Global Approaches to Digital Sovereignty: Legal Mechanisms for Managing Data and Digital Infrastructure

1. Elizabeth Harper: Department of Law, University of Edinburgh, Edinburgh, UK
2. James Millard*: Department of Law, University of Edinburgh, Edinburgh, UK

*Correspondence: e-mail: Jamesjmillarduk@gmail.com

Abstract

The rapid evolution of digital technologies and the increasing interconnectedness of global markets have raised significant concerns regarding digital sovereignty. Digital sovereignty refers to the control that nations assert over their digital infrastructures, including data governance, privacy protection, and cybersecurity. As the digital economy continues to expand, countries are seeking ways to manage their digital resources while balancing national interests with the demands of international cooperation. This narrative review explores the legal frameworks employed by various regions and countries in managing data sovereignty, highlighting both opportunities and challenges. The review examines key mechanisms such as data localization laws, cross-border data flows, and privacy protection regulations, with a focus on prominent jurisdictions such as the European Union, the United States, and China. It also investigates the role of emerging technologies like blockchain and artificial intelligence in shaping digital sovereignty policies. Furthermore, the review discusses the global challenges faced by nations in asserting digital sovereignty, including jurisdictional conflicts, cybersecurity concerns, and the influence of global tech giants. In conclusion, the review provides recommendations for policymakers on how to balance national control with international collaboration in the digital age. Key recommendations include the need for adaptable legal frameworks, enhanced cybersecurity measures, and multilateral cooperation on global digital governance standards. As digital sovereignty continues to evolve, it is crucial for countries to engage in international dialogues and develop harmonized regulations that promote both national security and global digital cooperation.

Keywords: digital sovereignty, data localization, cross-border data flows, privacy protection, blockchain, artificial intelligence

Received: 17 August 2024
Revised: 11 September 2024
Accepted: 24 September 2024
Published: 01 October 2024

Citation: Harper, E. & Millard, J. (2024). Global Approaches to Digital Sovereignty: Legal Mechanisms for Managing Data and Digital Infrastructure. *Legal Studies in Digital Age*, 3(4), 36-46.

1. Introduction

Digital sovereignty refers to the control that a state exercises over the data, infrastructure, and technologies that pertain to its citizens, institutions, and borders within the increasingly interconnected global digital landscape. This concept has emerged as a critical aspect of modern governance due to the profound influence of digital technologies, which have reshaped not only how information flows but also how states interact with and regulate that information. As digital technologies advance rapidly, from cloud computing to artificial intelligence and blockchain, the need for countries to assert sovereignty over their digital environments has intensified. The surge in data generation, the growing power of tech corporations, and the increasing risks

associated with cyber threats have all prompted a reevaluation of national control over digital resources. The growing significance of data as a central asset in the global economy, as well as its potential to influence political, economic, and social power, further underscores the importance of digital sovereignty. States are now more concerned about data protection, surveillance, cyber-attacks, and the influence of foreign tech companies than ever before, driving legal and policy innovations in the realm of digital sovereignty (Zamani, 2017).

The relevance of digital sovereignty in the modern world cannot be overstated, particularly in the context of global governance and the rapid digital transformation of societies. As states grapple with balancing economic development through technology and safeguarding national security, the concept of digital sovereignty has become a key focus of policy and legal discussions. In an era dominated by interconnected digital networks, where data flows freely across borders, questions of jurisdiction, ownership, and control of data have become critical. Governments are increasingly called upon to protect the rights of their citizens, ensure the security of their digital infrastructure, and prevent the undue influence of foreign entities over domestic affairs (Jalili et al., 2024). Furthermore, the rise of global platforms and corporations that dominate the digital economy has raised concerns about the concentration of power in the hands of a few multinational entities, prompting calls for stronger legal mechanisms to ensure that sovereign rights are not undermined by external forces (Pourkhaghan et al., 2019).

The purpose of this review is to critically analyze the global approaches to digital sovereignty, focusing on the legal mechanisms that countries have developed to manage their data and digital infrastructure. This article will examine the intersection of technology and law, exploring the various ways in which different countries have responded to the challenges posed by digital sovereignty. The review will cover a range of approaches from major jurisdictions, such as the European Union, the United States, and China, as well as emerging strategies from countries in the Global South. By examining these diverse legal frameworks, the review aims to identify common themes, unique solutions, and ongoing challenges in the management of data sovereignty and digital infrastructure. The review will also discuss the broader implications of these legal mechanisms for international relations, trade, and privacy protection in the digital age (Sadat Bidgoli, 2023).

This narrative review employs a descriptive analysis method to explore the evolving legal frameworks surrounding digital sovereignty. The primary goal of the review is to present a comprehensive understanding of how different legal systems are adapting to the challenges posed by technological advancements in data management and infrastructure control. Through the examination of academic literature, legal documents, and case studies from various regions, this article will highlight the diversity of approaches adopted by states while also identifying commonalities and areas of convergence. The review method allows for an in-depth examination of both theoretical and practical aspects of digital sovereignty, providing readers with a nuanced understanding of how countries are navigating the intersection of law, technology, and national security (Crum & Merlo, 2020).

2. Conceptual Framework of Digital Sovereignty

Digital sovereignty is a multi-faceted concept that encompasses several dimensions of control, governance, and protection of digital resources within a nation's borders. At its core, digital sovereignty involves a state's right to govern the flow of data, regulate digital infrastructures, and assert authority over the technological systems that shape its economic, political, and social environments. One of the key aspects of digital sovereignty is data control. In the digital age, data has become a critical asset that shapes not only economic outcomes but also political and social power. The ability to control and protect data within a nation's borders is seen as an essential component of sovereignty, as it enables governments to ensure the privacy of their citizens, safeguard sensitive information, and protect national interests. Data protection laws, data localization policies, and the regulation of cross-border data flows are thus fundamental pillars of digital sovereignty (Rastgar-Khalid et al., 2020).

Another key pillar of digital sovereignty is national security. As more critical infrastructure, services, and processes become digitized, the vulnerability to cyberattacks, surveillance, and external interference has increased. States are now tasked with ensuring the security of their digital infrastructures, ranging from telecommunications networks to financial systems and even electoral processes. This concern is compounded by the increasing involvement of foreign technology companies in national infrastructures, raising questions about potential espionage, data theft, and the manipulation of information. National security in the context of digital sovereignty also extends to the protection of citizens from cybercrime and ensuring that national defense mechanisms can function securely in a digital environment (Shahbazianni, 2023).

Privacy protection is another fundamental component of digital sovereignty. With the growing integration of digital technologies into everyday life, citizens' personal data is increasingly exposed to various actors, from corporations to governments. In this context, digital sovereignty involves the protection of individuals' privacy rights, ensuring that their personal information is not exploited or mishandled. This requires robust legal frameworks, such as data protection laws, which govern how personal data can be collected, processed, and stored by both public and private entities. The balance between individual rights to privacy and the state's need for surveillance and security is a central challenge in defining the scope of digital sovereignty (Mazaheri-Jabali et al., 2020).

The concept of digital sovereignty, while rooted in traditional notions of state control, is increasingly being challenged by the global nature of the internet and digital technologies. Unlike traditional sovereignty, which is geographically confined, digital sovereignty is inherently transnational, as data and information flow seamlessly across borders. This raises questions about the legitimacy and enforcement of national sovereignty over digital resources in a world where global networks dominate. As states attempt to regulate digital infrastructures and protect their citizens, they often face difficulties in enforcing laws that conflict with the practices of global technology companies or international agreements. The rise of global digital platforms has created new dynamics, where private companies wield significant influence over the digital lives of individuals and nations. These challenges highlight the complex nature of digital sovereignty and the need for legal frameworks that can effectively govern both national interests and global digital realities (Zamani & Nikoui, 2017).

The tension between digital sovereignty and traditional national sovereignty is also evident in the ways states approach the regulation of global tech giants. In many instances, national governments find themselves at odds with multinational corporations that operate across borders, making it difficult to impose national laws and regulations on these companies. The influence of tech companies often extends beyond economic interests to include social and political influence, raising concerns about the erosion of national autonomy. This intersection between digital sovereignty and national sovereignty is a critical area of debate, as states struggle to reconcile their need for control over digital resources with the realities of a globalized digital economy (Grzybowski, 2019).

Moreover, the notion of digital sovereignty also intersects with international law and the need for cross-border cooperation. In an increasingly interconnected world, states must navigate complex legal issues related to the flow of data, privacy rights, and cybersecurity. International legal mechanisms, such as treaties and conventions, are crucial for harmonizing regulations and ensuring that digital sovereignty does not become a tool for protectionism or isolationism. As the digital landscape continues to evolve, the concept of digital sovereignty will need to adapt to the challenges posed by new technologies, international legal frameworks, and the broader geopolitical context (Hartmann, 2017).

3. Legal and Policy Mechanisms for Managing Data

Data localization has become one of the central strategies employed by countries to assert digital sovereignty and maintain control over their national data infrastructure. These laws require that data generated within a country's borders be stored and processed within the same geographical area, limiting its flow to foreign jurisdictions. The primary rationale behind data localization laws is national security, economic interests, and privacy protection. In an era where data is seen as a critical national resource, states have increasingly focused on ensuring that they retain control over the data generated by their citizens and businesses. The growing concern about data security and the ability of foreign governments or corporations to access sensitive information has led to the development of such laws in a variety of countries.

For instance, in the European Union, the General Data Protection Regulation (GDPR) has become a cornerstone of data protection, incorporating strong provisions on data sovereignty. Although GDPR does not mandate data localization per se, it imposes strict rules on cross-border data transfers, ensuring that personal data of EU citizens is adequately protected when transferred outside the EU. This regulation has created a strong incentive for companies to consider localizing their data operations in Europe to comply with its requirements (Crum & Merlo, 2020). Similarly, Russia has enacted laws requiring that all data about its citizens be stored within the country’s borders, with strict penalties for non-compliance. This is part of a broader strategy to protect national security, particularly in light of tensions with foreign powers. Russia’s data localization laws have had significant implications for multinational companies operating in the country, forcing them to rethink their data storage and processing strategies (Sadat Bidgoli, 2023).

China's cybersecurity laws, too, are among the most stringent in the world, mandating that companies operating within the country store critical data domestically. The Chinese government has positioned itself as a key player in the global digital economy, and its data localization laws are seen as part of a larger effort to assert control over its vast digital infrastructure. These laws not only require domestic storage of data but also grant the state access to it under certain circumstances, raising concerns about privacy and surveillance (Zamani & Nikoui, 2017). The legal implications of such data localization laws for multinational companies are profound. Companies are often forced to establish local data centers, modify their data storage practices, and comply with stringent national regulations. These laws can create significant barriers to the free flow of information, especially for companies whose operations span multiple jurisdictions, and raise complex legal questions regarding data ownership and cross-border data rights (Pourkhaghan et al., 2019).

The free flow of data across borders has been a cornerstone of the global digital economy. However, the increasing emphasis on data sovereignty and national security concerns has led to greater scrutiny of cross-border data flows. As countries introduce data localization requirements, the unrestricted movement of data faces growing legal and regulatory hurdles. The challenge lies in balancing the need for open, global data flows with the desire of states to maintain control over the data generated within their borders. This tension is particularly evident in the context of international trade, where data is seen as a vital economic resource. As a result, the regulation of cross-border data flows has become a central issue in discussions on digital sovereignty and international law.

To address these challenges, various international treaties and agreements have been developed to facilitate the free flow of data while ensuring privacy and security standards. The EU-U.S. Privacy Shield Framework, for example, was established to ensure that personal data transferred from the EU to the U.S. is protected in line with EU standards. This agreement, however, faced significant challenges in terms of privacy protections and was eventually invalidated by the European Court of Justice in 2020, raising questions about the adequacy of cross-border data protection mechanisms (Mazaheri-Jabali et al., 2020). Similarly, the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) system seeks to establish a harmonized approach to data privacy protection across the APEC region, allowing businesses to transfer personal data across borders while ensuring compliance with privacy laws. These agreements, while aimed at facilitating the flow of data, have also highlighted the complexities of balancing national sovereignty with the need for international cooperation in the digital age (Jalili et al., 2024).

The challenge of cross-border data flows is further compounded by the differences in national data protection laws. While some countries have robust data protection frameworks, others may have less stringent regulations, creating disparities in how data is protected and managed across borders. This disparity creates a significant challenge for companies and individuals seeking to navigate the global digital ecosystem while ensuring that their data is adequately protected. Additionally, as countries increasingly prioritize their national interests over global trade considerations, the regulation of cross-border data flows is likely to become an area of intense negotiation and legal contention (Shahbazianni, 2023).

The global landscape of data protection laws has undergone significant transformation in recent years, driven by growing concerns about privacy, security, and the impact of new technologies on individuals' rights. One of the most significant developments in this area has been the introduction of the General Data Protection Regulation (GDPR) in the European Union. This regulation is widely regarded as the gold standard for data protection, establishing stringent requirements for the collection, processing, and storage of personal data. The GDPR not only grants individuals greater control over their personal data but also imposes significant obligations on businesses that process personal data, including requirements for explicit consent, data breach notifications, and the appointment of data protection officers. The regulation has had a far-reaching impact, influencing data protection laws in other jurisdictions and setting a new benchmark for privacy protection globally (Bytyci & Phillips, 2017).

In the United States, data protection laws are more fragmented, with sectoral regulations governing specific industries such as healthcare, finance, and telecommunications. The California Consumer Privacy Act (CCPA) is one of the most significant state-level privacy laws in the U.S. and serves as a model for other states seeking to implement data protection measures. While the CCPA provides some rights to consumers, such as the right to opt-out of data sales and the right to request data deletion, it falls short of the comprehensive protections offered by the GDPR. The lack of a federal data protection law in the U.S. creates a complex legal environment for companies operating across state lines, as they must navigate a patchwork of state-level

regulations. This fragmentation contrasts sharply with the more unified approach seen in Europe and presents challenges for businesses and consumers alike (Grzybowski, 2019).

Data protection laws are a crucial element in asserting digital sovereignty. By establishing clear rules for data collection, processing, and sharing, these laws give states the authority to regulate how data is used within their borders and to ensure that citizens' privacy is protected. In this context, data protection serves not only as a mechanism for safeguarding individual rights but also as a tool for protecting national interests in the digital economy. As more countries adopt or strengthen their data protection laws, digital sovereignty is increasingly being framed in terms of the right of states to control the data that flows within and outside their borders. Data protection laws, therefore, play a central role in defining the boundaries of digital sovereignty and ensuring that the digital rights of citizens are upheld (Sadat Bidgoli, 2023).

4. National Approaches to Digital Sovereignty

The European Union has taken a leading role in the development of a comprehensive strategy for digital sovereignty, grounded in a robust legal framework that seeks to protect the rights of individuals while ensuring that the EU's digital infrastructure remains secure and resilient. The cornerstone of this strategy is the GDPR, which provides a comprehensive set of rules for data protection and privacy, applicable to all businesses operating within the EU or processing data of EU citizens. The GDPR not only addresses data protection concerns but also plays a critical role in reinforcing the EU's digital sovereignty by ensuring that personal data is processed in compliance with EU law, regardless of where the data is stored or processed globally. This regulation also empowers EU citizens with greater control over their personal data, thereby asserting their sovereignty in the digital realm (Pourkhaghan et al., 2019).

In addition to the GDPR, the EU has introduced several other regulatory measures aimed at bolstering its digital sovereignty. The Digital Services Act (DSA) and the Digital Markets Act (DMA) are recent legislative efforts designed to regulate digital platforms and prevent anti-competitive behavior in the digital economy. The DSA aims to create a safer online environment by holding platforms accountable for illegal content and ensuring that users' rights are protected, while the DMA seeks to regulate the behavior of large digital platforms that act as gatekeepers in the digital economy. These laws reflect the EU's commitment to regulating the digital market and asserting its control over the digital economy, reinforcing its digital sovereignty (Jalili et al., 2024).

In contrast to the European Union's comprehensive approach to digital sovereignty, the United States has a more fragmented legal landscape regarding data protection and privacy. There is no overarching federal data protection law akin to the GDPR, and instead, data protection is regulated through sectoral laws such as the Health Insurance Portability and Accountability Act (HIPAA) for healthcare data and the Gramm-Leach-Bliley Act (GLBA) for financial data. While these laws provide some degree of protection for specific types of data, they do not offer the same level of broad-based privacy protection seen in the EU. The lack of a comprehensive national data protection framework has led to calls for stronger federal privacy legislation, especially in light of growing concerns over surveillance, data breaches, and the influence of tech companies (Crum & Merlo, 2020).

The U.S. approach to digital sovereignty is also marked by the dominant role of private companies in shaping the digital landscape. Tech giants in Silicon Valley exert significant influence over the way data is collected, processed, and used, often creating tensions with government attempts to regulate their activities. This creates a unique challenge for the U.S. as it seeks to balance its commitment to market freedom with the need to protect citizens' digital rights and national security. Moreover, the U.S. legal system has a more open stance towards cross-border data flows compared to the EU, advocating for the free movement of data across borders, which has led to conflicts with other nations advocating for data localization (Mazaheri-Jabali et al., 2020).

China's approach to digital sovereignty is among the most assertive and comprehensive in the world. The Chinese government has enacted stringent data protection and localization laws that require foreign companies to store data domestically and grant the state access to this data when necessary. These laws are part of a broader strategy to ensure the security and control of China's digital infrastructure, which is heavily regulated by the government. The country's Cybersecurity Law, enacted in 2017, mandates that critical data be stored within the country's borders and imposes strict requirements on foreign companies operating in China to comply with Chinese data protection standards. China's approach to digital sovereignty is

deeply intertwined with its broader goals of economic development, political stability, and national security (Sadat Bidgoli, 2023).

China also employs sophisticated state surveillance techniques, which include monitoring internet activity and controlling the flow of information. The government has developed extensive systems for collecting data on its citizens, which it uses for both security and political control. This approach has raised significant concerns about privacy rights and the potential for abuse, particularly as the state has significant influence over digital platforms and technologies within the country. In this context, digital sovereignty for China is not only about protecting its national data but also about asserting control over its digital ecosystem and ensuring that foreign entities cannot disrupt or influence its internal affairs (Shahbazianni, 2023).

Other countries have also developed distinct approaches to digital sovereignty, shaped by their unique political, economic, and legal environments. For example, India has introduced the Personal Data Protection Bill, which aims to regulate the processing of personal data and ensure that citizens' privacy is protected. The bill is seen as a response to growing concerns about data privacy and the influence of foreign tech companies operating in India. Similarly, Russia's approach to digital sovereignty is characterized by stringent data localization requirements and a strong focus on national security, while Brazil's General Data Protection Law (LGPD) follows a similar model to the GDPR in the European Union, emphasizing transparency and accountability in data processing (Zamani & Nikoui, 2017). Each of these countries, despite having different legal and political contexts, recognizes the importance of asserting control over digital resources and ensuring that data is processed in ways that align with national interests.

5. Global Challenges in Digital Sovereignty

As digital technologies increasingly transcend national borders, jurisdictional conflicts have become a major challenge in asserting digital sovereignty. The global nature of the internet means that data generated in one country can easily flow across borders, creating tensions between different national legal systems. These conflicts arise from the difficulty of determining which jurisdiction's laws apply to cross-border data flows, as well as the challenges in enforcing these laws effectively. For instance, when personal data is transferred from one country to another, the data may be subject to conflicting regulations, making it difficult for businesses to comply with all relevant laws. Additionally, some countries may impose stringent data protection requirements, while others may prioritize the free flow of information for economic or national security reasons, leading to significant tension in regulating cross-border data movement (Beijerman, 2018).

One of the core issues in jurisdictional conflicts is the legal and practical difficulty of enforcing laws across different jurisdictions. Data is often stored and processed in multiple countries, which complicates the application of national laws. In cases where data privacy laws differ significantly between countries, enforcement mechanisms may become ineffective or overly complex. For example, the European Union's GDPR includes extraterritorial provisions, meaning that it applies to organizations outside the EU if they handle data belonging to EU citizens. However, enforcement of these rules in jurisdictions that do not adhere to similar privacy standards presents significant challenges, as national courts may not have the authority to enforce foreign laws or compel compliance from companies operating in other regions (Crum & Merlo, 2020). Similarly, countries that prioritize national security over privacy may refuse to comply with foreign data protection regulations, creating a complex and fragmented landscape for multinational businesses.

These conflicts are further exacerbated by the lack of a consistent and universally accepted legal framework for regulating cross-border data flows. As more countries adopt different standards for data protection and digital infrastructure, the potential for jurisdictional disputes increases. In particular, the increasing use of cloud computing and global data centers, which store data across various jurisdictions, complicates the enforcement of national laws and regulations. The challenge of resolving these conflicts while maintaining effective governance over digital resources has led to growing calls for international cooperation and the development of more harmonized legal frameworks (Sadat Bidgoli, 2023).

Balancing the need for digital sovereignty with the realities of globalization presents another critical challenge. On one hand, states seek to assert control over their digital infrastructure, ensuring that data generated within their borders is protected and used in accordance with national interests. On the other hand, the digital economy thrives on the free flow of information, and excessive restrictions on cross-border data flows can stifle innovation, limit economic opportunities, and hinder international collaboration. This tension between national control and global connectivity has led to the need for nuanced approaches to

digital sovereignty, where states must find ways to protect their interests without undermining the broader benefits of globalization.

At the heart of this issue is the question of how to regulate the digital economy without isolating national markets from global trade. Countries that enforce strict data localization laws or limit cross-border data flows may risk alienating foreign businesses, stifling technological innovation, and limiting access to global markets. The global nature of the digital economy means that companies rely on data from multiple jurisdictions to operate, and overly restrictive policies may disrupt business operations and hinder global competitiveness (Touhidi et al., 2023). Furthermore, in a world where digital technologies and platforms are increasingly interconnected, it becomes difficult for countries to achieve complete sovereignty without significantly impacting international partnerships and collaborations.

The challenge is especially pronounced in the context of emerging technologies such as artificial intelligence and blockchain, which are inherently global and require the free movement of data to function effectively. For example, AI systems often rely on vast amounts of data from various sources to improve their models, and restricting data flows could impede innovation in these fields. Similarly, blockchain technology relies on decentralized networks that transcend national borders, making it difficult to enforce national laws in a way that would maintain the benefits of the technology. Striking a balance between protecting national interests and facilitating global cooperation is thus one of the most difficult aspects of digital sovereignty, as countries seek to assert control over their digital environments without undermining the global digital economy (Zamani & Nikoui, 2017).

The role of global technology companies in shaping national and global digital sovereignty frameworks cannot be overstated. Large multinational tech firms such as Google, Amazon, Facebook, and others dominate the global digital landscape, controlling vast amounts of data and infrastructure. These companies play a significant role in the digital economy by facilitating the flow of data across borders, providing essential services to consumers and businesses alike. However, their dominance has raised concerns about privacy, competition, and the concentration of power in the hands of a few global entities. As a result, governments have increasingly sought to regulate these companies to ensure that they respect national laws and contribute to the maintenance of digital sovereignty.

One of the primary concerns surrounding the influence of global tech giants is the control they exert over personal data. These companies collect and process massive amounts of data on individuals, often without full transparency or clear consent. This has raised alarms among privacy advocates, who argue that such companies should be held accountable for how they use and share personal information. In response, some governments have implemented or proposed regulations that require these companies to comply with stricter privacy standards. For instance, the European Union's GDPR has imposed significant fines on companies that fail to comply with data protection rules, sending a clear message that even global tech giants must adhere to national laws regarding data privacy (Crum & Merlo, 2020). Similarly, other countries are exploring or enacting similar laws to ensure that tech companies respect the digital rights of their citizens.

The increasing power of these global corporations also presents challenges for national governments seeking to assert control over their digital infrastructure. Large tech companies often have the resources to navigate complex regulatory environments and may use their influence to shape the legal frameworks that govern their operations. This has led to concerns about the erosion of national sovereignty as these companies exert disproportionate influence over the digital landscape. Additionally, the cross-border nature of these corporations means that national governments often struggle to enforce their laws on companies that operate globally. The complexity of regulating these entities while ensuring the protection of national interests highlights the difficulties of maintaining digital sovereignty in an era of corporate globalization (Shahbazianni, 2023).

Cybersecurity and national security concerns are increasingly at the forefront of discussions surrounding digital sovereignty. As digital infrastructure becomes more integrated into every aspect of governance, commerce, and everyday life, the potential for cyberattacks and other malicious activities targeting critical infrastructure has grown. Countries are increasingly focusing on protecting their digital infrastructure from external threats while maintaining control over their own cybersecurity frameworks. The challenge lies in ensuring that national security concerns do not infringe on citizens' rights to privacy and freedom of expression, particularly in cases where surveillance measures are implemented to safeguard against cyber threats.

Legal mechanisms to protect digital infrastructure have become more sophisticated in response to the growing risks of cyberattacks. Many countries have developed national cybersecurity strategies and enacted legislation aimed at strengthening digital defenses. For instance, the U.S. has established various cybersecurity frameworks, such as the Cybersecurity Act of

2015, which mandates that critical infrastructure entities share cybersecurity information with the government. Similarly, the EU has implemented the Network and Information Systems Directive, which seeks to enhance the resilience of critical infrastructure across member states. These legal mechanisms are designed to protect digital systems from external threats, but they also raise questions about the balance between security and privacy. As states enhance their cybersecurity measures, concerns about mass surveillance and the erosion of individual freedoms have become more pronounced (Beijerman, 2018).

At the same time, national security concerns often collide with digital sovereignty when countries seek to assert control over foreign digital infrastructure. Governments may demand access to data stored by foreign companies or in foreign jurisdictions, citing national security concerns as a justification. However, this can conflict with international privacy standards and data protection laws, creating legal dilemmas regarding the extraterritorial reach of national laws. This tension is particularly evident in cases where governments demand access to encrypted data or seek to compel tech companies to hand over information for national security purposes. The challenge for policymakers is to develop legal frameworks that balance the need for national security with the protection of individual privacy rights and the broader principles of digital sovereignty (Sadat Bidgoli, 2023).

6. Legal Innovations and Solutions for Digital Sovereignty

In response to the growing challenges posed by digital sovereignty, several innovative legal frameworks are being explored to better manage the intersection of national control, international trade, and digital infrastructure. One of the most significant developments in this area has been the introduction of the Digital Markets Act (DMA) in the European Union, which aims to regulate large digital platforms that function as gatekeepers in the digital economy. The DMA seeks to ensure that these platforms operate in a way that is fair and transparent, providing equal opportunities for smaller companies and preventing anti-competitive behavior. By regulating the largest tech companies, the DMA represents a proactive approach to digital sovereignty, ensuring that digital markets remain open and competitive (Zamani & Nikoui, 2017).

Another area of legal innovation is the growing focus on artificial intelligence (AI) regulation. As AI technologies become increasingly central to digital economies, their potential to impact national security, privacy, and individual rights has led to calls for greater legal oversight. Many countries are exploring new regulatory frameworks to govern the development and deployment of AI technologies, focusing on ensuring transparency, accountability, and ethical standards. For example, the EU has proposed the Artificial Intelligence Act, which seeks to regulate AI systems based on their potential risk to users and society. Such legal innovations aim to strike a balance between fostering innovation and protecting national interests, while also addressing the broader implications of AI for digital sovereignty (Shahbazianni, 2023).

The integration of technological tools with legal frameworks represents another promising solution to the challenges of digital sovereignty. Blockchain technology, for instance, has emerged as a potential tool for enhancing data sovereignty by providing decentralized, transparent, and secure methods for storing and transferring data. Blockchain could offer a way for countries to retain control over their digital assets while ensuring that data remains accessible and verifiable across borders. Similarly, AI technologies are being explored to help enforce legal frameworks for digital sovereignty, by automating compliance with data protection laws and enhancing security measures. The integration of such technologies into legal frameworks has the potential to streamline governance, improve compliance, and reduce the risks associated with cross-border data flows and jurisdictional conflicts (Touhidi et al., 2023).

Multilateral cooperation is crucial for addressing the challenges of digital sovereignty on a global scale. While countries may have differing priorities and approaches to digital governance, there is growing recognition that international collaboration is necessary to address cross-border issues such as data protection, cybersecurity, and digital trade. Efforts to harmonize legal frameworks for digital sovereignty are underway through various international organizations, such as the OECD, which is working to establish global standards for privacy protection and digital infrastructure governance. By fostering greater cooperation between nations, these initiatives aim to create a more cohesive and consistent approach to digital sovereignty that balances national control with the needs of the global digital economy (Crum & Merlo, 2020).

7. Future Directions and Recommendations

The evolution of digital sovereignty is closely tied to the rapid advancements in digital technologies, which continue to reshape the global landscape of data governance and international relations. One key trend that is expected to drive the future

of digital sovereignty is the increasing emphasis on artificial intelligence (AI), machine learning, and blockchain technologies. These emerging technologies have the potential to significantly alter how data is managed, stored, and shared across borders, raising new questions about national control and the protection of digital infrastructure. AI, in particular, is expected to play a pivotal role in automating compliance with data protection laws and enabling more efficient cross-border data management. Its ability to process vast amounts of data and adapt to new regulatory environments makes it a valuable tool for governments seeking to balance digital sovereignty with the need for global cooperation (Sadat Bidgoli, 2023).

Blockchain, on the other hand, offers a promising solution for enhancing data sovereignty by providing decentralized, transparent, and secure mechanisms for data storage and transfer. By using blockchain, countries could potentially avoid some of the risks associated with centralized data storage, such as data breaches or unauthorized access. Furthermore, blockchain's ability to ensure data integrity and traceability could improve accountability in digital transactions and data exchanges, which is a crucial aspect of asserting sovereignty in the digital age. As these technologies continue to evolve, they will likely become central to the ongoing discourse surrounding digital sovereignty, offering new ways for governments to control their digital infrastructure while promoting transparency and cooperation (Zamani & Nikoui, 2017).

Another emerging trend in digital sovereignty is the increasing adoption of data localization laws and regulations, which require companies to store and process data within national borders. While data localization is often seen as a way for governments to protect their citizens' privacy and assert control over their digital resources, it also poses significant challenges for multinational companies that rely on the free flow of data to conduct business. This tension between national sovereignty and the need for global digital infrastructure will continue to shape the future of digital governance. Over the coming years, it is likely that we will see an expansion of data localization requirements, particularly in regions where digital sovereignty is seen as critical for national security or economic development. However, this will also spark further debate about the economic impact of such policies and their potential to disrupt global trade and innovation (Touhidi et al., 2023).

To navigate the complex landscape of digital sovereignty, policymakers must develop strategies that balance national control with the need for international cooperation and economic growth. One of the key recommendations for policymakers is the need for a flexible and adaptable legal framework that can accommodate the rapidly changing digital environment. While it is important for governments to assert control over their digital infrastructure, it is equally essential that they engage in international dialogues and negotiations to develop harmonized regulations that facilitate cross-border data flows and global collaboration. This could involve creating international agreements that set universal standards for data protection, privacy, and cybersecurity, while allowing for national variations based on local needs and concerns. Such agreements could help mitigate jurisdictional conflicts and promote consistency in digital governance across borders (Sadat Bidgoli, 2023).

Another important policy recommendation is the need for greater investment in cybersecurity and digital infrastructure. As the digital landscape becomes increasingly interconnected, countries must ensure that their digital infrastructures are secure and resilient to cyber threats. This requires not only strengthening national security measures but also promoting collaboration with international partners to address global cybersecurity risks. Multilateral initiatives, such as the establishment of cybersecurity norms and frameworks for sharing information about cyber threats, could help improve global digital governance and reduce the risk of cyberattacks that could undermine national sovereignty. Furthermore, governments should focus on developing legal mechanisms that ensure the protection of critical digital infrastructure, such as cloud computing platforms and data centers, from foreign interference or control (Beijerman, 2018).

Policymakers should also focus on encouraging innovation while safeguarding digital sovereignty. This can be achieved by fostering an environment that supports technological innovation through regulatory sandboxes and pilot projects that allow companies to test new technologies in a controlled environment. At the same time, regulations should be put in place to ensure that these innovations align with national interests, particularly with regard to data privacy, national security, and competition. A proactive approach to regulating emerging technologies such as AI, blockchain, and the Internet of Things (IoT) will be critical for maintaining sovereignty in the digital economy while encouraging the development of cutting-edge technologies that can benefit both the public and private sectors (Crum & Merlo, 2020).

Finally, a significant area where legal reform is needed is in the realm of international data protection standards. As more countries introduce their own data protection laws, there is an increasing need for alignment and harmonization to avoid conflicting regulations that could complicate global business operations. Policymakers should work toward the establishment of international standards for data protection that ensure the privacy and security of individuals' data while allowing for the

free movement of information across borders. This could involve further strengthening international agreements such as the EU-U.S. Privacy Shield or developing new frameworks for cross-border data transfers that are fair, transparent, and aligned with the principles of digital sovereignty (Shahbazianni, 2023).

8. Conclusion

This review has examined the complex and evolving issue of digital sovereignty, focusing on the legal mechanisms that countries employ to manage their data and digital infrastructure. The concept of digital sovereignty, as it intersects with traditional national sovereignty, has become a critical concern in the context of rapid technological advancements and globalization. It is evident that digital sovereignty encompasses a wide range of legal, economic, and political issues, including data localization laws, cross-border data flows, and the increasing role of multinational tech companies. The review has highlighted the varying approaches that different countries take to assert control over their digital environments, from the strict regulatory frameworks of the European Union to the more market-oriented approach of the United States. The role of emerging technologies, such as AI and blockchain, in shaping the future of digital sovereignty is also a key area of focus, with these technologies offering both opportunities and challenges for managing digital resources and protecting national interests (Mazaheri-Jabali et al., 2020).

Furthermore, the review has underscored the global challenges that arise from jurisdictional conflicts, the tension between national sovereignty and globalization, and the influence of global tech giants. These challenges have prompted calls for greater international cooperation and the development of more harmonized legal frameworks to address issues such as cross-border data flows, data protection, and cybersecurity. The role of multilateral organizations, such as the OECD, in promoting collaboration and the establishment of global standards for digital governance will be crucial in shaping the future of digital sovereignty. At the same time, policymakers must consider the legal innovations and technological solutions that are emerging to address these challenges, including new laws for regulating AI and digital markets, as well as the integration of blockchain and other technologies into national legal frameworks (Crum & Merlo, 2020).

As the digital economy continues to grow and evolve, the need for effective digital sovereignty frameworks will become even more pronounced. Balancing the desire for national control over digital infrastructure with the realities of a globalized digital economy will remain a significant challenge for policymakers. The key to successfully navigating this complex landscape will lie in the development of flexible legal frameworks that promote both national interests and international cooperation. Digital sovereignty must be seen not only as a means of protecting national security and privacy but also as an opportunity to foster innovation, promote competition, and ensure fair access to digital resources for all. Moving forward, the ability of governments to adapt to technological changes while maintaining sovereignty over their digital environments will be a defining feature of the digital age (Sadat Bidgoli, 2023). The future of digital sovereignty is likely to be shaped by the continued integration of emerging technologies with legal frameworks, the expansion of multilateral cooperation, and the pursuit of fair and effective international agreements that safeguard both national interests and global collaboration.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all participants who participate in this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

Beijerman, M. (2018). Conceptual confusions in debating the role of NGOs for the democratic legitimacy of international law. Transnational Legal Theory, 9(2), 147-173.
Crum, B., & Merlo, S. (2020). Democratic legitimacy in the post-crisis EMU. Journal of European Integration, 42(3), 399-413.
Mazaheri-Jabali, Shahin, Behnam-Roudsari, & Yekta. (2020). How to recognize and not recognize a state (some practical considerations). Research on Nations, 50(5), 55-69.
Sadat Bidgoli. (2023). An analysis of the challenge of legitimacy of Ashraf Ghani's government. Iranian History Journal, 16(2), 225-246.
Shahbazianni. (2023). The concept of state recognition under international law: A case study of the Taliban in Afghanistan. Studies in Political Science, Law, and Jurisprudence, 48(9), 129-138.
Sadeghi, Raei, & Raisi. (2022). Popular sovereignty and state recognition. Journal of Public Law Studies, University of Tehran, 52(3), 1299-1317.
Touhidi, Ghassami Shahi, & Mohammadamir. (2023). The paradox of state practice regarding non-recognition of the Taliban government with an emphasis on Iran's strategy. Strategic Journal, 31(4), 695-728.
Zamani, Masoud, & Nikoui. (2017). Legitimacy of third-party military intervention based on the host country's invitation: An analysis of military interventions in Mali, Ukraine, Syria, and Yemen. Public Law Research, 18(54), 289-317.
Crum, B., & Merlo, S. (2020). Democratic legitimacy in the post-crisis EMU. Journal of European Integration, 42(3), 399-413.
Grzybowski, J. (2019). The paradox of state identification: De facto states, recognition, and the (re-)production of the international. International Theory, 11, 241–263.
Hartmann, I. (2017). Let the users be the filter? Crowdsourced filtering to avoid online intermediary liability. Journal of the Oxford Centre for Socio-Legal Studies, 1, 21-47.
Rollo, T. (2019). Imperious temptations: Democratic legitimacy and indigenous consent in Canada. Canadian Journal of Political Science, 52(1), 1-19.
Beijerman, M. (2018). Conceptual confusions in debating the role of NGOs for the democratic legitimacy of international law. Transnational Legal Theory, 9(2), 147-173.
Crum, B., & Merlo, S. (2020). Democratic legitimacy in the post-crisis EMU. Journal of European Integration, 42(3), 399-413.
Bytyci, F., & Phillips, D. L. (2017). State-building and the making of democracy: Kosovo in comparative perspective. Journal of Balkan and Near Eastern Studies, 19(1), 68-86.
Grzybowski, J. (2019). The paradox of state identification: De facto states, recognition, and the (re-)production of the international. International Theory, 11, 241–263.
Hartmann, I. (2017). Let the users be the filter? Crowdsourced filtering to avoid online intermediary liability. Journal of the Oxford Centre for Socio-Legal Studies, 1, 21-47.
Rollo, T. (2019). Imperious temptations: Democratic legitimacy and indigenous consent in Canada. Canadian Journal of Political Science, 52(1), 1-19.
Mazaheri-Jabali, Shahin, Behnam-Roudsari, & Yekta. (2020). How to recognize and not recognize a state (some practical considerations). Research on Nations, 50(5), 55-69.
Beijerman, M. (2018). Conceptual confusions in debating the role of NGOs for the democratic legitimacy of international law. Transnational Legal Theory, 9(2), 147-173.
Crum, B., & Merlo, S. (2020). Democratic legitimacy in the post-crisis EMU. Journal of European Integration, 42(3), 399-413.
Bytyci, F., & Phillips, D. L. (2017). State-building and the making of democracy: Kosovo in comparative perspective. Journal of Balkan and Near Eastern Studies, 19(1), 68-86.
Grzybowski, J. (2019). The paradox of state identification: De facto states, recognition, and the (re-)production of the international. International Theory, 11, 241–263.
Hartmann, I. (2017). Let the users be the filter? Crowdsourced filtering to avoid online intermediary liability. Journal of the Oxford Centre for Socio-Legal Studies, 1, 21-47.
Rollo, T. (2019). Imperious temptations: Democratic legitimacy and indigenous consent in Canada. Canadian Journal of Political Science, 52(1), 1-19.