"Digital Sovereignty and Constitutional Autonomy: Reconsidering State Power in the Age of Transnational Internet Governance"

SUBMITTED TO :- **Dr. BHAWNA BATRA**

SUBMITTED BY :- **NANDINI GAUTHAM** A03104426058

AMITY UNIVERSITY UTTAR PRADESH

AMITY LAW SCHOOL NOIDA

ABSTRACT

Digital sovereignty has emerged as a defining challenge for modern states, especially as public administration, economic stability, communication, and national security increasingly rely on privately managed networks and a globally distributed digital landscape. However, true sovereignty in the digital age cannot be defined simply by where a server is physically located or a government's ability to block certain online services. The reality is far more complex: data might be stored in one country, managed by a company headquartered in another, processed via infrastructure spanning multiple jurisdictions, and accessed by authorities operating under entirely different legal frameworks. These layers of complexity disrupt the traditional link between physical territory, state authority, and constitutional accountability.

This paper explores the intersection of digital sovereignty and constitutional autonomy, utilizing a comparative analysis centered on India with meaningful references to the European Union and the United States. It examines critical issues such as cross-border data flows, data localization, cloud governance, platform regulation, privacy, and freedom of expression. It also addresses the risks inherent when either state authorities or private tech giants wield excessive control over digital ecosystems. By looking at Indian constitutional rulings on privacy and internet restrictions, this study assesses how state actions should be constrained, even when justified by security or administrative necessity.[1] Recent developments in Indian cloud governance—notably the March 2026 framework designed to identify sensitive government systems and dictate deployment options—serve as a practical example of the growing push for tighter control over critical public data.[2]

The central argument of this paper is that meaningful digital sovereignty should not be mistaken for digital isolation. Instead, it should be viewed as a state's ability to make and enforce legitimate public policy while simultaneously protecting constitutional rights, maintaining technical resilience, ensuring democratic oversight, and fostering international cooperation. To this end, India should move toward a risk-based approach: implementing stronger safeguards for sensitive public systems, ensuring restrictions are both accountable and proportionate, establishing transparent rules for cross-border transfers, allowing for

[1] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 : AIR 2017 SC 4161; *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637 : AIR 2020 SC 1308.

[2] Ministry of Electronics and Information Technology (MeitY), Government of India, framework on cloud deployment options for government applications and databases (Mar. 2026), as reported in "Desi Data to Get Top Secret & A-B Sovereign Cover under New Cloud Rules", *The Economic Times*, Mar. 27, 2026. The precise legal status

of the document is yet to be verified against official notifications.

independent review, and prioritizing interoperability to avoid becoming permanently tethered to a handful of global providers.

INTRODUCTION

The rise of the internet has fundamentally unsettled the territorial logic upon which public law was built. While a government can regulate behavior within its physical borders, the very infrastructure enabling that behavior is often owned by multinational corporations, hosted in foreign data centers, routed through various countries, and governed by contracts written under foreign legal systems.[3] For instance, a person in India might communicate via an app operated by a foreign company, with their data backed up across several regions and business decisions made in a different part of the world. This creates a persistent friction between the territorial nature of constitutional authority and the borderless reality of digital life.

This mismatch creates significant stakes for the state. Public institutions manage sensitive records; hospitals and financial networks depend on interconnected systems; elections and public discourse happen on private platforms; and cyber threats can traverse borders in an instant. A state that lacks access to secure infrastructure or the power to enforce its own laws may find its formal sovereignty diminished in practice. A sudden disruption to a cloud provider, a change in a platform's terms of service, or a foreign court order affecting stored information can impact citizens who were never part of the decision-making process. Consequently, digital dependence has become a critical issue for administrative continuity, economic security, and democratic integrity.

At the same time, broad claims of "digital sovereignty" can easily be weaponized to justify censorship, mass surveillance, unnecessary data retention, or the suppression of lawful communication.[4] The rhetoric of national security is often used to implement measures that far exceed the actual risks involved. Similarly, data localization is sometimes marketed as a total privacy solution, even when the state or the service provider can access that data without sufficient safeguards. The core challenge, therefore, is not merely increasing state control, but learning how to distinguish legitimate public capacity from the exercise of arbitrary power.

---

[3] Jack Goldsmith & Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press, New York, 2006); Jennifer Daskal, "The Un-Territoriality of Data", 125 *Yale L.J.* 326 (2015).

[4] Julia Pohle & Thorsten Thiel, "Digital Sovereignty", 9(4) *Internet Policy Review* (2020), DOI: 10.14763/2020.4.1532.

The fundamental question is not whether the state should have authority over digital systems, but how that authority is designed and limited. Constitutional autonomy requires more than just the power to command; it requires that public power remains legally authorized, subject to review, proportionate, and compatible with fundamental rights.[5] A similar tension exists regarding private platforms, whose control over search engines, app stores, cloud services, and online communication deeply influences the practical choices available to citizens, businesses, and governments alike.[6]

This paper addresses three interconnected questions: First, how do we define digital sovereignty when data and infrastructure are inherently transnational? Second, how can constitutional principles limit state power in the digital realm without undermining necessary security and governance? Third, what lessons can India draw from the European Union's rights-centered approach to data transfers[7] and the United States' model regarding lawful access and technology markets?[8] Using doctrinal and comparative analysis, this study examines constitutional provisions, statutes, policy frameworks, and judicial decisions, while acknowledging the rapid pace of digital regulation.

The discussion is organized into seven parts. It begins by distinguishing the various dimensions of digital sovereignty, followed by an exploration of constitutional autonomy and fundamental rights. It then moves into an analysis of cross-border data flows and cloud governance, before concluding with a discussion of India's evolving regulatory landscape and its digital public infrastructure. The fifth section compares various approaches taken by the European Union and the United States, while the sixth examines the complexities of transnational internet governance and the influence of private platforms. The final part proposes a constitutional model for India, built upon practical technological capacity, accountability, and risk-sensitive safeguards.

[5] Aharon Barak, *Proportionality: Constitutional Rights and their Limitations* (Cambridge University Press, Cambridge, 2012); *see also Puttaswamy (Privacy)*, supra note 1.

[6] Kate Klonick, "The New Governors: The People, Rules, and Processes Governing Online Speech", 131 *Harv. L. Rev.* 1598 (2018).

[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2016 O.J. (L 119) 1.

[8] Clarifying Lawful Overseas Use of Data Act, 2018, Pub. L. No. 115-141, div. V, 132 Stat. 1213 (2018) (codified at 18 U.S.C. § 2713).

1. UNDERSTANDING DIGITAL SOVEREIGNTY BEYOND TERRITORIAL CONTROL

Digital sovereignty is frequently used to describe a state's power to control its digital infrastructure, data, platforms, and the rules that govern online activity. The term is popular because it bridges digital policy with traditional concepts of national independence and public authority.[9] However, this label can often mask a variety of different goals: securing national security, ensuring public data is subject to domestic laws, building local technological strength, protecting personal privacy, regulating massive platforms, and reducing reliance on foreign vendors. While these objectives often overlap, they are not the same. For instance, a policy meant to boost local industry might not actually protect privacy, just as a privacy measure might not require data to be stored locally.

A more nuanced analysis suggests at least four distinct dimensions. Territorial sovereignty focuses on where data and infrastructure are physically located. Jurisdictional sovereignty deals with which laws apply and which courts have the authority to issue binding orders. Operational sovereignty concerns whether institutions can access, secure, migrate, and recover their systems without being tied to a single supplier. Finally, constitutional sovereignty looks at whether the exercise of public authority remains accountable to the people and bound by constitutional rights. Each dimension addresses a different challenge, and a state might be strong in one area while remaining dangerously vulnerable in another.

Simply having a server located within national borders does not automatically grant data sovereignty. A foreign provider might still hold technical control, manage encryption keys, maintain administrative access, or hold contractual rights that dictate who can access information. Furthermore, software often depends on updates, licenses, or security services managed from abroad. On the other hand, data stored in a different country can still be protected through enforceable contracts, robust encryption, independent oversight, and reliable legal remedies. In short, location is just one part of control, not the whole picture.[10]

Digital sovereignty also operates on both public and private levels. The public dimension involves a state's capacity to perform lawful duties, protect vital systems, and enforce its laws. The private dimension involves the power held by tech companies over communication,

[9] Luciano Floridi, "The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU", 33 *Philosophy & Technology* 369 (2020); *see also* Pohle & Thiel, supra note 4.

[10] Anupam Chander & Uyên P. Lê, "Data Nationalism", 64 *Emory L.J.* 677 (2015); *see also* Daskal, supra note 3.

infrastructure, markets, and data.[11] These two sides are deeply intertwined. A government might rely on a private cloud provider to run public services, even as a platform relies on state permission to operate in a market. This relationship is often a complex mix of cooperation, competition, and conflict.

It is also important not to confuse digital sovereignty with technological autarky. It is unrealistic for any state to produce every single component of the digital economy—from semiconductors and network gear to operating systems and cybersecurity tools—without incurring massive costs and losing efficiency. Total self-sufficiency is not a

requirement for meaningful autonomy. A more practical goal is to avoid unmanageable dependencies, maintain viable alternatives whenever possible, and ensure that essential services remain secure and functional during political or commercial disputes.[12]

Additionally, we must distinguish between sovereignty over systems and control over people. A government might require its agencies to use secure, domestic infrastructure without claiming absolute authority over every piece of personal data generated by its citizens. A constitutional government views individuals as rights-holders, not just as data sources for the state. Therefore, digital sovereignty is only legitimate if it strengthens public capacity without stripping away the privacy, dignity, and freedom of the people whose information is being processed.[13]

These distinctions clarify why the success of digital sovereignty policies cannot be judged solely by the number of local data centers or the amount of data stored domestically. More meaningful indicators include a state's ability to recover from an incident, enforce security requirements, switch providers, challenge illegal access, and maintain services without facing arbitrary interference. The true measure is effective, accountable control, not mere territorial symbolism.

2. CONSTITUTIONAL AUTONOMY, PRIVACY AND THE LIMITS OF STATE POWER

The Indian Constitution does not feature a single, standalone provision for "digital sovereignty." Instead, the framework is woven into fundamental rights, institutional

---

[11] Julie E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press, New York, 2019).

[12] Milton L. Mueller, *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace* (Polity Press, Cambridge, 2017).

[13] *Puttaswamy (Privacy)*, supra note 1.

accountability, and the principles that limit state power. Article 21 protects life and personal liberty; Article 19 protects essential freedoms like speech, expression, and the right to conduct business; and Articles 32 and 226 provide the pathways for constitutional review.[14] Furthermore, Article 14's guarantee against arbitrary state action is critical when digital rules are being designed or enforced.[15] Together, these provisions mandate that public authorities must justify any use of power that impacts individuals in the digital realm.

In the landmark case of *Justice K.S. Puttaswamy (Retd.) v Union of India*, the Supreme Court recognized privacy as a fundamental right.[16] In a digital age, this includes concerns regarding how personal information is collected, aggregated, inferred, and used. Data that seems harmless on its own can reveal deeply intimate patterns once it is combined with other records. When you combine location history, financial records, health data, and communication metadata, you get a strikingly detailed picture of a person's entire life.[17] Because of this, a constitutional approach cannot just look at whether a specific piece of data was collected; it must also examine the scale of that collection, why it is being processed, the risk of linking different datasets together, and the potential fallout if that data is misused. Privacy doesn't mean the state is strictly prohibited from collecting data. Governments genuinely need information to manage benefits, stop fraud, plan public services, and investigate serious crimes. The real constitutional question is whether any interference with privacy has a legal basis and serves a legitimate goal through methods that are both necessary and proportionate.[18] The state should be able to justify why it needs certain information, prove that there aren't less intrusive ways to get it, and explain who can access it, how long it will be kept, and what happens if things go wrong.[19] Simply claiming that data collection makes things more "efficient" isn't a good enough answer to these questions.

The distinction between collecting data and actually using it is vital. Information gathered for one reason might later be repurposed, shared with a different agency, or merged with an

[14] The Constitution of India, arts. 19, 21, 32 and 226.

[15] *E.P. Royappa v. State of Tamil Nadu*, (1974) 4 SCC 3 : AIR 1974 SC 555; *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248 : AIR 1978 SC 597.

[16] *Puttaswamy (Privacy)*, supra note 1.

[17] Daniel J. Solove, "A Taxonomy of Privacy", 154 *U. Pa. L. Rev.* 477 (2006).

[18] *Puttaswamy (Privacy)*, supra note 1; *Modern Dental College & Research Centre v. State of Madhya Pradesh*, (2016) 7 SCC 353 : AIR 2016 SC 2601.

[19] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Ministry of Electronics and Information Technology, Government of India, July 2018).

unrelated database. This kind of "function creep" often happens so gradually that no single decision feels particularly intrusive.[20] To prevent the state from slowly expanding its power beyond its original mandate, there must be clear limits on purpose, strict access controls, audit logs, and rules against unauthorized sharing. If a new use of data significantly changes its impact on people, it needs to be backed by proper legal authority and careful scrutiny.

The *Anuradha Bhasin v Union of India* case is a landmark because it addressed internet restrictions in Jammu and Kashmir.[21] The Supreme Court recognized that speech and commerce happening online deserve constitutional protection, emphasizing the need for proportionality, the publication of official orders, and the ability to review restrictions. This case proved that internet access isn't just a technical convenience that a government can switch off without consequence. In today's world, the internet is how people work, learn, stay informed, participate in democracy, and maintain their social and professional lives.

Internet shutdowns can impact massive numbers of people, even if the intended goal was to target a specific area or activity. These restrictions can derail education, healthcare, business, journalism, and access to essential government services. Therefore, a constitutional analysis must ask if a restriction is limited in time and geography, whether there were less disruptive options available, and if the reasoning and review processes are transparent. While emergency powers may sometimes be necessary, they shouldn't become a routine way to manage digital systems just because they are harder to regulate through standard legal channels.[22]

The *Shreya Singhal v Union of India* case serves as another reminder that online expression must meet constitutional standards.[23] The Supreme Court struck down Section 66A of the Information Technology Act, partly because its vague wording created a "chilling effect" on free speech.[24] The broader lesson here is that digital regulations must use clear legal standards so people aren't left guessing whether their lawful speech might lead to punishment. Vague rules often lead platforms to over-censor content to avoid the risk of penalties.

Ultimately, constitutional autonomy should be viewed as "disciplined state capacity." The state must be strong enough to protect its systems and enforce the law, but citizens must retain the right to challenge the legal basis and consequences of those actions. Transparency, independent

[20] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 SCC 1 : AIR 2018 SC 1841.

[21] *Anuradha Bhasin*, supra note 1.

[22] The Telecommunications Act, 2023 (Act 44 of 2023), s. 20; *Anuradha Bhasin*, supra note 1.

[23] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 : AIR 2015 SC 1523.

[24] The Information Technology Act, 2000 (Act 21 of 2000), s. 66A (struck down).

oversight, judicial review, and effective legal remedies are not hindrances to sovereignty; rather, they are what separate a true constitutional government from a system of unchecked control.[25] A digital policy that boosts administrative power at the expense of accountability might make the state machinery run more smoothly, but it undermines the very essence of constitutional governance.

3. CROSS-BORDER DATA FLOWS, LOCALISATION AND THE CLOUD

Cross-border data flows are the backbone of modern commerce, scientific research, global communication, and cloud computing. A single business might use one provider for customer support, another for processing payments, and a third for data storage. Cloud applications often replicate information across different regions to prevent downtime, and security services might analyze traffic from multiple global locations. Researchers collaborate across borders, and citizens often use services provided by companies that have no physical presence in their own country. While these setups increase reliability and lower costs, they make it much harder to figure out which laws apply and which authorities have the right to access data.[26]

A company might face a lawful data request from one government while simultaneously being bound by privacy or secrecy laws in another. Businesses often find themselves caught between legal regimes that don't align, forced to choose between preserving records or disclosing them.[27] For individuals, it can be incredibly difficult to know which authority to turn to for a complaint or a remedy. When the service provider, the user, the data itself, and the physical infrastructure are all in different jurisdictions, the old idea that one country's law governs an entire relationship starts to fall apart.

Data localization is one way to address this. By requiring certain types of data to be stored or processed within a country's borders, governments can ensure better regulatory access, operational continuity, and national security. For highly sensitive public records, requiring localization—or using designated sovereign infrastructure—can be a sensible part of managing national risk. It can also help ensure that public institutions maintain direct contractual and operational ties with providers that fall under domestic supervision. However, these benefits depend far more on how things are implemented than on where the data is physically located. Universal localization requirements can impose heavy costs, particularly on smaller businesses

---

[25] Barak, supra note 5; *Puttaswamy (Privacy)*, supra note 1.

[26] Chander & Lê, supra note 10; Daskal, supra note 3.

[27] GDPR, supra note 7, art. 48; CLOUD Act, supra note 8.

that depend on global cloud services. Such mandates can limit access to efficient infrastructure, fragment services, and make it much harder for companies to operate on an international scale.[28] Furthermore, localization can create concentrated risks if data is stored in just a few facilities or if domestic infrastructure lacks sufficient redundancy. A country might end up with more data physically within its borders, yet have fewer reliable ways to recover it following a major outage or cyberattack.

A more productive question is which specific risks justify which particular safeguards. Public records involving identity, taxation, the courts, payments, or critical infrastructure may require much stricter controls than ordinary, low-risk commercial information. These controls could include domestic storage, encryption with keys managed by an accountable Indian entity, segmented access, audit logs, disaster-recovery protocols, incident reporting, and thoroughly tested migration plans.[29] These steps address practical risks that physical location alone cannot solve. They also allow the level of regulation to match the sensitivity and potential fallout of a data breach.

India's government-cloud program, GI Cloud or MeghRaj, represents an effort to provide a common infrastructure for public services.[30] The March 2026 MeitY document regarding cloud deployment options is particularly relevant here, as it maps sensitive categories of government data and applications—such as Aadhaar, e-Courts, PAN, and UPI—to government providers or sovereign-cloud options when required, alongside safeguards like regular backups and disaster recovery.[31] This shows a practical shift toward offering differentiated protection for high-risk public systems. However, before treating such policies as legally binding, their precise status and any subsequent notifications should be verified.

The cloud example also demonstrates that sovereignty depends on procurement and architecture just as much as it does on legislation. Government contracts must clearly identify who controls encryption keys, where administrators are allowed to operate from, which subcontractors are involved, how foreign legal demands will be managed, and how data can be

[28] Chander & Lê, supra note 10.

[29] Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics and Information Technology, Directions under Sub-section (6) of Section 70B of the Information Technology Act, 2000 relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe & Trusted Internet, No. 20(3)/2022-CERT-In (Apr. 28, 2022).

[30] Department of Electronics and Information Technology (now MeitY), Government of India, *GI Cloud (MeghRaj): Strategic Direction Paper and Adoption and Implementation Roadmap* (2013).

[31] MeitY framework, supra note 2.

moved to a different provider. Contracts should also specify breach notification protocols, service availability, independent audits, data deletion, and the return of records once an engagement ends. Without these specific conditions, a state might pay for a domestic cloud only to find itself locked into an external vendor's technical and contractual whims.[32]

Resilience is another vital component of cloud sovereignty. A secure system is not automatically a resilient one. If a public service relies on a single vendor, network, or region, an outage can block access even if no data has been stolen. Critical systems need tested backup arrangements, clear recovery-time objectives, continuity procedures, and defined responsibilities for restoring service. Rather than simply relying on the assurances found in procurement documents, the government should periodically test whether it can actually migrate workloads and recover data in a real-world scenario.

Cross-border governance should also acknowledge that cooperation is essential. Cybercrime investigations, fraud prevention, and responses to large-scale attacks often rely on technical assistance or evidence from abroad. A policy that makes international transfers practically impossible could end up obstructing legitimate investigations and international cooperation.[33] The goal should be to facilitate controlled and accountable transfers—complete with clear conditions and remedies—rather than assuming that national security is best served by isolating data from all external systems.

4. INDIA'S EMERGING FRAMEWORK: DATA PROTECTION, PUBLIC INFRASTRUCTURE AND PLATFORM GOVERNANCE

India's digital policy is shaped by several overlapping frameworks rather than a single, unified sovereignty code. The Digital Personal Data Protection Act, 2023, along with the Digital Personal Data Protection Rules, 2025, provides a statutory structure for processing digital personal data.[34] Its actual application must be understood in light of specific commencement timelines and subsequent notifications. Notably, the Act's approach to cross-border transfers is not a blanket rule requiring all personal data to stay in India; instead, transfer restrictions and government powers operate within a specific statutory framework.[35] This distinction is

[32] Ministry of Finance, Department of Expenditure, Government of India, *General Financial Rules, 2017*, r. 144.

[33] Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185, arts. 23–35.

[34] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023); The Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), dated Nov. 13, 2025.

[35] DPDP Act and Rules, supra note 34, s. 16 (Act) and r. 15 (Rules).

important, as public debate often mistakenly equates data protection with universal localization.

Data protection should be judged not just by the existence of a law, but by how those protections work in the real world. Individuals need to know what information is being collected, why it is being processed, and how they can exercise their rights. Notices should be easy to understand, rather than being written in a technical jargon that is "available" but practically impossible to grasp. Grievance mechanisms must be user-friendly, and institutions must

have the actual capacity to investigate complaints and enforce corrective measures.[36] Rights that cannot be understood or enforced offer very little practical protection.

While consent is important, it isn't a complete solution in situations where services are essential, bargaining power is lopsided, or individuals cannot realistically refuse data processing. For instance, a person applying for public benefits may have very little meaningful choice when asked to provide required information. Similarly, a user might technically agree to a platform's terms while having no real alternative.[37] In these contexts, legal rules regarding purpose, security, necessity, and accountability remain vital, even when consent has been obtained. The true strength of a data protection system isn't just about whether someone clicked a "consent" box; it's about how well the system manages underlying power imbalances.

India's digital public infrastructure—spanning Aadhaar, UPI, DigiLocker, and various connected public services—shows just how much shared digital architecture can achieve in large-scale service delivery.[38] Digital identity and payment systems can strip away friction, making essential services more accessible and enabling rapid transfers. By using standardized interfaces, different institutions can work together seamlessly without the need to build entirely new systems from scratch. These are massive public wins, particularly in a country where sheer scale and administrative complexity often make service delivery a struggle.

However, this same architecture makes careful design even more critical. While interoperability and data reuse prevent duplication, linked systems also mean that a single breach, an incorrect record, or unauthorized access can have a massive ripple effect. If one identifier becomes the master key to multiple services, a single error can spread across several

---

[36] DPDP Act, supra note 34, ss. 5 and 13.

[37] DPDP Act, supra note 34, ss. 6–7.

[38] The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (Act 18 of 2016); The Payment and Settlement Systems Act, 2007 (Act 51 of 2007); *see also Puttaswamy (Aadhaar)*, supra note 20.

institutions. Similarly, if a payment system or identity service goes down, it can impact millions of people all at once. Because of this, security, error-correction mechanisms, fallback procedures, and independent audits must be treated as fundamental design requirements, not just optional add-ons implemented after the fact.[39]

Digital public infrastructure also brings the risk of exclusion. Many people still lack reliable internet, proper devices, digital literacy, or even up-to-date records. Technical glitches, biometric failures, or inaccurate data can effectively lock an otherwise eligible person out of the services they need.[40] A sovereignty strategy that focuses solely on controlling infrastructure might miss these very real, practical harms. In a constitutional democracy, digital systems must be backed by accessible alternatives, human assistance, and reliable ways to fix errors—especially when these systems determine access to essential life benefits.

Then there is the issue of platform regulation. Search engines, app stores, social media, and cloud providers hold immense power over how people communicate and how businesses find customers. In the Android proceedings involving Google, Indian competition authorities looked closely at how pre-installed apps, default settings, and app distribution affect the market.[41] While competition law and constitutional law tackle different issues, this case proves that digital power isn't just a state matter. Private gatekeepers can heavily influence consumer choice, market access, and the actual availability of alternatives.

India's real challenge lies in coordinating a web of privacy, cybersecurity, competition, telecom, intermediary, and procurement rules without turning every issue into a reason for more centralized control.[42] When institutions overlap too much, it creates uncertainty for businesses and inconsistent results for users. To avoid this, there needs to be clear statutory responsibility, published standards, well-reasoned decisions, and strong coordination mechanisms that respect specialized expertise rather than duplicating work. A framework that is easy for both citizens and businesses to understand is far more likely to encourage compliance than a messy patchwork of vague obligations.

[39] DPDP Act, supra note 34, s. 8(5)–(6).

[40] Reetika Khera (ed.), *Dissent on Aadhaar: Big Data Meets Big Brother* (Orient BlackSwan, Hyderabad, 2019).

[41] The Competition Act, 2002 (Act 12 of 2003), s. 4; *Umar Javeed v. Google LLC*, Case No. 39 of 2018 (Competition Commission of India, Oct. 20, 2022); *Google LLC v. Competition Commission of India*, Competition Appeal (AT) No. 1 of 2023 (National Company Law Appellate Tribunal, Mar. 29, 2023).

[42] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), dated Feb. 25, 2021.

The balance between innovation and regulation must also be managed with care. If rules are too rigid, they drive up costs for smaller firms, inadvertently helping the biggest players who have the resources to handle heavy compliance burdens. On the flip side, weak safeguards can destroy public trust and leave people vulnerable to harms that undermine the legitimacy of digital services entirely. A balanced approach should identify the specific risks that justify intervention, allow room for secure innovation, and regularly update rules as technology and business models evolve.

5. COMPARATIVE PERSPECTIVE: THE EUROPEAN UNION AND THE UNITED STATES

The European Union provides a useful comparison, particularly in how its data protection framework treats personal data as a fundamental right while still allowing for international transfers under specific conditions.[43] The General Data Protection Regulation (GDPR) uses tools like adequacy decisions and standard contractual clauses to manage this.[44] The core philosophy isn't that information should never leave the region, but rather that moving it shouldn't strip individuals of the protections their legal system guarantees them. In this sense, transfer rules act as a way to extend accountability across borders rather than just acting as a barrier to information flow.[45]

The Court of Justice of the EU's *Schrems II* judgment highlighted a vital point: it is not enough to just make contractual promises; one must also assess whether foreign government access is a practical threat.[46] The case showed that contracts might not be enough if the recipient is subject to laws that undermine the very protections being promised. This doesn't mean every international transfer is illegal, but it does mean that the legal and practical reality of the receiving country matters when deciding if safeguards are actually effective.

The EU Data Act also addresses a related concern: access to non-personal data and requests from foreign authorities for data held within the Union.[47] This approach recognizes that digital sovereignty isn't just about personal privacy—it's also about maintaining control over

[43] Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 391, art. 8.

[44] GDPR, supra note 7, arts. 45–46.

[45] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press, New York, 2020).

[46] Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd. and Maximillian Schrems*, ECLI:EU:C:2020:559 (Court of Justice of the European Union, July 16, 2020).

[47] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act), 2023 O.J. (L 2023/2854), art. 32.

industrial, commercial, and public-sector information. Rules regarding interoperability and cloud switching are also key, as they help prevent "vendor lock-in."[48] The ability to move data and applications easily reduces the risk of an organization becoming trapped by technical or contractual barriers.

The European model offers several lessons for India. Most importantly, cross-border transfer policy can focus on creating enforceable safeguards rather than assuming that physical location is the only way to ensure protection.

Second, when data crosses borders, having independent oversight and clear ways to seek remedies is essential. Third, digital sovereignty is also about interoperability and the right to switch providers, as these ensure people aren't locked into a single service. However, the EU's model is built on specific institutions, legal traditions, and market structures. It shouldn't be blindly copied without considering India's own administrative capacity and constitutional framework.

The United States offers a different perspective. Its CLOUD Act framework manages how law enforcement can access data held by service providers, even if that data is stored abroad, provided it follows statutory rules and legal processes.[49] This highlights a major reality of digital jurisdiction: where a server is physically located might not be what determines which government can demand data.[50] A provider's legal status, its control over the information, and its domestic legal obligations can be just as decisive as the server's location.

For nations worried about foreign access, the real challenge is managing clashing legal demands while protecting users and maintaining transparency. A government might need information for a legitimate investigation, while another country's laws might demand privacy or secrecy. Without clear protocols, providers end up stuck between impossible duties, and users are left in the dark. To manage these tensions, countries need international agreements, clearly defined thresholds for data access, notice requirements, and ways to challenge improper requests.[51]

It is a mistake to view this as a simple binary between a rights-focused Europe and a security-focused United States. Both systems are layered with complex rules, exceptions, and

---

[48] Data Act, supra note 47, arts. 23–31.

[49] CLOUD Act, supra note 8, 18 U.S.C. § 2713; *see also United States v. Microsoft Corp.*, 138 S. Ct. 1186 (2018).

[50] Daskal, supra note 3.

[51] 18 U.S.C. § 2523 (executive agreements).

institutional checks, and both are influenced by political and commercial interests.[52] Similarly, India cannot simply adopt either model. India has its own unique constitutional structure, public service architecture, market scale, and institutional strengths. Comparative law is most valuable when it identifies core principles and trade-offs rather than treating another country's laws as a plug-and-play solution.

A comparative lens also reveals the limits of "sovereignty" rhetoric. If every nation demands absolute control over all data linked to its citizens, the global internet could fragment into incompatible silos.[53] On the other hand, if no country can enforce its laws against transnational companies, regulatory decisions lose their teeth. The most practical middle ground is a system of bounded jurisdiction, international cooperation, and strong safeguards, with heightened protections for high-risk data and transparent ways to resolve conflicts. India can learn from European safeguards and American experience with cross-border access while staying true to its own constitutional values.

6. TRANSNATIONAL INTERNET GOVERNANCE AND THE PROBLEM OF PRIVATE POWER

Internet governance is spread across a wide range of actors: states, international bodies, technical standard-setters, network operators, cloud providers, and digital platforms. Some rules are written into formal law, while others emerge from technical protocols, terms of service, content moderation policies, and procurement contracts.[54] This decentralized structure makes the internet resilient, but it also makes it hard to pin down responsibility. A user whose account is suspended or whose data is exposed might have to navigate a platform's internal rules, a domestic regulator, a foreign court, and various contractual terms all at once. No single entity controls everything, yet every actor holds significant influence over certain parts of the system.

Private power becomes particularly problematic when a provider becomes "too big to fail" or too difficult to replace. A government that relies on just a few cloud companies may face massive costs if it tries to move, struggle with proprietary formats, or face uncertainty about service continuity during geopolitical tensions. These aren't just business problems; they impact a state's ability to provide public services and function during emergencies. This same

---

[52] Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* (Oxford University Press, New York, 2023).

[53] Mueller, supra note 12.

[54] Laura DeNardis, *The Global War for Internet Governance* (Yale University Press, New Haven, 2014).

dependency affects hospitals, universities, small businesses, and civil society groups that lack the leverage to negotiate with tech giants.[55]

The issue isn't that large tech companies are inherently bad. Global providers offer high-level security and infrastructure that would be incredibly expensive for any single nation to build from scratch. The real risk is when this dependency becomes irreversible, or when a company's private rules start functioning like public laws without the same level of accountability. When a platform decides which voices are heard, which apps can reach users, or which businesses can function on its infrastructure, its decisions have massive implications for social and economic opportunity.[56]

A smart sovereignty strategy should prioritize portability, interoperability, open standards, and healthy competition. Public contracts should include clear "exit" clauses, rights to export data, documented interfaces, audit access, and plans for service continuity.[57] Instead of assuming a service is secure just because a provider has a certain certification, critical services should be regularly tested for their ability to migrate or recover. While domestic capability is important, it should be measured by actual, verifiable resilience rather than just the nationality of the provider. Finally, competition law can play a vital role in preventing companies from locking users in or using their dominance in one area to unfairly control another.[58] The legal proceedings in India regarding Android highlight how things like default settings, pre-installed software, and control over app stores can fundamentally shape competition within a digital ecosystem.[59] These issues are central to sovereignty; when a market offers very few real alternatives, both public and private users are left vulnerable to the whims of just a handful of companies. While competition isn't a cure-all for security risks, it does help prevent a single provider from becoming too indispensable.

At the same time, the state's regulation of digital platforms must be carefully constrained. Vague or opaque instructions regarding content removal can stifle public debate, damage journalism, and limit political participation.[60] The constitutional precedents set by cases like *Shreya Singhal* remain vital, as ambiguous legal obligations often push platforms to over-

---

[55] Cohen, supra note 11.

[56] Klonick, supra note 6.

[57] Data Act, supra note 47, arts. 23–31.

[58] Competition Act, supra note 41.

[59] *Umar Javeed*, supra note 41.

[60] The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, G.S.R. 781(E), dated Oct. 27, 2009.

moderate, deleting more content than the law actually requires.[61] When companies face uncertain penalties, they tend to prioritize compliance over free expression, especially when dealing with controversial or politically sensitive topics. To prevent this "chilling effect," we need transparent directives, clear reasoning, and accessible ways to review and remedy decisions.

Global internet governance is also deeply influenced by technical architecture. Standards for encryption, routing protocols, domain-name systems, and cybersecurity practices all play a role in how power is distributed. While technical standards might seem neutral, they essentially decide who gets to participate, which systems can work together, and how easily surveillance or censorship can be deployed.[62] Because of this, public authorities should actively engage with technical communities and civil society, rather than treating internet governance as a niche issue reserved solely for security agencies or executive departments.

Furthermore, the state should avoid using "domestic origin" as a shortcut for accountability. A local provider can still mishandle data, release insecure products, or abuse market power. Conversely, a foreign provider might offer superior security and be bound by enforceable contractual safeguards. While nationality is a relevant factor in assessing jurisdiction and risk, it shouldn't be the sole deciding factor. Instead, procurement and regulatory choices should be driven by transparent standards regarding security, resilience, auditability, and access to remedies.[63]

The most effective approach is one of shared responsibility. Public authorities should set lawful standards and remain accountable for any coercive actions they take. Companies must be transparent about their practices, maintain robust security, and offer meaningful ways for users to file complaints. Technical communities have a duty to preserve an open, secure, and interoperable network, while individuals and organizations must have the tools to challenge decisions that harm them. Finally, international cooperation is indispensable; issues like cybercrime, security breaches, and cross-border evidence cannot be effectively managed through isolated national actions.[64]

---

61 *Shreya Singhal*, supra note 23.

62 DeNardis, supra note 54.

63 General Financial Rules, supra note 32.

64 Convention on Cybercrime, supra note 33.

7. TOWARD A CONSTITUTIONAL MODEL OF DIGITAL SOVEREIGNTY FOR INDIA

India should build a model of digital sovereignty rooted in risk management, accountability, and practical capacity. The process must begin with classification: not every dataset or service carries the same level of risk, and therefore, not every risk requires the same level of intervention. Highly sensitive areas—such as identity, judicial, financial, and critical infrastructure systems—may require strict controls over hosting, privileged access, and key management. Lower-risk services, however, might be better managed through transfer safeguards, contractual duties, and recognized security standards rather than mandatory local storage.[65] These risk classifications must be based on transparent criteria and updated regularly as technology evolves.

First, public authorities need to publish clear rules regarding data classification and cloud procurement. The criteria used to decide whether a system belongs in a government, private, hybrid, or sovereign cloud environment should be easy to understand and subject to review. Policy documents that are merely administrative or indicative should be clearly labeled as such, rather than being treated as formal legislation. Any decision that imposes a significant burden must state its legal basis and explain exactly which risk it is trying to mitigate. This creates predictability for both public bodies and suppliers while allowing citizens to judge whether such measures are truly justified.[66]

Second, rules regarding cross-border data transfers and access must be transparent. When the government requests information from service providers, the process should follow established legal procedures, be limited to legitimate purposes, and include safeguards against unnecessary disclosure. In cases where foreign legal demands clash with Indian obligations, providers and institutions need clear, predictable procedures for escalation. Rather than relying on sweeping localization mandates, India can use international agreements and cooperation mechanisms to manage these tensions.[67] Clear rules are also needed to address evidence preservation, emergency requests, and the ability to challenge demands that are unlawful or disproportionate.

Third, constitutional safeguards must be baked into digital policy from the ground up. Any power related to surveillance or data access must be grounded in clear legal authority,

---

65 MeitY framework, supra note 2.

66 General Financial Rules, supra note 32; *Puttaswamy (Privacy)*, supra note 1.

67 DPDP Act, supra note 34, s. 16; Convention on Cybercrime, supra note 33.

necessity, and proportionality.[68] Internet restrictions should be time-limited, well-reasoned, and—whenever legally possible—published and subject to prompt review.[69] Individuals must have accessible ways to seek remedies for the unlawful collection, disclosure, or restriction of their data. Furthermore, independent audits should look at how policies are actually practiced on the ground, not just whether companies are checking boxes for formal compliance. Even when secrecy is temporarily necessary, there must be independent scrutiny and eventual accountability.

Fourth, public procurement should be used to reduce unnecessary dependence. Contracts should explicitly cover data portability, technical documentation, subcontractor transparency, and assistance with service termination. For critical systems, the government must maintain a realistic plan for migration or recovery and test it periodically. Procurement officers need to look at the full lifecycle cost of a system, including the "exit costs" of moving data and the expense of maintaining alternatives. A low initial price tag can quickly become a massive liability if an agency finds itself unable to move its data or applications without an expensive and extensive redevelopment process.[70]

Fifth, India must strengthen institutional coordination. Regulatory bodies overseeing data protection, cybersecurity, competition, telecommunications, and public procurement often look at the same digital systems through different lenses, necessitating a more unified approach. A coordinated approach can allow institutions to share technical expertise without undermining their individual legal roles. By using joint guidance, standardized definitions, and clear referral processes, agencies can avoid conflicting demands. However, coordination must never become a loophole for avoiding accountability; responsibility must remain easy to pinpoint. Every major decision needs to be traceable back to an authority with a clear, legal mandate.

Sixth, transparency should be viewed as a practical safeguard. Within reasonable security limits, governments can publish high-level data on information requests, cybersecurity incidents, service outages, and the use of internet restrictions.[71] In public procurement, the criteria used for evaluation and the safeguards required of vendors should be disclosed.

---

68 *Puttaswamy (Privacy)*, supra note 1; *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301 : AIR 1997 SC 568; The Information Technology Act, 2000 (Act 21 of 2000), s. 69; The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, G.S.R. 780(E), dated Oct. 27, 2009.

69 *Anuradha Bhasin*, supra note 1.

70 General Financial Rules, supra note 32; Data Act, supra note 47, arts. 23–31.

71 *Anuradha Bhasin*, supra note 1.

Furthermore, impact assessments can clarify how specific policies affect privacy, market competition, small businesses, and access to services. This type of transparency doesn't mean revealing sensitive operational secrets; it means providing enough context for the public and other institutions to conduct meaningful oversight.

Seventh, digital inclusion must be a core part of any sovereignty policy. A system is a failure if it remains secure from foreign influence but effectively locks out citizens who struggle to navigate it. Public services should maintain accessible alternatives, offer assisted channels, and provide clear ways to correct inaccurate data. A technical glitch should never be used as automatic proof that someone is ineligible for a benefit or service. Human oversight is especially vital when automated systems make decisions that impact a person's livelihood, identity, or access to essential resources.[72]

Eighth, domestic capability should be cultivated through research, skill-building, healthy competition, and open technical standards. Investing in cybersecurity expertise, public-sector technical talent, and secure software development can gradually reduce dependency on external actors. While supporting local suppliers can be a valid policy goal, protectionism should not stifle competition or excuse poor performance. The most resilient ecosystem is one where multiple capable providers can meet transparent standards, and where public institutions actually understand the systems they are tasked with supervising.

Finally, the success of digital sovereignty should be measured by its impact on the public. Key indicators should include service continuity, incident recovery speed, the cost and ease of switching providers, the effectiveness of privacy protections, the transparency of state restrictions, and the availability of independent oversight. Simply counting domestic data centers or tracking how much data is stored locally is insufficient. Sovereignty holds constitutional value only when it fosters accountable self-governance and protects the people the state is meant to serve.

This model won't resolve every conflict. Strict security rules might drive up costs; data safeguards can be difficult to enforce; and transparency must often be balanced against necessary operational secrecy. The goal of a constitutional framework isn't to bypass these difficult choices, but to ensure they are explicit, evidence-based, and subject to review. Decisions should clearly state the objective, explain the intended benefit, consider less intrusive

---

[72] *Puttaswamy (Aadhaar)*, supra note 20; Khera, supra note 40.

alternatives, and include a way to fix mistakes.[73] This approach transforms digital sovereignty from an open-ended claim of executive power into a structured legal framework.

CONCLUSION

The global nature of the internet hasn't erased state sovereignty, but it has fundamentally changed how it works. States are still responsible for protecting rights, securing critical infrastructure, and regulating activities within their borders. However, data, infrastructure, and corporate influence constantly cross borders, even as citizens become increasingly dependent on digital tools for work, education, finance, and public services. The solution isn't as simple as declaring that all data must stay within national borders. While physical location matters, it alone cannot guarantee legal access, operational independence, privacy, or resilience.

India's constitutional framework provides vital checks on digital power. The *Puttaswamy* ruling establishes privacy as a fundamental right; *Anuradha Bhasin* ensures that internet restrictions are legally grounded and proportionate; and *Shreya Singhal* guards against vague curbs on online expression.[74] These principles must hold even when the state is pursuing legitimate goals like cybersecurity or public order. They mandate that the state explain its actions and provide avenues for appeal. The Constitution is not separate from digital sovereignty; rather, it defines the boundaries within which sovereign power can be exercised legitimately.

Looking at the European Union and the United States shows that data location, legal jurisdiction, and provider control are different issues. International data transfers can be managed through safeguards, and legal access requests can reach far beyond where data is physically stored. The EU model emphasizes the need for strong protections during cross-border data movement and the ability to switch cloud providers easily.[75] Meanwhile, the US experience shows why provider obligations and lawful-access procedures can often be more important than where a server is located.[76] Neither model is a perfect template for India, but both demonstrate that digital governance requires rules that work across borders.

India should aim for a strategy that combines risk-based cloud controls with robust data protection, transparent legal processes, interoperability, healthy competition, and effective

---

[73] Barak, supra note 5.

[74] *Puttaswamy (Privacy)*, supra note 1; *Anuradha Bhasin*, supra note 1; *Shreya Singhal*, supra note 23.

[75] GDPR, supra note 7, arts. 44–46; Data Act, supra note 47, arts. 23–31.

[76] CLOUD Act, supra note 8, 18 U.S.C. § 2713.

ways for citizens to seek remedies. The March 2026 MeitY cloud-deployment document serves as a timely illustration of the shift toward specialized protection for sensitive public systems, though its exact status and any follow-up

updates should be double-checked before anything is formally published.[77] The broader takeaway here is that public infrastructure needs to be categorized based on its specific risks and managed through a combination of clear contracts, strict access controls, robust recovery plans, and independent oversight. While hosting data domestically might make sense for certain systems, it shouldn't be used as a shortcut; it must be a component of a much wider governance framework.

At its core, digital sovereignty shouldn't imply that the state must eliminate all external dependence at any price, nor should it mean that citizens are forced to trade their privacy and liberty for the sake of national control. Instead, it should mean that India has the ability to make deliberate, enforceable decisions about its digital path while staying true to its constitutional principles. Achieving this requires the ability to safeguard critical infrastructure, the legal restraint to keep public power in check, market environments that prevent over-reliance on private players, and the kind of international cooperation necessary to tackle issues that no single nation can handle alone.

Ultimately, the most resilient form of sovereignty isn't found in isolating oneself from the global internet. Rather, it is found in the ability to engage with it on terms that are secure, fair, and democratically accountable. A constitutional approach to digital sovereignty understands that while the state needs enough authority to govern effectively, that power must never be so unchecked that individual rights are sidelined. In the long run, things like legitimacy, resilience, and public trust aren't hurdles to national digital autonomy—they are actually its most essential foundations.

---

[77] MeitY framework, supra note 2.

BIBLIOGRAPHY

A. Constitutional Provisions, Statutes and Delegated Legislation (India)

The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (Act 18 of 2016).

The Competition Act, 2002 (Act 12 of 2003). The Constitution of India, 1950.
The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

The Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), dated Nov. 13, 2025. The Information Technology Act, 2000 (Act 21 of 2000).
The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), dated Feb. 25, 2021.

The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, G.S.R. 781(E), dated Oct. 27, 2009.

The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, G.S.R. 780(E), dated Oct. 27, 2009.

The Payment and Settlement Systems Act, 2007 (Act 51 of 2007). The Telecommunications Act, 2023 (Act 44 of 2023).

B. International and Foreign Instruments

Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 391.

Clarifying Lawful Overseas Use of Data Act, 2018, Pub. L. No. 115-141, div. V, 132 Stat. 1213 (2018) (United States).

Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural

persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2016 O.J. (L 119) 1.

Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act), 2023 O.J. (L 2023/2854).

C. Government Reports and Documents

Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Ministry of Electronics and Information Technology, Government of India, July 2018).

Department of Electronics and Information Technology (now MeitY), Government of India, *GI Cloud (MeghRaj): Strategic Direction Paper and Adoption and Implementation Roadmap* (2013).

Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics and Information Technology, Directions under Sub-section (6) of Section 70B of the Information Technology Act, 2000 relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe & Trusted Internet, No. 20(3)/2022-CERT-In (Apr. 28, 2022).

Ministry of Electronics and Information Technology (MeitY), Government of India, framework on cloud deployment options for government applications and databases (Mar. 2026).

Ministry of Finance, Department of Expenditure, Government of India, *General Financial Rules, 2017*.

D. Books

Barak, Aharon, *Proportionality: Constitutional Rights and their Limitations* (Cambridge University Press, Cambridge, 2012).

Bradford, Anu, *Digital Empires: The Global Battle to Regulate Technology* (Oxford University Press, New York, 2023).

Bradford, Anu, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press, New York, 2020).

Cohen, Julie E., *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press, New York, 2019).

DeNardis, Laura, *The Global War for Internet Governance* (Yale University Press, New Haven, 2014).

Goldsmith, Jack & Wu, Tim, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press, New York, 2006).

Khera, Reetika (ed.), *Dissent on Aadhaar: Big Data Meets Big Brother* (Orient BlackSwan, Hyderabad, 2019).

Mueller, Milton L., *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace* (Polity Press, Cambridge, 2017).

E. Articles

Chander, Anupam & Lê, Uyên P., "Data Nationalism", 64 *Emory L.J.* 677 (2015). Daskal, Jennifer, "The Un-Territoriality of Data", 125 *Yale L.J.* 326 (2015).

Floridi, Luciano, "The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU", 33 *Philosophy & Technology* 369 (2020).

Klonick, Kate, "The New Governors: The People, Rules, and Processes Governing Online Speech", 131 *Harv. L. Rev.* 1598 (2018).

Pohle, Julia & Thiel, Thorsten, "Digital Sovereignty", 9(4) *Internet Policy Review* (2020), DOI: 10.14763/2020.4.1532.

Solove, Daniel J., "A Taxonomy of Privacy", 154 *U. Pa. L. Rev.* 477 (2006).

F. Case Laws

Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 : AIR 2020 SC 1308.

Data Protection Commissioner v. Facebook Ireland Ltd. and Maximillian Schrems, Case C-311/18, ECLI:EU:C:2020:559 (Court of Justice of the European Union, July 16, 2020).

E.P. Royappa v. State of Tamil Nadu, (1974) 4 SCC 3 : AIR 1974 SC 555.

Google LLC v. Competition Commission of India, Competition Appeal (AT) No. 1 of 2023 (National Company Law Appellate Tribunal, Mar. 29, 2023).

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 : AIR 2017 SC 4161. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 SCC 1 : AIR 2018 SC 1841. *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248 : AIR 1978 SC 597.
Modern Dental College & Research Centre v. State of Madhya Pradesh, (2016) 7 SCC 353 : AIR 2016 SC 2601.

People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301 : AIR 1997 SC 568.

Shreya Singhal v. Union of India, (2015) 5 SCC 1 : AIR 2015 SC 1523.

Umar Javeed v. Google LLC, Case No. 39 of 2018 (Competition Commission of India, Oct. 20, 2022).

United States v. Microsoft Corp., 138 S. Ct. 1186 (2018).

G. Newspaper Reports

"Desi Data to Get Top Secret & A-B Sovereign Cover under New Cloud Rules", *The Economic Times*, Mar. 27, 2026.