

DIGITAL SOVEREIGNTY: BALANCING NATIONAL INTERESTS AND GLOBAL INTERCONNECTIVITY

Dr Deepa Kaushik*
Aditya Tandon**

As the world progresses towards a digital era, the idea of digital sovereignty has never been more critical in landscapes pertaining to international law, global governance, geopolitics, and national security. Digital sovereignty means a country has the ultimate authority over its digital assets and the flow of information within its borders. The rapid growth of the internet, social media, and cloud computing has created new challenges for states seeking to assert their authority over digital space. This study analyses the evolution of digital sovereignty, its relationship with traditional notions of sovereignty, and the legal framework that governs digital activities. The paper also points out various implication that private individuals might come across when Acts and Bills related to personal data and digital privacy laws are presented either at national or international levels. This paper aims to enable a deeper understanding of the complex and ever-evolving concept of digital sovereignty and its relevance in the near future of governance, geopolitics, and legal framework. For the study, the information has been gathered from various primary as well as secondary sources in the form of statutes, articles, research papers, and opinions of jurists and people working in the fields of law, governance, geopolitics, digital eco-system etc.

Keywords- Governance, Digital Sovereignty, Geopolitics, Data Protection

Introduction

Digital sovereignty refers to a country or organization's ability to control its digital future. With respect to business houses, digital sovereignty can be interpreted as an enterprise's ability to control and manage its digital assets, data, technological infrastructure by reducing dependency on external factors. It is an ever-evolving complex concept tracing its roots from the broader notion of state sovereignty, which traditionally is referred to as a nation's authority to govern itself without foreign or external interferences. As we understand the concept digital sovereignty

* Associate Professor, Department of Law, Maharaja Agrasen Institute of Management Studies, Delhi

** Student Department of Law, MAIMS, Delhi

and the legalities related to the same, the entire population has been split into not only two but various segments and each of these segments having its own opinions which they feel is right. But every segment has a common belief that a shift from theoretical understanding to practical application is the key to realize the benefits of digital sovereignty thereby protecting data, privacy and strengthening democratic values.

However, in the current digital era, the traditional definition has taken a new form which extends to the control over digital infrastructure, technologies, data, and internet. Although playing such a pivotal role in the current generation, the concept of digital sovereignty lacks a universally accepted definitions, as its interpretation varies depending on the context.¹ Today India is the world's second biggest market for smartphones, and has among the most users on social media platforms. Many big tech firms have increasingly been caught in the government's crosshair- from a Facebook plan from free internet access being blocked, to content takedown requests to ordering google to change how it markets its android operating system (OS). Tech experts and right-wing members have raised concerns over increased state surveillance and tightening of freedoms in online spaces, stating that such actions on government's behalf will have enormous repercussions for the country's 1.4 billion population. The concept has proved itself to be of great concern for many policymakers across the globe as they feel that too much control is ceded in very few places, very less options in the tech market, and too much power in the hands of a few big tech giants, who control massive amounts of data about their users. Every country implements a differed approach to digital sovereignty. Due to such varied approach being opted by different states the geopolitical competition around the same has deepened between China, USA, and the EU.

In this paper the concept of digital sovereignty aims to enable enterprises to re-attain and to take calculated decision regarding their digital footprints as they face various dynamic limitations. The same provides countries and corporations to:

- Improve data protection, security and minimizing unauthorised access of information to very best ability

1 Philanthropy Communications. (2024, October 3). *What's Digital Sovereignty? Lessons from Brazil to the World: Implications, Risks, and Global Insights* | Internet Society Foundation. Internet Society Foundation. <https://www.isocfoundation.org/2024/10/whats-digital-sovereignty-lessons-from-brazil-to-the-world-implications-risks-and-global-insights/>

- Enhancing the compliances regarding the data privacy regulations that dictates location where the data is stored and the method by which it is being processed.
- Decreasing the amount of support that is taken from third-parties.

Role of Digital Sovereignty in State autonomy and the security of National infrastructures

As global networks emerged, countries have become more aware of their vulnerabilities and have expressed their voice in the matters of infrastructural control. European governments and policymakers are raising concerns, they want stronger parameters in place to use and store data locally, which will ensure European countries can manage their own data, improve their digital ecosystem, and increase digital sustainability. In India, there is a need to build and maintain Strong Data Centres (SDCs). Following are some of the suggestions that can be applied towards policy measures:

- Application of legal and regulatory frameworks to the systems of cloud computing and data sovereignty
- Restricting the transfer of crucial information such as health records, financial transaction would deem countries to be unsafe and implying a lack of data protection laws
- Licence regimes could be implemented over the cloud providers on the conditions that if the foreign based MNCs want to provide their service in the nation, they will be compelled to set-up local data centres.

The Ministry of Electronics and Information Technology (MEITY)² have expressed their intent for development of a State Data Centre (SDC)³ as part of core infrastructural development, which shall be playing a vital role in supporting the National E-Governance Plan (NeGP).⁴ The cloud providers have been requested by the government to create an “E-Discover” system

2 The Ministry of Electronics and Information Technology (MeitY) is responsible for formulating and implementing policies relating to information technology, electronics manufacturing, internet governance, and digital services in India. Available at <https://www.mygov.in/group/ministry-electronics-and-information-technology>

3 SDCs are multiple data centers set up in various states of India to provide fundamental IT infrastructure for various eGovernance programs.

4 NeGP aims at improving delivery of Government services to citizens and businesses with the following vision: “Make all Government services accessible to the common man in his locality, through common service delivery outlets and ensure efficiency, transparency & reliability of such services at affordable costs to realise the basic needs of the common man.”

which shall allow only a government entity to search and retrieve data stored in cloud system. The ministry has mandated data encryption as a 'standard security process' for all the digital data stored by the government in the cloud. MEITY has also asked the cloud providers to report any incidents related to unauthorized access of data by any government office holder or by the cloud provider. Ministry also stated that information stored on cloud should not be advertised or published by the provider to any other person or any organization without the permission of the government entity.⁵

Digital Sovereignty & Fundamental Right of individuals

In the current generation of digitalisation, in order to protect and safeguard fundamental rights of individuals, the current legal system need to adapt itself. Today, freedom of expression and privacy is closely interlinked with digital rights that allow people to access and use computers, other electronic devices and communications network. Digital technologies are not only transforming basic fundamental rights such as freedom of expression and access to information are exercised, protected, and violated but is also leading to the recognition of new rights. Hence, the law is shaping itself to embrace the new era with the development of digital rights and citizenship, allowing and regulating access to online information in a secure and transparent manner. As per UN Digital rights are just an extension of the already existing Universal Declaration of human Right. Despite this, supranational bodies such as the European Union (EU) are proposing a common framework, at least with respect to the right to personal data protection. For example, the General Data Protection Regulation (GDPR), which came into force in 2018, obliges member countries both to preserve citizens' personal data and to allow the free movement of data. In the USA, by contrast, there is no federal data protection law and each state applies different regulations. There are more than 100 countries in the world that have some kind of legislation protecting personal data and access to information on the Internet. In 2022, the European Commission made a Declaration on the protection of the rights of its citizens in the digital world, which covers the rights of all European citizens.⁶

5 Anushka. (2017, April 23), Digital Sovereignty: Meaning, Importance and Issues available at <https://www.gktoday.in/digital-sovereignty-meaning-importance-and-issues/>

6 Iberdrola. (2024). Digital rights, essential in the Internet age, available at <https://www.iberdrola.com/innovation/what-are-digital-rights>

Some instances where positive digital sovereignty involves states implementing the concept on behalf of their citizens. While sovereignty is generally associated with the rights of states, the very same concept has been applied by indigenous communities to assert control over resources and heritage that they argue should rightfully be theirs.

Impact on Business

The measure taken by governments to ensure application of data sovereignty is not only to ensure user sovereignty in digital space but also to constrain platform powers from big tech corporation which are most of the times foreign entities. A common manner in which such constraints can be imposed is through industrial policy and infrastructure building, thus making the private companies redundant. A prime example can be of the GAIA-X project of EU, which declared its objective to create a federated secure data infrastructure for the whole of Europe to compete with countries like US and China that house globe's most powerful tech giants. However, at the end of the day such projects end up involving US & Chinese players or their European subsidiaries, portraying the difficulty in pursuing the digital autonomy of citizens and states without a competitive digital market. Finally, countries fitting this model are likely to fine big corporations and put forward or at least debate strong market and *content regulations* to preserve competition and prevent hate speech, like France, Germany, the UK, and Brazil. Platform liability can also be enforced with more robust measures, such as Brazil's ban on Telegram because the company refused to cooperate with an investigation into neo-Nazi groups.⁷

National Perspective

The Indian government's path to digital sovereignty is primarily focused on data sovereignty – ensuring adequate protections for Indian users and ensuring that personal data is stored in-country. The Indian government started a consultation process with the key stakeholders to come up with a data protection policy. The objectives of this policy were to unlock the potential of the digital economy for India, to protect the data of Indian citizens, and to protect them from the state's unregulated control of their data. India has not reached its much-awaited stop in relation to digital sovereignty and that is the draft of Digital Personal Data Protection (DPDP)

7 Fratini, S., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2024). Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models available at <https://doi.org/10.1007/s44206-024-00146-7>

Rules⁸ release by MEITY. The DPDP Act, has been formulated after years of recommendations and judicial decisions that shaped the landscape of data protection. The start of this journey was the Justice A.P. Shah committee of 2011, which laid out the foundation for privacy laws to protect digital rights of individuals. The privacy laws in India reached new heights with the passing of the landmark judgement of *K.S. Puttaswamy (Retd.) Vs. Union of India*,⁹ where the judgement recognised right to privacy as a fundamental right. The current bill governs the processing of personal data by government companies incorporated in India, foreign companies dealing with personal data of individuals in India.¹⁰ These entities are obliged to process the collected data only with prior individual consent and for a specific and lawful purpose. They are also tasked to set up transparency and accountability measures to address individual complaints. The bill also includes a requirement for data localisation of sensitive personal data. The bill explains that information such as financial, biometric, caste, religious, political beliefs data is to fall under the category of sensitive personal data. As per the bill, all the earlier stated data should be stored in India and shall only be communicated outside the country having the explicit authorization of the person whose data is sent. The Indian government views the data localisation requirements as a necessity to respond to foreign tech companies generating revenue from the data of the Indian citizens. This phenomenon is also referred to as data colonialism by some local industrialists, academics, and politicians. This stance is supported by domestic civil society and big private players in India like the Reliance Jio and Paytm. However, there has been criticism from smaller digital players that data localisation would mean increased compliance costs. Data localisation could also have trade policy implications if other countries impose reciprocal measures

Global Perspective

As India wants to increase state power and access to data, but considers economic, rather than purely security interests. Its draft data localization law has recently been shelved, and the government's approach is broadly

8 These Rules mark the full operationalisation of the Digital Personal Data Protection Act, 2023 (DPDP Act). They place equal weight on individual rights and lawful data processing.

9 AIR 2018 SC (SUPP) 1841

10 Singh Khyati, Data Protection Frameworks of India and the US: Data Sovereignty vs Market Flexibility - MP-IDSA. (2025, March). Available at <https://www.idsa.in/publisher/issuebrief/data-protection-frameworks-of-india-and-the-us-data-sovereignty-vs-market-flexibility/>

framed as protecting critical infrastructure and data as an uprising in data breach is being noticed, and bolstering hosting capacity and the digital economy.

* **Asia-Pacific Countries**

The main drivers of measure of digital sovereignty in the countries like Australia, China, India, and Vietnam are to protect national security, citizens, and social stability; and economic protectionism to bolster domestic industry. Other motivations include safeguarding social and cultural norms and values (as defined by the state) and helping people control their data.

- China is a regional and global first-mover in defining, implementing, and exporting a state centred methodology to digital sovereignty, characterized by greater state control of the Internet and data localization. Other governments — for instance, Viet Nam — appear to be attracted to this model, and to the opportunities for greater investment in state capacity and the economy offered by China's Belt and Road Initiative.
- Australia's Cyber Security Strategy 2020 aims to spur "new sovereign Australian cyber capabilities and companies" and "promote innovation in sovereign cyber security research and development," yet the overall picture is an effort to balance national security interests with a liberalized trade agenda. Australia has yet to require data localization: Its national hosting strategy does not prescribe domestic ownership and control or localization of government data and was recently changed so that non-Australian-owned and based companies may qualify.¹¹

* **Europe**

EU and its member, France, Germany, and Italy — frame digital sovereignty primarily in the context of economic competitiveness, developing local industry, and protecting against cyberattacks. Although, EU has a great number of strong assets consisting of world-leading AI research community and a strong industry, it possesses certain detrimental weaknesses that is holding it back in the global race to develop new technologies. For instance, in the sector of AI technology EU is lacking behind US and China in terms of private investments. Also, the level at which companies and general public are adopting AI technologies, is significantly lower

11 CC BY-NC-SA 4.0 Navigating Digital Sovereignty and its Impact on the Internet. (2022) available at <https://www.internetsociety.org/wp-content/uploads/2022/11/Digital-Sovereignty.pdf>

than what is seen in US. US also attracts higher amount of AI talent and researchers and is also leading the race of patent applications. On the other hand, China is leading the race on data collection and access and has made monumental progress in developing latest hardware equipment such as supercomputers. Furthermore, the US and China are leading in regards patents on quantum-computing technologies, while Europe's level of investment in blockchain technologies and IoT is comparatively low

EU policymakers are designing measures to adapt EU industrial and technological capacity to the competitive environment. In February 20 the European Data Strategy was adopted which was a blueprint towards creation of data spaces to make sure that every possible data is made available for the betterment of economy and society, while also protecting the interests of individuals and organisations. EU has also adopted an approach for developing AI technologies that shall assure adherence to highest level of ethical standards and aims to lead the AI technologies race.¹²

* USA

The US has long been at the forefront of digital technologies. It has maintained its hegemony through industrial policy aimed at developing critical technologies, especially when faced with potential competitors, such as Japan in the 1980s. More recently, industrial policy has made a strong comeback in the US with the Inflation Reduction Act (IRA) and the Creating Helpful Incentives to Produce Semiconductors and Science (CHIPS) Act. Pushing the rhetoric of a “free and open internet” on the global stage, the American tech industry has largely relied on corporate self-regulation in their harvesting and use of data. The government-supported multi-stakeholder approach to global internet governance through organisations like the Internet Corporation for Assigned Names and Numbers (ICANN) has given its tech giants an outsized role in formulating global standards till this date.¹³

12 Madiega, T. (2020). *BRIEFING EPRS Ideas Paper Towards a more resilient EU*. Available at [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI\(2020\)651992_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf)

13 Musoni, M., Karkare, P., Teevan, C., & Domingo, E. (2023). *Global approaches to digital sovereignty: Competing definitions and contrasting policy*. <https://ecdpm.org/application/files/7816/8485/0476/Global-approaches-digital-sovereignty-competing-definitions-contrasting-policy-ECDPM-Discussion-Paper-344-2023.pdf>

International Cooperation for Digital Sovereignty

On September 29, 2021, the United States and the European Union's (EU) new Trade and Technology Council (TTC) held their first summit. Following the meeting, the U.S. and the EU declared their opposition to artificial intelligence (AI) that does not respect human rights and referenced rights-infringing systems, such as social scoring systems. During the meeting, the TTC clarified that *"The United States and European Union have significant concerns that authoritarian governments are piloting social scoring systems with an aim to implement social control at scale. These systems pose threats to fundamental freedoms and the rule of law, including through silencing speech, punishing peaceful assembly and other expressive activities, and reinforcing arbitrary or unlawful surveillance systems."*

Historically, with the development of the world wide web opportunities were created for the world to be interconnected as one large global digital ecosystem. Unfortunately, with the increasing mistrust among nations has caused for a rise in digital sovereignty, referring to a nation's ability to lay footwork to its digital destiny, which may as well include taking control over the entire AI supply chain, from data to hardware and software. A consequence of the trend toward greater digital sovereignty—which then drives the trend further—is increasing fear of being cut off from critical digital components such as computer chips and a lack of control over the international flow of citizens' data. These developments threaten existing forms of interconnectivity, causing markets for high technology to fragment and, to varying degrees, retrench back into the nation state.

Conclusion

The concept of digital sovereignty has emerged as a pivotal element in the global digital landscape, emphasizing a nation's authority over its digital assets and data privacy. As countries navigate the complexities of the digital era, the balance between national interests and global interconnectivity becomes increasingly essential. The need for robust legal frameworks, as seen in various approaches from major regions including the proactive stance of China, the EU's focus on economic competitiveness, and India's efforts to safeguard personal data highlights a growing awareness of vulnerabilities in digital infrastructure and the implications for national security. Digital sovereignty empowers individuals and organizations to control their digital environments while simultaneously confronting the challenges posed by dominant tech giants. The diversity of interpretations and implementations of digital sovereignty across the globe illustrates

the lack of a universal definition, further complicating engagements in an interconnected world. Continued prioritization of individual rights, data protection, and regulatory oversight is vital as governments seek to reclaim digital autonomy while fostering a competitive technological ecosystem. Ultimately, ensuring that digital sovereignty is exercised responsibly involves recognizing the fundamental rights of individuals and adapting legal systems to evolving digital realities, thereby reinforcing democratic values against the backdrop of increasing global digital interdependencies.