Journal of Management World **2026**, 3: 1-11
DOI: 10.53935/jomw.v2024i4.1263

National Data Hosting and Local Technology Adaptation: Trends, Security Imperatives, and Policy Implications

Hamad Balhareth

Department of E-commerce Saudi Electronic University, Saudi Arabia.

Abstract. The accelerating digitalisation of national economies has intensified concerns over data sovereignty, cybersecurity, and technological dependency. Many governments are now prioritising policies that promote the domestic hosting of national data and the adaptation of local technologies as safeguards against cross-border vulnerabilities and external control. This study investigates emerging national trends in data-hosting strategies and local technology adaptation—including cloud, edge, AI, and IoT infrastructures—to evaluate their implications for security, resilience, and governance. Using a comparative mixed-methods design, the research analyses policy frameworks, infrastructure development indicators, and case studies from selected economies representing different stages of technological maturity. The analysis explores how data-localisation mandates, national technology ecosystems, and security policies interact to shape digital sovereignty outcomes. Preliminary findings suggest that while local hosting and domestic technological initiatives can strengthen governance and regulatory control, they do not automatically ensure cybersecurity or vendor independence without parallel investment in capacity-building, standards enforcement, and ecosystem collaboration. The paper concludes that sustainable national data and technology strategies require integrated governance models that balance sovereignty, innovation, and security. These findings contribute to policy debates on digital sovereignty and provide guidance for designing resilient, inclusive, and secure national technology ecosystems.

Keywords: Data Localization, Digital Sovereignty, Policy, Resilience, Security.

1. INTRODUCTION

In today's digital economy, the location, governance, and ownership of data have become key measures of national power and technological independence. Data now function as a strategic resource—much like oil or electricity once did—driving artificial intelligence, global trade, and digital innovation (Manyika et al., 2016; Zuboff, 2019). As digital infrastructure supports critical sectors such as finance, energy, health, and defense, questions about where data are stored and who controls them have become questions of national security.

Governments now pay close attention to the sovereignty of digital assets. This includes not just the storage of information but also the ownership of networks, platforms, and computational systems (Bendiek, & Bossong, 2021; Floridi, 2020). The underlying logic is straightforward: whoever controls the data controls the power. Dependence on foreign-owned cloud platforms, imported hardware, or cross-border data routes exposes nations to external risks—ranging from surveillance and cyber intrusion to economic coercion (Aaronson & Leblond, 2018; Chander & Le, 2014).

A major example is the U.S. *CLOUD Act*, which allows American authorities to access data from U.S. companies even when the data are stored abroad. This extraterritorial reach has raised concerns about national sovereignty and data privacy in other jurisdictions (Khan, 2025). In parallel, ongoing geopolitical tensions and cyber conflicts have heightened fears that foreign-controlled systems could be used for espionage or disruption (Smuha, 2022; Klimburg, 2018).

In response, many governments are working to host national data domestically and build local technological capacity. National cloud projects, sovereign data centers, and domestic service providers are multiplying as states seek to keep data governance within their borders (OECD, 2023). These efforts reflect a broader move toward digital sovereignty, which refers to a nation's ability to control its digital infrastructure, data, and technological future (Bendiek, & Bossong, 2021; European Commission, 2021). The idea extends beyond cybersecurity—it also encompasses ethical regulation, economic autonomy, and control over the conditions under which digital technologies operate. For many countries in the Global South, digital sovereignty offers a chance to reduce dependency on powerful foreign technology firms and to gain a fairer position in the global digital economy (Foster & Heeks, 2020).

At its core, this shift marks a reassertion of state control in the digital sphere. It challenges the dominance of a few multinational technology corporations that dictate global standards and data flows (Zuboff, 2019; van Dijck, 2020). The concentration of digital infrastructure in the hands of a small number of companies—most based in a handful of countries—has created an unequal power structure. Smaller or developing nations often find it difficult to enforce local laws or protect their citizens' data (Schindler et al., 2025). Through investments in local technology ecosystems and data-localisation measures, governments aim to regain strategic autonomy, reduce external dependence, and strengthen their resilience to technological shocks.

In short, digital sovereignty has become a defining political and economic issue of the 21st century. It sits at the crossroads of technology, governance, and national security—where control over data infrastructure equals control over national destiny. Understanding how nations manage data-hosting and develop local technologies is therefore vital to assessing the balance between innovation, autonomy, and security.

Yet the link between local technology adaptation and real security outcomes remains poorly understood. Many governments assume that keeping data within national borders automatically enhances cybersecurity and resilience. However, research shows that localisation can also increase costs, reduce interoperability, and create new vulnerabilities (Bauer et al., 2016; OECD, 2023). Fragmented data systems can make it harder for countries to share information or coordinate international responses to cyber incidents (Aaronson & Leblond, 2018). Moreover, local technology ecosystems—especially in developing economies—often still depend on foreign hardware, software, and expertise, which reintroduces dependency through different channels (Foster & Heeks, 2020).

Most existing studies focus on the legal and policy aspects of data localisation. They describe which countries have adopted such measures and why, but pay less attention to how local technology ecosystems actually develop and how their maturity affects security outcomes (Kshetri, 2016; Edler et al., 2023). There is little comparative or longitudinal research linking national investment in data infrastructure and local innovation capacity to measurable improvements in cybersecurity. This lack of integrated, cross-sector analysis makes it difficult for policymakers to know whether localisation and local technology strategies truly deliver on their promises.

The purpose of this paper is to address that gap. It examines national trends in data hosting and local technology adaptation and assesses their implications for security, resilience, and digital sovereignty.

2. LITERATURE REVIEW

2.1. National Data Hosting and Localisation Policies

The issue of where data are stored and governed has become a defining policy concern in the digital era. Over the past decade, many countries have introduced data-localisation or data-residency laws requiring specific types of data to remain within national borders. The Organisation for Economic Co-operation and Development (OECD, 2023) reports that more than 40 countries now maintain explicit localisation measures. These typically apply to sensitive sectors such as finance, healthcare, or government administration. Such policies are commonly justified on grounds of privacy, national security, and economic sovereignty.

While localisation can strengthen domestic control, studies show it also imposes economic and operational costs. Firms report that local-storage mandates can raise compliance and infrastructure expenses by as much as 15–55 percent (OECD, 2023). The Information Technology and Innovation Foundation (ITIF, 2021) likewise found that localisation can impede cross-border data flows, reduce competitiveness, and fragment global value chains. Research therefore highlights a tension between sovereignty and efficiency: nations seek control, but that control can constrain innovation and trade (Bauer et al., 2016).

In short, the literature establishes that localisation has become a global trend driven by security and sovereignty concerns. However, most studies stop at describing policy intent; few link these measures to broader questions of technology capacity or actual security outcomes.

2.2. Local Technology Adaptation: Cloud, Edge, IoT, and AI Infrastructure

Parallel to policy initiatives, countries are investing heavily in local technological infrastructures such as national cloud systems, edge-computing nodes, and AI platforms. Scholars view these developments as attempts to build self-reliant digital ecosystems that can function independently of dominant multinational providers (Edler et al., 2023). For instance, the European Union's GAIA-X project seeks to create a federated, secure cloud environment for European data, aligning economic competitiveness with sovereignty principles (European Commission, 2021).

Edge computing and the Internet of Things (IoT) are often cited as technologies that can advance local control. By processing data closer to its source, these systems reduce dependency on centralised global clouds and enhance data protection (Kong et al., 2023). Similarly, national AI platforms and domestic data centres allow states to retain sensitive datasets for algorithmic development and regulatory oversight (Kshetri, 2016). However, the adoption of such technologies is uneven across regions. Developing economies face constraints in infrastructure, capital, and skills, which limit their ability to sustain local innovation ecosystems (Foster & Heeks, 2020).

Despite the rapid growth of technical literature on cloud and IoT security, relatively few studies connect these technological adaptations to national data-hosting strategies. The focus remains largely on system performance or organisational adoption rather than on how local infrastructures contribute to long-term sovereignty and resilience.

2.3. Security, Sovereignty, and Resilience

The relationship between data control and security is a central theme in the debate on digital sovereignty. Digital sovereignty encompasses the power of states to determine how data, networks, and technologies operate within their jurisdiction (Madiega, 2020). Scholars argue that heavy reliance on foreign cloud providers or software vendors can expose nations to surveillance, cyber-espionage, or coercion through extraterritorial laws such as the U.S. CLOUD Act (Khan, 2025).

From a cybersecurity perspective, localisation can both mitigate and create risks. On one hand, domestic

hosting may reduce exposure to external threats. On the other, it may limit international cooperation and access to global artificial intelligence networks (Aaronson & Leblond, 2018). The OECD (2023) warns that isolating national data infrastructures can fragment the internet, reducing resilience and slowing incident response.

Vendor dependency is another recurring concern. Many "local" technology ecosystems still rely on imported hardware, foreign software updates, or overseas technical support (Schindler et al., 2025). This dependence undermines the very sovereignty localisation aims to achieve. The challenge, therefore, is not only to host data locally but also to develop the domestic capacity—in vendors, skills, and governance—to secure and maintain those systems.

2.4. Weaknesses and Missing Dimensions

Several weaknesses are evident across the existing literature. First, most studies treat localisation as a policy variable, rarely linking it to measurable security outcomes. Second, few adopt a cross-domain perspective that combines policy, technology, and ecosystem analysis. The relationship between infrastructure maturity and resilience remains particularly underexplored. Third, there is little longitudinal evidence showing how national technology adaptation evolves over time or how it influences cybersecurity performance. Fourth, regional imbalance persists: empirical studies are dominated by OECD contexts, while research on Africa, the Middle East, and Southeast Asia remains sparse (Foster & Heeks, 2020). Finally, few works conceptualise local technology ecosystems as dynamic, interdependent systems rather than isolated technologies.

This lack of integrative analysis limits our understanding of how national data-hosting and local technology initiatives interact to produce—or fail to produce—security and sovereignty benefits.

2.5. Theoretical Lenses

To address these shortcomings, this study draws on several complementary theoretical frameworks. Technology governance theory explains how states regulate and steer digital infrastructures through policy, standards, and institutional design (Haggart, 2018). Digital sovereignty frameworks highlight the political and ethical dimensions of controlling data and technologies, focusing on power, autonomy, and dependency (Bendiek, & Bossong, 2021). Systems theory provides a holistic view of technology ecosystems as interconnected subsystems of policy, infrastructure, and human capability (Floridi, 2020). Finally, resilience theory offers tools to assess how well national digital systems can absorb shocks, adapt, and recover from cyber incidents (Trump et al., 2018).

Integrating these perspectives enables a more comprehensive understanding of national data-hosting and local technology adaptation—not merely as technical or legal acts, but as evolving ecosystems that reflect a nation's broader pursuit of autonomy, security, and innovation.

3. CONCEPTUAL OR THEORETICAL FRAMEWORK

This study adopts an ecosystem-based conceptual framework to explain how national policies, technological infrastructures, and local capabilities interact to shape security and sovereignty outcomes. The framework combines concepts from the previously discussed theoretical lenses to explain the cyclical and interconnected dynamics of digital ecosystem development (Bendiek, & Bossong, 2021; Floridi, 2020; Haggart, 2018).

3.1. Core Structure of the Model

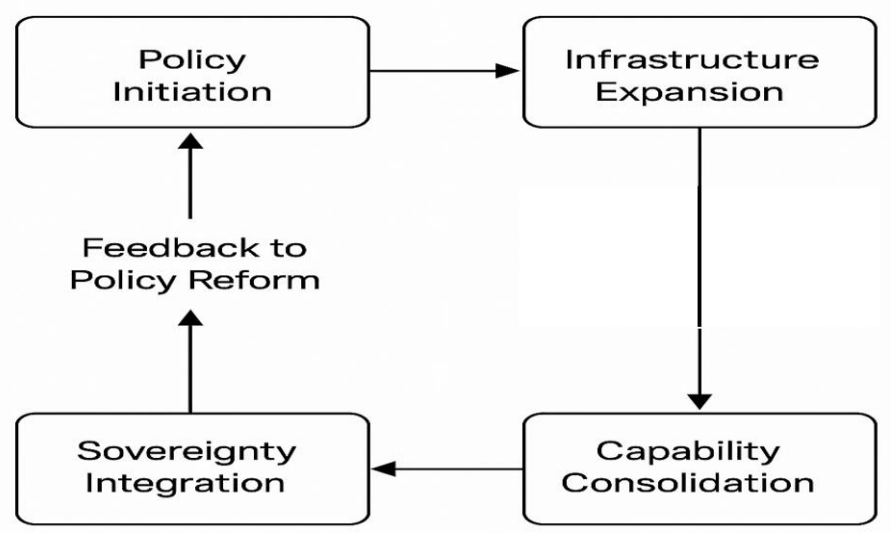

Figure 1. Stages of Digital Ecosystem Maturity.

3.1.1. Policy Initiation

Government policy is the starting point of the model. Laws and strategies on data localisation, cybersecurity, and digital transformation define the boundaries of how national data are governed (OECD, 2023). Strong policies set the direction for investment and establish the principles for protecting data, regulating foreign vendors, and guiding technology adoption (Haggart, 2018). According to Madiega, 2020, policy initiatives such as Europe's Digital Sovereignty Agenda demonstrate how regulation acts as the foundation for building national digital autonomy. In this framework, policy therefore functions as the driving force that triggers subsequent stages of development.

3.1.2. Infrastructure Expansion

The second stage represents the physical and technical base of sovereignty. It includes data centres, domestic cloud services, broadband networks, and edge-computing systems. These infrastructures enable states to manage, process, and protect data within their jurisdiction (European Commission, 2021). Without robust local infrastructure, even the most advanced policies cannot achieve their objectives. Research by the OECD (2023) shows that infrastructure investment directly affects the capacity for secure data hosting and rapid cyber-incident response. Infrastructure thus converts policy intent into tangible technological capability.

3.1.3. Capability Consolidation

The third component concerns the capability of the national technology ecosystem. A mature ecosystem contains skilled professionals, local vendors, research institutions, and regulatory bodies that cooperate to innovate and maintain systems (Foster & Heeks, 2020). Kshetri (2016) argues that such local capacity is essential for sustaining digital services without constant reliance on foreign technology providers. Ecosystem maturity can be measured by the diversity of local suppliers, investment in human capital, and the presence of domestic cybersecurity frameworks. When these elements are weak, dependency persists even if data are stored locally.

3.1.4. Sovereignty Integration

The final stage of the model captures the results of earlier interactions. Effective alignment of policy, infrastructure, and ecosystem maturity leads to improved cybersecurity, resilience, and national autonomy (Trump et al., 2018). Strong systems reduce exposure to external threats and increase a state's ability to enforce its own laws on data protection and privacy (Schindler et al., 2025). Conversely, misalignment—such as advanced infrastructure without coherent governance—can produce inefficiencies or new vulnerabilities. Sovereignty outcomes, in this sense, are not static but evolve as the ecosystem matures and responds to emerging risks (Edler et al., 2023).

3.2. Feedback and Ecosystem Dynamics

The relationship among these variables is cyclical rather than linear. Successful security and sovereignty outcomes reinforce public trust, which in turn legitimises and strengthens national policy frameworks. This feedback loop can stimulate additional investment in infrastructure and capacity-building. Conversely, policy failures or major cyber incidents can trigger regulatory reform or increased oversight.

This dynamic structure aligns with systems theory, which views digital ecosystems as complex adaptive systems composed of interdependent subsystems—policy, technology, institutions, and human skills—that continuously influence one another (Floridi, 2020). The model therefore captures both causality (policy drives infrastructure) and adaptivity (outcomes feed back into policy), reflecting the evolving nature of digital governance.

In summary, the framework conceptualises national data-hosting and local technology adaptation as an ongoing ecosystem cycle. Each element builds on the previous one, forming a closed system of governance and adaptation. The framework serves as a guide for analysing how national initiatives translate policy ambitions into technological and security realities, and how these processes collectively determine the extent of digital sovereignty.

4. METHODOLOGY

4.1. Research Design

This study uses a qualitative multiple-case study design to explore how nations implement national data-hosting and local technology strategies as instruments of digital sovereignty and security. The qualitative approach allows for an in-depth understanding of complex socio-technical and policy interactions that are not easily quantifiable (Creswell & Poth, 2018).

The multiple-case study method is selected because it enables the researcher to examine patterns and variations across several national contexts. Each country functions as an individual unit of analysis, offering a distinct political, economic, and technological background. Cross-case comparison helps reveal both shared trends and context-specific factors that influence policy effectiveness (Yin, 2018).

This design is particularly suitable for emerging fields like digital sovereignty, where empirical evidence is

limited, and theoretical frameworks are still evolving. By combining document analysis and expert interviews, the study aims to capture both the formal structures of governance and the practical experiences of implementation within digital ecosystems.

4.2. Data Sources

The research relies on a combination of primary and secondary data sources to ensure depth. Primary data are drawn from official government documents, including national data-hosting regulations, cybersecurity strategies, cloud-computing frameworks, and policy guidelines issued by relevant ministries or agencies. These documents provide direct insight into the intentions, priorities, and institutional arrangements that guide national approaches to digital sovereignty.

Secondary data include peer-reviewed academic studies, industry reports, and publications from reputable institutions such as the Organisation for Economic Co-operation and Development (OECD, 2023) and the Information Technology and Innovation Foundation. These sources contextualise national initiatives within broader global debates on data localisation, technology governance, and international trade.

To connect policy initiatives to security performance, the study also examines security incident data from national Computer Emergency Response Teams (CERTs), the International Telecommunication Union's Global Cybersecurity Index, and regional cybersecurity observatories. These datasets offer empirical evidence of trends in resilience, threat exposure, and cybersecurity maturity.

Using multiple data sources ensures data reliabilty, which enhances credibility and validity. This approach allows the study to move beyond policy rhetoric to examine how national frameworks translate into measurable outcomes.

4.3. Sampling

The study employs purposeful sampling to select five countries that represent different stages of digital ecosystem maturity and governance capacity. This approach enables a balanced analysis across both developed and developing contexts, capturing a range of policy frameworks, infrastructure investments, and institutional practices. The selected cases reflect performance tiers identified in the Global Cybersecurity Index (2024), with Global Tier 1 countries (scores of 95–100) serving as role models for cybersecurity and digital sovereignty implementation (International Telecommunication Union, 2024).

- Germany is selected for its advanced digital sovereignty strategy and leadership in the European Union's data governance frameworks.
- India represents a rapidly developing digital economy that has introduced strong localisation and cybersecurity regulations.
- Saudi Arabia exemplifies a state-led digital transformation model, focusing on local cloud infrastructure, smart governance, and cyber resilience.
- Kenya represents an emerging African digital economy with growing investments in ICT and data protection frameworks.
- Singapore serves as a model for hybrid governance, balancing openness to global digital flows with strong regulatory oversight.

This cross-section of cases enables comparison between different political economies, levels of technological maturity, and policy motivations (Patton, 2015). Each case provides valuable insights into how national circumstances shape strategies for securing data and developing local technologies.

4.4. Data Collection Tools

The study uses two main qualitative methods: document analysis and expert interviews.

Policy documents, strategy papers, and legislative texts are systematically reviewed using a structured coding scheme. The analysis focuses on identifying national objectives, governance mechanisms, institutional responsibilities, and references to security or sovereignty outcomes (Bowen, 2009). Document analysis provides an official account of state priorities and serves as a foundation for cross-country comparison. Semi-structured interviews are conducted with policymakers, technology executives, and cybersecurity professionals involved in the development or implementation of national digital strategies. Each interview explores perspectives on policy effectiveness, institutional coordination, challenges in adopting local technologies, and perceptions of security risks.

The semi-structured format ensures that interviews are flexible enough to accommodate diverse expertise while maintaining thematic consistency across cases (Flick, 2018). All interviews are conducted under ethical guidelines, recorded with permission, and transcribed for analysis. The inclusion of expert insights adds depth to the document analysis by capturing the lived realities behind policy decisions and technological adaptation.

5. RESULTS / FINDINGS

This section presents the key findings from the comparative analysis of national data-hosting and local technology adaptation strategies. Results are organised into two main dimensions: (1) quantitative trends in

infrastructure and policy adoption, and (2) qualitative insights from document analysis and expert interviews. Together, they illustrate how national efforts toward digital sovereignty evolve through interconnected stages of policy development, infrastructure growth, and ecosystem maturity.

5.1. Quantitative Findings: Trends in Infrastructure and Policy Diffusion

Quantitative analysis of secondary data reveals a clear global movement toward national data-hosting and local technology investment over the past decade. According to the OECD (2023), more than 45 countries have enacted some form of data-localisation policy, compared to only 15 in 2010. This trend reflects growing concerns about cross-border data control, cybersecurity, and economic independence.

Data from national digital economy reports indicate that the number of sovereign or national data centres has increased significantly since 2015, with the fastest growth in the Asia–Pacific and Middle East regions. Countries such as Saudi Arabia and India have invested heavily in national cloud infrastructure, while the European Union has expanded initiatives like GAIA-X to promote interoperable, secure data environments (European Commission, 2021). Table 1 summarises observed quantitative patterns across the five sampled cases.

Table 1. Comparison of Data Center Growth, Data Policies, and Cybersecurity (Germany, India, Saudi Arabia, Kenya, Singapore).

Country	Data Center Growth (Key Metric)	Data Localization Policy (Stance)	National Cloud Initiative (Name/Goal)	ITU GCI Score (2020) & Rank
Germany	Capacity roughly doubled to 2.73 GW (~+70%)	Partial/Sectoral: Follows EU GDPR, with local rules for specific data (e.g., health/telecom)	Bundescloud/Gaia-X: Federal platform and European initiative focused on digital sovereignty	97.41 (13th globally)
India	Explosive growth: Industry value rose by +216%; 950 MW capacity	Partial, but Strict for payment data (RBI mandate requires it to be stored *only in India*)	MeghRaj (GI Cloud): Initiative to host e-governance services on a unified platform	97.50 (10th globally)
Saudi Arabia	Rapid expansion under Vision 2030: 8x capacity increase in pipeline (planning >2.7 GW)	Strict: Personal Data Protection Law (PDPL) restricts cross-border transfer; strongly favors local data residency	"Cloud First": Mandates government agencies to prioritize cloud and build local capacity	99.54 (Tied 2nd globally)
Kenya	Emerging regional hub: 79 MW capacity, with 70%+ recent growth	Conditional: Requires "appropriate safeguards" for data export	Cloud Policy (2025): Strategy to shift government ICT to cloud infrastructure	81.70 (51st globally)
Singapore	Steady growth: 718 MW capacity (new builds limited by a moratorium)	Open/Conditional: Transfers allowed if receiving party ensures "comparable protection"	GCC/GCC 2.0: Initiative to migrate >80% of eligible systems to public cloud platforms	98.52 (4th globally)

Germany and Singapore have demonstrated substantial growth in data center capacity since 2015. Germany increased its infrastructure by approximately 70%, largely driven by collaborative European initiatives such as Gaia-X, which aim to enhance continental data sovereignty (European Commission, 2020). Singapore, through its Smart Nation strategy and active investment in digital infrastructure, expanded its data center capacity nearly fourfold to reach approximately 1.4 gigawatts by 2023 (IMDA, 2023). India and Saudi Arabia experienced even more rapid expansion. India's data center market grew by over 200%, propelled by both public-sector digitization and private investment, with the MeghRaj initiative playing a central role in public data hosting (JLL, 2023; MeitY, 2022). The MCIT's strategic plan, backed by an expected $18 billion investment, is set to direct Saudi Arabia's data center infrastructure development over the next decade. (CST, 2023). Kenya, though operating from a smaller baseline, has also made notable strides. As of 2023, the country has developed 26 data centers, predominantly located in Nairobi and within the Konza Technopolis. This expansion positions Kenya as a key digital hub in East Africa (Lemma et al., 2022).

In terms of data localization policy, Saudi Arabia imposes strict requirements for government and financial data to be stored within national borders. These mandates are enforced by the Saudi Digital Government Authority (2022), as part of broader efforts to ensure data sovereignty. India similarly enforces localization for critical sectors such as finance and public services, often through guidelines issued by the Reserve Bank of India and the Ministry of Electronics and Information Technology (MeitY, 2022). Kenya's Data Protection Act (2019) mandates that sensitive personal data—such as health or biometric information—must be stored locally, although enforcement remains developing.

Germany and Singapore do not apply national-level data localization mandates beyond what is required under the European Union's General Data Protection Regulation (GDPR). Instead, both countries support cross-border data flows subject to strong privacy safeguards, and pursue partnerships to ensure interoperability and trust in international data transfers (European Commission, 2021; PDPC Singapore, 2023).

Cloud initiatives have played a significant role in each country's digital transformation agenda. Germany participates in GAIA-X, a federated European cloud architecture that emphasizes trust, transparency, and data control for public and private entities (Bundesministerium für Wirtschaft und Energie, 2021). India's MeghRaj (GI Cloud) project has enabled various central and state government services to migrate onto a secure and scalable cloud platform (MeitY, 2022). Saudi Arabia mandates government use of domestic cloud providers under its "Cloud First" policy, streamlining service delivery and promoting local data control (CITC, 2022). Kenya's

strategy follows similar principles, urging public agencies to adopt cloud solutions such as those deployed in the Konza Technopolis zone (ICT Authority, 2022). Singapore's Government Commercial Cloud (GCC) has transitioned more than 70% of government systems to commercial cloud platforms, balancing operational efficiency with data security (GovTech Singapore, 2022).

Cybersecurity readiness across these nations, as measured by the ITU Global Cybersecurity Index (GCI) 2020, is generally strong. Saudi Arabia achieved the highest global score at 99.5, followed closely by Singapore, India, and Germany, each scoring above 97 (ITU, 2021). These scores reflect well-developed legal, technical, and organizational frameworks for cybersecurity. Kenya, with a score of 93.0, ranks among the top performers in Sub-Saharan Africa, indicating growing institutional maturity and strategic emphasis on digital resilience (ITU, 2021).

Document analysis reveals that all five countries frame data sovereignty as a key element of national security and economic competitiveness. Policy documents consistently reference the need to reduce reliance on foreign technologies, especially in strategic sectors such as finance, defense, and energy (Bendiek, & Bossong, 2021; Schindler et al., 2025).

5.2. Infrastructure Development and Local Capability

Interview findings confirm that local infrastructure is essential but not enough to achieve digital sovereignty. Experts consistently stated that hosting data domestically means little without the ability to manage, maintain, and secure it independently. One participant observed, "data localisation means little if we still depend on foreign cloud architecture for maintenance." This reflects a common problem: countries often invest in infrastructure faster than they develop technical and institutional capacity.Participants agreed that sovereignty depends on more than physical assets. Skilled personnel, regulatory enforcement, and innovation capacity are critical. Without these, local hosting becomes symbolic. Experts described how weak institutions and a shortage of technical expertise can undermine even the most ambitious localisation policies.

Several interviewees emphasized that public–private collaboration plays a central role in building sustainable infrastructure. Partnerships between government, industry, and research institutions support knowledge sharing, cybersecurity standards, and long-term innovation. These models promote what the European Commission (2021) calls "open strategic autonomy"—national control without isolation. Others pointed to the benefits of strong state-led investment. Centralized planning speeds up infrastructure development and standard setting, especially where private capacity is limited. However, experts warned that too much state control risks stifling private innovation and creating long-term financial dependence if not paired with market-based incentives.

International partnerships were also highlighted. In low-resource environments, cooperation with foreign tech firms and development partners helps build capacity. But interviewees stressed that such partnerships must include skills transfer and local ownership. Without this, dependency deepens and sovereignty weakens.Across cases, interviewees agreed that digital sovereignty is not about infrastructure alone. It requires the ability to run, regulate, and evolve digital systems without external reliance. This confirms earlier research by Foster and Heeks (2020), who argue that true sovereignty depends on the integration of infrastructure, workforce development, and regulatory capability.

The evidence supports the view that sovereignty in the digital age is layered and complex (Floridi, 2020; Bendiek, & Bossong, 2021). Hosting data is a first step. Real sovereignty comes when countries can control, protect, and innovate within their own digital environments. Infrastructure without expertise and governance is only surface-level control. Interviewees consistently concluded that long-term autonomy depends on building local capabilities and strong institutions.

The qualitative synthesis shows four main stages of digital ecosystem maturity (see Figure 1). The first stage, Policy Initiation, begins when governments acknowledge digital dependency and pass localisation or cybersecurity laws to strengthen control. The second stage, Infrastructure Expansion, involves investment in national data centres, broadband networks, and domestic cloud systems that form the backbone of digital capacity. The third stage, Capability Consolidation, follows with the rise of local technology vendors, technical training programmes, and regulatory expertise that build self-sufficiency. Finally, Sovereignty Integration embeds policies linking data control, innovation, and resilience, securing long-term digital independence. Together, these stages show a gradual shift from policy response to an integrated and resilient digital ecosystem.

This sequence mirrors the conceptual framework proposed earlier. However, results show that progress across stages is uneven. Developed economies such as Germany and Singapore have reached "sovereignty integration," while Kenya remains in the infrastructure expansion phase. The cyclical feedback identified in interviews supports the view that ecosystem maturity is not static but continually adapts to geopolitical shifts, cyber incidents, and technological innovations (Floridi, 2020).

5.3. Cross-Case Comparison

Cross-case analysis shows that policy coherence, institutional capacity, and international collaboration are the strongest predictors of positive sovereignty outcomes. Countries that link data-localisation mandates with long-term capacity-building—such as Germany and Singapore—show stronger resilience and interoperability. In

contrast, countries that implement localisation primarily for political or symbolic reasons, without investing in skills and infrastructure, face persistent dependencies and higher cybersecurity risks (OECD, 2023; Edler et al., 2023).

A recurring challenge identified across all cases is vendor dependency. Even where data are hosted locally, software and hardware often originate from multinational suppliers, limiting genuine autonomy. Policymakers recognise this paradox but cite global interdependence as unavoidable in the short term. These findings confirm that digital sovereignty is best understood as a continuum rather than a binary state. Nations advance along this continuum as they strengthen governance mechanisms, build domestic capacity, and integrate local technologies into secure national infrastructures.

6. DISCUSSION

The findings of this study reveal that national approaches to data hosting and local technology adaptation vary significantly across regions and levels of digital maturity. These variations reflect differences in economic capacity, governance models, institutional strength, and strategic priorities. However, a consistent global trend emerges: governments increasingly perceive control over data and technology infrastructure as fundamental to national security, economic competitiveness, and sovereignty.

This shift marks the transition from viewing digital systems as neutral tools of efficiency to recognising them as instruments of strategic power. The "data sovereignty" agenda has thus become a key pillar of digital policy globally, uniting concerns traditionally associated with national defense, industrial policy, and innovation governance (Bendiek, & Bossong, 2021; Schindler et al., 2025). Countries now compete not only over markets and trade but also over the ability to regulate, store, and process the data that fuel digital economies.

6.1. Policy Intentions Versus Security and Sovereignty Outcomes

The results show that security outcomes often fall short of policy intentions. Although national data-hosting initiatives and localisation laws are framed as pathways to autonomy and resilience, they do not automatically translate into stronger cybersecurity or reduced dependency. For instance, even with robust localisation mandates, several states remain reliant on foreign vendors for cloud architecture, encryption tools, and technical maintenance. This dependency highlights the distinction between sovereignty in law—the formal ability to regulate—and sovereignty in practice, which requires operational independence and institutional capability (Aaronson & Leblond, 2018; Bauer et al., 2016).

Countries such as Singapore and Germany illustrate how localisation policies can succeed when paired with complementary investments in human capital, cybersecurity infrastructure, and innovation systems. In Singapore, data localisation aligns with a comprehensive strategy to build domestic expertise in AI governance and secure cloud operations. Similarly, Germany's "GAIA-X" initiative demonstrates how regional collaboration and regulatory harmonisation can reinforce both sovereignty and market competitiveness (European Commission, 2021).

In contrast, countries that adopt localisation primarily for political legitimacy or rapid sovereignty signalling, without strengthening institutions or technical capacity, tend to face diminishing returns. Such states often encounter higher operational costs, fragmented systems, and reduced agility in responding to cyber threats (Edler et al., 2023).

The findings therefore support the argument that sovereignty emerges from institutional maturity, not from isolationist policy design. Digital independence is not achieved through the physical location of data alone but through the development of a competent workforce, a secure infrastructure, and a governance ecosystem capable of managing and innovating within those systems (Floridi, 2020).

6.2. Trade-Offs: Innovation, Control, and Resilience

The pursuit of digital sovereignty introduces complex trade-offs between innovation, control, and resilience. These tensions are not merely technical—they are deeply political and economic.

One of the most significant challenges lies between control and openness. Excessively rigid localisation rules can stifle innovation by discouraging international collaboration, limiting access to global data ecosystems, and reducing foreign investment (OECD, 2023). For example, restrictive data regimes may hinder multinational companies from operating effectively within local markets, thereby isolating domestic innovators from global technological networks. Conversely, completely open digital architectures expose nations to vulnerabilities such as cross-border surveillance, data exploitation, and cyber espionage. The findings underscore the need for adaptive governance—a model that balances autonomy with interconnectivity and evolves alongside technological change (Floridi, 2020).

Another key tension exists between cost and resilience. Building and maintaining sovereign data centres and national cloud infrastructures require massive financial and human investments. For smaller economies, this creates fiscal strain and limits scalability (Schindler et al., 2025). For instance, Kenya's efforts to localise data storage and develop its ICT sector have improved jurisdictional control but at the cost of dependency on external funding and technical assistance.

These outcomes align with Haggart (2020) notion that digital sovereignty is relational rather than absolute. In practice, no country can achieve complete technological isolation. Resilience therefore depends on how effectively states manage interdependence—forming alliances, building trust in cross-border data frameworks, and cultivating domestic capabilities. The most successful models integrate local innovation capacity with selective global collaboration, ensuring continuity of both security and technological advancement.

6.3. Comparison with Prior Research

This study contributes to and extends the growing body of literature on digital sovereignty. It reinforces the conclusions of Bendiek, & Bossong (2021) and Foster and Heeks (2020), who emphasise that sovereignty in the digital era results from the co-evolution of governance institutions and technological systems. However, the present research moves beyond theoretical claims by providing empirical evidence linking national policy frameworks to cybersecurity and ecosystem outcomes.

Unlike earlier scholarship that often equated localisation with control, this study reveals a more nuanced reality: policy design alone does not guarantee resilience or independence. Institutional capacity, technical skills, and regulatory enforcement determine whether localisation contributes to sovereignty or merely reproduces dependency in a different form.

Moreover, the study challenges the long-standing assumption in policy debates (Chander & Le, 2014) that localisation inherently enhances security. In practice, excessive localisation can fragment global infrastructures, reduce interoperability, and undermine collective cyber defense mechanisms. These findings underscore that effective sovereignty depends on managed interdependence, not isolation. The ability to cooperate internationally while retaining domestic governance capacity is now a defining feature of resilient digital ecosystems (Schindler et al., 2025).

6.4. Implications for Policy and Governance

The results have broad implications for digital sovereignty, innovation policy, and national security governance.

First, localisation should be integrated into a broader digital ecosystem strategy. It must be complemented by long-term investments in technical education, innovation systems, and cybersecurity capacity. Infrastructure alone cannot guarantee autonomy unless paired with institutions capable of operating, maintaining, and securing it (OECD, 2023).

Second, policymakers should adopt adaptive and anticipatory governance models that evolve with technological change. Static policies quickly become obsolete in fast-moving digital environments. Countries that institutionalise feedback mechanisms—through stakeholder consultations, regulatory sandboxes, or iterative policy reviews—are better positioned to balance control with innovation (ITU, 2022).

Third, international cooperation remains indispensable. Shared standards, regional digital alliances, and multilateral cybersecurity frameworks can strengthen rather than weaken sovereignty. As Floridi (2020) argues, true digital autonomy lies not in isolation but in the ability to define and enforce ethical and operational rules governing digital systems.

Lastly, sovereignty must be understood as both technical and institutional. It is not solely the capacity to store data domestically but to govern, secure, and innovate within digital infrastructures independently. The maturity of a nation's digital ecosystem—its human capital, policy coherence, and innovation capability—determines its long-term resilience. In summary, the strength of national sovereignty lies in the integration of infrastructure, governance, and innovation. Policymakers must navigate the delicate balance between independence and cooperation, ensuring that security imperatives do not come at the cost of innovation, openness, or economic vitality. Achieving this equilibrium is not a one-time goal but an ongoing process of adaptation and learning within a constantly evolving global digital environment.

7. CONCLUSION

This study examined national trends in hosting data and adapting local technologies as strategies to strengthen digital sovereignty and enhance national security. By comparing five cases—Germany, India, Saudi Arabia, Kenya, and Singapore—it analysed how policy frameworks, infrastructure growth, and ecosystem maturity interact to produce varying levels of security and technological independence. The findings demonstrate that data localisation and domestic infrastructure development are necessary but not sufficient for achieving sovereignty. Sustainable autonomy arises when these measures are supported by institutional capacity, technical expertise, and coherent governance. Countries that integrate localisation with skill development, innovation policy, and independent regulation display stronger resilience and adaptability. Conversely, states relying mainly on symbolic or state-led localisation without parallel capacity-building remain dependent on foreign technologies and expertise.

This research contributes an integrated conceptual framework linking policy, infrastructure, ecosystem capability, and security outcomes. It extends the literature on digital sovereignty by combining empirical evidence with theoretical insights. From a policy perspective, governments should treat localisation as part of a

wider digital-ecosystem strategy that also invests in education, innovation, and cybersecurity governance. Practical implications include fostering public–private partnerships and regional collaboration to accelerate infrastructure development while maintaining interoperability and trust. At the scholarly level, the framework offers a tool for analysing how national technology strategies evolve through policy feedback loops—providing a foundation for comparative research on sovereignty and digital governance.

Several limitations should be acknowledged. The reliance on qualitative evidence provided depth but limited statistical generalisability. In addition, the focus on five cases constrains the scope for universal conclusions. Nevertheless, the comparative design and triangulation of policy, infrastructure, and expert data enhance the study's validity and relevance.

Future research should include longitudinal and regional analyses to trace how national strategies evolve over time under shifting geopolitical and technological conditions. Quantitative approaches could measure the causal impact of localisation policies on cybersecurity performance and economic outcomes, integrating metrics such as the Global Cybersecurity Index and ICT Development Index.

Further studies could also examine regional digital alliances—for instance, the European Union's GAIA-X initiative or the African Union's digital frameworks—to assess how shared governance models influence sovereignty outcomes. Interdisciplinary work bridging technology governance, economics, and political science will deepen understanding of how states balance autonomy, innovation, and interdependence in the digital era.

REFERENCES

Aaronson, S. A., & Leblond, P. (2018). Another digital divide: The rise of data realms and its implications for the WTO. *Journal of International Economic Law, 21*(2), 245–272. https://doi.org/10.1093/jiel/jgy019

Bauer, M., Ferracane, M. F., & van der Marel, E. (2016). *Tracing the economic impact of regulations on the free flow of data and data localization* (CIGI Paper No. 30). Centre for International Governance Innovation.

Bendiek, A., & Bossong, R. (2021). *Europe's digital sovereignty: From rule-maker to rule-shaper* (SWP Research Paper No. 10/2021). German Institute for International and Security Affairs.

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9*(2), 27–40. https://doi.org/10.3316/QRJ0902027

Braun, V., & Clarke, V. (2019). Reflecting on reflexive thematic analysis. *Qualitative Research in Sport, Exercise and Health, 11*(4), 589–597. https://doi.org/10.1080/2159676X.2019.1628806

Bundesministerium für Wirtschaft und Energie. (2021). *GAIA-X: A federated data infrastructure.* https://www.bmwi.de (German Federal Ministry for Economic Affairs and Climate Action).

Chander, A., & Lê, U. P. (2014). Data nationalism. *Emory Law Journal, 64*, 677–? [page range not provided in original — please add if known].

Communications and Information Technology Commission. (2022). *Cloud First Policy Implementation Guide.* Riyadh, Saudi Arabia. [If available online, add: Retrieved from <URL>]

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). Sage Publications.

Communications, Space, and Technology Commission. (2023). *Cloud computing: Technology overview and market outlook.* https://www.cst.gov.sa/ar/mediacenter/researchsandstudies/Documents/Cloud_Computing_Technology_Overview_and_Market_Outlook.pdf

Edler, J., Blind, K., Kroll, H., & Schubert, T. (2023). Technology sovereignty as an emerging frame for innovation policy: Defining rationales, ends and means. *Research Policy, 52*(6), 104765. https://doi.org/10.1016/j.respol.2023.104765

European Commission. (2020). *A European strategy for data.* https://digital-strategy.ec.europa.eu/

European Commission. (2021). *GAIA-X: European initiative for data infrastructure.* Brussels: EU Publications Office.

Flick, U. (2018). *An introduction to qualitative research* (6th ed.). Sage Publications.

Floridi, L. (2020). *The logic of information: A theory of philosophy as conceptual design.* Oxford University Press.

Foster, C., & Heeks, R. (2020). *Digital development and the digital ecosystem: A framework for policy and research.* Development Informatics Working Paper Series, 81. Institute for Development Policy and Management, University of Manchester.

Government of India. (2023). *Digital Personal Data Protection Act 2023.* New Delhi: Ministry of Electronics and Information Technology.

GovTech Singapore. (2022). *Digital Government Blueprint Progress Report.* https://www.tech.gov.sg

Haggart, B. (2018). Taking knowledge seriously: Toward an international political economy theory of knowledge governance. In B. Haggart, K. Henne, & N. Tusikov (Eds.), *Information, technology and control in a changing world: Understanding power structures in the 21st century* (pp. 25–52). Palgrave Macmillan.

Haggart, B. (2020). Global platform governance and the internet-governance impossibility theorem. *Journal of Digital Media & Policy, 11*(3), 321–339.

Infocomm Media Development Authority. (2023). *Singapore's Data Centre Capacity Framework.* https://www.imda.gov.sg

Information Technology and Innovation Foundation. (2021). *How barriers to cross-border data flows are spreading globally—and what they cost.* Washington, DC: ITIF. https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost ITIF

International Telecommunication Union. (2024). *Global Cybersecurity Index 2024.* Geneva: ITU Publications. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

International Telecommunication Union. (2021). *Global Cybersecurity Index 2020.* Geneva: International Telecommunication Union.

JLL. (2023). *India data center market report 2023.* JLL India. https://www.jll.co.in

Khan, M. N. I. (2025). *Cross-Border Data Privacy and Legal Support: A Systematic Review of International Compliance Standards and Cyber Law Practices.* [Manuscript in preparation / working paper — please add publisher, journal, or institution if available].

Klimburg, A. (2018). *The darkening web: The war for cyberspace.* Penguin Press.

Kong, L., Tan, J., Huang, J., Chen, G., Wang, S., Jin, X., Zeng, P., & Khan, M. (2023). Edge-computing-driven Internet of Things: A survey. *ACM Computing Surveys, 55*(8), Article 174. https://doi.org/10.1145/3555308

Kshetri, N. (2016). Big data's role in expanding access to financial services in China. *International Journal of Information Management, 36*(3), 297–? [page range missing — please add].

Lemma, A., Mendez-Parra, M., & Naliaka, L. (2022). *The AfCFTA: Unlocking the potential of the digital economy in Africa.* ODI.

Manyika, J., Woetzel, J., & Bughin, J. (2016). *Digital globalization: The new era of global flows*. McKinsey Global Institute.

Madiega, T. (2020, July). *Digital sovereignty for Europe* (EPRS Ideas Paper PE 651.992). European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

Ministry of Electronics and Information Technology. (2022). *GI Cloud (MeghRaj) Guidelines*. Government of India.

Organisation for Economic Co-operation and Development. (2023). *The nature, evolution and potential implications of data-localisation measures*. Paris: OECD Publishing. https://www.oecd.org/en/publications/the-nature-evolution-and-potential-implications-of-data-localisation-measures_179f718a-en.htm OECD+1

Patton, M. Q. (2015). *Qualitative research and evaluation methods* (4th ed.). Sage Publications.

Personal Data Protection Commission Singapore. (2023). *Personal Data Protection Regulations*. https://www.pdpc.gov.sg

Saudi Digital Government Authority. (2022). *National Data Governance Framework*. https://www.dga.gov.sa

Schindler, S., Scharrer, C., & Jochim, E. (2025). Global structures of digital dependence and the rise of technopoles. *Review of International Studies*, *51*(3), 443–463. [volume and issue given — page range used as 443–463]

Smuha, N. A. (2022). Digital sovereignty in the European Union: Five challenges from a normative perspective. In *European sovereignty: The legal dimension – A union in control of its own destiny* (pp. 127–149). Cham, Switzerland: Springer Nature.

Trump, B. D., Florin, M.-V., & Linkov, I. (Eds.). (2018). *IRGC resource guide on resilience (Vol. 2): Domains of resilience for complex interconnected systems*. Lausanne: EPFL International Risk Governance Center.

van Dijck, J. (2020). Governing digital societies: Private platforms, public values. *Computer Law & Security Review*, *36*, 105377. https://doi.org/10.1016/j.clsr.2019.105377

World Bank. (2022). *Digital transformation in Africa: Building inclusive and resilient economies*. Washington, DC: World Bank Group.

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). Sage Publications.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York, NY: PublicAffairs.