แนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา

น.ส.รติมา สุระรัตน์ชัย

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญานิติศาสตรมหาบัณฑิต
สาขาวิชานิติศาสตร์
คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2565

The guidelines of personal data protection in criminal investigation

Miss Ratima Suraratchai

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Laws in Laws

FACULTY OF LAW

Chulalongkorn University

Academic Year 2022

หัวข้อวิทยานิพนธ์	แนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา
โดย	น.ส.รติมา สุระรัตน์ชัย
สาขาวิชา	นิติศาสตร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	ศาสตราจารย์ ดร.คณพล จันทน์หอม

คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญานิติศาสตรมหาบัณฑิต

..... คณบดีคณะนิติศาสตร์
(ผู้ช่วยศาสตราจารย์ ดร.ปารีณา ศรีวนิชย์)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(ศาสตราจารย์ณรงค์ ใจหาญ)

..... อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(ศาสตราจารย์ ดร.คณพล จันทน์หอม)

..... กรรมการ
(อาจารย์ ดร.ปราโมทย์ เสริมศีลธรรม)

รติมา สุระรัตน์ชัย : แนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา. (The guidelines of personal data protection in criminal investigation) อ.ที่ปรึกษาหลัก : ศ. ดร.คณพล จันทน์หอม

วิทยานิพนธ์ฉบับนี้มีวัตถุประสงค์เพื่อวิเคราะห์ปัญหาและเสนอแนวทางในการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาในประเทศไทย สืบเนื่องจากการสืบสวนและสอบสวนคดีอาญาได้รับยกเว้นไม่ให้อยู่ภายใต้บังคับของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เว้นแต่ในส่วนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย ทำให้การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาต้องอาศัยมาตรการทางกฎหมายที่มีอยู่เดิม ซึ่งมีข้อจำกัดและมีมาตรฐานที่ไม่เทียบเท่ากับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

จากการศึกษาพบว่า บทยกเว้นมิให้การสืบสวนและสอบสวนคดีอาญาอยู่ภายใต้บังคับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นอาจเป็นการยกเว้นที่กว้างขวางเกินกว่าความจำเป็น เพราะหากมีความจำเป็น รัฐพึงกำหนดเป็นกฎเกณฑ์เฉพาะหรือข้อยกเว้นรายมาตรามากกว่าการจำกัดการคุ้มครองโดยเด็ดขาด จะเห็นได้จากกฎหมายระหว่างประเทศและกฎหมายต่างประเทศที่การสืบสวนและสอบสวนคดีอาญายังอยู่ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลควบคู่ไปกับกฎหมายวิธีพิจารณาความอาญา

ดังนั้น วิทยานิพนธ์ฉบับนี้จึงมีข้อเสนอแนะให้มีการแก้ไขปรับปรุงกฎหมายวิธีพิจารณาความอาญาของไทยให้สอดคล้องกับเกณฑ์การปกป้องสิทธิ วิทยานิพนธ์ฉบับนี้จึงมีข้อเสนอแนะให้มีการแก้ไขปรับปรุงกฎหมายวิธีพิจารณาความอาญาของไทยให้สอดคล้องกับเกณฑ์การปกป้องสิทธิควบคู่ไปกับการกำหนดให้การสืบสวนและสอบสวนคดีอาญาอยู่ภายใต้กฎเกณฑ์เฉพาะในการคุ้มครองข้อมูลส่วนบุคคล โดยยกเว้นมิให้นำหลักความโปร่งใสมาใช้บังคับแก่การสืบสวนและสอบสวนคดีอาญา พร้อมกำหนดกลไกการใช้สิทธิโดยอ้อมของเจ้าของข้อมูลส่วนบุคคล

สาขาวิชา นิติศาสตร์ ลายมือชื่อนิสิต .....

ปีการศึกษา 2565 ลายมือชื่อ อ.ที่ปรึกษาหลัก .....

6380104734 : MAJOR LAWS

KEYWORD: Privacy, Personal data protection, Criminal investigation, Personal data, the Personal Data Protection Act B.E. 2562

Ratima Suraratchai : The guidelines of personal data protection in criminal investigation. Advisor: Prof. KANAPHON CHANHOM, Ph.D.

This thesis aimed to examine issues and provide guidelines of personal data protection in a criminal investigation of Thailand. According to The Personal Data Protection Act B.E. 2562 prescribed that this Act shall not apply to a criminal investigation, except for security measures. The existing legal measures, therefore, shall be applied to protect personal data in this context, despite the fact that they have limitations and standards that are not equivalent to the Personal Data Protection Act B.E. 2562.

From the study, the researcher found that the aforementioned exemption is too broadly more than necessary. Because the state may impose specific rules or exemptions made on a case-by-case basis instead of completely restricting the protection of personal data if needed. Is supported by international law and foreign legislation, in which criminal investigation is governed by personal data protection law and criminal procedural law.

In conclusion, this thesis recommends that there should be an amendment to the Thai criminal procedural code to be aligned with the Safeguard principle and enactment of criminal investigation to be subjected to the specific rule for personal data protection by not applying the transparency principle and establishing mechanisms for the indirect exercise of personal data subjects' rights.

Field of Study: Laws Student's Signature .....

Academic Year: 2022 Advisor's Signature .....

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลงลุล่วงได้ ด้วยความอนุเคราะห์จากอาจารย์ผู้ทรงคุณวุฒิทุกท่าน โดยเฉพาะศาสตราจารย์ ดร. คณพล จันทน์หอม ซึ่งได้กรุณารับเป็นที่ปรึกษาวิทยานิพนธ์ โดยท่านได้สละเวลาตรวจสอบแก้ไขวิทยานิพนธ์ ให้คำแนะนำ ทุ่มเทเอาใจใส่ ให้กำลังใจนิสิตในที่ปรึกษาเสมอมา นอกจากนี้ ผู้วิจัยขอกราบขอบพระคุณ ศาสตราจารย์ณรงค์ ใจหาญ ประธานกรรมการสอบวิทยานิพนธ์ ที่กรุณาชี้แนะและให้ข้อเสนอแนะในการแก้ไขปรับปรุงวิทยานิพนธ์นี้ให้มีความสมบูรณ์ และอาจารย์ ดร. ปราโมทย์ เสริมศีลธรรม กรรมการสอบวิทยานิพนธ์ ที่เมตตาให้ความช่วยเหลือและให้คำแนะนำที่เป็นประโยชน์ต่อการทำวิจัยตลอดภาคการศึกษา อีกทั้ง ขอกราบขอบพระคุณ ผู้ช่วยศาสตราจารย์ ดร. นคร เสรีรักษ์ และรองศาสตราจารย์ คณาธิป ทองรวีวงศ์ ที่งานวิจัยของท่านเป็นแรงบันดาลใจให้ผู้วิจัยศึกษาและค้นคว้าในชั้นปริญญามหาบัณฑิตนี้

นอกเหนือจากอาจารย์ผู้ทรงคุณวุฒิทุกท่าน วิทยานิพนธ์ฉบับนี้ยังสำเร็จลุล่วงได้ด้วยกำลังใจจากคนรอบข้าง ไม่ว่าจะเป็นบิดา มารดา น้องชาย และนางโสรยา ผู้เป็นครอบครัวที่รักยิ่งของผู้วิจัย กัลยาณมิตรทุกท่าน ทั้งเพื่อนหอวัง เพื่อนพี่น้อง กสม. และนายอัครวินท์ ที่สนับสนุนผู้วิจัยในทุกด้าน และขอขอบคุณเพื่อนร่วมรุ่นปริญญาโท ได้แก่ นายวิรัชกฤตย์ นางสาววริศรา โดยเฉพาะนายจตุพร ที่คอยรับฟังและช่วยเหลือตลอดระยะเวลาการศึกษา ตลอดจนขอขอบพระคุณเจ้าหน้าที่และบุคคลผู้มีส่วนเกี่ยวข้องอีกหลายท่าน ซึ่งไม่อาจกล่าวนามได้ทั้งหมดในที่นี้

ผู้วิจัยหวังเป็นอย่างยิ่งว่า วิทยานิพนธ์ฉบับนี้จะทำให้องค์ความรู้เรื่องสิทธิความเป็นส่วนตัวในข้อมูลเจริญงอกงามต่อไปในประเทศไทย ซึ่งหากวิทยานิพนธ์ฉบับนี้มีคุณประโยชน์ประการใด ผู้วิจัยขอมอบความดีให้แก่บุคคลที่กล่าวมาทั้งหมด แต่หากมีข้อผิดพลาดประการใด ผู้วิจัยขอกราบอภัยและน้อมรับความผิดไว้เพียงผู้เดียว

รติมา สุระรัตน์ชัย

สารบัญ

หน้า

สารบัญตาราง

หน้า

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญของปัญหา

ปัจจุบัน ปัญหาการละเมิดข้อมูลส่วนบุคคลเป็นเรื่องที่มีการเผชิญหน้ากันอยู่สองประเด็นหลัก อันได้แก่ การใช้ประโยชน์จากข้อมูลผู้บริโภคประการหนึ่ง และการที่รัฐต้องการควบคุมประชาชนผ่านการสอดแนมอีกประการหนึ่ง[1] แต่ท่ามกลางกระแสความตื่นตัวของกฎหมายคุ้มครองข้อมูลส่วนบุคคลหลายภาคส่วนในประเทศไทยกลับให้ความสำคัญเฉพาะการคุ้มครองข้อมูลส่วนบุคคลในภาคธุรกิจ ทั้งที่ตามความเป็นจริง รัฐไทยก็เผชิญกับข้อครหาเรื่องการละเมิดความเป็นส่วนตัวในข้อมูลของประชาชนอยู่จำนวนไม่น้อย โดยเฉพาะจากการดำเนินงานในชั้นสืบสวนและสอบสวนคดีอาญา

ตัวอย่างเช่น การสอดแนมเพื่อประโยชน์ในการควบคุมกิจกรรมทางการเมือง ไม่ว่าจะเป็นการเรียกดูและถ่ายรูปบัตรประชาชนโดยไม่มีฐานทางกฎหมายที่ชัดเจน การนำหมายเลขโทรศัพท์ส่วนตัวไปติดต่อข่มขู่ การเยี่ยมบ้านและถ่ายรูปที่ตั้งของบ้าน การติดตั้งกล้องวงจรปิดหรือใช้โดรนบันทึกภาพในพื้นที่กิจกรรม การใช้เครื่องติดตามตำแหน่ง (GPS) และกรณีล่าสุด การจัดทำ “Watch list” หรือบัญชีความมั่นคง ประกอบด้วยรายชื่อบุคคลจำนวน 183 คน และบัญชีโซเชียลมีเดีย (Social media) อีก 19 บัญชี พร้อมข้อมูลวันเดือนปีเกิด เลขประจำตัวประชาชน สถานะคดี รวมถึงข้อมูลการเดินทางปรากฏอยู่ในบัญชี ซึ่งเชื่อกันว่ารัฐบาลไทยเป็นผู้จัดทำขึ้นเพื่อประโยชน์ในการเฝ้าจับตา[2] สอดคล้องกับที่ผู้ประกอบการโทรคมนาคมเคยออกมาเปิดเผยว่าหน่วยงานความมั่นคงและเจ้าหน้าที่ตำรวจของไทย

---

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

[2] โครงการอินเทอร์เน็ตเพื่อกฎหมายประชาชน (iLaw), "ย้อนดู "การเยี่ยมบ้าน" นักกิจกรรมในยุค คสช. กับคำถามถึงสถานะทางกฎหมาย" [ออนไลน์] เข้าถึงเมื่อ 20 กันยายน 2564. แหล่งที่มา: https://freedom.ilaw.or.th/node/710?fbclid=IwAR1HHjIRR5QEBC; โครงการอินเทอร์เน็ตเพื่อกฎหมายประชาชน (iLaw), "บันทึกการคุกคามนักกิจกรรม นักเคลื่อนไหว ก่อนเวทีรับฟังความคิดเห็นสร้างนิคมอุตสาหกรรมจะนะ" [ออนไลน์] เข้าถึงเมื่อ 20 กันยายน. แหล่งที่มา: https://freedom.ilaw.or.th/node/831; โครงการอินเทอร์เน็ตเพื่อกฎหมายประชาชน (iLaw), "แกะรอยการสร้างความกลัว: สรุปการคุกคามเยาวชน-แกนนำจัดชุมนุม ก.ค.-ส.ค.63" [ออนไลน์] เข้าถึงเมื่อ 2564, 20 กันยายน. แหล่งที่มา: https://freedom.ilaw.or.th/node/842 ; มติชนออนไลน์, "'ก้าวไกล-ก้าวหน้า' ฉะ watch list สุดอัปยศ ตีตรา ปชช.เป็นศัตรู" [ออนไลน์] เข้าถึงเมื่อ 2564, 20 กันยายน. แหล่งที่มา: www.matichon.co.th/politics/news_2876820

มีการติดต่อขอข้อมูลส่วนตัวของผู้ใช้บริการโทรศัพท์อยู่บ่อยครั้ง ทั้งเพื่อติดตามบุคคล ตรวจสอบผู้ที่บุคคลเป้าหมายติดต่อสื่อสาร หรือกระทั่งลอบดักฟังโทรศัพท์[3] เป็นต้น

ยิ่งไปกว่านั้น มีนักสิทธิมนุษยชนจำนวนไม่น้อยที่วิพากษ์วิจารณ์ถึงปฏิบัติการบังคับตรวจสุ่มสารพันธุกรรม (DNA) และมาตรการสองแชะที่เก็บข้อมูลอัตลักษณ์ใบหน้าบุคคลผ่านการลงทะเบียนซิมการ์ดโทรศัพท์ในพื้นที่จังหวัดชายแดนภาคใต้ของประเทศไทย เนื่องจากข้อมูลสารพันธุกรรมและอัตลักษณ์บนใบหน้าของบุคคลเป็นข้อมูลชีวมิติที่มีความอ่อนไหวเป็นพิเศษตามหลักสากล แต่รัฐไทยกลับใช้ปฏิบัติการจัดเก็บข้อมูลเหล่านี้อย่างเหมารวม และเพ่งเล็งไปที่กลุ่มมลายูมุสลิม โดยไม่ปรากฏว่าเจ้าหน้าที่ของรัฐมีการขอความยินยอมหรือมีการแจ้งข้อกล่าวหาตามกฎหมายแต่อย่างใด ปฏิบัติการในพื้นที่จังหวัดชายแดนใต้นี้จึงสุ่มเสี่ยงที่จะเป็นการละเมิดสิทธิมนุษยชน และยังอาจถูกมองว่าเป็นการเลือกปฏิบัติต่อกลุ่มชนด้วยเหตุผลทางเชื้อชาติ[4]

นอกเหนือจากการสอดแนมข้อมูลส่วนบุคคล ปัญหาการละเมิดข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาในรูปแบบอื่น ๆ ก็ยังคงปรากฏขึ้นในสังคมไทยอยู่เป็นระยะ เช่น การแถลงข่าวโดยเปิดเผยข้อมูลส่วนตัวและรูปถ่ายของผู้ต้องหาหรือผู้เสียหาย การเก็บรักษาข้อมูลทะเบียนประวัติอาชญากรถาวรโดยไม่มีกำหนดทำลาย ทั้งละเลยไม่ทำให้ข้อมูลถูกต้องเป็นปัจจุบัน ซ้ำร้าย ยังมีกรณีที่เจ้าหน้าที่ตำรวจใช้ระบบสืบค้นข้อมูลราชการเพื่อรับจ้างตรวจทะเบียนราษฎรอีกด้วย[5] ดังนั้น จะเห็นได้ว่าปัญหาการละเมิดข้อมูลส่วนบุคคลในสังคมไทยไม่ได้เกิดขึ้นเฉพาะในส่วนของภาคธุรกิจ แต่สามารถเป็นผลจากการดำเนินงานของภาครัฐได้เช่นเดียวกัน

ทั้งนี้ มีข้อสังเกตว่าปัญหาการละเมิดข้อมูลส่วนบุคคลโดยภาครัฐนี้มักจะเกิดขึ้นภายใต้ข้ออ้างเกี่ยวกับความมั่นคงหรือการรักษาความสงบเรียบร้อย โดยเฉพาะประเด็นการป้องกันและปราบปราม

---

[3] นคร เสรีรักษ์, ความเป็นส่วนตัว: ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย, พิมพ์ครั้งที่ 2 (แพร่: พี.เพรส,, 2563), หน้า 339-342.

[4] ประชาไท, "มูลนิธิผสานวัฒนธรรมเปิดสถิติ 'ปิดล้อมบังคับ-ข่มขู่เก็บ DNA' ชายแดนใต้" [ออนไลน์] เข้าถึงเมื่อ 19 กันยายน 2564. แหล่งที่มา: https://prachatai.com/journal/2019/12/85538; สาวออฟฟิศ (Nisit Recorder), "มูลนิธิผสานวัฒนธรรม, “จังหวัดชายแดนใต้: ห้องทดลอง Bio-metric ของรัฐไทย" [ออนไลน์] เข้าถึงเมื่อ 19 กันยายน 2564. แหล่งที่มา: https://crcfthailand.org/2020/09/06/จังหวัดชายแดนใต้-ห้องท/

[5] กรศุทธิ์ ขอพ่วงกลาง และวัฒนกร อุทัยวิวัฒน์กุล, "สรุปสาระสำคัญจากเสวนาวิชาการ หัวข้อ "ลบประวัติ ล้างความผิด คืนชีวิตด้วยสิทธิตามกฎหมาย"" [ออนไลน์] เข้าถึงเมื่อ 23 กันยายน. แหล่งที่มา: https://www.law.tu.ac.th/seminar-summary-deletion-of-criminal-records/ ; สปริงนิวส์, "ถึงเป็นตำรวจทำผิดก็ต้องโดนจับ ! รวบสารวัตรเปิดเพจรับจ้างเช็คทะเบียนราษฎร์" [ออนไลน์] เข้าถึงเมื่อ 24 กันยายน. แหล่งที่มา: https://www.springnews.co.th/news/397608

อาชญากรรม ส่งผลให้การสืบสวนและสอบสวนคดีอาญาในประเทศไทยมีส่วนเกี่ยวข้องกับปัญหาการละเมิดความเป็นส่วนตัวในข้อมูลของบุคคลอยู่เรื่อยมา[6]

อย่างไรก็ตาม หากพิจารณาถึงบทบัญญัติกฎหมายที่เกี่ยวข้อง จะพบว่าในระบบกฎหมายไทย เจ้าพนักงานของรัฐมีอำนาจดุลพินิจค่อนข้างกว้างในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา แต่ถึงกระนั้น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งเป็นกฎหมายกลางว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลฉบับแรกในประเทศไทย กลับยกเว้นมิให้นำพระราชบัญญัตินี้ไปใช้บังคับแก่การสืบสวนและสอบสวนคดีอาญา เพียงแต่กำหนดให้ต้องมีการรักษาความมั่นคงปลอดภัยให้เป็นไปตามมาตรฐานเท่านั้น ประกอบกับพระราชบัญญัติดังกล่าวเปิดช่องให้ภาคเอกชนอาจเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล เพื่อส่งต่อให้ภาครัฐได้ โดยไม่ต้องอาศัยความยินยอมของเจ้าของข้อมูลส่วนบุคคล ในกรณีที่เป็นการปฏิบัติหน้าที่ตามกฎหมายของเอกชนนั้น[7] ด้วยเหตุนี้ สิทธิในข้อมูลส่วนบุคคลของประชาชนชาวไทยจึงอาจไม่ได้รับความคุ้มครองอย่างเหมาะสมเพียงพอ เมื่อเผชิญกับการดำเนินงานในชั้นสืบสวนและสอบสวนคดีอาญา

สภาพปัญหาดังกล่าวไม่เพียงส่งผลกระทบต่อสิทธิความเป็นส่วนตัวในข้อมูลของบุคคล แต่ยังอาจกระทบในแง่ความสัมพันธ์ระหว่างประเทศอีกด้วย เนื่องจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลในหลายประเทศมีข้อกำหนดการโอนข้อมูลระหว่างประเทศ โดยห้ามมิให้ส่งหรือโอนข้อมูลไปยังประเทศปลายทางที่ไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ[8] ซึ่งการพิจารณามาตรฐานดังกล่าวจะเป็นการพิจารณาสภาพแวดล้อมทางกฎหมายในภาพรวม คือประเมินความสอดคล้องของบทบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคล ไปจนถึงกลไกการคุ้มครองข้อมูลส่วนบุคคลจากการแทรกแซงโดยหน่วยงานภาครัฐ ดังนั้น ข้อเท็จจริงของการมีอยู่ของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยจึงไม่เพียงพอที่จะถือว่าประเทศไทยมีระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ[9] อันอาจกระทบต่อการค้าและความร่วมมือทางอาญาระหว่างประเทศ เพราะประเทศไทยไม่อาจแลกเปลี่ยนถ่ายโอนข้อมูลระหว่างประเทศได้อย่างเสรี

---

[6] นคร เสรีรักษ์, ความเป็นส่วนตัว: ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย, หน้า; สาวตรี สุขศรี, กฎหมายว่าด้วยอาชญากรรมคอมพิวเตอร์และอาชญากรรมไซเบอร์ (กรุงเทพฯ: โครงการตำราและเอกสารประกอบการสอน คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2563), หน้า.

[7] อนุสิษฐ คุณากร และคณะ, การคุ้มครองข้อมูลส่วนบุคคลกับสังคมไทย (กรุงเทพฯ: สถาบันนโยบายการศึกษา ภายใต้มูลนิธิส่งเสริมนโยบายการศึกษา, 2563), หน้า 46-47.

[8] คณาธิป ทองรวีวงศ์, คำอธิบาย หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล, พิมพ์ครั้งที่ 2 (กรุงเทพฯ: นิติธรรม, 2565), หน้า 536-537.

[9] คณาธิป ทองรวีวงศ์, "การปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน,"(2560).

ฉะนั้น จึงมีความจำเป็นที่ประเทศไทยต้องพัฒนาแนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา โดยศึกษาแนวทางกฎหมายระหว่างประเทศและกฎหมายต่างประเทศที่มีพัฒนาการด้านการคุ้มครองข้อมูลส่วนบุคคลก้าวหน้ากว่าประเทศไทย อันเป็นโอกาสอันดีที่จะเพิ่มความเชื่อมั่นในกระบวนการยุติธรรมทางอาญาของประเทศไทยต่อไป

1.2 วัตถุประสงค์การวิจัย

1. เพื่อให้คนในสังคมไทยตระหนักถึงความจำเป็นของการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา ในฐานะหลักประกันสิทธิส่วนบุคคลขั้นพื้นฐาน
2. เพื่อวิเคราะห์แนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาตามกฎหมายไทย โดยศึกษาเปรียบเทียบกับกฎหมายระหว่างประเทศและกฎหมายต่างประเทศ
3. เพื่อเสนอแนะแนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาที่มีความเหมาะสมกับลักษณะกระบวนการยุติธรรมทางอาญาไทย

1.3 สมมุติฐานการวิจัย

แม้การสืบสวนและสอบสวนคดีอาญามีความจำเป็นที่จะต้องเก็บรวบรวมและใช้ประโยชน์จากข้อมูลส่วนบุคคลเป็นจำนวนมาก แต่ประเทศไทยกลับไม่มีมาตรการทางกฎหมายที่เหมาะสมเพียงพอในการคุ้มครองข้อมูลส่วนบุคคลในกระบวนการดังกล่าว จนเป็นเหตุให้ความเป็นส่วนตัวของประชาชนถูกล่วงละเมิดเกินกว่าที่จำเป็นอยู่หลายกรณี จึงสมควรกำหนดแนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาเป็นการเฉพาะ โดยกำหนดเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลให้ยืดหยุ่นกว่ากรณีทั่วไป กำหนดข้อจำกัดสิทธิของเจ้าของข้อมูลขึ้นใหม่ และให้องค์กรอิสระมีบทบาทตรวจสอบกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาเพิ่มเติมต่อไป

1.4 ขอบเขตการศึกษา

วิจัยฉบับนี้เป็นการศึกษาวิจัยทางนิติศาสตร์ ซึ่งมุ่งศึกษาแนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนตามกฎหมายไทย กฎหมายระหว่างประเทศ คือ Directive (EU) 2016/680 (LED) ของสหภาพยุโรป ตลอดจนกฎหมายต่างประเทศ ได้แก่ สหราชอาณาจักร สหรัฐอเมริกา และสาธารณรัฐเกาหลี โดยจำกัดขอบเขตการศึกษาเฉพาะแนวทางการคุ้มครองข้อมูลส่วนบุคคลที่มีลักษณะเป็นหลักเกณฑ์กลางทั่วไป มิได้ทำการศึกษาในรูปแบบเฉพาะเจาะจงเป็นรายกิจกรรม

1.5 ระเบียบวิธีวิจัย

วิจัยฉบับนี้เป็นการศึกษาวิจัยทางเอกสาร (Document research) โดยค้นคว้าและรวบรวมข้อมูลหลักกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาจากแหล่งข้อมูลทั้งภายในประเทศไทยและต่างประเทศ มาวิเคราะห์เปรียบเทียบเพื่อนำมาสู่ข้อสรุปและข้อเสนอแนะต่อไป

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1. ทำให้ทราบถึงทฤษฎี แนวคิด และหลักการที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา ตลอดจนตระหนักถึงความจำเป็นที่รัฐจะต้องให้การคุ้มครองข้อมูลส่วนบุคคลในกระบวนการยุติธรรมทางอาญา ซึ่งเป็นเรื่องใหม่ในสังคมไทย
2. ทำให้สามารถประเมินความเหมาะสมของแนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาในประเทศไทยและต่างประเทศได้
3. ทำให้เกิดการพัฒนาแนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาเป็นการทั่วไป ซึ่งไม่เพียงแต่เป็นสร้างหลักประกันสิทธิและเสรีภาพของประชาชน แต่ยังมีผลเป็นการลดอุปสรรคการแลกเปลี่ยนข้อมูลในมิติความสัมพันธ์ระหว่างประเทศอีกด้วย
4. ทำให้อาจต่อยอดแนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาได้ กล่าวคือ ใช้เป็นฐานในการกำหนดแนวทางการคุ้มครองข้อมูลส่วนบุคคลที่เฉพาะเจาะจงเป็นรายกิจกรรม หรือต่อยอดไปถึงขั้นตอนการดำเนินงานอื่น ๆ ในกระบวนการยุติธรรมอาญาได้เช่นกัน ซึ่งจะช่วยเพิ่มความเป็นไปได้ที่การสืบสวนสอบสวนคดีอาญาของประเทศไทยอาจนำเทคโนโลยีสมัยใหม่มาใช้ โดยไม่ลดความเชื่อมั่นที่มีต่อกระบวนการยุติธรรม

1.7 ทบทวนวรรณกรรม

ตามที่ผู้เขียนได้ศึกษาค้นคว้าและสำรวจการศึกษาวิจัยเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาของประเทศไทยในเบื้องต้น พบว่ามีการศึกษาวิจัยที่เกี่ยวข้องอยู่ไม่มากนัก และไม่ปรากฏการวิจัยที่มุ่งศึกษาแนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาอย่างเฉพาะเจาะจงแต่ประการใด

สำหรับการศึกษาวิจัยเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล พบว่าปี พ.ศ. 2548 ปรากฏงานวิจัยของผู้ช่วยศาสตราจารย์ ดร. นคร เสรีรักษ์ เรื่อง การคุ้มครองข้อมูลส่วนบุคคล: ข้อเสนอเพื่อ

การพัฒนาสิทธิรับรู้ข้อมูลข่าวสารในกระบวนการธรรมรัฐไทย โดยผู้ช่วยศาสตราจารย์ ดร. นคร เสรีรักษ์ ได้ศึกษาสภาพข้อเท็จจริงของการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย ก่อนที่จะตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พร้อมกับศึกษาแนวทางการคุ้มครองข้อมูลส่วนบุคคลและปัญหาทางปฏิบัติจากประเทศที่มีพัฒนาการด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคลมาก่อนประเทศไทย

ผลการวิจัยของผู้ช่วยศาสตราจารย์ ดร. นคร เสรีรักษ์ ชี้ให้ถึงความไม่เพียงพอของการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย เนื่องจากความตระหนักรู้เรื่องข้อมูลส่วนบุคคลของสังคมไทยยังมีอยู่น้อยมาก ทำให้ประเทศไทยประสบปัญหาการละเมิดข้อมูลส่วนบุคคลเรื่อยมา โดยเฉพาะจากภาครัฐซ้ำร้าย พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ที่มีขอบเขตการคุ้มครองเฉพาะข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานรัฐก็ไม่อาจคุ้มครองข้อมูลส่วนบุคคลได้อย่างเหมาะสม เพราะองค์กรกำกับดูแลตามกฎหมายก็ยังคงมีปัญหาเรื่องความเป็นอิสระและประสิทธิภาพในการปฏิบัติงาน ผู้ช่วยศาสตราจารย์ ดร. นคร เสรีรักษ์ จึงเสนอให้มีการตรากฎหมายเฉพาะในการคุ้มครองข้อมูลส่วนบุคคล สร้างความตระหนักรู้ให้แก่สังคมทุกฝ่าย และให้มีองค์กรอิสระมากำกับดูแลการคุ้มครองความเป็นส่วนตัว

ต่อมา ปรากฏงานวิจัยในปี พ.ศ. 2549 ของผู้ช่วยศาสตราจารย์ กิตติพงศ์ กมลธรรมวงศ์ เรื่อง การคุ้มครองข้อมูลข่าวสารส่วนบุคคลในระบบกฎหมายไทย : ปัญหาและแนวทางแก้ไข ซึ่งเป็นการศึกษาเปรียบเทียบการคุ้มครองข้อมูลส่วนบุคคลในระบบกฎหมายไทยกับข้อตกลงระหว่างประเทศ ตลอดจนกฎหมายต่างประเทศ ซึ่งผลจากการศึกษาพบว่าภาพรวมของการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยมีปัญหาสำคัญอยู่สามประการ ดังนี้

1. บทบัญญัติรัฐธรรมนูญยังขาดกฎหมายคุ้มครองข้อมูลส่วนบุคคลในภาคเอกชน
2. ระบบกฎหมายประเทศไทยยังคงมีข้อจำกัดในการตีความเพื่อขยายความคุ้มครองข้อมูลส่วนบุคคลที่ถูกนำไปใช้ประโยชน์ในลักษณะอื่นจากความก้าวหน้าของเทคโนโลยี
3. หน่วยงานของรัฐมีอำนาจกว้างขวางในการจัดเก็บข้อมูลส่วนบุคคลโดยมีกฎหมายน้อยฉบับที่บัญญัติถึงข้อห้ามในการจัดเก็บและกำหนดหลักเกณฑ์ที่เป็นมาตรฐานเดียวกัน

ในการวิเคราะห์ปัญหาประการที่สาม ผู้ช่วยศาสตราจารย์ กิตติพงศ์ กมลธรรมวงศ์ ได้กล่าวถึงกลุ่มกฎหมายพิเศษที่รัฐมีอำนาจแทรกแซงข้อมูลส่วนบุคคล ซึ่งจะปรากฏอยู่ในรูปแบบการสืบสวนและสอบสวนคดีอาญาอีกด้วย ไม่ว่าจะเป็นพระราชบัญญัติป้องกันและปราบปรามยาเสพติด พ.ศ. 2519 พระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ. 2528 พระราชบัญญัติคุ้มครองพยานในคดีอาญา พ.ศ. 2546 พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 และพระราชกำหนดบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ. 2548

การศึกษาวิจัยของผู้ช่วยศาสตราจารย์ ดร. นคร เสรีรักษ์ และผู้ช่วยศาสตราจารย์ กิตติพงศ์ กมลธรรมวงศ์ จึงสะท้อนถึงปัญหาการคุ้มครองข้อมูลส่วนบุคคลในระบบกฎหมายไทย โดยได้ชูประเด็นเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลจากการใช้อำนาจรัฐอีกด้วย แต่นอกเหนือไปจากงานวิจัยทั้งสองฉบับข้างต้น การศึกษาวิจัยอื่น ๆ ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยก็จะเป็นการศึกษาวิเคราะห์ปัญหาการบังคับใช้พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 หรือเป็นการวิจัยเพื่อเสนอแนะแนวทางในการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... ซึ่งขณะนั้นยังไม่ได้มีการประกาศใช้ และเมื่อมีการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การวิจัยเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลก็จะเป็นการศึกษาปัญหาการคุ้มครองข้อมูลส่วนบุคคลภายใต้พระราชบัญญัติดังกล่าวในภาพรวมและเฉพาะเรื่องเฉพาะกรณี แต่ก็ยังไม่ปรากฏว่ามีการวิจัยที่ศึกษาแนวทางในการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาโดยตรง

ในส่วนของการศึกษาวิจัยในด้านกฎหมายอาญาและกระบวนการยุติธรรมทางอาญา แม้จะมีงานวิจัยอยู่จำนวนหนึ่งที่มุ่งศึกษากรอบการใช้อำนาจในชั้นสืบสวนและสอบสวนคดีอาญาเพื่อคุ้มครองสิทธิส่วนบุคคล แต่การศึกษาดังกล่าวก็มิได้มุ่งที่จะศึกษาถึงหลักเกณฑ์ทั่วไปว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ฉะนั้น ข้อเสนอแนะจากการศึกษาวิจัยโดยส่วนใหญ่จึงเป็นเรื่องของการกำหนดหลักเกณฑ์การใช้อำนาจสืบสวนและสอบสวนภายใต้บทบัญญัติเฉพาะเรื่องเฉพาะกรณีไป

ตัวอย่างเช่น งานวิจัยปี พ.ศ. 2549 ของนารี กิตติสมบูรณ์สุข เรื่อง การแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลจากข้อมูลอิเล็กทรอนิกส์ในอาชญากรรมคอมพิวเตอร์ ซึ่งผลจากการศึกษาวิจัยนารี กิตติสมบูรณ์สุข เสนอแนะให้มีการตราบทบัญญัติกฎหมายขึ้นใหม่ หรือแก้ไขปรับปรุงบทบัญญัติที่มีอยู่เดิมให้รองรับการแสวงหาพยานหลักฐานข้อมูลอิเล็กทรอนิกส์ เพื่อลดอุปสรรคในการดำเนินคดีของเจ้าหน้าที่รัฐ ทั้งนี้ อาจเป็นเพราะในขณะที่นารี กิตติสมบูรณ์สุขศึกษาวิจัย พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 ก็ยังไม่ได้มีการประกาศใช้เป็นกฎหมาย

อย่างไรก็ตาม จะเห็นได้ว่าข้อเสนอแนะในการคุ้มครองข้อมูลส่วนบุคคลของนารี กิตติสมบูรณ์จะมีลักษณะเป็นการตราบทบัญญัติเฉพาะเรื่องมาเป็นกรอบการใช้อำนาจของเจ้าหน้าที่รัฐเป็นรายกรณี มิใช่บทบัญญัติทั่วไปในการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา ดังที่ผู้เขียนจะได้นำเสนอในวิจัยฉบับนี้ต่อไป

บทที่ 2
แนวคิด หลักการ และทฤษฎีที่เกี่ยวข้องกับ การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา

เพื่อประโยชน์ในการติดตามจับกุมผู้กระทำผิดมาดำเนินคดี กฎหมายจึงให้อำนาจเจ้าพนักงานสืบสวนสอบสวนในการแสวงหาข้อเท็จจริงและรวบรวมพยานหลักฐาน แต่อีกด้านหนึ่ง ก็ไม่อาจปฏิเสธได้ว่าการใช้อำนาจดังกล่าวย่อมมีผลกระทบต่อสิทธิและเสรีภาพของประชาชน ดังนั้น การสืบสวนและสอบสวนจึงต้องเป็นไปตามกรอบที่กฎหมายบัญญัติ บนพื้นฐานหลักความได้สัดส่วน เพื่อป้องกันไม่ให้สิทธิและเสรีภาพของประชาชนถูกล่วงละเมิดเกินกว่าที่จำเป็น[10]

อย่างไรก็ดี ในบรรดาสิทธิและเสรีภาพที่ได้รับความคุ้มครองในชั้นนี้ สิทธิในข้อมูลส่วนบุคคลกลับไม่ได้รับความสนใจมากนักเมื่อเปรียบเทียบกับสิทธิและเสรีภาพประเภทอื่น หรือหากมีการกล่าวถึงก็จะเป็นในลักษณะการวิพากษ์วิจารณ์มาตรการสืบสวนสอบสวนเป็นรายกรณีไปมากกว่าที่จะเสนอให้มีการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนเป็นการทั่วไป ซึ่งอาจเป็นเพราะวัตถุประสงค์ของการสืบสวนและสอบสวนคือการค้นหาความจริงในคดีอาญา การสืบสวนและสอบสวนจึงเลี่ยงไม่ได้ที่จะต้องเก็บรวบรวม ใช้ และเปิดเผยข้อมูลของผู้มีส่วนเกี่ยวข้องเป็นจำนวนมาก ไม่ว่าจะเป็นผู้ต้องหา จำเลย ผู้เสียหาย หรือพยาน หลายภาคส่วนจึงเกรงว่าหากนำหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลมาใช้บังคับ ก็อาจมีผลเป็นการขัดขวางการป้องกันและปราบปรามอาชญากรรม

ในมุมมองของผู้เขียน ผู้เขียนเห็นว่าความเข้าใจข้างต้นนี้อาจเป็นความเข้าใจที่คลาดเคลื่อนไป เนื่องจากกระบวนการยุติธรรมอาญาที่ดีพึงรักษาสมดุลระหว่างการใช้อำนาจรัฐในการนำตัวผู้กระทำผิดมาลงโทษกับหลักประกันสิทธิและเสรีภาพของประชาชน โดยไม่โน้มเอียงไปทางใดทางหนึ่งจนเกินไป[11] ฉะนั้น แม้มีความจำเป็นที่การสืบสวนและสอบสวนต้องล่วงละเมิดข้อมูลส่วนบุคคล แต่ในขณะเดียวกันบทบัญญัติกฎหมายก็จำเป็นที่จะต้องจำกัดขอบเขตการสืบสวนและสอบสวนมิให้กระทบกระเทือนต่อสิทธิในข้อมูลส่วนบุคคลจนไม่ได้สัดส่วน เพราะสิทธิในข้อมูลส่วนบุคคลก็ถือเป็นสิทธิขั้นพื้นฐานที่ได้รับการรับรองตามรัฐธรรมนูญเช่นเดียวกันกับสิทธิและเสรีภาพประเภทอื่น การคุ้มครองข้อมูลส่วนบุคคล

---

[10] ณรงค์ ใจหาญ, หลักกฎหมายวิธีพิจารณาความอาญา เล่ม 1, พิมพ์ครั้งที่ 14 (กรุงเทพฯ: วิญญูชน, 2565), หน้า 19; ปกป้อง ศรีสนิท, สิทธิมนุษยชนในกระบวนการยุติธรรมทางอาญา (กรุงเทพฯ: วิญญูชน, 2563), หน้า 117-118.

[11] เกียรติขจร วัจนะสวัสดิ์, คำอธิบาย หลักกฎหมายวิธีพิจารณาความอาญา ว่าด้วย การดำเนินคดีในขั้นตอนก่อนการพิจารณา, พิมพ์ครั้งที่ 7 (กรุงเทพฯ: หจก. สำนักพิมพ์ พลสยาม พริ้นติ้ง, 2558), หน้า 1-2.

จึงไม่ได้เป็นปฏิปักษ์ต่อการสืบสวนและสอบสวนโดยสิ้นเชิง แต่เป็นสิ่งที่เข้ามาช่วยเสริมเพื่อให้เกิดความเป็นธรรมในกระบวนการสืบสวนและสอบสวนคดีอาญามากยิ่งขึ้น

เพื่อยืนยันทรรศนะข้างต้น ผู้เขียนจึงได้รวบรวมแนวคิด หลักการ รวมถึงทฤษฎีที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลและการสืบสวนสอบสวนคดีอาญามานำเสนอในบทนี้ เพื่อนำไปสู่บทสรุปว่าท้ายที่สุด แนวคิดทั้งสองอาจสอดประสานกันหรือไม่ อย่างไร โดยมีรายละเอียดดังนี้

2.1 การคุ้มครองข้อมูลส่วนบุคคล

ความเป็นมนุษย์ของบุคคลหนึ่ง ๆ ย่อมประกอบไปด้วยข้อมูลจำนวนมาก ไม่ว่าจะเป็นชื่อสกุล อายุ เพศ รูปพรรณ ความเชื่อ รสนิยม ตลอดจนวิถีชีวิต ซึ่งอาจเรียกโดยรวมได้ว่า “ข้อมูลส่วนบุคคล” เนื่องจากข้อมูลเหล่านี้เป็นสิ่งผูกพันและยืนยันความเป็นมนุษย์ของบุคคลหนึ่งที่แตกต่างจากบุคคลอื่น หรืออีกนัยหนึ่งคือเป็นเครื่องบ่งชี้ถึงตัวตนของบุคคล ข้อมูลส่วนบุคคลจึงถูกมองว่าเป็นเอกสิทธิ์ส่วนตัวของเจ้าของข้อมูลโดยแท้[12] การก้าวล่วงข้อมูลส่วนบุคคลโดยปราศจากความยินยอมหรือเหตุอันสมควรจึงเป็นเรื่องที่ไม่อาจยอมรับได้ เพราะเป็นการละเมิดเอกสิทธิ์ส่วนตัวของบุคคล

ทว่าในสถานการณ์ที่เทคโนโลยีเข้ามาเกี่ยวข้อง บทบัญญัติกฎหมายรูปแบบดั้งเดิมก็ไม่อาจให้ความคุ้มครองข้อมูลส่วนบุคคลได้อย่างเหมาะสมเพียงพอ เนื่องจากเทคโนโลยีสมัยใหม่สามารถเข้าถึงและเผยแพร่ข้อมูลต่าง ๆ ได้อย่างรวดเร็วโดยไร้พรมแดน กฎหมายคุ้มครองข้อมูลส่วนบุคคลจึงเกิดขึ้นโดยมีกฎหมายระดับมลรัฐของรัฐเฮสเซน (Hessen) ประเทศสหพันธ์สาธารณรัฐเยอรมนี เป็นกฎหมายฉบับแรกของโลก และต่อมา ประเทศสวีเดนก็ได้ตรา Data Protection Act ซึ่งเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลระดับประเทศในปี ค.ศ. 1973 จากนั้น กฎหมายคุ้มครองข้อมูลส่วนบุคคลจึงแพร่หลายทั่วภาคพื้นยุโรป ไปจนถึงระดับความร่วมมือระหว่างประเทศ ตั้งแต่สหประชาชาติ (United Nations) องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (Organization for Economic Co-operation and Development: “OECD”) สหภาพยุโรป (European Union: “EU”) ไปจนถึงความร่วมมือทางเศรษฐกิจเอเชีย-แปซิฟิก (Asia-Pacific Economic Cooperation: “APEC”) ต่างก็กำหนดมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้เกิดความแน่นอนในการถ่ายโอนข้อมูลระหว่างประเทศ[13] ทำให้กฎหมายคุ้มครองข้อมูลส่วนบุคคลหลายประเทศมีรากฐานจากมาตรฐานเหล่านี้ รวมถึงประเทศไทย

---

[12] นคร เสรีรักษ์, ความเป็นส่วนตัว: ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย, หน้า 61-103.

[13] เรื่องเดียวกัน, หน้า 145-147.

สำหรับประเทศไทย แนวคิดว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลแต่เดิมจะได้รับอิทธิพลจากมาตรฐานของ OECD แต่ต่อมา พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ถูกยกร่างขึ้นโดยมีกฎหมายของสหภาพยุโรป ได้แก่ REGULATION (EU) 2016/679 (General Data Protection Regulation: "GDPR")[14] เป็นต้นแบบ ซึ่งอาจเป็นเพราะ GDPR มีการขยายขอบเขตการบังคับใช้ไปถึงนอกสหภาพยุโรป ในกรณีที่มีการประมวลผลข้อมูลส่วนบุคคลของพลเมืองยุโรปตามที่กฎหมายกำหนด ประกอบกับ GDPR มีข้อกำหนดให้การโอนข้อมูลไปต่างประเทศจะกระทำได้ต่อเมื่อประเทศปลายทางมีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอเท่านั้น และเมื่อโทษสูงสุดของการฝ่าฝืน GDPR คือการปรับเป็นจำนวนเงินสูงถึง 20 ล้านยูโร หรือจำนวนเงินร้อยละ 2-4 ของรายได้ต่อปีทั่วโลก ขึ้นอยู่กับว่าจำนวนใดจะสูงกว่า ประเทศไทยจึงเลี่ยงไม่ได้ที่จะต้องพัฒนากฎหมายคุ้มครองข้อมูลส่วนบุคคลภายในให้สอดคล้องกับมาตรฐานของ GDPR[15]

ด้วยเหตุนี้ การศึกษาแนวคิด หลักการ และทฤษฎีที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลในหัวข้อที่ 2.1 จึงเป็นการอ้างอิงตามมาตรฐานของ OECD และสหภาพยุโรปเป็นสำคัญ เพราะทั้งสองแนวทางต่างมีอิทธิพลต่อข้อความคิดว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย อีกทั้งยังเป็นมาตรฐานขั้นต่ำที่ได้รับการยอมรับจากนานาประเทศทั่วโลก โดยจะเริ่มต้นทำการศึกษาความหมายของข้อมูลส่วนบุคคล ก่อนจะศึกษาแนวคิดและหลักการพื้นฐานในการคุ้มครองข้อมูลส่วนบุคคลต่อไป

2.1.1 ความหมายของข้อมูลส่วนบุคคล

ในเบื้องต้น จำเป็นต้องทำความเข้าใจเสียก่อนว่าข้อมูลใดถือเป็น "ข้อมูลส่วนบุคคล" ที่ได้รับความคุ้มครองตามกฎหมาย โดยนิยามคำว่าข้อมูลส่วนบุคคลนั้นอาจมีความแตกต่างกันในรายละเอียดตามแต่กฎหมายแต่ละฉบับ ดังนี้

OECD นิยามข้อมูลส่วนบุคคล (Personal data) ว่าหมายความถึงข้อมูลใด ๆ เกี่ยวกับบุคคลซึ่งระบุหรือทำให้สามารถระบุถึงเจ้าของข้อมูลได้[16]

---

[14] 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).

[15] อนุสิษฐ คุณากร และคณะ, การคุ้มครองข้อมูลส่วนบุคคลกับสังคมไทย, หน้า 11-22.

[16] The OECD Privacy Framework 2013, at 1 Definition. ""Personal data" means any information relating to an identified or identifiable individual (data subject)."

ในทำนองเดียวกัน กฎหมายของสหภาพยุโรปก็ได้ให้ความหมายของข้อมูลส่วนบุคคลเอาไว้ว่า หมายถึงข้อมูลใด ๆ เกี่ยวกับบุคคล ซึ่งระบุหรือทำให้สามารถระบุถึงบุคคลธรรมดาผู้เป็นเจ้าของข้อมูล ไม่ว่าจะโดยตรงหรือโดยอ้อมก็ตาม โดยเฉพาะอย่างยิ่ง ด้วยการอ้างอิงจากสิ่งระบุอัตลักษณ์โดยเฉพาะ เช่น ชื่อ เลขประจำตัว ตำแหน่งที่อยู่ สิ่งระบุอัตลักษณ์ออนไลน์ หรือปัจจัยซึ่งเจาะจงถึงอัตลักษณ์ทางกายภาพ สรีรวิทยา พันธุกรรม จิตใจ เศรษฐกิจ วัฒนธรรม หรือสังคมของบุคคล[17]

ดังนั้น นิยามของข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปจึงอาจอธิบายแยกได้เป็นองค์ประกอบสี่ประการด้วยกัน[18] ได้แก่

1.) ข้อมูลใด ๆ (Any information)
เป็นคำที่มีความเป็นกลาง จึงสามารถตีความได้อย่างกว้าง ครอบคลุมทั้งข้อมูลที่เป็นรูปธรรมและนามธรรม โดยไม่จำกัดรูปแบบและไม่คำนึงว่าเป็นความจริงแท้หรือไม่
2.) เกี่ยวกับบุคคล (Relating to)
อาจเป็นความเกี่ยวข้องในแง่เนื้อหา วัตถุประสงค์ในการประมวลผล หรือผลกระทบที่มีต่อบุคคลผู้เป็นเจ้าของข้อมูลก็ได้
3.) ซึ่งระบุหรือสามารถระบุถึงตัว (An identified or identifiable)
ข้อมูลนั้นจะต้องมีความสามารถในการแยกแยะบุคคลหนึ่งออกจากบุคคลอื่น ไม่ว่าโดยทางตรงหรือทางอ้อมก็ตาม
4.) บุคคลธรรมดา (Natural person)
คือบุคคลธรรมดาซึ่งยังมีชีวิตอยู่เท่านั้น ไม่รวมถึงผู้ถึงแก่กรรมและนิติบุคคล

นอกเหนือจากนิยามของ OECD และสหภาพยุโรป นิยามตามมาตรฐาน NIST SP 800-122 ของสหรัฐอเมริกา[19] ก็เป็นอีกหนึ่งนิยามที่องค์กรต่าง ๆ ในประเทศไทยนิยมใช้อธิบายความหมายของข้อมูลส่วนบุคคล โดยข้อมูลส่วนบุคคล (Personally identifiable information) ตามมาตรฐานนี้จะหมายถึงข้อมูลใด ๆ เกี่ยวกับบุคคล ซึ่งอยู่ในความครอบครองขององค์กรต่าง ๆ และข้อมูลดังกล่าวนั้นมีความสามารถในการระบุถึงตัวเจ้าของข้อมูล ซึ่งอาจจำแนกได้เป็นสามลักษณะด้วยกัน[20] คือ

---

[17] GDPR, Article 4 (1).; LED, Article 3 (1).

[18] The Article 29 Working Party, "Opinion 4/2007 on the Concept of Personal Data, at Iii. Analysis of the Definition of "Personal Data" According to the Data Protection Directive."

[19] National Institute of Standards and Technology Special Publication 800-122

[20] National Institute of Standards and Technology, "National Institute of Standards and Technology (Nist Special Publication 800-122) Guide to Protecting the Confidentiality of Personally Identifiable Information (Pii),"(2010), pp. 26-

1.) ข้อมูลที่สามารถใช้ “แยกแยะ” บุคคล (Distinguish)
คือข้อมูลที่มีความสามารถในการแยกแยะบุคคลออกจากกันได้โดยตรง โดยไม่จำต้องอาศัยข้อมูลอื่นมาประกอบ เช่น ชื่อสกุล เลขประจำตัวประชาชน เลขประกันสังคม รูปถ่าย หรือข้อมูลชีวมิติ

2.) ข้อมูลที่สามารถ “ติดตาม” บุคคล (Trace)
คือข้อมูลที่อาจใช้เพื่อติดตามกิจกรรมหรือพฤติกรรมของบุคคลได้ เช่น ข้อมูลจราจรคอมพิวเตอร์ (log file) ที่นำมาใช้เพื่อระบุถึงพฤติกรรมการใช้งานระบบคอมพิวเตอร์หรืออินเตอร์เน็ตได้

3.) ข้อมูลที่ “ถูกเชื่อมโยง” หรือ “อาจถูกเชื่อมโยง” ถึงบุคคล (Linked or Linkable)
คือข้อมูลที่นำไปประกอบกับข้อมูลอื่นแล้วเชื่อมโยงเพื่อระบุตัวบุคคลได้ เช่น เชื้อชาติ ตำแหน่งที่อยู่ เบอร์โทรศัพท์ วันเกิด ข้อมูลสุขภาพ ประวัติการทำงาน สถานะการเงิน โดยจะจำแนกรูปแบบการเชื่อมโยงเป็นสองรูปแบบดังนี้

3.1) การเชื่อมโยงชุดข้อมูลจากฐานข้อมูลที่มีสิทธิเข้าถึง หรือการเชื่อมโยงจากฐานข้อมูลข้างเคียงในองค์กรที่ไม่มีระบบรักษาความปลอดภัย ซึ่งข้อมูลที่อาจเชื่อมโยงได้ในรูปแบบนี้ จะถูกอธิบายว่าเป็นข้อมูลที่ถูกเชื่อมโยงแล้ว เพราะการเชื่อมโยงกระทำได้โดยใช้เพียงฐานข้อมูลในองค์กร

3.2) การเชื่อมโยงที่ต้องอาศัยฐานข้อมูลอื่นเพิ่มเติม อาทิ ข้อมูลสาธารณะหรือข้อมูลบนอินเตอร์เน็ต ข้อมูลนั้นจะถูกพิจารณาว่าเป็นเพียงข้อมูลที่อาจถูกเชื่อมโยงได้เท่านั้น

จากการศึกษาความหมายของข้อมูลส่วนบุคคลในหัวข้อนี้ จะเห็นได้ว่านิยามในแต่ละแนวทางนั้นมีความคล้ายคลึงกัน และอาจสรุปได้ว่าเส้นแบ่งสำคัญระหว่างข้อมูลทั่วไปกับข้อมูลส่วนบุคคลอยู่ที่ความสามารถในการ “บ่งชี้เฉพาะ” (Identifiability) ตัวบุคคลออกจากบุคคลอื่น จึงจะอยู่ในขอบเขตความหมายของข้อมูลส่วนบุคคลที่กฎหมายมุ่งคุ้มครอง[21]

27; ปิยะบุตร บุญอร่ามเรือง และคณะ, แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (กรุงเทพฯ: โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย, 2563), หน้า 26-27.

[21] นคร เสรีรักษ์, ความเป็นส่วนตัว: ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย, หน้า 100.

2.1.2 แนวคิดว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

เมื่อสารัตถะของข้อมูลส่วนบุคคลคือการเป็นสิ่งชี้เฉพาะตัวบุคคล ข้อมูลส่วนบุคคลจึงอาจเป็นความลับซึ่งเจ้าของข้อมูลต้องการปกปิดหรือจำกัดการใช้ข้อมูล การคุ้มครองข้อมูลส่วนบุคคลจึงมีฐานทางความคิดมาจากสิทธิความเป็นส่วนตัว (Privacy)[22] โดยสิทธิความเป็นส่วนตัวนี้ถูกพิจารณาว่าเป็นสิทธิธรรมชาติซึ่งติดตัวมนุษย์ตั้งแต่กำเนิด เพราะในสภาวะธรรมชาติ มนุษย์ย่อมมีขอบเขตส่วนบุคคลที่หวงแหนและไม่ประสงค์จะให้ผู้อื่นมาก้าวล่วง สิทธิความเป็นส่วนตัวจึงถือเป็นหนึ่งในสิทธิมนุษยชนขั้นพื้นฐาน[23] และได้รับการบัญญัติไว้ในปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights) [24] ไว้ดังนี้

> “บุคคลจะถูกแทรกแซงตามอำเภอใจในความเป็นส่วนตัว ครอบครัว ที่อยู่อาศัย หรือการสื่อสาร หรือจะถูกลบหลู่เกียรติยศ และชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับการคุ้มครองของกฎหมายจากการแทรกแซงสิทธิหรือการลบหลู่ดังกล่าวนั้น”

มีข้อสังเกตว่าการอธิบายสิทธิส่วนบุคคลในยุคเริ่มแรกนั้นจะเป็นการอธิบายเพื่อคุ้มครองชีวิตเนื้อตัวร่างกาย ครอบครัว ชื่อเสียง และกรรมสิทธิ์ในทรัพย์สิน โดยมองว่าเป็นความชอบธรรมที่บุคคลจะหวงแหนไม่ให้บุคคลอื่นหรือแม้แต่รัฐเข้ามาแทรกแซง ในแง่นี้ ความเป็นส่วนตัวจึงหมายถึงสิทธิที่จะอยู่โดยลำพังหรือแยกตัวอย่างสันโดษ (Solitude) โดยจำกัดการเข้าถึงของบุคคลภายนอก และยังอาจหมายความรวมถึงสิทธิที่จะปกปิดความลับ (Secrecy) ไม่ให้บุคคลภายนอกรู้เห็น[25]

ต่อมา การคุ้มครองสิทธิส่วนบุคคลนี้ก็ได้ขยายไปถึงข้อมูลส่วนบุคคลด้วย เนื่องจากเทคโนโลยีสมัยใหม่สามารถเข้าถึงและเผยแพร่ข้อมูลข่าวสารได้อย่างรวดเร็ว ส่งผลให้ข้อมูลส่วนบุคคลถูกนำไปใช้ประโยชน์หรือเปิดเผยโดยที่เจ้าของข้อมูลไม่ได้รู้เห็นหรือให้ความยินยอมอยู่บ่อยครั้ง และในหลายกรณีการแทรกแซงความเป็นส่วนตัวในข้อมูลก็เกิดขึ้นในพื้นที่ซึ่งเป็นขอบเขตสาธารณะ เช่น การเฝ้าดูด้วยกล้องตรวจจับภาพ หรือการเก็บรวบรวมข้อมูลพฤติกรรมการบริโภคทางอินเทอร์เน็ต ฯลฯ ส่งผลให้มีการอธิบายความเป็นส่วนตัวในแง่ของการมีอิสระในการปกครองตนเอง (Autonomy) นั่นคือบุคคลจะมีความเป็นอยู่ส่วนตัวต่อเมื่อสามารถควบคุมเกี่ยวกับข้อมูลเกี่ยวกับตนได้ หรืออีกนัยหนึ่ง คือสามารถที่จะคิดและตัดสินใจได้ว่าบุคคลอื่นสามารถกระทำต่อข้อมูลส่วนบุคคลของตนได้หรือไม่ เพียงใด โดย

---

[22] เรื่องเดียวกัน, หน้า 97-102.

[23] คณาธิป ทองรวีวงศ์, คำอธิบาย หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล, หน้า 3-9; บุญชู ณ ป้อมเพชร, "คำอธิบายกฎหมายข้อมูลข่าวสารของราชการ,"(PUB HTML5).

[24] Universal Declaration of Human Rights, Article 12.

[25] นคร เสรีรักษ์, ความเป็นส่วนตัว: ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย, หน้า 63-66.

ปราศจากการก้าวก่ายจากบุคคลอื่นหรือรัฐ[26] ความเป็นส่วนตัวในแง่ของการมีอิสระในการปกครองตน จึงเป็นที่มาของ “หลักความยินยอม” ในกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ทั้งนี้ เพราะผลกระทบจากการละเมิดความเป็นส่วนตัวในข้อมูลไม่ได้เป็นแต่เพียงการเปิดเผยความลับ แต่ยังอาจเป็นผลให้เจ้าของข้อมูลรู้สึกเดือดร้อนรำคาญ ถูกดูหมิ่นเหยียดหยาม ไม่ได้รับความสันโดษ หรือกระทั่งกังวลในความปลอดภัยของชีวิตและทรัพย์สินจนไม่อาจดำเนินชีวิตได้โดยปกติสุข การคุ้มครองความเป็นส่วนตัวในข้อมูลจึงมีผลเป็นการปกป้องผลร้ายที่อาจเกิดขึ้นจากการล่วงละเมิดข้อมูลส่วนบุคคลอีกด้วย[27] โดยทางทฤษฎี อาจจำแนกประเภทภัยคุกคามได้สี่กลุ่มพฤติกรรม ซึ่งแต่ละกลุ่มก็จะประกอบด้วยการกระทำย่อยหลากหลายรูปแบบ[28] อันได้แก่

1.) การเก็บรวบรวมข้อมูล (Information collection)
ประกอบด้วยการกระทำย่อย คือการสอดแนม และการสอบถาม
2.) การประมวลผลข้อมูล (Data processing)
ประกอบด้วยการกระทำย่อย คือการรวมข้อมูล การระบุตัวบุคคล การกระทำที่ก่อให้เกิดความไม่ปลอดภัย การนำข้อมูลไปใช้โดยไม่สอดคล้องกับวัตถุประสงค์ตั้งต้น
3.) การเปิดเผยข้อมูล (Information dissemination)
ประกอบด้วยการกระทำย่อย คือการเปิดเผย การทำผิดต่อหน้าที่ตามความไว้วางใจ การสร้างโอกาสเข้าถึง การขู่เปิดเผยความลับ การใช้ประโยชน์ การเผยแพร่ข้อมูลเท็จ
4.) การรุกราน (Invasion)
ประกอบด้วยการกระทำย่อย คือการแทรกแซง และการแทรกแซงการตัดสินใจ

การจำแนกกลุ่มพฤติกรรมข้างต้นมีผลต่อการบัญญัติหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลในหลายประเทศ ในแง่ที่ว่ากฎเกณฑ์นั้นจะมุ่งคุ้มครองข้อมูลส่วนบุคคลจากพฤติกรรมกลุ่มใด อย่างไร เช่น หมวด 2 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ก็จะประกอบไปด้วยกฎเกณฑ์การเก็บรวบรวมข้อมูลส่วนบุคคลในส่วนที่ 2 และการใช้หรือเปิดเผยข้อมูลส่วนบุคคลในส่วนที่ 3 ตามลำดับ สะท้อนให้เห็นว่าพระราชบัญญัติดังกล่าวมีเจตนารมณ์คุ้มครองข้อมูลส่วนบุคคลในขั้นตอนเก็บรวบรวม ใช้ และเปิดเผยข้อมูลเป็นสำคัญ[29]

---

[26] คณาธิป ทองรวีวงศ์, คำอธิบาย หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล, หน้า 20-22; นคร เสรีรักษ์, ความเป็นส่วนตัว: ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย, หน้า 63-66.

[27] เรื่องเดียวกัน, หน้า 97-102; ปิยะบุตร บุญอร่ามเรือง และคณะ, แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล, หน้า 17.

[28] คณาธิป ทองรวีวงศ์, คำอธิบาย หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล, หน้า 22-23.

[29] เรื่องเดียวกัน.

นอกจากนี้ การให้ความคุ้มครองข้อมูลส่วนบุคคลยังมีความสัมพันธ์กับแนวคิดการรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์หรือสารสนเทศ (Computer or Information Security) และแนวคิดการรักษาคุณภาพของข้อมูล (Data Quality) โดยรองศาสตราจารย์คณาธิป ทองรวีวงศ์ ให้คำอธิบายว่า แนวคิดการรักษาความมั่นคงปลอดภัยหมายถึงการรักษาความปลอดภัยของระบบ ซึ่งเกี่ยวข้องกับการคุ้มครองในมิติของการปกป้องข้อมูลส่วนบุคคลให้พ้นจากภัยคุกคาม เนื่องจากการดำเนินการต่อข้อมูลในปัจจุบันมักอาศัยระบบคอมพิวเตอร์เป็นเครื่องมือ ในขณะที่แนวคิดการรักษาคุณภาพของข้อมูลจะเป็นหลักการที่เรียกร้องให้รักษาคุณภาพของข้อมูลให้มีความถูกต้อง สมบูรณ์ น่าเชื่อถือ และสามารถเข้าถึงได้เมื่อจำเป็นต้องใช้งาน เพื่อให้ข้อมูลมีความเหมาะสมสำหรับการใช้งานตามวัตถุประสงค์ จึงไม่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลโดยตรง[30]

อย่างไรก็ตาม สิทธิความเป็นส่วนตัวในข้อมูลไม่ใช่สิทธิเด็ดขาดและอาจถูกจำกัดได้ในบางกรณีเพื่อให้ความคุ้มครองสิทธิอื่นหรือคุณค่าอื่นที่เหนือกว่า[31] ดังที่ปรากฏตามอนุสัญญายุโรปว่าด้วยสิทธิมนุษยชน (European Convention on Human Rights: “ECHR”)[32] ความว่า

> “บุคคลทุกคนย่อมมีสิทธิที่จะได้รับการเคารพความเป็นส่วนตัว ชีวิตครอบครัว ที่อยู่อาศัย และการติดต่อสื่อสารส่วนบุคคล
>
> รัฐไม่อาจแทรกแซงสิทธิดังกล่าวได้ เว้นแต่เป็นไปตามที่กฎหมายบัญญัติและปรากฏถึงความจำเป็นในสังคมประชาธิปไตย เพื่อความมั่นคงของชาติ ความปลอดภัยของสาธารณะ ความผาสุกทางเศรษฐกิจ การป้องกันและปราบปรามอาชญากรรม การรักษาสุขอนามัย ศีลธรรมอันดี ตลอดจนการคุ้มครองสิทธิและเสรีภาพของผู้อื่น”

ด้วยเหตุนี้ การให้ความคุ้มครองสิทธิความเป็นส่วนตัว รวมถึงข้อมูลส่วนบุคคล จึงจำเป็นต้องชั่งน้ำหนักระหว่างขอบเขต “ส่วนบุคคล” และขอบเขต “สาธารณะ” อยู่เสมอ ซึ่งผู้ช่วยศาสตราจารย์ ดร. นคร เสรีรักษ์ เห็นว่าเป็นเรื่องยากในการชี้ชัดลงไป เพราะข้อความคิดทั้งสองมีจุดยืนที่ตรงข้ามกัน กล่าวคือ ไม่มีความสอดคล้องตรงกัน แต่ได้รับเนื้อหามาจากกันและกัน ประกอบกับมุมมองเรื่องความส่วนตัวมีนัยที่ซับซ้อน และแตกต่างกันไปตามแต่ระเบียบแบบแผนและวัฒนธรรมของสังคม[33]

---

[30] เรื่องเดียวกัน, หน้า 23-28 และ หน้า 31-32.

[31] เรื่องเดียวกัน, หน้า 16.

[32] The European Convention on Human Rights (ECHR), Article 8.

[33] นคร เสรีรักษ์, ความเป็นส่วนตัว: ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย, หน้า 75-81.

เช่น ในประเทศไทย มุมมองเรื่องสิทธิความเป็นส่วนตัวนั้นจะเป็นมุมมองของสังคมตะวันออก ซึ่งมีแนวคิดยอมรับสถานะที่แตกต่างระหว่างบุคคลและเคยชินกับการอยู่ภายใต้โครงสร้างเชิงอำนาจในลักษณะผู้ปกครอง-ผู้ถูกปกครอง โดยมองว่าผู้ปกครองมีหน้าที่ดูแลทุกข์สุขของบ้านเมือง ในขณะที่ผู้ถูกปกครองก็ต้องช่วยเหลือเกื้อกูลกันในสังคม เพราะสังคมตะวันออกมีค่านิยมและความเชื่อพื้นฐานมาจากคำสอนทางศาสนาพุทธที่ส่งเสริมความสัมพันธ์ในทางที่เมตตาต่อกัน ส่งผลให้เดิม สังคมไทยมองว่าสิทธิเสรีภาพเป็นสิ่งที่ผู้ปกครองหยิบยื่นให้ด้วยความเมตตา และแม้ว่าทรรศนะดังกล่าวในสังคมไทยจะมีการเปลี่ยนแปลงไปบ้างตามยุคสมัย แต่ค่านิยมและความเชื่อพื้นฐานในการอยู่รวมกันเป็นสังคมก็ยังคงหลงเหลืออยู่ คือมองว่าปัจเจกบุคคลมีหน้าที่ต้องเสียสละเพื่อส่วนรวม ดังนั้น ประเทศไทยจึงต้องเผชิญความขัดแย้งระหว่างสิทธิส่วนบุคคลกับประโยชน์สาธารณะอยู่บ่อยครั้ง โดยมักมีเหตุผลเกี่ยวกับความมั่นคงของชาติมารองรับ เป็นต้น[34]

2.1.3 หลักการพื้นฐานของการคุ้มครองข้อมูลส่วนบุคคล

เมื่อแนวปฏิบัติเกี่ยวกับข้อมูลส่วนบุคคลของ OECD และกฎหมาย GDPR ของสหภาพยุโรปมีอิทธิพลต่อกฎหมายคุ้มครองข้อมูลส่วนบุคคลในหลายประเทศทั่วโลก รวมถึงประเทศไทย ในหัวข้อนี้ผู้เขียนจึงจะนำเสนอหลักการสำคัญในการคุ้มครองข้อมูลส่วนบุคคลของทั้งสองแนวทาง รวมถึงหลักการอื่นใด เพื่อเป็นพื้นฐานในการศึกษาวิเคราะห์กฎหมายคุ้มครองข้อมูลส่วนบุคคลในบทต่อ ๆ ไป

2.1.3.1 หลักการคุ้มครองข้อมูลส่วนบุคคลตามแนวปฏิบัติของ OECD

หลักการพื้นฐานในการคุ้มครองข้อมูลส่วนบุคคลของ OECD ปรากฏอยู่ในแนวปฏิบัติ The OECD Guidelines Governing The Protection of Privacy and Transborder Flows of Personal Data ซึ่งได้มีการแก้ไขปรับปรุงล่าสุดเมื่อปี ค.ศ. 2013 โดยแนวปฏิบัตินี้มีจุดเริ่มต้นมาจากปัญหาการขัดกันของกฎหมายคุ้มครองข้อมูลส่วนบุคคล อันส่งผลกระทบต่อการไหลเวียนข้อมูลระหว่างประเทศสมาชิก OECD จึงกำหนดแนวปฏิบัตินี้ขึ้นเพื่อสร้างความเป็นหนึ่งเดียวกันของกฎเกณฑ์ โดยมีหลักการคุ้มครองข้อมูลส่วนบุคคลที่สำคัญดังนี้[35]

1.) <u>หลักข้อจำกัดในการเก็บรวบรวมข้อมูล (Collection Limitation Principle)</u>
การเก็บรวบรวมข้อมูลส่วนบุคคลต้องกระทำด้วยวิธีการที่ชอบด้วยกฎหมายและเป็นธรรม โดยให้เจ้าของข้อมูลรับทราบและยินยอมในการเก็บรวบรวมข้อมูล[36]

---

[34] เรื่องเดียวกัน, หน้า 91-97.

[35] เรื่องเดียวกัน, หน้า 147-149.

[36] OECD Privacy Framework 2013, at 7 Collection Limitation Principle.

2.) หลักคุณภาพของข้อมูล (Data Quality Principle)
ข้อมูลส่วนบุคคลที่จัดเก็บต้องมีความเกี่ยวข้องกับวัตถุประสงค์ของการใช้ข้อมูล รวมถึงเป็นข้อมูลที่ถูกต้อง สมบูรณ์ เป็นปัจจุบัน[37]

3.) หลักการกำหนดวัตถุประสงค์ (Purpose Specification Principle)
ก่อนเก็บรวบรวมข้อมูลส่วนบุคคล ให้กำหนดวัตถุประสงค์ของการเก็บรวบรวมข้อมูลดังกล่าวไว้โดยชัดแจ้ง[38]

4.) หลักการจำกัดการใช้ข้อมูล (Use Limitation Principle)
ห้ามมิให้มีการใช้หรือเปิดเผยข้อมูลส่วนบุคคล นอกเหนือไปจากวัตถุประสงค์ในคราวแรก เว้นแต่ได้รับความยินยอมหรือได้รับอนุญาตตามกฎหมาย[39]

5.) หลักการรักษาความปลอดภัย (Security Safeguards Principle)
จัดมาตรการรักษาความมั่นคงปลอดภัยป้องกันไม่ให้ข้อมูลสูญหาย หรือเสียหายจากการเข้าถึง ทำลาย แก้ไขเปลี่ยนแปลง ใช้ และเปิดเผยโดยไม่ได้รับอนุญาต[40]

6.) หลักการเปิดเผยข้อมูล (Openness Principle)
ให้จัดทำนโยบายทั่วไป ซึ่งกำหนดวิธีการ รูปแบบ และหลักเกณฑ์ในการเปิดเผยข้อมูลส่วนบุคคล โดยไม่กระทบต่อสิทธิความเป็นส่วนตัวของบุคคล[41]

7.) หลักการมีส่วนร่วมของปัจเจกบุคคล (Individual Participation Principle)
เจ้าของข้อมูลส่วนบุคคลย่อมมีสิทธิในการตัดสินใจและควบคุมการดำเนินการที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของตน ดังต่อไปนี้[42]

7.1) สิทธิที่จะได้รับแจ้งว่าข้อมูลส่วนบุคคลถูกประมวลผลหรือไม่ อย่างไร

7.2) สิทธิที่จะตรวจสอบข้อมูลส่วนบุคคลภายในระยะเวลาที่เหมาะสม และหากมีค่าใช้จ่าย ค่าใช้จ่ายนั้นก็ต้องสมเหตุสมผล

7.3) สิทธิที่จะทราบเหตุแห่งการปฏิเสธการใช้สิทธิตามข้อ 7.1) หรือ 7.2) รวมถึงสิทธิในการอุทธรณ์การปฏิเสธดังกล่าว

7.4) สิทธิโต้แย้งการประมวลผลข้อมูลส่วนบุคคล เพื่อขอให้ลบหรือแก้ไขเปลี่ยนแปลงข้อมูลส่วนบุคคล

---

[37] OECD Privacy Framework 2013, at 8 Data Quality Principle.

[38] OECD Privacy Framework 2013, at 9 Purpose Specification Principle.

[39] OECD Privacy Framework 2013, at 10 Use Limitation Principle.

[40] OECD Privacy Framework 2013, at 11 Security Safeguards Principle.

[41] OECD Privacy Framework 2013, at 12 Openness Principle.

[42] OECD Privacy Framework 2013, at 13 Individual Participation Principle.

8.) หลักความรับผิดชอบ (Accountability Principle)

ผู้ควบคุมข้อมูลส่วนบุคคลต้องรับผิดชอบในการปฏิบัติตามหลักเกณฑ์ข้างต้น[43]

มีข้อสังเกตว่าหลักการตามแนวปฏิบัติของ OECD เป็นหลักการทั่วไปในการคุ้มครองข้อมูลส่วนบุคคล โดยไม่แบ่งแยกระหว่างหน่วยงานรัฐหรือเอกชนแต่อย่างใด

2.1.3.2 หลักการคุ้มครองข้อมูลส่วนบุคคลตาม GDPR ของสหภาพยุโรป

GDPR เป็นข้อกำหนดทั่วไปว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปซึ่งแทนที่ EU Directive 95/46/EC ที่มีผลบังคับใช้มาตั้งแต่ ค.ศ. 1995 เพื่อยกระดับการคุ้มครองข้อมูลส่วนบุคคลของพลเมืองของสหภาพยุโรปให้เหมาะสมกับสถานการณ์ที่เปลี่ยนแปลงไป โดย GDPR ได้วางหลักการพื้นฐานที่เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลดังต่อไปนี้[44]

1.) หลักความชอบด้วยกฎหมาย เป็นธรรม และโปร่งใส (Lawfulness, Fairness and Transparency Principle)

ข้อมูลส่วนบุคคลต้องถูกประมวลผลโดยชอบด้วยกฎหมาย เป็นธรรม ด้วยวิธีการอันโปร่งใส และในการประมวลผลข้อมูลจะต้องมีฐานทางกฎหมาย (legal basis) อย่างหนึ่งอย่างใดดังต่อไปนี้[45]

1.1) ฐานความยินยอม (Consent)

1.2) ฐานสัญญา (Contract)

1.3) ฐานหน้าที่ตามกฎหมาย (Legal Obligation)

1.4) ฐานประโยชน์สำคัญอันเกี่ยวเนื่องถึงชีวิต (Vital Interest)

1.5) ฐานภารกิจของรัฐ (Public Task)

1.6) ฐานประโยชน์อันชอบธรรม (Legitimate Interests)

2.) หลักการจำกัดวัตถุประสงค์ (Purpose Limitation Principle)

ข้อมูลส่วนบุคคลต้องถูกรวบรวมเพื่อวัตถุประสงค์ที่ชัดแจ้งเฉพาะเจาะจง และในการประมวลผลข้อมูลจะต้องไม่ดำเนินการนอกเหนือไปจากวัตถุประสงค์ตั้งต้น

---

[43] OECD Privacy Framework 2013, at 14 Accountability Principle.

[44] GDPR, Article 5.

[45] GDPR, Article 6.

3.) หลักการใช้ข้อมูลให้น้อยที่สุด (Data Minimisation Principle)
ข้อมูลส่วนบุคคลต้องจำกัดเท่าที่เพียงพอ จำเป็น และเกี่ยวข้องกับวัตถุประสงค์ที่ข้อมูลนั้นถูกประมวลผล

4.) หลักความถูกต้องสมบูรณ์ (Accuracy Principle)
ข้อมูลส่วนบุคคลต้องถูกต้อง สมบูรณ์ และเป็นปัจจุบัน

5.) หลักการจำกัดการเก็บรักษา (Storage Limitation Principle)
ข้อมูลส่วนบุคคลต้องถูกเก็บรักษาในรูปแบบที่ระบุตัวตนของเจ้าของข้อมูลได้ไม่นานเกินกว่าที่จำเป็นสำหรับวัตถุประสงค์ของการประมวลผลข้อมูล

6.) หลักความสมบูรณ์และเป็นความลับ (Integrity and Confidentiality Principle)
ข้อมูลส่วนบุคคลต้องถูกประมวลผลด้วยวิธีการที่รับประกันความมั่นคงปลอดภัย เพื่อป้องกันการประมวลผลที่ไม่ได้รับอนุญาตหรือที่ไม่ชอบด้วยกฎหมาย รวมถึงป้องกันไม่ให้ข้อมูลถูกทำลายหรือสูญหายไป โดยใช้มาตรการทางเทคนิคหรือการจัดการองค์กรตามสมควร

7.) หลักความรับผิดชอบ (Accountability Principle)
ผู้ควบคุมข้อมูลส่วนบุคคลต้องเป็นผู้รับผิดชอบและปฏิบัติตามหลักการคุ้มครองข้อมูลส่วนบุคคลตามข้อ 1.) ถึงข้อ 6.) นี้

อย่างไรก็ดี แตกต่างจากแนวปฏิบัติของ OECD หลักการพื้นฐานของ GDPR จะไม่ได้มีผลใช้บังคับแก่การประมวลผลข้อมูลส่วนบุคคลทุกกรณี โดย GDPR จะให้ความสำคัญแก่การคุ้มครองข้อมูลส่วนบุคคลของผู้บริโภคจากภาคธุรกิจเป็นหลัก

ในภาพรวม จะเห็นได้ว่าหลักการคุ้มครองข้อมูลส่วนบุคคลทั้งหมดนี้ตั้งอยู่บนพื้นฐานเดียวกัน คือการคุ้มครองข้อมูลส่วนบุคคลโดยครอบคลุม “อำนาจควบคุมเหนือข้อมูล” ในการเก็บรวบรวมและใช้ประโยชน์จากข้อมูลส่วนบุคคล มากกว่าที่จะคำนึงว่าข้อมูลอยู่ในความครอบครองของผู้ใด เนื่องด้วยลักษณะและความสามารถของเทคโนโลยีและระบบคอมพิวเตอร์สมัยใหม่ที่สามารถบันทึกและถ่ายโอนข้อมูลจากที่หนึ่งไปอีกที่หนึ่งโดยไร้พรมแดน

2.2 การสืบสวนและสอบสวนคดีอาญา

เมื่อเป้าหมายของกระบวนการยุติธรรมทางอาญาคือการนำตัวผู้กระทำความผิดมาดำเนินคดี เจ้าพนักงานในกระบวนการยุติธรรมจึงมีหน้าที่ร่วมกันค้นหาความจริงว่าการกระทำความผิดเกิดขึ้นได้อย่างไรและใครเป็นผู้กระทำ เพื่อนำตัวผู้กระทำความผิดที่แท้จริงมาลงโทษ และป้องกันมิให้ผู้บริสุทธิ์ได้รับผลร้าย ด้วยเหตุนี้ การค้นหาความจริงจึงเป็นสาระสำคัญในการดำเนินคดีอาญา[46]

โดยทั่วไป เจ้าพนักงานสืบสวนสอบสวนจะเป็นองค์กรแรกที่มีบทบาทในการค้นหาความจริงในคดีอาญาด้วยการแสวงหาข้อเท็จจริงและการรวบรวมพยานหลักฐาน ตามที่ปรากฏในประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 2 ซึ่งได้ให้นิยามการสืบสวนและการสอบสวนเอาไว้ว่า

> “การสืบสวน หมายความถึง การแสวงหาข้อเท็จจริงและหลักฐานซึ่งพนักงานฝ่ายปกครองหรือตำรวจได้ปฏิบัติไปตามอำนาจและหน้าที่ เพื่อรักษาความสงบเรียบร้อยของประชาชน และเพื่อที่จะทราบรายละเอียดแห่งความผิด”[47]

> “การสอบสวน หมายความถึง การรวบรวมพยานหลักฐานและการดำเนินการทั้งหลายอื่นตามบทบัญญัติแห่งประมวลกฎหมายนี้ ซึ่งพนักงานสอบสวนได้ทำไปเกี่ยวกับความผิดที่กล่าวหา เพื่อที่จะทราบข้อเท็จจริงหรือพิสูจน์ความผิดและเพื่อเอาตัวผู้กระทำผิดมาฟ้องลงโทษ”[48]

บทนิยามข้างต้นแสดงให้เห็นว่าการสืบสวนอาจกระทำได้ แม้ความผิดจะยังไม่เกิดขึ้น เพื่อให้เจ้าพนักงานรัฐสามารถป้องกันและระงับเหตุที่กำลังจะเกิดขึ้นได้ทันท่วงที อันเป็นการรักษาความสงบเรียบร้อยของสังคม แต่หากมีความผิดเกิดขึ้นแล้ว การแสวงหาข้อเท็จจริงและหลักฐานในชั้นสืบสวนก็จะเป็นไปเพื่อให้ทราบรายละเอียดเกี่ยวกับความผิด จากนั้นจึงเป็นหน้าที่ของเจ้าพนักงานสอบสวนในการรวบรวมพยานหลักฐาน เพื่อให้ทราบข้อเท็จจริงหรือพฤติการณ์ในคดี รู้ตัวผู้กระทำผิด และพิสูจน์ให้เห็นความผิดหรือความบริสุทธิ์ของผู้ถูกกล่าวหาต่อไป[49]

---

[46] ณรงค์ ใจหาญ, หลักกฎหมายวิธีพิจารณาความอาญา เล่ม 1, หน้า 15; สมัคร เชาวภานันท์, "หลักสิทธิมนุษยชนกับการค้นหาความจริงในคดีอาญา," วารสารศาลรัฐธรรมนูญ 20, 59 (พฤษภาคม - สิงหาคม 2561).

[47] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 2 (10).

[48] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 2 (11).

[49] ณรงค์ ใจหาญ, หลักกฎหมายวิธีพิจารณาความอาญา เล่ม 1, หน้า 19.

อย่างไรก็ตาม เพื่อให้ได้มาซึ่งความจริงในคดี การสืบสวนและสอบสวนก็มีการเก็บรวบรวม ใช้ ตลอดจนเปิดเผยข้อมูลข่าวสารเกี่ยวกับบุคคลเป็นจำนวนมาก อันอาจส่งผลกระทบกระเทือนต่อสิทธิในข้อมูลส่วนบุคคล เนื่องจากการสืบสวนและสอบสวนนั้นเป็นการใช้อำนาจบังคับตามกฎหมาย โดยทั่วไปประชาชนจึงไม่อาจปฏิเสธหรือกล่าวอ้างเรื่องความยินยอมในประเด็นที่เกี่ยวกับข้อมูลส่วนบุคคลได้

ฉะนั้น ในหัวข้อถัดไป ผู้เขียนจะประเมินถึงความจำเป็นของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา ก่อนจะศึกษาหลักการและแนวคิดต่าง ๆ ซึ่งเป็นกรอบการใช้อำนาจสืบสวนและสอบสวนคดีอาญาให้เป็นไปอย่างเหมาะสมต่อไป

2.2.1 ความจำเป็นของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา

เมื่อการสืบสวนและการสอบสวนเป็นการค้นหาความจริงในชั้นเจ้าพนักงาน จึงมีความจำเป็นที่เจ้าพนักงานสืบสวนสอบสวนจะต้องได้มาซึ่งข้อมูลข่าวสาร ข้อเท็จจริง ตลอดจนพยานหลักฐานต่าง ๆ เพื่อประโยชน์ในการรักษาความสงบเรียบร้อย หรือนำตัวผู้กระทำความผิดมาลงโทษ ดังนี้

ประการแรก ข้อมูลข่าวสารที่ต้องดำเนินการสืบสวนก่อนเกิดเหตุ

การสืบสวนก่อนเกิดเหตุ คือการสืบสวนหาข้อมูลข่าวสารซึ่งกระทำเป็นปกติ เพื่อจัดทำข้อมูลท้องถิ่นหรือบัญชีในทางลับ อันเป็นประโยชน์ในการรักษาความสงบเรียบร้อยในทางป้องกันหรือระงับเหตุร้าย โดยข้อมูลข่าวสารที่ต้องดำเนินการสืบสวนก่อนเกิดเหตุอาจจำแนกได้เป็นสี่ประเภท[50] ได้แก่

1.) <u>ภูมิประเทศ</u>

เป็นการศึกษาข้อมูลสภาพพื้นที่และเส้นทางคมนาคมในเขตที่รับผิดชอบ โดยต้องหมั่นตรวจตราพื้นที่และเส้นทางซึ่งล่อแหลมต่อการเกิดอาชญากรรม เพื่อหาทางป้องกันและระงับเหตุดังกล่าว

2.) <u>สถานที่</u>

เป็นการรวบรวมข้อมูลเกี่ยวกับอาคารและสถานที่ในเขตที่รับผิดชอบ เช่น ที่พักอาศัยของบุคคลสำคัญ สถานศึกษา โรงงาน โรงแรม โรงมหรสพ ธนาคาร สถานที่ราชการ หรือสถานที่ล่อแหลมต่อการก่อความไม่สงบ โดยให้ทำแผนที่แสดงที่ตั้งอาคารและสถานที่เหล่านี้ประจำไว้ที่สถานี

---

[50] ระเบียบการตำรวจเกี่ยวกับคดี ลักษณะ 2 การสืบสวน บทที่ 1 หลักทั่วไป ข้อที่ 7; สำนักงานตำรวจแห่งชาติ, "คู่มือการฝึกอบรมข้าราชการตำรวจที่ปฏิบัติหน้าที่งานสืบสวนในสถานีตำรวจ พ.ศ. 2557."

3.) <u>ประเภทและความประพฤติของบุคคล</u>

เป็นการรวบรวมข้อมูลเกี่ยวกับบุคคลในเขตที่รับผิดชอบว่าผู้ใดเป็นบุคคลสำคัญ เป็นผู้มีอิทธิพล เป็นอันธพาล มีประวัติทางโจรกรรม เป็นซ่องโจรหรือรับของโจร เป็นผู้เคยต้องโทษ ผู้เสพสุราหรือสารเสพติดเป็นอาจิณ หรือผู้ประพฤติเที่ยวเตร่ไม่ประกอบอาชีพหรือไม่มีที่อยู่เป็นหลักแหล่ง ฯลฯ เพื่อจัดทำบัญชีไว้ในทางลับ โดยให้ติดตามสืบสวนอย่างใกล้ชิด เพื่อให้ทราบถึงความประพฤติต่อไป

4.) <u>กิริยาของบุคคล</u>

เป็นการสืบถึงกิริยาอันเป็นพิรุธหรือน่าสงสัยของบุคคล อาทิ มีบาดแผลที่ร่างกาย มีการมั่วสุมประชุมเลี้ยงสุรา หรือมีอาวุธเที่ยวเตร่ไปมา โดยไม่มีถิ่นที่อยู่เป็นปกติ เพื่อเป็นแนวทางการสืบสวนขั้นต่อไปว่าบุคคลเหล่านี้จะไปกระทำความผิด หรือได้กระทำผิดแล้วหลบหนีมาหรือไม่

5.) <u>สิ่งของที่ควรสงสัย</u>

เป็นการสืบและตรวจค้นบุคคลหรือสิ่งของที่ควรสงสัย โดยมีเหตุและรายละเอียดตามสมควร เช่น การตรวจค้นผู้มีที่อาวุธเปื้อนคราบโลหิต หรือผู้มีที่ทรัพย์สินเกินกว่าฐานะ ซึ่งบุคคลทั่วไปไม่อาจมีได้หรือมีพิรุธที่น่าสงสัยว่าได้มาโดยไม่สุจริต

ประการที่สอง ข้อเท็จจริงและหลักฐานที่ต้องดำเนินการสืบสวนและสอบสวนหลังเกิดเหตุ

การสืบสวนและสอบสวนหลังเกิดเหตุ มีวัตถุประสงค์เพื่อแสวงหาพยานหลักฐานในคดีในทางที่จะนำตัวผู้กระทำผิดมาดำเนินคดีและลงโทษ ข้อเท็จจริงและพยานหลักฐานที่ต้องดำเนินการสืบสวนและสอบสวนหลังเกิดเหตุนั้นจึงประกอบไปด้วยข้อเท็จจริงและพยานหลักฐานดังต่อไปนี้[51]

1.) <u>ข้อเท็จจริงและพยานหลักฐานซึ่งทำให้ทราบรายละเอียดและพฤติการณ์ในคดี</u>

เป็นการรวบรวบข้อมูลและพยานหลักฐานเบื้องต้นว่าการกระทำความผิดเกิดที่ใด เมื่อไหร่ แก่ใคร และผลจากการกระทำนั้นเป็นอย่างไร ซึ่งโดยส่วนใหญ่จะเป็นสิ่งที่ตรวจพบในสถานที่เกิดเหตุ เช่น รอยนิ้วมือ คราบโลหิตหรือสารคัดหลั่งต่าง ๆ สิ่งของตกหล่น รอยล้อรถ ภาพจากกล้องวงจรปิด ลักษณะบาดแผลหรือความเสียหายที่เกิดกับทรัพย์สิน เป็นต้น

2.) <u>ข้อเท็จจริงและพยานหลักฐานซึ่งทำให้รู้ถึงตัวผู้กระทำผิด</u>

เป็นการขยายผลจากข้อเท็จจริงและพยานหลักฐานที่ตรวจพบในสถานที่เกิดเหตุ เพื่อเชื่อมโยงถึงตัวผู้กระทำผิด เช่น การตรวจสอบข้อมูลการเป็นเจ้าของทรัพย์สิน

---

[51] เรื่องเดียวกัน.

หรือยานพาหนะจากฐานข้อมูลทะเบียน การขอรายการเคลื่อนไหวทางบัญชีจากสถาบันการเงิน การเรียกดูข้อมูล IP address และข้อมูลจราจรคอมพิวเตอร์จากผู้ให้บริการ การส่งตรวจพิสูจน์รอยนิ้วมือ คราบโลหิต สารคัดหลั่งด้วยวิธีการทางวิทยาศาสตร์ รวมถึงการสืบประวัติภูมิหลังของผู้เสียหาย เพื่อค้นหามูลเหตุจูงใจในการกระทำความผิด

3.) ข้อเท็จจริงและพยานหลักฐานซึ่งพิสูจน์ความผิดหรือความบริสุทธิ์ของบุคคล เป็นการวิเคราะห์เชื่อมโยงข้อเท็จจริงและพยานหลักฐานที่รวบรวมประกอบกันก่อนจะสรุปข้อเท็จจริงทางคดี ซึ่งยืนยันความผิดหรือบริสุทธิ์ของผู้ต้องหาต่อไป

นอกจากนี้ เพื่อประโยชน์ในการติดตามจับกุมผู้กระทำความผิด เจ้าพนักงานสืบสวนสอบสวนยังอาจสืบค้นข้อมูลที่อยู่ของผู้ต้องหาจากฐานข้อมูลทะเบียนราษฎร หรือสถานที่ทำงานจากฐานข้อมูลประกันสังคม รวมถึงตรวจสอบตำแหน่งจากการใช้โทรศัพท์เคลื่อนที่อีกด้วย

จะเห็นได้ว่าข้อเท็จจริงและพยานหลักฐานที่จำต้องดำเนินการสืบสวนและสอบสวนนั้นล้วนมีข้อมูลส่วนบุคคลประกอบอยู่ด้วยจำนวนมาก ไม่ว่าจะเป็นข้อมูลประเภทหรือพฤติกรรมของคนในท้องที่ ตำแหน่งที่พักอาศัย ภาพถ่ายในคดี ชื่อสกุล ตำหนิรูปพรรณ ข้อมูลพันธุกรรมจากการตรวจพิสูจน์ ฯลฯ ทั้งนี้ เพราะข้อมูลส่วนบุคคลเป็นสิ่งสามารถใช้ในการเชื่อมโยงถึงตัวตนของบุคคล ทั้งยังอาจใช้ในการติดตามหรือยืนยันถึงการกระทำและพฤติกรรมของบุคคล การดำเนินงานในชั้นสืบสวนและสอบสวนคดีอาญาจึงประกอบด้วยการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ซึ่งถือเป็นส่วนหนึ่งของการประมวลผลข้อมูลส่วนบุคคลตามแนวคิดว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

ฉะนั้น เมื่อพิจารณาถึงความจำเป็นเพื่อประโยชน์สาธารณะ การประมวลผลข้อมูลส่วนบุคคลจึงเป็นกระบวนการที่มีความสำคัญอย่างยิ่งในการค้นหาความจริงในคดีอาญา คนในสังคมทั่วไปจึงให้การยอมรับว่าสิทธิในข้อมูลส่วนบุคคลนั้นอาจถูกจำกัดได้ในชั้นสืบสวนและสอบสวนคดีอาญา ส่งผลให้การใช้อำนาจสืบสวนและสอบสวนคดีอาญาอาจก่อให้เกิดผลกระทบทางลบต่อข้อมูลส่วนบุคคล

2.2.2 ข้อพิจารณาในการใช้อำนาจสืบสวนและสอบสวนคดีอาญา

แม้ว่าการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลจะเป็นการดำเนินการที่จำเป็นในการค้นหาความจริงในชั้นสืบสวนและสอบสวนคดีอาญา แต่ก็มิได้หมายความว่าเจ้าพนักงานจะสามารถใช้อำนาจได้โดยไร้ขอบเขต เพราะหลักการพื้นฐานของกระบวนการยุติธรรมทางอาญาคือการรักษาสมดุลระหว่างการป้องกันและปราบปรามอาชญากรรมกับหลักประกันสิทธิและเสรีภาพของประชาชน การใช้อำนาจสืบสวนและสอบสวนจึงควรมีกรอบและขอบเขตทางกฎหมายมากำกับอยู่เสมอ

ในทางทฤษฎี อาจอธิบายการรักษาสมดุลข้างต้นตามรูปแบบการดำเนินกระบวนการยุติธรรมทางอาญาในทรรศนะของ Herbert L. Packer ซึ่งจำแนกออกเป็นสองทฤษฎี คือ[52]

1. ทฤษฎีการควบคุมอาชญากรรม (Crime control)
   ทฤษฎีนี้เห็นว่ากระบวนการยุติธรรมทางอาญาควรให้ความสำคัญกับเรื่อง “ประสิทธิภาพ” เป็นอันดับแรก กล่าวคือการดำเนินการต่าง ๆ ควรเป็นไปอย่างรวดเร็ว ไม่ยึดติดแบบพิธี และมีข้อจำกัดให้น้อยที่สุด เพื่อให้รัฐสามารถบรรลุจุดมุ่งหมายในการป้องกันปราบปรามอาชญากรรม ซึ่งเป็นภารกิจที่สำคัญที่สุดของกระบวนการยุติธรรมทางอาญา
2. ทฤษฎีการควบคุมการใช้อำนาจรัฐ หรือศุภนิติกระบวน (Due process)
   ต่างจากทฤษฎีแรก ทฤษฎีนี้เห็นว่ากระบวนการยุติธรรมทางอาญาควรให้ความสำคัญกับการป้องกันและขจัดข้อผิดพลาดที่อาจเกิดขึ้นในกระบวนการยุติธรรม ด้วยการ “ควบคุมการใช้อำนาจรัฐ” และปฏิเสธที่จะยอมรับกระบวนการที่ไม่ชอบด้วยกฎหมาย เพื่อป้องกันไม่ให้ประชาชนถูกละเมิดสิทธิและเสรีภาพอย่างไม่เป็นธรรม

ศาสตราจารย์พิเศษ ธานิศ เกศวพิทักษ์ ขยายความเกี่ยวกับประเด็นนี้ไว้ว่า เมื่อใดก็ตามที่รัฐให้ความสำคัญกับการควบคุมอาชญากรรม การควบคุมการใช้อำนาจรัฐก็ย่อมลดลงไป แต่ในทางกลับกัน เมื่อใดก็ตามที่รัฐเพิ่มการควบคุมการใช้อำนาจรัฐ ประสิทธิภาพของการควบคุมอาชญากรรมก็อาจจะลดลงไป กระบวนการยุติธรรมทางอาญาจึงต้องถ่วงดุลระหว่างสองหลักการให้มีความเหมาะสม[53]

ในทรรศนะของผู้เขียน การรักษาสมดุลระหว่างการควบคุมอาชญากรรมและการควบคุมการใช้อำนาจรัฐนั้นพึงนำ “หลักความได้สัดส่วน” (Proportionality) มาพิจารณาประกอบ เนื่องจากหลักความได้สัดส่วนนี้เป็นหลักกฎหมายมหาชนทั่วไปซึ่งใช้ในการควบคุมตรวจสอบการใช้อำนาจรัฐที่ส่งผลกระทบต่อสิทธิและเสรีภาพของประชาชน โดยสาระสำคัญของหลักความได้สัดส่วนจะประกอบไปด้วยหลักการย่อยอยู่สามประการด้วยกัน อันได้แก่[54]

---

[52] Herbert L. Packer, "Two Models of the Criminal Process," University of Pennsylvania Law Review 113, 1 (November 1964): 1-68.

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

[54] 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" (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, สาขากฎหมายอาญา คณะนิติศาสตร์, มหาวิทยาลัยธรรมศาสตร์, 2557), หน้า 28-29.

1.) <u>หลักความเหมาะสม หรือหลักความสัมฤทธิ์ผล</u>

การใช้อำนาจรัฐจะต้องเลือกมาตรการที่เหมาะสม กล่าวคือต้องเป็นมาตรการที่ทำให้เจตนารมณ์หรือวัตถุประสงค์ของการใช้อำนาจนั้นสัมฤทธิ์ผล

2.) <u>หลักความจำเป็น</u>

การใช้อำนาจรัฐจะต้องเลือกมาตรการที่เหมาะสม ซึ่งก่อให้เกิดผลกระทบที่น้อยที่สุด กล่าวคือในบรรดามาตรการที่เหมาะสม จะต้องไม่มีมาตรการอื่นที่ให้ผลเช่นเดียวกัน โดยอาจส่งผลกระทบต่อสิทธิขั้นพื้นฐานน้อยกว่า มาตรการนั้นจะถือเป็นมาตรการที่จำเป็นในการใช้อำนาจรัฐ

3.) <u>หลักความได้สัดส่วนในความหมายอย่างแคบ</u>

การใช้อำนาจรัฐจะต้องมีการชั่งน้ำหนักระหว่างประโยชน์มหาชนกับความเสียหายที่อาจเกิดขึ้นต่อปัจเจกชน โดยการใช้อำนาจรัฐจะพึงกระทำต่อเมื่อประโยชน์สาธารณะที่ได้มีน้ำหนักมากกว่าผลร้ายที่เกิดขึ้นการใช้อำนาจรัฐ

2.3 บทสรุป การคุ้มครองข้อมูลส่วนบุคคลและการสืบสวนสอบสวนคดีอาญา

จากการศึกษาแนวคิดว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พบว่าสิทธิในข้อมูลส่วนบุคคลเป็นสิทธิมนุษยชนขั้นพื้นฐานที่มีรากฐานมาจากสิทธิความเป็นส่วนตัว แต่ด้วยผลกระทบจากเทคโนโลยีและระบบคอมพิวเตอร์สมัยใหม่ แนวคิดเกี่ยวกับความเป็นส่วนตัวในข้อมูลจึงมีคำอธิบายที่แตกต่างไปจากสิทธิส่วนบุคคลดั้งเดิม โดยการคุ้มครองข้อมูลส่วนบุคคลจะให้ความสำคัญกับความเป็นอิสระของบุคคลในการควบคุมและตัดสินใจเกี่ยวกับข้อมูลของตนตามหลักความยินยอม (Consent) หรืออีกนัยหนึ่งคือการรับรองให้บุคคลมีอิสระในการปกครองตนเอง (Autonomy) โดยปราศจากการแทรกแซง นอกจากนี้การคุ้มครองข้อมูลส่วนบุคคลยังสัมพันธ์กับแนวคิดการรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์หรือสารสนเทศและการรักษาคุณภาพของข้อมูลอีกด้วย

อย่างไรก็ดี สิทธิในข้อมูลส่วนบุคคลนี้ไม่ใช่สิทธิเด็ดขาด การให้ความคุ้มครองข้อมูลส่วนบุคคลจึงอาจถูกจำกัดลงได้เมื่ออยู่ภายใต้ขอบเขตของการสืบสวนและสอบสวนคดีอาญา เพื่อประโยชน์ในการป้องกันและปราบปรามอาชญากรรม แต่การจำกัดเช่นว่านั้นก็ยังคงต้องอยู่ภายใต้หลักความได้สัดส่วน กล่าวคือรัฐจะต้องเลือกใช้มาตรการที่เหมาะสม ซึ่งก่อให้เกิดผลกระทบที่น้อยที่สุด และประโยชน์สำคัญที่ได้นั้นจะต้องมีน้ำหนักมากกว่าผลร้ายที่จะเกิดขึ้นจากการจำกัดสิทธิและเสรีภาพดังกล่าว

ดังนั้น ความท้าทายของการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาจึงเป็นเรื่องของการรักษาสมดุลระหว่างประโยชน์สาธารณะกับสิทธิความเป็นส่วนตัวในข้อมูลของบุคคลให้ได้สัดส่วนกัน โดยไม่โน้มเอียงไปทางหนึ่งทางใดจนเกินไป

เกี่ยวกับประเด็นดังกล่าว OECD ให้ข้อเสนอแนะอยู่ว่าในสังคมประชาธิปไตย การยกเว้นการให้ความคุ้มครองข้อมูลส่วนบุคคลควรจำกัดให้น้อยที่สุด เท่าที่จำเป็น และการยกเว้นนั้นจะต้องเป็นไปโดยเปิดเผยต่อสาธารณะเป็นการทั่วไป ทั้งนี้ สำหรับการดำเนินงานบางประเภท เช่น การรายงานข้อมูลของธนาคาร รวมถึงการสืบสวนและสอบสวนคดีอาญา รัฐสมาชิกอาจเลือกที่จะสร้างกฎเกณฑ์เฉพาะในการคุ้มครองข้อมูลส่วนบุคคลที่แตกต่างจากหลักเกณฑ์ทั่วไปได้[55]

ข้อเสนอแนะของ OECD จึงไม่เพียงแต่แสดงให้เห็นถึงความเป็นไปได้ที่ในระบบกฎหมายจะมีหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา แต่ยังสะท้อนให้เห็นอีกว่าการสืบสวนและสอบสวนนั้นไม่ใช่ข้อยกเว้นของการคุ้มครองข้อมูลส่วนบุคคลโดยเด็ดขาด เพราะหากมีความจำเป็น รัฐก็อาจบัญญัติกฎเกณฑ์เฉพาะสำหรับการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาให้มีความยืดหยุ่นและเคร่งครัดน้อยกว่าหลักเกณฑ์ทั่วไปได้ เพื่อป้องกันมิให้การให้ความคุ้มครองข้อมูลส่วนบุคคลลดประสิทธิภาพของรัฐในการป้องกันและปราบปรามอาชญากรรม

[55] The OECD Privacy Framework 2013, at Paragraph 4: Exceptions to the Guidelines.

บทที่ 3
การคุ้มครองข้อมูลส่วนบุคคล
ในชั้นสืบสวนและสอบสวนคดีอาญาตามกฎหมายไทย

จุดเปลี่ยนสำคัญของการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยเริ่มต้นขึ้นเมื่อปี พ.ศ. 2540 จากการประกาศใช้รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540 และพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 เนื่องจากรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540 มีการบัญญัติรับรองสิทธิส่วนบุคคลอย่างครบถ้วนครอบคลุมมากที่สุด[56] เมื่อเทียบกับรัฐธรรมนูญฉบับก่อน ๆ ในขณะที่พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 เป็นกฎหมายฉบับแรกของประเทศไทยที่บัญญัตินิยามคำว่า “ข้อมูลข่าวสารส่วนบุคคล” พร้อมกำหนดกฎเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานของรัฐไว้ในหมวด 3 ของพระราชบัญญัตินี้[57]

ต่อมา สิทธิในข้อมูลส่วนบุคคลก็ได้รับการแยกบัญญัติไว้ในรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550 ซึ่งรับรองให้บุคคลมีสิทธิได้รับการคุ้มครองข้อมูลส่วนบุคคลตามที่กฎหมายบัญญัติ[58] อันเป็นการใช้ถ้อยคำแตกต่างจากรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ที่บัญญัติห้ามมิให้นำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าทางใด เว้นแต่มีกฎหมายอนุญาตให้กระทำได้เท่าที่จำเป็นเพื่อประโยชน์สาธารณะ[59] ทั้งนี้ ผู้ช่วยศาสตราจารย์ ดร. นคร เสรีรักษ์ มีความเห็นว่ากฎหมายในที่นี้น่าจะหมายความถึงพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562[60] ซึ่งเป็นกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลฉบับแรกในประเทศไทยที่มีผลใช้บังคับเป็นการทั่วไป ครอบคลุมทุกภาคส่วนทั้งภาครัฐและเอกชน[61] ตั้งแต่วันที่ 1 มิถุนายน พ.ศ. 2565 เป็นต้นมา[62]

---

[56] โปรดดู รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540 มาตรา 34.

[57] นคร เสรีรักษ์, ความเป็นส่วนตัว: ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย, หน้า 239-241.

[58] โปรดดู รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550 มาตรา 35.

[59] โปรดดู รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 มาตรา 32.

[60] นคร เสรีรักษ์, "ความเป็นส่วนตัวภายใต้รัฐธรรมนูญฉบับใหม่ "ต้องจับตา"" [ออนไลน์].

[61] คณาธิป ทองรวีวงศ์, คำอธิบาย หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล, หน้า 50.

[62] โปรดดู พระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2563 และพระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (ฉบับที่ 2) พ.ศ. 2564.

แม้ว่าในปัจจุบัน ประเทศไทยจะมีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นกฎหมายเฉพาะในการคุ้มครองข้อมูลส่วนบุคคล แต่สิทธิในข้อมูลส่วนบุคคลตามพระราชบัญญัติดังกล่าวก็อาจถูกจำกัดลงได้หลายกรณี ซึ่งรวมไปถึงการดำเนินการในชั้นสืบสวนและสอบสวนคดีอาญา ทำให้การคุ้มครองข้อมูลส่วนบุคคลในชั้นนี้จำต้องอาศัยมาตรการทางกฎหมายที่มีอยู่เดิมเป็นหลัก อันได้แก่ หมวด 3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และกฎหมายวิธีพิจารณาความอาญา โดยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะมีผลบังคับใช้ในชั้นสืบสวนและสอบสวนคดีอาญาเพียงบางส่วนเท่านั้น ทั้งที่การสืบสวนและสอบสวนคดีอาญามีการดำเนินงานที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลเป็นจำนวนมาก

ฉะนั้น บทที่ 3 ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาตามกฎหมายไทย จึงสมควรพิจารณาว่าบทบัญญัติกฎหมายที่มีอยู่นั้นอาจให้ความคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาได้มากน้อยเพียงใด และมีข้อจำกัดหรือไม่ อย่างไร เพื่อประเมินถึงความเหมาะสมของการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาของประเทศไทย โดยมีรายละเอียดดังนี้

3.1 กฎหมายวิธีพิจารณาความอาญา

โดยทั่วไป กฎหมายวิธีพิจารณาความอาญา หมายถึง กฎหมายที่ว่าด้วยหลักเกณฑ์และวิธีการค้นหาความจริงเกี่ยวกับการกระทำความผิด รวมถึงการนำตัวผู้กระทำความผิดมาดำเนินคดีและลงโทษ กฎหมายวิธีพิจารณาความอาญาจึงจำเป็นต้องให้อำนาจแก่เจ้าพนักงานในกระบวนการยุติธรรมในการร่วมกันค้นหาความจริงในคดีอาญา[63] ซึ่งในระบบกฎหมายไทย กฎเกณฑ์ดังกล่าวมีบทบัญญัติหลักอยู่ที่ประมวลกฎหมายวิธีพิจารณาความอาญา[64]

อย่างไรก็ตาม มีข้อสังเกตว่าประมวลกฎหมายวิธีพิจารณาความอาญาของไทยจะไม่ได้บัญญัติกฎเกณฑ์การสืบสวนไว้ชัดแจ้ง แต่ปล่อยให้เป็นไปตามระเบียบปฏิบัติภายใน เพื่อให้เกิดความคล่องตัว เพราะการสืบสวนอาจจำเป็นต้องกระทำในทางลับและมีเทคนิคเฉพาะตัว[65] ในขณะที่กฎเกณฑ์ว่าด้วยการสอบสวนจะถูกบัญญัติอยู่ในภาค 2 ประมวลกฎหมายวิธีพิจารณาความอาญา ซึ่งบัญญัติถึงอำนาจทั่วไปของเจ้าพนักงานสอบสวนไว้ว่า

---

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

[64] เรื่องเดียวกัน, หน้า 16-18.

[65] เรื่องเดียวกัน, หน้า 126.

> “ให้พนักงานสอบสวนรวบรวมหลักฐานทุกชนิด เท่าที่สามารถจะทำได้ เพื่อประสงค์จะทราบข้อเท็จจริง และพฤติการณ์ต่าง ๆ อันเกี่ยวกับความผิดที่ถูกกล่าวหา เพื่อจะรู้ตัวผู้กระทำผิดและพิสูจน์ให้เห็นความผิดหรือความบริสุทธิ์ของผู้ต้องหา”[66]

จะเห็นได้ว่าพนักงานสอบสวนมีอำนาจหน้าที่ในการรวบรวมหลักฐานทุกชนิด โดยไม่จำกัดว่าพยานหลักฐานจะเป็นคุณหรือเป็นโทษแก่ผู้ถูกกล่าวหา[67] และไม่ว่าพยานหลักฐานนั้นจะเป็นพยานวัตถุ พยานเอกสาร หรือพยานบุคคล โดยอาจใช้อำนาจได้ดังต่อไปนี้

1.) อำนาจทั่วไปในการรวบรวมพยานหลักฐาน (มาตรา 132) ได้แก่
    1.1.) อำนาจตรวจ (มาตรา 132 (1))
    1.2.) อำนาจค้น (มาตรา 132 (2)) แบ่งได้อีกสามประเภท[68] คือ
        1.2.1.) อำนาจค้นที่รโหฐาน
        1.2.2.) อำนาจค้นตัวบุคคล
        1.2.3.) อำนาจค้นเอกสารทางไปรษณีย์โทรเลข
    1.3.) อำนาจเรียก (มาตรา 132 (3))
    1.4.) อำนาจยึด (มาตรา 132 (4))
2.) อำนาจในการตรวจพิสูจน์ด้วยวิธีการทางวิทยาศาสตร์ (มาตรา 131/1)
3.) อำนาจในการสอบสวนผู้ต้องหา (มาตรา 134)
4.) อำนาจในการถามปากคำผู้เสียหายหรือพยาน (มาตรา 133)
5.) อำนาจอื่นใดตามที่กฎหมายบัญญัติ

ภายหลังรวบรวมพยานหลักฐาน เจ้าพนักงานสอบสวนจะต้องทำบันทึกการสอบสวน และให้เอาบันทึกเอกสารรวมเข้าสำนวนไว้ แต่หากพยานหลักฐานเป็นสิ่งของอื่นก็ให้บัญชีรายละเอียดรวมเข้าสำนวนแทน โดยเจ้าพนักงานสอบสวนอาจบันทึกรายชื่อ ที่อยู่ หมายเลขโทรศัพท์ของพยานบุคคลเก็บไว้ในที่ทำการ เพื่อประโยชน์ในการติดตามพยานให้ไปตามกำหนดนัดของศาลได้[69]

---

[66] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 131.

[67] พยานหลักฐานที่เป็นคุณย่อมมีความหมายครอบคลุมทั้งพยานหลักฐานที่พิสูจน์ความบริสุทธิ์ และพยานหลักฐานที่แสดงเหตุลดโทษหรือเหตุบรรเทาโทษ (โปรดดู ธานิศ เกศวพิทักษ์, คำอธิบาย ประมวลกฎหมายวิธีพิจารณาความอาญา เล่ม 1, หน้า 256-257.)

[68] ณรงค์ ใจหาญ, หลักกฎหมายวิธีพิจารณาความอาญา เล่ม 1, หน้า 311.

[69] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 139.

นอกเหนือจากอำนาจตามประมวลกฎหมายวิธีพิจารณาความอาญา เจ้าพนักงานของรัฐอาจมีอำนาจพิเศษในการสืบสวนและสอบสวนคดีอาญาบางประเภทตามพระราชบัญญัติเฉพาะอีกด้วย อาทิ อำนาจในการสะกดรอย โดยเครื่องมือสื่อสารโทรคมนาคม เครื่องมืออิเล็กทรอนิกส์ หรือวิธีการอื่นใด[70] อำนาจในการเรียกข้อมูลจราจรทางคอมพิวเตอร์หรือข้อมูลเกี่ยวกับผู้ใช้บริการจากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์[71] และอำนาจในการเข้าถึงหรือได้มาซึ่งข้อมูลข่าวสารที่ส่งผ่านสิ่งติดต่อสื่อสาร ไม่ว่าจะเป็นไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ อุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยี[72] ทั้งนี้ เพื่อประโยชน์ในการดำเนินคดีต่อความผิดที่มีลักษณะสลับซับซ้อนหรือความผิดที่มีผลกระทบร้ายแรงต่อสังคมเป็นสำคัญ

ด้วยเหตุนี้ จึงอาจสรุปได้ว่ากฎหมายวิธีพิจารณาความอาญาของไทยนั้นมีที่มาจากทั้งประมวลกฎหมายวิธีพิจารณาความอาญาและพระราชบัญญัติเฉพาะ อย่างไรก็ดี โดยที่การใช้อำนาจสืบสวนและสอบสวนคดีอาญาตามกฎหมายต่าง ๆ ข้างต้นมีผลเป็นการก้าวล่วงสิทธิและเสรีภาพของบุคคล การใช้อำนาจดังกล่าวจึงอยู่ในบังคับที่จะต้องปฏิบัติตามหลักเกณฑ์และวิธีการที่กำหนดไว้ให้ถูกต้องครบถ้วน เพื่อสอดคล้องหลักประกันสิทธิและเสรีภาพภายใต้รัฐธรรมนูญแห่งราชอาณาจักรไทย ซึ่งรวมถึงสิทธิในข้อมูลส่วนบุคคล โดยมีกฎเกณฑ์ที่เกี่ยวข้องดังนี้

3.1.1 ขอบเขตของข้อมูลส่วนบุคคล

จากการศึกษาพบว่ากฎหมายวิธีพิจารณาความอาญาของไทยนั้นไม่ได้มีการบัญญัตินิยามของข้อมูลส่วนบุคคลไว้แต่ประการใด เนื่องจากเจตนารมณ์ของกฎหมายวิธีพิจารณาความอาญาคือการให้อำนาจเจ้าหน้าที่รัฐควบคู่กับการจำกัดการใช้อำนาจ เพื่อสร้างหลักประกันสิทธิในกระบวนการยุติธรรมโดยทั่วไป มิได้คุ้มครองเฉพาะข้อมูลส่วนบุคคล การกำหนดขอบเขตของข้อมูลส่วนบุคคลจึงต้องอาศัยการตีความบทกฎหมายอื่นแทน ซึ่งปัจจุบัน มีกฎหมายเพียงสองฉบับที่บัญญัตินิยามดังกล่าวไว้ ได้แก่ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งจะได้กล่าวรายละเอียดในหัวข้อที่ 3.2.1 ต่อไป

---

[70] โปรดดู พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 มาตรา 21.

[71] โปรดดู พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 มาตรา 18 (2) และ (3).

[72] โปรดดู พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 25 และพระราชบัญญัติป้องกันและปราบปรามการค้ามนุษย์ พ.ศ. 2551 มาตรา 30 และพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 มาตรา 17.

3.1.2 หลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคล

เมื่อกฎหมายวิธีพิจารณาความอาญามิได้มุ่งคุ้มครองสิทธิในข้อมูลส่วนบุคคล จึงไม่ปรากฏว่ากฎหมายวิธีพิจารณาความอาญามีบทบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลอย่างเฉพาะเจาะจง แต่ถึงกระนั้น กฎหมายวิธีพิจารณาความอาญาก็มีการบัญญัติหลักเกณฑ์และวิธีการ อันเป็นกรอบการใช้อำนาจสืบสวนและสอบสวนคดีอาญาอยู่เป็นจำนวนมาก จึงสมควรศึกษาว่ากรอบการใช้อำนาจตามกฎหมายวิธีพิจารณาความอาญาของไทยนั้นอาจปกป้องมิให้ข้อมูลส่วนบุคคลถูกล่วงละเมิดเกินกว่าที่จำเป็นเพื่อประโยชน์สาธารณะได้มากน้อยเพียงใด โดยมีรายละเอียดดังนี้

3.1.2.1 การเก็บรวบรวมข้อมูลส่วนบุคคล

ในภาพรวม กรอบการใช้อำนาจสืบสวนและสอบสวนคดีอาญาที่เกี่ยวข้องกับการเก็บรวบรวมข้อมูลตามกฎหมายวิธีพิจารณาความอาญาอาจจำแนกได้เป็นสามรูปแบบใหญ่ด้วยกัน คือ

รูปแบบที่หนึ่ง การกำหนดเหตุแห่งการใช้อำนาจ โดยระบุสถานการณ์ที่เจ้าพนักงานสืบสวนสอบสวนอาจใช้อำนาจในการเก็บรวบรวมข้อมูลส่วนบุคคลได้ อาทิ

- การใช้อำนาจทั่วไป ได้แก่ การตรวจ การค้น การเรียก และการยึด ให้กระทำได้เพื่อประโยชน์ในการรวบรวมพยานหลักฐาน[73]
- การแจ้งข้อหาและการสอบสวนผู้ต้องหาจะกระทำได้ต่อเมื่อมีหลักฐานตามสมควรว่าผู้นั้นน่าจะได้กระทำผิดตามข้อกล่าวหา[74]
- การตรวจตัวผู้เสียหายจะกระทำได้เมื่อได้รับความยินยอม[75]
- การค้นที่รโหฐานจำต้องมีคำสั่งหรือหมายของศาลเสมอ เว้นแต่ปรากฏเหตุยกเว้นอย่างหนึ่งอย่างใดตามกฎหมาย[76] และในการออกหมายค้นก็จะต้องปรากฏพยานหลักฐานตามสมควรที่ทำให้ศาลเชื่อว่ามีเหตุในการออกหมายค้นตามที่กฎหมายบัญญัติ[77]
- การค้นตัวบุคคลในที่สาธารณสถานจะกระทำได้เมื่อมีเหตุอันควรสงสัยตามที่กฎหมายกำหนด[78]

---

[73] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 132.

[74] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 134 วรรคสอง.

[75] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 132 (1).

[76] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 92.

[77] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 59/1 ประกอบกับมาตรา 69.

[78] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 93.

- การค้นเอกสารทางไปรษณีย์โทรเลขจะกระทำได้ต่อเมื่อมีคำสั่งศาล โดยการได้มาซึ่งเอกสารจะต้องเป็นประโยชน์แก่การดำเนินคดี และต้องมิใช่เอกสารระหว่างผู้ต้องหาหรือจำเลยกับทนายความ[79]
- การตรวจพิสูจน์ทางวิทยาศาสตร์ ด้วยวิธีการตรวจเก็บส่วนประกอบของร่างกายจะกระทำได้เฉพาะในคดีที่มีอัตราโทษจำคุกอย่างสูงเกินสามปี รวมถึงต้องได้รับความยินยอมจากผู้ถูกตรวจ[80]
- การออกหมายเรียกพยานบุคคลมาให้ถ้อยคำจะกระทำได้หากมีเหตุอันควรเชื่อว่าถ้อยคำของบุคคลดังกล่าวอาจเป็นประโยชน์แก่คดี[81]
- การเรียกข้อมูลจราจรทางคอมพิวเตอร์หรือข้อมูลเกี่ยวกับผู้ใช้บริการจากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์จะกระทำได้ต่อเมื่อมีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือในกรณีที่มีการร้องขอจากพนักงานสอบสวน เมื่อมีข้อมูลหรือระบบคอมพิวเตอร์เกี่ยวข้องกับการกระทำความผิดอาญาตามกฎหมายอื่น[82]
- การได้มาซึ่งเอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางสิ่งสื่อสารจะต้องมีเหตุอันควรเชื่อได้ว่าเอกสารหรือข้อมูลข่าวสารนั้นถูกใช้หรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิด โดยพนักงานเจ้าหน้าที่จะต้องยื่นคำขอฝ่ายเดียวต่อศาลเพื่อมีคำสั่งอนุญาตให้ได้มา[83]
- การสะกดรอยด้วยเครื่องมือสื่อสารโทรคมนาคม เครื่องมืออิเล็กทรอนิกส์ หรือด้วยวิธีการอื่นจะต้องมีเหตุจำเป็นเพื่อการสืบสวน จับกุม แสวงหาและรวบรวมพยานหลักฐานในการดำเนินคดีฐานกระทำหรือจะกระทำความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ[84]

รูปแบบที่สอง การกำหนดวิธีการใช้อำนาจ โดยระบุขั้นตอนในการเก็บรวบรวมข้อมูลว่าต้องดำเนินการเช่นไร มีขอบเขตหรือข้อจำกัดอย่างไรบ้าง เช่น

---

[79] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 105.

[80] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 131/1 วรรคสอง.

[81] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 133 วรรคแรก.

[82] โปรดดู มาตรา 18 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560.

[83] โปรดดู พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 25 และพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 มาตรา 17 และพระราชบัญญัติป้องกันและปราบปรามการค้ามนุษย์ พ.ศ. 2551 มาตรา 30.

[84] โปรดดู พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 มาตรา 21.

- การตรวจผู้เสียหายหรือผู้ต้องหาซึ่งเป็นหญิง ให้เจ้าพนักงานซึ่งเป็นหญิงหรือหญิงอื่นเป็นผู้ตรวจ โดยหญิงผู้ถูกตรวจอาจร้องขอให้มีบุคคลอื่นใดมาอยู่ร่วมในการตรวจ[85]
- การค้นที่รโหฐานให้กระทำได้เฉพาะในเวลากลางวัน เว้นแต่มีเหตุยกเว้นตามกฎหมาย[86] และให้ค้นเฉพาะเพื่อหาตัวคนหรือสิ่งของที่ต้องการค้น[87] โดยก่อนลงมือค้น ต้องแจ้งข้อความในหมาย[88] และแสดงความบริสุทธิ์เท่าที่จะกระทำได้ คือให้ค้นต่อหน้าผู้ครอบครองสถานที่ หากไม่มีบุคคลดังกล่าว ให้ค้นต่อหน้าพยานอย่างน้อยสองคนแทน[89]
- การค้นบุคคลในที่สาธารณสถานต้องกระทำโดยเจ้าพนักงานผู้มีอำนาจ[90]
- การตรวจพิสูจน์ทางวิทยาศาสตร์ ด้วยวิธีการเก็บตรวจส่วนประกอบของร่างกายให้กระทำเท่าที่จำเป็นและสมควร โดยใช้วิธีการที่ไม่เป็นอันตรายและก่อให้เกิดความเจ็บปวดน้อยที่สุดเท่าที่จะกระทำได้[91]
- การสอบสวนผู้ต้องหา ให้แจ้งข้อหาประกอบกับข้อเท็จจริงเกี่ยวกับการกระทำผิด[92] โดยเจ้าพนักงานสอบสวนต้องแจ้งสิทธิต่าง ๆ ให้ผู้ต้องหาทราบและดำเนินการให้เป็นไปตามสิทธิดังกล่าว[93] ทั้งนี้ ห้ามมิให้มีการถามคำให้การ ในลักษณะที่เป็นการให้คำมั่นสัญญา ขู่เข็ญ หลอกลวง ทรมาน ใช้กำลังบังคับ หรือกระทำโดยมิชอบประการใด[94]
- การถามปากคำผู้เสียหายหรือพยาน ห้ามมิให้ตักเตือน พูดให้ท้อใจ หรือใช้กลอุบายอื่นใดเพื่อป้องกันมิให้บุคคลให้ถ้อยคำ[95]
- ในกรณีที่ผู้เสียหาย พยาน หรือผู้ต้องหาเป็นเด็กอายุไม่เกินสิบแปดปี ให้พนักงานสอบสวนใช้วิธีการที่บัญญัติไว้ในกฎหมายเป็นพิเศษ[96]

---

[85] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 132 (1).

[86] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 96.

[87] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 98.

[88] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 62.

[89] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 102.

[90] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 93.

[91] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 131/1 วรรคสอง.

[92] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 134 วรรคแรก.

[93] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 134/1–134/4.

[94] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 135.

[95] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 133.

รูปแบบที่สาม การตรวจสอบถ่วงดุลโดยองค์กรภายนอกที่เป็นกลาง โดยทั่วคือการให้ศาลตรวจสอบเหตุแห่งการใช้อำนาจก่อนที่จะออกหมายของศาลหรือมีคำสั่งอนุญาตให้ดำเนินการ ซึ่งปัจจุบัน ประมวลกฎหมายวิธีพิจารณาความอาญากำหนดให้มีการตรวจสอบถ่วงดุลดังกล่าวอยู่เพียงสองกรณี ได้แก่ การค้นในที่รโหฐาน และการค้นเอกสารทางไปรษณีย์โทรเลข

นอกจากนี้ การได้มาซึ่งเอกสารหรือข้อมูลข่าวสารที่ส่งผ่านสิ่งติดต่อสื่อสารโดยอาศัยอำนาจตามพระราชบัญญัติเฉพาะอื่น ๆ ก็ต้องได้รับคำสั่งอนุญาตจากศาลเช่นกัน ซึ่งในการสั่งอนุญาตศาลจะต้องพิจารณาถึงผลกระทบต่อสิทธิส่วนบุคคลหรือสิทธิอื่นใด ประกอบเหตุผลกับความจำเป็นในการสืบสวนและสอบสวน เช่น มีเหตุอันควรเชื่อว่าจะมีหรือมีการกระทำความผิด หรือเหตุอันควรเชื่อว่าจะได้ข้อมูลข่าวสารเกี่ยวกับการกระทำผิด หรือไม่อาจใช้วิธีที่มีประสิทธิภาพกว่านั้นได้ โดยศาลจะสั่งอนุญาตได้คราวละไม่เกิน 90 วัน และอาจกำหนดเงื่อนไขใด ๆ ไปพร้อมคำสั่งอนุญาตได้[97] ในขณะที่การสะกดรอยด้วยเครื่องมือสื่อสารโทรคมนาคม เครื่องมืออิเล็กทรอนิกส์ หรือด้วยวิธีการอื่นใด จะเป็นการอนุญาตโดยอัยการสูงสุด ผู้บัญชาการตำรวจแห่งชาติ หรือผู้ได้รับมอบหมายแล้วแต่กรณี[98]

3.1.2.2 การใช้และเปิดเผยข้อมูลส่วนบุคคล

สำหรับการใช้และเปิดเผยข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา พบว่าประมวลกฎหมายวิธีพิจารณาความอาญาไม่ได้มีการบัญญัติหลักเกณฑ์การใช้และเปิดเผยข้อมูลที่ได้มาในชั้นสืบสวนและสอบสวนเอาไว้โดยชัดแจ้ง ทั้งยังไม่ปรากฏบทกำหนดความรับผิดสำหรับการใช้หรือเปิดเผยข้อมูลที่ได้มาโดยมิชอบ จะมีเพียงระเบียบปฏิบัติที่ห้ามมิให้เจ้าหน้าที่ตำรวจอนุญาตหรือจัดให้สื่อมวลชนถ่ายภาพ สัมภาษณ์ หรือให้ข่าวของผู้เสียหายและผู้ต้องหาในระหว่างควบคุมตัว รวมทั้งภาพที่มีลักษณะอุจาดหรือทารุณโหดร้าย หรือล่วงละเมิดสิทธิบุคคลตามคำสั่งสำนักงานตำรวจแห่งชาติ[99]

---

[96] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 133 ทวิ และมาตรา 134/2.

[97] โปรดดู พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 25 และพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 มาตรา 17 และพระราชบัญญัติป้องกันและปราบปรามการค้ามนุษย์ พ.ศ. 2551 มาตรา 30 และพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มาตรา 46.

[98] โปรดดู พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 มาตรา 21 ประกอบกับข้อบังคับของอัยการสูงสุดว่าด้วยการสะกดรอยผู้ต้องสงสัย ตามพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 มาตรา 21 พ.ศ. 2556.

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

ในทางกลับกัน หากพิจารณาพระราชบัญญัติเฉพาะ จะพบว่าพระราชบัญญัติเฉพาะมีหลักเกณฑ์การใช้และเปิดเผยข้อมูลที่ได้มาจากการสืบสวนและสอบสวนคดีอาญาอยู่บ้าง โดยเฉพาะกรณีการได้มาซึ่งเอกสารหรือข้อมูลซึ่งส่งทางสิ่งสื่อสารหรือโดยใช้เทคนิคพิเศษต่าง ๆ

ยกตัวอย่างเช่น พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 กำหนดว่าการใช้ประโยชน์จากข้อมูลข่าวสารในสิ่งสื่อสารซึ่งได้มาในคดีพิเศษ จะต้องเป็นไปเพื่อการสืบสวนหรือใช้เป็นพยานหลักฐานเฉพาะในการดำเนินคดีพิเศษที่ได้รับอนุญาตตามคำสั่งศาลเท่านั้น[100] และห้ามมิให้มีการเปิดเผยข้อมูลข่าวสารนั้นโดยมิชอบ มิฉะนั้น ก็อาจมีความรับผิดอาญา โดยให้ระวางโทษเพิ่มเป็นสามเท่าในกรณีที่ผู้ฝ่าฝืนเป็นเจ้าพนักงานซึ่งมีอำนาจหน้าที่[101] ในทำนองเดียวกัน พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 กำหนดให้ผู้ที่ทำการสะกดรอยเพื่อแสวงหาประโยชน์อันมิชอบ นอกเหนือวัตถุประสงค์ตามพระราชบัญญัตินี้ จะไม่ได้รับการคุ้มครอง และหากการกระทำนั้นเป็นความผิดอาญา ก็ให้ระวางโทษเป็นสองเท่าของโทษที่กำหนดไว้[102] เป็นต้น ซึ่งนอกเหนือจากตัวอย่างข้างต้น ยังมีพระราชบัญญัติเฉพาะอื่น ๆ อีกจำนวนหนึ่งที่บัญญัติหลักเกณฑ์ในลักษณะนี้ เพียงแต่จะมีความแตกต่างกันในรายละเอียด อาทิ อัตราโทษต่างกัน หรือพระราชบัญญัติบางฉบับก็ไม่มีการเพิ่มโทษในกรณีที่ผู้ฝ่าฝืนเป็นเจ้าพนักงาน[103]

อย่างไรก็ตาม กรณีที่เป็นการโอนข้อมูลไปยังต่างประเทศในชั้นสืบสวนและสอบสวน ไม่พบว่ากฎหมายวิธีพิจารณาความอาญาของไทยมีการกำหนดหลักเกณฑ์เกี่ยวกับประเด็นนี้ไว้ชัดแจ้ง และแม้พระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. 2535 จะบัญญัติกฎเกณฑ์การส่งมอบพยานหลักฐาน เอกสาร หรือข่าวสารไปยังต่างประเทศ เมื่อได้รับคำร้องขอความช่วยเหลือ แต่บทบัญญัติเหล่านั้นก็มิได้มีเจตนารมณ์เพื่อคุ้มครองข้อมูลส่วนบุคคลแต่อย่างใด[104]

3.1.2.3 การเก็บรักษาข้อมูลส่วนบุคคล

ในทำนองเดียวกันกับการใช้และเปิดเผยข้อมูลส่วนบุคคล ไม่พบว่าประมวลกฎหมายวิธีพิจารณาความอาญาได้บัญญัติกฎเกณฑ์การเก็บรักษาข้อมูลส่วนบุคคลไว้ แต่ในทางปฏิบัติ พบว่ามีการเก็บรักษาและทำลายสำนวนการสืบสวนสอบสวนตามระเบียบปฏิบัติภายใน อาทิ คำสั่งสำนักงาน

---

[100] โปรดดู พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 25.

[101] โปรดดู พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 26 ประกอบกับมาตรา 39.

[102] โปรดดู พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 มาตรา 21 ประกอบกับมาตรา 30.

[103] มติชนออนไลน์, "เปิดร่าง ป.วิอาญา 'ดักฟัง' อัยการเทียบเนื้อหา พ.ร.บ. 7 ฉบับ ชี้ข้อมูลลักลั่น" [ออนไลน์] เข้าถึงเมื่อ 20 กุมภาพันธ์ 2565. แหล่งที่มา: https://www.matichon.co.th/local/crime/news_552146.

[104] โปรดดู พระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. 2535 ส่วนที่ 2 และ 3.

ตำรวจแห่งชาติที่ 419/2556 กำหนดให้หัวหน้างานสอบสวนเป็นผู้รับผิดชอบในการเก็บรักษาสำนวนการสอบสวนมิให้สูญหายและอยู่ในสภาพที่เรียบร้อย โดยสำนวนการสอบสวนจะถูกทำลายลง เมื่อคดีขาดอายุความ เว้นแต่สำนวนชันสูตรพลิกศพที่ผู้ว่าราชการจังหวัดส่งมาเก็บ ให้ทำลายเมื่อครบกำหนด 20 ปี นับแต่วันที่ได้รับแจ้งการตาย[105] เป็นต้น

สำหรับกรณีการได้มาซึ่งเอกสารหรือข้อมูลที่ส่งทางสิ่งสื่อสาร โดยอาศัยอำนาจตามพระราชบัญญัติเฉพาะ พบว่ามีกฎเกณฑ์ในการเก็บรักษาเอกสารหรือข้อมูลข่าวสารที่ได้ในชั้นสืบสวนและสอบสวน โดยกำหนดให้พนักงานเจ้าหน้าที่เก็บรักษาเฉพาะเอกสารหรือข้อมูลข่าวสารที่เกี่ยวกับการกระทำความผิด[106] นอกจากนี้ พระราชบัญญัติบางฉบับ เช่น พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 และพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 มีบทบัญญัติบังคับให้ทำลายเอกสารหรือข้อมูลข่าวสารอื่นที่ไม่เกี่ยวข้องอีกด้วย[107]

3.1.2.4 สิทธิของเจ้าของข้อมูลส่วนบุคคล

แม้ว่าประมวลกฎหมายวิธีพิจารณาความอาญามีบทบัญญัติรับรองสิทธิในชั้นสืบสวนและสอบสวนคดีอาญาอยู่หลายประการ ตั้งแต่สิทธิในการพบและปรึกษาทนายความ สิทธิที่จะให้การหรือไม่ก็ได้ สิทธิที่จะให้ทนายความหรือผู้ซึ่งตนไว้วางใจเข้าร่วมการสอบปากคำ[108] ตลอดจนสิทธิในการตรวจดู คัดสำเนา หรือถ่ายรูปสิ่งที่ยื่นเป็นพยานหลักฐาน[109] ฯลฯ ทว่าสิทธิเหล่านี้เป็นสิทธิที่ถูกกำหนดเพื่อให้เกิดความเป็นธรรมในการดำเนินกระบวนการยุติธรรมทางอาญาเป็นสำคัญ จึงมิได้มีลักษณะเป็นการรับรองสิทธิบุคคลในฐานะเจ้าของข้อมูลส่วนบุคคล

3.1.2.5 สภาพบังคับและบทกำหนดโทษ

เมื่อมีการฝ่าฝืนหลักเกณฑ์และวิธีการที่บัญญัติไว้ในกฎหมายวิธีพิจารณาความอาญาโดยหลัก ข้อมูลข่าวสารซึ่งได้มาจากการฝ่าฝืนย่อมเป็นพยานหลักฐานที่ได้มาโดยไม่ชอบด้วยกฎหมายในแง่ของการพิจารณาคดี ศาลจึงต้องปฏิเสธไม่รับฟังข้อมูลข่าวสารดังกล่าว เว้นแต่ศาลใช้ดุลพินิจรับฟังตามมาตรา 226/1 ประมวลกฎหมายวิธีพิจารณาความอาญา

---

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

[106] โปรดดู พระราชบัญญัติป้องกันและปราบปรามการค้ามนุษย์ พ.ศ. 2551 มาตรา 30.

[107] โปรดดู พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 25 และพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 มาตรา 17.

[108] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 134/4.

[109] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 8.

ในแง่ของความรับผิด ประมวลกฎหมายวิธีพิจารณาความอาญาไม่ได้มีบทกำหนดโทษสำหรับการเก็บรวบรวม ใช้ เปิดเผย หรือการเก็บรักษาข้อมูลข่าวสารโดยมิชอบ ขณะที่พระราชบัญญัติเฉพาะก็มีการบัญญัติความรับผิดอาญาเฉพาะกรณีการเปิดเผยข้อมูลข่าวสารโดยไม่ชอบเท่านั้น ดังนั้น ความรับผิดในกรณีอื่น ๆ จึงอาจต้องอาศัยการปรับใช้ความผิดฐานเจ้าพนักงานปฏิบัติหน้าที่โดยมิชอบตามมาตรา 157 ประมวลกฎหมายอาญา ซึ่งเป็นบททั่วไปแทน และหากเกิดความเสียหาย ผู้เสียหายก็จะมีสิทธินำคดีไปฟ้องร้องทางแพ่งเพื่อให้มีการเยียวยาทางแพ่งต่อไป

3.2 กฎหมายคุ้มครองข้อมูลส่วนบุคคล

ปัจจุบัน หน่วยงานของรัฐในประเทศไทยมีหน้าที่ต้องปฏิบัติตามกฎเกณฑ์ว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายสองฉบับ คือ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เนื่องจากการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มิได้มีผลเป็นการยกเลิกกฎเกณฑ์การคุ้มครองข้อมูลข่าวสารส่วนบุคคลในพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ทำให้เกิดความซ้อนทับในการบังคับใช้กฎหมายในประเด็นเดียวกัน คือการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความรับผิดชอบของหน่วยงานรัฐ[110]

อย่างไรก็ดี หากเปรียบเทียบขอบเขตการบังคับใช้ของพระราชบัญญัติทั้งสองฉบับ จะพบว่าการสืบสวนและสอบสวนยังอยู่ภายใต้พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 แตกต่างจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่การคุ้มครองข้อมูลส่วนบุคคลอาจถูกจำกัดลงเพื่อประโยชน์ในการสืบสวนและสอบสวนคดีอาญาได้ด้วยกันสองลักษณะ[111] อันได้แก่

กรณีที่หนึ่ง การยกเว้นไม่ให้กิจกรรมบางประเภทอยู่ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลตามมาตรา 4 ซึ่งเป็นการยกเว้นเพื่อระบุขอบเขตเชิงสาระของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไม่ให้ใช้บังคับแก่การดำเนินการบางลักษณะ[112] โดยมีบทบัญญัติที่เกี่ยวข้องกับการสืบสวนและสอบสวนคดีอาญา ดังนี้

---

[110] บุญชู ณ ป้อมเพชร, "คำอธิบายกฎหมายข้อมูลข่าวสารของราชการ."

[111] คณาธิป ทองรวีวงศ์, "สิทธิในข้อมูลส่วนบุคคลที่ไม่ได้รับการคุ้มครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 : การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามกฎหมายเกี่ยวกับความมั่นคงของรัฐ," วารสารกฎหมายสิทธิมนุษยชน 1, 1 (มกราคม - เมษายน 2563).

[112] คณาธิป ทองรวีวงศ์, คำอธิบาย หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล, หน้า 50-52.

1.) มาตรา 4 (2) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
กำหนดว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะไม่นำไปใช้บังคับแก่การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลัง การรักษาความปลอดภัยของประชาชน การป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ การรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งสำนักงานตำรวจแห่งชาติเห็นว่าหน่วยงานในสังกัดตำรวจถูกยกเว้นตามมาตรานี้[113] การสืบสวนและสอบสวนคดีอาญาซึ่งดำเนินการโดยหน่วยงานในสังกัดตำรวจจึงน่าจะอยู่ในขอบเขตของบทยกเว้นตามมาตรา 4 (2) กรณีหนึ่ง

2.) มาตรา 4 (5) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
กำหนดว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะไม่นำไปใช้บังคับแก่การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา จึงอาจพิจารณาได้ว่าการสืบสวนและสอบสวนอยู่ในขอบเขตของบทยกเว้นตามมาตรา 4 (5) อีกกรณีหนึ่ง ในฐานะที่เป็นส่วนหนึ่งของการดำเนินงานตามกระบวนการยุติธรรมอาญา

มีข้อสังเกตว่า การดำเนินการที่ได้รับยกเว้นตามมาตรา 4 (2) และ (5) ต้องพิจารณาจากปัจจัยด้านองค์กรประกอบกับวัตถุประสงค์ของกิจกรรม กล่าวคือ การดำเนินการต่อข้อมูลส่วนบุคคลที่ได้รับยกเว้นนั้นจะต้องเป็นการดำเนินการโดยหน่วยงานของรัฐ (ปัจจัยด้านองค์กร) และเป็นการดำเนินการตามอำนาจหน้าที่ตามกฎหมาย เพื่อรักษาความมั่นคงของรัฐหรือเป็นการดำเนินกระบวนการยุติธรรมอาญา (ปัจจัยด้านวัตถุประสงค์)[114] หากขาดปัจจัยอย่างใดอย่างหนึ่ง การดำเนินการดังกล่าวย่อมไม่ถือเป็นการดำเนินการที่ได้รับการยกเว้นตามบทบัญญัติมาตรา 4

โดยผลของการยกเว้นตามมาตรา 4 คือการดำเนินการต่อข้อมูลส่วนบุคคลนั้นจะได้รับยกเว้นจากหน้าที่ทั่วไปในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แต่ยังคงมีหน้าที่ในการรักษาความมั่นคงปลอดภัยตามมาตรา 37 ให้เป็นไปตามมาตรฐานของประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565[115]

---

[113] กลุ่มงานตรวจสอบและควบคุมมาตรฐานทางเทคโนโลยี กองบังคับการสนับสนุนทางเทคโนโลยี สำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานตำรวจแห่งชาติ, "เอกสารประกอบการเตรียมความพร้อม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562."

[114] คณาธิป ทองรวีวงศ์, คำอธิบาย หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล, หน้า 53-58 และ 60.

[115] เรื่องเดียวกัน, 63-64.

กรณีที่สอง การยกเว้นให้การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลสามารถกระทำได้โดยไม่ต้องอาศัยความยินยอม ตามมาตรา 24 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

การยกเว้นตามมาตรา 24 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไม่ได้ยกเว้นการใช้บังคับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ดังเช่นมาตรา 4 แต่เป็นการยกเว้นให้ผู้ประกอบการภาคเอกชนเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล แล้วส่งให้หน่วยงานของรัฐโดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เนื่องจากเป็นกรณีที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24 (6) กำหนดว่าเป็นการปฏิบัติหน้าที่ตามกฎหมาย[116]

ด้วยเหตุนี้ การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาของประเทศไทยจึงต้องอาศัยกฎเกณฑ์ในหมวด 3 ของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 เป็นหลักและอยู่ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เฉพาะในส่วนการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลเท่านั้น โดยอาจสรุปหลักเกณฑ์ที่เกี่ยวข้องได้ดังต่อไปนี้

3.2.1 ขอบเขตของข้อมูลส่วนบุคคล

เมื่อข้อมูลส่วนบุคคลเป็นวัตถุแห่งสิทธิที่กฎหมายมุ่งคุ้มครอง จึงจำเป็นต้องพิจารณาเสียก่อนว่าข้อมูลส่วนบุคคลมีความหมายว่าอย่างไร เพื่อประโยชน์ในการจำแนกว่าข้อมูลใดที่ได้รับความคุ้มครอง ซึ่งในระบบกฎหมายไทย นิยามของข้อมูลส่วนบุคคลปรากฏอยู่ในกฎหมายสองฉบับ คือพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

อย่างไรก็ดี การกำหนดขอบเขตของข้อมูลส่วนบุคคลในหัวข้อนี้เป็นเพียงเกณฑ์การพิจารณาว่าข้อมูลลักษณะใดที่ได้รับความคุ้มครองตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยไม่มีผลต่อการให้ความคุ้มครองตามกฎหมายวิธีพิจารณาความอาญาแต่อย่างใด

3.2.1.1 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 บัญญัติคำว่า “ข้อมูลข่าวสารส่วนบุคคล” ขึ้นพร้อมกำหนดนิยามให้หมายความว่า[117]

---

[116] คณาธิป ทองรวีวงศ์, "สิทธิในข้อมูลส่วนบุคคลที่ไม่ได้รับการคุ้มครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 : การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามกฎหมายเกี่ยวกับความมั่นคงของรัฐ," วารสารกฎหมายสิทธิมนุษยชน.

[117] พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มาตรา 4 และมาตรา 24.

> “ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้นหรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึก ลักษณะเสียงของคนหรือรูปถ่าย และให้หมายความรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย”

> “เพื่อประโยชน์แห่งหมวดนี้ "บุคคล" หมายความว่า บุคคลธรรมดาที่มีสัญชาติไทย และบุคคลธรรมดาที่ไม่มีสัญชาติไทยแต่มีถิ่นที่อยู่ในประเทศไทย”

ข้อมูลข่าวสารส่วนบุคคลพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 จึงมีองค์ประกอบอยู่สองประการด้วยกัน กล่าวคือ การมีข้อเท็จจริงที่เป็นสิ่งเฉพาะตัวของบุคคล และการมีสิ่งชี้ตัวบุคคล คือทำให้รู้ได้ว่าสิ่งเฉพาะตัวนั้นเป็นของบุคคลใด[118] โดยบุคคลในที่นี้จะหมายความเฉพาะบุคคลธรรมดา ไม่ว่าถึงแก่กรรมแล้วหรือไม่ก็ตาม แต่ต้องมีสัญชาติไทยหรือมีถิ่นที่อยู่ในประเทศไทย

3.2.1.2 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นิยาม “ข้อมูลส่วนบุคคล” ว่า

> “ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ”[119]

นิยามของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จึงแตกต่างไปจากพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 กล่าวคือ ข้อมูลส่วนบุคคลที่จะได้รับคุ้มครองภายใต้พระราชบัญญัตินี้ คือข้อมูลที่ทำให้สามารถระบุถึงตัวบุคคลได้ โดยไม่จำต้องเป็นสิ่งเฉพาะตัวของบุคคล องค์ประกอบของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จึงไม่ได้มีครบทั้งสององค์ประกอบอย่างข้อมูลข่าวสารส่วนบุคคล[120]

ยิ่งไปกว่านั้น บุคคลที่ได้รับการคุ้มครองตามพระราชบัญญัตินี้ยังไม่จำกัดเฉพาะบุคคลสัญชาติไทยหรือมีถิ่นที่อยู่ในประเทศไทย เพราะพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มุ่งควบคุมการใช้อำนาจเหนือข้อมูลตามหลักการสากล การคุ้มครองข้อมูลส่วนบุคคลในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จึงไม่คำนึงถึงสัญชาติหรือถิ่นที่อยู่ของเจ้าของข้อมูล นอกจากนี้ยังสามารถขยายขอบเขตการคุ้มครอง ในกรณีที่เจ้าของข้อมูลส่วนบุคคลที่อยู่ในประเทศไทยถูกเสนอ

---

[118] บุญชู ณ ป้อมเพชร, "คำอธิบายกฎหมายข้อมูลข่าวสารของราชการ."

[119] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 6.

[120] บุญชู ณ ป้อมเพชร, "คำอธิบายกฎหมายข้อมูลข่าวสารของราชการ."

ขายสินค้าบริการ หรือถูกเฝ้าติดตามพฤติกรรมอีกด้วย[121] แต่มีข้อสังเกตว่าข้อมูลที่ได้รับความคุ้มครองตามพระราชบัญญัติดังกล่าวจะไม่ครอบคลุมถึงข้อมูลผู้ถึงแก่กรรมแต่อย่างใด

3.2.2 หลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคล

เมื่อการสืบสวนและสอบสวนคดีอาญาเป็นการดำเนินการซึ่งได้รับยกเว้นจากหน้าที่ทั่วไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาในประเทศไทยจึงต้องอาศัยกฎเกณฑ์ตามหมวด 3 แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 เป็นหลัก โดยมีรายละเอียดดังนี้

3.2.2.1 การเก็บรวบรวมข้อมูลส่วนบุคคล

หมวด 3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ระบุให้หน่วยงานรัฐมีหน้าที่ต้องปฏิบัติเกี่ยวกับการจัดระบบข้อมูลข่าวสารส่วนบุคคล ดังต่อไปนี้

1.) ให้มีระบบข้อมูลข่าวสารส่วนบุคคลเพียงเท่าที่เกี่ยวข้อง และจำเป็นเพื่อให้การดำเนินงานของหน่วยงานสำเร็จตามวัตถุประสงค์เท่านั้น[122]

2.) ให้พิมพ์รายการแสดงรายละเอียดของข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความครอบครองลงในราชกิจจานุเบกษา และตรวจสอบแก้ไขรายการดังกล่าวให้ถูกต้องอยู่เสมอ[123] เพื่อให้บุคคลทั่วไปสามารถตรวจสอบได้ว่าข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับตนอาจถูกจัดเก็บได้โดยหน่วยงานรัฐใด อย่างไร และเจ้าของข้อมูลมีสิทธิประการใดเกี่ยวด้วยข้อมูลตนบ้าง[124]

---

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

[122] พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มาตรา 23 (1).

[123] โปรดดู พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มาตรา 23 (3) รายการที่หน่วยงานรัฐต้องพิมพ์ประกาศลงในราชกิจจานุเบกษานั้นประกอบไปด้วย

(ก) ประเภทของบุคคลที่มีการเก็บข้อมูลไว้

(ข) ประเภทของระบบข้อมูลข่าวสารส่วนบุคคล

(ค) ลักษณะการใช้ข้อมูลตามปกติ

(ง) วิธีการขอตรวจดูข้อมูลข่าวสารของเจ้าของข้อมูล

(จ) วิธีการขอให้แก้ไขเปลี่ยนแปลงข้อมูล

(ฉ) แหล่งที่มาของข้อมูล

[124] วิริยะ รามสมภพ, "ความสัมพันธ์เชิงวิเคราะห์ของร่างพระราชบัญญัติคุ้มครองข้อมูลข่าวสารส่วนบุคคล พ.ศ. ... กับ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540,"(สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ, 2562).

3.) ให้พยายามเก็บข้อมูลข่าวสารโดยตรงจากเจ้าของข้อมูล โดยเฉพาะอย่างยิ่งในกรณีที่จะกระทบถึงประโยชน์ได้เสียโดยตรงของบุคคลนั้น[125]

4.) ให้แจ้งข้อมูลดังต่อไปนี้แก่เจ้าของข้อมูล ในกรณีที่มีการเก็บรวบรวมข้อมูลจากเจ้าของข้อมูลโดยตรง โดยอาจแจ้งให้ทราบล่วงหน้า หรือพร้อมกันกับการขอข้อมูลก็ได้[126]

- วัตถุประสงค์และลักษณะการใช้ข้อมูลตามปกติ
- การขอข้อมูลเป็นกรณีที่อาจให้ข้อมูลได้โดยความสมัครใจหรือเป็นกรณีที่มีกฎหมายบังคับ กล่าวคือแจ้งให้เจ้าของข้อมูลทราบว่าตนมีสิทธิปฏิเสธการให้ข้อมูลหรือไม่
- ในกรณีที่มีการจัดส่งข้อมูลข่าวสารส่วนบุคคลซึ่งมีผลให้บุคคลทั่วไปทราบข้อมูลข่าวสารได้ ก็จำต้องแจ้งให้เจ้าของข้อมูลทราบ เว้นแต่เป็นลักษณะการใช้ข้อมูลตามปกติ

3.3.2.2 การใช้หรือเปิดเผยข้อมูลส่วนบุคคล

หมวด 3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ไม่ได้มีการกำหนดเกณฑ์การใช้ข้อมูลข่าวสารส่วนบุคคลไว้อย่างชัดแจ้ง คงมีเพียงเกณฑ์เกี่ยวกับการเปิดเผยข้อมูลที่ได้รับการบัญญัติไว้ในมาตรา 24 ภายใต้หลักการที่ว่า “ปกปิดเป็นหลัก เปิดเผยเป็นข้อยกเว้น” แตกต่างจากหลักการเปิดเผยข้อมูลข่าวสารของราชการทั่วไปที่ให้เปิดเผยเป็นหลัก ปกปิดเป็นข้อยกเว้น ทั้งนี้ เพราะข้อมูลข่าวสารส่วนบุคคลเป็นเรื่องส่วนตัว ซึ่งเจ้าของข้อมูลอาจไม่ประสงค์ให้มีการเปิดเผยโดยทั่วไป การเปิดเผยข้อมูลข่าวสารส่วนบุคคลจึงกระทำได้อย่างจำกัด เฉพาะในกรณีต่อไปนี้เท่านั้น[127]

1.) ได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลที่ให้ไว้ล่วงหน้าหรือขณะนั้น

2.) หากไม่ได้รับความยินยอม จะเปิดเผยได้เฉพาะกรณีต่อไปนี้

- เปิดเผยต่อเจ้าหน้าที่รัฐในหน่วยงาน เพื่อนำไปใช้ตามอำนาจหน้าที่
- เป็นการใช้ข้อมูลตามปกติภายในวัตถุประสงค์
- เปิดเผยต่อหน่วยงานของรัฐที่ทำงานด้วยการวางแผน หรือการสถิติหรือสำมะโนต่าง ๆ ซึ่งมีหน้าที่ต้องรักษาข้อมูลข่าวสารส่วนบุคคลไว้ไม่ให้เปิดเผยต่อไปยังผู้อื่น

---

[125] พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มาตรา 23 (2).

[126] พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มาตรา 23 วรรคสองและวรรคสาม.

[127] พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มาตรา 24.

- เปิดเผยเพื่อเป็นประโยชน์ในการศึกษาวิจัย โดยไม่ระบุชื่อหรือส่วนที่ทำให้รู้ว่าเป็นข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับบุคคลใด
- เปิดเผยต่อหอจดหมายเหตุแห่งชาติ กรมศิลปากร หรือหน่วยงานอื่นของรัฐตามมาตรา 26 วรรคหนึ่งเพื่อตรวจดูคุณค่าในการเก็บรักษา
- เปิดเผยต่อเจ้าหน้าที่ของรัฐ เพื่อป้องกันการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย หรือเพื่อการสืบสวน สอบสวน หรือฟ้องคดี
- เป็นการจำเป็น เพื่อป้องกันหรือระงับอันตรายต่อชีวิตหรือสุขภาพ
- เปิดเผยต่อศาล และเจ้าหน้าที่รัฐหรือหน่วยงานของรัฐหรือบุคคลที่มีอำนาจตามกฎหมายที่จะขอข้อเท็จจริงดังกล่าว
- กรณีอื่นตามที่กำหนดในพระราชกฤษฎีกา[128]

นอกเหนือจากการเปิดเผยต่อเจ้าหน้าที่ของรัฐในหน่วยงานของตน และการใช้ข้อมูลข่าวสารตามปกติ การเปิดเผยข้อมูลข่าวสารส่วนบุคคลในกรณีอื่น หน่วยงานของรัฐจะต้องจัดทำบัญชีแสดงการเปิดเผยกำกับไว้กับข้อมูลข่าวสารตามหลักเกณฑ์และวิธีการที่กำหนดในกฎกระทรวง

3.2.2.3 การเก็บรักษาข้อมูลส่วนบุคคล

หมวด 3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มีการกำหนดหน้าที่เกี่ยวกับการเก็บรักษาและการทำลายข้อมูลข่าวสารส่วนบุคคลให้แก่หน่วยงานของรัฐไว้ดังนี้

1.) ตรวจสอบแก้ไขข้อมูลข่าวสารส่วนบุคคลในความรับผิดชอบให้ถูกต้องเสมอ[129]
2.) จัดระบบรักษาความปลอดภัยป้องกันมิให้มีการนำข้อมูลข่าวสารส่วนบุคคลไปใช้โดยไม่เหมาะสมหรือเป็นผลร้ายต่อเจ้าของข้อมูล[130]
3.) ให้ยกเลิกการจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคล เมื่อหมดความจำเป็น[131]

นอกจากนี้ การเก็บรักษาข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญายังต้องเป็นไปตามมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อีกด้วย เพราะการสืบสวนและสอบสวนไม่ได้รับยกเว้นจากหน้าที่ดังกล่าว โดยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลได้กำหนดหน้าที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลแยกเป็นสองกรณี ได้แก่

---

[128] ปัจจุบัน (พ.ศ. 2565) ยังไม่ปรากฏว่ามีการตราพระราชกฤษฎีกำหนดการเปิดเผยกรณีอื่นเพิ่มเติม

[129] พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มาตรา 23 (4).

[130] พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มาตรา 23 (5).

[131] พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มาตรา 23 (1).

1.) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม และให้มีการทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป เพื่อคงไว้ซึ่งประสิทธิภาพในการรักษาความมั่นคงปลอดภัย ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด[132] กล่าวคือ มาตรฐานตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ซึ่งให้ความสำคัญกับการธำรงซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) ตลอดจนสภาพพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคล โดยจะต้องประกอบด้วยมาตรการเชิงองค์กร เทคนิค และทางกายภาพ ที่เหมาะสมกับระดับความเสี่ยง โดยอย่างน้อยต้องประกอบด้วยการดำเนินการต่อไปนี้[133]

- การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศที่สำคัญ (Access control)
- การบริหารจัดการสิทธิในการเข้าถึงข้อมูลส่วนบุคคลหรือระบบของผู้ใช้งาน (User access management)
- การกำหนดความรับผิดชอบของผู้ใช้งาน (User responsibilities)
- การจัดให้มีวิธีการตรวจสอบย้อนหลัง (Audit trails)

2.) เมื่อมีเหตุการละเมิดข้อมูลส่วนบุคคล ให้แจ้งเหตุการละเมิดนั้นแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมงนับแต่ทราบเหตุ และกรณีที่การละเมิดมีความเสี่ยงสูงที่จะกระทบสิทธิและเสรีภาพของบุคคล หน้าที่ในการแจ้งจะขยายไปถึงการแจ้งต่อเจ้าของข้อมูลด้วย[134]

3.2.2.4 สิทธิของเจ้าของข้อมูลส่วนบุคคล

หมวด 3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 รับรองสิทธิในข้อมูลข่าวสารส่วนบุคคลของประชาชนเอาไว้อยู่สองประการ[135] คือ

---

[132] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (1).

[133] ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565.

[134] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (4).

[135] พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มาตรา 25.

1.) สิทธิที่จะรู้ข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับตน โดยยื่นคำขอเป็นหนังสือให้หน่วยงานของรัฐที่ควบคุมดูแลข้อมูลข่าวสารส่วนบุคคล เพื่อตรวจดูหรือรับสำเนาข้อมูลข่าวสารส่วนบุคคลนั้น
2.) สิทธิที่จะแก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับตน ในส่วนที่ไม่ถูกต้องตามความเป็นจริง โดยให้ยื่นคำขอเป็นหนังสือให้หน่วยงานของรัฐที่ควบคุมดูแลข้อมูลข่าวสารนั้น

ในกรณีที่เจ้าของข้อมูลเป็นผู้เยาว์ คนไร้ความสามารถ คนเสมือนไร้ความสามารถ หรือในกรณีที่เจ้าของข้อมูลถึงแก่ความตาย บุคคลตามที่ระบุในกฎกระทรวง[136] มีสิทธิที่จะดำเนินการแทนเจ้าของข้อมูลข่าวสารส่วนบุคคลนั้นได้ด้วยเช่นกัน

3.2.2.5 สภาพบังคับและบทกำหนดโทษ

หากพิจารณาในส่วนของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 พบว่าพระราชบัญญัตินี้ไม่ได้มีบทกำหนดความรับผิด ในกรณีที่มีการฝ่าฝืนหลักเกณฑ์ในหมวด 3 แต่อย่างใดคงมีเพียงระบบการตรวจสอบด้วยการอุทธรณ์ต่อคณะกรรมการ ซึ่งแบ่งเป็นสองกรณี[137] ได้แก่

1.) ในกรณีที่หน่วยงานของรัฐมีคำสั่งไม่แก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสารส่วนบุคคล ให้เจ้าของข้อมูลมีสิทธิที่จะอุทธรณ์ต่อคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารภายใน 30 วัน นับแต่ได้รับแจ้งคำสั่ง[138]
2.) ในกรณีที่หน่วยงานของรัฐฝ่าฝืนไม่ปฏิบัติตามหน้าที่ ปฏิบัติหน้าที่ล่าช้า หรือไม่ให้ความสะดวกโดยไม่มีเหตุอันสมควร ให้ประชาชนมีสิทธิในการร้องเรียนต่อคณะกรรมการข้อมูลข่าวสารของราชการ[139]

ในทางกลับกัน หากเป็นการฝ่าฝืนหน้าที่ในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เจ้าของข้อมูลส่วนบุคคลจะมีสิทธิร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญ โดยคณะกรรมการผู้เชี่ยวชาญจะมีอำนาจในการออกคำสั่งให้มีการปฏิบัติหรือแก้ไขการดำเนินการให้ถูกต้อง หรือออกคำสั่งห้ามมิให้กระทำการใดที่ก่อความเสียหายแก่เจ้าของหรือให้กระทำการเพื่อระงับความเสียหายภายในระยะเวลาที่กำหนด ซึ่งหากมีการฝ่าฝืนไม่ปฏิบัติตาม

---

[136] โปรดดู กฎกระทรวง ฉบับที่ 2 (พ.ศ. 2541) ออกตามความในพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

[137] วิริยะ รามสมภพ, "ความสัมพันธ์เชิงวิเคราะห์ของร่างพระราชบัญญัติคุ้มครองข้อมูลข่าวสารส่วนบุคคล พ.ศ. ... กับ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540."

[138] พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มาตรา 25.

[139] พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มาตรา 13.

คำสั่งดังกล่าว ก็ให้นำบทบัญญัติเกี่ยวกับการบังคับทางปกครองตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองมาใช้บังคับโดยอนุโลม[140]

นอกจากนี้ ผู้ที่ฝ่าฝืนก็อาจต้องระวางโทษปรับทางปกครองเป็นจำนวนไม่เกินสามล้านบาท[141] และหากมีความเสียหายเกิดขึ้นต่อเจ้าของข้อมูลส่วนบุคคล ก็จำเป็นต้องมีการชดใช้ค่าสินไหมทดแทน ไม่ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่[142] โดยศาลมีอำนาจในการสั่งให้มีการจ่ายค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มขึ้นจากจำนวนค่าสินไหมทดแทนที่แท้จริงที่ศาลกำหนดได้ตามที่เห็นสมควร เมื่อคำนึงถึงพฤติการณ์ต่าง ๆ ที่เกี่ยวข้อง แต่จะต้องไม่เกินสองเท่าของค่าสินไหมทดแทนที่แท้จริง[143]

3.3 บทสรุป การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาของไทย

จากการศึกษาแนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาของประเทศไทยในบทที่ 3 จึงอาจสรุปได้ว่า ผลกระทบจากการที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยกเว้นไม่ให้การสืบสวนและสอบสวนคดีอาญาอยู่ในบังคับของพระราชบัญญัตินี้ เว้นแต่ในส่วนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของข้อมูล ส่งผลให้การคุ้มครองข้อมูลส่วนบุคคลจากการดำเนินการในชั้นสืบสวนและสอบสวนคดีอาญาต้องอาศัยมาตรการทางกฎหมายที่มีอยู่เดิมเป็นหลัก อันได้แก่ กฎหมายวิธีพิจารณาความอาญา และหมวด 3 ในพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ซึ่งอาจสรุปเป็นภาพรวมได้ดังนี้

---

[140] โปรดดู พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 73-74.

[141] โปรดดู พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 83.

[142] โปรดดู พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 77.

[143] โปรดดู พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 78.

ตารางที่ 1 สรุปการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาของไทย

หลักเกณฑ์ที่เกี่ยวข้อง	กฎหมายวิธีพิจารณความอาญา	กฎหมายคุ้มครองข้อมูลส่วนบุคคล
ขอบเขตข้อมูลส่วนบุคคล	ไม่มีบทนิยามคำว่าข้อมูลส่วนบุคคล	มีนิยามที่แตกต่างกันตามกฎหมายแต่ละฉบับ กล่าวคือ (1) พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 นิยามคำว่าข้อมูลข่าวสารส่วนบุคคลว่าเป็นข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคลธรรมดา ไม่ว่าจะถึงแก่กรรมหรือไม่ก็ตาม แต่ต้องมีสัญชาติไทยหรือมีถิ่นที่อยู่ในประเทศไทย (2) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นิยามคำว่าข้อมูลส่วนบุคคลว่าข้อมูลที่ระบุถึงตัวบุคคลธรรมดาได้ แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม
การเก็บรวบรวม	มีบทบัญญัติกำหนดกรอบการใช้อำนาจอยู่สามรูปแบบใหญ่ ได้แก่ (1) เหตุแห่งการใช้อำนาจ (2) วิธีการใช้อำนาจ และ (3) ตรวจสอบถ่วงดุลโดยองค์กรอื่น	อยู่ภายใต้หมวด 3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ซึ่งกำหนดให้หน่วยงานของรัฐมีหน้าที่ต่อไปนี้ (1) ให้มีระบบข้อมูลข่าวสารส่วนบุคคลเพียงเท่าที่เกี่ยวข้องและจำเป็น (2) ให้พิมพ์รายการแสดงรายละเอียดของข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความครอบครองลงในราชกิจจานุเบกษา (3) ให้พยายามเก็บข้อมูลข่าวสารโดยตรงจากเจ้าของข้อมูล (4) ให้แจ้งรายละเอียดเกี่ยวกับการใช้ข้อมูลแก่เจ้าของข้อมูล

หลักเกณฑ์ที่เกี่ยวข้อง	กฎหมายวิธีพิจารณาความอาญา	กฎหมายคุ้มครองข้อมูลส่วนบุคคล
การใช้และเปิดเผย	มีกฎเกณฑ์ที่เกี่ยวข้องโดยตรงไม่มากนัก โดยจะพบในพระราชบัญญัติเฉพาะหรือระเบียบภายใน แต่ไม่จะพบในประมวลกฎหมายวิธีพิจารณาความอาญาซึ่งเป็นบทบัญญัติหลักแต่อย่างใด	อยู่ภายใต้หมวด 3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ซึ่งโดยหลัก ห้ามมิให้มีการเปิดเผยข้อมูลข่าวสารส่วนบุคคล เว้นแต่ได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลหรือเข้าข้อยกเว้นตามกฎหมาย
การเก็บรักษา	มีกฎเกณฑ์ที่เกี่ยวข้องโดยตรงไม่มากนัก โดยจะพบในพระราชบัญญัติเฉพาะหรือระเบียบภายใน แต่ไม่จะพบในประมวลกฎหมายวิธีพิจารณาความอาญาซึ่งเป็นบทบัญญัติหลักแต่อย่างใด	อยู่ภายใต้หมวด 3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ซึ่งกำหนดให้หน่วยงานของรัฐมีหน้าที่ต่อไปนี้ (1) ให้ตรวจสอบแก้ไขข้อมูลข่าวสารส่วนบุคคลให้ถูกต้องเสมอ (2) ให้จัดระบบรักษาความปลอดภัย (3) ให้ยกเลิกระบบข้อมูลข่าวสารส่วนบุคคล เมื่อหมดความจำเป็น นอกจากนี้ ในส่วนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยจะอยู่ภายใต้บังคับของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งมีหน้าที่ที่เกี่ยวข้องอยู่สองประการ คือ (1) ให้จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม และให้มีการทบทวนมาตรการดังกล่าว ให้เป็นไปตามมาตรฐานขั้นต่ำ (2) แจ้งเหตุต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือเจ้าของข้อมูล แล้วแต่กรณี เมื่อมีเหตุการละเมิดข้อมูลส่วนบุคคล

หลักเกณฑ์ที่เกี่ยวข้อง	กฎหมายวิธีพิจารณความอาญา	กฎหมายคุ้มครองข้อมูลส่วนบุคคล
สิทธิของเจ้าของข้อมูล	ไม่มีบทบัญญัติรับรองสิทธิของบุคคลในฐานะเจ้าของข้อมูลส่วนบุคคล	มีบทบัญญัติรับรองสิทธิในข้อมูลข่าวสารส่วนบุคคลอยู่สองประการ คือ (1) สิทธิที่จะรู้ข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับตน (2) สิทธิแก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับตนในส่วนที่ไม่ถูกต้องตามความเป็นจริง
สภาพบังคับและโทษ	เมื่อมีการฝ่าฝืนหลักเกณฑ์ ข้อมูลข่าวสารซึ่งได้มาย่อมเป็นพยานหลักฐานที่ได้มาโดยไม่ชอบ โดยหลักจึงไม่อาจรับฟังได้ เว้นแต่ศาลใช้ดุลพินิจรับฟัง ส่วนในแง่ความรับผิด จะมีเพียงพระราชบัญญัติเฉพาะที่กำหนดความรับผิดสำหรับการเปิดเผยข้อมูลข่าวสารโดยไม่ชอบเท่านั้น ความรับผิดกรณีอื่น ๆ จึงต้องอาศัยบททั่วไปแทน และหากเกิดความเสียหาย ผู้เสียหายก็สามารถนำคดีไปฟ้องร้องทางแพ่งเพื่อให้มีการเยียวยาความเสียหายต่อไป	ในกรณีที่มีการฝ่าฝืนหมวด 3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 จะไม่มีบทกำหนดความรับผิดไว้โดยเฉพาะ แต่จะใช้ระบบการตรวจสอบด้วยการอุทธรณ์ต่อคณะกรรมการ แต่หากเป็นกรณีที่ฝ่าฝืนหน้าที่ในการรักษาความมั่นคงปลอดภัยของข้อมูลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นอกเหนือจากการร้องเรียนต่อคณะกรรมการเพื่อให้คณะกรรมการมีคำสั่งให้ปฏิบัติหรือห้ามกระทำการที่ทำให้เจ้าของข้อมูลส่วนบุคคลเสียหาย ผู้ที่ฝ่าฝืนยังอาจมีความรับผิดทางแพ่งและทางปกครองได้อีกด้วย

หากพิจารณาเพียงผิวเผิน ดูเหมือนว่าประเทศไทยจะมีมาตรการทางกฎหมายที่เพียงพอในการคุ้มครองข้อมูลส่วนบุคคลจากการดำเนินงานในชั้นสืบสวนและสอบสวนคดีอาญา แต่เมื่อวิเคราะห์โดยละเอียด จะพบว่ามาตรการทางกฎหมายที่มีอยู่นี้มีข้อจำกัดบางประการ อันอาจเป็นช่องว่างในการให้ความคุ้มครองข้อมูลส่วนบุคคล โดยมีรายละเอียดดังนี้

3.3.1 ข้อจำกัดของกฎหมายวิธีพิจารณาความอาญา

ข้อจำกัดแรก กฎหมายวิธีพิจารณาความอาญาของไทยเปิดช่องให้เจ้าหน้าที่รัฐมีอำนาจในการเก็บรวบรวมข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนอย่างกว้างขวาง โดยมีข้อสังเกตดังนี้

ประการที่หนึ่ง การค้นที่อยู่ในบังคับที่จะต้องมีคำสั่งหรือหมายค้นจากศาลมีขอบเขตค่อนข้างจำกัด เพราะประมวลกฎหมายวิธีพิจารณาความอาญาของไทยบัญญัติโดยแยก “การค้น” กับ “การรวบรวมพยานหลักฐาน” ออกจากกัน อีกทั้ง ยังมีการแบ่งการค้นเป็นอีกสามประเภทย่อย ได้แก่ การค้นตัวบุคคลในที่สาธารณสถาน การค้นในที่รโหฐาน และการค้นเอกสารทางไปรษณีย์โทรเลข ซึ่งมีการค้นสองประเภทหลังเท่านั้นที่อยู่ในบังคับจะต้องมีหมายค้นหรือคำสั่งศาลเป็นฐานอำนาจ ส่งผลให้การแสวงหาข้อเท็จจริงและการรวบรวมพยานหลักฐานตามประมวลกฎหมายวิธีพิจารณาความอาญาโดยมากจะเป็นอำนาจดุลพินิจของเจ้าพนักงานสืบสวนสอบสวนโดยลำพัง

ประการที่สอง การได้มาซึ่งข้อมูลข่าวสารโดยอาศัยอำนาจตามพระราชบัญญัติเฉพาะมีขอบเขตการใช้อำนาจอย่างกว้าง เนื่องจากถ้อยคำในบทบัญญัติขาดความชัดเจนและเฉพาะเจาะจง กล่าวคือ ไม่มีการระบุสถานการณ์ ตัวชี้วัด และเกณฑ์พิจารณาเงื่อนไขในการใช้อำนาจที่ชัดเจน แต่จะใช้ถ้อยคำกว้าง ๆ แต่เพียงว่า “เพื่อให้ได้มาซึ่งข้อมูลข่าวสาร” เท่านั้น[144] อันเป็นการเปิดช่องให้มีการเข้าถึงหรือได้มาซึ่งข้อมูลส่วนบุคคลโดยไม่จำกัดวิธีการ อาทิ

พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 มีการบัญญัติให้พนักงานเจ้าหน้าที่ตรวจสอบและเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจร รวมถึงอุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ โดยไม่ระบุมาตรการที่เฉพาะเจาะจง[145] นอกจากนี้ การใช้อำนาจดังกล่าวยังขยายขอบเขตไปถึงความผิดอื่น ซึ่งใช้ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรืออุปกรณ์คอมพิวเตอร์เป็นองค์ประกอบหรือเป็นส่วนหนึ่งในการกระทำความผิดอาญา หรือมีข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับความผิดอาญาอื่น[146] โดยที่ไม่กำหนดบัญชีฐานความผิดที่ชัดเจน ทั้งที่ตามความเป็นจริง

---

[144] ตัวอย่างเช่น พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 25 และพระราชบัญญัติป้องกันและปราบปรามการค้ามนุษย์ พ.ศ. 2551 มาตรา 30.

[145] พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 มาตรา 18.

[146] อ้างแล้ว.

การกระทำความผิดในปัจจุบันมักเกี่ยวข้องกับการใช้หรือการสื่อสารทางคอมพิวเตอร์ รองศาสตราจารย์คณาธิป ทองรวีวงศ์ จึงมีความเห็นว่าการกำหนดขอบเขตความผิดเช่นนี้เป็นการกำหนดที่กว้างเกินไป เพราะบุคคลทั่วไปย่อมไม่สามารถคาดหมายได้ว่ารวมถึงความผิดใดบ้าง[147] เป็นต้น

ยิ่งไปกว่านั้น คู่มือการฝึกอบรมข้าราชการตำรวจที่ปฏิบัติหน้าที่สืบสวนในสถานีตำรวจ ก็มีการระบุถึงเครื่องมือเทคนิคพิเศษ ไม่ว่าจะเป็นอุปกรณ์แอบถ่าย เครื่องดักฟัง อุปกรณ์ค้นหาตำแหน่ง เครื่องอ่านข้อมูลจากโทรศัพท์หรือซิมการ์ด เครื่องดูดขยายเสียง และโปรแกรม Spy Phone ในฐานะที่เป็นวิธีการเพื่อให้ได้มาซึ่งข้อมูลลับปกปิด[148] โดยไม่ได้ระบุเกณฑ์การใช้เครื่องมือเหล่านี้อย่างชัดแจ้ง จึงเป็นที่น่ากังขาว่าเครื่องมือเทคนิคพิเศษเหล่านี้จะถูกนำมาใช้ในคดีประเภทใด ในสถานการณ์ใด และด้วยเงื่อนไขอย่างไร จึงจะไม่กระทบสิทธิและเสรีภาพของประชาชนเกินกว่าที่จำเป็น

ประการที่สาม การขอข้อมูลข่าวสารจากผู้ประกอบการภาคเอกชน หากมิใช่ข้อความในสิ่งสื่อสาร ถือเป็นอำนาจสอบสวนทั่วไป ไม่อยู่ในบังคับที่จะต้องผ่านกระบวนการตรวจสอบจากศาล ตามความเห็นของคณะกรรมการกฤษฎีกา เรื่องเสร็จที่ 343/2549 โดยคณะกรรมการกฤษฎีกาได้ให้เหตุผลว่า การขอข้อมูลโทรคมนาคมอย่าง ชื่อ ที่อยู่ หมายเลขโทรศัพท์ รวมถึงรายละเอียดการเชื่อมต่ออินเตอร์เน็ตของผู้ใช้บริการ มิได้เป็นไปเพื่อทราบรายละเอียดในข้อมูลส่วนบุคคล เพราะข้อมูลดังกล่าวไม่ใช่ข้อความในสิ่งสื่อสารที่บุคคลติดต่อกันหรือข้อมูลข่าวสารที่ถูกหรืออาจถูกใช้เพื่อประโยชน์ในการกระทำความผิด จึงเป็นกรณีที่พนักงานสอบสวนใช้อำนาจออกหมายเรียกบุคคลซึ่งครอบครองเอกสารให้จัดส่งข้อมูลดังกล่าวได้ตามมาตรา 132 (3) ประมวลกฎหมายวิธีพิจารณาความอาญา[149] เป็นเหตุให้ในทางปฏิบัติ การขอข้อมูลข่าวสารจากผู้ประกอบการภาคเอกชนมักกระทำในรูปแบบหมายเรียกหรือหนังสือขอความร่วมมือจวบจนปัจจุบัน

ข้อจำกัดที่สอง บทบัญญัติกฎหมายวิธีพิจารณาความอาญาไม่ได้ถูกออกแบบให้สอดคล้องกับลักษณะธรรมชาติของความเป็นส่วนตัวในข้อมูล เพราะกฎหมายวิธีพิจารณาความอาญามีเจตนารมณ์ในการให้อำนาจและควบคุมการใช้อำนาจในกระบวนการยุติธรรมทางอาญา โดยมิได้มุ่งคุ้มครองเฉพาะข้อมูลส่วนบุคคล เป็นเหตุให้กฎหมายวิธีพิจารณาความอาญาขาดกฎเกณฑ์และมาตรการที่จำเป็นที่จะให้ความคุ้มครองข้อมูลส่วนบุคคลได้อย่างเพียงพอ ดังนี้

---

[147] อนุสิษฐ คุณากร และคณะ, การคุ้มครองข้อมูลส่วนบุคคลกับสังคมไทย, หน้า 51.

[148] สำนักงานตำรวจแห่งชาติ, "คู่มือการฝึกอบรมข้าราชการตำรวจที่ปฏิบัติหน้าที่งานสืบสวนในสถานีตำรวจ พ.ศ. 2557."

[149] โปรดดู เรื่องเสร็จที่ 343/2549 บันทึกสำนักงานคณะกรรมการกฤษฎีกา เรื่อง อำนาจของเจ้าพนักงานตำรวจในการปิดกั้นเว็บไซต์ที่ไม่เหมาะสมทางอินเตอร์เน็ต และของพนักงานสอบสวนตาม 132 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา.

ประการที่หนึ่ง กฎหมายวิธีพิจารณาความอาญาไม่มีกฎเกณฑ์ซึ่งครอบคลุมรูปแบบพฤติกรรมหรือการดำเนินการต่อข้อมูลส่วนบุคคลครบถ้วนทุกลักษณะ ดังจะเห็นได้จากตารางที่ 1 ว่าการใช้ การเปิดเผย และการเก็บรักษาข้อมูลส่วนบุคคล จะมีหลักเกณฑ์ที่เกี่ยวข้องโดยตรงไม่มากนัก เนื่องจากกฎหมายวิธีพิจารณาความอาญามักมุ่งเน้นการควบคุมการใช้อำนาจแสวงหาข้อเท็จจริงและรวบรวมพยานหลักฐานของเจ้าหน้าที่รัฐ ซึ่งหากพิจารณาในแง่พฤติกรรมต่อข้อมูลส่วนบุคคล จะเป็นในขั้นตอน “การเก็บรวบรวม” เป็นสำคัญ จึงอาจเกิดช่องว่างในการคุ้มครองข้อมูลส่วนบุคคลจากการดำเนินการลักษณะอื่น นอกเหนือจากการเก็บรวบรวมข้อมูลส่วนบุคคลได้

ประการที่สอง กฎหมายวิธีพิจารณาความอาญาไม่มีบทบัญญัติรับรองสิทธิของบุคคลในฐานะเจ้าของข้อมูลส่วนบุคคล การคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายวิธีพิจารณาความอาญาจึงเป็นการให้ความคุ้มครองเช่นเดียวกับสิทธิและเสรีภาพทั่วไป ทั้งที่ความเป็นส่วนตัวในข้อมูลมีสารัตถะแตกต่างไปจากสิทธิและเสรีภาพประเภทอื่น คือเป็นการรับรองให้บุคคลมีสิทธิตัดสินใจเกี่ยวกับข้อมูลของตน[150] การคุ้มครองข้อมูลส่วนบุคคลจึงให้ความสำคัญกับการมีส่วนร่วมของเจ้าของข้อมูล

ประการที่สาม กฎหมายวิธีพิจารณาความอาญาไม่มีสภาพบังคับและบทกำหนดโทษที่เหมาะสมกับการละเมิดข้อมูลส่วนบุคคล เพราะเจตนารมณ์ของกฎหมายวิธีพิจารณาความอาญามุ่งกำกับการให้ดำเนินกระบวนการยุติธรรมทางอาญาเป็นไปด้วยความเรียบร้อย ดังนั้น สภาพบังคับของกฎหมายวิธีพิจารณาความอาญาจึงไม่ได้มีมาตรการเชิงป้องกันหรือกลไกตรวจสอบกำกับดูแลให้มีการปฏิบัติหรือแก้ไขการดำเนินการให้เป็นไปตามมาตรฐาน ต่างจากกฎหมายคุ้มครองข้อมูลส่วนบุคคล

นอกจากนี้ ไม่ปรากฏว่ากฎหมายวิธีพิจารณาความอาญาของไทยกำหนดความรับผิดหรือโทษสำหรับการละเมิดข้อมูลส่วนบุคคลอย่างครอบคลุม โดยดร.ธนกฤต วรธนัชชากุล ให้ข้อสังเกตว่าในปัจจุบัน มีเพียงโทษฐานเปิดเผยข้อมูลข่าวสารโดยไม่ชอบเท่านั้น แต่ไม่มีพระราชบัญญัติใดเลยที่กำหนดโทษฐานเจ้าหน้าที่รัฐนำข้อมูลที่ได้มาไปใช้ประโยชน์อื่น นอกเหนือไปจากการปฏิบัติหน้าที่[151] และหากพิจารณาในด้านผู้เสียหาย แม้ผู้เสียหายจะมีสิทธินำคดีไปฟ้องร้องเรียกร้องค่าเสียหายทางแพ่ง แต่ผู้เสียหายก็ตกต้องเป็นผู้มีภาระพิสูจน์ตามหลักทั่วไป[152] ทั้งที่ข้อเท็จจริงและรายละเอียดการสืบสวนและสอบสวนมักอยู่ในความรู้เห็นของเจ้าหน้าที่รัฐโดยลำพัง จึงเป็นการยากที่ผู้เสียหายจะต่อสู้คดี

---

[150] จันทจิรา เอี่ยมมยุรา, "การคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย," วารสารนิติศาสตร์มหาวิทยาลัยธรรมศาสตร์ 34, 4 (ธันวาคม 2547); นคร เสรีรักษ์, ความเป็นส่วนตัว: ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย, หน้า 298.

[151] มติชนออนไลน์, "เปิดร่างป.วิอาญา’ดักฟัง’ อัยการเทียบเนื้อหาพ.ร.บ. 7 ฉบับ ชี้ข้อมูลลักลั่น" [ออนไลน์].

[152] จันทจิรา เอี่ยมมยุรา, "การคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย," วารสารนิติศาสตร์มหาวิทยาลัยธรรมศาสตร์.

3.3.2 ข้อจำกัดของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

เป็นระยะเวลากว่า 20 ปีที่พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มีผลบังคับใช้ แต่พระราชบัญญัตินี้ก็ไม่อาจให้ความคุ้มครองข้อมูลข่าวสารส่วนบุคคลได้อย่างมีประสิทธิภาพเพียงพอ ซึ่งอาจเป็นเพราะหมวด 3 ว่าด้วยข้อมูลข่าวสารส่วนบุคคลของพระราชบัญญัติดังกล่าว ได้รับยกร่างขึ้นตั้งแต่ปี พ.ศ. 2540 โดยมีบทบัญญัติอยู่เพียง 5 มาตรา กฎเกณฑ์ในพระราชบัญญัติดังกล่าวจึงล้าสมัยและรายละเอียดปฏิบัติค่อนข้างน้อย เมื่อเทียบกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยมีข้อสังเกตอยู่สี่ประการด้วยกัน ได้แก่

ประการที่หนึ่ง ขอบเขตข้อมูลข่าวสารส่วนบุคคลที่ได้รับความคุ้มครองตามหมวด 3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มีความแตกต่างไปจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยสรุปได้ดังนี้

ตารางที่ 2 ความแตกต่างของขอบเขตข้อมูลที่ได้รับความคุ้มครองตามกฎหมายไทย

ขอบเขต	พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
นิยามศัพท์	ข้อมูลข่าวสารส่วนบุคคล	ข้อมูลส่วนบุคคล
องค์ประกอบข้อมูลที่ได้รับความคุ้มครอง	ข้อมูลที่มีองค์ประกอบดังต่อไปนี้ - มีข้อเท็จจริงที่เป็นสิ่งเฉพาะตัว และ - มีสิ่งชี้ตัวบุคคล	ข้อมูลซึ่งทำให้สามารถระบุตัวบุคคลได้ ไม่ว่าโดยตรงหรือโดยอ้อม โดยไม่จำต้องเป็นสิ่งเฉพาะตัว
บุคคลที่ได้รับการคุ้มครอง	บุคคลธรรมดาซึ่งมีสัญชาติไทย หรือมีถิ่นที่อยู่ในประเทศไทย	บุคคลธรรมดาที่มีชีวิตอยู่ โดยไม่จำกัดสัญชาติหรือถิ่นที่อยู่ (อาจขยายขอบเขตการบังคับใช้ไปนอกราชอาณาจักรไทยได้ในบางกรณี)
ข้อมูลผู้ถึงแก่กรรม	ได้รับความคุ้มครอง	ไม่ได้รับความคุ้มครอง

เมื่อขอบเขตของข้อมูลซึ่งได้รับความคุ้มครองแตกต่างกัน ตามที่ปรากฏในตารางที่ 2 การบังคับใช้กฎหมายจึงเกิดความลักลั่นขึ้น โดยเฉพาะกับหน่วยงานรัฐที่อยู่ภายใต้กฎหมายทั้งสองฉบับ เนื่องจากข้อมูลที่ได้รับความคุ้มครองเปลี่ยนแปลงไปตามกฎหมายแต่ละฉบับ ในปัจจุบัน จึงปรากฏถึงความพยายามในการแก้ไขปรับปรุงบทนิยามในพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ต่อไป[153]

[153] โปรดดู ร่างพระราชบัญญัติข้อมูลข่าวสารสาธารณะ พ.ศ. .... เสนอโดย นายวรภพ วิริยะโรจน์ สมาชิกสภาผู้แทนราษฎร กับคณะ.

ประการที่สอง เกณฑ์การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลข่าวสารส่วนบุคคลตามหมวด 3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 โดยส่วนใหญ่เป็นเพียงหลักการกว้าง ๆ ซึ่งเมื่อเปรียบเทียบกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะพบว่า พระราชบัญญัตินี้ขาดรายละเอียดการปฏิบัติที่ชัดเจน โดยมีตัวอย่างดังนี้

- หมวด 3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ไม่ได้มีบทบัญญัติเกี่ยวกับฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคล และไม่ได้มีการกำหนดหน้าที่บันทึกรายการประมวลผลข้อมูลส่วนบุคคล เพื่อให้เจ้าของข้อมูลและหน่วยงานกำกับดูแลตรวจสอบ อีกทั้ง ไม่พบว่าว่ามีเกณฑ์การคุ้มครอง “ข้อมูลอ่อนไหว” แต่อย่างใด
- เกณฑ์เกี่ยวกับ “ความยินยอม” ยังขาดความชัดเจนในรายละเอียด คือ ไม่มีการระบุเงื่อนไขในการขอความยินยอม และไม่ได้รับรองสิทธิในการถอนความยินยอม อีกทั้ง ไม่ได้กำหนดให้มีการแจ้งรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลให้แก่เจ้าของข้อมูล[154]
- พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ไม่มีบทบัญญัติห้ามมิให้เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล แตกต่างไปจากวัตถุประสงค์ที่แจ้งต่อเจ้าของข้อมูลไว้ก่อนหรือขณะเก็บรวบรวม อีกทั้งไม่ปรากฏว่ามีบทบัญญัติเกี่ยวกับการแจ้งวัตถุประสงค์ใหม่
- พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ไม่ได้กำหนดให้ลบหรือทำลายข้อมูลข่าวสารส่วนบุคคล เมื่อพ้นระยะเวลาเก็บรักษา[155]
- หมวด 3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ไม่ได้มีกฎเกณฑ์สำหรับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ
- พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ไม่ได้กำหนดให้ผู้มีหน้าที่รับผิดชอบปฏิบัติตามหมวด 3 เป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมถึงไม่ได้กำหนดให้มีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

---

[154] พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 กำหนดให้กรณีที่เก็บข้อมูลข่าวสารโดยตรงจากเจ้าของข้อมูล หน่วยงานของรัฐต้องแจ้งให้เจ้าของข้อมูลทราบแต่เพียงว่าเป็นกรณีที่อาจให้ข้อมูลได้ด้วยความสมัครใจหรือเป็นกรณีมีกฎหมายบังคับเท่านั้น (โปรดดู พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มาตรา 23 วรรคสอง.)

[155] พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ไม่ได้กำหนดให้หน่วยงานของรัฐกำหนดระยะเวลาเก็บรักษาข้อมูลข่าวสารส่วนบุคคล แต่จะบัญญัติเพียงให้ยกเลิกระบบข้อมูลข่าวสารส่วนบุคคลเมื่อหมดความจำเป็น (โปรดดู พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มาตรา 23 (1).)

จะเห็นได้ว่าเกณฑ์ในหมวด 3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ยังขาดความครบถ้วนสมบูรณ์ในรายละเอียดอยู่มาก หากเปรียบเทียบกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ฉะนั้น หากปล่อยให้การสืบสวนและสอบสวนคดีอาญาอยู่ภายใต้หมวด 3 ของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ก็จะส่งผลให้การสืบสวนและสอบสวนคดีอาญามีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ต่ำกว่าการดำเนินงานของภาครัฐประเภทอื่น ซึ่งปัจจุบันอยู่ในบังคับที่จะต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ประการที่สาม การรับรองสิทธิเจ้าของข้อมูลส่วนบุคคลตามหมวด 3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ยังไม่มีความครอบคลุม เพราะเมื่อเปรียบเทียบกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะพบว่าพระราชบัญญัติดังกล่าวมีการรับรองสิทธิเจ้าของข้อมูลอยู่เพียงสองประการ คือสิทธิที่จะรู้ข้อมูลข่าวสารส่วนบุคคลเกี่ยวกับตน และสิทธิที่จะแก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสารส่วนบุคคลในส่วนที่ไม่ถูกต้องเท่านั้น นอกจากนี้ ในการปฏิเสธไม่ดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคล พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ก็มิได้มีการบัญญัติเหตุแห่งการปฏิเสธไว้ชัดแจ้ง[156] การดำเนินการให้เป็นไปตามสิทธิของเจ้าของข้อมูลจึงขึ้นอยู่กับดุลพินิจของหน่วยงานรัฐเป็นรายกรณีไป โดยไม่มีหลักเกณฑ์ที่ชัดเจน

ประการที่สี่ การบังคับใช้พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ไม่มีประสิทธิภาพเพียงพอ ด้วยข้อจำกัดของหน่วยงานที่มีอำนาจหน้าที่ในการกำกับดูแล กล่าวคือ

โครงสร้างและองค์ประกอบองค์กรที่มีอำนาจหน้าที่ในการคุ้มครองข้อมูลส่วนบุคคล ได้แก่ คณะกรรมการข้อมูลข่าวสารของราชการ และคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสาร มีที่มาจากฝ่ายราชการเป็นส่วนใหญ่ ผู้ช่วยศาสตราจารย์ ดร. นคร เสรีรักษ์ และผู้ช่วยศาสตราจารย์ กิตติพงศ์ กมลธรรมวงศ์ จึงมีความเห็นว่าโครงสร้างและองค์ประกอบเช่นนี้ทำให้การปฏิบัติหน้าที่ขององค์กรทั้งสองนี้ขาดความคล่องตัวและขาดความเป็นอิสระอย่างแท้จริง[157]

ในส่วนของอำนาจหน้าที่ ผู้ช่วยศาสตราจารย์ ดร. จันทจิรา เอี่ยมมยุรา ให้ข้อสังเกตเกี่ยวกับอำนาจหน้าที่ของคณะกรรมการข้อมูลข่าวสารของราชการอีกว่า คณะกรรมการดังกล่าวไม่ได้มีอำนาจสืบสวนสอบสวน (Investigation power) การกระทำที่เข้าข่ายเป็นการฝ่าฝืนการคุ้มครองข้อมูล

---

[156] โปรดดู พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มาตรา 25.

[157] กิตติพงษ์ กมลธรรมวงศ์, "การคุ้มครองข้อมูลข่าวสารส่วนบุคคลในระบบกฎหมายไทย : ปัญหาและแนวทางการแก้ไข" (นิติศาสตร์มหาบัณฑิต, คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2549), หน้า 401; นคร เสรีรักษ์, ความเป็นส่วนตัว: ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย, หน้า 309-321.

ข่าวสารส่วนบุคคล[158] อีกทั้ง ผู้ช่วยศาสตราจารย์ ดร. นคร เสรีรักษ์ ได้ตั้งข้อสังเกตว่า คณะกรรมการข้อมูลข่าวสารของราชการมีอำนาจเรียกให้บุคคลมาให้ถ้อยคำ หรือส่งวัตถุ เอกสาร หรือพยานหลักฐานมาประกอบการพิจารณาเท่านั้น ซึ่งหากฝ่าฝืนก็มีเพียงระวางโทษจำคุกไม่เกิน 3 เดือน หรือปรับไม่เกิน 5,000 บาท หรือทั้งจำทั้งปรับ ประกอบกับพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ไม่มีบทกำหนดความผิดและโทษ ในกรณีที่หน่วยงานของรัฐฝ่าฝืนหรือไม่ปฏิบัติตามกฎเกณฑ์การคุ้มครองข้อมูลข่าวสารส่วนบุคคลแต่อย่างใด การดำเนินการกับผู้กระทำความผิดที่ผ่านมาจึงเป็นการฟ้องร้องทางแพ่งเรียกค่าสินไหมทดแทนเพื่อการละเมิด หรือฟ้องร้องดำเนินคดีอาญา[159]

3.3.3 ปัญหาการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาของไทย

เมื่อการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาของประเทศไทยยังคงอาศัยมาตรการทางกฎหมายที่มีอยู่เดิม ซึ่งมีข้อจำกัดในการคุ้มครองข้อมูลส่วนบุคคลอยู่หลายประการ โดยอาจสรุปเป็นภาพรวมของสภาพปัญหาได้ ดังนี้

ตารางที่ 3 สรุปปัญหาการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาของไทย

<table>
<tr><th>หลักเกณฑ์ที่เกี่ยวข้อง</th><th>กฎหมายวิธีพิจารณาความอาญา</th><th>หมวด 3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540</th></tr>
<tr><td>ขอบเขตข้อมูลส่วนบุคคล</td><td>ไม่ได้มีการกำหนดขอบเขตหรือนิยามของข้อมูลส่วนบุคคลไว้</td><td>ไม่สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562</td></tr>
<tr><td>การเก็บรวบรวม</td><td>บทบัญญัติเปิดช่องให้เจ้าหน้าที่รัฐมีอำนาจอย่างกว้างขวาง</td><td rowspan="2">เป็นเพียงหลักการอย่างกว้างขาดรายละเอียดการปฏิบัติที่ชัดเจน</td></tr>
<tr><td>การใช้และเปิดเผย</td><td rowspan="4">ขาดกฎเกณฑ์ที่ครอบคลุมและสอดคล้องกับธรรมชาติของสิทธิในข้อมูลส่วนบุคคล</td></tr>
<tr><td>การเก็บรักษา</td><td rowspan="3"></td></tr>
<tr><td>สิทธิของเจ้าของข้อมูล</td></tr>
<tr><td>สภาพบังคับและโทษ</td><td>หน่วยงานกำกับดูแลมีข้อจำกัดทางโครงสร้างและอำนาจหน้าที่</td></tr>
</table>

[158] จันทจิรา เอี่ยมมยุรา, "การคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย," วารสารนิติศาสตร์มหาวิทยาลัยธรรมศาสตร์.

[159] นคร เสรีรักษ์, ความเป็นส่วนตัว: ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย, หน้า 254; วิริยะ รามสมภพ, "ความสัมพันธ์เชิงวิเคราะห์ของร่างพระราชบัญญัติคุ้มครองข้อมูลข่าวสารส่วนบุคคล พ.ศ. ... กับ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540."

ด้วยเหตุนี้ ผู้เขียนจึงเห็นว่าสาเหตุของปัญหาการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาตามกฎหมายไทยเกิดจากการที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดบทยกเว้นทั่วไป มิให้นำพระราชบัญญัตินี้มาใช้บังคับแก่การสืบสวนและสอบสวนคดีอาญา ทั้งที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีสถานะเป็นกฎหมายกลาง ซึ่งควรมุ่งคุ้มครองสิทธิเสรีภาพเป็นหลักและมีข้อยกเว้นเท่าที่จำเป็นเท่านั้น การกำหนดบทยกเว้นทั่วไปให้แก่การสืบสวนและสอบสวนคดีอาญาจึงอาจเกินความจำเป็นและไม่ได้สัดส่วนกับสิทธิในข้อมูลส่วนบุคคล เนื่องจากเป็นการยกเว้นให้การสืบสวนและสอบสวนคดีอาญาไม่อยู่ภายใต้ขอบเขตของพระราชบัญญัติดังกล่าวทั้งกิจการเป็นการทั่วไป แทนการจำกัดสิทธิเฉพาะเรื่องเฉพาะกรณี การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนจึงมีมาตรฐานไม่เทียบเท่ากับการดำเนินงานของรัฐประเภทอื่น ซึ่งได้ยกระดับไปตามมาตรฐานของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ทำให้สิทธิในข้อมูลส่วนบุคคลขาดหลักประกันที่เหมาะสมเพียงพอ เมื่ออยู่ในชั้นสืบสวนและสอบสวนคดีอาญา เพราะพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะใช้บังคับแก่การสืบสวนและสอบสวนคดีอาญาเฉพาะในส่วนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยเท่านั้น

กล่าวโดยสรุป แม้สิทธิในข้อมูลส่วนบุคคลอาจถูกจำกัดลงได้เพื่อประโยชน์สาธารณะ ในกรณีนี้คือเพื่อป้องกันและปราบปรามอาชญากรรม แต่ก็มิได้หมายความว่าการสืบสวนและสอบสวนคดีอาญาจะไร้ซึ่งพันธะในการคุ้มครองสิทธิในข้อมูลส่วนบุคคลโดยสิ้นเชิง การกำหนดบทยกเว้นทั่วไปให้แก่การสืบสวนและสอบสวนคดีอาญาในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้น จึงเป็นการสร้างข้อยกเว้นที่กว้างจนเกินไป ฉะนั้น ในการเสนอแนะแนวทางแก้ไขปัญหา จึงสมควรศึกษาแนวทางตามกฎหมายระหว่างประเทศและกฎหมายต่างประเทศว่าการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาสามารถกระทำได้หรือไม่ อย่างไร จึงจะไม่เป็นอุปสรรคต่อการดำเนินงานในชั้นสืบสวนและสอบสวนคดีอาญา ซึ่งจะได้กล่าวรายละเอียดในบทต่อ ๆ ไป

บทที่ 4
การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา ตามกฎหมายระหว่างประเทศและกฎหมายต่างประเทศ

เมื่อการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาตามกฎหมายไทยยังคงมีข้อจำกัดอยู่หลายประการดังที่วิเคราะห์ไว้ในบทที่ 3 ในการเสนอแนวทางแก้ไขปัญหา จึงควรศึกษาแนวทางการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายระหว่างประเทศและกฎหมายต่างประเทศที่ระบบกฎหมายคุ้มครองข้อมูลส่วนบุคคลมีพัฒนาการยาวนานกว่าประเทศไทย ดังนี้

ในระดับกฎหมายระหว่างประเทศ มีกฎระเบียบของสหภาพยุโรปเป็นวัตถุแห่งการศึกษาหลัก เพราะในปัจจุบัน มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปได้รับการยอมรับโดยทั่วไปในทางสากลและมีอิทธิพลอย่างมากต่อการจัดทำกฎหมายคุ้มครองข้อมูลส่วนบุคคลของหลายประเทศ รวมถึงพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของประเทศไทย การศึกษาวิจัยเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลจึงเลี่ยงไม่ได้ที่จะต้องนำมาตรฐานของสหภาพยุโรปมาเป็นเกณฑ์ขั้นต่ำในการพิจารณาความเหมาะสมของแนวทางการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย

สำหรับกฎหมายต่างประเทศ จะเป็นการศึกษาแนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาของสหราชอาณาจักร สหรัฐอเมริกา และสาธารณรัฐเกาหลี (เกาหลีใต้) เพื่อให้เห็นแนวทางการคุ้มครองข้อมูลส่วนบุคคลที่แตกต่างกันตามเงื่อนไขในแต่ละภูมิภาค โดยผู้เขียนจะนำเสนอแนวทางของสหราชอาณาจักรเป็นลำดับแรก เนื่องจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักรมีหลักการมาจากกฎระเบียบของสหภาพยุโรปเช่นเดียวกันกับกฎหมายของไทย ยิ่งไปกว่านั้น พบว่าแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย[160] ก็มีการอ้างอิงแนวปฏิบัติของ Information Commissioner's Office ("ICO") หรือสำนักงานคณะกรรมาธิการด้านข้อมูลข่าวสารของสหราชอาณาจักรอยู่จำนวนมาก แนวทางสหราชอาณาจักรจึงน่าจะมีความเหมาะสมที่จะปรับใช้ได้ในบริบทของสังคมไทย เพราะมีหลักการพื้นฐานที่สอดคล้องกัน

นอกเหนือจากสหราชอาณาจักร แนวทางของสหรัฐอเมริกาก็เป็นอีกแนวทางหนึ่งที่น่าสนใจ เนื่องจากการคุ้มครองข้อมูลส่วนบุคคลของสหรัฐอเมริกาจะมีลักษณะเฉพาะแตกต่างจากแนวทางของสหภาพยุโรป กล่าวคือสหรัฐอเมริกาจะไม่มีกฎหมายกลางว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล แต่จะ

---

[160] แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย ที่จัดทำโดยศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

อาศัยการคุ้มครองตามกฎหมายเฉพาะเรื่องเฉพาะกรณี โดยในชั้นสืบสวนและสอบสวนคดีอาญาจะมีบทบัญญัติแก้ไขเพิ่มเติมรัฐธรรมนูญฉบับที่ 4 (Fourth Amendment) เป็นหลักการสำคัญ จึงเห็นควรนำแนวทางของสหรัฐอเมริกามาศึกษาเปรียบเทียบ

สุดท้าย เพื่อให้เห็นแนวทางการคุ้มครองข้อมูลส่วนบุคคลของประเทศที่มีบริบททางสังคมและวัฒนธรรมที่ใกล้เคียงกับประเทศไทย โดยเฉพาะอย่างยิ่ง กลุ่มประเทศในแถบตะวันออกซึ่งอาจไม่ได้ถือเรื่องความเป็นส่วนตัวเข้มข้นเท่าสังคมตะวันตก ผู้เขียนจึงศึกษาแนวทางการคุ้มครองข้อมูลส่วนบุคคลของประเทศในทวีปเอเชียอีกประเทศหนึ่งอีกด้วย

แต่จากการค้นคว้าในเบื้องต้น ผู้เขียนพบว่าในกลุ่มประเทศอาเซียน (ASEAN) ไม่มีประเทศใดมีแนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาที่ชัดเจน แม้แต่ประเทศสิงคโปร์ที่มีความก้าวหน้าในเรื่องนี้มากที่สุด โดยศุภัสรา ชัยพิพัฒน์ ให้ความเห็นเกี่ยวกับประเด็นนี้ว่าประเทศในกลุ่มอาเซียนมีแนวโน้มที่จะละเว้นมิให้การดำเนินงานของรัฐผูกพันกับพันธะในการคุ้มครองข้อมูลส่วนบุคคล เนื่องจากประเทศกลุ่มอาเซียนสนับสนุนการคุ้มครองข้อมูลส่วนบุคคลในฐานะที่เป็นเครื่องมือในการรวมกลุ่มทางเศรษฐกิจกับนานาชาติ มากกว่าจะคำนึงถึงการปกป้องสิทธิของประชาชน ทำให้ประเทศอาเซียนไม่สามารถแก้ปัญหาการละเมิดความเป็นส่วนตัวโดยรัฐ[161] ด้วยเหตุนี้ ผู้เขียนจึงเลือกทำการศึกษาแนวทางของสาธารณรัฐเกาหลีแทน เพราะสาธารณรัฐเกาหลีเป็นประเทศเอเชียหนึ่งที่สหภาพยุโรปยอมรับถึงระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอตามมาตรฐาน GDPR ดังนี้

4.1 กฎหมายระหว่างประเทศ: กฎระเบียบของสหภาพยุโรป (EU)

หากพิเคราะห์ขอบเขตในทางเนื้อหาของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปจะพบว่า GDPR มีข้อยกเว้นไม่บังคับใช้แก่การประมวลผลข้อมูลที่ดำเนินการโดยหน่วยงานที่มีอำนาจหน้าที่ในการป้องกัน สืบสวน ตรวจจับ ดำเนินคดี ลงโทษทางอาญา รวมถึงป้องกันภัยคุกคามต่อความมั่นคงปลอดภัยของสาธารณะ[162] การสืบสวนและสอบสวนคดีอาญาจึงไม่อยู่ภายใต้บังคับของ GDPR ในทำนองเดียวกันกับที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดยกเว้น

---

[161] ศุภัสรา ชัยพิพัฒน์, "การกำกับดูแลของอาเซียนด้านความเป็นส่วนตัวของข้อมูล: ความท้าทายของภูมิภาคต่อการคุ้มครองความเป็นส่วนตัวของข้อมูลและข้อมูลส่วนบุคคลในไซเบอร์สเปซ" (สารนิพนธ์ปริญญามหาบัณฑิต สาขาวิชาความสัมพันธ์ระหว่างประเทศ ภาควิชาความสัมพันธ์ระหว่างประเทศ คณะรัฐศาสตร์, จุฬาลงกรณ์มหาวิทยาลัย, 2562), หน้า 52-61.

[162] GDPR, Article 2 (2) (d).

อย่างไรก็ตาม การยกเว้นของสหภาพยุโรปนี้ไม่ใช่การยกเว้นโดยเด็ดขาด เพราะสหภาพยุโรปได้วางกลไกสำคัญสองประการในการคุ้มครองข้อมูลส่วนบุคคลจากการใช้อำนาจรัฐ อันได้แก่

ประการแรก การตรวจสอบความสอดคล้องกับหลักสิทธิมนุษยชน โดยการชั่งน้ำหนักว่าการจำกัดสิทธิและเสรีภาพของบุคคลด้วยบทบัญญัติกฎหมายนั้นมีความสอดคล้องกับหลักสิทธิมนุษยชนตามอนุสัญญาสิทธิมนุษยชนยุโรปหรือไม่ เพียงใด[163]

ประการที่สอง การบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล เนื่องจากในการปฏิรูประบบกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป สหภาพยุโรปได้มีการประกาศใช้ Directive (EU) 2016/680 (Law Enforcement Directive: “LED”) คู่ขนานไปกับ GDPR เพื่อให้กิจการที่เกี่ยวข้องกับการป้องกัน สืบสวน ตรวจจับ ดำเนินคดี ลงโทษอาญา รวมถึงความมั่นคงปลอดภัยของสาธารณะอยู่ภายใต้กฎเกณฑ์ที่เฉพาะเจาะจงมากยิ่งขึ้น[164] สอดคล้องกับข้อเสนอแนะของ OECD ซึ่งเห็นว่าการสืบสวนและสอบสวนอาจมีกฎเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลแตกต่างจากหลักเกณฑ์ทั่วไปได้

4.1.1 เกณฑ์การตรวจสอบความสอดคล้องกับหลักสิทธิมนุษยชน

แม้อนุสัญญาสิทธิมนุษยชนยุโรปจะวางหลักไว้ว่าความเป็นส่วนตัวของบุคคลนั้นอาจถูกจำกัดด้วยบทบัญญัติกฎหมาย แต่บทบัญญัติกฎหมายดังกล่าวก็ต้องมีความสอดคล้องหลักสิทธิมนุษยชน ซึ่งเรียกว่า “หลักเกณฑ์ปกป้องสิทธิ” (Safeguard principle) เพื่อป้องกันมิให้เจ้าหน้าที่รัฐใช้อำนาจโดยอำเภอใจ โดยมีตัวอย่างหลักเกณฑ์สำคัญ ๆ ดังนี้[165]

(ก.) หลักความเฉพาะเจาะจง กฎหมายจำกัดสิทธิในข้อมูลส่วนบุคคลควรมีขอบเขตที่ชัดเจนเพียงพอให้ประชาชนคาดหมายได้ (Foreseeability) ว่าการจำกัดสิทธิในข้อมูลส่วนบุคคลนั้นอาจเกิดขึ้นในสถานการณ์ใด ภายใต้เงื่อนไขอย่างไร เพื่อป้องกันไม่ให้เกิดการใช้อำนาจรัฐโดยอำเภอใจ ซึ่งอาจพิจารณาได้ในสี่แง่มุมด้วยกัน ได้แก่

---

[163] คณาธิป ทองรวีวงศ์, "สิทธิในข้อมูลส่วนบุคคลที่ไม่ได้รับการคุ้มครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 : การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามกฎหมายเกี่ยวกับความมั่นคงของรัฐ," วารสารกฎหมายสิทธิมนุษยชน.

[164] LED, Recital 11; GDPR, Recital 19.

[165] คณาธิป ทองรวีวงศ์, "การปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน."; คณาธิป ทองรวีวงศ์, "สิทธิในข้อมูลส่วนบุคคลที่ไม่ได้รับการคุ้มครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 : การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามกฎหมายเกี่ยวกับความมั่นคงของรัฐ," วารสารกฎหมายสิทธิมนุษยชน; อนุสิษฐ คุณากร และคณะ, การคุ้มครองข้อมูลส่วนบุคคลกับสังคมไทย, หน้า 49-58.

1.) ในแง่เหตุแห่งการใช้อำนาจ

กฎหมายควรระบุปัจจัยสำคัญอันเป็นเหตุแห่งการใช้อำนาจอย่างชัดแจ้งและเฉพาะเจาะจง โดยเฉพาะการกำหนดประเภทความผิดให้ชัดเจน ซึ่งอาจเป็นการระบุฐานความผิดหรือบัญญัติเกณฑ์ที่เฉพาะเจาะจงไว้ เพื่อป้องกันไม่ให้รัฐตรากฎหมายสอดแนมข้อมูลเป็นวงกว้างหรือโดยลับ โดยศาลสิทธิมนุษยชนยุโรปเคยตัดสินว่า กฎหมายที่บัญญัติให้เจ้าหน้าที่รัฐมีอำนาจดักรับข้อมูลในความผิดร้ายแรง ร้ายแรงมาก และร้ายแรงที่สุดนั้น เป็นการกำหนดที่กว้างไป เพราะความผิดประเภทต่าง ๆ อาจจัดอยู่ในความผิดทั้งสามกลุ่มได้ทั้งสิ้น จึงไม่สอดคล้องกับ ECHR[166]

2.) ในแง่ของมาตรการ

มาตรการซึ่งจำกัดสิทธิในข้อมูลส่วนบุคคลควรได้รับการบัญญัติอย่างชัดเจนและเฉพาะเจาะจง การบัญญัติกฎหมายเปิดช่องให้เจ้าหน้าที่ใช้มาตรการใด ๆ ตามที่เห็นว่าจำเป็น โดยไม่กำหนดมาตรฐานที่เจาะจง จึงขัดต่อ ECHR[167]

3.) ในแง่ของเป้าหมาย

กฎหมายควรนิยามประเภทหรือกลุ่มบุคคลเป้าหมายที่อยู่ในขอบเขตของการแทรกแซงสิทธิส่วนบุคคลไว้อย่างแคบและชัดเจน การกำหนดกลุ่มเป้าหมายด้วยถ้อยคำว่าบุคคลอื่นใดที่อาจเกี่ยวข้องกับการกระทำความผิดอาญา โดยไม่มีคำอธิบายหรือคำจำกัดความ จึงเป็นการบัญญัติที่กว้างจนเกินไป ขัดต่อหลักความเฉพาะเจาะจงตาม ECHR[168]

4.) ในแง่ของระยะเวลา

กฎหมายควรมีข้อจำกัดด้านระยะเวลา รวมถึงเกณฑ์การขยายระยะเวลาที่ชัดเจน เพื่อป้องกันไม่ให้มีการสอดแนมเข้าถึงข้อมูลอย่างต่อเนื่อง[169]

---

[166] คณาธิป ทองรวีวงศ์, "การปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน."; "Iordachi and Others V. Moldova ", (European Court of Human Rights, 2009).; Iordachi And Others v Moldova ,25198/02, [2009] ECHR 256.

[167] Kruslin v France 12 EHRR 547 24 APRIL 1990.

[168] อนุสิษฐ คุณากร และคณะ, การคุ้มครองข้อมูลส่วนบุคคลกับสังคมไทย, หน้า 49-58.; Iordachi And Others v Moldova ,25198/02, [2009] ECHR 256.

[169] คณาธิป ทองรวีวงศ์, "สิทธิในข้อมูลส่วนบุคคลที่ไม่ได้รับการคุ้มครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 : การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามกฎหมายเกี่ยวกับความมั่นคงของรัฐ," วารสารกฎหมายสิทธิมนุษยชน.; Joined Cases C-293/12 and C-594/12.

(ข.) หลักการตรวจสอบถ่วงดุล การจำกัดสิทธิในข้อมูลส่วนบุคคลตามกฎหมายควรอยู่ภายใต้กระบวนการตรวจสอบขององค์กรอิสระ (Independent) แยกต่างหากจากองค์กรบังคับใช้กฎหมายนั้น เช่น กำหนดให้มีการขอหมายศาลก่อนการใช้อำนาจ[170] โดยคำขอที่ยื่นต่อศาลก็ต้องระบุเหตุผลความจำเป็น ข้อมูลส่วนบุคคลที่ต้องการตรวจสอบ ตลอดจนมาตรการที่จะใช้ เพื่อให้ประชาชนสามารถเข้าถึงและตรวจสอบการใช้อำนาจรัฐ[171]

(ค.) หลักความจำเป็นและได้สัดส่วน กฎหมายควรชั่งน้ำหนักระหว่างความจำเป็นกับประโยชน์สำคัญที่กฎหมายมุ่งคุ้มครองให้เป็นไปโดยได้สัดส่วนกัน หรืออีกนัยหนึ่ง แม้จะปรากฏถึงความจำเป็นที่รัฐต้องดำเนินการต่อข้อมูลส่วนบุคคล แต่การดำเนินการดังกล่าวก็ต้องได้สัดส่วนกับการจำกัดสิทธิมนุษยชน โดยมีกระบวนการที่เพียงพอในการปกป้องสิทธิ[172]

นอกจากนี้ กฎหมายที่กำหนดขึ้นควรมีมาตรการในการคุ้มครองสิทธิส่วนบุคคลของบุคคลที่สาม (Third party) ด้วยเช่นกัน เนื่องจากข้อมูลข่าวสารหรือการสื่อสารหนึ่ง ๆ อาจเกี่ยวข้องกับบุคคลหลายฝ่ายด้วยผลจากเทคโนโลยีสมัยใหม่ จึงมีความเป็นไปได้ที่บุคคลที่สาม ซึ่งมีส่วนร่วมในข้อมูลข่าวสารหรือการสื่อสาร ได้รับการกระทบกระเทือนสิทธิ ทั้งที่ไม่มีส่วนร่วมในความผิด[173]

ดังนั้น แม้สหภาพยุโรปจะมีบทบัญญัติกฎหมายให้อำนาจเจ้าพนักงานสืบสวนสอบสวนในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล แต่พลเมืองยุโรปก็มีสิทธินำคดีให้ศาลสิทธิมนุษยชนยุโรป (The European Court of Human Rights: ECtHR) พิจารณาว่ากฎหมายดังกล่าวขัดแย้งกับสิทธิในข้อมูลส่วนบุคคลตามที่อนุสัญญาสิทธิมนุษยชนยุโรปรับรองหรือไม่ อย่างไร เกณฑ์การตรวจสอบความสอดคล้องกับหลักสิทธิมนุษยชนจึงเป็นหนึ่งในกลไกสำคัญของสหภาพยุโรป ที่ทำให้รัฐไม่อาจอ้างการรักษาความมั่นคงปลอดภัยหรือการรักษาความสงบเรียบร้อยในสังคม เพื่อตราบทบัญญัติกฎหมายให้อำนาจเจ้าพนักงานของรัฐแทรกแซงข้อมูลส่วนบุคคลของประชาชนอย่างกว้างได้[174]

อนึ่ง มีข้อสังเกตว่าหลักเกณฑ์ปกป้องสิทธิภายใต้ ECHR ข้างต้นอาจมีความเชื่อมโยงกับการคุ้มครองข้อมูลส่วนบุคคลในบริบทของการโอนข้อมูลระหว่างประเทศด้วย กล่าวคือสหภาพยุโรปได้ใช้หลักเกณฑ์ดังกล่าวเพื่อประเมินระดับการคุ้มครองข้อมูลส่วนบุคคลในภาพรวมว่า กฎหมายที่ให้อำนาจเจ้าหน้าที่รัฐล่วงละเมิดข้อมูลส่วนบุคคลนั้นมีความสมดุลกับการคุ้มครองสิทธิความเป็นส่วนตัวหรือไม่

---

[170] Ibid.

[171] คณาธิป ทองรวีวงศ์, "การปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน."

[172] อ้างแล้ว.

[173] คณาธิป ทองรวีวงศ์, "การปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน."

[174] คณาธิป ทองรวีวงศ์, "สิทธิในข้อมูลส่วนบุคคลที่ไม่ได้รับการคุ้มครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 : การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามกฎหมายเกี่ยวกับความมั่นคงของรัฐ," วารสารกฎหมายสิทธิมนุษยชน.

ซึ่งหากประเทศใดมีกฎหมายให้อำนาจเจ้าหน้าที่รัฐขัดแย้งกับหลักสิทธิมนุษยชน ประเทศนั้นก็อาจถูกพิจารณาได้ว่ามีระดับการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอ เพราะการพิจารณาระดับการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปจะเป็นการประเมินโดยพิจารณาจากปัจจัยแวดล้อมทั้งหมดของการโอนข้อมูลส่วนบุคคล[175] อันได้แก่[176]

1.) หลักนิติธรรมและการเคารพสิทธิเสรีภาพขั้นพื้นฐานของกฎหมายที่เกี่ยวข้อง อาทิ
   - กฎหมายคุ้มครองข้อมูลส่วนบุคคล
   - มาตรฐานความมั่นคงปลอดภัย และกฎเกณฑ์การโอนข้อมูลส่วนบุคคลไปยังประเทศที่สามหรือองค์การระหว่างประเทศ
   - กฎหมายเกี่ยวกับความปลอดภัยสาธารณะหรือความมั่นคงของชาติ หรือกฎหมายอาญาที่ให้อำนาจหน่วยงานสาธารณะเข้าถึงข้อมูลส่วนบุคคล
   - จริยธรรมขององค์กรวิชาชีพต่าง ๆ
   - คำพิพากษาของศาล
   - ความมีประสิทธิภาพและการมีผลบังคับใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล และการได้รับเยียวยาความเสียหายทั้งทางปกครองและทางศาล
2.) การมีอยู่ของหน่วยงานกำกับดูแลอิสระที่มีอำนาจหน้าที่บังคับให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล รวมถึงความมีประสิทธิภาพในการทำหน้าที่ของหน่วยงานกำกับดูแลอิสระข้างต้น ไม่ว่าจะเป็นความรับผิดชอบในการช่วยเหลือให้คำปรึกษาแก่เจ้าของข้อมูลส่วนบุคคล หรือการให้ความร่วมมือกับหน่วยงานกำกับดูแลอิสระของรัฐสมาชิกในสหภาพยุโรป
3.) ข้อตกลงระหว่างประเทศ ซึ่งประเทศนั้นเป็นภาคีสมาชิกหรือมีพันธกรณีที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

[175] คณาธิป ทองรวีวงศ์, "การปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน."

[176] LED, Article 36; GDPR, Article 45.

นอกจากนี้ การประเมินระดับการคุ้มครองข้อมูลส่วนบุคคลจากปัจจัยแวดล้อมทางกฎหมายซึ่งให้อำนาจหน่วยงานบังคับใช้กฎหมายเข้าถึงข้อมูลส่วนบุคคล ศาลยุติธรรมแห่งยุโรป (European court of justice) ได้ตีความบนพื้นฐานของ ECHR เอาไว้ว่ากฎหมายดังกล่าวจะต้องผ่านการทดสอบระดับ “ความเทียบเท่าที่จำเป็น” (Essential equivalence) ซึ่งประกอบด้วยหลักเกณฑ์ต่อไปนี้[177]

1.) การให้อำนาจหน่วยงานของรัฐแทรกแซงข้อมูลส่วนบุคคลจะต้องได้รับการบัญญัติในกฎหมายโดยชัดแจ้ง และบทบัญญัติกฎหมายดังกล่าวต้องมีการกำหนดขอบเขตของการใช้อำนาจแทรกแซงข้อมูลส่วนบุคคลในตัวเอง
2.) เพื่อให้เป็นไปตามหลักความได้สัดส่วน การแทรกแซงข้อมูลส่วนบุคคลจะต้องกระทำเท่าที่จำเป็นในสังคมประชาธิปไตย เพื่อบรรลุวัตถุประสงค์เฉพาะเกี่ยวกับประโยชน์สาธารณะเทียบเท่ากับที่รับรองใน ECHR ของสหภาพยุโรป และกฎหมายที่อนุญาตให้หน่วยงานของรัฐแทรกแซงข้อมูลส่วนบุคคลดังกล่าวจะต้องมีการกำหนดกฎเกณฑ์ที่ชัดเจนเพื่อควบคุมการแทรกแซงข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่ง ต้องระบุว่าการแทรกแซงข้อมูลส่วนบุคคลจะกระทำได้ในสถานการณ์ใด ภายใต้เงื่อนไขอย่างไร อีกทั้ง ยังต้องกำหนดมาตรการเชิงป้องกันรองรับไว้อีกด้วย
3.) บทบัญญัติกฎหมายต้องมีผลผูกพันภายใต้ระบบกฎหมายภายใน ทั้งต้องมีผลบังคับใช้โดยไม่จำต้องรอให้ศาลวินิจฉัยถึงความไม่ชอบด้วยกฎหมาย นอกจากนี้ ยังต้องมีการเปิดโอกาสให้เจ้าของข้อมูลเข้าถึง แก้ไข หรือลบข้อมูลเกี่ยวกับตน ตลอดจนมีโอกาสที่จะดำเนินคดีทางศาลที่มีความเป็นอิสระและเป็นกลาง

ทั้งนี้ การถูกพิจารณาว่ามีระดับการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอนั้นจะส่งผลกระทบต่อการโอนข้อมูลระหว่างประเทศ คือจะไม่สามารถส่งหรือรับโอนข้อมูลส่วนบุคคลจากสหภาพยุโรปได้ทั้งในภาคเอกชนและภาครัฐ[178] ดังจะได้เห็นจากสภาพปัญหาการโอนข้อมูลระหว่างสหภาพยุโรปและสหรัฐอเมริกา ซึ่งผู้เขียนจะหยิบยกเป็นกรณีศึกษาในหัวข้อที่ 4.2.2.2 ต่อไป

[177] 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."
[178] คณาธิป ทองรวีวงศ์, "การปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน."

4.1.2 กฎหมายคุ้มครองข้อมูลส่วนบุคคล (LED)

กรอบการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปจะประกอบด้วยกฎระเบียบสองฉบับ คือ GDPR และ LED ใช้บังคับคู่ขนานกันไป โดย GDPR จะใช้บังคับกับกิจกรรมการประมวลผลข้อมูลทั่วไป ขณะที่ LED มีขอบเขตการใช้บังคับเฉพาะการประมวลผลข้อมูลส่วนบุคคล ดังต่อไปนี้

1.) ขอบเขตในเชิงเนื้อหา (Material scope)[179]

1.1) การประมวลผลข้อมูลส่วนบุคคลนั้นเป็นการดำเนินการโดยหน่วยงานผู้มีอำนาจรับผิดชอบ (Competent authorities) กล่าวคือหน่วยงานของรัฐที่มีอำนาจหน้าที่ในการป้องกัน สืบสวน ตรวจจับ ดำเนินคดี ลงโทษทางอาญา หรือรักษาความปลอดภัยสาธารณะ โดยให้หมายรวมถึงหน่วยงานหรือนิติบุคคลใดที่ได้รับมอบหมายตามกฎหมายให้มีอำนาจหน้าที่ในลักษณะเดียวกัน[180]

1.2) การประมวลผลข้อมูลส่วนบุคคลนั้นมีวัตถุประสงค์เพื่อป้องกัน สืบสวน ตรวจจับ ดำเนินคดี ลงโทษทางอาญา หรือการรักษาความปลอดภัยของสาธารณะ[181]

1.3) การประมวลผลข้อมูลส่วนบุคคลนั้นใช้วิธีการอัตโนมัติ (Automated Means) ไม่ว่าจะทั้งหมดหรือบางส่วน หรือข้อมูลส่วนบุคคลที่ประมวลผลเป็นส่วนหนึ่งหรือมุ่งหมายที่จะให้เป็นส่วนหนึ่งของระบบแฟ้มข้อมูล (Filing System)[182]

หากการประมวลผลข้อมูลส่วนบุคคลไม่เป็นไปตามหลักเกณฑ์อย่างหนึ่งอย่างใดข้างต้น การประมวลผลข้อมูลนั้นก็จะไม่อยู่ในบังคับ LED แต่อยู่ภายใต้ GDPR แทน[183] เช่น กรณีเก็บข้อมูลด้วยแบบสำรวจความพึงพอใจการเข้ารับบริการของสถานีตำรวจเป็นการดำเนินการเพื่อวัตถุประสงค์อื่นที่มิใช่การบังคับใช้กฎหมาย การประมวลผลข้อมูลดังกล่าวจึงไม่อยู่ภายใต้บังคับ LED แม้จะดำเนินการโดยหน่วยงานตำรวจก็ตาม

2.) ขอบเขตในเชิงพื้นที่ (Territorial Scope)

LED จะมีผลบังคับใช้แก่กิจกรรมการประมวลผลในยุโรปเท่านั้น เนื่องจาก LED ไม่ได้มีบทบัญญัติขยายขอบเขตในเชิงพื้นที่ไปยังนอกสภาพยุโรป ขอบเขตในเชิงพื้นที่ของ LED จึงมีขอบเขตที่แคบกว่า GDPR

---

[179] LED, Article 2 (1).

[180] LED, Article 2 (1) and Article 3 (7).

[181] LED, Article 2 (1) and Article 1 (1).

[182] LED, Article 2 (2).

[183] LED, Article 9, and Recital 11.

เมื่อพิจารณาขอบเขตการบังคับใช้ จะเห็นได้ว่า LED เป็นกฎระเบียบที่สหภาพยุโรปออกแบบเพื่อคุ้มครองข้อมูลส่วนบุคคลในกระบวนการบังคับใช้กฎหมาย (Law enforcement) เป็นการเฉพาะ ด้วยสหภาพยุโรปเห็นว่าการประมวลผลข้อมูลส่วนบุคคลสำหรับการบังคับใช้กฎหมายมีความแตกต่างจากการดำเนินการประเภทอื่น ประกอบกับโดยทั่วไป การบังคับใช้กฎหมายย่อมอยู่ภายใต้บทบัญญัติกฎหมายภายในของแต่ละรัฐอยู่แล้ว การให้ความคุ้มครองข้อมูลส่วนบุคคลในบริบทของการบังคับใช้กฎหมายจึงจำเป็นที่จะต้องถูกกำกับด้วยกฎเกณฑ์ที่มีความเฉพาะเจาะจงยิ่งขึ้น[184]

อย่างไรก็ดี หากพิจารณาในรายละเอียดกลับพบว่าโครงสร้างและเนื้อหาของ LED นั้นมีความคล้ายคลึงกับ GDPR เนื่องจากสหภาพยุโรปต้องการให้กฎระเบียบทั้งสองฉบับมีความสอดคล้องกันให้มากที่สุดและให้มีกฎเกณฑ์เฉพาะเท่าที่จำเป็น[185] โดยมีสาระสำคัญดังต่อไปนี้

4.1.2.1 ขอบเขตของข้อมูลส่วนบุคคล

LED นิยามคำว่า “ข้อมูลส่วนบุคคล” (Personal data) ให้หมายความถึงข้อมูลใด ๆ เกี่ยวกับบุคคล ซึ่งระบุหรือทำให้สามารถระบุถึงบุคคลธรรมดาผู้เป็นเจ้าของข้อมูลได้ (Data subject) ไม่ว่าโดยตรงหรือโดยอ้อมก็ตาม[186] อันเป็นบทนิยามเดียวกันกับ GDPR แสดงให้เห็นว่าสหภาพยุโรปไม่ต้องการกำหนดกฎเกณฑ์เฉพาะในประเด็นนี้ ข้อมูลที่ได้รับความคุ้มครองตามกฎระเบียบทั้งสองจึงเป็นวัตถุแห่งสิทธิเดียวกัน และอาจอธิบายแยกเป็นองค์ประกอบได้สี่ประการ อันได้แก่

องค์ประกอบแรก “ข้อมูลใด ๆ” เป็นคำที่มีความหมายอย่างกว้างครอบคลุมข้อมูลทั้งที่เป็นรูปธรรม (Objective) เช่น น้ำหนักหรือส่วนสูงของบุคคล และที่เป็นนามธรรม (Subjective) อย่างข้อคิดเห็นหรือการประเมินต่าง ๆ เช่น ผลการประเมินประสิทธิภาพทำงานหรือความน่าเชื่อถือของผู้เข้าทำสัญญากู้ ฯลฯ โดยไม่คำนึงว่าจะถูกต้องตรงความจริงหรือไม่ เว้นแต่ความไม่ถูกต้องนั้นจะทำให้ไม่สามารถระบุถึงตัวเจ้าของข้อมูลได้[187]

---

[184] LED, Recital 10; GDPR, Recital 19.

[185] European Data Protection Supervisor, "Opinion 6/2015 a Further Step Towards Comprehensive Eu Data Protection: Edps Recommendations on the Directive for Data Protection in the Police and Justice Sectors."

[186] LED, Article 3 (1).

[187] The Article 29 Working Party, "Opinion 4/2007 on the Concept of Personal Data, at Iii. Analysis of the Definition of “Personal Data” According to the Data Protection Directive."

นอกจากนี้ คำว่าข้อมูลใด ๆ ยังเป็นองค์ประกอบที่มีความเป็นกลางทางเทคโนโลยี คือ ไม่จำกัดรูปแบบเฉพาะข้อมูลคอมพิวเตอร์หรือข้อมูลอิเล็กทรอนิกส์ ข้อมูลจึงอาจอยู่ในรูปแบบเอกสาร อักขระ หมายเลข รูปถ่าย เสียง ภาพเคลื่อนไหว หรือแม้แต่ส่วนประกอบร่างกาย[188] เช่น ตัวอย่างเลือด (Blood sample) ที่แม้ไม่ใช่ข้อมูลชีวมิติ (Biometric data) ในตัวเอง แต่การตรวจพิสูจน์ตัวอย่างเลือดก็มีผลเป็นการบ่งชี้เฉพาะถึงตัวบุคคลได้ ตัวอย่างเลือดจึงเป็นแหล่งของข้อมูลชีวมิติและอยู่ในขอบเขตของข้อมูลส่วนบุคคลที่ได้รับความคุ้มครองตามกฎหมาย[189]

องค์ประกอบที่สอง “เกี่ยวกับบุคคล” ข้อมูลจะเกี่ยวกับบุคคลต่อเมื่อข้อมูลนั้นมีการระบุอัตลักษณ์หรือพฤติกรรมของบุคคล หรือเมื่อการใช้ข้อมูลดังกล่าวก่อผลกระทบบางอย่างต่อบุคคล ซึ่งอาจพิจารณาได้จากสามปัจจัยด้วยกัน[190] กล่าวคือ

1.) <u>เนื้อหา (Content)</u>
คือเนื้อหาข้อมูลมีการให้ข้อมูลของบุคคลอย่างชัดเจน เช่น ประวัติทางการแพทย์หรือทะเบียนประวัติอาชญากรรม

2.) <u>วัตถุประสงค์ (Purpose)</u>
คือข้อมูลที่ถูกใช้โดยมีวัตถุประสงค์เพื่อประเมินหรือตัดสินใจที่จะปฏิบัติต่อบุคคลในลักษณะใดลักษณะหนึ่ง เช่น การเก็บข้อมูลพฤติกรรมการซื้อสินค้ามาวิเคราะห์เพื่อนำเสนอโฆษณาที่เหมาะสมกับผู้บริโภคนั้น ๆ

3.) <u>ผลกระทบ (Result)</u>
คือข้อมูลซึ่งอาจก่อให้เกิดผลกระทบต่อสิทธิหรือประโยชน์ของบุคคล เมื่อมีการประมวลผลข้อมูลดังกล่าว เช่น ข้อมูลตำแหน่งในแอปพลิเคชัน Food delivery แม้วัตถุประสงค์หลักในการประมวลผลข้อมูลดังกล่าวคือการค้นหาตำแหน่งของผู้ขับขี่ที่อยู่ใกล้เพื่อความสะดวกในการให้บริการ แต่ข้อมูลตำแหน่งนี้ก็อาจถูกใช้เพื่อตรวจสอบประสิทธิภาพการให้บริการของผู้ขับขี่ได้อีกด้วย ข้อมูลตำแหน่งจึงอาจถูกพิจารณาได้ว่าเป็นข้อมูลเกี่ยวกับบุคคล

---

[188] Ibid.; คณาธิป ทองรวีวงศ์, <u>คำอธิบาย หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล</u>, หน้า 83.

[189] The Article 29 Working Party, "Opinion 4/2007 on the Concept of Personal Data, at Iii. Analysis of the Definition of “Personal Data” According to the Data Protection Directive."

[190] Ibid.

องค์ประกอบที่สาม “ซึ่งระบุหรือสามารถระบุถึงตัว” หมายถึงความสามารถในการแยกแยะบุคคลหนึ่งออกจากบุคคลอื่น ๆ ไม่ว่าโดยตรงหรือโดยอ้อม ซึ่งมักจะเป็นการแยกแยะด้วยการอ้างอิงจากสิ่งระบุอัตลักษณ์ (Identifiers) เช่น ชื่อสกุล หมายเลขประจำตัว ลักษณะทางกายภาพ ฯลฯ โดยการประเมินว่าข้อมูลใดมีความสามารถในการแยกแยะตัวบุคคลนั้นจำต้องพิจารณาเป็นรายกรณีไป เนื่องจากความสามารถในการแยกแยะตัวบุคคลของข้อมูลมักเกี่ยวข้องกับหลายปัจจัย[191]

ตัวอย่างเช่น ลำพังชื่อของบุคคลก็อาจไม่เพียงพอที่จะใช้ระบุถึงตัวตนเจ้าของข้อมูลได้ในบางบริบท จึงจำเป็นต้องมีข้อมูลอื่นมาประกอบ เช่น นาย อ. ที่เรียนคณะนิติศาสตร์ ข้อมูลที่เกิดจากการเชื่อมโยงกันจึงจะเป็นข้อมูลที่แยกแยะความแตกต่างของบุคคลได้

ดังนั้น ความสามารถในการระบุตัวของข้อมูลจึงขึ้นอยู่กับบริบทของสถานการณ์และปัจจัยแวดล้อมที่เกี่ยวข้องกับข้อมูล ไม่ว่าจะเป็นลักษณะกิจกรรม วิธีการประมวลผลข้อมูล ตลอดจนระยะเวลา ค่าใช้จ่าย และเทคโนโลยีที่ใช้ในการระบุตัวตน เพื่อหาแนวโน้มว่ากิจกรรมนั้นสามารถชี้ชัดถึงตัวบุคคลได้มากน้อยเพียงใด ทว่าการระบุตัวตนนี้ไม่จำเป็นต้องถึงขนาดเป็นการเปิดเผยตัวตนแท้จริงของบุคคล เช่น การระบุตัวตนบนเว็บไซต์ด้วยบัญชีผู้ใช้ (Username) ก็ถือเป็นการแยกแยะบุคคลหนึ่งออกจากบุคคลอื่นได้ เนื่องจากบัญชีผู้ใช้สามารถเป็นตัวระบุความแตกต่าง อันไปนำสู่การคาดเดาและจัดหมวดหมู่พฤติกรรมของบุคคลธรรมดาผู้เป็นเจ้าของบัญชีผู้ใช้ได้ ในแง่นี้ บัญชีผู้ใช้จึงอยู่ในขอบเขตของข้อมูลส่วนบุคคลที่ได้รับความคุ้มครองตามกฎหมายเช่นกัน[192]

องค์ประกอบที่สี่ “บุคคลธรรมดา” จะมีความหมายครอบคลุมเฉพาะบุคคลธรรมดาที่ยังมีชีวิตอยู่เท่านั้น ข้อมูลผู้ถึงแก่กรรมหรือนิติบุคคลจึงไม่อยู่ในขอบเขตที่จะได้รับความคุ้มครอง[193]

4.1.2.2 หลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคล

เมื่อโครงสร้างและเนื้อหาของ LED เป็นไปในทิศทางเดียวกันกับ GDPR สาระสำคัญหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลตาม LED จึงตั้งอยู่บนพื้นฐานของการรับรองสิทธิของเจ้าของข้อมูลส่วนบุคคลและการตรวจสอบกำกับการประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามมาตรฐาน โดยมีรายละเอียดดังต่อไปนี้

---

[191] Ibid.; คณาธิป ทองรวีวงศ์, คำอธิบาย หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล, หน้า 83-85.

[192] The Article 29 Working Party, "Opinion 4/2007 on the Concept of Personal Data, at Iii. Analysis of the Definition of “Personal Data” According to the Data Protection Directive."

[193] Ibid.

4.1.2.2.1 หลักการประมวลผลข้อมูลส่วนบุคคล

การคุ้มครองข้อมูลส่วนบุคคลภายใต้ LED ล้วนอยู่บนพื้นฐานของหลักการเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล (Principles relating to processing of personal data)[194] ตามบทบัญญัติมาตรา 4 ซึ่งมีด้วยกันทั้งหมดเจ็ดประการ อันได้แก่

(ก.) หลักความชอบด้วยกฎหมายและเป็นธรรม (Lawfulness and fairness) กำหนดว่าการประมวลผลข้อมูลส่วนบุคคลต้องชอบด้วยกฎหมายและเป็นธรรม คือมีฐานทางกฎหมาย (Legal basis) มารองรับ ซึ่ง LED ได้รับรองฐานทางกฎหมายอยู่เพียงประการเดียว คือกรณีมีบทบัญญัติกฎหมายให้อำนาจ และการประมวลผลข้อมูลส่วนบุคคลนั้นเป็นการดำเนินการที่จำเป็นเพื่อบรรลุวัตถุประสงค์ในการบังคับใช้กฎหมายดังกล่าว[195] ด้วยเหตุนี้ ลำพังมีกฎหมายให้อำนาจจึงไม่เพียงพอที่จะถือได้ว่าเป็นการประมวลผลที่ชอบด้วยกฎหมายและเป็นธรรม หากแต่ต้องเป็นการดำเนินการที่จำเป็นและได้สัดส่วนระหว่างสิทธิส่วนบุคคลกับการสืบสวนและสอบสวนอีกด้วย[196]

ตัวอย่างเช่น หากการสอบปากคำในชั้นสอบสวนจะทำให้ได้มาซึ่งข้อมูลข่าวสารเช่นเดียวกับการดักฟังโทรศัพท์ การรวบรวมพยานหลักฐานก็ต้องใช้วิธีการสอบปากคำซึ่งเป็นมาตรการที่กระทบสิทธิน้อยกว่า โดยที่มิได้ลดประสิทธิภาพของการสอบสวนคดีอาญา[197]

---

[194] LED, Article 4 (1) Principles relating to processing of personal data.

"Member States shall provide for personal data to be:

(a) processed lawfully and fairly;

(b) collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;

(c) adequate, relevant and not excessive in relation to the purposes for which they are processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed;

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

[195] LED, Article 8 Lawfulness of processing.

[196] Council of Europe, "Practical Guide on the Use of Personal Data in the Police Sector."

[197] Ibid.

สำหรับข้อมูลอ่อนไหว (Sensitive data) อาทิ เชื้อชาติ ความเชื่อทางศาสนา ข้อมูลพันธุกรรม ข้อมูลชีวมิติ ข้อมูลสุขภาพ หรือวิถีทางเพศ ฯลฯ จะได้รับการจำแนกเป็นข้อมูลส่วนบุคคลประเภทพิเศษ (Special categories of personal data) เพื่อให้ความคุ้มครองโดยเคร่งครัดกว่าข้อมูลทั่วไป กล่าวคือการประมวลผลข้อมูลอ่อนไหวจะกระทำได้เฉพาะในกรณีที่มีความจำเป็นอย่างยิ่ง และเมื่ออยู่ในขอบเขตอย่างใดอย่างหนึ่งดังต่อไปนี้

- มีบทบัญญัติกฎหมายอนุญาตให้กระทำได้
- การประมวลผลเป็นไปเพื่อปกป้องประโยชน์สำคัญต่อชีวิต
- เป็นข้อมูลที่เจ้าของข้อมูลเปิดเผยต่อสาธารณะโดยชัดแจ้ง

แต่ไม่ว่ากรณีใด การประมวลผลข้อมูลอ่อนไหวจะต้องจัดให้มีการคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลอย่างเหมาะสม[198] เพื่อป้องกันผลกระทบอันไม่พึงประสงค์ ซึ่งรวมถึงการเลือกปฏิบัติต่อบุคคล เช่น การสืบสวนเพื่อค้นหาผู้มีส่วนเกี่ยวข้องกับการก่อความไม่สงบโดยเชื่อมโยงกับกลุ่มศาสนากลุ่มใดกลุ่มหนึ่งเป็นการเฉพาะ เช่นนี้จะกระทำไม่ได้[199]

นอกจากนี้ LED ยังห้ามมิให้ใช้การตัดสินใจอัตโนมัติ (Automated individual decision-making) โดยลำพัง หากการประมวลผลข้อมูลนั้นอาจก่อให้เกิดผลกระทบอย่างมีนัยสำคัญต่อเจ้าของข้อมูล เว้นแต่มีบทบัญญัติกฎหมายอนุญาตให้กระทำได้ ภายใต้เงื่อนไขว่าจะต้องมีการคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลอย่างเหมาะสม โดยอย่างน้อยที่สุด คือการให้มนุษย์มีส่วนแทรกแซงระบบอัตโนมัติดังกล่าว[200] เนื่องจากปัจจุบัน มีการใช้เทคโนโลยีในการประมวลผลข้อมูลจำนวนมาก ไม่ว่าจะเป็นการนำข้อมูลหลายแหล่งมาเชื่อมโยงสร้างประวัติของบุคคล (Profiling) หรือการใช้ปัญญาประดิษฐ์ (Artificial intelligence: “AI”) ฯลฯ จึงมีโอกาสที่การประมวลผลข้อมูลเหล่านี้จะเกิดความผิดพลาดขึ้น เพราะไม่ผ่านการตัดสินใจของมนุษย์แต่ประการใด[201]

อนึ่ง มีข้อสังเกตว่าหลักการพื้นฐานภายใต้ LED ไม่ได้มีการบัญญัติรับรองหลักความโปร่งใส (Transparency) ไว้โดยชัดแจ้ง แตกต่างจาก GDPR ที่หลักความโปร่งใสถือ

---

[198] LED, Article 10 Processing of special categories of personal data.

[199] Council of Europe, "Practical Guide on the Use of Personal Data in the Police Sector."

[200] LED, Article 11 Automated individual decision-making.

[201] 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); คณาธิป ทองรวีวงศ์, คำอธิบาย หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล, หน้า 500-502.

เป็นส่วนหนึ่งของหลักความชอบด้วยกฎหมายและเป็นธรรม[202] ทั้งนี้ อาจเพราะด้วยลักษณะธรรมชาติของการสืบสวนและสอบสวนคดีอาญา การดำเนินการบางลักษณะก็จำต้องกระทำในทางลับ จึงยากที่มีความโปร่งใสอย่างสมบูรณ์ในการประมวลผลข้อมูลส่วนบุคคล[203]

(ข.) หลักการจำกัดวัตถุประสงค์ (Purpose limitation) กำหนดว่าข้อมูลส่วนบุคคลต้องถูกเก็บรวบรวมเพื่อวัตถุประสงค์อันชัดแจ้งเฉพาะเจาะจง และห้ามมิให้มีการประมวลผลข้อมูลโดยไม่สอดคล้องกับวัตถุประสงค์ที่กำหนดไว้ในคราวแรก[204]

ฉะนั้น การเก็บรวบรวมข้อมูลในชั้นสืบสวนและสอบสวนคดีอาญาเป็นการทั่วไป โดยปราศจากวัตถุประสงค์ที่ชัดเจน จึงไม่อาจกระทำได้ภายใต้หลักการนี้ อย่างไรก็ตาม LED ได้ยืดหยุ่นให้การสืบสวนและสอบสวนอาจทำการประมวลผลข้อมูลส่วนบุคคล นอกเหนือไปจากวัตถุประสงค์กำหนดในคราวแรกได้ (Subsequent processing) หากมีบทบัญญัติกฎหมายมารองรับ หรืออีกนัยหนึ่ง เป็นการดำเนินการที่อยู่ในความคาดการณ์ของกฎหมาย เช่น การสืบสวนคดีฟอกเงิน เจ้าหน้าที่รัฐย่อมสามารถตรวจสอบข้อมูลเส้นทางการเงินของบุคคล ซึ่งเดิมถูกจัดเก็บเพื่อวัตถุประสงค์ทางภาษีได้ หากมีกฎหมายบัญญัติให้อำนาจไว้ เป็นต้น[205]

(ค.) หลักการใช้ข้อมูลให้น้อยที่สุด (Data minimisation) กำหนดให้จำกัดการประมวลผลข้อมูลให้น้อยที่สุดเท่าที่เพียงพอ จำเป็น และเกี่ยวข้องกับวัตถุประสงค์ของการประมวลผลข้อมูล[206] ดังนั้น ข้อมูลส่วนบุคคลที่จะนำมาประมวลผลในชั้นสืบสวนและสอบสวนจึงต้องมีความสัมพันธ์กับการกระทำความผิดที่เกิดขึ้นหรือที่กำลังจะเกิดขึ้นอย่างชัดแจ้ง[207]

ยกตัวอย่างเช่น การใช้อำนาจตรวจสอบข้อมูลจราจรคอมพิวเตอร์ในเบื้องต้น เจ้าหน้าที่ตำรวจต้องตอบคำถามให้ได้เสียก่อนว่าการเข้าถึงข้อมูลนั้นมีความจำเป็นอย่างไร และแม้จะปรากฏความจำเป็น การเข้าถึงข้อมูลดังกล่าวก็ต้องจำกัดเท่าที่เกี่ยวข้องกับการสืบสวนและสอบสวนคดีอาญา กล่าวคือให้จำกัดการเข้าถึงเฉพาะข้อมูลของบุคคลที่ต้องสงสัยในช่วงเวลาที่ต้องการสืบสวนและสอบสวนเท่านั้น โดยไม่อาจเข้าถึงข้อมูลทั้งหมดได้ เพราะเป็นการขัดต่อหลักการนี้[208]

---

[202] โปรดดู GDPR, Article 5 (1) (a).

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

[204] LED, Article 4 (1) (b) and Recital 29.

[205] Council of Europe, "Practical Guide on the Use of Personal Data in the Police Sector."

[206] LED, Article 4 (1) (c).

[207] Council of Europe, "Practical Guide on the Use of Personal Data in the Police Sector."

[208] Ibid.

(ง.) หลักความถูกต้องสมบูรณ์ (Accuracy) กำหนดว่าต้องรักษาข้อมูลส่วนบุคคลให้มีความถูกต้อง สมบูรณ์ และเป็นปัจจุบัน[209] โดย LED ขยายความเพิ่มเติมต่อไปว่าการใช้หลักการนี้ควรคำนึงถึงธรรมชาติและวัตถุประสงค์ของการประมวลผลข้อมูลที่เกี่ยวข้อง เพราะในบางบริบท ก็ยากที่จะตรวจสอบความถูกต้องสมบูรณ์ของข้อมูล เช่น ข้อมูลส่วนบุคคลที่บันทึกจากการสอบปากคำพยานนั้นเป็นข้อมูลที่มีพื้นฐานมาจากการรับรู้ข้อเท็จจริงของบุคคล จึงไม่อาจตรวจสอบได้อย่างแน่ชัดว่าข้อมูลส่วนบุคคลดังกล่าวถูกต้องตรงความจริงหรือไม่ ในแง่นี้ ความถูกต้องสมบูรณ์จึงนำมาใช้เฉพาะในส่วนของข้อเท็จจริงที่ว่าพยานได้มีการระบุข้อมูลดังกล่าวเท่านั้น[210]

นอกเหนือจากการดำเนินการให้ข้อมูลถูกต้อง สมบูรณ์ เป็นปัจจุบัน LED ได้กำหนดหน้าที่พิเศษอีกประการหนึ่ง ซึ่งไม่ปรากฏอยู่ในบทบัญญัติของ GDPR คือหน้าที่ในการแยกแยะประเภทข้อมูลส่วนบุคคล ซึ่งประกอบด้วยหน้าที่ย่อยสองประการด้วยกัน ได้แก่

1.) <u>การแยกแยะประเภทของเจ้าของข้อมูลส่วนบุคคล</u>

คือการแบ่งหมวดหมู่ว่าข้อมูลส่วนบุคคลนั้นเป็นข้อมูลของผู้ต้องสงสัย ผู้ต้องคำพิพากษาว่ากระทำความผิด ผู้เสียหาย หรือผู้มีส่วนเกี่ยวข้องอื่นใด[211] เพื่อกำหนดระยะเวลาจัดเก็บข้อมูลแต่ละประเภท[212] แต่การแยกแยะประเภทดังกล่าวจะต้องไม่ส่งผลกระทบต่อข้อสันนิษฐานความบริสุทธิ์[213]

2.) <u>การแยกแยะคุณภาพของข้อมูลส่วนบุคคล</u>

เป็นการแยกแยะระหว่างข้อเท็จจริงและข้อคิดเห็น เพื่อใช้ในการประเมินความน่าเชื่อถือและตรวจสอบความถูกต้องของข้อมูลก่อนส่งต่อหรือเผยแพร่ ซึ่งหากมีการส่งต่อหรือเผยแพร่ข้อมูลที่ไม่ถูกต้องออกไป จะต้องทำการแจ้งไปยังผู้รับข้อมูลโดยไม่ชักช้า พร้อมต้องแก้ไข ทำลาย หรือจำกัดการประมวลผลของข้อมูลที่ไม่ถูกต้อง[214]

---

[209] LED, Article 4 (1) (d).

[210] LED, Recital 30.

[211] LED, Article 6 Distinction between different categories of data subject.

[212] Leiser, M. and B. Custers, "The Law Enforcement Directive: Conceptual Challenges of Eu Directive 2016/680," <u>European Data Protection Law Review</u>.

[213] LED, Recital 31.

[214] LED, Article 7 Distinction between personal data and verification of quality of personal data.

(จ.) หลักการจำกัดการเก็บรักษา (Storage limitation) กำหนดว่าข้อมูลส่วนบุคคลจะถูกเก็บรักษาในรูปแบบที่ระบุตัวตนเจ้าของข้อมูลได้ไม่นานเกินกว่าที่จำเป็นเพื่อบรรลุวัตถุประสงค์ของการประมวลผลข้อมูล โดยต้องกำหนดระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล (Retention Period) พร้อมจัดให้มีระบบตรวจสอบเพื่อลบ ทำลาย หรือทำให้ข้อมูลซึ่งพ้นระยะเวลาเก็บรักษาเป็นข้อมูลนิรนาม ทั้งต้องทบทวนความเหมาะสมของกำหนดระยะเวลาอยู่เสมอ เพื่อประกันว่าจะไม่มีการเก็บรักษาข้อมูลส่วนบุคคลไว้นานเกินกว่าความจำเป็น[215] แสดงให้เห็นว่าการดำเนินการต่อข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนจะต้องคำนึงถึงหลักความจำเป็นในทุกขั้นตอน[216]

(ฉ.) หลักความสมบูรณ์และเป็นความลับ (Integrity and confidentiality) กำหนดให้การประมวลผลข้อมูลส่วนบุคคลต้องมีมาตรการที่ประกันความมั่นคงปลอดภัย เพื่อป้องกันการประมวลผลที่ไม่ได้รับอนุญาตหรือที่ไม่ชอบด้วยกฎหมาย และป้องกันไม่ให้ข้อมูลถูกทำลายหรือสูญหาย โดยใช้มาตรการเชิงเทคนิคหรือเชิงบริหารที่เหมาะสมกับความเสี่ยง[217]

มีข้อสังเกตว่า LED ได้บัญญัติแจกแจงมาตรการรักษาความมั่นคงปลอดภัยสำหรับการประมวลผลข้อมูลส่วนบุคคลในส่วนที่ใช้วิธีการอัตโนมัติ ซึ่งประกอบด้วยมาตรการหลายรูปแบบ อาทิ การควบคุมสื่อข้อมูล โดยการป้องกันการอ่าน คัดลอก แก้ไข หรือลบสื่อข้อมูล หรือการมีระบบกู้คืน เพื่อรักษาความสมบูรณ์ของข้อมูลในกรณีที่มีข้อผิดพลาด[218] ขณะที่ GDPR จะไม่ได้มีการแยกบัญญัติแนวทางการรักษาความมั่นคงปลอดภัยสำหรับการประมวลผลด้วยวิธีการอัตโนมัติ

ยิ่งไปกว่านั้น ในกรณีที่การประมวลผลข้อมูลมีแนวโน้มจะก่อให้เกิดความเสี่ยงสูงต่อสิทธิและเสรีภาพของบุคคล โดยเฉพาะอย่างยิ่ง จากการใช้เทคโนโลยีที่มีความซับซ้อน LED ได้กำหนดให้มีการประเมินความเสี่ยงผลกระทบต่อข้อมูลส่วนบุคคล (Data protection impact assessment: “DPIA”)[219] พร้อมกำหนดให้มีการปรึกษาหารือกับหน่วยงานกำกับดูแล ก่อนจะทำการประมวลผลดังกล่าว[220] อันเป็นการเปิดโอกาสให้หน่วยงานกำกับดูแลที่เกี่ยวข้องเข้ามาประเมินและให้ข้อเสนอแนะเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล เพื่อจัดการความเสี่ยงต่อไป

---

[215] LED, Article 4 (1) and Article 5.

[216] Council of Europe, "Practical Guide on the Use of Personal Data in the Police Sector."

[217] LED, Article 29 (1) Security of processing.

[218] LED, Article 29 (2) Security of processing.

[219] LED, Article 28 Data protection impact assessment.

[220] LED, Article 29 Prior consultation of the supervisory authority.

นอกจากแนวทางในการรักษาความมั่นคงปลอดภัยข้างต้น เมื่อเกิดการรั่วไหลของข้อมูลส่วนบุคคล ซึ่งอาจก่อให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูล LED กำหนดให้มีการแจ้งเหตุต่อหน่วยงานกำกับดูแลโดยไม่ชักช้า และหากการแจ้งเหตุไม่ได้กระทำภายใน 72 ชั่วโมงนับแต่ทราบเหตุ ก็จะต้องมีการแจ้งเหตุผลของความล่าช้ามา[221] แต่ในกรณีที่การรั่วไหลของข้อมูลส่วนบุคคลมีแนวโน้มจะทำให้เกิดความเสี่ยงอย่างสูงต่อสิทธิและเสรีภาพของบุคคล การแจ้งเหตุต้องมีการแจ้งไปยังเจ้าของข้อมูลส่วนบุคคลร่วมด้วย โดยอย่างน้อยจะต้องให้ข้อมูลชื่อและรายละเอียดการติดต่อเพื่อขอข้อมูลเพิ่มเติม ผลกระทบที่อาจเกิดขึ้น และมาตรการแก้ไขปัญหา ด้วยภาษาที่ชัดเจนและไม่ซับซ้อน เว้นแต่มีเหตุยกเว้นตามที่กฎหมายบัญญัติ[222]

(ช.) หลักความรับผิดชอบ (Accountability) กำหนดให้ต้องมีบุคคลผู้รับผิดชอบดำเนินการให้สอดคล้องกับหลักการคุ้มครองข้อมูลส่วนบุคคล โดย LED กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้มีหน้าที่รับผิดชอบ เช่นเดียวกันกับ GDPR[223] แต่ภายใต้บทนิยาม LED ผู้ควบคุมข้อมูลส่วนบุคคล (Data controller) จะหมายถึงหน่วยงานผู้มีอำนาจรับผิดชอบ ซึ่งกำหนดวัตถุประสงค์และวิธีการประมวลผลข้อมูล[224] หรืออีกนัยหนึ่งคือ เป็นหน่วยงานผู้บังคับใช้กฎหมายที่มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล

เมื่อผู้ควบคุมข้อมูลส่วนบุคคลมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจึงย่อมมีความรับผิดชอบในการดำเนินงานให้เป็นไปตามมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของ LED ตั้งแต่การประมวลผลข้อมูลให้สอดคล้องกับฐานทางกฎหมาย การรักษาความมั่นคงปลอดภัย ตลอดจนการจัดให้มีกระบวนการตรวจสอบและติดตามการปฏิบัติตามกฎหมาย[225] ซึ่งมีหน้าที่ที่เกี่ยวข้องด้วยกันหลายประการ อาทิ

1.) <u>หน้าที่บันทึกรายการประมวลผลข้อมูลส่วนบุคคล</u>

สำหรับหน้าที่นี้ LED ไม่เพียงกำหนดให้มีการบันทึกข้อมูลรายละเอียดของการประมวลผลข้อมูลส่วนบุคคล[226] แต่ยังกำหนดให้บันทึกข้อมูลจราจร (Logs) ซึ่งประกอบด้วย (1) ข้อมูลการดำเนินการต่อข้อมูลส่วนบุคคล (2) วันและเวลา

---

[221] LED, Article 30 Notification of a personal data breach to the supervisory authority.

[222] LED, Article 31 Communication of a personal data breach to the data subject.

[223] LED, Article 4 (4).

[224] LED, Article 3 (8).

[225] คณาธิป ทองรวีวงศ์, <u>คำอธิบาย หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล</u>, หน้า.

[226] LED, Article 24 Records of processing activities and Recital 56.

ที่ดำเนินการ (3) บุคคลผู้ดำเนินการ และผู้รับข้อมูล (ถ้ามี) รวมถึง (4) เหตุผลในการดำเนินการ เท่าที่จะกระทำได้[227] หน้าที่บันทึกรายการประมวลผลข้อมูลส่วนบุคคลของ LED จึงมีความเคร่งครัดมากกว่า GDPR

2.) <u>หน้าที่ควบคุมกำกับผู้ประมวลผลข้อมูลส่วนบุคคล</u>
หากการประมวลผลข้อมูลมีบุคคลหรือนิติบุคคลอื่น หรือที่เรียกว่าผู้ประมวลผลข้อมูลส่วนบุคคล (Data processor) ดำเนินการในนามผู้ควบคุมข้อมูลส่วนบุคคล[228] กรณีเช่นนี้จะเป็นหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลที่ต้องกำกับให้ผู้ประมวลผลข้อมูลส่วนบุคคลไม่ทำการประมวลผลข้อมูลนอกเหนือไปจากคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล และปฏิบัติให้สอดคล้องกับ LED โดยทำสัญญา ข้อตกลง หรือเอกสารอื่นใด เพื่อให้มีผลผูกพันทางกฎหมาย[229]

3.) <u>หน้าที่แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล</u>
เพื่อให้มีการตรวจสอบการปฏิบัติตาม LED ของหน่วยงานผู้มีอำนาจรับผิดชอบ ผู้ควบคุมข้อมูลส่วนบุคคลจึงมีหน้าที่ที่จะต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data protection officer: “DPO”)[230] อย่างไรก็ดี LED จะไม่ได้มีบทบัญญัติคุ้มครองความเป็นอิสระของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไว้อย่างชัดแจ้ง แตกต่างจาก GDPR

นอกเหนือจากหน้าที่สามประการข้างต้น ผู้ควบคุมข้อมูลส่วนบุคคลยังมีหน้าที่ดำเนินการให้เป็นไปตามสิทธิของเจ้าของข้อมูลส่วนบุคคล เมื่อมีการร้องขอจากเจ้าของข้อมูลส่วนบุคคล ซึ่งจะได้กล่าวรายละเอียดในหัวข้อถัดไป

---

[227] LED, Article 25 Logging and Recital 57.

[228] LED, Article 3 (9).

[229] LED, Article 22 Processor.

[230] LED, Section 3 Data protection officer.

4.1.2.2.2 สิทธิของเจ้าของข้อมูลส่วนบุคคล

LED ได้รับรองสิทธิของเจ้าของข้อมูลส่วนบุคคลอยู่สามประการ ได้แก่

(ก.) สิทธิในการได้รับแจ้งข้อมูล (Right to be informed) คือ สิทธิของเจ้าของข้อมูลที่จะได้รับแจ้งรายละเอียดของการประมวลผลข้อมูลที่เกี่ยวกับตน ดังนี้[231]

1.) ข้อมูลทั่วไป (General information)
เป็นการแจ้งข้อมูลหรือรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล ซึ่งผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องจัดให้มีโดยเปิดเผยต่อสาธารณะเป็นการทั่วไป เช่น ข้อมูลการติดต่อผู้ควบคุมข้อมูลส่วนบุคคลหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล วัตถุประสงค์ของการประมวลผลข้อมูลตลอดจนสิทธิต่าง ๆ ของเจ้าของข้อมูล[232]

2.) ข้อมูลจำเพาะ (Specific information)
เป็นการแจ้งข้อมูลและรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลเพิ่มเติม เพื่อให้เจ้าของข้อมูลสามารถใช้สิทธิต่าง ๆ ตามกฎหมายได้ อาทิ ฐานทางกฎหมายในการประมวลผลข้อมูล ระยะเวลาเก็บรักษา หรือรายละเอียดของผู้รับโอนข้อมูล ฯลฯ โดยผู้ควบคุมข้อมูลส่วนบุคคลควรแจ้งข้อมูลเหล่านี้ให้เจ้าของข้อมูลทราบในโอกาสแรก ก่อนการประมวลผลข้อมูล เว้นแต่การแจ้งดังกล่าวมีผลเป็นการขัดต่อวัตถุประสงค์ของการประมวลผล ให้การแจ้งกระทำภายหลังจากนั้น[233]

เพื่อให้เป็นไปตามสิทธิของเจ้าของข้อมูลส่วนบุคคล การแจ้งข้อมูลข้างต้นจะต้องอยู่ในรูปแบบที่เข้าถึงได้ง่าย และใช้ภาษาเรียบง่ายชัดเจน ไม่ซับซ้อน โดยเฉพาะในการสื่อสารกับเจ้าของข้อมูลที่เป็นกลุ่มเปราะบาง เช่น เด็กหรือผู้เยาว์ เป็นต้น[234]

---

[231] Council of Europe, "Practical Guide on the Use of Personal Data in the Police Sector."

[232] Ibid.; LED, Article 13 (1).

[233] Ibid.; LED, Article 13 (2).

[234] LED, Recital 39.

(ข.) สิทธิที่จะเข้าถึงข้อมูล (Right to access) เป็นการรับรองสิทธิของเจ้าของข้อมูลที่จะได้รับการยืนยันว่าข้อมูลส่วนบุคคลเกี่ยวกับตนถูกนำไปประมวลผลหรือไม่ อย่างไร โดยให้เจ้าของข้อมูลเข้าถึงและรับสำเนาข้อมูลส่วนบุคคล รวมถึงข้อมูลที่เกี่ยวข้อง[235] อาทิ

- วัตถุประสงค์หรือฐานทางกฎหมายในการประมวลผล
- ประเภทของข้อมูลส่วนบุคคลที่ถูกนำไปประมวลผล
- ผู้ที่ได้รับการเปิดเผยข้อมูลส่วนบุคคล
- ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
- สิทธิของเจ้าของข้อมูลส่วนบุคคล
- ที่มาของข้อมูลส่วนบุคคลดังกล่าว

ด้วยเหตุนี้ สิทธิที่จะเข้าถึงข้อมูลจึงเป็นสิทธิขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล เนื่องจากเป็นการทำให้เจ้าของข้อมูลรับรู้รายละเอียดต่าง ๆ เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลของตน เจ้าของข้อมูลจึงมีโอกาสที่จะตรวจสอบและใช้สิทธิประเภทอื่นได้ต่อไป[236]

อนึ่ง สำหรับการเปิดเผยที่มาของข้อมูล ผู้ควบคุมข้อมูลส่วนบุคคลต้องพึงระมัดระวังไม่ให้มีข้อมูลที่เปิดเผยตัวบุคคลธรรมดาเผยแพร่ออกไป โดยเฉพาะอย่างยิ่ง ในกรณีที่แหล่งที่มาของข้อมูลส่วนบุคคลนั้นมาจากแหล่งข้อมูลลับ[237]

(ค.) สิทธิที่จะแก้ไข ลบ หรือจำกัดการประมวลผลข้อมูล (Right to rectification or erasure of personal data and restriction of processing) หมายถึงสิทธิของเจ้าของข้อมูลส่วนบุคคลที่จะร้องขอให้มีการดำเนินการดังต่อไปนี้

กรณีที่ข้อมูลส่วนบุคคลไม่ถูกต้องสมบูรณ์ เจ้าของข้อมูลส่วนบุคคลย่อมมีสิทธิที่จะร้องขอให้แก้ไขข้อมูลดังกล่าว[238] แต่หากเป็นกรณีที่ข้อมูลส่วนบุคคลถูกประมวลผลโดยมิชอบด้วยกฎหมาย กล่าวคือเป็นการดำเนินการที่ไม่สอดคล้องหรือฝ่าฝืนหลักการพื้นฐานตามมาตรา 4 หลักความชอบด้วยกฎหมายและเป็นธรรมตามมาตรา 8 และหลักเกณฑ์การประมวลผลข้อมูลอ่อนไหวตามมาตรา 10 หรือในกรณีที่ข้อมูลส่วนบุคคลต้องถูกลบเพื่อให้เป็นไปตามพันธกรณีทางกฎหมายของ

---

[235] LED, Article 14.

[236] Council of Europe, "Practical Guide on the Use of Personal Data in the Police Sector."

[237] LED, Recital 43.

[238] LED, Article 16 (1).

ผู้ควบคุมข้อมูลส่วนบุคคล เช่น ข้อมูลที่ครบกำหนดระยะเวลาการเก็บรักษา กรณีเช่นนี้ เจ้าของข้อมูลจะมีสิทธิในการร้องขอให้มีการลบข้อมูลส่วนบุคคลซึ่งเกี่ยวกับตนได้[239]

อย่างไรก็ตาม ผู้ควบคุมข้อมูลส่วนบุคคลอาจจำกัดการประมวลผลข้อมูลแทนการลบได้ หากเป็นกรณีที่จำเป็นต้องเก็บรักษาข้อมูลดังกล่าวเพื่อใช้เป็นหลักฐาน หรือกรณีที่มีการโต้แย้งความไม่ถูกต้องของข้อมูล แต่ไม่สามารถยืนยันความถูกต้องของข้อมูลนั้นได้[240]

เมื่อข้อมูลส่วนบุคคลถูกแก้ไข ลบ หรือจำกัดการประมวลผลข้อมูล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งไปยังผู้รับข้อมูล เพื่อให้ทำการแก้ไข ลบ หรือจำกัดการประมวลผลข้อมูลส่วนบุคคลที่อยู่ในความครอบครองดังกล่าวด้วย[241]

ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ในการดำเนินการให้เป็นไปตามสิทธิทั้งสามประการข้างต้นนี้ โดยต้องอำนวยความสะดวกให้การใช้สิทธิเป็นไปโดยง่าย และต้องตอบสนองหรือปฏิบัติตามคำขอของเจ้าของข้อมูลโดยไม่ชักช้า เว้นแต่คำขอไม่สมเหตุสมผล (Unfounded) หรือฟุ่มเฟือยเกินความจำเป็น (Excessive) อย่างชัดแจ้ง[242] หรือมีเหตุปฏิเสธตามกฎหมาย[243] ได้แก่

- เพื่อไม่ให้เป็นอุปสรรคต่อการป้องกัน สืบสวน ตรวจจับ ดำเนินคดีหรือลงโทษทางอาญา
- เพื่อรักษาความมั่นคงปลอดภัยของสาธารณะ
- เพื่อรักษาความมั่นคงปลอดภัยของชาติ
- เพื่อปกป้องสิทธิและเสรีภาพของบุคคลอื่นใด

ยกตัวอย่างเช่น เมื่อมีการร้องขอให้แก้ไขความถูกต้องของข้อมูลส่วนบุคคลในคำให้การพยาน โดยที่ไม่สามารถยืนยันความถูกต้องของข้อมูลได้ชัดเจน ผู้ควบคุมข้อมูลส่วนบุคคลก็อาจปฏิเสธการใช้สิทธิดังกล่าวได้ เพราะจะส่งผลกระทบต่อการบังคับใช้กฎหมาย[244] เป็นต้น

ในกรณีที่มีการปฏิเสธคำขอ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งเหตุผลในการปฏิเสธให้เจ้าของข้อมูลทราบเป็นลายลักษณ์อักษรโดยไม่ชักช้า เว้นแต่การแจ้งเหตุดังกล่าวจะเป็น

---

[239] LED, Article 16 (2).

[240] LED, Article 16 (3).

[241] LED, Article 16 (6).

[242] LED, Article 12 (4).

[243] LED, Article 13 (3), Article 15 and Article 16 (4).

[244] LED, Recital 47.

อุปสรรคต่อการสืบสวนสอบสวนตามเหตุปฏิเสธต่าง ๆ ข้างต้น[245] ผู้ควบคุมข้อมูลส่วนบุคคลอาจเลือกที่จะปฏิเสธการใช้สิทธิ โดยไม่ให้เหตุผลได้ (Neutral reply) แต่ไม่ว่าในกรณีใด จะต้องมีการแจ้งสิทธิของเจ้าของข้อมูลที่จะได้รับการเยียวยา และสิทธิร้องเรียนต่อหน่วยงานกำกับดูแล เพราะเมื่อ LED มีข้อจำกัดการใช้สิทธิมากกว่า GDPR จึงจำเป็นต้องมีกลไกให้เจ้าของข้อมูลสามารถใช้สิทธิ “ทางอ้อม” ผ่านหน่วยงานกำกับดูแล[246] โดยร้องขอให้มีการตรวจสอบความชอบด้วยกฎหมายของการประมวลผล ซึ่งอย่างน้อยที่สุด หน่วยงานกำกับดูแลจะต้องแจ้งว่าได้ดำเนินการตรวจสอบอย่างไรบ้าง[247]

4.1.2.2.3 กลไกการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล

เพื่อบังคับใช้ LED สหภาพยุโรปกำหนดให้มีการจัดตั้งหน่วยงานกำกับดูแลที่มีความเป็นอิสระ (Independent supervisory authorities)[248] โดยหน่วยงานกำกับดูแลดังกล่าวจะมีหน้าที่ควบคุมกำกับดูแลให้มีการปฏิบัติตาม LED ตั้งแต่ให้คำแนะนำ วินิจฉัยเรื่องร้องเรียน ตรวจสอบความชอบด้วยกฎหมายของการประมวลผลข้อมูลส่วนบุคคล ซึ่งครอบคลุมถึงชั้นสืบสวนและสอบสวน และในกรณีที่มีการฝ่าฝืน LED หน่วยงานกำกับดูแลจะมีอำนาจออกคำเตือน สั่งแก้ไขปรับปรุง กระทั่งจำกัดหรือระงับการประมวลผลข้อมูลส่วนบุคคล อย่างไรก็ตาม การควบคุมกำกับดูแลนั้นต้องไม่กระทบความเป็นอิสระของศาล[249] ทั้งนี้ หน่วยงานกำกับดูแลภายใต้ LED อาจจัดตั้งให้เป็นหน่วยงานเดียวกันกับหน่วยงานที่มีอำนาจหน้าที่กำกับดูแลตาม GDPR ได้[250]

นอกเหนือจากการควบคุมกำกับดูแลการประมวลผลข้อมูลส่วนบุคคลภายในสภาพยุโรป LED ยังกำหนดเงื่อนไขการโอนข้อมูลส่วนบุคคลไปยังประเทศนอกสหภาพยุโรปด้วย โดยบัญญัติให้การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศจะกระทำได้ต่อเมื่อ[251]

---

[245] LED, Article 15 and Article 16 (4).

[246] LED, Article 17.

[247] Laura Drechsler, "Comparing Led and Gdpr Adequacy: One Standard Two Systems," Global Privacy Law Review 1, 2 (2020); Salami, E., "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."

[248] LED, Article 41-42.

[249] LED, Article 45 (2), 46-47.

[250] LED, Article 41 (3).

[251] LED, Article 35.

1.) การโอนนั้นเป็นการดำเนินการที่มีความจำเป็นเพื่อการป้องกัน สืบสวน ตรวจจับ ดำเนินคดี ลงโทษทางอาญา หรือรักษาความปลอดภัยสาธารณะ
2.) การโอนดังกล่าวเป็นการโอนไปยังผู้ควบคุมข้อมูลส่วนบุคคลที่มีวัตถุประสงค์เพื่อป้องกัน สืบสวน ตรวจจับ ดำเนินคดี ลงโทษทางอาญา หรือรักษาความปลอดภัยสาธารณะ
3.) กรณีที่ข้อมูลส่วนบุคคลเป็นข้อมูลที่ได้รับมาจากรัฐสมาชิกอื่นให้โอนได้ต่อเมื่อได้รับอนุญาตล่วงหน้า ตามที่กฎหมายของรัฐสมาชิกนั้นกำหนดไว้ เว้นแต่มีความจำเป็นเพื่อความมั่นคงหรือประโยชน์สาธารณะ และการอนุญาตล่วงหน้าไม่อาจกระทำได้ในเวลาที่เหมาะสม
4.) ประเทศปลายทางจะต้องมีระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพออย่างหนึ่งอย่างใด ต่อไปนี้
    - ได้รับการวินิจฉัยถึงระดับการคุ้มครองข้อมูลที่เพียงพอ (Adequacy decision) ตามมาตรา 36
    - มีการจัดมาตรการป้องกันที่เหมาะสม (Appropriate safeguards) ตามมาตรา 37
    - ในกรณีที่ประเทศปลายทางไม่มีระดับการคุ้มครองที่เพียงพอ การโอนจะกระทำได้เฉพาะในสถานการณ์พิเศษที่กำหนดไว้ในมาตรา 38
5.) ในกรณีที่มีการโอนข้อมูลส่วนบุคคลต่อไป จะต้องได้รับอนุญาตจากหน่วยงานผู้มีอำนาจรับผิดชอบซึ่งดำเนินการโอนเดิมหรือรัฐสมาชิกอื่นที่มีอำนาจ โดยคำนึงถึงปัจจัยที่เกี่ยวข้องทั้งหมด เช่น ความร้ายแรงของการกระทำผิด วัตถุประสงค์เดิมของการโอน และระดับการคุ้มครองข้อมูลส่วนบุคคล

สุดท้าย LED กำหนดให้รัฐสมาชิกของสหภาพยุโรปกำหนดบทลงโทษสำหรับกรณีที่มีการฝ่าฝืนกฎระเบียบ LED อีกด้วย เพื่อประกันว่า LED จะมีผลบังคับใช้ได้จริงในทางปฏิบัติ โดยต้องมีการกำหนดบทลงโทษทั้งสำหรับบุคคลธรรมดาและหน่วยงานที่เป็นนิติบุคคล[252]

[252] LED, Article 57 and Recital 89.

4.2 กฎหมายต่างประเทศ

สำหรับแนวทางตามกฎหมายต่างประเทศ ผู้เขียนกำหนดวัตถุแห่งการศึกษาอยู่สามประเทศ ได้แก่ สหราชอาณาจักร สหรัฐอเมริกา และสาธารณรัฐเกาหลี ตามลำดับ

4.2.1 สหราชอาณาจักร

ในระบบกฎหมายสหราชอาณาจักร สิทธิในความเป็นส่วนตัวและสิทธิที่จะได้รับความคุ้มครองข้อมูลส่วนบุคคลเป็นสิทธิที่มีคุณค่าในระดับรัฐธรรมนูญ โดยจะปรากฏอยู่ในคำพิพากษา (Case law) พระราชบัญญัติ และอนุสัญญาระหว่างประเทศที่สหราชอาณาจักรมีพันธะผูกพัน โดยเฉพาะ ECHR ซึ่ง The Human Rights Act 1998 บัญญัติอย่างชัดเจนว่าการดำเนินการใด ๆ ของหน่วยงานสาธารณะที่ไม่สอดคล้องกับหลักประกันสิทธิและเสรีภาพของ ECHR ถือเป็นการกระทำที่ไม่ชอบด้วยกฎหมาย[253] ดังนั้น เมื่อสิทธิในข้อมูลส่วนบุคคลเป็นสิทธิประการหนึ่งที่มีการรับรองไว้ใน ECHR สหราชอาณาจักรจึงจำเป็นต้องวางกลไกต่าง ๆ ในระบบกฎหมาย เพื่อปกป้องข้อมูลส่วนบุคคลจากการบังคับใช้กฎหมาย ซึ่งรวมถึงการสืบสวนและสอบสวนคดีอาญา อันอาจสรุปเป็นภาพรวมได้ คือ[254]

1.) การสืบสวนและสอบสวนต้องเป็นไปตามที่บทบัญญัติกฎหมายให้อำนาจ
2.) การสืบสวนและสอบสวนต้องมีกลไกตรวจสอบถ่วงดุลการใช้อำนาจ
3.) การสืบสวนและสอบสวนต้องอยู่ภายใต้กลไกกำกับดูแลภายใน โดยให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ทำหน้าที่ตรวจสอบให้การปฏิบัติงานภายในสอดคล้องกับหลักการคุ้มครองข้อมูลส่วนบุคคล
4.) การสืบสวนและสอบสวนจะต้องมีการทำงานร่วมกันกับหน่วยงานกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคล
5.) การสืบสวนและสอบสวนต้องสามารถถูกตรวจสอบจากหน่วยงานกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคลได้ โดยเฉพาะเมื่อข้อมูลมีการรั่วไหล

จะเห็นได้ว่าสหราชอาณาจักรมีมาตรการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาที่คล้ายคลึงกับสหภาพยุโรป กล่าวคือสหราชอาณาจักรมีการประกันสิทธิในข้อมูลส่วนบุคคลโดยกำหนดกรอบการใช้อำนาจสืบสวนและสอบสวนในบทบัญญัติกฎหมายต่าง ๆ พร้อมทั้งกำหนดให้การสืบสวนและสอบสวนคดีอาญาอยู่ในบังคับของกฎหมายคุ้มครองข้อมูลส่วนบุคคล ดังนี้

---

[253] The Human Rights Act 1998, Article 6 (1).

[254] UK Department for Digital Culture Media & Sport, "Explanatory Framework for Adequacy Discussion, Section F: Law Enforcement,"(2020).

4.2.1.1 กฎหมายวิธีพิจารณาความอาญา

เมื่อการสืบสวนและสอบสวนคดีอาญามีการดำเนินงานที่อาจส่งผลกระทบต่อสิทธิในข้อมูลส่วนบุคคล การสืบสวนและสอบสวนคดีอาญาจึงต้องดำเนินการให้สอดคล้องกับหลักประกันสิทธิในข้อมูลส่วนบุคคลภายใต้ ECHR ซึ่งกำหนดไว้ว่า การแทรกแซงสิทธิในความเป็นส่วนตัวจะต้องเป็นไปตามที่กฎหมายบัญญัติ เพื่อประโยชน์สาธารณะ โดยการแทรกแซงนั้นจะต้องมีลักษณะที่คาดหมายได้ คือมีพื้นฐานทางกฎหมายที่ชัดเจน ทั้งต้องมีมาตรการป้องกันสิทธิและเสรีภาพที่เหมาะสม[255]

ด้วยเหตุนี้ การประมวลผลข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาจึงต้องมีฐานทางกฎหมาย หรือบทบัญญัติกฎหมายรองรับอยู่เสมอ ซึ่งในระบบกฎหมายของสหราชอาณาจักร รายละเอียดของบทบัญญัติกฎหมายดังกล่าวอาจมีความแตกต่างกันไปตามระบบกฎหมายแต่ละพื้นที่ ได้แก่ (1) สกอตแลนด์ (2) อังกฤษและเวลส์ และ (3) ไอร์แลนด์เหนือ[256] แต่ในภาพรวม กฎหมายของสหราชอาณาจักรมีการกำหนดกรอบการใช้อำนาจสืบสวนและสอบสวนคดีอาญา ดังต่อไปนี้

ประการแรก การเก็บรวบรวมข้อมูลข่าวสาร เอกสาร หรือวัตถุ ที่มีข้อมูลส่วนบุคคลเป็นส่วนประกอบในชั้นสืบสวนและสอบสวนคดีอาญา ซึ่งรวมถึงการรวบรวมข้อมูลจากผู้ประกอบการภาคเอกชน จะกระทำได้ต่อเมื่อมีหมายค้น (Search warrants) หรือคำสั่งศาล (Production orders) โดยมีบทบัญญัติกฎหมายที่เกี่ยวข้องคือ[257]

- Criminal Law (Consolidation) (Scotland) และ Criminal Justice (Scotland) Act 2016 ใช้บังคับในสกอตแลนด์
- Police and Criminal Evidence Act 1984 (“PACE 1984”) ใช้บังคับในอังกฤษและเวลส์
- Police and Criminal Evidence Order ใช้บังคับในไอร์แลนด์เหนือ

ทั้งนี้ ในการขอหมายค้นหรือคำสั่งของศาล เจ้าหน้าที่ตำรวจสหราชอาณาจักรจะต้องยื่นคำร้องขอ โดยแสดงเหตุผลอันสมควร ความจำเป็นในการใช้อำนาจ พร้อมทั้งต้องระบุรายละเอียดเกี่ยวกับบุคคล สิ่งของ ตลอดจนสถานที่ที่ต้องการค้นให้ได้มากที่สุดเท่าที่จะกระทำได้ เพื่อให้การค้น

---

[255] 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."

[256] UK Department for Digital Culture Media & Sport, "Explanatory Framework for Adequacy Discussion, Section F: Law Enforcement."

[257] 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."

ก้าวล่วงสิทธิส่วนบุคคลเท่าที่จำเป็นและเกี่ยวข้องกับวัตถุประสงค์ในการสืบสวนและสอบสวนคดีอาญามิฉะนั้น การค้นดังกล่าวก็อาจถูกโต้แย้งได้ว่าเป็นการค้นที่ไม่ชอบด้วยกฎหมาย[258]

ตัวอย่างเช่น คดี R (F) v. Blackfriars Crown Court (2014) ซึ่งปรากฏข้อเท็จจริงว่ามีการออกหมายค้นโดยระบุสิ่งของที่ต้องการค้นว่า จดหมายโต้ตอบ เอกสาร สำนวน ใบค่าธรรมเนียม ใบแจ้งหนี้ที่เกี่ยวข้องกับคดี รวมถึงคอมพิวเตอร์หรืออุปกรณ์จัดเก็บข้อมูลอื่น ๆ ที่สามารถจัดเก็บข้อมูลข้างต้นนั้น ศาลวินิจฉัยว่าเป็นหมายค้นที่ไม่ชอบด้วยกฎหมาย เนื่องจากหมายค้นดังกล่าวระบุสิ่งของที่ต้องการค้นไว้อย่างกว้าง โดยขาดการระบุรายละเอียดที่ชัดเจน หมายค้นในกรณีนี้จึงไม่มีหลักประกันอย่างเพียงพอว่าการค้นจะจำกัดเฉพาะข้อมูลหรือการสื่อสารที่เกี่ยวข้อง[259]

ประการที่สอง การใช้อำนาจสอบสวนพิเศษ (Investigatory powers) จะต้องผ่านกระบวนการตรวจสอบถ่วงดุลสองชั้น หรือที่เรียกว่า “Double-lock” โดยมี Investigatory Powers Act 2016 (“IPA 2016”) เป็นบทบัญญัติหลัก ประกอบกับบทบัญญัติต่อไปนี้[260]

- Regulation of Investigatory Powers Act 2000 (“RIPA”) ใช้บังคับในอังกฤษ เวลส์ และไอร์แลนด์เหนือ
- Regulation of Investigatory Powers (Scotland) Act 2000 (“RIPSA”) ใช้บังคับในสกอตแลนด์

โดยอำนาจสอบสวนพิเศษภายใต้ IPA 2016 หมายถึงการใช้มาตรการที่มีผลเป็นการแทรกแซงสิทธิความเป็นส่วนตัว ไม่ว่าจะเป็นการดักรับข้อมูลการสื่อสาร (Targeted interceptions) การได้มาซึ่งข้อมูลการสื่อสาร (Acquisition of communications data) การกำหนดให้ผู้ประกอบการเก็บรักษาข้อมูลการสื่อสาร (Retention of communications data) ตลอดจนการใช้อุปกรณ์รบกวนการสื่อสาร (Targeted equipment interference) เป็นต้น ซึ่งในระบบกฎหมายสหราชอาณาจักร การใช้อำนาจสอบสวนพิเศษตาม IPA 2016 จะจำกัดเฉพาะเพื่อการสืบสวนและสอบสวนอาชญากรรมร้ายแรง (Serious crimes)[261] และเป็นอำนาจเฉพาะของหน่วยงานบังคับใช้กฎหมายบางแห่งเท่านั้น[262]

---

[258] Ibid.

[259] R (F) v Blackfriars Crown Court [2014] EWHC 1541 (admin).

[260] 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."

[261] โปรดดู IPA, Article 263 (1).

[262] ยกตัวอย่างเช่น the Director General of the National Crime Agency, the Commissioner of Police of the Metropolis, the Chief Constable of the Police Service of Northern Ireland, the Chief Constable of the Police Service of Scotland, the Commissioner for Her Majesty’s Revenue and Customs, the Chief of Defence Intelligence, and etc.

ในขณะเดียวกัน การใช้อำนาจสอบสวนพิเศษดังกล่าวก็จำต้องอาศัยอำนาจตามหมาย ซึ่งออกโดยผ่านกระบวนการ Double-lock ที่มีระบบการตรวจสอบถ่วงดุลสองชั้น กล่าวคือ

1.) <u>การออกหมายโดยหน่วยงานผู้มีอำนาจหน้าที่</u>
โดยทั่วไป รัฐมนตรี (Secretary of State)[263] เป็นบุคคลผู้มีอำนาจออกหมายตามคำร้องขอของหน่วยงานบังคับใช้กฎหมาย ตามเงื่อนไขและหลักเกณฑ์ที่ระบุไว้ใน IPA 2016 เป็นลำดับแรก[264]

2.) <u>การอนุมัติหมายโดยศาล</u>
ภายหลังจากรัฐมนตรีออกหมาย หมายดังกล่าวจะต้องได้รับการอนุมัติจากศาล (Judicial Commissioners) อีกขั้นตอนหนึ่ง เว้นแต่ในกรณีเร่งด่วน ที่สามารถดำเนินการก่อนได้โดยไม่ต้องผ่านการอนุมัติจากศาล อย่างไรก็ตาม ภายใน 3 วัน นับแต่ออกหมายในกรณีเร่งด่วน จะต้องมีการนำหมายในกรณีนั้นมาให้ศาล เพื่อพิจารณาอนุมัติอีกครั้ง ซึ่งหากศาลไม่เห็นชอบ การดำเนินการตามหมายนั้นจะต้องยุติลงทันที และให้ทำลายสิ่งของที่ได้มาโดยอาศัยอำนาจตามหมายนั้นด้วย[265]

การออกหมายด้วยกระบวนการ Double-lock จึงเป็นกลไกที่มีความสำคัญอย่างยิ่งในการถ่วงดุลการใช้อำนาจสอบสวนพิเศษตาม IPA 2016 เนื่องจากเป็นการให้ฝ่ายตุลาการตรวจสอบความจำเป็นและความได้สัดส่วนของการออกหมายอีกชั้นหนึ่ง ยิ่งไปกว่านั้น มีข้อสังเกตว่า IPA 2016 มีการบัญญัติกฎเกณฑ์ทั่วไปเพื่อคุ้มครองความเป็นส่วนตัวของบุคคล (General privacy protection) เอาไว้อีกด้วย[266] สะท้อนให้เห็นว่า ระบบกฎหมายของสหราชอาณาจักรให้ความสำคัญกับการประกันสิทธิส่วนบุคคล ครอบคลุมไปถึงการดำเนินงานในชั้นสืบสวนและสอบสวนคดีอาญา

4.2.1.2 กฎหมายคุ้มครองข้อมูลส่วนบุคคล (The UK DPA)

ปัจจุบัน สหราชอาณาจักรเป็นเพียงประเทศเดียวที่ได้รับการรับรองจากสหภาพยุโรปถึงระดับการคุ้มครองข้อมูลที่เพียงพอตามมาตรฐาน GDPR และ LED ในวันที่ 28 มิถุนายน ค.ศ. 2021 ภายหลังจากสหราชอาณาจักรถอนตัวจากการเป็นสมาชิกภาพของสหภาพยุโรปอย่างเป็นทางการเมื่อวันที่ 31 มกราคม ค.ศ. 2020 ทั้งนี้ เนื่องจากในการสิ้นสุดความเป็นสมาชิกภาพ สหราชอาณาจักรได้

---

[263] ในบางกรณี อำนาจในการออกหมายจะเป็นอำนาจของ Scottish minister โปรดดู IPA, Article 21-22.

[264] โปรดดู IPA, Article 18-20.

[265] โปรดดู IPA, Article 23-25.

[266] โปรดดู IPA, Part 1 General privacy protection.

ทำข้อตกลงร่วมกับสหภาพยุโรปให้มีระยะเวลาการเปลี่ยนผ่าน (Transition Period) เพื่อให้กฎหมายของสหภาพยุโรปมีผลถึงวันที่ 31 ธันวาคม ค.ศ. 2020 และแม้จะพ้นช่วงระยะเวลาเปลี่ยนผ่านดังกล่าว กฎหมายสหภาพยุโรปบางส่วนก็ยังถือเป็นส่วนหนึ่งของกฎหมายภายในสหราชอาณาจักร หรือที่เรียกว่า “EU-derived domestic legislation” ด้วยการประกาศใช้ the European Union Withdrawal Act 2018 (“the EUWA”)[267] ซึ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคล (the Data Protection Act 2018: “the UK DPA”) ก็เป็นหนึ่งใน EU-derived domestic legislation ภายใต้ the EUWA ด้วยเช่นกัน การคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักรจึงยังคงมีสาระสำคัญเช่นเดียวกันกับกฎหมายของสหภาพยุโรป โดย the UK DPA ได้แยกการคุ้มครองข้อมูลส่วนบุคคลออกเป็นสามระบบ ได้แก่[268]

1.) PART 2: General Processing
เป็นกฎเกณฑ์การประมวลผลข้อมูลส่วนบุคคลทั่วไปที่มีพื้นฐานจาก GDPR ของสหภาพยุโรป หรือที่เรียกว่า “the UK GDPR”
2.) PART 3: Law Enforcement Processing
เป็นกฎเกณฑ์เฉพาะสำหรับการประมวลผลข้อมูลส่วนบุคคลที่มีวัตถุประสงค์เพื่อการบังคับใช้กฎหมายอาญา โดยมีฐานมาจาก LED ของสหภาพยุโรป
3.) PART 4: Intelligence Services Processing
เป็นกฎเกณฑ์พิเศษแยกต่างหากสำหรับการประมวลผลข้อมูลส่วนบุคคลในหน่วยข่าวกรองของสหราชอาณาจักรโดยเฉพาะ

จะเห็นได้ว่าสหราชอาณาจักรไม่ได้จัดทำพระราชบัญญัติเฉพาะในการคุ้มครองข้อมูลส่วนบุคคลจากการบังคับใช้กฎหมายอาญา แต่จะใช้วิธีการบัญญัติหลักเกณฑ์แยกเป็นหมวดหมู่ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับเดียว โดยสหราชอาณาจักรไม่เพียงแต่กำหนดหลักเกณฑ์เฉพาะสำหรับการบังคับใช้กฎหมายอาญา แต่ยังแยกการดำเนินงานในหน่วยข่าวกรองออกมาอีกด้วย เพื่อให้เกิดความชัดเจนในการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล

อนึ่ง เนื่องด้วยวิจัยฉบับนี้เป็นการศึกษาแนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา ผู้เขียนจึงจำกัดขอบเขตการศึกษาเฉพาะ PART 3: Law Enforcement Processing ซึ่งเป็นกฎเกณฑ์เฉพาะสำหรับการประมวลผลข้อมูลส่วนบุคคลที่มีวัตถุประสงค์เพื่อการบังคับใช้กฎหมายอาญาเท่านั้น โดยมีสาระสำคัญดังนี้

---

[267] 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."
[268] Information Commission’s Office (ICO), "An Overview of the Data Protection Act 2018."

Part 3: Law Enforcement Processing มีขอบเขตการบังคับใช้ (Material Scope) เฉพาะการประมวลผลข้อมูลส่วนบุคคลภายในสหราชอาณาจักร ที่มีลักษณะต่อไปนี้[269]

1.) การประมวลผลข้อมูลส่วนบุคคลนั้นเป็นดำเนินการโดยหน่วยงานผู้มีอำนาจรับผิดชอบ (Competent Authorities)[270]
2.) วัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลต้องเป็นไปเพื่อบังคับใช้กฎหมายอาญา (Law Enforcement Purposes) อาทิ เพื่อป้องกัน สืบสวน ตรวจสอบ ดำเนินคดี ลงโทษอาญา หรือรักษาความปลอดภัยสาธารณะ[271]
3.) การประมวลผลข้อมูลส่วนบุคคลใช้วิธีการอัตโนมัติ ไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลส่วนบุคคลที่ถูกประมวลผลเป็นส่วนหนึ่งหรือมุ่งหมายที่จะให้เป็นส่วนหนึ่งของระบบแฟ้มข้อมูล[272]

มีข้อสังเกตว่าขอบเขตการบังคับใช้ Part 3: Law Enforcement Processing ข้างต้นเป็นขอบเขตเช่นเดียวกับ LED กล่าวคือมีผลบังคับใช้ครอบคลุมไปถึงการสืบสวนและสอบสวนคดีอาญาเพียงแต่สหราชอาณาจักรมีการระบุรายชื่อหน่วยงานภาครัฐที่อยู่ในความหมายของหน่วยงานผู้มีอำนาจรับผิดชอบในตารางที่ 7 ของ the UK DPA[273] เพื่อไม่ให้เกิดปัญหาการตีความ แต่ในกรณีที่มีหน่วยงานอื่นใดที่มีอำนาจหน้าที่ นอกเหนือจากที่ระบุไว้ในตาราง the UK DPA ก็มีบทบัญญัติเปิดช่องให้สามารถตีความครอบคลุมถึงหน่วยงานเหล่านี้ด้วย[274]

นอกเหนือจากขอบเขตการใช้บังคับ นิยามของข้อมูลส่วนบุคคลที่ได้รับความคุ้มครอง รวมถึงหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาตาม Part 3: Law Enforcement Processing ต่างมีสาระสำคัญเป็นอย่างเดียวกับ LED ของสหภาพยุโรปทั้งสิ้น เนื่องจาก Part 3: Law Enforcement Processing ถูกจัดทำขึ้นโดยอนุวัติการหลักเกณฑ์ของ LED ให้มากที่สุด

---

[269] 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."; Information Commission's Office (ICO), "Guide to Law Enforcement Processing " [Online] Accessed: 14 December 2020. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/

[270] The UK DPA, Article 29.

[271] The UK DPA, Article 31.

[272] The UK DPA, Article 29 (1).

[273] โปรดดู The UK DPA, SCHEDULE 7 Competent authorities.

[274] The UK DPA, Article 30.

เท่าที่จะกระทำได้[275] ไม่ว่าจะเป็นบทนิยาม หลักการประมวลผลข้อมูลส่วนบุคคล[276] สิทธิของเจ้าของข้อมูลส่วนบุคคล[277] หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล[278] ตลอดจนการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ[279] จึงไม่แปลกที่สหภาพยุโรปรับรองให้สหราชอาณาจักรมีระดับการคุ้มครองข้อมูลส่วนบุคคลที่เทียบเท่ากับมาตรฐาน LED ของสหภาพยุโรป

แต่ถึงกระนั้น พบว่า PART 3: Law Enforcement Processing ของ the UK DPA และ LED กลับมีข้อแตกต่างสำคัญอยู่ประการหนึ่งคือ “ฐานการประมวลข้อมูลส่วนบุคคล” เนื่องจาก PART 3: Law Enforcement Processing ยอมรับให้ความยินยอมของเจ้าของข้อมูลเป็นหนึ่งในฐานการประมวลผลข้อมูลส่วนบุคคลในการบังคับใช้กฎหมาย[280] ขณะที่สหภาพยุโรปเห็นว่าการประมวลผลข้อมูลส่วนบุคคลเพื่อการบังคับใช้กฎหมายควรอยู่บนพื้นฐานของบทบัญญัติกฎหมายเท่านั้น[281]

เหตุที่สหราชอาณาจักรยอมรับให้ความยินยอมของเจ้าของข้อมูลส่วนบุคคลเป็นฐานในการประมวลผลข้อมูลส่วนบุคคลได้ เนื่องจากสหราชอาณาจักรมองว่าบางสถานการณ์ การขอความยินยอมจากเจ้าของข้อมูลจะมีความเหมาะสมมากกว่า เช่น ในกรณีที่เป็นการขอข้อมูลส่วนบุคคลของผู้เสียหาย หรือการขออนุญาตตรวจสอบสารพันธุกรรมของบุคคลผู้สูญหาย เพื่อเชื่อมโยงข้อมูลกับร่างของผู้เสียชีวิตที่ไม่สามารถระบุตัวตนได้ เป็นต้น[282] แต่ในบริบทของการบังคับใช้กฎหมาย ICO ระบุว่าความยินยอมอาจไม่ใช่ฐานการประมวลที่เหมาะสมนัก การสืบสวนและสอบสวนคดีอาญาจึงควรอาศัยความยินยอมเป็นฐานการประมวลผลข้อมูลส่วนบุคคลอย่างจำกัดเฉพาะในบางสถานการณ์เท่านั้น ทั้งนี้การขอความยินยอมจะต้องเป็นไปโดยชัดแจ้ง ใช้ภาษาที่เข้าใจง่าย โดยเจ้าของข้อมูลต้องมีอิสระในการตัดสินใจให้ความยินยอม และต้องสามารถถอนความยินยอมด้วยวิธีที่กระทำได้โดยง่ายอีกด้วย[283]

---

[275] UK Department for Digital Culture Media & Sport, "Explanatory Framework for Adequacy Discussion, Section F: Law Enforcement."

[276] โปรดดู The UK DPA, CHAPTER 2 Principle.

[277] โปรดดู The UK DPA, CHAPTER 3 Rights of the data subject.

[278] โปรดดู The UK DPA, CHAPTER 4 Controller and processor.

[279] โปรดดู The UK DPA, CHAPTER 5 Transfers of personal data to third countries etc.

[280] The UK DPA, Article 35 (2).

[281] 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."

[282] Ibid.

[283] Information Commission’s Office (ICO), "Guide to Law Enforcement Processing "

สำหรับการบังคับใช้ PART 3: Law Enforcement Processing ของ the UK DPA องค์กรที่มีอำนาจหน้าที่จะเป็น ICO องค์กรอิสระที่สหราชอาณาจักรจัดตั้งขึ้นเพื่อให้ควบคุมกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคลเป็นการเฉพาะ ทั้งในส่วนของการประมวลผลข้อมูลส่วนบุคคลทั่วไป และการประมวลผลข้อมูลส่วนบุคคลในการบังคับใช้กฎหมาย ซึ่ง ICO จะมีอำนาจหน้าที่ในการตรวจสอบการละเมิดข้อมูลส่วนบุคคล โดยใช้อำนาจสอบสวนเข้าถึงข้อมูลและเอกสารที่เกี่ยวข้อง ซึ่งหากพบว่ามีการละเมิดเกิดขึ้นจริง ICO จะมีอำนาจออกคำเตือนหรือคำสั่งให้มีการแก้ไข ดำเนินการ หรือยุติการดำเนินการ[284] อีกทั้ง ICO ยังมีบทบาทในการให้คำปรึกษาและจัดทำแนวปฏิบัติ (Guidance) รวมถึงมีบทบาทเชิงรุกในการตรวจสอบและประเมินความสอดคล้องกับ the UK DPA ของการดำเนินงานต่าง ๆ รวมถึงการดำเนินงานในชั้นสืบสวนและสอบสวนคดีอาญา โดยเฉพาะกรณีการใช้เทคโนโลยีสมัยใหม่ เช่น การตรวจสอบการใช้เทคโนโลยีจดจำใบหน้าของ South Wales Police (2020) หรือเทคโนโลยีเมทริกซ์ที่เรียกว่า “Gang matrix” ของ Metropolitan Police Service[285]

สุดท้าย เพื่อให้การบังคับใช้มีประสิทธิภาพ สหราชอาณาจักรจึงกำหนดให้การฝ่าฝืนบทบัญญัติตาม PART 3: Law Enforcement Processing ของ the UK DPA อาจนำไปสู่โทษปรับทางปกครอง และความรับผิดทางอาญา เช่นเดียวกับการประมวลผลข้อมูลส่วนบุคคลในกรณีทั่วไป[286]

4.2.2 สหรัฐอเมริกา

แม้แนวคิดเกี่ยวกับสิทธิความเป็นส่วนตัวในสหรัฐอเมริกาจะได้รับการจุดประกายครั้งใหญ่จากการเผยแพร่บทความเรื่อง “The Right to Privacy” ของ Louis Brandeis และ Samuel Warren[287] แต่สหรัฐอเมริกาก็ไม่มีการจัดทำกฎหมายคุ้มครองข้อมูลส่วนบุคคลในลักษณะกฎหมายกลางแต่อย่างใด แนวทางการคุ้มครองข้อมูลส่วนบุคคลของสหรัฐอเมริกาจึงมีรูปแบบเป็นกฎหมายเฉพาะเรื่องเฉพาะกรณี (Sectoral Law) ตามแต่ประเภทกิจการและลักษณะปัญหาที่เกิดขึ้น กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหรัฐอเมริกาจึงมีบ่อเกิดกฎหมายที่หลากหลาย ปรากฏอยู่ในรูปแบบต่าง ๆ ต่อไปนี้[288]

---

[284] 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."

[285] Ibid.; UK Department for Digital Culture Media & Sport, "Explanatory Framework for Adequacy Discussion, Section F: Law Enforcement."

[286] The UK DPA, Article 170-173.

[287] นคร เสรีรักษ์, ความเป็นส่วนตัว: ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย, หน้า 157.

[288] อ้างแล้ว, หน้า 159-162.; ประสิทธิ์ ปิวาวัฒนพานิช, "กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกาและประเทศออสเตรเลีย," วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ 34, 4 (ธันวาคม 2547).

1.) รัฐธรรมนูญและคำวินิจฉัยของศาลสูง

2.) กฎหมายสหพันธรัฐ (Federal Law) และกฎหมายมลรัฐ (State Law)

3.) ข้อบังคับ (Regulations)

4.) คำพิพากษาของศาล (Case Law) และหลักคอมมอนลอว์ (Common Law)

ทั้งนี้ ศาสตราจารย์ ดร. ประสิทธิ์ ปิวาวัฒนพานิช ให้ความเห็นว่า รูปแบบการคุ้มครองข้อมูลส่วนบุคคลเช่นนี้อาจมีที่มาจากเหตุผลทางปรัชญาและประวัติศาสตร์การสร้างชาติของสหรัฐอเมริกาที่ไม่ประสงค์ให้เจ้าหน้าที่รัฐลิดรอนสิทธิและเสรีภาพ และขณะเดียวกัน ก็ต้องการรับรองให้ประชาชนมีสิทธิและเสรีภาพที่จะดำเนินธุรกิจแบบทุนนิยม[289] เช่นเดียวกับที่รองศาสตราจารย์คณาธิป ทองรวีวงศ์ เห็นว่าพื้นฐานทางวัฒนธรรมของประชาชนสหรัฐอเมริกา จะมีความสงสัยต่อรัฐบาล ให้ความไว้วางใจกับธุรกิจและเทคโนโลยี รวมถึงให้ความสำคัญกับอิสระในการพูดหรือแสดงความคิดเห็น สหรัฐอเมริกาจึงไม่ต้องการควบคุมการใช้ข้อมูลของภาคเอกชนเข้มงวดเท่าสหภาพยุโรป[290]

สำหรับการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา แม้สหรัฐอเมริกาจะมิได้มีกฎหมายกลางในการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาเป็นการเฉพาะ แต่ผู้เขียนเห็นว่า การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนของสหรัฐอเมริกานั้นได้รับการพัฒนาผ่านหลักการภายใต้รัฐธรรมนูญมาตั้งแต่อดีต โดยเฉพาะบทบัญญัติแก้ไขรัฐธรรมนูญครั้งที่ 4 ที่มุ่งคุ้มครองความเป็นส่วนตัวของพลเมืองจากการใช้อำนาจรัฐโดยมิชอบ

นอกจากบทบัญญัติแก้ไขรัฐธรรมนูญครั้งที่ 4 การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาของสหรัฐอเมริกายังอยู่ภายใต้บังคับของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในระดับสหพันธรัฐหรือมลรัฐอีกด้วย อย่างไรก็ดี มีความเป็นไปได้ที่การดำเนินงานในชั้นสืบสวนและสอบสวนคดีอาญาของสหรัฐอเมริกาจะมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องมากกว่าหนึ่งฉบับ เพราะรูปแบบการคุ้มครองข้อมูลส่วนบุคคลของสหรัฐอเมริกาจะปรากฏเป็นกฎหมายเฉพาะเรื่องเฉพาะกรณีกระจัดกระจายกันไป ดังนั้น ในหัวข้อที่ 4.2.2.2 ว่าด้วยกฎหมายคุ้มครองข้อมูลส่วนบุคคล ผู้เขียนจึงจำกัดขอบเขตการศึกษาไว้เฉพาะ The Privacy Act of 1974 เท่านั้น เนื่องจากกฎหมายดังกล่าวเป็นกฎหมายในระดับสหพันธรัฐฉบับแรกที่มุ่งคุ้มครองความเป็นส่วนตัวในข้อมูลของประชาชนมิให้ถูกล่วงละเมิดจากการอำนาจรัฐ ซึ่งรวมถึงการสืบสวนและสอบสวนคดีอาญา โดยมีรายละเอียดดังนี้

---

[289] อ้างแล้ว.

[290] คณาธิป ทองรวีวงศ์, "การปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน."

4.2.2.1 บทบัญญัติแก้ไขรัฐธรรมนูญครั้งที่ 4 (The Fourth Amendment)

บทบัญญัติแก้ไขรัฐธรรมนูญครั้งที่ 4 ของสหรัฐอเมริกา[291] บัญญัติไว้ว่า

“สิทธิในร่างกาย เคหสถาน เอกสาร และทรัพย์สินของประชาชนจะถูกละเมิดจากการค้นหรือยึดโดยปราศจากเหตุผลอันสมควรมิได้ และห้ามมิให้ออกหมายเพื่อกระทำการเช่นนั้น เว้นแต่จะมีเหตุอันควร ซึ่งรับรองด้วยคำสัตย์สาบานหรือคำปฏิญาณ โดยให้ระบุถึงสถานที่ ทรัพย์สิน และบุคคลที่จะทำการค้นหรือยึดอย่างเฉพาะเจาะจง”

แม้บทบัญญัติแก้ไขรัฐธรรมนูญครั้งที่ 4 ไม่ได้บัญญัติรับรองสิทธิความเป็นส่วนตัวหรือสิทธิในข้อมูลส่วนบุคคลไว้โดยชัดแจ้ง แต่จากแนวทางคำวินิจฉัยของศาลสูงในหลายกรณี พบว่าศาลสูงของสหรัฐอเมริกาได้อาศัยบทบัญญัติแก้ไขรัฐธรรมนูญครั้งที่ 4 เป็นฐานคุ้มครองสิทธิความเป็นส่วนตัว โดยรับรองให้บุคคลเป็นอิสระจากการค้นและยึดที่ไม่ชอบด้วยกฎหมาย[292] และกำหนดให้พยานหลักฐานที่ได้มาจากการค้นและยึดที่ไม่ชอบด้วยกฎหมายไม่อาจใช้เพื่อพิสูจน์ความผิดของผู้ถูกกล่าวหาได้[293]

ในอดีต ศาลสูงของสหรัฐอเมริกาตีความในคดี Olmstead v. United States (1928) ว่าการค้น (Searches) และยึด (Seizures) ภายใต้บทบัญญัติแก้ไขรัฐธรรมนูญครั้งที่ 4 มีขอบเขตจำกัดเฉพาะการค้นและยึดทางกายภาพเท่านั้น ไม่รวมถึงการแอบดักฟังการสนทนา[294] แต่ต่อมา คำวินิจฉัยดังกล่าวก็ถูกกลับในคดี Katz v. United States (1967)

คดี Katz v. United States (1967) มีข้อเท็จจริงว่าเจ้าหน้าที่กรมสอบสวนคดีพิเศษได้แอบบันทึกการสนทนาส่วนตัวขณะที่ Katz ใช้โทรศัพท์สาธารณะเพื่อติดต่อเล่นการพนัน แต่ในคดีนี้ศาลสูงได้วางหลัก “Reasonable Expectation of Privacy” หรือความคาดหมายในความเป็นส่วนตัวขึ้นมาเป็นครั้งแรก โดยศาลสูงได้วินิจฉัยว่าแม้การบันทึกการสนทนาจะเกิดขึ้นในตู้โทรศัพท์สาธารณะ แต่โดยทั่วไป บุคคลย่อมคาดหมายถึงความเป็นส่วนตัวในการติดต่อสื่อสารทางโทรศัพท์ พื้นที่ดังกล่าว

---

[291] Fourth Amendment.

“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized”

[292] คณาธิป ทองรวีวงศ์, "การปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน."

[293] ปิติ เอี่ยมจำรูญลาภ, "กฎหมายเกี่ยวกับการกำหนดให้รัฐเข้าถึง หรือได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกัน : กรณีศึกษาประเทศสหรัฐอเมริกา,"(ธันวาคม 2561).

[294] 277 US 438 (1928).

จึงเป็นพื้นที่ส่วนตัวที่อยู่ในขอบเขตความคุ้มครองตามบทบัญญัติแก้ไขรัฐธรรมนูญครั้งที่ 4[295] แสดงให้เห็นว่าบทบัญญัติแก้ไขรัฐธรรมนูญครั้งที่ 4 มุ่งคุ้มครองสิทธิส่วนบุคคล มิใช่สถานที่[296]

อย่างไรก็ตาม ในคดี Smith v. Maryland (1979) ซึ่งปรากฏข้อเท็จจริงว่าเจ้าหน้าที่ตำรวจขอความร่วมมือจากผู้ประกอบกิจการโทรคมนาคม ติดตั้งอุปกรณ์ Pen register เพื่อตรวจสอบประวัติการโทรศัพท์ รวมถึงบุคคลที่จำเลยติดต่อนั้น ศาลสูงของสหรัฐอเมริกากลับวินิจฉัยว่าเป็นกรณีที่ไม่ได้รับการคุ้มครองตามบทบัญญัติแก้ไขรัฐธรรมนูญครั้งที่ 4 โดยให้เหตุผลว่าเมื่อจำเลยใช้โทรศัพท์ จำเลยย่อมคาดหมายได้ว่าผู้ให้บริการอาจมีการบันทึกรายการข้อมูลการใช้โทรศัพท์ เพื่อประโยชน์ในการบริการได้ จำเลยจึงไม่อาจคาดหมายความเป็นส่วนตัวในกรณีนี้[297]

ผลของคำพิพากษาคดี Smith v. Maryland (1979) จึงกลายเป็นที่มาของหลักการ “The third-party doctrine” กล่าวคือบุคคลที่สมัครใจให้ข้อมูลส่วนบุคคลของตนให้แก่บุคคลที่สาม เช่น ผู้ประกอบกิจการโทรคมนาคม หรือธนาคารพาณิชย์ ย่อมไม่อาจคาดหมายความเป็นส่วนตัวจากข้อมูลที่ตนให้แก่บุคคลที่สามไปด้วยความสมัครใจ[298]

นอกจากนี้ ยังปรากฏคำพิพากษาเกี่ยวกับการใช้อุปกรณ์ติดตาม (Tracking device) ในการสืบสวนและสอบสวนคดีอาญาอีกด้วย เช่น คดี United States v. Knotts (1983) ซึ่งศาลสูงของสหรัฐอเมริกาวินิจฉัยว่าการติดตั้งอุปกรณ์ติดตามบนสิ่งของ เพื่อตรวจสอบความเคลื่อนไหวของจำเลยระหว่างที่ขับขี่ยานพาหนะบนถนนสาธารณะนั้น ไม่เป็นการละเมิดบทบัญญัติแก้ไขรัฐธรรมนูญครั้งที่ 4 เพราะบุคคลทั่วไปย่อมมีความคาดหมายความเป็นส่วนตัวบนถนนสาธารณะน้อยกว่าที่พักอาศัย อีกทั้งอุปกรณ์ติดตามก็เป็นเพียงเครื่องมือเพิ่มประสิทธิภาพการทำงานของเจ้าหน้าที่ตำรวจเท่านั้น กล่าวคือแม้ไม่มีการติดตั้งอุปกรณ์ดังกล่าว เจ้าหน้าที่ตำรวจก็ยังอาจติดตามความเคลื่อนไหวของจำเลยในพื้นที่สาธารณะได้[299] แตกต่างจากข้อเท็จจริงในคดี United States v. Karo (1984) ซึ่งเป็นการใช้อุปกรณ์ติดตามเพื่อตรวจสอบความเคลื่อนไหวของจำเลยขณะอยู่ในที่พักอาศัย จึงได้รับความคุ้มครองภายใต้บทบัญญัติแก้ไขรัฐธรรมนูญครั้งที่ 4 ที่ต้องมีหมายค้นจากศาล[300]

---

[295] 389 US 347 (1967).

[296] คณาธิป ทองรวีวงศ์, "มาตรการทางกฎหมายในการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวของผู้ถูกดักฟังการสื่อสารข้อมูล," วารสารกระบวนการยุติธรรม 8, 1 (2556).

[297] 442 U.S. 735, 742 (1979).

[298] ประพิณ ประดิษฐากร, "กฎหมายว่าด้วยการเข้าถึงและได้มาซึ่งข้อมูลของบุคคล และร่างพระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 131/2 "(2554).

[299] 460 U.S. 276 (1983).

[300] 468 U.S. 705 (1984).

ด้วยเหตุนี้ ผู้ช่วยศาสตราจารย์ ดร. นคร เสรีรักษ์ จึงตั้งข้อสังเกตเกี่ยวกับบทบัญญัติแก้ไขรัฐธรรมนูญครั้งที่ 4 ว่า หลักความคาดหมายในความเป็นส่วนตัวตามบทบัญญัติแก้ไขรัฐธรรมนูญครั้งที่ 4 อาจไม่เพียงพอที่จะคุ้มครองข้อมูลส่วนบุคคลได้อย่างเหมาะสม โดยเฉพาะอย่างยิ่ง เมื่อเผชิญกับเทคโนโลยีที่มีความซับซ้อน เนื่องจากเทคโนโลยีเหล่านี้อาจเป็นเรื่องที่พ้นจากความคาดหมายของคนในสังคม[301] ในทำนองเดียวกัน Andrew Guthrie Ferguson ก็มีความเห็นว่า การคุ้มครองภายใต้บทบัญญัติแก้ไขรัฐธรรมนูญครั้งที่ 4 นั้นอาจไม่เท่าทันต่อกระแสความเปลี่ยนแปลงทางเทคโนโลยี เมื่อมีชุดข้อมูลขนาดใหญ่ ที่เรียกว่าข้อมูลมหัต (Big data) เข้ามาเกี่ยวข้อง อาทิ หลักการเกี่ยวกับการค้นและการยึดโดยจำกัด (Stop and Frisk) ในคดี Terry v. Ohio ซึ่งศาลสูงของสหรัฐอเมริกาได้วางหลักไว้ว่าอาจกระทำได้ หากปรากฏข้อเท็จจริงเกี่ยวกับการกระทำผิดที่เฉพาะเจาะจงและชัดเจน อันนำมาสู่ความสงสัยที่สมเหตุสมผล (Reasonable Suspicion) ของเจ้าหน้าที่ตำรวจ[302] แต่ปัจจุบัน ข้อเท็จจริงที่นำมาสู่ความสงสัยที่สมเหตุสมผลเช่นว่านี้ไม่ได้มีเฉพาะข้อมูลขนาดเล็ก (Small data) เหมือนในอดีต เพราะหน่วยงานของรัฐล้วนมีฐานข้อมูลขนาดใหญ่ จึงสามารถเข้าถึงข้อมูลส่วนบุคคลได้ง่ายและรวดเร็ว จึงอาจเป็นช่องว่างให้เจ้าหน้าที่ตำรวจของสหรัฐอเมริกาใช้อำนาจอย่างกว้างขวาง จนส่งผลกระทบต่อสิทธิและเสรีภาพของประชาชนเกินสมควร[303]

อนึ่ง มีข้อสังเกตเพิ่มเติมว่าการสืบสวนและสอบสวนคดีอาญาในสหรัฐอเมริกาไม่ได้อยู่ภายใต้บทบัญญัติแก้ไขรัฐธรรมนูญครั้งที่ 4 ฉบับเดียว แต่ยังมีกฎหมายอื่น ๆ ที่มีการกำหนดกรอบการใช้อำนาจสืบสวนและสอบสวนไว้อีกด้วย อาทิ กฎหมายวิธีพิจารณาความอาญา (U.S. Code) ก็มีการบัญญัติวิธีการและขั้นตอนการขออนุญาตเข้าถึงและได้มาซึ่งข้อมูลการสื่อสารที่ชัดเจน พร้อมทั้งกำหนดรายละเอียดการเก็บรักษาข้อมูลที่ได้มา กำหนดกระบวนการที่เปิดโอกาสให้ผู้ได้รับผลกระทบมีสิทธิในการโต้แย้งไม่ให้ศาลรับฟังข้อมูลที่ได้มาโดยไม่ชอบเป็นพยานหลักฐาน ตลอดจนกำหนดโทษทางอาญาและวิธีการคำนวณค่าเสียหายทางแพ่งอย่างชัดเจน[304]

---

[301] นคร เสรีรักษ์, ความเป็นส่วนตัว: ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย, หน้า 69-70.

[302] 392 US 1 (1968).

[303] Andrew Guthrie Ferguson, "Big Data and Predictive Reasonable Suspicion," University of Pennsylvania Law Review 163, 2 (January 2015).

[304] ปิติ เอี่ยมจำรูญลาภ, "กฎหมายเกี่ยวกับการกำหนดให้รัฐเข้าถึง หรือได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกัน : กรณีศึกษาประเทศสหรัฐอเมริกา."

4.2.2.2 กฎหมายคุ้มครองข้อมูลส่วนบุคคล (The Privacy Act of 1974)

The Privacy Act of 1974 ของสหรัฐอเมริกานั้นเป็นผลพวงมาจากคดีวอเตอร์เกต (Watergate) ซึ่งเกิดการโจรกรรมข้อมูลจากพรรคการเมืองฝ่ายตรงข้ามโดยมีเจ้าหน้าที่ฝ่ายรัฐบาลอยู่เบื้องหลัง สภาคองเกรสจึงได้ตรากฎหมายฉบับนี้ขึ้นเพื่อกำหนดหน้าที่ให้หน่วยงานในระดับสหพันธรัฐต้องจัดเก็บข้อมูลส่วนบุคคลจากเจ้าของข้อมูลโดยตรง และต้องมีมาตรการที่เหมาะสมเพื่อป้องกันมิให้มีการใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ และรับรองสิทธิต่าง ๆ ของเจ้าของข้อมูลส่วนบุคคล[305] สาระสำคัญของ The Privacy Act of 1974 จึงคล้ายคลึงกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลทั่วไป โดยมีรายละเอียดโดยสังเขป ดังนี้

The Privacy Act of 1974 มุ่งคุ้มครองบันทึกข้อมูล (Records) ซึ่งเป็นชุดหรือกลุ่มของข้อมูลเกี่ยวกับบุคคลที่อยู่ในความรับผิดชอบของหน่วยงานรัฐในระดับสหพันธรัฐ[306] และจะจำกัดขอบเขตการคุ้มครองเฉพาะบุคคลสัญชาติอเมริกันหรือบุคคลผู้มีภูมิลำเนาถาวรในสหรัฐอเมริกาเท่านั้น โดยมีการรับรองสิทธิของเจ้าของข้อมูลในการเข้าถึงและโต้แย้งความถูกต้องของข้อมูลตน[307]

อย่างไรก็ตาม สหรัฐอเมริกาจะไม่มีองค์กรอิสระที่เป็นองค์กรกลางทำหน้าที่ควบคุมกำกับดูแลการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลตามแนวทางสหภาพยุโรป แต่จะมีองค์กรที่มีอำนาจหน้าที่ตามกฎหมายเฉพาะเรื่องไปควบคุมกำกับดูแล ประกอบกับการใช้กลไกกำกับดูแลตนเอง (Self-regulation) ซึ่งเป็นการควบคุมตรวจสอบกันเองภายใน ไม่ว่าจะด้วยการกำหนดระเบียบปฏิบัติหรือการกำกับดูแลตามสายบังคับบัญชาเป็นสำคัญ[308]

The Privacy Act of 1974 กำหนดให้การเปิดเผยบันทึกข้อมูลต้องได้รับคำร้องขอหรือได้รับความยินยอมเป็นลายลักษณ์อักษรล่วงหน้าจากเจ้าของข้อมูล[309] และกำหนดให้หน่วยงานในระดับสหพันธรัฐจะต้องจัดเก็บบันทึกข้อมูลในลักษณะต่อไปนี้[310]

---

[305] ประสิทธิ์ ปิวาวัฒนพานิช, "กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกาและประเทศออสเตรเลีย," วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ ; ปิติ เอี่ยมจำรูญลาภ, "กฎหมายเกี่ยวกับการกำหนดให้รัฐเข้าถึง หรือได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกัน : กรณีศึกษาประเทศสหรัฐอเมริกา."

[306] § 552a. (a)(4).

[307] ประสิทธิ์ ปิวาวัฒนพานิช, "กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกาและประเทศออสเตรเลีย," วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์

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

[309] § 552a. (b).

[310] § 552a. (e).

- เก็บรักษาเฉพาะข้อมูลที่เกี่ยวข้องและจำเป็นเพื่อให้บรรลุวัตถุประสงค์
- พยายามเก็บรวบรวมข้อมูลจากเจ้าของข้อมูลโดยตรง โดยเฉพาะกรณีที่อาจมีผลกระทบต่อเจ้าของข้อมูล
- แจ้งให้เจ้าของข้อมูลแต่ละคนทราบถึงรายละเอียดการใช้บันทึกข้อมูล
- เผยแพร่รายละเอียดของระบบบันทึกข้อมูลซึ่งอยู่ในความรับผิดชอบลงใน Federal Register
- เก็บรักษาบันทึกข้อมูลให้มีความถูกต้อง เป็นปัจจุบัน ครบถ้วนสมบูรณ์ และมีความเกี่ยวข้องกับวัตถุประสงค์ของหน่วยงาน
- ก่อนมีการเปิดเผยบันทึกข้อมูล ให้ตรวจสอบตามสมควรว่าบันทึกข้อมูลถูกต้อง เป็นปัจจุบัน ครบถ้วนสมบูรณ์ และเกี่ยวข้อง
- ไม่เก็บรักษาบันทึกที่ระบุข้อมูลการใช้สิทธิและเสรีภาพในการแสดงออกตามบทบัญญัติแก้ไขรัฐธรรมนูญครั้งที่ 1 (First Amendment)
- หากบันทึกข้อมูลของบุคคลถูกเปิดเผยต่อบุคคลอื่นภายใต้กระบวนการบังคับกฎหมาย ให้ใช้ความพยายามตามสมควรในการแจ้งให้บุคคลนั้นทราบ เมื่อกระบวนการดังกล่าวกลายเป็นบันทึกข้อมูลสาธารณะ
- กำหนดระเบียบปฏิบัติสำหรับบุคคลที่เกี่ยวข้องกับการออกแบบ พัฒนา ดำเนินการ หรือบำรุงรักษาระบบบันทึกข้อมูล พร้อมฝึกอบรมบุคลากร อีกทั้ง ต้องกำหนดบทลงโทษเมื่อมีการฝ่าฝืนระเบียบปฏิบัติ
- จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งในด้านของการบริหาร มาตรการเชิงเทคนิคและทางกายภาพ
- หากมีการใช้บันทึกข้อมูลด้วยวัตถุประสงค์ใหม่ ซึ่งมิใช่การใช้ตามปกติ ให้เปิดโอกาสผู้มีส่วนได้เสียได้โต้แย้ง เป็นอย่างน้อย 30 วัน ก่อนที่จะเผยแพร่รายละเอียดของระบบบันทึกข้อมูลใน Federal Register

ยิ่งไปกว่านั้น ในกรณีที่บันทึกข้อมูลเป็นบันทึกข้อมูลที่เก็บรักษาไว้โดยหน่วยงานที่มีอำนาจหน้าที่ในการบังคับการให้เป็นไปตามกฎหมายอาญา ตั้งแต่กระบวนการในชั้นตำรวจ อัยการ ศาล ไปจนถึงราชทัณฑ์ หัวหน้าของหน่วยงานดังกล่าวอาจประกาศกฎระเบียบ เพื่อยกเว้นการเข้าถึงบันทึกข้อมูลได้ (General exemption) หากบันทึกข้อมูลนั้นประกอบด้วย[311]

---

[311] § 552a. (j)(2).; สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์, "รายงานผลการดำเนินการ โครงการพัฒนามาตรการในการดำเนินการ การพิจารณาความเหมาะสม ความเป็นไปได้ เพื่อจัดทำแนวทาง ขั้นตอนและวิธีการในการเข้าร่วมหรือทำความตกลงตามกรอบว่าด้วยการคุ้มครองข้อมูลความเป็นส่วนตัวของ Apec,"(คณะกรรมการข้อมูลข่าวสารของราชการ, ธันวาคม 2557).

- ข้อมูลข่าวสารที่รวบรวมไว้เพื่อวัตถุประสงค์ในการแจ้งว่าบุคคลใดเป็นผู้ถูกกล่าวหา (Alleged offenders) หรือเป็นผู้กระทำความผิดอาญา (Criminal offenders) โดยจะต้องประกอบด้วยข้อมูลแสดงสถานภาพการจับกุม ลักษณะและการดำเนินการต่อข้อกล่าวหาทางอาญา ไม่ว่าจะเป็นการพิจารณาคดี การพิพากษาลงโทษ การพ้นโทษ การทำทัณฑ์บน หรือการคุมประพฤติ
- ข้อมูลข่าวสารที่รวบรวมไว้เพื่อวัตถุประสงค์ในการสืบสวนและสอบสวนคดีอาญา โดยให้รวมถึงบันทึกรายงานของผู้ให้ข้อมูลหรือสายสืบ ที่อาจทำให้ระบุถึงตัวบุคคลได้
- บันทึกรายงานที่สามารถระบุถึงตัวบุคคลผู้เกี่ยวข้องกับการดำเนินงานในกระบวนการยุติธรรมทางอาญา

นอกเหนือจากบันทึกข้อมูลที่รวบรวมไว้เพื่อวัตถุประสงค์ข้างต้น ข้อมูลข่าวสารที่เป็นข้อมูลการสืบสวนและสอบสวนคดีอาญา (Investigatory Material) ซึ่งรวบรวมไว้เพื่อวัตถุประสงค์อื่นในการบังคับใช้กฎหมายอาญา หัวหน้าของหน่วยงานระดับสหพันธรัฐก็อาจกำหนดหลักเกณฑ์สำหรับการเข้าถึงระบบบันทึกข้อมูลข่าวสารนั้นได้อีกด้วย (Specific exemption)[312]

แม้ว่า The Privacy Act of 1974 จะกำหนดข้อยกเว้นการเปิดเผยบันทึกข้อมูลการสืบสวนและสอบสวนคดีอาญาต่อบุคคลที่สามเพิ่มเติมจากกรณีทั่วไป โดยให้อำนาจหัวหน้าหน่วยงานออกกฎระเบียบเพิ่มเติม แต่หากพิจารณาในด้านการบังคับใช้กฎหมาย (Law enforcement activity) กลับพบว่า The Privacy Act of 1974 มีข้อยกเว้นอยู่จำนวนหนึ่ง ซึ่งให้อำนาจหน่วยงานของรัฐเก็บรวบรวมและเปิดเผยบันทึกข้อมูลได้มากกว่ากรณีปกติ โดยเฉพาะในชั้นสืบสวนและสอบสวนคดีอาญา อาทิ ยกเว้นให้สามารถเก็บรักษาบันทึกข้อมูลการใช้สิทธิและเสรีภาพในการแสดงออกตามบทบัญญัติแก้ไขรัฐธรรมนูญครั้งที่ 1 (First Amendment) ตามที่กฎหมายกำหนด[313] และยกเว้นให้หน่วยงานอื่นอาจเปิดเผยข้อมูลต่อหน่วยงานบังคับใช้กฎหมายอาญาได้ แม้ไม่ได้รับความยินยอมจากเจ้าของข้อมูล หากการเปิดเผยนั้นเป็นไปตามที่กฎหมายบัญญัติ และมีคำร้องขอเป็นลายลักษณ์อักษรจากหน่วยงานบังคับใช้กฎหมาย โดยจะต้องระบุบันทึกข้อมูลเฉพาะส่วนที่ต้องการ[314] เป็นต้น

---

[312] § 552a. (k)(2).; อ้างแล้ว.

[313] § 552a. (e)(7).

[314] § 552a. (b)(7).

ทั้งนี้ Erin Murphy ตั้งข้อสังเกตเกี่ยวกับประเด็นดังกล่าวเอาไว้ว่า การดำเนินงานในกระบวนการยุติธรรมอาญา ซึ่งครอบคลุมถึงการสืบสวนและสอบสวนคดีอาญา มักปรากฏอยู่ในฐานะข้อยกเว้นตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลเกือบทุกฉบับ เนื่องจากกระแสหลักของการคุ้มครองข้อมูลส่วนบุคคลในสหรัฐอเมริกาเป็นเรื่องของการคุ้มครองข้อมูลผู้บริโภค[315]

อย่างไรก็ดี การที่สหรัฐอเมริกามีแนวทางการคุ้มครองข้อมูลส่วนบุคคลแตกต่างจากสหภาพยุโรป คือไม่มีกฎหมายกลางคุ้มครองข้อมูลส่วนบุคคล ทำให้สหรัฐอเมริกาไม่ได้รับการวินิจฉัยถึงระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ จนเป็นอุปสรรคต่อการโอนข้อมูลระหว่างสหรัฐอเมริกาและสหภาพยุโรป โดยเฉพาะในการดำเนินกิจกรรมทางธุรกิจต่าง ๆ แต่เพื่อบรรเทาผลกระทบดังกล่าว สหรัฐอเมริกาและสหภาพยุโรปจึงได้มีการทำข้อตกลงระหว่างประเทศในระดับทวิภาคีเป็นกรอบปฏิบัติในการโอนข้อมูลขึ้น ซึ่งเดิมคือความตกลงตามโครงการ Safe Harbor มีผลใช้บังคับเมื่อปี ค.ศ. 2000 โดยให้ถือว่าองค์กรที่ปฏิบัติตาม Safe Harbor มีระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ[316]

ทว่าในปี ค.ศ. 2015 ศาลยุติธรรมแห่งยุโรปกลับตัดสินให้ความตกลง Safe Harbor สิ้นผลไปในคดี Case C-362/14 ซึ่งรองศาสตราจารย์คณาธิป ทองรวีวงศ์ ได้วิเคราะห์ว่าปัจจัยสำคัญที่ทำให้ศาลวินิจฉัยให้ความตกลงตามโครงการ Safe Harbor ไม่ชอบด้วยกฎหมายนั้น มิได้เกี่ยวข้องกับหลักการคุ้มครองข้อมูลส่วนบุคคลใน Safe Harbor โดยตรง แต่อยู่ที่สภาพแวดล้อมทางกฎหมายของสหรัฐอเมริกา ที่มีกฎหมายให้อำนาจหน่วยงานรัฐสอดแนมข้อมูลเป็นการทั่วไป (Generalized basis) ประกอบกับหลักการในความตกลง Safe Harbor ก็อาจถูกจำกัดได้ด้วยเหตุผลด้านความมั่นคงของรัฐ ประโยชน์สาธารณะ การบังคับใช้กฎหมาย โดยที่ไม่มีมาตรการทางกฎหมายใดที่เปิดโอกาสให้เจ้าของข้อมูลได้รับการเยียวยาความเสียหายหรือใช้สิทธิเพื่อเข้าถึง แก้ไข และลบข้อมูลเกี่ยวกับตน อันเป็นการลดทอนสาระสำคัญแห่งสิทธิและเสรีภาพในชีวิตส่วนตัวตามที่ ECHR รับรองไว้[317] โดยเฉพาะอย่างยิ่งเมื่อการคุ้มครองสิทธิความเป็นส่วนตัวตามบทบัญญัติแก้ไขรัฐธรรมนูญครั้งที่ 4 ยังมีข้อจำกัด ในกรณีความคาดหมายในความเป็นส่วนตัวของข้อมูลที่ให้แก่บุคคลที่สามไปด้วยความสมัครใจ และกรณีที่มีอาจใช้เทคโนโลยีสมัยใหม่ที่อยู่นอกเหนือความคาดหมายของบุคคล[318]

---

[315] Erin Murphy, "The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions," Michigan Law Review 111, 4 (2013).

[316] คณาธิป ทองรวีวงศ์, "การปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน."; นคร เสรีรักษ์, ความเป็นส่วนตัว: ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย, หน้า 165-167.

[317] คณาธิป ทองรวีวงศ์, "การปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน."

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

ภายหลังจากที่ความตกลง Safe Harbor สิ้นผล การโอนข้อมูลระหว่างสหรัฐอเมริกาและสหภาพยุโรปจึงเกิดความไม่แน่นอนอยู่ช่วงหนึ่ง ต่อมา สหรัฐอเมริกาและสหภาพยุโรปจึงได้มีการทำความตกลงภายใต้โครงการใหม่ที่เรียกว่า Privacy Shield เมื่อปี ค.ศ. 2016 แต่ถึงกระนั้น ก็ปรากฏข้อโต้แย้งว่าความตกลง Privacy Shield ยังมีความไม่ชัดเจนในประเด็นการคุ้มครองข้อมูลส่วนบุคคลจากการสอดแนมโดยรัฐบาลของสหรัฐอเมริกา ในปีเดียวกันนี้ สหรัฐอเมริกาและสหภาพยุโรปจึงได้ทำความตกลง Umbrella Agreement เพิ่มเติมอีกฉบับหนึ่ง เพื่อคุ้มครองข้อมูลส่วนบุคคลซึ่งโอนในการบังคับใช้กฎหมายระหว่างสหรัฐอเมริกาและสหภาพยุโรปตามความตกลงร่วมมือระหว่างประเทศที่มีอยู่ โดยความตกลงดังกล่าวได้รับรองให้พลเมืองยุโรปมีสิทธิได้รับการพิจารณาทางศาล (Judicial review) ในกรณีที่หน่วยงานบังคับใช้กฎหมายของสหรัฐอเมริกามีการเปิดเผยข้อมูลส่วนบุคคล หรือปฏิเสธสิทธิในการเข้าถึงหรือแก้ไขข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานนั้น อีกนัยหนึ่ง คือเป็นการขยายขอบเขตการคุ้มครองตาม The Privacy Act of 1974 ที่เดิมจะจำกัดขอบเขตการคุ้มครองเฉพาะพลเมืองของสหรัฐอเมริกาเท่านั้น[319]

จะเห็นได้ว่าความขัดแย้งในเรื่องของการโอนข้อมูลส่วนบุคคลระหว่างสหรัฐอเมริกาและสหภาพยุโรปมีปัจจัยแวดล้อมทางกฎหมายหลายประการเข้ามาเกี่ยวข้อง ได้แก่

- กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหรัฐอเมริกาเป็นกฎหมายที่ให้ความคุ้มครองเฉพาะภาคส่วน โดยที่ไม่มีกฎหมายกลางคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป
- กฎหมายที่ให้อำนาจหน่วยงานรัฐเข้าถึงหรือสอดแนมข้อมูลส่วนบุคคลในสหรัฐอเมริกาไม่สอดคล้องกับหลักสิทธิมนุษยชนที่ ECHR รับรอง
- สิทธิในข้อมูลส่วนบุคคลของพลเมืองยุโรปมีหลักประกันที่ไม่เทียบเท่ากับพลเมืองสหรัฐอเมริกา

ฉะนั้น การวินิจฉัยถึงระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอของสหภาพยุโรปจึงไม่ได้พิจารณาเฉพาะการมีอยู่ของกฎหมายคุ้มครองข้อมูลส่วนบุคคล แต่จะประเมินสภาพแวดล้อมทางกฎหมายอื่นประกอบอีกด้วย

---

[319] คณาธิป ทองรวีวงศ์, "การปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน."

4.2.3 สาธารณรัฐเกาหลี (เกาหลีใต้)

สาธารณรัฐเกาหลีเป็นหนึ่งในประเทศที่ได้รับการวินิจฉัยถึงระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอตามมาตรฐาน GDPR โดยในระบบกฎหมายสาธารณรัฐเกาหลี การคุ้มครองข้อมูลส่วนบุคคลจะมีพื้นฐานมาจากบทบัญญัติรัฐธรรมนูญ ในฐานะที่เป็นส่วนหนึ่งของสิทธิส่วนบุคคล (Private life)[320] และความเป็นส่วนตัวในการติดต่อสื่อสาร (Privacy of communications)[321] ซึ่งได้รับการรับรองและคุ้มครองอย่างชัดเจนว่าเป็นสิทธิและเสรีภาพขั้นพื้นฐาน การจำกัดสิทธิดังกล่าวจึงกระทำได้เฉพาะเมื่อมีบทบัญญัติกฎหมายให้อำนาจ ในกรณีที่มีความจำเป็นเพื่อความมั่นคงของชาติ เพื่อธำรงไว้ซึ่งกฎหมาย เพื่อรักษาความสงบเรียบร้อยในสังคม หรือเพื่อสวัสดิภาพแห่งรัฐเท่านั้น แต่ไม่ว่าในกรณีใด การจำกัดสิทธิดังกล่าวจะต้องไม่เป็นการละเมิดสารัตถะสำคัญแห่งสิทธิและเสรีภาพนั้น[322]

นอกเหนือจากการรับรองสิทธิส่วนบุคคล รัฐธรรมนูญของสาธารณรัฐเกาหลียังบัญญัติรับรองอีกว่าการจับกุม กักขัง สอบปากคำ ค้น หรือยึดทรัพย์สินใด ๆ ของบุคคลจะกระทำไม่ได้ เว้นแต่เป็นไปตามที่กฎหมายบัญญัติ[323] อีกทั้ง การค้นและยึดจะกระทำได้ต่อเมื่อได้รับหมายจากศาลเท่านั้น ยกเว้นในสถานการณ์พิเศษ เจ้าพนักงานสืบสวนสอบสวนจะทำการค้นหรือยึดไปก่อนได้ แต่ต้องขอหมายศาลภายหลังจากที่การค้นและยึดสิ้นสุด[324] ยิ่งไปกว่านั้น มีข้อสังเกตว่าการคุ้มครองสิทธิในข้อมูลส่วนบุคคลภายใต้บทบัญญัติรัฐธรรมนูญข้างต้นมิได้จำกัดเฉพาะพลเมืองของสาธารณรัฐเกาหลี แต่ยังครอบคลุมถึงบุคคลสัญชาติอื่นอีกด้วย เนื่องจากศาลรัฐธรรมนูญแห่งสาธารณรัฐเกาหลีได้มีคำวินิจฉัยว่าสิทธิในการควบคุมข้อมูลเกี่ยวกับตนนั้นเป็นสิทธิขั้นพื้นฐานของมนุษย์ทุกคน[325]

ดังนั้น ในระบบกฎหมายของสาธารณรัฐเกาหลี สิทธิความเป็นส่วนตัวในข้อมูลของบุคคลจึงมีหลักประกันขั้นพื้นฐานตามบทบัญญัติรัฐธรรมนูญเป็นลำดับแรก และหลักการทั่วไปในรัฐธรรมนูญนี้ก็ได้กลายเป็นรากฐานของบทบัญญัติกฎหมายต่าง ๆ เพื่อคุ้มครองข้อมูลส่วนบุคคลจากการดำเนินงานในชั้นสืบสวนและสอบสวนคดีอาญา โดยมีรายละเอียดดังต่อไปนี้

---

[320] Constitution of the Republic of Korea, Article 17.

[321] Constitution of the Republic of Korea, Article 18.

[322] Constitution of the Republic of Korea, Article 37 (2).

[323] Constitution of the Republic of Korea, Article 12 (1).

[324] Constitution of the Republic of Korea, Article 12 (3).

[325] Constitutional Court Decision 93 Hun-MA120, 29 December 1994.; Constitutional Court Decision 99HeonMa494, 29 November 2001.

4.2.3.1 กฎหมายวิธีพิจารณาความอาญา

ภายใต้หลักการของรัฐธรรมนูญสาธารณรัฐเกาหลี การค้นและยึดจะมีหมายของศาลเป็นฐานการใช้อำนาจเป็นหลัก ส่วนการค้นและยึดโดยไม่มีหมายจะกระทำได้อย่างจำกัดเฉพาะในบางสถานการณ์ อาทิ กรณีจับกุมผู้ต้องสงสัยขณะกระทำผิด (Flagrante delicto) หรือกรณีที่ผู้ต้องสงสัยกระทำความผิดอาญาที่มีอัตราโทษจำคุกสามปีขึ้นไป มีความเสี่ยงจะหลบหนีหรือทำลายพยานหลักฐาน อย่างไรก็ตาม เจ้าพนักงานสืบสวนสอบสวนจะต้องมีการขอหมายจากศาล (Ex post facto warrant) ย้อนหลังในทุกกรณี เพื่อเปิดโอกาสให้ศาลตรวจสอบความชอบด้วยกฎหมายของการค้นหรือยึดนั้น[326] ซึ่งในระบบกฎหมายสาธารณรัฐเกาหลี อาจแบ่งได้เป็นสามรูปแบบด้วยกัน อันได้แก่

รูปแบบที่หนึ่ง การค้นและยึดทั่วไปภายใต้ The Criminal Procedure Act (“CPA”)

โดยหลัก การค้นหรือยึดจะกระทำได้ต่อเมื่อได้รับหมายจากศาล โดยเจ้าหน้าที่ตำรวจหรือพนักงานอัยการผู้ร้องขอจะต้องยื่นเอกสารแสดงเหตุที่สงสัยว่ามีบุคคลกระทำความผิดอาญา และมีความจำเป็นที่จะต้องดำเนินการสืบสวนและสอบสวน อีกทั้ง บุคคลหรือสิ่งของที่ต้องการค้นหรือยึดต้องมีความเกี่ยวข้องกับอาชญากรรมดังกล่าว[327] ในทางกลับกัน การค้นหรือยึดโดยไม่มีหมายของศาลจะกระทำเฉพาะในกรณีที่กฎหมายระบุดังต่อไปนี้

1.) สิ่งของที่ต้องการค้นหรือยึดนั้นเป็นสิ่งของถูกทิ้ง หรือเป็นกรณีที่เจ้าของหรือผู้ครอบครองสิ่งของอนุญาตด้วยความสมัครใจ[328]
2.) การค้นหรือยึดกระทำในขณะที่จับกุมหรือควบคุมตัวผู้ต้องสงสัย[329]
3.) กรณีที่มีความจำเป็นเร่งด่วนที่ไม่อาจขอให้ศาลออกหมายได้ อย่างไรก็ตามจะต้องมีการขอหมายในภายหลัง โดยไม่ชักช้า[330]

ในกรณีที่สิ่งของที่ต้องการค้นหรือยึดเป็นสื่อบันทึกข้อมูล (Data storage medium) ให้จำกัดการค้นหรือยึดเฉพาะข้อมูลที่เกี่ยวข้อง เว้นแต่เป็นไปไม่ได้อย่างมากที่จะคัดแยกข้อมูลดังกล่าว หรือการคัดแยกนั้นจะทำให้วัตถุประสงค์ในการค้นหรือยึดไม่บรรลุผล[331] และภายหลังจากที่ศาลได้รับ

---

[326] Constitution of the Republic of Korea, Article 12 (3).

[327] CPA, Article 215.; 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."

[328] CPA, Article 218.

[329] CPA, Article 216 (1)-(2).

[330] CPA, Article 216 (3).

[331] CPA, Article 106 (3).

ข้อมูลข่าวสารที่ได้มาจากการค้นหรือยึดสื่อบันทึกข้อมูลข้างต้น ศาลจะมีหน้าที่ในการแจ้งข้อเท็จจริงที่เกี่ยวข้องไปยังเจ้าของข้อมูลโดยไม่ชักช้า[332]

รูปแบบที่สอง การเก็บรวบรวมข้อมูลการติดต่อสื่อสารภายใต้ The Communication Privacy Protection Act (“CPPA”) ซึ่งแบ่งประเภทข้อมูลการติดต่อสื่อสารเป็นสองประเภท ได้แก่

1.) ข้อมูลที่ยืนยันการติดต่อสื่อสาร (Communication confirmation data) หมายถึง ข้อมูลทั่วไปที่สามารถใช้ยืนยันถึงการติดต่อสื่อสารของบุคคล เช่น วันและระยะเวลาที่มีการติดต่อสื่อสาร หรือหมายเลขโทรศัพท์ที่ใช้
2.) เนื้อความของการติดต่อสื่อสาร (Communication restricting measure) หมายถึง ข้อมูลที่เป็นเนื้อหาสาระ (Content) ของการติดต่อสื่อสาร

ภายใต้ CPPA การเก็บรวบรวมข้อมูลการติดต่อสื่อสารทั้งสองประเภทจะต้องได้รับคำสั่งอนุญาตจากศาลก่อนการดำเนินการ เว้นแต่ในกรณีฉุกเฉิน ให้การขออนุญาตกระทำภายหลังได้ แต่หากศาลมีคำสั่งไม่อนุญาตในภายหลัง ข้อมูลที่ได้มาจะต้องถูกทำลายทั้งหมด[333]

แม้การเก็บรวบรวมข้อมูลการติดต่อสื่อสารทั้งสองประเภทจะกระทำได้ต่อเมื่อได้รับหมายจากศาลเช่นเดียวกัน แต่ CPPA จะกำหนดเงื่อนไขและหลักเกณฑ์ในการเข้าถึงเนื้อความของการติดต่อสื่อสารอย่างเคร่งครัดมากกว่า กล่าวคือการใช้มาตรการเข้าถึงเนื้อความการติดต่อสื่อสารจะต้องเป็นวิถีทางสุดท้าย อีกนัยหนึ่ง คือไม่ปรากฏว่ามีมาตรการอื่นใดที่เหมาะสมกว่า และการใช้มาตรการนี้จะจำกัดเฉพาะความผิดร้ายแรงตามที่ระบุในบัญชีของ CPPA และห้ามดำเนินการอย่างต่อเนื่องเกินกว่าที่จำเป็น โดยมีระยะเวลาขั้นสูงคือไม่เกินกว่าสองเดือน เว้นแต่มีเหตุในการขยายตามที่กฎหมายกำหนด แต่ระยะเวลาทั้งหมดจะต้องไม่เกินกว่า 1 ปี หรือ 3 ปี สำหรับอาชญากรรมร้ายแรง[334]

นอกจากนี้ CPPA ได้กำหนดให้หน่วยงานของรัฐมีหน้าที่แจ้งข้อเท็จจริงเกี่ยวกับการเก็บรวบรวมข้อมูลการติดต่อสื่อสารให้เจ้าของข้อมูลทราบเช่นเดียวกัน โดยพนักงานอัยการจะมีหน้าที่แจ้งข้อเท็จจริงภายใน 30 วัน นับแต่มีคำสั่งฟ้องหรือจับกุม เว้นแต่การแจ้งมีผลกระทบต่อความมั่นคง ความสงบเรียบร้อยของสังคม หรือเป็นอันตรายแก่บุคคลอื่น โดยได้รับอนุญาตจากหัวหน้าสำนักงานอัยการเขตให้เลื่อนการแจ้งเตือน[335]

---

[332] CPA, Article 106 (4).

[333] CPPA, Article 13.

[334] CPPA, Article 6 (8).

[335] CPPA, Article 9-2 (1).

รูปแบบที่สาม การเก็บรวบรวมข้อมูลผู้ใช้บริการจากผู้ให้บริการธุรกิจโทรคมนาคมบนพื้นฐานของความสมัครใจภายใต้ The Telecommunications Business Act (“TBA”)

ผู้ให้บริการธุรกิจโทรคมนาคม (Telecommunication provider) อาจให้ข้อมูลของผู้ใช้บริการได้ หากมีคำร้องขอเป็นลายลักษณ์อักษรจากเจ้าหน้าที่ของรัฐ โดยคำร้องขอจะต้องระบุเหตุทางกฎหมาย ขอบเขตของข้อมูลที่ต้องการ รวมถึงความเกี่ยวข้องข้อมูลดังกล่าวกับการกระทำความผิดที่ได้ดำเนินการสืบสวนและสอบสวน[336] และแม้เป็นกรณีฉุกเฉิน เจ้าหน้าที่รัฐก็จำต้องทำคำร้องดังกล่าวย้อนหลังทันทีที่เหตุฉุกเฉินสิ้นสุดลง โดยข้อมูลที่อาจเก็บรวบรวมได้จะจำกัดเฉพาะข้อมูลบางประเภทเท่านั้น เช่น ชื่อ ที่อยู่ วันที่สมัครหรือยุติการใช้บริการ หมายเลขอุปกรณ์โทรศัพท์ เป็นต้น[337]

มีข้อสังเกตว่าการให้ข้อมูลข้างต้นจะต้องอยู่บนพื้นฐานความสมัครใจของผู้ให้บริการธุรกิจโทรคมนาคม กล่าวคือผู้ให้บริการอาจปฏิเสธที่จะให้ข้อมูลหรือไม่ก็ได้ อีกทั้ง การให้ข้อมูลนั้นต้องสอดคล้องกับหลักการคุ้มครองข้อมูลส่วนบุคคลตาม South Korea’s PIPA คือต้องประเมินผลกระทบโดยห้ามทำการเปิดเผย หากการเปิดเผยจะกระทบผลประโยชน์ของเจ้าของข้อมูลหรือบุคคลที่สามโดยไม่เป็นธรรม แต่ในกรณีที่มีการเปิดเผยข้อมูล เจ้าของข้อมูลจะต้องได้รับแจ้งข้อเท็จจริงถึงการเปิดเผยดังกล่าว เว้นแต่การแจ้งจะเป็นอุปสรรคต่อการสืบสวนและสอบสวนคดีอาญาที่ดำเนินการอยู่ หรือจะก่อให้เกิดอันตรายต่อชีวิต ร่างกาย หรือผลประโยชน์ของบุคคลอื่นที่มีความสำคัญกว่าสิทธิส่วนบุคคลของเจ้าของข้อมูล ให้การแจ้งข้อเท็จจริงเกี่ยวกับการเปิดเผยกระทำในภายหลังได้[338]

4.2.3.2 กฎหมายคุ้มครองข้อมูลส่วนบุคคล (South Korea’s PIPA)

South Korea’s PIPA เป็นกฎหมายกลางว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐเกาหลี South Korea’s PIPA จึงมีขอบเขตการใช้บังคับโดยกว้าง ครอบคลุมทั้งหน่วยงานภาครัฐและเอกชน โดย South Korea’s PIPA นิยามคำว่าข้อมูลส่วนบุคคล (Personal information) ให้หมายความถึง ข้อมูลใด ๆ เกี่ยวกับบุคคลธรรมดาที่มีชีวิตอยู่ ดังต่อไปนี้[339]

---

[336] TBA, Article 83 (3).

[337] 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."

[338] Ibid.

[339] South Korea’s PIPA, Article 2.

- ข้อมูลที่ระบุถึงตัวบุคคลโดยตรง เช่น ชื่อ หมายเลขประจำตัว ภาพถ่าย
- ข้อมูลที่ไม่ได้ระบุถึงตัวบุคคลโดยตรง แต่สามารถนำไปประกอบกับข้อมูลอื่นใดเพื่อระบุตัวบุคคลได้โดยง่าย
- ข้อมูลแฝง (Pseudonymized information) กล่าวคือข้อมูลส่วนบุคคลที่ผ่านกระบวนการแฝง จนไม่อาจใช้เพื่อระบุถึงตัวบุคคลได้โดยตรง หากไม่มีการรวมข้อมูลหรือทำให้กลับสู่สภาพเดิม

การกำหนดขอบเขตข้อมูลส่วนบุคคลที่ได้รับการคุ้มครองตาม South Korea's PIPA จึงเป็นไปในทิศทางเดียวกับสหภาพยุโรป แต่สำหรับหลักการทั่วไปในการประมวลผลข้อมูลส่วนบุคคล South Korea's PIPA ได้วางหลักการไว้แปดประการสำคัญด้วยกัน อันได้แก่[340]

1.) การประมวลผลข้อมูลส่วนบุคคลจะต้องระบุวัตถุประสงค์อย่างชัดแจ้ง และการเก็บรวบรวมข้อมูลส่วนบุคคลนั้นต้องเป็นไปโดยชอบด้วยกฎหมายและเป็นธรรม ในขอบเขตขั้นต่ำเท่าที่จำเป็นเพื่อบรรลุวัตถุประสงค์ดังกล่าว
2.) การประมวลผลข้อมูลส่วนบุคคลต้องเป็นไปโดยเหมาะสมเท่าที่จำเป็นเพื่อบรรลุวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล และจะต้องไม่ใช้ข้อมูลส่วนบุคคลเกินกว่าขอบเขตตามวัตถุประสงค์นั้น
3.) ข้อมูลส่วนบุคคลจะต้องได้รับการตรวจสอบให้มีความถูกต้อง สมบูรณ์ และเป็นปัจจุบันเท่าที่จำเป็นและเกี่ยวข้องกับวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล
4.) ข้อมูลส่วนบุคคลต้องได้รับการรักษาความมั่นคงปลอดภัยตามแต่ประเภทหรือวิธีการในการประมวลผลข้อมูลส่วนบุคคล โดยให้คำนึงถึงความเสี่ยงรวมถึงความรุนแรงของการละเมิดข้อมูลส่วนบุคคลในการออกแบบระบบรักษาความมั่นคงปลอดภัยนั้นด้วย
5.) การประมวลผลข้อมูลส่วนบุคคลจะต้องเปิดเผยนโยบายความเป็นส่วนตัว (Privacy Policy) หรือเอกสารอื่นใดที่เกี่ยวข้องต่อสาธารณะ และจะต้องมีการประกันสิทธิของเจ้าของข้อมูลส่วนบุคคล
6.) การประมวลผลข้อมูลส่วนบุคคลจะต้องเป็นไปในลักษณะที่ก่อให้เกิดความเสี่ยงต่อการละเมิดความเป็นส่วนตัวให้น้อยที่สุด

[340] South Korea's PIPA, Article 3 Principles for Protecting Personal Information.

7.) หากวัตถุประสงค์ในการรวบรวมข้อมูลส่วนบุคคลสามารถบรรลุผลได้ด้วยข้อมูลนิรนาม[341] หรือข้อมูลแฝง[342] ให้การประมวลผลข้อมูลส่วนบุคคลนั้นประมวลผลโดยทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลนิรนาม หรือเป็นข้อมูลแฝงในกรณีที่ไม่อาจบรรลุวัตถุประสงค์โดยการประมวลผลข้อมูลนิรนามได้

8.) ผู้ควบคุมข้อมูลส่วนบุคคลย่อมมีความรับผิดชอบในการปฏิบัติตามกฎเกณฑ์ในบทบัญญัตินี้ รวมถึงบทบัญญัติอื่นใดที่มีความเกี่ยวข้อง

นอกเหนือจากหลักการทั่วไป South Korea's PIPA ยังมีการบัญญัติหน้าที่ของรัฐในการคุ้มครองข้อมูลส่วนบุคคล (Obligations of State, etc.) ไว้อย่างเฉพาะเจาะจง[343] กล่าวคือ

1.) รัฐและส่วนราชการท้องถิ่นจะต้องกำหนดนโยบายเพื่อป้องกันมิให้เกิดการรวบรวมข้อมูลส่วนบุคคลเกินกว่าขอบวัตถุประสงค์ และป้องกันการละเมิดข้อมูลส่วนบุคคล การใช้ข้อมูลส่วนบุคคลโดยมิชอบ หรือการสอดแนมและเฝ้าติดตามบุคคลอย่างต่อเนื่อง (Indiscrete Surveillance and Tracking) อีกทั้ง ยังต้องกำหนดนโยบายที่ส่งเสริมศักดิ์ศรีความเป็นมนุษย์และสิทธิในความเป็นส่วนตัวของบุคคล

2.) รัฐและส่วนราชการท้องถิ่นจะต้องกำหนดมาตรการที่จำเป็น ในการประกันสิทธิของเจ้าของข้อมูล ที่ South Korea's PIPA ได้รับรองไว้ ไม่ว่าจะเป็นสิทธิที่จะได้รับการแจ้งเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล สิทธิที่จะให้ความยินยอมหรือไม่ให้ความยินยอม สิทธิที่จะเข้าถึงและรับสำเนาของข้อมูลส่วนบุคคล สิทธิที่จะขอให้ระงับการประมวลผล หรือขอให้แก้ไข ลบ หรือทำลายข้อมูลส่วนบุคคล ตลอดจนสิทธิที่จะได้รับการชดใช้เยียวยาเมื่อมีความเสียหายเกิดขึ้นจากการประมวลผลข้อมูลส่วนบุคคล[344]

---

[341] ข้อมูลนิรนาม (anonymized personal information) หมายถึง ข้อมูลที่ผ่านกระบวนการลดความเสี่ยงในการระบุถึงตัวของเจ้าของข้อมูลให้เหลือน้อยจนแทบไม่ต้องให้ความสำคัญกับความเสี่ยง (โปรดดู หัวข้อ G. แนวปฏิบัติเกี่ยวกับการจัดทำข้อมูลนิรนาม ใน ปิยะบุตร บุญอร่ามเรือง และคณะ, แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล, หน้า 265-304.)

[342] ข้อมูลแฝง (pseudonymised personal information) หมายถึง ข้อมูลที่ผ่านกระบวนการแทนสิ่งที่ระบุตัวเจ้าของข้อมูลโดยตรงข้อมูลนั้นจึงไม่อาจระบุถึงตัวเจ้าของข้อมูลได้หากปราศจากการใช้ข้อมูลเพิ่มเติมประกอบ โดยข้อมูลเพิ่มเติมนี้จะต้องมีการเก็บรักษาไว้แยกออกจากกัน (โปรดดู หัวข้อ G. แนวปฏิบัติเกี่ยวกับการจัดทำข้อมูลนิรนาม ในปิยะบุตร บุญอร่ามเรือง และคณะ, แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล, หน้า 265-304.)

[343] South Korea's PIPA, Article 5 Obligations of State, etc.

[344] South Korea's PIPA, Article 4 Rights of Data Subjects.

3.) รัฐและส่วนราชการท้องถิ่นจะต้องเคารพ ส่งเสริม และสนับสนุนกลไกการควบคุมกำกับดูแลตนเอง (Self-regulating) เพื่อคุ้มครองข้อมูลส่วนบุคคล

4.) รัฐและส่วนราชการท้องถิ่นจะต้องตราหรือแก้ไขบทบัญญัติกฎหมายใด ๆ ให้เป็นไปตามวัตถุประสงค์ของ South Korea's PIPA

ทั้งนี้ มีข้อสังเกตว่าหลักการทั่วไป หน้าที่ของรัฐ รวมถึงสิทธิของเจ้าของข้อมูลข้างต้นได้รับการบัญญัติอยู่ใน CHAPTER 1 General Provisions ซึ่งเป็นบททั่วไปของ South Korea's PIPA กฎเกณฑ์เหล่านี้จึงเป็นพื้นฐานการคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐเกาหลี และมีผลใช้บังคับครอบคลุมกิจกรรมหรือการดำเนินการทุกประเภท

อย่างไรก็ตาม แม้ว่า CHAPTER 1 General Provisions ของ South Korea's PIPA จะมีผลใช้บังคับอย่างครอบคลุม แต่ South Korea's PIPA ก็ได้กำหนดบทยกเว้นมิให้นำ CHAPTER 2 ถึง CHAPTER 7 ซึ่งเป็นรายละเอียดและข้อปฏิบัติต่าง ๆ ไปใช้บังคับแก่สี่กิจการต่อไปนี้[345]

- การประมวลผลข้อมูลส่วนบุคคลโดยหน่วยงานรัฐตาม the Statistics Act
- การประมวลข้อมูลส่วนบุคคล อันเกี่ยวข้องกับความมั่นคงของชาติ
- การประมวลผลข้อมูลส่วนบุคคลชั่วคราว ในกรณีที่มีความจำเป็นเร่งด่วนต่อความมั่นคงปลอดภัยของสาธารณะหรือสาธารณสุข
- การประมวลผลข้อมูลส่วนบุคคล เพื่อใช้ในการนำเสนอข่าวของสื่อมวลชน กิจกรรมองค์กรศาสนา และการเสนอชื่อของผู้สมัครโดยพรรคการเมือง

จะเห็นได้ว่าการสืบสวนและสอบสวนคดีอาญาไม่ใช่กิจการที่ได้รับการยกเว้นมิให้นำ CHAPTER 2 ถึง CHAPTER 7 มาใช้บังคับ การสืบสวนและสอบสวนคดีอาญาในสาธารณรัฐเกาหลีจึงยังคงอยู่ภายใต้บังคับ South Korea's PIPA ทั้งฉบับ เพียงแต่ South Korea's PIPA จะมีการกำหนดข้อยกเว้นบางประการให้แก่การสืบสวนและสอบสวนคดีอาญาเป็นรายบทบัญญัติไป เพื่อให้เกิดความเหมาะสมในการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลแก่การสืบสวนและสอบสวนคดีอาญา เช่น ได้รับยกเว้นให้สามารถใช้กล้องตรวจจับภาพ (Visual Data Processing Devices) ในพื้นที่สาธารณะหากเป็นไปเพื่อป้องกันและปราบปรามอาชญากรรม[346] อีกทั้ง ยังได้รับยกเว้นจากการจดทะเบียนและเปิดเผยแฟ้มข้อมูลส่วนบุคคล (Personal information files) ที่บันทึกข้อมูลการสืบสวนสอบสวน[347]

---

[345] The South Korea's PIPA, Article 58 (1).

[346] South Korea's PIPA, Article 25 (1).

[347] South Korea's PIPA, Article 32 (2).

และในกรณีที่มีการใช้ข้อมูลนอกเหนือจากวัตถุประสงค์ดั้งเดิม การสืบสวนและสอบสวนคดีอาญาก็จะได้รับการยกเว้นไม่ให้ต้องบันทึกฐานทางกฎหมาย[348] เป็นต้น

สำหรับกลไกการบังคับใช้ South Korea's PIPA จะอยู่ในรูปแบบขององค์กรอิสระ คือมี Personal Information Protection Commission ("PIPC") ทำหน้าที่ควบคุมและกำกับดูแลการประมวลผลข้อมูลส่วนบุคคลในกิจการทุกประเภท รวมถึงการดำเนินงานในชั้นสืบสวนและสอบสวน ควบคู่ไปกับองค์กรคุ้มครองสิทธิทั่วไป อาทิ อัยการ ศาล หรือคณะกรรมการสิทธิมนุษยชนแห่งชาติ และผู้ที่กระทำฝ่าฝืนก็จะมีความรับผิดทางอาญาหรือปกครองอีกด้วย[349]

[348] South Korea's PIPA, Article 18.

[349] 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."

บทที่ 5
บทวิเคราะห์และเปรียบเทียบความเหมาะสมของแนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา

หากพิจารณาในมิติของกฎหมายคุ้มครองข้อมูลส่วนบุคคล การสืบสวนและสอบสวนคดีอาญาย่อมเป็นกิจกรรมการประมวลผลข้อมูลส่วนบุคคล เนื่องจากการแสวงหาข้อเท็จจริงและพยานหลักฐานมีขั้นตอนการดำเนินงานที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ในทางทฤษฎีการสืบสวนและสอบสวนจึงเป็นภัยคุกคามต่อความเป็นส่วนตัวในข้อมูล อย่างไรก็ตาม หากพิจารณาในด้านประโยชน์สาธารณะ การสืบสวนและสอบสวนคดีอาญาก็เป็นความชอบธรรมของรัฐประการหนึ่งในการละเมิดสิทธิในข้อมูลส่วนบุคคล เพราะในหลายกรณี ข้อมูลส่วนบุคคลก็เป็นพยานหลักฐานที่ใช้สืบสาวความจริงเกี่ยวกับการกระทำผิดในคดีอาญา และเมื่อสิทธิในข้อมูลส่วนบุคคลไม่ใช่สิทธิเด็ดขาด กฎหมายคุ้มครองข้อมูลส่วนบุคคลในหลายประเทศจึงมักยกเว้นหรือจำกัดการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา[350] รวมถึงสหภาพยุโรปที่ยกเว้นให้การประมวลผลข้อมูลส่วนบุคคลที่ดำเนินการโดยหน่วยงานที่มีอำนาจหน้าที่ป้องกัน สืบสวน ตรวจจับ ดำเนินคดี และบังคับโทษอาญาไม่อยู่ภายใต้บังคับของ GDPR ของสหภาพยุโรป[351] การยกเว้นหรือจำกัดการคุ้มครองข้อมูลส่วนบุคคลเช่นนี้จึงอยู่บนพื้นฐานของทฤษฎีควบคุมอาชญากรรม (Crime control)

แต่ถึงกระนั้น มิได้หมายความว่ารัฐมีอำนาจละเมิดข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนเช่นไรก็ได้ เนื่องจากสิทธิความเป็นส่วนตัวในข้อมูลเป็นสิทธิมนุษยชนขั้นพื้นฐาน การจำกัดสิทธิดังกล่าวจึงต้องมีกฎหมายให้อำนาจไว้ชัดแจ้ง บนพื้นฐานความจำเป็นและได้สัดส่วน[352] ตามแนวคิดของทฤษฎีศุภนิติกระบวน (Due process) และเพื่อให้เป็นไปตามหลักการดังกล่าว สหภาพยุโรปจึงมีกลไกสำคัญสองประการในการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา อันได้แก่

กลไกที่หนึ่ง การตรวจสอบความสอดคล้องกับหลักสิทธิมนุษยชนของกฎหมายที่จำกัดสิทธิในข้อมูลส่วนบุคคล ซึ่งโดยทั่วไปคือกฎหมายวิธีพิจารณาความอาญา

กลไกที่สอง การบังคับใช้ LED กฎหมายคุ้มครองข้อมูลส่วนบุคคลสำหรับการประมวลผลข้อมูลที่เกี่ยวข้องกับการบังคับใช้กฎหมายอาญาเป็นการเฉพาะ

---

[350] คณาธิป ทองรวีวงศ์, "การปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน."

[351] GDPR, Article 2 (d).

[352] ECHR, Article 8.

ในทางกลับกัน แม้รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 มีบทบัญญัติรับรองให้สิทธิในข้อมูลส่วนบุคคลมีคุณค่าในระดับรัฐธรรมนูญ โดยห้ามมิให้นำข้อมูลส่วนบุคคลไปใช้ประโยชน์เว้นแต่อาศัยอำนาจตามบทบัญญัติกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ แต่ในระบบกฎหมายไทย การสืบสวนและสอบสวนคดีอาญากลับได้รับยกเว้นให้ไม่อยู่ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เว้นแต่ในส่วนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยข้อมูล โดยหลัก การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาในประเทศไทยจึงยังคงต้องอาศัยมาตรการทางกฎหมายที่มีอยู่เดิม กล่าวคือ กฎหมายวิธีพิจารณาความอาญาและหมวด 3 ว่าด้วยข้อมูลข่าวสารส่วนบุคคลตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ซึ่งจากการศึกษาในบทที่ 3 พบว่าแต่ละมาตรการต่างมีข้อจำกัดบางประการในการคุ้มครองข้อมูลส่วนบุคคล

เมื่อเปรียบเทียบกับต่างประเทศ ได้แก่ สหราชอาณาจักร สหรัฐอเมริกา และสาธารณรัฐเกาหลี จะพบว่าแม้ประเทศต่าง ๆ ข้างต้นจะมีกฎหมายที่เป็นกรอบการใช้อำนาจสืบสวนและสอบสวนอยู่เดิม แต่ก็ไม่ปรากฏว่ามีประเทศใดบัญญัติยกเว้นให้การสืบสวนและสอบสวนคดีอาญาไม่อยู่ภายใต้บังคับของกฎหมายคุ้มครองข้อมูลส่วนบุคคลโดยสิ้นเชิง การดำเนินงานในชั้นสืบสวนและสอบสวนคดีอาญาของทั้งสามประเทศจึงอยู่ในบังคับที่จะต้องปฏิบัติตามหลักเกณฑ์ในกฎหมายวิธีพิจารณาความอาญาควบคู่ไปกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล เช่นเดียวกันกับแนวทางของสหภาพยุโรป

ฉะนั้น เพื่อให้ได้มาซึ่งบทสรุปและข้อเสนอแนะในการแก้ไขปัญหาในบทสุดท้าย จึงเห็นสมควรวิเคราะห์และเปรียบเทียบมาตรการทางกฎหมายเชิงควบคู่ แบ่งเป็น กฎหมายวิธีพิจารณาความอาญาและกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยผู้เขียนจะหยิบยกแนวคิด หลักการ และทฤษฎีที่เกี่ยวข้อง รวมถึงแนวทางตามกฎหมายระหว่างประเทศและกฎหมายต่างประเทศมาวิเคราะห์และเปรียบเทียบกับบทบัญญัติกฎหมายไทย โดยใช้เกณฑ์ของสหภาพยุโรปเป็นพื้นฐาน เนื่องจากแนวทางของสหภาพยุโรปเป็นมาตรฐานที่ได้รับการยอมรับจากนานาประเทศและเป็นต้นแบบกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยในปัจจุบัน

5.1 กฎหมายวิธีพิจารณาความอาญา

โดยที่กฎหมายวิธีพิจารณาความอาญามิใช่บทบัญญัติกฎหมายที่มีเจตนารมณ์ในการคุ้มครองข้อมูลส่วนบุคคลเป็นการเฉพาะ กฎหมายวิธีพิจารณาความอาญาจึงมีข้อจำกัดโดยสภาพในการคุ้มครองข้อมูลส่วนบุคคล เนื่องจากกฎหมายวิธีพิจารณาความอาญาไม่ได้ถูกออกแบบมาให้สอดรับกับลักษณะธรรมชาติของความเป็นส่วนตัวในข้อมูล

อย่างไรก็ตาม เมื่อกฎหมายวิธีพิจารณาความอาญาเป็นกฎหมายที่ให้อำนาจเจ้าหน้าที่ของรัฐเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ซึ่งโดยหลักแล้ว เป็นการกระทำที่ละเมิดสิทธิส่วนบุคคล กฎหมายวิธีพิจารณาความอาญาจึงมีความสัมพันธ์อย่างมีนัยสำคัญกับการคุ้มครองข้อมูลส่วนบุคคล เพราะหากกฎหมายวิธีพิจารณาความอาญาให้น้ำหนักกับการควบคุมอาชญากรรมมากกว่าการคุ้มครองสิทธิส่วนบุคคล กฎหมายนั้นก็อาจเอื้อให้รัฐสามารถก้าวล่วงข้อมูลส่วนบุคคลจากการดำเนินงานในชั้นสืบสวนและสอบสวนคดีอาญาได้อย่างกว้างขวาง และย่อมส่งผลตามมาว่าสภาพแวดล้อมทางกฎหมายมีระดับการคุ้มครองข้อมูลส่วนบุคคลที่ลดลง[353] กฎหมายวิธีพิจารณาความอาญาจึงเป็นปัจจัยแวดล้อมทางกฎหมายประการหนึ่ง ที่สภาพยุโรปนำมาวินิจฉัยถึงระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอด้วยการใช้เกณฑ์การปกป้องสิทธิเป็นฐานในการพิจารณาความสอดคล้องกับหลักสิทธิมนุษยชน โดยมีตัวอย่างเกณฑ์การพิจารณาที่สำคัญ ดังต่อไปนี้

1.) <u>หลักความเฉพาะเจาะจง</u>
กฎหมายวิธีพิจารณาความอาญาควรกำหนดขอบเขตการใช้อำนาจในชั้นสืบสวนและสอบสวนให้ชัดเจนเพียงพอที่ประชาชนทั่วไปสามารถคาดหมายได้ ทั้งในแง่เหตุแห่งการใช้อำนาจ มาตรการที่ใช้ เป้าหมาย และระยะเวลา

2.) <u>หลักการตรวจสอบถ่วงดุล</u>
การใช้อำนาจสืบสวนและสอบสวนตามกฎหมายวิธีพิจารณาความอาญาควรอยู่ภายใต้กระบวนการตรวจสอบขององค์กรอื่น

3.) <u>หลักความจำเป็นและได้สัดส่วน</u>
กฎหมายวิธีพิจารณาความอาญาต้องรักษาสมดุลระหว่างการควบคุมอาชญากรรมกับการคุ้มครองสิทธิและเสรีภาพ โดยมีมาตรการที่เพียงพอในการคุ้มครองสิทธิความเป็นส่วนตัวในข้อมูลของบุคคล

ทั้งนี้ ผลกระทบจากการที่กฎหมายวิธีพิจารณาความอาญาไม่เป็นไปตามเกณฑ์การปกป้องสิทธิอาจทำให้การคุ้มครองข้อมูลส่วนบุคคลในภาพรวมถูกประเมินได้ว่า “ไม่เพียงพอ” ตามกรอบกฎหมายของสหภาพยุโรป จนเกิดเป็นอุปสรรคในการโอนข้อมูลระหว่างประเทศ คือจะไม่สามารถรับโอนข้อมูลจากกลุ่มประเทศสหภาพยุโรปได้อย่างเสรี[354]

---

[353] คณาธิป ทองรวีวงศ์, "การปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน."

[354] อ้างแล้ว.

5.1.1 บทวิเคราะห์กฎหมายไทย

แม้กฎหมายวิธีพิจารณาความอาญาจะเป็นบทบัญญัติหลักที่ควบคุมการใช้อำนาจสืบสวนและสอบสวนคดีอาญาในประเทศไทย แต่จากการศึกษาในบทที่ 3 พบว่ากฎหมายวิธีพิจารณาความอาญามีข้อจำกัดในการให้ความคุ้มครองข้อมูลส่วนบุคคล สรุปได้ดังนี้

ตารางที่ 4 ข้อจำกัดของกฎหมายวิธีพิจารณาความอาญาไทย

ลักษณะของข้อจำกัด	รายละเอียด
ข้อจำกัดที่ 1 กฎหมายวิธีพิจารณาความอาญาเปิดช่องให้เจ้าหน้าที่รัฐมีอำนาจในการเก็บรวบรวมข้อมูลส่วนบุคคลอย่างกว้างขวาง	1.1 การค้นที่อยู่ในบังคับที่จะต้องได้รับหมายหรือคำสั่งจากศาลมีขอบเขตอย่างจำกัด 1.2 การได้มาซึ่งข้อมูลข่าวสารตามพระราชบัญญัติเฉพาะของไทยมีขอบเขตการใช้อำนาจอย่างกว้าง เนื่องจากถ้อยคำในบทบัญญัติขาดความชัดเจนและเฉพาะเจาะจง 1.3 การขอข้อมูลข่าวสารจากผู้ประกอบการภาคเอกชนเป็นอำนาจสอบสวนทั่วไป จึงไม่ได้ผ่านกระบวนการตรวจสอบจากศาล
ข้อจำกัดที่ 2 กฎหมายวิธีพิจารณาความอาญาไม่ได้ถูกออกแบบให้สอดคล้องกับลักษณะธรรมชาติของความเป็นส่วนตัวในข้อมูล	2.1 ไม่มีกฎเกณฑ์ครอบคลุมรูปแบบพฤติกรรมหรือการดำเนินการต่อข้อมูลส่วนบุคคลครบถ้วนทุกลักษณะ 2.2 ไม่มีบทบัญญัติรับรองสิทธิเจ้าของข้อมูลส่วนบุคคล 2.3 ไม่มีสภาพบังคับและบทกำหนดโทษที่เหมาะสม อีกทั้ง เมื่อเกิดความเสียหาย ผู้เสียหายยังคงมีภาระพิสูจน์ตามหลักทั่วไป

ข้อวิเคราะห์ที่ 1 แม้ว่ากฎหมายวิธีพิจารณาความอาญากับกฎหมายคุ้มครองข้อมูลส่วนบุคคลจะเป็นกฎหมายคนละฉบับกัน แต่กฎหมายวิธีพิจารณาความอาญาก็มีความเชื่อมโยงกับระดับของการคุ้มครองข้อมูลส่วนบุคคล โดยเหตุที่ว่ากฎหมายวิธีพิจารณาความอาญาประกอบด้วยมาตรการที่ส่งผลกระทบต่อข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่ง จากการดำเนินงานในชั้นสืบสวนและสอบสวนคดีอาญาจึงมีปัญหาที่จะต้องพิจารณาว่า กฎหมายวิธีพิจารณาความอาญาของไทยนั้นส่งผลกระทบต่อภาพรวมการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยเพียงใด ซึ่งหากพิเคราะห์ถึงความสอดคล้องกับหลักสิทธิมนุษยชนตามเกณฑ์การปกป้องสิทธิของสหภาพยุโรป พบว่ากฎหมายวิธีพิจารณาความอาญาของไทยมีแนวโน้มจะถูกพิจารณาว่าไม่สอดคล้องกับเกณฑ์ดังกล่าว เนื่องจากกฎหมายวิธีพิจารณาความอาญาของไทยเปิดช่องให้เจ้าหน้าที่รัฐเก็บรวบรวมข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาอย่างกว้างขวางตามที่ปรากฏเป็นข้อจำกัดที่ 1 ในตารางที่ 4 โดยมีข้อควรพิเคราะห์สามประการคือ

ข้อวิเคราะห์ที่ 1.1 การค้นซึ่งอยู่ในบังคับที่จะต้องได้รับหมายค้นหรือคำสั่งของศาล มีขอบเขตอย่างจำกัด ส่งผลให้ในทางปฏิบัติ การใช้อำนาจสืบสวนและสอบสวนคดีอาญาในหลายกรณีไม่ได้ผ่านกระบวนการตรวจสอบจากศาล จึงไม่สอดคล้องกับ “หลักการตรวจสอบถ่วงดุล” ตามเกณฑ์การปกป้องสิทธิของสหภาพยุโรปแต่อย่างใด

ทั้งนี้ เพราะประมวลกฎหมายวิธีพิจารณาความอาญาของไทยบัญญัติแยก “การค้น” กับ “การรวบรวมพยานหลักฐาน” ออกจากกัน ทั้งยังแบ่งการค้นเป็นสามประเภท ได้แก่ การค้นบุคคลในที่สาธารณสถาน การค้นในที่รโหฐาน และการค้นเอกสารทางไปรษณีย์โทรเลข ซึ่งมีเพียงการค้นสองประเภทหลังเท่านั้นที่กฎหมายกำหนดให้ต้องมีคำสั่งหรือหมายของศาล[355] ฉะนั้น หากเป็นการใช้อำนาจลักษณะอื่นนอกเหนือจากการค้นที่กฎหมายบัญญัติ ก็มีแนวโน้มที่เจ้าหน้าที่รัฐจะกล่าวอ้างว่าเป็นการรวบรวมพยานหลักฐาน ซึ่งเป็นอำนาจสืบสวนสอบสวนทั่วไป เพื่อไม่ให้อยู่ภายใต้บังคับที่จะต้องได้รับคำสั่งหรือหมายของศาล เช่น การบันทึกภาพด้วยโดรน การใช้เทคโนโลยีตรวจจับใบหน้า การค้นหาตำแหน่งจากเสาสัญญาณโทรศัพท์ หรือกระทั่งการขอข้อมูลข่าวสารจากผู้ประกอบการภาคเอกชน ซึ่งจะได้กล่าวในรายละเอียดในข้อพิจารณาต่อ ๆ ไป

ข้อวิเคราะห์ที่ 1.2 การได้มาซึ่งข้อมูลข่าวสารตามพระราชบัญญัติเฉพาะ มีขอบเขตการใช้อำนาจกว้างขวาง เนื่องจากบทบัญญัติที่ให้อำนาจขาดความชัดเจนเฉพาะเจาะจง บุคคลทั่วไปจึงไม่อาจคาดหมายได้ว่าการได้มาซึ่งข้อมูลข่าวสารในชั้นสืบสวนและสอบสวนกระทำได้ในสถานการณ์ใดด้วยเงื่อนไขอย่างไร จนอาจนำไปสู่การใช้ดุลพินิจตามอำเภอใจของเจ้าหน้าที่รัฐ การใช้อำนาจนั้นจึงมีความไม่สอดคล้องกับ “หลักความเฉพาะเจาะจง” ตามเกณฑ์สหภาพยุโรป กล่าวคือ

1.) <u>ความเฉพาะเจาะจงในแง่ “เหตุแห่งการใช้อำนาจ”</u>

แม้โดยทั่วไป การได้มาซึ่งข้อมูลข่าวสารตามพระราชบัญญัติเฉพาะจะจำกัดขอบเขตประเภทความผิดเพื่อการสืบสวนสอบสวนหรือบังคับใช้กฎหมายนั้น แต่พระราชบัญญัติบางฉบับก็ขยายขอบเขตการใช้อำนาจไปเกินกว่านั้น อาทิ พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 ซึ่งขยายขอบเขตความผิดไปถึงความผิดอื่นที่ใช้ระบบคอมพิวเตอร์หรือมีข้อมูลคอมพิวเตอร์เกี่ยวข้อง ในปัจจุบัน ความผิดอาญาแทบทุกประเภทจึงอาจถูกพิจารณาได้ว่าอยู่ในขอบเขตความผิดตามพระราชบัญญัตินี้ได้[356]

---

[355] ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 92 และมาตรา 105.

[356] คณาธิป ทองรวีวงศ์, "การปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน."

2.) <u>ความเฉพาะเจาะจงในแง่ “มาตรการที่ใช้”</u>

พระราชบัญญัติเฉพาะที่ให้อำนาจเจ้าหน้าที่รัฐได้มาซึ่งข้อมูลข่าวสารในไทยมักบัญญัติด้วยถ้อยคำอย่างกว้างว่า “เพื่อให้ได้มาซึ่งข้อมูลข่าวสาร” เท่านั้น โดยไม่ระบุมาตรการที่ใช้อย่างชัดเจน จึงเป็นการเปิดโอกาสให้เจ้าหน้าที่รัฐใช้มาตรการต่าง ๆ เพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลตามอำเภอใจ โดยไม่จำกัดวิธีการ จนอาจส่งผลกระทบต่อสิทธิส่วนบุคคลเกินกว่าสมควร

3.) <u>ความเฉพาะเจาะจงในแง่ “เป้าหมาย”</u>

การได้มาซึ่งข้อมูลข่าวสารในประเทศไทย จะไม่ได้มีการกำหนดขอบเขตในแง่เป้าหมายที่ตัวบุคคล แต่จะเป็นการกำหนดขอบเขตที่ข้อมูลข่าวสาร ที่ถูกใช้หรืออาจถูกใช้เพื่อกระทำผิด ข้อมูลที่เจ้าหน้าที่รัฐอาจเข้าถึงได้จึงไม่ได้จำกัดเฉพาะข้อมูลของผู้ต้องสงสัยหรือผู้กระทำผิดเท่านั้น[357]

4.) <u>ความเฉพาะเจาะจงในแง่ “ระยะเวลา”</u>

ในบรรดาพระราชบัญญัติเฉพาะที่มีบทบัญญัติให้อำนาจเจ้าหน้าที่รัฐได้มาซึ่งข้อมูลข่าวสาร พบว่ามีพระราชบัญญัติจำนวนหนึ่งที่มีการกำหนดระยะเวลาในการสั่งอนุญาตที่ชัดเจน[358] แต่ก็มีพระราชบัญญัติเฉพาะอีกจำนวนหนึ่งที่ไม่ได้กำหนดขอบเขตแง่ระยะเวลาที่ชัดเจน เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 อันเป็นการเปิดช่องให้พนักงานเจ้าหน้าที่ใช้อำนาจได้อย่างต่อเนื่อง[359]

ข้อวิเคราะห์ที่ 1.3 การเก็บรวบรวมข้อมูลข่าวสารจากผู้ประกอบการภาคเอกชนถือเป็นอำนาจสอบสวนทั่วไป ทำให้การเก็บรวบรวมข้อมูลดังกล่าวเป็นดุลพินิจของเจ้าหน้าที่รัฐโดยลำพัง จะเห็นได้จากรูปแบบการใช้อำนาจที่ทำเป็นหนังสือขอความร่วมมือ โดยไม่ผ่านกระบวนการตรวจสอบจากศาล อีกทั้ง ไม่ปรากฏว่ามีข้อจำกัดการใช้อำนาจที่ชัดเจน การเก็บรวบรวมข้อมูลจากภาคเอกชนในชั้นสืบสวนและสอบสวนของไทย จึงอาจถูกพิจารณาได้ว่าไม่สอดคล้องกับ “หลักความเฉพาะเจาะจง” และ “หลักการตรวจสอบถ่วงดุล” ตามเกณฑ์ของสหภาพยุโรป

---

[357] อ้างแล้ว.

[358] โปรดดู พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 25 หรือพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 มาตรา 17 หรือพระราชบัญญัติป้องกันและปราบปรามการค้ามนุษย์ พ.ศ. 2551 มาตรา 30 หรือพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มาตรา 46.

[359] คณาธิป ทองรวีวงศ์, "การปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน."

เหตุที่การเก็บรวบรวมข้อมูลข่าวสารส่วนบุคคลจากภาคเอกชนกลายเป็นปัญหาหนึ่งของการละเมิดความเป็นส่วนตัวในชั้นสืบสวนและสอบสวนคดีอาญา มีสาเหตุมาจากการที่ในปัจจุบันผู้ประกอบธุรกิจมีข้อมูลส่วนบุคคลผู้บริโภคในครอบครองจำนวนมาก โดยเฉพาะในธุรกิจโทรคมนาคมที่มีกฎหมายบังคับให้จัดเก็บข้อมูลระบุตัวตนผู้ใช้บริการ[360] และเมื่อพิจารณาประกอบกับแนวปฏิบัติที่เจ้าพนักงานสืบสวนสอบสวนมักเรียกเอาข้อมูลจากผู้ประกอบการ ในรูปแบบหนังสือขอความร่วมมือ[361] เป็นเหตุให้การเก็บรวบรวมข้อมูลข่าวสารส่วนบุคคลจากภาคเอกชนในไทยกลายเป็นอำนาจดุลพินิจของเจ้าหน้าที่รัฐโดยลำพัง เพราะไม่ว่าการกระทำความผิดประเภทใด ในสถานการณ์อย่างไร เจ้าหน้าที่รัฐก็สามารถขอตรวจดูข้อมูลข่าวสารได้ โดยที่ไม่จำต้องได้รับคำสั่งหรือหมายจากศาลแต่อย่างใด

สุดท้าย หากนำข้อวิเคราะห์ที่ 1.1-1.3 มาพิจารณาร่วมกับ “หลักความจำเป็นและได้สัดส่วน” เห็นว่า แม้กฎหมายวิธีพิจารณาความอาญาของไทยจะมีการบัญญัติถึงหลักความจำเป็นอยู่บ้าง[362] แต่ลำพังการระบุถ้อยคำว่า “จำเป็น” ก็อาจไม่เพียงพอที่จะสอดคล้องกับเกณฑ์การปกป้องสิทธินี้ เพราะถ้อยคำดังกล่าวเป็นเพียงหลักการกว้าง ๆ ไม่มีรายละเอียดชัดเจน[363] ดังนั้น แม้จะปรากฏความจำเป็นที่กฎหมายวิธีพิจารณาความอาญาต้องให้อำนาจเจ้าหน้าที่รัฐทำการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา เพื่อแสวงหาข้อเท็จจริงและรวบรวมพยานหลักฐานในการดำเนินคดี แต่เมื่อกฎหมายวิธีพิจารณาความอาญาของไทยไม่อาจควบคุมการใช้อำนาจสืบสวนและสอบสวนให้เป็นไปตามเกณฑ์การปกป้องสิทธิ ตามที่ปรากฏในข้อวิเคราะห์ต่าง ๆ ข้างต้น การสืบสวนและสอบสวนคดีอาญาจึงอาจส่งผลกระทบต่อสิทธิในข้อมูลส่วนบุคคลจนไม่ได้สัดส่วน

ด้วยเหตุนี้ จึงอาจสรุปได้ว่ากฎหมายวิธีพิจารณาความอาญาของไทยยังไม่สอดคล้องกับเกณฑ์การปกป้องสิทธิของสหภาพยุโรปเท่าที่ควร จึงมีความเสี่ยงที่จะภาพรวมการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยอาจถูกพิจารณาได้ว่ามีระดับที่ไม่เพียงพอตามมาตรฐานสหภาพยุโรป ด้วยกฎหมายที่ให้อำนาจเจ้าหน้าที่รัฐเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาขาดมาตรการที่เหมาะสมเพียงพอในการปกป้องความเป็นส่วนตัวในข้อมูลของบุคคล

---

[360] อ้างแล้ว.

[361] ศักดา เตชะเกรียงไกรและคณะ, "คู่มือการสืบสวน" [ออนไลน์]. แหล่งที่มา: http://wutthi.central.police.go.th.

[362] โปรดดู ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 131/1 ที่วางหลักให้การตรวจพิสูจน์ซึ่งจำเป็นต้องตรวจเก็บตัวอย่างเลือด เนื้อเยื่อ ผิวหนัง เส้นผมหรือขน น้ำลาย ปัสสาวะ อุจจาระ สารคัดหลั่ง สารพันธุกรรมหรือส่วนประกอบของร่างกายจากบุคคล ให้กระทำเพียงเท่าที่จำเป็นและสมควร หรือ พระราชบัญญัติว่าด้วยกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 มาตรา 18 มีการวางหลักให้การตรวจสอบและเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ จะต้องกระทำเฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด เป็นต้น

[363] คณาธิป ทองรวีวงศ์, "การปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน."

ข้อวิเคราะห์ที่ 2 แม้ในระบบกฎหมายไทย กฎหมายวิธีพิจารณาความอาญาเป็นทั้งบทบัญญัติที่ให้อำนาจและจำกัดอำนาจของเจ้าหน้าที่รัฐในการล่วงล้ำข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวน ทว่ากฎหมายวิธีพิจารณาความอาญาก็มิได้มีเจตนารมณ์ในการคุ้มครองข้อมูลส่วนบุคคลโดยตรง แต่มุ่งควบคุมให้การดำเนินกระบวนการยุติธรรมเป็นไปด้วยความเรียบร้อย กฎหมายวิธีพิจารณาความอาญาจึงไม่ได้มีบทบัญญัติที่สอดคล้องกับธรรมชาติของสิทธิในข้อมูลส่วนบุคคล ปรากฏเป็นข้อจำกัดที่ 2 ในตารางที่ 4 และย่อมส่งผลตามมาว่ากฎหมายวิธีพิจารณาความอาญาไม่อาจคุ้มครองข้อมูลส่วนบุคคลในลักษณะเดียวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลได้

ตัวอย่างเช่น ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 131/1 กำหนดหลักเกณฑ์และวิธีการตรวจเก็บตัวอย่างสารพันธุกรรมว่า ให้แพทย์หรือผู้เชี่ยวชาญดำเนินการตรวจเท่าที่จำเป็นและใช้วิธีการที่ก่อให้เกิดความเจ็บปวดน้อยที่สุดเท่าที่กระทำได้ โดยไม่กำหนดหลักเกณฑ์อื่นใดเพิ่มเติม ทั้งที่สารพันธุกรรมถือเป็นข้อมูลอ่อนไหวตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ทำให้การใช้ การเก็บรักษาและการทำลายข้อมูลสารพันธุกรรมในชั้นสืบสวนและสอบสวน ขาดกฎเกณฑ์ที่แน่ชัดมาควบคุมกำกับ จึงก่อให้เกิดความเสี่ยงที่ข้อมูลจะถูกละเมิดในขั้นตอนการดำเนินการเหล่านี้ อาทิ มีการนำข้อมูลไปใช้ประโยชน์โดยมิชอบหรือข้อมูลเกิดการรั่วไหล เป็นต้น

เมื่อมาตรการในกฎหมายวิธีพิจารณาความอาญายังไม่เพียงพอที่จะคุ้มครองข้อมูลส่วนบุคคลได้อย่างเหมาะสม ด้วยข้อจำกัดโดยสภาพของกฎหมายดังกล่าว จึงมีความจำเป็นที่ประเทศไทยจะต้องกำหนดมาตรการทางกฎหมายอื่นในการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาควบคู่ไปกับกฎหมายวิธีพิจารณาความอาญา ซึ่งจะได้พิเคราะห์ในหัวข้อต่อ ๆ ไป

5.1.2 บทเปรียบเทียบกับกฎหมายต่างประเทศ

เมื่อเปรียบเทียบกับกฎหมายต่างประเทศในบทที่ 4 กล่าวคือ สหราชอาณาจักร สหรัฐอเมริกา และสาธารณรัฐเกาหลี พบว่ามีข้อควรพิจารณาดังต่อไปนี้

ข้อพิจารณาที่ 1 เพื่อประโยชน์ในการป้องปรามการกระทำความผิดอาญา ระบบกฎหมายของประเทศสหราชอาณาจักร สหรัฐอเมริกา และสาธารณรัฐเกาหลี จึงมีบทบัญญัติให้อำนาจเจ้าหน้าที่รัฐเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา เช่นเดียวกับกฎหมายวิธีพิจารณาความอาญาของไทย แต่ในขณะเดียวกัน กฎหมายของประเทศต่าง ๆ ข้างต้นก็มีการกำหนดกรอบการใช้อำนาจสืบสวนและสอบสวนคดีอาญา โดยมีรายละเอียดดังนี้

ข้อพิจารณาที่ 1.1 “การค้นและยึดทั่วไป” ตามบทบัญญัติกฎหมายทั้งสามประเทศอยู่ในบังคับที่จะต้องมีหมายหรือคำสั่งของศาลเป็นหลัก ส่วนการค้นและยึดโดยไม่มีหมายหรือคำสั่งศาลจะเป็นกรณียกเว้นเท่านั้น จึงสอดคล้องกับหลักการตรวจสอบถ่วงดุลตามเกณฑ์ของสหภาพยุโรป ดังที่ปรากฏรายละเอียดในตารางที่ 5 ต่อไปนี้

ตารางที่ 5 การค้นและยึดทั่วไปตามกฎหมายต่างประเทศ

ประเทศ	กรอบการใช้อำนาจ
สหราชอาณาจักร	การค้นทั่วไปจะต้องมีหมายค้นหรือคำสั่งของศาลเป็นฐานอำนาจ โดยในการร้องขอหมายค้นหรือคำสั่งศาล จะต้องระบุเหตุอันสมควรและความจำเป็น รวมถึงรายละเอียดบุคคล สิ่งของ และสถานที่ที่ต้องการค้นมากที่สุดเท่าที่กระทำได้
สหรัฐอเมริกา	ได้รับคุ้มครองตาม The Fourth Amendment โดยห้ามมิให้ค้นและยึดโดยปราศจากเหตุผลอันสมควร และห้ามมิให้มีการออกหมายเพื่อค้นและยึดโดยไม่มีเหตุอันควร
สาธารณรัฐเกาหลี	โดยหลัก การค้นหรือยึดจะกระทำได้ต่อเมื่อได้รับหมายจากศาล การค้นหรือยึดโดยไม่มีหมายจะกระทำได้อย่างจำกัดเฉพาะในบางสถานการณ์ หรือในกรณีจำเป็นเร่งด่วน แต่ให้ขอหมายจากศาลภายหลังจากที่การค้นหรือยึดสิ้นสุดแทน นอกจากนี้ หากสิ่งที่ต้องการค้นหรือยึดเป็นสื่อบันทึกข้อมูล ให้ค้นหรือยึดเฉพาะข้อมูลที่เกี่ยวข้อง โดยศาลจะมีหน้าที่ในการแจ้งข้อเท็จจริงดังกล่าวให้เจ้าของข้อมูลทราบ

หากเปรียบเทียบกับกฎหมายวิธีพิจารณาความอาญาของไทย จะพบว่าการค้นและยึดที่อยู่ในบังคับที่จะต้องได้รับคำสั่งหรือหมายจากศาลตามกฎหมายทั้งสามประเทศมีขอบเขตที่กว้างกว่ากฎหมายไทย โดยเฉพาะอย่างยิ่ง ในสหรัฐอเมริกาที่ตีความ “การค้นและยึด” ครอบคลุมการแสวงหาพยานหลักฐานหลากหลายรูปแบบ ไม่ว่าจะเป็นการติดตั้งเครื่องติดตาม[364] การสะกดรอยจากตำแหน่งสมาร์ตโฟน[365] การบันทึกภาพหรือเฝ้าระวังทางเฮลิคอปเตอร์[366] ฯลฯ ในขณะที่ประเทศไทย มีการค้นเพียงสองกรณีที่ต้องมีหมายศาลเป็นฐานอำนาจ จึงมีความจำเป็นที่ประเทศไทยต้องพิจารณาทบทวนว่านอกเหนือจากการค้นที่รโหฐานและการค้นเอกสารทางไปรษณีย์เอกสาร มีการแสวงหาพยานหลักฐานรูปแบบอื่นใดหรือไม่ที่ควรจะอยู่ภายใต้กระบวนการตรวจสอบถ่วงดุลของศาล โดยเฉพาะการแสวงหาพยานหลักฐานที่มีเทคโนโลยีสมัยใหม่มาเกี่ยวข้อง

---

[364] 468 U.S. 705 (1984).

[365] 84 U.S. 489 (1873).

[366] 488 U.S. 445 (1989).

ข้อพิจารณาที่ 1.2 สำหรับ “การได้มาซึ่งข้อมูลข่าวสารส่วนบุคคล” ในการสืบสวนและสอบสวนคดีอาญาตามกฎหมายสหราชอาณาจักร สหรัฐอเมริกา และสาธารณรัฐเกาหลี จะมีการกำหนดกรอบการใช้อำนาจที่เข้มงวดกว่าการค้นและยึดทั่วไป ได้แก่ (1) กระบวนการตรวจสอบถ่วงดุล (2) หลักเกณฑ์และเงื่อนไขการใช้อำนาจ และ (3) มาตรการคุ้มครองสิทธิ โดยมีรายละเอียดดังนี้

ตารางที่ 6 การได้มาซึ่งข้อมูลข่าวสารส่วนบุคคลตามกฎหมายต่างประเทศ

ประเทศ	กรอบการใช้อำนาจ
สหราชอาณาจักร	อยู่ภายใต้ IPA 2016 โดยมีกฎเกณฑ์ที่เกี่ยวข้องคือ 1. กระบวนการตรวจสอบถ่วงดุล: ผ่านกระบวนการ Double-lock คือในการออกหมายต้องผ่านการขออนุญาตทั้งจากหน่วยงานผู้มีอำนาจหน้าที่และศาล (สองชั้น) 2. หลักเกณฑ์และเงื่อนไขการใช้อำนาจ: แจกแจงมาตรการที่ใช้ และจำกัดเฉพาะการสืบสวนสอบสวนอาชญากรรมร้ายแรง อีกทั้ง จำกัดระยะเวลาที่หมายมีผลเป็น 6 เดือนนับแต่วันที่ออกหมาย เว้นแต่เป็นหมายในกรณีเร่งด่วน จะมีกำหนดระยะเวลา 5 วัน 3. มาตรการคุ้มครองสิทธิ: บัญญัติกฎเกณฑ์ทั่วไปในการคุ้มครองความเป็นส่วนตัว
สหรัฐอเมริกา	อยู่ภายใต้ The Fourth Amendment เพราะหลัก “ความคาดหมายความเป็นส่วนตัว” ขยายขอบเขตการคุ้มครอง ไม่จำกัดเฉพาะการค้นและยึดทางกายภาพ 1. กระบวนการตรวจสอบถ่วงดุล: เป็นไปตาม The Fourth Amendment 2. หลักเกณฑ์และเงื่อนไขการใช้อำนาจ: เป็นไปตามกฎหมายแต่ละฉบับ อาทิ The U.S. Code กำหนดรายละเอียดเกี่ยวกับการขออนุญาตและวิธีการใช้อำนาจ เช่น การบ่งชี้รายละเอียด ระบุบัญชีความผิด กำหนดวิธีการบันทึกข้อมูล และจำกัดเวลา 3. มาตรการคุ้มครองสิทธิ: ให้จัดทำรายงานแสดงความคืบหน้าของการดำเนินการตามระยะเวลาที่ศาลกำหนด และเปิดโอกาสให้ผู้ได้รับผลกระทบอาจโต้แย้งได้
สาธารณรัฐเกาหลี	อยู่ภายใต้ CPPA ซึ่งมีการแบ่งประเภทข้อมูลการติดต่อสื่อสารเป็นสองระดับ ได้แก่ (1) ข้อมูลที่ยืนยันการติดต่อสื่อสาร และ (2) เนื้อความของการติดต่อสื่อสาร 1. กระบวนการตรวจสอบถ่วงดุล: มีหมายศาลเป็นฐานอำนาจ แต่หากเป็นกรณีเร่งด่วนให้มีการขออนุญาตจากศาลย้อนหลังแทน ซึ่งหากศาลมีคำสั่งไม่อนุญาตในภายหลัง ข้อมูลที่ได้มาก็ต้องทำลายทั้งสิ้น 2. หลักเกณฑ์และเงื่อนไขการใช้อำนาจ: การเข้าถึงเนื้อความของการติดต่อสื่อสารเป็นวิถีทางสุดท้าย จึงมีหลักเกณฑ์ที่เคร่งครัดกว่าการได้มาซึ่งข้อมูลที่ยืนยันการติดต่อสื่อสาร 3. มาตรการคุ้มครองสิทธิ: ให้แจ้งเจ้าของข้อมูลทราบถึงข้อเท็จจริงเกี่ยวกับการได้มาซึ่งข้อมูลการติดต่อสื่อสาร เพื่อที่ว่าเจ้าของข้อมูลจะใช้สิทธิตรวจสอบได้ เว้นแต่การแจ้งนั้นจะมีผลกระทบต่อประโยชน์อื่นที่มีความสำคัญยิ่งกว่า

จะเห็นได้ว่าการได้มาซึ่งข้อมูลข่าวสารส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาตามกฎหมายทั้งสามประเทศต่างมีคำสั่งหรือหมายของศาลเป็นฐานอำนาจเช่นเดียวกันกับประเทศไทย แต่หากพิจารณารายละเอียด จะพบว่าหลักเกณฑ์และเงื่อนไขการใช้อำนาจของประเทศต่าง ๆ ข้างต้นจะมีรายละเอียดที่เฉพาะเจาะจงมากกว่าประเทศไทย กล่าวคือมีการกำหนดขอบเขตประเภทความผิดที่ชัดเจน โดยสหรัฐอเมริกาและสาธารณรัฐเกาหลีจะระบุเป็นบัญชีฐานความผิด ส่วนสหราชอาณาจักรจะใช้การบัญญัตินิยามเป็นเกณฑ์พิจารณาว่าความผิดประเภทใดเป็นความผิดร้ายแรง (Serious crime) ทำให้เกิดความเฉพาะเจาะจงในแง่เหตุแห่งการใช้อำนาจ

นอกจากนี้ สำหรับความเฉพาะเจาะจงในแง่ของมาตรการ เป้าหมาย และระยะเวลา พบว่ากฎหมายวิธีพิจารณาความอาญาของทุกประเทศพยายามที่จะระบุรายละเอียดเงื่อนไขเหล่านี้ให้ชัดเจนมากที่สุดเท่าที่จะกระทำได้ อาทิ สหราชอาณาจักรมีการแจกแจงมาตรการที่ใช้ตาม IPA 2016 หรือสหรัฐอเมริกามีการกำหนดเนื้อหาคำร้องขออนุญาต โดยให้บรรยายรายละเอียดบ่งชี้เกี่ยวกับการกระทำผิดและบุคคลที่เป็นเป้าหมาย ในขณะที่สาธารณรัฐเกาหลีแบ่งประเภทข้อมูลการติดต่อสื่อสารเป็นสองระดับ เพื่อกำหนดเกณฑ์การใช้อำนาจตาม CPPA ให้มีความเหมาะสมกับข้อมูลแต่ละประเภท และไม่ว่ากฎหมายของประเทศใดก็ล้วนแล้วแต่มีการกำหนดกรอบระยะเวลาขั้นสูงในการใช้อำนาจและมาตรการเพื่อคุ้มครองสิทธิของบุคคลทั้งสิ้น อย่างไรก็ดี มีข้อสังเกตว่าการคุ้มครองตามบทบัญญัติแก้ไขเพิ่มเติมรัฐธรรมนูญฉบับที่ 4 ของสหรัฐอเมริกา อาจมีข้อจำกัดในกรณีที่เจ้าหน้าที่ใช้เทคโนโลยีสมัยใหม่ที่มีความซับซ้อนในการสืบสวนและสอบสวนคดีอาญา เพราะเทคโนโลยีเหล่านี้มักอยู่นอกเหนือขอบเขตความคาดหมายความเป็นส่วนตัวของบุคคล

เมื่อเปรียบเทียบกับประเทศไทย เห็นว่าในบรรดากรอบควบคุมการใช้อำนาจข้างต้น มาตรการคุ้มครองสิทธิของบุคคลจะเป็นมาตรการที่ไม่ได้บัญญัติไว้ในกฎหมายวิธีพิจารณาความอาญาของไทยแต่อย่างใด ประเทศไทยจึงไม่มีกลไกทางกฎหมายเพื่อบรรเทาผลกระทบที่อาจเกิดขึ้นกับบุคคล อีกทั้ง การได้มาซึ่งข้อมูลข่าวสารในชั้นสืบสวนและสอบสวนคดีอาญาของไทยนั้นก็ขาดความสอดคล้องกับหลักความเฉพาะเจาะจงของสหภาพยุโรป โดยเฉพาะพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 ตามที่ปรากฏในข้อวิเคราะห์ที่ 1.2 จึงเห็นควรที่ประเทศไทยพิจารณาทบทวนแก้ไขปรับปรุงกฎหมายวิธีพิจารณาความอาญา โดยบัญญัติหลักเกณฑ์และเงื่อนไขการใช้อำนาจในชั้นสืบสวนและสอบสวนให้ชัดเจนไม่คลุมเครือ พร้อมทั้งกำหนดมาตรการคุ้มครองสิทธิของบุคคล ซึ่งอาจนำแนวทางของสหราชอาณาจักร สหรัฐอเมริกา และสาธารณรัฐเกาหลีมาปรับใช้ได้ เช่น เพิ่มขั้นตอนการแจ้งข้อเท็จจริง รวมถึงเปิดโอกาสให้เจ้าของข้อมูลมีสิทธิที่จะตรวจสอบ เป็นต้น

ข้อพิจารณาที่ 1.3 “การเก็บรวบรวมข้อมูลข่าวสารจากผู้ประกอบการภาคเอกชน” ตามกฎหมายต่างประเทศ จะมีหลักเกณฑ์ที่เกี่ยวข้องดังต่อไปนี้

ตารางที่ 7 การเก็บรวบรวมข้อมูลข่าวสารจากภาคเอกชนตามกฎหมายต่างประเทศ

ประเทศ	กรอบการใช้อำนาจ
สหราชอาณาจักร	การขอข้อมูลข่าวสารจากภาคเอกชนถือเป็นการค้นและยึดทั่วไป จึงอยู่ในบังคับที่จะต้องมีหมายค้นหรือคำสั่งศาลเป็นฐานอำนาจ
สหรัฐอเมริกา	อาจไม่ได้รับความคุ้มครองตามบทบัญญัติแก้ไขเพิ่มเติมรัฐธรรมนูญฉบับที่ 4 เพราะหลักการ “The third-party doctrine” ซึ่งวางหลักว่า บุคคลย่อมไม่อาจคาดหมายความเป็นส่วนตัวจากข้อมูลที่ตนให้แก่บุคคลที่สามไปด้วยความสมัครใจ
สาธารณรัฐเกาหลี	จำกัดเฉพาะข้อมูลที่ยืนยันการติดต่อสื่อสารของพลเมืองสาธารณรัฐเกาหลี โดยเป็นการขอความร่วมมือบนพื้นฐานความสมัครใจ ภาคเอกชนจึงมีสิทธิปฏิเสธ นอกจากนี้ หากมีการเปิดเผยข้อมูลตามคำขอของเจ้าหน้าที่รัฐ ผู้ประกอบการจะมีหน้าที่ในการแจ้งข้อเท็จจริงให้เจ้าของข้อมูลทราบอีกด้วย

แตกต่างจากข้อพิจารณาที่ 1.1 และที่ 1.2 การเก็บรวบรวมข้อมูลข่าวสารจากเอกชนในระบบกฎหมายของสามประเทศข้างต้นจะมีพื้นฐานการใช้อำนาจที่แตกต่างกัน โดยสหราชอาณาจักรเห็นว่าการเรียกข้อมูลข่าวสารจากผู้ประกอบการภาคเอกชน ซึ่งเป็นบุคคลที่สาม มีระดับความรุนแรงเทียบเท่าได้กับการค้นและยึดทั่วไป จึงต้องมีคำสั่งหรือหมายจากศาลเป็นฐานการใช้อำนาจ ในขณะที่การเก็บรวบรวมข้อมูลข่าวสารจากผู้ประกอบการภาคเอกชนของสหรัฐอเมริกาและสาธารณรัฐเกาหลีไม่อยู่ในบังคับที่จะต้องได้รับคำสั่งหรือหมายจากศาล เช่นเดียวกับประเทศไทย

อย่างไรก็ตาม การเก็บรวบรวมข้อมูลจากภาคเอกชนดังกล่าวก็เป็นปัจจัยหนึ่งที่ทำให้สหภาพยุโรปประเมินว่าการคุ้มครองข้อมูลส่วนบุคคลของสหรัฐอเมริกามีระดับที่ไม่เพียงพอ เนื่องจากสหรัฐอเมริกาไม่มีมาตรการทางกฎหมายควบคุมตรวจสอบการเรียกเอาข้อมูลจากภาคเอกชนที่ชัดเจน จะเห็นได้จากการที่หน่วยงานบังคับใช้กฎหมายในสหรัฐอเมริกามีการบอกรับสมาชิกซื้อฐานข้อมูลจากภาคเอกชน (Purchase subscriptions to commercial data bases) บริบทแวดล้อมทางกฎหมายของสหรัฐอเมริกาจึงเอื้อให้เจ้าหน้าที่รัฐสามารถเข้าถึงข้อมูลส่วนบุคคลได้อย่างกว้างขวาง[367] โดยเฉพาะเมื่อศาลสหรัฐอเมริกาวางหลัก The third-party doctrine (บุคคลย่อมไม่คาดหมายความเป็นส่วนตัวจากข้อมูลที่ให้แก่บุคคลที่สามไปด้วยความสมัครใจ) บทบัญญัติแก้ไขเพิ่มเติมรัฐธรรมนูญฉบับที่ 4 จึงไม่

[367] European Parliament, "A Comparison between Us and Eu Data Protection Legislation for Law Enforcement."

อาจนำมาปรับใช้เพื่อให้การคุ้มครองในกรณีเช่นว่านี้ได้ เป็นเหตุให้การโอนข้อมูลระหว่างสหรัฐอเมริกาและสหภาพยุโรปไม่อาจกระทำได้อย่างเสรี ด้วยข้อจำกัดการโอนตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลในการแลกเปลี่ยนข้อมูลจึงต้องมีการทำข้อตกลงระหว่างประเทศระดับทวิภาคี

ในทางกลับกัน แม้สาธารณรัฐเกาหลีจะได้รับการรับรองถึงระดับการคุ้มครองข้อมูลที่เพียงพอตามมาตรฐาน GDPR แต่มีข้อสังเกตว่าในคำวินิจฉัยดังกล่าว สาธารณรัฐเกาหลีได้มีการชี้แจงเกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคลจากภาคเอกชน โดยเฉพาะธุรกิจโทรคมนาคมภายใต้ TBA ว่าการขอข้อมูลการติดต่อสื่อสารจากผู้ประกอบการเอกชนจะจำกัดเฉพาะข้อมูลที่ยืนยันการติดต่อสื่อสารของผู้ใช้บริการ (Users) ที่เป็นพลเมืองสาธารณรัฐเกาหลีเท่านั้น จึงไม่มีผลกระทบต่อพลเมืองยุโรป[368] ซึ่งในทรรศนะของผู้เขียน ปัจจัยดังกล่าวน่าจะเป็นสาเหตุสำคัญที่ทำให้การวินิจฉัยถึงระดับการคุ้มครองข้อมูลส่วนบุคคลระหว่างสหรัฐอเมริกากับสาธารณรัฐเกาหลีแตกต่างกันไป เพราะการวินิจฉัยถึงระดับการคุ้มครองที่เพียงพอเป็นการวินิจฉัยเพื่อประกันว่า การโอนข้อมูลระหว่างประเทศจะไม่ทำให้ระดับการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายของสหภาพยุโรปถูกลดทอนไป[369] ดังนั้น เมื่อขอบเขตของการเก็บรวบรวมข้อมูลข่าวสารจากภาคเอกชนในสาธารณรัฐเกาหลีนั้นไม่ครอบคลุมถึงข้อมูลส่วนบุคคลของพลเมืองยุโรป การมีอยู่ของข้อเท็จจริงนี้จึงไม่ลดทอนหลักประกันสิทธิส่วนบุคคลของพลเมืองยุโรป อีกทั้ง เมื่อเปรียบเทียบกับประเทศไทย จะพบว่าสาธารณรัฐเกาหลีมีมาตรการคุ้มครองสิทธิของบุคคลโดยให้ทำการแจ้งไปยังเจ้าของข้อมูล และการให้ข้อมูลนั้นยังอยู่บนพื้นฐานความสมัครใจอีกด้วย

ฉะนั้น หากไม่มีปัจจัยใดเพิ่มเติม ประเทศไทยที่การขอข้อมูลข่าวสารส่วนบุคคลจากผู้ประกอบการภาคเอกชนในชั้นสืบสวนและสอบสวนคดีอาญาไม่มีข้อกำหนดในการใช้อำนาจที่ชัดเจนและเป็นดุลพินิจของเจ้าหน้าที่รัฐฝ่ายเดียว จึงมีความเสี่ยงที่จะถูกประเมินเช่นเดียวกับสหรัฐอเมริกาว่ามีระดับการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอ จนเป็นอุปสรรคในการโอนข้อมูลระหว่างประเทศได้ จึงสมควรกำหนดขอบเขตการเก็บรวบรวมข้อมูลข่าวสารส่วนบุคคลจากผู้ประกอบการภาคเอกชนในชั้นสืบสวนและสอบสวนคดีอาญาในประเทศไทยให้ชัดเจนขึ้น โดยผู้เขียนเห็นว่าเบื้องต้น อาจนำกฎหมายสาธารณรัฐเกาหลีมาเป็นแนวทางได้ โดยเริ่มจากแบ่งระดับข้อมูลที่เก็บรวบรวมจากภาคเอกชนในไทยเพื่อกำหนดเกณฑ์ เงื่อนไข และกระบวนการตรวจสอบการใช้อำนาจ ให้สอดคล้องกับความรุนแรงของผลกระทบที่อาจเกิดขึ้นกับสิทธิส่วนบุคคล

---

[368] 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."

[369] GDPR Article 44; LED Article 35.

ข้อพิจารณาที่ 2 จากการเปรียบเทียบกฎหมายต่างประเทศในข้อพิจารณาที่ 1 อาจกล่าวได้ว่า กฎหมายวิธีพิจารณาความอาญาของประเทศสหราชอาณาจักร สหรัฐอเมริกา และสาธารณรัฐเกาหลี มีมาตรการทางกฎหมายเพื่อป้องกันมิให้การสืบสวนและสอบสวนคดีอาญากระทบกระเทือนต่อสิทธิในข้อมูลส่วนบุคคลที่รัดกุมมากกว่ากฎหมายวิธีพิจารณาความอาญาของไทยอยู่หลายด้าน แต่ถึงกระนั้น การให้ความคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาของประเทศต่าง ๆ เหล่านี้ก็ยังคงอาศัยกฎหมายคุ้มครองข้อมูลส่วนบุคคลอยู่ เพราะกฎหมายวิธีพิจารณาความอาญาและกฎหมายคุ้มครองข้อมูลส่วนบุคคลมีเจตนารมณ์และสาระสำคัญที่แตกต่างกัน ตามที่ผู้เขียนได้นำเสนอไปข้างต้น ลำพังกฎหมายวิธีพิจารณาความอาญาจึงไม่อาจคุ้มครองข้อมูลส่วนบุคคลได้อย่างครอบคลุม แต่จำเป็นต้องมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นมาตรการควบคู่กันไปด้วย ซึ่งจะได้วิเคราะห์โดยละเอียดในหัวข้อที่ 5.2 ต่อไป

5.2 กฎหมายคุ้มครองข้อมูลส่วนบุคคล

เมื่อสิทธิในข้อมูลส่วนบุคคลมิใช่สิทธิเด็ดขาดและอาจถูกจำกัดได้เพื่อประโยชน์ในการป้องกันและปราบปรามอาชญากรรม กฎหมายคุ้มครองข้อมูลส่วนบุคคลในหลายประเทศ รวมถึงประเทศไทย จึงมักกำหนดข้อยกเว้นหรือข้อจำกัดการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา อย่างไรก็ตาม สิทธิในข้อมูลส่วนบุคคลก็เป็นหนึ่งในสิทธิมนุษยชนขั้นพื้นฐาน การจำกัดสิทธิดังกล่าวจึงควรกระทำให้น้อยที่สุดเท่าที่มีความจำเป็น

ด้วยเหตุนี้ แม้การดำเนินงานในชั้นสืบสวนและสอบสวนคดีอาญาจะไม่อยู่ภายใต้ GDPR ของสหภาพยุโรป แต่การสืบสวนและสอบสวนคดีอาญาก็อยู่ในบังคับ LED ซึ่งเป็นกฎเกณฑ์เฉพาะสำหรับการประมวลผลข้อมูลที่ดำเนินการโดยหน่วยงานที่มีอำนาจหน้าที่ป้องกัน สืบสวน ตรวจจับ ดำเนินคดี ลงโทษทางอาญา และการป้องกันภัยคุกคามต่อความมั่นคงปลอดภัยสาธารณะแทน[370] ซึ่งสาระสำคัญของ LED อาจจำแนกออกเป็นสี่ส่วนใหญ่ กล่าวคือ

(ก.) ขอบเขตของข้อมูลส่วนบุคคลที่ได้รับความคุ้มครอง

“ข้อมูลส่วนบุคคล” (Personal data) หมายถึง ข้อมูลใด ๆ เกี่ยวกับบุคคล ซึ่งระบุหรือทำให้ระบุถึงบุคคลธรรมดาผู้เป็นเจ้าของข้อมูลได้ ไม่ว่าโดยตรงหรือโดยอ้อมก็ตาม โดยไม่จำกัดสัญชาติหรือถิ่นที่อยู่ของบุคคลธรรมดา ทว่าไม่รวมถึงข้อมูลผู้ถึงแก่กรรมแต่อย่างใด[371]

---

[370] LED, Recital 11; GDPR, Recital 19.

[371] LED, Article 3 (1).

(ข.) หลักการประมวลผลข้อมูลส่วนบุคคล

การประมวลผลข้อมูลส่วนบุคคลใน LED ประกอบด้วยหลักการพื้นฐานเจ็ดประการ[372] คือ

1.) หลักความชอบด้วยกฎหมายและเป็นธรรม (Lawfulness and Fairness)
การประมวลผลข้อมูลส่วนบุคคลจะต้องมีฐานทางกฎหมาย คือมีกฎหมายบัญญัติรองรับและต้องเป็นการดำเนินการที่จำเป็นในการบังคับใช้กฎหมายอาญา อีกทั้งหากข้อมูลที่ประมวลผลเป็นข้อมูลอ่อนไหวจะต้องระมัดระวังไม่ให้เกิดผลกระทบอันไม่พึงประสงค์ต่อเจ้าของข้อมูลด้วย

2.) หลักการจำกัดวัตถุประสงค์ (Purpose Limitation)
การประมวลผลข้อมูลส่วนบุคคลจะต้องมีวัตถุประสงค์อันชัดแจ้งเฉพาะเจาะจงและห้ามมิให้ประมวลผลข้อมูลโดยไม่สอดคล้องกับวัตถุประสงค์ที่กำหนดไว้

3.) หลักการใช้ข้อมูลให้น้อยที่สุด (Data Minimisation)
การประมวลผลข้อมูลส่วนบุคคลจะต้องจำกัดให้น้อยที่สุดเท่าที่เพียงพอ จำเป็นและเกี่ยวข้องสัมพันธ์กับการกระทำความผิดที่สืบสวนและสอบสวน

4.) หลักความถูกต้องสมบูรณ์ (Accuracy)
ข้อมูลส่วนบุคคลจะต้องได้รับการรักษาให้ถูกต้อง สมบูรณ์ และเป็นปัจจุบัน โดยให้แยกแยะประเภทของข้อมูลส่วนบุคคลออกเป็นสองรูปแบบ คือ แยกแยะตามเจ้าของข้อมูลออกเป็นผู้ต้องสงสัย ผู้ต้องคำพิพากษาว่ากระทำผิด ผู้เสียหาย หรือผู้มีส่วนเกี่ยวข้อง รวมถึงแยกแยะคุณภาพข้อมูลระหว่างข้อเท็จจริงกับข้อคิดเห็น นอกจากนี้ ต้องจัดให้มีการบันทึกข้อมูลจราจร (Logs) อีกด้วย

5.) หลักการจำกัดการเก็บรักษา (Storage Limitation)
ข้อมูลส่วนบุคคลจะต้องถูกเก็บรักษาในรูปแบบที่ระบุตัวตนของเจ้าของข้อมูลได้ไม่นานเกินกว่าที่จำเป็นเพื่อบรรลุวัตถุประสงค์ในการสืบสวนและสอบสวน

6.) หลักความสมบูรณ์และเป็นความลับ (Integrity and Confidentiality)
การประมวลผลข้อมูลส่วนบุคคลต้องมีมาตรการที่ประกันความมั่นคงปลอดภัย

7.) หลักความรับผิดชอบ (Accountability)
ผู้ควบคุมข้อมูลส่วนบุคคลต้องรับผิดชอบให้การดำเนินการสอดคล้องกับหลักการคุ้มครองข้อมูลส่วนบุคคล ซึ่งรวมถึงการกำกับผู้ประมวลผลข้อมูลส่วนบุคคล และการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

---

[372] LED, Article 4 (1).

(ข.) สิทธิของเจ้าของข้อมูลส่วนบุคคล

โดยหลัก ผู้ควบคุมข้อมูลส่วนบุคคลจะมีหน้าที่ตอบสนองการใช้สิทธิของเจ้าของข้อมูล เว้นแต่การใช้สิทธิดังกล่าวไม่สมเหตุสมผล ฟุ่มเฟือยเกินความจำเป็น หรือมีเหตุการปฏิเสธตามกฎหมาย ทั้งนี้ LED ได้บัญญัติรับรองสิทธิของเจ้าของข้อมูลส่วนบุคคลสามประการ[373] ได้แก่

1.) สิทธิที่จะได้รับแจ้งข้อมูล (Right to be informed)
2.) สิทธิที่จะเข้าถึงข้อมูล (Right to access)
3.) สิทธิที่จะแก้ไข ลบ หรือจำกัดการประมวลผลข้อมูล (Right to rectification or erasure of personal data and restriction of processing)

อย่างไรก็ดี การใช้สิทธิของเจ้าของข้อมูลจะต้องไม่กระทบการสืบสวนและสอบสวนคดีอาญาหน่วยงานผู้มีอำนาจหน้าที่จึงอาจปฏิเสธที่จะให้ข้อมูลตามคำขอของเจ้าของข้อมูล ซึ่งรวมถึงเหตุผลในการปฏิเสธการใช้สิทธิของเจ้าของข้อมูลได้ หากเป็นไปเพื่อประโยชน์ในการป้องปรามอาชญากรรม แต่เจ้าของข้อมูลก็มีสิทธิที่จะร้องเรียนต่อหน่วยงานกำกับดูแล เพื่อให้ตรวจสอบความชอบด้วยกฎหมายของการประมวลผลข้อมูล โดยถือว่าเป็นการใช้สิทธิโดยอ้อมของเจ้าของข้อมูลส่วนบุคคล[374]

(ค.) กลไกการบังคับใช้

สำหรับกลไกการบังคับใช้ LED จะอยู่ในรูปแบบหน่วยงานกำกับดูแลอิสระ ซึ่งอาจเป็นองค์กรเดียวกับหน่วยงานที่กำกับดูแล GDPR[375] อีกทั้ง LED ได้บัญญัติเกณฑ์การโอนข้อมูลไปยังต่างประเทศโดยกำหนดให้ประเทศปลายทางจะต้องมีระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอตามมาตรฐานและจะต้องปรากฏความจำเป็นเพื่อการบังคับใช้กฎหมายอาญา[376] นอกจากนี้ เพื่อประกันการบังคับใช้สหภาพยุโรปเห็นควรให้กำหนดความรับผิดและโทษสำหรับการฝ่าฝืนหลักเกณฑ์ LED อีกด้วย[377]

อนึ่ง เมื่อเปรียบเทียบกับ GDPR พบว่า LED มีข้อแตกต่างจาก GDPR สรุปได้โดยสังเขปดังนี้

---

[373] LED, CHAPTER III Rights of the data subject.

[374] Drechsler, L., "Comparing Led and Gdpr Adequacy: One Standard Two Systems," Global Privacy Law Review; Salami, E., "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."

[375] LED, Article 41-42.

[376] LED, Article 35.

[377] LED, Article 57 and Recital 89.

ตารางที่ 8 ความแตกต่างระหว่าง LED กับ GDPR

ประเทศ	ความแตกต่างระหว่าง LED กับ GDPR
ขอบเขตข้อมูลส่วนบุคคลที่ได้รับการคุ้มครอง	LED นิยามข้อมูลส่วนบุคคลเช่นเดียวกับ GDPR แต่จะไม่มีการขยายขอบเขตการคุ้มครองเชิงพื้นที่ไปนอกสหภาพยุโรป
หลักการประมวลผลข้อมูลส่วนบุคคล	LED ไม่รับรองหลักความโปร่งใสให้เป็นหลักการพื้นฐาน และรับรองฐานการประมวลผลข้อมูลเฉพาะกรณีที่มีกฎหมายให้อำนาจ และการประมวลผลนั้นจำเป็นในการบังคับใช้กฎหมาย
สิทธิเจ้าของข้อมูลส่วนบุคคล	LED รับรองสิทธิเจ้าของข้อมูลส่วนบุคคลอยู่สามประการ และจำกัดการใช้สิทธิของเจ้าของข้อมูล หากเป็นอุปสรรคต่อการสืบสวนและสอบสวน โดยให้เจ้าของข้อมูลใช้สิทธิทางอ้อมผ่านหน่วยงานกำกับดูแลแทน
กลไกการบังคับใช้	หน่วยงานกำกับดูแลที่เป็นองค์กรอิสระ ซึ่งอาจเป็นหน่วยงานเดียวกับ GDPR แต่การใช้อำนาจนั้นจะต้องไม่กระทบหลักความเป็นอิสระของศาล

ฉะนั้น ข้อแตกต่างสำคัญที่สุดระหว่าง LED กับ GDPR คือการที่ LED จำเป็นต้องรักษาสมดุลระหว่างการคุ้มครองสิทธิความส่วนตัวในข้อมูลของบุคคลกับการป้องกันและปรามอาชญากรรมในชั้นสืบสวนและสอบสวนคดีอาญา มาตรฐานและหลักประกันสิทธิของเจ้าของข้อมูลส่วนบุคคลภายใต้ LED จึงถูกจำกัดและลดทอนจาก GDPR ทำให้เกณฑ์การคุ้มครองข้อมูลส่วนบุคคลใน LED มีลักษณะเฉพาะแตกต่างจากหลักเกณฑ์ทั่วไป เพราะเป็นกฎเกณฑ์ที่ถูกออกแบบโดยคำนึงถึงธรรมชาติของการสืบสวนและสอบสวนคดีอาญาเป็นสำคัญ

5.2.1 บทวิเคราะห์กฎหมายไทย

แม้ว่าในปัจจุบัน ประเทศไทยจะมีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นกฎหมายกลางในการคุ้มครองข้อมูลส่วนบุคคล แต่หากพิจารณาขอบเขตการบังคับใช้พระราชบัญญัติดังกล่าว จะพบว่าการสืบสวนและสอบสวนคดีอาญาได้รับยกเว้นไม่ให้นำพระราชบัญญัตินี้มาใช้บังคับตามมาตรา 4 (2) และ (5) เว้นแต่ในส่วนที่เกี่ยวข้องกับมาตรการรักษาความมั่นคงปลอดภัย การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาของประเทศไทยจึงยังคงต้องอาศัยหมวด 3 ว่าด้วยข้อมูลข่าวสารส่วนบุคคล ตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ทว่าจากการศึกษากลับพบว่าบทบัญญัติดังกล่าวไม่เพียงพอที่จะคุ้มครองข้อมูลส่วนบุคคลได้อย่างเหมาะสม กล่าวคือ

ตารางที่ 9 ข้อจำกัดของหมวด 3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

ลักษณะของข้อจำกัด	รายละเอียด
ข้อจำกัดที่ 1 ขอบเขตข้อมูลข่าวสารส่วนบุคคล	“ข้อมูลข่าวสารส่วนบุคคล” ตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มีนิยามที่ไม่สอดคล้องกับ “ข้อมูลส่วนบุคคล” ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ทำให้เกิดความสับสนในการบังคับใช้กฎหมาย
ข้อจำกัดที่ 2 เกณฑ์การเก็บรวบรวม ใช้ และเปิดเผย	หมวด 3 ในพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 เป็นเพียงหลักการโดยกว้าง ขาดรายละเอียดปฏิบัติที่ชัดเจน เช่น - ไม่มีบทบัญญัติเกี่ยวกับฐานทางกฎหมาย และไม่ได้กำหนดหน้าที่บันทึกรายการ เพื่อให้สามารถตรวจสอบ - ไม่มีเกณฑ์การคุ้มครอง “ข้อมูลอ่อนไหว” - ไม่มีเกณฑ์เกี่ยวกับ “ความยินยอม” ที่ชัดเจน - ไม่มีบทบัญญัติห้ามมิให้ประมวลผลข้อมูลส่วนบุคคลแตกต่างไปจากวัตถุประสงค์ที่แจ้งต่อเจ้าของข้อมูลไว้ก่อนหรือขณะเก็บรวบรวม - ไม่มีบทบัญญัติให้ลบหรือทำลายข้อมูลส่วนบุคคล เมื่อพ้นระยะเวลาเก็บรักษา - ไม่มีเกณฑ์การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ - ไม่ได้มีบทบัญญัติให้ผู้มีหน้าที่รับผิดชอบเป็นผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล และงไม่ได้กำหนดให้มีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
ข้อจำกัดที่ 3 การรับรองสิทธิเจ้าของข้อมูลส่วนบุคคล	3.1 ไม่ได้รับรองสิทธิเจ้าของข้อมูลส่วนบุคคลอย่างครอบคลุม 3.2 ไม่มีเหตุตามกฎหมายในการปฏิบัติไม่ดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลที่ชัดเจน
ข้อจำกัดที่ 4 การบังคับใช้กฎหมาย	4.1 โครงสร้างและองค์ประกอบหน่วยงานกำกับดูแล มีที่มาจากฝ่ายราชการ จึงขาดความคล่องตัวและความเป็นอิสระ นอกจากนี้หน่วยงานกำกับดูแลยังไม่มีอำนาจสืบสวนสอบสวนอีกด้วย 4.2 ไม่มีบทกำหนดความผิดและโทษ ในกรณีที่มีการฝ่าฝืนหรือไม่ปฏิบัติตามเกณฑ์การคุ้มครองข้อมูลข่าวสารส่วนบุคคล

ข้อวิเคราะห์ที่ 1 บทยกเว้นในมาตรา 4 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีผลเป็นการยกเว้นสืบสวนและสอบสวนคดีอาญาทั้งกิจการไม่อยู่ภายใต้บังคับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เว้นแต่ในส่วนของการรักษาความมั่นคงปลอดภัยข้อมูล ซึ่งต้องเป็นไปตามมาตรฐานประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ทั้งที่ตามความเป็นจริง การสืบสวนและสอบสวนคดีอาญามีการใช้มาตรการต่าง ๆ ซึ่งอาจส่งผลกระทบต่อสิทธิในข้อมูลส่วนบุคคลจำนวนมาก

ด้วยเหตุนี้ จึงมีความเห็นว่าบทยกเว้นทั่วไปในลักษณะนี้มีขอบเขตที่กว้างขวางเกินกว่าจำเป็น ไม่สอดคล้องกับหลักการสากลและรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ซึ่งวางหลักให้การตรากฎหมายจำกัดสิทธิในข้อมูลส่วนบุคคลพึงกระทำเท่าที่จำเป็น เพื่อประโยชน์สาธารณะเท่านั้น โดยเฉพาะอย่างยิ่ง เมื่อพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีฐานะเป็นกฎหมายกลางว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย จึงควรมุ่งเน้นการคุ้มครองสิทธิในข้อมูลส่วนบุคคลมากกว่าจำกัดสิทธิเสียเอง เพราะหากมีความจำเป็น ก็อาจบัญญัติบทยกเว้นเป็นรายกรณีได้ตามความเหมาะสม ดังจะเห็นได้จากมาตรา 4 วรรคสอง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เปิดช่องให้การยกเว้นไม่ให้นำพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ไม่ว่าทั้งหมดหรือแต่บางส่วนมาใช้บังคับแก่ผู้ควบคุมข้อมูลส่วนบุคคลในลักษณะใด กิจการใด หรือหน่วยงานใดทำนองเดียวกับผู้ควบคุมข้อมูลส่วนบุคคลที่ได้รับยกเว้นตามมาตรา 4 วรรคหนึ่ง หรือเพื่อประโยชน์สาธารณะให้สามารถตราเป็นพระราชกฤษฎีกาได้

ข้อวิเคราะห์ที่ 2 แม้การสืบสวนและสอบสวนคดีอาญาของไทยจะอยู่ภายใต้เกณฑ์การคุ้มครองข้อมูลข่าวสารส่วนบุคคลตามหมวด 3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 แต่โดยที่หมวด 3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มีบทบัญญัติอยู่เพียง 5 มาตรา อีกทั้งได้รับการยกร่างตั้งแต่ในปี พ.ศ. 2540 ทำให้การคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติดังกล่าวมีข้อจำกัดตามตารางที่ 8 และไม่ประสบผลสำเร็จดังที่ควรจะเป็น จะเห็นได้จากการที่สถานีตำรวจเพียงไม่กี่แห่งที่ดำเนินการพิมพ์รายการตามมาตรา 23 (3) ลงราชกิจจานุเบกษา โดยไม่มีการแก้ไขปรับปรุงรายการตั้งแต่ในปี พ.ศ. 2547 สอดคล้องกับที่ผู้ช่วยศาสตราจารย์ ดร. นคร เสรีรักษ์ ได้อ้างอิงถึงข้อมูลการสำรวจของสถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์ เมื่อปี พ.ศ. 2547 ซึ่งพบว่ามีหน่วยงานจำนวนร้อยละ 50 แจ้งว่าไม่ได้ดำเนินการจัดระบบข้อมูลข่าวสารส่วนบุคคลให้แล้วเสร็จ[378]

---

[378] นคร เสรีรักษ์, ความเป็นส่วนตัว: ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย, หน้า 259.

เมื่อหมวด 3 ของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ไม่อาจนำมาบังคับใช้ได้อย่างมีประสิทธิภาพ ผู้เขียนจึงมีความเห็นว่าพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 จึงมิใช่มาตรการทางกฎหมายที่เหมาะสมในการคุ้มครองข้อมูลส่วนบุคคลอีกต่อไป โดยเฉพาะอย่างยิ่งเมื่อพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีผลใช้บังคับแล้ว จึงไม่สมควรปล่อยให้การสืบสวนและสอบสวนคดีอาญาอยู่ภายใต้หมวด 3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มิฉะนั้น การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาของไทยก็จะมีมาตรฐานที่ต่ำกว่ากิจการประเภทอื่นที่ปัจจุบันอยู่ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

5.2.2 บทเปรียบเทียบกฎหมายต่างประเทศ

เมื่อเปรียบเทียบกับกฎหมายต่างประเทศในบทที่ 4 กล่าวคือ สหราชอาณาจักร สหรัฐอเมริกา และสาธารณรัฐเกาหลี พบว่ามีข้อควรพิจารณาดังต่อไปนี้

ข้อพิจารณาที่ 1 แม้เป็นที่ยอมรับกันโดยทั่วไปว่าการคุ้มครองข้อมูลส่วนบุคคลอาจถูกยกเว้นหรือจำกัดได้ในชั้นสืบสวนและสอบสวนคดีอาญา แต่จากการศึกษากฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักร สหรัฐอเมริกา รวมถึงสาธารณรัฐเกาหลี กลับพบว่าไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศใดที่กำหนดบทยกเว้นทั่วไป ในลักษณะมาตรา 4 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การสืบสวนและสอบสวนคดีอาญาของประเทศต่าง ๆ เหล่านี้จึงยังคงอยู่ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยมีบทบัญญัติกฎหมายที่เกี่ยวข้องดังนี้

ตารางที่ 10 กฎหมายคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนของต่างประเทศ

ประเทศ	กฎหมายคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา
สหราชอาณาจักร	การสืบสวนและสอบสวนคดีอาญาอยู่ภายใต้ PART 3: Law Enforcement Processing ของ The UK DPA ซึ่งเป็นกฎเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลจากการบังคับใช้กฎหมายอาญาเป็นการเฉพาะ ตามแนวทาง LED ของสหภาพยุโรป
สหรัฐอเมริกา	กฎหมายคุ้มครองข้อมูลส่วนบุคคลอยู่ในรูปแบบกฎหมายเฉพาะเรื่องเฉพาะกรณี ซึ่งสำหรับหน่วยงานระดับสหพันธรัฐ การสืบสวนและสอบสวนคดีอาญาจะอยู่ภายใต้ The Privacy Act of 1974 โดยที่ไม่มีกฎเกณฑ์เฉพาะสำหรับการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา แต่จะใช้การกำหนดข้อยกเว้นเป็นรายกรณี
สาธารณรัฐเกาหลี	การสืบสวนและสอบสวนคดีอาญาอยู่ภายใต้ South Korea's PIPA โดยที่ไม่มีกฎเกณฑ์เฉพาะสำหรับการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา แต่จะใช้การกำหนดข้อยกเว้นเป็นรายกรณี

จากตารางที่ 10 จะเห็นได้ว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศต่าง ๆ ข้างต้นไม่ได้ยกเว้นให้การสืบสวนและสอบสวนคดีอาญาโดยเด็ดขาด แต่เพื่อไม่ให้การคุ้มครองข้อมูลส่วนบุคคลเป็นอุปสรรคต่อการป้องกันและปราบปรามอาชญากรรม ทุกประเทศจึงพยายามออกแบบให้การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญามีกฎเกณฑ์ยืดหยุ่นกว่ากิจการทั่วไป โดยอาจแบ่งลักษณะของกฎเกณฑ์ได้สองรูปแบบใหญ่ด้วยกัน ได้แก่

1.) <u>การบัญญัติเป็นหลักเกณฑ์เฉพาะ</u>
โดยมีตัวอย่างคือสหราชอาณาจักรที่แยกกฎเกณฑ์สำหรับการบังคับใช้กฎหมายออกมาเป็นหมวดเฉพาะ (PART 3: Law Enforcement Processing)

2.) <u>การกำหนดข้อยกเว้นรายกรณี โดยไม่มีหลักเกณฑ์เฉพาะ</u>
จะเห็นได้จากสหรัฐอเมริกาและสาธารณรัฐเกาหลีที่การสืบสวนและสอบสวนยังอยู่ภายใต้กฎเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลทั่วไป เพียงแต่จะมีการกำหนดข้อยกเว้นเป็นรายมาตราตามความเหมาะสม

สิ่งเหล่านี้สะท้อนให้เห็นว่า ไม่มีความจำเป็นที่การสืบสวนและสอบสวนคดีอาญาจะต้องได้รับหารยกเว้นหรือไม่นำหลักการคุ้มครองข้อมูลส่วนบุคคลมาใช้บังคับโดยสิ้นเชิง เพราะหากมีความจำเป็นกฎหมายก็สามารถบัญญัติหลักเกณฑ์เฉพาะหรือข้อยกเว้นรายกรณีได้ ประเทศไทยจึงควรพิจารณานำเอาการสืบสวนและสอบสวนคดีอาญากลับมาอยู่ภายใต้หลักการคุ้มครองข้อมูลส่วนบุคคล เช่นเดียวกับการดำเนินงานประเภทอื่น เพื่อสร้างหลักประกันสิทธิในข้อมูลส่วนบุคคลของประชาชนในชั้นสืบสวนและสอบสวนคดีอาญา โดยอาจกำหนดเป็นหลักเกณฑ์เฉพาะตามที่ปรากฏความจำเป็น

ข้อพิจารณาที่ 2 การที่ประเทศไทยจะกำหนดให้การสืบสวนและสอบสวนคดีอาญาอยู่ภายใต้หลักการคุ้มครองข้อมูลส่วนบุคคลตามแนวทางประเทศต่าง ๆ ข้างต้น จำเป็นที่จะต้องพิจารณาต่อไปว่าเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญานั้นควรเป็นเช่นไร จึงจะรักษาสมดุลระหว่างการป้องกันและปราบปรามอาชญากรรมกับการคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสม โดยมีข้อควรพิจารณาสี่ประการดังนี้

ข้อพิจารณาที่ 2.1 โดยทั่วไป กฎหมายคุ้มครองข้อมูลส่วนบุคคลต่างประเทศจะไม่ได้กำหนดหลักเกณฑ์เฉพาะสำหรับ “ขอบเขตของข้อมูลส่วนบุคคล” ในชั้นสืบสวนและสอบสวนคดีอาญา ข้อมูลส่วนบุคคลที่ได้รับความคุ้มครองในชั้นสืบสวนและสอบสวนจึงมีนิยามเช่นเดียวกับกิจการทั่ว ๆ ไป ตามที่ปรากฏในตารางที่ 11 กล่าวคือ

ตารางที่ 11 ขอบเขตของข้อมูลส่วนบุคคลตามกฎหมายต่างประเทศ

ประเทศ	นิยามและขอบเขตของข้อมูลส่วนบุคคลที่ได้รับการคุ้มครอง
สหราชอาณาจักร	The UK DPA นิยามข้อมูลส่วนบุคคล (Personal data) หมายถึงข้อมูลใด ๆ เกี่ยวกับบุคคล ซึ่งระบุหรือทำให้ระบุถึงบุคคลธรรมดาที่มีชีวิตอยู่ ไม่ว่าโดยตรงหรือโดยอ้อม
สหรัฐอเมริกา	The Privacy Act of 1974 นิยามว่า บันทึกข้อมูล (Record) หมายถึงชุดหรือกลุ่มข้อมูลเกี่ยวกับบุคคล ซึ่งอยู่ในความครอบครองของหน่วยงานระดับสหพันธรัฐ และต้องเป็นบุคคลสัญชาติอเมริกันหรือมีถิ่นที่อยู่ในสหรัฐอเมริกา
สาธารณรัฐเกาหลี	South Korea's PIPA นิยามให้ข้อมูลส่วนบุคคล (Personal Information) หมายถึงข้อมูลใด ๆ เกี่ยวกับบุคคลที่มีชีวิตอยู่ ไม่ว่าระบุถึงตัวบุคคลโดยตรง หรือนำไปประกอบกับข้อมูลอื่นเพื่อระบุตัวบุคคล และให้หมายความรวมถึงข้อมูลแฝง

จะเห็นได้ว่า นิยามและขอบเขตข้อมูลส่วนบุคคลตามกฎหมายต่างประเทศส่วนใหญ่เป็นไปในทิศทางเดียวกับนิยามตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป คือมุ่งคุ้มครองข้อมูลบ่งชี้ถึงตัวบุคคลธรรมดาที่มีชีวิตอยู่ แต่มีข้อสังเกตว่าขอบเขตของข้อมูลที่ได้รับการคุ้มครองของสหรัฐอเมริกาจะมีความแตกต่างออกไป กล่าวคือ The Privacy Act of 1974 จะคุ้มครองบันทึกข้อมูลในความครอบครองของหน่วยงานระดับสหพันธรัฐเท่านั้น เนื่องจากสหรัฐอเมริกาไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เป็นกฎหมายกลาง และ The Privacy Act of 1974 จะจำกัดความคุ้มครองเฉพาะบุคคลสัญชาติอเมริกันหรือมีถิ่นที่อยู่ในสหรัฐอเมริกา[379] อย่างไรก็ดี การที่ The Privacy Act of 1974 จำกัดความคุ้มครองเฉพาะพลเมืองสหรัฐอเมริกา ก็เป็นเหตุให้สหภาพยุโรปประเมินว่าระบบกฎหมายของสหรัฐอเมริกาไม่อาจคุ้มครองข้อมูลส่วนบุคคลของพลเมืองยุโรปจากหน่วยงานบังคับใช้กฎหมายได้อย่างเหมาะสมเพียงพอ และเพื่อแก้ไขปัญหาดังกล่าว สหรัฐอเมริกาและสหภาพยุโรปจึงทำความตกลง Umbrella Agreement โดยให้พลเมืองยุโรปสามารถใช้สิทธิใน The Privacy Act of 1974 เช่นเดียวกันกับพลเมืองของสหรัฐอเมริกา[380]

เมื่อเปรียบเทียบกับประเทศไทย ขอบเขตข้อมูลส่วนบุคคลที่ได้รับความคุ้มครองตามกฎหมายไทยอาจพิจารณาแยกได้เป็นสองส่วนตามกฎหมายแต่ละฉบับ อันได้แก่

---

[379] ประสิทธิ์ ปิวาวัฒนพานิช, "กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกาและประเทศออสเตรเลีย," วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์

[380] คณาธิป ทองรวีวงศ์, "การปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน."

1.) <u>ขอบเขตตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540</u>
คุ้มครองข้อมูลข่าวสารส่วนบุคคล ซึ่งเป็นข้อมูลที่มีข้อเท็จจริงที่เป็นสิ่งเฉพาะตัว และมีสิ่งชี้ตัวบุคคล ซึ่งรวมถึงข้อมูลผู้ถึงแก่กรรม แต่จำกัดความคุ้มครองเฉพาะบุคคลสัญชาติไทยหรือมีถิ่นที่อยู่ในประเทศไทย

2.) <u>ขอบเขตตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562</u>
ข้อมูลที่ทำให้สามารถระบุตัวบุคคลได้ ไม่ว่าโดยตรงหรือโดยอ้อม โดยไม่จำต้องเป็นสิ่งเฉพาะตัวและไม่จำกัดสัญชาติหรือถิ่นที่อยู่ของบุคคล แต่จะไม่รวมข้อมูลของผู้ถึงแก่กรรม ทั้งนี้ เจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในประเทศไทยอาจได้รับการคุ้มครองจากการประมวลผลข้อมูลส่วนบุคคลที่เกิดขึ้นนอกราชอาณาจักรได้ หากการประมวลผลข้อมูลนั้นมีลักษณะตามที่กฎหมายบัญญัติ

ด้วยเหตุนี้ จึงอาจสรุปได้ว่าขอบเขตของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จึงสอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปและมากกว่าพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ซึ่งปัจจุบัน ประเทศไทยก็มีการเสนอให้แก้ไขบทนิยามข้อมูลข่าวสารส่วนบุคคลตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จึงเห็นสมควรกำหนดขอบเขตของข้อมูลส่วนบุคคลที่ได้รับความคุ้มครองในชั้นสืบสวนและสอบสวนคดีอาญาของประเทศไทยตามนิยามมาตรา 6 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ทว่าในส่วนของการขยายขอบเขตการคุ้มครองข้อมูลส่วนบุคคลของเจ้าของข้อมูลซึ่งอยู่ในประเทศไทยจากการประมวลผลข้อมูลส่วนบุคคลที่เกิดขึ้นนอกประเทศ ตามมาตรา 5 วรรคสอง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ผู้เขียนเห็นควรยกเว้นให้การสืบสวนและสอบสวนคดีอาญาไม่นำหลักการขยายขอบเขตการบังคับใช้เชิงพื้นที่ดังกล่าว ตาม LED และ The UK DPA เนื่องจากการสืบสวนและสอบสวนคดีอาญาเกี่ยวพันกับอำนาจอธิปไตยของแต่ละรัฐ จึงไม่อาจบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลแก่การสืบสวนและสอบสวนคดีอาญานอกราชอาณาจักรได้

ข้อพิจารณาที่ 2.2 สำหรับ “เกณฑ์การคุ้มครองในชั้นสืบสวนและสอบสวนคดีอาญา” ตามกฎหมายต่างประเทศ พบว่าในแต่ละประเทศมีพื้นฐานที่คล้ายคลึงกัน เพียงแต่มีความแตกต่างกันในรายละเอียดเท่านั้น โดยประกอบไปด้วยสาระสำคัญสองส่วน ได้แก่ (1) ฐานทางกฎหมาย กำหนดว่าการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนกระทำได้ในสถานการณ์ใด และ (2) หลักการประมวลผลข้อมูลส่วนบุคคล กำหนดว่าการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลจะต้องดำเนินการเช่นไร จึงไม่กระทบต่อสิทธิส่วนบุคคลเกินกว่าสมควร ซึ่งในชั้นสืบสวนและสอบสวนคดีอาญาจะต้องคำนึงประโยชน์สาธารณะที่เกี่ยวข้องประกอบด้วย ซึ่งอาจสรุปได้โดยสังเขปดังนี้

ตารางที่ 12 เกณฑ์การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนของต่างประเทศ

ประเทศ	เกณฑ์การคุ้มครองข้อมูลส่วนบุคคล
สหราชอาณาจักร	PART 3: Law Enforcement Processing ของ The UK DPA มีกฎเกณฑ์เช่นเดียวกับ LED ของสหภาพยุโรป เว้นแต่การยอมรับให้ “ความยินยอม” เป็นฐานการประมวลผลข้อมูลส่วนบุคคลเพื่อการบังคับใช้กฎหมายอาญา
สหรัฐอเมริกา	The Privacy Act of 1974 มีการบัญญัติหลักเกณฑ์ที่เกี่ยวข้องดังนี้ 1. กำหนดเกณฑ์การจัดเก็บบันทึกข้อมูลให้เป็นไปตามหลักการคุ้มครองข้อมูลส่วนบุคคล 2. ห้ามมิให้เปิดเผยข้อมูล เว้นแต่ได้รับคำร้องขอหรือความยินยอมจากเจ้าของข้อมูล อย่างไรก็ตาม หน่วยงานบังคับใช้กฎหมายอาญามักได้รับยกเว้นให้สามารถเก็บรวบรวมและเปิดเผยบันทึกข้อมูลได้มากกว่ากิจการประเภทอื่น และได้รับยกเว้นให้สามารถกำหนดหลักเกณฑ์หรือข้อยกเว้นสำหรับการเข้าถึงบันทึกข้อมูลได้เพิ่มเติมอีกด้วย
สาธารณรัฐเกาหลี	South Korea’s PIPA กำหนดให้การประมวลผลข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาต้องมีบทบัญญัติกฎหมายเป็นฐานอำนาจ พร้อมบัญญัติหลักเกณฑ์การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ดังต่อไปนี้ 1. หลักการทั่วไปในการประมวลผลข้อมูลส่วนบุคคลแปดประการ 2. หน้าที่ของหน่วยงานรัฐในการคุ้มครองข้อมูลส่วนบุคคล ทั้งนี้ การสืบสวนและสอบสวนคดีอาญาอาจได้รับการยกเว้นจากข้อกำหนดบางประการในกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นรายบทบัญญัติ

จากตารางที่ 12 ผู้เขียนตั้งข้อสังเกตว่าโดยส่วนใหญ่ กฎหมายต่างประเทศยอมรับให้นำเอาเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลตามมาตรฐานสากลมาใช้บังคับแก่การสืบสวนและสอบสวนคดีอาญาเกือบทั้งสิ้น โดยกำหนดข้อยกเว้นเฉพาะในบางประเด็นเท่านั้น กล่าวคือ

1.) <u>ฐานทางกฎหมายสำหรับการสืบสวนและสอบสวนคดีอาญา</u>

การสืบสวนและสอบสวนได้รับการยกเว้นให้สามารถเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลได้ โดยไม่จำต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หากมีกฎหมายให้อำนาจ เว้นแต่ในบางบริบท กฎหมายต่างประเทศก็ยอมรับให้ใช้ความยินยอมเป็นฐานทางกฎหมายในชั้นสืบสวนและสอบสวนคดีอาญาได้ จึงแตกต่างจาก LED ของสหภาพยุโรปที่ไม่บัญญัติรับรองให้ความยินยอมเป็นฐานการประมวลผลข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา เนื่องจากเห็นว่าในชั้นสืบสวนและสอบสวนคดีอาญา เจ้าของข้อมูลอาจไม่ได้มีอิสระในการความยินยอมอย่างแท้จริง

2.) <u>หลักการประมวลผลข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา</u>

โดยหลัก การสืบสวนและสอบสวนคดีอาญายังคงอยู่ภายใต้หลักการประมวลผลข้อมูลส่วนบุคคลอย่างเดียวกันกับกิจการประเภทอื่น ยกเว้นหลักความโปร่งใสที่การสืบสวนและสอบสวนคดีอาญาไม่อาจอยู่ในบังคับได้โดยบริบูรณ์ เพราะหลักดังกล่าวเรียกร้องให้มีการเปิดเผยต่อเจ้าของข้อมูลว่า ข้อมูลส่วนบุคคลนั้นจะถูกประมวลผลอย่างไร ด้วยเหตุผลใด จึงขัดกับลักษณะของการสืบสวนและสอบสวน จะเห็นได้จากการที่ LED และ The UK DPA ไม่บัญญัติรับรองหลักความโปร่งใส ส่วน The Privacy Act of 1974 บัญญัติให้หน่วยงานรัฐมีอำนาจกำหนดข้อจำกัดการเข้าถึงบันทึกข้อมูลที่เกี่ยวข้องกับการสืบสวนและสอบสวนได้เพิ่มเติม[381] หรือ South Korea's PIPA ก็ยกเว้นให้การสืบสวนและสอบสวนไม่จำต้องจดทะเบียนและเปิดเผยแฟ้มข้อมูล และไม่ต้องบันทึกฐานทางกฎหมาย เมื่อใช้ข้อมูลแตกต่างไปจากวัตถุประสงค์ดั้งเดิม[382]

อย่างไรก็ตาม แม้ว่ากฎหมายของสหภาพยุโรปและสหราชอาณาจักรจะยกเว้นมิให้นำหลักความโปร่งใสมาใช้บังคับแก่การสืบสวนและสอบสวน แต่ในทางกลับกัน LED และ The UK DPA ก็มีมาตรการเพื่อถ่วงดุลข้อยกเว้นข้างต้น อาทิ[383] กำหนดให้จัดเก็บข้อมูล Logs เพิ่มเติมจากการบันทึกรายการทั่วไป[384] กำหนดหลักเกณฑ์การประมวลผลข้อมูลด้วยวิธีการอัตโนมัติให้เคร่งครัดกว่า GDPR[385] รวมถึงกำหนดให้มีการประเมินความเสี่ยงและปรึกษาหารือกับหน่วยงานกำกับดูแลก่อนจะดำเนินการหากการประมวลผลข้อมูลส่วนบุคคลนั้นมีความเสี่ยงที่จะกระทบต่อสิทธิและเสรีภาพของบุคคลสูง[386] เป็นต้น สะท้อนให้เห็นว่าในบริบทของการสืบสวนและสอบสวนคดีอาญา ข้อจำกัดอำนาจที่ชัดเจนอาจเหมาะสมกว่าการมุ่งเน้นไปที่สิทธิของเจ้าของข้อมูลส่วนบุคคล[387]

---

[381] § 552a. (j)(2) and (k)(2).

[382] South Korea's PIPA, Article 32 (2) and Article 18.

[383] มีข้อสังเกตว่า ผู้เขียนไม่ได้กล่าวถึง "การแยกแยะประเภทข้อมูลส่วนบุคคล" ซึ่งเป็นมาตรการพิเศษใน LED เนื่องจากมาตรการดังกล่าวมีเจตนารมณ์เพื่อให้การแลกเปลี่ยนข้อมูลส่วนบุคคลระหว่างรัฐสมาชิกเป็นไปโดยสะดวกเป็นหลัก อีกทั้ง ในทางปฏิบัติก็พบปัญหาบางประการในการบังคับใช้มาตรการดังกล่าว (โปรดดู Leiser, M. and B. Custers, "The Law Enforcement Directive: Conceptual Challenges of Eu Directive 2016/680," <u>European Data Protection Law Review</u>. เพิ่มเติม)

[384] LED, Article 25.; The UK DPA, Article 62.

[385] LED, Article 29 (2).; The UK DPA, Article 49-50.

[386] LED, Article 28.; The UK DPA, Article 64-65.

[387] Leiser, M. and B. Custers, "The Law Enforcement Directive: Conceptual Challenges of Eu Directive 2016/680," <u>European Data Protection Law Review</u>.

จากข้อพิจารณาต่าง ๆ ข้างต้น ผู้เขียนจึงเห็นว่าเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลจากดำเนินงานในชั้นสืบสวนและสอบสวนคดีอาญาใน LED ของสหภาพยุโรปและกฎหมายต่างประเทศสามารถนำมาเป็นแนวทางสำหรับประเทศไทยในการกำหนดเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ดังนี้

ประการแรก ฐานการประมวลผลข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาพิเคราะห์แล้วเห็นว่า การสืบสวนและสอบสวนคดีอาญาของไทยสามารถเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล โดยไม่ต้องอาศัยความยินยอมได้ หากมีกฎหมายบัญญัติให้อำนาจโดยชัดแจ้ง และในอีกด้านหนึ่ง หน่วยงานหรือพนักงานเจ้าหน้าที่ยังสามารถใช้อำนาจตามกฎหมายสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลอื่นเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล เพื่อประโยชน์ในการสืบสวนและสอบสวนคดีอาญา โดยอาศัยฐานการปฏิบัติหน้าที่ตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล ในมาตรา 24 (6) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562[388]

อนึ่ง หากข้อมูลส่วนบุคคลที่เก็บรวบรวม ใช้ และเปิดเผยในชั้นสืบสวนและสอบสวนคดีอาญาเป็นข้อมูลอ่อนไหวตามมาตรา 26 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เช่น ข้อมูลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความเห็นทางการเมือง ความเชื่อ ศาสนา ปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ เจ้าพนักงานสืบสวนและสอบสวนอาจจำเป็นต้องจัดมาตรการที่เหมาะสมในการคุ้มครองสิทธิขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคลเพิ่มเติม เนื่องจากข้อมูลอ่อนไหวมีความละเอียดอ่อนต่อสิทธิและเสรีภาพของบุคคลเป็นพิเศษ และถือว่าเป็นข้อมูลที่เป็นส่วนตัวอย่างแท้จริง จึงจำเป็นต้องได้รับความคุ้มครองเหนือกว่าข้อมูลส่วนบุคคลทั่วไป ตามหลักการสากล

ประการที่สอง หลักการประมวลผลข้อมูลส่วนบุคคลสำหรับการสืบสวนและสอบสวนคดีอาญาของไทย มีข้อสังเกตว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะไม่ได้บัญญัติหลักการประมวลผลข้อมูลส่วนบุคคลโดยชัดแจ้ง แต่บทบัญญัติต่าง ๆ ในพระราชบัญญัติดังกล่าวต่างก็มีพื้นฐานมาจากหลักการประมวลผลข้อมูลส่วนบุคคลตามแนวทางของสหภาพยุโรปทั้งสิ้น ผู้เขียนจึงเห็นควรนำแนวทางของ LED มาปรับใช้กับประเทศไทย โดยให้การสืบสวนและสอบสวนคดีอาญายังคงอยู่ในบังคับที่จะต้องปฏิบัติหลักการประมวลผลข้อมูลส่วนบุคคลอื่น ๆ เว้นแต่ “หลักความโปร่งใส” ซึ่งในทรรศนะของผู้เขียน การยกเว้นมิให้นำหลักความโปร่งใสมาใช้บังคับย่อมมีผลกระทบต่อการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาในสองมิติ กล่าวคือ

---

[388] อ้างแล้ว, หน้า 229.

1.) ผลกระทบต่อการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

ในด้านหนึ่ง เมื่อการสืบสวนและสอบสวนไม่อาจดำเนินการด้วยความโปร่งใสต่อบุคคลได้อย่างบริบูรณ์ จึงเป็นการยากที่เจ้าของข้อมูลส่วนบุคคลจะใช้สิทธิในการควบคุมและตัดสินใจเกี่ยวกับข้อมูลของตน เพราะเจ้าของข้อมูลไม่มีโอกาสทราบข้อเท็จจริงและรายละเอียดที่เกี่ยวข้องแต่แรกเริ่ม ซึ่งจะได้กล่าวต่อไป

2.) ผลกระทบต่อหน้าที่ของหน่วยงานสืบสวนและสอบสวนคดีอาญา

เมื่อการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญามีข้อจำกัด ในอีกด้านหนึ่ง จึงมีความจำเป็นที่การสืบสวนและสอบสวนคดีอาญาจะต้องกำหนดมาตรการทดแทน เพื่อถ่วงดุลกับการจำกัดการใช้สิทธิ

ข้อพิจารณาที่ 2.3 เพื่อมิให้เป็นอุปสรรคต่อการป้องกันและปราบปรามอาชญากรรม จึงมีความจำเป็นที่ “สิทธิของเจ้าของข้อมูลส่วนบุคคล” ในชั้นสืบสวนและสอบสวนคดีอาญาจะต้องถูกจำกัดมากกว่ากรณีปกติ ซึ่งตามกฎหมายต่างประเทศจะมีรายละเอียดดังนี้

ตารางที่ 13 สิทธิเจ้าของข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาในต่างประเทศ

ประเทศ	สิทธิเจ้าของข้อมูลส่วนบุคคล
สหราชอาณาจักร	The UK DPA แยกบัญญัติสิทธิเจ้าของข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนไว้ใน PART 3: Law Enforcement Processing โดยรับรองสิทธิเจ้าของข้อมูลส่วนบุคคลอยู่เพียงสามประการ (น้อยกว่าการประมวลผลข้อมูลส่วนบุคคลทั่วไป) อันได้แก่ 1. สิทธิที่จะได้รับแจ้งข้อมูล 2. สิทธิที่จะเข้าถึงข้อมูล 3. สิทธิที่จะแก้ไข ลบ หรือจำกัดการประมวลผลข้อมูล นอกจากนี้ The UK DPA ยังกำหนดให้หน่วยงานบังคับใช้กฎหมายสามารถปฏิเสธการใช้สิทธิ โดยไม่ให้เหตุผลได้ รวมถึงกำหนดกลไกในการใช้สิทธิทางอ้อมผ่านหน่วยงานที่มีอำนาจหน้าที่กำกับดูแล เช่นเดียวกับ LED ของสหภาพยุโรปอีกด้วย
สหรัฐอเมริกา	The Privacy Act of 1974 รับรองสิทธิของเจ้าของข้อมูลในการเข้าถึงและโต้แย้งความถูกต้องของบันทึกข้อมูล เช่นเดียวกับการดำเนินการประเภทอื่น อย่างไรก็ดี หน่วยงานบังคับใช้กฎหมายอาญาอาจกำหนดหลักเกณฑ์หรือข้อยกเว้นสำหรับการเข้าถึงบันทึกข้อมูลได้เพิ่มเติมอีกด้วย
สาธารณรัฐเกาหลี	South Korea’s PIPA มีการรับรองสิทธิเจ้าของข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา เช่นเดียวกับการดำเนินงานประเภทอื่น

จากตารางข้างต้น จะเห็นได้ว่ามีเพียงสหราชอาณาจักรที่บัญญัติแยกสิทธิของเจ้าของข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาออกเป็นหลักเกณฑ์เฉพาะ พร้อมกำหนดกลไกการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลโดยอ้อมผ่านหน่วยงานที่มีอำนาจหน้าที่ในการกำกับดูแล ในขณะที่สหรัฐอเมริกาและสาธารณรัฐเกาหลีจะไม่ได้มีกฎเกณฑ์เฉพาะแต่อย่างใด การใช้สิทธิของเจ้าของข้อมูลในชั้นสืบสวนและสอบสวนคดีอาญาของสหรัฐอเมริกาและสาธารณรัฐเกาหลีจึงมีลักษณะเช่นเดียวกับการดำเนินงานประเภทอื่น เพียงแต่หน่วยงานหรือเจ้าหน้าที่รัฐอาจอ้างเหตุทางกฎหมายในการปฏิเสธการใช้สิทธิของเจ้าของข้อมูลได้ เพื่อไม่ให้การใช้สิทธิของเจ้าของข้อมูลกระทบกระเทือนต่อการสืบสวนและสอบสวนคดีอาญา เช่น South Korea's PIPA กำหนดให้หน่วยงานบังคับใช้กฎหมายปฏิเสธการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลได้ หากการปฏิเสธนั้นเป็นไปตามกฎหมาย หรือการใช้สิทธิดังกล่าวจะทำให้เสียหายแก่ชีวิต ร่างกาย ทรัพย์สิน หรือประโยชน์ของบุคคลอื่นใด[389] หรือสหรัฐอเมริกาก็บัญญัติให้อำนาจหน่วยงานบังคับใช้กฎหมายกำหนดหลักเกณฑ์หรือข้อยกเว้นสำหรับการเข้าถึงบันทึกข้อมูลที่เกี่ยวข้องกับการสืบสวนและสอบสวนคดีอาญาได้เพิ่มเติมจาก The Privacy Act of 1974[390]

อย่างไรก็ตาม มีข้อพึงระวังว่าการที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดเฉพาะเหตุแห่งการปฏิเสธ โดยไม่เปิดช่องให้เจ้าของข้อมูลส่วนบุคคลใช้สิทธิทางอื่นนั้น อาจเป็นการจำกัดสิทธิของประชาชนเกินกว่าสมควร เพราะย่อมเป็นการปิดโอกาสไม่ให้บุคคลมีสิทธิที่จะควบคุมและตัดสินใจเกี่ยวกับข้อมูลของตน ทั้งที่สิทธิดังกล่าวเป็นพื้นฐานสำคัญของการคุ้มครองข้อมูลส่วนบุคคล ด้วยเหตุนี้ LED และ The UK DPA จึงกำหนดให้เจ้าของข้อมูลส่วนบุคคลใช้สิทธิโดยอ้อม หากการใช้สิทธิดังกล่าวจะกระทบต่อการสืบสวนและสอบสวนคดีอาญา กล่าวคือในกรณีที่หน่วยงานบังคับใช้กฎหมายปฏิเสธการใช้สิทธิไม่ว่าจะให้เหตุผลหรือไม่ก็ตาม เจ้าของข้อมูลยังคงมีสิทธิที่จะร้องขอให้หน่วยงานกำกับดูแลตรวจสอบความชอบด้วยกฎหมายของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา และให้แจ้งผลการตรวจสอบไปยังเจ้าของข้อมูล[391] แทนการใช้สิทธิโดยตรงได้ เนื่องจากการเปิดเผยข้อมูลหรือรายละเอียดการสืบสวนและสอบสวนคดีอาญาต่อเจ้าของข้อมูลโดยตรงย่อมมีความเสี่ยงที่การสืบสวนและสอบสวนคดีอาญาไม่บรรลุผลมากกว่าการใช้สิทธิโดยอ้อม

ฉะนั้น เมื่อพิจารณาถึงความเหมาะสมของการใช้ของสิทธิเจ้าของข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา จึงเห็นควรให้ประเทศไทยกำหนดกลไกการใช้สิทธิตามแนวทางของกฎหมายสหภาพยุโรปและสหราชอาณาจักรแทน

---

[389] South Korea's PIPA, Article 35 and 37.

[390] § 552a. (j)(2); § 552a. (k)(2).

[391] LED, Article 17.; The UK DPA, Article 51.

ข้อพิจารณาที่ 2.4 สุดท้าย “กลไกการบังคับใช้” กฎหมายคุ้มครองข้อมูลส่วนบุคคล พบว่าแต่ละประเทศจะไม่ได้กำหนดกลไกการบังคับใช้เฉพาะสำหรับการสืบสวนและสอบสวนคดีอาญา แต่จะใช้กลไกเช่นเดียวกับการดำเนินงานประเภทอื่น ตามที่ปรากฏในตารางดังต่อไปนี้

ตารางที่ 14 กลไกการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในต่างประเทศ

ประเทศ	กลไกการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล
สหราชอาณาจักร	บังคับใช้ The UK DPA โดย ICO ซึ่งเป็นองค์กรอิสระทำหน้าที่ควบคุมและกำกับดูแลการประมวลผลข้อมูลส่วนบุคคลในกิจการทุกประเภท พร้อมมีบทกำหนดโทษทางอาญาและโทษปรับทางปกครอง เช่นเดียวกับการดำเนินงานประเภทอื่น นอกจากนี้ PART 3: Law Enforcement Processing ได้มีการกำหนดข้อจำกัดการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศตามแนวทาง LED ของสหภาพยุโรปอีกด้วย
สหรัฐอเมริกา	ไม่มีองค์กรอิสระ การบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลจึงกระทำโดยองค์กรที่มีอำนาจหน้าที่ตามกฎหมายเฉพาะประกอบกับกลไกกำกับดูแลตนเอง และการฝ่าฝืนหลักเกณฑ์ The Privacy Act of 1974 ก็อาจนำไปสู่ความรับผิดทางอาญาได้
สาธารณรัฐเกาหลี	บังคับใช้ South Korea’s PIPA โดย PIPC ซึ่งเป็นองค์กรอิสระควบคุมและกำกับดูแลการประมวลผลข้อมูลส่วนบุคคลในกิจการทุกประเภท อีกทั้ง South Korea’s PIPA ก็มีบทกำหนดความรับผิดในทางอาญาและทางปกครองตลอดจนข้อจำกัดการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศเช่นเดียวกัน

จะเห็นว่าโดยอย่างน้อยที่สุด กฎหมายทุกประเทศต่างก็มีบทกำหนดความรับผิดและโทษสำหรับการฝ่าฝืนกฎเกณฑ์การคุ้มครองข้อมูลส่วนบุคคล อีกทั้ง กฎหมายของสหราชอาณาจักรและสาธารณรัฐเกาหลีได้มีการบัญญัติข้อกำหนดเกี่ยวกับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศด้วย โดยสหราชอาณาจักรจะบัญญัติเป็นหลักเกณฑ์เฉพาะใน PART 3: Law Enforcement Processing ตามแนวทาง LED[392] เช่นเดียวกับเกณฑ์การคุ้มครองในชั้นสืบสวนและสอบสวนคดีอาญาตามข้อพิจารณาที่ 2.2 ในขณะที่สาธารณรัฐเกาหลีจะไม่ได้มีการจัดทำเป็นหลักเกณฑ์เฉพาะแต่อย่างใด

นอกจากนี้ หากพิจารณาในแง่องค์กรที่มีอำนาจหน้าที่บังคับใช้กฎหมาย ก็อาจจำแนกได้ออกเป็นสองรูปแบบใหญ่ด้วยกัน อันได้แก่

[392] The UK DPA, Article 71.

1.) <u>องค์กรอิสระที่มีอำนาจหน้าที่ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล</u>
มีประเทศที่ใช้รูปแบบนี้คือ สหราชอาณาจักรและสาธารณรัฐเกาหลี โดยจะเป็นองค์กรอิสระในรูปแบบคณะกรรมการ ที่มีอำนาจหน้าที่คุ้มครองข้อมูลส่วนบุคคลในทุกกิจการเป็นการทั่วไป รวมถึงการดำเนินงานในชั้นสืบสวนและสอบสวน ซึ่งเป็นแนวทางที่ LED ของสหภาพยุโรปเสนอแนะให้กระทำได้ เพียงแต่มีข้อสังเกตจาก Salami Emmanuel Akintunde ว่าการรวมอำนาจหน้าที่ตามกฎหมายไว้ที่หน่วยงานเดียว อาจเป็นการลดประสิทธิภาพการบังคับใช้กฎหมายได้[393]

2.) <u>องค์กรที่มีอำนาจตามกฎหมายเฉพาะเรื่อง และกลไกกำกับดูแลตนเอง</u>
แตกต่างจากแนวทางของสหภาพยุโรป สหรัฐอเมริกาจะไม่ได้มีองค์กรอิสระที่มีอำนาจหน้าที่คุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป ในการบังคับใช้กฎหมายจึงต้องอาศัยองค์กรเฉพาะประกอบกับกลไกกำกับดูแลตนเองของแต่ละหน่วยงาน ซึ่งสหภาพยุโรปเห็นว่า กลไกเช่นนี้เป็นข้อจำกัดประการหนึ่งของสหรัฐอเมริกาที่ทำให้ระดับการคุ้มครองข้อมูลส่วนบุคคลยังไม่เหมาะสมเพียงพอ[394]

สำหรับประเทศไทย การบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในปัจจุบันจะเป็นไปตามแนวทางของสหภาพยุโรป คือมีองค์กรอิสระในรูปแบบคณะกรรมการที่เรียกว่า “คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล” ทำหน้าที่เป็นหน่วยงานกลางกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย ซึ่งปัจจุบัน คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลจะมีอำนาจควบคุมและกำกับดูแลการสืบสวนและสอบสวนคดีอาญาเฉพาะส่วนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของข้อมูล จึงเห็นควรให้ขยายอำนาจหน้าที่ของคณะกรรมการดังกล่าวให้ครอบคลุมถึงการตรวจสอบการปฏิบัติตามหลักการคุ้มครองข้อมูลส่วนบุคคลในด้านอื่น ๆ ด้วย โดยเฉพาะเชิงนโยบายหรือเทคนิคที่ต้องอาศัยความรู้ความเชี่ยวชาญเฉพาะด้าน ในขณะที่การดำเนินการอื่นที่เกี่ยวข้องกับการดำเนินงานในกระบวนการยุติธรรมทางอาญา อาจให้ศาลทำหน้าที่เป็นองค์กรหลักในการตรวจสอบแทน

[393] Salami, E., "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."

[394] European Parliament, "A Comparison between Us and Eu Data Protection Legislation for Law Enforcement."

5.3 บทสรุป ผลการวิเคราะห์และเปรียบเทียบความเหมาะสมของแนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาสำหรับประเทศไทย

จากการศึกษาวิเคราะห์และเปรียบเทียบแนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา อาจสรุปได้ว่าระบบกฎหมายของสหภาพยุโรปและกฎหมายต่างประเทศ ได้แก่ สหราชอาณาจักร สหรัฐอเมริกา และสาธารณรัฐเกาหลี มิได้จำกัดการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาโดยเด็ดขาด แต่เลือกที่จะกำหนดให้การสืบสวนและสอบสวนคดีอาญาอยู่ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล ควบคู่ไปกับการบังคับใช้กฎหมายวิธีพิจารณาความอาญา ดังนั้น ในการกำหนดแนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาสำหรับประเทศไทยจึงจำเป็นต้องพิจารณาทั้งในด้านกฎหมายวิธีพิจารณาความอาญาและกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยมีประเด็นและข้อสรุป ดังต่อไปนี้

ประเด็นที่ 1 ความสัมพันธ์ของกฎหมายวิธีพิจารณาความอาญากับหลักประกันสิทธิในข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา

แม้ว่ากฎหมายวิธีพิจารณาความอาญากับกฎหมายคุ้มครองข้อมูลส่วนบุคคลจะเป็นกฎหมายคนละฉบับ แต่กฎหมายวิธีพิจารณาความอาญาก็เป็นกฎหมายที่ให้อำนาจเจ้าหน้าที่รัฐเก็บรวบรวม ใช้และเปิดเผยข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา ซึ่งเป็นมาตรการที่กระทบต่อสิทธิในข้อมูลส่วนบุคคล กฎหมายวิธีพิจารณาความอาญาจึงมีความสัมพันธ์กับการคุ้มครองข้อมูลส่วนบุคคลในแง่ที่ว่า หากกฎหมายวิธีพิจารณาความอาญาไม่มีกรอบจำกัดอำนาจที่เหมาะสม หลักประกันสิทธิในข้อมูลส่วนบุคคลของประชาชนก็ย่อมถูกลดทอนเมื่ออยู่ในชั้นสืบสวนและสอบสวนคดีอาญา จึงมีความจำเป็นที่รัฐแต่ละรัฐจะต้องออกแบบให้กฎหมายวิธีพิจารณาความอาญาให้สามารถรักษาสมดุลระหว่างการควบคุมอาชญากรรมกับการคุ้มครองสิทธิความเป็นส่วนตัวให้มีความเหมาะสม

อย่างไรก็ตาม เมื่อได้ทำการวิเคราะห์และเปรียบเทียบกฎหมายวิธีพิจารณาความอาญาของไทยกับเกณฑ์การปกป้องสิทธิของสหภาพยุโรป ตลอดจนกฎหมายวิธีพิจารณาความอาญาของต่างประเทศ กลับพบว่า อำนาจสืบสวนและสอบสวนตามกฎหมายวิธีพิจารณาความอาญาของไทยนั้นมีแนวโน้มที่จะไม่สอดคล้องกับเกณฑ์การปกป้องสิทธิ เพราะมีบทบัญญัติเปิดช่องให้เจ้าหน้าที่รัฐมีอำนาจเก็บรวบรวมข้อมูลส่วนบุคคลอย่างกว้างขวาง จนอาจนำไปสู่ความเสี่ยงที่ประเทศไทยจะถูกประเมินว่ามีระดับการคุ้มครองข้อมูลส่วนบุคคลจากการดำเนินงานของภาครัฐที่ไม่เพียงพอ ดังนั้น จึงเห็นควรให้ประเทศไทยพิจารณาแก้ไขปรับปรุงกฎหมายวิธีพิจารณาความอาญาของไทยให้สอดคล้องกับเกณฑ์การปกป้องสิทธิ เพื่อให้การก้าวล่วงสิทธิในข้อมูลส่วนบุคคลจากการดำเนินงานในชั้นสืบสวนและสอบสวนคดีอาญาอยู่บนพื้นฐานของหลักความจำเป็นและได้สัดส่วนต่อไป

ประเด็นที่ 2 ความจำเป็นที่การสืบสวนและสอบสวนคดีอาญาต้องอยู่ภายใต้บังคับกฎหมายคุ้มครองข้อมูลส่วนบุคคล เช่นเดียวกับการดำเนินงานประเภทอื่น

แม้โดยทั่วไป การสืบสวนและสอบสวนคดีอาญาจะถือเป็นความชอบธรรมของรัฐประการหนึ่งที่จะจำกัดการคุ้มครองข้อมูลส่วนบุคคล แต่การกำหนดบทยกเว้นทั่วไปมิให้นำกฎหมายคุ้มครองข้อมูลส่วนบุคคลมาใช้บังคับกับการสืบสวนและสอบสวนคดีอาญานั้น อาจเป็นข้อยกเว้นที่กว้างขวางเกินกว่าความจำเป็น เพราะเมื่อได้ทำการศึกษากฎหมายระหว่างประเทศและกฎหมายต่างประเทศที่เกี่ยวข้อง พบว่ามีหลายประเทศที่ไม่ได้กำหนดให้การสืบสวนและสอบสวนคดีอาญาเป็นข้อยกเว้นของการคุ้มครองข้อมูลส่วนบุคคลโดยเด็ดขาด แต่จะกำหนดข้อยกเว้นเป็นรายกรณีหรือกำหนดเป็นกฎเกณฑ์เฉพาะให้เกิดความเหมาะสมเท่านั้น ทั้งนี้ เนื่องจากสิทธิความเป็นส่วนตัวในข้อมูลเป็นสิทธิมนุษยชนขั้นพื้นฐาน รัฐจึงย่อมมีพันธกรณีที่จะต้องคุ้มครองสิทธิดังกล่าว ไม่ว่าจากการดำเนินงานประเภทใด ประกอบกับสิทธิความเป็นส่วนตัวในข้อมูลมีลักษณะเฉพาะ แตกต่างจากสิทธิและเสรีภาพรูปแบบดั้งเดิม เป็นเหตุให้กฎหมายทั่วไป ซึ่งรวมถึงกฎหมายวิธีพิจารณาความอาญา มีข้อจำกัดในการคุ้มครองข้อมูลส่วนบุคคลโดยสภาพ จึงมีความจำเป็นที่จะต้องกำหนดให้การสืบสวนและสอบสวนคดีอาญาอยู่ภายใต้หลักการคุ้มครองข้อมูลส่วนบุคคลเพิ่มเติม เพื่อให้สิทธิในข้อมูลส่วนบุคคลของประชาชนมีมาตรการที่เหมาะสมและสอดคล้องกับลักษณะของความเป็นส่วนตัวในข้อมูลมารองรับ แต่เพื่อป้องกันไม่ให้เกิดผลกระทบต่อประสิทธิภาพของรัฐในการป้องกันและปราบปรามอาชญากรรม การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาจึงควรที่จะกำหนดหลักเกณฑ์เฉพาะหรือข้อยกเว้นรายบทบัญญัติไป

ฉะนั้น การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาจึงต้องประกอบด้วยมาตรการทางกฎหมายสองกลไกควบคู่กันไป จะขาดกลไกหนึ่งกลไกใดไปเสียไม่ได้ มิฉะนั้น ก็อาจทำให้เกิดช่องว่างในการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา เนื่องจากกฎหมายทั้งสองฉบับต่างมีสาระสำคัญและเจตนารมณ์ที่แตกต่างกันออกไป

บทที่ 6
บทสรุปและข้อเสนอแนะ

จากสมมุติฐานของวิทยานิพนธ์ที่ว่า “แม้การสืบสวนและสอบสวนคดีอาญามีความจำเป็นที่จะต้องเก็บรวบรวมและใช้ประโยชน์จากข้อมูลส่วนบุคคลเป็นจำนวนมาก แต่ประเทศไทยกลับไม่มีมาตรการทางกฎหมายที่เหมาะสมเพียงพอในการคุ้มครองข้อมูลส่วนบุคคลในกระบวนการดังกล่าว จนเป็นเหตุให้ความเป็นส่วนตัวของประชาชนถูกล่วงละเมิดเกินกว่าที่จำเป็นอยู่หลายกรณี จึงสมควรกำหนดแนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาเป็นการเฉพาะ โดยกำหนดเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลให้ยืดหยุ่นกว่ากรณีทั่วไป กำหนดข้อจำกัดสิทธิของเจ้าของข้อมูลขึ้นใหม่ และกำหนดให้องค์กรอิสระมีบทบาทตรวจสอบกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาเพิ่มเติมต่อไป” เมื่อศึกษาวิจัยเสร็จสิ้น พบว่าสมมุติฐานที่ตั้งไว้ถูกต้อง โดยมีบทสรุปและข้อเสนอแนะเพื่อแก้ไขปรับปรุงกฎหมายไทย ดังต่อไปนี้

6.1 บทสรุป

ในปัจจุบัน แม้ว่าประเทศไทยจะมีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นกฎหมายกลางว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล แต่พระราชบัญญัติดังกล่าวก็ยกเว้นให้การสืบสวนและสอบสวนคดีอาญาไม่อยู่ในบังคับพระราชบัญญัตินี้ เว้นแต่ในส่วนที่เป็นมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาจึงต้องอาศัยมาตรการทางกฎหมายที่มีอยู่เดิมเป็นหลัก ได้แก่ กฎหมายวิธีพิจารณาความอาญา และหมวด 3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 แต่จากการศึกษาพบว่า ทั้งสองมาตรการต่างมีข้อจำกัดในการให้ความคุ้มครองข้อมูลส่วนบุคคล กล่าวคือ

1.) <u>ข้อจำกัดของกฎหมายวิธีพิจารณาความอาญา</u>

กฎหมายวิธีพิจารณาความอาญาของไทย มักใช้ถ้อยคำในบทบัญญัติอย่างกว้าง ๆ จึงเป็นการเปิดช่องให้เจ้าพนักงานสืบสวนสอบสวนมีอำนาจดุลพินิจเก็บรวบรวมข้อมูลส่วนบุคคลอย่างกว้างขวาง ประกอบกับกฎหมายวิธีพิจารณาความอาญาก็ไม่ได้มีเจตนารมณ์ในการคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะ จึงย่อมมีข้อจำกัดโดยสภาพในการคุ้มครองข้อมูลส่วนบุคคล ทั้งในแง่ความครอบคลุมของกฎเกณฑ์

การรับรองสิทธิเจ้าของข้อมูลส่วนบุคคล รวมถึงสภาพบังคับและบทกำหนดโทษที่ไม่สอดคล้องกับลักษณะเฉพาะของความเป็นส่วนตัวในข้อมูล

2.) ข้อจำกัดของหมวด 3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 เมื่อเปรียบเทียบกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พบว่าหมวด 3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 จะมีรายละเอียดการปฏิบัติที่ไม่ชัดเจน เพราะมีบทบัญญัติอยู่เพียง 5 มาตรา และได้รับการตราขึ้นตั้งแต่ปี พ.ศ. 2540 โดยไม่มีการแก้ไขปรับปรุงเพิ่มเติมแต่อย่างใด มาตรฐานการคุ้มครองข้อมูลข่าวสารส่วนบุคคลในหมวด 3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 จึงอาจไม่เทียบเท่ามาตรฐานสากลในปัจจุบัน

สภาพปัญหาดังกล่าวไม่เพียงแต่ส่งผลกระทบต่อสิทธิในข้อมูลส่วนบุคคลของประชาชน แต่ยังอาจส่งผลกระทบต่อการแลกเปลี่ยนถ่ายโอนข้อมูลส่วนบุคคลในระดับระหว่างประเทศด้วย เพราะเมื่อประเทศไทยไม่มีมาตรการที่เหมาะสมเพียงพอในการคุ้มครองข้อมูลส่วนบุคคลจากการดำเนินงานในชั้นสืบสวนและสอบสวนคดีอาญา ก็ย่อมส่งผลตามมาว่าภาพรวมของระดับการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยอาจถูกพิจารณาได้ว่าไม่เพียงพอตามมาตรฐานสากล เนื่องจากการวินิจฉัยถึงระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอจะไม่ได้พิจารณาเฉพาะกฎหมายคุ้มครองข้อมูลส่วนบุคคลโดยลำพัง แต่พิจารณาไปถึงว่า ระบบกฎหมายในประเทศนั้นได้ให้อำนาจเจ้าหน้าที่รัฐล่วงละเมิดข้อมูลส่วนบุคคลสมดุลกับการคุ้มครองสิทธิในความเป็นส่วนตัวหรือไม่ จึงสมควรที่ประเทศไทยจะต้องพิจารณาทบทวนกำหนดแนวทางการคุ้มครองข้อมูลในชั้นสืบสวนสอบสวนคดีอาญา เพื่อแก้ไขปัญหาข้างต้นต่อไป

อย่างไรก็ตาม ข้อท้าทายสำคัญที่สุดในการกำหนดแนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา ก็คือการตอบคำถามว่าการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญามีความจำเป็นเพียงใด และจะกระทำได้หรือไม่ อย่างไร โดยมิให้กระทบกระเทือนต่อการป้องกันและปราบปรามอาชญากรรม อันเป็นประโยชน์สาธารณะของสังคม

จากการศึกษาแนวคิดและทฤษฎีที่เกี่ยวข้อง ผู้เขียนพบว่าสิทธิความเป็นส่วนตัวในข้อมูลมิใช่สิทธิเด็ดขาด จึงอาจถูกจำกัดการคุ้มครองได้เพื่อประโยชน์ในการป้องปรามอาชญากรรมในชั้นสืบสวนและสอบสวนคดีอาญา ตามทฤษฎีการควบคุมอาชญากรรม แต่ถึงกระนั้น การจำกัดดังกล่าวก็ต้องอยู่บนพื้นฐานหลักความจำเป็นและได้สัดส่วนตามทฤษฎีศุภนิติกระบวนเช่นกัน เพราะความเป็นส่วนตัวในข้อมูลถือเป็นสิทธิมนุษยชนขั้นพื้นฐานของบุคคล จึงไม่อาจถือได้ว่าการสืบสวนและสอบสวนคดีอาญาเป็นข้อจำกัดการคุ้มครองสิทธิในข้อมูลส่วนบุคคลโดยเด็ดขาด ซึ่งมีความจำเป็นที่รัฐจะต้องจัดให้มีการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา เพื่อป้องกันมิให้รัฐล่วงละเมิดความเป็น

ส่วนตัวในข้อมูลของประชาชนเกินกว่าสมควร ดังจะเห็นได้จากกฎหมายสหภาพยุโรป ซึ่งเป็นต้นแบบกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย รวมถึงกฎหมายต่างประเทศที่เป็นกรณีศึกษา ไม่ว่าจะเป็นสหราชอาณาจักร สหรัฐอเมริกา รวมถึงสาธารณรัฐเกาหลี ก็มิได้ยกเว้นหรือจำกัดการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาโดยเด็ดขาด ซึ่งจากการศึกษาพบว่าการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาตามกฎหมายระหว่างประเทศและต่างประเทศจะประกอบด้วยมาตรการทางกฎหมายสองกลไกควบคู่กันไป อันได้แก่

1.) <u>กฎหมายวิธีพิจารณาความอาญา</u>

ในด้านหนึ่ง กฎหมายวิธีพิจารณาความอาญาจะต้องมีความเฉพาะเจาะจง และมีกลไกตรวจสอบถ่วงดุลการใช้อำนาจ เพื่อป้องกันไม่ให้เจ้าหน้าที่รัฐใช้อำนาจตามอำเภอใจ ยิ่งไปกว่านั้น กฎหมายวิธีพิจารณาความอาญาควรมีมาตรการคุ้มครองสิทธิและเสรีภาพของบุคคล เพื่อให้การจำกัดสิทธิและเสรีภาพนั้นเป็นไปโดยได้สัดส่วนกับประโยชน์ที่ได้จากการป้องปรามอาชญากรรม

2.) <u>กฎหมายคุ้มครองข้อมูลส่วนบุคคล</u>

ในอีกด้านหนึ่ง การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาก็จำเป็นต้องมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลเข้ามาเสริม เพราะสิทธิในข้อมูลส่วนบุคคลมีลักษณะเฉพาะแตกต่างไปจากสิทธิและเสรีภาพแบบดั้งเดิม กล่าวคือ ความเป็นส่วนตัวในข้อมูลนั้นจะมุ่งคุ้มครองความเป็นอิสระในการปกครองตนเองในแง่การควบคุมและตัดสินใจเกี่ยวกับข้อมูล ซึ่งมาตรการทางกฎหมายที่มีอยู่เดิมจะไม่มีกฎเกณฑ์รับรองการใช้สิทธิในรูปแบบนี้แต่ประการใด

ทั้งนี้ มีข้อสังเกตว่าการนำกฎหมายคุ้มครองข้อมูลส่วนบุคคลมาใช้บังคับแก่การสืบสวนและสอบสวนคดีอาญานั้น อาจไม่จำเป็นต้องใช้กฎเกณฑ์เช่นเดียวกันกับดำเนินงานประเภทอื่น เพราะหากมีความจำเป็น ก็สามารถบัญญัติเป็นหลักเกณฑ์เฉพาะหรือกำหนดเป็นข้อยกเว้นรายกรณีตามความเหมาะสมได้ เพื่อป้องกันไม่ให้การคุ้มครองข้อมูลส่วนบุคคลเป็นอุปสรรคต่อการสืบสวนและสอบสวนคดีอาญา

ฉะนั้น เพื่อแก้ไขปัญหาการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาของประเทศไทย ผู้เขียนจึงได้ดำเนินการศึกษาแนวคิดและทฤษฎีที่เกี่ยวข้อง รวมถึงวิเคราะห์เปรียบเทียบแนวทางตามกฎหมายของสหภาพยุโรปและต่างประเทศ ทั้งในส่วนของกฎหมายวิธีพิจารณาความอาญาและกฎหมายคุ้มครองข้อมูลส่วนบุคคล อันนำมาสู่ข้อเสนอแนะในลำดับถัดไป

6.2 ข้อเสนอแนะ

เมื่อได้พิจารณาถึงความจำเป็น แนวคิดและทฤษฎีที่เกี่ยวข้อง ตลอดจนแนวทางตามกฎหมายระหว่างประเทศและกฎหมายต่างประเทศแล้ว ผู้เขียนจึงเห็นควรมีข้อเสนอแนะในการกำหนดแนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาสำหรับประเทศไทย โดยใช้แนวทางของ LED เป็นสำคัญ ทั้งนี้ เนื่องจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปถือเป็นต้นแบบพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การนำมาปรับใช้กับระบบกฎหมายไทยจึงน่าจะมีความเหมาะสม เพราะเป็นพื้นฐานของกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ประเทศไทยมีความคุ้นเคย ซึ่งจากการศึกษาวิจัยพบว่า หลักการพื้นฐานประการสำคัญของ LED ในการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาคือการกำหนดให้ “การประมวลผลข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาจะกระทำได้แต่โดยมีกฎหมายบัญญัติให้อำนาจโดยชัดแจ้ง บนพื้นฐานของหลักความได้สัดส่วน” จึงเห็นสมควรให้ประเทศไทยกำหนดแนวทางในการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาได้ตามข้อเสนอแนะต่าง ๆ ดังต่อไปนี้

6.2.1 การแก้ไขปรับปรุงกฎหมายวิธีพิจารณาความอาญาของไทยให้มีความสอดคล้องกับหลักสิทธิมนุษยชน หรือเกณฑ์ปกป้องสิทธิ

เมื่อหลักการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาอยู่บนพื้นฐานของ “การมีบทบัญญัติกฎหมายให้อำนาจโดยชัดแจ้ง” จึงมีความจำเป็นที่การสืบสวนและสอบสวนคดีอาญาของประเทศไทยจะต้องมีกฎหมายเป็นฐานอำนาจเสมอ ซึ่งปัจจุบัน กฎหมายวิธีพิจารณาความอาญาถือเป็นบทบัญญัติหลักที่ให้อำนาจเจ้าหน้าที่รัฐเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในชั้นนี้

อย่างไรก็ตาม ลำพังการมีอยู่ของกฎหมายวิธีพิจารณาความอาญาก็ไม่ได้หมายความว่าการใช้อำนาจสืบสวนและสอบสวนจะเป็นไปด้วยความเหมาะสม จะเห็นได้จากการที่สหภาพยุโรปเรียกร้องให้กฎหมายซึ่งให้อำนาจรัฐในการแทรกแซงข้อมูลส่วนบุคคลจะต้องมีกรอบจำกัดอำนาจที่เหมาะสม โดยสหภาพยุโรปได้ใช้เกณฑ์ปกป้องสิทธิในการประเมิน เพื่อรับประกันว่ากฎหมายวิธีพิจารณาความอาญาจะสอดคล้องกับหลักสิทธิมนุษยชน ประกอบด้วย (1) หลักความเฉพาะเจาะจง (2) หลักการตรวจสอบถ่วงดุล และ (3) หลักความจำเป็นและได้สัดส่วน จึงเห็นสมควรให้ประเทศไทยพิจารณาแก้ไขปรับปรุงกฎหมายวิธีพิจารณาความอาญาให้มีความสอดคล้องกับเกณฑ์ปกป้องสิทธิดังกล่าว เพื่อลดผลกระทบที่อาจเกิดขึ้นต่อสิทธิในข้อมูลส่วนบุคคลจากการใช้มาตรการบังคับต่าง ๆ ต่อไปนี้

ข้อเสนอแนะที่ 1 ประเทศไทยควรพิจารณาทบทวนว่า การแสวงหาพยานหลักฐานรูปแบบใดควรจัดให้อยู่ในขอบเขต “การค้นและยึด” ที่ต้องผ่านกระบวนการตรวจสอบถ่วงดุลจากศาล โดยเฉพาะการแสวงพยานหลักฐานที่มีการใช้เทคโนโลยีสมัยใหม่ ซึ่งละเมิดความเป็นส่วนตัวโดยง่าย ดังจะเห็นได้

จากกฎหมายและคำพิพากษาในต่างประเทศ ที่มีการขยายขอบเขตการค้นและยึดที่อยู่ในบังคับจะต้องได้รับหมายหรือคำสั่งจากศาลเป็นฐานอำนาจ ให้ครอบคลุมการแสวงหาพยานหลักฐานหลายรูปแบบ เพื่อให้มีความสอดคล้องกับบริบททางสังคมที่เปลี่ยนแปลงไป ทั้งนี้ เนื่องจากการค้นและยึดที่อยู่ภายใต้กระบวนการตรวจสอบถ่วงดุลตามกฎหมายวิธีพิจารณาความอาญาของไทยมีขอบเขตจำกัดอยู่เฉพาะการค้นในที่รโหฐานและการค้นเอกสารทางไปรษณีย์เอกสารเท่านั้น

ข้อเสนอแนะที่ 2 ประเทศไทยควรพิจารณาแก้ไขเกณฑ์การได้มาซึ่งข้อมูลข่าวสารส่วนบุคคลในพระราชบัญญัติเฉพาะต่าง ๆ ให้มีความชัดเจนและเฉพาะเจาะจงเพียงพอที่ประชาชนทั่วไปสามารถคาดหมายได้ เพื่อจำกัดดุลพินิจของเจ้าหน้าที่รัฐ โดยการให้รายละเอียดเกี่ยวกับเหตุแห่งการใช้อำนาจ มาตรการที่ใช้ เป้าหมาย และกรอบระยะเวลาให้ได้มากที่สุดเท่าที่จะกระทำได้ ซึ่งสำหรับประเทศไทยอาจเริ่มต้นจากการแก้ไขพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2540 เป็นอันดับแรก เนื่องจากการได้มาซึ่งข้อมูลข่าวสารส่วนบุคคลตามพระราชบัญญัติดังกล่าวมีขอบเขตอย่างกว้างขวางและมีแนวโน้มไม่สอดคล้องกับเกณฑ์การปกป้องสิทธิของสหภาพยุโรปหลายประการ

นอกจากนี้ ประเทศไทยควรพิจารณากำหนดมาตรการคุ้มครองสิทธิตามแนวทางของกฎหมายต่างประเทศเพิ่มเติมอีกด้วย ไม่ว่าจะเป็นกระบวนการแจ้งข้อเท็จจริงหรือกระบวนการโต้แย้งความชอบด้วยกฎหมายของการได้มาซึ่งข้อมูลข่าวสารส่วนบุคคล เพื่อเปิดโอกาสให้ประชาชนได้ตรวจสอบถ่วงดุลการใช้อำนาจของเจ้าหน้าที่รัฐมิให้เป็นไปโดยอำเภอใจ

ข้อเสนอแนะที่ 3 ประเทศไทยควรพิจารณากำหนดข้อจำกัดการเก็บรวบรวมข้อมูลข่าวสารจากภาคเอกชนในชั้นสืบสวนและสอบสวนคดีอาญา เพื่อมิให้เป็นอำนาจดุลพินิจของเจ้าหน้าที่รัฐโดยลำพัง อย่างไรก็ดี การกำหนดให้การขอข้อมูลข่าวสารจากภาคเอกชนต้องผ่านกระบวนการตรวจสอบจากศาลในทุกกรณีนั้นอาจจะทำให้การสืบสวนและสอบสวนคดีอาญาขาดความคล่องตัว จึงยังไม่เหมาะสมกับบริบทของประเทศไทยในปัจจุบัน ในเบื้องต้น จึงเห็นควรให้ประเทศไทยแบ่งประเภทข้อมูลข่าวสารที่เจ้าหน้าที่รัฐเก็บรวบรวมจากภาคเอกชนตามระดับความรุนแรงและผลกระทบที่อาจเกิดขึ้นกับสิทธิของบุคคล พร้อมกำหนดหลักเกณฑ์ เงื่อนไข รวมถึงกระบวนการตรวจสอบให้มีความสอดคล้องกับประเภทของข้อมูลข่าวสารนั้น ๆ ต่อไป อาทิ กำหนดเงื่อนไขการออกหมายเรียกพยานเอกสารในการขอข้อมูลโดยต้องระบุความเกี่ยวข้องของข้อมูลที่ต้องการเก็บรวบรวมกับการกระทำความผิดที่กำลังสืบสวนหรือสอบสวนคดีอาญา เพื่อให้ผู้บังคับบัญชาหรือศาลได้ตรวจสอบ เป็นต้น

อนึ่ง มีข้อสังเกตว่าการพัฒนาหรือแก้ไขปรับปรุงกฎหมายวิธีพิจารณาความอาญาของไทยนั้นอาจไม่จำกัดเพียงวิธีการที่ผู้เขียนเสนอแนะในเบื้องต้น เนื่องจากมีงานวิจัยในประเทศไทยอีกจำนวนมากที่มีข้อเสนอแนะเกี่ยวกับการคุ้มครองสิทธิและเสรีภาพในกระบวนการสืบสวนและสอบสวนคดีอาญา

ซึ่งผู้เขียนเห็นว่าสามารถนำมาปรับใช้เพื่อส่งเสริมให้กฎหมายวิธีพิจารณาความอาญาของไทยสอดคล้องกับเกณฑ์การปกป้องสิทธิของสหภาพยุโรปมากยิ่งขึ้นได้เช่นกัน

6.2.2 การกำหนดให้การสืบสวนและสอบสวนคดีอาญาในประเทศไทยอยู่ภายใต้บังคับของหลักการคุ้มครองข้อมูลส่วนบุคคล

นอกเหนือจากการมีบทบัญญัติกฎหมายให้อำนาจ การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญายังต้องอยู่บนพื้นฐานของ “ความได้สัดส่วน” กล่าวคือต้องเป็นการดำเนินงานที่จำเป็นเพื่อบรรลุวัตถุประสงค์ในการสืบสวนและสอบสวนคดีอาญา และจะต้องไม่ก่อให้เกิดผลกระทบต่อสิทธิความเป็นส่วนตัวในข้อมูลของบุคคลเกินกว่าสมควร เมื่อชั่งน้ำหนักกับประโยชน์สาธารณะที่ได้สอดคล้องไปกับรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ซึ่งวางหลักให้การตรากฎหมายจำกัดสิทธิในข้อมูลส่วนบุคคลพึงกระทำเท่าที่จำเป็น เพื่อประโยชน์สาธารณะเท่านั้น

ด้วยเหตุนี้ การยกเว้นไม่นำกฎหมายคุ้มครองข้อมูลส่วนบุคคลมาบังคับใช้แก่การสืบสวนและสอบสวนคดีอาญาโดยสิ้นเชิงจึงอาจไม่สอดคล้องกับหลักความได้สัดส่วน จึงเห็นสมควรให้ประเทศไทยกำหนดให้การสืบสวนและสอบสวนคดีอาญาอยู่ภายใต้หลักการคุ้มครองข้อมูลส่วนบุคคลเช่นเดียวกับการดำเนินงานประเภทอื่น ๆ แต่เพื่อให้สอดคล้องกับธรรมชาติของการสืบสวนและสอบสวนคดีอาญาก็มีความจำเป็นที่ประเทศไทยจะต้องกำหนดหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาเป็นการเฉพาะ แยกออกมาจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งแนวทางที่สามารถกระทำได้อย่างรวดเร็ว และน่าจะมีความเหมาะสมกับบริบทของการสืบสวนและสอบสวนคดีอาญาในประเทศไทยมากที่สุด คือการบัญญัติหลักการคุ้มครองข้อมูลส่วนบุคคลทั่วไปไว้ในมาตรา 131 ประมวลกฎหมายวิธีพิจารณาความอาญา ด้วยการเพิ่มเติมข้อความดังนี้

“ให้พนักงานสอบสวนรวบรวมหลักฐานทุกชนิด เท่าที่สามารถกระทำได้ เพื่อประสงค์จะทราบข้อเท็จจริง และพฤติการณ์ต่าง ๆ อันเกี่ยวกับความผิดที่ถูกกล่าวหา เพื่อจะรู้ตัวผู้กระทำผิดและพิสูจน์ให้เห็นความผิดหรือความบริสุทธิ์ของผู้ต้องหา

<u>การรวบรวมหลักฐานตามวรรคหนึ่งต้องกระทำในขอบเขตที่กฎหมายกำหนด เท่าที่จำเป็นและได้สัดส่วน โดยคำนึงถึงผลกระทบต่อสิทธิส่วนบุคคล ทั้งนี้ ตามหลักเกณฑ์และวิธีการคุ้มครองข้อมูลส่วนบุคคลที่กฎกระทรวงและระเบียบกำหนด</u>”

กล่าวคือ เป็นการนำสารัตถะของหลักการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาภายใต้ LED มาบัญญัติในประมวลกฎหมายวิธีพิจารณาความอาญา ซึ่งเป็นบทบัญญัติหลักที่

ใช้บังคับในชั้นสืบสวนและสอบสวนคดีอาญาของไทย จากนั้นจึงจะกำหนดรายละเอียดของหลักเกณฑ์และวิธีการคุ้มครองข้อมูลส่วนบุคคลในกฎกระทรวงที่ออกโดยรัฐมนตรีว่าการกระทรวงยุติธรรม หรือในระเบียบสำนักงานตำรวจแห่งชาติ แล้วแต่กรณี ซึ่งผู้เขียนเห็นว่าสามารถนำหลักเกณฑ์ของ LED มาบัญญัติได้ โดยมีแนวทางดังต่อไปนี้

ข้อเสนอแนะที่ 1 ประเทศไทยควรกำหนดขอบเขตของข้อมูลส่วนบุคคลที่ได้รับคุ้มครองในชั้นสืบสวนและสอบสวนคดีอาญา ให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยไม่จำต้องกำหนดหลักเกณฑ์ใหม่แต่อย่างใด เพื่อให้ข้อมูลส่วนบุคคลที่ได้รับความคุ้มครองในระบบกฎหมายไทยมีความเป็นเอกภาพและสอดคล้องกับหลักสากล จะเห็นได้จากการที่ LED ก็มิได้กำหนดขอบเขตของข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาเป็นการเฉพาะ แต่ใช้บทนิยามเดียวกับการประมวลผลข้อมูลส่วนบุคคลกรณีทั่วไป

ดังนั้น ข้อมูลส่วนบุคคล ซึ่งเป็นวัตถุแห่งสิทธิที่ได้รับความคุ้มครองในชั้นสืบสวนและสอบสวนคดีอาญาจึงหมายความถึง “ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ” โดยบุคคลในที่นี้มิได้หมายความจำกัดเฉพาะจำเลยหรือผู้ต้องหาในคดีอาญา แต่ยังครอบคลุมถึงผู้เสียหาย พยาน หรือผู้เกี่ยวข้องอื่น ๆ ด้วย

อย่างไรก็ดี การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาย่อมไม่สามารถนำหลักการขยายขอบเขตเชิงพื้นที่มาใช้บังคับได้ เนื่องจากหลักการดังกล่าวมีผลเป็นการขยายขอบเขตการคุ้มครองข้อมูลส่วนบุคคลของบุคคลที่อยู่ในประเทศไทยจากการประมวลผลข้อมูลในบางลักษณะที่เกิดขึ้นนอกประเทศ อันอาจเป็นการก้าวล่วงอำนาจอธิปไตยของรัฐอื่น จึงไม่สมควรจะใช้บังคับในชั้นสืบสวนและสอบสวนคดีอาญา

ข้อเสนอแนะที่ 2 ประเทศไทยควรพิจารณากำหนดเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา ดังนี้

ข้อเสนอแนะที่ 2.1 การประมวลผลข้อมูลส่วนบุคคล ไม่ว่าจะเป็นการเก็บรวบรวม ใช้และเปิดเผยข้อมูลในชั้นสืบสวนและสอบสวนคดีอาญา ต้องมีบทบัญญัติกฎหมายเป็นฐานการใช้อำนาจอย่างชัดเจน และการประมวลผลข้อมูลส่วนบุคคลนั้นจะต้องเป็นการดำเนินงานที่จำเป็นเพื่อประโยชน์ในการสืบสวนและสอบสวนคดีอาญา กล่าวคือต้องได้มีความสัดส่วน เมื่อพิจารณาถึงผลกระทบที่อาจเกิดขึ้นกับสิทธิความเป็นส่วนตัวในข้อมูลของบุคคล

นอกจากนี้ ผู้เขียนยังเห็นควรอนุโลมให้การสืบสวนและสอบสวนคดีอาญาอาจอาศัยความยินยอมเป็นฐานทางกฎหมายในบางบริบทตามแนวทางของสหราชอาณาจักร โดยเฉพาะในกรณี

ที่ข้อมูลส่วนบุคคลนั้นเป็นข้อมูลของบุคคลอื่นที่มิใช่ผู้ต้องสงสัยหรือผู้กระทำผิด เช่น การขอข้อมูลจากครอบครัวหรือญาติเพื่อยืนยันตัวตนของผู้เสียชีวิต เป็นต้น แต่การใช้ฐานความยินยอมนี้จะต้องกระทำอย่างจำกัดและต้องปฏิบัติตามเงื่อนไขการขอความยินยอมอย่างเคร่งครัด เพื่อประกันว่าความยินยอมดังกล่าวเป็นความยินยอมที่บริสุทธิ์และเป็นอิสระอย่างแท้จริง ซึ่งอาจนำหลักเกณฑ์ของมาตรา 19 ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาปรับใช้ได้ อาทิ กำหนดให้การขอความยินยอมต้องมีแบบหรือข้อความที่เข้าใจได้ง่าย แยกส่วนจากข้อความอื่นจากชัดเจน พร้อมให้แจ้งวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลอย่างชัดเจน ฯลฯ

สำหรับข้อมูลอ่อนไหว เห็นว่าการสืบสวนและสอบสวนคดีอาญาจะประมวลผลข้อมูลดังกล่าวได้เฉพาะในกรณีที่มีความจำเป็นอย่างยิ่ง และจะต้องจัดให้มีมาตรการคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

ข้อเสนอแนะที่ 2.2 หลักการประมวลผลข้อมูลส่วนบุคคล มีความเห็นว่าการสืบสวนและสอบสวนคดีอาญาในประเทศไทยสามารถอยู่ภายใต้หลักการประมวลผลข้อมูลส่วนบุคคลทั่วไปตามแนวทางของ LED ได้ กล่าวคือจะต้องประมวลผลโดยชอบด้วยกฎหมายและเป็นธรรม อีกนัยหนึ่งคือ มีฐานทางกฎหมายรองรับตามข้อเสนอแนะที่ 2.1 และกระทำเท่าที่จำเป็นในขอบเขตวัตถุประสงค์ อีกทั้งควรเก็บรักษาข้อมูลส่วนบุคคลให้ถูกต้องเป็นปัจจุบัน พร้อมทั้งลบหรือทำลายเมื่อพ้นกำหนดระยะเวลาเก็บรักษาหรือเมื่อหมดความจำเป็น ตลอดจนจัดให้มีมาตรการรักษาความมั่นคงปลอดภัย ซึ่งเป็นหน้าที่ที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้ต้องกระทำอยู่เดิม

ทั้งนี้ เหตุที่ผู้เขียนเห็นว่าประเทศไทยสามารถนำหลักการประมวลผลข้อมูลส่วนบุคคลเหล่านี้มาใช้บังคับแก่การสืบสวนและสอบสวนคดีอาญาได้ เป็นเพราะหลักการเหล่านี้มิได้ส่งผลกระทบโดยตรงต่อการดำเนินงานในชั้นสืบสวนและสอบสวนคดีอาญา จะเห็นได้จากการที่พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ซึ่งการสืบสวนและสอบสวนคดีอาญาอยู่ภายใต้บังคับ ก็มีการบัญญัติหลักการต่าง ๆ ข้างต้นในหมวด 3 เพียงแต่จะขาดรายละเอียดการปฏิบัติเท่านั้น อย่างไรก็ตาม เพื่อให้เกิดความเหมาะสม การตีความและบังคับใช้ก็จำต้องคำนึงถึงบริบทและธรรมชาติของการสืบสวนและสอบสวนคดีอาญาประกอบด้วย อาทิ ความถูกต้องของข้อมูลที่ได้จากการสอบปากคำบุคคล อาจเป็นความถูกต้องของข้อเท็จจริงที่ว่าบุคคลมีการระบุข้อมูลดังกล่าวเท่านั้น หรือการลบหรือทำลายข้อมูลที่พ้นระยะเวลาเก็บรักษา หน่วยงานที่มีอำนาจหน้าที่ในการสืบสวนและสอบสวนคดีอาญาอาจใช้วิธีการทำให้เป็นข้อมูลที่ระบุตัวตนของบุคคลไม่ได้แทนการลบหรือทำลายโดยสิ้นเชิง เพื่อที่ว่าข้อมูลนั้นอาจนำกลับมาใช้ประโยชน์ในการป้องกันและปราบปรามอาชญากรรมได้ เป็นต้น

ในทางกลับกัน หลักการที่ไม่อาจบังคับใช้แก่การสืบสวนและสอบสวนคดีอาญาได้คือ “หลักความโปร่งใส” เพราะการสืบสวนและสอบสวนคดีอาญาย่อมไม่สามารถเปิดเผยรายละเอียดของการสืบสวนและสอบสวนคดีอาญาให้เจ้าของข้อมูลทราบในทุกกรณี มิฉะนั้น การสืบสวนและสอบสวนคดีอาญาก็อาจไม่บรรลุผลในการปราบปรามอาชญากรรม โดยเฉพาะในกรณีที่เจ้าของข้อมูลส่วนบุคคลเป็นผู้ต้องสงสัยหรือผู้กระทำผิด แต่เพื่อมิให้หลักประกันสิทธิในข้อมูลส่วนบุคคลถูกลดทอนเกินสมควร ประเทศไทยจึงควรกำหนดมาตรการถ่วงดุลเพิ่มเติมตามแนวทางของ LED เช่น จัดให้มีระบบที่จัดเก็บข้อมูลจราจร (Logs) ในฐานข้อมูลออนไลน์ หรือประเมินความเสี่ยง ก่อนที่จะประมวลผลข้อมูลโดยใช้เทคโนโลยีสมัยใหม่ที่มีความซับซ้อน นอกจากนี้ เมื่อหมดความจำเป็นที่ต้องปกปิดรายละเอียดข้อมูลในการสืบสวนและสอบสวนคดีอาญา ก็ควรมีมาตรการในการแจ้งข้อเท็จจริงให้เจ้าของข้อมูลได้ทราบว่าข้อมูลเกี่ยวกับตนนั้นถูกนำไปประมวลผลในชั้นสืบสวนและสอบสวนคดีอาญา เพื่อเปิดโอกาสให้บุคคลผู้ได้รับผลกระทบได้ใช้สิทธิในฐานะเจ้าของข้อมูลต่อไป

ข้อเสนอแนะที่ 3 ประเทศไทยควรรับรองให้บุคคลสามารถใช้สิทธิในฐานะเจ้าของข้อมูลในชั้นสืบสวนและสอบสวนคดีอาญาได้ โดยอย่างน้อยที่สุด ควรมีการรับรองสิทธิพื้นฐานอย่างสิทธิที่จะได้รับแจ้งข้อมูล สิทธิที่จะเข้าถึงข้อมูล รวมถึงสิทธิที่จะแก้ไข ลบ หรือจำกัดการประมวลผลข้อมูลส่วนบุคคล อีกทั้ง ควรบัญญัติเหตุแห่งการปฏิเสธให้ชัดเจน เพื่อลดอำนาจดุลพินิจในการปฏิเสธหรือดำเนินการให้เป็นไปตามสิทธิของเจ้าของข้อมูล

อย่างไรก็ดี ด้วยข้อจำกัดที่สืบสวนและสอบสวนคดีอาญาไม่อาจดำเนินการด้วยความโปร่งใสต่อเจ้าของข้อมูลได้โดยบริบูรณ์ ในการปฏิเสธการใช้สิทธิ จึงควรบัญญัติข้อยกเว้นไม่ให้หน่วยงานหรือเจ้าหน้าที่รัฐต้องให้เหตุผลในการปฏิเสธโดยละเอียด หากการให้เหตุผลดังกล่าวจะส่งผลกระทบต่อการป้องกันและปราบปรามอาชญากรรม และด้วยข้อจำกัดข้างต้น ผู้เขียนจึงเห็นควรให้ประเทศไทยบัญญัติแนวทางการใช้สิทธิโดยอ้อมในชั้นสืบสวนและสอบสวนคดีอาญาเป็นการเฉพาะ โดยให้เจ้าของข้อมูลมีสิทธิในการร้องขอให้ศาลหรือคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตรวจสอบความชอบด้วยกฎหมายของการดำเนินงานในชั้นสืบสวนและสอบสวนคดีอาญา ทั้งในแง่ที่ว่าการประมวลผลข้อมูลส่วนบุคคลเป็นไปตามหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลที่กำหนดไว้หรือไม่ รวมถึงการปฏิเสธการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลนั้นมีความชอบธรรมหรือไม่ อย่างไร

ข้อเสนอแนะที่ 4 ประเทศไทยควรกำหนดให้การสืบสวนและสอบสวนคดีอาญาอยู่ภายใต้กลไกตรวจสอบความสอดคล้องกับหลักการคุ้มครองข้อมูลส่วนบุคคล เช่นเดียวกับการดำเนินงานประเภทอื่น โดยนอกเหนือจากคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เห็นว่าศาลก็เป็นองค์กรหลักอีกองค์กรหนึ่งที่สามารถควบคุมกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาควบคู่ไป

กับคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้ เพราะการควบคุมกำกับดูแลของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลจะเป็นในเชิงบังคับใช้นโยบาย มาตรการป้องกัน หรือปัญหาทางเทคนิค ในขณะที่ศาลจะเป็นเรื่องของขั้นตอนการดำเนินกระบวนการยุติธรรมทางอาญา ไม่ว่าจะเป็นการตรวจสอบเหตุหรือความจำเป็นในการออกหมายและคำสั่ง รวมถึงการกำหนดเงื่อนไขการใช้อำนาจเพิ่มเติม เป็นต้น

สุดท้าย ในกรณีที่มีการฝ่าฝืนหลักเกณฑ์และวิธีการคุ้มครองข้อมูลส่วนบุคคลตามที่กำหนดในกฎกระทรวงหรือระเบียบ ก็ควรมีบทกำหนดความรับผิดและโทษ เพื่อให้เกิดสภาพบังคับของกฎหมายลำดับรองดังกล่าว นอกจากนี้ ประเทศไทยควรพิจารณาบัญญัติข้อกำหนดการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศเพิ่มเติม โดยอาจนำแนวทางตาม LED มาบัญญัติไว้ในกฎหมายว่าด้วยความร่วมมือทางอาญาของประเทศไทยได้ เพื่อยกระดับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลในอนาคต

กล่าวโดยสรุป จะเห็นได้ว่าข้อเสนอแนะของผู้เขียนเป็นเพียงแนวทางเบื้องต้นในการกำหนดเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา แต่องค์ความรู้สำคัญที่เกิดขึ้นจากการศึกษาวิจัยครั้งนี้ คือการแสดงให้เห็นถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลจากการดำเนินงานในชั้นสืบสวนและสอบสวน และพิสูจน์ให้เห็นว่า “มีความเป็นไปได้ที่ในระบบกฎหมายไทยจะจัดให้มีการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญา” โดยรักษาสมดุลระหว่างการป้องปรามอาชญากรรมกับการคุ้มครองสิทธิส่วนบุคคล ซึ่งผู้เขียนคาดหวังว่าวิทยานิพนธ์ฉบับนี้จะกระตุ้นเตือนให้เกิดความตระหนักรู้ในสังคมไทยในแง่การคุ้มครองสิทธิความเป็นส่วนตัวในข้อมูลของประชาชนจากการดำเนินงานในกระบวนการยุติธรรมอาญา และสามารถนำไปปรับใช้เป็นแนวทางเพื่อคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาได้อย่างแท้จริง ตลอดจนสามารถใช้เพื่อต่อยอดในการพัฒนาระบบกฎหมายไทย ไม่ว่าจะเป็นการพัฒนากฎหมายวิธีพิจารณาความอาญาให้มีมีความสอดคล้องกับหลักสิทธิมนุษยชนมากยิ่งขึ้น หรือพัฒนากฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยใช้องค์ความรู้ที่ได้จากวิทยานิพนธ์นี้เป็นพื้นฐานในการกำหนดแนวทางการคุ้มครองข้อมูลส่วนบุคคลในชั้นสืบสวนและสอบสวนคดีอาญาเป็นรายกิจกรรม หรือเป็นพื้นฐานในการพิจารณาความเหมาะสมของการคุ้มครองข้อมูลส่วนบุคคลในการดำเนินงานอื่น ๆ นอกเหนือการสืบสวนและสอบสวนคดีอาญา เพราะหากมีความจำเป็น ประเทศไทยย่อมสามารถกำหนดหลักเกณฑ์เฉพาะหรือข้อยกเว้นรายกรณีให้เหมาะสมกับการดำเนินงานแต่ละประเภทได้ โดยไม่จำเป็นต้องยกเว้นไม่ให้นำกฎหมายคุ้มครองข้อมูลส่วนบุคคลมาใช้บังคับโดยสิ้นเชิง เพื่อที่ว่าอย่างน้อยที่สุด หลักประกันสิทธิความเป็นส่วนตัวในข้อมูลของประชาชนชาวไทยจะได้รับการคุ้มครองตามกฎหมายต่อไป

บรรณานุกรม

Council of Europe. "Practical Guide on the Use of Personal Data in the Police Sector."

Drechsler, L. Comparing Led and Gdpr Adequacy: One Standard Two Systems. Global Privacy Law Review 1, 2 (2020): 93-103.

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."

———. "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."

———. "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."

European Data Protection Supervisor. "Opinion 6/2015 a Further Step Towards Comprehensive Eu Data Protection: Edps Recommendations on the Directive for Data Protection in the Police and Justice Sectors."

European Parliament. "A Comparison between Us and Eu Data Protection Legislation for Law Enforcement." 2015.

Ferguson, A. G. Big Data and Predictive Reasonable Suspicion. University of Pennsylvania Law Review 163, 2 (January 2015): 327-410.

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.

———. "An Overview of the Data Protection Act 2018."

"Investigatory Powers Act 2016 ".

"Iordachi and Others V. Moldova ". European Court of Human Rights, 2009.

Leiser, M., and Custers, B. The Law Enforcement Directive: Conceptual Challenges of Eu Directive 2016/680. European Data Protection Law Review 5, 3 (October

2019): 367-378.

Murphy, E. The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions. Michigan Law Review 111, 4 (2013): 485-546.

National Institute of Standards and Technology. "National Institute of Standards and Technology (Nist Special Publication 800-122) Guide to Protecting the Confidentiality of Personally Identifiable Information (Pii)." 2010.

Packer, H. L. Two Models of the Criminal Process. University of Pennsylvania Law Review 113, 1 (November 1964): 1-68.

Salami, E. "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.

The Article 29 Working Party. "Opinion 4/2007 on the Concept of Personal Data, at Iii. Analysis of the Definition of “Personal Data” According to the Data Protection Directive."

UK Department for Digital Culture Media & Sport. "Explanatory Framework for Adequacy Discussion, Section F: Law Enforcement." 2020.

กรศุทธิ์ ขอพ่วงกลาง และวัฒนกร อุทัยวิวัฒน์กุล. สรุปสาระสำคัญจากเสวนาวิชาการ หัวข้อ "ลบประวัติ ล้างความผิด คืนชีวิตด้วยสิทธิตามกฎหมาย" [ออนไลน์]. 2563. แหล่งที่มา: https://www.law.tu.ac.th/seminar-summary-deletion-of-criminal-records/ [เข้าถึงเมื่อ 23 กันยายน]

กลุ่มงานตรวจสอบและควบคุมมาตรฐานทางเทคโนโลยี กองบังคับการสนับสนุนทางเทคโนโลยี สำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานตำรวจแห่งชาติ. "เอกสารประกอบการเตรียมความพร้อม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562."

กิตติพงษ์ กมลธรรมวงศ์. การคุ้มครองข้อมูลข่าวสารส่วนบุคคลในระบบกฎหมายไทย : ปัญหาและแนวทางการแก้ไข. นิติศาสตร์มหาบัณฑิต, คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์. 2549.

เกียรติขจร วัจนะสวัสดิ์. คำอธิบาย หลักกฎหมายวิธีพิจารณาความอาญา ว่าด้วย การดำเนินคดีในขั้นตอนก่อนการพิจารณา. พิมพ์ครั้งที่ 7. กรุงเทพฯ: หจก. สำนักพิมพ์ พลสยาม พริ้นติ้ง, 2558.

คณาธิป ทองรวีวงศ์. "การปฏิรูปกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อเข้าสู่ประชาคมอาเซียน." 2560.

———. คำอธิบาย หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล. พิมพ์ครั้งที่ 2. กรุงเทพฯ: นิติธรรม, 2565.

———. มาตรการทางกฎหมายในการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัวของผู้ถูกดักฟังการสื่อสารข้อมูล. วารสารกระบวนการยุติธรรม 8, 1 (2556).

———. สิทธิในข้อมูลส่วนบุคคลที่ไม่ได้รับการคุ้มครองตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 : การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามกฎหมายเกี่ยวกับความมั่นคงของรัฐ. วารสารกฎหมายสิทธิมนุษยชน 1, 1 (มกราคม - เมษายน 2563): 45-72.

โครงการอินเทอร์เน็ตเพื่อกฎหมายประชาชน (iLaw). ย้อนดู "การเยี่ยมบ้าน" นักกิจกรรมในยุค คสช. กับคำถามถึงสถานะทางกฎหมาย [ออนไลน์]. 2562. แหล่งที่มา: https://freedom.ilaw.or.th/node/710?fbclid=IwAR1HHjIRR5QEBC [เข้าถึงเมื่อ 20 กันยายน 2564]

———. แกะรอยการสร้างความกลัว: สรุปการคุกคามเยาวชน-แกนนำจัดชุมนุม ก.ค.-ส.ค.63 [ออนไลน์]. 2563. แหล่งที่มา: https://freedom.ilaw.or.th/node/842 [เข้าถึงเมื่อ 2564, 20 กันยายน]

———. บันทึกการคุกคามนักกิจกรรม นักเคลื่อนไหว ก่อนเวทีรับฟังความคิดเห็นสร้างนิคมอุตสาหกรรมจะนะ [ออนไลน์]. 2563. แหล่งที่มา: https://freedom.ilaw.or.th/node/831 [เข้าถึงเมื่อ 20 กันยายน]

จันทจิรา เอี่ยมมยุรา. การคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย. วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ 34, 4 (ธันวาคม 2547): 627-652.

ณรงค์ ใจหาญ. หลักกฎหมายวิธีพิจารณาความอาญา เล่ม 1. พิมพ์ครั้งที่ 14. กรุงเทพฯ: วิญญูชน, 2565.

ธานิศ เกศวพิทักษ์. คำอธิบาย ประมวลกฎหมายวิธีพิจารณาความอาญา เล่ม 1. พิมพ์ครั้งที่ 16. กรุงเทพฯ: สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา, 2564.

นคร เสรีรักษ์. ความเป็นส่วนตัวภายใต้รัฐธรรมนูญฉบับใหม่ "ต้องจับตา" [ออนไลน์]. 2559. แหล่งที่มา: https://ilaw.or.th/node/4255 [เข้าถึงเมื่อ 23 กันยายน 2564]

———. ความเป็นส่วนตัว: ความคิด ความรู้ ความจริง และพัฒนาการเรื่องการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย. พิมพ์ครั้งที่ 2. แพร่: พี.เพรส,, 2563.

บรรเจิด สิงคะเนติ. หลักความได้สัดส่วน (Principle of Proportionality) ในการตรวจสอบขอบเขตอำนาจรัฐ ตามมาตรา 23 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย (พุทธศักราช 2550).

กรุงเทพฯ: สำนักงานศาลรัฐธรรมนูญ, 2558.

บุญชู ณ ป้อมเพชร. "คำอธิบายกฎหมายข้อมูลข่าวสารของราชการ." PUB HTML5.

ปกป้อง ศรีสนิท. สิทธิมนุษยชนในกระบวนการยุติธรรมทางอาญา. กรุงเทพฯ: วิญญูชน, 2563.

ประชาไท. มูลนิธิผสานวัฒนธรรมเปิดสถิติ 'ปิดล้อมบังคับ-ข่มขู่เก็บ DNA' ชายแดนใต้ [ออนไลน์]. 2562. แหล่งที่มา: https://prachatai.com/journal/2019/12/85538 [เข้าถึงเมื่อ 19 กันยายน 2564]

ประพิณ ประดิษฐากร. "กฎหมายว่าด้วยการเข้าถึงและได้มาซึ่งข้อมูลของบุคคล และร่างพระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 131/2 ", 2554.

ประสิทธิ์ ปิวาวัฒนพานิช. กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกาและประเทศออสเตรเลีย. วารสารนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ 34, 4 (ธันวาคม 2547): 535-556.

ปรียาชาติ หาลำเจียก. การตรวจสอบและถ่วงดุล: ศึกษากรณีการสะกดรอยด้วยเครื่องมือสื่อสารโทรคมนาคมและเครื่องมืออิเล็กทรอนิกส์ตามพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 มาตรา 21. วิทยานิพนธ์นิติศาสตรมหาบัณฑิต , สาขากฎหมายอาญา คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์. 2557.

ปิติ เอี่ยมจำรูญลาภ. "กฎหมายเกี่ยวกับการกำหนดให้รัฐเข้าถึง หรือได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกัน : กรณีศึกษาประเทศสหรัฐอเมริกา." ธันวาคม 2561.

ปิยะบุตร บุญอร่ามเรือง และคณะ. แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล. กรุงเทพฯ: โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย, 2563.

มติชนออนไลน์. เปิดร่างป.วิอาญา'ดักฟัง' อัยการเทียบเนื้อหาพ.ร.บ. 7 ฉบับ ชี้ข้อมูลลักลั่น [ออนไลน์]. 2560. แหล่งที่มา: https://www.matichon.co.th/local/crime/news_552146 [เข้าถึงเมื่อ 20 กุมภาพันธ์ 2565]

———. 'ก้าวไกล-ก้าวหน้า' ฉะ watch list สุดอัปยศ ตีตรา ปชช.เป็นศัตรู [ออนไลน์]. 2564. แหล่งที่มา: www.matichon.co.th/politics/news_2876820 [เข้าถึงเมื่อ 2564, 20 กันยายน]

วิริยะ รามสมภพ. "ความสัมพันธ์เชิงวิเคราะห์ของร่างพระราชบัญญัติคุ้มครองข้อมูลข่าวสารส่วนบุคคล พ.ศ. ... กับ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540." สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ, 2562.

ศักดา เตชะเกรียงไกรและคณะ. คู่มือการสืบสวน [ออนไลน์]. แหล่งที่มา: http://wutthi.central.police.go.th]

ศุภัสรา ชัยพิพัฒน์. การกำกับดูแลของอาเซียนด้านความเป็นส่วนตัวของข้อมูล: ความท้าทายของภูมิภาคต่อการคุ้มครองความเป็นส่วนตัวของข้อมูลและข้อมูลส่วนบุคคลในไซเบอร์สเปซ. สาร

นิพนธ์ปริญญามหาบัณฑิต สาขาวิชาความสัมพันธ์ระหว่างประเทศ ภาควิชาความสัมพันธ์ระหว่างประเทศ คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. 2562.

สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์. "รายงานผลการดำเนินการ โครงการพัฒนามาตรการในการดำเนินการ การพิจารณาความเหมาะสม ความเป็นไปได้ เพื่อจัดทำแนวทางขั้นตอนและวิธีการในการเข้าร่วมหรือทำความตกลงตามกรอบว่าด้วยการคุ้มครองข้อมูลความเป็นส่วนตัวของ Apec." คณะกรรมการข้อมูลข่าวสารของราชการ, ธันวาคม 2557.

สปริงนิวส์. ถึงเป็นตำรวจทำผิดก็ต้องโดนจับ ! รวบสารวัตรเปิดเพจรับจ้างเช็คทะเบียนราษฎร์ [ออนไลน์]. 2561. แหล่งที่มา: https://www.springnews.co.th/news/397608 [เข้าถึงเมื่อ 24 กันยายน]

สมัคร เชาวภานันท์. หลักสิทธิมนุษยชนกับการค้นหาความจริงในคดีอาญา. วารสารศาลรัฐธรรมนูญ 20, 59 (พฤษภาคม - สิงหาคม 2561): 214-232.

สาวตรี สุขศรี. กฎหมายว่าด้วยอาชญากรรมคอมพิวเตอร์และอาชญากรรมไซเบอร์. กรุงเทพฯ: โครงการตำราและเอกสารประกอบการสอน คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2563.

สาวออฟฟิศ (Nisit Recorder). มูลนิธิผสานวัฒนธรรม, “จังหวัดชายแดนใต้: ห้องทดลอง Bio-metric ของรัฐไทย [ออนไลน์]. 2562. แหล่งที่มา: https://crcfthailand.org/2020/09/06/จังหวัดชายแดนใต้-ห้องท/ [เข้าถึงเมื่อ 19 กันยายน 2564]

สำนักงานตำรวจแห่งชาติ. "คู่มือการฝึกอบรมข้าราชการตำรวจที่ปฏิบัติหน้าที่งานสืบสวนในสถานีตำรวจ พ.ศ. 2557."

อนุสิษฐ คุณากร และคณะ. การคุ้มครองข้อมูลส่วนบุคคลกับสังคมไทย. กรุงเทพฯ: สถาบันนโยบายการศึกษา ภายใต้มูลนิธิส่งเสริมนโยบายการศึกษา, 2563.

ประวัติผู้เขียน

ชื่อ-สกุล รติมา สุระรัตน์ชัย

วุฒิการศึกษา สำเร็จการศึกษานิติศาสตรบัณฑิต จากคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ สอบไล่ได้ความรู้ชั้นเนติบัณฑิต ในสมัยที่ 71 และผ่านหลักสูตรวิชาว่าความของสำนักฝึกอบรมวิชาว่าความแห่งสภาทนายความ รุ่นที่ 50 ต่อมา ได้เข้าศึกษาต่อปริญญามหาบัณฑิต หลักสูตรนิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย