อธิปไตยทางดิจิทัล: การออกแบบการกำกับดูแลและธรรมาภิบาลในมิติที่หลากหลาย

Digital Sovereignty: The Design of Regulation and Governance in Multiple Dimensions

เกียรติอนันต์ ล้วนแก้ว[1] วรกฤษณ์ นุ้ยพิน[2] และจิรภัทร บุญอาจ[3]

Kiatanantha Lounkaew[1], Worakrit Nuypin[2] and Jirapat Boonart[3]

[1] ผู้ช่วยศาสตราจารย์ประจำคณะเศรษฐศาสตร์ มหาวิทยาลัยธรรมศาสตร์

[2,3] บริษัท ไมลส์ คอนซัลติ้ง กรุ๊ป จำกัด

[1] Assistant Professor of Faculty of Economics, Thammasat University

[2,3] Miles Consulting Group Co.,Ltd.

E-mail : klounakew@econ.tu.ac.th[1], gunnerair21@gmail.com[2], suksamran4444@gmail.com[3]

Received: Jun. 30, 2025; **Revised: Dec.** 12, 2025; **Accepted: Dec.** 15, 2025

บทคัดย่อ

บทความนี้วิเคราะห์แนวคิดอธิปไตยทางดิจิทัลและการออกแบบการกำกับดูแลในมิติต่าง ๆ ท่ามกลางการเปลี่ยนแปลงทางเทคโนโลยีและภูมิรัฐศาสตร์ที่รวดเร็ว การศึกษานี้ครอบคลุมการวิเคราะห์มิติที่สำคัญของอธิปไตยทางดิจิทัล ได้แก่ อธิปไตยของรัฐ อธิปไตยทางเศรษฐกิจ อธิปไตยของปัจเจกบุคคล อธิปไตยทางเทคโนโลยี และอธิปไตยทางข้อมูล โดยพิจารณาทั้งรูปแบบการกำกับดูแลที่แตกต่างกัน การออกแบบและการนำกฎระเบียบไปปฏิบัติ รวมถึงความท้าทายและความตึงเครียดที่เกิดขึ้น การวิเคราะห์กรณีศึกษาจากสหภาพยุโรปและประเทศต่าง ๆ แสดงให้เห็นว่าการรักษาอธิปไตยทางดิจิทัลต้องการการสร้างสมดุลระหว่างการควบคุมและการเปิดกว้าง การพัฒนาความสามารถภายในประเทศและความร่วมมือระหว่างประเทศ การวิเคราะห์เผยให้เห็นความซับซ้อนในการนำกรอบอธิปไตยทางดิจิทัลไปปฏิบัติ โดยเฉพาะในด้านการจัดเก็บข้อมูลในประเทศ การพัฒนาโครงสร้างพื้นฐาน และการแข่งขันในตลาด การวิจัยเน้นย้ำความสำคัญของการพัฒนากรอบการกำกับดูแลที่ยืดหยุ่นและปรับตัวได้ บทความมีข้อเสนอแนะสำหรับการพัฒนากรอบการกำกับดูแลที่มีประสิทธิภาพและยั่งยืน โดยเน้นความสำคัญของความยืดหยุ่น การมีส่วนร่วม และการปรับตัวต่อการเปลี่ยนแปลง

คำสำคัญ: อธิปไตยทางดิจิทัล การกำกับดูแลดิจิทัล ธรรมาภิบาลดิจิทัล ความมั่นคงทางไซเบอร์ การคุ้มครองข้อมูล นโยบายดิจิทัล การพัฒนาเทคโนโลยี

Abstract

This article analyzes digital sovereignty and regulatory design across multiple dimensions amid rapid technological and geopolitical changes. The study examines key dimensions of digital sovereignty, including state sovereignty, economic sovereignty, individual sovereignty, technological sovereignty, and data sovereignty, considering different governance models, regulatory design and implementation, as well as emerging challenges and tensions. Case studies from the European Union and various countries demonstrate that maintaining digital sovereignty requires balancing control and openness, developing domestic capabilities while fostering international cooperation, and considering the rights and interests of diverse stakeholders. The analysis reveals the complexities in implementing digital sovereignty

frameworks, particularly in areas such as data localization, infrastructure development, and market competition. The research highlights the importance of developing flexible and adaptive regulatory frameworks that can address emerging challenges while protecting national interests and individual rights. Through comprehensive examination of policy instruments, governance mechanisms, and implementation strategies, the study provides insights into effective approaches for achieving digital sovereignty. The findings suggest that success in maintaining digital sovereignty depends on developing comprehensive policies and regulatory mechanisms that address all dimensions and respond to rapidly evolving challenges. The article concludes with recommendations for developing effective and sustainable regulatory frameworks, emphasizing the importance of flexibility, participation, and adaptability to change.

Keywords: Digital Sovereignty, Digital Regulation, Digital Governance, Cybersecurity, Data Protection, Digital Policy, Technology Development

บทนำ

ในโลกดิจิทัลที่มีการเชื่อมต่อและพึ่งพากันมากขึ้น แนวคิดเรื่องอธิปไตยทางดิจิทัล (Digital Sovereignty) ได้กลายเป็นประเด็นสำคัญในการกำหนดนโยบายและการกำกับดูแลระดับโลก โดยเฉพาะอย่างยิ่งในช่วงทศวรรษที่ผ่านมา การเปิดเผยข้อมูลของ Edward Snowden ในปี 2013 เกี่ยวกับการสอดแนมข้อมูลในวงกว้างโดยหน่วยงานความมั่นคงของสหรัฐอเมริกา ได้กระตุ้นให้เกิดความตระหนักถึงความเสี่ยงของการพึ่งพาโครงสร้างพื้นฐานดิจิทัลที่ควบคุมโดยประเทศมหาอำนาจและบริษัทเทคโนโลยีขนาดใหญ่ (Pohle and Thiel, 2020) การพัฒนาอย่างรวดเร็วของเทคโนโลยีดิจิทัลและการขยายตัวของบริษัทเทคโนโลยียักษ์ใหญ่ได้ท้าทายแนวคิดดั้งเดิมเรื่องอธิปไตยของรัฐที่มักผูกติดกับดินแดนทางกายภาพ

ความสำคัญของอธิปไตยทางดิจิทัลยิ่งเพิ่มขึ้นท่ามกลางความขัดแย้งทางภูมิรัฐศาสตร์และการแข่งขันทางเทคโนโลยีระหว่างมหาอำนาจ โดยเฉพาะระหว่างสหรัฐอเมริกา จีน และสหภาพยุโรป Floridi (2020) ชี้ให้เห็นว่าการควบคุมโครงสร้างพื้นฐานดิจิทัล ข้อมูล และมาตรฐานเทคโนโลยีได้กลายเป็นแหล่งที่มาของอำนาจในศตวรรษที่ 21 ประเทศและภูมิภาคต่างๆ จึงพยายามพัฒนากรอบนโยบายและกลไกการกำกับดูแลเพื่อปกป้องผลประโยชน์ทางดิจิทัลของตน โดยสหภาพยุโรปได้เป็นผู้นำในการกำหนดมาตรฐานการคุ้มครองข้อมูลและการกำกับดูแลแพลตฟอร์มดิจิทัลผ่านกฎหมายอย่าง GDPR, Digital Markets Act และ Digital Services Act

การพัฒนาแนวคิดเรื่องอธิปไตยทางดิจิทัลมีความซับซ้อนเนื่องจากต้องคำนึงถึงผู้มีส่วนได้ส่วนเสียที่หลากหลาย ทั้งรัฐบาล ภาคธุรกิจ และภาคประชาสังคม Roberts et al. (2021) เสนอว่าอธิปไตยทางดิจิทัลไม่ควรถูกมองเพียงมิติของการควบคุมโดยรัฐ แต่ควรพิจารณาถึงสิทธิและเสรีภาพของพลเมือง การแข่งขันทางเศรษฐกิจ และความมั่นคงปลอดภัยทางไซเบอร์ด้วย การสร้างสมดุลระหว่างผลประโยชน์ที่แตกต่างและบางครั้งขัดแย้งกันของผู้มีส่วนได้ส่วนเสียเหล่านี้เป็นความท้าทายสำคัญในการออกแบบกรอบการกำกับดูแลอธิปไตยทางดิจิทัล

ในขณะที่แต่ละประเทศพัฒนาแนวทางที่แตกต่างกันในการจัดการกับอธิปไตยทางดิจิทัล Moerel and Timmers (2021) ระบุว่ามีความจำเป็นต้องมีความร่วมมือระหว่างประเทศเพื่อจัดการกับความท้าทายข้ามพรมแดน เช่น การไหลเวียนของข้อมูล ความมั่นคงปลอดภัยทางไซเบอร์ และการกำกับดูแลแพลตฟอร์มดิจิทัลระดับโลก อย่างไรก็ตาม การสร้างกรอบการกำกับดูแลระหว่างประเทศที่มีประสิทธิภาพยังคงเป็นความท้าทาย เนื่องจากความแตกต่างในค่านิยม ผลประโยชน์ทางเศรษฐกิจ และแนวทางการกำกับดูแลระหว่างประเทศต่าง ๆ

วิกฤตโควิด-19 ได้เน้นย้ำความสำคัญของอธิปไตยทางดิจิทัล โดย Braun and Hummel (2024) ชี้ให้เห็นว่าการพึ่งพาแพลตฟอร์มดิจิทัลและบริการคลาวด์ที่ควบคุมโดยบริษัทต่างชาติในช่วงการระบาดได้กระตุ้นให้หลายประเทศทบทวนนโยบายด้านโครงสร้างพื้นฐานดิจิทัลและความมั่นคงทางข้อมูล การพัฒนาความสามารถภายในประเทศและการลดการพึ่งพาเทคโนโลยีต่างชาติจึงได้รับความสำคัญมากขึ้นในวาระนโยบายดิจิทัลของหลายประเทศ

บทความนี้มุ่งศึกษามิติที่หลากหลายของอธิปไตยทางดิจิทัลและการออกแบบการกำกับดูแล โดยจะเริ่มจากการวิเคราะห์กรอบแนวคิดและมิติต่าง ๆ ของอธิปไตยทางดิจิทัล จากนั้นจะอภิปรายเกี่ยวกับรูปแบบการกำกับดูแลที่แตกต่างกัน การออกแบบและการนำกฎระเบียบไปปฏิบัติ ความท้าทายและความตึงเครียดที่สำคัญ กรณีศึกษาที่น่าสนใจ และข้อเสนอแนะสำหรับทิศทางในอนาคต การวิเคราะห์จะครอบคลุมทั้งมุมมองด้านนโยบาย กฎหมาย เทคโนโลยี และการกำกับดูแล เพื่อนำเสนอภาพรวมที่ครอบคลุมของประเด็นที่ซับซ้อนนี้ ซึ่งจะทำให้ผู้อ่านได้เข้าใจประเด็นของอธิปไตยทางดิจิทัล และเห็นตัวอย่างที่เป็นรูปธรรม ตลอดจนมีความเข้าใจถึงโอกาสที่ภัยคุกคามไซเบอร์จะสามารถทำให้ระบบโครงสร้างพื้นฐานสำคัญต้องหยุดชะงัก บั่นทอนความมั่นคงระดับชาติ หรือแม้แต่ก่อให้เกิดอันตรายต่อภาคประชาชนได้

กรอบแนวคิด: มิติของอธิปไตยทางดิจิทัล

อธิปไตยทางดิจิทัลเป็นแนวคิดที่มีความซับซ้อนและหลากหลายมิติ ซึ่งได้รับการพัฒนาและตีความแตกต่างกันไปตามบริบทของแต่ละประเทศและภูมิภาค Pohle and Thiel (2020) ชี้ให้เห็นว่าการทำความเข้าใจมิติต่าง ๆ ของอธิปไตยทางดิจิทัลมีความสำคัญต่อการออกแบบนโยบายและการกำกับดูแลที่มีประสิทธิภาพ โดย Floridi (2020) เสนอว่าอธิปไตยทางดิจิทัลไม่ควรถูกมองเพียงมิติของการควบคุมโดยรัฐ แต่ควรพิจารณาถึงมิติทางเศรษฐกิจ สังคม และเทคโนโลยีที่เชื่อมโยงกัน การวิเคราะห์มิติต่างๆ เหล่านี้จะช่วยให้เข้าใจความซับซ้อนของอธิปไตยทางดิจิทัลและแนวทางในการจัดการกับความท้าทายที่เกี่ยวข้อง

มิติด้านอธิปไตยของรัฐ

มิติด้านอธิปไตยของรัฐเป็นมิติพื้นฐานที่สำคัญของอธิปไตยทางดิจิทัล โดย Moerel and Timmers (2021) อธิบายว่าอธิปไตยของรัฐในบริบทดิจิทัลเกี่ยวข้องกับความสามารถของรัฐในการควบคุมและกำกับดูแลโครงสร้างพื้นฐานดิจิทัล ข้อมูล และกิจกรรมทางดิจิทัลภายในเขตอำนาจของตน ความสำคัญของมิตินี้เพิ่มขึ้นท่ามกลางความกังวลเกี่ยวกับการแทรกแซงจากต่างชาติและการพึ่งพาเทคโนโลยีต่างประเทศ

การศึกษาของ Glasze et al. (2023) แสดงให้เห็นว่ารัฐต่าง ๆ มีแนวทางที่แตกต่างกันในการรักษาอธิปไตยทางดิจิทัล โดยประเทศจีนและรัสเซียเน้นการควบคุมอย่างเข้มงวดผ่านการสร้าง "อินเทอร์เน็ตแห่งชาติ" และกฎหมายที่เข้มงวด ในขณะที่สหภาพยุโรปเน้นการสร้างกรอบกฎหมายที่สมดุลระหว่างการควบคุมและการเปิดกว้าง โดยมุ่งเน้นการปกป้องสิทธิของพลเมืองและการส่งเสริมนวัตกรรม

Bellanova, Carrapico, & Duez (2022) เสนอว่าอธิปไตยของรัฐในยุคดิจิทัลไม่ได้จำกัดอยู่เพียงการควบคุมทางกายภาพ แต่รวมถึงความสามารถในการกำหนดมาตรฐาน กฎระเบียบ และการมีอิทธิพลต่อพฤติกรรมในโลกดิจิทัล การบรรลุเป้าหมายนี้ต้องอาศัยความร่วมมือระหว่างภาครัฐ ภาคเอกชน และภาคประชาสังคม ตัวอย่างที่เป็นรูปธรรมที่แสดงว่า รัฐสามารถมีอิทธิพลต่อมาตรฐานระดับโลก ได้แก่ การออกกฎหมายที่บริษัททั่วโลกจำเป็นต้องปฏิบัติตาม เช่น GDPR (General Data Protection Regulation) (Issaoui, Örtensjö, & Islam, 2023) การสร้างหรือผลักดันมาตรฐานเทคโนโลยีผ่านองค์กรระหว่างประเทศ เช่น NIST, ITU (Casaril & Galletta, 2023) การสนับสนุนเทคโนโลยีที่กลายเป็นมาตรฐานกลางของตลาด เช่น 5G, IPv6 (Lemmi, Puliafito, Virdis, Mingozzi, 2024) การใช้เวที G20/UN/OECD เพื่อผลักดันแนวคิดด้านข้อมูล เช่น DFFT (Christakis, 2024) การบังคับใช้มาตรฐานผ่านการจัดซื้อจัดจ้างของรัฐ (เช่น FedRAMP) (Pranith, 2023) ตัวอย่างเหล่านี้สะท้อนว่าอธิปไตยของรัฐในยุคดิจิทัลไม่ใช่แค่การควบคุม

ภายในประเทศ แต่เป็นความสามารถในการ “กำหนดกฎของเกมระดับโลก” ผ่านกฎหมาย เทคโนโลยี และสถาบันระหว่างประเทศ

มิติด้านอธิปไตยทางเศรษฐกิจ

อธิปไตยทางเศรษฐกิจในบริบทดิจิทัลเกี่ยวข้องกับความสามารถในการควบคุมและพัฒนาระบบเศรษฐกิจดิจิทัลที่เป็นอิสระ Roberts et al. (2021) ชี้ให้เห็นว่าการพึ่งพาแพลตฟอร์มดิจิทัลและบริการคลาวด์ที่ควบคุมโดยบริษัทต่างชาติสร้างความเสี่ยงต่อความมั่นคงทางเศรษฐกิจและความสามารถในการแข่งขันของประเทศ โดยมีนักวิจัย Autolitano and Pawlowska (2021) วิเคราะห์โครงการ Gaia-X ของสหภาพยุโรปซึ่งเป็นตัวอย่างของความพยายามในการสร้างอธิปไตยทางเศรษฐกิจดิจิทัล โดยมุ่งพัฒนาโครงสร้างพื้นฐานคลาวด์ที่เป็นอิสระและสอดคล้องกับมาตรฐานของยุโรป การริเริ่มนี้สะท้อนให้เห็นถึงความสำคัญของการลดการพึ่งพาผู้ให้บริการต่างชาติและการสร้างระบบนิเวศดิจิทัลที่ยั่งยืน นอกจากนี้ Falkner, Heidebrecht, Obendiek, & Seidl (2024) ยังเน้นย้ำความสำคัญของการพัฒนาความสามารถในการแข่งขันด้านเทคโนโลยีและการส่งเสริมนวัตกรรมภายในประเทศ โดยเฉพาะในเทคโนโลยีสำคัญเช่น ปัญญาประดิษฐ์ การประมวลผลควอนตัม และเซมิคอนดักเตอร์ ซึ่งจะเป็นกุญแจสำคัญในการรักษาอธิปไตยทางเศรษฐกิจในอนาคต

ในที่นี้ขอยกตัวอย่างเพิ่มเติมในคำว่า ระบบเศรษฐกิจดิจิทัลที่เป็นอิสระ ได้แก่ การพึ่งพาเทคโนโลยีหลักจากต่างชาตินิ้อยลง (ลด Digital Dependency)หมายถึง รัฐสามารถใช้หรือพัฒนาเทคโนโลยีของตนเองสำหรับโครงสร้างพื้นฐานที่สำคัญ เช่น ระบบคลาวด์ของรัฐ เป็นต้น เพื่อไม่ให้ประเทศถูกครอบงำโดยเทคโนโลยีของบริษัทต่างชาติ เช่น AWS, Google, Huawei เป็นต้น ซึงช่วยในการลดความเสี่ยงว่าบริการจะถูกปิดกั้น ควบคุม หรือเงื่อนไขถูกกำหนดจากภายนอก (Ali, & Osmanaj, 2020) การควบคุมห่วงโซ่อุปทานเทคโนโลยีที่สำคัญ (Strategic Tech Supply Chains) หมายถึง รัฐสามารถเข้าถึงหรือผลิตส่วนประกอบสำคัญ เช่น ชิป (Anwar, et al., 2025) การบริหารข้อมูลของประเทศได้ด้วยตนเอง (Data Sovereignty) ระบบเศรษฐกิจดิจิทัลที่เป็นอิสระต้องสามารถกำหนดกฎเกณฑ์การส่งออกข้อมูลป้องกันการนำข้อมูลไปใช้เพื่อผลประโยชน์ของต่างชาติ (Belli, Gaspar,& Jaswant, 2024) การสร้างแพลตฟอร์มเศรษฐกิจดิจิทัลของตนเอง (Domestic Digital Ecosystem) หมายถึง ประเทศมีความสามารถสร้าง/สนับสนุนแพลตฟอร์มที่สำคัญ เช่น บริการโฆษณาออนไลน์เพื่อไม่ให้เศรษฐกิจดิจิทัลถูกครอบครองโดยแพลตฟอร์มข้ามชาติ (Krasyuk Kolgan, Medvedeva, 2022) การกำหนดกฎเกณฑ์เศรษฐกิจดิจิทัลได้เอง (Regulatory Autonomy) หมายถึง รัฐสามารถกำหนดกฎการแข่งขันได้ด้วยตนเองโดยไม่ถูกบีบบังคับจากตลาดต่างประเทศหรือแรงกดดันทางการทูต (Burri & Kugler, 2024) การสร้างนวัตกรรมและอุตสาหกรรมดิจิทัลในประเทศ (Domestic Digital Innovation) ระบบเศรษฐกิจดิจิทัลที่เป็นอิสระต้องมีสตาร์ทอัพของตนเองเพื่อให้ประเทศสามารถแข่งขันได้ในระยะยาว (Uršič, & Čater, 2025)

มิติด้านอธิปไตยของปัจเจกบุคคล

Braun and Hummel (2024) นำเสนอมุมมองที่สำคัญเกี่ยวกับมิติด้านอธิปไตยของปัจเจกบุคคลในบริบทดิจิทัล โดยเน้นความสำคัญของการให้อำนาจแก่พลเมืองในการควบคุมข้อมูลส่วนบุคคลและตัวตนดิจิทัลของตน การคุ้มครองสิทธิส่วนบุคคลและความเป็นส่วนตัวเป็นองค์ประกอบสำคัญของมิตินี้ Tan, Chi-Hung, & Lam (2023) อธิบายแนวคิดเรื่องอัตลักษณ์ดิจิทัลที่พึ่งพาตนเองได้ (Self-Sovereign Identity) ซึ่งเป็นรูปแบบใหม่ของการจัดการตัวตนดิจิทัลที่ให้อำนาจแก่ปัจเจกบุคคลในการควบคุมข้อมูลของตนเองอย่างเต็มที่ แนวคิดนี้สะท้อนการเปลี่ยนแปลงจากการควบคุมโดยองค์กรไปสู่การให้อำนาจแก่ผู้ใช้ การศึกษาของ Celeste (2021) ยังชี้ให้เห็นว่าการรักษาสมดุลระหว่างอธิปไตยของรัฐและสิทธิของปัจเจกบุคคลเป็นความท้าทายสำคัญในการออกแบบนโยบายดิจิทัล โดยเฉพาะในประเด็นเกี่ยวกับการเฝ้าระวังทางดิจิทัล การรวบรวมข้อมูล และการใช้เทคโนโลยีที่มีผลกระทบต่อสิทธิมนุษยชน

หลักการสำคัญของ อัตลักษณ์ดิจิทัลที่พึ่งพาตนเองได้(Self-Sovereign Identity:SSI) SSI สร้างขึ้นบนเทคโนโลยีบล็อกเชน (Blockchain) หรือระบบบัญชีแยกประเภทแบบกระจายศูนย์ (Distributed Ledger Technology - DLT) เพื่อให้เกิดความปลอดภัยและความโปร่งใส หลักการพื้นฐานที่สำคัญมีดังนี้: (Soltani, Zaman, Joshi, Sampalli, 2022) ความเป็นเจ้าของ (Ownership): ผู้ใช้ข้อมูลเป็นเจ้าของและควบคุมข้อมูลอัตลักษณ์ทั้งหมดของท่าน ซึ่งตัดสินใจว่าจะแบ่งปันอะไร

กับใคร และเมื่อใด (Quinn, & Connolly, 2021) การกระจายศูนย์ (Decentralization): อัตลักษณ์ไม่ได้ถูกเก็บไว้ในฐานข้อมูลส่วนกลาง แต่จะถูกบันทึกในรูปแบบที่กระจายศูนย์บนบล็อกเชน ทำให้ยากต่อการถูกแฮกหรือถูกควบคุมโดยหน่วยงานใดหน่วยงานหนึ่ง (Anthony Jnr, 2023) ตัวระบุอัตลักษณ์ดิจิทัล (Decentralized Identifiers - DIDs): เป็นรหัสเฉพาะที่อยู่บนบล็อกเชน ใช้เพื่อระบุตัวตนของผู้ใช้อย่างถาวรและไม่สามารถเปลี่ยนแปลงได้ DIDs ไม่ได้เปิดเผยข้อมูลส่วนตัวใดๆ โดยตรง (Zhao, Zhong, & Cui, 2023)

-ข้อมูลรับรองที่ตรวจสอบได้ (Verifiable Credentials - VCs) นี่คือ "ใบรับรองดิจิทัล" ที่ใช้แทนเอกสารจริง เช่น ใบขับขี่ ปริญญาบัตร หรือบัตรประชาชน หน่วยงานที่ออก (Issuer) จะลงนามด้วยลายเซ็นดิจิทัล (cryptographic signature) เพื่อรับรองความถูกต้อง ผู้ถือ (Holder) คือผู้ใช้เอง และสามารถนำไปแสดงให้ผู้ตรวจสอบ (Verifier) ตรวจสอบได้โดยตรงผ่านบล็อกเชน (Gudipati, 2025)

มิติด้านอธิปไตยทางเทคโนโลยี

มิติด้านอธิปไตยทางเทคโนโลยีเกี่ยวข้องกับความสามารถในการพัฒนา ควบคุม และกำหนดมาตรฐานเทคโนโลยี Sheikh (2022) วิเคราะห์ความสำคัญของการพัฒนาความสามารถทางเทคโนโลยีภายในประเทศ โดยเฉพาะในด้านโครงสร้างพื้นฐานที่สำคัญ เช่น เครือข่าย 5G ระบบคลาวด์ และเทคโนโลยีปัญญาประดิษฐ์ การศึกษาของ Chander and Sun (2021) อธิบายว่าอธิปไตยทางเทคโนโลยีไม่ได้หมายถึงการแยกตัวออกจากระบบเทคโนโลยีโลก แต่เป็นการสร้างความสามารถในการตัดสินใจอย่างอิสระเกี่ยวกับการใช้และการพัฒนาเทคโนโลยี รวมถึงการมีส่วนร่วมในการกำหนดมาตรฐานระดับโลก ในขณะที่ Lehuedé (2024) เน้นย้ำความสำคัญของการพิจารณามิติทางเทคโนโลยีในบริบทของความเป็นธรรมและความยั่งยืน โดยเฉพาะการคำนึงถึงผลกระทบของการพัฒนาเทคโนโลยีต่อสิ่งแวดล้อมและสังคม การสร้างอธิปไตยทางเทคโนโลยีจึงควรคำนึงถึงการพัฒนาที่ยั่งยืนและเป็นธรรม

ตัวอย่างของอธิปไตยทางเทคโนโลยี ได้แก่ อธิปไตยด้านคำนวณ (Compute Sovereignty) เช่น การมีศูนย์ข้อมูล (data center) หรือ “ศูนย์ประมวลผล AI” ภายในประเทศ เพื่อไม่ต้องพึ่งพาโครงสร้างพื้นฐานคอมพิวต์ของต่างชาติ (Misraa, Barikb ,& Kvalvik, 2025). อธิปไตยโมเดล AI (AI / Model Sovereignty) เช่น การพัฒนา “โมเดลภาษา” หรือ “โมเดลปัญญาประดิษฐ์” (Large Language Models, LLM) ภายในประเทศ เพื่อไม่ต้องใช้โมเดลของต่างชาติทั้งหมด (Sayankina, Tsen, Tan, & Ko, 2025). อธิปไตยนโยบายและกฎหมาย (Governance Sovereignty) เช่น การออกกฎหมายมาตรฐานทางดิจิทัล “digital governance” ที่เอื้อให้ประเทศควบคุมการไหลของข้อมูล และกำกับดูแลเทคโนโลยีอย่างมีอำนาจ (Spandler, Hartelius, Monti, & Söderbaum, 2024)

มิติด้านอธิปไตยทางข้อมูล

มิติสุดท้ายที่สำคัญคือด้านอธิปไตยทางข้อมูล Pohle and Santaniello (2024) อธิบายว่าการควบคุมข้อมูลเป็นองค์ประกอบสำคัญของอธิปไตยในยุคดิจิทัล ครอบคลุมทั้งการจัดเก็บ การประมวลผล และการไหลเวียนของข้อมูลข้ามพรมแดนDonnelly, Ríos Camacho, & Heidebrecht (2024) วิเคราะห์ความสำคัญของการกำหนดนโยบายและกฎระเบียบเกี่ยวกับการจัดการข้อมูล โดยเฉพาะในภาคการเงินดิจิทัล การกำหนดมาตรฐานการคุ้มครองข้อมูลและความปลอดภัยทางไซเบอร์เป็นส่วนสำคัญของการรักษาอธิปไตยทางข้อมูล โดย Hoeffler and Mérand (2024) เน้นย้ำความสำคัญของการสร้างสมดุลระหว่างการไหลเวียนข้อมูลเสรีและการปกป้องข้อมูลสำคัญ โดยชี้ให้เห็นว่าการจำกัดการไหลเวียนข้อมูลมากเกินไปอาจส่งผลเสียต่อนวัตกรรมและการพัฒนาเศรษฐกิจดิจิทัล ในขณะที่การเปิดเสรีมากเกินไปอาจเสี่ยงต่อความมั่นคงและความเป็นส่วนตัว

ตัวอย่างมิติ “อธิปไตยทางข้อมูล” (Data Sovereignty) ได้แก่ นโยบายเก็บข้อมูลในประเทศ (Data Localization) เช่น บางประเทศบังคับให้ข้อมูลสำคัญ (เช่น ข้อมูลส่วนบุคคล) ต้องเก็บอยู่บนเซิร์ฟเวอร์ในประเทศของตน (Swire, Kennedy-Mayo, Bagley, Krasser, Modak, & Bausewein, 2024) คลาวด์ในประเทศ (Sovereign Cloud) เช่น รัฐหรือองค์กรภาครัฐอาจสร้าง “คลาวด์แห่งชาติ” (sovereign cloud) ที่ให้บริการจัดเก็บและประมวลผลข้อมูลภายในประเทศภายใต้กฎหมายท้องถิ่น (Rone, 2024) กฎหมายควบคุมการส่งข้อมูลข้ามประเทศ เช่น บางประเทศมีกฎหมายห้ามหรือ

จำกัดการส่งข้อมูลออกนอกประเทศโดยเฉพาะข้อมูลสำคัญหรือข้อมูลส่วนบุคคล เพื่อรักษาความเป็นเจ้าของและการควบคุมข้อมูลของรัฐ ตัวอย่างเช่นในจีนมีกฎหมาย “Data Security Law” ที่ควบคุมการจัดเก็บและโอนย้ายข้อมูลเพื่อรักษาความมั่นคงของชาติ (Ducato, 2020) การควบคุมสิทธิการเข้าถึงและใช้งานข้อมูล เช่น Google Workspace มีแนวทาง “digital sovereignty” ให้ลูกค้าเลือกได้ว่าข้อมูลขององค์กรจะจัดเก็บและประมวลผลที่ใด และควบคุมสิทธิ์การเข้าถึง ขณะเดียวกันต้องปฏิบัติตามกฎระเบียบของแต่ละประเทศ (Jansen, Kadenko, Broeders, van Eeten, Borgolte, & Fiebig, 2023) การปกป้องความมั่นคงของชาติผ่านข้อมูล เช่น ข้อมูลบางประเภทมีผลกระทบต่อความมั่นคงของประเทศ (เช่น ข้อมูลเกี่ยวกับโครงสร้างพื้นฐาน, ข้อมูลภูมิศาสตร์, ข้อมูลทหาร) รัฐอาจกำหนดให้ข้อมูลเหล่านี้ “อยู่ในเขตอำนาจ” ของตนเท่านั้น (Oerlemans, & Langenhuijzen, 2024).

การบูรณาการมิติต่างๆ ของอธิปไตยทางดิจิทัล

การทำความเข้าใจความสัมพันธ์และการเชื่อมโยงระหว่างมิติต่าง ๆ ของอธิปไตยทางดิจิทัลมีความสำคัญต่อการพัฒนานโยบายและการกำกับดูแลที่มีประสิทธิภาพ Fratini, Hine, Novelli, Roberts, & Floridi (2024) เสนอว่าการพิจารณามิติต่าง ๆ แยกจากกันอาจนำไปสู่การกำหนดนโยบายที่ขาดความสอดคล้องและอาจก่อให้เกิดผลกระทบที่ไม่พึงประสงค์ การบูรณาการมิติต่าง ๆ จึงเป็นสิ่งจำเป็นในการสร้างกรอบการกำกับดูแลที่ครอบคลุมและมีประสิทธิภาพ การศึกษาของ Monsees and Lambach (2022) วิเคราะห์ว่าการสร้างสมดุลระหว่างมิติต่างๆ มีความซับซ้อนเนื่องจากแต่ละมิติมีเป้าหมายและความต้องการที่อาจขัดแย้งกัน เช่น การรักษาความมั่นคงของรัฐอาจกระทบต่อสิทธิความเป็นส่วนตัวของปัจเจกบุคคล หรือการส่งเสริมการแข่งขันทางเศรษฐกิจอาจต้องแลกกับการพึ่งพาเทคโนโลยีต่างประเทศ การหาจุดสมดุลระหว่างผลประโยชน์ที่ขัดแย้งกันเหล่านี้เป็นความท้าทายสำคัญในการกำหนดนโยบาย ในขณะที่ Kaloudis (2021) นำเสนอแนวคิดเรื่อง "อธิปไตยทางดิจิทัลแบบบูรณาการ" (Integrated Digital Sovereignty) ที่เน้นการพิจารณาความเชื่อมโยงระหว่างมิติต่างๆ และผลกระทบที่มีต่อกัน การพัฒนานโยบายภายใต้แนวคิดนี้ต้องคำนึงถึงผลกระทบทั้งทางตรงและทางอ้อมที่อาจเกิดขึ้นในมิติอื่นๆ เพื่อหลีกเลี่ยงการเกิดผลลัพธ์ที่ไม่พึงประสงค์ สอดคล้องกับ Heidebrecht (2024) เสริมว่าความสำเร็จในการบูรณาการมิติต่างๆ ของอธิปไตยทางดิจิทัลขึ้นอยู่กับการมีส่วนร่วมของผู้มีส่วนได้ส่วนเสียที่หลากหลาย ทั้งภาครัฐ ภาคเอกชน ภาควิชาการ และภาคประชาสังคม การสร้างกลไกการมีส่วนร่วมและการปรึกษาหารือที่มีประสิทธิภาพจะช่วยให้การพัฒนานโยบายสามารถตอบสนองต่อความต้องการและข้อกังวลของทุกภาคส่วน

ความท้าทายในการบูรณาการมิติต่าง ๆ ยังรวมถึงความแตกต่างในระดับการพัฒนาและความพร้อมระหว่างประเทศ Leese (2024) ชี้ให้เห็นว่าประเทศที่มีความก้าวหน้าทางเทคโนโลยีและทรัพยากรที่จำกัดอาจมีข้อจำกัดในการพัฒนาความสามารถในทุกมิติพร้อมกัน การจัดลำดับความสำคัญและการวางแผนการพัฒนาอย่างเป็นขั้นตอนจึงมีความสำคัญ โดยต้องคำนึงถึงทรัพยากรที่มีอยู่และความเร่งด่วนของความท้าทายในแต่ละมิติ และท้ายที่สุด Roberts (2024) เน้นย้ำความสำคัญของการพัฒนากรอบการประเมินและติดตามผลที่ครอบคลุมทุกมิติของอธิปไตยทางดิจิทัล การมีตัวชี้วัดและเครื่องมือการประเมินที่เหมาะสมจะช่วยให้สามารถติดตามความก้าวหน้า ระบุช่องว่างและความท้าทาย และปรับปรุงนโยบายให้มีประสิทธิภาพมากขึ้น การพัฒนาดัชนีอธิปไตยทางดิจิทัลที่ครอบคลุมทุกมิติจึงเป็นก้าวสำคัญในการสนับสนุนการกำหนดนโยบายที่มีประสิทธิภาพ

รูปแบบการกำกับดูแลและแนวทางต่าง ๆ

การกำกับดูแลอธิปไตยทางดิจิทัลมีรูปแบบและแนวทางที่หลากหลาย สะท้อนถึงความแตกต่างในค่านิยม ระบบการเมือง และเป้าหมายทางยุทธศาสตร์ของแต่ละประเทศและภูมิภาค Pohle and Thiel (2020) ชี้ให้เห็นว่าการทำความเข้าใจรูปแบบการกำกับดูแลที่แตกต่างกันมีความสำคัญต่อการวิเคราะห์นโยบายและการพัฒนากรอบการกำกับดูแลที่เหมาะสม โดยแต่ละรูปแบบมีจุดแข็ง ข้อจำกัด และผลกระทบที่แตกต่างกันต่อการพัฒนาเศรษฐกิจดิจิทัลและสังคม

รูปแบบการกำกับดูแลที่เน้นสิทธิ (Rights-Based Model)

รูปแบบการกำกับดูแลที่เน้นสิทธิ ซึ่งเป็นแนวทางที่สหภาพยุโรปเป็นผู้นำ ให้ความสำคัญกับการคุ้มครองสิทธิพื้นฐานของพลเมืองในยุคดิจิทัล Floridi (2020) อธิบายว่าแนวทางนี้มุ่งเน้นการสร้างสมดุลระหว่างการพัฒนาเทคโนโลยีและการปกป้องสิทธิมนุษยชน โดยเฉพาะสิทธิความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคล Celeste (2021) วิเคราะห์ว่าความสำเร็จของ GDPR ในการกำหนดมาตรฐานการคุ้มครองข้อมูลระดับโลกแสดงให้เห็นถึงอิทธิพลของแนวทางที่เน้นสิทธิ การที่บริษัทเทคโนโลยีทั่วโลกต้องปรับตัวให้สอดคล้องกับมาตรฐานของสหภาพยุโรปสะท้อนถึงพลังของการกำกับดูแลที่เน้นการคุ้มครองสิทธิพื้นฐาน อย่างไรก็ตาม Moerel and Timmers (2021) ชี้ให้เห็นว่าการนำแนวทางนี้ไปปฏิบัติมีความท้าทาย โดยเฉพาะในการสร้างสมดุลระหว่างการคุ้มครองสิทธิและการส่งเสริมนวัตกรรม การกำหนดกฎระเบียบที่เข้มงวดเกินไปอาจส่งผลกระทบต่อความสามารถในการแข่งขันและการพัฒนาเทคโนโลยีใหม่ๆ

รูปแบบการกำกับดูแลที่เน้นตลาด (Market-Oriented Model)

รูปแบบการกำกับดูแลที่เน้นตลาด ซึ่งเป็นแนวทางที่สหรัฐอเมริกาเป็นผู้นำ ให้ความสำคัญกับการส่งเสริมนวัตกรรมและการแข่งขันเสรี Chander and Sun (2021) อธิบายว่าแนวทางนี้เน้นการกำกับดูแลที่ยืดหยุ่นและการให้ภาคเอกชนมีบทบาทนำในการพัฒนาเทคโนโลยีและบริการดิจิทัล Roberts et al. (2021) วิเคราะห์ว่าแนวทางที่เน้นตลาดมีส่วนสำคัญในการสร้างบริษัทเทคโนโลยีระดับโลกและการพัฒนานวัตกรรมที่เปลี่ยนแปลงโลก อย่างไรก็ตาม แนวทางนี้ก็มีข้อจำกัด โดยเฉพาะในการจัดการกับความท้าทายด้านความเป็นส่วนตัว การผูกขาด และผลกระทบทางสังคมของเทคโนโลยีดิจิทัล Hoeffler and Mérand (2024) เสริมว่าการขาดการกำกับดูแลที่เข้มงวดในแนวทางที่เน้นตลาดอาจนำไปสู่การสะสมอำนาจมากเกินไปในมือของบริษัทเทคโนโลยีขนาดใหญ่ ซึ่งอาจส่งผลกระทบต่อความเป็นธรรมในการแข่งขันและการคุ้มครองผู้บริโภค

รูปแบบการกำกับดูแลแบบรวมศูนย์ (Centralization Model)

รูปแบบการกำกับดูแลแบบรวมศูนย์ ซึ่งเป็นแนวทางที่จีนและรัสเซียเป็นตัวอย่าง เน้นการควบคุมโดยรัฐอย่างเข้มงวด Glasze et al. (2023) อธิบายว่าแนวทางนี้ให้ความสำคัญกับความมั่นคงของรัฐและการควบคุมเนื้อหาดิจิทัล โดยรัฐมีบทบาทสำคัญในการกำหนดทิศทางและควบคุมการพัฒนาเทคโนโลยีดิจิทัล การศึกษาของ Pohle and Santaniello (2024) แสดงให้เห็นว่าแนวทางแบบรวมศูนย์สามารถนำไปสู่การพัฒนาความสามารถทางเทคโนโลยีที่แข็งแกร่งและการปกป้องผลประโยชน์ของชาติได้อย่างมีประสิทธิภาพ อย่างไรก็ตาม แนวทางนี้มักถูกวิจารณ์ในประเด็นเรื่องการละเมิดสิทธิมนุษยชนและการจำกัดเสรีภาพในการแสดงออก ในขณะที่ Falkner et al. (2024) เน้นย้ำว่าแม้แนวทางแบบรวมศูนย์จะมีข้อดีในแง่ของการควบคุมและการวางแผนเชิงยุทธศาสตร์ แต่อาจส่งผลเสียต่อนวัตกรรมและการพัฒนาเศรษฐกิจดิจิทัลในระยะยาว การขาดการแข่งขันและการจำกัดการไหลเวียนของข้อมูลอาจทำให้ประเทศพลาดโอกาสในการพัฒนาและการเรียนรู้จากประสบการณ์ระดับโลก

รูปแบบการกำกับดูแลแบบผสมผสาน (Hybrid/Multilevel Governance)

รูปแบบการกำกับดูแลแบบผสมผสานเป็นแนวทางที่พยายามรวมจุดแข็งของรูปแบบต่าง ๆ เข้าด้วยกัน Sheikh (2022) อธิบายว่าแนวทางนี้เน้นการสร้างสมดุลระหว่างการควบคุมโดยรัฐ การมีส่วนร่วมของภาคเอกชน และการคุ้มครองสิทธิของพลเมือง โดยมีการกระจายอำนาจการตัดสินใจไปยังระดับต่าง ๆ ตามความเหมาะสม Braun and Hummel (2024) วิเคราะห์ว่าการกำกับดูแลแบบผสมผสานมีความยืดหยุ่นและสามารถปรับตัวให้เข้ากับบริบทที่แตกต่างกันได้ดี ตัวอย่างเช่น สิงคโปร์ได้พัฒนารูปแบบการกำกับดูแลที่ผสมผสานระหว่างการควบคุมโดยรัฐที่เข้มแข็งกับการส่งเสริมนวัตกรรมและการแข่งขันในภาคเอกชน ทำให้สามารถรักษาสมดุลระหว่างความมั่นคงและการพัฒนาทางเศรษฐกิจได้อย่างมีประสิทธิภาพ สอดคล้องกับ Lehuedé (2024) เสริมว่าความสำเร็จของการกำกับดูแลแบบผสมผสานขึ้นอยู่กับการมีกลไกประสานงานที่มีประสิทธิภาพระหว่างผู้มีส่วนได้ส่วนเสียต่าง ๆ และการมีกรอบกฎหมายที่ชัดเจนในการกำหนดบทบาทและความรับผิดชอบของแต่ละฝ่าย

บทบาทของผู้มีส่วนได้ส่วนเสียที่ไม่ใช่รัฐ (Role of Non-State Actors)

ในการกำกับดูแลอธิปไตยทางดิจิทัล บทบาทของผู้มีส่วนได้ส่วนเสียที่ไม่ใช่รัฐมีความสำคัญเพิ่มขึ้น Donnelly et al. (2024) ชี้ให้เห็นว่าภาคเอกชน โดยเฉพาะบริษัทเทคโนโลยีขนาดใหญ่ มีอิทธิพลอย่างมากต่อการพัฒนาและการกำหนดมาตรฐานทางเทคโนโลยี การมีส่วนร่วมของภาคเอกชนในการกำหนดนโยบายและการกำกับดูแลจึงมีความสำคัญต่อความสำเร็จของการรักษาอธิปไตยทางดิจิทัล สอดคล้องกับ Kaloudis (2021) วิเคราะห์บทบาทของภาคประชาสังคมและองค์กรระหว่างประเทศในการสร้างความสมดุลระหว่างผลประโยชน์ของรัฐและเอกชน องค์กรเหล่านี้มักทำหน้าที่เป็นตัวกลางในการสร้างความร่วมมือและการแลกเปลี่ยนความรู้ระหว่างผู้มีส่วนได้ส่วนเสียต่าง ๆ การศึกษาของ Monsees and Lambach (2022) เน้นย้ำความสำคัญของการสร้างเครือข่ายความร่วมมือระหว่างภาครัฐ ภาคเอกชน และภาคประชาสังคมในการพัฒนาและนำนโยบายด้านอธิปไตยทางดิจิทัลไปปฏิบัติ การมีส่วนร่วมของทุกภาคส่วนช่วยให้การกำกับดูแลมีความครอบคลุมและตอบสนองต่อความต้องการที่หลากหลายมากขึ้น

ทั้งนี้ การเลือกรูปแบบหนึ่งรูปแบบใดนั้น ยังไม่มีความสมบูรณ์ในตนเอง ทั้งนี้ การเลือกรูปแบบดังที่กล่าวมาข้างต้นต้องปรับให้เหมาะสมกับบริบทแวดล้อม และสถานการณ์ของแต่ละประเทศนั้น ๆ และการปรับเปลี่ยนจากรูปแบบหนึ่งไปรูปแบบหนึ่งต้องพิจารณาถึงความคุ้มค่าในการปรับเปลี่ยนด้วย ดังที่จะได้นำเสนอในหัวข้อต่อไป

ความท้าทายในการเลือกและการนำรูปแบบการกำกับดูแลไปปฏิบัติ

Heidebrecht (2024) ระบุความท้าทายสำคัญในการเลือกและการนำรูปแบบการกำกับดูแลไปปฏิบัติ โดยเฉพาะในประเด็นเรื่องความแตกต่างของบริบททางการเมือง เศรษฐกิจ และสังคมระหว่างประเทศ การเลือกรูปแบบการกำกับดูแลที่เหมาะสมต้องคำนึงถึงปัจจัยเหล่านี้และความพร้อมในการนำไปปฏิบัติ การศึกษาของ Roberts (2024) เสนอว่าการประเมินผลกระทบและการติดตามผลการดำเนินงานอย่างต่อเนื่องมีความสำคัญต่อความสำเร็จของการกำกับดูแล การมีระบบการประเมินที่มีประสิทธิภาพจะช่วยให้สามารถปรับปรุงและพัฒนารูปแบบการกำกับดูแลให้เหมาะสมกับสถานการณ์ที่เปลี่ยนแปลงไป Ruohonen (2021) ย้ำว่าความยืดหยุ่นและความสามารถในการปรับตัวเป็นคุณสมบัติสำคัญของรูปแบบการกำกับดูแลที่มีประสิทธิภาพ เนื่องจากเทคโนโลยีดิจิทัลมีการเปลี่ยนแปลงอย่างรวดเร็ว การกำกับดูแลจึงต้องสามารถปรับตัวให้ทันต่อการเปลี่ยนแปลงและความท้าทายใหม่ ๆ ที่เกิดขึ้น

การออกแบบและการนำกฎระเบียบไปปฏิบัติ

การออกแบบและการนำกฎระเบียบด้านอธิปไตยทางดิจิทัลไปปฏิบัติเป็นกระบวนการที่ซับซ้อนและต้องการการพิจารณาอย่างรอบคอบ Adonis (2019) เสนอว่าความสำเร็จของการกำกับดูแลขึ้นอยู่กับการออกแบบกฎระเบียบที่มีประสิทธิภาพและการสร้างกลไกการนำไปปฏิบัติที่เหมาะสม ซึ่งต้องคำนึงถึงทั้งมิติทางเทคนิค กฎหมาย และการบริหารจัดการ

เครื่องมือและกรอบนโยบาย

Leese (2024) วิเคราะห์ว่าเครื่องมือนโยบายที่ใช้ในการกำกับดูแลอธิปไตยทางดิจิทัลมีหลายรูปแบบ ตั้งแต่กฎหมายและข้อบังคับที่มีผลผูกพันทางกฎหมาย ไปจนถึงแนวปฏิบัติและมาตรฐานความสมัครใจ การเลือกใช้เครื่องมือที่เหมาะสมขึ้นอยู่กับบริบทและวัตถุประสงค์ของการกำกับดูแล สอดคล้องกับ Bria (2015) อธิบายว่าการผสมผสานเครื่องมือนโยบายต่าง ๆ เช่น การให้แรงจูงใจทางการเงิน การกำหนดมาตรฐานทางเทคนิค และการสร้างความร่วมมือระหว่างภาครัฐและเอกชน สามารถเพิ่มประสิทธิภาพของการกำกับดูแล โดยเฉพาะในการจัดการกับความท้าทายที่ซับซ้อนของอธิปไตยทางดิจิทัล การศึกษาของ Pohle and Santaniello (2024) แสดงให้เห็นว่าการพัฒนากรอบนโยบายที่ยืดหยุ่นและสามารถปรับตัวได้มีความสำคัญ เนื่องจากเทคโนโลยีและภูมิทัศน์ดิจิทัลมีการเปลี่ยนแปลงอย่างรวดเร็ว กรอบนโยบายจึงควรสามารถรองรับการเปลี่ยนแปลงและความท้าทายใหม่ๆ ที่อาจเกิดขึ้นในอนาคต

การกำกับดูแลแบบล่วงหน้าและย้อนหลัง

การกำกับดูแลแบบล่วงหน้า (Ex-ante) และแบบย้อนหลัง (Ex-post) มีบทบาทสำคัญในการรักษาอธิปไตยทางดิจิทัล Hoeffler and Mérand (2024) วิเคราะห์ว่าการกำกับดูแลแบบล่วงหน้า เช่น การกำหนดเงื่อนไขการเข้าสู่ตลาดและมาตรฐานการดำเนินงาน มีความสำคัญในการป้องกันปัญหาและความเสี่ยงที่อาจเกิดขึ้น Donnelly et al. (2024) เสริมว่าการกำกับดูแลแบบย้อนหลัง เช่น การตรวจสอบการละเมิดกฎระเบียบและการบังคับใช้บทลงโทษ มีความจำเป็นในการสร้างความรับผิดชอบและการปฏิบัติตามกฎระเบียบ การผสมผสานระหว่างการกำกับดูแลทั้งสองรูปแบบจะช่วยเพิ่มประสิทธิภาพของการกำกับดูแลโดยรวมAutolitano and Pawlowska (2021) นำเสนอกรณีศึกษาของ GDPR ที่ใช้ทั้งมาตรการล่วงหน้าในการกำหนดหลักการและมาตรฐานการคุ้มครองข้อมูล และมาตรการย้อนหลังในการตรวจสอบและลงโทษการละเมิด ซึ่งแสดงให้เห็นถึงประสิทธิภาพของการผสมผสานแนวทางทั้งสองแบบ

มาตรฐานโครงสร้างพื้นฐานและเทคโนโลยี

Sheikh (2022) ย้ำความสำคัญของการกำหนดมาตรฐานโครงสร้างพื้นฐานและเทคโนโลยีในการรักษาอธิปไตยทางดิจิทัล การมีมาตรฐานที่ชัดเจนช่วยให้การพัฒนาและการใช้งานเทคโนโลยีมีความปลอดภัย มีความเป็นมาตรฐาน และสามารถทำงานร่วมกันได้ สอดคล้องกับ Moerel and Timmers (2021) วิเคราะห์บทบาทของมาตรฐานในการส่งเสริมความร่วมมือระหว่างประเทศและการสร้างระบบนิเวศดิจิทัลที่ยั่งยืน การมีมาตรฐานที่เป็นที่ยอมรับในระดับสากลช่วยลดอุปสรรคในการทำงานร่วมกันและส่งเสริมการพัฒนานวัตกรรม และการศึกษาของ Glasze et al. (2023) เน้นย้ำความสำคัญของการมีส่วนร่วมในการกำหนดมาตรฐานระดับโลก โดยเฉพาะในเทคโนโลยีใหม่ๆ เช่น 5G, ปัญญาประดิษฐ์ และ Internet of Things การมีบทบาทในการกำหนดมาตรฐานช่วยให้ประเทศสามารถปกป้องผลประโยชน์และมีอิทธิพลต่อทิศทางการพัฒนาเทคโนโลยีในอนาคต

กรอบการกำกับดูแลข้อมูล

การกำกับดูแลข้อมูลเป็นองค์ประกอบสำคัญของอธิปไตยทางดิจิทัล Fratini et al. (2024) อธิบายว่ากรอบการกำกับดูแลข้อมูลที่มีประสิทธิภาพต้องครอบคลุมทั้งการจัดเก็บ การประมวลผล การแบ่งปัน และการปกป้องข้อมูล โดยต้องสร้างสมดุลระหว่างการใช้ประโยชน์จากข้อมูลและการคุ้มครองสิทธิความเป็นส่วนตัว Bellanova et al. (2022) วิเคราะห์ว่าการกำหนดกฎเกณฑ์เกี่ยวกับการไหลเวียนข้อมูลข้ามพรมแดนมีความสำคัญต่อการรักษาอธิปไตยทางดิจิทัล โดยเฉพาะในยุคที่ข้อมูลกลายเป็นทรัพยากรสำคัญทางเศรษฐกิจและยุทธศาสตร์ การมีกรอบการกำกับดูแลที่ชัดเจนช่วยให้ประเทศสามารถควบคุมการไหลเวียนของข้อมูลและปกป้องผลประโยชน์แห่งชาติ Tan et al. (2023) เสริมว่าการพัฒนากรอบการกำกับดูแลข้อมูลต้องคำนึงถึงความแตกต่างของประเภทข้อมูล เช่น ข้อมูลส่วนบุคคล ข้อมูลธุรกิจ และข้อมูลที่เกี่ยวข้องกับความมั่นคง แต่ละประเภทอาจต้องการมาตรการคุ้มครองและการกำกับดูแลที่แตกต่างกัน

กฎระเบียบด้านการแข่งขันทางการตลาด

Falkner et al. (2024) นำเสนอว่าการกำกับดูแลการแข่งขันในตลาดดิจิทัลมีความสำคัญต่อการรักษาอธิปไตยทางดิจิทัล โดยเฉพาะในการจัดการกับอำนาจผูกขาดของแพลตฟอร์มดิจิทัลขนาดใหญ่ กฎระเบียบด้านการแข่งขันต้องสามารถรองรับลักษณะเฉพาะของตลาดดิจิทัล เช่น ผลกระทบเครือข่าย (network effects) และการผูกขาดโดยธรรมชาติ Celeste (2021) วิเคราะห์ว่าการส่งเสริมการแข่งขันที่เป็นธรรมในตลาดดิจิทัลต้องอาศัยทั้งมาตรการเชิงโครงสร้างและมาตรการเชิงพฤติกรรม เช่น การป้องกันการใช้อำนาจเหนือตลาดในทางมิชอบ การส่งเสริมการเข้าถึงข้อมูลและโครงสร้างพื้นฐานอย่างเท่าเทียม และการสนับสนุนผู้ประกอบการรายใหม่ และ Lambach and Oppermann (2022) เน้นย้ำความสำคัญของการสร้างสภาพแวดล้อมที่เอื้อต่อการแข่งขันและนวัตกรรม โดยเฉพาะสำหรับผู้ประกอบการท้องถิ่นและวิสาหกิจขนาดกลางและขนาดย่อม การมีกฎระเบียบที่เหมาะสมจะช่วยลดการพึ่งพาแพลตฟอร์มต่างชาติและส่งเสริมการพัฒนาระบบนิเวศดิจิทัลภายในประเทศ

กลไกการบังคับใช้

Roberts (2024) อธิบายว่าประสิทธิภาพของการกำกับดูแลขึ้นอยู่กับความสามารถในการบังคับใช้กฎระเบียบอย่างมีประสิทธิภาพ การมีกลไกการบังคับใช้ที่เข้มแข็ง ทั้งในด้านกฎหมาย การบริหารจัดการ และทรัพยากร มีความสำคัญต่อ

ความน่าเชื่อถือของระบบการกำกับดูแล สอดคล้องกับ Kaloudis (2021) วิเคราะห์ความสำคัญของการสร้างความร่วมมือระหว่างหน่วยงานกำกับดูแลในระดับประเทศและระหว่างประเทศ เนื่องจากความท้าทายด้านอธิปไตยทางดิจิทัลมักมีลักษณะข้ามพรมแดน การแลกเปลี่ยนข้อมูลและการประสานงานระหว่างหน่วยงานจึงมีความสำคัญต่อประสิทธิภาพของการบังคับใช้ และ Lehuedé (2024) เสริมว่าการพัฒนาขีดความสามารถของหน่วยงานกำกับดูแลและการสร้างความเชี่ยวชาญในด้านเทคโนโลยีดิจิทัลมีความสำคัญต่อการบังคับใช้กฎระเบียบอย่างมีประสิทธิภาพ การลงทุนในการพัฒนาบุคลากรและโครงสร้างพื้นฐานสำหรับการกำกับดูแลจึงเป็นสิ่งจำเป็น

ความท้าทายและความตึงเครียด

มิติความท้าทายและความตึงเครียดในการดำเนินการด้านอธิปไตยทางดิจิทัลเป็นประเด็นที่ซับซ้อนและต้องการการจัดการอย่างระมัดระวัง Braun and Hummel (2024) ชี้ให้เห็นว่าการสร้างสมดุลระหว่างผลประโยชน์ที่แข่งขันกันและการจัดการกับข้อจำกัดต่าง ๆ เป็นความท้าทายสำคัญในการพัฒนานโยบายและการกำกับดูแลอธิปไตยทางดิจิทัล

การสร้างสมดุลระหว่างการเปิดกว้างและการควบคุม

ความท้าทายสำคัญประการแรกคือการสร้างสมดุลระหว่างการเปิดกว้างทางดิจิทัลและการควบคุม Pohle and Thiel (2020) อธิบายว่าการเปิดกว้างมีความสำคัญต่อการพัฒนานวัตกรรมและการเติบโตทางเศรษฐกิจ แต่ในขณะเดียวกันก็ต้องมีการควบคุมที่เพียงพอเพื่อปกป้องผลประโยชน์แห่งชาติและความมั่นคง สอดคล้องกับ Chander and Sun (2021) วิเคราะห์ว่าการสร้างสมดุลนี้มีความซับซ้อนเพิ่มขึ้นในบริบทของการแข่งขันระหว่างประเทศและภัยคุกคามทางไซเบอร์ที่เพิ่มขึ้น ประเทศต่าง ๆ ต้องพิจารณาอย่างรอบคอบว่าจะเปิดรับการลงทุนและเทคโนโลยีจากต่างประเทศในระดับใด โดยที่ยังสามารถรักษาความมั่นคงและอธิปไตยทางดิจิทัลไว้ได้ และ Floridi (2020) เสริมว่าการสร้างกรอบการกำกับดูแลที่ยืดหยุ่นและปรับตัวได้มีความสำคัญในการจัดการกับความตึงเครียดระหว่างการเปิดกว้างและการควบคุม โดยกรอบดังกล่าวควรสามารถปรับเปลี่ยนระดับการควบคุมตามความเสี่ยงและผลกระทบที่อาจเกิดขึ้น

การพึ่งพาทางเทคนิคและโครงสร้างพื้นฐาน

Moerel and Timmers (2021) ชี้ให้เห็นว่าการพึ่งพาทางเทคนิคและโครงสร้างพื้นฐานจากต่างประเทศเป็นความท้าทายสำคัญต่ออธิปไตยทางดิจิทัล โดยเฉพาะในด้านเทคโนโลยีขั้นสูงเช่น เซมิคอนดักเตอร์ การประมวลผลคลาวด์ และระบบ 5G การลดการพึ่งพาดังกล่าวต้องใช้เวลาและทรัพยากรจำนวนมาก Autolitano and Pawlowska (2021) วิเคราะห์กรณีของโครงการ Gaia-X ที่แสดงให้เห็นความท้าทายในการพัฒนาโครงสร้างพื้นฐานทางเลือก แม้จะมีความพยายามในการสร้างระบบคลาวด์ของยุโรป แต่การแข่งขันกับผู้ให้บริการที่มีความก้าวหน้าทางเทคโนโลยีและส่วนแบ่งตลาดที่สูงกว่าเป็นเรื่องยาก Sheikh (2022) เน้นย้ำความสำคัญของการลงทุนในการวิจัยและพัฒนา การสร้างความร่วมมือระหว่างประเทศและการพัฒนาบุคลากรในการลดการพึ่งพาทางเทคนิค อย่างไรก็ตาม การดำเนินการดังกล่าวต้องคำนึงถึงความคุ้มค่าทางเศรษฐกิจและความเป็นไปได้ในทางปฏิบัติ

ความซับซ้อนด้านเขตอำนาจศาล

Lehuedé (2024) อธิบายว่าความซับซ้อนด้านเขตอำนาจศาลในโลกดิจิทัลสร้างความท้าทายสำคัญในการกำกับดูแลอธิปไตยทางดิจิทัล เนื่องจากการไหลของข้อมูลและการให้บริการดิจิทัลไม่จำกัดอยู่ภายในพรมแดนประเทศ การกำหนดขอบเขตอำนาจและการบังคับใช้กฎหมายจึงมีความซับซ้อน Donnelly et al. (2024) วิเคราะห์ความท้าทายในการประสานงานระหว่างหน่วยงานกำกับดูแลในประเทศต่าง ๆ และการจัดการกับความขัดแย้งด้านกฎหมายและกฎระเบียบ การสร้างกรอบความร่วมมือระหว่างประเทศและกลไกการระงับข้อพิพาทที่มีประสิทธิภาพจึงมีความสำคัญ Monsees and Lambach (2022) เสริมว่าการพัฒนากรอบกฎหมายระหว่างประเทศที่ครอบคลุมและการสร้างความร่วมมือระหว่างหน่วยงานบังคับใช้กฎหมายมีความสำคัญในการจัดการกับความท้าทายด้านเขตอำนาจศาล อย่างไรก็ตาม การสร้างฉันทามติระหว่างประเทศในประเด็นดังกล่าวเป็นเรื่องที่ท้าทาย

ความตึงเครียดระหว่างนวัตกรรมและการกำกับดูแล

Hoeffler and Mérand (2024) ชี้ให้เห็นถึงความท้าทายในการสร้างสมดุลระหว่างการส่งเสริมนวัตกรรมและการกำกับดูแลที่มีประสิทธิภาพ การกำกับดูแลที่เข้มงวดเกินไปอาจจำกัดการพัฒนานวัตกรรมและความสามารถในการแข่งขัน ในขณะที่การกำกับดูแลที่หละหลวมเกินไปอาจนำไปสู่ความเสี่ยงและผลกระทบที่ไม่พึงประสงค์ Roberts et al. (2021) วิเคราะห์ว่าการออกแบบกรอบการกำกับดูแลที่ยืดหยุ่นและตอบสนองต่อการเปลี่ยนแปลงทางเทคโนโลยีมีความสำคัญ โดยเฉพาะในยุคที่เทคโนโลยีมีการพัฒนาอย่างรวดเร็ว การใช้แนวทาง "regulatory sandbox" และการทดลองนโยบายในขอบเขตจำกัดอาจช่วยให้เกิดความสมดุลระหว่างการส่งเสริมนวัตกรรมและการควบคุมความเสี่ยง Bellanova et al. (2022) เสริมว่าการสร้างความร่วมมือระหว่างภาครัฐและภาคเอกชนในการพัฒนากรอบการกำกับดูแลมีความสำคัญ การรับฟังความคิดเห็นจากผู้มีส่วนได้ส่วนเสียและการปรับปรุงกฎระเบียบอย่างต่อเนื่องจะช่วยให้การกำกับดูแลมีประสิทธิภาพและไม่เป็นอุปสรรคต่อการพัฒนานวัตกรรม

ความขัดแย้งระหว่างผลประโยชน์ระดับชาติและความร่วมมือระหว่างประเทศ

Kaloudis (2021) อธิบายว่าการรักษาสมดุลระหว่างผลประโยชน์ระดับชาติและความร่วมมือระหว่างประเทศเป็นความท้าทายสำคัญในการดำเนินการด้านอธิปไตยทางดิจิทัล ในขณะที่ประเทศต่างๆ ต้องการปกป้องผลประโยชน์แห่งชาติ แต่ความท้าทายหลายประการในโลกดิจิทัลต้องการความร่วมมือระหว่างประเทศในการแก้ไข Glasze et al. (2023) วิเคราะห์ว่าการแข่งขันทางภูมิรัฐศาสตร์และความไม่ไว้วางใจระหว่างประเทศเป็นอุปสรรคต่อการสร้างความร่วมมือด้านอธิปไตยทางดิจิทัล โดยเฉพาะในประเด็นที่เกี่ยวข้องกับความมั่นคงและการแข่งขันทางเศรษฐกิจ การสร้างกลไกความร่วมมือที่สร้างความไว้วางใจและผลประโยชน์ร่วมกันจึงมีความสำคัญ Falkner et al. (2024) เน้นย้ำความสำคัญของการพัฒนากรอบความร่วมมือระหว่างประเทศที่ยืดหยุ่นและคำนึงถึงผลประโยชน์ของทุกฝ่าย การสร้างมาตรฐานและแนวปฏิบัติร่วมกัน รวมถึงการแบ่งปันข้อมูลและทรัพยากร อาจช่วยลดความขัดแย้งและส่งเสริมการพัฒนาอธิปไตยทางดิจิทัลที่ยั่งยืน

ความท้าทายด้านทรัพยากรและขีดความสามารถ

Ruohonen (2021) ชี้ให้เห็นว่าการพัฒนาและรักษาอธิปไตยทางดิจิทัลต้องการทรัพยากรและขีดความสามารถที่สำคัญ ทั้งในด้านการเงิน บุคลากร และโครงสร้างพื้นฐาน ประเทศที่มีทรัพยากรจำกัดอาจเผชิญความท้าทายในการพัฒนาความสามารถที่จำเป็นสำหรับการรักษาอธิปไตยทางดิจิทัล โดย Bria (2015) วิเคราะห์ความสำคัญของการลงทุนในการพัฒนาทรัพยากรมนุษย์และโครงสร้างพื้นฐานดิจิทัล การสร้างความร่วมมือระหว่างภาครัฐ ภาคการศึกษา และภาคเอกชนในการพัฒนาขีดความสามารถ รวมถึงการแสวงหาความร่วมมือระหว่างประเทศในการแบ่งปันความรู้และทรัพยากร อาจช่วยลดข้อจำกัดด้านทรัพยากร และAdonis (2019) เสริมว่าการจัดลำดับความสำคัญของการลงทุนและการใช้ทรัพยากรอย่างมีประสิทธิภาพมีความสำคัญ การพัฒนาแผนยุทธศาสตร์ที่ชัดเจนและการประเมินความคุ้มค่าของการลงทุนจะช่วยให้การพัฒนาอธิปไตยทางดิจิทัลมีประสิทธิภาพภายใต้ข้อจำกัดด้านทรัพยากร

กรณีศึกษาด้านอธิปไตยทางดิจิทัล

กรณีศึกษาต่าง ๆ ในการดำเนินการด้านอธิปไตยทางดิจิทัลให้ข้อมูลเชิงลึกที่มีคุณค่าเกี่ยวกับความท้าทาย โอกาส และแนวทางปฏิบัติที่มีประสิทธิภาพ Pohle and Thiel (2020) เสนอว่าการวิเคราะห์กรณีศึกษาช่วยให้เข้าใจวิธีการที่ประเทศและภูมิภาคต่าง ๆ จัดการกับความท้าทายด้านอธิปไตยทางดิจิทัลในบริบทที่แตกต่างกัน

ยุทธศาสตร์ดิจิทัลของสหภาพยุโรป

Floridi (2020) วิเคราะห์ว่ายุทธศาสตร์ดิจิทัลของสหภาพยุโรปเป็นตัวอย่างที่น่าสนใจของการพัฒนากรอบการกำกับดูแลที่ครอบคลุม โดยเฉพาะการบูรณาการระหว่าง GDPR, Digital Markets Act (DMA) และ Digital Services Act (DSA) สหภาพยุโรปได้พัฒนาแนวทางที่เน้นการคุ้มครองสิทธิพื้นฐาน การส่งเสริมการแข่งขันที่เป็นธรรม และการรักษาอธิปไตยทางดิจิทัล สอดคล้องกับ Hoeffler and Mérand (2024) ชี้ให้เห็นว่า DMA และ DSA เป็นตัวอย่างของการกำกับ

ดูแลแบบล่วงหน้าที่มุ่งจัดการกับอำนาจตลาดของแพลตฟอร์มดิจิทัลขนาดใหญ่ กฎหมายทั้งสองฉบับสะท้อนความพยายามของสหภาพยุโรปในการสร้างสมดุลระหว่างการส่งเสริมนวัตกรรมและการปกป้องผลประโยชน์สาธารณะ และ Celeste (2021) เสริมว่าความสำเร็จของ GDPR ในการกำหนดมาตรฐานการคุ้มครองข้อมูลระดับโลกแสดงให้เห็นถึงศักยภาพของสหภาพยุโรปในการมีอิทธิพลต่อการกำกับดูแลดิจิทัลระดับโลก แม้จะเผชิญความท้าทายในการบังคับใช้ แต่ GDPR ได้กลายเป็นต้นแบบสำหรับกฎหมายคุ้มครองข้อมูลในหลายประเทศ

โครงการ Gaia-X

Autolitano and Pawlowska (2021) วิเคราะห์โครงการ Gaia-X ซึ่งเป็นความพยายามของสหภาพยุโรปในการพัฒนาโครงสร้างพื้นฐานคลาวด์ที่เป็นอิสระ โครงการนี้สะท้อนความท้าทายในการสร้างทางเลือกที่แข่งขันได้กับผู้ให้บริการคลาวด์ระดับโลก โดยเฉพาะในด้านการระดมทุน การพัฒนาเทคโนโลยี และการสร้างระบบนิเวศที่ยั่งยืน Fratini et al. (2024) ชี้ให้เห็นว่าความท้าทายของ Gaia-X รวมถึงการสร้างสมดุลระหว่างการเปิดกว้างสำหรับความร่วมมือระหว่างประเทศและการรักษาอธิปไตยทางดิจิทัล การตัดสินใจให้บริษัทเทคโนโลยีต่างชาติเข้าร่วมโครงการได้สร้างคำถามเกี่ยวกับความสามารถของโครงการในการบรรลุเป้าหมายด้านอธิปไตยทางดิจิทัล และ Sheikh (2022) เสริมว่าบทเรียนจาก Gaia-X แสดงให้เห็นความสำคัญของการมีวิสัยทัศน์ระยะยาว การสร้างพันธมิตรที่เข้มแข็ง และการพัฒนาความสามารถทางเทคนิคในการดำเนินโครงการโครงสร้างพื้นฐานดิจิทัลขนาดใหญ่

นโยบายด้าน 5G และโครงสร้างพื้นฐาน

Moerel and Timmers (2021) วิเคราะห์แนวทางที่แตกต่างกันของประเทศต่างๆ ในการจัดการกับความท้าทายด้านความมั่นคงในโครงสร้างพื้นฐาน 5G โดยเฉพาะในประเด็นเกี่ยวกับการมีส่วนร่วมของผู้ผลิตอุปกรณ์จากประเทศที่อาจมีความเสี่ยงด้านความมั่นคง การตัดสินใจของแต่ละประเทศสะท้อนการชั่งน้ำหนักระหว่างความกังวลด้านความมั่นคงและผลกระทบทางเศรษฐกิจ โดย Bellanova et al. (2022) ชี้ให้เห็นว่าการพัฒนากรอบการประเมินความเสี่ยงและมาตรการความมั่นคงสำหรับโครงสร้างพื้นฐาน 5G เป็นตัวอย่างของการสร้างสมดุลระหว่างความมั่นคงและการพัฒนาทางเศรษฐกิจ แนวทางที่ยืดหยุ่นและอิงหลักฐานช่วยให้ประเทศต่างๆ สามารถปรับนโยบายให้เหมาะสมกับบริบทของตน และ Lambach and Oppermann (2022) เสริมว่าประสบการณ์จากการพัฒนาโครงสร้างพื้นฐาน 5G แสดงให้เห็นความสำคัญของการมีกรอบการกำกับดูแลที่โปร่งใสและการสร้างความเชื่อมั่นระหว่างผู้มีส่วนได้ส่วนเสียต่าง ๆ

นโยบายการจัดเก็บข้อมูลในประเทศ

Donnelly et al. (2024) วิเคราะห์นโยบายการจัดเก็บข้อมูลในประเทศ (Data Localization) ซึ่งเป็นแนวทางที่หลายประเทศนำมาใช้เพื่อรักษาอธิปไตยทางข้อมูล โดยเฉพาะในภาคการเงินและข้อมูลส่วนบุคคล นโยบายเหล่านี้มีทั้งข้อดีในแง่การควบคุมและปกป้องข้อมูล และข้อจำกัดในด้านต้นทุนและประสิทธิภาพการดำเนินงาน โดย Glasze et al. (2023) ชี้ให้เห็นว่าการบังคับใช้นโยบายการจัดเก็บข้อมูลในประเทศมีความท้าทายหลายประการ ทั้งในด้านการกำหนดขอบเขตของข้อมูลที่ต้องจัดเก็บในประเทศ การตรวจสอบการปฏิบัติตาม และผลกระทบต่อการดำเนินธุรกิจระหว่างประเทศ ประสบการณ์จากประเทศต่าง ๆ แสดงให้เห็นความสำคัญของการออกแบบนโยบายที่สมดุลและมีความยืดหยุ่น Tan et al. (2023) เสริมว่าความสำเร็จของนโยบายการจัดเก็บข้อมูลในประเทศขึ้นอยู่กับการมีโครงสร้างพื้นฐานที่เพียงพอ กรอบกฎหมายที่ชัดเจน และการสร้างความร่วมมือกับภาคเอกชน การพิจารณาต้นทุนและผลประโยชน์อย่างรอบด้านมีความสำคัญต่อการออกแบบนโยบายที่มีประสิทธิภาพ

โครงการอธิปไตยทางคลาวด์

Lehuedé (2024) วิเคราะห์โครงการพัฒนาบริการคลาวด์ระดับชาติในประเทศต่าง ๆ ซึ่งเป็นความพยายามในการลดการพึ่งพาผู้ให้บริการต่างชาติและเพิ่มความมั่นคงของข้อมูล โครงการเหล่านี้แสดงให้เห็นทั้งโอกาสในการพัฒนาความสามารถภายในประเทศและความท้าทายในการแข่งขันกับผู้ให้บริการระดับโลก โดย Roberts (2024) ชี้ให้เห็นว่าความสำเร็จของโครงการอธิปไตยทางคลาวด์ขึ้นอยู่กับหลายปัจจัย รวมถึงการลงทุนในโครงสร้างพื้นฐาน การพัฒนาบุคลากร และการสร้างความเชื่อมั่นในบริการ ประสบการณ์จากโครงการต่าง ๆ แสดงให้เห็นความสำคัญของการมียุทธศาสตร์ระยะ

ยาวและการสร้างระบบนิเวศที่เข้มแข็ง และ Kaloudis (2021) เสริมว่าการพัฒนาบริการคลาวด์ระดับชาติควรคำนึงถึงการทำงานร่วมกับระบบนานาชาติและการรักษามาตรฐานความปลอดภัยระดับสากล การสร้างสมดุลระหว่างความเป็นอิสระและการเชื่อมโยงกับระบบโลกมีความสำคัญต่อความยั่งยืนของโครงการ

การพัฒนาระบบนิเวศดิจิทัลภายในประเทศ

Monsees and Lambach (2022) วิเคราะห์ความพยายามของประเทศต่าง ๆ ในการพัฒนาระบบนิเวศดิจิทัลภายในประเทศ ซึ่งรวมถึงการส่งเสริมผู้ประกอบการท้องถิ่น การพัฒนาแพลตฟอร์มดิจิทัลของตนเอง และการสร้างมาตรฐานและกฎระเบียบที่เหมาะสม กรณีศึกษาเหล่านี้แสดงให้เห็นความสำคัญของการมีแนวทางที่ครอบคลุมและการสนับสนุนที่ต่อเนื่อง โดย Hoeffler and Mérand (2024) ชี้ให้เห็นว่าการพัฒนาระบบนิเวศดิจิทัลที่ยั่งยืนต้องการการบูรณาการระหว่างนโยบายหลายด้าน ทั้งการศึกษา การวิจัยและพัฒนา การส่งเสริมธุรกิจ และการคุ้มครองผู้บริโภค ความสำเร็จขึ้นอยู่กับการสร้างสภาพแวดล้อมที่เอื้อต่อนวัตกรรมและการเติบโตของธุรกิจท้องถิ่น และ Chander and Sun (2021) เสริมว่าประสบการณ์จากประเทศต่างๆ แสดงให้เห็นความสำคัญของการสร้างความสมดุลระหว่างการปกป้องผู้ประกอบการในประเทศและการเปิดรับการแข่งขันจากต่างประเทศ การมีนโยบายที่ยืดหยุ่นและปรับตัวได้มีความสำคัญต่อการพัฒนาระบบนิเวศที่แข็งแกร่ง

บทสรุป

การศึกษาอธิปไตยทางดิจิทัล: การออกแบบการกำกับดูแลและธรรมาภิบาลในมิติที่หลากหลายใช้กรอบการวิเคราะห์ในมิติของอธิปไตยทางดิจิล ได้แก่ มิติด้านอธิปไตยของรัฐซึ่งเป็นบริบทดิจิทัลเกี่ยวข้องกับความสามารถของรัฐในการควบคุมและกำกับดูแลโครงสร้างพื้นฐานดิจิทัล ข้อมูล และกิจกรรมทางดิจิทัลภายในเขตอำนาจของตนมิติด้านอธิปไตยทางเศรษฐกิจในบริบทดิจิทัลเกี่ยวข้องกับความสามารถในการควบคุมและพัฒนาระบบเศรษฐกิจดิจิทัลที่เป็นอิสระมิติด้านอธิปไตยของปัจเจกบุคคลซึ่งเน้นความสำคัญของการให้อำนาจแก่พลเมืองในการควบคุมข้อมูลส่วนบุคคลและตัวตนดิจิทัลของตน การคุ้มครองสิทธิส่วนบุคคลและความเป็นส่วนตัว มิติด้านอธิปไตยทางเทคโนโลยีเกี่ยวข้องกับความสามารถในการพัฒนา ควบคุม และกำหนดมาตรฐาน มิติด้านอธิปไตยทางข้อมูลเป็นการควบคุมข้อมูลซึ่งครอบคลุมทั้งการจัดเก็บการประมวลผล และการไหลเวียนของข้อมูลข้ามพรมแดน การกำกับดูแลอธิปไตยทางดิจิทัลมีรูปแบบและแนวทางที่หลากหลาย ได้แก่ รูปแบบการกำกับดูแลที่เน้นสิทธิซึ่งให้ความสำคัญกับการคุ้มครองสิทธิพื้นฐานของพลเมืองในยุคดิจิทัล รูปแบบการกำกับดูแลที่เน้นตลาดซึ่งให้ความสำคัญกับการส่งเสริมนวัตกรรมและการแข่งขันเสรี รูปแบบการกำกับดูแลแบบรวมศูนย์ซึ่งเน้นการควบคุมโดยรัฐอย่างเข้มงวด รูปแบบการกำกับดูแลแบบผสมผสานเซึ่งเน้นการสร้างสมดุลระหว่างการควบคุมโดยรัฐ การมีส่วนร่วมของภาคเอกชน และการคุ้มครองสิทธิของพลเมือง โดยมีการกระจายอำนาจการตัดสินใจไปยังระดับต่าง ๆ ตามความเหมาะสม การออกแบบและการนำกฎระเบียบไปปฏิบัติ ได้แก่ การพัฒนากรอบการกำกับดูแลข้อมูลต้องคำนึงถึงความแตกต่างของประเภทข้อมูล เช่น ข้อมูลส่วนบุคคล ข้อมูลธุรกิจ และข้อมูลที่เกี่ยวข้องกับความมั่นคง แต่ละประเภทอาจต้องการมาตรการคุ้มครองและการกำกับดูแลที่แตกต่างกัน การมีกฎระเบียบที่เหมาะสมจะช่วยลดการพึ่งพาแพลตฟอร์มต่างชาติและส่งเสริมการพัฒนาระบบนิเวศดิจิทัลภายในประเทศ และการพัฒนาขีดความสามารถของหน่วยงานกำกับดูแลและการสร้างความเชี่ยวชาญในด้านเทคโนโลยีดิจิทัลมีความสำคัญต่อการบังคับใช้กฎระเบียบอย่างมีประสิทธิภาพ

ข้อเสนอแนะและแนวทางการแก้ไข

การพัฒนาอธิปไตยทางดิจิทัลเป็นกระบวนการที่ต่อเนื่องและต้องการการปรับตัวอย่างสม่ำเสมอ Braun and Hummel (2024) เสนอว่าการกำหนดทิศทางและข้อเสนอแนะที่ชัดเจนมีความสำคัญต่อการพัฒนานโยบายและการกำกับดูแลที่มีประสิทธิภาพในอนาคต

วิวัฒนาการของกรอบการกำกับดูแล

Pohle and Santaniello (2024) วิเคราะห์แนวโน้มการพัฒนากรอบการกำกับดูแลในอนาคต โดยเน้นความสำคัญของความยืดหยุ่นและการปรับตัวได้ กรอบการกำกับดูแลในอนาคตควรสามารถรองรับเทคโนโลยีใหม่ ๆ และรูปแบบธุรกิจที่เปลี่ยนแปลงไป โดยยังคงรักษาหลักการพื้นฐานของการคุ้มครองสิทธิและผลประโยชน์สาธารณะ โดย Falkner et al. (2024) เสนอว่าการพัฒนากรอบการกำกับดูแลควรให้ความสำคัญกับการมีส่วนร่วมของผู้มีส่วนได้ส่วนเสียและการใช้หลักฐานเชิงประจักษ์ในการกำหนดนโยบาย การสร้างกลไกการปรึกษาหารือและการประเมินผลกระทบที่มีประสิทธิภาพจะช่วยให้การพัฒนากรอบการกำกับดูแลตอบสนองต่อความต้องการที่แท้จริง และ Roberts (2024) เน้นย้ำความสำคัญของการพัฒนากรอบการกำกับดูแลที่สามารถรองรับความท้าทายระดับโลก เช่น การจัดการกับภัยคุกคามทางไซเบอร์ การคุ้มครองข้อมูลข้ามพรมแดน และการส่งเสริมนวัตกรรมดิจิทัล การสร้างความร่วมมือระหว่างประเทศในการพัฒนากรอบการกำกับดูแลจึงมีความสำคัญมากขึ้น

กลไกการประสานงานด้านนโยบาย

Moerel and Timmers (2021) วิเคราะห์ความสำคัญของการพัฒนากลไกการประสานงานด้านนโยบายที่มีประสิทธิภาพ ทั้งภายในประเทศและระหว่างประเทศ การสร้างความเชื่อมโยงระหว่างหน่วยงานที่เกี่ยวข้องและการแลกเปลี่ยนข้อมูลอย่างมีประสิทธิภาพจะช่วยเพิ่มประสิทธิภาพของการดำเนินนโยบาย โดย Lehuedé (2024) เสนอแนวทางการพัฒนากลไกการประสานงานที่เน้นความโปร่งใสและการมีส่วนร่วม โดยให้ความสำคัญกับการสร้างเวทีแลกเปลี่ยนความคิดเห็นและการพัฒนาฐานข้อมูลร่วมสำหรับการตัดสินใจเชิงนโยบาย การใช้เทคโนโลยีดิจิทัลในการสนับสนุนการประสานงานจะช่วยเพิ่มประสิทธิภาพของกระบวนการนโยบาย และ Bellanova et al. (2022) เน้นย้ำความสำคัญของการสร้างกลไกการประสานงานที่คล่องตัวและตอบสนองต่อการเปลี่ยนแปลงอย่างรวดเร็วในโลกดิจิทัล การพัฒนาระบบการแจ้งเตือนและการตอบสนองต่อความท้าทายใหม่ๆ อย่างทันท่วงทีมีความสำคัญต่อประสิทธิภาพของนโยบาย

การสร้างสมดุลระหว่างผลประโยชน์ที่แข่งขันกัน

Sheikh (2022) วิเคราะห์ความท้าทายในการสร้างสมดุลระหว่างผลประโยชน์ที่แข่งขันกันในอนาคต โดยเฉพาะระหว่างการพัฒนาเศรษฐกิจ การคุ้มครองสิทธิ และความมั่นคง การพัฒนากรอบการตัดสินใจที่โปร่งใสและเป็นระบบจะช่วยให้การสร้างสมดุลมีประสิทธิภาพมากขึ้น Donnelly et al. (2024) เสนอแนวทางการใช้การประเมินผลกระทบและการวิเคราะห์ต้นทุน-ผลประโยชน์ในการตัดสินใจเชิงนโยบาย การมีข้อมูลที่ครบถ้วนและการวิเคราะห์ที่รอบด้านจะช่วยให้การตัดสินใจมีความสมเหตุสมผลและได้รับการยอมรับจากผู้มีส่วนได้ส่วนเสีย Kaloudis (2021) เน้นย้ำความสำคัญของการสร้างกระบวนการมีส่วนร่วมที่มีความหมายในการตัดสินใจเชิงนโยบาย การรับฟังความคิดเห็นจากภาคส่วนต่าง ๆ และการสื่อสารที่มีประสิทธิภาพจะช่วยให้การสร้างสมดุลระหว่างผลประโยชน์ต่าง ๆ เป็นไปอย่างเหมาะสม

โอกาสในความร่วมมือระหว่างประเทศ

Fratini et al. (2024) วิเคราะห์โอกาสในการพัฒนาความร่วมมือระหว่างประเทศด้านอธิปไตยทางดิจิทัล การแลกเปลี่ยนประสบการณ์และแนวปฏิบัติที่ดี การพัฒนามาตรฐานร่วมกัน และการสร้างกลไกการระงับข้อพิพาทที่มีประสิทธิภาพจะช่วยส่งเสริมการพัฒนาอธิปไตยทางดิจิทัลในระดับโลก

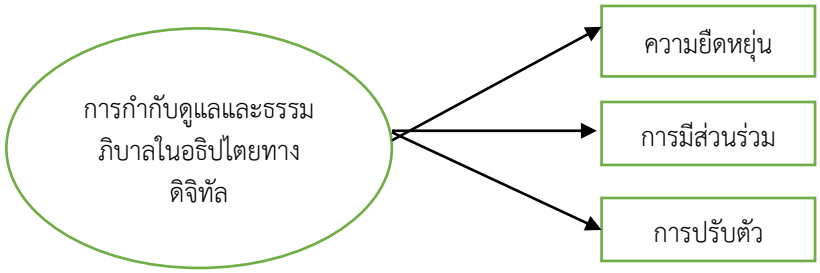
การเตรียมพร้อมสำหรับความท้าทายในอนาคต

Lambach and Oppermann (2022) เสนอว่าการเตรียมพร้อมสำหรับความท้าทายในอนาคตเป็นสิ่งสำคัญในการรักษาอธิปไตยทางดิจิทัล โดยเฉพาะการรับมือกับเทคโนโลยีที่เกิดขึ้นใหม่ เช่น ปัญญาประดิษฐ์ขั้นสูง ควอนตัมคอมพิวติง และเทคโนโลยี 6G การพัฒนาความสามารถในการคาดการณ์และการวางแผนรับมือกับความท้าทายใหม่ ๆ จึงมีความสำคัญยิ่ง โดย Ruohonen (2021) วิเคราะห์ความสำคัญของการลงทุนในการวิจัยและพัฒนา การสร้างความร่วมมือกับภาควิชาการและการพัฒนาบุคลากรที่มีความเชี่ยวชาญ การเตรียมความพร้อมด้านทรัพยากรมนุษย์และองค์ความรู้จะ ช่วยให้ประเทศสามารถรับมือกับความท้าทายในอนาคตได้อย่างมีประสิทธิภาพ และ Chander and Sun (2021) เน้นย้ำความสำคัญของ

การสร้างความยืดหยุ่นและความสามารถในการปรับตัวของระบบการกำกับดูแล การพัฒนากรอบการกำกับดูแลที่สามารถรองรับการเปลี่ยนแปลงและความไม่แน่นอนจะช่วยให้การรักษาอธิปไตยทางดิจิทัลมีความยั่งยืนในระยะยาว

องค์ความรู้ใหม่

การศึกษานี้สร้างองค์ความรู้ใหม่ที่สำคัญในการทำความเข้าใจเกี่ยวกับอธิปไตยทางดิจิทัลในการออกแบบการกำกับดูแลและธรรมาภิบาลในมิติที่หลากหลาย โดยนำเสนอองค์ความรู้ใหม่ ดังรูปที่ 1



รูปที่ 1 องค์ความรู้ใหม่ที่ได้จากการวิจัย

จากรูปที่ 1 อธิบายได้ว่า การกำกับดูแลและธรรมภิบาลในอธิปไตยทางดิจิทัล ประกอบด้วยความยืดหยุ่นเป็นความสามารถขององค์กรในการนำกลไกต่างๆ ตลอดจนการสร้างสมดุลระหว่างผลประโยชน์มาปรับใช้ได้ การมีส่วนร่วมของทุกภาคส่วนและผู้มีส่วนได้ส่วนเสียในการกำกับดูแลและธรรมาภิบาลของอธิปไตยทางดิจิทัล การปรับตัวเป็นคุณสมบัติสำคัญของรูปแบบการกำกับดูแลที่มีประสิทธิภาพ เนื่องจากเทคโนโลยีดิจิทัลมีการเปลี่ยนแปลงอย่างรวดเร็ว การปรับตัวจึงต้องกระทำอย่างสม่ำเสมอ

เอกสารอ้างอิง

Adonis, A. A. (2019). Critical engagement on digital sovereignty in international relations: Actor transformation and global hierarchy. *Global Jurnal Politik Internasional, 21*(2), 262-282. https://doi.org/10.7454/global.v21i2.412

Ali,O., & Osmanaj,V. (2020). The role of government regulations in the adoption of cloud computing: A case study of local government. *Computer Law & Security Review,36*,105396. https://doi.org/10.1016/j.clsr.2020.105396

Anthony Jnr, B. (2023). Distributed ledger and decentralised technology adoption for smart digital transition in collaborative enterprise, *Enterprise Information Systems, 17*(4), 465-498, https://doi.org/10.1080/17517575.2021.1989494

Anwar, U.A.A., Rahayu, A., Wibowo, L.A., Sultan,M.A., Aspiranti, A., Furqon, C., & Rani, A.M. (2025). Supply chain integration as the implementation of strategic management in improving business performance. *Discover Sustainability, 6*, 101. https://doi.org/10.1007/s43621-025-00867-w

Autolitano, S., & Pawlowska, A. (2021). *Europe's quest for digital sovereignty: GAIA-X as a case study*. Istituto Affari Internazionali.

Belli,L., Gaspar,W.B., & Jaswant,S.S. (2024). Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries. *Computer Law & Security Review, 54*, 106017. https://doi.org/10..1016/j.clsr.2024.106017.

Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital/sovereignty and European security *integration: An introduction. European Security*, 31(3), 337-355.https://doi.org/10.1080/09662839.2022.2101887

Braun, M., & Hummel, P. (2024). Is digital sovereignty normatively desirable? Information, *Communication & Society*, 1–14. https://doi.org/10.1080/1369118X.2024.2332624

Bria, Francesca. (2015). *Public policies for digital sovereignty*. Platform Cooperativism Consortium conference, New York. Retrieved October 26, 2024, from https://www.academia.edu/19102224/

Burri, M., & Kugler, K. (2024).Regulatory autonomy in digital trade agreements, *Journal of International Economic Law*, 27(3), 397–423, https://doi.org/10.1093/jiel/jgae025

Casaril,F. & Galletta, L. (2023). Developing security metrics for space systems: A study considering the NIST cybersecurity framework 2.0 and the NIS2. *International Journal of Critical Infrastructure Protection*, 51, 100805, https://doi.org/10.1016/j.ijcip.2025.100805

Celeste, E. (2021). Digital Sovereignty in the EU: Challenges and Future Perspectives. In F. Fabbrini, E. Celeste, & J. Quinn (Eds.), *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty* (pp. 29–82). Hart Publishing.

Chander, A., & Sun, H. (2021). *Sovereignty 2.0*. Georgetown University Law Center.

Christakis, T. (2024). Data free flow with trust: current landscape, challenges and opportunities. *Journal of Cyber Policy, 9*(1), 95–120. https://doi.org/10.1080/23738871.2024.2421838.

Donnelly, S., Ríos Camacho, E., & Heidebrecht, S. (2024). Digital sovereignty as control: The regulation of digital finance in the European Union. *Journal of European Public Policy, 3*1(8), 2226-2249. https://doi.org/10.1080/1369118X.2024.2332624

Ducato,R. (2020). Data protection, scientific research, and the role of information. *Computer Law & Security Review, 37*, 105412. https://doi.org/10.1016/j.clsr.2020.105412

Falkner, G., Heidebrecht, S., Obendiek, A., & Seidl, T. (2024). Digital sovereignty - Rhetoric and reality. *Journal of European Public Policy*, 31(8), 2099-2120. https://doi.org/10.1080/13501763.2024.2358984

Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU.
Philosophy & Technology, 33, 369-378. 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*, 3(3), 1-10 https://doi.org/10.2139/ssrn.4816020

Glasze, G., Cattaruzza, A., Douzet, F., Dammann, F., Bertran, M-G., Bômont, C., Braun, M., Danet, D., Desforges, A., Géry, A.,Grumbach, S., Hummel, P. (2023). Contested spatialities of digital sovereignty. *Geopolitics,* 28(2), 919-958. https://doi.org/10.1080/14650045.2022.2050070

Gudipati,R.R. (2025). Verifiable credentials: Transforming digital identity in the real world. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 11*(2), 684-692, https://doi.org/10.32628/CSEIT25112382.

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

Issaoui, A., Örtensjö, J. & Islam, M.S. (2023). Exploring the general data protection regulation (GDPR) compliance in cloud services: Insights from Swedish public organizations on privacy compliance. *Future Business Journal*, 9(1),107. https://doi.org/10.1186/s43093-023-00285-2

Jansen,B., Kadenko,N., Broeders,D., van Eeten,M., Borgolte,M., & Fiebig ,T. (2023). Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions. *Government Information Quarterly, 40*(4), 101862. https://doi.org/10.1016/j.giq.2023.101862.

Kaloudis, M. (2021). Digital sovereignty--European union's action plan needs a common understanding to succeed. *History Compass*, 19(12), e12698. https://doi.org/10.1111/hic3.12698

Krasyuk, I.A, Kolgan, M.V, Medvedeva,Y. (2022). Digital ecosystem structure formation depending on the archetype of distribution network participants. *European Journal of Management and Business Economics, 31*(2), 176–191,https://doi.org/10.1108/EJMBE-07-2021-0202.

Lambach, D., & Oppermann, K. (2022). Narratives of digital sovereignty in German political discourse. *Governance,* 36(3), 693-709. https://doi.org/10.1111/gove.12690

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). https://doi.org/10.1177/20539517231221778

Lemmi, L.; Puliafito, C.;Virdis, A.; Mingozzi, E. (2024). SRv6-based edge service continuity in 5G mobile networks. Future Internet, 16, 138.https://doi.org/10.3390/fi16040138

Moerel, L., & Timmers, P. (2021). *Reflections on digital sovereignty. EU Cyber Direct, Research in Focus series 2021*. Retrieved October 26, 2024, from https://ssrn.com/abstract=3772777

Monsees, L., & 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

Misraa,S., Barikb ,K., & Kvalvik,P. (2025). Digital Sovereignty in the era of industry 5.0: Challenges and opportunities. *Procedia Computer Science,254, 108*–117. https://doi.org/10.1016/j.procs.2025.02.069.

Oerlemans, J. J., & Langenhuijzen, S. (2024). Balancing national security and privacy: Examining the use of commercially available information in OSINT practices. International Journal

of Intelligence and CounterIntelligence, 38(2), 579–597. https://doi.org/10.1080/08850607.2024.2387850.

Pranith,S. (2023) Risk reporting to management on federal offers and How to navigate the conundrum?. *Journal of Economics & Management Research*, 4(6), 1-4. https://doi.org/10.47363/JESMR/2022(4)217.

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

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review, 9*(4).), 1-4. https://doi.org/10.14763/2020.4.1532

Quinn, J., & Connolly, B. (2021). Distributed ledger technology and property registers: displacement or status quo. *Law, Innovation and Technology, 13*(2), 377–397. https://doi.org/10.1080/17579961.2021.1977223

Roberts, H. (2024). Digital sovereignty and artificial intelligence: A normative approach. *Ethics and Information Technology, 26*, 70. https://doi.org/10.1007/s10676-024-09810-5

Roberts, H., Cowls, J., Casolari, F., Morley, J., Taddeo, M., & Floridi, L. (2021). Safeguarding European values with digital sovereignty: An analysis of statements and policies. *Internet Policy Review*, 10(3). https://doi.org/10.14763/2021.3.1575

Rone, J. (2024). 'The sovereign cloud' in Europe: diverging nation state preferences and disputed institutional competences in the context of limited technological capabilities. *Journal of European Public Policy, 31*(8), 2343–2369. https://doi.org/10.1080/13501763.2024.2348618

Ruohonen, J. (2021). The Treachery of Images in the Digital Sovereignty Debate. Minds and Machines, *31*(3), 439-456. https://doi.org/10.1007/s11023-021-09566-7

Sayankina, S., Tsen, E., Tan, E. W., & Ko, R. K. L. (2025). Defining the intension and extension of nations' sovereignty in the age of generative AI. *Territory, Politics, Governance*, 1–16. https://doi.org/10.1080/21622671.2025.2568474

Sheikh, H. (2022). European Digital Sovereignty: A layered approach. *Digital Society,* 1, 25 https://doi.org/10.1007/s44206-022-00025-z

Soltani, R.; Zaman, M.;Joshi, R.; Sampalli, S. (2022). Distributed ledger technologies and their applications: A Review. *Applied. Sciences. 12*, 7898. https://doi.org/10.3390/app12157898.

Spandler,K., Hartelius,J., Monti,A., & Söderbaum,F. (2024). Sovereignty scripts and regional governance: ASEAN's response to the Covid-19 pandemic, The Pacific Review, 37(3), 604-633, https://doi.org/10.1080/09512748.2023.2205164

Swire, P.,Kennedy-Mayo,D.,Bagley,D., Krasser,S.,Modak,A., & Bausewein,C. (2024). Risks to cybersecurity from data localization, organized by techniques, tactics and procedures, *Journal of Cyber Policy, 9*(1), 20-51, https://doi.org/10.1080/23738871.2024.2384724.

Tan, K. L., Chi-Hung, C., & Lam, K.-Y. (2023). Survey on digital sovereignty and identity: From digitization to digitalization. *ACM Computing Surveys*, 56(3), 61. https://doi.org/10.1145/3616400

Uršič,D. & Čater,T.(2025). Digital innovation in management and business: A comprehensive review, multi-level framework, and future research agenda, *Journal of Business Research, 197*,115475. https://doi.org/10.1016/j.jbusres.2025.115475

Zhao, X.; Zhong, B.; Cui, Z. (2023). Design of a decentralized identifier-based authentication and access control model for smart homes. *Electronics. 12*, 3334. https://doi.org/10.3390/electronics12153334.