Page: 814-846 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 3 | Issue 4

2025

DOI: https://doi.org/10.70183/lijdlr.2025.v03.156

SOVEREIGNTY AND RIGHTS: CHALLENGES OF DIGITAL CONSTITUTIONALISM FOR INDIA IN THE AGE OF GLOBAL INTERNET GOVERNANCE, WITH COMPARATIVE INSIGHTS FROM FRANCE

Rushikesh Suresh Belagali[1]

I. ABSTRACT

The conflict between constitutional rights and national sovereignty has escalated due to the rise of global internet governance, posing serious concerns for India's digital future. Transnational platforms, data flows, and algorithmic regulation present issues for India's constitutional structure, which is based on democratic principles. On the one hand, the state uses policies like data localization, platform responsibility, and content restriction to try and establish digital sovereignty. On the other hand, it is required by the constitution to defend fundamental rights like equality, free speech, and privacy in a digital world that is becoming more and more influenced by private actors and international norms. This dual goal highlights the vulnerability of India's digital constitutionalism, where rights-based strategies seem to undermine state authority while sovereignty-driven policies run the risk of restricting rights. A comparative perspective on France provides insightful information. The European Union's French constitutional tradition serves as an example of how supranational government and rights protection can coexist. France strikes a balance between national authority and the enforcement of collective rights through independent regulators, constitutional courts, and EU-level structures. This comparison highlights the need for institutional innovation in India. In order to achieve a hybrid paradigm of digital constitutionalism, the study contends that India must transcend the dichotomy of sovereignty vs rights. A model like this would safeguard cultural and political sovereignty, uphold democratic principles online, and position India as a global leader in fair, rights-based internet governance. The increasing complexity of global digital governance demands that India navigate both

[1] Student of LLM (IP) At Amity Law school, Amity University, Noida, Uttar Pradesh (India). Email: rishibelagali@gmail.com

 (ISSN: 2583-7753)

international pressures and domestic constitutional guarantees. As global internet frameworks continue to evolve, India's digital constitutionalism faces a critical crossroad: balancing national interests with global standards. India's approach must embrace technological innovation while ensuring fundamental rights are not compromised in the pursuit of sovereignty. The challenge lies in crafting policies that respect both state autonomy and the protection of individual freedoms in an interconnected world.

II. KEYWORDS

Digital Constitutionalism; Internet Governance; State Sovereignty; Fundamental Rights; Data Protection; Platform Regulation; Algorithmic Governance; Privacy and Surveillance

III. INTRODUCTION

Global constitutional discussions have changed as a result of the digital era, compelling states to address the conflict between rights and sovereignty in cyberspace. As one of the biggest digital markets in the world, India faces a particularly difficult task: it must strike a balance between the need for national control over data and platforms and its constitutional obligation to uphold fundamental rights like equality, privacy, and free speech. This balance is complicated by the emergence of global internet governance, which is dominated by transnational businesses, supranational organizations, and multi-stakeholder frameworks. It frequently weakens the authority of domestic legislation while simultaneously calling for more robust rights safeguards.

India's goal to establish control over digital infrastructures is reflected in its pursuit of digital sovereignty through measures including platform regulation, intermediary liability, and data localization. However, these actions often violate constitutional norms, giving rise to worries about surveillance, censorship, and the diminution of personal liberties. However, rights-based strategies run the danger of coming to be seen as weak in the face of global power disparities, making India susceptible in discussions on internet governance standards. The paper examines the normative stakes of internet governance,

the institutional reforms required, and the comparative pathways that can guide India toward becoming a global voice in shaping equitable digital futures.

A. RESEARCH QUESTIONS

In order to achieve the purpose of this study, the following research questions are to be addressed.

- How can India reconcile the tension between digital sovereignty and the protection of constitutional rights in the context of global internet governance?
- What institutional, legal, and policy mechanisms can strengthen India's digital constitutionalism while ensuring both state authority and individual freedoms?
- What lessons can India draw from France's rights-oriented approach to develop a hybrid model of digital constitutionalism that safeguards sovereignty while ensuring rights protection?

B. RESEARCH HYPOTHESIS

This study is based on three main hypotheses.

- First, India's efforts to strengthen digital sovereignty through policies such as data localization and platform regulation may weaken constitutional rights if not supported by strong safeguards.
- Second, new institutional mechanisms, including digital tribunals, judicial review, and multi-stakeholder governance, are necessary to balance state authority with the protection of individual freedoms.
- Third, lessons from France's rights-oriented approach within the European Union suggest that India can adopt a hybrid model of digital constitutionalism that protects sovereignty while ensuring rights. Together,

these hypotheses guide the analysis of how India can uphold democratic principles while engaging with global internet governance.

C. RESEARCH METHODOLOGY

This paper follows a doctrinal and comparative approach, examining constitutional principles, legal frameworks, and judicial developments in India and France to understand how digital sovereignty and rights are balanced. The analysis is supported by general literature on digital constitutionalism, internet governance, data protection, and platform regulation, along with relevant policy reports and academic commentary. These methods and sources together provide a broad foundation for evaluating the challenges India faces in the evolving landscape of global digital governance.

D. LITERATURE REVIEW

Existing research characterizes digital constitutionalism as an ongoing framework that redefines constitutional rights, state power, and institutional responsibility in the digital and algorithmic age. De Gregorio describes it as a restructuring of constitutional principles to confront platform power and automated decision-making, whereas Bradford's Brussels Effect illustrates how European digital legislation influences global norms outside EU borders.

Citron and Pasquale's work on algorithmic due process, as well as UN Human Rights Council reports on privacy, reveal a strong rights-based strand that emphasizes openness, accountability, and remedies to surveillance and automated governance. European treaties such as Convention 108+ and the Digital Services Act demonstrate how these principles are put into practice through binding regulation and enforcement, with France serving as a significant national implementation site.

The global internet governance literature (WGIG, NETmundial, IGF, IETF) emphasizes a multistakeholder system that undermines traditional sovereignty while raising questions about legitimacy and enforceability. In contrast, Indian policy and scholarship (TRAI,

MeitY) take a more sovereignty-oriented approach, attempting to reconcile innovation, security, and fundamental rights despite institutional capacity constraints.

Overall, the research suggests a persisting contradiction between digital sovereignty and rights protection, with Europe focusing on rights-based regulation and India balancing constitutional principles within a fragmented global governance ecosystem. This research addresses that gap by doing a comparative examination of India and France.

IV. FRAMING DIGITAL CONSTITUTIONALISM: GLOBAL GOVERNANCE AND INDIA'S SOVEREIGNTY–RIGHTS TENSION

In reaction to the expanding power of international internet governance organizations that frequently function beyond the purview of national legal systems, the idea of "digital constitutionalism" has evolved. These organizations, which include multinational technology companies, supranational organizations, and multi-stakeholder forums, influence the laws of the digital realm in ways that go against conventional ideas of state sovereignty. The challenge for India is balancing the demands of establishing control over digital infrastructures and data flows with its constitutional commitment to basic rights.

A. DEFINING DIGITAL CONSTITUTIONALISM

Edoardo Celeste, a prominent thinker, in his book Digital Constitutionalism: The Role of Internet Bills of Rights in the year 2022, defines digital constitutionalism as "The movement that seeks to articulate a set of normative principles, rights, and rules to frame the power of digital actors and ensure the protection of fundamental rights in the digital environment". In other words, it refers to the normative framework for governing digital spaces that emphasises digital rights, platform accountability, and transnational governance.[2] Digital constitutionalism can be understood with the help of the following key elements that explain its true purpose.

[2] Dublin City University | DCU https://share.google/NQpwGLmXaF4ymNN3R

B. ONLINE PROTECTION OF RIGHTS

The expansion of fundamental rights into the digital sphere, guaranteeing that people have the same constitutional protections online as they do outside, is one of the central tenets of digital constitutionalism. The protection of rights, including privacy, freedom of expression, equality, and due process, becomes crucial as digital technologies continue to influence communication, transportation, education, employment, and political engagement.

This need is met by digital constitutionalism, which maintains that constitutional principles hold true despite advancements in technology. This implies that online spaces must function within a framework that respects human rights, regardless of whether they are run by corporations, governments, or private platforms. It stops biased algorithmic techniques, illegal spying, and arbitrary censorship. Additionally, it guarantees that when people's rights are violated in digital situations, they have meaningful remedies. It aims to safeguard the fundamental rights such as expression, privacy, equality, etc, which extends the reach of rights into cyberspace.

C. RULE OF LAW IN THE DIGITAL SPHERE

The rule of law in the digital sphere is a central feature of digital constitutionalism, ensuring that digital technologies and online platforms operate within a framework of predictable, transparent, and accountable legal norms. As digital systems increasingly influence social, economic, and political life, it becomes essential that technological power, whether held by governments or private corporations, is exercised in a manner consistent with constitutional principles.

Transparency and rationale for activities in the digital sphere are necessary for the rule of law. When the government blocks websites, social media companies remove information, or artificial intelligence makes judgments that have an impact on people, the justification must be available to the public, reviewable, and susceptible to judicial challenge. This principle guarantees that technical systems function in support of constitutional safeguards rather than superseding them. The rule of law guarantees that

legal boundaries, human judgment, and democratic accountability continue to be crucial in a world where algorithms, artificial intelligence, and data infrastructures create social order.

D. LIMITATION OF POWER IN THE DIGITAL SPHERE

This principle guarantees that all kinds of digital power are subject to constitutional limits in a digital world when governments and platforms have previously unheard-of powers for data processing, surveillance, and behavioral molding. Digital constitutionalism emphasises checks and balances on governmental power in the digital domain. Modern states can monitor communications, collect biometric data, deploy facial-recognition technologies, and influence public discourse through digital regulations. Without constitutional limits, such powers risk violating privacy, chilling free expression, and enabling authoritarian control.

Therefore, legal safeguards such as data-protection laws, judicial oversight, and legislative accountability are essential to restrain state dominance over digital life. The limitation of power requires participatory governance in the digital ecosystem. Citizens, civil society groups, and independent oversight authorities must be involved in decisions about digital regulation and platform governance. This distributes power across multiple actors and prevents domination by any single entity.

E. DEMOCRATIC PARTICIPATION IN THE DIGITAL SPHERE

Digital constitutionalism aims to ensure equitable and meaningful access to digital tools and information. Citizens who lack adequate access cannot successfully participate in discussions, elections, or public affairs. Ensuring ubiquitous internet access, digital literacy, and nondiscriminatory platform design is critical to protecting democratic rights. Digital environments facilitate free, open, and pluralistic public discourse. This involves defending online freedom of expression, opposing political censorship, and protecting people from misinformation and deception. Democratically oriented digital frameworks aim to strike a compromise between transparency and protection against online harms that distort public reasoning.

Digital constitutionalism promotes participatory governance, in which citizens can shape digital legislation, data regulations, and platform norms. This could involve public consultations, multi-stakeholder governance structures, and transparent regulatory systems that reflect democratic values rather than arbitrary governmental or corporate decisions.[3]

F. ALGORITHMIC JUSTICE

Algorithmic justice tries to address the unfairness and discrimination inherent in computerized systems. Algorithms frequently rely on data sets including historical disparities or systemic biases. Without constitutional safeguards, these systems may exacerbate racial, gender, economic, or geographic imbalances. As a result, digital constitutionalism calls for obligatory audits, anti-discrimination standards, and rights-based design principles to ensure that algorithmic outcomes respect equality and dignity.

It focuses on transparency and explainability. Traditional constitutional governance requires a rationale for actions affecting individual rights, but many algorithmic choices are made in "black boxes" that users cannot comprehend or contest. Algorithmic justice requires explainable AI standards, public disclosure of decision factors, and methods that enable individuals to learn how and why a decision impacting them was made.

Algorithmic justice emphasizes human oversight as a constitutional safeguard. Automated technologies cannot replace human judgment when basic rights are at issue. Human-in-the-loop models, restitution procedures, and access to human review all contribute to keeping automated errors from creating lasting harm. Overall, algorithmic justice assures that the advent of AI does not jeopardize constitutional ideals, but rather works within a framework of fairness, transparency, and human dignity.[4]

[3] Giovanni De Gregorio, Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society, 19 Int'l J. Const. L.
[4] Danielle Keats Citron & Frank Pasquale, "The Scored Society: Due Process for Automated Predictions," 89 *Washington Law Review* 1 (2014).

G. GLOBAL SOLIDARITY IN THE DIGITAL SPHERE

Digital constitutionalism emphasizes communal accountability, cross-border cooperation, and a shared commitment to safeguarding human rights in the digital age. As digital technologies cross national borders, issues such as data exploitation, cyber-surveillance, misinformation, and algorithmic discrimination necessitate collaborative, global answers. Global solidarity represents the belief that no single state can successfully control the digital environment alone. The internet is fundamentally transnational, with platforms operating globally. As a result, protecting digital rights necessitates collaboration among governments, international organizations, civil society groups, and technology corporations. Joint regulatory frameworks are becoming increasingly important, including global data protection standards, cybersecurity regulations, and cross-border human rights processes.[5]

V. UNDERSTANDING GLOBAL INTERNET GOVERNANCE

Global Internet Governance refers to the frameworks, institutions, and processes that the global community uses to control the internet's technological, legal, economic, and political characteristics. As a borderless and decentralized network, the internet cannot be managed by a single state or organization. Instead, its governance is the result of a complex interplay between governments, international organisations, private enterprises, civil society groups, and technical bodies.

Technological decisions made by one actor or country have an impact on users all over the world; therefore, global internet governance is based on multistakeholder engagement, transparency, cooperation, and shared accountability. It recognises that digital technologies influence economies, political processes, and human rights, necessitating governance models that can balance innovation, security, and freedom in the global digital world.

[5] United Nations Human Rights Council, *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/27/37 (2014).

The Working Group on Internet Governance (WGIG), in the year 2005, defined internet governance as the "Development and application by governments, private sectors and civil society, in their respective roles of shared principles, norms, values, rules, decision-making procedures and programs that shape the evolution and use of the internet". [6] Today, internet governance is shaped by a complex mix of institutions, players, and norms that influence how the global digital ecosystem runs. As internet activities spread across borders and influence every sector, new regulatory issues and coordinating requirements have arisen. The following aspects describe the key elements that define this changing governance landscape.

A. MULTISTAKEHOLDER GOVERNANCE

Global Internet governance is based on a multistakeholder approach in which governments, business sector entities, civil society organizations, and technical communities work together to develop policies. This framework assures that no single actor, state, or corporation has complete control over digital ecosystems, preserving the Internet's openness and interoperability. The concept uses consensus-based mechanisms to balance opposing interests in areas like content control, cybersecurity, privacy, and digital public goods. [7]

B. DECENTRALISED AND DISTRIBUTED INSTITUTIONAL FRAMEWORK

A decentralized governance structure increases the Internet's resilience, stability, and openness by ensuring that no single government or organization has control over its essential design. Various entities, including ICANN, IETF, and W3C, manage certain technical and policy functions, resulting in a balanced distribution of authority. This eliminates political capture, encourages innovation through open standards, and allows various technical communities to contribute to Internet development. The distributed

[6] Working Group on Internet Governance, *Report of the Working Group on Internet Governance* ¶ 10 (2005), available at https://www.itu.int/net/wsis/docs2/contributions/wgig/WGIG-report.pdf.

[7] NETmundial Multistakeholder Statement, Global Multistakeholder Meeting on the Future of Internet Governance (2014), https://netmundial.br

framework also improves security because failures in one section of the system do not affect the entire network. Decentralization promotes worldwide interoperability and ensures the Internet remains a shared, borderless resource for all.[8]

C. TECHNICAL STANDARDS AND PROTOCOL DEVELOPMENT

The development of open technical standards assures that the Internet is interoperable, innovative, and universally accessible. The IETF and W3C rely on transparent, consensus-based mechanisms that encourage global engagement from engineers, researchers, and technical groups. Because many standards, like TCP/IP, DNS, and HTML, are publicly defined and freely implementable, they avoid proprietary lock-in and promote continual technological innovation. Openness in protocol design improves cybersecurity by allowing for peer review, rapid upgrades, and collaborative problem solutions. These collaborative methods ensure that the Internet grows into a resilient, scalable, and future-ready network.

D. ROLE OF THE PRIVATE SECTOR AND PLATFORM GOVERNANCE

The private sector plays a pivotal and highly constructive role in shaping the functioning of the global Internet ecosystem. Technology businesses, particularly Internet service providers, cloud providers, and digital platforms, invest heavily in infrastructure such as data centers, undersea cables, satellites, and cybersecurity systems to ensure the stability and growth of global connectivity. Their ability to innovate quickly allows them to create new tools, protocols, and services that improve user experience, reinforce online safety, and handle emerging digital dangers far faster than traditional regulatory systems.

Platforms also contribute to governance by establishing extensive community standards, content policies, and transparency reports, which assist in creating safer online environments and provide accountability mechanisms for billions of users. Private enterprises contribute technical experience, operational capability, and data-driven insights to evidence-based policymaking through collaborations with governments, civil

8 Internet Engineering Task Force (IETF), Overview of the IETF, https://www.ietf.org/about

society, and technical bodies. Overall, the private sector's leadership in innovation, infrastructure, and policy experimentation improves the Internet governance landscape and boosts its resilience in an ever-changing digital environment.

E. CROSS-BORDER JURISDICTION

Cross-border jurisdiction encourages states to rethink rigid territorial boundaries and engage with the reality of global digital flows. As online activities span multiple countries, courts and regulators increasingly adopt more flexible and adaptive interpretations of jurisdiction. This promotes legal creativity, comparative learning, and the development of doctrines that better reflect the interconnected nature of the digital world. Such adaptability also helps protect users by ensuring that harmful online conduct can be addressed even when perpetrators operate outside a single territory. [9]

F. GLOBAL REGULATORY INTERACTION

The rise of digital technology has compelled national governments to look beyond their borders and participate in global regulatory frameworks. This interaction has become a crucial component of modern internet governance because it improves coherence, increases accountability, and harmonizes standards across jurisdictions. States can now address complex digital concerns that cross borders by agreeing with international norms such as the EU's General Data Protection Regulation (GDPR), the Council of Europe's Convention 108+[10], or the UN Guiding Principles on Business and Human Rights.

G. INTEGRATION OF HUMAN RIGHTS NORMS AND DIGITAL FREEDOMS

Institutions such as the United Nations Human Rights Council, the Council of Europe, and regional tribunals are increasingly acknowledging that online rights such as privacy, expression, association, and access to information are natural extensions of offline

[9] Jack Goldsmith & Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press 2006)

[10] Council of Europe *Convention 108+: Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data* (2018), available at https://www.coe.int/en/web/data-protection/convention108/modernised

liberties. This harmonization gives digital governance principles legitimacy based on long-standing international human rights law.

A rights-based approach promotes a culture of responsible innovation, encouraging governments, private platforms, and global institutions to embed safeguards like privacy-by-design, non-discrimination, transparency, and due process into their policies. As a result, the digital ecosystem evolves not merely as a technological space, but as a domain shaped by dignity, autonomy, and justice.

VI. INDIA'S EVOLVING POSITION UNDER DIGITAL CONSTITUTIONALISM

India's position in digital constitutionalism reflects a dual commitment: asserting digital sovereignty through policies like data localization and platform regulation, while safeguarding constitutional rights such as privacy, free expression, and equality in the digital sphere. This balancing act places India at the center of debates on how national authority can coexist with global internet governance. The following are the current characteristics of India's position in the digital age;

A. EVOLVING CONSTITUTIONAL CONTEXT

The Indian Constitution was drafted for an analogue age, yet its flexibility and rights-based framework allow reinterpretation for the digital era. Courts and policymakers are gradually "constitutionalizing" the digital sphere, especially through privacy and free speech jurisprudence.

India's constitutional framework is increasingly being interpreted in light of digital realities. The expansion of rights discourse now includes informational autonomy, data protection, and digital inclusion, reflecting how constitutional values are adapting to new technological challenges. Parliamentary debates on the Digital Personal Data Protection Act, 2023, illustrate how privacy and state power are being re-negotiated within constitutional boundaries. Similarly, discussions around net neutrality, intermediary

liability, and data localization show how constitutional principles of equality, freedom, and sovereignty are being projected into cyberspace.

This changing environment shows how India's constitutionalism is expanding beyond the conventional spheres of speech and privacy to include digital citizenship, technology company accountability, and state duty in cyberspace. It lays the groundwork for viewing digital constitutionalism as a dynamic process as opposed to a rigid framework.

B. RIGHT TO PRIVACY AND DATA PROTECTION

In Justice K. S. Puttaswamy (Retd.) and Anr. v Union of India,[11] The right to privacy was recognised as a fundamental right under Article 21. This formed the constitutional foundation for digital rights, including protection from state surveillance and data misuse. Importantly, the Court rejected earlier cases (*M.P. Sharma* and *Kharak Singh* in part) that had denied or limited privacy protections.

The judgment introduced a three-fold test for any State intrusion into privacy:

- **Legality–** there must be a valid law.
- **Legitimate Aim –** the restriction must pursue a legitimate State purpose.
- **Proportionality –** the measure must be necessary, narrowly tailored, and the least restrictive option.

The Court also emphasised informational privacy, recognising that digital technologies enable the State and private actors to collect, process, and profile individuals at an unprecedented scale. It acknowledged that the digital age requires robust data protection, calling upon the State to create a comprehensive data protection framework.[12]

The judgment stressed that privacy is rooted in natural law traditions, not created by the Constitution but recognized by it. A sense of privacy originates from dignity and is deeply inherited in personhood.

[11] [2017] 10 SCC 1.
[12] Ibid.

The court highlighted that privacy is not absolute and is prone to reasonable restrictions under Article 21 through the test of proportionality. Overall, the *Puttaswamy* judgment marks a quiet yet decisive constitutional shift, reaffirming that dignity, autonomy, and individual freedom remain central even in a rapidly digitising India.

C. FREEDOM OF EXPRESSION ONLINE

In Shreya Singhal v Union of India,[13] Section 66A of the IT Act was a law that criminalized sending offensive or menacing messages through a computer or communication device. However, the Indian Supreme Court struck down this section in 2015 for being vague and unconstitutional, violating freedom of speech reinforcing free speech in the digital space.

A major reason for striking down Section 66A was its vagueness, wherein terms like "annoying," "offensive," "grossly menacing," and "inconvenience" were undefined and subjective. The Court held that such vague laws restrict free speech by making citizens afraid of unpredictable criminal liability. Section 66A criminalised a vast range of harmless or legitimate speech, making it overbroad and disproportionate.

The Court reaffirmed that restrictions on Article 19(1)(a) must be narrowly tailored to the eight grounds under Article 19(2). The Court read down, i.e, narrowed down the scope of Section 79 and the IT Intermediary Guidelines, clarifying that intermediaries are only required to take down content upon court orders or government notifications that comply with Article 19(2). The judgment emphasised that due process and transparency must accompany online content takedowns. It also recognised the Internet as a Crucial Medium for Democratic Participation.

D. STATE-LED DIGITAL GOVERNANCE

Aadhaar, Digital India, and India Stack are examples of India's techno-sovereign strategy, in which the government leverages domestically produced digital infrastructure to

[13] [2015] 5 SCC 1.

increase governance capacity, improve service delivery, and promote social inclusion. Aadhaar enables biometric identification on a massive scale, allowing for targeted welfare distribution and reduced leakages; Digital India provides an ecosystem for digital access, connectivity, and public platforms; and India Stack, which includes layers such as e-KYC, UPI, DigiLocker, and consent-based data sharing, builds a foundational architecture for secure, interoperable public services. Together, these initiatives offer a model in which the state exercises control over key digital infrastructure while also attempting to democratize access and promote citizen-state interaction through technology-driven governance.

E. DIGITAL SOVEREIGNTY VS. GLOBAL INTERDEPENDENCE

India promotes data localization and digital public infrastructure to assert sovereignty over data and the digital economy. However, India remains deeply embedded in global internet governance, reliant on global tech platforms and transnational data flows. This creates a constitutional tension between asserting control and upholding rights within international norms.

F. JUDICIAL AND INSTITUTIONAL RESPONSES

The Indian judiciary has been reactive rather than proactive, addressing digital issues case-by-case rather than through a unified doctrine. Regulatory institutions such as MeitY[14]CERT-In and the Data Protection Board often prioritize executive control over independent oversight. These institutions reflect a state-centric model of digital governance. While this strengthens sovereignty and centralized decision-making, it raises constitutional concerns about checks and balances, transparency, and the protection of fundamental rights in the digital sphere.

1. Civil Society and Rights Discourse

In order to influence discussions on digital policy, civil society organizations, digital rights organizations, and academia have increasingly used constitutional terms like

[14] Ministry of Electronics and Information Technology, Government of India

autonomy, due process, and dignity. This central approach accelerates the speed of digital constitutionalism and strengthens the foundation of law in the digital age.

2. Cybersecurity oversight

CERT-In (Indian Computer Emergency Response Team), established in 2000 under the IT Act, issues mandatory directions to service providers, data centers, and intermediaries to report cybersecurity incidents. It governs the cybersecurity measures along with the other key institutions.

3. Right to Information and Access

The right to information includes access to truthful and timely content online. Digital access also plays a role in education, health, and legal aid. In Anuradha Bhasin v. Union of India[15]The Supreme Court of India gave a significant judgment related to freedom of speech, internet access, and government restrictions. This case was significant because it was the first time the Supreme Court gave detailed guidelines on internet shutdowns and explained how digital rights relate to fundamental rights in the Constitution.[16]

4. Role of Private Tech Companies

Private businesses are not directly obligated by the Constitution, in contrast to governments. Nonetheless, they have a significant influence over our digital lives. However, their presence creates obstacles for emerging businesses as they dominate the market, leaving users with limited alternatives. Terms of service are often unclear, enabling data misuse, leading to a lack of due process.

[15] [2020] 3 SCC 637.

[16] Rajbhar. Vivek Kumar, Digital Constitutionalism and Fundamental Rights: A Contemporary Legal Analysis, article published on vintage legal. https://www.vintagelegalvl.com/post/digital-constitutionalism-and-fundamental-rights-a-contemporary-legal-analysis

VII. FRANCE'S MODEL OF DIGITAL CONSTITUTIONALISM AND ITS GLOBAL REGULATORY FOOTPRINT

France has emerged as one of the most active constitutional actors in the digital sphere, influencing both national rights frameworks and larger global governance issues. The French model, which is based on a strong republican constitutionalism history, extends fundamental guarantees of privacy, dignity, and freedom of expression into the digital world with exceptional clarity. France not only protects digital rights domestically through strong institutions like the Constitutional Council and CNIL, but it also impacts worldwide standards through its leadership in the European Union and active participation in global forums. This dual function positions France as a critical normative force, balancing technical innovation with human-centric constitutional principles in an increasingly linked digital world. The following are the key elements that explain the nature of digital constitutionalism in France and its global regulatory framework.

Strong Constitutional Protection of Digital Rights: France incorporates digital rights into its constitutional system through the Constitutional Council's jurisprudence, which extends traditional rights of privacy, dignity, liberty, and expression to the digital era. The Council has invalidated intrusive surveillance rules, requiring proportionality, legality, and necessity. Its decisions ensure that technology advancements do not undermine constitutional guarantees. By interpreting constitutional standards in light of modern digital realities, France protects liberties while adjusting governance to technology concerns.[17]

- **GDPR-Driven Data Protection:** France treats data protection as a fundamental right, deeply influenced by EU law, especially the GDPR and the EU Charter of Fundamental Rights. The French data regulator, CNIL, enforces strict standards regarding consent, transparency, purpose limitation, and accountability. This creates a rights-protective digital infrastructure

[17] *Conseil Constitutional*, Decision No. 2015-713 DC (Oct. 23, 2015).

where data processing becomes constitutionally grounded. CNIL's decisions shape national compliance and strengthen trust in digital systems.[18]

- **Constitutional Limits on State Surveillance:** Despite serious internal security challenges, France's Constitutional Council has reined in unrestrained surveillance. Measures enabling bulk metadata access, algorithmic surveillance, and real-time interceptions have been struck down or modified to include judicial authorisation and oversight. These decisions reflect a constitutional insistence that national security cannot override core liberties. France thus maintains a structured balance between security imperatives and digital rights.
- **Digital Platform Accountability as a Public-Order Responsibility:** France pioneered platform regulation by setting requirements on digital intermediaries, particularly with harmful material, algorithmic opacity, and transparency. Early laws, such as the Avia Law, and later alignment with the EU's Digital Services Act (DSA), demonstrate France's commitment to controlling private digital power. These approaches incorporate constitutional principles, expression, dignity, and equality into platform governance, thereby increasing democratic accountability.[19]
- **Strong Civil Society and Digital Rights Advocacy:** Civil society organizations, particularly La Quadrature du Net, digital researchers, and privacy activists, play a critical role in defining France's digital constitution. They use smart litigation and public campaigning to oppose state overreach and corporate opacity, promoting participatory and transparent digital regulation. Their activities turn constitutional principles like autonomy, dignity, and access to information into enforceable online rights.[20]

[18] Commission Nationale de l'Informatique et des Libertés (CNIL), *Annual Report* (2022).

[19] Regulation (EU) 2022/2065 (Digital Services Act).

[20] La Quadrature du Net, *Strategic Litigation Dossiers* (2023).

- **Active Leadership in EU Digital Policy-Making:** France is a driving force behind important EU digital changes such as the DSA, DMA, and the upcoming AI Act. It proposes a concept in which digital marketplaces and platforms are subject to democratic oversight. France fosters a human-centric European digital order through policymaking influence and political leadership, while also promoting rights abroad through EU regulatory export.
- **Promotion of Digital Sovereignty:** France promotes "souveraineté numérique," claiming that governments and the EU must maintain strategic control over digital infrastructures, cloud systems, and data flows. This viewpoint strives to lessen reliance on non-European IT behemoths while ensuring secure digital autonomy. The French concept views sovereignty as essential not only for national security but also for protecting constitutional rights in globalized digital environments.[21]
- **Engagement in Multistakeholder Global Forums:** France actively engages in global digital governance, including the IGF, the OECD's digital committees, UNESCO, and the Council of Europe, which promote collaborative and democratic standards. Its leadership in these fora focuses on human rights, open internet principles, and fair digital practices, promoting the notion that global government must be inclusive and rights-protecting.[22]
- **Support for Global Standards on AI Ethics:** France was a key player in negotiating UNESCO's Recommendation on the Ethics of AI (2021), one of the first worldwide normative frameworks governing AI. The Recommendation encourages fairness, openness, accountability, and nondiscrimination.

[21] La Quadrature du Net – Strategic Litigation https://www.laquadrature.net/en/category/strategic-litigation/
[22] Internet Governance Forum (IGF), France – National and Regional Initiatives Report (2023).

France's involvement reflects its commitment to prioritizing human dignity in AI development, affecting international digital ethics debates.[23]

- **Balancing Security and Liberties in a Global Digital Order:** Given the recurring terror threats, France must strike a compromise between cybersecurity obligations and fundamental freedoms. Its global collaboration on data sharing, cybercrime, and cross-border enforcement is guided by constitutional provisions that prevent disproportionate interference. France thus serves as a bridge between security imperatives and rights-based governance in international discussions, protecting liberty as a constitutional constant even in global settings.[24] France's approach of digital constitutionalism, which is based on strong data protection, judicial oversight of surveillance, and tight platform responsibility, has become a key reference point in global digital governance. Its rights-based and sovereignty-oriented strategy provides valuable lessons for India as it develops its own digital regulatory framework. Drawing on French examples, India may tighten judicial monitoring, improve platform regulation, and strike a balance between technology autonomy and constitutional rights. Thus, France's experience has a subtle but substantial impact on India's growing digital governance architecture.

VIII. CHALLENGES OF DIGITAL CONSTITUTIONALISM FOR INDIA IN THE AGE OF GLOBAL INTERNET GOVERNANCE

India's digital transformation has reached a point where constitutional ideals, technological ambition, and global governance forces collide with unprecedented force. Not only is the country regulating digital technologies, but it is also interpreting constitutional rights in algorithmic, biometric, and platform-mediated situations. As India exerts greater sovereign control over data, platforms, and digital infrastructure, it

[23] UNESCO Recommendation on the Ethics of AI https://unesdoc.unesco.org/ark:/48223/pf0000381137
[24] Council of Europe Cybercrime Convention Committee (TCY)

faces a complicated situation in which constitutional guarantees of privacy, dignity, and free expression must coexist with geopolitical realities, global norms, and rising digital hazards. This confluence generates a new generation of challenges: not repeated arguments, but wholly new constitutional questions built between national sovereignty and global digital interdependence.

A. CONFLICT BETWEEN EXPANDING STATE SOVEREIGNTY AND CONSTITUTIONAL RIGHTS

India's quest for digital sovereignty has accelerated, as the government seeks greater control over data flows, digital platforms, and online information ecosystems. Data localisation rules, mandated traceability, extended interception powers, and tight platform compliance frameworks are all intended to improve national security, regulatory autonomy, and technological self-reliance. However, these measures frequently conflict with constitutional guarantees of privacy, free expression, informational autonomy, and procedural fairness.

Under digital constitutionalism, any restriction on rights must pass the standards of legality, necessity, and proportionality as laid down in the Puttuswamy case. However, India's sovereign digital interventions frequently lack independent monitoring, open reasoning, or clearly defined limitations, resulting in a structural contradiction between the State's ambition for control and citizens' constitutional rights. The task, therefore, is not to deny sovereignty, but to create a constitutional framework in which sovereign digital authority can be exercised without undermining the rights architecture of the Indian Constitution.

This contradiction has especially been obvious in contexts such as encryption debates, algorithmic policing, biometric welfare systems, and large-scale data processing, where technology accelerates the State's authority as constitutional safeguards evolve.

 (ISSN: 2583-7753)

B. PRESSURE FROM GLOBAL INTERNET GOVERNANCE STANDARDS

India's digital regulatory structure is increasingly at odds with global norms that value transparency, cross-border interoperability, and rights-based internet governance. While international organizations such as the Internet Governance Forum (IGF), ITU, and OECD advocate standards based on democratic governance, transparent data practices, and international data mobility, India's sovereignty-driven policies frequently diverge. Measures such as data localisation require compliance for global platforms and increased state authority over digital operations attempt to improve national sovereignty, but they can conflict with multistakeholder internet governance models that emphasise decentralization and shared responsibility.

This gap is most obvious in discussions over cross-border data flows, cybersecurity regulations, and platform responsibility, as India's regulatory aggressiveness is considered to be heading toward a more centralised, state-preferred digital order. While global norms promote the fewest obstacles and maximum cooperation, India's strategy prioritises strategic independence, security concerns, and domestic institutional supremacy. This creates a complex regulatory environment in which aligning national digital policy with global standards while preserving constitutional rights remains a perennial constitutional and diplomatic dilemma.[25]

C. SURVEILLANCE EXPANSION WITHOUT ROBUST INDEPENDENT OVERSIGHT

The Central Monitoring System (CMS), NETRA, and the Crime and Criminal Tracking Network System (CCTNS) have all contributed to the rapid expansion of state surveillance capabilities in India's digital governance environment. While these systems are justified in terms of national security and administrative efficiency, they lack a specific independent supervision mechanism, raising serious constitutional concerns. According to digital constitutionalism, monitoring must be limited by legality, necessity,

[25] Internet Governance Forum (IGF), *About the IGF* (United Nations), https://www.intgovforum.org/en/about

proportionality, and clear permission. However, India's existing structure, based on the Information Technology Act and the Telegraph Act, gives the administration broad latitude without judicial approval or post-facto accountability.

This disparity becomes more evident in an era of global internet governance, where international human rights standards, particularly those stated by the UN Human Rights Committee, need procedural safeguards, due process, and rights-respecting surveillance measures. India's departure from these principles challenges its conformity with global expectations while also creating internal concerns about privacy, autonomy, and informational self-determination.

The challenge is therefore twofold: the constitutional concern arising from excessive executive control, and the global governance pressure that expects transparent, rights-protective surveillance systems. This dual tension places India at a difficult intersection between sovereign security imperatives and digital constitutionalist commitments to fundamental rights.[26]

D. FRAGMENTED REGULATORY CAPACITIES AND ASYMMETRY OF POWER

India confronts a structural problem in establishing digital sovereignty because its regulatory capacity has not kept up with the technological complexity and commercial domination of global digital firms. Big Tech platforms operate across borders, have data centers in numerous jurisdictions, and employ proprietary algorithms that are opaque to national regulators. India's attempts to enforce constitutional norms such as openness, accountability, and user rights frequently fail due to the practical difficulties of implementing domestic mandates on corporations whose operational centers are located outside of its borders.

This asymmetry puts a strain on India's sovereignty as it struggles to fully implement its regulatory vision, including algorithmic disclosure, competition oversight, and cross-

[26] Jack Goldsmith & Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press 2006)

border data access. Additionally, gaps in enforcement impact Indian users' digital autonomy, privacy, and due process. The outcome is a protective gap, in which neither national law nor global governance fills the regulatory void, leaving individuals exposed while the state is restrained in exercising constitutional safeguards.

This imbalance was highlighted in *Competition Commission of India v. Google LLC*,[27] where the Commission noted the structural imbalance between regulatory oversight and the market power exercised by global digital platforms. The CCI observed that opaque algorithms, cross-border data flows, and vertically integrated digital ecosystems significantly limit the effectiveness of domestic regulatory interventions, thereby creating enforcement gaps that directly impact user rights and market fairness.

E. NAVIGATING COMPETING GLOBAL MODELS

India must function in a digital ecosystem shaped by three main global governance models: the European Union's rights-protective framework, the United States' innovation-driven market system, and China's sovereignty-focused, state-controlled structure. Each model imposes its own normative expectations on topics like data flows, platform responsibility, encryption, and AI regulation.

For India, these disparities cause ongoing regulatory friction. Aligning too closely with the EU may impose enormous compliance obligations on growing companies;[28] leaning toward the United States may result in insufficient privacy and user rights protection; and replicating China's model would violate India's constitutional pledges to freedom and transparency.

The outcome is a strategic quandary: India must stay compatible with global frameworks for commerce, cybersecurity, and digital cooperation while still retaining its autonomy to govern in accordance with socioeconomic goals, democratic ideals, and developmental

[27] Umar Javeed v. Google LLC, Case No. 39 of 2018 (Competition Commission of India, Oct. 20, 2022)
[28] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020) https://academic.oup.com/book/36491

needs. This fragmented global context challenges policy coherence, slows reform, and necessitates a constant rethinking of India's digital constitutional agenda.

F. BALANCING NATIONAL SECURITY IMPERATIVES WITH DIGITAL RIGHTS

National security considerations have a significant impact on India's digital governance landscape, particularly in terms of encryption control, cross-border data access, foreign platform regulation, and cybersecurity preparation. While serious security concerns require strong state capability, tensions arise when wide statutory powers or opaque monitoring methods infringe on constitutionally protected rights like privacy, free expression, and procedural fairness. In the absence of public judicial scrutiny, clearly defined necessity-proportionality requirements, and independent audit systems, digital interventions justified by "security" risk becoming unchecked instruments of state authority.

This difficulty is exacerbated in the global internet governance context, where counter-terror frameworks, cyber-warfare rules, and geopolitical rivalry influence India's approach to data localization, intermediary regulation, and network control. The challenge is to create a mechanism that allows India to defend its digital borders while maintaining the constitutional promise of dignity, autonomy, and democratic accountability.

G. FRAGMENTED REGULATORY LANDSCAPE AND INSTITUTIONAL OVERLAPS

India's digital governance architecture is characterized by a patchwork of sectoral legislation, overlapping authorities, and conflicting policy mandates, resulting in tension between constitutional rights and administrative practices. Multiple authorities, including MeitY, TRAI, CERT-In, the Data Protection Board, and sector regulators, manage digital ecosystems, but there is no uniform constitutional or rights-based coordination framework. This fragmentation frequently leads to contradicting policies,

such as varying standards for data retention, encryption, and content moderation, leaving both citizens and platforms without a consistent rights-protective framework.

In the broader context of global internet governance, where harmonization and interoperability are critical, institutional inconsistency undermines India's negotiating position and hampers the adoption of international best practices. The lack of a coherent digital constitutional framework consequently becomes a structural challenge: rights may be recognized in theory but jeopardized in practice due to regulatory incoherence and administrative overreach.[29]

H. CAPACITY CONSTRAINTS AND TECHNOLOGICAL DEPENDENCY

India's aspiration for digital sovereignty is often hampered by a lack of domestic capacity in crucial technology fields such as semiconductor production, sophisticated AI models, cloud infrastructure, and cybersecurity tooling. This reliance on foreign technology, notably Big Tech platforms, global cloud service providers, and proprietary software ecosystems, results in a structural mismatch between rights protection and national security concerns. Even when constitutional principles require transparency and accountability, the technical architecture is nonetheless controlled by private or foreign entities, making enforcement impossible.

In the global internet governance domain, these capacity disparities limit India's ability to establish standards or assert norms without aligning with technologically dominant states. As a result, India finds itself in a catch-22: it wants to protect digital autonomy and user rights while remaining reliant on external systems that impact data flows, platform governance, and infrastructure decision-making. This dependence jeopardizes the establishment of a completely sovereign, constitutionally rooted digital environment.[30]

[29] Telecom Regulatory Authority of India (TRAI), *Recommendations on Privacy, Security and Ownership of Data in the Telecom Sector* (2018).
[30] Ministry of Electronics & Information Technology (MeitY), *National Strategy on Artificial Intelligence* (2023)

IX. FUTURE OUTLOOK AND SUGGESTIONS FOR IMPROVING DIGITAL CONSTITUTIONALISM IN INDIA

India's digital constitutionalism is in its early stages, shaped by judicial doctrines, legislative experimentation, and rapid technical change. To ensure that constitutional principles remain relevant in a globalized digital world, India need a forward-thinking, rights-centered, institutionally resilient strategy. The recommendations below provide a practical and normative roadmap:

A. STRENGTHENING THE PROPORTIONALITY FRAMEWORK IN ALL DIGITAL GOVERNANCE MEASURES

As India develops its digital legislation, whether in data protection, platform governance, cybersecurity, or AI oversight, it must incorporate a strict proportionality test into all policies and executive actions. The Puttaswamy (2017) decision established proportionality as a constitutional requirement, although its application remains inconsistent across multiple digital laws. To strengthen this framework, every restriction on privacy, speech, or autonomy must meet four conditions: a legitimate governmental objective, a rational relationship, necessity, and a stringent balance of rights with public interest.

A future-ready India should therefore require every new digital measure such as data access mandates, content takedown directives, or surveillance technologies to undergo transparent proportionality assessments. This will prevent regulatory overreach, ensure judicially reviewable standards, and promote a rights-respecting digital state. A strong proportionality culture ultimately aligns India with global constitutional best practices and enhances citizens' trust in digital governance.

B. BUILD INDEPENDENT AND EMPOWERED OVERSIGHT INSTITUTIONS

A future-ready digital constitutional framework for India requires strong, autonomous, and well-resourced oversight bodies that can check state power and ensure accountability in the digital domain. While India has established sectoral regulators such

as the Data Protection Board under the DPDP Act, their independence, functional autonomy, and capacity remain limited.

Strengthening digital governance demands institutions that are:

- Structurally independent from executive influence,
- Legally empowered with clear mandates for investigation, monitoring, and enforcement,
- Technically competent, with experts in AI, cybersecurity, data governance, and human rights, and
- Transparent and publicly accountable through regular reporting and review mechanisms.

Such bodies could oversee surveillance authorisations, algorithmic decision-making, digital ID systems, and platform regulation. An empowered oversight ecosystem similar to France's CNIL would not only safeguard constitutional rights but also foster public trust by ensuring that state digital initiatives remain lawful, proportionate, and rights-protective.

C. INVESTING IN DIGITAL LITERACY AND BRIDGING THE DIGITAL DIVIDE

For digital constitutionalism to succeed in India, citizens must be empowered to meaningfully exercise their digital rights. This is possible only when digital infrastructure, literacy, and access are equitably distributed. Despite rapid digital expansion, India still faces significant divides between rural-urban, gender-based, socio-economic, linguistic, and disability-related.

Investing in digital capabilities transforms citizens from mere users into rights-bearing digital participants, enabling them to demand accountability, identify harms, and participate in democratic digital governance. A digitally literate society thus becomes the

foundation of a constitutional culture that protects freedoms, strengthens participation, and reduces inequality in India's digital future.

D. DEVELOPING A COMPREHENSIVE CONSTITUTIONAL FRAMEWORK FOR AI

India should adopt a rights-anchored, constitutionally coherent framework that treats AI not merely as a technology to be regulated sector-by-sector, but as a systemic public law issue implicating fundamental rights, democratic governance, and distributional justice. Such a framework would translate digital constitutionalism into operational rules and institutions that govern design, deployment, oversight, and redress for AI systems across the public and private sectors.

E. PRESERVING FEDERALISM IN DIGITAL GOVERNANCE

Digital governance systems such as national digital identity systems, centralised data repositories, and platform-based welfare delivery tend to create technological centralisation, even in domains where States constitutionally retain significant competence (e.g., health, police, agriculture, local governance). Without deliberate safeguards, this "default centralisation" of digital infrastructures can dilute the autonomy of State governments and weaken local innovation.

A digital constitutionalist approach in India must therefore embed federal sensitivity into the design, deployment, and regulation of digital systems. It should treat federalism not merely as an administrative arrangement but as a structural constitutional value that shapes how digital power is allocated and exercised.

X. CONCLUSION

The evolving terrain of digital governance compels constitutional democracies to rethink how sovereignty, rights, and technological power interact. India's experience demonstrates the complexity of safeguarding constitutional values in a rapidly digitising environment where global platforms, transnational data flows, and extra-territorial regulatory regimes increasingly challenge the traditional boundaries of State authority.

At the same time, the Indian constitutional project grounded in dignity, equality, and federal balance faces pressures from centralising digital infrastructures, opaque algorithmic decision-making, and expansive surveillance capabilities. These developments raise fundamental questions about how constitutionalism can adapt to a domain where neither the State nor private actors operate within clear territorial limits.

The comparative lens of France offers valuable insights. France's rights-oriented digital regulatory trajectory, its robust data protection culture, and its assertive approach to platform governance illustrate how constitutional traditions can be mobilised to constrain digital power and articulate national sovereignty in a globalised technological ecosystem. While India and France differ in institutional histories and political economies, both grapple with similar tensions: asserting digital sovereignty without undermining individual freedoms, ensuring accountability of private intermediaries without stifling innovation, and navigating global internet governance without ceding constitutional autonomy.

Ultimately, the challenge for India is to develop a form of digital constitutionalism that is neither isolationist nor permissive, but one that balances sovereign regulatory authority with a rights-protective posture. This requires embedding constitutional principles federalism, privacy, due process, transparency, and democratic oversight into digital systems by design. It also demands active engagement in global governance forums, not merely as a participant but as a norm-entrepreneur shaping equitable, multi-stakeholder rules. Comparative experiences such as France underscore that constitutional resilience in the digital age is possible when legal systems are willing to innovate institutionally, scrutinize technological power, and reaffirm fundamental rights.

In this sense, the future of India's digital constitutionalism lies in constructing a framework that respects its democratic commitments while effectively negotiating the realities of a borderless internet. The task ahead is not only to regulate technology but to constitutionalise it to ensure that digital transformation strengthens, rather than diminishes, the promise of a rights-based and sovereign constitutional order.

 (ISSN: 2583-7753)

XI. REFERENCES

- Giovanni De Gregorio, Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society, 19 Int'l J. Const. L.
- Danielle Keats Citron & Frank Pasquale, "The Scored Society: Due Process for Automated Predictions," 89 Washington Law Review 1 (2014).
- United Nations Human Rights Council, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (2014).
- Working Group on Internet Governance, Report of the Working Group on Internet-Governance-10(2005),available-at https://www.itu.int/net/wsis/docs2/contributions/wgig/WGIG-report.pdf.
- NETmundial Multistakeholder Statement, Global Multistakeholder Meeting on the Future of Internet Governance (2014), https://netmundial.br
- Internet Engineering Task Force (IETF), Overview of the IETF, https://www.ietf.org/about
- Council of Europe Convention 108+: Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (2018)
- Rajbhar.Vivek Kumar, Digital Constitutionalism and Fundamental Rights: A Contemporary Legal Analysis, article published on vintage legal. https://www.vintagelegalvl.com/post/digital-constitutionalism-and-fundamental-rights-a-contemporary-legal-analysis
- Regulation (EU) 2022/2065 (Digital Services Act).
- La Quadrature du Net, Strategic Litigation Dossiers (2023).

- Internet Governance Forum (IGF), France – National and Regional Initiatives Report (2023).
- Council of Europe – Cybercrime Convention Committee (T-CY)https://www.coe.int/en/web/cybercrime/t-cy
- Internet Governance Forum (IGF), About the IGF (United Nations), https://www.intgovforum.org/en/about
- Anu Bradford, The Brussels Effect: How the European Union Rules the World (Oxford University Press 2020) https://academic.oup.com/book/36491
- Telecom Regulatory Authority of India (TRAI), Recommendations on Privacy, Security and Ownership of Data in the Telecom Sector (2018).
- Ministry of Electronics & Information Technology (MeitY), National Strategy on Artificial Intelligence (2023)