



การกำกับดูแลอำนาจอธิปไตยทางดิจิทัล: การวิเคราะห์เปรียบเทียบการกำกับดูแลแบบ Ex-ante และ Ex-post ในสหภาพยุโรป จีน และอินเดีย Regulating Digital Sovereignty: A Comparative Analysis of Ex-ante and Ex-post Regulation in the EU, China, and India

¹เกียรติอนันต์ ล้วนแก้ว, ²ธัญพร สุนทรธรรม, ³ทงศักดิ์ ศิริยงค์, ⁴วรกฤษณ์ นัยพิน

¹Kiatanantha Lounkaew, ²Thanyaporn Soontornthum, ³Tanongsak Siriyong,

⁴Worakrit Nuypin

¹คณะเศรษฐศาสตร์ มหาวิทยาลัยธรรมศาสตร์

²วิทยาลัยสหวิทยาการ มหาวิทยาลัยธรรมศาสตร์

³สถาบันอาณานิคมศึกษา มหาวิทยาลัยธรรมศาสตร์

⁴บริษัท ไมล์ คอนซัลติ้ง กรุ๊ป จำกัด

¹Faculty of Economics, Thammasat University

²College of Interdisciplinary Studies, Thammasat University

³Thammasat Institute of Area Studies (TIARA), Thammasat University

⁴Miles Consulting Group Co.,Ltd., Thailand

¹Corresponding author, e-mail: klounakew@econ.tu.ac.th

Received: September 05, 2025; Revised: November 15, 2025; Accepted: November 24, 2025



บทคัดย่อ

บทความนี้เป็นการศึกษาเปรียบเทียบการกำกับดูแลอำนาจอธิปไตยทางดิจิทัลผ่านกรอบการกำกับดูแลเชิงป้องกัน (Ex-ante) และการกำกับดูแลภายหลัง (Ex-post) โดยมุ่งเน้นกรณีศึกษาของสหภาพยุโรป จีน และอินเดีย ผ่านการวิเคราะห์กรอบการกำกับดูแล กลไกการบังคับใช้ และโครงสร้างสถาบัน การศึกษาพบว่า สหภาพยุโรปใช้การกำกับดูแลเชิงป้องกันด้วยกรอบที่ครอบคลุมอย่างกฎหมายคุ้มครองข้อมูลส่วนบุคคล (General Data Protection Regulation หรือ GDPR) และพระราชบัญญัติตลาดดิจิทัล (Digital Market Act หรือ DMA) จีนใช้แนวทางแบบผสมผสานที่รวมกฎระเบียบเข้มงวดกับการบังคับใช้ที่ยืดหยุ่น ขณะที่อินเดียกำลังเปลี่ยนจากการกำกับดูแลภายหลังไปสู่รูปแบบผสมผสาน ผลการวิจัยชี้ว่าประสิทธิภาพของแนวทางเหล่านี้ได้รับอิทธิพลจากขีดความสามารถของสถาบัน แรงจูงใจทางเศรษฐกิจ และบริบททางการเมือง แนวทางการกำกับดูแลเชิงป้องกันของสหภาพยุโรปสร้างความชัดเจนแต่อาจขัดขวางนวัตกรรมเนื่องจากต้นทุนการปฏิบัติตามสูง รูปแบบผสมผสานของจีนมีความยืดหยุ่นแต่สร้างความไม่แน่นอนในการบังคับใช้ กรอบของอินเดียแสดงถึงความท้าทายของประเทศกำลังพัฒนาในการสร้างสมดุลระหว่างการเติบโตทางเศรษฐกิจดิจิทัลกับข้อกังวลด้านอธิปไตย งานวิจัยยังชี้ให้เห็นแนวโน้มการหลอมรวมระหว่างแนวทางการกำกับดูแลเชิงป้องกันและการกำกับดูแลภายหลัง การเสริมสร้างขีดความสามารถของสถาบัน และความสำคัญของความร่วมมือระหว่างประเทศ ผลการวิจัยมีส่วนช่วยทั้งในด้านความเข้าใจเชิงทฤษฎีและการพัฒนานโยบาย โดยชี้ว่ากรอบอำนาจ



อธิปไตยทางดิจิทัลที่ประสบความสำเร็จต้องปรับเทียบระหว่างมาตรการเชิงป้องกันและเชิงตอบสนองตามบริบทของแต่ละประเทศ

คำสำคัญ: อำนาจอธิปไตยทางดิจิทัล; การกำกับดูแลเชิงป้องกัน; การกำกับดูแลภายหลัง; การกำกับดูแลข้อมูล; กรอบการกำกับดูแล

Abstract

This paper examines the comparative approaches to digital sovereignty regulation through ex-ante and ex-post frameworks, focusing on three significant case studies: the European Union, China, and India. Through a systematic analysis of regulatory frameworks, enforcement mechanisms, and institutional structures, we investigate how different jurisdictions balance preventive and reactive regulatory approaches in maintaining digital sovereignty. The study reveals that while the EU predominantly employs ex-ante regulation through comprehensive frameworks like General Data Protection Regulation (GDPR) and Digital Market Act (DMA), China adopts a hybrid approach combining stringent rules with flexible enforcement, and India is transitioning from an ex-post to a hybrid model. Our findings indicate that the effectiveness of these regulatory approaches is heavily influenced by institutional capacity, economic incentives, and political contexts. The EU's strict ex-ante approach provides clarity but may impede innovation due to high compliance costs, while China's hybrid model offers flexibility but creates uncertainty in enforcement. India's evolving framework demonstrates the challenges developing nations face in balancing digital economic growth with sovereignty concerns. The research also highlights emerging trends in digital sovereignty regulation, including increasing convergence between ex-ante and ex-post approaches, growing emphasis on institutional capacity building, and rising importance of international cooperation. These findings contribute to both theoretical understanding of digital sovereignty regulation and practical policy development, suggesting that successful digital sovereignty frameworks require careful calibration of preventive and reactive measures based on national contexts and capabilities.

Keywords: Digital sovereignty; Ex-ante regulation; Ex-post regulation; Data governance; Regulatory Frameworks

บทนำ

ในทศวรรษที่ผ่านมา แนวคิดเรื่องอำนาจอธิปไตยทางดิจิทัลได้กลายเป็นประเด็นสำคัญในการกำกับดูแลโลกไซเบอร์และเทคโนโลยีดิจิทัล โดยรัฐต่างๆ ทั่วโลกพยายามที่จะรักษาอำนาจอธิปไตยของตนในยุคดิจิทัล ท่ามกลางความท้าทายจากการไหลเวียนของข้อมูลข้ามพรมแดนและอิทธิพลของบริษัทเทคโนโลยียักษ์ใหญ่ (Pohle & Thiel, 2020) อำนาจอธิปไตยทางดิจิทัลครอบคลุมประเด็นสำคัญหลายด้าน ทั้งการควบคุมข้อมูล โครงสร้างพื้นฐานดิจิทัล และการกำกับดูแลแพลตฟอร์มออนไลน์ โดยมีเป้าหมายเพื่อปกป้องผลประโยชน์ของประเทศและพลเมืองในยุคดิจิทัล



การกำกับดูแลอำนาจอธิปไตยทางดิจิทัลสามารถดำเนินการได้สองรูปแบบหลัก คือ การกำกับดูแลเชิงป้องกัน (Ex-ante) และการกำกับดูแลภายหลัง (Ex-post) โดยการกำกับดูแลเชิงป้องกันมุ่งเน้นการวางกฎระเบียบและมาตรการล่วงหน้าเพื่อป้องกันปัญหาที่อาจเกิดขึ้น ในขณะที่การกำกับดูแลภายหลังเน้นการตอบสนองและแก้ไขปัญหาเมื่อเกิดขึ้นแล้ว (Floridi, 2020) การเลือกใช้รูปแบบการกำกับดูแลที่เหมาะสมมีความสำคัญอย่างยิ่งต่อประสิทธิภาพในการรักษาอำนาจอธิปไตยทางดิจิทัล

ในช่วงไม่กี่ปีที่ผ่านมา หลายประเทศได้พัฒนากรอบการกำกับดูแลที่แตกต่างกันไป สหภาพยุโรปเน้นการกำกับดูแลเชิงป้องกันผ่านกฎหมายสำคัญอย่าง GDPR และ Digital Markets Act โดยวางมาตรฐานที่ครอบคลุมและเข้มงวดตั้งแต่ต้นเพื่อป้องกันการละเมิดสิทธิและสร้างความปลอดภัยในระบบนิเวศดิจิทัล ในขณะที่จีนใช้แนวทางผสมผสานระหว่างการกำกับดูแลเชิงป้องกันและภายหลัง โดยมีกฎหมายที่เข้มงวดแต่ยืดหยุ่นในการบังคับใช้ตามบริบทและความจำเป็นทางเศรษฐกิจและความมั่นคงของประเทศ (Belli, 2024) สำหรับอินเดีย ประเทศกำลังพัฒนาที่มีตลาดดิจิทัลขนาดใหญ่ กำลังอยู่ในช่วงเปลี่ยนผ่านจากการกำกับดูแลภายหลังที่เน้นการตอบสนองต่อปัญหาเฉพาะกรณีไปสู่การพัฒนากรอบการกำกับดูแลที่ครอบคลุมมากขึ้น โดยพยายามสร้างสมดุลระหว่างการส่งเสริมการเติบโตของเศรษฐกิจดิจิทัลกับการรักษาอำนาจอธิปไตยและความมั่นคงของประเทศ การศึกษาเปรียบเทียบแนวทางการกำกับดูแลเหล่านี้จะช่วยให้เข้าใจข้อดีข้อเสียและความท้าทายของแต่ละรูปแบบได้ชัดเจนยิ่งขึ้น

ความท้าทายสำคัญในการกำกับดูแลอำนาจอธิปไตยทางดิจิทัล คือ การสร้างสมดุลระหว่างการปกป้องผลประโยชน์ของประเทศกับการส่งเสริมนวัตกรรมและการเติบโตทางเศรษฐกิจ การกำกับดูแลที่เข้มงวดเกินไปอาจส่งผลเสียต่อการพัฒนาเศรษฐกิจดิจิทัล ในขณะที่การกำกับดูแลที่หละหลวมเกินไปอาจทำให้ประเทศสูญเสียอำนาจในการควบคุมข้อมูลและโครงสร้างพื้นฐานสำคัญ (Vila Seoane, 2021) นอกจากนี้ ความแตกต่างของบริบททางการเมือง เศรษฐกิจ และสังคมยังส่งผลต่อการเลือกใช้รูปแบบการกำกับดูแลที่เหมาะสมของแต่ละประเทศ การวิเคราะห์เปรียบเทียบแนวทางการกำกับดูแลอำนาจอธิปไตยทางดิจิทัลระหว่างประเทศจึงมีความสำคัญต่อการพัฒนานโยบายที่มีประสิทธิภาพ โดย Gupta and Sony (2021) ชี้ให้เห็นว่าการแลกเปลี่ยนบทเรียนและประสบการณ์ระหว่างประเทศจะช่วยให้เกิดการเรียนรู้และพัฒนากรอบการกำกับดูแลที่เหมาะสมยิ่งขึ้น ทั้งนี้ความร่วมมือระหว่างประเทศยังมีความจำเป็นในการจัดการกับความท้าทายข้ามพรมแดนที่เกี่ยวข้องกับอำนาจอธิปไตยทางดิจิทัล

บทความวิจัยนี้จะนำเสนอการวิเคราะห์เปรียบเทียบรูปแบบการกำกับดูแลอำนาจอธิปไตยทางดิจิทัลระหว่างสหภาพยุโรป จีน และอินเดีย โดยมุ่งเน้นที่ความแตกต่างระหว่างการกำกับดูแลเชิงป้องกันและการกำกับดูแลภายหลัง ในส่วนถัดไปจะอธิบายถึงกรอบแนวคิดทฤษฎีเกี่ยวกับการกำกับดูแลทั้งสองรูปแบบ ตามด้วยระเบียบวิธีวิจัยและการวิเคราะห์กรณีศึกษาของแต่ละประเทศ จากนั้นจะเป็นการอภิปรายผลการศึกษาและข้อเสนอแนะเชิงนโยบาย และสรุปด้วยข้อสังเกตสำคัญเกี่ยวกับอนาคตของการกำกับดูแลอำนาจอธิปไตยทางดิจิทัล

วัตถุประสงค์การศึกษา

การวิจัยนี้มีวัตถุประสงค์เพื่อวิเคราะห์เปรียบเทียบแนวทางการกำกับดูแลอำนาจอธิปไตยทางดิจิทัลระหว่างการกำกับดูแลเชิงป้องกัน (Ex-ante regulation) และการกำกับดูแลภายหลัง (Ex-post regulation) ในสหภาพยุโรป จีน และอินเดีย ศึกษากรอบการกำกับดูแล กลไกการบังคับใช้ และโครงสร้างสถาบันของแต่ละกรณีศึกษา รวมทั้งประเมินประสิทธิภาพและความท้าทายของแต่ละแนวทางในบริบททางการเมือง เศรษฐกิจ และสังคมที่แตกต่างกัน เพื่อนำไปสู่ความเข้าใจเกี่ยวกับการสร้างสมดุล

ระหว่างมาตรการเชิงป้องกันและเชิงตอบสนองในการรักษาอำนาจอธิปไตยทางดิจิทัลที่เหมาะสมตามบริบทของแต่ละประเทศ

กรอบแนวคิดทฤษฎี

การศึกษาเปรียบเทียบการกำกับดูแลอำนาจอธิปไตยทางดิจิทัลจำเป็นต้องอาศัยความเข้าใจพื้นฐานเกี่ยวกับแนวคิดทฤษฎีที่เกี่ยวข้อง โดยเฉพาะความแตกต่างระหว่างการกำกับดูแลเชิงป้องกัน (Ex-ante) และการกำกับดูแลภายหลัง (Ex-post) รวมถึงองค์ประกอบสำคัญของอำนาจอธิปไตยทางดิจิทัล การทบทวนวรรณกรรมที่เกี่ยวข้องแสดงให้เห็นว่าการกำกับดูแลทั้งสองรูปแบบมีจุดแข็งและข้อจำกัดที่แตกต่างกัน โดยประสิทธิภาพของแต่ละรูปแบบขึ้นอยู่กับบริบทและเป้าหมายของการกำกับดูแล

การกำกับดูแลเชิงป้องกัน (Ex-ante Regulation) เป็นแนวทางที่มุ่งเน้นการวางกฎระเบียบและมาตรการล่วงหน้าเพื่อป้องกันปัญหาที่อาจเกิดขึ้น Khasanova and Tai (2024) อธิบายว่าแนวทางนี้มักใช้ในกรณีที่ความเสียหายที่อาจเกิดขึ้นมีความรุนแรงและยากต่อการแก้ไขในภายหลัง ตัวอย่างที่เห็นได้ชัดคือการกำกับดูแลของสหภาพยุโรปผ่านกฎหมาย GDPR ที่กำหนดมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลอย่างเข้มงวดตั้งแต่ต้น การกำกับดูแลเชิงป้องกันมีข้อดีในแง่ของการสร้างความชัดเจนและความแน่นอนในการปฏิบัติตามกฎระเบียบ ผู้ประกอบการสามารถทราบล่วงหน้าว่าต้องปฏิบัติตามอย่างไร ช่วยลดความเสี่ยงและต้นทุนในการดำเนินการ อย่างไรก็ตาม Braun and Hummel (2024) ชี้ให้เห็นว่าการกำกับดูแลเชิงป้องกันอาจสร้างภาระและต้นทุนที่สูงเกินจำเป็น และอาจไม่สามารถปรับตัวให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีได้อย่างรวดเร็ว

ในทางตรงกันข้าม การกำกับดูแลภายหลัง (Ex-post Regulation) เน้นการตอบสนองและแก้ไขปัญหาเมื่อเกิดขึ้นแล้ว Vila Seoane (2021) อธิบายว่าแนวทางนี้มีความยืดหยุ่นมากกว่าและสามารถปรับตัวให้เข้ากับสถานการณ์ที่เปลี่ยนแปลงได้ดี อย่างไรก็ตาม ความท้าทายสำคัญ คือ การแก้ไขความเสียหายที่เกิดขึ้นแล้วอาจทำได้ยากหรือมีต้นทุนสูง ประเทศต่างๆ มักใช้การผสมผสานระหว่างการกำกับดูแลทั้งสองรูปแบบ โดย Donnelly et al. (2024) ชี้ให้เห็นว่าจีนใช้แนวทางผสมผสานในการกำกับดูแลข้อมูลส่วนบุคคลและความมั่นคงทางไซเบอร์ โดยมีทั้งมาตรการเชิงป้องกันผ่านกฎหมายความมั่นคงทางไซเบอร์ และการตอบสนองภายหลังผ่านการบังคับใช้กฎหมายและการลงโทษ

อำนาจอธิปไตยทางดิจิทัลประกอบด้วยหลายมิติที่เชื่อมโยงกัน Pohle and Santaniello (2024) ระบุองค์ประกอบสำคัญสามประการ ได้แก่ การควบคุมข้อมูล โครงสร้างพื้นฐานดิจิทัล และการกำกับดูแลแพลตฟอร์ม การควบคุมข้อมูลเป็นองค์ประกอบพื้นฐาน ครอบคลุมทั้งการกำหนดนโยบายการจัดเก็บข้อมูลในประเทศ (Data Localization) และการควบคุมการไหลเวียนของข้อมูลข้ามพรมแดน โครงสร้างพื้นฐานดิจิทัลเป็นอีกองค์ประกอบสำคัญที่รัฐต้องควบคุมเพื่อรักษาอำนาจอธิปไตย Sheikh (2022) อธิบายว่าการพึ่งพาโครงสร้างพื้นฐานจากต่างประเทศมากเกินไปอาจทำให้ประเทศเสียเปรียบและขาดความมั่นคง โดยเฉพาะในด้านการสื่อสารและการประมวลผลข้อมูล การกำกับดูแลแพลตฟอร์มดิจิทัลเป็นองค์ประกอบที่มีความสำคัญมากขึ้นในปัจจุบัน เนื่องจากแพลตฟอร์มขนาดใหญ่มีอิทธิพลอย่างมากต่อเศรษฐกิจและสังคม Hoeffler and Mérand (2024) ชี้ให้เห็นว่าการกำกับดูแลแพลตฟอร์มต้องคำนึงถึงทั้งมิติด้านการแข่งขัน ความมั่นคง และการคุ้มครองผู้บริโภค

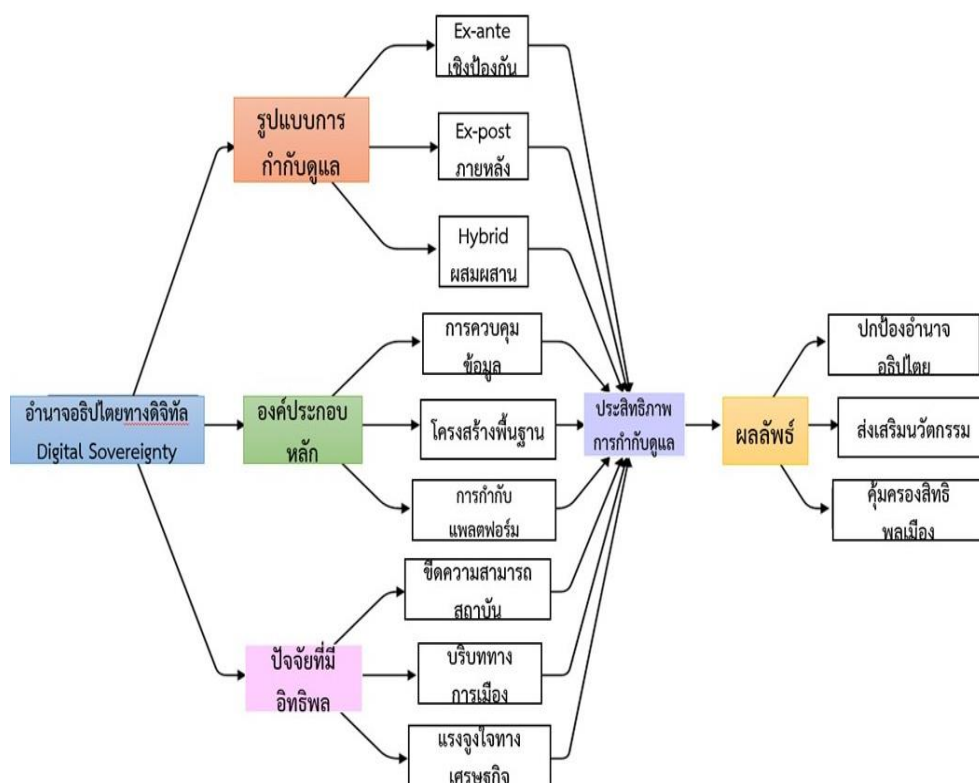
การบังคับใช้และการกำกับดูแลอำนาจอธิปไตยทางดิจิทัลมีความซับซ้อนและแตกต่างกันในแต่ละประเทศ Leese (2024) พบว่า ประสิทธิภาพของการกำกับดูแลขึ้นอยู่กับปัจจัยหลายประการ ทั้งความเข้มแข็งของสถาบันกำกับดูแล กลไกการบังคับใช้กฎหมาย และความร่วมมือระหว่างหน่วยงานที่



เกี่ยวข้องกับ Fratini et al. (2024) ซึ่งให้เห็นความแตกต่างระหว่างประเทศที่มีหน่วยงานกำกับดูแลแบบรวมศูนย์กับแบบกระจายอำนาจ ซึ่งแต่ละรูปแบบมีข้อดีและข้อจำกัดที่แตกต่างกัน นอกจากนี้ บทบาทของภาคเอกชนในการกำกับดูแลก็มีความสำคัญไม่น้อย Lehuédé (2024) อธิบายว่าในหลายประเทศภาคเอกชนมีส่วนร่วมในการพัฒนามาตรฐานและแนวปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคล

การรักษาอำนาจอธิปไตยทางดิจิทัลต้องเผชิญกับความท้าทายในการสร้างสมดุลระหว่างผลประโยชน์ที่แข่งขันกัน Belli (2024) วิเคราะห์ว่าประเทศต่างๆ ต้องพิจารณาถึงผลกระทบทั้งด้านความมั่นคง เศรษฐกิจ และสิทธิเสรีภาพของประชาชน การกำกับดูแลที่เข้มงวดเกินไปอาจส่งผลกระทบต่อพัฒนานวัตกรรมและการเติบโตทางเศรษฐกิจ ในขณะที่การกำกับดูแลที่หละหลวมเกินไปอาจทำให้ประเทศสูญเสียความสามารถในการควบคุมข้อมูลและโครงสร้างพื้นฐานที่สำคัญ ความท้าทายอีกประการหนึ่งคือการรักษาสมดุลระหว่างความร่วมมือระหว่างประเทศกับการปกป้องผลประโยชน์แห่งชาติ Gupta and Sony (2021) อธิบายว่าในโลกดิจิทัลที่เชื่อมโยงกัน การโดดเดี่ยวตัวเองโดยสมบูรณ์เป็นสิ่งที่เป็นไปได้ยาก ประเทศต่างๆ จึงต้องหาจุดสมดุลระหว่างการรักษาอำนาจอธิปไตยกับการมีส่วนร่วมในระบบดิจิทัลโลก

จากการทบทวนกรอบแนวคิดทฤษฎีข้างต้น จะเห็นว่าอำนาจอธิปไตยทางดิจิทัลเป็นแนวคิดที่มีความซับซ้อนและหลายมิติ การเลือกใช้รูปแบบการกำกับดูแลที่เหมาะสมต้องคำนึงถึงปัจจัยต่างๆ อย่างรอบด้าน ทั้งด้านการบังคับใช้กฎหมาย การสร้างขีดความสามารถ และผลกระทบทางเศรษฐกิจ นอกจากนี้ยังต้องพิจารณาถึงบริบทเฉพาะของแต่ละประเทศและความท้าทายในการสร้างสมดุลระหว่างผลประโยชน์ที่แข่งขันกัน ภาพที่ 1 แสดงกรอบแนวคิดการวิเคราะห์การกำกับดูแลอำนาจอธิปไตยทางดิจิทัลที่ใช้ในการศึกษานี้ โดยเชื่อมโยงความสัมพันธ์ระหว่างรูปแบบการกำกับดูแล องค์ประกอบสำคัญ และปัจจัยที่มีอิทธิพล



ภาพที่ 1 กรอบแนวคิดการวิเคราะห์การกำกับดูแลอำนาจอธิปไตยทางดิจิทัล

วิธีดำเนินการวิจัย

การศึกษานี้เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) ที่มุ่งเน้นการทำความเข้าใจเชิงลึกเกี่ยวกับปรากฏการณ์การกำกับดูแลอำนาจดิจิทัลในบริบทที่แตกต่างกัน โดยใช้การวิจัยเชิงเอกสาร (Documentary Research) โดยเก็บข้อมูลเชิงลึกประกอบด้วยบทความวิชาการด้านนโยบายสาธารณะและการกำกับดูแลดิจิทัล บทความด้านกฎหมาย ซึ่งได้รับการตีพิมพ์ในวารสารที่มีการประเมินโดยผู้ทรงคุณวุฒิ (Peer-reviewed Journals) ในช่วงปี 2020-2024 และนโยบายไซเบอร์ เอกสารนโยบาย ตลอดจนรายงานการวิจัยจากหน่วยงานที่เกี่ยวข้อง รวมถึงกฎหมายและนโยบายที่เกี่ยวข้องของแต่ละประเทศ เพื่อให้ได้ข้อมูลที่ทันสมัยและสะท้อนพลวัตของการกำกับดูแลในปัจจุบัน

การเลือกสหภาพยุโรป จีน และอินเดียเป็นกรณีศึกษาอยู่บนพื้นฐานของเกณฑ์สามประการสำคัญ ดังนี้ ประการแรก ทั้งสามกรณีแสดงให้เห็นความหลากหลายของแนวทางการกำกับดูแล โดยสหภาพยุโรปเน้น ex-ante regulation จีนใช้แนวทางผสมผสาน และอินเดีกำลังพัฒนาจาก ex-post สู่แนวทางผสมผสาน ประการที่สอง ทั้งสามกรณีเป็นตัวแทนของตลาดดิจิทัลขนาดใหญ่และมีอิทธิพลต่อการกำหนดนโยบายดิจิทัลในระดับโลก และประการที่สาม การเลือกกรณีศึกษาที่มีระดับการพัฒนาแตกต่างกันช่วยให้เข้าใจความท้าทายและแนวทางการกำกับดูแลในบริบทที่หลากหลาย

การวิเคราะห์เปรียบเทียบใช้กรอบที่พัฒนาจากการทบทวนวรรณกรรม โดยมุ่งเน้นการศึกษาพัฒนาการของกรอบการกำกับดูแล แนวทางการกำกับดูแลแบบ ex-ante และ ex-post บทบาทของสถาบันและโครงสร้างการกำกับดูแล รวมถึงความท้าทายและผลกระทบของการกำกับดูแล การวิเคราะห์ครอบคลุมทั้งมิติเชิงกฎหมาย สถาบัน และผลกระทบทางเศรษฐกิจและสังคมอย่างกว้างขวาง มีข้อจำกัดว่า การวิเคราะห์อาศัยข้อมูลทุติยภูมิเป็นหลัก การเข้าถึงข้อมูลบางส่วนอาจมีข้อจำกัด โดยเฉพาะในกรณีของจีน นอกจากนี้ การเปลี่ยนแปลงอย่างรวดเร็วของนโยบายและการกำกับดูแล รวมถึงความแตกต่างทางภาษาและวัฒนธรรมอาจส่งผลกระทบต่อความถูกต้อง การตระหนักถึงข้อจำกัดเหล่านี้ช่วยให้สามารถพิจารณาผลการศึกษได้อย่างเหมาะสมและระบุโอกาสสำหรับการวิจัยในอนาคต

ผลการศึกษา

ผลการศึกษาในสามกรณีศึกษาเผยให้เห็นความหลากหลายของแนวทางที่สะท้อนบริบททางการเมือง เศรษฐกิจ และสังคมที่แตกต่างกัน ดังนี้

1) สหภาพยุโรป กรณีศึกษาของการกำกับดูแลเชิงป้องกันผ่านกรอบกฎหมายที่ครอบคลุม

สหภาพยุโรปเป็นตัวอย่างที่โดดเด่นของการใช้แนวทางการกำกับดูแลเชิงป้องกัน (ex-ante regulation) ในการรักษาอำนาจดิจิทัลทางดิจิทัล Christakis (2020) วิเคราะห์ว่าแนวทางของสหภาพยุโรปมุ่งเน้นการสร้างกรอบกฎหมายที่ครอบคลุมและการวางมาตรฐานที่ชัดเจนล่วงหน้า โดยมี GDPR เป็นตัวอย่างสำคัญของการกำกับดูแลในลักษณะนี้

การพัฒนากรอบการกำกับดูแลของสหภาพยุโรปมีพื้นฐานมาจากความตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลและสิทธิพื้นฐานของพลเมือง Sheikh (2022) ชี้ให้เห็นว่าเหตุการณ์สำคัญที่กระตุ้นให้เกิดการพัฒนากรอบการกำกับดูแลที่เข้มแข็ง คือ การเปิดเผยข้อมูลของ Edward Snowden เกี่ยวกับการสอดแนมข้อมูลในวงกว้างโดยหน่วยงานความมั่นคงของสหรัฐอเมริกา

GDPR ที่มีผลบังคับใช้ในปี 2018 เป็นกฎหมายที่กำหนดมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ครอบคลุมและเข้มงวด Broeders et al. (2023) อธิบายว่า GDPR ไม่เพียงแต่กำหนดหลักการพื้นฐานในการประมวลผลข้อมูลส่วนบุคคล แต่ยังรวมถึงกลไกการบังคับใช้ที่มีประสิทธิภาพ เช่น การกำหนด



บทลงโทษที่รุนแรงสำหรับการละเมิด และการจัดตั้งหน่วยงานกำกับดูแลในแต่ละประเทศสมาชิก นอกจาก GDPR แล้ว สหภาพยุโรปยังได้พัฒนากฎหมายสำคัญอื่นๆ เพื่อกำกับดูแลระบบนิเวศดิจิทัล Digital Markets Act (DMA) และ Digital Services Act (DSA) เป็นตัวอย่างของกฎหมายที่มุ่งควบคุมแพลตฟอร์มดิจิทัลขนาดใหญ่ Hoeffler and Mérand (2024) วิเคราะห์ว่ากฎหมายเหล่านี้สะท้อนความพยายามของสหภาพยุโรปในการสร้างสมดุลระหว่างการส่งเสริมนวัตกรรมกับการปกป้องสิทธิของผู้บริโภคและการแข่งขันที่เป็นธรรม

ในด้านโครงสร้างพื้นฐาน สหภาพยุโรปได้ริเริ่มโครงการ GAIA-X ซึ่งเป็นความพยายามในการสร้างระบบคลาวด์ที่มีความเป็นอิสระและปลอดภัย Autolitano and Pawlowska (2021) อธิบายว่าโครงการนี้มีเป้าหมายเพื่อลดการพึ่งพาผู้ให้บริการคลาวด์จากสหรัฐอเมริกาและจีน และสร้างระบบนิเวศดิจิทัลที่สอดคล้องกับมาตรฐานและค่านิยมของยุโรป

อย่างไรก็ตาม การกำกับดูแลแบบเชิงป้องกันของสหภาพยุโรปก็เผชิญกับความท้าทายบางประการ Monsees and Lambach (2022) ชี้ให้เห็นว่าการบังคับใช้กฎหมายที่เข้มงวดอาจสร้างภาระให้กับผู้ประกอบการ โดยเฉพาะธุรกิจขนาดเล็กและขนาดกลาง นอกจากนี้ความแตกต่างในการตีความและการบังคับใช้กฎหมายระหว่างประเทศสมาชิกก็เป็นประเด็นที่ต้องจัดการ แม้จะมีความท้าทาย แต่แนวทางการกำกับดูแลของสหภาพยุโรปได้กลายเป็นแบบอย่างสำหรับหลายประเทศ Lehuedé (2024) วิเคราะห์ว่า “Brussels Effect” หรืออิทธิพลของมาตรฐานการกำกับดูแลของสหภาพยุโรปได้ส่งผลให้หลายประเทศพัฒนากฎหมายคุ้มครองข้อมูลส่วนบุคคลที่คล้ายคลึงกับ GDPR นอกจากนี้บริษัทเทคโนโลยีขนาดใหญ่ก็ต้องปรับตัวให้สอดคล้องกับมาตรฐานของสหภาพยุโรปเพื่อให้สามารถดำเนินธุรกิจในตลาดยุโรปได้

2) จีน กรณีสึกษาของการผสมผสานระหว่างการควบคุมที่เข้มงวดและความยืดหยุ่นในการบังคับใช้

จีนนำเสนอรูปแบบที่น่าสนใจของการผสมผสานระหว่างการกำกับดูแลเชิงป้องกันและการกำกับดูแลภายหลัง Khasanova and Tai (2024) วิเคราะห์ว่าจีนได้พัฒนารอบกฎหมายที่ครอบคลุมสำหรับการกำกับดูแลข้อมูลและความมั่นคงทางไซเบอร์ โดยมีกฎหมายสำคัญสามฉบับ ได้แก่ กฎหมายความมั่นคงทางไซเบอร์ (Cybersecurity Law) กฎหมายความมั่นคงข้อมูล (Data Security Law) และกฎหมายคุ้มครองข้อมูลส่วนบุคคล (Personal Information Protection Law)

การพัฒนารอบการกำกับดูแลของจีนมีลักษณะเฉพาะที่สะท้อนบริบททางการเมืองและเศรษฐกิจของประเทศ Fratini et al. (2024) ชี้ให้เห็นว่าจีนให้ความสำคัญกับการรักษาความมั่นคงของรัฐและการควบคุมเนื้อหาออนไลน์ ในขณะที่เดียวกันพยายามส่งเสริมการพัฒนาอุตสาหกรรมเทคโนโลยีภายในประเทศ การกำกับดูแลจึงต้องสร้างสมดุลระหว่างการควบคุมที่เข้มงวดกับการส่งเสริมนวัตกรรม

ในด้านโครงสร้างการกำกับดูแล จีนมีการกระจายอำนาจระหว่างหลายหน่วยงาน Vila Seoane (2021) อธิบายว่าหน่วยงานหลักในการกำกับดูแล ได้แก่ Cyberspace Administration of China (CAC) Ministry of Industry and Information Technology (MIIT) และหน่วยงานระดับท้องถิ่น การมีหลายหน่วยงานที่เกี่ยวข้องสร้างความท้าทายในการประสานงาน แต่ก็ช่วยให้การกำกับดูแลมีความยืดหยุ่นและตอบสนองต่อบริบทที่แตกต่างกันได้ดีขึ้น

กฎหมายความมั่นคงทางไซเบอร์ของจีนที่มีผลบังคับใช้ในปี 2017 วางรากฐานสำคัญสำหรับการกำกับดูแลข้อมูลและความมั่นคงทางไซเบอร์ Leese (2024) วิเคราะห์ว่ากฎหมายนี้ให้อำนาจรัฐในการควบคุมการไหลเวียนของข้อมูลและกำหนดมาตรฐานความปลอดภัยสำหรับโครงสร้างพื้นฐานที่สำคัญ นอกจากนี้ยังกำหนดให้ข้อมูลสำคัญต้องจัดเก็บภายในประเทศจีน โดยการบังคับใช้กฎหมายของจีนมี



ลักษณะที่ยืดหยุ่นและเลือกใช้ตามความเหมาะสม Donnelly et al. (2024) ชี้ให้เห็นว่าแม้จะมีกฎระเบียบที่เข้มงวด แต่การบังคับใช้มักคำนึงถึงผลกระทบทางเศรษฐกิจและความเป็นไปได้ในทางปฏิบัติ ตัวอย่าง เช่น การผ่อนปรนระยะเวลาในการปฏิบัติตามข้อกำหนดบางประการ หรือการเปิดโอกาสให้มีการหารือเพื่อปรับปรุงกฎระเบียบให้เหมาะสมยิ่งขึ้น

จีนยังให้ความสำคัญกับการพัฒนาเทคโนโลยีและนวัตกรรมภายในประเทศ Hoeffler and Mérand (2024) อธิบายว่านโยบาย Made in China 2025 และแผนพัฒนาเทคโนโลยีอื่นๆ สะท้อนความพยายามของจีนในการลดการพึ่งพาเทคโนโลยีต่างชาติและสร้างความเป็นผู้นำในอุตสาหกรรมเทคโนโลยีขั้นสูง การกำกับดูแลจึงต้องสนับสนุนเป้าหมายเชิงยุทธศาสตร์นี้ด้วย อย่างไรก็ตาม แนวทางการกำกับดูแลของจีนก็เผชิญกับข้อวิจารณ์บางประการ Belli (2024) ชี้ให้เห็นว่าการควบคุมที่เข้มงวดของรัฐอาจส่งผลกระทบต่อสิทธิเสรีภาพของประชาชนและการแข่งขันในตลาด นอกจากนี้ความไม่ชัดเจนในการตีความกฎหมายและการทับซ้อนของอำนาจหน้าที่ระหว่างหน่วยงานเป็นประเด็นที่ต้องได้รับการแก้ไข

3) อินเดีย กรณีศึกษาของการพัฒนาแนวทางการกำกับดูแลท่ามกลางการเปลี่ยนแปลงทางดิจิทัล

อินเดียนำเสนอกกรณีศึกษาที่น่าสนใจของประเทศกำลังพัฒนาที่กำลังพยายามสร้างสมดุลระหว่างการพัฒนาเศรษฐกิจดิจิทัลกับการรักษาอำนาจอธิปไตยทางดิจิทัล Prasad (2022) วิเคราะห์ว่าอินเดียมีการพัฒนารอบการกำกับดูแลที่ค่อยๆ ปรับเปลี่ยนจากการตอบสนองต่อปัญหาเฉพาะหน้า (ex-post) ไปสู่การวางระบบการกำกับดูแลที่ครอบคลุมมากขึ้น

โครงการ Aadhaar ซึ่งเป็นระบบยืนยันตัวตนทางดิจิทัลขนาดใหญ่ที่สุดในโลก เป็นตัวอย่างสำคัญของความพยายามในการสร้างโครงสร้างพื้นฐานดิจิทัลของอินเดีย Vila Seoane (2021) อธิบายว่า Aadhaar ไม่เพียงแต่เป็นระบบการยืนยันตัวตน แต่ยังเป็นรากฐานสำคัญสำหรับการพัฒนาบริการดิจิทัลและการรวบรวมข้อมูลของรัฐ แม้จะมีข้อกังวลเรื่องความเป็นส่วนตัวและการรั่วไหลของข้อมูล

ในด้านการคุ้มครองข้อมูลส่วนบุคคล อินเดียได้พัฒนาร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Bill) ที่ได้รับอิทธิพลจาก GDPR ของสหภาพยุโรป Gupta and Sony (2021) วิเคราะห์ว่ากฎหมายนี้พยายามสร้างสมดุลระหว่างการคุ้มครองสิทธิของประชาชนกับการส่งเสริมนวัตกรรมและการพัฒนาเศรษฐกิจดิจิทัล แม้จะมีการวิพากษ์วิจารณ์ว่าให้อำนาจรัฐมากเกินไปในบางประเด็น

นอกจากนี้ อินเดียยังมีนโยบาย “Digital India” ที่มุ่งส่งเสริมการพัฒนาโครงสร้างพื้นฐานดิจิทัลและการใช้เทคโนโลยีเพื่อพัฒนาประเทศ Belli (2024) ชี้ให้เห็นว่านโยบายนี้สะท้อนความพยายามของอินเดียในการใช้เทคโนโลยีดิจิทัลเป็นเครื่องมือในการพัฒนาเศรษฐกิจและสังคม ในขณะเดียวกันก็พยายามรักษาอำนาจอธิปไตยทางดิจิทัลผ่านมาตรการต่างๆ เช่น การกำหนดให้จัดเก็บข้อมูลในประเทศ

การตัดสินใจห้ามแอปพลิเคชันจากจีนจำนวนมากในปี 2020 แสดงให้เห็นถึงความกังวลด้านความมั่นคงและอำนาจอธิปไตยทางดิจิทัลของอินเดีย Monsees and Lambach (2022) วิเคราะห์ว่าการตัดสินใจดังกล่าวสะท้อนให้เห็นว่าอินเดียพร้อมที่จะใช้มาตรการเด็ดขาดเพื่อปกป้องผลประโยชน์ด้านความมั่นคง แม้จะมีผลกระทบต่อผู้ใช้งานและภาคธุรกิจ

อย่างไรก็ตาม การพัฒนารอบการกำกับดูแลของอินเดียยังเผชิญกับความท้าทายหลายประการ Lehuédé (2024) ชี้ให้เห็นปัญหาสำคัญ เช่น ความล่าช้าในการออกกฎหมายและกฎระเบียบที่จำเป็น ข้อจำกัดด้านขีดความสามารถในการบังคับใช้กฎหมาย และความขัดแย้งระหว่างหน่วยงานกำกับดูแล



ต่างๆ นอกจากนี้ ความเหลื่อมล้ำทางดิจิทัลที่สูงในอินเดียก็เป็นอุปสรรคต่อการพัฒนานโยบายที่มีประสิทธิภาพ แม้จะมีความท้าทาย แต่ประสบการณ์ของอินเดียในการพัฒนารอบการกำกับดูแลอำนาจอิทธิพลทางดิจิทัลมีความสำคัญอย่างยิ่งสำหรับประเทศกำลังพัฒนาอื่นๆ โดยเฉพาะในประเด็นการสร้างสมดุลระหว่างการพัฒนาเศรษฐกิจดิจิทัลกับการรักษาอำนาจอธิปไตยและความมั่นคงของประเทศ

4) การเปรียบเทียบกรณีศึกษา

ผู้วิจัย เปรียบเทียบลักษณะสำคัญของทั้ง 3 กรณีศึกษาจำแนกตามมิติการวิเคราะห์ โดยรายละเอียดดังแสดงในตารางที่ 1

ตารางที่ 1 การเปรียบเทียบกรณีศึกษา

มิติการวิเคราะห์	สหภาพยุโรป (Ex-ante Focus)	จีน (Hybrid Approach)	อินเดีย (Ex-post to Hybrid)
กฎหมายและ กรอบการกำกับ ดูแลหลัก	GDPR (2018), Digital Markets Act, Digital Services Act	Cybersecurity Law (2017), Data Security Law (2021), Personal Information Protection Law (2021)	Draft Personal Data Protection Bill, Information Technology Act, Aadhaar Act
แนวทางการ กำกับดูแล	เน้นการวางกฎเกณฑ์ ล่วงหน้า มาตรฐาน ชัดเจน บทลงโทษ เข้มงวด	ผสมผสานระหว่าง กฎเกณฑ์ล่วงหน้าและ การตอบสนองภายหลัง ยืดหยุ่นในการบังคับใช้	เริ่มจากการตอบสนอง เฉพาะกรณี กำลังพัฒนา ไปสู่การมีกรอบที่ ครอบคลุม
โครงสร้างองค์กร กำกับดูแล	หน่วยงานกำกับดูแล ระดับชาติ European Data Protection Board มาตรฐานกลาง ชัดเจน	CAC, MIIT และ หน่วยงานระดับท้องถิ่น กระจายอำนาจ มีความ ซ้ำซ้อน	หลายหน่วยงานกำกับ ดูแล อยู่ระหว่างการ พัฒนาโครงสร้าง ขาด การประสานงานที่มี ประสิทธิภาพ
การบังคับใช้และ การลงโทษ	เข้มงวด บทลงโทษสูง (4% ของรายได้ทั่วโลก) มีแนวปฏิบัติชัดเจน	เลือกบังคับใช้ตามความ เหมาะสม คำนึงถึง ผลกระทบทางเศรษฐกิจ ยืดหยุ่น	ไม่สม่ำเสมอ ขีด ความสามารถจำกัด ขาด ประสิทธิภาพในการ บังคับใช้
จุดเน้นของ นโยบาย	สิทธิพื้นฐาน การ คุ้มครองผู้บริโภค การ แข่งขันที่เป็นธรรม การ คุ้มครองข้อมูล	ความมั่นคงของรัฐ การ ควบคุมเนื้อหา การ พัฒนาอุตสาหกรรม ภายในประเทศ	การพัฒนาเศรษฐกิจ ดิจิทัล การรักษาความ มั่นคง การพัฒนา โครงสร้างพื้นฐาน
ความท้าทายหลัก	ต้นทุนในการปฏิบัติตาม สูง ความแตกต่างในการ	ความไม่ชัดเจนในการ ตีความ การทับซ้อนของ	ขีดความสามารถจำกัด ความล่าช้าในการออก



มิติการวิเคราะห์	สหภาพยุโรป (Ex-ante Focus)	จีน (Hybrid Approach)	อินเดีย (Ex-post to Hybrid)
	บังคับใช้ระหว่างประเทศ สมาชิก	อำนาจ ผลกระทบต่อ นวัตกรรม	กฎหมาย ความเหลื่อมล้ำ ทางดิจิทัล
ผลกระทบต่อ นวัตกรรม	อาจชะลอนวัตกรรม เนื่องจากกฎระเบียบ เข้มงวด ต้นทุนการ ปฏิบัติตามสูง	สนับสนุนนวัตกรรม ภายในประเทศ จำกัด การแข่งขันจากต่างชาติ	พยายามสร้างสมดุล ระหว่างนวัตกรรมและ การกำกับดูแล ขาดระบบ นิเวศที่เอื้อต่อนวัตกรรม
การคุ้มครอง ข้อมูลส่วนบุคคล	ครอบคลุมและเข้มงวด เน้นสิทธิของเจ้าของ ข้อมูล หลักความยินยอม	เน้นความมั่นคงควบคู่กับ การคุ้มครอง รัฐมีอำนาจ เข้าถึงข้อมูล	อยู่ระหว่างพัฒนา กฎหมาย ได้รับอิทธิพล จาก GDPR แต่ให้อำนาจ รัฐมากกว่า

5) ข้อจำกัดในการใช้แพลตฟอร์มทางดิจิทัล

ขีดจำกัดในการใช้แพลตฟอร์มทางดิจิทัลในสหภาพยุโรป จีน และอินเดียสะท้อนให้เห็นถึงความแตกต่างของแนวทางการกำกับดูแลและลำดับความสำคัญของแต่ละภูมิภาค โดยแต่ละประเทศมีวิธีการและเกณฑ์ที่แตกต่างกันในการจำกัดการดำเนินงานของแพลตฟอร์มดิจิทัล

สหภาพยุโรปใช้แนวทางการกำหนดขีดจำกัดผ่านกรอบกฎหมายที่ครอบคลุม โดยเฉพาะผ่าน Digital Markets Act (DMA) และ Digital Services Act (DSA) ที่กำหนดภาระหน้าที่พิเศษสำหรับแพลตฟอร์มขนาดใหญ่หรือ “Gatekeepers” Hoeffler and Mérand (2024) วิเคราะห์ว่าข้อกำหนดสำคัญ ได้แก่ การห้ามให้ความได้เปรียบกับบริการของตนเองในแพลตฟอร์ม การอนุญาตให้ผู้ใช้ออนการติดตั้งแอปพลิเคชันที่ติดตั้งมาล่วงหน้า การเปิดให้มีการติดตั้งแอปจากแหล่งอื่น (sideloading) และการเปิดเผยข้อมูลกับคู่แข่งในบางกรณี ส่งผลให้แพลตฟอร์มยักษ์ใหญ่อย่าง Apple Google Meta และ Amazon ต้องปรับเปลี่ยนโมเดลธุรกิจในตลาดยุโรปอย่างมีนัยสำคัญ เช่น Apple ต้องเปิดให้ติดตั้งแอปนอก App Store และ Google ต้องให้ผู้เลือกใช้เครื่องมือค้นหาเริ่มต้น นอกจากนี้ DSA ยังกำหนดให้แพลตฟอร์มมีความรับผิดชอบในการกำกับดูแลเนื้อหา ต้องทำการประเมินความเสี่ยงเชิงระบบและโปร่งใสในการใช้อัลกอริทึม Broeders et al. (2023) ชี้ให้เห็นว่าแม้ข้อกำหนดเหล่านี้สร้างความชัดเจน แต่ก็สร้างภาระต้นทุนสูงโดยเฉพาะสำหรับธุรกิจขนาดเล็กและขนาดกลาง และอาจส่งผลให้บริษัทเทคโนโลยีบางแห่งลดการลงทุนหรือชะลอการเปิดตัวบริการใหม่ในตลาดยุโรป

จีนมีแนวทางที่แตกต่างอย่างชัดเจน โดยเน้นการควบคุมเนื้อหาและความมั่นคงของรัฐเป็นหลัก Khasanova and Tai (2024) อธิบายว่าจีนใช้ระบบ “Great Firewall” ปิดกั้นแพลตฟอร์มต่างชาติหลักเกือบทั้งหมด เช่น Facebook Google Twitter YouTube และ Instagram ทำให้ประชาชนต้องพึ่งพาแพลตฟอร์มในประเทศ เช่น WeChat Weibo Baidu และ Douyin ซึ่งต้องปฏิบัติตามข้อกำหนดการควบคุมเนื้อหาที่เข้มงวด มีระบบตรวจสอบและลบเนื้อหาที่ละเมิดกฎหมายหรือคุกคามความมั่นคง Fratini et al. (2024) ชี้ให้เห็นว่าแพลตฟอร์มที่มีผู้ใช้จำนวนมากต้องจัดเก็บข้อมูลในประเทศและให้ความร่วมมือกับหน่วยงานรัฐในการเข้าถึงข้อมูล ตั้งแต่ปี 2021 จีนเริ่มกำกับดูแลบริษัทเทคโนโลยีในประเทศอย่างเข้มงวดมากขึ้น โดยเฉพาะด้านการผูกขาดและการคุ้มครองข้อมูล ส่งผลให้บริษัทยักษ์ใหญ่อย่าง Alibaba และ Tencent ต้องปรับเปลี่ยนการดำเนินงาน นอกจากนี้ยังมีการห้ามบริษัทที่มีข้อมูล



ส่วนบุคคลจำนวนมากเข้าจดทะเบียนในตลาดหุ้นต่างประเทศโดยไม่ได้รับอนุญาต เช่น กรณีของ Didi Chuxing ทั้งนี้ Donnelly et al. (2024) สังเกตว่าแม้จะมีกฎระเบียบเข้มงวด แต่การบังคับใช้มีความยืดหยุ่นและเลือกใช้ตามความเหมาะสม คำนึงถึงผลกระทบทางเศรษฐกิจ แต่ก็สร้างความไม่แน่นอนให้กับทั้งบริษัทในประเทศและต่างชาติ

อินเดียมีแนวทางที่สะท้อนการพัฒนากรอบการกำกับดูแลที่กำลังเปลี่ยนผ่าน Prasad (2022) วิเคราะห์ว่า อินเดียค่อนข้างเปิดกว้างต่อแพลตฟอร์มต่างชาติ แต่เริ่มกำหนดข้อจำกัดมากขึ้น กฎ IT Rules 2021 กำหนดให้แพลตฟอร์มโซเชียลมีเดียและบริการ OTT ต้องแต่งตั้งเจ้าหน้าที่ปฏิบัติตามกฎหมายที่อยู่ในอินเดีย มีกลไกรับเรื่องร้องเรียน และลบเนื้อหาผิดกฎหมายภายในกรอบเวลาที่กำหนด เหตุการณ์สำคัญคือการห้ามแอปพลิเคชันจากจีนกว่า 200 แอป รวมถึง TikTok, WeChat และ PUBG Mobile ในปี 2020 ภายใต้เหตุผลความมั่นคงแห่งชาติ Monsees and Lambach (2022) ระบุว่ามาตรการนี้แสดงให้เห็นความพร้อมใช้มาตรการเด็ดขาดเพื่อปกป้องผลประโยชน์ด้านความมั่นคง และเปิดโอกาสให้แพลตฟอร์มอินเดียอย่าง ShareChat และ Chingari เติบโต Vila Seoane (2021) ชี้ให้เห็นว่าอินเดียมีข้อกำหนด Data Localization ให้บริษัทบางประเภท โดยเฉพาะสถาบันการเงินและอีคอมเมิร์ซ ต้องจัดเก็บข้อมูลผู้ใช้ในประเทศ แต่การบังคับใช้ยังไม่สม่ำเสมอและมีข้อยกเว้นหลายกรณี อย่างไรก็ตาม อินเดียยังเผชิญความท้าทาย เช่น ความล่าช้าในการออกกฎหมาย ข้อจำกัดด้านขีดความสามารถในการบังคับใช้ ความขัดแย้งระหว่างหน่วยงาน และความเหลื่อมล้ำทางดิจิทัลที่สูง ซึ่ง Gupta and Sony (2021) ระบุว่า เป็นอุปสรรคต่อการพัฒนานโยบายที่มีประสิทธิภาพ

อภิปรายผลการวิจัย

การอภิปรายผลการวิจัยนี้จะนำเสนอตามวัตถุประสงค์การวิจัยที่กำหนดไว้ ดังนี้

1) การเปรียบเทียบแนวทางการกำกับดูแลเชิงป้องกันและการกำกับดูแลภายหลัง ผลการศึกษาแสดงให้เห็นความแตกต่างที่ชัดเจนระหว่างการกำกับดูแลเชิงป้องกันและการกำกับดูแลภายหลังในสามกรณีศึกษา สหภาพยุโรปเป็นตัวอย่างที่โดดเด่นของการใช้แนวทางเชิงป้องกันผ่าน GDPR และ DMA ซึ่งวางกฎเกณฑ์ล่วงหน้าอย่างครอบคลุม Monsees and Lambach (2022) ชี้ให้เห็นว่าแนวทางนี้สร้างความชัดเจนและความแน่นอนให้กับผู้ประกอบการ แต่ก็มีต้นทุนในการปฏิบัติตามที่สูง โดยเฉพาะสำหรับธุรกิจขนาดเล็กและขนาดกลาง ข้อดีของแนวทางนี้คือสามารถป้องกันปัญหาก่อนเกิดและสร้างมาตรฐานที่เป็นสากล อย่างไรก็ตาม ข้อจำกัดที่สำคัญ คือ ความยืดหยุ่นที่จำกัดและอาจส่งผลกระทบต่อนวัตกรรม ดังที่ Broeders et al. (2023) วิเคราะห์ว่าบริษัทเทคโนโลยีบางแห่งชะลอการเปิดตัวบริการใหม่ในตลาดยุโรปเนื่องจากความซับซ้อนของข้อกำหนด

ในทางตรงกันข้าม การกำกับดูแลภายหลังที่เคยใช้ในอินเดียมีความยืดหยุ่นมากกว่า แต่ก็เผชิญกับปัญหาการตอบสนองที่ล่าช้าและไม่มีประสิทธิภาพ Vila Seoane (2021) ชี้ให้เห็นว่าการรอให้ปัญหาเกิดขึ้นก่อนแล้วจึงดำเนินการแก้ไขทำให้เกิดความเสียหายที่ยากต่อการฟื้นฟู โดยเฉพาะในกรณีการรั่วไหลของข้อมูลส่วนบุคคลหรือการละเมิดสิทธิของผู้บริโภค ข้อค้นพบนี้สอดคล้องกับ Khasanova and Tai (2024) ที่อธิบายว่าการกำกับดูแลภายหลังเหมาะสมในบริบทที่เทคโนโลยีเปลี่ยนแปลงรวดเร็วและยากต่อการคาดการณ์ แต่จำเป็นต้องมีขีดความสามารถสถาบันที่เข้มแข็งในการบังคับใช้อย่างมีประสิทธิภาพ

จึงนำเสนอแนวทางผสมผสานที่มีลักษณะเฉพาะตัวที่น่าสนใจ โดยมีกฎระเบียบเชิงป้องกันที่เข้มงวด แต่การบังคับใช้มีความยืดหยุ่นตามบริบท Donnelly et al. (2024) วิเคราะห์ว่าแนวทางนี้ช่วยให้จีนสามารถสร้างสมดุลระหว่างการควบคุมที่เข้มงวดกับการส่งเสริมนวัตกรรมภายในประเทศ อย่างไรก็ตาม



ความไม่แน่นอนในการบังคับใช้สร้างความท้าทายให้กับบริษัท โดยเฉพาะบริษัทต่างชาติที่ต้องเผชิญกับความเสี่ยงที่ไม่สามารถคาดการณ์ได้ ผลการศึกษายังพบว่ามีแนวโน้มการหลอมรวมระหว่างสองแนวทางโดยสหภาพยุโรปเริ่มมีความยืดหยุ่นมากขึ้นในบางประเด็น และอินเดียกำลังพัฒนาไปสู่การมีกรอบเชิงป้องกันที่ชัดเจนมากขึ้น

2) กรอบการกำกับดูแล กลไกการบังคับใช้ และโครงสร้างสถาบัน

การวิเคราะห์กรอบการกำกับดูแลของสามกรณีศึกษาแสดงให้เห็นความแตกต่างที่สำคัญในการออกแบบและการดำเนินงาน กรอบการกำกับดูแลของสหภาพยุโรปมีลักษณะครอบคลุมและเป็นระบบ โดย GDPR กำหนดหลักการพื้นฐานที่ชัดเจน เช่น หลักความยินยอม การจำกัดวัตถุประสงค์ และสิทธิของเจ้าของข้อมูล ในขณะที่ DMA และ DSA กำหนดภาระหน้าที่เฉพาะสำหรับแพลตฟอร์มขนาดใหญ่ Hoeffler and Mérand (2024) ชี้ให้เห็นว่าการมี European Data Protection Board เป็นกลไกประสานงานช่วยสร้างมาตรฐานกลางและลดความแตกต่างระหว่างประเทศสมาชิก แม้จะยังคงมีความท้าทายในการตีความและการบังคับใช้ที่สอดคล้องกัน

กรอบการกำกับดูแลของจีนมีความซับซ้อนมากกว่า โดยมีกฎหมายหลายฉบับที่ครอบคลุมด้านต่างๆ ได้แก่ Cybersecurity Law, Data Security Law และ Personal Information Protection Law Fratini et al. (2024) วิเคราะห์ว่าการมีหลายหน่วยงานกำกับดูแล เช่น CAC และ MIIT สร้างความท้าทายในการประสานงาน แต่ก็ช่วยให้สามารถตอบสนองต่อบริบทที่แตกต่างกันได้ดีขึ้น ความเข้มงวดในการบังคับใช้มักขึ้นอยู่กับความสำคัญเชิงยุทธศาสตร์และผลกระทบต่อความมั่นคงของรัฐ ซึ่งแตกต่างจากสหภาพยุโรปที่เน้นการบังคับใช้อย่างสม่ำเสมอ

อินเดียอยู่ในระหว่างการพัฒนากรอบการกำกับดูแลที่ครอบคลุม โดยมี IT Rules 2021 และร่าง Personal Data Protection Bill เป็นรากฐานสำคัญ Prasad (2022) ชี้ให้เห็นว่าความล่าช้าในการออกกฎหมายและข้อจำกัดด้านขีดความสามารถสถาบันเป็นอุปสรรคสำคัญ โครงสร้างสถาบันยังขาดการประสานงานที่มีประสิทธิภาพระหว่างหน่วยงานต่างๆ ส่งผลให้การบังคับใช้ไม่สม่ำเสมอ อย่างไรก็ตาม การห้ามแอปพลิเคชันจากจีนแสดงให้เห็นว่าอินเดียสามารถใช้มาตรการเด็ดขาดเมื่อเกี่ยวข้องกับความมั่นคงแห่งชาติ

กลไกการบังคับใช้ของสหภาพยุโรปมีความเข้มงวดและมีบทลงโทษที่รุนแรง โดยกำหนดค่าปรับสูงสุดถึง 4% ของรายได้ทั่วโลกสำหรับการละเมิด GDPR Broeders et al. (2023) อธิบายว่าบทลงโทษที่สูงนี้สร้างแรงจูงใจให้บริษัทปฏิบัติตามอย่างจริงจัง ในขณะที่จีนใช้แนวทางเลือกสรรในการบังคับใช้ โดยคำนึงถึงผลกระทบทางเศรษฐกิจและความจำเป็นในการพัฒนาอุตสาหกรรม อินเดียมีข้อจำกัดด้านขีดความสามารถในการบังคับใช้ ทำให้การลงโทษมักไม่มีประสิทธิภาพเท่าที่ควร Gupta and Sony (2021) เสนอว่าการเสริมสร้างขีดความสามารถสถาบันเป็นสิ่งจำเป็นสำหรับอินเดียในการพัฒนาการกำกับดูแลที่มีประสิทธิภาพ

3) ประสิทธิภาพและความท้าทายของแต่ละแนวทางในบริบทที่แตกต่าง

การประเมินประสิทธิภาพของแต่ละแนวทางต้องพิจารณาในบริบททางการเมือง เศรษฐกิจ และสังคมที่ต่างกัน แนวทางของสหภาพยุโรปมีประสิทธิภาพในการสร้างมาตรฐานที่สูงและปกป้องสิทธิของพลเมือง Lehouedé (2024) วิเคราะห์ว่า “Brussels Effect” แสดงให้เห็นถึงอิทธิพลของมาตรฐานยุโรปที่ส่งผลให้หลายประเทศพัฒนากฎหมายที่คล้ายคลึงกัน อย่างไรก็ตาม ความท้าทายสำคัญคือการสร้างสมดุลระหว่างการคุ้มครองกับการส่งเสริมนวัตกรรม โดยเฉพาะในบริบทที่เทคโนโลยี



เปลี่ยนแปลงอย่างรวดเร็ว ต้นทุนการปฏิบัติตามที่สูงอาจส่งผลให้สตาร์ทอัพและ SMEs ในยุโรปเสียเปรียบในการแข่งขันกับบริษัทขนาดใหญ่ที่มีทรัพยากรมากกว่า

แนวทางของจีนมีประสิทธิภาพในการรักษาความมั่นคงและส่งเสริมอุตสาหกรรมภายในประเทศ Khasanova and Tai (2024) ชี้ให้เห็นว่าการควบคุมที่เข้มงวดช่วยให้รัฐสามารถจัดการกับเนื้อหาและข้อมูลได้อย่างมีประสิทธิภาพ ในขณะที่ความยืดหยุ่นในการบังคับใช้ช่วยส่งเสริมการเติบโตของบริษัทเทคโนโลยีจีน อย่างไรก็ตาม Belli (2024) วิพากษ์ว่าแนวทางนี้อาจส่งผลกระทบต่อสิทธิเสรีภาพของประชาชนและสร้างอุปสรรคต่อบริษัทต่างชาติ ความไม่แน่นอนในการบังคับใช้เป็นความท้าทายสำคัญที่ส่งผลกระทบต่อความเชื่อมั่นของนักลงทุนต่างชาติ

อินเดียเผชิญกับความท้าทายที่ซับซ้อนในการสร้างสมดุลระหว่างการพัฒนาเศรษฐกิจดิจิทัลกับการรักษาอำนาจอธิปไตย Prasad (2022) วิเคราะห์ว่าความเหลื่อมล้ำทางดิจิทัลที่สูงทำให้การพัฒนา นโยบายที่เหมาะสมกับทุกกลุ่มเป็นเรื่องท้าทาย นโยบาย Digital India แสดงให้เห็นความพยายามในการใช้เทคโนโลยีเพื่อพัฒนาประเทศ แต่การขาดกรอบการกำกับดูแลที่ชัดเจนสร้างความไม่แน่นอนให้กับภาคธุรกิจ ความล่าช้าในการออกกฎหมายคุ้มครองข้อมูลส่วนบุคคลส่งผลให้อินเดียตกอยู่ในสภาพเปราะบางต่อการละเมิดข้อมูล

ปัจจัยสำคัญที่ส่งผลกระทบต่อประสิทธิภาพของแต่ละแนวทาง ได้แก่ ชีตความสามารถของสถาบัน แรงจูงใจทางเศรษฐกิจ และบริบททางการเมือง Leese (2024) พบว่าสหภาพยุโรปมีสถาบันที่เข้มแข็งและประสบการณ์ยาวนานในการกำกับดูแล ในขณะที่จีนมีความสามารถในการระดมทรัพยากรและประสานงานระหว่างหน่วยงานได้ดี อินเดียยังต้องพัฒนาขีดความสามารถสถาบันและแก้ไขปัญห การขาดการประสานงานระหว่างหน่วยงาน แรงจูงใจทางเศรษฐกิจก็มีบทบาทสำคัญ โดยจีนและอินเดียต้องพิจารณาผลกระทบต่อการเติบโตทางเศรษฐกิจมากกว่าสหภาพยุโรปที่เน้นการคุ้มครองสิทธิเป็นหลัก

ข้อเสนอแนะ

จากผลการศึกษาและการอภิปรายข้างต้น มีข้อเสนอแนะเชิงนโยบายสำหรับประเทศต่างๆ ดังนี้ ประการแรก การพัฒนากฎการกำกับดูแลควรคำนึงถึงบริบทเฉพาะของแต่ละประเทศ Monsees and Lambach (2022) เสนอว่าไม่มีรูปแบบใดที่เหมาะสมกับทุกบริบท ประเทศควรเลือกใช้แนวทางที่สอดคล้องกับระดับการพัฒนา ชีตความสามารถสถาบัน และเป้าหมายทางเศรษฐกิจและสังคม ประเทศกำลังพัฒนาอาจเริ่มต้นด้วยแนวทางผสมผสานที่มีความยืดหยุ่น แล้วค่อยพัฒนาไปสู่กรอบที่ครอบคลุมมากขึ้นเมื่อมีขีดความสามารถเพียงพอ

ประการที่สอง การเสริมสร้างขีดความสามารถสถาบันเป็นสิ่งจำเป็น Vila Seoane (2021) แนะนำให้เพิ่มการลงทุนในการพัฒนาบุคลากร เทคโนโลยี และโครงสร้างพื้นฐานที่จำเป็นสำหรับการกำกับดูแลที่มีประสิทธิภาพ การสร้างหน่วยงานกลางที่มีอำนาจและทรัพยากรเพียงพอจะช่วยเพิ่มประสิทธิภาพในการบังคับใช้และลดความซ้ำซ้อน

ประการที่สาม การส่งเสริมความร่วมมือระหว่างผู้มีส่วนได้ส่วนเสียเป็นกุญแจสู่ความสำเร็จ Hoeffler and Mérand (2024) เน้นความสำคัญของการสร้างความร่วมมือระหว่างภาครัฐ เอกชน และประชาสังคมในการพัฒนาและบังคับใช้นโยบาย การมีส่วนร่วมของภาคเอกชนในการออกแบบกฎระเบียบจะช่วยให้นโยบายมีความเป็นไปได้ในทางปฏิบัติและลดภาระที่ไม่จำเป็น

ประการสุดท้าย การเพิ่มความร่วมมือระหว่างประเทศเป็นสิ่งจำเป็นในการจัดการกับความท้าทายข้ามพรมแดน Belli (2024) เสนอให้พัฒนามาตรฐานและแนวปฏิบัติร่วมกันในระดับภูมิภาคและระดับโลก

โดยเฉพาะในประเด็นการไหลเวียนของข้อมูลข้ามพรมแดนและการจัดการกับบริษัทเทคโนโลยีข้ามชาติ การแลกเปลี่ยนประสบการณ์และบทเรียนระหว่างประเทศจะช่วยให้เกิดการเรียนรู้และพัฒนากรอบนโยบายที่ดีขึ้น

องค์ความรู้ที่ได้

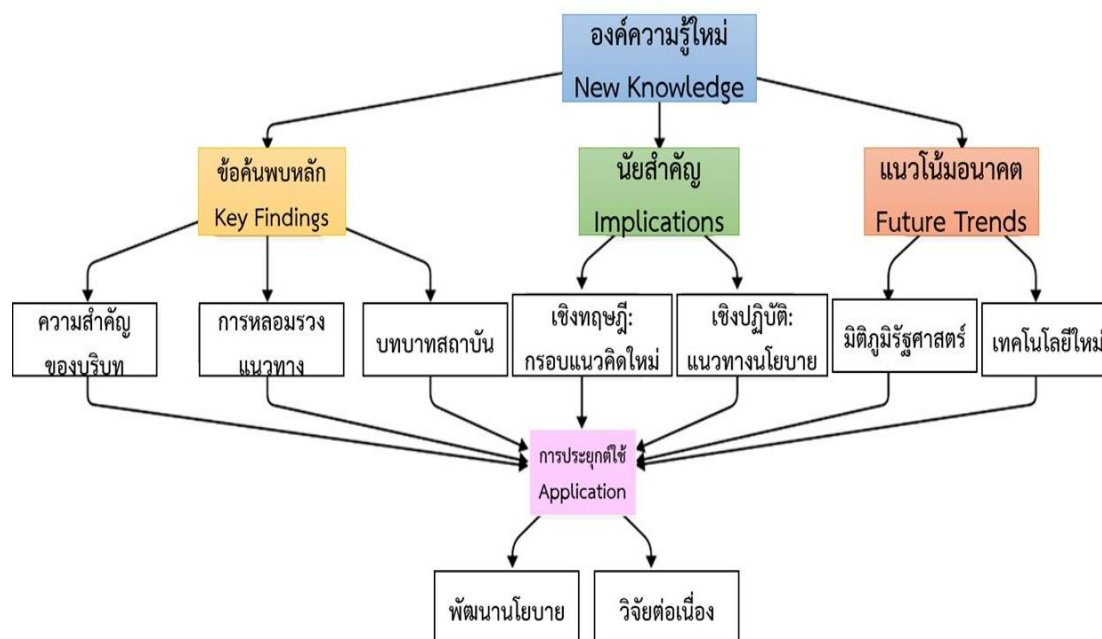
การศึกษานี้สร้างองค์ความรู้ใหม่ที่สำคัญในการทำความเข้าใจการกำกับดูแลอำนาจดิจิทัลทางดิจิทัลในบริบทที่แตกต่างกัน ข้อค้นพบหลักสามประการที่โดดเด่นจากการวิเคราะห์เปรียบเทียบสามกรณีศึกษา ประการแรก Lehoucq (2024) สรุปว่าประสิทธิภาพของการกำกับดูแลขึ้นอยู่กับบริบททางการเมือง เศรษฐกิจ และสังคมของแต่ละประเทศอย่างมีนัยสำคัญ การเลือกใช้แนวทางการกำกับดูแลจึงต้องคำนึงถึงปัจจัยเหล่านี้ โดยไม่สามารถนำรูปแบบจากประเทศหนึ่งไปใช้กับอีกประเทศหนึ่งได้โดยตรง ประการที่สอง Monsees and Lambach (2022) พบว่าแนวโน้มในการผสมผสานระหว่าง ex-ante และ ex-post regulation กำลังเพิ่มขึ้น เพื่อสร้างสมดุลระหว่างความชัดเจนและความยืดหยุ่น ซึ่งสะท้อนให้เห็นว่าทั้งสหภาพยุโรปและอินเดียกำลังปรับแนวทางให้มีความยืดหยุ่นมากขึ้น ในขณะที่จีนพยายามสร้างความชัดเจนในกฎระเบียบมากขึ้น ประการที่สาม Hoeffler and Mérand (2024) ชี้ให้เห็นว่าความเข้มแข็งของสถาบันกำกับดูแลและการประสานงานระหว่างหน่วยงานมีความสำคัญต่อประสิทธิภาพของการกำกับดูแลมากกว่ารูปแบบการกำกับดูแลที่เลือกใช้ โดยประเทศที่มีสถาบันเข้มแข็งสามารถใช้ทั้งแนวทาง ex-ante และ ex-post ได้อย่างมีประสิทธิภาพ

การศึกษานี้มีนัยสำคัญทั้งในเชิงทฤษฎีและการปฏิบัติ Gupta and Sony (2021) เสนอว่าในเชิงทฤษฎีช่วยขยายความเข้าใจเกี่ยวกับความสัมพันธ์ระหว่างรูปแบบการกำกับดูแลกับประสิทธิภาพและผลกระทบในบริบทที่แตกต่างกัน โดยเฉพาะการค้นพบว่าการกำกับดูแลเชิงป้องกันไม่จำเป็นต้องเหนือกว่าการกำกับดูแลภายหลังในทุกบริบท แต่ประสิทธิภาพขึ้นอยู่กับปัจจัยอื่นๆ ที่สำคัญไม่แพ้กัน โดยเฉพาะขีดความสามารถสถาบัน แรงจูงใจทางเศรษฐกิจ และบริบททางการเมือง และยังชี้ให้เห็นว่ามีแนวโน้มการหลอมรวมระหว่างสองแนวทาง (convergence) ซึ่งเป็นข้อค้นพบใหม่ที่สำคัญต่อการพัฒนาทฤษฎีการกำกับดูแลดิจิทัล นอกจากนี้ Sheikh (2022) ชี้ให้เห็นว่าการศึกษานี้เสนอกรอบแนวคิดใหม่ในการวิเคราะห์อำนาจดิจิทัลทางดิจิทัลที่เชื่อมโยงระหว่างรูปแบบการกำกับดูแล องค์ประกอบสำคัญ (การควบคุมข้อมูล โครงสร้างพื้นฐาน การกำกับแพลตฟอร์ม) และปัจจัยที่มีอิทธิพล ซึ่งสามารถนำไปใช้วิเคราะห์กรณีศึกษาอื่นๆ ได้ในเชิงปฏิบัติ Belli (2024) ชี้ให้เห็นว่าข้อค้นพบจากการศึกษาสามารถนำไปใช้ในการพัฒนานโยบายและกรอบการกำกับดูแลที่เหมาะสมสำหรับแต่ละประเทศ โดยเฉพาะในประเด็นการสร้างสมดุลระหว่างการควบคุมกับการส่งเสริมนวัตกรรม สำหรับประเทศกำลังพัฒนาที่กำลังออกแบบกรอบการกำกับดูแล การศึกษานี้แสดงให้เห็นว่าควรเริ่มต้นด้วยการเสริมสร้างขีดความสามารถสถาบันก่อน แล้วจึงค่อยพัฒนากรอบกฎหมายที่ครอบคลุม มากกว่าการพยายามลอกเลียนแบบ GDPR โดยตรง Frattini et al. (2024) เสริมว่าการศึกษานี้ยังให้ข้อมูลสำคัญเกี่ยวกับขีดจำกัดในการใช้แพลตฟอร์มดิจิทัล ซึ่งช่วยให้ผู้กำหนดนโยบายเข้าใจผลกระทบที่เป็นรูปธรรมของการกำกับดูแลต่อภาคธุรกิจและผู้บริโภค ความร่วมมือระหว่างประเทศก็เป็นอีกประเด็นสำคัญที่การศึกษานี้ชี้ให้เห็นความจำเป็น โดยเฉพาะในการพัฒนามาตรฐานร่วมและการแลกเปลี่ยนประสบการณ์ที่จะช่วยให้ประเทศต่างๆ เรียนรู้จากความสำเร็จและความผิดพลาดของกันและกัน

นอกจากนี้ ยังเผยให้เห็นแนวโน้มสำคัญในอนาคต Vila Seoane (2021) และ Khasanova and Tai (2024) ชี้ให้เห็นว่าการกำกับดูแลอำนาจดิจิทัลทางดิจิทัลกำลังเป็นเครื่องมือทางภูมิรัฐศาสตร์มากขึ้น โดยประเทศต่างๆ ใช้การกำกับดูแลเป็นวิธีในการแข่งขันเชิงยุทธศาสตร์กับมหาอำนาจอื่นๆ ความ



ตั้งเครือข่ายระหว่างทางเปิดกว้างทางเศรษฐกิจกับการปกป้องความมั่นคงจะเพิ่มมากขึ้น ส่งผลให้ประเทศต่างๆ ต้องหาจุดสมดุลใหม่ระหว่างการส่งเสริมนวัตกรรมกับการรักษาอำนาจอธิปไตย ความท้าทายจากเทคโนโลยีใหม่ เช่น ปัญญาประดิษฐ์ Web3 และ quantum computing จะต้องการกรอบการกำกับดูแลที่ยืดหยุ่นและสามารถปรับตัวได้อย่างรวดเร็ว องค์ความรู้จากการศึกษานี้จึงเป็นรากฐานสำคัญในการพัฒนานโยบายที่จะรับมือกับความท้าทายเหล่านี้ในอนาคต รายละเอียดตามที่แสดงไว้ในภาพที่ 2



ภาพที่ 2 องค์ความรู้ใหม่ที่ได้จากการวิจัย

บทสรุป

การศึกษาเปรียบเทียบการกำกับดูแลอำนาจอธิปไตยทางดิจิทัลระหว่างสหภาพยุโรป จีน และอินเดียเป็นการวิเคราะห์เปรียบเทียบกรอบการกำกับดูแลเชิงป้องกันและกรอบการกำกับดูแลภายหลัง แสดงให้เห็นลักษณะเฉพาะที่แตกต่างกัน กรอบการกำกับดูแลเชิงป้องกันของสหภาพยุโรปผ่าน GDPR และ DMA สร้างความชัดเจนและมาตรฐานที่แข็งแกร่ง การศึกษากรอบการกำกับดูแลและโครงสร้างสถาบันเผยให้เห็นความแตกต่างที่สำคัญ ดังนี้ สหภาพยุโรปมีโครงสร้างที่เป็นระบบผ่าน European Data Protection Board จีนมีหลายหน่วยงานกระจายอำนาจซึ่งสร้างความยืดหยุ่นแต่ท้าทายในการประสานงาน อินเดียยังพัฒนาขีดความสามารถสถาบันและเผชิญปัญหาความล่าช้าในการออกกฎหมาย การประเมินประสิทธิภาพแสดงให้เห็นว่าบริบทมีบทบาทสำคัญ สหภาพยุโรปประสบความสำเร็จในการสร้างมาตรฐานสูงแต่ต้องสร้างสมดุลกับนวัตกรรม จีนมีประสิทธิภาพในการรักษาความมั่นคงและส่งเสริมอุตสาหกรรมภายในประเทศ แต่มีความไม่แน่นอนในการบังคับใช้ อินเดียกำลังพัฒนากรอบที่สมดุลแต่ยังต้องเสริมสร้างขีดความสามารถสถาบัน โดยมีข้อเสนอแนะสำหรับการวิจัยในอนาคตควรมุ่งเน้น (1) การศึกษาผลกระทบระยะยาวของกรอบการกำกับดูแลที่แตกต่างกัน (2) การวิเคราะห์ความสัมพันธ์ระหว่างการกำกับดูแลกับการพัฒนานวัตกรรม (3) การศึกษาบทบาทของความร่วมมือระหว่างประเทศ (4) การพัฒนาตัวชี้วัดประสิทธิภาพที่วัดได้อย่างเป็นรูปธรรม และ (5) การขยายขอบเขตไปยังกรณีศึกษาอื่นๆ ในภูมิภาคต่างๆ



เอกสารอ้างอิง

- Autolitano, S., & Pawlowska, A. (2021). *Europe's quest for digital sovereignty: GAIA-X as a case study*. Istituto Affari Internazionali (IAI). <https://www.jstor.org/stable/resrep30940>
- Belli, L. (2024). *Building good digital sovereignty through digital public infrastructures and digital commons in India and Brazil*. Cyber BRICS. <https://doi.org/10.2139/ssrn.4966348>
- Braun, M., & Hummel, P. (2024). Is digital sovereignty normatively desirable? *Information, Communication & Society*, 1–14. <https://doi.org/10.1080/1369118X.2024.2332624>
- Broeders, D., Cristiano, F., & Kaminska, M. (2023). In search of digital sovereignty and strategic autonomy: Normative power Europe to the test of its geopolitical ambitions. *Journal of Common Market Studies*, 61(5), 1261–1280. <https://doi.org/10.1111/jcms.13462>
- Christakis, T. (2020). *European digital sovereignty: Successfully navigating between the Brussels effect and Europe's quest for strategic autonomy*. Multidisciplinary Institute on Artificial Intelligence/Grenoble Alpes Data Institute. <https://doi.org/10.2139/ssrn.3748098>
- Donnelly, S., Ríos Camacho, E., & Heidebrecht, S. (2023). Digital sovereignty as control: the regulation of digital finance in the European union. *Journal of European Public Policy*, 31(8), 2226–2249. <https://doi.org/10.1080/13501763.2023.2295520>
- Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Contemporary Social Science*, 15(3), 330–345. <https://doi.org/10.1007/s13347-020-00423-6>
- Fratini, S., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2024). Digital sovereignty: A descriptive analysis and a critical evaluation of existing models. *Digital Society*, 59. <https://doi.org/10.1007/s44206-024-00146-7>
- Gupta, S., & Sony, R.A.L. (2021). Quest of data colonialism and cyber sovereignty: India's strategic position in cyberspace. *Legal Issues in the Digital Age*, 2, 68–81. <https://doi.org/10.17323/2713-2749.2021.2.68.81>
- Heidebrecht, S. (2024). From market liberalism to public intervention: Digital sovereignty and changing European union digital single market governance. *Journal of Common Market Studies*, 62(1), 205–223. <https://doi.org/10.1111/jcms.13488>
- Hoeffler, C., & Mérand, F. (2024). Digital sovereignty, economic ideas, and the struggle over the digital markets act: A political-cultural approach. *Journal of European Public Policy*, 31(8), 2121–2146. <https://doi.org/10.1080/13501763.2023.2294144>
- Khasanova, L., & Tai, K. (2024). Shades of authoritarian digital sovereignty: Divergences in Russian and Chinese data localisation regimes. *Journal of Cyber Policy*, 9(1), 70–94. <https://doi.org/10.1080/23738871.2024.2413938>
- Leese, M. (2024). Staying in control of technology: Predictive policing, democracy, and digital sovereignty. *Democratization*, 31(5), 963–978. <https://doi.org/10.1080/13510347.2023.2197217>



- Lehuedé, S. (2024). An alternative planetary future? Digital sovereignty frameworks and the decolonial option. *Big Data & Society*, 11(1), 1-13. <https://doi.org/10.1177/20539517231221778>
- Monsees, D., & Lambach, D. (2022). Digital sovereignty, geopolitical imaginaries, and the reproduction of European identity. *European Security*, 31(3), 377-394. <https://doi.org/10.1080/09662839.2022.2101883>
- Pohle, J. & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, 9(4), 1-19. <https://doi.org/10.14763/2020.4.1532>
- Pohle, J., & Santaniello, M. (2024). From multistakeholderism to digital sovereignty: Toward a new discursive order in internet governance? *Policy & Internet*, 1-20. <https://doi.org/10.1002/poi3.426>
- Prasad, R. (2022). People as data, data as oil: The digital sovereignty of the Indian state. *Information, Communication & Society*, 25(6), 801-815. <https://doi.org/10.1080/1369118X.2022.2056498>.
- Sheikh, H. (2022). European digital sovereignty: A layered approach. *Digital Society*, 1(25). <https://doi.org/10.1007/s44206-022-00025-z>
- Vila Seoane, M. F. (2021). Data securitisation: The challenges of data sovereignty in India. *Third World Quarterly*, 42(8), 1733-1750. <https://doi.org/10.1080/01436597.2021.1915122>

