห็นควรให้ประเทศไทยพิจารณาแก้ไขเกณฑ์การได้มาซึ่งข้อมูลข่าวสารในพระราชบัญญัติเฉพาะต่าง ๆ ให้ชัดเจนและเฉพาะเจาะจงเพียงพอที่ประชาชนทั่วไปสามารถคาดหมายได้ ด้วยการให้รายละเอียดเกี่ยวกับเหตุแห่งการใช้อำนาจ มาตรการที่ใช้ บุคคลเป้าหมาย และกรอบระยะเวลาให้ได้มากที่สุดเท่าที่จะกระทำได้ พร้อมทั้งกำหนดมาตรการคุ้มครองสิทธิของบุคคลเพิ่มเติม โดยอาจเริ่มต้นจากการแก้ไขพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นอันดับแรก เนื่องจากพระราชบัญญัตินี้มีแนวโน้มที่จะไม่สอดคล้องกับเกณฑ์การปกป้องสิทธิของสหภาพยุโรปหลายประการ

(3) เห็นควรให้ประเทศไทยพิจารณากำหนดข้อจำกัดอำนาจในการเก็บรวบรวมข้อมูลข่าวสารจากภาคเอกชนเพิ่มเติม เพื่อมิให้เป็นอำนาจดุลพินิจของเจ้าหน้าที่รัฐโดยลำพัง อย่างไรก็ดี การกำหนดให้การขอข้อมูลข่าวสารจากภาคเอกชนต้องได้รับอนุญาตจากศาลในทุกกรณีอาจจะทำให้การสืบสวนและสอบสวนคดีอาญาขาดความคล่องตัว จึงอาจไม่เหมาะสมกับบริบทของประเทศไทย ในเบื้องต้นจึงเห็นควรให้ประเทศไทยแบ่งประเภทข้อมูลข่าวสารตามระดับความรุนแรงและผลกระทบที่อาจเกิดขึ้น เพื่อกำหนดหลักเกณฑ์ เงื่อนไข รวมถึงกระบวนการตรวจสอบให้สอดคล้องกับลักษณะของข้อมูล

อนึ่ง มีข้อสังเกตว่าแนวทางการแก้ไขปรับปรุงกฎหมายวิธีพิจารณาความอาญาอาจไม่จำกัดเพียงวิธีการต่าง ๆ ข้างต้น เนื่องจากมีงานวิจัยในประเทศไทยอีกจำนวนมากที่มีข้อเสนอแนะเกี่ยวกับ

การคุ้มครองสิทธิและเสรีภาพในชั้นสืบสวนและสอบสวนคดีอาญา ซึ่งสามารถนำมาปรับใช้เพื่อส่งเสริมให้กฎหมายวิธีพิจารณาความอาญาของประเทศไทยให้สอดคล้องกับหลักเกณฑ์การปกป้องสิทธิได้มากยิ่งขึ้นเช่นกัน[124]

8.2 ข้อเสนอแนะเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล

นอกเหนือจากการมีกฎหมายให้อำนาจโดยชัดแจ้ง การให้ความคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญายังต้องอยู่บนพื้นฐานของ “ความได้สัดส่วน” กล่าวคือ การเก็บรวบรวม ใช้และเปิดเผยข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญากระทำเท่าที่จำเป็นเพื่อบรรลุวัตถุประสงค์ในการสืบสวนและสอบสวนคดีอาญา และจะต้องไม่ก่อให้เกิดผลกระทบต่อสิทธิความเป็นส่วนตัวเกินกว่าสมควร เมื่อชั่งน้ำหนักกับประโยชน์สาธารณะที่ได้ สอดคล้องกับรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ซึ่งวางหลักให้การตรากฎหมายจำกัดสิทธิในข้อมูลส่วนบุคคลพึงกระทำเท่าที่จำเป็น เพื่อประโยชน์สาธารณะเท่านั้น[125]

ด้วยเหตุนี้ การยกเว้นไม่นำกฎหมายคุ้มครองข้อมูลส่วนบุคคลมาบังคับใช้แก่การสืบสวนและสอบสวนคดีอาญาโดยสิ้นเชิงจึงอาจไม่สอดคล้องกับหลักความได้สัดส่วน จึงสมควรให้ประเทศไทยกำหนดให้การสืบสวนและสอบสวนคดีอาญาอยู่ภายใต้หลักการคุ้มครองข้อมูลส่วนบุคคลเช่นเดียวกับการดำเนินงานอื่น ๆ แต่เพื่อให้สอดคล้องกับธรรมชาติของการสืบสวนและสอบสวน ก็มีความจำเป็นที่ประเทศไทยจะต้องกำหนดหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาเป็นการเฉพาะ แยกออกมาจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งนอกเหนือจากการบัญญัติกฎเกณฑ์เฉพาะหรือข้อยกเว้นบางส่วนโดยตราเป็นพระราชกฤษฎีกาตามมาตรา 4 วรรคสอง ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แนวทางที่สามารถกระทำได้อย่างรวดเร็วและน่าจะเหมาะสมกับบริบทของการสืบสวนและสอบสวนคดีอาญาในประเทศไทย คือการบัญญัติหลักการคุ้มครองข้อมูลส่วนบุคคลทั่วไปไว้ในมาตรา 131 ประมวลกฎหมายวิธีพิจารณาความอาญาด้วยการเพิ่มเติมข้อความดังต่อไปนี้ในวรรคสอง

---

[124] โปรดดู คณาธิป ทองรวีวงศ์, “มาตรการทางกฎหมายในการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวของผู้ถูกดักฟังการสื่อสารข้อมูล”, **วารสารกระบวนการยุติธรรม** 8, 1 (2556); ประพิณ ประดิษฐากร, “กฎหมายว่าด้วยการเข้าถึงและได้มาซึ่งข้อมูลของบุคคล และร่างพระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 131/2 “(2554); ปรียาชาติ หาลำเจียก, “การตรวจสอบและถ่วงดุล: ศึกษากรณีการสะกดรอยด้วยเครื่องมือสื่อสารโทรคมนาคมและเครื่องมืออิเล็กทรอนิกส์ตามพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 มาตรา 21,”; ปิติ เอี่ยมจำรูญลาภ, “กฎหมายเกี่ยวกับการกำหนดให้รัฐเข้าถึง หรือได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกัน : กรณีศึกษาประเทศสหรัฐอเมริกา.”; ศศิประภา ไผ่งาม. **ปัญหาทางกฎหมายเกี่ยวกับการคุ้มครองสิทธิและเสรีภาพส่วนบุคคลในการสืบสวนและสอบสวนคดีอาญาด้วยการใช้เทคนิคพิเศษ**. วิทยานิพนธ์ปริญญานิติศาสตรมหาบัณฑิต สาขาวิชานิติศาสตร์ บัณฑิตวิทยาลัย มหาวิทยาลัยธุรกิจบัณฑิตย์, 2552.

[125] มาตรา 32 รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560

> *“การรวบรวมหลักฐานตามวรรคหนึ่งต้องกระทำในขอบเขตที่กฎหมายกำหนด เท่าที่จำเป็นและได้สัดส่วน โดยคำนึงถึงผลกระทบต่อสิทธิส่วนบุคคล ทั้งนี้ ตามหลักเกณฑ์และวิธีการคุ้มครองข้อมูลส่วนบุคคลที่กฎกระทรวงและระเบียบกำหนด”*

กล่าวคือ เป็นการนำสารัตถะของหลักการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา มาบัญญัติในประมวลกฎหมายวิธีพิจารณาความอาญา ซึ่งเป็นบทบัญญัติหลัก จากนั้นจึงจะกำหนดรายละเอียดของหลักเกณฑ์และวิธีการคุ้มครองข้อมูลส่วนบุคคลในกฎกระทรวงที่ออกโดยรัฐมนตรีว่าการกระทรวงยุติธรรม หรือในระเบียบสำนักงานตำรวจแห่งชาติ แล้วแต่กรณี ซึ่งผู้เขียนเห็นว่าสามารถนำหลักเกณฑ์ของ LED มาเป็นแนวทางในการบัญญัติเนื้อหาได้ โดยมีข้อเสนอแนะ 4 ประการดังนี้

(1) เห็นควรให้ประเทศไทยกำหนดขอบเขตของข้อมูลส่วนบุคคลที่ได้รับความคุ้มครองในชั้นสืบสวนและสอบสวนคดีอาญาตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยไม่จำต้องบัญญัติเป็นหลักเกณฑ์ใหม่ เพื่อให้ข้อมูลส่วนบุคคลในระบบกฎหมายไทยมีความเป็นเอกภาพและสอดคล้องกับหลักการสากล อย่างไรก็ดี เพื่อไม่ให้เป็นการก้าวล่วงอำนาจอธิปไตยของรัฐอื่น จึงเห็นควรมิให้นำหลักการขยายขอบเขตเชิงพื้นที่มาใช้บังคับแก่การสืบสวนและสอบสวนคดีอาญา เพราะหลักการดังกล่าวมีผลเป็นการขยายขอบเขตการคุ้มครองข้อมูลส่วนบุคคลของเจ้าของข้อมูลที่อยู่ในประเทศไทยจากการประมวลผลข้อมูลส่วนบุคคลบางลักษณะที่เกิดขึ้นนอกราชอาณาจักรไทย

(2) เห็นควรให้ประเทศไทยกำหนดให้การสืบสวนและสอบสวนคดีอาญาอยู่ภายใต้บังคับของหลักการประมวลผลข้อมูลส่วนบุคคลทั่วไปตามแนวทางของ LED ได้ โดยกำหนดให้การสืบสวนและสอบสวนคดีอาญาต้องทำการประมวลผลโดยชอบด้วยกฎหมายและเป็นธรรม อีกนัยหนึ่งคือ มีฐานทางกฎหมายรองรับและกระทำเท่าที่จำเป็นในขอบวัตถุประสงค์[126] โดยไม่นำหลักความโปร่งใสมาบังคับใช้ เพราะการสืบสวนและสอบสวนคดีอาญาย่อมไม่สามารถเปิดเผยรายละเอียดของการสืบสวนและสอบสวนคดีอาญาได้ในทุกกรณี มิฉะนั้น การปราบปรามอาชญากรรมก็อาจไม่บรรลุผล โดยเฉพาะในกรณีที่เจ้าของข้อมูลตกเป็นผู้ต้องสงสัยหรือผู้กระทำผิด แต่เพื่อมิให้หลักประกันสิทธิในข้อมูลส่วนบุคคลถูกลดทอนเกินสมควร จึงสมควรจัดให้มีมาตรการถ่วงดุลเพิ่มเติมตามแนวทางของ LED เช่น ระบบจัดเก็บข้อมูลจราจร (Logs) ในฐานข้อมูลออนไลน์ หรือหากเป็นการสืบสวนและสอบสวนคดีอาญาโดยใช้เทคโนโลยี

---

[126] หากเปรียบเทียบกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีข้อสังเกตว่า การประมวลผลข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาจะสามารถอาศัยฐานการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะตามมาตรา 24 (4) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาได้เป็นหลัก อย่างไรก็ดี ผู้เขียนเห็นว่าในบางบริบท การใช้ความยินยอมเป็นฐานทางกฎหมายในชั้นสืบสวนและสอบสวนคดีอาญาก็มีความเหมาะสมมากกว่าได้ เช่น การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของบุคคลอื่นที่มิใช่ผู้ต้องสงสัยหรือผู้กระทำผิด แต่การอาศัยความยินยอมดังกล่าวก็ต้องภายใต้เงื่อนไขว่าเจ้าหน้าที่รัฐจะต้องปฏิบัติตามเงื่อนไขการขอความยินยอมตามหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด

สมัยใหม่ที่ซับซ้อน ก็ให้ประเมินความเสี่ยงและปรึกษาหารือกับคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลก่อนดำเนินการ เป็นต้น

(3) เห็นควรให้ประเทศไทยบัญญัติหลักเกณฑ์การใช้สิทธิของเจ้าของข้อมูลในชั้นสืบสวนและสอบสวนคดีอาญาเป็นการเฉพาะ โดยให้บัญญัติเหตุแห่งการปฏิเสธการใช้สิทธิให้ชัดเจนและกำหนดกลไกการใช้สิทธิทางอ้อมของเจ้าของข้อมูล โดยให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิร้องขอให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตรวจสอบความชอบด้วยกฎหมายของการดำเนินงานในชั้นสืบสวนและสอบสวนคดีอาญา แทนการใช้สิทธิโดยตรง

(4) เห็นควรให้ประเทศไทยกำหนดกลไกการบังคับใช้หลักการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาเป็นสองมิติ โดยในด้านหนึ่ง คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลก็ต้องกำกับดูแลการปฏิบัติตามหลักการคุ้มครองข้อมูลส่วนบุคคล โดยเฉพาะในเชิงเทคนิคหรือนโยบายที่ต้องอาศัยความรู้ความเชี่ยวชาญเฉพาะด้าน และในอีกด้านหนึ่ง ดำเนินการอื่นที่เกี่ยวข้องกับกระบวนการยุติธรรมทางอาญาโดยตรง ก็อาจให้ศาลทำหน้าที่เป็นองค์กรหลักในการตรวจสอบถ่วงดุลแทน นอกจากนี้เพื่อให้เกิดสภาพบังคับ ก็จำเป็นที่ประเทศไทยต้องบัญญัติบทกำหนดความรับผิดและโทษสำหรับการฝ่าฝืนและข้อกำหนดการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศเพิ่มเติมด้วย

กล่าวโดยสรุป หากดำเนินการตามข้อเสนอแนะข้างต้นแล้ว สิทธิในข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาจะได้รับความคุ้มครองมากยิ่งขึ้น โดยรักษาดุลยภาพระหว่างการคุ้มครองสิทธิส่วนบุคคลกับการป้องกันและปราบปรามอาชญากรรม อย่างไรก็ดี ข้อเสนอแนะที่กล่าวมานั้นเป็นเพียงแนวทางเบื้องต้นในการกำหนดเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาสำหรับประเทศไทยเท่านั้น แต่องค์ความรู้สำคัญที่ได้จากการศึกษาวิจัยนี้ คือการแสดงให้เห็นถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลจากการดำเนินงานในชั้นสืบสวนและสอบสวนคดีอาญา และพิสูจน์ให้เห็นว่า “มีความเป็นไปได้ที่ระบบกฎหมายไทยจะจัดให้มีการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา” ด้วยการบังคับใช้กฎหมายวิธีพิจารณาความอาญาควบคู่ไปกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อที่ว่าอย่างน้อยที่สุด สิทธิความเป็นส่วนตัวในข้อมูลของประชาชนชาวไทยจะยังคงมีหลักประกันในกฎหมายต่อไป