บทความวิชาการ

ข้อเสนอแนะในการแก้ไขกฎหมายกรณีการใช้ปัญญาประดิษฐ์ในการประมวลผลข้อมูลส่วนบุคคล

วรวิทย์ กิติกุศล* และ พงษ์พิสิฐ วุฒิดิษฐโชติ
ภาควิชาการสื่อสารข้อมูลและเครือข่าย คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

* ผู้นิพนธ์ประสานงาน โทรศัพท์ 08 1556 5590 อีเมล: worawit55@hotmail.com DOI: 10.14416/j.kmutnb.2025.01.003
รับเมื่อ 22 สิงหาคม 2567 แก้ไขเมื่อ 11 ตุลาคม 2567 ตอบรับเมื่อ 27 พฤศจิกายน 2567 เผยแพร่ออนไลน์ 27 มกราคม 2568

บทคัดย่อ

บทความวิชาการนี้มุ่งเน้นการวิเคราะห์กรอบกฎหมายและแนวปฏิบัติของ GDPR และ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่เกี่ยวข้องกับการใช้ AI ในการคุ้มครองข้อมูลส่วนบุคคลการศึกษาเน้นการทำความเข้าใจถึงหลักการสำคัญของกฎหมายทั้งสองฉบับที่เกี่ยวข้องกับการประมวลผลข้อมูลโดย AI เช่น การตัดสินใจอัตโนมัติ (Automated Decision-Making) การประเมินผลกระทบด้านความเป็นส่วนตัว (Privacy Impact Assessment) และการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล บทความวิชาการนี้ยังได้รวบรวมแนวปฏิบัติและตัวอย่างการนำ AI ไปใช้ในบริบทที่ปลอดภัยและสอดคล้องกับกฎหมาย นอกจากนี้ยังนำเสนอแนวทางจากกฎหมาย GDPR และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในการลดความเสี่ยงและเพิ่มประสิทธิภาพในการคุ้มครองข้อมูลส่วนบุคคล รวมถึงการอภิปรายเกี่ยวกับความท้าทายและข้อจำกัดในการปรับใช้กฎหมายดังกล่าวในบริบทของประเทศไทย ซึ่งควรได้รับการปรับปรุงให้มีความชัดเจนและครอบคลุมการใช้ AI ในการประมวลผลข้อมูลมากยิ่งขึ้น โดยเฉพาะอย่างยิ่งในกรณีที่การตัดสินใจโดย AI อาจส่งผลกระทบต่อสิทธิของเจ้าของข้อมูลส่วนบุคคล ควรเพิ่มข้อกำหนดในการแจ้งเตือนและเปิดโอกาสให้เจ้าของข้อมูลส่วนบุคคลสามารถคัดค้านหรือขอให้มีการตรวจสอบการตัดสินใจโดยมนุษย์ได้

คำสำคัญ: ปัญญาประดิษฐ์ การคุ้มครองข้อมูลส่วนบุคคล GDPR PDPA การตัดสินใจอัตโนมัติ

การอ้างอิงบทความ: วรวิทย์ กิติกุศล และ พงษ์พิสิฐ วุฒิดิษฐโชติ, "ข้อเสนอแนะในการแก้ไขกฎหมายกรณีการใช้ปัญญาประดิษฐ์ในการประมวลผลข้อมูลส่วนบุคคล," *วารสารวิชาการพระจอมเกล้าพระนครเหนือ*, ปีที่ 35, ฉบับที่ 4, หน้า 1–8, เลขที่บทความ 254-187668, ต.ค.–ธ.ค. 2568.

Academic Article

Suggested Amendments to the Law Regarding the Use of Artificial Intelligence in Processing Personal Data

Worawit Kitikusoun* and Pongpisit Wuttidittachotti
Department of Digital Network and Information Security Management, Faculty of Information Technology and Digital Innovation, King Mongkut's University Of Technology North Bangkok, Bangkok, Thailand

* Corresponding Author, Tel. 08 1556 5590, E-mail: worawit55@hotmail.com DOI: 10.14416/j.kmutnb.2025.01.003
Received 22 August 2024; Revised 11 October 2024; Accepted 27 November 2024; Published online: 27 January 2025

Abstract

This academic article focuses on analyzing the legal frameworks and practices of the General Data Protection Regulation (GDPR) and Thailand's Personal Data Protection Act B.E. 2562 (2019) concerning the use of AI in personal data protection. The study emphasizes understanding the key principles of both laws related to data processing by AI, such as automated decision-making, privacy impact assessments, and the protection of data subjects' rights. The article compiles best practices and examples of the safe and lawful use of AI in various contexts. Furthermore, it presents approaches from the GDPR and Thailand's Personal Data Protection Act B.E. 2562 (2019) to mitigate risks and enhance the efficiency of personal data protection. It also discusses the challenges and limitations of implementing these laws within Thailand's context, suggesting the need for clearer and more comprehensive regulations to address AI-based data processing. Particular attention is given to cases where AI decision-making may impact the rights of data subjects. It recommends the inclusion of provisions requiring notification and providing opportunities for data subjects to object or request human review of AI decisions.

Keywords: Artificial Intelligence, Personal Data Protection, GDPR, PDPA, Automated Decision-Making

Please cite this article as: W. Kitikusoun and P. Wuttidittachotti, "Suggested amendments to the law regarding the use of artificial intelligence in processing personal data," *The Journal of KMUTNB*, vol. 35, no. 4, pp. 1–8, ID. 254-187668, Oct.–Dec. 2025 (in Thai).

1. บทนำ

การพัฒนาและการนำเทคโนโลยีปัญญาประดิษฐ์ (AI) มาใช้ได้เปลี่ยนแปลงวิธีการทำงานในหลายอุตสาหกรรม โดยส่งผลให้เกิดประสิทธิภาพและนวัตกรรมที่ก้าวหน้า อย่างไรก็ตาม การใช้งาน AI ที่ไม่ได้รับการกำกับดูแลอย่างเหมาะสมอาจก่อให้เกิดความเสี่ยงต่อการละเมิดข้อมูลส่วนบุคคลและสิทธิความเป็นส่วนตัว ซึ่งเป็นประเด็นที่สำคัญและส่งผลให้แต่ละประเทศได้พิจารณากฎหมายและแนวทางปฏิบัติเพื่อควบคุมการใช้ AI ให้เป็นไปตามมาตรฐานที่กำหนด

ในสหภาพยุโรป กฎระเบียบการคุ้มครองข้อมูลทั่วไป (General Data Protection Regulation; GDPR) ได้กลายเป็นมาตรฐานสากลในการคุ้มครองข้อมูลและความเป็นส่วนตัว กฎหมายนี้กำหนดแนวทางที่เข้มงวดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งในระบบที่ใช้การตัดสินใจโดยอัตโนมัติ ซึ่งมักอาศัย AI เป็นส่วนหนึ่งในการดำเนินงาน การที่ GDPR ให้ความสำคัญกับการประเมินผลกระทบด้านความเป็นส่วนตัว (Privacy Impact Assessment) และการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลได้กลายเป็นต้นแบบสำหรับกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศอื่น ๆ รวมถึงพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ของประเทศไทยด้วย [1]–[3] ซึ่งในประเทศสิงคโปร์ยังมีการพัฒนามาตรฐานและแนวทางสำหรับการใช้ AI อย่างปลอดภัย เช่น Model AI Governance Framework และยังกำหนดให้ระบบ AI ต้องมีความโปร่งใส (Transparency) และสามารถอธิบายการตัดสินใจได้ (Explainability) ซึ่งเป็นหลักการสำคัญในการสร้างความไว้วางใจในระบบ AI นอกจากนี้ AI ต้องคำนึงถึงสิทธิของเจ้าของข้อมูลส่วนบุคคลและไม่สร้างความเสียหายต่อสิทธิความเป็นส่วนตัวของบุคคล การใช้ AI ในสิงคโปร์จึงต้องปฏิบัติตามหลักการ Accountability ที่องค์กรผู้ใช้ AI ต้องรับผิดชอบต่อผลลัพธ์ที่เกิดขึ้นจากการตัดสินใจของ AI นอกจากนี้ กฎหมายยังให้ความสำคัญกับการใช้ AI ในการตัดสินใจอัตโนมัติ (Automated Decision-Making) โดยกำหนดให้ต้องมีมาตรการตรวจสอบความเป็นธรรมและลดความลำเอียง (Bias) ในการประมวลผลข้อมูล

บทความวิชาการนี้มุ่งเน้นการวิเคราะห์กรอบกฎหมายและแนวปฏิบัติที่เกี่ยวข้องกับการใช้ AI เพื่อคุ้มครองข้อมูลส่วนบุคคล โดยศึกษาการประยุกต์ใช้ GDPR และ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในการลดความเสี่ยงและสร้างความปลอดภัยในการใช้ AI นอกจากนี้ยังได้รวบรวมตัวอย่างกรณีศึกษาจากหลายประเทศเพื่อนำมาเสนอแนวทางปฏิบัติที่เหมาะสมในบริบทของประเทศไทย [4], [5]

2. ความรู้ที่เกี่ยวข้อง

การนำปัญญาประดิษฐ์มาใช้ในการประมวลผลข้อมูลส่วนบุคคลมีความสำคัญอย่างยิ่งในยุคดิจิทัล โดยเฉพาะในด้านการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายที่เกี่ยวข้อง เช่น GDPR ของสหภาพยุโรป และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act, B.E. 2562)

ของประเทศไทย GDPR ถือเป็นกฎหมายที่มีความเข้มงวดในการปกป้องสิทธิของเจ้าของข้อมูลส่วนบุคคล โดยมาตราสำคัญที่เกี่ยวข้องกับการประยุกต์ใช้ AI ได้แก่ มาตรา 5 ซึ่งกำหนดหลักการพื้นฐานในการประมวลผลข้อมูล เช่น ความชอบด้วยกฎหมาย ความเป็นธรรม และความโปร่งใส (Lawfulness, Fairness, and Transparency) มาตรา 13–14 เกี่ยวกับสิทธิในการรับรู้และการแจ้งเตือน (Right to be Informed) ที่กำหนดให้ผู้ควบคุมข้อมูลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงการประมวลผลข้อมูล รวมถึงการใช้ AI ในการตัดสินใจอัตโนมัติที่อาจส่งผลต่อเจ้าของข้อมูลส่วนบุคคล [1], [6], [7] นอกจากนี้ มาตรา 35 ของ GDPR ยังระบุให้ต้องมีการประเมินผลกระทบด้านความเป็นส่วนตัว (Data Protection Impact Assessment; DPIA) เมื่อมีการนำ AI มาใช้ในกระบวนการที่มีความเสี่ยงสูง เช่น การตัดสินใจที่เกี่ยวข้องกับการอนุมัติสินเชื่อหรือการคัดกรองผู้สมัครงาน [3], [5], [8]

ในขณะที่ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีหลักการที่คล้ายคลึงกับ GDPR แต่ยังมีข้อจำกัดในหลายด้านที่เกี่ยวข้องกับการใช้ AI ในการประมวลผลข้อมูลส่วนบุคคล พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ระบุให้ผู้ควบคุมข้อมูลต้องแจ้งให้

เจ้าของข้อมูลส่วนบุคคลทราบถึงการนำข้อมูลไปใช้ แต่ไม่ได้ระบุถึงการแทรกแซงของมนุษย์ในกรณีที่มีการใช้ AI ในการตัดสินใจเหมือนกับ GDPR และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังขาดข้อบังคับที่ชัดเจนเกี่ยวกับการประเมินผลกระทบด้านความเป็นส่วนตัว (Privacy Impact Assessment) ซึ่งเป็นองค์ประกอบสำคัญในการประเมินความเสี่ยงจากการใช้ AI ในการประมวลผลข้อมูลส่วนบุคคล นอกจากนี้ แนวคิด Privacy by Design ระบบต้องสามารถป้องกันการรั่วไหลของข้อมูลส่วนบุคคลและมีมาตรการรักษาความปลอดภัยที่เหมาะสม เช่น การเข้ารหัสข้อมูล (Encryption) และการไม่อนุญาตให้เข้าถึงข้อมูลเกินความจำเป็นและ Privacy by Default ระบบ หรือบริการต้องตั้งค่าให้มีการปกป้องข้อมูลส่วนบุคคลมากที่สุด เช่น ไม่แชร์ข้อมูลส่วนบุคคลไปยังบุคคลที่สามโดยอัตโนมัติ ผู้ใช้ต้องเลือกเปิดเผยข้อมูลเท่าที่จำเป็นเท่านั้นซึ่งเป็นหลักการที่ GDPR กำหนดให้เป็นมาตรฐานในการออกแบบระบบเพื่อคุ้มครองข้อมูลส่วนบุคคลตั้งแต่ต้น แต่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังคงขาดกลไกในการบังคับใช้ในลักษณะเดียวกัน [3], [9], [10] การพัฒนาพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จึงควรมุ่งเน้นไปที่การเพิ่มเติมข้อกำหนดที่ชัดเจนและครอบคลุมเกี่ยวกับการใช้ AI รวมถึงการบูรณาการแนวคิดการคุ้มครองข้อมูลตั้งแต่ขั้นตอนการออกแบบระบบ เพื่อเสริมสร้างมาตรฐานการคุ้มครองข้อมูลในประเทศไทยให้เทียบเท่ากับสากล [11]–[13]

การละเมิดกฎหมายคุ้มครองข้อมูลส่วนบุคคลทั้งภายใต้ GDPR และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สะท้อนให้เห็นถึงความท้าทายในการนำ AI มาใช้ ตัวอย่างหนึ่งที่เป็นที่รู้จักภายใต้ GDPR คือ กรณี Clearview AI ซึ่งเป็นบริษัทที่พัฒนาเทคโนโลยีจดจำใบหน้า (Facial Recognition) โดยรวบรวมภาพใบหน้าของผู้คนจากแหล่งออนไลน์โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล บริษัทถูกหน่วยงานคุ้มครองข้อมูลในหลายประเทศในยุโรปสอบสวนและถูกตัดสินว่าละเมิดมาตรา 5 และมาตรา 6 ของ GDPR ที่กำหนดให้การประมวลผลข้อมูลต้องได้รับความยินยอมจากเจ้าของข้อมูลและเป็นไปอย่างถูกต้องตามกฎหมาย [8], [12] ในกรณีนี้ Clearview AI ถูกปรับในหลายประเทศ เช่น ประเทศกรีซที่สั่งปรับเป็นเงิน 20 ล้านยูโร และสั่งให้ลบข้อมูลที่ได้มาโดยไม่ชอบด้วยกฎหมาย [14] นอกจากนี้ ยังมีกรณีในอิตาลีที่ตรวจพบว่า ระบบการตรวจสอบออนไลน์ของมหาวิทยาลัยสำหรับการสอบออนไลน์มีการเก็บข้อมูลและประมวลผลโดยไม่ได้รับความยินยอมจากนักศึกษา ทำให้หน่วยงานคุ้มครองข้อมูลส่วนบุคคลของอิตาลีสั่งปรับมหาวิทยาลัยดังกล่าว [13], [15] และ กรณี SCHUFA (2023) เป็นคดีสำคัญที่ศาลยุติธรรมแห่งสหภาพยุโรป (CJEU) ตัดสินเกี่ยวกับการใช้ AI ในการคำนวณคะแนนเครดิตของลูกค้าธนาคาร ซึ่งศาลได้ระบุว่าการใช้ AI ในการตัดสินใจโดยอัตโนมัติเกี่ยวกับเครดิตต้องปฏิบัติตามข้อกำหนดของ GDPR โดยเฉพาะในมาตรา 22 ซึ่งเกี่ยวข้องกับการตัดสินใจอัตโนมัติ ศาลยังชี้ว่าในการตัดสินใจสุดท้าย ผู้ตรวจสอบของมนุษย์ต้องมีส่วนร่วมอย่างมีความหมายในการทบทวนผลลัพธ์ของ AI [16] ซึ่งเมื่อพิจารณา พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เกี่ยวกับเทคโนโลยีใหม่ เช่น ข้อมูลชีวมิติและ Mac Address ชี้ให้เห็นถึงความจำเป็นในการปรับปรุงกฎหมายให้สอดคล้องกับเทคโนโลยีในปัจจุบัน [17]

ในปัจจุบันประเทศไทยมีการบังคับใช้กฎหมาย แต่มีการละเมิดที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมอยู่บ้าง ซึ่งส่วนใหญ่เกิดจากการเก็บข้อมูลลูกค้าในลักษณะที่ไม่โปร่งใส หรือการใช้ข้อมูลเพื่อวัตถุประสงค์อื่นนอกเหนือจากที่ได้แจ้งไว้ การขาดมาตรการการควบคุมที่เข้มงวดและการไม่ตระหนักถึงข้อกำหนดของกฎหมายใหม่ทำให้เกิดการละเมิดบ่อยครั้ง ซึ่งชี้ให้เห็นถึงความจำเป็นในการเสริมสร้างกลไกการบังคับใช้กฎหมายและการให้ความรู้แก่ผู้ควบคุมข้อมูลในทุกภาคส่วน [4], [10], [18]

นอกจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลแล้ว ประเทศไทยยังมีกฎหมายและแนวทางในการกำกับดูแลการใช้เทคโนโลยีปัญญาประดิษฐ์ (AI) ซึ่งเกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล กฎหมายและกรอบนโยบายเหล่านี้มีบทบาทสำคัญในการสนับสนุนการพัฒนา AI อย่างปลอดภัยและเป็นธรรม โดยเฉพาะในบริบทที่ AI ถูกนำมาใช้ในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว หนึ่งในนั้น คือ

กรอบนโยบายปัญญาประดิษฐ์แห่งชาติ พ.ศ. 2564–2570 ซึ่งถูกพัฒนาขึ้นโดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (DE) นโยบายนี้มุ่งเน้นการส่งเสริมการพัฒนา AI อย่างมีจริยธรรมและสอดคล้องกับหลักการความปลอดภัยและความเป็นส่วนตัว [9], [11], [19] นอกจากนี้ นโยบายยังครอบคลุมถึงการวางแนวทางในการใช้ AI อย่างรับผิดชอบเพื่อป้องกันการละเมิดสิทธิของบุคคล ความเชื่อมโยงระหว่างกฎหมาย AI ของประเทศไทยกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อยู่ในประเด็นการใช้ AI ในการประมวลผลข้อมูลส่วนบุคคล โดยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นกฎหมายหลักที่กำกับดูแลเรื่องการคุ้มครองข้อมูลส่วนบุคคล ซึ่งมีความเกี่ยวข้องโดยตรงเมื่อ AI ถูกนำมาใช้ในการตัดสินใจอัตโนมัติ เช่น การพิจารณาสินเชื่อ การตรวจสอบประวัติทางการเงิน หรือการคัดกรองผู้สมัครงาน ที่อาจส่งผลกระทบต่อสิทธิและความเป็นส่วนตัวของบุคคล [10]

ซึ่งเห็นควรเพิ่มสิทธิในการคัดค้านการประมวลผลโดย Automated Decision Making และการประเมินผลกระทบด้านความเป็นส่วนตัว และการบูรณาการแนวคิดการคุ้มครองข้อมูลตั้งแต่ขั้นตอนการออกแบบระบบ [9], [15], [19]

การพัฒนากฎหมายพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ให้สอดคล้องกับกรอบนโยบาย AI ของประเทศไทยจะช่วยให้การใช้ AI เป็นไปอย่างรับผิดชอบและมีความโปร่งใสมากขึ้น ซึ่งจะเป็นการยกระดับการคุ้มครองข้อมูลส่วนบุคคลให้ครอบคลุมทั้งด้านกฎหมายและนโยบายเชิงกลยุทธ์ที่สนับสนุนการพัฒนา AI อย่างยั่งยืนและเป็นธรรมในบริบทของประเทศไทย [14] การพัฒนาจึงควรมุ่งเน้นไปที่การเพิ่มเติมข้อกำหนดที่ชัดเจนและครอบคลุมเกี่ยวกับการใช้ AI รวมถึงการบูรณาการแนวคิดการคุ้มครองข้อมูลตั้งแต่ขั้นตอนการออกแบบระบบ เพื่อเสริมสร้างมาตรฐานการคุ้มครองข้อมูลในประเทศไทยให้ทัดเทียมกับสากล การพัฒนานี้สามารถทำได้โดยการปรับปรุงและเพิ่มเติมมาตราที่เกี่ยวข้องในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ดังนี้

การเพิ่มข้อกำหนดเกี่ยวกับการตัดสินใจอัตโนมัติในมาตรา 23 (หน้าที่ของผู้ควบคุมข้อมูล) มาตรา 23 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้ผู้ควบคุมข้อมูลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบเมื่อมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล อย่างไรก็ตาม มาตรานี้ยังขาดข้อกำหนดเกี่ยวกับการตัดสินใจอัตโนมัติ (Automated Decision-Making) ที่อาจส่งผลกระทบต่อสิทธิของเจ้าของข้อมูลส่วนบุคคล เช่น การตัดสินใจด้านสินเชื่อ การประเมินประสิทธิภาพ หรือการวิเคราะห์พฤติกรรม การปรับปรุงควรรวมถึงการเพิ่มข้อกำหนดที่ระบุว่าหากมีการใช้ AI ในการตัดสินใจที่ส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลต้องแจ้งให้ทราบถึงการใช้ AI ดังกล่าว พร้อมทั้งเปิดโอกาสให้เจ้าของข้อมูลส่วนบุคคล Data Subject สามารถคัดค้านหรือขอให้มีการตรวจสอบการตัดสินใจโดยมนุษย์ได้ เช่นเดียวกับที่ระบุไว้ใน GDPR มาตรา 22 [17]

การกำหนดมาตรฐานด้านจริยธรรม (AI Ethics) เป็นการวางหลักเกณฑ์ในการพัฒนาและใช้งานปัญญาประดิษฐ์ เพื่อให้มั่นใจว่าการใช้งาน AI จะเป็นไปอย่างมีความรับผิดชอบและคำนึงถึงผลกระทบทางสังคม หนึ่งในหลักการสำคัญ คือ ความโปร่งใส (Transparency) ซึ่งหมายถึงการที่ผู้ใช้งานสามารถเข้าใจได้ว่า AI ตัดสินใจอย่างไร และทำไมถึงได้ผลลัพธ์นั้น การสร้างความโปร่งใสช่วยเพิ่มความไว้วางใจและลดความเข้าใจผิด นอกจากนี้ยังต้องคำนึงถึงความยุติธรรม (Fairness) โดยต้องป้องกันไม่ให้ AI มีความลำเอียง (Bias) ต่อกลุ่มบุคคลหรือข้อมูลใด ๆ เพื่อให้เกิดความเป็นธรรมในทุกกระบวนการตัดสินใจของ AI มาตรฐานด้านจริยธรรมยังรวมถึง ความรับผิดชอบ (Accountability) ที่กำหนดให้ผู้พัฒนาหรือองค์กรที่ใช้ AI ต้องรับผิดชอบต่อผลกระทบที่เกิดขึ้นจากการใช้ AI รวมถึงความเป็นส่วนตัว (Privacy) ซึ่งต้องมีการปกป้องข้อมูลส่วนบุคคลในทุกขั้นตอนของการประมวลผลเพื่อป้องกันการละเมิดข้อมูล เช่นเดียวกับกฎหมาย Personal Data Protection Act (PDPA) ของประเทศสิงคโปร์

การบังคับใช้การประเมินผลกระทบด้านความเป็นส่วนตัว ใน มาตรา 30 (มาตรการรักษาความปลอดภัยของข้อมูล

ส่วนบุคคล) ในปัจจุบัน มาตรา 30 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้ผู้ควบคุมข้อมูลต้องมีมาตรการรักษาความปลอดภัยที่เหมาะสม แต่ไม่ได้ระบุรายละเอียดเกี่ยวกับการประเมินผลกระทบด้านความเป็นส่วนตัว (Privacy Impact Assessment; PIA) การปรับปรุงควรรวมถึงการบังคับให้มีการดำเนินการประเมิน PIA เมื่อมีการใช้ AI ในการประมวลผลข้อมูลที่มีความเสี่ยงสูง เช่น การคัดกรองผู้สมัครงานหรือการวิเคราะห์พฤติกรรมการบริโภค [20] เพื่อให้สามารถระบุความเสี่ยงที่อาจเกิดขึ้นและจัดทำมาตรการป้องกันได้อย่างมีประสิทธิภาพ เช่นเดียวกับที่กำหนดไว้ใน GDPR มาตรา 35 [19]

การบูรณาการแนวคิด Privacy by Design และ Privacy by Default ในมาตรา 37 (หน้าที่ของผู้ควบคุมข้อมูลในการรักษาความปลอดภัยข้อมูล) มาตรา 37 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เน้นการกำหนดให้ผู้ควบคุมข้อมูลมีหน้าที่รักษาความปลอดภัยของข้อมูลส่วนบุคคล แต่ยังขาดแนวทางที่ชัดเจนเกี่ยวกับการบูรณาการการคุ้มครองข้อมูลเข้าไปในกระบวนการพัฒนาและออกแบบระบบตั้งแต่เริ่มต้น การเพิ่มเติมควรรวมถึงการกำหนดให้มีการใช้แนวคิด Privacy by Design และ Privacy by Default เช่นเดียวกับ GDPR เพื่อให้มั่นใจว่าระบบที่ใช้ AI จะมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่ถูกออกแบบมาอย่างเหมาะสมตั้งแต่ขั้นตอนการวางแผนพัฒนา โดยระบุให้ผู้ควบคุมข้อมูลต้องคำนึงถึงความปลอดภัยของข้อมูลและสิทธิของเจ้าของข้อมูลส่วนบุคคลในทุกขั้นตอนของการพัฒนาระบบ [18]

การกำหนดหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูล (Data Protection Officer; DPO) อย่างชัดเจนใน มาตรา 41 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้ผู้ควบคุมข้อมูลที่มีการประมวลผลข้อมูลในปริมาณมากต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูล แต่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังขาดความชัดเจนในเรื่องบทบาทและความรับผิดชอบของ DPO ในบริบทของการใช้ AI การปรับปรุงในส่วนนี้ควรระบุให้ DPO มีหน้าที่เฉพาะในการตรวจสอบและกำกับดูแลการใช้ AI ในการประมวลผลข้อมูลส่วนบุคคล เช่น การทบทวนการประเมินผลกระทบด้านความเป็นส่วนตัว (DPIA) การตรวจสอบการปฏิบัติตามกฎหมาย และการให้คำปรึกษาเกี่ยวกับการใช้ AI อย่างถูกต้องตามกฎหมาย [21]

การปรับปรุงและเพิ่มเติมข้อกำหนดเหล่านี้จะช่วยให้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สามารถรองรับการประยุกต์ใช้ AI ในการประมวลผลข้อมูลส่วนบุคคลได้อย่างครอบคลุมและมีประสิทธิภาพมากยิ่งขึ้น ทำให้มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยมีความเทียบเท่ากับ GDPR และมาตรฐานสากลอื่น ๆ [2], [14], [19] แต่การบังคับใช้กฎหมายในประเทศไทยยังเผชิญกับความท้าทายจากการขาดบุคลากรที่มีความเชี่ยวชาญและทรัพยากรที่จำเป็น รวมถึงการขาดมาตรฐานที่ชัดเจนในการใช้ AI อย่างมีจริยธรรม ภาคเอกชนยังขาดความพร้อมในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างครบถ้วน การประสานงานระหว่างหน่วยงานรัฐและภาคเอกชนยังมีความซับซ้อน ทำให้การบังคับใช้กฎหมายเป็นไปได้อย่างล่าช้า

3. อภิปรายผลและสรุป

ในอนาคตการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยควรได้รับการเสริมสร้างให้มีความแข็งแกร่งและทันสมัยยิ่งขึ้น เพื่อตอบสนองต่อการเปลี่ยนแปลงทางเทคโนโลยี โดยเฉพาะการพัฒนาและการใช้ AI ที่มีความซับซ้อนเพิ่มขึ้น หนึ่งในสิ่งที่ควรเพิ่มเติม คือ การออกกฎหมายหรือแนวทางเฉพาะสำหรับการใช้งาน AI ซึ่งครอบคลุมถึงการกำหนดมาตรฐานด้านจริยธรรม (AI Ethics) และข้อกำหนดทางเทคนิคที่เกี่ยวข้อง เช่น การใช้ระบบ AI ที่มีความโปร่งใส สามารถอธิบายการตัดสินใจได้ (Explainability) และมีมาตรการในการป้องกันความลำเอียง (Bias) ที่อาจเกิดขึ้นจากการประมวลผลข้อมูล

นอกจากนี้ ควรมีการพัฒนาระบบการกำกับดูแลที่สามารถติดตามและประเมินผลการใช้ AI อย่างต่อเนื่อง รวมถึงการกำหนดบทบาทของเจ้าหน้าที่คุ้มครองข้อมูลให้มีอำนาจในการตรวจสอบการใช้ AI ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลมากขึ้น การเสริมสร้างการให้ความรู้แก่ประชาชนเกี่ยวกับสิทธิของตนตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

พ.ศ. 2562 และการประยุกต์ใช้ AI ยังเป็นอีกหนึ่งแนวทางที่สำคัญ เพื่อให้เจ้าของข้อมูลส่วนบุคคลมีความเข้าใจและสามารถปกป้องสิทธิของตนเองได้อย่างมีประสิทธิภาพ

การนำแนวคิดเกี่ยวกับการคุ้มครองข้อมูลเชิงรุก (Proactive Data Protection) มาใช้ตั้งแต่ขั้นตอนการพัฒนาเทคโนโลยี AI และการกำหนดให้มีการประเมินผลกระทบ (DPIA) จากการใช้ AI อย่างสม่ำเสมอเป็นสิ่งที่ควรเพิ่มเติม เพื่อให้มาตรการการคุ้มครองข้อมูลสามารถปรับตัวตามความท้าทายใหม่ ๆ ได้อย่างทันท่วงที การบูรณาการเหล่านี้จะช่วยให้ประเทศไทยสามารถรักษามาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เทียบเท่ากับมาตรฐานสากลในอนาคต และสามารถเผชิญกับความซับซ้อนทางเทคโนโลยีได้อย่างมีประสิทธิภาพ

เอกสารอ้างอิง

[1] I. Calzada, "Technological sovereignty: Protecting citizens' digital rights in the AI-driven and post-GDPR algorithmic and city-regional european realm," *Regions eZine*, no.4, 2019, doi: 10.1080/13673882.2018.00001038

[2] D. Torrea, S. Abualhaija, M. Sabetzadehand, L. Briand, K. Baetens, P. Goes, and S. Forastier, "An AI-Assisted approach for checking the completeness of privacy policies against GDPR," *Presented at IEEE International Conference on Requirements Engineering*, vol. 2020, pp136–146, 2020, doi: 10.1109/RE48521.2020.00025

[3] M. Lippi, P. Przemysław, C. Giuseppe, L. Francesca, M. Hans, S. Giovanni, and T. Paolo, "CLAUDETTE: An automated detector of potentially unfair clauses in online terms of service. *Artificial Intelligence and Law*, vol. 27, no. 2, pp. 117–139, Jun. 2019, doi: 10.1007/s10506-019-09243-2

[4] M. Butterworth, "The ICO and artificial intelligence: The role of fairness in the GDPR framework," *Computer Law and Security Review*, vol. 34, no. 2, pp. 257–268, Apr. 2018, doi: 10.1016/j.clsr.2018.01.004

[5] A. J. Wulf and O. Seizov, "Please understand we cannot provide further information: Evaluating content and transparency of GDPR-mandated AI disclosures," *AI & Society*, vol. 39, pp. 235–256, 2020, doi: 10.1007/s00146-022-01424-z

[6] F. Lore`, P. Basile, A. Appice, M. de Gemmis, D. Malerba, and G. Semeraro, "An AI framework to support decisions on GDPR compliance," *Journal of Intelligent Information Systems*. vol. 60, pp. 541–568, Mar. 2023, doi: 10.1007/s10844-023-00782-4

[7] F. Kakava, "The 'Nebulous' concept of detriment under recital 42 of the GDPR," *SSRN Electronic Journal*, vol. 5, no. 4, pp. 527–540, 2019.

[8] F. Ufert, "Insight AI regulation through the lens of fundamental rights: How well does the GDPR address the challenges posed by AI?," *European Papers*, vol. 5, no. 2, pp. 1087–1097, 2019, doi: 10.15166/2499-8249/394

[9] G. P. L. Chong, "Cashless China: Securitization of everyday life through Alipay's social credit system—Sesame credit," *Chinese Journal of Communication*, vol. 12, no .3, pp. 290–307, 2019, doi: 10.1080/17544750.2019.1583261

[10] S. Wachter, B. Mittelstadt, and L. Floridi, "Why a right to explanation of automated decision-making does not exist in the general data protection regulation," *International Data Privacy Law*, no. 7, no. 2, pp. 76–99. 2017, doi: 10.1093/idpl/ipx005

[11] C. Cheng and S. Ou, "The status quo and problems of the building of China's social credit system and suggestions," *International Business and Management*, vol. 8, no. 2, pp. 169–173, 2014.

[12] A. Broumas and P. Charalampakis. (2022). Greek DPA imposes 20M euro fine on Clearview AI for unlawful processing of personal data. [Online]. Available: https://iapp.org/news/a/greek-dpa-imposes-20m-euro-fine-on-clearview-ai-for-unlawful-processing-of-personal-data/

[13] S. Gal, A. Huberman, and B. Johanson, "Data governance in AI systems: Privacy by design and GDPR compliance," *Journal of Information Systems and Technology Management*, vol. 20, no. 1, pp. 35–52, 2022.

[14] M. Ienca, J. Fins, R. Jox, F. Jotterand, S. Voeneky, R. Andorno, T. Ball, C. Castelluccia, R. Chavarriaga, H. Chneiweiss, A. Ferretti, O. Friedrich, S. Hurst, G. Merkel, F. Molnár Gábor, J. Rickli, J. Scheibner, E. Vayena, R. Yuste, and P. Kellmeyer, "Towards a governance framework for brain data," *Neuroethics*, vol. 15, no. 2, 2022.

[15] J. Meszaros and C.-H Ho, "AI research and data protection: Can the same rules apply for commercial and academic research under the GDPR?," *Computer Law and Security Review*, vol. 41, pp. 83–92, 2021.

[16] D. Felz, W. Nauwelaerts, and A. Portnoy. (2023, Sep.). EU's Highest Court Issues Major AI Decision With Wide-Reaching Impact. Alston & Bird. [Online]. Available: https://www.alstonprivacy.com/eus-highest-court-issues-major-ai-decision-with-wide-reaching-impact/.

[17] J. J. Bryson, "The past decade and future of AI's impact on society," *Ethics and Information Technology*, vol. 20, no. 3, pp. 185–191, 2019, doi: 10.1007/s10676-018-9467-5.

[18] L. Edwards and M. Veale, "Enslaving the algorithm: From a 'Right to Explanation' to a 'Right to Better Decisions'?," *IEEE Security & Privacy*, vol. 16, no. 3, pp. 46–54, 2018, doi: 10.1109/MSP.2018.2701152.

[19] M. Ananny and K. Crawford, "Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability," *New Media & Society*, vol. 20, no. 3, pp. 973–989, 2018, doi: 10.1177/1461444816676645

[20] A. Sitthitheerarut, "Legal problems concerning electronic personal data protection," M.S. thesis, Faculty of Law, Thammasat University, 2015 (in Thai).

[21] S. Kuebler-Wachendorff, R. Luzsa, J. Kranz, S. Mager, E. Syrmoudis, S. Mayr, and J. Grossklags, "The right to data portability: Conception, status quo, and future directions," *Informatik-Spektrum*, vol. 44, no. 4, pp. 264–272. Aug. 2021, doi: 10.1007/s00287-021-01372-w.