Page 2247 - 2254 **DOI:** *https://doij.org/10.10000/IJLMH.1110075*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 3

2025

Reclaiming Control in Cyberspace: An Overview of Digital Sovereignty and its Global Evolution

KHUSHBU PRASAD[1] AND DR. TARU MISHRA[2]

ABSTRACT

Digital sovereignty is a nation's ability to control its own digital space—its data, infrastructure and online services—just as it manages physical borders. This paper traces how the idea grew from the internet's open beginnings through rising cybersecurity concerns, the Snowden disclosures and the COVID-19 digital surge. It shows how regions like the European Union protect privacy with rules such as the GDPR, how the United States leverages market power and global standards, and how China and Russia enforce strict state control. It also looks at efforts in developing countries, including India's Data Localization proposals, which balance foreign partnerships with local innovation. The study highlights risk of digital fragmentation, authoritarian overreach, technological gaps and powerful private platforms. It concludes that true digital sovereignty requires balancing national security and economic independence with an open, cooperative internet that protects citizens' rights and supports global innovation.

I. INTRODUCTION

In the 21st century, the rapid growth of digital technologies has brought major changes to the way governments operate, economies function, national security is maintained, and people exercise their rights.[3] From online banking and digital health records to smart cities and artificial intelligence, digital tools are now a part of almost every aspect of life. As a result, countries across the world are becoming more dependent on digital infrastructure, such as the internet, data networks, cloud computing, and digital platforms. This has raised an important question—who has control over these digital resources? The answer lies in the evolving concept of **digital sovereignty**.

Digital sovereignty refers to a country's ability to control its own digital space. Just as a nation

[1] Author is a Research Scholar at Amity Law School, Amity University, Lucknow Campus, India.
[2] Author is an Assistant Professor at Amity Law School, Amity University, Lucknow Campus, India.
[3] United Nations Conference on Trade and Development. (2021). *Digital economy report 2021: Cross-border data flows and development – For whom the data flow*. United Nations. https://unctad.org/system/files/official-document/der2021_en.pdf

 [ISSN 2581-5369]

controls its physical borders, it now seeks to control its digital borders.[4] This includes managing the flow of data within and across its territory, regulating digital services, and protecting its citizens' data from foreign influence. With rising global interdependence and the growing power of large tech companies—many of which operate across borders—countries are worried about losing control over their digital resources. This concern has made digital sovereignty a critical issue in public policy, lawmaking, and international relations.[5]

Today, much of the world's data is stored and processed by foreign-owned cloud services and digital platforms. This makes many countries dependent on foreign technologies for essential services, which could be risky in times of conflict or crisis. Moreover, cyberattacks, online surveillance, and data misuse have shown how digital tools can be used to interfere in another country's internal affairs. This is why digital sovereignty is not just about technology—it is also about **national security, economic independence, and protecting the rights of citizens**.[6]

As a result, countries are taking steps to strengthen their digital control. Some governments are creating laws that require data about their citizens to be stored locally, a concept known as **data localization**.[7] Others are developing their own digital platforms and encouraging local innovation to reduce reliance on foreign technology. Debates around digital sovereignty also include discussions about internet governance, cybersecurity policies, privacy protection, and ensuring fair access to technology. While some worry that such measures might lead to censorship or internet fragmentation, others believe that digital sovereignty is necessary to protect national interests.

At the same time, there is no single model of digital sovereignty. Different countries are adopting different approaches, depending on their political systems, technological capabilities, and global partnerships. For instance, the European Union focuses on data protection and digital rights through laws like the General Data Protection Regulation (GDPR),[8] while countries like China emphasize strict control over digital platforms and data flows.[9]

---

[4] European Commission. (2020). *Shaping Europe's digital future*. https://ec.europa.eu/digital-strategy/en/policies/shaping-europes-digital-future

[5] DeNardis, L. (2014). *The global war for Internet governance*. Yale University Press.

[6] International Telecommunication Union. (2020). *Global ICT regulatory outlook 2020: Regulatory governance in the digital economy*. https://www.itu.int/en/publications/ITU-D/Pages/publications.aspx?parent=T-DREG-GLOB_OUTL.01-2020

[7] Kerry, C. F. (2019). *Why data localization laws and trade restrictions threaten the open internet*. The Brookings Institution. https://www.brookings.edu/articles/why-data-localization-laws-and-trade-restrictions-threaten-the-open-internet/

[8] General Data Protection Regulation (GDPR). (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[9] Creemers, R. (2017). *Cyber China: Upgrading propaganda, public opinion work and social management for*

This paper aims to give a clear and detailed understanding of digital sovereignty. It will explain what the term means, how the idea has developed over time, and how it is being addressed around the world today. By exploring global trends, legal frameworks, and national strategies, this study seeks to highlight the importance of digital sovereignty in a world that is increasingly shaped by technology.

II. DEFINITION OF DIGITAL SOVEREIGNTY

Digital sovereignty is the ability of a government or state to control, manage, and regulate the digital data, infrastructure, and services that are available in its area, in line with its laws, values, and interests.[10] Digital sovereignty is all about giving a country control over its digital assets, like user data, software, algorithms, artificial intelligence, and the internet's physical infrastructure, like servers and data centres.[11] This way, foreign entities can't change a country's digital policies or operations without permission.[12] The idea has many parts:

Technological sovereignty means having control over the hardware and software that make up digital infrastructure.[13]

Data Sovereignty means having the legal right to control how data is stored, accessed, and flows.[14] Cyber Sovereignty means being able to put cybersecurity measures in place and enforce laws in a national digital environment.[15] Regulatory Sovereignty means having the power to make rules and laws that control how people interact with each other online in a state's jurisdiction.[16] Digital sovereignty isn't just a legal or technological idea; it's also a political declaration that says people should be able to control their digital lives without relying on foreign companies or governments.[17]

---

the twenty-first century. Journal of Contemporary China, **26**(103), 85–100. https://doi.org/10.1080/10670564.2016.1206281

[10] Pohle, J., & Thiel, T. (2020). *Digital sovereignty*. Internet Policy Review, 9(4), 1–17. https://doi.org/10.14763/2020.4.1532

[11] Floridi, L. (2020). *The fight for digital sovereignty: What it is, and why it matters, especially for the EU*. Philosophy & Technology, 33(3), 369–378. https://doi.org/10.1007/s13347-020-00423-6

[12] Chander, A., & Lê, U. P. (2015). *Data nationalism*. Emory Law Journal, 64(3), 677–739.

[13] European Commission. (2020). *Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu

[14] Greenleaf, G. (2018). *Global data privacy laws 2017: 120 national data privacy laws, including Indonesia and Turkey*. Privacy Laws & Business International Report, (145), 10–13.

[15] Segal, A. (2017). *The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age*. PublicAffairs.

[16] Kuner, C., Cate, F. H., Lynskey, O., & Millard, C. (2015). *Data localization and the free flow of data*. International Data Privacy Law, 5(1), 1–4.

[17] Mueller, M. (2010). *Networks and states: The global politics of Internet governance*. MIT Press.

 [ISSN 2581-5369]

III. HISTORICAL DEVELOPMENT

The concept of digital sovereignty is relatively new but is rooted in the broader evolution of **sovereignty** and **technology governance**. Its development can be traced through several key historical phases:

A. Early Internet and the Global Commons (1990s–early 2000s)

In the early stages of the internet, digital spaces were often considered **borderless** and operated under the ideal of a **global commons**. [18] Internet governance was largely decentralized, managed by organizations like the Internet Corporation for Assigned Names and Numbers (ICANN) and governed by multi-stakeholder models involving governments, academia, civil society, and corporations.[19]

During this period, the United States and its tech giants dominated the digital landscape, leading to what some critics call the "digital hegemony" of the West.[20]

B. The Rise of Cybersecurity and National Concerns (2005–2013)

Events such as the 9/11 attacks and rising cyber threats led to growing recognition of the **vulnerabilities** in the digital ecosystem.[21] Cybersecurity became a matter of **national security**, and states began asserting control over digital networks to protect their critical infrastructure and sensitive data.[22]

This period also witnessed debates over **jurisdiction in cyberspace**, such as the implications of the USA PATRIOT Act, which allowed U.S. agencies to access data held by American companies, even if stored abroad.[23]

C. Snowden Revelations and the Push for Sovereignty (2013–2016)

The 2013 revelations by Edward Snowden about the NSA's global surveillance programs marked a turning point.[24] Countries around the world realized the extent of U.S. surveillance over global internet infrastructure.[25] This catalyzed calls for **data localization**, **national control of digital infrastructure**, and **digital independence**.

---

[18] Ibid.
[19] DeNardis, L. (2014). *The Global War for Internet Governance*. Yale University Press.
[20] Morozov, E. (2011). *The Net Delusion: The Dark Side of Internet Freedom*. PublicAffairs.
[21] Clarke, R. A., & Knake, R. K. (2010). *Cyber War: The Next Threat to National Security and What to Do About It*. Ecco.
[22] Nye, J. S. (2014). The Regime Complex for Managing Global Cyber Activities. *Global Commission on Internet Governance Paper Series*, 1.
[23] Swire, P. P. (2012). From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud. *International Data Privacy Law*, 2(4), 200–206.
[24] Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. Metropolitan Books.
[25] Lyon, D. (2015). *Surveillance after Snowden*. Polity Press.

 [ISSN 2581-5369]

In Europe, the GDPR (General Data Protection Regulation) was adopted in 2016 to assert stronger control over data privacy.[26] In Russia and China, digital sovereignty took more authoritarian forms, with strict data laws and internet controls.[27]

D. COVID-19 and the Acceleration of Digitalization (2020–present)

The COVID-19 pandemic accelerated the global digital transformation, making societies more reliant on digital services.[28] With this came increased scrutiny over **foreign tech dependence**, especially on platforms such as Zoom, Microsoft, and Google.

The geopolitical rivalry between the U.S. and China, particularly over companies like Huawei, TikTok, and Alibaba, further intensified the focus on digital sovereignty.[29] States began investing in **indigenous technologies**, building **national cloud infrastructure**, and reinforcing regulatory oversight over foreign platforms.[30]

IV. GLOBAL TRENDS IN DIGITAL SOVEREIGNTY

The pursuit of digital sovereignty varies across regions depending on their political ideologies, economic capabilities, and geopolitical interests. Key global trends include:

Europe: Regulatory Sovereignty and Digital Autonomy

The European Union has emerged as a leader in digital sovereignty through its regulatory frameworks.[31] The GDPR, which came into effect in 2018, set a global benchmark for data protection. Initiatives like GAIA-X aim to establish a federated, European cloud infrastructure that is transparent, secure, and interoperable.[32]

The Digital Services Act (DSA) and Digital Markets Act (DMA) are recent EU regulations targeting platform accountability and fair competition. These laws are designed to reduce dependence on U.S. tech giants and promote European technological self-reliance.

United States: Strategic Dominance and Market-Driven Model

The U.S. remains home to the world's largest digital companies—Google, Apple, Facebook, Amazon, and Microsoft (GAFAM)—which have significant influence over global digital

[26] Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer.
[27] Creemers, R. (2017). Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century. *Journal of Contemporary China*, 26(103), 85–100.
[28] UNCTAD. (2021). *COVID-19 and E-commerce: A Global Review*. United Nations.
[29] Segal, A. (2020). *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. PublicAffairs.
[30] OECD. (2021). *Digital Economy Outlook 2020*. OECD Publishing.
[31] European Commission. (2020). *Shaping Europe's Digital Future*. https://ec.europa.eu/digital-strategy
[32] European Parliament. (2022). *The Digital Services Act and Digital Markets Act*. https://www.europarl.europa.eu/

infrastructure.[33] Although the U.S. emphasizes a free and open internet, its digital policies are also guided by strategic and commercial interests.

Washington has increasingly leveraged its technological superiority as a tool of geopolitical influence, particularly in blocking the adoption of Chinese technologies in allied countries.[34] U.S. efforts to shape global digital standards often align with the interests of its tech corporations.

China: Cyber Sovereignty and Digital Authoritarianism

China promotes the concept of "cyber sovereignty", where each country has the right to regulate and control its internet according to its own laws.[35] This model emphasizes state control over content, platforms, and data flows.

The Great Firewall, data localization laws, and the Social Credit System exemplify China's approach to digital sovereignty.[36] Simultaneously, China is exporting its digital governance model through the Digital Silk Road, part of its Belt and Road Initiative, offering digital infrastructure to developing nations.

Russia: Digital Isolation and Strategic Sovereignty

Russia has adopted a defensive form of digital sovereignty, particularly after facing international sanctions.[37] The "Sovereign Internet Law" (2019) empowers the state to isolate its internet from the global web in case of emergencies.[38]

Russia has developed domestic alternatives to Western platforms, such as Yandex and VKontakte, and has been strengthening state surveillance over the digital sphere, citing national security concerns.

Developing Countries: Balancing Act and Digital Dependence

Countries in Asia, Africa, and Latin America often find themselves navigating between competing global powers for digital influence.[39] While many are concerned about digital colonization, they lack the infrastructure and resources to build autonomous systems.

India, for instance, has taken steps toward digital sovereignty through initiatives like Data

[33] Zuboff, S. (2019). *The Age of Surveillance Capitalism*. PublicAffairs.
[34] Nye, J. S. (2010). Cyber Power. *Belfer Center for Science and International Affairs*.
[35] Creemers, R. (2016). Cyber China: Internet Control in the Xi Jinping Era. *Asia Papers*, 1(1), 1–30.
[36] Qiang, X. (2019). The Road to Digital Unfreedom: President Xi's Surveillance State. *Journal of Democracy*, 30(1), 53–67.
[37] Soldatov, A., & Borogan, I. (2015). *The Red Web: The Kremlin's Wars on the Internet*. PublicAffairs.
[38] Ermoshina, K., & Musiani, F. (2020). Russia's "Sovereign Internet" and the Struggle for Network Control. *Internet Policy Review*, 9(4).
[39] Gurumurthy, A., & Chami, N. (2020). *Digital Sovereignty and Development: A Scoping Review*. IT for Change.

 [ISSN 2581-5369]

Localization proposals and the Digital India program, while maintaining partnerships with foreign tech firms.[40] However, the path to sovereignty is complicated by trade dependencies and digital divide challenges.

V. CHALLENGES AND CRITICISMS OF DIGITAL SOVEREIGNTY

While the concept of digital sovereignty is appealing as a means of ensuring state autonomy in the digital realm, it is fraught with several significant challenges:

- **Global Interdependence:** The internet functions as a transnational infrastructure. Efforts to assert absolute digital sovereignty risk disrupting global services, fragmenting the internet, and stifling innovation through the creation of digital silos.[41]
- **Authoritarian Overreach:** In certain regimes, digital sovereignty is often used as a pretext for censorship, mass surveillance, and the suppression of dissent, raising serious concerns about human rights and democratic freedoms.[42]
- **Technological Gaps:** Many countries lack the technical expertise, infrastructure, and financial resources necessary to develop and maintain sovereign digital ecosystems, thereby increasing their reliance on foreign technologies and platforms.[43]
- **Conflict with Open Internet Values:** The move toward digital borders and nationalized internet policies undermines the foundational principles of the internet—openness, interoperability, and universal access—threatening its integrity as a global commons.[44]
- **Dominance of the Private Sector:** In the digital domain, private corporations often wield more influence than states, controlling critical platforms, infrastructure, and vast amounts of user data.[45]

This challenges the ability of governments to fully exercise digital sovereignty without negotiating or contending with corporate power.

In light of these complexities, digital sovereignty remains a contested and evolving concept, requiring a careful balance between national interests, global cooperation, and the protection of fundamental rights.

---

[40] Ministry of Electronics and Information Technology. (2020). *Data Protection Framework for India*. https://meity.gov.in
[41] Mueller, M. (2017). Will the Internet Fragment? Sovereignty, Globalization and Cyberspace. *Polity Press*.
[42] Freedom House. (2023). *Freedom on the Net Report*. https://freedomhouse.org
[43] ITU. (2020). *Measuring Digital Development: Facts and Figures 2020*. International Telecommunication Union.
[44] Internet Society. (2019). *Consolidation in the Internet Economy*. https://www.internetsociety.org
[45] Srnicek, N. (2016). *Platform Capitalism*. Polity Press.

 [ISSN 2581-5369]

VI. Conclusion

Digital sovereignty is a multidimensional concept that is reshaping the global digital landscape. As states grapple with issues of control, autonomy, and security in cyberspace, the contours of sovereignty are being redefined beyond physical borders into the digital realm. Whether pursued through regulation, technological innovation, or cyber defense, digital sovereignty reflects a growing awareness that control over digital infrastructure is essential for national sovereignty in the information age.

However, the path forward must balance national interests with global cooperation. Ensuring digital rights, maintaining an open and inclusive internet, and avoiding digital fragmentation are essential goals alongside the pursuit of sovereignty. The future of digital sovereignty lies in reconciling autonomy with interoperability, privacy with innovation, and control with collaboration.

*****

 [ISSN 2581-5369]