DIGITAL SOVEREIGNTY: THE LEGAL CHALLENGES OF COUNTRIES ATTEMPTING TO BAN OR HEAVILY RESTRICT GLOBAL SOCIAL MEDIA NETWORKS

Rohan Swaroop, Advocate, Delhi High Court

Tanu Swaroop, IIMT university, Meerut

ABSTRACT

The notion of digital sovereignty is becoming an essential concept of modern governance, expressing the desire of the states to have greater control over digital infrastructure, data, and platforms in their territories. The rapid growth of social media networks worldwide gave rise to heated discussions on the issues of national security, misinformation, data protection, cybercrimes, and interference of foreign entities. As a result, some countries opted to introduce bans or very strict regulations concerning such social media networks. Although the governments may justify such actions through the desire to preserve the public order, national interests, or cultural heritage, the regulations pose significant legal challenges for freedom of expression, right to access information, competition policy, international data transfer, and international trade relations. This paper attempts to analyze the legal challenges posed by the state regulation of social media networks, considering the experiences of different countries, such as India, China, European Union, Russia, Australia, and the US. The analysis shows that the intersection between domestic constitutional framework and international human rights law creates certain tensions. However, digital sovereignty represents a legitimate goal of the state, but very strict regulation causes conflicts with the requirements of international law of proportionality and necessity. According to the paper, sustainability in digital governance is achieved through balanced regulations rather than total prohibition, with accountability, judicial review, algorithm transparency, and international cooperation being highlighted. Through an assessment of the conflicting legal interests, the research adds value to existing scholarly debates regarding the reconciliation of state sovereignty and digital rights in the growing global information environment.

Keywords: Digital sovereignty, social media regulations, freedom of expression, international law, data governance, cybersecurity, platform regulations, digital rights.

1. Introduction

The digital revolution has changed the world of communication, trade, governance, and civic engagement. Social networking sites have become vital forums for politics, business transactions, learning, and cultural exchanges. [1]Sites like Facebook, X (formerly Twitter), Instagram, TikTok, YouTube, and WhatsApp offer instant communications beyond national borders, providing great opportunities for worldwide connections. But along with this, their growing significance has led to some major legal and political issues.

These issues have reinforced the idea of digital sovereignty, which involves a government's attempt to acquire more control over the digital infrastructure, data, and platforms in its territory. [2]Digital sovereignty implies an adaptation of the notion of state sovereignty into the context of cyberspace and revolves around the ability of a nation-state to manage digital technology in its interest and according to its laws.[3]

While the notion of digital sovereignty gains recognition as a legitimate political agenda, strict limitations imposed on the use of social networks globally often lead to constitutional and international law disputes. [4]Complete bans can violate the right to freedom of speech, access to information, and privacy, while having repercussions for international business and innovation.[5] Thus, states need to take into account both security and democratic concerns as well as international obligations.

The paper analyzes the legal difficulties involved in the efforts of governments to prohibit or limit social media sites globally. [6]The paper uses a comparative approach to analyze the efforts that different countries have made in relation to digital sovereignty while considering the problem of proportionality.

---

[1] Anthony Smith, "Freedom of Expression and Social Media: How Employers and Employees Can Benefit from Speech Policies Rooted in International Human Rights Law", 32 Indiana International & Comparative Law Review 629 (2022).
[2]Wolff Heintschel von Heinegg, "Legal Implications of Territorial Sovereignty in Cyberspace", NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) 7 (2012).
[3] A. Shokri, "Sovereignty in Cyberspace from the Viewpoint of International Law", Asian Journal of International Law 12 (2024).
[4] L. von Ditfurth, "The European Union's Pursuit of Digital Sovereignty Through Legislation", 14 Journal of Intellectual Property, Information Technology and E-Commerce Law (JIPITEC) 46 (2023).
[5] L. L. Rebelo, "Can Prior Censorship be a Necessary Tool for the Protection of Human Rights?", 40 American University International Law Review 615 (2025).
[6] M. F. Taşçı, "Another Click in the Wall: A Legal Analysis of the Proposed Turkish Social Media Ban for Children", Verfassungsblog, Nov. 14, 2024.

2. Digital Sovereignty

Digital sovereignty is the concept in which the state can govern digital technologies, data flows, and Internet-based services within the borders of the state without compromising its national security, economic interests, and the rights of its citizens.[7] This differs from the traditional concept of sovereignty, as this form of sovereignty is not limited to physical borders but rather expands into cyberspace, where information travels across borders almost immediately.[8]

Some of the key motivations for digital sovereignty in the current environment are:

1. Ensuring national security from cybersecurity threats.
2. Protecting against foreign political intervention.[9]
3. Control of misinformation and other negative content on the Internet.
4. Citizens' personal data protection.
5. Development of digital industries in the country.
6. Maintenance of culture and language.

The emergence of COVID-19 pandemic made it imperative for the governments to turn their focus toward digital governance, as social media became an essential tool of public communication and information dissemination during the crisis.[10]

But this does not mean that digital sovereignty will imply unlimited state control over online communications. The constitutions of most democratic countries provide that any state powers are limited by constitutional protection of human rights. [11]Hence, any legal regulation has to comply with the standards of legality, necessity, proportionality, and judicial review.[12]

---

[7] Julia Pohle and Thorsten Thiel, "Digital Sovereignty", 9 Internet Policy Review 4 (2020).
[8] P. M. Taylor, "Cyberspace and State Sovereignty: The Evolution of Boundaries in a Digital Age", 22 Journal of Conflict and Security Law 115 (2017).
[9] Tim Maurer, Cyber Mercenaries: The State, Hackers, and Power 42 (Cambridge University Press, Cambridge, 2018)
[10] S. R. Sharma, "Digital Governance during Crises: Lessons from the COVID-19 Pandemic", 56 Journal of the Indian Law Institute 204 (2021)
[11]Madhav Khosla, The Indian Constitution 88 (Oxford University Press, New Delhi, 2012)
[12]K. S. Puttaswamy v. Union of India, (2017) 10 SCC 1

3. Legal Basis for Government Regulation

There are different legal bases for regulation of digital platforms by governments. First, there is usually a constitutional and statutory authority for governments to legislate on public order, public morality, public health, and national security.[13] Laws on cybersecurity, telecommunications, data protection, and criminal law are some of the means through which governments regulate online platforms.[14]

States also have international legal rights to regulate internal matters. States are sovereign and equal, according to Article 2(1) of the Charter of the United Nations, which gives governments the right to make laws on matters of national interest. [15]It is now becoming common in international cybersecurity debates that states have regulatory powers over digital infrastructures.[16]

But there are limitations to those powers. There are legal limitations through international human rights law. As per Article 19 of the Universal Declaration of Human Rights and International Covenant on Civil and Political Rights, there is freedom of opinion and expression which includes the freedom to seek, receive and impart information and ideas through any media and regardless of frontiers.[17]

This means that governmental restrictions on these powers are subject to a test of proportionality, legality, and necessity. Total bans without sufficient justification will be unconstitutional.[18]

4. Different Legal Approaches

Different states have embraced different regulatory approaches, which differ from each other owing to different constitutional traditions, political systems, and security interests.

[13] M. P. Jain, Indian Constitutional Law 542 (LexisNexis, Nagpur, 8th ed., 2018).
[14] Apar Gupta, "Regulating the Digital Commons: A Study of India's IT Rules", 63 Journal of the Indian Law Institute 145 (2021).
[15] Charter of the United Nations, 1945, art. 2, para. 1.
[16] Michael N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 15 (Cambridge University Press, Cambridge, 2017).
[17] International Covenant on Civil and Political Rights, 1966, art. 19, G.A. Res. 2200A (XXI), 21 U.N. GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316 (1966).
[18] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.

China can be viewed as the state with the most developed model of digital sovereignty. Due to legislative regulation and technological control, various social media platforms available abroad are inaccessible, while similar services operating within China's territory fall under the jurisdiction of the nation's regulations. [19]The justification for such steps lies in the necessity of maintaining cybersecurity and national security; however, these steps raise criticism as the access to information is limited.

India has opted for a rather selective approach to the problem. Various digital applications originating from foreign countries have been restricted due to national security issues in cases when security of data or geopolitics was viewed as important.[20] At the same time, India has passed intermediary liability regulations obliging digital platforms to cooperate with governmental agencies, develop effective grievance redressal, and content moderation system.[21]

A rights-based approach is adopted in the European Union with an emphasis on accountability as opposed to prohibition. [22]In its attempt not to ban activities or technologies, but instead regulate them, Europe ensures transparency requirements, risk assessments, consumer protection, privacy protections, and platform liability. This model aims at fostering an open digital marketplace through regulation.

Russia has continued to embrace digital autonomy, such that it requires data localization and restricts certain foreign digital platforms. [23]While the justification of these moves is national cybersecurity and reduced dependency on foreign tech providers, there are concerns internationally regarding the restrictions on free media and online speech.

Market-oriented digital governance prevails in Australia and the United States along with some targeted legislative measures regarding online safety, privacy issues, protection of children, and national security. [24]The regulations do not involve any bans; instead, they aim at enhancing

[19] Rogier Creemers, "China's Conception of Cyber Sovereignty", 11 Journal of Cyber Policy 45 (2020)
[20] S. Narayan, "Geopolitics of Data: India's Ban on Chinese Applications", 55 Economic and Political Weekly 18 (2020).
[21] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
[22] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act).
[23] F. Leshchenko, "The Russian Sovereign Internet Law: A Comparative Study of Digital Autonomy", 15 Russian Law Journal 88 (2023).
[24] Online Safety Act 2021 (Act No. 76 of 2021, Australia).

platform liability.

5. Major Legal Issues

5.1 Freedom of Expression

Undoubtedly, one of the major legal issues is the issue of the right to freedom of expression. It should be noted that social media have now become primary spaces for political participation, journalism, academic discussion, and public activity. [25]Thus, complete governmental regulation might significantly impede the constitutional rights of free expression and democracy.[26]

Indeed, international human rights law always requires from the government that any restrictions on the right of expression are based on strict criteria of legality, necessity, and proportionality.[27]

5.2 Data Protection and Cross-Border Regulation of Data

Data transfers across countries pose yet another legal hurdle. Global social networks process the personal data of users in different jurisdictions, creating issues with regard to data protection, surveillance, and potential access by foreign governments to such data.[28]

A number of countries have sought to address this issue through imposing localization obligations, which require that certain types of personal data must stay in the country.[29] While these regulations may enhance regulatory oversight, they also increase costs and create problems with international trade deals in the sphere of e-commerce.[30]

5.3 Cybersecurity and National Security

National security is another strong basis for limiting global social media websites under

[25] J. Sunstein, "Social Media and the Future of Free Speech", 14 Harvard Law & Policy Review 301 (2020)
[26] Shreya Singhal v. Union of India, (2015) 5 SCC 1
[27] United Nations Human Rights Committee, General Comment No. 34 (Article 19: Freedoms of opinion and expression), U.N. Doc. CCPR/C/GC/34 (2011)
[28] Christopher Kuner, Transborder Data Flows and Data Privacy Law 85 (Oxford University Press, Oxford, 2013)
[29] The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023)
[30] Anupam Chander, "The Coming Data Wars: Data Localization, Data Sovereignty, and Cyber-Nationalism", 114 American Journal of International Law 152 (2020)

existing law. In modern times, governments claim that foreign-owned social media websites may pose cybersecurity risks in terms of exposing private information, conducting cyber espionage, engaging in campaigns of foreign influence, or disseminating misinformation which can undermine the functioning of democratic processes. [31]The increased use of social media websites during elections, wars, and crises has raised concerns about their role from the perspective of national security.

However, there are certain problems associated with the application of this justification in a legal manner. Democratic courts usually demand governments to provide credible evidence rather than just hypothetical concerns related to national security. Moreover, imposing total bans on social media websites without any clear procedure or oversight may violate such fundamental principles of constitutional law as judicial review and due process of law. [32]The other risk is the potential for abuse of national security exceptions by politicians who would like to limit the freedom of speech of dissenting groups or journalists.

Thus, the legal regulation in question should clearly differentiate between cybersecurity threats and political/ commercial conflicts.

5.4 Economic and International Trade Implications of Social Media Restrictions

Restrictions on social media networks around the world have major economic and international trade implications. Digital technologies are used by firms to conduct transactions across borders and advertise, innovate and become entrepreneurs. Hence, any restrictions on digital platforms can negatively impact domestic businesses, content makers and consumers.[33]

In terms of international law, restrictive digital practices may be related to international obligations in the realm of international digital trade within the context of WTO and regional trade agreements for digital services. While States have a right to regulate in accordance with legitimate purposes, such regulation must not constitute arbitrariness and discriminatory treatment towards foreign service suppliers as well as obstacles to international trade.[34]

[31] Michael N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 18 (Cambridge University Press, Cambridge, 2017).
[32] Anuradha Bhasin v. Union of India, AIR 2020 SC 1308.
[33] J. Sunstein, "Social Media and the Future of Free Speech", 14 Harvard Law & Policy Review 315 (2020).
[34] General Agreement on Trade in Services, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183.

Rapid growth of the digital economy has thus led to debates about international standards that would strike the balance between regulatory sovereignty and international competitiveness of the digital market place.

5.5 Jurisdictional and Enforcement Difficulties

Another important legal characteristic associated with the nature of social media is the fact that these services are by definition transnational. Digital services are usually deployed in several jurisdictions, whereas users, servers, and company headquarters can be situated in other jurisdictions.[35] As a result, issues related to jurisdiction, the application of laws, and enforcement become difficult.

The situation becomes complicated if the requirements of one state come into conflict with those of another state. [36]A platform might be obliged to delete certain content due to the laws of one nation while, at the same time, being guaranteed freedom of speech in another nation. Another example is that of conflicting requirements of data localization with obligations for data flow freedom.

As one can see, jurisdiction issues demonstrate that there are certain limits to the effectiveness of unilaterally regulation. Modern regulation relies on international cooperation and cooperation in the legal realm in particular.

6. Human Rights Approach

The connection between digital sovereignty and human rights constitutes perhaps the most significant debate in modern digital governance. International documents on human rights state that freedom of expression and access to information are basic prerequisites of democratic societies. [37]Internet access is increasingly considered a necessary condition for the exercise of civil, political, economic, and social rights.[38]

[35] Christopher Kuner, Transborder Data Flows and Data Privacy Law 92 (Oxford University Press, Oxford, 2013).
[36] Google Inc. v. Equustek Solutions Inc., 2017 SCC 34 (Canada).
[37] Universal Declaration of Human Rights, 1948, art. 19, G.A. Res. 217A (III), U.N. Doc A/810 at 71 (1948).
[38] United Nations Human Rights Council, Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet, U.N. Doc. A/HRC/32/L.20 (2016).

Governmental limitations of social media might have an effect on journalists, scholars, students, companies, NGOs, and ordinary citizens using digital communication means. However, overregulation may result in a lack of transparency, decrease access to various perspectives, and stifle innovation.[39]

Nevertheless, human rights laws do not prohibit any regulation. States are obliged to protect their citizens from different threats that may come from cyberspace, such as terrorism, pedophilia, criminal activity, hate speech, and disinformation.[40]

Some of the basic principles that international human rights institutions have been constantly reiterating as guidelines for proper digital regulation include:

1. Legality through transparent legislation.
2. Necessity from public interest.
3. Proportionality in government objectives and limitations.[41]
4. Judicial review by independent judges.
5. Accountability and transparency in the regulatory process.
6. Availability of remedies for those affected.

These principles form a crucial basis for assessing the conformity of limitations on social media to international law standards.[42]

7. Emerging Trends in Global Digital Governance

The field of digital governance is rapidly developing as states search for substitutes for the total ban of certain platforms. [43]While the traditional approach is still based on prohibitions, the

[39] Julia Pohle and Thorsten Thiel, "Digital Sovereignty and Human Rights: Balancing Security and Freedom", 9 Internet Policy Review 12 (2020)
[40] Michael N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 26 (Cambridge University Press, Cambridge, 2017).
[41] United Nations Human Rights Committee, General Comment No. 34 (Article 19: Freedoms of opinion and expression), U.N. Doc. Corporate/C/GC/34 (2011)
[42] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.
[43] G. Greenleaf, "The Future of Platform Regulation and Digital Governance", 15 Journal of Cyber Policy 102 (2024).

current one implies the adoption of regulatory mechanisms based on principles of transparency, accountability, and risk management.[44]

Among the emerging trends in legislation, there are new requirements for improving content moderation, making algorithms transparent, ensuring children's internet security, disclosing political advertisements, and cooperating with regulators. [45]AI governance is also closely connected with digital sovereignty in terms of automated content recommendations and algorithmic accountability.[46]

One more emerging trend is related to increased international cooperation. Cyber threats, fake news online, and problems of data protection have shown that the current issues need multilateral dialogue and regional cooperation.[47]

This shows that in the future, responsible platform governance will probably prevail over censorship and technological isolationism.[48]

8. Policy Recommendations

Digital sovereignty requires a balance between government interest and the constitution as well as international law. Several policy recommendations can be deduced from the above discussion.

First, there ought to be narrowly tailored legislation defining the conditions for applying the restriction. Vagueness or over-breadth of laws is bound to introduce uncertainty as well as potential for arbitrary application of the regulation.[49]

Second, the restrictions need to be proportionate to the identified threat. While temporary and targeted measures dealing with specific forms of unlawful activity are desirable, general

[44] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act).
[45] Apar Gupta, "The Shift from Censorship to Co-regulation of Intermediaries", 64 Journal of the Indian Law Institute 210 (2022).
[46] S. Benjamin, "Algorithmic Governance and the Constitutional Mandate of Accountability", 38 Harvard Journal of Law & Technology 145 (2025).
[47] United Nations General Assembly, Resolution on International Cooperation on Cyber-Security and Combating Disinformation, U.N. Doc. A/RES/79/112 (2025).
[48] Jack M. Balkin, "Free Speech in the Algorithmic Society: The Case Against Digital Isolationism", 137 Harvard Law Review 874 (2024).
[49] Shreya Singhal v. Union of India, (2015) 5 SCC 1.

blanket bans on all users irrespective of their individual behavior are not.[50]

Third, important regulatory actions must be subjected to independent judicial review. The courts are vital for maintaining governmental accountability and constitutional rights.

Fourth, there should be transparency of the decisions by the regulator in explaining the enforcement actions taken.[51]

Fifth, governments should promote collaboration among various stakeholders including digital platforms, NGOs, scholars and other industry participants during the process of creating the new laws.[52]

Lastly, international cooperation should remain an important element of digital governance.[53] There will be harmonization of regulations on cybersecurity, privacy, algorithmic accountability and cross border data governance issues, thereby reducing regulatory fragmentation.[54]

9. Conclusion

In the era of the twenty-first century, the concept of digital sovereignty becomes absolutely necessary for effective governance in the face of the legal, political, and technological challenges of global digital platforms. [55]There is no doubt that governments can regulate online activities in order to secure national security, social order, cybersecurity, and citizens' personal data. However, this regulation should be conducted under legal and international legal limitations protecting people's rights and democratic values.[56]

As comparative law shows, there are many different ways that states can follow in terms of regulating digital platforms from restrictive measures towards platforms to human rights-

[50] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.
[51] L. L. Rebelo, "Can Prior Censorship be a Necessary Tool for the Protection of Human Rights?", 40 American University International Law Review 615 (2025)
[52] Apar Gupta, "The Shift from Censorship to Co-regulation of Intermediaries", 64 Journal of the Indian Law Institute 210 (2022).
[53] United Nations General Assembly, Resolution on International Cooperation on Cyber-Security and Combating Disinformation, U.N. Doc. A/RES/79/112 (2025).
[54] Jack M. Balkin, "Free Speech in the Algorithmic Society: The Case Against Digital Isolationism", 137 Harvard Law Review 874 (2024).
[55] Julia Pohle and Thorsten Thiel, "Digital Sovereignty", 9 Internet Policy Review 4 (2020).
[56] United Nations Human Rights Committee, General Comment No. 34 (Article 19: Freedoms of opinion and expression), U.N. Doc. CCPR/C/GC/34 (2011)

oriented models of regulation that focus on accountability and transparency.[57] Despite significant differences between national contexts, there are some basic legal principles that still govern proper digital regulation legality, necessity, proportionality, judicial review, and human rights.

Instead of focusing on platform bans, digital governance in the future should rely more on regulation that would address the needs of security but, at the same time, would protect such vital values as freedom of speech, innovation, economic growth, and international cooperation. [58]This goal can be achieved only through continuous dialogue between governments, tech companies, international organizations, and civil society.

[57] Nehaluddin Ahmad, Faizah Rahim et al., "Bridging Legal Theory and Comparative Law: Implications for Cyber Law and Its Role in Modern Society", 17 Journal of East Asia and International Law 159 (2024).
[58] Jack M. Balkin, "Free Speech in the Algorithmic Society: The Case Against Digital Isolationism", 137 Harvard Law Review 874 (2024).