บทแนะนำหนังสือ
Data Protection and Artificial Intelligence

ธิดารัตน์ เลี่ยมสมบูรณ์*
ผู้พิพากษาประจำสำนักงานศาลยุติธรรม
Thidarat Liamsomboon
Judge of the Office of the Judiciary

วันที่รับบทความ ๖ ธันวาคม ๒๕๖๗; วันที่ตอบรับบทความ ๙ ธันวาคม ๒๕๖๗

บทคัดย่อ

หนังสือ “Data Protection and Artificial Intelligence” (กฎหมายคุ้มครองข้อมูลและปัญญาประดิษฐ์) เป็นหนังสือเล่มที่ ๑๓ ของซีรีส์หนังสือ Data Protection and Privacy โดยสำนักพิมพ์ Hart เป็นหนังสือที่มีเนื้อหาครอบคลุมกฎหมายคุ้มครองข้อมูลส่วนตัวของสหภาพยุโรปและกฎหมายที่เกี่ยวข้องในมุมมองเชิงลึก อันเกี่ยวกับผลกระทบของเทคโนโลยีปัญญาประดิษฐ์ (AI) ต่อความเป็นส่วนตัวของข้อมูล โดยหนังสือเล่มนี้ได้รวบรวมบทความวิชาการที่น่าสนใจรวม ๘ ฉบับ ที่วิเคราะห์ถึงความท้าทายและผลกระทบของเทคโนโลยีปัญญาประดิษฐ์ (AI) ต่อความเป็นส่วนตัวของข้อมูลส่วนตัวในแง่มุมต่าง ๆ ให้ผู้อ่านได้เข้าใจถึงบริบทของปัญหาและความท้าทายเกี่ยวกับเทคโนโลยีปัญญาประดิษฐ์ (AI) นี้ โดยรวมบทความบรรยายถึง

---

* BBA (Thammasart International Program) (มหาวิทยาลัยธรรมศาสตร์ หลักสูตรนานาชาติ), น.บ. (มหาวิทยาลัยสุโขทัยธรรมาธิราช), น.บ.ท., ประกาศนียบัตรกฎหมายภาษีอากรระหว่างประเทศ (มหาวิทยาลัยธรรมศาสตร์), LL.M. in Health law (University of Washington, Seattle, USA), LL.M. in International Environmental Law (Nottingham University, UK), SJD Candidate in Digital Health Law (Southern Methodist University, USA) (ทุนสำนักงานศาลยุติธรรม).

(๑) กรอบการกำกับดูแล (Regulatory Frameworks) ของกฎหมายคุ้มครองข้อมูลส่วนตัวในสหภาพยุโรป (EU) และการปรับใช้กับเทคโนโลยีปัญญาประดิษฐ์ (AI) รวมถึงคำวิเคราะห์ถึงความสามารถของกฎหมายที่มีในปัจจุบันกับการรับมือความท้าทายของปัญญาประดิษฐ์ (AI)

(๒) ปัญหาจริยธรรม (Ethical Considerations) ที่เกิดจากเทคโนโลยีปัญญาประดิษฐ์ (AI) รวมถึงประเด็นด้านความโปร่งใส ความรับผิดชอบ และความยุติธรรม โดยเน้นถึงการพัฒนาปัญญาประดิษฐ์ (AI) ที่เคารพสิทธิความเป็นส่วนตัวของบุคคลและสอดคล้องกับมาตรฐานจริยธรรม และ

(๓) การประยุกต์ใช้ในทางปฏิบัติ (Practical Applications) ระหว่างปัญญาประดิษฐ์ (AI) และการบังคับใช้กฎหมาย การคุ้มครองข้อมูลส่วนตัว ในแต่ละภาคส่วนอุตสาหกรรม เช่น สาธารณสุข การเงิน และการปกครอง เป็นต้น พร้อมทั้งตัวอย่างกรณีศึกษาที่แสดงให้เห็นถึงความท้าทายในทางปฏิบัติและการนำเสนอแนวทางแก้ไขสำหรับการนำเทคโนโลยีปัญญาประดิษฐ์ (AI) มาใช้อย่างมีความรับผิดชอบ

หนังสือเล่มนี้เหมาะสำหรับผู้อ่านที่อยากทำความเข้าใจความซับซ้อนของการกำกับดูแลเทคโนโลยีปัญญาประดิษฐ์ (AI) ในกรอบของกฎหมายเพื่อปกป้องสิทธิความเป็นส่วนตัวของบุคคล อีกทั้งแนวทางการบังคับใช้หรือบัญญัติกฎหมายไปในทางที่สนับสนุนนวัตกรรมทางเทคโนโลยีไปพร้อมกัน

คำสำคัญ : กฎหมายคุ้มครองข้อมูลส่วนตัว, เทคโนโลยีปัญญาประดิษฐ์, สหภาพยุโรป, สิทธิความเป็นส่วนตัว

Abstract

The book “Data Protection and Artificial Intelligence” (Volume 13 of the Data Protection and Privacy series) by Hart Publishing provides a comprehensive and insightful exploration of the impact of artificial intelligence (AI) on data privacy.

The book compiles eight academic articles that analyze the challenges and implications of AI on personal data privacy, offering insights into regulatory frameworks, ethical considerations, and practical applications. The book is structured to provide a multifaceted perspective on the subject:

(1) Regulatory Frameworks: It examines existing data protection regulations in the European Union (EU) and their application to AI technologies. It also analyzes the adequacy of current legal frameworks in addressing the challenges posed by AI.

(2) Ethical Considerations: It explores the ethical issues arising from AI, including transparency, accountability, and fairness. The articles emphasize the importance of developing AI systems that respect individual privacy rights and align with ethical standards.

(3) Practical Applications: It highlights real-world scenarios where AI and data protection intersect, such as in healthcare, finance, and law enforcement. The case studies illustrate practical challenges and propose solutions for integrating AI responsibly in various sectors.

All in all, this book is suitable for readers who wish to understand the complexities of regulating AI in a way that balance individual privacy rights and technological innovation.

Keywords : Data Privacy Laws, Artificial Intelligence, European Unions, Privacy Rights

หนังสือ “Data Protection and Articial Intelligence” (กฎหมายคุ้มครองข้อมูลและปัญญาประดิษฐ์ (AI) เป็นหนังสือเล่มที่ ๑๓ ของซีรีส์หนังสือ Data Protection and Privacy โดยสำนักพิมพ์ Hart เป็นหนังสือที่มีเนื้อหาครอบคลุมกฎหมายคุ้มครองข้อมูลส่วนตัวของ

สหภาพยุโรปและกฎหมายที่เกี่ยวข้องในมุมมองเชิงลึก อันเกี่ยวกับผลกระทบของเทคโนโลยีปัญญาประดิษฐ์ (AI) ต่อความเป็นส่วนตัวของข้อมูล โดยหนังสือเล่มนี้ได้รวบรวมบทความวิชาการที่น่าสนใจรวม ๘ ฉบับ ที่วิเคราะห์ถึงความท้าทายและผลกระทบของเทคโนโลยีปัญญาประดิษฐ์ (AI) ต่อความเป็นส่วนตัวของข้อมูลส่วนตัวในแง่มุมต่าง ๆ ให้ผู้อ่านได้เข้าใจถึงบริบทของปัญหาและความท้าทายเกี่ยวกับเทคโนโลยีปัญญาประดิษฐ์ (AI) นี้ โดยแต่ละบทความมีเนื้อหาโดยย่อ ดังนี้

สำหรับบทความแรก “Don’t Accept Candy from Strangers: An Analysis of Third-Party Mobile SDKs” โดย Alvaro Feal, Julien Gamba และผู้เขียนท่านอื่น ๆ บทความนี้นำเสนอเกี่ยวกับความเสี่ยงของการใช้ชุดเครื่องมือสร้างแพลตฟอร์ม (Software Development Kits (SDKs)) ที่พัฒนาโดยผู้พัฒนาบุคคลที่สาม (Third-party developers) ในการพัฒนาแอปพลิเคชันในโทรศัพท์เคลื่อนที่ ชุดเครื่องมือสร้างแพลตฟอร์ม (SDKs) นี้ได้รับความนิยมอย่างแพร่หลายในหมู่นักพัฒนา เนื่องจากชุดเครื่องมือนี้ช่วยลดขั้นตอน ประหยัดเวลา และลดต้นทุนในการสร้างแอปพลิเคชัน ชุดเครื่องมือนี้เป็นชุดเครื่องมือที่ทำออกมาหลากหลายรูปแบบเพื่อเพิ่มฟังก์ชันต่าง ๆ ในแอปพลิเคชัน ได้แก่ การวิเคราะห์ข้อมูล การโฆษณา และการเชื่อมต่อกับโซเชียลมีเดีย อย่างไรก็ตาม ความสะดวกสบายนี้มาพร้อมกับความท้าทายด้านความปลอดภัยและความเป็นส่วนตัวของผู้ใช้ เนื่องจากชุดเครื่องมือสร้างแพลตฟอร์ม (SDKs) ที่สร้างออกมาเป็นจำนวนมาก ใส่โค้ดเก็บรวบรวมข้อมูลส่วนตัวผู้ใช้ เช่น รหัสประจำอุปกรณ์ (Device Identifiers) ข้อมูลตำแหน่งที่ตั้ง และข้อมูลส่วนบุคคล (PII) โดยที่ผู้ใช้หรือแม้กระทั่งนักพัฒนาแอปพลิเคชันเองอาจไม่ทราบ บางชุดเครื่องมือสร้างแพลตฟอร์ม (SDKs) อาจถูกออกแบบมาเพื่อหลีกเลี่ยงการป้องกันความเป็นส่วนตัวในระดับระบบปฏิบัติการ ซึ่งก่อให้เกิดปัญหาในการใช้งานข้อมูลที่ไม่เหมาะสมและไม่ตรงตามประสงค์ของผู้สร้างแพลตฟอร์ม ผู้เขียนบทความยังชี้ให้เห็นว่า ชุดเครื่องมือสร้างแพลตฟอร์ม (SDKs) เหล่านี้มักแบ่งปันข้อมูลที่รวบรวมจากมือถือของผู้ใช้ให้กับบุคคลที่สามเพื่อสร้างรายได้ผ่านการโฆษณา อนึ่ง ความไม่โปร่งใสของชุดเครื่องมือนี้เพิ่มความเสี่ยงทั้งต่อผู้ใช้ในการละเมิดความเป็นส่วนตัวและการใช้

ข้อมูลโดยไม่ได้รับอนุญาต และต่อนักพัฒนาในการทำผิดทางกฎหมายคุ้มครองข้อมูลส่วนตัว ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล ดังนั้น นักพัฒนาจึงต้องตรวจสอบชุดเครื่องมือสร้างแพลตฟอร์ม (SDKs) อย่างละเอียดก่อนการใช้งาน เลือกใช้เฉพาะผู้ให้บริการชุดเครื่องมือสร้างแพลตฟอร์ม (SDKs) ที่มีชื่อเสียง และทำการตรวจสอบการอัปเดตเป็นประจำเพื่อให้มั่นใจว่า ระบบปฏิบัติการแอปพลิเคชันยังสอดคล้องกับกฎหมาย ส่วนผู้ใช้งานก็ควรระมัดระวังในการให้สิทธิการเข้าถึงแอปพลิเคชันและพิจารณาใช้เครื่องมือเพิ่มความเป็นส่วนตัว เช่น VPN หรือแอปบล็อกเกอร์ข้อมูลอีกด้วย นอกจากนี้ หน่วยงานกำกับดูแลควรบังคับใช้นโยบายที่เข้มงวดขึ้นเกี่ยวกับความโปร่งใสของชุดเครื่องมือสร้างแพลตฟอร์ม (SDKs) และการจัดการข้อมูล

บทความที่สอง “AI and the Right to Explanation: Three Legal Bases under the GDPR” โดย Tiago Sergio Cabral ได้วิเคราะห์ถึงการมีอยู่ของหลัก “สิทธิในการได้รับคำอธิบาย” (Right to Explanation) ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation (GDPR)) ในแง่การตัดสินใจอัตโนมัติของอัลกอริทึมในปัญญาประดิษฐ์ (AI) ซึ่งแม้ว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) นี้จะพูดถึงหลักความโปร่งใส (transparency) แต่กฎหมายก็ไม่ได้ระบุอย่างชัดเจนถึงสิทธิในการได้รับคำอธิบายอย่างละเอียด ในบทความนี้ ผู้เขียนได้เริ่มบทความด้วยการระบุหลักกฎหมายสามหลัก ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) ที่อาจสนับสนุน “สิทธิในการได้รับคำอธิบาย” (Right to Explanation) ในบริบทของกฎหมาย กล่าวคือ *ประการแรก* สิทธิในการรับข้อมูล (Right to Information) ตามมาตรา ๑๓, ๑๔ กำหนดให้องค์กรที่เป็นผู้ควบคุมข้อมูล (Data Controller) ให้ข้อมูลที่ชัดเจน เข้าถึงได้ และโปร่งใสแก่เจ้าของข้อมูล อันเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลที่เก็บรวบรวมโดยตรงจากเจ้าของข้อมูล หรือจากแหล่งข้อมูลอื่น *ประการที่สอง* สิทธิในการเข้าถึงข้อมูล (Right to Access) ตามมาตรา ๑๕ กำหนดให้องค์กรที่เป็นผู้ควบคุมข้อมูล (Data Controller) ต้องอนุญาตหรือรับคำรองของเจ้าของข้อมูลในการมีสิทธิเข้าถึงข้อมูลส่วนตัวของเจ้าของข้อมูลที่องค์กรใช้ในการประมวลผลข้อมูล รวมถึงวัตถุประสงค์ตรรกะที่ใช้ในการประมวลผลและผลกระทบที่อาจ

เกิดขึ้นจากการประมวลผลข้อมูล อันรวมถึงระบบการตัดสินใจอัตโนมัติของปัญญาประดิษฐ์ (AI) และ*ประการที่สาม* สิทธิในการไม่ถูกตัดสินใจโดยระบบอัตโนมัติ (Right not to be subject to automated individual decision making) ตามมาตรา ๒๒ ซึ่งคุ้มครองบุคคลจากการถูกระบบประมวลผลอัตโนมัตินำข้อมูลมาทำการตัดสินใจบางอย่าง รวมถึงการทำโปรไฟล์ (profiling) ที่มีผลกระทบต่อบุคคลดังกล่าว เว้นแต่การประมวลผลข้อมูลนั้นเป็นไปตามเงื่อนไขบางประการ ผู้เขียนยังกล่าวถึงความท้าทายหลายประการ เช่น ความซับซ้อนทางเทคนิคของระบบปัญญาประดิษฐ์ (AI) โดยเฉพาะ Black-Box, การที่องค์กรมักหลีกเลี่ยงการเปิดเผยตรรกะและอัลกอริทึมของปัญญาประดิษฐ์ (AI) โดยละเอียด เนื่องจากความกังวลเกี่ยวกับทรัพย์สินทางปัญญาและความลับทางการค้า ทำให้หน่วยงานกำกับดูแลต้องเผชิญกับความยากลำบากในการบังคับกฎหมาย เป็นต้น

บทความที่สาม “A Comparison of Data Protection Regulations for Automotive Systems” โดย Ala’a Al-momani, Christoph Bosch, และ Frank Kargl วิเคราะห์ผลกระทบของกฎหมายคุ้มครองข้อมูลต่อระบบยานยนต์สมัยใหม่ โดยเฉพาะในบริบทของการพัฒนาเทคโนโลยีรถยนต์ที่เชื่อมต่อและขับเคลื่อนอัตโนมัติ (connected and autonomous vehicles) เพื่อมาเป็นรถขนส่งเอกชน (Taxicab) เนื่องจากยานพาหนะในยุคปัจจุบันมีการเก็บและประมวลผลข้อมูลจำนวนมหาศาล เช่น ข้อมูลส่วนบุคคล (PII) ข้อมูลจากตัวรถ (เช่น ตำแหน่งและรูปแบบการขับขี่) และข้อมูลจากเซนเซอร์ (เช่น กล้องและเรดาร์) แม้ว่าความสามารถเหล่านี้จะช่วยเพิ่มฟังก์ชันการทำงาน เช่น การขับขี่อัตโนมัติและข้อมูลจราจรแบบเรียลไทม์ แต่ก็สร้างความกังวลอย่างมากเกี่ยวกับความเป็นส่วนตัวและความปลอดภัย ผู้ให้บริการยานยนต์และผู้ผลิตรถยนต์จึงจำเป็นต้องมีระบบการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม เพื่อหลีกเลี่ยงการละเมิดความไว้วางใจของผู้บริโภคหรือข้อบังคับด้านการคุ้มครองข้อมูล บทความนี้เปรียบเทียบกรอบกฎหมายคุ้มครองข้อมูลของสามประเทศ กล่าวคือ ประเทศในกลุ่มสหภาพยุโรป ประเทศสหรัฐอเมริกา และประเทศญี่ปุ่น รวมถึงการวิเคราะห์ความท้าทายที่จะเกิดขึ้นจากการใช้ข้อกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่แตกต่างกันในแต่ละประเทศทั่วโลก เพื่อประเมินความ

เหมาะสมในการจัดการความท้าทายเหล่านี้ ผู้เขียนยังได้ระบุถึงความท้าทายหลายประการในการปฏิบัติตามข้อกำหนดด้านการคุ้มครองข้อมูล โดยหนึ่งในปัญหาหลักคือ ความแตกต่างของกฎระเบียบทั่วโลก ซึ่งทำให้บริษัทที่ดำเนินธุรกิจรถยนต์ในหลายภูมิภาคต้องเผชิญกับความยากลำบากในการปรับแนวทางปฏิบัติให้สอดคล้องกับข้อกำหนดที่หลากหลาย นอกจากนี้ การประมวลผลข้อมูลของระบบรถยนต์นั้นมีการเปลี่ยนแปลงอย่างต่อเนื่อง เช่น ข้อมูลแบบเรียลไทม์ในระบบยานยนต์นั้นยังเพิ่มความซับซ้อนในการที่ผู้ควบคุมข้อมูลจะปฏิบัติตามสิทธิของเจ้าของข้อมูล เช่น การลบข้อมูลหรือการปฏิเสธการใช้ข้อมูลอีกด้วย นอกจากนี้ การแชร์ข้อมูลกับบุคคลที่สาม ซึ่งเป็นส่วนสำคัญของการรวมแอปพลิเคชันกับฟังก์ชันการบริการในยานพาหนะ ก็จำต้องมีกลไกที่มีประสิทธิภาพในการจัดการเพื่อให้เป็นไปตามข้อกำหนดของกฎหมาย และยิ่งไปกว่านั้นการขาดมาตรฐานที่เป็นสากลในอุตสาหกรรมยานยนต์นั้น ทำให้การปฏิบัติตามข้อกำหนดกฎหมายมีความยากลำบากมากขึ้น เนื่องจากไม่มีแนวทางที่เป็นที่ยอมรับในระดับสากลสำหรับการคุ้มครองข้อมูลที่ผู้ผลิตรถยนต์สามารถนำมาเป็นแนวทางปฏิบัติหลักได้

บทความที่สี่ “Misaligned Union Laws? A Comparative Analysis of Certification in the Cybersecurity Act and the General Data Protection Regulation” โดย Irene Kamara นั้น วิเคราะห์เปรียบเทียบกลไกการรับรอง (certification) ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (CSA) และกฎหมายคุ้มครองข้อมูลส่วนบุคคล (GDPR) ของสหภาพยุโรป โดยผู้เขียนเห็นว่า แม้กฎหมายทั้งสองฉบับนี้จะมีความสอดคล้องกันที่เป้าหมายของกฎหมายที่คำนึงถึงความมั่นคงปลอดภัยของข้อมูลและการคุ้มครองข้อมูลเป็นแนวคิดพื้นฐาน แต่อย่างไรก็ตาม กฎหมายทั้งสองก็มีความแตกต่างกันในขอบเขตวิธีการดำเนินการและการบังคับใช้กฎหมาย อนึ่ง การสอดคล้องกันนั้นก็ไม่ได้หมายถึงการทับซ้อนกัน เนื่องจากความมั่นคงปลอดภัยทางไซเบอร์มีขอบเขตที่กว้างกว่า โดยไม่ได้จำกัดเฉพาะความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล แต่ครอบคลุมถึงข้อมูลทุกประเภท ในขณะที่การคุ้มครองข้อมูลส่วนบุคคลนั้นมีลักษณะหลายมิติ ซึ่งความมั่นคงปลอดภัยของข้อมูลเป็นเพียงหนึ่งมิติเท่านั้น การคุ้มครองข้อมูลส่วนบุคคลยังรวมถึงหลักความเป็นธรรม (fairness) และความชอบ

ด้วยกฎหมาย (lawfulness) การเก็บใช้ข้อมูลเท่าที่จำเป็น (data minimization) การกำหนดวัตถุประสงค์ที่ชัดเจน (purpose specification) ความรับผิดชอบ (accountability) และการคุ้มครองสิทธิของบุคคลในสาระสำคัญอีกด้วย นอกจากนี้ ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล (GDPR) กลไกการรับรอง (certification) เป็นกลไกทางเลือกที่มีความหลากหลายแตกต่างในแต่ละประเทศสมาชิก องค์กรจะใช้การรับรองนี้เพื่อแสดงความสอดคล้องกับบทบัญญัติของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศนั้น ๆ โดยมุ่งเน้นไปที่การรับรองในส่วนของกระบวนการหรือบริการเฉพาะ อันทำให้การรับรองในทางปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (GDPR) มีจำนวนน้อยกว่าพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (CSA) อนึ่ง การรับรองภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (CSA) นั้นมีกรอบการรับรองด้านความมั่นคงปลอดภัยทางไซเบอร์ที่ชัดเจน สำหรับทั้งสหภาพยุโรป ซึ่งมีระดับการประเมินความมั่นคง ๓ ระดับ สำหรับผลิตภัณฑ์ บริการและกระบวนการด้านไอซีที ทั้งภาคสมัครใจ และภาคบังคับตามกฎหมายภายในของประเทศสมาชิกที่บังคับให้มีการรับรองด้านความมั่นคงปลอดภัยทางไซเบอร์ อนึ่ง ผู้เขียนเห็นว่า การปรับกลไกการรับรอง (certification) ของกฎหมายทั้งสองฉบับให้สอดคล้องกันนั้นเป็นสิ่งสำคัญเพื่อหลีกเลี่ยงความไม่มีประสิทธิภาพและเสริมสร้างความแข็งแกร่งของกฎหมายสหภาพยุโรปในด้านการคุ้มครองข้อมูลและความปลอดภัยทางไซเบอร์ โดยผู้เขียนได้เสนอแนวทางในการปรับกลไกการรับรองอย่างหลากหลาย เช่น การรวมมาตรฐานหรือพัฒนากลไกการยอมรับร่วมกันระหว่างการรับรองทั้งสองแบบ การเพิ่มความร่วมมือระหว่าง European Data Protection Board (EDPB) และ European Union Agency for Cybersecurity (ENISA) รวมถึงการให้คำแนะนำที่ชัดเจนยิ่งขึ้นเกี่ยวกับวิธีการรับรองภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล (GDPR) และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ CSA เป็นต้น

บทความที่ห้า “Aggregation, Synthesisation and Anonymisation: A Call for a Risk-Based Assessment of Anonymisation Approaches” โดย Sophie Stalla-Bourdillon และ Alfred Rossi กล่าวถึงความสำคัญที่เพิ่มขึ้นของการทำข้อมูลให้ไม่ระบุตัวตน

(anonymisation) เพื่อสร้างสมดุลระหว่างการประมวลผลข้อมูลและการคุ้มครองความเป็นส่วนตัว เนื่องจากความต้องการที่จะแบ่งปันข้อมูลข้ามองค์กรเพิ่มขึ้นมากในหลายภาคส่วนอุตสาหกรรม เช่น ภาคสาธารณสุข ภาคการวิจัย และภาคธุรกิจ เป็นต้น การทำข้อมูลให้ไม่ระบุตัวตน (anonymisation) นั้นจึงมีความสำคัญในการปกป้องความเป็นส่วนตัวของข้อมูลส่วนบุคคล โดยที่ผู้ควบคุมข้อมูล (data controller) ยังคงสามารถใช้ชุดข้อมูลในการประมวลผลตามวัตถุประสงค์ของผู้ควบคุมได้ บทความเริ่มต้นด้วยการอธิบายแนวคิดของการทำข้อมูลให้ไม่ระบุตัวตน (anonymisation) ตามกรอบของกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูล เช่น กฎหมายคุ้มครองข้อมูลส่วนบุคคล (GDPR) กำหนดนิยามของการทำข้อมูลให้ไม่ระบุตัวตน (anonymisation) ว่าเป็นกระบวนการที่ทำให้ข้อมูลไม่สามารถเชื่อมโยงกลับไปยังตัวบุคคลได้อย่างถาวร ซึ่งแตกต่างจากการใช้ข้อมูลนามแฝง (pseudonymisation) ที่ยังคงมีลิงก์กลับไปหาตัวบุคคลผ่านข้อมูลเพิ่มเติม ในทางกลับกันกฎหมายคุ้มครองความเป็นส่วนตัวของผู้บริโภคของมลรัฐแคลิฟอร์เนีย (CCPA) เห็นว่า การทำให้ข้อมูลไม่ระบุตัวตนไม่รวมถึงการรวบรวมข้อมูล (Aggregation) ผู้เขียนได้จัดหมวดหมู่วิธีการทำข้อมูลให้ไม่ระบุตัวตน (anonymisation) ออกเป็นสามประเภทหลัก กล่าวคือ การรวมข้อมูล (Aggregation) ซึ่งเป็นการจัดกลุ่มข้อมูลให้อยู่ในหมวดหมู่ที่กว้างขึ้นเพื่อลดรายละเอียดเฉพาะบุคคล (เช่น การเปลี่ยนอายุที่แน่นอนเป็นช่วงอายุ) การสังเคราะห์ข้อมูล (Synthesisation) ที่เลียนแบบข้อมูลจริงโดยไม่มีการเชื่อมโยงโดยตรงกับบุคคล และการปรับแต่งข้อมูล (local Anonymisation via Perturbation or local anonymisation) โดยเปลี่ยนชื่อหรือแทนค่าข้อมูล หรือเพิ่มข้อมูลเพื่อลดความแม่นยำและความสามารถในการระบุตัวบุคคลในขณะที่ยังคงรักษาประโยชน์ของข้อมูล ซึ่งแต่ละวิธีมีข้อดีและข้อเสียแตกต่างกัน รวมถึงผลกระทบต่อการใช้งานข้อมูลความเป็นส่วนตัว และความเสี่ยงในการแปลงข้อมูลกลับเพื่อระบุตัวตน อนึ่ง ในบทความผู้เขียนสนับสนุนแนวทางการประเมินความเสี่ยงสำหรับวิธีการทำข้อมูลให้ไม่ระบุตัวตน (anonymisation) ต่าง ๆ ตามบริบทและลักษณะของข้อมูลที่จะนำมาประมวลผล เพื่อลดความเสี่ยงจากการโจมตีแบบรวมชุดข้อมูลเพื่อระบุตัวบุคคล และสมดุลระหว่างการใช้ประโยชน์ของเทคโนโลยี

และความปลอดภัยของข้อมูลให้มีประสิทธิภาพมากขึ้น

บทความที่หก “The Role of the EU Fundamental Right to Data Protection in an Algorithmic and Big Data World” โดย Yordanka Ivanova วิเคราะห์ถึงความท้าทายและผลกระทบของการรักษาสิทธิขั้นพื้นฐานด้านการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปในยุคของเทคโนโลยีที่ใช้ข้อมูลขนาดใหญ่ (big data) และการตัดสินใจด้วยอัลกอริทึม (algorithmic decision-making) โดยผู้เขียนได้เน้นถึงความท้าทายในการสร้างสมดุลระหว่างการพึ่งพาเทคโนโลยีที่ขับเคลื่อนด้วยข้อมูลกับหลักกฎหมายคุ้มครองสิทธิขั้นพื้นฐานของสหภาพยุโรป (Charter of Fundamental Rights of the European Union: CFR) และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation: GDPR) อันรวมถึงขอบเขตหน้าที่ และข้อจำกัดของสิทธิขั้นพื้นฐานในการคุ้มครองข้อมูลส่วนบุคคลนี้ ผู้เขียนได้วิเคราะห์การตีความและการบังคับใช้ของกฎหมายต่าง ๆ ตามคำพิพากษาล่าสุดของศาลยุติธรรมแห่งสหภาพยุโรป (CJEU) ได้แก่ *คดี Digital Rights Ireland (คดีที่ C-293/12 และ C-594/12) และ Tele 2 Sverige (คดีที่ C-203/15 และ C-698/15)* ที่ศาลยุติธรรมแห่งสหภาพยุโรป (CJEU) ได้พิจารณาความชอบด้วยกฎหมายของ Directive 2006/24/EC (Data Retention Directive) และกฎหมายของประเทศสมาชิก ในบริบทของมาตรา ๗ และ ๘ ของหลักกฎหมายคุ้มครองสิทธิขั้นพื้นฐานแห่งสหภาพยุโรป (Charter of Fundamental Rights of the European Union), คดี Schrems (คดี C-362/14) ที่ศาลยุติธรรมแห่งสหภาพยุโรป (CJEU) ได้พิจารณาความชอบด้วยกฎหมายของ Safe Harbor Agreement ซึ่งเป็นข้อตกลงที่อนุญาตให้มีการโอนข้อมูลส่วนบุคคลระหว่างสหภาพยุโรป (EU) และสหรัฐอเมริกา (US) โดยศาลยุติธรรมแห่งสหภาพยุโรป (CJEU) ได้ตัดสินให้ข้อตกลงนี้เป็นโมฆะ เนื่องจากไม่สอดคล้องกับมาตรา ๗ และ ๘ ของ Charter of Fundamental Rights of the European Union ที่คุ้มครองสิทธิในความเป็นส่วนตัวและคุ้มครองข้อมูลส่วนบุคคล และคดี Google Spain (คดี C-131/12) ที่ศาลยุติธรรมแห่งสหภาพยุโรป (CJEU) ได้ตัดสินเกี่ยวกับสิทธิที่จะถูกลืม (Right to be Forgotten) โดยพิจารณาว่า บุคคลมีสิทธิที่จะขอให้ผู้ควบคุมข้อมูล

ลบข้อมูลส่วนบุคคลของเจ้าของข้อมูลออกจากผลการค้นหาของ Google Search Engine หากข้อมูลนั้นไม่เกี่ยวข้อง ไม่เหมาะสมหรือเกินความจำเป็น โดยให้เหตุผลว่าสิทธิในการคุ้มครองข้อมูล (มาตรา ๘) และสิทธิในความเป็นส่วนตัว (มาตรา ๗) มีน้ำหนักมากกว่าผลประโยชน์ทางเศรษฐกิจของผู้ควบคุมข้อมูล และมากกว่าสิทธิในการรับรู้ข้อมูลของสาธารณชนในบางกรณี เป็นต้น อนึ่ง ผู้เขียนได้เสนอให้ปรับแนวคิดใหม่ในสาระสำคัญของการคุ้มครองข้อมูลส่วนตัวผ่านแนวคิดแบบองค์รวมของ “การควบคุม” ที่พัฒนาขึ้นจากแนวคิดการควบคุมของบุคคลที่มีอยู่ในงานวิชาการดั้งเดิม แต่เพิ่มการให้ความสำคัญกับกลไกการป้องกัน, การกำหนดข้อห้าม, และการกำกับดูแลในเชิงส่วนรวม ซึ่งกลไกเหล่านี้ควรมีบทบาทสำคัญเชิงเครื่องมือสำหรับการปกป้องคุณค่าในวงกว้างและสิทธิขั้นพื้นฐานทั้งหมดในยุคของ Big Data และปัญญาประดิษฐ์ (AI)

บทความที่เจ็ด “Implementing AI in Healthcare: An Ethical and Legal Analysis Based on Case Studies” โดย Eduard Fosch-Villaronga, Davit Chokoshvili, Vibeke Binz Vallevik, Marcello Ienca และ Robin L. Pierce วิเคราะห์มิติด้านจริยธรรมและกฎหมายที่เกี่ยวข้องกับการบูรณาการปัญญาประดิษฐ์ (AI) ในระบบสุขภาพ ผ่านกรณีศึกษาจริง โดยเริ่มจากการอธิบายถึงภาพรวมของการนำปัญญาประดิษฐ์ (AI) ว่า ปัจจุบันได้มีการนำปัญญาประดิษฐ์ (AI) มาใช้ในการวินิจฉัยโรคเฉพาะบุคคล การตรวจหาความเสี่ยงของโรคในระยะเริ่มต้น การพยากรณ์ความเสี่ยงของโรค การเข้ารักษาในโรงพยาบาลแบบเข้าพัก (Admission) และการค้นคว้ายารักษาโรคชนิดใหม่เพื่อเพิ่มประสิทธิภาพในการรักษาความปลอดภัย และความสามารถในการรักษาผู้ป่วยแบบเฉพาะที่เหมาะสมกับผู้ป่วยรายคนมากขึ้น (personalized care) โดยระบบนี้สามารถประมวลผลข้อมูลจำนวนมหาศาล เรียนรู้จากประสบการณ์ และปรับปรุงประสิทธิภาพการทำงานของระบบได้ด้วยตนเองอัตโนมัติ (autonomous improvement) ผู้เขียนยังเน้นถึงความท้าทาย โอกาส และช่องว่างในด้านกฎหมายและด้านจริยธรรมที่เกิดขึ้นจากการใช้งานปัญญาประดิษฐ์ (AI) ในวงการแพทย์ เนื่องจากกฎหมายที่มีอยู่ไม่ได้ออกแบบมารองรับระบบของปัญญาประดิษฐ์ (AI) ที่มีคุณสมบัติในการปรับตัวและพัฒนาระบบเอง

อัตโนมัติ นอกจากนี้ การประมวลผลข้อมูลที่สามารถประเมิน วิเคราะห์ และทำนายผลที่เกี่ยวกับสุขภาพของปัญญาประดิษฐ์ (AI) นี้อาจมีผลกระทบต่อสิทธิตามกฎหมายเกี่ยวกับการคุ้มครองข้อมูลความปลอดภัยทางจริยธรรมและแง่มุมอื่น ๆ ของผู้ป่วยอีกด้วย อนึ่ง ผู้เขียนได้ยกกรณีศึกษาเพื่อการอธิบายความท้าทายของการใช้ปัญญาประดิษฐ์ (AI) ในระบบสุขภาพเพิ่มเติม เช่น ตัวอย่างของการใช้ปัญญาประดิษฐ์ (AI) ในการวิเคราะห์ภาพถ่ายผลเอกซเรย์หรือภาพอื่น ๆ ทางการแพทย์ ซึ่งแสดงให้เห็นถึงความกังวลเกี่ยวกับการพึ่งพาการตัดสินใจอัตโนมัติ หรือการประมวลผลของระบบปัญญาประดิษฐ์ (AI) มากเกินไปของบุคลากรทางการแพทย์ และเน้นถึงความจำเป็นของการมีมนุษย์ในกำกับดูแลการวินิจฉัยโรคของระบบปัญญาประดิษฐ์ (AI) กรณีการใช้ปัญญาประดิษฐ์ (AI) ในการแพทย์เฉพาะบุคคลเพื่อวิเคราะห์โครงสร้างพันธุกรรม อันแสดงให้เห็นประเด็นทางกฎหมายเกี่ยวกับการเป็นเจ้าของข้อมูลพันธุกรรมของผู้ป่วย และความเสี่ยงที่ข้อมูลพันธุกรรม อันเป็นข้อมูลส่วนบุคคลที่อ่อนไหวอาจจะถูกใช้โดยบุคคลที่สาม และกรณีศึกษาของปัญญาประดิษฐ์ (AI) ในงานด้านเอกสารทางการแพทย์ อันเป็นระบบอัตโนมัติ ซึ่งเผยให้เห็นถึงความเสี่ยงของการจัดการข้อมูลและความเป็นไปได้ที่จะเกิดความผิดพลาดและการรั่วไหลของข้อมูลส่วนบุคคลที่อ่อนไหวนี้ ผู้เขียนได้นำเสนอคำแนะนำในการจัดการกับความท้าทายเหล่านี้ โดยเพิ่มความโปร่งใสในการพัฒนาระบบปัญญาประดิษฐ์ (AI) ที่สามารถอธิบายเหตุผลของการตัดสินใจได้ชัดเจน และเพิ่มแนวทางจริยธรรมที่เข้มแข็งสำหรับการพัฒนาและการใช้งานปัญญาประดิษฐ์ (AI) ในระบบสุขภาพโดยเฉพาะ พร้อมทั้งปรับปรุงกฎหมายปัจจุบันให้รองรับความเสี่ยงที่เฉพาะเจาะจงของปัญญาประดิษฐ์ (AI) และรณรงค์ให้ผู้มีส่วนได้เสียทั้งหลาย เช่น ผู้ป่วย บุคลากรทางการแพทย์ นักกฎหมาย และนักจริยศาสตร์ ได้มีส่วนร่วมในการพัฒนาปัญญาประดิษฐ์ (AI) เพื่อให้สามารถยกระดับการดูแลสุขภาพผู้ป่วย สร้างความเท่าเทียม และเคารพสิทธิของผู้ป่วยในยุคที่สุขภาพดิจิทัล (Digital Health) กำลังเติบโต

บทความที่แปดบทความสุดท้าย หัวข้อ “Technological Experimentation Without Adequate Safeguards? Interoperable EU Databases and Access to the Multiple

Identity Detector by SIRENE Bureaux" โดย Diana Dimitrova และ Teresa Quintel ผู้เขียนอธิบายถึงผลกระทบของการทดลองใช้เทคโนโลยีในบริบทของฐานข้อมูลที่เชื่อมโยงกันของสหภาพยุโรป (EU) และการใช้งาน Multiple Identity Detector (MID) โดยหน่วยงาน SIRENE Bureaux โดยผู้เขียนตั้งคำถามถึงความสามารถของกลไกการป้องกันทางกฎหมายและการบังคับใช้กฎหมายที่มีอยู่ในการจัดการกับความเสี่ยงที่อาจจะเกิดขึ้น โดยเฉพาะอย่างยิ่งในแง่ความเป็นส่วนตัวของเจ้าของข้อมูล การคุ้มครองข้อมูล และสิทธิขั้นพื้นฐาน เนื่องจากผู้เขียนเห็นว่า การใช้เทคโนโลยีนั้นจักต้องอยู่ภายใต้การควบคุมดูแลอย่างรอบคอบ เพื่อให้เทคโนโลยีสามารถตอบสนองตามวัตถุประสงค์ที่ตั้งไว้ โดยไม่กระทบต่อสิทธิและเสรีภาพของบุคคล ในบทความผู้เขียนเริ่มจากการอธิบายถึงการพัฒนาฐานข้อมูลที่เชื่อมโยงหลายระบบของสหภาพยุโรปเข้าด้วยกัน เพื่อสนับสนุนการบังคับใช้กฎหมายเกี่ยวกับการจัดการผู้อพยพและเพิ่มความปลอดภัยภายในประเทศต่าง ๆ ของสหภาพยุโรป อันอาจกระทบจากการข้ามพรมแดนของผู้อพยพจำนวนมากในปัจจุบัน เช่น Schengen Information System (SIS), Visa Information System (VIS) และ Eurodac MID เป็นต้น การเชื่อมโยงฐานข้อมูลนั้นถูกออกแบบมาเพื่อช่วยระบุบุคคลที่มีมากกว่าหนึ่งตัวตน หรืออัตลักษณ์ (multiple identities) ที่บันทึกในฐานข้อมูล โดยมีหน่วยงาน SIRENE Bureaux ทำหน้าที่จัดการข้อมูลและอำนวยความสะดวกในการดำเนินการของระบบ ผู้เขียนยังชี้ถึงความเสี่ยงที่อาจจะเกิดขึ้นจากการใช้เทคโนโลยีดังกล่าว เช่น กรณีที่มีความผิดพลาดในฐานข้อมูลที่เชื่อมโยงในระบบใดระบบหนึ่ง ข้อผิดพลาดนั้นอาจส่งผลต่อระบบอื่น ๆ ให้มีข้อมูลที่ผิดไปด้วย ความเสี่ยงที่จะระบุตัวตนผิดหรือมีข้อมูลบางส่วนสูญหาย อันอาจส่งผลให้ผู้อพยพถูกปฏิเสธสิทธิหรือถูกติดตามโดยไม่เป็นธรรม และการนำฐานข้อมูลมาใช้ผิดวัตถุประสงค์ ซึ่งอาจนำไปสู่การละเมิดสิทธิขั้นพื้นฐานของประชาชน เป็นต้น ผู้เขียนวิเคราะห์ถึงความท้าทายดังกล่าวในขอบเขตของกฎหมายที่เกี่ยวข้อง กล่าวคือ กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation: GDPR) และหลักกฎหมายคุ้มครองสิทธิขั้นพื้นฐานแห่งสหภาพยุโรป (Charter of Fundamental Rights of the European Union: CFR) รวมทั้งเสนอคำเสนอแนะ

ในการแก้ไขปัญหาดังกล่าว เช่น การพัฒนามาตรการทางเทคนิคและกฎหมายที่แข็งแกร่งเพื่อสร้างความมั่นใจในความถูกต้องของข้อมูลและป้องกันการใช้งานในทางที่ผิด การเพิ่มความโปร่งใสโดยการแจ้งข้อมูลที่ชัดเจน และการจัดตั้งหน่วยงานอิสระเพื่อกำกับดูแลการใช้งาน MID และตรวจสอบความสอดคล้องกับกฎหมายคุ้มครองข้อมูล เป็นต้น

กล่าวโดยสรุป ข้าพเจ้าเห็นว่าหนังสือเล่มนี้เป็นหนังสือที่น่าสนใจ และเหมาะสำหรับนักกฎหมาย ผู้กำหนดนโยบาย นักวิจัย ผู้เชี่ยวชาญด้านเทคโนโลยี หรือบุคคลทั่วไปที่มีความสนใจทางด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคลและเทคโนโลยีปัญญาประดิษฐ์ เนื่องจากหนังสือเล่มนี้ได้รวบรวมบทความที่น่าสนใจเกี่ยวกับความสัมพันธ์ระหว่างเทคโนโลยีของปัญญาประดิษฐ์ และกฎหมายที่เกี่ยวข้องมาให้อ่านและทำความเข้าใจ เช่น บทบาทของปัญญาประดิษฐ์ในระบบสุขภาพ ความซับซ้อนทางกฎหมายของฐานข้อมูลที่เชื่อมโยงกันของสหภาพยุโรป และความท้าทายในการสร้างสมดุลระหว่างนวัตกรรมทางเทคโนโลยีและความเป็นส่วนตัวของข้อมูลและสิทธิขั้นพื้นฐานของประชาชน