



Federalism in the Digital Governance Framework of India

Dr. Santosh Kumar

B.Sc. (Maths), LL.M., NET, JRF, SRF, Ph.D. (LAW)

ARTICLE DETAILS	ABSTRACT
Research Paper	
Keywords :	
Federalism, Digital Governance, Cooperative Federalism, Data Protection, E-Governance, India	<i>Federalism in India represents the dynamic interplay between the Centre and the States in the governance process, aimed at balancing unity with diversity. The emergence of the digital state has transformed traditional governance paradigms, introducing new questions about the distribution of powers in the technological domain. Digital governance—through initiatives such as the Digital India Mission, e-Governance projects, Aadhaar infrastructure, and the Digital Personal Data Protection Act, 2023—has redefined administrative structures and intergovernmental relations. The convergence of technology and governance challenges the federal equilibrium, as data localization, digital identity management, cybersecurity, and e-service delivery transcend territorial and jurisdictional boundaries. This paper examines the constitutional, administrative, and policy dimensions of India's federal structure in the context of digital governance. It evaluates the evolving Centre–State relationships in the digital age, explores judicial interventions, and compares India's experience with global models of digital federalism. The study concludes that cooperative and fiscal federalism must adapt to the realities of networked governance, data sovereignty, and digital rights, ensuring inclusivity, accountability, and technological autonomy within the federal framework.</i>

1. Introduction

Federalism, as a constitutional principle, represents the distribution of governmental powers between the national and subnational levels. In India, it is a system designed to accommodate vast territorial, linguistic,



and cultural diversity while maintaining national unity. However, the digital revolution has introduced a new dimension to this relationship, transforming the traditional mechanisms of policy formulation, administration, and accountability. The proliferation of digital platforms, cloud-based governance, and artificial intelligence in public administration necessitates a re-examination of how federal principles operate in a digitally connected environment.

The concept of digital governance—the use of information and communication technology (ICT) in public service delivery—has evolved into an essential pillar of governance. The Government of India launched the Digital India Mission (2015) with the vision of transforming India into a knowledge-based economy and digitally empowered society. However, the implementation of these initiatives has predominantly been centralized, raising debates over the extent of State participation, autonomy, and digital capacity. Federalism in the digital era is thus not merely about jurisdictional distribution but about collaborative governance in an interconnected policy space.

The constitutional basis of federalism in India is embedded in the Seventh Schedule, which divides legislative powers into Union, State, and Concurrent Lists. Subjects such as communications, inter-state trade, and coordination of information technology fall under the Union List, granting the Centre substantial legislative authority over digital infrastructure. Nonetheless, the success of e-governance, digital literacy, and public service digitization depends heavily on State-level implementation. Therefore, digital governance has become a shared responsibility, demanding cooperative federalism in the digital domain.

This paper explores how the evolving digital ecosystem affects Indian federalism. It analyzes the constitutional foundations, administrative policies, and institutional frameworks governing digital transformation. It further evaluates how new legislation—such as the Digital Personal Data Protection Act, 2023, and the Information Technology Act, 2000—redefines the boundaries between centralization and decentralization. The discussion also includes the judiciary's role in adjudicating digital rights, such as privacy and data sovereignty, which intersect with federal power dynamics.

2. Constitutional and Federal Basis of Digital Governance

2.1 The Constitutional Framework of Indian Federalism

The framers of the Indian Constitution envisioned a quasi-federal structure characterized by a strong Centre. Articles 245 to 263 define the legislative, administrative, and intergovernmental framework of India's federalism. The Seventh Schedule delineates subjects between the Union and the States, with the



Union List containing critical technological subjects like telecommunications, inter-state trade, and coordination of scientific research.

The Constitution (101st Amendment) Act, 2016, which introduced the Goods and Services Tax (GST), marked a shift toward cooperative federalism. A similar model is visible in digital governance, where fiscal and administrative coordination between the Centre and States determines the success of digital projects. Article 263 further empowers the President to establish inter-state councils for policy coordination—an instrument that can be effectively used in digital governance harmonization.

2.2 Federal Distribution of Powers in the Digital Context

The digital domain blurs traditional jurisdictional boundaries. Data flows, cybercrimes, and e-commerce transactions operate beyond state and national borders, making exclusive legislative control impractical. Under Entry 31 of the Union List, the Centre retains power over “posts and telegraphs; telephones, wireless, broadcasting, and other forms of communication.” This entry provides constitutional backing for central initiatives like the Digital India Mission, Aadhaar, and National Digital Health Mission.

However, several areas—such as education, health, and public service delivery—fall within the State List or Concurrent List, implying that digitalization of these sectors requires coordination. For example, e-governance portals, state data centers, and digital payment systems often depend on central funding but local implementation. This structural interdependence transforms the federal relationship into a form of cooperative digital federalism.

2.3 Digital Federalism and the Role of Cooperative Governance

The term digital federalism refers to the adaptation of federal principles in managing digital infrastructure, policies, and data governance. It emphasizes collaboration, resource-sharing, and policy harmonization between different tiers of government. India’s NITI Aayog and Ministry of Electronics and Information Technology (MeitY) have promoted cooperative models through schemes like Digital India, e-Kranti, and Common Service Centres (CSCs). These programs integrate central technological frameworks with State-level operational networks.

States such as Kerala (e-District), Andhra Pradesh (Real-Time Governance Society), and Maharashtra (MAHAIT) have developed robust digital ecosystems aligned with central policies. This reflects a federal synergy in the digital domain, where technology functions as a unifying instrument rather than a divisive factor. Nonetheless, the issue of data control—who owns, processes, and secures citizen data—remains contentious, reflecting the tension between autonomy and uniformity.



2.4 Judicial Interpretation and Federal Digital Rights

The judiciary has played a critical role in defining the boundaries of federalism and digital rights. In *K.S. Puttaswamy v. Union of India* (2017), the Supreme Court recognized privacy as a fundamental right under Article 21, thereby constraining both central and state authorities in data governance. Later, in *Justice K.S. Puttaswamy (Aadhaar) v. Union of India* (2018), the Court upheld the constitutional validity of Aadhaar while emphasizing proportionality and necessity in data collection.

These judgments highlight the constitutional interplay between central legislation and state autonomy in implementing digital identification systems. States must adhere to central data protection norms while maintaining localized control over service delivery. Thus, the judiciary reinforces a balanced federal digital framework based on constitutional supremacy, rule of law, and human rights.

2.5 Centre–State Fiscal Dynamics in Digital Governance

Digital governance projects require substantial financial investment in infrastructure, connectivity, and human resource development. The Centre’s control over fiscal resources—through centrally sponsored schemes—often tilts the balance in its favor. Programs like the Digital India Mission, BharatNet, and PMGDISHA (Pradhan Mantri Gramin Digital Saksharta Abhiyan) are centrally designed but depend on State cooperation for last-mile execution.

The Finance Commission’s recommendations and the Digital India Infrastructure Fund reflect the growing fiscal integration between the Centre and the States. This financial interdependence promotes cooperation but may also undermine fiscal autonomy if States are bound by uniform guidelines and conditional grants. Ensuring fiscal federalism in the digital era thus requires flexible funding mechanisms and greater State participation in policy design.

2.6 Federalism and Emerging Digital Legislation

Recent legislation, including the Digital Personal Data Protection Act, 2023, and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, exemplify central dominance in digital regulation. These laws primarily empower the Union government to frame rules for data protection, intermediary liability, and online content moderation. States, however, play minimal roles in enforcement, except through cyber police units.

This centralization has led to concerns over asymmetrical digital federalism, where the Union dictates standards without significant State input. To maintain cooperative balance, the creation of a Digital

Federal Council, analogous to the GST Council, could institutionalize State participation in digital policymaking, ensuring inclusivity and accountability in the national digital architecture.

3. Digital India Mission and the Federal Framework of Governance

3.1 Evolution of Digital India as a Federal Policy Instrument

The Digital India Mission (2015) represents one of the largest administrative transformations in post-independence India, aimed at bridging the digital divide and fostering a technology-driven governance ecosystem. Conceptualized as an umbrella program under the Ministry of Electronics and Information Technology (MeitY), it encompasses various e-governance initiatives across departments and levels of government.

Digital India is founded on three core vision areas: (a) digital infrastructure as a utility to every citizen, (b) governance and services on demand, and (c) digital empowerment of citizens. While the central government provides the overarching policy framework, funding, and technological standards, the States and Union Territories serve as the principal implementing agencies. This shared structure situates Digital India within the federal cooperative paradigm, balancing national uniformity with regional adaptability.

Under the constitutional framework, digital infrastructure—such as telecommunications, electronic communication, and cybersecurity—falls within the Union’s legislative competence (Entry 31, Union List). However, implementation areas like e-health, e-education, and e-agriculture are subject matters in the State or Concurrent Lists, requiring coordination through intergovernmental mechanisms. Hence, Digital India’s success depends on how effectively the Centre and States collaborate, share data, and harmonize regulatory frameworks.

3.2 Institutional Mechanisms for Cooperative Digital Governance

The operational framework of Digital India demonstrates a multi-tiered approach:

National e-Governance Division (NeGD): Functions as the central coordinating body under MeitY, responsible for program management, policy guidance, and inter-departmental integration.

State e-Governance Mission Teams (SeMTs): Serve as state-level counterparts of NeGD, overseeing the implementation of e-Governance projects within their jurisdictions.

District e-Governance Societies (DeGS): Act as local implementation units facilitating service delivery through Common Service Centres (CSCs).

This decentralized structure promotes administrative participation across federal layers. However, the degree of effectiveness varies across states due to disparities in digital infrastructure, fiscal capacity, and technical expertise. States like Kerala, Andhra Pradesh, and Karnataka have emerged as leaders in e-governance, while others lag due to inadequate institutional support.

3.3 Digital Public Infrastructure and Federal Integration

India's emerging Digital Public Infrastructure (DPI)—comprising Aadhaar, Unified Payments Interface (UPI), DigiLocker, and the India Stack—illustrates how federal coordination enables scalable digital ecosystems. Aadhaar, for instance, is centrally maintained by the Unique Identification Authority of India (UIDAI), yet its use in welfare delivery depends on State cooperation. Similarly, UPI's interoperability across public and private banks exemplifies cooperative technological federalism.

Nonetheless, this integrated infrastructure also centralizes data control under the Union government. States rely on central APIs, protocols, and authentication systems, limiting their autonomy over citizen data management. The debate over data federalism—who owns and governs public digital data—has thus emerged as a key constitutional and policy issue.

3.4 Centre–State Coordination through Digital Councils and Committees

To operationalize federal cooperation, several committees and councils facilitate Centre–State coordination:

National e-Governance Plan (NeGP) Apex Committee: Provides policy direction, with representation from States.

Digital India Advisory Group: Involves State IT Secretaries to ensure intergovernmental alignment.

Inter-State Council (Article 263): Occasionally discusses digital coordination but lacks a dedicated mandate.

Despite these mechanisms, there is no constitutionally mandated “Digital Governance Council.” A Digital Federal Council, analogous to the GST Council, could institutionalize dialogue between the Centre and the States, addressing issues of interoperability, cybersecurity, and digital equity.

3.5 State-Level Innovations in Digital Governance

Federalism in digital governance is reflected in the diversity of state-level initiatives, many of which complement the national Digital India agenda.

Kerala: The “e-District” and “Akshaya Centres” have established universal access points for citizen services, supported by community participation.

Andhra Pradesh: The “Real-Time Governance Society (RTGS)” integrates data from multiple departments for real-time decision-making.

Maharashtra: The “Aaple Sarkar” platform provides 400+ citizen services online, combining state-level data hubs with central authentication mechanisms.

Tamil Nadu: The “e-Sevai” project delivers over 12 crore digital transactions annually, reflecting localized adaptation of central frameworks.

These examples highlight the federal diversity of digital governance, where innovation arises from state autonomy within a shared policy architecture.

3.6 Fiscal Federalism and Digital Transformation

Fiscal arrangements play a crucial role in determining the balance of power in digital governance. The **Centrally Sponsored Schemes (CSS)** model enables the Union government to fund digital infrastructure projects such as BharatNet, CSCs, and e-Kranti, with partial State contributions. However, conditional grants and standardization requirements often restrict States’ flexibility.

The Fifteenth Finance Commission (2021–26) emphasized the need for States to enhance digital capacity for fiscal management and service delivery. It recommended performance-based grants to incentivize digital transparency. In effect, fiscal federalism is transitioning toward digital fiscal cooperation, where resource allocation depends on digital readiness and governance performance.

3.7 Challenges in Federal Digital Governance

Despite progress, several challenges persist in the federal digital governance framework:

Centralized Data Ownership: The concentration of digital identities, authentication, and databases under central agencies undermines State autonomy.

Uneven Technological Capacity: States differ widely in ICT infrastructure, leading to asymmetric digital federalism.

Legal Ambiguity: Overlapping jurisdictions between MeitY, State IT departments, and regulators create administrative confusion.

Cybersecurity Coordination: While the Centre handles national cyber threats, local cybercrime investigation remains under State jurisdiction, causing coordination delays.



Digital Divide: Socio-economic disparities across States hinder equal participation in the digital transformation process.

3.8 Toward a Model of Cooperative Digital Federalism

Cooperative digital federalism requires redefining intergovernmental relations through shared governance principles—consultation, consensus, and capacity-building. Institutional innovations such as interoperable data frameworks, joint technology missions, and federal data-sharing agreements can ensure equitable participation of States in digital policy formulation.

As the Indian digital landscape expands under initiatives like Digital India 2.0, the balance between centralization and decentralization will shape the future of Indian federalism. Digital governance can strengthen unity only if it preserves diversity, autonomy, and accountability across the federal structure.

4. Comparative Perspectives: Digital Federalism in Other Jurisdictions

4.1 The United States: Cooperative and Competitive Digital Federalism

In the United States, the federal structure grants extensive autonomy to States, resulting in a pluralistic digital ecosystem. Each State regulates data privacy and cybersecurity within its jurisdiction. For example, the California Consumer Privacy Act (CCPA, 2018) establishes stringent rights for data subjects, influencing national discourse. However, the absence of a comprehensive federal digital law creates fragmentation.

The U.S. federal model highlights the advantages of local experimentation and innovation but also demonstrates challenges in harmonizing interstate digital policies. India, by contrast, has pursued a centralized approach, which ensures uniformity but limits localized flexibility.

4.2 The European Union: Harmonized Digital Sovereignty

The European Union exemplifies supranational digital federalism through regulatory harmonization across member states. The General Data Protection Regulation (GDPR, 2018) enforces uniform data protection standards, balancing national autonomy with collective sovereignty. Similarly, the Digital Services Act (DSA) and Digital Markets Act (DMA) establish EU-wide frameworks for online governance and competition regulation.

India can draw lessons from the EU's federal coordination model, particularly the establishment of data protection authorities at both Union and national levels. Such dual regulatory structures ensure consistent enforcement while preserving regional oversight.

4.3 Australia and Canada: Intergovernmental Collaboration

Australia's Digital Transformation Agency (DTA) operates under a cooperative federal framework involving Commonwealth and State governments. It coordinates digital identity and cybersecurity strategies while allowing local adaptation. Canada follows a similar approach, where provinces manage digital health and education systems under a shared national data policy.

These models demonstrate that effective digital federalism relies on institutionalized coordination and shared standards rather than centralized control. For India, adopting a federal digital council mechanism could harmonize policy without eroding State autonomy.

4.4 Comparative Implications for India

Comparative experience suggests that digital federalism functions best under a hybrid model—where centralization ensures interoperability and decentralization fosters innovation. India's federal structure, with its strong Centre and diverse States, can evolve into a collaborative digital federation if institutional mechanisms for joint policy-making are formalized.

The transition from analog to digital governance thus requires reimagining federalism as a living, adaptive system that incorporates technology, inclusivity, and shared accountability into its constitutional design.

5. Legal and Institutional Challenges in Digital Federalism

5.1 Introduction

The digital transformation of governance has created a new constitutional and administrative ecosystem in India, where federal principles must interact with technology, privacy, and cybersecurity concerns. While the Centre has initiated most digital laws and platforms, the States are responsible for local enforcement and citizen interface. This multi-layered governance structure generates several legal and institutional challenges, ranging from jurisdictional ambiguities to data ownership conflicts. Ensuring a balanced and cooperative approach between the Union and the States in digital regulation is thus vital for the success of Indian federalism in the twenty-first century.

5.2 Centralization of Legislative Competence in Digital Regulation

The Indian Constitution assigns technological subjects primarily to the Union List, particularly under Entry 31, which empowers the Parliament to legislate on "telegraphs, telephones, wireless broadcasting, and other forms of communication." This broad entry now encompasses the entire digital communication



spectrum. Consequently, the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023 (DPDP Act) are enacted solely by Parliament, leaving States with limited regulatory scope.

This concentration of legislative authority has been criticized as a form of digital centralism, where the Centre dictates standards for cybersecurity, data governance, and online content moderation. The absence of parallel State legislation restricts local innovation and creates dependency on centrally issued notifications and rules. For example, the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 confer extensive powers on the Union Government to demand content removal, without requiring State consultation.

To maintain cooperative digital federalism, it is essential to design mechanisms enabling State participation in rule-making processes and consultative policy formulation. A federal approach ensures contextual adaptation, particularly in areas like e-health, e-agriculture, and digital education, which fall under State or Concurrent jurisdiction.

5.3 Jurisdictional and Administrative Overlaps

Another challenge arises from the overlap between central agencies—such as the Ministry of Electronics and Information Technology (MeitY), the Indian Computer Emergency Response Team (CERT-In), and the National Critical Information Infrastructure Protection Centre (NCIIPC)—and State-level cybercrime units. While CERT-In handles national cybersecurity incidents, the investigation of cybercrimes, including financial fraud, defamation, and harassment, falls under State police jurisdiction.

This dual structure often leads to coordination failures. States lack direct access to central cybersecurity alerts, while CERT-In depends on State reports for localized response. Moreover, differences in capacity, funding, and expertise among State cyber cells exacerbate inequalities, creating an asymmetrical federal cybersecurity system.

The Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) attempts to modernize procedural investigation, incorporating provisions for digital evidence collection and cybercrime investigation. Yet, its effective implementation requires intergovernmental coordination and standardized digital forensics infrastructure across States.

5.4 Data Federalism and Ownership Conflicts

The emergence of data as the new economic resource raises critical questions about ownership, access, and control between the Union and the States. The DPDP Act, 2023, centralizes regulatory authority under



a single Data Protection Board of India, leaving States without equivalent institutions. While this approach ensures national uniformity, it neglects regional differences in data governance needs.

For instance, health data collected under the Ayushman Bharat Digital Mission (ABDM) and education data managed by State boards fall within the State's administrative domain but are stored in centrally managed digital repositories. This concentration of data governance in the hands of the Centre limits State sovereignty over locally generated data.

Scholars have thus called for a framework of data federalism, wherein States have defined rights over the collection, processing, and utilization of data generated within their territories. This would align with the principle of fiscal and administrative decentralization inherent in the federal design.

5.5 Cybersecurity and Federal Coordination

Cybersecurity presents perhaps the most complex challenge for Indian digital federalism. The National Cyber Security Policy (2013) outlines a central strategy, but the absence of State-level cybersecurity policies creates implementation gaps. While the Union deals with critical infrastructure protection, State police handle cybercrimes under local jurisdiction. However, cyberattacks often transcend territorial boundaries, necessitating a coordinated national response.

The National Critical Information Infrastructure Protection Centre (NCIIPC) is empowered to secure systems vital to national security, economy, and public health. Yet, cooperation with State agencies remains voluntary, not mandatory. The lack of a federal cybersecurity framework results in uneven preparedness, where technologically advanced States can respond faster than resource-constrained ones.

A model similar to the U.S. Federal–State Cyber Partnership Framework, involving real-time data sharing and co-funded cybersecurity programs, could ensure consistency and capacity-building across Indian States.

5.6 Digital Rights, Privacy, and Federalism

The right to privacy, recognized in *K.S. Puttaswamy v. Union of India (2017)*, introduced a constitutional dimension to digital governance. Both the Centre and the States are obligated to respect and protect this right while implementing digital programs. However, the centralization of data processing and surveillance under the Union raises concerns about overreach.

The Aadhaar project, though upheld in *Justice K.S. Puttaswamy (Aadhaar) v. Union of India (2018)*, was limited in scope to essential welfare schemes. The judgment highlighted the need for proportionality, data

minimization, and federal accountability in digital welfare administration. States, while implementing Aadhaar-linked services, must ensure compliance with these constitutional safeguards.

In this sense, the federal protection of digital rights requires both central uniformity in standards and decentralized enforcement through State authorities. Creating State Data Protection Officers, under the oversight of the central Data Protection Board, could operationalize this balance.

5.7 Institutional Capacity and Digital Justice Delivery

The capacity gap between the Centre and the States extends to the judicial and forensic domains. Although the Bharatiya Sakshya Adhiniyam, 2023 (Sections 61 and 63) recognizes electronic evidence, many trial courts lack the expertise and infrastructure to examine digital records properly.

Furthermore, coordination between central investigative agencies (like CBI and NIA) and State police remains weak in cyber investigations. Without shared digital evidence standards, inter-state investigations face procedural hurdles.

The establishment of National and State Digital Forensic Laboratories, along with training programs for judges and prosecutors, is crucial to bridging this gap. An institutionalized Federal Digital Investigation Council could oversee standardization and cooperation between jurisdictions.

5.8 Fiscal and Administrative Disparities

Federal fiscal asymmetries affect the capacity of States to invest in digital infrastructure. Central grants under Digital India and BharatNet are often conditional, requiring matching contributions from States. Poorer States, unable to meet these requirements, risk lagging behind.

Additionally, centrally designed procurement and software architecture may not suit local conditions. To enhance inclusivity, the Finance Commission should introduce digital equalization grants—similar to fiscal equalization—to bridge inter-state disparities in digital governance.

5.9 The Digital Divide and Federal Equity

Federalism also entails the equitable distribution of resources and opportunities among constituent units. India's digital divide—across rural–urban, gender, and linguistic lines—undermines the promise of digital governance. States with lower literacy or weaker infrastructure struggle to deliver e-services effectively.

To achieve federal equity in digital transformation, the Centre must adopt differentiated strategies that empower lagging States through technical assistance, infrastructure investment, and knowledge transfer. The success of cooperative digital federalism depends on narrowing these technological inequalities.

5.10 The Path toward Cooperative and Participatory Digital Federalism

Addressing these challenges requires a transformation in intergovernmental relations. The creation of a National Digital Governance Council, with equal representation of States, could institutionalize consultation and coordination in digital policy. Regular intergovernmental conferences on data protection, cybersecurity, and digital rights could promote mutual learning.

Further, adopting the principle of subsidiarity—where decision-making authority is exercised at the most local competent level—would prevent unnecessary centralization. Decentralized innovation, backed by uniform technical standards, would ensure both efficiency and inclusivity.

Digital federalism must thus evolve as a dynamic model of shared sovereignty, blending central leadership with State autonomy. The ultimate objective should be the realization of a federal digital republic, where governance is technologically advanced yet constitutionally balanced, inclusive, and rights-based.

6. Conclusion

The digital revolution has redefined the meaning of governance, citizenship, and federalism in India. While the Centre's leadership in developing national digital infrastructure has accelerated modernization, excessive centralization threatens to erode the federal balance envisioned in the Constitution. The challenge before India is not technological but structural—how to align rapid digitalization with constitutional federalism.

A future-ready federal digital framework must therefore rest on three foundational pillars:

Cooperative Governance: Institutionalized coordination through a National Digital Council and intergovernmental committees.

Data Federalism: Recognizing the States' role in managing and protecting locally generated data.

Fiscal and Capacity Equity: Ensuring equitable digital resources and capacity-building support across States.

Digital India can truly succeed only when it becomes Federated India in the Digital Age—a system where every State participates as an equal partner in digital policymaking, implementation, and accountability. The evolution of digital governance in India thus represents both a test and an opportunity: a test of federal adaptability in the age of technology, and an opportunity to strengthen democracy through cooperative, inclusive, and rights-oriented digital federalism.



References

- Barfield, W., & Pagallo, U. (Eds.). (2020). *Research handbook on the law of artificial intelligence*. Edward Elgar Publishing.
- Bhattacharya, S. (2021). *Federalism and digital governance in India: Emerging trends and challenges*. *Indian Journal of Public Administration*, 67(3), 245–262. <https://doi.org/10.1177/001955612111030678>
- Government of India. (2023). *Bharatiya Sakshya Adhiniyam, 2023*. Ministry of Law and Justice. <https://egazette.gov.in>
- Government of India. (2023). *Digital Personal Data Protection Act, 2023*. Ministry of Electronics and Information Technology. <https://www.meity.gov.in>
- K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).
- MeitY. (2015). *Digital India Programme: Vision and roadmap*. Government of India.
- NITI Aayog. (2021). *Strategy for digital transformation and cooperative governance*. <https://niti.gov.in>
- Puttaswamy (Aadhaar) v. Union of India, (2018) 1 SCC 809 (India).
- Rai, A. (2022). *Data federalism and digital constitutionalism in India*. *Journal of Indian Law and Society*, 13(2), 112–134.
- Sharma, R. (2020). *Federalism in the age of technology: Challenges to cooperative governance in India*. *Indian Law Review*, 4(2), 178–195.
- World Bank. (2022). *Digital governance and federal coordination: Lessons for India*. Washington, DC: World Bank Publications.