Journal of Economics Bibliography
econsciences.com
Volume 12 June 2025 Issue 2

New Digital Work II: Digital Sovereignty of Companies and Organizations. *By* Ulrike Schmuntzsch, Alexandra Shajek, & Ernst Andreas Hartmann (Eds.), Springer 2025

By Hideo Takeo FUMIO †

Abstract. This edited volume, the second in the "New Digital Work" series, addresses the critical and rapidly evolving concept of digital sovereignty within the context of corporate and organizational structures. The book analyzes the challenges and opportunities presented by digitalization, focusing on how companies can maintain control over their data, infrastructure, and strategic development in an environment dominated by global platform providers and complex supply chains. The volume is structured around four main themes: the Fundamentals of Digital Sovereignty, Organizational Challenges, the Role of Data and Technology, and Impacts on Employees and Skills. Key chapters investigate the legal and technical requirements for achieving digital autonomy, examining topics such as open-source solutions, cloud infrastructure dependence, and data governance models. A central argument is that digital sovereignty is not merely a technical issue but a strategic prerequisite for future competitiveness and resilience. The book provides practical insights and case studies on how organizations can develop a comprehensive sovereignty strategy, addressing the necessary cultural shift, skills development (especially in IT), and the establishment of robust data control mechanisms. Ultimately, the work serves as an essential guide for managers, policymakers, and researchers seeking to navigate the strategic implications of digitalization on corporate autonomy..
Keywords. Digital Sovereignty; Corporate Digital Sovereignty; Data Governance; Digitalization; Digital Transformation; IT Infrastructure; Organizational Strategy.
JEL. D83; K15; L86; M15; O33.

Book Review

New Digital Work II: Digital Sovereignty of Companies and Organizations, edited by Ulrike Schmuntzsch, Alexandra Shajek, and Ernst Andreas Hartmann, is a timely and highly relevant compilation that meticulously explores the concept of digital sovereignty from the perspective of the private and public sector organization. Published as an open-access volume, the book serves as an essential intellectual toolkit for navigating the complex web of dependency, control, and strategy in the era of platform capitalism and pervasive digitalization. The volume moves the discussion on digital sovereignty beyond its frequent focus on the nation-state to the level of the firm, arguing that corporate autonomy over data, infrastructure, and technology is a prerequisite for competitiveness, security, and long-term resilience.

The core premise is that rapid digitalization, while offering unprecedented efficiencies, has created new forms of dependency, notably on a few dominant, non-European cloud and software providers. This reliance exposes organizations to risks related to data access, vendor lock-in, price volatility, and geopolitical influence (e.g., foreign laws governing data access). The book

† Johns Hopkins University in Baltimore, USA.

is structured to provide a comprehensive, multi-faceted analysis, dissecting the concept into its strategic, technical, legal, and human dimensions.

Part I: Conceptualizing and Defining Digital Sovereignty

The initial chapters focus on establishing a clear, actionable definition of digital sovereignty for organizations. The editors and contributors stress that sovereignty is not isolationism or autarky—an organization cannot cut itself off from global digital ecosystems—but rather the ability to act autonomously and self-determinedly within those ecosystems. This includes:

1. Data Sovereignty: Maintaining complete control over the location, access, usage, and sharing of organizational data, often linked to the legal requirements of GDPR and specific national regulations.
2. Technological Sovereignty: Having the capacity to select, adapt, or reject core software and hardware components, thereby avoiding proprietary vendor lock-in. This often involves embracing open-source solutions and modular infrastructure.
3. Strategic Sovereignty: The ability to independently define business processes and digital strategy without being dictated by the proprietary logic of external platforms or systems.

The chapters contrast the "illusion of control" often sold by Big Tech with the necessity of genuine technological self-determination. The authors argue that merely migrating to a third-party cloud is an outsourcing of dependency, not a path to sovereignty. Instead, the focus must shift to creating a strategic technology portfolio that allows for flexible switching, interoperability, and the retention of critical in-house knowledge.

Part II: Organizational and Strategic Challenges

This section explores the organizational hurdles and strategic demands of achieving digital autonomy. The core message is that digital sovereignty is a management task, not solely an IT function.

A key challenge lies in risk assessment and governance. Chapters discuss the difficulty in accurately quantifying the long-term costs and risks associated with vendor lock-in, particularly when the immediate short-term cost of adopting a proprietary platform is lower than developing an open-source alternative. This requires a cultural shift within organizations, moving from a short-sighted focus on minimizing immediate procurement costs to prioritizing strategic endurance and risk resilience.

Furthermore, the book delves into the "make or buy" dilemma in the context of digital services. While complete in-house development is often impractical, organizations must identify which components (e.g., core IP, security architecture, core data models) are sovereignty-critical and must remain under proprietary control. Case studies illustrate how companies navigate the trade-offs between leveraging global economies of scale (e.g., using hyperscale clouds) and maintaining crucial technological leverage. The conclusion is a push toward hybrid and decentralized architectures that blend public and private cloud elements, ensuring that critical data remains under the organization's jurisdiction.

Part III: The Role of Data and Technology: Tools for Autonomy

The focus here shifts to the technical enablers of digital sovereignty. The book dedicates significant attention to the potential of open-source software (OSS) and data spaces (such as the European GAIA-X initiative).

- Open-Source Solutions: OSS is highlighted as a critical tool for combating technological lock-in. By providing transparency and allowing for independent auditing and customization, open-source technology enables organizations to truly own and control their operating environment, reducing dependency on external vendors. The legal complexities of OSS licensing and implementation are also addressed, ensuring a balanced view.
- Data Spaces and Interoperability: Chapters explore new data governance models designed to facilitate data exchange while preserving data sovereignty. Initiatives like GAIA-X aim to build a decentralized, trustworthy data infrastructure where participants retain control over their data usage rights. This model contrasts sharply with the centralized, extractive model of large platform providers and is presented as a crucial mechanism for securing the economic benefits of data sharing without compromising autonomy.

The section also examines the importance of IT skills and digital literacy among employees. Sovereignty is maintained not just by technology, but by the organization's capacity to understand, maintain, and adapt that technology—a requirement that demands significant investment in in-house expertise.

Part IV: Impacts on Employees and the Future of Work

The final part examines the human element, connecting digital sovereignty to the future of work. The adoption of new technologies and sovereign infrastructure necessarily impacts organizational roles and required skills.

The book discusses how the implementation of sovereign technology affects employee trust and work routines. For instance, data governance policies must be transparent to ensure employees understand how their data is being used and that their rights are protected. Furthermore, the volume explores the need to develop a sovereignty-aware corporate culture—one where privacy, data ethics, and technological self-determination are embedded in every aspect of digital work, from product development to customer interaction. This requires new training programs and a managerial commitment to developing skills in areas like data analytics, cloud architecture, and open-source development.

Overall Assessment and Conclusion

New Digital Work II is a robust and timely academic resource. The editors have successfully curated a multidisciplinary volume that translates the abstract concept of digital sovereignty into concrete, organizational imperatives. Its primary strengths are:

1. Practical Relevance: It offers actionable policy recommendations for managers (e.g., strategic use of open source, defining sovereignty-critical assets) that move beyond mere conceptual discussion.

2. Multifaceted Analysis: By integrating technical, legal, economic, and human dimensions, the book provides a holistic view of the sovereignty challenge.
3. Focus on Autonomy: It provides a necessary counterpoint to the prevailing, often uncritical, adoption of hyperscale cloud and platform services, forcing organizations to confront the long-term risks of technological dependency.

This book is essential reading for corporate executives, IT leaders, policymakers in digital economy regulation, and scholars of business strategy and information systems. It successfully elevates digital sovereignty from a buzzword to a fundamental strategic requirement for sustained organizational performance in the contemporary global economy.